2.3 DoS/DDoS 攻撃観察日記(3) ～ボットネット PushDo による SSL 接続攻撃を振り返って～

橘　喜胤　寺田真敏（日本シーサート協議会）

2010 年 2 月 3 日

多数の発信元から，443/tcp（HTTPS）ポートに対して不正な形式の SSL 接続が大量に発生するという DoS 攻撃が観測され始めた．観測事象と公開情報とをつき合わせていくと，この DoS 攻撃は，ボットネット PushDo によるものであるということが分かった．

ここで紹介する事例は，日本シーサート協議会とその加盟チームがかかわったインシデントである[1]．日本シーサート協議会は，シーサート（CSIRT：Computer Security Incident Response Team；コンピュータセキュリティにかかるインシデントに対処するための組織の総称）同士が互いに協調し，共通の問題を解決する場として，2007 年に設立された協議会である．2013 年 3 月時点で 35 チームが加盟している．今回の DoS 特集に寄せて，当時の日本シーサート協議会での情報共有状況と攻撃対象となったサイトの対応を振り返りながら紹介する．DoS 攻撃に関するニュース記事を目にすることも増えてはいるが，そのインシデントの詳細が公開されることはあまりないのが現状である．事例の 1 つとして参考になれば幸いである．

攻撃活動の概要

今回の DoS 攻撃をしかけてきたボットネット PushDo と，その攻撃手法である不正な形式の SSL 接続による DoS 攻撃（以降，不正な形式の SSL 接続攻撃）について紹介する．

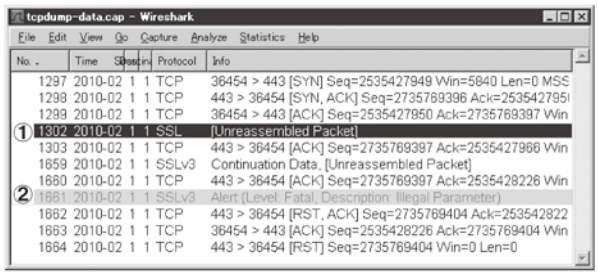
■ ボットネット PushDo とは

ボットは，指令者からの遠隔操作によって，多岐にわたる活動を実現するマルウェアの 1 つである．ボットに感染した PC はボットネットと呼ばれるネットワークを形成する．指令者は，指令サーバ経由でボットネットに制御命令を同報することで，多数のボットが命令に従って一斉に動作する．PushDo は，2007 年 1 月頃に存在が確認されたボットネットの 1 つであり，Pandex，Cutwail とも呼ばれている．2009 年の MessageLabs の報告によれば，『スパム配信用ボットネットで，180 億メール／日に達し，110 万～ 160 万ノード規模』と推定されている．また，2010 年のトレンドマイクロのレポート[2] によれば，『活動中のスパム配信用ボットネットのうち最大規模の 1 つ』と報告されている．

2010 年 8 月 25 日に，8 つのホスティングプロバイダによってボットネット PushDo の指令サーバとして特定された 30 台のうち 20 台が停止されたが，2012 年の Kindsight Security Labs の報告[3] によれば，いまだボットネットのトップ 10 の 1 つとして挙げられている状況にある．

■ 不正な形式の SSL 接続攻撃とは

PushDo がしかけてきた DoS 攻撃は，エラーが発生するような SSL の接続手順を使って，攻撃先にアクセスするというものであった．SSL の接続手順は 11 パケットの通信から構成され（図 -1），DoS 攻撃では，この接続手順が大量に繰り返されることになる．接続手順の大まかな流れは，TCP コネクション確立後に，形式が不正な SSL ネゴシエーシ



