3　サイバーセキュリティ技術：ダークネット観測・分析技術
3-1　NICTER のダークネット長期分析

笠間貴弘

NICTER プロジェクトでは、ダークネットに届く大規模かつ無差別型の攻撃通信の観測・分析を継続して行っている。本稿では、2011 年から 2015 年までの 5 年間のダークネット観測結果について報告し、ダークネット観測がとらえてきたインターネットにおけるサイバー攻撃の変遷について概観する。

1　はじめに

サイバー攻撃対策の第一歩は実際に発生している攻撃活動を迅速かつ正確に把握することから始まる。我々は、インターネット上における大規模かつ無差別な攻撃活動について、その大局的な攻撃傾向を把握するためにインシデント分析センタ NICTER（Network Incident analysis Center for Tactical Emergency Response）の研究開発を推進し、2005 年から約 11 年間にわたりダークネット観測・分析を行ってきた[1]–[3]。ダークネットとはインターネット上で到達可能かつ未使用の IP アドレス空間のことを指す。正規のサーバやコンピュータが接続されていないダークネットには本来、通信（パケット）が届くことはないはずだが、実際に観測を行うと大量のパケットがダークネットに届いていることがわかる。これらのパケットは主にマルウェア（不正プログラム）に感染したコンピュータが次の攻撃先を探索する活動（スキャン）や、送信元 IP アドレスを詐称し送られた DDoS 攻撃（分散型サービス妨害攻撃）に対する応答であるバックスキャッタなど、何らかの不正な活動に起因しているため、ダークネット観測を通じてインターネット上で発生しているサイバー攻撃の大局的な傾向を把握することができる。

本稿では、NICTER のダークネット観測結果について統計的な分析を行い、攻撃活動の変遷を明らかにするとともに、特徴的な攻撃活動について述べる。

2　ダークネットアドレス数の推移

一般的に観測対象のダークネットアドレス数が増えるほど、より多くの攻撃活動が観測できる。また、観測された攻撃活動が局地的なものか広範囲で発生しているかを把握するためにも観測対象のダークネットは特定のアドレス帯ではなく、インターネット上に広く分布している方が望ましい。そのため、NICTER では国内外の様々な組織との連携を基にダークネットセンサを分散配置し、それらのセンサで観測したダークネットトラフィックをリアルタイムにセンタに集約・管理するダークネット観測網を構築している。2005 年に約 1.6 万アドレスから開始したダークネット観測網は、2016 年 4 月時点で 30 万アドレスまで到達し、国内では最大のダークネット観測網を構築している。

3　ダークネット観測統計の推移

3.1　観測パケット数及びユニークホスト数の推移

ダークネット観測結果の量的な変化を明らかにするため、図 1 及び 2 に 2011 年 1 月 1 日から 2015 年 12 月 31 日までにダークネット観測で観測された日ごとのパケット数とユニークな送信元 IP アドレス数（以下、ユニークホスト数）の推移（全パケット、TCP パケットのみ、UDP パケットのみ）を示す。なお、以降の時系列折れ線グラフにおいて、観測パケット数については観測対象のダークネットアドレス数の増減の影響を強く受けるためセンサ数（ダークネットアドレス数）で正規化し、観測パケット数とユニークホスト数ともに傾向を把握しやすいように 2 週間の移動平均を示している。

図 1 からわかるとおり、ダークネットで観測されるパケット数は多少の増減はあるものの長期的に見れば増加傾向を示しており、特に 2014 年以降は急激に観測パケット数が増加している様子がわかる。この増加の主な原因は、後述する組込み機器に関連した攻撃活動や、DRDoS（Distributed Reflection Denial of Service）攻撃などの DDoS 攻撃の活発化の影響である。また、観測パケット数の増加に対応して、図 2 のユニー

