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

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 ロールに関するデータ制約として検索を使用する予定の場合は、それを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」（P.46-9）を参照）。

検索の実行

ライセンス：任意

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

ステップ 1　[Analysis] > [Search] を選択します。

[Search] ページが表示されます。

ステップ 2　[Table] 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リロードされます。

ステップ 3　オプションで、検索設定を保存するには、[Name] フィールドに検索設定の名前を入力します。

名前を入力しない場合、検索の保存時に自動的に名前が作成されます。

ステップ 4　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カンマ区切りの列挙を使用できます。複数の条件を入力すると、すべての基準を満たすレコードのみが検索で返されます。
- 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（*）を使用できます。
- 任意のフィールドで `n/a` を指定すると、そのフィールドの情報がないイベントを識別できます。一方、フィールドに情報があるイベントを識別すには `!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あるオブジェクト追加アイコン（  ）をクリックします。

ステップ 5　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」（P.56-9）
- 「アプリケーションの検索」（P.38-46）
- 「アプリケーションの詳細の検索」（P.38-51）
- 「キャプチャ ファイルの検索」（P.34-29）
- 「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」（P.16-31）
- 「相関イベントの検索」（P.39-58）
- 「ディスカバリ イベントの検索」（P.38-19）
- 「ファイル イベントの検索」（P.34-12）
- 「ヘルス イベントの検索」（P.55-59）

- 「ホスト属性の検索」（P.38-33）
- 「ホストの検索」（P.38-27）
- 「侵入イベントの検索」（P.18-39）
- 「マルウェア イベントの検索」（P.34-24）
- 「スキャン結果の検索」（P.43-26）
- 「サーバの検索」（P.38-42）
- 「脆弱性の検索」（P.38-56）
- 「[Rule Update Import Log] の検索」（P.53-28）
- 「修復ステータス イベントの検索」（P.41-22）
- 「サードパーティの脆弱性の検索」（P.38-60）
- 「ユーザの検索」（P.38-66）
- 「ユーザ アクティビティの検索」（P.38-71）
- 「コンプライアンス ホワイト リスト イベントの検索」（P.27-37）
- 「ホワイト リスト違反の検索」（P.27-42）

ステップ 6　他のユーザが再使用できるような形式で検索を保存する場合には、[Save As Private] チェック ボックスをオフにします。そうでない場合は、このチェック ボックスを選択したままにして、検索をプライベートとして保存します。

ヒント　カスタム ユーザ ロールに関するデータ制約として検索を使用する予定の場合は、それをプライベート検索として保存する**必要があります**。

ステップ 7　次の選択肢があります。

- 検索を開始するには、[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 タイトルの近くの [（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。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。
- 既存の検索を変更している場合、[Save] をクリックすると変更内容が保存されます。
- [Save As New Search] をクリックすると、検索条件が保存されます。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て保存され）、あとでそれを使用できます。

保存済み検索設定のロード

ライセンス：任意

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

ステップ 1　次の 2 つのオプションから選択できます。

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

[Search] ページが表示されます。

ステップ 2　ページの左側にある保存済み検索設定のリストから、ロードする検索設定を選択し、[Load] をクリックします。

保存済み検索設定の設定値が検索制約フィールドに入力されます。

ステップ 3　オプションで、検索制約を変更します。

ステップ 4　[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

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

保存済みの検索設定を削除する方法：

アクセス：Admin/Any Security Analyst

ステップ 1　次の 2 つのオプションから選択できます。

- ワークフローの任意のページから [Search] をクリックします。
- [Analysis] > [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。

[Search] ページが表示されます。

ステップ 2　保存済み検索設定のリストから、削除する検索設定を選択して [Delete] 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

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「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

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

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 45-1　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（今日の午後 12:45）
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 45-2　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

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 またはプレフィクス長の表記を使って IP アドレスのブロックを指定すると、FireSIGHT システムは、マスクまたはプレフィクス長で指定されたネットワーク IP アドレス部分**のみ**を使用します。たとえば `10.1.2.3/8` と入力すると、FireSIGHT システムは `10.0.0.0/8` を使用します。

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」（P.45-5）を参照してください。

表 45-3　使用可能な IP アドレス構文

指定する項目	入力内容	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 アドレスからなる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`
CIDR ブロックまたはプレフィ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 アドレスの表記法」（P.1-19）を参照してください。

表 45-3　使用可能な IP アドレス構文 （続き）

指定する項目	入力内容	例
CIDR ブロックやプレフィ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

検索でのポートの指定

ライセンス：任意

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 45-4　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

サポート対象デバイス：任意防御センター

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、指定した分数より長く実行されているクエリを検出し、それらのクエリを停止することができます。クエリを停止すると、このツールによって監査ログと syslog にイベントが記録されます。

防御センターでのシェル 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。

使用方法：

```
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ーを表示します。

`-k, --kill query_id [...]`
ID で指定されるクエリを強制終了します。このオプションでは、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。

防御センター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

ステップ 1　ssh を使用して防御センターに接続します。

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