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」（P.15-1）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防御センター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。

防御センター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、防御センター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」（P.41-1）
- 「修復ステータス イベントの使用」（P.41-18）

修復の作成

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防御センター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」（P.41-3）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」（P.41-8）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動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」（P.41-12）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」（P.41-16）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、防御センター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」（P.41-18）を参照してください。

シスコ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、防御センター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、[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防御センターにインストールする方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Modules] を選択します。

[Modules] ページが表示されます。

ステップ 2　[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）。

ステップ 3　[Install] 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。

モジュールを防御センターで表示または削除する方法：

アクセス：Admin/Discovery Admin

ステップ 1　[Policies] > [Actions] > [Modules] を選択します。

[Modules] ページが表示されます。

ステップ 2　次のいずれかの操作を実行します。

- [View] をクリックして、モジュールを表示します。

  [Module Detail] ページが表示されます。
- 削除するファイルの横の [Delete] をクリックします。シスコ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

シスコでは、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がトリガーとして使用したときに起動するよう設定している場合のみです。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

ステップ 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。

ステップ 2　防御センターで、防御センター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」（P.41-4）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」（P.41-5）
- 「Cisco IOS ブロック宛先ネットワーク修復」（P.41-6）
- 「Cisco IOS ブロック送信元修復」（P.41-7）
- 「Cisco IOS ブロック送信元ネットワーク修復」（P.41-7）

ステップ 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）、防御センター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

ステップ 1　[Policies] > [Actions] > [Instances] を選択します。

[Instances] ページが表示されます。

ステップ 2　[Add a New Instance] リストから[Cisco IOS Null Route (v1.0)] を選択し、[Add] をクリックします。

[Edit Instance] ページが表示されます。

ステップ 3　[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。

ステップ 4　[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　[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　[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。

ステップ 7　[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。

ステップ 8　[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 CIDR 表記を使用する方法の詳細については、「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 9　[Create] をクリックします。

インスタンスが作成され、ページの [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、次の項を参照してください。

- 「Cisco IOS ブロック宛先修復」（P.41-5）
- 「Cisco IOS ブロック宛先ネットワーク修復」（P.41-6）
- 「Cisco IOS ブロック送信元修復」（P.41-7）
- 「Cisco IOS ブロック送信元ネットワーク修復」（P.41-7）

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

ステップ 1　[Policies] > [Actions] > [Instances] を選択します。

[Instances] ページが表示されます。

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。

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」（P.41-4）を参照してください。

[Edit Instance] ページが表示されます。

ステップ 3　[Configured Remediations] セクションで、[Block Destination] を選択し、[Add] をクリックします。

[Edit Remediation] ページが表示されます。

ステップ 4　[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。

ステップ 5　必要に応じて、[Description] フィールドに、修復の説明を入力します。

ステップ 6　[Create] をクリックし、次に [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

ステップ 1　[Policies] > [Actions] > [Instances] を選択します。

[Instances] ページが表示されます。

ステップ 2　修復を追加するインスタンスの横で、[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」（P.41-4）を参照してください。

[Edit Instance] ページが表示されます。

ステップ 3　[Configured Remediations] セクションで、[Block Destination Network] を選択し、[Add] をクリックします。

[Edit Remediation] ページが表示されます。

ステップ 4　[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。

ステップ 5　必要に応じて、[Description] フィールドに、修復の説明を入力します。

ステップ 6　[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 7　[Create] をクリックし、次に [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

ステップ 1　[Policies] > [Actions] > [Instances] を選択します。

[Instances] ページが表示されます。

ステップ 2　修復を追加するインスタンスの横で、[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」（P.41-4）を参照してください。

[Edit Instance] ページが表示されます。

ステップ 3　[Configured Remediations] セクションで、[Block Source] を選択し、[Add] をクリックします。

[Edit Remediation] ページが表示されます。

ステップ 4　[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。

ステップ 5　必要に応じて、[Description] フィールドに、修復の説明を入力します。

ステップ 6　[Create] をクリックし、次に [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

ステップ 1　[Policies] > [Actions] > [Instances] を選択します。

[Instances] ページが表示されます。

ステップ 2　修復を追加するインスタンスの横で、[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」（P.41-4）を参照してください。

