修復の設定

相関ポリシー違反の発生時に、FireSIGHT システムを設定して、1 つまたは複数の応答を開始できます。この中には、修復（Nmap スキャンの実行など）とさまざまなタイプのアラートが含まれます。

起動可能な最も基本的なタイプの応答はアラートです。アラートは電子メール、SNMP トラップ サーバ、または syslog によってポリシー違反をユーザに通知します。アラートの作成については、外部アラートの設定（43-1 ページ）を参照してください。

起動可能なもう 1 つの応答は修復です。修復はネットワーク トラフィックが相関ポリシーに違反したときに Defense Center が実行するプログラムです。FireSIGHT システムには出荷時に定義済みの修復が含まれています。この修復は、ポリシーの違反時にファイアウォールまたはルータでホストをブロックしたりホストをスキャンしたりするアクションを実行します。

Defense Center が修復を起動すると、修復ステータス イベントが生成されます。他のイベントと同様に修復ステータス イベントを検索、表示、および削除できます。

FireSIGHT システムはまた、相関ポリシー違反に応答するためのカスタム修復モジュールを作成できる柔軟な API を提供します。たとえば、Linux ベースのファイアウォールを実行している場合、相関ポリシーに違反するトラフィックをブロックするように、Linux サーバ上の `iptables` ファイルを動的に更新する修復モジュールを作成し、アップロードすることができます。独自の修復モジュールの作成に関する詳細については、『Cisco *Remediation API Guide*』を参照してください。

（注） 修復を設定および使用するには、Defense Center を使用する必要があります。

詳細については、以下を参照してください。

- 修復の作成（54-1 ページ）
- 修復ステータス イベントの使用（54-18 ページ）

修復の作成

TopicAlias=ModuleList

ライセンス：FireSIGHT

相関ポリシー違反を簡単に通知できるアラートに加えて、*修復*という応答を設定することもできます。修復は、相関ポリシー違反が発生したときに Defense Center が実行するプログラムです。これらのプログラムは、違反の原因となったイベントで提供される情報を使用して、特定のアクションを実行します。

FireSIGHT システムには出荷時に次のような複数の定義済み修復モジュールが含まれています。

- Cisco IOS ヌル ルート モジュール。Cisco IOS® バージョン 12.0 以降を使用する Cisco ルータが実行中の場合、相関ポリシーに違反する IP アドレスまたはネットワークに送信されるトラフィックを動的にブロックできます。

  詳細については、Cisco IOS ルータ用修復の設定（54-3 ページ）を参照してください。

- Cisco PIX Shun モジュール。Cisco PIX® ファイアウォール バージョン 6.0 以降を実行中の場合、相関ポリシーに違反する IP アドレスから送信されたトラフィックを動的にブロックできます。

  詳細については、Cisco PIX ファイアウォール用修復の設定（54-8 ページ）を参照してください。

- Nmap スキャン モジュール。特定のターゲットを能動的にスキャンし、そうしたホスト上で稼働中のオペレーティング システムおよびサーバを判別できます。

  詳細については、Nmap 修復の設定（54-12 ページ）を参照してください。

- セット属性値モジュール。相関イベントが発生するホストのホスト属性を設定できます。

  セット属性修復の構成（54-17 ページ）を参照してください。

各修復モジュールについて複数のインスタンスを作成できます。各インスタンスは特定のアプライアンスへの接続を表します。たとえば、修復を送信する Cisco IOS ルータが 4 台ある場合、Cisco IOS 修復モジュールのインスタンスを 4 つ設定する必要があります。

インスタンスを作成する際、Defense Center がアプライアンスとの接続を確立するために必要な設定情報を指定します。次に、設定済みの各インスタンスで、ポリシーに違反した場合にアプライアンスが実行するアクションを説明する修復を追加します。

修復を設定した後で、応答グループと呼ばれるものに追加するか、または相関ポリシー内のルールに個別に割り当てることができます。システムがこれらの修復を実行すると、修復ステータス イベントが生成されます。この中には、修復の名前、その原因となったポリシーとルール、および終了ステータス メッセージといった詳細が含まれます。これらのイベントの詳細については、修復ステータス イベントの使用（54-18 ページ）を参照してください。

Ciscoが提供するデフォルトのモジュールに加えて、ポリシー違反がトリガーとして使用したときに他の特定のタスクを実行する、カスタム修復モジュールを作成できます。独自の修復モジュールを作成し、Defense Center にインストールする方法の詳細については、『*Remediation API Guide*』を参照してください。カスタム モジュールをインストールする場合、[モジュール（Modules）] ページを使用して、新しいモジュールのインストール、表示、および削除を行うことができます。

新しいモジュールを Defense Center にインストールする方法:

アクセス: Admin/Discovery Admin

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

[モジュール（Modules）] ページが表示されます。

手順 2　[参照（Browse）] をクリックして、カスタム修復モジュールを含むファイルを保存した場所に移動します（詳細については『*Remediation API Guide*』を参照）。

手順 3　[Install（インストール）] をクリックします。

カスタム修復モジュールがインストールされます。

モジュールを Defense Center で表示または削除する方法:

アクセス: Admin/Discovery Admin

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

[モジュール(Modules)] ページが表示されます。

手順 2　次のいずれかの操作を実行します。

- [表示(View)] をクリックして、モジュールを表示します。

  [モジュールの詳細(Module Detail)] ページが表示されます。
- 削除するファイルの横の [削除(Delete)] をクリックします。Cisco で提供されるデフォルトのモジュールは削除**できません**。

  修復モジュールが削除されます。

Cisco IOS ルータ用修復の設定

ライセンス: FireSIGHT

Cisco では、相関ポリシーに違反した場合に、シスコの「null route」コマンドを使用して単一の IP アドレスまたはアドレスのブロック全体をブロックできる、Cisco IOS ヌル ルート修復モジュールを提供します。このモジュールは、相関ポリシーに違反したイベントに送信元または宛先ホストとして示された、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をルータのヌル インターフェイスに転送し、ドロップします(違反ホストまたはネットワーク**から**送信されたトラフィックはブロックされないことに注意してください)。

Cisco IOS ヌル ルート修復モジュールは Cisco IOS 12.0 以上を実行している Cisco ルータをサポートします。Cisco IOS 修復を実行するには、ルータに対してレベル 15 の管理アクセスを持っている必要があります。

(注)　宛先ベースの修復が機能するのは、接続イベントまたは侵入イベントに基づく相関ルールによってトリガーされたときに起動するように設定されている場合だけです。ディスカバリ イベントは送信元ホストのみを送信します。

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。ブロックされた IP アドレスまたはネットワークをルータから削除するには、ルータ自体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 を実行しているルータの修復を作成する方法:

アクセス: Admin/Discovery Admin

手順 1　Cisco ルータで Telnet を有効にします。

Telnet を有効にする方法の詳細については Cisco ルータまたは Cisco IOS ソフトウェアのマニュアルを参照してください。

手順 2　Defense Center で、Defense Center と共に使用する予定の各 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。

