

Internet Infrastructure Review Vol.23

May
2014

インフラストラクチャセキュリティ

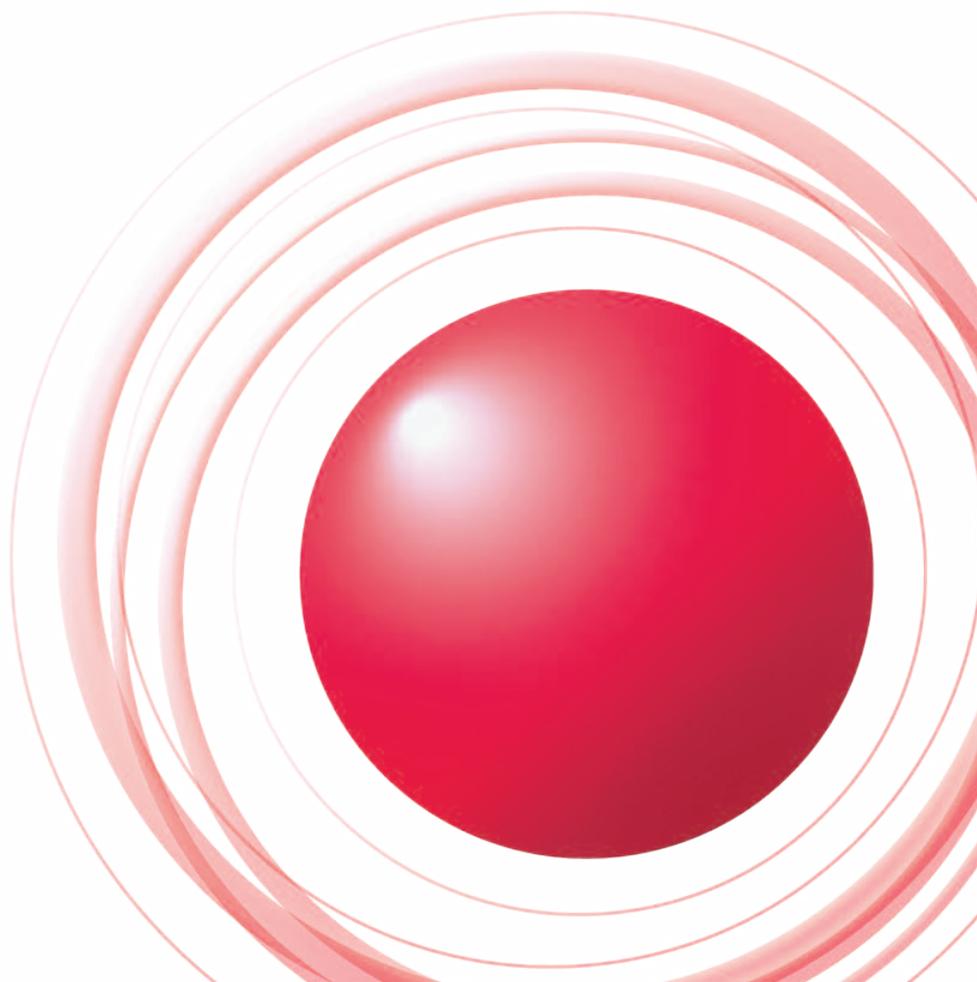
PlugXの背後にいる攻撃者について

メッセージングテクノロジー

送信ドメイン技術の導入状況と標準化の動向

技術トレンド

ビッグデータ解析の現状



エグゼクティブサマリ	3
1. インフラストラクチャセキュリティ	4
1.1 はじめに	4
1.2 インシデントサマリ	4
1.3 インシデントサーベイ	12
1.3.1 DDoS攻撃	12
1.3.2 マルウェアの活動	14
1.3.3 SQLインジェクション攻撃	17
1.3.4 Webサイト改ざん	18
1.4 フォーカスリサーチ	19
1.4.1 PlugXの背後にいる攻撃者	19
1.4.2 DrDoS攻撃とその対策	22
1.4.3 電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会	24
1.5 おわりに	27
2. メッセージングテクノロジー	28
2.1 はじめに	28
2.2 迷惑メールの動向	28
2.2.1 2010年中頃から割合が減少	28
2.2.2 直近の迷惑メール割合は減少	29
2.2.3 メールをトリガにした危険度は高まる	29
2.2.4 迷惑メール送信元の動向	29
2.3 メールの技術動向	30
2.3.1 送信ドメイン認証技術の普及状況	30
2.3.2 送信ドメイン認証技術の普及の推移	31
2.3.2 SPFの標準化動向	32
2.4 おわりに	33
3. 技術トレンド	34
3.1 ビッグデータの現状	34
3.2 ビッグデータ解析基盤の技術動向:リアルタイム化	36
3.3 リアルタイム化に伴うビッグデータ解析の変化	38
3.3.1 ソーシャルビッグデータとしてのWikipedia	38
3.3.2 Wikipedia PVCの時系列変動の分析	38
3.4 まとめ	39

エグゼクティブサマリ

総務省が2014年3月14日に発表した資料によると、2013年11月時点での我が国のブロードバンドサービス契約者の総ダウンロードトラフィックは、推定で約2.5Tbpsとなり、前年同月比で33.2%増となりました。前回の本レポートでも報告しましたように、それらのトラフィックを運んでいるアプリケーションは、徐々にHTTP/Webへシフトする傾向を示しています。また、ガートナー社が2013年8月に公表した「先進テクノロジーのハイブ・サイクル: 2013年」では、鍵となるテーマは人とマシン間の進化しつつある関係にあるとされており、ハイブ・サイクルにおいては、以下の6つの要因をサポートするテクノロジーに焦点が当てられている、とされていました。すなわち「テクノロジーによる人間の能力の増大」「マシンによる人間の作業の代行」「人とマシンのコラボレーション」「マシンによる人と環境の認識力の向上」「マシンへの人の理解の高まり」「より賢くなる人とマシン」です。そして、それらの実現のためのキーテクノロジーである「ビッグデータ」は、ちょうどハイブ・サイクルの頂点に差し掛かっているとされていました。

個人のプライバシーに関わるデータのセキュリティを確保することは、インターネットを安心・安全に活用する際に不可欠となりますが、それとは並行して、よりコンピュータを活用し、人間の能力や社会を進歩させるトレンドを進めるのであれば、インターネットやクラウド上でやり取りされたり蓄積されたりしているデータを積極的に活用して行くことも必要とされている、ということになるでしょう。

本レポートは、このような状況の中で、IJ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1月から3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、PlugXの検体群を解析することで背後にどのような標的型攻撃グループが関与しているかを調査した結果の解説と、昨年末頃から増えてきているDrDoSと呼ばれる攻撃手法とその対策についての説明、及び、電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会について解説します。

「メッセージングテクノロジー」の章では、2013年4月1日から2014年3月30日までの52週分の迷惑メールの動向分析を、2013年12月30日から2014年3月30日までの直近13週にフォーカスを当てて実施した結果をご報告いたします。また、メールの技術解説では、送信ドメイン認証技術の導入状況や、2006年にExperimental RFCとして標準化されたSPFの改訂作業について解説します。

「技術トレンド」の章では、現在のビッグデータに関わる現状と、それに伴ってリアルタイム化を指向する解析基盤に関わる技術動向、更に時系列データからの知見を得るビッグデータ解析手法の多様化について概観します。また、ビッグデータの時系列に着目した分析の例としてWikipedia PVCを用いたトレンド分析の結果を解説します。

IJ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IJ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、IJ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IJ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。

PlugXの背後にいる攻撃者について

今回は、標的型攻撃に使われているマルウェア、PlugXの背後にいる攻撃者について、調査結果とその背景を紹介すると共に、最近のDDoS攻撃の傾向とその対策、総務省の電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会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IJ自身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、IJ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1月から3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、NTPを悪用したDDoS攻撃が頻発し、1つの攻撃で400Gbpsもの攻撃の通信量が発生したと報告されています。ccTLDなど、国単位で影響を受けるドメインハイジャック事件も続いています。加えて、昨年より国内で被害が増加しているオンラインバンキングを悪用した金銭被害についても、本年も引き続き増加傾向にあります。昨年末に米国で発覚した、マルウェアにより小売店のPoSシステムから多くの情報を盗まれた事件では、その影響の大きさから対策に関する数多くの議論が行われました。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。

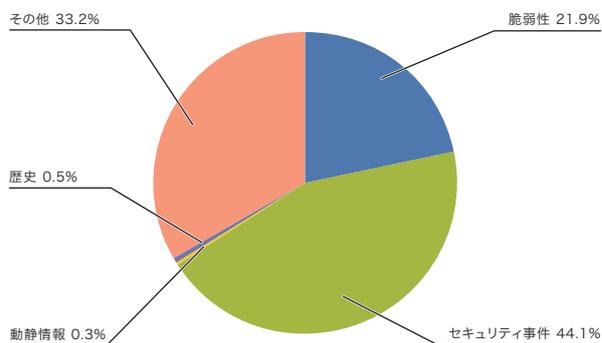


図-1 カテゴリ別比率(2014年1月～3月)

*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、過去の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。

2 この攻撃についてはNATO報道官であるOana Lungescu氏のTwitter (@NATOPress) で確認できる (<https://twitter.com/NATOPress/statuses/445112624578306048>)。

1.2 インシデントサマリ

ここでは、2014年1月から3月までの期間にIJ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。1月には、ブラジルの複数の政府関連サイトに対してWeb改ざんの被害が発生しています。同じく1月には、昨年自殺した活動家にちなみ、マサチューセッツ工科大学(MIT)のWebサイトが改ざんされています(OpLastresort)。

ウクライナ情勢では、EUやウクライナとロシアやその周辺国のAnonymousなどによって、政府機関へのDDoS攻撃や野党議員のメールの漏えい、クレジットカード情報の漏えいやマスコミのWebサイトへの攻撃などが複数発生しています。更に、3月には、これに関連していると考えられる、北大西洋条約機構(NATO)へのDDoS攻撃が発生しました*2。

他にも、南米や欧州を中心に、世界各国の政府とその関連サイトに対して、Anonymousなど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MicrosoftやSkypeなどの著名な企業も含まれていました。

■ 脆弱性とその対応

この期間中では、Microsoft社のWindows^{*3 *4 *5 *6}、Internet Explorer^{*7 *8}、などで修正が行われました。Adobe社のAdobe Flash Player、Adobe Reader及びAcrobat、Shockwave Playerなど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提供され、多くの脆弱性が修正されました。なお、この更新ではセキュリティ機能の変更が行われ、署名の付いていないJavaアプレットについては実行が制限されるなど、初期設定でのセキュリティの強化が行われています^{*9}。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いる更新が提供され、多くの脆弱性が修正されました。また、DNSサーバのBIND9では、NSEC3を用いてDNSSEC署名されたゾーンを保持している権威DNSサーバとして運用していた場合に、DNS問い合わせ受信時の処理の不具合によるnamedが異常終了する脆弱性が見つかり修正されました^{*10}。時刻同期に利用されているNTPについても、サーバの管理機能を悪用して、他者へのDDoS攻撃に繋がる不具合が見つかり、修正が行われました。また、この不具合を悪用した攻撃が複数発生しており、注意喚起が行われています。詳細については「1.4.2 DrDoS攻撃とその対策」も併せてご参照ください。

3月には半年に1度行われるCisco Systems社のIOSで定

例アップデートが行われ、システム停止の可能性のある脆弱性などが修正されています^{*11}。CMSとして利用されるWordPressについてもPingback機能を悪用した他者へのDDoS攻撃に繋がる不具合が見つかり、また、実際にこの不具合を悪用した攻撃が発生しています^{*12}。

■ Webサービスに対する攻撃

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、なりすましによる不正ログインなどのWebサービスへの不正ログインや、Web改ざんによるマルウェア感染が継続しています。

ISPやゲームサイト、交通機関のサイトやクレジットカード会社、SNSなど様々なサイトでリスト型攻撃による不正ログインの試みが行われる事件が多く発生しています。この内、航空会社のマイレージサービスで発生した不正ログイン事件では、サイト上のポイントを他のギフトポイントに不正に交換されるなどの被害が発生しました。被害が発生した一部のサイトについては、ユーザが設定できるパスワードの文字列の長さが少ないことなど、仕様に問題があることが以前から指摘されていました。このように不正アクセス事件は継続して数多く発生しており引き続き注意が必要です。

また、この期間ではWebサイトの改ざんと、改ざんされたWebサイトからマルウェアへ誘導される事件が多く発生

*3 「マイクロソフト セキュリティ情報 MS14-002 - 重要 Windows カーネルの脆弱性により、特権が昇格される」(<https://technet.microsoft.com/library/security/ms14-002>)。

*4 「マイクロソフト セキュリティ情報 MS14-007 - 緊急 Direct2D 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/library/security/ms14-007>)。

*5 「マイクロソフト セキュリティ情報 MS14-011 - 緊急 VBScript スクリプト エンジンの脆弱性により、リモートでコードが実行される」(<https://technet.microsoft.com/library/security/ms14-011>)。

*6 「マイクロソフト セキュリティ情報 MS14-013 - 緊急 Microsoft DirectShow 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/library/security/ms14-013>)。

*7 「マイクロソフト セキュリティ情報 MS14-010 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム」(<https://technet.microsoft.com/library/security/ms14-010>)。

*8 「マイクロソフト セキュリティ情報 MS14-012 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム」(<https://technet.microsoft.com/library/security/ms14-012>)。

*9 Oracle、「開発者 - ブラウザでのJavaコンテンツ - セキュリティ・マニフェストの変更」(https://www.java.com/ja/download/faq/signed_code.xml)。

*10 株式会社日本レジストリサービス(JPRS)、「(緊急)BIND 9.xの脆弱性(DNSサービスの停止)について(2014年1月14日公開)」(<http://jprs.jp/tech/security/2014-01-14-bind9-vuln-nsec3-handling.html>)。

*11 "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" (http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar14.html)。

*12 攻撃の詳細については、次のKrebs on Security Blogに詳しい。"Blogs of War: Don't Be Cannon Fodder" (<http://krebsonsecurity.com/2014/03/blogs-of-war-dont-be-cannon-fodder/>)。

1月のインシデント

1	脆	1日: Cisco社の複数のLinksys機器にリモートからルータのリセットや、adminパスワードの取得が可能なバックドアが見つかり、研究者が詳細を公開した。 詳細については次の研究者のGitHubを参照のこと。"elvanderb/TCP-32764" (https://github.com/elvanderb/TCP-32764)。
2		
3	セ	2日: US-CERTは、12月に発覚した大手小売り事業者の情報流出の原因となったPOS端末に感染するマルウェアについて、注意喚起を行った。 US-CERT, "Alert (TA14-002A) Malware Targeting Point of Sale Systems" (http://www.us-cert.gov/ncas/alerts/TA14-002A)。
4		
5	セ	4日: 複数のオンラインゲームで、何者かによるDDoS攻撃が行われ、サービス停止などの影響が出た。この攻撃は特定の利用者に対する攻撃の可能性が指摘されている。
6		
7	セ	6日: 独立行政法人日本原子力研究開発機構は、高速増殖炉もんじゅの事務処理用パソコン1台がウイルスに感染し、情報流出の可能性があることを公表した。 「コンピュータウイルス感染による情報漏えいの可能性について」 (http://www.jaea.go.jp/02/press2013/p14010601/index.html)。
8	セ	6日: 米国Yahoo!は、年末年始の期間に欧州の自社サイトに配信した広告のいくつかで不正サイトからのマルウェアへの誘導が行われていたことを公表した。 詳細については例えば次のトレンドマイクロ社のSECURITY BLOGを参照のこと。「『Yahoo!』広告経由での感染事例、被害の分かれ目はパッチ管理とセキュリティ対策ソフト」 (http://blog.trendmicro.co.jp/archives/8421)。
9		
10		
11	セ	8日: 韓国で、大手クレジットカード3社から延べ8,500万件のクレジットカード情報が、カード会社と契約していた信用情報会社の社員により流出していたことが発覚した。
12		
13	セ	11日: オンラインストレージサービスのDropboxでメンテナンス時の不具合により、2日間に渡るサービス障害が発生した。 この障害については、次のDropboxの公式blogに詳しい。"Outage post-mortem" (https://tech.dropbox.com/2014/01/outage-post-mortem/)。
14		
15	脆	15日: ntpdのmonlist機能がDoSを引き起こす可能性のあるとして、注意喚起が行われた。 US-CERT, "Alert (TA14-013A) NTP Amplification Attacks Using CVE-2013-5211" (http://www.us-cert.gov/ncas/alerts/TA14-013A)。
16	脆	15日: Microsoft社は、2014年1月のセキュリティ情報を公開し、MS14-002を含む4件の重要な更新をリリースした。 「2014年1月のセキュリティ情報」 (http://technet.microsoft.com/ja-jp/security/bulletin/ms14-jan)。
17	脆	15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。 「APSB14-01: 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/acrobat/apsb14-01.html)。
18	脆	15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。 「APSB14-02: 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/apsb14-02.html)。
19	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36件の脆弱性を含む合計144件の脆弱性を修正した。 "Oracle Critical Patch Update Advisory - January 2014" (http://www.oracle.com/technetwork/topics/security/cpujan2014-1972949.html)。
20	セ	15日: Symantec社は、日本の大手出版社のWebサイトが改ざんされ、Toolkitによる不正サイトからのマルウェアへの誘導が行われていたことを発表した。 詳細については次のSymantec社のSecurity Response Blogを参照のこと。「日本の大手出版社の Web サイトが Gongda 悪用ツールキットに利用される」 (http://www.symantec.com/connect/ja/blogs/web-gongda)。
21		
22		
23	他	23日: セキュリティ関連企業から、動画再生ソフトであるGOM playerの更新機能を不正利用したマルウェア感染について注意喚起が行われた。 1月6日に発表された、日本原子力研究開発機構で発生したウイルス感染事件の原因とされている。詳細については次の韓国GRETECH JAPAN Corp社のお知らせを参照のこと。「マルウェア(ウイルス)感染に関するお詫びと調査結果のご報告」 (http://www.gomplayer.jp/player/notice/view.html?intSeq=300)。
24		
25	他	29日: GMOグローバルサイン社のルート証明書が有効期限を迎え、更新されていない場合に接続ができなくなったり、クライアント側で警告が出るなどの影響が発生した。 GMOグローバルサイン社、「旧ルート証明書の有効期限切れに伴う影響範囲について」 (https://jp.globalsign.com/support/faq/538.html)。
26		
27	他	30日: IPAより、2012年10月から2013年12月までの標的型攻撃メールを分析した技術レポート「標的型攻撃メールの傾向と事例分析 <2013年>」が公開された。 「標的型攻撃メールの傾向と事例分析 <2013年>」 (http://www.ipa.go.jp/security/technicalwatch/20140130.html)。
28		
29	セ	31日: 米国Yahoo!のYahoo! Mailで一部アカウントに対するリスト型攻撃による不正ログインが発生した。 Yahoo! Inc., "Important Security Update for Yahoo Mail Users" (http://yahoo.tumblr.com/post/75083532312/important-security-update-for-yahoo-mail-users)
30		
31		

[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

しました。SNS関連サイトや出版・放送関連の複数の企業のWebサイト、交通機関や金融機関のWebサイトでも発生しています。誘導されたサイトでは、未修正の脆弱性を含むいくつかの脆弱性を悪用して、ドライブバイダウンロードによるマルウェアの感染活動が行われていました。これらのWeb改ざんは著名な企業のWebサイトでも発生しており今後も注意が必要です。

■ ccTLDへの攻撃

ccTLDを含むドメインレジストリに対する攻撃と、それによるドメインハイジャックや情報の漏えいも継続して複数発生しています。1月には、モンテネグロのドメインである.meが何者かによる不正アクセスを受け、約3,500ドメインがハイジャックされる事件が発生しました。GoogleやYahoo、AmazonやFacebookなどのドメインの管理を行っているドメイン管理サービスのMarkMonitor社では、Syrian Electronic Armyを名乗る何者かによる管理ツールへの不正なアクセスによって、これらのドメイン情報の一部が書き換えられる事件が発生しています。

3月には、ベネズエラのISPが、Google Public DNS (8.8.8.8)の経路情報を広報したことから、ベネズエラとブラジルのネットワークでGoogle Public DNS宛の通信に影響が出ています。Google Public DNSについては、トルコで本来のサーバとは異なるサーバと通信している可能性があることが分かり、政府による検閲の可能性が指摘されています^{*13}。また、トルコでは、これ以外にもTwitterやYouTubeへのアクセスが禁止されていて、政府によるインターネットへの制限が強化されていることが伺えます。

■ Bitcoin

仮想通貨であるBitcoin^{*14}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Bitcoin取引所の1つであるMt.Goxが、技術的な問題が発生したとして一時的に取引を中止する措置を発表し

ました。この数日後には、同じくBitcoin取引所の1つであるBitstampでも問題が発生したとして取引を一時的に停止しました。これらの取引所では、BitcoinのTransaction Malleabilityの問題を悪用したDoS攻撃を受けていたことを公表しています^{*15}。この問題は、Bitcoinの取引に使われる固有の番号であるトランザクションIDを書き換えて広報することで、取引の妨害や多重取引を行える可能性があるものでした。Bitstampは、その後、対応を行ったとして取引を再開しましたが、Mt.Goxについては、この問題により、預かっていたBitcoinが盗まれたとして、約65億円の負債により経営破たんし、日本の民事再生法の適用を申請しました。しかし、破たん前から不透明な取引が指摘されていたことから、事業内容が明らかでないとして申し立ては棄却され、破産手続きが開始されています^{*16}。

Mt.Goxについては、この問題が2011年から指摘されていたにも関わらず、システム改修を行わず放置していたことが明らかとなっています。さらに、盗まれたとされた資産の一部が古いBitcoinウォレットから見つかったことを公表したり^{*17}、第三者による調査結果が公表され、問題によって盗まれた可能性のある約74万XBTのBitcoinのうち、この問題によって盗まれたのは、約386XBTだけである可能性が指摘されています。

これ以外にも、仮想通貨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、WebサイトへのDDoS攻撃や、不正侵入によりBitcoinそのものが盗まれたり、サイトのアカウント情報が盗まれるなどの事件が多く発生しています。また、米国の複数の報道機関でBitcoinの作者とされるSatoshi Nakamoto氏が見つかったとの報道がされましたが、Nakamoto氏とされた本人は否定しています。更に、現在Bitcoinの取り扱いに関する議論が各国で活発に行われています。日本でも3月に通貨に該当しないとの見解について閣議決定が行われています。

*13 Google Online Security Blog, "Google's Public DNS intercepted in Turkey" (<http://googleonlinesecurity.blogspot.jp/2014/03/googles-public-dns-intercepted-in-turkey.html>).

