L-016

ダークネットに対するネットワークスキャナのサブネット単位の振る舞い調査
Analyzing subnet-level behaviors of network scanners in Darknet

鹿内 嵩天† 角田 裕‡
Takuma Shikanai Hiroshi Tsunoda

1. はじめに

ダークネットは到達可能かつ未使用な IP アドレス空間であり，そこで観測されるトラフィックは不特定多数を標的としたサイバー攻撃の分析において重要な情報源である．近年，セキュリティ関連組織が行う調査目的スキャンが増加傾向にあり[1]，これらが分析上のノイズとなることが指摘されている[2][3]．スキャナ判定指標のひとつに，プレフィックス長が/16 のネットワーク（/16 ネットワーク，以下同様）単位で判定を行う手法がある．しかし，スキャナと判定されたネットワーク全体が一様にスキャナ的な性質を持つのか，あるいは一部のサブネットのみがスキャナとして活動しているのかという点は明らかでない．

本研究では，ダークネットに到達したパケットの送信元に対し，より細かい単位でスキャナ判定指標を適用し，スキャナと判定されたものについて，さらに細かく内部構造や振る舞いを調査する．その結果，スキャナと判定されたサブネットの内部では，ほぼ全てにおいて，それらを構成する/24 サブネットのうち一部のみがスキャナの特性を有していたことを確認した．

2. サブネット単位の振る舞い調査の流れ

まず送信元の/16 ネットワークを構成するサブネット群のうち，パケット送信の有無に基づいて調査対象候補を絞り込む．次に，各候補に対し既存の調査目的スキャナ判定指標を適用し，スキャナと判定されたサブネットを内部の構造や振る舞いの調査対象とする．

2.1 調査対象サブネットの絞り込み

/16 ネットワークを構成する/24 サブネットのうち，1 個以上のパケットを送信している（以下，アクティブ）サブネットを特定する．そして，隣接するアクティブなサブネットの集約を繰り返して分析対象を絞り込む．集約による絞り込みの概要を図 1 に示す．

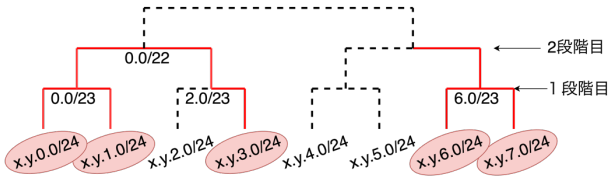

図 1 /24 サブネット集約方法の概要

図 1 の 8 つの/24 サブネットは同一/16 ネットワークに属し，赤枠のサブネットがアクティブなものを示す．1 段階目の集約では，隣接する/24 サブネットのペアのいずれかがアクティブなら/23 サブネットへ集約する．2 段階目以降は，ペアを構成する/24 サブネットの過半数がアクティブな場合のみ集約する．これはアクティブなサブネットが過半数未満の場合，アクティブなサブネット同士の間隔が大きく離れ，異なるものであると考えられるためである．集約が発生しなくなった時点で絞り込みは終了する．

† 東北工業大学大学院工学研究科 Graduate School of Engineering, Tohoku Institute of Technology
‡ 東北工業大学工学部情報通信工学課程 Department of Information and Communication Engineering, Tohoku Institute of Technology

2.2 調査目的スキャナの判定

絞り込みによって調査対象候補となった各サブネットについて，既存の調査目的スキャナ判定指標を適用し，スキャナと判定されたものを振る舞い調査の対象とする．本研究では中川らによって提案された/16 ネットワーク単位でスキャナを判定する判定指標[4]を用いる．この指標のスキャナ判定条件の概要を図 2 示す．

