# 悪質化するPUA

**今回は、悪質化するPUA、前号に続きID管理技術の実際の利用例と安全性を高める取り組み、HDDのファームウェアを再プログラミングするマルウェアのIOCの検討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2015年1月から3月までの期間では、依然としてAnonymousなどのHacktivismによる攻撃が複数発生しており、SNSアカウントの乗っ取りやWebサイト改ざんなどの攻撃も多発しています。不正アクセスによる情報漏えいも多く発生しており、米国で発生した医療保険会社の事件では最大8,000万人分の個人情報が漏えいした可能性が指摘されています。PCにプリインストールされていたソフトウェアには暗号化されたWebブラウザの通信を第三者に傍受されたり、偽装されたWebサイトを正規のものと認識してしまう可能性のある問題が見つかっています。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。

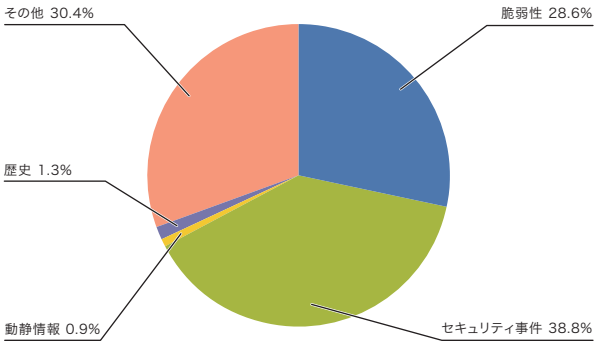



**図-1 カテゴリ別比率(2015年1月～3月)**

## 1.2 インシデントサマリ

ここでは、2015年1月から3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。様々な状況や主張に応じて、多数の国の企業や政府関連サイトに対するDDoS攻撃や情報漏えい事件が発生しました。1月には、一昨年自殺した活動家にちなみ、マサチューセッツ工科大学(MIT)の複数のWebサイトが改ざんされています。同じく、フィリピンではミンダナオ島で1月に発生した警察と武装組織との間の戦闘への抗議から政府の複数のWebサイトが改ざんされています。2月にはサウジアラビア王室への抗議からサウジアラビアの複数の銀行に対してDDoS攻撃が発生しています(OpSaudi)。またSyrian Electronic Armyを名乗る何者かによるSNSアカウントの乗っ取りも継続して発生しており、被害を受けた企業にはフランスの新聞社の1つであるLe Monde社なども含まれていました。これ以外にも、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達による攻撃が継続して行われました。政府機関や著名人のSNSアカウントの乗っ取り事件も継続して発生しています。

また、ISILもしくはその関連組織を名乗る何者かによる、SNSアカウントの乗っ取りなどの攻撃が世界中で頻発しています。この期間でも、1月に米国中央軍のTwitterとYouTubeの公式アカウントが乗っ取られる事件や、マレーシア航空

*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。

のWebサイトがDNSハイジャックによって別のWebサイトに誘導される事件が発生しました[*2]。日本でも3月に複数の企業を含むWebサイトが改ざんされる事件が発生して話題となりました。これらのWebサイト改ざん事件では、WordPressプラグインの脆弱性を悪用した攻撃が行われたと考えられます[*3]。この改ざん事件では、日本だけでなく世界中で同様の攻撃が発生していることから、米国でも4月にFBIから注意喚起が行われています[*4]。これらの攻撃に対し、フランスで発生した週刊誌襲撃事件に対するAnonymousによると考えられるイスラム過激派サイトへの攻撃が行われたり(OpCharlieHebdo)、ISIL関連のTwitterやFacebookなどのSNSアカウントについてアカウントリストを公開すると共にアカウントの停止や過去の投稿を削除するなどの攻撃が発生しています(OpISIS)。更にISILに関連していると考えられるVPNやWebサイト、そのホスティング企業のリストを公開して、停止や削除を促すなどの活動が継続して行われています。

### ■ 脆弱性とその対応

この期間中では、Microsoft社のWindows[*5][*6][*7]、Internet Explorer[*8][*9]などで修正が行われました。Adobe社のAdobe Flash Playerでも修正が行われました。Oracle社のJavaSEでも四半期ごとに行われている更新が提供され、多くの脆弱性が修正されました。これらの脆弱性のいくつかは修正が行われる前に悪用が確認されています。

サーバアプリケーションでは、データベースサーバとして利用されているOracleを含むOracle社の複数の製品で四半期ごとに行われている更新が提供され、多くの脆弱性が修正されました。DNSソフトウェアのBIND9ではDNSSECのトラストアンカーの管理において不具合があり、特定の条件下でサーバの異常動作やサービスの停止が可能となる脆弱性が修正されています。時刻同期に利用されているntpdについても、細工を施したパケットにより、ACLによる制限の回避や異常終了などの可能性のある脆弱性が複数修正されました。Linuxディストリビューションなどに含まれるThe GNU C Library(glibc)ではバッファオーバーフローによりアプリケーションの異常終了などの可能性がある脆弱性が修正されています。SSL/TLSの実装にも、1990年代に行われていた米国の暗号輸出規制で使われていた512ビット以下の弱いRSA鍵を受け入れる実装があり、これを悪用した中間者攻撃により暗号化された情報を復号される可能性のある脆弱性などが公表され、OpenSSLで修正が行われています[*10]。

Google社のProject Zeroからは、DRAMの高密度化によるメモリアクセス時のメモリセル間の干渉によって発生するエラーの問題(Row Hammer問題)を利用し、権限昇格が可能なことが発表され、話題となりました。シスコ社のIOSについても、半年ごとの定例アップデートが提供され、DoS攻撃を誘発したりメモリリークを引き起こしたりする恐れのある複数の脆弱性が修正されています。

### ■ ホームルータへの攻撃

この期間では、複数のホームルータに脆弱性が見つかり、修正されています。このうちいくつかの脆弱性については、第三者がルータの管理権限を不正に取得することが可能であったり、設定を任意に変更できる可能性のある脆弱性で

＊2　Malaysia Airlines、"Media Statement on Malaysia Airlines' Website"(http://www.malaysiaairlines.com/my/en/corporate-info/press-room/2015/media-statement-malaysia-airlines-website.html)。
＊3　警察庁、「『Islamic State(ISIS)』と称する者によるウェブサイト改ざんに係る注意喚起について」(http://www.npa.go.jp/cyberpolice/detect/pdf/20150312.pdf)。
＊4　The Internet Crime Complaint Center(IC3)、"ISIL DEFACEMENTS EXPLOITING WORDPRESS VULNERABILITIES"(https://www.ic3.gov/media/2015/150407-1.aspx)。
＊5　「マイクロソフト セキュリティ情報 MS15-002 - 緊急 Windows Telnet サービスの脆弱性により、リモートでコードが実行される(3020393)」(https://technet.microsoft.com/ja-jp/library/security/ms15-002.aspx)。
＊6　「マイクロソフト セキュリティ情報 MS15-010 - 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(3036220)」(https://technet.microsoft.com/ja-jp/library/security/ms15-010.aspx)。
＊7　「マイクロソフト セキュリティ情報 MS15-011 - 緊急 グループ ポリシーの脆弱性により、リモートでコードが実行される(3000483)」(https://technet.microsoft.com/ja-jp/library/security/ms15-011.aspx)。
＊8　「マイクロソフト セキュリティ情報 MS15-009 - 緊急 Windows Telnet Internet Explorer 用のセキュリティ更新プログラム(3034682)」(https://technet.microsoft.com/ja-jp/library/security/ms15-009.aspx)。
＊9　「マイクロソフト セキュリティ情報 MS15-018 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム(3032359)」(https://technet.microsoft.com/ja-jp/library/security/ms15-018.aspx)。
＊10　"OpenSSL Security Advisory [08 Jan 2015] DTLS segmentation fault in dtls1_get_record(CVE-2014- 3571)"(https://www.openssl.org/news/secadv_20150108.txt)。

## 1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**：カナダや米国のニュースサイトで利用していた広告配信基盤を経由してマルウェアが配布される事件が複数発生した。
詳細については次のCyphort社のBlogに詳しい。"HuffingtonPost Serving Malware via AOL Ad-Network"（http://www.cyphort.com/huffingtonpost-serving-malware/）。

脆 **9日**：OpenSSLにサービス停止や任意のコード実行の可能性を含む複数の脆弱性が発見され、修正された。
"DTLS segmentation fault in dtls1_get_record（CVE-2014-3571）"（https://www.openssl.org/news/secadv_20150108.txt）。

他 **9日**：Microsoft社は、毎月定例で行われているセキュリティ更新プログラムについて、BlogやWebでの概要の事前通知を停止することを発表した。
「2015年にマイクロソフトの事前通知サービス（ANS）を変更」（http://blogs.technet.com/b/jpsecurity/archive/2015/01/09/evolving-microsoft-s-advance-notification-service-ans-in-2015.aspx）。

他 **9日**：政府は、サイバーセキュリティ基本法の施行に基づき、サイバーセキュリティ戦略本部を設置し、政府のサイバーセキュリティの司令塔機能を担う組織として、内閣官房の情報セキュリティセンターを改称した内閣サイバーセキュリティセンターを設置した。
「内閣サイバーセキュリティセンターの設置について」（http://www.nisc.go.jp/press/pdf/reorganization.pdf）。

他 **12日**：オバマ大統領は、情報漏えいの発覚後、30日以内に情報が流出したことを顧客に通知するよう企業に求めるなど、個人情報保護の対策強化に向けた複数の法律案を公表した。
Whitehouse.gov、"FACT SHEET: Safeguarding American Consumers & Families"（https://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families）。

セ **13日**：何者かにより、米国中央軍のTwitterアカウント（@CENTCOM）とYouTubeアカウントが乗っ取られ、極秘情報とされるファイルが複数公開された。
なお、公開されたファイルについてはその後公開情報であったことが確認された。U.S. Central Command、"Statement from U.S. Central Command Regarding Twitter/YouTube Compromise"（http://www.centcom.mil/en/news/articles/statement-from-u.s.-central-command-regarding-twitter-youtube-compromise）。

脆 **14日**：Microsoft社は、2015年1月のセキュリティ情報を公開し、MS15-002の1件の緊急と7件の重要な更新を含む合計8件の修正をリリースした。
「2015年1月のマイクロソフト セキュリティ情報の概要」（https://technet.microsoft.com/ja-jp/library/security/ms15-jan）。

脆 **14日**：Adobe Flash Playerに、任意のコード実行の可能性がある、複数の脆弱性が発見され、修正された。
「APSB15-01：Adobe Flash Player用のセキュリティアップデート公開」（https://helpx.adobe.com/jp/security/products/flash-player/apsb15-01.html）。

セ **19日**：公立大学法人首都大学東京は、学校内で利用していたNASがFTP接続によって外部からアクセス可能な状態となっており、格納していた個人情報データが閲覧できるようになっていたことを公表した。
「首都大学東京における個人情報を含むＮＡＳに対する外部からのアクセスについて ＜お詫び＞」（http://www.tmu.ac.jp/news/topics/8448.html?d=assets/files/download/news/press_150119.pdf）。

他 **19日**：ENISAは、脅威情報の組織間共有を行うためのフォーマットや基準、ツールなどの情報をまとめ公表した。
"Standards and tools for exchange and processing of actionable information"（https://www.enisa.europa.eu/activities/cert/support/actionable-information/standards-and-tools-for-exchange-and-processing-of-actionable-information）。

脆 **21日**：Oracle社は、Oracleを含む複数製品について、四半期ごとの定例アップデートを公開し、Java SEの19件の脆弱性を含む合計169件の脆弱性を修正した。なお、Java7は2015年4月でサポートが終了となることから、自動更新機能を有効にしていた場合には自動的にJava8にアップデートされる措置が実施されている。
"Oracle Critical Patch Update Advisory - January 2015"（http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html）。

他 **21日**：FBIは、CryptolockerやCryptWallなどのランサムウェアによる被害が増加しているとして注意喚起を行った。
FBI、"Ransomware on the RiseFBI and Partners Working to Combat This Cyber Threat"（http://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise）。

脆 **23日**：ASUSTeK社の複数の無線LANルータにおいて、管理画面にログインした状態で悪意あるWebサイトを閲覧した場合にクロスサイトリクエストフォージェリ及びOSコマンドインジェクションにより意図しない操作が行われる可能性のある脆弱性が見つかり、修正された。
「無線LANルーター製品のクロスサイトリクエストフォージェリおよびOSコマンドインジェクションの脆弱性に対する対策済みファームウェア適用のお願い」（http://www.asus.com/jp/News/PNzPd7vkXtrKWXHR）。

脆 **23日**：Adobe Flash Playerに、任意のコード実行の可能性がある脆弱性が発見され、修正された。
「APSB15-02：Adobe Flash Playerに関するセキュリティアップデート公開」（https://helpx.adobe.com/jp/security/products/flash-player/apsb15-02.html）。

他 **23日**：テレコム・アイザック推進会議の主催により、会員企業であるISPや重要インフラ事業者など12組織が参加する大規模な通信インフラへのサイバー攻撃を想定した演習を実施した。
「通信インフラへのサイバー攻撃を想定した演習の実施【2014年度サイバー攻撃対応演習（CAE2014:Cyber Attack Exercise）】」（https://www.telecom-isac.jp/news/news20150120.html）。