*14 Bitcoinについては、本レポートのVol.21 (http://www.ijj.ad.jp/development/iir/pdf/iir_vol21.pdf)の「1.4.3 仮想通貨Bitcoin」で紹介している。

*15 Bitstamp, "BITCOIN WITHDRAWAL PROCESSING SUSPENDED" (<http://www.bitstamp.net/article/bitcoin-withdraws-suspended/>).

*16 株式会社MTGOX, 「破産手続開始決定のお知らせ - 基本的なご質問に対する回答」 (http://www.mtgox.com/img/pdf/20140424_announce_qa_ja.pdf).

*17 株式会社MTGOX, 「当社保有ビットコインの残高に関するお知らせ」 (<http://www.mtgox.com/img/pdf/20140320-btc-announce.pdf>).

2月のインシデント

1	セ 3日：航空会社の会員向けWebサイトで不正アクセスが発生し、通信販売サイトのポイントに交換される事件が発生した。
2	セ 3日：東京大学 国際高等研究所 カブリ数物連携宇宙研究機構で、スーパーコンピュータシステムが外部からの不正アクセスを受けたことを公表した。この事件では侵入されたシステムを通じて、共同研究を行っていた国立天文台など、外部の研究機関への不正アクセスも確認されたことから各研究機関で対応が行われた。
3	「カブリ数物連携宇宙研究機構(Kavli IPMU)の発表を参照のこと。」「カブリ数物連携宇宙研究機構の研究用計算機への不正アクセスについて」(http://www.ipmu.jp/ja/node/1831)。
4	脆 5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。
5	「APSB14-08: 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/apsb14-06.html)。
6	他 5日：経済産業省と一般社団法人JPCERTコーディネーションセンターは、制御システムにおける国内外の技術動向の紹介を通じ、制御システムのセキュリティ向上に向けた検討を行う「制御システムセキュリティカンファレンス 2014」を開催した。
7	JPCERTコーディネーションセンター、「制御システムセキュリティカンファレンス 2014開催のご案内」(https://www.jpCERT.or.jp/event/ics-conference2014.html)。
8	セ 6日：独立行政法人 国立がん研究センターは、国立がん研究センター東病院のパソコン2台がウイルス感染し、患者情報などが漏えいした可能性があることを公表した。
9	詳細については次の国立がん研究センターの発表を参照のこと。「国立がん研究センター東病院における動画再生ソフトウェアアップデートプログラムによるコンピュータウイルス感染について」(http://www.ncc.go.jp/jp/information/20140206.html)。
10	セ 7日：Bitcoinの取引所の1つであるMt. Goxは、技術トラブルを修正するためとしてビットコインの払い出しを一時停止した。この後、2月28日にサイバー攻撃によるBitcoinと銀行預金の流出のため、債務超過に陥ったとして、民事再生手続を申請した。
11	
12	セ 12日：Bitcoin取引所のMtGoxやBitStampなどが、トランザクション展性を悪用した取引妨害攻撃を受けたとして口座からの引き出しを一時停止した。この影響でBitcoinの対ドルレートが一時急落するなどの影響が出た。
13	この問題については、チューリッヒ大学の研究者チームによってMt.GOXに対する検証が行われており、この問題による影響は限定的だったとの反論も行われている。Christian Decker and Professor Roger Wattenhofer, "Bitcoin Transaction Malleability and MtGox" (http://arxiv.org/pdf/1403.6676v1.pdf)。
14	脆 12日：Microsoft社は、2014年2月のセキュリティ情報を公開し、MS14-007やMS14-010、MS14-011を含む4件の緊急と3件の重要な更新をリリースした。
15	「2014年2月のセキュリティ情報」(http://technet.microsoft.com/ja-jp/security/bulletin/ms14-feb)。
16	脆 12日：Adobe Shockwave 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。
17	「APSB14-06: Adobe Shockwave Player用セキュリティアップデート公開」(http://helpx.adobe.com/jp/security/products/shockwave/apsb14-06.html)。
18	他 12日：一昨年発生したパソコン遠隔操作ウイルス事件で、昨年逮捕された容疑者の初判が東京地裁で行われた。
19	他 13日：米国立標準技術研究所(NIST)は重要インフラ分野の組織や企業が情報セキュリティ対策を行う上で指標となる"Framework for Improving Critical Infrastructure Cybersecurity"を公表した。
20	NIST, "NIST Releases Cybersecurity Framework Version 1.0" (http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm)。
21	脆 17日：米国 Cisco Linksys社の複数のルータに、CGIスクリプトの脆弱性があり、これを悪用したTheMoonと呼ばれるマルウェアの感染が複数発生していることが報告された。
22	詳細については次の米国SANS ISCのInfoSec Diaryを参照のこと。"Linksys Worm "TheMoon" Summary: What we know so far" (https://isc.sans.edu/forums/diary/Linksys+Worm+TheMoon+Summary+What+we+know+so+far/17633)。
23	他 17日：日本発の情報セキュリティ国際会議としてCODEBLUEが2日間の日程で開催された。
24	詳細については次のCODEBLUE公式サイト(http://codeblue.jp/)を参照のこと。
25	セ 18日：検索サイトの検索連動型広告を悪用し、複数の金融機関の偽サイトへの誘導が行われていたことが発覚し、対応が行われた。
26	この事件については次の発表を参照のこと。「検索連動型広告の悪用に関する続報と対策について」(http://advertisingblog.yahoo.co.jp/2014/02/post_33.html)。
27	脆 20日：Microsoft社は、Internet Explorerに未修正の脆弱性があり、悪用されるとリモートでコードが実行される可能性があるとしてアドバイザリを公開した。この脆弱性については公開された時点で既に悪用が確認されていた。
28	「マイクロソフト セキュリティ アドバイザリ (2934088) Internet Explorer の脆弱性により、リモートでコードが実行される。」(http://technet.microsoft.com/ja-jp/security/advisory/2934088)。
29	脆 21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。
30	「APSB14-07: 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/apsb14-07.html)。
31	セ 24日：はてなは、提供しているサービスに対して、外部から不正ログインされた可能性があるとしてパスワード変更や登録内容の確認を行うよう注意喚起を行った。
32	株式会社はてな、「不正ログイン防止のため、パスワードと登録情報のご確認をお願いします」(http://hatena.g.hatena.ne.jp/hatena/20140224/1393211701)。
33	他 27日：IPAは、オフィス機器や家電製品のインターネット接続に伴う新たな脅威や、不用意な外部公開を確認する手順をまとめた「増加するインターネット接続機器の不適切な情報公開とその対策」を公開した。
34	「IPAテクニカルウォッチ「増加するインターネット接続機器の不適切な情報公開とその対策」」(http://www.ipa.go.jp/security/technicalwatch/20140227.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

■ 業務システムへの攻撃

昨年11月に発生した、米国の大手小売業者による顧客のカード情報の漏えい事件では、その後の調査で4000万人分のカード情報と、それ以外に7000万人分の顧客データが盗まれた可能性があることが判明しています。また、その手口についてはカードリーダーとレジを狙う特殊なマルウェアであるPOSマルウェアが利用されたことが分かりました。更に、この企業以外にも高級百貨店など複数の企業が同様の攻撃を受けていたことを発表しています^{*18}。

これらの攻撃で使われたマルウェアは、暗号化してやりとりされているクレジットカードなどのデータを、支払処理の際に、レジで復号したタイミングを狙って情報を盗み出すようになっており、盗んだデータは外部のサーバに送信されていました^{*19}。

今回の事件では、被害にあった事業者の取引業者に貸与したIDが不正に盗まれて悪用されたため、この事業者のネットワークに侵入した上で、攻撃が行われていたとされています。この事業者では、設備の管理システムと顧客情報の管理システムがネットワークで繋がっていたことなどが伝えられており、情報セキュリティ対策に不備があったことも、大規模な情報漏えいに繋がった原因とされています。

産業用システムやPOSシステムなどの業務用端末は、インターネットに直接つながっていなかったりすることから、企業で利用しているPCでは行われているセキュリティ上の対策やソフトウェア更新などが行われていないなど、適切な管理が行われていない場合が多く見受けられます。そのような状況から、POS端末などの業務システムに対する攻撃は今後も継続することが考えられ、注意が必要です。

■ 正規のソフトウェアを介した攻撃

1月には、独立行政法人日本原子力研究開発機構の高速増殖原型炉もんじゅで、従業員が共同で使用しているPCからウイルスが見つかったとの発表が行われました^{*20}。また、2月には国立がん研究センター東病院で同じくPC2台がウイルスに感染していたことが公表されています^{*21}。これらのウイルス感染は、動画再生ソフトの正規のアップデート機能を悪用したものでした。この事件ではユーザがインストールしていた正規のソフトウェアが利用しているアップデートサーバが不正アクセスを受けて、改ざんされていました。このため、ソフトウェアのアップデートの際に、本来のアップデートサーバから意図しない外部の第三者のサイトに誘導され、該当ソフトウェアのアップデートプログラムを装ったマルウェアがダウンロード、実行される可能性がありました^{*22}。

このように正規のソフトウェア管理の仕組みを悪用された事例としては、2013年3月に韓国の複数の放送局や金融機関で多数のPCでシステム停止が発生した事件があります。この事件では被害企業内の更新管理サーバ(Patch Management System)が不正アクセスを受け、これを介してシステム破壊を行うマルウェアが企業内の端末に配布されていました^{*23}。また、最近では正規のアプリやブラウザの拡張機能などを入手し、正規のソフトウェアに不正な機能を組み込んでアップデートとして配布する事件も発生しています^{*24}。

これらの問題に対処するためには、インストール済みのソフトウェアのアップデートが正当なものであるかどうかを検証する仕組みの導入や、企業内のソフトウェアアップデートサーバのセキュリティの強化などを行う必要があります。

*18 Krebs on Security, "Hackers Steal Card Data from Neiman Marcus" (<http://krebsonsecurity.com/2014/01/hackers-steal-card-data-from-neiman-marcus/>)。

*19 詳細については、次のKaspersky Lab社のBlogに詳しい。「レジやPOSを狙うマルウェア」(<http://blog.kaspersky.co.jp/ram-scrapers-and-other-point-of-sale-malware/>)。

*20 独立行政法人日本原子力研究開発機構、「コンピュータウイルス感染による情報漏えいの可能性について」(<http://www.jaea.go.jp/02/press2013/p14010601/index.html>)。

*21 独立行政法人国立がん研究センター、「国立がん研究センター東病院における動画再生ソフトアップデートプログラムによるコンピュータウイルス感染について」(<http://www.ncc.go.jp/jp/information/20140206.html>)。

*22 株式会社グレテックジャパン、「マルウェア(ウイルス)感染に関するお詫びと調査結果のご報告」(<http://www.gomplayer.jp/player/notice/view.html?intSeq=300&page=1>)。

*23 この事件については、本レポートのVol.19 (http://www.ij.ad.jp/development/iir/pdf/iir_vol19.pdf)の「1.4.1 韓国3.20大乱」で解説している。

*24 この事件については、例えば、実際に3万人のユーザがいたchrome拡張機能を売却した際の顛末を、作者であるAmit Agarwal氏がブログで報告している。"Selling a Google Chrome Extension is Easy but Monetizing is Tricky" (<http://www.labno.org/internet/sold-chrome-extension/28377/>)。

3月のインシデント

1	脆	5日：フランス国立情報学自動制御研究所 (INRIA) のセキュリティ研究者によって、中間者攻撃によりクライアント証明書が盗まれる可能性のある TLS への新たな攻撃手法が公表された。
2		詳細については次の発表を参照のこと。"Triple Handshakes Considered Harmful Breaking and Fixing Authentication over TLS" (https://secure-resumption.com/)。
3	脆	6日：GnuTLS に、特定の条件における証明書の検証に不具合があり、正規の Web サイトを装った中間者攻撃を仕掛けることが可能な脆弱性が見つかり修正された。
4		US-CERT、"GnuTLS Releases Security Update" (http://www.us-cert.gov/ncas/current-activity/2014/03/05/GnuTLS-Releases-Security-Update)。
5	他	7日：日本政府は、ビットコインに関する質問主意書に対し、日本においては通貨に該当しないなどの政府見解をまとめ、閣議決定を行い公表した。参議院、「ビットコインに関する質問主意書」 (http://www.sangiin.go.jp/japanese/joho1/kousei/syuisyo/186/meisai/m186028.htm)。
6	セ	10日：別の航空会社の会員向け Web サイトで不正ログインが発生し、マイルを別のポイントに交換される事件が発生したことを公表した。
7	他	10日：IPA は、脆弱性の発見方法、対策について実習形式で体系的に学習できる脆弱性学習ツール「AppGoat」について、新しい演習テーマと脆弱性の修正演習を追加したウェブアプリケーション版を公開した。
8		「脆弱性体験学習ツール AppGoat」 (http://www.ipa.go.jp/security/vuln/appgoat/index.html)。
9	脆	12日：Microsoft 社は、2014年3月のセキュリティ情報を公開し、MS14-012とMS14-013の2件の緊急と3件の重要な更新をリリースした。
10		「2014年3月のセキュリティ情報」 (http://technet.microsoft.com/ja-jp/security/bulletin/ms14-mar)。
11	脆	12日：Adobe Flash Player に、情報漏えいの可能性がある脆弱性を含む複数の脆弱性が発見され、修正された。
12		「APSB14-08: 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/apsb14-08.html)。
13	脆	12日：Adobe Shockwave 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。
14		「APSB14-08: 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/apsb14-08.html)。
15	セ	12日：CMS である WordPress で投稿にリンクが張られたことを知らせる Pingback 機能を悪用した大規模な DDoS 攻撃が発生した。
16		Sucuri Blog、"More Than 162,000 WordPress Sites Used for Distributed Denial of Service Attack" (http://blog.sucuri.net/2014/03/more-than-162000-wordpress-sites-used-for-distributed-denial-of-service-attack.html)。
17	脆	13日：Samsung Galaxy シリーズに、リモートからファイルの操作を実行可能な機能が含まれていることが公表された。
18		詳細については次の Free Software Foundation の Blog を参照のこと。"Replicant developers find and close Samsung Galaxy backdoor" (http://www.fsf.org/blogs/community/replicant-developers-find-and-close-samsung-galaxy-backdoor)。
19	セ	17日：ブラジルとベネズエラで Google Public DNS の経路が一時的に BGP ハイジャックされる事件が発生した。
20		この事件については次の BGP Mon の twitter のつぶやきで確認できる。 (https://twitter.com/bgpmon/status/445266642616868864/photo/1)。
21	脆	18日：メッセージアプリの IP 電話機能に発信者番号の偽装ができる不具合が見つかり、話題となった。
22	他	18日：全府省庁や内閣官房情報セキュリティセンター、重要インフラ事業者などの担当者約 100 人が参加し、府省庁をまたがる情報の収集や共有、緊急対応の訓練を行った。
23		内閣官房情報セキュリティセンター、「全府省庁等の参加による大規模な政府サイバー攻撃対処訓練を初実施 ～【3・18訓練】～」 (http://www.nisc.go.jp/active/kihon/pdf/318.pdf)。
24	脆	19日：Apache HTTP Server に DoS 攻撃可能な脆弱性を含む複数の脆弱性が見つかり修正された。
25		The Apache Software Foundation、"Apache HTTP Server 2.2.27 Released" (http://www.apache.org/dist/httpd/Announcement2.2.html)。
26	他	19日：2002年に開設され、脆弱性情報の公開や議論の場として活用されてきた Full Disclosure ML が終了した。なお、3月25日に別の管理者によって、同名の Full Disclosure ML として再開されている。
27		seclists.org、"Administrivia: The End" (http://seclists.org/fulldisclosure/2014/Mar/332)。
28		seclists.org、"Administrivia: A Fresh Start" (http://seclists.org/fulldisclosure/2014/Mar/333)。
29	他	20日：一般社団法人インターネットコンテンツセーフティ協会は、4月1日よりファイル共有ソフトを悪用した児童ポルノ流通防止対策の取り組みとして、当該コーザに対する連絡メールの送信を実施することを発表した。
30		「ファイル共有ソフトを悪用した児童ポルノ流通への対策について」 (http://www.netsafety.or.jp/p2p/index.html)。
31	脆	25日：Microsoft 社は、Microsoft Word に任意のコード実行が可能な未修正の脆弱性があり、この脆弱性を悪用した標的型攻撃が確認されたとして、アドバイザリーを公開した。
32		「Microsoft Word 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/library/security/2953095)。
33	他	26日：防衛省は、高度化・複雑化するサイバー攻撃の脅威に対応するため、サイバー防衛隊を新編した。
34		防衛省、「サイバー防衛隊の新編について」 (http://www.mod.go.jp/j/press/news/2014/03/25d.html)。
35	他	27日：警察庁は、サイバー犯罪の検挙状況についてまとめた「平成25年中のサイバー犯罪の検挙状況等について」を公表した。検挙件数は 8,113 件で前年比 10.6% 増となっており過去最高を記録している。
36		警察庁、「平成25年中のサイバー犯罪の検挙状況等について」 (https://www.npa.go.jp/cyber/statics/h25/pdf01-2.pdf)。
37	他	31日：IPA より、「2014年版 情報セキュリティ10大脅威」が公表された。
38		「2014年版 情報セキュリティ10大脅威」 (https://www.ipa.go.jp/security/vuln/10threats2014.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

