S.S.R.C.定期
トレンドレポート
Vol.32

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.32

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 2017 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：2017/4/1～2017/6/30

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 IIS 6.0 のゼロデイ脆弱性、遠隔で任意のコード実行が可能に (トレンドマイクロ) http://blog.trendmicro.co.jp/archives/14663 ● 今週でサポート終了の「Windows Vista」 - 数十万台規模が国内で稼働か (Security NEXT) http://www.security-next.com/080486 ● Microsoft Office の未解決の脆弱性を突く攻撃が横行、メールで届く Word ファイルに注意（ITMedia） http://www.itmedia.co.jp/enterprise/articles/1704/11/news052.html ● Microsoft、4 月の月例更新を公開　Windows Vista の更新は今回が最後 (ITMedia) http://www.itmedia.co.jp/enterprise/articles/1704/12/news055.html ● マイクロソフトを語る偽警告が Web ページ閲覧中に表示される事例 (窓の杜) http://forest.watch.impress.co.jp/docs/news/1057163.html ● Windows に新たな未解決の脆弱性、Google 研究者が「最悪」と報告 (ITMedia) http://www.itmedia.co.jp/news/articles/1705/09/news056.html ● Microsoft、マルウェア対策エンジンの重大な脆弱性を修正　(ITMedia) http://www.itmedia.co.jp/news/articles/1705/10/news052.html ● Microsoft、Windows XP にも更新プログラム公開　WannaCry 再発防止に向け (ITMedia) http://www.itmedia.co.jp/news/articles/1706/14/news058.html ● 「Skype」に深刻な脆弱性、悪質なコード実行のおそれ--修正済み (CNET Japan) https://japan.cnet.com/article/35103434/

2. Apple

関連記事	● 「iOS 10.3.1」がリリース--セキュリティ改善など (CNET Japan) https://japan.cnet.com/article/35099191/ ● Pegasus：iOS と Android を狙う究極のスパイウェア (カスペルスキー) https://blog.kaspersky.co.jp/pegasus-spyware/15217/ ● マルウェアが引き続き増加傾向、特に Mac を狙うものは前年比 744%と急増 (ScanNetSecurit) https://scan.netsecurity.ne.jp/article/2017/04/18/39667.html ● 「iPhone」や Android 端末にも搭載の Broadcom 製 Wi-Fi チップに脆弱性 (CNET Japan) https://japan.cnet.com/article/35099353/ ● Apple、多数の脆弱性に対処した「iOS 10.3.2」を公開　(ITpro) http://itpro.nikkeibp.co.jp/atcl/news/17/051601410/ ● iPhone が発端となったフィッシング詐欺事例：窃盗犯とサイバー犯罪者の共謀か (トレンドマイクロ) http://blog.trendmicro.co.jp/archives/14864 ● Mac を標的としたランサムウェアを販売する「MacRansom」が確認される。 (AAPL Ch.) http://applech2.com/archives/20170612-ransomware-as-a-service-macransom.html ● Mac ユーザーを標的にしたマルウェアがダークウェブに出回っている (GIGAZINE) http://gigazine.net/news/20170615-mac-computer-ransomware/

3. Adobe

関連記事	● 深刻な脆弱性に対処した「Adobe Flash Player」のアップデート (Security NEXT) http://www.security-next.com/080558 ● 「Adobe Flash Player」に深刻な脆弱性 - 修正アップデートがリリース (Security NEXT) http://www.security-next.com/081400 ● 「Adobe Flash Player」に 9 件の深刻な脆弱性 (Security NEXT) http://www.security-next.com/082705 ● Adobe Flash Player の脆弱性対策について (IPA) http://www.ipa.go.jp/security/ciadr/vul/20150624-adobeflashplayer.html ● 「Adobe Flash Player 26」が正式公開 ～CVE 番号ベースで 9 件の脆弱性を修正 (窓の杜) http://forest.watch.impress.co.jp/docs/news/1065116.html

