ハニーポット攻撃ログの
データ分析

王磊
9月28日

攻撃のパタン

特徴は3つのカテゴリーにわけました

- **時間**
- 場所
- テクニック

特徴のカテゴリー

- **時間のカテゴリー:**
  - date
  - month
  - day
  - hour at Japan time
  - hour at local time

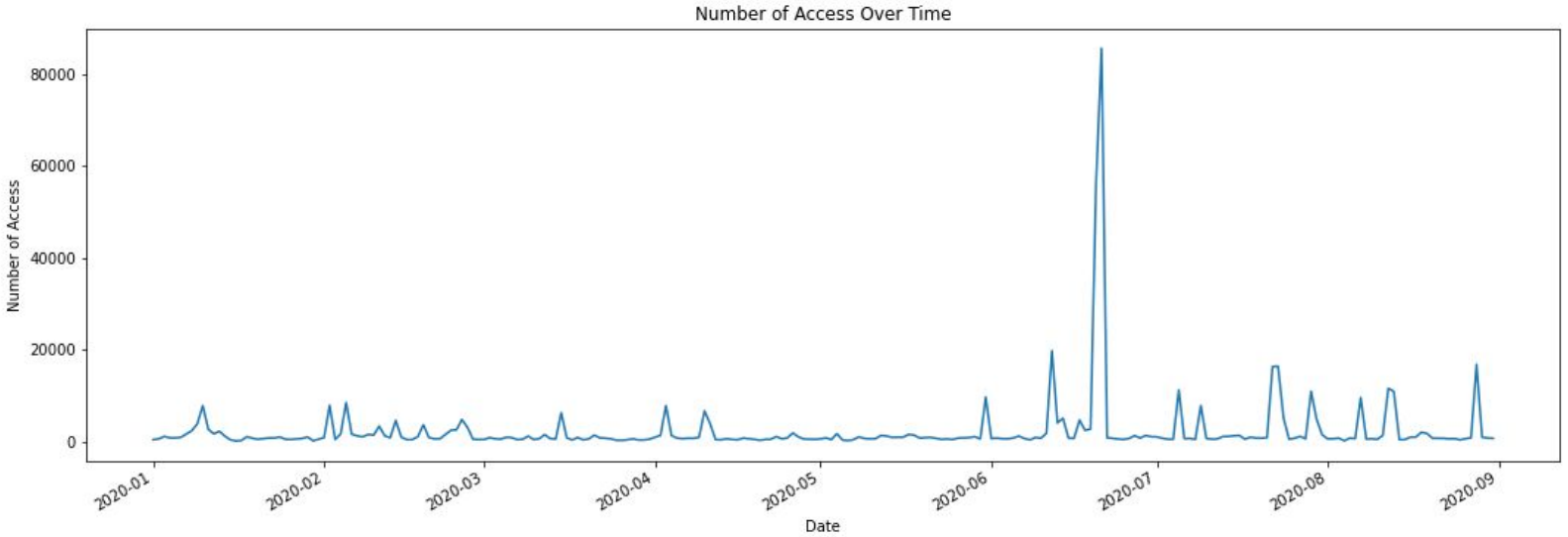
特徴のカテゴリー