① 攻撃者⇒サーバ： 形式が不正なSSLネゴシエーションパケット
② サーバ⇒攻撃者： 形式が不正なためエラー応答し，終了する．

図 -1　不正な形式の SSL 接続

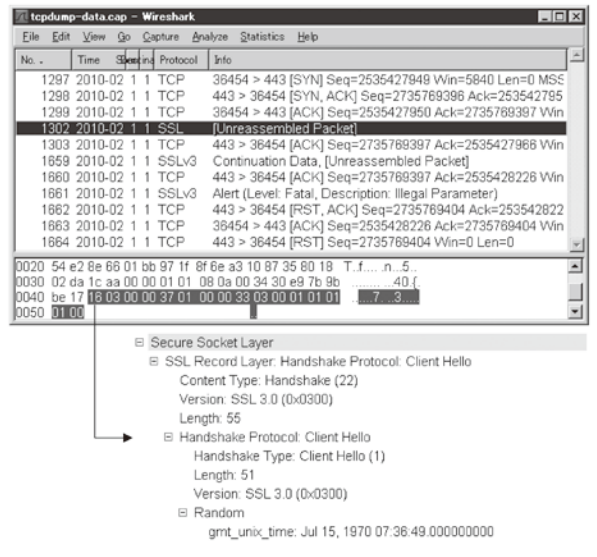


図 -2　攻撃者⇒サーバ：形式が不正な SSL ネゴシエーションパケット

ョンパケット（攻撃者⇒サーバ）（図 -2）が送信され，形式が不正なために，エラー応答パケット（サーバ⇒攻撃者）（図 -3）が返送される．

DoS 攻撃の観測中に取得した 3,000 フレームほどの通信キャプチャデータを調べてみたところ，不正な形式の SSL 接続攻撃の特徴は，次の通りであった（図 -4）．

- 11 パケットを中心に 9 ～ 12 パケットで構成
- TCP データサイズで見ると 282 ～ 283 バイト，イーサネットフレームサイズでは 540 バイト～ 680 バイト
- キャプチャデータからトラフィック量を算出すると，約 1,300pps，約 0.9Mbps（イーサネットフレームサイズ試算）

  上り（攻撃者⇒サーバ）：620pps, 0.57Mbps

  下り（サーバ⇒攻撃者）：662pps, 0.35Mbps

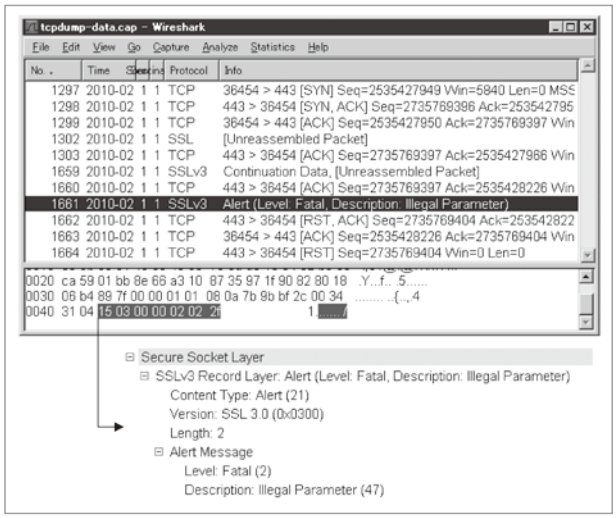


図 -3　サーバ⇒攻撃者：エラー応答パケット

■ 攻撃活動全般の経緯

攻撃活動全般の流れは，2010 年 1 月末に不正な形式の SSL 接続攻撃が始まり，5 月連休前に，この攻撃機能を備えたマルウェアの存在が顕在化し始めた．

2010 年 1 月 29 日：PushDo 443/tcp（HTTPS）ポートへの DoS 攻撃活動の開始

セキュリティの技術集団である Shadowserver から，PushDo による DoS 攻撃が開始されたことと，www.cia.gov，tips.fbi.gov など，340 カ所近くが攻撃対象になっているとの報告が公開された [4]．

