# Forward Secrecy

**今回は、大容量メモリを搭載した端末のメモリフォレンジックにおける注意点、暗号通信の安全性を高める技術であるForward Secrecy、Webクローラによる Webサイト改ざん調査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自身が取得した一般情報、インシデントの観測情報、サービスに関連する情報、協力関係にある企業や団体から得た情報を元に、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10月から12月までの期間では、前回の期間に続いてAnonymousなどのHaktivismによる攻撃が複数発生しており、日本に対する活動も実施されました。また、国外で数千万人分のユーザのIDやパスワードが漏えいする事件が発生するなど、認証情報を狙った攻撃も継続しています。これに関連して、オンラインサービスに対するリスト型攻撃も頻発しています。12月にはNTPサーバを踏み台とした100Gbpsを超える大規模なDDoS攻撃が複数発生しました。このように、インターネットでは依然として多くのインシデントが発生する状況が続いています。

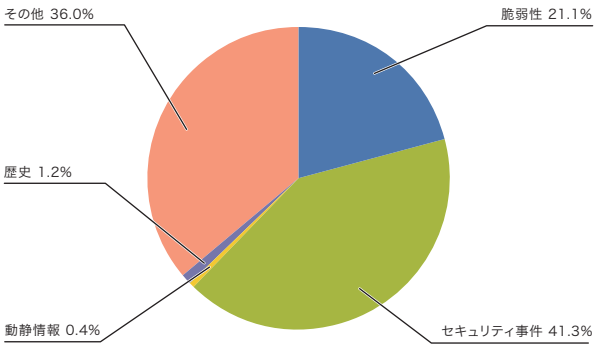



**図-1 カテゴリ別比率(2013年10月〜12月)**

## 1.2 インシデントサマリ

ここでは、2013年10月から12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。10月にはギリシャ、ポーランド及びウクライナなどの国々や欧州安全保障協力機構(OSCE)において、Anonymousによる攻撃により大量の内部資料の漏えいが発生しています(OpGoldenDawn)。11月にはオーストラリアの情報機関によるインドネシア政府に対する諜報活動への抗議として、インドネシアのAnonymousによるオーストラリアのWebサイトへのDDoS攻撃が活発に行われました。また日本の複数の政府機関のWebサイトをターゲットにしたAnonymousによる攻撃予告が行われましたが、12月になって日本のWebサイトから一部の設定情報などの情報漏えいが確認されたものの、特に組織だった攻撃活動は見られませんでした(OpKillingBay)。他にも主に南米や欧州など世界中の各国政府とその関連サイトに対して、AnonymousなどのHacktivistによる攻撃が継続して行われました。またSyrian Electronic Armyを名乗る何者かによるドメインハイジャックやWebサイト改ざん、SNSアカウントの乗っ取り攻撃も継続して発生しています。

*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。

### ■ 脆弱性とその対応

この期間中では、Microsoft社のWindows[*2 *3 *4 *5 *6]、Internet Explorer[*7 *8 *9]、Office[*10]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でも四半期ごとに行われている定例の更新が行われ、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[*11]。

サーバアプリケーションでは、データベースサーバとして利用されているOracleを含むOracle社の複数の製品で四半期ごとに行われてる更新が提供され、多くの脆弱性が修正されました。また、DNSサーバのBIND9 Windows版では、namedのlocalnetsアクセスコントロールリストが誤って設定されてしまう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として人気の高いRuby on Railsでは、XSS可能な脆弱性を含む複数の脆弱性が見つかり、修正されています[*12]。Webアプリケーションフレームワークの Apache Strutsでも、特定のパラメータを介したアクセスによってアクセス制御を回避される脆弱性[*13]など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Joomla!についても任意のファイルをアップロードすることができる脆弱性が修正されています[*14]。

### ■ 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。10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。コスタリカのドメインである.crでも複数の有名なドメインがハイジャックされる事件が発生しています。カタールのドメインである.qaを管理しているccTLDレジストリであるdomains.qaでも不正アクセスにより、GoogleやFacebook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。アフリカのルワンダのドメインである.rwでも何者かによる不正アクセスを受け、TwitterやGoogle、Facebookなどの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ています。また、10月にはホスティング事業者や複数のアンチウイルスベンダ、セキュリティベンダ、SNS事業者など多くの企業のサイトが、何者かにドメインハイジャックされる事件が連続して発生しました。これらの事件では複数のレジストラが集中して狙われていました。

---

*2 「マイクロソフト セキュリティ情報 MS13-081 - 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 (2870008)」(http://technet.microsoft.com/ja- jp/security/bulletin/ms13-081)。
*3 「マイクロソフト セキュリティ情報 MS13-083 - 緊急 Windowsコモン コントロール ライブラリの脆弱性により、リモートでコードが実行される (2864058)」(http://technet.microsoft.com/ja- jp/security/bulletin/ms13-083)。
*4 「マイクロソフト セキュリティ情報 MS13-089 - 緊急 Windows Graphics Device Interfaceの脆弱性により、リモートでコードが実行される (2876331)」(http://technet.microsoft.com/ja- jp/security/bulletin/ms13-089)。
*5 「マイクロソフト セキュリティ情報 MS13-090 - 緊急 ActiveXのKill Bitの累積的なセキュリティ更新プログラム (2900986)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-090)。
*6 「マイクロソフト セキュリティ情報 MS13-099 - 緊急 Microsoft Scripting Runtime オブジェクトライブラリの脆弱性により、リモートでコードが実行される (2909158)」(http://technet.microsoft.com/ja- jp/security/bulletin/ms13-099)。
*7 「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)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-080)。
*8 「マイクロソフト セキュリティ情報 MS13-088 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (2888505)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-088)。
*9 「マイクロソフト セキュリティ情報 MS13-097 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (2898785)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms13-097)。
*10 「マイクロソフト セキュリティ情報 MS13-096 - 緊急 Microsoft Graphics コンポーネントの脆弱性により、リモートでコードが実行される (2908005)」(http://technet.microsoft.com/ja- jp/security/bulletin/ms13-096)。
*11 例えば、IPAでは次の注意喚起を行っている「Microsoft Office 等の脆弱性(CVE-2013-3906)を悪用する国内の組織に対する標的型攻撃を確認 ～不審メールへの警戒、緊急対策の実施を～」(http://www.ipa.go.jp/security/topics/alert20131120.html)。
*12 Ruby on Rails、"Rails 3.2.16 and 4.0.2 have been released!"(http://weblog.rubyonrails.org/2013/12/3/Rails_3_2_16_and_4_0_2_have_been_released/)。
*13 The Apache Software Foundation.,"S2-018:Broken Access Control Vulnerability in Apache Struts2" (http://struts.apache.org/release/2.3.x/docs/s2-018.html)。
*14 JVN、「Joomla! にファイルアップロードに関する脆弱性」(https://jvn.jp/vu/JVNVU99659350/index.html)。

## 10月のインシデント

1 他 **1日**：総務省は、複数のISP事業者やセキュリティベンダー等と連携し、利用者のマルウェアへの感染防止と駆除の取り組みとして、マルウェア配布サイトへのアクセスを未然に防止する実証実験などを行う官民連携プロジェクト（ACTIVE）を11月1日から実施することを公表した。
「『ACTIVE』の実施及び『ACTIVE推進フォーラム』」の開催（http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000059.html）。

2 他 **2日**：米国議会の暫定予算案不成立により、一部の連邦政府機関が閉鎖され、国立標準技術研究所（NIST）など複数の政府関係のサイトが閲覧できなくなった。この措置は10月17日に解除された。

3 セ **3日**：GitHubが大規模なDDoS攻撃を受け、翌日までの間、断続的にサービス障害が発生した。
詳細については、次のGitHubStatusの10月3日のメッセージで確認できる。"Status Messages"（https://status.github.com/messages/2013-10-3）。

4 セ **3日**：米国連邦捜査局（FBI）はTorネットワークを利用したアンダーグランドサイトであるSilk Roadのテイクダウンを行い、容疑者を逮捕した。
詳細については例えば次のKrebs on Security Blogに詳しい。"Feds Take Down Online Fraud Bazaar 'Silk Road', Arrest Alleged Mastermind"（http://krebsonsecurity.com/2013/10/feds-take-down-online-fraud-bazaar-silk-road-arrest-alleged-mastermind/）。

5 セ **4日**：Adobe社は、システムへの不正侵入が発生し、290万人分のユーザ情報と複数の製品のソースコードが漏えいした疑いがあることを公表した。
詳細については、次のAdobe社の発表などに詳しい。「お客様情報のセキュリティに関する重要なお知らせ」（http://blogs.adobe.com/japan-conversations/セキュリティに関する重要なお知らせ/）。

6 セ **8日**：スロバキアのESET社やルーマニアのBitdefender社、ドイツのAvira社など複数のアンチウイルスベンダのサイトが何者かにドメインハイジャックされる事件が発生した。
詳細については、例えば被害を受けた企業の1つであるAVG社のBlogなどを参照のこと。"Website issue, Tuesday 8 October"（http://blogs.avg.com/news-threats/website-issue-tuesday-8-october/）。

7 他 **8日**：国際的なインターネット関連10団体は、インターネットに関わる新たな課題について会合を行い、これらの課題に対する「今後のインターネット協力体制に関するモンテビデオ声明」を発表した。
一般社団法人日本ネットワークインフォメーションセンター（JPNIC）、「インターネット関連10団体が『今後のインターネット協力体制に関するモンテビデオ声明』を発表」（https://www.nic.ad.jp/ja/topics/2013/20131008-01.html）。
"ICANN Montevideo Statement on the Future of Internet Cooperation"（http://www.icann.org/en/news/announcements/announcement-07oct13-en.htm）。

8 脆 **9日**：Microsoft社は、2013年10月のセキュリティ情報を公開し、MS13-080やMS13-081、MS13-083を含む4件の緊急と4件の重要な更新をリリースした。
「2013年10月のセキュリティ情報」（http://technet.microsoft.com/ja-jp/security/bulletin/ms13-oct）。

9 脆 **9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。
「APSB13-25: Adobe Reader及びAcrobat用セキュリティアップデート公開」（http://www.adobe.com/jp/support/security/bulletins/apsb13-25.html）。

10 セ **11日**：マレーシアのドメインである.myで、何者かによるドメインハイジャックにより、GoogleのWebサイトが別のWebサイトに誘導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。"MYNIC Official Announcement"（http://mynic.my/en/news.php?id=162）。

11 セ **12日**：米国のセキュリティベンダであるRapid7社のMetasploit.com、Rapid7.comの2つのサイトが何者かにドメインハ イジャックされる事件が発生した。
詳細については次のKaspersky Lab Threatpostなどを参照のこと。"Phony Order Faxed to Registrar Leads to Metasploit Defacement"（http://threatpost.com/phony-order-faxed-to-registrar-leads-to-metasploit- defacement/102576）。

12 脆 **13日**：D-Link社の複数のルータ製品に特定の文字列をUser-Agentに設定することで、管理画面の認証を回避できることが公表され、修正が行われた。
JVN、「JVNVU#90204379 複数のD-Link製ルータに認証回避の脆弱性」（http://jvn.jp/cert/JVNVU90204379/）。

13 セ **15日**：コスタリカのドメインである.crが何者かによる不正アクセスを受け、GoogleやYahoo!といった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。

14 脆 **16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127件の脆弱性を修正した。
なお、今回の定例アップデートからJavaの脆弱性の修正（51件）も含まれるようになっている。"Oracle Critical Patch Update Advisory - October 2013"（http://www.oracle.com/technetwork/topics/security/cpuoct2013-1899837.html）。

15 セ **19日**：カタールの.qaのccTLDレジストリであるdomains.qaが、何者かによる不正アクセスを受け、GoogleやFacebook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。

16 セ **25日**：ルワンダのドメインである.rw が何者かによる不正アクセスを受け、Googleのサイトがドメインハイジャックされる事件が発生した。
詳細については例えば次のUmbrella Security Labs社のBlogなどに詳しい。"THE GOOGLE.RW HIJACK NOBODY ELSE NOTICED"（http://labs.umbrella.com/2013/10/25/google-rw-hijack-nobody-else-noticed/）。

17 セ **25日**：一般家庭からインターネットに接続する際に使用するＩＤやパスワードが盗まれ、サイバー攻撃に悪用される被害が発生してしていることが報道された。原因については、2012年に公表された脆弱性のあるホームルータによるものと考えられ、対象として30万台出荷されていることから広く注意喚起が行われた。
詳細については次のNHK「かぶん」ブログに詳しい。「家庭のネットＩＤなど悪用被害１５０件超」（http://www9.nhk.or.jp/kabun-blog/1000/171059.html）。
また、この脆弱性については7月にTelecom-ISAC Japanからも注意喚起が行われている。「【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）。

18 他 **31日**：JPCERT/CCは、ユーザの利用環境におけるDNSサーバとブロードバンドルータなどのネットワーク機器が、オープンリゾルバでないかをユーザが確認できるサイトを公開した。
JPCERTコーディネーションセンター、「オープンリゾルバ確認サイト公開のお知らせ」（http://www.jpcert.or.jp/pr/2013/pr130002.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