- **場所のカテゴリー:**
  - IP
  - country
  - city

特徴のカテゴリー

- **テクニックのカテゴリー:**
  - method
  - Http version

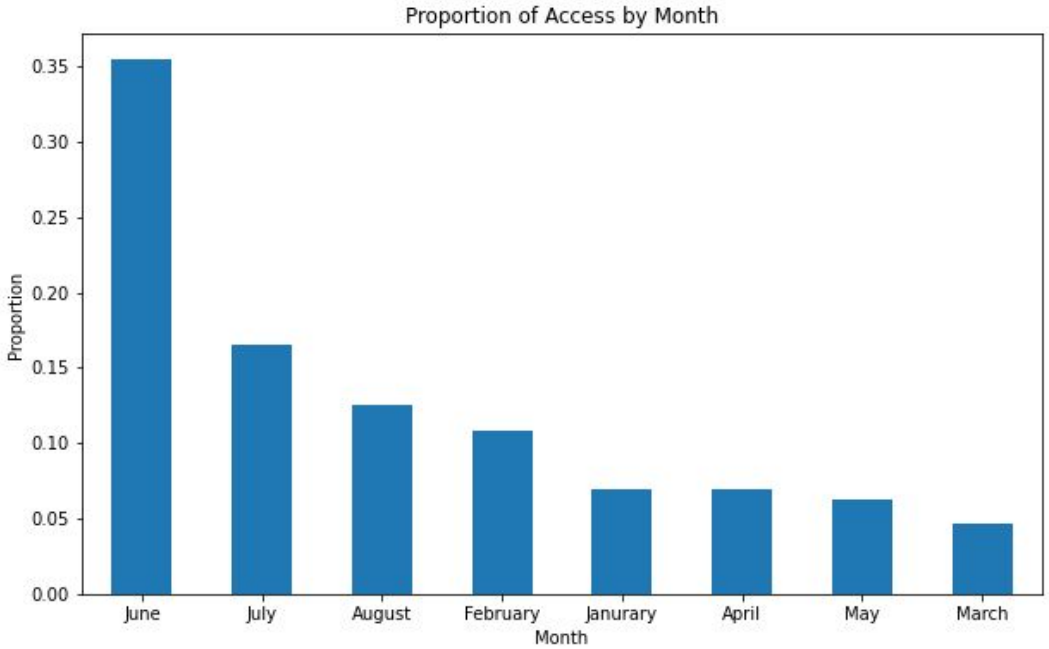
時間について— date



6月にピークがあります、他の月は小さいピークだけあります

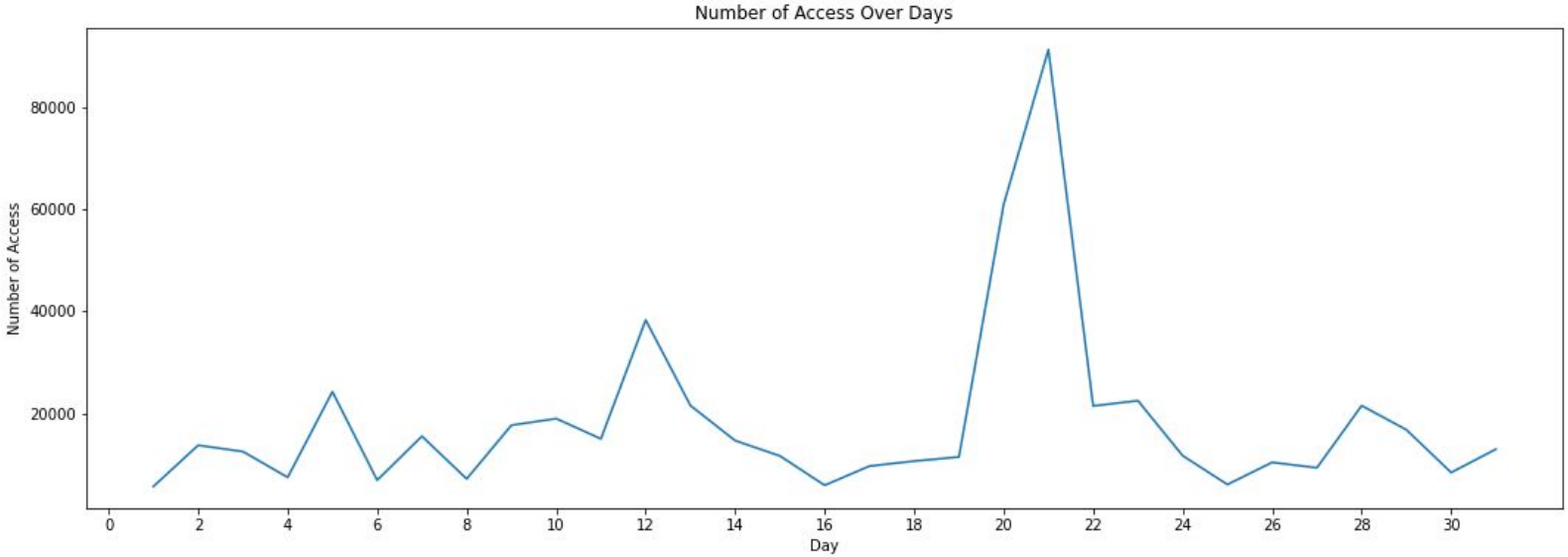
