3.3 DoS/DDoS 攻撃対策（3）～ダークネット観測網を用いたバックスキャッタ分析～

専

井上大介　中里純二　衛藤将史　中尾康二（（独）情報通信研究機構）

バックスキャッタとは

Kevin Mitnick が発信元 IP アドレスを詐称した TCP SYN Flood 攻撃を世に放ってから，およそ 20 年の歳月が過ぎようとしている．その間，同種の DoS（Denial of Service）攻撃は衰えることなく，世界中のサーバを日夜襲い続けている．

発信元 IP アドレスが無作為に詐称された DoS 攻撃は，真の発信元を隠匿するばかりでなく，攻撃を受けているサーバ（以下，被攻撃サーバ）側での発信元 IP アドレスに基づく攻撃の峻別を無力化するため，DoS 攻撃の早期検知やブロック等の対策を困難にする．

その一方で，IP アドレス詐称がなされた TCP SYN Flood 攻撃が発生すると，被攻撃サーバから TCP の SYN-ACK フラグが設定された大量のパケットがインターネットに撒き散らされる．これは，被攻撃サーバが，詐称された発信元の 1 つ 1 つに応答☆1 を行うためであり，この被攻撃サーバが送出する SYN-ACK パケットをバックスキャッタと呼ぶ．

バックスキャッタはいわば，被攻撃サーバから届く悲鳴であり，その悲鳴に注意深く耳を傾けることで，この種の DoS 攻撃の手がかりを掴むことができる．

本稿では，バックスキャッタの観測および分析について，最新の研究結果を紹介する．

☆1 TCP 3 ウェイハンドシェイクの 2 番目の通信．
☆2 2008 年に感染爆発した Conficker などが送信．

ダークネット観測網

被攻撃サーバからの悲鳴を克明に捉えるためには？
そこで用いられるのが，
ダークネット観測網である．

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．未使用の IP アドレスに対しパケットが送信されることは，通常のインターネット利用の範囲においては稀であるが，実際には相当数のパケットがダークネットに到着する．これらのパケットの多くは，ネットワークを経由して感染を広げるワーム型のマルウェアが次の感染対象を探すためのスキャンや，マルウェア同士が P2P ネットワークを確立するためのランデブー用のパケット☆2 など，インターネット上に無作為に（したがって，未使用 IP アドレスに対しても）送出される不正な活動に起因している．そして，バックスキャッタもまた，被攻撃サーバが無作為に拡散させる通信であるがゆえに，ダークネットにおいて大量に観測される．

