アラート応答による外部アラート

次のトピックでは、アラート応答を使用して Firepower Management Center から外部イベント アラートを送信する方法を示します。

- Firepower Management Center アラート応答 （1 ページ）
- SNMP アラート応答の作成 （3 ページ）
- Syslog アラート応答の作成 （4 ページ）
- 電子メール アラート応答の作成 （7 ページ）
- 影響フラグ アラートの設定 （8 ページ）
- 検出イベント アラートの設定 （9 ページ）
- ネットワーク向け AMP アラートの設定 （10 ページ）

Firepower Management Center アラート応答

SNMP、syslog、または電子メールでの外部イベント通知はクリティカルなシステムのモニタリングに役立ちます。Firepower Management Center はアラート応答を構成して外部サーバと対話します。アラート応答は、電子メール、SNMP、syslog サーバへの接続を表す構成です。これが応答と呼ばれるのは、これを使用して Firepower により検出されたイベントに応答してアラートを送信できるためです。異なるタイプのアラートを異なるモニタリング サーバまたはユーザ（あるいはその両方）に送信するための複数のアラート応答を構成できます。

（注） デバイスおよび Firepower のバージョンによっては、アラート応答は syslog メッセージを送信する最適な方法ではない可能性があります。Syslog についておよびセキュリティ イベント syslog メッセージングを設定するためのベストプラクティスを参照してください。

（注） アラート応答を使用するアラートは、Firepower Management Center によって送信されます。アラート応答を使用しない侵入の電子メール アラートも、Firepower Management Center によって送信されます。対照的に、個別の侵入ルールのトリガーに基づく SNMP および syslog アラートは管理対象デバイスから直接送信されます。詳細については、侵入イベントに関する外部アラートを参照してください。

ほとんどの場合、外部アラートに含まれる情報はデータベースにロギングされたいずれかの関連イベントに含まれる情報と同じです。ただし、相関ルールに接続トラッカーが含まれる相関イベントアラートについては、受信する情報はベースのイベントの種類に関係なく、トラフィック プロファイル変更のアラート情報と同じです。

アラート応答の作成や管理は [アラート（Alerts）] ページ（**[Policies]** > **[Actions]** > **[Alerts]**）で行います。新しいアラート応答は自動的に有効になります。アラート応答を削除するのではなく無効にすることで、アラートの生成を一時的に止めることができます。

アラート応答への変更は、接続ログを SNMP トラップまたは syslog サーバに送信する場合を除き、ただちに有効になります。

マルチドメイン展開では、アラート応答を作成すると、作成された応答は現在のドメインに属します。このアラート応答は子孫ドメインでも使用できます。

アラート応答のサポート設定

アラート応答を作成した後、それを使用して、次のような外部アラートを Firepower Management Center から送信できます。

アラート/イベントのタイプ	詳細情報
侵入イベント（インパクト フラグ別）	影響フラグ アラートの設定 （8 ページ）
検出イベント（タイプ別）	検出イベント アラートの設定 （9 ページ）
ネットワーク向け AMP（「ネットワークベース」）によって検出されたマルウェアとレトロスペクティブ マルウェア イベント	ネットワーク向け AMP アラートの設定 （10 ページ）
相関イベント（相関ポリシー違反ごと）	ルールとホワイトリストに応答を追加する
相関イベント（ログ ルールまたはデフォルト アクション別）（電子メールアラートのサポートなし）	ログ可能なその他の接続
ヘルス イベント（ヘルス モジュールおよび重大度レベル別）	ヘルス モニタ アラートの作成

SNMP アラート応答の作成

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）	を除きFTD任意	任意（Any）	Admin

SNMPv1、SNMPv2、または SNMPv3 を使用して SNMP アラート応答を作成できます。

（注） SNMP プロトコルの SNMP バージョンを選択する場合、SNMPv2 では読み取り専用コミュニティのみがサポートされ、SNMPv3 では読取り専用ユーザのみがサポートされることに注意してください。SNMPv3 は、AES128 での暗号化をサポートします。