脆 **25日**：Adobe Flash Playerに、任意のコード実行の可能性がある脆弱性が発見され、修正された。
「APSB15-03：Adobe Flash Playerに関するセキュリティアップデート公開」（https://helpx.adobe.com/jp/security/products/flash-player/apsb15-03.html）。

脆 **26日**：2004年に発売された有線LANルータに、SSDPリフレクション攻撃の踏み台となる可能性のある脆弱性が確認されたとして、設定でUPnP機能を無効にする対応情報を公開した。
JVN、「JVN#27142693 NP-BBRMにおけるUPnPに関する脆弱性」（http://jvn.jp/jp/JVN27142693/）。

脆 **28日**：glibcライブラリに、バッファオーバーフローにより、サービス停止や任意のコード実行が可能な脆弱性が見つかり、修正された。
"Qualys Security Advisory CVE-2015-0235 GHOST：glibc gethostbyname buffer overflow"（https://www.qualys.com/research/security-advisories/GHOST-CVE-2015-0235.txt）。

［ 凡 例 ］ 脆 脆 弱 性　セ セキュリティ事件　動 動 静 情 報　歴 歴　史　他 そ の 他

※日付は日本標準時

した。また、DrDoS攻撃[*11]の踏み台として悪用される可能性のある脆弱性も見つかり修正されています。脆弱性を悪用したホームルータに対する攻撃については、2011年にブラジルなどで発生した、ルータのDNS設定を書き換えて攻撃者が用意したDNSサーバを参照させることで偽サイトへの誘導が行われた事件などがあります[*12]。また、同様の攻撃は継続して発生しており、例えば、3月にもWebアクセス解析サービスのURLを悪用した広告配信を行っていた事件が報告されています[*13]。国内でも、2014年に不正アクセスに利用されていたプロキシサーバを運用していたとして逮捕された事業者の事件では、2012年に修正が行われていたホームルータの脆弱性を悪用して、設定されていたPPPoEの認証IDやパスワードを不正に取得していたとされています。

ホームルータについては、更新が定期的に行われるPCなどとは異なり、一度設定を行ってしまえば、ユーザがその後設定の確認やファームウェアの更新などを怠りがちです。このため、脆弱性の修正が行われていても長期間にわたりその脆弱性が放置されてしまうことがあります。このような、管理が不十分なホームルータなどのネットワーク機器を狙った攻撃については今後も継続して発生すると考えられることから、定期的に設定の確認やファームウェアの更新が提供されていないかチェックするなどの適切な管理を行うことが必要です。

### ■ なりすましによる不正ログイン

この期間でも、昨年から多数発生しているユーザのIDとパスワードを狙った試みと、取得したIDとパスワードのリストを使用したと考えられる不正ログインの試みが継続して発生しています。ポイントサービスのサイトや、新聞社の関連サイト、ISPのサポートサイトなど様々なWebサイトが攻撃対象となっています。このうち、いくつかの事件ではWebサイト上のポイントを不正に交換されるなどの金銭的な被害も発生しています。

### ■ 不正アクセスによる情報漏えい

不正アクセスによる情報漏えいも引き続き発生しています。1月には日本のプロスポーツ協会のWebサイトが不正アクセスを受け、内部の写真データ約２万点が流出する事件が発生しました。2月には米国の医療保険会社が、内部のデータベースに不正アクセスを受け、既存及び過去の顧客と従業員合わせて最大約8,000万人分の情報が漏えいする事件が発生しています。3月にはICANN（Internet Corporation for Assigned Names and Numbers）が、再び不正アクセスを受け、新gTLDのシステムが停止する事件が発生しました。更に、2月には国内のドメインレジストラへの不正アクセス事件が発生し、ドメイン登録の際に登録した管理者情報が漏えいするなどの被害が発生しました。この事件では、被害を受けた企業では早期のサービス再開が難しいとしてサービス再開を行わず、他業者への移管を実施することを発表しています[*14]。また、この期間では、国内の商社や新聞社など複数の企業で、マルウェア感染とそれによる情報漏えい事件が発生しました。これらの事件では、発信元を詐称してマルウェアが添付された、なりすましメールによって感染したPCなどの端末から、取引先の情報やメールの内容などが外部に送信されていた痕跡があったことなどが発表されています。

### ■ 政府機関の取り組み

政府機関のセキュリティ対策の動きとしては、昨年成立したサイバーセキュリティ基本法が1月に施行され、サイバーセキュリティ戦略本部が設置されました。併せて、内閣官房情報セキュリティセンターが改組し、内閣サイバーセキュリティセンターとして発足しました。更に、2月にはサイバーセキュリティ戦略本部の第1回会合が行われ、今後の活動内容についての確認とサイバーセキュリティ施策の基本的な方針について定める新たなサイバーセキュリティ戦略についての議論が行われています。3月には個人情報の保護を図りつつ、パーソナルデータの利活用の促進による新産

＊11　詳細については、本レポートのVol.23（http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol23.pdf）の「1.4.2 DrDoS攻撃とその対策」も参照のこと。
＊12　詳細については、次のIIJ-SECT Blog、「ホームルータへの不正な設定変更による偽DNSサーバの参照」（https://sect.iij.ad.jp/d/2012/06/148528.html）などを参照のこと。
＊13　Ara Labs Technology、"Ad-Fraud Malware Hijacks Router DNS – Injects Ads Via Google Analytics"（http://aralabs.com/2015/03/25/ad-fraud-malware-hijacks-router-dns-injects-ads-via-google-analytics/）。
＊14　有限会社テレワークコミュニケーションズ、「お客様情報の漏えいに関するお詫びとご報告」（http://www.ariqui.net/）。

## 2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

脆 **1日**：英国のセキュリティ企業の研究者より、Microsoft社のInternet Explorer11にユニバーサルクロスサイトスクリプティング（XSS）の未修正の脆弱性があることが公表された。

セ **2日**：複数日に渡り、特定のドメインに対する大規模なDoS攻撃が発生し、国内の複数社のDNSサーバで障害が発生した。

脆 **4日**：ntpdに、IPアドレスの偽装によるACLの制限回避（CVE-2014-9298）や細工したパケットによる情報漏えいや異常終了などの可能性のある脆弱性（CVE- 2014-9297）が見つかり、修正された。
JVN、「JVNVU#96605606 Network Time Protocol daemon（ntpd）に複数の脆弱性」（http://jvn.jp/vu/JVNVU96605606/）。

セ **4日**：2013年に発生した遠隔操作ウイルス事件について、容疑者である男性に対し懲役8年の実刑判決が言い渡された。

セ **5日**：米国の医療保険会社であるAnthemは、既存及び過去の顧客と従業員合わせて約8,000万人分の情報を含むデータベースが不正侵入を受けたことを公表した。
Anthem、"How to Access & Sign Up For Identity Theft Repair & Credit Monitoring Services"（https://www.anthemfacts.com/）。

脆 **6日**：Adobe Flash Playerに、任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「APSB15-04：Adobe Flash Playerに関するセキュリティアップデート公開」（https://helpx.adobe.com/jp/security/products/flash-player/apsb15-04.html）。

他 **6日**：IPAより、「情報セキュリティ10大脅威 2015」が公表された。
「情報セキュリティ10大脅威 2015」（http://www.ipa.go.jp/security/vuln/10threats2015.html）。

他 **10日**：政府の第1回サイバーセキュリティ戦略本部の会合が開催され、サイバーセキュリティに関する施策の総合的かつ効果的な推進を図るためのサイバーセキュリティ戦略の策定について議論が行われた。
「第１回会合（平成２７年２月１０日）」（http://www.nisc.go.jp/conference/cs/index.html#cs01）。

脆 **11日**：Microsoft社は、2015年2月のセキュリティ情報を公開し、MS15-009やMS15-010、MS15-011の3件の緊急と6件の重要な更新を含む合計9件の修正をリリースした。
「2015 年 2 月のマイクロソフト セキュリティ情報の概要」（https://technet.microsoft.com/ja-jp/library/security/ms15-feb）。

他 **13日**：米国で、政府機関と民間企業の間でサイバー空間での脅威やシステム侵害から守るために情報共有を求める大統領令が発効された。
Whitehouse.gov、"FACT SHEET：Executive Order Promoting Private Sector Cybersecurity Information Sharing"（https://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform）。

他 **18日**：Microsoft社は、サイバー犯罪対策の研究センターであるサイバークライムセンターの日本サテライトを開設し、政府機関や企業などの顧客に対する情報提供や技術支援を行っていくことを発表した。
「日本におけるサイバーセキュリティへの取り組みを強化、「マイクロソフト サイバークライムセンター 日本サテライト」を展開」（http://news.microsoft.com/ja-jp/2015/02/18/150218-cybercrimecenter-japan/）。

脆 **19日**：BIND9に、トラストアンカーの自動更新の例外処理の実装に不具合があり、サーバの異常動作やサービスの停止が可能となる脆弱性が見つかり、修正された。
Internet Systems Consortium、"CVE-2015-1349: A Problem with Trust Anchor Management Can Cause named to Crash"（https://kb.isc.org/article/AA-01235）。

セ **20日**：PCにプリインストールされたソフトウェアに証明書を偽装した不正なサイトになりすましたり、MITM攻撃が可能となる複数の問題が見つかり、修正された。
この問題については次のLenovo社の発表などを参照のこと。「Superfishに関するレノボの見解」（http://www.lenovo.com/news/jp/ja/2015/02/0220.shtml）。

他 **20日**：独立行政法人情報処理推進機構（IPA）は、利用者が翻訳サービスのWebサイトに入力した内容がインターネットに公開されるなど、Webサービスの利用による意図しない情報漏えいの問題が発生しているとして注意喚起を行った。
「プレス発表【注意喚起】クラウドサービスに入力した内容の意図しない情報漏えいに注意」（http://www.ipa.go.jp/about/press/20150220.html）。

セ **25日**：欧州刑事警察機構のEuropol's European Cybercrime Centre（EC3）は、Microsoft社やSymantec社などの複数のセキュリティベンダーと共同でRamnitボットネットのテイクダウンを行ったことを発表した。
"Botnet taken down through international law enforcement cooperation"（https://www.europol.europa.eu/content/botnet-taken-down-through-international-law-enforcement-cooperation）。

［ 凡 例 ］ 脆 脆 弱 性　セ セキュリティ事件　動 動 静 情 報　歴 歴　史　他 そ の 他

※日付は日本標準時

業・サービスの創出と国民の安全・安心の向上の実現を図る、改正個人情報保護法案が閣議決定されています。この中では、個人情報の保護及び有用性の確保に資するため、個人情報の定義の明確化や個人情報の復元ができないように加工した匿名加工情報の取り扱いについての規律を定めることや個人情報の取り扱いの監視監督権限を有する第三者機関として個人情報保護委員会を新設することなどが定められています。また、情報漏えい事件を受け、個人情報が記録されているデータベースから情報を不正に提供・盗用する行為について、個人情報データベース提供罪が創設されるなどの罰則の強化も図られています。なお、この閣議決定では特定個人情報（マイナンバーを含む情報）の利用の推進に係る制度も改正されており、マイナンバーの金融・医療などの分野における利用範囲の拡充が図られることになっています。

### ■ PCにプリインストールされたソフトウェアの問題

この期間では、Lenovo社のPCにプリインストールされていたソフトウェアの問題が話題となりました。2014年9月から2015年1月に停止されるまでの間に出荷されたPCにインストールされていたこのソフトウェアは、ユーザのブラウザ表示に広告を挿入して表示させる機能を持ったいわゆるアドウェアであり、特に自己署名証明書をローカルの証明書ストアにインストールすることで暗号化されたSSL/TLS通信にも割り込んで広告表示を行っていたことから問題となりました。更に、このインストールされた証明書の強度が十分でない暗号化方式だったことや、インストールされた証明書の秘密鍵がソフトウェア内に含まれており、秘密鍵が明らかとなってしまうなど、複数の問題があったことが指摘されています。この問題については、実際にはこのソフトウェアが利用していたSDKの問題であったことから、同じSDKを利用している複数のソフトウェアでも同じ問題があることが判明し注意喚起が行われています[*15]。Lenovo社では公表すると共にソフトウェアの除去のためツールを提供するなどの対応を行っており、セキュリティベンダーなどとも共同で対処したことから、問題のあるPCは減少していることが報告されています[*16]。しかしながら、このようなユーザの通信を傍受するような取り組みはユーザのプライバシーやセキュリティを危険にするとの指摘が米国の非営利組織などからされています[*17]。

### ■ その他

1月にはカナダや米国のニュースサイトで利用していた広告配信基盤を経由してマルウェアが配布される事件が複数発生しました。この攻撃については2014年10月に発生したYouTubeを経由した偽広告によるマルウェアへ誘導する攻撃[*18]と類似点が指摘されています。このような広告配信の仕組みを使った攻撃はMalvertisingとも呼ばれ、国内でも2010年に複数の報道機関やニュースサイトで利用されていた広告配信サーバが不正アクセスによって改ざんされる事件がありましたが[*19]、その後も継続して確認されています。更に、改ざんだけでなく正規の広告枠を利用した不正なソフトウェアへの誘導も頻発しており、大量のマルウェア感染を可能にする効率的な手法として認識されています。このような広告配信の仕組みを悪用した攻撃は今後も継続して発生すると考えられることから引き続き注意が必要です。

