ホームルータのセキュリティ

**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IIJが取得した一般情報、インシデントの観測情報、サービスに関連する情報、協力関係にある企業や団体から得た情報を元に、IIJが対応したインシデントについてまとめたものです。今回のレポートで対象とする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。

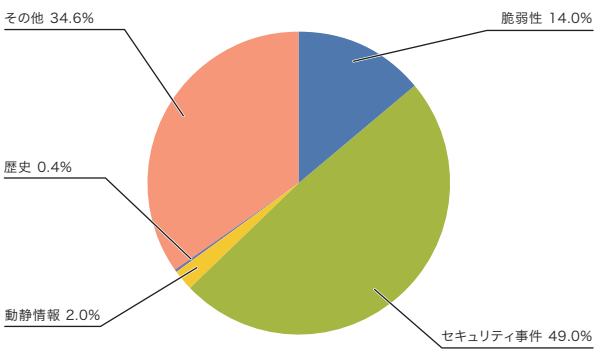


図-1 カテゴリ別比率(2013年4月〜6月)

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IIJが取り扱ったインシデントと、その対応を示します。まず、この期間に取り扱ったインシデントの分布を図-1に示します[*1]。

■ Anonymousなどの活動

この期間においてもAnonymousに代表されるHacktivistによる攻撃活動は継続しています。様々な事件や主張に応じて、多数の国の企業や政府関連サイトに対するDDoS攻撃や情報漏えい事件が発生しました。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(OpIsrael)、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見つかり、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、複数の脆弱性が見つ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した。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.jpcert.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.jpcert.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に対策を！」(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.jpcert.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**：goolID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して、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goolID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、「goolID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ことが分かり、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リーボードより、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.jpcert.or.jp/at/2013/at130018.html）。

12 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）。

13 脆 **10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。
「APSB13-11: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）。

14 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）。

15 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、移動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）。

16 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カウントに、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。

17 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。

18 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）。

19 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）。

20

21 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）。

22

23 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。

24 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。

25 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のサーバー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）。

26 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）。

27 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。

28 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。

29 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。

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

■ 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
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31

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。
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/)。

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。
「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)。

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)。

セ **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。

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)。
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)。

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。
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/)。

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。
「2013 年 5 月のセキュリティ情報」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-May)。

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。
「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)。

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。
「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)。

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。
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)。

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。
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)。

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。
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/)。

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。

セ **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。

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アンプによる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。
"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)。

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。

[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は匿名のまま仮想の通貨を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
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30

セ **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)。

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/)。

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)。

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)。

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)。

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)。

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)。

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(ビックデータ)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)。

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/cq06101845.html)。

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)。

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)。

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てい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 ontvreemden containers met coca?ne」(http://www.om.nl/actueel/nieuws-persberichten/@161061/drugshandelaren/)(オランダ語)。

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)。

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)。

セ **19日**：Opera社は、標的型攻撃により侵入され、コードサイニング証明書を盗まれたことを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た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)。

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/)。

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)。

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/)。

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カウントにアクセスしたとして、書類送検された。

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？我々が得るべき教訓は？」(http://blog.trendmicro.co.jp/archives/7462)。

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)。

[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、捜査が終結しました。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されるメールアカウント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こり、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IIJ DDoS対策サービスで取り扱ったDDoS攻撃の状況を示します。

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

DDoS攻撃には多くの攻撃手法が存在し、攻撃対象となった環境の規模(回線容量やサーバの性能)によって、その影響度合が異なります。図-2では、DDoS攻撃全体を、回線容量に対する攻撃[*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ヵ月間でIIJ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も大規模な攻撃は、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。

