クラウドセキュリティの国際標準規格

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10月から12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。日本を主な対象としたオペレーションも行われ、政府機関のWebサイトを含む複数のWebサイトがDDoS攻撃の標的となりました。DDoS攻撃では仮想通貨による金銭の要求など脅迫を伴う攻撃が多く発生し、複数のグループが活動している状況が確認できます。不正アクセスによる情報漏えいも多く発生しており、米国のホテルチェーンを中心としてクレジットカード情報を含む多くの個人情報が漏えいする被害が発生しました。このように、インターネットでは依然として多くのインシデントが発生する状況が続いています。

1.2 インシデントサマリ

ここでは、2015年10月から12月までの期間にIIJが取り扱ったインシデントと、その対応を示します。まず、この期間に取り扱ったインシデントの分布を図-1に示します[*1]。

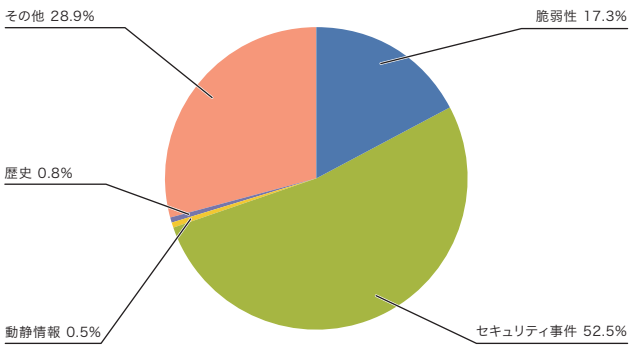


図-1 カテゴリ別比率(2015年10月〜12月)

■ 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。パリ同時テロ事件に対する報復として、AnonymousによるISIL関連のSNSアカウントを特定し、凍結させる活動が行われています(OpParis)。12月にはトルコ政府がISILを支援しているとの主張からトルコの.trドメインのDNSサーバに対して大規模なDDoS攻撃が発生しています。この攻撃は数日にわたって行われ、トルコドメインのDNSセカンダリを行っていたRIPEにも影響が出ています[*2]。また、DNSサーバだけでなくトルコの政府機関や大手銀行に対しても、攻撃が行われました。更に、英国の放送局BBCのWebサイトに対するDDoS攻撃が発生しましたが、これについてもアンチISILのグループが犯行声明を出しています。

中東に関連しては、イスラエルのラジオ局のWebサイトが改ざんされる被害が10月に発生したり、11月にはイスラエルの新聞社のTwitterアカウントが乗っ取られメッセージが投稿されるなどしています。更に、イスラエルミサイル防衛協会のWebサイトが不正アクセスを受け、ユーザデータが漏えいする事件も発生しています。このように、イスラエルの政府関連サイトや民間企業のWebサイトに対する攻撃も継続して発生しています。

9月から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

＊1　このレポートでは取り扱ったインシデントを、脆弱性、動静情報、歴史、セキュリティ事件、その他の5種類に分類している。
脆弱性:インターネットや利用者の環境でよく利用されているネットワーク機器やサーバ機器、ソフトウェアなどの脆弱性への対応を示す。
動静情報:要人による国際会議や、国際紛争に起因する攻撃など、国内外の情勢や国際的なイベントに関連するインシデントへの対応を示す。
歴史:歴史上の記念日などで、過去に史実に関連して攻撃が発生した日における注意・警戒、インシデントの検知、対策などの作業を示す。
セキュリティ事件:ワームなどのマルウェアの活性化や、特定サイトへのDDoS攻撃など、突発的に発生したインシデントとその対応を示す。
その他:イベントによるトラフィック集中など、直接セキュリティに関わるものではないインシデントや、セキュリティ関係情報を示す。

＊2　攻撃の詳細については、次のRIPEのDNS-WGのメールアーカイブからも確認できる。"[dns-wg] RIPE NCC Authoritative and Secondary DNS services on Monday 14 December"(https://www.ripe.net/ripe/mail/archives/dns-wg/2015-December/003184.html)。

が発生しています(OpKillingBay、OpWhales)。このオペレーションによる攻撃は日本だけではなく、世界動物園水族館協会(WAZA)やワシントン条約(CITES)といった機関に対しても行われていますが、日本においては、10月になっても継続して関係する組織や地方自治体、空港会社や首相の個人サイトといったWebサイトに対し、繰り返し攻撃が行われていました。攻撃手法についてもDDoS攻撃だけでなくSQLインジェクション攻撃などによるとみられる情報漏えいが行われるようになるなど変化が見られ、攻撃を受けた組織には報道機関やISP、出版社など、直接抗議活動とは関係がない組織も含まれるようになるなどの状況が見られます。本稿執筆時点の1月になっても日本の政府機関を含む複数の組織に対するこれらの攻撃は継続しており、引き続き注意が必要な状況です。

米国では、現在行われている大統領予備選挙に関連して、過激な言動を行っている候補者に関連するWebサイトへの攻撃が行われています。更に米国の秘密結社に関連して、この団体の支持者と考えられる人たちのSNSページのリストが公開されるなどしました。これ以外にも、世界中の各国政府とその関連サイトに対して、AnonymousなどのHacktivist達による攻撃が継続して行われています。

■ 脆弱性とその対応

この期間中では、Windows[*3][*4][*5][*6][*7]、Internet Explorer[*8][*9][*10]、Office[*11][*12][*13]、Edge[*14]などで修正が行われました。Adobe社のAdobe Flash 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。これらの脆弱性のいくつかは修正が行われる前に悪用が確認されています。

サーバアプリケーションでは、データベースサーバとして利用されているOracleを含むOracle社の複数の製品で四半期ごとに行われている更新が提供され、多くの脆弱性が修正されました。ntpdでも、認証を回避してシステムの時刻設定が操作可能な脆弱性や、細工したパケットによるDoS攻撃可能な脆弱性など複数の脆弱性が見つかり、修正されています。DNSサーバのBIND9でも、不正なクラス属性を持つレコードに対する問い合わせで、DoS攻撃可能な脆弱性などが見つかり、修正されています。CMSとして利用されるDrupalについても、オープンリダイレクトの脆弱性などが見つかり、修正されています[*15]。同じくCMSとして利用されるJoomla!でも、第三者からリモートでコード実行可能な脆弱性を含む複数の脆弱性が見つかり、修正されました。仮想マシン環境構築ソフトウェアであるVMwareでは、任意のコード実行の

*3 「マイクロソフト セキュリティ情報 MS15-109 - 緊急 リモートでのコード実行に対処するWindows Shell用のセキュリティ更新プログラム(3096443)」(https://technet.microsoft.com/ja-jp/library/security/ms15-109.aspx)。
*4 「マイクロソフト セキュリティ情報 MS15-111 - 重要 特権の昇格に対処するWindowsカーネル用のセキュリティ更新プログラム(3096447)」(https://technet.microsoft.com/ja-jp/library/security/ms15-111.aspx)。
*5 「マイクロソフト セキュリティ情報 MS15-126 - 緊急 リモートでのコード実行に対処するJScriptおよびVBScript用の累積的なセキュリティ更新プログラム(3116178)」(https://technet.microsoft.com/ja-jp/library/security/ms15-126.aspx)。
*6 「マイクロソフト セキュリティ情報 MS15-128 - 緊急 リモートでのコード実行に対処するMicrosoft Graphicsコンポーネント用のセキュリティ更新プログラム(3104503)」(https://technet.microsoft.com/ja-jp/library/security/ms15-128.aspx)。
*7 「マイクロソフト セキュリティ情報 MS15-135 - 重要 特権の昇格に対処するWindowsカーネルモードドライバー用のセキュリティ更新プログラム(3119075)」(https://technet.microsoft.com/ja-jp/library/security/ms15-135.aspx)。
*8 「マイクロソフト セキュリティ情報 MS15-106 - 緊急 Internet Explorer用の累積的なセキュリティ更新プログラム(3096441)」(https://technet.microsoft.com/ja-jp/library/security/ms15-106.aspx)。
*9 「マイクロソフト セキュリティ情報 MS15-112 - 緊急 Internet Explorer用の累積的なセキュリティ更新プログラム(3104517)」(https://technet.microsoft.com/ja-jp/library/security/ms15-112.aspx)。
*10 「マイクロソフト セキュリティ情報 MS15-124 - 緊急 Internet Explorer用の累積的なセキュリティ更新プログラム(3116180)」(https://technet.microsoft.com/ja-jp/library/security/ms15-124.aspx)。
*11 「マイクロソフト セキュリティ情報 MS15-110 - 重要 リモートでのコード実行に対処するMicrosoft Office用のセキュリティ更新プログラム(3096440)」(https://technet.microsoft.com/ja-jp/library/security/ms15-110.aspx)。
*12 「マイクロソフト セキュリティ情報 MS15-116 - 重要 リモートでのコード実行に対処するMicrosoft Office用のセキュリティ更新プログラム(3104540)」(https://technet.microsoft.com/ja-jp/library/security/ms15-116.aspx)。
*13 「マイクロソフト セキュリティ情報 MS15-131 - 緊急 リモートでのコード実行に対処するMicrosoft Office用のセキュリティ更新プログラム(3116111)」(https://technet.microsoft.com/ja-jp/library/security/ms15-131.aspx)。
*14 「マイクロソフト セキュリティ情報 MS15-125 - 緊急 Microsoft Edge用の累積的なセキュリティ更新プログラム(3116184)」(https://technet.microsoft.com/ja-jp/library/security/ms15-125.aspx)。
*15 "Drupal Core - Overlay - Less Critical - Open Redirect - SA-CORE-2015-004"(https://www.drupal.org/SA-CORE-2015-004)。

10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 **2日：Androidのlibutilsに、細工されたファイルを介して、任意のコードを実行される可能性がある脆弱性（CVE-2015-6602）が見つかり、修正された。**
詳細については、次のZIMPERIUM, INC.のBlogを参照のこと。"Zimperium zLabs is Raising the Volume：New Vulnerability Processing MP3/MP4 Media."（https://blog.zimperium.com/zimperium-zlabs-is-raising-the-volume-new-vulnerability-processing-mp3mp4-media/）。

セ **2日：米国の携帯電話事業者であるT-Mobile US, Inc.の信用調査業務を請け負っていた、Experian Information Solutions, Inc.が不正アクセスを受け、1,500万人分の社会保障番号を含む契約者情報が流出した。**
詳細については、次のT-Mobile USのBlog "T-Mobile CEO on Experian's Data Breach"（http://www.t-mobile.com/landing/experian-data-breach.html）、及びExperian Information Solutions, Inc.のサイト"Overview：Unauthorized Acquisition of Personal Information"（http://www.experian.com/data-breach/t-mobilefacts.html）を確認のこと。

セ **5日：韓国のソウルメトロが不正アクセスを受け、サーバを含む複数のPCがマルウェアに感染する事件が2014年7月に発生していたことが判明した。**

セ **5日：和歌山県太地町の公式Webサイトに対し、AnonymousによるDDoS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）。**

他 **6日：JPCERTコーディネーションセンターより、Webアプリケーションの脆弱性の1つで、正規のユーザが悪意あるWebサイトを経由して意図していない動作を行ってしまうクロスサイトリクエストフォージェリ（CSRF）について、その解説と対策をまとめ公表した。**
「クロスサイトリクエストフォージェリ（CSRF）とその対策」（http://www.jpcert.or.jp/securecoding/materials-csrf.html）。

セ **10日：成田空港や中部空港の公式Webサイトに対し、AnonymousによるDDoS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）。**

セ **13日：米国連邦捜査局（FBI）と英国国家犯罪対策庁（NCA）は共同で、オンラインバンキングのアカウントなどを狙ったマルウェアであるBugat（DRIDEX/CRIDEX）の複数のC&Cサーバを閉鎖した。**
詳細については、次の米国連邦捜査局の発表などを参照のこと。"Bugat Botnet Administrator Arrested and Malware Disabled"（https://www.fbi.gov/pittsburgh/press-releases/2015/bugat-botnet-administrator-arrested-and-malware-disabled）。

脆 **14日：Microsoft社は、2015年10月のセキュリティ情報を公開し、MS15-106やMS15-108などを含む3件の緊急と3件の重要な更新を含む合計6件の修正をリリースした。**
「2015 年 10 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-oct）。

脆 **14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。**
「APSB15-25：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/apsb15-25.html）。

脆 **14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。**
「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/reader/apsb15-24.html）。

脆 **15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脆弱性（CVE-2015-7645）が公表された。この脆弱性は10月17日に修正が公表されている。**
「APSA15-05：Adobe Flash Playerに関するセキュリティ情報」（https://helpx.adobe.com/jp/security/products/flash-player/apsa15-05.html）。

脆 **17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。**
「APSB15-27：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/apsb15-27.html）。

脆 **19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154件の脆弱性を修正した。**
"Oracle Critical Patch Update Advisory - October 2015"（http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html）。

他 **20日：国立研究開発法人情報通信研究機構（NICT）は、システム設計者の目的に応じた暗号プロトコルの適切な利用ができるよう、標準化された51個の暗号プロトコル及びその他の代表的な7個の暗号プロトコルについて、暗号プロトコルのセキュリティ評価結果をリスト化し公開した。**
「暗号プロトコルのセキュリティ評価結果をリスト化・公開」（http://www.nict.go.jp/press/2015/10/20-2.html）。

