S.S.R.C.定期
トレンドレポート
Vol.33

株式会社　日立システムズ

セキュリティリサーチセンタ

S.S.R.C.トレンドトレポート Vol.33

目次

1. はじめに

S.S.R.C.(Shield Security Research Center)は、株式会社日立システムズ　セキュリティリサーチセンタが運営するセキュリティ情報公開サイトです。本サイトでは、セキュリティリサーチセンタによるリサーチ結果を随時配信しております。

本文書は、株式会社日立システムズ、SHIELD セキュリティセンタで日々収集を行っている世界中のセキュリティトレンド情報にもとづき、セキュリティリサーチセンタのセキュリティアナリストが、月ごとでのセキュリティトレンドの動向をまとめたレポートです。

次に示す、ご利用条件を十分にお読み頂き、ご了承頂いた上でご利用頂きます様、よろしくお願い致します。

2. ご利用条件

本文書内の文章等すべての情報掲載に当たりまして、株式会社日立システムズ(以下、「当社」といいます。）と致しましても細心の注意を払っておりますが、その内容に誤りや欠陥があった場合にも、いかなる保証もするものではありません。本文書をご利用いただいたことにより生じた損害につきましても、当社は一切責任を負いかねます。

本文書に掲載されている情報は、掲載した時点での情報です。掲載した時点以降に変更される場合もありますので、あらかじめご了承ください。

3.

3.1. セキュリティトレンド情報

当期間確認された情報セキュリティに関する情報は以下の通りです。

1. Microsoft

関連記事	● 2017 年 7 月のセキュリティ更新プログラム（月例） https://blogs.technet.microsoft.com/jpsecurity/2017/07/12/201707-security-bulletin/ (Microsoft) ● Outlook の脆弱性を修正するセキュリティ更新プログラムを定例外で公開 https://blogs.technet.microsoft.com/jpsecurity/2017/07/28/outlookoobrelease/ (Technet) ● 2017 年 8 月のセキュリティ更新プログラム（月例） https://blogs.technet.microsoft.com/jpsecurity/2017/08/09/201708-security-bulletin/ (Microsoft) ● 既知の Office 脆弱性「CVE-2017-0199」を狙う攻撃が増加 http://www.security-next.com/085376 (Security-NEXT) ● 2017 年 9 月のセキュリティ更新プログラム（月例） https://blogs.technet.microsoft.com/jpsecurity/2017/09/13/201709-security-bulletin/ (Microsoft)

2. Apple

関連記事	● 偽の macOS アップデートを装い、感染した Mac を偽のネットバンキングへ誘導する「OSX_DOK.C」が確認される。 http://applech2.com/archives/20170712-osx-dok-c-mitm-attack-and-hijack-user-traffic.html (APPL Ch.) ● Mac のネットワーク設定を変更し、さらにインターネットバンキングやモバイルデバイスを狙う「OSX/Dok」の亜種が確認される。 http://applech2.com/archives/20170717-macos-malware-osx-dok-target-android.html (APPL Ch.) ● Apple がセキュリティアップデート一挙公開、iOS や macOS の脆弱性を修正 http://www.itmedia.co.jp/enterprise/articles/1707/20/news044.html (ITmedia) ● 数百台の Mac に感染しているのに数年間気づかれなかったマルウェア「FruitFly」 http://gigazine.net/news/20170725-mac-malware-fruitfly/ (GIGAZINE) ● 「macOS High Sierra」、パスワード盗まれるゼロデイ脆弱性の指摘 https://japan.cnet.com/article/35107753/ (cnet japan) ● iOS 上で大量のアイコンを作成する不正プロファイル「YJSNPI ウイルス」こと「iXintpwn」を解説 http://blog.trendmicro.co.jp/archives/16007 (トレンドマイクロ)

