Computer Security Symposium 2019
21 - 24 October 2019

ダークネット観測によるスキャンパケットの傾向と分析

有本 純 [1,†1]　曽根 直人 [2]　森井 昌克 [1]

概要：未使用の IP アドレス空間であるダークネットには，マルウェアの感染活動やスキャン活動などの不正な活動に起因しているパケットが観測される．ダークネットのパケットを観測することにより，インターネット上で発生している不正な活動が把握可能になる．本研究の目的はダークネットを観測することにより，スキャンパケットの傾向と分析を行うこととした．初めに，大学機関が所有する IP アドレスによる不正トラフィックの解析を行った．解析結果の中から特徴的な挙動を示した IP アドレスを抜粋し，その挙動の解析を行った．次に，スキャンパケットの IP アドレスが詐称されているかどうかを調べた．また，ドメインと IP アドレスを対応付けて管理するシステムである DNS の逆引きを使用し，どれくらいのパケットが詐称されているのかを調べた．最後に，健全なネットワークを構築するために，IP アドレスの詐称を防ぐ取り組みである BCP38 の普及や，使用している IP アドレスの情報を提供して管理することを提案した．これらを実行することにより，ダークネット観測の有効性を発揮し，悪性のトラフィックを早急に検知することが可能になる．

キーワード：ダークネット，スキャン，パケット

Trends and Analysis of Scan Packets by Darknet Observation

Jun Arimoto[1,†1]　Naoto Sone[2]　Masakatu Morii[1]

Abstract: The darknet observed packets originating from malicious activities such as malware infection and scanning activities. By observing darknet packets, it is possible to grasp illegal activities occurring on the Internet. The purpose of this research is trends and analysis of scan packets by darknet observation. First, we analyzed illegal traffic using IP addresses owned by university institutions. From the analysis results, IP addresses that showed characteristic behavior were analyzed. Next, we investigated whether the IP address of the scan packet was spoofed. Using reverse DNS lookup, we examined how many packets were spoofed. Finally, in order to build a healthy network, we proposed the spread of BCP38 and the exchange of information about the IP addresses used. By executing these, the effectiveness of darknet observation is demonstrated. It becomes possible to detect malignant traffic immediately.

Keywords: Darknet, Scan, Packets

1. はじめに

パーソナルコンピュータやスマートフォン，ネットワークカメラ，IoT 機器等手軽にインターネットへ接続できるデバイスが急速に普及している．インターネットの利用により多くの有益な情報が得られるが，セキュリティの不十分な端末に対して攻撃を行うマルウェアなどの脅威に晒される可能性がある．これらの脅威に対して対策を講じるためには，ネットワーク上で不正トラフィックを検知，解析し攻撃者の挙動を把握する必要がある．広域なネットワーク上で不正トラフィックを検知する方法として，ダークネットと呼ばれる未使用の IP アドレス空間を用いたパケット観測がある．実際に利用されているライブネットでは正規の通信と不正な通信が混在するが，未使用なネットワークであるダークネットではほとんどが不正な通信である．それを解析することにより不正トラフィックを効率よく解析することが可能になる．

本研究では，/18 のダークネットを観測し，大学機関が所有する IP アドレスを発信源とする不正トラフィックの解析を行った．解析対象の大学数は 294 大学であり，その解析結果の中から特徴的な挙動を示した IP アドレスを抜粋し，その挙動の解析を行った．

次に，スキャンパケットの IP アドレスが詐称されている可能性について考察した．また，DNS の逆引きを使用することにより，どの程度パケットが詐称されているのか推測を行なった．最後に，健全なネットワークを構築するために，BCP38 の普及や使用している IP アドレスの情報を提供して管理することを提案する．これらを実行することにより，ダークネット観測の有効性を発揮し，悪性のトラフィックを早急に検知することが可能になる．

