### rex

指定したフィールドから正規表現を用いてフィールドを抽出します。

#### 構文

rex field={FIELD|line} "REGEX"

必須パラメータ

**field=FIELD**

正規表現を用いて文字列を抽出する対象フィールド。

**"REGEX"**

フィールド名を付与できる拡張正規表現。正規表現グループを作成する際に (?<field>.\*) の形式で指定すると、グループにマッチした文字列を**field**フィールドに出力します。

#### 使用例

**line**フィールドからGET /game/flash/またはPOST /game/flash/で始まるファイルパスを検索し、マッチした文字列を**filename**フィールドに出力

rex field=line "(GET|POST) /game/flash/(?<filename>([^ ]\*))"

**line**フィールドからタイムスタンプパターンの文字列を抽出し、**timestamp**フィールドに出力

rex field=line "(?<timestamp>\d+-\d+-\d+ \d+:\d+:\d+)"

**line**フィールドから文字列を抽出し、**url**および**querystring**フィールドに出力

rex field=line "(GET|POST) (?<url>[^ ]\*) (?<querystring>[^ ]\*) "