3. Adobe

関連記事	● 「Adobe Flash Player」に深刻な脆弱性 - 早急にアップデートを http://www.security-next.com/083742 (Security-NEXT) ● アドビ、「Flash」を 2020 年に終了へ https://japan.zdnet.com/article/35104776/ (ZDNet Japan) ● 「Adobe Acrobat/Reader」が脆弱性 67 件を修正 - 43 件が「クリティカル」 http://www.security-next.com/084719 (Security-NEXT) ● 「Adobe Flash Player」のセキュリティアップデートがリリース - 深刻な脆弱性へ対応 http://www.security-next.com/084711 (Security-NEXT) ● 「Adobe Flash Player」に深刻な脆弱性「IE」や「Edge」同梱版は早急に更新を http://www.security-next.com/085715 (Security-NEXT)

4. Android

関連記事	● 1400 万台に感染した Android マルウェア「CopyCat」、端末を root 化して広告詐欺 http://www.itmedia.co.jp/news/articles/1707/07/news056.html (ITmedia) ● Android 端末を狙うランサムウェア「SLocker」、「WannaCry」を模倣して活動を再開 http://blog.trendmicro.co.jp/archives/15401 (トレンドマイクロ) ● LeakerLocker：暗号化しないモバイル　ランサムウェア http://blogs.mcafee.jp/mcafeeblog/2017/07/leakerlocker-f63f.html (Macafee) ● 音声や動画を窃取する Android 端末向けバックドア型不正アプリ「GhostCtrl」 http://blog.trendmicro.co.jp/archives/15502 (トレンドマイクロ) ● Android を狙う標的型スパイウェア、Google Play で配信　Google が削除 http://www.itmedia.co.jp/news/articles/1707/27/news041.html (ITmedia) ● Android 端末の情報を中国のサーバに送信、「問題ない」とメーカー反論 http://www.itmedia.co.jp/enterprise/articles/1708/02/news044.html (ITmedia) ● Android の月例セキュリティ情報公開、メディアフレームワークに深刻な脆弱性 http://www.itmedia.co.jp/news/articles/1708/09/news054.html (ITmedia) ● 「Android」の各種アプリストアに 1000 件超のスパイウェアアプリ https://japan.cnet.com/article/35105756/ (cnet japan) ● スパイウェアを仕込む SDK、Google 公式ストアで配信のアプリ 500 本が利用 http://www.itmedia.co.jp/enterprise/articles/1708/23/news043.html (ITmedia) ● Google Play にまたマルウェア感染アプリ、高度な技術でチェックかわす http://www.itmedia.co.jp/news/articles/1709/15/news057.html (ITmedia) ● オンラインバンキングアプリを狙う「BankBot」を「Google Play」上で確認、国内銀行 7 行も対象 http://blog.trendmicro.co.jp/archives/15950 (トレンドマイクロ)

5. 情報漏洩

関連記事	● 不正アクセスで問合顧客の個人情報が流出か - 日産化学工業 http://www.security-next.com/083583 (Security-NEXT) ● ベライゾンの顧客情報 1400 万人分が公開状態に https://japan.zdnet.com/article/35104197/ (ZDNet Japan) ● ハワイアンズモールのクレジットカード情報流出、原因は OpenSSL の脆弱性「HeartBleed」 http://itpro.nikkeibp.co.jp/atcl/news/17/071201895/ (ITpro) ● Instagram の情報流出、一般ユーザーにも被害 http://www.itmedia.co.jp/news/articles/1709/04/news039.html (ITmedia) ● FX 取引サービスの M2J に不正アクセス、顧客情報流出か http://www.security-next.com/083927 (Security-NEXT) ● 通販サイトへ不正アクセス、クレカなど個人情報が流出か - 日本文化センター http://www.security-next.com/083999 (Security-NEXT) ● スウェーデン政府が誤ってほぼ全国民分の個人情報＆軍の機密情報を流出 http://gigazine.net/news/20170725-sweden-accidentally-leaks-personal-details/ (GIGAZINE) ● 投資情報サイトに不正アクセス、クレカ情報が流出か http://www.security-next.com/084174 (Security-NEXT) ● 米テレビ局がハッキング被害、「Game of Thrones」の脚本など流出 http://www.itmedia.co.jp/news/articles/1708/01/news051.html (ITmedia) ● HIS で個人情報 1 万人超流出　サイト刷新時のミスが原因 http://www.itmedia.co.jp/business/articles/1708/22/news083.html (ITmedia) ● 米個人情報機関最大手 Equifax、1 億 4300 万人の社会保障番号など漏えい http://www.itmedia.co.jp/news/articles/1709/08/news058.html (ITmedia)