サイバー攻撃への対応能力の強化に向けた取り組みの1つとして官民や民間企業同士の情報共有の必要性が言われています。しかし、異なる組織や企業の間での攻撃などの脅威情報の共有では、どのような情報が必要でどれを共有すべきかなど、情報の取り扱いが明確に決まっていないことから情報共有しにくいといった問題が指摘されていました。米国の非営利組織であるMITRE Corporation（MITRE）[*20]が中心となって仕様策定を進めている、攻撃などの脅威情報を構造化し、サイバー攻撃の分析、特徴となる事象の特定、サイバー攻撃対応の管理、サイバー攻撃に関する情報の共有などを目的としたXMLを用いた記述仕様であるSTIX

＊15 JVN、「JVNVU#92865923 Komodia RedirectorがルートCA証明書と秘密鍵をインストールする問題」（http://jvn.jp/vu/JVNVU92865923/）。
＊16 Microsoft Malware Protection Center、"MSRT March：Superfish cleanup"（http://blogs.technet.com/b/mmpc/archive/2015/03/10/msrt-march-superfish-cleanup.aspx）。
＊17 Electronic Frontier Foundation（EFF）、"Dear Software Vendors：Please Stop Trying to Intercept Your Customers' Encrypted Traffic"（https://www.eff.org/deeplinks/2015/02/dear-software-vendors-please-stop-trying-intercept-your-customers-encrypted）。
＊18 トレンドマイクロセキュリティブログ、「YouTube上の偽広告からランサムウェア感染へ誘導、主に米国で被害」（http://blog.trendmicro.co.jp/archives/10094）。
＊19 マイクロアド社、「【障害報告】弊社サービスの改ざんに関するお詫びと報告」（http://www.microad.co.jp/news/information/detail.php?newid=News-0118）。
＊20 MITRE Corporation（http://www.mitre.org/）。

## 3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 **3日**：空港会社のWebサイトが何者かに不正侵入され、別のWebサイトに誘導されるよう改ざんされる事件が発生した。
成田国際空港株式会社、「弊社ホームページ改ざんに関するお詫びと復旧のご報告」(http://www.narita-airport.jp/jp/news/150305.html)。

脆 **4日**：TLS/SSLプロトコルに、米国による暗号の輸出規制が行われた時の弱いRSA暗号に起因し、特定の条件下で中間者攻撃が可能な脆弱性など複数の脆弱性が見つかり、修正された。
この攻撃手法の詳細については次の発見者による解説などを参照のこと。"FREAK：Factoring RSA Export Keys"(https://www.smacktls.com/#freak)。

セ **7日**：BitTorrentクライアントソフトの1つであるμTorrentでBitcoinのマイニングを行うソフトウェアがユーザーの許可なくインストールされるとして問題となった。
この問題に経緯については次のμTorrentのユーザフォーラムで確認できる。"Warning：EpicScale "riskware" installed with latest uTorrent"(http://forum.utorrent.com/topic/95041-warning-epicscale-riskware-installed-with-latest-utorrent/)。

脆 **10日**：DRAMの高密度化によるメモリアクセス時のメモリセル間の干渉によって発生するエラーの問題(Row Hammer問題)を利用し、権限昇格が可能なことが発表された。
詳細については次のGoogle社のProject Zeroによる発表を参照のこと。"Exploiting the DRAM rowhammer bug to gain kernel privileges"(http://googleprojectzero.blogspot.in/2015/03/exploiting-dram-rowhammer-bug-to-gain.html)。

他 **10日**：政府は、個人情報保護法と番号利用法の改正案を閣議決定し、国会に法案を提出した。
内閣官房、第189回通常国会 国会提出法案「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律案」(http://www.cas.go.jp/jp/houan/189.html)。

脆 **11日**：Microsoft社は、2015年3月のセキュリティ情報を公開し、MS15-018など5件の緊急と9件の重要な更新を含む合計14件の修正をリリースした。
「2015年3月のマイクロソフト セキュリティ情報の概要」(https://technet.microsoft.com/ja-jp/library/security/ms15-mar)。

セ **11日**：国内の複数のWebサイトについて、WordPressの脆弱性を悪用したと考えられる改ざん事件が発生した。
警察庁、「『Islamic State(ISIS)』と称する者によるウェブサイト改ざんについて」(http://www.npa.go.jp/keibi/biki/201503kaizan.pdf)。

他 **12日**：警察庁は、平成26年中のサイバー空間をめぐる脅威の情勢について公表した。サイバー犯罪の検挙件数が減少した一方で、都道府県警察の相談窓口で受理した相談件数は前年より増加し、過去最高の件数を記録している。また、手口が悪質化、巧妙化しており、インターネットバンキングに関わる不正送金事犯においては、発生件数、被害額共に過去最悪の被害となっていることなどが述べられている。
「平成26年中のサイバー空間をめぐる脅威の情勢について」(http://www.npa.go.jp/kanbou/cybersecurity/H26_jousei.pdf)。

他 **12日**：IPAは、Webサイトの情報漏えいや改ざんなどの意図しない被害を防ぐために開発者や運用者が考慮すべき点についてまとめた、「安全なウェブサイトの作り方」の改訂第7版を公開した。
今回の改訂ではパスワードリスト攻撃など複数の攻撃についての対策を追加している。「安全なウェブサイトの作り方」(https://www.ipa.go.jp/security/vuln/websecurity.html)。

脆 **13日**：Adobe Flash Playerに、任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「APSB15-05：Adobe Flash Playerに関するセキュリティアップデート公開」(https://helpx.adobe.com/jp/security/products/flash-player/apsb15-05.html)。

他 **17日**：国立国会図書館は、情報通信に関わる政策や深刻化しているサイバーセキュリティについて現状と課題をまとめた、調査報告書「情報通信をめぐる諸課題」「情報通信技術の進展とサイバーセキュリティ」を刊行した。
「情報通信をめぐる諸課題(平成26年度 科学技術に関する調査プロジェクト)」(http://www.ndl.go.jp/jp/diet/publication/document/2015/index.html)。

セ **18日**：中国国内のサイトブロックの状況を知ることのできるGreatFire.orgが、大規模なDDoS攻撃を受けていることを公表した。
この攻撃についてはGreatFire.org、"We are under attack"(https://en.greatfire.org/blog/2015/mar/we-are-under-attack)を参照のこと。

脆 **26日**：シスコ社は、IOSに対する半年ごとの定例アップデートを公開し、DoS攻撃を誘発したり、メモリリークを引き起こしたりする恐れのある合計7件の修正をリリースした。
"Cisco Event Response：March 2015 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication"(http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar15.html)。

セ **26日**：米国のGitHub社が複数日に渡る大規模なDDoS攻撃を受けた。
GitHub社の発表は次の"Large Scale DDoS Attack on github.com"(https://github.com/blog/1981-large-scale-ddos-attack-on-github-com)で確認できる。

他 **31日**：IPAより、効果的な脆弱性対策を行うための脆弱性情報の収集及び集めた情報の活用方法についての手引きをまとめた「脆弱性対策の効果的な進め方(実践編)」が公開された。
「IPAテクニカルウォッチ『脆弱性対策の効果的な進め方(実践編)』」(http://www.ipa.go.jp/security/technicalwatch/20150331.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

(Structured Threat Information eXpression)について、解説を行った「脅威情報構造化記述形式STIX概説」が、IPAより公表されています[*21]。

3月に米国のGitHub社に対し、複数日にわたる大規模なDDoS攻撃が発生しました[*22]。この攻撃では中国国外のユーザが中国の検索サービス事業者を利用した際に、何者かによるJavaScriptの改ざんが行われ、攻撃に利用された可能性が指摘されています[*23]。

同じく3月には、エジプトの中間認証局から複数のGoogleドメインの証明書が不正に発行される事件が発生しています。これらの証明書については、主要なブラウザで当該証明書を無効にする対応が順次行われました。この事件では、証明書を発行する際の正当性の確認を、証明書を発行するドメイン名のメールアドレスを使って連絡可能であることを確認するだけで行っていたとされています。また、複数の認証局でこのように証明書発行時の正当性の確認が不十分であることが分かり、注意喚起が行われています[*24]。

## 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、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、2015年1月から3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

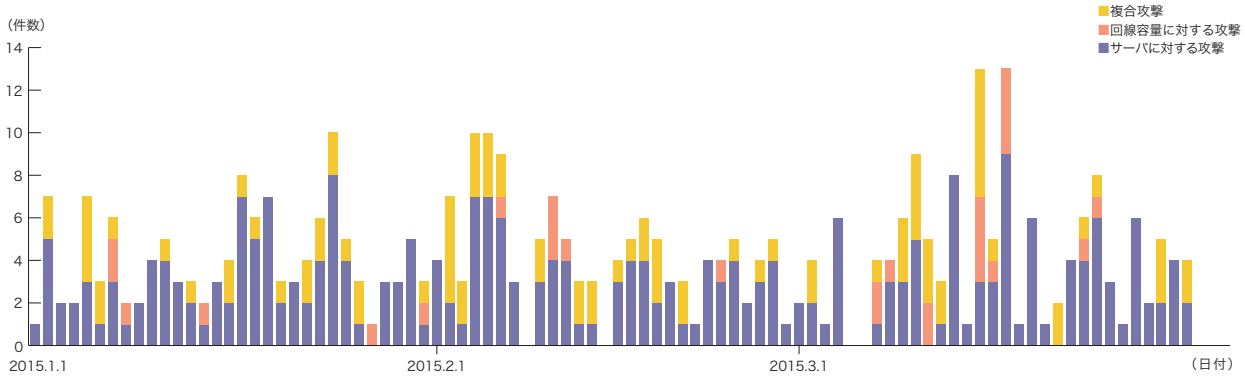



**図-2 DDoS攻撃の発生件数**

*21 IPA、「脅威情報構造化記述形式STIX概説」(http://www.ipa.go.jp/security/vuln/STIX.html)。
*22 この攻撃については、例えば次のSophos社のNakedsecurity Blog、"Greatfire.org faces daily $30,000 bill from DDoS attack"(https://nakedsecurity.sophos.com/2015/03/20/greatfire-org-faces-daily-30000-bill-from-ddos-attack/)などを参照のこと。
*23 攻撃手法については、次のレポートに詳しい。"Using Baidu 百度 to steer millions of computers to launch denial of service attacks"(https://drive.google.com/file/d/0ByrxblDXR_yqeUNZYU5WcjFCbXM/view)。
*24 JVN、「JVNVU#92002857複数の認証局においてメールアドレスのみに基づいて証明書を発行している問題」(https://jvn.jp/vu/JVNVU92002857/index.html)。

量に対する攻撃[*25]、サーバに対する攻撃[*26]、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、384件のDDoS攻撃に対処しました。1日あたりの対処件数は4.27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ました。DDoS攻撃全体に占める割合は、サーバに対する攻撃が69.3%、複合攻撃が23.4%、回線容量に対する攻撃が7.3%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117万9千ppsのパケットによって2.83Gbpsの通信量を発生させる攻撃でした。

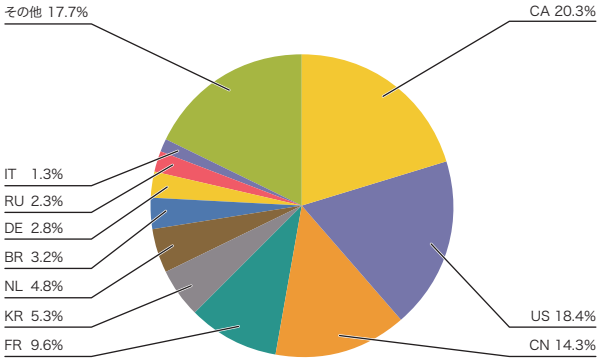



**図-3 DDoS攻撃のbackscatter観測による攻撃先の国別分類**

攻撃の継続時間は、全体の82.6%が攻撃開始から30分未満で終了し、17.4%が30分以上24時間未満の範囲に分布しており、24時間以上継続した攻撃はありませんでした。なお、今回最も長く継続した攻撃は、複合攻撃に分類されるもので10時間37分にわたりました。

攻撃元の分布としては、多くの場合、国内、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[*27]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[*28]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[*29]によるDDoS攻撃のbackscatter観測結果を示します[*30]。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。

