IIJ
Internet Initiative Japan

Internet Infrastructure Review Vol.21

November 2013

インフラストラクチャセキュリティ

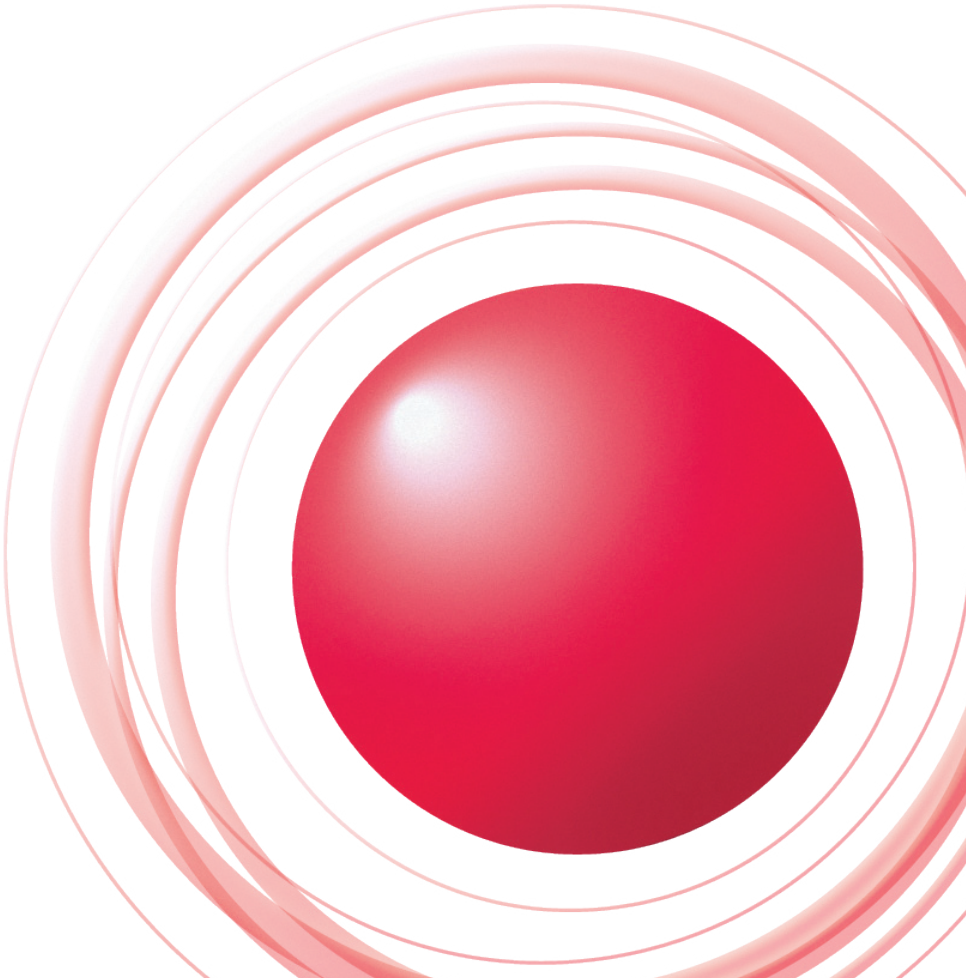
標的型攻撃で利用されるRAT「PlugX」

インターネットオペレーション

DNS オープンリゾルバ問題

クラウドコンピューティングテクノロジー

「SDN」の最新動向



Internet Infrastructure Review

Vol.21 November 2013

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

エグゼクティブサマリ

インターネットが社会インフラであると考えられるようになってから、既に10年以上が経ちました。インフラというと固定的で安定したものというイメージがありますが、今も成長し続けています。例えばブロードバンドトラフィック量に関して見ると、2012年から2013年にかけて17%も増加していますし、スマートフォンの契約数は2012年度の4878万台から2013年末には6508万台に増加するという予測もあります。このような状況から、インターネットというインフラは、広く国民生活に浸透しており、かつ、更に新たな利用方法やコンテンツを導入しながら、日々成長し続けているインフラだと言えるでしょう。

インターネットというインフラのもう1つの大きな特徴として、インフラ機能の運営からその上のサービスに至るまで、かなりの部分がソフトウェアにより実装され、制御されているという点が挙げられます。更に、それらのソフトウェアの運用がユーザにも広く解放されたオープンな形態で行われており、そのことがインターネットに大きな柔軟性や拡張性をもたらしている一方、本レポートにもいくつか示されているように、脆弱性や悪意を持った攻撃の可能性をもたらしてしまっている、とも言えます。更に、ここ数年SDN(Software Defined Networking)という考え方が導入され、ネットワークのインフラの運用やサービスの実現を更に柔軟に、ソフトウェア制御ができるようにしよう、という動きも出てきています。

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

「インフラストラクチャセキュリティ」の章では、2013年7月から9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、標的型攻撃で利用されるRAT「PlugX」について、連続する標的型メール攻撃について、仮想通貨Bitcoinについて解説します。

「インターネットオペレーション」の章は、これまで「メッセージングテクノロジー」というタイトルで、迷惑メールに関する統計情報や技術情報をご提供しておりましたが、今後は迷惑メールに関する報告は年1回とさせていただきます。代わりに、この章はタイトルを刷新し、広くインフラやサービス関連の取り組みについてご報告いたします。今回は、大規模なDDoS攻撃を行うための手法として最近よく用いられているDNS amp攻撃について解説し、この攻撃の踏み台として使われるオープンリゾルバの問題について考察します。

「クラウドコンピューティングテクノロジー」の章では、仮想ネットワークをソフトウェアにより構築、運用するための技術である、SDNの最新動向を紹介します。また、IIJの関連会社であるストラトスフィア社で開発を進めているOmniSphereという、オフィスLAN環境にSDNを適用する製品の概要と、ソフトウェアの内部構成について簡単に紹介します。

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

執筆者:

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

標的型攻撃で利用されるRAT「PlugX」

今回は、標的型攻撃で利用されるRAT「PlugX」について紹介すると共に、連続する標的型メール攻撃の実例とその対策、一部のインターネット利用者の間で新しい通貨として流通し始めている仮想通貨Bitcoin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7月から9月までの期間では、太平洋戦争の歴史的日付に関連して大規模な攻撃が予測されていましたが、一部Webサイト改ざんなどの被害を除いて、全体としては小規模な攻撃にとどまりました。しかし、AnonymousなどのHacktivismによる攻撃は複数発生しています。Webサーバへの不正侵入とそれによるWebサイトの改ざんや情報漏えいも相次ぎました。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発生しています。DNS Open Resolverの探査やそれを悪用したDDoS攻撃についても確認されています。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。

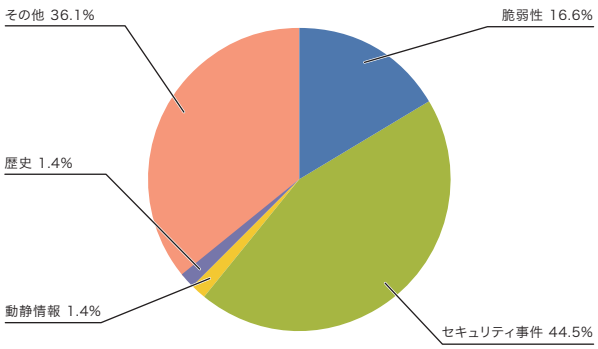


図-1 カテゴリ別比率(2013年7月〜9月)

1.2 インシデントサマリ

ここでは、2013年7月から9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。主な攻撃としては、米国政府や関連するWebサイトへの攻撃が複数発生し、米議会関係者のメールアドレスとパスワードや米緊急事態管理庁(FEMA)の情報が漏えいするなど、アカウント情報や内部情報の情報漏えいが発生しています(OpLastResort)。8月にはパキスタンとインドの独立記念日前後でお互いの政府や関連するWebサイトへの攻撃が多く発生しました[*2]。この攻撃では、政府機関のWebサイトだけでなく、パキスタン軍のFacebookページが改ざんされるなど、政府関連の外部のSNSサービスなどにも攻撃が波及しています。

9月には、主に南米の各国政府とその関連サイトに対して、それぞれの国のAnonymousによる攻撃が継続して行われました。また、Syrian Electronic Armyによると考えられる、トルコの政府機関を含む関連サイトへの攻撃も継続して発生しています。更に、7月から再開した米銀行へのDDoS攻撃(Operation Ababil)の第4弾など、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。

*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 これらの攻撃については、次のHackmageddon.comなどでまとめられている。"Timeline of Cyber Attacks in Conjunction with the Pakistan and India Independence Days"(http://hackmageddon.com/2013/08/22/timeline-of-cyber-attacks-in-conjunction-with-the-pakistan-and-india-independence-days/)。

■ 脆弱性とその対応

この期間中では、Microsoft社のWindows[*3][*4]、Internet Explorer[*5][*6][*7]、Office[*8][*9]などで修正が行われました。Adobe社のAdobe FlashPlayer、Adobe Reader及びAcrobat、Shockwave Player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。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、Microsoft社のSharePoint Server[*10]にリモートから細工されたパケットを受信することで任意のコード実行が可能な脆弱性を含む複数の脆弱性の修正や、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、細工されたリクエストに対する処理により、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。

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。これらの脆弱性の悪用も含め、更新されていないCMSアプリケーションを利用しているWebサイトで改ざんが多く発生していることから、IPAから注意喚起が行われています[*11]。

■ 動静や歴史的背景による攻撃

この期間では毎年、太平洋戦争の歴史的日付や、竹島や尖閣諸島などに関連したインシデントが発生しています。本年も攻撃予告などの情報から、これらに関連した日本国内の複数の政府機関や民間企業のWebサイトに対し、SQLインジェクションや、ブルートフォースなどによる侵入による改ざんやDDoS攻撃が発生することが予測されたため、警戒を行いました。しかしながら、一部のWebサイトで改ざんが発生したことが報道などで確認されましたが、大規模な攻撃の発生は確認されていません。

IIJの観測した攻撃では、9月17日に最大で3Gbps弱のUDP FloodとSYN FloodによるDDoS攻撃を確認しており、これ以外にも、比較的短時間の大規模な攻撃を複数確認しています。また、9月18日の前後には、DDoS攻撃が平常時よりも多く見られました。しかしながら、攻撃の規模や回数は昨年の同期間に比べるとかなり減少しています。

例年に比べて大規模な同時多発的攻撃が発生しなかった理由は定かではありませんが、2010年や2012年の同時期の状況とは異なり、日本と近隣諸国との間で、攻撃のきっかけとなるような大きな事件が発生しなかったためではないかと考えられます。

---

*3 「マイクロソフト セキュリティ情報 MS13-053 - 緊急　Windows カーネルモード ドライバーの脆弱性により、リモートでコードが実行される (2850851)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-053)。

*4 「マイクロソフト セキュリティ情報 MS13-060 - 緊急　Unicode スクリプト プロセッサの脆弱性により、リモートでコードが実行される (2850869)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-060)。

*5 「マイクロソフト セキュリティ情報 MS13-055 - 緊急　Internet Explorer 用の累積的なセキュリティ更新プログラム (2846071)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-055)。

*6 「マイクロソフト セキュリティ情報 MS13-059 - 緊急　Internet Explorer 用の累積的なセキュリティ更新プログラム (2862772)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-059)。

*7 「マイクロソフト セキュリティ情報 MS13-069 - 緊急　Internet Explorer 用の累積的なセキュリティ更新プログラム (2870699)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-069)。

*8 「マイクロソフト セキュリティ情報 MS13-054 - 緊急　GDI+ の脆弱性により、リモートでコードが実行される (2848295)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-054)。

*9 「マイクロソフト セキュリティ情報 MS13-068 - 緊急　Microsoft Outlook の脆弱性により、リモートでコードが実行される (2756473)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-068)。

*10 「マイクロソフト セキュリティ情報 MS13-067 - 緊急　Microsoft SharePoint Server の脆弱性により、リモートでコードが実行される (2834052)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-067)。

*11 IPA、「WordPressやMovable Typeの古いバージョンを利用しているウェブサイトへの注意喚起」(http://www.ipa.go.jp/security/topics/alert20130913.html)。「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)。

7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**：韓国で、6月25日に続きメディア関連企業を含む複数のWebサイトが改ざんされる攻撃が発生した。
この事件の詳細については、例えば次のnprotect's Blogを参照のこと。[긴급]6.25 사이버전, 국내 주요 사이트 해킹 공격 받는 중 Update # 130701-21（http://erteam.nprotect.com/429）（韓国語）。

セ **1日**：マレーシアのドメインである.myのドメインレジストリであるMYNICが何者かによる不正アクセスを受け、Microsoftや Dellといった有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。
この事件の詳細については次のMYNICの発表を参照のこと。".my DOMAIN NAME INCIDENT RESOLVED"（http://mynic.my/en/news.php?id=155）。

セ **2日**：宇宙航空研究開発機構（JAXA）は4月に発生した不正アクセスに関する調査結果を公表した。
宇宙航空研究開発機構、「JAXAのサーバーに対する外部からの不正アクセスに関する調査結果について」（http://www.jaxa.jp/press/2013/07/20130702_security_j.html）。

セ **3日**：研究者により、モトローラ社の携帯端末で、利用者が意図しない個人情報の収集が行われていることが報告された。この報告では外部のWebサービスのアカウント情報などを含む個人情報がモトローラ社関連のドメインのホストに送信されているとしている。
詳細については、次の発見者であるBen Lincoln氏のBlogを参照のこと。Beneath the Waves, "Motorola Is Listening"（http://www.beneaththewaves.net/Projects/Motorola_Is_Listening.html）。

脆 **4日**：Androidでアプリケーションが正当なものであるかどうかを判断するために使われている署名に脆弱性があることが公表され、多くのデバイスに影響があるとの報告がされた。この脆弱性については、8月に行われたBlack Hat USA 2013で詳細が公表された。
詳細については、次のBlack Hat USA 2013でのJeff Forristal氏の発表を参照のこと。Android: One Root to Own Them All（https://media.blackhat.com/us-13/US-13-Forristal-Android-One-Root-to-Own-Them-All-Slides.pdf）。

他 **4日**：総務省のICT成長戦略会議より、ICTによる経済成長と国際社会への貢献への重点ポイントをまとめたICT成長戦略が公表された。
「『ICT成長戦略』の公表」（http://www.soumu.go.jp/menu_news/s-news/01tsushin01_02000108.html）。

セ **9日**：ベルギー（.be）のドメインレジストリであるdns belgiumのWebサーバのコンテンツが何者かに改ざんされる事件が発生した。この事件では、DNS登録情報での被害はなかったとしている。
詳細については、次のdns belgiumからの発表も参照のこと。"Deface hack on DNS.be website"（http://www.dns.be/en/news/recent_news/deface-hack-on-dnsbe-website2#.UlyiaVBzPkc）。

セ **9日**：オランダ（.nl）のドメインレジストリであるSIDNは、SQLインジェクション攻撃による不正アクセスを受け、いくつかのサービスを停止したことを公表した。また、予防保全のため、全レジストラのパスワードをリセットする対応を実施した。

脆 **10日**：Microsoft社は、2013年7月のセキュリティ情報を公開し、MS13-053やMS13-055を含む6件の緊急と1件の重要な更新をリリースした。
「2013 年 7 月のセキュリティ情報」（http://technet.microsoft.com/ja-jp/security/bulletin/ms13-jul）。

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。
「APSB13-17: 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/apsb13-17.html）。

他 **11日**：一般社団法人JPCERT コーディネーションセンターは、2013年4月から6月のインシデント報告対応レポートを発表し、不審なiframeや難読化されたJavaScript がページに挿入された改ざんされたと考えられるWebサイトが非常に多く報告された。
「JPCERT/CC インシデント報告対応レポート [2013年4月1日～2013年6月30日]」（http://www.jpcert.or.jp/pr/2013/IR_Report20130711.pdf）。

脆 **17日**：Oracle社は、Oracleを含む複数製品について、四半期ごとの定例アップデートを公開し、合計89件の脆弱性を修正した。
"Oracle Critical Patch Update Advisory - July 2013"（http://www.oracle.com/technetwork/topics/security/cpujuly2013-1899826.html）。

脆 **17日**：Apache Strutsに第三者によるリモートから任意のOSコマンドの実行が可能な脆弱性（CVE-2013-2251）を含む複数の脆弱性が見つかり、修正された。
例えば次のJPCERTコーディネーションセンターからの注意喚起を参照のこと。「JPCERT/CC Alert 2013-07-19 Apache Struts の脆弱性 (S2-016) に関する注意喚起」（http://www.jpcert.or.jp/at/2013/at130033.html）。

セ **17日**：米国Network Solutions社が大規模なDDoS攻撃を受け、ユーザのページが閲覧できないなどの影響が発生した。
事件については、次のNetwork Solutions社の発表を参照のこと。"A Note to Our Customers"（https://www.networksolutions.com/blog/2013/07/a-note-to-our-customers/?channelid=P99C425S627N0B142A1D38E0000V100）。

セ **19日**：GitHubが大規模なDDoS攻撃を受け、サービスを停止する事件が発生した。
この事件については、次のGitHub Statusで概要を確認することができる。"Status Messages"（https://status.github.com/messages/2013-07-19）。

脆 **27日**：BIND 9.7系以上に、不正なRDATAを含む特別に細工されたクエリにより、サービスを停止することのできる脆弱性が見つかり、修正された。BIND 9.7については、既にEOLとなっていたため、本脆弱性が修正されたバージョン（BIND 9.8.5-P2/9.9.3-P2）への更新が推奨された。
Internet Systems Consortium、「CVE-2013-4854 [JP]: 特別に細工されたクエリによってBINDが異常終了する」（https://kb.isc.org/article/AA-01023）。

セ **28日**：ベルギー（.be）のドメインレジストリであるdns belgiumのWebサーバのコンテンツが再び何者かに改ざんされる事件が発生した。
詳細については、次のdns belgiumからの発表も参照のこと。"A detailed account of the hack on DNS.be"（http://www.dns.be/en/news/recent_news/a-detailed-account-of-the-hack-on-dnsbe#.Ul0wxFBzPkc）。

