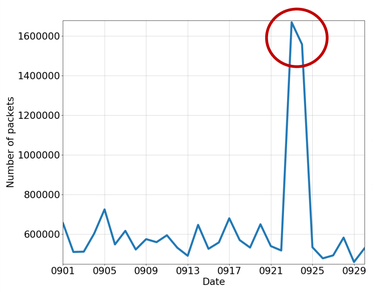
SecHack365

Twitterとダークネットの相関に関する研究

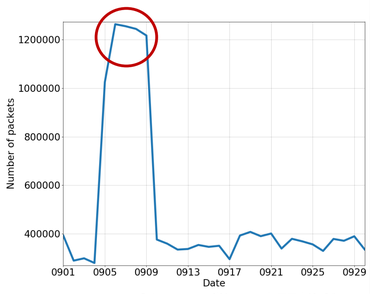
研究駆動コース　持田捷宏

研究背景

- ダークネットはサイバー攻撃の予兆観測のために用いられる
- ダークネットでは原因不明なトラフィックが観測される
- Twitterに多種多様な情報が扱われる
- Twitterとダークネットの相関に関する調査は十分行われていない



パケット数の時間推移
（2018年9月 中国）



パケット数の時間推移
（2018年9月 オランダ）

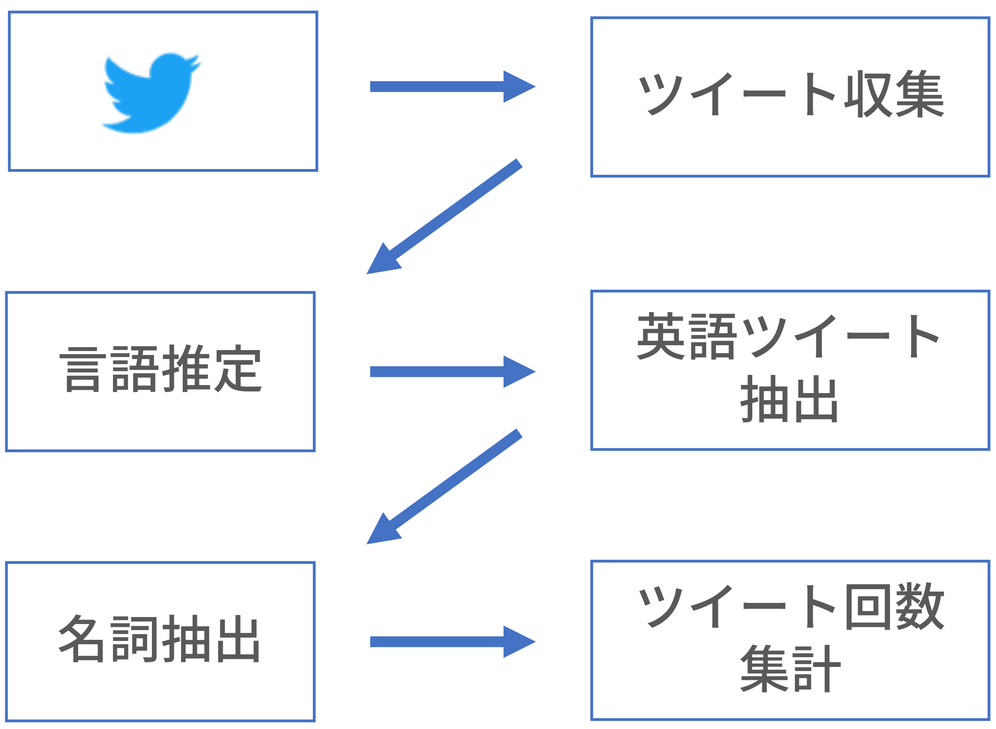
研究目的

- Twitterとダークネットの相関の有無を調査する

Twitterとダークネットの可視化Webインターフェース

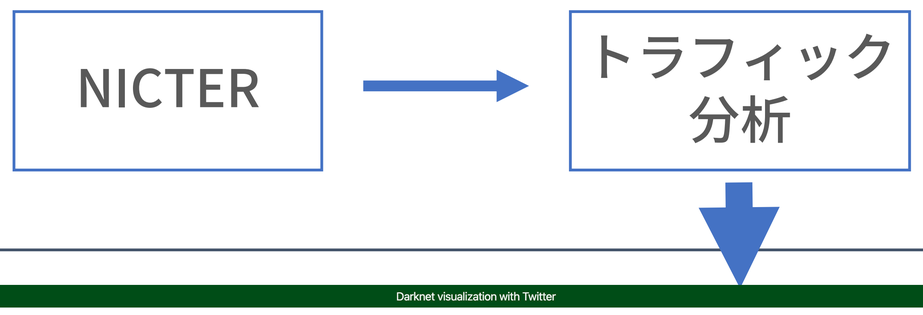
Twitter

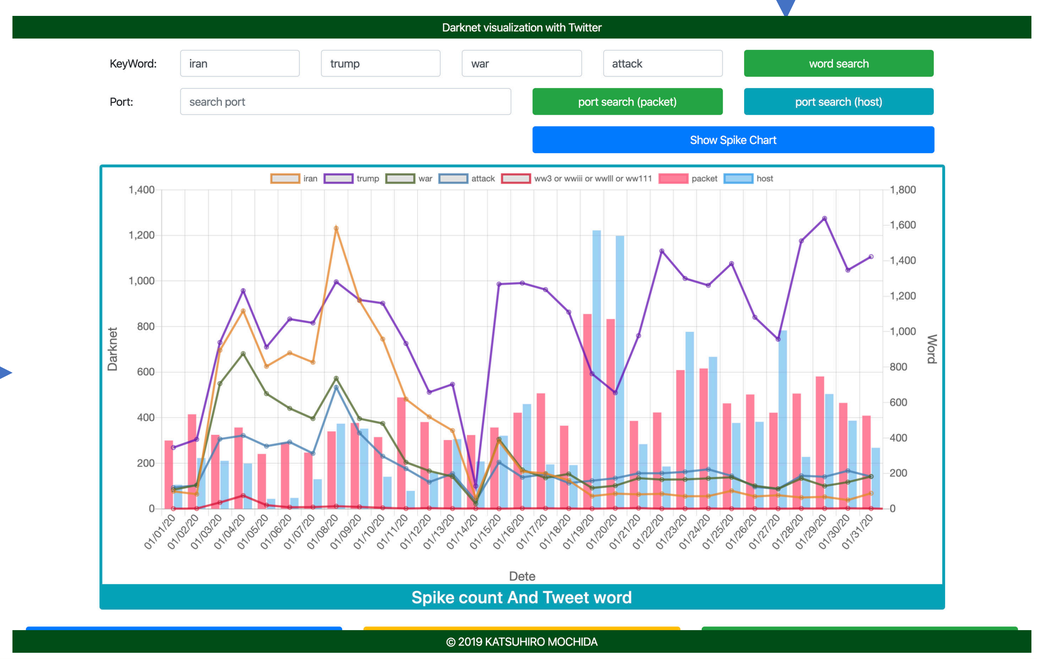
- 100,067アカウントから収集したツイート
- 英語のツイートのみを対象
- 名詞のみを抽出集計



ダークネット

- NICTERのパケットキャプチャデータ
