### timechart

指定した時間単位ごとに集計関数の結果を計算します。by句でグループフィールドを指定した場合、グループフィールドの値ごとにフィールドが生成され、フィールドごとの統計値が算出されます。

#### 構文

timechart span=INT{y|mon|w|d|h|m|s} AGGR\_FUNC [as ALIAS], ... [by GRP\_FIELD, ...]

必須パラメータ

**span=INT{y|mon|w|d|h|m|s}**

**\_time**フィールドの時間単位を指定します。y（年）、mon（月）、w（週）、d（日）、h（時）、m（分）、s（秒）単位で指定可能です。例えば、10mは10分単位を意味します。月単位monを使用する場合、集計が可能なのは12の約数である1mon、2mon、3mon、4mon、6monのみです。つまり、3monは許可されますが、5monは許可されません。12monの代わりに1yを使用してください。単位がyの場合、1yのみ指定可能です。

**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)\*\*のように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

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

集計に使用するグループフィールドのリスト。区切り文字はカンマ（,）です。

#### 使用例

10分単位のログ発生件数

timechart span=10m count

1分単位でのbytesの推移

timechart span=1m sum(bytes)

各宛先ポートごとの1時間単位ログ発生件数

timechart span=1h count by dst\_port