手順については、Cisco IOS インスタンスの追加(54-4 ページ)を参照してください。

手順 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特定の修復を作成します。

使用可能な修復の各タイプについて、次の項で説明しています。

- Cisco IOS ブロック宛先修復（54-5 ページ）
- Cisco IOS ブロック宛先ネットワーク修復（54-6 ページ）
- Cisco IOS ブロック送信元修復（54-7 ページ）
- Cisco IOS ブロック送信元ネットワーク修復（54-7 ページ）

手順 4　特定の相関ポリシー ルールに対する Cisco IOS 修復の割り当てを開始します。

Cisco IOS インスタンスの追加

ライセンス：FireSIGHT

Cisco IOS ルータで Telnet アクセスを設定した後で（Telnet アクセスを有効にする方法の詳細については Cisco ルータまたは Cisco IOS ソフトウェアのマニュアルを参照）、Defense Center にインスタンスを追加できます。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する必要があります。

Cisco IOS インスタンスを追加する方法：

アクセス：Admin/Discovery Admin

手順 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。

[インスタンス（Instances）] ページが表示されます。

手順 2　[新規インスタンスの追加（Add a New Instance）] リストから [Cisco IOS ヌル ルート (v1.0)（Cisco IOS Null Route (v1.0)）] を選択し、[追加（Add）] をクリックします。

[インスタンスの編集（Edit Instance）] ページが表示されます。

手順 3　[インスタンス名（Instance Name）] フィールドに、インスタンスの名前を入力します。

選択する名前には、スペースや特殊文字を含めず、説明的である必要があります。たとえば、複数の Cisco IOS ルータを接続する場合、複数のインスタンスがあるため、`IOS_01` および `IOS_02` などの名前を選択することをお勧めします。

手順 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。

手順 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。

手順 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。両方のフィールドに入力したパスワードが一致している必要があります。

手順 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。両方のフィールドに入力したパスワードが一致している必要があります。

手順 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 アドレスを 1 行につき 1 つ入力します。CIDR 表記または特定の IP アドレスを使用できます。たとえば、次のホワイトリストはシステムによって受け入れられます。

```
10.1.1.152
172.16.1.0/24
```

このホワイトリストは作成したコンプライアンスのホワイトリストに関連付けられていないことに注意してください。FireSIGHT システムでの CIDR 表記の使用法の詳細については、IP アドレスの表記規則（1-24 ページ）を参照してください。

手順 9　[作成（Create）] をクリックします。

インスタンスが作成され、ページの [設定された修復（Configured Remediations）] セクションに修復が表示されます。相関ポリシーで使用するために特定の修復を追加する必要があります。詳細については、次の各項を参照してください。

- Cisco IOS ブロック宛先修復（54-5 ページ）
- Cisco IOS ブロック宛先ネットワーク修復（54-6 ページ）
- Cisco IOS ブロック送信元修復（54-7 ページ）
- Cisco IOS ブロック送信元ネットワーク修復（54-7 ページ）

Cisco IOS ブロック宛先修復

ライセンス：FireSIGHT

Cisco IOS ブロック宛先修復により、ルータから相関イベントの宛先ホストに送信されるトラフィックをブロックできます。

（注）　ディスカバリ イベントに基づいた相関ルールに対する応答としてこの修復を使用**しない**でください。ディスカバリ イベントは送信元ホストのみを送信し、宛先ホストを送信しません。接続イベントまたは侵入イベントに基づいた相関ルールに応じてこの修復を使用できます。

修復を追加する方法：

アクセス：Admin/Discovery Admin

手順 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。

[インスタンス（Instances）] ページが表示されます。

手順 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。

インスタンスを追加したことがない場合は、Cisco IOS インスタンスの追加（54-4 ページ）を参照してください。

[インスタンスの編集（Edit Instance）] ページが表示されます。

手順 3　[設定された修復（Configured Remediations）] セクションで、[ブロック宛先（Block Destination）] を選択し、[追加（Add）] をクリックします。

[修復の編集（Edit Remediation）] ページが表示されます。

手順 4　[修復名（Remediation Name）] フィールドに修復の名前を入力します。

選択する名前には、スペースや特殊文字を含めず、説明的である必要があります。たとえば、Cisco IOS ルータが複数台あり、各インスタンスに複数の修復がある場合、`IOS_01_BlockDest` などの名前を指定することお勧めします。

手順 5　必要に応じて、[宛先（Description）] フィールドに、修復の説明を入力します。

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

修復が追加されます。

Cisco IOS ブロック宛先ネットワーク修復

ライセンス: FireSIGHT

Cisco IOS ブロック宛先ネットワーク修復により、ルータから相関イベントの宛先ホストのネットワークに送信されるすべてのトラフィックをブロックできます。

(注) ディスカバリ イベントに基づいた相関ルールに対する応答としてこの修復を使用**しない**でください。ディスカバリ イベントは送信元ホストのみを送信し、宛先ホストを送信しません。接続イベントまたは侵入イベントに基づいた相関ルールに応じてこの修復を使用できます。

修復を追加する方法:

アクセス: Admin/Discovery Admin

手順 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。

[インスタンス(Instances)] ページが表示されます。

手順 2 修復を追加するインスタンスの横で、[表示(View)] をクリックします。

インスタンスを追加したことがない場合は、Cisco IOS インスタンスの追加(54-4 ページ)を参照してください。

[インスタンスの編集(Edit Instance)] ページが表示されます。

手順 3 [設定された修復(Configured Remediations)] セクションで、[ブロック宛先ネットワーク(Block Destination Network)] を選択し、[追加(Add)] をクリックします。

[修復の編集(Edit Remediation)] ページが表示されます。

手順 4 [修復名(Remediation Name)] フィールドに修復の名前を入力します。

選択する名前には、スペースや特殊文字を含めず、説明的である必要があります。たとえば、Cisco IOS ルータが複数台あり、各インスタンスに複数の修復がある場合、`IOS_01_BlockDestNet` などの名前を指定することお勧めします。

手順 5 必要に応じて、[宛先(Description)] フィールドに、修復の説明を入力します。

手順 6 [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。

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

修復が追加されます。

Cisco IOS ブロック送信元修復

ライセンス：FireSIGHT

Cisco IOS ブロック送信元修復により、ルータから、相関ポリシーに違反する相関イベントに含まれている送信元ホストに送信される、すべてのトラフィックをブロックできます。送信元ホストは、相関ルールに基づいた接続イベントまたは侵入イベントの送信元 IP アドレス、またはディスカバリ イベントのホスト IP アドレスです。

修復を追加する方法：

アクセス：Admin/Discovery Admin

手順 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。

[インスタンス（Instances）] ページが表示されます。

手順 2　修復を追加するインスタンスの横で、[表示（View）] をクリックします。

インスタンスを追加したことがない場合は、Cisco IOS インスタンスの追加（54-4 ページ）を参照してください。

[インスタンスの編集（Edit Instance）] ページが表示されます。

手順 3　[設定された修復（Configured Remediations）] セクションで、[ブロック送信元（Block Source）] を選択し、[追加（Add）] をクリックします。

