S.S.R.C.定期
トレンドレポート
Vol.36

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.36

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. トレンドレポート 2018 年第 2 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：2018/4/1～2018/6/30

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	● Microsoft のマルウェアスキャンエンジン「MPE」に再び RCE 脆弱性、修正パッチを定例外で緊急公開 https://internet.watch.impress.co.jp/docs/news/1115272.html (Internet Watch) ● 挙動監視と機械学習で大規模な「Dofoil」によるコインマイニング攻撃を阻止 https://blogs.technet.microsoft.com/jpsecurity/2018/04/12/behavior-monitoring-combined-with-machine-learning-spoils-a-massive-dofoil-coin-mining-campaign/ (Microsoft) ● Microsoft の「hcsshim」に深刻な脆弱性、臨時更新プログラムで対処 http://www.itmedia.co.jp/enterprise/articles/1805/07/news041.html (ITMedia) ● 「OneDrive」「Skype」など MS 製複数アプリに脆弱性 - 修正は次期バージョン以降 http://www.security-next.com/093452 (Security NEXT) ● Office ドキュメントベースのダウンローダーが前月比 3.4 倍に http://www.security-next.com/094860 (Security NEXT) ● 2018 年 6 月のセキュリティ更新プログラム (月例) https://blogs.technet.microsoft.com/jpsecurity/2018/06/13/201806-security-updates/ (Microsoft)

2. Apple

関連記事	● Apple がセキュリティアップデートを公開、早期の適用を呼びかけ https://scan.netsecurity.ne.jp/article/2018/04/02/40751.html (ScanNetSecurity) ● 4 月の MS 月例パッチ、「緊急」22 件含む脆弱性 65 件を修正 http://www.security-next.com/092148 (Security NEXT) ● 5 月の MS 月例パッチで脆弱性 67 件を解消 - 2 件でゼロデイ攻撃が発生 http://www.security-next.com/093076 (Security NEXT) ● Apple、「iOS 11.4」を公開 - AirPlay 2 やメッセージの iCloud 保存をサポート 脆弱性の修正も https://forest.watch.impress.co.jp/docs/news/1124592.html (Forbes JAPAN) ● iOS に「外部からのアンロックが困難になる」機能が実装か、 端末を 1 時間放置すると Lightning ポートを介したデータ通信が不可に https://gigazine.net/news/20180605-apple-iphone-usb-restricted-mode/ (GIGAZINE) ● アップル、仮想通貨マイニングを禁止 - 「iPhone」などで https://japan.cnet.com/article/35120658/ (cnet Japan) ● macOS の「クイックルック」は暗号化ドライブのファイルまでキャッシュ しており、データは永続的に保管されいつでも閲覧できる https://gigazine.net/news/20180619-macos-leaks-secrets-stored-date/ (GIGAZINE) ● Mac で動作するマルウェア「フルーツフライ」 https://eset-info.canon-its.jp/malware_info/trend/detail/180628.html (キヤノン IT ソリューションズ)

3. Adobe

関連記事	● サイバー攻撃、Adobe Flash の脆弱性から Microsoft の脆弱性へシフト https://news.mynavi.jp/article/20180405-610400/ (マイナビニュース) ● Flash Player の更新版公開、複数の深刻な脆弱性を修正 http://www.itmedia.co.jp/news/articles/1804/11/news064.html (ITMedia) ● 北朝鮮悪用の Flash 脆弱性、広く悪用される状態に 海外中心に攻撃が拡大、国内でも http://www.security-next.com/092519 (Security NEXT) ● 「Adobe Flash Player」のアップデートが公開 - 深刻な脆弱性を解消 http://www.security-next.com/093070 (Security NEXT) ● グーグル、「Android」端末メーカーに 定期セキュリティパッチの提供を義務づけへ https://japan.cnet.com/article/35119071/ (cnet Japan) ● Adobe が 48 件の重大なセキュリティアップデートをリリース https://gigazine.net/news/20180515-adobe-security-update/ (GIGAZINE) ● 「iOS 11.4」では「EFAIL」含む脆弱性 35 件に対処 http://www.security-next.com/093965 (Security NEXT) ● Apple、Mac と Safari、Windows 向け iCloud のセキュリティアップデート公開 http://www.itmedia.co.jp/enterprise/articles/1806/04/news059.html (ITMedia) ● 「Adobe Flash Player」が緊急アップデート - すでにゼロデイ攻撃が発生 http://www.security-next.com/094209 (Security NEXT)