脆 **22日：ntpdに、不正なパケットの受信により、認証を回避してシステムの時刻設定が操作可能な脆弱性（CVE2015-7871）や細工したパケットによる異常終了などの可能性のある脆弱性など複数の脆弱性が見つかり、修正された。**
"October 2015 NTP-4.2.8p4 Security Vulnerability Announcement（Medium）"（http://support.ntp.org/bin/view/Main/SecurityNotice#October_2015_NTP_4_2_8p4_Securit）。

脆 **30日：複数メーカのルータ製品に、当該製品にログインしているユーザが、細工されたページにアクセスすることで意図しないルータの操作が行われる可能性のある脆弱性が見つかり、修正された。**
「JVN#48135658　複数のルータ製品におけるクリックジャッキングの脆弱性」（http://jvn.jp/jp/JVN48135658/）。

他 **30日：独立行政法人情報処理推進機構（IPA）は、注文連絡や複合機からの自動送信などを装い、Word文書ファイルが添付された不審なメールに関する相談が増えているとして注意喚起を行った。**
「【注意喚起】特定の組織からの注文連絡等を装ったばらまき型メールに注意」（http://www.ipa.go.jp/security/topics/alert271009.html）。

※ 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

可能性がある複数の脆弱性が見つかり、修正されています[*16]。Linuxで広く採用されているブートローダであるGRUB2では、バックスペースキーを連続で押すだけでパスワード保護を無効化できる脆弱性が発見され、修正されています[*17]。

Androidに関連しては、細工されたファイルを介して、任意のコードを実行される可能性がある脆弱性(Stagefright 2.0)が見つかり、修正が行われています。Androidアプリ向けソフトウェア開発キット(SDK)の1つであるMoplus SDKでWormholeと呼ばれる脆弱性[*18]があることや、攻撃者が遠隔で端末の情報を読み取ったり、制御が可能な不具合が指摘され、修正が行われました。また、これに関連して、別のSDK(Push SDK)でも、悪意ある第三者が端末の情報を取得できる可能性のある脆弱性が見つかり、修正が行われています[*19]。

産業用制御システムに関連しては、オムロン社製のPLCとそのプログラムを行うソフトウェアであるCX-Programmerで、パスワードを平文で送信していたことから通信経路上で盗聴された場合にパスワードが取得される可能性やシステム内のファイルからパスワードが取得される可能性があるなど、パスワード処理に関する複数の脆弱性が見つかり、修正されました[*20]。国内メーカの製品では、9月にも三菱電機社製の制御システム用シーケンサーであるMELSEC FXシリーズでサービス拒否攻撃を許してしまう脆弱性が見つかり、修正が行われています[*21]。産業用制御システムについては、閉鎖的な環境で利用されることも多いことから、これまで対策が遅れがちでしたが、近年ではこれらを標的とした攻撃が増えてきており、従来のソフトウェアと同様に、脆弱性情報や攻撃情報を定期的にチェックするなどの対応が必要になりつつあります[*22]。

■ DDoS攻撃

この期間では、大規模なDDoS攻撃がいくつか発生しています。2015年5月頃より、金融機関などに対し、DD4BCを名乗る何者かによる脅迫を伴ったDDoS攻撃が発生していますが、11月に入ってからは、別のグループによるDDoS攻撃もいくつか発生しています。このうち、Armada Collectiveを名乗る何者か[*23]による攻撃では、スイスのProton Technologies社が脅迫を受け、支払いをしたにも関わらず攻撃が継続した事件も発生しています。このグループは、これ以外にも各国の金融機関やホスティングサービスなどに対して攻撃を行っており、英国のホスティングサービス事業者がサービス停止に追い込まれた事件でも関与していたと考えられます[*24]。ホスティング事業者への攻撃では、米国Linode社に対しても12日間にも及ぶ大規模なDDoS攻撃が発生しています。これ以外にも12月にはPhantom Squadを名乗る何者かによるXbox LIVEやPSN、EAなど複数のゲーム関係サーバに対する攻撃により、一時的にサービスにアクセスしにくくなるなどの被害が発生しています。

■ 不正アクセスなどによる情報漏えい

この期間、企業のシステムへの不正アクセスによる大規模な顧客情報などの漏えい事件が引き続き発生しています。

米国の携帯電話事業者T-Mobileの信用調査業務を請け負っているExperian社の内部サーバが不正アクセスを受け、氏名や社

*16 "VMSA-2015-0007.2 VMware vCenter and ESXi updates address critical security issues."(https://www.vmware.com/security/advisories/VMSA-2015-0007)。
*17 詳細については、次の発見者による発表を参照のこと。"Back to 28:Grub2 Authentication 0-Day"(http://hmarco.org/bugs/CVE-2015-8370-Grub2-authentication-bypass.html)。
*18 脆弱性については、次のWooYun.orgで確認できる。"WooYun-2015-148406 WormHole虫洞漏洞总结报告(附检测结果与测试脚本)(http://www.wooyun.org/bugs/wooyun-2015-0148406)(中国語)。
*19 バイドゥ株式会社では、自社のアプリが該当のSDKを利用していたとして修正を行っている。「『Simejiプライバシーロック』について」(http://www.baidu.jp/info/press/report/151113.html)。
*20 「JVNVU#99817917 オムロン製PLCおよびCX-Programmerに複数の脆弱性」(https://jvn.jp/vu/JVNVU99817917/)。
*21 "Advisory(ICSA-15-146-01)Mitsubishi Electric MELSEC FX-Series Controllers Denial of Service"(https://ics-cert.us-cert.gov/advisories/ICSA-15-146-01)。
*22 産業用制御システムの脆弱性については、米国ICS-CERT(https://ics-cert.us-cert.gov/)などが情報提供などを行っており、参考になる。日本でもIPAが制御システム利用者向けのレポートやICS-CERTやENISAのレポートの日本語訳などの情報を提供している。IPA、「制御システムのセキュリティ」(https://www.ipa.go.jp/security/controlsystem/)。
*23 Armada Collectiveについては、例えばスイス政府のCERTチームのBlogなどで確認できる。"Armada Collective blackmails Swiss Hosting Providers"(http://www.govcert.admin.ch/blog/14/armada-collective-blackmails-swiss-hosting-providers)。
*24 この攻撃の詳細については、次の攻撃を受けたMoonfruitの発表を参照のこと。"DDoS attack update:14/12/2015"(https://support.moonfruit.com/hc/en-us/articles/207109805-DDoS-attack-update-14-12-2015)。

11月のインシデント

1 セ **1日：Facebookで特定の意見に賛同している人たちの公開されている個人情報をまとめたリストが公開され、プライバシーや名誉棄損などの問題から話題となった。後にリストを作成したと考えられる人物についても本名や勤務先などが判明し、リストは削除された。**

2

3 セ **4日：ZeusやSpyEyeなどのマルウェアを販売目的で所持していたとして、不正指令電磁的記録保管・提供など複数の容疑で中学生が逮捕された。また、逮捕された中学生からマルウェアを購入・譲渡していたとして、複数の中高生が不正指令電磁的記録取得容疑で書類送検された。**

4 セ **4日：スイスのProton Technologies社が提供している暗号化電子メールサービスProtonMailに対し、脅迫を伴う大規模なDDoS攻撃（100Gbps以上）が発生した。この事件では、影響を受けた他の企業などと協議した結果、15BTC（約70万円）を支払ったが、攻撃が停止せず、対策のため、寄付を募るなどの対応が行われている。**
詳細については、次の"ProtonMail Statement about the DDOS Attack"（https://protonmaildotcom.wordpress.com/2015/11/05/protonmail-statement-about-the-ddos-attack/）を参照のこと。

5

6 脆 **6日：Androidアプリ向けソフトウェア開発キット（SDK）の1つであるMoplus SDKにバックドア機能が見つかり、修正された。**
調査したトレンドマイクロ社では、Moplus SDKを組み込んだアプリが、検証時点でバージョンが異なるものやSHA1ハッシュ値が異なるものなども合わせ、14,112存在しているとしている。「脆弱性を抱えるソフトウェア開発キット『Moplus』、実はバックドア機能の実装が判明」（http://blog.trendmicro.co.jp/archives/12540）。

7

8

9

10 セ **10日：Facebookへ他人のIDとパスワードを使用して不正アクセスを行ったとして通信機器販売会社の男が不正アクセス禁止法違反の疑いで警視庁に逮捕された。この事件はわいせつ図画像公然陳列容疑での捜査中に、男のPCからFacebookとiCloudのID・パスワードがリスト化されたファイル771名分が見つかったことによる。**

11 脆 **11日：Microsoft社は、2015年11月のセキュリティ情報を公開し、MS15-112やMS15-115を含む4件の緊急と8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 11 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-nov）。

12

13

14 脆 **11日：Adobe Flash Playerに、不正終了や任意のコード実行の可能性がある複数の脆弱性が見つかり、修正された。**
「APSB15-28：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/apsb15-28.html）。

15

16 セ **16日：国内で販売されている複数のスマートフォンで、アプリやアップデートサーバを経由して、意図しない広告が配信される事件が相次いで発生した。**
例えば、ZTE社の場合はアプリの通知機能の制御ミスであったことを公表している。「【重要なご案内】Blade S（g03）及びBlade S Lite（g02）への広告誤配信についてのお詫び」（http://www.zte.co.jp/products/handsets/sim_free/phone/info/201511/t20151117_445962.html）。

17

18 他 **17日：JPCERTコーディネーションセンターより、標的型攻撃など高度サイバー攻撃への対処におけるログの活用と分析方法の解説が公表された。**
「高度サイバー攻撃への対処におけるログの活用と分析方法」（http://www.jpcert.or.jp/research/apt-loganalysis.html）。

19

20 セ **20日：厚生労働省のWebサイトに対し、AnonymousによるDDoS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）。この事件では攻撃を受け、11月21日から23日にかけて、ホームページが停止している。**
厚生労働省、「厚生労働省ホームページの復旧について」（http://www.mhlw.go.jp/stf/houdou/0000104929.html）。

21

22 セ **21日：シェラトンやウェスティンなどStarwood系列の50軒以上の北米のホテルでPoSマルウェアによる感染により、カード情報などの顧客データが流出する事件が発覚した。**

23 Starwood Hotels & Resorts Worldwide, Inc. "Letter From Our President - Updated"（http://www.starwoodhotels.com/html/HTML_Blocks/Corporate/Confidential/Letter.htm?EM=VTY_CORP_PAYMENTCARDSECURITYNOTICE）。

24

25 脆 **24日：ルート証明書をプリインストールされた状態で出荷されたPCや、このメーカの提供していたサポートツールがソフトウェアのインストール時にルート証明書をインストールしていたことが分かり、証明書の発行に使う秘密鍵が付属した状態だったことから、第三者が不正なサイトになりすましたり、MITM攻撃が可能なことから問題となった。**

26 詳細については、次のDELL社のBlogを参照のこと。"Response to Concerns Regarding eDellroot Certificate"（http://en.community.dell.com/dell-blogs/direct2dell/b/direct2dell/archive/2015/11/23/response-to-concerns-regarding-edellroot-certificate）。

27

28 セ **30日：銀行の残高照会ダイヤルの本人確認にシステム仕様上の不備があったことから悪用され、振り込み時に依頼人名として入力した電話番号が漏えいする事件が発生した。**

29 株式会社三菱東京 UFJ 銀行、「会員制サイト等の利用者として入力された電話番号の漏えいについて」（http://www.bk.mufg.jp/news/news2015/pdf/news1130.pdf）。

30 他 **30日：電気通信事業者がDoS攻撃などの通信を識別し、その対処を適法に実施するためのガイドライン「電気通信事業者におけるサイバー攻撃等への対処通信の秘密に関するガイドライン 第4版」が改定され、電気通信事業関連5団体より公表された。**
「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドラインの改定について」（https://www.jaipa.or.jp/topics/2015/11/post.php）。

※ 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

会保障番号など1,500万人分の個人情報が漏えいした可能性のある事件が発生しています。英国の通信会社TalkTalkでもWebサイトがSQLインジェクション攻撃による不正アクセスを受け、契約者400万人の情報が流出した可能性のある事件が発生しています。この事件に関連して、何者かにより漏えいした顧客データを公開するとしてビットコインによる脅迫が行われるなどしていましたが[*25]、その後15歳の少年がコンピュータ不正使用の容疑で逮捕されています。この事件では、原因としてWebサイトのXSSの脆弱性が指摘されています[*26]。米国のオンライン証券会社Scottrade社でも不正アクセスを受け、約460万人分の情報が流出したことを公表しています[*27]。オンラインフォーラムとして利用されているvBulletinの未修正の脆弱性を悪用し、vBulletin.comの利用者48万人分のパスワードデータを含む個人情報が漏えいする事件も発生しています。この脆弱性についてはすぐに修正されましたが、PoCコードが公開されるなどしたことから、攻撃が多く発生する可能性が指摘されています[*28]。また、日本のキャラクターのファン向けコミュニティサイトで、ユーザ情報330万件が誤って公開されていたことが判明し、対応が行われたり[*29]、米国の有権者情報1億9千万人分の個人情報が公開されているのが発見されています[*30]。この2つの事件では、サーバの設定不備により、第三者がアクセス可能な状態となっていたことが、セキュリティ研究者から指摘されています。

