Bashの脆弱性Shellshockについて

**今回は、話題となったBashの脆弱性Shellshockについて、
SSLv3への新たな攻撃手法POODLE attackについて、
昨年から発生し続けているリスト型攻撃の発生状況と対策について解説します。**

1.1 はじめに

このレポートは、インターネットの安定運用のためにIIJ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2014年7月から9月までの期間では、国内の報道機関など複数のサイトにおいて、DNSハイジャックによりマルウェア感染に誘導される事件が発生しました。また、非常に多くの製品やサービスに影響するGNU Bashの脆弱性が発見されています。オンラインサービスに対するリスト型攻撃による不正ログイン事件や、オンラインバンキングを悪用した不正送金事件が依然として継続的に発生しています。DDoS攻撃においては、DNSやNTPに続いてSSDPを踏み台とする攻撃が国内においても発生しました。国外では、200Gbpsを超えるようなDDoS攻撃が散発的に発生しています。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。

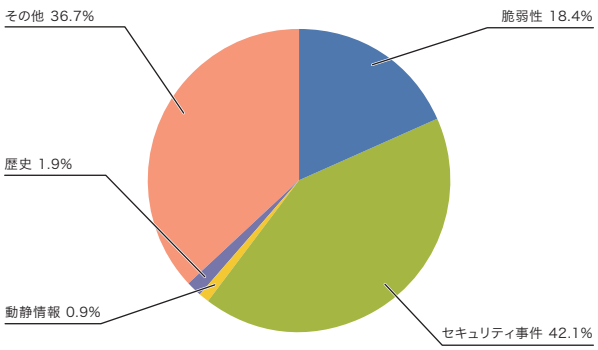


図-1 カテゴリ別比率(2014年7月〜9月)

1.2 インシデントサマリ

ここでは、2014年7月から9月までの期間にIIJが取り扱ったインシデントと、その対応を示します。まず、この期間に取り扱ったインシデントの分布を図-1に示します[*1]。

■ 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。7月から8月にかけて、パレスチナ自治区ガザでの紛争に関連し、イスラエルの複数の政府関連サイトや民間企業のWebサイトに対し、Web改ざんやDDoS攻撃、情報漏えいの被害が発生しています(OpSaveGaza)。紛争に関連するところでは、ロシアとウクライナ、インドとインドネシア、インドとパキスタンなどで、相互に攻撃が行われています。8月から9月にかけては、パキスタン政府への抗議から、複数の政府関連サイトに対するWeb改ざんやDDoS攻撃、SQLインジェクションによる情報漏えいの被害が発生しました(OpPakistan)。9月には、香港での選挙制度の問題に対するデモ活動と関連して中国政府や香港行政府のWebサイトに対するDDoS攻撃やメールアカウント情報の漏えいなどが発生しています(OpHongKong)。

他にも、世界中の各国政府とその関連サイトに対して、AnonymousなどのHacktivist達による攻撃が継続して行われました。また、Syrian Electronic Armyを名乗る何者かによるSNSアカウントの乗っ取りやWebサイト改ざんも継続して発生しており、被害を受けたアカウントにはイスラエル国防軍なども含まれていました。

*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]、Internet Explorer[*4][*5][*6]などで修正が行われました。Adobe社のAdobe Flash Player、Adobe Reader及びAcrobatでも修正が行われました。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。

Cisco Unified Communications Domain Managerには、権限昇格を含む複数の脆弱性が見つかり、修正されています。修正された脆弱性には初期設定のSSH秘密鍵の利用による脆弱性が含まれていました。機器の初期設定のSSH秘密鍵を更新せず利用することは、同じ秘密鍵を持つ第三者から悪用される可能性が高いことから行うべきではありません[*7]。

LinuxなどUNIX系のOSで利用されているシェルのBashでは、任意のOSコマンドが実行できる脆弱性(CVE-2014-6271)が見つかり、修正されました。この脆弱性はShellshockと呼ばれ、CGIプログラムが動くWebサーバ、ルータやゲートウェイ製品など、多くのアプリケーションや機器に影響があったことから問題となりました。この問題の詳細については「1.4.1 Bashの脆弱性Shellshockについて」を併せてご参照ください。

■ なりすましによる不正ログイン

この期間でも、昨年から多数発生しているユーザのIDとパスワードを狙った試みと、取得したIDとパスワードのリストを使用したと考えられる不正ログインの試みが継続して発生しています。アンケートサイト、インターネット通販サイト、物流事業者のサポートサイト、携帯電話会社のサイト、SNSなど様々なサイトが攻撃対象となっています。このうちのいくつかの事件では、サイト上のポイントを他サービスのギフトポイントに不正に交換されるなどの被害も発生しています。このように、リスト型攻撃の脅威が依然として続いていることから、様々な企業のWebサービスやアプリケーションで、2段階認証の導入やパスワードの文字数や使用できる文字の制限緩和などの認証機能の強化といった対策が進められています。また、ユーザが安易な使い回しを行ったり、推測されやすい簡易なパスワードを設定するなどの問題も指摘されていることから[*8]、利用者側も安全な利用をする上で注意が必要です。詳細については「1.4.3 リスト型攻撃の発生状況と対策」も併せてご参照ください。

■ Web改ざんと不正なソフトウェアへの誘導

この期間では、前回の期間に続いてWebサイトの改ざんによる不正なソフトウェアへ誘導される事件が多く発生しました。ツアー会社、自動車販売会社、セキュリティ企業のWebサイトでの改ざんとそれによる不正なソフトウェアへの誘導が発生しています。また、不正なソフトウェアへの誘導だけでなく、独立行政法人のWebサイトが改ざんされた事件では、Web改ざんによってフィッシングサイトとして悪用しようとする試みも発生しています[*9]。また、テキスト

---

*2 「マイクロソフト セキュリティ情報 MS14-038 – 緊急 Windows Journalの脆弱性により、リモートでコードが実行される(2975689)」(https://technet.microsoft.com/ja-JP/library/security/ms14-038.aspx)。
*3 「マイクロソフト セキュリティ情報 MS14-043 - 緊急 Windows Media Centerの脆弱性により、リモートでコードが実行される(2978742)」(https://technet.microsoft.com/ja-JP/library/security/ms14-043.aspx)。
*4 「マイクロソフト セキュリティ情報 MS14-037 – 緊急 Internet Explorer用の累積的なセキュリティ更新プログラム(2975687)」(https://technet.microsoft.com/ja-jp/library/security/ms14-037.aspx)。
*5 「マイクロソフト セキュリティ情報 MS14-051 - 緊急 Internet Explorer用の累積的なセキュリティ更新プログラム(2976627)」(https://technet.microsoft.com/ja-JP/library/security/ms14-051.aspx)。
*6 「マイクロソフト セキュリティ情報 MS14-052 - 緊急　Internet Explorer用の累積的なセキュリティ更新プログラム(2977629)」(https://technet.microsoft.com/ja-JP/library/security/ms14-052.aspx)。
*7 同じ秘密鍵を利用するリスクについては、IIJ Security Diary、「SSL/TLS, SSHで利用されている公開鍵の多くが意図せず他のサイトと秘密鍵を共有している問題」(https://sect.iij.ad.jp/d/2012/08/109998.html)も参照のこと。
*8 例えば、IPAが実施した「『オンライン本人認証方式の実態調査』報告書について」(http://www.ipa.go.jp/security/fy26/reports/ninsho/index.html)などを参照のこと。
*9 例えば、次の独立行政法人 防災科学技術研究所の発表を参照のこと。「防災科研公開 web に対する改ざんについて」(http://www.bosai.go.jp/press/2014/pdf/20140811_01.pdf)。

7月のインシデント

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

脆 **3日**：Cisco Unified Communications Domain Managerに権限昇格を含む複数の脆弱性が見つかり、修正された。
"Multiple Vulnerabilities in Cisco Unified Communications Domain Manager"（http://www.cisco.com/cisco/web/support/JP/112/1122/1122753_cisco-sa-20140702-cucdm-j.html）。

脆 **9日**：Microsoft社は、2014年7月のセキュリティ情報を公開し、MS14-037とMS14-038の2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。
「2014 年 7 月のマイクロソフト セキュリティ情報の概要」（https://technet.microsoft.com/ja-JP/library/security/ms14-jul）。

脆 **9日**：Adobe Flash Playerに、任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「APSB14-17: Adobe Flash Player用のセキュリティアップデート公開」（http://helpx.adobe.com/jp/security/products/flash-player/apsb14-17.html）。

セ **9日**：通信教育企業は、同社の約2070万人分の顧客情報が名簿業者など外部に流出したことを公表した。その後、9月に公表された最終報告では約4858万人分の個人情報が漏えいしたことが判明している。

セ **9日**：インド政府のルート認証局の傘下で中間認証局を運営するインド国立情報工学センター（NIC）で複数のGoogleドメインやYahoo!ドメインの証明書が不正に発行されたことが判明し、複数のブラウザで当該証明書を無効にする対応が行われた。原因については証明書発行プロセスが破られたためとされている。
Google Online Security Blog、"Maintaining digital certificate security"（http://googleonlinesecurity.blogspot.jp/2014/07/maintaining-digital-certificate-security.html）。

他 **15日**：6月に成立した改正児童買春・ポルノ禁止法が施行された。ただし、自己の性的好奇心を満たす目的での児童ポルノの所持等を処罰する改正法７条１項の規定については、適切に廃棄などの措置ができるよう猶予期間として、施行の日から１年間は適用しないことが附則に定められたことから平成27年7月15日から適用される。
詳細については次の法務省による解説も参照のこと。「児童買春, 児童ポルノに係る行為等の処罰及び児童の保護等に関する法律の一部を改正する法律案」（http://www.moj.go.jp/keiji1/keiji11_00008.html）。

他 **15日**：総務省より、情報通信の現況及び情報通信の政策の動向について掲載した「情報通信白書平成26年版」が公表された。
情報通信白書ホームページ（http://www.soumu.go.jp/johotsusintokei/whitepaper/index.html）。

脆 **16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20件の脆弱性を含む合計113件の脆弱性を修正した。
"Oracle Critical Patch Update Advisory - July 2014"（http://www.oracle.com/technetwork/jp/topics/ojkbcpujul2014-2244696-ja.html）。

他 **16日**：IPAは、標的型攻撃を受けた組織に対する被害拡大と再発の抑止・低減、速やかな対策による連鎖の遮断などの支援を行うサイバーレスキュー隊を正式に発足した。
「プレス発表　標的型サイバー攻撃への対策支援『サイバーレスキュー隊』を発足」（https://www.ipa.go.jp/about/press/20140716_1.html）。

セ **17日**：通信教育企業の顧客情報が外部に漏えいした事件について、業務委託企業の元派遣社員が不正競争防止法違反（営業秘密の複製）の容疑で逮捕された。

セ **18日**：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は、インターネットバンキングに係るマルウェア（Game Over Zeus）の国際的な感染駆除作戦に関連し、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（ACTIVE）を通じて、該当マルウェアに感染している利用者への注意喚起を実施することを発表した。
「インターネットバンキングに係るマルウェア感染者に対する注意喚起について」（https://www.telecom-isac.jp/news/news20140718.html）。

他 **22日**：インターネットの安定的な運用に関する協議会より、「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」の第３版が公開された。
「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン（第３版）」（http://www.jaipa.or.jp/other/mtcs/guideline_v3.pdf）。

他 **23日**：総務省は、行政機関及び独立行政法人などが保有するパーソナルデータについて、その特質を踏まえた調査・検討を行うため、「行政機関等が保有するパーソナルデータに関する研究会」を開催することを発表した。
「行政機関等が保有するパーソナルデータに関する研究会」（http://www.soumu.go.jp/main_sosiki/kenkyu/gyousei_personal/index.html）。

セ **24日**：欧州中央銀行は、Webサイトに侵入され、イベント登録者の電子メールアドレスなどの個人データが漏えいしたことを公表した。この事件は漏えいしたデータと引き換えに金銭を要求する匿名のメールが届いたことから発覚した。
詳細については次の欧州中央銀行の発表を参照のこと。"24 July 2014 - ECB announces theft of contact information"（https://www.ecb.europa.eu/press/pr/date/2014/html/pr140724.en.html）。

セ **25日**：国内の複数の企業や行政機関より、自サイトのホームページを模倣したWebサイトに対する注意喚起が相次いで行われた。

脆 **29日**：複数のIPカメラに認証回避の脆弱性があり、認証情報を含む機器の設定内容が取得された上で任意の操作が実行される可能性があり、修正された。
JVN、「JVNDB-2014-000087　アイ・オー・データ機器製の複数の IP カメラにおける認証回避の脆弱性」（http://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-000087.html）。

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

※日付は日本標準時

編集ソフトのサポートサイトで発生したWeb改ざん事件では、アクセスしたユーザが別サイトに誘導されて不正なソフトウェアのインストールが行われただけでなく、事件発覚後に正規のアップデートファイルのコンテンツが改ざんされ、ウイルスを含んだファイルを利用者にアップデートファイルとしてインストールさせようとしていたことも判明しています。このような、正規ソフトウェアのアップデートの仕組みを悪用したマルウェアの感染活動は今後も継続すると考えられます。

