イベント検索

以下のトピックでは、ワークフロー内のイベントの検索方法について説明します。

イベントの検索

システムでは、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が生成されます。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。ご使用の環境用にカスタマイズされた、さまざまなイベントタイプの検索を作成および保存し、後で再使用するために保存できます。

検索設定を保存するときには、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。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。カスタム分析のダッシュボード ウィジェット、レポート テンプレート、カスタム ユーザ ロールも、保存した検索を使用できます。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。

いくつかのイベントタイプに関しては、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、後で再利用することができます。

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。

（注） カスタム テーブルの検索には、若干異なる手順が必要です。

関連トピック

カスタム テーブルの検索

検索の制約

データベーステーブルごとに、検索を制約する値を入力できる独自の検索ページがあります。入力した値は、そのテーブルに定義されているフィールドに適用されます。フィールドのタイプによっては、特殊なシンタックスを使用して、ワイルドカード文字や数値の範囲などの基準を指定できます。

検索結果はワークフローページに表示され、カラム式レイアウトでテーブルの各フィールドが示されます。一部のデータベース テーブルは、ワークフロー ページにカラムとして表示されないフィールドを使用した検索も行えます。ワークフローページで結果を確認する際に、該当する制約が検索結果に適用されているかどうかを判別するには、**[展開矢印（Expand Arrow）]**（  ） をクリックして、検索に現在有効になっている制約を表示します。

一般的な検索の制約

イベントを検索するときは、次の一般的な注意事項を順守してください。

- 多くのフィールドでは、部分一致検索にワイルドカードが必要です。これらの検索では、すべてのフィールドでワイルドカードを使用できます。

  検索で使用するワイルドカードと記号 （3 ページ）を参照してください。

- 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。

- 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。
- 多くの数値フィールドの前には、より大きい（>）、以上（>=）、より小さい（<）、以下（<=）、等しい（=）または等しくない（<>）の演算子を付けることができます。

ヒント 長い複雑な値を（SHA-256ハッシュ値など）を含むフィールドを検索する場合は、ソース資料から検索基準値をコピーし、検索ページの適切なフィールドに貼り付けることができます。

検索で使用するワイルドカードと記号

接続イベントとセキュリティ インテリジェンス イベントのすべてのテキストフィールド、および他のイベントタイプのほとんどのテキストフィールドを検索する場合、テキストフィールドで部分一致を検索するには、文字列内の指定されていない文字を表すためにアスタリスク（*）が必要です。アスタリスクを使用しない検索は、これらのフィールドでの完全一致検索になります。ワイルドカードを必要としないフィールドでも、部分一致検索には常にワイルドカードを使用することを推奨します。

たとえば、`example.com`、`www.example.com`、または `department.example.com` を見つけるには、`*.example.com` で検索します。`example.com` で検索すると、ほとんどの場合、`example.com` のみが返されます。

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とします。

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

次のように入力します。

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

検索でのオブジェクトとアプリケーションのフィルタ

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（Object）]**（⊕） が表示され、これをクリックすることができます。

関連トピック

オブジェクト マネージャ

検索で指定する時間制約

時間値を指定できる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 *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-DD*MM- *HH*:*MM*:*SS*	`2006-03-22 14:22:59`

時間値の前に、以下のいずれか 1 つの演算子を指定できます。

表 *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 時 45 分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

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。IP アドレスを使用してホストを検索した場合、結果には、少なくとも 1 つの IP アドレスが検索条件と一致するホストがすべて含まれます（つまり、IPv6 のアドレスの検索では、プライマリ アドレスが IPv4 であるホストが返されることがあります）。

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、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` と入力すると、システムは `10.0.0.0/8` を使用します。

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の追加の**[オブジェクト（Object）]**（⊕）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。

表 *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）。
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`

ブロックされたホストまたはモニター対象の（そうでなければブロックされた）ホスト ホスト プロファイルのアイコンを参照してください。	接続イベントとセキュリティ インテリジェンス イベントの、[イニシエータIP（Initiator IP）] フィールドと [レスポンダIP（Responder IP）] フィールド： • block • monitor	--

