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

半澤　映拓 †

明治大学総合数理学部 先端メディアサイエンス学科 菊池研究室 †

1　はじめに

近年，匿名性から違法な売買でも用いられている暗号通貨 Bitcoin に注目が集まっている．Bitcoin はその匿名性から違法な売買でも用いられているが，Bitcoin ネットワークの複雑さのため送信元の解析は困難であるとされている．

そこで，本研究ではビットコインネットワークの観測を行い，その拡大状況等を明らかにすることを目的とする．そのため，未使用ネットワークアドレス空間であるダークネットに到達した，ビットコインのピア探索に用いられる 8333/tcp ポート宛パケットのヘッダー情報に注目し，ビットコイン P2P ネットワークのトラフィックや特徴について調査，分析を試みる．

本研究の目的は次の 2 つである．

(1) NICTER Darknet へ到達した 8333/tcp ポート宛のパケット本体，ヘッダー情報の収集を行うシステムの構築
(2) 収集したヘッダー情報の送信元に関する調査

2　要素技術

2.1　NICTER Darknet，NONSTOP について

NICTER Darknet は国立研究法人 情報通信研究機構が開発しているインシデント分析システム NICTER（Network Incident analysis for Tactical Emergency Response）[2] プロジェクトで観測を行っている/20 の連続したダークネットである．NONSTOP（NICTER Open Network Security Test-Out Platform）は NICTER の保有するサイバーセキュリティ情報を外部から利用するための分析基盤である．

NICTER Darknet に到達したパケットは PCAP サーバに日毎にダンプファイルとして保存される．パケットの IP ヘッダ，TCP ヘッダ，UDP ヘッダ，ICMP ヘッダそれら以外のプロトコルを使用するパケットのヘッダ，ペイロード情報，オプション情報を DB サーバに保存する．

図 1　Bitcoin ネットワーク接続の仕組み

2.2　Bitcoin ネットワーク

図 1 に Bitcoin ネットワークに接続する際の動作である“Peer Discovery”と“Connecting to Peers”について示す．

“Peer Discovery”は Bitcoin ネットワークに接続する際に隣接するピアを探索する動作である．初回は DNS シードと呼ばれるハードコーディングされたドメイン一覧を照会する．60 秒以内に応答がなかった場合はハードコーディングされた IP アドレスを照会する．以降接続する際には，前回までに接続が成功しているピアを照会する．

“Connecting to Peers”は“Peer Discovery”が成功した後に peerP_1 が Bitcoin ネットワークへの接続を維持する動作である．P_1 は P_2 の宛先ポート 8333 に対して TCP 接続を試みる．接続が成功すると通信プロトコルのバージョン番号等を含む version メッセージを送信する．接続先の P_2 は verack メッセージと version メッセージで応答し，それに対して verack メッセージを送ることで接続が確立される．接続が確立された後は接続先の P_2 に P_1 の IP アドレスを含む addr メッセージと他のピアの IP アドレスリストを要求する getaddr メッセージを送信する．また，接続しているピアの内，30 分以上メッセージを送信していないピアに対しては，ping メッセージを送信し起動状態を確認する．ピアの起動状態が 90 分以

†Akihiro Hanzawa, Department of Frontier Media Science, School of Interdisciplinary Mathematical Science, Meiji University, Kikuchi Laboratory.

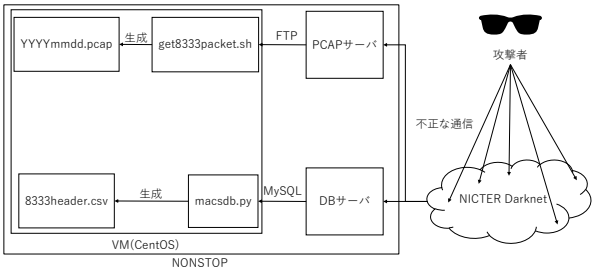

図 2　システム構成図

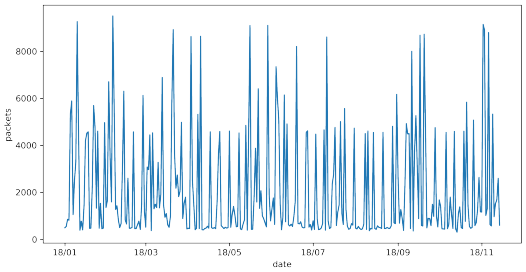

図 3　パケット数の推移 (2018 年)

上確認されなかった場合，そのピアを接続リストから除外する．

2.3　先行研究

今村ら [1] が複雑な Bitcoin ネットワークの分析を行う手法として，ダークネットに到達するパケットを用いた分析を提案している．その中で本来ダークネット上で観測されることが想定されない 8333/tcp 宛のパケットが 2012 年ごろから確認されており，ハッキング被害を受けた Mt.Gox が閉鎖された 2014 年 2 月 24 日前後でダークネット上で 1 日に観測される平均パケット数が大幅に増加していることを明らかにしている．