図 -1 は情報通信研究機構で研究開発を行ってい

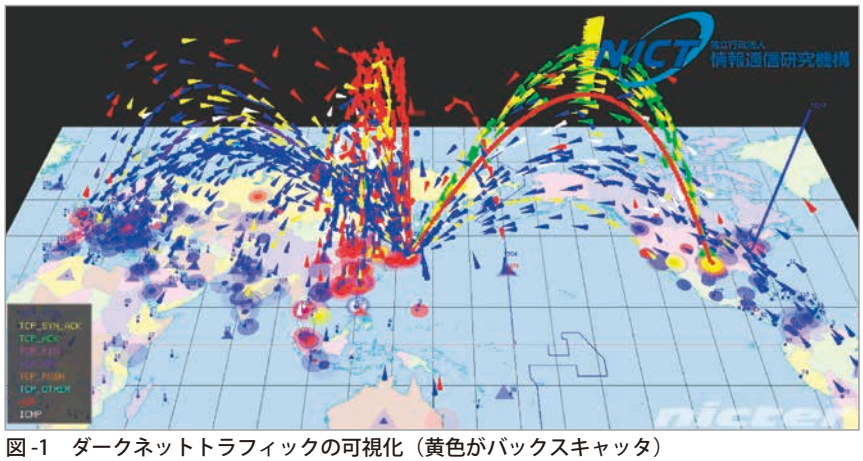

図 -1　ダークネットトラフィックの可視化（黄色がバックスキャッタ）

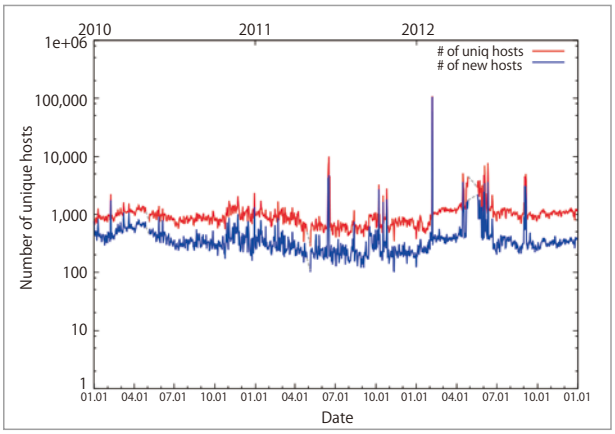

図 -2　バックスキャッタ ユニークホスト数

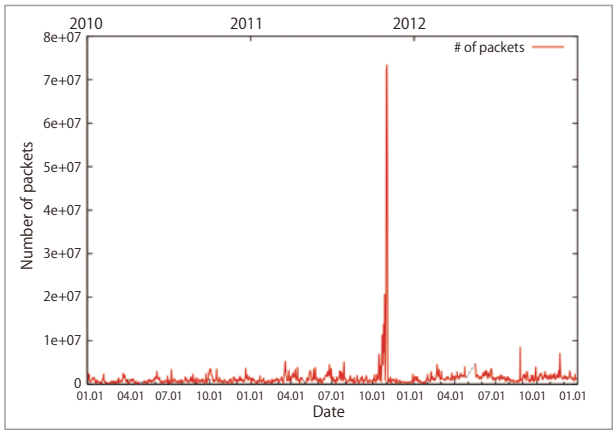

図 -3　バックスキャッタ パケット数

るインシデント分析システム nicter[1] の大規模ダークネット観測網☆3 によって観測されたパケットを，可視化エンジン Atlas 上で視覚化したものである．図中のロケット状の 3D オブジェクトのうち，黄色のものが TCP の SYN-ACK パケット，すなわちバックスキャッタである．図が示すように，米国，アジア圏，ヨーロッパ圏の国々を中心に，多くのバックスキャッタが観測されている．

バックスキャッタ長期観測

本章では，nicter によるバックスキャッタの長期観測結果を示す．ここでは，nicter のセンサのうち，クラス B（65,536 アドレス）のダークネットに設置したブラックホールセンサ☆4 による観測データを扱う．

■ ユニークホスト数の推移

図 -2 に 2010 年 1 月 1 日から 2012 年 12 月 31 日の約 3 年間に観測した，バックスキャッタ発信元ホスト数の日ごとの推移を示す（縦軸は対数軸）．

図 -2 の赤線は，ある 1 日にバックスキャッタが観測されたホストのユニーク数を表しており，3 年間を通して 1,000 ホスト前後で推移している．すなわち，IP アドレス詐称がなされた TCP SYN Flood 攻撃を受けている被攻撃サーバが，1 日に少なくとも 1,000 台（1,000 アドレス）程度観測されていることを示している．

図 -2 の青線は 2010 年 1 月 1 日以降に新たにバックスキャッタが観測されたホストのユニーク数を示しており，約 300 前後のホストが毎日新たに観測されている．一方，約 700 前後のホストは，複数の日においてバックスキャッタが観測されており，比較的長期間 TCP SYN Flood 攻撃を受けているものと推定される．

2012 年 2 月 6 日には，約 10.4 万という多数のホストから，新たにバックスキャッタを観測している．この事案では，バックスキャッタ発信元ホストの多くが同一のクラス B アドレスに属しており，発信元ポート番号は 3,389 番ポートであった．これは，特定の /16 ネットワークを中心に，Windows のリモートデスクトッププロトコル（RDP）をターゲットにした TCP SYN Flood 攻撃が行われたものと考えられる．

■ パケット数の推移

図 -3 は，前節と同様のブラックホールセンサで観測された，1 日あたりのバックスキャッタのパケット数の推移を示している（2010 年 1 月 1 日から 2012 年 12 月 31 日）．