### ■ 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、2013年3月頃から多数発生しているユーザのIDとパスワードを狙った試みと、取得したIDとパスワードのリストを使用したと考えられるなりすましによる不正ログインの試みが継続して発生しています。携帯向けSNSなどの会員向けサービスサイトやポイントサービス、通信販売サイト、カード会員向けのサービスサイトなど多くのWebサイトに対し、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が行われる事件が多く発生しています。

また、10月にはAdobe社で不正アクセスが発生し、同社の顧客情報や一部の製品のソースコードが流出する事件が発生しています。この事件では当初290万人分とされた個人情報の流出がその後の調査で少なくとも3800万人分であることが判明するなど大規模な情報流出事件となりました。更に漏えいした会員情報が何者かにインターネットで公開されたことで、Facebookや複数の企業ではリストにあったユーザアカウントを一時的に停止してパスワードの変更を促すなどの対応が行われました[*15]。このように、IDとパスワードの組み合わせリストを利用したと考えられる不正アクセスは継続しており、引き続き注意が必要です。

### ■ 政府機関の取り組み

ビッグデータを使った取り組みや新しいサービスが話題となっていますが、それと同時に消費者の購買履歴や電子マネーの利用履歴などの個人に関する情報（パーソナルデータ）を含んだビッグデータの利活用とプライバシーの保護については様々な問題が指摘されたり議論されてきました。政府としても、平成25年6月に閣議決定された、「世界最先端IT国家創造宣言[*16]」において、より積極的なIT・データの利活用の推進を宣言しており、2013年9月から、パーソナルデータに関する利活用ルールの明確化等に関する調査及び検討を行うため、高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）のパーソナルデータに関する検討会[*17]及びその技術検討ワーキンググループを開催して検討を行っていました。

12月に、保護されるパーソナルデータの範囲を明確化し、個人が特定される可能性を低減した加工データについては、第三者提供にあたり本人同意を要しない類型とし、取り扱う事業者が負うべき義務等を法的に措置するなどのパーソナルデータの利活用に関する「パーソナルデータの利活用に関する制度見直し方針案」がまとめられました。この中では、独立した第三者機関を設置するなどパーソナルデータの保護に向けた体制の整備も併せて提言されています。これを受けて12月20日に開催された、IT総合戦略本部第63回会合で同方針案が決定しました。今後、課題の検討や整理を行いながら個人情報保護法の改正を含んだ法整備が行われていくことになります。

11月から、総務省の「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」が開催されています。これは、現在行われている電気通信事業者によるガイドライン[*18]による対応について、巧妙化・複雑化するサイバー攻撃に対し、電気通信事業者が通信の秘密等に配慮しつつ、新たな対策や取り組みを講じていくことが可能となるように、必要に応じて適正な対処の在り方について検討を行うことを目的としています。

### ■ NSA関連

米国家安全保障局（NSA）及びその協力機関の諜報活動に関して、6月より欧米のメディア各社による報道が継続して行われていますが、この期間においても新たな情報が次々と明るみに出ました。特に欧州各国における電話盗聴、世界各国の首脳の電話盗聴、米国大使館における通信傍受などの報道については、その対象となった関係各国において、米国や英国によるこれらの活動に対する非難が起こっており、外交などへの影響が懸念されています。

これに対し、10月にはインターネット関連10団体が共同

＊15 詳細については次のKrebs on Security Blogに詳しい、"Facebook Warns Users After Adobe Breach"（http://krebsonsecurity.com/2013/11/facebook-warns-users-after-adobe-breach/）。
＊16 「世界最先端IT国家創造宣言について」（http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20130614/siryou1.pdf）。
＊17 「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）。
＊18 電気通信事業関連の4団体による、「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン第2版」（http://www.jaipa.or.jp/other/mtcs/110325_guideline.pdf）。

## 11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

脆 **6日**：Microsoft社は、Microsoft Graphics コンポーネントに脆弱性（CVE-2013-3906）があり、特別に細工されたファイルにより、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。この脆弱性については公表時に既に攻撃が確認されていた。
「マイクロソフト セキュリティ アドバイザリ (2896666) Microsoft Graphics コンポーネントの脆弱性により、リモートでコードが実行される」（http://technet.microsoft.com/ja-jp/security/advisory/2896666）。

他 **6日**：Apple社は、初めてとなる2013年1月から6月の期間のTransparency Reportを公開した。
"Report on Government Information Requests"（http://images.apple.com/pr/pdf/131105reportongovinforequests3.pdf）。

他 **8日**：IPAは、複合機等のオフィス機器の情報がインターネットから閲覧できる状態になっている問題について、必要がなければネットワークに接続しないことや適切な管理を行うことなどの対策をまとめた注意喚起を公表した。
「プレス発表　複合機等のオフィス機器をインターネットに接続する際の注意点」（http://www.ipa.go.jp/about/press/20131108.html）。

脆 **12日**：ジャストシステム社の一太郎に、細工されたファイルにより任意のコードが実行される可能性のある脆弱性が見つかり、修正された。この脆弱性については、修正が行われる前に攻撃が確認されている。
「[JS13003] 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/js13003.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。
「APSB13-26: 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/apsb13-26.html）。

脆 **13日**：Microsoft社は、2013年11月のセキュリティ情報を公開し、MS13-088とMS13-089及びMS13-090の3件の緊急と5件の重要な更新をリリースした。
「2013年11月のセキュリティ情報」（http://technet.microsoft.com/ja-jp/security/bulletin/ms13-nov）。

セ **13日**：Anonymousによる日本の政府機関や関連組織への攻撃を予告したOpKillingBayが発表された。

他 **13日**：Microsoft社は、アプリケーションの脆弱性を緩和するセキュリティツールであるEnhanced Mitigation Experience Toolkit（EMET）4.1をリリースした。
詳細については次のTechNet Blogsなどを参照のこと。「EMET 4.1を公開 ～ 構成ファイルや管理機能の強化」（http://blogs.technet.com/b/jpsecurity/archive/2013/11/15/3611107.aspx）。

セ **14日**：京都大学、筑波大学、高エネルギー加速器研究機構など複数の研究機関は、それぞれのスーパーコンピュータシステムが外部からの不正アクセスを受けたことを公表した。
詳細については、例えば、次の高エネルギー加速器研究機構（KEK）の発表などを参照のこと。
「KEKコンピューターシステムに対する不正アクセスについて」（http://www.kek.jp/ja/NewsRoom/Release/20131114180000/）。
「KEKコンピューターシステムに対する不正アクセスについて(続報)」（http://www.kek.jp/ja/NewsRoom/Release/20131210170000/）。

セ **18日**：LG社のスマートTV（ネットワーク機能を搭載したテレビ）で、利用者の意図しない利用情報の送信を行っていたことが英国の技術者により公表された。
詳細については次の発見者のBlogなどを参照のこと。DoctorBeet's Blog,"LG Smart TVs logging USB filenames and viewing info to LG servers"（http://doctorbeet.blogspot.ru/2013/11/lg-smart-tvs-logging-usb-filenames-and.html）。

セ **19日**：GitHubでBrute Force攻撃による不正ログイン事件が発生した。
詳細については、次のGitHubのBlogを参照のこと。"Weak passwords brute forced"（https://github.com/blog/1698-weak-passwords-brute-forced）。

脆 **20日**：IPAより、11月6日にMicrosoft社より公表された Microsoft Graphics コンポーネントの脆弱性(CVE-2013-3906) について、国内の組織に対し、当該脆弱性を悪用した「履歴書.zip」などのファイルをメールに添付した攻撃の事例が確認されたとして注意喚起が行われた。
「Microsoft Office等の脆弱性(CVE-2013-3906)を悪用する国内の組織に対する標的型攻撃を確認　～不審メールへの警戒、緊急対策の実施を～」（https://www.ipa.go.jp/security/topics/alert20131120.html）。

他 **23日**：Twitter社は、ユーザ情報の保護の強化を目的として、SSL通信のForward Secrecyに対応したことを公表した。
Twitter, Inc、Engineering Blog、"Forward Secrecy at Twitter"（https://blog.twitter.com/2013/forward-secrecy-at-twitter-0）。

脆 **28日**：Microsoft社は、Windows XP及びWindows Server 2003のカーネルコンポーネントに脆弱性（CVE-2013-5065）があり、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 (2914486) Microsoft Windows カーネルの脆弱性により、特権が昇格される」（http://technet.microsoft.com/ja-jp/security/advisory/2914486）。

他 **29日**：総務省は、電気通信事業におけるサイバー攻撃への適正な対処の在り方について検討を行うことを目的として、電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会を開催した。
「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」（http://www.soumu.go.jp/main_sosiki/kenkyu/denki_cyber/index.html）。

［ 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

で「今後のインターネット協力体制に関するモンテビデオ声明」を発表しており、全世界の利用者の、インターネットに対する信頼と信任が損なわれる結果となっていることに強い懸念を表明しています。12月には国連総会でも個人のプライバシーについてデジタル通信も含めた保護を各国に求める"The right to privacy in the digital age"が全会一致で採択されています。またYahoo!やGoogleなどのデータセンター間の通信を、NSAが盗聴しているとの報道に関して、これらの事業者は対応を迫られました。これまで平文で行われていた通信の暗号化やPerfect Forward Secrecy (PFS)への対応など、通信の盗聴への対策を推進する動きが事業者において活発に行われました。PFSの詳細については「1.4.2 Forward Secrecy」も併せてご参照ください。

12月にはこれらの対象として名前の挙がった大手IT企業の7社が、政府による情報収集活動に対する法律による制限や通信の制限に対する規制を撤廃することなどを求めていく活動を開始しています。さらに、この問題を受けて情報機関による通信情報の収集活動について調査を行っていた米国大統領の諮問委員会では情報収集活動にいき過ぎがあったとして、安全保障上必要な機能を維持しつつ改革を行うよう提言が行われました。

### ■ クラウドサービスの利用とリスク

近年、オンラインストレージやオンライングループウェアなどクラウド環境を利用した機能やサービスが増えてきています。これらの機能は、様々な場所やデバイスから必要な時に利用できる利便性の良さからその利用が拡がってきています。一方で、これらの機能を業務で利用する場合には注意が必要な場合もあります。例えば、2013年7月には民間企業が提供していたグループメールサービスの利用に伴い、サービスの設定を、誤って公開状態としたことから、公開を前提としていない情報や機密情報の漏えい事案が複数の省庁で発生しています[*19]。

この期間では、日本語IME (Input Method Editor)のクラウド機能について話題となりました。IMEは日本語などのマルチバイト文字を扱う環境において必要な機能です。最近では、このIMEに常時インターネット接続を必要とする、クラウド関連の機能が実装されることが多くなってきています。これらのクラウド機能では、ユーザの入力内容に基づいて、変換候補を提示したり、ユーザ辞書を複数の端末で共有するなどの機能を提供しています。このうち、一部の日本語IMEで設定の状態に関わらず、ユーザの入力内容の一部を送信していた事例が見つかりました。この事例では不具合によって送信されていましたが、問題となった複数のIMEは、パソコンや携帯端末にプリインストールされていたり、他のソフトウェアにバンドルされてインストールされる場合もあり、状況によってはユーザが意図せずに利用している可能性がありました。このため、不具合が修正されると共に初期設定でクラウド機能を使わないような修正が行われています。

これらの機能は非常に便利なものですが、一方でその入力内容や登録内容が外部に送信されていることにもなり、状況によっては情報漏えい事件などに繋がる可能性があります。このため、特に企業など組織での利用については注意する必要があります[*20]。

### ■ Bitcoin

仮想通貨であるBitcoin[*21]についても、その取引が拡がるにつれて、様々な事件が発生しています。この期間では、Bitcoinによる取引を行っていたアンダーグランドサイトであるSilk Roadに対し、FBIによるテイクダウンが行われ、サイト所有者が麻薬取締法違反容疑で逮捕されています。Silk Roadでは違法薬物だけでなく、他にも違法な取り引きの場となっていたとされており、テイクダウンの際には約3万XBT(Bitcoinの取引単位)が押収されています。また、仮想通貨交換所や口座管理サービスに対する攻撃も相次いでおり、これらのサイトへのDDoS攻撃や、不正侵入によりBitcoinそのものが盗まれたり、サイトのアカウント情報

*19 内閣官房情報セキュリティセンターで開催された情報セキュリティ対策推進会議(CISO等連絡会議)などで 詳細が確認できる。「第11回会合(平成25年7月11日)」(http://www.nisc.go.jp/conference/suishin/index.html#2013_3)。
*20 IIJでもIIJ-SECT Security DiaryでIMEのクラウド関連機能について注意喚起を行っている。「IMEのオンライン機能利用における注意について」(https://sect.iij.ad.jp/d/2013/12/104971.html)。
*21 Bitcoinについては、本レポートのVol.21 (http://www.iij.ad.jp/development/iir/pdf/iir_vol21.pdf)の「1.4.3 仮想通貨Bitcoin」で紹介している。

