### mpsearch

数千件以上のキーワードパターンを高速かつ一括で検索します。サブクエリで指定されたパターンが検索対象フィールドで検出されると、**\_mp\_result**フィールドに検出されたすべてのパターンリストを含めて出力します。

#### 構文

mpsearch FIELD,... [ SUBQUERY ]

**FIELD,...**

マルチパターンを検索する対象フィールドのリスト。カンマ（,）で区切ります。フィールドを指定しない場合、すべてのフィールドが検索対象となります。

**[ SUBQUERY ]**

検索するキーワードパターンのリストを取得するクエリ文を角括弧（[ ]）内に記述します。

#### 説明

サブクエリの出力には、**expr**、**expr2**、**rule**の文字列フィールドを含める必要があります。

* **expr**（必須）：文字列をブール式で組み合わせて記述します。スキャン対象フィールドの文字列値から該当する文字列を高速に検出した後、式と一致するかを確認します。
* **expr2**（任意）：**expr**フィールドのブール式が真の場合、他のフィールドの値を利用して追加検索を行う機会を任意で提供します。
* **rule**（必須）：パターン識別子または名称を記述します。

パターンの例は以下の通りです。

**パターン例**

|  |  |  |
| --- | --- | --- |
| expr（必須） | expr2（任意） | rule（必須） |
| "addextendedproc" and "xp\_cmdshell" |  | xp\_cmdshell |
| "REMOTE\_ADDR" and ("fputs" or "fwrite") | path == "lib.php" | zb now\_connect |

たとえば、xp\_cmdshellパターンのみが検出された場合、**\_mp\_result**フィールドの値は以下のようになります。

[ { "expr": "\"addextendedproc\" and \"xp\_cmdshell\"", "rule": "xp\_cmdshell" } ]

#### 使用例

外部DBからパターンリストをロードし、signatureフィールドを対象にマルチパターンマッチングを実行する例：

mpsearch signature [ dbquery RULE\_DB select rule, expr, expr2 from web\_rules ]