AnonymousによるOpJapan

今回はAnonymousによる日本を対象としたOperationの状況を紹介すると共に、マルウェアFlameと、ZeuSとその亜種について解説を行います。

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2012年4月から6月までの期間では、7月に予定されていたDNS Changerの感染者用の参照DNSサーバの停止にむけて、注意喚起や駆除の努力が行われました。結果として7月9日の停止の際には、大きな混乱もなく、1つのインシデントを終了させることに成功しました。しかし、依然として他のマルウェアの活動は継続しています。また、米国では重要インフラの1つである天然ガスパイプラインへのサイバー攻撃が報告され、Anonymousによる日本の企業や政府関連機関を対象とした活動が複数実施されました。国内においては複数のサーバ事業者で大規模な障害が発生し、可用性の観点から大きな話題となりました。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。

1.2 インシデントサマリ

ここでは、2012年4月から6月までの期間にIIJが取り扱ったインシデントと、その対応を示します。まず、この期間に取り扱ったインシデントの分布を図-1に示します[*1]。

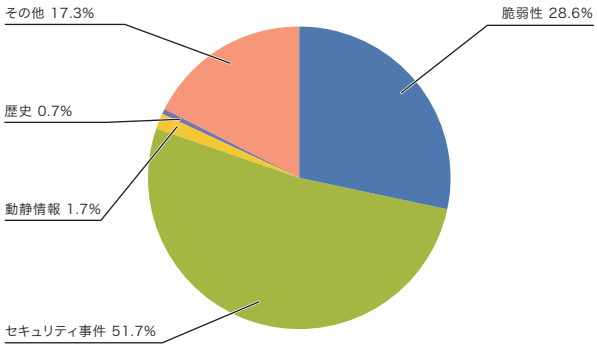

図-1 カテゴリ別比率(2012年4月〜6月)

*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:インターネットやユーザ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。

■ 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。

3月末から活動を開始していたAnonymous Chinaは、4月に入ってから活発に活動を行っており、数百に及ぶ中国国内の政府機関や地方自治体のWebサイトで、改ざんや不正侵入による情報漏えい事件が発生しています。4月には英国で、逮捕された容疑者の米国への引き渡しへの抗議活動として、英国内務省WebサイトへのDDoS攻撃が発生しました。また、同じ時期に首相官邸など複数の英国政府サイトに対する攻撃も発生しています。これ以外にも欧州においてはACTA[*2]への反対活動も活発に行われ、欧州各国の政府関連サイト、関連団体や企業などが攻撃対象となり同時期に米国内では、CISPA法案に対する抗議活動として、支持を表明している防衛企業や通信業界団体などに対するDDoS攻撃が行われました。CISPAに対する抗議活動はその後も継続して行われており、複数の政府機関や企業に対し、不正侵入による情報漏えいやDDoS攻撃などが行われました。この他にも、インドでも政府によるインターネットのフィルタリングに対して複数の政府機関へのDDoS攻撃が発生するなど、政府による規制などを理由とした攻撃が多く発生しています。

グローバル企業を攻撃対象とした活動としては、5月末からコンゴ民主共和国でのレアメタル採掘問題への抗議活動として、OpGreenRightsから派生したOpColtanが行われました。これは、複数の携帯電話製造会社や半導体メーカ、原材料メーカなどが攻撃対象となっており、複数の企業でDDoS攻撃や不正侵入による情報漏えいなどの被害が発生しました。

同じく、グローバル企業を攻撃対象としていたOpNewSonでは、最初に公開された攻撃リストに日本の企業が複数含まれていたため、一部で話題となりました。結果として作戦は失敗に終わり、日本企業が攻撃されることはなく、攻撃自体もそれほど大規模なものとはなりませんでした。また、日本を対象とした活動として、OpJapanも行われました。この活動では、元々日本で活動していたAnonymousによって、ACTAへの抗議デモなどが行われていましたが、海外のAnonymousが参加したことにより、著作権法改正による違法ダウンロードの刑事罰化への抗議活動として、日本の政府機関や著作権団体などを攻撃対象とする活動に変化しました。これにより、複数の政府機関、政党や企業のWebサイトに対して、改ざんやDDoS攻撃などが行われました。これらの事件については、「1.4.1 日本を対象としたAnonymousによる攻撃作戦」も併せてご参照ください。

■ 政府機関などの事件と動き

Anonymous以外の攻撃者による政府機関や関連団体を狙った攻撃も継続しており、マルウェアの送付やWebサイトの改ざん、DDoS攻撃などが引き続き行われています。この期間では内閣府を騙り、マルウェアが添付された電子メールが数多く送信される事件や、情報通信研究機構のWebサイトの一部が不正アクセスにより改ざんされる事件、原子力安全機構で利用している端末にマルウェア感染が見つかるなどの事件が発生しています。

これらの状況を受け、政府の取り組みとして、6月に府省庁などに対するサイバー攻撃に対し、被害拡大防止、復旧、原因調査及び再発防止のための技術的な支援及び助言を行うことを目的として、情報セキュリティ緊急支援チーム（CYMAT）が設置されました。

また、4月21日からAdobe Reader及びAdobe Acrobatで、これまで利用者が個別にインストールする必要があったGPKI認証局[*3]の自己署名証明書の自動配信が行われるようになりました。これを受け、内閣官房情報セキュリティセンターから、「PDFファイルの改ざんによるサイバー攻撃への対策について」が公表されました。この文章では、多くの政府機関において文書の交換や資料の公表に使われているPDFファイルについて、PDFファイルの改ざんによる攻撃への

＊2　模倣品や海賊版の拡散などによる知的財産権の侵害に対し国際的に対処するための協定。詳細については次の外務省の解説ページを参照のこと。「偽造品の取引の防止に関する協定（ACTA）」（http://www.mofa.go.jp/mofaj/gaiko/ipr/acta.html）。

＊3　電子署名の利用に必要な証明書の認証局など日本の行政機関が利用している認証基盤のこと。詳細については次の政府認証基盤の案内ページも参照のこと。「政府認証基盤（GPKI）」（https://www.gpki.go.jp/）。

4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 **3日**：Mozilla Firefoxでセキュリティリスク軽減のため、古いJavaプラグインをブロックリストに追加し、無効化する措置が行われた。
Mozilla Japanブログ、「セキュリティリスクを軽減するため、古いJavaプラグインを強制的に無効化する措置を取りました」(http://mozilla.jp/blog/entry/8013/)。

他 **4日**：総務省より、公衆無線LANサービスを提供している2社に対し、通信の秘密を侵害する事案があったとして再発防止を求める行政指導が行われた。

セ **5日**：4月4日から内閣府のメールアドレスを騙った電子メールが多方面に配信されているとして、内閣府から注意喚起が行われた。
「内閣府を騙った電子メールについて」(http://www.cao.go.jp/press/20120405notice.html)。

セ **9日**：Anonymousにより、CISPAを支持している防衛企業や業界団体のWebサイトへのDDoS攻撃が発生した。
これらの攻撃については、例えば攻撃を受けた米国テレコム協会の発表などを参照のこと。"US Telecom Website Subject of Denial-of-Service Attack" (http://www.ustelecom.org/news/press-release/ustelecom-website-subject-denial-service-attack)。

脆 **10日**：Sambaに細工したRPCのパケットにより任意のコード実行ができる脆弱性(CVE-2012-1182)が見つかり、修正された。
JVN、「JVNDB-2011-005032:SambaのRPC コードジェネレータ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/2011/JVNDB-2011-005032.html)。

セ **10日**：韓国で中央選挙管理委員会のWebサイトを含む複数サイトに対するDDoS攻撃が発生した。

脆 **11日**：Microsoft社は2012年4月のセキュリティ情報を公開し、MS12-027を含む4件の緊急と2件の重要な更新をリリースした。
「2012 年 4 月のセキュリティ情報」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-apr)。

脆 **11日**：Adobe Reader及びAcrobatにサービス停止や任意のコード実行の可能性などの複数の脆弱性が見つかり、修正された。
「APSB12-08:Adobe ReaderおよびAcrobat用セキュリティアップデート公開」(http://www.adobe.com/jp/support/security/bulletins/apsb12-08.html)。

脆 **11日**：Pythonの複数のバージョンでHashDoSの脆弱性(CVE-2012-1150)を含む複数の脆弱性を修正したバージョンがリリースされた。
例えば、Python 3.2.3では次のリリースを参照のこと。"Python 3.2.3"(http://www.python.org/download/releases/3.2.3/)。

セ **11日**：GooglePlay(公式マーケット)で、日本の利用者の個人情報を外部に送信しているアプリが複数確認され、問題となった。
このアプリについての詳細は、例えば次のSymantec社のブログなどで解説されている。「日本のAndroid ユーザーから個人情報を盗み出す "The Movie" マルウェア」(http://www.symantec.com/connect/ja/blogs/android-movie)。

他 **11日**：総務省より、利用者情報の取り扱いに関し、必要な対応などについて検討を行っていた「スマートフォンを経由した利用者情報の取扱いに関するWG」での中間取りまとめの公表が行われた。
「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会『スマートフォンを経由した利用者情報の取扱いに関するWG中間取りまとめ』の公表」(http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000073.html)。

脆 **12日**：Apple社のJava for OS X Lion及びJava for Mac OS X 10.6で、Javaに起因する複数の脆弱性が修正された。
「Java for OS X 2012-003 および Java for Mac OS X 10.6 Update 8 のセキュリティコンテンツについて」(http://support.apple.com/kb/HT5247?viewlocale=ja_JP)。

脆 **13日**：Apple社から、OS X Lion向けにFlashbackマルウェアの除去ツールが提供された。
「Flashback マルウェア除去ツールのセキュリティコンテンツについて」(http://support.apple.com/kb/HT5254?viewlocale=ja_JP)。

動 **13日**：北朝鮮が予告していた衛星打ち上げを行ったが、飛翔体は黄海に墜落し、打ち上げそのものは失敗に終わった。

脆 **18日**：Oracle社はOracleについて四半期ごとの定例アップデートを公開し、複数製品の合計88件の脆弱性を修正した。
"Oracle Critical Patch Update Advisory - April 2012"(http://www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html)。

脆 **19日**：OpenSSLに任意のコード実行が可能な脆弱性を含む複数の脆弱性が発見され修正された。
"OpenSSL Security Advisory [19 Apr 2012]"(https://www.openssl.org/news/secadv_20120419.txt)。

脆 **21日**：WordPressで権限昇格やクロスサイトスクリプティングを許す脆弱性を含む複数の脆弱性が修正された。
「WordPress 3.3.2 (そして WordPress 3.4 ベータ 3)」(http://ja.wordpress.org/2012/04/21/wordpress-3-3-2/)。

他 **25日**：内閣官房情報セキュリティセンターより、PDFファイルに対する脅威に対し、GPKIを使った電子署名の自動配信による改ざん検知など政府機関における取り組みが発表された。
「PDF ファイルの改ざんによるサイバー攻撃への対策について」(http://www.nisc.go.jp/press/pdf/pdf_kaizan_press.pdf)。

セ **25日**：VMware社は、2003年から2004年のVMware ESXのソースコードの一部が漏えいしていたことを公表した。
"VMware Security Note"(http://blogs.vmware.com/security/2012/04/vmware-security-note.html)。

脆 **27日**：Microsoft社のWindows Live Hotmailのパスワード再設定機能に任意のアカウントのパスワードを変更できる脆弱性が見つかり、修正した。
次のMicrosoft Security Response Teamのツイートで修正が報告された(https://twitter.com/msftsecresponse/status/195568235654021121)。

他 **27日**：米国下院で、インターネットでの犯罪行為防止のための個人情報共有などについて定めたCyber Intelligence Sharing and Protection Act (CISPA)が可決された。
U.S Government Printing Office(GPO)、"H.R. 3523 (RFS) - Cyber Intelligence Sharing and Protection Act"(http://www.gpo.gov/fdsys/pkg/BILLS-112hr3523rh/pdf/BILLS-112hr3523rh.pdf)。

他 **30日**：日米首脳会談が行われ、サイバー空間における協力体制の構築などを謳った「日米協力イニシアティブ」が発表された。
詳細については次の外務省のサイトを参照のこと、「日米首脳会談(平成24年4月30日)」(http://www.mofa.go.jp/mofaj/kaidan/s_noda/usa_120429/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

対策として、ソフトウェアを最新のバージョンに更新すること、GPKIによる電子署名による改ざん確認をすることなどを挙げています。

また、特に標的型サイバー攻撃などへの対応において、情報セキュリティ人材が不足しているという状況に対し、情報セキュリティ政策会議の「普及啓発・人材育成専門委員会」における検討結果をまとめた「情報セキュリティ人材育成プログラムを踏まえた2012年度以降の当面の課題等について」が、同じく内閣官房情報セキュリティセンターから公表されています。

