複数のダークネット観測拠点で同時期に急増する攻撃を検知する手法の提案

村上 洸介† 蒲谷 武正† 千賀 渉† 鈴木 将吾‡ 小出 駿‡ 島村 隼平*
牧田 大佑‡§ 笠間 貴弘§ 衛藤 将史§ 吉岡 克成‡§ 井上 大介§ 中尾 康二†§

† KDDI 株式会社 163-8003 東京都新宿区西新宿 2-3-2 KDDI ビル
{ko-murakami, ta-kamatani, wa-senga, ko-nakao}@kddi.com
‡ 横浜国立大学 240-8501 神奈川県横浜市保土ケ谷区常盤台 79-1
{suzuki-shogo-mb, koide-takashi-mx}@ynu.jp, yoshioka@ynu.ac.jp
* 株式会社クルウィット 181-0013 東京都三鷹市下連雀 3-34-8 三鷹ハイデンス 509 号
shimamura@clwit.co.jp
§ 情報通信研究機構 184-8795 東京都小金井市貫井北町 4-2-1
{d.makita, kasama, eto, dai}@nict.go.jp

あらまし 新たな脆弱性を狙うマルウェアの出現などインターネット上で発生する大規模なインシデントの際には，攻撃のためのスキャン活動の影響によりダークネットで観測される攻撃元ホスト数が急増する事例が数多く報告されている．そのため，それらスキャン活動の増加をいち早く捉え情報共有を行うことで，ネットワーク管理者などによる早期警戒や対策につなげることが重要である．そこで本稿では，複数のダークネット観測拠点で得られた観測データから，各センサにおける特定ポートに対する攻撃元ホスト数の急増を検出し，同様の事象が同一時期に一定数以上のセンサで観測されるか否かを判定することで，大規模なスキャン活動の発生を高い精度で検知する手法を提案する．提案手法にダークネットで観測したトラフィックを適用して行った評価実験から，ルータのバックドアやLinuxに感染するマルウェアのポートに対するスキャンを検知し，これらが同時期に各拠点のセンサで観測されていることを確認した．また，いくつかの事例では各センサにスキャンを行うホスト数が急激に増加する時刻に最大で3日程度の差があることから，早期警戒の可能性などについて考察する．

A Proposal of Method for Detecting Synchronized Increase of Attacks on Multiple Darknet Sensors

Kosuke Murakami† Takemasa Kamatani† Wataru Senga† Shogo Suzuki‡
Takashi Koide‡ Jumpei Shimamura* Daisuke Makita‡§ Takahiro Kasama§
Masashi Eto§ Katsunari Yoshioka‡§ Daisuke Inoue§ Koji Nakao†§

† KDDI Corporation
KDDI Bldg, 2-3-2 Nishishinjuku, Shinjuku-ku, Tokyo 163-8003 Japan
{ko-murakami, ta-kamatani, wa-senga, ko-nakao}@kddi.com
‡ Yokohama National University
79-1 Tokiwadai, Hodogaya-ku, Yokohama-shi, Kanagawa, 240-8501 Japan
{ suzuki-shogo-mb, koide-takashi-mx}@ynu.jp, yoshioka@ynu.ac.jp
* clwit Inc.
3−34−8-509 Shimorenjaku, Mitaka-shi, Tokyo, 181-0013, Japan
§ National Institute of Information and Communications Technology
4-2-1, Nukui-Kitamachi, Koganei-shi, Tokyo 184-8795, Japan
{d.makita, kasama, eto, dai}@nict.go.jp

Abstract In the case of a large scale incidents over the Internet related to malwares targeted to new vulnerabilities, events have been often reported that number of attacking source hosts are getting rapidly increased. That is, by means of observing rapidly increased scan behaviors, early warning and prompt response are getting recognized as important solutions. In this paper, we propose a new detection method of a large scale scan behaviors. The method is starting to detect increasing number of source attacking hosts in the specific port from each sensor located in several countries/regions, and then detect a number of synchronized and similar events behaviors so as to identify a large scale scan behaviors which will be impacting to global regions. According to the results of a field trial that is applying the new method to the traffic data captured in the darknet, it is successfully to detect a synchronized attack (scan) targeted to the port used in the router's backdoor and malware which is infected in Linux system. Furthermore, it was also recognized that timings of scan behaviors observed by the several sensors in different countries vary about three days at maximum, and it is therefore considered that the result of this detection by means of our new method will be utilized for practical early warning.

1 はじめに

到達可能で実際には機器が接続されていない未使用の IP アドレス空間，ダークネットには通常のインターネット利用において通信が到達することは考えにくい．しかし，実際に観測を行うとダークネットには日々大量の通信が届いており，これらの多くはマルウェアからのスキャンや送信元 IP アドレスを詐称した DoS 攻撃の跳ね返り（バックスキャッタ）などインターネット上での何らかの不正活動に関連した通信である．近年ではルータや NAS などに代表される組み込み機器の脆弱性を狙ったスキャンや，DRDoS に使用されるリフレクタの探索を行うスキャンなどもダークネット観測により報告されている[7,14,17,19]．

