

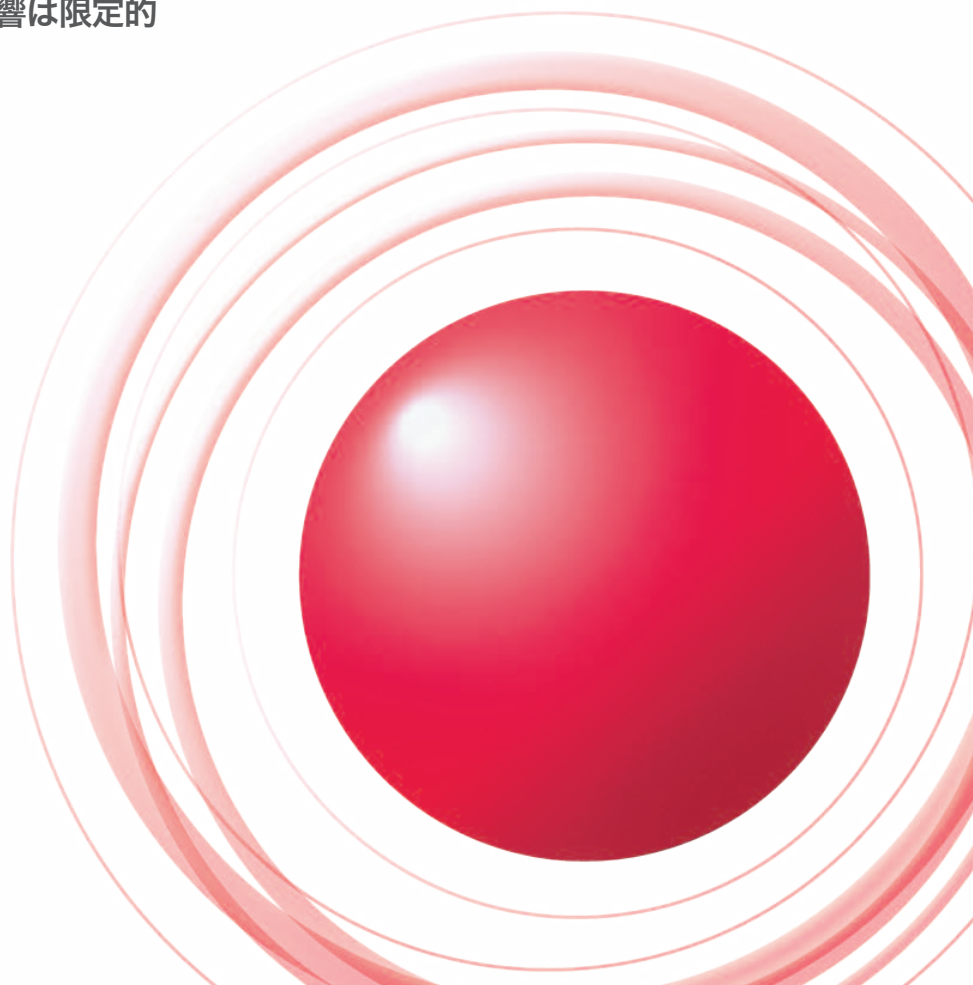
Internet Infrastructure Review Vol.20

August
2013

インフラストラクチャセキュリティ
ホームルータのセキュリティ

メッセージングテクノロジー
迷惑メール送信を目的とした
不正SMTP認証の増加

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



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
1.4 フォーカスリサーチ	18
1.4.1 ZeroAccessとそのIOCに関する考察	18
1.4.2 ホームルータのセキュリティ	21
1.4.3 頻発する不正ログイン事件	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 不正SMTP認証によるアクセスの動向	28
2.2.1 不正SMTP認証	28
2.2.2 不正SMTP認証の特定	28
2.2.3 不正SMTP認証の観測	29
2.3 おわりに	31
3. ブロードバンドトラフィックレポート	32
3.1 概要	32
3.2 データについて	32
3.3 利用者の1日の使用量	33
3.4 ポート別使用量	35
3.5 まとめ	37
インターネットトピック：IIJmio高速モバイル/Dサービスとオンラインチャージング	38

エグゼクティブサマリ

数ヵ月程前から、Facebookで見知らぬ人からの友達リクエストが増えているように思います。最近では「友達」になりすましてリクエストを送ってくるケースも増えています。友達だと思って承認しようとしたら、よく見ると漢字が1文字違っていたなど、巧妙なものもあります。これらのリクエストが悪意を持ったものである場合、不用意に承認をしてしまうと、相手にアカウントを乗っ取られてしまうことがあります。たかがFacebookの友達リクエストだからと気楽に何でも承認してはいけない状況になってきています。

今年6月には、元CIA職員により、国家安全保障局(NSA)などアメリカの情報機関に、Facebookを始めとするSNS加入者の個人情報が提供されていたことが暴露され、大きな波紋を呼びました。全世界のFacebookのユーザ数は10億人を超えたと言われていいますので、それが何らかの犯罪を目的としたものであるうが、何らかの統制を目的としたものであるうが、個人情報を手際良く集めようと思った時に、とても便利なツールであることに間違いありません。

インターネットがオープンで拡張性に富む基盤であるが故に、これまでにない便利さと同時に、これまでにない危うさも同居しています。その両面をきちんと理解した上で、便利さを享受し、危うさにはきちんと対応して行く姿勢が、基盤の運用者、そして利用者にも今後ますます求められるようになるでしょう。

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、2013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、ZeroAccessとそのIOC(Indicator of Compromise)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、不正な手段でアカウントと認証情報を入手した第三者による、不正SMTP認証について取り上げ、2013年4月から6月までの直近13週間の不正SMTP認証アクセスの動向を分析し、傾向の変化について報告します。

「ブロードバンドトラフィックレポート」の章では、IJが運用しているブロードバンド接続サービスの、2013年6月3日から9日の1週間分のトラフィックデータを分析し、前に行った2012年5月28日から6月3日の分析結果と比較します。また、過去6年間の月平均トラフィックの推移に着目し、この期間に起こった2回にわたる著作権法改正や、東日本大震災がブロードバンドトラフィックに与えた影響について分析します。

「インターネットトピック」では、IJが「IJmio高速モバイル/Dサービス」において、2012年2月、世界に先駆けて提供を開始したユニークな料金プラン、オンラインチャージングを実現する仕組みについて解説します。

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。

ホームルーターのセキュリティ

今回は、マルウェアZeroAccessの検出に関する考察を紹介すると共に、様々なリスクを誘発するホームルーターのセキュリティの状況、及び今年に入ってから頻発している不正ログイン事件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2013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、Webサーバへの不正侵入とそれによるWebサイトの改ざんも相次ぎました。4月にはポータルサイトやショッピングサイトへの不正なアクセスが多く発生し、いくつかの事件は他のWebサイトから入手したと考えられるID/パスワードのリストを使ったなりすましの試みと推測されています。ccTLDを含むドメインレジストリに対しての攻撃と、それによるドメインハイジャックや情報漏えいも継続して複数発生しています。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。

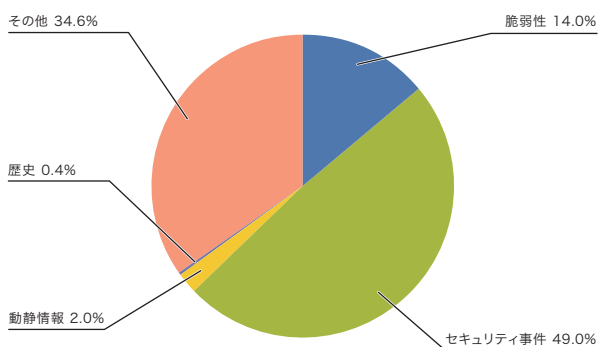


図-1 カテゴリ別比率(2013年4月~6月)

1.2 インシデントサマリ

ここでは、2013年4月から6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。目立った攻撃としては、北朝鮮の政府や関連するWebサイトへの攻撃が相次いで発生し、Webサイトの改ざんやアカウント情報などの漏えいが複数発生しています(OpNorthKorea)。また、イスラエル政府や関連サイトへの攻撃(Opsrael)、それに対する報復と見られるイスラエル側からの攻撃も複数発生しました。この攻撃に関連してヨルダンで攻撃に関与したとして複数人が逮捕されています。更にトルコでは、公共事業に対する抗議デモへの警察の取り締まりに対する抗議として、政府機関やメディアのWebサイトに対するDDoS攻撃が行われました(OpTurkey)。この事件でも攻撃に関与したとして、トルコ当局によって30人以上の容疑者が逮捕されています。いずれの事件でも、容疑者の逮捕への抗議として更に攻撃が行われるなど、報復が続いています。5月に米国の政府機関や金融機関を対象として行われた攻撃(OpUSA)では、数百のWebサイトの改ざんや不正侵入による情報漏えい、DDoS攻撃などが行われましたが、影響は限定的なものに止まりました*2。6月には国際的な石油ガス会社や産油国

*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。

*2 攻撃の詳細については、次のTrend Micro SECURITY BLOGなどに詳しい。「『OpUSA』攻撃失敗から垣間見える攻撃者たちの戦術」(<http://blog.trendmicro.co.jp/archives/7266>)。

に対しての攻撃(OpPetrol)が行われましたが、こちらも大規模な攻撃ではありませんでした。

Anonymous以外のグループによる活動も継続しており、引き続き活発な活動を行っています。

■ 脆弱性とその対応

この期間中では、Microsoft社のWindows^{*3}、Internet Explorer^{*4*5*6*7}、Office^{*8}などで修正が行われました。Adobe社のAdobe Flash Player、Adobe Reader及びAcrobatなどでも修正が行われました。Oracle社のJavaでも複数の更新が行われ、多くの脆弱性が修正されています。ジャストシステム社の一太郎では、任意のプログラムが実行可能な脆弱性が分かり、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、特定のリソースレコードに対する問い合わせ処理により、サーバの異常停止などを引き起こす脆弱性が修正されています^{*9}。

サーバ管理ツールとして利用されているParallels Plesk Panelでは、サポートが終了したバージョンでPHPの不適切な設定が原因の未修正の脆弱性が公表されました。この脆弱性については、簡単に悪用されることが報告^{*10}されたこと

から、サポートされている最新バージョンへの更新を行うようユーザに対して呼びかけが行われています。WebアプリケーションフレームワークのApache Strutsでも、複数の脆弱性が分かり修正されました。CMSとして利用されるWordPressについても、権限の昇格やクロスサイトスクリプティング脆弱性を含む複数の脆弱性が修正されました。

■ Webサーバへの不正侵入の増加

この期間では、Webサーバへの不正侵入と、それによるWebサイトの改ざんが話題となりました。改ざんされたWebサイトの多くは、別のWebサイトへ誘導するiframeや難読化されたJavaScriptが埋め込まれており、ユーザが改ざんされたWebサイトを閲覧すると、不正なWebサイトに誘導され、マルウェアに感染する可能性があります。これらの誘導された不正なWebサイトには、BHEK2(Blackhole Exploit Kit Version 2)などを含むExploit kitが設置されており、組織的な活動を行っていたと考えられます。企業や団体を含む複数のWebサイトが改ざんされており、JPCERTコーディネーションセンターの注意喚起^{*11}では、本年4月以降、注意喚起の時点で約1,000件が報告されているとしています。

これらの改ざんされたWebサイトでは、サポート期限切れのバージョンを含む、古いバージョンのCMS(Content Management System)やサーバ管理ツールなどの脆弱性が多く狙われました^{*12}。このため、特に危険と考えられるいくつかの脆弱性については注意喚起が行われています^{*13}。

-
- *3 「マイクロソフト セキュリティ情報 MS13-029 - 緊急 リモート デスクトップ クライアントの脆弱性により、リモートでコードが実行される (2828223)」(<http://technet.microsoft.com/ja-jp/security/bulletin/ms13-029>)。
 - *4 「マイクロソフト セキュリティ情報 MS13-028 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (2817183)」(<http://technet.microsoft.com/ja-jp/security/bulletin/ms13-028>)。
 - *5 「マイクロソフト セキュリティ情報 MS13-037 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (2829530)」(<http://technet.microsoft.com/ja-jp/security/bulletin/ms13-037>)。
 - *6 「マイクロソフト セキュリティ情報 MS13-038 - 緊急 Internet Explorer 用のセキュリティ更新プログラム (2847204)」(<http://technet.microsoft.com/ja-jp/security/bulletin/ms13-038>)。
 - *7 「マイクロソフト セキュリティ情報 MS13-047 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (2838727)」(<http://technet.microsoft.com/ja-jp/security/bulletin/ms13-047>)。
 - *8 「マイクロソフト セキュリティ情報 MS13-051 - 重要 Microsoft Office の脆弱性により、リモートでコードが実行される (2839571)」(<http://technet.microsoft.com/ja-jp/security/bulletin/ms13-051>)。
 - *9 この脆弱性については、JPCERTコーディネーションセンターからも注意喚起が行われている。「JPCERT/CC Alert 2013-06-05 ISC BIND 9 サービス運用妨害の脆弱性(CVE-2013-3919)に関する注意喚起」(<http://www.jpccert.or.jp/at/2013/at130026.html>)。
 - *10 この脆弱性についての詳細は、例えば次のCisco Blogsなどで確認できる。「Plesk 0-Day Targets Web Servers」(<http://blogs.cisco.com/security/plesk-0-day-targets-web-servers/>)。
 - *11 JPCERTコーディネーションセンター、「JPCERT/CC Alert 2013-06-07 Web サイト改ざんに関する注意喚起」(<https://www.jpccert.or.jp/at/2013/at130027.html>)。
 - *12 例えば、独立行政法人情報処理推進機構から6月に公表された、「今月の呼びかけ ウェブサイトが改ざんされないよう対策を！」(<http://www.ipa.go.jp/security/txt/2013/06outline.html>) では、IPAに寄せられたWeb改ざんの原因で最も多かったとしている。
 - *13 JPCERTコーディネーションセンター、「旧バージョンの Parallels Plesk Panel の利用に関する注意喚起」(<http://www.jpccert.or.jp/at/2013/at130018.html>)。

4月のインシデント

1	セ	1日：全国200の自治体で、住民基本台帳ネットワークが利用できないトラブルが発生した。これは3月に発生した障害によるデータの確認作業が長引いたことによる。
2	セ	2日：goo!Dへの不正ログインの試みが発生し、4月9日までに108,716アカウントが不正ログインの可能性があると、アカウントロックが行われた。この事件では、他社サービスから流出したID/パスワードのリストをgoo!Dシステムに対して試行している痕跡が認められたとしている。NTTレゾナント株式会社、「goo!Dへの不正ログイン被害について(終報)」(http://pr.goo.ne.jp/detail/1703/)。
3		
4	セ	4日：フレッツ光の会員制サイトで、不正ログインの試みが発生し、30アカウントに不正ログインの可能性があると分かり、アカウントの規制やサイトへのログインを規制する措置が取られた。東日本電信電話株式会社、「フレッツ光メンバーズクラブ会員サイトへの不正アクセスについて」(http://www.ntt-east.co.jp/release/detail/20130404_02.html)。
5		
6	セ	5日：電子書籍販売サイトで、2013年4月1日から4月5日にかけて不正ログインが発生し、779アカウントについて、不正が疑われるIPアドレスからのログインが行われたとして、当該ユーザIDのパスワードの初期化が行われた。
7	セ	5日：会員制ポイントサイトへの不正ログインによるなりすましが3月26日に発生し、299IDでポイントが利用される被害が発生したことが公表された。
8	他	5日：総務省の情報セキュリティアドバイザーボードより、情報セキュリティの推進にあたって、短期的及び中長期的に講ずべき対策や、既存の取り組みの改善などの方向性について、幅広い観点からの助言をまとめた「総務省における情報セキュリティ政策の推進に関する提言」が公表された。「総務省における情報セキュリティ政策の推進に関する提言」の公表」(http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000044.html)。
9		
10	他	6日：WordPress.comは、google認証システムを利用した二段階認証のオプションに対応したことを発表した。WordPress.com 日本語ブログ、「2段階認証でセキュリティを向上」(http://ja.blog.wordpress.com/2013/04/09/two-step-authentication/)。
11	他	8日：JPCERTコーディネーションセンターは、不正なApacheモジュールが設置されるWeb改ざんが発生している事例について、旧バージョンのParallels Plesk Panelが使われている場合が多いとして、注意喚起を行った。「JPCERT/CC Alert 2013-04-08 旧バージョンの Parallels Plesk Panel の利用に関する注意喚起」(https://www.jpccert.or.jp/at/2013/at130018.html)。
12		
13	脆	10日：Microsoft社は、2013年4月のセキュリティ情報を公開し、MS13-028とMS13-029の2件の緊急とMS13-035を含む7件の重要な更新をリリースした。「2013年4月のセキュリティ情報」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-Apr)。
14	脆	10日：Adobe Flash Playerに、不正終了や、任意のコード実行の可能性のある複数の脆弱性が発見され、修正された。「APSB13-11:Adobe Flash Player用セキュリティアップデート公開」(https://www.adobe.com/jp/support/security/bulletins/apsb13-11.html)。
15	他	10日：各府省庁においてCSIRTなどの体制が整備されたことから、各府省庁CSIRTの代表者(PoC: Point of Contact)で構成する、第1回PoC会合が開催された。内閣官房情報セキュリティセンター、「第1回各府省庁PoC会合の開催について」(http://www.nisc.go.jp/press/pdf/01poc.pdf)。
16	セ	11日：複数の金融機関の偽Webサイトが見つかり、話題となった。この件については、移动通信向けの変換サービスの可能性が指摘されている。例えば、JPCERTコーディネーションセンターのTwitterでは、次のような呼びかけがされた(https://twitter.com/jpcert/status/322282948554530816)。
17	セ	12日：遠隔操作ウイルス事件に関連して、犯人が利用したとされるメールアドレスに、報道機関の記者が複数回に渡り、アクセスしていたことが報道された。
18		
19	セ	15日：ケニアの.keのccTLDレジストラであるFootprint Computer Solutionsが何者かの不正アクセスを受け、GoogleやMSNなど複数の著名なサイトがドメインハイジャックされる事件が発生した。
20	脆	17日：Oracle社は、Java SE JDK及びJREの定例アップデートを公開し、任意のコードが実行可能な脆弱性を含む42件の脆弱性を修正した。「Oracle Java SE Critical Patch Update Advisory - April 2013」(http://www.oracle.com/technetwork/topics/security/javacpuapr2013-1928497.html)。
21	脆	17日：Oracle社は四半期ごとの定例アップデートを公開し、OracleやMySQLなど複数製品の合計86件の脆弱性が修正された。「Oracle Critical Patch Update Advisory -April 2013」(http://www.oracle.com/technetwork/topics/security/cpuapr2013-1899555.html)。
22		
23	他	18日：Microsoft社は、不正アクセスに対するセキュリティ機能向上のため、Microsoftアカウントの二段階認証機能の提供を発表した。The official Microsoft Japan Blog、「Microsoft アカウントのセキュリティを向上」(http://blogs.technet.com/b/microsoft_japan_corporate_blog/archive/2013/04/23/microsoft.aspx)。
24	セ	19日：キルギスタンの.kgのNICが不正アクセスを受け、GoogleやPayPalといった著名なドメインを含む複数のドメインがハイジャックされる事件が発生した。
25	他	19日：インターネットを利用した選挙運動が可能となる改正公職選挙法が参議院で可決し、成立した。
26	セ	23日：宇宙航空研究開発機構(JAXA)は、4月17日にサーバに外部から不正アクセスがあり、国際宇宙ステーションの運用関連の情報が漏えいした可能性があることを公表した。「JAXAのサーバに対する外部からの不正アクセスについて」(http://www.jaxa.jp/press/2013/04/20130423_security_j.html)。
27	セ	23日：オマーンの.omのccTLDレジストラの1つであるOman Telecommunications Companyが侵入され、Googleなど複数の著名なサイトがドメインハイジャックされる事件が発生した。Oman National CERT、「Signs of a DNS Cache Poisoning Attack」(http://www.cert.gov.om/media_news_details.aspx?news=20#UgoN5pJzPkD)。
28		
29	セ	24日：AP通信のTwitterアカウントが何者かに不正アクセスされ、虚偽の情報が配信された。これにより、ニューヨーク株式市場で一時株価が急落するなどの影響が生じた。
30	セ	25日：Torを使用して、他人のIDに不正アクセスし、パスワードやメールアドレスを無断で変更したとして、15歳の少年が不正アクセス禁止法違反容疑で逮捕された。
	セ	28日：日本の政府高官が私用で利用していた外部メールサービスのアカウントが不正アクセスされ、関係者にウイルス付きメールが送信されていたことが報道された。