[Edit Instance] ページが表示されます。

ステップ 3　[Configured Remediations] セクションで、[Block Source Network] を選択し、[Add] をクリックします。

[Edit Remediation] ページが表示されます。

ステップ 4　[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。

ステップ 5　必要に応じて、[Description] フィールドに、修復の説明を入力します。

ステップ 6　[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 7　[Create] をクリックし、次に [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

シスコは、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がトリガーとして使用したときに起動するよう設定している場合のみです。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

ステップ 1　ファイアウォール上で Telnet または SSH を有効にします（シスコは 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。

ステップ 2　防御センターで、防御センター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」（P.41-9）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」（P.41-10）
- 「Cisco PIX ブロック送信元修復」（P.41-11）

ステップ 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、防御センター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　シスコは、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

ステップ 1　[Policies] > [Actions] > [Instances] を選択します。

[Instances] ページが表示されます。

ステップ 2　[Add a New Instance] リストから、[Cisco PIX Shun] を選択し、[Add] をクリックします。

[Edit Instance] ページが表示されます。

ステップ 3　[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。

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

ステップ 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。

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

ステップ 7　[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。

ステップ 8　[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。

ステップ 9　[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 CIDR 表記を使用する方法の詳細については、「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 10　[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。

ステップ 11　[Create] をクリックします。

インスタンスが作成され、ページの [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、次の項を参照してください。

- 「Cisco PIX ブロック宛先修復」（P.41-10）
- 「Cisco PIX ブロック送信元修復」（P.41-11）

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

ステップ 1　[Policies] > [Actions] > [Instances] を選択します。

[Instances] ページが表示されます。

ステップ 2　修復を追加するインスタンスの横で、[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」（P.41-9）を参照してください。

[Edit Instance] ページが表示されます。

ステップ 3　[Configured Remediations] セクションで、[Block Destination] を選択し、[Add] をクリックします。

[Edit Remediation] ページが表示されます。

ステップ 4　[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。

ステップ 5　必要に応じて、[Description] フィールドに、修復の説明を入力します。

ステップ 6　[Create] をクリックし、次に [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

ステップ 1　[Policies] > [Actions] > [Instances] を選択します。

[Instances] ページが表示されます。

ステップ 2　修復を追加するインスタンスの横で、[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」（P.41-9）を参照してください。

[Edit Instance] ページが表示されます。

ステップ 3　[Configured Remediations] セクションで、[Block Source] を選択し、[Add] をクリックします。

[Edit Remediation] ページが表示されます。

ステップ 4　[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。

ステップ 5　必要に応じて、[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」（P.41-12）
- 「Nmap スキャン修復」（P.41-13）

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、防御センターのローカルの 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防御センター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

ステップ 1　[Policies] > [Actions] > [Instances] を選択します。

[Instances] ページが表示されます。

ステップ 2　[Add a module type] ドロップダウン リストから、[Nmap Remediation (v1.0)] を選択し、[Add] をクリックします。

[Edit Instance] ページが表示されます。

ステップ 3　[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。

ステップ 4　[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。

ステップ 5　オプションで、[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。次の構文を使用します。

- IPv6 ホストの場合は厳密な IP アドレス（たとえば、`2001:DB8::fedd:eeff`）
- IPv4 ホストの場合は厳密な IP アドレス（たとえば、`192.168.1.101`）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 `192.168.1.1` から `192.168.1.254` までの 254 ホスト（両端を含む）をスキャンします）

ブラックリスト化されたネットワーク上にあるホストを特にスキャン対象とした場合、スキャンは実行されません。FireSIGHT システム で CIDR 表記を使用する方法の詳細については、「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 6　オプションで、防御センターの代わりに、リモートの管理対象デバイスからスキャンするには、[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。

ステップ 7　[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 修復を作成することにより、Nmap スキャンの設定を定義できます。Nmap 修復は、相関ポリシーの応答として、オンデマンドで実行するために使用することも、指定時刻に実行するようにスケジュール設定することもできます。Nmap スキャンの結果をネットワーク マップに表示するには、スキャンされるホストがネットワーク マップに存在している必要があります。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の詳細については、「Nmap 修復の概要」（P.43-2）を参照してください。