■ 動静や歴史的背景による攻撃

この期間では毎年、太平洋戦争の歴史的日付や、竹島や尖閣諸島などに関連したインシデントが発生しています。本年もこれらに関連した日本国内の複数の政府機関や民間企業のWebサイトに対し、SQLインジェクションや、ブルートフォースなどによる侵入による改ざんやDDoS攻撃が発生すると予測されたため、警戒を行いました。しかし、一部でSQLインジェクション攻撃などの不正なアクセスが増加していたり[*10]、Webサイトの改ざんが確認されていますが[*11]、大規模な攻撃の発生は確認されませんでした。IIJの観測では、DDoS攻撃が平常時よりも若干多く見られましたが、攻撃の規模や回数は過去の同期間に比べるとかなり減少しています。

■ 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。8月にはLizard Squadを名乗る何者かによるPSNやXbox LIVE、League of Legendsなど複数のゲームサーバに対する攻撃が発生しています。PSNの事件では263.35GbpsのNTPリフレクション攻撃を受けたとされています。更に、この事件ではDDoS攻撃だけでなく、役員が搭乗していた航空機に爆発物を仕掛けたなどの発言を犯人がオンライン上で行ったことから、実際に搭乗していた航空機の運航に支障が出るなどの影響がありました。この攻撃者によると思われるゲーム関連サーバに対する攻撃は、9月に入っても断続的に発生しています。日本では、5月末に複数のISPにおいて、DNSサーバに対する断続的なDDoS攻撃が発生していますが、一部のISPに対しては7月に入っても継続しています。また、3月に海外のDDoS攻撃の代行サービスを利用して、ゲームサーバに対する攻撃を行ったとして、9月に電子計算機損壊等業務妨害容疑で高校生が書類送検されました。

■ 企業におけるマルウェア感染と情報漏えい

この期間、企業のシステムがマルウェア感染したこと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。特に米国では、8月に物流大手企業で、国内の51ヵ所の代理店でマルウェア感染が確認され、顧客のクレジットカード情報などが流出した可能性があることが発表されています。日本でも航空会社で社内の端末へのマルウェア感染によって、顧客情報が外部に送信され漏えいした可能性のある事件などが発生しています。9月には、ホームセンター大手企業で、約5600万枚分の決済カード情報や電子メールアドレスが流出した可能性のある事件が発生しました。この事件では昨年から発生しているPOSシステムを狙ったマルウェアの亜種が使われたとされており、クレジットカードなどの情報が漏えいした可能性がありました。これ以外にも病院や小売り業者など複数の企業でマルウェアによる情報漏えい事件が発生しています。特に、POSマルウェアについては、昨年終わりごろより大規模な情報漏えい事件を複数回引き起こしており、US-CERTからも複数回注意喚起が行われています[*12]。新種のPOSマルウェアが継続して確認されていることから[*13]、今後も引き続き注意が必要です。

■ 政府機関の取り組み

政府機関のセキュリティ対策の動きとしては、政府の情報セキュリティ政策会議第40回会合が開催され、2013年度の我が国におけるサイバーセキュリティ全般の状況について、政府機関、重要インフラ事業者、各府省庁の関連施策の実施状況、関係資料などを1つに取りまとめた初めての年次報告書である「サイバーセキュリティ政策に係る年次報告（2013 年度）」や、各府省庁のサイバーセキュリティに

＊10 例えば、IBM社のTokyo SOC Reportでは特定の国からのSQLインジェクションなどの攻撃が増加傾向であることが報告されている。「柳条湖事件が起こった9月18日前後の攻撃動向について」（https://www-304.ibm.com/connections/blogs/tokyo-soc/?lang=ja ）。
＊11 Web改ざんについては次のエフセキュアブログなどを参照のこと。「9.18のサイバー攻撃に関して（追記）」（http://blog.f-secure.jp/archives/50734688.html）。
＊12 US-CERTでは、1月に"TA14-002A: Malware Targeting Point of Sale Systems" (www.us-cert.gov/ncas/alerts/TA14-002A)、8月に"Alert (TA14-212A) Backoff Point-of-Sale Malware"（https://www.us-cert.gov/ncas/alerts/TA14-212A）と、継続的に注意喚起を行っている。
＊13 例えば、トレンドマイクロ社のブログ「急増するPOSシステムへの攻撃とPOSマルウェアファミリ」（http://blog.trendmicro.co.jp/archives/9902）などを参照のこと。

8月のインシデント

1 セ **1日**：US-CERTは、POSシステムを対象とした新種の不正プログラムBackoffが確認されたとして、注意喚起を行った。
"Alert (TA14-212A) Backoff Point-of-Sale Malware"(https://www.us-cert.gov/ncas/alerts/TA14-212A)。

2 他 **1日**：Microsoft社は、アプリケーションの脆弱性を緩和するセキュリティツールであるEnhanced Mitigation Experience Toolkit(EMET)5.0を公開した。
詳細については次のTechNet Blogsなどを参照のこと。「EMET 5.0 公開しました」(http://blogs.technet.com/b/jpsecurity/archive/2014/08/01/emet-5-released.aspx)。

3

4 セ **2日**：Mozilla Developer Networkは、データベースダンプファイルが誤って公開状態になっていたことから、7万6千のMDNユーザのメールアドレスと4,000ユーザの暗号化されたパスワードが漏えいした可能性があることを公表した。
Mozilla Developer Network、「MDNデータベースの情報漏洩について」(http://www.mozilla.jp/blog/entry/10418/)。

5

6

7 セ **4日**：各国の政府機関が情報収集活動に利用しているとされる商用監視ソフトウェアFinSpy(FinFisher)について、提供元のGamma Internationalが不正アクセスを受け、40GBにもなる内部文書とソースコードが公開された。

8

9 セ **8日**：米国のセキュリティ企業より、2014年2月から5月にかけて、BGPハイジャックにより、仮想通貨のマイニングプールへのトラフィックを偽のマイニングプールに振り向ける攻撃が行われていたことが報告された。この攻撃では、19のISPが影響を受けたとされており、攻撃者は8万3000ドルの利益を得ていた可能性があることが指摘されている。
詳細については次のDell SecureWorksのブログを参照のこと。"BGP Hijacking for Cryptocurrency Profit"(http://www.secureworks.com/cyber-threat-intelligence/threats/bgp-hijacking-for-cryptocurrency-profit/)。

10

11

12 セ **12日**：米国で、インターネットの速度が低下したり、通信が不安定になるなどの現象が発生した。原因については、広報されたBGPの経路情報が、古いルータでBGPのルーティングテーブルの上限である512kを超えたためと考えられる。
詳細については例えば、次のBGPmon.netのブログを参照のこと。"What caused today's Internet hiccup"(http://www.bgpmon.net/what-caused-todays-internet-hiccup/)。

13

14

15 脆 **13日**：Microsoft社は、2014年8月のセキュリティ情報を公開し、MS14-043とMS14-051の2件の緊急と7件の重要な更新をリリースした。
「2014 年 8 月のマイクロソフト セキュリティ情報の概要」(https://technet.microsoft.com/ja-JP/library/security/ms14-aug)。

16 脆 **13日**：Adobe Flash Playerに、任意のコード実行の可能性がある複数の脆弱性が発見され、修正された。
「APSB14-18: Adobe Flash Player用のセキュリティアップデート公開」(http://helpx.adobe.com/jp/security/products/flash-player/apsb14-18.html)。

17 脆 **13日**：Adobe Reader及びAcrobatに、リモートから任意のコード実行の可能性がある脆弱性が発見され、修正された。
「APSB14-19: Adobe ReaderおよびAcrobat用セキュリティアップデート公開」(http://helpx.adobe.com/jp/security/products/reader/apsb14-19.html)。

18 セ **13日**：テキスト編集ソフトの日本語と簡体字中国語のサポートサイトが改ざんされ、利用者のユーザ名、パスワード、IPアドレスを盗もうとする痕跡が見つかったことが公表された。その後、8月18日に再度Webサイトが改ざんされ、当該シェアウェアの更新チェック機能を利用して悪意あるファイルがインストールされる事件も発生している。

19

20

21 脆 **15日**：Microsoft社は、2014年8月に修正をリリースしたMS14-045について、適用した場合には異常終了や起動失敗が発生する可能性があるとして、問題が発生していない場合でも、予防的処置としてこれらの更新プログラムをアンインストールすることを推奨すると発表した。
詳細については、次の日本のセキュリティチーム公式ブログによる解説も参照のこと「【リリース後に確認された問題】2014 年 8 月 13 日公開の更新プログラムの適用により問題が発生する場合がある」(http://blogs.technet.com/b/jpsecurity/archive/2014/08/16/2982791-knownissue3.aspx)。

22

23

24

25 セ **21日**：米国UPSは、国内の51ヵ所の代理店でマルウェア感染が確認され、顧客のクレジットカード情報などが流出した可能性があることを公表した。
詳細については次のUnited Parcel Service of America, Inc.の発表などを参照のこと。"The UPS Store, Inc. Notifies Customers Of Potential Data Compromise and Incident Resolution"(http://www.pressroom.ups.com/Press+Releases/Archive/2014/Q3/The+UPS+Store%2C+Inc.+Notifies+Customers+Of+Potential+Data+Compromise+and+Incident+Resolution)。

26

27

28 セ **25日**：何者かによって、PlayStation Network(PSN)及びSony Entertainment Network(SEN)へのDDOS攻撃が行われ、大規模な障害が発生した。
攻撃については、例えば次のPlayStation.Blogなどを参照のこと。"Update: PlayStation Network is Back Online"(http://blog.us.playstation.com/2014/08/24/playstation-network-update-2/)。

29

30

31 脆 **28日**：Microsoft社は、適用後に異常終了や起動失敗などの不具合が発生していたMS14-045について、修正を行い、再公開した。
「マイクロソフト セキュリティ情報 MS14-045 重要 カーネルモード ドライバーの脆弱性により、特権が昇格される (2984615)」(https://technet.microsoft.com/ja-jp/library/security/ms14-045.aspx)。

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

※日付は日本標準時

関する今年度の施策などを取りまとめた、「サイバーセキュリティ 2014」などが決定しています[*14]。

本年6月に公表された「パーソナルデータの利活用に関する制度改正大綱」を受け、行政機関及び独立行政法人などが保有するパーソナルデータについて、その特質を踏まえた調査・検討を行うため、「行政機関等が保有するパーソナルデータに関する研究会」が総務省にて開催されています。同じく総務省より、電気通信事業者が取り扱う位置情報について、通信の秘密や個人情報・プライバシーを適切に保護しながら、ビジネス利用も含めたその社会的利活用を促進するため、位置情報の取得、利用及び第三者提供時における適切な取り扱いについて取りまとめた「位置情報プライバシーレポート～位置情報に関するプライバシーの適切な保護と社会的利活用の両立に向けて～」も公表されています[*15]。

警察庁からは、平成26年度の警察白書が発表され、サイバー犯罪の検挙件数が過去最多を記録したことや、インターネットバンキングに係る不正送金事犯が急増していることなどが記載されています。また、サイバー空間の脅威に対する官民の連携の推進を進めているなどの取り組みについても解説されています。

■ その他

6月より対策活動が実施されている、オンラインバンキングなどの情報窃取を行うマルウェアであるGameOver Zeusについて[*16]、7月には本作戦で得られた該当マルウェアの感染端末に関する情報を元に、ISP事業者に対し、感染者に関する情報提供とそれを用いた注意喚起が実施されることが発表されています[*17]。また、このような国際的なサイバー犯罪に対処するため、9月には欧州刑事警察機構(Europol)が、欧州や米国、カナダなどを含む複数国によるJoint Cybercrime Action Taskforce(J-CAT)を発足させるなど[*18]、国際的な連携の枠組みの構築も進められています。

7月には、様々な団体や企業から模倣したWebサイトについての注意喚起が行われました[*19]。8月に入ってから、政府機関でも同様の事例について注意喚起が行われています。これらの事例は特定の企業や団体などを狙ったものではなく、Webプロキシサービスによるものと考えられます。同様の事例としては、昨年中国の携帯電話事業者が提供していたWebページの変換サービス用プロキシによる事例がありますが[*20]。他にも同様のサービスを提供している場合が多くありますが、提供者がはっきりとしていないことも多いため、利用には注意が必要です[*21]。

同じく7月には、通信教育企業の顧客情報が漏えいした事件が明るみに出ました。これは別の企業が入手した名簿を元にダイレクトメールを送っていたことで判明したものです。情報漏えいした企業の業務委託企業の元派遣社員が不正に持ち出して名簿業者などに販売していたとして、不正競争防止法違反(営業秘密の複製)罪で逮捕されています。

電気通信事業者がDoS攻撃などの大量通信を識別し、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大量通信等への対処と通信の秘密に関するガイドライン」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[*22]。これは、総務省で行われていた、電気通信事