■ 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、1月に「第38回情報セキュリティ政策会議」が開催され、昨年6月に決定した「サイバーセキュリティ戦略」*25とそれを受けて、2013年度の各府省庁の取り組みを定めた「サイバーセキュリティ 2013」*26について、評価指標に基づくデータの把握と評価に関する基本方針が取りまとめられました。また、政府機関の情報セキュリティ対策のための統一規範などについても検討されています。更には深刻化・高度化するサイバー空間の脅威やその対応策等について理解を深めるため、2月の最初のワーキングデーを「サイバーセキュリティの日」と定め、サイバー空間の安全に資する取り組みを重点的に行うことを決定しています。また、2月には「IT利活用セキュリティ総合戦略推進部会」が開催され、今後のIT利活用を見据えた情報セキュリティ政策の総合的・戦略的推進について、検討が行われています。3月18日には、複数の政府機関を同時に狙うサイバー攻撃が発生したことを想定し、内閣官房情報セキュリティセンターと各府省庁及び重要インフラ事業者等との間の情報収集・共有訓練とCYMAT要員による緊急対処訓練が実施されました。

■ その他

1月にはICANNより新しいgTLDとして「TOKYO」と「NAGOYA」が承認されました。また3月には「OKINAWA」も承認されています*27。これは2012年1月からICANNが進めているgTLDの新規承認プロセス*28によるものです。現在、世界中から二千近い新gTLDの申請が行われており、今後も次々と新たなgTLDが承認されていくこととなります。

警察庁から、「平成25年中のインターネットバンキングに係る不正送金事犯の発生状況等について」*29が発表され、

平成25年中の発生状況は、1,315件となり、被害金額も約14億600万円と過去最大の被害であったことが報告されました。また、特に6月以降に発生件数が急増しており、IDやパスワードの入手手段として、ウイルスにより表示された不正画面に入力を促して盗むものが多くみられたことや、11月以降には、メールによるフィッシングサイトへの誘導が多発していることが報告されています。

2月には不正に入手したIDとパスワードを用いてISPへのアクセスを行ったとして、プロキシサーバを運営していた会社の社長他2名が、不正アクセス禁止法違反容疑で逮捕されています。この会社で運営していたプロキシサーバは、記録を取っておらず、利用者の追跡ができない状態で運用されていたことから、ネットバンキングの不正送金や標的型攻撃のメール送信に利用されていたとされています。

同じく2月には、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の初公判が行われました。容疑者は無罪を主張しています。

3月には総務省から、ISPやインターネットエクスチェンジ及び研究者の協力を得て実施している、インターネットにおけるトラヒックの定期的な集計・試算の2013年11月の集計結果が公表されました*30。これによると2013年11月時点のブロードバンドサービス契約者の推定総ダウンロードトラヒックは、約2.6Tbpsとなり、前年同月に比べ35.6%増加となっています。また、総アップロードトラヒックは、推定で約834Gbpsとなっており、こちらも前年同月に比べて25.2%増加しています。

*25 内閣官房情報セキュリティセンター、「情報セキュリティ政策会議 第35回会合(平成25年6月10日)」(<http://www.nisc.go.jp/conference/seisaku/index.html#seisaku35>)。

*26 内閣官房情報セキュリティセンター、「情報セキュリティ政策会議 第36回会合(平成25年6月27日)」(<http://www.nisc.go.jp/conference/seisaku/index.html#seisaku36>)。

*27 承認されたgTLDについては次のICANN"DELEGATED STRINGS"(<http://newgtlds.icann.org/en/program-status/delegated-strings>)で確認できる。

*28 ICANN, "New gTLDs Update: Applications Accepted Today; New Guidebook Posted; Financial Assistance for Qualifying Applicants" (<http://www.icann.org/en/news/announcements/announcement-11jan12-en.htm>)。

*29 警察庁、「平成25年中のインターネットバンキングに係る不正送金事犯の発生状況等について」(http://www.npa.go.jp/cyber/pdf/H260131_banking.pdf)。

*30 総務省、「我が国のインターネットにおけるトラヒックの集計・試算」(http://www.soumu.go.jp/menu_news/s-news/01kiban04_02000077.html)。

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、脆弱性等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1月から3月の期間にIJ DDoSプロテクション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、IJ DDoSプロテクション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。IJ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IJは、495件のDDoS攻撃に対処しました。1日あたりの対処件数は5.5件で、平均発生件数は前回のレポート期間と比べてほとんど変わりません。DDoS攻撃全体に占める割合は、サーバに対する攻撃が61%、複合攻撃が20.8%、回線容量に対する攻撃が18.2%でした。

今回の対象期間で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60万1千ppsのパケットによって2.86Gbps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90.5%が攻撃開始から30分未満で終了し、9.5%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、今回もっと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10時間55分にわたりました。また、この期間中に話題となったNTPによる攻撃では、最大で51万7千ppsのパケットによって1.8Gbpsの通信量を発生させる攻撃が発生しています。

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。

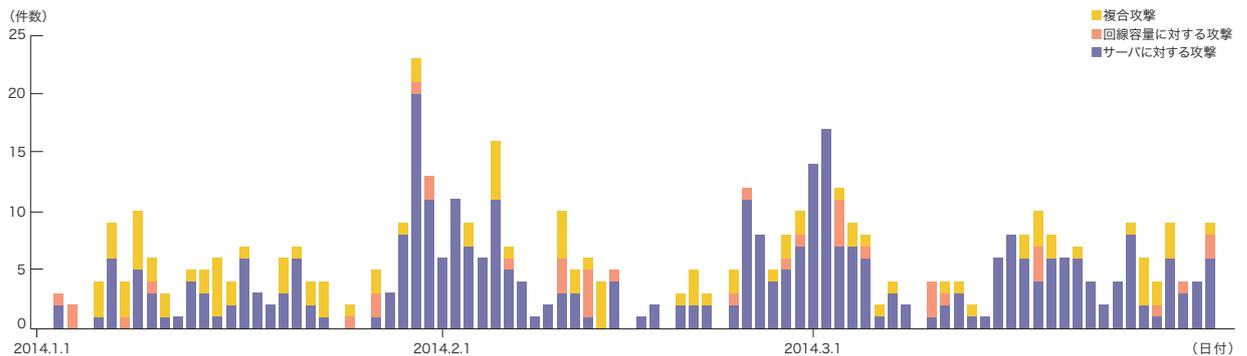


図-2 DDoS攻撃の発生件数

*31 攻撃対象に、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、IJJ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1月から3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33.1%を占めています。またDNSに

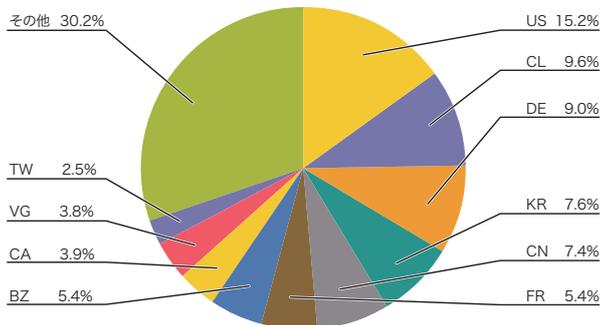


図-3 backscatter観測によるDDoS攻撃対象の分布 (国別分布、全期間)

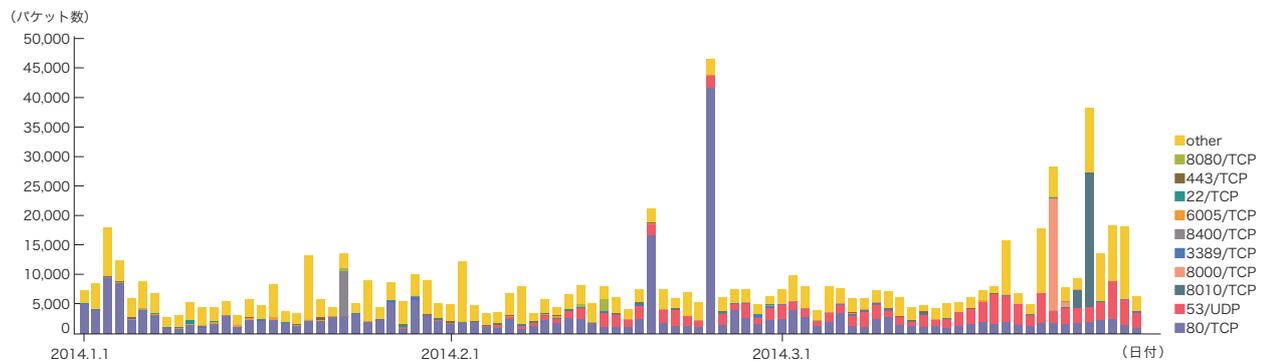


図-4 DDoS攻撃によるbackscatter観測(観測パケット数、ポート別推移)

*35 IJJ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。「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、本レポートのVol.8 (http://www.ijj.ad.jp/development/ijr/pdf/ijr_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、IJJによる観測結果の一部について紹介している。

利用される53/UDP、リモートデスクトップで利用される3389/TCPやSSHで利用される22/TCPなどへの攻撃、通常は利用されない8010/TCPや8000/TCPなどの攻撃が観測されています。

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15.2%が最も大きな割合を占めていました。その後にチリの9.6%、ドイツの9.0%といった国が続いています。前回に引き続きチリのIPアドレスを多く観測していますが、これは複数のIPアドレスから複数のハニーポットの445/TCPに対するパケットを当期間中、合計で7万2千回以上観測したためです。

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、1月2日から4日にかけて米国のホスティング事業者、2月18日にはドイツのホスティング事業者、また、2月23日から24日にかけて香港のホスティング事業者がベリーズ国内に持つIPアドレスに対する攻撃をそれぞれ観測しています。1月23日には中国国内のサーバに対する8400/TCPへの攻撃が、3月24日にはドイツにあるロシア語サイトに対する8000/TCPへの攻撃が、また、3月26日から27日にかけて英領バージン諸島のISPが持つIPアドレスに対する8010/TCPへの攻撃が観測されています。

今回の期間では、2月4日からDNS(53/UDP)のbackscatterが増加傾向にあります。そのほとんどは、多数のIPアドレス

に、ランダムな文字列を含むドメイン名を問い合わせた結果と考えられるパケットでした。これらのパケットと直接に関連するかどうかは不明ですが、4月15日にJPRSからキャッシュポイズニング攻撃の危険性増加に対して注意喚起が発表されています*37。DNSサーバの設定を再確認すると共に、今後の動向に注意していく必要があります。

また、1月4日にオンラインゲーム関連のサーバに対する攻撃を観測しましたが、これは複数のゲーム関連や技術関連のニュースサイトで報じられた攻撃の一部でした。

1.3.2 マルウェアの活動

ここでは、IJが実施しているマルウェアの活動観測プロジェクトMITF*38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*39を利用して、インターネットから到着する通信を観測

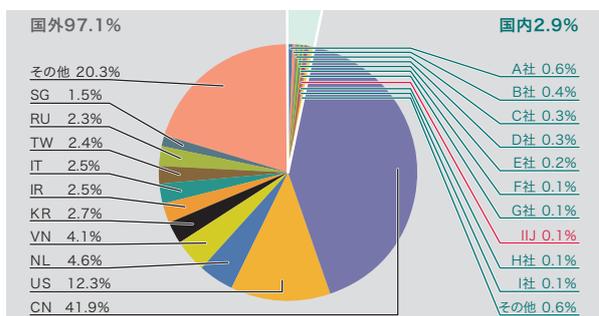


図-5 発信元の分布(国別分類、全期間)

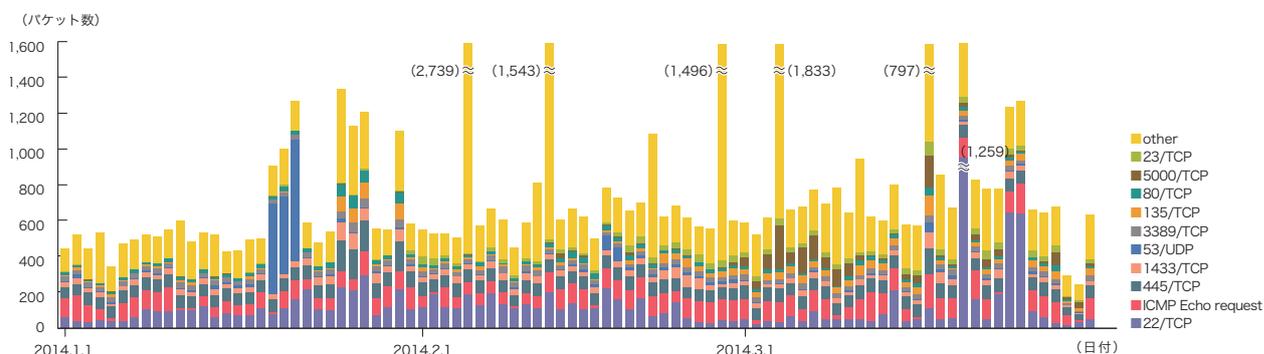


図-6 ハニーポットに到着した通信の推移(日別・宛先ポート別・1台あたり)

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。

■ 無作為通信の状況

2014年1月から3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SQL Server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、SSHで利用される22/TCP、HTTPで利用される80/TCP、ICMP Echo Request、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

*37 JPRS、「(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>)。

*38 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。

*39 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。

例えば3月20日に発生している通信はシンガポールと韓国、3月24日から3月25日にかけて発生している通信は、イタリアに割り当てられたIPアドレスからのものです。また、1月中旬から2月にかけて、SSHの通信が前回の期間中に比べて増加しています。これは主に中国に割り当てられたIPアドレスからの通信が増加したためです。

1月19日から1月21日にかけて、DNSの通信が増加しています。通信内容を確認したところ、オランダに割り当てられたIPアドレスが28ドメインに対し、ANYレコードの問い合わせを繰り返し試行していました。詳細に調査したところ、28のドメインはいずれも応答として比較的大きなサイズの応答をしていることから、攻撃者がこのオランダのIPアドレスを詐称して問い合わせを繰り返すことで、そのIPアドレスに対するDNSAmP攻撃の試行をしていたとIJでは考えています^{*40}。

また、2月5日にベトナム、2月12日、2月27日、3月4日に中国に割り当てられた1つのIPアドレスから、広範囲に繰り返し探査行為が行われています。対象となるポートは1000から9999までのTCPと一部のUDPでした。

(1台あたりの平均パケット数)

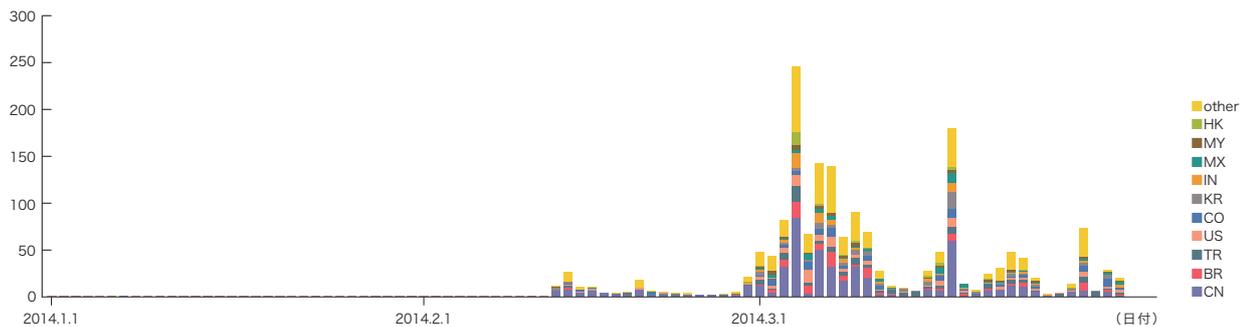


図-7 ハニーポットに到着した5000/TCPの通信の発信元IPアドレスの国別推移(ハニーポット1台あたりの平均値)

*40 ハニーポットはDNSの問い合わせを拒否するため、当該IPアドレスには増幅された応答は届いてはいない。

*41 警察庁の発表は以下のとおり。「脆弱性が存在するNASの探索と考えられる宛先ポート5000/TCPに対するアクセスの急増について(<http://www.npa.go.jp/cyberpolice/detect/pdf/20140305.pdf>)」。SANS ISCでは、次の4つのブログエントリで本事象に関するハニーポットのデータやマルウェアの調査結果を報告している。「TCP/5000 - The OTHER UPNP Port」(<https://isc.sans.edu/diary/TCP5000+-+The+OTHER+UPNP+Port/17763>)。「Port 5000 traffic and snort signature」(<https://isc.sans.edu/diary/Port+5000+traffic+and+snort+signature/17771>)。「Let's Finally "Nail" This Port 5000 Traffic - Synology owners needed.」(<https://isc.sans.edu/diary/Let%27s+Finally+%22Nail%22+This+Port+5000+Traffic+-+Synology+owners+needed./17859>)。「More Device Malware: This is why your DVR attacked my Synology Disk Station (and now with Bitcoin Miner!)」(<https://isc.sans.edu/diary/More+Device+Malware%3A+This+is+why+your+DVR+attacked+my+Synology+Disk+Station+%28and+now+with+Bitcoin+Miner!%29/17879>)。

*42 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。

*43 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。

■ 組み込み機器(NAS、DVR)に対する探査と攻撃

期間中、2月中旬以降から5000/TCPに対する探査行為が増加し始め、3月に大幅に増加しました。ハニーポットに到着した5000/TCP通信の送信元IPアドレスの総量(到着パケット数)の推移(ハニーポット1台あたりの平均値)を図-7に示します。

これは、Synology社のNASやHikvision社のDVR (Digital Video Recorder)製品への脆弱性の探査もしくは攻撃であると考えています。この製品に対する任意のコード実行が可能な脆弱性が2013年に発見されており、Exploitも既に公開されています。警察庁やSANS ISCもブログで同様の事象と思われる内容を複数回に渡って報告^{*41}しており、攻撃を受けたと思われる製品からこの製品には本来存在しないマルウェアと思われるプログラムが検出されたと報告しています。

■ 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-8に、マルウェアの総取得検体数の推移を図-9に、そのうちのユニーク検体数の推移を図-10にそれぞれ示します。このうち図-9と図-10では、1日あたりに取得した検体^{*42}の総数を総取得検体数、検体の種類をハッシュ値^{*43}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-9と図-10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114、ユニーク検体数が21でした。1月25日と3月17日にotherが増加しています。これらは、それぞれブラジルと台湾に割り当てられたIPアドレスからのAllapple^{*44}ファミリーが増加したことによります。Allappleはポリモーフィックマルウェアであることが知られており、図-10により顕著に表れていることが確認できます。

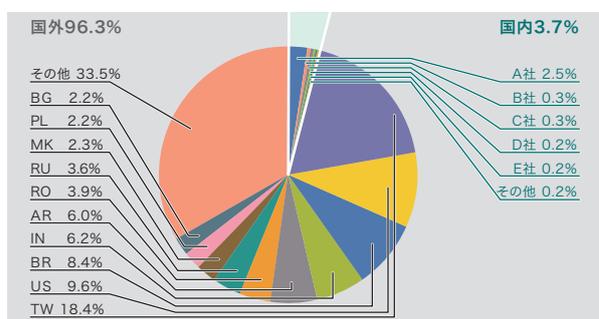


図-8 総取得検体数の分布

未検出の検体をより詳しく調査した結果、インドなど、複数の国に割り当てられたIPアドレスからワーム^{*45}が観測されました。また、未検出の検体の約71%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PC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。

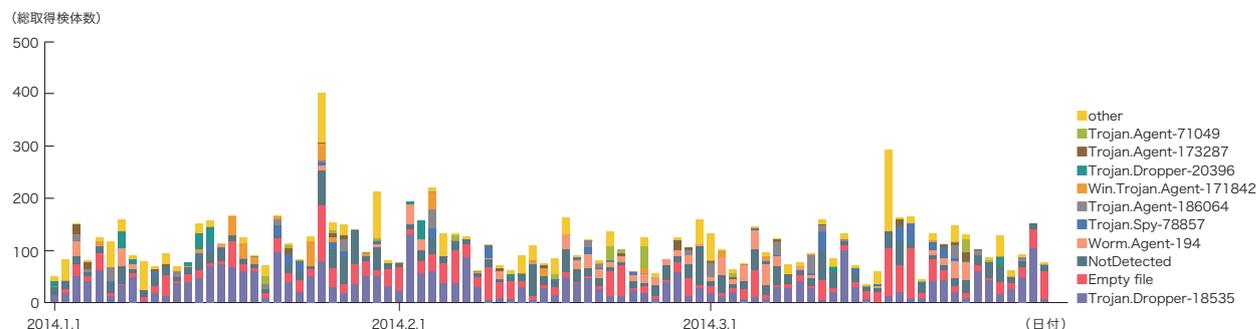


図-9 総取得検体数の推移 (Confickerを除く)

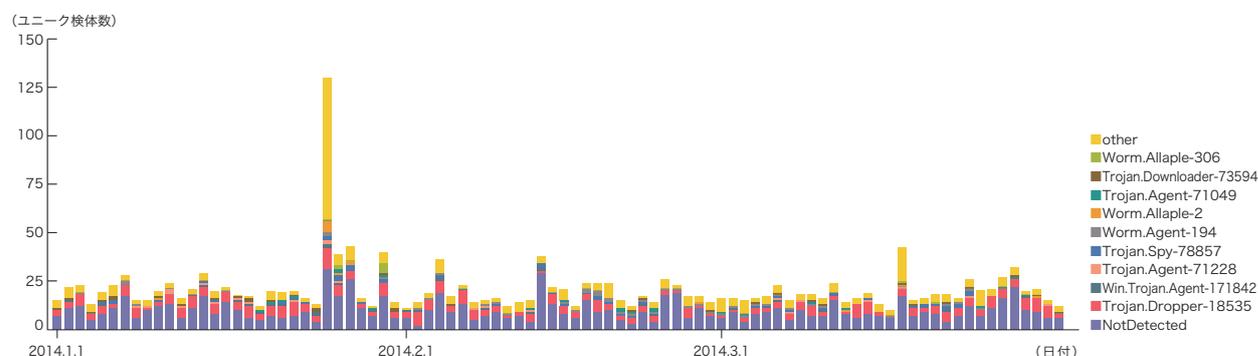


図-10 ユニーク検体数の推移 (Confickerを除く)

*44 Win32/Allapple (<http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?name=Win32%2fAllapple>).

