経路ハイジャック

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7月から9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、DDoS攻撃や不正アクセスによる情報漏えい、Webサイト改ざんなどの攻撃が多発しています。イタリアのセキュリティ企業が攻撃を受け、400GBもの内部情報が漏えいした事件では、この企業が保持していたとされる他社ソフトウェアの複数の未修正の脆弱性が公となり、修正が行われています。不正アクセスとそれによる情報漏えいやWebサイトの改ざんも多く発生しており、国内のいくつかの事件では改ざんされたWebサイトが標的型攻撃の踏み台として悪用されたりしています。このように、インターネットでは依然として多くのインシデントが発生する状況が続いています。

1.2 インシデントサマリ

ここでは、2015年7月から9月までの期間にIIJが取り扱ったインシデントと、その対応を示します。まず、この期間に取り扱ったインシデントの分布を図-1に示します*1。

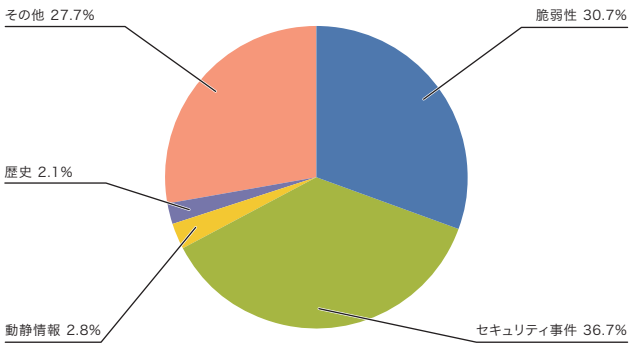


図-1 カテゴリ別比率(2015年7月〜9月)

■ 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。

この期間でも継続して、ISILもしくはその理念に共感していると考えられる個人や組織による、Webサイトの改ざんやSNSアカウントの乗っ取りなどが世界中で発生しています。7月にはシリアの人権監視団体のWebサイトやヨルダンを支援しているとしてジョージアのNATO関連サイトが改ざんされたり、マレーシア警察のFacebookやTwitterなどのSNSアカウントの乗っ取りなどが発生しました。これ以外にも紛争や外交などの情勢や混乱に応じて、インターネット上でも攻撃が発生しています。

政府によるインターネットや通信などの規制に対する抗議としてもいくつか攻撃が発生しています。カナダでは、6月に成立した対テロ法案への抗議から、地方機関を含むいくつかの政府機関に対するDDoS攻撃や不正侵入による内部情報の漏えいなどの攻撃が発生しています(OpC51)。インドではインターネットの規制強化を進めている政府に対する抗議として、インド政府が出資している通信事業者への不正アクセスが行われ、3000万人以上のアカウント情報が漏えいするなどの被害が発生しています(OpIndia)。ベトナムでは、国が実施しているオンライン検閲に対する抗議として、政府機関のWebサイトの改ざんが行われています。フィリピンでも同様に電子通信委員会のWebサイトが改ざんされています。タイでも、国による通信の検閲強化への抗議から複数の政府関連Webサイトに対してDDoS攻撃が発生しています。

日本では9月に、イルカや小型クジラの追い込み漁への抗議活動から、Anonymousによると考えられるDDoS攻撃によって、和歌山県太地町のWebサイトが一時閲覧できなくなるなどの被害が発生しています(OpKillingBay)。このオペレー

*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。

ションでの攻撃は10月になっても継続しており、関係する組織や政府機関、空港や報道機関といったWebサイトに対し攻撃が行われました。更に本稿執筆時点では抗議活動との関連が不明な組織にも攻撃が拡がっていることから注意が必要です。

カナダで水力発電のためのダム建設に伴う抗議活動を行っていたAnonymousのメンバーが現地で射殺された報復として、カナダ連邦警察（RCMP）へのDDoS攻撃や、カナダ安全情報局（CSIS）に侵入して内部の極秘文書を報道機関に送付するなどの活動が行われています。米国では、TPP（環太平洋戦略的経済連携協定）交渉への抗議から、米国勢調査局（United States Census Bureau）が不正アクセスを受け、約4,200名分の雇用者の個人情報が漏えいする事件が発生しています。

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。

■ 脆弱性とその対応

この期間中では、7月に、Microsoft社のWindows 10が公開されたことから、Windows 10で新たに採用されたブラウザのEdge[*2][*3]で修正が行われたのをはじめとして、Windows[*4][*5][*6][*7][*8][*9][*10]、Internet Explorer[*11][*12][*13]、Office[*14][*15][*16]などで修正が行われました。Adobe社のAdobe Flash Player、Shockwave Player、Adobe Acrobat及びReaderでも修正が行われています。Oracle社のJava SEでも四半期ごとの更新が行われ、多くの脆弱性が修正されました。Apple社のOS Xについても多数の脆弱性の修正が行われてます。これらの脆弱性のいくつかは修正が行われる前に悪用が確認されています。

サーバアプリケーションでは、データベースサーバとして利用されているOracleを含むOracle社の複数の製品で四半期ごとに行われてる更新が提供され、多くの脆弱性が修正されました。DNSサーバのBINDでも、細工されたクエリを受信することで外部からのDoS攻撃可能な脆弱性が見つかり、修正されています。Webアプリケーションフレームワークの Apache

＊2 「マイクロソフト セキュリティ情報 MS15-091 - 緊急 Microsoft Edge用の累積的なセキュリティ更新プログラム（3084525）」（https://technet.microsoft.com/ja-jp/library/security/ms15-091.aspx）。
＊3 「マイクロソフト セキュリティ情報 MS15-095 - 緊急 Microsoft Edge用の累積的なセキュリティ更新プログラム（3089665）」（https://technet.microsoft.com/ja-jp/library/security/ms15-095.aspx）。
＊4 「マイクロソフト セキュリティ情報 MS15-066 - 緊急 VBScript スクリプト エンジンの脆弱性により、リモートでコードが実行される（3072604）」（https://technet.microsoft.com/ja-jp/library/security/ms15-066.aspx）。
＊5 「マイクロソフト セキュリティ情報 MS15-067 - 緊急 RDPの脆弱性により、リモートでコードが実行される（3073094）」（https://technet.microsoft.com/ja-jp/library/security/ms15-067.aspx）。
＊6 「マイクロソフト セキュリティ情報 MS15-068 - 緊急 Windows Hyper-Vの脆弱性により、リモートでコードが実行される（3072000）（https://technet.microsoft.com/ja-jp/library/security/ms15-068.aspx）。
＊7 「マイクロソフト セキュリティ情報 MS15-077 - 重要 ATM フォント ドライバーの脆弱性により、特権が昇格される（3077657）」（https://technet.microsoft.com/ja-jp/library/security/ms15-077.aspx）。
＊8 「マイクロソフト セキュリティ情報 MS15-080 - 緊急 Microsoft Graphics コンポーネントの脆弱性により、リモートでコードが実行される（3078662）」（https://technet.microsoft.com/ja-jp/library/security/ms15-080.aspx）。
＊9 「マイクロソフト セキュリティ情報 MS15-097 - 緊急 Microsoft Graphics コンポーネントの脆弱性により、リモートでコードが実行される（3089656）」（https://technet.microsoft.com/ja-jp/library/security/ms15-097.aspx）。
＊10 「マイクロソフト セキュリティ情報 MS15-098 - 緊急 Windows Journalの脆弱性により、リモートでコードが実行される（3089669）（https://technet.microsoft.com/ja-jp/library/security/ms15-098.aspx）。
＊11 「マイクロソフト セキュリティ情報 MS15-065 – 緊急 Internet Explorer用のセキュリティ更新プログラム（3076321）（https://technet.microsoft.com/ja-jp/library/security/ms15-065.aspx）。
＊12 「マイクロソフト セキュリティ情報 MS15-079 - 緊急 Internet Explorer用の累積的なセキュリティ更新プログラム（3082442）（https://technet.microsoft.com/ja-jp/library/security/ms15-079.aspx）。
＊13 「マイクロソフト セキュリティ情報 MS15-094 - 緊急 Internet Explorer用の累積的なセキュリティ更新プログラム（3089548）」（https://technet.microsoft.com/ja-jp/library/security/ms15-094.aspx）。
＊14 「マイクロソフト セキュリティ情報 MS15-070 – 重要 Microsoft Officeの脆弱性により、リモートでコードが実行される（3072620）」（https://technet.microsoft.com/ja-jp/library/security/ms15-070.aspx）。
＊15 「マイクロソフト セキュリティ情報 MS15-081 - 緊急 Microsoft Officeの脆弱性により、リモートでコードが実行される（3080790）」（https://technet.microsoft.com/ja-jp/library/security/ms15-081.aspx）。
＊16 「マイクロソフト セキュリティ情報 MS15-099 - 緊急 Microsoft Officeの脆弱性により、リモートでコードが実行される（3089664）」（https://technet.microsoft.com/ja-jp/library/security/ms15-099.aspx）。

7月のインシデント

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31

他 **1日：協定世界時の調整のため、うるう秒の挿入が日本時間8時59分60秒に行われた。**
独立行政法人情報通信研究機構（NICT）、「2015年7月1日は1日が1秒長い」（http://jjy.nict.go.jp/news/leap-info2015.html）。

他 **2日：金融庁より、金融分野のサイバーセキュリティ強化に向けた5つの方針を定めた「金融分野におけるサイバーセキュリティ強化に向けた取組方針」が公表された。**
「『金融分野におけるサイバーセキュリティ強化に向けた取組方針』の公表について」（http://www.fsa.go.jp/news/27/20150702-1.html）。

セ **6日：イタリアのセキュリティ企業、Hacking Teamが何者かによって侵入され、400GBの内部データがP2Pによって漏えいする事件が発生した。なお、この事件で漏えいした内部情報には、HackingTeamが保有していたFlashPlayerなどの未修正の脆弱性などが含まれていたことから、これらを悪用した攻撃がいくつか発生している。**
この事件については次のHackingTeamの発表を参照のこと。"Information related to the attacks on HackingTeam on July 6, 2015"（http://www.hackingteam.com/index.php/about-us）。

他 **7日：総務省は、IP電話等の電話サービスが不正利用され、利用者に高額な国際電話料金の請求がなされる問題が発生しているとして、電気通信事業者関係団体に対し、不正利用による被害を未然に防止し、被害の拡大を防ぐために適切な対応を講じるよう周知することへの協力を要請した。**
「第三者によるIP電話等の不正利用への対策について（要請）」（http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000096.html）。

脆 **8日：BIND9に、DNSSEC検証が有効に設定しているなど条件を満たしている場合に外部からのDoS攻撃可能な脆弱性が見つかり、修正された。**
JVN、「JVNVU#93531657 ISC BIND 9にサービス運用妨害（DoS）の脆弱性」（https://jvn.jp/vu/JVNVU93531657/）。

脆 **9日：Adobe Flash Playerに、細工したWebサイトを閲覧することで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見つかり、修正された。**
「APSB15-16: 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/apsb15-16.html）。

脆 **11日：Adobe Flash Playerに、細工したWebサイトを閲覧することで不正終了や任意のコード実行の可能性がある脆弱性（CVE-2015-5122）があることが公表された。この脆弱性は7月15日に修正プログラム（APSB15-18）が公表された。**
"APSA15-04 Security Advisory for Adobe Flash Player"（https://helpx.adobe.com/security/products/flash-player/apsa15-04.html）。

セ **11日：米国人事管理局（OPM）は、6月に発生した不正アクセスによる現在の調査状況を公表し、現在及び元や将来の連邦従業員や請負業者などの情報、2,150万人分が漏えいしたことを明らかにした。更に、対応のため専用窓口やコールセンターの設置を行うことも併せて発表している。**
"OPM Announces Steps to Protect Federal Workers and Others From Cyber Threats"（https://www.opm.gov/news/releases/2015/07/opm-announces-steps-to-protect-federal-workers-and-others-from-cyber-threats/）。

脆 **15日：Microsoft社は、2015年7月のセキュリティ情報を公開し、MS15-065やMS15-066、MS15-067を含む4件の緊急と10件の重要な更新の合計14件の修正をリリースした。**
「2015年7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-jul）。

脆 **15日：Adobe Reader及びAcrobatに、不正終了や任意のコード実行の可能性がある複数の脆弱性が見つかり、修正された。**
「APSB15-15: Adobe AcrobatおよびReader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/acrobat/apsb15-15.html）。

脆 **15日：Adobe Shockwave Playerに、攻撃者によって制御されたり、任意のコード実行の可能性がある複数の脆弱性が見つかり、修正された。**
「APSB15-17: Adobe Shockwave Player用セキュリティアップデート公開」（https://helpx.adobe.com/jp/security/products/shockwave/apsb15-17.html）。

脆 **15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見つかり、修正された。**
「APSB15-18: 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/apsb15-18.html）。