■ 脆弱性とその対応

この期間中ではMicrosoft社のWindows[*4]、Internet Explorer[*5][*6]、Word[*7]、Office[*8][*9]、Adobe社 のAdobe Reader及びAcrobat、Adobe FlashPlayer、Oracle社のJavaSEといったアプリケーションで多くの脆弱性が発見され修正されています。また、Apple社のJava for OS X Lion及びJava for Mac OS X 10.6でも修正が行われました。これらの脆弱性のいくつかは修正が行われる前に悪用が確認されています。

サーバアプリケーションでは、データベースサーバとして利用されているOracleで四半期ごとに行われている更新が提供され、複数の脆弱性が修正されています。また、CMSとして利用されるWordPressについても権限の昇格やクロスサイトスクリプティング脆弱性を含む複数の脆弱性が修正されました。DNSサーバのBINDでは、特定のリソースレコードにより、サーバの異常停止などを引き起こす脆弱性が修正されています。また、OpenSSLでも巧妙に細工されたデータを送付することにより、DoS攻撃が可能な脆弱性が修正されました。

■ DNS Changerマルウェアへの対応

DNS Changerマルウェア[*10]については、FBIからの依頼でISCにより運用されていた、感染者用の暫定DNSサーバの停止期限が3月9日から7月9日に延長されていました。このDNSサーバが停止した時点で、感染している人はインターネットが利用できなくなるため、駆除に向けた感染者への対応や注意喚起[*11]が行われてきました。

検索サービスのGoogleやSNSのFacebookでは、感染者がアクセスした場合に警告メッセージを表示する対応を行いました。また、世界各国でDNS Changerマルウェアに感染していないか確認が行えるWebサイトが設置される[*12]など、一般に向けた注意喚起が大規模に行われました。日本では、JPCERTコーディネーションセンターがDNS Changerマルウェア感染確認サイトを公開したり[*13]、テレコム・アイザック推進会議が注意喚起[*14]を行うなどの対応が行われました。

このような取り組みの成果もあり、代替DNSサーバの運用は日本時間の7月9日13時1分をもって停止しましたが、日本や各国で特に大きな混乱は確認されませんでした。

＊4　「マイクロソフト セキュリティ情報 MS12-036 - 緊急 リモート デスクトップの脆弱性により、リモートでコードが実行される (2685939)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-036)。
＊5　「マイクロソフト セキュリティ情報 MS12-023 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (2675157)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-023)。
＊6　「マイクロソフト セキュリティ情報 MS12-037 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム (2699988)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-037)。
＊7　「マイクロソフト セキュリティ情報 MS12-029 - 緊急 Microsoft Word の脆弱性により、リモートでコードが実行される (2680352)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-029)。
＊8　「マイクロソフト セキュリティ情報 MS12-027 - 緊急 Windows コモン コントロールの脆弱性により、リモートでコードが実行される (2664258)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-027)。
＊9　「マイクロソフト セキュリティ情報 MS12-034 - 緊急 Microsoft Office、Windows、.NET Framework、Silverlight 用のセキュリティ更新プログラムの組み合わせ (2681578)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-034)。
＊10　DNS Changerマルウェアについては、IIR Vol.15(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol15.pdf)の「1.4.2 DNS Changerマルウェア」も参照のこと。
＊11　JPCERTコーディネーションセンター、「DNS 設定を書き換えるマルウエア (DNS Changer) 感染に関する注意喚起」(http://www.jpcert.or.jp/at/2012/at120008.html)。
＊12　各国のチェックサイトは次のDCWGで確認できる。"How can you detect if your computer has been violated and infected with DNS Changer?"(http://www.dcwg.org/?page_id=381)。
＊13　JPCERTコーディネーションセンター、「DNS Changer マルウエア感染確認サイト公開のお知らせ」(http://www.jpcert.or.jp/pr/2012/pr120002.html)。
＊14　Telecom-ISAC Japan、「DNS Changer マルウェア感染に関する注意喚起について」(https://www.telecom-isac.jp/news/news20120530.html)。

5月のインシデント

1 セ **1日**：情報通信研究機構のWebサイトの一部が不正アクセスにより改ざんされた。
「情報通信研究機構 Webサイトへの不正アクセスについて」(http://www.nict.go.jp/press/2012/05/01-1.html)。

2
3 脆 **4日**：Adobe Flash Playerに第三者による任意のコード実行が可能な脆弱性を含む複数の脆弱性が見つかり修正された。
「APSB12-09: Adobe Flash Player に関するセキュリティアップデート公開」(http://kb2.adobe.com/jp/cps/936/cpsid_93612.html)。

4 他 **4日**：地方自治体と民間企業のポイントカードを利用した図書館の企画・運営に関する提携が発表され、貸出履歴などの個人情報の取り扱いについて話題となった。

5 他 **7日**：米国ICS-CERTは天然GASパイプラインが攻撃されているとして注意喚起を行った。
この件については、例えば5月に発表されたICS-CERTのMONTHLY MONITORなどで確認できる。"ICS-CERT Monthly Monitor May 2012"(http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Apr2012.pdf)。

6
7 脆 **9日**：Adobe Shockwave Playerに任意のコード実行が可能な複数の脆弱性が見つかり、修正された。
「APSB12-13: Adobe Shockwave Player に関するセキュリティアップデート公開」(http://www.adobe.com/jp/support/security/bulletins/apsb12-13.html)。

8 脆 **9日**：Microsoft社は2012年5月のセキュリティ情報を公開し、MS12-034を含む3件の緊急と4件の重要な更新をリリースした。
「2012 年 5 月のセキュリティ情報」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-may)。

9 セ **9日**：日本を含む世界中のUstreamで、ロシアの市民ジャーナリストの配信チャンネルを狙ったと考えられるDDoS攻撃が発生した。
この事件は次のUstream技術チームのTwitter上でのつぶやきなどで確認できる(https://twitter.com/UstreamTech_JP/status/200161225479430144)。

10 他 **9日**：消費者庁はインターネット上で行われている、いわゆるステルスマーケティングの手法について、景品表示法上の不当表示として問題であるとして「インターネット消費者取引に係る広告表示に関する景品表示法上の問題点及び留意事項」の一部を改定することを公表した。
「『インターネット消費者取引に係る広告表示に関する景品表示法上の問題点及び留意事項』の一部改定について」(http://www.caa.go.jp/representation/pdf/120509premiums_1.pdf)。

11
12 他 **9日**：FBIは、関連団体を通じてホテルのインターネット接続を利用したソフトウェアのアップデートを装ってマルウェアに感染させる事例があるとして注意喚起を行った。
The Internet Crime Complaint Center(IC3)、"MALWARE INSTALLED ON TRAVELERS' LAPTOPS THROUGH SOFTWARE UPDATES ON HOTEL INTERNET CONNECTIONS"(https://www.ic3.gov/media/2012/120508.aspx)。

13
14 セ **11日**：Anonymousにより、インド政府によるインターネット規制への抗議行動(OpIndia)として複数のインド政府機関へのDDoS攻撃が発生した。

15 脆 **15日**：Apple Mac OS XのQuickTimeに、整数オーバーフローの脆弱性による任意のコード実行の可能性がある脆弱性が見つかり修正された。
"About the security content of QuickTime 7.7.2"(http://support.apple.com/kb/HT5261?viewlocale=ja_JP)。

16 脆 **16日**：ロジテック社製無線LANブロードバンドルータの製品の一部で外部から接続IDやパスワードが取得される脆弱性が公表された。
この件については次のロジテック社の発表を参照のこと。「ロジテック製300Mbps無線LANブロードバンドルータ(LAN-W300N/R、LAN-W300N/RS、LAN-W300N/RU2) に関するお詫びとお願い」(http://www.logitec.co.jp/info/2012/0516.html)。

17 セ **16日**：Anonymousの一派であるTheWikiBoatによるOperation NewSonが5/26に攻撃を行うことが予告され、複数の日本企業がターゲットとなっていることが話題となった。
4月11日に最初に予告された内容は次のとおり。PASTEBIN、"Operation NewSon (OpNewSon) #TheWikiBoat"(http://pastebin.com/wq6KdgDg)。

18
19 他 **17日**：総務省にて、「IPv6によるインターネットの利用高度化に関する研究会」の第18回会合が行われ、日本のインターネット環境下でのIPv6フォールバック問題などが話題となった。
総務省、「IPv6によるインターネットの利用高度化に関する研究会」(http://www.soumu.go.jp/main_sosiki/joho_tsusin/policyreports/chousa/ipv6_internet/index.html)。

20
21 セ **18日**：4月に発生した不審なAndroidアプリが複数見つかった事件で、警視庁が不正指令電磁的記録供用容疑で、東京都内のIT関連会社などを家宅捜索していたと報道された。

22
23 他 **18日**：消費者庁はSNSで提供されているゲームのアイテム販売の手法について見解をまとめ、景品表示法に基づく懸賞商品制限告示第5項で禁止されている「カード合わせ」に該当するとの判断を示した。
「『カード合わせ』に関する景品表示法(景品規制)上の考え方の公表及び景品表示法の運用基準の改正に関するパブリックコメントについて」(http://www.caa.go.jp/representation/pdf/120518premiums_1.pdf)。

24
25 セ **23日**：Google社はDNS Changerの感染が疑われる利用者に対し、注意喚起の表示を始めた。
Google Online Security Blog、"Notifying users affected by the DNSChanger malware"(http://googleonlinesecurity.blogspot.jp/2012/05/notifying-users-affected-by-dnschanger.html)。

26
27 他 **23日**：独立行政法人情報処理推進機構より、なりすましメールへの対策としてSPF(Sender Policy Framework)導入についての手引きが公表された。
「なりすましメール撲滅に向けたSPF(Sender Policy Framework)導入の手引き」(http://www.ipa.go.jp/security/topics/20120523_spf.html)。

28 セ **26日**：Anonymousの一派であるTheWikiBoatによるOperation NewSonが実施されたが失敗に終わった。

29 セ **29日**：ネットワークトラフィックの傍受やキー入力の不正送信といった複数の機能を持った高度なマルウェア、Flameが発見された。
このマルウェアに関しては、例えば次のKaspersky Lab社のSECURELIST Blogなどに詳しい。"The Flame: Questions and Answers"(http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers)。

30
31 他 **31日**：米国政府の後援を受けた民間団体であるIndustry Botnet Group(IBG)は、ボットネットの影響を軽減するための自主的な9原則を発表した。
"Principles for Voluntary Efforts to Reduce the Impact of Botnets in Cyberspace"(http://www.industrybotnetgroup.org/principles/)。

[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

■ 国内クラウドサービスなどにおける障害とその影響

この期間では、複数のレンタルサーバ事業者で発生した不具合や障害が問題となりました。あるレンタルサーバで提供されていたDNSサービスでは、既に登録されているドメインのサブドメインを同じサービスを利用している他者が登録できる状態となっていたため、悪意のある第三者がドメインの一部を乗っとることができる不具合が見つかり、修正されました。

また、別のレンタルサーバ事業者では、メンテナンス作業を行った際の不具合により、ファイルを消失させてしまう障害が発生し、約5,700顧客に影響が出ました。この障害では、データのバックアップが適切に行われていなかったため、大部分のデータの復旧ができないことが判明しました。また、復旧されたデータにも別の問題が発生したことから、データの復旧は行わないとの発表がなされました。

これらの事件を受け、クラウドサービスやホスティングなどのサービス利用については、バックアップを取ったり、データや処理を複数の事業者に分散するなど、事業継続性の観点からその利用の仕方を見直す声が挙がっています。

■ スマートフォンを取り巻く状況

スマートフォンの普及により、公衆無線LAN環境の整備が急速に進められていますが、それに伴い、様々な問題が発生しています。コンビニエンスストアの公衆無線LANサービスを提供する事業者が、特定のECサイトに接続できないように設定して運用していたことが判明しました。また、別の事業者が提供する公衆無線LANサービスでは、利用者に無断で端末のMACアドレスや特定のSNSアカウントIDを記録・保存していたことが判明しました。いずれの事業者も問題点については既に是正を行っていましたが、電気通信事業法第4条に規定されている「通信の秘密」の侵害に当たるとして、総務省より行政指導を受けました。

また、スマートフォンに対するウイルスやマルウェアなどの脅威も大きくなっています。この期間では、公式マーケットであるGoogle Playに公開されていたAndroidアプリに、日本の利用者をターゲットとした不審なアプリが複数見つかり、話題となりました。これらのアプリは、有名アプリに関連しているような名前が付けられており、インストールする際に、ネットワーク通信や個人情報に関するデータの読み取りなど、必要以上のパーミッションを要求してきます。起動すると動画などを再生しますが、そのバックグラウンドで、インストールした端末の電話番号や、連絡先に登録されている個人情報を外部のサーバに送信していました。これらのアプリは問題が指摘された後に公式マーケットから削除されましたが、数百万人分の個人情報が流出した可能性が指摘されています。この事件については、警視庁が不正指令電磁的記録供用容疑で、東京都内のIT関連会社などを家宅捜索しています。また、このようなアプリは、公式マーケットではない場所でも確認されており、IPAから注意喚起が行われています[*15]。