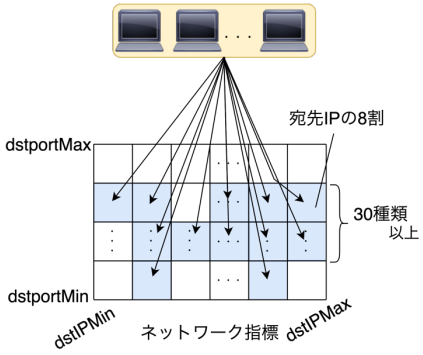

図 2 調査目的スキャナ判定指標の概要

この指標では，あるネットワークが 1 日に送信したパケットが以下の両方の条件を満たす場合にそのネットワークをスキャナと判定する．

条件 1 特定のポートに対してダークネットのアドレスレンジの 8 割以上にパケットを送信
条件 2 **条件 1** を満たすポートが 30 種類以上

指標の適用後，スキャナ判定されたサブネットについて，それを構成する/24 サブネット毎に振る舞いを調査する．

3. サブネット単位の振る舞い調査の結果

3.1 調査対象サブネットの決定

本研究室で運用している数百程度の IP アドレスを有する小規模なダークネットで 2025 年 3 月 1 日に観測された 12,215 種類の送信元/16 ネットワークから，調査対象を絞り込み，それらにスキャナ判定指標を適用した．スキャナと判定されたサブネットについて内部構造や振る舞いを調査した．なお，絞り込みにおいては 2025 年 3 月 1 日～7 日の 7 日間にパケットを 1 個以上送ってきたサブネットをアクティブと判断した．これは，日によってアクセス対象が変化する送信元もあるため，1 日分のデータでは/24 サブネットの活動を正確に把握できない可能性があるためである．

調査対象候補のサブネットが 31,564 個あり，そのうちの 15 個が調査対象となった．詳しい内訳は表 1 に示す．スキャナと判定され，調査対象となったサブネットのうち 13 個が/23 サブネットであり小規模なサブネットだった．また，/17，/18，/19 などの大規模なサブネットの中でスキャナと判定されたものは 1 個のみであった．

表 1 調査対象サブネット数

プレフィックス長	/23	/22	/21	/20	/19	/18	/17
スキャナ	13	1	0	0	1	0	0
非スキャナ	28140	2196	647	379	139	42	6

3.2 調査対象サブネットの内部構造の調査結果

15 個のサブネットの内部構造を調査した．13 個の/23 サブネットのうち 11 個は，内部にアクティブな/24 サブネットを 1 つしか持っていなかった．また，/19 サブネットを構成する/24 サブネットのうち，ダークネットに対するアクセス数が多かったものは 1 つのみで，その他からの送信パケット数は数十から数百個程度にとどまった．

/22 サブネットについては，内部を構成する 4 つの/24 サブネットのうち 1 つが 1 種類のポートに対して，約 500 個のパケットを送信してきていた．残りの 3 つの/24 サブネット A, B, C は数千から数万個規模のパケットを送信してきていた．これらのサブネットのアクセス先ポートを調査した結果，協調している可能性がある．サブネット A, B からダークネットへのアクセスパターンについて可視化図を用いてより詳細に調査した．それぞれのアクセスパターンを図 3, 4 に示す．各図の横軸は当該ネットワークから送信されたパケットの宛先 IP アドレス，縦軸は宛先ポートを示す．点はこの送信元からアクセスされた IP アドレスとポートのペア，色はパケット数に対応する．なお，宛先ポートについてはウェルノウンポートの範囲は個別に，それ以降のポートは 5000 番ずつ集約して可視化している．

図 3, 4 より，/22 サブネットを構成する/24 サブネットがアクセス対象としているポートを一部共有しているが，異なるポートに対してもアクセスしていることが分かる．具体的には，サブネット A は 25001 番から 30000 番ポートにアクセスしているがサブネット B はアクセスしていない．一方，サブネット B は 45001 番から 50000 番ポートにアクセスしているが，サブネット A はアクセスしていない．

また，パケット数が多い 5,001 番から 10,000 番ポート内部も詳細に調査した結果，同様にサブネット A, B はどちらも共通して 7443, 8443 番などのポートにアクセスしているが，8888 番や 8899 番などのポートに対してはいずれか一方のサブネットのみアクセスしていた．また，サブネット C においてもサブネット A, B と一部同じポートにアクセスしているが，それだけではなくサブネット C のみがアクセスするポートもあり，これらのサブネットが協調してスキャン活動を行っていると推測できる．