脆 **15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25件の脆弱性を含む合計193件の脆弱性を修正した。**
「"Oracle Critical Patch Update Advisory - July 2015"（http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html）。

脆 **21日：Microsoft社は、任意のコード実行の可能性がある脆弱性（CVE-2014-2426）の修正を定例外で公開した。**
「マイクロソフト セキュリティ情報 MS15-078 - 緊急 Microsoft フォント 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（3079904）」（https://technet.microsoft.com/ja-jp/library/security/ms15-078.aspx）。

脆 **27日：Fiat Chrysler Automobiles（FCA）UConnect に車両を遠隔操作することができる脆弱性が見つかり、修正された。なお、この脆弱性については米国で販売されたものだけ該当し、米国ではメーカによるリコールで対応が行われた。**
JVN、「JVNVU#90018179 Fiat Chrysler Automobiles（FCA）UConnect に車両の遠隔操作の脆弱性」（http://jvn.jp/vu/JVNVU90018179/）。

脆 **28日：Android Stagefrightに、攻撃者によってデバイス上のファイルにアクセスされたり、コード実行が可能な複数の脆弱性があることが公表された。**
JVN、「JVNVU#92141772　Android Stagefright に複数の脆弱性」（http://jvn.jp/vu/JVNVU92141772/）。

セ **29日：米国Yahoo!の広告ネットワークを利用し、ユーザをAngler Exploit Kitへと誘導する、大規模なMalvertisingが発生した。**
詳細については、次のMALWAREBYTES CORPORATIONのBlogを参照のこと。"Large Malvertising Campaign Takes on Yahoo!"（https://blog.malwarebytes.org/malvertising-2/2015/08/large-malvertising-campaign-takes-on-yahoo/）。

セ **31日：内閣府NPOホームページのNPOサポートデスクの問い合わせ対応メールアドレスが何者かに乗っ取られ、外部に不正にメールを送信していたことを公表した。**
「【重要なお知らせ】NPOサポートデスク アカウントの不正利用について」（https://www.npo-homepage.go.jp/uploads/20150731.pdf）。

※ 日付は日本標準時

【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

Struts2では、特定の条件を満たした場合に任意のコード実行やXSS可能な脆弱性が複数見つかり、修正されています[*17]。CMSとして利用されるWordPressについても、複数のバージョンでXSSの脆弱性などサイトへの不正侵入の可能性のある複数の脆弱性が見つかり、修正されています。

7月にはFiat Chrysler Automobiles(FCA)の車内システム「Uconnect」に、リモートで自動車の制御を奪われ、ブレーキやステアリング操作など任意の操作が第三者によって行われる可能性のある脆弱性[*18]が公表されています。また、Android端末に、遠隔の攻撃者によって、任意のファイルアクセスや、デバイス上でコードを実行可能な複数の脆弱性が見つかり修正されています。これらの脆弱性については概要のみ公開されていましたが、8月にラスベガスで開催された世界最大のセキュリティカンファレンスであるBlack Hat USA 2015で、発見者からそれぞれ詳細が発表されています。

■ 不正アクセスなどによる情報漏えい

不正アクセスとそれによる情報漏えいも引き続き発生しています。7月には米国の医療機関UCLA Healthが、氏名や病歴などを含む個人情報が記録されているコンピューターネットワークに不正アクセスを受け、およそ450万人の個人情報が流出した可能性があることを発表しています[*19]。9月には米国の医療保険会社が不正アクセスを受け、同じく氏名や社会保障番号などを含む個人データ約1,050万件が漏えいした可能性のある事件が発生しています。6月に発生した、米国人事管理局(OPM)が不正アクセスを受け、約400万人分の連邦政府職員の情報が漏えいした事件では、その後の調査により、連邦職員や請負業者などの情報、2,150万人分が漏えいしていたことや、最大で560万人分の登録されていた指紋データが漏えいした可能性があることなどが公表されています[*20]。

日本でも、7月に教育関連会社のWebサイトが不正アクセスを受け、最大22,108人分の情報が流出した可能性のある事件が発生しています。同じく7月には旅行関連会社のWebサイトが不正アクセスを受け、会員登録されたメールアドレスとパスワード、約8,400件が流出した可能性のある事件が発生しました。これ以外にも、玩具会社のWebサイトからオンラインショップに登録されていた個人情報など約10万件が漏えいする事件が発生したり、食品会社やギフト会社など、事業分野や規模を問わず、SQLインジェクションなどのアプリケーションの脆弱性を悪用したWebサイトへの不正アクセスとそれによる個人情報の流出事件が多く発生しました。

国内の企業・組織のWebサイトに対しては、このような不正アクセスによる情報漏えいだけでなく、不正アクセスによるWebサイト改ざんによるマルウェアのへの誘導や、標的型攻撃のC&Cサーバとして悪用されたりする事例が6月以降確認されているとして、IPAとJPCERT/CCから、Webサイトの管理者向けに確認すべき項目や点検の頻度など、運用上留意すべき点について具体的に示した注意喚起が行われています[*21]。

■ 標的型攻撃によるマルウェア感染と情報漏えい

この期間でも、組織内部の端末へのマルウェア感染とそれによる情報漏えいなどの事件が相次ぎました。7月には、大学で業務用PCがメールに添付されていたマルウェアに感染したことで、学生の個人情報など36,300件の情報が漏えいした可能性のあることが公表されました。8月には、鉄道会社で、顧客を装った標的型メールによるマルウェア感染が発生し、内部の複数の業務PCがマルウェアに感染していたことが公表されています。6月に発生した日本年金機構の個人情報流出事件については、8月に複数の組織から検証報告書が公表され、事件対応についての検証と今後の再発防止に向けた情報セキュリティ対策の強化について、それぞれの立場から総括が行われました。

*17 The Apache Software Foundation、"Apache Struts 2 Documentation S2-025 Cross-Site Scripting Vulnerability in Debug Mode and in exposed JSP files"(https://struts.apache.org/docs/s2-025.html)。
*18 詳細については、次の脆弱性の発表者が公開したホワイトペーパーを参照のこと。"Remote Exploitation of an Unaltered Passenger Vehicle"(http://illmatics.com/Remote%20Car%20Hacking.pdf)。
*19 UCLA Health、"UCLA Health Victim of a Criminal Cyber Attack"(https://www.uclahealth.org/news/ucla-health-victim-of-a-criminal-cyber-attack)。
*20 "Statement by OPM Press Secretary Sam Schumach on Background Investigations Incident"(https://www.opm.gov/news/releases/2015/09/cyber-statement-923/)。
*21 IPA・JPCERT/CC、「注意喚起『ウェブサイトへのサイバー攻撃に備えた定期的な点検を』」(http://www.jpcert.or.jp/pr/2015/pr150003.html)。

8月のインシデント

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

脆 **5日：CMSアプリケーションのWordPressにXSSの脆弱性などサイトへの不正侵入の可能性のある複数の脆弱性が見つかり、修正された。**
WordPress.org、「WordPress 4.2.4 セキュリティとメンテナンスのリリース」(https://ja.wordpress.org/2015/08/06/wordpress-4-2-4-security-and-maintenance-release/)。

他 **5日：IPAより、標的型サイバー攻撃の被害拡大防止のため、被害の低減と攻撃の連鎖の遮断を支援する目的で発足したサイバーレスキュー隊(J-CRAT)の活動報告が公表された。**
「サイバーレスキュー隊(J-CRAT)の活動報告」(http://www.ipa.go.jp/files/000047193.pdf)。

セ **6日：ICANNは、Webサイトに登録されていたユーザ名やメールアドレスと暗号化されたパスワードが流出した可能性があるとしてパスワードのリセットを実施したことを公表した。**
"Reset ICANN.org Website Login Password"(https://www.icann.org/news/announcement-2015-08-05-en)。

脆 **7日：Android端末の多くにインストールされているモバイル遠隔サポートツール(mRST)の認証に脆弱性(Certifi-gate)があり、悪意のあるアプリケーションを使ってユーザデータへのアクセスが可能となる脆弱性が公表された。**
詳細については、次のCheck Point Blogを参照のこと。"Certifi-gate：Hundreds of Millions of Android Devices Could Be Pwned"(http://blog.checkpoint.com/2015/08/06/certifigate/)。

脆 **12日：Microsoft社は、2015年8月のセキュリティ情報を公開し、MS15-079、MS15-080、MS15-081、MS15-091の4件の緊急と10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8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-Aug)。

脆 **12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見つかり、修正された。**
「APSB15-19: 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/apsb15-19.html)。

セ **12日：Cisco社は、IOSデバイスに管理者権限でアクセスし、悪質なROMMONイメージをインストールする攻撃が確認されたとして注意喚起を行った。**
"Evolution in Attacks Against Cisco IOS Software Platforms"(http://tools.cisco.com/security/center/viewAlert.x?alertId=40411)。

脆 **14日：Apple社は、OS Xについて複数の脆弱性の修正を含むアップデートを公開した。**
「OS X Yosemite v10.10.5 およびセキュリティアップデート 2015-006のセキュリティコンテンツについて」(https://support.apple.com/ja-jp/HT205031)。

脆 **17日：イタリアのセキュリティ研究者により、OS Xの未修正の複数の脆弱性がPoCと共に公表された。**
この脆弱性は他の脆弱性と併せ、10月1日に「OS X El Capitan v10.11のセキュリティコンテンツについて」(https://support.apple.com/ja-jp/HT205267)で修正されている。

脆 **18日：古い無線LANルータに、SSDPリフレクター攻撃の踏み台にされ、DDoS攻撃に利用される可能性のあることが分かり、修正などの対応が行われた。なお、1つの製品についてはサポートが終了しているとして使用停止が呼び掛けられている。**
JVN、「JVN#17964918　複数のアイ・オー・データ製ルータにおけるUPnPに関する脆弱性」(https://jvn.jp/jp/JVN17964918/index.html)。

脆 **19日：Microsoft社は、Internet Explorerに細工されたWebページの閲覧による任意のコード実行の可能性がある脆弱性(CVE-2015-2502)が見つかったとして、修正を公開した。**
「マイクロソフト セキュリティ情報 MS15-093 - 緊急 Internet Explorer 用のセキュリティ更新プログラム(3088903)」(https://technet.microsoft.com/ja-jp/library/security/ms15-093.aspx)。

他 **20日：日本年金機構で6月に発生した個人情報流出事件についての検証報告書が日本年金機構や関係省庁からそれぞれ公表された。**
それぞれの報告書については次を参照のこと。内閣サイバーセキュリティセンター、「日本年金機構における個人情報流出事案に関する原因究明調査結果」(http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf)。日本年金機構、「不正アクセスによる情報流出事案に関する調査結果報告書」(http://www.nenkin.go.jp/files/e7wRRjRfiKiN1.pdf)。厚生労働省(8月21日発表)、「日本年金機構における不正アクセスによる情報流出事案検証委員会検証報告書」(http://www.mhlw.go.jp/kinkyu/dl/houdouhappyou_150821-02.pdf)。

セ **25日：米国のGitHub社がDDoS攻撃を受け、サービス提供に障害が発生した。**
この攻撃については次のGitHub社のStatusページ(https://status.github.com/messages/2015-08-26)で確認できる。

セ **29日：英国国家犯罪対策庁(NCA)はLizard Stresserを利用してDDoS攻撃を行った容疑で未成年6人を逮捕もしくは事情聴取していることを公表した。**
National Crime Agency(NCA)、"Operation Vivarium targets users of Lizard Squad's website attack tool"(http://www.nationalcrimeagency.gov.uk/news/691-operation-vivarium-targets-users-of-lizard-squad-s-website-attack-tool)。

※ 日付は日本標準時

【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

■ 動静や歴史的背景による攻撃

この期間では毎年、太平洋戦争の歴史的日付や、竹島や尖閣諸島などに関連したインシデントが発生しています。本年もこれらに関連した日本国内の複数の政府機関や民間企業のWebサイトに対し、SQLインジェクションや不正アクセスによるWebサイトの改ざんやDDoS攻撃が発生することが予測されたため、警戒を行いました。DDoS攻撃については、平常時よりも若干多く見られましたが、大規模な攻撃については確認されておらず、攻撃の規模や回数は過去の同期間に比べると減少しています。

■ 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、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が閣議決定しています。この中では、2020年東京オリンピック・パラリンピックを踏まえた今後3年程度の基本的な施策の方向性を示しており、6月に発生した日本年金機構の個人情報流出事件を踏まえ、政府機関全体としてサイバーセキュリティを強化するため、内閣サイバーセキュリティセンター(NISC)の機能強化と共に、監視対象に独立行政法人や府省庁と一体となり公的業務を行う特殊法人などを含むことで、対策の総合的な強化を図ることが新たに掲げられました。また、サイバーセキュリティ戦略の決定を受け、これにに基づく最初の年次計画となるサイバーセキュリティ2015がサイバーセキュリティ戦略本部で決定しています[*22]。