## 12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 **4日**：Ruby on Railsにクロスサイトスクリプティングを含む複数の脆弱性が見つかり、修正された。
"Rails 3.2.16 and 4.0.2 have been released!"（http://weblog.rubyonrails.org/2013/12/3/Rails_3_2_16_and_4_0_2_have_been_released/）。

セ **6日**：Microsoft社のデジタルクライムユニット（DCU）は、FBIやEuropolなど複数の捜査機関や企業と共同でZeroAccessボットネットのテイクダウンを実施したことを公表した。
詳細については次のMicrosoft社の発表を参照のこと。"Microsoft, the FBI, Europol and industry partners disrupt the notorious ZeroAccess botnet"（http://www.microsoft.com/en-us/news/press/2013/dec13/12-05zeroaccessbotnetpr.aspx）。

他 **6日**：Microsoft社は政府によるインターネットの監視活動への対応として、同社製品やサービスにおける暗号の強化等の発表を行った。
詳細については次のMicrosoft社の公式Blog"Protecting customer data from government snooping"（http://blogs.technet.com/b/microsoft_blog/archive/2013/12/04/protecting-customer-data-from-government-snooping.aspx）

セ **8日**：フランスの政府系認証局であるANSSI傘下の中間認証局で複数のGoogleドメインの証明書が不正に発行されたことが判明し、複数のブラウザで当該証明書を無効にする対応が行われた。原因については人為的なミスであったとしている。
詳細については次のANSSIの発表を参照のこと。"Revocation of an IGC/A branch"（http://www.ssi.gouv.fr/en/the-anssi/events/revocation-of-an-igc-a-branch-808.html）。

他 **9日**：内閣官房情報セキュリティセンターの主催で、重要インフラにおける分野横断的演習「CIIREX2013（シーレックス2013）」が実施された。
「重要インフラにおける分野横断的演習の実施概要について【CIIREX 2013(シーレックス2013)】」（http://www.nisc.go.jp/active/infra/pdf/ciirex2013_2.pdf）。

他 **10日**：Google社やMicrosoft社など、米国の大手IT企業の7社は共同で各国政府による情報収集活動に対する法律による制限や通信の制限に対する規制を撤廃することなどを求めていく活動を開始した。
次のサイトでは活動方針や米国大統領と連邦政府議会に宛てた請願書などを公開している。Reform Government Surveillance（http://reformgovernmentsurveillance.com/）。

脆 **11日**：Microsoft社は、2013年12月のセキュリティ情報を公開し、MS13-096やMS13-097、MS13-099を含む5件の緊急と6件の重要な更新をリリースした。
「2013年12月のセキュリティ情報」（http://technet.microsoft.com/ja-jp/security/bulletin/ms13-dec）。

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。
「APSB13-28: Adobe Flash Player用のセキュリティアップデート公開」（http://helpx.adobe.com/jp/security/products/flash-player/apsb13-28.html）。

脆 **12日**：PHPに、OpenSSLモジュールに不正な証明書を処理した際にメモリー破損が発生することで、コード実行やシステムの停止が可能な脆弱性（CVE-2013-6420）などが見つかり、修正された。
JVN、「JVNDB-2013-005585 PHP の ext/openssl/openssl.c 内の asn1_time_to_time_t 関数における任意のコードを実行される脆弱性」（http://jvndb.jvn.jp/ja/contents/2013/JVNDB-2013-005585.html）。

他 **12日**：情報セキュリティ対策推進会議（CISO等連絡会議）の第14回会合が行われ、各政府機関におけるWindowsXP、複合機などの使用・対策状況についての調査結果が報告された。
内閣官房情報セキュリティセンター 情報セキュリティ対策推進会議（ＣＩＳＯ等連絡会議）、「第１４回会合（平成２５年１２月１２日）」（http://www.nisc.go.jp/conference/suishin/index.html#2013_6）。

脆 **17日**：Google社のAndroid OSに任意のJavaのメソッドからAndroid OSの機能を実行したり、任意のコードが実行できる脆弱性が見つかり修正された。
JVN、「JVN#53768697 Android OS において任意の Java のメソッドが実行される脆弱性」（https://jvn.jp/jp/JVN53768697/index.html）。

他 **17日**：2011年9月に発覚した、防衛関連企業に対する標的型攻撃によるマルウェア感染事件について、偽計業務妨害容疑で捜査が行われていたが容疑者不詳のまま時効となった。

他 **19日**：米国大統領の諮問委員会は国家安全保障局（NSA）の情報収集活動に対する報告とその活動には制限が必要とする勧告をまとめ公開した。
White House,"Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies"（http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf）。

他 **20日**：国連総会で、個人のプライバシーについてデジタル通信も含めた保護を各国に求める"The right to privacy in the digital age"が全会一致で採択された。
United Nations、"General Assembly backs right to privacy in digital age"（http://www.un.org/apps/news/story.asp?NewsID=46780&Cr=privacy&Cr1=）。

他 **20日**：高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）第63回会合において、個人情報を含むいわゆるパーソナルデータの利活用に向けた、個人情報保護制度の見直し方針を決定した。
内閣、「高度情報通信ネットワーク社会推進戦略本部（第６３回）　議事次第」（http://www.kantei.go.jp/jp/singi/it2/dai63/gijisidai.html）。

動 **26日**：日本の内閣総理大臣が靖国神社に参拝した。

他 **26日**：日本語IMEのオンライン機能について、利用者の意図しない情報が送信されている事例があることが報道された。

セ **27日**：クリスマスシーズンの期間に大規模なNTPによるリフレクション攻撃が観測されたことが報告された。
詳細については次のSymantec社のBlogなどを参照のこと。"Hackers Spend Christmas Break Launching Large Scale NTP-Reflection Attacks"（http://www.symantec.com/connect/blogs/hackers-spend-christmas-break-launching-large-scale-ntp-reflection-attacks）。

セ **31日**：オンラインゲームのLeague of Legendsなど複数のゲームのゲームサーバに対し、何者かによるDDoS攻撃が発生した。
例えば、League of Legendsで発生した攻撃については、次のREDDIT掲示板などにまとめられている。"Servers down? Discuss here."（http://www.reddit.com/r/leagueoflegends/comments/1u1pcz/servers_down_discuss_here/）。

［ 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

が盗まれる事件が多く発生しています。また、フリーソフトにBitcoinのマイニングを行う機能が見つかったり、マイニングを行うマルウェアが流行するなどしています*22。Bitcoinによる取引は拡大しており、その影響が無視できないほどの規模となっています。中国では中国人民銀行が取引について警告を実施しました*23。これを受け、BTC Chinaでは一時通貨による取引を停止しています*24。インドでも同様に金融当局による警告が行われ*25、インドのいくつかの取引所が停止しました。

### ■ その他

2011年9月に発覚した、防衛関連企業に対する標的型攻撃によるマルウェア感染事件について、偽計業務妨害容疑で捜査が行われていましたが、送信元の特定には至らず容疑者不詳のまま12月に時効となりました。標的型攻撃では、自らの活動の記録などの痕跡を消すなどして発見をされないように活動することから、攻撃を受けた場合には、その攻撃に気がつかないだけでなく、発覚後の調査でも被害の状況や行為者を特定することが困難な場合が多くあります。このため、境界での通信の制御や情報システムの設計や運用による内部対策、記録の適切な保存などの対策が重要となります*26。

米国立標準技術研究所(NIST)が策定した暗号アルゴリズム(Dual_EC_DRBG)の一部に、米国家安全保障局(NSA)によるバックドアが含まれるため、解読される可能性があるとの報道があり、NISTでは該当の暗号を利用しないように勧告を行っていました*27。12月に、この暗号アルゴリズムを採用する米国EMC社のRSA製品について、この暗号を優先的に取扱うことで報酬を受け取っていたとの報道が行われましたが、EMC社は否定しています*28。

12月にはシマンテック社がブログで大規模なNTPによるDDoS攻撃を報告しています。この攻撃ではNTPのmonlist機能が悪用されており、2014年1月になってDDoS攻撃などに悪用される可能性があるとして脆弱性への注意喚起が行われています*29。2013年12月末から本稿執筆時点にかけても、何者かによるゲーム関連サイトなどに対する、この機能を悪用したと考えられるDDoS攻撃が複数発生し、その攻撃規模が100Gbpsを超えたと報道されています。これらを受けて対象ネットワーク上に応答を返すNTPサーバが存在しないかどうかをチェックできるOpenNTPProject.org*30が開始されるなど対策に向けた活動が進められています。

＊22 例えば、次のトレンドマイクロ社のSecurity Blogを参照のこと。「日本でも約3,000台の感染が確認された脅威『ビットコイン発掘不正プログラム』とは」(http://blog.trendmicro.co.jp/archives/8271)。
＊23 中国人民銀行、"比特币相关事宜答记者问"(http://www.pbc.gov.cn/publish/goutongjiaoliu/524/2013/20131205153950799182785/20131205153950799182785_.html)。
＊24 BTC China"An Open Letter from Bobby Lee, CEO of BTC China"(https://vip.btcchina.com/page/notice20131220)。
＊25 The Reserve Bank of India、"RBI cautions users of Virtual Currencies against Risks"(http://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=30247)。
＊26 標的型攻撃対策については、独立行政法人情報処理推進機構(IPA)の「『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)も参照のこと。
＊27 2013年9月にNIST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)。
＊28 米EMC社の公式発表については次の公式Blogに詳しい、"RSA RESPONSE TO MEDIA CLAIMS REGARDING NSA RELATIONSHIP" (http://blogs.rsa.com/news-media-2/rsa-response/)。
＊29 JVN、「JVNVU#96176042 NTPがDDoS攻撃の踏み台として使用される問題」(http://jvn.jp/vu/JVNVU96176042/)。
＊30 OpenNTPProject.org - NTP Scanning Project(http://openntpproject.org/)。

## 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10月から12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-2では、DDoS攻撃全体を、回線容量に対する攻撃[*31]、サーバに対する攻撃[*32]、複合攻撃(1つの攻撃対象に対し、同時に数種類の攻撃を行うもの)の3種類に分類しています。

この3ヵ月間でIIJは、498件のDDoS攻撃に対処しました。1日あたりの対処件数は5.4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41.6%、複合攻撃が51.8%、回線容量に対する攻撃が6.6%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105万5千ppsのパケットによって2.94Gbps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89.2%が攻撃開始から30分未満で終了し、10.6%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、今回もっとも長く継続した攻撃は、複合攻撃に分類されるもので3日と8時間51分(80時間51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、国外を問わず非常に多くのIPアドレスが観測されました。これは、IPスプーフィング[*33]の利用や、DDoS攻撃を行うための手法としてのボットネット[*34]の利用によるものと考えられます。

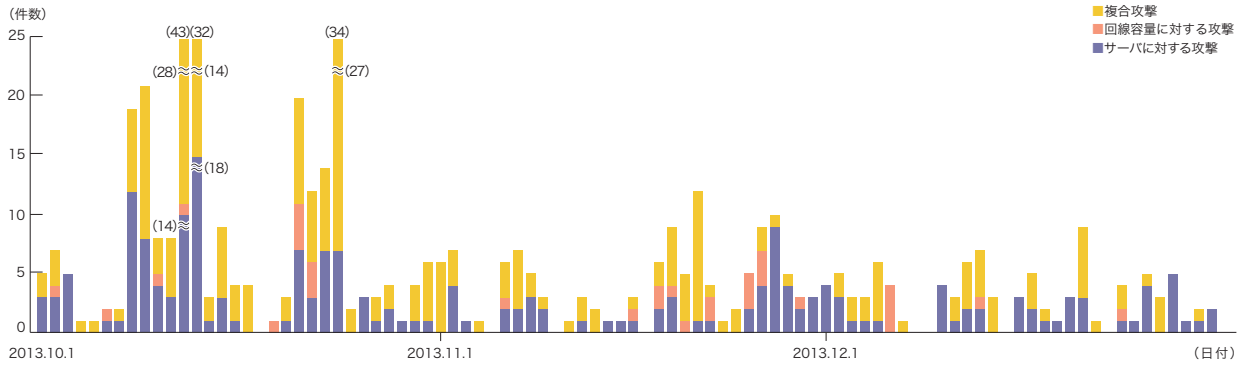



**図-2 DDoS攻撃の発生件数**

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

*32 TCP SYN floodやTCP connection flood、HTTP GET flood攻撃等。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等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。

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

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

### ■ backscatterによる観測

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

2013年10月から12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45.8%を占めています。またストリーミング通信で利用される1935/TCPや、SSHで利用されている22/TCPなどへの攻撃、通常は利用されない8000/tcpや8877/TCPなどの攻撃が観測されています。