6月以後(6月-8月)ピークが多い

時間について— month



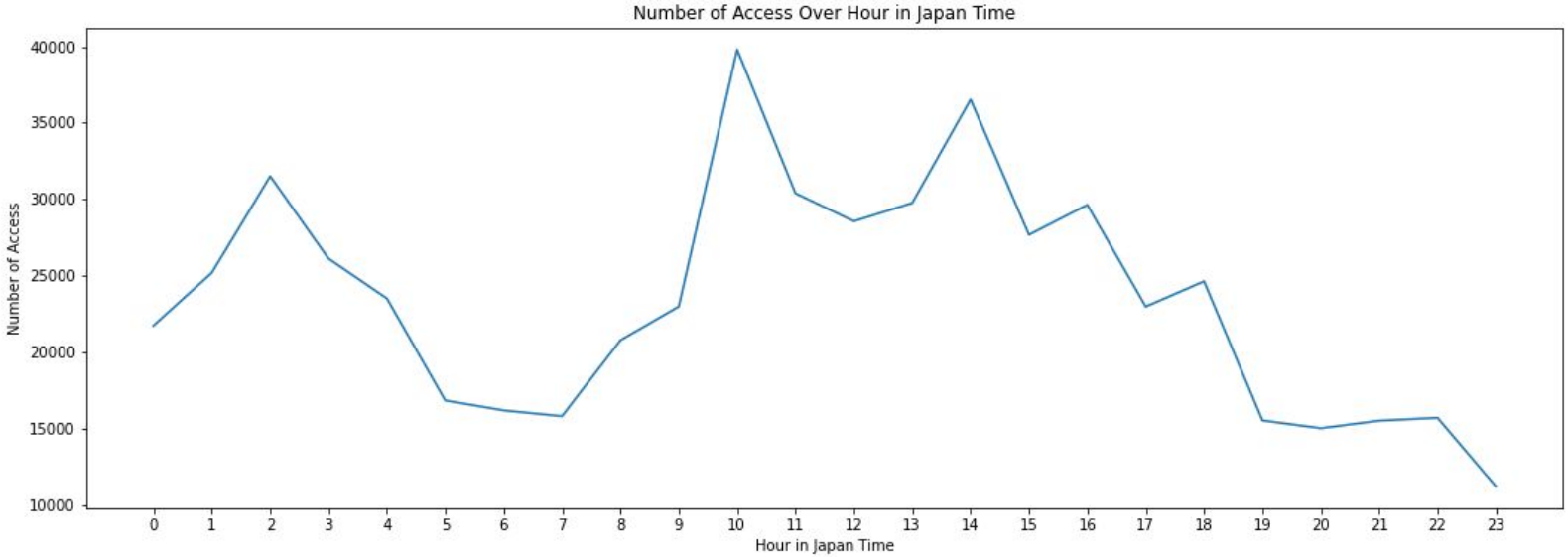
6月の攻撃数が最も多く、
6月、7月、8月の攻撃数は他の月よりも多い

時間についてー day



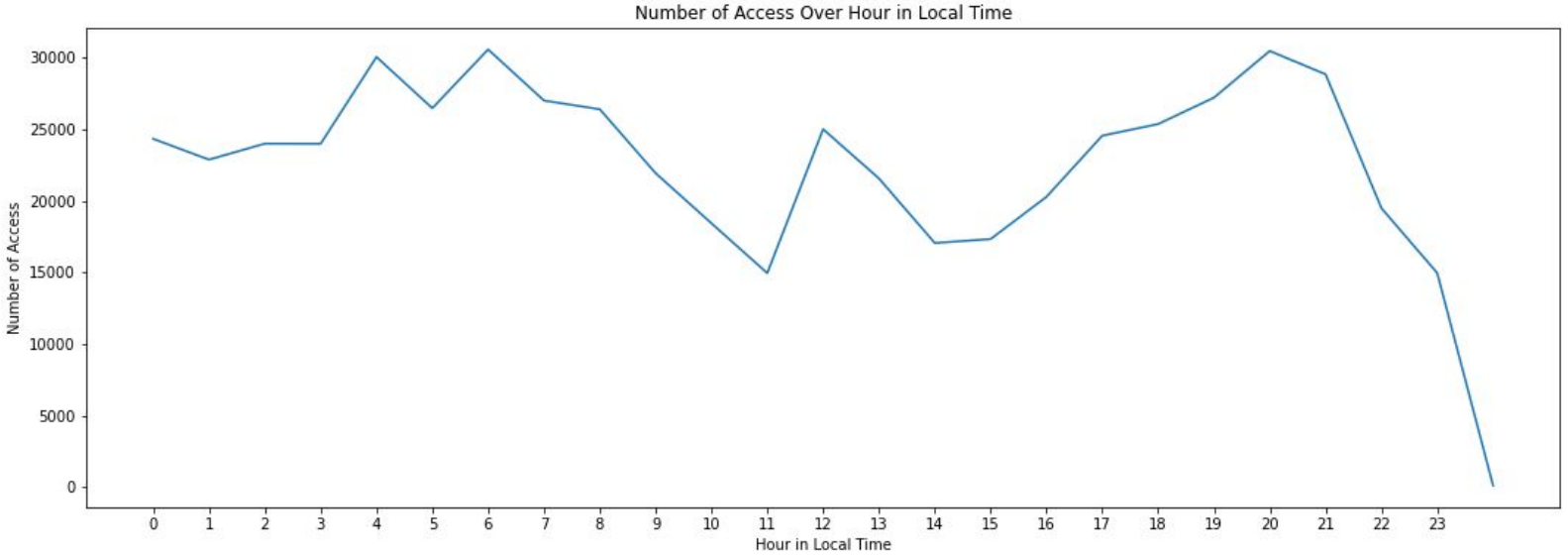
一般に、21日と12日攻撃数が比較的に多い

時間について— hour (JP time)