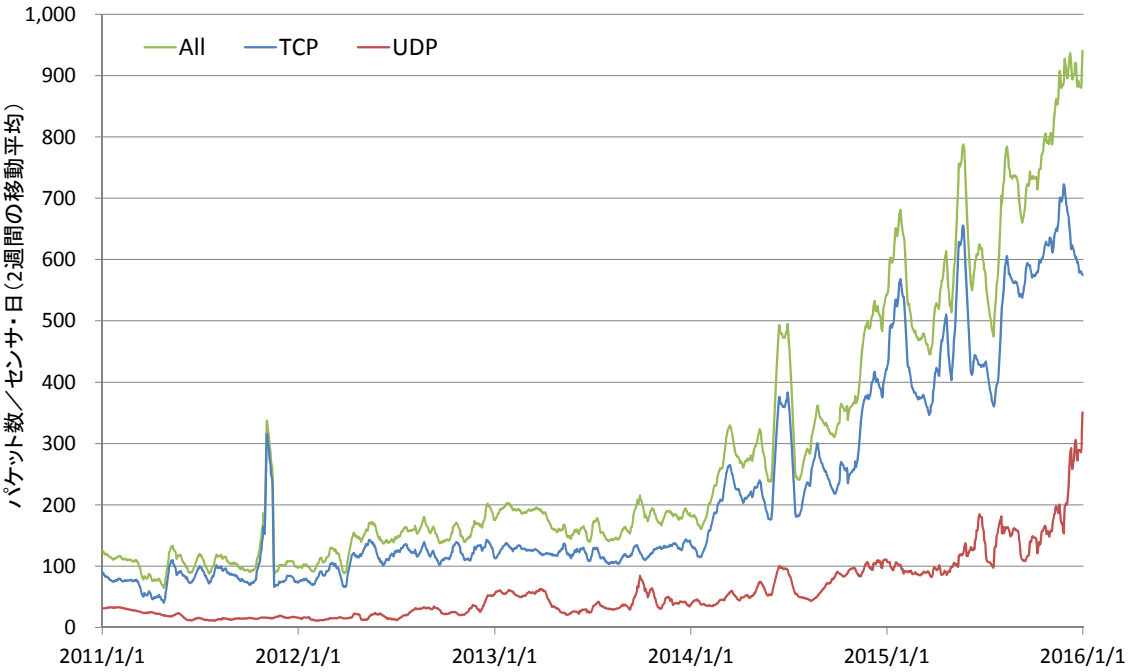

図 1　5 年間の観測パケット数の推移

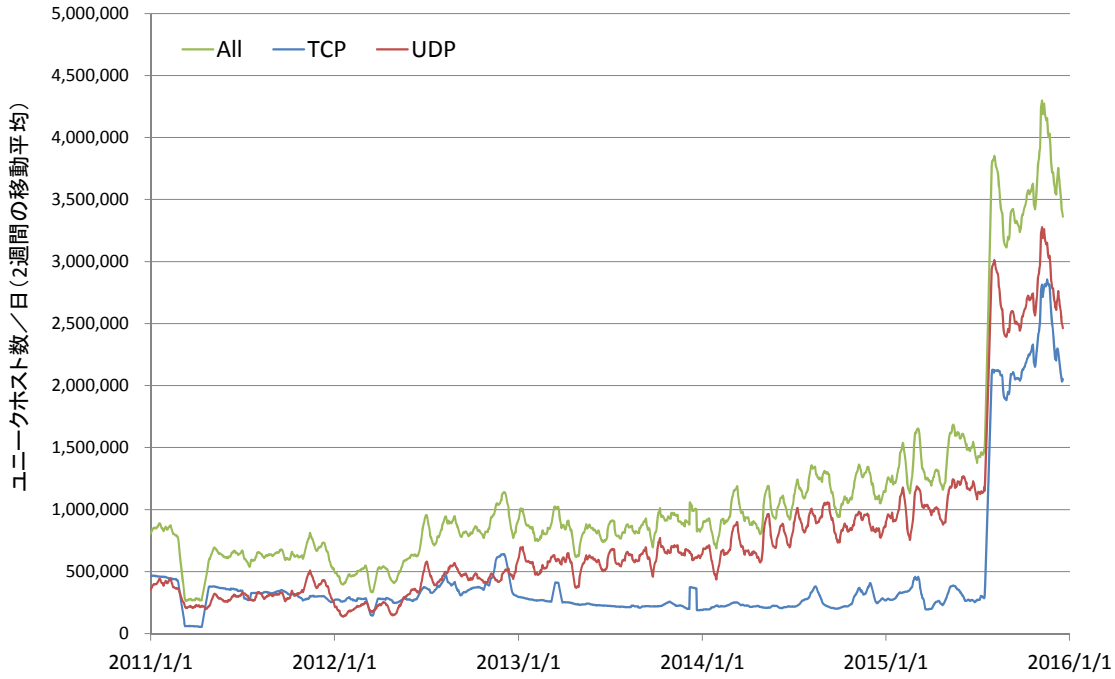

図 2　5 年間のユニークホスト数の推移

クホスト数についてもセンサ数増加の影響はあるものの、全体として増加傾向を示している。なお、2015 年中旬からの急増は P2P（Peer-to-Peer）と見られるパケットをダークネットに送信するホストが大量に観測されている影響であるが、詳細な原因については明らかになっていない。

従来、ダークネットで観測されるパケットの多くはワーム型のマルウェアによる（主に Windows OS をねらった）スキャンであったが、2008 年前半まではダークネットで観測されるユニークホスト数の減少も相まって、2000 年代前半に発生した Sasser や Blaster、SQL Slammer のようなワーム型マルウェアの大規模感染はもう起りえないとまで言われていた。しかしながら、2008 年後半の Conficker ワーム、2011 年の Morto ワーム、2012 年の Carna ボットネットなど、広範囲のネットワークスキャンを通じて大規模感染を引き起こすマルウェアはその後も次々と出現し、観測パケット数は増加し続けている。また近年では、

表 1　あて先ポート・プロトコル別の年間観測パケット数の割合

2011年		2012年		2013年		2014年		2015年	
Port	%	Port	%	Port	%	Port	%	Port	%
445/TCP	51.3	445/TCP	47.8	445/TCP	36.0	23/TCP	20.9	23/TCP	21.4
1433/TCP	6.4	3389/TCP	8.8	3389/TCP	5.7	445/TCP	15.1	445/TCP	7.0
53/UDP	5.1	1433/TCP	6.6	10320/UDP	5.5	22/TCP	6.2	22/TCP	4.7
22/TCP	2.6	23/TCP	6.6	53/UDP	4.3	80/TCP	4.5	80/TCP	3.1
3389/TCP	2.3	22/TCP	3.3	1433/TCP	3.8	3389/TCP	3.7	8888/TCP	2.2