6. 脆弱性

関連記事	● PHP に脆弱性 - セキュリティアップデートがリリース http://www.security-next.com/083569 (Security-NEXT) ● 「Apache Struts 2」にリモートより攻撃可能な脆弱性 - 「Struts 1 Plugin」利用時に影響 http://www.security-next.com/083614 (Security-NEXT) ● Windows 標準の日本語入力システム「Microsoft IME」に脆弱性 http://forest.watch.impress.co.jp/docs/news/1069615.html (窓の杜) ● Hikvision 製ネットワークカメラに複数の脆弱性 http://jvn.jp/vu/JVNVU92379282/ (JVN) ● Oracle、同社製品群への定例更新で脆弱性 308 件を修正 http://www.security-next.com/083947 (Security-NEXT) ● リモートで悪用可能な Wi-Fi チップセットの脆弱性、Black Hat で詳細発表 http://www.itmedia.co.jp/enterprise/articles/1707/24/news057.html (ITmedia) ● 数百万台のセキュリティ・カメラに乗っ取り可能な脆弱性 http://news.mynavi.jp/news/2017/07/21/130/ (マイナビニュース) ● 米 FDA、心臓ペースメーカーのリコール発表　脆弱性を突かれ患者に危害が及ぶ恐れ http://www.itmedia.co.jp/news/articles/1708/31/news045.html (ITmedia) ● Apache Struts に重大な脆弱性、直ちに更新を http://www.itmedia.co.jp/news/articles/1709/06/news046.html (ITmedia) ● Bluetooth 経由でスマホから PC まで乗っ取れる攻撃手法が発覚 http://pc.watch.impress.co.jp/docs/news/1080650.html (Impress Watch) ● Apache Tomcat、リモートコード実行の脆弱性など修正 http://www.itmedia.co.jp/enterprise/articles/1709/20/news053.html (ITmedia) ● 「Apache Tomcat」にゼロデイ脆弱性、JPCERT/CC が回避策を案内 http://internet.watch.impress.co.jp/docs/news/1082834.html (Impress Watch)

7. サイバー攻撃

関連記事	● ウクライナ保安局「ロシアのサイバー攻撃」断定　現金詐取は見せかけ、真の目的は情勢「不安定化」と声明 http://www.sankei.com/world/news/170701/wor1707010058-n1.html (産経新聞) ● 「BlackTech」によるサイバー諜報活動の足跡を追う http://blog.trendmicro.co.jp/archives/15393 (トレンドマイクロ) ● 2016 年の韓国軍への不正アクセスと 2017 年の ATM 不正引き出しの関連を発見 http://www.kaspersky.co.jp/about/news/virus/2017/vir13072017# (カスペルスキー) ● 韓国外交部へのサイバー攻撃やハッキングの試み、中国発が今年に入り急増 http://www.recordchina.co.jp/b190197-s0-c10.html (Record China) ● 「スマート水槽」がハッカーの侵入口に、北米のカジノで被害 https://www.cnn.co.jp/tech/35104512.html (CNN) ● 自由党のホームページ改ざん　不正アクセス、数日前から http://www.asahi.com/articles/ASK815HLVK81ULBJ00M.html (朝日新聞) ● 北朝鮮のハッカー集団が、サイバー攻撃を世界中で繰り広げる「合理的な理由」 https://wired.jp/2017/08/01/north-korea-cyberattacks/ (WIRED) ● ベネズエラで同時サイバー攻撃、大統領府など標的 反乱集団を支持 http://news.livedoor.com/article/detail/13445237/ (livedoor ニュース) ● 船の「盲点」突くサイバー攻撃急増 http://jp.reuters.com/article/cyber-threats-ships-idJPKBN1AR065 (ロイター) ● 正規のソフトウェアアップデートにマルウェア、法人顧客に配信 http://www.itmedia.co.jp/news/articles/1708/16/news044.html (IT media) ● サイバー攻撃集団「APT28」が NSA のツールを使いホテル宿泊客のデータを盗む https://the01.jp/p0005610/ (THE ZERO/ONE)