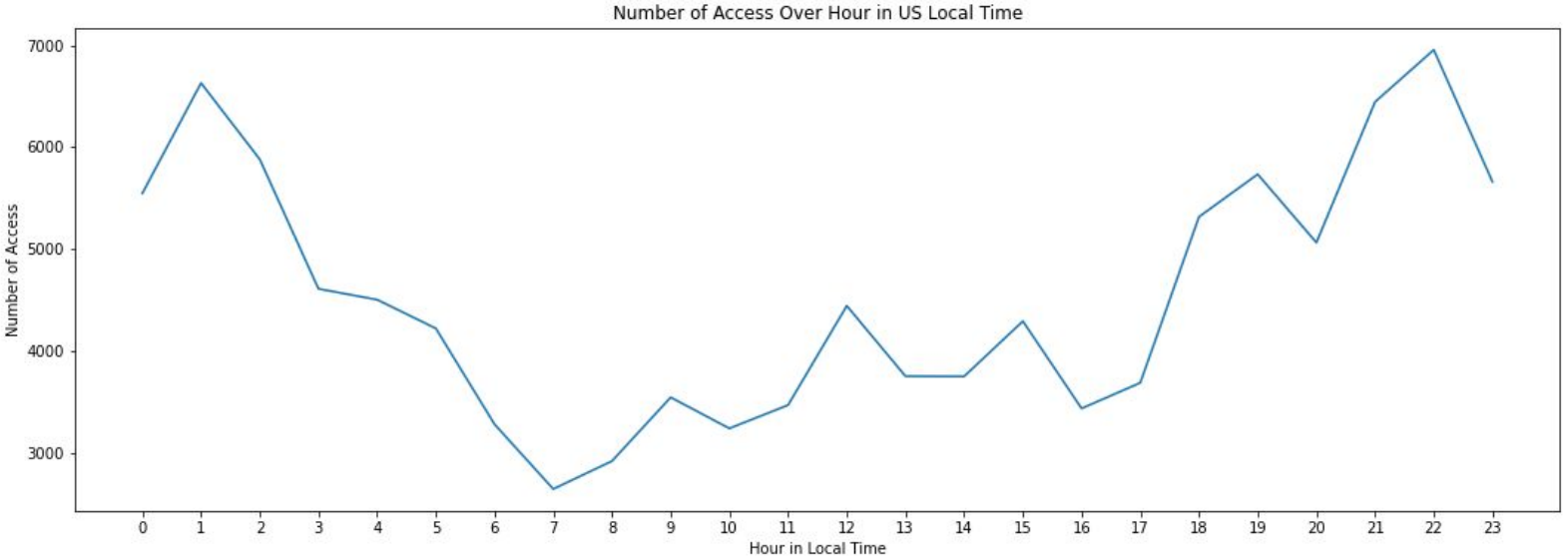
午前10時と午後2時、攻撃数が比較的に多い

時間について— hour (local time all)



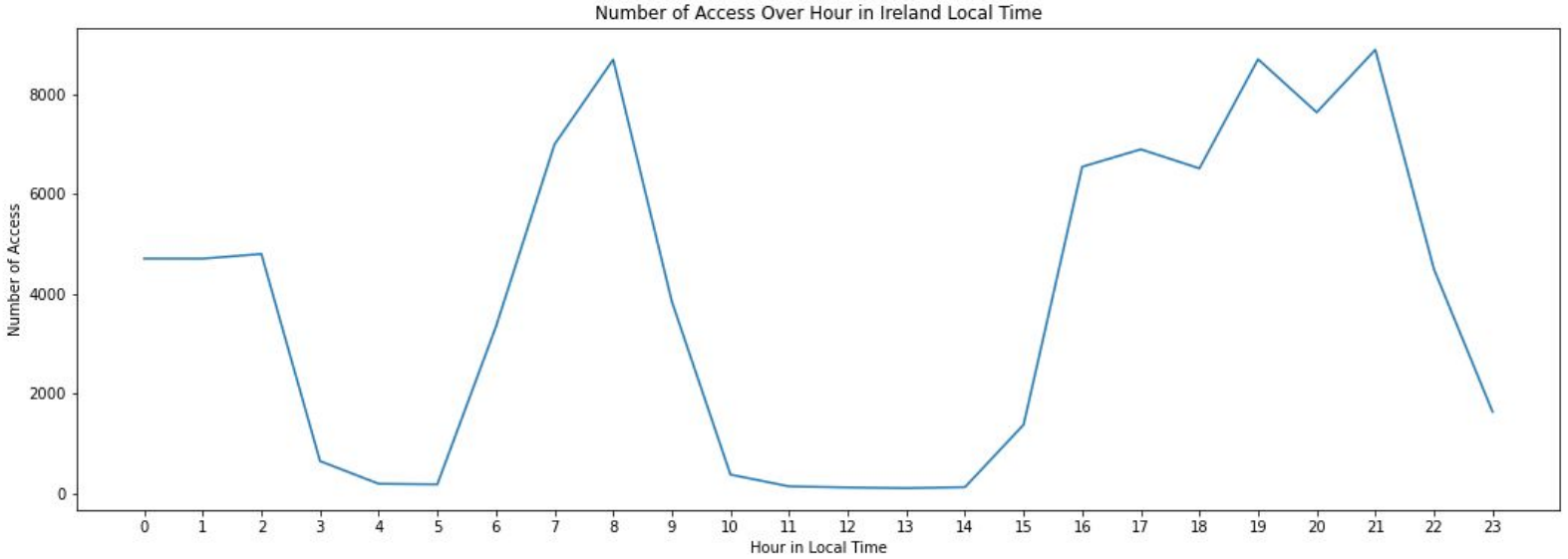
午前4時、6時、午後8時、攻撃数が比較的に多い

時間について— hour (US local time)