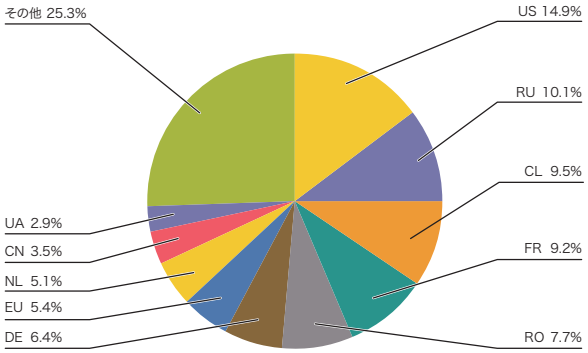



**図-3 DDoS攻撃のbackscatter観測による攻撃先の国別分類**

図-3で、DDoS攻撃の対象となったIPアドレスと考えられるbackscatterの発信元の国別分類を見ると、今回の期間では米国が14.9%が最も大きな割合を占めていました。その後にロシアの10.1%、チリの9.5%といった国が続いています。今回チリからの攻撃を多く観測していますが、これは特定のハニーポットに対して複数のIPアドレスからの445/TCPの攻撃をこの期間中合計で8万5千回以上観測したためとなります。

特に多くのbackscatterを観測した場合について、攻撃先のポート別にみると、まず、Webサーバ(80/TCP)への攻撃としては、10月17日にアゼルバイジャンのニュース事業者のWebサーバからのbackscatterを観測しています。この事業者への攻撃は10月23日にも同様に観測されています。10月26日には、ウクライナのISPとルーマニア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。

今回の期間ではチリからの攻撃を多く観測していますが、これは特定のハニーポットで445/TCPに対する攻撃を観測したためで、複数のIPアドレスからの攻撃が12月11日や12月14日、12月24日に多く観測されています。この通信は期間中、合計で8万5千回以上観測しています。10月2日にはイランのサーバに対するポートスキャンによると考えられる通信を、同じく11月9日にはアルゼンチンのサー

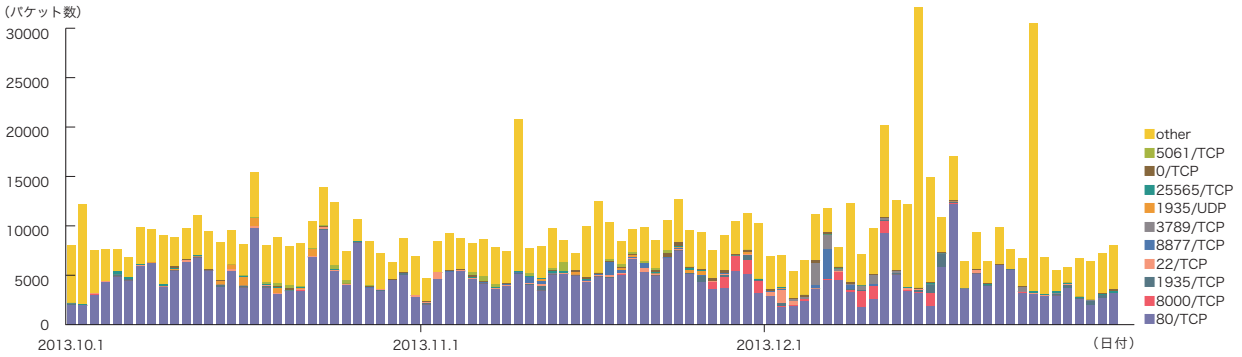



**図-4 DDoS攻撃によるbackscatter観測(観測パケット数、ポート別推移)**

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

*36 この観測手法については、本レポートのVol.8(http://www.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。

バに対する攻撃を観測しています。11月9日や12月9日など複数の日時にドイツのホスティング事業者のサーバに対する8000/TCPへの攻撃を、11月17日と12月6日にはロシアのホスティング事業者のサーバに対する8877/TCPへの攻撃をそれぞれ観測しています。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、10月から複数発生したGitHubに対する攻撃、同じく10月に発生したAnonymousによると考えられるInterpol IndonesiaのWebサーバに対する攻撃、11月に発生したAnonymousによると考えられるロシアの政府機関への攻撃、12月に発生した英国の金融機関への攻撃を観測しています。

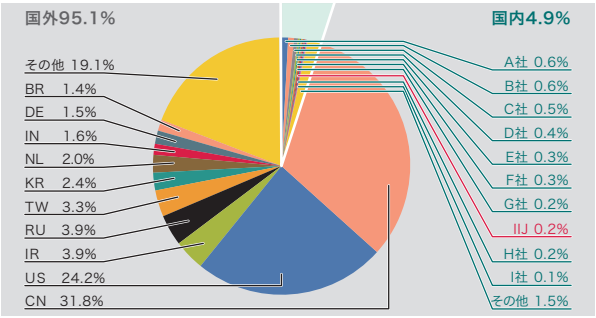



**図-5 発信元の分布(国別分類、全期間)**

### 1.3.2 マルウェアの活動

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

#### ■ 無作為通信の状況

2013年10月から12月の期間中に、ハニーポットに到着した通信の発信元IPアドレスの国別分類を図-5に、その総量(到着パケット数)の推移を図-6に、それぞれ示します。MITFでは、数多くのハニーポットを用いて観測を行っていますが、ここでは1台あたりの平均を取り、到着したパケットの種類(上位10種類)ごとに推移を示しています。また、この観測では、MSRPCへの攻撃のような特定のポートに複数回の接続を伴う攻撃は、複数のTCP接続を1回の攻撃と数えるように補正しています。

ハニーポットに到着した通信の多くは、Microsoft社のOSで利用されているTCPポートに対する探索行為でした。また、同社のSQL Serverで利用される1433/TCPやWindowsのリモートログイン機能である、RDPで利用される3389/TCP、SSHで利用される22/TCP、HTTPで利用される80/TCP、ICMP Echo Request、DNSで利用される53/UDPによる探査行為も観測されています。

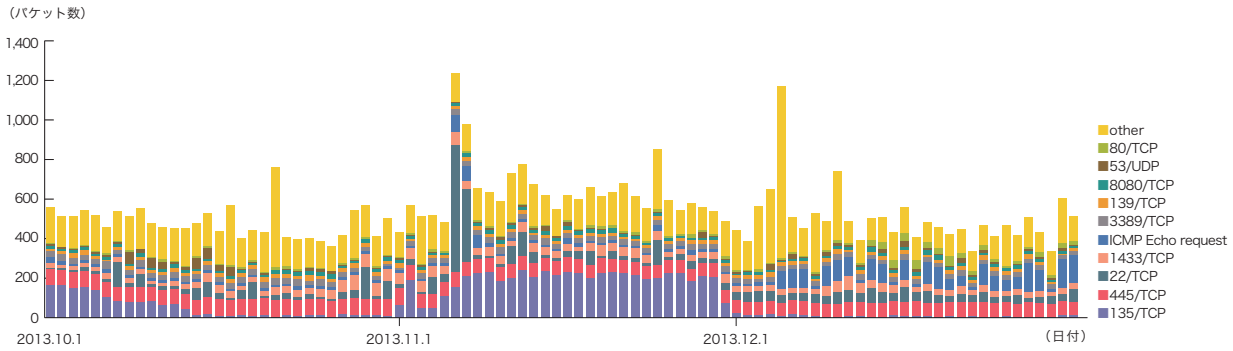



**図-6 ハニーポットに到着した通信の推移(日別・宛先ポート別・1台あたり)**

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

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

期間中、SSHの辞書攻撃の通信も散発的に発生しており、例えば11月6日から11月7日にかけて発生している通信は、中国に割り当てられたIPアドレスからのものです。また9月中旬以降に発生していたDNS Open Resolverの探査行為と思われる通信は継続しており、10月、12月に発生しています[*39]。今回の期間においては、中国と共にオランダ、米国に割り当てられたIPアドレスからも同種の探査の通信を大量に観測しています。1433/TCPについては、通常の倍程度の通信が到着していますが、その多くは中国に割り当てられたIPアドレスからのものでした。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、攻撃対象もしくは攻撃の踏み台として悪用することのできる対象を探す試みが、継続していることがうかがえます。また、米国に割り当てられたIPアドレスから135/TCP宛てのRPCサーバの探査行為の通信も継続しており、10月上旬から中旬にかけてと11月に大規模に観測されています。

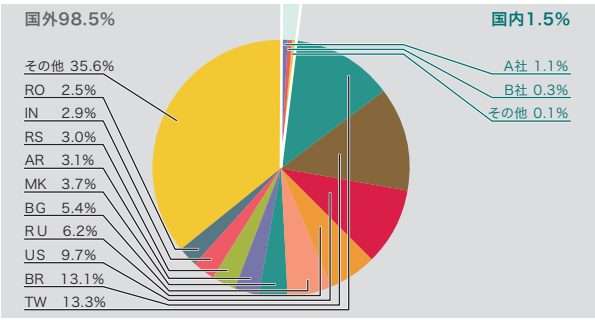



**図-7 検体取得元の分布(国別分類、全期間、Conficker除く)**

### ■ ネットワーク上でのマルウェアの活動

同じ期間中でのマルウェアの検体取得元の分布を図-7に、マルウェアの総取得検体数の推移を図-8に、そのうちのユニーク検体数の推移を図-9にそれぞれ示します。このうち図-8と図-9では、1日あたりに取得した検体[*40]の総数を総

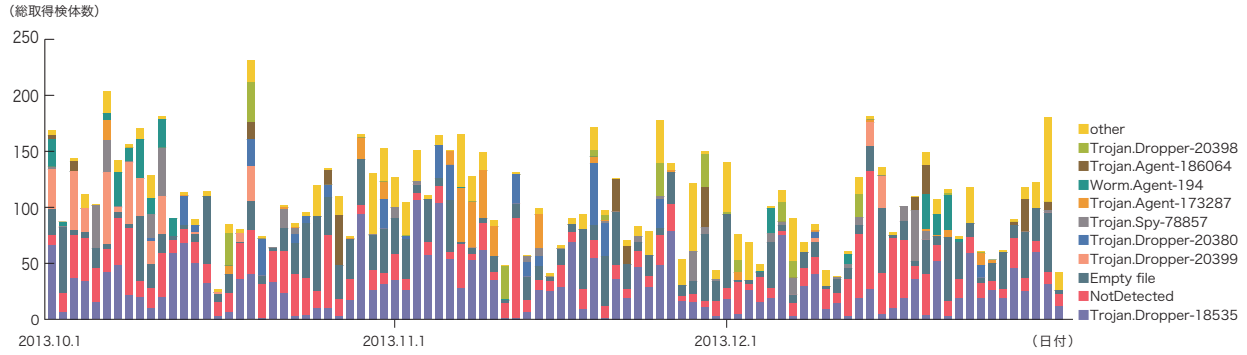



**図-8 総取得検体数の推移(Conficker除く)**

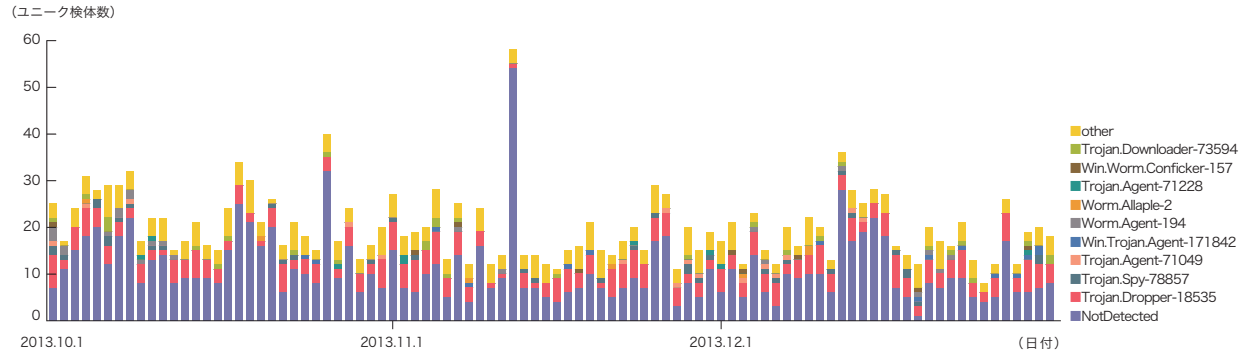



**図-9 ユニーク検体数の推移(Conficker除く)**

*39 例えば、10月8日に観測された通信は、CNotesの「DNS amp - source address 2」(http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=DNS+amp+-+source+address+2)で報告されている内容と同じ送信元からのスキャンであったことを確認している。

*40 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。

取得検体数、検体の種類をハッシュ値[*41]で分類したものをユニーク検体数としています。

また、検体をウイルス対策ソフトで判別し、上位10種類の内訳をマルウェア名称別に色分けして示しています。なお、図-8と図-9は前回同様に複数のウイルス対策ソフトウェアの検出名によりConficker判定を行い、Confickerと認められたデータを除いて集計しています。

期間中での1日あたりの平均値は、総取得検体数が108、ユニーク検体数が20でした。未検出の検体をより詳しく調査した結果、米国など、複数の国に割り当てられたIPアドレスからワーム[*42]が観測されたほか、フィリピンに割り当てられたIPアドレスからIRCサーバで制御されるタイプのボット[*43]も継続的に観測されました。また今回の期間では未検出の検体の約3分の2がテキスト形式でした(前回は約3割)。これらのテキスト形式の多くは、HTMLであり、Webサーバからの404や403によるエラー応答であるため、古いワームなどのマルウェアが感染活動を続けているものの、新たに感染させたPCがマルウェアをダウンロードしに行くダウンロード先のサイトがすでに閉鎖させられていると考えられます。

