侵入ルールの外部アラートの設定

FireSIGHT システムは、Web インターフェイスで侵入イベントのさまざまなビューを提供しますが、企業によっては、重要なシステムの継続的なモニタリングを容易にするために、外部侵入のイベント通知を定義したいという要望があります。特定のユーザに重大イベントについてすぐに通知したい場合は、電子メール アラートを設定できます。さらに、syslog ファシリティへのロギングを有効にしたり、SNMP トラップ サーバにイベント データを送信したりできます。

各侵入ポリシー内では、侵入イベントの通知制限を指定し、外部ロギング ファシリティへの侵入イベント通知をセットアップし、侵入イベントへの外部応答を設定できます。

ヒント

アナリストによっては、同じ侵入イベントに対して複数のアラートを受信することは望まないものの、特定の侵入イベントの発生については、頻度を制限したうえで通知を受信したいと考えています。詳細については、ポリシー単位の侵入イベント通知のフィルタリング（32-25 ページ）を参照してください。

侵入ポリシー以外にも、FireSIGHT システムで実行可能な別のタイプのアラートがあります。特定の影響フラグが設定された侵入イベントや特定のアクセス コントロール規則によって記録された接続イベントなど、他のタイプのイベントに対して電子メール、SNMP、syslog アラートによる応答を設定できます。詳細については、外部アラートの設定（43-1 ページ）を参照してください。

外部侵入イベント通知の詳細情報については、次の項を参照してください。

- SNMP 応答の使用（44-2 ページ）では、指定された SNMP トラップ サーバにイベント データを送信する場合に設定可能なオプションや、SNMP アラート オプションを指定する手順について説明します。
- Syslog 応答の使用（44-4 ページ）では、外部 syslog にイベント データを送信する場合に設定可能なオプションや、syslog アラート オプションを指定する手順について説明します。
- 電子メール アラートについて（44-7 ページ）では、電子メールで侵入イベントの通知を送信する場合に設定可能なオプションについて説明します。

SNMP 応答の使用

ライセンス：Protection

*SNMP トラップ*は、ネットワーク管理に関する通知です。侵入イベントに関する通知を SNMP トラップ（*SNMP アラート*とも呼ばれる）として送信するようにデバイスを設定できます。各 SNMP アラートには次のものが含まれます。

- トラップを生成するサーバの名前
- アラートを検出したデバイスの IP アドレス
- アラートを検出したデバイスの名前
- イベント データ

さまざまな SNMP アラート パラメータを設定できます。使用可能なパラメータは、使用する SNMP のバージョンによって異なります。SNMP アラートを有効化および無効化する方法の詳細については、侵入ポリシーの詳細設定の設定（31-8 ページ）を参照してください。

ヒント　ネットワーク管理システムで Management Information Base（MIB）ファイルが必要な場合は、Defense Center の `/etc/sf/DCEALERT.MIB` から取得できます。

SNMP v2 オプション

SNMP v2 の場合、次の表で説明されているオプションを指定できます。

表 44-1　SNMP v2 オプション

オプション	説明
トラップ タイプ（Trap Type）	アラートに表示される IP アドレスに使用するトラップ タイプ。 ネットワーク管理システムによって INET_IPV4 アドレス タイプが正常にレンダリングされた場合は、[バイナリとして（as Binary）] を選択できます。そうでない場合は、[文字列として（as String）] を選択します。たとえば、HP Openview では String タイプが必要になります。
トラップ サーバ（Trap Server）	SNMP トラップ通知を受信するサーバ。 単一の IP アドレスまたはホスト名を指定できます。
コミュニティ ストリング（Community String）	コミュニティ名。

SNMP v3 オプション

SNMP v3 の場合、次の表で説明されているオプションを指定できます。

（注）　SNMP v3 を使用する場合、アプライアンスは Engine ID 値を使用してメッセージをエンコードします。SNMP サーバでは、メッセージをデコードするためにこの値が必要です。現在、この Engine ID 値は常に、文字列の末尾に `01` が付く、アプライアンスの IP アドレスの 16 進数バージョンになります。たとえば、SNMP アラートを送信するアプライアンスの IP アドレスが `172.16.1.50` である場合、Engine ID は `0xAC10013201` になります。また、アプライアンスの IP アドレスが `10.1.1.77` である場合、Engine ID `0x0a01014D01` が使用されます。