6月に日本年金機構で発生した個人情報流出事件については、8月にNISCと厚生労働省から検証報告書がそれぞれ公表されています。これを受け、サイバーセキュリティ戦略本部から厚生労働大臣に対して、サイバーセキュリティ基本法第27条第3項に基づき、年金機構への監督強化や厚生労働省の担当部署の役割や責任の明確化、インシデント発生時の緊急体制の整備などの勧告が行われました。

9月には、「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(マイナンバー法)」と「個人情報保護法」の改正がそれぞれ衆議院で可決成立しています。マイナンバー法では、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行われました。マイナンバー法については10月に施行されましたが、平成28年1月から開始される個人番号カードの交付など本格運用に向け、特定個人情報の漏えい事案などが発生した場合の対応について[*23]などのガイドラインが特定個人情報保護委員会から公表されています[*23]。個人情報保護法では、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ました[*23]。

同じく9月には、総務省の「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」より、第二次取りまとめが策定されています。今回の取りまとめでは、マルウェア感染端末の利用者に対する注意喚起の実施や、C&Cサーバなどとの通信遮断などについて整理が行われました。これを受け、研究会の検討結果を通信事業の実務上の状況に適用させるためのガイドライン[*24]の改訂が、インターネットの安定的運用に関する協議会などの場で進められることになります。

■ その他

7月には、イタリアのセキュリティ企業Hacking Teamが攻撃を受け、400GBもの内部資料が漏えいする事件が発生しています。また、この企業の公式Twitterアカウントも乗っ取りを受け、盗みだされた資料が発信されるなどしています。この企業は各国政府や法執行機関向けに、PCやスマートフォンなどを対象とした監視ツールを販売していました。盗まれた情報はBitTorrentでも公開され、同社の顧客リストや電子メールの内容なども含まれていたことから、アジア、欧州、北米、南米、アフリカなど世界各国の多数の国家や情報機関が顧客だったことが明らかになっています。更に、漏えいした内部資料から、Adobe社のAdobe Flash PlayerやMicrosoft社のWindows[*25]などの複数の未修正の脆弱性が見つかったことから、これらの脆弱性の修正が実施されるなど、対応が行われています。

＊22 内閣サイバーセキュリティセンター(NISC)、「サイバーセキュリティ戦略本部 5回会合(持ち回り開催)(平成27年9月25日)」(http://www.nisc.go.jp/conference/cs/index.html#cs05)。
＊23 マイナンバー制度に対する法令やガイドラインについては、次の特定個人情報保護委員会のWebサイト(http://www.ppc.go.jp/)なども参照のこと。
＊24 「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン(第3版)」(http://www.soumu.go.jp/main_content/000362139.pdf)。
＊25 「マイクロソフト セキュリティ情報 MS15-078 - 緊急 Microsoft フォント 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(3079904)」(https://technet.microsoft.com/ja-jp/library/security/ms15-078.aspx)。

9月のインシデント

1 セ 1日：英国国家犯罪対策庁（NCA）がLizard SquadによるDDoS攻撃を受け、一時的に閲覧できなくなるなどの影響が出た。8月にNCAが実施したLizard Stresserユーザが逮捕されたことへの報復と考えられる。

2

3 脆 3日：BIND9のDNSSECのRDATA処理に外部からのDoS攻撃可能な複数の脆弱性が見つかり、修正された。
Internet Systems Consortium、"CVE-2015-5986: An incorrect boundary check can trigger a REQUIRE assertion failure in openpgpkey_61.c"（https://kb.isc.org/article/AA-01291）。

4

5 他 4日：サイバー空間に対する我が国の方針を内外に明確化し、2020年東京オリンピック・パラリンピックに向けた今後3年程度の基本的な施策の方向性を示したサイバーセキュリティ戦略が閣議決定した。
内閣サイバーセキュリティセンター（NISC）、「サイバーセキュリティ戦略について」（http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf）。

6

7

8 セ 5日：和歌山県太地町の公式Webサイトに対し、イルカや小型クジラの追い込み漁への抗議活動から、AnonymousによるDoS攻撃が行われ、一時閲覧できなくなるなどの影響が出た（OpKillingBay）。

9

10 脆 9日：Adobe Shockwave Playerに、任意のコード実行の可能性がある複数の脆弱性が見つかり、修正された。
「APSB15-22: Adobe Shockwave Player用セキュリティアップデート公開」（https://helpx.adobe.com/jp/security/products/flash-player/apsb15-18.html）。

11 脆 9日：Microsoft社は、2015年9月のセキュリティ情報を公開し、MS15-094とMS15-095、MS15-099など5件の緊急と7件の重要な更新を含む合計12件の修正をリリースした。
「2015年9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-sep）。

12

13 他 9日：総務省より、電気通信事業者が通信の秘密等に配慮しつつ、新たな対策や取組を講じていくことが可能となるよう、電気通信事業におけるサイバー攻撃への適正な対処の在り方について検討を行っていた「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 第二次とりまとめ」が公表された。
「『電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 第二次とりまとめ』及び意見募集の結果の公表（総務省）」（http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000100.html）。

14

15

16 他 11日：サイバーセキュリティ戦略本部長から厚生労働大臣に対して、日本年金機構における個人情報流出事案に対する調査結果を踏まえ、サイバーセキュリティ基本法第27条第3項に基づく勧告が行われた。勧告では情報セキュリティ確保及び情報セキュリティ事案における対処のための体制整備や技術的対策、職員などに対する教育・訓練の実施、成果の評価と報告が求められている。
内閣サイバーセキュリティセンター（NISC）、「サイバーセキュリティ基本法第27条第３項に基づく勧告について」（http://www.nisc.go.jp/press/pdf/kankoku20150911_press.pdf）。

17

18 脆 16日：CMSアプリケーションのWordPressにXSSの脆弱性などサイトへの不正侵入の可能性のある複数の脆弱性が見つかり、修正された。
WordPress.org、「WordPress 4.3.1 セキュリティとメンテナンスのリリース」（https://ja.wordpress.org/2015/09/17/wordpress-4-3-1/）。

19

20 動 18日：毎年、歴史的な要因により、この日の前後に発生していた攻撃については、小規模な攻撃はあったが組織的な攻撃は見られなかった。

21

22

23 脆 23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見つかり、修正された。
「APSB15-23: 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/apsb15-23.html）。

24

25 他 25日：北米のインターネットアドレスの管理を行っているAmerican Registry for Internet Numbers（ARIN）は、割り当てられるIPv4アドレスのストックが枯渇したことを発表した。今後は待機リストに従って割り当てが行われる。
詳細については、"ARIN IPv4 Free Pool Reaches Zero"（https://www.arin.net/announcements/2015/20150924.html）を参照のこと。

26

27 他 25日：サイバーセキュリティ戦略本部の会合が行われ、サイバーセキュリティ戦略に基づく年次計画であるサイバーセキュリティ2015が決定した。
「サイバーセキュリティ戦略本部 5回会合（持ち回り開催）（平成２７年９月２５日）」（http://www.nisc.go.jp/conference/cs/index.html#cs05）。

28

29

30 他 30日：警察庁は、平成27年上半期のサイバー犯罪の傾向などをまとめた「平成27年上半期のサイバー空間をめぐる脅威の情勢について」を公表した。
「平成27年上半期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/H27_kami_jousei.pdf）。

※ 日付は日本標準時

【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

内閣府の関連サイトでは、サポートの問い合わせ対応用メールアドレスが何者かに乗っとられ、外部に約2万件のSPAMメールを不正送信する事件が発生しています。この事件では、短く推測されやすいパスワードを委託事業者が使用していた可能性が指摘されています。

9月には、Mandiant社とFireEye社が、改ざんされたファームウェアをインストールされたCisco社製のルータ製品を発見したことを発表しています[*26]。これは脆弱性によるものではなく、認証設定がデフォルトのままのルータなど、不適切な管理が行われている機器にマルウェアがインストールされていたものと考えられます。この攻撃については8月にCisco社から注意喚起が行われていましたが、その後に発表されたミシガン大学など学術機関の研究グループによる調査では、19ヵ国で79件発見されるなど[*27]、感染が拡がっています。

同じく9月には、Googleドメインの EV-SSL証明書が不正に発行される事件が発生しましたが、これは、発行者が誤って内部テスト用に発行した証明書だったとされています。Google社はこの証明書を失効情報に登録し無効化を行っています[*28]。

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

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

DDoS攻撃には多くの攻撃手法が存在し、攻撃対象となった環境の規模(回線容量やサーバの性能)によって、その影響度合が異なります。図-2では、DDoS攻撃全体を、回線容量に対する攻撃[*29]、サーバに対する攻撃[*30]、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。

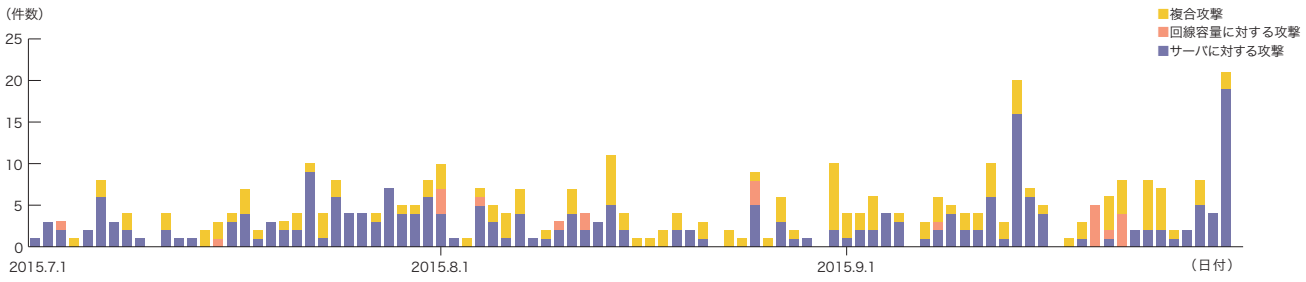


図-2 DDoS攻撃の発生件数

*26 この攻撃についての詳細は、次のFireEye社のBlogなどを参照のこと。"SYNful Knock - A Cisco router implant - Part I"(https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html)、"SYNful Knock - A Cisco router implant - Part II"(https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis0.html)。
*27 ZMap、"In Search of SYNful Routers"(https://zmap.io/synful/)。
*28 Google Online Security Blog、"Improved Digital Certificate Security"(https://googleonlinesecurity.blogspot.jp/2015/09/improved-digital-certificate-security.html)。
*29 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。
*30 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。

この3ヵ月間でIIJは、400件のDDoS攻撃に対処しました。1日あたりの対処件数は4.35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59.3%、複合攻撃が34.9%、回線容量に対する攻撃が5.8%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28万9千ppsのパケットによって4.5Gbps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81.5%が攻撃開始から30分未満で終了し、17.8%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0.7%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2日と22時間35分(70時間35分)にわたりました。

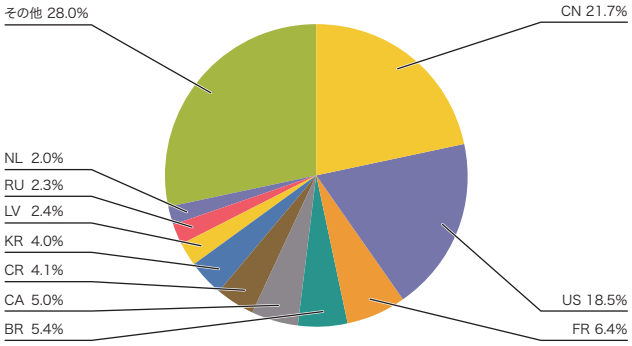


図-3 DDoS攻撃のbackscatter観測による攻撃先の国別分類

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[*31]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[*32]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[*33]によるDDoS攻撃のbackscatter観測結果を示します[*34]。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7月から9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。

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DNSで利用される53/UDPで、全パケット数の53.2%を占めています。次いでWebサービスで利用される80/TCPが20.6%を占めており、上位2つで全体の73.8%に達しています。また、HTTPSで利用される443/TCP、SSHで利用される22/TCP、ゲームの通信で利用されることがある25565/TCPや27015/UDPへの攻撃、通常は利用されない3306/UDPや51127/TCPなどへの攻撃が観測されています。