2015年1月から3月の間に観測した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。

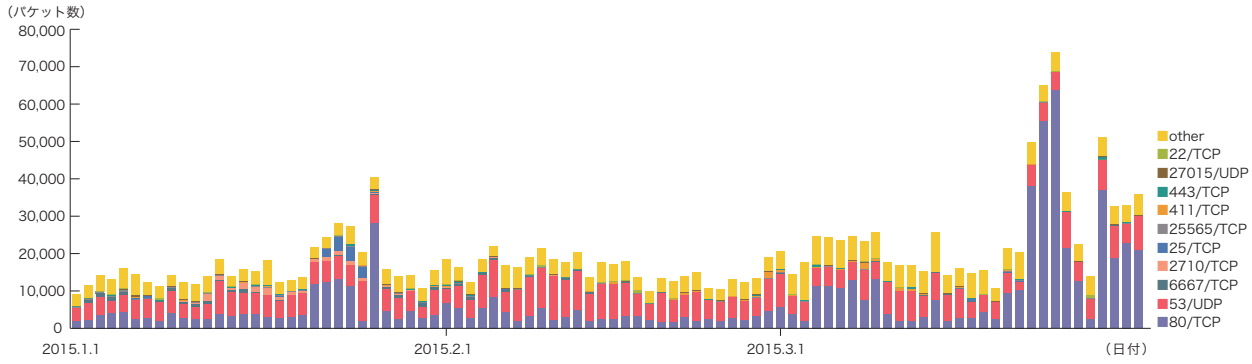



**図-4 DDoS攻撃によるbackscatter観測（観測パケット数、ポート別推移）**

＊25 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。

＊26 TCP SYN floodやTCP connection flood、HTTP GET flood攻撃など。TCP SYN flood攻撃は、TCP接続の開始の呼を示すSYNパケットを大量に送付することで、攻撃対象に大量の接続の準備をさせ、対象の処理能力やメモリなどを無駄に利用させる。TCP Connection flood攻撃は、実際に大量のTCP接続を確立させる。HTTP GET flood攻撃は、Webサーバに対しTCP接続を確立した後、HTTPのプロトコルコマンドGETを大量に送付することで、同様に攻撃対象の処理能力やメモリを無駄に消費させる。

＊27 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。

＊28 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。

＊29 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。

＊30 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。

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38.2%を占めています。次いでDNSで利用される53/UDPが31.8%を占めており、上位2つで全体の70%に達しています。また、IRC（Internet Relay Chat）で利用される6667/TCP、SMTPで利用される25/TCP、HTTPSで利用される443/TCPへの攻撃、通常は利用されない2710/TCPや25565/TCP、27015/UDPなどへの攻撃が観測されています。

2014年2月から多く観測されている53/UDPは、1日平均のパケット数を見ると、前回の約3,900から増加して約6,200になっており、依然として増加傾向にあります。

図-3で、DDoS攻撃の対象となったIPアドレスと考えられるbackscatterの発信元の国別分類を見ると、カナダの20.3%が最も大きな割合を占めています。その後に米国の18.4%、中国の14.3%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みると、Webサーバ（80/TCP）への攻撃としては、1月21日から26日にかけてカナダのホスティング事業者への攻撃を観測しています。この事業者では3月20日から再び、ある中国製ゲームに関連する複数のWebサイトに対象を絞った攻撃が継続して観測されています。また、3月4日から9日にかけて米国ホスティング事業者に対する攻撃を観測しています。他のポートへの攻撃としては、1月22日から25日にかけてフランスのゲーム関連サイトに対する25/TCPへの攻撃が観測されています。

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、1月1日から4日にかけてフィンランドの金融機関グループへの攻撃、1月11日にAnonymousによるイスラム過激派サイトへの攻撃（OpCharlieHebdo）、3月27日から29日にかけてGitHubへの攻撃をそれぞれ検知しています。GitHubへの攻撃については、報告されている攻撃手法ではbackscatterが発生しないことから、他の手法によるDDoS攻撃も並行して行われていたことが分かります。

### 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[*31]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[*32]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。

＊31 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。
＊32 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。

### ■ 無作為通信の状況

2015年1月から3月の期間中に、ハニーポットに到着した通信の発信元IPアドレスの国別分類を図-5に、その総量(到着パケット数)の推移を図-6に、それぞれ示します。MITFでは、数多くのハニーポットを用いて観測を行っていますが、ここでは1台あたりの平均を取り、到着したパケットの種類(上位10種類)ごとに推移を示しています。また、この観測では、MSRPCへの攻撃のような特定のポートに複数回の接続を伴う攻撃は、複数のTCP接続を1回の攻撃と数えるように補正しています。

ハニーポットに到着した通信の多くは、Microsoft社のOSで利用されているTCPポートに対する探索行為でした。また、同社のSQL Serverで利用される1433/TCP、SSHで利用される22/TCP、Telnetで利用される23/TCP、HTTP Proxyで用いられる8080/TCP、ICMP Echoリクエストや HTTPで使われる80/TCPや443/TCP、RDPで使われる3389/TCPに対する探査行為も観測されています。前号の11月以降継続していたTelnet(23/TCP)への通信の増加は2月まで続いていました。調査したところ、中国及び日本に割り当てられたIPアドレスから主に受信しています。2月17日から2月20日にかけて、中国、米国、香港、台湾、ロシアなどに割り当てられた多くのIPアドレスからの通信が増加しています。通信の多くはssh、Telnet、Proxyサーバなどを見つけるための探査行為でした。3月21日から3月23日には中国、米国などに割り当てられた多くのIPアドレスからの通信が増加しており、これについても同様の傾向になっていました。

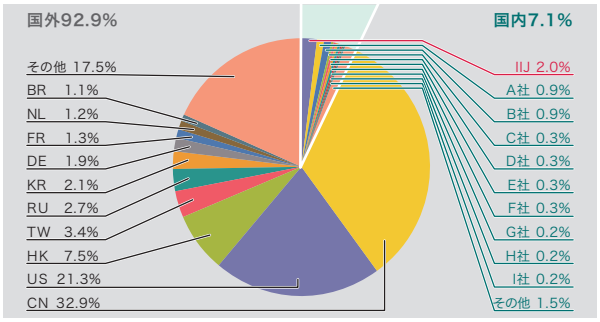



**図-5 発信元の分布(国別分類、全期間)**

### ■ ネットワーク上のマルウェアの活動

同じ期間中における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[*33]の総数を総取得検体数、検体の種類をハッシュ値[*34]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、Conickerと認められたデータを除いて集計しています。

期間中の1日あたりの平均値は、総取得検体数が87、ユニーク検体数が19でした。未検出の検体をより詳しく調査した

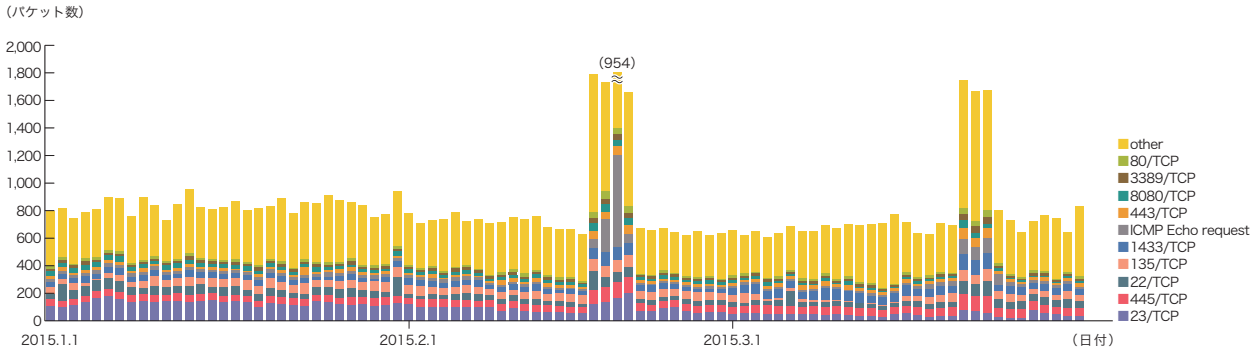



**図-6 ハニーポットに到着した通信の推移(日別・宛先ポート別・1台あたり)**

*33 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。

*34 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。

結果、中国、米国、インド、台湾などに割り当てられたIPアドレスでWormなどが観測されました。また、未検出の検体の約49%がテキスト形式でした。これらテキスト形式の多くはHTMLであり、Webサーバからの404や403によるエラー応答であるため、古いワームなどのマルウェアが感染活動を続けているものの、新たに感染させたPCが、マルウェアをダウンロードしに行くダウンロード先のWebサイトが既に閉鎖させられていると考えられます。

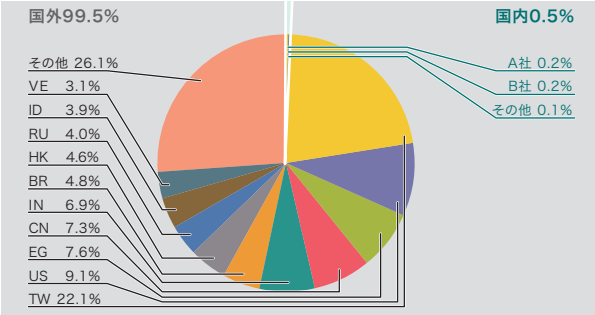



**図-7 検体取得元の分布(国別分類、全期間、Conficker除く)**

MITF独自の解析では、今回の調査期間中に取得した検体は、ワーム型94.3%、ボット型2.3%、ダウンローダ型3.4%でした。また解析により、105個のボットネットC&Cサーバ[*35]と14個のマルウェア配布サイトの存在を確認しました。ボットネットのC&Cサーバが前号に続き大幅に増加していますが、これはDGA(ドメイン生成アルゴリズム)を持つ検体が期間中に出現したためです。

## ■ Confickerの活動

本レポート期間中、Confickerを含む1日あたりの平均値は、総取得検体数が19,434、ユニーク検体数は608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99.5%、ユニーク検体数で97.0%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との比較で約19%増加し、ユニーク検体数は前号から約9%増加しました。Conficker Working Groupの観測記録[*36]によると、2015年4月3日

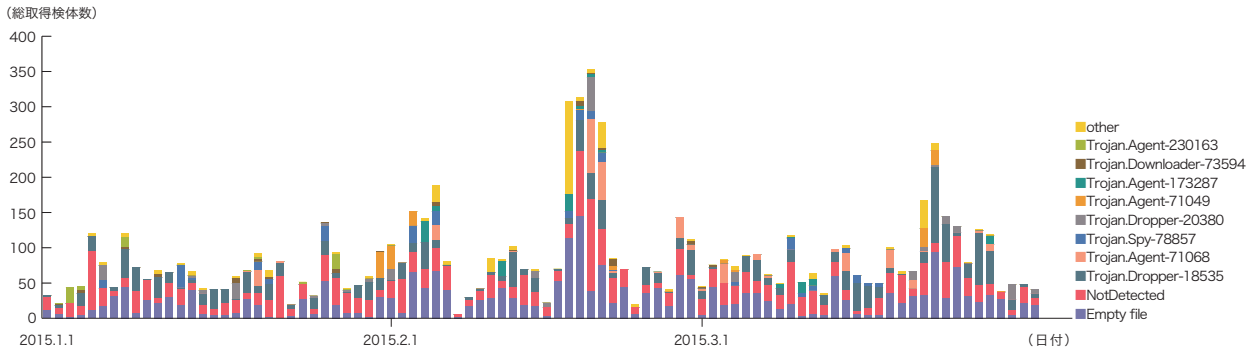



**図-8 総取得検体数の推移(Confickerを除く)**

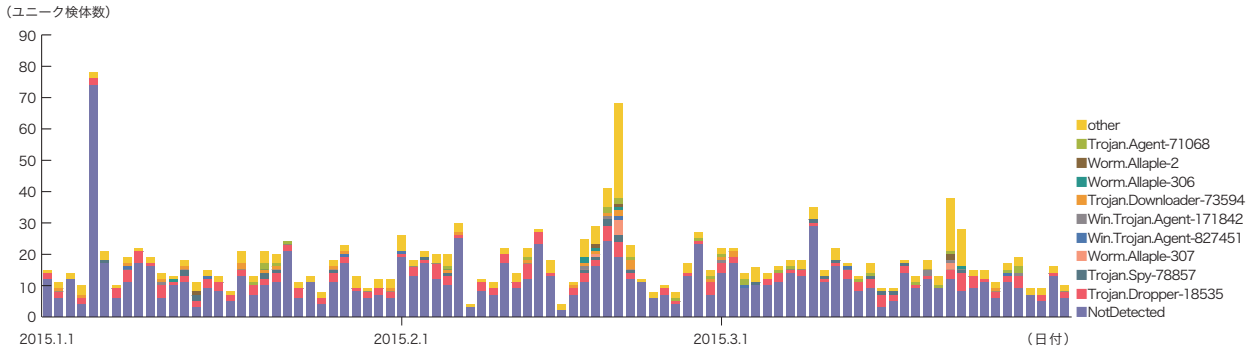



**図-9 ユニーク検体数の推移(Confickerを除く)**

*35 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。
*36 Conficker Working Groupの観測記録(http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTrackingblank)。

現在で、ユニークIPアドレスの総数は707,844とされています[*37]。2011年11月の約320万台と比較すると、約22%に減少したことになりますが、依然として大規模に感染し続けていることが分かります。

### 1.3.3 SQLインジェクション攻撃

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[*38]について継続して調査を行っています。SQLインジェクション攻撃は、過去にも度々流行し話題となった攻撃です。SQLインジェクション攻撃には、データを盗むための試み、データベースサーバに過負荷を起こすための試み、コンテンツ書き換えの試みの3つがあることが分かっています。