表 44-2　SNMP v3 オプション

オプション	説明
トラップ タイプ（Trap Type）	アラートに表示される IP アドレスに使用するトラップ タイプ。 ネットワーク管理システムによって INET_IPV4 アドレス タイプが正常にレンダリングされた場合は、[バイナリとして（as Binary）] を選択できます。そうでない場合は、[文字列として（as String）] を選択します。たとえば、HP Openview では String タイプが必要になります。
トラップ サーバ（Trap Server）	SNMP トラップ通知を受信するサーバ。 単一の IP アドレスまたはホスト名を指定できます。
認証パスワード（Authentication Password）	認証に必要なパスワード。SNMP v3 は、設定に応じて Message Digest 5（MD5）ハッシュ関数またはセキュア ハッシュ アルゴリズム（SHA）ハッシュ関数のいずれかを使用し、このパスワードを暗号化します。 認証パスワードを指定すると、認証が有効になります。
プライベート パスワード（Private Password）	プライバシー用の SNMP キー。SNMP v3 は Data Encryption Standard（DES）ブロック暗号を使用して、このパスワードを暗号化します。 プライベート パスワードを指定すると、プライバシーが有効になります。プライベート パスワードを指定する場合は、認証パスワードも指定する必要があります。
ユーザ名（User Name）	SNMP ユーザ名。

SNMP アラートの設定の詳細については、SNMP 応答の設定（44-3 ページ）を参照してください。

SNMP 応答の設定

ライセンス：Protection

侵入ポリシーで SNMP アラートを設定できます。アクセス コントロール ポリシーの一部としてポリシーを適用すると、システムは SNMP トラップで検出した侵入イベントをすべて通知するようになります。SNMP アラートの詳細については、SNMP 応答の使用（44-2 ページ）を参照してください。

SNMP アラート オプションの設定方法：

アクセス：Admin/Intrusion Admin

手順 1　[ポリシー（Policies）] > [侵入（Intrusion）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン（ ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

手順 3　左側のナビゲーション パネルの [詳細設定（Advanced Settings）] をクリックします。

[詳細設定（Advanced Settings）] ページが表示されます。

手順 4　外部応答の [SNMP アラート（SNMP Alerting）] が有効かどうかに応じて、次の 2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[SNMP アラート（SNMP Alerting）] ページが表示されます。

ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）を参照してください。

手順 5　IP アドレスに使用するトラップ タイプの形式を [バイナリとして（as Binary）] または [文字列として（as String）] のいずれかに指定します。

（注）　ネットワーク管理システムによって INET_IPV4 アドレス タイプが正常にレンダリングされた場合は、[バイナリとして（as Binary）] オプションを使用できます。正常にレンダリングされなかった場合は、[文字列として（as String）] オプションを使用します。たとえば、HP OpenView では [文字列として（as String）] オプションが必要になります。

手順 6　SNMP v2 または SNMP v3 を選択します。

- SNMP v2 を設定するには、使用するトラップ サーバの IP アドレスとコミュニティ名を対応するフィールドに入力します。SNMP v2 オプション（44-2 ページ）を参照してください。
- SNMP v3 を設定するには、使用するトラップ サーバの IP アドレス、認証パスワード、プライベート パスワード、およびユーザ名を対応するフィールドに入力します。詳細については、SNMP v3 オプション（44-2 ページ）を参照してください。