Nmap が提供するサーバおよびオペレーティング システムのデータは、別の Nmap スキャンを実行するまで静的なままであることに注意してください。Nmap を使用してホストのオペレーティング システムおよびサーバのデータをスキャンする場合、定期的にスケジュールされたスキャンをセットアップし、Nmap が提供するオペレーティング システムおよびサーバのデータを最新の状態にすることを推奨します。詳細については、「Nmap スキャンの自動化」（P.49-5）を参照してください。また、ホストがネットワーク マップから削除されると、そのホストのすべての Nmap スキャン結果が廃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 で、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

ステップ 1　[Policies] > [Actions] > [Scanners] を選択します。

[Scanners] ページが表示されます。

ステップ 2　修復を追加するスキャン インスタンスの横の [Add Remediation] をクリックします。

[Edit Remediation] ページが表示されます。

ステップ 3　[Remediation Name] フィールドに、1 ～ 63 文字の英数字を使用して修復の名前を入力します。スペースと下線（_）およびハイフン（-）以外の特殊文字を使用することはできません。

ステップ 4　[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修復の説明を入力します。

ステップ 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、[Scan Which Address(es) From Event?] オプションを設定します。

- [Scan Source and Destination Addresses] 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をスキャンします。
- [Scan Source Address 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をスキャンします。
- [Scan Destination Address 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をスキャンします。

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、デフォルトで、修復はイベントに含まれるホストの IP アドレスをスキャンします。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。

ステップ 6　次のように、[Scan type] オプションを設定します。

- TCP 接続を開始し、完了しないことにより、`admin` アカウントがロー パケット アクセスを持つホスト、または IPv6 が動作していないホストで、ステルス モードですばやくスキャンするには、[TCP Syn Scan] を選択します。
- 防御センターの `admin` アカウントがロー パケット アクセスを持つホスト、または IPv6 が動作しているホストで使用可能な、システムの `connect()` コールを使用してスキャンするには、[TCP Connect 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するために ACK パケットを送信するには、[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 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 Scan] を選択します。

ステップ 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、[Scan for UDP ports] オプションで [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。スキャンの速度を上げるには、このオプションを無効のままにします。

ステップ 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場合は、[Use Port From Event] オプションを設定します。

- [On] を選択して、ステップ 12 で指定したポートではなく、相関イベントのポートをスキャンします。

  相関イベントのポートをスキャンする場合、修復はステップ 8 で指定する IP アドレスのポートをスキャンすることに注意してください。これらのポートは、修復のダイナミックなスキャン ターゲットにも追加されます。
- [Off] を選択して、ステップ 12 で指定するポートのみをスキャンします。

ステップ 9　相関ポリシー違反への応答としてこの修復を使用し、イベントが検出された検出エンジンを実行するアプライアンスを使用してスキャンする場合、[Scan from reporting detection engine] オプションを設定します。

- レポート検出エンジンを実行するアプライアンスからスキャンするには、[On] を選択します。
- 修復に設定されたアプライアンスからスキャンするには、[Off] を選択します。

ステップ 10　[Fast Port Scan] オプションを設定します。

- 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、[On] を選択します。
- すべての TCP ポートをスキャンするには、[Off] を選択します。

ステップ 11　[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 ～ 65535 の値を指定します。複数のポートを、カンマまたはスペースを使用して区切ります。ハイフンを使用してポートの範囲を示すこともできます。TCP と UDP の両方のポートをスキャンする場合は、スキャンする TCP ポートのリストの先頭に T を、UDP ポートのリストの先頭に U を付けます。たとえば、UDP トラフィック用のポート 53 および 111 をスキャンし、TCP トラフィック用のポート 21-25 をスキャンするには、`U:53,111,T:21-25` を入力します。

ステップ 8 で説明しているように、修復が相関ポリシー違反への応答として起動されると、[Use Port From Event] オプションがこの設定をオーバーライドすることに注意してください。

ステップ 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、[Probe open ports for vendor and version information] を設定します。

- サーバ情報に関してホストの開いているポートをスキャンし、サーバ ベンダーおよびバージョンを識別するには、[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、[Off] を選択します。