■ 著作権法改正とサイバー犯罪条約への批准

著作権法の一部を改正する法律が6月20日、参議院本会議で可決・成立しました。この改正では、DVDリッピングの違法化や違法ダウンロード行為に対する刑罰化が加えられるなどの修正が行われています。違法ダウンロード刑罰化に関する規定については、本年10月1日から施行されます。

また、サイバー犯罪に関する条約（サイバー犯罪条約）[*16]について、6月26日の閣議で条約の批准が決定されました。この条約は2001年に署名されていたものの、国内の法整備が整っていなかったことから、批准が遅れていましたが、昨年の刑法改正などにより条件が整いました[*17]。7月3日に受諾書が欧州評議会に寄託[*18]されたことから、本年11月1日より効力が発生することになりました。

＊15 独立行政法人情報処理推進機構、「Android OSを標的とした不審なアプリに関する注意喚起」（http://www.ipa.go.jp/security/topics/alert20120523.html）。
＊16 本条約については、外務省が日本語版を公開している。「サイバー犯罪に関する条約（略称：日・サイバー犯罪条約）」（http://www.mofa.go.jp/mofaj/gaiko/treaty/treaty159_4.html）。
＊17 日本国内におけるインターネット関連の法整備については、IIR Vol.15（http://www.iij.ad.jp/development/iir/pdf/iir_vol15.pdf）の「1.4.1 不正アクセス禁止法改正について」で紹介している。
＊18 外務省、「『サイバー犯罪に関する条約』の受諾書の寄託」（http://www.mofa.go.jp/mofaj/press/release/24/7/0704_01.html）。

6月のインシデント

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30

脆 **4日**：Microsoft社はマイクロソフト認証機関の承認されていないデジタル証明書を使用した攻撃が行われていることを確認したとして、中間CA証明書を失効させるアップデートを提供した。
「マイクロソフト セキュリティ アドバイザリ (2718704) 承認されていないデジタル証明書により、なりすましが行われる」(http://technet.microsoft.com/ja-jp/security/advisory/2718704)。

脆 **5日**：BIND 9にサーバの停止などが可能な脆弱性(CVE-2012-1667)が見つかり、修正された。
Internet Systems Consortium、「長さ0のrdataによってnamedが異常停止する」(http://www.isc.org/advisories/cve-2012-1667-jp)。

セ **5日**：Facebookは、DNS Changer感染者に対し注意喚起を表示することを開始した。
この件については次のFacebook Securityのページで確認できる。"Notifying DNSChanger Victims"(https://www.facebook.com/notes/facebook-security/notifying-dnschanger-victims/10150833689760766)。

他 **6日**：恒久的にIPv6を有効にする取り組みであるWorld IPv6 Launchが、世界的なWebサービス事業者やISPも参加して実施された。
JAIPA、「World IPv6 Launch についてのご案内」(http://www.jaipa.or.jp/ipv6launch/index.html)。

他 **6日**：Google社は、標的型攻撃による被害が疑われるアカウントに対し、警告を表示することを開始した。
Google Online Security Blog、"Security warnings for suspected state-sponsored attacks"(http://googleonlinesecurity.blogspot.jp/2012/06/security-warnings-for-suspected-state.html)。

セ **7日**：LinkedInで、会員約650万件分のSHA-1パスワードハッシュが流出する大規模な漏えい事件が発生した。
この事件については次のLinkedIn Blogを参照のこと。"An Update on LinkedIn Member Passwords Compromised"(http://blog.linkedin.com/2012/06/06/linkedin-member-passwords-compromised/)。

セ **7日**：JPCERT/CCは、複数ISPでメールアカウントの乗っ取り被害が発生しているとして、メールアカウント不正使用に関する情報提供を呼びかけた。
「メールアカウント不正使用に関する情報提供のお願い」(http://www.jpcert.or.jp/pr/2012/pr120003.html)。

セ **8日**：改正不正アクセス禁止法の初の適用として、オンラインゲームのサーバに不正アクセスし、取得した利用者のIDやパスワードをネット掲示板に書き込んだとして少年が逮捕された。

脆 **9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。
「APSB12-14: Adobe Flash Player に関するセキュリティアップデート公開」(http://kb2.adobe.com/jp/cps/937/cpsid_93754.html)。

脆 **13日**：Microsoft社は2012年6月のセキュリティ情報を公開し、MS12-037を含む3件の緊急と4件の重要な更新をリリースした。
「2012 年 6 月のセキュリティ情報」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-jun)。

脆 **13日**：Oracle社はJavaSEに関する定例アップデートを公開し、合計14件の脆弱性を修正した。
"Oracle Java SE Critical Patch Update Advisory - June 2012"(http://www.oracle.com/technetwork/topics/security/javacpujun2012-1515912.html)。

脆 **13日**：Microsoft社はInternet Explorerにリモートから任意のコード実行の可能性がある脆弱性(CVE-2012-1889)についてアドバイザリと暫定対応であるFixItを公表した。本脆弱性は7月11日に公開された次のセキュリティ情報で修正が行われた。
「マイクロソフト セキュリティ情報 MS12-043 - 緊急 XML コア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 (2722479)」(http://technet.microsoft.com/ja-jp/security/bulletin/ms12-043)。

脆 **13日**：事業者の提供しているDNSサービスで、悪意のある第三者がドメインの一部を乗っとることのできる脆弱性が見つかり、修正が行われた。
この件に関してはその後、JPRSから注意喚起が行われた。「サービス運用上の問題に起因するドメイン名ハイジャックの危険性について」(http://jprs.jp/tech/security/2012-06-22-shared-authoritative-dns-server.html)。

セ **19日**：6月に修正されたMicrosoft社の脆弱性(MS12-037)を悪用した攻撃が発生しているとの報告がされた。
例えば次のIBM社のTokyo SOC Reportなどを参照のこと。「Internet Explorerの脆弱性(MS12-037:CVE-2012-1875)を悪用する攻撃を確認」(https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/ms12-037_20120619?lang=ja)。

他 **20日**：違法ダウンロードの刑事罰化を含む「著作権法の一部を改正する法律」が可決成立した。
文化庁、「平成24年通常国会　著作権法改正等について」(http://www.bunka.go.jp/chosakuken/24_houkaisei.html)。

セ **20日**：レンタルサーバ事業者の提供するサービスで障害が発生し、約5,700顧客に及ぶホームページやメールなどのデータが消失した。

セ **22日**：Internet Explorerの未修正の脆弱性(CVE-2012-1889)を悪用した攻撃が発生しているとの報告がされた。
例えば、次のSymantec社の日本語版セキュリティレスポンスブログなどを参照のこと。「狙われる CVE-2012-1889」(http://www.symantec.com/connect/blogs/cve-2012-1889)。

セ **26日**：AnonymousによるOpJapanが実施され、日本の政府機関や関連組織へのWeb改ざんやDDoS攻撃が複数発生した。

セ **28日**：地方公共団体のホームページに対するDoS攻撃が発生した。また関連して、Webのメールフォームにより1万通以上のメールが送りつけられる事件が発生した。

セ **29日**：総務省より「スマートフォン・クラウドセキュリティ研究会」の最終報告が公表された。
総務省、「スマートフォンを安心して利用するために実施されるべき方策『スマートフォン・クラウドセキュリティ研究会』の最終報告の公表」(http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000020.html)。

他 **29日**：内閣官房情報セキュリティセンターから、政府の取り組みとして府省庁の壁を越えて連携し機動的な支援を行う情報セキュリティ緊急支援チーム(CYMAT)を設置されたことが発表された。
内閣官房情報セキュリティセンター、「情報セキュリティ緊急支援チーム(CYMAT)設置について」(http://www.nisc.go.jp/press/pdf/cymat_press.pdf)。

セ **29日**：6月20日に発生したレンタルサーバ事業者の大規模な障害の復旧作業の際に、複数顧客の情報が混在したデータを復元したことによる情報漏えいが発生していたことが公表された。

[凡例]　脆 脆弱性　セ セキュリティ事件　動 動静情報　歴 歴史　他 その他

※日付は日本標準時

■ Flameマルウェア

5月にはイランでFlameと呼ばれるマルウェアが発見されました。これは中東地域を中心に感染が広まったと考えられ、機能ごとにモジュールが多数存在することや、20MBとマルウェアとしてはサイズが非常に大きいことから、すべての解析には数年かかるとされています。

更に、感染手法としてUSBメモリなどのリムーバブルディスクや、いくつかの既知の脆弱性を利用して感染するだけでなく、偽装した証明書を使い、Windows Updateの仕組みに中間者攻撃を行うことで、ローカルネットワーク上の他の端末に感染させる機能が確認されています[*19]。Microsoft社では、この問題の対処のため、偽装される可能性のある中間CA証明書を失効させる修正[*20]を公開しました。この事件については「1.4.2 Windows Updateへの中間者攻撃を行うマルウェアFlame」も併せてご参照ください。

■ 利用履歴と個人情報の取り扱い

この期間では、電子マネーに使われているICカードやポイントカードなどの利用履歴といった情報の取り扱いについて話題となりました。

あるコンビニエンスストアで提供されている無線LANサービスでは、利用時にポイントカードの番号を認証の一部として利用していましたが、その際に携帯電話の個体識別番号の情報を不適切に送信していたことなど、複数の問題が指摘され、修正が行われました。また、地方公共団体が民間企業と提携して図書館の利用カードとして民間企業のポイントカードを採用することを発表した件については、図書の貸し出し履歴などの情報を民間企業が利用することについて、問題点が指摘されました。更に、利用者のICカード乗車券の乗車履歴を鉄道会社社員が不正に閲覧していた事件が発生するなど、利用者情報の取り扱いが問題となる事件が発生しました。

日常的に蓄積されるこれらの情報については、個人を特定することができる情報であるだけでなく、利用者個人のプライバシーや思想を知ることができてしまうかもしれない機微な情報です。このため、慎重な取り扱いが求められています。

■ その他の動向

その他の動向としてはISP、ネットワーク機器メーカ、世界中のWebサービス事業者がIPv6を恒久的に有効にしてIPv6の展開を推進する取り組みである、World IPv6 Launchが行われました。また、総務省の「IPv6によるインターネットの利用高度化に関する研究会」では、フレッツ光サービスで発生するIPv6-IPv4フォールバック問題が議題となりました。この中ではGoogle社がIPv6の利用に問題があるネットワークのDNSサーバのリストを作成し[*21]、このネットワークからの利用についてはIPv6の利用を無効化する方針を明らかにしています。

また、JPCERTコーディネーションセンターでは、複数のISPでユーザのメールサービスのアカウント情報が何らかの方法で窃取され、その情報を使用したSPAMメールの大量送信が発生しているとして、メールアカウント情報の入手経路に関する情報提供を呼びかけました。ユーザのメールアカウント情報が第三者に不正に利用される事例については、Telecom-ISAC Japanでも2011年8月以降に急増している[*22]として注意喚起が行われています。

---

*19 Windows Updateを利用した感染機能については、例えば次のSymantec Official Blogなどに詳しい。「W32.Flamer: Windows Update を利用する中間者攻撃」(http://www.symantec.com/connect/blogs/w32flamer-windows-update)。

*20 「マイクロソフト セキュリティ アドバイザリ (2718704) 承認されていないデジタル証明書により、なりすましが行われる」(http://technet.microsoft.com/ja-jp/security/advisory/2718704)。

*21 Google社が作成したリストは次で確認できる。"Resolvers to which Google may not return AAAA records." (http://www.google.com/intl/en_ALL/ipv6/statistics/data/no_aaaa.txt)。

*22 Telecom-ISAC Japan、「認証情報を不正に利用したスパムメールの送信について」(https://www.telecom-isac.jp/news/news20111205.html)。

1.3 インシデントサーベイ

1.3.1 DDoS攻撃

現在、一般の企業のサーバに対するDDoS攻撃が、日常的に発生するようになっており、その内容は、状況により多岐にわたります。しかし、攻撃の多くは、脆弱性などの高度な知識を利用したものではなく、多量の通信を発生させて通信回線を埋めたり、サーバの処理を過負荷にしたりすることでサービスの妨害を狙ったものです。

■ 直接観測による状況

図-2に、2012年4月から6月の期間にIIJ DDoS対策サービスで取り扱ったDDoS攻撃の状況を示します。ここでは、IIJ DDoS対策サービスの基準で攻撃と判定した通信異常の件数を示しています。IIJでは、ここに示す以外のDDoS攻撃にも対処していますが、正確な攻撃の実態を把握することが困難なため、この集計からは除外しています。DDoS攻撃には多くの攻撃手法が存在し、攻撃対象となった環境の規模(回線容量やサーバの性能)によって、その影響度合が異なります。図-2では、DDoS攻撃全体を、回線容量に対する攻撃[*23]、サーバに対する攻撃[*24]、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、799件のDDoS攻撃に対処しました。1日あたりの対処件数は8.8件で、平均発生件数は前回のレポート期間と比べて倍増しています。DDoS攻撃全体に占める割合は、回線容量に対する攻撃が0.0%、サーバに対する攻撃が75.9%、複合攻撃が24.1%でした。