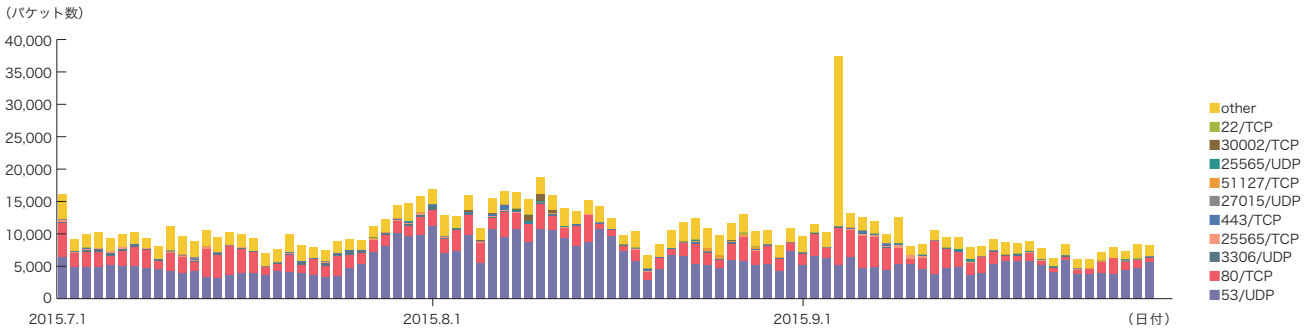


図-4 DDoS攻撃によるbackscatter観測(観測パケット数、ポート別推移)

*31 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。
*32 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。
*33 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。
*34 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。

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約5,800と、前回の約5,600とほぼ変化なく、引き続き高止まりの状態にあります。

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、中国の21.7%が最も大きな割合を占めています。その後に米国の18.5%、フランスの6.4%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及び443/TCP)への攻撃としては、7月1日に米国ホスティング事業者への攻撃、7月13日から17日にかけてカナダのホスティング事業者のサーバ群に対する攻撃、8月7日にはフランスとドイツのゲーム関連サイトへの攻撃、9月4日から10日にかけて米国CDN事業者のサーバ群への攻撃を観測しています。他のポートへの攻撃としては、8月21日から27日にかけてカナダのホスティング事業者のサーバに対する22/TCP、8080/TCP、22/UDPなどへの攻撃、9月5日から11日にかけてフランスのゲームサーバに対する25565/TCPへの攻撃を観測しています。また、9月4日にはラトビアにある特定のサーバに対する様々なポートへの大量の攻撃を観測しています。

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、7月10日から12日にかけてドイツに本社を置くインスタントメッセージングサービス事業者のサーバ群への攻撃、7月18日にカナダ連邦警察のサイトへの攻撃、8月18日にウクライナの右派団体関連サイトへの攻撃、8月25日にGitHubへの攻撃をそれぞれ検知しています。

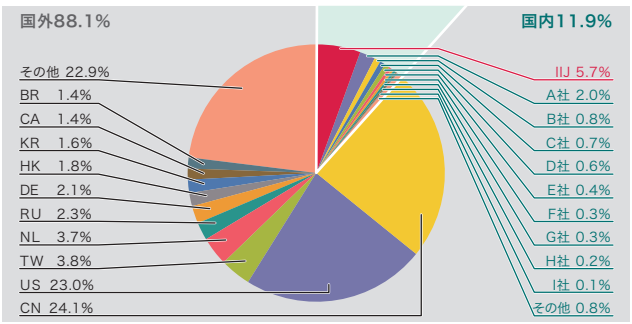


図-5 発信元の分布(国別分類、全期間)

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[*35]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[*36]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

2015年7月から9月の期間中に、ハニーポットに到着した通信の発信元IPアドレスの国別分類を図-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

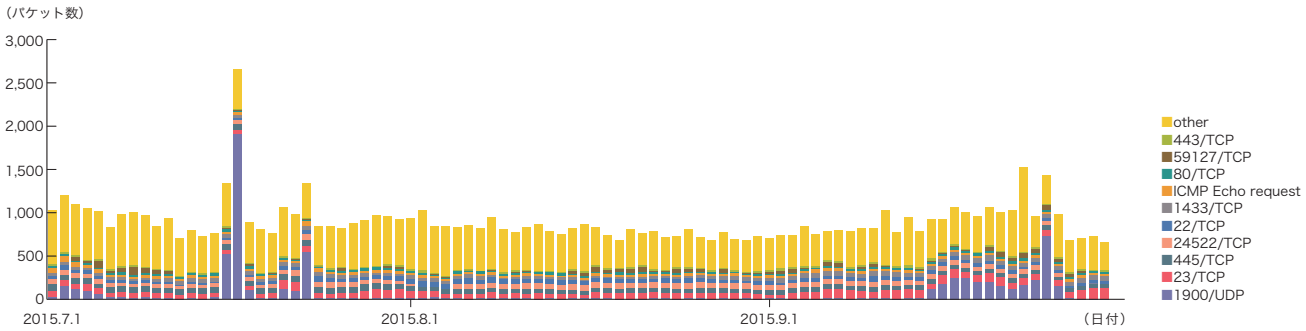


図-6 ハニーポットに到着した通信の推移(日別・宛先ポート別・1台あたり)

*35 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。
*36 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。

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。

本レポートの期間中にハニーポットに到着した通信の多くは、UPnPのSSDPプロトコルで使われる1900/UDP、telnetで使われる23/TCP、sshで使われている22/TCP、Microsoft社のOSで利用されている445/TCP、同社のSQL Serverで利用される1433/TCP、Webサーバで使われる80/TCP、443/TCPなどでした。

SSDPプロトコルである1900/UDPが断続的に増加しています。例えば、7月16日から17日にかけては米国、7月23日にはオランダ、9月中旬から下旬にかけては米国、オーストラリア、カナダなどに割り当てられたIPアドレスからSSDPの探査要求を受けています。これらは、SSDPリフレクターを使ったDDoS攻撃に利用可能な機器を探査する通信であると考えられます。

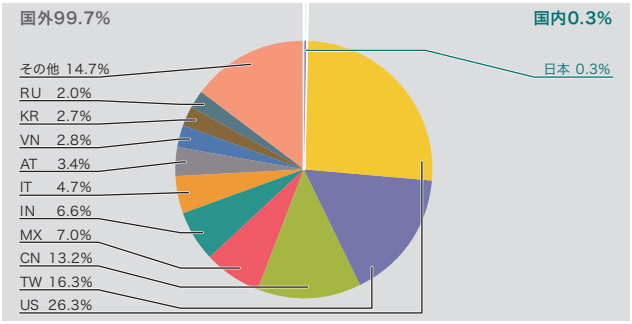


図-7 検体取得元の分布（国別分類、全期間、Conficker除く）

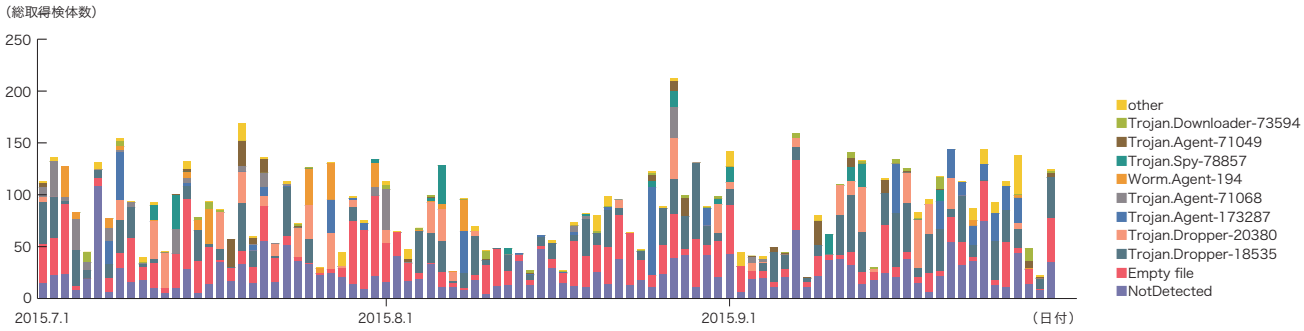


図-8 総取得検体数の推移（Conficker除く）

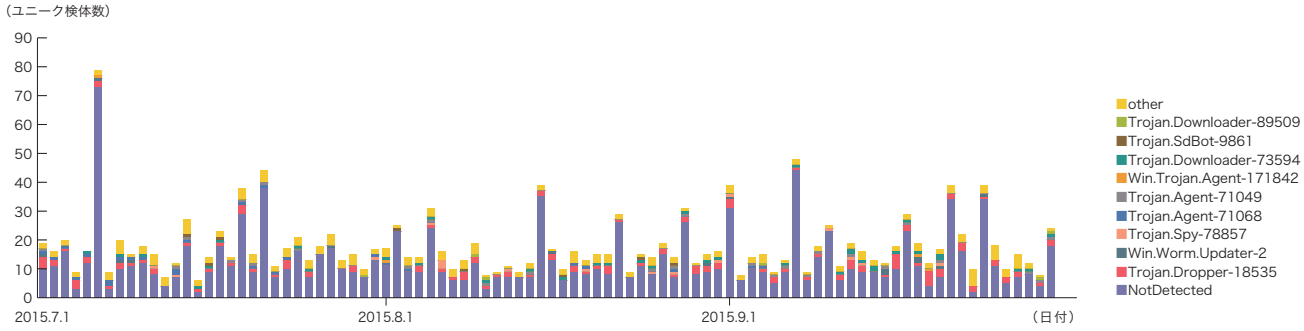


図-9 ユニーク検体数の推移（Conficker除く）

■ ネットワーク上のマルウェアの活動

同じ期間中でのマルウェアの検体取得元の分布を図-7に、マルウェアの総取得検体数の推移を図-8に、そのうちのユニーク検体数の推移を図-9にそれぞれ示します。このうち、図-8と図-9では、1日あたりに取得した検体[*37]の総数を総取得検体数、検体の種類をハッシュ値[*38]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。

期間中の1日あたりの平均値は、総取得検体数が89、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結果、中国、台湾、オーストリア、米国、タイ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、台湾においてIRCをC&Cサーバ[*39]とするBotも観測されています[*40]。

未検出の検体の約53%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サイトが既に閉鎖させられていると考えられます。

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84.6%、ボット型6.4%、ダウンローダ型9.0%でした。また解析により、102個のボットネットC&Cサーバと7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サーバの数が以前よりも高くなっていますが、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27,935、ユニーク検体数は543でした。7月に米国からの感染が増加したものの、その後は減少に転じており、短期間での増減を繰り返しながら、総取得検体数で99.5%、ユニーク検体数で98.8%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比較し、約44%増加し、ユニーク検体数は前号から約10%減少しました。総取得権対数の増加は、本レポートの期間中、米国に割り当てられたIPアドレスからの感染活動が増加したためです。Conficker Working Groupの観測記録[*41]によると、2015年10月1日現在で、ユニークIPアドレスの総数は675,680とされています。2011年11月の約320万台と比較すると、約21%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。

＊37 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。
＊38 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。
＊39 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。
＊40 WORM_SDBOT.FJK(http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=jp&name=WORM_SDBOT.FJK)。
＊41 Conficker Working Groupの観測記録(http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTrackingblank)。

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[*42]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。

2015年7月から9月までに検知した、Webサーバに対するSQLインジェクション攻撃の発信元の分布を図-10に、攻撃の推移を図-11にそれぞれ示します。これらは、IIJマネージドIPSサービスのシグネチャによる攻撃の検出結果をまとめたものです。発信元の分布では、日本28.2%、米国28.1%、中国20.3%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、日本や米国からの攻撃が増加したためです。

この期間中、7月18日には中国とドイツ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。これとは別の攻撃先に対して、英国やドイツ、トルコ、米国といった比較的広範囲の攻撃元から特定の攻撃先について攻撃が発生していました。7月24日には特定の攻撃元より、複数の特定の攻撃先への攻撃が発生しました。別に、米国とオランダの特定の攻撃元から特定の攻撃先への攻撃も発生しています。8月1日には中国の特定の攻撃元から特定の攻撃先への攻撃が発生しています。これとは別の攻撃先に対して、米国の特定の攻撃元からの攻撃も発生しています。9月17日には中国の特定の攻撃元より、特定の攻撃先への攻撃が発生しています。これらの攻撃は、Webサーバの脆弱性を探る試みであったと考えられます。

