IIR

Internet
Infrastructure
Review

Jun.2016
Vol.31

インフラストラクチャセキュリティ

各種のランサムウェアとその対策

メッセージングテクノロジー

迷惑メール最新動向

技術トレンド

TLSの動向

IIJ
Internet Initiative Japan

Internet Infrastructure Review

June 2016 Vol.31

エグゼクティブサマリ

最近、仮想通貨の基礎技術として使われているブロックチェーンについての記事を多く見かけるようになりました。暗号化技術と相まって新たなビジネスや技術の可能性を広げるものだと期待される一方、ランサムウェアによる身代金支払いにビットコインが使われたりと、複雑かつ高度になっていく技術を使うことへの不安が入り混じっていると感じています。インターネットを安心して安全に使うための技術動向についてこれまでも繰り返しご紹介してきましたが、インターネットのインフラだけでなく、社会インフラとしてインターネットを使う上でのセキュリティについての理解を深めていただくために技術情報を提供することによって、こうした不安を払拭していくことも私どもの使命だと考えています。

本レポートは、このような状況の中で、サービスプロバイダとしてのIIJが、インターネットやクラウドの基盤を支え、お客様に安心・安全に利用し続けていただくために継続的に取り組んでいる様々な調査・解析の結果や、技術開発の成果、ならびに、重要な技術情報を定期的にとりまとめ、ご提供するものです。

１章では日々のインシデントや期間中に起きた出来事を中心に、これまでに取り上げた攻撃や事件のその後を追跡し分析しています。相変わらず、AnonymousなどによるDDoS攻撃が続いており、捕鯨問題に関連するところから端を発した直接関係なさそうな官公庁や個人サイトへの攻撃も観測されています。ランサムウェアへの感染による被害拡大が身代金を要求する手口へと巧妙化している現状や、その対処方法について解説することにより、こうした状況への対応の一助になればと考えています。また、暗号に関わる国際的な標準化動向についての解説も加えています。

2章では、ほぼ1年ぶりにメッセージングテクノロジーについて取り上げました。迷惑メールの割合は、一時的な増加はあるものの、ここ数年は総じて減少傾向にあります。技術動向については、DMARCの特徴を詳細に解説しながら、IIJサービスの中から得られた情報から補足説明を加えて解説しています。

3章では、技術トレンドとしてIETFでのTLSの議論を紹介します。同様の技術として長らくSSLが使われてきましたが、2011年から利用禁止が推奨され、TLSへの移行が推奨されています。ただ、TLSが制定されてから約17年、現在主流となっているTLS 1.2が策定されてから既に8年が経過しており、TLS 1.3の策定作業が急ピッチで進んでいます。本章では、TLS 1.2での動作解説を行いながら、最終的には変更となる可能性がありますがTLS 1.3で取り込まれる新技術も紹介し、理解を深めていただこうと考えています。

本号を発行する頃には「G7伊勢志摩サミット2016」が終わり、世界中がリオデジャネイロオリンピック・パラリンピック一色になり、その影で社会インフラのセキュリティ対策強化が急ピッチで進んでいると思います。様々なセキュリティ対策を講じる必要性をより強く感じられる今日この頃ですが、インフラ側だけでなく使う側の皆様と一緒に、社会インフラとなったインターネットを守る取り組みを考える上でも、今回の記事は参考になりましたでしょうか。

IIJでは、このような活動を通じて、インターネットの安定性を維持しながらも、日々改善し発展させていく努力を続けております。今後も、お客様の企業活動のインフラとして最大限に活用していただけるよう、様々なサービス及びソリューションを提供し続けて参ります。

山井 美和（やまい よしかず）
IIJ 常務執行役員 サービス基盤本部長。
1999年6月IIJに入社と同時に株式会社クロスウェイブコミュニケーションズへ出向し、WDM・SONET網構築、広域LANサービスの企画、データセンター建設に従事し、2004年6月に帰任。帰任後は、IIJのサービス運用部門を担当。2016年4月からはインフラ運用部門を加え、IIJの法人ITサービス全般の運用を統括。同時にIIJのデータセンター事業を統括し、国内初の外気冷却を用いたコンテナ型の「松江データセンターパーク」の立ち上げを主導している。

各種のランサムウェアとその対策

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2016年1月から3月までの期間では、依然としてAnonymousなどのHacktivismによる攻撃が複数発生しており、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継続しており、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。ランサムウェアの感染による被害も国内外で急速に拡大しており、米国の病院などで身代金の支払いに応じる事例も報告されています。また、別のサイトから取得したIDとパスワードのリストを使用したと考えられる不正ログインの試みも継続して発生しており、ポイントの不正利用などの金銭的な被害も発生しています。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、2016年1月から3月までの期間にIIJが取り扱ったインシデントと、その対応を示します。まず、この期間に取り扱ったインシデントの分布を図-1に示します[*1]。

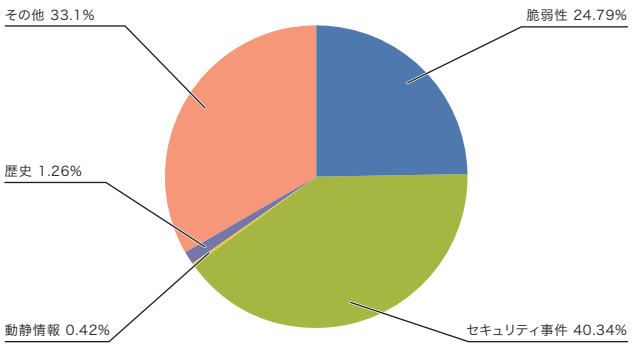


図-1 カテゴリ別比率(2016年1月〜3月)

■ 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。

日本で行われているイルカや小型クジラの追い込み漁への抗議活動として、昨年9月からAnonymousによると考えられる DDoS攻撃が断続的に行われていますが、この期間においても国内の多数のサイトにおいて被害が発生しています(OpKillingBay/OpWhales)。和歌山県太地町のWebサイトや捕鯨問題に関する映画の公式サイト、水族館のWebサイトなど直接関係するところだけに限らず、官公庁、空港会社、首相の個人サイトなど、過去に攻撃を実施したWebサイトも含めて繰り返し攻撃が行われていました。このオペレーションを実行していると思われる攻撃者らは攻撃対象とするターゲットリストをいくつか公開していますが、これらのリストに掲載されておらず、抗議活動とは直接には何ら関係がないと思われるWebサイトも多数被害を受けています。3月後半から攻撃活動はやや下火になっているものの、引き続き注意が必要な状況です。

フィリピンでは選挙管理委員会(COMELEC)のWebサイトが3月末にAnonymous Philippines及びLulzSec Philippinesという複数のグループによって攻撃されました。これによりWebサイトが改ざんされると共に、フィリピンの有権者およそ5,500万人分の個人情報が含まれるデータベースが盗まれ、インターネット上にすべて公開される事態となりました。データベースにはパスポートに関する情報や指紋情報なども含まれており、今後これらの情報が悪用される危険性が懸念されています。

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

■ 脆弱性とその対応

この期間中では、Microsoft社のWindows[*2*3*4*5*6*7*8]、Internet Explorer[*9*10*11]、Office[*12*13]、Edge[*14*15*16]などで多数の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でも四半期ごとに行われている更新が提供され、多くの脆弱性が修正されました。これらの脆弱性のいくつかは修正が行われる前に悪用が確認されています。

サーバアプリケーションでは、データベースサーバとして利用されているOracleを含むOracle社の複数の製品で四半期ごとに行われている更新が提供され、多くの脆弱性が修正されました。DNSサーバのBIND9でも、制御チャンネルの入力処理の不具合や、DNSSEC検証に利用される署名レコードの処理の不具合によって、外部からDoS攻撃が可能となる脆弱性などが見つかり修正されています。Linuxディストリビューションなどに含まれるThe GNU C Library(glibc)では、攻撃者が不正なDNS応答を送ることによって名前解決ライブラリの関数においてバッファオーバーフローが発生し、リモートからコード実行が可能となる脆弱性が見つかり修正されています[*17]。SSL/TLSの実装においても、ハッシュの衝突を利用してTLSの安全性を破る攻撃(SLOTH)、SSLv2の暗号通信を解読可能な攻撃(DROWN)、タイミング攻撃によってRSAの秘密鍵が復元可能となる攻撃(CacheBleed)などが見つかり、NSSやOpenSSLなどの実装においてそれぞれ脆弱性が修正されています。

ネットワーク機器に関して、製品にあらかじめ固定パスワードの管理用アカウントが設定されていて、バックドアとなりうる脆弱性がフォーティネット社やシスコ社の製品で見つかり、それぞれ修正されています。また鍵交換プロトコルIKEv1/IKEv2

*2 「マイクロソフト セキュリティ情報 MS16-003 - 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(3125540)」(https://technet.microsoft.com/ja-jp/library/security/MS16-003)。
*3 「マイクロソフト セキュリティ情報 MS16-005 - 緊急 リモートでのコード実行に対処する 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(3124584)」(https://technet.microsoft.com/ja-jp/library/security/MS16-005)。
*4 「マイクロソフト セキュリティ情報 MS16-012 - 緊急 リモートでのコード実行に対処する Microsoft Windows PDF ライブラリ用のセキュリティ更新プログラム (3138938)」(https://technet.microsoft.com/ja-jp/library/security/MS16-012)。
*5 「マイクロソフト セキュリティ情報 MS16-013 - 緊急 リモートでのコード実行に対処する Windows Journal 用のセキュリティ更新プログラム(3134811)」(https://technet.microsoft.com/ja-jp/library/security/MS16-013)。
*6 「マイクロソフト セキュリティ情報 MS16-026 - 緊急 リモートでのコード実行に対処するグラフィック フォント用のセキュリティ更新プログラム(3143148)」(https://technet.microsoft.com/ja-jp/library/security/MS16-026)。
*7 「マイクロソフト セキュリティ情報 MS16-027 - 緊急 リモートでのコード実行に対処する Windows Media 用のセキュリティ更新プログラム(3143146)」(https://technet.microsoft.com/ja-jp/library/security/MS16-027)。
*8 「マイクロソフト セキュリティ情報 MS16-028 - 緊急 リモートでのコード実行に対処する Microsoft Windows PDF ライブラリ用のセキュリティ更新プログラム (3143081)」(https://technet.microsoft.com/ja-jp/library/security/MS16-028)。
*9 「マイクロソフト セキュリティ情報 MS16-001 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム(3124903)」(https://technet.microsoft.com/ja-jp/library/security/MS16-001)。
*10 「マイクロソフト セキュリティ情報 MS16-009 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム(3134220)」(https://technet.microsoft.com/ja-jp/library/security/MS16-009)。
*11 「マイクロソフト セキュリティ情報 MS16-023 - 緊急 Internet Explorer 用の累積的なセキュリティ更新プログラム(3142015)」(https://technet.microsoft.com/ja-jp/library/security/MS16-023)。
*12 「マイクロソフト セキュリティ情報 MS16-004 - 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(3124585)」(https://technet.microsoft.com/ja-jp/library/security/MS16-004)。
*13 「マイクロソフト セキュリティ情報 MS16-015 - 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(3134226)」(https://technet.microsoft.com/ja-jp/library/security/MS16-015)。
*14 「マイクロソフト セキュリティ情報 MS16-002 - 緊急 Microsoft Edge 用の累積的なセキュリティ更新プログラム(3124904)」(https://technet.microsoft.com/ja-jp/library/security/MS16-002)。
*15 「マイクロソフト セキュリティ情報 MS16-011 - 緊急 Microsoft Edge 用の累積的なセキュリティ更新プログラム(3134225)」(https://technet.microsoft.com/ja-jp/library/security/MS16-011)。
*16 「マイクロソフト セキュリティ情報 MS16-024 - 緊急 Microsoft Edge 用の累積的なセキュリティ更新プログラム(3142019)」(https://technet.microsoft.com/ja-jp/library/security/MS16-024)。
*17 詳細については以下のIIJ Security Diaryの記事を参照のこと。「IIJ Security Diary:CVE-2015-7547 glibcにおけるgetaddrinfoの脆弱性について」(https://sect.iij.ad.jp/d/2016/02/197129.html)。「IIJ Security Diary:CVE-2015-7547 対策における信頼できるキャッシュサーバとは」(https://sect.iij.ad.jp/d/2016/02/225250.html)。

1月のインシデント

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

セ **6日：ドナルド・トランプ氏のWebサイトやPlayStation NetworkなどにDDoS攻撃が行われ、"New World Hacking"というグループが犯行声明を出した。**

脆 **7日：INRIAグループから、ハッシュの衝突を利用してTLSの安全性を破るSLOTH攻撃の手法が公開され、いくつかの実装でRSA-MD5を完全に利用不能にする修正が行われた。**
"miTLS, Triple Handshake, SMACK, FREAK, Logjam, and SLOTH"（http://www.mitls.org/pages/attacks/SLOTH）。

セ **12日：欧州各国の捜査機関の協力によりDD4BCの主要メンバーを逮捕したことを欧州刑事警察機構（EUROPOL）が発表した。**
"International action against DD4BC cybercriminal group | Europol"（https://www.europol.europa.eu/content/international-action-against-dd4bc-cybercriminal-group）。

脆 **12日：Adobe Acrobat及びReader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。**
「APSB16-02：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/apsb16-02.html）。

他 **12日：JPCERTコーディネーションセンターより、日本国内にある一定数の権威DNSサーバにて、ゾーン情報が取得可能であるとの情報が得られたことから、DNSゾーン転送の設定不備による情報流出の危険性に関する注意喚起が公表された。**
「DNS ゾーン転送の設定不備による情報流出の危険性に関する注意喚起」（https://www.jpcert.or.jp/at/2016/at160002.html）。

脆 **13日：Microsoft社は、2016年1月のセキュリティ情報を公開し、MS16-001など6件の緊急と3件の重要な更新を含む合計9件の修正をリリースした。**
「2016年1月のマイクロソフト セキュリティ情報の概要」（https://technet.microsoft.com/ja-jp/library/security/ms16-jan）。

セ **13日：国内企業のWebサーバに不正アクセスして顧客情報のリストを窃取した上で、当該企業に対して金銭を要求する恐喝未遂事件が発生した。**

セ **13日：日産自動車グループの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）。**

セ **13日：2015年に米CIA長官のJohn Brennan氏のメールアカウントを乗っ取ったハッカーグループが、米国家情報長官James Clapper氏のメールアカウントなども乗っ取った。**

他 **15日：Microsoft社がIntelの最新CPUである第6世代Core（開発コード名 Skylake）を搭載したパソコン、タブレットでのWindows 7/8.1のサポート期間について2017年7月17日で終了すると発表した。**
"Windows 10 Embracing Silicon Innovation | Windows Experience Blog"（https://blogs.windows.com/windowsexperience/2016/01/15/windows-10-embracing-silicon-innovation/）。

脆 **19日：Apple社はiOS 9.2.1とOS X El Capitan 10.11.3及びセキュリティアップデート2016-001をリリースし、ローカルユーザが特権を取得して任意のコードを実行できる可能性があるなどの複数の脆弱性を修正した。**
「iOS 9.2.1のセキュリティコンテンツについて - Apple サポート」（https://support.apple.com/ja-jp/HT205732）。「OS X El Capitan 10.11.3 およびセキュリティアップデート 2016-001のセキュリティコンテンツについて - Apple サポート」（https://support.apple.com/ja-jp/HT205731）。

脆 **20日：Oracle社は四半期ごとの定例アップデートを公開し、Java SEやOracle Database Serverなどを含む複数製品について、合計248件の脆弱性を修正した。**
"Oracle Critical Patch Update Advisory - January 2016"（http://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html）。

セ **23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）。**

他 **26日：サイバーセキュリティ戦略本部の第6回会合が行われ、サイバーセキュリティ推進体制の更なる機能強化に関する方針が決定された。**
内閣サイバーセキュリティセンター、「我が国のサイバーセキュリティ推進体制の更なる機能強化に関する方針」（http://www.nisc.go.jp/active/kihon/pdf/cs_kyoka_hoshin.pdf）。

セ **31日：金融庁、財務省、衆議院の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）。**

※ 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

において、転送量の増幅によってDoS攻撃の踏み台となるプロトコル仕様上の問題が見つかり、該当する複数の製品においてファームウェアの更新や回避策の公開などが行われています[*18]。

■ ランサムウェアによる被害の拡大

昨年後半からランサムウェアの感染による被害が国内外で拡大しており、この期間においても継続しています。ランサムウェアは「身代金要求型ウイルス」などと呼称されることもあるマルウェアの一種であり、感染するとコンピュータ内にある特定の種類のファイルなどを暗号化して人質にとり、復号のための鍵の提供に対してユーザにBitcoinなどで金銭を要求します。TeslaCrypt、Locky、Samas、Petyaなど複数種類のランサムウェアの感染活動が非常に活発になっており、個人ユーザだけでなく企業などの組織内でも被害が広がっています。特にこの期間内においては海外の病院での感染事例が多数報告されました。2月には米国のロサンゼルスにある病院で複数のコンピュータがランサムウェアに感染し、医療活動に支障が出る事態となりました。この病院では復旧を優先させるために総額で40BTC（約1万7千ドル）の身代金を支払ったと報告されています。この他にもドイツやニュージーランドでも病院でのランサムウェア感染被害が確認されています。こうしたことから3月にはUS-CERTがランサムウェアに関する注意喚起を行い、バックアップを取得しておくなどの対策を呼び掛けました。一方で一気に市場が拡大したことから暗号化の仕組みに不備があるような品質の低いものも多く、ランサムウェアの種類によっては身代金の支払いを行わなくてもファイルを復旧できる場合があります。ランサムウェアの詳細については「1.4.1 各種のランサムウェアとその対策」も併せてご参照ください。

■ 政府機関の取り組み

昨年に続いて政府は2月1日から3月18日までを「サイバーセキュリティ月間」と定め、政府機関はもとより、広く他の関係機関や団体などの協力の下、サイバーセキュリティに関する普及啓発活動を集中的に推進しました[*19]。

総務省は2月より「官民連携による国民のマルウェア対策支援プロジェクト（Advanced Cyber Threats response InitiatiVE（略称「ACTIVE」））」を通じたマルウェア感染者の被害未然防止の取り組みを開始したことを公表しました。一般財団法人日本データ通信協会テレコム・アイザック推進会議と連携して国内のインターネット・サービス・プロバイダ（ISP）事業者へ「ACTIVE」において得られたC&Cサーバに関する情報提供を行い、各ISP事業者において、当該情報に基づき、マルウェアとC&Cサーバ間の通信を抑止すると共に、マルウェアに感染した端末の利用者への注意喚起を行うことで被害を軽減するものです。この取り組みは総務省より昨年公表された「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」[*20]の内容に準じています。

また2月には「サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律案」が閣議決定されて第190回通常国会に提出され、両院での審議を経て4月14日に可決、成立しました。本改正案により、内閣官房内閣サイバーセキュリティセンター（NISC）による国の行政機関の情報システムの監視対象が、中央省庁だけでなく独立行政法人及び指定法人まで拡大し、監視体制の強化が段階的にすすめられます。またサイバーセキュリティに関する助言を行う国家資格「情報処理安全確保支援士」が新設されることになります。

■ その他

2015年12月に米国で起きたサンバーナーディーノ銃乱射事件の捜査に関連して、犯人の1人が所持していたiPhoneのロックをFBIが解除できるよう、技術的な支援を行うことをApple社に対して連邦裁判所が命令したことが2月に話題となりました。最新のiOSではiPhoneのロック解除やデータの抽出を製造元であるApple社自身も実施することは不可能な仕組みになっています。そのためFBIはロック解除に必要なパスコードを総当たりで試行できるように、このような試行を妨害するためのセキュリティ保護機能を無効にした特殊なソフトウェ

＊18 「JVNVU#91475438：Internet Key Exchange（IKEv1, IKEv2）がDoS 攻撃の踏み台として使用される問題」（https://jvn.jp/vu/JVNVU91475438/）。
＊19 内閣サイバーセキュリティセンター（NISC）、「2016年『サイバーセキュリティ月間』の実施について」（http://www.nisc.go.jp/press/pdf/csm2016_press1.pdf）。
＊20 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）。

2月のインシデント

1

セ 1日：Zeusマルウェアを自宅パソコンに保管していたとして、不正指令電磁的記録保管容疑で高校2年の少年が書類送検された。

2
3

脆 2日：Fisher-Price社のSmart Toyという幼児向けの知育玩具とhereOという子ども用GPS時計に認証機能を迂回されるなどの脆弱性が見つかり、修正された。
「JVNVU#99349751：フィッシャープライス Smart Toy 向けウェブサービスにおいて認証なしで API を呼び出せる脆弱性」(http://jvn.jp/vu/JVNVU99349751/index.html)。

4
5

セ 2日：国内の金融サービス事業者において、元従業員が顧客情報18件超と営業秘密を無断で社外に持ち出し、インターネット上に保存していたこれらの情報が第三者にも閲覧可能な状態となっていた。

6

他 2日：政府は「サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律案」を閣議決定し、国会に法案を提出した。
内閣官房、第190回通常国会国会提出法案「サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律案」(http://www.cas.go.jp/jp/houan/190.html)。

7
8

他 3日：欧州委員会と米国は、これまでのセーフハーバー協定に変わる新たなデータ移転の枠組み"EU-US Privacy Shield"の導入で合意した。
European Commission、"EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield"(http://europa.eu/rapid/press-release_IP-16-216_en.htm)。

9
10

他 6日：Twitter社が2015年半ばからテロ活動に関連する125,000件のアカウントを凍結したことを発表した。
"Combating Violent Extremism | Twitter Blogs"(https://blog.twitter.com/2016/combating-violent-extremism)。