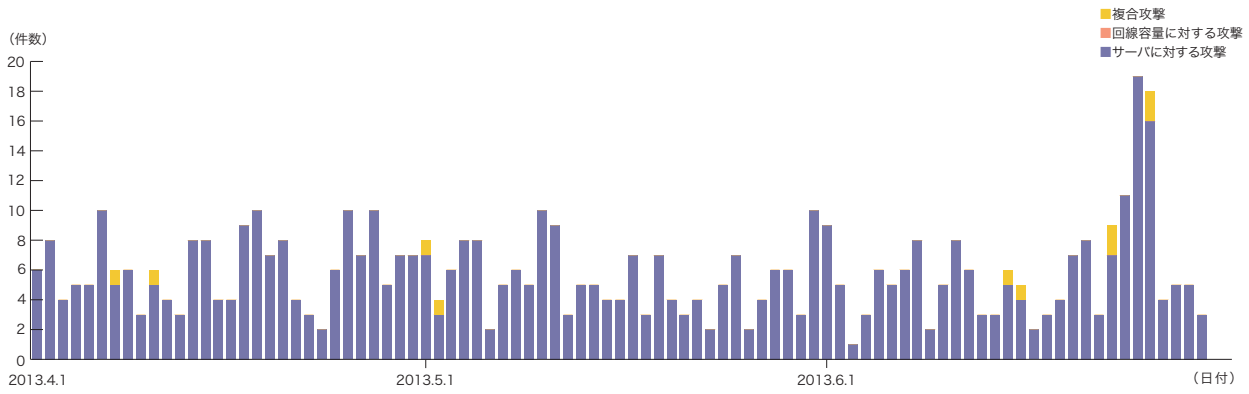


図-2 DDoS攻撃の発生件数

*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

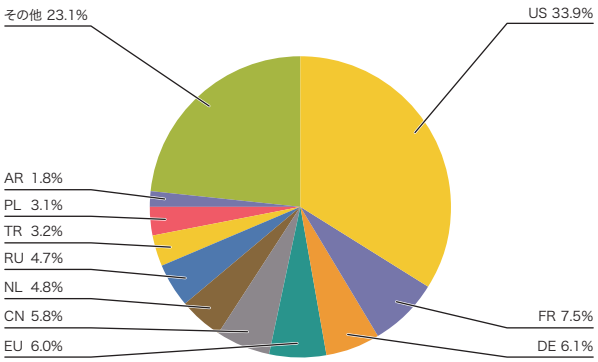


図-3 backscatter観測によるDDoS攻撃対象の分布（国別分布、全期間）

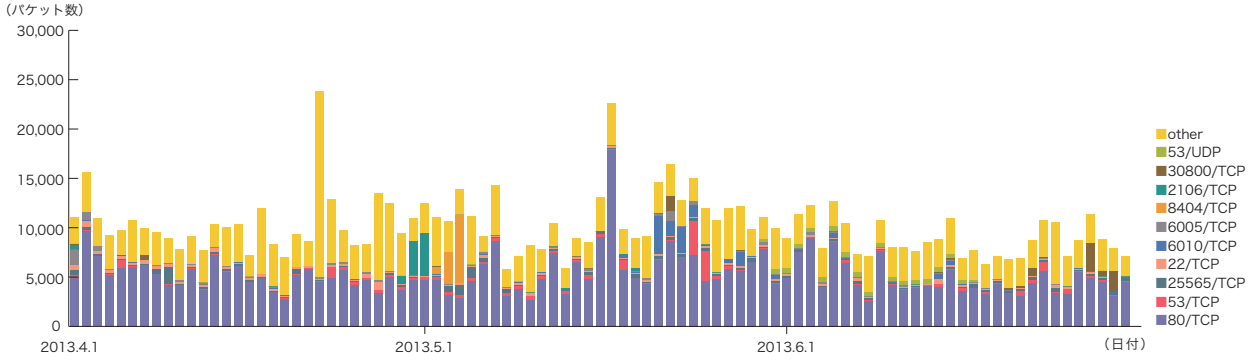


図-4 DDoS攻撃によるbackscatter観測(観測パケット数、ポート別推移)

*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.iij.ad.jp/development/iir/pdf/iir_vol08.pdf)の「1.4.2 DDoS攻撃によるbackscatterの観測」で仕組みとその限界、IIJによる観測結果の一部について紹介している。

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、IIJ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、IIJが実施しているマルウェアの活動観測プロジェクトMITF[*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[*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。