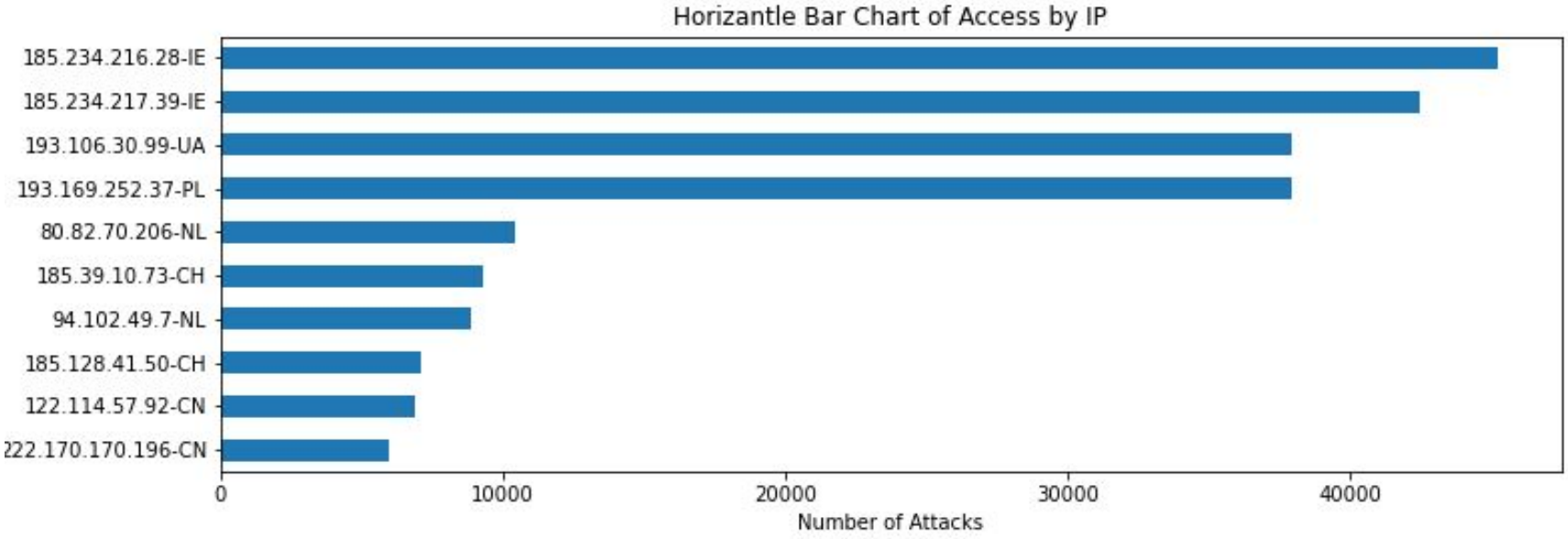
アメリカからの攻撃は、午前 1時、午後22時、攻撃数が比較的に多い

時間について— hour (Ireland local time)