［ 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

この期間でも、本年3月頃から多数発生している、IDとパスワードのリストを使用したと考えられるなりすましによる不正ログインの試みと、ユーザのIDとパスワードの窃取を狙った試みが継続して発生しています[*12]。

本期間では、通信販売のサイトや携帯向けSNSなどの会員向けサービスサイト、ゲーム関連企業や旅行関連の会員向けサービスサイトなど多くのWebサイトに対し、不正なログインの試みが行われる事件が多く発生しています。これらの事件の多くでは、不正なログインにより登録情報の閲覧が行われた可能性があり、一部では不正にポイントなどが利用される事件も発生しています。

IDとパスワードの取得を目的とした事件では、複数のSNSサイトで発生した不正アクセス事件では、海外の警察と協力の上で犯人を特定し、不正に取得されたデータの第三者への流出がないことの確認や、データの消去といった対応が行われたことが公表されました。

これらの事件の一部では、脆弱性などを利用して侵入され、会員情報が漏えいしただけでなく、そのWebサイトが改ざんされて、フィッシングや迷惑メールの送信などといった別の事件に利用されるなどの被害も発生しており、今後も引き続き注意が必要と考えられます。

■ DNS Open Resolverの通信

この期間では、DNS Open Resolverの探査の試みや攻撃がいくつか確認されています。DNS Open Resolverを踏み台としたDNSアンプによるDDoS攻撃については、本年3月に発生した、迷惑メール対策組織であるSpamhausに対する大規模なDDoS攻撃が話題となりましたが、IIJでも最大で3GbpsのDNSアンプによるDDoS攻撃を確認しており、その後も継続して同様の事件が複数発生しています。

9月には警察庁より、中国を発信元とする53/UDPに対するアクセスが増加しているとして注意喚起が行われました[*13]。図-2にハニーポットに到着した53/UDPの通信について、発信元IPアドレスの国別分類を示します。これに示した通り、9月10日以降中国を送信元とした通信が非常に多くなっていることが確認できます。また、これらの通信について確認を行ったところ、特定のいくつかのIPアドレスを送信元として、複数のドメイン名の名前解決を試みる通信が行われていました。これらの通信で問い合わせに使われたドメイン名は、情報量の大きなレスポンスが返るようになっていたことから、あらかじめ攻撃用に用意したドメインと考えられます。しかし、この期間に確認された通信では、ハニーポット1台あたりに到着した通信の総数があまり多くはなく、この通信が送信元によるOpen Resolverの探査活動か、送信元に対するDNSアンプによるDDoS攻撃なのか判断できませんでした。また、海外のハニーポットに対しても同様の通信が確認されており、日本に対す

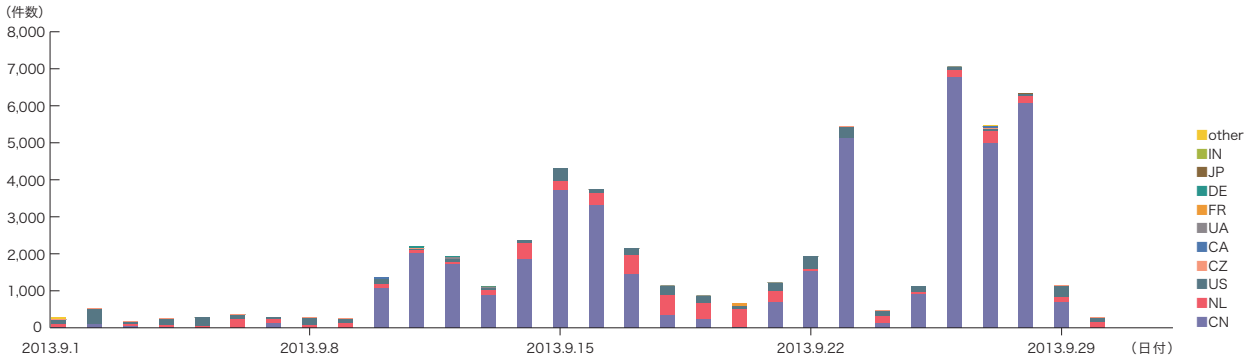


図-2 ハニーポットに到着した53/UDPの通信の推移(日別・国別)

*12 4月から6月の期間についての状況は、IIR Vol.20(http://www.iij.ad.jp/development/iir/pdf/iir_vol20.pdf)の「1.2 インシデントサマリ」を参照のこと。
*13 警察庁、「中国を発信元とする再帰問い合わせ可能なDNSサーバの探索行為の増加について」(http://www.npa.go.jp/cyberpolice/detect/pdf/20130911.pdf)。

8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

脆 **1日**：Black Hat USA 2013でドイツのセキュリティ研究者により、一部のSIMカードで56bitのDESが使われており、細工したSMSにより、SIMカードの暗号鍵が漏れる脆弱性があることが発表された。
詳細については、次のBlack Hat USA 2013での発表を参照のこと。"ROOTING SIM CARDS"（http://www.blackhat.com/us-13/archives.html#Nohl）。

他 **1日**：Twitter社は、各国政府などからの情報公開・削除要請件数をまとめた2013年前期のTransparency Reportを公開した。
Twitter, Inc.,"Transparency Report"（https://transparency.twitter.com/）。

脆 **2日**：Black Hat USA 2013でSSL/TLSに対する新たな攻撃手法BREACHが発表された。
詳細については、次の発表者の解説サイトBreachAttack.com（http://breachattack.com/）を参照のこと。

脆 **2日**：Open Shortest Path First（OSPF）プロトコルの仕様に、router-Link State Advertisement（LSA）の識別に関する問題があり、ルーティングテーブルの内容が改ざんされる可能性のある脆弱性が発表された。
JVN、「JVNVU#96465452 Open Shortest Path First (OSPF) プロトコルの Link State Advertisement(LSA) に関する問題」（http://jvn.jp/cert/JVNVU96465452/）。

脆 **2日**：LINE株式会社は、7月19日に発生した運営する複数のサービスで発生した不正アクセス事件について、不正アクセスを行った人物を国外の現地警察と共に特定し、取得された情報の削除を実施して、不正ログインによるアクセス、データの改ざん、第三者に提供した痕跡が確認されなかったことを公表した。
詳細については、次のLINE株式会社からのプレスリリースを参照のこと。「【NAVER】NAVER会員情報への不正アクセスに関するお知らせ(続報)」（http://linecorp.com/press/2013/0802585）。

脆 **4日**：Microsoft社はWindows PhoneのWPA2 wireless認証に使用されるPEAP-MS-CHAPv2の既知の脆さに起因する問題について、アドバイザリを公開した。
「マイクロソフト セキュリティ アドバイザリ (2876146)　ワイヤレス PEAP-MS-CHAPv2 認証により、情報漏えいが起こる可能性がある」（http://technet.microsoft.com/ja-jp/security/advisory/2876146）。

脆 **5日**：Torを利用した秘匿サービスのサービスプロバイダの1つで、6月に修正されたFirefoxの既知の脆弱性を利用した不正なコードが見つかったとして、話題となった。
詳細については、次のThe Tor Blogを参照のこと。"Hidden Services, Current Events, and Freedom Hosting"（https://blog.torproject.org/category/tags/freedom-hosting）。

セ **5日**：オランダ（.nl）のドメインレジストラの1つが管理パスワードが破られ、管理していた複数のWebホスティング会社のDNSが改ざんされたことにより、多数のWebサイトがマルウェアサイトにリダイレクトされる事件が発生した。

脆 **6日**：DEF CON 21で、自動車の制御システムの脆弱性の発表が行われた。
詳細については、次の発表者のChris Valasek氏とCharlie Miller氏の資料も参照のこと。"Car Hacking: The Content"（http://blog.ioactive.com/2013/08/car-hacking-content.html）。

他 **8日**：総務省は、ウイルス感染によりネットバンキングのID・パスワードが第三者に不正に利用され、不正送金を行う不正アクセス事案が多発しているとして、電気通信事業者関係団体に対し、電気通信事業者等が契約者や利用者に対して基本的なウイルス対策を講じるよう周知することへの協力などを要請した。
「ネットバンキングに係る不正アクセス事案への対応に関する利用者への注意喚起等について(要請)」（http://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000076.html）。

脆 **14日**：Microsoft社は、2013年8月のセキュリティ情報を公開し、MS13-059やMS13-060を含む3件の緊急と5件の重要な更新をリリースした。
「2013 年 8 月のセキュリティ情報」（http://technet.microsoft.com/ja-jp/security/bulletin/ms13-aug）。

セ **15日**：DNSSECの問題により、.govの名前解決が一時できなくなる障害が発生した。
詳細については、例えば次のISC Diaryなどを参照のこと。".GOV zones may not resolve due to DNSSEC problems."（https://isc.sans.edu/diary/.GOV+zones+may+not+resolve+due+to+DNSSEC+problems./16367）。

セ **15日**：GitHubが大規模なDDoS攻撃を受け、サービスを停止する事件が発生した。
この事件については、次のGitHub Statusで概要を確認することができる。"Status Messages"（https://status.github.com/messages/2013-08-15）。

他 **22日**：日本セキュリティオペレーション事業者協議会（ISOC-J）により、国内のWeb改ざん事件の概要などの解説や具体的な個別相談を行う「止まらない！ウェブ改ざんの実態と対策（個別相談会併設）」が開催された。
講演内容については、次のISOG-Jのホームページで確認できる。"ISOG-J主催セミナー「止まらない！ウェブ改ざんの実態と対策（個別相談会併設）」"（http://isog-j.org/event/index.html）。

セ **25日**：中国のドメインである.cnのDNSサーバに対して大規模なDDoS攻撃が発生した。
詳細については、次のCNNICの発表などを参照のこと。CNNIC"公告"（http://www.cnnic.net.cn/gywm/xwzx/xwzxtzgg/201308/t20130825_41322.htm）（中国語）。

セ **28日**：国内の複数のホスティング事業者でWordPressを狙ったと考えられるWeb改ざんが多数発生した。

セ **29日**：TrendMicro社は、Java 6に存在する未修正の脆弱性があり、攻撃が確認されたとして最新版のJavaに更新するよう注意喚起を行った。
詳細については、次のTrendMicro社のSecurity Blogを参照のこと。「Java 6に存在するゼロデイ脆弱性を確認、最新版への更新を！」（http://blog.trendmicro.co.jp/archives/7773）。

セ **29日**：独立行政法人情報処理推進機構（IPA）より、標的型メール攻撃の全体像や特徴、それに対するシステム設計による対策手法をまとめた「『標的型メール攻撃』対策に向けたシステム設計ガイド」が公開された。
「『標的型メール攻撃』対策に向けたシステム設計ガイド」の公開（http://www.ipa.go.jp/security/vuln/newattack.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

る攻撃を意図した通信である可能性は少ないと考えられます。なお、この調査の結果、少量ではあるものの中国を送信元としたDNS Open Resolverを探査する試みが、少なくとも本年1月から定期的に行われていたことが確認されています。この試みは本年8月下旬で観測されなくなりましたが、探索の通信はその後も不定期に確認されているため、今後も引き続き注意が必要と考えられます。

■ 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。7月には、マレーシアのドメインである.myを管理しているccTLDレジストリであるMYNICが何者かによる不正アクセスを受け、MicrosoftやDellといった有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。ベルギーのドメインである.beを管理しているccTLDレジストリであるDNS BelgiumのWebサイトが不正に書き換えられる事件が発生しています。DNS BelgiumのWebサイトは、この後にも再び不正侵入とWeb改ざんが発生しています。オランダのドメインである.nlを管理しているccTLDレジストリであるSIDNでも、SQLインジェクション攻撃による不正アクセスを受けて、アカウント情報のリセットが行われています。オランダでは、ccTLDレジストラの1つが不正アクセスを受け、ドメインハイジャックにより別のサイトに誘導される事件も発生しています。8月には、パレスチナのドメインである.psを管理しているccTLDレジストリであるPNINAが不正アクセスを受け、ドメインハイジャックにより、Googleのサイトが別のサイトに誘導される事件が発生しています。同じく8月には、複数の報道機関やTwitterの一部のドメインが正常にアクセスできなくなる事件が発生しましたが、これは被害を受けた企業が使っていたドメインレジストラのシステムが何者かに不正アクセスを受け、ドメインハイジャックされたことが原因でした[*14]。

■ 政府機関の取り組み

政府機関の動きでは、第11回情報セキュリティ対策推進会議（CISO等連絡会議）が行われ、政府機関による、民間企業の提供するグループメールサービスの利用に伴う情報漏えい事案について、当該省庁を含む複数の省庁から報告が行われました[*15]。これらの事例では適切なアクセス制限をかけていなかったことから、機密情報を含む業務情報が第三者に閲覧できる状態となっていました。また、同様のサービスを利用していた事例が複数確認されたとして、利用者への各府省庁の情報セキュリティポリシーの再徹底が確認されました。更に第12回会議において、機密情報などを含む業務情報の取り扱いと外部サービスの利用についての注意喚起が行われています[*16]。

7月には、総務省のICT成長戦略会議より、その議論について取りまとめた「ICT成長戦略」が公表されました。この中では、G空間（地理空間）情報やビッグデータの活用による新たな付加価値産業の創出など、3つのビジョンについて提言が行われています。同じく、総務省の利用者視点を踏まえたICTサービスに関わる諸問題に関する研究会からは、スマートフォンなどがかかえる課題について、安心・安全に利用できる環境を整備するために必要な対応についての検討結果をまとめた、「スマートフォン安心安全強化戦略」が公表されました。8月には、パソコンへのウイルス感染が原因で、ネットバンキングへの不正アクセスとそれによる不正送金を行う事案が多発しているとして、電気通信事業者関係団体に対し、各団体所属の電気通信事業者などがユーザに対して基本的なウイルス対策を講じるよう周知することなどへの協力の要請が行われました。国際連携では、9月に昨年11月より定期的に実施されている、日・ASEANサイバーセキュリティ協力に関する閣僚政策会議が行われ、共同閣僚声明が採択されました[*17]。

＊14 事件の詳細については、次のSophos社のNakedsecurity Blogなどに詳しい。"Syrian Electronic Army brings down Twitter and The New York Times through domain name provider hack"（http://nakedsecurity.sophos.com/2013/08/28/syrian-electronic-army-brings-down-twitter-and-the-new-york-times-through-domain-name-provider-hack/）。

＊15 内閣官房情報セキュリティセンター、「第11回会合（平成25年7月11日）」（http://www.nisc.go.jp/conference/suishin/index.html#2013_3）。

＊16 内閣官房情報セキュリティセンター、「第12回会合（平成25年7月30日）」（http://www.nisc.go.jp/conference/suishin/index.html#2013_4）の資料を参照のこと。

＊17 内閣官房情報セキュリティセンター、「日・ASEANサイバーセキュリティ協力に関する閣僚政策会議の 結果（報道発表資料）」（http://www.nisc.go.jp/press/pdf/aseanj_meeting20130913.pdf）。

9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

他 **2日**：パーソナルデータに関する利活用ルールの明確化などに関する調査及び検討を行うため、政府のIT総合戦略本部により設置された、パーソナルデータに関する検討会」の第1回検討会が開催された。
「パーソナルデータに関する検討会」(http://www.kantei.go.jp/jp/singi/it2/pd/index.html)。

他 **2日**：IPAより、内部不正の事例の紹介や内部不正対策についてまとめたガイドラインが公開された。
IPA、「組織における内部不正防止ガイドラインを公開」(http://www.ipa.go.jp/security/fy24/reports/insider/index.html)。

他 **4日**：総務省は、スマートフォンが持つ新たな課題についての提言をまとめたスマートフォン安心安全強化戦略を公表した。
『スマートフォン安心安全強化戦略』の公表(http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000122.html)。

セ **5日**：衆議院で、サーバがダウンし議員会館で使われている電子メールの閲覧ができない状態になる事件が発生した。

セ **6日**：自治体向け有料ニュースサイトが不正アクセスを受け、Webサイトの改ざんにより不正なコードが埋め込まれ、マルウェアに誘導される事件が発生した。

他 **6日**：Torのユーザ数が8月下旬から数百万人規模で増加していることが観測された。増加の原因としてはボットネットが利用しているためと推測されている。
"How to handle millions of new Tor clients"(https://blog.torproject.org/blog/how-to-handle-millions-new-tor-clients)。

他 **6日**：複数の報道機関により、米国国立標準技術研究所(NIST)が策定した暗号アルゴリズムの一部に、米国家安全保障局(NSA)によるバックドアがあり、解読される可能性があるとの報道がなされた。
その後、NISTでは意図的に脆弱な暗号を採用した可能性を否定する声明("Cryptographic Standards Statement"(http://www.nist.gov/director/cybersecuritystatement-091013.cfm))を発表し、同じく9月には、SP 800-90A(Dual_EC_DRBG)について利用しないことを推奨する勧告と見直しを行うことを発表している。"SUPPLEMENTAL ITL BULLETIN FOR SEPTEMBER 2013 NIST OPENS DRAFT SPECIAL PUBLICATION 800-90A, RECOMMENDATION FOR RANDOM NUMBER GENERATION USING DETERMINISTIC RANDOM BIT GENERATORS, FOR REVIEW AND COMMENT"(http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf)。

脆 **11日**：Microsoft社は、2013年9月のセキュリティ情報を公開し、MS13-067やMS13-068、MS13-069を含む4件の緊急と9件の重要な更新をリリースした。
「2013 年 9 月のセキュリティ情報」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-sep)。

脆 **11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。
「APSB13-21: 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/apsb13-21.html)。

脆 **11日**：Adobe Readerおよび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。
「APSB13-22: Adobe ReaderおよびAcrobat用セキュリティアップデート公開」(http://www.adobe.com/jp/support/security/bulletins/apsb13-22.html)。

脆 **11日**：Adobe Shockwave Playerに、任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「APSB13-23: Adobe Shockwave Player用セキュリティアップデート公開」(http://www.adobe.com/jp/support/security/bulletins/apsb13-23.html)。