■ その他

10月には、Trump Hotel Collectionで、社内システムへのマルウェア感染による不正アクセスによって、顧客のクレジットカード情報が漏えいした可能性のあることが公表されています。ホテルでの情報漏えい事件としては、11月にもStarwood系列の50軒以上の北米のホテルでPOSマルウェア感染による、カード情報など顧客データが流出する事件が発生しています。更に、12月にはHyatt Hotelsでも支払処理システムへのマルウェア感染により、クレジットカードなどの支払い情報が漏えいした可能性のある事件が発生するなど、米国の大手ホテルチェーンを中心に、POSマルウェアの感染による顧客情報の漏えい事件が立て続けに発生しています。被害を受けたホテルの中には日本で営業を行っているホテルも含まれていました。

国内では、複数の地方公共団体で相次いで職員による住民情報や有権者データなどの持ち出しや情報漏えい事件が発生しています。これらの事件では、理由は様々ですが内部の規約に違反し、資料やデータをコピーするなどして持ち帰っていました。このうち、神奈川県三浦市では、職員が市民の個人情報を含んだ行政文書などのファイル計約200万件をUSBメモリーで持ち出して自宅で保管していたことが発覚しています[*31]。熊本県阿蘇郡西原村では、職員が全村民の住民基本台帳のデータなど、18万件を超える個人情報をPCやHDDにコピーし持ち出していたことが発覚しました[*32]。これらの事件では、第三者への譲渡など外部への情報漏えいは確認されていないと発表されています。大阪府堺市では、約68万人分の有権者情報を含むファイルを職員が自宅に持ち帰り、自身が契約していた外部サーバに公開状態で掲載していたことから、第三者に漏えいしたとの発表が行われました[*33]。この事件では、当該行為を行った職員に対し、懲戒免職処分が行われています。

11月には、ZeusやSpyEyeなどのマルウェアを販売目的で所持していたとして、不正指令電磁的記録保管・提供など複数の容疑で中学生が逮捕されています。逮捕された中学生は、海外のインターネットサイトなどから、これらのマルウェア作成ツー

*25 KrebsOnSecurity、"TalkTalk Hackers Demanded £80K in Bitcoin"(http://krebsonsecurity.com/2015/10/talktalk-hackers-demanded-80k-in-bitcoin/)。
*26 "video.talktalk.co.uk Security Vulnerability"(https://www.xssposed.org/incidents/93183/)。
*27 Scottrade, Inc.、"Cyber Security Update"(https://about.scottrade.com/updates/cybersecurity.html)。
*28 例えば、次のシマンテック公式ブログでは悪用の試みが増加しているとして注意喚起を行っている。「脆弱なvBulletinが稼働しているサーバーをさかんに探っているサイバー犯罪者に備え、今すぐパッチの適用を!」(http://www.symantec.com/connect/ja/blogs/vbulletin)。
*29 「香港企業運営のサンリオキャラクターサイトの脆弱性報道について」(http://www.sanrio.co.jp/wp-content/uploads/2015/05/20151224.pdf)。
*30 詳細については、例えば次のDataBreaches.netなどを参照のこと。"191 million voters' personal info exposed by misconfigured database (UPDATE2)"(http://www.databreaches.net/191-million-voters-personal-info-exposed-by-misconfigured-database/)。
*31 神奈川県三浦市、「本市職員による不正な行政情報の持ち出しに対するお詫びと報告について」(http://www.city.miura.kanagawa.jp/hisho/press/2015/documents/151002info.pdf)。
*32 熊本県阿蘇郡西原村、「行政情報の不適切な取扱い事案について(ご報告と再謝罪)」(http://www.vill.nishihara.kumamoto.jp/oshirase/_2012.html)。
*33 大阪府堺市、「職員の不祥事案について」(http://www.city.sakai.lg.jp/shisei/koho/hodo/hodoteikyoshiryo/kakohodo/teikyoshiryo_h27/teikyoshiryo_h2712/1214_02.files/1214_02.pdf)。

12月のインシデント

1 他 **1日：BlackBerry社は、パキスタン政府から電子メールやメッセージの監視を可能にするように要請を受けたことを明らかにし、要求は受けられないとして2015年末にパキスタンから事業撤退することを公表した。**
詳細については、次のBlackBerry社のBlogを参照のこと。"Why BlackBerry is Exiting Pakistan(Updated Dec 31)"(http://blogs.blackberry.com/2015/11/why-blackberry-is-exiting-pakistan/)。なお、この後、パキスタン政府と交渉で事業を継続することを発表している。"Continuing our Operations in Pakistan"(http://blogs.blackberry.com/2015/12/continuing-our-operations-in-pakistan/)。

5 セ **5日：ファイルを暗号化して拡張子を「.vvv」などに書き換えるランサムウェア（ファイルを暗号化して身代金を要求するマルウェア）に感染する事例が相次いで発生し話題となった。**
詳細については、例えば次のIBM社のTokyo SOC Reportなどに詳しい。「ランサムウェア CryptoWall への感染を狙った攻撃を11月下旬から連日確認」(https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/ransomware_20151208?lang=ja)。

7 他 **7日：内閣サイバーセキュリティセンターの主催で、重要インフラにおける分野横断的演習が実施された。**
「重要インフラにおける分野横断的演習の実施概要について～【2015 年度分野横断的演習】～」(http://www.nisc.go.jp/active/infra/pdf/bunya_enshu2015gaiyou.pdf)。

9 脆 **9日：Microsoft社は、2015年12月のセキュリティ情報を公開し、MS15-124やMS15-131を含む8件の緊急と、MS15-135など4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 12 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-dec)。

10 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見つかり、修正された。**
「APSB15-32：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/apsb15-32.html)。

12 セ **10日：安倍首相の個人サイトに対し、AnonymousによるDDoS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）。**

14 セ **14日：トルコの.trのccTLDレジストラであるNIC.trが大規模なDDoS攻撃を受け、名前解決ができなくなるなどの影響が出た。この攻撃への対処のため、一時的に海外からの問い合わせに対するフィルタを行い、対応したとされている。なお、この攻撃ではセカンダリを行っていたRIPEでも遅延が発生するなどの影響が発生した。**
詳細については、次のNIC.trの報告などを参照のこと。"14/12/2015 Tarihinde Başlayan DDoS Saldırısı"(https://www.nic.tr/2015-12-DDoS-Saldirisi-Kamuoyu- Duyurusu-20151221.pdf)。

15 脆 **15日：Joomla!に第三者からリモートでコード実行可能な脆弱性CVE-2015-8562）を含む複数の脆弱性が見つかり、修正された。**
"Joomla! 3.4.6 Released"(https://www.joomla.org/announcements/release-news/5641-joomla-3-4-6-released.html)。

16 脆 **16日：BIND9に、攻撃者が不正なクラス属性を持つレコードに対する問い合わせを行わせることで、DoS攻撃可能な脆弱性など複数の脆弱性が見つかり、修正された。**
Internet Systems Consortium、"BIND 9 Security Vulnerability Matrix"(https://kb.isc.org/article/AA-00913/)。

17 セ **17日：ブラジルで、WhatsAppが裁判所命令を無視したとして、WhatsAppのアプリケーションをブロックする裁判所命令が決定し、通信会社によって一時遮断された。**
裁判所命令については、次のサンパウロ州司法裁判所の発表を参照のこと。"16/12/2015 - Justiça determina bloqueio do aplicativo WhatsApp"(http://www.tjsp.jus.br/Institucional/CanaisComunicacao/Noticias/Noticia.aspx?Id=29056)（ポルトガル語）。この決定では48時間の停止を言い渡していたが、12時間程で撤回され、ブロックが解除された。"17/12/2015 - TJSP CONCEDE LIMINAR PARA RESTABELECER WHATSAPP"(http://www.tjsp.jus.br/Institucional/CanaisComunicacao/Noticias/Noticia.aspx?Id=29057)（ポルトガル語）。

18 脆 **18日：Juniper Networks, Inc.は、ScreenOSに、管理者権限でのリモートアクセスが可能な脆弱性及びVPN通信の復号が可能となる脆弱性が見つかったとして修正を行った。**
"2015-12 Out of Cycle Security Bulletin：ScreenOS：Multiple Security issues with ScreenOS（CVE-2015-7755, CVE-2015-7756）"(http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10713&actp=search)。

23 セ **23日：日本のキャラクターのファン向けコミュニティサイトに脆弱性があり、登録していた個人情報などが閲覧可能な状態であったことを公表した。**
"Security Advisory：Corrected a vulnerability involving personal information of SanrioTown.com members"(http://blog.sanriotown.com/blog/2015/12/22/security-advisory-corrected-a-vulnerability-involving-personal-information-of-sanriotowncom-members/)。

24 セ **24日：ウクライナの複数の電力供給会社で、マルウェア感染による変電所のシステムへの不正アクセスを受け、大規模な停電が発生した。**
詳細については、例えば次のSANS Industrial Control Systems Security Blogを参照のこと。"Confirmation of a Coordinated Attack on the Ukrainian Power Grid"(https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid)。

26 セ **26日：米国のホスティング事業者であるLinode社に対し、12日間に及ぶ大規模なDDoS攻撃が発生した。**
一連の攻撃については、次のLinode社のBlogに詳しい。"The Twelve Days of Crisis – A Retrospective on Linode's Holiday DDoS Attacks"(https://blog.linode.com/2016/01/29/christmas-ddos-retrospective/)。

※ 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

ルキットを入手していたことが報道されています。また、この中学生からマルウェアを購入・譲渡していたとして不正指令電磁的記録取得容疑で複数の中高生が書類送検されています。

同じく11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、第二次とりまとめが9月に策定されたことを受け、その対処を適法に実施するためのガイドライン「電気通信事業者におけるサイバー攻撃等への対処通信の秘密に関するガイドライン」が改定され、電気通信事業関連5団体より公表されています。今回の改定では、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、新たに整理されました。詳細については「1.4.3 電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドラインについて」も併せてご参照ください。

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10月から12月の期間にIIJ DDoSプロテクションサービスで取り扱ったDDoS攻撃の状況を示します。

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

DDoS攻撃には多くの攻撃手法が存在し、攻撃対象となった環境の規模(回線容量やサーバの性能)によって、その影響度合が異なります。図-2では、DDoS攻撃全体を、回線容量に対する攻撃[*34]、サーバに対する攻撃[*35]、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、954件のDDoS攻撃に対処しました。1日あたりの対処件数は10.37件で、平均発生件数は前回のレポート期間と比べて大幅に増加しました。これは、特定の攻撃先への攻撃が大規模に発生していたためで、全体の攻撃数の63.8%を占めています。DDoS攻撃全体に占める割合は、サーバに対する攻撃が67.7%、複合攻撃が30.7%、回線容量に対する攻撃が1.6%でした。

今回の対象期間で観測された中で最も大規模な攻撃は、複合攻撃に分類したもので、最大120万2千ppsのパケットによって2.87Gbpsの通信量を発生させる攻撃でした。

攻撃の継続時間は、全体の89.6%が攻撃開始から30分未満で終了し、10.1%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0.3%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1日と14時間15分(38時間15分)にわたりました。

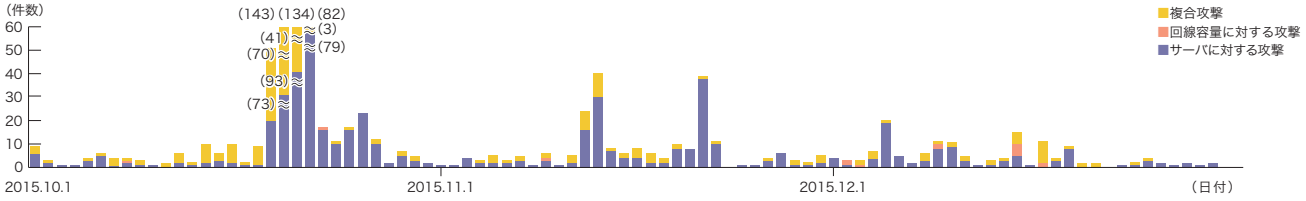


図-2 DDoS攻撃の発生件数

*34 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。

*35 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。

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[*36]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[*37]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[*38]によるDDoS攻撃のbackscatter観測結果を示します[*39]。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10月から12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49.4%を占めています。次いでWebサービスで利用される80/TCPが18.5%を占めており、上位2つで全体の67.9%に達しています。また、DNSで利用される53/TCP、HTTPSで利用される443/TCP、HTTPで利用されることがある8080/TCP、ゲームの通信で利用されることがある27015/UDPへの攻撃、通常は利用されない53261/TCPや3306/UDPなどへの攻撃が観測されています。

2014年2月から多く観測されている53/UDPは、1日平均のパケット数を見ると約4,600と、前回の約5,800から減少しましたが、引き続き高い水準にあると言えます。