2010 年 2 月 3 日：DoS 攻撃活動の活発化

IBM Internet Security Systems X-Force からも「PushDo による SSL を使用した DDoS 攻撃」に関する報告が公開されるなど，PushDo の不正な形式の SSL 接続攻撃が活発化し，国内でもいくつかの DoS 攻撃活動が観測され始めた．

2010 年 2 月 24 日：国内での発生状況の判明

jp ドメインについても 40 カ所近くが攻撃対象となっていること，この中に，日本シーサート協議会とその加盟チームがかかわったサイトが含まれていることが分かった [5]．

2010 年 4 月 28 日：DoS 攻撃を行うマルウェアに関する注意喚起

JPCERT/CC から，ガンブラー（Gumblar）などのホームページ誘導型マルウェアの中に，不正な形

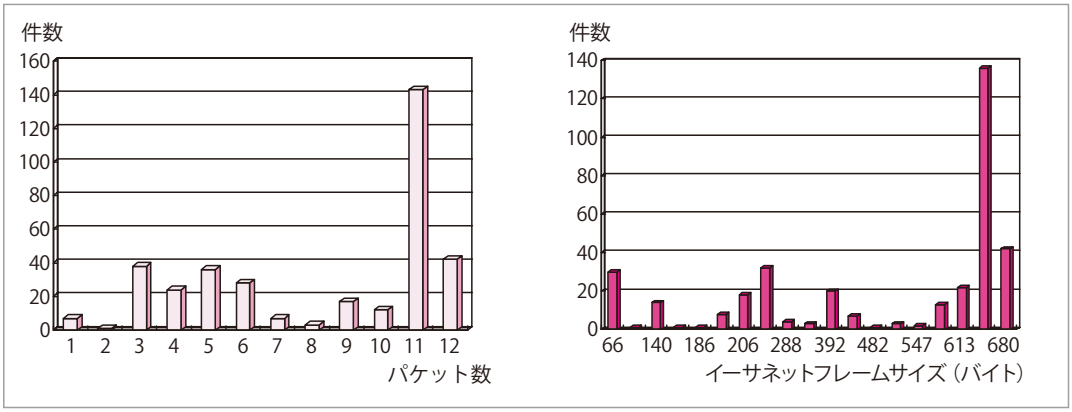


図-4　不正な形式の SSL 接続の通信パケット数とフレームサイズの分布

式の SSL 接続による DoS 攻撃を行う機能が追加されたとの注意喚起[6]が発行された．

日本シーサート協議会での対応経緯

日本シーサート協議会では，2010 年 2 月中旬に不正な形式の SSL 接続攻撃に関する情報共有を開始し，5 月連休明けに本インシデントに関する情報発信を実施した．

2010 年 2 月 10 日：情報共有の開始

日本シーサート協議会に，443/tcp（HTTPS）ポートへの SSL 接続が多数発生しているとの連絡が入った．加盟チームに問合せをしたところ，次のような関連情報を収集できた．

- PushDo というボットネットが存在し，最近 SSL を用いた DoS 攻撃をしかけている．
- 加盟チームが関与するサイトでも類似の攻撃が，ほぼ同時期から始まっている．

これらの情報から，PushDo による DoS 攻撃と観測している状況とに類似性があり，関連性が濃厚であった．しかし上述の Shadowserver から公開されていた攻撃対象リストに加盟チームが関与するサイトは含まれていなかった．

2010 年 2 月 24 日：追加情報の入手

Shadowserver から PushDo に関する追加情報を入手し，すでに公開されている攻撃対象リスト以外にも，攻撃対象先が存在することが明らかとなった．確かに，その攻撃対象リストには加盟チームが関与するサイトが含まれていた．