2015年1月から3月までに検知した、Webサーバに対するSQLインジェクション攻撃の発信元の分布を図-10に、

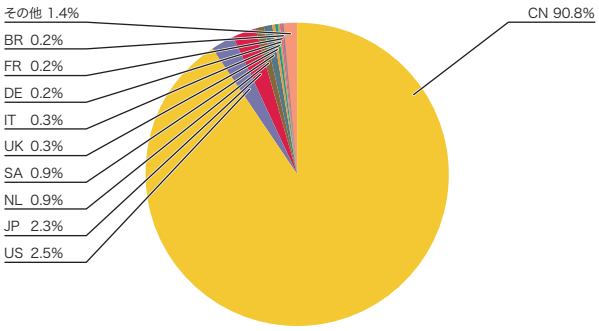



**図-10 SQLインジェクション攻撃の発信元の分布**

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、中国90.8%、米国2.5%、日本2.3%となり、以下、その他の国々が続いています。Webサーバに対するSQLインジェクション攻撃の発生件数は前回に比べて大幅に増加しました。これは主に中国からの攻撃が大幅に増加したためで、複数回にわたって大規模な攻撃が発生しています。

この期間中、2月13日には中国の複数の攻撃元から特定の攻撃先に対する攻撃が発生していました。2月16日にも別の複数の攻撃元より複数の攻撃先に対する攻撃が発生しています。2月20日から23日にかけ、中国の複数の攻撃元より、複数の攻撃先に対する大規模な攻撃が発生しました。このうち1つの攻撃先については、3月27日から3月30日にかけても別の中国の攻撃元からの攻撃が発生しています。この攻撃先に対する攻撃は、この期間中に発生した攻撃全体の66.3%を占めています。攻撃は複数の攻撃元から行われており、1つの攻撃元から40万回以上の攻撃を行っている場合が複数見られました。また、攻撃先に金融関連の企業が多いことから、これらの企業を対象とした大規模な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。

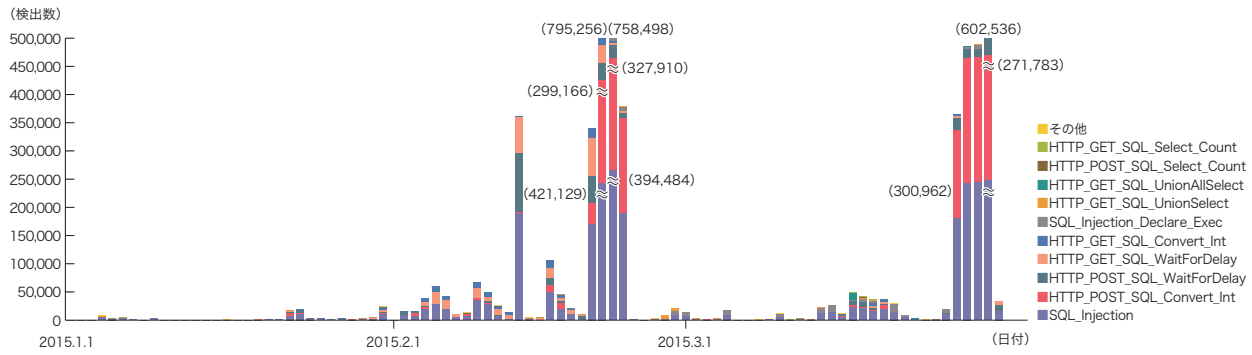



**図-11 SQLインジェクション攻撃の推移(日別、攻撃種類別)**

*37 Conficker Working Groupのデータは何らかの理由により、2015年3月28日から4月2日までの間、データが欠損しているように見えるため、影響を受けていないと思われる2015年4月3日のデータを採用している。

*38 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。

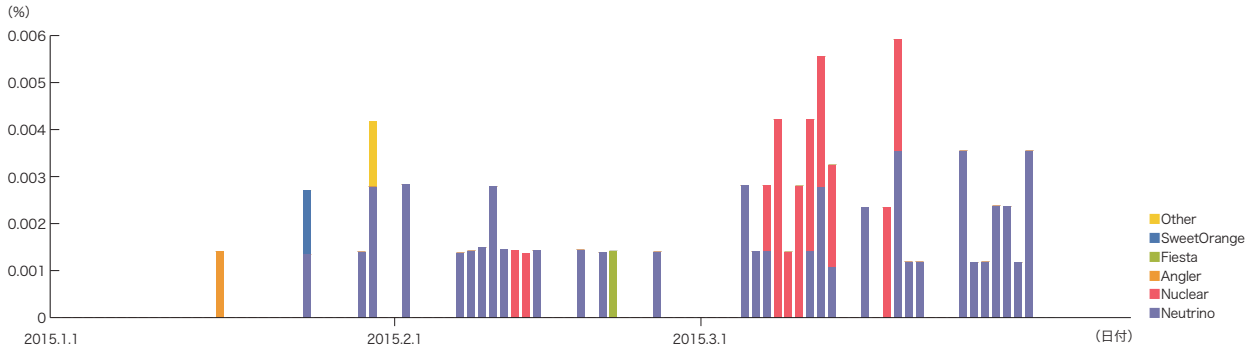
### 1.3.4 Webサイト改ざん

MITFのWebクローラ（クライアントハニーポット）によって調査したWebサイト改ざん状況を示します[*39]。

このWebクローラは国内の著名サイトや人気サイトなどを中心とした数万のWebサイトを日次で巡回しており、更に巡回対象を順次追加しています。また、一時的にアクセス数が増加したWebサイトなどを対象に、一時的な観測も行っています。一般的な国内ユーザによる閲覧頻度が高いと考えられるWebサイトを巡回調査することで、改ざんサイトの増減や悪用される脆弱性、配布されるマルウェアなどの傾向が推測しやすくなります。

2015年1月から3月の期間に観測されたドライブバイダウンロードは、既に減少傾向にあった2014年10月から12月の期間より更に10パーセント程度、減少しました（図-12）。特に1月中はほとんど活動がみられませんでした。また、攻撃数の増加してきた2月後半以降は、週末には検知数が急減する傾向が見られました。攻撃の内訳は、本Webクローラ稼働開始時から継続して検知しているNuclear及び、2014年2月以降検知されていなかった[*40]Neutrinoの2種類が大部分を占めました。どちらのExploit Kitも、昨今流行した他の多くのExploit Kitと同様に、Flashの脆弱性（CVE-2014-0515、CVE-2014-0569、CVE-2015-0313、CVE-2015-0336 など）を悪用する機能を備え、更に新規の脆弱性を悪用する機能を速いペースで追加しています[*41]。改ざんされ誘導元となっているWebサイトは、長期（3ヵ月以上）にわたって断続的に誘導元として観測されるケースがほとんどでした。また、コンテンツの傾向としては、成人向け動画コンテンツの紹介サイトや、中小規模のコンテンツ事業者のWebサイトなどが見られました。いずれも変わらない傾向です。

全体として、ドライブバイダウンロードの発生率はかなり低い状態にあったものが、仄かに増加しつつあると言える状況です。特に今回多数観測されたNuclearやNeutrinoはOperation Windigo[*42]との関連も指摘されている[*43]ため、攻撃者グループは、比較的大きな潜在力を保持している可能性があります。Webサイト運営者はWebコンテンツの改ざん対策、閲覧者側はブラウザや関連プラグインなど（特にFlash Player）の脆弱性対策を徹底し、注意を継続することを推奨します。




※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-12 Webサイト閲覧時のドライブバイダウンロード発生率（%）（Exploit Kit別）**

＊39 Webクローラによる観測手法については本レポートのVol.22（http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol22.pdf）の「1.4.3 Webクローラによるサイト改ざん調査」で仕組みを紹介している。

＊40 Neutrino Exploit Kitは、2013年10月ごろから国内外で猛威を振るっていたものが徐々に勢力を失い、2014年2月以降は本Webクローラで検知されなくなっていた。一方で、2014年11月には「Neutrino : The come back ! (or Job314 the Alter EK)」（http://malware.dontneedcoffee.com/2014/11/neutrino-come-back.html）にて新バージョンのリリースが報告されている。

＊41 例えば「CVE-2015-0336（Flash up to 16.0.0.305）and Exploit Kits」（http://malware.dontneedcoffee.com/2015/03/cve-2015-0336-flash-up-to-1600305-and.html）では、2015年3月12日に公開された脆弱性について、Nuclearでは3月19日、Neutrinoでは4月2日に悪用が確認されたと報告している。

＊42 ESET社のホワイトペーパー「OPERATION WINDIGO」（http://www.welivesecurity.com/wp-content/uploads/2014/03/operation_windigo.pdf）で公開された大規模な攻撃活動。2011年以降、25,000台以上のサーバが侵害され、スパム送信やクライアントのリダイレクションに悪用されたと報告している。

＊43 Nuclearについては「HAPPY NUCL(Y)EAR - EVOLUTION OF AN EXPLOIT KIT」（http://community.websense.com/blogs/securitylabs/archive/2015/01/15/evolution-of-an-exploit-kit-nuclear-pack.aspx）、Neutrinoについては「Exploit Kit Evolution - Neutrino」（https://isc.sans.edu/diary/Exploit+Kit+Evolution+-+Neutrino/19283）でそれぞれOperation Windigoとの関連が指摘されている。

## 1.4 フォーカスリサーチ

インターネット上で発生するインシデントは、その種類や規模が時々刻々と変化しています。このため、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繋げています。ここでは、これまでに実施した調査のうち、悪質化するPUA、ID管理技術、HDDのファームウェアを再プログラミングするマルウェアのIOCの検討の3つのテーマについて紹介します。

### 1.4.1 悪質化するPUA

PUAはPotentially Unwanted Applicationの略で、ユーザにとってそもそも不必要であったり、全体としては有益であっても一部不適切な機能を有するソフトウェア群の総称です。PUP(Potentially Unwanted Program)とも呼ばれています。ソフトウェアの利用中に広告を強制挿入するアドウェアもPUAの一種として扱われる場合もあります。PUAには、一見正当な機能を提供するだけで無害に見えるものも存在しますが、一部には利用者が気付かないうちに広告などに活用するために行動情報を取得、外部に送信する悪質なものも存在します。また近年、一部にはユーザを騙してPUAをインストールさせ、それを使って情報を盗み出したり、更に追加でPUAを次々とインストールさせたり、Webコンテンツの改ざんやUACを回避して特権昇格するなど、マルウェアと同様の手法を使う悪質なものが増加

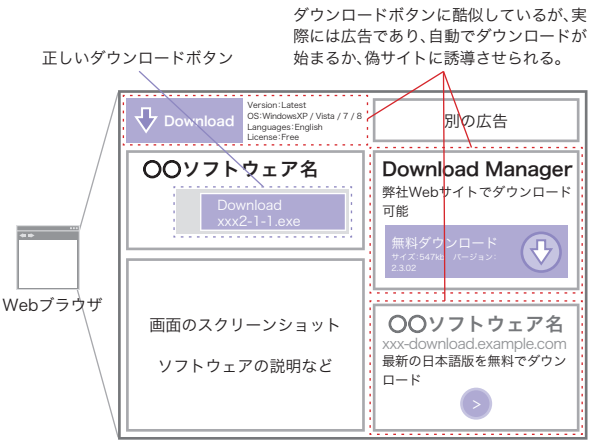



**図-13 ダウンロードサイトに混入した偽ダウンロードボタン(広告)の例**

しています。本稿では、IIJが最近解析した複数のPUAの解析結果から、それらが用いていた手法について解説します。

#### ■ PUAの定義

PUAの厳密な定義は専門家の間でも分かれます。直訳からも分かるとおり、悪性であるかどうかに関わらずユーザにとって不必要な機能を持つプログラムはすべてPUAとなり得るからです。ユーザにとってどのプログラムが不要であるかは個々の考え方や立場、状況、環境などによって異なります。そこで、ここではユーザがインストールを望んだソフトウェアとは関係がないにも関わらず、追加でインストールされてしまう不要なプログラムをすべてPUAと定義し、その中でもマルウェアと同様の手法を使うものを悪質なPUAと呼ぶことにします。

#### ■ 悪質なPUAの例

##### ■ 侵入経路

攻撃者はあらかじめWeb検索エンジンの検索結果をSEO Poisoning[*44]などの手法を使って操作し、ユーザを偽サイトに誘導する手口が多く見られます。例えば、あるソフトウェアをダウンロードしようと検索を行う際、検索キーワードにソフトウェアの名称と共にバージョンや"ダウンロード"などといったキーワードを指定して検索すると、オリジナルの配布サイトよりも上位に偽サイトが表示されてしまうケースが確認されています。また、検索結果と一緒に表示される広告にも偽の配布サイトが混入していることがあります。誘導先の偽サイトは、著名なダウンロードサイトにドメイン名やデザインを似せて作られている場合もあり、偽サイトであると容易には判別できないようになっています。また、いくつかの著名なダウンロードサイトのWebページ内に存在する広告にも、悪質なPUAをダウンロードさせるための偽のダウンロードボタンが混入していました。図-13はダウンロードサイトのデザインの一例です。複数の広告による偽のダウンロードボタンが混入しており、普段からこのWebサイトを使い慣れているユーザ以外、どれが本当のダウンロードボタンであるか気付くことが困難になっていました。更に、著名なダウンロードサイトのいくつかでは、そのサイト専用のダウンロード

*44 SEO(Search Engine Optimization)Poisoningとは、検索エンジンの最適化アルゴリズムを悪用して検索結果を意図的に操作し、自身の用意したページを本来の順番よりも上位に表示させる手法。本来はマーケティング用の手法だが、マルウェア感染などのように利用者に害を与える目的で悪用されることもある。