80/TCP	2.2	10320/UDP	3.2	23/TCP	3.8	53/UDP	3.6	8080/TCP	2.2
135/TCP	1.6	80/TCP	3.1	80/TCP	3.1	8080/TCP	3.6	3389/TCP	2.0
3306/TCP	1.1	8080/TCP	2.0	22/TCP	2.7	5000/TCP	3.2	53413/UDP	1.9
5060/UDP	1.1	210/TCP	1.6	8080/TCP	1.5	1433/TCP	2.9	443/TCP	1.6
23/TCP	0.9	3306/TCP	1.4	18991/UDP	1.3	443/TCP	2.6	53/UDP	1.5

Zmap や masscan などのオープンソースの高速ネットワークスキャナを用いたスキャンや、セキュリティベンダや研究組織による調査目的の定期的なスキャン、DRDoS 攻撃の事前準備のためリフレクタを探索するためのスキャンなど、従来のワーム型マルウェアのスキャンとは異なるパケットも数多く観測されており、ダークネット観測で把握できる攻撃活動は量的な増加だけでなく質的な観点でも多様性を増している。

3.2　攻撃対象サービスの変化

次に攻撃対象サービスの変化を把握するために、表 1 に 2011 年から 2015 年までの各年について、各あて先ポート・プロトコル別にパケット数を集計した上位 10 件を示す。

2008 年に世界中で大規模感染を引き起こした Conficker は 445 /TCP（Windows の Server サービス）の脆弱性を悪用して感染を拡げる機能を備えていたが、我々の観測では 445 /TCP への攻撃パケット数がいまだに上位を占めている様子が観測されている。Conficker Working Group の報告でも 2015 年末の時点において日に約 60 万 IP アドレスの感染ホストの観測が報告されており、発生から約 7 年が経過した今でも Conficker のスキャンの影響が大きいことがわかる。同様に 2011 年に出現した Morto ワームは 3389 /TCP（Windows リモートデスクトップ接続）に対してスキャンを行い、管理者としてログインすることで感染を広めようとするが、この 3389 /TCP に対するスキャンも継続して観測され続けている。