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89.2%、ボット型4.4%、ダウンローダ型6.4%でした。また解析により、16個のボットネットC&Cサーバ[*44]と6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36,340、ユニーク検体数は756でした。短期間での増減を繰り返しながらも、総取得検体数で99.7%、ユニーク検体数で97.3%を占めています。このように、今回の対象期間でも支配的な状況が変わらないことから、Confickerを含む図は省略しています。

本レポート期間中の総取得検体数は前号の対象期間中と比較し、約6%増加しています。また、ユニーク検体数は前号から約4%減少しました。Conficker Working Groupの観測記録[*45]によると、2013年12月31日現在で、ユニークIPアドレスの総数は1,267,162とされています。2011年11月の約320万台と比較すると、約40%に減少したことになりますが、依然として大規模に感染し続けていることが分かります。

*41 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。
*42 WORM_ATAK(http://about-threats.trendmicro.com/archiveMalware.aspx?language=jp&name=WORM_ATAK.D)。
*43 BKDR_QAKBOT(http://about-threats.trendmicro.com/malware.aspx?language=en&name=BKDR_QAKBOT)。
*44 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。
*45 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[*46]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10月から12月までに検知した、Webサーバに対するSQLインジェクション攻撃の発信元の分布を図-10に、攻撃の推移を図-11にそれぞれ示します。これらは、IIJマネージドIPSサービスのシグネチャによる攻撃の検出結果をまとめたものです。

発信元の分布では、日本46.4%、米国20.8%、中国9.9%となり、以下その他の国々が続いています。Webサーバに対するSQLインジェクション攻撃の発生件数は前回からあまり変化していません。

この期間中、11月7日に韓国の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。10月1日には香港や米国など複数の国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。10月9日には米国やドイツなど複数の国の攻撃元から特定の攻撃先への攻撃が発生していました。11月21日には国内の特定の攻撃元より特定の攻撃先への攻撃、米国の特定の攻撃元から特定の攻撃先への攻撃が発生しています。12月21日には国内の複数の攻撃元より、特定の攻撃先への攻撃が発生していました。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。

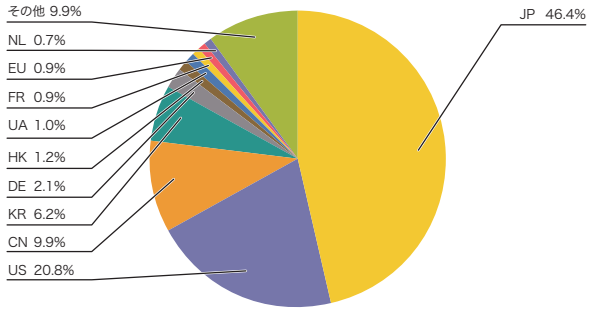



**図-10 SQLインジェクション攻撃の発信元の分布**

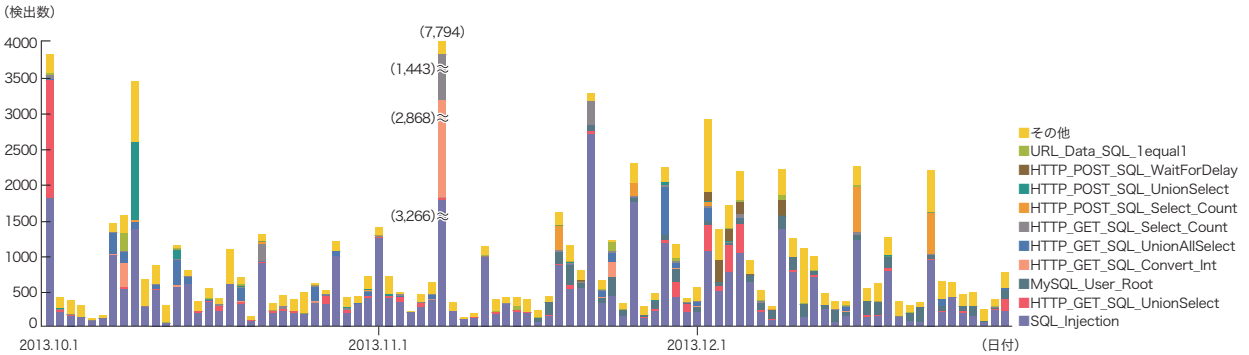



**図-11 SQLインジェクション攻撃の推移(日別、攻撃種類別)**

*46 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、大容量メモリを搭載した端末のメモリフォレンジックにおける注意点、Forward Secrecy、WebクローラによるWebサイト改ざん調査の3つのテーマについて紹介します。

### 1.4.1 大容量メモリを搭載した端末のメモリフォレンジックにおける注意点

PCの高性能化が進むにつれて、ハードディスクやメモリの容量も増えてきています。デジタルフォレンジックにおいては、大容量化したメディアの解析をいかに効率よく行うかが1つの課題として知られていますが、大容量になることによって、揮発性のデータであるメモリのフォレンジック解析が不可能になる事象があることはあまり知られていません。本節ではその原因や、利用するメモリフォレンジックツールの注意点に関して述べたいと思います。なお、本稿で述べるメモリフォレンジックはWindows OSのみを対象にしています。

#### ■ 事象の原因

問題となる事象を説明する前に、メモリフォレンジック*47について簡単に説明します。メモリフォレンジックはディスクフォレンジックと同様に、最初にメモリ全体のバイナリデータを保存する「取得(もしくは保全)」と呼ばれる作業を行った後、取得したデータから情報を独自に抽出する「解析」の2つのフェーズから成り立っています。取得したメモリのバイナリデータはメモリイメージと呼ばれます。メモリイメージには、raw(メモリのデータをそのまま抽出したもの)、crashdump(メモリのデータからハードウェアに予約された領域を除去し、先頭にヘッダを付加したもの)、hibernation(休止状態からの復旧用で圧縮されたもの)の3種類の形式がありますが、現状、取得ツールは、rawもしくはcrashdump形式で保存するものしかありません。また、ほとんどの解析ツールはrawしか解析できず、crashdumpやhibernationを解析できるツールはごく僅かです。よって、端末のハードディスクに残っているhibernationを解析するようなケースを除いて、メモリフォレンジックとはraw(必要に応じてcrashdump)形式のメモリを取得・解析する技術であるといえます。

メモリフォレンジックの解析の過程でキーとなるデータはいくつかありますが、とりわけ以下の2つはどのような情報を抽出するにしても必要になります。

1. 仮想アドレスから物理アドレスへ変換するための、カーネルやプロセスごとの変換テーブルの物理オフセット*48
2. OSのバージョンやプロセスリストへのポインタなどを含むデバッグ構造体*49

これらのデータを解析ツールが抽出するプロセスは、メモリイメージの形式によって異なります。rawの場合、それらを抽出するために各データのシグネチャを使ってメモリイメージ内を全検索します。一方、crashdumpは先頭のヘッダにそれらの情報を含んでいるため、データを検索する必要がありません。問題の事象は先に述べた2のデバッグ構造体を、raw形式のメモリの中から検索する際に起こります。x64アーキテクチャのWindowsがインストールされており、かつ大容量のメモリが搭載された端末*50において、そこから取得したメモリイメージ内にあるデバッグ構造体が、一定のアルゴリズムでエンコードされることがあります。その結果、解析ツールがデバッグ構造体を見つけられず、解析が異常終了します。

**表-1 メモリイメージ取得ツールの検証結果**

| | FTK Imager | Belkasoft Live RAM Capturer | Windows Memory Reader | winpmem | DumpIt |
|---|---|---|---|---|---|
| raw | デコードしない | デコードしない | デコードしない | デコードしない | デコードしない |
| crashdump | - | - | デコードしない | デコードしない | デコードする |

*47 IIJ-SECT Security Diaryでは、SpyEyeを例としてマルウェアに感染した端末のメモリを調査する手法を解説している。「メモリフォレンジックによるマルウェア感染痕跡の調査」(https://sect.iij.ad.jp/d/2011/12/194028.html)。
*48 DirectoryTableBaseとして定義されている。
*49 _KDDEBUGGER_DATA64として定義されている。
*50 IIJでは16GBのメモリを搭載したx64アーキテクチャのWindows7端末で事象を確認している。後で述べる、デバッグ構造体をデコードする独自のロジックを組み込んだ取得ツール(DumpIt)の作者であるMatthieu Suicheによると、OSはVista以降であれば起こりうる事象であるとのこと。

### ■ 取得ツールの検証

取得ツールの中には、取得時にエンコードされているデバッグ構造体をデコードするものが存在します。IIJではFTK Imager[*51]、Belkasoft Live RAM Capturer[*52]、Windows Memory Reader[*53]、winpmem[*54]、Dumplt[*55]の5つの取得ツールを検証し、デバッグ構造体をデコードするか否かの確認を行いました。その検証結果を表-1に示します。

結果から、Dumpltが生成するcrashdump形式のみ、デコードされたデバッグ構造体のデータを含んでいることが分かりました[*56]。エンコードされたデバッグ構造体のデータとデコードされたそれを比較した図を図-12に示します。上がFTK Imagerで取得したエンコードされたデータで、下がDumpltで取得したデコードされたデータです。デコードされたデータの方では、デバッグ構造体のヘッダ[*57]にあるシグネチャとなる"KDBG"という文字列や、デバッグ構造体のサイズ情報を確認できます。

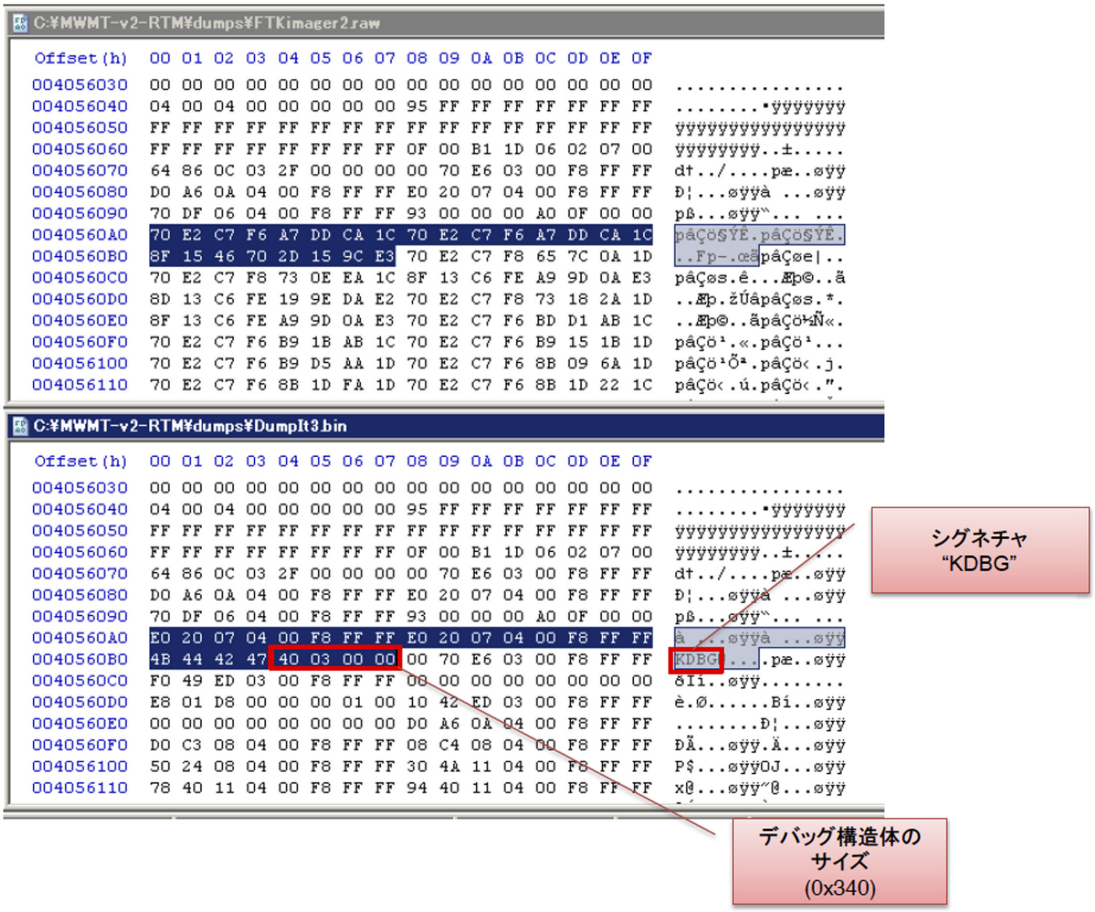



**図-12** デバッグ構造体のデータ比較

*51 バージョン3.1.4.6を利用(http://www.accessdata.com/support/product-downloads)。
*52 (http://forensic.belkasoft.com/en/ram-capturer)。
*53 バージョン1.0を利用(http://cybermarshal.com/index.php/cyber-marshal-utilities/windows-memory-reader)。
*54 バージョン1.4.1を利用(http://sourceforge.net/projects/volatility.mirror/files/?source=navbar)。
*55 バージョン2.0を利用(http://www.moonsols.com/windows-memory-toolkit/)。
*56 IIJによる検証では、列挙したツールの中でDumpltのcrashdump形式のみが、デコードされたデバッグ構造体を含んでいたが、同じOS環境・ツールで取得した場合でも異なる結果になる可能性がある。例えば以下の記事では、FTK ImagerやBelkasoft RAMCaptureによって取得されたメモリイメージを解析できたことが報告されている(ただし、作者は明示的にデバッグ構造体がエンコードされていることを確認しているわけではないようなので、これらのツールが明示的にデコードしたのではなく、この端末ではそもそもエンコードされていなかった可能性も考えられる)。このように、デバッグ構造体がエンコードされる条件は、Windows7以前のOSでは明確になっていない。BriMor Labs、"All memory dumping tools are not the same"(http://brimorlabs.blogspot.jp/2014/01/all-memory-dumping-tools-are-not-same.html)。
*57 _DBGKD_DEBUG_DATA_HEADER64として定義されている、_KDDEBUGGER_DATA64の先頭にあるヘッダ。