ダークネット観測を行っている組織・プロジェクトは国内外に多数存在[1,4,8,18,21,22]するが，その中の一つとして総務省の研究開発委託「国際連携によるサイバー攻撃予知技術の研究開発（以下，PRACTICE）」がある．PRACTICE では，国際連携の一環として連携国に対してダークネットセンサを設置し，ダークネットトラフィックの観測・分析，サイバー攻撃情報の共有等を行っているが，共有したダークネットトラフィックに対して分析を行った結果，同じサービスを狙っていると思われる多数のホストによる大規模なスキャン活動が複数ヶ国において同時期に観測されている事例が見つかった．それらの事象をさらに分析すると，各国のセンサ間で観測されたホスト数が急増するタイミングに時間差のあるケースが存在し，最大で 3 日程度の時間差がある事例も存在した．つまり，このようなスキャン活動の増加をいち早く捉え連携組織間で情報共有を行うことで，実際に攻撃活動が観測される前に情報を得ることができ，ネットワーク管理者などによる早期警戒や対策につなげられる可能性がある．

そこで，本論文では上記のような広範囲のインターネット空間に対して行われる大規模なネットワークスキャンを検知する手法を提案する．提案手法では，複数のダークネット観測拠点で得られた観測データから各センサにおける特定ポートに対する送信元ホスト数の急増を検出し，同様の事象が同一時期に一定数以上のセンサで観測されるか否かを判定することで，大規模なスキャン活動の発生を検知する．ダークネット観測で発生する事象には，必ずしも広範囲のスキャン活動だけではなく，特定のセンサのみで限定的に観測されるような攻撃活動も報告されている[2]ため，提案手法では観測拠点毎における検出結果を集約して判定を行うことで広範囲なインターネット空間に対する攻撃活動のみを検知対象とする．その結果として，提案手法によって検知された攻撃活動はまだ同様の事象が観測されていない観測拠点に対しても今後発生する可能性が高く，これらの検知結果を連携組織に対して展開することで早期警戒や対策につなげられることが期待できる．評価実験の結果，提案手法によってルータ等に存在するバックドアに対するスキャン活動や，Linux に感染するマルウェアがポート待ち受けを行うバックドアに対するスキャン活動などが，検知できていることが明らかになった．また，それらの事例を分析した結果，実際に各センサにおいて観測された攻撃元ホスト数が急増するタイミングに時間差が見られており，提案手法による検知時点では攻撃が観測されていなかった他のセンサでも，その後同様の攻撃の急増が観測されていたことから，攻撃が観測される前の早期アラートの発行が可能な事例が確認された．

以下，2 章では他組織によって報告されている特定ポートへのスキャン事例に関連したダークネット観測結果を示し，大規模なスキャン活動において，複数観測拠点による観測結果の傾向が類似することを示す．3 章では提案手法の概要及び実装について説明する．4 章では提案手法を実装し，各閾値を決定するための予備実験を行った上で，収集したダークネットトラフィックに対して提案手法を適用した評価実験について述べる．5 章において，実験結果に対する考察を行い，6 章でまとめとする．

2 ネットワークスキャン事例と各ダークネットセンサによる観測結果

本章では，文献[3,12,17]で実際にネットワークスキャン事例が報告されている 5000/tcp と 23/tcp の二つのポートに対するダークネット観測結果を示す．本論文では PRACTICE にて設置したダークネットセンサで観測・収集したダークネットトラフィックデータを用いる．以下に，各ダークネット観測拠

点の国情報およびそれぞれの観測対象 IP アドレス数を以下に示す. なお, 各センサの IP アドレスの第 1 オクテットはそれぞれ異なる.

(1) A 国 → 2,048 個(/24*8)
(2) B 国 → 256 個(/24)
(3) C 国 → 128 個(/25)
(4) D 国 → 128 個(/25)
(5) E 国 → 128 個(/25)

2.1 5000/tcp に対するスキャン活動

5000/tcp に対するネットワークスキャン事例が警察庁や Symantec から報告されている[3,17]. 当該ポートは脆弱性が公開された特定の NAS 製品の Web 管理機能[11]に用いられており, この脆弱性を狙ったスキャン活動だと推測される. 図 1 に上記の各ダークネットセンサで観測された, 宛先ポート 5000/tcp に対して TCP-SYN パケットを送信した IP アドレス数を 2014 年 2 月 1 日～2014 年 3 月 31 日にて 1 日毎に集計したグラフを示す. なお, 本論文における観測結果は全て日本標準時(JST)に合わせて集計している. 図 1 を見ると, 各センサで観測された送信元 IP アドレス数(観測ホスト数)の増減傾向が似た傾向を示していることがわかる. また, それまで 1 日当たりの観測ホスト数が数ホスト程度であったのに対し, 2014 年 2 月 12 日時点ですべてのセンサで数十ホストに増加していることを確認した. さらに, 2014 年 3 月 3 日～2014 年 3 月 8 日の間では今回の集計期間において各センサで観測した送信元ホスト数が最大となることが確認されたが, 2014 年 2 月 12 日の時点と異なりセンサ毎に最大となる日に数日程度の差が生じていた.

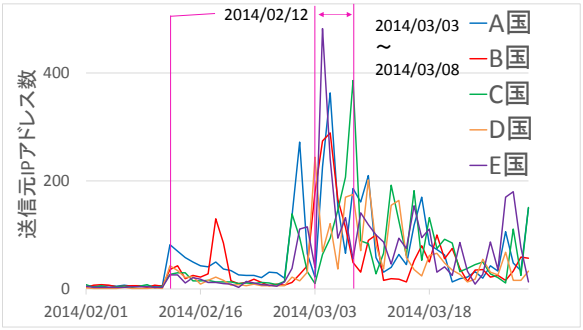

図 1 送信元 IP アドレス数の推移(5000/tcp)

2.2 23/tcp の事例

JPCERT や警察庁から, 23/tcp へのスキャンが 2014 年 1 月下旬から 2014 年 3 月にかけて活発に行われたと報告されている[3,12]. 図 2 に各ダークネットセンサで観測された 23/tcp へ TCP-SYN パケットを送信した IP アドレス数を 1 日毎に集計したグラフを示す. 図 2 を見ると, 5000/tcp に対する観測結果と同様にセンサ間で観測された送信元 IP アドレス数(観測ホスト数)の増減傾向が類似していることが見て取れる. ただし, 23/tcp に関しては, 各センサで観測ホスト数が最大となる日付にずれが無く, 完全に一致している点が異なる点である.