4. Android

関連記事	● Google、Android の月例セキュリティ情報を公開 （ITMedia） http://www.itmedia.co.jp/news/articles/1704/04/news059.html ● Android に標的型マルウェア、iOS への攻撃と類似点（ZDNet Japan） https://japan.zdnet.com/article/35099258/ ● 端末初期化でも消せない Android 向けマルウェア「Chrysaor」（PC Watch） http://pc.watch.impress.co.jp/docs/news/1053336.html ● 「スーパーマリオラン」に便乗する偽アプリ、Google Play 起動時にクレジットカード情報を詐取（トレンドマイクロ） http://blog.trendmicro.co.jp/archives/14686 ● Android 端末を侵入用の裏口に変える不正アプリを「Google Play」上で確認（トレンドマイクロ） http://blog.trendmicro.co.jp/archives/14777 ● 人気ゲームのガイドアプリにマルウェア、多数の Android デバイスが感染（CNET Japan） https://japan.cnet.com/article/35100328/ ● 「Android」マルウェアを 100 万台に感染、銀行に送金指示 （CNET Japan） https://japan.cnet.com/article/35101569/ ● Android の設計問題突く攻撃手法「Cloak & Dagger」、米研究者が論文公開（ITMedia） http://www.itmedia.co.jp/news/articles/1705/25/news080.html ● 「WannaCry」からデバイス守る、実はウソ――“偽 Android アプリ”に注意（ITMedia） http://www.itmedia.co.jp/news/articles/1705/25/news114.html ● Android を攻撃するランサムウェア「WannaLocker」に注意（マイナビニュース） http://news.mynavi.jp/news/2017/06/12/199/

5. 情報漏洩

関連記事	● 自転車通販ショップに不正アクセス - 顧客情報が流出の可能性 (Security NEXT) http://www.security-next.com/080332 ● フォレンジック調査で個人情報流出が確定 - GMO-PG (Security NEXT) http://www.security-next.com/080342 ● ハッカーグループ Shadow Brokers、NSA の機密情報を大量に公表 (TechCrunch) http://jp.techcrunch.com/2017/04/11/20170408shadow-brokers-be-back/ ● インドのマクドナルド「宅配アプリ」から 220 万人の個人情報が流出 (THE ZERO/ONE) https://the01.jp/p0004788/ ● 総務省、Struts2 の脆弱性を突かれて 2.3 万人の個人情報流出か (ITpro) http://itpro.nikkeibp.co.jp/atcl/news/17/041401147/ ● ぴあ、最大 3 万 2000 件のクレカ情報流出 (ITMedia) http://www.itmedia.co.jp/business/articles/1704/25/news083.html ● 配信前のドラマを違法入手したハッカー、リークされたくなければ金を払えと脅す (CinemaToday) https://www.cinematoday.jp/news/N0091391 ● ユナイテッド航空でコクピットへのアクセスコードがオンラインで流出 (GIGAZINE) http://gigazine.net/news/20170516-united-airlines-cockpit-code-leaked/ ● InterFM に不正アクセス、リスナーの個人情報が流出 - Twitter の投稿で判明 (Security NEXT) http://www.security-next.com/081900 ● ハッキングで得た情報で株不正取引の中国人に罰金 9 億円、複数の法律事務所を標的にした攻撃手法（The Register） https://scan.netsecurity.ne.jp/article/2017/05/31/39795.html

6. 脆弱性

関連記事	● IPA が提供する脆弱性体験学習ツール「AppGoat」に複数の脆弱性 (ScanNetSecurity) https://scan.netsecurity.ne.jp/article/2017/06/07/39815.html ● 国土交通省、Apache Struts2 の脆弱性を利用した不正アクセスでアンケート情報流出の可能性（ScanNetSecurity) https://scan.netsecurity.ne.jp/article/2017/06/07/39814.html ● 最多脆弱性ブラウザは Chrome、最もパッチが適用されていないブラウザは (ScanNetSecurity) https://scan.netsecurity.ne.jp/article/2017/04/10/39628.html ● 「Adobe Acrobat/Reader」に 47 件の脆弱性 - アップデートがリリース (Security NEXT) http://www.security-next.com/080568 ● Firefox 安定版「53.0.2」公開、1 件の脆弱性を修正 (ITMedia) http://www.itmedia.co.jp/news/articles/1705/08/news049.html ● WikiLeaks で発覚した Cisco IOS の重大な脆弱性を修正 (ITMedia) http://www.itmedia.co.jp/news/articles/1705/11/news049.html ● 「Joomla！」に SQL インジェクションの脆弱性 - アップデートがリリース (Security NEXT) http://www.security-next.com/081778 ● 複数の脆弱性を解消した「WordPress 4.7.5」がリリース - 即時更新を推奨 (Security NEXT) http://www.security-next.com/081758 ● Ubuntu、ログイン画面に不正アクセスできる脆弱性（マイナビニュース) http://news.mynavi.jp/news/2017/05/18/067/ ● 企業のアプリの 96%がオープンソースを利用、その 60%以上に脆弱性 (ScanNetSecurity) https://scan.netsecurity.ne.jp/article/2017/05/23/39770.html

