ビットコインネットワーク探索パケットのダークネット観測調査

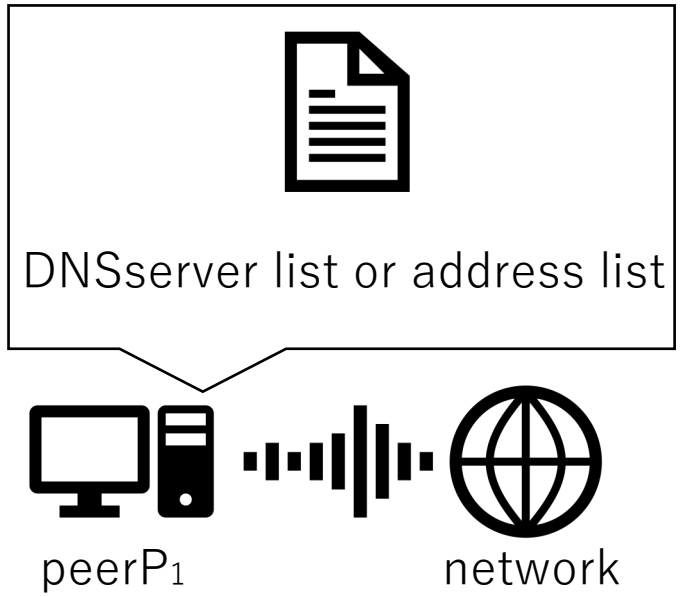
菊池研究室　4年
半澤映拓

研究背景

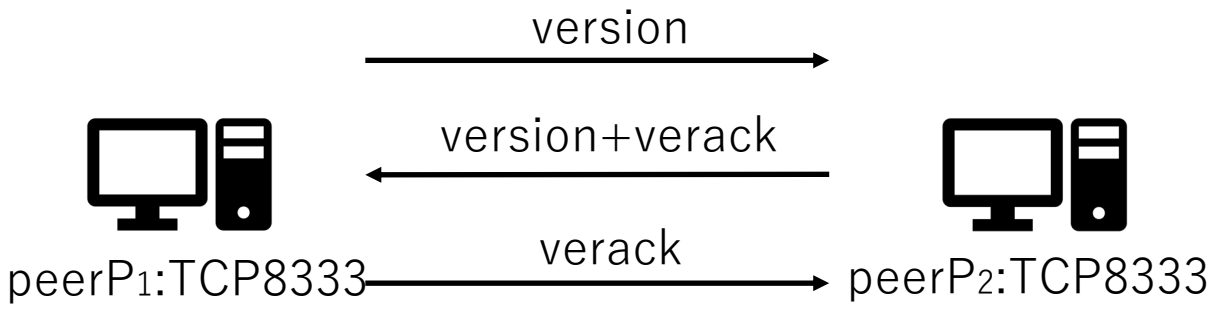
- ビットコインはその匿名性から送信元の解析は困難
- ダークネット上で本来観測されないはずのビットコインのピア探索パケットが観測されている[1]

[1]今村光良，面和成，“ダークネット観測情報を用いたビットコインネットワークの分析”，暗号と情報セキュリティシンポジウム(SCIS)2018,pp.1-8，2018

