IIJ
Internet Initiative Japan

Internet Infrastructure Review Vol.24

August 2014

インフラストラクチャセキュリティ

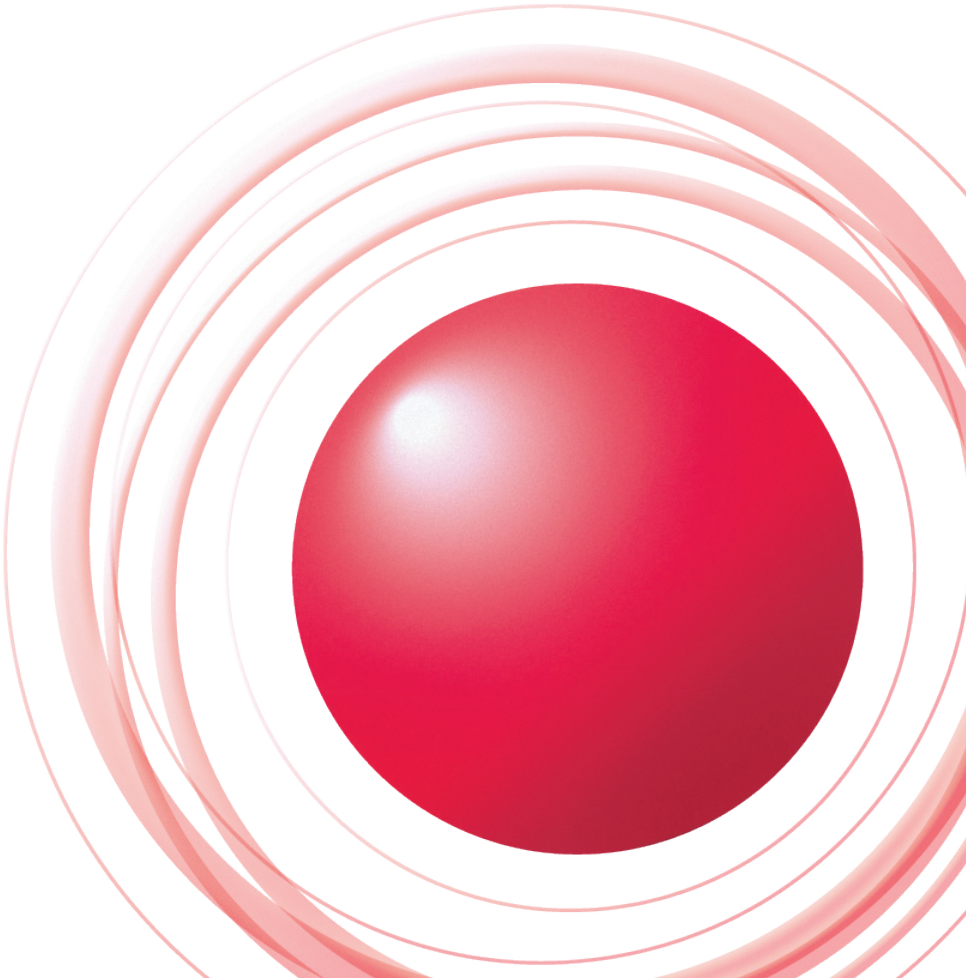
OpenSSLの脆弱性

ブロードバンドトラフィックレポート

この1年でトラフィック量は着実に増加、HTTPSの利用が拡大

技術トレンド

DNSを取り巻く環境



Internet Infrastructure Review Vol.24 August 2014

■IIJホームページ(http://www.iij.ad.jp/company/development/report/iir/)に、最新号及びバックナンバーのPDFファイルを掲載しております。併せてご参照ください。

エグゼクティブサマリ

2014年4月8日に、OpenSSLで発見された脆弱性の概要と、それに対する対応を呼びかけるセキュリティアドバイザリが公開され、様々な事業者が対応に追われました。OpenSSLは、インターネットショッピングやインターネットバンキングなどで個人情報や機密情報を暗号化してやりとりする際に用いられる、SSLという方式を実装したオープンソースソフトウェアで、UNIX系の環境で、広範囲で利用されているものです。今回見つかった脆弱性は、遠隔地からサーバ上の比較的大規模なメモリ領域にアクセスできるというもので、悪用すると、パスワードや秘密鍵などを簡単に盗みだせるため、その問題の深刻さから、Heartbleed(心臓出血)という呼び名が付けられています。

また、7月には教育関連事業を営む大手企業で、大規模な顧客情報の漏えい事件が発生しています。こちらは派遣社員が顧客の個人情報を持ち出して、何らかの方法でいわゆる名簿業者に売り渡した事件ですが、情報漏えいを起こしてしまった企業は総額200億円の補償を行う準備をすると表明しました。この額は当該企業の今期最終利益見込額に匹敵する額だそうですが、企業による顧客の個人情報管理の責任は大きく、もし万一、情報漏えい事件が起こった場合に被る損失は、企業経営に相当なインパクトを与えてしまうものになっています。

本レポートは、このような状況の中で、IIJがインターネットというインフラを支え、お客様に安心・安全に利用し続けていただくために継続的に取り組んでいる様々な調査・解析の結果や、技術開発の成果、ならびに、重要な技術情報を定期的にとりまとめ、ご提供するものです。

「インフラストラクチャセキュリティ」の章では、2014年4月から6月までの3ヵ月間に発生した主なインシデントを時系列に並べ、分類し、月ごとに概要をまとめると共に、期間全体での統計と解析結果をご報告します。また、対象期間中のフォーカスリサーチとして、4月8日に公開されたOpenSSLの脆弱性についての解説や、国内金融機関の認証情報を窃取するマルウェア「vawtrak」の解析結果と対策について、及び、クラウドの安全性確認と監査制度についてそれぞれ解説します。

「ブロードバンドトラフィックレポート」の章では、IIJが運用しているブロードバンド接続サービスの、2007年から7年間の月平均トラフィックの推移を解析し、長期的なブロードバンドトラフィックの傾向についての分析結果を報告します。更に、2014年5月26日から6月1日までの1週間分のトラフィックデータを分析し、前回行った2013年6月3日から6月9日までの分析結果と比較し、この1年間のトラフィック傾向の変化について詳細な解析を行い、報告します。

「技術トレンド」の章では、インターネットの重要なサービスの1つであるDNSを取り巻く環境の最新動向について解説します。特に、近年のTLDの追加で顕在化した名前衝突の問題や、コンテンツ配信事業者などが行っているDNSを用いた通信制御の実際と課題、そして、DNSに対する攻撃の現状と対策について詳しく解説します。

IIJでは、このような活動を通じて、インターネットの安定性を維持しながらも、日々改善し発展させて行く努力を続けております。今後も、お客様の企業活動のインフラとして最大限に活用していただくべく、様々なソリューションを提供し続けて参ります。

執筆者:

浅羽 登志也(あさば としや)
株式会社IIJイノベーションインスティテュート 代表取締役社長。株式会社ストラトスフィア 代表取締役社長。1992年、IIJの設立と共に入社し、バックボーンの構築、経路制御、国内外ISPとの相互接続などに従事。1999年より取締役、2004年より取締役副社長として技術開発部門を統括。2008年6月に株式会社IIJイノベーションインスティテュートを設立、同代表取締役社長に就任。2012年4月に株式会社ストラトスフィアを設立、同代表取締役社長に就任。

OpenSSLの脆弱性

**今回は、続けて発見され大きな影響を及ぼしたOpenSSLの脆弱性、
オンラインバンクなどの認証情報を盗み出すマルウェアvawtrak、
クラウドコンピューティングのセキュリティに関する監査制度について解説します。**

1.1 はじめに

このレポートは、インターネットの安定運用のためにIIJが取得した一般情報、インシデントの観測情報、サービスに関連する情報、協力関係にある企業や団体から得た情報を元に、IIJが対応したインシデントについてまとめたものです。今回のレポートで対象とする2014年4月から6月までの期間では、前回の期間に続いてAnonymousなどのHacktivismによる攻撃が複数発生しています。また、中間者攻撃により暗号化通信の間に割り込まれるOpenSSLの脆弱性が新たに発見され、広い範囲の影響がありました。更に、CDN事業者のサーバに設置されたコンテンツが改ざんされたことから、国内の複数のWebサービスにおいて利用者をマルウェア感染に誘導してしまう事件が発生しました。6月には香港の電子投票システムやオンラインゲームに対して、大規模なDDoS攻撃が発生しています。このように、インターネットでは依然として多くのインシデントが発生する状況が続いています。

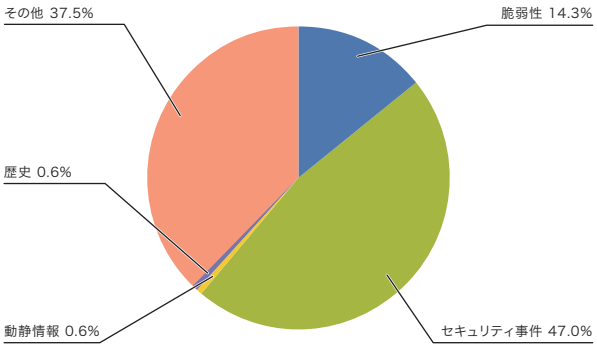


図-1 カテゴリ別比率(2014年4月～6月)

1.2 インシデントサマリ

ここでは、2014年4月から6月までの期間にIIJが取り扱ったインシデントと、その対応を示します。まず、この期間に取り扱ったインシデントの分布を図-1に示します[*1]。

■ Anonymousなどの活動

この期間においても、Anonymousに代表されるHacktivistによる攻撃活動は継続しています。様々な事件や主張に応じて、多数の国の企業や政府関連サイトに対するDDoS攻撃や情報漏えい事件が発生しました。4月にはイスラエルの複数の政府関連サイトに対し、Web改ざんや情報漏えいの被害が発生しています(OpIsrael)。同じく4月にはインドとパキスタンの間でも相互に攻撃が行われています。5月にはフィリピンと中国の間で発生している領土問題に関連して、Web改ざんやDDoS攻撃などが発生しており、特に中国政府やその関連機関に対する攻撃は現在も継続しています(OpChina)。同様に、中国とベトナムとの間でもWeb改ざんや情報漏えい、DDoS攻撃などが相互で発生しています。6月にはブラジルで開催されたサッカーのFIFAワールドカップに関連してブラジルの政府機関やTV局など複数のWebサイトに対する攻撃が発生しています。ワールドカップ関連では、そのスポンサー企業などに対する攻撃なども計画されましたが、あまり大規模な攻撃とはなりませんでした。これ以外にも世界中の各国政府とその関連サイトに対して、AnonymousなどのHacktivistによる攻撃が継続して行われました。また、Syrian Electronic Armyを名乗る何者かによるSNSアカウントの乗っ取りやWebサイト改ざんも継続して発生しており、被害を受けた企業にはThe Wall Street JournalやReutersなどの報道機関のアカウントも含まれていました。

*1 このレポートでは、取り扱ったインシデントを、脆弱性、動静情報、歴史、セキュリティ事件、その他の5種類に分類している。
脆弱性:インターネットや利用者の環境でよく利用されているネットワーク機器やサーバ機器、ソフトウェアなどの脆弱性への対応を示す。
動静情報:要人による国際会議や、国際紛争に起因する攻撃など、国内外の情勢や国際的なイベントに関連するインシデントへの対応を示す。
歴史:歴史上の記念日などで、過去に史実に関連して攻撃が発生した日における注意・警戒、インシデントの検知、対策などの作業を示す。
セキュリティ事件:ワームなどのマルウェアの活性化や、特定サイトへのDDoS攻撃など、突発的に発生したインシデントとその対応を示す。
その他:イベントによるトラフィック集中など、直接セキュリティに関わるものではないインシデントや、セキュリティ関係情報を示す。

■ 脆弱性とその対応

この期間中では、Microsoft社のWindows[*2]、Internet Explorer[*3][*4][*5][*6]、Office[*7][*8][*9]などで修正が行われました。また、Adobe社のAdobe Flash Player、Adobe Reader及びAcrobatでも修正が行われました。Oracle社のJava SEでも四半期ごとに行われている更新が行われ、多くの脆弱性が修正されました。これらの脆弱性のいくつかは修正が行われる前に悪用が確認されています。

サーバアプリケーションでは、データベースサーバとして利用されているOracleを含むOracle社の複数の製品で四半期ごとに行われてる更新が提供され、多くの脆弱性が修正されました。また、DNSサーバのBINDでは、特別に作成されたDNSリクエストにより、namedが異常終了する脆弱性が見つかり、修正されました。

暗号処理ライブラリのOpenSSLについても、秘密鍵などの機微なデータが漏えいする可能性がある脆弱性や、MITM攻撃が可能な脆弱性が見つかり[*10]、修正されました。特に、前者の脆弱性についてはHeartbleedと呼ばれ、IPAなど複数の機関から注意喚起が行われています。また、実際にこの不具合を悪用した攻撃が複数発生しました。詳細については「1.4.1 OpenSSLの脆弱性」も併せてご参照ください。OpenSSLについては以前から深刻な脆弱性がいくつか発見されていますが、このような広く利用されているライブラリでは、脆弱性が見つかったときの影響が広範囲に及びます。そのため、OpenSSLのような重要度の高いオープンソースプロジェクトを支援するCore Infrastructure Initiative[*11]が設立されたり、OpenSSLを元に、よりセキュアな実装を目指したLibreSSLプロジェクト[*12]が立ち上がるなど、複数の問題解決に向けた活動が行われています。

WebアプリケーションフレームワークのApache Strutsでも、3月に修正されたClassLoaderが操作可能な脆弱性について、修正が不十分だったことから再度修正が行われました。この脆弱性については、既に2013年にサポートが終了しているApache Struts1についても影響があることが判明したことから、複数のWebサイトで一時的にサービスを停止して修正を行うなどの対応が行われました。更に、実際に脆弱性を悪用した攻撃が複数確認されています[*13]。

■ なりすましによる不正ログイン

この期間でも、昨年から多数発生しているユーザのIDとパスワードを狙った試みと、取得したIDとパスワードのリストを使用したと考えられる、不正ログインによるなりすましの試みが継続しています。携帯電話のユーザサポートサイト、インターネット通販サイト、ゲームサイト、SNSなど様々なサイトでIDとパスワードの組み合わせリストを利用したと考えられる、不正なログインの試みが行われる事件が多く発生しています。このうちのいくつかの事件では、サイト

---

*2 「マイクロソフト セキュリティ情報 MS14-025 - 重要 グループ ポリシー基本設定の脆弱性により、特権が昇格される (2962486)」(https://technet.microsoft.com/ja-jp/library/security/ms14-025.aspx)。
*3 「マイクロソフト セキュリティ情報 MS14-018 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (2950467)」(https://technet.microsoft.com/ja-jp/library/security/ms14-018.aspx)。
*4 「マイクロソフト セキュリティ情報 MS14-021 - 緊急 Internet Explorer 用のセキュリティ更新プログラム (2965111)」(https://technet.microsoft.com/ja-jp/library/security/ms14-021.aspx)。
*5 「マイクロソフト セキュリティ情報 MS14-029 - 緊急 Internet Explorer 用のセキュリティ更新プログラム (2962482)」(https://technet.microsoft.com/ja-jp/library/security/ms14-029.aspx)。
*6 「マイクロソフト セキュリティ情報 MS14-035 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (2969262)」(https://technet.microsoft.com/ja-jp/library/security/ms14-035.aspx)。
*7 「マイクロソフト セキュリティ情報 MS14-024 - 重要 Microsoft コモン コントロールの脆弱性により、セキュリティ機能のバイパスが起こる (2961033)」(https://technet.microsoft.com/ja-jp/library/security/ms14-024.aspx)。
*8 「マイクロソフト セキュリティ情報 MS14-017 - 緊急 Microsoft Word および Office Web Apps の脆弱性により、リモートでコードが実行される (2949660)」(https://technet.microsoft.com/ja-jp/library/security/ms14-017.aspx)。
*9 「マイクロソフト セキュリティ情報 MS14-034 - 重要 Microsoft Word の脆弱性により、リモートでコードが実行される (2969261)」(https://technet.microsoft.com/ja-jp/library/security/ms14-034.aspx)。
*10 詳細については、次の発見者である株式会社レピダム 菊池氏の記事も参照のこと。「CCS Injection Vulnerability」(http://ccsinjection.lepidum.co.jp/ja.html)。
*11 詳細については、次のLinux Foundation.のBlogを参照のこと。「Core Infrastructure Initiative の速やかな進行」(http://www.linuxfoundation.jp/news-media/blogs/browse/2014/06/jp_announcing-rapid-progress-core-infrastructure-initiative)。
*12 LibreSSL(http://www.libressl.org/)。
*13 例えば、次の警察庁の発表などを参照のこと。「Apache Struts2 の脆弱性を狙ったアクセスの検知について 」(http://www.npa.go.jp/cyberpolice/detect/pdf/20140427.pdf)。

4月のインシデント

1 他 **1日**：一般社団法人JPCERTコーディネーションセンターは、脆弱性対策情報ポータルサイトであるJVNにおける脆弱性の深刻度の評価尺度表示を、それまでの独自評価から、共通脆弱性評価システム（CVSS：Common vulnerability scoring system）とすることを公表した。
「JVN が脆弱性の深刻度評価尺度表示に国際標準の共通脆弱性評価システム（CVSS）を採用」（https://www.jpcert.or.jp/pr/2014/PR20140401-jvn.pdf）。

2 3 他 **2日**：総務省より、クラウドサービス提供事業者が実施すべきセキュリティ対策や利用者との間で取り決めるべき合意事項のひな形などを示した「クラウドサービス提供における情報セキュリティ対策ガイドライン」が公表された。
「クラウドサービス提供における情報セキュリティ対策ガイドラインの公表」（http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000073.html）。

4 5 脆 **8日**：OpenSSLのTLS Heartbeat拡張処理の不具合により、メモリ上の情報が第三者に漏えいする脆弱性（CVE-2014-0160）が発見され、修正された。
詳細については次の解説も参照のこと。"The Heartbleed Bug"（http://heartbleed.com/）。

6 7 8 脆 **8日**：不特定のホストから送られた通信により、古いファームウェアのルータが再起動したりハングアップするなどの事象が報告された。
例えば、ヤマハ株式会社から次のアナウンスが行われている。「インターネットからの攻撃によるヤマハルーターのリブート等について」（http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/attack-from-internet-201404.html）。

8 9 脆 **9日**：Microsoft社は、2014年4月のセキュリティ情報を公開し、MS14-017とMS14-018の2件の緊急と2件の重要な更新をリリースした。
「2014 年 4 月のマイクロソフト セキュリティ情報の概要」（https://technet.microsoft.com/ja-JP/library/security/ms14-apr）。

9 10 他 **9日**：Microsoft社は、Windows XP、Microsoft Office 2003、Internet Explorer6のサポートを終了した。
「Windows XP と Office 2003 のサポートを終了させていただきました」（http://www.microsoft.com/ja-jp/windows/lifecycle/xp_eos.aspx）。

11 12 13 他 **13日**：Google社は、AndroidのVerify apps機構を強化し、インストールしたアプリについてもセキュリティ上の問題がないか、常時監視する機構の提供を開始した。
詳細については次のGoogle Android Official Blogを参照のこと。"Expanding Google's security services for Android"（http://officialandroid.blogspot.jp/2014/04/expanding-googles-security-services-for.html）。

13 14 脆 **14日**：Android版Adobe Reader Mobileに、リモートから任意のコード実行の可能性がある脆弱性が発見され、修正された。
「APSB14-12: Adobe Reader Mobile用のセキュリティアップデート公開」（http://helpx.adobe.com/jp/security/products/reader-mobile/apsb14-12.html）。

15 16 脆 **15日**：JPRSは、ソースポートランダマイゼーションが有効でないキャッシュDNSサーバに対するキャッシュポイズニング攻撃が増加しているとして注意喚起を行った。
「（緊急）キャッシュポイズニング攻撃の危険性増加に伴うDNSサーバーの設定再確認について」（http://jprs.jp/tech/security/2014-04-15-portrandomization.html）。

17 18 脆 **15日**：Oracle社はOracleを含む複数製品について、四半期ごとの定例アップデートを公開し、Java SEの37件の脆弱性を含む合計104件の脆弱性を修正した。
"Oracle Critical Patch Update Advisory - April 2014"（http://www.oracle.com/technetwork/topics/security/cpuapr2014-1972952.html）。

19 20 セ **15日**：カナダ歳入庁のWebサイトに対して、OpenSSLの脆弱性（CVE-2014-0160）を悪用した攻撃が発生し、納税者およそ900人分の社会保障番号が漏えいしたことを発表した。なお、4月17日に学生が容疑者として逮捕された。
詳細については次のカナダ歳入庁の公式発表を参照のこと。"Notice - Heartbleed bug vulnerability"（http://www.cra-arc.gc.ca/gncy/sttmnt2-eng.html）。

21 22 セ **16日**：国立感染症研究所は、Webメールの管理者を騙ったメールによって、メールアカウントのユーザ名とパスワードが盗取され、迷惑メールが送信されたことを公表した。
「国立感染症研究所のメールアカウントの不正利用と迷惑メール送出について」（http://www.nih.go.jp/niid/ja/maintenance/4575-incidence140416.html）。

23 24 他 **22日**：米国立標準技術研究所（NIST）は、セキュリティ上の懸念が示されている擬似乱数生成アルゴリズム Dual_EC_DRBGについて、SP800-90/90Aから削除するドラフトを提示した。
"NIST Removes Cryptography Algorithm from Random Number Generator Recommendations"（http://www.nist.gov/itl/csd/sp800-90-042114.cfm）。