ツールを利用しており、そのツール経由でユーザがインストールを望むソフトウェアをダウンロードさせます。しかし、一部にはそのツールにPUAが同梱されているケースが存在します。それ以外にも、ダウンロードサイトがソフトウェア作者に個別に同意を取った上でPUAを同梱したインストーラを提供している場合も存在します。

### ■ PUA導入のフレームワーク

ダウンロードさせられたPUAは単一のアドウェアである場合もありますが、一部のケースではダウンローダ型のプログラムになっており、更に複数のPUAをインストールするものが存在しました。ある事例では、追加でダウンロードされるPUAは多岐にわたり、数や種類は時々刻々と変化していたことから、PUAフレームワークの構築者が、依頼元からの要望に応じて利用者のシステムにPUAをインストールして金銭を得るPay-per-install[*45]が行われていると考えられます。

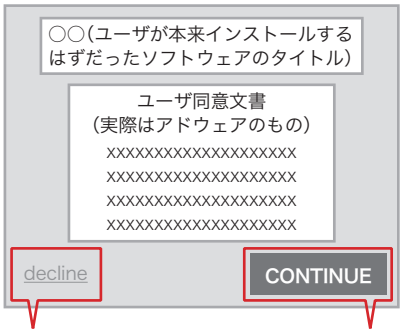
ダウンローダ型のPUAはインストールされると定期的にC&Cサーバと通信をし、自己アップデートや新たなPUAをダウンロードします。また多くの場合、PUAはユーザが本来インストールしようとしていたソフトウェアもインストールするため、ユーザが騙されていることに気付きにくくなっています。

インストーラ形式のPUAの場合、利用者に分かりにくいデザインを悪用して、インストール時にPUAのインストールに関するユーザ同意を取り付けている事例も見受けられます。図-14はあるアドウェアのインストーラデザインの一例です。ユーザがインストールを望んでいるソフトウェアのインストーラに見せかけていますが、利用規約の文章はそれとは別のアドウェアに関するものであり、「CONTINUE」をユーザがクリックすると、裏ではそのアドウェアがインストールされます。ユーザは注意深く見てインストールしない限り、アドウェアのインストールに同意したとみなされてしまいます。

一部のPUAは自分自身のインストールに対する同意を取らずにインストールしていました。このようなPUAを実行してしまった場合では、利用者が提示されるソフトウェアの導入を拒否したとしても、本体はPC上に存在しつづけ、新たなPUAのダウンロードや、自身をアップデートしようとする試みが継続して行われます。また、追加ダウンロードされるPUAも、その一部はユーザに同意を取らずにインストールされていました。

### ■ Webコンテンツの改ざん

PUAの一部にはWebブラウザのプラグインやWebブラウザ拡張として動作、もしくはWebブラウザにPUA自身のコードをインジェクションして送受信用のAPIをフックし、乗っ取ることによってユーザがアクセスしたURLをすべて盗みだし、それに基づいた広告を閲覧中のWebコンテンツ内に挿入して改ざんする手法が採られているものがありました。挿入されるコンテンツの内容は異なるものの、これはZeuS、SpyEyeやvawtrak[*46]のようなBanking




拒否するには**decline**をクリックしなければならないが、小さい文字、分かりづらい単語、グレーアウトしていて押せないように見えるなど、様々な工夫がされている。

**CONTINUE**となっているが、これをクリックした時点でアドウェアがインストールされる。

**図-14 PUAのインストーラのデザイン例**

*45 クリック報酬型アフィリエイトはPay-per-accessとも呼ばれ、クリックさせた広告の量によって報酬が決定する。それと同様に、Pay-per-installはインストールさせたソフトウェアの量で支払われる報酬が決定する。依頼者側は、例えばアフィリエイトサイトに連続してアクセスさせることで金銭を稼ぐアドウェアの作者の場合、より多くのPCにインストールされればそれだけ金銭を稼ぎやすくなるので、このようなフレームワークを持つ組織に依頼を行う。受託側はより多くインストールさせれば、依頼者からより多くの金銭を得られるために、このようなフレームワークが構築されていると考えられる。近年ではマルウェアでもこのモデルが使われているとも言われている。

*46 ZeuSは、本レポートのVol.16(http://www.iij.ad.jp/company/development/report/iir/016.html)の「1.4.3 ZeuSとその亜種について」、SpyEyeは、本レポートのVol.13(http://www.iij.ad.jp/company/development/report/iir/013.html)の「1.4.2 SpyEye」、vawtrakは、本レポートのVol.24(http://www.iij.ad.jp/company/development/report/iir/024/01_04.html)の「1.4.2 国内金融機関の認証情報などを窃取するマルウェア「vawtrak」」でそれぞれ詳しく解説している。また、同様にWebInjectの機能を持つZeuS亜種のCitadelも、本レポートのVol.18(http://www.iij.ad.jp/company/development/report/iir/018.html)の「1.4.2 ZeuSの亜種Citadel」で詳しく解説している。

TrojanによるWebInject[*47]と同様の手法です。このようなタイプの攻撃手法を使うものをWebブラウザハイジャッカーとも呼びます。

この手法以外として、自己署名されたルート証明書をインストールしておき、PUA自身はHTTP(S)のローカルプロキシとして動作してWebブラウザからの通信をすべて自分宛てにねじ曲げ、Webサーバからの証明書を横取りして改ざんし、自身がインストールしたルート証明書で署名を行う手法があります。これにより、MITM[*48]を行って通信を傍受することで、コンテンツに広告などを挿入して改ざんするタイプも発見されています。

どちらの手法とも暗号化されたHTTP通信のコンテンツであってもユーザに気付かれることなく改ざんすることが可能であり、非常に危険な手法です。また、Webブラウザのツールバーとして動作し、アドウェア業者によって提供される検索エンジンを使用することを強制したり、検索キーワードを盗み出すものも存在します。

### ■ Windowsの仕様を悪用

例えばPlugX[*49]やDridex[*50]などのマルウェアはそれぞれ異なる手法を用いてUAC[*51]のポップアップを回避し、自動的に管理者権限を奪取する機能を備えています。今回解析したいくつかのPUAにも、このような特権昇格を行う機能(多くはDridexと同様の方式で特権昇格する)が含まれていました。PUAが管理者権限を奪取するのは、後に複数のPUAを追加ダウンロードした際、ユーザに気付かれずにシステムフォルダにインストールするために必要だからです。

### ■ 難読化

いくつかのPUAは、追加でダウンロードされるPUAが独自の形式で圧縮、もしくは難読化されており、通信路上では実行ファイル形式になっていないため、IDSやIPSなどで検出しにくくなっていました。また、PUA自体にもコードの難読化や重要な文字列の難読化が施されており、特徴として検出することや解析することが困難になっていました。

### ■ Sandbox対策

いくつかのPUAはインストールされた際、スタートアップに登録するだけで終了してしまい、次回PCを再起動するまで実行されないようになっていました。これは動的解析を行って短時間で判定を行うSandbox製品の検出を回避するための行為として、一部のマルウェアが使用していた手法と同様です。インストール直後に手動で実行したりPCの再起動を試みた場合でも、C&Cサーバへの通信は発生するものの、すぐには新たなPUAがサーバからダウンロードされないようになっており、数日から長い場合で数ヵ月経ってから新たなPUAがダウンロードされるようになっていました。これもSandboxによる検出を回避するための手法の1つだと考えられます。

---

*47 Webinjectとは、Webブラウザの通信系APIをフックすることによってブラウザのメモリ上のWebコンテンツを改ざんする機能。ZeuSやSpyEyeなど、Banking Trojan系のマルウェアのほとんどはこのような機能を持ち、感染者が金融機関などにログインする際、二要素認証などの情報を追加で入力させて奪うことで、金銭を窃取しようと試みる。Webinjectは、本レポートのVol.18(http://www.iij.ad.jp/company/development/report/iir/018.html)の「1.4.2 ZeuSの亜種Citadel」や、本レポートのVol.13(http://www.iij.ad.jp/company/development/report/iir/013.html)の「1.4.2 SpyEye」で詳しく解説をしている。

*48 MITM(Man-In-The-Middle)攻撃とは、攻撃者が通信を行う両端の間に割り込んで通信を横取りし、暗号化の解読を行って利用者に気付かれることなく盗聴や改ざんを行う手法。中間者攻撃。

*49 PlugXについては、本レポートのVol.21(http://www.iij.ad.jp/company/development/report/iir/021.html)の「1.4.1 標的型攻撃で利用されるRAT「PlugX」」及び、Black Hat Asia 2014での発表「I Know You Want Me - Unplugging PlugX」(https://www.blackhat.com/docs/asia-14/materials/Haruyama/Asia-14-Haruyama-I-Know-You-Want-Me-Unplugging-PlugX.pdf)で詳しく解説している。その中で、UACの回避による特権昇格についても解説している。

*50 Dridexが用いているUACの回避手法については、JPCERT/CC 分析センターだより「Dridexが用いる新たなUAC回避手法(2015-02-09)」(https://www.jpcert.or.jp/magazine/acreport-uac-bypass.html)で詳しく解説されている。

*51 Windows Vista以降にはUAC(User Account Control、ユーザアカウント制御)と呼ばれる機能がついており、管理者権限を持つアカウントでログインしていても、通常時は重要な権限が無効になっている。プログラムがシステムを変更するような重要な操作を行った場合にユーザに対して許可を求めるポップアップが表示され、許可された場合のみ、権限が付与される。UACには4段階の設定が存在するが、Windows 7以降、マイクロソフト社はユーザの要望により、4段階中、上から2番目のレベルを初期設定にしている(Vistaは最高レベルが初期設定)。このレベルではユーザが操作したものであるとWindowsが判断した場合はUACのポップアップを表示せず、自動昇格が行われる。近年では、マルウェアがこの仕様を悪用し、ユーザが操作したように見せかけた振る舞いをすることで、UACのポップアップを表示させずに管理者権限に自動昇格する攻撃手法が複数確認されている。

### VM検知

多くのマルウェアにも仮想環境やSandboxでの実行を妨害する機能がついていますが、今回解析したPUAにもこのような機能が含まれていました。特に、執筆者がこれまでマルウェア解析を行った際には見ることのなかったHyper-VやXen、KVMなどの仮想環境も検知されるようになっていました。これは、WMI、WBEM[*52]の機能を使い、BIOSの情報などを取得することで判定を行っています。それ以外の手法も組み合わせ、現存するほぼすべての仮想環境を検知できるようになっており、検出すると実行を停止するなど、その挙動を変更するような仕組みが入っています。これも解析妨害の1つです。

### 組織がPUAに感染することのリスク

今回紹介したWebブラウザハイジャッカー型のPUAは、ユーザがアクセスしたWebサイトのURLなどをすべて外部に送信します。組織内でこのようなPUAに感染した場合、イントラネットのサーバ名やURLのパス情報、GETパラメータなどが一緒に漏えいします。これは企業などの組織の内部情報を守る観点では好ましくありません。

更に、PUAフレームワークによって追加でインストールされるプログラムにマルウェアが混入する可能性も考えられます。加えて、近年、広告サイト自体が改ざん[*53]され、ドライブバイダウンロード[*54]によってマルウェアがインストールされるケースもあります。アドウェアが表示した広告を閲覧した際に、悪意のあるWebサイトに誘導されて感染するような可能性がないとも言い切れません。このような事態にならないよう、PUAと言えど組織やユーザにとって不必要なソフトウェアがインストールされないように監視を行い、感染を発見した場合は速やかに対処できるような体制を構築しておくべきでしょう。

### 対策

悪質なPUAに感染しないようにするためには、まずユーザ自身が利用するソフトウェアの公式サイトを普段から把握しておくことでしょう。常に公式サイト、もしくはそこからたどることの可能な正規のミラーサイトのみを利用することで、偽のWebサイトから悪質なPUAをダウンロードすることを防ぐことができます。ダウンロードボタンに模した悪質な広告をクリックしてダウンロードをさせられてしまう可能性もあるため、公式サイトに記載されているハッシュ値と照合することなども、このような手法に騙されることを防ぐ手段の1つとなります[*55]。また、安易に無名な、もしくは出所の分からないソフトウェアをインストールしないように日頃から気をつけるべきです。もしあなたが管理者であれば、ユーザが勝手に任意のソフトウェアをインストールできないように一般ユーザ権限のみを与えることを検討するとよいでしょう。また、ユーザディレクトリ内にインストールするタイプのソフトウェアも存在するため、ソフトウェアの制限ポリシーやAppLockerなどのWindowsの機能を使って、システムディレクトリ内とプログラム置き場以外からのプログラムの実行を禁止することで、勝手にユーザがソフトウェアをダウンロードして使用することを防ぐことができます。

有名なソフトウェアの一部やプレインストールされているソフトウェアであってもインストール、もしくはアップデートの際にPUAをインストールさせようとするものも存在します。説明を読まず、安易に「次へ」ボタンをクリックしないようにしましょう。

また、PCにプリインストールされているソフトウェアにアドウェアが含まれているという事件も発生していることから、PCを調達する際にも注意が必要です。いくつかのメー

＊52 WBEM（Web-Based Enterprise Management）は分散コンピューティングを管理するための技術仕様で、標準化を行う業界団体DMTF（Desktop Management Task Force）によって策定された。WMIはWindows Management Instrumentationの略で、WindowsをWBEMで管理するための実装。WMIによりローカル、もしくはリモートのWindows上の様々な情報（ハードウェア、ソフトウェア、OS、ユーザ、プロセスなどあらゆる情報）を取得したり、状態変更をすることができる。