Bitcoinネットワークの接続の仕組み



Peer Discovery



Connecting to Peers

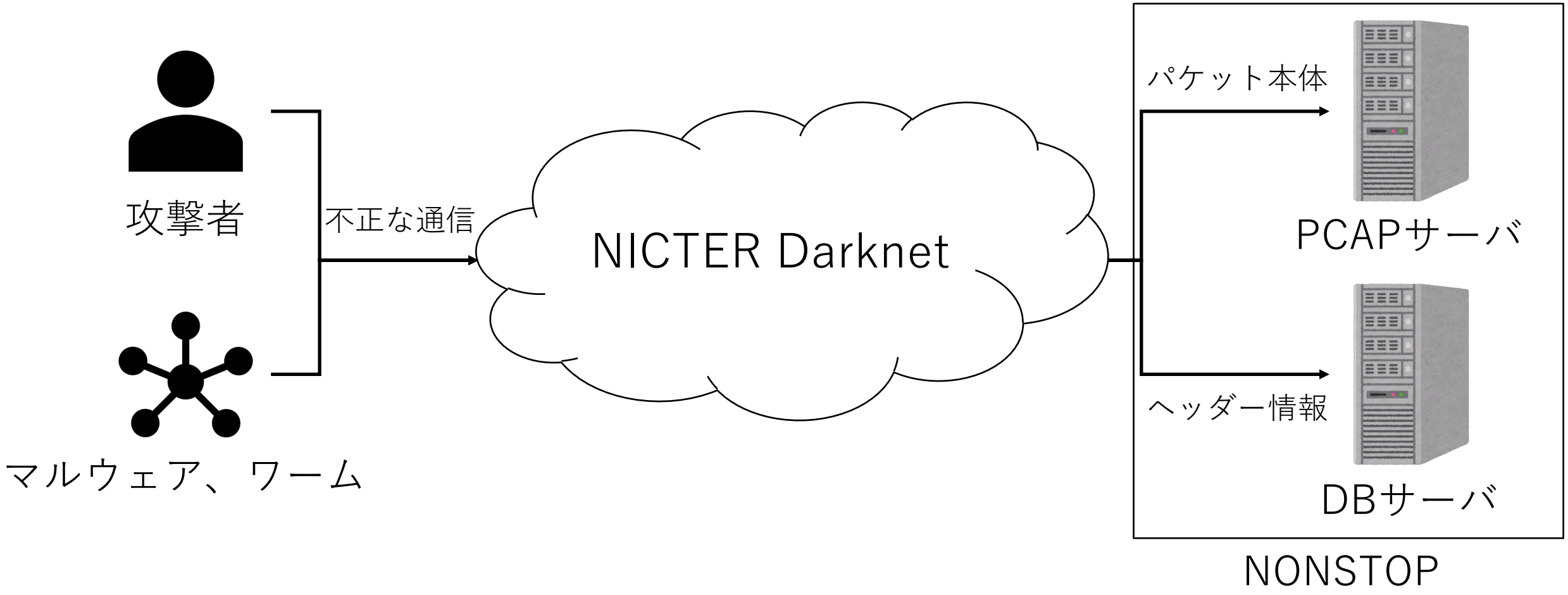
研究目的

- ダークネットに到達するビットコインのピア探索パケットの送信元に関する情報(アドレス、ポート、国)の調査と解析