*45 WORM_ATAK (http://about-threats.trendmicro.com/archive/Malware.aspx?language=jp&name=WORM_ATAK.D).

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92.4%、ボット型4.6%、ダウンロード型3.0%でした。また解析により、16個のボットネットC&Cサーバ^{*46}と7個のマルウェア配布サイトの存在を確認しました。

■ 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35,739、ユニーク検体数は787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99.7%、ユニーク検体数で97.3%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2%減少しています。また、ユニーク検体数は前号から約4%増加しました。Conficker Working Groupの観測記録^{*47}によると、2014年3月31日現在で、ユニークIPアドレスの総数は1,277,911とされています。2011年11月の約320万

台と比較すると、約40%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

IJ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^{*48}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、過去にもたびたび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1月から3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-11に、攻撃の推移を図-12にそれぞれ示します。これらは、IJ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。

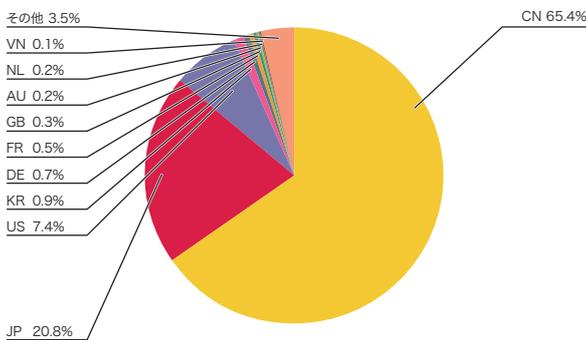


図-11 SQLインジェクション攻撃の発信元の分布

発信元の分布では、中国65.4%、日本20.8%、米国7.4%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大幅な増加が見られましたが、これはこの期間中、中国からの大規模な攻撃が複数発生したためで、これを除いた検知傾向はそれほど変化していません。

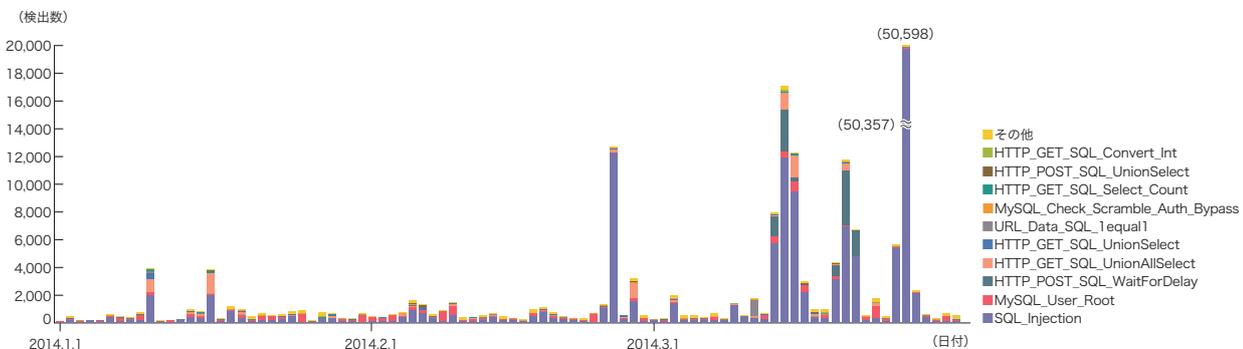


図-12 SQLインジェクション攻撃の推移(日別、攻撃種類別)

*46 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。

*47 Conficker Working Groupの観測記録(<http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking>)。

*48 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。

この期間中、2月25日には、中国の特定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。3月13日から15日にかけては、別の中国の複数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。この攻撃は3月19日から21日にかけても、中国の同じ特定の攻撃元を含む複数の攻撃元より同じ特定の攻撃先に対する攻撃が発生しています。3月25日から27日にかけては、別の中国の特定の攻撃元より別の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。

ここまでを示したとおり、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

ここでは、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*49(図-13)。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サイトなども観測対象に加えています。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1月から2月の中旬ごろまでは、Sweet Orange Exploit Kit及びRamayana Exploit Pack(別名DatkaChefまたはDotCacheF Exploit Kit)による攻撃が多くを占めていました。これは、昨年末から続いている傾向で、改ざんされ攻撃に悪用されているのも、中小企業やネットショップなど、比較的小規模なWebサイトが多くを占めていました。これらの攻撃は、Exploit Kitの傾向から、主に古いバージョンのJREの脆弱性などを攻撃対象にしているものと考えられます。

一方、2月後半以降は、攻撃の総数が激減し、Sweet Orange Exploit Kitを用いた攻撃はまったく観測されなくなりました。代わりに、Infinity Exploit Kit(別名Red Kit v2またはGoon Exploit Kit)による攻撃が増加しており、2月20日に公開され、当時パッチが未公開であったMicrosoft Internet Explorerの脆弱性(CVE-2014-0322)を悪用する攻撃が観測されました。この時期は、比較的高い知名度の大手企業のWebサイトの改ざんが複数発生しており、それらのほとんどのケースで前述のInternet Explorerの脆弱性を悪用する攻撃が行われていました。

3月下旬には、攻撃はほぼ収束傾向となり、国内でのドライブバイダウンロード攻撃が減少傾向にあるものと推測される状況となっています。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ため、Webサイト運営者、訪問者共に、引き続き注意が必要です。

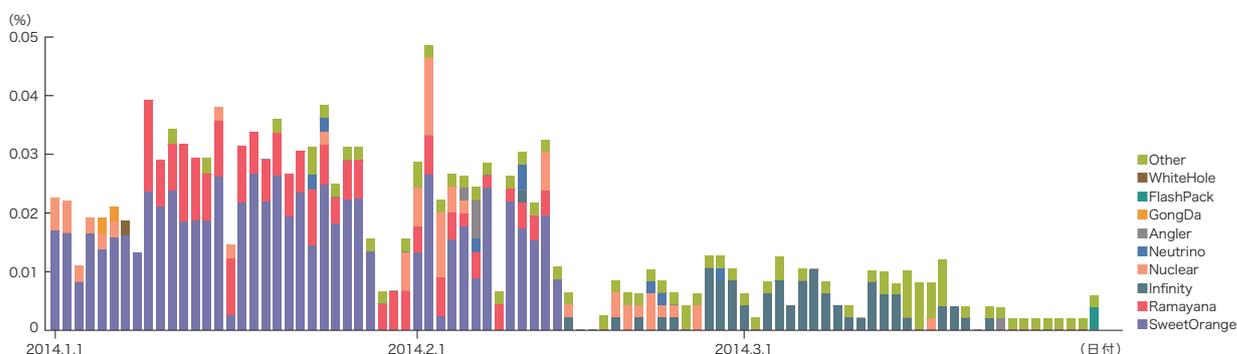


図-13 Webサイト閲覧時のドライブバイダウンロード発生率(%) (Exploit Kit別)

※ 調査対象は日本国内の数万サイト。

近年のExploit Kitでは、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、試行環境やクロールタイミングなどの状況によって異なる結果が得られる場合がある。

※ 2月15日及び16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。

*49 Webクローラによる観測手法については本レポートのVol.22 (http://www.ijj.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。

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、IJ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、PlugXの背後にいる攻撃者について、DrDoS攻撃とその対策、電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会、の3つのテーマについて紹介します。

1.4.1 PlugXの背後にいる攻撃者

2014年3月、IJではBlack Hat Asia 2014^{*50}において、PlugX^{*51}に関する講演を行いました。この講演は、PlugXの検体からC&Cサーバなどの設定情報を抽出して解析することで、PlugXの検体群から共通項を見つけてグループ化し、それらPlugXグループの背後にどのような標的型攻撃のグループが関与しているかを調査したものです。本章では、その結果を共有すると共に、なぜこの調査を行ったのかを併せて解説します。

■ PlugXの亜種

PlugXは、2012年3月に発見されたRAT^{*52}であり、標的型攻撃での利用が度々確認されています。IJでは、PlugXの亜種が本稿執筆時点で大きくわけて3タイプ存在することを確認しています。ここでは、それらをType I、II、IIIと呼ぶことにします。Type Iは、PlugXが発見されてから今まで一番多く発見されている検体であり、以前、本レポートのVol.21^{*51}で解説しています。Type IIは、IJ-SECT Security

Diaryで新型PlugX^{*53}として報告したとおり、2013年の第3四半期に発見された亜種です。PlugXの特徴であった"GULP"というシグネチャを含むヘッダを取り除き、Basic認証付きのProxyを通過する機能を持つなど、Type Iよりも大きく進化しています。Type IIIはType Iより前から存在しており、PlugXの前身^{*54}として過去の事件に使用されたことが報告されています。C&Cサーバからの命令を処理するコマンドや、通信の特徴はType IやIIとほぼ同一でありながら、コードの特徴は大幅に異なり、耐解析機能もより強化されています。また、Type IやIIと同様に、現在でもアップデートされ続けています。

■ 各PlugX検体からの設定情報の抽出

PlugXの各亜種は、それぞれコードの特徴が大きく異なります。そこで、IJでは各亜種に対応する抽出スクリプトをそれぞれ作成することで、すべての亜種から有用な設定情報(C&Cサーバや、サービス名、レジストリ値といった自動実行に関する情報など)の抽出を可能にしました。Type IとIIに関しては、多くの処理を共通化することができたため、1つのImmunity Debugger^{*55}用のスクリプトとして実装しています。Type IIIは、PlugXのコードを特定するための特徴が、難読化などの耐解析機能によって正規化できなかったため、半自動で抽出を行うIDA Python^{*56}スクリプトとして実装しました。これらのスクリプトを利用して、150のユニークハッシュ値を持つPlugXの検体から設定情報の抽出を試みました。このうち、27検体については設定情報を持たない、デモバージョン^{*57}でした。よって、残りの123検体について分類の対象としています。

*50 Black Hat (<https://www.blackhat.com/>) は米国、ヨーロッパ、アジアの主に3地域で毎年開催されている世界最大規模のITセキュリティのカンファレンス。IJでは今回アジア地域で行われたBlack Hat Asia 2014にて講演を行った。

*51 PlugXはIIR vol.21 (<http://www.ij.ad.jp/company/development/report/iir/021.html>) で詳しく解析している。

*52 Remote Administration Toolの略で、主にホストを遠隔から操作するためのマルウェアの一種。標的型攻撃ではこの種のマルウェアを起点に攻撃が行われることから、IJでもこのマルウェアに注目して解析を行っている。専門家によってはRemote Access ToolやRemote Access Trojanの略であると定義する場合もある。

*53 IJ Security Diary「新型PlugXの出現(<https://sect.ij.ad.jp/d/2013/11/197093.html>)」。Type IIやType IIIの亜種についてそれぞれ触れている。

*54 「SK Hack by an Advanced Persistent Threat (https://www.commandfive.com/papers/C5_APT_SKHack.pdf)」によると、2011年の攻撃で、Destory RATと呼ばれるRATが使用されていることが報告されている。これはPlugX Type IIIとほぼ同一であることをIJでは確認している。

*55 Immunity DebuggerはImmunity社が提供しているWindows用のデバグガ(<https://www.immunityinc.com/products-immdbg.shtml>)。OllyDbgを基に作成されており、Python拡張が特徴の1つ。プラグインやスクリプトをPythonで記述できる。

*56 IDA PythonはHex-Rays社が提供する逆アセンブラ、デバグガであるIDA Pro(<https://www.hex-rays.com/products/ida/>)で処理を自動化するためのPython拡張。

*57 PlugXのデモバージョンに関する詳細は次のサイトが詳しい「An Analysis of PlugX (<http://lastline.com/labs/plugx/>)」。デモバージョンの場合、設定情報は文字列 "XXXX" でパディングされることが多いため、情報を抽出することはできない。ただし、一部の検体ではデモバージョンのフラグが立っているにもかかわらず、設定情報を持ち、パディングがされない検体が存在することも確認している。そのような検体は解析対象に含めている。

■ PlugXの分類

図-14は、PlugXの分類手法を図示したものです。前述のスク립トを用いて設定情報を抽出後、各検体の共通項を見つけて分類しています。

第一段階としてサービス名を基に分類しました。PlugXは、感染ホストが再起動した場合でも継続的に活動できるよう、感染時にサービスやレジストリのRunキーに登録を行います。これらの値で特徴的なものをグルーピングしました^{*58}。第二段階では、C&Cサーバの情報(FQDN、IPアドレス)^{*59}、ドメイン名、ドメイン所有者のメールアドレスや、コード内のデバッグ文字列^{*60}を基に異なるグルーピングを行いました。

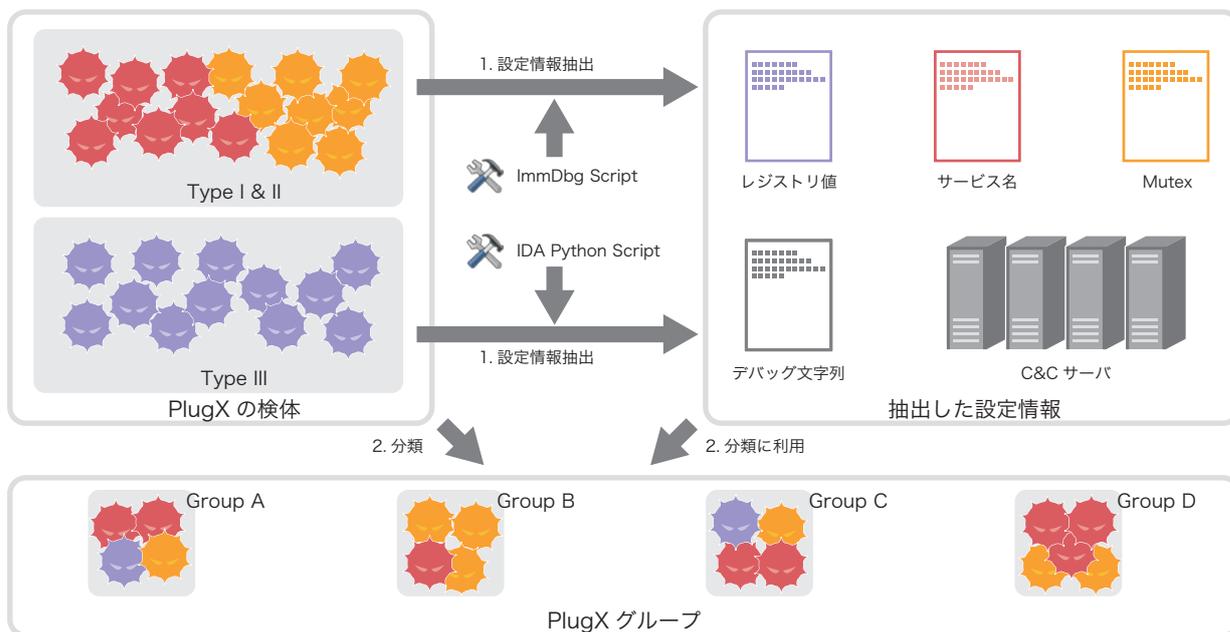
これらの作業を繰り返してできたグループを表-1に示します。全PlugX検体の約3分の2を7グループに分類することができました。なお、今回は、最低4つの検体が属しているものを1グループとしています。

表-1 PlugX検体の分類結果

PlugXグループ名	Type I	Type II	Type III	グループの合計
*Sys	15	0	5	20
*Http	12	3	0	15
Starter	13	7	4	24
Graphedt	8	0	0	8
WS	6	1	0	7
360	4	0	0	4
cochin	0	0	4	4
- (Others)	30	8	3	41 ^{※注}

全検体の
約3分の2
(67%)

※注：内8検体は標的型攻撃者グループと関連が確認された。



1. 各PlugXの検体からそれぞれのタイプに応じたスク립トを用いて設定情報を抽出する。
2. 抽出した設定情報を基に、各検体間で設定情報の値が一致、もしくは整合性があるものを同じグループとして分類する。

図-14 PlugXの分類方法

*58 サービス名でグルーピングする際「SxS」、「XXX」、「TVT」といった、デフォルト値はグルーピングのキーから除いた。一方、サービス名で同一グループとして分類された検体の多くは、その検体間でC&Cサーバの情報が一致するか、類似性が見られた。このことから、一定の時期もしくは攻撃者ごとに独自のサービス名をつけている可能性が高いと考えられる。

*59 FQDNを名前解決したのものも含む。

*60 PlugXの検体の多くは現在も開発が頻繁に行われている。そのためかデバッグを有効にしてコンパイルされている検体が多く存在する。PlugXで何らかの処理中にエラーが発生した場合、そのエラーの内容と共に、どのバージョンで不具合が発生したかを示すバージョン情報や中国語圏の文字列を含むパス情報を併せてログとして記録するルーチンが存在する。このパス情報の文字列は数多くのパターンが存在するため、この情報も同一攻撃主体を示すもの1つとして利用できると考えられる。次のWebサイトでは、多くのデバッグ文字列例が紹介されている。「CASSIDIAN CyberSecurity Blog PlugX: some uncovered points (<http://blog.cassidiancybersecurity.com/post/2014/01/plugx-some-uncovered-points.html?2014/01/plugx-some-uncovered-points.html>)」。