11
12
13

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。
「APSB16-04：Adobe Flash Playerに関するセキュリティアップデート公開」(https://helpx.adobe.com/jp/security/products/flash-player/apsb16-04.html)。

セ 9日：米CIA長官や米国家情報長官のアカウント乗っ取りを行ったハッカーグループが米司法省のコンピュータに侵入し、数万人分の連邦政府職員の情報などを不正に取得して公開した。このハッカーグループのメンバーはその後イギリスなどで相次いで逮捕された。

14
15
16

脆 10日：Microsoft社は、2016年2月のセキュリティ情報を公開し、MS16-009など6件の緊急と7件の重要な更新を含む合計13件の修正をリリースした。
「2016年2月のマイクロソフト セキュリティ情報の概要」(https://technet.microsoft.com/ja-jp/library/security/ms16-feb)。

セ 10日：日本証券金融株式会社、国税庁、日本貿易振興機構の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)。

17
18
19

脆 17日：glibcライブラリに、バッファオーバーフローによってリモートからコード実行が可能となる脆弱性が見つかり、修正された。
"Google Online Security Blog：CVE-2015-7547：glibc getaddrinfo stack-based buffer overflow"(https://security.googleblog.com/2016/02/cve-2015-7547-glibc-getaddrinfo-stack.html)。

20
21

他 17日：FBIがサンバーナーディーノ銃乱射事件の犯人のiPhoneのロックを解除できるように、Apple社に対して技術支援を求める連邦裁判所の命令が出されるがApple社は命令に従うことを拒否した。
"Apple Litigation | USAO-CDCA | Department of Justice"(https://www.justice.gov/usao-cdca/apple-litigation)。

22
23

セ 18日：米国のロサンゼルスにある病院で複数のコンピュータがランサムウェアに感染し、医療活動にも大きな支障が出たため、システムの迅速な復旧を優先させるために総額40BTC(約1万7千ドル)の身代金を支払った。
Hollywood Presbyterian Mecical Center(http://hollywoodpresbyterian.com/default/assets/File/20160217%20Memo%20from%20the%20CEO%20v2.pdf)。

24
25

セ 19日：ファイル共有ソフトを使用した著作権法違反の一斉取り締まりが29府県警察において実施され、全国93箇所を捜索、44人が検挙された。
警察庁、「ファイル共有ソフトを使用した著作権法違反事件の一斉集中取締りの実施について」(http://www.npa.go.jp/cyber/warning/h28/H280219.pdf)。

26
27
28
29

セ 22日：Linuxのディストリビューションの1つであるLinux Mintのサーバが外部から不正に侵入され、ISOイメージファイルにマルウェアが混入した状態で一時的に公開された。またユーザフォーラムのデータベースにも侵入され、メールアドレスや暗号化されたパスワードなどのアカウント情報が流出した。
The Linux Mint Blog、"Beware of hacked ISOs if you downloaded Linux Mint on February 20th!"(http://blog.linuxmint.com/?p=2994)。The Linux Mint Blog、"All forums users should change their passwords."(http://blog.linuxmint.com/?p=3001)。

他 26日：総務省は「官民連携による国民のマルウェア対策支援プロジェクト(Advanced Cyber Threats response InitiatiVE(略称「ACTIVE」))」を通じたマルウェア感染者の被害未然防止の取り組みを開始したことを公表した。
総務省、「マルウェアに対する被害未然防止の実施」(http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000106.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

アを作成することをApple社に要求しました。これに対してApple社は裁判所命令を拒否して法廷で争う姿勢を見せていましたが、3月になってFBIが別の手段によってロック解除に成功したことから、訴訟は取り下げられて決着しました。しかし今回FBIがロック解除に成功した方法は最新機種のiPhoneには有効ではなく、他の捜査に関連して同様の要求がApple社に対して既に行われています。また米国議会ではテクノロジー企業に対して暗号解除を義務づける法案を提出する動きがあり、暗号規制をめぐる今後の動向が注目されています。

この期間でも、別のサイトから取得したIDとパスワードのリストを使用したと考えられる不正ログインの試みが継続して発生しています。ポイントサービスのサイトや、ゲームサイトなどが攻撃対象となっており、Webサイト上のポイントを不正に交換されるなどの金銭的な被害も発生しています。

フィッシング対策協議会に報告されているフィッシングの件数は昨年12月から急増しており、特に2月に入って金融機関の名を騙るフィッシングが複数の銀行で発生したことから、2月の報告件数は2,935件に昇っています[*21]。金融機関によっては、フィッシングメールではなく、SMSで誘導されるフィッシングサイトも見つかっており、引き続き注意が必要な状況です。

2月にはバングラデッシュ中央銀行において1億ドルを越える不正送金が発生し、銀行単一の被害金額としては過去最大の事件となりました。犯人は銀行内のシステムに不正にアクセスし、ニューヨーク連邦準備銀行が管理するバングラデッシュ中央銀行の外為為替口座からフィリピンとスリランカの銀行口座に不正な送金を指示しました。このとき送金先の口座名にスペルミスがあったことから不正が発覚しましたが、それまでに1億ドルを越える金額既に送金され、その大半は回収できていません。

2015年10月に米CIA長官John Brennan氏のAOLのメールアカウントなど、複数の米政府関係者のアカウントがハッカーグループに乗っ取られるという事件が起きました。このグループは1月に米国家情報長官James Clapper氏のアカウントを乗っ取ると、更に2月には米司法省の職員のコンピュータに侵入し、不正に取得した数万人分の連邦政府職員の情報をインターネット上のサイトに公開しました。その後このグループの複数のメンバーがイギリスなどで相次いで逮捕されましたが、いずれもティーンエイジャーでした。彼らはこれらの侵入を行うにあたりソーシャルエンジニアリングのテクニックを巧みに利用しました。例えばCIA長官が利用している電話会社Verizon社の技術者になりすましてVerizon社に電話して長官個人のアカウント情報を聞き出し、この情報を利用してメールアカウントのパスワードをリセットしました。また司法省の職員になりすましてヘルプデスクに電話して、コンピュータに侵入するのに必要なトークン情報を入手したりしていました。こういった攻撃手法は技術的な対策のみで防ぐことは難しく、情報開示ルールの整備と運用、教育など、人が弱点になることを考慮した多面的な対策が求められます。

1.3 インシデントサーベイ

1.3.1 DDoS攻撃

現在、一般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。

*21 フィッシング対策協議会、「2016/02 フィッシング報告状況」(https://www.antiphishing.jp/report/monthly/201602.html)。

3月のインシデント

1 セ 1日：出会い系サイトMate1.comからユーザのメールアドレスと平文パスワード約2,700万人分が漏えいし、ダークWeb上の掲示板で売りに出されていることが確認された。

1 脆 1日：SSLv2の暗号通信を解読可能なDROWN攻撃の手法、タイミング攻撃によってRSAの秘密鍵が復元可能となるCacheBleed攻撃の手法がそれぞれ研究者によって公開された。OpenSSLでは1.0.2gと1.0.1sでこれらの脆弱性を修正した。
"DROWN Attack"（https://drownattack.com/）。"CacheBleed：A Timing Attack on OpenSSL Constant Time RSA"（https://ssrg.nicta.com.au/projects/TS/cachebleed/）。"OpenSSL Security Advisory [1st March 2016]"（https://www.openssl.org/news/secadv/20160301.txt）。

3 セ 3日：国内のインターネットショッピングサイトにおいて、なりすましによる不正ログインが発生し、ポイントが不正に利用された。

3 他 3日：米国防総省が連邦政府機関としては初の試みとなる"Hack the Pentagon"というバグバウンティ（脆弱性発見報奨金制度）のプログラムを実施することを発表した。
U.S. DEPARTMENT OF DEFENSE、"Statement by Pentagon Press Secretary Peter Cook on DoD's "Hack the Pentagon" Cybersecurity Initiative"（http://www.defense.gov/News/News-Releases/News-Release-View/Article/684106/statement-by-pentagon-press-secretary-peter-cook-on-dods-hack-the-pentagon-cybe）。

8 脆 8日：Adobe Acrobat及びReader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。
「APSB16-09：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/apsb16-09.html）。

9 脆 9日：Microsoft社は、2016年3月のセキュリティ情報を公開し、MS16-023など6件の緊急と8件の重要な更新を含む合計14件の修正をリリースした。
「2016年3月のマイクロソフト セキュリティ情報の概要」（https://technet.microsoft.com/ja-jp/library/security/ms16-mar）。

10 脆 10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。
「APSB16-08：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/apsb16-08.html）。

17 他 17日：警察庁は、平成27年中のサイバー空間をめぐる脅威の情勢について公表した。標的型メール攻撃の報告件数が大幅に増加して過去最多となり、またインターネットバンキングに関わる不正送金事犯においても被害額が過去最悪となったことなどが述べられている。
警察庁、「平成27年中のサイバー空間をめぐる脅威の情勢について」（http://www.npa.go.jp/kanbou/cybersecurity/H27_jousei.pdf）。

21 脆 21日：Apple社はiOS 9.3とOS X El Capitan 10.11.4及びセキュリティアップデート2016-002をリリースし、リモートの攻撃者によって任意のコードが実行される可能性があるなどの複数の脆弱性を修正した。
「iOS 9.3のセキュリティコンテンツについて - Apple サポート」（https://support.apple.com/ja-jp/HT206166）。「OS X El Capitan v10.11.4およびセキュリティアップデート 2016-002のセキュリティコンテンツについて - Apple サポート」（https://support.apple.com/ja-jp/HT206167）。

24 脆 24日：Oracle Java SEにリモートから任意のコード実行が可能となる脆弱性（CVE-2016-0636）が見つかり、修正された。
"Oracle Security Alert for CVE-2016-0636"（http://www.oracle.com/technetwork/topics/security/alert-cve-2016-0636-2949497.html）。

25 セ 25日：米司法省はニューヨーク州にあるダムの制御システムや米国の主要な金融機関にサイバー攻撃を仕掛けたとして、イラン人7人を起訴したと発表した。
Department of Justice、"Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector"（https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged）。

27 他 31日：JPCERTコーディネーションセンターより、企業や組織が高度サイバー攻撃（APT）に備え対応するためのガイドとして利用することを想定した資料が公表された。
「高度サイバー攻撃（APT）への備えと対応ガイド～企業や組織に薦める一連のプロセスについて」（https://www.jpcert.or.jp/research/apt-guide.html）。

31 他 31日：IPAより、情報セキュリティ分野の専門家らによって選出された注目すべき脅威をまとめた解説資料「情報セキュリティ10大脅威2016」が公表された。
「情報セキュリティ10大脅威 2016」（https://www.ipa.go.jp/security/vuln/10threats2016.html）。

31 他 31日：病院などでのランサムウェアによる感染被害が世界的に拡大していることから、US-CERTから注意喚起が出された。
"Ransomware and Recent Variants"（https://www.us-cert.gov/ncas/alerts/TA16-091A）。

※ 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

■ 直接観測による状況

図-2に、2016年1月から3月の期間にIIJ DDoSプロテクションサービスで取り扱ったDDoS攻撃の状況を示します。

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

DDoS攻撃には多くの攻撃手法が存在し、攻撃対象となった環境の規模(回線容量やサーバの性能)によって、その影響 度合が異なります。図-2では、DDoS攻撃全体を、回線容量に対する攻撃[*22]、サーバに対する攻撃[*23]、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、293件のDDoS攻撃に対処しました。1日あたりの対処件数は3.22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減少しました。DDoS攻撃全体に占める割合は、サーバに対する攻撃が59.04%、複合攻撃が38.91%、回線容量に対する攻撃が2.05%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106万6千ppsのパケットによって2.86Gbps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85.67%が攻撃開始から30分未満で終了し、13.99%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0.34%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12時間26分(36時間26分)にわたりました。

攻撃元の分布としては、多くの場合、国内、国外を問わず非常に多くのIPアドレスが観測されました。これは、IPスプーフィング[*24]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[*25]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[*26]によるDDoS攻撃のbackscatter観測結果を示します[*27]。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。

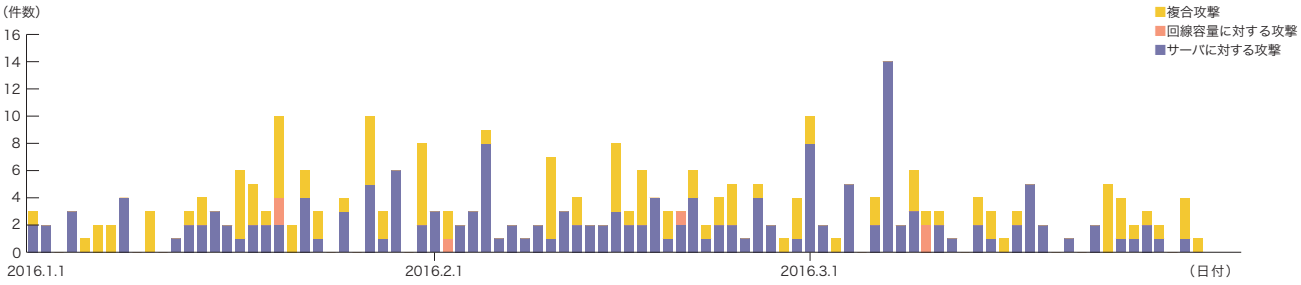


図-2 DDoS攻撃の発生件数

*22 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。

*23 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。

*24 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。

*25 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。

*26 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。

*27 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。

2016年1月から3月の間に観測したbackscatterについて、発信元IPアドレスの国別分類を図-3に、ポート別のパケット数推移を図-4にそれぞれ示します。

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49.5%を占めています。次いでWebサービスで利用される80/TCPが18.6%を占めており、上位2つで全体の68.1%に達しています。また、DNSで利用される53/TCP、バージョン管理システムCVSのサーバで利用される2401/TCP、HTTPSで利用される443/TCP、ゲームの通信で利用されることがある27015/UDPや25565/TCPへの攻撃、通常は利用されない83/TCPや43783/TCP、7829/TCP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で約5,300と、引き続き高い水準にあります。

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、米国の20.5%が最も大きな割合を占めています。その後に中国の20.1%、フランスの9.0%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、前回調査期間内の2015年11月27日から断続的に2月25日までオランダのデータセンター事業者のサーバへの攻撃、1月14日から20日にかけてと2月2日から13日にかけてフランスの非営利団体への攻撃、1月28日から3月10日にかけて中国のホスティング事業者のサーバへの攻撃、3月26日から31日にかけて米国アリゾナ州裁判所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、1月2日と1月19日から2月1日にかけて前回に引き続き米国CDN事業者の複数のDNSサーバに対する53/TCPへの攻撃、2月6日から3月16日にかけてクロアチアの通信事業者が持つ特定のIPアドレスに対する2401/TCPへの攻撃、2月27日から3月4日にかけてと3月28日から29日にかけてポーランドの企業Webサイトに対する83/TCPへの攻撃、3月11日から24日にかけてバングラデシュのISPが持つ特定のIPアドレスに対する7829/TCPへ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、期間中断続的に米大統領予備選挙候補者のWebサイトへの攻撃、1月3日から5日にかけてサウジアラビア国防省に対する攻撃、1月22日から24日にかけてアイルランド政府に対する攻撃、1月22日と25日に日本の空港会社のWebサイトへの攻撃、3月13日に米国ソルトレイクシティ警察のWebサイトへの攻撃をそれぞれ検知しています。

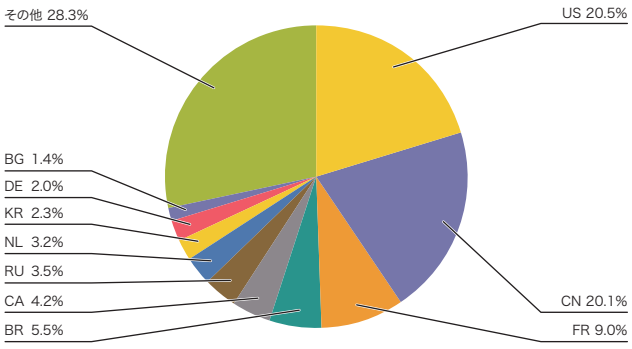


図-3 DDoS攻撃のbackscatter観測による攻撃先の国別分類

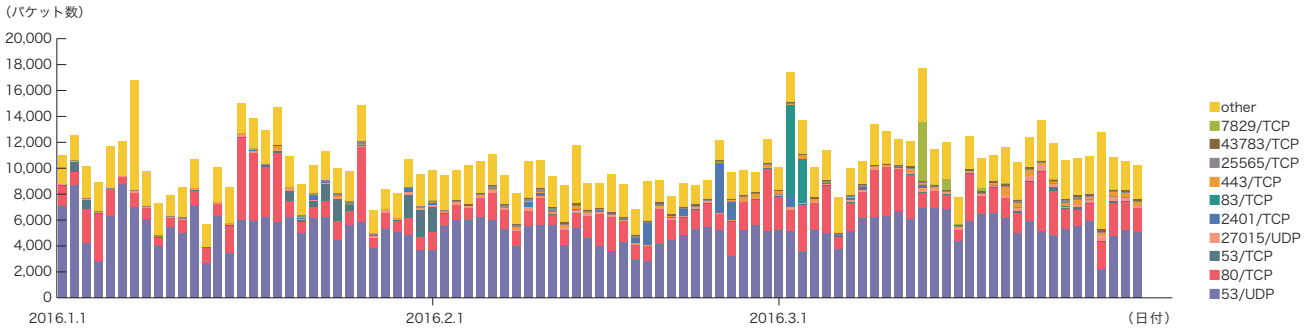


図-4 DDoS攻撃によるbackscatter観測(観測パケット数、ポート別推移)

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[*28]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[*29]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。

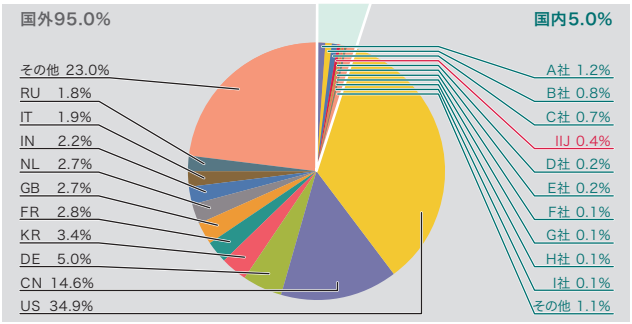


図-5 発信元の分布(国別分類、全期間)

■ 無作為通信の状況

2016年1月から3月の期間中に、ハニーポットに到着した通信の発信元IPアドレスの国別分類を図-5に示します。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はその他の通信よりも突出して多かったため、図-6に別途記載し、残りの推移を図-7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は国別に、図-7で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。

前回のレポート期間と同様に、53/UDPの通信が高い値を示しています。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

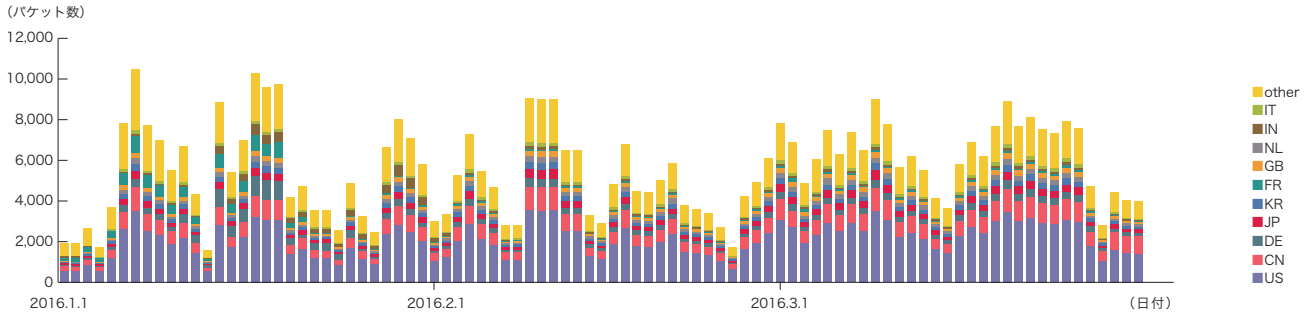


図-6 ハニーポットに到着した通信の推移(日別・53/UDP・1台あたり)

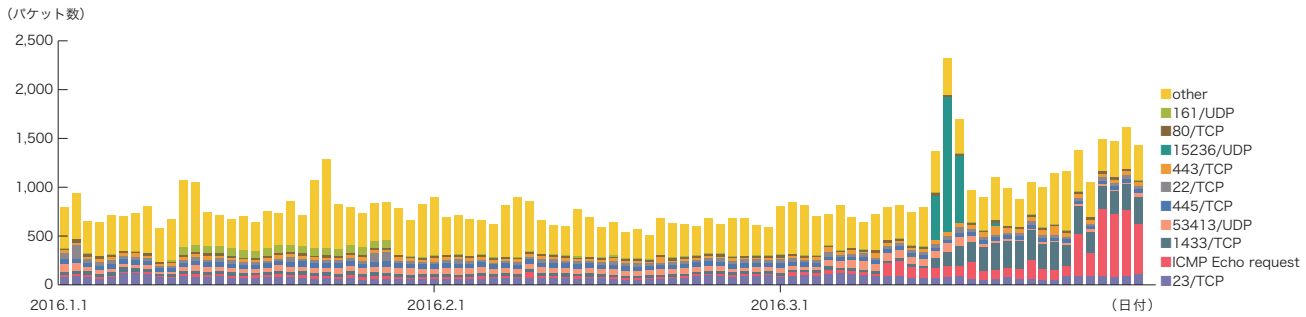


図-7 ハニーポットに到着した通信の推移(日別・宛先ポート別・1台あたり)

*28 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。
*29 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。