＊14 内閣官房情報セキュリティセンター、「情報セキュリティ政策会議　第40回会合(平成26年7月10日)」(http://www.nisc.go.jp/conference/seisaku/index.html#seisaku40)。
＊15 総務省、「緊急時等における位置情報の取扱いに関する検討会　報告書『位置情報プライバシーレポート～位置情報に関するプライバシーの適切な保護と社会的利活用の両立に向けて～』の公表」(http://www.soumu.go.jp/menu_news/s- news/01kiban08_02000144.html)。
＊16 Department of Justice、"U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator" (http://www.justice.gov/opa/pr/2014/June/14-crm-584.html)。
＊17 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、「インターネットバンキングに係るマルウェア感染者に対する注意喚起について」(https://www.telecom-isac.jp/news/news20140718.html)。
＊18 詳細については次のEuropolの発表を参照のこと。"EXPERT INTERNATIONAL CYBERCRIME TASKFORCE IS LAUNCHED TO TACKLE ONLINE CRIME" (https://www.europol.europa.eu/content/expert-international-cybercrime-taskforce-launched-tackle-online-crime)。
＊19 例えば、次の大阪府警察などの発表を参照のこと「緊急：大阪府警察ホームページを模倣したウェブサイトにご注意！」(http://www.police.pref.osaka.jp/15topics/caution_domain.html)。
＊20 例えば、次のJPCERTコーディネーションセンターのつぶやき(https://twitter.com/jpcert/status/322282948554530816)を参照のこと。
＊21 この事例については次のトレンドマイクロ社のブログ『プロキシ回避システム』がもたらした『模倣サイト』の混乱、その事例から学ぶ教訓とは?」(http://blog.trendmicro.co.jp/archives/9713)なども参照のこと。
＊22 インターネットの安定的な運用に関する協議会は電気通信事業関連の5つの業界団体により構成されている。このガイドラインの策定については次を参照のこと。社団法人日本インターネットプロバイダー協会(JAIPA)「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドラインの改定について」(http://www.jaipa.or.jp/topics/?p=695)。

9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

セ **1日**：米国で、ハリウッド女優などのプライベート写真が、掲示板に掲載される事件が発生した。この事件は、流出した複数の著名人のiCloudアカウントに不正アクセスが行われたことが原因とされている。
調査を実施したApple社は次の発表を行っている。"Apple Media Advisory Update to Celebrity Photo Investigation"（http://www.apple.com/pr/library/2014/09/02Apple-Media-Advisory.html）。

他 **1日**：総務省より、平成25年度に発生した電気通信事故の報告状況を取りまとめた「電気通信サービスの事故発生状況（平成25年度）」が公表された。
「電気通信サービスの事故発生状況（平成25年度）」（http://www.soumu.go.jp/menu_news/s-news/01kiban05_02000072.html）。

セ **3日**：米国の小売り大手であるHome Depotで大規模なカード情報の流出が発生した。
詳細については、次のThe Home Depot社の発表を参照のこと。"The Home Depot Reports Findings in Payment Data Breach Investigation"（https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf）。

他 **4日**：警察庁は、平成26年上半期のインターネットバンキングに係る不正送金事犯の発生状況を公表した。被害金額が平成25年下半期に続き、増加していることや、対象が地方銀行や信用金庫、信用組合に拡大していること、法人名義の口座に対する被害が急増していることなどが挙げられている。
「平成26年上半期のインターネットバンキングに係る不正送金事犯の発生状況について」（http://www.npa.go.jp/cyber/pdf/H260904_banking.pdf）。

脆 **10日**：Microsoft社は、2014年9月のセキュリティ情報を公開し、MS14-052の緊急と3件の重要な更新をリリースした。
「2014年9月のマイクロソフト セキュリティ情報の概要」（https://technet.microsoft.com/ja-JP/library/security/ms14-sep）。

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発見され、修正された。
「APSB14-21: Adobe Flash Player用のセキュリティアップデート公開」（http://helpx.adobe.com/jp/security/products/flash-player/apsb14-21.html）。

他 **11日**：警察庁は、平成26年上半期のサイバー犯罪の傾向などをまとめた「平成26年上半期のサイバー空間をめぐる脅威の情勢について」を公表した。
「平成26年上半期のサイバー空間をめぐる脅威の情勢について」（http://www.npa.go.jp/kanbou/cybersecurity/H26_kami_jousei.pdf）。

脆 **17日**：Adobe Reader及びAcrobatに、不正終了や、リモートから任意のコード実行の可能性がある脆弱性が発見され、修正された。
「APSB14-20：Adobe ReaderおよびAcrobat用セキュリティアップデート公開」（http://helpx.adobe.com/jp/security/products/reader/apsb14-20.html）。

セ **18日**：ゲームサーバにDDoS攻撃を複数回行い、ゲーム会社の業務を妨害したとして高校生が電子計算機損壊等業務妨害容疑で書類送検された。

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

他 **22日**：LINE株式会社は、多発しているLINEアカウントの乗っ取り被害を抑止する対策の1つとして、スマートフォン版LINEアプリでPINコード（4桁の番号）の設定を必須とする措置を講じた。
詳細については次のLINE公式ブログ「【重要】不正ログイン（乗っ取り）の被害拡大を防ぐため、PINコードの設定を必須にします」（http://official-blog.line.me/ja/archives/1009539887.html）を参照のこと。

セ **24日**：航空会社でマルウェア感染による不正アクセスが発生し、最大で73万件の会員の個人情報が漏えいした可能性があることが公表された。

脆 **25日**：Bashにリモートから任意のコード実行が可能な脆弱性が見つかり、修正された。その後、修正が不十分なことが判明したことから、複数の脆弱性が改めて修正されている。
JVN、「JVNVU#97219505 GNU BashにOSコマンドインジェクションの脆弱性」（http://jvn.jp/vu/JVNVU97219505/）。

脆 **26日**：大手クラウドプロバイダが未公開のXenの脆弱性を理由に大規模なメンテナンスの実施を行い話題となった。10月2日になり、CVE-2014-7188への対応だったことが公表された。
詳細については次のXen Project Blogなどを参照のこと。"XSA-108: Additional Information from the Xen Project"（https://blog.xenproject.org/2014/10/02/xsa-108-additional-information-from-the-xen-project-2/）。

セ **26日**：物流事業者のサポートサイトへパスワードリスト攻撃と考えられる不正ログインがあり、一部の会員の個人情報が閲覧されることで漏えいした可能性があることが公表された。
同様の事件は28日に別の物流事業者のサポートサイトでも発生している。

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

※日付は日本標準時

業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の「第一次とりまとめ」が4月に公表されたこと[*23]を踏まえて追加修正を行ったもので、DNSアンプ攻撃などの新たな脅威への対応が図られています。

また、9月初旬から10月にかけて、国内の複数の組織で利用していた.comドメインがDNSハイジャックを受け、不正なソフトウェアのインストールを試みる事件が発生しました[*24]。この事件では、レジストリに登録されたネームサーバ情報をなんらかの方法で書き換え、攻撃者が用意した偽のWebサイトに誘導していたことから、JPCERT/CCやJPRSより注意喚起が行われています[*25]。

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、状況により多岐にわたります。しかし、攻撃の多くは、脆弱性などの高度な知識を利用したものではなく、多量の通信を発生させて通信回線を埋めたり、サーバの処理を過負荷にしたりすることでサービスの妨害を狙ったものになっています。

■ 直接観測による状況

図-2に、2014年7月から9月の期間にIIJ DDoSプロテクションサービスで取り扱ったDDoS攻撃の状況を示します。

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

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

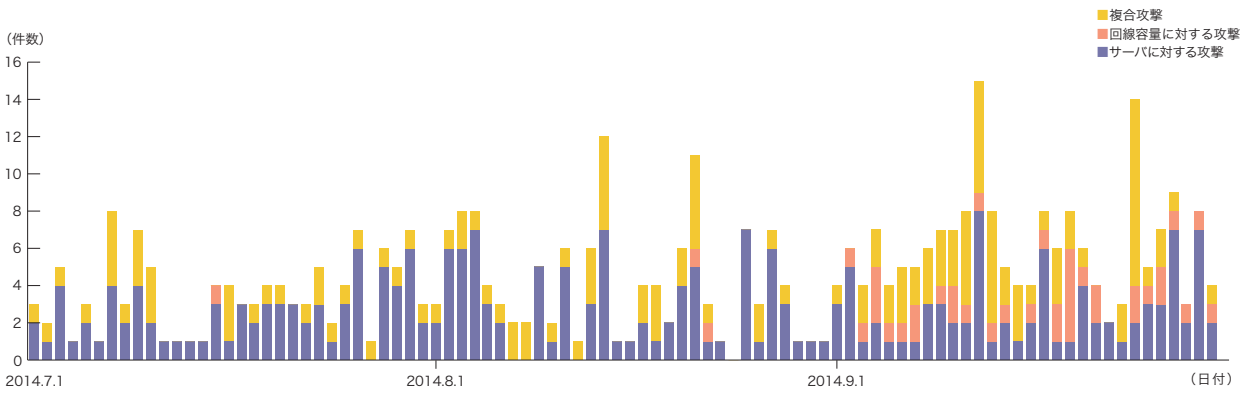


図-2 DDoS攻撃の発生件数

*23 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一次とりまとめ』及び意見募集の結果の公表」（http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000074.html）。

*24 Volexity Blog、"Democracy in Hong Kong Under Attack"（http://www.volexity.com/blog/?p=33）。

*25 株式会社日本レジストリサービス（JPRS）、「（緊急）登録情報の不正書き換えによるドメイン名ハイジャックとその対策について（2014年11月5日公開）」（http://jprs.jp/tech/security/2014-11-05-unauthorized-update-of-registration-information.html）。

量に対する攻撃[*26]、サーバに対する攻撃[*27]、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、340件のDDoS攻撃に対処しました。1日あたりの対処件数は3.7件で、平均発生件数は前回のレポート期間と比べて減少しました。DDoS攻撃全体に占める割合は、サーバに対する攻撃が71.5%、複合攻撃が16.8%、回線容量に対する攻撃が11.8%でした。

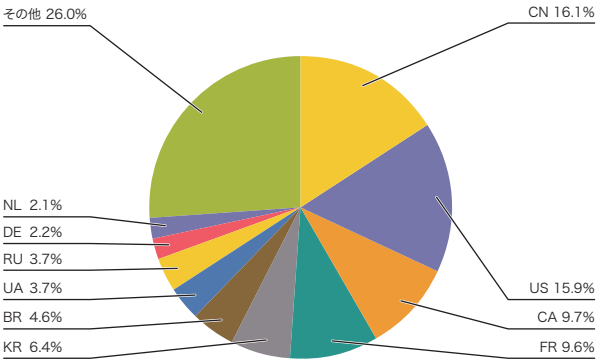


図-3 DDoS攻撃のbackscatter観測による攻撃先の国別分類

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48万6千ppsのパケットによって4.88Gbps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90.9%が攻撃開始から30分未満で終了し、9.1%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ありませんでした。なお、今回もっとも長く継続した攻撃は、複合攻撃に分類されるもので17時間36分にわたりました。

また、毎年この期間では、歴史的日付の前後でDDoS攻撃が多く見られます。9月に入ってからDDoS攻撃が増加しており、攻撃の傾向も変化が見られましたが、組織的な攻撃ではないことから、関連は確認できませんでした。

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[*28]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[*29]の利用によるものと考えられます。

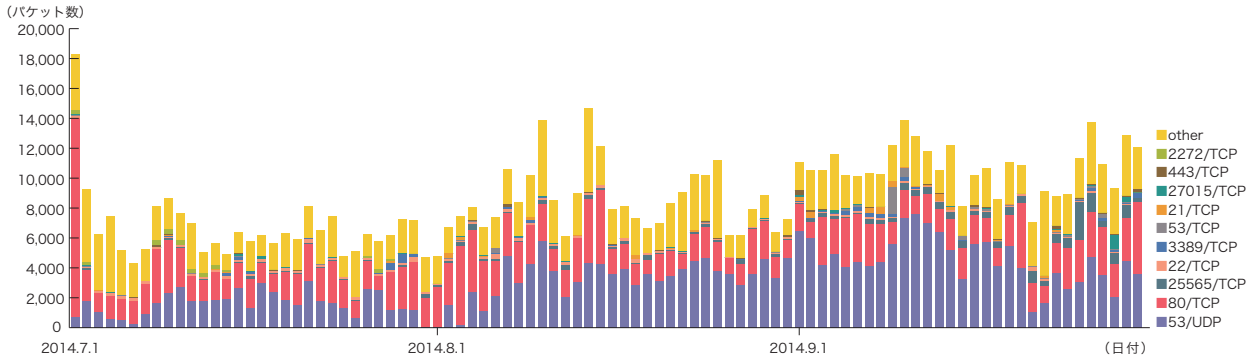


図-4 DDoS攻撃によるbackscatter観測（観測パケット数、ポート別推移）

＊26 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。

＊27 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。

＊28 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。

＊29 ボットとは、感染後に外部のC&Cサーバからの命令を受けて攻撃を実行するマルウェアの一種。ボットが多数集まって構成されたネットワークをボットネットと呼ぶ。

■ backscatterによる観測

次に、IIJでのマルウェア活動観測プロジェクトMITFのハニーポット[*30]によるDDoS攻撃のbackscatter観測結果を示します[*31]。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。

2014年7月から9月の間に観測したbackscatterについて、発信元IPアドレスの国別分類を図-3に、ポート別のパケット数推移を図-4にそれぞれ示します。

観測されたDDoS攻撃の対象ポートのうち最も多かったものはDNSで利用される53/UDPで、対象期間における全パケット数の36.2%を占めています。次いでWebサービスで利用される80/TCPが27.3%を占めており、上位2つで全体の63.5%に達しています。またDNSに利用される53/TCP、SSHで利用される22/TCP、リモートデスクトップで利用される3389/TCP、FTPで利用される21/TCP、HTTPSで利用される443/TCPへの攻撃、通常は利用されない25565/TCPや27015/TCP、2272/TCPなどへの攻撃が観測されています。

今年2月から増加傾向にある53/UDPのbackscatterは、今回の期間も増加を続け、観測パケット数の最も多いポートになりました。これらのパケットのほとんどは「DNS水責め攻撃(Water Torture)[*32]」と呼ばれる攻撃手法の特徴を持っています。また、観測されたパケットの発信元アドレスは広範にわたっています。

