### search

指定した式と一致する入力データを検索します。

#### 構文

search [limit=INT] EXPR

必須パラメータ

**EXPR**

検索条件式。例えば、"KEY == VALUE" または "KEY != VALUE" 形式の比較条件式、あるいはブール条件式を指定できます。and、or などの論理演算子を用いて条件式を組み合わせることも可能です。

EXPRが真の場合のみ、データは次のクエリコマンドに渡されます。

オプションパラメータ

**limit=INT**

返却する最大レコード数（デフォルト：制限なし）

#### 使用例

**line**フィールドにgameという文字列を含むログ（ワイルドカード対応）

search line == "\*game\*"

ステータスコードが200ではないログ

search status != 200

src\_ipが1.2.3.4で、かつdst\_portが22の場合

search src\_ip == ip("1.2.3.4") and dst\_port == 22