図 -3 中のスパイクは，2011 年 11 月 1 日と 2 日の両日に観測された 7,000 万パケットを超える大規模なバックスキャッタである．これは中国に存在す

☆3　2012 年 11 月末時点で約 19 万の未使用 IPv4 アドレスで構成されている．
☆4　パケットの発信元に対し，応答を行わないセンサ．保守が容易であり大規模なダークネット観測に向く．マルウェアの感染活動の初期段階であるスキャンは観測可能であるが，それ以降の挙動を観測することはできない．

発信元ポート番号	ユニークホスト数
80	44,293
22	2,383
53	2,003
113	1,949
0	1,775

(a) 2010 年の Top5

発信元ポート番号	ユニークホスト数
80	55,180
53	7,231
139	6,063
1,863	3,225
22	2,025

(b) 2011 年の Top5

発信元ポート番号	ユニークホスト数
3,389	107,559
80	80,567
22	9,754
6,005	3,050
445	2,042

(c) 2012 年の Top5

表 -1　発信元ポート番号 Top 5 の推移

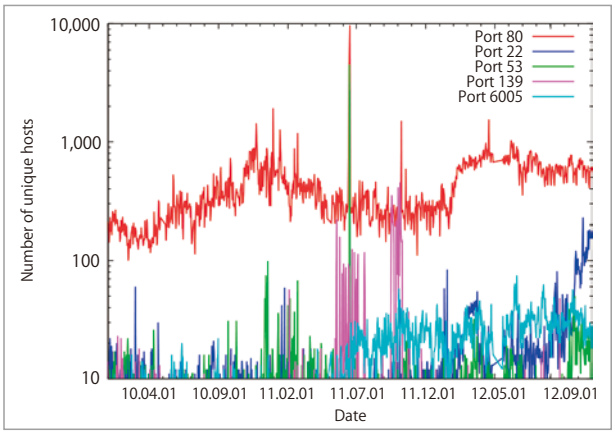

図 -4　発信元ポート番号ごとのユニークホスト数

る 1 つの IP アドレスからのバックスキャッタであった．

2010 年の 1 日あたりの平均パケット数は約 85 万パケットであったのに対し，2012 年の同パケット数は約 145 万パケットであり，バックスキャッタのパケット数は増加傾向にあることが分かる．図 -2 で見たように，バックスキャッタの発信元ホスト数に大きな増加が見られないことを勘案すると，被攻撃サーバと攻撃者の双方における処理能力向上や通信帯域の拡大に伴い，一度の DoS 攻撃活動で用いられるパケット数が増加しているものと考えられる．

■ 発信元ポート番号の推移

バックスキャッタの発信元ポート番号は，TCP SYN Flood 攻撃の送信先ポート番号と一致する．したがって，バックスキャッタの発信元ポート番号を観測することで，被攻撃サーバにおいて攻撃対象となっているサービスが分かる．

表 -1 は，2010 年～ 2012 年の 3 年間の，バックスキャッタの発信元ポート番号の Top 5 を，ユニークホスト数をもとに集計したものである．2012 年の特異的な 3,389 番ポート（RDP）を別にすれば，80 番ポート（HTTP）が支配的であり，Web サーバが攻撃対象のトップであることが分かる．次いで 22 番ポート（SSH）が常に上位に入っている．

図 -4 はバックスキャッタの発信元ポートの上位（80，22，53，139，6005）について，2010 年～ 2012 年の 1 日ごとのユニークホスト数の推移を示したものである．図より発信元ポート 80 番のバックスキャッタを送出するホスト（すなわち TCP SYN Flood 攻撃を受けている Web サーバ数）は，定常的に数百以上のオーダで遷移するとともに，2010 年は増加傾向を示している．2011 年は若干の減少傾向を示すが，2012 年前半に再度増加傾向に転じている．

2011 年 6 月 16 日には，3 年間で最大のスパイクを観測しており，発信元ポート 53 番のバックスキャッタを約 4,500 ホストから，発信元ポート 80 番のバックスキャッタも通常時の 10 倍以上の約 1 万ホストから観測している．この時期は，アノニマスによるトルコ政府への攻撃が報じられた時期と符合しており，バックスキャッタの発信元ホストの 8 割以上がトルコのホストであった．