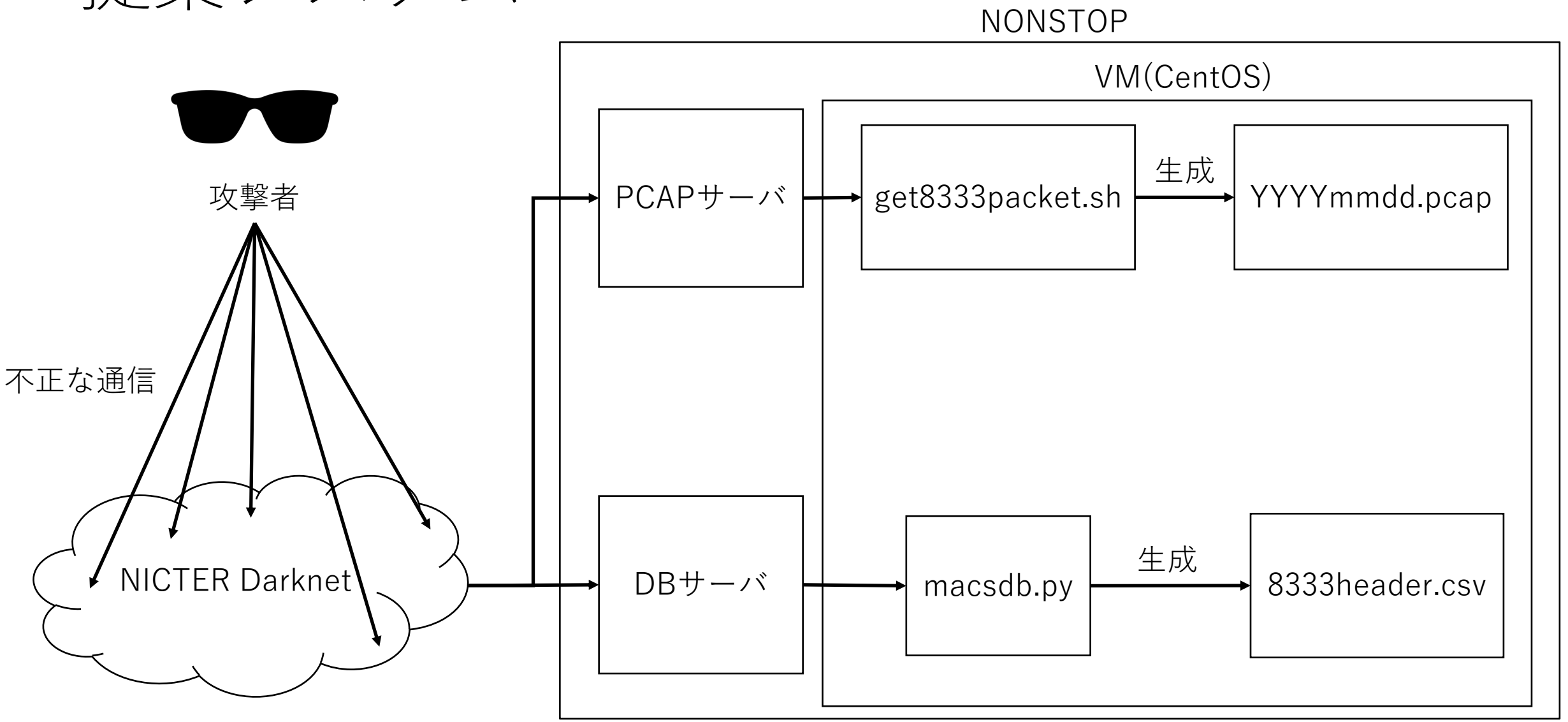
解決手法

- ピア探索パケットの本体、ヘッダー情報の収集を行うシステムの構築

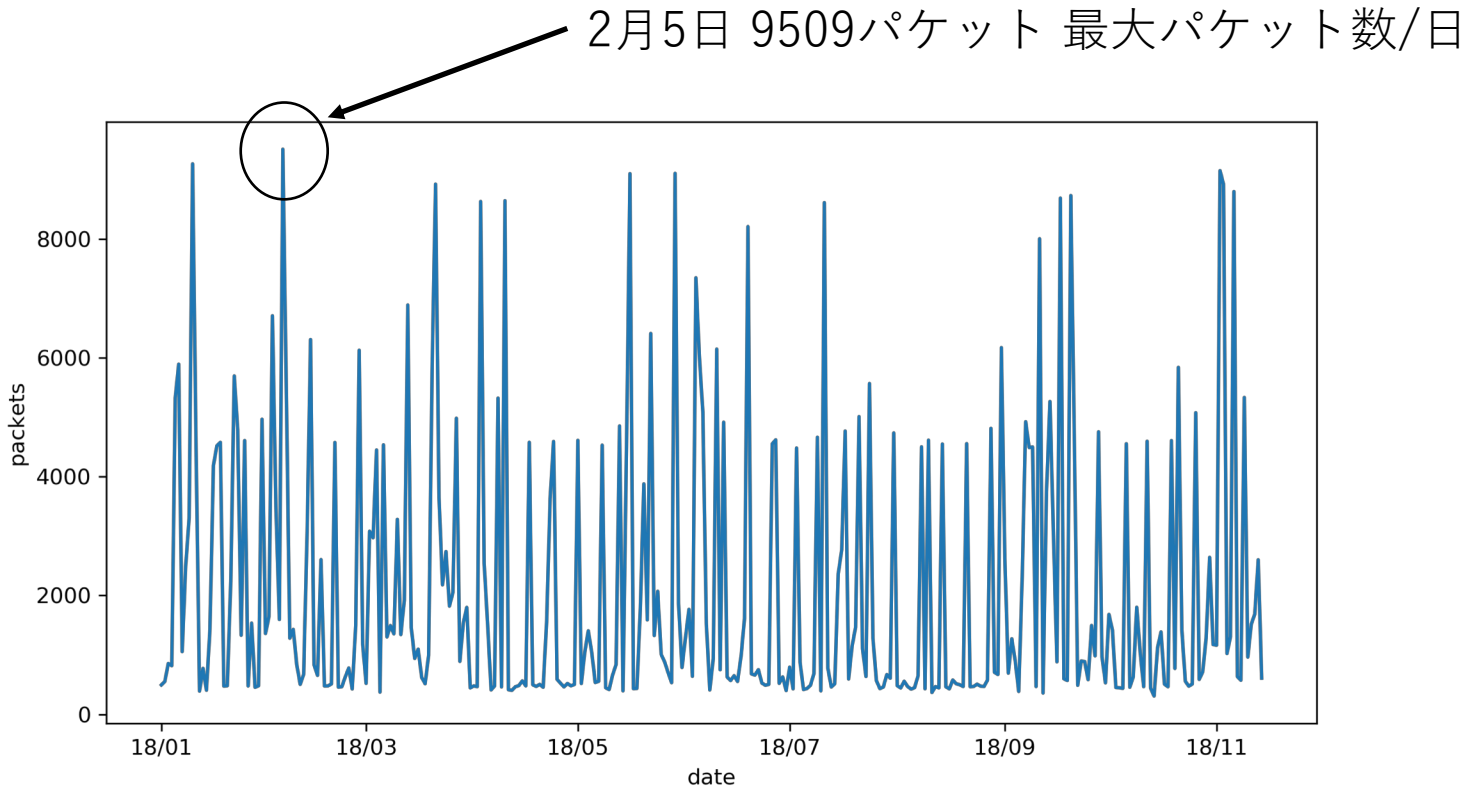
NICTER Darknet、NONSTOPについて



提案システム