本研究ではこれらの点に注目，ダークネット上での当該パケット観測を行い，ビットコインネットワークの傾向を探る．

3　提案システム

3.1　システム

本調査では，NONSTOP を利用してシステムを構築した．図 2 に構成図を示す．DB サーバには，IP ヘッダ，TCP・UDP ヘッダの情報を，PCAP サーバには，pcap ファイルや spam メールを移動する．本研究で提案したシステムでは DB サーバから TCP8333 宛パケットの到着日時，送信元アドレス，送信元ポート，国コードを 8333header.csv に出力する．

3.2　観測

本研究では，2018 年 1 月 1 日から 11 月 12 日の 316 日間にかけて 3.1 節で提案したシステムを用いて観測を行い，8333/tcp ポート宛パケットの TCP ヘッダ情報のパケット受信日時，送信元アドレス，送信元ポート，送信元国コードを収集した．

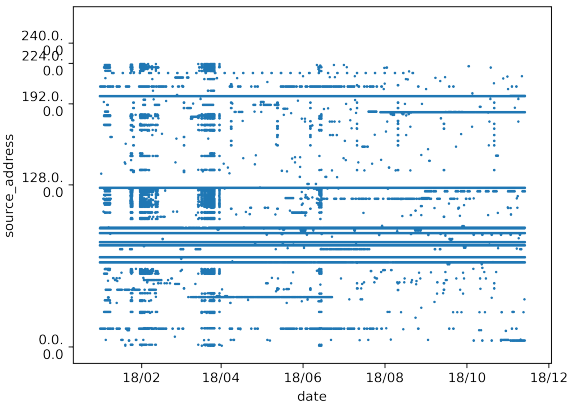

図 4　受信日時についての送信元アドレス

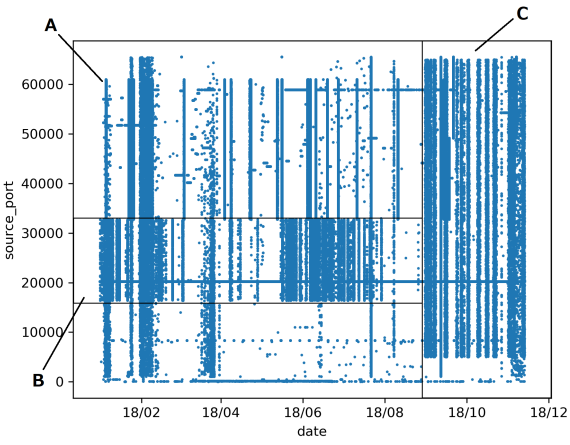

図 5　受信日時についての送信元ポート

図 3 にダークネット上の 8333/tcp ポートに対するパケット数の推移を示す．最もパケット数の多かった日は 2 月 5 日で 9509 パケット，総パケット数は 674,304 であった．

受信時刻と送信元アドレス，送信元ポートについての散布図を図 4 と 5 に示す．送信元アドレスのユニーク数は 11947 アドレスであった．

送信元ポートの種類数は 53,110 だった．8 月 31 日

表 1　グループごとのパケット送信件数上位国

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	
CN[1]	48735	23.1%	US	51957	40.1%	US	73351	42.2%
US[2]	45105	21.4%	NL	41725	32.2%	CN	47280	27.2%
CL[3]	33778	16.0%	VN[4]	13249	10.2%	NL	16201	9.3%
RU[5]	29746	14.1%	CN	12870	9.9%	GB[6]	13105	7.5%
NL[7]	17933	8.5%	IS[8]	5590	4.3%	RU	12604	7.3%
計	210722		計	116515		計	174178	

表 2　送信元国コード別パケット送信数と GeoIP2 を参照した際の送信元国別パケット送信数

送信元国コード	送信件数	GeoIP2	送信件数
US	320460	US	316600
CN	115552	CN	115550
NL	75868	SC[9]	57860
RU	42380	NL	48438
CL	33778	GB	41481
国数	45	国数	45

表 3　NICTER NONSTOP と GeoIP2 で送信元国が異なるパケット数

NICTER NONSTOP	GeoIP2	パケット数
NL	SC	57859
CL	NL	23473
RU	GB	17181
CL	US	10304
RU	BG	8508
US	NL	8165

表 4　送信元ポート別パケット送信件数とアドレスのユニーク数

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

以前のポート番号 16000 から 33000 の間，ポート番号 33000 以上，8 月 31 日以降に特徴的な送信パターンがあることが観測できる．そこでこれらをグループ *A*，*B*，*C* に分け，この正体について分析を行う．