バックスキャッタ観測事例

本章では，nicter のバックスキャッタ観測事例として，2011 年と 2012 年に発生した，アノニマスによる 2 つの攻撃活動を紹介する．

■ #OpSony

PlayStation 3 のハッキング情報を公開した George Hotz 他に対して Sony Computer Entertainment America が起こした訴訟に端を発し，2011 年 4 月にアノニマスが Sony グループに対する攻撃活動 #OpSony を開始した．図 -5 は #OpSony の際に nicter で観測したバックスキャッタを可視化エンジン Atlas 上で視覚化したものである（20 万倍速で

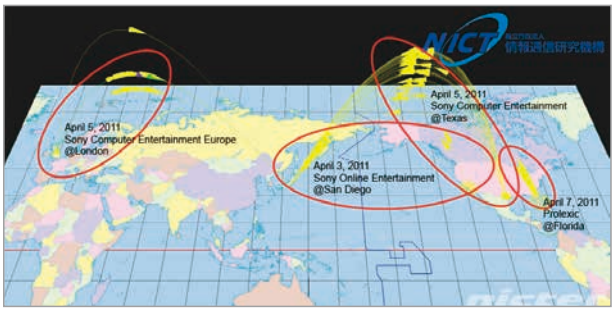

図-5　Sony グループからのバックスキャッタ

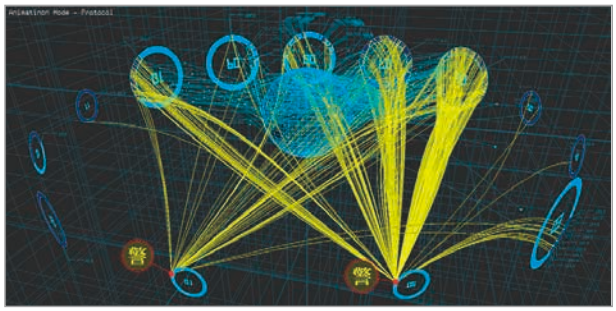
図-6　民主党サイトからのバックスキャッタ

再生）．アノニマスが IRC（Internet Relay Chat）と呼ばれるチャット上で共有する攻撃指令と同期して，2011 年 4 月 3 日に Sony Online Entertainment America（サンディエゴ）から，4 月 5 日には Sony Computer Entertainment America（テキサス）と Sony Computer Entertainment Europe（ロンドン）から，4 月 7 日には Sony が DoS 攻撃対策のために Web サイトの管理を依頼した Prolexic 社（フロリダ）からのバックスキャッタが観測された．

■ #OpJapan

日本における違法ダウンロードの罰則化を盛り込んだ改正著作権法の成立に対する抗議として，2012 年 6 月にアノニマスが日本の複数組織に対する攻撃活動 #OpJapan を開始した．図-6 は，攻撃対象の 1 つであった民主党の Web サイト☆5 からのバックスキャッタを，nicter アラートシステムの可視化エンジン DAEDALUS-VIZ[2] で視覚化したものである．図下部の 2 つのリングが，民主党の Web サイトで使用されていた 2 つの IP アドレスを表しており，その他のリングは，nicter のブラックホールセンサを設置した組織群のネットワークを表している．民主党のサイトから複数の組織にバックスキャッタ（黄色のライン）が広く拡散している様子が分かる．

バックスキャッタの分類

nicter のダークネット長期観測を通して，インターネット上に無作為に拡散しているように見えるバックスキャッタに，さまざまな特徴があることが分かってきた．このバックスキャッタの特徴は，DDoS（Distributed DoS）攻撃対策装置のシグネチャ生成や，攻撃者（攻撃集団）のプロファイリングなど，新たな DoS 攻撃対策に繋がる可能性を有している．