[修復の編集（Edit Remediation）] ページが表示されます。

手順 4　[修復名（Remediation Name）] フィールドに修復の名前を入力します。

選択する名前には、スペースや特殊文字を含めず、説明的である必要があります。たとえば、Cisco IOS ルータが複数台あり、各インスタンスに複数の修復がある場合、`IOS_01_BlockSrc` などの名前を指定することお勧めします。

手順 5　必要に応じて、[宛先（Description）] フィールドに、修復の説明を入力します。

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

修復が追加されます。

Cisco IOS ブロック送信元ネットワーク修復

ライセンス：FireSIGHT

Cisco IOS ブロック送信元ネットワーク修復により、ルータから相関イベントの送信元ホストのネットワークに送信されるすべてのトラフィックをブロックできます。送信元ホストは、相関ルールに基づいた接続イベントまたは侵入イベントの送信元 IP アドレス、またはディスカバリ イベントのホスト IP アドレスです。

修復を追加する方法：

アクセス：Admin/Discovery Admin

手順 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。

[インスタンス（Instances）] ページが表示されます。

手順 2　修復を追加するインスタンスの横で、[表示（View）] をクリックします。

インスタンスを追加したことがない場合は、Cisco IOS インスタンスの追加（54-4 ページ）を参照してください。

[インスタンスの編集（Edit Instance）] ページが表示されます。

手順 3　[設定された修復（Configured Remediations）] セクションで、[ブロック送信元ネットワーク（Block Source Network）] を選択し、[追加（Add）] をクリックします。

[修復の編集（Edit Remediation）] ページが表示されます。

手順 4　[修復名（Remediation Name）] フィールドに修復の名前を入力します。

選択する名前には、スペースや特殊文字を含めず、説明的である必要があります。たとえば、Cisco IOS ルータが複数台あり、各インスタンスに複数の修復がある場合、`IOS_01_BlockSourceNet` などの名前を指定することお勧めします。

手順 5　必要に応じて、[宛先（Description）] フィールドに、修復の説明を入力します。

手順 6　[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。

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

修復が追加されます。

Cisco PIX ファイアウォール用修復の設定

ライセンス：FireSIGHT

Cisco は、シスコの「shun」コマンドを使用して IP アドレスまたはネットワークをブロックできる、Cisco PIX Shun 修復モジュールを提供します。これは、相関ポリシーに違反した送信元ホストまたは宛先ホストのいずれかから送信されるすべてのトラフィックをブロックし、現行の接続をすべて閉じます（ファイアウォールを介してホストに送信されるトラフィックはブロックされないことに注意してください）。

Cisco PIX Shun 修復モジュールは Cisco PIX ファイアウォール 6.0 以上をサポートします。Cisco PIX 修復を起動するにはレベル 15 以上の管理アクセスが必要です。

（注）　宛先ベースの修復が機能するのは、接続イベントまたは侵入イベントに基づく相関ルールによってトリガーされたときに起動するように設定されている場合だけです。ディスカバリ イベントは送信元ホストのみを送信します。

注意　Cisco PIX 修復がアクティブになる際、タイムアウト期間は使用されません。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、手動でファイアウォールのルールを削除する必要があります。

Cisco PIX ファイアウォール用の修復を作成する方法:

アクセス: Admin/Discovery Admin

手順 1　ファイアウォール上で Telnet または SSH を有効にします（Cisco は SSH を推奨します）。

SSH または Telnet を有効にする方法の詳細については Cisco PIX ファイアウォールのマニュアルを参照してください。

手順 2　Defense Center で、Defense Center と共に使用する予定の各 Cisco PIX ファイアウォールに対する Cisco PIX Shun インスタンスを追加します。

手順については、Cisco PIX インスタンスの追加（54-9 ページ）を参照してください。

手順 3　相関ポリシーに違反した場合にファイアウォールで実現する応答のタイプに基づき、インスタンスごとに特定の修復を作成します。

使用可能な修復タイプは次の項で説明されています。

- Cisco PIX ブロック宛先修復（54-10 ページ）
- Cisco PIX ブロック送信元修復（54-11 ページ）

手順 4　特定の相関ポリシー ルールに対する Cisco PIX 修復の割り当てを開始します。

Cisco PIX インスタンスの追加

ライセンス: FireSIGHT

Cisco PIX ファイアウォールで SSH または Telnet を設定した後で、Defense Center にインスタンスを追加できます。修復を送信するファイアウォールが複数ある場合は、各ファイアウォールに対して別々のインスタンスを作成する必要があります。

（注）　Cisco は、Telnet 接続の代わりに SSH 接続を使用することを推奨します。SSH を使用して送信されるデータは暗号化されるので、Telnet よりもはるかに安全です。

Cisco PIX インスタンスを追加する方法:

アクセス: Admin/Discovery Admin

手順 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。

[インスタンス（Instances）] ページが表示されます。

手順 2　[新規インスタンスの追加（Add a New Instance）] リストから、[Cisco PIX Shun（Cisco PIX Shun）] を選択し、[追加（Add）] をクリックします。

[インスタンスの編集（Edit Instance）] ページが表示されます。

手順 3　[インスタンス名（Instance Name）] フィールドに、インスタンスの名前を入力します。

選択する名前には、スペースや特殊文字を含めず、説明的である必要があります。たとえば、複数の Cisco ファイアウォールを接続する場合、複数のインスタンスがあるため、`PIX_01`、`PIX_02` などの名前を選択することをお勧めします。

手順 4　オプションで、[宛先（Description）] フィールドに、インスタンスの説明を入力します。

手順 5　[PIX IP] フィールドに、修復のために使用する Cisco PIX ファイアウォールの IP アドレスを入力します。

手順 6　デフォルト（pix）以外の特定のユーザ名が必要な場合は、[ユーザ名（Username）] フィールドに入力します。

手順 7　[接続パスワード（Connection Password）] フィールドに、SSH または Telnet を使用してファイアウォールに接続するためのパスワードを入力します。両方のフィールドに入力したパスワードが一致している必要があります。

手順 8　[イネーブル パスワード（Enable Password）] フィールドに、SSH または Telnet のイネーブル パスワードを入力します。これは、ファイアウォールの特権モードに入るために使用するパスワードです。両方のフィールドに入力したパスワードが一致している必要があります。

手順 9　[ホワイトリスト（White List）] フィールドに、修復から除外する IP アドレスを 1 行につき 1 つ入力します。CIDR 表記または特定の IP アドレスを使用できます。たとえば、次のホワイトリストはシステムによって受け入れられます。

```
10.1.1.152
192.168.1.0/255.255.255.0
172.16.1.0/24
```

このホワイトリストは作成したコンプライアンスのホワイトリストに関連付けられていないことに注意してください。FireSIGHT システムでの CIDR 表記の使用法の詳細については、IP アドレスの表記規則（1-24 ページ）を参照してください。