今回の対象期間で観測された中で最も大規模な攻撃は、複合攻撃に分類したもので、最大8万5000ppsのパケットによって672Mbps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67.2%が攻撃開始から30分未満で終了し、24.0%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8.8%ありました。今回もっとも長く継続した攻撃は、サーバに対する攻撃と複合攻撃に分類されるもので4日間と1時間22分(97時間22分)にわたりました。また、この期間中、IIJ DDoS対策サービス以外においては、最大1.97Gbpsや38.7万ppsといった攻撃が発生しています。

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[*25]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[*26]の利用によるものと考えられます。

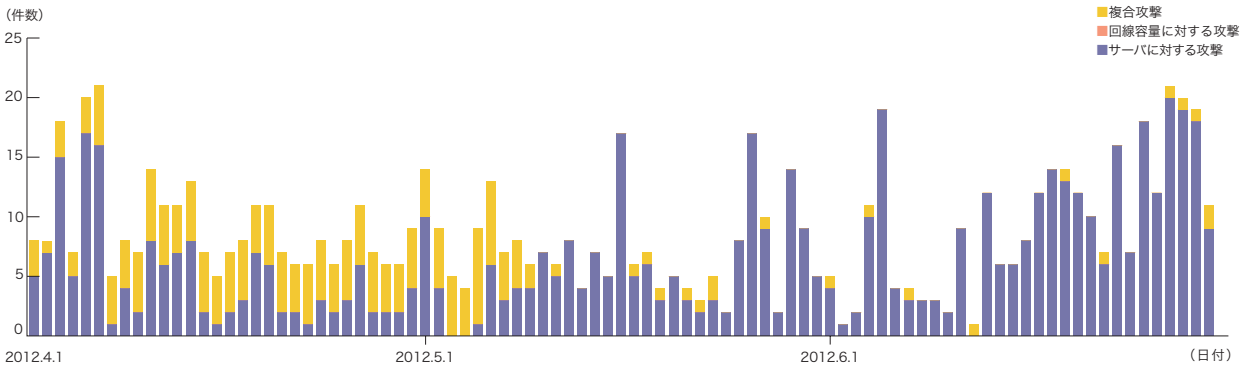

図-2 DDoS攻撃の発生件数

*23 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。

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

*25 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。

*26 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[*27]によるDDoS攻撃のbackscatter観測結果を示します[*28]。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。

2012年4月から6月の期間中に観測したbackscatterについて、発信元IPアドレスの国別分類を図-3に、ポート別のパケット数推移を図-4にそれぞれ示します。観測されたDDoS攻撃の対象ポートのうち最も多かったものは、Webサービスで利用される80/TCPで、対象期間における全パケット数の59%を占めています。また、SSHで利用されている22/TCPやリモートデスクトップで利用される3389/TCP、HTTPSで利用されている443/TCPなどへの攻撃も観測されています。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、米国37.4%、中国22.8%が比較的大きな割合を占めており、以下その他の国々が続いています。

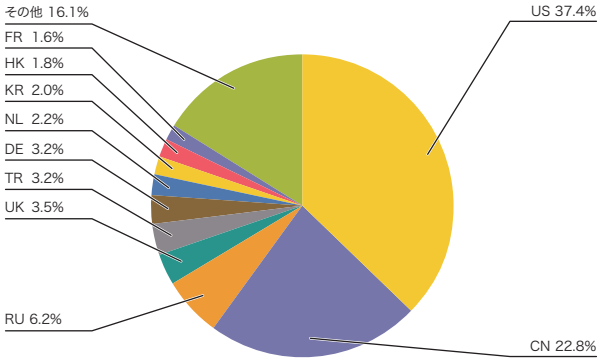

図-3 backscatter観測によるDDoS攻撃対象の分布（国別分布、全期間）

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、4月7日に米国内にある複数のホスティング事業者の攻撃が観測されています。4月21日には、中国国内の複数のWebサーバ、4月24日には米国内にあるファイル共有サイトのWebサーバ、5月12日には中国国内の別のWebサーバへの攻撃を観測しています。5月17日にも多くのbackscatterを観測していますが、これは別の米国内のホスティング事業者に対する攻撃でした。

5月29日や5月31日、6月4日にWebサーバ(443/TCP)への攻撃が多く発生していますが、これらの攻撃は英国のDDoS対策サービス事業者のサーバに対する攻撃でした。

4月28日と4月30日前後には、米国内のサーバに対する20480/TCPへの攻撃を観測しています。5月13日から5月15日にかけては、ロシア国内と中国国内のサーバに対する7777/TCPへの攻撃を観測しました。この攻撃はある範囲のIPアドレスに対して一定数行われていました。7777/TCPへの攻撃については、5月27日にもロシア国内のサー

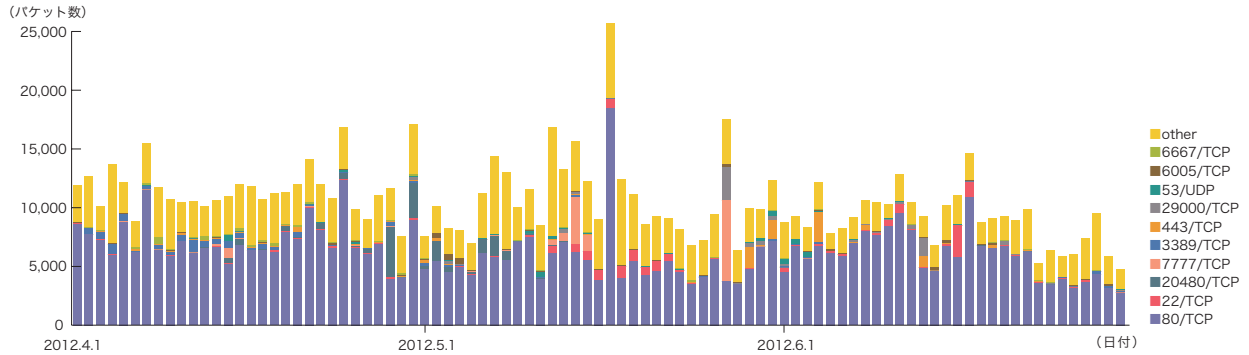

図-4 DDoS攻撃によるbackscatter観測(観測パケット数、ポート別推移)

*27 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。

*28 この観測手法については、IIR Vol.8(http://www.iij.ad.jp/company/development/report/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。

バへの攻撃を観測していますが、こちらは特定のサーバに対する攻撃でした。同じ日には、中国国内のサーバに対する29000/TCPの攻撃も観測しています。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、4月から発生したAnonymousによる英国政府サイトに対する攻撃、同じく4月から発生したUGNaziによると考えられる米国政府サイトや地方政府サイトへの攻撃、5月に発生した、Anonymous ATeamによると考えられるNATOサイトへの攻撃、6月に発生したAnonymousによるOpColtanと考えられる攻撃によるbackscatterをそれぞれ検知しています。

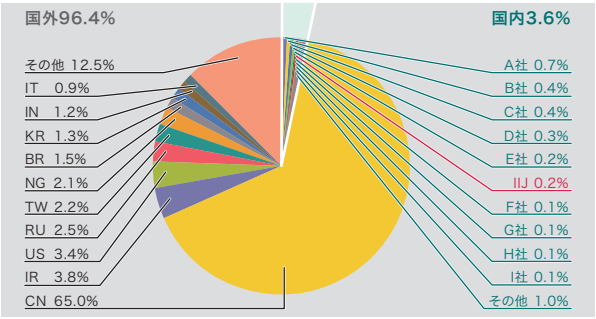

図-5 発信元の分布(国別分類、全期間)

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[*29]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[*30]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

2012年4月から6月の期間中に、ハニーポットに到着した通信の発信元IPアドレスの国別分類を図-5に、その総量(到着パケット数)の推移を図-6に、それぞれ示します。

MITFでは、数多くのハニーポットを用いて観測を行っていますが、ここでは1台あたりの平均を取り、到着したパケットの種類(上位10種類)ごとに推移を示しています。また、この観測では、MSRPCへの攻撃のような特定のポートに複数回の接続を伴う攻撃は、複数のTCP接続を1回の攻撃と数えるように補正しています。

ハニーポットに到着した通信の多くは、Microsoft社のOSで利用されているTCPポートに対する探索行為でした。また、同社のSQL Serverで利用される1433/TCPやWindowsのリモートログイン機能である、RDPで利用される3389/TCP、SSHで利用される22/TCP、telnetで利

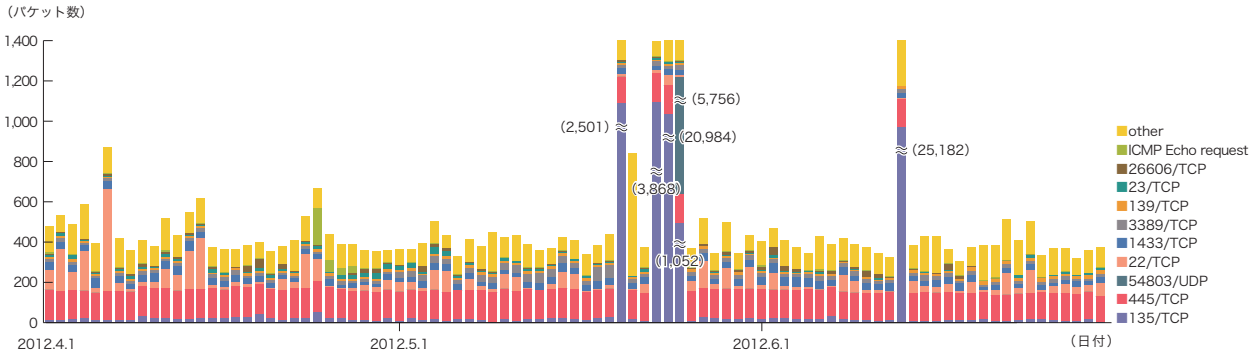

図-6 ハニーポットに到着した通信の推移(日別・宛先ポート別・1台あたり)

*29 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。

*30 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。

用される23/TCPに対する探索行為も観測されています。これらに加えて、26606/TCPなど、一般的なアプリケーションでは利用されない、目的が不明な通信も観測されました。また、54803/UDPの通信が5月25日に急増していますが、これについて多数の送信元から特定のハニーポットに対して数時間の間に集中的に到着したもので、その目的は不明です。送信元のIPアドレスの83.4%はイランに割り当てられたIPアドレスでした。図-5で発信元の国別分類を見ると、中国の65.0%、イランの3.8%と日本国内の3.6%が比較的大きな割合を占めています。

期間中、135/TCPが5月20日、5月23日から5月25日の間と6月13日に急増しました。これらはそれぞれ中国に割り当てられた2つのIPアドレス（ネットワークアドレスは共通）から大量の通信が行われたものです。また、SSHの辞書攻撃と思われる通信も発生しており、例えば4月6日は中国、韓国、イスラエルの各1つのIPアドレスからそれぞれ集中的に通信が発生しています。