8. ランサムウェア

関連記事	● WannaCryptor の相談事例から学ぶ一般利用者が注意すべきセキュリティ環境 http://www.ipa.go.jp/security/anshin/mgdayori20170713.html (IPA) ● 進化するランサムウェアサービス--被害者の場所をマップ表示する「Philadelphia」 https://japan.zdnet.com/article/35104787/ (ZDNet Japan) ● 「Trickbot」マルウェアが「WannaCry」の手法を模倣、悪質化 https://japan.zdnet.com/article/35105017/ (ZDNet Japan) ● 「WannaCry」犯人、身代金のビットコインを全額引き出し--14 万ドル相当 https://japan.zdnet.com/article/35105298/ (ZDNet Japan) ● ランサムウェア「Cerber」がまた凶悪化--Bitcoin ウォレットも狙う https://japan.zdnet.com/article/35105381/ (ZDNet Japan) ● 身代金ウイルスで「損失額 300 億円」デンマークの海運企業が発表 https://forbesjapan.com/articles/detail/17381 (Forbes Japan) ● :Google がランサムウエアの身代金ルートを追跡、月間 1 億円を稼ぐウイルスも http://itpro.nikkeibp.co.jp/atcl/column/15/061500148/081000121/ (ITpro) ● 再流行し始めた Locky ランサムウェア http://sophos-insight.jp/blog/20170904 (SOPHOS　INSIGHT) ● nRansom ヌード写真を要求するランサムウェア https://blog.kaspersky.co.jp/nransom-nude-ransomware/17993/ (カスペルスキー) ● 2 種類のランサムウェアによる新たなスパムキャンペーン--2 度感染する恐れも https://japan.cnet.com/article/35107474/ (cnet japan) ● ランサムウェア最大の脅威は身代金ではない……中小企業の被害調査結果 http://internet.watch.impress.co.jp/docs/column/security/1079521.html (Impress Watch)

9. フィッシング

関連記事	● Apple をかたるフィッシング http://www.antiphishing.jp/news/alert/apple_20170705.html (フィッシング対策協議会) ● Google 装う偽サイトで 1000 人から 2000 万円以上だまし取る　詐欺の疑いで男 2 人を再逮捕 http://www.itmedia.co.jp/news/articles/1707/27/news040.html (ITmedia) ● ツイッター偽ログイン画面でＩＤ７３００件不正入手容疑で札幌の私立大生逮捕 http://www.sankei.com/affairs/news/170727/afr1707270008-n1.html (産経新聞) ● すぐ役立つ!フィッシング詐欺を見抜くためのポイントとは？ http://blog.trendmicro.co.jp/archives/15539 (トレンドマイクロ) ● 警察庁の偽サイト現る　「違反行為した」と「罰金」要求 http://www.itmedia.co.jp/news/articles/1707/31/news118.html (ITmedia) ● Google Chrome の人気拡張機能に不正なコード混入、 作者にフィッシング詐欺攻撃 http://www.itmedia.co.jp/enterprise/articles/1708/03/news051.html (ITmedia) ● フィッシング報告、URL ともに 3 カ月連続で増加 - 偽 Apple は短縮 URL を愛用 http://www.security-next.com/084475 (Security-NEXT) ● より高度な「ファイルレス活動」を実現した一連のマルウェアを確認 http://blog.trendmicro.co.jp/archives/15653 (トレンドマイクロ) ● Amazon をかたるフィッシング http://www.antiphishing.jp/news/alert/amazon_20170821.html (フィッシング対策協議会) ● フィッシング報告、17 カ月ぶりに 1000 件を突破 - URL も大幅増 http://www.security-next.com/085403 (Security-NEXT)