25 26 27 脆 **24日**：Apache Struts2の脆弱性（CVE-2014-0094）の修正に不十分なところがあり、第三者から特定の操作が可能となる脆弱性（CVE-2014-0112）（CVE-2014-0113）が見つかり、修正された。
この問題については、例えば4月17日にIPAより、CVE-2014-0094に対する注意喚起が行われていたが、その後、更新が行われて本脆弱性も含んだ注意喚起となっている。詳細については「Apache Struts2 の脆弱性対策について(CVE-2014-0094)(CVE-2014-0112)(CVE-2014-0113)」（http://www.ipa.go.jp/security/ciadr/vul/20140417-struts.html）を確認のこと。

28 29 脆 **28日**：Microsoft社は、Internet Explorerの複数のバージョンにリモートでコードが実行可能な未修正の脆弱性があることを公表した。
「マイクロソフト セキュリティ アドバイザリ 2963983　Internet Explorer の脆弱性により、リモートでコードが実行される」（https://technet.microsoft.com/ja-jp/library/security/2963983）。

30 脆 **29日**：Adobe Flash Playerに、不正終了や、任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「APSB14-13: Adobe Flash Player用のセキュリティアップデート公開」（http://helpx.adobe.com/jp/security/products/flash-player/apsb14-13.html）。

［ 凡 例 ］ 脆 脆 弱 性　セ セキュリティ事件　動 動 静 情 報　歴 歴　史　他 そ の 他

※日付は日本標準時

上のポイントを他サービスのギフトポイントに不正に交換されるなどの被害も発生しています。また、メッセージングアプリのアカウントが不正利用された事件では、乗っ取ったアカウントから友人になりすまして、メッセージを送信し、電子マネーの購入を持ちかけるなどの手法が取られるケースが確認されています。このように、IDとパスワードの組み合わせリストを利用したと考えられる不正アクセスは継続しており、自分が利用しているIDとパスワードの管理について見直すことや、最新の手口を知っておくなどの注意が、引き続き必要な状況です。

■ Web改ざんと正規のソフトウェアを狙った攻撃の増加

この期間では、Webサイトの改ざんにより、不正なソフトウェアへ誘導される事件が多く発生しました。5月には、CDNサービスのサーバに不正侵入されたことによって、複数の企業サイトが改ざんされました。この事件では、別のサイトに誘導されて不正なソフトウェアのインストールが行われただけでなく、サービスを利用していた企業が置いていたアップデートファイルなどの正規のコンテンツが改ざんされ、マルウェアを含んだファイルを利用者にインストールさせようとしていたことも判明しています。同様の事例としては、産業用制御システムの正規ソフトウェアの配布元を改ざんしてマルウェアに感染させる事例[*14]が報告されています。また、6月には広告配信サービスからAdobe Flash Playerダウンロードサイトを騙る悪意あるWebサイトへ誘導し、不正なプログラムのダウンロードを促す事件も発生しています[*15]。これは、問題となった広告配信サービスが米国の別の広告配信サービスから日本国内向けの配信を受けた際に、特定の悪意ある広告が混入したことによるものでした。このような、正規ソフトウェアの信頼性を悪用したマルウェアの感染活動は今後も継続すると考えられます。

■ Bitcoin

仮想通貨であるBitcoinについても、その取引が拡がるにつれて、様々な事件が発生しています。この期間では、2月に破綻したBitcoin取引所の1つであるMt.Goxが民事再生手続きを断念したため、東京地方裁判所から保全管理命令を受けています。また、この事件などを受け、消費者庁からBitcoinなどインターネット上の仮想通貨の取引や利用について、注意喚起が行われています[*16]。米国でも米証券取引委員会から、Bitcoinを含む仮想通貨について、盗難や投資詐欺についての注意喚起が行われました[*17]。一方で、米連邦選挙委員会からは選挙の際にBitcoinによる寄付について、認める見解を出すなど、Bitcoinの取り扱いに関する議論などが各国で活発に行われています。また、引き続き仮想通貨の交換所や口座管理サービスに対する攻撃も相次いでおり、これらのWebサイトへのDDoS攻撃や、不正侵入により仮想通貨そのものが盗まれる事件など、多く発生しています。

■ DDoS攻撃

この期間では大規模なDDoS攻撃がいくつか発生しています。5月にはUltraDNSに対し、DDoS攻撃が発生しました[*18]。攻撃の規模は100Gbpsとされており、これによってsalesforceなど複数企業のサービスが影響を受けました。また、6月にはEvernoteやFeedlyといったサービスがDDoS攻撃を受け、一部では金銭を要求される事件も発生しています[*19]。香港でも、民主化活動をする団体の投票システムサイトに対し、最大で300Gbpsとなる大規模なDDoS攻撃が確認されています。日本でも、5月に複数のISPでDNSクエリが急増したことにより、いくつかのISPで障害が発生しています。6月にはオンラインゲームのWebサーバやゲームサーバに対する大規模なDDoS攻撃が発生し、サービスが数日にわたり停止するなどの被害が発生しています[*20]。

＊14 例えば、次のエフセキュアブログでは、ICS/SCADAシステムを狙ったマルウェアの1つであるHavexについて解説しているが、感染手法の1つとしてICSベンダーのサイトを侵害して、トロイの木馬を入れたソフトウェアインストーラを使っていることが示されている。「HavexがICS/SCADAシステムを探し回る」(http://blog.f-secure.jp/archives/50730250.html)。

＊15 Kaspersky Lab社、カスペルスキー公式ブログ「ニコニコ動画の視聴中に怪しいポップアップが出現！」(http://blog.kaspersky.co.jp/fake-flash-player/)。

＊16 消費者庁、「ビットコインを始めとするインターネット上の仮想通貨の利用について」(http://www.caa.go.jp/adjustments/pdf/140428adjustments_1.pdf)。

＊17 U.S. Securities and Exchange Commission、"Investor Alert: Bitcoin and Other Virtual Currency-Related Investments"(http://investor.gov/news-alerts/investor-alerts/investor-alert-bitcoin-other-virtual-currency-related-investments#.U4RTq_l_v24)。

＊18 この事件については、例えば次のInfoSec Handlers Diary Blogなどに詳しい。"UltraDNS DDOS"(https://isc.sans.edu/diary/UltraDNS+DDOS/18051)。

＊19 詳細については、攻撃を受けた企業の1つであるFeedlyのBlogなどを参照のこと。"Denial of service attack [Neutralized]"(http://blog.feedly.com/2014/06/11/denial-of-service-attack/)。

＊20 例えば、次のアナウンスを参照のこと(http://pso2.jp/players/news/?id=3835)。

5月のインシデント

1
2 脆 **2日**：Microsoft社は、公表していたInternet Explorerの複数のバージョンにリモートでコードが実行可能な未修正の脆弱性について、更新をリリースした。
「マイクロソフト セキュリティ情報 MS14-021 緊急 Internet Explorer 用のセキュリティ更新プログラム (2965111)」(https://technet.microsoft.com/ja-jp/library/security/ms14-021)。
3
4 他 **8日**：米証券取引委員会(SEC)は、Bitcoinを含む仮想通貨への投資について、投資詐欺などの犯罪に巻き込まれる可能性があるとして注意喚起を行った。
"Investor Alert: Bitcoin and Other Virtual Currency-Related Investments"(http://investor.gov/news-alerts/investor-alerts/investor-alert-bitcoin-other-virtual-currency-related-investments)。
5
6 脆 **9日**：BIND 9.10.0に、実装上の不具合により外部からのサービス不能攻撃が可能となる脆弱性が見つかり、修正された。
「(緊急)BIND 9.10.0の脆弱性(DNSサービスの停止)について(2014年5月9日公開)」(http://jprs.jp/tech/security/2014-05-09-bind9-vuln-prefetch.html)。
7
8 他 **9日**：米連邦取引委員会(FTC)は、写真共有アプリの1つであるSnapchatについて、設定によって相手の端末から写真データが消えるサービスなどについて、実際には消去されていないなど虚偽の説明を行っていたことや、1月に発生した460万件の個人情報流出事件で管理に問題があったとして処分を公表した。
"Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False"(http://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were)。
9
10 脆 **14日**：Microsoft社は、2014年5月のセキュリティ情報を公開し、MS14-022とMS14-029の2件の緊急と6件の重要な更新をリリースした。
「2014 年 5 月のマイクロソフト セキュリティ情報の概要」(https://technet.microsoft.com/ja-JP/library/security/ms14-may)。
11 脆 **14日**：Adobe Reader及びAcrobatに、不正終了や、任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「APSB14-15: Adobe ReaderおよびAcrobat用セキュリティアップデート公開」(http://helpx.adobe.com/jp/security/products/reader/apsb14-15.html)。
12 脆 **14日**：Adobe Flash Playerに、不正終了や、任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「APSB14-14: Adobe Flash Player用のセキュリティアップデート公開」(http://helpx.adobe.com/jp/security/products/flash-player/apsb14-14.html)。
13
14 他 **14日**：サイバーセキュリティ基本法案が衆議院で可決した。その後、参議院に付託されたが6月20日に継続審査となった。
参議院、「サイバーセキュリティ基本法案」(http://www.sangiin.go.jp/japanese/joho1/kousei/gian/186/meisai/m18605186035.htm)。
15 セ **15日**：JPCERTコーディネーションセンターは、Movable Typeの既知の脆弱性を使用した攻撃により、不正なファイルが設置されたり、攻撃サイトへと誘導するiframeや難読化されたJavaScriptが埋め込まれたりする事件が多く確認されているとして注意喚起を行った。
「JPCERT/CC Alert 2014-05-15 旧バージョンの Movable Type の利用に関する注意喚起」(https://www.jpcert.or.jp/at/2014/at140024.html)。
16
17
18 他 **19日**：遠隔操作ウイルスに関連する一連の事件で逮捕され、威力業務妨害罪などに問われていた容疑者について、公判中に犯人からと称するメールが送信された件について、容疑者自ら行っていたことから、保釈が取り消された。その後、容疑者は一連の事件の犯人であることを自白し、自らの犯行であることを認めた。
19
20 セ **20日**：FBIは、ファイルやアカウント情報を盗むRAT Blackshadesに関わったとされる、共同作成者を含む100人以上を逮捕したことを発表した。
この事件の詳細については例えば次のFBIの発表を参照のこと。"Manhattan U.S. Attorney And FBI Assistant Director-In-Charge Announce Charges In Connection With Blackshades Malicious Software That Enabled Users Around The World To Secretly And Remotely Control Victims' Computers"(http://www.justice.gov/usao/nys/pressreleases/May14/BlackshadesPR.php)。
21
22 他 **20日**：経済産業省は、ソフトウエア等脆弱性関連情報取扱基準について、製品開発者と連絡が取れない場合の脆弱性の公表基準などを新たに定めるなどの改正を行った。
「ソフトウエア等脆弱性関連情報取扱基準の改正について」(http://www.meti.go.jp/policy/netsecurity/default.htm)。
23 他 **20日**：IPAは、標的型攻撃を受けた組織に対する被害拡大と再発の抑止・低減、速やかな対策の実施を支援する組織として、サイバーレスキュー隊(仮)を発足するため、その準備チームを立ち上げることを公表した。
「プレス発表 『サイバーレスキュー隊(仮称)』発足に向けた準備チームを5月20日に立ち上げ」(https://www.ipa.go.jp/about/press/20140520.html)。
24
25
26 脆 **22日**：Microsoft社のInternet Explorer 8に任意のコードを実行される可能性ある未修正の脆弱性が見つかり、公表された。
この脆弱性は6月11日に「マイクロソフト セキュリティ情報 MS14-035 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (2969262)」(https://technet.microsoft.com/ja-jp/library/security/ms14-035.aspx)で修正された。
27
28 他 **22日**：米国下院で、国家安全保障局(NSA)による情報収集活動の改革法案である"USA FREEDOM Act"が可決された。
Librarian of Congress、"Bill Summary & Status 113th Congress (2013 - 2014) H.R.3361 All Information"(http://thomas.loc.gov/cgi-bin/bdquery/z?d113:HR03361:@@@L&summ2=m&)。
29
30 セ **27日**：オーストラリアなど複数の国で、iPhoneなどApple社製の端末が遠隔ロックされ、金銭を要求される事件が発生した。
この事件では、Apple社が提供しているFind My iPhoneの機能を悪用したと考えられているが手口の詳細については明らかになっていない。
31 セ **29日**：複数のプロバイダでDNSサーバへの問い合わせが急増したことによる障害が発生した。

[凡例] 脆 脆弱性 セ セキュリティ事件 動 動静情報 歴 歴史 他 その他

※日付は日本標準時

■ 政府機関の取り組み

政府機関のセキュリティ対策の動きとしては、4月に総務省より、「クラウドサービス提供における情報セキュリティ対策ガイドライン」が公表されました。これまでは、2008年にまとめられた「ASP・SaaSにおける情報セキュリティ対策ガイドライン」[*21]にて、クラウド事業者が行うべき情報セキュリティ対策が示されていましたが、PaaSやIaaSなど、インフラ領域のクラウドサービスとASP・SaaSなどのアプリケーションを提供するクラウドサービスが連携するなど、複数のクラウドサービスや事業者にまたがった利用の広がりを受け、クラウド事業者に向けた、利用者との取り決めや、事業者間連携における実務のポイントについてまとめられています。

6月には、改正児童買春・ポルノ禁止法が可決、成立しています。この改正では、個人が児童ポルノの写真や映像を持つ単純所持の禁止やインターネットの利用に係る事業者の努力規定が新設されるなどしています。

同じく6月には、政府のサイバー攻撃対応の向上を目的とした、サイバーセキュリティ基本法案が衆議院で可決されました。この中では、国や自治体が主体となってサイバー攻撃への対応ができるように、官房長官を本部長とする「サイバーセキュリティ戦略本部」を設置することや、政府機関に対策実施を勧告することができるなど、政府の対応能力の向上や機能強化だけでなく、民間の重要インフラ事業者が対策に協力することなど、官民が連携してサイバー攻撃への対応能力の強化に向けた取り組みを進めることなどが示されています。この法案についてはその後、参議院で審議となりましたが、今国会中に成立することができなかったことから、継続審議となっています。

また、パーソナルデータの利活用促進への課題の解決に向けた法的措置についての議論が、政府の「パーソナルデータに関する検討会」で進められていましたが、一定の規律の下で、原則として本人の同意が求められる第三者提供などを本人の同意がなくても行うことを可能とする枠組みの導入、基本的な制度の枠組みとこれを補完する民間の自主的な取り組みの活用、第三者機関の体制整備などによる実効性ある制度執行の確保などを示した、「パーソナルデータの利活用に関する制度改正大綱」が公表されています。

経済産業省からは、「ソフトウエア等脆弱性関連情報取扱基準」の改正が公表されています。長期間にわたって製品開発者と連絡がとれないなど、製品開発者との間で公表の合意が得られない場合には、有識者による第三者委員会を設置して脆弱性情報の公表の可否を審議し、その意見を踏まえて判定することが定められています。

■ オンラインバンキングを狙った攻撃

この期間ではオンラインバンキングの情報を狙ったフィッシングやマルウェアによる攻撃が話題となりました。4月には地方銀行に対し、リストを利用したと考えられる不正ログインが発生しています。フィッシングについても、複数の金融機関を対象とした、フィッシングサイトやフィッシングメールが確認されています[*22]。また、日本の金融機関をターゲットとしたマルウェアが確認される[*23]など、その手口も巧妙化しています。マルウェアによる攻撃の詳細については「1.4.2 国内金融機関の認証情報などを窃取するマルウェア『vawtrak』」も併せてご参照ください。更に、4月には、約1万3千件のネットバンキングのIDやパスワードを含む口座情報が国内のサーバに不正に保管されていたとの報道がありました。この事件で確認された情報については、ネットバンキングの利用時に偽のサイトを表示させるウイルスに感染したことで盗まれたとされています。このように、日本のユーザを対象として、金銭目的でクレジットカードやオンラインバンキングなどの認証情報を狙った攻撃は継続しており、その手口も巧妙化していることから、引き続き注意が必要です。

＊21 総務省「ASP・SaaSにおける情報セキュリティ対策ガイドライン」(http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/asp_saas/)。

＊22 発生状況については次のフィッシング対策協議会(http://www.antiphishing.jp/)の緊急情報で確認できる。

＊23 例えば、次のトレンドマイクロ社のブログ「クレジットカード情報も狙うオンライン銀行詐欺ツール『VAWTRAK』、国内で検出報告増加を確認」(http://blog.trendmicro.co.jp/archives/9192)などを参照のこと。

6月のインシデント

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30

セ **3日**：5月後半から発生していた複数サイトの不正アクセスによるコンテンツやファイルの改ざん事件について、利用していたCDNサービスの提供事業者が不正侵入を受けたことによるものと判明した。

セ **3日**：米司法省は、オンラインバンキングなどの情報窃取を行うマルウェアであるGameOver Zeusについて、10ヵ国以上の法執行機関と共同でテイクダウンを実施し、関連サイトの差し押さえや管理者の逮捕などが行われたことを公表した。
Department of Justice、"U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator"（http://www.justice.gov/opa/pr/2014/June/14-crm-584.html）。日本では警察庁が協力している。この作戦についての説明は「国際的なボットネットのテイクダウン作戦」（http://www.npa.go.jp/cyber/goz/index.html）を参照のこと。

脆 **6日**：OpenSSLに、Man-in-the-middle（MITM）攻撃可能な脆弱性（CVE-2014-0224）が見つかり、修正された。
"OpenSSL Security Advisory [05 Jun 2014] SSL/TLS MITM vulnerability (CVE-2014-0224)"（https://www.openssl.org/news/secadv_20140605.txt）。

脆 **11日**：Microsoft社は、2014年6月のセキュリティ情報を公開し、MS14-035とMS14-036の2件の緊急と5件の重要な更新をリリースした。
「2014 年 6 月のマイクロソフト セキュリティ情報の概要」（https://technet.microsoft.com/ja-jp/library/security/ms14-jun）。

脆 **11日**：Adobe Flash Playerに、任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「APSB14-16: Adobe Flash Player用のセキュリティアップデート公開」（http://helpx.adobe.com/jp/security/products/flash-player/apsb14-16.html）。

脆 **12日**：BIND 9.10.xに、外部からのサービス不能（DoS）攻撃が可能となる脆弱性（CVE-2014-3859）が見つかり、修正された。
Internet Systems Consortium"CVE-2014-3859: BIND named can crash due to a defect in EDNS printing processing"（https://kb.isc.org/article/AA-01166/）。

セ **12日**：サポート終了となった日本独自のブログ作成ツールについて、約8割が問題のある状態で運用されており、攻撃者の標的になっているとして注意喚起が行われた。
詳細については、次のKaspersky Lab社のBlogに詳しい。「日本独自のブログ作成ツールが攻撃者の標的に！」（http://blog.kaspersky.co.jp/obsolete-japanese-cms-targeted-by-criminals/）。

セ **13日**：香港の民主化を求めて活動する団体の電子投票システムに対する大規模なDDoS攻撃が発生した。
詳細については、例えば次のHarvard University Internet Monitor Berkman Center for Internet & SocietyのBlogなどで確認できる。"DDoS Attacks in Hong Kong Target Pro-Democracy Websites"（https://blogs.law.harvard.edu/internetmonitor/2014/06/20/ddos-attacks-in-hong-kong-attack-silence-pro-democracy-websites/）。

他 **18日**：単純所持の禁止などを追加した、改正児童買春・ポルノ禁止法が可決され、成立した。
この改正については、7月15日に施行された。詳細については次の法務省による解説も参照のこと。「児童買春, 児童ポルノに係る行為等の処罰及び児童の保護等に関する法律の一部を改正する法律案」（http://www.moj.go.jp/keiji1/keiji11_00008.html）。

セ **19日**：広告配信サーバによって、Adobe Flash Playerの更新を促す通知に見せかけた悪意あるサイトに誘導する広告が表示される事件が発生した。
「«広告配信障害に関するプレスリリースの追記に関して»」（http://www.microad.co.jp/news/detail.php?News_ID=252）。

他 **19日**：第12回パーソナルデータに関する検討会が行われ、「パーソナルデータの利活用に関する制度改正大綱（検討会案）」が示された。
首相官邸、「第１２回 パーソナルデータに関する検討会　議事次第」（http://www.kantei.go.jp/jp/singi/it2/pd/dai12/gijisidai.html）。

他 **27日**：米国政府による、2013年度のTransparency Reportが公開された。
詳細については、次のレポートを参照のこと（http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013）。

他 **29日**：Facebookが、約70万人のユーザを対象にニュースフィードの表示操作による心理実験を行っていたことが発表された論文から分かり、倫理的に問題がある可能性が指摘されたことから話題となった。
問題となった論文については"Experimental evidence of massive-scale emotional contagion through social networks"（http://www.pnas.org/content/111/24/8788.full）で確認できる。

セ **30日**：Microsoft社は、Bladabindi（NJrat）とJenxcus（NJw0rm）の2つのマルウェアファミリーが利用していたダイナミックDNSサービスであるNO-IPの23ドメインについて、テイクダウンを実施したことを公表した。
The Official Microsoft Blog、"Microsoft takes on global cybercrime epidemic in tenth malware disruption"（http://blogs.microsoft.com/blog/2014/06/30/microsoft-takes-on-global-cybercrime-epidemic-in-tenth-malware-disruption/）。また、NO-IPを運用していたVitalwerks Internet Solutions, LLCからも声明が発表されている。"No-IP's Formal Statement on Microsoft Takedown"（https://www.noip.com/blog/2014/06/30/ips-formal-statement-microsoft-takedown/）。

［ 凡 例 ］ 脆 脆 弱 性　セ セキュリティ事件　動 動 静 情 報　歴 歴　史　他 そ の 他

※日付は日本標準時

■ その他

4月にはJPRSより、カミンスキー型攻撃手法[*24]によるものと考えられるキャッシュDNSサーバへのアクセスが増加しているとして、注意喚起が行われました[*25]。また、現在新たなgTLDが次々と承認されています。これに伴い、これまで企業などの内部ネットワークで利用していたドメイン名が、新しく追加されたドメイン名と衝突することで発生する可能性のある、情報漏えいやサービスが利用できないなどの事象について、JPNICより注意喚起が行われています[*26]。