手順 10　[プロトコル（Protocol）] リストから、ファイアウォールに接続するために使用する方式を選択します。

手順 11　[作成（Create）] をクリックします。

インスタンスが作成され、ページの [設定された修復（Configured Remediations）] セクションに修復が表示されます。相関ポリシーで使用するために特定の修復を追加する必要があります。詳細については、次の各項を参照してください。

- Cisco PIX ブロック宛先修復（54-10 ページ）
- Cisco PIX ブロック送信元修復（54-11 ページ）

Cisco PIX ブロック宛先修復

ライセンス：FireSIGHT

Cisco PIX ブロック宛先修復により、相関イベントの宛先ホストから送信されるトラフィックをブロックできます。

（注）　ディスカバリ イベントに基づいた相関ルールに対する応答としてこの修復を使用**しない**でください。ディスカバリ イベントは送信元ホストのみを送信し、宛先ホストを送信しません。接続イベントまたは侵入イベントに基づいた相関ルールに応じてこの修復を使用できます。

修復を追加する方法：

アクセス：Admin/Discovery Admin

手順 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。

[インスタンス（Instances）] ページが表示されます。

手順 2　修復を追加するインスタンスの横で、[表示（View）] をクリックします。

インスタンスを追加したことがない場合は、Cisco PIX インスタンスの追加（54-9 ページ）を参照してください。

[インスタンスの編集(Edit Instance)] ページが表示されます。

手順 3　[設定された修復(Configured Remediations)] セクションで、[ブロック宛先(Block Destination)] を選択し、[追加(Add)] をクリックします。

[修復の編集(Edit Remediation)] ページが表示されます。

手順 4　[修復名(Remediation Name)] フィールドに修復の名前を入力します。

選択する名前には、スペースや特殊文字を含めず、説明的である必要があります。たとえば、Cisco PIX ファイアウォールが複数台あり、各インスタンスに複数の修復がある場合、`PIX_01_BlockDest` などの名前を指定することお勧めします。

手順 5　必要に応じて、[宛先(Description)] フィールドに、修復の説明を入力します。

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

修復が追加されます。

Cisco PIX ブロック送信元修復

ライセンス: FireSIGHT

Cisco PIX ブロック送信元修復により、相関ポリシーに違反するイベントに含まれる送信元ホストから送信されるすべてのトラフィックをブロックできます。送信元ホストは、相関ルールに基づいた接続イベントまたは侵入イベントの送信元 IP アドレス、またはディスカバリ イベントのホスト IP アドレスです。

修復を追加する方法:

アクセス: Admin/Discovery Admin

手順 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。

[インスタンス(Instances)] ページが表示されます。

手順 2　修復を追加するインスタンスの横で、[表示(View)] をクリックします。

インスタンスを追加したことがない場合は、Cisco PIX インスタンスの追加(54-9 ページ)を参照してください。

[インスタンスの編集(Edit Instance)] ページが表示されます。

手順 3　[設定された修復(Configured Remediations)] セクションで、[ブロック送信元(Block Source)] を選択し、[追加(Add)] をクリックします。

[修復の編集(Edit Remediation)] ページが表示されます。

手順 4　[修復名(Remediation Name)] フィールドに修復の名前を入力します。

選択する名前には、スペースや特殊文字を含めず、説明的である必要があります。たとえば、Cisco PIX ファイアウォールが複数台あり、各インスタンスに複数の修復がある場合、`PIX_01_BlockSrc` などの名前を指定することお勧めします。

手順 5　必要に応じて、[宛先(Description)] フィールドに、修復の説明を入力します。

修復が追加されます。

Nmap 修復の設定

ライセンス：FireSIGHT

トリガー イベントが発生したホストをスキャンすることにより、相関イベントに応答できます。相関イベントをトリガーとして使用したイベントからポートのみをスキャンすることができます。

相関イベントに応じて Nmap スキャンをセットアップするには、最初に Nmap スキャン インスタンスを作成してから Nmap スキャン修復を追加する必要があります。その後、ポリシー内のルールの違反に対する応答として Nmap スキャンを設定できます。

次の項を参照してください。

- Nmap スキャン インスタンスの追加（54-12 ページ）
- Nmap スキャン修復（54-13 ページ）

Nmap スキャン インスタンスの追加

ライセンス：FireSIGHT

ネットワーク上のホストのオペレーティング システムおよびサーバの情報をスキャンするために使用する、Nmap の各モジュールに対して個別のスキャン インスタンスをセットアップできます。スキャン インスタンスのセットアップは、Defense Center のローカルの Nmap モジュールおよびスキャンをリモートから実行するために使用する任意の管理対象デバイスに対して行うことができます。各スキャンの結果は、リモートの管理対象デバイスからスキャンを実行した場合であっても、スキャンを設定する Defense Center に常に保存されます。ミッション クリティカルなホストへの不慮のスキャンや悪意のあるスキャンを防ぐには、インスタンスのブラックリストを作成し、そのインスタンスで決してスキャンしてはならないホストを指示できます。

既存のスキャン インスタンスと同じ名前のスキャン インスタンスを追加できないことに注意してください。

スキャン インスタンスを作成する方法：

アクセス：Admin/Discovery Admin

手順 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。

[インスタンス（Instances）] ページが表示されます。

手順 2　[モジュール タイプの追加（Add a module type）] ドロップダウン リストから、[Nmap 修復 (v1.0)（Nmap Remediation (v1.0)）] を選択し、[追加（Add）] をクリックします。

[インスタンスの編集（Edit Instance）] ページが表示されます。

手順 3　[インスタンス名（Instance Name）] フィールドに、1 文字から 63 文字の英数字の名前を入力します。アンダースコア（_）とハイフン（-）以外の特殊文字およびスペースは使用できません。

手順 4　[説明（Description）] フィールドに、スペースと特殊文字を含む、0 ～ 255 文字の英数字を使用して説明を指定します。

手順 5　オプションで、[ブラックリスト化されたスキャン ホスト（Black Listed Scan hosts）] フィールドで、このスキャン インスタンスがスキャン*しない*ホストまたはネットワークを指定します。

- IPv6 ホストの場合、厳密な IP アドレス（`2001:DB8::fedd:eeff` など）
- IPv4 ホストの場合、厳密な IP アドレス（`192.168.1.101` など）または CIDR 表記を使用した IP アドレス ブロック（たとえば、`192.168.1.0/24` は、両端を含めて `192.168.1.1` から `192.168.1.254` の間の 254 個のホストをスキャンします）

ブラックリストに含まれるネットワーク内のホストをスキャン対象として特定すると、スキャンは実行されません。FireSIGHT システムでの CIDR 表記の使用法の詳細については、IP アドレスの表記規則（1-24 ページ）を参照してください。

手順 6　オプションで、Defense Center の代わりに、リモートの管理対象デバイスからスキャンするには、[リモート デバイス名（Remote Device Name）] フィールドで管理対象デバイスの名前または IP アドレスを指定します。