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

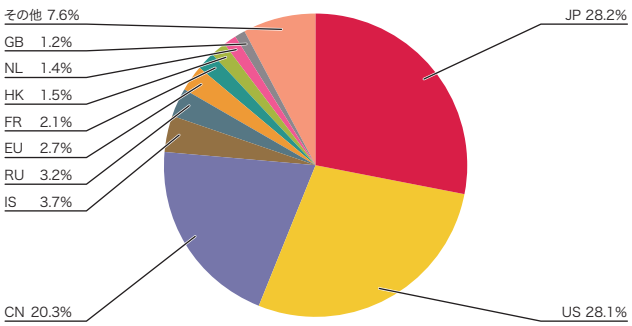


図-10 SQLインジェクション攻撃の発信元の分布

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[*43]。

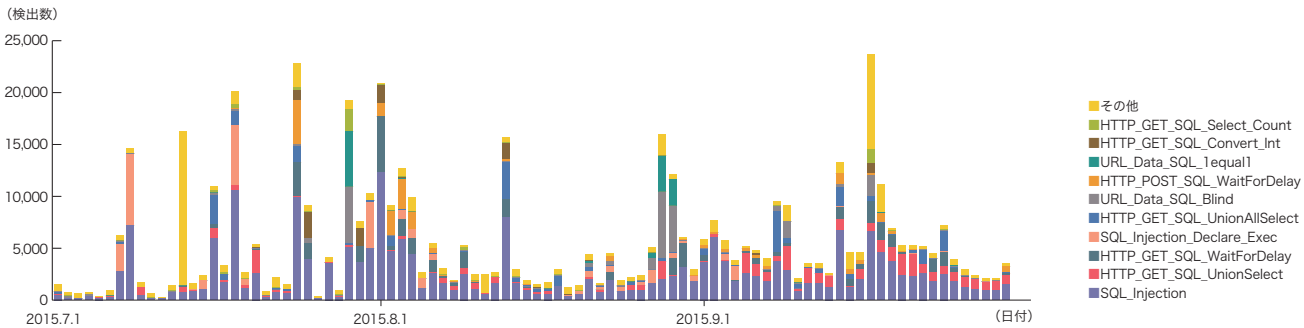


図-11 SQLインジェクション攻撃の推移（日別、攻撃種類別）

*42 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。

*43 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 Webサイト改ざん調査」で仕組みを紹介している。

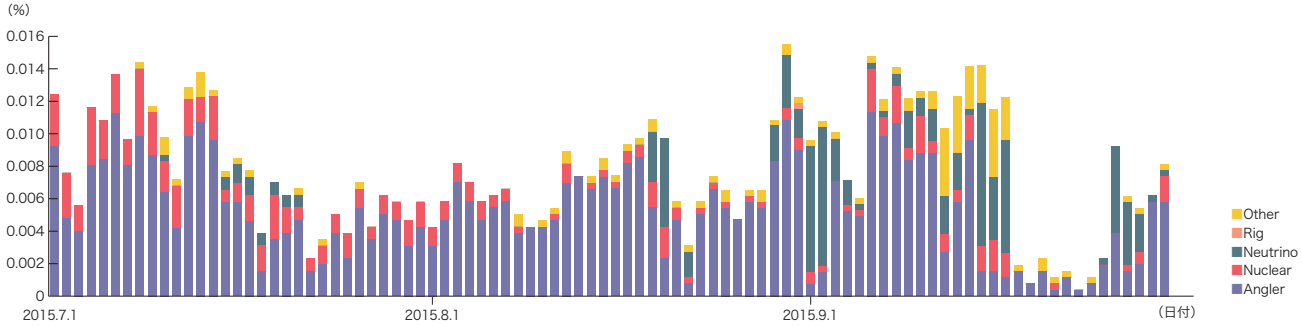
このWebクローラは、国内の著名サイトや人気サイトなどを中心とした数十万のWebサイトを日次で巡回しており、更に巡回対象を順次追加しています。また、一時的にアクセス数が増加したWebサイトなどを対象に、一時的な観測も行っています。一般的な国内ユーザによる閲覧頻度が高いと考えられるWebサイトを巡回調査することで、改ざんサイトの増減や悪用される脆弱性、配布されるマルウェアなどの傾向が推測しやすくなります。

2015年7月から9月の期間は、Anglerが猛威を振るいました(図-12)[*44]。ドライブバイダウンロード攻撃の総数は、2015年4月から6月に集計した値に比べて10倍近くになっています。期間を通じて、攻撃の大部分をAnglerが占めていますが、8月下旬には、それまでAnglerを用いていた攻撃主体が、一部でNeutrinoを用いるようになりました。以降は、同じ改ざんWebサイトから、タイミングなどによりAnglerとNeutrinoのいずれかのExploitKitによる攻撃が観測されるようになりました。日ごとにこの両者の比率が変動する様子は、攻撃主体が複数の攻撃ツールを天秤にかけているようにも見えます。

ダウンロードされるマルウェアは、9月初頭まではTeslaCrypt2.0が多くを占めていましたが、以降はCryptoWall3.0が取って代わり、TeslaCrypto2.0は検知されなくなりました。また、AnglerやNeutrinoの一部の攻撃では、BedepやNecursがダウンロードされるケースも観測されました。

なお、9月18日から9月25日にかけて、攻撃の検知数が激減しています。この期間、改ざんされたWebサイトからExploitKitやそのRedirectorへ誘導するリンクが削除されたり、Redirectorから次段のInfectorへの誘導が行われないケースなどが複数確認されました。攻撃主体の意図は不明ですが、その後、検知件数は再び増加傾向になりました。

ドライブバイダウンロードによる攻撃がきわめて多く発生している状況が継続しています。改ざんされたWebサイトだけでなく、Webサイトに掲載している広告コンテンツを経由してInfectorへと誘導される(Malvertising)ケースも多数確認されています[*45]。Webサイト運営者は、Webコンテンツの改ざん対策に加えて、広告や集計サービスなど、外部の第三者から提供されるマッシュアップコンテンツを適切に管理することが求められます。コンテンツ提供者のセキュリティ方針や、その評判などを把握しておくことを推奨します。また、ブラウザ利用環境では、OSやブラウザ関連プラグインの脆弱性をよく確認し、更新の適用やEMETの有効化などの対策を徹底することが重要です。



※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)

＊44 2015年7月のAngler観測状況や、その機能については本レポートのVol.28(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol28.pdf)の「1.4.2 猛威を振るうAngler Exploit Kit」で詳しく紹介している。
＊45 例えばMalware「Large Malvertising Campaign Goes (Almost) Undetected」(https://blog.malwarebytes.org/malvertising-2/2015/09/large-malvertising-campaign-goes-almost-undetected/)などでも同時期のMalvertisingについて言及されている。

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つなげています。ここでは、これまでに実施した調査のうち、経路ハイジャックとTLS1.3最新動向の2つのテーマについて紹介します。

1.4.1 経路ハイジャック

2015年1月、IIJ管理下のあるIPv4アドレスブロックが、第三者によって不正にインターネットで経路広告されていることが分かりました。これを受けて、IIJでは即座に対応と原因の調査を行いました。ここでは、不正な経路広報の現状や今回の事例から得られた知見について解説します。

■ 経路制御の仕組み

IPアドレスはインターネットで通信する際に通信機器を識別し、通信先を指し示すために使われています。無論、IPアドレスが重複するとうまく通信できなくなってしまうので、その一意性を担保するためにインターネットでは階層的管理構造を持つインターネットレジストリ(IR)がIPアドレスの分配を担っています。日本では多くの場合、アジア太平洋地域の地域別IR(RIR)であるAPNICか、日本の国別IR(NIR)であるJPNICに申請してIPアドレスの分配を受けています。

APNICやJPNICはIPアドレスの分配とそれに付随する登記情報の管理までは担いますが、そのIPアドレスを利用した際の到達性などは、分配を受けた側が担うことになります。インターネットで到達性を確保するためには、利用するIPアドレスブロックの情報を他のネットワークに通知する必要があります。現在は、BGPという経路制御プロトコルがネットワーク間の経路制御で標準的に利用されているため、各ネットワークはBGPを用いてそれぞれで利用しているIPアドレスブロックの情報を生成し、他のネットワークに通知しています。これを経路広告と呼びます。この経路広告を受けた他のネットワークでは、そのIPアドレスブロック宛のIPパケットを経路広告したネットワークに向けて転送するようになります。実際にはそれぞれのネットワークでBGPの経路制御ポリシーがあり、異なる経路で同一宛先からの経路広告を受信した場合、ルータで優先度などから最適経路として選択された経路のみがパケット転送に利用されています。

BGPの経路広告自体はとても簡単な作業で、ルータに数行のコマンドを追加するだけで完了しますし、その仕様上、誰でもどんな経路でも広報できます。また、一旦広告された経路情報は経路広告したネットワークで取り消されるまで有効な経路情報として利用されます。つまり、間違って経路広告された情報は瞬時に世界に流通し、明示的に設定を取り除くまでは残り続けてしまうのです。このため、新たに経路広告する際は設定ミスや確認ミスがないように細心の注意が必要です。しかし、インターネットの広がりと共に世界の様々なネットワークがBGPで経路交換しているため、どうしてもどこかで間違いは発生する可能性があります。また、BGPで経路交換しているルータが悪意ある人間に乗っ取られた場合、勝手に経路広告される可能性もあります。各ネットワークで運用しているルータはアクセス制御や監視、定期的な設定の監査を通じて、適切に運用されてることを確認しておくことが重要です。

■ 経路のセキュリティ

設定ミスを削減、また不正な経路広報の影響を軽減するために幾つかの手段があります。まず、経路広告する際には、そのIPアドレスブロックを経路広告する正当性を確認します。APNICやJPNICなどのIRは分配したIPアドレスの登記情報をwhoisで公開しているため、これを参照して分配を受けた組織とIPアドレスブロックに間違いがないか確認できます。また、不正な経路情報の流通を防ぐため、経路フィルタをネットワークの相互接続箇所に導入することも有効です。特に、トランジットと呼ばれる経路情報の中継を提供しているネットワークで受信経路に厳密な経路フィルタを適用することで、不正な経路情報の影響範囲を局所化することができます。このため、トランジットを提供する組織では、顧客が広報する予定のIPアドレスブロックの情報を事前に通知してもらい、それに応じて経路フィルタを更新するような運用をしている場合が多いです。それでも現実には不正な経路広告の発生が絶えません。これらの事象は「経路ハイジャック」と呼ばれることもありますが、報告される多くの事象は広報直後に訂正したと思われる経路広報が多く、意図しない設定ミスによるものがほとんどと推測されており、全般の実情を表すなら「権威なき経路広告」程度の表現が妥当だと考えています。

これら権威なき経路広告も到達性に影響を及ぼすことがあるので、発生次第検知する必要があります。検出に関しては世

界で様々な取り組みが行われており、日本国内ではTelecom-ISAC JapanとJPNICが協力して経路ハイジャック検知システム「経路奉行」を運営しています。経路奉行はJPNICが運営するインターネットルーティングレジストリ（IRR）であるJPIRRに登録されたrouteオブジェクトを正常な経路状態として判断基準に採用し、これと日本国内のISPからシステムに提供されているBGP経路情報とを逐次比較して異常経路を判別するシステムです。routeオブジェクトで登録された広報元と異なる広報元から経路が広報された場合に異常と判別しており、設定ミスによる異常経路を検出するには有用なシステムです。また日本国内のISPから経路情報を得ていることから、日本国内での影響をある程度推測することもできます。IIJも当初からこのシステムの運用に加わっており、より良い検出に向けて活動を続けています。また、IIJ自身の経路を監視するために利用者としてもシステムを利用しており、実際過去にIIJが広報している経路を他ネットワークから広報された際には経路奉行からの警報を受信して対応を行っています。

検出システムで不正な経路広告を分類することは難しい作業です。例えば、経路奉行ではrouteオブジェクトの登録ミスなどによっても異常として検出しますが、これは、外部からはIPアドレスブロックの管理者が、どこでどんな利用を意図しているか分からないことから、この設定が正常かどうかの確認が困難なため、経路ハイジャックの"疑われる"事例としています。また、不正な経路広告の発生源から原因の報告を受けることも稀です。Telecom-ISAC Japanで共有されている事例でも、検出に基づいて経路広告元のネットワークに問い合わせをしても「修正しました」との回答だけで、発生理由については現場の設定ミスによるものだったのか、他の理由があったのか分からないままにされている場合が多くあります。今回、IIJが対応した事例は、原因の追求過程で行為者の悪意を明確にできた「経路ハイジャック」の貴重な事例だと考えています。

■ 経路ハイジャック事件の概要

2015年2月4日、日本・ネットワーク・オペレーターズ・グループ（JANOG）のメーリングリストに一通のメールが投稿されました。IIJで管理しているIPv4アドレスのある/16のブロックが他のネットワークから広報されており、SpamHausのブロックリストに掲載されているという内容でした。これを受けて即座に対応を開始しました。確かに当該ブロックは米国のISPから経路広告されていたことから、経路の奪還と広告元からの経路停止を最初の目標にしました。IPの経路制御では細かい経路情報の方が優先されるため、一時的に細かい経路情報を広告して他のネットワークでIIJからの経路広告を優先するようにしました。並行して米国の当該ISPの連絡先を調べて連絡を取りました。ISPには営業の問い合わせやサービスごとのサポート窓口など様々なコンタクト先がありますが、適切な窓口に連絡しないと対応に時間がかかったり窓口に無関係な問い合わせとして放置されてしまう可能性もあります。今回のような経路制御の問題は該当組織のネットワーク運用部門（NOC）を見つける必要があり、whoisやISPのWebなどを調べて、最もそれらしい窓口を探して連絡しました。