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、多くが中国の通販サイトやゲーム、SF小説などに関連のサイトでした。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[*30]。

3月17日以降、ICMP Echo Request、1433/TCPが増加しています。調査したところ、中国に割り当てられたIPアドレスを中心とした多数のIPアドレスからの通信でした。

本レポート期間中、53413/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によって報告されており[*31]、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[*32]。

1月中旬から下旬にかけて、日本のIPアドレスからSNMPが増加しています。調査したところ、ヤマハ社製のルータのCPU使用率や稼働時間、送信バイト数などのリクエストが繰り返し行われていました。

■ 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-8に、マルウェアの総取得検体数の推移を図-9に、そのうちのユニーク検体数の推移を図-10にそれぞれ示します。このうち図-9と図-10では、1日あたりに取得した検体[*33]の総数を総取得検体数、検体の種類をハッシュ値[*34]で分類したものをユニーク検体数としています。また、検体をウイルス対策ソフトで判別し、上位10種類の内訳をマルウェア名称別に色分けして示しています。なお、図-9と図-10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。

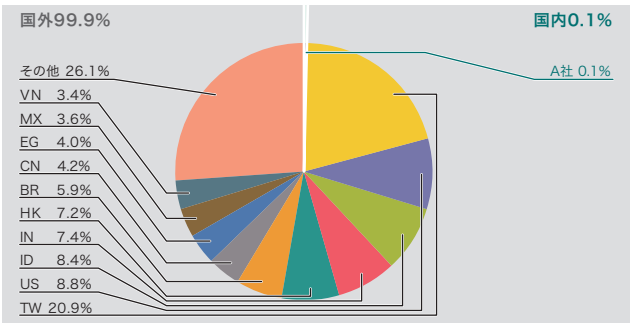


図-8 検体取得元の分布(国別分類、全期間、Confickerを除く)

*30 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。

*31 「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)。

*32 「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)。

*33 ここでは、ハニーポットなどで取得したマルウェアを指す。

*34 様々な入力に対して一定長の出力をする一方向性関数(ハッシュ関数)を用いて得られた値。ハッシュ関数は異なる入力に対しては可能な限り異なる出力を得られるよう設計されている。難読化やパディングなどにより、同じマルウェアでも異なるハッシュ値を持つ検体を簡単に作成できてしまうため、ハッシュ値で検体の一意性を保証することはできないが、MITFではこの事実を考慮した上で指標として採用している。

期間中の1日あたりの平均値は、総取得検体数が91、ユニーク検体数が14でした。未検出の検体をより詳しく調査した結果、台湾などに割り当てられたIPアドレスでWorm[*35]や、インドに割り当てられたIPアドレスでトロイの木馬[*36]などが観測されています。

未検出の検体の約58%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89.6%、ボット型7.8%、ダウンローダ型2.6%でした。また解析により、7個のボットネットC&Cサーバ[*37]の存在を確認しました。

■ Conficker の活動

本レポート期間中、Confickerを含む1日あたりの平均値は、総取得検体数が11,902、ユニーク検体数は428でした。総取得検体数で99.5%、ユニーク検体数で96.8%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33%減少し、ユニーク検体数は前号から約11%減少しました。本レポート期間中、全体的に緩やかに減少していました。Conficker Working Groupの観測記録[*38]によると、2016年4月現在で、ユニークIPアドレスの総数は60万台とされています。2011年11月の約320万台と比較すると、約19%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。

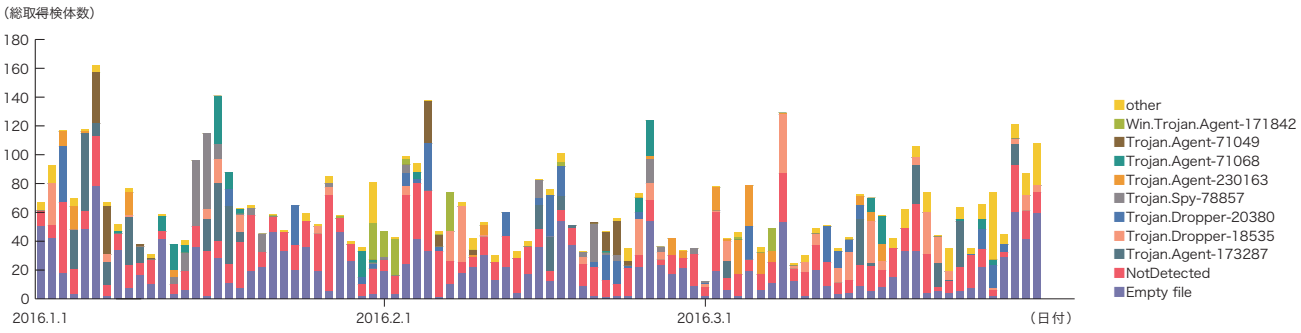


図-9 総取得検体数の推移(Confickerを除く)

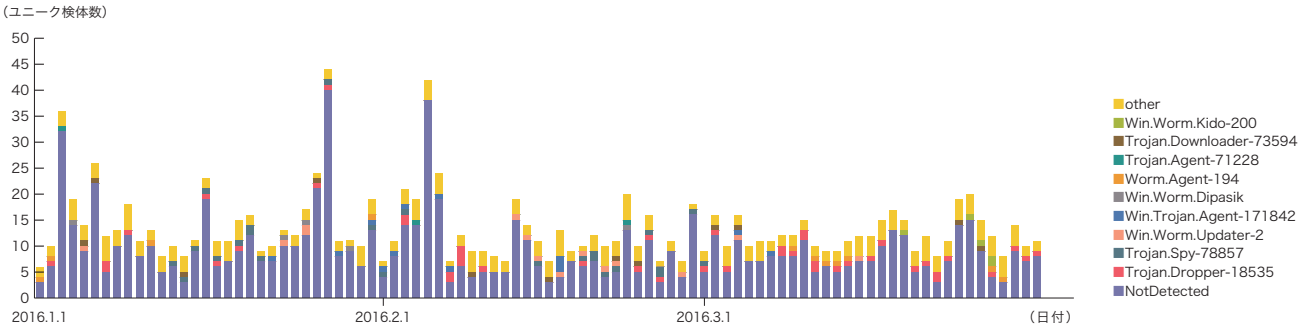


図-10 ユニーク検体数の推移(Confickerを除く)

*35 Worm:Win32/Dipasik.A(https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Worm:Win32/Dipasik.A)。
*36 Virus:Win32/Ceg.A(https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Virus:Win32/Ceg.A)。
*37 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。
*38 Conficker Working Groupの観測記録(http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking)。本レポート期間中、数値のデータが1月7日以降表示されていないため、4月前半の最高値をグラフから目視で確認して採用している。

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[*39]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。

2016年1月から3月までに検地した、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-11に、攻撃の推移を図-12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38.0%、米国27.2%、中国24.5%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は日本以外の国では前回と比べて減少傾向にありますが、日本を送信元とする攻撃が前回の3倍弱に増加しているため、発生件数の合計は前回より増加しています。

この期間中、1月25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。3月7日には中国の特定の攻撃元から特定の攻撃先に対する攻撃が発生しています。3月27日から29日にかけて日本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。

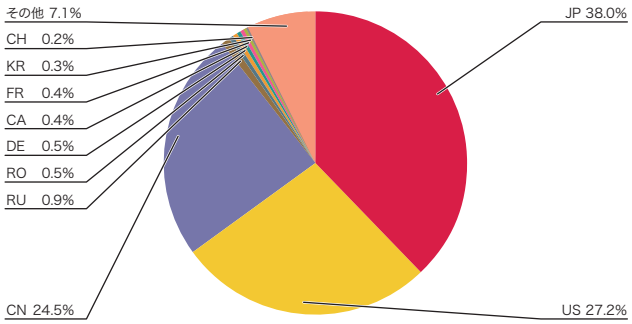


図-11 SQLインジェクション攻撃の発信元の分布

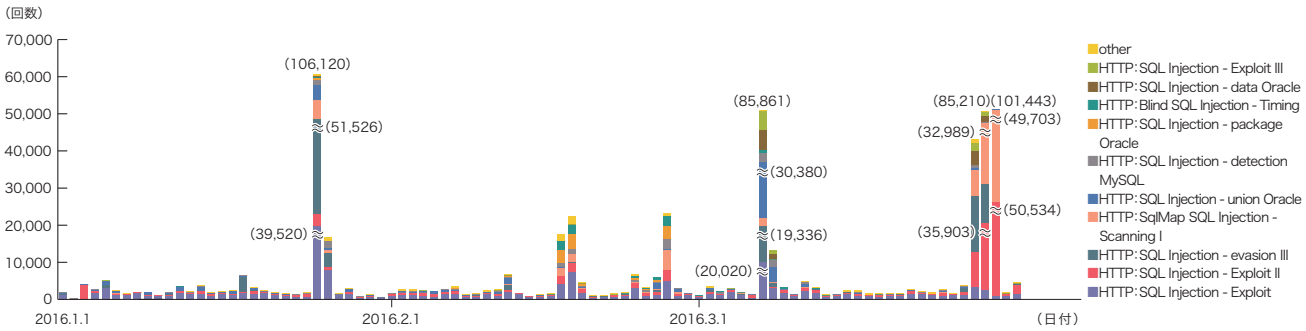


図-12 SQLインジェクション攻撃の推移(日別、攻撃種類別)

*39 Webサーバに対するアクセスを通じて、SQLコマンドを発行し、その背後にいるデータベースを操作する攻撃。データベースの内容を権限なく閲覧、改ざんすることにより、機密情報の入手やWebコンテンツの書き換えを行う。

1.3.4 Webサイト改ざん

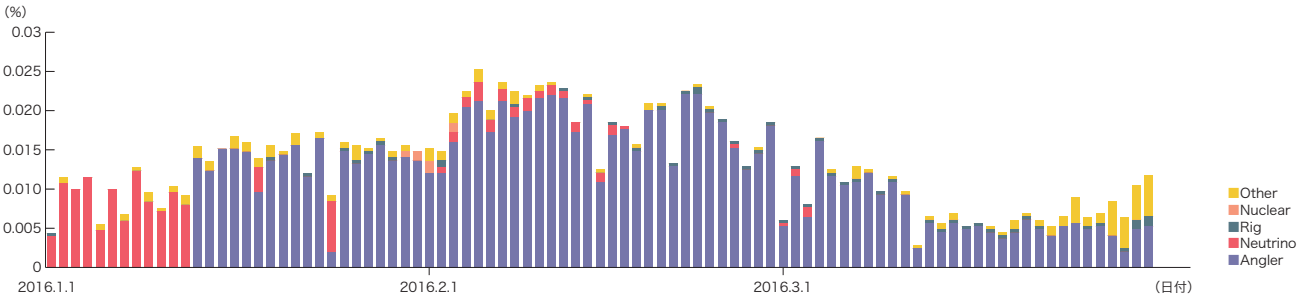
MITFのWebクローラ（クライアントハニーポット）によって調査したWebサイト改ざん状況を示します[*40]。

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。

2016年1月から3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-13）。この傾向は2015年7月から継続しています[*41]。ただし、元旦から12日間はAnglerによる攻撃が一切検知されず、代わりにNeutrinoが検知されていました。2015年7月以降、AnglerとNeutrinoの傾向が一時的に入れ替わる状況は複数回観測されていますが、このように長期間Anglerがまったく検知されなかったことはありませんでした。1月中旬以降は、ほぼ全期間にわたってAnglerによる攻撃が大部分を占めていました。他に、NuclearやRigによる攻撃を観測しました。Nuclearは小規模かつ一時的なものでしたが、Rigは小規模ではあるものの、期間を通して継続しました。これらのExploitKitに加え、PC故障を仄めかす偽のダイアログなどを表示して、スカムウェアやアドウェアなどのインストールや偽のサポートセンターへの電話を促す詐欺サイトへの誘導を観測しました。いずれも以前から続いている傾向です。

ダウンロードされるマルウェアは当初CryptoWall4.0が大部分を占めていましたが、2月中旬頃からTeslaCrypt3.0が取って代わりました。その他にNecurs、Bedep、Locky、Andromedaなどを検知しましたが、いずれも少数でした。特にLockyは同時期にメール経由での感染で大規模に拡散しているランサムウェアでしたが[*42][*43]、ドライブバイダウンロードのペイロードとして検知したものは極めて少数で、期間も短いものでした。

ドライブバイダウンロードによる攻撃は増加傾向が続いています。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。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[*44]。



※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-13 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）

＊40 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。
＊41 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。
＊42 メール経由でのLockyの猛威についてはSymantec社のブログ記事「ランサムウェア Locky、被害者を狙う攻撃が激化」（http://www.symantec.com/connect/ja/blogs/locky）などで報告されている。
＊43 主にドライブバイダウンロードで感染するランサムウェアについて、本レポートの「1.4.1 各種のランサムウェアとその対策」で紹介している。
＊44 ブラウザ利用環境におけるマルウェア感染対策については、本レポート「1.4.2 マルウェアに感染しないためのWindowsクライアント要塞化（前編）」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、各種のランサムウェアとその対策、マルウェアに感染しないためのWindowsクライアント要塞化(前編)、耐量子暗号の動向の3つのテーマについて紹介します。

1.4.1 各種のランサムウェアとその対策

ランサムウェアとは、実行したコンピュータ上のファイルを暗号化するなどしてコンテンツを利用不可能な状態にした上で画面上に脅迫文を表示し、復元(復号)と引き換えに金銭やBitcoin、あるいは、AmazonやiTunes Storeのポイントなどを支払うように要求するマルウェアの総称です。脅迫文は利用者の環境に応じた言語に合わせて表示される場合もあります。例えば、Lockyでは図-14のように日本語化されています。このような種類のマルウェアは1989年頃から知られており[*45]、2005年に大きく取り上げられたPGPCoder[*46]を皮切りに、繰り返し話題になってきました。本稿では、2015年10月から2016年3月までの期間にMITFのWebクローラシステムで収集したランサムウェアを対象に、機能の概要と対処・対策における検討事項を紹介します。

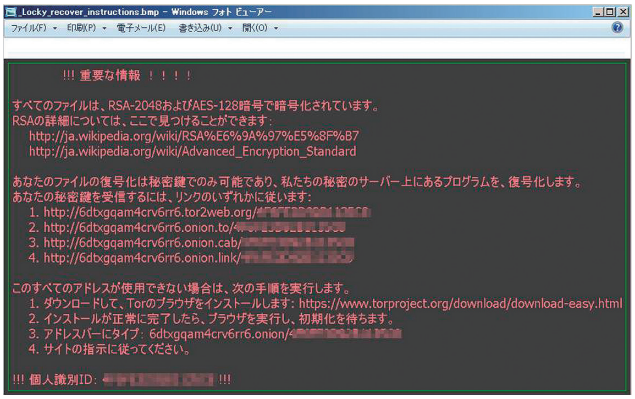


図-14 Lockyの脅迫文

■ ランサムウェアの動向

2015年10月から2016年3月までにIIJのWebクローラで検知したランサムウェアの種類と件数を図-15に、ランサムウェアの一覧を表-1に示します。期間当初はほぼすべてがCryptoWall3.0でしたが、2015年10月下旬から11月上旬までの期間でCryptoWall4.0へとバージョンアップしました。また、この時期には少数のTeslaCrypt2.0/2.2も検知されています。特にTeslaCrypt2.2は、メール経由での感染活動も継続しており、日本国内では一時期「vvvウイルス」という名称で話題になりました[*47]。なお、メールの添付ファイルとしては、EXE、JS、DOC(Macro)、SCR及びそれらをZIP圧縮したものなどが用いられていました。これは後述のLockyのケースでも同様です。その後はCryptoWall4.0の寡占状態が続いていましたが、2016年2月上旬を境に極めて短期間のうちに、TeslaCrypt3.0に置き換えられました。以前のバージョンのTeslaCryptにはファイルの暗号化に用いた共通鍵を攻撃者のサーバに伝達するための仕組みに問題があり、公開ツールを用いて復号可能であることが知られていました[*48]が、3.0以降ではこの問題が修正されました。また、2016年2月上旬に検知したLockyは、当時メール経由で大規模に拡散していた[*49]ものですが、Web経由では小規模の検知にとどまりました。TeslaCrypt4.0は2016年3月中旬頃にリリースされ、3.0のバグ修正や暗号化ファイルへの拡張子付与を廃止するなど多少の変更が行われたものです[*50]。なお、TeslaCryptは2016年5月に開発中止が宣言され、その際にマスターキーが公開された

*45 1989年に作られたAIDSというトロイの木馬はHDD上のファイル名を暗号化して金銭の支払いを要求した。例えばSecurityFocus社(現Symantec社)のコラム、"The Original Anti-Piracy Hack"(http://www.securityfocus.com/columnists/102)などで言及されている。

*46 2005年に流行したgpcodeというランサムウェアについて、例えばKaspersky Lab社のレポート"Malware Evolution: April June 2005"(https://securelist.com/analysis/malware-evolution-monthly/36052/malware-evolution-april-june-2005/)などで言及されている。

*47 暗号化されたファイルに設定される拡張子からこの通称が用いられた。トレンドマイクロ社のブログ記事「『vvvウイルス』の正体とは？ ランサムウェア『CrypTesla』の流入は限定的」(http://blog.trendmicro.co.jp/archives/12632)などが詳しい。

*48 IIJでは、"TeslaCrack"(https://github.com/Googulator/TeslaCrack)によってTeslaCrypt2.0/2.2で暗号化されたファイルの復号が可能であることを確認した。

*49 メール経由でのLockyの猛威についてはSymantec社のブログ記事「ランサムウェア Locky、被害者を狙う攻撃が激化」(http://www.symantec.com/connect/ja/blogs/locky)などで報告されている。

*50 Bleeping Computer社のブログ記事、"TeslaCrypt 4.0 Released with Bug Fixes and Stops Adding Extensions"(http://www.bleepingcomputer.com/news/security/teslacrypt-4-0-released-with-bug-fixes-and-stops-adding-extensions/)などで詳しく紹介されている。

ため、ESET社などによってバージョン3.0以降に対応した復号ツールが作成、公開されています[*51]。

■ 動作の流れ

CryptoWall、TeslaCrypt、Lockyなどのランサムウェアが被害者のコンピュータ上で実行されると、次のような過程でファイルの暗号化と被害者への脅迫が行われます。

1. グローバルIPアドレスの確認
   一般的なIPアドレス確認サービスに接続してコンピュータのインターネット接続性とグローバルIPアドレスを確認します。これは次に行われる公開鍵のダウンロード処理が行えるかを確認する事前準備と考えられます。CryptoWall3.0は、この処理が実行できない場合、以降の処理が実行されません。また、接続に際してコンピュータのProxy設定を利用するものとそうでないものがあります。なお、CryptoWall4.0やTeslaCrypt3.0/4.0は、このようなグローバルIPアドレスの確認を行いません。
2. サーバとの鍵交換
   金銭などを支払った被害者に復号手段を提供するため、攻撃者は何らかの方法で復号手段を手元(支払い手順を実行するサーバ上など)に保持しておく必要があります。LockyやCryptoWallは後述する暗号化の際に必要となる公開鍵をサーバからダウンロードする仕組みであるため、サーバとの接続を妨げることができれば、以降の処理は実行されません。一方、TeslaCryptはあらかじめ実行ファイルにECDH鍵パラメータが埋め込まれているため、サーバとの接続の有無によらず、暗号化が実行されます。
3. VSS管理ファイルの削除
   被害者がWindows Vista以降に標準搭載されているバックアップ機能のVolume Shadow Copy Service

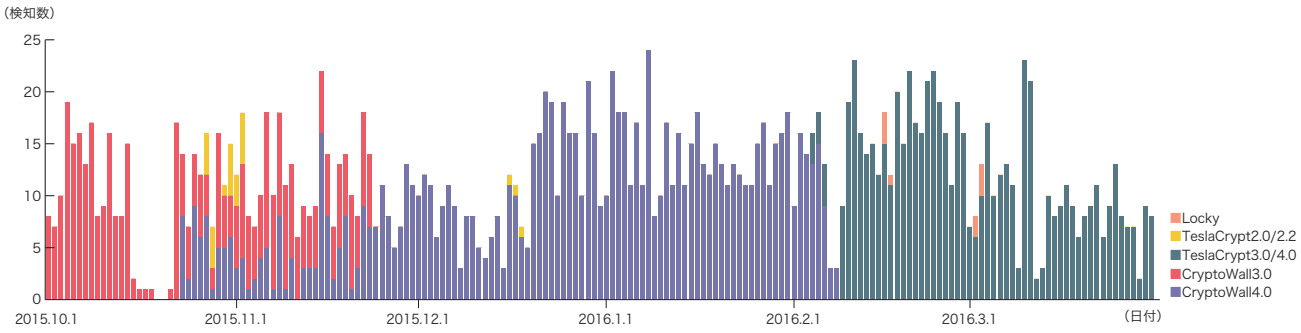


図-15 IIJ MITF Webクローラが検知したランサムウェアの種類と件数(2015年10月1日～2016年3月31日)

表-1 IIJ MITF Webクローラが検知したランサムウェア一覧

	CryptoWall3.0	CryptoWall4.0	TeslaCrypt2.0	TeslaCrypt2.2	TeslaCrypt3.0	TeslaCrypt4.0	Locky
出現時期	2015年1月	2015年11月	2015年7月	2015年12月	2016年2月	2016年3月	2016年2月
IPアドレス確認	ip-addr.esに接続	なし	ipinfo.ioに接続	myexternalip.comに接続	なし	なし	なし
Proxy対応	非対応	対応	非対応	対応	対応	対応	非対応
オフラインでの暗号化	不可	不可	可能	可能	可能	可能	不可
VSS削除	実施	実施	実施	実施	実施	実施	実施
備考	・IPアドレス確認や、サーバとの鍵交換が行えない場合、暗号化されない		・CryptoWallの脅迫文を盗用 ・公開ツールで復元可能	・日本国内ではVVVウイルスとも呼ばれた ・公開ツールで復元可能		・3.0のバグ修正 暗号化ファイルの拡張子廃止	・接続中ではないネットワーク共有に対しても再接続、暗号化を試みる