4. Android

関連記事	● Android の月例セキュリティ情報公開　多数の脆弱性を修正 http://www.itmedia.co.jp/news/articles/1804/03/news066.html (ITMedia) ● 「Monero」を発掘する Android 端末向け不正アプリ「HIDDENMINER」、端末に不具合を発生させる可能性も http://blog.trendmicro.co.jp/archives/17191 (トレンドマイクロ) ● Google、5 月の Android セキュリティ情報を公開 NVIDIA コンポーネントの脆弱性などを修正 http://www.itmedia.co.jp/enterprise/articles/1805/08/news058.html (ITMedia) ● 北朝鮮からの亡命者を標的にした Google Play のマルウェア https://blogs.mcafee.jp/malware-on-google-play-targets-north-korean-defectors (マカフィー) ● 「仮想キーボード」アプリで、3,000 万人以上のユーザーの個人情報が漏えい https://eset-info.canon-its.jp/malware_info/special/detail/180517.html (キヤノン IT ソリューションズ) ● 数百機種の Android デバイスにマルウェア - ファームウェアレベルで混入 http://www.security-next.com/093684 (Security NEXT) ● 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/enterprise/articles/1806/06/news062.html (ITMedia) ● Android ユーザー注意、 Google Play にダウンロード数を偽るアプリ https://news.mynavi.jp/article/20180613-645208/ (マイナビニュース) ● Telegram のプロトコルを利用する Android RAT に要注意 https://news.mynavi.jp/article/20180620-650007/ (マイナビニュース) ● Android に存在するメモリ関連の脆弱性「RAMpage」、重要情報流出の恐れ http://www.itmedia.co.jp/enterprise/articles/1806/29/news078.html (ITMedia)

5. 情報漏洩

関連記事	● 高級百貨店、買い物客の決済カード情報流出 ハッキング集団が 500 万枚の売り出し公言 http://www.itmedia.co.jp/news/articles/1804/03/news062.html (ITMedia) ● 省庁職員の公用アドレス流出＝数千件か、内閣が注意喚起 https://www.jiji.com/jc/article?k=2018040400589 (時事ドットコム) ● 前橋市教委、個人情報流出は 4 万 7839 件 - 既往症や口座情報なども http://www.security-next.com/092544 (Security NEXT) ● がん治療認定医の変更届システムに不正アクセス(日本がん治療認定医機構) https://scan.netsecurity.ne.jp/article/2018/04/12/40800.html (ScanNetSecurity) ● 顧客サポートソフトがマルウェア感染、 Delta や Sears 利用者のカード情報に不正アクセス http://www.itmedia.co.jp/news/articles/1804/06/news064.html (ITMedia) ● 尼崎市健康サイトにサイバー攻撃　１．２万人の情報流出 https://www.asahi.com/articles/ASL4L566KL4LPIHB01S.html (朝日新聞) ● 会員情報２７万件流出 - プレミアムアウトレット https://www.nikkei.com/article/DGXMZO29410450V10C18A4CC1000/ (日本経済新聞) ● 森永乳業の通販サイト、個人情報流出は最大 9 万人超 http//www.itmedia.co.jp/news/articles/1806/04/news102.html (ITMedia) ● 約 9200 万人の個人情報が DNA 解析サービス「MyHeritage」から流出 https://gigazine.net/news/20180606-dna-testing-myheritage-hacked/ (GIGAZINE) ● 米人気チケットサイトで起きた大規模顧客データ流出と個人でできる対策 http://ascii.jp/elem/000/001/690/1690148/ (ASCII.jp)