4月には韓国の金融監督院が、複数のクレジットカード事業者の約20万人のクレジットカード情報が流出したことを公表しました。これは、2013年12月に発生したPOS端末管理業者のサーバが侵害された事件の捜査に関連して明らかになったとしています。POS端末などの業務システムに対する事件としては、昨年11月に米国の大手小売業者で発生した情報漏えい事件があります。米国の事件ではPOS端末を対象としたマルウェアが利用されたことから、1月にUS-CERTから注意喚起が行われています[*27]。更に、この事件を受け、5月には複数の小売業者が中心となって、セキュリティ情報の共有・分析を行う組織としてRetail Cyber Intelligence Sharing Center（R-CISC）が発足しています[*28]。POSマルウェアについては、日本でも感染した事例があるとの報道もあることから、今後もこのような業務システムに対する攻撃については注意が必要です。

一昨年話題となった、遠隔操作ウイルスに関連する一連の事件で逮捕され、威力業務妨害罪などに問われた容疑者については、5月になって、公判中に真犯人と名乗る何者かからのメールが送信された事件に関連していたとして保釈が取り消される事態となり、その後、本人が犯人であることを自白しています。

5月には、オーストラリアなどを中心にiPhone、iPadなどApple社製の端末がロックされ、身代金が要求される事件が複数発生しました。これは紛失時などに使う管理サービスのアカウントが何者かに不正に利用されたとされています。

同じく5月には、欧州司法裁判所にて、Google Spain及びGoogle Inc.に対し、ユーザからの申告があった場合、検索結果から個人情報を含むサイトへのリンクを削除する責任が生じるとの裁定が行われました[*29]。欧州では、個人情報を含むデータの取り扱いについて、個人情報の管理者はその情報の主体である個人の請求があった場合には当該データの削除を義務づけること（いわゆる忘れられる権利）などが、EUデータ保護規則案として議論が進められていることから[*30]、今後も、個人情報保護の強化に向けた様々な動きがあると考えられます。

＊24 詳細についてはIIR Vol.2（http://www.iij.ad.jp/development/iir/pdf/iir_vol02.pdf）の「1.4.1 DNSキャッシュポイズニング」を参照のこと。
＊25 株式会社日本レジストリサービス、「（緊急）キャッシュポイズニング攻撃の危険性増加に伴うDNSサーバーの設定再確認について（2014年4月15日公開）」（http://jprs.jp/tech/security/2014-04-15-portrandomization.html）。
＊26 一般社団法人日本ネットワークインフォメーションセンター（JPNIC）、「新gTLD大量導入に伴う名前衝突(Name Collision)問題とその対策について」（https://www.nic.ad.jp/ja/dom/new-gtld/name-collision/name-collision-report.pdf）。
＊27 US-CERT、"Alert (TA14-002A) Malware Targeting Point of Sale Systems"（http://www.us- cert.gov/ncas/alerts/TA14-002A）。
＊28 Retail Cyber Intelligence Sharing Center（R-CISC）、"Retailers Launch Comprehensive Cyber Intelligence Sharing Center"（http://www.rila.org/rcisc/home/Pages/default.aspx）。
＊29 Court of Justice of the European Union、"An internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties"（http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf）。
＊30 現在進められているEUデータ保護規則（案）については、例えば次の一般社団法人電子情報技術産業協会による「EU データ保護指令改定に関する調査・分析報告書」（http://home.jeita.or.jp/page_file/20120427161714_ljwGedlUnB.pdf）などで確認することができる。

1.3 インシデントサーベイ

1.3.1 DDoS攻撃

現在、一般の企業のサーバに対するDDoS攻撃が、日常的に発生するようになっており、その内容は、状況により多岐にわたります。しかし、攻撃の多くは、脆弱性などの高度な知識を利用したものではなく、多量の通信を発生させて通信回線を埋めたり、サーバの処理を過負荷にしたりすることでサービスの妨害を狙ったものになっています。

■ 直接観測による状況

図-2に、2014年4月から6月の期間にIIJ DDoS対策サービスで取り扱ったDDoS攻撃の状況を示します。

ここでは、IIJ DDoS対策サービスの基準で攻撃と判定した通信異常の件数を示しています。IIJでは、ここに示す以外のDDoS攻撃にも対処していますが、正確な攻撃の実態を把握することが困難なため、この集計からは除外しています。

DDoS攻撃には多くの攻撃手法が存在し、攻撃対象となった環境の規模(回線容量やサーバの性能)によって、その影響度合が異なります。図-2では、DDoS攻撃全体を、回線容量に対する攻撃[*31]、サーバに対する攻撃[*32]、複合攻撃(1つの攻撃対象に対し、同時に数種類の攻撃を行うもの)の3種類に分類しています。

この3ヵ月間でIIJは、388件のDDoS攻撃に対処しました。1日あたりの対処件数は4.3件で、平均発生件数は前回のレポート期間と比べて減少しました。DDoS攻撃全体に占める割合は、サーバに対する攻撃が78.6%、複合攻撃が16.2%、回線容量に対する攻撃が5.2%でした。

今回の対象期間に観測された中で最も大規模な攻撃は、複合攻撃に分類したもので、最大9,000ppsのパケットによって72.9Mbpsの通信量を発生させる攻撃でした。攻撃の継続時間は、全体の94.8%が攻撃開始から30分未満で終了し、5.2%が30分以上24時間未満の範囲に分布しており、24時間以上継続した攻撃はありませんでした。なお、今回最も長く継続した攻撃は、サーバに対する攻撃に分類されるもので15時間57分にわたりました。このように、今回の対象期間では、前回と比べて攻撃の回数と量に大幅な減少がみられています。しかしながら、世界的に話題となっているように、DNSやNTPを悪用したDrDoS攻撃は散発的に発生しており、引き続き注意が必要な状況です。

攻撃元の分布としては、多くの場合、国内、国外を問わず非常に多くのIPアドレスが観測されました。これは、IPスプーフィング[*33]の利用や、DDoS攻撃を行うための手法としてのボットネット[*34]の利用によるものと考えられます。

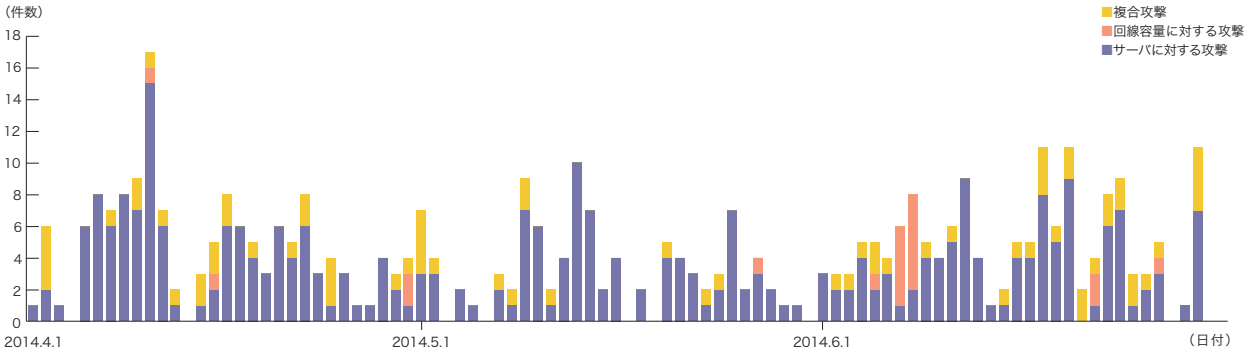


図-2 DDoS攻撃の発生件数

*31 攻撃対象に対し、本来不必要な大きなサイズのIPパケットやその断片を大量に送りつけることで、攻撃対象の接続回線の容量を圧迫する攻撃。UDPパケットを利用した場合にはUDP floodと呼ばれ、ICMPパケットを利用した場合にはICMP floodと呼ばれる。

*32 TCP SYN floodやTCP connection flood、HTTP GET flood攻撃など。TCP SYN flood攻撃は、TCP接続の開始の呼を示すSYNパケットを大量に送付することで、攻撃対象に大量の接続の準備をさせ、対象の処理能力やメモリなどを無駄に利用させる。TCP Connection flood攻撃は、実際に大量のTCP接続を確立させる。HTTP GET flood攻撃は、Webサーバに対しTCP接続を確立した後、HTTPのプロトコルコマンドGETを大量に送付することで、同様に攻撃対象の処理能力やメモリを無駄に消費させる。

*33 発信元IPアドレスの詐称。他人からの攻撃に見せかけたり、多人数からの攻撃に見せかけたりするために、攻撃パケットの送出時に、攻撃者が実際に利用しているIPアドレス以外のアドレスを付与した攻撃パケットを作成、送出すること。

*34 ボットとは、感染後に外部のC&Cサーバからの命令を受けて攻撃を実行するマルウェアの一種。ボットが多数集まって構成されたネットワークをボットネットと呼ぶ。

■ backscatterによる観測

次に、IIJでのマルウェア活動観測プロジェクトMITFのハニーポット[*35]によるDDoS攻撃のbackscatter観測結果を示します[*36]。backscatterを観測することで、外部のネットワークで発生したDDoS攻撃の一部を、それに介在することなく第三者として検知できます。

2014年4月から6月の期間中に観測したbackscatterについて、発信元IPアドレスの国別分類を図-3に、ポート別のパケット数推移を図-4にそれぞれ示します。

観測されたDDoS攻撃の対象ポートのうち最も多かったものはWebサービスで利用される80/TCPで、対象期間における全パケット数の22.6%を占めています。またDNSに利用される53/UDP、53/TCP、SSHで利用される22/TCPなどへの攻撃、通常は利用されない3477/TCPや5000/TCPなどへの攻撃が観測されています。前回に引き続き観測されているDNS(53/UDP)のbackscatterは、増減を繰り返しながら1日平均約1,500パケットで推移しており、今後もDNSサーバに対するDDoS攻撃やDNSキャッシュポイズニング攻撃などへの注意が必要です。

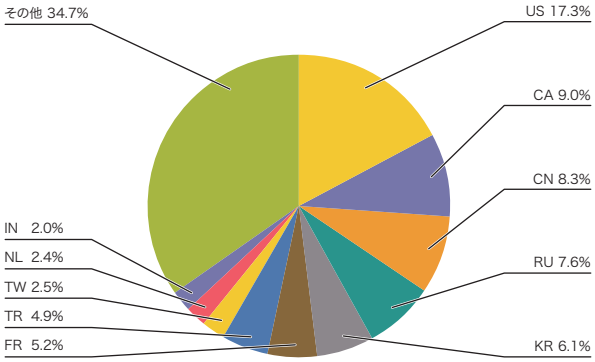


図-3 DDoS攻撃のbackscatter観測による攻撃先の国別分類

図-3で、DDoS攻撃の対象となったIPアドレスと考えられるbackscatterの発信元の国別分類を見ると、米国の17.3%が最も大きな割合を占めています。その後にカナダの9.0%、中国の8.3%といった国が続いています。

特に多くのbackscatterを観測した場合について、攻撃先のポート別にみると、Webサーバ(80/TCP)への攻撃としては、4月15日には米国で主に日本向けサービスを提供しているホスティング事業者、4月16日にはロシアのホスティング事業者、6月30日には米国のCDN事業者のサーバに対する攻撃をそれぞれ観測しています。4月6日から8日にかけて3477/TCPへの攻撃が観測されましたが、backscatterの発信元IPアドレスがプライベートアドレスのため、攻撃対象は不明です。4月23日にカナダのホスティング事業者に対するDNS(53/TCP)への攻撃が、6月21日には同事業者に対する5000/TCPと5001/TCP、6005/TCPへの攻撃が、6月23日にはSSH(22/TCP)への攻撃が観測されています。5月15日にロシアにある特定のサーバに対する様々なTCPポートへの攻撃を観測しています。

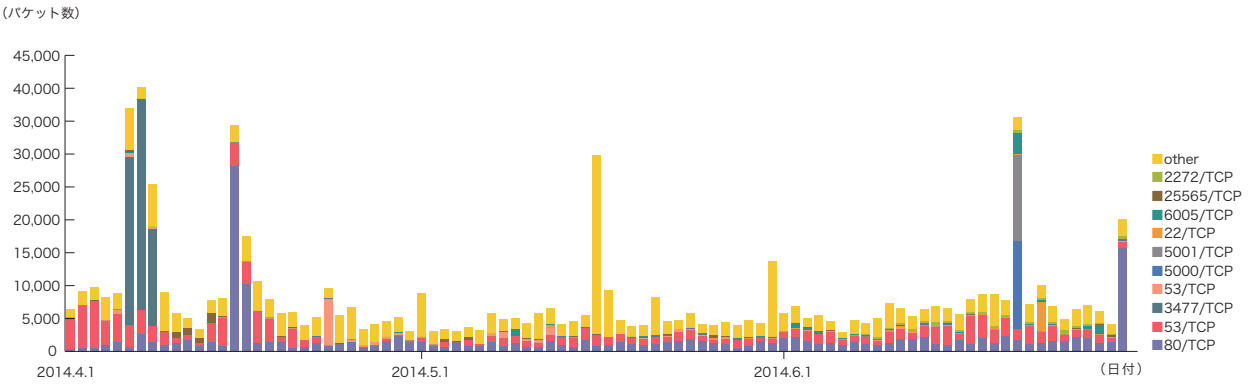


図-4 DDoS攻撃によるbackscatter観測(観測パケット数、ポート別推移)

*35 IIJのマルウェア活動観測プロジェクトMITFが設置しているハニーポット。本レポート「1.3.2 マルウェアの活動」も参照。

*36 この観測手法については、IIR Vol.8(http://www.iij.ad.jp/development/iir/pdf/iir_vol08.pdf)の「1.4.2 DDoS攻撃によるbackscatterの観測」で仕組みとその限界、IIJによる観測結果の一部について紹介している。

また、今回の対象期間中に話題となったDDoS攻撃のうち、IIJのbackscatter観測で検知した攻撃としては、4月初めに複数のニュースサイトが報じた米国カンザス州のオンライン試験サイトに対するDDoS攻撃を検知しています。この攻撃は、報道の後も断続的に続いている様子が観測されています。他に、5月1日には米国のUltraDNSへの攻撃、5月21日にはカナダの大規模SNSサイトへの攻撃、6月11日にEvernoteへの攻撃をそれぞれ検知しています。

1.3.2 マルウェアの活動

ここでは、IIJが実施しているマルウェアの活動観測プロジェクトMITF[*37]による観測結果を示します。MITFでは、一般利用者と同様にインターネットに接続したハニーポット[*38]を利用して、インターネットから到着する通信を観測しています。そのほとんどがマルウェアによる無作為に宛先を選んだ通信か、攻撃先を見つけるための探索の試みであると考えられます。

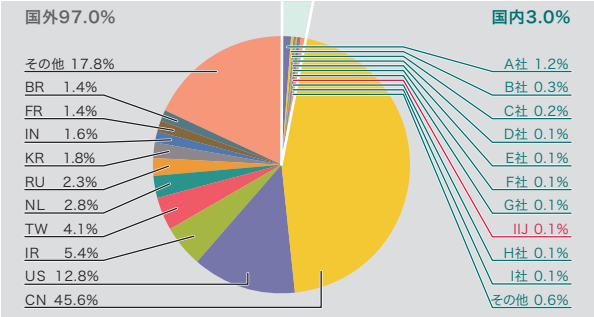


図-5 発信元の分布（国別分類、全期間）

■ 無作為通信の状況

2014年4月から6月の期間中に、ハニーポットに到着した通信の発信元IPアドレスの国別分類を図-5に、その総量（到着パケット数）の推移を図-6に、それぞれ示します。MITFでは、数多くのハニーポットを用いて観測を行っていますが、ここでは1台あたりの平均を取り、到着したパケットの種類（上位10種類）ごとに推移を示しています。また、この観測では、MSRPCへの攻撃のような特定のポートに複数回の接続を伴う攻撃は、複数のTCP接続を1回の攻撃と数えるように補正しています。

ハニーポットに到着した通信の多くは、Microsoft社のOSで利用されているTCPポートに対する探索行為でした。また、同社のSQLServerで利用される1433/TCPやWindowsのリモートログイン機能である、RDPで利用される3389/TCP、ICMP Echo Request、SSHで利用される22/TCP、DNSで利用される53/UDP、Telnetで利用される23/TCPによる探査行為も観測されています。

期間中、SSHの辞書攻撃の通信も散発的に発生しており、例えば4月12日に中国、5月4日にタイと中国、6月1日に中国にそれぞれ割り当てられたIPアドレスから行われていました。4月3日、4日のICMP Echo Requestは、中国に割り当てられている500以上のIPアドレス群から単一のIPアドレスに対して通信が行われたものを検知しています。4月12日、5月17日には、イランに割り当てられたIPアドレスから、特定のハニーポットのIPアドレスに対して3395/UDPに

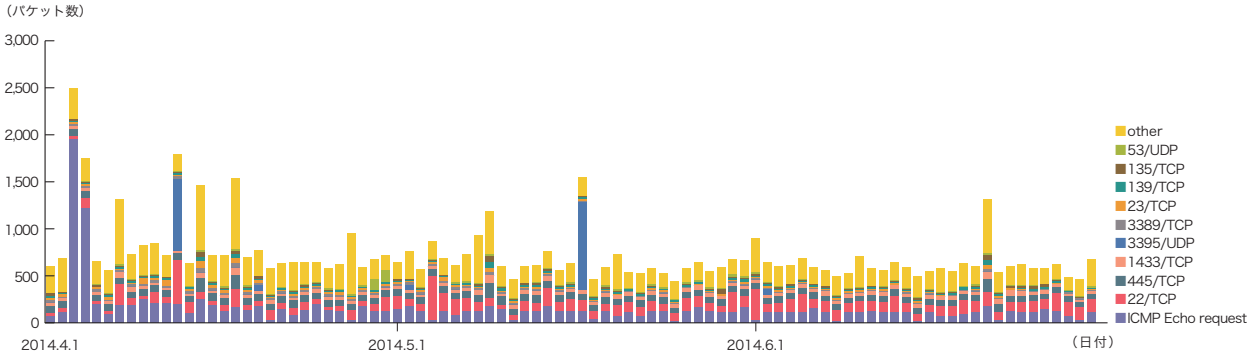


図-6 ハニーポットに到着した通信の推移（日別・宛先ポート別・1台あたり）

＊37 Malware Investigation Task Forceの略。MITFは2007年5月から開始した活動で、ハニーポットを用いてネットワーク上でマルウェアの活動の観測を行い、マルウェアの流行状況を把握し、対策のための技術情報を集め、対策につなげる試み。

＊38 脆弱性のエミュレーションなどの手法で、攻撃を受けつけて被害に遭ったふりをし、攻撃者の行為やマルウェアの活動目的を記録する装置。

対する通信が行われています。この通信の調査を行ったところ、長さは数十から数百バイトのランダムなデータが送信されていました。

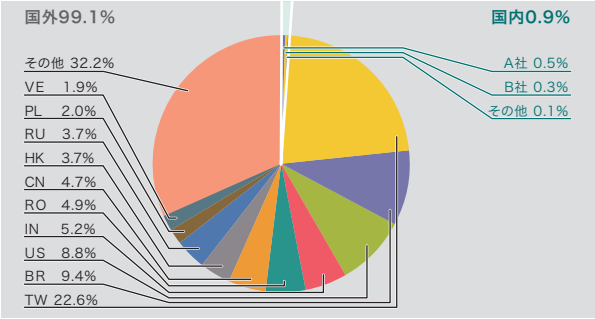


図-7 検体取得元の分布（国別分類、全期間、Conficker除く）

■ ネットワーク上でのマルウェアの活動

同じ期間中でのマルウェアの検体取得元の分布を図-7に、マルウェアの総取得検体数の推移を図-8に、そのうちのユニーク検体数の推移を図-9にそれぞれ示します。このうち図-8と図-9では、1日あたりに取得した検体[*39]の総数を総取得検体数、検体の種類をハッシュ値[*40]で分類したものをユニーク検体数としています。また、検体をウイルス対策ソフトで判別し、上位10種類の内訳をマルウェア名称別に色分けして示しています。なお、図-8と図-9は前回同様に複数のウイルス対策ソフトウェアの検出名によりConficker判定を行い、Confickerと認められたデータを除いて集計しています。

期間中での1日あたりの平均値は、総取得検体数が121、ユニーク検体数が22でした。未検出の検体をより詳しく調査した結果、米国、中国、インドなど、複数の国に割り当てら