このような過去に流行したワーム型マルウェアのスキャンがいまだに観測され続けていることに加え、新たな攻撃活動も多数観測されている。この 5 年間で最も顕著な変化としては、23 /TCP（Telnet）に対するスキャンの増加である。Telnet はネットワーク越しに他のコンピュータにアクセスしてリモート操作するためのプロトコルであるが、Telnet 自体は認証や通信を暗号化しないため、インターネット上で利用することは危険性が高い。ところが、ここ数年の IoT（Internet of Things）の気運の高まりに応じて多種多様な機器がインターネットにつながるようになっているが、これらの機器の多くでは Linux OS が搭載され、さらに Telnet サービスが稼働しインターネット上からアクセス可能な状況であることが明らかになっている。こうした組込み機器をねらった Telnet に対する攻撃活動が 2012 年頃から活発化した結果、ダークネット観測においても多数の Telnet に対するスキャンが観測されている。Telnet 以外にも 2014 年の 5000 /TCP、2015 年の 53413 /UDP などもルータや NAS（Network Attached Storage）といった特定の機器の脆弱性に対する攻撃活動である。こうした従来の Windows OS を対象とした攻撃活動とは異なる攻撃活動が、今後も活発化していくことが予想される。他には、2011 年より DNS オープンリゾルバを探索する 53 /UDP あてのスキャンが顕著に増加しており、割合としても上位になっている。DNS に限らず、NTP や SNMP などの DRDoS 攻撃に悪用可能な各種リフレクタの探索活動も増加している。

4　ケーススタディ

本節では、この 5 年間の観測における特徴的な観測事象について述べる。

4.1　組込み機器をねらった攻撃の増加

表 1 で示したように、ここ 2 年間において 23 /

TCP（Telnet）に対するスキャンが急増している。図3に23/TCPに関する観測パケット数とユニークホスト数の推移を示す。図3を見ると、2012年後半にユニークホスト数が急激なピークを示し、1日あたり30万ホスト以上が観測されていることがわかる。我々の分析の結果、このスキャンは同時期に活動していたCarnaボットによる大規模スキャンが観測されていたことがわかっている[4]。Carnaボットは2012年に匿名の人物によって作成され、Telnetに対する大規模スキャンと辞書攻撃によるログイン試行によって、インターネット上につながった約42万台ものルータやWebカメラ等の組込み機器に感染したと報告されている。これらの組込み機器に多くは「admin」「password」「1234」など、デフォルトで設定されている安易なIDとパスワードのままで運用されており、簡単に管理者権限でインターネット上からログインが可能となっていた。Carnaボットの作成者はそれらの機器を悪用しIPv4アドレス空間全体に対してスキャンを行い、その結果をインターネット上で公開した。Carnaボットは短期間の活動後に活動を終了したため、ダークネットでのTelnetに対するスキャンもいったん沈静化したが、2014年初めから再度活発化し、以降は継続して多数のスキャンを観測している。

そこで、これらのTelnetに対してスキャンを行っている攻撃元ホストの素性を明らかにするため、我々は2015年8月25日から8月31日までの1週間でスキャンを観測した約20万アドレスに対して、Telnet及びHTTPでアクセスを行い、得られた応答情報から機器の識別を試みた。その結果、約2割の4万アドレスから応答を収集でき、それらの機器が実際にデジタルビデオレコーダやWebカメラ、Wi-Fiルータであることを確認した[5]。これらの機器は通常のPCやサーバとは異なり、設置後のファームウェアアップデートなどの適切な運用がなされていないことが多いため、攻撃者の格好の攻撃対象となり、既に多数の機器が感染していることがわかった。また、実際に組込み機器に感染を行うマルウェアを捕獲・解析するためのハニーポットシステムを開発し観測・解析を行った結果、11の異なるCPUアーキテクチャで動作する43種のマルウェアの活動を観測し、感染した機器がDDoS攻撃などの様々な攻撃活動に悪用されることが明らかになっている[6]。