■ 分類で用いるフィールド

本節では，バックスキャッタの分類のために，着目するパケットのフィールドを示す．

- **送信先 IP アドレス**：バックスキャッタの送信先 IP アドレス群には，攻撃者の発信元 IP アドレスの詐称方法が特徴として表れる．
- **送信先ポート番号**：バックスキャッタの送信先ポート番号には，攻撃者の発信元ポート番号の選択方法が特徴として表れる．
- **シーケンス番号**：バックスキャッタのシーケンス番号は被攻撃サーバによって設定されるが，確認応答番号との組合せで，攻撃パケットの再送の有無が判定できる．
- **確認応答番号**：バックスキャッタの確認応答番号は，攻撃パケットのシーケンス番号に 1 を加算した値☆6 であるため，攻撃者のシーケンス番号の設定方法が特徴として表れる．

■ 分類ルール

前節で示したフィールドを組み合わせ，バックスキャッタを分類するための 11 のルールを定義する．

☆5 http://www.dpj.or.jp
☆6 TCP 3 ウェイハンドシェイクの最初の通信である SYN パケットを受信した場合，受信データサイズは 0 バイトであるため，シーケンス番号＋ 1 の確認応答番号が設定された SYN-ACK パケットが返される．

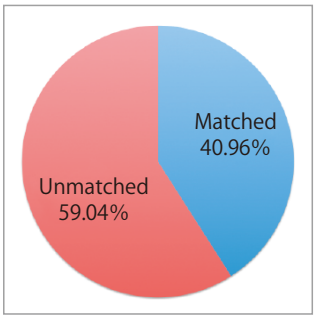

図 -7　ルール 1

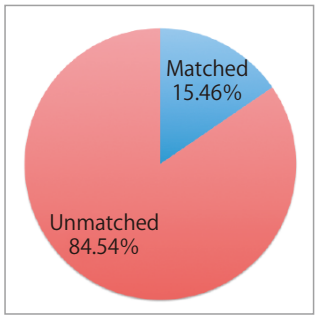

図 -8　ルール 2

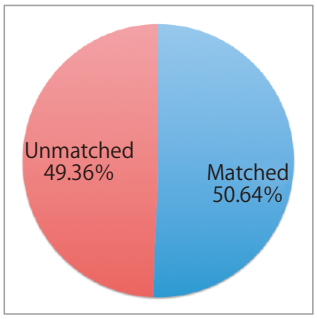

図 -9　ルール 3

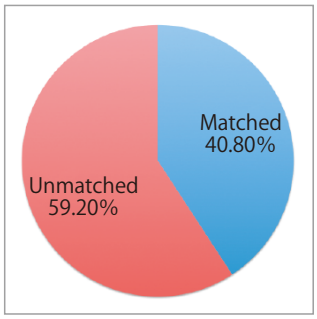

図 -10　ルール 4

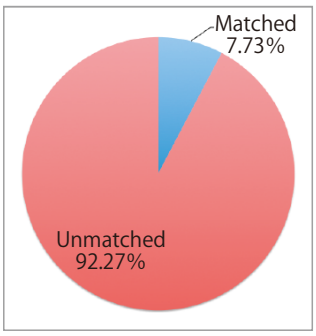

図 -11　ルール 5

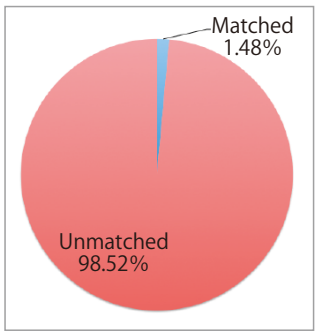

図 -12　ルール 6