他 **12日**：日・ASEAN友好協力40周年の記念事業の1つとして、サイバーセキュリティ分野での各国間の協力を閣僚レベルで議論する日・ASEANサイバーセキュリティ協力に関する閣僚政策会議が開催され、共同閣僚声明が採択された。
内閣官房情報セキュリティセンター(NISC)、「日・ASEAN サイバーセキュリティ協力に関する閣僚政策会議の開催 」(http://www.nisc.go.jp/press/pdf/aseanj_meeting20130911.pdf)。

脆 **18日**：Microsoft社は、ASP.NETに脆弱性があり、悪用されるとサーバー上の暗号化された情報が読み取られる可能性があるとして、アドバイザリを公開した。この脆弱性については、9月21日に限定的な攻撃が確認された。
「マイクロソフト セキュリティ アドバイザリ (2416728)　ASP.NET の脆弱性により、情報漏えいが起こる」(http://technet.microsoft.com/ja-jp/security/advisory/2416728)。

脆 **18日**：Microsoft社は、Internet Explorer に脆弱性があり、特別に細工されたウェブページをIEで閲覧した際に、リモートでコードを実行させられる可能性があるとして、アドバイザリを公開した。
「マイクロソフト セキュリティ アドバイザリ (2887505)　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/2887505)。なお、この脆弱性は10月9日に「マイクロソフト セキュリティ情報 MS13-080 - 緊急　Internet Explorer 用の累積的なセキュリティ更新プログラム (2879017)」(https://technet.microsoft.com/ja-jp/security/bulletin/ms13-080)で修正されている。

セ **18日**：歴史的な要因によりこの日の前後に、複数のWebサーバに対する改ざんやDDoS攻撃が発生した。しかしながら昨年と比べると小規模な攻撃にとどまった。

脆 **21日**：Apache StrutsにDynamic Method Invocationがデフォルトで有効なことで、利用者の意図しない処理が行われるなどの影響が考えられる脆弱性(CVE-2013-4316)が見つかり、修正された。
Apache Software Foundation、"Apache Struts 2 Documentation　S2-019"(http://struts.apache.org/release/2.3.x/docs/s2-019.html)。

他 **22日**：米国のセキュリティ企業であるFireEye社から、Internet Explorerの未修正の脆弱性を悪用し、日本の組織を標的とした攻撃を確認したことが報告された。
詳細については、次のFireEye社のBlogに詳しい。"Operation DeputyDog: Zero-Day (CVE-2013-3893) Attack Against Japanese Targets"(http://www.fireeye.com/blog/technical/cyber-exploits/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html)。

他 **25日**：総務省は、サイバー攻撃への対応能力の向上を目的として、大規模な模擬環境を用いた実践的なサイバー防御演習を実施することを公表した。
「『実践的サイバー防御演習(CYDER)』の実施」(http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000057.html)。

セ **26日**：Kaspersky Lab社は、日本と韓国をターゲットにしたAPTキャンペーン"Icefog"についてレポートを公開した。
詳細については、次のKaspersky Lab社の報告を参照のこと。「Kaspersky Lab、日本と韓国のサプライチェーンを主な攻撃対象とする新たなサイバースパイ活動「Icefog」を暴く」(http://www.kaspersky.co.jp/news?id=207585858)。

他 **26日**：政府の情報セキュリティ対策推進会議(CISO等連絡会議)の第13回会合が開催され、標的型攻撃など、高度なサイバー攻撃から重要な情報を保護するため、各府省庁で、業務システムの防護策を講じるためのガイドラインなどが決定された。
内閣官房情報セキュリティセンター、「第１３回会合(平成２５年９月２６日)」(http://www.nisc.go.jp/conference/suishin/index.html#2013_5)。

[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

■ スマートフォンへの脅威

この期間では、スマートフォンの脆弱性やその動向についても話題となりました。

モトローラ社の携帯端末の一部で、利用者が意図しない個人情報の収集が行われていることが研究者により公表されました。この中では、収集した情報の中には利用者の外部SNSなどのIDとパスワードも含まれていたことや、収集した情報を元にログインを試みたと考えられる外部サービスからのログイン警告が送られてきた事例があったことなどが報告されています。

米国で行われたBlack Hat USA 2013では、Android OSに、ファイルの暗号化認証の認証プロセスに脆弱性があり、正当に署名されたapkファイルなどの署名を壊すことなくファイルを改ざんすることが可能な脆弱性が報告されました。また、別の研究者からは、一部のSIMカードでDESによる暗号通信を利用していることから、その暗号強度の問題により、SMSを利用した端末への攻撃が可能なことが発表されました。このSIMカードの脆弱性については、日本でも数多くのデバイスが対象となる可能性があったことから、報道などで話題となりました。

スマートフォンなどの携帯端末が広く普及したことで、これらの問題の影響を受ける端末の数は数億台といった大きな数にのぼります。今回発表された脆弱性などでは、修正が速やかに実施されたり、特定の条件に依存するなど、実際の影響は限定的なものでしたが、1つの問題が数多くの端末に影響し、大規模な脅威となる可能性があるため、引き続き注意する必要があります。

■ その他

8月には、警察庁より、平成25年度上半期におけるサイバー攻撃の状況をまとめた、「平成25年上半期のサイバー攻撃情勢について」が公表されました[*18]。この中では、標的型メール攻撃における情報提供などを詐称するメールを関係者に送付する「ばらまき型」攻撃が減少し、攻撃対象の業務に関連する内容のメールのやりとりを行った上で標的型メールを送付する「やりとり型」攻撃が増加していることが報告されています。やりとりの内容としては、採用に関する質問や、製品に関する不具合の問い合わせなどが多かったとされています。

7月には、国内の主要通信事業者、ISPの業界団体であるTelecom-ISAC Japanより、不正ログインなどの複数の事件に関連して、特定の製品における脆弱性について、修正の適用や設定の確認などの対策を促す注意喚起が行われました[*19]。この団体では、日本国内のネットワークに接続するデバイスの脆弱性の保有状況について、会員ISPのIPアドレス帯に対する実態把握を目的とした調査を6月より行っています[*20]。

9月には、IPAより、内部不正の事例の紹介や内部不正対策の状況を把握するためのチェックシート、対策のヒントとなるQ&Aなどにより、対策の整備を可能とする「組織における内部不正防止ガイドライン」が公開されました。この中では対策について解説すると共に、発生してしまった際の早期発見・拡大防止についても併せて解説を行っており、内部不正対策について検討していなかった企業でも利用しやすい内容となっています。

同じくIPAからは、標的型メール攻撃を主流とする「新しいタイプのサイバー攻撃」に対し、標的型攻撃の全体像を分析することでその攻撃の意図や背景、全体像を明らかにし、組織の情報システム系全体について、システム構築時に取るべき設計手法や運用者が取るべき対策をまとめた「『標的型メール攻撃』対策に向けたシステム設計ガイド」が公開されました。この中では、標的型メール攻撃を段階に分けて分析し、その対策を示しており、組織内部に侵入された場合でも、情報システムの設計や運用による対策により、活動を制限し、侵入拡大や情報の盗取を防ぐ様々な取組みが紹介されています。

＊18　警察庁、「平成25年上半期のサイバー攻撃情勢について」(http://www.npa.go.jp/keibi/biki3/250822kouhou.pdf)。
＊19　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)。
＊20　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)。

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-3に、2013年7月から9月の期間にIIJ DDoSプロテクションサービスで取り扱ったDDoS攻撃の状況を示します。

ここでは、IIJ DDoSプロテクションサービスの基準で攻撃と判定した通信異常の件数を示しています。IIJでは、ここに示す以外のDDoS攻撃にも対処していますが、攻撃の実態を正確に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-3では、DDoS攻撃全体を、回線容量に対する攻撃[*21]、サーバに対する攻撃[*22]、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、628件のDDoS攻撃に対処しました。1日あたりの対処件数は6.9件で、平均発生件数は前回のレポート期間と比べて増加しています。DDoS攻撃全体に占める割合は、サーバに対する攻撃が75.3%、複合攻撃が22.6%、回線容量に対する攻撃が2.1%でした。

今回の対象期間で観測された中で最も大規模な攻撃は、複合攻撃に分類したもので、最大32万2千ppsのパケットによって3.2Gbps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71.3%が攻撃開始から30分未満で終了し、28.5%が30分以上24時間未満の範囲に分布しており、24時間以上継続した攻撃も0.2%ありました。なお、今回最も長く継続した攻撃は、複合攻撃に分類されるもので1日と8時間27分(32時間27分)にわたりました。

また、毎年この期間では、歴史的日付の前後でDDoS攻撃が多く見られます。本年も9月15日から9月18日にかけて、DDoS攻撃が通常より増加していることを確認しています。攻撃の規模としては最大2.5Gbpsで約70万ppsの複合攻撃を確認しています。

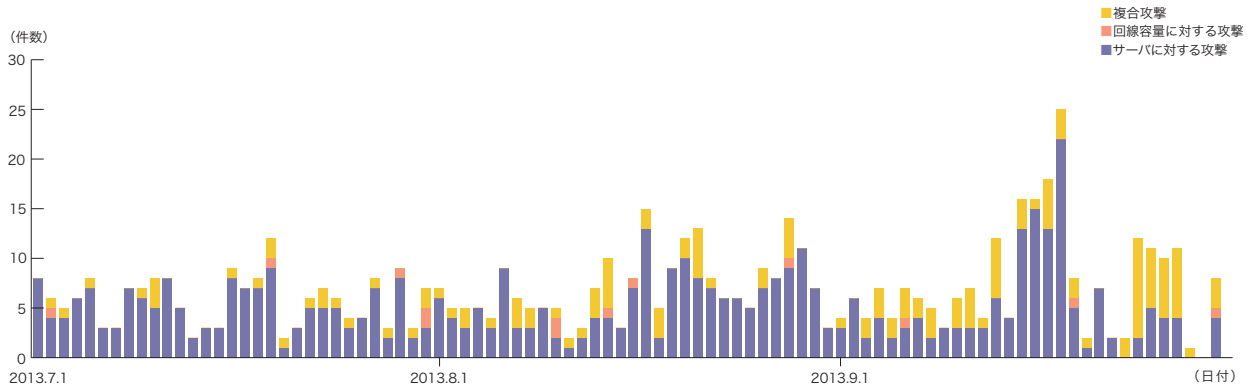


図-3 DDoS攻撃の発生件数

*21 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。

*22 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。

攻撃元の分布としては、多くの場合、国内、国外を問わず非常に多くのIPアドレスが観測されました。これは、IPスプーフィング[*23]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[*24]の利用によるものと考えられます。

■ 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[*25]によるDDoS攻撃のbackscatter観測結果を示します[*26]。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。

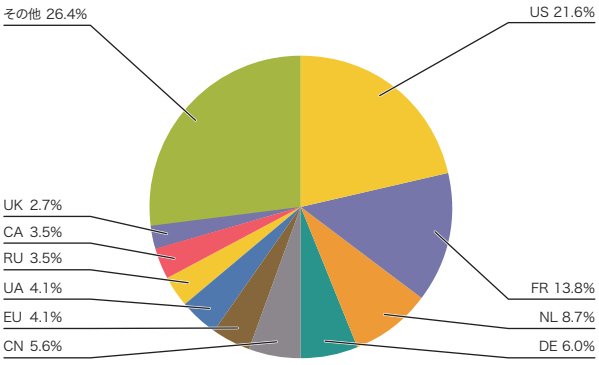


図-4 backscatter観測によるDDoS攻撃対象の分布（国別分布、全期間）

2013年7月から9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-4に、ポート別のパケット数推移を図-5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49.6%を占めています。また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30800/TCP、ストリーミング通信で利用される1935/TCP、通常は利用されない25565/TCPなどの攻撃が観測されています。

図-4で、DDoS攻撃の対象となったIPアドレスと考えられるbackscatterの発信元の国別分類を見ると、今回の期間では米国の21.6%が最も大きな割合を占めていました。その後にフランスの13.8%、オランダの8.7%といった国が続いています。

特に多くのbackscatterを観測した場合について、攻撃先のポート別に見ると、まず、Webサーバ(80/TCP)への攻撃としては、8月27日にフィリピンのホスティング事業者のWebサーバからのbackscatterを観測しています。8月13日から14日にかけて、レバノン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。9月18日には、中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。

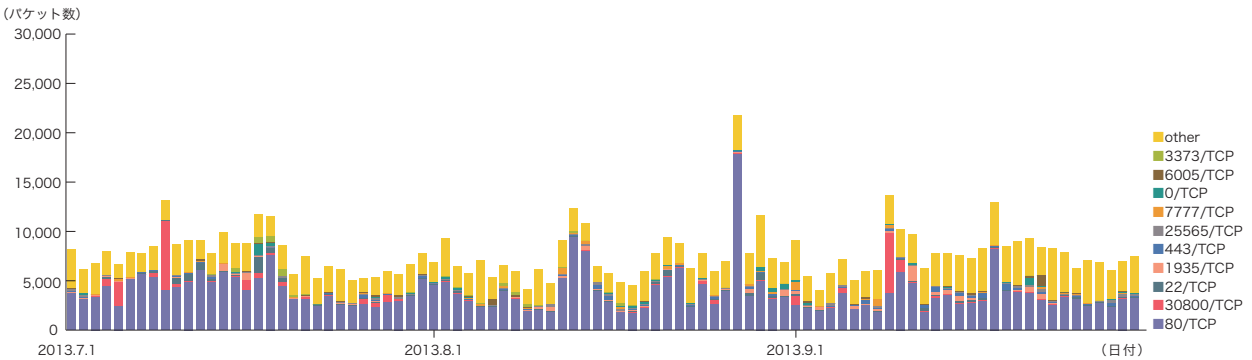


図-5 DDoS攻撃によるbackscatter観測(観測パケット数、ポート別推移)

*23 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。

*24 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。

*25 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。

*26 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。

9月11日には1935/TCPに対するスウェーデンとカナダの複数のホスティング事業者の複数のサーバへの攻撃を観測しています。7月9日と9月9日には30800/TCPに対するフランスとオランダの複数のホスティング事業者のサーバへの攻撃を観測しています。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、9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を検知しています。

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[*27]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[*28]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。

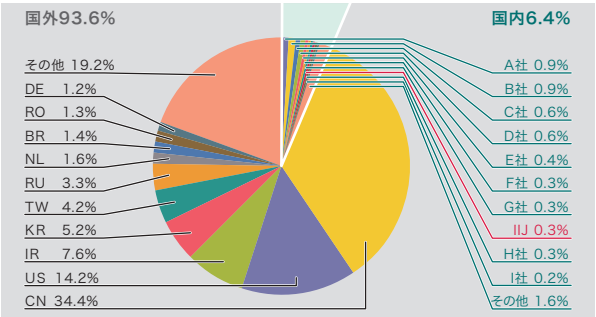


図-6 発信元の分布（国別分類、全期間）

■ 無作為通信の状況

2013年7月から9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-6に、その総量（到着パケット数）の推移を図-7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、Telnetで利用される23/TCP、ICMP Echo Request、DNSで利用される53/UDPによる探査行為も観測されています。

期間中、SSHの辞書攻撃と思われる通信も発生しており、例えば7月24日は中国、9月2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。9月中旬以降、中国に割り当てられたIPアドレスから集中的に53/UDPの通信が通常の数十倍に増加したのを観測して

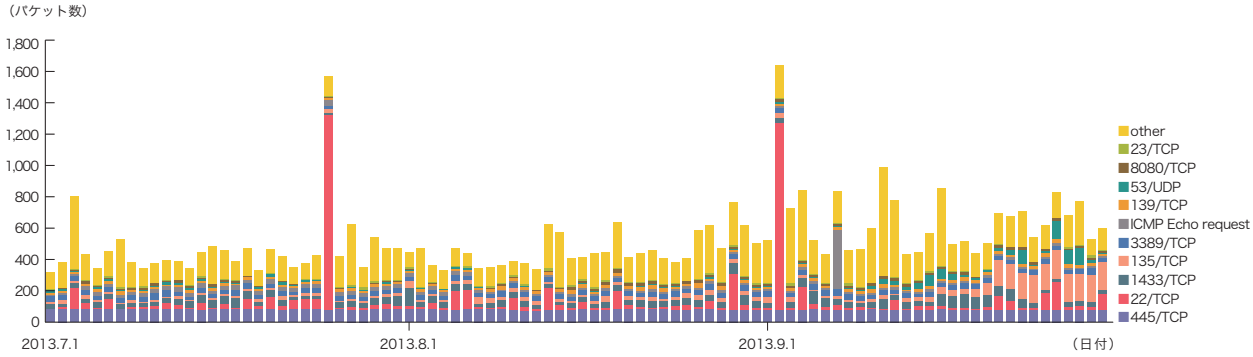


図-7 ハニーポットに到着した通信の推移（日別・宛先ポート別・1台あたり）

*27 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。

*28 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。

います。調査した結果、DNSアンプ攻撃を行うためのOpen Resolverを探す探査行為であると考えられます。更に8月末から9月中旬にかけて、中国に割り当てられたIPアドレスからのアクセスが通常の倍程度に増加しています。これは改ざん可能なSQLサーバを探すための探査行為であると考えられます。どちらも非常に広範囲のIPアドレスに対して通信が行われており、攻撃することが可能、または攻撃に利用することが可能なサーバを探していることが窺えます。また、米国に割り当てられたIPアドレスからの135/TCPの通信が9月下旬にそれまでの水準の数十倍に急増しています。通信内容を調査したところ、DCOMのIOXIDResolverオペレーションを利用してServerAlive2 requestが届いていました。これはリモートホスト上でMicrosoftRPCサーバが動作しているかを確認するための仕組みであるため、RPCサーバの探査行為であると考えられます。また急増した期間中、米国に割り当てられたIPアドレスからの通信はユニークで100を超えていましたが、中でも2つのAS番号で総通信量の8割を超えていたため、攻撃者の持つインフラに偏りがあったことも特徴として挙げられます。