なお、我々の観測ではTelnetに対して最も多くの攻撃活動を観測しているが、Telnet以外にも組込み機器に関連した脆弱性も複数報告されており、それに応じた攻撃活動がダークネットでも観測されている。例えば、2014年1月にはSynology社製のNASに脆弱性（5000/TCP）が報告されたが、直後の2月初めに5000/TCPに対するスキャンの急激な増加が観測されている他、CiscoやNetGear社製などのルータに発見されたバックドア（32764/TCP）やNetis製ルータに存在した脆弱性（53413/TCP）など、特にウェルノウンポート以外で動作するサービスについては、脆弱性が報告される前後で観測されるスキャンが急激に

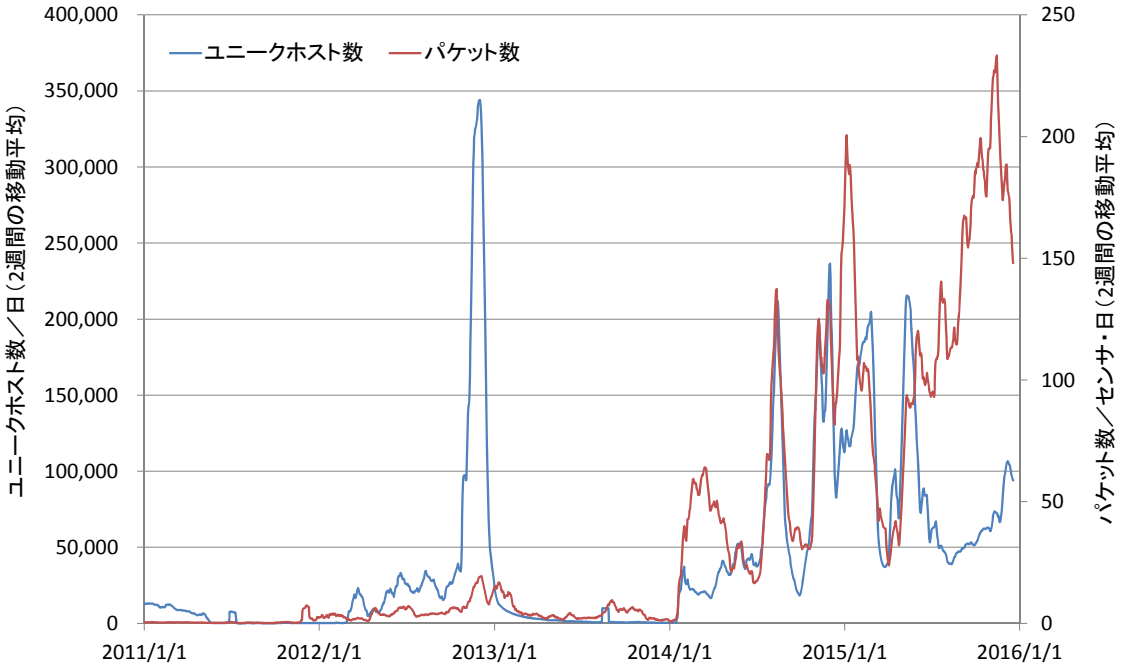

図3　23/TCP (Telnet) に関するダークネット観測統計

増加するため、こうした変化をいち早くとらえることが重要である。

4.2　DDoS 攻撃（DRDoS 攻撃）の増加

DRDoS 攻撃は DDoS 攻撃の一種であり、リフレクタ攻撃やアンプ攻撃とも呼ばれる。DRDoS 攻撃では、攻撃者はインターネット上で利用可能なリフレクタ（典型的には DNS オープンリゾルバなど）に対して送信元 IP アドレスを被害者 IP アドレスに詐称したクエリをリフレクタに対して大量に送信する。その結果、クエリサイズよりもデータサイズが増幅されたレスポンスが大量のリフレクタから被害者に送信され回線が埋め尽くされる（図 4）。こうしたリフレクタ攻撃の存在自体は古くから知られていたが、2013 年には Spamhaus に対する最大 300 Gbps にも達する大規模な DRDoS 攻撃が発生し大きな話題となった。攻撃の背景には、各家庭のホームルータに DNS オープンリゾルバ [7] となっているものが多数存在していることも挙げられる。また、DNS 以外にも NTP や SNMP など多くのプロトコルが DRDoS 攻撃に悪用可能であることが知られており、多数の攻撃事例が報告されている。DRDoS 攻撃を効率的に行うためには、事前にリフレクタの探索が必要となるため、DRDoS 攻撃の活発化に応じて、各種リフレクタ探索のスキャンも増加している。図 5 に DRDoS 攻撃で悪用されることの多い DNS（53 /UDP）、NTP（123 /UDP）、SNMP（1900 /UDP）に対するダークネット観測パケット数の推移を