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23.6%が最も大きな割合を占めています。その後に米国の20.0%、フランスの6.0%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、10月21日から11月6日にかけてと、11月13日及び18日にはISILに関連していると考えられるWebサイトへの攻撃、11月3日と6日に米国のオンラインカジノへの攻撃を観測しています。また、11月27日から29日にかけて家庭用ゲーム機のオンラインサービスプラットフォームへの攻撃、12月27日にはオランダのホスティング事業者のサーバに対する攻撃を観測しています。他のポートへの攻撃としては、10月14日から12月11日にかけて断続的に米国CDN事業者の複数のDNSサーバに対する53/TCPへの攻撃、11月25日から30日にかけてフランスのホスティング事業者のサーバに対する8080/TCPなどへの攻撃を観測しています。

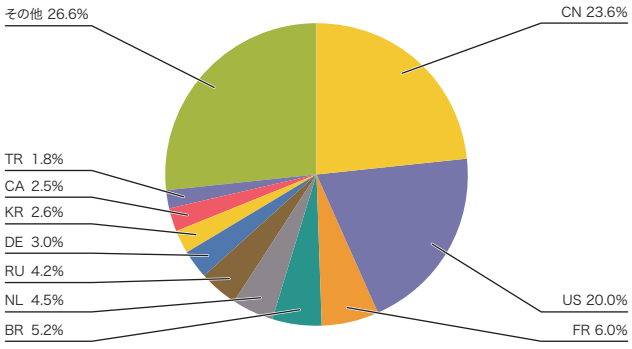


図-3 DDoS攻撃のbackscatter観測による攻撃先の国別分類

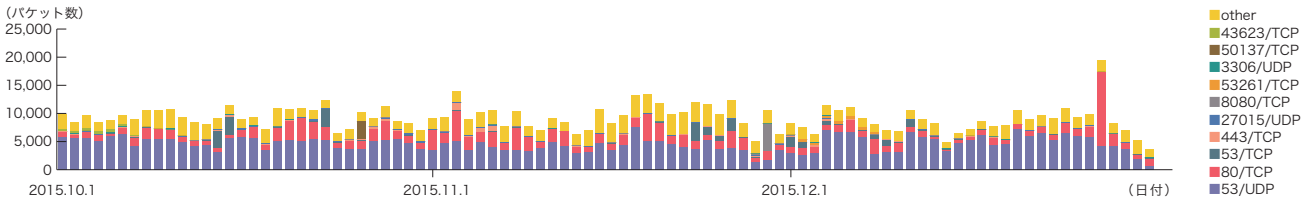


図-4 DDoS攻撃によるbackscatter観測(観測パケット数、ポート別推移)

*36 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。

*37 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。

*38 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。

*39 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。

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、12月14日から15日にかけてトルコを表すtrドメインのDNSサーバ群に対する攻撃、12月22日と24日にAnonymousによるトルコの政府と複数の銀行に対する攻撃、12月31日にイギリスの放送局が持つ複数のWebサーバに対する攻撃をそれぞれ検知しています。

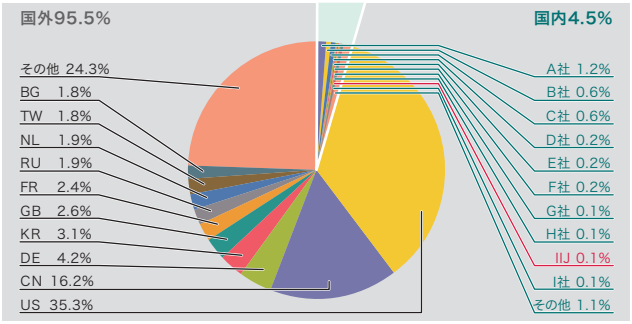


図-5 発信元の分布（国別分類、全期間）

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[*40]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[*41]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10月から12月の期間中に、ハニーポットに到着した通信の発信元IPアドレスの国別分類を図-5に示します。また総量（到着パケット数）に関して、本レポートの期間中に一番接続回数の多かった53/UDPと2番目を占める1900/UDPについて、その他の通信よりも突出して多かったため、それぞれ図-6、図-7に別途記載し、残りの推移を図-8に示します。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、図-6、図-7は国別に、図-8で

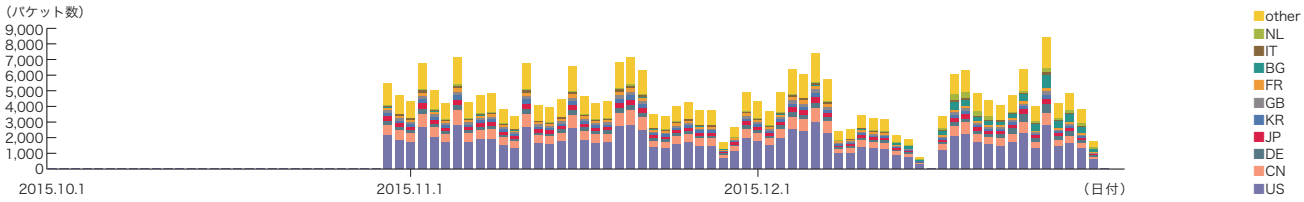


図-6 ハニーポットに到着した通信の推移（日別・53/UDP・1台あたり）

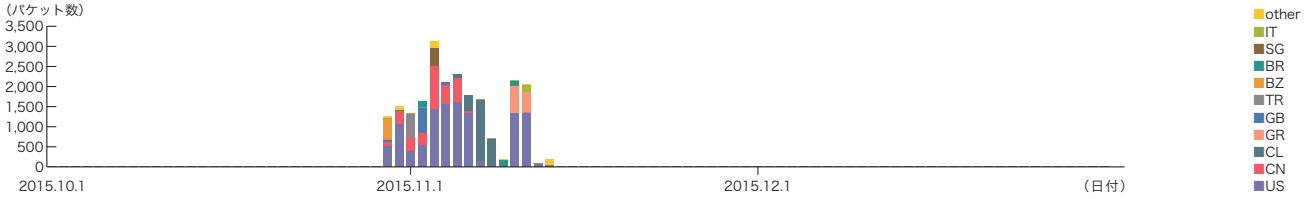


図-7 ハニーポットに到着した通信の推移（日別・1900/UDP・1台あたり）

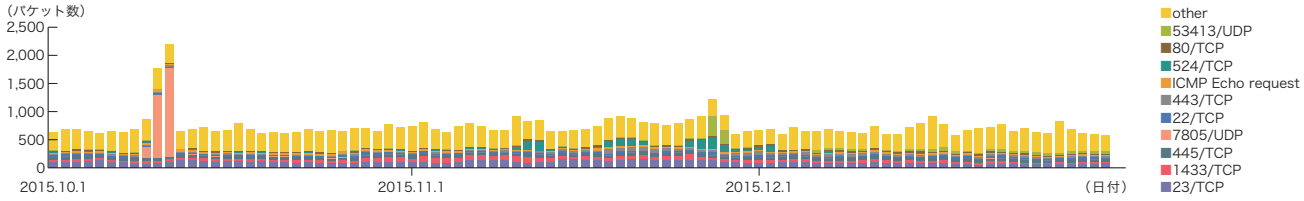


図-8 ハニーポットに到着した通信の推移（日別・宛先ポート別・1台あたり）

*40 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。
*41 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。

は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、DNSで使われる53/UDP、UPnPのSSDPプロトコルで使われる1900/UDP、telnetで使われる23/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、sshで使われている22/TCP、Webサーバで使われる80/TCP、443/TCP、ICMP Echo Request、NetWare Core Protocol（NCP）で使われる524/TCPなどでした。

10月30日より、53/UDPの通信が急増しています。この通信について調査したところ、特定のMITFハニーポットのIPアドレスに対し、主に米国、中国などに割り当てられた様々な送信元IPアドレスからのDNS名前解決のリクエストを繰り返し受けています。対象となるドメイン名も複数確認されていますが、多くが中国のギャンブルやゲーム、SF小説などに関連するサイトでした。これらの通信のほとんどは「ランダム.存在するドメイン」の名前解決を繰り返し試みたものであったことから、DNS水責め攻撃（DNS Water Torture）であると判断しています[*42]。

10月30日から11月13日にかけてSSDPプロトコルである1900/UDPが増加しています。主に米国、中国、チリ、ギリシャ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。

10月9日から11日にかけて7805/UDPが増加しています。調査したところ、様々な送信元IPアドレスから複数のDNS名に対する名前解決の戻りパケットのみが集中的に着信していました。

11月27日から28日にかけて53423/UDPが増加しています。調査したところ、Netis、Netcore製のルータの脆弱性を狙った攻撃の通信でした。この脆弱性は、2014年8月にトレンドマイクロ社によって報告されており[*43]、JPCERT/CCが2015年4月から6月にかけて攻撃が増加したことを報告しています[*44]。

■ 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-9に、マルウェアの総取得検体数の推移を図-10に、そのうちのユニーク検体数の推移を図-11にそれぞれ示します。このうち図-10と図-11では、1日あたりに取得した検体[*45]の総数を総取得検体数、検体の種類をハッシュ値[*46]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-10と図-11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73、ユニーク検体数が15でした。未検出の検体をより詳しく調査した結果、台湾、米国、メキシコ、中国などに割り当てられたIPアドレスでWorm[*47]などが観測されています。

未検出の検体の約55%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

＊42 Secure64 Software Corporation、"Water Torture：A Slow Drip DNS DDoS Attack"（https://blog.secure64.com/?p=377）。日本語での解説としては、株式会社日本レジストリサービス森下氏による次の資料が詳しい。「DNS水責め（Water Torture）攻撃について」（http://2014.seccon.jp/dns/dns_water_torture.pdf）。MITFハニーポットはDNSの問い合わせパケットを受信しても、権威サーバやキャッシュサーバに問い合わせに行かないため、攻撃には加担していない。
＊43 「UDPポートを開放した状態にするNetis製ルータに存在する不具合を確認」（http://blog.trendmicro.co.jp/archives/9725）。
＊44 「インターネット定点観測レポート（2015年4～6月）」（https://www.jpcert.or.jp/tsubame/report/report201504-06.html）。
＊45 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。
＊46 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。
＊47 Worm：Win32/Dipasik.A（https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Worm:Win32/Dipasik.A）。

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85.7%、ボット型1.4%、ダウンローダ型12.9%でした。また解析により、7個のボットネットC&Cサーバ[*48]と1個のマルウェア配布サイトの存在を確認しました。

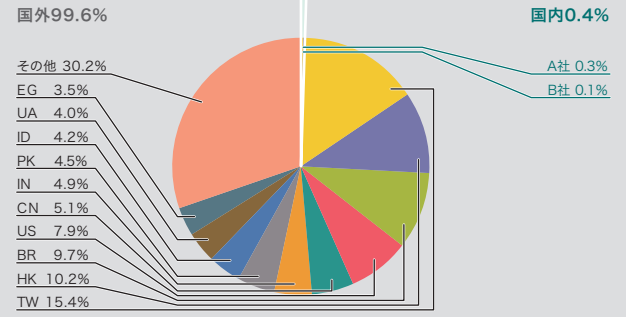


図-9 検体取得元の分布（国別分類、全期間、Conficker を除く）

■ 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17,905、ユニーク検体数は480でした。総取得検体数で99.6%、ユニーク検体数で96.9%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36%減少し、ユニーク検体数は前号から約12%減少しました。これは前号で報告したとおり、7月に増加した米国に割り当てられたIPアドレスからの感染活動が8月以降、観測されていないためです。Conficker Working Groupの観測記録[*49]によると、2016年1月1日現在で、ユニークIPアドレスの総数は426,262とされています。2011年11月の約320万台と比較すると、約13%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。

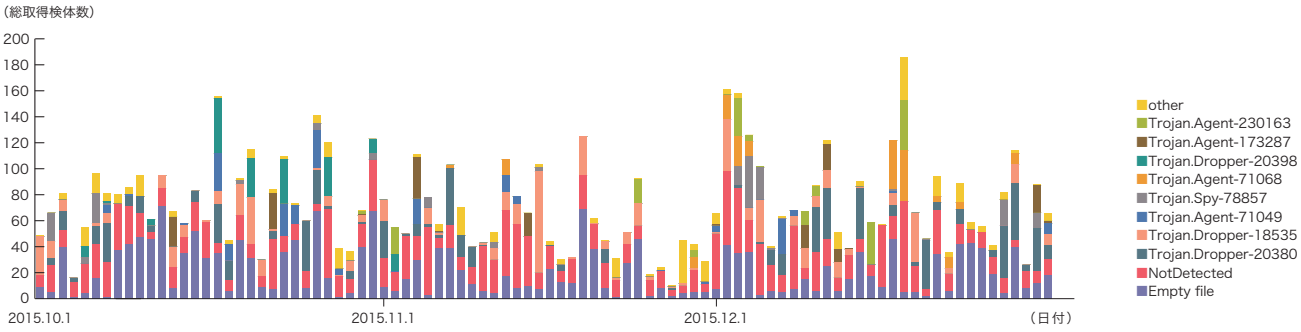


図-10 総取得検体数の推移（Conficker を除く）

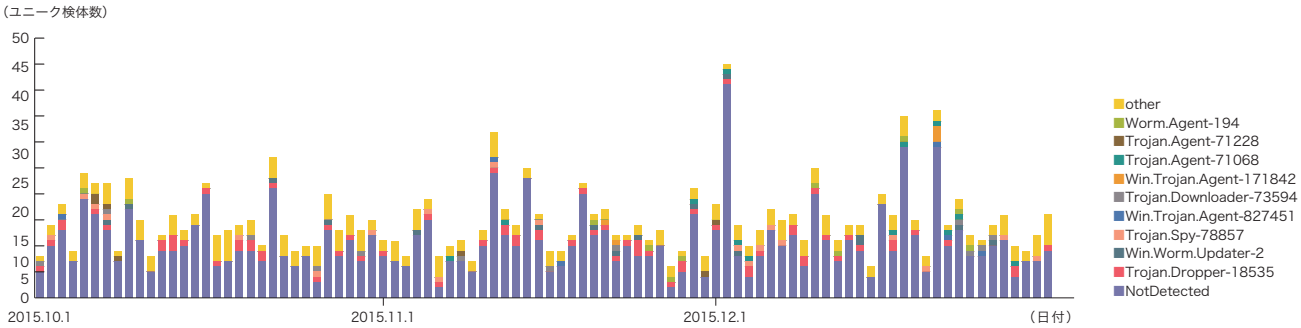


図-11 ユニーク検体数の推移（Conficker を除く）

*48 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。
*49 Conficker Working Groupの観測記録（http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking）。

