イベントの検索

シスコのアプライアンスは、データベース テーブルにイベントとして保存される情報を生成します。イベントには、アプライアンスがイベントを生成する原因となったアクティビティを示すいくつかのフィールドが含まれます。

FireSIGHT システムに備わっている定義済みの検索設定をサンプルとして使用すると、ネットワークに関する重要な情報にすばやくアクセスできます。ネットワーク環境に合わせて定義済み検索設定のフィールドを変更し、検索設定を保存して、あとで再利用することができます。また、独自の検索条件を使用することもできます。

検索の種類に応じて、使用できる検索条件は異なりますが、メカニズムは同じです。検索の実行方法と、検索フィールドで使用する正しい構文の詳細については、以下の項を参照してください。

検索設定の実行と保存

ライセンス：任意（Any）

任意のイベント タイプに関する検索設定を作成し、保存することができます。検索設定を作成するときには、その検索設定の名前を付け、それを自分だけで使用するか、それともアプライアンスの全ユーザが使用できるようにするかを指定します。カスタム ユーザ ロールのデータの制限として検索を使用する場合は、**必ず**プライベート検索として保存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。

（注） カスタム テーブルを検索する場合には、少し異なる手順に従います（カスタム テーブルの検索（59-10 ページ）を参照）。

検索の実行

ライセンス：任意（Any）

いくつかのイベント タイプに関しては、FireSIGHT システムに備わっている定義済みの検索設定をサンプルとして使用すると、ネットワークについての重要な情報にすばやくアクセスできます。ネットワーク環境に合わせて定義済み検索設定のフィールドを変更し、検索設定を保存して、あとで再利用することができます。また、独自の検索条件を使用することもできます。

検索を実行する方法：

アクセス：Admin/Any Security Analyst

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

[検索（Search）] 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 リストから、検索するイベント タイプまたはデータを選択します。

適切な検索制約に従ってページが更新されます。

手順 3　該当するフィールドに検索条件を入力します。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「`A`」または「`B`」または「`C, D, E`」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに `A` または `B`、または `C`、`D`、`E` のすべてを含むレコードが一致します。
- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク（*）を受け入れます。
- フィールドでその情報を利用できないイベントを示すには、そのフィールドで `n/a` を指定します。フィールドに情報が入力されているイベントを示すには `!n/a` を使用します。
- 検索条件としてオブジェクトを使用するには、検索フィールドの横に表示されるオブジェクトの追加アイコン（ ＋ ）をクリックします。

手順 4　使用可能な検索条件の詳細については、次の項を参照してください。

- 監査レコードの検索（69-9 ページ）
- アプリケーションの検索（50-48 ページ）
- アプリケーションの詳細の検索（50-53 ページ）
- キャプチャ ファイルの検索（40-37 ページ）

- コンプライアンス ホワイト リスト イベントの検索（52-36 ページ）
- 接続およびセキュリティ インテリジェンスのデータの検索（39-35 ページ）
- 相関イベントの検索（51-64 ページ）
- ディスカバリ イベントの検索（50-18 ページ）
- ファイル イベントの検索（40-14 ページ）
- ヘルス イベントの検索（68-61 ページ）
- ホスト属性の検索（50-33 ページ）
- ホストの検索（50-27 ページ）
- 侵入イベントの検索（41-45 ページ）
- マルウェア イベントの検索（40-29 ページ）
- ルール アップデートのインポート ログの検索（66-29 ページ）
- 修復ステータス イベントの検索（54-23 ページ）
- スキャン結果の検索（47-26 ページ）
- サーバの検索（50-43 ページ）
- サードパーティの脆弱性の検索（50-63 ページ）
- ユーザの検索（50-70 ページ）
- ユーザ アクティビティの検索（50-75 ページ）
- 脆弱性の検索（50-59 ページ）
- ホワイト リスト違反の検索（52-41 ページ）

手順 5　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　カスタム ユーザ ロールのデータの制限として検索を使用する場合は、**必ず**プライベート検索として保存する必要があります。

手順 6　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 7　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、検索されるテーブルのデフォルト ワークフローで表示され、該当する場合には時間で制約されます。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。スキャン結果には別のワークフローを使用**できない**ことに注意してください。

保存済み検索設定のロード

ライセンス：任意（Any）

以前に検索設定を保存した場合、それをロードし、必要に応じて修正して、検索を開始することができます。

保存済みの検索設定をロードする方法：

アクセス：Admin/Any Security Analyst

手順 1　次の選択肢があります。

- ワークフローの任意のページから [検索（Search）] をクリックします。
- [分析（Analysis）] > [検索（Search）] を選択し、検索するイベント タイプを選択します。

[検索（Search）] ページが表示されます。

手順 2　[カスタム検索（Custom Searches）] リストまたは [定義済み検索（Predefined Searches）] リストから、ロードする検索を選択します。