手順 7　[作成（Create）] をクリックします。

スキャン インスタンスが作成されます。

Nmap スキャン修復

ライセンス：FireSIGHT

Nmap 修復を作成して、Nmap スキャンの設定を定義できます。Nmap 修復は、相関ポリシー内で応答として使用したり、オン デマンドで実行したり、特定の時間に実行するようにスケジュールしたりできます。Nmap スキャンの結果をネットワーク マップ内に表示するには、スキャン対象のホストがネットワーク マップ内にすでに存在していなければなりません。ホスト入力機能である NetFlow とシステム自体がホストをネットワーク マップに追加できることに注意してください。

Nmap 修復の具体的な設定について詳しくは、Nmap 修復の概要（47-2 ページ）を参照してください。

Nmap により提供されるサーバやオペレーティング システムのデータは、もう一度 Nmap スキャンを実行するまで静的な状態のままであることに注意してください。Nmap を使用してホスト内でオペレーティング システムやサーバのデータをスキャンすることを計画している場合は、定期的なスキャンのスケジュールをセットアップして、Nmap によって提供されるオペレーティング システムやサーバのデータを最新に保つこともできます。詳細については、Nmap スキャンの自動化（62-5 ページ）を参照してください。ホストがネットワーク マップから削除されると、そのホストに関する Nmap スキャン結果は破棄されることにも注意してください。

Nmap の機能に関する一般情報については、http://insecure.org にある Nmap のマニュアルを参照してください。

Nmap 修復を作成する方法：

アクセス：Admin/Discovery Admin

手順 1　[ポリシー（Policies）] > [アクション（Actions）] > [スキャナ（Scanners）] を選択します。

[スキャナ（Scanners）] ページが表示されます。

手順 2　修復を追加するスキャン インスタンスの隣の [修復の追加（Add Remediation）] をクリックします。

[修復の編集（Edit Remediation）] ページが表示されます。

手順 3　[修復名（Remediation Name）] フィールドに、1 文字から 63 文字の英数字を使用して修復の名前を入力します。アンダースコア（_）とハイフン（-）以外の特殊文字およびスペースは使用できません。

手順 4　[説明（Description）] フィールドに、0 文字から 255 文字の英数字を使用して修復の説明を入力します。スペースや特殊文字を使用できます。

手順 5　侵入イベント、接続イベント、またはユーザ イベントでトリガーとして使用する相関ルールに応じてこの修復を使用する場合は、[イベントに基づくアドレスのスキャン（Scan Which Address(es) From Event?）] オプションを設定します。

- イベントの送信元 IP アドレスと宛先 IP アドレスによって表されるホストをスキャンするには、[送信元および宛先アドレスのスキャン（Scan Source and Destination Addresses）] を選択します。
- イベントの送信元 IP アドレスによって表されるホストをスキャンするには、[送信元アドレスのみのスキャン（Scan Source Address Only）] を選択します。
- イベントの宛先 IP アドレスによって表されるホストをスキャンするには、[宛先アドレスのみのスキャン（Scan Destination Address Only）] を選択します。

ディスカバリ イベントまたはホスト入力イベントに対してトリガーする相関ルールへの応答としてこの修復を使用する計画の場合は、デフォルトでそのイベントに関連するホストの IP アドレスが修復によってスキャンされます。このオプションを設定する必要はありません。

（注）　トラフィック プロファイルの変更でトリガーとして使用する相関ルールへの応答として Nmap 修復を割り当て**ない**でください。

手順 6　次のように、[スキャン タイプ（Scan type）] オプションを設定します。

- TCP 接続を開始して完了していない状態で、`admin` アカウントが raw パケット アクセス権を持つホストや IPv6 が実行されていないホスト上でステルス モードですばやくスキャンするには、[TCP Syn スキャン（TCP Syn Scan）] を選択します。
- システム コール `connect()`（Defense Center 上の `admin` アカウントが raw パケット アクセス権を持っていないホストや IPv6 が実行されているホスト上で使用できる）を使用してスキャンするには、[TCP Connect スキャン（TCP Connect Scan）] を選択します。
- ACK パケット送信して、ポートがフィルタ処理されているかどうか検査するには、[TCP ACK スキャン（TCP ACK Scan）] を選択します。
- ポートがフィルタリングされているかどうかを確認し、ポートが開いているか閉じているかも判別するために ACK パケットを送信するには、[TCP Window スキャン（TCP Window Scan）] を選択します。
- FIN/ACK プローブを使用して BSD 派生システムを識別するには、[TCP Maimon スキャン（TCP Maimon Scan）] を選択します。

手順 7　オプションで、TCP ポートに加えて UDP ポートをスキャンするには、[UDP ポートのスキャン（Scan for UDP ports）] オプションで [オン（On）] を選択します。

ヒント　UDP ポートスキャンは TCP ポートスキャンよりも時間がかかります。スキャン時間を短縮するには、このオプションを無効のままにします。

手順 8　相関ポリシー違反への応答としてこの修復を使用する計画の場合は、[イベントからのポートを使用（Use Port From Event）] を以下のように設定します。

- 相関イベント内のポートをスキャンし、ステップ 12 で指定するポートをスキャンしない場合は、[オン（On）] を選択します。

  相関イベント内のポートをスキャンする場合は、ステップ 8 で指定した IP アドレス上のポートが修復によりスキャンされることに注意してください。これらのポートも修復の動的スキャンのターゲットに追加されます。
- ステップ 12 で指定するポートのみスキャンするには、[オフ（Off）] を選択します。

手順 9　相関ポリシー違反への応答としてこの修復を使用する計画で、イベントを検出した検出エンジンを実行しているアプライアンスを使用してスキャンを実行するには、[レポート検出エンジンからスキャン（Scan from reporting detection engine）] オプションを以下のように設定します。

- レポート検出エンジンを実行しているアプライアンスからスキャンするには、[オン（On）] を選択します。
- 修復内で設定されているアプライアンスからスキャンするには、[オフ（Off）] を選択します。

手順 10　[高速ポート スキャン（Fast Port Scan）] オプションを以下のように設定します。

- スキャンを実行する管理対象デバイスの `/var/sf/nmap/share/nmap/nmap-services` ディレクトリにある `nmap-services` ファイルに記述されたポートのみをスキャンし、他のポート設定を無視するには、[オン（On）] を選択します。
- すべての TCP ポートをスキャンするには、[オフ（Off）] を選択します。

手順 11　[ポート範囲とスキャン順序（Port Ranges and Scan Order）] フィールドに、デフォルトでスキャンするポートを入力します。Nmap 構文を使用し、ポートをスキャンする順序で入力します。

1 から 65535 までの値を指定します。ポートを区切るには、カンマかスペースを使用します。ハイフンを使用してポートの範囲を指示することもできます。TCP ポートと UDP ポートの両方ともスキャンする場合は、スキャン対象の TCP ポートのリストの先頭に T を挿入し、UDP ポートのリストの先頭に U を挿入します。たとえば UDP トラフィックのポート 53 と 111 をスキャンしてから TCP トラフィックのポート 21 ～ 25 をスキャンするのであれば `U:53,111,T:21-25` と入力します。