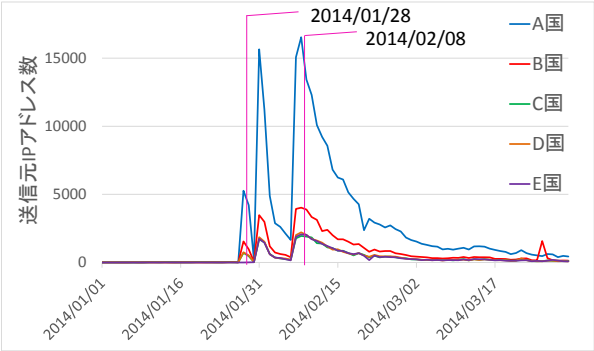

図 2 送信元 IP アドレス数の推移(23/tcp)

上記の 23/tcp および 5000/tcp に対するダークネット観測結果を見ると, 第 1 オクテットから異なる IP アドレス帯に設置された各観測拠点に置いて観測ホスト数の増加が確認されており, また他組織からも同様に攻撃活動の増加に関する複数の報告[3,12,17]がなされていることから, IPv4 アドレス空間の広範囲に対する大規模なスキャン活動が行われていることが推測される. さらに, 5000/tcp のケースでは, 各観測拠点間で攻撃が最も活発化した日時に数日程度の時間差があるため, 先に攻撃を観測した拠点からの情報を素早く展開することで, 他の拠点において実際に攻撃が活発化する前に攻撃情報の共有が可能であり, 早期警戒に役立てることができると考えられる.

そこで, 本論文では各ポートへ通信を行うホスト数の推移を各観測拠点に設置したダークネットセンサ毎に観測し, ホスト数の増加が同時期に複数拠点で発生するか否かによって, 広範囲にわたる大規模なネットワーク攻撃を検知する手法について提案する.

3 複数の観測拠点で同時期に急増する攻撃を検知する手法の提案

本章では, 2 章で説明した複数拠点で同時期にスキャンホスト数の増加が観測されるような大規模なネットワークスキャンを検知する手法を提案する. 以下, 3.1 節では提案手法の流れを説明し, 3.2 節で具体的な実装について述べる.

3.1 提案手法

提案手法は観測拠点毎にスキャンホスト数の増加率を算出するフェーズと, 複数拠点の上記の算出結果から大規模なスキャン活動を検知するフェーズの二つからなる. 提案手法では, 大量のダークネットトラフィックに対してリアルタイムの判定を可能とするために, 各宛先ポートに対する送信元 IP アドレス数の推移のみを用いたシンプルな判定を行う. 以下, 各フェーズの流れについて説明する.

【フェーズ 1】

フェーズ 1 ではダークネットで観測したパケットの情報から, 観測拠点毎にホスト数の増加指標を計算する. まず, 増加指標の計算のために必要な情報として, 観測した各パケットに関して以下の情報を抽出する.

- 観測センサ ID
- タイムスタンプ
- プロトコル
- 送信元 IP アドレス

- 宛先ポート番号

その後，各観測センサ ID の各プロトコル・宛先ポート番号に対して，以下に示す送信元 IP アドレスの増加程度を示す指標である増加率を算出する．なお，各センサで観測対象 IP アドレス数が異なるため，観測対象 IP アドレスの多寡によらない増加指標として，同ポートに対して過去にスキャンを行ったホスト数と現在のスキャンホスト数の変化（増加率 R）を以下の式で表現する．

t: パケット p のタイムスタンプ

$IP_{24h}(t)$: t より過去 24 時間以内に同ポートに通信を行った送信元 IP アドレス数

$IP_{avg}(t,x,y)$: t より x 日前から y 日間の間に同ポートに通信を行った送信元 IP アドレス数の 1 日平均

とするとき，

$$増加率\ R = \frac{1 + IP_{24h}(t)}{1 + IP_{avg}(t,x,y)}$$

なお，$IP_{avg}(t,x,y)$は期間中に観測されたホストが存在しない場合 0 になるため，分子と分母にそれぞれ 1 を加えて評価している．

【フェーズ 2】

次に，フェーズ 1 で算出した増加率 Rを基に，大規模スキャン活動の検知を行う．

Th_r: 増加率Rの閾値
Th_s: 観測センサ数の閾値
W: 検査対象期間

としたとき，各プロトコル・宛先ポートに対して，閾値 Th_rを超える増加率 R が期間 W の間に算出されている観測センサ ID 数が Th_sを超えた場合，検知アラートを出力する．

3.2 提案手法の実装

図 3 に今回の提案手法の実装概要を示す．まず提案手法の入力形式としては，pcap ファイル形式のダークネットトラフィックデータを入力とした．現状の我々の観測では，A 国のセンサに関しては 1 時間毎に，それ以外の国に設置されたセンサに関しては 1 分毎のトラフィックが一つの pcap ファイルとして作成されるため，これを順次入力として用いる．入力された各 pcap ファイルに対して，3.1 節で示した各パケット情報のデータベースへの登録を行う．