6. 脆弱性

関連記事	● 「Spring Framework」に複数の脆弱性、アップデートがリリース - 「同 4.3.x」は再修正も http://www.security-next.com/092076 (Security NEXT) ● Drupal の脆弱性を悪用可能な実証コードが公開、攻撃発生に警戒 https://japan.zdnet.com/article/35117714/ (ZDNet Japan) ● Oracle が定例アップデート、脆弱性 254 件を修正 - 143 件は RCE の脆弱性 http://www.security-next.com/092427 (Security NEXT) ● 「Minecraft」の脆弱性狙う破壊型マルウェア - 5 万アカウント以上で被害か http://www.security-next.com/092456 (Security NEXT) ● BMW 車から 14 件の脆弱性が発見される 車両に触れずに遠隔から操作可能になる「危険性が高い」ものも https://gigazine.net/news/20180524-bmw-smart-car-hacking/ (GIGAZINE) ● Steam クライアントで過去 10 年にわたってユーザーの PC をリモート制御できる深刻な脆弱性が放置されていたとの報告 https://gigazine.net/news/20180601-steam-serious-vulnerability/ (GIGAZINE) ● アーカイブファイル関連の脆弱性「Zip Slip」、大手プロジェクト多数に影響 http://www.itmedia.co.jp/enterprise/articles/1806/06/news061.html (ITMedia) ● シスコ、大量のセキュリティアップデートを公開 - 遠隔操作などの恐れ https://japan.zdnet.com/article/35120440/ (ZDNet Japan) ● WordPress でメディアファイル編集時にサーバー上の任意のファイルを削除可能な脆弱性、バージョン 4.9.6 でも未修正 https://gigazine.net/news/20180629-wordpress-vulnerability-file-delete/ (GIGAZINE)

7. サイバー攻撃

関連記事	● 「パスワードスプレー」攻撃に警戒を - 日米で注意喚起 https://japan.zdnet.com/article/35117214/ (ZDNet Japan) ● 世界中のネットワーク機器約 20 万台に大規模な攻撃が発生。 「米国の選挙を妨害するな」と表示も意図は不明確 https://jp.techcrunch.com/2018/04/09/engadget-20/ (TechCrunch) ● 防衛省ＯＢら標的、中国ハッカー集団関与か　情報流出の恐れ https://www.sankei.com/world/news/180412/wor1804120001-n1.html (産経新聞) ● 米国で複数の「天然ガスパイプライン事業者」がサイバー攻撃の影響を受ける https://the01.jp/p0006660/ (the ZERO/ONE) ● 日本を狙う標的型サイバー攻撃キャンペーン「ChessMaster」、 4 月に確認された最新攻撃手法を解説 http://blog.trendmicro.co.jp/archives/17280 (トレンドマイクロ) ● 北朝鮮のサイバー犯罪集団「Hidden Cobra」による世界規模のサイバー攻撃 幅広い業界でデータ流出被害 https://blogs.mcafee.jp/global-malware-ghostsecret (マカフィー) ● メキシコの銀行システムにサイバー攻撃 16 億円以上盗まれる http://www.afpbb.com/articles/-/3175033 (AFPBB News) ● 千葉・八千代 ネット公開　水位監視カメラに不正アクセス https://mainichi.jp/articles/20180426/k00/00m/040/057000c (朝日新聞) ● 中国ハッカー、米海軍の機密データ盗む　対艦ミサイルなど https://www.cnn.co.jp/tech/35120574.html (CNN) ● 米大統領首席補佐官の携帯にハッキング被害。 2017 年夏に発見、トランプ政権発足当時から気づかず https://japanese.engadget.com/2018/06/11/2017/ (engadget)

8. ランサムウェア

関連記事	● ランサムウェアの脅威は健在、手口が巧妙化した新種も https://japan.zdnet.com/article/35117465/ (ZDNet Japan) ● ランサムウェア「GandCrab」、Flash の脆弱性で拡散開始か https://japan.zdnet.com/article/35117475/ (ZDNet Japan) ● 「PUBG」を 1 時間プレイすることが解除条件のランサムウェアを確認 https://scan.netsecurity.ne.jp/article/2018/04/12/40793.html (ScanNetSecurity) ● ダークウェブに潜入してランサムウェアを取り巻く環境を知る http://www.atmarkit.co.jp/ait/articles/1804/18/news009.html (@IT) ● 仮想通貨マイニング攻撃、ランサムウェアを超える https://news.mynavi.jp/article/20180419-618283/ (マイナビニュース) ● 医療業界に広がる WannaCry の脅威とそこから学ぶべき対策とは https://news.mynavi.jp/article/20180531-wannacry_healhcare/ (マイナビニュース) ● 大手海運会社クラークソンがランサムウェア脅迫を拒絶 https://eset-info.canon-its.jp/malware_info/special/detail/180531.html (キヤノン IT ソリューションズ) ● ランサムウェア攻撃に転換点、標的を企業にする傾向 https://japan.zdnet.com/article/35121054/ (ZDNet Japan)