ステップ 8 で説明されているように、相関ポリシー違反への応答として修復が起動する場合には、[イベントからのポートを使用（Use Port From Event）] オプションによりこの設定が上書きされることに注意してください。

手順 12　サーバ ベンダーおよびバージョン情報に関して開いているポートをプローブするには、[ベンダーおよびバージョン情報に関するオープン ポートのプローブ（Probe open ports for vendor and version information）] を設定します。

- ホスト上のオープン ポートでサーバ情報をスキャンして、サーバ ベンダーとバージョンを識別するには、[オン（On）] を選択します。
- ホストのサーバ情報を使用して続行するには、[オフ（Off）] を選択します。

手順 13　オープン ポートの調査を選択する場合は、[サーバ バージョン強度（Service Version Intensity）] ドロップダウン リストから数値を選択して、使用するプローブの数を設定します。

- 選択する数値が大きいほど使用するプローブの数が増えるので、スキャンは長時間になり精度が上がります。
- 選択する数値が小さいほど、使用するプローブの数が減るので、スキャンは高速になり精度が下がります。

手順 14　オペレーティング システム情報をスキャンするには、[オペレーティング システムの検出（Detect Operating System）] を以下のように設定します。

- ホストに対してオペレーティング システムを識別する情報をスキャンするには、[オン（On）] を選択します。
- ホストのオペレーティング システム情報を使用して続行するには、[オフ（Off）] を選択します。

手順 15 ホスト ディスカバリが発生するかどうか、および使用可能なホストに対してのみポート スキャンが実行されるかどうかを判別するには、[すべてのホストをオンラインとして処理（Treat All Hosts As Online）] を設定します。

- ホスト ディスカバリ プロセスを省略し、ターゲット範囲内のすべてのホスト上でのポート スキャンを実行するには、[オン（On）] を選択します。
- [ホスト ディスカバリ方式（Host Discovery Method）] と [ホスト ディスカバリ ポート リスト（Host Discovery Port List）] の設定を使用してホスト ディスカバリを実行し、使用不能なホスト上でのポート スキャンを省略するには、[オフ（Off）] を選択します。

手順 16 ホストが存在していて利用可能であるかどうかを Nmap がテストする際に使用する方式を以下から選択します。

- SYN フラグが設定された空の TCP パケットを送信し、使用可能なホスト上のクローズ ポート上の RST 応答かオープン ポート上の SYN/ACK 応答を引き起こすには、[TCP SYN] を選択します。

  このオプションはデフォルトでポート 80 をスキャンすることと、TCP SYN スキャンはステートフル ファイアウォール ルールが指定されたファイアウォールでブロックされる可能性が低いことに注意してください。
- ACK フラグが設定された空の TCP パケットを送信し、使用可能なホスト上の RST 応答を引き起こすには、[TCP ACK] を選択します。

  このオプションはデフォルトでポート 80 をスキャンすることと、TCP ACK スキャンはステートレス ファイアウォール ルールが指定されたファイアウォールでブロックされる可能性が低いことに注意してください。
- UDP パケットを送信し、使用可能なホスト上のクローズ ポートからのポート到達不能応答を引き起こすには、[UDP] を選択します。このオプションは、デフォルトでポート 40125 をスキャンします。

手順 17 ホスト ディスカバリ時にポートのカスタム リストをスキャンする場合は、[ホスト ディスカバリ ポート リスト（Host Discovery Port List）] に、選択したホストのディスカバリ方法に適したポートのリストをカンマで区切って入力します。

手順 18 ホスト ディスカバリを行い、サーバ、オペレーティング システム、脆弱性 のディスカバリを行う Nmap スクリプトのデフォルト セットを使用するかどうかを制御するには、[デフォルト NSE スクリプト（Default NSE Scripts）] オプションを以下のように設定します。

- Nmap スクリプトのデフォルト セットを実行するには、[オン（On）] を選択します。
- Nmap スクリプトのデフォルト セットを省略するには、[オフ（Off）] を選択します。

デフォルト スクリプトのリストについては、http://nmap.org/nsedoc/categories/default.html を参照してください。

手順 19 スキャン プロセスのタイミングを設定するには、タイミングのテンプレート番号を選択します。選択する数値が大きいほどスキャンは高速で幅が狭くなり、小さいほどスキャンは低速で包括的になります。

手順 20 [保存（Save）] をクリックし、[完了（Done）] をクリックします。

修復が作成されます。

セット属性修復の構成

ライセンス：FireSIGHT

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、相関イベントに応答できます。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することを選択できます。ホスト属性の詳細については、事前定義のホスト属性の使用（49-34 ページ）および ユーザ定義のホスト属性の使用（49-35 ページ）を参照してください。

相関イベントへの応答として属性値を設定するには、まず属性設定インスタンスを作成してからセット属性の修復を追加します。その後、ポリシー内のルールの違反に対する応答として属性値更新を設定できます。

詳細については、次の項を参照してください。

- セット属性値インスタンスの追加（54-17 ページ）
- セット属性値修復（54-17 ページ）

セット属性値インスタンスの追加

ライセンス：FireSIGHT

相関ルール違反への応答として、属性値を設定するインスタンスを設定できます。

セット属性インスタンスを作成する方法：

アクセス：Admin/Discovery Admin

手順 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。

[インスタンス（Instances）] ページが表示されます。

手順 2　[モジュール タイプの追加（Add a module type）] ドロップダウン リストから、[セット属性値（v1.0）（Set Attribute Value (v1.0)）] を選択し、[追加（Add）] をクリックします。

[インスタンスの編集（Edit Instance）] ページが表示されます。

手順 3　[インスタンス名（Instance Name）] フィールドに、1 文字から 63 文字の英数字の名前を入力します。アンダースコア（_）とハイフン（-）以外の特殊文字およびスペースは使用できません。

手順 4　[説明（Description）] フィールドに、スペースと特殊文字を含む、0 ～ 255 文字の英数字を使用して説明を指定します。

手順 5　[作成（Create）] をクリックします。

インスタンスが作成されます。

セット属性値修復

ライセンス：FireSIGHT

相関ルール違反への応答として設定する各属性値のセット属性値修復を作成できます。設定する属性がテキスト属性の場合、イベントの説明を属性値として使用する修復を設定できます。

セット属性値修復を作成する方法:

アクセス: Admin/Discovery Admin

手順 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。

[インスタンス(Instances)] ページが表示されます。

手順 2　修復を追加するスキャン インスタンスの横の [表示(View)] をクリックします。

[インスタンスの編集(Edit Instance)] ページが表示されます。

手順 3　[新規修復タイプの追加(Add a new remediation of type)] ドロップダウン リストから [セット属性値(Set Attribute Value)] を選択します。

[修復の編集(Edit Remediation)] ページが表示されます。

手順 4　[修復名(Remediation Name)] フィールドに、1 文字から 63 文字の英数字を使用して修復の名前を入力します。アンダースコア(_)とハイフン(-)以外の特殊文字およびスペースは使用できません。