2010 年 4 月：情報発信に向けて

今回の不正な形式の SSL 接続攻撃は，攻撃対象サイトをダウンさせるほどの活動ではなく，また，攻撃対象リストに挙がっているサイト間に共通点があまり見受けられなかった．言い換えれば，『流れ弾 DDoS 攻撃』と呼べるインシデントであった．2010 年 2 月上旬，この表現を裏付けるような記事が CNET News に掲載されている[7]．この記事によれば，PushDo は，偽の SSL ヘッダを使用しており，ボットと指令サーバとの通信を隠蔽するために，SSL トラフィックを発生させているのではないかとしている．このような背景と流れ弾 DDoS 攻撃の数少ない事例であると考え，情報発信することを決定した．

2010 年 5 月 7 日：情報掲載

今回の不正な形式の SSL 接続攻撃を記録として残しつつ，事例として活用してもらうことを考え，加盟チームの協力を得ながら，Web サイト『2010 年 2 月上旬から始まったボットネット PushDo による SSL 接続攻撃について』を公開した．

観測日記

観測日記は，日本シーサート協議会とその加盟チームがかかわった 2 件のインシデントを，サイト視点での対応活動として紹介する．

■ サイト A の観測日記

サイト A の観測日記は，Web サーバが，443/

tcp（HTTPS）ポートを稼働させておらず，Web サーバ手前に設置した負荷分散装置が，SSL 接続を受け付ける設定であったサイトでの対応と観測事象である．

2010 年 2 月 4 日：DoS 攻撃の検知

サイトに設置していた IDS のログの解析を行っていたところ，通常よりも検知数が多いことに気がつく．特に DMZ セグメントの特定の IP アドレスに対して SSL の脆弱性を狙っていると思われる攻撃トラフィックが多数検知されていた（図 -5）．

攻撃対象となっている IP アドレスは，ファイアウォール（FW）で 443/tcp（HTTPS）のアクセスを許可しているが Web サーバはサービスを提供していないはず．けれど不思議なことに，ログを見る限り，すべてが SSL 接続エラーで終了している．DMZ セグメントの構成を把握しているサーバ担当者に確認したところ，図 -6 に示すサイト構成であることが分かった．

```
02/04-00:03:19 [**] [1:8427:9] WEB-MISC SSLv3 openssl get shared ciphers
overflow attempt [**] [Classification: Attempted Administrator Privilege Gain]
[Priority: 1] {TCP} 144.122.XX.XX:16239 -> 202.XX.XX.XX:443
```

図 -5　IDS 検知ログ

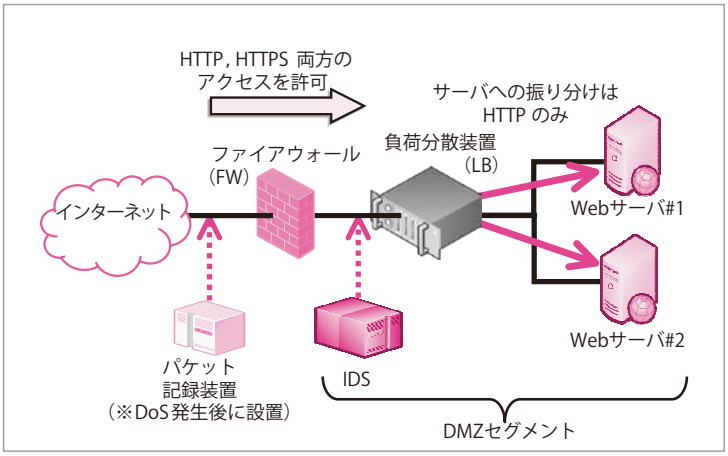


図 -6　サイト A の構成

図 -6 で分かるように，攻撃対象 IP アドレスへの HTTP アクセスは，負荷分散装置（LB）を経由してバックエンドに存在する 2 台の Web サーバのいずれかに届く．負荷分散装置は，HTTP と HTTPS の両方を処理するように設定しているが，バックエンドの Web サーバは，HTTP のみ処理する設定であった．このため，通常のブラウザでの HTTPS アクセスは，SSL 接続できるものの，すべてエラーになるわけであった．当然コンテンツは HTTP 用のみで，Web サーバも HTTPS アクセスは想定していない．