*51 ESET社のブログ記事、"ESET releases new decryptor for TeslaCrypt ransomware"(http://www.welivesecurity.com/2016/05/18/eset-releases-decryptor-recent-variants-teslacrypt-ransomware/)などで紹介されている。

(VSS)を用いてファイルを復元することを妨げるために、VSS管理ファイルを削除します。UACの設定にもよりますが、初期設定であれば確認ダイアログが表示されます。また、ランサムウェアが管理者権限のないアカウントで実行された場合は、この処理は行われません。

4. 対象ファイルの暗号化
   拡張子などによって暗号化対象のファイルを選択し、ランダムに生成した鍵を使ってAESで暗号化し、その共通鍵を暗号化したファイルのヘッダ部分に埋め込みます。このとき、TeslaCryptではECDH、CryptoWallやLockyではRSAを用いて共通鍵を第三者に解読できない形にします。
5. 脅迫文の表示
   Textや、PNG、HTMLなど複数のフォーマットのファイルを表示して、コンテンツが暗号化された旨と、支払い用のWebサーバへの接続手順を表示します(図-16、図-17)。TeslaCryptでは、Webサーバへアクセスすると、お試しで任意のファイルの復号を持ちかけて被害者に暗号化されたファイルをアップロードを促し、暗号化に使った共通鍵の回収を試みます。

■ 対処

ランサムウェアが実行され、コンテンツファイルが利用不能な状態になってしまった場合、自力による復号は非常に困難です。ただし、前述のTeslaCryptのようにマルウェア作成者の不手際や、あるいは鍵情報、ランサムウェアのDecryptorの流出などのために、実効性のある復号ツールが存在する場合がまれにあります。ツールの出自や内容に注意を払う必要はありますが、それらを試行することは選択肢として検討する価値があります。

しかし、残念ながら多くの場合、自力での復号は不可能なので攻撃者の要求を受け入れるか否かの選択しかありません。被害者の業務内容やコンテンツファイルの保存ポリシーにもよりますが、ストレージ故障と同様に機器交換やクリーンインストールで対処することをまず検討すべきです。組織的な観点に立てば、個々のPCのファイルシステムの重要性はそれ程高くない場合が多いのではないでしょうか。一方で、利用不能になったファイルが直ちに人命に関わるようなものであった場合には、攻撃者と取引した事例も存在します[*52]。ファイルの重要度や対価の捉え方、依存する事業の性質にもよるので模範解答は存在しませんが、万が一脅迫に屈するという選択をとる場合には、最低限、次の2点に留意する必要があります。

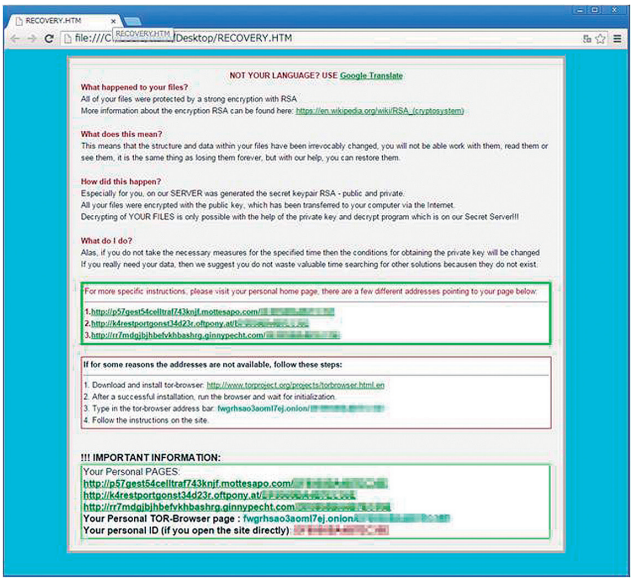


図-16 TeslaCrypt3.0の脅迫文

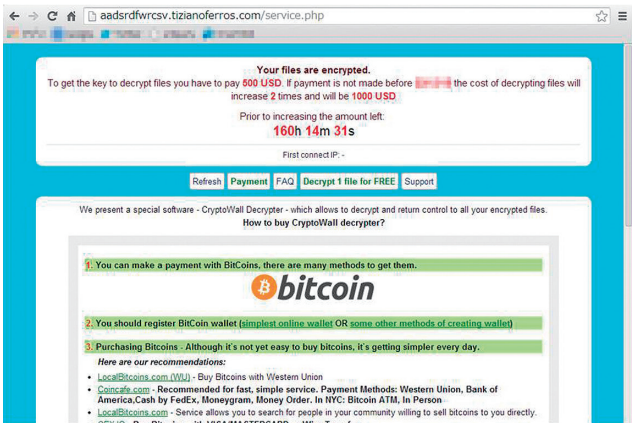


図-17 TeslaCrypt2.2の支払い用Webサーバ接続画面

*52 Hollywood Presbyterian Medical Centerのプレスリリース(http://hollywoodpresbyterian.com/default/assets/File/20160217%20Memo%20from%20the%20CEO%20v2.pdf)では、迅速な業務復旧のために支払いを実施した旨が発表されている。

・支払いをしてもすべてのファイルが復号されるという保証はない*53
・反社会勢力と取引することになる（事実が公開される可能性がある場合には、相応の説明が必要になる）

なお、攻撃者のサーバに接続した際に、1ファイルだけ、あるいは数ファイルに限って無料で復号すると表示される場合があります。ここでファイルを送信して復号を試す場合は、復号したファイルの内容が攻撃者に漏えいするリスクを受容することになります。

■ 対策

感染を前提とした対策として、ファイルシステムのバックアップが非常に重要です。個々のコンピュータのファイルシステム全体あるいはコンテンツ保存領域、書き込み可能なネットワークドライブについて、定期的なバックアップを実施する運用を推奨します。バックアップファイルが暗号化されてしまう可能性もあるので、例えばファイルサーバの共有ディレクトリとして設定されていないディレクトリやドライブに保存するなど、バックアップファイルは感染が想定されるコンピュータからアクセスできない状態で保持する必要があります。クライアントPCやファイルサーバを仮想環境で運用している場合は、スナップショットによる差分バックアップ機能の活用が効果的です。

Windowsクライアントシステムにおけるマルウェア感染対策ついては、「1.4.2 マルウェアに感染しないためのWindowsクライアント要塞化（前編）」をご参照ください。

1.4.2 マルウェアに感染しないためのWindowsクライアント要塞化（前編）

本レポートの「1.4.1 各種のランサムウェアとその対策」や、過去のIIRでも触れているように、近年はExploit Kitなどによる Webサイト経由やメール経由でのマルウェア感染が数多く確認されています。そこで本稿及び次号のIIRでは、Windowsの要塞化設定の中から、前述の感染経路を経由してマルウェアを受け取った場合の感染の予防や被害を緩和するための設定について紹介します。

■ 要件

OSはWindows 7 SP1以上、各OSのEditionはProfessional（もしくはPro）以上を対象とします。Home Editionでもいくつかの対策については設定可能ですが、ソフトウェアの制限のポリシーやAppLockerのようなプログラムの実行可能範囲を制限するための機能が実装されていないため、ビジネス用途での利用には向かないと判断し、対象外にしています。

■ 前提条件

ここでの説明はドメインに属していないWindowsにてローカルグループポリシーエディターを使用して行っていますが、後述するEMETを含め、Windowsドメインのグループポリシー管理エディターを使用し、配下のクライアントに対して一斉適用することも可能です。また、画像のほとんどはWindows 10 Enterprise Edition 64bitを使用していますが、各Windowsのバージョンによって設定できる項目に若干の差異がある場合があります。WindowsはC:\にインストールされていることを想定しています。

■ 基本

まずはソフトウェアをアップデートし、最新に保ちます。

・Windows Update（他のマイクロソフト製品を含む）
・Webブラウザ（FirefoxやGoogle Chromeなどのサードパーティ製品を含む）
・メーラー（Thunderbirdなどのサードパーティ製品を含む）
・Webブラウザプラグイン（Flash Player、Adobe Reader、Java）

この他に利用しているソフトウェアや、出荷時からインストールされているソフトウェアなどがあれば、それらも最新に保ちます。また、不要なソフトウェアは削除しておくとよいでしょう。

*53 Bleeping Computer社のブログ記事、"Paying the Coverton Ransomware May Not get your Data Back"（http://www.bleepingcomputer.com/news/security/paying-the-coverton-ransomware-may-not-get-your-data-back/）では支払いをしても復号に失敗する「Coverton」というランサムウェアが紹介されている。

ウイルス対策ソフトウェアを導入し最新版に保ち、最新パターンファイルに更新します。パーソナルファイアウォールの有効化も必要です。

■ 利用者に管理者権限を与えない

本稿で紹介する対策は管理者権限によって一般ユーザにポリシーを強制し、プログラムの新規インストールを禁止することを前提とした対策を行います。しかし、もし利用者も管理者権限を持っていると、ポリシーを自由に変更してしまうため、一般ユーザ権限のみを付与する必要があります。

■ アプリケーションホワイトリスティング

WindowsやマイクロソフトⅡ社製品標準のプログラムはC:\WindowsやC:\Program Filesフォルダ以下にインストールされています。また、管理者が用意するプログラムもこれらのフォルダにインストールされることがほとんどです。そこで、これらのフォルダ以外のプログラムの実行やロードを禁止することで、受信したメールにマルウェアが添付されていた場合や、ドライブバイダウンロードによって最終的にマルウェアがダウンロードされた場合に、それらが実行されたりロードされたりすることを防ぎます。この手法はアプリケーションホワイトリスティングと呼ばれ、海外では政府機関などが利用を推奨しています[*54]。ここではAppLockerとソフトウェアの制限のポリシー(SRP)の2つを用いて制限する方法を紹介します。

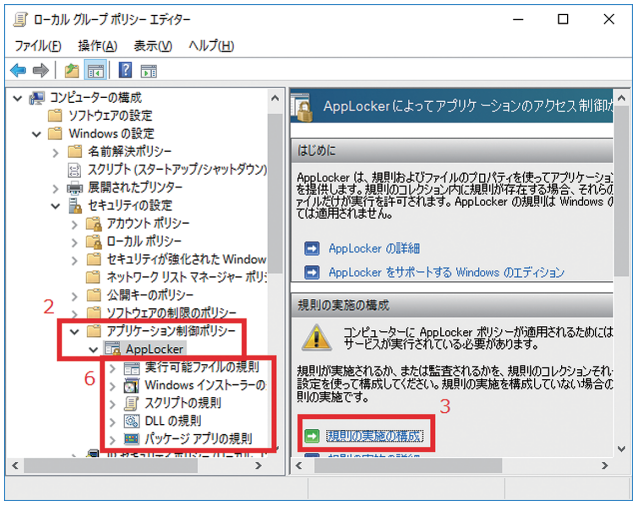


図-18 AppLockerの設定画面

■ AppLocker

マイクロソフトは、Windows 7からAppLockerと呼ばれる機能を追加しました。これは、後述するソフトウェアの制限のポリシー(SRP)をより柔軟かつ詳細に管理するための上位版に位置づけられる機能です。Windows 7以降のEnterprise EditionであればAppLockerが使用できます[*55]。

1. 管理者権限でローカルグループポリシーエディターを起動してください。これはgpedit.mscを実行することで起動することが可能です(図-18)。
2. メニュー左側のツリーからコンピューターの構成、Windowsの設定、セキュリティの設定、アプリケーション制御ポリシーの設定、AppLockerとたどります(図-18)。
3. AppLockerのメニューが右側に表示されるため、規則の実施の構成をクリックします(図-18)。
4. プロパティが開くので、詳細設定タブに切り替え、DLLの規則のコレクションを有効にするにチェックをつけ、適用をクリックします(図-19)。
5. プロパティ画面で実施タブに切り替え、すべての規則に対して構成済みにチェックをつけ、セレクトボックスが規則の実施になっていることを確認してOKをクリックして、プロパティウィンドウを閉じます(図-20)。

---

*54 例えば米NSAは米政府機関向けのホスト構築ガイドでApplication Whitelistingを最初に紹介している。"Host Mitigation Package" (https://www.iad.gov/iad/library/ia-guidance/security-tips/host-mitigation-package.cfm)。また、ソフトウェアの制限のポリシー(SRP)を使ってApplication Whitelistingを行う手順書も公開している。"Application Whitelisting using Software Restriction Policies"(https://www.iad.gov/iad/library/ia-guidance/security-configuration/operating-systems/application-whitelisting-using-srp.cfm)。Australian Signals Directorate(ASD、オーストラリアの情報機関)は彼らが対応した豪政府機関のインシデントの85%はTop4の対策で対応可能だったことを公表している。その1番目がApplication Whitelistingである。また、Implementation Guideの中にAppLockerが紹介されている。"Strategies to Mitigate Targeted Cyber Intrusions"(http://www.asd.gov.au/infosec/mitigationstrategies.htm)。

*55 Windowsドメインのポリシーのツリー構成やサービスの制御などの部分の操作が若干異なるため、適宜読み替えること。例えばWindowsドメインのグループポリシー管理エディター上では、AppLockerはコンピューターの構成、ポリシー、Windowsの設定、セキュリティの設定、アプリケーション制御ポリシー、AppLocker、とたどることができる。また、サービスは同じくグループポリシー管理エディターでコンピューターの構成、ポリシー、Windowsの設定、セキュリティの設定、システムサービス、とたどるとサービスの自動起動を強制するための設定画面を表示することができる。

6. AppLocker以下にある各規則[*56]を右クリックし、既定の規則の作成を選択します(図-18)。
7. 管理ツールなどからサービス管理画面を開き、Application Identityサービスを起動します。また、スタートアップの種類を自動に切り替えないと、次回リブート時にApplication Identityサービスが自動起動しないため、忘れずに実施してください[*57]。
8. ポリシーを強制したいホストを再起動するか、管理者権限でコマンドプロンプトを開き、gpupdate /forceコマンドを実行すると、AppLockerが有効になります。

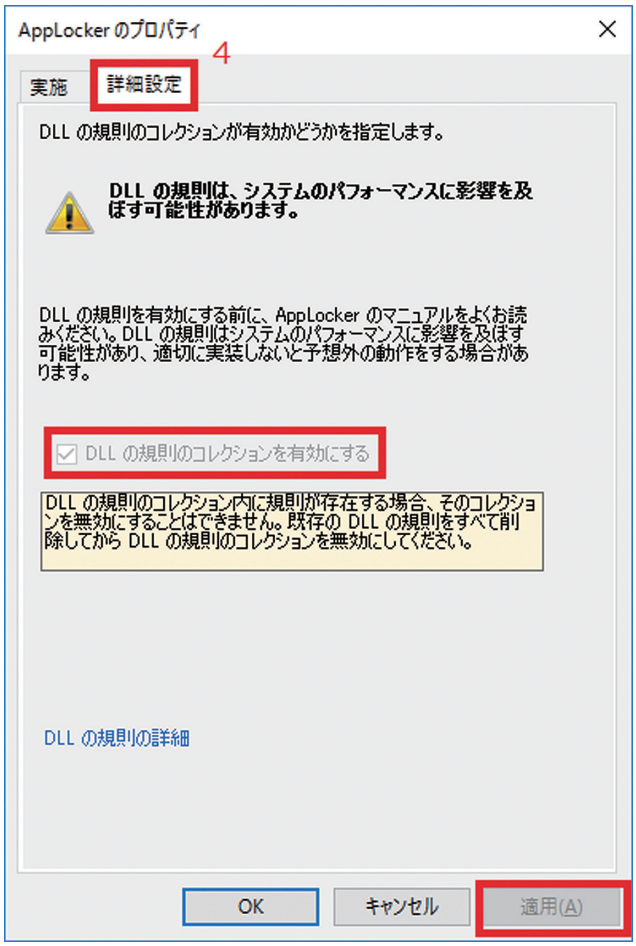


図-19 AppLockerのプロパティ(詳細設定)

許可されていないアプリケーションを起動しようとすると、図-21のようなポップアップが出現します。

また、許可、拒否のログは共にイベントログに出力されます。イベントビューアーより、アプリケーションとサービスログ、

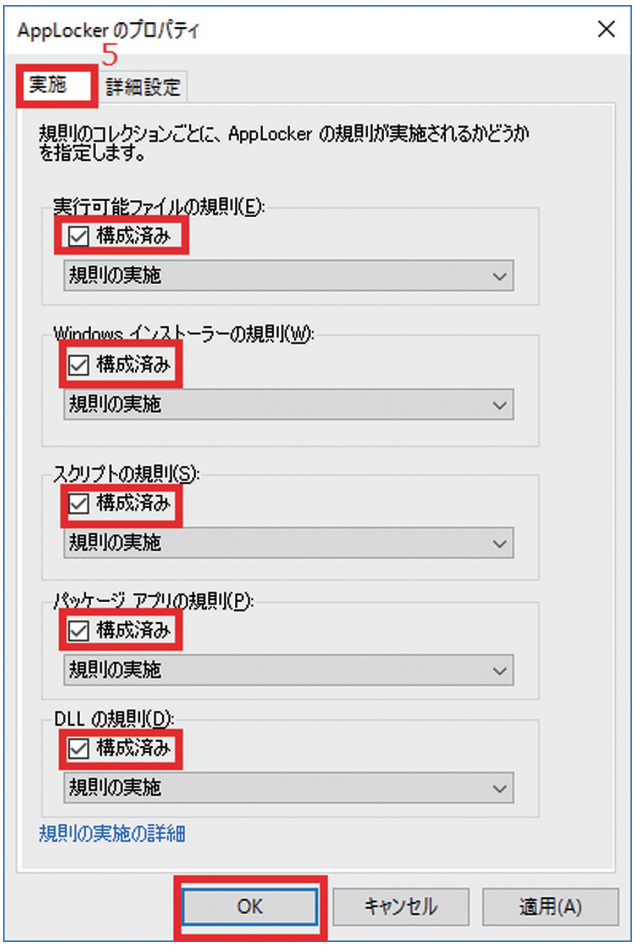


図-20 AppLockerのプロパティ(実施)

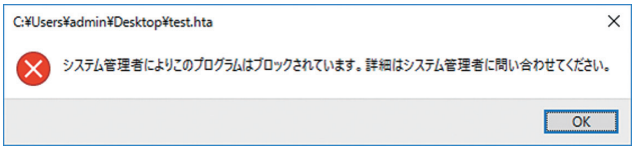


図-21 AppLocker - ブロックされたときに出現するポップアップ

*56 Windows7では、パッケージアプリの規則は存在しない。
*57 Windows10の環境では、なぜか管理者権限で操作してもアクセスが拒否されましたという旨のメッセージが出て自動にすることができなかった。このような症状の場合は、管理者権限でコマンドプロンプトを起動し、次のコマンドを実行することで、スタートアップの種類が自動になることを確認している。sc config appidsvc start=auto。

Microsoft、Windows、AppLocker、とたどるとカテゴリごとにログが出力されています（図-22）。

ソフトウェアの制限のポリシー（SRP）

AppLockerがEnterprise Editionのみに付属することからも、マイクロソフトはビジネス環境ではEnterprise Editionを利用すべきであると考えていることが窺えます。しかし、ビジネス用途でWindowsがプリインストールされたクライアントPCを購入した場合、Pro Editionが付属していることがほとんどです。そのため、実際のビジネス環境においてはAppLockerを利用できない場合も少なくありません。また、Windows7より前のOS（Vistaなど）にはどのEditionであってもAppLockerを利用できません。このような場合は、ソフトウェアの制限のポリシーを使用して制限をかけることになります。AppLockerと比較した場合、プログラムの種類別にルールを分けて作成することができない、ライブラリ（DLL）の拒否イベントがログに記録されない、ストアアプリの制御ができない、ルールの強制がカーネルモードではなく、ユーザモードで行われる、ポリシーのインポートができないなど不便な点や機能が欠けている点はありますが、多くの場合でAppLocker同様に有効です[*58]。ちなみにソフトウェアの制限のポリシーとAppLockerを両方設定できるOS上でどちらも設定した場合は、ソフトウェアの制限のポリシーの設定は無視されます。

1. 管理者権限でローカルグループポリシーエディターを起動してください。これはgpedit.mscを実行することで起動することが可能です（図-23）。
2. メニュー左側のツリーからコンピューターの構成、Windowsの設定、セキュリティの設定、ソフトウェアの制限のポリシー、とたどります（図-23）。
3. ソフトウェアの制限のポリシーを右クリックして、新しいソフトウェアの制限のポリシーを選択します（図-23）。
4. 強制をダブルクリックします（図-23）。
5. プロパティが開くので、ソフトウェアのファイルすべて