特に多くのbackscatterを観測した場合について、攻撃先のポート別にみると、Webサーバ(80/TCP)への攻撃としては、7月23日から8月15日にかけてウクライナのテレビ局、7月1日から24日にかけてロシアのホスティング事業者のサーバに対する攻撃をそれぞれ観測しています。特に後者は前回対象期間中の6月16日から攻撃が継続しています。また、9月に入って25565/TCPへの攻撃が多く観測されています。このポートは、特定のゲームのサーバで使われることがあります。攻撃対象は広範にわたっており、ロシアのホスティング事業者が持つ複数のサーバが攻撃される様子などが観測されています。9月9日から10日にかけて、パキスタンのドメインである.pkゾーンを担う複数のDNSサーバに対するDNS(53/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、7月から8月初めにかけてAnonymousによる複数のイスラエル政府関連サイトへの攻撃を観測しています。

1.3.2 マルウェアの活動

ここでは、IIJが実施しているマルウェアの活動観測プロジェクトMITF[*33]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[*34]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。

*30 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。
*31 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。
*32 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)。
*33 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。
*34 脆弱性のエミュレーションなどの手法で、攻撃を受けつけて被害に遭ったふりをし、攻撃者の行為やマルウェアの活動目的を記録する装置。

■ 無作為通信の状況

2014年7月から9月の期間中に、ハニーポットに到着した通信の発信元IPアドレスの国別分類を図-5に、その総量（到着パケット数）の推移を図-6に、それぞれ示します。MITFでは、数多くのハニーポットを用いて観測を行っていますが、ここでは1台あたりの平均を取り、到着したパケットの種類（上位10種類）ごとに推移を示しています。また、この観測では、MSRPCへの攻撃のような特定のポートに複数回の接続を伴う攻撃は、複数のTCP接続を1回の攻撃と数えるように補正しています。

ハニーポットに到着した通信の多くは、Microsoft社のOSで利用されているTCPポートに対する探索行為でした。また、同社のSQL Serverで利用される1433/TCP、SSHで利用される22/TCP、DNSで利用される53/UDP、Telnetで利用される23/TCP、HTTP Proxyで用いられる8080/TCPに対する探査行為も観測されています。

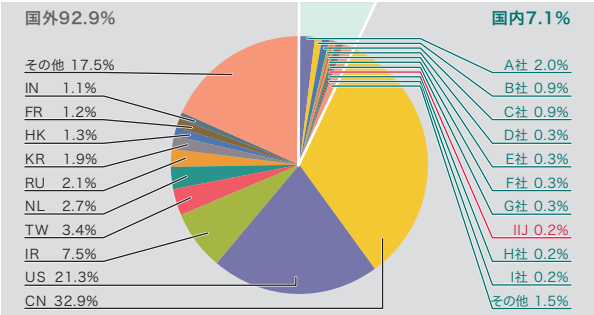


図-5 発信元の分布（国別分類、全期間）

期間中、7月27日、8月14日、9月12日に53/UDPの通信が大量に発生しています。これらのパケットのほとんどはbackscatterによる観測でも触れた「DNS水責め攻撃（Water Torture）」のパケットを受信したためです[*35]。主に米国、カナダ、中国などに割り当てられた大量のIPアドレスから各ハニーポットに対して1回から数回程度の少ない回数の問い合わせが行われています。この傾向から、攻撃者はボットネットなどを使ったと推測されます。問い合わせ内容は「ランダム文字列.実在するドメイン」のAレコードの解決要求でした。また9月8日にイランに割り当てられた1つのIPアドレスから、特定のハニーポットのIPアドレスに対して3395/UDPに対する通信が行われています。この通信の調査を行ったところ、長さは数十から数百バイトのランダムなデータが送信されていました。

■ ネットワーク上でのマルウェアの活動

同じ期間中でのマルウェアの検体取得元の分布を図-7に、マルウェアの総取得検体数の推移を図-8に、そのうちのユニーク検体数の推移を図-9にそれぞれ示します。このうち図-8と図-9では、1日あたりに取得した検体[*36]の総数を総取得検体数、検体の種類をハッシュ値[*37]で分類したものをユニーク検体数としています。また、検体をウイルス対策ソフトで判別し、上位10種類の内訳をマルウェア名称別に色分けして示しています。なお、図-8と図-9は前回同様に複数のウイルス対策ソフトウェアの検出名によりConficker判定を行いConfickerと認められたデータを除いて集計しています。

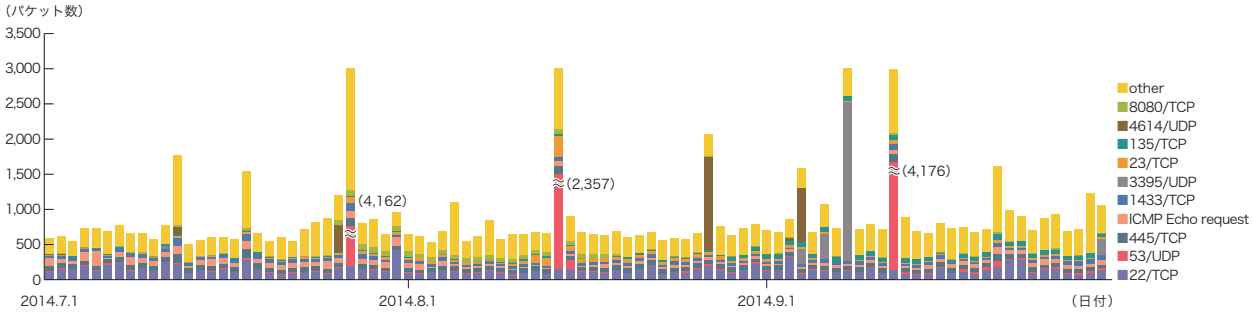


図-6 ハニーポットに到着した通信の推移（日別・宛先ポート別・1台あたり）

＊35 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。
＊36 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。
＊37 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93、ユニーク検体数が20でした。未検出の検体をより詳しく調査した結果、シンガポールとフィリピンに割り当てられたIPアドレスからパスワードを盗み出すマルウェアなどが観測されました。また、未検出の検体の約54%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96.0%、ダウンローダ型4.0%でした。また解析により、1個のボットネットC&Cサーバ[*38]と16個のマルウェア配布サイトの存在を確認しました。

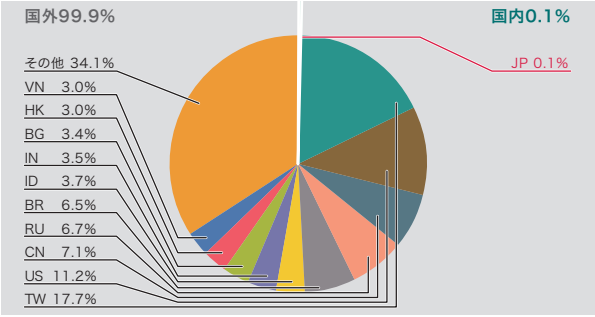


図-7 検体取得元の分布(国別分類、全期間、Confickerを除く)

■ 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25,435、ユニーク検体数は672でした。短期間での増減を繰り返しながらも、総取得検体数で99.6%、ユニーク検体数で97.0%を占めています。このように、今回の対象期間でも支配的な状況が変わらないことから、Confickerを含む図は省略しています。本レポート期間中の総取得検体数は前回の対象期間と比較し、約20%減少

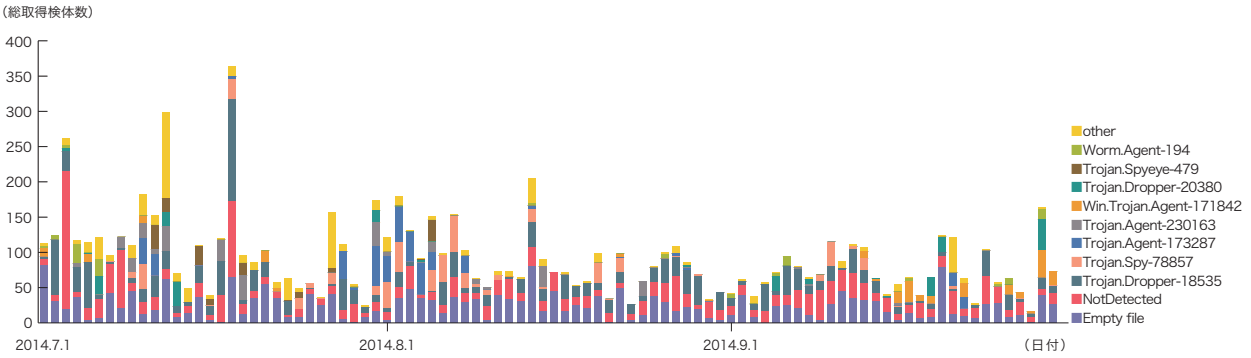


図-8 総取得検体数の推移(Confickerを除く)

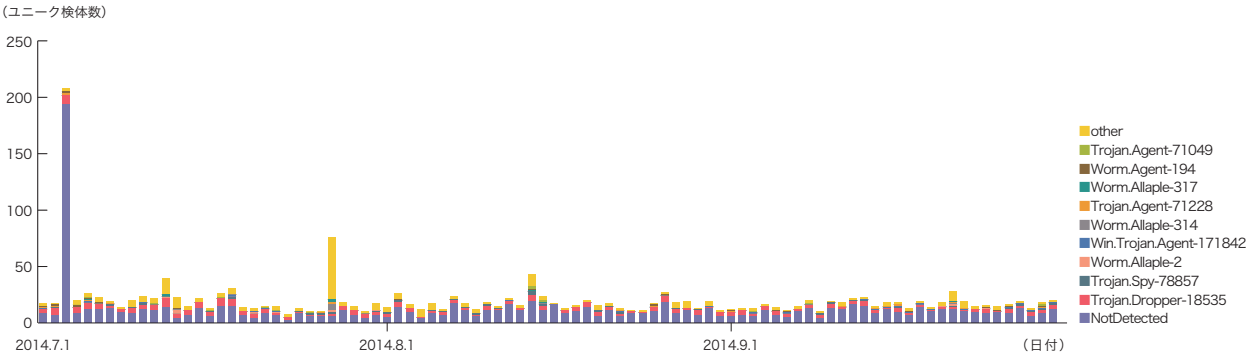


図-9 ユニーク検体数の推移(Confickerを除く)

*38 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。

しています。また、ユニーク検体数は前号から約7%減少しました。Conficker Working Groupの観測記録[*39]によると、2014年9月30日現在で、ユニークIPアドレスの総数は1,026,417とされています。2011年11月の約320万台と比較すると、約32%に減少したことになりますが、依然として大規模に感染し続けていることが分かります。

1.3.3 SQLインジェクション攻撃

IIJでは、Webサーバに対する攻撃のうち、SQLインジェクション攻撃[*40]について継続して調査を行っています。SQLインジェクション攻撃は、過去にも度々流行し話題となった攻撃です。SQLインジェクション攻撃には、データを盗むための試み、データベースサーバに過負荷を起こすための試み、コンテンツ書き換えの試みの3つがあることが分かっています。

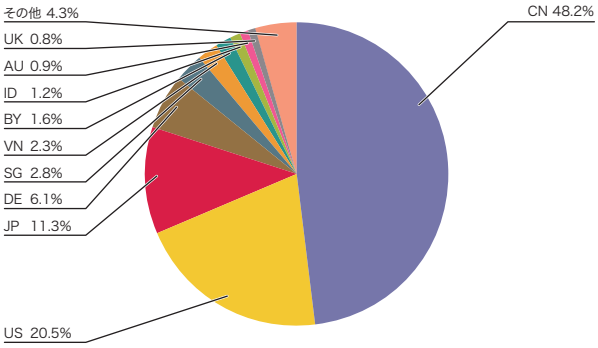


図-10 SQLインジェクション攻撃の発信元の分布

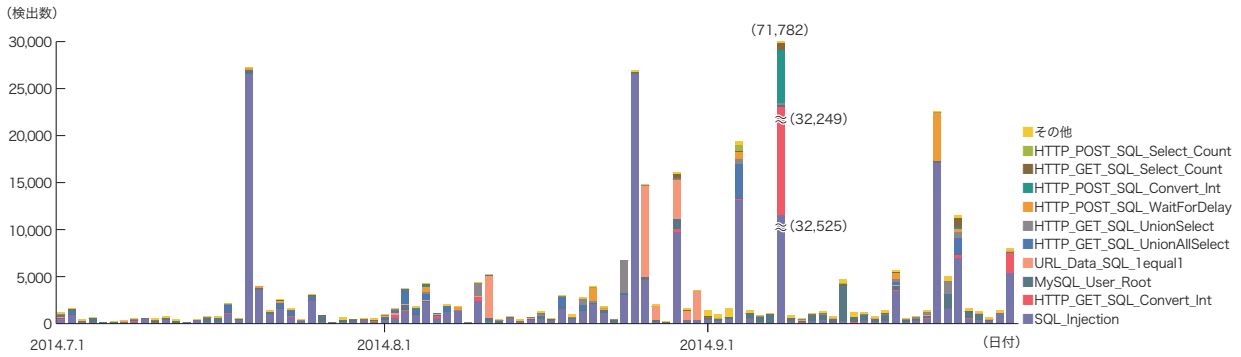


図-11 SQLインジェクション攻撃の推移(日別、攻撃種類別)