■ 既知の標的型攻撃者グループとの比較

最後に、前項で生成したPlugXグループが、既知の標的型攻撃者グループとの関係があるかを調査しました。具体的には、標的型攻撃の外部レポートに記載されている検体のハッシュ値や、C&Cサーバの情報が一致しているかを調査しました。図-15は、それらの関係性をまとめたものです。今回の調査では7つのPlugXグループのうち、5グループが何らかの既存の事件に関連していることが分かりました。特に、5グループ中4グループが、APT1^{*61}と呼ばれる攻撃者グループと関連していることが今回の調査で分かりました。これは、多くのPlugXを使う攻撃者がAPT1に属している、もしくは、少なくとも異なる攻撃者グループ間でインフラを共有していることを示しています。また、今回グループに分類しきれなかったPlugXのうち、8検体についてはAPT1やWinnti^{*62}など、何らかの既知の標的型攻撃者グループに関わりがあることが判明しました。

■ 新たな対策手法の検討

今回は、PlugXを例にしてこのような調査を行いました。標的型攻撃では、少数の特定組織が狙われるため、攻撃者の意図、組織の規模、攻撃に使うツール、インフラ設備などの全

貌が見えにくいという側面があります。各組織が入手できる検体数も限られており、少数の検体から得られた情報を頼りに対策を行うことになりがちです。それに対して、もし多くの検体を集められた場合、今回のように、多くのPlugXグループがAPT1との関連が見つかるなどの新たな事実が判明する可能性があります。もしそのようなことが分かれば、例えば、APT1の攻撃者がRATを経由して組織内に侵入した後に使用する攻撃手法や、攻撃ツールの特徴を基にした検出や対策が行えるなど、攻撃の進行状況に応じた多角的な対策を取ることができるようになります。

Black Hat ASIAにおける発表では、講演資料や設定情報抽出スクリプトに加え、各PlugXの検体と既知の標的型攻撃者グループとの相関図も併せて配布^{*63}しています。これはSVGと呼ばれる画像フォーマットになっています。SVGは、画像でありながら実際にはXML形式でもあるため、これを解析することでC&Cサーバなど、今回開示した情報をすべて取り出すことができます。そのため、このデータを利用して出口対策などが可能になります。

標的型攻撃を受けた各組織が、もっと広く詳細に情報を開示

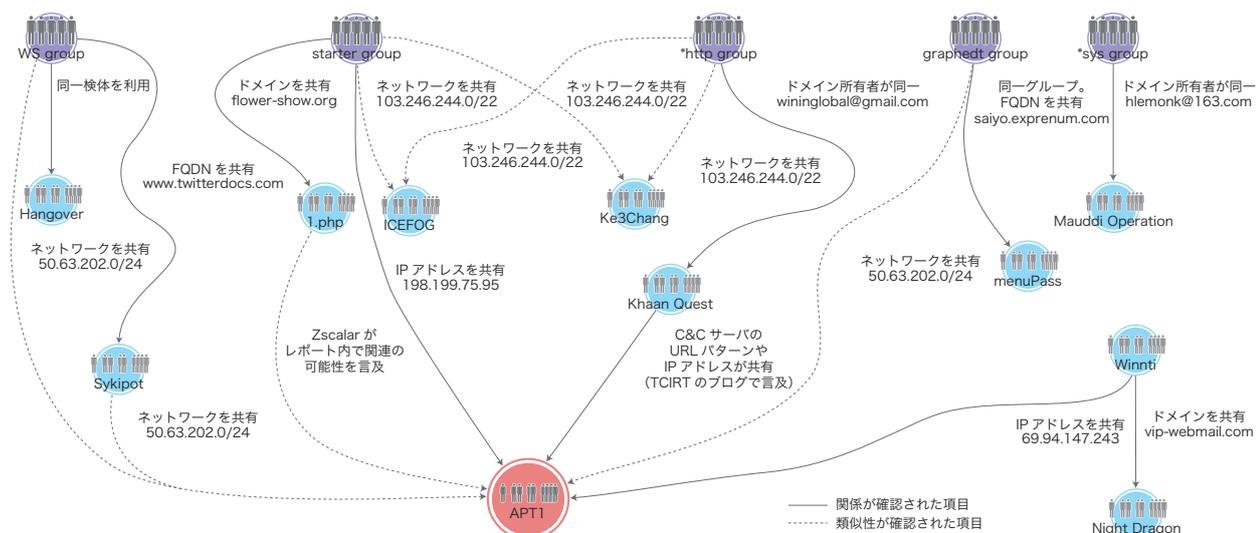


図-15 PlugXグループと標的型攻撃者グループとの相関図

*61 APT1はMandiant社が報告した標的型攻撃を行うグループの1つ (<http://intelreport.mandiant.com/>)。

*62 WinntiはKaspersky Lab社が報告した、ゲーム業界を標的とする標的型攻撃 (<https://www.securelist.com/en/downloads/vlpdfs/winnti-more-than-just-a-game-130410.pdf>)。

*63 今回の講演資料、抽出スクリプト及び相関図はBlack Hatのアーカイブサイトから入手できる (<https://www.blackhat.com/asia-14/archives.html#Haruyama>)。スクリプトは更新版を以下でも配布している (<http://takahiroharuyama.github.io/blog/2014/03/27/id-slash-idapython-scripts-extracting-plugx-configs/>)。

し合うことが標的型攻撃の対策につながります。IJではこの様な解析や調査活動を継続し、積極的に情報を開示することによって、標的型攻撃の対策に向けた活動を行っていきます。

1.4.2 DrDoS攻撃とその対策

2013年3月に、DNSのオープンリゾルバを悪用したDDoS攻撃が問題となりました^{*64}。この攻撃は、外部からの再帰的な問い合わせを許可しているDNSキャッシュサーバを悪用し、攻撃対象のIPアドレスに送信元IPアドレスを偽装した問い合わせを行うことで、その応答を攻撃対象のサーバに対するDDoS攻撃として送りつけるものでした。

10月頃には、NTPによるDDoS攻撃が観測されており^{*65}、12月には米国Symantec社がブログで、NTPによるDDoS攻撃に関する報告を行いました^{*66}。これらのNTPによるDDoS攻撃では、NTPの管理機能の1つであるmonlistを悪用しており、DNSによる攻撃と同様に送信元IPアドレスを偽装した問い合わせを行うことでDDoS攻撃を行っていました。この問題については2014年1月に入り、DDoS攻撃に悪用される可能性が高いとして、日本でもJPCERTコーディネーションセンターなど複数の組織から注意喚起が行われており^{*67}、実際に、この攻撃によると考えられる被害や、踏み台となった事件が複数確認されています。更に、欧米では2013年12月頃から何者かによるゲーム関連サイトなどに対するNTPによるDDoS攻撃が複数発生しており、最大で80Gbpsにも達したことが、米国のDDoS対策事業者の1つであるStaminus社によってブログで報告されています^{*68}。また、クラウド事業者であるCloudFlare社のブログでは、同社の顧客に対して、攻撃規模としては最大で400Gbpsの攻撃があったことを報告しており^{*69}、更

に、ArborNetworks社からは、同社の複数ISPネットワークにおける観測情報として、NTPによる通信量が最大で800Gbpsにも上ったと報告されています^{*70}。

これらの攻撃は、Distributed Reflection Denial of Service attacks (以下、DrDoS攻撃)と呼ばれ、その攻撃の容易さと増幅率による影響の大きさから問題となっています。本稿では、DrDoS攻撃について解説すると共にその対策について検討します。

■ DrDoS攻撃の仕組み

DrDoS攻撃はその名のとおりに、ある通信の応答(反射)を悪用した攻撃です。DNSやNTPなど、UDPのサービスが悪用されることが多いですが、これはUDPがコネクションレスの Protokol であることに起因しており、攻撃の容易さに繋がっています。攻撃は踏み台となった脆弱な機器のIPアドレスからの攻撃に見えるため、被害者からは本当の攻撃者が分かりません。このため、攻撃元からの通信を遮断するなどの対処を行ったとしても、新たな踏み台を見つけて攻撃が継続できることから、被害者側での対策が攻撃の根本対処にはつながらない場合もあります。

更に、攻撃先を直接攻撃する場合に比べ、DrDoS攻撃では、問い合わせに対する応答のデータ量が多いことを利用して、その攻撃規模を数倍から数十倍に増幅させます。例えば、DNSの場合では理論上の増幅率は70倍まで増幅される可能性があります^{*71}。今回問題となった、NTPのmonlist機能を悪用した攻撃の場合、1つの問い合わせに対し、理論上の最大値で返答した場合、約200倍のデータが送られることとなります。このように、NTPの場合には増幅率が非常に

*64 DNSオープンリゾルバ問題については、本レポートのVol.21「2. インターネットオペレーション DNS オープンリゾルバ問題」も参照のこと、(http://www.ij.ad.jp/company/development/report/iir/pdf/iir_vol21.pdf)。

*65 リトアニアの研究教育機関のネットワークであるLITNETのCERTチームの報告で確認できる。LITNET CERT, "NTP DoS reflection attacks" (<https://cert.litnet.lt/en/docs/ntp-distributed-reflection-dos-attacks>)。

*66 Symantec Cyber Readiness & Response Blog, "Hackers Spend Christmas Break Launching Large Scale NTP-Reflection Attacks" (<http://www.symantec.com/connect/blogs/hackers-spend-christmas-break-launching-large-scale-ntp-reflection-attacks>)。

*67 JVN, 「JNVU#96176042 NTP が DDoS 攻撃の踏み台として使用される問題」(<https://jvn.jp/vu/JNVU96176042/index.html>)。

*68 Staminus Communications, "Mitigating 80 Gbps Attacks – NTP Amplification Attacks on the Rise" (<https://blog.staminus.net/mitigating-80-gbps-attacks-ntp-amplification-attacks-on-the-rise>)。

*69 CloudFlare, "Technical Details Behind a 400Gbps NTP Amplification DDoS Attack" (<http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack>)。

*70 ArborNetworks, "NTP attacks continue – a quick look at traffic over the past few months" (<http://www.arbornetworks.com/asert/2014/03/ntp-attacks-continue-a-quick-look-at-traffic-over-the-past-few-months/>)。

*71 実際にはキャッシュDNSサーバの設定などにより増幅率が律速されるため、最大で8倍から40倍程度となる。

高いことが分かります*72。DrDoS攻撃では、これにより、攻撃先の回線容量を超える通信量を発生させています。

■ NTPによるDrDoS攻撃とその影響

今回、問題となったNTPのmonlistによるDrDoS攻撃の可能性については、NTPの実装に関する開発者のコミュニティで2010年に指摘されており、同年5月には修正が行われていました*73。しかしながら、この修正はDevelopment（開発版）のみに反映され、Stable（安定版）は4.2.6p5のまま、本修正は反映されていませんでした。このため、一部のntpdの実装を使っていたルータなどの機器やUNIX系OSでは、この修正が反映されていませんでした*74。

図-16に今回問題となったNTPによるDrDoS攻撃について示します。ntpdなど一部のNTPの実装では、管理のために、参照しているクライアントのIPアドレスの一覧を返すmonlistコマンドが実装されています。外部からのこの問

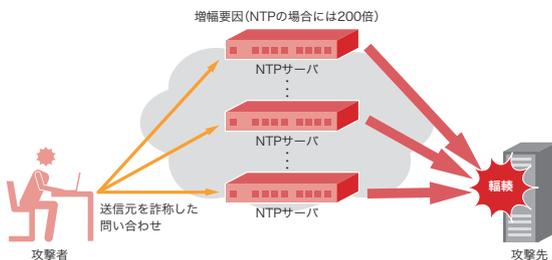


図-16 DrDoS攻撃の概要(NTPの場合)

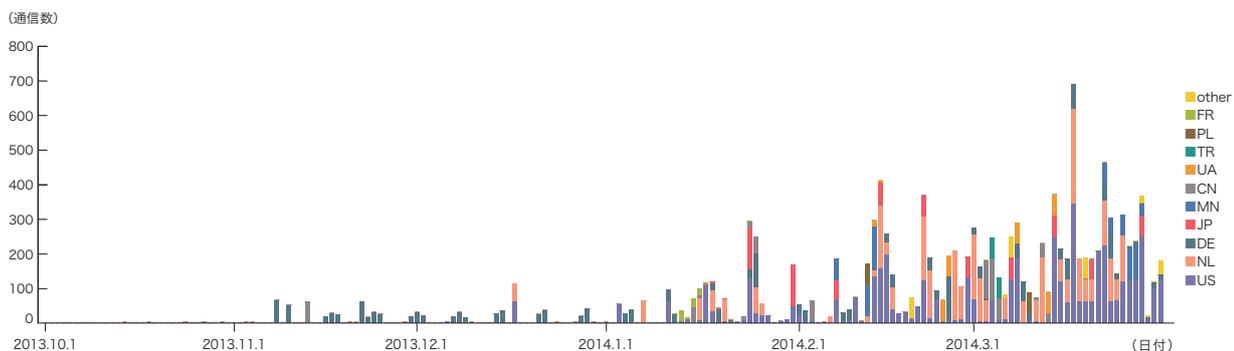


図-17 ハニーポットに到着したNTP(123/UDP)の通信

*72 攻撃に使われるプロトコルの増幅率については、CERT/CCのアドバイザリでも注意喚起が行われている。"Alert (TA14-017A) UDP-based Amplification Attacks" (<https://www.us-cert.gov/ncas/alerts/TA14-017A>)。

*73 4.2.7p26以前のntpdが本脆弱性の影響を受ける。修正については次のntp.orgのBugレポートなども参照のこと。"Bug 1532 - remove ntpd support for ntpdc's monlist (use ntpq's mrulist)" (http://bugs.ntp.org/show_bug.cgi?id=1532)。

*74 例えば、FreeBSDなどが該当している。The FreeBSD Project, "ntpd distributed reflection Denial of Service vulnerability" (<http://www.freebsd.org/security/advisories/FreeBSD-SA-14:02.ntpd.asc>)。

い合わせに応答するルータやサーバなどの機器があった場合、送信元を攻撃先のIPアドレスに偽装した問い合わせを送ることで、返答が攻撃先に返ることになります。攻撃者は、このような通信を多数の機器に対して行うことで攻撃を行います。ntpdでは、参照しているクライアントのIPアドレスを、最大で600までリストとして持つことから、今回の攻撃では、攻撃者は外部から詐称したIPアドレスで連続して問い合わせを行うことで、リストを最大値まで増やした後に、実際の攻撃先を詐称して攻撃を行っていたと考えられます。

今回のNTPの問題について、NTPサーバにおいて2つ注意する点があります。1つは、DrDoS攻撃の踏み台として悪用される可能性です。これらの攻撃の踏み台となってしまった場合には、攻撃の被害者であると同時に加害者となってしまふこととなります。もう1つは、情報漏えいの可能性です。今回の問題では、管理機能として参照しているクライアントのIPアドレスの一覧を返すmonlistコマンドが使われています。このため、外部からの問い合わせに答えることで、このNTPサーバを利用しているネットワーク上のクライアントのIPアドレスなどの情報が外部に漏れる可能性があります。

■ ハニーポットによる観測状況

図-17に昨年10月初めから今年3月末の期間で、ハニーポットに到着したNTP (123/UDP)の通信について、発信元IPア

ドレスの国別分類を示します。ここに示したとおり、11月中旬よりドイツを発信元とした通信が行われていたことが確認できます。この後、今年の1月中旬にCERT/CCなどから脆弱性情報が公表^{*75}された時期から継続的に通信が発生していることが確認できます。国別で見ると、米国が36.8%と最も多く、オランダの25%、ドイツの14.3%と続いており、欧米からの通信が多いことが確認できます。日本からの通信も4位で5.9%ありました。このことから、この問題が公表されてから問題の確認を行ったり、攻撃の試みを行う活動が増加したことが推測できます。また、DrDoS攻撃では、送信元を偽装した問い合わせを問題のあるサーバなどに対して行いますが、この期間に確認された通信では、総数があまり多くないため、外部からの問い合わせを許可しているサーバやルータなどを探索する活動なのか、送信元に対する攻撃なのか判断することはできませんでした。しかしながら、送信元の一部がゲーム関連のサービスを提供していると考えられるIPアドレスであったことなどから、攻撃と探査活動の両方が行われていたと考えられます。

■ DrDoS攻撃への対処

DrDoS攻撃では、IPアドレスを詐称することで比較的容易に攻撃が行えるため、悪用できる脆弱性や新たな攻撃手法が公表されると、すぐに悪用の試みが行われる傾向があります。DrDoS攻撃の発生情報に注意し、自分の管理するシステムが攻撃に悪用される可能性について検討し、対処する努力が必要です。

また、今回の事件では、NTPが問題となりましたが、DrDoS攻撃に利用されるプロトコルはNTPだけではなく、DNSやSNMP、ECHO、Chargenなども悪用される可能性があります。サーバやルータなどの機器をインターネットに接続する場合には、まず、機器の脆弱性情報に注意し、ファームウェアなどについてセキュリティの問題のないバージョンを利用することが必要です。更に、機器において初期状態から動作しているサービスについて、利用者が認識していない状態で、踏み台として悪用されてしまうような場合も見受けられます。このような状況にならないために、機

器の導入時には不要なサービスを停止し、適切にアクセス制御を設定します。導入後においても、動作するサービスについてインターネット側から継続的に調査することで、設定ミスを早期に発見することができ、外部から第三者に悪用される可能性を減らすことができます。

また、DrDoS攻撃では、送信元を詐称して攻撃を行うため、適切な通信制御を行うことでその影響を低減することができます。例えば、送信元検証(Source Address Validation)^{*76}のような、詐称した通信がネットワークに流入することを防ぐ技術を利用することで、このような送信元のIPアドレスを詐称した攻撃を防ぐことが可能となります。

更に、ISPのネットワーク網において、これを遮断することについて、総務省の研究会などで検討されています。この議論については、「1.4.3 電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」も併せて参照してください。

■ まとめ

これまで解説したとおり、DrDoS攻撃は、攻撃の容易さに比べるとその攻撃の影響が非常に大きいことから、注意すべき脅威の1つです。一方で、攻撃としては比較的古くから知られていたものの、具体的な脅威があまりなかったことから、これまで十分な対策が行われているとはいえませんでした。今後も、同様の手法を用いた新たな攻撃が出現することが考えられます。これに備えるためにも、日頃から利用している機器の管理を適切に行う必要があります。IJとしても、業界団体などを通じて、適切な対策に向けた活動を今後も継続して行っていきます。

1.4.3 電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会^{*77}

ここでは2013年11月から2014年3月までの期間に実施された、総務省の研究会「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」の検討内容について解説します。この研究会は有識者や通信関連団体

*75 CERT/CC、"Vulnerability Note VU#348126 NTP can be abused to amplify denial-of-service attack traffic" (<http://www.kb.cert.org/vuls/id/348126>)。

*76 送信元検証については次の弊社解説も参照のこと。「送信元検証『Source Address Validation』」 (<http://www.ij.ad.jp/company/development/tech/activities/sav/>)。

*77 総務省、「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」 (http://www.soumu.go.jp/main_sosiki/kenkyu/denki_cyber/index.html)。

により構成されていますが、技術的な内容を検討するためのワーキンググループが組織され、また各関連団体においても検討の場が設けられるなど、短い期間に多くの人が関わる複数の場で、数々の議論がなされました。研究会の議事は要旨のみの公開となっていますが、ここでは公開された「第一次とりまとめ」を元に、検討のポイントについて紹介します。

■ 5つの課題と検討

この研究会では、最近の攻撃に関連する課題として次の5つについて検討を行っています。

- ・マルウェア配布サイトへのアクセス防止^{*78}
- ・C&Cサーバで入手した情報を元にしたマルウェア感染駆除の拡大
- ・新たなDDoS攻撃であるDNSAmP攻撃の防止
- ・SMTP認証の情報を悪用した迷惑メールへの対処
- ・攻撃の未然の防止と被害拡大の防止