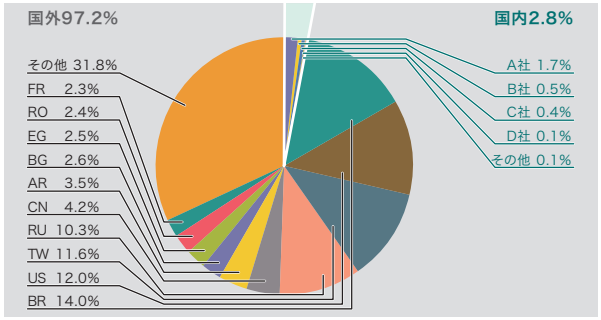


図-8 検体取得元の分布（国別分類、全期間、Confickerを除く）

■ ネットワーク上でのマルウェアの活動

同じ期間中でのマルウェアの検体取得元の分布を図-8に、マルウェアの総取得検体数の推移を図-9に、そのうちのユニーク検体数の推移を図-10にそれぞれ示します。このうち図-9と図-10では、1日あたりに取得した検体[*29]の総数を

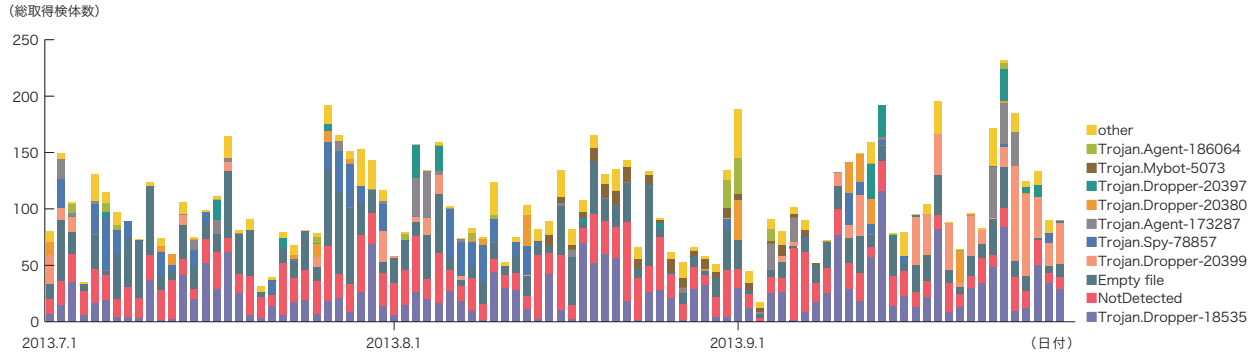


図-9 総取得検体数の推移（Confickerを除く）

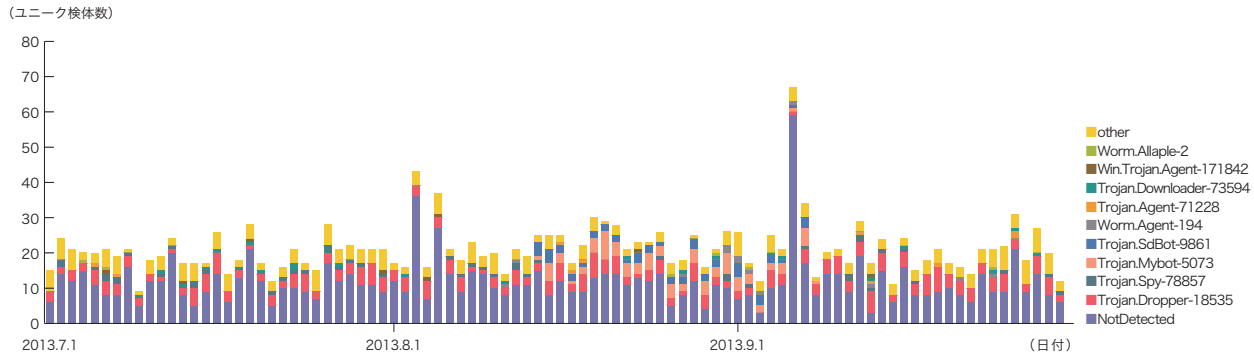


図-10 ユニーク検体数の推移（Confickerを除く）

*29 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。

総取得検体数、検体の種類をハッシュ値[*30]で分類したものをユニーク検体数としています。

また、検体をウイルス対策ソフトで判別し、上位10種類の内訳をマルウェア名称別に色分けして示しています。なお、図-9と図-10は、前回同様に複数のウイルス対策ソフトウェアの検出名によりConficker判定を行い、Conficker と認められたデータを除いて集計しています。

期間中での1日あたりの平均値は、総取得検体数が105、ユニーク検体数が21でした。未検出の検体をより詳しく調査した結果、7月から8月前半に米国とフランスに割り当てられたIPアドレスからのワーム[*31]、8月中旬にはフィリピンIRCサーバで制御されるタイプのボット[*32]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79.4%、ボット型15.3%、ダウンローダ型4.9%でした。また解析により、21個のボットネットC&Cサーバ[*33]と10個のマルウェア配布サイトの存在を確認しました。

■ Confickerの活動

本レポート期間中、Confickerを含む1日あたりの平均値は、総取得検体数が34,387、ユニーク検体数は788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5%増加しています。また、ユニーク検体数は前号から約3%減少しました。Conficker Working Groupの観測記録[*34]によると、2013年10月4日現在（注：Conficker Working Groupの9月30日から10月3日までのデータが極端に少ないため、異常値であると判断し、今回はこの値を用いています）で、ユニークIPアドレスの総数は1,450,964とされています。2011年11月の約320万台と比較すると、約45%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。

＊30 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。
＊31 WORM_DEBORM.AP（http://about-threats.trendmicro.com/Malware.aspx?id=36201&name=WORM_DEBORM.AP&language=au）。
＊32 BKDR_QOKBOT（http://about-threats.trendmicro.com/malware.aspx?language=en&name=BKDR_QAKBOT）。
＊33 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。
＊34 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[*35]について継続して調査を行っています。SQLインジェクション攻撃は、過去にもたびたび流行し話題となった攻撃です。SQLインジェクション攻撃には、データを盗むための試み、データベースサーバに過負荷を起こすための試み、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7月から9月までに検知した、Webサーバに対するSQLインジェクション攻撃の発信元の分布を図-11に、攻撃の推移を図-12にそれぞれ示します。これらは、IIJマネージドIPSサービスのシグネチャによる攻撃の検出結果をまとめたものです。

発信元の分布では、日本54.1%、米国15.2%、モロッコ9.8%となり、以下その他の国々が続いています。

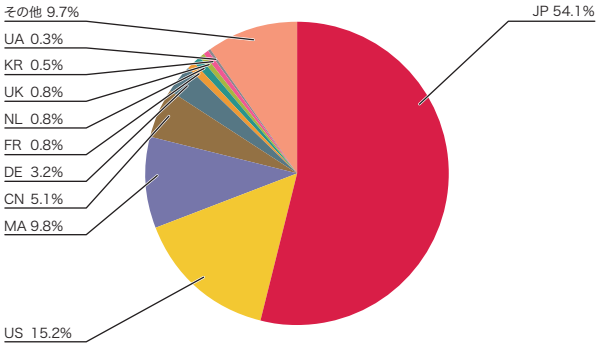


図-11 SQLインジェクション攻撃の発信元の分布

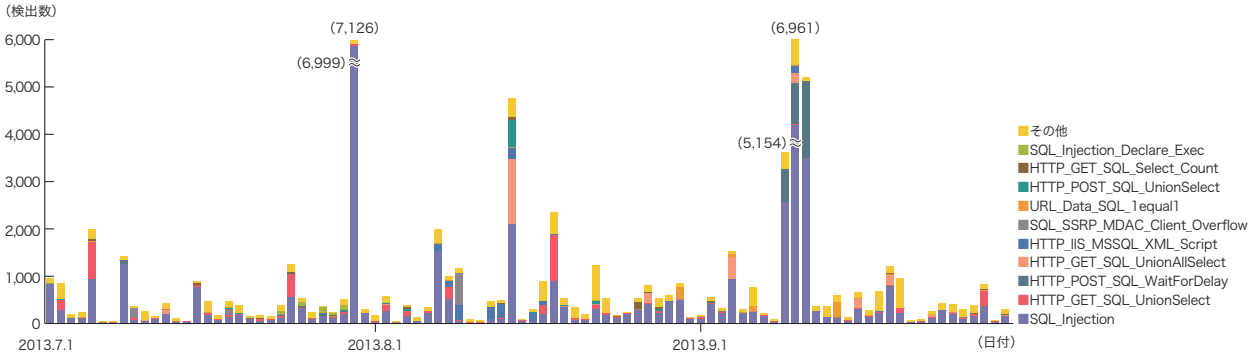


図-12 SQLインジェクション攻撃の推移(日別、攻撃種類別)

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からあまり変化していません。モロッコからの攻撃が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、9月9日から11日にかけて国内の特定の攻撃元より、特定の攻撃先に対する大規模な攻撃が発生しています。7月30日には、モロッコ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。8月14日には、米国の特定の攻撃元から特定の攻撃先へ、米国やドイツ、イギリスの特定の攻撃元より別の特定の攻撃先への攻撃が発生していました。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。

*35 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、標的型攻撃で利用されるRAT「PlugX」、連続する標的型メール攻撃について、仮想通貨Bitcoinの3つのテーマについて紹介します。

1.4.1 標的型攻撃で利用されるRAT「PlugX」

PlugXはKorplug、Gulpixなどとも呼ばれ、Poison Ivyなどと共に標的型攻撃で頻繁に悪用が確認されているRAT[*36]の一種です。IIJでは最近発生した標的型攻撃で実際に使用された検体を入手し、詳細に解析を行いました。この検体の機能を報告すると共に、このマルウェアの発見手法について考察します。

■ PlugXの概要

PlugXは2012年3月に発見されたマルウェアで、発見後も継続的にアップデートされています。このマルウェアはファイル操作（作成やコピー、ダウンロードやアップロード、実行や停止など）やレジストリ操作、サービスの起動や停止、キーボード入力の盗聴、画面キャプチャ、リモートシェル実行などのRATの基本機能に加え、ポートスキャンや、SQLサーバに接続して情報を窃取するための機能も存在します。更に名前も示しているとおり、プラグインでの拡張が可能なことも特徴の1つです。

■ 特徴

図-13は、IIJが入手した検体を実行した際のマルウェアの実行フローを示しています。メールに添付されたzipファイルが送信されており、このzipファイルを解凍すると、exeファイルが出現します。メールの受信者がこのファイルをダブルクリックしてしまうと、Dropperが実行されます。この

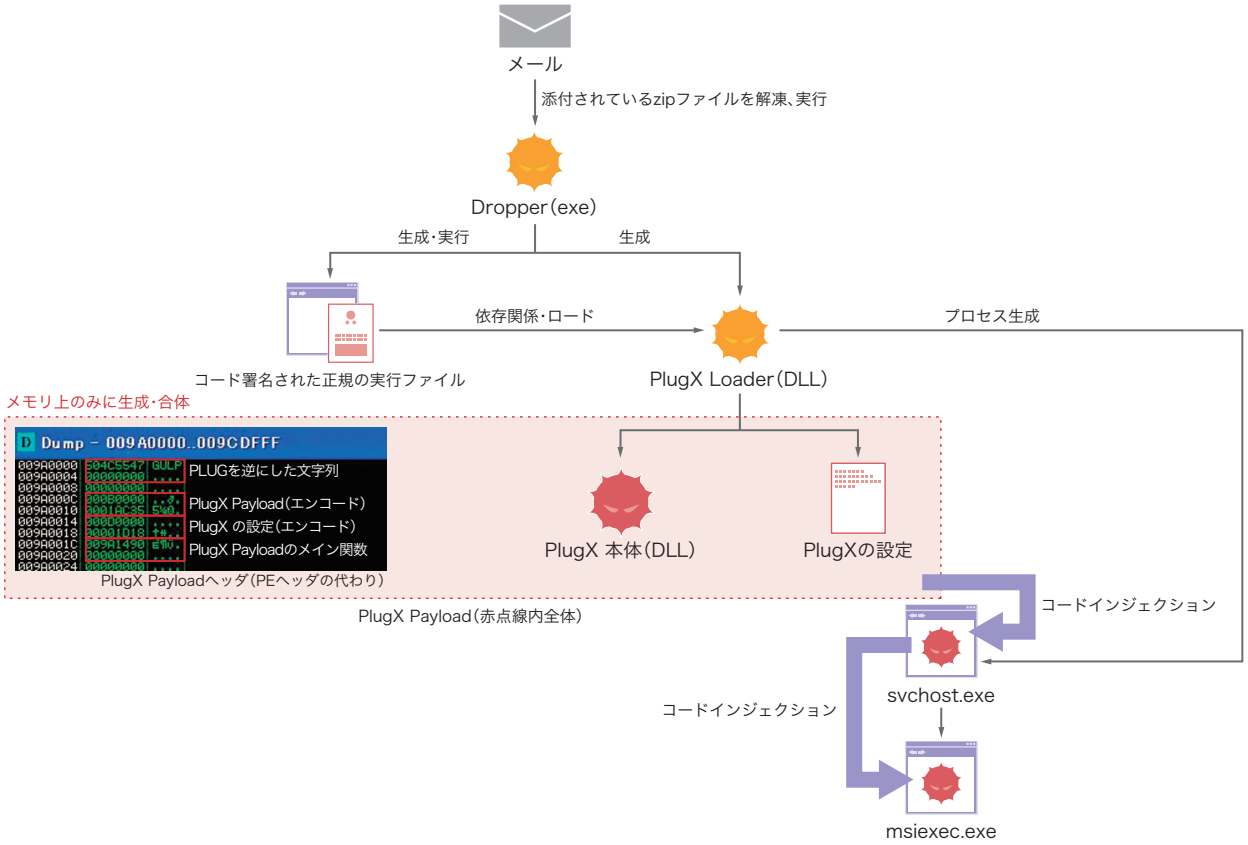
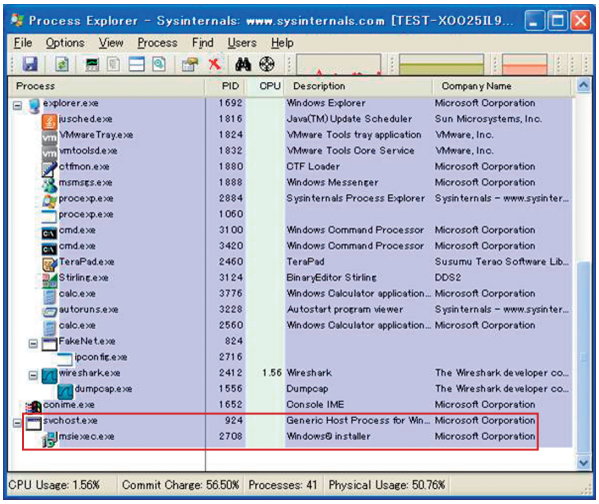


図-13 PlugXの実行フロー

*36 Remote Administration Toolの略で、インストールされたホストを遠隔から操作するためのソフトウェア。Remote Access ToolやRemote Access Trojanなどと呼ばれることもある。

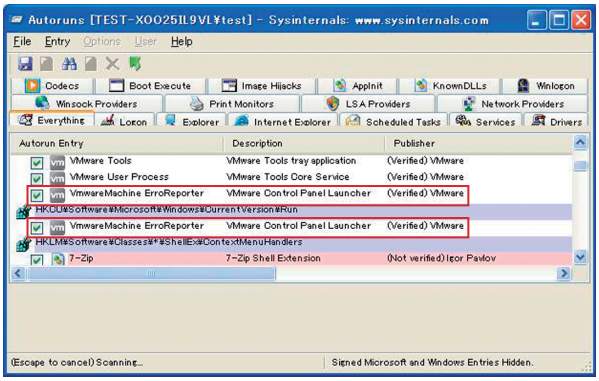
Dropperはコード署名されたexe(正規アプリケーションであり、マルウェアではない)とPlugXをロードする役割を持つdll(以下PlugX Loaderとする)を同一フォルダ内に生成し、コード署名されたexeを実行します。このexeは実行時に依存関係のあるdllをロードしますが、PlugX Loaderはその依存関係を持つdllと同一名称になっているため、dllを読み込む際の優先順位を悪用(同一フォルダに存在するdllが最優先でロードされる)し、本来ロードされるべき正規のdllではなく、PlugX Loaderをロードさせることでコードを実行します。PlugX Loaderはメモリ上にPlugX本体のdllと設定をデコードし、それをPlugX Loader自らが生成したsvchost.exeプロセスにコードインジェクションすることから始めて、PlugX本体を実行していきます。ただし、svchost.exeにインジェクションせず、dllのロード優先順位の悪用も行わず、PlugX Loaderの処理を単一の実行ファイル(署名されていないexeファイル)で行い、PlugX本体や設定をその実行ファイル内に展開する「スタンドアロン型」の検体も存在します。コードインジェクションを行う際、PEヘッダを"GULP"(PLUGを逆にした文字列)から始まるヘッダに改変します。このヘッダは、エンコードされた設定と自分自身のコードへのポインタとサイズ及びPlugXのメイン関数へのポインタが格納されており、そのヘッダの後にPlugX本体のPEヘッダ以外の領域(コード、データ)が格納されます。これらインジェクションされるパーツを総称して、PlugX Payloadと呼びます。コードインジェクションされたPlugX Payloadはmsiexec.exeをプロセス生成し、そこにもコードインジェクションを行います。一方でPlugX Loader自体はプロセスを終了してしまうため、Process Explorer[*37]などで確認しても、一見するとsvchost.exeとmsiexec.exeが動作しているようにしか見えません(図-14)。

また、PlugX Loaderは端末起動時に自動実行するためにレジストリを登録しますが、登録される実行ファイルは前述のとおりコード署名されたexeです。そのため、Autoruns[*38]などを使ってマルウェアの痕跡を探した場合、正しいコード署名がなされたプログラムが登録されているように見えるため、マルウェアを発見しにくくしています[*39](図-15)。