その後，入力された pcap ファイルに含まれるパケットの各ユニーク宛先ポート番号に対して，増加率 Rを計算し，データベースに以下の情報をホスト数増加ログとして格納する．なお，タイムスタンプについては，対象 pcap 内で各宛先ポートに送信されたパケットのうち一番新しいパケットのタイムスタンプを用いる．

- 観測センサ ID
- タイムスタンプ
- プロトコル
- 宛先ポート番号
- 増加率 R

一方，アラート出力プログラムは，定期的にデータベースを参照し，ホスト数増加ログを取得し，アラート出力判定を行う．現在の実装では，A 国のセンサ以外の pcap ファイルが 1 分おきに出力され，逐次データベースに情報が格納されていることから，アラート出力判定も 1 分おきに行っている．判定時は，データベースより最新の 1 分間のログを抽出し，その中に含まれるプロトコル・宛先ポート毎に，3.1 節のフェーズ 2 で説明した基準で，アラート出力判定を行う．アラート出力時は，以下の情報がアラート情報として出力される．

- 時刻
- プロトコル
- 宛先ポート番号
- Rが Th_r以上になった観測センサ数
- アラートに関連した，各センサの最新のホスト数増加ログ

本稿では，提案手法のための 2 つのプログラムとデータベースを 1 台の物理マシン（OS：Ubuntu 14.04，CPU：Intel Xeon E5620，メモリ：16GB）上に実装した．データベースとしては Elasticsearch v1.2.1[5]を用いたほか，パケット情報登録・増加率計算プログラムは C 言語で実装し，アラート出力プログラムは Perl スクリプトによって実装した．

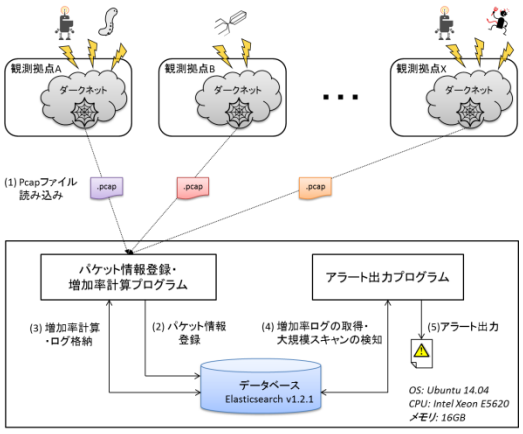

図 3 提案手法の実装概要

表 1 各ダークネットセンサへの適用期間

センサ設置国	適用期間			備考
A国	2014/01/09	～	2014/07/31	2014/04/06～2014/04/17の期間はトラフィックのキャプチャが出来ていなかった.
B国	2013/12/25	～	2014/07/31	
C国	2013/12/25	～	2014/07/31	
D国	2013/12/25	～	2014/07/31	
E国	2014/01/29	～	2014/07/31	

表 2 R算出期間

センサ設置国	適用期間			備考
A国	2014/02/09	～	2014/07/31	2014/05/03/～2014/05/20の期間は適用対象外とした.
B国	2014/01/25	～	2014/07/31	
C国	2014/01/25	～	2014/07/31	
D国	2014/01/25	～	2014/07/31	
E国	2014/02/28	～	2014/07/31	

4 評価実験

本章では 3 章で提案した手法の評価のために行った実験について説明を行う. 4.1 節では 3.2 節で述べた, 提案手法の送信元 IP アドレス数増加指標に対する閾値 Th_rを設定するための予備実験及びその結果について説明する. 4.2 節では提案手法に収集したダークネットトラフィックを適用した実験について説明する. また, 4.3 節では提案手法との比較のため, 各センサで観測されたトラフィックを区別せずに一つに結合し提案手法のうちフェーズ 1 を適用した実験について説明する. 各ダークネットセンサでの観測期間を表 1 に示す. A 国と E 国に関してはセンサの稼働期間の関係で提案手法に適用した期間が他国のセンサと異なる.

4.1 予備実験

本節では, 提案手法の増加率 R の閾値 Th_rを決定するために行った予備実験について説明をする. 予備実験では, 2 章で説明をした 5000/tcp の事例を参考に Th_r, Th_s, Wを決定した.

まず, $IP_{avg}(t,x,y)$のパラメータ(x,y)については一定期間過去の状態の平均を見るべきであると考え, (30,7)を設定した. そのうえで各センサにて観測された 5000/tcp のトラフィックに対して Rを計算し, プロットしたグラフが図 4 である. 提案手法ではタイムスタンプから 24 時間前までのホスト数をカウントするが, 図 4 では簡単のために$IP_{24h}(t)$は 0 時～24 時までの 1 日毎の集計とし, $IP_{avg}(t,30,7)$に関しても同様に計算を行った.

図 4 から, 2.1 節で分析した際と同様に, 2014 年 2 月 12 日に 4 センサで同時に増加率 Rが増加することが分かる. また, 2014 年 3 月 3 日～2014 年 3 月 8 日の期間で各センサにて増加率 R の値が最大となる. 上記の期間中で各センサの値が最大となる日付は図 1 で送信元 IP アドレス数が最大となる日付と一致していた. また, 最初に送信元 IP アドレス数が増加しているとみられる 2014 年 2 月 12 日の時点で, 4 拠点のセンサの Rは 10 以上となっていることから, 閾値 Th_rを 10 と設定した. Wと Th_sに関しては, Wは上記の事例より送信元 IP アドレス数が最大になる日がセンサ毎に最大 6 日の差が観測されている点を考慮し, 7 日間とした. Th_sは今回の評価実験の対象とする 5 センサの過半数となるセンサ数 3 を設定した.