9. フィッシング

関連記事	● フィッシング報告数、前月比約 2.3 倍に - 悪用 URL の増加は限定的 http://www.security-next.com/091778 (Security NEXT) ● 「日本郵便」偽装サイトへのアクセス、1 週間で 2500 件以上 豪郵便公社も被害 http://www.security-next.com/091958 (Security NEXT) ● 簡単な操作で EC サイトを模倣できるフィッシング詐欺キット登場 https://news.mynavi.jp/article/20180426-622025/ (マイナビニュース) ● 2018/04 フィッシング報告状況 https://www.antiphishing.jp/report/monthly/201804.html (フィッシング対策協議会) ● Apple ID の窃取を狙う新しいフィッシング詐欺を確認、 AES 方式の暗号化によって検出を回避 http://blog.trendmicro.co.jp/archives/17404 (トレンドマイクロ) ● 「フィッシングレポート 2018」 公開のお知らせ https://www.antiphishing.jp/news/info/press_phishing_report2018.html (フィッシング対策協議会) ● わずか 6 グループで偽ショッピングサイト 2 万件を設置 APWG も脅威として定義追加へ http://www.security-next.com/094147 (Security NEXT) ● 6 国公私大、フィッシング被害 http://www.fukuishimbun.co.jp/articles/-/611209 (福井新聞) ● 「WannaCry」に感染させると脅すフィッシング詐欺が登場 - 英機関が警告 http://japan.zdnet.com/article/35121437/ (ZDNet Japan)

10. マルウェア

関連記事	● ルーターの DNS 改竄によりダウンロードされる「facebook.apk」の内部構造を読み解く https://blog.kaspersky.co.jp/malicious-facebook-apk/19968/ (カスペルスキー) ● ヘルスケア機器経由で企業スパイするマルウェア「Kwampirs」が登場 https://gigazine.net/news/20180425-healthcare-espionage-x-ray-mri/ (GIGAZINE) ● 5000 超 Web サイト、PHP マルウェア「Brain Food」に感染 https://news.mynavi.jp/article/20180525-634986/ (マイナビニュース) ● 米政府、北朝鮮攻撃グループが悪用したマルウェア「Joanap」「Brambul」の情報を公開 http://www.security-next.com/093874 (Security NEXT) ● SQL Server を通信に用いる新種のバンキング型トロイの木馬「MnuBot」 https://news.mynavi.jp/article/20180531-638532/ (マイナビニュース) ● セキュア USB メモリを使うマルウェア攻撃、Windows XP や 2003 を標的に http://japan.zdnet.com/article/35121409/ (ZDNet Japan) ● オンラインバンキングマルウェア「DreamBot(Ursnif/Gozi)」の今 https://www.mbsd.jp/blog/20180607.html (三井物産セキュアディレクション) ● マルウェア「Satori」による攻撃を国内初観測、従来のファイアウォール機能では対応が難しい？ http://www.atmarkit.co.jp/ait/articles/1806/27/news083.html (@IT) ● 米国政府、北朝鮮政府関与のトロイの木馬「TYPEFRAME」に注意喚起 https://news.mynavi.jp/article/20180618-647437/ (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. 2018 年 4 月のウイルスレビュー

関連記事	● 2018 年 4 月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=12569

2. 2018 年 5 月のウイルスレビュー

関連記事	● 2018 年 5 月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=12616

3. 2018 年 6 月のウイルスレビュー

関連記事	● 2018 年 6 月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=12667

4. 2018 年 4 月のモバイルマルウェア

関連記事	● 2018 年 4 月のモバイルマルウェア（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=12576

5. 2018 年 5 月のモバイルマルウェア

関連記事	● 2018 年 5 月のモバイルマルウェア（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=12618