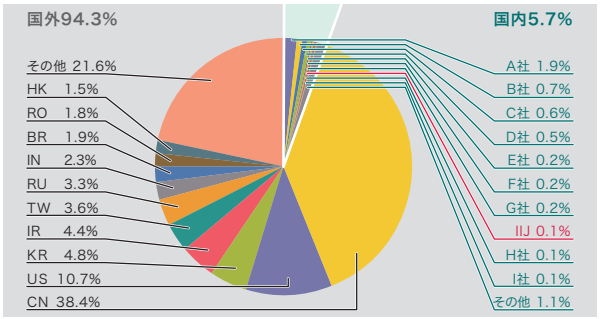


図-5 発信元の分布(国別分類、全期間)

■ 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による探査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

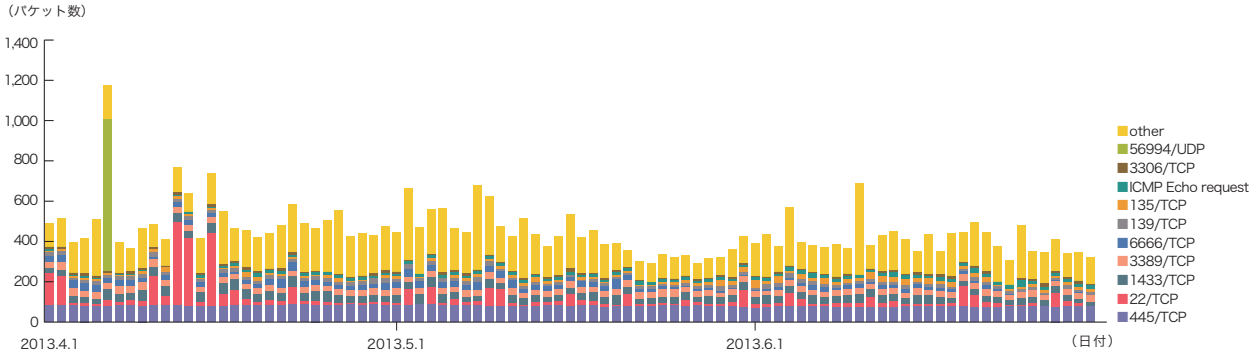


図-6 ハニーポットに到着した通信の推移(日別・宛先ポート別・1台あたり)

*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、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宛て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、その探査行為であると考えられます。

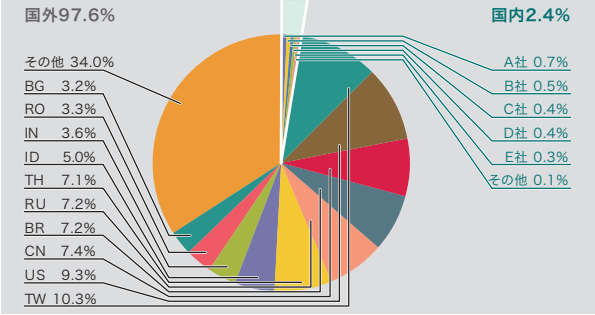


図-7 検体取得元の分布(国別分類、全期間、Conficker除く)