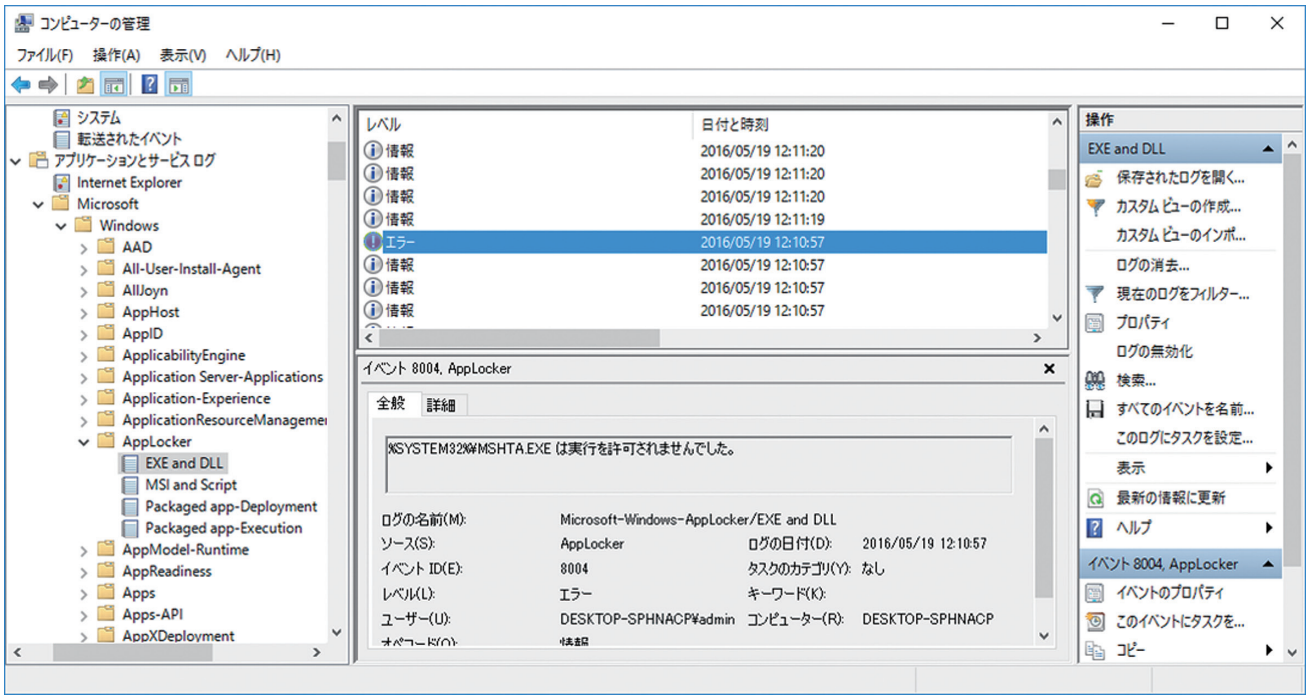


図-22 AppLocker - イベントログ

*58 AppLockerとソフトウェアの制限のポリシーの比較は次のURLが詳しい。"Use AppLocker and Software Restriction Policies in the Same Domain"（https://technet.microsoft.com/library/hh994614）。

を選択します。また、証明書の規則を適用するを選択し、OKを押してプロパティを閉じます(図-24)。

6. 指定されたファイルの種類をダブルクリックし、プロパティを開きます(図-23)。
7. プロパティでLNKを選択し、削除をクリックします(図-25)。プログラムが制限なしで実行される旨のポップアップが出てきますが、はいをクリックしてポップアップを閉じ、プロパティ画面でOKを押して、プロパティを閉じます。ここでLNKを削除しておかないと、デスクトップ上やスタートメニューなどに存在するすべてのショートカットファイルまでブロックされてしまい、使い物にならないため、ここでは対象から外します。悪意のあるショートカット(LNK)[*59]については、その中に存在するVBScriptやJScriptなどが危険であるため、別の対処を行います(この部分については次号のIIRで説明します)。
8. セキュリティレベルをダブルクリックし、許可しないをダブルクリックします。

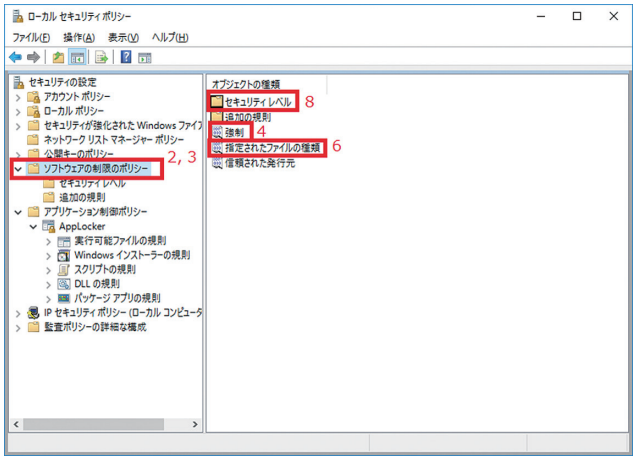


図-23 ソフトウェアの制限のポリシー(SRP)の設定画面

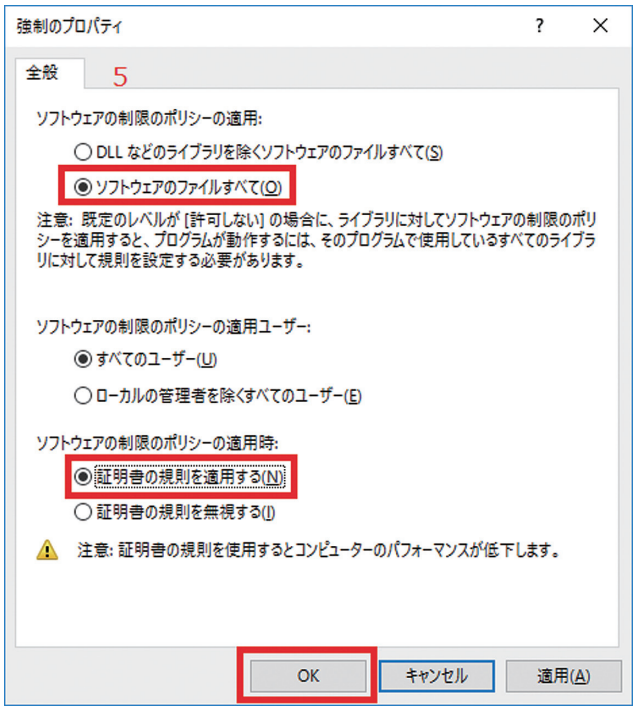


図-24 SRP - 強制のプロパティ

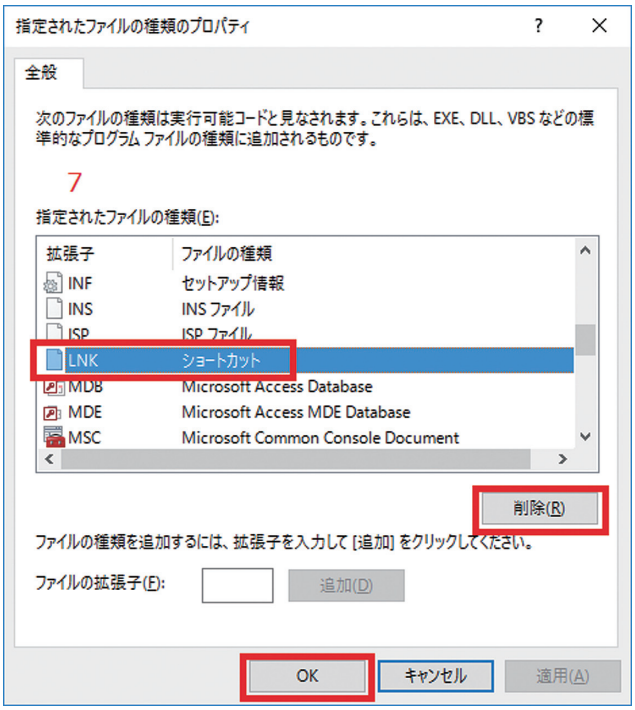


図-25 SRP - 指定されたファイルの種類のプロパティ

*59 LNK内にVBScriptを挿入し、実行させる手口は例えば次のようなものが報告されている。「ドキュメントにないLNKの機能に隠れるJanicab」(http://blog.f-secure.jp/archives/50747074.html)。また悪意のあるLNKの事例は国内でも確認されている。例えばJ-CSIPで扱った事例の中には履歴書と称するLNKを開かせようとする事例が紹介されている。「サイバー情報共有イニシアティブ(J-CSIP) 2014年度 活動レポート 別冊 添付資料『X』による攻撃メール一覧」(https://www.ipa.go.jp/files/000046020.pdf)。

9. プロパティが開くので、既定値として設定をクリックします(図-26)。一部のプログラムが動作しなくなるという旨のポップアップが表示されるため、はいをクリックしてポップアップを閉じます。プロパティに戻るので、OKを押してプロパティを閉じます。
10. ポリシーを強制したいホストを再起動するか、管理者権限でコマンドプロンプトを開き、gpupdate /forceコマンドを実行すると、ソフトウェアの制限のポリシーが有効になります。

実行がブロックされると、AppLockerと同様に次のようなポップアップが表示されます(図-27)。

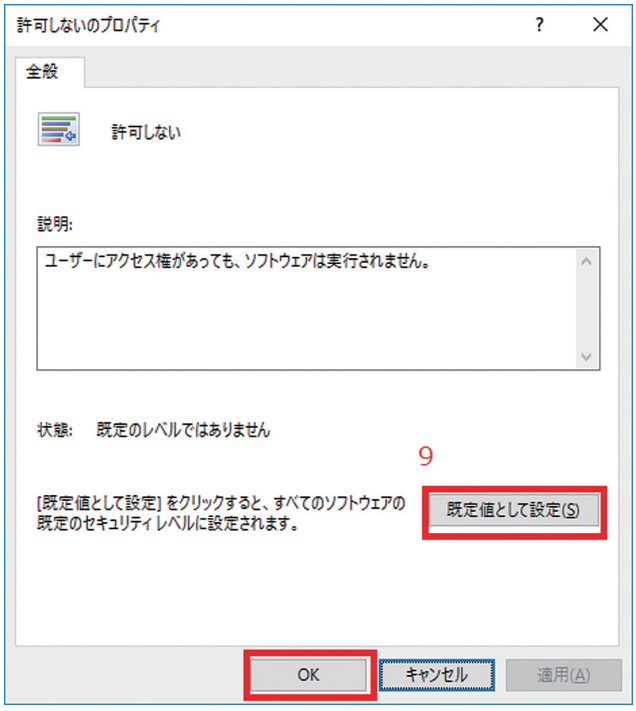


図-26 SRP - 許可しないのプロパティ

またブロックされた場合のみ、イベントログのアプリケーションに記録されます(図-28)。

■ 制限回避の脆弱性

マルウェアは一般ユーザ権限で動作した場合、ユーザディレクトリ以下にマルウェアのインストールを試みることが多いため、これらの機能を有効にすれば、多くのマルウェア感染を防ぐことができるでしょう。ただし、初期設定のままではいくつかの脆弱な点が存在します。例えば、C:\Windows\Tempフォルダは、任意のユーザで書き込みと実行が可能であるため、攻撃者がここにマルウェアを生成して実行した場合、初期設定の制限がかかっていても、突破できてしまいます。このようなことがないように、SysinternalsのAccessEnumやAccessChk[*60]のようなツールを使い、実行を許可しているフォルダ以下に一般ユーザが書きこめる場所がないかを調査し、そのフォルダ以下の実行を拒否するルールを追加していく必要があります。また、これ以外にも複数の脆弱性が研究者によって報告されています[*61]。厳密に制限をかけていきたい場合は、これらについても精査し、ルールとして追加をしていく必要があります。

■ WinSxSフォルダについて

WinSxSフォルダはWindows Updateのバックアップや Windowsの様々な機能(PowerShell、.Net Framework、Hyper-Vなど)が格納されています。機能を有効にするとこのフォルダ内にあるファイルのハードリンクがSystem32フォルダなどに作られるため、ユーザはパスを気にせずに利用できるようにな

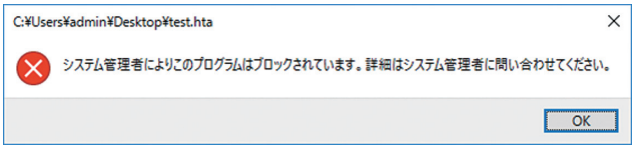


図-27 SRP - ブロックされたときに出現するポップアップ

*60 AccessEnum(https://technet.microsoft.com/ja-jp/sysinternals/accessenum.aspx)。AccessChk(https://technet.microsoft.com/ja-jp/sysinternals/accesschk.aspx)。

*61 例えば、次のURLではいくつかのAppLockerの制限を回避する手法とその対策について紹介している。"Protecting Windows Networks – AppLocker"(https://dfir-blog.com/2016/01/03/protecting-windows-networks-applocker/)。"Application Whitelist Bypass Techniques"(https://github.com/subTee/ApplicationWhitelistBypassTechniques)。また次のURLでは、regsvr32.exeを用いてリモートからスクリプトをダウンロードして実行する手法について紹介している。"Bypass Application Whitelisting Script Protections - Regsvr32.exe & COM Scriptlets (.sct files)"(http://subt0x10.blogspot.jp/2016/04/bypass-application-whitelisting-script.html)。

ります。ただし有効にする前の状態でも、WinSxSから直接プログラムを実行することは可能です。例えばPowerShellやrundll32.exeなどはこのフォルダ内に存在するため、これらの悪用を防ぐには拒否しておかなければなりません。WinSxSフォルダ以下全体の実行やロードを制限すれば済むのではないか、と考える方もいるかもしれません。しかし、一部のコンポーネントはWinSxS以下に存在するライブラリを直接ロードしていることが、調査した結果分かっています。

AppLockerであれば、実行ファイル(exe)とライブラリ(DLL)のルールを別々に管理できるため、実行ファイルは全体で拒否し、ライブラリについては拒否しない、もしくは一旦すべて拒否しておき、不具合が出たライブラリのみ、ログを確認しながら追加していくという運用が可能です。しかし、ソフトウェアの制限のポリシーはプログラムの種類別に設定することができないため、WinSxS全体を拒否した上で、不具合が出たプログラムのみを部分的に許可するという運用方法しかとれません。しかし切り分けを行う際、ソフトウェアの制限のポリシーによってロードが拒否されたライブラリ(DLL)がログに出力されないため、何を許可して良いのか簡単には分からないという問題も存在します。そこで検証時にWinSxSを許可した状態でSysinternalsのSysmon、Process Monitor、Process Explorer[*62]などを利用してライブラリのロードイベントを記録し、それを許可ルールとして追加するという運用を行うことで、この問題を回避できます。

■ 管理者権限の制限について

AppLockerは既定のルールにAdministratorsグループに属するユーザを許可しています。これらのルールを削除すれば一般ユーザ同様に制限することが可能です。ソフトウェアの制限のポリシーは初期設定ですべてのユーザが対象になっています(図-24)。

《次号に続く》

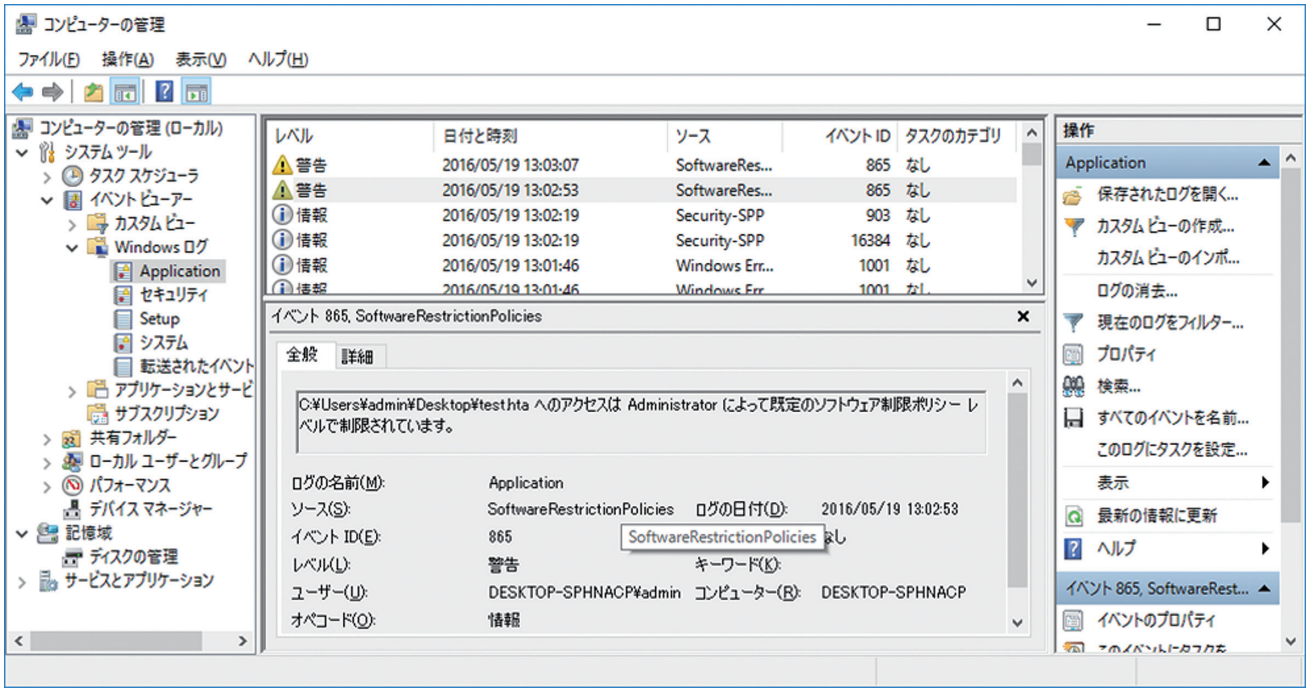


図-28 SRP - イベントログ

*62 Sysmon(https://technet.microsoft.com/ja-jp/sysinternals/sysmon)。Process Monitor(https://technet.microsoft.com/ja-jp/sysinternals/bb896645)。Process Explorer(https://technet.microsoft.com/en-us/sysinternals/bb896653.aspx)。

1.4.3 耐量子暗号の動向

2016年2月、福岡市にて耐量子暗号について扱う国際会議PQCrypto2016（Post-Quantum Cryptography 2016）[*63]が開催されました。本会議の初日には、米国における情報セキュリティ関連の標準文書を策定しているNIST（National Institute of Standards and Technology）から耐量子暗号のコンペティションを開催する旨のアナウンスがなされました[*64]。そのためNISTの今後の動向に注目する研究者や、今後の製品ラインナップの方向性を定めたいベンダーなど幅広い関係者が参加し、同規模の国際会議としては異例の多さで、国内外からの参加者は200名を超えました。今回のNISTによるアナウンスのほか、欧州にて多額の研究資金が投入されるプロジェクトが昨年立ち上がっているなど、この分野の研究が活発化しています。本節では耐量子暗号に関わる技術背景、今後の動向について報告します。

■ 量子計算機の登場による暗号技術への影響

耐量子暗号（Post-Quantum Cryptography）[*65]は2003年にDaniel J. Bernstein教授によって提唱された概念で、量子計算機の登場に伴い、現在利用されている暗号技術の置き換えを目指す暗号アルゴリズムの総称を指します。Post-Quantum Cryptographyの他にもQuantum Safe Cryptography、Quantum resistant Cryptographyなどの用語が使用されていますが、いずれも同じ概念を指します。

現在公開鍵暗号方式として広く利用されているRSAや（EC）DHは、それぞれ素因数分解の困難性、離散対数問題の困難性が前提となって安全性を担保する暗号アルゴリズムです。現在の計算機アーキテクチャの基ではこれら2つは非常に難しい問題であることが知られています。これに対して1994年に提案されたShorアルゴリズム[*66]は量子計算機を用いることにより、これら2つの問題が多項式時間で解けることが示されました[*67]。そのため現在主流の公開鍵暗号アルゴリズムは量子計算機の登場により脅威に晒されることになります。

では、現在の暗号アルゴリズムはどのくらい使い物にならなくなるのでしょうか？これをビット安全性[*68]という指標を用いて説明することができます。暗号アルゴリズムの強度、もしくは危殆化の進行状況を示す概念として「nビット安全性」という表現が用いられます。パラメータnは当該アルゴリズムの攻撃に必要な計算量が2^n（2のn乗）であることを示しており、共通鍵暗号においては、全数探索に必要な鍵空間の大きさ2^n（nは共通鍵ビット長）に該当します。ハッシュ関数においては出力ビット長がnビットのとき、原像計算困難性に対しては2^n、衝突困難性としては$2^{n/2}$が攻撃に必要な計算量の理論値となります。

一般的に、暗号アルゴリズムは徐々に新しいものに移行していく必要があります。NISTによるアルゴリズム移行計画を示すSP 800-131Aは2015年11月に改訂されて、112ビット未満の安全性しか持たないアルゴリズムは利用禁止（Disallowed）となりました[*69]。共通鍵暗号としては2-key Triple-DES（112ビット鍵を利用しますが総当り方式よりも効率のよい攻撃手法が存在）が除外されています。HMACなどのMAC（メッセージ認証コード）に用いられる鍵長も112ビット以上のみを利用

---

*63 The Seventh International Conference on Post-Quantum Cryptography（https://pqcrypto2016.jp/）。Winter Schoolと称された2日間のレクチャー（https://www.youtube.com/playlist?list=PLCAbx7kHwCGKLMt1-geJmx9QmOCvXLRdz）と本会議の模様（https://www.youtube.com/playlist?list=PLCAbx7kHwCGLPpgETzBqQg11comaFCF_H）が公開されている。

*64 PQCrypto2016本会議で以下のプレゼンテーションが行われた。Dustin Moody、"Post-Quantum Cryptography: NIST's Plan for the Future"（https://pqcrypto2016.jp/data/pqc2016_nist_announcement.pdf）。

*65 Daniel J. Bernstein、"A brief survey of post-quantum cryptography"、PQCrypto2008 invited lecture、2008（http://cr.yp.to/talks/2008.10.18/slides.pdf）。