2. ダークネットを利用した大学機関の不正アクセス解析

2.1 ダークネット観測に関する関連研究

ダークネット観測の関連研究として，NICT が公開して

1 神戸大学
Kobe University
†1 arimoto@stu.kobe-u.ac.jp

2 鳴門教育大学
Naruto University of Education

いる観測レポート[1]がある．NICT が構築したダークネット観測網を利用することにより，サイバー攻撃関連通信の観測・分析結果を公開している．ダークネット観測網の年間総観測パケット数は年々増加しており，一つの IP アドレス当たりの年間総観測パケット数も増加している．2018 年の総観測パケット数は 2017 年と比較して約 600 億増加した．その理由は，海外組織からの調査目的と見られるスキャンが増加したからである．総パケットに対するスキャンパケットが占める割合が，2017 年の 6.8%から 2018 年は 35%へと大幅に増加した．

また，2018 年は全体の約半数が IoT 機器で動作するサービスや脆弱性を狙った攻撃を行っている．IoT 機器の脆弱性が公開されると，その脆弱性を悪用するマルウェアの攻撃が観測され始める．IoT 機器の脆弱性対策は，感染の未然防止や被害の拡大防止のために重要な課題となっている．

2.2 国内大学機関からのパケットに着目したダークネット観測

ダークネットは未使用であり，ここに到達するパケットの多くは，マルウェアの感染活動などインターネットで発生している何らかの不正な活動に起因している．それらのパケットを観測することにより,インターネットの不正な活動の傾向把握が可能になる．

大学はある程度の大きさを持つ IP アドレス空間を所有しており，組織自身が管理運用を行なっている．適切に管理されていれば，ダークネットにパケットを送信することは少ないと考えられている．そこで，ダークネットに飛来するパケットを解析し，国内大学からダークネットへの攻撃が存在しているかどうかを調査した．

解析期間は 2016 年 1 月から 2018 年 12 月までとした．2016 年 12 月~2017 年 3 月と 2018 年 1 月~3 月まではデータが欠損しているため，対象外とした．ダークネットに飛来するパケットの送信元 IP アドレスに，国内の大学機関が所有する IP アドレスが含まれるかを調べた．解析対象となる IP アドレスを所有している大学数は 294 大学である．2016 年から 2018 年にかけて，ダークネットでパケットを観測した大学は 59 大学であった．次に，パケットが観測された大学数の変化について説明する．年々増加傾向にあり，2016 年に 25 大学，2017 年に 35 大学，2018 年に 39 大学が観測された．また，3 年連続でパケットが観測された大学は 9 大学であり，長期間継続してダークネットでパケットを観測した大学は少ないことが判明した．年次ごとの観測結果を表 1 に示す．次に 3 年間の内，1 年間のみパケットが観測された大学数の変化について説明する．2016 年に 10 大学，2017 年に 19 大学，2018 年に 17 大学が観測された．

表 1　3 年連続で観測された大学のパケット数の変化

大学名	2016年	2017年	2018年
大阪大学	15	25	218
慶應義塾大学	71	215	19
早稲田大学	77	11	12
東京大学	4213	4195	810
広島市立大学	263	401	30
久留米工業大学	1	1	58
愛媛大学	3	1	90
産業医科大学	26	10	7
鳴門教育大学	19	5256	32

表 2　2016 年から 2018 年の解析結果

大学名	年/月	パケット数	宛先ポート番号
名古屋工業大学	2016/4	1353	23
東京大学	2016/7	4205	2375
東京大学	2017/11～12	4096	23, 2323
京都大学	2017/12	16360	3389
東京大学	2018/4	810	8222
東京電機大学	2018/11	839	22

2.3 送信先 IP アドレスのスキャンパターン

表 2 にパケットの観測数の多かった大学の結果を示す．ダークネットにも日本の大学から多くのパケットが飛来していることが確認できた．観測数の多かった大学について不正アクセスの可能性があるかを調べるため，観測時間と宛先 IP アドレスについてのグラフによる可視化を行うと，スキャン行為を行っていることが判明した．スキャンパターンの定義は，ある一ヶ月単位における 1 つの IP アドレスから，宛先 IP アドレスを 200 以上スキャンしたものをスキャンパケットと定義した．送信先 IP アドレスのスキャン方法で分類すると，3 種類のスキャンパターンがあることが判明した．第一に，送信先 IP アドレスが逐次的に増加したスキャンパターンである（名古屋工業大学）．第二に，送信先 IP をランダムにスキャンしたパターンである（2017 年の東京大学，2018 年の東京大学，東京電機大学）．第三には複数の範囲を同時にスキャンするパターンである（2016 年の東京大学，京都大学）．