Irelandからの攻撃は、午前 8時、午後19/21時、攻撃数が比較的に多い

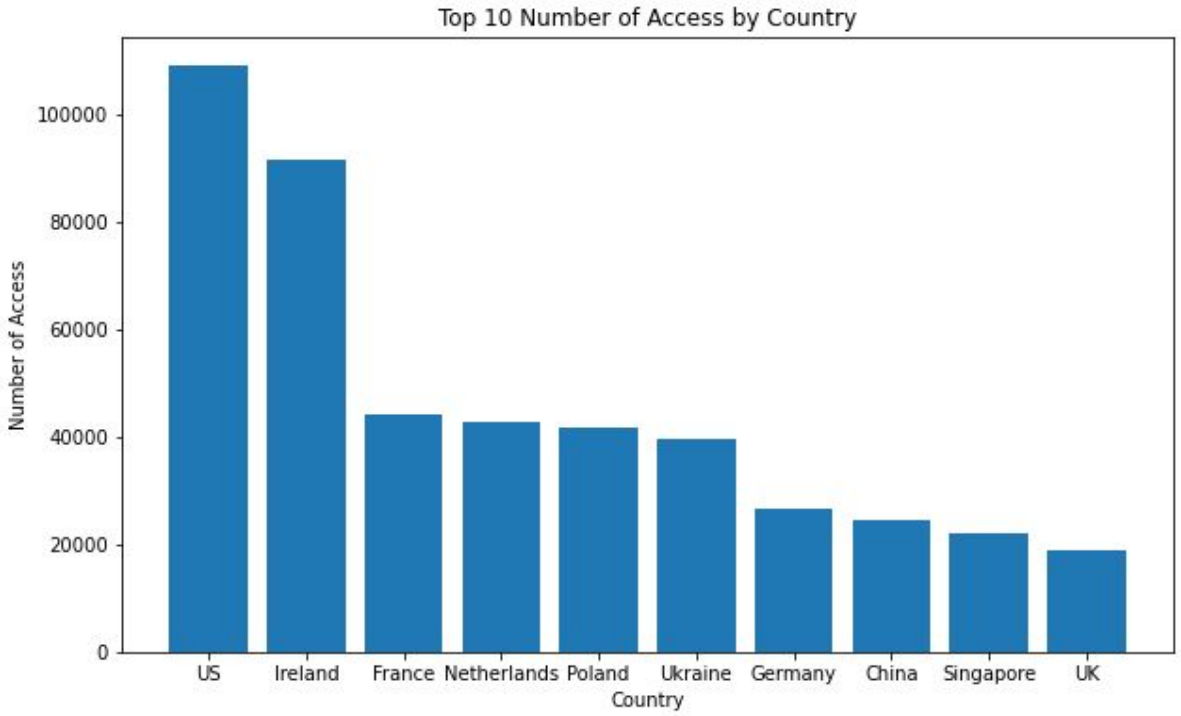
場所について— IP


Horizantle Bar Chart of Access by IP
185.234.216.28-IE
185.234.217.39-IE
193.106.30.99-UA
193.169.252.37-PL
80.82.70.206-NL
185.39.10.73-CH
94.102.49.7-NL
185.128.41.50-CH
122.114.57.92-CN
222.170.170.196-CN
0
10000
20000
30000
40000
Number of Attacks

場所について— IP

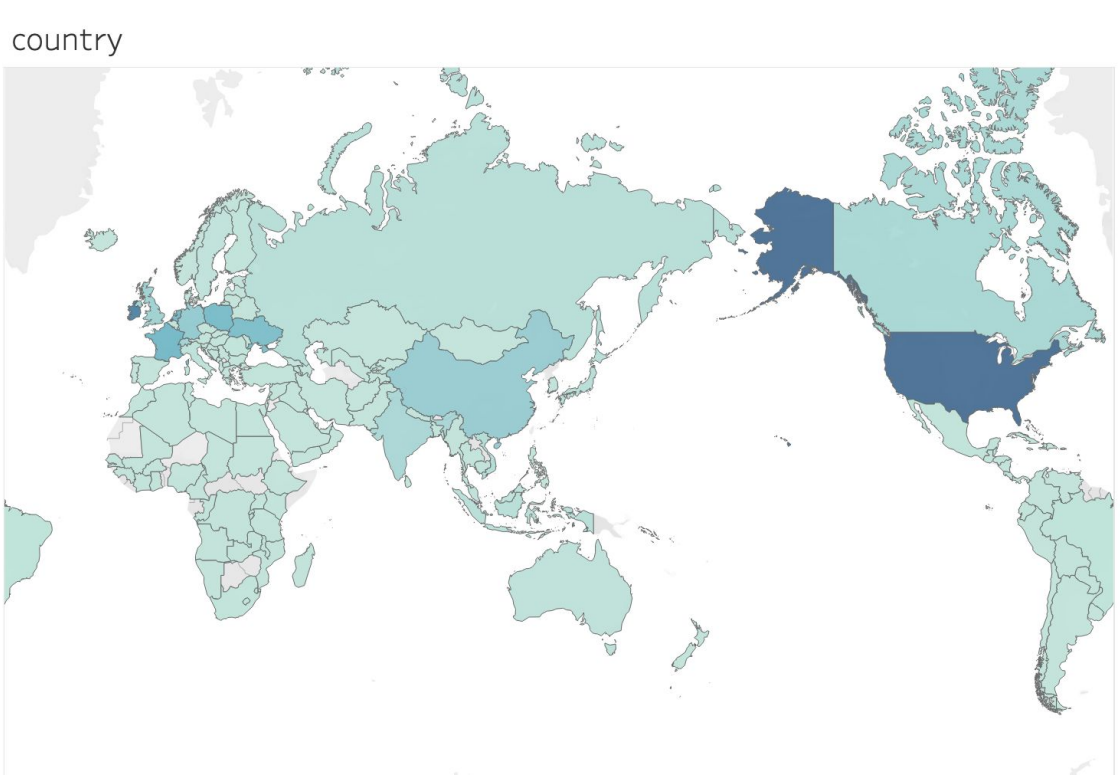
ip_country	country	
185.234.216.28-IE	Ireland	45191
185.234.217.39-IE	Ireland	42428
193.106.30.99-UA	Ukraine	37926
193.169.252.37-PL	Poland	37913
80.82.70.206-NL	Netherlands	10444
185.39.10.73-CH	Switzerland	9280
94.102.49.7-NL	Netherlands	8840
185.128.41.50-CH	Switzerland	7116
122.114.57.92-CN	China	6840
222.170.170.196-CN	China	5952