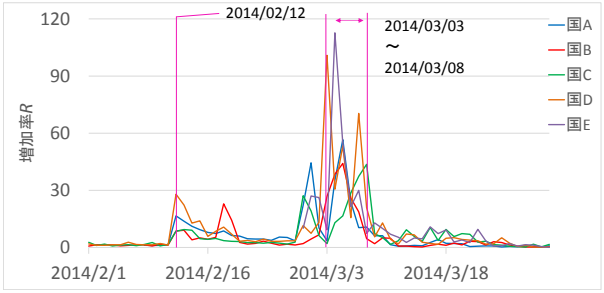

図 4 5000/tcp における R値の変化

4.2 評価実験

本節では, 提案手法に設置したダークネットセンサで観測されたトラフィックを適用して行った評価実験について述べる. 提案手法に適用したダークネットトラフィックの観測期間は表 1 のとおりである. 増加率 Rの算出期間は表 2 に示した. センサの稼働停止期間の関係から, $IP_{avg}(t,30,7)$の計算期間にセンサの稼働停止期間が 4 日以上重なる 2014 年 05 月 03 日～2014 年 05 月 20 日については増加率 Rの算出対象外とした. また, 入力とするパケットは TCP-SYN パケットに限定した.

評価実験にてアラートが出力されたポートの一覧を表 3 に示す. 評価実験の期間において, 51 ポートに対してアラートが出力された.

4.3 比較実験

提案手法ではそれぞれのセンサで観測されたダークネットトラフィック毎に, 増加率 R を計算し, 一定数のセンサで同時期に増加率 R が閾値を超えることをもってアラートを出力している. そこで, 提案手法による上記のセンサ間の同時期性を考慮する点の効果を評価するために, 各センサで観測されたトラフィックを個別に扱わずに単純に結合して入力し, 増加率 Rを計算する手法(以下, 非センサ区別手法)を実装した. 具体的には, 3.1 節で述べた提案手法のフェーズ 1 を適用し増加率 Rを計算した際に, 閾値 Th_rが 10 を超えた段階でアラートを出力する処理とした. 各センサで同時刻に収集したトラフィックのうち, TCP-SYN パケットのみを一つの pcap ファイルに結合し入力として, 実験を行った. この際, 1 時間ごとに作成される A 国のセンサについてはその他センサで同時 00 分に作成される pcap ファイルと結合した. まず, 提案手法による検知結果の妥当性に関する評価として 2014 年 6 月 1 日から 2014 年 6 月 30 日の期間のトラフィックに対して非センサ区別手法を適用した. また, 処理にかかる時

間の比較として，2014 年 7 月 1 日の 24 時間のトラフィックに対して提案手法及び非センサ区別手法を適用し，それぞれの pcap ファイルの処理にかかる時間を計測した．

実験結果を表 4 に示す．

表 3 アラート出力ポート番号

ポート番号					
11	502	3128	8080	20000	59953
15	771	3790	8081	20111	
17	902	4911	8088	21320	
21	992	5000	8089	32764	
23	993	5900	8333	34205	
80	1080	5985	8834	34567	
102	1723	5986	9160	44818	
135	1911	6000	9981	49152	
201	2067	7557	10073	58455	
501	2628	7778	11211	59901	

表 4 比較実験の結果

① 比較のための手法によりアラートが出力されたポート	251ポート
② 同期間に提案手法によりアラートが出力されたポート	7ポート
③ 比較のための手法で1ファイルの処理にかかった平均時間	1.043秒
④ 提案手法で1ファイルの処理にかかった平均時間	0.998秒

5 考察

本章では4章で行った実験の結果について考察を行う．5.1 節では提案手法により SHODAN[20]などの団体による調査目的と思われるスキャンを検知していることについて述べる．5.2 節では，4.2 節で検知したポートについて報告されているスキャン事例との比較を行う．5.3 節では各センサでスキャンホスト数の増加が検知されるまでの時間差があることから，本手法がネットワーク攻撃の早期警戒に貢献できる可能性について述べる．

5.1 調査目的と思われるスキャンの検知

4.2 節で示した，アラートが出力された TCP ポートに通信を行った送信元 IP アドレス数を集計したところ，10~20 程度の IP アドレスからスキャンを行われている事例が多く含まれていることが分かった．そこで，それらの IP アドレスに対して Google Public DNS(8.8.8.8)を使用して DNS の逆引きを試みた．この結果，

****.shodan.io

****.****.rapid7.com.

などのホスト名が得られた．これらは，SHODAN[20]，Rapid7[10,16]などの団体による脆弱性をもった機器の存在を調査する目的のスキャンと考えられる．また，表 5は4.2節の評価実験でアラートが出力された全ポートに対して，アラート出力から過去 24 時間以内の送信元 IP アドレスのホスト名を以下のステップで調査を行った結果である．

1. **アラートが出力された時刻から，過去 24 時間以内に当該ポートに通信を行った IP アドレス数が全センサで合計 20 以下の場合 2.に進む．**
2. **各送信元 IP アドレスを Google Public DNS を使用して逆引きを行う．**
3. **逆引きの結果，以下の文字列をホスト名中に含む IP アドレスが 5 割を超えた場合，調査を目的とした団体のスキャンとする．**
   shodan, rapid7, sslsonar,
   shadowserver

提案手法が出力するアラートには SHODAN や Rapid7 によるスキャンが多く含まれている．これらはマルウェアが行う感染目的のスキャンなどとは異なるが，少なくとも今回調査した団体については DNS 逆引きにより特定ができるため提案手法によるアラート出力時も排除が可能であると考えられる．また，脆弱な機器の調査を目的としていることから，これらの団体が調査しているポートについて知ることは無意味ではない．