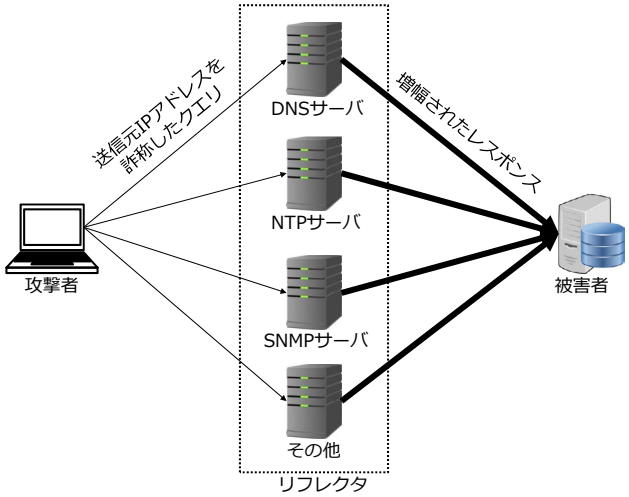

図 4　DRDoS 攻撃の概要図

示す。図 5 を見ると、DNS については 2013 年頃、NTP と SNMP については 2014 年頃からスキャンが観測されている状況がわかる。Anonymous によるイルカ漁抗議を目的とした DDoS 攻撃（OpKillingBay）や、企業のサイトに DDoS 攻撃を仕掛け攻撃を中止する代わりにビットコインの支払いを求める犯罪組織 DD4 BC（DDos for BitCoin）など、様々な目的で DDoS 攻撃が行われており、DDoS 攻撃に関連した攻撃活動をとらえることは増々重要になっている。