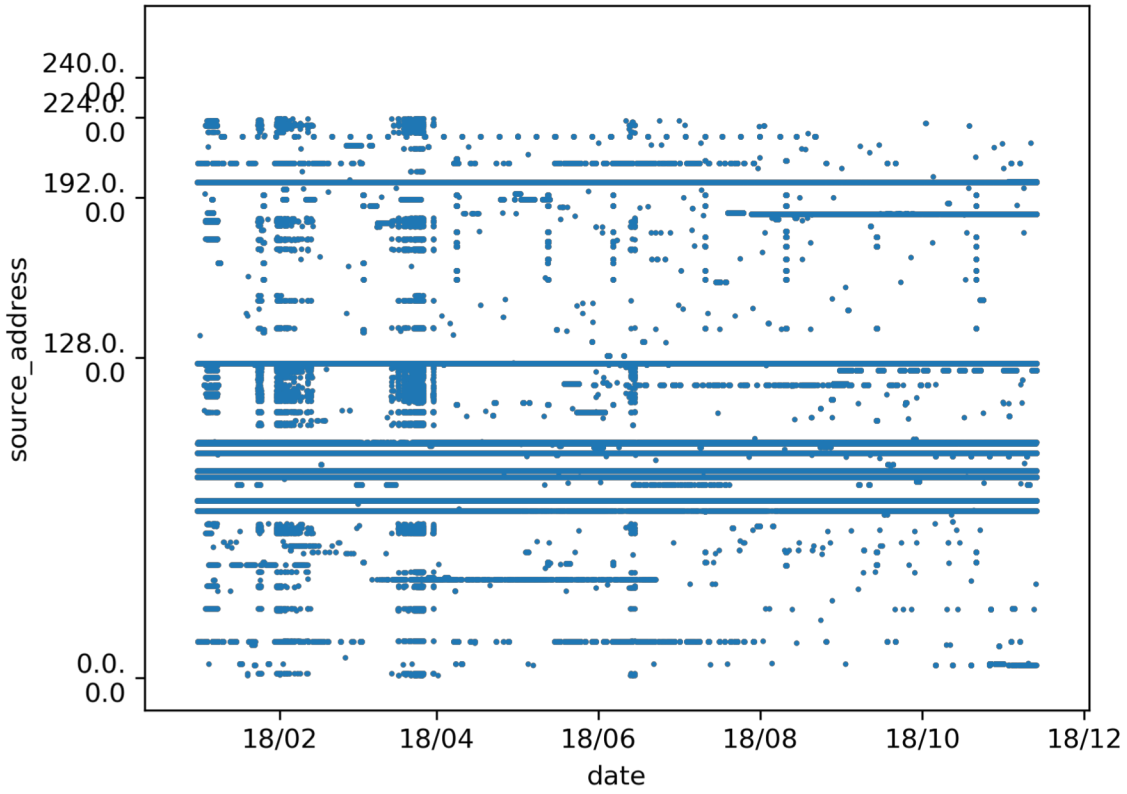

NONSTOP
VM(CentOS)
攻撃者
不正な通信
NICTER Darknet
PCAPサーバ
get8333packet.sh
生成
YYYYmmdd.pcap
DBサーバ
macsdb.py
生成
8333header.csv