1.3.3 SQLインジェクション攻撃

IIJでは、Webサーバに対する攻撃のうち、SQLインジェクション攻撃[*50]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10月から12月までに検知した、Webサーバに対するSQLインジェクション攻撃の発信元の分布を図-12に、攻撃の推移を図-13にそれぞれ示します。これらは、IIJマネージドIPS/IDS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35.4%、米国25.2%、日本17.9%となり、以下その他の国々が続いています。Webサーバに対するSQLインジェクション攻撃の発生件数は前回に比べて増加しています。

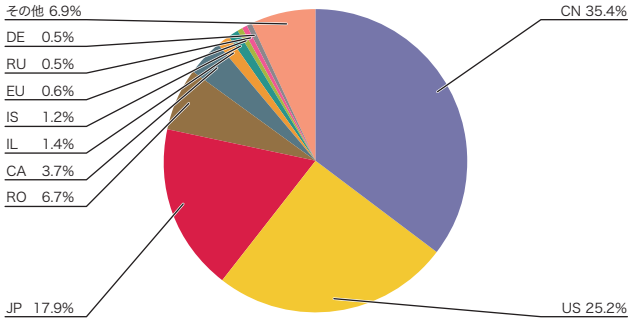


図-12 SQLインジェクション攻撃の発信元の分布

この期間中、10月10日には米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。10月12日から13日にかけて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。この攻撃元は11月3日にも別の特定の攻撃先への攻撃も行っています。11月8日にはイスラエル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。11月12日にはカナダ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。

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[*51]。

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。

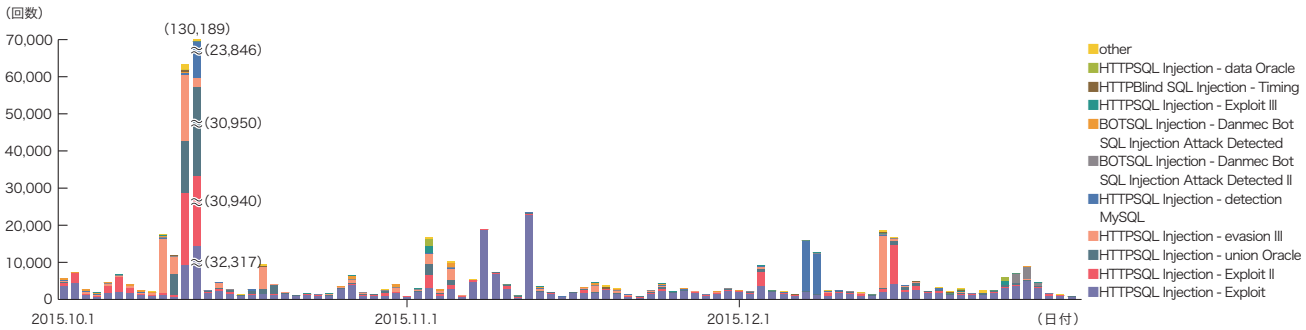


図-13 SQLインジェクション攻撃の推移(日別、攻撃種類別)

*50 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。

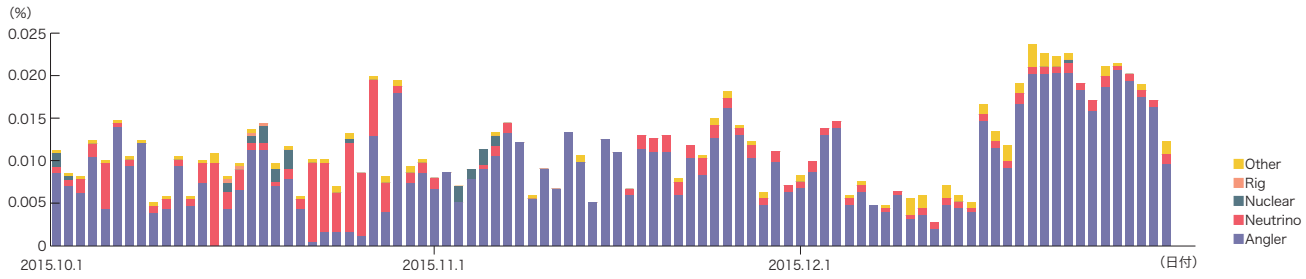
*51 Webクローラによる観測手法については本レポートのVol.22(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol22.pdf)の「1.4.3 Webクローラによる Webサイト改ざん調査」で仕組みを紹介している。

2015年10月から12月までの期間は、検知したドライブバイダウンロード攻撃の大部分をAnglerが占めました(図-14)[*52]。これは7月頃から変わらない傾向です。ドライブバイダウンロード攻撃の総数は、7月から9月に集計した値に比べて約4割増加しています。また、10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。その後11月には、ほとんどすべての攻撃でAnglerを用いるように戻りました。攻撃主体は、何らかの理由により、一時的にツールを変更していたようです。同様のツール切り換え、切り戻しと思われる変化は、8月及び9月にも断続的に合計3回観測されています。なお、期間中にはNuclearやRigによる攻撃も観測されましたが、いずれも小規模にとどまりました。

ダウンロードされるマルウェアの大部分はCryptoWall3.0/4.0でした。10月中はTeslaCrypt2.0/2.2も少数ながら確認されましたが、11月以降、TeslaCryptは観測されなくなりました。その他には、Necurs、Bedep、Tinbaなどのダウンロードが確認されました。また、Webサイト改ざんやMalvertisingによってExploitKitへ誘導される際に、遷移の途中で一般のオープンリダイレクタを経由させられるケースが複数確認されました。これは、Infectorへの直接のリダイレクト元を偽装したり、HTTPSのリダイレクタを使わせてProxyサーバなどに記録されるリファラヘッダを削除することで、攻撃へ至る遷移の分析を妨害したりする意図があるものと推測されます。

その他に、ブラウザにWindowsのブルースクリーンを模した画面を表示してマルウェアに感染したかのようなエラーを演出する詐欺サイトへの誘導が、11月下旬以降多数観測されました。これらのサイトでは、更に、ポップアップウィンドウで警告を表示して技術サポートと称する番号に電話をかけるよう促します。これらの詐欺サイトへの誘導では、過去に何らかのサービスに利用されていた複数のドメインが、失効後に再取得され不正サイトの入り口として悪用されていました[*53]。

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する状況が継続しています。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、外部から利用可能なリダイレクタを公開している場合は、前述のようなリンク元ロンダリングに悪用される可能性も考慮する必要があります。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の導入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十万サイト。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-14 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)

*52 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。

*53 同種の詐欺サイトについては弊社Security Diary「ISP情報を表示して偽のサポート窓口へ誘導する詐欺サイトに関する注意喚起」(https://sect.iij.ad.jp/d/2015/12/258504.html)で詳しく紹介している。

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、クラウドセキュリティの国際標準規格、Let's Encryptプロジェクトと証明書自動発行のためのACMEプロトコル、電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドラインについての3つのテーマについて紹介します。

1.4.1 クラウドセキュリティの国際標準規格

クラウドコンピューティングの概念は2006年にグーグル社によって提唱され、既に10年が経過しました。当初はその定義などについて様々な議論が沸き起こり、セキュリティ面での不安により導入を見送る組織も数多くありましたが、現在では広く一般に認知され、なくてはならないものとして受け入れられています。

しかしながら、組織が実際にクラウドサービスを利用しようとした場合、最も懸念することはセキュリティの問題であることに今も変わりはありません。その懸念を払拭すべく、クラウドサービス事業者（以下、事業者）はセキュリティ対策を行っていますが、対策の内容が各社によって異なるため、クラウドサービス利用者（以下、利用者）はどのサービスがより安全であるかを比較、判断し辛くなっています。クラウドサービスを利用するために相当の労力が必要となっていることも事実でしょう。

そのような問題を解決するための1つの手段として、クラウドサービスのセキュリティ管理に関する国際標準が検討されており、2015年12月にISO/IEC 27017:2015（以下、ISO 27017）が発行されました。ここでは、ISO 27017を活用するためのポイントなどについて解説を行います。

■ ISO 27017策定の背景

■ クラウドサービスの特徴

まず、ISO 27017を理解する前に、クラウドサービスの特徴を振り返ります。クラウドサービスはカスタマイズを行わない定型のサービスです。事業者はサービスの提供において、人が介在する要素を減らして自動化を行い、設備や運用体制を集約、共用してリソースを効率的に使用するなど様々な工夫を行うことで、コスト面やスケール面などのメリットを生み出しています。そのためクラウドサービスは、人手による個別対応やシステム内部の情報開示などを行うことが本質的に困難なサービスです。これはクラウドサービスの特徴として理解しておく必要があります。

この特徴は利用者によるセキュリティ管理を難しいものとしています。自組織の情報を管理するためには、自組織の情報を誰がどのように扱っているのかと詳細な管理状態を知る必要があります。しかし、自組織のセキュリティポリシーを適用する個別のシステム開発などと異なり、共用リソースであるクラウドサービスに対して特定組織のセキュリティポリシーを適用することはできません。そのため、事業者がセキュリティ管理状況を開示しない前提で、利用者は事業者が主張する安全策を自ら検証することなく契約し、クラウドサービスを利用することになります。

■ ISO 27017の策定

前述のようにクラウドサービスでは、利用者と事業者の間にセキュリティ管理についてのギャップが存在し、そのギャップを埋める様々な方法が考えられています。その1つとして、本レポートのVol.24ではクラウドセキュリティ推進協議会によるクラウド情報セキュリティ監査制度を取り上げました[*54]。クラウドサービスの安全性を確認するために各種のセキュリティ基準を使うことは、利用者にとっては事業者がどの程度セキュリティ基準に適合しているかが分かりやすく、また、事業者にとってはセキュリティ対策のレベルを容易に示すことができるなど、双方にメリットのある方法です。そのため、関連する国内、国外の組織、団体によって個別に様々な基準やガイドライン、認定制度などが作られました。しかしその結果として、数多くの独自基準ができてしまい、逆に事業者や利用者の混乱を生んでいることも否めません。クラウドセキュリティ管理基準の国際的な統一化は必然的に必要な状況となっていました。

そのような状況下で、日本では世界に先駆けて、クラウドセキュリティのガイドラインを経済産業省が発行しました[*55]。ISO 27017は経済産業省発行のガイドラインをベースに検討が開

*54 本レポート Vol.24「1.4.3 クラウドの安全性確認と監査制度」（http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol24.pdf）。
*55 経済産業省、「クラウドサービス利用のための情報セキュリティマネジメントガイドライン　2013年度版」（http://www.meti.go.jp/press/2013/03/20140314004/20140314004-2.pdf）。

始されており、日本が非常に重要な役割を担った国際規格と言えます。策定にあたっては、米英など各国の他にCloud Security Allianceなども参加し、多くの議論が交わされることとなりました。サービス提供が主体となる地域や国、また、その逆にサービス利用が主体となる地域や国、個別のセキュリティ規制を持つ地域や国など、立場が異なる人々の様々な意見を取り入れることにより、ISO 27017は少し複雑な構造になっています。次に、ISO 27017を理解するためのポイントをいくつか紹介します。

■ ISO 27017理解のポイント

■ 利用する立場の違い

繰り返しとなりますが、クラウドサービスは事業者が定めたスペックのサービスから自組織の要件に合うサービスを利用者が判断し選択します。これがISO 27017の基本的な発想であり、記述内容は利用者と事業者両方の内容が記載されています。ISO 27017を適用するにあたっては、事業者の立場でこの規格に準拠するか利用者の立場でこの規格に準拠するか、それとも両方の立場でこの規格に準拠するかをしっかりと認識することが混乱を避けるために重要です。

そこで必要となるのは、どこまでが事業者の責任範囲で、どこからが利用者の責任範囲となるかを明確にすることです。そうすることで、組織の責任範囲において、行うべき管理策が何かが分かります。そのためISO 27017では、利用者と事業者が、セキュリティの管理についてどちらが何をどのように行うべきか明確に区分するよう、責任分界(Shared responsibility)の項目が追加されています。