- IPアドレスの第2オクテットまでを同一ホストとして集計

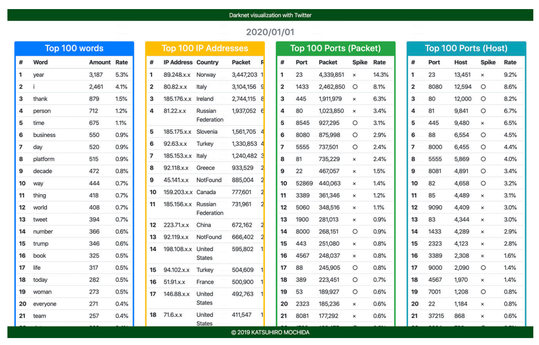




観測期間　2020年1月1日～2020年1月31日

研究結果

- Twitterとダークネットの可視化Webインターフェースを構築した
- 443番ポートへのパケット数と「trump」に相関のようなものが見られた



今後の課題

- 相関が見られても因果関係があるのか不明瞭なため裏付けを取るための追調査する必要がある
  - 相関が見られたトラフィックについてバックスキャッタを調査しDDoS被害にあっているサーバがないか調査し、相関が見られたキーワードに関連するものであるかOSINTツールなどを用いて調査する

国立研究開発法人 情報通信研究機構

Sudip Mittal, Prajit Kumar Das, Varish Mulwad, Anupam Joshi,Tim Finin. Cybertwitter: Using twitter to generate alerts for cybersecurity threats and vulnerabilities. In 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), pages 860–867. IEEE, 2016.