### stats

グループを対象として動作する集計関数の評価結果を出力します。

#### 構文

stats [parallel=BOOL] AGGR\_FUNC [as ALIAS], ... [by GRP\_FIELD, ...]

必須パラメータ

**AGGR\_FUNC [as ALIAS], ...**

実行する集計関数（AGGR\_FUNC）を用いて式を入力します。as句を利用して、集計関数の値を格納するフィールド名（ALIAS）を指定できます。名前を指定しない場合、**count()**、**sum(sent\_pkts)** など関数名がフィールド名として使用されるため、フィールド名（ALIAS）を指定することを推奨します。

オプションパラメータ

**parallel=BOOL**

クエリ結果の並列出力の有無（デフォルト: f）。処理速度は向上しますが、データの順序は保証されません。データの順序が重要なクエリでは、このオプションを使用しないでください。

1. t: クエリ結果を並列で出力
2. f: クエリ結果を並列で出力しない

**by GRP\_FIELD, ...**

by句を利用して、集計関数の結果をグループ化するフィールドを指定します。グループ化フィールドを指定しない場合、前のクエリコマンドから渡された全ログを1つのグループとして計算します。グループフィールドを基準にソートされる副次的な効果もあります。

#### 使用例

全レコード数の集計

stats count

**src\_ip**フィールドごとのレコード数を集計

stats count by src\_ip

**src\_ip**、**dst\_ip**フィールドの組み合わせでグループ化し、レコード数を集計

stats count by src\_ip, dst\_ip

**src\_ip**、**dst\_ip**フィールドの組み合わせでグループ化し、[sum(bytes)](https://docs.logpresso.comnull)およびレコード数（[count](https://docs.logpresso.comnull)）を集計

stats sum(bytes) as bytes, count by src\_ip, dst\_ip