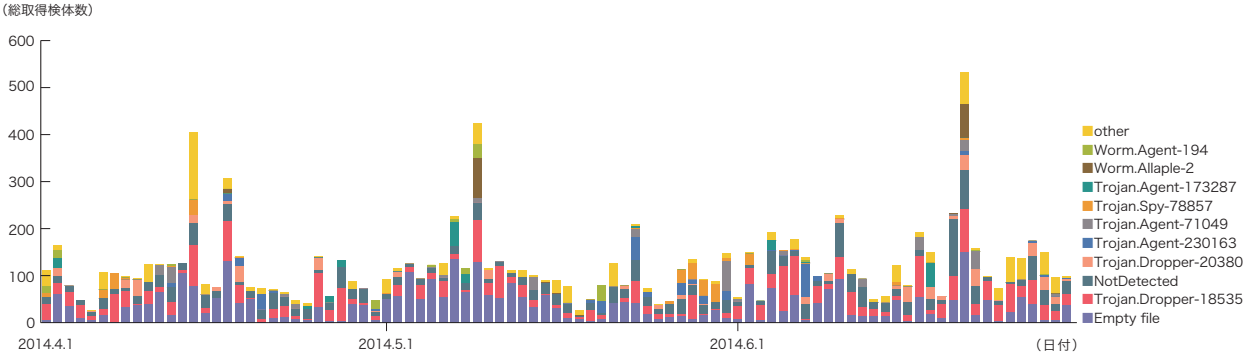


図-8 総取得検体数の推移（Confickerを除く）

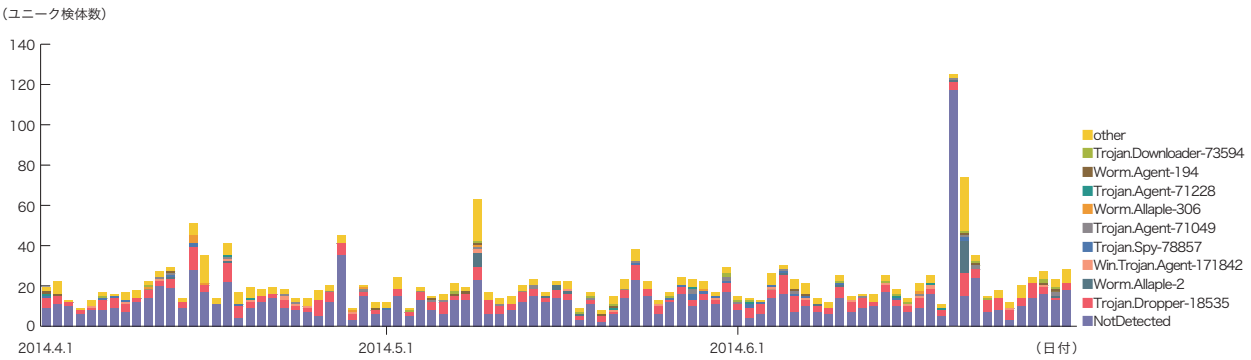


図-9 ユニーク検体数の推移（Confickerを除く）

＊39 ここでは、ハニーポットなどで取得したマルウェアを指す。

＊40 様々な入力に対して一定長の出力をする一方向性関数（ハッシュ関数）を用いて得られた値。ハッシュ関数は異なる入力に対しては可能な限り異なる出力を得られるよう設計されている。難読化やパディングなどにより、同じマルウェアでも異なるハッシュ値を持つ検体を簡単に作成できてしまうため、ハッシュ値で検体の一意性を保証することはできないが、MITFではこの事実を考慮した上で指標として採用している。

れたIPアドレスからワーム[*41]が観測されました。また、未検出の検体の約54%がテキスト形式でした。これらテキスト形式の多くは、HTMLであり、Webサーバからの404や403によるエラー応答であるため、古いワームなどのマルウェアが感染活動を続けているものの、新たに感染させたパソコンが、マルウェアをダウンロードしに行くダウンロード先のサイトが既に閉鎖させられていると考えられます。MITF独自の解析では、今回の調査期間中に取得した検体は、ワーム型94.8%、ボット型1.0%、ダウンローダ型4.2%でした。また解析により、7個のボットネットC&Cサーバ[*42]と123個のマルウェア配布サイトの存在を確認しました。マルウェア配布サイトの数が増加していますが、これは検体の1つがDGAを使用していたためです。

■ Conficker の活動

本レポート期間中、Confickerを含む1日あたりの平均値は、総取得検体数が31,955、ユニーク検体数は718でした。短期間での増減を繰り返しながらも、総取得検体数で99.6%、ユニーク検体数で96.9%を占めています。このように、今回の対象期間でも支配的な状況が変わらないことから、Confickerを含む図は省略しています。本レポート期間中の総取得検体数は前号の対象期間中と比較し、約11%減少しています。また、ユニーク検体数は前号から約9%減少しました。Conficker Working Groupの観測記録[*43]によると、2014年6月30日現在で、ユニークIPアドレスの総数は1,020,045とされています。2011年11月の約320万台と比較すると、約32%に減少したことになりますが、依然として大規模に感染し続けていることが分かります。

1.3.3 SQLインジェクション攻撃

IIJでは、Webサーバに対する攻撃のうち、SQLインジェクション攻撃[*44]について継続して調査を行っています。SQLインジェクション攻撃は、過去にも度々流行し話題となった攻撃です。SQLインジェクション攻撃には、データを盗むための試み、データベースサーバに過負荷を起こすための試み、コンテンツ書き換えの試みの3つがあることが分かっています。

2014年4月から6月までに検知した、Webサーバに対するSQLインジェクション攻撃の発信元の分布を図-10に、攻撃の推移を図-11にそれぞれ示します。これらは、IIJマネージドIPSサービスのシグネチャによる攻撃の検出結果をまとめたものです。

発信元の分布では、米国35.3%、中国24.6%、日本13.1%となり、以下その他の国々が続いています。Webサーバに対するSQLインジェクション攻撃の発生件数は、前回に比べてやや減少しました。

この期間中、5月7日には、欧州の複数の攻撃元より特定の攻撃先への攻撃が発生していました。5月12日には、中国の複数の攻撃元より特定の攻撃先に対する攻撃が発生していました。5月25日には、欧州や中国の複数の攻撃元より特定の攻撃先に対する攻撃が発生しています。5月30日には、欧米の複数の攻撃元から特定の攻撃先に対する攻撃と、中国の特定の攻撃元より別の特定の攻撃先に対する攻撃が発生していました。6月27日には、韓国と中国の特定の攻撃元より特定の攻撃先に対する大規模な攻撃が発生しています。これらの攻撃は、Webサーバの脆弱性を探る試みであったと考えられます。

ここまでに示したとおり、各種の攻撃はそれぞれ適切に検出され、サービス上の対応が行われています。しかし、攻撃の試みは継続しているため、引き続き注意が必要な状況です。

1.3.4 Webサイト改ざん

MITFのWebクローラ（クライアントハニーポット）によって調査したWebサイト改ざん状況を示します[*45]。このWebクローラは、国内の著名サイトや人気サイトなどを中心とした数万のWebサイトを日次で巡回しており、更に巡回対

*41 WORM_ATAK（http://about-threats.trendmicro.com/archiveMalware.aspx?language=jp&name=WORM_ATAK.D）。
*42 Command&Controlサーバの略。多数のボットで構成されたボットネットに指令を与えるサーバ。
*43 Conficker Working Groupの観測記録（http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking）。
*44 Webサーバに対するアクセスを通じて、SQLコマンドを発行し、その背後にいるデータベースを操作する攻撃。データベースの内容を権限なく閲覧、改ざんすることにより、機密情報の入手やWebコンテンツの書き換えを行う。
*45 Webクローラによる観測手法についてはIIR Vol.22（http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol22.pdf）の「1.4.3 WebクローラによるWebサイト改ざん調査」で仕組みを紹介している。

象を順次追加しています。また、一時的にアクセス数が増加したWebサイトなどを対象に、一時的な観測も行っています。一般的な国内ユーザによる閲覧頻度が高いと考えられるWebサイトを巡回調査することで、改ざんサイトの増減や悪用される脆弱性、配布されるマルウェアなどの傾向が推測しやすくなります。

2014年4月から6月の期間に観測されたドライブバイダウンロードは、Angler及びNuclearによる攻撃が多くを占めています(図-12)。いずれもJavaやFlashなどのプラグインの脆弱性を悪用する機能を備えていますが、特にAnglerは、Silverlightの脆弱性(CVE-2013-0074/CVE-2013-3896)も対象としている点が特徴的です。

小規模な攻撃として、Exploit Kitを使わず、redirector上のJavaScriptでLocation要素を用いて直接マルウェア(exe)を実行させようとする攻撃が数件観測されました。このような誘導では、ブラウザが実行の要否を確認するダイアログを表示させるため、厳密にはドライブバイダウンロードとは言えません。しかし、ユーザが不用意に実行を許可すると、マルウェアが実行されてしまいます。また、改ざんされ誘導元として利用されているWebサイトについて、最初に改ざんを観測してから、6週間以上断続的に同じ状態が継続するサイトが複数見受けられました。

全体として、ドライブバイダウンロードの発生率は減少傾向が継続しているものと推測される状況です。ただし、このような傾向は攻撃者の意図によって急変する可能性があるので、Webサイト運営者、訪問者共に、引き続き注意が必要です。

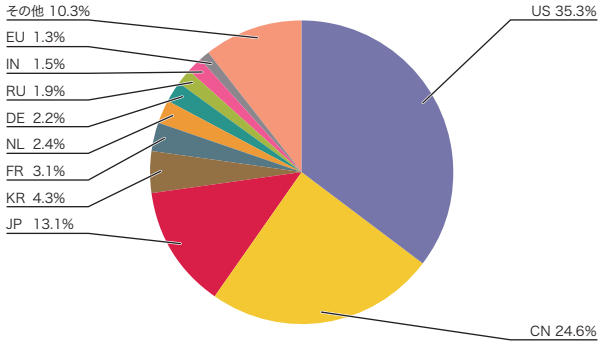


図-10 SQLインジェクション攻撃の発信元の分布

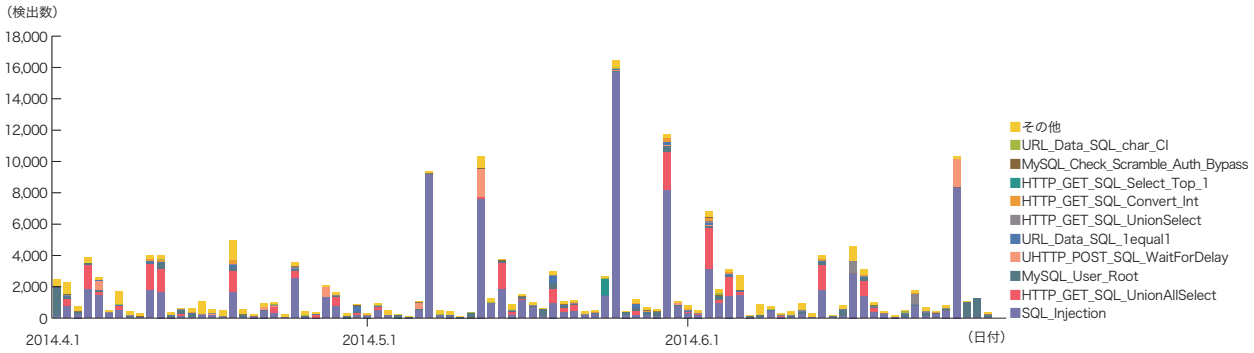
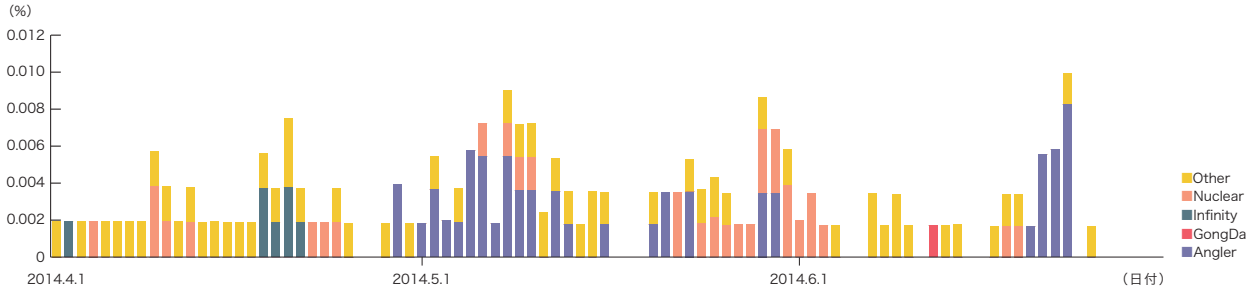


図-11 SQLインジェクション攻撃の推移(日別、攻撃種類別)



※調査対象は日本国内の数万サイト。近年のドライブバイダウンロードは、クライアントのシステム環境やセッション情報、送信元アドレスの属性、攻撃回数などのノルマ達成状況などによって攻撃内容や攻撃の有無が変わるよう設定されているため、試行環境や状況によって大きく異なる結果が得られる場合がある。
※6月26日～6月30日はWebクローラを停止していたため、攻撃を検知していない。

図-12 Webサイト閲覧時のドライブバイダウンロード発生率(%)(Exploit Kit別)

1.4 フォーカスリサーチ

インターネット上で発生するインシデントは、その種類や規模が時々刻々と変化しています。このため、IIJでは、流行したインシデントについて独自の調査や解析を続けることで対策につなげています。ここでは、これまでに実施した調査のうち、OpenSSLの脆弱性、国内金融機関の認証情報などを窃取するマルウェア「vawtrak」、クラウドの安全性確認と監査制度の3つのテーマについて紹介します。

1.4.1 OpenSSLの脆弱性

OpenSSL[*46]は、オープンソースの暗号処理ライブラリの実装であり、UNIX環境において広く使用されています。類似の機能を持つ実装としては、GnuTLS[*47]やNetwork Security Services(NSS)[*48]があります。Windows環境においては、OSの標準機能として、Cryptographic API(CryptoAPI)やCryptography API Next Generation(CNG)が組み込まれています。これらのライブラリは、Webなどの通信の暗号化、サーバ証明に用いられる処理を受け持っており、秘匿性の高いデータを扱っています。最もよく目にする使用箇所としては、Webサービスにおける秘密の保護です。ユーザの認証や、オンラインショッピングにおけるクレジットカードなどの決済情報の入力時への利用がこれにあたります。

OpenSSLライブラリの脆弱性や、SSL/TLSにおいて利用可能な特定の暗号方式に対する効率的な攻撃方法は過去にいくつも公開されました。しかし、これらの脆弱性では攻撃の成立に様々な前提条件が要求されたり、攻撃が成立した結果得られる情報も断片的であったりと、即座に深刻な影響を受けるものはほとんどありませんでした。

表-1 Heartbleed影響実装一覧

実装	脆弱性
OpenSSL1.0.1系	影響あり
OpenSSL1.0.0系	影響なし
OpenSSL0.9.8系	影響なし
他の実装	影響なし

一方で、今回発見されたHeartbleedではサーバ側に保存されている秘密鍵やデータの漏えいが、CCS Injectionでは暗号化された通信が解読できるなど、致命的な影響があるため、大きく話題となりました。どちらの脆弱性も、特定の暗号方式やSSL/TLSの仕様における問題ではなく、OpenSSLの実装に起因する問題であったため、他の実装においてはこれらの脆弱性の影響を受けませんでした。

■ Heartbleedとは

この脆弱性は、2014年4月7日にOpenSSLのセキュリティアドバイザリ(CVE-2014-0160)[*49]として公開されました。系列ごとの影響の有無を表-1に示します。この脆弱性の影響を受けるOpenSSLのバージョンは、1.0.1以降のみでした。クライアント、サーバ実装の組み合わせに関わらず、該当バージョンであれば脆弱性の影響を受けました。

OpenSSL 1.0.1以降のバージョンは、新しいプロトコルバージョンであるTLS v1.1、TLS v1.2を利用するために必要です。TLS v1.1、TLS v1.2は過去に発見された仕様に起因する問題の修正、強度の高い暗号方式が追加されるなど、様々なセキュリティが強化されたプロトコルバージョンです。影響の有無は、このOpenSSLのバージョンを境界として分かれており、セキュリティ強化のために新しいプロトコルバージョンをサポートした箇所に限って、影響を受けてしまうという皮肉な結果になりました。具体的には、ハートビート処理の実装に問題があり、細工したデータをリクエストとして送ることにより、本来読み出せないプロセスのメモリ領域をレスポンスに含めさせることが可能となっていました。

このように、本来読めないはずのメモリ上のデータが読めてしまう脆弱性は、ローカルのみから攻撃可能なカーネルやドライバの脆弱性としては、過去にも多く発見されています。しかし、今回のHeartbleedの脆弱性においては、それがネットワーク越しに可能であること、読み出し可能なサイズが大きいこと、攻撃を受けてもログが残らないことから大きな問題となりました。

*46 OpenSSL:The Open Source toolkit for SSL/TLS(http://www.openssl.org/)。
*47 The GnuTLS Transport Layer Security Library(http://www.gnutls.org/)。
*48 Network Security Services(https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS)。
*49 "OpenSSL Security Advisory [07 Apr 2014] TLS heartbeat read overrun(CVE-2014-0160)"(http://www.openssl.org/news/secadv_20140407.txt)。

攻撃により得られるメモリ上のデータは、OS、メモリアロケータ、アプリケーションの実装や稼働状態に依るため、必ずしも狙ったデータが得られる訳ではありません。しかし、この攻撃は非破壊的な攻撃手法であり、何度でも試行が可能でした。得られるデータには、サーバの保持する秘密鍵や、他のユーザの認証情報など、本来外部から知り得ないデータが含まれる可能性も指摘されていました。

この脆弱性の公開後に、CloudFlare社によって、この脆弱性を用いてサーバに保存された秘密鍵を奪取することを試みる、The Heartbleed Challenge[*50]が開催されました。開始後まもなく鍵の奪取の成功が複数報告され、秘密鍵の漏えいが現実的な脅威であることが示されました。また、秘密鍵の情報を完全に奪取しなくても、部分的な情報から秘密鍵を復元できることも指摘されています[*51]。

この脆弱性への対応として対策版へのバージョンアップも必要ですが、併せて秘密鍵の漏えいを考慮し、新しい鍵ペアの作成とそれを用いた証明書の再発行、既存の証明書の失効が必要になります。これは、過去において攻撃を受けていないことを証明するのが困難であり、既に秘密鍵が漏えいしていた場合を想定した対応が必要なためです。

■ CCS Injectionとは

この脆弱性は、2014年6月5日にOpenSSLのセキュリティアドバイザリ（CVE-2014-0224）[*52][*53]として公開されました。影響を受けるOpenSSLのバージョンは0.9.8以降であり、公開時点においてサポート中の全バージョンが対象でした。この脆弱性の影響を受ける実装の組み合わせを、表-2に示します。クライアントは0.9.8以降、サーバは1.0.1以降の組み合わせにおいてのみ脆弱性の影響を受けました。

この脆弱性は、SSL/TLSのネゴシエーション完了後に暗号化通信に切り替えるChange Cipher Specメッセージの処理に問題があり、中間者攻撃による暗号化通信の完全な解読や改ざんが可能となっていました。

過去において、今回の脆弱性同様に完全な形式での解読が可能な脆弱性としてはSSL v2の問題がありました。SSL v2については、ネゴシエーション時の通信が保護されていないため、容易に改ざんすることができました。このため、通信に用いる暗号アルゴリズムを、攻撃者が解読可能な強度の弱い暗号アルゴリズムに強制的にダウングレードさせることが可能でした。SSL v3以降において、ネゴシエーション時の通信改ざんを検知する仕組みが導入されたため、この問題はなくなりました。しかしながら、今回の脆弱性で利用されたChange Cipher Specメッセージは、改ざん検知の対象から外れており、OpenSSLの実装では中間者攻撃にて挿入することが可能でした。

Change Cipher Specメッセージの処理は、同じバージョンのOpenSSLにおいても、サーバ側とクライアント側で異な

表-2 CCS Injection影響実装一覧

		クライアント実装			
		OpenSSL1.0.1系	OpenSSL1.0.0系	OpenSSL0.9.8系	他の実装
サーバ実装	OpenSSL1.0.1系	影響あり	影響あり	影響あり	影響なし
	OpenSSL1.0.0系	影響なし	影響なし	影響なし	影響なし
	OpenSSL0.9.8系	影響なし	影響なし	影響なし	影響なし
	他の実装	影響なし	影響なし	影響なし	影響なし

＊50 The Heartbleed Challenge（https://www.cloudflarechallenge.com/heartbleed）。
＊51 部分的な情報からの秘密鍵の復元については、IIJ-SECTのblogでも考察を行っている。IIJ-SECT blog、「Heartbleed bugによる秘密鍵漏洩の現実性について」（https://sect.iij.ad.jp/d/2014/04/159520.html）。
＊52 "OpenSSL Security Advisory [05 Jun 2014] SSL/TLS MITM vulnerability（CVE-2014-0224）"（http://www.openssl.org/news/secadv_20140605.txt）。
＊53 この脆弱性の説明や発見の経緯については、発見者である株式会社レピダムのblogに詳しい。株式会社レピダム、「CCS Injection Vulnerability」（http://ccsinjection.lepidum.co.jp/ja.html）及び、「CCS Injection脆弱性(CVE-2014-0224)発見の経緯についての紹介」（https://lepidum.co.jp/blog/2014-06-05/CCS-Injection/）を参照のこと。

ります。この差異が使用箇所によって、影響を受けるバージョンが異なる理由です。脆弱性の特性上、サーバ、クライアント双方を攻撃する必要があるため、いずれかが脆弱性の対象ではないバージョン、またはOpenSSL以外の実装を使用している場合は影響を受けません。他にも影響の有無を分ける細かい条件はありますが、こちらについてもIIJ Security Diary[*54]において考察をしています。

こちらの脆弱性は、Heartbleedと異なり、サーバに保存されている秘密鍵の漏えいなどは発生しませんので、対策版へのバージョンアップのみで問題ありません。

■ まとめ

OpenSSLのような広く使われているライブラリに脆弱性が見つかると、その影響は広範囲に及びます。更に、暗号処理を必要とする通信は、重要な情報を扱っている場合が多いため、必然的に大きな問題になります。

今回のHeartbleedが大きな問題となった後、Linux Foundationは大手IT企業と共に、基盤となるオープンソースプロジェクトを支援するCore Infrastructure Initiative[*55]を立ち上げました。この支援先候補として、OpenSSLプロジェクトが挙げられています。

OpenBSDプロジェクトは、新しくLibreSSLプロジェクト[*56]を立ち上げました。LibreSSLは、OpenSSLのコードを元として、リファクタリング、不要な機能やコードの削減、セキュリティを重視した実装への変更を進めています。

Google社も同様にBoringSSLプロジェクト[*57]を立ち上げました。こちらはOpenSSLの置き換えを目的としておらず、自社のソフトウェア向けに特化した派生プロジェクトです。まずはその成果をChromeのベースとなっているChromiumへ適用し、将来的にはAndroidなどへ展開する計画のようです。