6. 2018 年 6 月のモバイルマルウェア

関連記事	● 2018 年 6 月のモバイルマルウェア（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=12665

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。

※Hitachi Incident Response Team より抜粋

1. チェックしておきたい脆弱性情報 ＜2018.04.02＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.04.02＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180402.html

2. チェックしておきたい脆弱性情報＜2018.04.09＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.04.09＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180409.html

3. チェックしておきたい脆弱性情報＜2018.04.16＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.04.16＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180416.html

4. チェックしておきたい脆弱性情報＜2018.04.23＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.04.23> http://www.hitachi.co.jp/hirt/publications/csirt/memo20180423.html

5. チェックしておきたい脆弱性情報＜2018.04.30＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.04.30＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180430.html

6. チェックしておきたい脆弱性情報＜2018.05.07＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.05.07＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180507.html

7. チェックしておきたい脆弱性情報＜2018.05.14＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.05.14＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180514.html

8. チェックしておきたい脆弱性情報＜2018.05.21＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.05.21＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180521.html

9. チェックしておきたい脆弱性情報＜2018.05.28＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.05.28＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180528.html

10. チェックしておきたい脆弱性情報＜2018.06.04＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.06.04＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180604.html

11. チェックしておきたい脆弱性情報＜2018.06.11＞

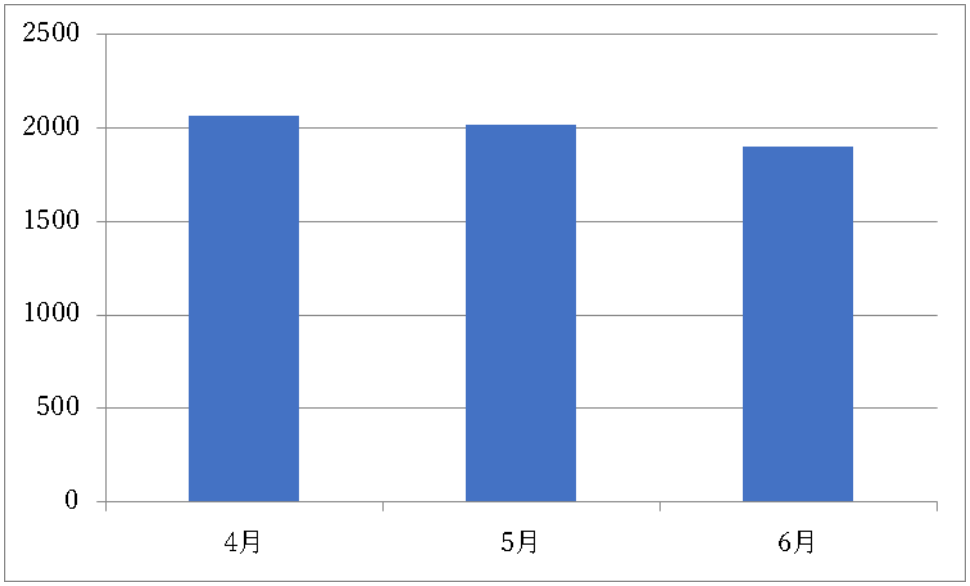
プレス リリース	● チェックしておきたい脆弱性情報＜2018.06.11＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180611.html

12. チェックしておきたい脆弱性情報＜2018.06.18＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.06.18＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180618.html