表 1 にグループごとのパケット送信数上位の国を示す．グループ *A* は 210,722 レコードで全体の 31.3 %，グループ *B* は 116,515 レコードで全体の 17 %，グループ *C* は 174,178 レコードで全体の 26 %を占める．3 グループすべての上位に米国（US）と中国（CN）が入っているが，グループ *B* の CN は他の 2 グループでの CN の送信数に比べて少ない．NL が *A*，*B*，*C* で，RU が *A*，*C* で上位に入っている．

3.3　送信元国について

表 2 に送信元国コードから送信パケット数上位の国と観測された国数，並びに送信元 IP アドレスを MaxMind の提供する GeoIP2 database サービスで参照した送信パケット数上位の国と観測された国の数を示す．

これらの結果から US と CN は NICTER NONSTOP と GeoIP2 で共に順位は変わらず，パケット数の差も US は 3860 件，CN は 2 件なので大きな差がないことがわかる．一方，NL は 27430 件減少し，RU と CL は上位 5 カ国から外れ，代わりに SC と GB が上位 5 カ国に入るなど，NONSTOP と GeoIP2 で送信元国が異なるレコードも存在することがわかる．NONSTOP と GeoIP2 で送信元国が異なるレコードについての集計を表 3 に示す．

表 2 と表 3 より GeoIP2 で送信元国が SC と判定されたパケット 57860 件のうち，57859 件は NICTER NONSTOP で NL から送信されたパケットであると判定されている．

3.4　送信元ポートについて

表 4 にパケット送信数上位の送信元ポートとそれらの送信元ポートからパケットを送信した IP アドレス数を示す．

[1]中国
[2]アメリカ
[3]チリ
[4]ベトナム
[5]ロシア
[6]イギリス
[7]オランダ
[8]アイスランド
[9]セイシェル

表 5　送信元ポート 20217 からのパケット送信件数が多いホストとその国コード

送信元アドレス	送信元国コード	送信件数
80.82.77.139	NL	16509
80.82.77.33	NL	16263
125.212.217.215	VN	8562
125.212.217.214	VN	8527
71.6.146.185	US	7371
71.6.158.166	US	6766
89.248.167.131	NL	6536
93.174.95.106	NL	6331
71.6.146.186	US	5716
71.6.167.142	US	5484

表 6　送信元ポート 20217 の送信元国とパケット送信件数

送信元国コード	送信件数
US	57369
NL	55843
VN	17089
IS	7540
RO[10]	19
CN	2

送信元ポート番号 20217 からの通信は 137,862 件あるにも関わらず，33 のホストからしか送信されていない．これらのレコードについて送信件数の多いホスト上位 8 つを表 5 に，送信元国を上位から表 6 に示す．

3.5　考察

3.2 節では受信日時と送信元ポートの散布図から特徴的な部分についてグループ分けを行い，グループごとに上位を占める国の構成に差異があることを示した．したがって，国によって 8333/tcp にパケットを送信する際に使用するポートの傾向が異なると考えられる．

3.3 節では NICTER NONSTOP で割り振られた送信元国コードと GeoIP2 database サービスを参照し IP アドレスから割り出した送信元国の差について分析を行った．GeoIP2 で SC の IP アドレスであると判断されたレコードのほぼ全てが NICTER NONSTOP では NL からの送信者であると判定されていることがわかった．NICTER は送信元国の判定を行う際，送信元アドレスではない情報から決定を行っていると考えられる．

3.4 節では送信元ポート番号 20217 のパケットに注目して送信元の国，アドレスについて分析を行った．表 6 より US と NL がその通信の大半を占めることや上位 2 アドレスが 3 位のアドレスの 2 倍近い送信件数であることがわかった．一方で全体では送信数が 2 番目に多かった中国が当該ポートからの通信は 2 件のみの結果となっており，国によって送信者の特徴が異なる特性を示した．表 5 の送信件数上位のホストの中で NL から送信されたものに対して IP アドレスから送信元の国を調査したところ、全て SC からの送信されたものとなっており 3.3 節の分析と合わせて，NL からの通信と SC の関係についてさらに調査が必要であると考える．

[10] ルーマニア

4　おわりに

本研究では，ダークネット上に到達した 8333/tcp ポート宛のパケットの送信元について調査を行い，送信元国，送信元ポート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国に差異が見られた．今後は到達パケットのペイロードについて調査し，ダークネットに当該ポート宛パケットが到達する要因について分析を行うことを課題とする．

参考文献

[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

[2] D. Inoue, et al., S nicter: An incident analysis system toward binding network monitoring with malware analysis. In Information Security Threats Data Collection and Sharing, 2008. WISTDCS'08. WOMBAT Workshop on, pp. 58-66. IEEE, 2008.