[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

■ IDとパスワードを狙った攻撃と

なりすましによる不正ログイン

この期間では、ユーザのIDとパスワードを狙った試みと、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の試みが多く発生しました。4月からSNSや通信販売サイト、企業の会員向けサービスサイトなどに対し、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とそれに関連した事件が多く発生しました。このうち、いくつかの事件ではポイントが不正に利用されたり、パスワードの変更が行われるなどの被害も発生しています。

また、脆弱性などを悪用して不正侵入が行われ、サーバからデータが漏えいしたり、ユーザ名やパスワードなどを抽出したファイルが見つかるなど、リストそのものを狙ったと考えられる事件も複数発生しています。このうち、情報流出した事件の1つでは、ユーザIDやパスワードの情報や個人情報と共に、クレジットカードの認証として使われるセキュリティコードも合わせて保存するなど不適切な管理をしていたこと^{*14}から、ユーザだけでなくカード会社などを含め、大きな影響が出ました。

IDやパスワードを狙い、文字列の組み合わせを総当たりで試す攻撃(Brute Force Attack)や、今回の事件のようにリストを使ったと考えられる攻撃については、以前から度々発生していますが、これらの攻撃は個別のサイトに対して行われることが多く、今回のように、国内の複数サイトに対し、大規模な攻撃が行われることは過去にあまり例がありません。更に、ログイン認証のみ確認するなど行為者の意図が不明な事例も発生しています。

今回の事件では、どこからか入手したID/パスワードのリストを使い、他のサイトで同一の組み合わせで利用しているユーザを狙い、攻撃を行っていたと考えられます^{*15}。

このような、複数のWebサイトで同一のIDとパスワードを利用することのリスクについては、以前から指摘されており、例えば、2012年に警察庁が公表した「連続自動入力プログラムによる不正ログイン攻撃の観測結果について」では、調査の結果、ユーザの6.7%でいわゆる使い回しをしていたことが確認されています^{*16}。IDとパスワードの使い回しの危険性については度々指摘されていますが、今回の事件を受け、一般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から改めて注意喚起が行われています^{*17}。

この事件の詳細については「1.4.3 頻発する不正ログイン事件」も併せてご参照ください。

■ TLDへの攻撃

ccTLDを含むドメインレジストリに対しての攻撃と、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。4月には、ケニアのドメインである.keを管理しているccTLDレジストラであるFootprint Computer Solutionsが何者かの不正アクセスを受け、GoogleやMSNなど複数の著名なサイトがドメインハイジャックされる事件が発生しています。また、キルギスタンのドメインである.kgのNICでも不正アクセスを受け、GoogleやPayPalといった著名なドメインを含む複数のドメインがハイジャックされる事件が発生しました。更に、オマーンのドメインである.omのccTLDレジストラの1つであるOman Telecommunications Companyでも不正アクセスが行われ、Googleなど複数の著名なサイトがドメインハイジャックされる事件が発生しています。これ以外にも、ウガンダのドメインである.ugや、ブルンジのドメインである.biなどのドメインでもドメインハイジャックされる事件が発生しています。いずれの事件でもドメインハイジャックされた場合には、GoogleやPayPalなどの世界的に著名な企業のドメインが狙われました。

*14 例えば、JIPDECで公表している「クレジット加盟店向け「情報セキュリティのためのガイド」(PCI DSS / ISMS準拠のためのガイド)」(<http://www.isms.jipdec.or.jp/doc/JIP-ISMS118-20.pdf>)を確認すると、PCI DSSの要件3でセンシティブ認証データにセキュリティコードが含まれており、加盟店で保存を禁止していることが確認できる。

*15 被害を受けた企業の1つでは、最終報告の中で1つのログインIDについて試行するパスワードの数が少ないことから他サービスのログインIDとパスワードを不正に入手して適用可否を試行したとの見解を示している。

*16 警察庁、「平成23年中の不正アクセス行為の発生状況等の公表について」(<http://www.npa.go.jp/cyber/statics/h23/pdf040.pdf>)。

*17 一般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、「【注意喚起】ユーザID/パスワードの不正利用の多発、および、利用者への推奨対策」(<https://www.telecom-isac.jp/news/news20130412.html>)。

5月のインシデント

1	セ	1日: トロント大学のCitizen Labより、各国の政府機関が情報収集活動に利用しているとされる商用監視ソフトウェアFinSpy (FinFisher) についての最新レポートが公開された。
2		詳細については、次のCitizen Labのレポートを参照のこと。"For Their Eyes Only: The Commercialization of Digital Spying" (https://citizenlab.org/2013/04/for-their-eyes-only-2/)。
3	脆	4日: Microsoft社は、IE8における未修正の脆弱性 (CVE-2013-1347) があり、悪意のあるWebサイトを参照した場合、リモートでコードが実行される可能性があるとして、セキュリティ アドバイザリ (2847140) を公開した。この脆弱性については、5月15日にMS13-038で修正された。
4		「マイクロソフト セキュリティ アドバイザリ (2847140) 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/2847140)。
5	セ	8日: Anonymousにより、米国の政府機関や金融機関のサイトなど数百のWebサイトが改ざんされたり、情報漏えいやDDoS攻撃が行われた (OpUSA)。攻撃対象など、攻撃の詳細については、次のPastebinの予告で確認できる。"#OpUSA target list" (http://pastebin.com/LXHkjsfg)。
6		8日: 通信販売サイトで不正ログインの試みが発生し、5月4日から5月8日にかけて約111万件の不正なアクセスがあり、うち約15,000アカウントで不正なログインを確認したとして、該当ユーザのログインロックを行ったことを公表した。これについては、5月16日に追加情報を公表し、他社サービスから入手したID/パスワードのリストを使っていることが推測されることから、パスワードの使い回しを行わないよう注意喚起を行っている。
7	セ	10日: インドのクレジットカード処理会社に不正侵入し、預金や引出し上限のデータを改ざんし、世界中のATMから45億ドルを盗んだハッカーグループ8人が起訴された (Unlimited Operation)。
8		この事件についての詳細は、次のUnited States Attorney's Office for the Eastern District of New Yorkの発表に詳しい。"Eight Members Of New York Cell Of Cybercrime Organization Indicted In \$45 Million Cybercrime Campaign" (http://www.justice.gov/usao/nye/pr/2013/2013may09.html)。
9	他	11日: Bloomberg L.P.社は、Bloomberg Newsの記者が、別部門である金融情報提供サービスを利用している顧客のデータに不適切なアクセスが可能であったことを認め、是正措置を行ったことを公表した。
10		詳細については、次のBloomberg L.P.社からの発表などで確認できる。"Safeguarding Customer Data" (http://blog.bloomberg.com/2013-05-10/safeguarding-customer-data/)。
11	脆	15日: Microsoft社は、2013年5月のセキュリティ情報を公開し、MS13-037とMS13-038の2件の緊急とMS13-039を含む8件の重要な更新をリリースした。
12		「2013年5月のセキュリティ情報」 (http://technet.microsoft.com/ja-jp/security/bulletin/ms13-May)。
13	脆	15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。
14		「APSB13-14: Adobe Flash Player用のセキュリティアップデート公開」 (http://www.adobe.com/jp/support/security/bulletins/apsb13-14.html)。
15	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。
16		「APSB13-15: Adobe Reader および Acrobat に関するセキュリティアップデート公開」 (http://www.adobe.com/jp/support/security/bulletins/apsb13-15.html)。
17	セ	17日: Yahoo! JAPANは、5月16日にYahoo! JAPAN IDを管理しているサーバに外部からの不正アクセスがあり、最大2,200万件のIDのみが抽出されたファイルが作成され、流出した可能性があることを公表した。その後、5月23日に約148万件については、不可逆暗号化されたパスワード、パスワードを忘れてしまった場合の再設定に必要な情報の一部が流出した可能性があることを追加で公表している。
18		ヤフー株式会社、「当社サーバへの不正なアクセスについて」 (http://pr.yahoo.co.jp/release/2013/0517a.html)。『「当社サーバへの不正なアクセスについて」(5/17発表)の追加発表』 (http://pr.yahoo.co.jp/release/2013/0523a.html)。
19	脆	23日: Apache Strutsに、任意のコマンド実行が可能な複数の脆弱性 (CVE-2013-1965, CVE-2013-1966) が見つかり、修正された。
20		The Apache Software Foundation, "S2-014? A vulnerability introduced by forcing parameter inclusion in the URL and Anchor Tag allows remote command execution, session access and manipulation and XSS attacks" (http://struts.apache.org/release/2.3.x/docs/s2-014.html)。
21	他	24日: 「行政手続における特定の個人を識別するための番号の利用などに関する法律 (マイナンバー法)」が参議院で可決し、成立した。
22		詳細については、次の内閣官房のホームページで確認できる。『社会保障・税番号制度』 (http://www.cas.go.jp/jp/seisaku/bangoseido/)。
23	脆	27日: Apache Strutsに、任意のコマンド実行が可能な複数の脆弱性 (CVE-2013-1966, CVE-2013-2115) が見つかり、修正された。なお、CVE-2013-1966は前回修正されていたが、対策が不完全であることから再修正されている。
24		27日: 海外旅行者向けに携帯電話やモバイルWi-Fiルータのレンタルを行っている事業者のWebサイトが、4月23日に不正アクセスを受け、最大146,701件のセキュリティコードなどのクレジットカード情報を含む顧客情報が漏えいしたことを公表した。
25	セ	31日: DDoS対策サービスを提供している米国Prolexic Technologies社は、金融取引市場システムに対する167GbpsのDNSアンブによるDDoS攻撃を防いだことを公表した。この攻撃では、攻撃に参加した機器の92%がOpen Resolverだったとしている。
26		"167 Gbps Attack Targeted Real-Time Financial Exchange Platform" (http://www.prolexic.com/news-events-pr-prolexic-stops-largest-ever-dns-reflection-ddos-attack-167-gbps.html)。
27	セ	31日: マラウィのドメインレジストリであるnic.mwやregister.mwのWebサイトが何者かに改ざんされた。
28		

[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

DNSレジストラの1つである米国Monikerは、不正アクセスを受け、クレジットカード情報を含む顧客情報にアクセスされた可能性があるとして、全顧客のアカウントのパスワードをリセットする対応を行っています。DNSホスティングプロバイダの1つである米国name.comでも不正アクセスを受け、顧客情報にアクセスされた可能性があるとして、全顧客のパスワードをリセットする対応が行われました^{*18}。マラウィのドメインである.mwを管理しているドメインレジストリのnic.mwやregister.mwといったWebサイトが何者かに改ざんされる事件も発生しています。

6月には、複数のDNSホスティングサービス事業者に対して、その権威DNSサーバへのDDoS攻撃が発生し、サービスが停止するなどの影響が出る事件が発生しましたが、この攻撃はこれらサービス事業者の権威DNSサーバを利用したDNSアンプによる他サーバへのDDoS攻撃だったことが判明しています^{*19}。また、同じく6月には、米国Network Solutions社で、DDoS攻撃対応時のオペレーションミスにより、約5,000のドメインがドメインハイジャックされたように見える事故が発生しました^{*20}。

■ Bitcoinへの攻撃

この期間では、ネット上の仮想通貨であるBitcoinとそのシステムに対する攻撃が複数発生し話題となりました。Bitcoinは4月に通貨との交換レートが最高で\$266を記録するなど、その価値が上昇していました。これに伴い、Bitcoinを狙った攻撃やフィッシングなどが多く発生しています。4月3日にはBitcoinの取引所の1つであるMt.GoxがDDoS攻撃を受け、一時的にサービスに影響が出る被害を受けています^{*21}。また、Bitcoinの採掘を行うマルウェアが確認される^{*22}など、間接的にBitcoinを狙った攻撃も増加してきています。Bitcoinは匿名のまま仮想通貨のやりと

りできるため、WikiLeaksへの寄付などに使われるなど、名前を明かさずに利用できるメリットがありますが、一方で、犯罪などのマネーロンダリングに使われる可能性などの問題も指摘されており、その利用には注意が必要です。

■ 政府機関の取り組み

政府機関の動きでは、情報セキュリティ政策会議にて、2010年度に策定された「国民を守る情報セキュリティ戦略」に代わる情報セキュリティに関する新たな基本戦略として、策定が進められていた「サイバーセキュリティ戦略」が決定しました^{*23}。また、推進体制の強化のため、NISCについては必要な機能強化を図り、2015年度を目途として「サイバーセキュリティセンター（仮称）」とすることなどが決定しました。更に、これに基づき、政府機関における緊急対応能力の向上や、攻撃への解析機能の整備、国際協調も含めた連携機能の強化、人材育成やリテラシー向上など、2013年度に実施する具体的な取り組みを年次計画としてまとめた「サイバーセキュリティ 2013」が決定しています^{*24}。

また、4月1日には政府機関や民間企業を狙ったサイバー攻撃の増加を受け、13の都道府県でサイバー攻撃特別捜査隊が発足しました。6月には更なる捜査の効率化を図るため、警視庁生活安全部サイバー犯罪対策課に警視庁の捜査員及び道府県警察から派遣される捜査員によって編成されたサイバー犯罪特別対処班が、7月に新設されることが発表されました。5月には防衛省でも、防衛省・自衛隊のシステム及びネットワークに対するサイバー攻撃への対処を統合的に実施する能力を強化するため、サイバー空間防衛隊（仮称）を新設することが発表されるなど、サイバー攻撃への対応体制の強化が行われています。更に、外交・安全保障政策を立案する国家安全保障会議（いわゆる日本版NSC）の設置については、国家安全保障会議の創設に関する有識者会

*18 Name.com Blog, "We got hacked" (<http://www.name.com/blog/general/2013/05/we-got-hacked/>)。

*19 攻撃の詳細については、次の攻撃を受けた事業者の1つであるDNSimple社のblogに詳しい。"Incident Report: DNS Outage due to DDoS Attack" (<http://blog.dnsimple.com/incident-report-dns-outage-due-to-ddos-attack/>)。

*20 詳細については、次のCisco Blogに詳しい。"Hijacking" of DNS Records from Network Solutions" (<http://blogs.cisco.com/security/hijacking-of-dns-records-from-network-solutions/>)。

*21 この事件については、次のMt.Gox社の発表を参照のこと。"It's been an epic few days: What happened?" (https://www.mtgox.com/press_release_20130404.html)。

*22 このマルウェアの詳細については、例えば次のKaspersky Lab社のSECURELIST BLOGなどを参照のこと。"Skypemageddon by bitcoining" (http://www.securelist.com/en/blog/208194210/Skypemageddon_by_bitcoining)。