関連トピック

IP アドレスの規則

検索での URL

URL を検索するときは、ワイルドカードを含めます。たとえば、***example.com*** を使用すると、**https://example.com**、**division.example.com**、**example.com/division/** など、ドメインのすべてのバリエーションを検索します。

検索での管理対象デバイス

デバイスをグループ化している場合（Management Center で、または実際の高可用性設定あるいは拡張性設定として）、グループの名前を検索すると、グループ内のすべてのデバイスに対する結果が正しく返されます。

システムでグループ、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。

検索でのポート

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。

- 1 つのポート番号
- コンマで区切られたポート番号リスト
- ポート番号範囲を示すのにダッシュで区切られた 2 つのポート番号
- 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。

表 *4:* ポート構文例

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 の TCP 関連侵入イベントをすべて戻します。
`21/tcp,25/tcp`	ポート 21、25 の TCP 関連侵入イベントをすべて戻します。
`21-25`	ポート 21 から 25 のイベントをすべて戻します。

検索のイベント フィールド

イベントを検索するときは、検索条件として次のフィールドを使用できます。

- 監査ログのワークフロー フィールド
- アプリケーション データ フィールド
- アプリケーションの詳細データ フィールド
- キャプチャされたファイルのフィールド
- 許可（Allow）リストイベントのフィールド
- 接続およびセキュリティ関連の接続イベントフィールド
- 相関イベントのフィールド
- ディスカバリ イベントのフィールド
- [ヘルス イベント（Health Events）] テーブル
- ホスト属性データ フィールド
- ホスト データ フィールド
- ファイルおよびマルウェア イベント フィールド
- 侵入イベント フィールド
- 侵入ルール更新のログの詳細
- 修復ステータスのテーブル フィールド
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Nmap Scan Results Fields*」を参照してください
- サーバー データ フィールド
- サードパーティの脆弱性データのフィールド
- ユーザー関連フィールド
- 脆弱性データのフィールド
- 許可（Allow）リスト違反のフィールド

検索の実行

検索を実行するには、管理者権限またはセキュリティアナリスト権限が必要です。

手順

ステップ 1 **[分析（Analysis）] > [検索（Search）]** を選択します。

ヒント また、ワークフローの任意のページから [検索（Search）] をクリックすることもできます。

ステップ 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。

ステップ 3 該当するフィールドに検索基準を入力します。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。

- 検索の制約 （2 ページ）
- 監査ログのワークフロー フィールド
- アプリケーション データ フィールド
- アプリケーションの詳細データ フィールド
- キャプチャされたファイルのフィールド
- 許可（Allow）リストイベントのフィールド
- 接続およびセキュリティ関連の接続イベントフィールド
- 相関イベントのフィールド
- ディスカバリ イベントのフィールド
- [ヘルス イベント（Health Events）] テーブル
- ホスト属性データ フィールド
- ホスト データ フィールド
- ファイルおよびマルウェア イベント フィールド
- 侵入イベント フィールド
- 侵入ルール更新のログの詳細
- 修復ステータスのテーブル フィールド
- Cisco Secure Firewall Management Center デバイス構成ガイドの「*Nmap Scan Results Fields*」を参照してください
- サーバー データ フィールド
- サードパーティの脆弱性データのフィールド
- ユーザー データのフィールド
- ユーザー アクティビティ データのフィールド
- 脆弱性データのフィールド
- 許可（Allow）リスト違反のフィールド

ステップ 4 将来検索を再度使用する場合は、その検索を保存します。詳細については、検索設定の保存 （9 ページ）を参照してください。

ステップ 5 [検索（Search）] をクリックして、検索を開始します。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。