2.3.1 スキャンパターン(1)

2016 年 4 月 14 日の 18 時 15 分から 40 分の間に，名古屋工業大学が所有す IP アドレスから届いたパケットの観測結果を図 1 に示す．送信先 IP アドレスの第 1 オクテットと第 2 オクテットは伏せてある．図 1 より，単一の送信元 IP アドレスから送信先 IP アドレスを逐次的に変更しながら IP 空間を包括的にスキャンしていることがわかる．また，このスキャン行為は周期的に複数回実行されている．スキャンレンジは/24 の範囲でスキャンしている．宛先ポート番号は全て 23 番であり，NICTER 観測レポート[2]より 2016

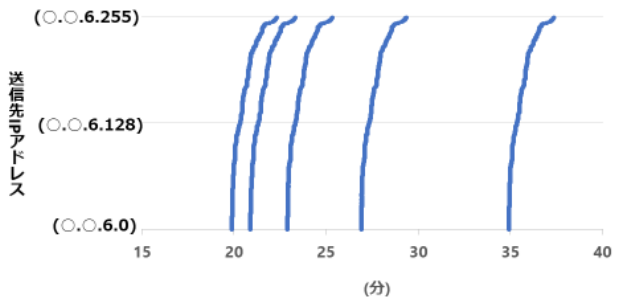

図 1　宛先 IP アドレスと観測時間の可視化　名古屋工業大学

年で最も攻撃されたポート番号は 23 番である．さらに，送信元 IP アドレスは 2018 年 6 月 8 日時点でブラックリスト[3]にも登録されていた．

2.3.2　スキャンパターン(2)

2018 年 11 月 1 日から 4 日の間に，東京電機大学が所有する IP アドレスから届いたパケットの観測結果を図 2 に示す. 図 2 は単一の送信元 IP アドレスから届いたパケットを示す．送信先 IP アドレスが重複しており，送信先 IP アドレスをランダムにスキャンする行為が行われた．本研究で使用しているダークネットのレンジは，第 3 オクテットが 0 から 63 までであり，ダークネットだけでは観測できない範囲があるため. 他の IP アドレスを検索している可能性がある．宛先ポート番号は全て 22 番であり，NICTER 観測レポート[1]より 2018 年で 4 番目に攻撃されたポート番号は 22 番である．さらに，送信元 IP アドレスは 2019 年 4 月 1 日時点でブラックリスト[4]にも登録されていた．

2.3.3　スキャンパターン(3)

2016 年 7 月 11 日の 3 時から 4 時半の間に，東京大学が所有する IP アドレスから届いたパケットの観測結果を図 3 に示す. 図 3 は単一の送信元 IP アドレスから届いたパケットを示しており, 隣接する一定の範囲内の送信先 IP アドレスを断続的にスキャンする行為が繰り返し実行されている．