また，501/tcp 及び 34567/tcp を個別に調査したところ，ミシガン大学に割り当てられた IP アドレスからスキャンが行われていることが分かった．ミシガン大学では高速ネットワークスキャンツールである ZMap[23]を開発しており，同ツールを使用したスキャンを行っていることが推測される．

表 5 調査目的スキャンの確認

ポート番号 - 調査系スキャンのチェック			
11	SHODAN	5985	SHODAN
15	SHODAN	5986	SHODAN
17	SHODAN	6000	SHODAN
21		7557	Rapid7
23		7778	
80		8080	
102	SHODAN	8081	
135		8088	
201	Rapid7	8089	SHODAN
501		8333	SHODAN
502	SHODAN	8834	SHODAN
771	SHODAN	9160	SHODAN
902		9981	SHODAN
992	SHODAN	10073	
993	Rapid7, SHODAN	11211	SHODAN
1080		20000	SHODAN
1723	SHODAN	20111	Rapid7
1911	SHODAN	21320	
2067	SHODAN	32764	
2628	SHODAN	34205	Rapid7
3128		34567	
3790	SHODAN	44818	SHODAN
4911	SHODAN	49152	SHODAN
5000		58455	
5900		59901	Rapid7
		59953	Rapid7

5.2 ネットワーク攻撃事例との比較

本節では，4.2 節で行った実験で検知したポートのうち，32764/tcp 及び 58455/tcp の事例について各種報告等との比較を行う．

表 6 初回アラートの出力日時

ポート	初アラート出力日時
32764	2014/2/21 23:59
58455	2014/2/21 22:58

5.2.1 32764/tcp について

当ポートに関しては，複数の企業が販売しているルータにデフォルトでバックドアの存在する脆弱性が報告[15]されており，その使用ポートとされている．当脆弱性は github にて 2014 年 1 月 1 日に公開[6]されており，同月 5 日には poc も公開されている．しかしながら，提案手法での当該ポートへの初のアラート出力日時は表 6 に示したとおり 2014 年 2 月 21 日であり，これらの情報公開日とは対応していない．図 5 は当該ポートに通信を行った IP アドレス数の集計である．ホスト数が増加する初期の段階をアラートとして出力していることが分かる．また，2014 年 2 月 21 日 0 時から 2014 年 2 月 22 日 0 時の間にそれぞれのセンサに 32764/tcp ポートをスキャンした送信元 IP アドレス数を調査したところ 176 ホストであり，このうち半数近くの 87 ホストが同日に 58455/tcp にもスキャンしていることが観測されていた．このことから，次節で説明する 58455/tcp を使用するマルウェアと関連が深いネットワークスキャンであると考えられる．

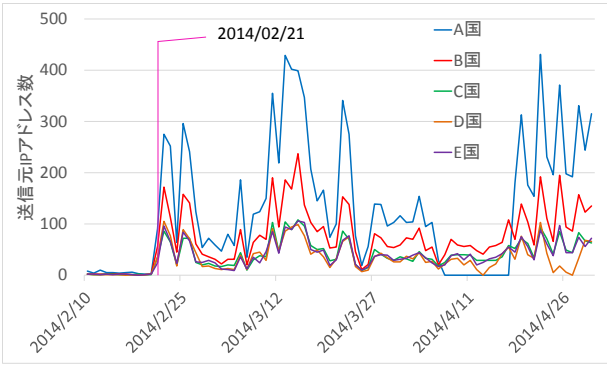

図 5 32764/tcp 宛送信元 IP アドレス数

5.2.2 58455/tcp について

提案手法では本ポートでのアラートを表 6 に示すように，2014 年 2 月 21 日に初めて出力している．本ポートへ通信を行った送信元 IP アドレス数を集計した図 6 から，32764/tcp の事例と同じくホスト数増加の初期段階を捉えていることがわかる．

Symantec のレポート[13]によれば，本ポートは Linux 系 OS に感染する Linux.Darlloz が HTTP で自身の拡散やコマンド待ち受けのためのバックドアとして使用する．また，レポート[13]には当該マルウェアが 58455/tcp をスキャンする挙動を示すという記載は無いが，各国のダークネットで観測された 58455/tcp に通信を行ったいくつかのホストでは 58455/tcp が待ち受け状態となっていることが確認できたため，当該ポートが Linux.Darlloz 間の通信にも使用されている可能性もある．文献[9]では 2014 年 1 月中旬には Linux.Darlloz にコインマイニングの機能が追加されたと報告されており，作成者が別途何らかのアップデートを行った結果，58455/tcp 及び 32764/tcp へのスキャンを行う機能が付加された可能性がある．

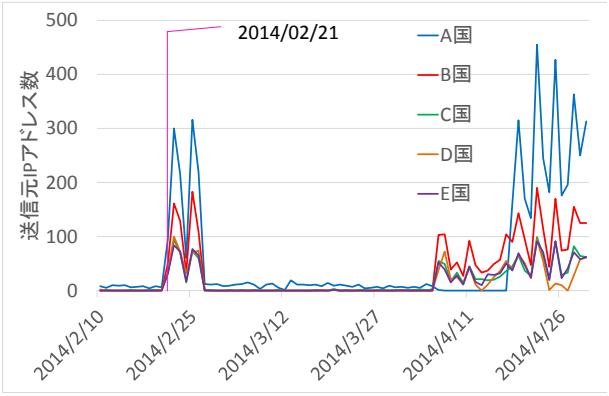

図 6 58455/tcp 宛送信元 IP アドレス数

5.3 早期警戒に関する考察

本節では，提案手法により検知されるトラフィックの急増が各センサで観測されるまでに時間差がある場合があることを示し，このことから提案手法により出力されるアラートを各ダークネットセンサ設置国に通知することでネットワークスキャンの早期警戒に繋がる可能性について述べる．