観測したデータ

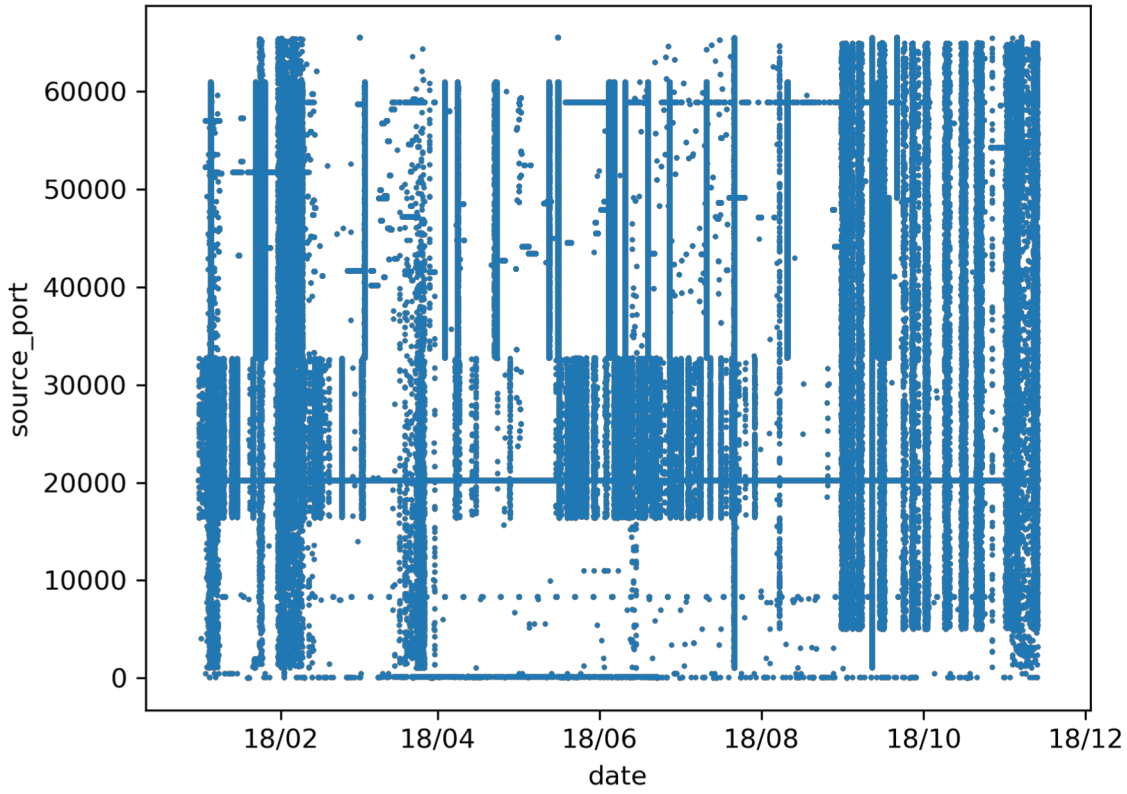


観測期間	収集したデータ	総パケット数
2018年1月1日～11月12日	送信元アドレス、送信元ポート、送信元国コード	674,304

アドレスとポートの散布図

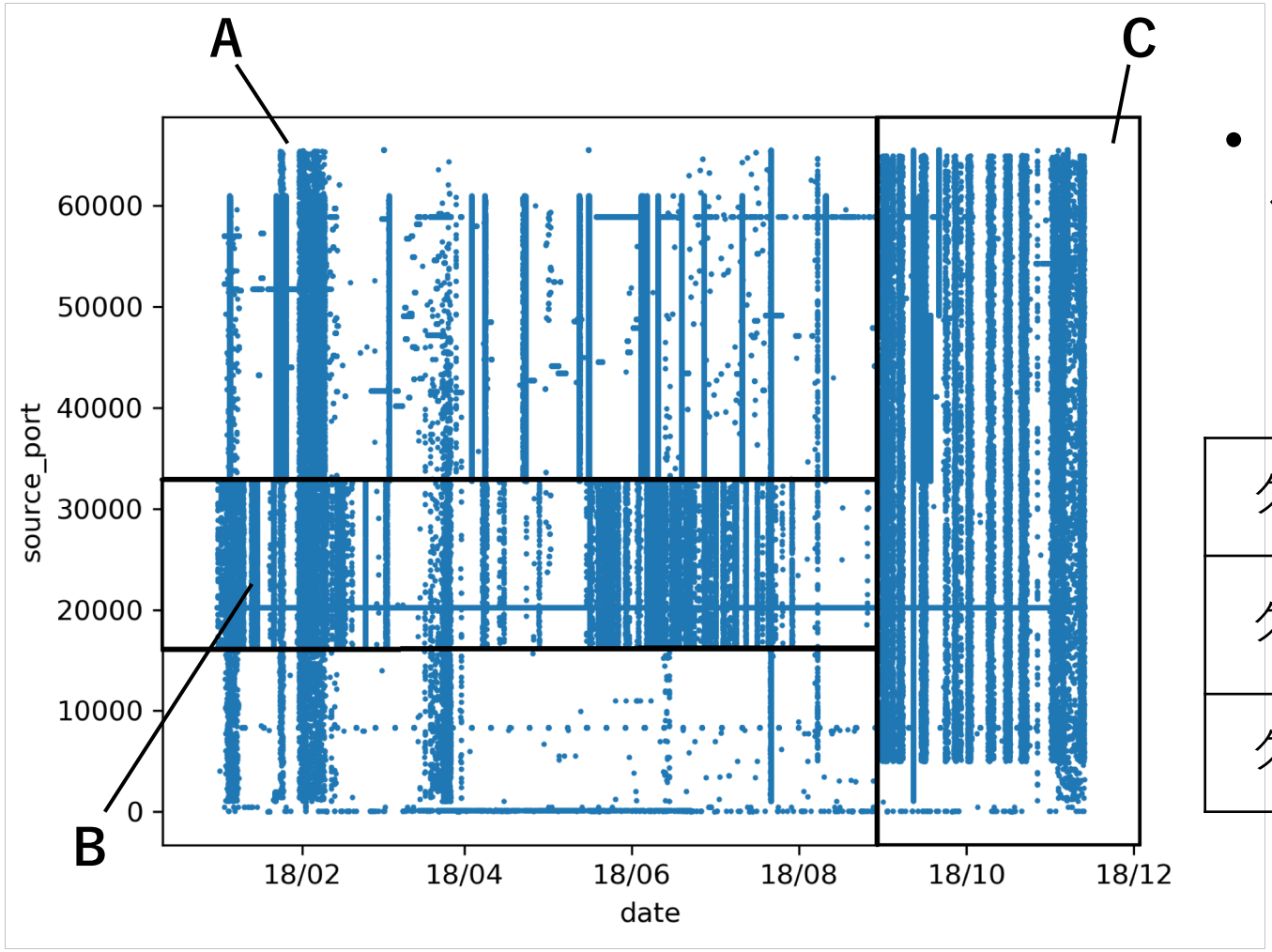


受信日時についての送信元アドレス



受信日時についての送信元ポート

ポート・日時でのグループ分け



- 受信日時と送信元ポートについて送信パターンごとにグループ分けし、グループごとの送信元の国を集計

グループA	8月31日以前のポート33000以上
グループB	8月31日以前のポート16000～33000
グループC	8月31日以降

グループA	送信件数	グループB	送信件数	グループC	送信件数
中国	48735	アメリカ	51957	アメリカ	73351
アメリカ	45105	オランダ	41725	中国	47280
チリ	33778	ベトナム	13249	オランダ	16201
ロシア	29746	中国	12870	イギリス	13105
オランダ	17933	アイスランド	5590	ロシア	12604
計	210722	計	116515	計	174178

- 3グループ全てアメリカと中国が入っているが、グループBに関しては中国の割合が小さい。
- オランダがグループABCで、ロシアがグループACで入っている。

NICTERとGeoIP 2 の比較

- NICTERで割り振られた国コードとGeoIP2 databaseサービスでIPアドレスを参照した結果を比較、異なる結果となったパケットを算出

NICTER	GeoIP2	パケット数
オランダ	セイシェル	57859
チリ	オランダ	23473
ロシア	イギリス	17181
チリ	アメリカ	10304
ロシア	ブルガリア	8508
アメリカ	オランダ	8165

送信元ポート別の分析

送信元ポート番号	送信件数	送信元アドレス ユニーク数
8333	192507	361
20217	137862	33
58914	13781	4294
49139	4107	8
52842	4107	7
43404	4103	7

送信元国	送信件数
アメリカ	57369
オランダ	55843
ベトナム	17089
アイスランド	7540
ルーマニア	19
中国	2

おわりに

- ダークネット上に到達した8333/tcpポート宛のパケットについて、送信元のアドレス、ポート、国に基づく解析を行った。

- 特定の期間、送信元ポート区間において送信元の国に差異が見られた。