SNMP で 64 ビット値をモニタする場合は、SNMPv2 または SNMPv3 を使用する必要があります。SNMPv1 は 64 ビットのモニタリングをサポートしていません。

始める前に

- ネットワーク管理システムで Firepower Management Center の管理情報ベース（MIB）ファイルが必要な場合は、`/etc/sf/DCEALERT.MIB` で取得できます。

手順

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

ステップ 2 [アラートの作成（Create Alert）] ドロップダウン メニューから、[SNMP アラートの作成（Create SNMP Alert）] を選択します。

ステップ 3 SNMP 応答を識別する [名前（Name）] を入力します。

ステップ 4 [トラップサーバ（Trap Server）] フィールドに、SNMP トラップ サーバのホスト名または IP アドレスを入力します。

（注） このフィールドに無効な IPv4 アドレス（192.169.1.456 など）を入力した場合でも、システムは警告を**表示しません**。無効なアドレスはホスト名として扱われます。

ステップ 5 [バージョン（Version）] ドロップダウンリストから、使用する SNMP バージョンを選択します。SNMP v3 がデフォルトです。

ステップ 6 使用する SNMP のバージョンに応じて、次のいずれかを実行します。

- SNMP v1 または SNMP v2 の場合は、[コミュニティ ストリング（Community String）] フィールドに SNMP コミュニティ名を入力して、手順 12 に進みます。
- SNMP v3 の場合、[ユーザ名（User Name）] フィールドに SNMP サーバで認証するユーザの名前を入力し、次の手順に進みます。

ステップ 7 [認証プロトコル（Authentication Protocol）] ドロップダウンリストから、認証に使用するプロトコルを選択します。

ステップ 8 [認証パスワード（Authentication Password）] フィールドに、SNMP サーバの認証に必要なパスワードを入力します。

ステップ 9 [プライバシー プロトコル（Privacy Protocol）] リストから、[なし（None）] を選択してプライバシー プロトコルを使用しないか、または [DES] を選択してプライバシー プロトコルにデータ暗号規格を使用します。

ステップ 10 [プライバシー パスワード（Privacy Password）] フィールドに、SNMP サーバに必要なプライバシー パスワードを入力します。

ステップ 11 [エンジン ID（Engine ID）] フィールドに、SNMP エンジンの識別子を偶数桁の 16 進表記で入力します。

SNMPv3 を使用する場合、メッセージの符号化にはエンジン ID 値が使用されます。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。

Firepower Management Center の IP アドレスの 16 進数バージョンを使用することを推奨します。たとえば、Firepower Management Center の IP アドレスが `10.1.1.77` である場合、`0a01014D0` を使用します。

ステップ 12 [保存（Save）] をクリックします。

次のタスク

変更内容は、次の場合を除き、ただちに有効になります。

アラート応答を使って接続ログを送信している場合、これらのアラート応答を編集したあとに設定の変更を展開する必要があります。

Syslog アラート応答の作成

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

syslog アラート応答を設定する際、syslog サーバで確実に正しく処理されるようにするために、syslog メッセージに関連付けられる重大度とファシリティを指定できます。ファシリティはメッセージを作成するサブシステムを示し、重大度はメッセージの重大度を定義します。ファシリティと重大度は syslog に示される実際のメッセージには表示されませんが、syslog メッセージを受信するシステムに対して、メッセージの分類方法を指示するために使用されます。

ヒント　syslog の機能とその設定方法の詳細については、ご使用のシステムのマニュアルを参照してください。UNIX システムでは、`syslog` および `syslog.conf` の `man` ページで概念情報および設定手順が説明されています。

syslog アラート応答の作成時に任意のタイプのファシリティを選択できますが、syslog サーバに基づいて意味のあるものを選択する必要があります。すべての syslog サーバがすべてのファシリティをサポートしているわけではありません。UNIX syslog サーバの場合、`syslog.conf` ファイルで、どのファシリティがサーバ上のどのログファイルに保存されるかを示す必要があります。