次のタスク

- ワークフローを使用して検索結果を分析する場合は、ワークフローの使用を参照してください。

関連トピック

イベント ビューの設定

検索設定の保存

検索を保存するには、管理者権限またはセキュリティアナリスト権限が必要です。

マルチドメイン展開では、現在のドメインで作成された保存済みの検索が表示されます。これは編集できます。先祖ドメインで作成された保存済みの検索も表示されますが、これは編集できません。下位のドメインで作成された検索を表示および編集するには、そのドメインに切り替えます。

始める前に

- 検索の実行 （7 ページ）で説明するように検索条件を設定するか、保存済み検索設定のロード （10 ページ）で説明するように保存した検索をロードします。

手順

ステップ 1 [検索（Search）] ページから、自分だけがアクセスできるように検索設定をプライベートとして保存する場合は、[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。

ステップ 2 次の 2 つの対処法があります。

- ロードした検索設定の新しいバージョンを保存する場合は、[新規に保存（Save As New）] をクリックします。
- 新しい検索結果を保存する場合や、同じ名前を使用してカスタム検索を上書きする場合は、[保存（Save）] をクリックします。 コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

保存済み検索設定のロード

保存済み検索をロードするには、管理者権限またはセキュリティアナリスト権限が必要です。

マルチドメイン展開では、現在のドメインで作成された保存済みの検索が表示されます。これは編集できます。先祖ドメインで作成された保存済みの検索も表示されますが、これは編集できません。下位のドメインで作成された検索を表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 **[分析（Analysis）]** > **[検索（Search）]**を選択します。

ヒント また、ワークフローの任意のページから [検索（Search）] をクリックすることもできます。

ステップ 2 テーブルのドロップダウンリストから、検索するイベントまたはデータのタイプを選択します。

ステップ 3 [カスタム検索（Custom Searches）] リストまたは [定義済の検索（Predefined Searches）] リストから、ロードする検索を選択します。

ステップ 4 別の検索条件を使用するには、検索の制約を変更します。

ステップ 5 変更した検索を将来再度使用する場合は、検索を保存しておきます。詳細については、検索設定の保存 （9 ページ）を参照してください。

ステップ 6 **[検索（Search）]** をクリックします。

シェルによるクエリ オーバーライド

システム管理者は、Linux 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。

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。ユーザー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。

`admin` 内部ユーザーは Management Center CLI にアクセスできることに注意してください。CLI 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ーもまた CLI にログインできます。

（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。

シェルベースのクエリ管理の構文

実行時間が長いクエリを管理するには、次の構文を使用します。

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

表 5: *query_manager* オプション

オプション	説明
`-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、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 [...]`	指定された ID を持つクエリを強制終了します。オプションは複数の ID を取得する場合があります。
`--kill-all minutes`	指定された時間（分単位）を超え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 システム セキュリティ上の理由から、アプライアンスでは追加の Linux シェル ユーザーを確立しないことを強く推奨します。

実行時間が長いクエリの停止

CLI アクセス権がある **admin** ユーザーまたは外部で認証されたユーザーである必要があります

手順

ステップ 1 `ssh` を使用して Secure Firewall Management Center に接続します。

ステップ 2 CLI `expert` コマンドを使用して Linux シェルにアクセスします。

ステップ 3 シェルベースのクエリ管理の構文 （11 ページ）で説明された構文を使用して、`sudo` で `query_manager` を実行します。

イベントの検索の履歴

機能	最小 Management Center	最小 Threat Defense	詳細
多くのフィールドでの部分一致検索では、ワイルドカードが必要になりました	6.6	任意（Any）	たとえば、URL を検索する場合、**`*example.com*`** を使用して、**`example.com`** のすべてのバリエーションを検索します。 この動作の変更は、接続またはセキュリティ インテリジェンス イベントを検索するときの、[分析（Analysis）] > [検索（Search）] ページでの検索に適用されます。この検索ページは、他のページのリンクからもアクセスできます。 部分一致検索にワイルドカードを必要としないフィールドでは、オプションでワイルドカードを使用できます。 影響を受けるプラットフォーム：Management Center

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。