10. マルウェア

関連記事	● 各 OS に対応する Java の RAT「ADWIND」が再び確認。スパムメールで拡散 http://blog.trendmicro.co.jp/archives/15445 (トレンドマイクロ) ● ベトナムの IoT 設備、ウイルス感染率が中国に次ぐ 2 位 http://www.viet-jo.com/news/social/170720180040.html (VIETJO) ● 脆弱性「SambaCry」を利用する Linux マルウェアを新たに確認 http://blog.trendmicro.co.jp/archives/15470 (トレンドマイクロ) ● WikiLeaks、CIA 関与のマルウェア情報を新たに 5 つ公開 http://news.mynavi.jp/news/2017/07/23/039/ (マイナビニュース) ● 新手口のウイルスメール　ー通常対策をすり抜け https://this.kiji.is/262505852461236231 (共同通信) ● 仮想通貨取引所等のウェブサイトが「DreamBot」の標的となるおそれ https://www.jc3.or.jp/topics/dces.html (JC3) ● モバイルバンクを狙った新たなトロイの木馬が発見 http://news.mynavi.jp/news/2017/08/02/068/ (マイナビニュース) ● 身近に迫るサイバー戦争の脅威――電力網を狙い停電を引き起こすマルウェア「CRASHOVERRIDE」 http://engineer.fabcross.jp/archeive/170704_dragos.html (fabcross) ● 新たに「ビットコイン」を狙う「URSNIF」を国内で確認 http://blog.trendmicro.co.jp/archives/15633 (トレンドマイクロ) ● 大使館を狙うバックドア「Gazer」を発見 http://news.mynavi.jp/news/2017/09/01/070/ (マイナビニュース) ● Avast 傘下の「CCleaner」にマルウェア混入、正規ルートで配信 http://www.itmedia.co.jp/news/articles/1709/19/news051.html (ITmedia) ● 新たな FinFisher 監視キャンペーンを発見 - ISP レベルで中間者攻撃 http://news.mynavi.jp/news/2017/09/26/053/ (マイナビニュース)

4. 新種ウイルス情報

当期間確認された新種ウイルス情報は以下の通りです。

1. 2017 年 7 月のウイルスレビュー

関連記事	● 2017 年 7 月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=11402

2. 2017 年 8 月のウイルスレビュー

関連記事	● 2017 年 8 月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=11444

3. 2017 年 9 月のウイルスレビュー

関連記事	● 2017 年 9 月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=11503

4. 2017 年 7 月のモバイルマルウェア

関連記事	● 2017 年 7 月のモバイルマルウェア（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=11394

5. 2017 年 8 月のモバイルマルウェア

関連記事	● 2017 年 8 月のモバイルマルウェア（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=11447

6. 2017 年 9 月のモバイルマルウェア

関連記事	● 2017 年 9 月のモバイルマルウェア（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=11505

4.1. 脆弱性情報

当期間確認された主な脆弱性情報は以下の通りです。

※ITpro Hitachi Incident Response Team の CSIRT メモより抜粋

1. チェックしておきたい脆弱性情報＜2017.07.03＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.07.03＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170703.html

2. チェックしておきたい脆弱性情報＜2017.07.10＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.01.09＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170710.html

3. チェックしておきたい脆弱性情報＜2017.07.17＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.07.17＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170717.html

4. チェックしておきたい脆弱性情報＜2017.07.24＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.07.24＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170724.html

5. チェックしておきたい脆弱性情報＜2017.07.31＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.07.31＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170731.html

6. チェックしておきたい脆弱性情報＜2017.08.07＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.08.07＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170807.html

7. チェックしておきたい脆弱性情報＜2017.08.14＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.08.14＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170814.html

8. チェックしておきたい脆弱性情報＜2017.08.21＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.08.21＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170821.html

9. チェックしておきたい脆弱性情報＜2017.08.27＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.08.27＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170827.html

10. チェックしておきたい脆弱性情報＜2017.09.04＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.09.04＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170904.html

11. チェックしておきたい脆弱性情報＜2017.09.11＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.09.11＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170911.html

12. チェックしておきたい脆弱性情報＜2017.09.18＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.09.18＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170918.html

13. チェックしておきたい脆弱性情報＜2017.09.25＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.09.25＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170925.html