手順 5　[説明(Description)] フィールドに、0 文字から 255 文字の英数字を使用して修復の説明を入力します。スペースや特殊文字を使用できます。

手順 6　侵入イベント、ユーザ イベント、または接続イベントで発生する相関ルールへの応答としてこの修正を使用する場合は、[イベントに基づくホストの更新(Update Which Host(s) From Event)] オプションを設定します。

- [送信元および宛先ホストの更新(Update Source and Destination Hosts)] を選択して、イベントの送信元 IP アドレスと宛先 IP アドレスによって表されるホストの属性値を更新します。
- [送信元ホストのみの更新(Update Source Host Only)] を選択して、イベントの送信元 IP アドレスで表されるホストの属性値を更新します。
- [宛先ホストのみの更新(Update Destination Host Only)] を選択して、イベントの宛先 IP アドレスで表されるホストの属性値を更新します。

ディスカバリ イベントまたはホスト入力イベントに対してトリガーする相関ルールへの応答としてこの修復を使用する計画の場合は、デフォルトでそのイベントに関連するホストの IP アドレスが修復によってスキャンされます。このオプションを設定する必要はありません。

手順 7　[イベントの説明を属性値に使用(テキスト属性のみ)(Use Description From Event For Attribute Value (text attributes only))] オプションを設定します。

- イベントの説明を属性値として使用するには、[オン(On)] を選択します。
- 修復の [属性値(Attribute Value)] 設定を属性値として使用するには、[オン(Off)] を選択します。

手順 8　イベントの説明を使用しない場合は、[属性値(Attribute Value)] フィールドに、設定する属性値を入力します。

手順 9　[保存(Save)] をクリックし、[完了(Done)] をクリックします。

修復が作成されます。

修復ステータス イベントの使用

ライセンス: FireSIGHT

修復がトリガーとして使用すると、修復ステータス イベントが生成されます。これらのイベントはデータベースに記録され、[修復ステータス(Remediation Status)] ページで確認できます。修復ステータス イベントの検索、表示、および削除を行うことができます。

詳細については、以下を参照してください。

- イベント時間の制約の設定（58-27 ページ）
- 修復ステータス イベントの検索（54-23 ページ）

修復ステータス イベントの表示

ライセンス：FireSIGHT

修復ステータス イベントにアクセスするときに表示されるページは、使用するワークフローにより異なります。修復のテーブル ビューを含む定義済みワークフローを使用できます。テーブル ビューには、各修復ステータス イベントの行が含まれます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。カスタム ワークフローの作成方法については、カスタム ワークフローの作成（58-44 ページ）を参照してください。

次の表では、修復ステータス イベント ワークフローのページで実行できる具体的なアクションの一部を説明します。

表 54-1　修復ステータス イベントの表示オプション

目的	操作
表示された列の詳細を表示する	修復ステータス テーブルについて（54-21 ページ）で詳細を参照してください。
表示されたイベントの時刻と日付の範囲を変更する	イベント時間の制約の設定（58-27 ページ）を参照してください。 イベント ビューを時間によって制約している場合は、（グローバルかイベントに特有かに関係なく）アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベント ビューに表示されることがあることに注意してください。これは、アプライアンスのスライドの時間範囲を設定しても発生する可能性があります。
イベントをソートして制限する	イベントの制約（58-35 ページ）およびドリルダウン ワークフロー ページのソート（58-39 ページ）を参照してください。
一時的に他のワークフローを使用する	ワークフローのタイトルの横の [（ワークフローの切り替え）（(switch workflow)）] をクリックします。詳細については、ワークフローの選択（58-19 ページ）を参照してください。
相関イベントのビューへ移動して、関連するイベントを表示する	[相関イベント（Correlation Events）] をクリックします。詳細については、ワークフロー間のナビゲート（58-41 ページ）を参照してください。
すぐに再表示できるように、現在のページをブックマークする	[このページをブックマーク（Bookmark This Page）] をクリックします。詳細については、ブックマークの使用（58-42 ページ）を参照してください。
ブックマークの管理ページへ移動する	[ブックマークの表示（View Bookmarks）] をクリックします。詳細については、ブックマークの使用（58-42 ページ）を参照してください。
テーブル ビューのデータに基づいてレポートを生成する	[レポート デザイナ（Report Designer）] をクリックします。詳細については、イベント ビューからのレポート テンプレートの作成（57-10 ページ）を参照してください。

表 54-1　修復ステータス イベントの表示オプション（続き）

目的	操作
特定の値に制限して、ワークフロー内の次のページにドリルダウンする	次のいずれかの方法を使用します。 • カスタム ワークフローで作成したドリルダウン ページで、行内の値をクリックします。テーブル ビューの行内の値をクリックすると、テーブル ビューが制限され、次のページに**ドリルダウンされない**ことに注意してください。 • 一部のユーザに制限して次のワークフロー ページにドリルダウンするには、次のワークフロー ページに表示するユーザの横にあるチェックボックスをオンにしてから、[表示（View）] をクリックします。 • 現在の制限を維持して次のワークフロー ページにドリルダウンするには、[すべてを表示（View All）] をクリックします。 **ヒント**　テーブル ビューでは、必ずページ名に「Table View」が含まれます。 詳細については、イベントの制約（58-35 ページ）を参照してください。
システムから修復ステータス イベントを削除する	次のいずれかの方法を使用します。 • 特定のイベントを削除するには、削除するイベントの横にあるチェック ボックスをオンにしてから、[削除（Delete）] をクリックします。 • 現在の制限ビュー内のすべてのイベントを削除するには、[すべて削除（Delete All）] をクリックしてから、すべてのイベントを削除することを確認します。
修復ステータス イベントを検索する	[検索（Search）] をクリックします。詳細については、修復ステータス イベントの検索（54-23 ページ）を参照してください。

修復ステータス イベントを表示する方法:

アクセス:管理

手順 1　[分析（Analysis）] > [相関（Correlation）] > [ステータス（Status）] を選択します。

デフォルトの修復ワークフローの最初のページが表示されます。カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [（ワークフローの切り替え）（(switch workflow)）] をクリックします。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。イベントが表示されない場合は、時間範囲の調整が必要な可能性があります。イベント時間の制約の設定（58-27 ページ）を参照してください。

ヒント　修復のテーブル ビューが含まれないカスタム ワークフローを使用する場合、ワークフローのタイトルの横の [（ワークフローの切り替え）（(switch workflow)）] メニューをクリックし、[修復ステータス（Remediation Status）] を選択します。

修復ステータス イベントの使用

ライセンス：FireSIGHT

イベント ビューのレイアウトを変更したり、ビュー内のイベントをフィールド値で制限したりできます。

カラムを無効にすると、そのカラムは（後で元に戻さない限り）そのセッションの期間中は無効になります。最初のカラムを無効にすると、[カウント（Count）] カラムが追加されることに注意してください。