使用する解析ツールがraw形式しか対応していない場合は、DumpItで取得したcrashdumpをrawに変換することで対応できます。ところで、Windows Memory Readerとwinpmemでは、crashdumpを生成することができます。crashdumpの場合、ファイルの先頭ヘッダに解析に必要な情報が入っていることは前述しました。ということは、crashdumpを変換せずに直接解析できるツールであれば、デバッグ構造体がエンコードされていても関係なく結果を返せるはずです。ところが、解析ツールによってはraw形式と同様に解析が異常終了してしまうものがあります。具体的には、Volatility Framework[*58]は、crashdumpの場合でもデバッグ構造体を検索してしまう実装のため、解析が失敗します[*59]。CrashDumpAnalyzer[*60]はcrashdumpのヘッダ情報のみを用いて解析を行うので、Windows Memory Readerとwinpmemによって生成された(デバッグ構造体がエンコードされている)crashdumpも解析することができます。

### ■ まとめ

ここまで説明してきたように、メモリフォレンジックの取得・解析ツールは、一見同じ形式を取得・解析しているように見えて、その実装は大きく異なります。アナリストは、それらツールの特性を十分に理解した上で利用しないと、今回の事象のようにメモリフォレンジックから揮発性の情報を全く抽出できない状況に陥る可能性があります。日頃からツールを検証し、広く情報を収集し、問題が起きた場合にそれを見過ごすのではなく、真摯にその原因を追究していく姿勢が大切です。

## 1.4.2 Forward Secrecy

本稿ではNSAに関する一連の報道に伴い、注目されているForward Secrecyについて取り上げます。昨年末SNSなどの主要サイトにおいて、SSL/TLSサーバのForward Secrecy対応が進められました。以下、Forward Secrecyが必要であると認識された背景、技術的解説、適用する際の注意点について紹介します。

### ■ Forward Secrecyが必要であると認識された背景

最近(Perfect)Forward Secrecy[*61]が注目を集めていますが、少なくともEUROCRYPT'89で発表された論文[*62]には登場していた概念です。暗号学的な定義はここでは解説しませんが、Diffie-Hellman[*63]などの鍵交換プロトコルを利用する手順において、そのセッションでしか利用しない一時的な鍵ペアを生成します。もし仮に、この一時的な公開鍵に対応する秘密鍵が漏えいしても、暗号通信が解読される範囲を一部に限定することができます。

一方で、毎回同じ公開鍵を用いて暗号化されているケースでは、一旦暗号化されたデータが広域ネットワークを通して伝播されている場合、暗号通信が何十年という単位で長期間に渡って記録され続けていて、将来のいつか秘密鍵が漏えいすることにより、過去に遡って復号できてしまいます。Forward Secrecyはこの問題を防ぐ技術として注目されています。

Forward Secrecyが注目されるきっかけとなったのは米国家安全保障局(NSA)による通信傍受に関する一連の報道

---

*58 オープンソースのPythonで書かれたメモリ解析ツール。raw/crashdump/hibernation全てに対応している。Volatilityはプロセス構造体をリストする際、どの形式でも必ずデバッグ構造体を検索するジェネレータを使う仕様になっているため、それがエンコードされていると解析が失敗する。(https://code.google.com/p/volatility/)。

*59 以下の記事によると、Volatility Frameworkでは、解析中にデバッグ構造体をデコードするコードを試験的に実装しており、トレーニング参加者には配布される予定とのこと。デバッグ構造体がエンコードされてしまう事象は、Windows8やServer 2012などの新しいOSにおいては、メモリのサイズにかかわらず起こりうると述べている。Volatility Labs、"The Secret to 64-bit Windows 8 and 2012 Raw Memory Dump Forensics" (http://volatility-labs.blogspot.jp/2014/01/the-secret-to-64-bit-windows-8-and-2012.html)。

*60 EnCaseの拡張スクリプト言語であるEnScriptで書かれたcrashdump解析ツール。Volatilityに比べると抽出できる情報は限定的。(http://takahiroharuyama.github.io/blog/2014/01/05/some-old-stuffs/)。

*61 Perfect Forward SecrecyとForward Secrecyの二つの言い方が存在しているが、両者とも同じ意味・文脈で利用されているため、本稿ではForward Secrecyに統一している。

*62 Christoph G. Günther, "An Identity-Based Key-Exchange Protocol", EUROCRYPT1989, LNCS vol.434, pp.29-37, 1989.

*63 一般的なDiffie-Hellman鍵共有方式は以下のとおりである。十分大きな素数pに対して有限体GF(p)の生成元gを定め、p及びgを公開パラメータとする(秘密にしておく必要はない)。ユーザAとユーザBはそれぞれ秘密鍵x,yを1からp-1の整数からランダムに選択し、$X=g^x \bmod p$と$Y=g^y \bmod p$をユーザA及びBの公開鍵としてお互いに開示する。ユーザAはユーザBの公開鍵Yを用いて$Y^x = (g^y)^x \bmod p$を計算できる。一方でユーザBはユーザAの公開鍵Xを用いて$X^y = (g^x)^y \bmod p$を計算できることから$g^{xy} \bmod p$をユーザAとBだけで秘密裏に共有することができる。g, $g^x$, pからxを求める離散対数問題は十分大きな素数pにおいて困難とされている。

です。昨年9月、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ました。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を発表し、擬似乱数生成アルゴリズムDual_EC_DRBGについて、利用しないことを推奨する勧告がなされています*64。また国内においても、CRYPTRECから本件が周知されました*65。これを受けて米EMC社は、デフォルトでDual_EC_DRBGが使用される設定になっていた暗号ライブラリRSA BSAFEの顧客に対して、本アルゴリズムを使用しないように伝えています*66。その後もEMC社とNSAに関する報道がなされました。Dual_EC_DRBGは、擬似乱数出力の32バイトを入手すれば、それ以後生成される乱数列を特定可能という脆弱性が2007年の時点で発表されていました*67。このような問題が発覚していたにも関わらず、暗号アルゴリズムの利用現場では使い続けられていたことになります。

攻撃者が擬似乱数生成モジュールを管理下に置くことで、通信時に用いられるあらゆる擬似乱数やそこから生成された暗号化用鍵に関する情報などを、リアルタイムに窃取する問題が考えられます。実際、擬似乱数生成モジュールのエントロピーが小さいことに起因する問題は、例えばDebianのOpenSSLにおける脆弱性などが知られています*68。この脆弱性は、Debianの特定バージョンにおけるOpenSSLを使って鍵生成を行った場合、極端に少ない鍵空間からしか秘密鍵を導出していないという問題です。この問題については2008年に指摘があったにも関わらず、現在でもその脆弱な鍵を利用しているサイトが存在しています。またAndroid上の一部のbitcoinアプリケーションにおいても、乱数生成時の問題が報告されています*69。bitcoinで用いられているECDSA署名では、署名演算を行うたびに、毎回ランダムな乱数パラメータを生成する必要があります。このとき異なる署名生成時に同じパラメータを使用した場合、秘密鍵が漏えいしてしまいます。これも擬似乱数のエントロピーの低さに起因する問題です。

暗号アルゴリズムにバックドアを仕掛ける方法以外にも、NSAによる通信傍受の仕組みが明らかになってきました。NSAが米Verizonに対し電話の通話記録の収集を求めていたこと、PRISMと呼ばれるインターネット上の動画・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もと運用されていたことが昨年6月に報道されました。更に10月には、NSAによるリアルタイム通信傍受プロジェクトの存在が暴露され、Yahoo!とGoogleのデータセンター間の通信を盗聴していたことが公開されています。また、E-mailプロバイダであるLavabitは、FBIから秘密鍵供託を指示されたことから、利用者のプライバシーを保護することができなくなったと判断し、自らサービスを停止しました。このようにセキュアプロトコルを利用することで通信を暗号化していても、通信内容をNSAや他の組織に傍受されている可能性があることが、具体的な事例を通して認識されつつあります。昨年11月に開催されたIETF-88においても、Pervasive Surveillance（広域監視）がメイントピックとして取り上げられています*70 *71 *72。Forward Secrecyは、その対策方法の一つとして取り上げられるようになりました。

＊64 NIST、"SUPPLEMENTAL ITL BULLETIN FOR SEPTEMBER 2013"（http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf）。
＊65 CRYPTREC、擬似乱数生成アルゴリズムDual_EC_DRBGについて（http://www.cryptrec.go.jp/topics/cryptrec_20131106_dual_ec_drbg.html）。
＊66 ArsTechica、"Stop using NSA-influenced code in our products, RSA tells customers"（http://arstechnica.com/security/2013/09/stop-using-nsa-influence-code-in-our-product-rsa-tells-customers/?comments=1&post=25330407#comment-25330407）。
＊67 Dan Shumow、Niels Ferguson、"On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng"、Rump session in CRYPTO2007（http://rump2007.cr.yp.to/15-shumow.pdf）。
＊68 Debian Security Advisory、"DSA-1571-1 openssl -- predictable random number generator"（http://www.debian.org/security/2008/dsa-1571）。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。
＊69 bitcoin.org、"Android Security Vulnerability"（http://bitcoin.org/en/alert/2013-08-11-android）。また本件に関して以下の論文で実被害が観測されている。Joppe W. Bos、J. Alex Halderman、Nadia Heninger、Jonathan Moore、Michael Naehrig、Eric Wustrow、"Elliptic Curve Cryptography in Practice"（https://eprint.iacr.org/2013/734）。
＊70 IETF Blog、"We Will Strengthen the Internet"（http://www.ietf.org/blog/2013/11/we-will-strengthen-the-internet/）。
＊71 CA Security COUNCIL Blog、"IETF 88 - Pervasive Surveillance"（https://casecurity.org/2013/11/26/ietf-88-pervasive-surveillance/）。
＊72 "IETF 88 Technical Plenary: Hardening The Internet"（https://www.youtube.com/watch?v=oV71hhEpQ20）。

### ■ Forward Secrecyの概要

上述の問題は、ストレージの暗号化など、コンテンツセキュリティの分野においてはすでに認識されていました。一旦暗号化したデータがそのまま第三者に公開された時点で、ブルートフォース攻撃（総当たり攻撃）の対象となるためです。つまり、暗号化データの公開時点で対象データの解読を行うことが可能な状況下に置かれ、攻撃者はAESなどの共通鍵暗号方式においてすべての鍵で復号を試みることができます。一方で、署名については長期保存署名として規格化されており、タイムスタンプと併用してある時点の検証情報に更に署名していく形式により、長期間に渡り検証を可能にしています。しかし、データ暗号化については長期保存技術が確立していません。

一方でSSL/TLSなどのセキュア通信プロトコルにおいて、クライアントとサーバで確立したセキュアチャネルを流れるデータの完全性は、長期に渡って保証する必要がないため、長期署名の概念は必要ありません。しかし、機密性については上記に示したように、暗号通信が何十年という単位で長期間に渡って記録され続けることで破られる可能性があるため、それを保証する仕組みが必要になりました。セキュアデータストレージにおいては、遠い将来に復号するような状況が想定されるため、暗号化に用いた鍵を適切に管理する事が要求されています。一方で、セキュア通信プロトコルを用いて一時的に暗号化する場合には、暗号化に用いた鍵を保存しておく必要はありません。このように暗号鍵管理の観点においては大きく異なります。Forward Secrecyのアイデアは、この特徴の違いである「一時的に用いた鍵は捨ててもよい」ということを利用しています。