*23 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>)。

*24 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>)。

6月のインシデント

1	セ	4日:DNSimpleやeasyDNSなど、複数のDNSホスティングサービスの権威DNSサーバに対し、DDoS攻撃が発生しサービスが停止するなどの影響が出た。詳細については、例えば次の攻撃先の1つとなったTPP Wholesale Pty Ltdのアナウンスなどで確認できる。"Unscheduled Service Interruption? TPP Wholesale DNS? 3rd June 2013" (http://www.tppwholesale.com.au/support/service-alerts/unscheduled-service-interruption-tpp-wholesale-dns-3rd-june-2013)。"More information on recent DDoS attacks? June 2013" (http://www.tppwholesale.com.au/support/service-alerts/more-information-recent-ddos-attacks)。
2		
3	脆	5日: BIND 9.xに特定のデータにより、外部からサービス停止可能な脆弱性(CVE-2013-3919)が見つかり、修正された。 Internet Systems Consortium, "CVE-2013-3919: A recursive resolver can be crashed by a query for a malformed zone" (https://kb.isc.org/article/AA-00967/)。
4	脆	5日: Apache Strutsに、任意のコマンド実行が可能な複数の脆弱性(CVE-2013-2134, CVE-2013-2135)が見つかり、修正された。 The Apache Software Foundation, "S2-015? A vulnerability introduced by wildcard matching mechanism or double evaluation of OGNL Expression allows remote command execution." (http://struts.apache.org/release/2.3.x/docs/s2-015.html)。
5		
6	脆	6日: Parallels Plesk Panel versions 9.0 - 9.2.3に、リモートで任意のコード実行が可能な脆弱性がセキュリティ関連のメーリングリストに発表された。この脆弱性は既にサポートが終了している古いバージョンでのみ影響があるため、バージョンアップを行うよう呼びかけている。 Parallels社, 「Parallels Plesk Panel: phppath/PHPの脆弱性」 (http://kb.parallels.com/jp/116241)。
7	セ	6日: Microsoft社は、FBIやFS-ISACなど複数のパートナーと共同で「Citadel」ボットネットの摘発を行ったことを公表した。 "Microsoft, financial services and others join forces to combat massive cybercrime ring" (http://www.microsoft.com/en-us/news/Press/2013/Jun13/06-05DCUPR.aspx)。
8		
9	他	7日: JPCERT/CCより、国内でWebサイト改ざんのインシデントが多く発生しているとして、注意喚起が行われた。2013年4月以降、約1,000件報告されており、改ざんされたWebサイトの多くが攻撃サイトへの誘導に使われているとしている。 「JPCERT/CC Alert 2013-06-07 Web サイト改ざんに関する注意喚起」 (https://www.jpCERT.or.jp/at/2013/at130027.html)。
10	脆	12日: Microsoft社は、2013年6月のセキュリティ情報を公開し、MS13-047の1件の緊急とMS13-051など、4件の重要な更新をリリースした。 「2013年6月のセキュリティ情報」 (http://technet.microsoft.com/ja-jp/security/bulletin/ms13-Jun)。
11	他	12日: 個人に関する情報(パーソナルデータ)を含む大量の情報(ビッグデータ)の適切な利用と、プライバシーに配慮した利便性の高いサービスを提供するために必要な情報の流通について、検討した結果をまとめた報告書が、総務省のパーソナルデータの利用・流通に関する研究会より公表された。 「『パーソナルデータの利用・流通に関する研究会』報告書の公表」 (http://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000071.html)。
12	脆	13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。 「APSB13-16: Adobe Flash Player用セキュリティアップデート公開」 (http://helpx.adobe.com/jp/flash-player/kb/cq60101845.html)。
13	他	14日: 米国ICS-CERTは、40ベンダーの約300の医療機器について、ハードコーディングされたパスワードが使われているとして、適切な管理とアクセス制限を行うよう注意喚起を行った。 "Alert (ICS-ALERT-13-164-01) Medical Devices Hard-Coded Passwords" (http://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01)。
14		
15	脆	18日: 一太郎に、任意のコード実行が可能な脆弱性が見つかり、修正された。 *株式会社ジャストシステム, 「[JS13002] 一太郎の脆弱性を悪用した不正なプログラムの実行危険性について」 (http://www.justsystems.com/jp/info/js13002.html)。
16	セ	18日: オランダとベルギーの複数機関の合同捜査により、アントワープの港湾システムに侵入し、武器や麻薬を密輸していたグループが検挙されたことが公表された。この事件については、次のオランダ検察の発表に詳しい。"Drugshandelaren hacken rederijen en onvreemde containers met coca?ne" (http://www.om.nl/actueel/nieuws-persberichten/@161061/drugshandelaren/) (オランダ語)。
17	脆	19日: Oracle社は、Java SE JDK及びJREの四半期ごとの定例アップデートを公開し、任意のコードが実行可能な脆弱性を含む40件の脆弱性を修正した。 "Oracle Java SE Critical Patch Update Advisory - June 2013" (http://www.oracle.com/technetwork/topics/security/javacpujun2013-1899847.html)。
18	脆	19日: Google ChromeのFlashプラグインに、Flashアプリケーションで適切な権限管理がされておらず、第三者により、クリックジャッキング攻撃などを介し、マシンの物理的環境から重要な情報を取得される可能性のある脆弱性が見つかり、修正された。 "Stable Channel Update" (http://googlechromereleases.blogspot.jp/2013/06/stable-channel-update_18.html)。
19		
20	セ	19日: Opera社は、標的型攻撃により侵入され、コードサイン証明書が盗まれたことを6月26日に公表した。日本時間10時から10時36分の間に不正な証明書を利用して更新ファイルが自動更新の仕組みを利用して配布されたことで、数千人のWindowsユーザが影響を受けた可能性あることも併せて公表している。 The Opera Security group, "Security breach stopped" (http://my.opera.com/securitygroup/blog/2013/06/26/opera-infrastructure-attack)。
21	セ	21日: 米国Network Solutions社で、DDoS攻撃対応時のオペレーションミスにより、約5,000のドメインがドメインハイジャックされたかに見える事故が発生した。Network Solutions社の公式な発表は次の"Important Update for Network Solutions Customers Experiencing Website Issues" (https://www.networksolutions.com/blog/2013/06/important-update-for-network-solutions-customers-experiencing-website-issues/)を参照のこと。事件の詳細については次のCisco Blogに詳しい。"Hijacking" of DNS Records from Network Solutions" (http://blogs.cisco.com/security/hijacking-of-dns-records-from-network-solutions/)。
22	脆	22日: FacebookのDownload Your Information toolに一部ユーザの連絡先情報が意図せず露出する脆弱性があり、修正された。 "Important Message from Facebook's White Hat Program" (https://www.facebook.com/notes/facebook-security/important-message-from-facebooks-white-hat-program/10151437074840766)。
23	脆	22日: WordPressで、攻撃者がサイトへのアクセスを得られる可能性を持つサーバーサイドのリクエストフォージェリへの修正を含む12件の脆弱性を修正された。 WordPress.com 日本語ブログ, 「WordPress 3.5.2 メンテナンス & セキュリティリリース」 (http://ja.wordpress.org/2013/06/22/wordpress-3-5-2/)。
24	セ	25日: 複数の報道関係者が、遠隔操作ウイルス事件に関連して事件に利用された犯人のものとされるメールアドレスにアクセスしたとして、書類送検された。
25	セ	25日: 韓国で複数の政府系Webサイトや企業のWebサイトの改ざん、DDoS攻撃などが発生した。また、マルウェアによると考えられるシステム停止についても併せて複数発生した。 詳細については例えば次のTrend Micro SECURITY BLOGに詳しい。"再び起こった韓国への大規模サイバー攻撃: 何があったのか? 我が国が得るべき教訓は?" (http://blog.trendmicro.co.jp/archives/7462)。
26		
27	他	28日: Adobe社は、「サイバー攻撃対策」の一環として、「地方公共団体組織認証基盤(LGPKI)」のPDFへの電子署名の取り組みに対し、Adobe Reader及びAcrobatでLGPKIの電子署名を簡単に検証できる仕組みを整えたことを公表した。 「アドビシステムズ、財団法人 地方自治情報センターの「サイバー攻撃」対策に協力」 (http://www.adobe.com/jp/aboutadobe/pressroom/pressreleases/20130628_LGPKI.html)。
28		
29		
30		

[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

議^{*25}を経て、国家安全保障会議設置関連法案が閣議決定されています。

■ その他

4月には、インターネットを利用した選挙運動が可能となる改正公職選挙法が可決し、成立しています。これにより、候補者や政党がFacebookやTwitterなどのインターネットを利用した選挙活動が可能となりました。一方で、電子メールで選挙活動を行うことは禁止するなど、有権者がインターネットで活動するには一定の制限もあるため、注意が必要となります^{*26}。

昨年の10月より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は、2月に逮捕された容疑者に対する捜査が進められ、7つの事件に対して偽計業務妨害などの罪で起訴され、捜査が終了しました。また、これに関連して、昨年10月に遠隔操作ウイルス事件で利用された犯人のものとなるメールアドレスにアクセスしていたとして、複数の報道関係者が書類送検されています。

6月には、英国の新聞社が掲載した、米国国家安全保障局(NSA)の活動に関する記事について話題となりました。NSAでは以前から、テロ関連の情報収集活動を行っていま

したが、この対象に米国国民も含まれていることや、電話の通話記録の収集と共に、PRISMと呼ばれるインターネット上の動画や写真、電子メールなどのデータを監視するプログラムが米国の主要なインターネット関連企業の協力の下、運用されていたことなどが報道されました。このため、関連を指摘された複数の企業で、法律に基づくデータの受け渡しであったとする説明や、政府機関からのデータの開示要求の件数を公開するなどの対応が行われました。また、NSAの情報収集活動には、インターネットトラフィックを伝送する光ケーブルネットワークの傍受や、国際会議などでも情報収集活動が行われていた可能性が指摘されるなどの報道がされ、米国だけでなくEUも含めた世界各国で、活動に対する非難が起り、外交への影響が懸念されています。

韓国では、6月25日に複数の政府系Webサイトや企業のWebサイトが改ざんされたり、DNSサーバに対するDDoS攻撃などの事件が発生しました。この事件では、複数の攻撃者による攻撃が同時に行われたと考えられており、Anonymousによると考えられるWeb改ざんなどと共に、マルウェアによると考えられるシステム停止も複数発生しました。また、攻撃の傾向が似ていることから、3月に発生した3.20大乱との関連も疑われています^{*27}。

*25 首相官邸、「国家安全保障会議の創設に関する有識者会議」(http://www.kantei.go.jp/jp/singi/ka_yusiki/)。

*26 法改正に伴う選挙運動については、例えば次の総務省の「インターネット選挙運動の解禁に関する情報」(http://www.soumu.go.jp/senkyo/senkyo_s/naruhodo/naruhodo10.html)などで確認できる。

*27 この事件でも、使われたマルウェアには決められた時間に攻撃を開始するなど、複数の機能に共通点が見られる。マルウェアの動作については、例えば、次のSymantec社のセキュリティレスポンスブログに詳しい。「韓国に対して4年間続いたDarkSeoulのサイバー攻撃、朝鮮戦争の開戦記念日にも続く」(<http://www.symantec.com/connect/ja/blogs/4-darkseoul>)。

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、2013年4月から6月の期間にIJ 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、IJ 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。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、その影響度合いが異なります。図-2では、DDoS攻撃全体を、回線容量に対する攻撃^{*28}、サーバに対する攻撃^{*29}、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か月間でIJは、514件のDDoS攻撃に対処しました。1日あたりの対処件数は5.65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ています。DDoS攻撃全体に占める割合は、サーバに対する攻撃が98.1%、複合攻撃が1.9%、回線容量に対する攻撃はありませんでした。

今回の対象期間に観測された中で最大規模な攻撃は、サーバに対する攻撃に分類したもので、最大5万5,000ppsのパケットによって295Mbps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78.8%が攻撃開始から30分未満で終了し、21%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も0.2%ありました。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、2日と6時間37分(54時間37分)にわたりました。

攻撃元の分布としては、多くの場合、国内外を問わず、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^{*30}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^{*31}の利用によるものと考えられます。

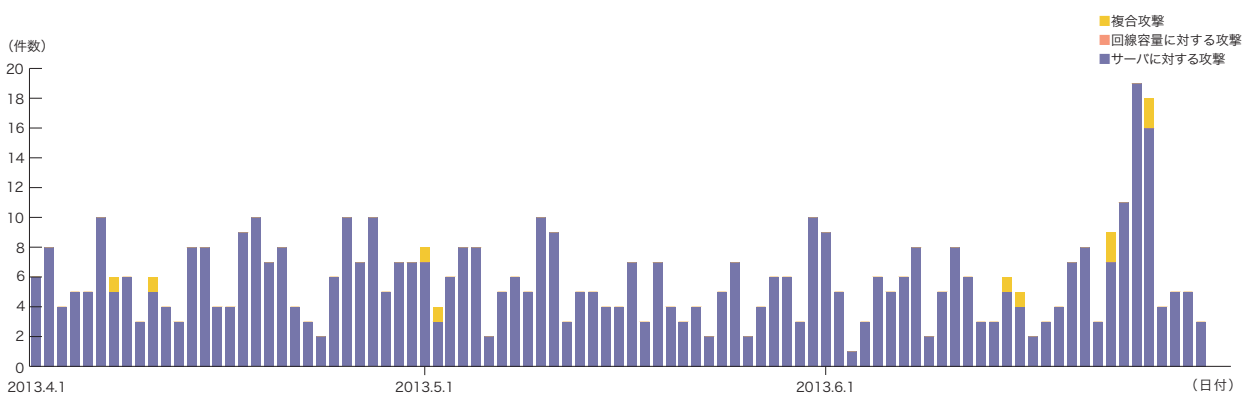


図-2 DDoS攻撃の発生件数

*28 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。

*29 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接続を確立したのち、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。

*30 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。

*31 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^{*32}によるDDoS攻撃のbackscatter観測結果を示します^{*33}。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。

2013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51.8%を占めています。また、DNSで利用されている53/TCPや、SSHで利用されている22/TCP

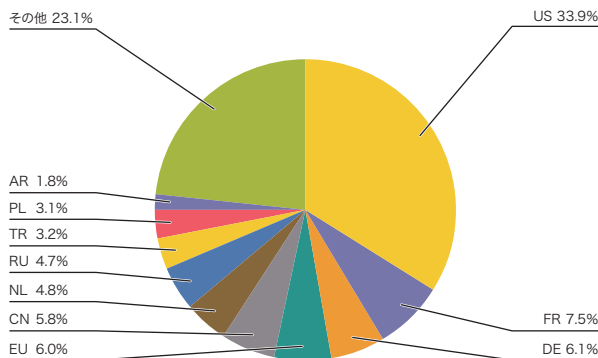


図-3 backscatter観測によるDDoS攻撃対象の分布
(国別分布、全期間)

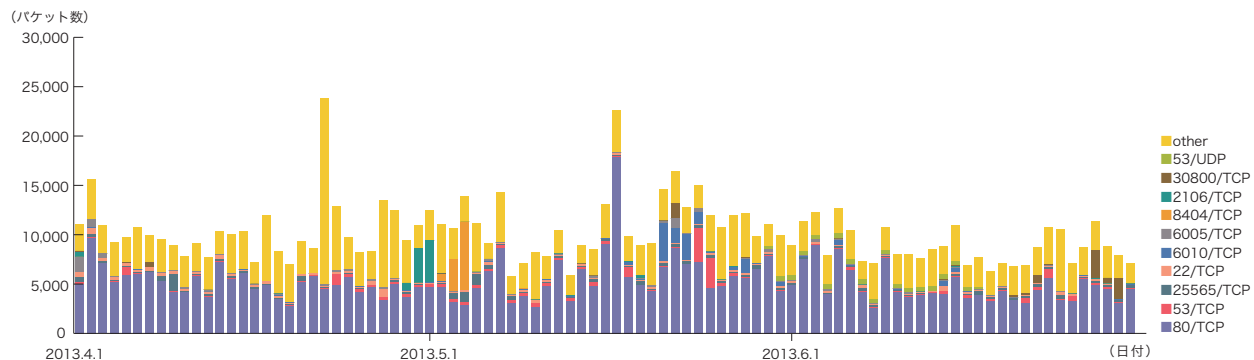


図-4 DDoS攻撃によるbackscatter観測(観測パケット数、ポート別推移)

*32 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。「1.3.2 マルウェアの活動」も参照。

*33 この観測手法については、IIR Vol.8(http://www.ijj.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。

などへの攻撃やゲーム関連と考えられる25565/TCP、通常は利用されない6010/TCPや6005/TCPなどの攻撃が観測されています。

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見ると、まず、Webサーバ(80/TCP)への攻撃としては、4月2日に複数のWebサーバからのbackscatterを観測しており、カナダの科学関連サイトと米国のホスティング事業者のWebサーバへの攻撃を観測しています。5月17日にも、別の米国のホスティング事業者のWebサーバへの攻撃が確認されています。6月3日には、ドイツのセキュリティ事業者のWebサーバへの攻撃を観測しています。6月5日には、米国のホスティング事業者のWebサーバ、中国の通信販売事業者のWebサーバへの攻撃を観測しています。

SSH(22/TCP)に対する攻撃も多く発生しており、スイスのホスティング事業者や、米国のホスティング事業者、オランダのホスティング事業者のサーバに対する攻撃を観測しています。ゲーム関連と考えられる25565/TCPへの攻撃については、米国の複数のホスティング事業者に対して観測されました。

4月30日から5月1日にかけては、米国のホスティング事業者に対する2106/TCPへの攻撃が多く観測されました。5月21日から5月30日にかけては、オランダのホスティング事業者のサーバに対する6010/TCPへの攻撃が観測されています。これらの攻撃は特定の日に多いという

訳ではなく、継続して攻撃を観測しており、この期間の合計で1万回以上観測されています。これらのポートは通常のアプリケーションで利用するポートではないため、それぞれの攻撃の意図は不明です。また、今回の対象期間中に話題となったDDoS攻撃のうち、IJJのbackscatter観測で検知した攻撃としては、4月に発生したAnonymousによると考えられる北朝鮮関連サイトへの攻撃、5月に発生した米国の政府機関や金融機関への攻撃、6月に発生した複数のスウェーデン政府機関への攻撃を観測しています。また、イスラエルの情報機関への攻撃、5月から6月にかけて米国の著名なセキュリティ専門家のWebサイトへの攻撃、米国の過激な行動を行う宗教団体への攻撃やMITに対する攻撃によると考えられるBackscatter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、IJJが実施しているマルウェアの活動観測プロジェクトMITF*34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

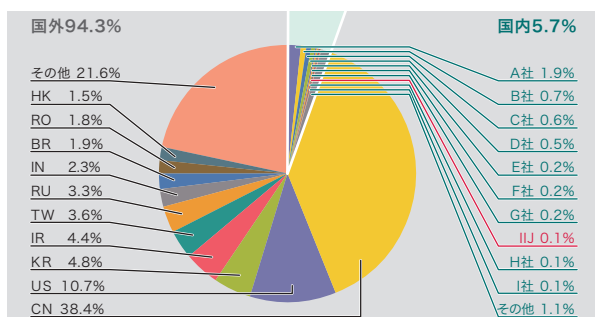


図-5 発信元の分布(国別分類、全期間)

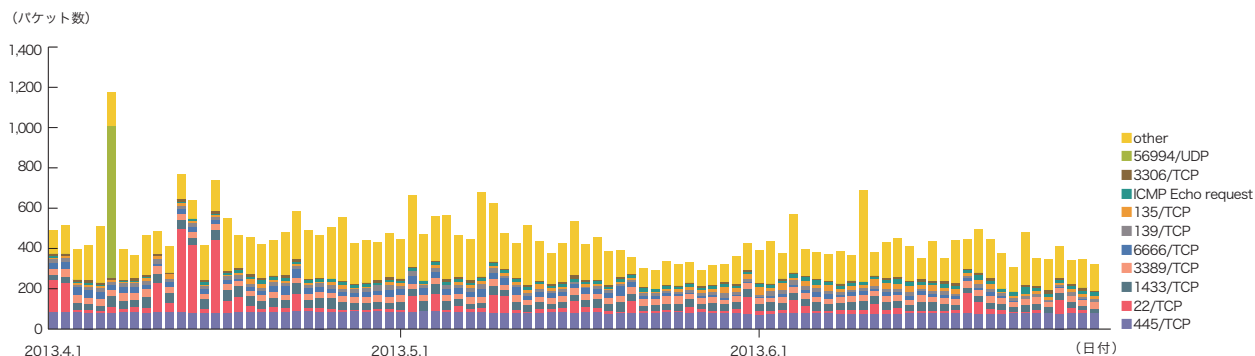


図-6 ハニーポットに到着した通信の推移(日別・宛先ポート別・1台あたり)

ト*35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。

■ 無作為通信の状況

2013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、MySQLで使用される3306/TCP、ICMP Echo Requestによる探索行為も観測されています。これらに加えて、6666/TCPや56994/UDPなど、一般的なアプリケーションでは利用されない、目的が不明な通信も観測されました。

期間中、SSHの辞書攻撃と思われる通信も発生しており、例えば4月12日はインド、中国、韓国、4月13日は韓国、中

*34 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。

*35 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て、攻撃者の行為やマルウェアの活動目的を記録する装置。

国、4月15日は韓国に割り当てられたIPアドレスからそれぞれ集中的に通信が発生しています。また、4月6日にはイランに割り当てられた1つの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、56994/UDP宛での通信が発生しています。データ長、データ共にランダムであったため、

その目的は不明です。4月下旬から5月中旬にかけて、主に中国、米国から広域のハニーポットのIPアドレスに対し、6666/TCPから6675/TCPの通信が増加したことを確認しました。6667/TCPはIRCに用いられるポートですが、一部のIRCではこの周辺のポートも使用しているため、その調査行為であると考えられます。

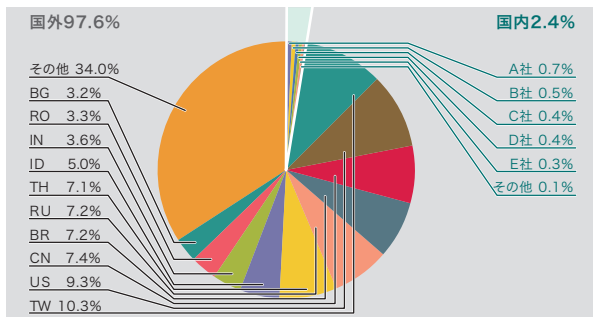


図-7 検体取得元の分布(国別分類、全期間、Confickerを除く)