大規模なサブネットは，各/24 サブネットの送信パケット数が少量でも，全体の送信パケット数が多くなる傾向があり，スキャナと判定されやすいと考えられる．そのため，スキャナと判定された大規模サブネットでは，多くの/24 サブネットがスキャンに関与していると想定していた．

しかし本調査では，1000 個以上のパケットを送信していた/24 サブネットは少数であり，ほぼ全ての/24 サブネットは数十〜数百程度の少量にとどまっていた．想定していたような広範囲にわたるスキャン活動は確認されなかった．

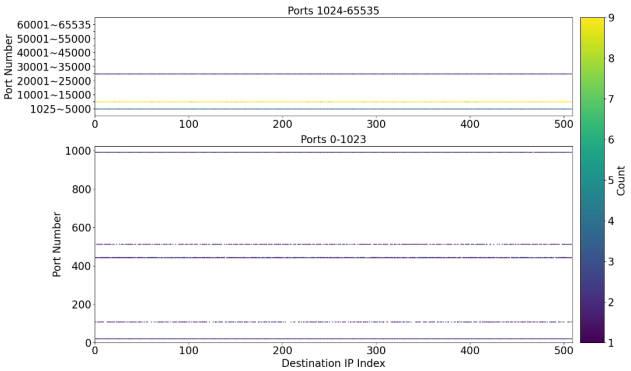

図 3 /22 サブネットを構成する/24 サブネット A

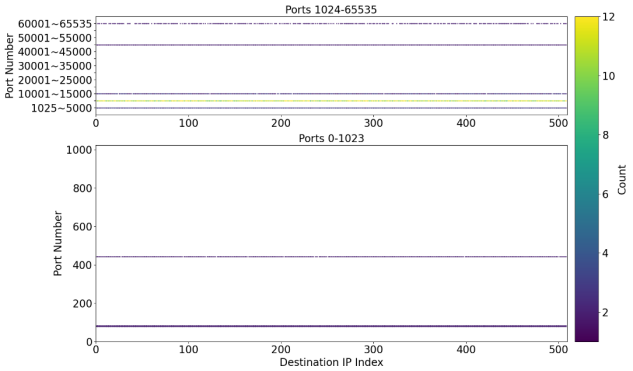

図 4 /22 サブネットを構成する/24 サブネット B

また，スキャナとは判定されなかった/17〜/19 サイズの大規模サブネットについても調査を行った．その結果，アクセスしてきた/24 サブネットの数は多かったものの，各サブネットの送信パケット数はやはり少量であった．

ただし，本調査は 1 日分のデータを対象としており，長期的な活動傾向は評価できていない．今後は，長期間のデータを用いた調査により，これらのサブネットがスキャナとして機能している可能性を検討する必要がある．

4. おわりに

本稿では/16 ネットワークについて．内部のアクティブな/24 サブネットから調査対象候補を絞り込み，それらに調査目的判定指標を適用した．さらにスキャナと判定されたサブネットについて，内部構造や振る舞いについて調査した．スキャナと判定されたサブネットは内部を構成する少数の/24 サブネットが多量のアクセスをしていたことを明らかにした．この結果から，スキャナと判定されたものについて内部のサブネットの構造やその振る舞いを調査することで，より厳密にスキャン活動に寄与している IP アドレスの範囲を特定することができる．

参考文献

[1] 国立研究開発法人情報通信研究機構，“NICTER 観測レポート 2023”, https://csl.nict.go.jp/nicter-report.html (参照 2025-06-12)
[2] 笠間ら，“Can’t Stop The Scan: インターネットスキャンのオプトアウト実態調査”, 信学技報, ICSS2022-76, pp. 169-174, 2023.
[3] C. Han, et al., “Dark-TRACER: Early Detection Framework for Malware Activity Based on Anomalous Spatiotemporal Patterns”, IEEE Access, vol. 10, pp 13038-13058, 2022.
[4] 中川ら, ”ダークネットトラフィックの分析に基づく継続的な広域ネットワークスキャンの調査”, CSS2019, pp. 1422 – 1428,2019.