赤線部がPlugXによって生成されたプロセスだが、どちらもWindowsに標準で付属している実行ファイルであるため、一見しただけではマルウェアであると断定ができない。

図-14 Process Explorerで確認した際の様子



赤線部の2ヵ所がPlugXによって追加されたレジストリエントリだが、正しくコード著名された実行ファイルであるため、Autorunsは要調査である赤や黄色に変化させていない。

図-15 レジストリエントリ

*37 Process Explorerとは、実行中のプログラムの状態を調べるツールで、Microsoft社のWindows Sysinternalsで配布されている(http://technet.microsoft.com/ja-jp/sysinternals/bb896653.aspx)。Windows標準のタスクマネージャよりも詳細に情報を確認することが可能。

*38 Autorunsとは、Windowsの起動時に自動実行されるプログラムの一覧を表示させるためのツールで、Process Explorerと同様にMicrosoft社のWindows Sysinternalsで配布されている(http://technet.microsoft.com/ja-jp/sysinternals/bb963902)。オフラインでも解析が可能であるため、インシデントレスポンス時に有用なツールの1つ。

*39 Autorunsの検出を迂回する仕組みとして、PlugXのようにdllのロードの優先順位を悪用する手法の他にも、バッファオーバフローの脆弱性が存在しているコード署名されたexeやdllを用意して登録し、その実行時の引数にshellcodeやマルウェア本体を含む長いデータ列を渡すことで脆弱性を突き、バッファオーバフローさせて任意のコード実行をし、結果的にマルウェアを実行させるという事例も存在する。例えば2013年10月に行われたVB2013では、Simbotと呼ばれるマルウェアがこのようなトリックを悪用して検出を逃れようとする事例が報告されている(http://www.virusbtn.com/pdf/conference_slides/2013/Szappanos-VB2013.pdf)。よって、インシデントレスポンス時にはこの様な点にも留意して探す必要がある。

C&Cサーバとの通信には、TCP、UDP、ICMP及びHTTPを使用でき、1つのIPアドレスで複数の通信手段を併用することが可能です。通信は独自方式のアルゴリズムでエンコードされているため、これを解かない限りPlugXの通信であると特定することは困難です。ただし、HTTPで通信を行う場合、図-16に示すようないくつかの特徴(POSTリクエストかつパス部が"/update?id=8桁の16進数"や、"X-Session"などの独自のHTTPヘッダ)が存在します。また、TCPとHTTPに関しては、Proxyサーバを利用して通信を行うことが可能な構造になっています。設定上では静的に4ヵ所のC&Cサーバを定義することができ、外部のWebサーバからもHTTPで通信を行うためのC&Cサーバの設定をダウンロードすることができる構造になっていました。

その他の特徴として、UAC(User Account Control)の迂回機能が挙げられます。Windows Vistaから導入されたUACですが、Windows 7以降ではデフォルトで最高レベルから1段階下げた値が適用されています。このレベルはプログラムが変更を行う場合のみUACのポップアップが出現するように制限されており、ユーザが直接行ったと思われる操作はUACのポップアップを出現させず、管理者権限に自動昇格します。PlugXはこれを悪用し、ユーザが行った作業であると誤認させることでUACを迂回してユーザの同意なしに管理者権限を取得します。

```
POST /update?id=000fad10 HTTP/1.1
Accept: */*
X-Session: 0
X-Status: 0
X-Size: 61456
X-Sn: 1
User-Agent: Mozilla/4.0 (compatible;
2.0.50727; .NET CLR 3.0.4506.2152;
Host: 54.250.220.230
Content-Length: 0
Connection: Keep-Alive
Cache-Control: no-cache
```

図-16 HTTPによるC&Cサーバとの通信

■ 検出方法

PlugXはHTTPで通信を行う場合、前述のような特徴が存在します。これらはPlugX本体のコード内にハードコーディングされており、通信相手であるC&Cサーバ側の修正も必要になることから、比較的変更されにくい特徴[*40]であると言えるでしょう。ゲートウェイやIPSなどでこれらをチェックすることで感染端末を発見することができます。ただし、最近IIJが入手した検体では、独自HTTPヘッダが"MJ1X"から"MJ4X"にそれぞれ変更されていました[*41]。そのため、HTTPヘッダの特徴で検出できない場合は、次に示すホストのメモリ上の特徴も併せて検出するのが良いでしょう。

PlugX本体はsvchost.exeにコードインジェクションを行う際、前述のとおり"GULP"から始まるヘッダに変更されます。インジェクション先のプロセスは設定で変更可能であるものの、"GULP"という文字列はヘッダの先頭に存在するだけでなく、コード内でPlugXがインジェクション先で実行されていることを確認するための文字列としてハードコーディングされているため、開発者以外は変更しにくい文字列の1つであると言えます。更に、この文字列はメモリ領域の先頭に暗号化などがされず、そのまま存在しているため、検出することが容易です。また、PlugXの領域はPAGE_EXECUTE_READWRITE属性になっています。よって、すべてのプロセスのメモリ領域を走査し、この文字列から始まる領域とその属性をチェックすることで、検出することができるでしょう。これらの特徴と併せ、以下も合わせて検出することで、誤検知を減らすことが可能です。

- **PlugXのエンコード、デコードルーチンの特徴**
  PlugXは通信やコンフィグなどをエンコードするための関数が存在します。そのアルゴリズムには、0x11111111、0x22222222、0x33333333、0x44444444など、特徴的な即値が用いられています。

*40 昨今のマルウェアは商用製品としてアンダーグラウンドで売買されており、ビジネスモデルが確立されている。このようなモデルの例としてBlackhole Exploit kitなどに代表されるExploit kitや近年日本での被害が急増しているZeuS(Citadel、Gameoverなどの亜種を含む)やSpyEyeなどのCrimeware kitなどが挙げられる。PlugXにもデモ版が存在しており、このモデルが採られている可能性がある。次のURLではPlugXのデモ版の存在が報告されている(http://www.lastline.com/an-analysis-of-plugx)。このように分業化が進んでいる昨今では、開発者と利用者(攻撃者)が異なることが多い。そのため利用者がマルウェアの設定を変更できる部分は、例えばC&Cのサーバ名やURLのパス部、いくつかの機能を有効や無効にする設定、レジストリの登録時のキーや値など一部に限られており、ソースコードを持つ開発者のように自由にコードを変更することは比較的難しい。また、たとえ開発者であったとしても、通信プロトコルなどを変更するためにはC&Cサーバのコード変更も同時に行わなければならず、既に通信中のマルウェアとの互換性の問題が出てくるため、このような場合も比較的変更しにくい箇所であると言える。このことから、通信プロトコルや通信やデータのエンコード、デコードのアルゴリズム、マルウェアが自身のコードを識別するための値、マルウェアが持つ機能を実現するために必要なWindows APIなどをここでは「比較的変更されにくい特徴」と定義している。

*41 IIJでは数十種類のPlugXの検体を入手し解析したが、独自のHTTPヘッダが変更されていた検体は最近入手したごく一部の検体のみであり、それまでの検体はすべて図-16の特徴を持っていた。そのため、これからこのような変更された検体が主流になるのか、このタイプがレアケースであるかはまだ不明であるが、少なくとも変更される可能性があることも考慮にいれておく必要はある。

- **特権操作に関係する文字列**
  "SeDebugPrivilege"のようなデバッグ用の権限は通常のアプリケーションで要求されることは少ない。

メモリのチェックは、Mandiant社のRedline[*42]やVolatility Framework[*43]などで行うことが可能です。

■ **対策**

このようなマルウェアに感染しないためには、従来の対策であるOSやインストール済みの各アプリケーションをすべて最新版にすることや、ウイルス対策ソフトウェアを用い、最新版にするなどは当然のこと、何重もの対策をしておくことが必要です。

例えば、Windows XP以降でWindows OSに標準搭載されているソフトウェア制限ポリシー、またはAppLockerを用いて実行ファイルの実行可能領域を限定することで、デスクトップやマイドキュメント、tempフォルダ上にある実行ファイルを実行してしまうことを防ぐことができます。これは、文書ファイルに見せかけた実行ファイルを誤って開こうとした場合に実行されることを防ぐことや、脆弱性を利用された場合でも、tempフォルダに展開されたマルウェアが実行されることを防ぐ効果があります。IIJが入手した検体も、多くはユーザディレクトリの配下に設置されるようになっていたため、実行可能領域を"C:\Program Files"以下、"C:\Windows"以下のみに限定していれば、感染を防ぐことが可能でした。またデフォルトではdllなどのライブラリが制限対象になっていないため、これらも対象にすることで、今回のようにユーザディレクトリ配下のdllがロードされることを防ぐことができます。前述のとおり、PlugXはUACの迂回機能を持っているため、Windows 7以降はUACを最高レベルに変更することで、UACが迂回されることを防ぎ、万が一感染した場合でも、PlugXを利用して攻撃者がその後の活動を行うことを制限、もしくは遅延させることができます。また、マルウェアは悪意のある文書ファイルを通してインストールされるケースも多いため、EMET[*44]を利用して、未知の脆弱性に対する緩和策を設けることで、脆弱性を突いてExploitやその後のマルウェアが実行されることを緩和することができます。Webアクセス時のブラウザプラグインを対象とした攻撃を防ぐため、Mozilla FirefoxやGoogle Chromeに実装されているClick-to-Playを有効にする[*45]ことも、攻撃から身を守る1つの手段と言えるでしょう。

インシデントに関する情報収集を行い、常日頃から発見できる仕組みを考え、実装しておくことも必要です。今回の事例で検出方法の一例として挙げたIOCは、いくつかのWebサイトで有志によって公開されていますが、ファイル名やハッシュ値、レジストリのキーなど、攻撃者が設定で簡単に変更可能なものがほとんどです。そのため、過去の事例には適用可能であっても、今後発生しうるインシデントでは検出はできない可能性が高いと考えられます。よって、マルウェアを自身で詳細に解析し、前述した攻撃者が変更しにくい特徴を元にIOCルールを作成することで、長期に渡って継続的に検出することが可能になります。その際、ファイルを検査しようとすると難読化やパックされているなどの理由で特徴が見えなくなっているため、メモリ上に存在する実行中のコードやデータを精査することで、より効果的に検出することが可能になります。

1.4.2 連続する標的型メール攻撃

2013年8月下旬から10月下旬にかけて、ある組織に対してRATを添付したメールを送信する攻撃が繰り返し行われました。本稿では、この一連の攻撃と、それを受けた組織における対応について紹介します。

*42 Mandiant Redline（http://www.mandiant.com/resources/download/redline）はHDDイメージやメモリイメージからマルウェアなどの痕跡を見つけ出すためのインシデントレスポンスツール。あらかじめ定義されたルール以外にもIOC（Indicator Of Compromise）と呼ばれるxml形式で記述された独自ルールを定義することが可能。

*43 Volatility Framework（https://www.volatilesystems.com/default/volatility）はメモリイメージを解析するためのツールであり、こちらもYARA（http://code.google.com/p/yara-project/）と呼ばれるパターンマッチを行うためのモジュールが存在するため、インシデントレスポンス時に役立つ。

*44 EMET（Enhanced Mitigation Experience Toolkit）はMicrosoft社が提供するソフトウェアの脆弱性が悪用されるのを緩和するためのツール。

*45 Click-to-Playはプラグインを自動実行せずユーザに確認（クリック）を促す機能。ドライブバイダウンロードではプラグインの表示領域が隠ぺいされることが多いため、確認ボタンも目視されない。このためユーザが誤ってクリックしてしまう可能性もなくなる。

■ 一連のメールとその概要

最初のメールは、8月29日に送信されたもので、図-17に示すような文面でした。このメールには、本文中で言及している「連絡網」をほのめかす名称のZIPファイルが添付されており、その内部には同名の実行ファイル(EXE)がアーカイブされていました。実行ファイルはRAT本体ですが、アイコン画像がMicrosoft EXCELの文書ファイルを偽装しています。このため、アイコンに騙されて拡張子を確認せずにファイルをダブルクリックすると、RATを実行してしまいます。添付されていたRATはPoison Ivyで、C&Cサーバやそのアカウント ID、パスワードについては図-18のような設定がなされていました。当該組織のドメイン名の一部がアカウントIDに用いられていたことは、同メールが無差別に行われた攻撃ではなく、明確に当該組織を対象として行われたものであることを示していると考えられます。

このメールを皮切りに、10月21日までの間に計11種類の標的型メールが当該組織に送付されました。

■ 共通する特徴

表-1にこの組織に対して送信された標的型メールの一覧を示します。送付された11種類のメールの多くで共通する特徴として以下のAからFが挙げられます。

To: 個人、ML 等
From: *部署名_ 個人名* <*個人名*@aol.com>
Subject: Fw:_08/29(木)_職員連絡網の最新版データ送付
Date: Thu, 29 Aug 2013 04:10:26 -0400 (EDT)

各位

お世話になります。

標記の件、添付データを送付いたしますのでよろしくご査収ください。

「旧名簿」とありますが電話番号と住所、E-MAILは最新データです。

個人名
****
組織名
部署名 個人名
組織の住所
組織のレンジに近い電話番号
組織のレンジに近いFAX番号
E-mail:*個人名*@*組織のドメイン*

組織名(英文)
WEB:*組織のWebサイトURL*
****

図-17 8月29日(木)に送信された標的型メール(1)

A. Poison IvyまたはPlugXを添付(11/11)
B. Poison IvyのC&Cサーバパスワードとして頻出文字列[*46]を設定(7/7)
C. フリーのWebメールサービスを使って送信(11/11)
D. Webメールへの接続元は国内の特定ISPのIPアドレス(10/10)
E. 会社組織などでの業務上のやりとりを偽装した文面や添付ファイル名(10/11)
F. RATの実行ファイルはアイコン偽装してZIPアーカイブされている(10/11)

一連の標的型メールは、添付されていたRATの種類(Poison IvyまたはPlugX)によって二分されますが、CからFの特徴は両者に共通します。Poison Ivyが添付されていたグループに関しては、利用されているC&Cサーバやそのパスワード文字列などの共通点から、同一の主体によって実施されている可能性が高いと考えられます。

(4)のPlugXは、C&Cサーバや送信元IPなど、(9)から(11)で利用されたPlugXと毛色が異なって見える部分がありますが、添付されていたPlugXの解析結果から、インストール情報やサービス名などに関して、同一の内容が設定されていることが分かっています。

更に、(9)から(11)のPlugXと(8)のPoison Ivyが同じC&Cサーバを設定されていたという事実が、一連の攻撃がすべて同一の主体によって行われていることを示唆しています。

なお、Cはすべてに共通する特徴ですが、これは個人利用などのメールアドレスを演出するだけでなく、正規のメールサービスを利用することで、メールの詐称を検出する、SPF・DKIMを迂回する意図があるものと推測されます。

C&Cサーバ:drives.methoder.com(50.2.160.125)
アカウントID:drive.●829
パスワード:keaidestone

※●は当該組織ドメイン名の一部

図-18 メール(1)に添付されていたPoison ivyの設定内容

*46 FireEye社の「Poison Ivy: Assessing Damage and Extracting Intelligence」(http://www.fireeye.com/resources/pdfs/fireeye-poison-ivy-report.pdf)において「keaidestone」「smallfish」はいずれも各々にC&Cサーバパスワードとして用いられた文字列であることが報告されている。

一方、攻撃の質に注目してみると、以下のような不備が目立ちます。

a. 日本語を装っているが、言い回しや体裁などに不自然な箇所がある。
b. 文書中では一般的な会社組織に存在するような部署名や日本人に一般的な名字などが用いられているが、当該組織に存在しない場合があった。
c. 既知の比較的有名なRATが用いられ、同じC&Cサーバが繰り返し使用された。

約2ヵ月間繰り返し攻撃が行われていたにもかかわらず、本質的な変化は見られません。(5)(6)のメールに添付されたPoison IvyのC&Cサーバのアカウント名の設定などは、流れ作業の一環のような印象を受けます。

前述の共通点とこの質的な状況を鑑みると、特別に当該組織を対象とした高度な攻撃が企てられたというよりは、当該組織など個別の組織を対象としながらも、半自動化・手順化され、比較的広範に対して行われるような低レベルの攻撃の一環であったのではないかと考えられます。実際に、IIJでは、今回の攻撃で利用されたRATのC&Cサーバと同じ、あるいは近傍アドレスのC&Cサーバを用いた攻撃が、少なくとも7つの他の組織に対して行われていたことを確認しています。

■ 当該組織における対応と影響

一連のメールのうち、(2)は当該組織で利用していたメールゲートウェイのアンチウイルスソフトウェアで検知・削除されました。また、(9)から(11)のメールは、メールゲートウェイに設定された添付ファイルフィルタによって削除されました。この添付ファイルフィルタは、(8)のメール受信後に当該組織が設定したもので、実行ファイルが添付されたメールを遮断します。