2014年7月から9月までに検知した、Webサーバに対するSQLインジェクション攻撃の発信元の分布を図-10に、攻撃の推移を図-11にそれぞれ示します。これらは、IIJマネージドIPSサービスのシグネチャによる攻撃の検出結果をまとめたものです。

発信元の分布では、中国48.2%、米国20.5%、日本11.3%となり、以下その他の国々が続いています。Webサーバに対するSQLインジェクション攻撃の発生件数は前回に比べて大幅に増加しました。これは中国を発信元とする攻撃が大幅に増えたためです。

この期間中、7月19日には、中国の特定の攻撃元より特定の攻撃先に対する攻撃が発生しています。8月25日には米国の複数の攻撃元より、特定の攻撃先に対する攻撃が発生しています。9月8日には中国の特定の攻撃元より、特定の攻撃先への大規模な攻撃が発生していました。9月23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した。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。

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

*40 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[*41]。このWebクローラは国内の著名サイトや人気サイトなどを中心とした数万のWebサイトを日次で巡回しており、更に巡回対象を順次追加しています。また、一時的にアクセス数が増加したWebサイトなどを対象に、一時的な観測も行っています。一般的な国内ユーザによる閲覧頻度が高いと考えられるWebサイトを巡回調査することで、改ざんサイトの増減や悪用される脆弱性、配布されるマルウェアなどの傾向が推測しやすくなります。

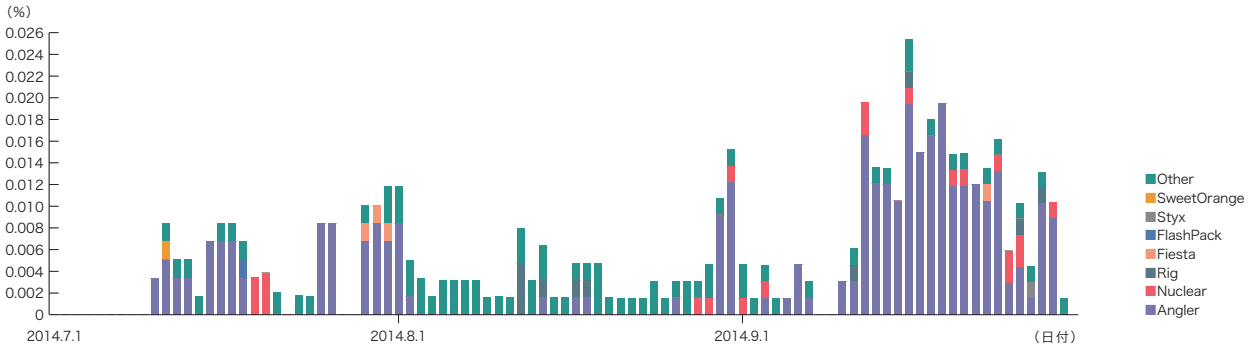
2014年7月から9月の期間は、4月から6月の期間に比べると、約2倍程度の頻度でドライブバイダウンロードが観測されています（図-12）。攻撃の内訳は、前期間と同じくAngler及びNuclearによる攻撃が多くを占めており、これらのExploit Kitは、いずれもJavaやFlash、Silverlightなどのプラグインの脆弱性を悪用する機能を備えています。特にAnglerは精力的に機能追加が行われており、8月下旬には感染時にクライアントのディスク上にマルウェアファイルを保存させないことでアンチウイルスソフトウェアによる検知の回避を試みる仕組みが確認されました[*42]。

また、9月中旬にWebクローラシステムの攻撃検出ロジックを一部改良したところ、Anglerの観測数が急増しました。このことから、一時的にAnglerが消滅しているように見える8月中も、実は同Exploit Kitによる攻撃が継続していた可能性が高いと推測されます。

新たな傾向として、8月中旬ごろから、Rigが観測され始めました。これは比較的新しいExploit Kitで、前述のAngler、Nuclearと同じくJavaやFlash、Silverlightの脆弱性を攻撃する機能を備えており、有償のサービスとして提供されています[*43]。なお、Rigによる攻撃が観測された一部のケースでは、1ヵ所の誘導元Webサイトから複数のExploit Kitへの誘導が観測されました。

一方、改ざんされ、誘導元となっているWebサイトに関しては、比較的知名度の低いWebサイトなどで、2〜4週間程度改ざんされた状態が継続するケースが多数確認されており、改ざん原因の調査や根本的な対策が行われていないケースが後を絶たない状況であることが窺えます。

全体として、ドライブバイダウンロードの発生率が増加傾向となっているものと推測される状況です。Webサイト運営者はWebコンテンツの改ざん対策、閲覧者側はブラウザや関連プラグインなどの脆弱性対策を徹底し、注意を継続することを推奨します。



※調査対象は日本国内の数万サイト。近年のドライブバイダウンロードは、クライアントのシステム環境やセッション情報、送信元アドレスの属性、攻撃回数などのノルマ達成状況などによって攻撃内容や攻撃の有無が変わるよう設定されているため、試行環境や状況によって大きく異なる結果が得られる場合がある。
※7月1日〜7月7日はWebクローラを停止していたため、攻撃を検知していない。

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

*41 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。

*42 同機能については、Malware don't need Coffee「Angler EK : now capable of "fileless" infection (memory malware)」（http://malware.dontneedcoffee.com/2014/08/angler-ek-now-capable-of-fileless.html）で詳解されている。

*43 Rigについては、Kahu Security「RIG Exploit Pack」（http://www.kahusecurity.com/2014/rig-exploit-pack/）で詳解されている。

1.4 フォーカスリサーチ

インターネット上で発生するインシデントは、その種類や規模が時々刻々と変化しています。このため、IIJでは、流行したインシデントについて独自の調査や解析を続けることで対策につなげています。ここでは、これまでに実施した調査のうち、Bashの脆弱性Shellshockについて、POODLE attack、リスト型攻撃の発生状況と対策の3つのテーマについて紹介します。

1.4.1 Bashの脆弱性Shellshockについて

■ Shellshockとは

この脆弱性CVE-2014-6271[*44]は、2014年9月24日にBash[*45]の対策バージョンと共に公開されました。脆弱性の影響としてはリモートから任意のコード実行が可能です。Bashは通常ローカルで使用されるシェルプログラムであるため、リモートからの攻撃とは無縁と思われがちですが、その影響が明らかになるにつれて大きな騒ぎになりました。

脆弱性公開と同時に対策バージョンがリリースされましたが、公開後から約1週間で、関連する複数の新しい脆弱性が立て続けに公開されました。表-1が関連する脆弱性の一覧です。CVE-2014-7169[*46]は元々の修正が不十分であったとして新しい脆弱性として登録されました。CVE-2014-7186[*47]、CVE-2014-7187[*48]は修正の過程で発見された脆弱性です。CVE-2014-6277[*49]、CVE-2014-6278[*50]はパッチがアップストリームに取り込まれる過程で作り込まれました。Shellshockによる攻撃を防ぐためには、これらの脆弱性すべてに対応する必要があります。

■ 脆弱性への対応

Bashはシェルプログラムという性質上、サーバプログラムやスクリプト言語のインタープリタなどとは異なり、最新版の機能が必要とされる機会はあまりありません。そのため、多くの場合で各ディストリビューションの提供するバイナリパッケージを使用しています。Shellshockには複数の脆弱性が関連していますが、アップストリームに取り込まれた修正のみ影響を受ける脆弱性もあるため、適用されているパッチの状態により対応が必要な脆弱性は異なります。

ディストリビューションの例として、CentOS[*51]の各種リリースにおける各脆弱性の対応状況を表-2に示します。CVE-2014-6271の対策版において、修正が不十分であった点は他と変わりませんが、それ以降の脆弱性においては同時に対応し、アップストリームの修正に起因するCVE-2014-6277、CVE-2014-6278については影響を受けていません。

表-1 Shellshock関連脆弱性一覧

CVE ID	公開日時	影響	備考
CVE-2014-6271	2014年9月24日	任意コード実行	発端となる脆弱性
CVE-2014-7169	2014年9月25日	任意コード実行	CVE-2014-6271の修正不十分に起因
CVE-2014-7186	2014年9月26日	DoS	-
CVE-2014-7187	2014年9月26日	DoS	-
CVE-2014-6277	2014年9月27日	DoS	アップストリーム版の修正に起因
CVE-2014-6278	2014年9月27日	任意コード実行	アップストリーム版の修正に起因

表-2 CentOS各リリースにおける対策版bashパッケージ

CVE ID	CentOS5系	CentOS6系	CentOS7系
CVE-2014-6271	bash-3.2-33.el5.1	bash-4.1.2-15.el6_5.1	bash-4.2.45-5.el7_0.2
CVE-2014-7169	bash-3.2-33.el5_10.4	bash-4.1.2-15.el6_5.2	bash-4.2.45-5.el7_0.4
CVE-2014-7186			
CVE-2014-7187			
CVE-2014-6277	対策不要	対策不要	対策不要
CVE-2014-6278	対策不要	対策不要	対策不要

*44 CVE-2014-6271 bash：specially-crafted environment variables can be used to inject shell commands（https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2014-6271）。
*45 GNU Bash：The GNU Bourne-Again SHell（http://www.gnu.org/software/bash/）。
*46 CVE-2014-7169 bash：code execution via specially-crafted environment Incomplete fix for CVE-2014-6271（https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2014-7169）。
*47 CVE-2014-7186 bash：parser can allow out-of-bounds memory access while handling redir_stack（https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2014-7186）。
*48 CVE-2014-7187 bash：off-by-one error in deeply nested flow control constructs（https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2014-7187）。
*49 CVE-2014-6277 bash：uninitialized here document closing delimiter pointer use（https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2014-6277）。
*50 CVE-2014-6278 bash：incorrect parsing of function definitions with nested command substitutions（https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2014-6278）。
*51 CentOS Project（http://www.centos.org/）。

これはCentOSの元となるRed Hat Enterprise Linux[*52]がBashの最新版へのアップデートではなく、ベースとなるパッケージに対して、脆弱性を修正するパッチを当てて対応しているためです。他のディストリビューションにおいても同様に、修正方法により影響有無が分かれています。

■ 脆弱性の影響

ローカルシェルとして使用されるBashにおける脆弱性が、何故リモートから悪用可能な脆弱性へ発展したのでしょうか。今回の脆弱性は、特定の環境変数の値が設定された状態において、Bashプログラムが起動されると影響を受けるというものです。Bashがシェル関連の呼び出しで使われる/bin/shを兼ねている環境もあり、こちらも同様の影響を受けます。

実際にこの脆弱性を用いた攻撃は既に観測されており、最も狙われている箇所はCGI[*53]です。分かりやすい影響例として、Webサーバ上で動作するBashで書かれたCGIプログラムがありますが、実際の環境においてはほぼ利用されていないと考えられます。しかしながら、他の言語で作られたCGIプログラムであったとしても、内部的にシェルに依存しているために影響を受ける場合があります。

また、アプライアンス製品や組み込み機器の制御OSとしてもLinuxが多く採用されています。身近な物としてはロードバランサ、ホームルータ、ファイルサーバなどが挙げられます。これらにもBashが組み込まれていたり、管理画面においてCGIが使われていたりと、普通のUNIXサーバ同様の影響を受けてしまう場合もあります。これらを踏まえて、今回の脆弱性の影響を理解するにあたり、UNIX環境におけるプログラムの実行と、CGIの処理の流れについて説明します。

■ UNIX環境におけるプログラム実行

UNIX環境においては、Windows環境とは異なり完全新規のプロセスを作成することができず、親プロセスの複製(fork)を経て、子プロセスを実行対象のプロセスへ変化(exec)させる手順を辿ります。最終的には子プロセスは実行対象のプログラムへと変化して親プロセスとは別物になりますが、複製を経由するため一部のデータが引き継がれます。図-13にこの処理の流れを示します。

変化する際に呼び出すexec関数には表-3に示すとおり複数の種類があり、今回の脆弱性において鍵となる環境変数の扱いが異なっています。呼び出し時に明示的に環境変数を指定しないexec関数においては、親プロセスから子プロセスに引き継がれた環境変数が、そのまま実行対象のプロセスへ変化した後も使用されます。

■ CGIの処理の流れ

CGIはWebサーバ経由で動的コンテンツを提供する仕組みです。Webアプリケーションフレームワークの普及に伴い、以前よりは少なくなっていますが依然として使われています。WebサーバはHTTP経由で受け取ったヘッダを、環境変数へ展開してCGIプログラムを起動します。この仕様が今回の脆弱性において、CGIが最も影響を受けやすい箇所となっている理由です。CGIプログラムとして直接Bashが起動されない限り、この時点では影響を受けません。ですが、

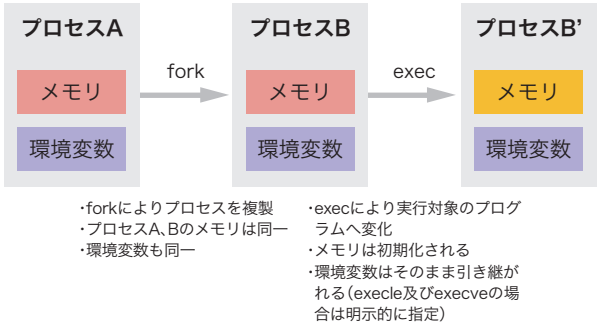


図-13 UNIX環境における外部プログラム実行

表-3 exec系関数の動作

関数名	環境変数の扱い
execl	引き継ぐ
execle	明示的に指定
execlp	引き継ぐ
execv	引き継ぐ
execve	明示的に指定
execvp	引き継ぐ