保存済み検索の設定値が検索制約に入力されます。

手順 3　オプションで、検索制約を変更します。

手順 4　[検索（Search）] をクリックします。

検索制約に一致するイベントが表示されます。

保存済み検索設定の削除

ライセンス：任意（Any）

保存済みの検索設定がある場合、[検索（Search）] ページからそれらを削除できます。

保存済み検索設定を削除する方法：

アクセス：Admin/Any Security Analyst

手順 1　次の選択肢があります。

- ワークフローの任意のページから [検索（Search）] をクリックします。
- [分析（Analysis）] > [検索（Search）] を選択し、削除する検索設定のイベント タイプを選択します。

[検索（Search）] ページが表示されます。

手順 2　[カスタム検索(Custom Searches)] リストから削除する検索を選択して、検索名の横に表示される削除アイコン(✖)をクリックします。

検索設定が削除されます。

検索でのワイルドカードと記号の使用

ライセンス:任意(Any)

検索ページの多くのテキスト フィールドでは、文字列内の文字に一致させるためのアスタリスク(*)を使用できます。たとえば `net*` と指定すると、`network`、`netware`、`netscape` などに一致します。

英数字以外の文字(アスタリスク文字を含む)を検索するには、検索文字列を引用符で囲みます。たとえば、次の文字列を検索するには、

```
Find an asterisk (*)
```

次のように入力します。

```
"Find an asterisk (*)"
```

ワイルドカードを使用できるテキスト フィールドで、部分的な文字列に一致させるには、ワイルドカードを使用する**必要**があることに注意してください。たとえば、ページ ビューを含む(つまりメッセージが「ページ ビュー(Page View)」である)すべての監査レコードを監査ログ内で検索する場合、「`Page`」を検索しても結果は返されません。代わりに、「`Page*`」と指定してください。

検索でのオブジェクトとアプリケーション フィルタの使用

ライセンス:任意(Any)

FireSIGHT システムでは、ネットワーク構成の一部として使用可能な名前付きオブジェクト、オブジェクト グループ、およびアプリケーション フィルタを作成できます。検索を実行または保存するときには、検索条件としてこれらのオブジェクト、グループ、およびフィルタを使用できます。

検索を実行するときに、オブジェクト、オブジェクト グループ、およびアプリケーション フィルタは `${object_name}` という形式で表示されます。たとえば、オブジェクト名 `ten_ten_network` であるネットワーク オブジェクトは、検索では `${ten_ten_network}` と表されます。

検索基準としてオブジェクトを使用できる検索フィールドの横にはオブジェクト追加アイコン(✚)が表示され、これをクリックすることができます。

検索での時間制約の指定

ライセンス:任意(Any)

時間による検索制約を指定するには、いくつかの形式を使用できます。一致させる時間を入力し、オプションで、その時間の前後に一致させるために「より小さい」(<)または「より大きい」(>)演算子を入力できます。

時間値を持つ検索条件フィールドで使用可能な形式を、次の表に示します。

表 60-1　検索フィールドにおける時間指定

時間の形式	例
today [at HH:MMam|pm]	today today at 12:45pm
YYYY-MM-DD HH:MM:SS	2006-03-22 14:22:59

時間値の前に、以下のいずれか 1 つの演算子/キーワードを指定できます。

表 60-2　時間指定の演算子

演算子	例	説明
<	< 2006-03-22 14:22:59	2006 年 3 月 22 日午後 2:23 より前のタイムスタンプを持つイベントを返します。
>	> today at 2:45pm	今日の午後 2:45 より後のタイムスタンプを持つイベントを返します。

検索での IP アドレスの指定

ライセンス: 任意（Any）

検索で IP アドレスを指定するときには、個別の IP アドレス、複数アドレスのカンマ区切りリスト、アドレス ブロック、またはハイフン（-）で区切った IP アドレス範囲を入力することができます。また、否定を使用することもできます。

IPv6 をサポートする検索（侵入イベント、接続データ、相関イベントの検索など）では、IPv4 アドレス、IPv6 アドレス、および CIDR/プレフィックス長アドレス ブロックを任意に組み合わせて入力できます。

CIDR またはプレフィックス長の表記を使用して IP アドレスのブロックを指定する場合、FireSIGHT システム は、マスクまたはプレフィックス長で指定されたネットワーク IP アドレスの部分**のみ**を使用します。たとえば、10.1.2.3/8 と入力した場合、FireSIGHT システム では 10.0.0.0/8 が使用されます。

次の表に、IP アドレスを入力する適切な方法を例示します。IP アドレスをネットワーク オブジェクトによって表すことができるため、IP アドレス検索フィールドの横にあるネットワーク オブジェクト追加アイコン（ ＋ ）をクリックして、ネットワーク オブジェクトを IP アドレス検索基準として使用することもできます。詳細については、検索でのオブジェクトとアプリケーション フィルタの使用（60-5 ページ）を参照してください。

表 60-3　使用可能な IP アドレス構文

指定する項目	タイプ	例
単一の IP アドレス	その IP アドレス	192.168.1.1 2001:db8::abcd
リストを使用した複数の IP アドレス	IP アドレスのカンマ区切りリスト。カンマの前後にスペースを追加**しない**でください。	192.168.1.1,192.168.1.2 2001:db8::b3ff,2001:db8::0202

表 60-3　使用可能な IP アドレス構文(続き)