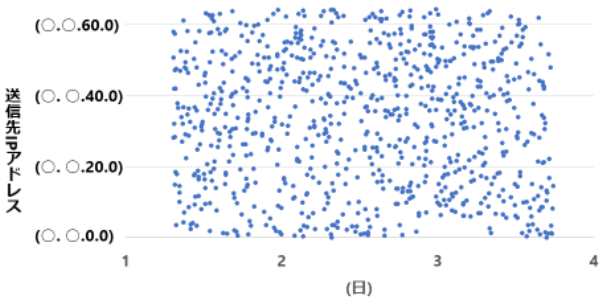

図 2　宛先 IP アドレスと観測時間の可視化　東京電機大学

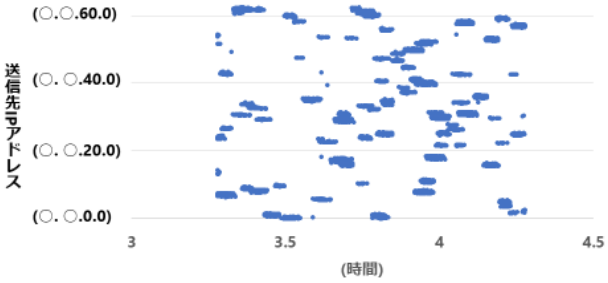

図 3　宛先 IP アドレスと観測時間の可視化　東京大学

また，同時に複数の範囲をスキャンしている．この一連の断続的なスキャン行為は, 送信元 IP アドレスが重複しないように設定されている．本研究で使用しているダークネットのレンジだけでは観測できない範囲があるため．他の IP アドレスも検索している可能性がある. 送信元 IP アドレスは 2019 年 4 月 1 日時点で，ブラックリストにも[5]にも登録されていた．

2.4　スキャンパケットの考察

2019 年 4 月 1 日現在で，表 3 に記載した 2016 年の東京大学はブラックリストにも[5]にも登録されており, 2017 年の東京大学と 2018 年東京電機大学もブラックリスト[4]に登録されている．2018 年 6 月 8 日時点で 2016 年の名古屋工業大学もブラックリスト[3]にも登録されている．表 3 に示してある 6 大学の内，4 大学がブラックリストに登録されていた．また，図 1 から図 3 で示した 3 種類のスキャンパターンは送信元 IP アドレスが大学以外場合も観測した．つまり，これらは大学内外で同じツールによって実行されたスキャンを観測した可能性があり，なんらかのマルウェアもしくは研究用のスキャンが実施された痕跡と考えられる．

3.　IP アドレス詐称の可能性について

ダークネットは TCP の 3 ウェイ・ハンドシェイクの応答部分である syn＋ack を返信しないため，観測したパケットの送信元 IP アドレスが詐称されているか, または真にその送信元 IP アドレスから送信されているか判断できない. そこで，ダークネットのデータだけでは詐称されているのかどうかを見分けるのが困難であるため，連続して観測するスキャンパケットとそれ以外の単発のパケットについて考察を行なった．

3.1　スキャンパケットの詐称

IP アドレスを詐称してスキャンをしても, 詐称した IP アドレスに返答するので，スキャナには応答がなくスキャンの意味がない．スキャン的な挙動のものは応答結果が知り

たいため，IP アドレスを詐称せずに行っている可能性が高い．

syn+ack の跳ね返りを利用する DDoS では送信元を詐称する可能性がある．DDoS を行う人がランダムに送信元 IP アドレスを偽装していると仮定する．本研究で使用するダークネットに含まれる IP アドレスを詐称した TCP パケットを誰かが送信したと仮定すると，跳ね返りの syn+ack がダークネットに届く．そこで，本研究で使用するダークネットに syn＋ack パケットが届いているかを調べた．対象期間は，2017 年 4 月から 10 月と 2018 年 4 月から 7 月までとした．syn+ack が観測された IP アドレスは 2 つだけであり，ほとんど観測されなかった．以上より，観測しているダークネットの IP アドレスを詐称する TCP パケットはほぼ発信されていないと考えられる．

3.1.1 スキャンパケットの割合

スキャンパケットの割合を調べるために，2019 年 1 月の観測データを使用した．この期間にダークネットに届いたパケットのユニーク送信元 IP アドレスは 660 万 8608 個であった．観測したパケットを送信元 IP アドレス毎に計数し，全パケットと比較した割合を表 3 に示す．ダークネットで観測されるパケットの送信元 IP の約半数は観測パケット数が 3 個以下であり，ダークネットに対して少数のパケットしか送信していない．一方，パケット数が 200 以上観測されたものをスキャンパケットと仮定すると，スキャンパケットを送出している IP は全体の約 2.4%であり，ほとんど観測されなかった．ダークネットで観測される IP アドレスの内，スキャン行為を行っているものは少ないことが判明した．