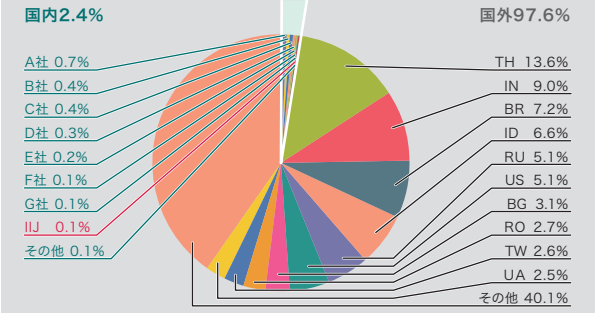

図-7 検体取得元の分布（国別分類、全期間、Conficker除く）

■ 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

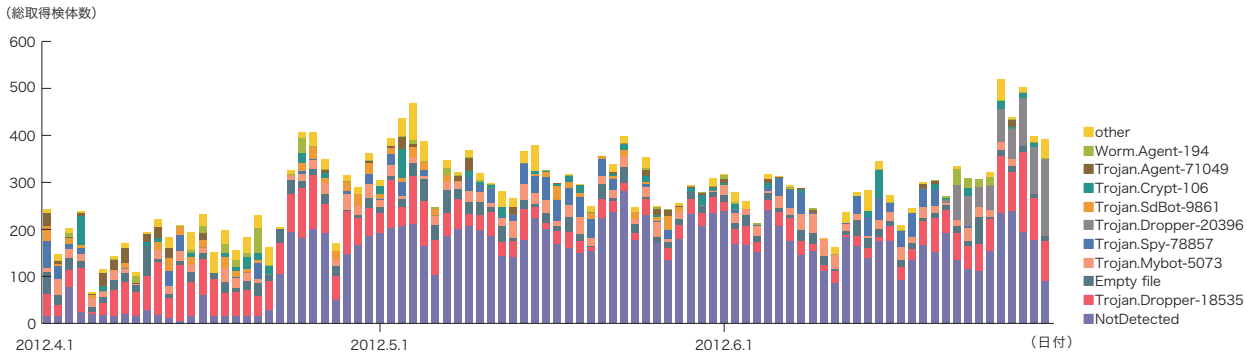

図-8 総取得検体数の推移（Conficer除く）

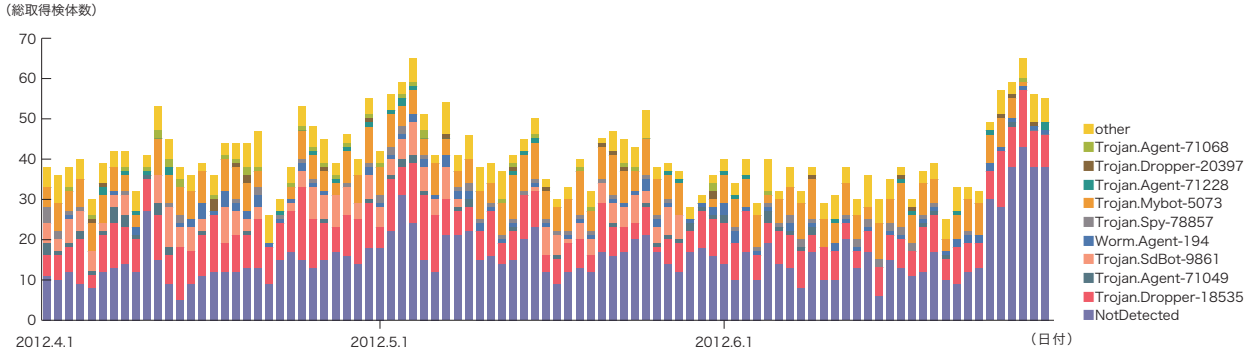

図-9 ユニーク検体数の推移（Conficer除く）

図-8と図-9では、1日あたりに取得した検体[*31]の総数を総取得検体数、検体の種類をハッシュ値[*32]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283、ユニーク検体数が41でした。前号より総取得検体数が倍増していますが、これは前号では一部の期間しか出ていなかった、タイ及びインドネシアからの未検出の検体取得がほぼ全期間にわたって出現したためです。この未検出の検体をより詳しく調査した結果、IRCサーバで制御されるタイプのボット2種類[*33][*34]が活発に活動していたことが分かりました。

MITFの独自の解析では、今回の調査期間中に取得した検体は、ワーム型66.3%、ボット型29.9%、ダウンローダ型3.8%でした。また解析により、26個のボットネットC&Cサーバ[*35]と9個のマルウェア配布サイトの存在を確認しました。

■ Confickerの増減

期間中、Confickerの動きに変化が見られました。総取得検体数が5月16日から6月19日までの期間で約2割減少し、その後以前の水準に復帰しました。この現象の原因は不明です。調査の結果、特定の検体に関わる事象ではなく、検体取得元IPアドレスをみても、国別などの傾向は見られませんでした。

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[*36]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。

＊31 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。
＊32 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。
＊33 Trojan:Win32/Ircbrute（http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?name=Trojan%3AWin32%2FIrcbrute）。
＊34 Win32/Hamweq（http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Win32%2fHamweq）。
＊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 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。

2012年4月から6月までに検知した、Webサーバに対するSQLインジェクション攻撃の発信元の分布を図-10に、攻撃の推移を図-11にそれぞれ示します。これらは、IIJマネージドIPSサービスのシグネチャによる攻撃の検出結果をまとめたものです。

発信元の分布では、中国65.4%、日本14.5%、US3.1%となり、以下その他の国々が続いています。中国からの攻撃が大幅に増加していますが、これは中国からの攻撃が一部の日に大量に発生したためで、これらを除いた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、6月23日に発生した攻撃では、中国の特定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す。6月19日についても別の中国の特定の攻撃元から別の特定の攻撃先に対する攻撃が発生しています。これらの攻撃はWebサーバの脆弱性を探る試みであったと考えられます。また、5月10日と6月5日に発生した攻撃は、中南米諸国の様々な攻撃元から特定の攻撃先に対する攻撃でした。

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。

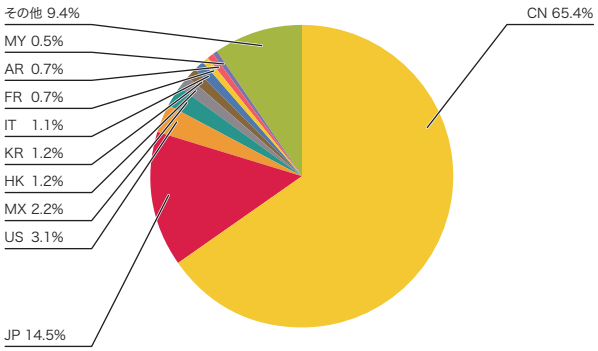

図-10 SQLインジェクション攻撃の発信元の分布

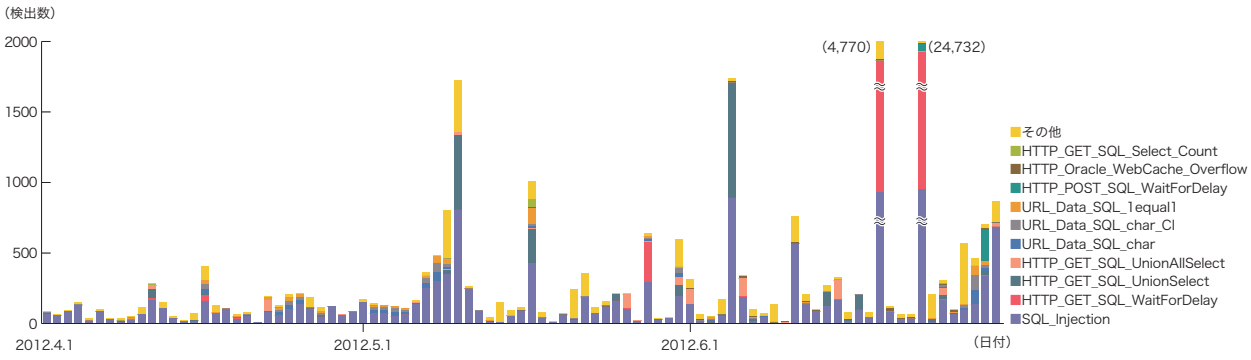

図-11 SQLインジェクション攻撃の推移(日別、攻撃種類別)

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、日本を対象としたAnonymousによる攻撃作戦について解説すると共に、Windows Updateへの中間者攻撃を行うマルウェアFlameと、ZeuSとその亜種について解説します。

1.4.1 日本を対象としたAnonymousによる攻撃作戦

本稿では、4月から6月の期間に発生した、日本をターゲットに含むAnonymousの攻撃作戦(OpNewSonとOpJapan)について、攻撃発生に至る経緯及び実際の攻撃の状況と対応について紹介します(表-1、表-2)。

■ Operation NewSon

4月11日に、TheWikiBoatを名乗るグループが攻撃作戦Operation NewSon(OpNewSon)を発表しました[*37]。これは、5月25日(日本時間では5月26日)に日本企業3社を含む46の大企業のサイトに対するDDoS攻撃の実施を呼び掛けるものでした。TheWikiBoatはAnonymousから派生した4〜5人のグループで、彼らの声明によると、4月1日から活動を開始しています。Anonymousの攻撃作戦にも一時参加していたものの、Anonymousとは別のグループだと主張しており、自分達で実施する攻撃作戦としては、実質的に今回が初めてということでした。また攻撃予告日の1ヵ月以上も前に発表されていたため、当初は国内だけでなく、海外でもまったく注目されていませんでした。

TheWikiBoatの攻撃理由や攻撃対象の選定基準は不明確ではあるものの、実際に攻撃が実施される可能性も否定できません。そのため攻撃予告日が近くなると、米国ではFBIが対象企業に注意喚起をしたり[*38]、国内でも同様に攻撃に備える動きが見え始めたり、一部のメディアによる報道も見られたりしました。また、TheWikiBoatが攻撃予告にあたって参加を呼び掛けたIRCのチャネルでは、実際の攻撃に関する指示なども出始めました。

■ 攻撃状況

攻撃開始時刻(日本時間の5月26日午前8時)にむけてIRCへの参加者が徐々に増えはじめ、400人を越えるまでになりました。しかし、その大半は会話や攻撃に参加するのではなく、活動を監視する目的か、単なる傍観者のようでした。

開始時刻を過ぎると、TheWikiBoatからIRCとTwitterで攻撃対象が指示されました。この対象は事前に提示されていたリストに含まれていたサイトの1つでした。しかし、30分程が経過してもサイトがダウンする気配はないまま、何らかの理由によってIRCのチャネルが突然閉鎖され、作戦は中断されました。攻撃はその後も再開されることはなかったため、この作戦は結果的に完全な失敗に終わったと言えます。

■ 攻撃への対応

攻撃対象が公表されていたことから、対象となった企業は、あらかじめ攻撃に備えることが可能でした。しかし、攻撃に至るまでの状況を見る限り、TheWikiBoatは明らかに準備不足で大規模な攻撃になるとは考えにくく、実際には防御側としてやや過剰な反応だったと言えなくもありません。詳細な情報がないまま対応を余儀なくされた企業もあり、事前の情報共有のあり方や、各組織における情報収集及び分析の能力について、今後に課題を残しました。また攻撃予告があってから慌てて対応するのではなく、緊急時に対応できる体制を常に整備しておくことが求められていると言えます。

表-1 Operation NewSon

2012年 4月 1 日	TheWikiBoat活動開始。
4月11日	TheWikiBoatが"Operation NewSon(OpNewSon)"のプレスリリースを発表。同時に46の攻撃対象リストを公開。
5月23日	主要メディアとしては最初にFOX Newsが報道。
5月24日	FBIが攻撃予告の内容についてメールで注意喚起。
5月25日	攻撃開始時刻が日本時間の5月26日午前8時と発表される。
5月26日	1サイトに対して攻撃が実施されるが失敗に終わる。

*37 "Operation NewSon(OpNewSon)#TheWikiBoat"(http://pastebin.com/wq6KdgDg)。
*38 Kaspersky Lab Threatpost、"FBI Warns Top Firms Of Anonymous Protest Hacks on May 25"(http://threatpost.com/en_us/blogs/fbi-warns-top-firms-anonymous-protest-hacks-may-25-052412)。

■ Operation Japan

続いて6月25日にAnonymous（AnonOps）がOperation Japan（OpJapan）のプレスリリースを発表しました[*39]。これは違法ダウンロードの刑罰化などを盛り込んだ改正著作権法が国会で可決、成立したことに抗議するものです。併せてJASRAC（日本音楽著作権協会）などの音楽権利者団体が、違法音楽ファイルを特定するための仕組み[*40]の導入を国内ISPに働きかけるという発表をしたことについても、プライバシー上の懸念を表明しています。プレスリリースでは、日本政府とRIAJ（日本レコード協会）に対して攻撃を行うことを示唆していました[*41]。

■ 攻撃状況

6月25日深夜に、財務省の関連Webサイトが改ざんされることから攻撃が始まりました。そのページに載せられたAnonymousからのメッセージには、インターネットにおける規制を強化するインド政府に対して攻撃を行い、成功したこと（Operation India）、次のターゲットは日本であることなどが書かれていました。

翌6月26日に攻撃は本格化し、裁判所のWebサイトへのDDoS攻撃、国土交通省の関連Webサイトの改ざん、自民党、民主党のWebサイトへのDDoS攻撃と続きました。更に6月27日には、JASRAC、経団連のWebサイトもDDoS攻撃の対象となりました。その後も小規模な攻撃は断続的に行われたものの、本稿執筆時点では攻撃はほぼ沈静化しています。しかし、今回の攻撃理由を考えると、攻撃側が目標を達成したとは言えず、攻撃がいつ再開してもおかしくありません[*42]。

■ 攻撃への対応

今回の攻撃では、攻撃対象は事前にはあまり明確ではなく、IRCチャットの中で示唆されたWebサイトに対して突発的に攻撃が行われるといった状況でした。また著作権法の改正と、直接には何の関係もないと考えられるサイトも攻撃されており、統率のとれた攻撃作戦ではありませんでした。