■ ネットワーク上でのマルウェアの活動

同じ期間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^{*36}の総数を総取得検体数、検体の種類をハッシュ値^{*37}分類したものをユニーク検体数としています。

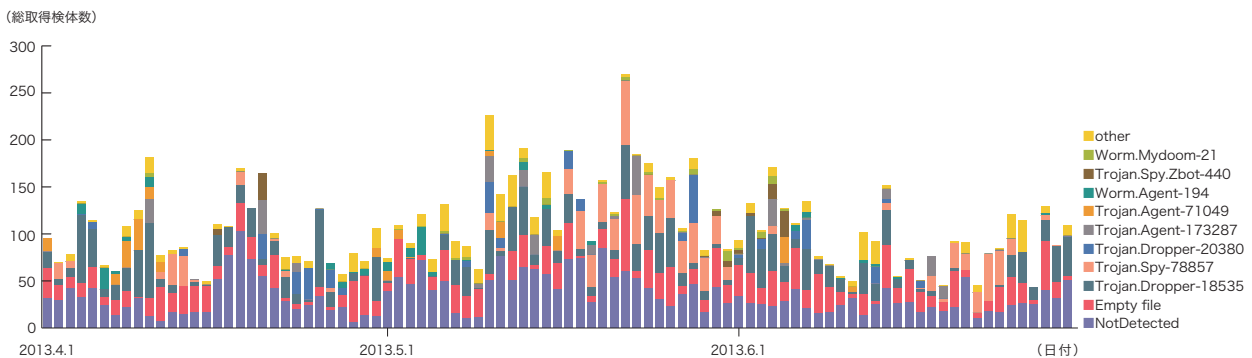


図-8 総取得検体数の推移(Confickerを除く)

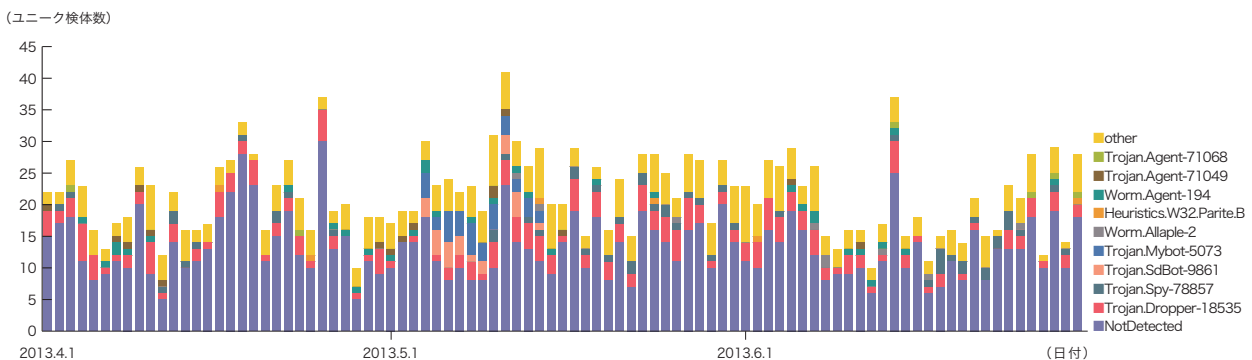


図-9 ユニーク検体数の推移(Confickerを除く)

*36 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。

*37 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。

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109、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、4月にはタイ、インドネシアやフィリピンでアカウントを盗み出すマルウェア^{*38}、5月、6月に同様の国でIRCサーバで制御されるタイプのボット2種類^{*39*40}、4月前半と6月後半に米国とフランスで米国、香港に割り当てられたIPアドレスからのワーム^{*41}も継続的に観測されました。

MITFの独自の解析では、今回の調査期間中に取得した検体は、ワーム型40.4%、ボット型53.2%、ダウンロード型6.4%でした。また解析により、120個のボットネットC&Cサーバ^{*42}と15個のマルウェア配布サイトの存在を確認しました。C&Cサーバの数が前号より大幅に増加していますが、これはDGA(Domain Generation Algorithm)^{*43}機能

を持つ1種類のマルウェアが存在したためです。このマルウェアが生成するドメインは「www.ランダムな英字6文字.com」であることがIJの解析から分かっています。

■ 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33,250、ユニーク検体数は791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、前回の対象期間中と比較し、約13%増加しています。また、ユニーク検体数は前号から約2%減少しました。Conficker Working Groupの観測記録^{*44}によると、2013年6月30日現在で、ユニークIPアドレスの総数は1,312,964とされています。2011年11月の約320万台と比較すると、約41%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。

*38 Trojan:Win32/Neurevt.A (<http://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Trojan%3AWin32%2FNeurevt.A>)。

*39 Trojan:Win32/Ircbrute (<http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?name=Trojan%3AWin32%2FIrcbrute>)。

*40 Win32/Hamweq (<http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fHamweq>)。

*41 WORM_DEBORM.AP (http://about-threats.trendmicro.com/Malware.aspx?id=36201&name=WORM_DEBORM.AP&language=au)。

*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 DGA(Domain Generation Algorithm)とは、時刻など、ある一定の規則を基に接続するC&Cサーバのドメイン名をマルウェアが自動生成する仕組み。URLフィルタリング装置を回避したり、接続中のC&Cサーバが停止させられても新たに生成したドメイン名に再接続することで、復帰し、活動を継続できるようにするために利用する。

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

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^{*45}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。

2013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、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。

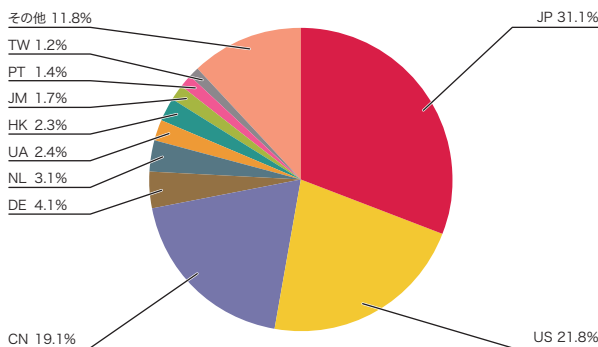


図-10 SQLインジェクション攻撃の発信元の分布

発信元の分布では、日本31.1%、米国21.8%、中国19.1%となり、以下その他の国が続いています。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、減少しています。中国からの攻撃が3位と上昇していますが、これは特定の攻撃先への大規模な攻撃が一部の日に発生したことによります。

この期間中、5月1日から2日にかけて米国やオランダなど複数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。5月2日には他にも米国の特定の攻撃元より、特定の攻撃先に対する攻撃が発生していました。4月19日には中国の特定の攻撃元から特定の攻撃先に対する攻撃、6月3日には中国の複数の攻撃元から同じ特定の攻撃先に対する攻撃、6月9日にはTorからと考えられる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す。また、6月27日には中国の特定の攻撃元より、複数の攻撃先への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。

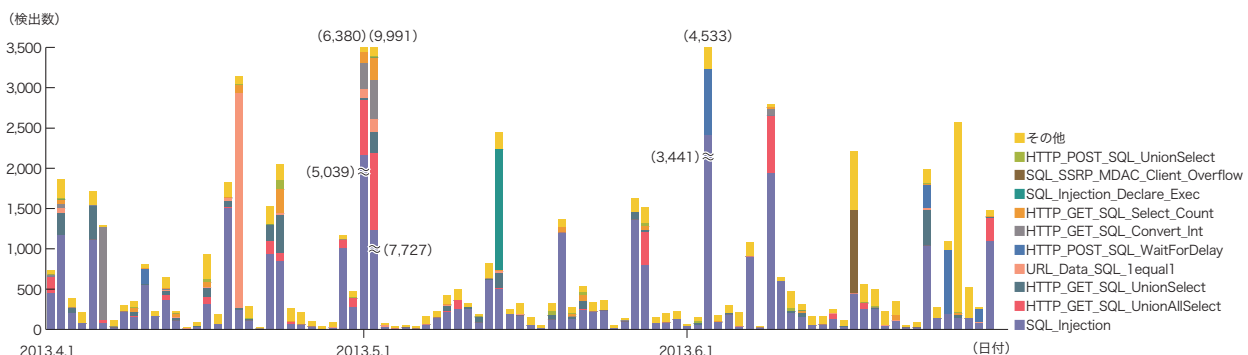


図-11 SQLインジェクション攻撃の推移(日別、攻撃種類別)

*45 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。

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、マルウェアZeroAccessの検出手法の検討、ホームルータを悪用される可能性とそのリスクについて、頻発する不正ログインについての3つのテーマについて紹介します。

1.4.1 ZeroAccessとそのIOCに関する考察

ZeroAccessは2009年頃から観測され始めたボット型マルウェアです。昨年9月、Sophos社はZeroAccessに関しての解析レポートを公開しました^{*46}。レポートでは、その当時までに世界中で900万台の端末がZeroAccessに感染していたことや、国別の感染ノード割合などが示され

ており、日本においても多数の端末が当時感染していたことが窺えます。その目的は、主に感染端末上でのクリック詐欺やBitcoinのマイニングによる金銭の搾取ですが、SpyEyeやZeuS亜種^{*47}と同様に、ZeroAccessもプラグインDLLの実行機能を備えているため、今後は新たな機能が搭載されてくる可能性があります。

本節では、IJが解析したZeroAccessの最近の亜種の動作を説明すると共に、それを感染端末から検出するためのIOC (Indicator of Compromise)^{*48}についての知見を述べます。

■ ユーザモード型ZeroAccessの動作

ZeroAccessは多くの場合、BlackholeをはじめとするExploit Kit^{*49}のドライブバイダウンロード^{*50}や、偽のクラック版ソフトウェアなどとして配布するソーシャルエンジニアリング的な手口によってインストールされます。ZeroAccessの近年の亜種は、P2Pでボットネットを構成したり、ユー

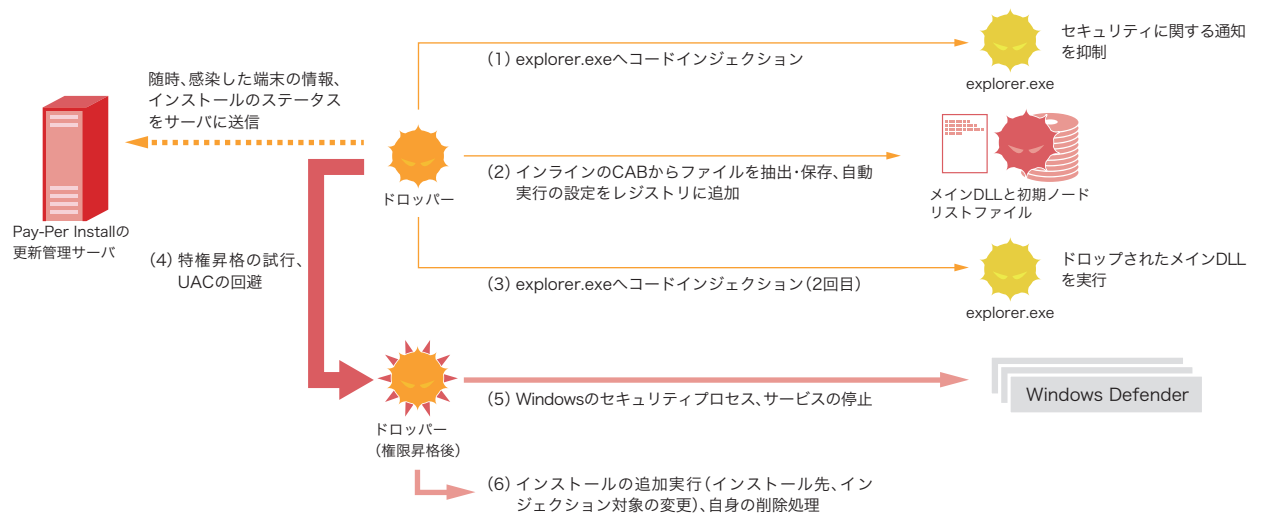


図-12 ユーザモード型ZeroAccessの動作(ドロッパー)

*46 Sophos社は、同社レポートの中で、日本はスーパーノード(他の感染ノードから直接アクセスできるグローバルIPを持つノード)の感染割合に関して3位、非スーパーノードの感染割合に関して10位だったと報告している。"The ZeroAccess Botnet: Mining and Fraud for Massive Financial Gain"(http://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/Sophos_ZeroAccess_Botnet.pdf)。

*47 SpyEyeについては、IJR Vol.13「1.4.2 SpyEye」(http://www.ij.ad.jp/company/development/report/iir/pdf/iir_vol13.pdf)で解説している。また、ZeuSの挙動やその亜種については、IJR Vol.16「1.4.3 ZeuSとその亜種について」(http://www.ij.ad.jp/company/development/report/iir/pdf/iir_vol16.pdf)や、IJR Vol.18「1.4.2 ZeuSの亜種Citadel」(http://www.ij.ad.jp/company/development/report/iir/pdf/iir_vol18.pdf)で解説している。

*48 IOC(Indicator of Compromise)とは脅威が存在することを示す痕跡のこと。マルウェアの場合は、それが行う通信の特徴やOSのアーティファクトに与える変化を元に痕跡を定義する。一度痕跡を定義しておけば、次回以降同じマルウェアに感染した場合に迅速なインシデント対応が可能になる。IOCの規格としては、OpenIOCやCybOX、IODEFなどがある。次のRSA Conference 2013での、Chris Harrington氏の発表では、それぞれの規格の良い点と悪い点を比較している。"Sharing Indicators of Compromise: An Overview of Standards and Formats"(http://www.rsaconference.com/writable/presentations/file_upload/dsp-w25a.pdf)。

*49 Exploit kitは、2010年のIJ Technical Weekで解説している。「IJ Technical WEEK 2010 セキュリティ動向 2010 (1) Web感染型マルウェアの動向」(http://www.ij.ad.jp/company/development/tech/techweek/pdf/techweek_1119_1-3_hiroshi-suzuki.pdf)。

*50 ドライブバイダウンロードとは、Webコンテンツを閲覧した際に脆弱性を悪用され、マルウェアに強制感染すること。閲覧者の使用する端末に脆弱性がある場合は、そのWebコンテンツを閲覧しただけでマルウェア感染してしまう。

ザモードのみで動作したりするなど、初期のころと比べると実装が大きく変化してきています。ユーザモード型ZeroAccessは、ドロッパーとドロッパーによってインストールされるDLLで構成されています。図-12及び図-13にユーザモード型ZeroAccess^{*51}の動作概略を示します。

ドロッパーは、より安定したインストールを目指して、随所でWindowsのセキュリティ機能を無効にするコードを実行します。例えば、MSASCui.exeやwscntfy.exeなどWindowsのセキュリティ機能に関するプロセスを停止したり、explorer.exeにコードをインジェクションし、wscntfy.dllまたはactioncenter.dllのIATテーブルをフックすることで、セキュリティに関する通知を抑制します。UACをDLLのロード順序を悪用^{*52}してバイパスした後は、多くのセキュリティに関するプロセスやサービスを停止させます。また、ドロッパーは、そのインストールの過程で外部と頻繁に通信を行い、感染した端末の情報、インストールのステータスを送信します。その理由は、Pay-Per-Installと呼ばれるサービス^{*53}に必要な情報収集のためだと考えられています。

その後インストールされたDLLは、初期ノードリストファイルを元にZeroAccessのP2Pネットワークに接続し、UDPでポットコマンドの送受信、TCPでプラグインのファイルのダウンロード・アップロードを行います。冒頭で述べたようなクリック詐欺やBitcoinのマイニングなどの機能は、プラグインによって実現されているので、インストールされたDLL自体は、他のピアとの通信をメインに行います。プラグインのファイルについて、ZeroAccessは、NTFSファイルシステムのエントリ情報に含まれるExtended Attribute(EA)から、そのサイズやタイムスタンプなどのファイルのメタデータとその署名を抽出して検証します。更に、ファイルのリソースセクションからデータに関する署名を抽出して検証するので、例えば、ZeroAccessの作者ではない第三者が、任意の実行ファイルをアップロードして、他のピアにダウンロードかつ実行させるのは困難と言えます。

■ IOCに関する考察

上記のようなユーザモード型ZeroAccessの動作を踏まえた上で、それを感染した端末から検出するためのIOCを

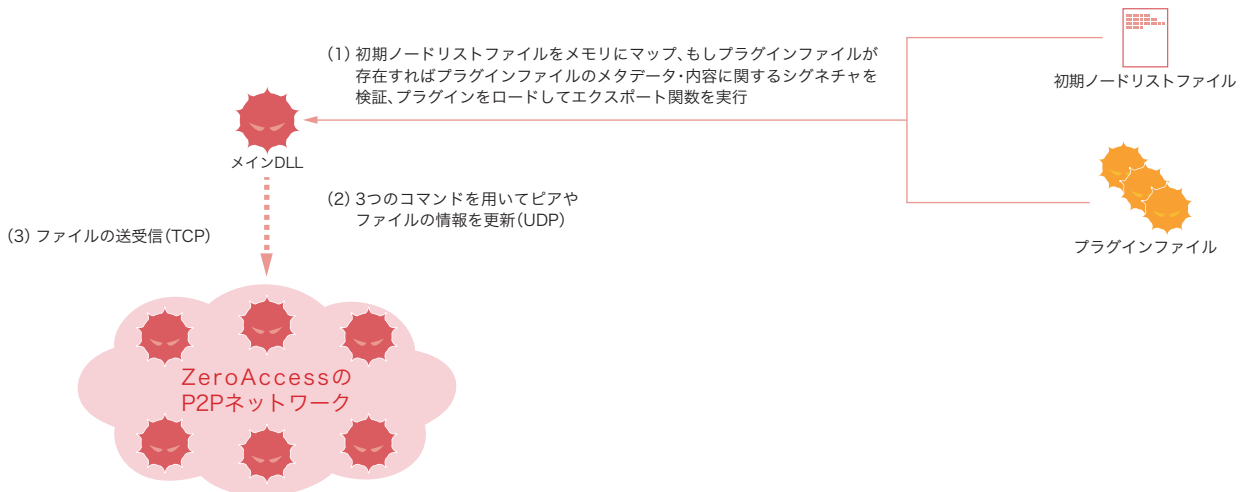


図-13 ユーザモード型ZeroAccessの動作(インストールされたDLL)

*51 IJで把握しているユーザモード型ZeroAccessの実装には、ここで説明している亜種の他にservice.exeにパッチを充てる亜種も存在するが、基本的な動作は同じことを確認している。

*52 最近の亜種の場合、Adobe Flashのインストーラがドロッパーのデータ領域内のCABに格納されており、ドロッパーはまずそれを抽出してテンポラリフォルダに配置した後、そこに自身を「msimg32.dll (Adobe Flashのインストーラに利用されるDLLと同じファイル名)」というファイル名で保存する。その後、インストーラの実行に伴ってUACのプロンプトが表示されるが、ユーザがそのプロンプトで「はい(Y)」を押してしまうと、特権状態でドロッパーが再実行される。