3.2 IP アドレスを詐称しているパケットの割合

ダークネットで観察されるパケットの大部分を占めるスキャン以外のパケットにおいて，詐称パケットが存在するかを調査した．宛先ポート番号が 25 番(SMTP)かつ国内の送信元 IP アドレスからダークネットにパケットが送信されているかを調べた．国内の殆どの ISP がスパムメールやウイルスメールの送信を抑制するため OP25B を実施しており，個人向けのインターネット接続回線からは直接 ISP 外部への TCP 25 番ポートの通信をブロックしている．そのため，OP25B を実施している ISP を送信元とする SMTP 通信は本来ならば存在しないはずである．

表 3 ダークネットで観測されたパケットの送信元 IP アドレス毎の割合

パケット数	割合(%)
1個以下	26.00%
2個以下	40.30%
3個以下	52.00%
4個以下	59.00%
5個以下	64.30%
10個以下	78.8%
100個以下	96.00%
200個以下	97.63%
1000個以下	99.40%

本研究で使用したダークネットの対象期間は 2017 年の 4 月から 12 月と 2018 年の 4 月から 7 月とした．宛先ポート番号が 25 番かつ国内の IP アドレスは 44 個発見した．その内，DNS の逆引きに成功した IP アドレスは 40 個であった．その内訳は，国内かつ家庭向けの ISP で利用している IP アドレス 24 個，国内にあるがサーバー向けの事業で利用している IP アドレス 16 個であった．家庭向けのアドレスを送信元とする SMTP 接続は ISP でフィルターされているため届かないはずのパケット(24 個)を観測した事実が確認された．

送信元詐称パケットの割合がどれくらいあるのかを考察する．詐称されていない IP の場合，組織や ISP から割当てられたアドレスのため DNS の逆引き情報が登録されている可能性が高い．一方，詐称の場合はランダムに IP アドレスを生成したと仮定すると逆引き情報が未登録の可能性が高い．粗雑ではあるが，DNS の逆引き情報が未登録の送信元を詐称 IP と仮定し，2019 年 1 月の観測データを調査した．ダークネットに届いたユニーク IP アドレスは 660 万 8608 個であった．その内，ランダムに 10 万個の IP アドレスを取り出し，DNS の逆引きが可能かどうかを調べた．逆引きができなかった IP は 63776 個であり，少なくとも 63.7%が詐称していることが判明した．

最後に，スキャン行為をしている IP と，スキャン行為をしていない IP がどれくらい詐称されているかを調べた．送信元 IP アドレスに対する観測パケット数ごとに場合分けを行い，その IP アドレスが DNS で逆引可能かを調べた．DNS で逆引きできないものを詐称されている IP アドレスと仮定すると，送信元 IP アドレスに対する観測されたパケット数が多いものほど，逆引き可能であり詐称の割合が減少した．その結果を表 4 に示す．1000 パケット以上確認された IP アドレスは，全ての送信元 IP アドレスが逆引き可能であった．但し，観測パケット数が 1～199 と 200～999 の場合はランダムに送信元 IP アドレスを 2 万個取り出し

表 4 観測されたパケット数ごとに対する IP アドレスの詐称の割合

パケット数	詐称の割合(%)
1～199	67.91%
200～999	63.92%
1000～4999	61.88%
5000～9999	45.47%
10000以上	44.00%

確認した．表 4 より，スキャン行為をしていない IP よりも，スキャン行為をしている IP の方が詐称の割合が低いことが判明した．これは 3.1 でスキャン行為を行う送信元 IP は詐称の可能性が低いことを裏付ける結果である．

4. 健全なネットワークを構築するには

送信元 IP アドレスの詐称を防ぐ取り組みとして BCP38 が提唱されているが，現状はあまり普及していない[6]．2 章と 3 章の結果より，ダークネットの観測パケットに占める詐称パケットの割合が多いことからも普及していないことが推測される．BCP38 を導入することにより，内部から送信元を詐称したパケットが送出されることは防げるが，未導入のネットワークが存在すれば，そこから詐称したパケットが送出可能なため，BCP38 を導入したとしても，自組織の IP が詐称に利用されることは防げない．しかし BCP38 を導入したネットワークが増えていくことで送信元 IP アドレスを詐称したパケットを減らすことが可能になるため，より積極的な普及活動が必要と考える．インターネットとマルチホーム接続していない組織であれば，簡単なフィルターで実装できるため，まず大学で積極的な導入が望まれる．