上記のような状況にもかかわらず，突然，この IP アドレス宛に，大量の SSL 接続が届き始めた理由については，まったく検討もつかない．当初は，何らかの新規の脆弱性を狙った探査活動ではないかと疑った．発信元 IP アドレスは，世界中に散らばっているので，ボットを使ったアクセスであることは間違いない．しかし，HTTPS サービスを提供していない，この Web サーバが狙われる理由も目的も分からない．DoS 攻撃の可能性も疑ったものの，帯域が数 Mbps 程度と少なめであったことと，サービスをしていない HTTPS へ DoS 攻撃を行う意図が不明であったため，DoS 攻撃と断定はできなかった．

2010 年 2 月 8 日：DoS 攻撃への対応

この攻撃への対応策として次のような選択肢が考えられた．

1. ファイアウォールでの HTTPS 遮断
2. 負荷分散装置での HTTPS 遮断
3. なにもしない

サーバ管理者と相談し，攻撃対象 IP アドレス宛の 443/tcp（HTTPS）アクセスをファイアウォールで遮断する方法である案 1 を選択した．この選択は，今回の攻撃対象の Web サーバが HTTP のみをサービスしていたからできた対処であり，幸運だったと言える．

次に，ファイアウォールのインターネット側のスイッチングハブのミラーポートにパケット記録装置をしかけ，攻撃対象 IP アドレス宛の HTTPS アクセスの推移観測を開始した．その際，今後，攻撃が拡大したときの場合を想定し，攻撃パケット数にしきい値を設け，管理者宛にアラートメール通知を飛ばす設定を行った．この追加施策の背景には，変更を少なくしたいということもあったが，実は，IDS

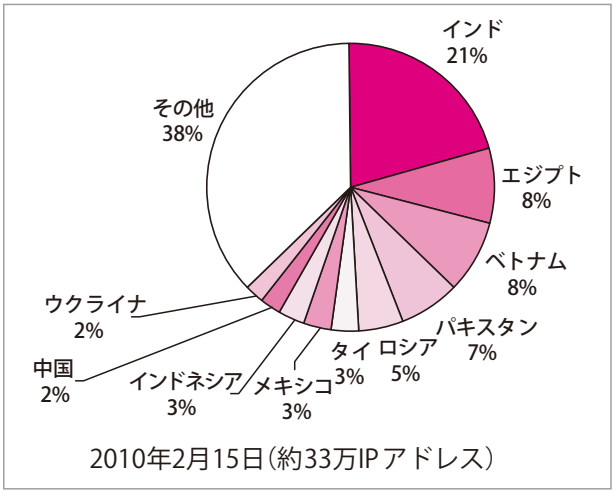


図 -7　攻撃元 IP アドレスの国別分析

の監視対象が DMZ セグメントであったために，案 1 を選択した結果，IDS を用いた状況把握ができなくなってしまったからという理由もあった．

2010 年 2 月 11 日：情報収集

日本シーサート協議会のメーリングリストで，この SSL に対する攻撃について情報を持っている加盟チームはいないかと問いかけた結果，複数の加盟チームから情報を得ることができた．観測事象と入手した情報とをつき合わせていくと，ボットネット PushDo からの攻撃であることが判明した．

2010 年 2 月～ 5 月：分析・経過観察

2 月 15 日の攻撃元 IP アドレスを国別分析してみたところ，インド，エジプト，ベトナム，パキスタンが上位を占めていた（図 -7）．またトラフィックで見ると，サウジアラビア，インドが上位に観測されていた．攻撃の規模は，ピーク時で約 2,300pps 程度で，DoS 攻撃としては小規模なものである．