一部で脆弱なWebサイトの改ざんも行ってはいますが、今回の主な攻撃方法はDoS攻撃です。IRCの様子から、

表-2 Operation Japan及びそれに関連する出来事

2012年 6月 4 日	JASRAC、RIAJなど音楽権利者6団体2社が違法音楽配信対策を推進するとのプレスリリースを発表。
6月 9 日	日本のAnonymousが他のグループと連携して、仙台で反ACTA[*43]の抗議デモを実施。
6月15日	日本のAnonymousが反ACTAを訴える抗議活動「オペレーション・ジャパン（OpJapan）」を発表。
6月20日	著作権法の一部を改正する法律案（改正著作権法）が参議院本会議で可決、成立。
6月25日	海外のAnonOpsが改正著作権法などに抗議する"Operation Japan（OpJapan）"のプレスリリースを発表。
6月26日	財務省関連Webサイトが改ざんされる。
	裁判所のWebサイトがDDoS攻撃を受ける。
	国土交通省関連Webサイトが改ざんされる。
	自由民主党のWebサイトがDDoS攻撃を受ける。
	民主党のWebサイトがDDoS攻撃を受ける。
6月27日	JASRACのWebサイトがDDoS攻撃を受ける。
	日本経済団体連合会のWebサイトがDDoS攻撃を受ける。
6月29日	JASRACのWebサイトがDDoS攻撃を受ける（以降、断続的に小規模な攻撃が続く）。
7月 3 日	街頭清掃作戦（Operation Anonymous Cleaning Service/OpA.C.S）のプレスリリースが発表される（反ACTAの抗議活動をしていたAnonymousとは別の日本のグループが主催）。
7月 7 日	渋谷で第一回お掃除OFF会が実施される。

＊39 "#opJapan - Expect US"（http://anonpr.net/opjapan-expect-us-512/）。
＊40 このシステムについては次の一般社団法人著作権情報集中処理機構のホームページを参照のこと（http://www.cdc.or.jp/）。
＊41 6月15日に日本のアノニマスを名乗るグループがACTA（偽造品の取引の防止に関する協定）への抗議行動を呼び掛けており、先にオペレーション・ジャパン（OpJapan）という名称を使っていた。Twitterのハッシュタグも同じものを使っているが、両者には直接的な関係は何もない。また7月7日に街頭清掃作戦（Operation Anonymous Cleaning Service/OpA.C.S）と称して渋谷駅周辺での清掃活動を行ったグループもアノニマスを名乗っているが、これはAnonOpsによる攻撃活動をきっかけに集った日本の参加者が行っているものである。これらのグループはすべて異なっており、それぞれが独自の活動を行っている。
＊42 Anonymousによる他のOperation、例えばOperation India（OpIndia）の場合、ほぼ1年以上にわたって攻撃作戦が継続している。
＊43 外務省、「偽造品の取引の防止に関する協定（ACTA）」（http://www.mofa.go.jp/mofaj/gaiko/ipr/acta.html）。

HOIC[*44]や、Slowloris[*45]TorsHammer[*46]などのツールが攻撃に利用されたと考えられます。またボットネットによる攻撃も観測されています。攻撃されたWebサイトによっては、サイトへのアクセスがしづらくなったように、DDoS攻撃が成功したところもあれば、特に影響がみられず、攻撃が失敗に終わったところもあります。これはDoS攻撃の発生を想定した防御策や、緊急時の体制の整備など、事前の対応の有無が結果を分けたと考えられます。

■ 今後の課題

OpNewSonやOpJapanの攻撃規模はさほど大きいものではなく、結果的に攻撃による影響は限定的なものでした。しかし、海外のAnonymousも日本国内の動きにも興味を持っており、何かきっかけさえあれば、攻撃作戦に発展する可能性があることが示されたと言えます。これは注目に値する新しい動きであり、今後しばらくは同様の活動に注意が必要です。

一方で、Anonymousによる攻撃だからといって、特別な対策が必要になるわけではありません。従来どおりに、Webサイトからの情報漏えいや改ざんを防ぐための既知の脆弱性への対応や、DDoS攻撃への対応、また、緊急時に対応できる体制の整備などを行うことが求められています。

1.4.2 Windows Updateへの中間者攻撃を行うマルウェア Flame

本節では、2012年5月にイランで発見されたFlameと呼ばれるマルウェアの概要と、そのマルウェアが悪用したコード署名機能への攻撃によるWindows Updateへの中間者攻撃について紹介します。

■ Flameの概要

Flameは別名Flamer、sKyWIperとしても知られ、Iran National CERTにより存在が確認され[*47]、中東地域を中心に感染が広まったマルウェアです。このマルウェアは米国及びイスラエル軍によるイランへのサイバー攻撃の一環で開発されたマルウェアであるとの報道もあります。Flameには機能ごとにモジュールが多数存在し、本体及び全モジュールのコードの総量は20MBと、マルウェアとしてはサイズが非常に大きいことが特徴の1つとして挙げられます[*48]。本稿執筆時点では完全に解析されたわけではありませんが、ブタペスト工科大学のLaboratory of Cryptography and System Security（CrySyS Lab.）による詳細な解析結果が公開され[*49]、その後もKaspersky Lab社などの各セキュリティベンダによって解析の情報が順次公開されています。

Flameは複数の感染手法を持っており、USBメモリなどのリムーバブルデバイスやいくつかの脆弱性を使用して感染します[*50]。更に、Windows Updateの仕組みに中間者攻撃を行うことで、ローカルネットワーク上の他の端末に感染させる機能を持っていたことが最大の特徴の1つです[*51]。またFlameは、通信の盗聴、アカウント情報の収集やスクリーンキャプチャ、マイクの録音機能を持っており、他にもファイルシステムや各種ドキュメント、Zipアーカイブの解析を行って情報を収集する機能も存在しています。このように、Flameには感染端末及びその周辺の情報を収集するための機能が搭載されています。

＊44 HOIC（High Orbit Ion Cannon）はターゲットとなるサーバにHTTP GETリクエストを大量に送るDoS攻撃ツール。Boosterと呼ばれる設定ファイルを変えることで、様々なリクエストを送信することができる。

＊45 SlowlorisはApacheなどのWebサーバの脆弱性を利用したDoS攻撃ツール。Webサーバに不完全なリクエストを送ることによって、サーバのプロセスが待機状態になることを悪用する。

＊46 DoS攻撃ツールの1つ。Slowlorisに似ているがHTTPのGETメソッドのかわりにPOSTメソッドを利用する。またTor（The Onion Router）を利用して通信経路を匿名化する。

＊47 Iran National CERT、"Identification of a New Targeted Cyber-Attack"（http://www.certcc.ir/index.php?name=news&file=article&sid=1894）。

＊48 Kaspersky Lab SECURELIST Blog、"The Flame:Questions and Answers"（http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers）。

＊49 Laboratory of Cryptography and System Security（Budapest University of Technology and Economics）、"sKyWIper（a.k.a. Flame a.k.a. Flamer）:A complex malware for targeted attacks v1.05（May 31, 2012）"（http://www.crysys.hu/skywiper/skywiper.pdf）。

＊50 CrySyS Labは前述のレポート内で、脆弱性としてStuxnetで使用されたMS10-061の脆弱性及びMS10-046が使用されている可能性があることを言及している。また、Kaspersky Lab社では、前述のブログの中でMS10-033の脆弱性が使われている可能性に言及している。

＊51 Kaspersky Lab社のSECURELIST Blogでは、Windows Updateの通信を感染端末にリダイレクトすることで中間者攻撃を行い、コード署名されたバイナリをネットワーク上の他の端末にインストールする機能がGadgetモジュールに存在することを報じている。「'Gadget' in the middle: Flame malware spreading vector identified」（http://www.securelist.com/en/blog/208193558/Gadget_in_the_middle_Flame_malware_spreading_vector_identified）。

■ Windows Updateへの中間者攻撃

Flameには、あたかもMicrosoft社が保証した正式なプログラムの実行形式であるかのように偽装してダウンロードし、インストールさせるバイパス機能が搭載されていることがKaspersky Lab社やMicrosoft社によって明らかになりました。ソフトウェアの確からしさを保証する仕組みの1つとして知られるCode Signingは、SSL/TLSなどで用いられるPKIの枠組みを用いて実行ファイルにデジタル署名を施すことにより、動作させる際にデジタル署名と発行元を検証することで、不正なソフトウェアを排除することができます[*52]。Flameは、このデジタル署名を偽造してMicrosoft社が署名しているように見せかけるように仕組まれていました。

Windows Updateを介してモジュールをダウンロードする際には、Code Signingの機能により、ソフトウェアの確からしさを保証することができます。例えば、通信への中間者攻撃により、Microsoft社のサーバではない偽のサーバに接続して、不正なソフトウェアをダウンロードしたとしても、Microsoft社が保証したものでない場合には、Code Signingの機能によりこの不正をチェックすることができます。しかし、Flameに含まれる実行ファイルの1つはWindows OSの信頼するPKI証明書の階層下に置かれた偽造証明書で署名されていて、OSが正しいソフトウェアとして認識してしまうという問題が発生していました。この偽造署名は、用いられたMicrosoft社保有のPKI証明書の内容不備と、デジタル署名に用いられるハッシュ関数として、既に危殆化しているMD5を利用していたことに起因しています。

偽造署名の報告を受けて、現地時間6月3日にMicrosoft社より更新プログラムが公開されました[*53]。この更新プログラムは、偽造に用いられる可能性のあるMicrosoft社保有の中間CA証明書3枚を無効にします。無効化される証明書は、主体名を表わすX.509証明書のフィールドCommon Name(CN)としてMicrosoft Enforced Licensing Intermediate PCAを持つ異なる証明書2枚と、CNがMicrosoft Enforced Licensing Registration Authority CA(SHA1)である証明書1枚です[*54]。

一部の証明書を無効にする仕組みは、CRLの配布などにより行えるにも関わらず、この時点で、中間CA証明書自体を無効にする措置が取られました。当初、証明書がどのように偽造されたかに関する情報が公開されていなかったため、この措置は過剰な反応であったと考えられましたが、DigiNotarの不正発行事件のように迅速に対応することが、信頼回復のために有効な手段であるという認識の下、このような対処がなされたという解釈を行うこともできました。

しかし、6日6日に公開されたMicrosoft社からの続報で事態は急変します。偽造された証明書は、署名に用いられるハッシュ関数としてMD5が使われており、MD5に対するchosen prefix collision attackの手法を用いて証明書そのものが偽造されているという事実が公開されました[*55]。

更に、今回の問題は中間CA証明書のフォーマットにも原因があることが分かりました。証明書にはその用途を表すKey UsageやExtended Key Usageが含まれており、Digital Signature、Certificate Sign、CRL Sign、Code Signingなどの情報が記載されます。今回、無効処理された中間CA証明書Microsoft Enforced Licensing Intermediate PCAには、本来その用途として利用するはずのないCode Signingが含まれていることが分かりました。これは、偽造された証明書の上位に位置する中間CA証明書の用途としてCode Signingが含まれていないのであれば、検証時のチェックで不正利用として検出することができたことを意味しています[*56]。

---

*52 Code signingの仕組みについては、Windowsハードウェアデベロッパーセンター、「Windowsのドライバー署名の要件」(http://msdn.microsoft.com/ja-jp/library/windows/hardware/gg487317.aspx)などに詳しい。

*53 Microsoft社、「マイクロソフト セキュリティ アドバイザリ(2718704)承認されていないデジタル証明書により、なりすましが行われる」(http://technet.microsoft.com/ja-jp/security/advisory/2718704)。

*54 TechNet Blogs:Security Research & Defense、"Microsoft certification authority signing certificates added to the Untrusted Certificate Store"(http://blogs.technet.com/b/srd/archive/2012/06/03/microsoft-certification-authority-signing-certificates-added-to-the-untrusted-certificate-store.aspx)。

*55 TechNet Blogs、"Security Research & Defense, Flame malware collision attack explained"(http://blogs.technet.com/b/srd/archive/2012/06/06/more-information-about-the-digital-certificates-used-to-sign-the-flame-malware.aspx)。

*56 今回と同様の証明書の問題については、IIR Vol.14の1.4.1「公開鍵証明書発行に関するいくつかの問題」(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol14.pdf)にてDigiCert Sdn. Bhd.社の発行ポリシーの問題として紹介している。

図-12にマルウェアFlameの動作概要を示します。Flameの一連の動作の中で、インストールが試みられるWuSetupV.exeに付随の証明書は、Microsoft社によるものではなく偽造されたものでした[*57][*58]。このCN="MS"という名前を持つ偽造証明書は、ルート証明書Microsoft Root Authorityまで証明書パスを遡ることで、正しい証明書であることが保証されていました。これまでにも、実際に中間CA証明書を偽造することに成功した事例はありましたが、MD5アルゴリズムの脆弱性が実社会においてここまで脅威となった事例は初めてと考えられます。