*52 Red Hat Enterprise Linux(http://www.redhat.com/en/technologies/linux-platforms/enterprise-linux)。
*53 RFC3875 The Common Gateway Interface Version 1.1(http://www.ietf.org/rfc/rfc3875.txt)。

前述のとおり環境変数は子プロセスに引き継がれていくため、他の言語で書かれていたとしてもシェルを経由して外部プログラムを呼び出してしまうと、影響を受ける可能性があります。直接呼び出したプログラムに限らず、ライブラリやモジュールを経由して、間接的に呼び出されたプログラムであったとしても同様です。図-14にCGI経由のプログラム呼び出しにおける影響の有無を示します。

また、スクリプト言語においてはプログラムの記述方法により、意図せずにシェルが呼び出されてしまうこともあります。スクリプト言語の例としてPerl[*54]における動作を示したものが表-4です。このように、同一の関数による呼び出しであっても、引数次第で暗黙的にシェル経由の呼び出しへ展開されてしまいます。環境変数はすべて引き継がれていますので、シェル経由の呼び出しへ展開される場合は、今回の脆弱性の影響を受けます。

■ まとめ

これまで説明したように、Bashという一見リモートからの攻撃とは無縁に見えるプログラムの脆弱性であったとしても、利用のされ方により、外部からこの脆弱性狙った攻撃にさらされることになります。

このような影響条件は、ソースコードを元にした静的な調査などではすべての実行パスを網羅的に調査することは困難です。一方、Bashのアップデートはサーバプログラムなどとは異なり、多くの場合において再起動を必要としないため、少しでも影響が疑われる箇所であれば速やかに対策版へ更新することをお勧めします。

アプライアンス製品や組み込み機器については、ベンダーによるファームウェア修正が必要になります。対策版ファームウェアのリリースに時間がかかる製品もありますので、その場合は影響が疑われる箇所へのアクセスを制限するなどの暫定的な対策も有効です。

脆弱性への対策としては、回避策の適用、対策版への更新、セキュリティ装置による防御などの様々な手段があります。対象のシステム構成により、最適な対策は異なりますので、その都度判断して適切に対処することが重要です。

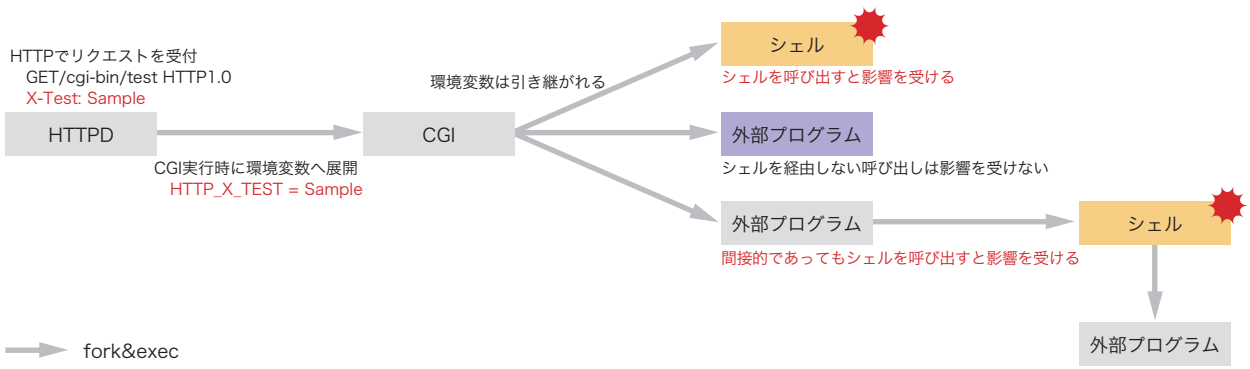


図-14 CGIにおける影響

表-4 Perlにおける外部プログラム呼び出し

Perlコード	exec関数への展開	シェル呼び出し	環境変数
`/bin/ls`	execvp("/bin/ls", ["/bin/ls"])	なし	引き継ぐ
`/bin/ls 2>/dev/null`	execl("/bin/sh", ["-c", "/bin/ls 2> /dev/null"])	あり	引き継ぐ
system("/bin/ls")	execvp("/bin/ls", ["/bin/ls"])	なし	引き継ぐ
system("/bin/ls &")	execl("/bin/sh", ["-c", "/bin/ls &"])	あり	引き継ぐ
open(FH, "/bin/ls |")	execvp("/bin/ls", ["/bin/ls"])	なし	引き継ぐ
open(FH, "/bin/ls 2>/dev/null |")	execl("/bin/sh", ["-c", "/bin/ls 2>/dev/null"])	あり	引き継ぐ

*54 The Perl Programming Language(https://www.perl.org/)。

1.4.2 POODLE attack

米国時間2014年10月14日に、Googleの研究チームからSSLv3[*55]への新たな攻撃が公開されました[*56]。POODLE attack(Padding Oracle On Downgraded Legacy Encryption attack)と呼ばれる本手法はBEAST攻撃[*57]に類似した中間者攻撃で、ブラウザから大量のリクエストをサーバに送りつけることによるトライ&エラーを繰り返すことでSSLで暗号化された攻撃対象データを1バイトずつ復号する攻撃手法です。現実的な被害としては、Cookieの搾取が挙げられています。なお本手法は一見TLSv1.0[*58]にも適用可能であるかのように見えますが、SSLv3.0とTLSv1.0のパディング手法の違いにより、TLSv1.0では現実的な攻撃にはなりません。一方でSSLv3.0では1バイトを盗み見るために最大255回のクエリをサーバに送りつけるだけで攻撃が可能となります。本節では、POODLE attackの技術的背景と本攻撃の現実性について取り上げます[*59]。

■ CBCモードの概要とCBCモードが持つ潜在的な脆弱性

POODLE attackはBEAST攻撃と同じく暗号モードとしてCBC(Cipher Block Chaining)モードが利用されたときのみ成功します。RC4をはじめとしたストリーム暗号は、鍵情報をもとに発生させたキーストリームを平文にXOR演算で足しこむことで暗号化を行う方式であり、任意長のデータを暗号化することができます。一方で、DESやAESなどのブロック暗号は定められた入力長(ブロック長:DESは64ビット、AESは128ビット)のデータを暗号化アルゴリズムに入力し、入力長と同じブロック長の暗号文を得る方式です。通常ブロック暗号を利用する際には、ブロック長よりもはるかに長いデータを暗号化しますので、何度も逐次的に暗号化アルゴリズムで暗号処理を行う必要があります。1つ前のブロック暗号処理で得られたデータを次のデータ処理でどのように利用するかを定めた方式のことを暗号モードと呼び、いくつもの方式が提案されています。図-15はその1つであるCBC暗号モード[*60]の概要を示しています。まず初期値としてブロック長のIV(Initial Vector)[*61]を用意します。平文をブロック長ごとに分割したときの最初のパートであるP_1にIVをXOR演算で足し合わせたデータに、実際のブロック暗号における暗号化処理を行い、その出力として暗号文C_1が得られます。次の平文パートP_2を暗号化するには、前のブロック暗号化処理で得られたC_1をXOR演算で足し合わせたデータを平文として入力して暗号化し、同様にC_2を得ます。このように$C_i = ENC(P_i \oplus C_{i-1})$という暗号化処理を繰り返すことで、平文全体の暗号化を計算します。逆に復号する際には$P_i = DEC(C_i) \oplus C_{i-1}$という復号処理を逐次的に繰り返すことで、平文を復元することができます。

この暗号化処理において、ブロック長でちょうど割り切れないデータを扱う場合にはパディング処理が必要となります。これは、平文の最後のパートがブロック長に満たない場合、何がしかのデータでブロック長になるように埋めてブロック暗号化処理が行えるようにする処理です。TLSではPKCS#5

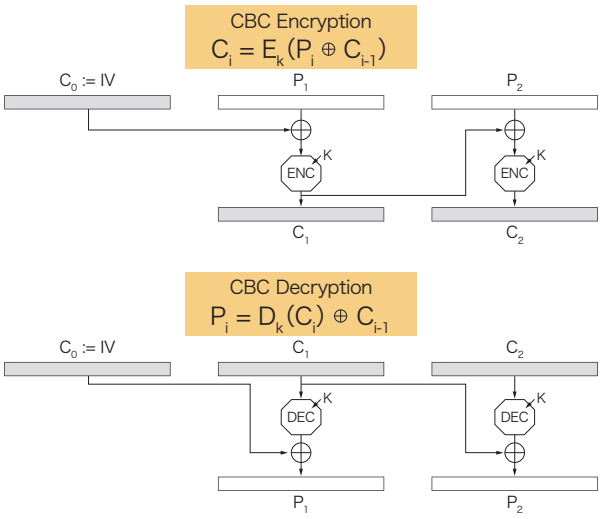


図-15 CBC暗号モードの概要

*55 IETF、"The SSL Protocol Version 3.0"(http://tools.ietf.org/html/rfc6101)。
*56 Bodo Möller, Thai Duong, Krzysztof Kotowicz, "This POODLE Bites: Exploiting The SSL 3.0 Fallback"(https://www.openssl.org/~bodo/ssl-poodle.pdf)。
*57 Thai Duong, Juliano Rizzo, "BEAST - Here Come The XOR Ninjas", 2011。
*58 IETF、"The TLS Protocol Version 1.0"(http://tools.ietf.org/html/rfc2246)。
*59 本節は技術的な解説に重きをおいている。POODLE attackの概要については、以下に示す暗号プロトコル評価技術コンソーシアムによる速報を参照のこと。SSLv3仕様そのものに対するPOODLE attackについて(https://www.cellos-consortium.org/jp/index.php?PoodleAttack_20141015_J)。
*60 NIST、"NIST Special Publication 800-38A Recommendation for Block Cipher Modes of Operation: Methods and Techniques"(http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf)。
*61 IV(Initial Vector)は秘密にする必要はない。ただし復号時には鍵と同様にIVが必要となる。

padding方式[*62]が採用されており、図-16はブロック長が8バイト（例えばDES）の場合のパディングの例を表しています。(a)はブロック長に満たすまでに3バイト足りないためパディングデータとして3バイト分を0x03で埋めます。同様に(b)は5バイト足りないため5バイト分を0x05で埋めています。(c)はちょうどブロック長の倍数のデータを暗号化しようとするケースですが、平文のどこまでパディングされていたかの境界を復号時に認識できるようにするために「8バイト分（ちょうどブロック長）足りない」ということにして当該ブロックのすべてを0x08で埋めていきます。

一方でSSLv3.0では異なるパディング方式が採用されており、この違いが今回のPOODLE attackを生み出すきっかけの1つとなってしまいました。図-17はPKCS#5 paddingとSSLv3 paddingの違いを示しています。SSLv3で採用されているパディング方式では、パディングする最終バイトをPKCS#5 padding方式と同様に「パディングするバイト長」とし、それ以外のパディングデータはランダムデータを埋めていくと定められています。不運なことに、SSLv3でもTLSでもこのパディングされるエリアは、通信路でデータが改ざんされていないことを示すデータであるMAC（Message Authentication Code）の対象範囲には入っていません。そのため、パディングデータを改ざんされたとしてもMACの検証では、改ざんを検知することができません。一方で、TLSにおいては上記説明したパディングデータの制約条件を用いて、パディング部分の改ざんを検知できる可能性はありますが、SSLv3では最終バイト以外のパディングデータを改ざんされたとしてもそれを検知することができません。POODLE attackはこのちょっとした隙間を狙った攻撃とも言えます。

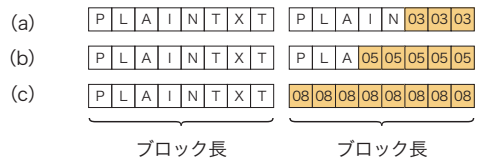
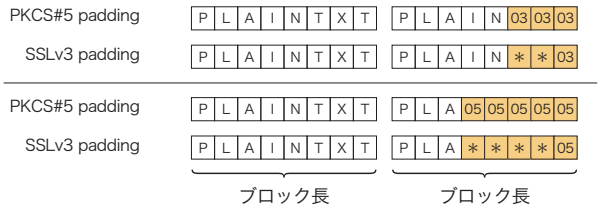


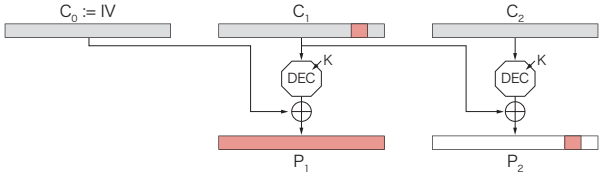
図-16 ブロック長が8バイトの場合のPKCS#5 paddingの例



※色付けされたパディングデータにおける*はランダムなデータであることを示している。

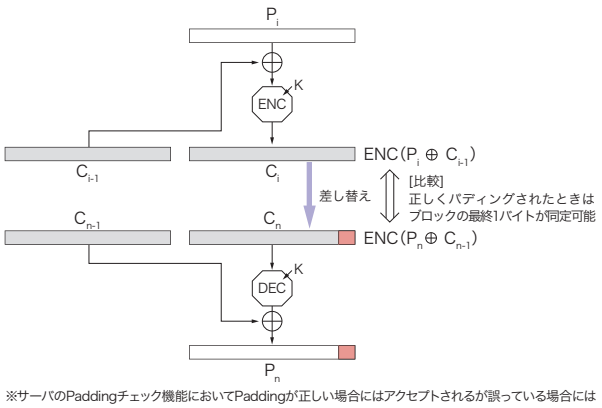
図-17 PKCS#5 paddingとSSLv3 paddingの違い

図-18はCBCモードを利用した復号時において、暗号文が改ざんされた場合の波及範囲を示しています。この図において暗号文C_1の一部を改ざんすることで平文P_1はブロック全体が変更されてしまいますが、平文P_2は攻撃者の意図する箇所を自由に変換することができます。図-19はこの特徴を用いたPadding Oracle Attack[*63]の原理を示しています。平文の長さが分かっているという前提でP_nまでのデータが暗号化されている場合、最後のブロックC_nを中間者が「攻撃対象」、つまり復号したいデータであるC_iに差し替えます。この