7. サイバー攻撃

関連記事	● 世界の銀行を狙うサイバー攻撃、北朝鮮が関与か （IT Media） http://www.itmedia.co.jp/enterprise/articles/1704/05/news057.html ● 中国とロシアのサイバー攻撃特性の違い－ ASERT Japan 名誉アドバイザー 名和利男 （arbornetworks） http://jp.arbornetworks.com/%E4%B8%AD%E5%9B%BD%E3%81%A8%E3%83%AD%E3%82%B7%E3%82%A2%E3%81%AE%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E6%94%BB%E6%92%83%E7%89%B9%E6%80%A7%E3%81%AE%E9%81%95%E3%81%84%EF%BC%8D-asert-japan%E5%90%8D/ ● ブラジルの銀行、広範囲で攻撃を受ける （マイナビニュース） http://news.mynavi.jp/news/2017/04/07/081/ ● 激増するサイバースパイやランサムウェア、米機関も注意勧告 （IT Media） http://www.itmedia.co.jp/news/articles/1705/01/news041.html ● マクロン氏陣営「サイバー攻撃受けた」 大量の文書流出 仏大統領選 （afpbb） http://www.afpbb.com/articles/-/3127339 ● 「Pawn Storm 作戦」が利用するソーシャルエンジニアリングの威力 (トレンドマイクロ) http://blog.trendmicro.co.jp/archives/14801 ● 国内標的型サイバー攻撃の分析：巧妙化と高度化を続ける「気づけない攻撃」 (トレンドマイクロ) http://blog.trendmicro.co.jp/archives/14818 ● サイバー防衛に自衛隊本腰 反撃なら…９条との関係課題 （朝日新聞） http://www.asahi.com/articles/ASK4H6X9CK4HUTFK00B.html ● 英国人ハッカーが米国の軍事通信システムに侵入 （THE ZERO/ONE） https://the01.jp/p0005271/ ● 米フェデックス：傘下ＴＮＴにサイバー攻撃、グローバル業務で障害（Bloomberg） https://www.bloomberg.co.jp/news/articles/2017-06-28/OS9SQVSYF01U01

8. ランサムウェア

関連記事	● Apache Struts2 の脆弱性、ファイル暗号化のランサムウェアに悪用 (ITMedia) http://www.itmedia.co.jp/news/articles/1704/07/news051.html ● 過去 1 年で 1 割近くの企業がランサムウェア被害を経験--実態調査 (ScanNetSecurity) https://scan.netsecurity.ne.jp/article/2017/04/26/39704.html ● 2016 年に猛威振るったランサムウェア「Locky」が再出現、手法が巧妙に (ZDNet Japan) https://japan.zdnet.com/article/35100266/ ● 身代金ウイルス検出数は日本がアジアでトップ、シマンテックが分析 (ITpro) http://itpro.nikkeibp.co.jp/atcl/news/17/042601296/ ● ランサムウェア「WannaCry」世界で猛威、日本でも拡大のおそれ (ITMedia) http://www.itmedia.co.jp/news/articles/1705/15/news050.html ● WannaCry、ランサムウエアというよりむしろワームと考えるべきだった (ITpro) http://itpro.nikkeibp.co.jp/atcl/watcher/14/334361/051800839/ ● 「WannaCry」の拡散、電子メールが原因ではなかった (ITMedia) http://www.itmedia.co.jp/news/articles/1705/22/news057.html ● 欧州を中心に甚大な被害、暗号化ランサムウェア「PETYA」の活動を詳細解析 (トレンドマイクロ) http://blog.trendmicro.co.jp/archives/15353 ● ランサムウェアの脅威の変遷と今後の予測(トレンドマイクロ) http://blog.trendmicro.co.jp/archives/15216 ● Petya 亜種による世界サイバー攻撃、65 カ国に拡大　会計ソフト更新の仕組みを悪用か　(ITMedia) http://www.itmedia.co.jp/news/articles/1706/29/news057.html ● ランサムウェア「SamSam」、3 万ドル超の身代金要求も--研究者らが注意喚起 (ZDNet Japan) https://japan.zdnet.com/article/35103365/