一般的なセキュア通信プロトコルやセキュアデータストレージでは、共通鍵暗号と公開鍵暗号の両方を用いるハイブリッド方式が使われています。実データの暗号化には共通鍵暗号が利用され、コンテンツ鍵（データ暗号化に用いられる鍵）は公開鍵暗号で暗号化されています。例えば、AES暗号で用いたコンテンツ鍵を、RSA公開鍵で暗号化を行うという手順がその一例です。

SSL/TLSでは、鍵交換アルゴリズムとしてRSA、DH_RSA、DHE_RSAなどが定められています。鍵交換アルゴリズムは、コンテンツ鍵やMAC用鍵を導出するための元データを安全に共有するために用いられます。例えば、鍵交換アルゴリズムとしてRSAを選択した場合には、PreMasterSecretを安全に共有します。PreMasterSecretはクライアントが作成するランダムデータで、サーバ証明書に格納されている公開鍵を用いて暗号化することで、安全にサーバと共有することができます。つまりRSA暗号をサーバ認証と鍵交換の両方に利用しています。またDH_RSAでは、証明書に含まれているDH公開鍵を用いてDH鍵交換アルゴリズムにより安全なデータ共有を行います。一方でDHE_RSAでは、その都度異なる一時的なDH公開鍵・秘密鍵を生成します[*73]。

ここで、サーバ証明書に記載の公開鍵に対応する秘密鍵が後日漏えいしたケースを考えます。鍵交換アルゴリズムがRSAまたはDH_RSAの場合、固定された公開鍵を用いて鍵交換を行っていたため、暗号化された通信内容を長期的に盗聴されていた場合、その記録からコンテンツ鍵を導出できます。そのため暗号通信データから当時の通信内容が暴露してしまいます。

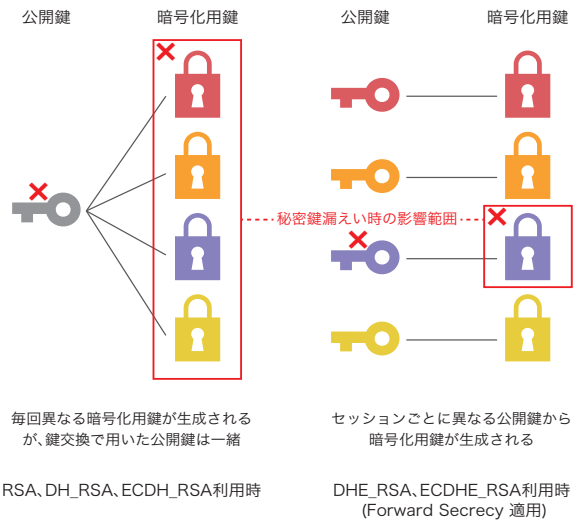



**図-13 TLSにおけるForward Secrecy不適用・適用の違い**

＊73 DHE_* の E は Ephemeral に由来する。RFCで定められているServerDHParamsの構造は最大$2^{16}$ビット長の素数p、生成元g、公開鍵 $Y=g^y$ (yは秘密鍵)の3つを格納し送付できるように設計されている。

一方でDHE_RSAでは、セッションごとにDH公開鍵・秘密鍵を生成しその都度捨ててしまうため、暗号通信データを復号するにはその通信に利用されていたDH秘密鍵の解読が必要となります。もし仮にDH秘密鍵の解読がされたとしても、対応するDH公開鍵を用いて安全に導出したコンテンツ鍵で暗号化された通信のみが暴露され、被害を限定的にすることができます。図-13は暗号化用鍵を導出するために利用された公開鍵の対応付けを表現しています。これは公開鍵に対応する秘密鍵が解読された際に暴露される暗号化用鍵の対応付けについて表現しているとも言えます。DHE_RSAの利用は、使い捨ての公開鍵をその都度作成して暗号通信を行っていることを意味します。このとき、一時的に生成されたDH公開鍵はサーバによるRSA署名により保証されており、DH鍵交換アルゴリズムが潜在的に持つ中間者攻撃への弱さを防いでいます。

TLSにおいては、1999年に策定されたRFC2246 (TLS1.0)から、Forward Secrecyが適用可能なCipherSuiteが定められています[*74]。最近では、DHの楕円曲線版であるECDHも利用されています[*75]。ECDHは2006年に策定されたRFC4492より利用可能となっており、Forward Secrecy対応の鍵交換アルゴリズムとしてはECDHE_*として記述されています[*76]。一般的にはDHよりもECDHが高速処理できるため、様々なクライアントやサーバにおいてECDHの利用が広がっています。

### ■ Forward Secrecyの適用事例と注意点

2011年から対応しているGoogle[*77]をはじめとして、2013年にはFacebook[*78]、Twitter[*79]、GitHub[*80]などがForward Secrecy対応または対応中であることを表明しています。またEFF (Electronic Frontier Foundation)により主要サイトの対応状況が随時更新されています[*81]。これらの対応に呼応する形で、技術者向けにApache+SSLなどでの具体的な設定方法例も紹介されています[*82]。しかし、Forward Secrecyを適用しても完全にPervasive Surveillanceを防ぐことはできません。以下Forward Secrecyを適用したとしても、防ぎきれない問題点について触れます。

まず、(EC)DH鍵交換アルゴリズムについての潜在的問題について説明します。サーバへの侵入などを通してRSA秘密鍵が漏えいした、またはRSAアルゴリズムが危殆化した時点で、Forward Secrecyに対応し使い捨て公開鍵を利用していたとしても、それ以降の暗号通信が漏えいする場合があります。例えばTLSにおける鍵交換アルゴリズムとしてDHE_RSAを利用する場合を考えます。クライアントはサーバから送られてきた一時的なDH公開鍵の正当性を確認しますが、クライアントとサーバに割り込んだ攻撃者はRSA秘密鍵を入手しているため、サーバから送信するDH公開鍵を書き換えることができ、中間者攻撃が可能となります。そのためRSA鍵が危殆化した場合、それ以降の暗号通信は解読可能となります。この場合、RSA鍵ペアとサーバ証明書の更新により対策することができます。

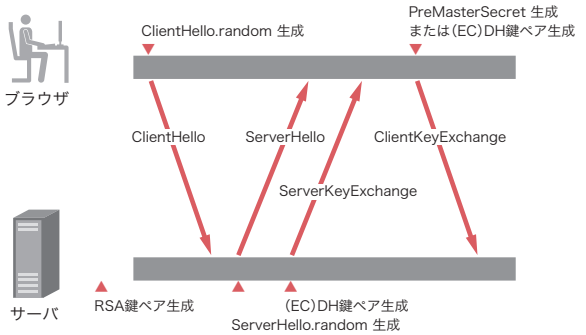
次に擬似乱数生成モジュールの問題について触れます。2013年に改訂された新しい電子政府推奨暗号リストでは、擬似乱数生成アルゴリズムのカテゴリ自体削除されており、電子政府システムや民間の情報システムにおいて、どのような擬似乱数を利用すべきかについては再考する

＊74 The TLS Protocol Version 1.0（http://www.ietf.org/rfc/rfc2246.txt)。
＊75 具体的なアルゴリズムは "Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" (http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf)の5.7.1節に記載されている。DHと同じく楕円曲線上の離散対数問題を安全性の根拠に置いている。
＊76 Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)(http://www.ietf.org/rfc/rfc4492.txt)。
＊77 Google Online Security Blog,"Protecting data for the long term with forward secrecy" (http://googleonlinesecurity.blogspot.jp/2011/11/protecting-data-for-long-term-with.html)。
＊78 Facebook Engineering,"Secure browsing by default"(https://www.facebook.com/notes/facebook-engineering/secure-browsing-by-default/10151590414803920)。
＊79 The Twitter Engineering Blog,"Forward Secrecy at Twitter"(https://blog.twitter.com/2013/forward-secrecy-at-twitter-0)。
＊80 The GitHub Blog,"Introducing Forward Secrecy and Authenticated Encryption Ciphers"（https://github.com/blog/1727-introducing-forward-secrecy-and-authenticated-encryption-ciphers)。
＊81 Electronic Frontier Foundation,"UPDATE: Encrypt the Web Report: Who's Doing What" (https://www.eff.org/deeplinks/2013/11/encrypt-web-report-whos-doing-what#crypto-chart)。
＊82 Qualys Community,"Configuring Apache, Nginx, and OpenSSL for Forward Secrecy" (https://community.qualys.com/blogs/securitylabs/2013/08/05/configuring-apache-nginx-and-openssl-for-forward-secrecy)。一部のCipherSuiteはTLS1.1やTLS1.2でしか使えないものもあるためOpenSSLなど暗号アルゴリズムの対応状況に依存する。例えばOpenSSLではバージョンが1.0.0h以降のライブラリでTLS1.2対応である。またOpenSSLではRFCで記載されているCipherSuiteと異なる記載方法が採用されている点にも注意(http://www.openssl.org/docs/apps/ciphers.html#CIPHER_SUITE_NAMES)。

必要があります。疑似乱数生成アルゴリズムの利用については、旧版のリストに対応したガイドラインに記載がありましたが、その後更新されておらず現在有効とはいえません[*83]。擬似乱数生成アルゴリズムには、互換性の確保が必要ではないという理由により、リストからカテゴリが削除されていると考えられますが、リストから削除されていても、どのような点に注意して利用・実装を行うべきかについての指針が望まれています。

乱数生成モジュールは、多くの場合、暗号ライブラリを通して利用されます。その暗号ライブラリの認定制度としては、CMVP[*84]、JCMVP[*85]があり、これらを活用することで安全に利用できると考えられます。しかし、前述したRSA BSAFEは政府機関のお墨付きを得ている暗号ライブラリだったにも関わらず、問題があったことが露呈しています。暗号ライブラリとして安全が確認されていても、擬似乱数生成モジュールに入力するSeedやNonceが短いなど、利用上の問題が発生していないかについて気を付ける必要があるでしょう。

図-14はTLSプロトコルにおいて擬似乱数モジュールを使うフェーズについてまとめたものです。TLSを利用する前にサーバはRSA鍵ペアを生成しサーバ証明書を作成します。その際にはサーバが擬似乱数生成モジュールを用いて素数を生成しますが、前述したDebian OpenSSL問題のように十分なエントロピーを確保する必要があります。TLSプロトコルはクライアントとサーバそれぞれでHelloを送信することから始まります。ClientHelloおよびServerHelloのメッセージ送信においてそれぞれ28バイトのランダムデータを含むrandomを生成します。さらに鍵交換アルゴリズムとしてRSAを選択した場合には、46バイトのランダムデータを含むPreMasterSecretをClientKeyExchangeメッセージを通して安全に共有します。またDHEやECDHEを利用する場合には一時的なDH鍵またはECDH鍵を生成して鍵交換アルゴリズムを実行しPreMasterSecretを共有します。このとき一時的な(EC)DH秘密鍵の選択範囲が少ないと、解読される危険性が増します。最後にClientHello.random、ServerHello.random、PreMasterSecretの3つのランダムデータからMasterSecretを算出します。このMasterSecretから、クライアントとサーバそれぞれのMAC鍵、コンテンツ鍵、(CBC暗号モード利用時の)初期ベクトル(IV)を導出することで安全な通信を行うことができます。TLSでは複数のランダムデータを利用して暗号化用鍵を導出する構造を持つ設計がなされていますが、安全に擬似乱数生成ができない、つまり生成される値に偏りがあるケースにおいてはTLSが安全に利用できなくなる可能性があります。




※▲▼ の箇所がTLSにおける擬似乱数生成モジュールを利用するタイミングを示している。
ここで安全な擬似乱数生成が行われないと通信の安全を脅かす可能性がある。

**図-14 TLSにおける擬似乱数生成のタイミング**

### 1.4.3 Webクローラによるwebサイト改ざん調査

IIJでは、マルウェア対策活動MITF(Malware Investigation Task Force)の一環として、Webサイト改ざん状況の調査及びドライブバイダウンロード型マルウェアの収集を目的とするWebクローラを2008年から運用しています。本稿では、現在のWebクローラ環境の概要と、最近の観測傾向を紹介します。

#### ■ Web改ざん事案の増加とWebクローラ

2013年6月、IPAや警察庁が相次いでWebサイト改ざん

＊83 電子政府推奨暗号の利用方法に関するガイドブック(http://www.cryptrec.go.jp/report/c07_guide_final_v3.pdf)にはいくつかのセキュアプロトコルでの利用に際して、同一の値が生成されないよう生成される値に十分な長さがあること、生成される値に偏りがないこと、生成される値が予測できないこと、という要件に関する記載がある。また2009年度版リストガイド(http://www.cryptrec.go.jp/report/c09_guide_final.pdf)第6章に擬似乱数生成器の章が設けられている。
＊84 Cryptographic Module Validation Program(CMVP)(http://csrc.nist.gov/groups/STM/cmvp/)はNISTが設立した暗号モジュールの試験制度である。
＊85 暗号モジュール試験及び認証制度(Japan Cryptographic Module Validation Program)(http://www.ipa.go.jp/security/jcmvp/)はCMVPの日本版であり、情報処理推進機構で運用されている。また、JCMVPとCMVPは相互に認証された製品を認める共同認証が適用されている(http://www.ipa.go.jp/about/press/20120227.html)。