*66 Peter W. Shor、"Algorithms for quantum computation：discrete logarithms and factoring"、35th Annual Symposium on Foundations of Computer Science（SFCS）、1994（https://www.computer.org/csdl/proceedings/focs/1994/6580/00/0365700.pdf）。現在の素因数分解の解読記録は2014年11月に公開された56153である（http://arxiv.org/abs/1411.6758）。

*67 Jason LeGrow、"Post-Quantum Security of Authenticated Key Establishment Protocols"、A thesis presented to the University of Waterloo、2016（https://uwspace.uwaterloo.ca/bitstream/handle/10012/10386/LeGrow_Jason.pdf）。

*68 暗号危殆化の事例や、ビット安全性、等価安全性に関する解説は本レポートの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。

*69 National Institute of Standards and Technology（NIST）、"Transitions：Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths"、NIST Special Publication 800-131A、2015（http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf）。

し、署名作成時のハッシュ関数としては既に危殆化したSHA-1ではなくSHA-2、SHA-3の利用のみとなります[*70]。

公開鍵暗号方式に対しても攻撃計算量を予測することで、それぞれのアルゴリズムに対してnビット安全性を持つ鍵長が定められています。その1つにNISTによるSP 800-57があり2016年1月に改訂されています[*71]。112ビット安全性は2030年まで有効で、それ以降は128ビット安全性を持つアルゴリズムにシフトすることが想定されています。112ビット安全性に等価な公開鍵としてはRSA-2048、DSA-2048、ECDSA-224、ECDH-224がありますので、これらよりも短い鍵長の利用はすでに禁止されており、2031年以降はRSA-3072、ECDH-256などへの移行が望まれることになります。

しかし量子計算機が登場すると、これらの想定が崩れてしまいます。それを示す指標の1つに1996年に発表されたGroverアルゴリズム[*72]があります。Groverによると現在のアーキテクチャの計算機でnビット安全性を有していた暗号アルゴリズムは、量子計算機の解読能力によるとn/2ビット安全性しか確保できないことが分かりました。例えば、現在利用されている共通鍵暗号の1つであるAES-128は64ビット安全性しか確保できないことを意味します。そのため128ビット安全性を確保するためには256ビット鍵を利用するAES-256にシフトする必要が出てきます。同様にハッシュ関数においてはSHA-256を署名に利用するケースを考えると、衝突困難性を確保するためには64ビット安全性しか有さないため、SHA-512やSHA3-512など、出力長として512ビット以上のアルゴリズムを使用しないと128ビット安全性を確保できないことになります。

公開鍵暗号方式においても同様のことを示すことができ、現在256ビット安全性を有すると信じられている鍵長を利用しないと128ビット安全性を確保できません。先程紹介したSP 800-57によるとRSA-15360、ECDH-512などがそれに該当します。更にETSI(European Telecommunications Standards Institute)による2015年6月発行のレポートにおいてはより強いことが示されていて[*73]、上記のように現時点で256ビット安全性を持つと信じられている鍵長を利用したとしても0ビット安全性であるとの記載があります。

■ 新しい安全性根拠を持つ暗号アルゴリズムの探索

上記の背景のもと、これまでとは異なる安全性根拠を持つ公開鍵暗号アルゴリズムが望まれるようになりました。アカデミアの動きとしては国際会議PQCryptoが2006[*74]年から約1年半ごとに開催されており、前述した会議が第7回目となりました。2013年からETSIはIQC(Institute for Quantum Computing)と共同でIQC/ETSI Quantum-Safe Crypto Workshop[*75]を開催しており、2015年10月の会議では耐量子暗号に関する標準化が必要というコンセンサスを得ました[*76]。本ワークショップは2016年9月には第4回が予定されるなど継続的に情報共有が行われる見込みです。

同様に欧州の動きとしてはH2020 PQCRYPTO projectがあります。H2020(Horizon 2020)[*77]はEUのファンドによる先駆的かつ欧州横断的な研究支援活動で、ECRYPT(European Network of Excellence in Cryptology)及びECRYPT2の活動を支援したFP7の後継と言われています。H2020 PQCRYPTO project[*78]は2015年3月から3年間限定で活動を開始したプロ

*70 ただし、署名検証における112ビット安全性未満の署名アルゴリズムやSHA-1はLegacy-useとして許容されている。また、署名生成・検証に関わらないSHA-1利用は、この制限を受けず利用可能(Acceptable)である。また、SHA-1は112ビット以上の原像計算困難性を持っているためHMAC-SHA-1は脆弱ではない点に注意する。なお SHA-2、SHA-3はダイジェスト出力長として 224,256,384,512 ビットのバリエーションを持つ。
*71 National Institute of Standards and Technology(NIST)、"Recommendation for Key Management、Part 1:General"、NIST Special Publication 800-57 Part 1 Revision 4、2016(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf)。
*72 Lov K. Grover、"A fast quantum mechanical algorithm for database search"、28th Annual ACM Symposium on the Theory of Computing (STOC)、1996(http://arxiv.org/abs/quant-ph/9605043)。
*73 European Telecommunications Standards Institute(ETSI)、"Quantum Safe Cryptography and Security"、ETSI White Paper No. 8, 2015(http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf)。
*74 PQCrypto2006:International Workshop on Post-Quantum Cryptography(http://postquantum.cr.yp.to/)。
*75 European Telecommunications Standards Institute(ETSI)、3rd ETSI/IQC Workshop on Quantum-Safe Cryptography(http://www.etsi.org/news-events/events/949-etsi-iqc-3)。
*76 European Telecommunications Standards Institute(ETSI)、"ETSI workshop confirms need to accelerate on Quantum-Safe Cryptography standards" (http://www.etsi.org/index.php/news-events/news/1013-2015-10-news-etsi-workshop-confirms-need-to-accelerate-on-quantum-safe-cryptography-standards)。
*77 European Commission、Horizon 2020(http://ec.europa.eu/programmes/horizon2020/)。
*78 PQCRYPTO(Post-Quantum Cryptography for Long-Term Security)project(https://pqcrypto.eu.org/)。

ジェクトで、耐量子暗号に関連する研究活動が行われています。活動を開始した半年後の2015年9月には、暫定版ではありますが耐量子暗号アルゴリズムの推奨リスト（ポートフォリオ）の案が既にまとめられています[*79]。

一方で米国ではNISTによる2016年2月のアナウンスに先立ち、2015年4月にPKC2015と併設してNIST主催のワークショップが開催されています[*80]。2015年8月には米国政府調達に利用されるSuite B 暗号リスト[*81]の参照を、特に新たに導入する機器・システムにおいては一旦取りやめるよう要請がありました。また、PQCrypto2016開催の前に3月締切のパブリックコメント[*82]を行い、4月にはNISTIR 8105として第1版のレポートが発行されました[*83]。2月のアナウンスにおいては2023年から2025年を目処に文書化することを想定し、以下のタイムラインに沿って技術的検証を行うことが示されました。2016年秋を目処に正式なコンペティションの概要が公開され、2017年11月を応募締切とし2018年初頭に応募者によるプレゼンテーションを中心としたワークショップが開催されます。その後、3年から5年程度で技術的解析を行ったあと標準化が行われる見込みです。その際にはAESやSHA-3コンペティションのように1つのアルゴリズムに絞らないことや、NESSIE[*84]のようにポートフォリオ提示に留まらず、きちんと標準化を行うという方向性が提示されています。

表-2 耐量子暗号の分類

種類	概要	解読チャレンジ
格子暗号 (Lattice-based cryptography)	実数上のn次元空間においてn個の基底に対して整数係数で張るベクトル空間を格子（Lattice）と呼ぶ。ある基底を持つ格子に対して、同じ格子を他の異なる基底で表現できる。ある格子が与えられたとき、最短ベクトル探索問題（SVP：Short Vector Problem）はnが大きくなると難しいとされ、この難しさを用いて公開鍵暗号が構成されている。NTRUは実用化されたアルゴリズムの1つである。SVP以外にもLWE（Learing with Errors）などの問題が提案されており、近年活発に研究されている分野の1つでもある。	TU Darmstadt Lattice Challenge[*85]
符号理論ベース暗号 (Code-based cryptography)	NP困難な問題として知られている、ランダムに与えられた線形符号の最尤復号問題（誤りが混入しているデータから最も距離の近い符号語を求める符号としての復号であることに注意）を安全性の根拠に置く公開鍵暗号方式。1978年に提案されたMcEliece暗号は n=1024、k=524、t=50 のパラメータを持つGoppa符号を利用しているが60ビット安全性程度と見積もられており、十分な安全性を確保するためには公開鍵データ量が大きくなるデメリットがある。	Cryptanalytic challenges for wild McEliece[*86]
多変数公開鍵関数 (Multivariate polynomial cryptography)	EUROCRYPT1988で発表された今井-松本暗号と呼ばれる2次多変数公開鍵暗号が起源と言われている。これを一般化した位数qの有限体上の元を係数に持つn変数の多項式を考える。このとき十分大きなnに対して連立方程式を求めることが困難であると考えられており、この困難性を用いて公開鍵暗号が構成されている。一方でグレブナー基底を用いる効率的な攻撃方法が存在している。	Fukuoka MQ Challenge[*87]
ハッシュベース署名 (Hash-based signatures)	2分木のリーフを署名対象データと考え、Merkle Treeを構成するようにハッシュ連鎖を繰り返してルートを生成し、ルートに対して署名を打つことで実現する署名方式。原像計算困難性を持つ暗号学的ハッシュ関数を連鎖的に用いることから、個々のハッシュ値の原像計算さえも困難であり、ツリー全体の改ざんは難しいと考えられている。現在CFRGにてXMSSと呼ばれる方式が標準化されているほか、昨年のEUROCRYPTで発表されたSPHINCSなどの方式がある。	

*79 PQCRYPTO project、"Initial recommendations of long-term secure post-quantum systems"、2015（https://pqcrypto.eu.org/docs/initial-recommendations.pdf）。
*80 National Institute of Standards and Technology（NIST）、Workshop on Cybersecurity in a Post-Quantum World（http://www.nist.gov/itl/csd/ct/post-quantum-crypto-workshop-2015.cfm）。
*81 The Information Assurance Directorate（IAD）、Commercial National Security Algorithm Suite（https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm）。
*82 National Institute of Standards and Technology（NIST）、"Public Comments Received on NISTIR 8105 - Draft Report on Post-Quantum Cryptograph"、2016（http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/nistir-8105/nistir-8105-public-comments-mar2016.pdf）。
*83 National Institute of Standards and Technology（NIST）、"Report on Post-Quantum Cryptography"、NISTIR 8105、2016（http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf）、"NIST Kicks Off Effort to Defend Encrypted Data from Quantum Computer Threat"、2016（http://www.nist.gov/itl/csd/nist-kicks-off-effort-to-defend-encrypted-data-from-quantum-computer-threat.cfm）。
*84 NESSIE（New European Schemes for Signatures, Integrity, and Encryption）consortium、"Portfolio of recommended cryptographic primitives"（https://www.cosic.esat.kuleuven.be/nessie/deliverables/decision-final.pdf）。
*85 TU Darmstadt Lattice Challenge（https://latticechallenge.org/）。SVP（Shortest Vector Problem）Challenge（https://latticechallenge.org/svp-challenge/index.php）。Ideal Lattice Challenge（https://latticechallenge.org/ideallattice-challenge/index.php）。
*86 Cryptanalytic challenges for wild McEliece（https://pqcrypto.org/wild-challenges.html）。
*87 Fukuoka MQ Challenge（https://www.mqchallenge.org/）。Takanori Yasuda et al.、"MQ Challenge：Hardness Evaluation of Solving Multivariate Quadratic Problems"（https://eprint.iacr.org/2015/275）。

■ 耐量子暗号アルゴリズムの有力候補

現在耐量子暗号に用いられると予想されている4つの方式を表-2に提示します。これらは量子計算機が登場しても解読されないと期待されています。

これらのうち、前述したH2020 PQCRYPTO projectによるポートフォリオでは符号理論ベース暗号、ハッシュベース署名がリストされています。一方で日本では格子暗号の解読[*88]が盛んに研究されていますし、日本発で多変数公開鍵暗号のコンペティションが行われています。また、IETFにおいてはCFRG (Crypto Forum Research Group)[*89]にて耐量子暗号の議論が行われており、ハッシュベース署名の1種であるXMSS (Extended Hash-Based Signatures)[*90]の策定が続けられているほか、2016年5月に開催されたEUROCRYPT2016で併設されたinterim meeting[*91]においては暗号のコミュニティからの意見を収集するなどの試みが続けられています。また2016年4月に開催されたIETF-95のCFRG meetingでも耐量子暗号についての議論が行われています[*92]。

NISTの標準化スケジュールを見て分かるとおり、耐量子暗号への移行は喫緊に対応すべき課題ではなく中長期的な視点での対応が望まれます。新しい安全性根拠に基づいた暗号方式であることから、まずはどのくらいの強度があると見積れるのかについて調査する必要があります。そのため表-2に示されるように各種コンペティションが行われていて、より効率的な攻撃手法について研究が進められている状況です。一方で、ある鍵空間から秘密鍵を選択して、当該鍵のみでしか復号することのできない落し戸付き関数を定義する計算量的な安全性に基づく方式ではなく、情報理論的に安全な方式についても研究が進められています[*93]。いずれの選択肢においても、運用コストや実用性を鑑みて緩やかに移行していく必要があり、今後の動向についてキャッチアップしておく必要があるでしょう。

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、各種ランサムウェアとその対策、マルウェアに感染しないためのWindowsクライアント要塞化（前編）、耐量子暗号の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 セキュリティ本部 本部長、セキュリティ情報統括室 室長兼務。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。

根岸 征史（1.2 インシデントサマリ）
小林 直、永尾 禎啓、鈴木 博志、小林 稔、梨和 久雄（1.3 インシデントサーベイ）
梨和 久雄（1.4.1 各種のランサムウェアとその対策）
鈴木 博志（1.4.2 マルウェアに感染しないためのWindowsクライアント要塞化（前編））
須賀 祐治（1.4.3 耐量子暗号の動向）
IIJ セキュリティ本部 セキュリティ情報統括室

協力：
桃井 康成、平松 弘行　IIJ セキュリティ本部 セキュリティ情報統括室

*88 清藤ら、「量子コンピュータの解読に耐えうる暗号アルゴリズム『格子暗号』の最新動向」、ディスカッションペーパーシリーズ2015-J-9、2015（http://www.imes.boj.or.jp/research/abstracts/japanese/15-J-09.html）。Yoshinori Aono et al.、"Improved Progressive BKZ Algorithms and their Precise Cost Estimation by Sharp Simulator"（https://eprint.iacr.org/2016/146）。
*89 IETF Datatracker、Crypto Forum（https://datatracker.ietf.org/rg/cfrg/documents/）。
*90 Andreas Huelsing et al.、"XMSS：Extended Hash-Based Signatures"（https://datatracker.ietf.org/doc/draft-irtf-cfrg-xmss-hash-based-signatures/）。
*91 Agenda of interim meeting at EuroCrypt2016（https://www.ietf.org/proceedings/interim/2016/05/12/cfrg/agenda/agenda-interim-2016-cfrg-1）。
*92 IETF95 CFRG meeting、"Post Quantum Secure Cryptography Discussion"（https://www.ietf.org/proceedings/95/slides/slides-95-cfrg-4.pdf）。
*93 Junji Shikata、"Trends and Development of Information-Theoretic Cryptography"、IEICE Transactions 98-A（1）、2015（http://search.ieice.org/bin/summary.php?id=e98-a_1_16）。

迷惑メール最新動向

2.1 はじめに

1年ぶりとなった、IIRのメッセージングテクノロジーでは、迷惑メールの動向や迷惑メール対策を含めた、メールに関する技術情報について報告します。迷惑メール量は、ここ数年は減少傾向が続いてきましたが、直近の2016年3月に一時的に増加しました。本レポートでは、増加の要因となった送信元地域の調査結果を報告します。メールの技術動向では、今後普及が望まれるDMARCを中心とする送信ドメイン認証技術の普及状況について調査結果を報告します。

2.2 迷惑メールの動向

ここでは、迷惑メールの動向として、IIJのメールサービスで提供している迷惑メールフィルタが検知した迷惑メール量の割合の推移を元に、迷惑メールの変化の動向について報告します。これまでと同様に迷惑メールの割合は、一週間単位で集計し全体の受信メール量に対して、迷惑メールと判断された受信メールの割合の推移をグラフなどで示します。ここしばらく迷惑メールの量及び割合は、IIRの発行当初の2008年に比べて大幅に減少してきましたが、2016年3月に一時的に増加しています。

図-1に示す迷惑メール割合の推移のグラフは、前回のIIR (Vol.27) からの1年間、2015年3月30日から2016年4月3日までの53週間を含む、3年分のデータです。これより以前の推移については、IIR Vol.27を参照してください。迷惑メールの割合は、グラフを見て分かるとおり、年末年始の長期休暇期間などを除き、概ね減少傾向が続いてきましたが、2015年あたりから下げ幅が縮小してきました。2015年度の平均割合は、24.2%でした。2014年度が31.7%でしたので、7.5%程度減少したことになります。2013年度から2014年度の減少幅は15.7%でした。しかし、2016年3月には再び増加傾向となり、2016年3月28日の週は、44.8%まで上昇しました。その後、速報値では再び20%前後に戻りましたので、一時的な増加と考えています。この時期に増えた迷惑メールの傾向については、後ほど分析します。

2.2.1 引き続き危険度は高い状況

警察庁が平成28年3月17日に発表した資料[*1]によれば、平成27年中のインターネットバンキングに係る不正送金事犯の被害額が、過去最高の昨年を更に上回り約30億7,300万円であったことが報告されています。標的型メール攻撃も、連携事業者などからの報告が、3,823件と過去最多となっており、引き続きメールに起因する危険度は高い状態が続いていると言えます。更に、標的型メールの送信元アドレスの多くが偽装されていると考えられるものが77%であったと報告されており、やはり送信者情報の詐称を防ぐ、送信ドメイン認証技術の普及及び導入が急務であると言えます。

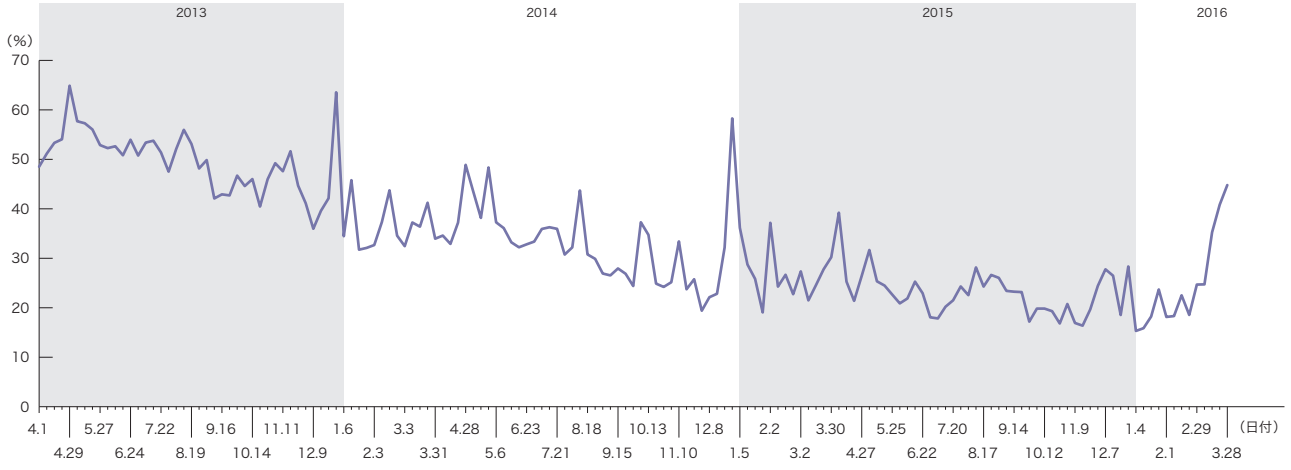


図-1 迷惑メール割合の推移

＊1　平成27年における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_jousei.pdf）。

2.2.2 迷惑メール送信元の割合

2015年度の第4四半期にあたる、直近の2016年1月から3月までの迷惑メールの送信元を地域別に示したグラフを図-2に示します。

この時期、最も迷惑メールを送信した地域は米国(US)で、16.8%でした。これまで発表してきた調査の中では、IIR Vol.10(2010年第3四半期)以来の1位でした。2位は中国(CN)で6.4%、これまで1位だったのですが今回は2位となりました。3位はブラジル(BR)で割合としては同じ数値となっていますが6.4%でした。4位も同じ割合ですが日本(JP)の6.4%でした。以後、インド(IN、6.3%)、ベトナム(VN、6.1%)、メキシコ(MX、5.4%)、香港(HK、3.1%)、アルゼンチン(AR、2.5%)、スペイン(ES、2.5%)と続きます。日本に近い、香港やベトナム以外は、国土が広くて人口の多い地域が上位となっていることが分ります。これら、上位10ヵ国の迷惑メール送信量の推移を図-3に示します。今回は、2016年3月の迷惑メール量の増加を分析するため、迷惑メール割合の推移ではなく、迷惑メール量の推移としています。そのため、縦軸の数値は示していませんが、それぞれの地域間での比較が具体的に分かるようになっています。

2.2.3 主要送信元地域の推移

図-3を見て分かるとおり、上位地域の中で、米国(US)、中国(CN)、日本(JP)、香港(HK)はもともとが送信量の多い地域ですが、2016年3月の増加時期でもそれ程大きな増加はありませんでした。この期間、最小送信数と最大送信数の差は2倍から3倍程度の違いでした。一方で、それ以外の上位地域、インド(IN)、ベトナム(VN)、メキシコ(MX)、ブラジル(BR)、アルゼンチン(AR)、スペイン(ES)の最小と最大の差は、いずれも10倍以上、特にアルゼンチン(AR)は、85倍の差がありました。いずれも迷惑メール割合の高かった2016年3月に増加している地域であることから、この時期の増加の要因であることが分ります。これらの地域が増加した原因の可能性としては、地域的にも分散していることから、ボットネットが活発に迷惑メールを送信していたのではないか、と推測しています。今後も、国際的な連携を元に、こうしたボットネットの対策をしていくことが必要と考えています。