（注）　SNMP v2 **または** SNMP v3 を選択する必要があります。

（注）　SNMP v3 パスワードを入力すると、パスワードは初期設定時にはプレーン テキストで表示されますが、暗号化形式で保存されます。

手順 7　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

Syslog 応答の使用

ライセンス：Protection

システム ログ、つまり *syslog* は、ネットワーク イベント ロギングの標準ロギング メカニズムです。侵入イベントの通知である *syslog アラート*をアプライアンスの syslog に送信できます。syslog では、syslog 内の情報を優先度別およびファシリティ別に分類することができます。*優先度*はアラートの重大度を反映し、*ファシリティ*はアラートを生成したサブシステムを示します。ファシリティおよび優先度は syslog の実際のメッセージに表示されませんが、その代わりに、syslog メッセージを受信するシステムにそれを分類する方法を指示するために使用されます。

syslog アラートには次の情報が含まれます。

- アラート生成の日時
- イベント メッセージ
- イベント データ
- トリガー イベントのジェネレータ ID
- トリガー イベントの Snort ID
- 改訂

侵入ポリシーでは、syslog アラートを有効にして、syslog の侵入イベントの通知に関連付けられている syslog の優先度およびファシリティを指定できます。アクセス コントロール ポリシーの一部として侵入ポリシーを適用した場合、システムは、検出した侵入イベントの syslog アラートをローカル ホストまたはポリシーで指定されたロギング ホストの syslog ファシリティに送信します。アラートを受信したホストは、syslog アラートの設定時に設定されたファシリティおよび優先度に関する情報を使用して、アラートを分類します。

次の表には、syslog アラートを設定する場合に選択できるファシリティを示します。使用するリモート syslog サーバの設定に基づいて、効果のあるファシリティの設定を行ってください。リモート システムにある `syslog.conf` ファイル（UNIX または Linux ベースのシステムに syslog メッセージをロギングしている場合）は、サーバのどのログ ファイルにどのファシリティが保存されるかを示します。

表 44-3　使用可能な syslog ファシリティ

ファシリティ	説明
AUTH	セキュリティと承認に関連するメッセージ。
AUTHPRIV	セキュリティと承認に関連する制限付きアクセス メッセージ。多くのシステムで、これらのメッセージはセキュア ファイルに転送されます。
CRON	クロック デーモンによって生成されるメッセージ。
DAEMON	システム デーモンによって生成されるメッセージ。
FTP	FTP デーモンによって生成されるメッセージ。
KERN	カーネルによって生成されるメッセージ。多くのシステムでは、これらのメッセージは表示されるときにコンソールに出力されます。
LOCAL0-LOCAL7	内部プロセスによって生成されるメッセージ。
LPR	印刷サブシステムによって生成されるメッセージ。
MAIL	メール システムで生成されるメッセージ。
NEWS	ネットワーク ニュース サブシステムによって生成されるメッセージ。
SYSLOG	syslog デーモンによって生成されるメッセージ。
USER	ユーザ レベルのプロセスによって生成されるメッセージ。
UUCP	UUCP サブシステムによって生成されるメッセージ。

このアラートで生成されるすべての通知を表示するには、次の標準的な syslog の優先度レベルのいずれかを選択します。

表 44-4　syslog の優先度レベル

水準器	説明
EMERG	すべてのユーザにブロードキャストするパニック状態
ALERT	すぐに修正する必要がある状態
CRIT	重大な状態
ERR	エラー状態
WARNING	警告メッセージ
NOTICE	エラー状態ではないが、注意が必要な状態
INFO	通知メッセージ
DEBUG	デバッグ情報を含むメッセージ

syslog の動作とその設定方法の詳細については、システムに付属の資料を参照してください。UNIX または Linux ベースのシステムの syslog にログインしている場合、`syslog.conf` man ファイル（コマンドラインで `man syslog.conf` と入力）および syslog man ファイル（コマンドラインで `man syslog` と入力）に、syslog の動作とその設定方法に関する情報が示されます。

syslog 応答の設定

ライセンス：Protection

侵入ポリシーで syslog アラートを設定できます。アクセス コントロール ポリシーの一部としてポリシーを適用すると、システムは syslog で検出した侵入イベントをすべて通知するようになります。syslog アラートの詳細については、Syslog 応答の使用（44-4 ページ）を参照してください。