*53 Pay-Per-Installとは、マルウェアをインストールした端末の数に応じて金銭を支払う仕組みのこと。GeolPやOSバージョン、取得した権限の種類など感染端末の様々な情報に応じて、支払われる金銭が異なる。前述のSophos社のレポートでは、このPay-Per-Installサービスの仕組みがZeroAccessの感染端末数を増加させている一因であると指摘されている。Pay-Per-Installサービスの市場調査や観測については、次のUSENIX Security '11のJuan Caballero氏他の発表に詳しい。"Measuring Pay-per-Install: The Commoditization of Malware Distribution" (http://usenix.org/events/sec11/tech/full_papers/Caballero.pdf)。

簡単に考察します。IOCの定義の中で一般的によく用いられるのは、ファイル名、ファイルのハッシュ値、レジストリキー、URLなどですが、これらの情報を定義するのは個人的にはお勧めできません。それらはマルウェアの動作に直接関わらない表面的な情報に過ぎないからです。実際、ユーザーモード型ZeroAccessでは、DLLのインストールされるパスは亜種によって異なります。

マルウェアの動作に関わる情報を定義することで、そのIOCは多くの亜種を検出できる汎用的なものになります。例えば、インストールされたDLLは、UDPでポットコマンドの送受信を行います。そのコマンド名は4バイトの文字列で定義されています*54。これはP2Pのプロトコルがまったく別のものに变化しない限り固定のもので、更に、コマンドの送受信の際には、そのペイロードは4バイトのキーをベースにXORされます。そのキーは通信を行う双方で一致している必要があるため、こちらの値も変化しにくいものであると言えます。また、ZeroAccessがインポートするAPI*55も特徴として定義することができます。このような情報を組み合わせていくことで、汎用的なIOCを生成できます。

ファイルシステム上のマルウェアには、通常バックと呼ばれる圧縮処理が施されているので、上記に述べた情報をベースにしたIOCを適用する対象は、必然的に揮発性のデータであるメモリのバイナリイメージになります。ここで1つ注意すべきことは、ZeroAccessの場合、ドロッパーとインストールされるDLLがまったく異なる実行ファイルであるということです。ドロッパーはDLLをインストールすると自身を削除するので、ドロッパーの特徴を定義したとしても、それをメモリイメージから検出することは現実的に不可能です。ドロッパーには、インジェクションするPIC (Position Independent Code)*56の中で用いられる、call/jmp命令などによるAPI関数の呼び出し、またはデータの取得、スタッ

ク領域の動的な拡張コード、トリッキーな削除処理*57のコードなど、特徴的なコードが多く含まれていますが、それらをIOCとして用いることはできません。

今回はユーザーモード型ZeroAccessの動作とそのIOCに関する考察を行いました。それより前に出現していたカーネルモード型についても、そのドライバがインポートするAPIなどを用いて汎用的なIOCを生成することができます。

■ まとめ

本節では、ZeroAccessの動作を解説すると共に、それを感染端末から検出するための汎用的なIOCについて簡単に考察しました。ZeroAccessの主要な感染経路は、Exploit Kitによるドライブバイダウンロードやインターネットで配布している偽プログラムの実行なので、感染を防ぐにはIIRでこれまで解説したマルウェアに関する記事でも述べてきたように、サードパーティを含めたソフトウェアのアップデートが必須であり、信頼できないプログラムを安易に実行しない心構えが重要です。

また、近年のマルウェアは、ZeroAccessの動作からも分かるように、Windowsのセキュリティ機能やアンチウイルスソフトウェアの動作を無効にします。よって一度感染してしまうと、その検出までには時間がかかることも多々あります。調査が必要な端末の数が多ければなおさらです。そのようなときでも、IOCを使って迅速に脅威を検出することができれば、インシデントの早期解決につながります。また、IOCは一定のフォーマットなので、簡単に共有できます。よって、マルウェアに関する専門的な知識を持たない人間でも調査に参加できるようになります。インシデント対応にIOCを定義して利用するというアプローチは、現状日本ではほとんど行われていませんが、前述のように多くのメリットがありますので、ぜひ皆さんも試してみてください。

*54 コマンドの種類としては、Lteg(通信開始:その後レスポンスを受けてピア情報の更新、ファイルのダウンロード)、Lter(Ltegに対するレスポンス:ピア情報の一部、ファイル情報を含む)、Lwen(新しいピアをポットネットにブロードキャスト)がある。

*55 例えば、ZeroAccessはコードインジェクションを行う時は、ZwQueryInformationThreadやZwQueueApcThread、レジストリやファイル操作の時には、ZwDeleteValueKeyやZwCreateFileなどの比較的低レイヤなAPIを用いる。

*56 シェルコードのように、その時の実行状況に依存せず目的の動作を行えるように構成されているコードのこと。

*57 環境変数を検索してシェルのパス(通常はcmd.exe)を取得、サスペンド状態でシェルを起動後、シェルプロセスの実行コンテキストとスタックを変更して実行中のドロッパーを削除する処理を行う。

1.4.2 ホームルータのセキュリティ

2013年3月ヨーロッパで発生した迷惑メール対策団体に対するDDoS攻撃は、最大300Gbpsという過去に類をみない大規模な攻撃となりました^{*58}。この攻撃には、DNSアンブ攻撃(詳細は後に解説)という手法が用いられ、設定に問題がある世界中のDNSサーバやホームルータ^{*59}などを踏み台にしたことで、この規模の攻撃になったとされています^{*60}。

ここでは、家庭で一般的に利用されているホームルータを取り巻く現状をまとめ、その状況を生み出す原因について議論を行い、この状況を打開する対策手法について考察します。

■ ホームルータが関係した事件

まず、この数年に発生したホームルータに対する攻撃、もしくはホームルータが関係したとされる事件について紹介します。

■ 脆弱性を悪用したDNSの設定変更

2011年、複数のホームルータ(ADSLモデム)に共通する脆弱性を悪用され、何者かによって用意された不正なDNSサーバを参照するように設定が変更されていたことが明らかとなりました^{*61}。世界中で最大450万台の設定がこの手法により不正に変更されていたとされています。不正なDNSサーバは、銀行などのサイトの名前解決に不正な応答を返し、偽のサーバに誘導するため、オンラインバンキングのIDとパスワードを盗まれたり、不正なプラグインをインストールされたりする被害が発生しました。

■ 管理インタフェースへの不正なアクセス

一部のホームルータでは、初期設定でアクセス制限を実施していません。この状態で、管理者のIDとパスワードも初

期設定のままで使用していると、外部から管理者権限でログインされてしまう問題が明らかとなっています^{*62}。多くの場合アクセス制御の機能は存在し、マニュアルなどにはその設定を促す記載がありますが、利用者が導入時に設定やパスワードの変更を実施しなかったために、管理者権限でのアクセスが可能となっていました。

また、ホームルータ上に設定した認証情報(例えば、ISPに接続するためのIDとパスワードなど)を平文で保存する機器があることも分かっています。このため、外部から管理者権限でアクセスされ、この情報が漏えいし、接続サービスの第三者による不正利用や、VoIPなどの付加サービスに不正に加入させられ金銭被害を受けるなどの事件が発生しています。

■ 家庭内のPCに感染したマルウェアからの設定変更

家庭内で利用するPCがマルウェアに感染していたために、そのマルウェアからホームルータの設定インタフェースに攻撃が行われ、DNSなどの設定が不正に変更されてしまう事件が発生しています。例えば2012年に収束したDNS Changerマルウェア^{*63}には、感染したPCのDNSの設定を変更するだけでなく、9社以上のホームルータに対する設定変更を試みる攻撃コードが内在していました。

■ DNS Open resolverによるDDoS攻撃への荷担

一部のホームルータでは、初期設定ではその機能を外部から利用されてしまう危険が存在します。特に、家庭内ネットワークに接続した機器がインターネットに通信するためにDNSによる名前解決を補助する機能については、インターネット側から悪用されることで、通信量を増幅する役割を

*58 この攻撃については、次のCloudFlare社のblogに詳しい。「The DDoS That Almost Broke the Internet」(<http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet>)。

*59 本稿ではケーブルテレビインターネット接続やDSL接続などの終端装置として機能するものをホームルータと呼ぶ。一般に通信事業者からはCustomer Premises Equipment(CPE:顧客宅内機器)とも呼ばれる。

*60 この攻撃を受け、世界中のIPアドレスを検査し、DNSアンブ攻撃に利用される可能性のある設定のアドレスを特定しているOpen Resolver Project(<http://openresolverproject.org/>)では、ホームルータなどのCPEデバイスの設定を見直すように注意喚起をしている。

*61 本件については、ブラジルのCSIRT組織CERT.brの次のプレゼンテーションに詳しい(<http://www.cert.br/docs/palestras/certbr-firstsymposium2012.pdf>)。また、次のIJ-SECT blogでも詳細を報告している。「ホームルータへの不正な設定変更による偽DNSサーバの参照」(<https://sect.ij.ad.jp/d/2012/06/148528.html>)。

*62 例えば、国内製品では次の例がある。Telecom-isac Japan、「【注意喚起】ロジテック製ルータの脆弱性、および、利用者が行うべき必要対策」(<https://www.telecom-isac.jp/news/news20120730.html>)。

*63 DNS Changerマルウェアについては、IIR Vol.15(http://www.ij.ad.jp/company/development/report/iir/pdf/iir_vol15.pdf)の「1.4.2 DNS Changerマルウェア」も参照のこと。また、銀行など個別サーバへのアクセスを不正サイトに誘導しようとした事件としては、例えば2012年にメキシコで発生した次の事件がある。トレンドマイクロ社、「Targeted Attack in Mexico: DNS Poisoning via Modems」(<http://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attack-in-mexico-dns-poisoning-via-modems/>)。

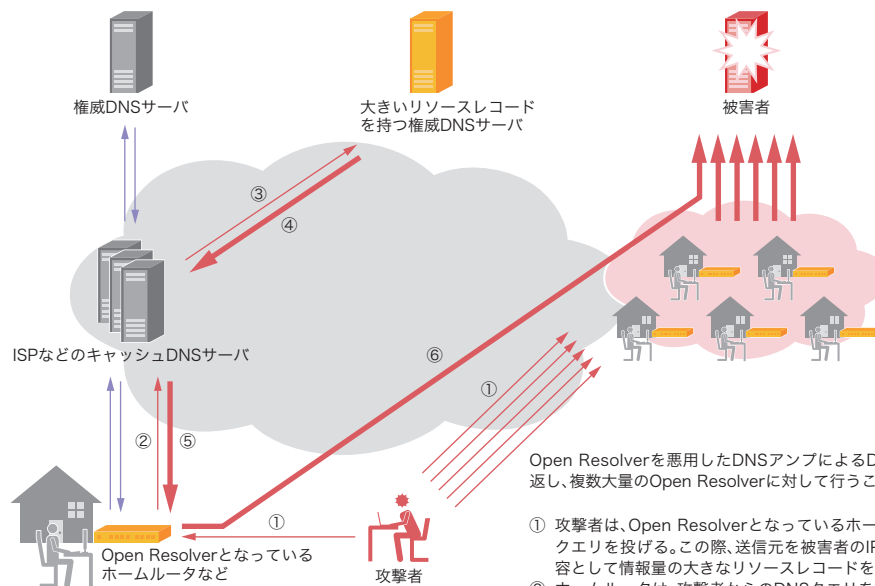
提供してしまうこととなります(図-14)。個々のホームルータの増幅する量が小さかったとしても、インターネット上の多数の機器が同じように悪用されることで、先に紹介した欧州の例のような大規模なDDoS攻撃となります。別の攻撃事例に関するCloudFlare社による発表^{*64}では、数多くの国のOpen Resolverが踏み台となっており、日本国内においても4,625のIPアドレスが荷担したとされています^{*65}。

この手法による攻撃は過去にも発生していましたが、例えば5月には167Gbpsに至る攻撃^{*66}に悪用されるなど、最

近では特に大規模な攻撃を引き起こすために悪用されています。また、IJJのMITFハニーポットによる観測でも、この攻撃を誘発する試みは日常的に実施されていることが分かっています。

libupnpの脆弱性

2013年1月に発表^{*67}されたUniversal Plug and Playのライブラリに関わる脆弱性は、一部のホームルータも影響を受けることが分かっています^{*68}。脆弱性対策を行ったファームウェアを利用していない場合、インターネット側からの攻撃にさらされる可能性があります^{*69}。



Open Resolverを悪用したDNSアンブによるDDoS攻撃では、次の手順を繰り返して、複数大量のOpen Resolverに対して行うことで、DDoS攻撃を発生させる。

- ① 攻撃者は、Open Resolverとなっているホームルータに対し、攻撃用のDNSクエリを投げる。この際、送信元を被害者のIPアドレスに詐称し、クエリの内容として情報量の大きなリソースレコードを要求する。
- ② ホームルータは、攻撃者からのDNSクエリを家庭内ネットワークからの要求と同様に処理し、ISPなどのDNSサーバに転送する。
- ③ ISPなどのDNSサーバでは、正当な利用者からの通信であるため、攻撃用のDNSクエリと正当なDNSクエリとを判別することができず、当該攻撃DNSクエリをインターネット上の権威DNSサーバに送付する。
- ④ 攻撃DNSクエリの内容に応じて、権威DNSサーバから情報量の大きなリソースレコードが、攻撃用のレスポンスとしてISPのDNSサーバに送付される。
- ⑤ ISPのDNSサーバは攻撃用のレスポンスをホームルータに転送する。
- ⑥ ホームルータは受け取った攻撃用のレスポンスを、送信元に転送する。この際送信元は攻撃者が詐称した被害者のIPアドレスとなっている。

通常のDNS名前解決では、紫の線で示した通り、家庭内ネットワークの機器がホームルータに対してDNSクエリを送付し、ホームルータはISPなどの外部のキャッシュDNSサーバにそのクエリを転送する。ISPなどのDNSサーバは最終的にインターネット上の権威DNSサーバにクエリを送ることで、クエリに対応するリソースレコードをレスポンスとして得る。このレスポンスをホームルータに転送し、ホームルータはクエリを出した機器にレスポンスを渡す。

図-14 DNS Open Resolverを踏み台としたDNSアンブによるDDoS攻撃

*64 Apricot 2013におけるCloudFlare社の発表"The curse of the Open Recursor"(http://www.apricot2013.net/_data/assets/pdf_file/0009/58878/tom-paseka_1361839564.pdf)によると、紹介された攻撃事例において攻撃に荷担したIPアドレスは、アジア太平洋地域では日本が1番多かったとされている。

*65 ただし、同プレゼンテーション内では、この攻撃に加担したOpen Resolverの多くはサーバ類であると指摘されており、攻撃の全体量のうち、ホームルータがどの程度寄与したかは分かっていない。

*66 この攻撃については、Prolexic社の次の発表に詳しい。"Prolexic Stops Largest-Ever DNS Reflection DDoS Attack"(<http://www.prolexic.com/news-events-prolexic-stops-largest-ever-dns-reflection-ddos-attack-167-gbps.html>)。

*67 次はRapid7社による複数の脆弱性に関する報告。"Portable SDK for UPnP Devices (libupnp) contains multiple buffer overflows in SSDP"(<http://www.kb.cert.org/vuls/id/922681>)。

*68 例えば次のJVNIによる情報では、複数指摘された脆弱性の影響を受ける製品に関する情報がまとまっている。JVNI、「JVNVU#90348117 Portable SDK for UPnP にバッファオーバーフローの脆弱性」(<https://jvni.jp/cert/JVNVU90348117/index.html>)。

*69 IPアドレスごとの実装に関する情報を収集しているSHODAN(<http://www.shodanhq.com/>)の、本稿執筆時点での検索結果では、UPnPの最初のネゴシエーションに利用するSSDPプロトコルに回答するIPアドレスは、世界中で約2千800万台(日本国内に約270万台)あるとされている。ただし、この数字はすべてがホームルータではなく、例えば大学などの比較的オープンなポリシーで運用しているネットワーク接続されたプリンタなども含まれていると考えられる。

■ 脆弱なホームルータのセキュリティ上のリスク

ホームルータを脆弱な状態のまま放置することで、次の3つの視点からそれぞれ異なるリスクが発生します。

■ 個人のプライバシーに関わるリスク

ホームルータは家庭内ネットワークの要となる装置であり、家庭からのインターネット利用状況を把握される危険があります。また、ホームルータを踏み台にして、家庭内のネットワーク対応家電の脆弱性などを悪用されると、家庭内の様子を勝手に覗き見られるなど、直接プライバシーの侵害となる危険性があります^{*70}。

■ 企業や組織にとってのリスク

昨今利用が拡大している持ち運び可能な情報通信機器(スマートフォンやタブレットなど)を通じて、間接的に企業や組織のリスクが発生します。特に、BYODなどで個人所有の機器による仕事を許可している場合、侵入された家庭環境に日常的に接続しているスマートフォンなどを信頼し、仕事の情報に触れて良いかどうかを問われることとなります。また、家庭のネットワーク環境から発せられる通信は、主に家族からのものであり、それを受け取った人は無条件に信頼してしまう傾向にあります。これは標的型攻撃などに、応用される危険性をはらんでいます。

■ インターネット全体にとってのリスク

ホームルータはその数が膨大であることから、個別に悪用される量が小さくても、総量としては深刻な規模の攻撃が発生します。また、ホームルータには通信の記録を取得する機能が乏しいものが多く、踏み台とされることで、真の犯人を追跡できる可能性が少なくなることも深刻な問題となります。

以上の想定から、この状況を放置することは複数の視点において極めて危険であり、早急に是正すべき状況にあると考えられます。

■ 国内における脆弱なホームルータの実態調査

これまで紹介した国外の調査では国内の現状を示す精度の高い情報が少ないため、国内の通信事業者が集ったセキュリティ団体であるTelecom-ISAC Japan^{*71}で、国内の状況に関する実態調査を行っています^{*72}。この調査では、ホームルータの管理インタフェースへのアクセスの可否、Universal Plug and Play関連のプロトコルへの応答の有無、DNS Open Resolverを含めたDNS通信の増幅要因の有無、の3点について独自の調査環境から調査を行い、信頼性と精度の高い数値をもって状況を把握するとしています。

本稿執筆時点では、調査結果の公開については明言されてはいませんが、特に深刻な状況であった場合には、状況を打開するための対策の検討のために用いるとしています。

■ この状況を解決するために

この状況を解決するためには、現時点では2つのアプローチが考えられます。1つは企業などの組織でネットワークを安全に運用するために取られている技術や手法を、家庭のネットワークに持ち込み、日常的な運用を行うことです。もう1つはリスクを低減することを目的にインターネット側で通信を規制することです。

企業などと同じように、家庭のネットワークを運用するためには、まずは利用者側で家庭内ネットワークに接続する装置すべてを把握し、それぞれの脆弱性情報に注意し、最新のファームウェアを利用するように心掛けます。そして、設定の健全性を確認し、日常的な通信ログを確認する必要があります。このためには膨大な量の作業が必要があり、日常生活の中で実施するためには、これらを補助するツールが必要不可欠となります。

また、ホームルータを提供する製品開発者側でも、その製品について、安全な実装を目指す活動、導入時に電源をいれるだけで安全に利用できる初期設定、脆弱性への早期対応、新

*70 現実に、例えば韓国Samsung社製のネットワーク対応TVでカメラ機能などが制御可能な脆弱性が指摘されている。Sophos Nakedsecurity Blog, "Samsung Smart TV security hole allows hackers to watch you, change channels or plug in malware" (<http://nakedsecurity.sophos.com/2012/12/12/samsung-tv-vulnerability/>)。