いずれもアプローチは異なりますが、基盤となるソフトウェアにHeartbleedのような大きな問題を再び起こさないために動いていると考えられます。このように、ソフトウェアを作成する側も様々な対策を講じていますが、それでもバグや脆弱性の根絶は困難です。そのため、ソフトウェアを利用する側も公開された脆弱性情報を理解し、影響を受ける脆弱性が公開された場合には、適切に対応する必要があります。

1.4.2 国内金融機関の認証情報などを窃取するマルウェア「vawtrak」

vawtrak（別名Neverquest、Snifula、ZeuS Based Ponyなど）は、2013年頃から海外で感染事例が報告されているマルウェア[*58]ですが、2014年4月から6月にかけて、日本国内で観測されるようになりました[*59]。感染したパソコンに保存されている認証情報や、オンラインバンキング利用時の認証情報などを窃取する機能、VNCプロトコルで外部からパソコンを直接操作する機能などを備えており、日本国内の改ざんされたWebサイトを経由して感染を広げていました。IIJでは、MITFのWebクローラ[*60]によって収集されたvawtrakの検体を抽出し、解析を行いました。本稿では、その解析結果と対策を紹介します。なお、当該検体のハッシュは以下のとおりです。

MD5: 8e8d2a1eafb5c685a02a9adf0890f3bc
SHA-1: 3174ee12fad4422a50655727b0d00222e09239ea
（Dropper）

MD5: aa8422fb8eee6f677cc044212cdd96b9
SHA-1: 7bf386bbf56fbcd16f35e5010f559bbd5cb14634
（32bit版DLLアンパック後）

＊54 IIJ-SECT blog、「OpenSSLのMan-in-the-middle攻撃可能な脆弱性の影響」（https://sect.iij.ad.jp/d/2014/06/069806.html）。
＊55 Core Infrastructure Initiative（http://www.linuxfoundation.org/programs/core-infrastructure-initiative）。
＊56 LibreSSL（http://www.libressl.org/）。
＊57 BoringSSL（https://boringssl.googlesource.com/）。
＊58 Microsoft社の「Malware Protection Center（http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Backdoor:Win32/vawtrak.A）」では2013年5月に初検出している。
＊59 IIJの観測に加え、例えばトレンドマイクロ社のブログ「5月最終週に日本を襲った２つのWeb経由攻撃：「VAWTRAK」と「AIBATOOK」（http://blog.trendmicro.co.jp/archives/9236）」でも2014年5月下旬をピークとして、日本国内でvawtrakの検出数が急増していたことを報告している。
＊60 MITF Webクローラについては、本レポート「1.3.4 Webサイト改ざん」を参照。

■ 主な機能と特徴

vawtrakの注目すべき特徴として、ZeuS（別名Zbot）[*61]及びPony（別名Fareit）[*62]に酷似した機能を備えていることが挙げられます。具体的には、Webinject[*63]、Dynamic Config、Report、VNC ServerやSOCKS Proxyといった ZeuSの特徴的な機能のほとんどを備えています。また、パソコンに保存されたWebブラウザ、メールクライアント、FTPクライアントやsshクライアントなどの設定ファイルからアカウント情報を収集する機能も持っており、この機能の対象とするアプリケーションの種類は、Ponyが対象としているものとほぼ一致します。今回のvawtrak検体におけるZeuS、Ponyとの実行コードの一致率（BinDiffによる）は、それぞれ約8%、20%でしたが、ZeuS、Ponyは、いずれも以前にソースコードがインターネット上に流出したことがあるため、これらのソースコードを参考に多くの機能を組み込んでいるのではないかと推測されます。

以下では、vawtrakの動作フローに沿って検体の各機能について紹介します。

感染時、最初に実行されるのはexe形式のDropperです。これは、実行環境に合わせて32bitまたは64bitのdllファイルを、ランダムなファイル名に.dat拡張子を付与した名前でCSIDL_COMMON_APPDATA（Windows Vista、7、8の場合はC:\ProgramData）にドロップし、起動時に自動実行されるようレジストリを改変します（図-13）。そして、先のdllファイルと同等のvawtrak本体をexplorer.exeにコードインジェクションした上で、自身を削除して終了します。

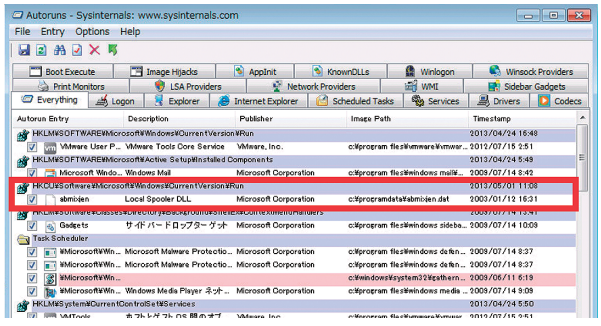


図-13 vawtrakによって改変されたレジストリ

Dropperは削除されてしまいますが、ドロップされたdllファイルや自動起動のレジストリエントリは比較的容易に見つけられるため、本検体感染のインジケータとして利用することが可能です[*64]。

explorer.exeにインジェクションされたコードは、更に、svchost.exeやwininit.exeなど一部のプロセスを除くすべてのプロセスにコードインジェクションを行います。その後、パソコンのユーザがInternet ExplorerやFirefoxなどのブラウザを起動してインターネット通信を始めると、vawtrakはあらかじめ決められたC&Cサーバに HTTPで接続し、追加の設定などが含まれるDynamic Configを受信します。Dynamic ConfigはaPLib[*65]で圧縮され、更に独自方式で暗号化されており、受信後に復号されます。また、再起動に備えてレジストリに保存されます。

本検体が保持していた接続先C&Cサーバを以下に示します。

baggonally.com	mentilix.com
bennimag.com	humpold.com
sandoxon.com	185.13.32.67
185.13.32.80	146.185.233.38
maxigolon.com	146.185.233.80
terekilpane.com	

Dynamic Configを取得して解析をしたところ、Webinjectを行う対象として、日本国内の大手金融機関などのオンラインバンキングやクレジットカード関連サービスを提供す

*61 ZeuSについては、IIR Vol.16（http://www.iij.ad.jp/company/development/report/iir/016.html）の「1.4.3 ZeuSとその亜種について」で詳しく解説している。
*62 Ponyについては、IIJ Security Diary「BHEK2を悪用した国内改ざん事件の続報（https://sect.iij.ad.jp/d/2013/03/225209.html）」で詳しく解説している。
*63 Webinjectとは、Webブラウザの通信系APIをフックすることによってブラウザのメモリ上のWebコンテンツを改ざんする機能。ZeuSやSpyEyeなど、BankingTrojan系のマルウェアのほとんどはこのような機能を持ち、感染者が金融機関などにログインする際、二要素認証などの情報を追加で入力させて奪うことで、金銭を窃取しようと試みる。Webinjectは、IIR Vol.18（http://www.iij.ad.jp/company/development/report/iir/018.html）の「1.4.2 ZeuSの亜種Citadel」や、IIR Vo.13（http://www.iij.ad.jp/company/development/report/iir/013.html）の「1.4.2 SpyEye」で詳しく解説をしている。
*64 これらの値やパスは容易に変更されるため、設定情報などの異なる他のvawtrak亜種ではインジケータとして利用できない可能性がある。
*65 Ibsen Software社によって公開されているオープンソースの圧縮ライブラリ（http://ibsensoftware.com/products_aPLib.html）。

るURLが記載されていました(図-14)[*66]。また、閲覧時の情報窃取の対象として、国内外の著名なSNSやクラウドサービス、動画共有サービス、ファイル共有サービスなどを提供するURLも列挙されていました。

vawtrakは、前述のDynamic Configに加えて、次に行うべき命令(Command)をC&Cサーバから受信します。今回の解析時には、vawtrak自身のバージョンアップ及びパソコンに保存されたデジタル証明書を窃取する命令を受信したことを確認しました。デジタル証明書窃取は、Windows OSの提供する証明書ストアに保持されているすべての証明書を抽出し、C&Cサーバに送信する機能です。パソコンに保存されるデジタル証明書にはいくつかの用途があり、証明書が漏えいした場合には、それぞれの用途で第三者によって成りすまされてしまう危険があります。

その他に、ZeuS、Ponyとは異なる機能として、ソフトウェア制限ポリシーを用いてマルウェア対策ソフトウェアを妨害する機能や、Rapport[*67]の無効化を試みる機能などを備えていました。vawtrakと、ZeuS、及びPonyとの機能の対応をまとめると表-3のようになります。

■ 感染経路

MITFのWebクローラは、国内のユーザを対象とした複数のWebサイトでvawtrakを取得しました。該当のWebサイトはいずれもトップページのHTMLファイルが改ざんされ、iframeタグを不正に挿入されていました。Webサイト閲覧者はこのiframeタグによって外部のWebサーバに誘導され、最終的にNuclear Exploit KitやAngler Exploit Kitを用いたドライブバイダウンロードによってvawtrakなどのマルウェアに感染させられてしまいます。

海外では、メールなどによってvawtrakが配布されていることが報告されています[*68]。日本国内では、主に改ざんされたWebサイトを経由したドライブバイダウンロードによって感染を広げているものと推測されます。

なお、改ざんされていたWebサイトのうち1件は、日本国内の著名なコンテンツプロバイダのグループ企業で、4月下旬から6月中旬まで、及び7月中旬から下旬までの期間、改ざんされた状態が断続的に観測されました。このような著名Webサイトを含む複数のWebサイトで、改ざんされた状態が長期間継続していることを観測しています。

※復号処理後に最初の4バイト「ECFG」の文字列(青枠部)をチェックする処理が行われているため、これはDynamic Configの冒頭を示すマジックワードとして用いられていると考えられる。ちなみに、ECFGはExtended ConfigまたはEncrypted Configを示す略語と推測される。この図では、標的となった金融機関それぞれについて、固有の情報については黒く塗りつぶしてある。

図-14 取得したvawtrakのDynamic Configの一部(復号済み・赤枠部は国内の金融機関などのサービスを示すURL)

*66 本稿執筆中(2014年8月1日)に収集したDynamic Configには、更に複数の地方銀行やクレジットカード会社のURLが追加されていた。

*67 RapportはTrusteer社のWebインジェクションやフィッシングなどオンラインバンキングの脅威対策に特化したマルウェア対策ソフトウェア(http://www.trusteer.com/ja/products/trusteer-rapport-for-online-banking-ja)。なお、Trusteer社はブログ記事「Carberp's Attempt to Bypass Trusteer Rapport is Effectively Resisted(http://www.trusteer.com/blog/carberps-attempt-to-bypass-trusteer-rapport-is-effectively-resisted)」を通じて、Carberpというマルウェアがvawtrakと同様にRapportの無効化を試みる仕組みについて、Rapportはマルウェアの意図するような影響を受けないとしている。

*68 例えばカスペルスキー社のブログ「Online Banking Faces a New Threat (http://securelist.com/blog/57881/online-banking-faces-a-new-threat/)」ではスパムメールを介して感染を広げている旨が記述されている。

■ 対策

ドライブバイダウンロードによるマルウェア感染を防止するためには、クライアントPCのOS、ブラウザ、及び関連プラグインを常に最新の状態に更新し、脆弱性のない状態に保つことが重要です。また、クライアントOSがWindowsの場合には、ソフトウェアの制限ポリシーを用いてプログラムの実行可能領域を制限したり、EMETをインストールして脆弱性の影響を緩和しておくことも効果的です[*69]。

万が一、vawtrakに感染してしまった場合には、クリーンインストールなどのパソコン復旧対応だけでなく、パソコンで利用していたデジタル証明書の失効処理と、パソコン上のクライアントアプリケーションで利用していた各種アカウントのパスワード変更が必要です。更に、該当パソコンでオンラインバンキングやSNSなどのWebサービスを利用していた場合は、それらのサービスのアカウント情報やサービス上でやりとりした情報についても、漏えいした可能性を念頭に、適宜変更や削除などの対処を行う必要があります。

一方、Webサイト運営者、管理者の立場では、サイトが改ざんされExploit Kitの誘導元にならないよう、運用に注力する責任があると考えるべきです。Webサーバ、コンテンツ管理システムやそのプラグイン、あるいはそれらが依存するフレームワークなど、利用しているシステムを網羅的に把握し、脆弱性攻撃の影響を受けないよう管理する必要があります。また、CDNや広告サービス、アクセス解析サービスなど、自社Webサイトに関連する外部（社外）リソースがセキュリティ侵害を受けたことにより、Webサイト閲覧者をマルウェア感染の危機に晒してしまうケース[*70]も散見されます。自社のシステムの診断を重ね、防御を固めるだけでは、このような外部システムに起因する脅威を排除することはできません。提供しているサービスの性質にもよりますが、完全性を担保できない外部リソースについては、その重要度に応じて内製化や廃止などを検討しておくことを推奨します。その上で、外部リソースの利用を継続する場合には、問題を少しでも早く直接把握するために、定期的に外部からWebサイトを閲覧し、実際にクライアントPCにダウンロードされるコンテンツを確認しておくことを推奨します。

1.4.3 クラウドの安全性確認と監査制度

ここでは、利用者がクラウドサービスを安心して利用するために公開されている、各種ガイドの利用について検討すると共に、クラウドセキュリティ推進協議会で検討されている「クラウド情報セキュリティ監査制度」について解説します。

表-3 vawtrakの特徴的な機能及びZeuS、Ponyとの対比

	vawtrak	Zeus（2.0.8.9）	Pony（1.9）	備考
パソコンに保存された認証情報の取得	✔	✔	✔	vawtrakとPony1.9は対象とするクライアントアプリケーション（約100種）がほぼ一致。ZeuSは20種程度で種類も異なる。また、Pony2.0とは一致しない。
パソコンに保存されたデジタル証明書の取得	✔	✔	✔	
Dynamic Config	✔	✔		設定の書式は異なる。
Webinject	✔	✔		
内部に保持する文字列の難読化	✔	✔		
Report機能	✔	✔		
SOCKS Proxy	✔	✔		
VNC Server	✔	✔		
32bit/64bit両対応	✔			
ソフトウェア制限ポリシーを用いたマルウェア対策ソフトウェアの動作妨害	✔			
Rapportの無効化の試行	✔			

*69 クライアント環境におけるマルウェア感染対策については、IIR Vol21（http://www.iij.ad.jp/company/development/report/iir/021.html）の「1.4.1 標的型攻撃で利用されるRAT「PlugX」」末尾で詳しく紹介している。

*70 例えば、次のSymantec社のSecurity Response Blogでは、CDNサービスを利用していた正規のWebサイトが侵害され、悪用された事件の詳細について解説している。「Adobe Flashの脆弱性を悪用して日本のユーザーの銀行口座情報を狙う攻撃」（http://www.symantec.com/connect/ja/blogs/adobe-flash-2）。

■ クラウドセキュリティに関するガイド

2006年にクラウドコンピューティングの概念が提唱されてから既に8年が経過しました。その後、クラウドコンピューティング技術を使ったサービス(以下クラウドサービス)が続々と提供され、広く一般に利用されています。しかし、当初よりその安全性については様々な疑問が投げかけられており、クラウドサービス導入の障壁としてセキュリティへの懸念が筆頭に挙げられていました。実際に、国内外を問わず大規模な情報セキュリティ事故が発生したことは記憶に新しいところです。その後様々な議論を経て、現在では、各種の団体からクラウドを安全に提供・利用するためのガイドなどが公表されています。ここで、表-4に代表的なガイドなどを例示し、その概要を説明します。

このように、クラウドセキュリティに関するガイドは様々な組織、団体から発行されています。ガイドの数が多くなると目的に合ったガイドの選択が難しくなる面はありますが、以前と比べて容易に情報が入手できるようになったことは歓迎すべきことです。

■ ガイド利用時の注意点

これらのガイドには、クラウドサービスを利用、もしくは提供する上で検討すべきセキュリティ事項に関しての有用な情報が数多く含まれており、チェックリストとしても広く活用されています。しかし、ガイドの対象者(利用者や事業者)、対象物(サービスや情報)をあいまいにすると様々な解釈が可能となり、誤解や混乱が起きやすくなります。

表-4 クラウドを安全に提供・利用するための代表的なガイドなど

タイトル	発行組織	発行年月	概要
クラウドサービス提供における情報セキュリティ対策ガイドライン*71	総務省	2014年4月	主にクラウドサービスの事業者に対して、どのように情報セキュリティ対策を行うべきか、どのような情報を公開すべきか、といったことを、実務的な観点からまとめたガイドです。
クラウドサービス利用者の保護とコンプライアンス確保のためのガイド*72	ASP・SaaS・クラウドコンソーシアム	2011年7月	主に企業がパブリッククラウドサービスを利用する場合において、適切なリスクマネジメントを行うためには何を考えるべきかが説明されています。
IaaS・PaaSの安全・信頼性に係る情報開示認定制度*73	マルチメディア振興センター	2012年8月	IaaS/PaaS事業者が安全・信頼性についての情報を適切に開示していることを認定するための仕組みです。同様の制度として、ASP・SaaS及びデータセンターの情報開示認定制度があります。
クラウドサービス利用のための情報セキュリティマネジメントガイドライン*74	経済産業省	2011年4月発行、2014年3月改訂	ISO/IEC27002をベースとしてクラウドサービスのセキュリティ管理基準を定めたものです。主に利用者を対象としていますが、事業者が利用者の要求に対してどのように答えるべきかといったことも記載されています。
金融機関などコンピュータシステムの安全対策基準・解説書(第8版追補)*75	金融情報システムセンター	2013年3月	従来の金融機関向けのセキュリティ指針に、クラウドを利用する際に検討すべき事項を追補として記載したものです。金融機関がクラウドサービスを利用する場合のリスクアセスメントに関して記載されています。
CSA Cloud Control Matrix(CCM)*76	Cloud Security Alliance	2014年7月 V3.0.1	CSAが発行している「クラウドセキュリティガイダンス」で記載されたコントロールと、その実装方針をまとめたものです。CCMで記載されたコントロールと、その他各種標準との対応づけもされています。
ISO/IEC CD 27017 Information technology – Security techniques – Code of practice for information security controls for cloud computing services based on ISO/IEC 27002*77	国際標準化機構(ISO)	2015年10月発行予定	現在協議中のクラウドセキュリティに関する国際標準です。ISO/IEC 27002を元にして、利用者や事業者がクラウドセキュリティの実装に必要なコントロールが追加されています。

*71 総務省、「クラウドサービス提供における情報セキュリティ対策ガイドライン」(http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000073.html)。
*72 ASP・SaaS・クラウドコンソーシアム、「クラウドサービス利用者の保護とコンプライアンス確保のためのガイド」(http://aspicjapan.org/information/guideline/pdf/jp_ver1.0.pdf)。
*73 マルチメディア振興センター、「IaaS・PaaSの安全・信頼性に係る情報開示認定制度」(http://www.fmmc.or.jp/ip-nintei/)。
*74 経済産業省、「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」初版(http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html)。2014年3月改訂版、及びガイドライン(http://www.meti.go.jp/press/2013/03/20140314004/20140314004.html)。
*75 金融情報システムセンター、「金融機関等コンピュータシステムの安全対策基準・解説書(第8版追補)」(https://www.fisc.or.jp/publication/disp_target_detail.php?pid=266)。
*76 Cloud Security Alliance、"CSA CCM"(https://cloudsecurityalliance.org/research/ccm/)。日本語版は(http://www.cloudsecurityalliance.jp/ccm_wg.html)。
*77 International Organization for Standardization、"ISO/IEC CD 27017 Information technology -- Security techniques -- Code of practice for information security controls for cloud computing services based on ISO/IEC 27002"(http://www.iso.org/iso/catalogue_detail.htm?csnumber=43757)。

例えば「特権アカウント」は、「クラウドサービスを提供している事業者がサービス全体の維持や保守に使うアカウント(1)」、「サービス事業者の情報システム部が持っている特権アカウント(2)」、「利用者がIaaSで利用している仮想マシンのroot(Administrator)アカウント(3)」、「SaaSでユーザ登録、削除などの保守を行うアカウント(4)」などの解釈が可能です。参照したガイドが利用者用ガイドであれば、「特権アカウント」は(3)もしくは(4)、事業者用ガイドであれば(1)もしくは(2)となります。解釈の違いによりチェックリストの設問の意味合いが異なるため、適切なリスク評価やサービス利用ができなくなる恐れがあります。

適切なリスク評価を行うための1つの方法は、対象者と対象物を明確にして事業者と利用者で合意をとることです。例えば、「特権アカウント」は利用するサービスの保守用アカウントのことである、ということを(利用者からでも事業者からでも、どちらからでもよいので)明確にして合意します。事業者と利用者のコミュニケーションが発生するため、時間や手間がかかりますが、認識のずれや思い込みを減らすことはできます。ただし、クラウドサービスの特徴である自動化を阻害しますし、すべての事業者がこのような個別の対応に答えてくれるとは限りません。

別の方法は、事業者が開示している情報を探してそのまま利用することです。どのようなセキュリティ機能が提供され、どのようなセキュリティ対策が取られているか、各事業者が何らかの形で公開していますので、これらの公開情報から、利用者の求めるセキュリティ水準が維持できるかを利用者自身で判断します。一般的なクラウドサービスによく見られるこの方法は、時間がかからず手軽である反面、事業者が公開可能とする情報や粒度がまちまちで、望んだ内容の回答が得られなかったり、回答の信頼性に関しての確認が難しかったりします。

他にも、SSAE16報告書などを利用する方法もあります。事業者は外部監査人に対してのみ情報を公開し、利用者は事業者の統制状態について第三者からの信頼できる評価結果を受け取ることが可能です。利用者、事業者共に利点がある方法ですが、この方法は外部監査人に対して非常に高度なIT知識を要求することや、事業者が支払うコスト負担が大きくなる(ひいてはサービス価格の上昇につながる)ことから、幅広くクラウドサービスで対応することは困難です。