場所について— country



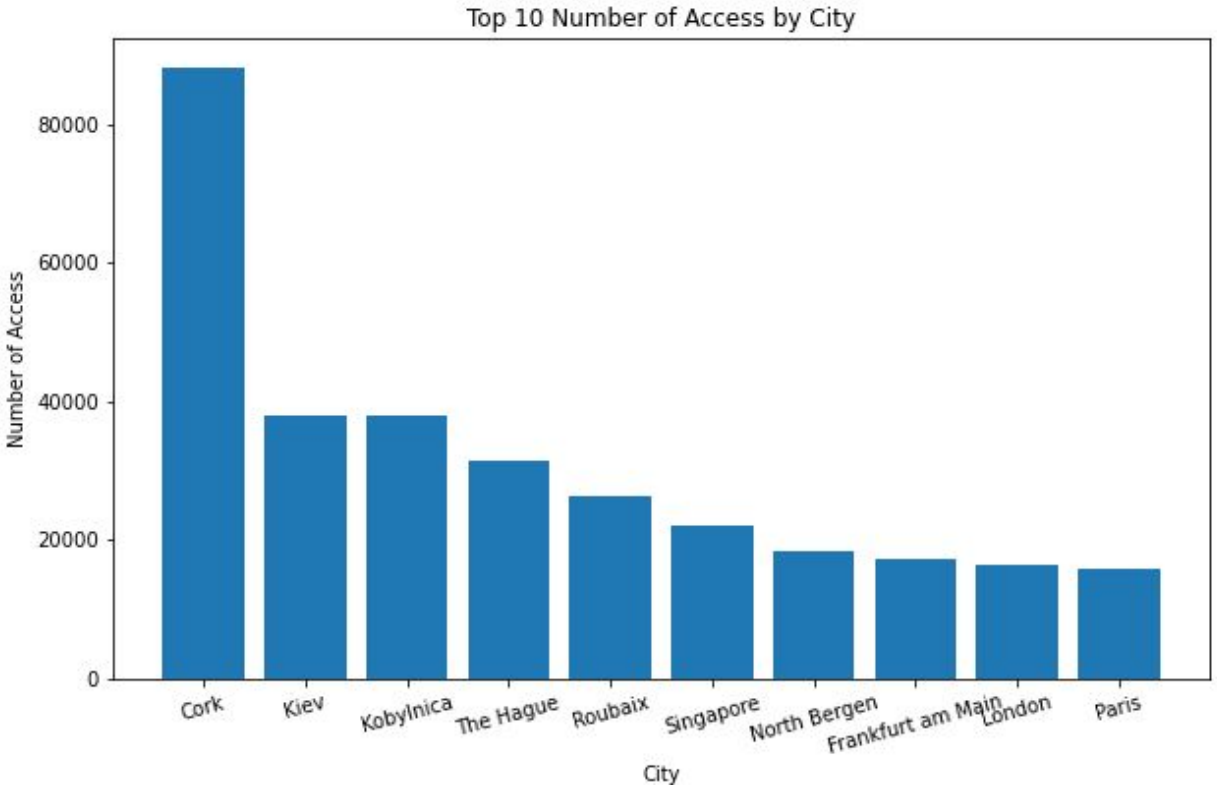
	country	count
0	US	108978
1	Ireland	91565
2	France	44303
3	Netherlands	42770
4	Poland	41847
5	Ukraine	39682
6	Germany	26578
7	China	24729
8	Singapore	22071
9	UK	18940

場所について— country



	country	count
0	US	108978
1	Ireland	91565
2	France	44303
3	Netherlands	42770
4	Poland	41847
5	Ukraine	39682
6	Germany	26578
7	China	24729
8	Singapore	22071
9	UK	18940