テーブル ビューの行内の値をクリックすると、テーブル ビューが制約されます（次のページにはドリルダウンされません）。

ヒント　テーブル ビューでは、必ずページ名に「Table View」が含まれます。

詳細は、次のトピックを参照してください。

- イベントの制約（58-35 ページ）
- 複合的な制約の使用（58-38 ページ）
- ドリルダウン ワークフロー ページのソート（58-39 ページ）
- 修復ステータス テーブルについて（54-21 ページ）

修復ステータス テーブルについて

ライセンス：FireSIGHT

Defense Centerを設定して、ポリシー違反およびディスカバリ イベントへのさまざまな応答を起動できます。こうした応答には、ポリシー違反時のファイアウォールまたはルータにおけるホストのブロックなどの修復が含まれます。修復がトリガーとして使用すると、修復ステータス イベント生成され、データベースに記録されます。修復の詳細については、修復の設定（54-1 ページ）を参照してください。

修復ステータス テーブルのフィールドについて、次の表で説明します。

表 54-2　修復ステータス フィールド

フィールド	説明
ポリシー	違反し、修復をトリガーとして使用した相関ポリシーの名前。
修復名（Remediation Name）	起動された修復の名前。

表 54-2　修復ステータス フィールド(続き)

フィールド	説明
結果メッセージ(Result Message)	修復の起動時に発生した事象を説明するメッセージ。ステータス メッセージには以下が含まれます。 • 修復は正常に完了しました(Successful completion of remediation) • 修復モジュールに提供された入力でエラーが発生しました(Error in the input provided to the remediation module) • 修復モジュールの設定でエラーが発生しました(Error in the remediation module configuration) • リモート デバイスまたはサーバへのログインでエラーが発生しました(Error logging into the remote device or server) • リモート デバイスまたはサーバで必要な権限が取得できませんでした(Unable to gain required privileges on remote device or server) • リモート デバイスまたはサーバへのログインがタイムアウトしました(Timeout logging into remote device or server) • リモート コマンドまたはサーバの実行がタイムアウトしました(Timeout executing remote commands or servers) • リモート デバイスまたはサーバに到達できませんでした(The remote device or server was unreachable) • 修復が試行されましたが、失敗しました(The remediation was attempted but failed) • 修復プログラムの実行に失敗しました(Failed to execute remediation program) • 原因不明または予期しないエラーが発生しました(Unknown/unexpected error) **(注)** カスタム修復モジュールがインストールされている場合、カスタム モジュールによって実装される追加のステータス メッセージが表示される場合があります。
ルール(Rule)	修復をトリガーとして使用したルールの名前。
時刻(Time)	Defense Center が修復を起動した日付と時刻。
メンバー数(Count)	各行に表示された情報と一致するイベントの数。[カウント(Count)] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

修復ステータス イベントのテーブル ビューを表示する方法:

アクセス:管理

手順 1　[分析(Analysis)] > [相関(Correlation)] > [ステータス(Status)] を選択します。

テーブル ビューが表示されます。修復ステータス イベントの使用の詳細については、修復ステータス イベントの使用(54-18 ページ)を参照してください。

ヒント　修復ステータス イベントのテーブル ビューが含まれないカスタム ワークフローを使用する場合、ワークフローのタイトルの横の [(ワークフローの切り替え)((switch workflow))] をクリックし、[修復ステータス(Remediation Status)] をクリックします。

修復ステータス イベントの検索

ライセンス：FireSIGHT

特定の修復が起動されたかどうか、およびいつ起動されたかを判別するために修復ステータス イベントを検索できます。実際のネットワーク環境に合わせてカスタマイズされた検索を作成して保存すると、あとで再利用できます。次の表で、ユーザが使用できる検索条件について説明します。

表 54-3　修復ステータスの検索条件

検索フィールド	説明
結果メッセージ（Result Message）	照合する結果メッセージ（修復が起動されたときに発生した事象を説明するメッセージ）の**正確な**名前を入力します有効なステータス メッセージは次のとおりです。 • 修復は正常に完了しました（Successful completion of remediation） • 修復モジュールに提供された入力でエラーが発生しました（Error in the input provided to the remediation module） • 修復モジュールの設定でエラーが発生しました（Error in the remediation module configuration） • リモート デバイスまたはサーバへのログインでエラーが発生しました（Error logging into the remote device or server） • リモート デバイスまたはサーバで必要な権限が取得できませんでした（Unable to gain required privileges on remote device or server） • リモート デバイスまたはサーバへのログインがタイムアウトしました（Timeout logging into remote device or server） • リモート コマンドまたはサーバの実行がタイムアウトしました（Timeout executing remote commands or servers） • リモート デバイスまたはサーバに到達できませんでした（The remote device or server was unreachable） • 修復が試行されましたが、失敗しました（The remediation was attempted but failed） • 修復プログラムの実行に失敗しました（Failed to execute remediation program） • 原因不明または予期しないエラーが発生しました（Unknown/unexpected error） **（注）** カスタム修復モジュールをインストールした場合、カスタム モジュールによって実装される追加のステータス メッセージを入力できる場合があります。
時刻（Time）	Defense Centerが修復を起動した日付と時刻を指定します。時間入力の構文については、検索での時間制約の指定（60-6 ページ）を参照してください。
修復名（Remediation Name）	起動された修復の正確な名前を入力します。これは修復を作成したときに指定した名前です。
ポリシー	修復をトリガーとして使用した相関ポリシーの名前を入力します。
ルール（Rule）	修復をトリガーとして使用した相関ルールの名前を入力します。

保存されている検索をロードおよび削除する方法など、検索の詳細については、イベントの検索（60-1 ページ）を参照してください。

修復ステータス イベントを検索する方法:

アクセス:管理

手順 1　[分析(Analysis)] > [検索(Search)] を選択します。

検索ページが表示されます。

手順 2　テーブルのドロップダウン メニューから、[修復ステータス(Remediation Status)] を選択します。

ヒント　データベース内で別の種類のイベントを検索するには、テーブルのドロップダウン リストから選択します。

手順 3　表修復ステータスの検索条件に記載されているように、該当するフィールドに検索基準を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。

手順 4　必要に応じて検索を保存する場合は、[プライベート(Private)] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　制限されたイベント アナリスト ユーザ向けに検索を制限として保存する場合は、**必ず**プライベート検索として保存します。

手順 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [保存(Save)] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [保存(Save)] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され([プライベート(Private)] を選択した場合は本人のアカウントでのみ閲覧可能)、後で実行できます。

- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[新規として保存(Save As New)] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [保存(Save)] をクリックします。検索が保存され([プライベート(Private)] を選択した場合は本人のアカウントでのみ閲覧可能)、後で実行できます。

手順 6　検索を開始するには、[検索(Search)] ボタンをクリックします。

検索結果は、現在の時刻範囲によって制限され、デフォルトの修復ステータス ワークフローに表示されます。カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [(ワークフローの切り替え)((switch workflow))] をクリックします。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定(71-3 ページ)を参照してください。