これら様々な課題を解決し、適切なリスク評価を行う方法として、クラウド事業者が共通の基準に従ってセキュリティを評価し、信頼できる情報を開示する取り組みが始まっています。次にその取り組みを紹介します。

■ クラウド情報セキュリティ監査制度

クラウドサービスを利用するということは、多数の利用者が資源を共同で利用するためにサービス事業者が用意したシステムを決められた使い方で利用するということです。従って、システムインテグレーションのように、利用者のシステム環境が専用で構築され、その構成や運用体制の詳細が明かされるといったことはありません。また、クラウドサービスは環境が動的に変化するため、その仕組みの内部を推測することにも意味はありません。コストをかけて監査を行ったとしても、事業者が利用者にすべての仕組みを明らかにすることはありません。クラウドサービスを「ブラックボックス」として利用することは避けられません。従来型のオンプレミス企業システムを前提としたセキュリティやリスク評価の考え方がクラウドサービスに適用しづらいのは、これが一因と言えます。

そこで、2013年4月に、日本セキュリティ監査協会(以下JASA)を発起人としてクラウドサービスに関連する事業者など25社が集まり、「JASA-クラウドセキュリティ推進協議会(以下J-CISPA)」が発足しました。JASAでは従来の情報セキュリティ監査制度をベースとして、それをクラウドコンピューティングに適用した、「クラウド情報セキュリティ管理基準」を2012年9月に公開しています。そこで定められている基準を元に、クラウドサービスに適したシステム監査を行い、適切なリスク管理を行うための情報を利用者に提供しようとしています。この試みは世界に先駆けて行われており、J-CISPAでは、活動で得られた知見を元に、クラウドセキュリティの国際標準として検討中のISO27017やISO27036-4への提案なども積極的に行っています。

J-CISPAで想定されている監査の仕組みを図-15と共に説明します。

J-CISPAでは、一般的にクラウドサービスで懸念されるリスク(表-5)を定めています。まず、クラウド事業者はそれらリスクに対してどのように対応しているかを明らかにして文書化します。その文書を「言明書」と呼びます。サンプルとして、IIJがパイロット監査(後述)で行った言明書を図-16に示します。次に、言明書で書かれた内容に対して、JASAで定める監査人資格を持った内部監査人が、言明書の内容に関して監査を行い、監査結果を記録します。内部監査人は、JASAの有識者WGで検討されたクラウド内部監査標準手続に定められた監査手続きを使って監査を行います。監査内容や手続きが詳細に定義されていますので、監査人が異なる場合でも監査品質は変わりません。共通の監査基準を利用することで、異なる事業者、異なるサービスでも、リスクにどう対応しているかの比較が行いやすくなります。

なお、この仕組みは、内部監査人が監査を行うことを前提としています。クラウドサービスの仕組みは発展途上であり、時々刻々と変わっていくため、IT技術に精通した専門家でなければ監査の情報が正しいかどうかを判断することが困難です。サービス事業者の内部監査人であれば正確なサービス知識を持った上での判断を行うことが可能であり、これも一定の監査品質を確保することに役立っています。加えて、クラウド事業者は自社のサービスに関する秘密情報を外部に出さなくてもよくなるため、事業者の負担も軽減されます。

しかし、いくら認定された内部監査人が決まった手続きで監査を行うとしても、利用者から見た場合には、ただの自己主張であることに変わりはありません。そこで、この監査制度では内部監査結果をうまく利用する形で外部監査を取り入れています。具体的には、内部監査で得られた「内部監査報告書」などを元に内部監査が正しい手続きで行われたものであるかどうかを外部監査人が検証するというものです。内部監査として技術的に確かな内容で、手続きや書式が均一の監査報告書が残るため、外部監査では「内部監査が正しく行われたかどうか」を監査すればよいということになります。

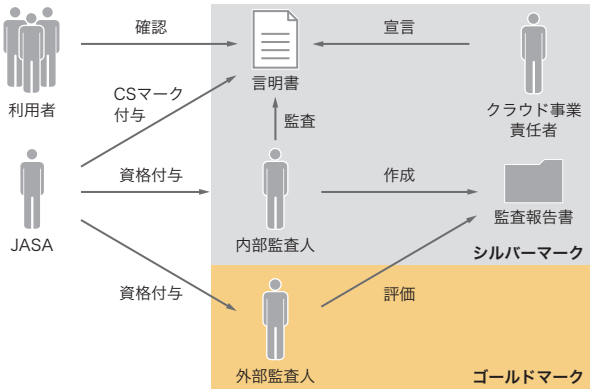


図-15 クラウドセキュリティ監査におけるそれぞれの役割

本監査制度ではこの2段階の仕組みを取り入れることで、クラウドサービスに関する技術情報の正確な判断と、正確な監査手続きを、可能な限り低コストで両立させようとしています。コストを抑えることでより多くのクラウドサービスが本制度に対応可能となります。J-CISPAでは内部監査人により監査された言明書にシルバーマーク、その結果が外部監査人により検証された場合はゴールドマーク、という形でマークを発行します。2013年度に、協議会のクラウドサービス事業者各社が「パイロット監査」として、この仕組みを試行しており、今年度は、この結果を元に本監査を行うべく、精力的に準備が行われています。

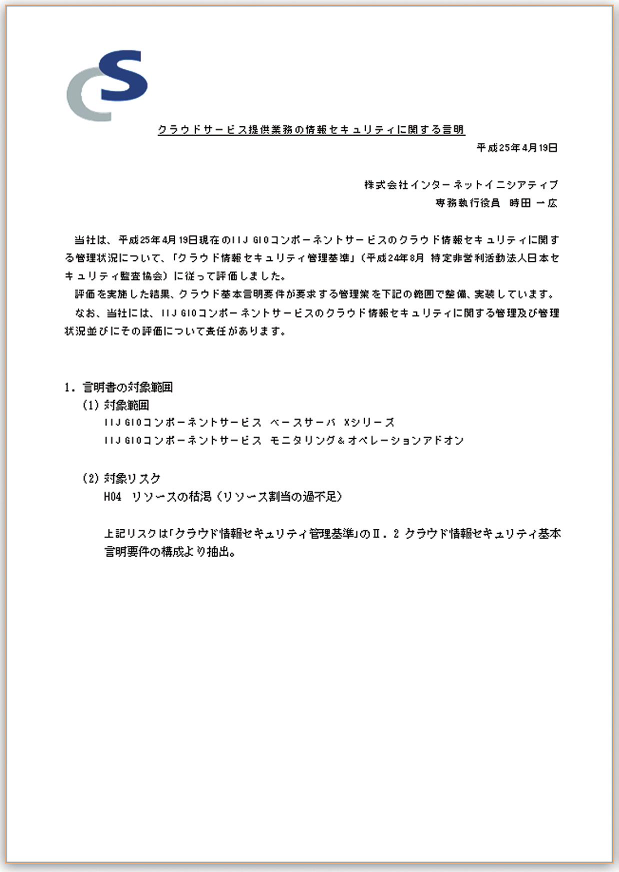
クラウドサービスを安心して利用していただくために、IIJはこのような新しい制度や国内、国際的なルール作りをこれからも積極的に推進して参ります。

表-5 クラウドサービスで懸念されるリスク(J-CISPAの資料から引用)

リスクの重大性	番号	リスクの識別名
高	H01	リソース・インフラの高集約によるインシデントの影響の拡大
	H02	仮想／物理の設計・運用の不整合
	H03	他の共同利用者の行為による信頼の喪失
	H04	リソースの枯渇(リソース割当の過不足)
	H05	隔離の失敗
	H06	サービスエンジンの侵害
中	M07	クラウドプロバイダでの内部不正ー特権の悪用
	M08	管理用インタフェースの悪用(操作、インフラストラクチャアクセス)
	M09	データ転送途上における攻撃、データ漏えい(アップロード時、ダウンロード時、クラウド間転送)
	M10	セキュリティが確保されていない、または不完全なデータ削除
	M11	クラウド内DDoS/DoS攻撃
低	L12	ロックインによるユーザの忌避
	L13	ガバナンスの喪失
	L14	サプライチェーンにおける障害
	L15	EDoS攻撃(経済的な損失を狙ったサービス運用妨害攻撃)
	L16	事業者が管理すべき暗号鍵の喪失
	L17	不正な探査・スキャンの実施
	L18	証拠提出命令と電子的証拠開示
	L19	司法権の違い
	L20	データ保護
	L21	ライセンス

1.5 おわりに

このレポートは、IIJが対応を行ったインシデントについてまとめたものです。今回は、OpenSSLの脆弱性、国内金融機関の認証情報などを窃取するマルウェア「vawtrak」、クラウドの安全性確認と監査制度についてまとめました。IIJでは、このレポートのようにインシデントとその対応について明らかにして公開していくことで、インターネット利用の危険な側面を伝えるように努力しています。このような側面についてご理解いただき、必要な対策を講じた上で、安全かつ安心してインターネットを利用できるように継続的に努力して参ります。


クラウドサービス提供業務の情報セキュリティに関する言明

平成25年4月19日

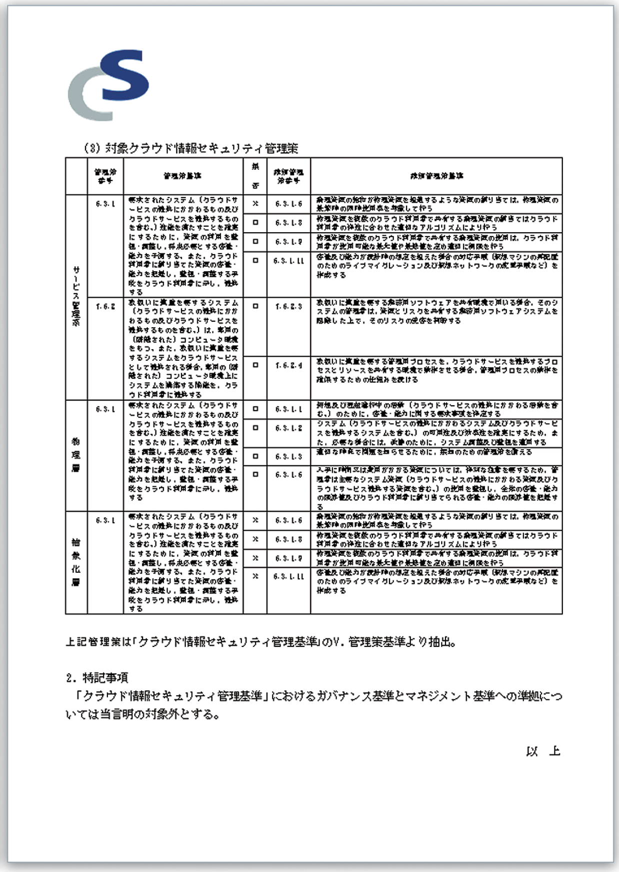
株式会社インターネットイニシアティブ
専務執行役員　時田 一広

当社は、平成25年4月19日現在のIIJ GIOコンポーネントサービスのクラウド情報セキュリティに関する管理状況について、「クラウド情報セキュリティ管理基準」（平成24年8月 特定非営利活動法人日本セキュリティ監査協会）に従って評価しました。
評価を実施した結果、クラウド基本言明要件が要求する管理策を下記の範囲で整備、実装しています。
なお、当社には、IIJ GIOコンポーネントサービスのクラウド情報セキュリティに関する管理及び管理状況並びにその評価について責任があります。

1．言明書の対象範囲
(1) 対象範囲
IIJ GIOコンポーネントサービス　ベースサーバ　Xシリーズ
IIJ GIOコンポーネントサービス　モニタリング＆オペレーションアドオン

(2) 対象リスク
H04　リソースの枯渇（リソース割当の過不足）

上記リスクは「クラウド情報セキュリティ管理基準」のⅡ．2 クラウド情報セキュリティ基本言明要件の構成より抽出。


(3) 対象クラウド情報セキュリティ管理策

	管理策番号	管理策基準	採否	詳細管理策番号	詳細管理策基準
サービス管理系	6.3.1	要求されたシステム（クラウドサービスの提供にかかわるもの及びクラウドサービスを提供するものを含む。）性能を満たすことを確実にするために、資源の利用を監視・調整し、将来必要とする容量・能力を予測する。また、クラウド利用者に割り当てた資源の容量・能力を把握し、監視・調整する手段をクラウド利用者に示し、提供する	※	6.3.1.6	論理資源の総和が物理資源を超過するような資源の割り当ては、物理資源の最繁時の同時使用率を考慮して行う
			□	6.3.1.8	物理資源を複数のクラウド利用者で共有する論理資源の割当てはクラウド利用者の特性に合わせた適切なアルゴリズムにより行う
			□	6.3.1.9	物理資源を複数のクラウド利用者で共有する論理資源の使用は、クラウド利用者が使用可能な最大値や最低値を定め適切に制限を行う
			□	6.3.1.11	容量及び能力が設計時の想定を超えた場合の対応手順（仮想マシンの再配置のためのライブマイグレーション及び仮想ネットワークの変更手順など）を作成する
	11.6.2	取扱いに慎重を要するシステム（クラウドサービスの提供にかかわるもの及びクラウドサービスを提供するものを含む。）は、専用の（隔離された）コンピュータ環境をもつ。また、取扱いに慎重を要するシステムをクラウドサービスとして提供される場合、専用の（隔離された）コンピュータ環境上にシステムを構築する機能を、クラウド利用者に提供する	□	11.6.2.3	取扱いに慎重を要する業務用ソフトウェアを共有環境で用いる場合、そのシステムの管理者は、資源とリスクを共有する業務用ソフトウェアシステムを識別した上で、そのリスクの受容を判断する
			□	11.6.2.4	取扱いに慎重を要する管理用プロセスを、クラウドサービスを提供するプロセスとリソースを共有する環境で動作させる場合、管理用プロセスの動作を確保するための仕組みを設ける
物理層	6.3.1	要求されたシステム（クラウドサービスの提供にかかわるもの及びクラウドサービスを提供するものを含む。）性能を満たすことを確実にするために、資源の利用を監視・調整し、将来必要とする容量・能力を予測する。また、クラウド利用者に割り当てた資源の容量・能力を把握し、監視・調整する手段をクラウド利用者に示し、提供する	□	6.3.1.1	新規及び現在進行中の活動（クラウドサービスの提供にかかわる活動を含む。）のために、容量・能力に関する要求事項を特定する
			□	6.3.1.2	システム（クラウドサービスの提供にかかわるシステム及びクラウドサービスを提供するシステムを含む。）の可用性及び効率性を確実にするため、また、必要な場合には、改善のために、システム調整及び監視を適用する
			□	6.3.1.3	適切な時期で問題を知らせるために、検知のための管理策を備える
			□	6.3.1.6	入手に時間又は費用がかかる資源については、特別な注意を要するため、管理者は主要なシステム資源（クラウドサービスの提供にかかわる資源及びクラウドサービス提供する資源を含む。）の使用を監視し、全体の容量・能力の限界値及びクラウド利用者に割り当てられる容量・能力の限界値を把握する
抽象化層	6.3.1	要求されたシステム（クラウドサービスの提供にかかわるもの及びクラウドサービスを提供するものを含む。）性能を満たすことを確実にするために、資源の利用を監視・調整し、将来必要とする容量・能力を予測する。また、クラウド利用者に割り当てた資源の容量・能力を把握し、監視・調整する手段をクラウド利用者に示し、提供する	※	6.3.1.6	論理資源の総和が物理資源を超過するような資源の割り当ては、物理資源の最繁時の同時使用率を考慮して行う
			※	6.3.1.8	物理資源を複数のクラウド利用者で共有する論理資源の割当てはクラウド利用者の特性に合わせた適切なアルゴリズムにより行う
			※	6.3.1.9	物理資源を複数のクラウド利用者で共有する論理資源の使用は、クラウド利用者が使用可能な最大値や最低値を定め適切に制限を行う
			※	6.3.1.11	容量及び能力が設計時の想定を超えた場合の対応手順（仮想マシンの再配置のためのライブマイグレーション及び仮想ネットワークの変更手順など）を作成する

上記管理策は「クラウド情報セキュリティ管理基準」のV．管理策基準より抽出。

2．特記事項
「クラウド情報セキュリティ管理基準」におけるガバナンス基準とマネジメント基準への準拠については当言明の対象外とする。

以　上

図-16 パイロット監査における言明書の例

執筆者:

齋藤 衛(さいとう まもる)
IIJ サービス本部 セキュリティ情報統括室 室長。法人向けセキュリティサービス開発などに従事の後、2001年よりIIJグループの緊急対応チームIIJSECTの代表として活動し、CSIRTの国際団体であるFIRSTに加盟。Telecom-ISAC Japan、日本シーサート協議会、日本セキュリティオペレーション事業者協議会など、複数の団体の運営委員を務める。

土屋 博英(1.2 インシデントサマリ)
土屋 博英、永尾 禎啓、鈴木 博志、梨和 久雄(1.3 インシデントサーベイ)
小林 直(1.4.1 OpenSSLの脆弱性)
梨和 久雄、鈴木 博志(1.4.2国内金融機関の認証情報などを窃取するマルウェア「vawtrak」)
加藤 雅彦(1.4.3クラウドの安全性確認と監査制度)
IIJサービスオペレーション本部 セキュリティ情報統括室

協力:
根岸 征史、須賀 祐治、春山 敬宏、小林 稔、桃井 康成　IIJ サービスオペレーション本部 セキュリティ情報統括室

この1年でトラフィック量は着実に増加、HTTPSの利用が拡大

この1年間のブロードバンドトラフィックを見ると、ダウンロード量は27%、アップロード量も13%増加して、着実にトラフィック量が増えています。
また、トラフィックのほとんどを占めるようになったWebトラフィックにおいては、プライバシー保護の意識の高まりからHTTPSを利用する傾向にあり、今後もこの割合が増えて行くと予想します。

2.1 概要

本レポートでは、毎年、IIJが運用しているブロードバンド接続サービスのトラフィックを分析して、その結果を報告しています[*1*2*3*4*5]。今回も、利用者の1日のトラフィック量やポート別使用量などを基に、この1年間のトラフィック傾向の変化を報告します。

図-1は、IIJのブロードバンドサービス全体の過去7年間の月平均トラフィックについて、最大値を1として正規化して示したグラフです。2010年1月のトラフィック減少は、2010年1月に施行された改正著作権法、いわゆるダウンロード違法化の影響だと考えられています。それ以降、ダウンロード量(OUT)が増えている一方で、アップロード量(IN)は横ばいとなっていて、P2Pファイル共有のトラフィック割合が減っていることが窺えます。2012年10月には、違法ダウンロードの刑事罰化を含む改正著作権法が施行され、その前後でトラフィックの増減が観測されました。それ以降、ダウンロード量は以前にも増して伸びていて、アップロード量も僅かながら増加傾向にあります。この1年のトラフィック量は、INは13%の増加、OUTは27%の増加となっています。

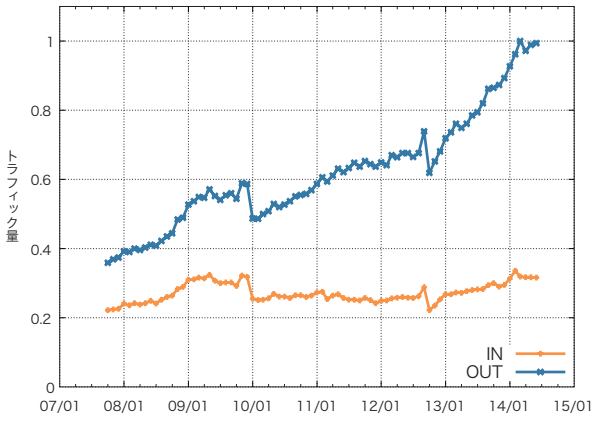


図-1 過去7年間のブロードバンドトラフィック量の推移

2.2 データについて

今回も前回までと同様に、個人及び法人向けのブロードバンド接続サービスについて、ファイバーとDSLによるブロードバンド顧客を収容するルータでSampled NetFlowにより収集した調査データを利用しています。ブロードバンドトラフィックは平日と休日で傾向が異なるため、1週間分のトラフィックを解析しています。今回は、2014年5月26日～6月1日の1週間分のデータを、前回解析した2013年6月3日～9日の1週間分と比較します。

各利用者の使用量は、利用者に割り当てられたIPアドレスと、観測されたIPアドレスを照合して求めています。また、NetFlowではパケットをサンプリングして統計情報を取得しています。サンプリングレートは、ルータの性能や負荷を考慮して、1/8192に設定されています。観測された使用量に、サンプリングレートの逆数を掛けることで全体の使用量を推定しています。サンプリングによって、使用量の少ない利用者のデータには少し誤差がでますが、ある程度以上使用量のある利用者に対しては統計的に意味のある数字が得られます。

IIJの提供するブロードバンドサービスにはファイバー接続とDSL接続がありますが、今ではファイバー接続の利用がほとんどとなっていて、2014年には観測されたユーザ数

＊1　長健二朗. ブロードバンドトラフィックレポート：違法ダウンロード刑事罰化の影響は限定的. Internet Infrastructure Review. vol.20. pp32-37. August 2013.
＊2　長健二朗. ブロードバンドトラフィックレポート：この1年間のトラフィック傾向について. Internet Infrastructure Review. vol.16. pp33-37. August 2012.
＊3　長健二朗. ブロードバンドトラフィックレポート：マクロレベルな視点で見た、震災によるトラフィックへの影響. Internet Infrastructure Review. vol.12. pp25-30. August 2011.
＊4　長健二朗. ブロードバンドトラフィックレポート：P2Pファイル共有からWebサービスへシフト傾向にあるトラフィック. Internet Infrastructure Review. vol.8. pp25-30. August 2010.
＊5　長健二朗. ブロードバンドトラフィック：増大する一般ユーザのトラフィック. Internet Infrastructure Review. vol.4. pp18-23. August 2009.