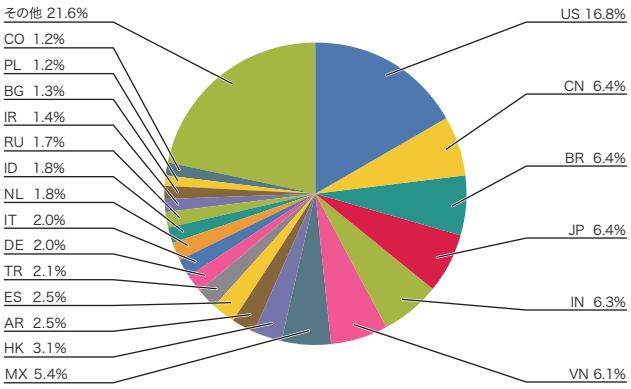


図-2 迷惑メール送信元地域の割合

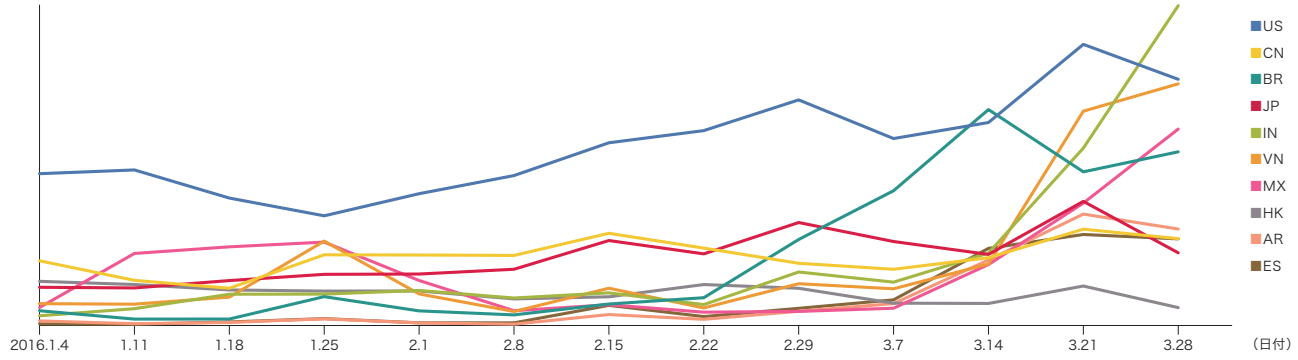


図-3 迷惑メール送信元上位10地域の推移

2.3 メールの技術動向

ここでは、迷惑メール対策にも有効な送信ドメイン認証技術、特にDMARC[*2]の普及状況や技術動向について報告します。

送信ドメイン認証技術は、これまでSPF[*3]とDKIM[*4]それぞれについて、技術詳細や普及の動向を述べてきましたが、今後は、それら2つの技術を基盤として利用するDMARCが主体になると考えています。

2.3.1 DMARCの概要

DMARCについては、既にIIR Vol.15から度々取り上げてきましたが、ここで改めてその特徴についてまとめておきます。DMARCも送信ドメイン認証技術の1つで、送信者情報から利用しているドメインが正しい送信者であるかを認証する技術です。主な特徴を以下に示します。

- SPFまたはDKIMで認証したドメインとメールヘッダ上のFrom (RFC5322.From)の一致(あるいは同じ組織であること)が前提
- 送信側(ドメインの管理側)が認証失敗時の受信側の振る舞いをポリシーとして表明可能
- 送信側が、認証失敗時のレポート先を指定可能
- これらの情報は、DNS上のTXT資源レコードで表明

つまりDMARCは、既に普及している、あるいは進みつつあるSPFとDKIMの認証結果を利用するもので、DMARC認証が「pass」したということは、メール受信者が参照可能なヘッダ上の送信者情報(RFC5322.From)とも一致していることを示す技術、ということになります。送信側では、認証が失敗した場合の情報をレポートとして受け取れることにより、メールが正しい経路で送信されているかを確認できます。これまで、SPFやDKIMで認証してきたドメインは、必ずしも最終的なメール受信者が確認しやすい送信者情報とは言えませんでした。DMARCで認証することにより、ある意味では、認証するドメインを統一することができ、受信者にも分かりやすい形になりました。

2.3.2 DMARCの普及状況

IIJのメールサービスでは、2014年よりDMARCに対応しており、受信するメールをDMARCで認証しています。ここでは、2016年1月から3月までの3ヵ月間で、DMARCでの認証結果の割合を図-4に示します。DMARC認証の前提となる、同期間でのSPFとDKIMの認証結果割合を図-5と図-6にそれぞれ示します。

まず、図-5のSPFの認証結果の割合ですが、今回SPFで認証できなかった「none」以外の割合、すなわち送信側でSPFを導入している割合は77.4%でした。前回調査結果を示したのは、2014年のIIR Vol.23で、このときから4.2%増加しました。送信側で

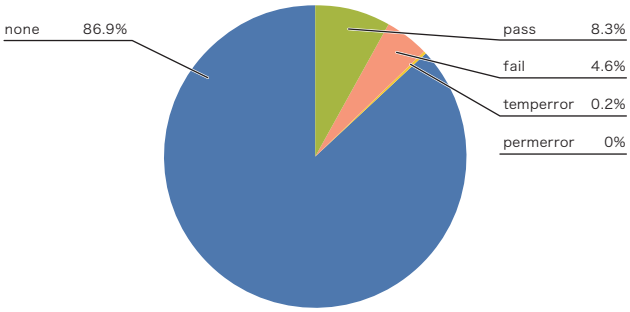


図-4 受信メールのDMARCでの認証結果割合

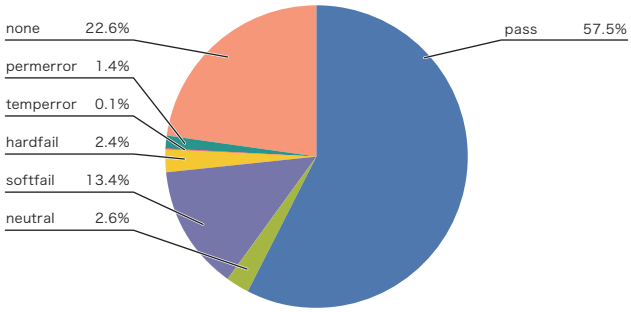


図-5 受信メールのSPFでの認証結果割合

*2 Domain-based Message Authentication, Reporting, and Conformance(DMARC), RFC7489(https://rfc-editor.org/rfc/rfc7489.txt)。
*3 Sender Policy Framework(SPF)for Authorizing Use of Domains in Email, Version 1, RFC7208(https://www.rfc-editor.org/rfc/rfc7208.txt)。
*4 DomainKeys Identified Mail(DKIM)Signatures, STD76, RFC6376(https://www.rfc-editor.org/rfc/rfc6376.txt)。

のSPFの導入は、比較的容易であることから、これまでもSPFの導入率は高い傾向がありましたが、今回の調査でも少しずつですが伸びていることが分ります。

図-6のDKIMの認証割合では、「none」以外の導入割合は20.1%でした。同様に前回からは8.5%伸びており、もともと送信側の導入にコストがかかるDKIMの導入率は低かったわけですが、それでもこちらも少しずつ導入割合が伸びていることが分かります。これらSPFあるいはDKIMを導入していることが、DMARC導入の前提となるのすが、図-4に示したとおり、DMARCでの認証ができなかった「none」以外の割合、すなわちDMARCの導入割合は、13.1%です。DMARCは、SPFあるいはDKIMを導入していれば、"_dmarc"サブドメインのTXT資源レコードにDMARCレコードを記述するだけで導入できますので、SPF及びDKIMより導入割合が低かったということは、まだDMARCに対する認知度が低いと考えられます。今後も、DMARCの利点及び導入方法について働きかけを行う必要があると考えます。

もう1つ、図-4のDMARCの認証割合で特徴的なのが、認証結果「fail」の割合が4.6%と高いことです。メールの転送時に認証が失敗しやすいSPFでは、予めそうした事象が想定される場合に「softfail」とやや弱めの失敗結果となるようにSPFレコードを宣言する傾向があります。そのため、SPFで「softfail」となる割合が13.4%と多いことは想定可能です。しかしながら、SPFでより強い認証の失敗結果である「hardfail」の2.4%、DKIMの「fail」の0.7%と比べると、DMARCの認証失敗だった4.6%はとても高い割合と言えます。この要因については、次節で分析します。

2.3.3 DMARC認証成功と失敗の要因

DMARCでは、SPFあるいはDKIMのどちらかの認証が成功した場合に、メールの「From:」ヘッダ上のドメインがDMARCレコードを宣言していた場合に、DMARC認証が評価されます。つまりDMARCの認証結果が「pass」であった、ということは、そのドメイン(RFC5322.From)とSPFあるいはDKIMで認証したドメインが一致あるいは関連のあるドメインで、SPFあるいはDKIMの認証結果のどちらかが「pass」であった、ということになります。そこで、DMARC認証が「pass」であった場合の、その要因について分析してみました。結果を図-7に示します。

DMARCが「pass」のときに最も多いSPFとDKIMの認証結果のパターンは、両方とも「pass」だった場合で、その割合は69.8%でした。つまり、DMARCレコードを宣言していて、正しくDMARC認証が「pass」するドメインの多くは、SPFとDKIMを共に導入しているドメイン、ということが分かりました。SPFとDKIMのどちらか一方の認証が失敗している、あるいは導入していない場合で、そのもう一方が「pass」だったためにDMARCとして

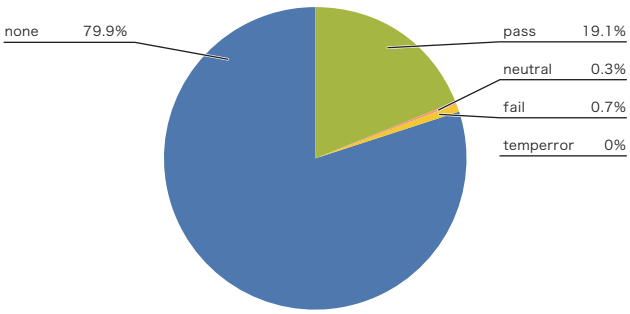


図-6 受信メールのDKIMでの認証結果割合

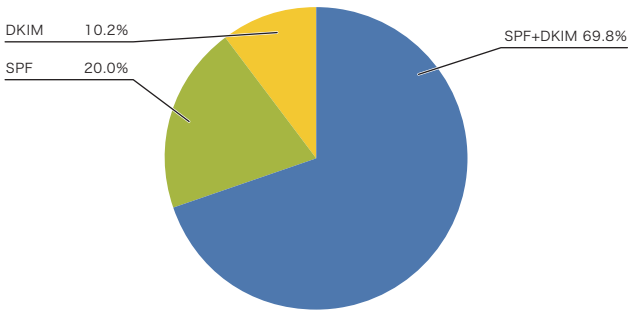


図-7 DMARCが「pass」の要因

は「pass」だった場合は、SPFが「pass」だった割合の方が多く、20.0%でした。DKIMだけが「pass」だった割合はそのおよそ半分で10.2%でした。SPFの普及率の高さが、そのままDMARC認証の「pass」の結果に結びついた、と考えられます。

今度は、DMARCが「fail」したときに最も多いSPFとDKIMの認証結果のパターンを図-8に示します。

DMARCが「fail」したときに、最も多いSPFとDKIMの認証結果のパターンは、SPFだけで認証し（DKIMは「none」）そのSPFの認証結果が「fail」だった場合です。逆に、DKIMだけの認証結果を利用した際、DKIMの認証結果が「fail」だったためにDMARCも「fail」となってしまった場合は、0.6%と非常に低い割合となりました。これもSPFとDKIMの普及率の違いと、DKIM認証の堅牢さを示した結果と考えられます。SPFとDKIMの両方が「fail」するパターンは、0.7%と低い数値でした。これらのことから、DMARCの認証失敗を防ぐためには、DKIMを導入することが有効である、ということが分かりました。

DMARC認証失敗要因の割合の中で、「DMARC」と示された10.6%は、SPFあるいはDKIMで認証したドメインとDMARCで認証するRFC5322.Fromのドメインが一致しないことにより、DMARCとして認証が「fail」してしまった割合です。これが、SPFやDKIMでの送信者情報を詐称してRFC5322.Fromだけを詐称元のドメインとしている場合であれば、正しく詐称が見破られた好例となります。しかし、もしこれが正規の正しいメールが「fail」しているとすれば、せっかくSPFあるいはDKIMを導入し、DMARCレコードを宣言しておきながら、認証するドメインが異なるために「fail」してしまう残念なケースと言えます。こうしたケースの中には、メール配送を他の事業者に委託しており、SPFあるいはDKIMの認証ドメインが、それら委託先のドメインで認証されることによるドメインの不一致が原因としてあるようです。私が受信したメールの中でも、大手銀行などから送られるメールマガジンなどが、このケースでDMARC認証が失敗しているものがありました。メールの送信者情報は、メールの送信元を示すものなので、SPFやDKIMで利用するドメインも、正しく送信者のドメインとして分かりやすいように利用すべきではないでしょうか。

図-8で示される「none」の割合の意味は、SPFとDKIMの両方の認証結果が「none」であるにも関わらず、DMARCとして認証結果が「fail」となったパターンです。これも、DMARCとして詐称が判断できたのであれば良いのですが、そうではないパターンもあるようです。詳しく調べると、DMARCの特徴である、RFC5322.Fromのドメインは、その上位ドメインも同じ組織のドメインとして扱うという「Organizational Domain」という仕組みも起因しているようです。つまり、送信しているメールがSPFとDKIMの両方に対応していないが、ヘッダ上のRFC5322.Fromドメインの上位ドメインがDMARCレコードを宣言していることで、DMARCとして認証しようとして、その結果「fail」

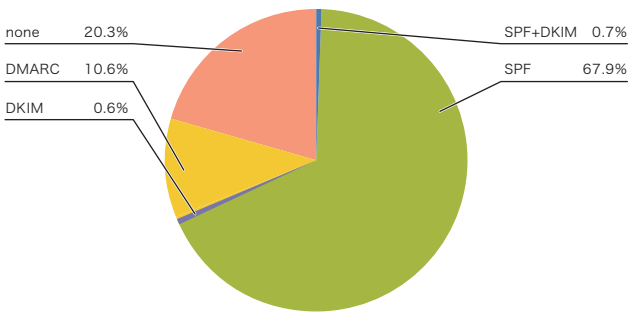


図-8 DMARCが「fail」の要因

となってしまう、ということです。ドメインの管理者としては、DMARCレコードを宣言する場合には、そのサブドメインも含めてSPFあるいはDKIMの設定もすることをお勧めします。

2.3.4 DMARCの関連技術動向

これまでIIRでは、メーリングリストやメール転送など、メールの再配送時に正しいメールであってもDMARCの認証が失敗してしまうケースがあることを紹介しました。DMARCの仕様を検討している組織でも、この問題は認識しており、今回この課題を補うための仕様の1つとして、ARC(Authenticated Received Chain)[*5]が提案されました。この技術は、その名前のとおりメールの再配送時などに、既に認証した情報をつないでいくことで、認証の連鎖を実現しようとするものです。ARCの仕様がある程度明確になった段階で、またその仕組みについて紹介したいと考えています。

2.4 おわりに

迷惑メールの割合は、2010年以降少しづつ減少してきましたが、本レポートで報告したとおり、一時的に増加した時期がありました。これまで減少してきた理由は、迷惑メールの主要な送信手法であるボットネットが活動できないような対策を継続してきたことで効果をあげてきたと言われています。今回の増加が一時的なものであれば良いのですが、こうした大量送信できる能力が依然として存在できるという状況は、やはり脅威であると考えています。

また、迷惑メールの質的な問題についても、引き続き注意が必要です。日本でも、迷惑メールが起因していると考えられる、金銭的な被害や情報漏えいなどの事象が引き続き高いレベルで発生しています。こうした被害の要因には、悪質なマルウェアが関係していると言われています。メールとして直接送信される場合もあるでしょうし、マルウェアに感染させるためのトリガとしてメールが利用される場合もあります。メールをコミュニケーション手段の基盤として引き続き維持していくためには、もう一段強い対策としての枠組みが必要なのかもしれません。

そうした対策の枠組みの1つの例として、前回のIIR(Vol.27)では、DMARCを中心とする送信ドメイン認証技術と、認証したドメインを評価するドメインレピュテーション、レピュテーションの精度を高めるためのフィードバックループの組み合わせについて解説しました。これらの機能要素は、それぞれが関連し合うことで機能を高める側面があります。なので、全体としてそれぞれが普及していくことが望ましいのですが、まずは送信側の導入が容易であり、既に標準化もされグローバル環境でも普及しつつあるDMARCが、もう少し日本で普及していても良いのではと考えています。まずは、現在の普及状況を知るために、今回のレポートではDMARCの認証結果の割合について調査し、報告しました。今後も引き続き、様々な調査を行い、対策に有効な技術の普及に貢献していきたいと考えています。

執筆者:
櫻庭 秀次(さくらば しゅうじ)
IIJ ネットワーク本部 アプリケーションサービス部 シニアエンジニア。
コミュニケーションシステムに関する研究開発に従事。特に快適なメッセージング環境実現のため、社外関連組織と協調した各種活動を行う。
M3AAWGの設立時からのメンバー。迷惑メール対策推進協議会 座長代理、幹事会 構成員、技術WG 主査。
一般財団法人インターネット協会 迷惑メール対策委員会 委員長。

*5 Authenticated Received Chain(ARC)、draft-andersen-arc-04(https://www.ietf.org/id/draft-andersen-arc-04.txt)。

TLSの動向

最近、IETF（Internet Engineering Task Force）ではTLS（Transport Layer Security）が盛んに議論されています。議論が活発になった理由は、何と言っても2013年にエドワード・スノーデン氏によって暴露されたアメリカ政府によるネット・電話の極秘監視・情報収集プログラムPRISMでしょう。PRISMに代表される広域監視（pervasive monitoring）の存在が明らかとなり、IETFはプライバシの問題を再考する必要にせまられました。RFC 7258で宣言されているように、今後IETFで策定されるプロトコルは、広域監視をやりにくくするよう設計されることになります。

HTTPに関して言えば、TLSの利用が強く推奨されていくことになるでしょう。事実、2015年に策定されたHTTP/2（RFC 7540）を利用する場合、主要ブラウザがTLSを要求するため、TLSの利用が実質的に必須となっています。もちろん、現在の主流であるHTTP/1.1でも、TLSの利用が強く推奨されています。TLSを利用するにはHTTPサーバに証明書が必要です。これまで証明書の発行は有償であり、そのせいでTLSの利用を思いとどまった方も多いでしょう。現在では、Let's Encryptというプロジェクトによって証明証を無償で発行してもらうこともできます。

TLSの最新のバージョンは1.2であり、策定後8年が経過しています。この間、TLSに対する様々な攻撃手法が発見されました。RFC 7457は、攻撃手法をまとめた素晴らしい文章です。新たな攻撃手法や暗号技術の老朽化に伴い、推奨されるTLSの利用方法も変わってきました。現時点でのお薦めの利用方法は、RFC 7525でまとめられています。これらの知見をもとに、現在IETFでTLS 1.3の策定が進められています。この記事では、TLSの仕組みを知っている方を対象に、TLSの動向について説明します。

バージョン	仕様	制定年	利用
SSL 2.0	ID 止まり	1995年	RFC 6176により利用禁止
SSL 3.0	RFC 6101	1996年 （RFC発行は2011年）	RFC 7568により利用禁止
TLS 1.0	RFC 2246	1999年	△
TLS 1.1	RFC 4346	2006年	△
TLS 1.2	RFC 5246	2008年	○
TLS 1.3	ID	策定中	

表-1 SSL/TLSのバージョン

3.1 バージョン

TLSの前身はNetscape Communications社が世に送り出したSSL（Secure Socket Layer）です。1995年にSSL 2.0、1996年にSSL 3.0の仕様が公開されました。SSL 2.0は設計上の様々な問題があり、RFC 6176により利用が禁止されました。SSL 3.0も、脆弱性POODLEに代表される攻撃や設計上の問題のため、RFC 7568により使用しないよう求められています。SSLはIETFに持ち込まれて標準化されTLSとなりました。策定されたTLSのバージョンは、1.0、1.1、1.2です。詳しくは後述しますが、現在ではデータの認証と暗号化のためにはAEAD（Authenticated Encryption with Associated Data）という方式を使うことが推奨されています。AEADは、TLS 1.0と1.1では使用できません。端的に言うと、現在TLSを安全に使うには、TLS 1.2を適切な利用方法で使用する必要があります。

SSL/TLSのバージョンに関する情報を表-1にまとめます（IDはInternet-Draftの略記です）。今回、TLS 1.3についても説明しますが、仕様は現在策定中ですので、最終的には少し変わるかもしれないことをご了承ください。

3.2 適切な暗号スイート

TLS 1.2を定めたRFC 5246で実装が必須とされている暗号スイートは、TLS_RSA_WITH_AES_128_CBC_SHAです。これは以下のような意味です。

- 鍵交換はRSA
- サーバ認証もRSA
- 通信の暗号化はAESのCBCモード
- MACを生成する関数がSHA1

HTTP/2で必須とされ、RFC 7525で第一候補にすべきとされているTLS 1.2の暗号スイートは、TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256です。これは、以下のように解釈します。