これらのような攻撃の多くは通信を媒介として発生します。また通信インフラ自体も攻撃にさらされることから、攻撃への対処の機能を通信の過程で実現することは、ある程度必要になることです。加えて、通信事業を行うISPにおいて攻撃に対処することで、数多く発生する被害を効果的に防ぐことも可能です。一方で、通信の過程において攻撃に対処することは、通信すべてについて情報(通信内容や、誰がいつどこに通信を行ったのかなどの外延情報も含む)を取得し、その情報を利用することで攻撃の有無やその様態を判断し、適切に攻撃の通信を止めることを意味します。これは電気通信事業法にある通信の秘密を犯す行為、つまり違法行為にあたります。

そこで、通信事業において攻撃への対処を行うために、攻撃それぞれについて、その発生の原因や影響と、取りうる対処法に関して、違法性が阻却されるかどうかを確認する必要があります。まず、通信の情報を利用した攻撃への対処は、通信の当事者である利用者が同意したうえで実施す

ることができますが、どのように有効な同意を得るかが大きな論点となります。また、利用者の同意の有無に関わらず、攻撃への対処として行う行為が、通信事業者にとっての正当防衛、緊急避難、正当業務行為などに該当する場合も考えられます。この研究会においても、5つの課題について、これらの検討を行っています。以下にそれぞれの検討の概要を示します^{*79}。

■ マルウェア配布サイトへのアクセス防止

総務省施策ACTIVEで実施している、Web感染型マルウェアなどへの感染防止の試みのうち、通信に介在する装置などを用いて、すべての利用者に包括的に実施するURLフィルタリングの可能性について検討されています。利用者の通信に関わる情報を利用した対策については、将来契約者の不利益に繋がる可能性のあることから、従来は個別同意が必要とされていました。この課題の検討では、約款に基づく包括同意において、

- ・利用者が契約約款に同意したあとでも同意内容を変更できる(設定変更できる)こと
- ・同意内容の変更の有無に関わらず、その他通信サービスの提供条件が変わらないこと
- ・必要最小限の通信の秘密の検知で実施すること
- ・注意喚起画面などを表示すると共に、同意内容を変更できることとその方法を説明すること

などの条件を満たす場合については、有効な同意と見なすことができるとしています。また、併せて契約約款に記載すべき事項や注意喚起画面の例を示しています。

■ C&Cサーバで入手した情報を元にしたマルウェア感染駆除の拡大

マルウェア対策を行う様々な組織の活動の結果、マルウェアを制御するサーバが差し押さえられる場合が増えてきています。そのサーバに蓄えられた情報を元に、感染に気づいていない利用者を特定し、感染の事実や駆除の方法を伝える注意喚起を実施することが検討されました。この場

*78 マルウェア配布サイトへのアクセスを未然に防止する等の実証実験を行う官民連携プロジェクト、ACTIVEの普及展開策の一つとして検討された。ACTIVE(Advanced Cyber Threats response Initiative)、「ACTIVE について」(<http://www.active.go.jp/active/index.html>)。総務省、「ACTIVE」の実施及び「ACTIVE推進フォーラム」の開催」(http://www.soumu.go.jp/menu_news/s-news/01_ryutsu03_02000059.html)。

*79 この研究会における事例の検討は、多くの条件を設定したもとの法解釈の検討であり、正確な検討内容については研究会の一次とりまとめを参照のこと。

合においては、C&Cサーバに蓄積された通信に関わる情報のうち、接続元のIPアドレスやタイムスタンプを元に、ISPにおいて顧客情報を検索し、利用者を特定することが通信の秘密(外縁情報)の侵害にあたります。この検討では、C&CサーバにIPアドレスなどの記録が残っている端末は、実際に当該サーバを利用するマルウェアに感染しており、そのマルウェアによる被害を受けるとしたうえで、C&Cサーバに残った記録を用いた対処方法について議論しています。結果として、当該IPアドレスから特定した利用者の情報を、注意喚起以外の用途で利用しない場合には、緊急避難として違法性が阻却されるとしています。

■ 新たなDDoS攻撃であるDNSAmP攻撃の防止

設定の緩いDNSリゾルバを踏み台とし、大きな通信量をとまなうDDoS攻撃(DNSAmP攻撃)が、2013年に多く発生しました。DNSAmP攻撃は、攻撃者からDNSリゾルバに向かう通信、DNSリゾルバからISPのDNSサーバに向かう通信、インターネット上のサーバからの増幅された応答といった、複数の通信により構成されます。ここでは、それぞれの通信の状況や、その通信で対処を行うことによる効果について議論を行った上で、攻撃者から踏み台になるDNSリゾルバに向かった、増幅を誘発するための通信をブロックする対処について検討しています。また、通常の状況では利用者が特定できない、動的IPアドレスの範囲に多数のDNSリゾルバが存在するために、包括的にブロックを行う必要がある状況を想定しています。

この検討では、動的IPアドレスの空間に対するDNSのクエリの通信をブロックすることについて、宛先のIPアドレス及びポート番号を確認した結果がDNSAmP攻撃の防止以外の用途で利用しない場合に、正当業務行為として違法性が阻却されるとしています。

■ SMTP認証の情報を悪用したスパムメールへの対処

迷惑メール送信対策として広く利用されているSMTP認証ですが、最近では利用者によるパスワードの使いまわしなどに起因して、リスト型攻撃などの不正アクセスの対象となり、第三者にメール送信機能を悪用される場合が発生しています。ここでは、この課題への対策として、

・接続元が瞬時に外国に移動するなど、SMTP認証のID・パス

ワードの不正利用の蓋然性が高いものへの対策。一時的に利用停止すると共に、利用者にパスワード変更を依頼する。
・SMTP認証の接続の過程において、特定のIDに対して多くのパスワードを試すような辞書攻撃により、ID・パスワードを盗み取ろうとする試みの防止。特定のIPアドレスからの通信で発生する大量のSMTP認証失敗の検出と、そのIPアドレスからのSMTP認証を一時的に停止する。

の2つについて検討しています。いずれの場合も、サーバに対する通信状況に関する情報を元に判断し、一時的に通信を行わせなくする行為ですが、利用者によるパスワード変更などで不正利用が解消するまでの期間、もしくは攻撃が継続する期間に限って行う場合には、正当業務行為として違法性が阻却されるとしています。

■ サイバー攻撃の未然の防止と被害の拡大防止

この課題としては、システムの脆弱性を悪用する内容を含む通信を検出し、通信先に届けられないことで攻撃を未然に防ぐ対策と、同時多発的なDDoS攻撃や国内のISPの利用者同士が攻撃をしあっている状況などに対する、ISP間の連携による対策について検討が行われました。しかし、前者は通信内容を直接判断する行為であり、また脆弱性を保有するシステムに依存する問題でもあること、後者は検討の前に連携が必要となる場面に関する整理が必要であることから、この一次取りまとめでは今後更に検討を進める必要があるとしています。

以上のように、この研究会では設定した5つの課題に関する検討を実施し、特に、いくつかの対策について、約款に基づく包括同意をもって利用者による有効な同意と解釈することや、従来攻撃の発生後に正当防衛や緊急避難として許容されてきた攻撃への直接的な対策について、正当業務行為として認められる検討結果を得ています。これらの結果は、今後ISPにおける攻撃対策を検討する上で、大きな影響を及ぼす成果であると考えられます。

■ 今後の活動

インターネット上の攻撃の状況は日々変化しており、今回具体的に検討された範囲においても、例えばNTPサーバを踏み台としたDDoS攻撃の発生については、その発生の事実を認識していることを言及するのみにとどまってい

ます。このことから研究会自体は今後も継続し、新しい攻撃とその対策について検討を進めるべきだと考えます。

また、今回検討された課題についても、ISPなどの通信事業者において実際に適用する場面では、より詳しく指針を示す必要があります。例えば、C&Cサーバをテイクダウンした場合において、どのような組織からの情報を信用して良いのか検討を要します。また、SMTP認証に関わる通信の異常についても、可能な限り多くの利用者や事業者が納得できる定量的な基準づくりを試みる必要があります。

このため、この研究会の検討結果を通信事業の実務上の状況に適用させるためのガイドラインづくりを、インターネットの安定的運用に関する協議会などの場で進めていきます^{*80}。

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、PlugXの背後にいる攻撃者についての調査の概要と、DrDoS攻撃とその対策、電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会について紹介しました。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努力を継続してまいります。

執筆者:



齋藤 衛(さいとう まもる)

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 室長。法人向けセキュリティサービス開発に従事した後、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、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)

永尾 慎啓、土屋 博英、鈴木 博志、梨和 久雄(1.3 インシデントサーベイ)

鈴木 博志、春山 敬宏(1.4.1 PlugXの背後にいる攻撃者)

土屋 博英(1.4.2 DrDoS攻撃とその対策)

齋藤 衛(1.4.3 電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会)

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:

加藤 雅彦、須賀 祐治、根岸 征史、小林 直、桃井 康成、小林 稔 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

*80 インターネットの安定的運用に関する協議会は、通信関連団体である社団法人電気通信事業者協会、社団法人テレコムサービス協会、社団法人日本インターネットプロバイダー協会、社団法人日本ケーブルテレビ連盟、財団法人日本データ通信協会テレコム・アイザック推進会議による協議会で、「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」の策定を行っている。JAIPA、「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドラインの改定について」(<http://www.jaipa.or.jp/topics/?p=400>)。

送信ドメイン技術の導入状況と標準化の動向

今回の報告は、2013年第14週から2014年第13週までの52週分のデータを含めた分析結果を

IIR Vol.1からのデータを参照しながら報告します。

また、メールの技術解説では、送信ドメイン認証技術の一つであるSPFの変更点について報告解説します。

2.1 はじめに

このレポートでは、迷惑メールの最新動向やメールに関連する技術解説、IJJが関わる様々な迷惑メール対策活動について報告しています。これまで、IIRのVol.1からVol.19までレポートを継続して掲載してきましたが、今後は不定期の報告、およそ1年に1回のレポートを予定しています。今回の報告では、日本の2013年度の第4四半期にあたる、2014年第1週(2013年12月30日～2014年1月5日)から第13週(2014年3月24日～3月30日)のデータを中心に、前回(Vol.19)からの1年間、2013年第14週(2013年4月1日～4月7日)から2014年第13週までのおよそ1年間、52週分のデータも含めた分析結果を報告します。また、IIR Vol.1からの6年近い304週分のデータについても適宜参照します。メールの技術解説では、これまで解説してきた送信ドメイン認証技術の導入状況や現在標準化作業が行われている、送信ドメイン認証技術の一つであるSPFの変更点について、報告解説します。

2.2 迷惑メールの動向

ここでは、迷惑メールの動向として、IJJのメールサービスで提供している迷惑メールフィルタが検知した割合の推移と、迷惑メールの送信元に関する分析結果を中心に報告します。今回は、迷惑メール割合の長期的な変化を分析するために、IIR Vol.1(2008年6月2日)からの割合の推移を図-1に示します。

2.2.1 2010年中頃から割合が減少

2008年及び2009年の迷惑メール割合は、年間の平均割合がそれぞれ82.3%と81.8%であり、受信したメールの大部分が迷惑メールという状況でした。こうした状況が変化したのは、2010年の第2四半期(2010年6月28日～10月3日)からで、この時期から少しずつ割合が減少してきました。2010年の平均割合は79.4%でしたが、2010年の第1四半期まで80%を超えていた割合が2010年の第2四半期では78.7%と調査開始以来初めて80%を下回りました。その後も減少を続け、2011年第2四半期以降、40%台が続いています。

迷惑メールの割合や量自体が減少した理由は、既にIIRでも何度か報告してきたとおり、迷惑メールの送信元であるボットネットの活動低下によるものと推測されています。

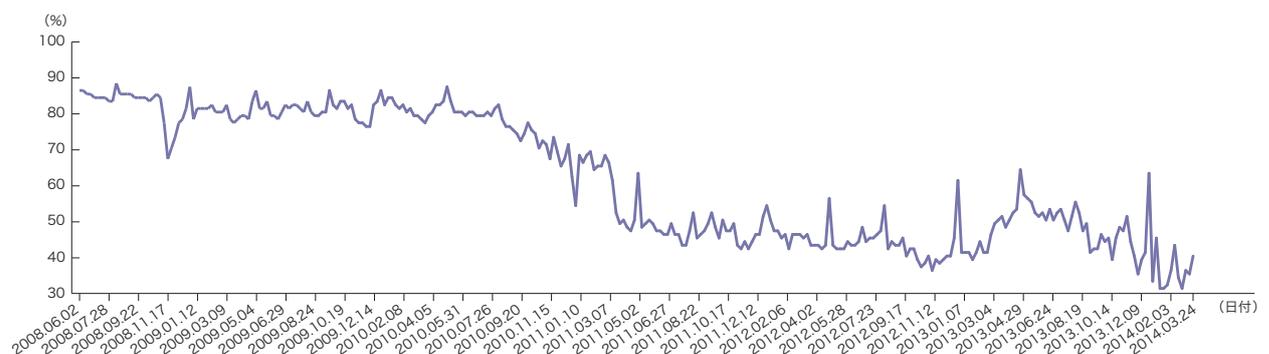


図-1 迷惑メール割合の推移

不正なソフトウェア¹に感染させられ、外部から制御された状態のPCをボット(bot)と呼びます。これらのボットの集合をボットネットと呼び、ボットを制御するサーバをC&Cサーバ²と呼びます。ボットネットの活動を止める効果的な方法は、このC&Cサーバを止めてボットネットへの指示を出せないようにすることです。各国の行政機関が、こうしたC&Cサーバを法的な手段などによって停止に追い込むことによって、ボットネットの活動を押しやえ込んだことが迷惑メール量の減少に繋がったといわれています。また、特定のC&Cサーバを持たない、P2P(Peer-to-Peer)型のボットネットに進化しているとの情報もありますので、引き続き警戒が必要です。

2.2.2 直近の迷惑メール割合は減少

2013年度の第4四半期にあたる2014年第1週(2013年12月30日～2014年1月5日)から第13週(2014年3月24日～3月30日)までの迷惑メール割合の平均は38.5%でした。前年同時期(2012年度第4四半期)の平均は45.5%だったので、7%減少したことになります。この期間、最も迷惑メールの割合が高かったのは、2014年の第1週の63.5%でした。この期間の迷惑メール量もそれなりに多かったのですが、年末年始の休暇期間であったことから、通常のメール量が少なかったことで相対的に割合が高くなったのが理由です。それ以外で週平均40%を超えたのは、第3週、第8週、第13週の4週間だけでした。

2.2.3 メールをトリガにした危険度は高まる

一時期に比べて迷惑メールは、受信メール全体に対する割合と迷惑メール量共に、大幅に減少しました。しかし、迷惑メールに起因する危険性の度合いについては増しているようです。従来は主に何らかの製品(非合法も含めて)の広告宣伝の道具としてメールが利用されるケースが多かったのに対し、最近では、組織内部にあるPCへの侵入の経路として、メールが使われているのでは、と思われるケースが増えています。

例えば、2014年1月30日に警察庁が発表した資料³によ

れば、平成25年中に発生した不正送金が1,315件、約14億600万円と過去最大の被害と報告されています。更に、メールによってフィッシングサイトへ誘導されるケースが増えていることが報告されています。つまり、迷惑メールが単に削除するのが面倒なもの、迷惑なもの、という範疇から、金銭的な犯罪被害のトリガになる、危険なものに変化している、ということが言えます。更に、こうしたオンラインバンキングの犯罪が発生している現状を考えれば、同様の手口で様々なIDとパスワードが搾取されている可能性も高いと考えられます。このような搾取された情報の中には、メール送信のためのIDやパスワードも含まれ、正規のメールサーバを踏み台にした、迷惑メール送信に利用される事例も多く発生しています。

2.2.4 迷惑メール送信元の動向

2013年度の第4四半期での、迷惑メールの送信元地域の分析結果を図-2に示します。この分析に利用したデータは、IJが提供するメールサービス全般を対象にしたものではないため、図-1で示した迷惑メールのすべての送信元を対象にしたデータとはなっていません。そのため、多少の偏りがあるかもしれないことを補足しておきます。

今回の調査期間での、迷惑メールの送信元の1位は中国(CN)で、迷惑メール全体の19.1%を占めていました。中国は、IIR Vol.11 (2010年度第4四半期)から迷惑メール送信

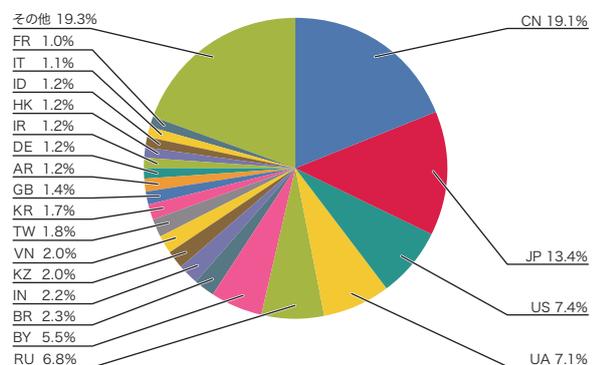


図-2 迷惑メール送信元地域の割合

*1 迷惑メール送信など悪意ある特定の目的のために作成されたソフトウェアを、より一般的な用語であるウイルスと区別して、悪意のあるソフトウェア(malicious software、malware)と呼ぶことがあります。

*2 C&Cサーバ(Command & Control Server)。

*3 平成25年中のインターネットバンキングに係る不正送金事犯の発生状況等について(http://www.npa.go.jp/cyber/pdf/H260131_banking.pdf)。

が最も多い状態が続いています。2位は日本(JP)で13.4%でした。日本もIIR Vol.16 (2012年度第1四半期)から継続して2位という状態が続いており、その1年程度前から上位に位置するようになりました。これらの地域は、2010年の中頃に受信メール全体に対する迷惑メールの割合が減少して以来(図-1参照)、ほぼ固定的に上位となっていることから、ボットネットの活動低下にあまり影響しない、固定的な送信元である可能性が高いと言えるでしょう。

3位は米国(US、7.4%)、4位はウクライナ(UA、7.1%)、5位はロシア(RU、6.8%)、ベラルーシ(BY、5.5%)という結果になりました。これまでは、アジアが迷惑メールの主要な送信元地域という結果でしたが、今回の結果から、東ヨーロッパや中央アジア(9位にカザフスタン、KZ)の地域も増えていることが分りました。

これら上位6地域(CN、JP、US、UA、RU、BY)について、今回の調査期間に加えその前の1年間、65週分の割合の推移を図-3に示します。このグラフから、上位2地域(CN、JP)がほぼ一貫して高い割合を維持していることが分ります。また、直近(2013年度第4四半期)では、中国(CN)と日本(JP)の割合の変化が連動しているようにも見えます。過去には2007年の「タクミ通信」逮捕の事例もあり、中国発の迷惑メール送信には、日本が関係していたこともありますので、その関係が深まっているのかもしれない。

2.3 メールの技術動向

ここでは、メールに関わる様々な技術動向について解説します。今回は、迷惑メール対策として期待されている送信ドメイン認証技術の導入状況について報告します。また、これらの技術は標準化され、同じ技術が広く使われることによって効果を上げます。その標準化の動向についても補足します。

2.3.1 送信ドメイン認証技術の普及状況

送信ドメイン認証技術は、既存のメール配送の仕組みであるSMTP⁴に直接影響を与えることなく、導入ができるように作られました。メールを認証するのは、メールの受信側ですが、メールの送信側が送信ドメイン認証技術を導入しているメールのみが認証できます。つまり、メールの送信側と受信側それぞれの判断とタイミングで送信ドメイン認証技術を導入することはできますが、送受信の両方が導入して初めて認証結果を得ることができます。