表-1 一連の標的型メール

	送信時期(JST)	送信者	サブジェクト	文字コード	添付ファイル名	感染方法	偽装アイコン	マルウェア(RAT)	送信元クライアント(Webメーラ利用元IPアドレス)	C&Cサーバ	PI ID	PI Password
(1)	8月29日(木)17時10分	▲@aol.com	Fw:_08/29(木)_職員連絡網の最新版データ送付	UTF-8	130829_連絡網(旧連絡網・使用不可.zip)	EXE(アイコン偽装)	XLS	Poison Ivy	126.114.231.116(JP)	drives.methoder.com 50.2.160.125(USA)	drive. ●829	keaidestone
(2)	8月30日(金)13時10分	▲@mail.goo.ne.jp	平成25年度後半年行政業務要点	UTF-8	平成25年度後半年行政業務要点.doc	CVE-2012-0158	--	Poison Ivy	(該当ヘッダなし)	scrlk.exprenum.com 50.2.160.125(USA)	GoodLuck830	keaidestone
(3)	9月5日(木)15時30分	▲@aol.com	平成25年度下期決算に向けての作業について	UTF-8	平成25年度下期決算に向けて.zip	EXE(アイコン偽装)	XLS	Poison Ivy	126.114.229.210(JP)	daddy.gostudyantivirus.com 50.2.160.84(USA)	●0905	smallfish
(4)	9月13日(金)15時20分	▲@yahoo.co.jp	ゴーヤー収穫のお知らせ	GB2312(実行ファイル名のみ)	130924行政現場視察(防衛省).zip	EXE(アイコン偽装)	--	PlugX	155.69.203.4(SG)	-- 54.250.220.230(AMAZON)	--	--
(5)	9月17日(火)12時50分	▲@aol.com	【締切09-17】2013年駐在員執務体制確認依頼の件	UTF-8	20130917_執務体制確認依頼書.zip	EXE(アイコン偽装)	XLS	Poison Ivy	126.19.84.213(JP)	daddy.gostudyantivirus.com 50.2.160.84(USA)	XXXXXXXXXX	smallfish
(6)	9月17日(火)12時50分	▲@aol.com	【報告】安全定期報告提出日のご案内	UTF-8	20130917安全定期報告提出日のご案内.zip	EXE(アイコン偽装)	PDF	Poison Ivy	126.19.84.213(JP)	daddy.gostudyantivirus.com 50.2.160.84(USA)	ZZZZZZZZZ	smallfish
(7)	9月24日(火)13時50分	▲@yahoo.co.jp	【新卒採用】履歴書を送付	UTF-8	▲.zip	EXE(アイコン偽装)	XLS	Poison Ivy	126.19.86.102(JP)	saiyo.exprenum.com 54.248.202.112(AMAZON)	saiyo0924	keaidestone
(8)	9月24日(火)15時50分	▲@aol.com	【送付】職員連絡網の最新版データ送付	UTF-8	20130924_職員連絡網最新版.zip	EXE(アイコン偽装)	DOC	Poison Ivy	126.65.195.56(JP)	saiyo.exprenum.com 54.248.202.112(AMAZON)	saiyo.ex	keaidestone
(9)	10月21日(月)16時31分	▲@aol.com	【重要】(事前連絡)合同会議並びに定期大会調整状況について	UTF-8	合同会議並びに定期大会調整状況.zip	EXE(アイコン偽装)	XLS	PlugX	126.15.4.120(JP)	saiyo.exprenum.com 54.248.202.112(AMAZON)	--	--
(10)	10月21日(月)16時32分	▲@aol.com	Fw:出版契約書	UTF-8	20131021仕様書_▲.zip	EXE(アイコン偽装)	XLS	PlugX	126.15.4.120(JP)	saiyo.exprenum.com 54.248.202.112(AMAZON)	--	--
(11)	10月21日(月)16時33分	▲@aol.com	Fw:自著紹介	UTF-8	20131021(月)自著紹介.zip	EXE(アイコン偽装)	XLS	PlugX	126.15.4.120(JP)	saiyo.exprenum.com 54.248.202.112(AMAZON)	--	--

●:攻撃を受けた組織のドメイン名の一部　▲:本文中で名乗っている送信者名などに関連した任意のアカウント名

経路で遮断されずエンドポイントまで配信されてしまったメールに対処するため、当該組織では標的型メールを受信するたびに、メール文面を添えた注意喚起を全組織的に行っていましたが、感染を完全に防ぐことはできませんでした。

この種の攻撃では感染を完全に防ぐことができない以上、感染を前提とした事後対応が重要になります。当該組織では、エンドポイントまでメールが配信されてしまった(1)及び(3)から(8)のケースについて、毎回以下のような流れで事案対応が行われました。

1. メールを不審に思った従業員が担当部門へ報告(=事案の発覚)
2. 添付ファイル(RAT)を解析
3. 解析結果に基づいてC&Cサーバへの通信を遮断(Firewall/DNS/Proxyなど)
4. 感染端末の調査(トラフィックログから端末を同定、適宜フォレンジック調査を実施)

攻撃のたびに、1から3が比較的迅速に実施されたため、当該組織は一連の攻撃によって情報漏えいや破壊・妨害行為などの被害を受けることはありませんでした。

■ 対策方針

一連の標的型メールのうち、アンチウイルスソフトウェアやメールサーバの設定などで遮断できなかったものについて、当該組織ではメールを受信した従業員の報告によって事案が発覚しています。しかしながら、配信ユーザの数や偽装の質によっては、報告が期待できない場合も考えられます。そのような攻撃でRAT感染してしまった場合に備えるためには、感染端末が組織内部で発生する不審な通信や認証試行などを検出・遮断するための「内部対策」[*47]の仕組みを用意しておくことが望まれます。

また、既に標的型メール攻撃を受けている場合には、今後も攻撃が継続することを前提として、次のような対応を推奨します。

- 過去の攻撃で利用されたC&Cサーバ及び近傍IPアドレスの遮断(Firewall)
- 過去の攻撃で利用されたC&Cサーバ関連ドメインの遮断(DNS、Proxy、Firewall)
- 過去の攻撃で利用されたC&C通信パターンの遮断(Proxy、IPS)
- 実行ファイル(EXE、DLL、SCRなど)添付メールの遮断
- 内部ネットワーク監視体制の強化(通信ログ記録内容の追加や分析頻度の増加など)

すべての標的型メール攻撃を防ぐものではありませんが、本稿の例のような、半自動化・手順化され、比較的広範に対して行われるような標的型メール攻撃に対しては、一定の効果が期待できます。

1.4.3 仮想通貨Bitcoin

本節では、一部のインターネット利用者の間で新しい通貨として流通し始めているBitcoinについて紹介します。Bitcoinには、現金による取引に比べ、いくつかのメリットがあります。このため、2009年1月に初めて通貨が作成されてから、現在も多くの取引が行われています。またこの体系では、通貨を作り出す採掘というプロセスにProof-of-workシステムを導入することで、計算リソースを仮想的な価値に変えることができます。現在では現金とも交換可能であるばかりか、店舗での支払いや、インターネット経由で現実世界の商品を買うことができるなど、実質的な通貨として認識されつつあります。本稿では、仮想通貨Bitcoinの技術的な解説とその周辺に起こっている事件、事故について紹介します。

Bitcoinは、P2Pネットワークと暗号技術を用い、利用者の匿名性を確保しながらコインの流通が可能な仮想通貨の一方式です。中本哲史氏を名乗る匿名の研究者による論文がBitcoinのコンセプトと共に2008年11月に公開されました[*48][*49]。約2ヵ月後の2009年1月には、The Cryptography Mailing ListにオープンソースであるBitcoin v0.1[*50]が投稿され、利用可能な実装が登場したことで、徐々に利用者が

*47 詳しくは、IPA「『標的型メール攻撃』対策に向けたシステム設計ガイド」(http://www.ipa.go.jp/security/vuln/newattack.html)参照。
*48 Satoshi Nakamoto、Bitcoin:A Peer-to-Peer Electronic Cash System(http://bitcoin.org/bitcoin.pdf)。
*49 中本 哲史、ビットコイン:P2P 電子マネーシステム(http://www.bitcoin.co.jp/docs/SatoshiWhitepaper.pdf)。この論文は日本語で書かれており、英語論文からの自動翻訳ではなく、日本語がネイティブな研究者により執筆されていると考えられている。なお、中本哲史氏は望月新一京都大学教授であるという指摘もある:Ted Nelson、"I Think I Know Who Satoshi Is"(http://www.youtube.com/watch?v=emDJTGTrEm0)。
*50 Bitcoin(http://sourceforge.net/projects/bitcoin/)。

増えました[*51]。この時点では、少数のコミュニティ参加者でP2Pネットワークが形成されてBitcoinの交換が行われており、Bitcoinそのものの価値は仮想的なものであったと考えられます。実際、初期に生成されたBitcoinは、まだ利用されていないものも多く見受けられます[*52]。

このように、狭い範囲の閉じた世界で流通していたBitcoinに対して、実世界での価値を見出し現実通貨との交換ができるようになったことが転機となります。当初は、Bitcoinでピザを購入するなどの取引事例はありましたが、現金との交換はできませんでした[*53]。その後、Bitcoinと実際の金銭とのやりとりが交換所でできるようになり、更にBitcoinによる支払いが可能な店舗・Webサイトも見られるようになりました[*54]。これは、クレジットカードに比べ手数料が低く、入金のタイミングが非常に早いことから、Webを使った通販業者などには十分なメリットがあったためと考えられます。Bitcoinと実際の金銭との交換所Mt.Goxは、現在最も知られた交換所の1つです[*55]。Mt.Goxにおける2011年から2013年までの米ドルとの交換レート[*56]を見ると、徐々に価値が上がっている様子が見てとれます。このようにBitcoinは研究者などの特定分野の利用層に留まらず、一般社会に受け入れられつつあります。

一方で、Bitcoinには悪用される側面もあります。2011年1月、Bitcoinの匿名性が注目され、インターネット市場Silk Road[*57]の決済方法として採用されました。ほぼ同時期に、Bitcoinの交換レートが急騰していたことからも、その熱狂ぶりが窺えます[*58]。決済時の匿名性確保というメリットにより、商取引を秘密裏に実施したいユーザが、この仕組みを利用しはじめたと分析できます。その後、Bitcoinの利用は拡大していきましたが、一方で、いくつかの事件に応じてその交換レートが大暴落するなどの変動も見せています。

■ 技術的解説

技術的側面でBitcoinを捉えると、以下の特徴を持っていることが分かります。

- コイン所有者に関する匿名性を持つ。
- 通貨発行などを行う中央組織は存在せず、コイン発行をユーザが行う。
- コイン利用は譲渡（所有者変更）を示すデータ（トランザクション）を作成する処理であり、デジタル署名により正当性が保証される。このトランザクションに付与された署名の連鎖を追うことで同一コインの多重利用を検知することができる。

現実世界での現金移動と比較すると、現金は各国政府の信用のもとに発行されています。また、インターネットを経由しての現金移動は、一般には匿名性を持つことが困難です。最後の特徴は、電子データは複製が容易であるという問題を解決するための仕組みを持つことです。以下、それぞれ3つの特徴について解説します。

まず、デジタル世界において通貨を扱うためには、所有者を示す識別子が必要となります。Bitcoinには、Bitcoin addressという一意に割り振られる識別子があります。Bitcoin addressはコイン所有者の公開鍵から生成されます。Bitcoinを利用したいユーザが鍵ペア生成を行うと、Bitcoin addressは自動

*51 Original Bitcoin client（https://en.bitcoin.it/wiki/Original_Bitcoin_client）によると中本氏は2010年末までチーフとメインの開発者として携わっていることが分かる。しかしその後の行方は不明となっている。
*52 最初のBitcoinに関する情報（https://blockchain.info/ja/block-height/0）。初期に生成されたコインはほとんど利用された形跡がないことが分かる。
*53 Bitcoin Forum、"Pizza for bitcoins?"（https://bitcointalk.org/index.php?topic=137.0）。現在に比べBitcoinの価値が遥かに低いレートであったことを示す例として知られる。
*54 例えばbitcoinstore（https://www.bitcoinstore.com/）やギフトカード購入サイトgyft（http://www.gyft.com/bitcoin/）、ファッション用品サイトBitfash（http://www.bitfash.com/）など。LocalBitcoins.com（https://localbitcoins.com/）では現在地を入力することでBitcoinの購入と利用が可能な店舗が検索できる。EFFなどでは早い段階からBitcoinによる寄付を受け付けている（https://www.eff.org/deeplinks/2011/01/bitcoin-step-toward-censorship-resistant）。また現地通貨とのBitcoinの交換方法についてはカナダにてBitcoin用ATMの販売が開始された（https://robocoinkiosk.com/）。更に中国BaiduではCloudFlareに似たサービスにおいてBitcoinでの支払いを開始するとのアナウンスがなされている（http://www.coindesk.com/chinese-internet-giant-baidu-starts-accepting-bitcoin/）。日本でもレストランでBitcoinが利用できる店舗が存在する。このように地理的にも分野としてもBitcoinの利用が拡大している。
*55 Mt.Gox（https://www.mtgox.com/）の他には、coinbase（https://coinbase.com/）、Bitstamp（https://www.bitstamp.net/）、BIT-e（https://btc-e.com/）などの現金との交換所がある。またLitecoin、Primecoin、Feathercoinなど他の仮想通貨との交換サービスを提供している交換所もある。
*56 現在までのレート変動の例として以下で参照できる。Bitcoin.org、"What determines bitcoin's price?"（http://bitcoin.org/en/faq#what-determines-bitcoins-price）。本校執筆期間においては、80米ドル/Bitcoinから260米ドル/Bitcoinまでの間で大きく変動している。
*57 Silk Road（https://silkroadvb5piz3r.onion.lu/）。現在は閉鎖されている。今年10月に取り扱う商品の問題から摘発され、巨額のBitcoinが押収された。
*58 Analysis of Silk Road's Historical Impact on Bitcoin（http://thegenesisblock.com/analysis-silk-roads-historical-impact-bitcoin/）。

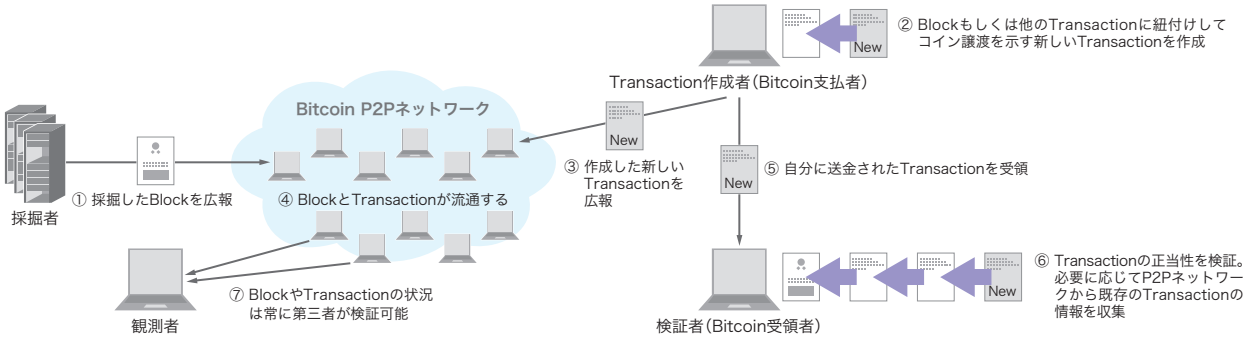
的にかつ他人と被ることなく割り振られます。この識別子の作成には、個人を特定するための情報は一切必要ないため、匿名性を確保することができます。更に、一人で複数のBitcoin Addressを生成することが可能であり、より匿名性を高めることができます。また、コイン利用時の情報の交換は、P2Pネットワークを介して行われるため、利用者の特定を困難にしています。

2つ目の特徴として、ユーザ自身がコインの発行を行うことが挙げられます。BitcoinではHashCash[*59]で導入された"Proof of work"という考え方が採用されています[*60]。新しいコインはある計算を行うことで発行され、この計算処理は採掘と呼ばれています[*61]。当初は非力なPCでもBitcoinが採掘できていましたが、現在ではGPUやASICを利用した採掘専用のハードウェアが開発され、販売が行われています[*62]。しかし、これらの装置は多大な電力を必要とするため、エコロジーの観点から問題視されていますし、採掘者が増えることで採掘の利益率は大きく減るようになっています[*63]。更に全体の通貨の発行量は、4年おきに減少することが定められています。これは、今から採掘に参加しても簡単に儲けることはできないことを意味しています。

最後は仮想通貨を安心して利用できることが保証されている点です。電子的な仮想通貨は、コイン複製が容易であるため、同一コインの多重利用を防ぐ必要があります。コインの移転を示すトランザクションは、連鎖的に構造化されており、別の過去のトランザクションと紐付けされています。あるトランザクションは、InputsとOutputsの情報で構成され、Inputsには入金されるコインを意味する既存のトランザクションのポインタ情報が、Outputsには譲渡先を示すBitcoin addressとコイン数量が記載されています。採掘された情報とトランザクションはすべて、Bitcoin利用者全員に行き渡っており、また不足があればP2Pネットワークで入手できます。そのため、取引時点もしくは後日に通貨の流れを把握したい場合には、どのトランザクションからどのようにコインが流れていったのかを一意に検証することができます。この仕組みにより、同一コインが多重利用されていないことを検証することができます。

■ Bitcoinの現状

このような背景のもと、仮想通貨交換所や口座管理サービスに対する攻撃が今年に入ってから急増しています。3月にBitInstantにてDNS詐称により現金窃取が[*64]、4月には



・[採掘] Bitcoinを採掘した者は、そのBitcoinに関する情報（Block）を、P2Pネットワーク上に広報する。
・[流通] Bitcoinの利用者は、現在見つかっているすべてのBitcoinの情報（Block）と、その流通を示すTransactionの情報もしくはそのポインタを、P2Pネットワークから取得している。
・[支払] Bitcoinで支払いをするとき、支払者は手元にあるBlockもしくはTransactionの情報から、新しいTransactionを作成し、それを受領者に渡すと共にP2Pネットワークに広報する。TransactionはBitcoin受領者とBitcoin数に関する情報が記載され、デジタル署名が施されるため、改ざん不可能である。
・[検証] Bitcoinの受領者は、手元にあるBlockとTransactionの情報もしくはポインタを利用してP2PネットワークからTransactionを収集することで、受け取ったTransactionの正当性を検証するために必要な情報を得る。
・[観測] 以上のように、発掘されたBitcoinとその利用の状況を、常時すべての利用者が共有、検索、検証できるようにすることで、Bitcoinの流れを把握し、同一Block/Transactionの多重利用を検知することができる。