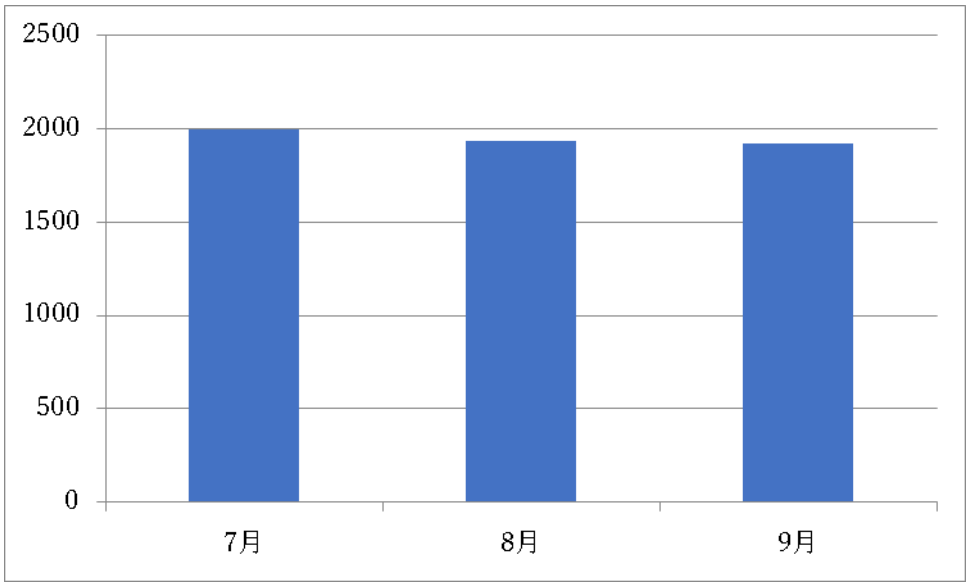
5. トレンドレポート 2017 年第 3 四半期度版

該当期間の代表的なセキュリティ情報は以下の通りです。

対象期間：2017/7/1～2017/9/30

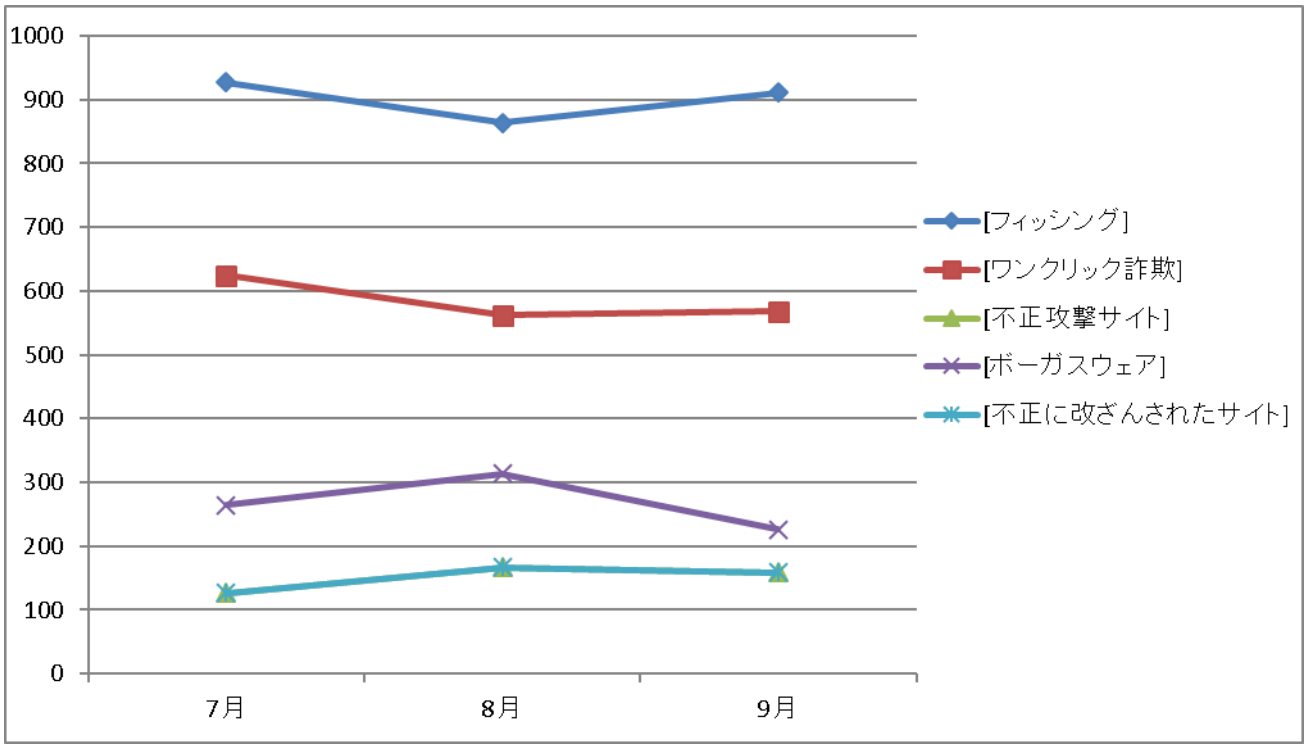
6. データからみるサイバー犯罪の傾向

インターネットユーザがウェブサイトの安全性を確認できるウェブサイトセキュリサービス*のデータをもとにした「危険な可能性」と判断されたウェブサイトの件数を以下に示します。



「危険な可能性」と判断されたウェブサイトの件数

* 株式会社セキュアブレインが提供する無料ウェブセキュリティサービス「gred でチェック」(http://check.gred.jp/)



脅威別検知数の月別推移(2017 年 7 月～9 月)

今期の「危険な可能性」と判断されたウェブサイトの件数は、7 月が 1996 件、8 月が 1934 件、9 月が 1919 件でした。過去 1 年間の 1 か月あたりの平均である 2100 件と比較すると、すべての月で約 10%減少しています。

大きな変化を見せた項目はボーガスウェアで、8 月に前月比で約 20%増加し、9 月には約 40%減少しています。この変化は、8 月に発生した Windows 向けボーガスウェアを配布する活動が翌月には収束したことが伺えます。(*1)

今期は不正攻撃サイトおよび不正に改ざんされたサイトの検出数に大きな変化はありませんでした。

(*1) インターネット詐欺リポート（2017 年 8 月度）https://prtimes.jp/main/html/rd/p/000000059.000008525.html)

7. 総括