送信ドメイン認証技術には、メールの送信元のIPアドレスを元に認証するSPF⁵と、メールの本文から電子署名を作成し、それを検証することによって認証するDKIM⁶があります。それぞれの技術について、送信側の導入状況を図-4、図-5に示します。これは、IIJの主要なメールサービスで、2014年1月～3月の間に受信したメール数に対する受信認証結果の割合を調査したものです。

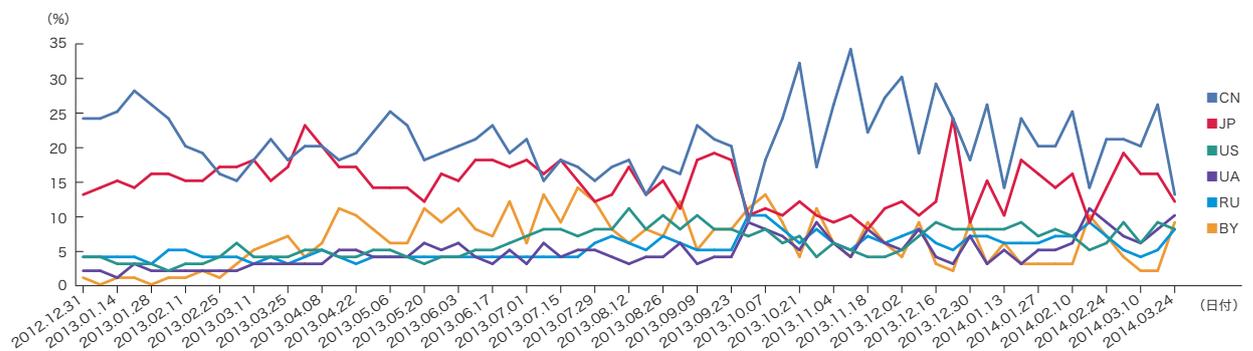


図-3 主要迷惑メール送信元地域の割合の推移

*4 SMTP(Simple Mail Transfer Protocol)、何度か改訂され、最新版はRFC5321として公開されている。

*5 SPF(Sender Policy Framework)、ExperimentalというカテゴリのRFC4408として公開された後、RFC7208(Standards Track)として改訂された。

*6 DKIM(DomainKeys Identified Mail)、RFC6376として公開後、STD76としてインターネット標準となった。

メールの送信側としてSPFを導入するには、メールに利用する(あるいは利用しない)ドメインのDNS TXT資源レコードにSPFレコードを宣言(設定)します。一度SPFレコードを設定すれば、そのドメイン名を利用するメールサーバのIPアドレスに変更がなければ、何もしなくて良いのがSPFの大きな利点です。

この利点もあり、SPFの導入率は、図-4をみても分かる通り、非常に高い割合になっています。送信側でSPFを導入している割合は、認証結果が「none」(認証できなかった)以外の割合となり、今回の調査期間では73.2%でした。認証結果「pass」(47.7%)は、正しく認証されたメールの割合を示します。「hardfail」(2.2%)と「softfail」(21.0%)は、認証が失敗した割合となり、これらはドメインが詐称されたか、メールが転送などにより配送経路が変わって認証できなかったことを示します。

一方DKIMは、送信するメールそれぞれに、メールの本文などから電子署名情報を作成し、それをメールのヘッダに挿入する追加処理が必要になります。そのため、送信用のメールサーバへの新たな機能追加が必要となり、署名を作成するための処理が新たに追加されることで、負荷が高くなる傾向もあるようです。つまり、SPFに比べて送信側での導入が簡単には行えない要因があり、そのため受信側も含めて導入があまり進まない傾向にあると考えられています。しかし、SPFの認証結果で触れたメールの配送経路の変更による認証失敗がほとんど発生しない、という大きな利点

があります。また、メール本文の内容から電子署名が作成されるため、途中経路でのメール本文の改ざんも検知できるなど、SPFに比べてより堅牢な送信ドメイン認証技術とされています。

今回の調査期間で、DKIMの認証結果から見た送信側の導入割合は、11.6%でした。この割合をもっと増やす施策が必要と考えます。

2.3.2 送信ドメイン認証技術の普及の推移

SPFの認証結果の割合の推移を図-6に、DKIMの認証結果の割合の推移を図-7に示します。

SPFは、調査開始(2009年8月)以降、順調に導入割合を伸ばしています。2013年以降はあまり導入割合が伸びていませんが、それでも70%以上と高い導入率を維持しています。この期間、最大で約32.7%導入率が伸びました。DKIMの導入割合はSPFほど急速に増えていませんが、それでも割合は少しずつ増えてはいます。この期間で導入割合は約11.1%増加しました。

Gmailを提供しているGoogle社が、2013年12月に発表したデータ⁷によれば、Gmailが受け取ったspam(迷惑メール)でないメールの91.4%がSPFあるいはDKIMで認証可能であった、と報告しています。本レポートで示している送信ドメイン認証の結果割合は、受信できたメール全体を対象にしているので(迷惑メールも含んでいる)、Google

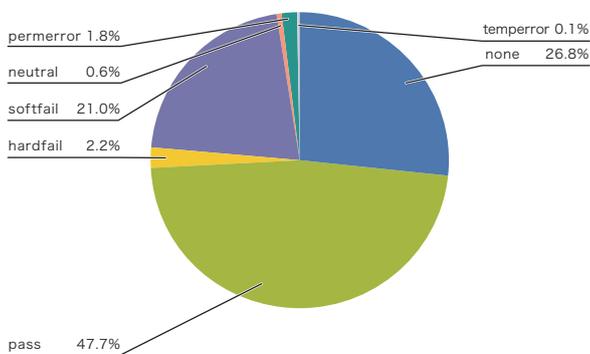


図-4 SPFによる認証結果の割合

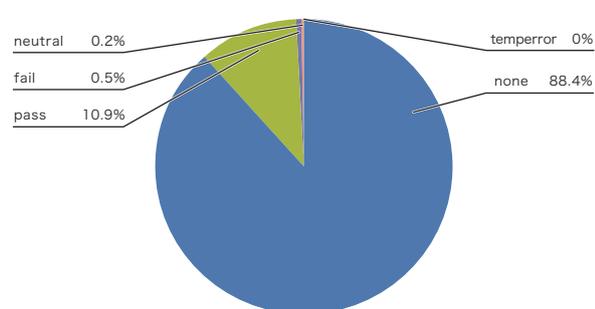


図-5 DKIMによる認証結果の割合

*7 Internet-wide efforts to fight email phishing are working (<http://http://googleonlinesecurity.blogspot.sg/2013/12/internet-wide-efforts-to-fight-email.html>).

社の報告とは、元になったデータの性質が異なっているので、単純には比較できませんが、かなり高い割合でした。

Google社の報告をより詳しく紹介すると、SPFの認証可能だったメールの割合は、89.1%で、DKIMでは76.9%でした。SPFとDKIMの両方が認証できた割合は74.7%ですが、SPFだけ、またはDKIMだけ、というドメインも存在するので、双方の和をとると、全体で91.4%になる、ということのようです。

Google社は、SPFとDKIMの両方の認証結果を利用する、DMARCを推進する企業の一つなので、このような高い導入割合を示し、既に世の中のメールは、DMARCの導入準備が整っている、ということを示していると考えられます。本文中でも、既に8万ドメインが、認証できなかったメールを拒否するポリシーをDMARCで表明しており、このポリシーに従い、毎週数億通のメールを拒否していると報告しています。

DMARCでは、現在利用されているメーリングリストの配送方法と相性の悪い部分が仕様として残っているので、DMARCのポリシーとして受信拒否(reject)を宣言するには難しいケースもありますので、注意が必要です。

2.3.2 SPFの標準化動向

SPFは、実験的(Experimental)RFCとして標準化された技術です。現在、このSPFの改訂作業が行われています。そもそもSPFは、同時期(2006年4月)に同じくExperimental RFCとして公開されたSender ID⁸との統合を目指して、IETFのMARID WGで検討が重ねられていた技術です。Sender IDの特徴であるPRA (Purported Responsible Address)について、提案元の会社が知的所有権を主張したことなどから統合の議論が不調に終わってしまった、という経緯がありました。

しかし、既にデータを示してきたとおり、SPFが送信ドメイン認証技術として、広く普及していることから、標準化

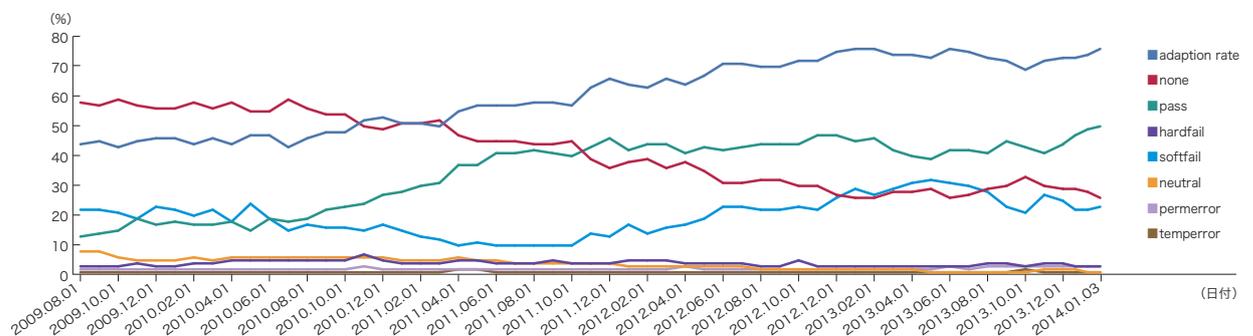


図-6 SPFによる認証結果割合の推移

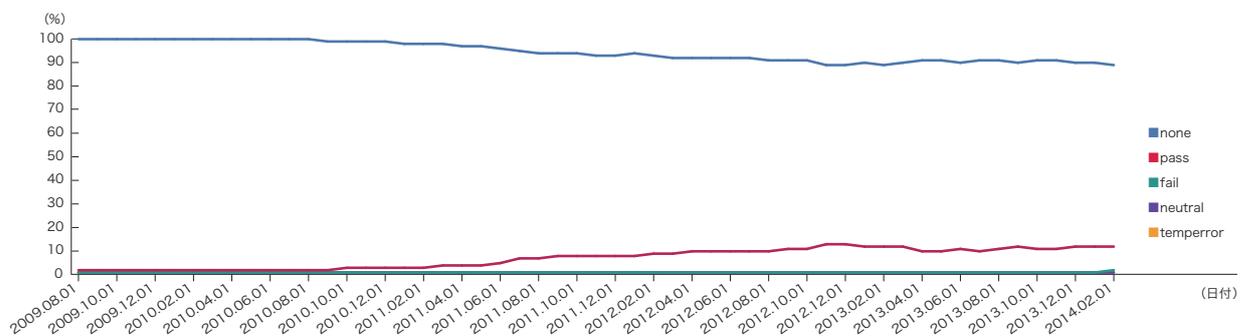


図-7 DKIMによる認証結果割合の推移

*8 Sender ID: RFC4406, RFC4407

を目指してこれまでの経験も踏まえてまとめよう、ということでは、IETF spfbis WGが2011年11月から議論を重ねて来ました。SPFは、2014年4月にRFC7208として、標準化への提唱(Standard Track)として公開されました。今回は、このRFC7208と従来のRFC4408との違いについて解説します。

まず、議論の前提として、以下のような見解を示しています。

- ・ SPFは成功したがSender-IDはそうではない(なのでSender IDの取り込みはしない)
- ・ SPFの仕様改訂のポイントは、間違いの訂正、利用していない機能の削除、既に広く使われている拡張の追加など
- ・ SPF自体の拡張や使われている機能の削除はしない

よって、spfbis WGによるIDでは、それほど大きな変更が加えられませんでした。現在のIDで示されている主な変更点は以下です。

1. SPFレコードは、DNS上のSPF RR type (99)ではなくTXT RR(16)を利用
2. 認証結果を保存するメールヘッダは、"Received-SPF"と"Authentication-Results"を併用

これ以外については、細かな間違いの修正などです。結局、認証失敗時のメールの取り扱いについてRFCでは指針を示すことはせず、受信側で方針を決めて判断することになりました。比較的複雑な書式を記述できるSPFのマクロ機能は、それほど積極的に使っているドメインは少ないと思いますが、仕様として残すことになりました。

SPFの課題である、メールの転送についても、明確に対処方法は示さず、転送時にRFC5321.From (エンベローブ

From)を書き換えたり、転送先で受け取るようホワイトリスト的な設定をすることなどが示されただけでした。SPFのInternet-Draftは、21版まで改訂されており、実際に変更されたポイントの割にはかなりの時間を要しました。SPFは、送信側の導入が用意であることから普及率も高く、この標準化作業によって、SPFの認証結果の活用が進むことを期待します。

2.4 おわりに

今回は、1年ぶりのメッセージングテクノロジーでしたので、少し詳しく迷惑メールの動向や送信ドメイン認証技術について解説しました。本文中でも述べたとおり、迷惑メールの量自体は減少傾向にありますが、(迷惑)メールに起因する危険度は高まっています。

例えば先日、大手銀行によるフィッシングメールの注意喚起のCMがテレビで放送されているのを見ました。テレビのような媒体で、一般の方々に注意を促さなければならないほど、被害が増えている、ということだと思います。そのCMでも、手口が巧妙になっていると述べられていました。インターネット上のセキュリティ的な脅威が高まるにつれて、企業などの組織や個人も含めて様々な対策をするようになってきました。しかしながら、現在のメールシステムは、様々な情報を受信者に直接届けることができる数少ないアプリケーションの一つです。そこを狙った攻撃がこうして続いている現在では、メール受信者個々の判断力に依存した形での脅威の回避方法には限界があるでしょう。メールシステムに関わる者としては、こうした危険性の高いものを判別し、メール利用者に届けることのない仕組みの提供を早く実現したい、と日々取り組んでいます。

執筆者:



櫻庭 秀次(さくらば しゅうじ)

IJ プロダクト本部 アプリケーション開発部 サービス開発課 シニアエンジニア。コミュニケーションシステムに関する研究開発に従事。特に快適なメッセージング環境実現のため、社外関連組織と協調した各種活動を行う。M³AAWGの設立時からのメンバー。迷惑メール対策推進協議会 座長代理、幹事会 構成員、送信ドメイン認証技術WG 主査、LAP 10 Tokyo 委員会 委員長。一般財団法人インターネット協会 迷惑メール対策委員。

ビッグデータ解析の現状

本レポートでは、既にエクサバイト級のデータが流通していると推定されるビッグデータの現状ならびに解析基盤の技術動向とそのリアルタイム化に伴うビッグデータ解析の変化について解説します。

3.1 ビッグデータの現状

近頃では、至る所で見聞きするようになった「ビッグデータ」ですが、その実態は相変わらず非常に捉え辛いままで。語り手の立場や意見によって「ビッグデータ」の意味するところが大きく異なることや、有効だとされる活用事例が様々な業種をまたいで多岐にわたることが、その主たる原因でしょう。ビッグデータに関わる現状の網羅的な把握を試みた総務省の平成25年度の調査では、国内でのビッグデータの流通量は年々拡大していることが報告されています。

メディア別の流通量では、POS、RFID、GPSから得られるデータの総量が多く、経年推移では医療系データ（電子カルテ、画像診断）とM2M系データ（GPS、RFID）が大きく伸

びていると報告されています。この調査では、メディアについて「データは出生が多様で様々な種類に及んでる」とし、



図-1 データ形式の異なる3種類のデータ

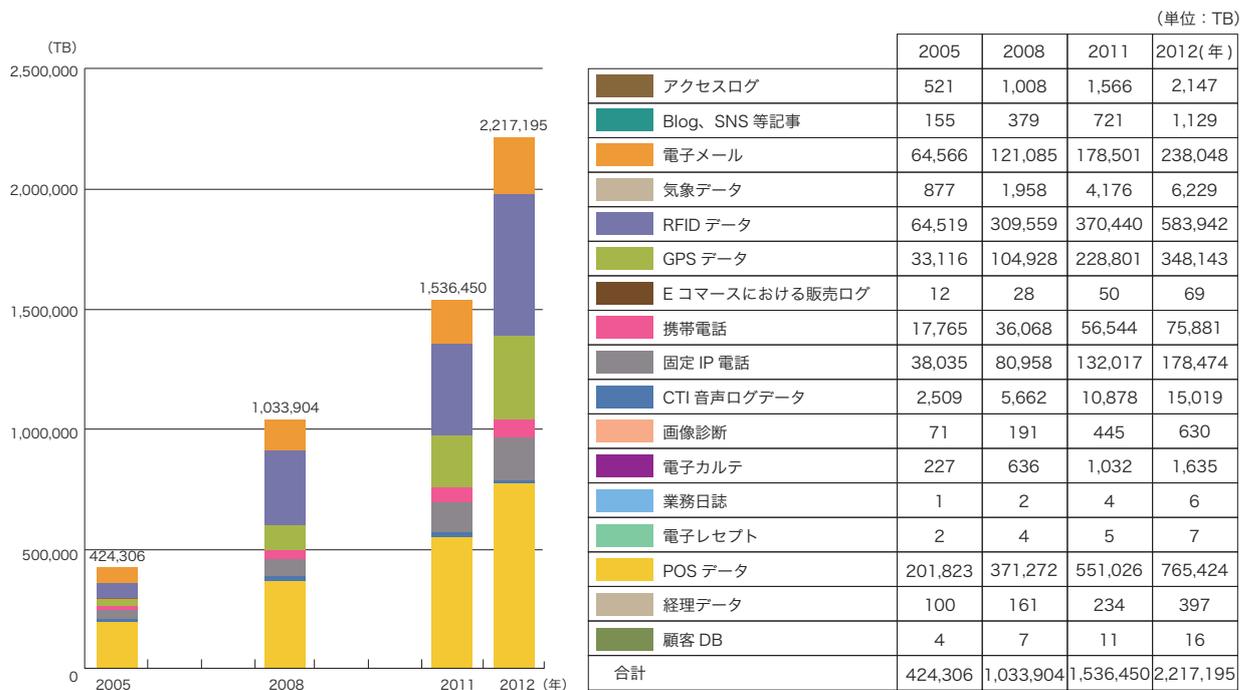


図-2 ビッグデータ流通量の推計^{*1}

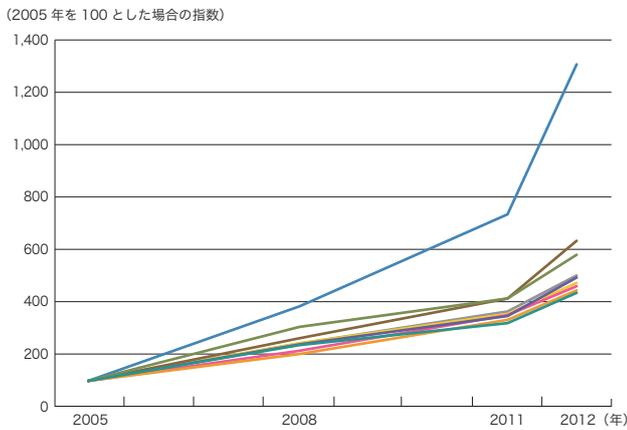
*1 <http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/html/nc113220.html>

「データ形式の異なる3種類のデータに分類される(図-1)」と説明されていますが、データ分析の視点から見ると非構造データ(新)に分類されるデータ群の中には、POS、RFID、GPSなどのように標準フォーマットが規定されている(すなわち構造化されている)事例もありますし、映像や音声、テキストなどのストリームデータでも、タイトルや著作者などのメタ情報を内蔵する事例があるので、実際には、構造型データと非構造型データを内包する複合型のデータと理解するべきでしょう。図-2は、国内で流通するビッグデータ