指定する項目	タイプ	例
CIDR ブロックまたはプレフィックス長で指定できる IP アドレスの範囲	IPv4 CIDR または IPv6 プレフィックス長表記の IP アドレス ブロック。	`192.168.1.0/24` これは、サブネット マスク 255.255.255.0 である 192.168.1.0 ネットワーク内の任意の IP を指定します(つまり 192.168.1.0 から 192.168.1.255 まで)。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。
CIDR ブロックやプレフィックスで指定できない IP アドレスの範囲	ハイフンを使用した IP アドレス範囲。ハイフンの前後にスペースを入力**しない**でください。	`192.168.1.1-192.168.1.5` `2001:db8::0202-2001:db8::8329`

他の方法で否定を使用して IP アドレスまたは IP アドレス範囲を指定	IP アドレス、ブロック、または範囲の先頭に感嘆符を付ける。	`192.168.0.0/32,!192.168.1.10`
		`!2001:db8::/32`
		`!192.168.1.10,!2001:db8::/32`

検索でのデバイスの指定

ライセンス:任意(Any)

管理対象デバイスを制約として使用して検索を作成する場合、[デバイス(Device)] 検索条件フィールドに次のいずれかを指定できます。

- 管理対象デバイス名、IP アドレス、またはホスト名
- デバイス グループ名
- デバイス スタック名
- デバイス クラスタ名

システムでグループ、クラスタ、またはスタックの一致が検出されると、検索を実行するために、そのグループ名、クラスタ名、またはスタック名が適切なメンバー デバイス名に置き換えられます。デバイス フィールドのデバイス グループ、クラスタ、またはスタックを使用する検索を保存すると、デバイス フィールドで指定した名前がシステムによって保存され、検索が実行されるたびにデバイス名の置換が再度実行されます。

詳細については、次の各項を参照してください。

- デバイスの操作(4-19 ページ)
- デバイス グループの管理(4-29 ページ)
- スタック構成のデバイスの管理(4-46 ページ)
- デバイスのクラスタリング(4-31 ページ)

検索でのポートの指定

ライセンス:任意（Any）

FireSIGHT システムでは、ポート番号を表す特定の構文を検索で指定できます。次の入力が可能です。

- 単一のポート番号
- 複数のポート番号を含むカンマ区切りリスト
- 2 つのポート番号をハイフンで区切ることにより、ポート番号の範囲を表す
- 1 つのポート番号の後に、スラッシュで区切られたプロトコル省略形（侵入イベントを検索する場合のみ）
- 1 つのポート番号またはポート番号範囲の前に 1 つの感嘆符（指定されたポートの否定を表す）

（注） ポート番号や範囲を指定するときには、スペースを使用**しない**でください。

次の表に、検索制約としてポートを入力する適切な方法を例示します。

\

表 60-4　　ポートの構文例

例	説明
`21`	ポート 21 でのすべてのイベントを返します（TCP および UDP イベントを含む）。
`!23`	ポート 23 上のイベントを除くすべてのイベントを返します。
`25/tcp`	ポート 25 でのすべての TCP 関連の侵入イベントを返します。
`21/tcp,25/tcp`	ポート 21 および 25 でのすべての TCP 関連の侵入イベントを返します。
`21-25`	ポート 21 から 25 までのすべてのイベントを返します。

実行時間が長いクエリの停止

ライセンス:任意（Any）

サポートされるデバイス:任意の Defense Center

システム管理者は、シェル ベースのクエリ管理ツールを使用して、実行時間の長いクエリを検出および停止することができます。

（注） Web インターフェイス内の検索ページを終了しても、クエリは停止しません。長い時間をかけて結果を返すクエリは、クエリ実行中にシステム全体のパフォーマンスに影響を与えます。

クエリ管理ツールでは指定した分数よりも実行時間が長いクエリを検索し、それらのクエリを停止することができます。ユーザがクエリを停止すると、このツールにより監査ログと syslog にイベントが記録されます。

Defense Center でのシェル アクセスを持つローカル作成されたユーザだけが、admin ユーザであることに注意してください。シェル アクセスを与える外部認証オブジェクトを使用する場合、シェル アクセス フィルタに一致するユーザもまたシェルにログインできます。

使用法:

```
query_manager [-v] [-l [minutes]] [-k query_id [...]]
[--kill-all minutes]
```

オプション

`-h, --help`
短いヘルプ メッセージを出力します。

`-l, --list [minutes]`
指定された時間(分単位)を超えるすべてのクエリをリストします。デフォルトでは、1 分より長くかかっているすべてのクエリを表示します。

`-k, --kill query_id [...]`
指定した ID でクエリを強制終了します。オプションには、複数の ID を指定できます。

`--kill-all minutes`
指定された時間(分単位)より長くかかっているすべてのクエリを強制終了します。

`-v, --verbose`
完全な SQL クエリを含む詳細な出力。

注意　シェル アクセスを、システム管理者のみに制限する必要があります。

Defense Center でクエリを停止する方法:

アクセス: admin またはシェル アクセスが付与されたユーザ

手順 1　ssh を使用してDefense Center に接続します。

手順 2　前述の構文を使用して、sudo で query_manager を実行します。