今期は 9 月 6 日に米信用情報機関の Equifax から、約 1 億 4300 万人分という大規模な個人情報の漏えいが発生したとの発表がありました。情報漏えいの原因は、今年 3 月 6 日に発見された Apache Struts2 の脆弱性（CVE-2017-5638）であることが判明しています。Equifax は脆弱性の修正に取り組んでいたものの、自社の Web アプリケーションに本脆弱性が存在することを検出できませんでした。その結果、5 月 13 日から 7 月 30 日まで外部から不正アクセスを継続して受けることになり、今回の漏えいに繋がりました。この問題は、脆弱性への対策が一部でも漏れてしまうと、そこを起点として攻撃を受ける可能性が残ってしまうことを示唆しています。つまり、脆弱性対策の一歩として、自身の保有するシステムを把握することがセキュリティの強化には必要不可欠なのです。

他方で、ビットコインをはじめとした仮想通貨の高騰により、仮想通貨に係る金銭的利益を狙ったマルウェアや攻撃手法が流行しています。一般的なバンキングマルウェアのようにクレデンシャル情報を狙うものから、感染させたコンピュータを仮想通貨の発掘に利用するなど、仮想通貨特有の仕組みを利用したマルウェアも存在しています。

また､不正アクセスにより仮想通貨の発掘を行う Java スクリプトを Web サイトに挿入し、閲覧者のコンピュータを無断で仮想通貨の発掘に利用するといった新たな攻撃手法も出現しています。(*2)

今後もこのような仮想通貨を狙ったサイバー攻撃は続くと見られ、動向を注視していく必要があります。

(*2) Dr.Web　2017 年 9 月のウイルスレビュー (https://news.drweb.co.jp/show/review/?lng=ja&i=11503)

株式会社　日立システムズ

〒141-8672 東京都品川区大崎 1-2-1

http://www.hitachi-systems.com/index.html

http://www.shield.ne.jp/ssrc/index.html