ステップ 13　開いているポートをプローブすることを選択する場合、[Service Version Intensity] ドロップダウン リストから数値を選択することにより、使用されるプローブの数を設定します。

- 使用するプローブを多くして、長いスキャンで高い精度を得るには、大きな数値を選択します。
- 使用するプローブを少なくして、低い精度で高速なスキャンを行うには、小さな数値を選択します。

ステップ 14　オペレーティング システム情報をスキャンするには、[Detect Operating System] 設定を構成します。

- オペレーティング システムを識別する情報に関してホストをスキャンするには、[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、[Off] を選択します。

ステップ 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、[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でポート スキャンを実行するには、[On] を選択します。
- [Host Discovery Method] および [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、使用不可能なすべてのホストでポート スキャンを省略するには、[Off] を選択します。

ステップ 16　ホストが存在して使用可能かどうかを Nmap がテストする場合に使用する方式を選択します。

- SYN フラグが設定された空の TCP パケットを送信し、使用可能なホストで閉じているポートの RST 応答または開いているポートの SYN/ACK 応答を得るには、[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 をスキャンし、TCP SYN スキャンはステートフル ファイアウォール ルールが設定されたファイアウォールにより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、使用可能なホストで RST 応答を得るために、[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 をスキャンし、TCP ACK スキャンはステートレス ファイアウォール ルールが設定されたファイアウォールにより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、使用可能なホストで閉じているポートのポート到達不能応答を得るには、[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。

ステップ 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、[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。

ステップ 18　[Default NSE Scripts] オプションを設定して、ホスト ディスカバリおよび、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に 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、[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、[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。

ステップ 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 テンプレート番号を選択します。番号が大きいほど高速で包括度が低いスキャンになり、番号が小さいほど低速で包括度が高いスキャンになります。

ステップ 20　[Save] をクリックし、次に [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」（P.37-35）および「ユーザ定義のホスト属性の使用」（P.37-35）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」（P.41-17）
- 「セット属性値修復」（P.41-17）

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

ステップ 1　[Policies] > [Actions] > [Instances] を選択します。

[Instances] ページが表示されます。

ステップ 2　[Add a module type] ドロップダウン リストから、[Set Attribute Value (v1.0)] を選択し、[Add] をクリックします。

[Edit Instance] ページが表示されます。

ステップ 3　[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。

ステップ 4　[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。

ステップ 5　[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

ステップ 1　[Policies] > [Actions] > [Instances] を選択します。

[Instances] ページが表示されます。

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

[Edit Instance] ページが表示されます。

ステップ 3　[Add a new remediation of type] ドロップダウン リストから [Set Attribute Value] を選択します。

[Edit Remediation] ページが表示されます。

ステップ 4　[Remediation Name] フィールドに、1 ～ 63 文字の英数字を使用して修復の名前を入力します。スペースと下線（_）およびハイフン（-）以外の特殊文字を使用することはできません。

ステップ 5　[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修復の説明を入力します。

ステップ 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、[Update Which Host(s) From Event] オプションを設定します。

- [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。
- [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。
- [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でトリガーとして使用する相関ルールへの応答としてこの修復を使用する場合、デフォルトで、修復はイベントに含まれるホストの IP アドレスをスキャンします。このオプションを設定する必要はありません。

ステップ 7　[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、[On] を選択します。
- 修復の [Attribute Value] 設定を属性値として使用するには、[Off] を選択します。

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

ステップ 9　[Save] をクリックし、次に [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、[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」（P.47-27）
- 「修復ステータス イベントの検索」（P.41-22）

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、特定の要件に一致する情報のみ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の詳細については、「カスタム ワークフローの作成」（P.47-45）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 41-1　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	詳細については、「修復ステータス テーブルについて」（P.41-21）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」（P.47-27）を参照してください。 イベント ビューを時間で制限する場合、アプライアンスで設定された時間範囲外で生成されたイベント（グローバルまたはイベント固有かどうかにかかわらず）がイベント ビューに表示される可能性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」（P.47-36）および「ドリルダウン ワークフロー ページのソート」（P.47-39）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 [(switch workflow)] をクリックします。詳細については、「ワークフローの選択」（P.47-19）を参照してください。
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	[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」（P.47-41）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	[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」（P.47-42）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	[View Bookmarks] をクリックします。詳細については、「ブックマークの使用」（P.47-42）を参照してください。
テーブル ビューのデータに基づいてレポートを生成する	[Report Designer] をクリックします。詳細については、「イベント ビューからのレポート テンプレートの作成」（P.44-2）を参照してください。
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、[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、[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」（P.47-36）を参照してください。