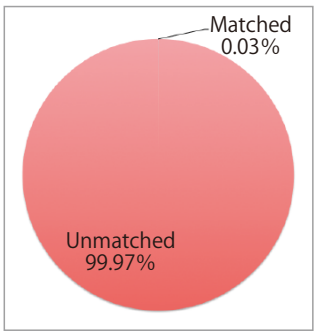

図 -13　ルール 7

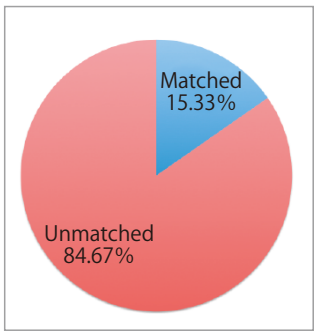

図 -14　ルール 8

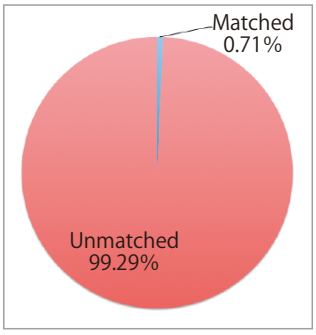

図 -15　ルール 9

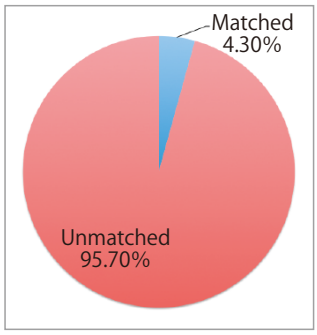

図 -16　ルール 10

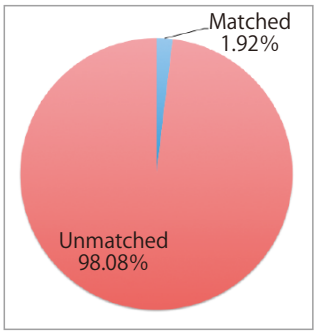

図 -17　ルール 11

これらのルールは，nicter のダークネット観測の経験から導き出されたものである．

また，各ルールを前述の /16 ダークネットの観測結果に適用した際の，適合／不適合の割合を示す（図 -7 ～図 -17）．観測期間は 2012 年 11 月の 1 カ月間とし，当該期間に初めてバックスキャッタを観測した 9,505 ホストのうち，100 パケット以上の送信が観測された 3,118 ホストを対象とした．観測期間内に同一ホストから送信されたすべてのバックスキャッタを 1 つのイベントとみなし☆7，各イベントに適合するルールを導出した（1 つのイベントが複数のルールに適合する場合もある）．なお，/16 ダークネットでは送信先 IP アドレスの第 1，第 2 オクテットは固定のため，ルール 1 とルール 2 については第 3，第 4 オクテットのみで検査を行った．

- **ルール 1（広範囲詐称型）**：バックスキャッタの送信先 IP アドレスの第 1 ～第 4 オクテットのそれぞれの値が 128 種類以上で構成されている場合，広範囲詐称型とする．
- **ルール 2（非ランダム詐称型）**：バックスキャッタの送信先 IP アドレスの第 1 ～第 4 オクテットを構成する数値の範囲が同じ場合，非ランダム詐称型とする．
- **ルール 3（特定ポート利用型）**：バックスキャッタが単一の送信先ポート番号を持つ場合（すなわち，攻撃者が単一の発信元ポートを使用している