古くからインターネットへ接続していた大学や組織では規模の大きなグローバル IP を所有しているが，現状は外部との通信がファイアウォール経由のみというところが多い．正しくネットワークを管理されていれば，所有するグローバル IP のうち，殆どの IP アドレスが送信元としてインターネットに出現しないはずである．メールの SPF レコードはメールの送信サーバーを DNS の txt レコードに明記することにより，偽装サーバーを検出する．IP アドレスにおいても，FW などで組織から発信されるパケットの IP アドレスが限定されている場合，その情報を交換することで，より簡単に詐称が検知できる．健全なネットワークを構築するために BCP38 の普及に加えて送信元 IP アドレスの情報を交換することでダークネット観測においても送信元の詐称を判断可能になる．迷惑メール対策の DMARC のように検知した詐称パケットの情報を詐称されているネットワークの管理者へ報告することも考えられる．

大学における研究の一環として，大規模なスキャンを実施する場合も，DNS の逆引き情報を登録するといった手順を決めることで，研究用のスキャンなのか不正な活動なのかを推測する手掛りになる．

5. まとめ

大学のネットワークが正しく管理されていると仮定し，悪質なトラフィックが存在していないかを調べた．大学の所有する IP アドレスから，本研究で使用したダークネット向けたパケットが観測された．ダークネットへ届いたパケットを解析するとスキャン行為を行っているものがあり，3 種類のスキャンパターンが存在した．これらのスキャンパターンは大学以外のネットワークを発信源とするスキャンでも観測している．また大学ネットワークを発信源とするスキャンの送信元 IP の過半数はブラックリストに登録されており送信元 IP が詐称されたのではなく，何らかの目的でスキャンを実行していた可能性が高いことが判明した．

次に，送信元 IP アドレスが詐称されているかどうかを調べた．スキャンパケットの場合，スキャンによる応答が知りたいため，詐称の可能性は低いと考えた．実際にダークネットに届くパケットの送信元を DNS の逆引きで確認すると，スキャンを実行している送信元 IP アドレスは登録されているが，少数のパケットしか観測できない送信元 IP は登録されていない割合が 63.7%と高いことがわかった．この結果は，少数しか観測しない送信元 IP は詐称されている可能性が高く，多く観測する送信元 IP は詐称されていない可能性が高いことを示唆すると考える．

最後に，健全なネットワークの構築方法について述べる．IP アドレスの詐称を防ぐ取り組みである BCP38 を実施することや，所有するグローバル IP のうち使用している IP アドレスの情報を利用できれば，ダークネット観測の有効性をさらに高めることができ，観測データの SN 比を向上させ，悪意のある通信を早急に検知することが可能になると考える．

5.1 謝辞

本研究を進めるにあたり，ご指導ご鞭撻いただいた神戸大学の壇慶人様にはこの場をお借りして厚くお礼を申し上げます．

参考文献

[1] 国立研究開発法人 情報通信研究機構 サイバーセキュリティ研究所 サイバーセキュリティ研究室，「NICTER 観測レポート 2018」，https://www.nict.go.jp/cyber/report/NICTER_report_2018.pdf

[2] 国立研究開発法人 情報通信研究機構 サイバーセキュリティ研究所 サイバーセキュリティ研究室，「NICTER 観測レポート 2016」 http://www.nict.go.jp/cyber/report/NICTER_report_2016.pdf

[3] “APEWS.ORG”, http://www.apews.org/

[4] “SPFBL.NET” https://dnsbl.spfbl.net

[5] “JustSpam.org”, http://www.justspam.org/

[6] “State of IP Spoofing”, https://spoofer.caida.org/summary.php