評価実験では，5000/tcp に対するアラートは 2014 年 2 月 12 日に初回の出力をしていた．これは，図 1 や図 4 から分かるように，初期の送信元 IP アドレス数増加を捉えたものである．一方で，2014 年 3 月 3 日～8 日の間で観測期間内の送信元 IP アドレス数がさらに増加するような時点も重要である．そこで，図 4 から 2014 年 3 月 3 日～8 日の間で過半数の 3 つのセンサでの増加率 R の値が 50 以上となっていることから，各事例で R の値が 50 以上となる時刻について調査を行い，結果を表 7 にまとめた．1 回目から 3 回目までのアラート出力を記載しており，一度 R の値が 50 以上となってから以後 24 時間は同じ回数としてカウントしている．

表 7 において黄色で着色されたマスは，各センサ間で同時期に発生していると思われる事象である．23/tcp の事例では B 国のセンサで増加率 R が 50 以上となってから C 国で同じく 50 以上となるまでに約 6 時間の差であった．また，32764/tcp，58455/tcp はともに最初のセンサで 50 以上の増加率 R が観測されてから 4 番目で観測されるまでに約 11 時間の時間差があることがわかった．5000/tcp の事例では，上記事例よりもさらに時間差が大きく最初のセンサと 5 番目のセンサで増加率 R が 50 以上となるまでに 3 日と 15 時間程度の時間差があった．

表 7 R の値が 50 以上となる時刻

5000/tcp

センサ設置国	1回目	2回目	3回目	備考
A国	2014/02/13 00:59	2014/02/28 23:51	2014/03/02 00:39	
B国	2014/02/18 19:11	2014/03/03 14:37	2014/03/04 15:42	
C国	2014/02/28 23:09	2014/03/06 05:29	2014/03/07 07:42	
D国	2014/03/03 03:32	2014/03/04 03:45	2014/03/05 03:45	
E国	2014/03/01 17:46	2014/03/02 18:09	2014/03/04 03:14	

23/tcp

センサ設置国	1回目	2回目	3回目	備考
A国	2014/02/09 09:59	2014/02/10 09:59	2014/02/11 10:59	1月は期間外
B国	2014/01/28 08:51	2014/01/29 08:52	2014/01/30 09:03	
C国	2014/01/28 15:03	2014/01/29 15:13	2014/01/31 04:09	
D国	2014/01/28 13:32	2014/01/29 13:33	2014/01/31 02:33	
E国	-	-	-	期間外

32764/tcp

センサ設置国	1回目	2回目	3回目	備考
A国	2014/02/22 10:59	2014/02/23 11:50	2014/02/24 12:59	
B国	2014/02/22 09:43	2014/02/23 10:19	2014/02/24 11:44	
C国	2014/02/22 20:13	2014/03/11 09:15	2014/03/12 09:30	
D国	2014/02/22 11:17	2014/02/23 17:48	2014/02/25 18:30	
E国	2014/03/11 10:16	2014/03/12 10:29	2014/03/13 10:30	

58455/tcp

センサ設置国	1回目	2回目	3回目	備考
A国	2014/02/26 02:56	2014/04/22 20:58	2014/04/25 04:58	
B国	2014/02/22 02:46	2014/02/23 02:49	2014/02/24 03:11	2014/04/06 16:05
C国	2014/04/07 00:56	2014/04/22 16:58	2014/04/23 16:58	
D国	2014/02/22 09:56	2014/02/23 14:26	2014/02/25 12:02	2014/04/07 02:57
E国	2014/04/06 22:35	2014/04/18 04:26	2014/04/19 12:19	

以上のことから，アラートに含まれる 3 つ以上のセンサで増加率 R の値が 50 を超える場合のような，スキャンの急激な増加を観測した際には，アラートの観測センサに含まれない拠点については最大で数日程度事前にアラートを取得できるため，早期に警戒し対応につなげられる可能性がある．

5.4 提案手法によるアラートの精度，処理時間の評価について

本節では，4.3 節で行った非センサ区別手法を用いた実験結果について考察を行う．

まず，2014 年 6 月の 1 か月間のトラフィックに対して行った実験ではアラートが出力されたポートは 251 ポートあった．これらのポートに対して 5.3 節と同様に，送信元 IP アドレス数が急激に増加する時点として増加率 R が 50 以上となるログが存在するかを確認したところ，8081/tcp，32764/tcp，58455/tcp の 3 ポートのみで確認ができた．これに対して提案手法による同期間に対するアラート出力ポートは 7 ポートであった．また，増加率 R が 3 つのセンサ以上で 50 以上となったアラートの存在するポートは非センサ区別手法と同じ 3 ポートであった．また，提案手法でアラートが出力されていて増加率 R が 50 以上とならなかったポートについては 5.1 節の調査から 3128/tcp を除いて SHODAN 等によるスキャ

ンであることがわかっている. 非センサ区別手法では増加率 R が 50 以上となるようなホスト数が大幅に増加しているスキャン以外にも 248 のポートでアラートを出力しており, これらを False Alert と考えると提案手法のほうが False Alert の発報が少ないとみることもできる.