☆7 1 つのイベントには，観測期間内の複数の時間帯に観測されたバックスキャッタが含まれている可能性がある．

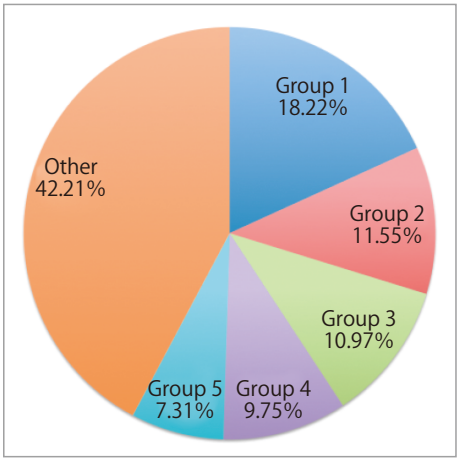

図 -18　バックスキャッタの分類結果

場合），特定ポート利用型とする．

- **ルール 4（特定確認応答番号利用型）**：バックスキャッタの確認応答番号が同一の場合（すなわち，攻撃パケットのシーケンス番号が同一の場合），特定確認応答番号利用型とする．
- **ルール 5（同一セット利用型）**：バックスキャッタのシーケンス番号以外のフィールド（送信先 IP アドレス，発信元ポート番号，送信先ポート番号，確認応答番号）が同一の場合，特定セット利用型とする．攻撃者から再送がある場合は，シーケンス番号も同一となるため，本ルールには適合しない．
- **ルール 6（第 4 オクテットランダム型）**：バックスキャッタの送信先 IP アドレスが /24 ネットワーク内にランダムに分散している場合（すなわち，/24 の範囲で IP アドレスを詐称している場合），第 4 オクテットランダム型とする．
- **ルール 7（第 3 オクテットランダム型）**：バックスキャッタの送信先 IP アドレスの第 1，第 2，第 4 オクテットが固定であり，第 3 オクテットがランダムに分散している場合，第 3 オクテットランダム型とする．
- **ルール 8（特定第 4 オクテット利用型）**：バックスキャッタの送信先 IP アドレスの第 4 オクテットの値が 128 種類の場合，特定第 4 オクテット利用型とする．
- **ルール 9（特定第 3 オクテット利用型）**：バックスキャッタの送信先 IP アドレスの第 3 オクテットの値が 128 種類の場合，特定第 3 オクテット利用型とする．
- **ルール 10（第 4 オクテット偏り型）**：バックスキャッタの送信先 IP アドレスの第 3 オクテットの値が 200 種類以上存在し，第 4 オクテットの値が 128 種類未満の場合，第 4 オクテット偏り型とする．
- **ルール 11（第 3 オクテット偏り型）**：バックスキャッタの送信先 IP アドレスの第 4 オクテットの値が 200 種類以上存在し，第 3 オクテットの値が 128 種類未満の場合，第 3 オクテット偏り型とする．

グループ	適合ルール	イベント数
グループ 1	1, 3, 4	568
グループ 2	8	360
グループ 3	なし	342
グループ 4	3, 4	304
グループ 5	1, 2, 3, 4	228

表 -2　Top 5 グループの内訳

■ 分類結果

2012 年 11 月に観測した 3,118 イベントに，上述の 11 のルールを適用し，各ルールへの適合／不適合をもとにイベントの分類を行った．その結果，イベントは 40 のグループに分類された．

図 -18 は，全 40 グループのうち，グループに含まれるイベント数の多い Top 5 を示したものである．最大のグループ 1 は 568 イベントを含み，それらのイベントはすべてルール 1，3，4 に適合している．すなわち，広範囲詐称型かつ，単一の送信先ポート番号，単一の確認応答番号を持つバックスキャッタである．

表 -2 は Top 5 グループの適合ルールの内訳と，グループに含まれていたイベント数を表している．

このように，バックスキャッタを詳細に分析することで，その拡散の仕方にさまざまな特徴があることが分かってきた．この情報をいかにインターネットサービスプロバイダ（ISP）やサイトのセキュリティ対策に繋げるかは，今後の研究課題である．

関連研究

DoS 攻撃に関する概要的な研究として，文献 3）～ 5）では，DoS 攻撃のさまざまな攻撃形態を詳細に分類し，既存の防御手法の提案に関する調査を行っている．

早くからこの分野の研究に取り組んできた Moore らは，文献 6）において，バックスキャッタを用いた DoS 攻撃検知の重要性について指摘している．ここでは，ダークネットにおいて観測されるバックスキャッタの数からインターネット全体で行われている DoS 攻撃の総数を確率的に推定する手法が提案されている．

米国ミシガン大学を中心とする研究チームは，クラス A（/8）アドレスを筆頭とする広大なダークネット空間を有しており，これを利用してダークネット観測および DoS 攻撃検知に関する一連の研究を行っている[7), 8)]．文献 7）では，ダークネット観測および分析の基礎的な手法の紹介とその効果に関する考察が行われている．さらに，文献 8）では，同研究チームが有するダークネット観測網におけるバックスキャッタと Tier-1 ISP[☆8] で収集された NetFlow[☆9] 情報の突き合わせを行い，DoS 攻撃の際の IP アドレス偽装に関する評価等を行っている．