長期的に観察を続けたところ，徐々に攻撃が減ってきていたが，4 月 27 日に，突然，今までで一番，大量の攻撃を検知した（図 -8）．この時点で，攻撃元 IP アドレスは，約 63 万個／日を越えており，発生当初の 2 月の 33 万個／日に比べて，大幅に増えている．攻撃元 IP アドレスの国別分析を実施したところ，トルコからの攻撃が増加していた．この後，1 週間ほど，比較的多くの攻撃を検知したものの，その後は，大きな変動はなく，徐々に攻撃は終息に向かっていった．

■ サイト B の観測日記

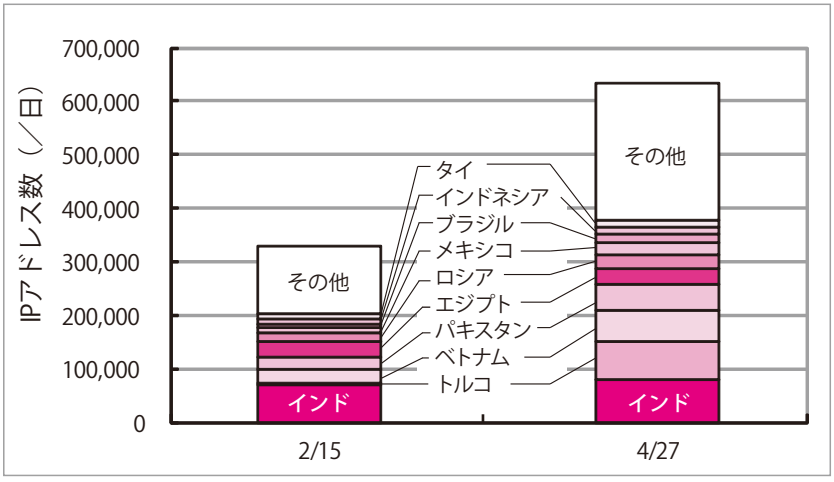
サイト B の観測日記は，Web サーバとして 80/tcp（HTTP）と 443/tcp（HTTPS）ポートを稼働させていたサイトでの対応と観測事象である．

2010 年 2 月 3 日：DoS 攻撃の検知

Web サーバの 443/tcp（HTTPS）ポートに対して，世界中の IP アドレスから不正な形式の SSL 接続が大量に発生し始めた．このとき，443/tcp（HTTPS）ポートでは，不正な形式の SSL 接続に対してネゴシエーションエラーで切断していたため，サーバへの実質的な侵害はなかったが，正規の SSL 接続ができなくなった．80/tcp（HTTP）ポートへの接続は，特に問題はなかった．Web サーバの SSL エラーログには 2 種類のエラーログが記録されていた（図 -9）．

2010 年 2 月 4 日：対策の第 1 弾

攻撃元 IP アドレスからのアクセスを遮断するブ



◂図 -8　攻撃元 IP アドレスの国別分析（2 月と 4 月の比較）

```
SSL3_GET_CLIENT_HELLO:no ciphers specified
SSL3_GET_CLIENT_HELLO:length mismatch
```

図 -9　Web サーバの SSL エラーログ

ラックリスト型フィルタ設定は一時的に有効ではあるが，ファイアウォールの設定保守がついていけず断念した．また，日本国内からのアクセスのみを許可するホワイトリスト型のフィルタ設定は，フィルタ設定が大量になることから断念した．その結果，Web サーバでの 443/tcp（HTTPS）ポート接続に対するタイムアウト時間（SSLSessionCacheTimeout）を短くするとともに，Web サーバのプロセス httpd を定期的（1 回／日）にリブートすることで SSL セッションを強制的にクリアする案を選択した（図 -10）．