始める前に

- この手順は、多くの場合、syslog メッセージを送信するための推奨される方法ではありません。詳細については、セキュリティ イベント syslog メッセージングを設定するためのベストプラクティスを参照してください。
- syslog サーバがリモート メッセージを受け入れられることを確認します。

手順

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

ステップ 2　[アラートの作成（Create Alert）] ドロップダウン メニューから、[Syslog アラートの作成（Create Syslog Alert）] を選択します。

ステップ 3　[名前（Name）] にアラートの名前を入力します。

ステップ 4　[ホスト（Host）] フィールドに、syslog サーバのホスト名または IP アドレスを入力します。

（注）　このフィールドに無効な IPv4 アドレス（192.168.1.456 など）を入力した場合でも、システムは警告を**表示しません**。無効なアドレスはホスト名として扱われます。

ステップ 5　[ポート（Port）] フィールドに、サーバが syslog メッセージに使用するポートを入力します。この値はデフォルトで 514 です。

ステップ 6　Syslog アラート ファシリティ （6 ページ）で説明されているとおりに、[ファシリティ（Facility）] リストからファシリティを選択します。

ステップ 7　syslog 重大度レベル （7 ページ）で説明されているとおりに、[重大度（Severity）] リストから重大度を選択します。

ステップ 8　[タグ（Tag）] フィールドに、syslog メッセージとともに表示するタグ名を入力します。

たとえば、syslog に送信されるすべてのメッセージの前に `FromMC` を付ける場合、このフィールドに `FromMC` と入力します。

ステップ 9　[保存（Save）] をクリックします。

次のタスク

変更内容は、次の場合を除き、ただちに有効になります。

アラート応答を使ってsyslogサーバに接続ログを送信している場合、これらのアラート応答を編集したあとに設定の変更を展開する必要があります。

セキュリティイベントに対するこのアラート応答を使用する場合は、ポリシーにアラート応答を指定する必要があります。セキュリティイベントのsyslogの設定場所を参照してください。

Syslog アラート ファシリティ

次の表に、選択可能な syslog ファシリティを示します。

表 *1* : 使用可能な *syslog* ファシリティ

ファシリティ	説明
ALERT	アラート メッセージ。
AUDIT	監査サブシステムによって生成されるメッセージ。
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。
CLOCK	クロック デーモンによって生成されるメッセージ。 Windows オペレーティング システムを実行している syslog サーバは CLOCK ファシリティを使用することに注意してください。
CRON	クロック デーモンによって生成されるメッセージ。 Linux オペレーティング システムを実行している syslog サーバは CRON ファシリティを使用することに注意してください。
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。

ファシリティ	説明
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。
NTP	NTP デーモン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。

syslog 重大度レベル

次の表に、選択可能な標準の syslog 重大度レベルを示します。

表 *2 : syslog* 重大度レベル

水準器	説明
ALERT	ただちに修正する必要がある状態。
CRIT	クリティカルな状態。
DEBUG	デバッグ情報を含むメッセージ。
EMERG	すべてのユーザに配信されるパニック状態。
ERR	エラー状態。
INFO	情報メッセージ。
NOTICE	エラー状態ではないが、注意が必要な状態。
WARNING	警告メッセージ。

電子メール アラート応答の作成

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

始める前に

- Firepower Management Center で、自身の IP アドレスを逆解決できることを確認します。
- メール リレー ホストおよび通知アドレスの設定の説明に従って、メール リレー ホストを設定します。

（注） 電子メールアラートを使用して、接続をログに記録することはできません。

手順

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

ステップ 2 [アラートの作成（Create Alert）] ドロップダウン メニューから、[電子メール アラートの作成（Create Email Alert）] を選択します。