また, 2014 年 7 月 1 日のトラフィックを使用して提案手法及び非センサ区別手法の処理時間の比較を行った実験からは, 1 ファイルあたりの処理時間は提案手法のほうが約 0.05 秒速いという結果になった. 1 ファイルの処理時間がおよそ 1 秒であることを考えると, 提案手法のほうが 5%ほど処理にかかる時間が短いとも言える. 提案手法に比べ非センサ区別手法では提案手法のフェーズ 2 にあたる部分を実行していないにもかかわらず, 提案手法のほうが処理にかかる時間が短い. これは, フェーズ 1 で増加率 R を計算する際に検索するデータベース領域に格納されているパケットデータが, センサ毎に領域が分かれている提案手法のほうが少なく, 検索にかかる時間が短くなるためだと思われる.

以上の点から, 提案手法では, 非センサ区別手法よりも検知精度・処理時間の点で優れていると言える.

6 まとめ

本論文では PRACTICE により複数ヶ国に設置したダークネットセンサの観測結果から, 複数のセンサで同時期に特定のポートへのトラフィックが急増する事象を検知する手法について提案した. 収集したダークネットトラフィックを使用して行った評価実験から, 32764/tcp や 58455/tcp といったポートへのスキャンが増加する初期の段階を提案手法により捉えていることを確認した. また, 多くのポートに対して脆弱性を持った機器の存在を調査する目的のスキャンが行われていることも確認された. 評価実験の結果から, 提案手法で検知されたスキャンの中には, 観測ホスト数の急増を検知するまでに数時間～数日程度の時間差がある事象が存在することがわかった. このことから特に数日程度の時間差が存在する場合, アラート出力段階で各組織に通知を行うことでホスト数の急増を観測していない組織には早期警戒として情報提供できる事例を示した. また, 提案手法ではセンサ毎に観測ホスト数の増加を評価することにより, 検知精度及び処理速度が向上することが分かった.

今後の課題としては, 提案手法を UDP のトラフィックに適用して評価を行うことと, リアルタイム処理のためにスループットを検証することや, 早期警戒の有効性について定量的に評価することなどが挙げられる.

謝辞

本研究の一部は総務省情報通信分野における研究開発委託「国際連携によるサイバー攻撃予知技術の研究開発」により行われた.

参考文献

[1] K. Nakao, K. Yoshioka, D. Inoue, M. Eto, "A Novel Concept of Network Incident Analysis based on Multi-layer Observations of Malware Activities," Proc. of the 2nd Joint Workshop on Information Security (JWIS2007), pp.267-279, 2007
[2] 鈴木 将吾, 小出 駿, 牧田 大佑, 村上 洸介, 笠間 貴弘, 島村 隼平, 衛藤 将史, 吉岡 克成, 松本 勉, 井上 大介, "複数国ダークネット観測による攻撃の局地性分析, " コンピュータセキュリティシンポジウム 2014
[3] @police インターネット観測結果等（平成 26 年 2 月期）, http://www.npa.go.jp/cyberpolice/detect/pdf/20140328.pdf
[4] @police インターネット定点観測, http://www.cyberpolice.go.jp/detect/observation.html
[5] Elasticsearch.org Open Source Distributed Real Time Search & Analytics | Elasticsearch, http://www.elasticsearch.org/
[6] elvanderb/TCP-32764, https://github.com/elvanderb/TCP-32764
[7] 発信元 IP アドレスを偽装したオープン・リゾルバの探索行為の増加について, http://www.npa.go.jp/cyberpolice/detect/pdf/20140217.pdf
[8] インターネット早期広域攻撃警戒システム WCLSCAN, http://www.wclscan.org/
[9] IoT Worm Used to Mine Cryptocurrency | Symantec Connect, http://www.symantec.com/connect/blogs/iot-worm-used-mine-cryptocurrency
[10] IT Security Data & Analytics, Risk Management, Compliance | Rapid7, http://www.rapid7.com/
[11] Japan Vulnerability Note(JVN) JVN#95919136 Synology Disk Station Manager にアクセス制御不備の脆弱性, https://jvn.jp/vu/JVNVU95919136/index.html,2014-8-10.
[12] JPCERT インターネット定点観測レポート（2014 年 1～3 月）, https://www.jpcert.or.jp/tsubame/report/report201401-03.html
[13] Linux.Darlloz Technical Details | Symantec, http://www.symantec.com/security_response/writeup.jsp?docid=2013-112710-1612-99&tabid=2
[14] ntpd の monlist 機能を使った DDoS 攻撃に関する注意喚起, https://www.jpcert.or.jp/at/2014/at140001.html
[15] NVD Vulnerability Summary for CVE-2014-0659, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0659
[16] Project Sonar: Welcome to Project Sonar! , https://community.rapid7.com/community/infosec/sonar/blog/2013/09/26/welcome-to-project-sonar
[17] Rise in 5000/TCP scanning highlights Synology appliance vulnerabilities, http://www.symantec.com/connect/blogs/rise-5000tcp-scanning-highlights-synology-appliance-vulnerabilities
[18] SANS Internet Storm Center, https://isc.sans.edu/
[19] Scans Increase for New Linksys Backdoor (32764/TCP), https://isc.sans.edu/diary/Scans+Increase+for+New+Linksys+Backdoor+%2832764TCP%29/17336
[20] SHODAN - Computer Search Engine, http://www.shodanhq.com/
[21] The Darknet Project - TEAM CYMRU CPMMUNITY SERVICES, http://www.team-cymru.org/Services/darknets.html
[22] TSUBAME(インターネット定点観測システム), https://www.jpcert.or.jp/tsubame/
[23] ZMap ・ The Internet Scanner, https://zmap.io/