■ 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。

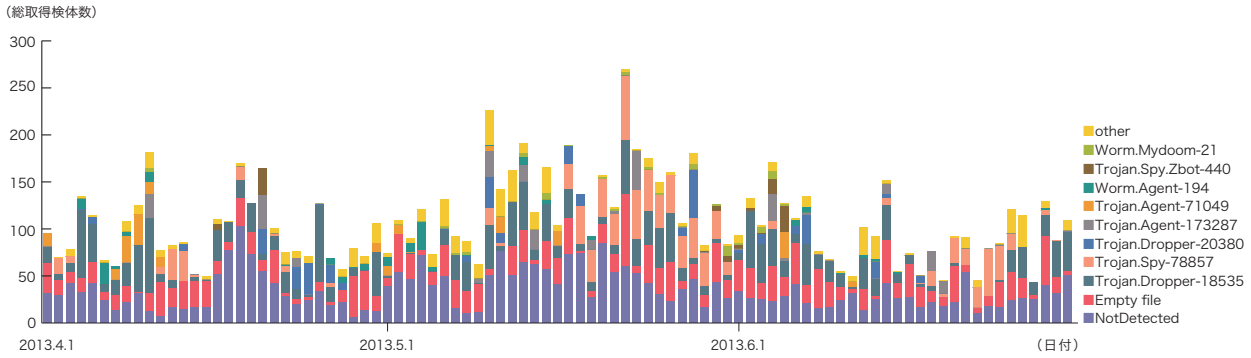


図-8 総取得検体数の推移(Conficker除く)

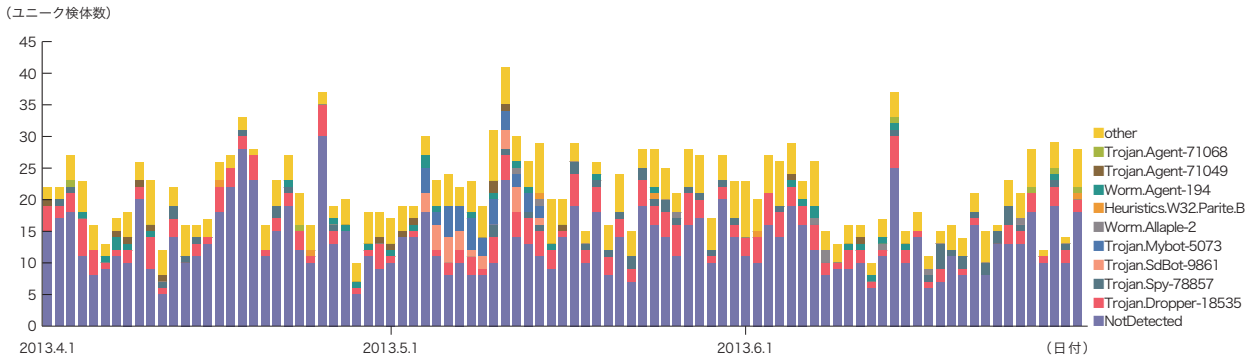


図-9 ユニーク検体数の推移(Conficker除く)

*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%、ダウンローダ型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IIJ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

IIJでは、Webサーバに対する攻撃のうち、SQLインジェクション攻撃[*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、IIJマネージドIPSサービスのシグネチャによる攻撃の検出結果をまとめたものです。