＊53 攻撃者が広告プラットフォームを改ざんし、そこにExploitを仕掛けて待ち伏せをする攻撃手法をMalvertisingという。MalvertisingはMaliciousとAdvertisingを掛け合わせた造語。広告プラットフォームは複数のWebサイトに対して広告を配信している場合が多く、改ざんさせた場合、Exploitを一斉配信させることが可能であり、攻撃者にとって効率的であるため、近年は度々狙われている。また、攻撃者自身がマルウェアに誘導するために広告を直接配信するケースも存在する。

＊54 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何らかの脆弱性を悪用され、マルウェアに強制感染させられること。閲覧者の使用する端末に脆弱性がある場合は、そのWebコンテンツを閲覧しただけでマルウェア感染してしまう。

＊55 ハッシュ値を用いた確認の重要性は、本レポートのVol.10（http://www.iij.ad.jp/company/development/report/iir/010.html）の「1.4.3 ソフトウェア配布パッケージの改ざん」で詳しく解説している。

カーはプリインストールされているソフトウェアの一覧が明示されているため、PCを選択する際の参考になります。また、一部メーカーの法人向けPCではプリインストールされるソフトウェアを出荷時に外せるようにカスタマイズできるものもあります。このようなPCの調達を検討するのも1つの手段になります。

それ以外にも脆弱性を突かれて強制インストールされる可能性もあることから、マルウェアへの対策と同等のことを行っておくことも必要です[*56]。今回紹介したように、UACを回避しようとWindowsの仕様を悪用する悪質なPUAも存在します。そのため、管理者アカウントでPCを管理している方はUACを最高レベルに引き上げておくことも検討してください。

### 1.4.2 ID管理技術〜利便性と安全性の観点から〜

本稿では前号に引き続き、ID管理(Identity Management)技術について取り上げます。IDを識別子(Identifier)という狭義の意味と捉え、秘密情報であるトークンと公開情報であるクレデンシャルの関係、認証と認可の違い、トークンを用いた認証から各種クレデンシャルの流通、アクセス権限付与までの一連の流れについて解説を行いました。今回はこれらの技術が実際にどのように利用されているかについて、具体的事例を含めて報告します。

#### ■ IDとトークンのバリエーション

前号の報告では、IDを持つエンティティが認証されることで、当該IDに属性情報や認可情報が紐付きされ、IDと紐付けされた情報であるクレデンシャルが発行されるという一連の流れを説明しました。このとき認証時には、そのIDを持つエンティティの確からしさを保証するためにトークンが用いられます。認証はレルム(認証や認可が有効な領域)ごとに行われるため、レルムごとにIDとトークンの組を持つことが一般的です。ここで、IDやトークンとして実際に使われている事例を紹介していきます。

認証に関する業務を行うIdP(Identity Provider)がレルムごとに存在し、ユニークなIDがレルムごとに割り振られます。これはインターネット上のサービスを最初に利用する際に、必要事項を入力する利用登録画面を考えると理解できます。登録時には「ユーザID」などの項目でIDを入力する欄があることに加え、他のユーザとIDが被っていないかチェックを行っています。一方でサービス側がランダムにIDを割り振るケースも存在します。いずれの場合も、利用登録時にはメールアドレスや電話番号などのパーソナルデータも入力することが一般的です。これは、この段階では仮登録に過ぎず、入力されたメールアドレスにメールを、もしくは電話番号にショートメッセージを「チャレンジ」と共に通知し、ユーザに当該チャレンジを入力させることで本人確認を行うためです。仮登録時もしくはチャレンジ入力時には、トークンの一種であるパスワードを入力することが一般的です。このようにしてIDとパスワードの組が登録完了した時点でサービスが利用可能になります。

IDをレルム独自に割り振るのではなくメールアドレスで代用するケースも見られるようになりました。レルム独自にIDを管理するためのコストを削減できるため、またユーザが決めたIDや特にIdPが割り振ったランダムなIDを忘れてしまう事態が発生しなくて済むというメリットがあるためです。レルム独自IDを割り振る場合は、本人確認に利用したメールアドレスや電話番号を再度入力させてIDリマインダやパスワードリセットなどを行うWebページを運用する必要が生じ、サービス側の負担が増えることになります。一方でIDとしてメールアドレスを利用した場合には、リスト型攻撃の対象になりうることに留意する必要があります。これはレルムごとに同じIDを使い回している場合にも同じリスクがあると言えます。もちろんパスワードの使い回しをしないことが根本的な対策になりますが、同じIDで漏えいデータの紐付け・名寄せをされてしまうというリスクも存在します[*57]。また、メールアドレスをIDに利用したためにSNSやショッピングサイトにおいてIDを入

*56 クライアント環境におけるマルウェア感染対策については、本レポートのVol.21(http://www.iij.ad.jp/company/development/report/iir/021.html)の「1.4.1 標的型攻撃で利用されるRAT「PlugX」」末尾で詳しく紹介している。

*57 もちろん、IDによる名寄せに限らず、登録時に入力した氏名や電話番号などの情報から名寄せされる脅威も残る。

力させるリマインダページに知人などのメールアドレスを入力することで、プライベートな情報が漏えいしてしまう事例が過去にありました。これらの状況を受けて、レルム独自IDの発行も行うが、メールアドレスもログイン時のIDとしても利用できるかどうか、ユーザに選択権を与えるといったシステムも見受けられるようになりました。

このようにIDはこれまで公開情報と考えられていましたが、秘匿しておくべき状況もありうると認識される事例も存在します。この問題に対する対策として、基本IDと派生IDという考え方について紹介します。各種ポータルサイトやSNSなどをIdPとして利用する場合には、同じIDとトークンの組で多種多用なサービスを利用するケースが存在します。このとき、サービスに応じて立場を変えたい、同じエンティティによる発言や操作であることを知られたくないというシチュエーションが出てきました。そこではじめに割り振られたIDを基本IDとして、実際にIDを利用する場面ではそれぞれのシチュエーションに応じて異なるIDを派生させるというアイデアが登場しています。これは、前述したようにIDが漏えいすること自体が脅威であるという状況を防ぐ単純な解法にあたります。派生IDによるログインを行う場合、基本IDに紐付けされたトークンを利用しますので、派生IDごとに別々のトークンを管理する煩雑さはなくなります。また、再ログイン時にトークンの再入力は必要なく、派生IDの切り替えのみでサービスに応じて異なる派生IDで立ち振る舞いを行うことができるようになります。注意すべき点は、どの派生IDでログインしているかを確認し忘れて、第三者から見て異なるユーザによる2つのアクティビティが紐付けされるケースが発生する可能性があることです。例えばログイン時に表示されているニックネームなどの情報に留意する必要があるでしょう。

IDを派生させるアイデアと同様に派生トークンという概念を考えることもできます。基本トークンとは別に、派生トークンを基本IDと結びつけることで、基本IDと派生トークンの組を認証に用いる手法になります。この派生トークンを1回使いきりのトークンと考えると、ワンタイムパスワードの亜種と考えることもできます。実際の用途としては、例えばスマートフォンのアプリケーションごとに派生トークンを保存(実際にはトークンそのものではなく、マスターパスワードなどを使って暗号化して格納しているケースも考えられます)させておくケースが考えられます。これはスマートフォンなどのパスワード入力が煩雑な環境においては有用な機能と考えられます。また、もし仮に特定のアプリケーションからのパスワード漏えいが発覚した場合でも、被害を限定させると共に、基本パスワードの変更ではなく派生パスワードの無効化のみで済むというメリットもあります。この観点では、権限委譲を行っていると考えることもでき、派生トークンを使った場合の認可範囲を、基本トークンの認可範囲よりも限定しておくことで、トークン漏えい時の影響を最小限に抑えることができます。

このように、ユーザの利便性(ID忘却)と安全性(ID使い回しやトークン漏えい)とのバランスを考慮した運用が望まれています。更に、この派生ID・派生トークンの概念を拡張させることで、図-15のように、基本IDと基本トークンの両方を使わない認証・認可の仕組みも可能となります。このような方式を利用している実際のシステムは現在見受けられませんが、プライバシー保護に留意しているユーザの将来的なニーズに応じて、こうした新しい使い方が今後実装されるかもしれません。

### ■ ワンタイムパスワードのバリエーション

ここまでIDとトークンの使い方に関するバリエーションを紹介してきました。次にトークンの一種であり、1回ごとに使い捨てるワンタイムパスワードについて解説します。ワンタイムパスワードはこれまで主にインターネットバンキングシステムにおいて利用されており、安全な認証方式と認識されてきました。しかし2015年2月、警視庁により

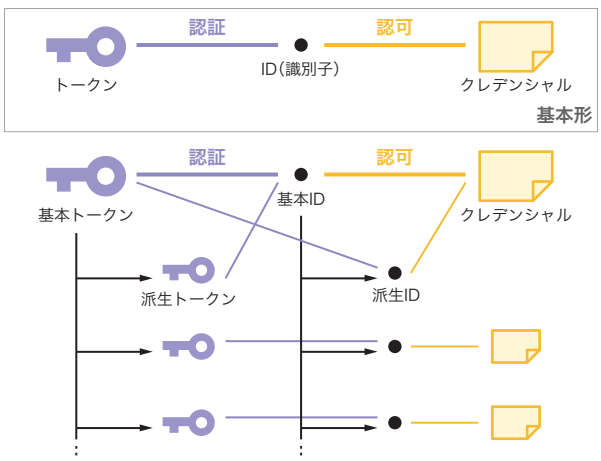



**図-15 派生トークンと派生IDの考え方**

2014年のインターネットバンキングにおいて不正送金の事例が公開され[*58]、被害金融機関数は100を超えるなど被害額も増加傾向にあることが分かりました。特に、送金額が比較的大きな法人口座における攻撃が注目されており、注意喚起がなされています[*59]。法人向けインターネットバンキングの認証において、パスワード単独で利用する方式に加え、X.509証明書によるクライアント認証(Strong Authentication)を使う方式も導入されており、より強固な手段として知られていました。しかし、この電子証明書を利用する場合でもマルウェアに感染したPC・ブラウザなどから自動的に振込が行われるケースが露呈しました[*60]。このようにSSL/TLSクライアント証明書を用いた認証方式でも対策が不十分な状況になっています。

このような背景のもと、インターネットバンキングシステムにおいて認証方式の強化が進められています。従来、用紙やカードに記載された乱数表やワンタイムパスワードを表示するハードウェアデバイスが利用されてきました。後者は、ATMなどでも認証に用いられるパスワードに該当する第一暗証番号(数字4桁の番号)と併用して一時的なパスワードも同時に入力することで認証する方式です。第一暗証番号が漏えいしていたとしても、1回ごとに使い捨てるワンタイムパスワードを利用することで、住所変更や多額の送金など特に重要な処理に関して本人確認を強化することができます。

しかし、Man-in-the-Browser攻撃[*61]や中間者攻撃に代表されるように、バンキングシステムにおけるトランザクションのうち、例えば送信先口座番号や送金額の書き換えが行われてしまうと、使い捨てのワンタイムパスワードを利用していたとしても、不正送金が可能となってしまいます。これは認証方式を強化したとしても、ブラウザなどで表示されている情報だけでは、正しいトランザクションかどうかをユーザ自身が明示的に確認することができず、攻撃者によって実際にはトランザクションを書き換えられている可能性を否定できない問題を示しています。この問題に対して、入力デバイスを備えたハードウェアデバイス利用の移行が進められています。

これまでも複数のバンキングシステムにおいて、認証時にハードウェアデバイスを併用する対策が採られていました。しかし、このハードウェアデバイスは入力インタフェースがなく単なるワンタイムパスワード生成器であったため、取引内容とは関係なく、正しいトークンを保持しているユーザかどうかのみを判定するためにしか利用できませんでした。また企業向けのバンキングシステムでは前述したX.509証明書の利用だけでなく、特定のIPアドレスや特定のPCからのトランザクションしか受け付けないなどの副次的な対策もなされていましたが、ユーザが目にするトランザクション自体を書き換えられている場合も考えられるため、根本的なMan-in-the-Browser攻撃対策を行うことはできません。つまり本人確認を強化しても無駄な対策になっていたわけです。

それに対して2015年に入り、金融機関によりワンタイムパスワードカード利用開始のアナウンスがありました。この新しいハードウェアデバイスは従来のデバイスと異なりテンキーなどの入力インタフェースを持つものであり、本人認証と共に書き換えられているかもしれないトランザクションの正しさも確認できる手法が採用されています。このデバイスは、従来のようにハードウェアデバイスからただ単に出力されるワンタイムパスワードのみを認証時に入力するのではありません。どの口座に入金しようとしているのかをユーザ自らが口座番号を入力することで、口座番号の正しさも保証するワンタイムパスワードをデバイスで生成・表示する機能を持ちます。これにより、攻撃者の意図する口座への入金を防ぐことができますが、他にもこのときはじかれたトランザクションのログを蓄積することで、攻撃者の持つ口座のブラックリストを自動的に形成することができるメリットがあります。また、ユーザ利便性