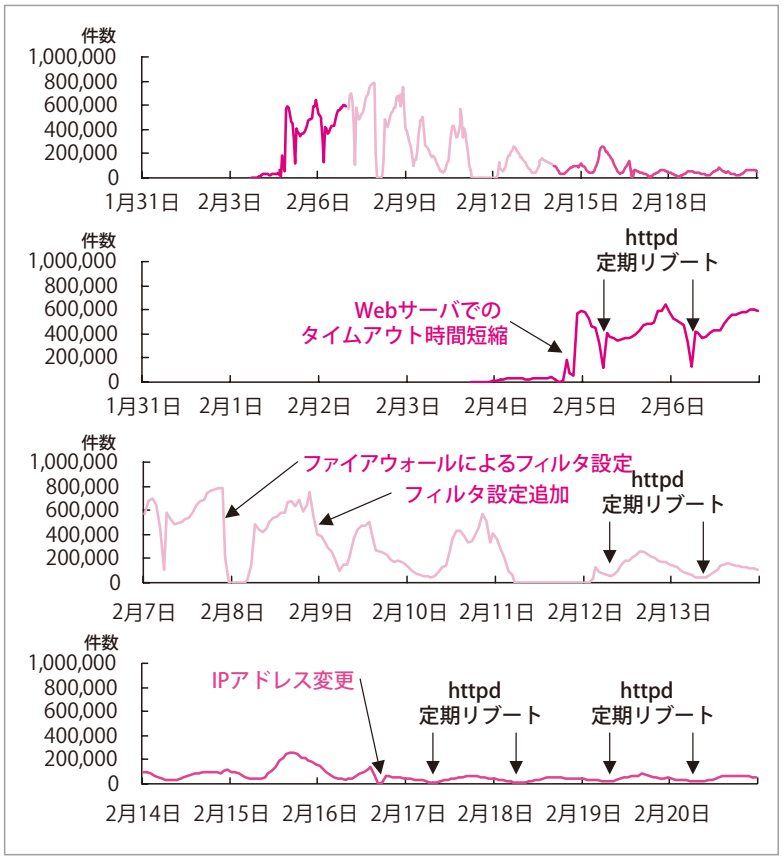


図 -10　Web サーバ SSL エラーログ件数に基づく攻撃活動の推移（／時）

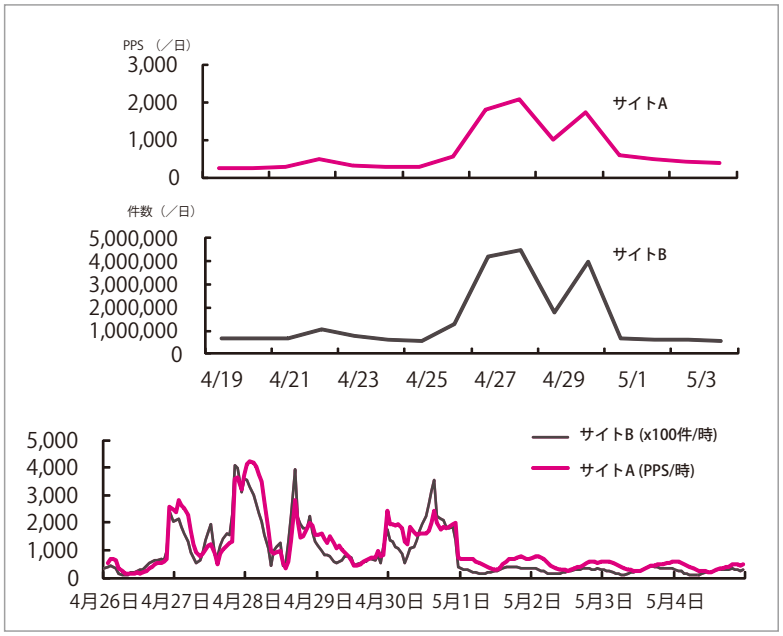


図 - 11　連休中のアクセス数の推移－上段：（／日），下段：（／時）

2010 年 2 月 16 日：対策の第 2 弾

『もしかすると，IP アドレス固定の狙い撃ち攻撃かもしれない』という望みを持ちつつ，攻撃対象から外れることを期待し，Web サーバの IP アドレスを変更してみたが，対策としては空振りに終わった．後日（2 月 24 日），攻撃対象がドメイン名で指定されているという情報で，空振りのなぞは解けた．