*71 財団法人データ通信協会 テレコムアイザック推進会議 (<https://www.telecom-isac.jp/>)。

*72 Telecom-ISAC Japan, 「ネットワークデバイスの脆弱性保有状況調査について」 (<https://www.telecom-isac.jp/news/news20130617.html>)。

しいファームウェアの広報や自動アップデートなどの修正を適切に配布する仕組みの構築、外部から利用されたことを検出できる機能の追加などが必要となります。加えて、家庭内ネットワークに接続された機器を保護する意味で、通信の概要を記録する機能を強化する必要もあるでしょう。

通信事業者やセキュリティ事業者などにおいては、インターネット側から設定ミスの有無の確認や、ホームルータの運用といったサービスを検査することが必要です。また、利用者の通信機器を保護する機能をもったWalled Garden^{*73}タイプの接続サービスを広範囲に提供することも検討に値します。

一方で、通信上の規制については、機会損失や副作用^{*74}の影響が考えられ、慎重に検討を進める必要があります。例えば、実態調査で数百万台規模の脆弱なホームルータが発見されるなど、製品開発者やISPにおける個別の努力では状況を是正できないことが明らかになったときに、はじめて通信の規制が現実的な対応策として検討されるものと考えられます。

ここで検討したような対応策の実現には、少なからず時間が必要です。今すぐにはじめられる対策として、一般の利用者に現状のホームルータの機能を用いてその健全性を確認することを促す努力が、複数のセキュリティ団体、インターネット関連団体、ISPなどにより開始されています。

1.4.3 頻発する不正ログイン事件

2013年3月頃から、日本国内の登録制オンラインサービスへの不正ログイン(なりすましログイン)^{*75}事件や、登録情報の窃取が目的と考えられる不正アクセス事件が頻発しています。本稿では一連の事件を整理して紹介し、ユーザ側で実施可能な対策を提案します。

■ 不正ログインとその手法

大規模な不正ログインでは、主に次の3種類の手法が用いられます^{*76}。最も単純な攻撃はIDやパスワードについて利用可能な文字列を総当たりで試行する(「aaaa」「aaab」「aac...」)「総当たり攻撃」と呼ばれます。もう少し効率の良い攻撃として、よく利用される文字列(例えば「password」や「abc123」など)を網羅した辞書を用意して順次施行す

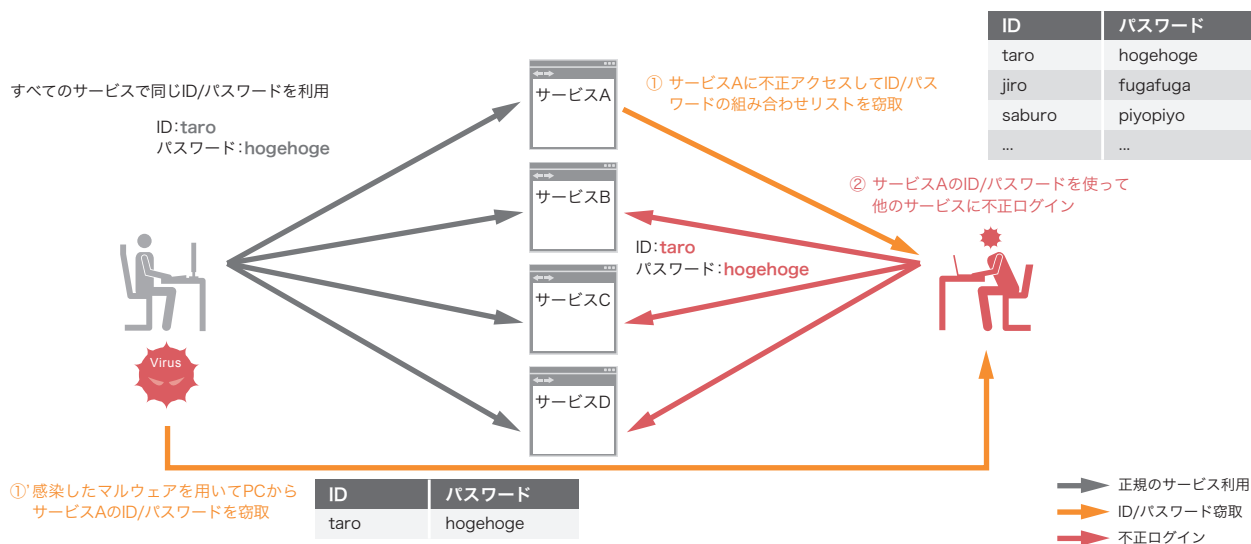


図-15 リスト型不正ログインのイメージ

*73 ISPにおけるWalled Gardenについては、例えばMAAWGにおける次の資料がある。"MAAWG BEST PRACTICES FOR THE USE OF A WALLED GARDEN"(http://www.maaWG.org/sites/maawg/files/news/MAAWG_Walled_Garden_BP_2007-09.pdf)。

*74 ここで言う副作用とは、通信を行いたいときに当該通信が不可能なインターネットとなること。例えばUniversal Plug and Playはインターネット上では利用できなくてもあまり影響は想定されない。しかし、Web管理インタフェースで使われているHTTPや、DNSの通信については、その規制の方向や在り方によって、自宅に自前のサーバを構築することが著しく難しくなるなど、今のインターネットとは異なる状況を産み出してしまう危険がある。

*75 本稿では認証を要する任意のオンラインサービスについて、本来のID所有者の意図に反して第三者がそのサービスにログインする行為を「不正ログイン」と呼称する。

*76 知人などを対象に手動で行われる小規模な不正ログインでは、プロフィールなどからパスワードを推測したり、相手を騙してパスワードを教えさせたりするソーシャルエンジニアリングが用いられることが多い。

る「辞書攻撃」と呼ばれる手法があります。最後は「リスト型攻撃」と呼ばれる手法で、攻撃者はあらかじめ入手したIDとパスワードの組み合わせリストを用いてログインを試行します。攻撃者は、他のオンラインサービスへの不正アクセスで窃取したアカウント情報やフィッシングで収集したアカウント情報、マルウェアを使ってユーザPCから直接窃取したアカウント情報^{*77}などからこのリストを作成すると考えられます(図-15)。

本来、オンラインサービスごとに異なるID、パスワードを利用していればリスト型攻撃は大きな問題にはなりません。しかし、IPAが2012年に実施した意識調査では、「サービスごとに異なるパスワードを設定している」とした回答者は僅か2割でした^{*78}。このような状況においては、リスト型攻撃はわざわざ効果的な手法であると言えます。

不正ログインが成功してしまうと、サービス事業者側ではそれが本来の利用者の意図によるものか否かを判別するこ

とが困難であるため、攻撃者はサービスの提供内容に応じて、個人情報の閲覧や物品の購入、金品の譲渡など任意の権限を行使することができます。実際に、ポイントサービスを提供しているオンラインショッピングサイトなどでは、不正ログインした攻撃者によってポイントが不正に使用された事件が複数公表されています。

■ 一連の攻撃とその目的

表-1は2013年に公表された主な不正ログイン・不正アクセスをまとめたものです。不正ログインに注目すると、通信関連サービスや通販サービスなど同業種のオンラインサービスが近い時期に攻撃を受けていることが分ります。これは、該当する攻撃について同一あるいは何らかの関係性を持つ攻撃主体の存在を示唆しています。このような攻撃主体を想定し、更に今年になって日本国内向けサービスを対象とした不正ログイン事件が頻発していることを鑑みると、日本人ユーザのIDやパスワードについて、有効性の高い辞書や組み合わせリストが攻撃者コミュニティ

表-1 2013年に公表された主要な不正ログイン及び不正アクセスによるアカウント漏えい事件

公表日	サービス分類		期間	事件の種類	不正ログイン件数/ 漏えいアカウント数	備考
4月 3日	検索ポータル	A社	4月1日~4月9日	不正ログイン試行	108,716	
4月 4日	通信関連サービス	B社	4月4日	不正ログイン試行	30	
4月 4日	検索ポータル	C社	~4月2日	不正アクセス	0	サーバ上で127万件のアカウント情報が収集されたが漏えいしていない
4月 5日	ポイント関連サービス	D社	3月26日	不正ログイン試行	299	ポイント不正利用あり
4月 6日	電子書籍サービス	E社	4月2日~4月5日	不正ログイン試行	779	クレジットカード情報漏えいの可能性あり
4月10日	通信関連サービス	B社	4月9日~4月10日	不正ログイン試行	77	
4月17日	運輸サービス	F社	3月31日	不正ログイン試行	97	
4月22日	決済サービス	G社	4月18日~4月19日	不正ログイン試行	5,450	
5月 8日	通販サービス	H社	5月4日~5月8日	不正ログイン試行	約15,000	
5月17日	美容サービス	I社	5月6日~5月12日	不正ログイン試行	682	
5月17日	検索ポータル	C社	~5月16日	不正アクセス	1,486,000	サーバ上で最大2200万件のアカウント情報が収集されたが漏えいした可能性があるのは148.6万件のみ
5月25日	通販サービス	J社	5月6日~5月23日	不正ログイン試行	8,289	
5月29日	通販サービス	K社	~5月13日	不正ログイン試行	2,382	クレジットカード情報漏えいの可能性あり
6月 3日	通販サービス	L社	4月24日~5月31日	不正ログイン試行	9,609(最大16,808)	クレジットカード情報漏えいの可能性あり
6月19日	通販サービス	M社	6月18日	不正ログイン試行	126	
7月 5日	ゲーム関連	N社	6月9日~7月4日	不正ログイン試行	23,926	
7月 9日	ゲーム関連	O社	6月13日~7月7日	不正ログイン試行	35,252	
7月10日	通販サービス	P社	5月10日~7月8日	不正ログイン試行	-	ポイント不正利用あり
7月17日	通信関連サービス	Q社	7月14日~7月16日	不正ログイン試行	21,184	
7月19日	ニュースポータル	R社	7月17日~7月18日	不正アクセス	1,692,496	攻撃者を特定し漏えいした情報の削除を確認
7月24日	通信関連サービス	S社	~7月23日、7月26日	不正アクセス	最大4,000,000	
7月26日	ポイント関連サービス	D社	7月15日	不正ログイン試行	27	ポイント不正利用あり
8月 8日	ソーシャルコンテンツ	T社	7月25日~8月5日	不正ログイン試行	39,590	
8月 8日	旅行サービス	U社	2月14日~2月16日、 6月3日~6月15日	不正ログイン試行	27,620	
8月12日	ソーシャルコンテンツ	V社	4月6日~8月3日	不正ログイン試行	243,266	

※表中の記載は被害に遭ったサービス事業者の発表内容に基づいています。

*77 2009年に日本国内のWeb環境に大きな影響を与えたGumblar攻撃では、ドライブバイダウンロードで感染するマルウェアによってPCに保存されたFTPアカウント情報が盗まれ、そのアカウント情報を用いて新たなWebサイトが改ざんされるという事件が繰り返し発生した。詳細は本レポートVol.4 (http://www.ij.ad.jp/company/development/report/iir/pdf/iir_vol04.pdf)の「1.4.2 ID・パスワード等を盗むマルウェア Gumblar」参照。

*78 IPA、「2012年度 情報セキュリティの脅威に対する意識調査」(<http://www.ipa.go.jp/security/fy24/reports/ishiki/>)。

などで利用しやすい状態になってきているのではないかと推測されます。

また、表-1に含まれているような不正アクセス事件によって窃取されたアカウント情報が、直ちに不正ログインに悪用(リスト型攻撃や辞書攻撃^{*79})されていた可能性も考えられます。

一方で、一連の不正ログインについては、攻撃者の意図が明らかではありません。一連の不正ログイン事件では、一部のショッピングサービスやポイント交換サービスでポイント不正利用が行われた3件を除くと、ログインされたこと以外に具体的な被害が伝えられていません。クレジットカード情報が漏えいした可能性に言及している事件も複数ありますが、ログインによってクレジットカード情報の閲覧が可能であったことを示唆するのみで、2013年8月時点では、漏えいしたクレジットカード情報が不正利用されるなどの被害は公表されていません。

このため、攻撃者は「試行したIDとパスワードの組み合わせが対象のオンラインサービスで有効であること」だけを確認しているように見えます。

また、いくつかのケースで公開されている情報によれば、攻撃者は少数の攻撃元から比較的短時間に不正ログイン試行を繰り返すなど、攻撃が露呈することについてあまり注意を払っていないかのように振る舞っています。攻撃が露呈すると、オンラインサービスの提供者がユーザにパスワードの変更を要請するため、せっかく確認した「有効なIDとパスワードの組み合わせ」が変更されてしまうということを考慮していないことになります。

この攻撃の様態に何らかの隠れた意図があるのか、あるいは単に気にしていないだけなのかを、推測することは困難ですが、今後より洗練された攻撃が行われうるということは警戒しておく必要があります。

■ サービス事業者側の不正ログイン対策

サービス事業者側で考慮すべき基本的な不正ログイン対策は以下のようなものです。

- (1) なるべく複雑で長いパスワードを使えるようにする
- (2) サービスごとに異なるパスワードを使うよう呼びかける
- (3) 二段階認証・多要素認証を提供する
- (4) ログイン履歴や購入手続きなどの履歴を確認する手段を提供する
- (5) 不正ログイン試行を検知・防御する

(1)(2)のような方針は2008年ごろからオンラインサービス事業者らによって繰り返し呼びかけられているものです^{*80}。特に(1)に関しては、パスワード設定時に、文字列が短すぎるものや、複雑さ(使う文字の種類)が足りないもの、辞書に載っている安易な語句をそのまま使っているものなどの登録ができないようにサービス事業者側で強制することを考慮すべきでしょう。

(3)への対応は、現在行われているようなリスト型攻撃による不正ログインを効果的に防ぐことができます。一部の金融サービスなどでは以前からハードウェアトークンを使う多要素認証が提供されています。また、今年に入って多くのポータルサイトやSNSなどが二段階認証に対応しました。

また、万が一被害が発生した場合や、あるいは被害が発生していないことを確認したい場合に備えて、(4)を実装しておくことを推奨します。不正ログインの直接的な被害者となるユーザ自身が被害や影響の有無を確認できるようにしておくことが重要です。

(5)は例えばアカウントごとや接続元IPアドレスごとに単位時間当たりのログイン試行回数や、同時ログイン数などに閾値を設け、不審な挙動を通知したり遮断する仕組みの

*79 窃取した組み合わせをそのまま用いるリスト型攻撃の他に、平文パスワードが入手できない場合などに、入手したIDのリストと一般的なパスワード辞書を用いた辞書攻撃が行われる可能性なども考えられる。

*80 ニフティ株式会社、「やめよう！同じパスワード」(http://support.nifty.com/support/information/1114_pass.htm)、楽天株式会社、「楽天会員のユーザIDとパスワードの管理にご注意ください」(<http://www.rakuten.co.jp/com/faq/information/20081029.html>)、ヤフー株式会社、「サイトごとに違うパスワードを！」(<http://security.yahoo.co.jp/attention/password/>)。

ことです。提供しているサービスの性質に応じて監視項目や閾値、検知時の対応などを考慮する必要があります。

また、今回の事件でみられたように、大規模な攻撃試行ではサーバが過負荷に陥ることがしばしばあるので、リソース監視によって不正ログイン試行が発見される場合もあります。

■ ユーザ側の不正ログイン対策

ユーザ側の対策はサービス事業者の提供する機能、特に前項(1)～(4)の機能を積極的に利用することです。(1)に関しては、アイディアに頼るのではなく、パスワード生成ツールなどを利用して複雑なパスワードを作ることが望まれます。その複雑なパスワードを束ねて(2)を無理なく実現するためには、パスワード管理ツールを利用することが効果的です。

なお、こういった高度なパスワード運用を行っていても、洗練されたフィッシングやソーシャルエンジニアリング、高度なマルウェアなどによってパスワードやセキュリティ

トークンを窃取され、不正ログインを行われてしまう可能性を完全に排除することはできません。

利用者の立場では、自衛のために、特に重要な金融サービスやショッピングサービスなどに関しては、(4)を定期的に確認しておくことが望ましいと言えます。

1.5 おわりに

このレポートは、IJ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、マルウェアZeroAccessの検出手法、脆弱なホームルータによる影響、頻発する不正ログイン事件についてまとめました。IJ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続けてまいります。

執筆者:



齋藤 衛(さいとう まもる)

IJ 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などに従事後、2001年よりIJグループの緊急対応チームIJJSECT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、鈴木 博志(1.3 インシデントサーベイ)

春山 敬宏(1.4.1 ZeroAccessとそのIOCに関する考察)

齋藤 衛(1.4.2 ホームルータのセキュリティ)

梨和 久雄(1.4.3 頻発する不正ログイン事件)

IJ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、齋藤 聖悟 IJ サービスオペレーション本部 セキュリティ情報統括室

迷惑メール送信を目的とした不正SMTP認証の増加

SMTP認証のためのIDやパスワードを使ってメールアカウントが第三者に利用され、迷惑メール送信に悪用される問題が増加傾向にあります。多くのケースにボットネットが利用されていること、そしてそのボットネットはSMTP認証をした上でメール送信を試みていることが分かっています。ここでは、IJのメールサービスで観測した不正SMTP認証によるアクセスの動向を紹介します。

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、IJが関わる様々な活動についてまとめています。今回は、IJのメールサービスで観測したデータを元にその分析結果を報告します。

最近、第三者が正当な利用者のアカウントと認証情報を利用して特定のサービスにログインを試みる事例が相次いでいます。ポータルサイトやウェブサービスにおいては、そのアカウント情報の搾取や改ざんが目的とされるケースが多いようです。一方、メールサービスにおいてもアカウントの不正な利用が以前から問題となっており、2012年にJPCERTコーディネーションセンターから、複数のISP事業者のメールサービスにおいて、メールアカウントの不正利用が観測されていることが報告されています*1。メールアカウントの不正利用の目的は、主に迷惑メールの送信であると言われており、その手口の多くにボットネットが利用されていることも分かっています。

本レポートでは、このメールアカウントの不正利用問題について取り上げ、IJのメールサービスで観測した不正SMTP認証によるアクセスの動向について報告します。

2.2 不正SMTP認証によるアクセスの動向

2.2.1 不正SMTP認証

本来、SMTP認証は、メールの送信者が正当な利用者本人であることを確認するために利用されています。しかし、近年、このSMTP認証に使うメールアカウントのIDやパスワードの情報が、ウイルス感染など何らかの手段で盗まれ、正当な利用者ではない第三者により、迷惑メールの送信に悪用される事象が問題となっています。本レポートでは、このような第三者が正当な利用者の認証情報を使ってSMTP認証を行うことを「不正SMTP認証」と表現します。そしてIJが提供するメールサービスにおいては、独自のサービス基準で、この不正SMTP認証によるアクセスの観測と対策を行っていますが、その観測数は増加傾向にあります。