- 鍵交換は使い捨て楕円Diffie Hellman（ECDHE：Elliptic Curve Diffie Hellman, Ephemeral）
- サーバ認証はRSA
- 通信の暗号化はAES 128のGCM（Galois/Counter Model）モード
- ハッシュ関数がSHA256

TLS 1.3では、TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256に加えてTLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256の実装も必須としています。サーバ認証が、RSAからECDSA（楕円暗号を用いたDSA）に変わっただけですね。

次に、このように推奨される暗号スイートが変化した理由を説明します。

3.3 公開鍵暗号と鍵交換

前述のように推奨される鍵交換の方法は、RSAから使い捨てDiffie Hellman系に変わりました。理由は、RSAが持たない前方秘匿性（forward secrecy）を使い捨てDiffie Hellman系が持つからです。前方秘匿性とは、将来に渡ってデータの秘匿性が守られることです。

鍵交換にRSAを用いると、前方秘匿性がない理由を考えましょう。クライアントがサーバにTLSで接続すると、サーバはクライアントに証明書を送ります。証明書とは、認証局の署名が付いたサーバの公開鍵のことです。クライアントは、サーバと共有すべき秘密を生成し、サーバのRSA公開鍵で暗号化してサーバに送ります。この暗号文を復号できるのは、RSA秘密鍵をもっているサーバのみです。これで、クライアントとサーバは秘密が共有できましたので、この秘密から生成される鍵を使い、共通鍵暗号で通信路を保護します。

この時点では、この暗号路は安全です。第三者が中身を盗聴することはほとんど不可能です。しかし、次のようなことが現実に起こると、盗聴されてしまいます。

ある広域監視が、この暗号路を流れるデータをすべて保存しています。そして、サーバの入れ替えに伴い、サーバを破棄する際に誤ってディスクの内容を消去しませんでした。広域監視がこのディスクを手に入れれば、秘密鍵が取り出せるので、保存していた暗号路のデータを順に復号できます。

一方、使い捨てDiffie Hellman系では、クライアントとサーバが、お互いに使い捨ての公開鍵と秘密鍵を生成します。これらの秘密鍵はディスクに保存されることはないので、前述のようなことは起こりません。

使い捨てDiffie Hellman系では、オリジナルのDHE（Diffie Hellman, Ephemeral）よりも楕円暗号で実現したECDHE（RFC 4492）の方が普及しそうです。その理由は、次のとおりです。

- DHEに比べて、ECDHEの方が交換するデータの量が少ない。
- DHEに比べて、ECDHEの方が計算速度が速い。
- ECDHEには、厳選されたパラメータがあらかじめ定義されている。DHEでも定義しようとするIDはあるが、まだRFCとなっていない。
- 前述のようにRFC 7525で第一候補だと定められている。

前方秘匿性については、「IIR Vol.22、1.4.2 Forward Secrecy」も参考にしてください。

3.4 共通鍵暗号の老朽化

TLS 1.1以前では、暗号文の形式は次の2つがあります。

- ストリーム暗号
- CBC（Cipher Block Chaining）モードのブロック暗号

ストリーム暗号として実質上唯一の選択肢であるRC4には、様々な攻撃方法が見つかっており、利用が禁止されています（RFC 7465）。

TLS 1.0以前のCBCモードのブロック暗号に関しては、BEASTという攻撃方法が有名です。また、TLS 1.2以前のCBCモードのブロック暗号は、「MAC後暗号化」という手法を取っています。MAC（Message Authentication Code）とは、データが改ざんされてないことを保証したり、認証したりするための補助データです。「MAC後暗号化」では、平文からMACを生成し、平文とMACを連結した後に全体を暗号化します。「MAC後暗号化」には、パディングオラクル攻撃という攻撃手法が見つかっています。そのためRFC 7366では、「MAC後暗号化」の代わりに「暗号化後MAC」という書式を提案しています。

TLS 1.2では暗号文の第3の形式として、AEAD（Authenticated Encryption with Associated Data）が定められました。AEADとは、暗号化と認証を同時に実行する方式です。現在では、ストリーム暗号とCBCモードのブロック暗号ではなく、AEADを利

用することが推奨されています。AEADで利用できる共通鍵暗号のモードは、次のとおりです。

- AESのGCM（Galois/Counter Model）モード
- AESのCCM（Counter with CBC-MAC）モード

TLS 1.3では、ストリーム暗号やCBCモードのブロック暗号の書式は削られ、AEADのみが定義されています。

3.5 ハンドシェイク

この節では、TLSの実際のやりとりについて説明します。

3.5.1 フルハンドシェイク

クライアントがサーバに初めて接続するときは、フルハンドシェイクをする必要があります。TLS 1.2でTLS_RSA_WITH_AES_128_CBC_SHAが選ばれると、図-1のようなやりとりになります。

- クライアントは、ClientHelloで暗号スイートの候補を提示します。
- サーバは、TLS_RSA_WITH_AES_128_CBC_SHAを選んだことをServerHelloで伝えます。Certificateには、サーバのRSA証明書が入っています。
- クライアントは、秘密を生成、サーバのRSA公開鍵で暗号化し、ClientKeyExchangeに格納して送ります。その後ChangeCipherSpecを送って、通信路を暗号路に切り替えます。この暗号路は、AESのCBCモードで暗号化されます。暗号路に切り替えた直後に、ハンドシェイクがうまくいった証拠としてFinishedを送ります。また、今後アプリケーションから受け取ったデータも、この暗号路を用いて送られます。図-1の灰色は、暗号路を表現しています。
- サーバは、サーバの秘密鍵を使って秘密を取り出し、クライアントと同様にChangeCipherSpecを送って、通信路を暗号路に切り替えます。

次に、TLS 1.2でTLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256が選ばれたときを説明します（図-2）。TLS_RSA_WITH_AES_128_CBC_SHAの場合と異なる点は、次のとおりです。

- ClientHelloを受け取ったサーバは、TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256を選択します。そして、ECDHEの使い捨て公開鍵と秘密鍵を生成します。この公開鍵は、ServerKeyExchangeの中に入れて送ります。
- クライアントも、ECDHEの使い捨て公開鍵と秘密鍵を生成します。自分の秘密鍵とサーバの公開鍵から、秘密を生成します。ClientKeyExchangeには、自分の公開鍵を入れて送ります。
- サーバは、自分の秘密鍵とクライアントの公開鍵から秘密を生成します。

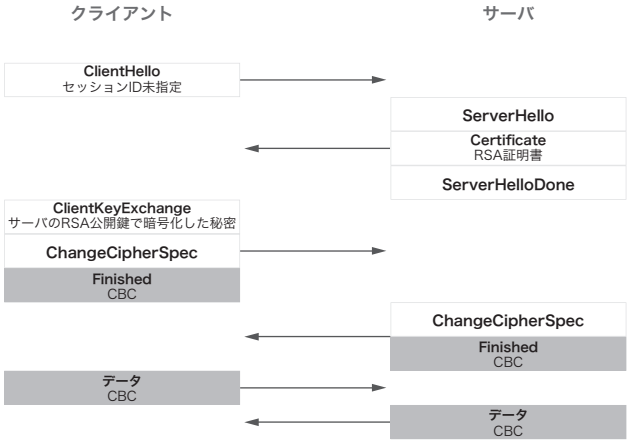


図-1 TLS 1.2フルハンドシェイク
TLS_RSA_WITH_AES_128_CBC_SHA

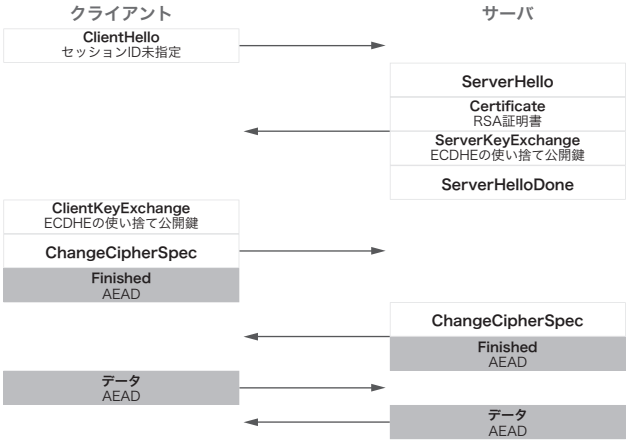


図-2 TLS 1.2フルハンドシェイク
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

フルハンドシェイクは、TLS 1.0、1.1、1.2では変わり映えしません。しかしながら、TLS 1.3のフルハンドシェイクは根本的に再設計されています。なんと言っても、Helloに鍵交換の役割を持たせることで、RTT（Round Trip Time）を1つ減らしているのです。

- クライアントは、ECDHEの使い捨て公開鍵と秘密鍵を作り、ClientHelloのオプションに公開鍵を格納して送ります。
- サーバも、ECDHEの使い捨て公開鍵と秘密鍵を作り、ServerHelloのオプションに格納して送ります。また、ここからすぐ通信路が暗号化されます。サーバの証明書を格納するCertificateやFinishedは、暗号化されて送られます。Finishedを送ったあとは、更に安全な暗号路へと切り替わります。図-3の灰色の濃さの違いは、この暗号路の違いを表現しています。
- クライアントは、現在の暗号路でFinishedを送った後、更に安全な暗号路へと切り替えます。

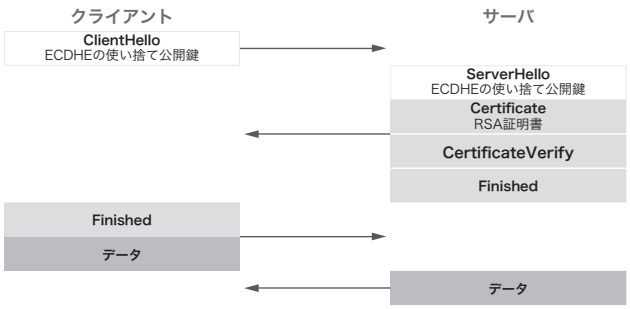


図-3 TLS 1.3フルハンドシェイク
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

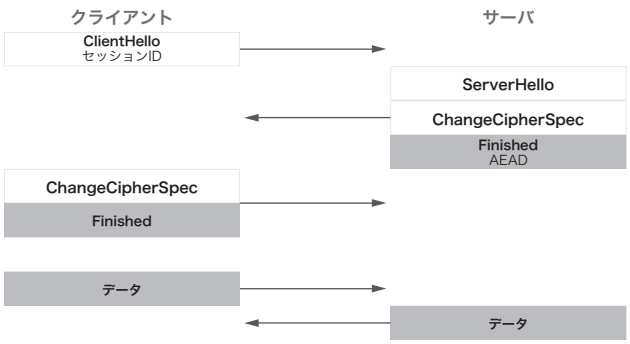


図-4 TLS 1.2セッション再開

3.5.2 セッションの再開

クライアントとサーバが、以前TLS 1.2でフルハンドシェイクしていれば、そのセッションを再開することで、鍵交換を省略できます。図-4をご覧ください。

- クライアントは、ClientHelloで再開したいセッションのIDを指定します。
- サーバは、指定されたセッションIDに対する状態を保存していれば、それを使って暗号路に切り替えます。

セッションの再開は、公開鍵暗号の重い計算を省略するばかりではなく、RTTも1回減らせます。しかし、この方法ではサーバがセッション情報を保持する必要があります。クライアントの数に比例して、保持すべき状態の数も増えます。サーバの負担が増えるこの方法は、あまりうまいとは言えません。

サーバの負担を減らす方法として、RFC 5077でセッションチケットが定義されています。セッションチケットとは、サーバのみが復号できる暗号化されたセッション情報のことです。セッションチケットを用いると、サーバはセッション情報を保持する必要がなくなります。

TLS 1.2でセッションチケットを使うためには、まずセッションチケットのためのフルハンドシェイクをする必要があります（図-5）。

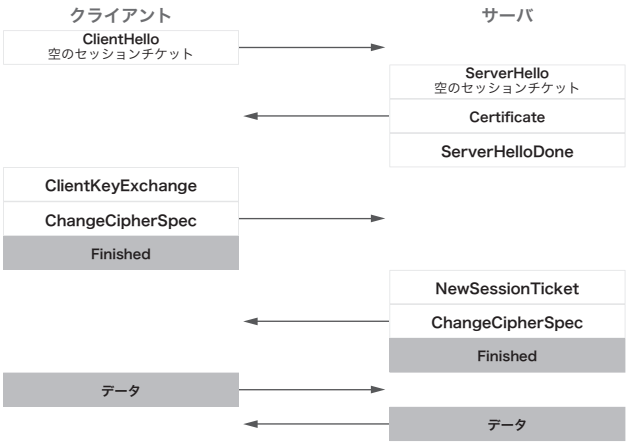


図-5 TLS 1.2セッションチケットのためのフルハンドシェイク

- クライアントは、ClientHelloの拡張として空のセッションチケットを送り、セッションチケットに対応していることをサーバに知らせます。
- サーバも、空のセッションチケットをServerHelloのオプションに指定することで、セッションチケットに対応していることをクライアントに知らせます。
- サーバは、ChangeCipherSpecを使って暗号路に切り替える直前に、生成したセッションチケットをNewSessionTicketに入れて送ります。
- クライアントは、現在のセッション情報と送られてきたセッションチケットを対応付けて保存します。

次に、TLS 1.2でセッションチケットを使ってセッションを再開する方法を説明します(図-6)。

- クライアントは再開するセッション情報とセッションチケットを取り出し、ClientHelloのオプションにセッションチケットを格納して送ります。
- サーバは、セッションチケットを復号して、セッション情報を得ます。必要であれば、新しいセッション情報をNewSessionTicketで送ります。その後、暗号路に切り替えます。
- クライアントは、前述のセッション情報を使って、暗号路に切り替えます。

TLS 1.3のセッションチケットは、RFC 4297で定義されているPSK(Pre-Shared Key)と統合されています。PSKとは、サーバやクライアントの認証のために、公開鍵ではなく、あらかじめ共有している秘密を用いる方式のことです。TLS 1.3のPSKハンドシェイクをセッションチケットの機能に限って使えば、TLS 1.2のそれとあまり変わりません(図-7)。細かな違いは、次のとおりです。

- フルハンドシェイクの後、サーバがいつでもNewSessionTicketを送信できます。
- TLS 1.3のフルハンドシェイクと同様、暗号路が2回切り替わります。

3.5.3 証明書を用いたクライアント認証

TLSを用いて、あるサーバのあるページにアクセスしている場合を考えましょう。そのページにあるリンクの先は、同じサーバにあるが、証明書を使ったクライアント認証が必要なコンテンツだったとします。

TLS 1.2では、途中で証明書を使ったクライアント認証が必要となった場合、再ネゴシエーションを用います。これは文字通り、ハンドシェイクを再び実行するのです。フルハンドシェイクと違うのは、暗号路の中でハンドシェイクすることです(図-8)。

- サーバは、HelloRequestを送ってクライアントに再ネゴシエーションを要求します。
- クライアントは、ClientHelloを送ります。
- サーバは、ServerHelloを送る際に、CertificateRequestも送ってクライアントの証明書を要求します。
- クライアントは、ClientKeyExchangeを送る際にクライアントの証明書をCertificateに入れて送ります。

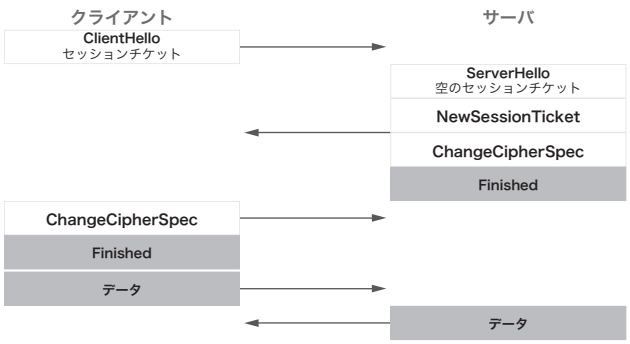


図-6 TLS 1.2セッションチケットを用いたセッションの再開

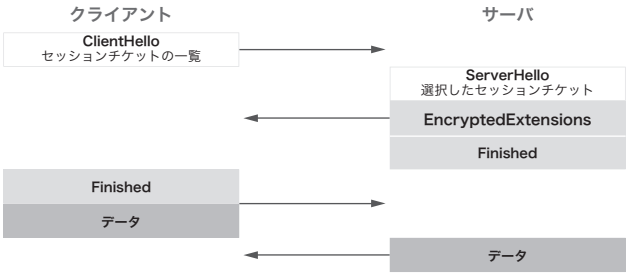


図-7 TLS 1.3セッションチケットを用いたセッションの再開

再ネゴシエーションの本来の目的は、暗号路をリフレッシュして暗号路の寿命を延ばすことです。証明書を用いたクライアント認証にも使われるのは、CertificateRequestをServerHelloの直後に送らなければならないというTLS 1.2の制約からです。

TLS 1.3では、暗号路のリフレッシュと証明書を用いたクライアント認証を明確に分けます。CertificateRequestは、いつでもサーバからクライアントに送れるようになります(図-9)。

3.5.4 0-RTT

TLS 1.3では、ClientHelloを送る際にアプリケーションのデータも暗号化して送る0-RTTというハンドシェイクが検討されています。少し複雑なので今回は説明を割愛します。興味がある方はTLS 1.3のIDを参照してください。

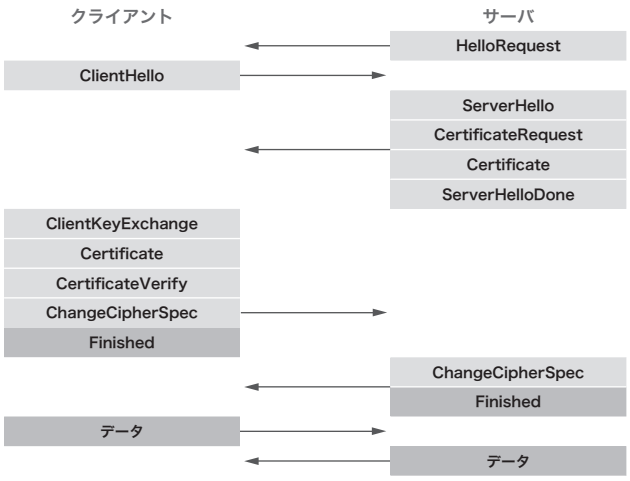


図-8 TLS 1.2での証明書を用いたクライアント認証

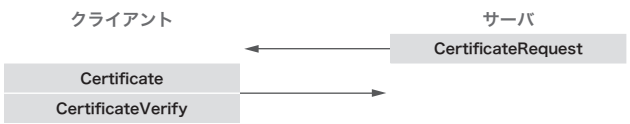


図-9 TLS 1.3での証明書を用いたクライアント認証

3.6 圧縮

TLS 1.2以前では、平文と暗号文に加えて、圧縮文という書式があります。圧縮機能を使う場合、平文が圧縮されて圧縮文となり、更に暗号化されて暗号化文となります。残念ながら、圧縮の機能を利用するとCRIMEやBREACHという攻撃にさらされることになります。

ですから、TLS 1.2を利用する場合、圧縮機能を利用してはいけません。平文を圧縮文を介さず直接暗号化し、暗号文にします。TLS 1.3では、圧縮文という書式は削られ、平文と暗号文のみが定義されています。

3.7 Let's Encrypt

Let's Encryptは、サーバの証明書を無償で自動発行するプロジェクトです。発行できる証明書の種類は、ドメイン認証(DV: DOmain Validation)のみで、企業認証(OV:Organization Validation)やEV(Extended Validation)認証の証明書は発行できません。現時点では、ワイルドカード証明書は発行できません。複数のサーバ名がある場合は、DV証明書をサーバ名の数だけ発行してもらうか、代替名(SAN:Subject Alternative Name)を利用するとよいでしょう。Let's Encryptが提供するコマンド群は、IETFが標準化を進めているACME(Automatic Certificate Management Environment)というプロトコルを実装しています。Let's Encryptについては、「IIR Vol.30、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」も参考にしてください。

3.8 おわりに

今回は、攻撃手法に関しては名前だけ示して、具体的方法については説明しませんでした。検索すれば、それぞれの攻撃手法に対する詳しい解説が簡単に見つかります。興味を持たれた方は、ぜひ読んでみるといいでしょう。

執筆者:
山本 和彦(やまもと かずひこ)
株式会社IIJイノベーションインスティテュート 技術研究所 主幹研究員。
プログラミング言語Haskellの並行技術をネットワークプログラミングへ応用することに興味を持つ。
最近取り組んでいるプロトコルはHTTP/2やTLS 1.3。
翻訳書に「プログラミングHaskell」「Haskellによる並列・並行プログラミング」がある。

June 2016 Vol.31

Internet Initiative Japan

株式会社インターネットイニシアティブ(IIJ)について

IIJは、1992年、インターネットの研究開発活動に関わっていた技術者が中心となり、日本でインターネットを本格的に普及させようという構想を持って設立されました。
現在は、国内最大級のインターネットバックボーンを運用し、インターネットの基盤を担うと共に、官公庁や金融機関をはじめとしたハイエンドのビジネスユーザに、インターネット接続やシステムインテグレーション、アウトソーシングサービスなど、高品質なシステム環境をトータルに提供しています。
また、サービス開発やインターネットバックボーンの運用を通して蓄積した知見を積極的に発信し、社会基盤としてのインターネットの発展に尽力しています。

株式会社インターネットイニシアティブ
〒102−0071 東京都千代田区富士見2-10-2　飯田橋グラン・ブルーム
E-mail : info@iij.ad.jp　URL : http://www.iij.ad.jp/