当該ISPにメールで詳細を送った後、すぐに電話でも連絡し、メールの受領確認と対応の依頼をしました。米国のISPでは、チケットシステムを導入して作業の進捗管理をしている場合が多いため、チケット番号の発行も依頼しました。チケット番号はメールにて返送しておくとのことだったので返信を待ちましたが、24時間以上待っても返信がなかったため、再度電話にて連絡し、その場でチケットの発行と対応を依頼しました。こうしてようやくチケット番号が割り当てられ、進捗が確認できるようになりました。電話口に出たのが前回と異なる担当者だったため、その場で再度whoisの情報などを確認してもらって、我々の連絡が正当性を持つものだと認識してもらいました。そのISPからの情報によると、問題のIPv4アドレスブロックは顧客からの依頼に基づいて広告開始したそうで、念のためその顧客に連絡してみて、特に返事がなくても24時間以内には経路広告を停止することにしてもらえました。こうして、2015年2月4日午後に連絡を取り始め、3日後の2015年2月7日未明には該当の経路広告が停止しました。このIPv4アドレスブロックはSpamHausのブロックリストにも掲載されていたため、不正な経路広告停止後に削除を申請し、翌日にはリストから削除されました。

IIJで保持している経路情報の履歴を見ると、この不正な経路情報は2015年1月5日に広告開始されていましたが、IIJではJANOGに情報が投稿されるまで気がつくことができませんでした。実はこのIPアドレスブロックはIPv4アドレス移転手続きに基づいてIIJが管理することになったIPアドレスブロックで、当時は特に経路広告せずに将来の利用に備えて在庫として保

持している状態でした。当然JPNICに登録したwhoisの情報などは最新の情報になっていましたが、経路広告していなかったこともあり、JPIRRなどの経路データベースには登録しておらず、先に挙げた経路奉行の監視対象になっていませんでした。このため、不正な経路広告が発生しても認識できていなかったのです。この事例を受けて管理下にあるすべてのIPアドレスブロックを見直して、JPIRRなどのIRRへの登録と経路広告を開始しました。これにより、現在はIIJ管理下にあるIPアドレスブロックはすべて経路奉行の監視対象となっています。

問題の再発を防ぐため、不正な経路広告元となった米国のISPに、経路広告の発端となった関連情報の提出を求めました。かなり粘り強く交渉を続けた結果、広告停止から3週間程度経った2015年2月27日に驚きの書面が送付されてきました。図-13はLetter of Authority（LoA）と呼ばれる書面で、顧客がISPに持ち込みのIPアドレスブロックの広報を依頼する際に提出する書面です。

組織からの正式な書類であることが求められるため、レターヘッドと呼ばれる書式が用いられ、書面上部に会社組織のロゴや連絡先が記載されています。内容は至って簡素で、ISPに経路広告を許諾する旨の内容、持ち込むIPアドレスブロック、責任者の連絡先と署名、日付などが記載されています。今回提出された内容を見てみると、書面では該当のIPv4アドレスブロックを移転前に管理していた組織を名乗っているように見えました。「名乗っているように見えました」というのは、組織名や連絡先が我々が知っているものと微妙に異なっていたのです。

念のため、この書面を持って、IPv4アドレス移転前に該当のIPv4アドレスブロックを管理していた組織を訪問し、内容を確認していただきました。結論から言えば、やはり内容を偽った偽装書類でした。記載された会社名は存在しないこと、ロゴと住所は関連会社のものを流用した可能性が高いこと、電話番号と担当者はかつてwhoisに登録されていた情報を流用した可能性が高いこと、連絡先に指定されたメールアドレスのドメイン名は知らないものであることなどを確認いただきました。書面ではかつての担当者名で署名されていましたが、その方にもそんな署名はしていないことを確認いただきました。ドメイン名は行為者が会社名に対応したそれらしいドメイン名を新たに登録して利用しているようで、ドメイン名のwhois情報も会社名や担当者名がLoAの書面と合致するように登録されていました。

ここで時間軸に沿って事象の流れを推測を交えて整理します（図-14）。LoAで利用された偽装用のドメイン名の登録日が2014年10月7日なので、これ以前にターゲットの選定を行っていたはずです。このとき、できるだけ長く利用できるように既存の経路広告がないことや連絡先が不確かなIPv4アドレスブロックを選定したのではないかと推測しています。次に2014年10月7日、ターゲットのwhois情報を元に偽装用のドメイン名の登録を行いました。その後、適当なサーバでメール

ロゴ

＜会社名＞
＜住所＞
＜電話番号＞

＜日付＞

＜宛先組織名＞

We authorize ＜宛先ISP＞ to announce the following IP blocks -

＜IPアドレスブロック＞

This authorization shall be valid until revoked by us writing or
by e-mail from ＜メールアドレス＞
I may be contacted at ＜電話番号＞ or ＜メールアドレス＞

Sincerely,
＜署名＞
＜担当者名＞
＜所属部署＞

図-13 LoAの例

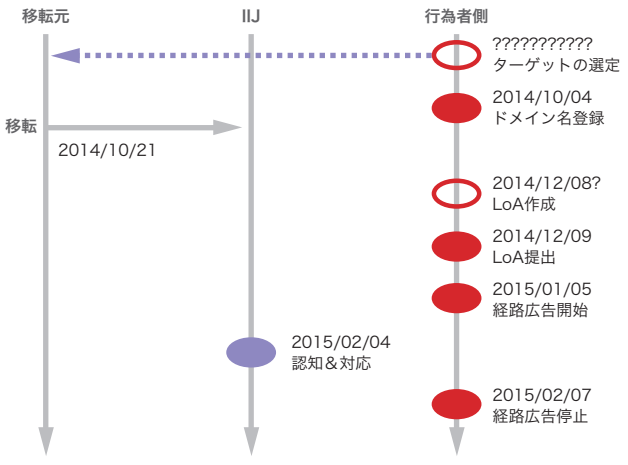


図-14 今回の事件の時系列まとめ

の受信ができるようにしたはずです。この後しばらく準備している間に、行為者の予想しなかったことが起こっています。IPv4アドレス移転です。2014年10月21日から当該IPv4アドレスブロックはIIJが管理することになりました。しかし、恐らく行為者側では認知していなかったのではないかと推測しています。行為者は2014年12月9日、それまで準備したとおり、移転前の管理組織に似せた名義でLoAを今回経路広告元となった米国のISPにpdfで提出しています。これを受けてISPでは、2015年1月5日から、IIJからの連絡を受けて2015年2月7日に広告を停止するまでの間、当該IPv4アドレスブロックを経路広告していました。

今回の周辺情報を調査した所、他にも疑わしい事例があったことが判明しました。IIJからの依頼に基づき当該IPアドレスブロックの広告が停止した3日後の2015年2月10日、なんとIPアドレスの数字的にその次のIPアドレスブロックが同じISPから経路広報され始めました。調査したところ、この件に関しても、同一の行為者で、経路広告するためにほぼ同様の手法が使われていたことが分かっています。こちらの件は独自に対応されたようで、2015年5月16日には経路広告が停止しています。日本は世界の他の地域に比べて早い段階からインターネットの導入が始まっており、インターネット黎明期に比較的大きなIPアドレスブロックの割り当てを受けた組織があります。このようなIPアドレスブロックのうち、whois情報が不完全あるいは連絡先が不明確になっているもの、在庫として保持している、あるいは内部のみで利用していてインターネットで経路広告していないものは、今回のような不正な経路広告のターゲットとして狙われやすいと考えられますので、後述する対策を検討されることをお勧めします。

行為者はネットワークを何に使っていたのでしょうか。実はIIJは今回の事例の詳細を把握できていません。偽装用のドメイン名の登録や偽装した書類など、周到かつかなりリスクの高い行為に及んでいるため、何らか悪用の意図があったと推測していますが、利用の証拠になるような情報は何もなく、該当のネットワークをどのような用途に利用していたのかは分かっていません。この件は引き続き調査を続けています。他の事例としては、spamの送信に悪用された事例が報告されています。南アジア地域のコミュニティであるSANOGでは、あるネットワークで突然管理者宛にspam送信に対する苦情が大量に届くようになった事例が共有されました。管理者が調べた所、一時的に経路ハイジャックにより不正に管理下のIPアドレスブロックが悪用され、そこから大量のspamが送信されたようだったとのことでした。管理者宛への苦情メールがきっかけで経路ハイジャックを認知することもあるため、連絡先の整備と苦情への対応を継続することも重要です。

■ 事件の教訓と経路ハイジャック対策

今回の事例では、当該ISPが書類審査をきちんと行っていれば不正な経路広報は防げていたはずです。LoAが到着した時点でJPNICのwhois情報はIIJの連絡先に書き換わっており、書面との相違があります。一方でwhoisの検索には多少の知識と技術も必要です。IPアドレスの登記情報を管理するIRは階層構造を成しているため、これを辿るように検索する必要があります。whoisクライアントの中にはある程度自動でこれに追従するものもありますが、国別のNIRが存在する地域は少なく、ほとんどのクライアントは地域別のRIRのwhois、つまりアジア太平洋地域ではAPNICのwhoisのレベルで検索して結果を表示するようです。JPNICに登録された情報は英語表記部分がAPNICのwhoisにも転記されて表示されるようになっていますが、これを正しく読み解くには何の情報がどう反映されているかを知っておく必要があります。インターネット黎明期に登録されたブロックはERXプロジェクトで登録者の属する地域のRIRに移管されていますし、最近では地域をまたいだIPv4移転も行えるようになってきているので、これらも適切に追従してwhois検索しないと正しい情報を得ることができません。whoisよりももう少しコンピュータで利用しやすい登記情報の形式ということで、Resource Public Key Infrastructure (RPKI)が標準化されて、利用できる状態になっています。これはIPアドレスなどの番号資源の割り振りや割り当てを電子証明書を利用して表現するものです。IRの登記情報に基づき、リソース証明書と呼ばれる電子証明書を発行することが可能で、これを検証することでIPアドレスの割り振りや割り当てを確認することができます。電子証明書を利用するため、文章への電子署名を追加することも可能です。例えばLoAにリソース証明書による電子署名を付加して、受領側で検証することで、正しいIPアドレスブロックの管理者からの文章であることが確認できます。また、経路制御にも利用可能で、現時点では経路生成元のAS番号を検証するOriginValidationという技術が標準化されて、ルータへの実装が進んでいます。運用者がPKIなど

の一般的な公開鍵暗号技術を学ぶ必要がありますが、うまく運用すれば大変強固な認証基盤になるはずです。利用の普及にはまだ時間がかかると考えられますが、IIJでも検証や運用を通じてRPKIの普及に協力できればと考えています。IPアドレスの割り振りや割り当てを受けている場合、現時点でどのような対策を講じられるでしょうか。今回の事例を通じて、ターゲットとして狙われにくくし、経路広告を依頼されたISPで異常に気がつけるようにするためには、次の2つのポイントが鍵になりそうだと分かりました。

1. whoisの連絡先を整備する
2. 経路広告する

1.のwhoisに関しては組織名や住所、電話番号、メールアドレスなど、できる限りの連絡先を正確に記載して、参照があった際に判別に利用できるようにしておくのがお勧めです。また苦情の連絡先を探す際にwhoisを参照する場合もあるので、これらの窓口では苦情の処理を担う可能性があること、公開窓口となるため、日常的にspamを受信することになるかもしれないことを認識しておく必要があります。苦情メールにはspamが添付されていることもあり、単純な学習型やキーワードマッチ型のspamフィルタを適用すると、苦情自体もspam判定してしまい、受信できなくなる場合があるため運用に注意が必要です。

2.の経路広告に関しては、インターネットへの到達性が必要ない場合でも、念のために経路広告しておいた方が適切に運用していることを示せて安全です。ただ、経路広告すると、そのIPアドレスブロック宛のIPパケットを吸い込むことになるため、脆弱性や稼働しているサービスを探索するためのIPパケットなどが到着するようになります。無用なリスクを増やさずに現状とほぼ同じ環境を維持するには、そのIPアドレスブロック宛のパケットをすべて破棄しつつ、経路のみ広告するのがお勧めです。既に何らかのインターネット接続サービスを利用している場合には、そのISPに相談すると対応してくれる場合もありますし、必要であればIIJにご相談いただければと考えています。経路広告に際しては、経路情報のデータベースであるJPIRRに適切にrouteオブジェクトを登録することで経路奉行の監視サービスを受けることができ、万が一、不正に経路広告された場合でも早期に検出できる可能性が高まるため、併せて検討をお勧めします。