2.2.2 不正SMTP認証の特定

不正SMTP認証によるアクセスを、正確かつリアルタイムに特定することは容易ではありません。メールアカウントの送信元IPアドレスの地理的傾向、メールの送信通数、宛先の傾向などを考慮し、総合的に判断する必要があるからです。その中でも、不正SMTP認証によるアクセスを特定するための重要な手掛かりとなるのが、送信元IPアドレスの地理的傾向です。不正SMTP認証によるアクセスは、地理的に分散した多数の送信元から行われていることが多く、これはボットネットからの迷惑メール送信に見られる特徴と共通しています。ボットネットは、その拡散と追跡を困難にするために年々知的化しており、最近では、ZeroAccess*2のようなP2P型のボットネットの脅威が報告されています。IJでは、独自のサービス基準で不正SMTP認証によるアクセスを日常的に検出し、対策を行っています。

*1 JPCERTコーディネーションセンター、「メールアカウント不正使用に関する情報提供のお願い」(<http://www.jpccert.or.jp/pr/2012/pr120003.html>)。

*2 Over 9 million PCs infected - ZeroAccess botnet uncovered(<http://nakedsecurity.sophos.com/2012/09/19/zeroaccess-botnet-uncovered/>)。

2.2.3 不正SMTP認証の観測

IJのメールサービスにおいて、特定期間に観測した不正SMTP認証によるアクセスを受けていたアカウントの数を図-1に示します。図-1から、不正SMTP認証によるアクセスを受けているメールアカウントが日常的に検出されていることが分かります。1日あたりの平均検出件数は数件程度で、多いときは数十件程度でした。

多くの場合、不正SMTP認証によるアクセスを受けていたアカウントに傾向は見られませんが、特定ドメインの複数アカウントが同時に不正SMTP認証によるアクセスを受けていたケースも観測されました。これは社内のウイルス感染により、SMTP認証に使われるメールアカウントのIDやパスワードの情報が搾取されたのではないかと推測できます。

検出されたメールアカウントについては、そのアクセス元IPアドレスが極めて多く、かつ地理的に広範囲に分散している点が共通していました。

■ アクセス元IPアドレスの地理的傾向

次に、アクセス元IPアドレスの地理的傾向について調べてみました。図-2は、今回の対象期間に検出されたアカウントのアクセス元IPアドレスのうち、上位を占めた地域をピックアップして時系列に並べたものです。

この期間では、ポーランド(PL)、及び、インド(IN)からのアクセスが他のアクセス元地域に比べて大きな割合を占めていたことが分かります。

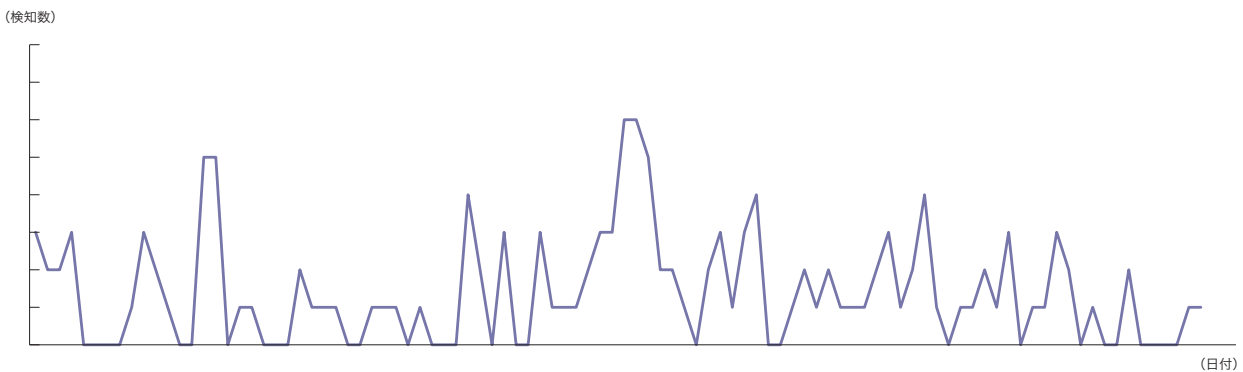


図-1 不正SMTP認証によるアクセスを受けたアカウント数

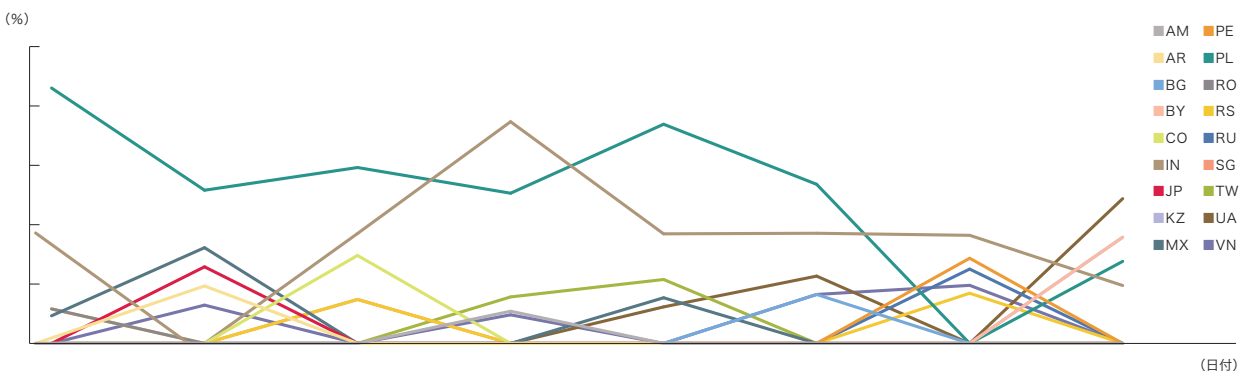


図-2 アクセス元地域の割合の推移

JPCERTコーディネーションセンターからの報告^{*1}によると、メールアカウントの不正利用の多くは迷惑メール送信に悪用されていることが窺えます。また、迷惑メールの上位送信国ランキングを定期的に発表しているSophos社のレポート^{*3}においても、ポーランド(PL)は2012年の迷惑メール送信国の10位、インド(IN)は1位にランクインしていました。これらの国は、今回の調査対象期間においても依然として迷惑メールの送信が多く行われていたことが推測できます。

また、アクセス元IPアドレスが数千を超えるような大規模なアクセスでは、前述した中東欧の地域に加え、アルゼンチン(AR)や南アフリカ共和国(ZA)なども含め、多いときには30を越える国からのアクセスがあるケースも観測されました。このように、アクセス元の上位には中東欧の地域が目立っていますが、ほぼ全世界からのアクセスが確認できており、不正SMTP認証によるアクセスにはボットネットワークが利用されていると推測できます。

■ アクセス元IPアドレス数の推移

図-3に、不正SMTP認証によるアクセスを検出したメールアカウントのアクセス元IPアドレス数の推移を示します。今回の対象期間において、検出したアクセス元IPアドレス数は平均で数百個、最大では数千個にも上りました。

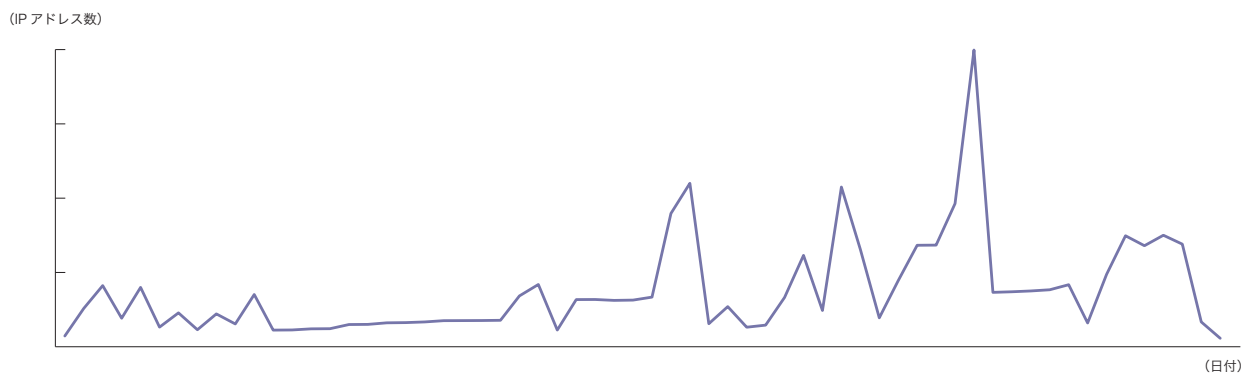


図-3 アクセス元IPアドレス数の推移

■ アクセス元IPアドレスと迷惑メール送信試行回数

今回の対象期間において、アクセス元IPアドレスが迷惑メール送信に使われる頻度を調査したところ、2つのパターンに分けられることが分かりました。一方は、1つのIPアドレスから数千通に及ぶメール送信を試みているケース、他方は1つのIPアドレスから数通程度のメール送信を試みているケースです。今回の対象期間に検出した結果では、後者が9割を占め、前者が1割でした。前者のケースについて、あるメールアカウントのアクセス元IPアドレスごとの不正SMTP認証によるメール送信の試行回数を図-4に、後者のケースについて同様に図-5に示します。

更に、図-4で調査を行ったアカウントに対して、各アクセス元IPアドレスのアクセス時間の間隔を調べたところ、1つのIPアドレスあたり約1時間に渡って、1秒あたり数回の頻度で連続的にメール送信を試みている形跡がありました。一方、図-5で調査を行ったアカウントに対しても同様に調べたところ、同一のIPアドレスから連続してメール送信を試みた形跡はありませんでした。

1つのIPアドレスから連続的かつ大量にメールを送信するのではなく、数通程しか送らずに大量のIPアドレスからメールを送信する手法は、アクセス元の追跡を困難にしようとする迷惑メール送信者の典型的な手法です。

*3 Sophos Security Threat Report 2013(<http://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf>)。

2.3 おわりに

本レポートでは、メールアドレスの不正利用問題について取り上げ、IIJのメールサービスにおける不正SMTP認証によるアクセスの傾向について、その観測状況を報告しました。不正SMTP認証によるアクセスの観測結果から、その送信元は、ほぼ全世界に分散した多数のIPアドレスであることから、ボットネットを利用したアクセスである可能性が高いと考えられます。また、送信元IPアドレスの地理的傾向から、迷惑メールの送信地域の上に報告されている地域から、依然として迷惑メール送信が試みられている可能性が高いことも窺えました。更に、不正SMTP認証によるメール送信の試行形態が一律でない点についても観測しました。不正SMTP認証アクセスによる証拠を正確に捉える

ことは容易ではありませんが、IIJでは独自のサービス基準で早期に不正なアクセスを検知し、対策を行っています。

その一方で、JPCERTコーディネーションセンターからの報告^{*1}によると、攻撃者がメールアドレスのSMTP認証情報を盗む手口としては、POPサーバに対する辞書攻撃、フィッシング、ウイルス感染などが代表的です。従って、端末へのウイルス対策やパスワードの定期更新、不要なメールアドレスの削除など、利用者側での適切な防御を継続的に行うことが求められています。

IIJでは、今後も継続的に不正SMTP認証によるアクセスの傾向を分析し対策を行うことで、安心して利用できるメールサービスの運用を行って参ります。

(メール送信試行回数)

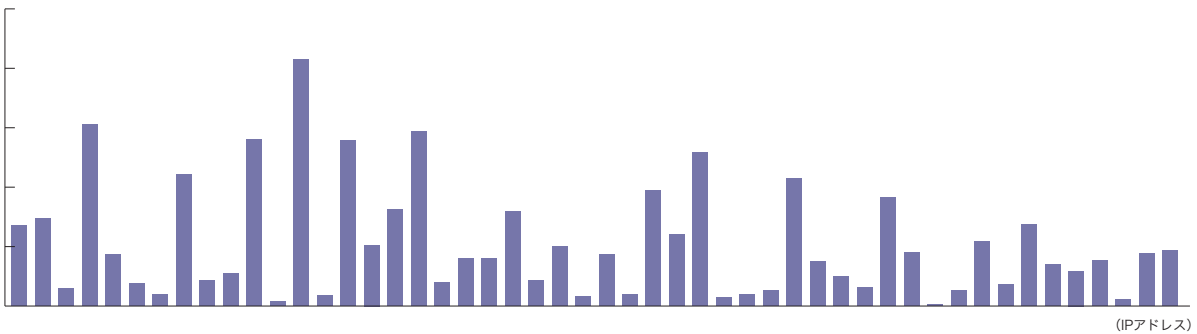


図-4 アクセス元IPアドレスあたりのメール送信試行回数

(メール送信試行回数)

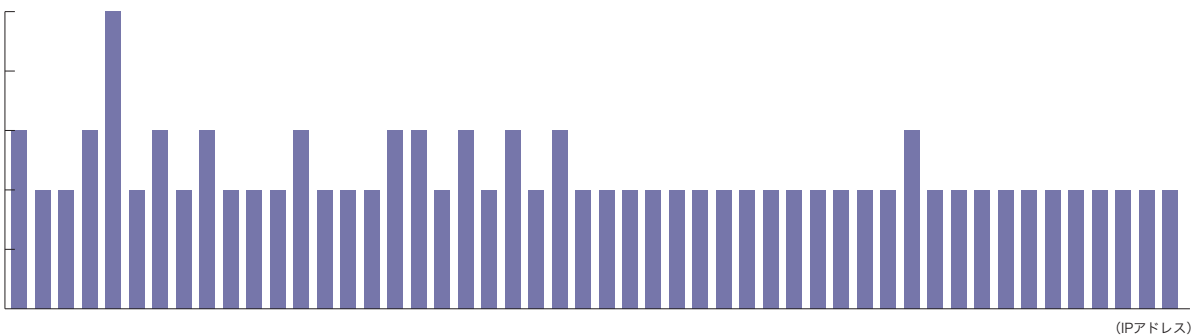


図-5 アクセス元IPアドレスあたりのメール送信試行回数

執筆者:



渡辺 崇文(わたなべ たかふみ)

IIJ プロダクト本部 プロダクト開発部 メッセージングサービス課。2009年入社。IIJメールサービスの開発に従事。M³AAWGメンバー。

違法ダウンロード刑事罰化の影響は限定的

法的強制措置の効果を検証する意味で、2012年10月1日の違法ダウンロード刑事罰化の影響について注目していました。

施行後3ヵ月間程はトラフィックが減少しましたが、その後はもとのトレンド曲線に戻ったことから、今回のダウンロード刑事罰化は一時的な心理効果しかなかったように見えます。

3.1 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}。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もとに、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、ブロードバンド全体の過去6年間の月平均トラフィックです。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。2011年3月の東日本大震災では、被災県でこそ設備と回線の被害や停電の影響によるトラフィック減少が観測されましたが、全国レベルで見た影響は大きくはありませんでした。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ました。その前後でトラフィックの増減が観測されましたが、その影響は限定的で、2010年のダウンロード違法化のときのような長期トレンドの変化はなかったと言えます。この1年のトラフィック量は、INは8%増加、OUTは16%増加しています。

3.2 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、2013年6月3日～9日の1週間分のデータを、前回解析した2012年5月28日～6月3日の1週間分と比較します。

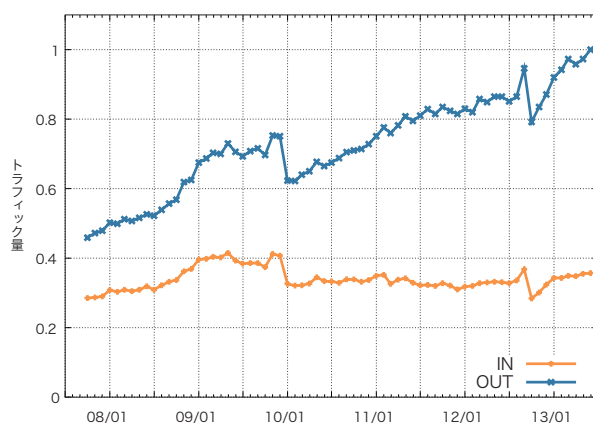


図-1 過去6年間のブロードバンドトラフィック量の推移

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。

- *1 長健二郎. 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.
- *2 長健二郎. 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.
- *3 長健二郎. 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.
- *4 長健二郎. 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.

ここ数年でDSLからファイバーへの移行が進み、2013年には観測されたユーザ数の93%はファイバー利用者で、トラフィック量全体の96%を占めるまでになっています。

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。

3.3 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、2012年と2013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いますが、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。2012年と

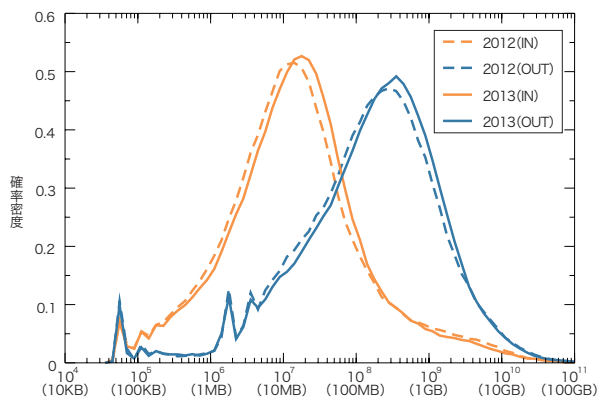


図-2 利用者の1日のトラフィック量分布
2012年と2013年の比較

2013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。

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が、ここ数年で、ピア型利用者の山は小さくなってきていますが、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2012年と2013年で比較すると、INでは14MBから18MBに、OUTでは282MBから355MB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れるので、2013年には、INの平均は397MB、OUTの平均は1038MBと、最頻出値よりかなり大きな値になります。2012年では、それぞれ410MBと1026MBだったので、平均値で見ると、INが減少して、OUTが増える傾向が続いています。

年	IN (MB/day)		OUT (MB/day)	
	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

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

図-3は、利用者ごとのIN/OUT使用量の中から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。

対角線の下側で対角線に沿って広がるクラスは、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がはっきり分かりましたが、今では識別が難しくなっています。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ウェブ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

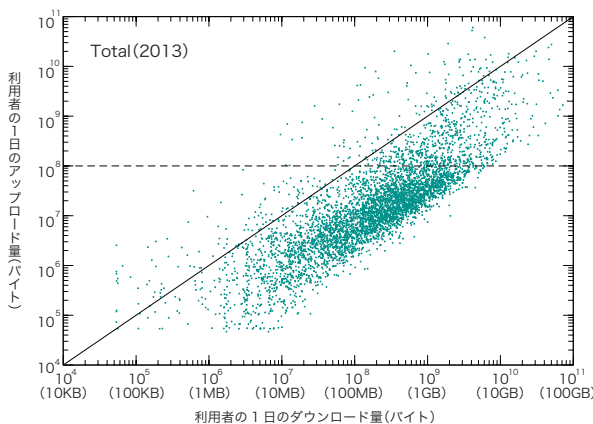


図-3 利用者ごとのIN/OUT使用量

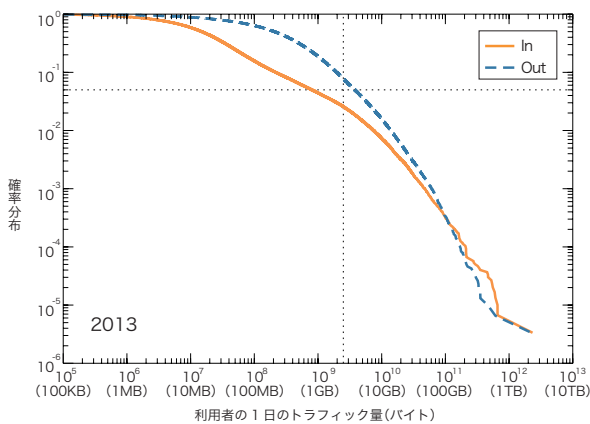


図-4 利用者の1日のトラフィック量の相補累積度分布

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、2012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。2012年と比較すると、グラフ右端のテール部分が若干右側に延びていて、昨年減った直線から右側に外れるような極端なヘビーユーザが再び観測されています。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71%、INの94%を占めています。更に、上位1%の利用者がOUTの32%、INの65%を占めています。