の95%はファイバー利用者で、トラフィック量全体の97%を占めています。

なお、本レポート中のトラフィックのIN／OUTはISPから見た方向を表し、INは利用者からのアップロード、OUTは利用者へのダウンロードとなります。

2.3 利用者の1日の使用量

まずは、ブロードバンド利用者の1日の利用量をいくつかの切口から見ていきます。ここでの1日の利用量は各利用者の1週間分のデータの1日平均です。

図-2は、利用者の1日の平均利用量の分布（確率密度関数）を示します。アップロード（IN）とダウンロード（OUT）に分け、利用者のトラフィック量をX軸に、その出現確率をY軸に示していて、2013年と2014年を比較しています。X軸はログスケールで、10KB（10^4）から100GB（10^{11}）の範囲を示しています。一部の利用者はグラフの範囲外にありますが、概ね100GB（10^{11}）までの範囲に分布しています。

INとOUTの各分布は、片対数グラフ上で正規分布となる、対数正規分布に近い形をしています。これはリニアなグラフで見ると、左端近くにピークがあり右へなだらかに減少するいわゆるロングテールな分布です。OUTの分布はINの分布より右にずれていて、ダウンロード量がアップロード量より、ひと桁以上大きくなっています。2013年と2014年で比較すると、INとOUT共に分布の山が右に少し移動していて、利用者全体のトラフィック量が増えていることが分かります。昨年の2012年と2013年の比較より移動量が増えていて、トラフィック量の増加率が大きくなっています。

OUTの分布を見ると、分布のピークはここ数年間で着実に右に移動していますが、右端のヘビーユーザの使用量はあまり増えていないので、分布の対称性が崩れてきています。一方で、INの分布は右側の裾が広がっています。以前は、ここによりはっきりした山がINとOUT両方にあり、IN／OUT量が対称なヘビーユーザを示していました。そこで便宜上、大多数のIN／OUT非対称な分布を「クライアント型利用者」、右側の小数のIN／OUT対称なヘビーユーザの分布を「ピア型利用者」と呼んできました。今回もその慣習に従います。ここ数年で、ピア型利用者の山は小さくなりほとんど識別できなくなりました。これは、ヘビーユーザの割合が減少していることを示しています。グラフ左側に少しヒゲが出ていますが、これはサンプリングレートの影響によるノイズで、1パケットのみ観測された場合の最小パケットサイズ及び最大パケットサイズに相当しています。

表-1は、平均値と、分布の山の頂点にある最頻出値の推移を示します。分布の最頻出値を2013年と2014年で比較すると、INでは18MBから28MBに、OUTでは355MBから447MBに増えていて、各利用者のトラフィック量が、特にダウンロード側で増えていることが分かります。一方、平均値はグラフ右側のヘビーユーザの使用量に引っ張ら

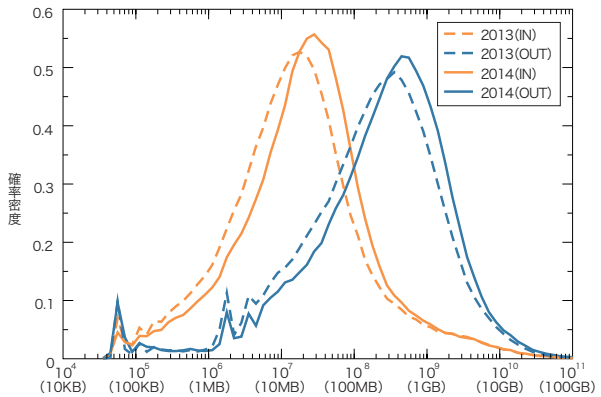


図-2 利用者の1日のトラフィック量分布 2013年と2014年の比較

	IN（MB/day）		OUT（MB/day）	
年	平均値	最頻出値	平均値	最頻出値
2005	430	3.5	447	32
2007	433	4	712	66
2008	483	5	797	94
2009	556	6	971	114
2010	469	7	910	145
2011	432	8.5	1,001	223
2012	410	14	1,026	282
2013	397	18	1,038	355
2014	437	28	1,287	447

表-1 利用者の1日のトラフィック量の平均値と最頻出値の推移

れるので、2014年には、INの平均は437MB、OUTの平均は1,287MBと、最頻出値よりかなり大きな値になります。2013年には、それぞれ397MBと1,038MBでした。2010年以降減少していたINが増加に転じて、P2Pファイル共有からWebサービスへの移行が一段落したように思われます。

図-3は、利用者ごとのIN／OUT使用量から5,000人をランダムに抽出してプロットしています。X軸はOUT（ダウンロード量）、Y軸はIN（アップロード量）で、共にログスケールです。利用者のIN／OUTが同量であれば対角線上にプロットされます。

対角線の下側に対角線に沿って広がるクラスタは、ダウンロード量がひと桁多いクライアント型の一般ユーザです。以前は、右上の対角線上あたりを中心に薄く広がるピア型のヘビーユーザのクラスタがはっきり分かりましたが、今

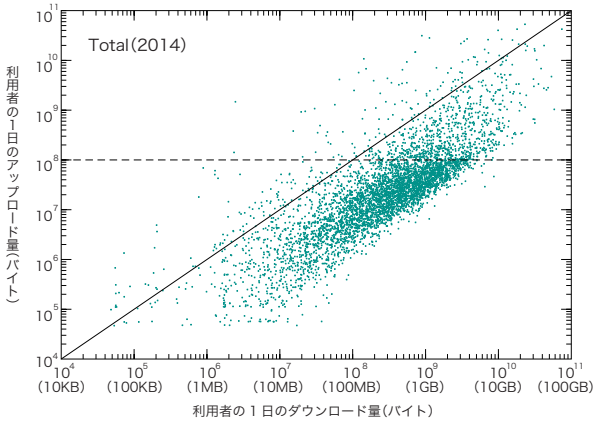


図-3 利用者ごとのIN/OUT使用量

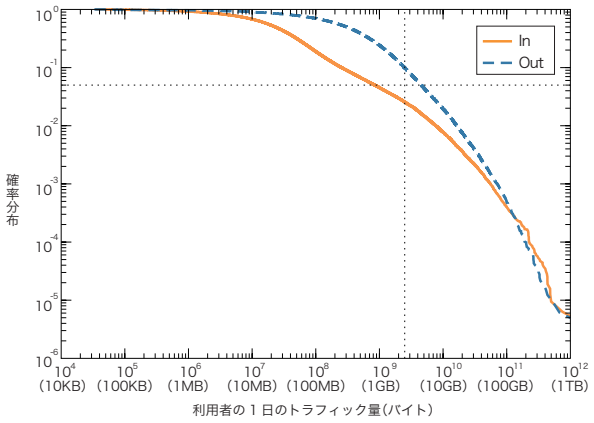


図-4 利用者の1日のトラフィック量の相補累積度分布

では識別ができなくなっています。便宜上、クライアント型とピア型に分けましたが、実際には、クライアント型の一般ユーザでもSkypeなどのピア型のアプリケーションを利用し、また一方のピア型のヘビーユーザもWebなどのダウンロード型のアプリケーションを利用しているので、その境界はあいまいです。つまり、多くの利用者は両タイプのアプリケーションを異なる割合で使用しています。また、各利用者の使用量やIN／OUT比率にも大きなバラツキがあり、多様な利用形態が存在することが窺えます。ここでは、2013年と比較しても、ほとんど違いは確認できません。

図-4は、利用者の1日のトラフィック量を相補累積度分布にしたものです。これは、使用量がX軸の値より多い利用者の、全体に対する割合をY軸に、ログ・ログスケールで示したもので、ヘビーユーザの分布を見るのに有効です。グラフの右側が直線的に下がっていて、ベキ分布に近いロングテールな分布であることが分かります。いずれにせよ、ヘビーユーザは統計的に分布していて、決して一部の特殊な利用者ではないと言えます。

図-5は、利用者間のトラフィック使用量の偏りを示します。使用量上位X%の利用者が、全体トラフィック量のY%を占めることを表します。使用量には大きな偏りがあり、結果として全体は一部利用者のトラフィックで占められています。例えば、上位10%の利用者がOUTの68%、INの93%を占めています。更に、上位1%の利用者がOUTの30%、INの65%を占めています。ここ数年のヘビーユーザ割合の減少に伴い、僅かながら偏りは減ってきています。

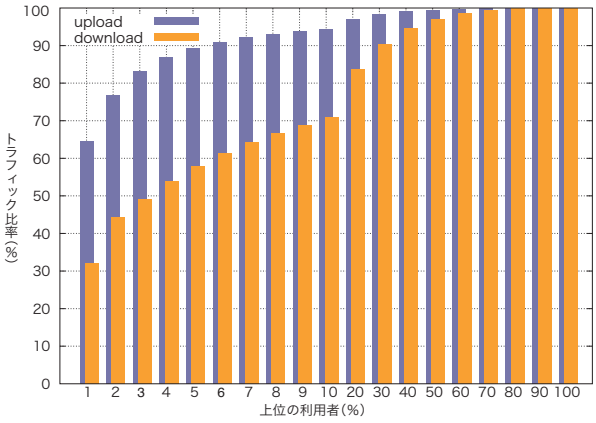


図-5 利用者間のトラフィック使用量の偏り

2.4 ポート別使用量概要

次に、トラフィックの内訳をポート別の使用量から見ていきます。最近では、ポート番号からアプリケーションを特定することは困難です。P2P系アプリケーションには、双方が動的ポートを使うものが多く、また、多くのクライアント・サーバ型アプリケーションが、ファイアーウォールを回避するため、HTTPが使う80番ポートを利用します。大雑把に分けると、双方が1024番以上の動的ポートを使っていればP2P系のアプリケーションの可能性が高く、片方が1024番未満のいわゆるウェルノウンポートを使っていれば、クライアント・サーバ型のアプリケーションの可能性が高いと言えます。そこで、TCPとUDPで、ソースとデスティネーションのポート番号の小さい方を取り、ポート番号別の使用量を見てみます。

また、全体トラフィックは、ピア型のヘビーユーザのトラフィックに支配されているので、クライアント型の一般利用者の動向を見るために、少し荒っぽいですが、1日のアップロード量が100MB未満のユーザを抜き出して、これをクライアント型利用者とします。これは、図-3では、IN=100MBにある水平線の下側の利用者にあたります。

図-6はポート使用の概要を、全体とクライアント型利用者について、2013年と2014年で比較したものです。また、表-2にその詳細を数値で示します。

2014年の全体トラフィックの80%はTCPです。HTTPの80番ポートの割合が、2013年の43%から45%に僅かに増えているのに加えて、HTTPSの443番ポートの割合も、4%から9%に増えています。減少傾向のTCPの動的ポートは、2013年の30%から2014年には24%にまで減りました。動的ポートでの個別のポート番号の割合は僅かで、Flash Playerが利用する1935番が最大で総量の約2%ありますが、後は0.5%未満となっています。TCP以外のトラフィックのほとんどはVPN関連です。

一方、クライアント型利用者に限ると、2013年には82%を占めていた80番ポートが、2014年には75%にと初めて減少に転じました。その代わりに、2番目に多いHTTPSの

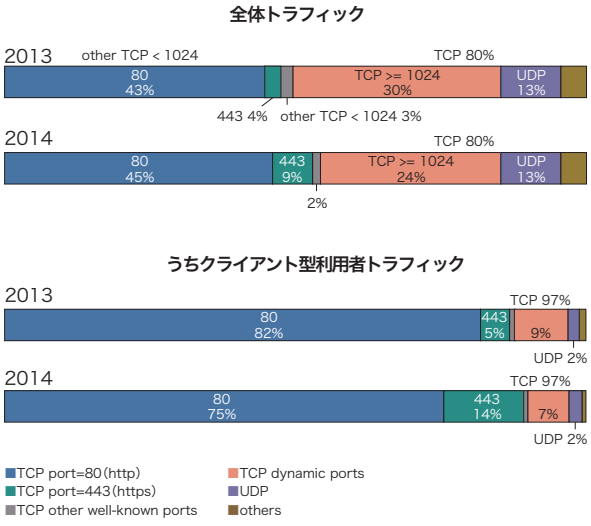


図-6 ポート別使用量概要

protocol port	2013		2014	
	total (%)	client type	total (%)	client type
TCP	**79.79**	**96.91**	**80.15**	**97.38**
(< 1024)	49.57	88.15	56.33	90.08
80(http)	43.44	81.61	44.87	74.81
443(https)	3.90	4.80	9.25	13.78
554(rtsp)	0.51	0.58	0.36	0.25
22(ssh)	0.24	0.04	0.31	0.03
(>= 1024)	30.22	8.76	23.82	7.30
1935(rtmp)	2.39	3.60	2.48	4.00
8080	0.34	0.19	0.40	0.17
7144(peercast)	0.40	0.04	0.32	0.02
UDP	**13.21**	**2.12**	**12.51**	**1.81**
ESP	**6.54**	**0.88**	**6.86**	**0.74**
IP-ENCAP	**0.13**	**0.00**	**0.24**	**0.00**
GRE	**0.20**	**0.06**	**0.20**	**0.04**
ICMP	**0.02**	**0.02**	**0.02**	**0.02**
IPv6	**0.01**	**0.01**	**0.01**	**0.00**
L2TP	**0.09**	**0.00**	**0.00**	**0.00**

表-2 ポート別使用量詳細

443番ポートが、2013年の5%から14%に増えています。また、動的ポートの割合は、9%から7%に減少しています。

HTTPSの利用拡大については、2013年6月に米国家安全保障局(NSA)の通信傍受プログラムの存在が問題になって以降、暗号化通信を行うHTTPSを常時使用するサービスが増えてきているためです。2014年のHTTPSを利用するトラフィック量について事業者別内訳を調べると、その59%(クライアント型利用者に限れば67%)はGoogle社関連で、同社の積極的なHTTPS採用の取り組みが窺えます。他にも、Akamai、Amazon、Facebook、Microsoft、Twitterなどが続いていて、今後もHTTPSの利用が拡大すると思われます。

図-7は、全体トラフィックにおけるTCPポート利用の週間推移を、2013年と2014年で比較したものです。ここでは、TCPのポート利用を80番、その他のウェルノウンポート、動的ポートの3つに分けてそれぞれの推移を示しており、ピーク時の総トラフィック量を1として正規化して表しています。2013年と比較すると、全体でも80番ポートの割合が更に増え、動的ポートの利用が減少している傾向が確認できます。全体のピークは21時〜1時、土日には昼間のトラフィックが増加していて、家庭での利用時間を反映しています。

図-8と図-9は、同様にTCPポート利用の週間推移について、クライアント型利用者とピア型利用者に分けて、それぞれ2013年と2014年を比較しています。クライアント型利用者では、ほとんどが80番ポートですが、HTTPSを含むその他のウェルノウンポートが増えています。ピーク時間は21時〜23時です。また、ピア型利用者においても、今回初めて80番ポートの割合が動的ポートの割合を上回りました。

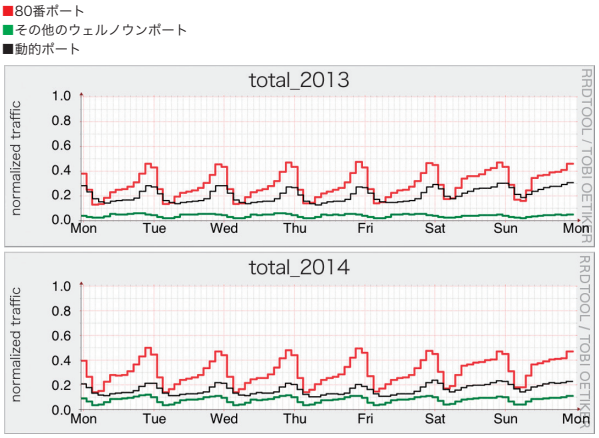


図-7 TCPポート利用の週間推移 2013年(上)と2014年(下)

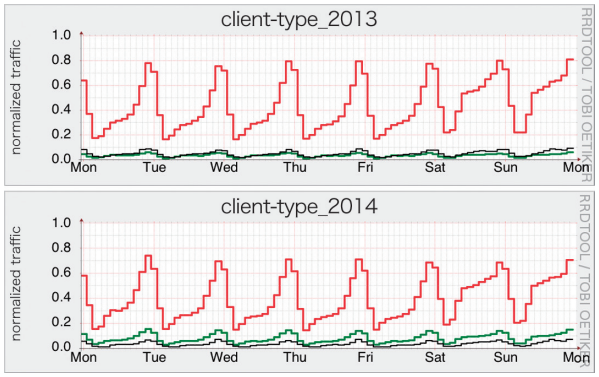


図-8 クライアント型利用者のTCPポート利用の週間推移 2013年(上)と2014年(下)

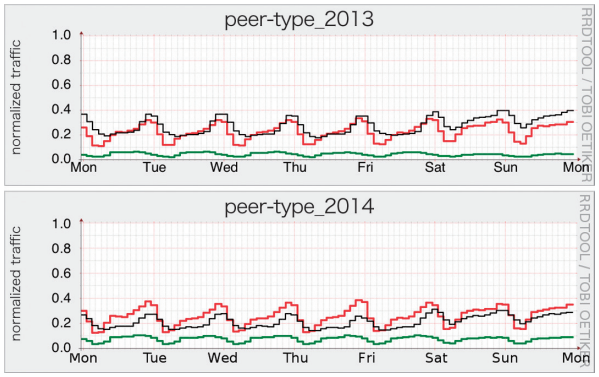


図-9 ピア型利用者のTCPポート利用の週間推移 2013年(上)と2014年(下)

2.5 まとめ

これまで見てきたように、この1年間のブロードバンドトラフィックは、全体のトレンドには大きな変化はなかったと言えます。全体として、ダウンロード量は27%、アップロード量も13%増加して、着実にトラフィック量が増えてきています。

また、トラフィックのほとんどを占めるようになったWebトラフィックにおいて、今回はHTTPSの利用が増えてきていることが確認できました。現状ではGoogle一社が突出しているようですが、プライバシー保護の意識の高まりを受けて、他社もHTTPSを常時利用するようになってきており、今後もHTTPSの割合が増えて行くと予想します。

さて、いよいよ2014年7月からNTT東日本でも1Gbpsのブロードバンドサービスが始まりました。これまでは、NTT西日本が2010年から1Gbpsサービスを提供しています。いまのところ、西日本の1Gbpsサービスの利用者のトラフィックは、他の利用者と比べて大きくは違わないようで、まだギガの帯域を必要としている利用者は多くはないのかも知れません。しかし、2001年に100Mbpsのファイバー接続サービスが始まった時にも同じように言われていました。ブロードバンドサービスは、ファイバー接続サービスの開始から13年経って大きな転換点を迎えていると考えられます。

プロトコルについても、現在HTTP/2が策定中で、15年ぶりに大きな改訂が予定されています。HTTP/2ではパフォーマンスの改善やネットワーク資源の有効利用など性能向上が図られています。このようなインフラとプロトコルの世代交代が進むことによって、次の世代のアプリケーションやサービスが出てくるための環境が整ってきているのです。その意味でも、今後の1Gbpsサービスの普及状況と、それに伴うトラフィック増加及びコンテンツの変化が注目されます。IIJは今後も継続的なトラフィックの観測を行い定期的にレポートをお届けしていく予定です。

執筆者:

長 健二朗（ちょう けんじろう）
株式会社IIJ イノベーションインスティテュート 技術研究所所長。

DNSを取り巻く環境

**DNSは多くのアプリケーションで利用されており、インターネットの重要なサービスの1つです。
ここでは最近のTLDの追加で顕在化した名前衝突の問題をはじめ、
DNSを取り巻く環境の最新動向について解説します。**

3.1 DNS最新動向

DNSは問い合わせに対応するレコードを応答してくれるサービスで、主にドメイン名に対応するIPアドレスを検索する名前解決に利用されています。インターネットでは、ほとんどのアプリケーションがDNSによる名前解決を利用しており、とても重要なサービスだと言えます。DNSでは、ゾーンという単位でドメイン名に対応するレコードを保持する権威サーバと、問い合わせを行うクライアントが登場します。ほとんどの場合、クライアントはDNSの面倒な反復問い合わせをISPなどが用意しているDNSキャッシュサーバに依頼して、結果のみを受け取ります。DNSキャッシュサーバは、rootと呼ばれる頂点のゾーン情報を提供する権威サーバのIPアドレスのみを知っており、そこから得られる情報を手がかりにより詳細な情報を保持しているであろう権威サーバをたどって必要なレコードを探します。また、毎回反復問い合わせを行っているとサーバの負荷や遅延が問題となるため、得られたレコードはしばらくキャッシュしておき、再び同じ問い合わせを受けた場合にはそのキャッシュから応答しています。最近はこの他にもブロードバンドルータやファイアウォールなど、通信経路上の機器にもDNS関連の機能が実装されており、DNS問い合わせの中継や制御ポリシーの適用に関わっている場合があります。

ドメイン名の名前空間は重複して登録されることがないように、トップレベルドメイン(TLD)ごとにレジストリと呼ばれる管理組織が指定されて管理しています。rootのゾーン情報はICANNが管理しており、ここから各TLDのレジストリに権威委任されて登録者からのドメイン名登録を処理しています。新規にドメイン名を登録したい場合は、レジストラと呼ばれる仲介業者を通じて登録したいドメイン名に対応するTLDのレジストリに申請しますが、各トップレベルやそのサブドメインの属性ドメインごとに登録ポリシーがあり、誰がどんな目的でドメイン名を登録できるのかが異なっている場合があります。例えば.jpドメインは株式会社日本インターネットレジストリサービス(JPRS)がレジストリを担っており、汎用jpと呼ばれるセカンドレベルドメイン名は日本に連絡のとれる住所を持つ個人・法人であれば誰でも登録できますが、co.jp属性型ドメイン名は日本に登記された会社組織のみが登録できます。また、特に制限を設けず、誰でも登録できるポリシーで運用されているTLDもあります。登録されたドメイン名の管理は登録者に権威委譲されるため、それぞれの登録者が運用ポリシーを持ち、適切に管理運用していく必要があります。

