### ログスキーマ参照

指定したログスキーマのフィールド構成情報を取得します。

#### HTTPリクエスト

GET /api/sonar/log-schemas/:code

cURL例

curl -H "Authorization: Bearer <API\_KEY>" \ https://HOSTNAME/api/sonar/log-schemas/session

リクエストパラメータ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| キー | 必須 | 型 | 説明 | 備考 |
| code | ○ | 文字列 | ログスキーマコード |  |

#### 正常応答

以下は、sessionログスキーマに対する参照例です。

{ "schema": { "code": "session", "name": "セッション", "description": "ファイアウォールセッションおよびネットワークフロー", "created": "2022-09-01 00:31:13+0900", "fields": [ { "name": "\_time", "display\_name": "時刻", "type": "DATE", "ordinal": 1 }, { "name": "src\_ip", "display\_name": "送信元IP", "type": "IP", "ordinal": 2 }, { "name": "src\_port", "display\_name": "送信元ポート", "type": "PORT", "ordinal": 3 }, { "name": "dst\_ip", "display\_name": "宛先IP", "type": "IP", "ordinal": 4 }, { "name": "dst\_port", "display\_name": "宛先ポート", "type": "PORT", "ordinal": 5 }, { "name": "protocol", "display\_name": "プロトコル", "type": "STRING", "ordinal": 6 }, { "name": "app", "display\_name": "アプリケーション", "type": "STRING", "ordinal": 7 }, { "name": "action", "display\_name": "対応", "type": "STRING", "ordinal": 8 }, { "name": "nat\_src\_ip", "display\_name": "NAT送信元IP", "type": "IP", "ordinal": 9 }, { "name": "nat\_src\_port", "display\_name": "NAT送信元ポート", "type": "PORT", "ordinal": 10 }, { "name": "nat\_dst\_ip", "display\_name": "NAT宛先IP", "type": "IP", "ordinal": 11 }, { "name": "nat\_dst\_port", "display\_name": "NAT宛先ポート", "type": "PORT", "ordinal": 12 }, { "name": "policy", "display\_name": "ポリシー", "type": "STRING", "ordinal": 13 }, { "name": "duration", "display\_name": "接続時間", "type": "LONG", "ordinal": 14 }, { "name": "total\_bytes", "display\_name": "バイト数", "type": "STRING", "ordinal": 15 }, { "name": "total\_pkts", "display\_name": "パケット数", "type": "STRING", "ordinal": 16 }, { "name": "sent\_pkts", "display\_name": "送信パケット数", "type": "LONG", "ordinal": 17 }, { "name": "rcvd\_pkts", "display\_name": "受信パケット数", "type": "LONG", "ordinal": 18 }, { "name": "sent\_bytes", "display\_name": "送信バイト数", "type": "LONG", "ordinal": 19 }, { "name": "rcvd\_bytes", "display\_name": "受信バイト数", "type": "LONG", "ordinal": 20 }, { "name": "src\_country", "display\_name": "送信元国", "type": "COUNTRY", "ordinal": 21 }, { "name": "dst\_country", "display\_name": "宛先国", "type": "COUNTRY", "ordinal": 22 } ] }}

* **schema**（マップ）: ログスキーマ定義
* **code**（文字列）: コード
* **name**（文字列）: 名称
* **description**（文字列）: 説明
* **created**（文字列）: 作成日時（yyyy-MM-dd HH:mm:ssZ形式）
* **fields**（配列）: 正規化されたフィールド定義リスト
* **name**（文字列）: フィールド名
* **display\_name**（文字列）: 表示名
* **type**（文字列）: 型。DATE、STRING、IP、PORT、INT、LONG、DOUBLE、COUNTRY、MD5、SHA1、URLのいずれか。
* **ordinal**（32ビット整数）: フィールド表示順

#### エラー応答

ログスキーマが存在しない場合

HTTPステータスコード 200 で応答

{ "schema": null}