ステップ 3 [名前（Name）] にアラート応答の名前を入力します。

ステップ 4 [宛先（To）] フィールドに、アラートを送信する電子メール アドレスをカンマで区切って入力します。

ステップ 5 [送信元（From）] フィールドに、アラートの送信者として表示する電子メール アドレスを入力します。

ステップ 6 [リレー ホスト（Relay Host）] の横に表示されるメール サーバが、アラートの送信に使用するサーバであることを確認します。

ヒント 電子メール サーバを変更するには、編集アイコン（）をクリックします。

ステップ 7 [保存（Save）] をクリックします。

影響フラグ アラートの設定

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）
脅威	保護	任意（Any）	任意（Any）	Admin

特定のインパクト フラグを持つ侵入イベントが発生するたびにアラートが生成されるようにシステムを設定できます。インパクト フラグは、侵入データ、ネットワーク検出データ、および脆弱性情報を関連付けることにより、侵入がネットワークに与える影響を評価するのに役立ちます。

手順

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

ステップ 2 [インパクト フラグ アラート（Impact Flag Alerts）] タブをクリックします。

ステップ 3 [アラート（Alerts）]セクションで、各アラートタイプで使用するアラート応答を選択します。

ヒント 新しいアラート応答を作成するには、任意のドロップダウンリストから[新規（New）]を選択します。

ステップ 4 [インパクト設定（Impact Configuration）] セクションで、該当するチェックボックスをオンにして、各インパクト フラグに対して受信するアラートを指定します。

インパクト フラグの定義については、侵入イベント影響レベルを参照してください。

ステップ 5 [保存（Save）] をクリックします。

検出イベント アラートの設定

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

特定のタイプの検出イベントが発生するたびにアラートが生成されるようにシステムを設定できます。

始める前に

- ネットワーク検出イベント ロギングの設定の説明に従って、アラートを設定する検出イベント タイプを記録するようにネットワーク検出ポリシーを設定します。

手順

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

ステップ 2 [検出イベント アラート（Discovery Event Alerts）] タブをクリックします。

ステップ 3 [アラート（Alerts）]セクションで、各アラートタイプで使用するアラート応答を選択します。

ヒント 新しいアラート応答を作成するには、任意のドロップダウンリストから[新規（New）]を選択します。

ステップ 4 [イベント設定（Events Configuration）] セクションで、各検出イベント タイプに対して、受信するアラートに対応するチェックボックスを選択します。

ステップ 5 [保存（Save）] をクリックします。

ネットワーク向け AMP アラートの設定

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）
マルウェア	マルウェア	任意（Any）	任意（Any）	Admin

レトロスペクティブ インベントなどのマルウェア イベントがネットワーク向け AMP によって生成された（つまり、「ネットワークベースのマルウェア イベント」が生成された）場合は常に通知するようにシステムを設定できます。エンドポイント向け AMP によって生成されたマルウェア イベント（「エンドポイントベースのマルウェア イベント」）にはアラートを生成できません。

始める前に

- マルウェア クラウド ルックアップを実行するファイル ポリシーを設定し、侵入ポリシーとファイル ポリシーを使用したアクセス制御の説明に従って、そのポリシーをアクセス コントロール ルールに関連付けます。

手順

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

ステップ 2 [高度なマルウェア保護アラート（Advanced Malware Protections Alerts）] タブをクリックします。

ステップ 3 [アラート（Alerts）]セクションで、各アラート タイプで使用するアラート応答を選択します。

ヒント 新しいアラート応答を作成するには、任意のドロップダウン リストから [新規（New）] を選択します。

ステップ 4 [イベント設定（Event Configuration）]セクションで、各マルウェア イベント タイプに対して、受信するアラートに対応するチェックボックスを選択します。

[すべてのネットワークベースのマルウェア イベント（All network-based malware events）] には [レトロスペクティブ イベント（Retrospective Events）] が含まれることに注意してください。

（定義により、ネットワークベースのマルウェア イベントにはエンドポイント向け AMP によって生成されたイベントは含まれません。）

ステップ 5 **[Save]** をクリックします。