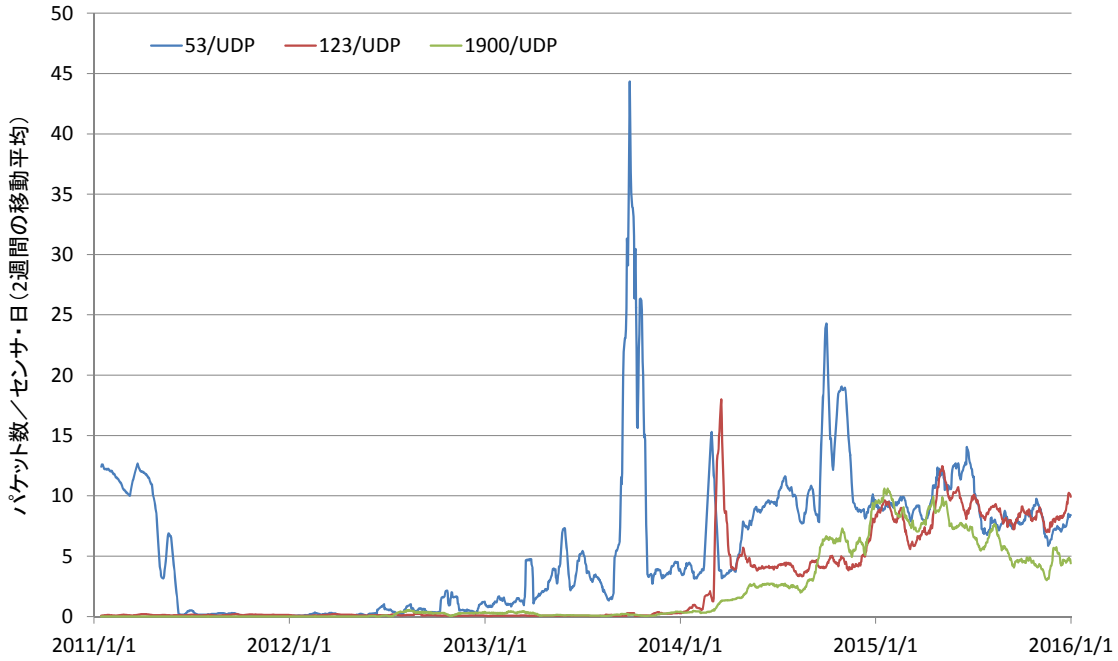

図 5　リフレクタ探索に関連した観測パケット数の統計

4.3　高速ネットワークスキャナの登場と調査系スキャン

近年、汎用的なスペックのマシンでも高速なネットワークスキャンを可能にするオープンソースのネットワークスキャナが開発されている。2013 年にミシガン大学が開発した Zmap はその中でも特に有名なスキャナであり、コネクションステートとトラッキングしないなどの各種高速化を施すことで条件が整えばわずか 45 分間でインターネットの IPv4 アドレス空間全体をスキャン可能であると報告されている。こうした高速なネットワークスキャナの存在は、セキュリティ研究を含むインターネットに関する研究を行う人間にとって有用であることは間違いないが、一方で攻撃者側もその恩恵にあずかることができる。

実際のスキャンにおける Zmap 利用の実態を把握するために、ダークネットで観測された 2015 年 6 月から 12 月の各月において観測された TCP SYN パケットのうち Zmap を用いたスキャンと推測できるトラフィックの割合を図 6 に示す。なお、Zmap で生成されたパケットか否かはヘッダ情報を基に特徴的なパケットを判定するシステム [8] を用いており、Zmap の場合デフォルト設定で IP ヘッダの ID 値に常に 54321 の値が設定されるなどの特徴を判定に用いている。図 6 を見ると、観測されている全 TCP SYN パケットのうち約 1 割前後のパケットが Zmap を用いて送信されていることがわかる。これは日単位で見ると約 1 ～ 3 千万パケットが観測されていることになり、Zmap を用いた多数のスキャンが観測されていることが明らかになった。

これらの送信元には Zmap を開発したミシガン大学も含まれており、彼らは Zmap を利用して調査目的でインターネット全域に対するスキャンを定期的に行っており、例えば OpenSSL に関する Heartbleed 脆弱性の影響を受けるサーバの把握や、インターネットに接続されている IoT 機器の把握などを行っている。近年、ミシガン大学に限らず Shodan や Shadowserver、Rapid7 など、調査目的で大規模なネットワークスキャンを行うセキュリティ関連の組織や研究機関が複数存在しており、これらの組織によるスキャントラフィックがダークネットでも多数観測され分析のノイズとして影響が出ている。そのため、分析の際にはこれらの調査目的のスキャンを適切に除外して分析を行う必要が出てきている。

5　おわりに

本稿では、2011 年から 2015 年にかけて NICTER で観測されたダークネットトラフィックに関して統計的な分析を行い、観測された特徴的な攻撃活動の変化について示した。

近年、Web を媒体とするドライブ・バイ・ダウンロード攻撃の登場や、特定の組織を執拗にねらう標的型攻撃など攻撃手法が多様化し、受動的な観測手法であるダークネット観測ではとらえられない攻撃が存在して