syslog アラート オプションの設定方法：

アクセス：Admin/Intrusion Admin

手順 1　[ポリシー（Policies）] > [侵入（Intrusion）] > [侵入ポリシー（Intrusion Policy）] の順に選択します。

[侵入ポリシー（Intrusion Policy）] ページが表示されます。

手順 2　編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

[ポリシー情報（Policy Information）] ページが表示されます。

手順 3　左側のナビゲーション パネルの [詳細設定（Advanced Settings）] をクリックします。

[詳細設定（Advanced Settings）] ページが表示されます。

手順 4　外部応答の [Syslog アラート（Syslog Alerting）] が有効かどうかに応じて、次の 2 つの選択肢があります。

- 設定が有効な場合、[編集（Edit）] をクリックします。
- 設定が無効である場合、[有効（Enabled）] をクリックし、[編集（Edit）] をクリックします。

[Syslog アラート（Syslog Alerting）] ページが表示されます。

ページ下部のメッセージは、設定を含む侵入ポリシー階層を示します。詳細については、ネットワーク分析ポリシーまたは侵入ポリシーでのレイヤの使用（24-1 ページ）を参照してください。

手順 5　オプションで、[ロギング ホスト（Logging Hosts）] フィールドに、ロギング ホストとして指定するリモート アクセス IP アドレスを入力します。複数のホストを指定する場合は、カンマで区切ります。

手順 6　ドロップダウン リストからファシリティおよび優先度のレベルを選択します。

ファシリティおよび優先度オプションの詳細については、Syslog 応答の使用（44-4 ページ）を参照してください。

手順 7　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、競合の解決とポリシー変更の確定（23-17 ページ）を参照してください。

電子メール アラートについて

ライセンス：Protection

*電子*メール アラートは、電子メールによる侵入イベントの通知です。電子メール アラートには次の情報が含まれます。

- データベース内のアラートの合計数
- 最後の電子メールの時刻（システムが最後の電子メール レポートを生成した時刻）
- 現在の時刻（システムが現在の電子メール レポートを生成した時刻）
- 新しいアラートの合計数
- 指定した電子メール フィルタに一致したイベントの数（特定のルールに対してイベントが設定されている場合）
- 各イベントのタイムスタンプ、プロトコル、イベント メッセージ、およびセッション情報（トラフィック方向が指定された送信元および宛先の IP およびポート）（[サマリ出力（Summary Output）] がオフの場合）

（注）　複数の侵入イベントが同じ送信元 IP から発生した場合、追加イベントの数を示すメモがイベントの下に表示されます。

- 宛先ポートあたりのイベント数
- 送信元 IP あたりのイベント数

ルールまたはルール グループごとに、侵入イベントの電子メール アラートを有効化または無効化できます。アクセス コントロール ポリシーの一部としてデバイスに適用する侵入ポリシーにかかわらず、電子メール アラート設定が使用されます。

次のリストには、電子メール アラートに設定できるパラメータを示します。

On/Off

電子メールによる通知を有効または無効にします。

送信元アドレス（From Address）

システムによる侵入イベントの送信元となる電子メール アドレスを指定します。

送信先アドレス（To Address）

システムによる侵入イベントの送信先となる電子メール アドレスを指定します。電子メールを複数の受信者に送信するには、電子メール アドレスをカンマで区切ります。次に例を示します。

```
user1@example.com, user2@example.com
```

[最大アラート数（Max Alerts）]

[頻度（秒）（Frequency（seconds））] で指定された時間枠で、システムが電子メールで送信する侵入イベントの最大数を指定します。

[頻度（秒）（Frequency（seconds））]

システムが侵入イベントをメール送信する頻度を指定します。この設定では、電子メール設定が保存される頻度も指定します。

最小頻度：300 秒
最大頻度：40 億秒

[アラートの結合（Coalesce Alerts）]

送信元 IP およびイベントによる侵入イベントのグループ化を有効または無効にし、同じ送信元 IP に対して生成された複数の同一侵入イベントが 1 つだけのイベントとしてページに表示されるようにします。

アラートの結合（グループ化）はイベントのフィルタリング後に行われることに注意してください。したがって、特定のルールで電子メール アラートを設定した場合、[電子メール アラート設定（Mail Alerting Configuration）] で指定した規則に一致するイベントのリストのみを受信します。