なお、IaaSを使ってSaaSを提供するようなサービスの事業者は同時に利用者でもあります。よって、そのようなサービスは利用者及び事業者両方の立場で準拠することとなります。

■ 章立て・構成

ISO 27017はISO/IEC 27002:2013(以下、ISO 27002)の追加管理策となっており、各章に記載されている管理策はISO 27002と番号が同じとなっています。そのため、ISO 27002をそのまま適用可能なものについては、"ISO/IEC 27002 apply."と記載されています。このことはつまり、本規格に準拠するためには、組織がISMSを実装できていることが前提となっている、ということです。

そもそもISO 27002はISO 27001を実装するための手引きという位置づけで、組織が自らのセキュリティ管理を具体的にどう行うか記載した文書であり、事業者が提供するサービスのセキュリティ管理策がどうあるべきかを定めるものではありません。よって、ISO 27002をベースとしているISO 27017も、利用者が自らのセキュリティ管理を行うにはどうするか、が基本的な考え方となっています。それに加えて、クラウドサービス事業者はクラウドサービス利用者の要求にどのように答えるべきか、という視点で内容が加筆されていると考えると分かりやすいでしょう。

実際の記述ですが、クラウド特有の考慮事項として、"Implementation guidance(実施の手引き)"が記載されています。"Implementation guidance"には、利用者が実装すべきこと、事業者が実装すべきことが個別に表形式で記載されています。双方が同じことを共同で行う場合は表が結合されて記載されています。実装の手引き以外に、注意すべき点や特筆すべき事項などがある場合には、"Other information"として記載されています。

加えて、ISO 27001にはそもそも存在していない、クラウドサービス特有の管理策がISO 27017には定義されています。具体的には、仮想環境のセキュリティ強化についての管理策、情報資産の消去についての管理策などがあります。これらクラウドサービス特有の管理策は本文内ではなく、Annex AにCLD x.y.zという番号で追加されているので、これらの考慮漏れがないように注意してください。

■ 利用方法

ここでは本規格の利用方法について説明します。利用者の利用方法としては、自組織でクラウドを利用する場合に、"Implementation guidance"に記載されている"Cloud service customer"の項目について実装を行います。先にも触れましたが、ISO 27017は、ISMSに準拠している組織がクラウドを利用するために何を追加的に行うかが記載されていますので、ISMSによるセキュリティ管理が行われていない場合は、まずそこから始める必要があります。ご注意ください。

一方、事業者の利用方法ですが、"Implementation guidance"に記載されている"Cloud service provider"の項目を参照して、利用者に提供する情報の内容やシステムが備えるべきセ

キュリティ機能を実装します。ログ管理や情報提供の仕組みなど、サービスの機能としてあらかじめ実装しておく必要があるものも存在するため、本規格に準拠するクラウドサービスを行う場合は、クラウドサービスを設計する時点で本規格の管理策を取り込むことが推奨されます。

■ 関連規格

ISO 27017以外にも、クラウドセキュリティに関連する国際標準規格が発行、並びに検討されています。具体的には現在検討中の物を含めて、ISO/IEC 17788:2014[*56]、17789:2014[*57]、NP 19086-4[*58]、27018:2014[*59]、DIS 27036-4[*60]などが挙げられますので、簡単に紹介します。なお、以下本文でISO/IECなどは省略しています。

17788はクラウドコンピューティングとは何か、どのような種類があるかといった定義や、ボキャブラリつまりクラウドの用語などを記載したものです。17789は、クラウドコンピューティングのアーキテクチャが記載されています。27017はこの2つの規格を踏まえて作られています。この2つの規格はオープンであり、ISOのWebサイトから自由にダウンロードして読むことが可能ですので、一読することをお勧めします。また、27018はクラウドサービスでプライバシーを扱う場合についての手引きが定義されています。その他に現在検討が行われているものとして、19086-4はクラウドサービスのSLAについて、27036-4はサプライチェーンの観点から、それぞれ標準化が試みられています。

更に、将来的にISO 27017を認証制度とすることが検討されており、国内では一般財団法人日本情報経済社会推進協会(JIPDEC)が認証を行うことを表明しています[*61]。認証制度が確立すれば、定められたセキュリティ水準に達しているクラウドサービスが第三者から認証されたサービスとして、より分かりやすくなりますので、利用者は手間なくその安全性を判断できることとなります。

■ まとめ

クラウドサービスを利用する上で懸念事項となっているセキュリティですが、管理策の国際標準化が行われることでより一層クラウドサービスを利用しやすくなる環境が整ってきました。IIJのクラウドサービスである「IIJ GIOサービス」でも、一部で既にISO 27017への対応を行っており、今後も対象範囲を順次拡大する予定です。IIJは、これからも積極的に国際標準の順守を推進し、安全安心なクラウドサービスを提供して参ります。

1.4.2 Let's Encryptプロジェクトと証明書自動発行のためのACMEプロトコル

X.509証明書[*62]は、公開鍵とその所有者の関係を保証するデータフォーマットで、サーバもしくはクライアントの公開鍵を安全に提示するためにSSL/TLSなどのセキュアプロトコルにおいて広く利用されています。公開鍵証明書は階層的に発行されており、証明書の発行者を順に辿ってトラストアンカーであるルート証明書に行き着くことで、当該証明書に格納される公開鍵を信用するPKI(Public Key Infrastructure)の仕組みを利用しています[*63]。SSL/TLSサーバに対しては商用のCAサービスで販売されており[*64]、サーバ証明書は表-1のように大きく分けて3種類に分類されます。このうち、DV証明書はドメイン名所有者かどうかの確認のみを行うため、ドメイン名所

*56 ISO/IEC 17788:2014 Information technology -- Cloud computing -- Overview and vocabulary(http://www.iso.org/iso/catalogue_detail?csnumber=60544)。
*57 ISO/IEC 17789:2014 Information technology -- Cloud computing -- Reference architecture(http://www.iso.org/iso/catalogue_detail?csnumber=60545)。
*58 ISO/IEC NP 19086-4 Information technology -- Cloud computing -- Service level agreement(SLA)framework and Technology -- Part 4:Security and privacy(http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=68242)。
*59 ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information(PII)in public clouds acting as PII processors(http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498)。
*60 ISO/IEC DIS 27036-4 nformation technology -- Security techniques -- Information security for supplier relationships -- Part 4:Guidelines for security of cloud services。
*61 JIPDEC、「ISMS適合性評価制度ISO/IEC 27017に基づくクラウドセキュリティ認証開始のお知らせ」(http://www.isms.jipdec.or.jp/topics/ISO27017_CLS.html)。
*62 RFC6818:Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List(CRL)Profile(https://datatracker.ietf.org/doc/rfc6818/)。
*63 本レポートのVol.13、「1.4.3 公開鍵証明書の不正発行事件」(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol13_infra.pdf)にてPKIの仕組みについて解説している。
*64 例えば、セコムトラストシステムズ社、「SSLサーバー証明書とは」(https://www.secomtrust.net/service/pfw/first/whatsssl.html)、クロストラスト社、「SSLとは?」(https://crosstrust.co.jp/support/beginner/ssl_about)。

有者がCSR（Certificate Signing Request）をCAの発行サイトに入力して発行依頼を行った後、当該ドメイン名の所有者かどうかを確認して証明書を発行する方法が一般的です。これに対し、OV証明書とEV証明書[*65]は、現実世界における組織の実在性確認を行うものであり、DV証明書とは大きく異なります。そのため、DV証明書は無償で発行する[*66]、もしくはそもそも発行しない事業者もあります。これはサーバ証明書の差別化を図るために、DV証明書ではなくOV証明書やEV証明書の購入を促すビジネスモデルにシフトしてきたとも考えられます。

Let's Encryptプロジェクト[*67]は、DV証明書を無償で自動発行する目的で設立されました。この自動証明書発行サービスでは、IETF ACME WGで策定されているACME（Automated Certificate Management Environment）プロトコル[*68]に準拠したものを利用しています。本稿では、Let's Encryptプロジェクトと、その実装で利用されているACMEプロトコルについて概要を説明します。

■ Let's Encryptプロジェクトの概要

Let's Encryptプロジェクトは、SSL/TLSで広く使われているサーバ証明書の自動発行サービスを提供しています。最近まで限られたテストユーザに対してだけ公開されていましたが、2015年12月初旬に一般に広く利用できるようになり、注目を浴びています[*69]。このプロジェクトは、非営利団体Internet Security Research Group（ISRG）[*70]により運営されており、ISRGのメンバー及びスポンサーには、Mozilla、EFF（Electronic Frontier Foundation）、Akamai、Ciscoなどの組織が名を連ねています[*71]。2015年12月、ブラウザベンダーの1つでメインプレイヤーであるChromeがプラチナスポンサーとして参画したことも注目すべき点です[*72]。

Let's Encryptプロジェクトでは、後述するACMEプロトコルを用いた参照実装が提供されています。ACMEクライアント（証明書発行依頼を行うユーザ）はLet's Encrypt clientを用い、ACMEサーバ（Let's Encryptプロジェクトが運営するCA）と通信することにより、証明書の発行、再発行、失効依頼などの処理を行うことができます[*73]。その中で、ドメイン名の保有者かどうかを確認するDomain Validationと呼ばれるいくつかの方式が提供されています。Let's EncryptプロジェクトのDomain Validationの解説[*74]では、ドメイン保有者であることの確認方法として、ACMEサーバ（CA）からのチャレンジに対して、（1）DNSレコードを制御する方法、（2）HTTPサーバのWebページを記載する方法の2種類のみが記載されていますが、ACMEプロトコルで定められている（3）SNI（Server Name Indication）を利用する方式も実装が対応しています。それぞれのDomain Validationの説明は後半を参照してください。

表-1 サーバ証明書の種類

DV（Domain Validated）証明書	ドメイン名の所在のみを確認して証明書を発行。
OV（Organization Validation）証明書	組織の所在（実在性）を確認をして証明書を発行。
EV（Extended Validation）証明書	CA/Bowser Forum で規定された手順に則り証明書を発行。ブラウザでURL記載部分が緑色になるなど、DV/OV証明書との更なる差別化が図られている。

*65 CA/Browser Forum、"EV SSL Certificate Guidelines"（https://cabforum.org/extended-validation/）。2007年に発行されて以来、改訂が続けられている。
*66 例えば、WoSign（https://buy.wosign.com/free/）やStartCom（https://www.startssl.com/Account）などがある。
*67 Let's Encrypt（https://letsencrypt.org/about/）。
*68 IETF、"Automated Certificate Management Environment（acme） - Documents"（https://datatracker.ietf.org/wg/acme/documents/）。
*69 Let's Encrypt、"Public Beta：December 3, 2015"（https://letsencrypt.org/2015/11/12/public-beta-timing.html）。
*70 Internet Security Research Group（ISRG）（https://letsencrypt.org/isrg/）。Chaos Communication Camp 2015においてISRGボードメンバーの1人であるPeter Eckersley（EFF）によるプレゼンが公開されている。"Let's Encrypt - A Certificate Authority To Encrypt the Entire Web"（https://media.ccc.de/v/camp2015-6907-let_s_encrypt）。
*71 Let's Encrypt、"Current Sponsors"（https://letsencrypt.org/sponsors/）。
*72 "Happy to announce that @GoogleChrome is a Platinum sponsor of Let's Encrypt!"（https://twitter.com/letsencrypt/status/679708931984248832）。
*73 "How It Works"（https://letsencrypt.org/howitworks/）にて、クライアントソフト（https://github.com/letsencrypt/letsencrypt）のインストール方法や利用方法が記載されている。"Welcome to the Let's Encrypt client documentation!"（https://letsencrypt.readthedocs.org/en/latest/）からより詳細な情報が得られる。また、ACMEサーバの参照実装（https://github.com/letsencrypt/boulder）に関する情報も記載されている。
*74 Technology（https://letsencrypt.org/howitworks/technology/）。

現在のLet's Encryptプロジェクトにおける様々なデータを閲覧することができます[*75]。その中には証明書発行枚数に関するデータがあり、執筆時では失効していない有効な証明書は70万枚程度との報告があります[*76]。24時間以内に処理された発行要求数と成功数に関するデータ[*77]によると、前述したDomain Validationのうち、HTTPサーバにページを追加する方式が7割から8割程度を占め、次いでSNIを利用する方式が見受けられます。一方で、DNSレコードを制御する方式は現状では数パーセントで推移しています。また、Let's Encryptプロジェクトにおける各種サーバ(Web、登録、OCSPサーバなど)のステータスやメンテナンス予告も参照できます[*78]。

Let's EncryptプロジェクトのACMEサーバから発行される証明書は"Let's Encrypt Authority X1"中間CAから発行されます。このとき"Let's Encrypt Authority X1"中間CA証明書はクロスルート証明書であり、2つの親を持ちます[*79]。そのうちの1つである"DST Root CA X3"は、OSやFireFoxの証明書ストア(信頼するルート証明書のリスト)に格納されています。そのため主要ブラウザのユーザは証明書ストアに手を加えることなく(トラストアンカーとしてルート証明書を追加することなく)Let's Encryptから発行されたサーバ証明書の検証に成功します。証明書の有効期間は90日[*80]に設定されており、これは通常購入できるサーバ証明書よりも短い期間となります。これは、秘密鍵が危殆化[*81]した際や、誤って証明書が発行された場合の影響を短くするためと説明されています。また、一部の環境では既に再発行作業も自動化されていることから、短い有効期限であっても、再発行に関わる工数は増えないと予測されます。