まとめ

本稿では，nicter のダークネット観測網によるバックスキャッタの長期観測結果と，観測事例を示すとともに，バックスキャッタの分類について述べた．バックスキャッタ観測によって DoS/DDoS 攻撃を“裏手”から迅速に把握することが可能になるが，その分析結果を有効活用するためには，DoS/DDoS 攻撃を“正面”から受け止めている，ISP やサイトとの連携が必須である．

☆8 インターネットの中核に位置付けられる大手プロバイダ．
☆9 IP トラフィック情報を収集するためのプロトコル．

参考文献

1) Inoue, D., Eto, M., Yoshioka, K., Baba, S., Suzuki, K., Nakazato, J., Ohtaka, K. and Nakao, K. : nicter : An Incident Analysis System Toward Binding Network Monitoring with Malware Analysis, WOMBAT Workshop on Information Security Threats Data Collection and Sharing (WISTDCS 2008), pp.58-66 (2008).
2) Inoue, D., Suzuki, K., Suzuki, M., Eto, M. and Nakao, K. : DAEDALUS-VIZ : Novel Real-time 3D Visualization for Darknet Monitoring-based Alert System, 9th International Symposium on Visualization for Cyber Security (VizSec 2012), pp.72-79 (2012).
3) Carl, G., Kesidis, G., Brooks, R. and Rai, S. : Denial-of-service Attack-detection Techniques, Internet Computing, IEEE, Vol.10, No.1, pp.82-89 (2006).
4) Glenn, M. : A Summary of DoS/DDoS Prevention, Monitoring and Mitigation Techniques in a Service Provider Environment, SANS Institute, Vol.21, p.34 (Aug. 2003).
5) Mirkovic, J. and Reiher, P. : A Taxonomy of DDoS Attack and DDoS Defense Mechanisms, ACM SIGCOMM Computer Communication Review, Vol.34, No.2, pp.39-53 (2004).
6) Moore, D., Shannon, C., Brown, D., Voelker, G. and Savage, S. : Inferring Internet Denial-of-service Activity, ACM Transactions on Computer Systems (TOCS), Vol.24, No.2, pp.115-139 (2006).
7) Bailey, M., Cooke, E., Jahanian, F., Myrick, A. and Sinha, S. : Practical Darknet Measurement, IEEE 40th Annual Conference on Information Sciences and Systems, pp.1496-1501 (2006).
8) Mao, Z., Sekar, V., Spatscheck, O., Van Der Merwe, J. and Vasudevan, R. : Analyzing Large DDoS Attacks Using Multiple Data Sources, 2006 SIGCOMM Workshop on Large-scale Attack Defense, pp.161-168, ACM (2006).

（2013 年 2 月 18 日受付）

■井上大介　dai@nict.go.jp

2003 年横浜国立大学大学院工学研究科博士課程後期修了後，通信総合研究所（現 情報通信研究機構）に入所．2006 年より nicter の研究開発に従事．現在ネットワークセキュリティ研究所 サイバーセキュリティ研究室 室長，サイバー攻撃対策総合研究センター サイバー防御戦術研究室 室長を兼務．博士（工学）．

■中里純二（正会員）　nakazato@nict.go.jp

2006 年東海大学博士課程後期修了．同年，情報通信研究機構入所．情報セキュリティの研究を経て，2008 年より nicter の研究開発に従事．電子情報通信学会会員．博士（工学）．

■衛藤将史　eto@nict.go.jp

2005 年情報通信研究機構入所．以来，nicter プロジェクトや IPv6 セキュリティなど，情報通信セキュリティ技術の研究開発に従事．nicter プロジェクトでは主に次世代型サイバー攻撃観測プラットフォームの研究に取り組む．博士（工学）．

■中尾康二（正会員）　ko-nakao@nict.go.jp

1979 年早稲田大学卒業後，国際電信電に入社．KDD 研究所を経て，現在 KDDI 情報セキュリティフェロー，および情報通信研究機構ネットワークセキュリティ研究所 主管研究員，同機構サイバー攻撃対策総合研究センター 研究統括を兼務．ネットワークおよびシステムを中心とした情報セキュリティ技術にかかわる技術開発に従事．