に関する注意喚起を公開しました*86。また、JPCERT/CCのレポートによれば2013年10月から12月の期間には、2,774件のWeb改ざん事案が報告されました*87。

近年のWebサイト改ざん事案は、コンテンツの書き換えそのものを目的とする愉快犯や政治犯ではなく、iframeタグなどをコンテンツに挿入して、閲覧者をマルウェア配布サイトに誘導することを目的とするものが多数を占めています。この種のWeb改ざん事案は、2008年のGumblar事件*88 以降、国内外で広く発生するようになり、その後も継続していましたが、2013年は特に国内の事案が増加しています*89 。一般に安全と考えられがちな著名サイトや人気サイトが改ざんされ、多くの閲覧者を危険な状態にしてしまった事例も複数発生しています。MITFではこのような状況において、有効な対策を実施するために、Web改ざんの動向を把握するための調査を行っています。

あるWebサイトが、閲覧者にマルウェアを感染させるような改ざん被害を受けているかどうかを調査するためには、通信のキャプチャや、アクセス先の一覧及びコンテンツの収集が可能で、確認が終わったら簡単に元の状態に戻すことができる環境を構築した上で、実際にWebブラウザを起動して手動で閲覧し、マルウェアに感染するか試してみるのが一番です。しかし、毎日多数のWebサイトを手動で閲覧し、マルウェア感染の有無を確認しようとすると膨大な手作業が必要となるため現実的ではありません。MITFのWebクローラは、このような作業を自動化する仕組みです。

### ■ クライアントハニーポットとその種類

MITFのWebクローラは、ドライブバイダウンロード*90によってマルウェアに感染する脆弱なクライアント、もしくは脆弱性を模擬する環境を用いて、調査対象のWebサイトを巡回する仕組みです。これは、クライアントハニーポットと呼ばれるシステムで、この環境からマルウェア感染が行われるように改ざんされたWebサイトを閲覧した場合には、改ざんされたコンテンツや、攻撃に用いられるファイル、攻撃者が感染を意図したマルウェアなどを収集することができます。

一般に、クライアントハニーポットは、実環境を模倣する方法によって大きく2種類に分類されます。

1)高インタラクション型クライアントハニーポット

Windows環境など、通常利用されるクライアントと同等のシステムを用意して対象Webサイトを閲覧し、ダウンロードされるコンテンツを収集します。一般のクライアント環境で閲覧した場合とほぼ同一の正確な情報が得られる反面、低インタラクション型に比べて個々のサイトの巡回に要する時間が長いことや、実際にマルウェアに感染してしまうため、毎回元の状態に戻す手間がかかること、システムの構築、運用に手間がかかる(特に複数バージョンのクライアント環境を用意する場合などは更に多くの手間がかかる)などのデメリットがあります。

2)低インタラクション型クライアントハニーポット

Webブラウザなどのクライアントアプリケーションをエミュレーションするツールを利用して、対象Webサイトのコンテンツを収集します。システムの構築、運用が容易で、巡回が高速なことに加え、あくまで脆弱性を模倣して攻撃コンテンツを収集するため、実際にマルウェアに感染することはないというアドバンテージがありますが、JavaScriptエンジンの実装の問題などにより、実環境の動作を再現できない場合があることや、ドライブバイダウンロードによって攻撃されるすべての機能(脆弱性)をエミュレーションするものではないため、攻撃の結果としてダウンロードされるペイロードを収集することが難しいなどのデメリットがあります。

---

＊86 IPA、「ウェブサイト改ざんの増加に関する一般利用者(ウェブ閲覧者)向け注意喚起」(http://www.ipa.go.jp/security/topics/alert20130626.html)及び「ウェブサイト改ざん等のインシデントに対する注意喚起～ウェブサイト改ざんが急激に増えています～」(http://www.ipa.go.jp/security/topics/alert20130906.html)、警察庁、「改ざんウェブサイト閲覧によるマルウェア感染に関する注意喚起について」(http://www.npa.go.jp/cyberpolice/detect/pdf/20130626.pdf)。

＊87 JPCERT/CC、「JPCERT/CCインシデント報告対応レポート[2013年10月1日～ 2013年12月31日]」(http://www.jpcert.or.jp/pr/2014/IR_Report20140116.pdf)。

＊88 Gumblarについては、本レポートの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」及びVol.6(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol06.pdf)の「1.4.1 Gumblarの再流行」で詳しく解説をしている。

＊89 2013年3月の国内Webサイト改ざん事案については、本レポートのVol.19(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol19.pdf)の「1.4.2 日本国内のWebサイト改ざんとドライブバイダウンロード」で詳しく解説している。

＊90 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、ユーザに無許可でソフトウェア(主にマルウェア)をインストールする行為。Webブラウザやプラグインなどの脆弱性を悪用して行われることが多い。

IIJではこれら2種類のクライアントハニーポットについて多くの実装を検証してきましたが、低インタラクション型クライアントハニーポットでは、主に再現性の面で十分な機能を備えた実装が存在しなかったため、現在は独自の高インタラクション型クライアントハニーポットを構築、運用しています。

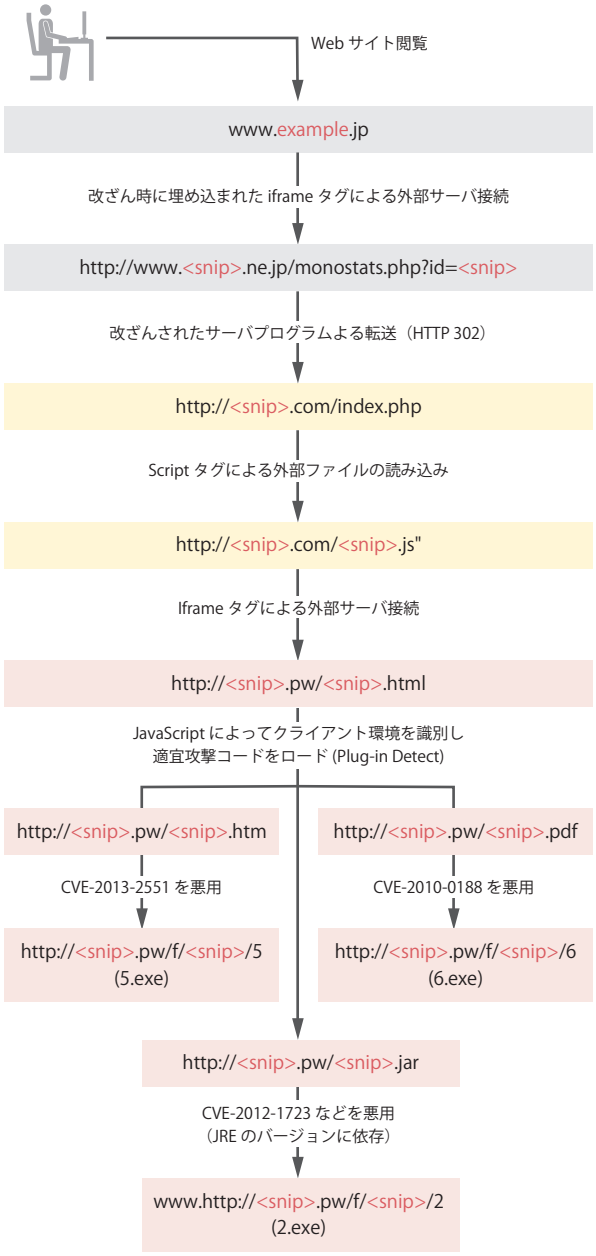
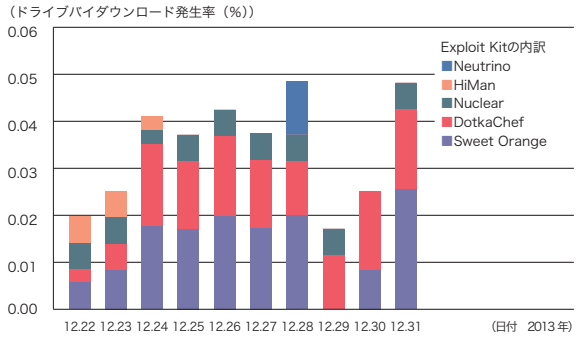



**図-15 改ざんWebサイト閲覧時の通信先フローの例**

### ■ リダイレクションの識別によるドライブバイダウンロード検出

クライアントハニーポットによる巡回後、個々のサイト閲覧時にドライブバイダウンロードが発生したか否かを判別する必要があります。しかし、Webコンテンツ改ざん時に挿入されるコードや攻撃成功時にダウンロードされるペイロードは頻繁に変更される場合が多いため、シグネチャベースの仕組みで最新の攻撃を検出することは困難です。そこで、MITFのWebクローラは、閲覧時に発生する通信の表層的な特徴を抽出することでドライブバイダウンロードの有無を分析し、攻撃が行われたと判定された場合には、サンドボックスで更に詳細な解析を行う仕組みになっています。

例えば、図-15は改ざんされたWebサイトを閲覧してドライブバイダウンロードが発生した際の典型的な接続先遷移を示したものですが、クライアントは、当初閲覧を意図したwww.example.jpとは異なるドメインの、3つのサーバに接続しています。また、それらの外部ドメインのサーバからPDFやJava（JAR）、Windows実行形式（EXE）など、通常のWeb閲覧では自動的にロードされることが稀な種類のコンテンツを取得しています。このため、ドメイン外へのリダイレクションを識別し、リダイレクション先との通信時のHTTPヘッダ情報（コンテンツタイプやファイルサイズ、User-Agentなど）を、あらかじめ設定したドライブバイダウンロードの特徴情報に基づいて評価することで、攻撃の有無を比較的高速に判別することが可能です[*91]。そし




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

**図-16 国内Webサイト閲覧時のドライブバイダウンロード発生率**

＊91　多くのWebサイトでは、外部ツールや広告などのマッシュアップコンテンツなど、運営者が意図して配置したドメイン外コンテンツが利用されているため、これらのホワイトリストなども設定する必要がある。

て、当該Webサイトが改ざんされている可能性があると判定した場合は、更にマルウェアの動的解析環境で閲覧時のシステムの挙動(利用するAPIや、ファイル、レジストリの書き込み内容など)を自動分析し、攻撃の有無及び内容について精度の高い情報を記録しています。

### ■ 巡回対象と最近の観測傾向

現在、MITFのWebクローラは国内の著名サイトや人気サイトなどを中心とした数万のWebサイトを日次で巡回しています。さらに、クローラの処理能力を調整しながら、巡回対象を順次追加しています。また、一時的にアクセス数が増加したWebサイトなどを対象に、一時的な観測も行っています。

2013年12月22日から31日の観測結果をまとめたものが図-16です。縦軸がWebサイト閲覧時のドライブバイダウンロード発生率を百分率で示し、更に、その内訳をExploit Kitの種類ごとに色分けしています。

この期間中に観測された攻撃の多くはSweet OrangeまたはDotkaChefが利用されています。Webクローラがダウンロードしたexploit及び、これらのExploit Kitの特徴[*92]から、日本国内のクライアントに対しては、主としてJREやIEの脆弱性を狙われているものと推測されます。また、この時期に観測した改ざんWebサイトには、改ざんされたコンテンツのURLや、改ざん内容などの特徴から、FTPなど正規のサーバ接続権限を奪われた上でコンテンツファイルまたはサーバ実行ファイルを改ざんされたと推測されるものや、2013年12月18日に公開されたOpenXの脆弱性[*93]を悪用して改ざんされたと推測されるものなどがありました。

このように、多数のWebサイトを巡回してドライブバイダウンロードを集計することで、改ざんサイトの増減や悪用される脆弱性の傾向などを把握できるようになり、予防策の優先順位が検討しやすくなりました。今後、このような観測傾向をIIRで定期的に公開するために、更にシステムの調整を進めています。また、改ざんを識別した個別事案に関しては、主にお客様やその関係者、場合によっては一般のインターネット利用者に対して迅速かつ効果的に報告や対応支援などを実施できるよう、運用体制の検討を進めています。IIJでは、今後もマルウェア対策を推進するため、状況の変化に応じてシステムを更新し、適切に対応していきます。

## 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、大容量メモリを搭載した端末のメモリフォレンジックにおける注意点、Forward Secrecy、WebクローラによるWebサイト改ざん調査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 大容量メモリを搭載した端末のメモリフォレンジックにおける注意点)
**須賀 祐治**(1.4.2 Forward Secrecy)
**梨和 久雄**(1.4.3 WebクローラによるWebサイト改ざん調査)
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

＊92 最近活発なExploit Kitの概要は「An Overview of Exploit Packs (Update 20) Jan 2014」(http://contagiodump.blogspot.jp/2010/06/overview-of-exploit-packs-update.html)などに詳しくまとめられている。

＊93 「Zero Day Vulnerability in OpenX Source 2.8.11 and Revive Adserver 3.0.1」(http://www.kreativrauschen.com/blog/2013/12/18/zero-day-vulnerability-in-openx-source-2-8-11-and-revive-adserver-3-0-1/)。