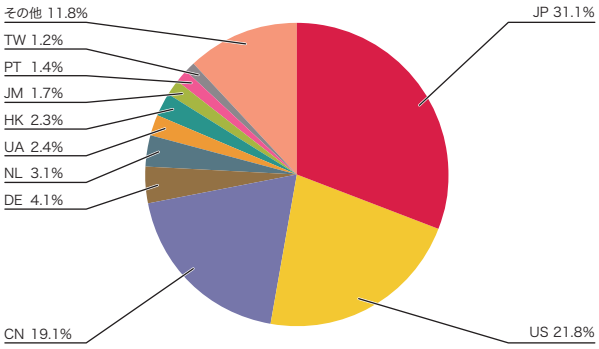


図-10 SQLインジェクション攻撃の発信元の分布

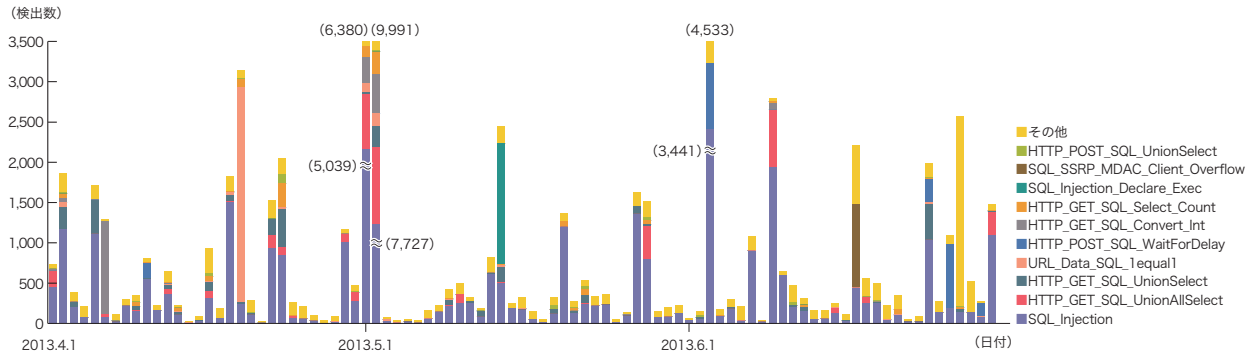


図-11 SQLインジェクション攻撃の推移(日別、攻撃種類別)

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。

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

*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、IIJでは、流行したインシデントについて独自の調査や解析を続けることで対策につなげています。ここでは、これまでに実施した調査のうち、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。昨年の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、IIJ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

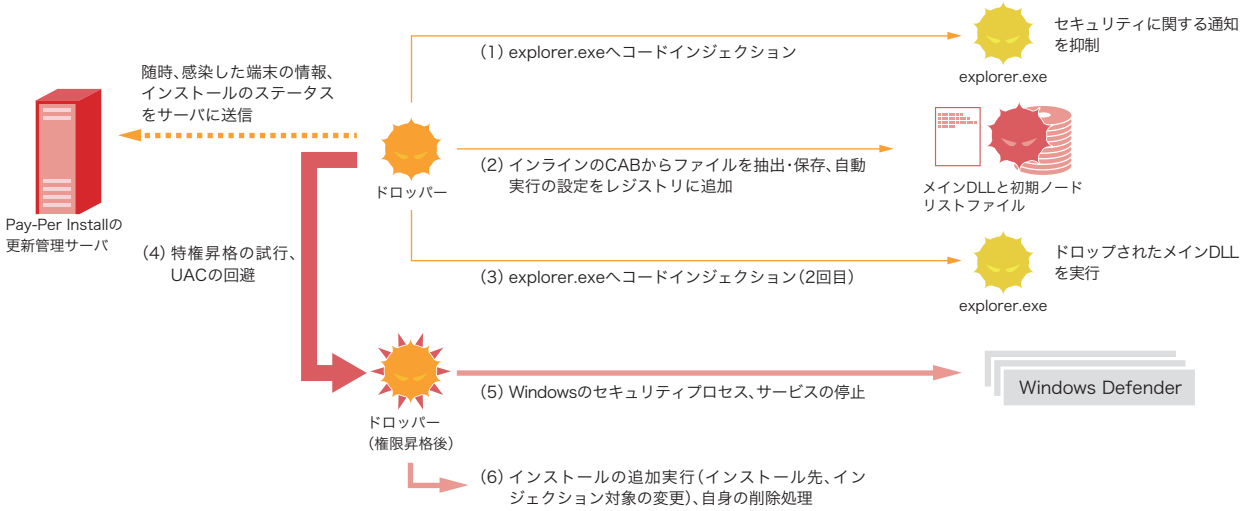


図-12 ユーザモード型ZeroAccessの動作(ドロッパー)

*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、IIR Vol.13「1.4.2 SpyEye」(http://www.iij.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、IIR Vol.16「1.4.3 ZeuSとその亜種について」(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol16.pdf)や、IIR Vol.18「1.4.2 ZeuSの亜種Citadel」(http://www.iij.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IIJ Technical Weekで解説している。「IIJ 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.iij.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係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でボ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