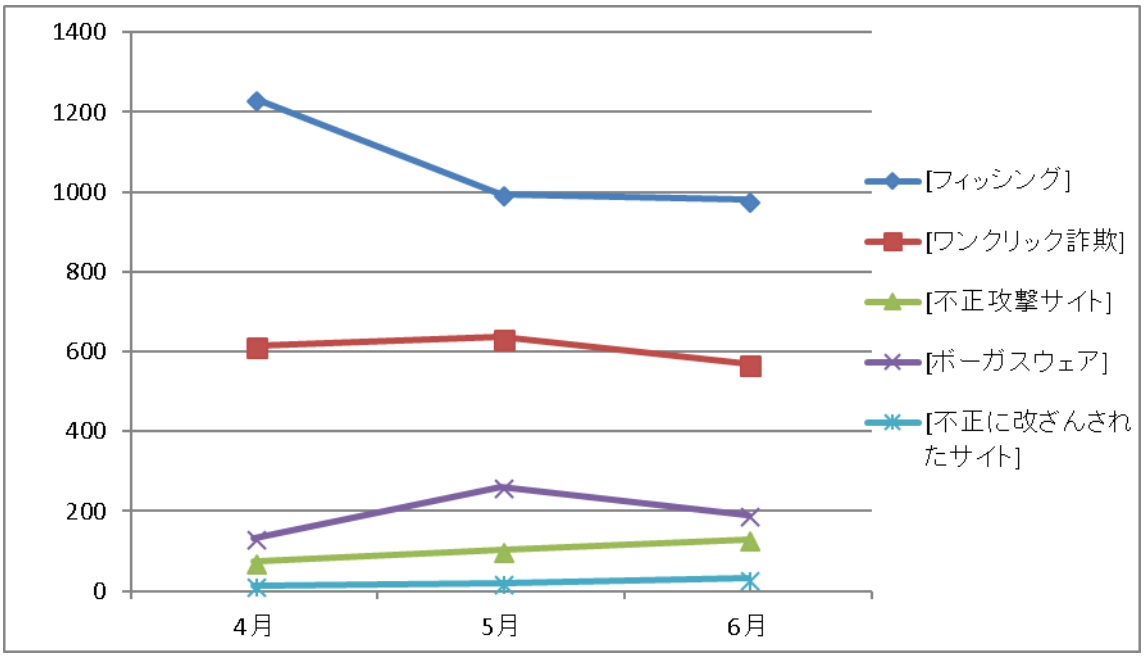
5. データからみるサイバー犯罪の傾向

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(2018 年 4 月～6 月)

4~6 月に「危険な可能性」と判断されたウェブサイトの件数は月平均で約 2000 件でした。今期のフィッシングの総数は減少傾向にあるものの、フィッシング対策協議会が公開したレポートによると(*1)、フィッシングサイトに誘導するスパムメールの本文に短縮 URL を使用したり、フィッシングサイトに SSL 証明書を用いてブラウザに鍵マークを表示させるなどの手法でユーザから怪しまれないような工夫が行われています。

短縮 URL にアクセスする際は、実際にアクセスすることになる URL を外部サービス等で確認することが必要です。

(*1) https://www.antiphishing.jp/report/pdf/phishing_report_2018.pdf

フィッシング対策協議会

6. 総括

今期は前期に引き続き、Adobe Flash Player の脆弱性を悪用したゼロデイ攻撃が報告されました。前期の 1 月には、2017 年 11 月から発生していたことが発覚した、北朝鮮によるものと思われる韓国を狙った標的型攻撃、今期 6 月には中東の企業や個人を狙った標的型攻撃が報告されています。いずれも悪意のある Flash コンテンツが含まれる Office ドキュメントをメールに添付して標的に開かせることで、Adobe Flash Player の脆弱性を悪用するものです。このように、Office ドキュメントを通じて Flash の脆弱性を悪用する攻撃が近年発生しているため、Web ブラウザだけでなく、Office ソフトウェアにおいても Flash の再生に関連する設定の確認を推奨します。2017 年よりサイバー攻撃の主な対象は Microsoft 製品の脆弱性に変化している(*1)ものの、Flash に対する攻撃には未だ注意が必要です。

また、4 月には 3 月末に公開された CMS(*2)の 1 つである、Drupal の脆弱性(CVE-2018-7600)に対する攻撃が発生しました(*3)。公開サービスであり、利用者が多い CMS の脆弱性は情報公開から僅かな時間で攻撃される可能性が高くなります。CMS の開発環境等が公開されたまま放置されていないか把握すると共に、攻撃より先に修正プログラムの適用を確実に行えるよう、管理体制の整備が必要です。

(*1) https://news.mynavi.jp/article/20180405-610400/ マイナビニュース

(*2)CMS(コンテンツマネジメントシステム):Web サイト管理システム

(*3)https://www.npa.go.jp/cyberpolice/important/2018/201804181.html 警察庁

株式会社　日立システムズ

〒141-8672 東京都品川区大崎 1-2-1

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

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