図-19 Bitcoinの仕組み

＊59 Hashcash（http://hashcash.org/）、（https://en.bitcoin.it/wiki/Hashcash）。
＊60 Proof of work（https://en.bitcoin.it/wiki/Proof_of_work）。生成するのが困難な、ある条件を満たしたデータ群のことを指す。Bitcoinで利用されている困難性は＊61を参照のこと。
＊61 一定期間に生成されたトランザクションのリストを記録したデータをブロックと呼ぶ。ブロックは約10分ごとに生成されるが、このブロックには優劣が設けられており、より良いブロックを計算できた採掘者に新しいコインが割り当てられる。ブロックにはノンスと呼ばれるランダムデータのエリアがあり、このノンスを変化させてブロック全体のハッシュ値を計算し、より先頭に0が並ぶハッシュ値を持つブロックを見つける競争を行っている。そのようにして見つけられたブロックは誰からも譲渡されていないコインそのものとなる。詳しくはMining（https://en.bitcoin.it/wiki/Mining）を参照のこと。またBlockchain（https://blockchain.info/）にてブロックの連鎖と新しいコインの割り当ての最新状況を確認することができる。
＊62 例えば、Monarch - Bitcoin Mining Card（http://www.butterflylabs.com/monarch/）などを参照のこと。
＊63 Bitcoin currency statistics（http://blockchain.info/stats）。
＊64 BitInstantの当時のWebサイトは既に存在しないが、当時のアナウンスは次のInternet Archiveで確認できる。（http://web.archive.org/web/20130513055208/http://blog.bitinstant.com/blog/2013/3/4/events-of-friday-bitinstant-back-online.html）。

Coinbaseからユーザ情報の漏えい事件、Mt.GoxにてDDoS攻撃による障害発生が起こっています[*65][*66]。同じく4月には、感染者のPCで勝手にBitcoinの採掘を行うマルウェアが、Skype経由で拡散しているとの報告もなされました[*67]。更に翌5月には、ネットワークゲームのクライアントにBitcoin採掘用のコードが密かに挿入されていたことが発覚しています[*68]。また、8月にはAndroidにおけるいくつかのBitcoin関連アプリケーションにおいて脆弱性が公開されています[*69]。

一方で、政府によるBitcoinに対する見解がいくつか出されています。米国テキサス州連邦裁判所は、Bitcoinは通貨であり規制されるべきという見解を示しました[*70]。同様にドイツでもBitcoinを通貨として認知し、課税可能との見解を示しました[*71]。一方で、タイ政府はBitcoinの利用を全面的に禁止しました[*72]。

匿名性を持って取引ができ、中央組織を持たずに国境を越えて自由に流通してきたBitcoinは、技術的にも信頼できる仕組みとして認識され、今まさに一般社会に受け入れられようとしています。しかし、実際には悪用されているという側面もあります。今後Bitcoinがどのように扱われていくのかは、現時点では予測できません。しかし、Bitcoinは先駆的な試みであり、同様の仮想通貨が形を変えながら今後も登場するものと考えられます。

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、標的型攻撃で利用されるRAT「PlugX」、連続する標的型メール攻撃、仮想通貨Bitcoin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参ります。

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IIJ-SECT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)
鈴木 博志、春山 敬宏(1.4.1 標的型攻撃で利用されるRAT「PlugX」)
梨和 久雄(1.4.2 連続する標的型メール攻撃)
須賀 祐治(1.4.3 仮想通貨Bitcoin)
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、根岸 征史、小林 直、桃井 康成 IIJ サービスオペレーション本部 セキュリティ情報統括室

*65 Data On Merchant Pages(http://blog.coinbase.com/post/47198421272/data-on-merchant-pages)。
*66 Statement Regarding Recent DDoS Attacks and Mitigation(https://www.mtgox.com/pdf/20130424_ddos_statement_and_faq.pdf)。
*67 Skypemageddon by bitcoining(http://www.securelist.com/en/blog/208194210/Skypemageddon_by_bitcoining)。
*68 詳細については次のESEAの公式発表を参照のこと。"Bitcoin Fiasco"(http://play.esea.net/index.php?s=news&d=comments&id=12692)。
*69 bitcoin.org、Android Security Vulnerability(http://bitcoin.org/en/alert/2013-08-11-android)。擬似乱数のエントロピーの低さから秘密鍵の情報が漏えいするという報告があった。同様の事例はIIR Vol.17(http://www.iij.ad.jp/development/iir/pdf/iir_vol17.pdf)の「1.4.1 SSL/TLS、SSHで利用されている公開鍵の多くが他のサイトと秘密鍵を共有している問題」にて紹介している。
*70 判決については公開されていないが、次のInternet Archiveで確認できる(http://ia800904.us.archive.org/35/items/gov.uscourts.txed.146063/gov.uscourts.txed.146063.23.0.pdf)。
*71 一連の経緯についてはドイツの政治家であるFrank Schäffler氏のBlogでドイツ財務省とのやりとりが公開されている。"Bitcoin: Alle Anfragen und Antworten im Volltext"(http://www.frank-schaeffler.de/bitcoin-alle-anfragen-und-antworten-im-volltext/)(ドイツ語)。
*72 Bitcoin Co. Ltd. ,"Trading suspended due to Bank of Thailand advisement"(https://bitcoin.co.th/trading-suspended-due-to-bank-of-thailand-advisement/)。

DNS オープンリゾルバ問題

適切にアクセス制限されていないキャッシュDNSサーバをDDoS攻撃の踏み台として悪用されるケースが相次いでいます。オープンリゾルバと呼ばれるこういったキャッシュDNSサーバの問題点について解説します。

2.1 はじめに

今年3月、「史上最大のサイバー攻撃」と呼ばれた大規模なDDoS攻撃が行われたと報じられました[*1]。迷惑メール対策団体のSpamhaus及びSpamhausをホスティングしているCloudFlare社が最大300GbpsものDDoS攻撃を受けた事件[*2]で、CloudFlareが「インターネットが崩壊寸前まで追いこまれた」といささか誇張した表現を使ったせいもあってか[*3]、大きく注目を集めました。

このときに使われたのが、DNS amplification attack（DNS amp）という手法です。CloudFlare事件後も、5月にはDDoS対策サービスのProlexic社が167GbpsにのぼるDNS amp攻撃を受けたことを発表しており[*4]、他にも公表されていない多数の事例があると思われます。IIJによる観測でも、ほぼ恒常的に行われていることが分かっています。

本稿では、DNS amp攻撃、ならびにこの攻撃の踏み台として使われるオープンリゾルバの問題について考察します。

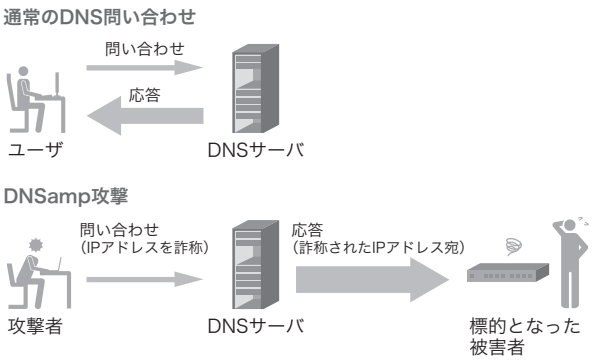


図-1 DNS amp

2.2 DNS ampとオープンリゾルバ

DNSは主にUDP上でやりとりされますが、UDPにはTCPのようなセッション確立手続きがありません。そのため、クライアントが悪意を持って自らのIPアドレスを詐称してもサーバはこれを検証できず、詐称されたIPアドレスに身に覚えのない応答が届けられることになります。これをリフレクション（反射）攻撃と呼びます。

DNSはもともと問い合わせよりも応答パケットの方がサイズが大きくなる性質があり、この比は最大で50倍以上にもなります。この増幅効果をリフレクション攻撃と組み合わせることで、攻撃者は少量の攻撃トラフィックを踏み台となるDNSサーバ（リフレクタ）に送るだけで標的のネットワークを埋めつくすことができます。これがDNS ampです（図-1）。ボットネットを利用すると更に効率的なトラフィック飽和攻撃が可能になります。

DNS ampは標的のネットワークに対する攻撃であり、ホストの特定の脆弱性を狙うものではありません。そのため対策が難しく、また、標的となった被害者からは踏み台とされたDNSサーバしか見えないため、真の攻撃者を特定するのが困難という特徴があります。

キャッシュDNSサーバは、組織ごとあるいはISPごとに用意しその内部のユーザだけにその機能を提供できれば十分で、不特定多数の用に供する必要はありません。このような外部からの不要なアクセスを制限していないキャッシュDNSサーバのことをオープンリゾルバと呼びます。

＊1 Internet Watch、「ネットを崩壊の瀬戸際に追い込んだ「史上最大のサイバー攻撃」が明るみに～早急な対策が望まれるオープンリゾルバーDNS問題」（http://internet.watch.impress.co.jp/docs/news/20130328_593523.html）。インターネットコム、「史上最大規模の DDoS 攻撃が、インターネット全体の速度低下を招く― SpamHaus と Cyberbunk 間のサイバー戦争で」（http://japan.internet.com/webtech/20130328/8.html）など。
＊2 http://www.apricot2013.net/__data/assets/pdf_file/0009/58878/tom-paseka_1361839564.pdf
＊3 http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet
＊4 http://www.prolexic.com/news-events-pr-prolexic-stops-largest-ever-dns-reflection-ddos-attack-167-gbps.html

オープンリゾルバはあらゆる送信元IPアドレスからの問い合わせに答えてしまうため、外部から自由にDNS amp攻撃の踏み台に悪用できてしまいます。非常に危険ですが、世界には多数存在しており、CloudFlareは3月の事件後、およそ8万のオープンリゾルバが関与していたと発表しています(アジア太平洋地域では日本が最多という残念な数字が出ています)[*5]。Open Resolver Projectの調査では、全世界に実に2800万ものオープンリゾルバが存在するとしており[*6]、対策の遅れが窺えます。

リフレクション攻撃やamp攻撃の手法自体は古くから知られており、遅くとも1999年には注意喚起されているようです[*7]。攻撃は主にDNSが使われますが、むしろUDPであることが本質なので、DNS以外のUDP上のプロトコル、例えばSNMPやNTPなどでも同様の攻撃が成立します[*8]。特に、SNMPは増幅率が1,000倍近くになることもあり[*9]、非常に危険性の高いものとなっています。

2.3 DNSキャッシュポイズニング攻撃

オープンリゾルバのキャッシュDNSサーバは、DNS amp攻撃の踏み台とされる以外に、キャッシュポイズニング攻撃を受けやすいという側面もあります。

キャッシュポイズニングは、キャッシュDNSサーバに対して細工された応答を注入し、偽の情報をキャッシュさせようとする攻撃です。これを成功させるには、キャッシュDNSサーバが権威DNSサーバに問い合わせを送った後、応答が返ってくるまでのわずか数ミリから数十ミリ秒程の間に偽造応答を割り込ませる必要があり、適切にアクセス制限されていれば、攻撃機会は非常に限定されます。

しかし、アクセス制限されていないキャッシュDNSサーバに対しては、攻撃者がトリガーとなる問い合わせを任意に送ることができ、偽造応答を送りこむタイミングも容易に制御できます。その結果、こういったサーバを利用しているユーザは、偽造された情報を受けとる危険性が高まることになります。

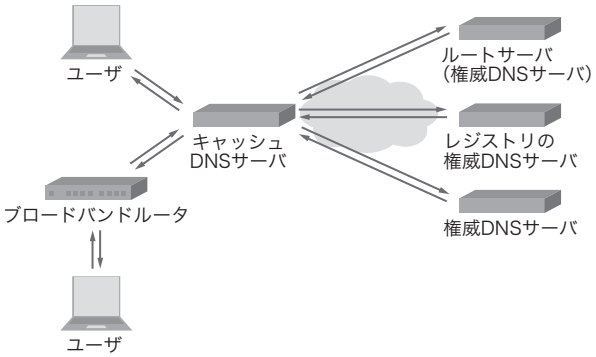
2.4 DNS ampの踏み台

リフレクション攻撃は、IPアドレスを詐称することで応答パケットの宛先を操作するものなので、DNSの応答を返すものはすべて踏み台になりえます(図-2)。

2.4.1 キャッシュ DNSサーバ

クライアントからの問い合わせを受けて、ルートサーバから順に権威サーバを探して名前解決を行うサーバです。前述のとおり、組織外からのアクセスは制限されるべきですが、現実にはそうではないものが多数存在しています。

例えば、権威DNSサーバとして運用しているつもりが、管理者の設定ミスや知識不足などの理由でキャッシュも有効になっていたなど、意図せずキャッシュDNSサーバとして動作しているものが踏み台にされるケースが多く見られるようです。



DNS応答を返すものはすべてampの踏み台になりえる。

図-2 DNSのプレーヤー

*5 前掲(http://www.apricot2013.net/__data/assets/pdf_file/0009/58878/tom-paseka_1361839564.pdf)。
*6 http://openresolverproject.org/breakdown.cgi
*7 http://www.auscert.org.au/render.html?it=80
*8 An Analysis of DrDoS SNMP/NTP/CHARGEN Reflection Attacks(http://www.prolexic.com/kcresources/white-paper/white-paper-snmp-ntp-chargen-reflection-attacks-drdos/index.html)。SNMP Reflected Amplification DDoS Attack Mitigation(http://www.bitag.org/documents/SNMP-Reflected-Amplification-DDoS-Attack-Mitigation.pdf)。
*9 http://mailman.nanog.org/pipermail/nanog/2013-July/060094.html

また、インターネット草創期にはこの攻撃手法が知られていなかったこともあり、相互扶助を意図してあえてアクセスを制限しないことも珍しくありませんでした。現在は当時と大きく事情が変化していますが、一度開放したものを後から制限するのは難しく、ISPなどでは歴史的経緯としてアクセス制限せず運用を続けているケースがあります。

2.4.2 ブロードバンドルータ

家庭用／業務用ブロードバンドルータの多くは、DNSフォワーダあるいはDNSプロキシと呼ばれる機能を持っています。宅内機器の名前解決のために使われるもので、本来LAN側からの名前解決要求にだけ答えればいいはずですが、一部に初期状態でWAN側からの問い合わせに無制限に答えてしまう製品が存在します[*10]。

ブロードバンドルータは、オープンリゾルバ以外にも外部から悪用される脆弱性を持つ製品が存在することが指摘されており、対策の必要性が議論されています。これについては、前号IIR Vol.20でも触れていますので参照ください。

2.4.3 権威DNSサーバ

DNSを構成するプレーヤーのうち、ゾーン情報を登録してキャッシュDNSサーバからの問い合わせに答える役割を担っているのが、権威DNSサーバ（コンテンツサーバ）です。

キャッシュDNSサーバやブロードバンドルータのDNSフォワーダは、外部から取得した情報のコピーを応答するので、増幅率が高くなるよう外部の攻撃者が情報を仕込むのも容易でした。しかし、権威DNSサーバは正当な管理者以外は情報を登録できないので、外部の攻撃者が意図的に増幅率の高い応答を返させるのは困難です。そのため、権威DNSサーバがDNS ampの踏み台として悪用されることはこれまでほとんどありませんでした。

しかし、DNSSECが有効になっていると、応答に電子署名が付加されるため、署名がない場合に比べて格段に応答が大きくなります。DNSSECはDNSのセキュリティ向上のための仕組みですが、見方を変えれば、攻撃者がわざわざ仕込まなくても十分に効率よく増幅できる踏み台を生み出してくれる仕組みであると考えることもできます。

権威DNSサーバの場合はオープンリゾルバとは呼ばれませんが、今後DNSSECの普及にともなってDNS ampの踏み台としての悪用事例も増えると想定され、対策が急がれています。

2.5 DNS amp対策

DNS amp攻撃に対する有効な対策手法をいくつか挙げてみます。RFC5358（BCP140）としてもまとめられていますので、そちらも参照してください[*11]。

2.5.1 アクセス制限

外部からのアクセスが適切に制限されていれば、仮にDNS ampの踏み台として狙われても、問い合わせが許可されていないとして無視するので、攻撃は成立しません。IPアドレスをアクセス許可されたものに詐称されている場合には制限が回避されてしまいますが、その場合でも応答する先は内部のネットワークになるため、少なくとも踏み台となって外部を攻撃することはなくなります。

また、LAN側インタフェースからの問い合わせのみを許可してWAN側からは無視する、といったネットワークインタフェースによる制限は、IPアドレスに頼らないため、外部からの不正な問い合わせ全般を防御できます。これはブロードバンドルータなど、複数のネットワークインタフェースを持つ機器では特に有効な対策です。

2.5.2 イングレスフィルタリング

リフレクション攻撃はパケットの送信元のIPアドレスを詐称することで行うので、ルータ側で詐称パケットの通過を許可しないように設定すると、攻撃は成立しなくなります。詐称IPアドレスによる攻撃手法は、他にもTCP SYN flood攻

＊10 JVN、「JVN#62507275 複数のブロードバンドルータがオープンリゾルバとして機能してしまう問題」（http://jvn.jp/jp/JVN62507275/）。ただし、この脆弱性レポートに記載されているもの以外にも、このような機器は広く販売されている（いた）ようなので注意が必要。
＊11 RFC5358（http://tools.ietf.org/html/rfc5358）。

撃やSmurf攻撃などいくつか知られており、これらも含めた根本対策として非常に有効です。この手法は、RFC2827(BCP38)で詳しく解説されています[*12]。

しかしながら、内部のネットワークから出ていくパケットに外部のIPアドレスが付与されている場合は比較的簡単に判別できますが、外部から流入してくるネットワークAからのパケットに、ネットワークBのIPアドレスが詐称されていても、それを判別するのは困難です。つまり、BCP38は外部からDNS ampの踏み台に悪用されないための防御策ではなく、内部のクライアントがIPアドレス詐称による不正行為を行えないようにするための対策となります。DNS amp攻撃は、自ら意図して攻撃を行うよりも、マルウェアに感染してボットとして意図せず攻撃に参加させられてしまうことが多いので、こういった攻撃がネットワーク内部から行われないようにするためにも必要な対策です。

世界中のネットワークでBCP38への対応が完了すれば、IPアドレス詐称による攻撃はなくなる理屈ですが、残念ながらほとんど対応は進んでいないのが現状です。

2.5.3 レート制限

キャッシュDNSサーバやブロードバンドルータと異なり、権威DNSサーバは不特定多数のキャッシュDNSサーバから広く問い合わせを受け付ける必要があり、アクセス制限するという手段は取れません。