インターネットでは今後も今回の事例のような経路ハイジャックが試みられる可能性があります。大きく2つの理由が想定できます。1つ目に様々な組織がspam送信やmalwareのホスティングなどを調査してIPアドレス単位のレピュテーションデータベースを構築しており、何にでも悪用できる新たなIPアドレスブロックへの要望があること、2つ目にIPv4アドレス在庫が世界的に枯渇してきており、徐々に既存のサービスを通じて必要な量のIPv4アドレスを確保することが困難になってきていること。これらの状況から、今後も経路ハイジャックのリスクはあると考えられます。また、前述したように日本ではインターネット黎明期に割り当てられた、whoisの情報がきちんと更新されていないIPアドレスブロックが多数あり、とてもターゲットになりやすい状況にあります。経路ハイジャックによって、管理するIPアドレスブロックを悪用された場合、知らない所でブロックリストに追加されたり、レピュテーションデータベースでの評価に影響する場合が考えられ、将来の通信に影響を及ぼす可能性があります。また、見知らぬ苦情対応に巻き込まれる可能性もあるため、相応の対策を講じておくことをお勧めします。

■ まとめ

経路ハイジャック対策でも他のセキュリティ対策と同様に、攻撃者側のコストを高める視点が重要です。つまり経路ハイジャックされにくい環境の整備、また経路ハイジャックされても早期に検出して対応できる体制の整備などを整えることが必要だと考えています。この実現のためには、IRの登記情報の信頼度向上やRPKIの活用を通じた持ち込みIPアドレスの検証方法の見直し、厳密な経路フィルタの運用やRPKIによる経路認証など不正な経路広報の流通を防ぐ方策の導入、経路奉行やその他の異常経路検出機構による不正経路の検出技術向上、ネットワーク間で必要な情報交換と協力した対応が取れる信頼のおける協調関係の構築など様々な技術的あるいは運用上の取り組みを検討する必要があります。また法執行機関などとも相談しながら、経路ハイジャックを再発させない環境づくりを構築したいと考えています。これらの取り組みはIIJのみならず、インターネットの経路制御に関わる多くの方々と協調しながら進めていくものであるため、広くIIJの知見を共有しながら、今後も検証や議論、改善を続けていければと考えています。

1.4.2 TLS1.3最新動向

広くブラウザに実装されているセキュアプロトコルSSL(Secure Socket Layer)/TLS(Transport Layer Security)に対する様々な種類の脆弱性が相次いで見つかったことから、根本的な解決を望む声を受けTLSの次バージョンであるTLS1.3に注目が集まっています。本稿では、これまでのバージョンの問題点や背景について触れたあと、現時点でのTLS1.3の動向について紹介します。

■ SSL/TLSの経緯

Netscape Communicationsから1995年にInternet draft "draft-hickman-netscape-ssl"が公開された時期と同じくして、当時のブラウザNetscape NavigatorにSSL2.0が実装されました。その後、いくつかの拡張と問題点が修正されたSSL3.0はつい最近まで利用されていましたが、昨年10月に発表されたPOODLE攻撃はSSL3.0における根本的な問題を露呈することになり、SSLの利用は安全ではないと認識されるようになりました。現在ではSSL2.0及びSSL3.0はそれぞれ利用しないことが推奨されています[*46]。SSLの後継でありIETFで策定されたTLSは、1.0/1.1/1.2が1999/2006/2008年にそれぞれRFCとして公開されています[*47]。それぞれのバージョンにおける主な変更点は、暗号技術評価プロジェクトCRYPTRECで作成されたガイドライン[*48]にて詳しく紹介されています。概要を抜粋すると、TLS1.0にはBEAST攻撃などにおいて広く露呈したCBCモード利用時の問題が指摘されており、TLS1.1でその問題を解消しています。更にTLS1.2では、認証暗号モードに分類されるGCM、CCMやSHA-2ファミリーなど、比較的新しい暗号アルゴリズムの利用が可能になっています。

表-1は、それぞれのバージョンにおけるワークアラウンドについてまとめたものです[*49]。TLS1.0は、サーバ設定・クライアントの実装でいくつかの仕様上の問題点をカバーすることで安全に利用でき、現在最も多く利用されているバージョンです。更に、新しいTLSライブラリや暗号モジュールを利用することでTLS1.1もしくはTLS1.2に対応することが可能であり、ブラウザ側も最新バージョンにアップデートすることで、ユーザは特に意識することなく、安全なバージョンを利用できる環境にあります。しかし、根本的な解決方法がない課題も残されていることが分かります。TLS1.3では、SSL/TLSに対する様々な種類の脆弱性に対し、根本的な解決を望む声を受け、執筆時現在も改訂・議論が繰り返されています。TLS1.3ドラフトの技術的な解説は後述します。

■ SSL/TLSの概要とその役割

SSL/TLSは、(1)通信の暗号化、(2)データ完全性の確保、(3)サーバ認証(場合によりクライアント認証)の機能を提供します。セッション層に位置することで、アプリケーション層ごとにセキュリティ確保のための仕組みを実装する必要がなく、

表-1 SSL/TLSバージョンの違いによるステータスの違い

プロトコル	バージョン	ステータス	ワークアラウンド	根拠
SSL	2.0	脆弱	N/A	RFC6167
	3.0	脆弱	N/A	RFC7568 (POODLE攻撃)
TLS	1.0	問題はあるが回避策あり(ただし回避策がないものもある)	Renegotiation機能を利用しない	RFC5746
			圧縮機能を利用しない	CRIME攻撃
			1/n-1分割法	BEAST攻撃
			リスク受容	Lucky13攻撃
	1.1	問題はあるが回避策あり(ただし回避策がないものもある)	圧縮機能を利用しない	CRIME攻撃
			リスク受容	Lucky13攻撃
	1.2	問題はあるが回避策あり	圧縮機能を利用しない	CRIME攻撃
			暗号モードとしてGCM、CCMのみを利用	Lucky13攻撃
	1.3	(安全に設計しようとしている)		

*46 これまでのSSL/TLS策定の歴史的背景については、Rolf Oppliger著、"SSL and TLS:Theory and Practice"に詳しい。また、SSLの利用が推奨されない理由については、以下の2つのRFCにまとまっている。"RFC 6176:Prohibiting Secure Sockets Layer(SSL) Version 2.0"(https://tools.ietf.org/html/rfc6176)、"RFC 7568:Deprecating Secure Sockets Layer Version 3.0"(https://tools.ietf.org/html/7568)。

*47 "RFC 2246:The TLS Protocol Version 1.0"(https://tools.ietf.org/html/2246)、"RFC 4346:The Transport Layer Security(TLS)Protocol Version 1.1"(https://tools.ietf.org/html/4346)、"RFC5246:The Transport Layer Security(TLS)Protocol Version 1.2"(https://tools.ietf.org/html/5246)。

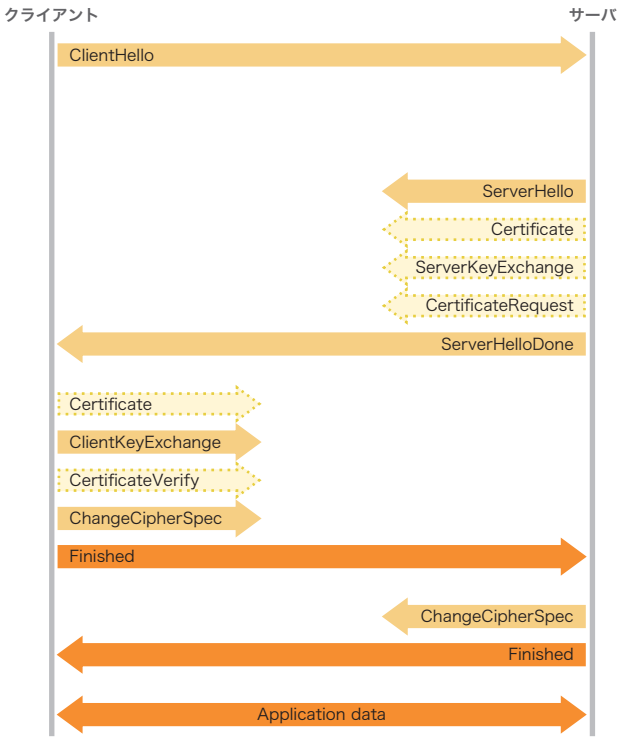
*48 IPA、「SSL/TLS 暗号設定ガイドライン~安全なウェブサイトのために(暗号設定対策編)~」(https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html)。

*49 前述したSSL/TLS暗号設定ガイドラインやMozillaプロジェクトによる"Security/Server Side TLS"(https://wiki.mozilla.org/Security/Server_Side_TLS)、"RFC 7525:Recommendations for Secure Use of Transport Layer Security(TLS) and Datagram Transport Layer Security(DTLS)"(http://tools.ietf.org/html/rfc7525)などで推奨設定が参照できる。また、"RFC 7457:Summarizing Known Attacks on Transport Layer Security(TLS) and Datagram TLS(DTLS)"(https://tools.ietf.org/html/rfc7457)が公開されおり、これまでの攻撃について概要を掴むことができる。

HTTP・SMTP・POPなど、様々なプロトコルの下位に位置して上記のセキュリティ機能を提供することができます。アプリケーション層の各種プロトコルに依存する必要がないメリットを持つため、幅広く実装される結果となりました。

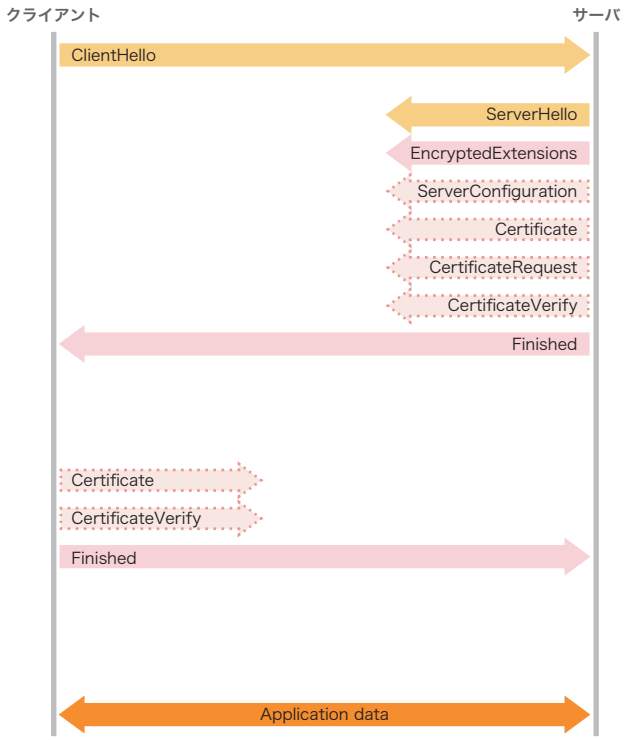
図-15は、TLS1.2におけるメッセージフローを示したものです。アプリケーションデータを暗号化するまでにはHandshakeメッセージと呼ばれる事前処理が存在しており、4-wayのフローで構成されていることが分かります。以下、Handshakeメッセージに関して簡単に役割を示します。(1)クライアント(ブラウザ)から、理解可能な暗号アルゴリズムリストであるCipherSuiteの束をサーバに送付します。(2)サーバは、その中から最も良いと考える1つのCipherSuiteを選択してServerHelloを通じて通知すると共に、サーバ認証に必要なX.509証明書や鍵交換のために必要な公開鍵などの情報をクライアントに返却します。(3)クライアントは、サーバ公開鍵を受領したことから、サーバにしか復号できない情報を送信することができます。これをサーバが受領し復号した時点で、各種鍵データの元となるMaster Secretを共有します。最後に「これから暗号化します」という意味を持つCCS(ChangeCipherSpec)を送った後、暗号化データFinishedを送付します。サーバはこれを復号し、内包されているMACデータ(メッセージ完全性を保証するデータ)をチェックし、これまでに送受信したメッセージが改ざんされていないことを確認します。(4)最後に、サーバからもCCS及び暗号化データFinishedを送付し、それを受け取ったクライアントはサーバ側の挙動と同様に復号処理とMACデータをチェックして、アプリケーションデータを安全に送受信する体制が整えることができます。

データ暗号化に用いる鍵は、公開鍵暗号方式を用いることでクライアントとサーバにしか分からないように生成することから、暗号化機能を提供しています。また、MACデータの保証範



図中、点線で囲まれているメッセージはオプショナルであること、オレンジ色のメッセージはMaster Secretから派生した鍵データで暗号化していることを意味する。

図-15 TLS1.2 メッセージフロー



TLS1.3ドラフトのMessage flow for full TLS Handshake(1-RTTとも呼ばれる)のみを記載。CertificateRequestとCertifcateVerifyをマージするなどの議論が継続しており最終的には変更される可能性が高い。また、これに準じないフローも存在するので注意。特にクライアントが事前情報の一種であるEarlyDataIndicationをClientHelloに格納して送付する0-RTTでは既に鍵を共有していることから大きくフローが異なっている。更にIETF-94ではクライアント認証をHandshake後に行う提案もあり、更にバリエーションが増える見込みである。図中、点線で囲まれているメッセージはオプショナルであること、ピンク色のメッセージはEphemeral Secretから派生した鍵データで暗号化していること、オレンジ色のメッセージはMaster Secretから派生した鍵データで暗号化していることを意味する。