※暗号文の1バイトを改ざんして復号処理した場合には、当該ブロックの平文はブロック全体に渡って影響が及ぶが、次ブロックにおける平文において意図した箇所を改ざんすることが可能である。

図-18 CBCモードにおける暗号文が改ざんされた場合の波及範囲



※サーバのPaddingチェック機能においてPaddingが正しい場合にはアクセプトされるが誤っている場合にはエラーが返却される。

図-19 Padding Oracle Attackの原理

*62 IETF、"PKCS #5：Password-Based Cryptography Specification Version 2.0"（http://tools.ietf.org/html/rfc2898）。

*63 SSL/TLSだけでなくSSHやIPsecにおいても同様の攻撃が公開されてきた。いずれも仕様で定められた「データ形式の制約」に則っているかどうかを、サーバからのエラー情報を基に判定して暗号化データを復号する攻撃手法である。M.R. Albrecht, K.G. Paterson, G.J. Watson, Plaintext Recovery Attacks Against SSH, 30th IEEE Symposium on Security and Privacy, 2009.（http://www.isg.rhul.ac.uk/~kp/SandPfinal.pdf）。J.P. Degabriele and K.G. Paterson, On the (In)security of IPsec in MAC-then-Encrypt Configurations, Proceedings of the 17th ACM Conference on Computer and Communications Security, 2010.（http://portal.acm.org/citation.cfm?id=1866363）。

とき平文の長さが既知のため、パディングされたデータ長が格納されているP_nの最終バイトは既知となります。SSL/TLSサーバは手順どおりパディングチェックを行い、もし仕様で定められたパディング方式に則っていない場合にはエラーを返却します。このエラー返却機能(Padding Oracle)を使うと、サーバが暗号化データをアクセプトした場合、パディング部分には正しいデータが格納されていることを意味します。SSLv3においてはP_iの最終バイトとP_nの最終バイトが一致するときにアクセプトされますので、$P_i \oplus C_{i-1}$の最終バイトと$P_n \oplus C_{n-1}$の最終バイトが一致することからP_iの最終バイトを(暗号化鍵を知らなくても)復元することができます。実際には、MACによるチェックが入るためパディングデータよりも前の平文部分が改ざんされたことが検知できますので、うまくいかないことがほとんどです。しかし、今回POODLE attackで指摘されたように、うまくそのブロックがパディングデータのみで埋め尽くされる状態(図-16の(c)のような状態)にすることでMACの影響範囲を最終ブロックから外すことができます。このとき最終の1バイトが合致しているか試行すると256回に1度だけ必ずアクセプトされます。一方でTLSにおいては、図-16(c)のように、ブロックすべてのバイトが同じデータで埋め尽くされる必要があります。この例ではブロック長が8バイトですから、2^{64}回の試行で1度だけ成功します。またAESではブロック長が16バイトですから2^{128}回の試行が必要なことからも、TLSにおいてこの攻撃は現実的ではない潜在的な問題点としてみなされてきました。しかし、今回指摘されたPOODLE Attackでは、1バイトを復元するために2^8程度の計算で済むため、現実的な攻撃として認識されました。

■ POODLE attackの現実性

SSHにおいては、CBCモード以外にも利用可能な暗号モードの1つであるCTRモードが利用可能であったため、CBCモードの利用を取りやめることでPadding Oracle Attackを防ぐことができました。しかし、SSL/TLSにおいてはCTRモードの利用は仕様上定められていません。またSSLv3においては、仕様で規定されているCipherSuites(暗号アルゴリズム)において、輸出規制のためにかつて利用されていた40ビット鍵の強度しか持たないアルゴリズムやNULL(暗号化なし)以外のものでCBCモードを利用しないときにはRC4を使わざるを得ません。しかしRC4には昨年新たな攻撃手法が立て続けに公開されており[*64][*65]、もはやRC4も脆弱なアルゴリズムであると認識されています。

POODLE attackと同様にPadding Oracle Attackに分類されているBEAST攻撃は、SSLv3及びTLSv1.0にて成功可能であり、TLSv1.1にて仕様としてこの脆弱性を回避する設計がなされています。具体的には前セッションの暗号化データを次セッションのIVとして利用する際の潜在的問題を回避し、新たにIVを作り直す工程が入りました。またBEAST攻撃が存在しながらもSSLv3及びTLSv1.0が現在も利用されてきたのは、1/n-1分割法と呼ばれる対策方法が有効であることが知られているためです[*66]。この手法は主要ブラウザにおいて既に対策されていますが、POODLE attackに適用することはできません。今後、1/n-1分割法と同様にSSLv3の延命技術が考案される可能性はありますが、現時点ではSSLv3を安全に利用する方法が皆無となりました。

今回の攻撃に対する根本的な対策として、1)SSLv3を無効にする(クライアント、サーバのいずれか)、2)TLS_FALLBACK_SCSVの導入(クライアント、サーバ共に対策が必要)、の2つが挙げられています。1)に関しては、主要ブラウザは今後SSLv3を無効にするとアナウンスされました[*67][*68][*69]。また、ブラウザに自ら設定してSSLv3を無効化する方法も案内されています[*70][*71]。サーバサイドにおいてもSSLv3を無

*64 Takanori ISOBE, Toshihiro OHIGASHI, Yuhei WATANABE, and Masakatu MORII, "Full Plaintext Recovery Attack on Broadcast RC4,", Proc. the 20th International Workshop on Fast Software Encryption(FSE 2013), 2013.(Revised Selected Papers, LNCS 8424, pp.179-202, Springer-Verlag, 2014)。
*65 N.AlFardan, D.J.Bernstein, K.G.Paterson, B.Poettering, J.C.Schuldt, On the Security of RC4 in TLS, USENIX Security 2013.(http://dl.acm.org/citation.cfm?id=2534793)。
*66 ImperialViolet、"POODLE attacks on SSLv3(14 Oct 2014)"(https://www.imperialviolet.org/2014/10/14/poodle.html)。
*67 Mozilla Security Blog、"The POODLE Attack and the End of SSL 3.0"(https://blog.mozilla.org/security/2014/10/14/the-poodle-attack-and-the-end-of-ssl-3-0/)。
*68 Google Online Security Blog、"This POODLE bites: exploiting the SSL 3.0 fallback"(http://googleonlinesecurity.blogspot.jp/2014/10/this-poodle-bites-exploiting-ssl-30.html)。
*69 「マイクロソフト セキュリティ アドバイザリ 3009008, SSL 3.0の脆弱性により、情報漏えいが起こる」(https://technet.microsoft.com/ja-jp/library/security/3009008)。
*70 SANS ISC InfoSec Handlers Diary Blog、"OpenSSL:SSLv3 POODLE Vulnerability Official Release"(https://isc.sans.edu/diary/OpenSSL%3A+SSLv3+POODLE+Vulnerability+Official+Release/18827)。
71 mozillaZine、"Security.tls.version."(http://kb.mozillazine.org/Security.tls.version.*)。

効にする方法が共有されつつあります[*72]。一方でレガシーな製品、特にフィーチャーフォンやゲーム機器などにおいては対策が難しいと考えられます。そのためSSL/TLSサーバがSSLv3非対応になることで、これらの機器からサイトが閲覧できなくなるケースが考えられます。

2)はダウングレード攻撃[*73]を根本的に防ぐために提案されている方式です[*74]。この方式ではTLS_FALLBACK_SCSVというCipherSuiteとエラーコードinappropriate_fallbackが新たに追加されており、クライアントとサーバの両者共にこのSCSV(Signaling Cipher Suite Value)[*75]に対応している場合にのみ、ダウングレード攻撃を防ぐことができます。挙動は非常にシンプルでクライアントは自身が対応可能な最高バージョン以外でサーバに繋ぐときにはClientHelloメッセージのCipherSuitesに本SCSVを含むようにします。一方、本SCSVを含むCipherSuitesを受け取ったサーバは、クライアントが指定したプロトコルバージョンがサーバで対応している最も高いバージョンより低い場合にはエラーを返します。これらの挙動により潜在的なダウングレード攻撃を回避することができます。現在はTLS WGでLast callというステータスのドラフトですが、今年2月よりGoogleサーバとChrome(バージョン33以降)にて本SCSVが実装されています。また10月15日に公開されたOpenSSLでもこのSCSVが実装されました。更にFirefoxも対応することが予定されており[*76]、今後サーバ・クライアント双方で利用が広がる見込みです。しかしこの対策はサーバ・クライアントの双方で対応しない限りPOODLE attackを防ぐことはできません。フィーチャーフォンなどのレガシーな環境において、この対策が浸透するとは考えられず、今後の潜在的な攻撃に備えて実装されている、と捉えることもできるでしょう。

POODLE attackの前提条件としてブラウザから大量にリクエストを発生させ、かつそのリクエストを経路上で一部書き換える(攻撃対象の暗号化データに差し替える)必要があることから、BEAST攻撃と同様に一般的な利用環境では容易に攻撃可能とは一概には言えません。しかし、今回はプロトコル仕様自体の問題であり、回避が難しいことからSSLv3はSSLv2と同様に脆弱なバージョンとして捉え、今後利用すべきではないと考えられます。実際Twitterなどのいくつかのサービスにおいて SSLv3無効化を行ったとのアナウンスが即座になされました[*77][*78]。

TLS仕様はTLSv1.0だけでなくBEAST攻撃に対処したTLSv1.1、より安全なハッシュ関数のSHA-256、SHA-384やCBC以外の暗号モードGCM、CCMに対応したTLSv1.2が規格化され、広く実装されています。更にTLSv1.3[*79]も現在TLS WGにおいて検討されています。暗号モードとしてCBCを除外するなどの検討がなされており、最新のプロトコルバージョンを利用することで安全に利用できる仕組みが整いつつあります。かつては安全と認識され広く利用されていたDESやMD5などの暗号アルゴリズムが危殆化[*80]し利用停止されたように、暗号プロトコルについても過去のバージョンを捨て速やかに新しいバージョンに移行していく必要があります。その際には、後方互換性(バージョンアップすることで繋がらなくなるSSLクライアントの比率)と安全性(対策の緊急度)のバランスを見ながら対応していくことが必要になります。

---

*72 F5 Networks、"CVE-2014-3566:Removing SSLv3 from BIG-IP"(https://devcentral.f5.com/articles/cve-2014-3566-removing-sslv3-from-big-ip)。

*73 意図的に古いプロトコルバージョンで接続させる中間者攻撃。ClientHelloにてクライアントが対応しているバージョンを明示する箇所があり、この部分をSSLv2であると指定することにより、意図せず弱い暗号アルゴリズムを利用させることができる。SSLv2ではこのメッセージはMACなどで守られていないためダウングレード攻撃の根本的な解決方法はなくSSLv2は脆弱なバージョンと認識されている。

*74 IETF、"TLS Fallback Signaling Cipher Suite Value(SCSV) for Preventing Protocol Downgrade Attacks"(https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv)。当初personalな提案だったドラフト(https://tools.ietf.org/html/draft-bmoeller-tls-downgrade-scsv)が現在TLS WG預かりに昇格していることが分かる。

*75 本来CipherSuiteはSSL/TLSで用いられる暗号アルゴリズムの組を示す2バイトデータであるが、2009年に発覚したRenegotiation機能の問題に対処するためにRFC5746(http://tools.ietf.org/html/rfc5746)で導入されたTLS_EMPTY_RENEGOTIATION_INFO_SCSVと同様、本来とは異なる用途で別の意味を持たせる拡張が行われている。

*76 http://www.ietf.org/mail-archive/web/tls/current/msg13905.html

*77 https://twitter.com/twittersecurity/status/522190947782643712

*78 CloudFlare blog、"SSLv3 Support Disabled By Default Due to POODLE Vulnerability"(https://blog.cloudflare.com/sslv3-support-disabled-by-default-due-to-vulnerability/)。

*79 The Transport Layer Security(TLS)Protocol Version 1.3(https://tools.ietf.org/html/draft-ietf-tls-tls13)。ディスカッションはhttps://github.com/tlswg/tls13-specを参照のこと。

*80 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。

1.4.3 リスト型攻撃の発生状況と対策

■ リスト型攻撃とは

昨年から様々なオンラインサービス(以下、サービス)において、リスト型攻撃またはリスト型アカウントハッキングと呼ばれる攻撃手法を用いた不正アクセスが頻発しています。リスト型攻撃とは、攻撃者がログインIDとパスワードを組み合わせたリストを用いて、サービスのログインを連続的に試行する攻撃です。攻撃に利用されるリストは、攻撃対象とは異なるサービスから流出した情報から作成されています。複数のサービスでログインIDとパスワードを使い回すユーザが多い[*81]ことから、攻撃者はリストを利用して攻撃しているのです。