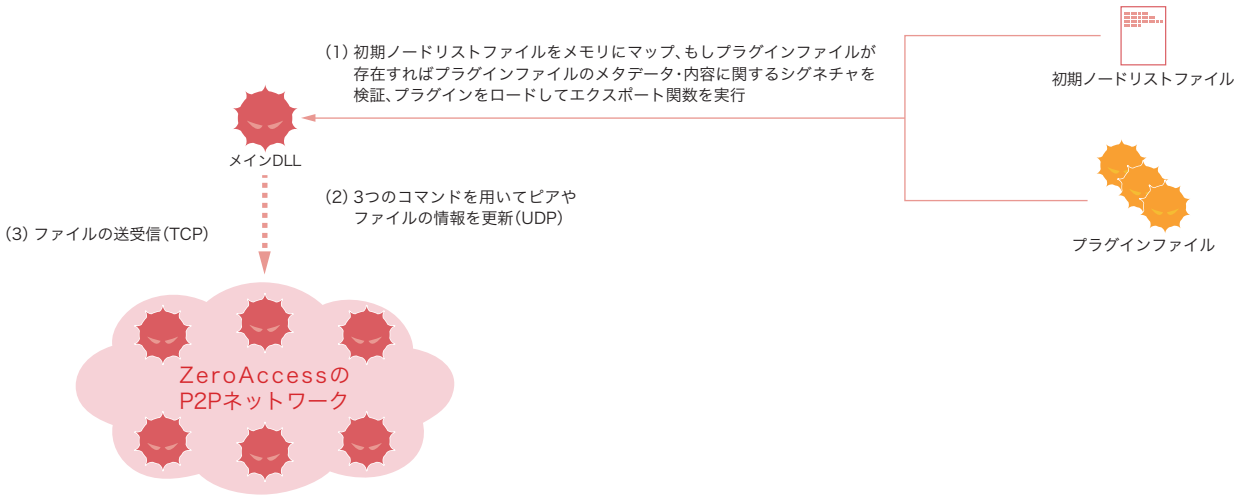


図-13 ユーザモード型ZeroAccessの動作(インストールされたDLL)

*51 IIJ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。GeoIP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でボットコマンドの送受信を行いますが、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変化しない限り固定のものです。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ので、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、通常パ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つ注意するべきことは、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。

今回はユーザモード型ZeroAccessの動作とそのIOCに関する考察を行いましたが、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はいかがでしょうか。

＊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（新しいピアをボ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アンプ攻撃（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はなく、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アンプ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IIJ-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.iij.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）。

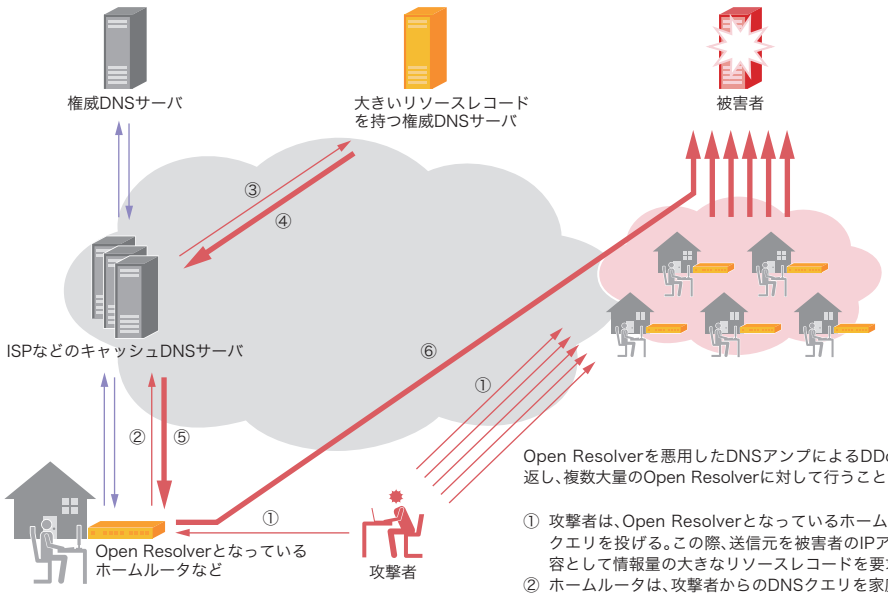
*63 DNS Changerマルウェアについては、IIR Vol.15（http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol15.pdf）の「1.4.2 DNS Changerマルウェア」も参照のこと。また、銀行など個別サーバへのアクセスを不正サイトに誘導しようとした事件としては、例えば2012年にメキシコで発生した次の事件がある。トレンドマイクロ社、"Targeted Attack in Mexico: DNS Poisoning via Modems"（http://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attack-in-mexico-dns-poison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