図-16 TLS1.3メッセージフロー

囲はFinishedよりも前の平文データすべてであるため、もし仮に途中の経路で改ざんされたとしてもそれを検知する仕組みを持っています。更に、X.509証明書を相手ノードに提示すると共に、証明書内の公開鍵に呼応する秘密鍵を保持していることを確認することで、サーバ認証・クライアント認証を行うことができます。

■ TLS1.3

TLS1.3[*50]は、執筆時現在も改訂・議論が繰り返されています。最終的な仕様との比較ではないですが、TLS1.2までと比べると、以下に列挙したようなかなりドラスティックな変更が行われる見込みです。

(1) 危殆化したアルゴリズム及び暗号モードの排除
(2) メッセージフローの簡素化とHandshakeメッセージの暗号化
(3) 擬似乱数関数の整理、Master Secretの計算方法や各種鍵生成方式の変更

上記は変更点のすべてではないですが、多くの改善を試みていることが分かり、エンジニアもその動向について注目しています。日本でもCELLOS(暗号プロトコル評価技術コンソーシアム)の呼びかけのもと、最新ドラフトの読み合わせ会が開催されているほか、それらのレビュー結果をTLS WGにフィードバックするなどの試みがなされました[*51]。

上記で挙げた変更点に関して、以下、技術的な側面について簡単に解説します。

■ (1)危殆化したアルゴリズム及び暗号モードの排除

脆弱であると認識されている暗号アルゴリズムDES、MD5、RC4などが排除されます[*52]。特に、RC4はTLS1.3策定とは独立して排除しようという動きが見られ、主要ブラウザベンダーからも2016年の早い時期にRC4を無効化するアナウンスが既になされています[*53]。SHA-1及びSHA-2シリーズのうちSHA-224についても署名における利用が排除されています。しかし、サーバ証明書を検証するために辿る証明書チェーンの中には完全にSHA-1を用いた証明書を排除できていないため、この点をどう扱うかに関しては現在も議論が進められています。また、BEAST攻撃やPOODLE攻撃などを誘引したCBC暗号モードが排除され、共通鍵暗号としてはAEAD(Authenticated Encryption with Associated Data)のみの利用に統一されます。AEADのコンペティションCAESAR[*54]が2013年より開催されており、現在Round-2のフェーズにあり、2017年末をめどにWinner(s)が決定する予定です。TLS1.3では、CAESARの結果が反映されるのかについて不明瞭ですが、現在のドラフトバージョンでは、AEADの1つであるChaCha20-Poly1305[*55]がAES-GCM、AES-CCM[*56]と並んで実装必須(Mandatory Algorithms)として記載されています。他の共通鍵暗号アルゴリズムとしては、韓国のARIAと日本製のCamelliaが記載されています[*57]。今後、他のアルゴリズ

*50 "The Transport Layer Security (TLS) Protocol Version 1.3"(https://tlswg.github.io/tls13-spec/)、または"The Transport Layer Security (TLS) Protocol Version 1.3"(https://datatracker.ietf.org/doc/draft-ietf-tls-tls13/)で参照可能である。執筆時のドラフト最新版は、バージョン10であった。
*51 6月から9月にかけて4回に渡って行われた勉強会では、ドラフトversion-08に対するコメントをまとめ、公開している(https://www.cellos-consortium.org/studygroup/tls_1_3-draft_08_issues_rev1.pdf)。このコメントは、TLS-WG MLにも展開され(http://www.ietf.org/mail-archive/web/tls/current/msg17904.html)、それらの現在の対応状況については、GitHubにて参照可能である(https://github.com/tlswg/tls13-spec/search?q=CELLOS&type=Issues&utf8=%E2%9C%93)。
*52 DESは、TLS1.2で既に排除済みである。MD5排除の背景は、"RFC 6151:Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms"(https://tools.ietf.org/html/6151)を参照のこと。同様に、RC4についても"RFC 7465:Prohibiting RC4 Cipher Suites"(https://tools.ietf.org/html/7465)で参照できる。
*53 The RC4 NOMORE Attack(https://www.rc4nomore.com/)が今夏のUSENIX security'15で公開されるなど、RC4排除に向けて追い討ちをかける結果となった。主要ブラウザベンダーの動きについては、以下のとおり、"Ending support for the RC4 cipher in Microsoft Edge and Internet Explorer 11"(http://blogs.windows.com/msedgedev/2015/09/01/ending-support-for-the-rc4-cipher-in-microsoft-edge-and-internet-explorer-11/)、"Deprecating the RC4 Cipher"(https://blog.mozilla.org/security/2015/09/11/deprecating-the-rc4-cipher/)、"Intent to deprecate:RC4"(https://groups.google.com/a/chromium.org/forum/#!msg/security-dev/kVfCywocUO8/vgi_rQuhKgAJ)。
*54 Cryptographic competitions、"CAESAR:Competition for Authenticated Encryption:Security, Applicability, and Robustness"(http://competitions.cr.yp.to/caesar.html)。
*55 "RFC 7539:ChaCha20 and Poly1305 for IETF Protocols"(https://tools.ietf.org/html/rfc7539)。
*56 "RFC 5288:AES Galois Counter Mode (GCM) Cipher Suites for TLS"(https://tools.ietf.org/html/rfc5288)、"RFC 6655:AES-CCM Cipher Suites for Transport Layer Security(TLS)"(https://tools.ietf.org/html/rfc6655)。
*57 "RFC 6209:Addition of the ARIA Cipher Suites to Transport Layer Security(TLS)"(https://tools.ietf.org/html/rfc6209)、"RFC 6367:Addition of the Camellia Cipher Suites to Transport Layer Security(TLS)"(https://tools.ietf.org/html/rfc6367)。

ム記載の要請が殺到することが予想されるため、どのようなプロセスで最終決定されるのかについては、詳細に詰められていくものと考えられます。

公開鍵暗号としては、離散対数問題の難しさが安全性を担保するDSAが排除されました。DSAは現時点で脆弱な暗号アルゴリズムではありませんが、楕円曲線上の演算を使うことで暗号処理を軽減したECDSAの利用にシフトしています（署名としてはECDSAだけではなく、暗号化もデジタル署名もRSAを利用するCipherSuitesが残されています）。一方で、鍵交換に使われるDHは排除されることなくECDHと共に残っています。また、DH、ECDHを利用する際には、Forward secrecy[*58]を満たすように毎回異なる鍵（Ephemeral keys）を生成するDHE、ECDHEのみがCipherSuitesリストに記載されています。また楕円曲線としては、近年のIETFでのPervasive Monitoring[*59]の議論を受け、NISTが策定したsecp256r1（Curve P-256）などのCurve[*60]だけでなく、D. J. Bernsteinにより、PKC2006にて発表されたCurve25519[*61]も実装することが推奨（SHOULD）されています。Curveに関する議論は、横浜で開催されたIETF-94や今年12月に日本で開催されるSSR2015（The 2nd International Conference on Research in Security Standardisation）でも最新の話題として取り上げられる見込みです[*62]。

■（2）メッセージフローの簡素化とHandshakeメッセージの暗号化

TLS1.2までのHandshakeにおいては、クライアントからCipherSuitesリストをサーバに送付してサーバが1つ選択する方式を採っています。一方TLS1.3では、この律儀な挙動を削減して、クライアントから1つのCipherSuiteを決め打ちで送付することから開始します。これにより、暗号化及びデータ完全性を保証するための鍵共有を、図-16のように4-wayから3-wayに削減することができます。更に、TLS1.2まではFinishedメッセージから暗号化していますが、TLS1.3ではMaster Secretを共有する前から、事前鍵を用意してHandshakeメッセージの一部を暗号化するように変更されています。

■（3）擬似乱数関数の整理、Master Secretの計算方法や各種鍵生成方式の変更

Handshakeメッセージを暗号化する際には、RFC 5869で規定されているHMACを用いた鍵導出関数を用いて鍵共有が行われています。この変更に伴い、Master Secretの導出方法も大きく見直されており、各フェーズにおいて独立した暗号鍵が用いられています。現在のところMaster Secret以外にもStatic SecretとEphemeral Secretと呼ばれる事前鍵が生成され、これらを用いてHandshakeメッセージの暗号化が

＊58 IIJ IIR vol.22、1.4.2 Forward Secrecy（http://www.iij.ad.jp/company/development/report/iir/022.html）。
＊59 "RFC 7258：Pervasive Monitoring Is an Attack"（https://tools.ietf.org/html/rfc7258）。
＊60 National Institute of Standards and Technology、"FIPS PUB 186-4、Digital Signature Standard（DSS）"（http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf）。
＊61 "A state-of-the-art Diffie-Hellman function"（http://cr.yp.to/ecdh.html）。
＊62 翌月東京で開催されるSSR2015（http://ssr2015.com/）では、招待講演またはパネルディスカッションのいずれかでCurvesを含む暗号アルゴリズム選定に関する話題が取り上げられる見込みである。IETF-94では楕円曲線に関するCipherSuitesを規定するRFC4492（https://tools.ietf.org/html/rfc4492）の改訂に関する議題も取り上げられている（https://www.ietf.org/proceedings/94/slides/slides-94-tls-0.pdf）。同会議ではRSA署名のフォーマットの移行に関しても触れられた。具体的にはRSASSA-PKCS1-v1_5（PKCS#1 version1.5で定義）をRSASSA-PSS（https://tools.ietf.org/html/rfc3447）に移行するトピックであった（https://www.ietf.org/proceedings/94/slides/slides-94-tls-4.pdf）。

段階的に行われる見込みです。また、これら2つの事前鍵からMaster Secretが生成されるように設計されています。なお、これら3つの鍵データから共通鍵暗号に用いられる実際の鍵が派生されますが、AEADは暗号化とMAC付与（メッセージ認証）を同時に行う方式のため、鍵派生においてはMAC用鍵を生成する方法が削除されています。

このように様々な試みが検討されており、TLS1.3が本当に安全なプロトコルであるのかについて透明性を持って議論が継続されています。もう1つの方向性としては、ProVerifなどの形式検証ツールを用いて当該プロトコルが安全であるかどうかを検証しようとする試みです[*63]。新しい暗号アルゴリズム提案時に、証明可能安全性を保証することが必須であるように、セキュアプロトコルについても同じような共通認識が生まれる可能性もあるでしょう。

■ 実装の問題を誘発する要因を排除したい

暗号アルゴリズムや擬似乱数生成モジュールの利用に対して、設計者は当然と考えていることが、実は実装者には周知されていないという問題があります。意図せず秘密鍵を共有していた公開鍵使い回し問題や、データ暗号化鍵がハードコーディングされ、毎回同じ鍵で暗号化されている実装などがそれにあたります[*64]。お互いにコンセンサスがないために実装時にぶれが生じてしまうだけでなく、脆弱性を誘発してしまうことが大きな要因と考えられています。更にRFCなどの仕様文書が自然言語で表現されていることから曖昧さが残り、実装者によって解釈が異なるという問題も残されています。TLS1.3ドラフトにおいても、文書・文章の在り方を再認識する必要があるでしょう。そのため、プロトコル自身も無駄な箇所を排除していくだけでなく、文章の曖昧さも削ぎ落としていく試みも必要ではないかと考えます。

1.5 おわりに

このレポートは、IIJが対応を行ったインシデントについてまとめたものです。今回は、経路ハイジャックとTLS1.3最新動向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）
松崎 吉伸 IIJ ネットワーク本部 技術企画室（1.4.1 経路ハイジャック）
須賀 祐治（1.4.2 TLS1.3最新動向）
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：
春山 敬宏、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

＊63 荒井、渡辺、櫻田、ProVerifによるTLS1.3ハンドシェイクプロトコルの形式検証、3C2-1、コンピュータセキュリティシンポジウム2015（http://www.iwsec.org/css/2015/program.htm#i3C2）。他にも、別の検証ツールを用いたTLS1.3への攻撃の報告も行われている（https://www.ietf.org/mail-archive/web/tls/current/msg18215.html）。

＊64 PKI Day 2012発表資料（http://www.jnsa.org/seminar/pki-day/2012/data/PM02_suga.pdf）やCRYPTREC シンポジウム2015資料（http://cryptrec.go.jp/topics/cryptrec_20150424_symposium2015_presentation.html）などを参考のこと。また、ランダムデータのミスユースについて考慮されている方式も存在する（https://tools.ietf.org/html/rfc6979）。DSAやECDSAでは署名する度にランダムなデータが必要になるが、これを署名対象データに応じて決定的（Deterministic）にすることで、実装のミスを減らそうとする試みである。