場所について— city

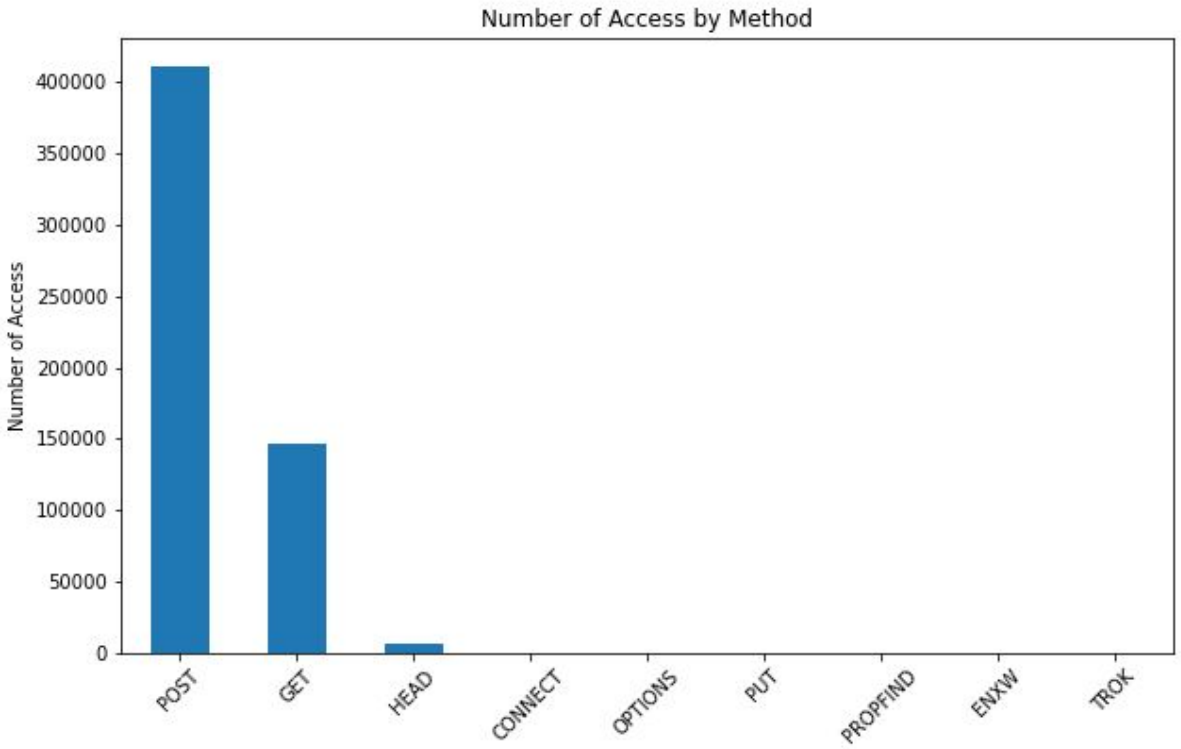


	city	count
0	Cork	88017
1	Kiev	37985
2	Kobylnica	37977
3	The Hague	31504
4	Roubaix	26215
5	Singapore	22071
6	North Bergen	18417
7	Frankfurt am Main	17266
8	London	16537
9	Paris	15948

場所について— city

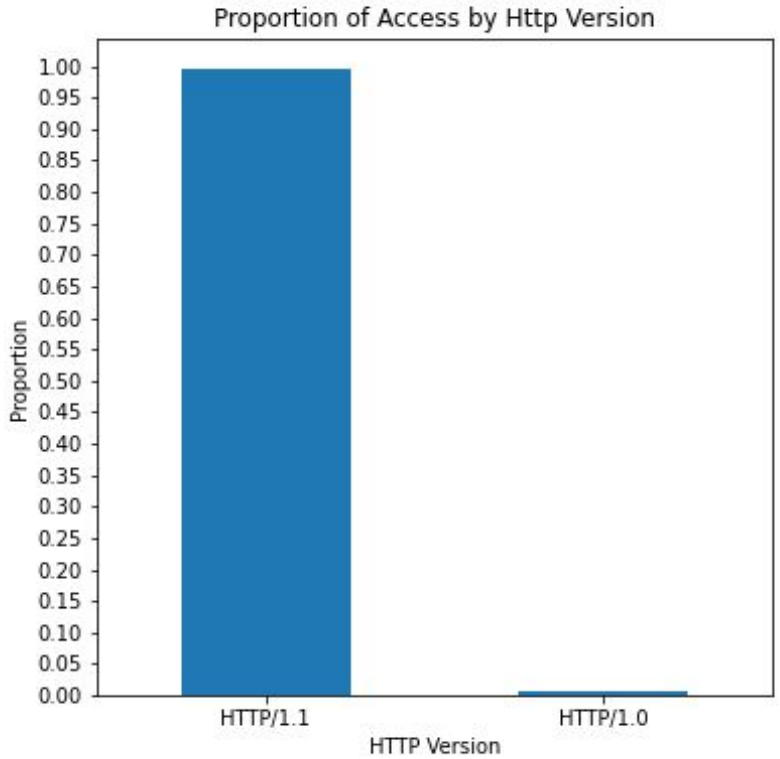
	city	count
0	Cork	88017
1	Kiev	37985
2	Kobylnica	37977
3	The Hague	31504
4	Roubaix	26215
5	Singapore	22071
6	North Bergen	18417
7	Frankfurt am Main	17266
8	London	16537
9	Paris	15948

テクニックについてー method



ほとんどのメソッドは postとgetです

テクニックについてー http version



99%のhttp versionはHTTP/1.1です