■ 証明書の偽造手法

Flameが利用する偽装署名に利用された証明書は、証明書そのものに対する暗号論的攻撃手法で作成されたものだと考えられています。今回の偽造は、2007年のEUROCRYPTで公開されたchosen prefix collision attack[*59]と、それを応用して2008年末に公開された偽造中間CA証明書生成の手法[*60]を用いていると筆者は考えていました。しかし、この偽造結果で得られるフォーマットと、Flameで使われた証明書のフォーマットが異なることをIIJでは確認しています。これまでの手法では、Netscape Comment extensionにダミーデータを押し込めることで攻撃を成功させていましたが、我々が入手した偽造証明書は、X.509v3拡張を含んでおらず、代わりにIssuer Unique Identifierにダミーデータを押し込める方法が取られていました。このダミーデータには、CRL Distribution Pointなどの情報が押し込められており、既存の正規に発行された証明書の署名部分を再利用する形で、被署名対象をうまく書き換えることにより偽造する点ではこれまでの手法と同じです。

本稿執筆時点では、この証明書の作成方法は明らかになっていませんが、研究が進んでいます。まず、前述の攻撃手法を公開した研究者らが、まったく新しいchosen prefix collision attackにより、証明書が偽造されていることを公

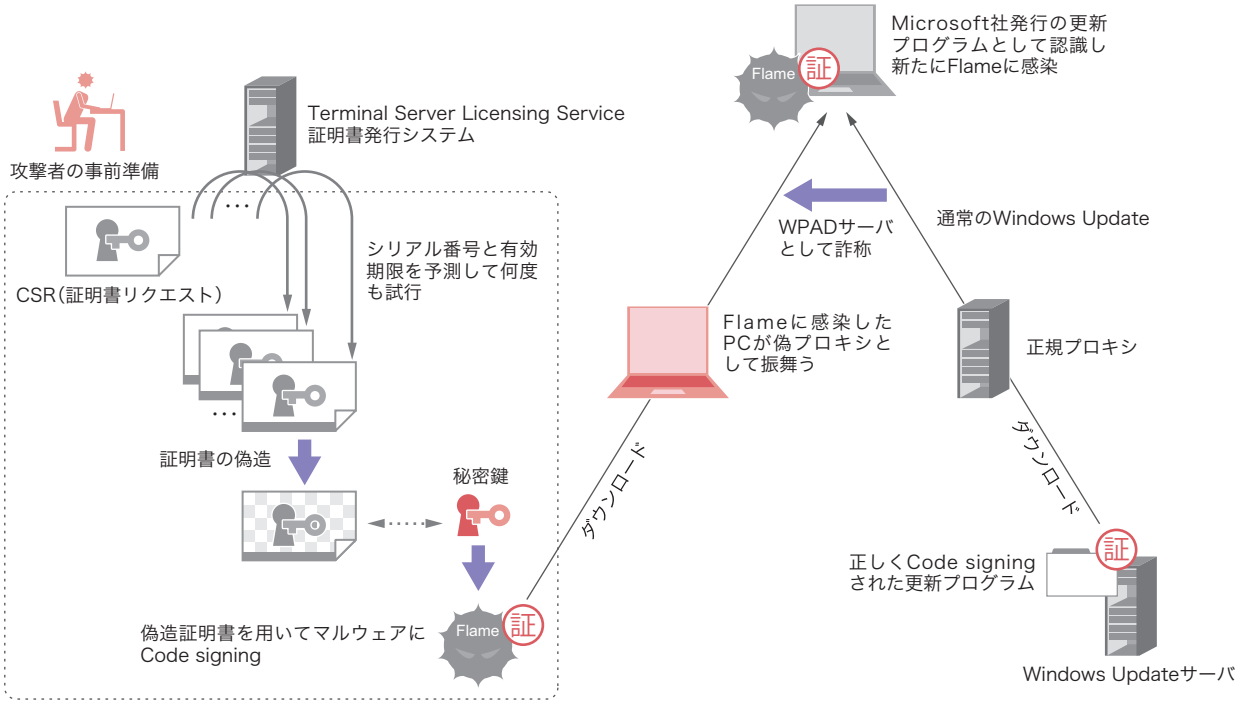

図-12 マルウェアFlameの動作概要

*57 エフセキュアブログ、「Microsoft Updateと最悪のシナリオ」(http://blog.f-secure.jp/archives/50667927.html)。
*58 CrySyS、"The Flame malware WuSetupV.exe certificate chain"(http://blog.crysys.hu/2012/06/the-flame-malware-wusetupv-exe-certificate-chain/)。
*59 Marc Stevens、Arjen Lenstra、Benne de Weger、"Chosen-Prefix Collisions for MD5 and Colliding X.509 Certificates for Different Identities"、EUROCRYPT2007。
*60 Alexander Sotirov、Marc Stevens、Jacob Appelbaum、Arjen Lenstra、David Molnar、Dag Arne Osvik、Benne de Weger、"MD5 considered harmful today" 2008(http://www.win.tue.nl/hashclash/rogue-ca/)。

開しました[*61]。更に、その研究チームの1人により、偽造証明書に関する詳細なレポートが公開されています[*62]。このレポートによると、中間CA証明書偽造の手法と同様に、証明書発行システムが割り振るシリアル番号を予測することで、攻撃者が欲する被署名データに対する正規なものと判断される偽の証明書を獲得する方法が紹介されています。しかし、シリアル番号の中には、発行時に割り振られるミリ秒単位のデータが格納されていることからも、この攻撃には相当量の計算能力が必要であり、今回の証明書偽造にこの手法が使われたかどうかは分かりません。

■ Microsoft社による抜本的な対策

Microsoft社では、今回のFlameにおける問題を鑑み、多くの抜本的な見直しと新しい取り組みが行われています。6月12日には、失効した証明書を自動で処理する更新プログラムが公開されました[*63]。これまで証明書の失効はWindows Update、もしくは手動で更新情報のアップデートを行う必要がありましたが、失効から1日を目処に自動的に最新の更新情報を反映することができるようになりました。また、翌月の定期アップデートにおいて、28枚の証明書を無効化する更新プログラムが配布されました[*64]。これは、Flameにおける偽造署名を用いた同様の攻撃を防止するため、問題を抱えている証明書を洗い出し、潜在的な偽造攻撃を防止する目的で配布されています。更に8月には、リスクを理解して利用すべきであると認識されている1024ビット未満のRSA鍵を受け入れない処置を行う更新プログラムの公開が予定されています[*65][*66]。具体的には、1024ビット未満のRSA鍵を持つ証明書がSSLやS/MIMEなどで利用された場合に、エラーメッセージを表示するなどの処理が行われるようになります。PKIを安心して使ってもらうためには、これらの取り組みに加え、MD5を用いた証明書を受け入れないなど、危険であると認識されている暗号アルゴリズムや鍵長を利用しないようにする仕組みと、業界全体でのコンセンサスづくりが必要です。

1.4.3 ZeuSとその亜種について

ZeuSは、2007年ごろから確認されているCrimeware Kit[*67]の1つです。今年の3月に、米Microsoft社は、金融業界の各社と協力して大部分のZeuSボットネットのテイクダウンに成功しました[*68]。その一方で、昨年の5月にZeuSのソースコードがインターネット上に流出して以来[*69]、ZeuSをベースにしていると思われるいくつかの亜種が確認されています。それらの中には、ウイルス対策ソフトウェアでまったく検知できなかったものや、新たな機能を備えていたものも少なくありません。

もし皆さんがZeuSボット（以下ZeuS）に感染した端末を調査する場合、例えば以下について明らかにしたいのではないでしょうか。

- 他端末における感染痕跡の検出という観点での、ボットネットサーバのURL
- 被害状況の把握という観点での、ZeuSが情報搾取のターゲットとしているURLのリスト、及び実際に盗まれた情報

*61 Centrum Wiskunde & Informatica、"CWI cryptanalist discovers new cryptographic attack variant in Flame spy malware"（http://www.cwi.nl/news/2012/cwi-cryptanalist-discovers-new-cryptographic-attack-variant-in-flame-spy-malware）。
*62 Alex Sotirov、"Analyzing the MD5 collision in Flame"（http://trailofbits.files.wordpress.com/2012/06/flame-md5.pdf）。
*63 TechNet Blogs、「失効証明書の自動更新処理を有効にするKB2677070の適用を推奨」（http://blogs.technet.com/b/jpsecurity/archive/2012/06/18/3504363.aspx）。
*64 Security TechCenter、「マイクロソフト セキュリティ アドバイザリ（2728973）承認されていないデジタル証明書により、なりすましが行われる」（http://technet.microsoft.com/ja-jp/security/advisory/2728973）。
*65 Windows PKI blog、"RSA keys under 1024 bits are blocked"（http://blogs.technet.com/b/pki/archive/2012/06/12/rsa-keys-under-1024-bits-are-blocked.aspx）。
*66 Windows PKI blog、"Blocking RSA Keys less than 1024 bits（part 2）" （http://blogs.technet.com/b/pki/archive/2012/07/13/blocking-rsa-keys-less-than-1024-bits-part-2.aspx）。
*67 Crimeware Kitとは、端末からアカウントやパスワード（特に金融関連のもの）などの個人情報を盗み出すマルウェアを生成するためのフレームワークを指す。同様のCrimeware Kitとしては、SpyEyeがある。SpyEyeについては、IIR Vol.13「1.4.2 SpyEye」（http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol13.pdf）で解説している。
*68 Microsoft社によるZeuSボットネットのテイクダウンについては次を参照のこと。"Microsoft and Financial Services Industry Leaders Target Cybercriminal Operations from Zeus Botnets"（http://blogs.technet.com/b/microsoft_blog/archive/2012/03/25/microsoft-and-financial-services-industry-leaders-target-cybercriminal-operations-from-zeus-botnets.aspx）。
*69 ZeuSのソースコードが流出した時期に、トレンドマイクロ社は流出したソースコードを犯罪組織が利用するのではないかという懸念を表明していた。Trend Micro MALWARE BLOG、"ZeuS Source Code Leaked, Now What?"（http://blog.trendmicro.com/the-zeus-source-code-leaked-now-what/）。

ZeuSは、上記のような情報をレジストリやファイルシステムに残したり、ネットワーク上で送受信します。しかし残念ながら、それらのほとんどについて、内容を簡単に確認することはできません。ZeuSによるデータの暗号化スキームは洗練されており、複数のデータ構造体に含まれる複数のキーを暗号化に用いているためです。そのスキームを理解するためには、ZeuSによるデータの取り扱いを把握する必要があります。

本節では最初に、流出したソースコードの調査や最近確認されている亜種の解析結果を基にして、ZeuSの感染動作をデータの取り扱いにフォーカスして説明します。次に、その動作に基づいたZeuSの感染痕跡や暗号化されたデータの調査方法を述べます。最後に、最近の亜種が新たに備えた機能についても触れます。

■ ZeuSボットの感染動作

ZeuSの感染動作は、大きく分けて初回のインストールと、インストールした後の情報を盗むためのコードインジェクション及びサーバとの通信の2つから成ります。感染動作の概略図を図-13に示します。ZeuSが使用するデータ構造はSpyEyeのそれに比べると複雑です。まず、動作及び主要なデータ構造体を説明します。

ZeuSは起動直後に2つのデータ構造体を初期化します。それらはBASECONFIG、COREDATAとして定義されています。BASECONFIGには、最初にボットネットサーバにアクセスするためのURL[*70]や、即値の文字列を基にしたRC4のキーなどが含まれます。COREDATAには、OSのGUID・バージョン、実行パス情報、主要なDLLのアドレス情報などのほか、PESETTINGSと呼ばれるインストール時にのみ