■ ACMEプロトコルの概要と策定状況

ACMEプロトコルについては、2014年11月にはMLが開設されて議論が進められており[*82]、2015年3月のIETF meeting 92ではBOF[*83]が開催されました。更に、2015年5月にはACME WGとして正式に活動を開始し[*84]、7月のIETF 93 meetingで会合が行われています[*85]。この時点では、メインのプロトコル仕様としてdraft-barnes-acme-04[*86]が議論されています。draft-barnes-acmeは、2015年1月から7月にかけて改訂された後、9月にはdraft-barnes-acme-04をベースにWG draftとしてacme-acme[*87]が登場し、本稿執筆時には-01のドラフトが登場しています。Editor's copy版[*88]は日付やdraft versionが正しくメンテナンスされていませんが、acme-acme-01から加筆されており、こちらが最も新しい仕様となります。acme-acmeはCharterによると、2016年3月までにIESG(Internet Engineering Steering Group)[*89]の提出を目指しており、現在もドラフトに関する議論が急ピッチで進められています。議論の内容はGitHubサイトで確認することができます[*90]。また、現在WG draftとして扱われている仕様はacme-acmeのみです。関連ドラフトとしてdraft-pepanbur-acme-proxy[*91]が挙げら

---

*75 Let's Encrypt Stats(https://letsencrypt.org/stats/)。
*76 Daily Activity(https://plot.ly/9/~letsencrypt/)。
*77 Challenges(last 24 hours)(https://plot.ly/11/~letsencrypt/)。
*78 Let's Encrypt、"All Systems Operational"(https://letsencrypt.status.io/)。
*79 Let's Encryptプロジェクトにおける証明書のパスは以下で確認できる。Certificates(https://letsencrypt.org/certificates/)。なおletsencrypt.org自身の証明書は"Let's Encrypt Authority X1"中間CAから発行されておらず、IdenTrust配下の別の中間CAから発行されている。
*80 Why ninety-day lifetimes for certificates?(https://letsencrypt.org/2015/11/09/why-90-days.html)。User Guide - Renewal(https://letsencrypt.readthedocs.org/en/latest/using.html#renewal)。
*81 暗号危殆化の事例は本レポートのVol.8(http://www.iij.ad.jp/development/iir/pdf/iir_vol08.pdf)の「1.4.1 暗号アルゴリズムの2010年問題」にて紹介している。
*82 acme@ietf.org Mail Archive(https://www.ietf.org/mailman/listinfo/acme)。
*83 ACME(Approved as BOF for IETF 92)(https://trac.tools.ietf.org/bof/trac/wiki/BofIETF92)。
*84 Automated Certificate Management Environment(acme):Charter for Working Group(https://datatracker.ietf.org/wg/acme/charter/)。
*85 IETF 93 meetingでのACME WGの議事録(https://www.ietf.org/proceedings/93/minutes/minutes-93-acme)やdraft-barnes-acmeに関するプレゼンテーション(https://www.ietf.org/proceedings/93/slides/slides-93-acme-1.pdf)が確認できる。
*86 draft-barnes-acme(https://datatracker.ietf.org/doc/draft-barnes-acme/)(https://letsencrypt.github.io/acme-spec/)。
*87 Automatic Certificate Management Environment(ACME)(https://datatracker.ietf.org/doc/draft-ietf-acme-acme/)。
*88 Automatic Certificate Management Environment(ACME)Editor's copy版(https://ietf-wg-acme.github.io/acme/)。
*89 Internet Engineering Steering Group(IESG)(http://www.ietf.org/iesg/)。
*90 GitHub、Automatic Certificate Management Environment(ACME)(https://github.com/ietf-wg-acme/acme)。acme-acmeに関するIssues(https://github.com/ietf-wg-acme/acme/issues)、Pull requests(https://github.com/ietf-wg-acme/acme/pulls)で策定状況を確認できる。
*91 ACME WGで扱うドキュメント一覧は次の"Automated Certificate Management Environment(acme)"(https://datatracker.ietf.org/wg/acme/documents/)で参照できる。執筆時は関連ドラフトとして"ACME Proxy Mode of Operation"(https://datatracker.ietf.org/doc/draft-pepanbur-acme-proxy/)が記載されている。

れていますが、IETF 94 meetingではacme-acmeのみが議論されました[*92]。

ここからは、ACMEプロトコルについてacme-acme-01のEditor's copy版(2016年2月12日取得)をベースに解説します。ACMEはJSON形式[*93]でやり取りするサーバ・クライアント間のプロトコルです。基本的には、ACMEサーバはHTTPSサーバとして振る舞い、ACMEメッセージはHTTPSで保護されています。ACMEサーバはCA側で証明書発行を受け付けるサーバで、ACMEクライアントは証明書発行依頼を行うユーザであり、Webサーバやメールサーバなど、サーバ証明書を必要とするサーバでクライアントソフトを動作させることを想定しています。このとき、クライアントとサーバは、共にPublic Key Pinning[*94]に対応することが推奨(SHOULD)されています。Public Key Pinningに対応することで、従来のような証明書チェーンを辿る方式と併用して、ACMEサーバの証明書が正しいものであることが保証されます。

HTTPSを通してクライアントからサーバに送信されるすべてのACMEメッセージはJWS(JSON Web Signature)[*95]を用いてクライアントにより署名が付与されます。この処理により、正しいクライアントからのメッセージであることを、サーバが検証可能となります。この仕組みを提供するためには、クライアントは証明書発行依頼などの前に、自身の公開鍵をACMEサーバに登録する作業が必要となります[*96]。具体的にはJSON Web Key形式[*97]の鍵データがメールアドレスや電話番号を格納するcontact情報と共にサーバに送付されます。このとき、署名に用いられる公開鍵は、サーバ証明書で用いられる公開鍵とは異なり、登録時に使用されるAccount Key Pairと呼ばれる別の鍵です。この登録時に利用された1つの鍵で、複数のFQDN(Fully-Qualified Domain Name)に対して証明書の発行依頼を行うことができます。本仕様においては、FQDNではなくidentifierという記載で抽象化されていますが、これは今後の拡張を想定しているためです。そのため現時点では、identifierの箇所をFQDNと読み替えても問題ありません。

ACMEサーバが提供するサービス一覧は、directoryと呼ばれるディスカバリサービス機能を用いて入手します。例えば、現在のLet's Encryptプロジェクトでは、クライアントがdirectoryに関するURLを指定することで、JSONデータを入手します[*98]。

ACMEではいくつかの種類のプロトコルメッセージが規定されており、クライアントは、directoryに記載されたURLに対して、規定されたデータにJWS形式で署名してPOSTで配送します。今回は、証明書発行から廃棄までの基本的なリソースのみを取り上げて説明します。通常、ACMEクライアントは以下のリソース順で一連の処理が行われます。

new-reg → new-authz → challenge → new-cert → revoke-cert

ACMEクライアントは、new-regリソースで登録処理を行った後、登録時に用いたAccount Key pairのうち秘密鍵を用いて署名を行います。そのためACMEサーバは、クライアントが登録したAccount Keyの管理をする必要があります。特に、同じAccount Keyで登録が行われた場合には、HTTPエラーとして409(Conflict)を返答することが規定されています。

*92 IETF meeting 94におけるACME WGのログ(https://www.ietf.org/proceedings/94/minutes/minutes-94-acme)やacme-acmeプレゼンテーション資料(https://www.ietf.org/proceedings/94/slides/slides-94-acme-0.pdf)が確認できる。
*93 "RFC7159:The JavaScript Object Notation(JSON)Data Interchange Format"(https://tools.ietf.org/html/rfc7159)。
*94 "RFC7469:Public Key Pinning Extension for HTTP"(https://tools.ietf.org/html/rfc7469)。IPAの「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/files/000045645.pdf)7.2.5節に、Public Key Pinningの設定方法が記載されている。
*95 "RFC7515:JSON Web Signature(JWS)"(http://tools.ietf.org/html/rfc7515)。URL-safeなBase64コーディング方法についてもAppendix Cに記載されている。通常のBase64エンコードした後"+"を"-"に、"/"を"_"(underline)に変換し、パディングデータである"="を削除する方式である。RFC4648にも同様の方法が記載されている。"Base 64 Encoding with URL and Filename Safe Alphabet"(http://tools.ietf.org/html/rfc4648#section-5)。
*96 2015年12月の時点ではLet's Encrypt プロジェクトのACMEサーバにおいてnew-regリソースのメッセージは確認できず、ディレクトリの入手後すぐにnew-certリソースメッセージが送付されている。
*97 "RFC7517:JSON Web Key(JWK)"(https://tools.ietf.org/html/rfc7517)。4.1節で"kty"(Key Type)Parameter にて鍵データ種類の記載が可能であり、"RFC7518:JSON Web Algorithms(JWA)"(https://tools.ietf.org/html/rfc7518)にて一覧できる。Let's Encryptプロジェクトの参照実装においてはRSAが利用されていたがRFC7518ではECが将来的に強く推奨(Recommended+)されており、実際Let's Encryptプロジェクトにおいても ECDSA証明書に対応されたことがアナウンスされている(https://twitter.com/letsencrypt/status/697504441075798016)。
*98 次のURLから入手できる(https://acme-v01.api.letsencrypt.org/directory)。JSONデータ内の"new-authz"などの第1項目はリソースと呼ばれており、acme-acme-01ではdirectoryリソースと合わせ5種類が定義されている。

登録処理後は、まず最初にnew-authzリソースを用いてidentifierの登録を行います。前述したように、identifierはFQDNですので、ここでは発行したいサーバ証明書の対象となるFQDNを登録することになります。ACMEクライアントはnew-regと同様にAccount Keyを用いてJWS形式で署名することで、当該Account Keyの所有者によるリクエストであることをサーバが認識できます。ACMEサーバはこのリクエストに対して、表-2に挙げられるDomain Validationのうちどれが可能かのリストを返却します。ACMEクライアントはchallengeリソースを用い、いずれか、または複数の手法を選択してchallengeのリクエストを送信します。サーバはFQDNの所有確認を行った後、その結果を返却します。成功時には、この時点で証明書発行の準備が整ったことになります。クライアントは、Account Keyとは別の公開鍵ペア(仕様ではSubject Public Keyと記載)を準備して、PKCS#10 Certificate Signing Request(CSR)を生成し、同様に、JWS形式の署名をAccount keyで施した上でnew-certリソースで証明書発行依頼を行います。サーバはJWSとCSR両方の署名検証を行い、証明書を発行した後、DERエンコーディングされた証明書を返却します。証明書を失効依頼する場合にはrevoke-certリソースを用い、当該証明書を格納してJWS形式の署名付でリクエストします。

Domain Validationとしてacme-acme-01では表-2に記載のhttp-01、dns-01、tls-sni-01などが規定されています。これらのタイプの接尾に「-01」とあるのは、ドラフトバージョンと連動していることを示しています。実際、既にtls-sni-02に対する議論が始まっています[*99]。ただし、今後ドラフト自体のバージョンアップのタイミングで手順が変更される場合には、ドラフトバージョンと連動して新しいタイプ名になりますが、Validationの手順に変更がない場合には、タイプ名はそのまま保持されます。

■ いくつかの懸念点

JWS署名の対象範囲は厳密に規定されておらず、緩やかな表現が現時点でのドラフトに記載されています。例えば、registrationリソースの形式としては、key、authorizations、certificatesフィールドも定義されていますが、実際にnew-regリソースをサーバが処理する際には、これらのフィールドを無視せねばなりません。ハッシュ関数に入力するデータのうち、処理が無視される箇所にダミーデータを格納することで、中間CA証明書の偽造[*100]やSLOTH攻撃[*101]が成功する要因となっており、潜在的な攻撃の余地を残すことになりかねません。

DV証明書は現実世界での実在性を確認しないため、悪用を意図したサーバに対しても発行される可能性があります。実際、Trojanの配布サーバに対して、Let's Encryptプロジェクトから発行された証明書が利用されていたことが、2016年1月初旬に報告されています[*102]。

表-2 acme-acme-01におけるDomain Validationの種類

	Type	クライアント側の処理	サーバ側の処理
HTTP (7.2節)	http-01	・tokenとAccount key(公開鍵)を連結して生成されるkey-authzデータを生成 ・80番ポートのHTTPサーバにHtttp://[FQDN]/.well-known/acme-challenge/[token]でアクセスできるようにし、key-authzデータを格納	・key-authzデータの生成 ・当該URLにアクセスして正しいデータが格納されているか検証
TLS SNI (7.3節)	tls-sni-01	・key-authzデータを生成 ・TLS SNI(RFC6066)の仕組みを用いてHTTPS経由でアクセスされるように準備 ・その際のSNIフィールドにはkey-authzにSHA-256でダイジェストを計算した後HEX表現に変換し、先頭32文字と接尾32文字から生成 ・上記SNIフィールドをsubjectAlternativeNameに持つ自己署名(オレオレ)証明書を発行しHTTPSサーバに設定	・key-authzデータの生成 ・TLS SNIの仕組みを利用してHTTPSサーバにアクセス ・証明書内のsubjectAlternativeNameが正しく生成されているか検証
DNS (7.5節)	dns-01	・key-authzデータを生成 ・key-authzにSHA-256でダイジェストを計算した後URL-safeなBase64エンコードしたデータを生成 ・DNSのTXTレコードに上記データを設定	・key-authzデータの生成 ・_acme-challenge.[FQDN]を正引きして正しく生成されているか検証