[サマリ出力（Summary Output）]

短い電子メール アラートを有効または無効にします。これは、ポケットベルなどのテキスト制限があるデバイスに適しています。短い電子メール アラートには、以下の情報が含まれています。

- イベントのタイムスタンプ
- イベントを生成したデバイスの IP アドレス（Defense Center の場合）
- イベントのプロトコル
- 送信元 IP およびポート
- 宛先 IP およびポート
- イベント メッセージ
- 同じ送信元 IP に対して生成された侵入イベントの数

次に例を示します。

```
2011-05-18 10:35:10 10.1.1.100 icmp 10.10.10.1:8 -> 10.2.1.3:0
snort_decoder: Unknown Datagram decoding problem! (116:108)
```

[特定のルール設定に基づく電子メール アラート（Email Alerting on Specific Rules Configuration）]

指定した電子メール アドレスにイベントを電子メールで送信するルールまたはルール グループを指定します。

電子メール アラートの設定の詳細については、電子メール アラートの設定（44-9 ページ）を参照してください。

電子メール アラートの設定

ライセンス：Protection

電子メール アラートを設定して、侵入イベントが特定のルールまたはルール グループに対して発生するたびにアプライアンスが通知するように設定できます。

電子メール アラートを受信できるようにするには、以下のことを**行う必要があります。**

- 電子メール アラートを受信するようにメール ホストを設定する（メール リレー ホストおよび通知アドレスの設定（63-20 ページ）を参照）
- 管理対象デバイスと Defense Center の両方がそれぞれの IP アドレスを互いに解決できることを確認する

電子メール アラート オプションを設定する方法：

アクセス：Admin/Intrusion Admin

手順 1　[ポリシー（Policies）] > [侵入（Intrusion）] > [電子メール（Email）] を選択します。

[電子メール アラート（Email Alerting）] ページが表示されます。

手順 2　[状態（State）] の横にある [on] を選択して電子メール アラートを有効にします。

手順 3　[送信元アドレス（From Address）] フィールドに、電子メール アラートの [送信元（From）] フィールドに表示するアドレスを入力します。

手順 4　[宛先アドレス（To Address）] フィールドに、電子メール アラートを受信するアドレスを入力します。

手順 5　[最大アラート数（Max Alerts）] フィールドに、単一の電子メールに含めるイベントの最大数を入力します。

手順 6　[最小頻度（Min Frequency）] フィールドに、電子メール アラートを受信する最小間隔の秒数を入力します。

手順 7　IP アドレス別にイベントをグループ化するには、[アラートの結合（Coalesce Alerts）] の横にある [on] を選択します。

手順 8　短い電子メール アラートを送信するには、[サマリ出力（Summary Output）] の横にある [on] を選択します。

ヒント　[サマリ出力（Summary Output）] を有効にする場合は、[アラートの結合（Coalesce Alerts）] を有効にして、生成されるアラートの数を減らすことを検討してください。また、デバイスのテキスト メッセージ バッファがオーバーフローしないように [最大アラート数（Max Alerts）] を 1 に設定することも検討してください。

手順 9　[タイム ゾーン（Time Zone）] フィールドで、ドロップダウン リストからタイム ゾーンを選択します。

手順 10 ルールごとに電子メール アラートを有効にするには、[ルールごとの電子メール アラート設定（Email Alerting per Rule Configuration）] をクリックします。

ルール グループが表示されます。

ヒント　すべてのカテゴリのすべてのルールについて電子メール アラートを受信するには、[すべて選択（Select All）] を選択します。

手順 11 次のいずれかまたは両方を実行します。

- カテゴリに属するすべてのルールで、電子メール アラートを受信するルール カテゴリの横にある [すべて（All）] をクリックします。
- そのカテゴリの個々のルールで電子メール アラートを指定するカテゴリ フォルダをクリックし、電子メール アラートを受信するルールを有効にします。

手順 12 [保存（Save）] をクリックします。

システムにより電子メール アラート設定が保存されます。該当する侵入イベントが発生すると、電子メール アラートが送信されます。