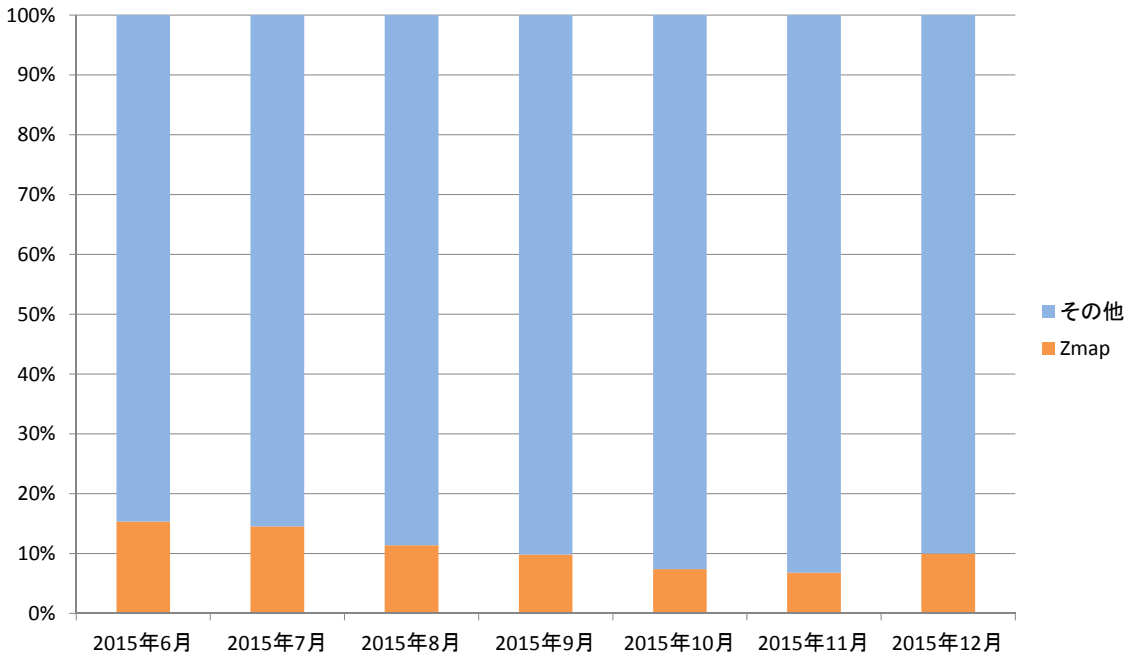

図 6　観測パケット数 (TCP SYN パケット) における Zmap パケット数の割合

いる。しかしながら我々の長期的な観測活動は、ダークネット観測で見える攻撃活動は減少するどころか、むしろ増加傾向にあり、従来からの攻撃活動に加えて新たな攻撃活動の出現もとらえていることを示しており、今後も継続的な観測と分析、その知見を活かした対策手法の研究開発が重要であると考えている。しかしその一方で、ダークネット観測だけでは攻撃活動の全体把握が困難な場合も存在するため、ハニーポットや Web クローラ、各種脆弱性情報など多種多様なサイバーセキュリティ情報を効果的に組み合わせた分析について更なる検討を進める必要がある。

【参考文献】

1 D. Inoue, M. Eto, K. Yoshioka, S. Baba, K. Suzuki, J. Nakazato, K. Ohtaka, and K. Nakao, “nicter: An Incident Analysis System Toward Binding Network Monitoring with Malware Analysis,” In WOMBAT Workshop on Information Security Threats Data Collection and Sharing, pp.58–66, 2008.

2 K. Nakao, D. Inoue, M. Eto, and K. Yoshioka, “Practical Correlation Analysis between Scan and Malware Profiles against Zero-Day Attacks Based on Darknet Monitoring,” IEICE TRANSACTIONS on Information and Systems, vol.E92-D, no.5, pp.787–798, May 2009.

3 M. Eto, D. Inoue, J. Song, J. Nakazato, K. Ohtaka, and K. Nakao, “nicter: A Large-Scale Network Incident Analysis System,” In Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS 2011), April 2011.

4 E. L. Malècot, and D. Inoue, “The Carna Botnet Through the Lens of a Network Telescope,” In Proceedings of the 6th International Symposium on Foundations and Practice of Security (FPS 2003), Oct. 2013.

5 笠間 貴弘 , 島村 隼平 , 井上 大介 ,“パッシブ観測とアクティブ観測を組み合わせた組込み機器の攻撃活動状況の把握 ,”電子情報通信学会論文誌 , vol.J99-A, no.2, pp. 94−105, 2016 年 2 月 .

6 Y. M. Pa Pa, S. Suzuki, K. Yoshioka, T. Tsutomu, T. Kasama, C. Rossow, “IoTPOT: Analysing the Rise of IoT Compromises,” In Proceedings of The 9th USENIX Workshop on Offensive Technologies (WOOT '15), Aug. 2015.

7 https://www.nic.ad.jp/ja/basics/terms/open-resolver.html

8 小出 駿 , 牧田 大佑 , 笠間 貴弘 , 鈴木 未央 , 井上 大介 , 中尾 康二 , 吉岡 克成 , 松本 勉 ,“通信プロトコルのヘッダの特徴に基づくパケット検知ツール tkiwa の実装と NICTER への導入 ,”電子情報通信学会 信学技報 , vol.115, no.334, ICSS2015-38, pp.19−24, 2015 年 11 月 .

笠間貴弘　（かさま　たかひろ）

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
研究員
博士（工学）
サイバーセキュリティ