＊58 警視庁、「平成26年中のインターネットバンキングに係る不正送金事犯の発生状況等について(平成27年2月)」(https://www.npa.go.jp/cyber/pdf/H270212_banking.pdf)。
＊59 IPA、「法人向けインターネットバンキングの不正送金対策、しっかりできていますか？(2014年8月)」(https://www.ipa.go.jp/files/000040703.pdf)。
＊60 トレンドマイクロセキュリティブログ、「法人ネットバンキングを狙う電子証明書窃取攻撃を解析」(http://blog.trendmicro.co.jp/archives/9417)。
＊61 第2回セキュアシステムシンポジウム　高木浩光、渡辺創、「Man-in-the-Browserの脅威と根本的な解決策」(https://www.risec.aist.go.jp/files/events/2014/0313-ja/risec-sympo2014-takagi.pdf)。

を考慮して、入力デバイスを持たない単なるワンタイムパスワード生成器としても利用できます。これはユーザがあらかじめ登録している口座は安全であるという前提のもと、これらの登録済み口座に対する送金においては口座番号の入力を省くという手法です。

現状のこの対策に関して分析してみます。まず1点目は口座番号のみを入力しているため、入金額に関してのトランザクションの正当性を保証することはできません。大多数のユーザが登録している、例えば学校法人の授業料入金口座などの場合、ある特定の短期間にトランザクションの入金額を変更するなどの業務妨害になりかねない攻撃が考えられます。2点目は送金する銀行を指定していない点です。この場合、攻撃対象となる口座に対して、他の銀行の同じ口座番号が攻撃者の管理下にある場合、不正に送金されてしまうリスクがあります。いずれも、口座番号だけをユーザが明示的に確認しているという点が問題になります。トランザクションのうち、例えば入金額や銀行コードなどもユーザが明示的に確認するなど、対策を講じれば講じるほど、ユーザがデバイスに入力するデータが増えることになります。この点については、ユーザがどのくらいトランザクションを書き換えられる可能性を感じているかに応じて、様々な選択肢を与えることが1つの解決策になると考えられます。これはIDとしてメールアドレスを許可するかどうかの選択と同じような考え方に基づきます。この点においても、ユーザの利便性と安全性のバランスを取った運用が望まれています。

更に、FIDO AllianceによるSecond Factor UX[*62]を実装したブラウザも現れました。パスワード入力の代わりに、USBなどのインタフェースを介して小さなハードウェアデバイスを持っていることでパスワード入力を省いて本人認証を行うことができる規格であり、昨年より利用が拡大しています。しかし、実際に利用が広まると以下のような懸念も生まれます。USBフラッシュメモリの持ち運びを禁止する組織があるように、FIDO規格のUSBデバイスの利用が制限される可能性です。そこで、社員証のように居室に入室する際に必ず携帯し、かつ安全に管理することが求められているICカード型のデバイスを併用するなどの製品が今後登場する可能性もあるでしょう。現在、これらの本人認証方式の移行は過渡期にあります。今後、パスワードに代表されるような"Something you know"だけの単体利用ではなく"Something you have"もしくは"Something you are"にカテゴライズされるトークンとの併用が必須となる時期が近づいており、ユーザは重要な通信に対し、多少利便性を損なってでも、強固な本人認証方式を選択できる時代が始まりつつあります。

### 1.4.3 HDDのファームウェアを再プログラミングするマルウェアのIOCの検討

2015年2月16日にKaspersky社はEquation Groupと呼ばれる攻撃グループに関する情報を公開しました[*63]。Equation Groupは「EquationLaser」「EquationDrug」「DoubleFantasy」「TripleFantasy」「Fanny」「GrayFish」といった様々なマルウェアのセットを用いますが、中でもEquationDrugやGrayFishに組み込まれるプラグインの1つである、ハードディスクドライブ(HDD)のファームウェアを再プログラミングするモジュールを利用している点がユニークであると言えます。同社によると、このモジュールの機能により、ファイルシステムの再フォーマットやOSの再インストール後もマルウェアを持続可能にしたり、HDDの中に不可視なデータ領域を生成することができ、マルウェアの検出も削除も困難な状況になると述べています。IIJでは同モジュールの初期動作を解析[*64]して、メモリ上からその存在を検出するためのIndicator of Compromise(IOC)[*65]を検討しました。

#### ■ 初期動作の概要

HDDのファームウェアを再プログラミングするモジュール(以下、nls_933w.dll)は、Platform Orchestratorと呼ばれ

*62 The FIDO Alliance(https://fidoalliance.org/specifications/overview/)。
*63 Kaspersky社の調査分析チーム(GReAT)からEquation Groupに関するレポートが公開されている。"EQUATION GROUP: QUESTIONS AND ANSWERS"(https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf)。
*64 検体のMD5ハッシュ値は11fb08b9126cdb4668b3f5135cf7a6c5。
*65 IOCとはネットワーク上や端末内に残る、マルウェア感染や不正侵入の脅威を示す痕跡のこと。メモリ上のIOCに関しては、本レポートのVol.26(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol26.pdf)の「1.4.2 端末のメモリ内に潜む脅威をスキャンするopenioc_scan」を参照のこと。

るDLL(mscfg32.dll)によってロードされます。ロード後、mscfg32.dllはnls_933w.dllがエクスポートする関数アドレスを複数呼び出し、文字列の難読化解除、mscfg32.dll側の関数アドレスのコピーなどの初期化処理後に、メインの処理を行う関数を実行します。

nls_933w.dllのメインの処理を行う関数では、まずリソースからドライバ(以下、win32m.sys)がロードされます。その後、DeviceIoControl APIを介してwin32m.sysを制御し、モジュールのバージョンの確認、IOリクエストハンドラのクリア・セットなどの初期化処理が行われ、問題がなければATAコマンドを発行するためのIOリクエストのキューイング処理に移ります。

同キューイング処理では、最初にHDDの情報を取得するためのコマンド(IDENTIFY DEVICE)をwin32m.sysに送信します。取得した情報の中から、シリアル番号、ファームウェアリビジョン、モデル番号などを中心にチェックした後、モデル番号に応じて更なるコマンド(INITIALIZE DEVICE PARAMETERS)を送信することもあります。その後、HDDの情報からファームウェアの再プログラミングが可能なターゲットであることが判明した場合、ファームウェアの更新に関するコマンド(DOWNLOAD MICROCODE)を送信します。

### ■ IOCの検討

冒頭に述べたとおり、nls_933w.dllはHDD内からマルウェアの検出も削除も困難な状況を作り出します。しかし、隠されたデータ領域にアクセスするには同DLLのAPIを必要とすることから、少なくともメモリ上には同DLLが存在している必要があります。そこで、上記に述べた初期動作から、同DLL(とそれがロードするドライバ)をメモリイメージ内から検出するためのIOCを検討してみます。

```
; enum win32m_ControlCode
IOCTL_WIN32M_GET_VERSION  = 870021C0h
IOCTL_WIN32M_INIT_IRQL_DPC_SPINLOCK  = 870021C4h ; set IO handlers
IOCTL_WIN32M_CLEAR_IRQL_DPC_SPINLOCK  = 870021C8h ; unset IO handlers
IOCTL_WIN32M_GET_LP_INFO  = 870021CCh
IOCTL_WIN32M_QUEUE_IO_REQUEST  = 870021D0h
IOCTL_WIN32M_SET_PARAMETERS  = 870021D4h
```

**図-16 nls_933w.dllによって用いられるIoControlCode**

最初にnls_933w.dllの検出に特化したIOCを検討します。DLLとドライバ双方で検出可能なIOCとしては、DeviceIoControl APIで指定するIoControlCodeがあります。今回のマルウェアでは図-16のように6つのIoControlCodeが使われており、これらすべてをAND条件でIOCとして定義できます。

また、nls_933w.dll内に存在する、ATAデバイスのレジスタの読み書きに用いる6バイトの構造体から成るバイナリシーケンスを定義することも、nls_933w.dllに特化した検出であれば有効です。この構造体は、レジスタオフセットや書き込むデータなどで構成され、例えばHDDの情報を取得するためのコマンド(IDENTIFY DEVICE)の場合、図-17のように2つの構造体(合計で12バイト)のバイナリシーケンスとしてメモリ上に存在しています。その他にもATAコマンドを含む構造体がモジュールに数多く含まれているので、それらをANDで組み合わせて定義します。一方ドライバの側にはこのような構造体は含まれていませんが、その構造体をパースするコードシーケンスを定義するのも1つの手でしょう。

次に、nls_933w.dllに限らず、同様の動作を行うマルウェアを検出するための汎用的なIOCを検討します。まず思い浮かぶのが、HDDのファームウェアを識別する過程で用いられる、「Maxtor STM」「WDC WD」などのモデル番号ですが、nls_933w.dllの場合それらは難読化されており、難読化解除後の文字列もスタックに積まれるため、事後に有効なメモリ空間内でそれらを見つけることは困難だと言えます。

別の汎用的なIOCとして考えられるのは、ドライバ側で用いられるハードウェアポートもしくはレジスタデータ入出力のためのAPIです。例えば、先程説明したATAデバイスレジスタへの書き込みにはWRITE_PORT_UCHARというAPIが利用されます。これ以外にも読み書きのサイズに

```
g_ATA_0xEC      dd 0            ; field_0_flag
                                ; DATA XREF: fn_ctr_Obj_ATA_0xEC+7↑o
                                ; 0=write, other=read ; length = 0xC
                db 6            ; field_4_reg_offset
                                ; 0=Data(R/W), 1=Error(R) or Features(W
                db 0            ; field_5_data
                dd 0            ; field_0_flag
                                ; 0=write, other=read
                db 7            ; field_4_reg_offset
                                ; 0=Data(R/W), 1=Error(R) or Features(W
                db 0ECh         ; field_5_data
```

**図-17 HDDの情報を取得するためのコマンド(IDENTIFY DEVICE)のための構造体**

応じて同様のAPIをインポートしており、それらをANDで定義することで、nls_933w.dllのみならず同じような機能を持つドライバを検出できる可能性があります。ただし、このような汎用的な定義には誤検出が生じる可能性が大きくなります。32bitのWindows XPとWindows 7の複数のメモリイメージでこの定義での検出を検証したところ、Windows 7の場合、複数のドライバで誤検出が発生します[*66]。よって、前述のAPI群だけでなく、その他の処理に関係するAPI群も定義します。具体的には、図-18のようにIOリクエストのキューイングに関わる処理(スレッドの生成、DPCのキューイング)を追加で定義することで、誤検出を排除できます。

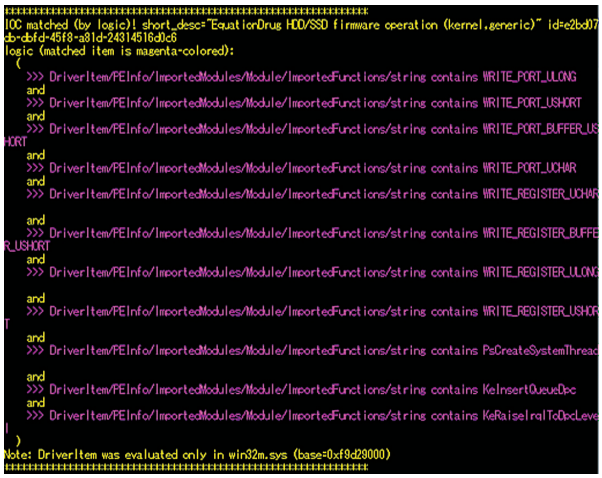



**図-18 利用するAPIに基づく検出**

その他、追加で定義できる汎用的なIOCには、前述のキューイング処理に関連した、カーネルタイマ関数の有無があります。この定義だけでは誤検出の可能性が高いので、前述した利用されるAPI群とANDで定義することを推奨します。

### ■ まとめ

本稿では、HDDのファームウェアを再プログラミングしてデータを隠蔽するマルウェアに対しては、まったく打つ手がないわけではなく、メモリからの検出が有効であることを示しました。今回、このマルウェアに特化して検出するためのIOCと、同様の機能を持つマルウェアを検出するための汎用的なIOCについて検討しましたが[*67]、後者に関して誤検出の少ないものを作るには、十分な解析と検証に基づいた、マルウェアの機能に即した定義が必要になります。よって、対応の緊急度合いに応じて臨機応変にどちらの観点で作るか判断していくと良いと思われます。

## 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、悪質化するPUA、HDDのファームウェアを再プログラミングするマルウェアのIOCの検討について紹介しました。IIJでは、このレポートのようにインシデントとその対応について明らかにして公開していくことで、インターネット利用の危険な側面を伝えるように努力しています。

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、永尾 禎啓、鈴木 博志、梨和 久雄**(1.3 インシデントサーベイ)
**鈴木 博志**(1.4.1 悪質化するPUA)
**須賀 祐治**(1.4.2 ID管理技術〜利便性と安全性の観点から〜)
**春山 敬宏**(1.4.3 HDDのファームウェアを再プログラミングするマルウェアのIOCの検討)
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:
**小林 稔、小林 直、加藤 雅彦、根岸 征史、桃井 康成、平松 弘行**　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

*66 実際には、今回入手した検体はVista以降でUACを有効にしている環境でドライバをロードできるように設計されていない。
*67 今回検討したIOCは以下で公開されている(https://github.com/TakahiroHaruyama/openioc_scan)。