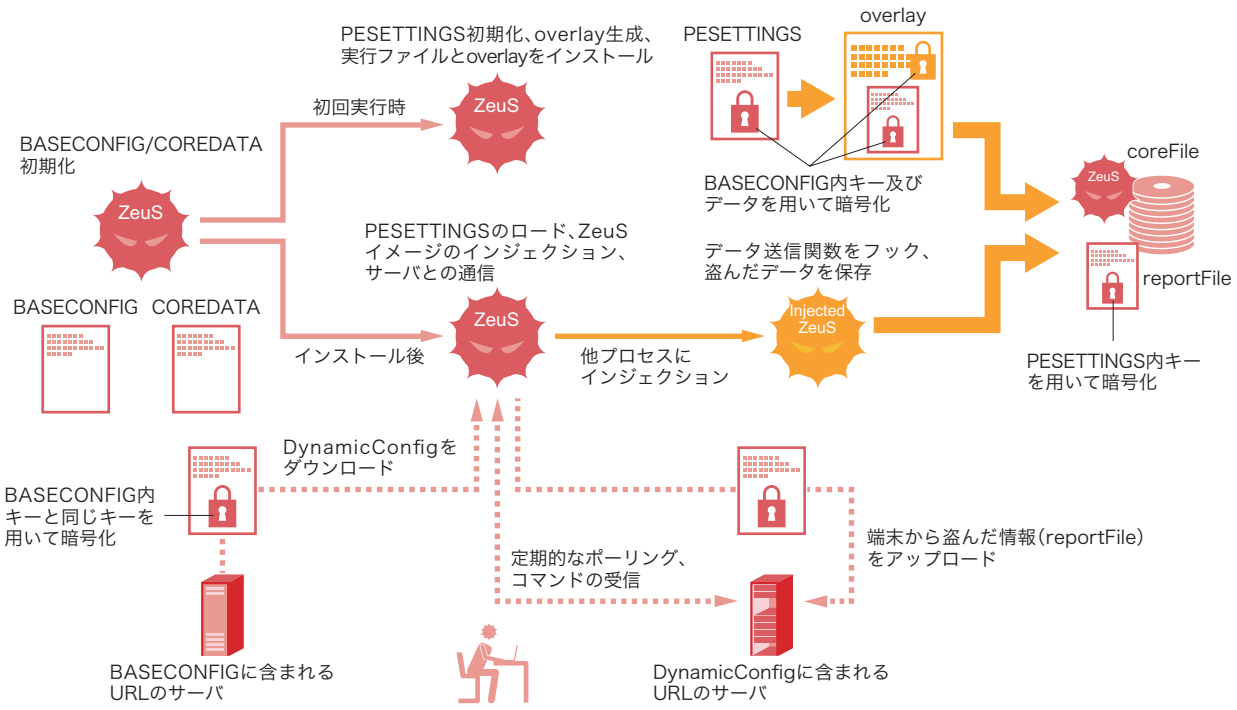

図-13 ZeuSボットの感染動作

*70 ZeuSにおいては、重要な文字列については一定のアルゴリズムを用いた難読化が施されている。最近の亜種は流出したソースコード内で確認できるアルゴリズムを改善したものを利用している。

初期化されるデータ構造体が含まれます。BASECONFIG、COREDATAの初期化が終わると、初回の実行であればインストールの処理に、そうでなければコードインジェクション及びサーバとの通信の処理に入ります。

■ インストール

インストールの動作の場合、ZeuSはまずPESETTINGSを初期化します。PESETTINGSにはZeuSが利用するファイルシステムやレジストリのパス情報(userPaths)、ランダム生成のバイナリデータを基にしたRC4のキーなどが含まれます。PESETTINGSは初期化された後、BASECONFIGに含まれるRC4のキーで暗号化されます。その後、暗号化されたPESETTINGSは、そのサイズやCRCの値、シグネチャ[*71]をヘッダとするデータの中に組み込まれ、BASECONFIGデータを基にしたRC4のキーで更に暗号化されます。このデータはoverlayと呼ばれ、ZeuSはuserPathsに記載のインストール先(coreFile)に実行ファイルをコピーする際に、その実行ファイル内にoverlayを組み込んだり、インストール先と同じフォルダに単体のファイルとして保存したりします[*72]。

userPaths内には、サーバへ送信するデータを保存するファイルパスの情報(reportFile)も含まれており、coreFileとreportFileは、両方ともCSIDL_APPDATAで指定されるフォルダ[*73]以下にランダムな名前で生成されます。最後に、インストールした実行ファイルのプロセスを生成し、自身をファイルシステム上から削除することで、インストールの動作が終了します。

■ コードインジェクション及びサーバとの通信

コードインジェクション及びサーバとの通信の動作の場合、まずoverlayからPESETTINGSを抽出してOSのGUIDやプロセスの実行パスがPESETTINGS内のそれと一致しているか確認します。一致している場合は、そのシステムで実行中のプロセスを列挙していき、インジェクション可能なプロセスに対して、ZeuSの実行ファイルイメージのインジェクションを行います。インジェクションされたプロセスにおいて、ZeuSはデータ送信関数のフックを行い、盗んだ情報をreportFileに保存します。

インジェクションが終わった後、ZeuSはBASECONFIGに含まれるURLにアクセスして、DynamicConfigと呼ばれるサーバ側にある設定データを取得します。このデータは暗号化されており、ZeuSはBASECONFIGに含まれるRC4のキーで復号化してからXOR[*74]を行い、暗号化前の状態に一度戻します。その後、データのハッシュ値などを確認後、データに対してXOR[*75]を再び行い、PESETTINGSに含まれるRC4のキーで暗号化してから、それをレジストリの値として設定します。そのレジストリパスは「HKCU¥SOFTWARE¥Microsoft」をベースとしてuserPathsに含まれるregKeyとregDynamicConfigを基に決定されます。以降、DynamicConfigを参照する際は、その都度データをレジストリから取得して復号化します。

DynamicConfigを取得した後は、それに含まれるボットネットサーバのURL(CFGID_URL_SERVER_0)と本格的な通信を開始します。具体的には、自身の生存確認のためのポーリングを行ったり、その端末から盗んだ情報(reportFile内に追加されるデータ)を送信したり、サーバから指定されたコマンドを受信して実行したりします。

■ 感染痕跡とデータの抽出

これまで述べたZeuSの感染動作及び利用するデータ構造体を把握することで、ZeuSに感染した端末に残されたデータやネットワーク上に流れるデータの復号化やパースが可能になります。それらの情報は、他端末における感染痕跡の検出や被害状況の把握に役立ちます。

例えば、BASECONFIGのデータを用いてoverlayを復号化しPESETTINGSを抽出することで、reportFileのパスや、

---

*71 "DAVE"という4バイトデータをシグネチャに使用している。
*72 overlayを実行ファイルの中に組み込むのか、単体のファイルとして保存するかの動作は、亜種によって異なる。
*73 Windows XPであれば「C:¥Documents and Settings¥ユーザ名¥Application Data」、Windows Vista及び7であれば「C:¥Users¥ユーザ名¥AppData¥Roaming」。CSIDL(constant special item ID list)については以下が詳しい。"CSIDL"(http://msdn.microsoft.com/en-us/library/windows/desktop/bb762494%28v=vs.85%29.aspx)。
*74 即値を使わず、エンコードされたデータの最後から隣り合わせのバイト同士をXORし、それをデータの最初まで繰り返すデクリメンタルXORを使用している。
*75 即値を使わず、エンコードされたデータの最初から隣り合わせのバイト同士をXORし、それをデータの最後まで繰り返すインクリメンタルXORを使用している。

DynamicConfigをはじめとする設定に関するレジストリ値を特定することができます[*76]。更に、PESETTINGSに含まれるRC4キーによる復号化とXOR処理を施すことによって、DynamicConfigをレジストリ値から抽出することができます。

また、BASECONFIGからはZeuSがDynamicConfigをダウンロードするURLを抽出でき、DynamicConfigからはZeuSが定常的に通信したり盗んだデータを送信したりする宛先のサーバのURLを抽出できるので、ネットワーク上の感染痕跡を調べるのに役立ちます。DynamicConfigには情報を盗む対象となるURLのリスト(CFGID_HTTP_INJECTS_LIST)も含まれているので、感染後にユーザがそのリストのどれかにアクセスして認証情報を入力した場合には、それが盗まれた可能性が高いと推測できます。ネットワーク上に流れるデータをキャプチャできている場合は、BASECONFIGに含まれるRC4のキーによる復号化とXOR処理によってそのデータを抽出できます。

■ 亜種による機能の拡張

最近確認されているZeuSの亜種には、ソースコードが流出した時点でのそれにはない、いくつかの機能が追加されています[*77]。それらの機能はボットネットサーバから発行されるコマンドに応じて実行されるもので、例えば以下のようなものがあります。

```
user_activate_imodule
user_restart_imodule
user_start_syn
user_stop_syn
user_start_ssh_scan
```

user_activate_imoduleと呼ばれるコマンドは、coreFileのパスにあらかじめ決められた名前のDLLをサーバからダウンロードして保存します。次にそのDLLをロードして、DLLがエクスポートしている関数であるTakeBotGuidを実行します。また、COREDATAの拡張された領域にDLLのハンドルやエクスポート関数のアドレス(Init/TakeBotGuid/Start)、ボットネットサーバのURLや端末の識別情報を格納します。その後、スレッドを起動してDLLのInit関数を実行します。user_restart_imoduleは、user_activate_imoduleでダウンロードしてきたDLLのエクスポート関数であるStartを実行します。

user_start_synは、コマンドの引数をCOREDATAの拡張された領域に格納した後、同じDLLのエクスポート関数であるSynを実行します。

user_start_ssh_scanも、同様にコマンドの引数をCOREDATAの拡張された領域に格納しますが、これまでのコマンドとは異なる別のモジュールのエクスポート関数である、start_ssh_checkerを実行します。

上記コマンドで用いられるDLLに関しては、IIJではこれまでのフォレンジック調査において実行可能な状態での取得ができていないため、それらの機能を明らかにできていません。上記コマンドのうち、user_activate_imoduleとuser_restart_imoduleについてはF-Secure社のブログ[*78]においても紹介されていますが、残りの3つに関して言及されていないことから、亜種の作者は、今もなお新しい機能を実装し続けているのではないかと推測されます。

■ まとめ

ZeuSは完成度の高いCrimeware Kitですが、その完成度の高さゆえに、亜種の作者はドラスティックな修正をせずに利用することが多いように見受けられます。よって、一度ZeuSによるデータの取り扱いについて理解しておくと、その感染痕跡や暗号化されたデータの調査を迅速に進められるようになります。

---

*76 インストールされた実行ファイルやoverlayなどにはフォレンジック調査から逃れるためにタイムスタンプの変更が施されるが、それらを格納する各サブフォルダのタイムスタンプの変更処理は、これまでの解析からは確認されていない。また、レジストリの最終更新時刻についても変更はされないので、ファイルシステムやレジストリのパス情報に関しては、これらの挙動を把握していれば簡単なタイムライン調査から関連データを芋づる式に見つけることも可能。

*77 その一方で、従来のZeuSが備えていた機能の一部(Socksサーバやスクリーンショット送信の機能など)が省略されている亜種も存在する。

*78 F-Secure社は昨年末にuser_activate_imodule及びuser_restart_imoduleに関しての動作を解説しており、この内容はIIJによる解析結果と一致する。エフセキュアブログ、「Suo Anteeksi：ZeuSの丁重な亜種」(http://blog.f-secure.jp/archives/50645412.html)。

ところで、犯罪組織はZeuSをExploit Kit[*79]などの既存の仕組みと組み合わせて用いることが多いようですが[*80]、流出したZeuSのソースコードを積極的に利用し、その機能を拡張することにも余念がないようです。McAfee社は、今年に入ってから行われた金銭を搾取する大規模な攻撃に関するレポート[*81]の中で、その攻撃で用いられたZeuSやSpyEyeの亜種が、不正送金のトランザクション自動化や物理的な二要素認証の回避など、これまで確認されていなかった機能を備えていたことを報告しています。

ZeuSをはじめとするCrimeware Kitは、これまで培ってきた手法をベースとして、今後、益々巧妙な犯罪手段として進化していくことは明らかです。インシデントハンドラーやマルウェアアナリストは、新たに強力な亜種が出現した場合でも速やかに対応できるように、それについての理解を深めておく必要があります。

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、日本を対象にしたAnonymousによる活動の状況と、Flame及びZeuSマルウェアについて解説しました。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公開していくことで、インターネット利用の危険な側面を伝えるように努力しています。このような側面についてご理解いただき、必要な対策を講じた上で、安全かつ安心してインターネットを利用できるように努力を継続して参ります。

執筆者:
齋藤 衛(さいとう まもる)
IIJ サービスオペレーション本部 セキュリティ情報統括室 室長。法人向けセキュリティサービス開発などに従事の後、2001年よりIIJグループの緊急対応チーム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)
根岸 征史(1.4.1 日本を対象としたAnonymousによる攻撃作戦)
須賀 祐治(1.4.2 Windows Updateへの中間者攻撃を行うマルウェアFlame)
春山 敬宏(1.4.3 ZeuSとその亜種について)
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、小林 直、桃井 康成、吉川 弘晃、齋藤 聖悟 IIJ サービスオペレーション本部 セキュリティ情報統括室

*79 ExploitkitについてはIIJ Technical WEEK 2010の「セキュリティ動向 2010 (1) Web感染型マルウェアの動向」で紹介している(http://www.iij.ad.jp/company/development/tech/techweek/pdf/techweek_1119_1-3_hiroshi-suzuki.pdf)。
*80 例えばKaspersky Lab社は、BlackHole Exploit Kitが脆弱性を利用した後にZeuSをインストールする事例を紹介している。SECURELIST Blog、"A gift from ZeuS for passengers of US Airways"(http://www.securelist.com/en/blog/208193439/A_gift_from_ZeuS_for_passengers_of_US_Airways/)。
*81 McAfee社は同社の分析レポートの中で、この攻撃に関するケーススタディや、これまでのCrimeware Kitに比べて進化した点を解説している。"Dissecting Operation High Roller"(http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf)。