いずれのtypeもchallengeにtokenと呼ばれるランダムデータが含まれており、これは必須の項目である。ACMEサーバはtokenをchallenge特定のために利用するため、サーバで毎回新たに生成する必要がある。またguess攻撃を防ぐ必要があるため、少なくとも128ビット以上のエントロピーからランダムデータを生成することが求められている(MUST)。tokenはURL-safeな Base64エンコーディング方式で符号化されている。

*99 "Proposed changes to TLS-SNI, autorenewal removal"(https://mailarchive.ietf.org/arch/msg/acme/OnLEcxUa_K30ERLIZI5kAreyyh8)。
*100 "MD5 considered harmful today"(http://www.win.tue.nl/hashclash/rogue-ca/)。
*101 "SLOTH:Security Losses from Obsolete and Truncated Transcript Hashes(CVE-2015-7575)"(https://www.mitls.org/pages/attacks/SLOTH)。
*102 TrendLabs Security Intelligence Blog、"Let's Encrypt Now Being Abused By Malvertisers"(http://blog.trendmicro.com/trendlabs-security-intelligence/lets-encrypt-now-being-abused-by-malvertisers/)。

Let's EncryptプロジェクトはCertificate Transparency (CT)[*103]に対応しており、発行された証明書はログサーバ[*104]に通知されているため、誰でも証明書が閲覧できる状況にあり[*105]、国内ではCTに関する問題が以前から噴出していました[*106]。指摘されている懸念事項の1つにプライバシ問題があります。例えば、今後サービスインする予定のサーバのFQDNがリリース前に漏れてしまう点などが考えられます。今後、メールの到達性のみを確認することでS/MIME証明書が同様の仕組みで発行され、CTによってメールアドレスを一覧されてしまうケースも考えられます。

本稿執筆時には不透明な箇所もありますが、冒頭で紹介したように、ACMEメインプロトコルは急ピッチで標準化されており、identifierやchallengeにおいて新たな拡張が行われる可能性があります。また、実装・運用という観点では、Let's Encryptプロジェクトとは別の同様のサービスが登場する可能性も秘めています。これは、現在の証明書ビジネスが変化していくターニングポイントに来ていると捉えることができるかもしれません。

1.4.3 電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドラインについて

2015年11月30日、通信関連団体5団体で構成されるインターネットの安定的な運用に関する協議会により、「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン」の第4版が公開されました[*107]。ここではこのガイドラインについて解説します。

■ 経緯と改定の概要

このガイドラインは、日々変化するサイバー攻撃に対応するために、ISPなどの通信事業者が取り得る対策について例示することを目的としたガイドラインです。通信事業者において通信の遮断などの対策を行う場合に、電気通信事業法などの関連法令を考慮し、通信の秘密の侵害などの違法行為を行うことなく対策を実施するための参考資料として位置付けられるものです。このガイドラインは2007年初版以来、民間団体において自主的に策定し改定を重ねているものですが、2015年改定の第3版より、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[*108]」と連動し、民間側で課題となっているサイバー攻撃の対処の適法性について総務省研究会で検討し、その結果をガイドラインに反映する形で改定を重ねています[*109]。

通信事業においてサイバー攻撃などに対処することは、多くの場合において通信の秘密の侵害に当たりますが、特定の攻撃への対処の目的と限定的な対策手法の範囲においては正当業務行為として違法性が阻却される場合があり、このガイドラインでは研究会でまとめられた考え方に基づいて、適法となる範囲の対処を示しています。

今回の第4版の改定は、研究会の第二次とりまとめ[*110]及び、とりまとめとは別に発せられた「第三者によるIP電話等の不正利用への対策について」[*111]を元にしています。この結果、タイトルを従来の「大量通信等」から「サイバー攻撃等」に変更し、ガイドラインの「電気通信役務の不正享受」への対策を追加すると共に、次の5つの対策に関する記述が追加されました。

---

*103 "Certificate Transparency"(https://www.certificate-transparency.org/)。"RFC6962:Certificate Transparency"(https://tools.ietf.org/html/rfc6962)。
*104 "Known Logs"(https://www.certificate-transparency.org/known-logs)。
*105 Let's Encrypt Authority X1(https://letsencrypt.org/certs/lets-encrypt-x1-cross-signed.pem)から発行された証明書一覧(https://crt.sh/?Identity=%25&iCAID=7395)。
*106 漆嶌 賢二、「Certificate TransparencyによるSSLサーバー証明書公開監査情報とその課題の議論」(http://www.slideshare.net/kenjiurushima/certificate-transparencyssl)。
*107 インターネットの安定的な運用に関する協議会、「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドラインの改定について」(https://www.jaipa.or.jp/topics/2015/11/post.php)。
*108 総務省、「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」(http://www.soumu.go.jp/main_sosiki/kenkyu/denki_cyber/)。
*109 「電気通信事業におけるサイバー攻撃への適切な対処の在り方に関する研究会第一次とりまとめ」については、本レポートのVol23「1.4.3 電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」(http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol23.pdf)において解説している。
*110 総務省、「『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」(http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000100.html)。
*111 総務省、「第三者によるIP電話等の不正利用への対策について」(http://www.soumu.go.jp/main_content/000367498.pdf)。

1. DNSの機能を用いたDDoS攻撃への対策の強化
2. 脆弱性を有するホームルータなどの利用者への注意喚起
3. マルウェア感染端末とC&Cサーバなどとの通信に関するレピュテーションDBに基づいた遮断
4. 他人の認証情報を悪用したインターネットの不正利用への対処
5. 他人の認証情報を悪用したIP電話などの電話サービスの不正利用への対処

次に、それぞれについて解説します[*112]。

■ DNSの機能を用いたDDoS攻撃への対策

DNSの名前解決の機能を悪用し、アクセス制御などに問題のあるホームルータなどを踏み台として名前解決要求を行い、応答を引き出すことで大量通信を発生させるDNSamp攻撃については、この数年来大きな問題となっており、本ガイドラインの第3版の改定においてもその対応策が検討されています。今回の改定では、同様にDNSの機能を用いたDDoS攻撃の一種で、存在しないサブドメインに対する名前解決要求を大量に発生させることで、権威サーバやISPなどの提供するキャッシュDNSサーバに負荷を与えるような攻撃[*113]について考え方と対策例を示しています（ガイドライン中P13（キ））。このような攻撃に対して、ISPなどが利用者の名前解決のために提供しているDNSキャッシュサーバにおいて、その名前解決のFQDNを常時監視し、攻撃に関係するFQDNを判断してリスト化し、そのリストに基づいて名前解決の通信を遮断する対策について示しています。

■ 脆弱性を有するホームルータなどの利用者への注意喚起

DNSに限らず、NTPやSSDPなど複数の通信プロトコルについて、設定や機能に問題のあるホームルータなどの機器が攻撃の踏み台となり、通信を増幅させて大量通信を発生させ、DDoS攻撃を深刻なものとしています。また、機器から認証情報が漏えいし、第三者に悪用されるような場合も増えてきています。このような機器の全体数について、各ISPや業界団体などによる実態調査が行われていますが、特定のIPアドレスを用いて接続された機器に脆弱性や設定の不備があると判明した場合でも、そのIPアドレスに関する契約情報を参照して利用者を特定する行為が通信の秘密の侵害に当たるため、注意喚起と対策につなげることができませんでした。今回の改定では、調査行為そのものに関する適法性を示すと共に、調査の結果明らかとなった脆弱性を有する機器について、利用者を特定して注意喚起を実施できるとしています（ガイドライン中P24（ヒ））。

■ マルウェア感染端末とC&Cサーバなどとの通信に関するレピュテーションDBに基づいた遮断

研究会第一次とりまとめ及びガイドライン第3版において、Webで感染するマルウェアの感染予防として、URLに関するレピュテーション情報を用いてアクセス制限を行い、注意喚起のコンテンツを表示する対策手法について検討が行われ、事前の契約約款における同意の在り方とオプトアウトの手法を用意する前提で対策を行ってよいという判断になりました。第4版では、Webを利用しない感染活動や、マルウェアによる感染後のC&Cサーバとの通信を阻害する対策を検討しています。このためにFQDNに関するレピュテーションDBを用いて、DNSの名前解決時に通信を遮断することで実現する対策について、適法に実施できるとしています（ガイドライン中P25（フ））。この手法では、通信の遮断の事実やマルウェアに関する注意喚起をWebブラウザに表示するなどして利用者に示すことができないため、遮断を行わないDNSキャッシュサーバを用意して遮断を望まない利用者が利用できるようにするなどのオプトアウト策を同時に実施することが必要とされています。また、実施にあたっては、ISPなどと利用者の間における契約約款に基づく同意の在り方が厳密に検討され、少なくとも約款において規定すべき項目が示されています（研究会第二次とりまとめP14）。更に、マルウェアに感染し被害を受けることを望む利用者はいないということなどを前提とした適法性の判断であることから、このマルウェア感染予防とマルウェアの活動防止の目的以外において、例えば、違法・有害コンテンツへのアクセスにおいて、この手法を取ることは通信の秘密の侵害にあたる可能性があると判断されました（研究会第二次とりまとめP12及びガイドラインP26③）。

---

*112 本稿では研究会及びガイドラインで検討した状況をより分かりやすく示すために、平易な言葉で説明している。各対策の実際の適用にあたっては研究会とりまとめ及びガイドラインの記載を十分に検討した上で実施すること。

*113 このタイプの攻撃は、ランダムサブドメイン攻撃やDNS水責め攻撃などと呼ばれる。JPRS、JPRSトピックス＆コラム「Bot経由でDNSサーバーを広く薄く攻撃～DNS水責め攻撃の概要と対策～」（https://jprs.jp/related-info/guide/021.pdf）。

■ 他人の認証情報を悪用したインターネットの不正利用への対処

脆弱性を有するホームルータなどの装置から、インターネットの接続に利用するISPが提供した認証情報を不正に取得され、第三者により犯罪などに悪用される事例があることから、認証情報の悪用に関する対策が検討されました。ISPなどの認証サーバにおける認証の様態を常時調査し、例えば短時間に大量の認証を繰り返すことや、北海道の利用者が瞬時に九州から接続し直すなど、実際の移動が不可能な短時間に地域的な移動が行われている場合など、不正利用の蓋然性が高い認証の試みを見つけること、及びその情報を持って認証の処理を一時停止して、利用者に状況を確認することが対策として示されました(ガイドラインP27(へ))。

■ 他人の認証情報を悪用したIP電話などの電話サービスの不正利用への対処

IP電話に利用するSIPサーバへの不正アクセスにより不正に国際電話をかけられ、正規の利用者が心当たりのない通信費用を請求される事案が発生しています[*114]。この問題への対応として、契約者の国際電話料金などを一定の頻度で検知した上で、平時と比較して急増した場合に、相手国、発信元電話番号、発信IPアドレスなどを分析し、正規の利用者によるものかどうかを判断してよいと示されました。そして正規の利用者によるものでない蓋然性が高い場合には、利用者に連絡をしたり、連絡が取れない場合に当該回線に関する国際発信を休止したり、当該IPアドレスからのSIP認証を一時停止したりすることが対策として示されています(ガイドラインP28(ホ)、P29(マ))。また、これらを含む不正利用対策では対応が困難な場合、不正利用に用いられていると認められる特定国宛ての発信一般を、一時的に規制する手法も示されています(ガイドラインP29(ミ))。

■ まとめ

これまで示したように、本ガイドラインでは今発生しているサイバー攻撃への対策に関して、個別の対策を検討し、その適法性を示しています。その実現にあたっては、各通信事業者に関わる攻撃の状況や、コスト、副作用を最小とするための技術的検討項目など、様々な条件があるため、これらの対策のすべてが実施されるわけではありません。しかし、サイバー攻撃を取り巻く状況が日々変化する中、いざというときにすぐに参照できる規範が示されていることは、多くの通信事業者、及びその利用者にとって有益なものとなっています。

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、クラウドセキュリティの国際標準規格とLet's Encryptプロジェクトと証明書自動発行のためのACMEプロトコル、電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン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)
加藤 雅彦(1.4.1 クラウドセキュリティの国際標準規格)
須賀 祐治(1.4.2 Let's Encrypt プロジェクトと証明書自動発行のためのACMEプロトコル)
齋藤 衛(1.4.3 電気通信事業者におけるサイバー攻撃などへの対処と通信の秘密に関するガイドラインについて)
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:
小林 稔、小林 直、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

*114 総務省、「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)。