3.2 名前衝突問題

ひとまず動けば良いと、利便のために導入された方式が後々問題を引き起こす場合があります。Name Collision（名前衝突）の問題もこれに該当すると言えます。例えば、社内や家庭内など、管理が明確で特定の人しか利用しない環境では、存在しないTLD（勝手TLD）を用いた独自の内部用ドメイン名空間が利用される場合があります。小規模の場合はhostsファイルなどを利用してホスト名を直接クライアントに登録してしまうこともありますし、クライアント数が増えてくると、社内向けキャッシュサーバやファイアウォールで内部からの勝手TLDの問い合わせに応答するようにDNSを設定し、クライアントを特に設定変更することなく内部用ドメイン名でアクセスできるようにしている場合もあります。設定時には当初の目的を達成し動くように見えるのですが、インターネットは変化し続けており、標準技術を利用して標準以外の設定を行っているとどこかで歪みが生じてしまいます。実は近年、rootゾーンに新規のTLDが追加されており、既にその数は300を越えてまだまだ追加が続いています。ここで内部で利便のために設定していた勝手TLDと追加されたTLDがぶつかると、正規に登録したドメイン名が利用できなかったり意図しないサイトに接続してしまったりといった問題が生じてしまいます。これを名前衝突問題と呼びます（図-1）。問題回避のためには、内部用ドメイン名であっても一意性が担保されたドメイン名を利用することです。既に何らかの登録しているドメイン名があるのならば、そのドメイン名に内部用のサブドメインを設定して利用したり、いっそのこと内部用に新規のドメイン名を登録したりすることで、利用しているドメイン名の一意性が将来にわたって担保できるため安心です。

名前衝突問題はサーバの電子証明書にも関わってきます。電子証明書を発行するパブリック認証局は、これまで組織内部のサーバでも電子証明書を利用できるように、勝手TLDの内部用ドメイン名であっても電子証明書を発行してきました。通常のサーバ用電子証明書であれば、電子メールやWebサイトへの特定文字列の登録などでドメイン名保持の確認ができるのですが、勝手TLDではそのような確認ができないので、特段の確認なく電子証明書が取得できていました。すると、新規に追加されたTLDでドメイン名を登録した場合、過去に誰かがそのドメイン名に対応する電子証明書を取得している可能性が出てきてしまいます。電子証明書関連の任意団体であるCA/Browser Forumでは、この名前衝突問題を受け、今後は段階的に内部用ドメイン名向けの電子証明書を制限する運営基準を策定しました。既に現状で発行されている内部用ドメイン名向けの電子証明書は、有効期限が2015年11月1日以降とならないように設定されています。また、新規TLDが追加された場合は、120日以内に関連する電子証明書が失効されるほか、2016年10月には、これまで発行された電子証明書を含め、勝手TLDやインターネットから存在が確認できないドメイン名を用いた内部用ドメイン名に対するすべての電子証明書が失効される予定です。

クライアントには、DNSで名前解決する際にドメイン名を補うサーチリストや、DNSサフィックスといった機能を実

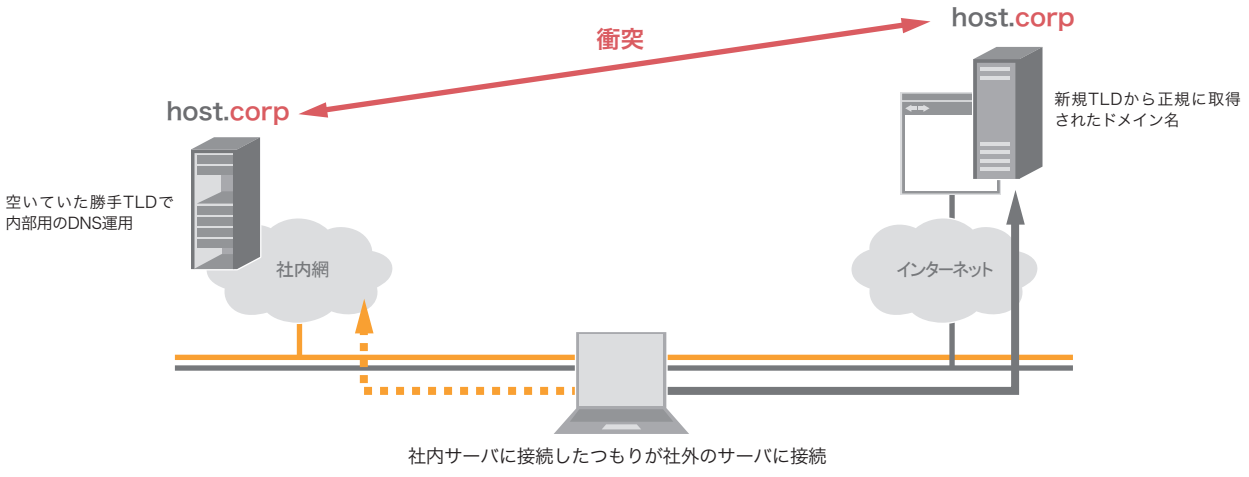


図-1 名前衝突の例

装している場合があります。これはユーザが完全なドメイン名(FQDN)を指定しなくても、その先頭部分を入力すれば意図するドメイン名を指定できるようにする機能です。組織内部ではドメイン名部分が共通の場合が多く、複数のサーバや機器に接続するのに何度も同じドメイン名を入力しなくても済むように利用されています。しかし、これもまた名前衝突問題と関わってきます。クライアントの実装に因るところが大きいのですが、「.」が1つでも含まれたドメイン名がアクセス先に指定されると、ひとまずそのドメイン名をDNSで問い合わせ、レコードが存在しなければサーチリストのドメイン名を補って再度問い合わせる挙動が多いようです。そうすると、これまでは初回の問い合わせに対応するドメイン名が存在しなかったために、ドメイン名が補完され意図したドメイン名で名前解決できていたものが、その後の環境変化で初回の問い合わせに応答が得られた場合、意図しないサイトに接続してしまう可能性があります。新たに登録されたTLDにはtokyoやnycといった地域名も含まれており、サブドメインでこれらの地域名を利用して運用している場合には特に注意が必要です。無論、実際にはすべての追加されるTLDと内部でのサブドメイン運用、DHCPなどで配布するDNSのサーチリストを総合的に見て影響を考える必要があります。利用者にはできるだけ完全なドメイン名でアクセスするように誘導しておくのが将来にわたって安心です。

ICANNでは名前衝突問題を早くから認識しており、影響を軽減するために対策を重ねてきました。先に挙げたCA/Browser Forumの運営基準はICANNとの対話による成果ですし、実際のDNSの問い合わせ状況に基づき、新規のTLD導入の危険性評価もしてきました。調査には主にDNS-OARCのA Day in the Life of the Internet(DITL)プロジェクト[*1]で収集された主要な権威サーバからのデータが利用されました。内部用ドメイン名は組織内などで利用されているはずですが、設定ミスやモバイル端末が外部で接続試行した場合などにDNS問い合わせが外部に漏れ出します。これはrootサーバなどでも検知できるため、勝手TLDの利用を推定することができます。この調査では特にhomeとcorpという勝手TLDを利用した問い合わせが格段に多いことが判明し、これらを新規TLDとして認めると問題が多すぎるということで、この2つに関しては無期限に委任保留する旨を決定しました[*2]。また、それ以外の新規TLDに関してもDITLなどのデータへの出現頻度に基づき、名前衝突の可能性が高い一部のセカンドレベルのドメイン名については、登録を禁止する制限付きで委任されることとなりました。

日本国内でもJPNICで新gTLD大量導入に伴うリスク検討・対策提言専門家チームを設立して、名前衝突問題に関する検討を行い提言を文章としてまとめています[*3]。名前衝突の問題は思わぬ所で影響が出てしまう可能性があるため、組織内の設定や文章に記載したURLなど、今までは問題なく動いていたものも含めて見直し、実は危うい前提に成り立っていないかを今一度確認してみてることをお勧めします。

＊1　https://www.dns-oarc.net/oarc/data/ditl
＊2　https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-1-07oct13-en.pdf
＊3　https://www.nic.ad.jp/ja/dom/new-gtld/name-collision/

3.3 DNSと通信制御

DNSは、Webサイトへの誘導やメールの配送制御など、利用者の通信を制御する機能をもち、また閲覧することもできます。つまり、DNSの応答を変化させることにより、クライアントの通信を制御することができます(図-2)。例えば、世界規模でコンテンツ配信を行っている事業者ではクライアントからのDNS問い合わせに対して遅延の低減や配信の効率化を目的に、クライアント近傍の配信サーバのIPアドレスを応答するように実装している場合もあります。実際には利用者の多くは、ISPなどの提供するDNSキャッシュサーバを利用しているため、コンテンツ事業者の管理する権威サーバではこのDNSキャッシュサーバ単位で利用者をグループ化し、最も適切だと思われるIPアドレスを応答するようにしているようです。一方で攻撃者に悪用された例もあります。攻撃者の管理するDNSキャッシュサーバを参照させて、悪意あるコンテンツをダウンロードさせる場合が多いようです。DNS Changerの事例では端末のDNS参照先を書き換えていますし、更に、ブロードバンドルータのDNS参照先も攻撃者のものに書き換えていたと報告されています。このような悪意あるデータを参照させられないように、DNSの設定には注意を払わなければなりませんが、DNSを取り巻く環境は複雑になってきています。

現状では多くの端末がDHCPの情報に基づいて参照先のDNSキャッシュサーバを設定しています。DHCP機能は組織内の管理者が意識的に運用している場合や、コンシューマ用途ではブロードバンドルータで標準的に提供されている場合があります。ブロードバンドルータでは、DNSの問い合わせをISPなどのDNSキャッシュサーバに単純に中継する機能を実装し、宅内の端末にはルータ自身をDNSの参照先として参照させるものが多いようです。ただしこの実装はDNSの仕様からすると、かなり限定された機能のみが提供されている場合があり、TCPでの問い合わせに対応していなかったり、EDNS0に対応しきれていないものがあるようです。この状況を踏まえて、RFC5625/BCP152[*4]としてブロードバンドルータなどにDNS中継機能を実装する際のガイドラインが公開されています。このガイドラインでは、DNS中継機能を将来にわたって問題なく利用し続けられるように、透過性に注意して実装することが推奨されています。

ブロードバンドルータの一部には、端末の参照先DNS設定に関わらず、通過するすべてのDNS問い合わせをブロードバンドルータに設定されたDNSキャッシュサーバ宛にねじ曲げる機種も存在します。この場合、端末にどんなIPアドレスを参照先DNSとして登録しても、端末からのDNS

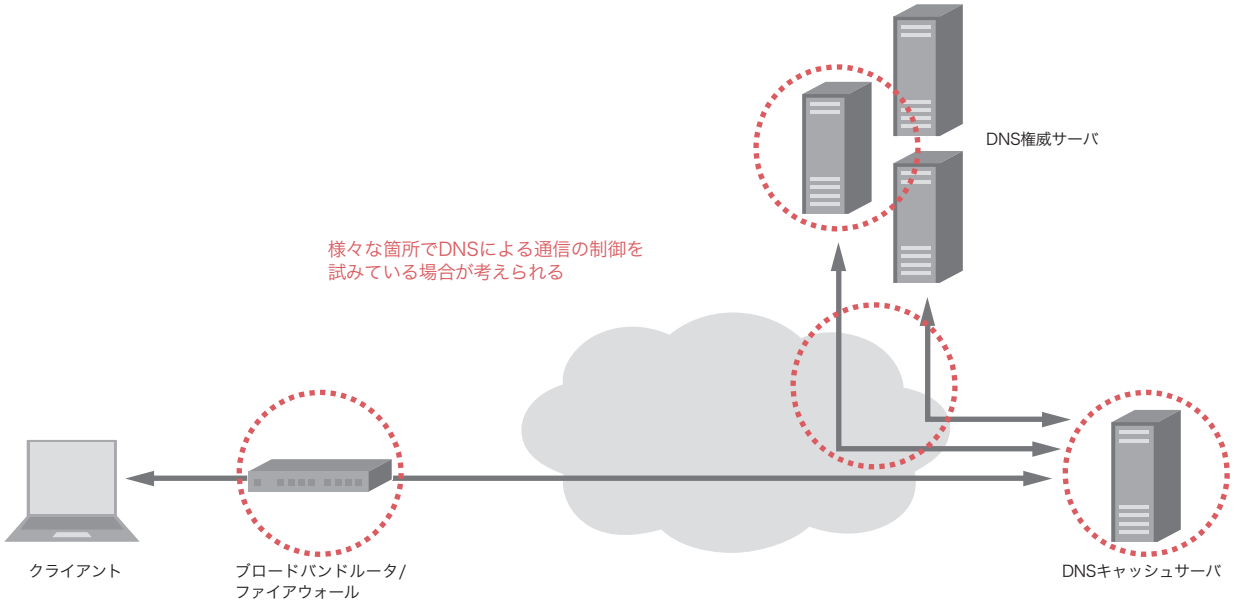


図-2 DNSと通信制御

*4 https://tools.ietf.org/html/rfc5625

問い合わせはブロードバンドルータを経由した瞬間に特定のDNSキャッシュサーバへの問い合わせとして書き換えられてしまうため、端末のDNS設定を見ただけでは実際にどのDNSキャッシュサーバを参照しているか判別できません。これは特定のDNSキャッシュサーバを強制する運用ポリシーの実装には便利な機能かもしれませんが、ひとたび問題が発生すると、利用者もその状態に気が付きにくいので切り分けがとても困難な仕様です。

ISPのDNSキャッシュサーバでも様々な制御が実装されてきています。IPv6閉域網に接続した端末がIPv4のみでインターネット側のサーバと通信する場合、IPv6での接続に失敗し、IPv6/IPv4フォールバックによる遅延や接続障害が発生する場合があります。IPv6でもインターネット接続があれば問題なく通信できるのですが、申し込みが必要であったりルータの更新が必要であったりするため、導入に時間がかかることが懸念されます。このようなユーザ環境での問題を軽減するため、DNSキャッシュサーバでIPv6のレコードであるAAAAレコードに対して応答しない、AAAAフィルタと呼ばれる機能が実装されている場合があります。また、児童ポルノの流通を防止するために、DNSキャッシュサーバで特定ドメイン名の応答を遮断する児童ポルノブロッキング[*5]が実装されている場合もあります。

一部の国や地域によっては、望ましくないコンテンツへのアクセスを遮断するために政府主導でDNSの制御を導入している場合があります。その地域でサービスを提供する各ISPのDNSキャッシュサーバで遮断している場合や、ネットワーク上にDNSの問い合わせを監視する機能を実装し、特定のドメイン名への問い合わせを遮断したり、偽の内容を応答する場合があるようです。ユーザからは通信障害なのか意図された遮断なのか分からない上に遮断ポリシーが明示されることは少ないため、問題なのかどうかも含めて切り分けが困難です。しかし、国や地域によって遮断されるコンテンツに傾向があるため、恐らく意図された遮断であろうとの推測は可能です。このように、DNSでは様々な箇所で制御が実装されている可能性があるため、問題を切り分ける際にはそれらを考慮して障害箇所を見つける必要があります。

3.4 DNSと攻撃

DNSは多くの機器に実装されており、多くのアプリケーションが実質的に依存しているため、攻撃に悪用されたり攻撃の対象となったりすることがあります。主にオープンリゾルバと呼ばれる、誰からの問い合わせにも応答するDNSキャッシュサーバを踏台にしたDNS増幅攻撃は、その増幅効率と攻撃分散の良さから広く悪用されてきました。多くのDNSキャッシュサーバが、何ら対策されないままに誰からの問い合わせにも応答する状態だったために踏台として悪用されました。国内のISPのDNSキャッシュサーバは近年徐々に設定を変更し、そのユーザからのみDNS問い合わせを受け付けるようになってきています。ただし、ブロードバンドルータに実装されいてる一部のDNS中継機能は標準でインターネットからのDNS問い合わせにも制限なく応答してしまうため、踏台として悪用されてしまいます。これらは個別のユーザによる対応が必要となるため、継続的な注意喚起が必要です。

DNSの権威サーバに対する攻撃やその悪用も発生しています。通常のDDoSと同じく、大量のトラフィックを権威サーバ宛に送信して輻輳によるサービス妨害を狙った攻撃や、DNSのプロトコルとしては正常な問い合わせを権威サーバに大量に投げつけてDNS増幅攻撃の踏台に悪用される事例が発生しています。単純な妨害トラフィックであれば適当なパケットフィルタなどで防御できますが、増幅攻撃の踏台として悪用された場合は攻撃を意図した問い合わせを単純に見分けることができないため、対応に検討が必要です。JP DNSを含むいくつかの権威DNSでは、Response Rate Limiting(RRL)と呼ばれる、連続した同一応答を抑制する機能を実装し、影響の軽減に努めています[*6]。ただし、この対策も万能ではないため、引き続き攻撃手法に注視し、適切な対応を模索していく必要があります。

ISPのDNSキャッシュサーバでは、2014年初旬から断続的にいくつかのドメイン名に関する大量のDNS問い合わせを観測しています。意図は不明ですが、恐らく該当ドメイン名の権威サーバに対する分散攻撃であろうと推測しています。ただし、この攻撃に付随した該当権威サーバとの通

*5 http://www.netsafety.or.jp/blocking/
*6 http://www.redbarn.org/dns/ratelimits

信が大量に発生するため、DNSキャッシュサーバでも過負荷になり、DNSキャッシュサーバ利用者の名前解決に遅延が生じるなどの障害が発生する場合があります。攻撃者がこれを意図しているかは別にして、利用者に影響が出てしまうようなら何らかの対策が必要ですが、オープンリゾルバになっているブロードバンドルータが踏台に利用されたり、ユーザの端末に感染したbotからのDNS問い合わせであったりと、ユーザからの通常のDNS問い合わせと同様に見えてしまうため、汎用的な対策が難しい攻撃です。異常な頻度の問い合わせ形式を注視して、都度状況に応じた対策が必要となります。

DNSでは問い合わせプロトコルとして主にUDPが利用されています。UDPはTCPと比べて通信の成りすましが容易で、攻撃者が偽の応答を注入できる可能性があります。偽の応答の注入に成功するには、問い合わせとIPアドレス、ポート番号、DNS ID、QNAMEの情報が一致する必要があります。防御側では問い合わせの該当情報が偽の応答と一致しないように努力する必要があります。DNS IDが既に十分乱数から生成されているとすると、残るは送信元ポート番号に良い乱数を利用することが必須です。送信元ポート番号を固定している古いDNS実装を利用している場合には最新のDNS実装に更新するなどして、推測しにくい問い合わせを送出できるように対策が必要です。また、一部ファイアウォールやNAPT機器では、せっかく問い合わせ元でDNS IDや送信元ポート番号に乱数を利用しても、これらの情報を上書きしてしまうものもあるため、併せて注意が必要です。

多くのDNS関連の攻撃には、送信元IPアドレスの偽装が利用されています。各ネットワークでBCP38[*7]を実装して、送信元IPアドレスの偽装ができない環境が整えば、現在のDNSを悪用した攻撃はほとんどが根絶可能です。BCP38を容易に実装できるようにとuRPF check機能も各社ルータに実装されているため、特に端末が接続しているようなネットワークでは送信元IPアドレスを偽装した攻撃の送出を未然に防げるように、積極的に送信元IPアドレスの検証導入をご検討ください。

3.5 まとめ

DNSはインターネットで多くのアプリケーションが依存する重要なサービスです。これが健康的な状態を維持して利用可能であるためには、権威サーバを始めとして名前解決を行うクライアントやDNSキャッシュサーバ、その他のDNSを仲介する機器が適切な協調のもとに管理、運用されている必要があります。DNSの名前空間は、昨今の新規TLD追加に伴って大きく変化しつつあります。勝手TLDを利用した内部向けのドメイン名や、サーチリストに依存した名前解決を利用している場合には、名前衝突の問題が発生する可能性があります。また、DNSは制御系としても広く利用されており、様々な箇所で制御を試みている可能性があるために複雑さが増してきています。複雑さはそれ自体問題の発生原因となるほか、問題解決の障害にもなるので注意が必要です。DNSに限りませんが、潤沢な帯域やCPU資源を背景に攻撃手法は変化しています。攻撃手法の変化に注視しつつ、時代に即した運用ができるように日々の情報収集や情報交換を心がけることをお勧めします。IIJでも自社の設備の適切な運用はもちろんのこと、必要に応じた情報共有や議論などを通じてインターネットの健康な発展に寄与していきたいと考えています。

執筆者:

松崎 吉伸（まつざき よしのぶ）
IIJ ネットワーク本部 ネットワークサービス部 技術開発課 シニアエンジニア。

*7 http://tools.ietf.org/html/bcp84

Vol.24 August 2014

株式会社インターネットイニシアティブ(IIJ)について

IIJは、1992年、インターネットの研究開発活動に関わっていた技術者が中心となり、日本でインターネットを本格的に普及させようという構想を持って設立されました。
現在は、国内最大級のインターネットバックボーンを運用し、インターネットの基盤を担うと共に、官公庁や金融機関をはじめとしたハイエンドのビジネスユーザに、インターネット接続やシステムインテグレーション、アウトソーシングサービス等、高品質なシステム環境をトータルに提供しています。
また、サービス開発やインターネットバックボーンの運用を通して蓄積した知見を積極的に発信し、社会基盤としてのインターネットの発展に尽力しています。

株式会社インターネットイニシアティブ

〒102−0071 東京都千代田区富士見2-10-2　飯田橋グラン・ブルーム
E-mail：info@iij.ad.jp　URL：http//www.iij.ad.jp/

IIJ-MKTG019XA-1408GR-09500PR