2010 年 5 月 7 日：観測に徹する

嵐が過ぎるのを待つという選択をしたわけであるが，待つだけでは経験値はプラスにならない．そこで，日本シーサート協議会を介して，サイト A に協力を依頼し，連休中のアクセス数を比較することを試みることにした．日単位で見た場合，両者のアクセス数の推移は似ている（図 -11 上段）．多数のボットが命令に従って制御されていることを垣間見ることができる．さらに，時間単位で見てみると，アクセス数の推移全体としては似ているが，多少のズレが見られる（図 -11 下段）．これは，攻撃元として利用されているボットネットのノードが異なることによる稼働の時差などが考えられる．なお，サイト B 側では運用上，攻撃元 IP アドレスの記録を断念していたので，攻撃元 IP アドレスの比較結果を提示することができない．残念である．

エピローグ

2012 年末現在，ボットネット PushDo からの不正な形式の SSL 接続攻撃は止まっているようである．しかし，いつ再発するか分からない．また，今回，紹介した事例では，攻撃者の意図は，はっきりとは分かってはいない．

この事例は，遠くで戦争をしていて，自分には関係ないと思っていたら，突然その流れ弾がとんできたようなものと感じている．自分の運営するサイトがこのような DoS 攻撃に遭遇する確率は低いかもしれないが，明日，出会ったとしてもまったく不思議ではない．もしも自分の運営するサイトに，今回のような流れ弾がとんできたときに，どういう対応が可能かどうか，それに備えて，どういう準備をしておくべきかを考えてみる機会になれば幸いである．

参考文献

1) 日本シーサート協議会 : 2010 年 2 月上旬から始まったボットネット PushDo による SSL 接続攻撃について，http://www.nca.gr.jp/2010/pushdo-ssl-ddos/
2) トレンドマイクロ : ＜ TrendLabs Report ＞「Pushdo」の脅威に関する主要なファクターとその防衛手段，http://blog.trendmicro.co.jp/archives/2852
3) InfoWorld : The baddest botnets of 2012, http://www.infoworld.com/slideshow/71263/the-baddest-botnets-of-2012-205739
4) Shadowserver : Pushdo DDoS'ing or Blending In?, http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20100129
5) マイクロソフト : TrojanDownloader : Win32/Cutwail.AZ, http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=TrojanDownloader%3AWin32%2FCutwail.AZ
6) JPCERT/CC : Alert 2010-04-28 : いわゆる Gumblar ウイルスによってダウンロードされる DDoS 攻撃を行うマルウェアに関する注意喚起，http://www.jpcert.or.jp/at/2010/at100011.txt
7) C|Net : Botnet Sends Fake SSL Pings to CIA, PayPal, Others, http://news.cnet.com/8301-27080_3-10445337-245.html

（2013 年 2 月 12 日受付）

■橘　喜胤　tachibana238@oki.com

丸紅 OKI ネットソリューションズ（株）インテグレーション本部セキュリティセンタ長／ OKI-CSIRT PoC．CSIRT 業務で主にネットワークセキュリティの監視を行う．2008 年より日本シーサート協議会運営委員．

■寺田真敏（正会員）　masato.terada.rd@hitachi.com

（株）日立製作所横浜研究所 主管研究員／ Hitachi Incident Response Team チーフコーディネーションデザイナ．コンピュータネットワーク，ネットワークセキュリティの研究開発に従事．JPCERT コーディネーションセンター専門委員，（独）情報処理推進機構研究員，Telecom-ISAC Japan 運営委員，日本シーサート協議会の副運営委員長を務める．