キャッシュDNSサーバは、その名のとおり、受け取った応答を一定時間キャッシュするので、その間は権威DNSサーバに再度同じ問い合わせをすることはないはずです。この考えに立ち、権威DNSサーバでは、時間あたりの応答レートを制限することで大量の応答を抑止するという手法(RRL)が有望視されています[*13]。.orgや.infoなどのレジストリであるAffiliasは、amp攻撃の踏み台に使われて最大で2.3Gbpsまで増大した外向きのトラフィックが、RRLの導入により70Mbpsまで抑止されたと報告しています[*14]。

なお、アクセス制限ではなくレート制限によりamp攻撃の踏み台として悪用されにくくするというアプローチは、キャッシュDNSサーバに対しても一部で行われており、Google Public DNSは、この対策を行うことで不特定多数のユーザにオープンリゾルバを提供しています[*15]。

2.6 おわりに

DNS amp攻撃は、その手法自体は比較的古くから知られていたものの、十分な対策はこれまであまりされておらず、実質的に野放しに近い状態にあります。

国内では、今年に入ってから通信事業者各社やセキュリティ団体によって注意喚起や実態調査の動きが活発になってきましたが、実際の対策となると緒に就いたばかりというところで、道のりはまだまだ険しいと言わざるを得ません。

ここまで他人事のように筆を進めてきましたが、実はIIJにもオープンリゾルバとなっているキャッシュDNSサーバは存在しており、現在まさに対策を進めているところです[*16]。これまでの過ちを正しながら、安全なサービスを提供できるよう努めて参ります。

執筆者:

山口 崇徳(やまぐち たかのり)
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。2006年入社。メールサービス、DNSサービスの運用に従事。

*12 RFC2827(http://tools.ietf.org/html/rfc2827)。BCP38(http://www.bcp38.info/)。
*13 http://www.redbarn.org/dns/ratelimits
*14 http://lists.redbarn.org/pipermail/ratelimits/2012-December/000144.html
*15 https://developers.google.com/speed/public-dns/docs/security#rate_limit
*16 IIJ、「オープンリゾルバ根絶に向けての取り組み」(http://www.iij.ad.jp/company/development/tech/activities/open_resolver/)。てくろぐ、「『昔IIJを使っていた人』にお願いです – オープンリゾルバ対策」(http://techlog.iij.ad.jp/archives/718)。

「SDN」の最新動向

SDNとその周辺の最近の動向、ならびに株式会社ストラトスフィアの製品Omnisphereについて解説します。

3.1 最近の動向

「SDN[*1]」という単語は、もはやバズワードと言われる程一般的に知られるようになり、関連分野のマーケット活動は非常に活発です。筆者の個人的視点から最近のトピックを表-1にまとめました。要素技術としてはOpenFlowやVXLANに関連しています。

表-1 最近のSDN関連ニュース

日付	トピック
2012年２月７日	Nicira社がステルスを解除する
２月29日	OpenvSwitch 1.4.0 Fedoraパッケージ化される
３月10日	自宅ラック勉強会 #2.5 秋葉原出張編 開催
３月21日	OpenvSwitch kernel module 取り込まれたLinux 3.3リリース
４月16日	CloudStackがApache incubationプログラムに入る
６月	GoogleがSDN-WANを発表
６月25日	OpenFlow 1.3発行
７月23日	VMWare社がNicira社を買収
９月６日	OpenFlow 1.3.1発行
９月27日	OpenStack Folsomリリース
９月	trema-edge forkされる
10月31日	SSP 1.0リリース
11月30日	SSP 1.0.2リリース
12月10日	VXLAN kernel module取り込まれたLinux 3.7リリース
12月19日	Omnisphereプロジェクト開始
2013年２月５日	JR東日本駅構内設備にOpenFlowを使うと発表。無線LANも対象
２月13日	SSP 1.0.3リリース
３月20日	Apache CloudStackがtop level projectになる
３月29日	SSP 1.1.1リリース
４月	OpenDayLightプロジェクト公開
４月３日	trema-edgeを使い始める
４月４日	OpenStack Grizzlyリリース
４月15日	RDO(Red Hat)公開
４月17日	trema-openwrt公開
４月25日	OpenFlow 1.3.2発行
５月28日	Apache CloudStack 4.1リリース
６月12日	Interop Tokyo 2013開催 - Omnisphere発表
６月25日	Indigo Virtual SwitchがOpen Sourceになる (Big Switch Networks)
７月５日	SSP 1.1.2リリース
８月５日	OpenFlow 1.4発行
９月17日	SDN Japan 2013開催 - Omnisphere 1.0リリース
10月１日	Apache CloudStack 4.2リリース
10月17日	OpenStack Havanaリリース

:ストラトスフィアの動き

仮想OpenStack、Cloudstackのニュースを挙げていますが、これらはオーケストレータと呼ばれるソフトウェアで、仮想マシンを管理するハイパーバイザとその周辺コンポーネントをまとめて制御します。マイグレーション機能を使った際には仮想マシン移動前後で同じネットワーク環境を構築しなければなりませんが、オーケストレータでは、その調整のためにOpenFlowを活用しています。OpenFlowの事実上の本家であるNicira社をVMWare社が買収したニュースはインパクトがありました。

また象徴的なものはGoogle SDN-WANの発表で、OpenFlowを用いたネットワーク制御を世界規模で実運用に使用しているというものでした。オーケストレータでの用途とは異なる側面で、ネットワークのトラフィック制御に重点が置かれています。従来からあるBGPなどで制御されたネットワークとOpenFlow制御のネットワークとを結合して運用していることも実証されており、また、普段あまり語られないGoogleのネットワーク運用を垣間見られるという側面もあり、業界では話題になりました。

3.2 オフィス環境のSDN

一方で私たちは、オフィス環境ネットワークの運用に問題を抱えていました。オフィスフロアにネットワーク回線を敷設する際に、電源系統と同様に情報コンセントを床下配線し、フロアラックにあるスイッチングハブで集中管理しています。部署ごとに異なるネットワークを割り当てて運用していますが、そこではスイッチの機能であるVLANを使用してネットワークを隔離しています。そのため、人事異動などでオフィス内の座席配置が変わるたびにフロア情報コンセントに対応するVLANの設定変更が必要となります。この運用負荷は大きく、更にループなどが原因で発生するストーム

＊1 https://www.opennetworking.org/ja/sdn-resources/sdn-definition

の原因特定やその問題解消も重荷になっていました。無線によるネットワーク運用でも問題が出てきています。無線機器が普及し、例えばDHCPでの割り当てアドレスが足りないなど、当初想定していた容量を超える問題が起きています。これらをSDNのアプローチで解決できないかと考えていました。

これまでOpenFlowというと、オーケストレータやSDN-WANが話題の中心となっていました。オーケストレータは主にマシン群が設置されるデータセンター環境を想定されていますし、SDN-WANはバックボーン回線などが行きかうNOCの環境です。OpenFlowの仕組み自体は分野を特定するものではありませんが、資金面・研究分野からの連続性といった理由から、SDNを扱うマーケットは大規模ネットワークが盛んでした。これに対して、Omnisphereは身近なオフィス環境にSDNを適用する試みの1つとなっています。

3.3 Inside Omnisphere

今後の実装では変更される可能性もありますが、現時点でのOmnisphereの実装内部について記述します。Omnisphereは図-1のような構成になっています。

3.4 OpenFlow Switch

オフィス環境にOpenFlowを導入する場合、まず課題となるのは、安価なOpenFlowスイッチが入手できるかどうかです。高価なOpenFlowスイッチを使ってデモンストレーションを行っても、実際に導入するイメージとの乖離が大きくては説得力がありません。

OpenFlowプロジェクト本体に、OpenFlow 1.0のリファレンス実装を用いた「Pantou for OpenWrt[*2]」というプロジェクトがありました。OpenWrt[*3]は、市販ルータのファームウェアを書き換えて、汎用的なLinuxとして使えるようにするプロジェクトです。専用のOpenFlowスイッチは現在でも簡単に手に入るものではありませんが、OpenFlowが作られはじめた当初から、OpenFlowスイッチの解の1つとして使われてきたようです。

日本のコミュニティに知れ渡ったのは「自宅ラック勉強会#2.5秋葉原出張編[*4]」でしょう。日曜大工的な感覚でOpenFlowハードウェアスイッチを作ることができるということで、ハッカー的な心をくすぐる課題となりました。自宅ラック勉強会#2.5は、安価に入手できるBuffalo AirStationをOpenFlow対応スイッチにして遊びましょう、という趣旨の会で、盛況だったそうです。余談ですがこの会の主催者の1人は、これを使って「Interop Tokyo 2012特別企画Open Router Competition」でNEC賞を受賞されています[*5]。そのような中、ストラトスフィアでもBuffalo AirStationを用いた実験を始めていました。この時点で有線・無線LANを同時に進めるのは自然な流れでした。

Omnisphereの開発にあたっては、いくつかの理由から総合的に判断し、OpenFlow 1.3をターゲットとしました。具体的には、1）オフィス環境に設置されるOpenFlowスイッチはNOC設置の想定よりは小さいリソースしかないものであり、その時点で最も省スペースに高性能な表現ができるプロトコルであること、つまり最新のプロトコルが望ましかったこと、また、2）OpenFlowを開発しているONF（Open Networking Foundation）においてOpenFlow 1.3で普及

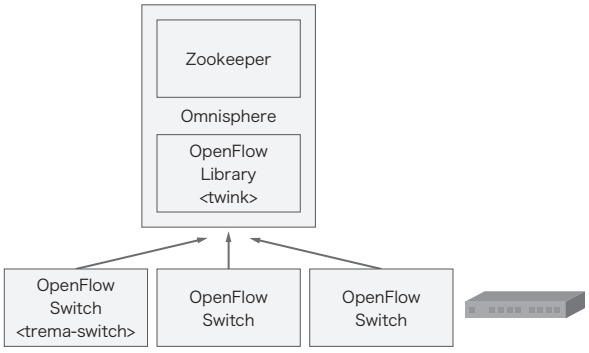


図-1 Omnisphereの構成

*2 http://archive.openflow.org/wk/index.php/Pantou_:_OpenFlow_1.0_for_OpenWRT
*3 https://openwrt.org/
*4 http://atnd.org/events/26147
*5 http://www.interop.jp/2012/orc/

を目指すという合意が一度なされていること、3)無線LANに対応した商用OpenFlowスイッチが存在せず、ほぼ新規に対応を目指すことになること、などです。ちょうどtremaがOpenFlow 1.3対応を目指したtrema-edge[*6]をforkして、開発がかなり進んでいたところでもありました。

tremaはOpenFlowコントローラのためのフレームワークとして知られていますが、trema-edgeにはそれに付随してC言語で記述されたOpenFlow 1.3ソフトウェアスイッチがあります。OpenFlow 1.3に対応したスイッチ実装は、他にofsoftswitch[*7]やIVS[*8]などがあります。OpenFlow 1.3を比較的シンプルに実装しているという理由で、私たちはtrema-edgeのスイッチを開発に活用することにしました。trema-switchをOpenWrt上で動作させるためには、OpenWrtのフィードを使ってファームを作ります。フィードは、GitHubで公開しています[*9]。Interop 2013ではこのスイッチ実装を用いて実際にデモンストレーションを行いました。

3.5 OpenFlow Library

OpenFlowプロトコル部分のフレームワークについては、必要な機能を満たすフレームワークが存在しなかったため、新規に作成しました。OpenFlowアプリケーションのフレームワークとしてはフロールールを書くことが簡単に、また簡潔に記述できることが重要になります。フロールールが簡潔にプログラム中に記載されているということは、そのままプログラムのメンテナンス性に直結します。そこでOpen vSwitch ovs-ofctlでの記述形式も使えるようにしました。

よくあるOpenFlowライブラリでは、OpenFlowメッセージの解析・組立がTCPサーバの機能と一体になっています。OpenFlowメッセージを作成する際には、ライブラリ独自の流儀に合わせるための学習コストが高いのはもちろん、ライブラリが対応していない部分については手が出せなくなってしまいます。OpenFlow 1.3で導入されたAuxiliary connectionでは、UDPのサブ接続を持つことができるのですが、サーバ機能が一体になっているものは対応が困難です。作成したライブラリでは、I/Oイベントループとプロトコル解析部分を分離し、コントローラのコアからはプロトコルバイナリフォーマットを翻訳する機能を一切なくしています。

実際の開発や運用ではOpenFlowスイッチがコントローラと接続中であっても、OpenFlowスイッチに対して直接状態の問い合わせを行いたいので、このような問い合わせを中継できるコントローラをフレームワーク内に用意しました。UNIX domain socketからの接続を外部プログラムからの中継の入り口として使えるようにもしました。OpenFlowスイッチからの出力をすべてモニタリングする外部出力も作りました。

構成についてまとめると、図-2のようになっています。コントローラが複数の上位アプリケーションと通信する際は、OpenFlowのBARRIERメッセージで隔離しています。フレームワーク中でOpen vSwitch表記で記述したフロールールはovs-ofctlの引数となって、コントローラを経由してOpenFlowスイッチへと届きます。モニターポートを設置する点はOpen vSwitchを参考にしました。中継ポートを使うと、複数のOpenFlowアプリケーションをチェーンすることもできます。

このような構成のため、ライブラリのコア部分はOpenFlowプロトコルバイナリフォーマットをそのまま使っています。プロトコルバイナリフォーマットを扱うライブラリは、OpenFlowのメッセージを直接的に作成したいときに必要になるので、別途単体で作成しました。

*6 https://github.com/trema/trema-edge
*7 http://cpqd.github.io/ofsoftswitch13/
*8 http://www.projectfloodlight.org/indigo-virtual-switch/
*9 https://github.com/iHiroakiKawai/trema-openwrt

3.6 Zookeeper

SDNはネットワーク制御部分とデータ通信部分を分離して、制御部分をよりプログラマブルに扱えるようにするアーキテクチャを指します。より具体的には、GoogleのOnix[*10]の発表にも登場します。制御部分を分離するということは、ますます高性能化する汎用サーバ機を使えるということで、一体化していた場合と比べて、制御部分のロジック拡張が飛躍的に自由になります。汎用サーバ機を計算資源として使うことは、暗に分散コンピューティングを行うことを示しています。SDNを成立させている背景には、そのような分散コンピューティングの環境が整ってきたことも要因だと考えています。

OmnisphereではApache Zookeeperを使っています。ZookeeperはHadoopから派生したプロジェクトで、Hadoop 2.0の基本コンポーネントです。合意アルゴリズムとして有名なPAXOSはGoogleのOnixで使われていましたが、ZookeeperではZabと呼ばれる同等のアルゴリズムを実装しています。

Zookeeperは分散したコンピュータ上で矛盾なく扱えるようにメンテナンスされたツリー構造を提供します。ツリー構造は直接使うこともできますが、そのままでは使いづらいので、ZookeeperにはRecipeと呼ばれるクラスが付属しています。Recipeはこのツリー構造を内部で使用して、キューやロックに始まり、リーダー選出アルゴリズムなど、使いやすいインタフェースを提供しています。アプリケーションから利用する際は、ツリー構造の一部をこのような機能に割り当てて使います。

3.7 まとめ

Omnisphereでは、スイッチ側にはフリーで利用できる実装を活用しつつ、コントローラ側には現代的なソフトウェア基盤を使って構築されております。

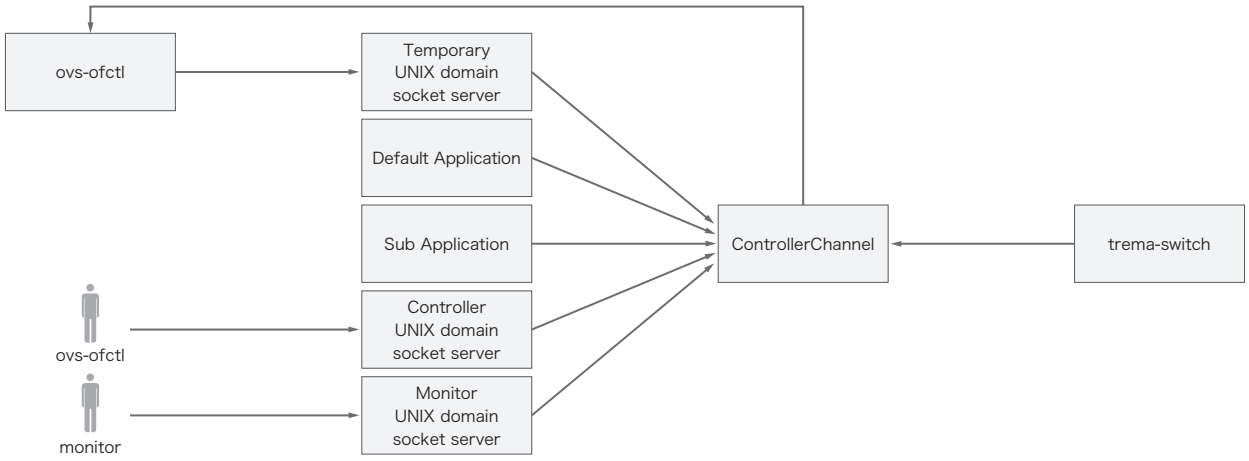


図-2 フレームワーク中でovs表記を使った場合

執筆者:
川井 浩陽(かわい ひろあき)
株式会社ストラトスフィア。2003年IIJ入社。2006年i-revo立ち上げに参加。関西在住でApache好きのオープンソース畑育ち。

*10 https://www.usenix.org/conference/osdi10/onix-distributed-control-platform-large-scale-production-networks

Vol.21 November 2013

株式会社インターネットイニシアティブ(IIJ)について

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

株式会社インターネットイニシアティブ

〒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@iij.ad.jp　URL：http//www.iij.ad.jp/

IIJ-MKTG019UA-1311GR-09300PR