は非構造化データよりも構造化データが圧倒的に多いことを示しています。

次に、産業別でのビッグデータの流通量(図-3)と蓄積量(図-4)の推定値について、総務省の調査では次のように報告しています。

この推定の大変興味深いところは、流通量に関しては(不動産を除くと)概ね同じ特性で増加しているのに対し、蓄積



	2005	2008	2011	2012(年)
製造業	100	233	320	431
建設	100	303	411	576
電力・ガス・水道	100	200	327	436
商業	100	239	345	496
金融・保険	100	211	349	459
不動産	100	378	732	1,310
運輸	100	260	410	632
情報通信	100	242	351	462
サービス	100	236	363	499

図-3 ビッグデータ流通量の推移(産業別) ^{*2}

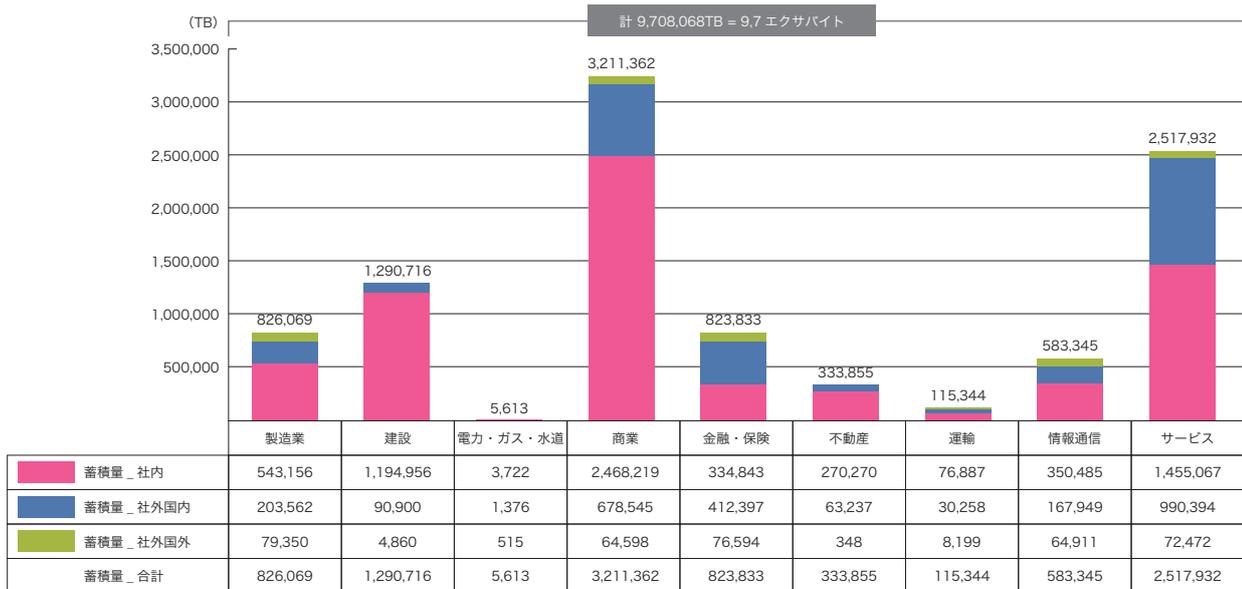


図-4 ビッグデータ蓄積量(産業別、2012年) ^{*3}

*2 <http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/html/nc113220.html>

*3 <http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/html/nc113230.html>

量は業種ごとに大きく異なることです。ビッグデータの蓄積量は、その利活用の度合いを表しているとするれば、これは業種ごとのビッグデータ利活用に対する取り組みの温度差を示していると理解することもできますが、業界ごとの慣行の違いが反映されている可能性もあります。産業別の蓄積量では、BtoBの業種よりもBtoCの業種の方が蓄積量は多いこと、更に、ビッグデータの多くが所有者の内部に留まっている非公開データであることにも注目されます。

総務省の調査結果に基づけば、既にエクサバイト級のデータが流通していると推定されることから、「ビッグデータの利活用は始まっている」と主張しても良いでしょう。しかしながら、「大量のデータソースから収集・蓄積したビッグデータを選別・分析することにより、新たな知見を得る」というビッグデータ本来の利活用は、端緒についたところという現状が浮かび上がってきます。

さて、今後のビッグデータの利活用を促進・加速する「ビッグデータに関わる今日的な課題」という議論では、「ビッグデータの共有化をどのよう、促進するのか?」、また、「ビッグデータの解析により、どのような新たな知見を得られるのか?」の2つの課題が掲げられることが多いのですが、その文脈で頻りに語られるのが、M2M、IoT、CPSの3つのキーワードです。各々の定義を確認すると、Machine-to-Machine (M2M)は、有線や無線の通信システムを用いて同じ種類のデバイスの間でのコミュニケーションを可能にする技術、Internet of Things (IoT)は、インターネットのような構造の中で仮想的に表現されるユニークに識別可能なオブジェクト、Cyber-Physical System (CPS)は、物理的な実体を制御する協調型計算エレメントによるシステムということで、各々は独立した概念というよりは、センサーなどのデバイスから構成されるネットワークに対して、3つの視点を提示していると理解するべきなのかもしれません。例えば、RFIDタグを用いた荷物の集配管理システムでは、個々の荷物にRFIDタグが付与されますが、その荷物がRFIDリーダーの近傍を通過すると、その位置情報を付加されたデータが生成されます。このデータを蓄積しておいて任意の荷物について位置情報をトレースすると、その荷物がどのような経路で移動して、現在どこで保管されているのかを調べることができます。更に、集配管理システムが取り扱うすべての荷物についてトレースすれば、荷物が集中して

いる配送センターを正確に把握することができます。スマートフォンが普及した今日では、同じ方法で人間の動態も把握できるわけですが、各デバイスが生成するデータを集めるとビッグデータが形成され、業務の最適化やマーケティングに有益な知見が得られると考えられています。

3.2 ビッグデータ解析基盤の技術動向：リアルタイム化

前述のようなM2M、IoT、CPSのコンセプトに基づくデバイスネットワークから生成されるビッグデータの解析には、即時性が求められることは自明ですので、必然的にビッグデータ解析基盤は、リアルタイム解析の要請に応えなければなりません。

ビッグデータ解析の基盤技術と言え、特にMapReduceに基づく分散処理基盤の技術を思い浮かべる方々が多いかと思いますが、バッチ処理を前提として設計されたMapReduceのアーキテクチャをリアルタイム解析に適用するには困難が伴います。バッチ処理ではジョブが終了するまでに処理結果が確定しないので、処理時間分の遅延が発生してしまいます。この時間を縮小する対策としては、まず処理そのものの最適化・高速化を図ることになりますが、自ずと限界があります。次なる対策としてはバッチ処理のサイズを小さくしていくことになりますが、あまり小さくしてしまうとバッチ処理として意味をなさなくなってしまいます。通常、MapReduceジョブは数分から数時間という処理時間を要することが一般的ですが、これをウェブサービスで許容される応答時間の数秒程度まで時間短縮することは事実上不可能だと言えるでしょう。

ビッグデータ解析基盤のリアルタイム化の研究では、2つのアプローチが検討されてきました。その1つは、「ユーザのリクエストにリアルタイムで応答する」アプローチで、この場合「MapReduceの基盤そのものを機能強化」して応答性能を向上させるケースと、「MapReduceを内包する基盤システム」として考えて、内部的にはMapReduceを利用しつつ、それ以外のところで応答性能の向上を図るケースがあります。もう1つは、「実際に実時間でデータ処理を実行する」、いわゆる「リアルタイムストリーム処理」を実現する基

盤技術を用いるアプローチで、この場合はMapReduceに置き換わる形になります。

「MapReduceの基盤そのものを機能強化」の事例としては、MapReduce Online^{*4}があります。この事例ではHadoopを大幅に改造してMap処理とReduce処理の間のデータの受け渡しのパイプライン化を図っています。この機能拡張によりユーザは処理中のジョブの状態を詳細に把握する、すなわちイベントモニタリングが可能になります。また、MapReduceアプリケーションでストリーム処理を記述することが可能です。

「MapReduceを内包する基盤システム」の事例としては、GoogleのDremel^{*5}のアイデアを踏襲する2つのオープンソース・クローン「Apache Drill^{*6}」と「Cloudera Impala^{*7}」が上げられます。いずれも、リアルタイムでのデータ処理を行っているわけではありませんが、それに匹敵する低遅延でのクエリー応答性能を発揮します。

「リアルタイムストリーム処理」の事例としては、Apache Storm (Twitter Storm)^{*8}があります。Stormは元々Twitterの分析を行っていたBackType社が開発したシステムですが、Twitter社によるBackType社の買収にともなってApache Project経由でオープンソース化された経緯がありますが、それ自体は汎用のビッグデータ処理基盤です。

Stormは、Complex Event-Processing (CEP) を実現するストリームエンジンが搭載されており、Spout/Boltと呼ばれるビッグデータ処理を行うエンティティに欠損のないデータストリームの供給を保証します。Stormでのストリームは、Tupleと呼ばれるデータ単位のフローで表現され、SpoutとBoltを繋ぎ合わせるTopologyを定義することにより、ストリーム処理全体を記述します。Spoutはデータソースを表現するエンティティであるのに対し、Boltはデータの変換・加工を司るエンティティです。定義や機能は全く異なりますが、MapReduceにおけるMap及び

Reduceを想像すると理解しやすいでしょう。

StormもHadoopと同じようにクラスタを構成することが可能で、Nimbus、Zookeeper、Supervisor、Workerの4種類のソフトウェアが動作します。Nimbusは、Workerのスケジューリングやモニタリングを司るマスター、Zookeeperは、Hadoopでも使用されている分散ロックマネージャ、SupervisorはNimbusからのリクエストを受け付けWorkerの起動・停止を制御し、Workerは、実際の処理を実行するプロセスとして機能します。これらのソフトウェアをクラスタ内のノードに適切に配置することにより、高いスケラビリティや耐障害性を実現しています。Storm自身は、Clojureと呼ばれるLISPライクな言語で記述されていますが、JavaVMの上で動作します。従って、JavaをはじめとするJavaVMの上で動作する各種の開発言語を使ってSpoutやBoltを記述することができます。

以上、ビッグデータ解析基盤のリアルタイム化に関する課題と幾つかの事例を紹介してきましたが、Apache Stormの登場をリアルタイムビッグデータ解析基盤のデファクトスタンダード化のトレンドと捉える見方が増えているように思えます。やはり、Hadoop (MapReduce) と共通するシンプルなプログラミングモデルとTwitter分析での実績は、汎用的なプラットフォームに期待される要件でしょう。

では、StormはHadoopに置き換わるオープンソースのビッグデータ解析基盤になるのでしょうか？この質問に対する答えは、「両者による棲み分けが進む」ということになりそうです。というのも、すべてのビッグデータ解析が即時性を求められる訳ではないからです。前述のような、即時応答を求められるビッグデータ解析の需要は、Stormに置き換わって行くでしょうが、従来のバッチ処理で十分(あるいはそれが必要)な需要にはHadoopが使われ続けることになるでしょう。またHadoopでの解析の前処理(データの整形、フィルタリング、マッチング)にStormを活用したり、ラムダアーキテクチャと呼ばれるバッチ処理とストリー

*4 <http://db.cs.berkeley.edu/papers/nsdi10-hop.pdf>

*5 <http://research.google.com/pubs/pub36632.html>

*6 <http://incubator.apache.org/drill/>

*7 <http://blog.cloudera.com/blog/2012/10/cloudera-impala-real-time-queries-in-apache-hadoop-for-real/>

*8 <http://storm.incubator.apache.org/>

ム処理を組み合わせたハイブリッドなシステム構築法も提案されています。現時点では、両者は相互補完の関係にあるという理解が一般的なようです。

3.3 リアルタイム化に伴うビッグデータ解析の変化

ビッグデータ解析基盤のリアルタイム化は、ビッグデータの定義でよく語られる3Vs (Volume, Variety, Velocity) のうちのVelocity方向への能力拡大への対応と理解されています。3Vsの定義を世に広めたGartnerによると、Velocityでは「データの生成と処理の高速性」について説明していますが、例えば、センサーデータやログデータの解析や、GPS情報を用いた時空間データ解析、あるいはソーシャルメディアから入手できるストリームデータの解析などが、Velocityの要件が問われる具体的な事例として上げられます。このような既存の解析では、異常検知や空間移動の履歴、センチメント分析など、蓄積している過去データから新たな知見を得る事例が良く知られていますが、リアルタイムビッグデータ解析基盤の即時性の向上により、今後は、より時間軸に重点をおいた時系列分析や、それに基づく予測などへと解析方法の多様化が進むと考えられています。

3.3.1 ソーシャルビッグデータとしてのWikipedia

我々は、ビッグデータの時系列に着目した分析の1例として、Wikipedia Pageview Count (Wikipedia PVC: <http://www.gryfon.ijj-ii.co.jp/ranking/>) を用いたトレンド分析を試みています。周知のように、Wikipediaは最も成功しているインターネット百科事典です。非常に開かれた運営方針が採用されており、そのデータベース等は無償で入手できることから、研究など様々な用途に活用されています。その一部として公開されているWikipedia PVCは、2013年1月頃から公開されるようになりましたが、これは各Wikipediaページの直近の1時間あたりのページビュー数を1~2時間の更新頻度で公開しています。Wikipedia PVCとWikipediaデータベースを組み合わせると、社会的トレンドを示す時系列データとして利用することができますが、これはインターネット経由で入手できるソーシャルビッグデータの1例と見なせます。百科事典としての特性を持つため、一般的なソーシャルメディア(SNSやブログ)

と比較すると次のような特徴があります。

- ・利用者自身の改変が認められていますが、ガイドライン等により記述内容の発散を防ぐ運用が行われているため社会全般に関する最大公約数的情報が得られます。
- ・百科事典であるが故に網羅性に優れており、閉じた空間内でLinked Dataを形成しています。
- ・一般利用者のサービス認知度が高く、利用者は未知のトピックの詳細や関連情報を知るために利用しています。
- ・多言語に対応しており、各言語間でのページごとの対応付けが明確である事例が多いです。

トレンド分析などにおいて、一般的なソーシャルメディアから取得したメッセージ等を用いてテキスト分析を行う場合、用語法の統一などが図られていないため、データ解析を行う上での障害となる場合が多いですが、意味的な発散が抑制されているWikipediaデータでは、そのような障害は起こりづらく、人間に理解しやすい分析結果が得られると考えています。

3.3.2 Wikipedia PVCの時系列変動の分析

百科事典として広く認知されているWikipediaでは、メインページ、あるいは外部のサーチエンジンから、知りたいトピックについて検索して該当するページにたどり着く利用パターンが一般的でしょう。

あるWikipediaページに着目して、そのPVCの時系列的変動を観察すると、いずれかのタイミングでピークが発生した後、徐々に減衰をすることが確認できます。特に、顕著なピークが現れる幾つかのページについて更に調査を進めたところ、テレビ放送やネットニュースで報道されたトピックを扱うページが反応していることが分かりました。すなわち、テレビ番組の視聴者やネットニュースの読者は、未知のトピックが現れた場合にWikipediaでその内容を調べる行動を取っている仮説が成り立ちます。

そこで、この仮説を検証するために、連続ドラマに着目しドラマの各回の放映時間と、Wikipedia PVCの時系列的変動との関係を調査しました。連続ドラマに着目した理由は、連続ドラマが放映されている時間には対応するWikipediaページのPVCにピークが発生する確率が極めて高いこ

とが確認できていたことによります。また、テレビドラマの場合は「視聴率」という広く認知されている指標があり、Wikipedia PVCによるピークとの関係を調べることができることも重要でした。

Wikipedia PVCは、2008年以降に民放で放映された連続ドラマ334件すべてのデータを入手できます。その中から、Wikipedia PVCにデータ欠損のないドラマ244件について、次のような方法で分析を行いました。

1. ドラマ1話分の放映時間を1時間と仮定し、放映時間から次回放映1時間前までの168時間を1つの時系列データとして抽出する。
2. 抽出した時系列データに対し回帰分析を行い、得られた係数をその回の社会的関心度とする。
3. 各回の社会的関心度とその回の平均視聴率の相関を調べ、その有意性を確認する。

[2]の回帰分析では、計量経済学で用いられる「社会的イベントは指数関数に基づいて変動する」との知見に基づき、回帰式 $pvc = \alpha * \exp(\beta * t) + \gamma$ を用いて分析を行いました。更に、放送時間の遅延や拡大を考慮してピーク値の補正を行いました。

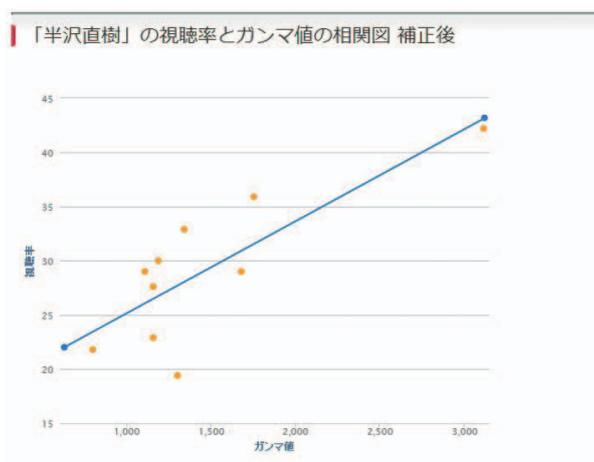


図-5 「半沢直樹」の各回の γ 値と平均視聴率との相関分析結果

執筆者:



藤田 昭人(ふじた あきと)

株式会社IIRイノベーションインスティテュート (IIR-II) 企画開発センター チーフアーキテクト。2008年IIR入社。構造化オーバーレイ研究の知見を活用したクラウドコンピューティング技術の研究開発に従事している。

非線形回帰分析の結果はいずれも放映時に高いピークを示し、その後 γ 値に収束します。分析により得られた係数 α, β, γ について平均視聴率との相関を調べたところ、 γ 値との間に相関が見られました。テレビドラマ「半沢直樹」の各回の γ 値と平均視聴率との相関分析結果を図-5に示します。

γ 値と平均視聴率の相関は、本稿執筆時には、有効データ244件のうち40件で分析を行い「有意性あり」の結果を得ています。残る204件についても相関分析を順次実施して行きますが、特に、視聴率の低いドラマの場合には、Wikipedia PVC変動と視聴行動が同期していない事例も見ついているため、有効データにおいて「有意性あり」が確認できる件数と、この解析方法が適用できるWikipedia PVC値の範囲を明らかにする計画です。

3.4 まとめ

本稿では、M2M、IoT、CPSのキーワードで語られる現在のビッグデータに関わる現状と、それに伴ってリアルタイム化を指向する解析基盤に関わる技術動向、更に時系列データからの知見を得るビッグデータ解析手法の多様化について概観しました。

「ライブで精緻なデータを取得」して、「即時性の高い処理基盤」を活用し、「今起きている何かを把握する」試みからは、従来の「静的でマクロな知見」を得るビッグデータ解析とは大きく異なる「動的でミクロな知見」が得られるものと想像しています。この新たな知見の中には「これから起こる何かの予兆」が含まれている可能性があります。誰よりも早くこのような予兆を見つけることが、今後のビッグデータに関わる課題になるかもしれません。

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など、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

〒101-0051 東京都千代田区神田神保町1-105 神保町三井ビルディング
E-mail: info@ijj.ad.jp URL: <http://www.ijj.ad.jp/>

本書の著作権は、当社に帰属し、日本の著作権法及び国際条約により保護されています。本書の一部あるいは全部について、著作権者からの許諾を得ずに、いかなる方法においても無断で複製、翻案、公衆送信等することは禁じられています。当社は、本書の内容につき細心の注意を払っていますが、本書に記載されている情報の正確性、有用性につき保証するものではありません。

©2008-2014 Internet Initiative Japan Inc. All rights reserved.

IJJ-MKTG019WA-1405GR-09000PR