表 41-1　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
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、[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、[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	[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」（P.41-22）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：Admin

ステップ 1　[Analysis] > [Correlation] > [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 [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、「イベント ビュー設定の設定」（P.58-3）を参照してください。イベントが表示されない場合、時間範囲を調整する必要がある場合があります。「イベント時間の制約の設定」（P.47-27）を参照してください。

ヒント　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 [(switch workflow)] メニューをクリックし、[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によって制限したりすることができます。

列を無効にすると、現在のセッションの間無効になります（その後再度追加しない場合）。最初の列を無効にすると、[Count] 列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。

詳細については、次のトピックを参照してください。

- 「イベントの制約」（P.47-36）
- 「複合的な制約の使用」（P.47-38）
- 「ドリルダウン ワークフロー ページのソート」（P.47-39）
- 「修復ステータス テーブルについて」（P.41-21）

修復ステータス テーブルについて

ライセンス：FireSIGHT

防御センターを設定して、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」（P.41-1）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 41-2　修復ステータス フィールド

フィールド	説明
Policy	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。
Remediation Name	起動された修復の名前。
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。 • Successful completion of remediation • Error in the input provided to the remediation module • Error in the remediation module configuration • Error logging into the remote device or server • Unable to gain required privileges on remote device or server • Timeout logging into remote device or server • Timeout executing remote commands or servers • The remote device or server was unreachable • The remediation was attempted but failed • Failed to execute remediation program • 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。
Rule	修復をトリガーとして使用したルールの名前。
Time	防御センターが修復を起動した日付と時刻。
Count	各行に表示される情報に一致するイベントの数。同一の行が複数作成される制約を適用した後にのみ、[Count] フィールドが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：Admin

ステップ 1　[Analysis] > [Correlation] > [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 イベントを使用の詳細については、「修復ステータス イベントの使用」（P.41-18）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 [(switch workflow)] をクリックし、[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。使用する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、保存して再利用することをお勧めします。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 41-3　修復ステータスの検索条件

検索フィールド	説明
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。 • Successful completion of remediation • Error in the input provided to the remediation module • Error in the remediation module configuration • Error logging into the remote device or server • Unable to gain required privileges on remote device or server • Timeout logging into remote device or server • Timeout executing remote commands or servers • The remote device or server was unreachable • The remediation was attempted but failed • Failed to execute remediation program • 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。
Time	防御センター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」（P.45-5）を参照してください。
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。
Policy	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。
Rule	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。

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」（P.45-1）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：Admin

ステップ 1　[Analysis & Reporting] > [Searches] > [Remediation Status] を選択します。

[Remediation Status] 検索ページが表示されます。

ヒント　異なる種類のイベントに関してデータベースを検索するには、[Table] ドロップダウン リストから選択します。

ステップ 2　オプションで、検索を保存するには、[Name] フィールドに検索の名前を入力します。

名前を入力しなかった場合、検索を保存するときに自動的に作成されます。

ステップ 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。複数の条件を入力した場合、すべての条件を満たすレコードだけが返されます。

ステップ 4　他のユーザがアクセスできるように検索を保存する場合、[Save As Private] チェック ボックスをオフにします。そうしない場合は、検索をプライベートとして保存するために、チェック ボックスをオンのままにします。

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。

ステップ 5　次の選択肢があります。

- 検索を開始するには、[Search] 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 [(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、「イベント ビュー設定の設定」（P.58-3）を参照してください。
- 既存の検索を変更し、その変更を保存したい場合は、[Save] をクリックします。
- 検索基準を保存する場合は、[Save as New Search] をクリックします。検索が保存され（[Save As Private] を選択した場合はユーザ アカウントに関連付けられ）、後で実行できます。