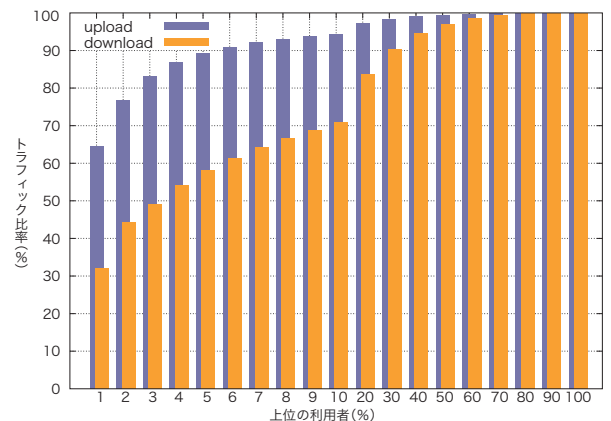


図-5 利用者間のトラフィック使用量の偏り

3.4 ポート別使用量

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、双方で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、少し荒っぽい方法ですが、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てします。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。

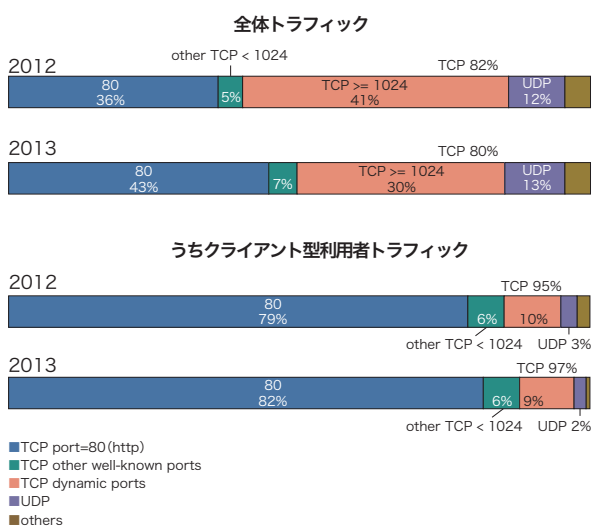


図-6 ポート別使用量概要

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、2012年と2013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。

2013年のトラフィックの80%はTCPです。更に、全体で見ると、2012年には総量の41%だったTCPの動的ポートが、2013年には30%にまで減少しました。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。逆に、80番ポートの割合は、2012年の36%から43%に増加しています。TCP以外のトラフィックのほとんどはVPN関連で、増加傾向にあります。

一方、クライアント型利用者に限ると、2012年には79%を占めていた80番ポートが、2013年には82%に増加しています。2番目に多いのは、HTTPSで使われる443番ポートで、2012年の3%から5%に増えています。これに対して、動的ポートの割合は、10%から9%に減少しています。

これらのデータから、TCP80番ポートのトラフィック増加傾向が一般利用者だけでなく、ヘビーユーザでも引き続き進行していることが確認できます。80番ポートにはビデオ

protocol port	2012		2013	
	total (%)	client type	total (%)	client type
TCP	81.86	95.09	79.79	96.91
(<1024)	41.23	85.25	49.57	88.15
80(http)	36.22	79.39	43.44	81.61
443(https)	2.45	3.43	3.90	4.80
554(rtsp)	0.77	1.01	0.51	0.58
22(ssh)	0.22	0.06	0.24	0.04
(>=1024)	40.63	9.84	30.22	8.76
1935(rtsp)	2.12	3.91	2.39	3.60
7144(peercast)	0.44	0.04	0.40	0.04
8080	0.30	0.17	0.34	0.19
UDP	12.38	2.94	13.21	2.12
ESP	5.29	1.79	6.54	0.88
GRE	0.16	0.14	0.20	0.06
IP-ENCAP	0.09	0.01	0.13	0.00
L2TP	0.14	0.00	0.09	0.00

表-2 ポート別使用量詳細

コンテンツやソフトウェアアップデートなども含まれているため、コンテンツタイプの特定はできませんが、クライアント・サーバ型の通信量が増えているのは明らかです。

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、2012年と2013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。2012年と比較すると、全体でも80番ポートの割合が更に増え、動的ポートの割合より大きくなってきているのが確認できます。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2012年と2013年を比較しています。クライアント型利用者では、大半が80番ポートで、ピーク時間は21時～23時となっており、昨年とほとんど違いは見られません。一方、ピア型利用者については、動的ポートの利用割合が減少しており、2013年には動的ポートが80番ポートより若干多い程度になっています。

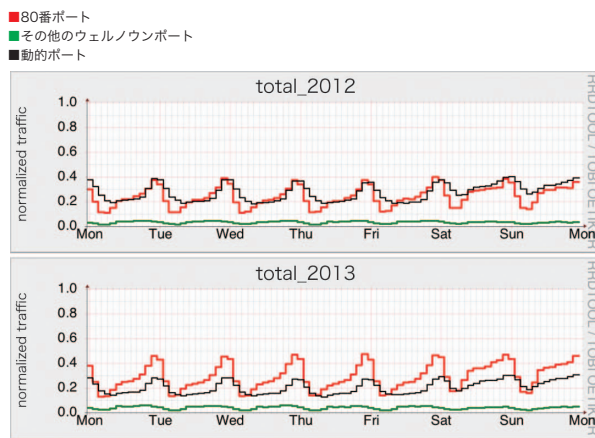


図-7 TCPポート利用の週間推移
2012年(上)と2013年(下)

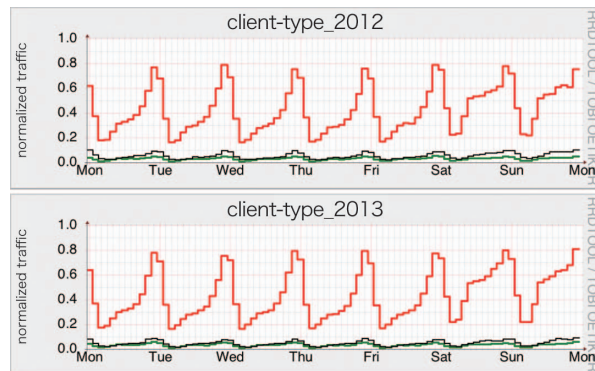


図-8 クライアント型利用者のTCPポート利用の週間推移
2012年(上)と2013年(下)

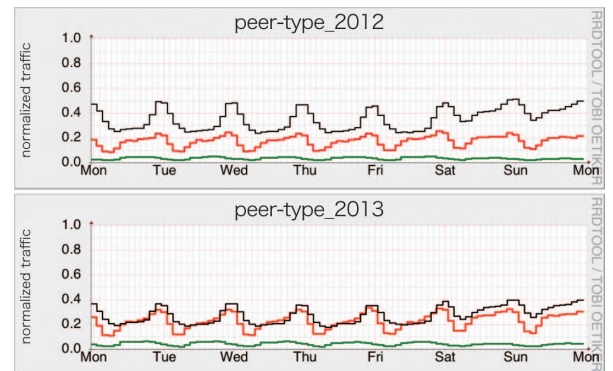


図-9 ピア型利用者のTCPポート利用の週間推移
2012年(上)と2013年(下)

3.5 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、2012年10月前後に増減があるものの、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16%増えました。アップロード量も2010年以降横ばいだったのが、8%の増加に転じました。また、TCP80番ポートの割合が更に増えていて、以前から報告しているWebサービスへの移行が一層進んだことが確認できます。

2012年10月1日に施行された違法ダウンロードの刑事罰化を盛り込んだ改正著作権法の影響は限定的でした。2010年1月のダウンロード違法化のときは、明らかにトラフィックの長期トレンドに影響が出ました。しかし、これは以前のレポートで議論したように、既にあった流れを加速するトリガーとなったに過ぎないという見方もできました。我々は、法的強制措置の効果を検証する意味で、今回の違法ダウンロードの刑事罰化の影響について注目していました。

結局、今回は、施行の前に駆け込みと思われるトラフィック増加が見られ、施行後3ヵ月程トラフィックが減少しま

したが、その後はもとのトレンド曲線に戻っています。マクロなトラフィック傾向だけで違法ダウンロードの増減を推測することはできませんが、今回の施行前後の増減は、一部ユーザの違法ダウンロード行動の反映と見ていいでしょう。しかし、3ヵ月で元のトレンド曲線に戻っていることや、他の数値からも特に傾向に大きな変化が見られないことを併せて考えても、今回のダウンロード刑事罰化は一時的な心理効果しかなかったように見えます。

法整備の役割には、技術的あるいは社会的な背景を持つユーザの行動変化の流れをうまくガイドする、という側面があります。その意味で、2010年の著作権法改正はWebサービスへの移行という流れに沿っており、対象ユーザにも受け入れられたため効果があったと考えられます。その一方で、2012年の改正は対象ユーザに受け入れられなかったように思われます。

IJでは、ユーザの利用形態の変化に迅速に対応できるよう、継続的なトラフィックの観測を行っています。今後も、定期的にレポートをお届けしていく予定です。

執筆者:



長 健二郎 (ちょう けんじろう)
株式会社IJ イノベーションインスティテュート 技術研究所所長。

インターネットトピック：IIJmio高速モバイル/Dサービスとオンラインチャージング

IIJがNTTドコモのLTE網を利用して2012年2月に開始したMVNO(仮想移動体通信事業者)サービス「IIJmio高速モバイル/Dサービス」。このサービスの最大の特徴は、これまでの定額制使い放題のモバイルサービスと異なり、従量制と定額制をミックスした独特な料金プランにあります。これにより、一部のヘビーユーザの重い設備コストをライトユーザが負担しなくてはならない従来のパケット定額料金の料金構造の常識を覆し、「モバイルで動画を見ない」「モバイルで大容量のファイル転送は行わない」というライトユーザ向けにリーズナブルな料金でサービスを提供できるようになりました。

この「IIJmio高速モバイル/Dサービス」の料金プランは、オンラインチャージングという課金の仕組みによって実現しています。従来の課金方式(オフラインチャージング)は、月の利用パケット数に対して後からその料金を算出する仕組みであり、本質的にバッチ処理です。これに対し、オンラインチャージングはどの程度の利用が可能であるか(利用権)をあらかじめ決め、リアルタイムに利用権の残りを計算しながら、利用権がなくなれば速やかにサービスの提供を終了します。例えるなら公衆電話でしょうか。公衆電話が利用権管理を端末側(公衆電話機)で行うのに対し、オンラインチャージングではその仕組みを網側で実装している点が唯一の違いかもしれません。

オンラインチャージングの仕様の標準化は、携帯電話技術の標準化プロジェクトである3GPPが担っています。3GPPが定めているPCC(Policy and Charging Control)システムアーキテクチャを図-1に示します。

ここでS-GW(LTE加入者パケット交換機)及びS-GWより左側の区間はIIJの設備ではなく、MNOであるNTTドコモの設備となります。P-GWは、MVNOが必ずしも導入する必要のない設備ですが、IIJではこの設備を自前で運用する構成(シ

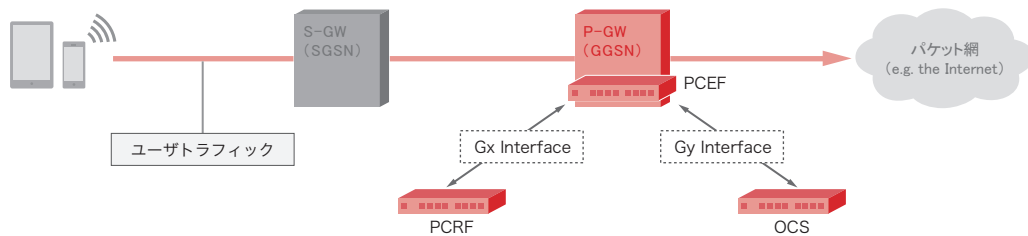
ヤ2MVNO)をとっています。P-GW(LTE閘門交換機)は高価で運用負荷も非常に高い装置ですが、これを導入するメリットは、今回構築したような新しい試み(世界でもほとんど例のない)を自由に企画し実現できることです。

まず、P-GWにはPCCをサポートしてPCEFがアドオンされたものを選定しました。このPCEFは、他の2つのサブシステムであるOCS、PCRFと連携し、P-GWを通過する通信に対して必要なポリシーを適用するネットワーク装置です。PCEFを通るお客様の通信には、例えば高速であるか、低速であるかなどのポリシーが適用されることとなります。

次にOCSは、お客様ごとに定義された利用権を管理します。IIJではこの利用権に対し「クーポン」という呼称をつけました。OCSはPCEFと継続的に通信することで、お客様のクーポンの残量を計算し格納します。これに対してPCRFは、お客様の通信ポリシーを管理します。OCSと連携し、クーポンを使い切ったお客様の通信に低速ポリシーを、翌月になりクーポンが付与されたお客様や追加でクーポンを購入されたお客様には高速ポリシーを、それぞれ適用すると決定した上でPCEFに指示を与えます。

この3つのサブシステムが連携して動作することで、「IIJmio高速モバイル/Dサービス」の料金プランは成立しています。このうちP-GW/PCEFは既製のネットワーク装置ですが、OCS、PCRFの2つは、ほぼIIJで独自に開発しました(ベースとなるDiameterサーバのみ既製品)。未だにOCSやPCRFに関する実装例やドキュメント、既製品などが非常に少ない中、これらを独自に開発したことで、非常にユニークな料金プランを世界に先駆けて提供できたと考えています。

なお、PCCを使わずに適用する通信ポリシーを切り替える方法として、APN(Access Point Name、端末から見た接続先識別のための文字列)を変更して通信ポリシーを切り替



PCCサブシステム名称		特徴
OCS	Online Charging System	<ul style="list-style-type: none"> お客様の通信量をリアルタイムに監視 決められた量の通信を行った端末に対し作動する「弁」
PCRF	Policy and Charging Rules Function	<ul style="list-style-type: none"> お客様の通信に適用されるポリシーをリアルタイムに管理 OCSと連携し、お客様の通信ポリシーを適時管理する
PCEF	Policy and Charging Enforcement Function	<ul style="list-style-type: none"> OCS、PCRFと連携し、お客様の通信にポリシーを適用するネットワーク装置

図-1 3GPPが定めているPCC(Policy and Charging Control)システムアーキテクチャ

える方法が考えられます。これは高速通信用APN、低速通信用APNなどを複数用意し、端末を網から切断し再接続して切り替える方法です。PCCに関するシステムが不要となる分、コストや運用負荷が下がることで若干のメリットはありますが、ポリシーの切り替えに際しては必然的に回線断を伴うことから、お客様にとっては通信が中断する、ポリシーの切り替えと通信の再開まで待たされる、といったデメリットもあります。これに対してIJmioのPCC実装は、PCEFを用いることで接続したまま(通信を中断せずに)ポリシーを切り替えることができるため、速度の切り替えに対して、よりストレスを感じない優れた方式であると思います。

■ IJmioクーポンスイッチアプリ「みおぼん」について

サービス開始当初、「IJmio高速モバイル/Dサービス」にはクーポンを能動的に切り替える機能はなく、クーポンがあれば高速通信、クーポンが尽きると低速通信という単純な制御のみでサービスを提供していました。その後、お客様から寄せられた要望により、クーポンがあってもお客様の操作次第で任意に低速通信状態に遷移できる機能を検討しました(図-2)。

PCCに求められた改修は大きなものではありませんでしたが、IJmioの利用者の多くがスマートフォンやタブレットで利用していることを考えると、クーポンを切り替えるアプリへのニーズは高いものと想定できたので、アプリからの切り替えに関する開発を行いました。

クーポンスイッチアプリには以下の機能が求められます。

- ・ クーポンのON/OFFを切り替えるためのUIの描画と実行
- ・ 操作対象の回線情報を収集し、クーポンのON/OFFを切り替えるためのWebAPIの実行

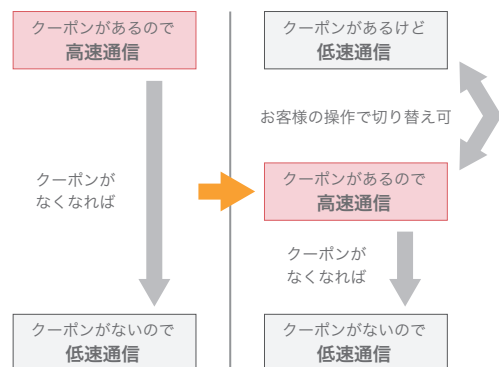


図-2 クーポンスイッチアプリによる状態遷移の変化

- ・ IDとパスワードを送信してIJmioの契約者であることを認証し、WebAPIへのアクセス認可(アクセストークン)を取得する仕組み

iOSとAndroidのクロスプラットフォーム開発の試みとして、これらの機能はHTML5ベースで実装しました。またクーポンスイッチアプリもすべてIJで独自開発しています。このように、社内でのモバイルアプリ開発における技術力向上を図ることで、機能拡張やUI改修が容易に行えるといったメリットを享受しています。

なお、クーポンスイッチアプリについては、何よりストレスなく実行し操作できるユーザビリティが求められることから、機能を必要最小限のものに絞り、UIを直感的に操作できるシンプルなものにしました(図-3)。IJmioのPCEFによる高速かつシームレスな速度切り替えと相まって、極めて快適に速度切り替えを実施していただけるものとなっています。「みおぼん」のインストールベースは、アプリ公開後3ヵ月間で3万(Android/iOSの合計)件に達し、App StoreやGooglePlayストアでの評価が4.5点以上と好評価をいただくなど、多くのお客様に日常的にご愛用いただいています。

■ 終わりに

「IJmio高速モバイル/Dサービス」は、MVNOとして既存の携帯電話事業者のいずれにも前例のない新しい料金プランを導入したという点で、極めてエポックメイキングなサービスであると思います。2012年2月のサービス開始以降も着実にサービスの新規展開や改善・改良を続けていますが、これにはIJの構築したPCCを始めとするシステムの柔軟性の高さが大きく寄与しています。今後とも多くのお客様にご利用いただけるよう、新しい試みに取り組んでいきたいと思っています。



図-3 クーポンスイッチアプリの操作画面

執筆者:



佐々木 太志(ささき ふとし)

IJ ネットワーク本部 ネットワークサービス部 モバイルサービス課 担当課長。2000年入社。ネットワークサービスの運用、運営に従事し、2007年にはIJモバイルの立ち上げに参加。その後IJmio高速モバイル/Dサービスの企画を担当。Twitterの公式アカウント@ijmioの中の人も務める。

株式会社インターネットイニシアティブ(IIJ)について

IJ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

〒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@ij.ad.jp URL: <http://www.ij.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。

©2008-2013 Internet Initiative Japan Inc. All rights reserved.

IJ-MKTG019TA-1308GR-09000PR