提供してしまうことになります(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、IIJ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]。



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。

Open Resolverを悪用したDNSアンプによるDDoS攻撃では、次の手順を繰り返し、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。

図-14 DNS Open Resolverを踏み台としたDNSアンプによる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-pr-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JVN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。JVN、「JVNVU#90348117 Portable SDK for UPnP にバッファオーバーフローの脆弱性」(https://jvn.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プロトコルに応答する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になります。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討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。

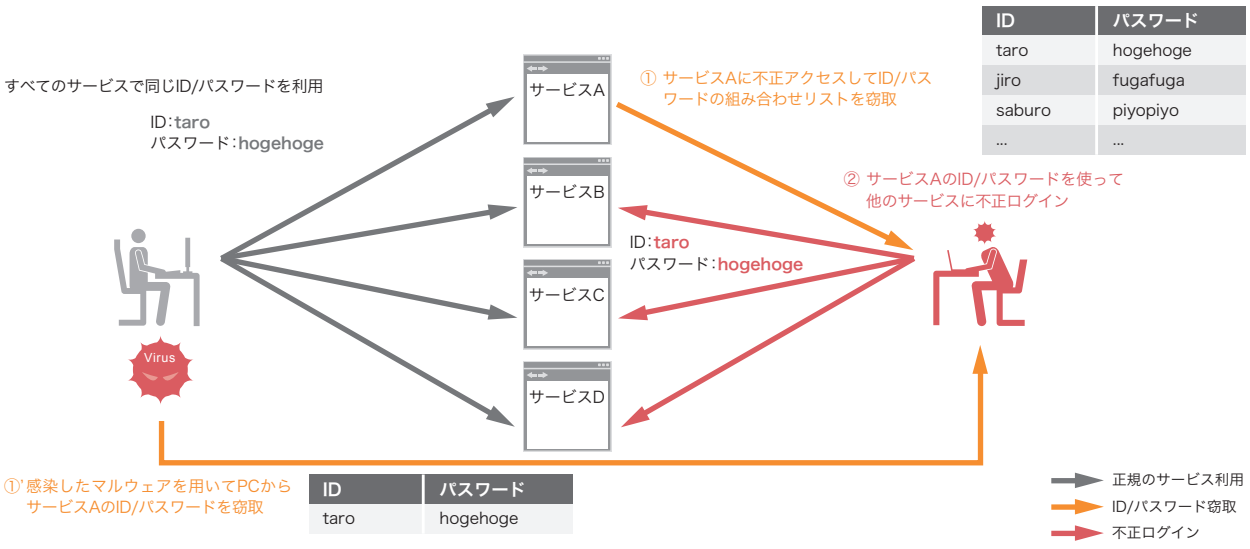
ここで検討したような対応策の実現には、少なからず時間が必要です。今すぐにはじめられる対策として、一般の利用者に現状のホームルータの機能を用いてその健全性を確認することを促す努力が、複数のセキュリティ団体、インターネット関連団体、ISPなどにより開始されています。

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」「aaac」...)「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



ID	パスワード
taro	hogehoge
jiro	fugafuga
saburo	piyopiyo
...	...

ID	パスワード
taro	hogehoge

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、リスト型攻撃はきわめて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ー

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	事件の分類	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.iij.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な状態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、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、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。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などに従事の後、2001年よりIIJグループの緊急対応チームIIJSECTの代表として活動し、CSIRTの国際団体であるFIRSTに加盟。Telecom-ISAC Japan、日本シーサート協議会、日本セキュリティオペレーション事業者協議会など、複数の団体の運営委員を務める。

土屋 博英(1.2 インシデントサマリ)
土屋 博英、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)
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、齋藤 聖悟 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