攻撃者がログインに成功しても、サービス提供者からは一見して、正規ユーザであるか否かを判別することは難しく、攻撃者は対策が行われる前に目的を達成することができます。ユーザがログインIDとパスワードの使い回しをしているサービスが多い程、ユーザの被害が大きくなってしまいます。

■ 他のログイン試行攻撃との違い

ログイン試行の攻撃手法としては、特定のログインIDに対して、様々なパスワードを試してみるブルートフォース攻撃や、パスワードとしてよく使われる単語やフレーズを試してみる辞書攻撃がよく知られています。リスト型攻撃では、試されるログインIDとパスワードの組み合わせが、あらかじめ決まっているという点がこれらの攻撃とは異なります。

■ 2014年のリスト型攻撃の発生状況

表-5は2014年1月1日から9月30日の間にリスト型攻撃として公表されたインシデントをまとめたものです。ほぼ毎月どこかのサービスがリスト型攻撃を受け、不正にログインされていることが分かります。金銭的被害も9件発生しており、クレジットカードで大量のチケットを購入し、換金する事例や、友人の名を騙ってメッセージを送り、ポイントカードを購入させる事例、他にもサービス独自のポイントをギフト券などへ不正に交換する事例などが発生しています。リスト型攻撃の発見の契機については、サービス提供者による発見数13件、ユーザによる発見数9件となっています。サービス提供者自身もリスト型攻撃に気がついていない状況が多くあることが窺えます。

■ オンラインサービスにおけるリスト型攻撃対策

最後にサービス提供者側とユーザ側、それぞれのリスト型攻撃への対策を以下に説明します[*82]。ただし、サービスを提供／利用する上での対策ですので、社内向けシステムなどには当てはまらない箇所もあります。

■ サービス提供者側のリスト型攻撃対策

サービス提供者側の主な対策は、(1)認証機能設計・実装の改善、(2)システム監視・運用の改善、(3)ユーザアクティビティ監視・通知機能の提供の3つです。なお、対策にあたって、ユーザに過度の負担を強いないような実装を考えなければなりません。

(1)の対策はログインID及びパスワード設定の改善やパスワード以外の認証機能の提供を行います。ログインIDとパスワードの使い回し防止のため、システムにポリシーに基づいたログインIDとパスワードを自動生成させることを検討してください。これにより、他サービスからのログインIDとパスワードの使い回しを防ぐことができます[*83]。ユーザに自由なパスワード設定を許容する場合、「弱いパスワード[*84]を受け付けない」「ログインIDとパスワードの使い回しをしないよう明示する」といった対策が必要となります。

その上で、使い回しをするユーザが必ずいることを想定し、多段階認証や多要素認証(ハードウェアトークンやICカード)で補強することを検討しなければなりません。この実装にはシステム改修が必要な場合があります。

---

*81 IPAとJPCERT/CCから公表された「STOP!! パスワード使い回し!! パスワードリスト攻撃による不正ログイン防止に向けた呼びかけ」(https://www.jpcert.or.jp/pr/2014/pr140004.html)の中で、金銭に関連したサービスサイトと同一のパスワードを使い回している人の割合が約4分の1(25.4%)であることが指摘されている。

*82 サービス提供者向けとして、総務省からも「リスト型アカウントハッキングによる不正ログインへの対応方策について」(http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000063.html)が公表されている。

*83 サービス提供者が生成したログインIDとパスワードを、ユーザが他のサービスに利用することを技術的に防ぐことは困難であるため、ユーザに対し他のサービスに利用しないように提示する必要がある。

*84 「password」や「123456」、「ユーザの名前や住所、生年月日」など推測しやすいものや、それらの組み合わせは弱いパスワードとして設定できないようにしなければならない。

また、自社のシステムの脆弱性などにより情報が漏えいする可能性もないとは言い切れません。自社からログインIDやパスワードが漏えいした場合に備え、攻撃者が認証情報を手に入れても、リスト型攻撃に利用することが困難になるような対策が必要になります。パスワードを保存する際は、平文保存や単純なハッシュ化ではなく、ソルトを追加したパスワードにストレッチングを施したハッシュ化を行うことで、パスワードを現実的な時間で解析できなくなります。自社で実装することが困難な場合、外部の組織が提供する認証機能を利用することもできます。しかし、外部が提供する認証システムに対して攻撃が行われるといったリスクも考慮しなければなりません。

(2)は攻撃の事前・事後に備えた対策です。リスト型攻撃が行われた際、平常時と比べて、「システムの負荷が高い」「ログイン失敗の回数が多い」「存在しないログインIDに対するログイン試行が多数行われている」「特定のIPアドレスからのログイン試行が異常に多く、ログインIDが毎回異なる」「平常時とは異なるIPアドレスブロックからアクセスが行われている」といった兆候が見られる場合があります。

このような兆候を検知して、管理者への通知や攻撃元IPアドレス自動遮断、アカウントロックするようなシステムを検討してください[*85]。また、長期間利用がないアカウントを削除することでリスト型攻撃による被害を未然に防ぐことができます。

表-5 2014年に発生したリスト型攻撃による事件

公表日	サービス分類	サービス提供者	期間	不正ログイン試行回数	不正ログイン件数	発見契機	金銭的被害	主な対策
1月24日	通信関連サービス	A社	1月16日	不明	165件	不明	なし	①②③⑤⑬
2月24日	ブログサービス	B社	不明	不明	不明	サービス提供者	不正なポイント交換	⑥⑯⑱
2月25日	SNS	C社	2月5日〜2月11日	不明	370件	ユーザ	なし	①⑥
2月28日	SNS	C社	2月28日	不明	16,972件	不明	なし	①⑤⑦⑬⑱
2月28日	通信関連サービス	D社	2月24日〜25日	約1万5,000回	344件	サービス提供者	不正なコンテンツ購入	②③④⑤⑦⑩⑬
3月16日	ポイント関連サービス	E社	3月16日〜3月17日	約94万回	約1万9,000件	サービス提供者	なし	④⑤⑦⑨⑬
4月23日	会員サイト	F社	3月23日〜4月21日	460万回以上	78,361件	サービス提供者	なし	③⑤⑦⑧⑨⑬⑭
4月30日	通信関連サービス	D社	4月14日〜4月28日	不明	724件	サービス提供者	不正なコンテンツ購入	②③④⑤⑦⑩⑬
5月2日	ポイント関連サービス	G社	4月19日〜4月29日	不明	273件	ユーザ	不正なポイント交換	②④⑦⑨
5月30日	通販サービス	H社	2013年9月〜2014年3月	不明	不明	不明	不正なコンテンツ購入	⑲
6月10日	動画サービス	I社	5月27日〜6月4日	2,203,590回	219,926件	ユーザ	不正なポイント交換	⑬⑰
6月12日	SNS	J社	不明	不明	303件	ユーザ	ポイントカード購入	③⑥
6月17日	SNS	C社	5月30日〜6月17日	約430万回	263,596件	ユーザ	なし	①③⑥⑬⑮
6月20日	ブログサービス	B社	6月16日〜6月19日	約160万回	2,398件	ユーザ	なし	⑫⑬
6月23日	ブログサービス	K社	6月19日〜6月23日	2,293,543回	38,280件	サービス提供者	なし	⑬
6月26日	アンケートサービス	L社	6月23日〜6月24日	不明	最大11,502件	ユーザ	不正なポイント交換	①③⑰
6月30日	ゲーム関連	M社	6月28日〜6月29日	1,796,629回	14,399件	サービス提供者	なし	③⑭
7月1日	広告サービス	N社	2013年8月ごろから不定期に発生	不明	不明	不明	不明	⑦
7月4日	アンケートサービス	O社	6月25日	3,420,000回	15,092件	サービス提供者	不正なポイント交換	③⑤⑬
7月4日	ゲーム関連	P社	不明	不明	不明	ユーザ	不明	⑤⑧
8月13日	通販サービス	Q社	8月7日〜8月12日	4,220,382回	20,957件	不明	なし	⑬
8月18日	ポイント関連サービス	E社	8月15日	約296,000回	756件	サービス提供者	なし	⑬
8月27日	ゲーム関連	P社	不明	不明	不明	ユーザ	不明	⑤⑧⑪
9月11日	運輸サービス	R社	9月10日〜9月11日	約1,152万回	約21,000件	サービス提供者	なし	⑤⑦⑧⑨⑬
9月23日	通販サービス	Q社	9月22日〜9月23日	18,663回	19件	不明	なし	⑬
9月26日	運輸サービス	S社	9月25日〜9月26日	約19万回	10,589件	サービス提供者	なし	①⑤⑦⑧⑨⑬
9月29日	運輸サービス	T社	不明	不明	34,161件	サービス提供者	なし	①⑤⑦⑧⑨⑬
9月30日	通信関連サービス	U社	9月27日〜9月29日	約225万回	6,072件	サービス提供者	なし	①⑤⑦⑧⑨⑪⑭

① 攻撃元IPアドレス遮断
② 検知システムの強化
③ 認証機能の強化
④ 監視体制の強化
⑤ 全ユーザにパスワード使い回し禁止を通知
⑥ 全ユーザにパスワード変更依頼
⑦ 全ユーザに定期的なパスワード変更依頼
⑧ 全ユーザに過去に使用したパスワード禁止を通知
⑨ 全ユーザに推測が容易なパスワード禁止を通知
⑩ 全ユーザにフィッシングサイトへの注意を通知
⑪ 全ユーザに2段階認証の利用推奨を通知
⑫ 不正ログインされたユーザを強制ログアウト
⑬ 不正ログインされたユーザをパスワードリセット／変更依頼
⑭ 不正ログインされたユーザのアカウントをロック
⑮ 休眠アカウントをロック
⑯ システムの改修
⑰ 一部システムの停止
⑱ 不正な書き込みの削除
⑲ 警察へ捜査協力

*85 このような兆候は現在の攻撃傾向を反映した結果であるため、今後は傾向が変わる可能性がある。最新の攻撃傾向を情報収集し、それに合わせた観点で監視を行う必要がある。また、兆候の把握やそれを基にした自動遮断など、通信の秘密に対する適法性については、「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 第一次とりまとめ(http://www.soumu.go.jp/main_content/000283608.pdf)」の「第4節 SMTP認証の情報を悪用したスパムメールへの対処」や「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン(http://www.jaipa.or.jp/other/mtcs/guideline_v3.pdf)」の「(4)SMTP認証の情報を悪用した迷惑メールへの対処」などを参照のこと。

不正ログインが発覚した場合、被害の拡大防止と調査のため、サービスの停止を検討してください。不正ログインされたアカウントのパスワードは、再び不正ログインされないように、パスワードリセットなどで変更しなければなりません。また、念のため、今回、不正ログインの対象となっていないアカウントのパスワードを変更することも検討してください。

(3)は重要な処理の際にユーザにアラートを通知する機能です。ログイン成功・失敗時や個人情報の閲覧・変更時、購入決済処理などの完了時にメールなどでユーザに通知することで、ユーザ自身が不正アクセスに気付くことができます。また、ログイン履歴や購入履歴を確認できる機能を提供することで、いつ頃から不正アクセスが起きているのか把握することができます。

■ ユーザ側のリスト型攻撃対策

ユーザが自分でパスワードを設定する場合、パスワード管理ソフトウェアを使用して、サービスごとに異なるパスワードを生成・管理するのが最も効果的です。Webベースのサービスの場合、Webブラウザにパスワード生成ツールで作成したパスワードを記憶させる方法もあります[*86]が、Webブラウザに起因するリスクに対応するため、マスターパスワードは必ず設定し[*87]、常に最新バージョンのWebブラウザを使用してください。

サービスが2段階認証を提供している場合は必ず使用するようにします。また、サービスの通知機能を有効にし、身に覚えのない利用通知がサービスから届いた場合は早急にパスワードを変更して、金銭的被害が発生していないか確認し、サービスの運営に連絡しましょう。また、使用する予定がなくなったサービスのアカウントは削除するようにしましょう。

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、Bashの脆弱性Shellshockについて、POODLE attack、リスト型攻撃の発生状況と対策についてまとめました。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。このような側面についてご理解いただき、必要な対策を講じた上で、安全かつ安心してインターネットを利用できるように努力を継続して参ります。

執筆者:

齋藤 衛(さいとう まもる)
IIJ サービスオペレーション本部 セキュリティ情報統括室 室長。法人向けセキュリティサービス開発などに従事の後、2001年よりIIJグループの緊急対応チーム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)
小林 直(1.4.1 Bashの脆弱性Shellshockについて)
須賀 祐治(1.4.2 POODLE attack)
小林 稔(1.4.3 リスト型攻撃の発生状況と対策)
IIJ サービスオペレーション本部 セキュリティ情報統括室

協力:
加藤 雅彦、根岸 征史、春山 敬宏、桃井 康成 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

*86 Webブラウザで管理する場合、マルウェアに感染したときにパスワードが窃取される可能性があるが、多数の複雑なパスワードを身近なツールで管理できるという点において、現実的な手段の1つとして考えることができる。

*87 Firefoxはマスターパスワードを設定することができる。その他の主要なWebブラウザ(Internet Explorer、Google Chrome、Safari)では、OSなどのセキュリティ機構を使用してパスワードが自動的に暗号化されて保存される。