9. フィッシング

関連記事	● マイクロソフトをかたるフィッシング（2017/03/31）（フィッシング対策協議会） http://www.antiphishing.jp/news/alert/microsoft_20170331.html ● MUFG カードをかたるフィッシング（2017/04/10）（フィッシング対策協議会） http://www.antiphishing.jp/news/alert/mufgcard_20170410.html ● インシデント報告件数は横ばい、フィッシングサイトは前四半期から 36%増加（JPCERT/CC） https://scan.netsecurity.ne.jp/article/2017/04/14/39658.html ● フィッシング攻撃の 47.48%は、金銭の窃取が目的 （カスペルスキー） http://www.kaspersky.co.jp/about/news/virus/2017/vir13042017b ● Apple をかたるフィッシング（2017/04/19） （フィッシング対策協議会） http://www.antiphishing.jp/news/alert/apple_20170419.html ● グーグル、ウェブアプリのチェック強化--偽「Google Docs」によるフィッシング対策 （CNET Japan） https://japan.cnet.com/article/35101209/ ● 「セゾン Net アンサー」「MUFG カード」をかたるフィッシングメールが出回る（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/1059592.html ● LINE をかたるフィッシング（2017/05/29） （フィッシング対策協議会） http://www.antiphishing.jp/news/alert/line_20170529.html ● HTTPS を悪用したフィッシング詐欺が急増 （マイナビニュース） http://news.mynavi.jp/news/2017/05/29/347/ ● 2017/04 フィッシング報告状況 （フィッシング対策協議会） http://www.antiphishing.jp/report/monthly/201704.html ● 2017/05 フィッシング報告状況 （フィッシング対策協議会） http://www.antiphishing.jp/report/monthly/201705.html

10. マルウェア

関連記事	● 「GitHub を使うプログラマー」を狙ったマルウェア攻撃が発生　コードを秘密裏に改ざんされる可能性　(@IT) http://www.atmarkit.co.jp/ait/articles/1704/03/news040.html ● Nintendo Switch 人気に便乗、エミュレータに見せかけマルウェアを配布 - YouTube で宣伝も　(Security NEXT) http://www.security-next.com/080209 ● ウイルス付きメールが拡散、商品発送通知や年次運用報告書など装う、警視庁が早期警戒情報ツイートで注意呼び掛け　(INTERNET Watch)s http://internet.watch.impress.co.jp/docs/news/1053732.html ● 同人ゲームで高得点を出さないと暗号化が解除されないマルウェアが発見されたそうだ。 https://security.srad.jp/story/17/04/10/0518216/ ● HP の PC にキーロガー？　セキュリティ企業が指摘　(ITMedia) http://www.itmedia.co.jp/news/articles/1705/12/news055.html ● 北朝鮮の洪水被害に便乗する標的型攻撃、マルウェアは日本にホストか (ZDNet Japan)　https://japan.zdnet.com/article/35101101/ ● 2017 年 1Q のバンキングトロジャンは 144 件 - 前四半期から半減 (Security NEXT)　http://www.security-next.com/082080 ● 日本と韓国を狙う巨大マルウェア、ゴミデータでファイルサイズ肥大化 100MB 超、検知を逃れる古典的な手口 (INTERNET Watch) http://internet.watch.impress.co.jp/docs/news/1062671.html ● 金融機関を狙うマルウェアの広がりは、ランサムウェアの 2 倍以上 (シマンテック)　https://www.symantec.com/connect/ja/blogs/2 ● マルウェア「Fireball」、世界中の 2 億 5000 台の PC に感染 (マイナビニュース)　http://news.mynavi.jp/news/2017/06/05/284/

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 4 月のウイルスレビュー

関連記事	● 2017 年 4 月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=11275

2. 2017 年 5 月のウイルスレビュー

関連記事	● 2017 年 5 月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=11310

3. 2017 年 6 月のウイルスレビュー

関連記事	● 2017 年 6 月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=11360

4. 2017 年 4 月のモバイルマルウェア

関連記事	● 2017 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=11277

5. 2017 年 5 月のモバイルマルウェア

関連記事	● 2017 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=11312

6. 2017 年 6 月のモバイルマルウェア

関連記事	● 2017 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=11358

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＜2017.04.03＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.04.03＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170403.html

2. チェックしておきたい脆弱性情報＜2017. 04.10＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.04.10＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170410.html

3. チェックしておきたい脆弱性情報＜2017.04.17＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.04.17＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170417.html

4. チェックしておきたい脆弱性情報＜2017. 04.24＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.04.24.＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170424.html

5. チェックしておきたい脆弱性情報＜2017. 05.01＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.05.01＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170501.html

6. チェックしておきたい脆弱性情報＜2017. 05.08＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.05.08＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170508.html

7. チェックしておきたい脆弱性情報＜2017. 05.15＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.05.15＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170515.html

8. チェックしておきたい脆弱性情報＜2017. 05.22＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.05.22＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170522.html

9. チェックしておきたい脆弱性情報＜2017. 05.29＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.05.29＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170529.html

10. チェックしておきたい脆弱性情報＜2017. 06.05＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.06.05＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170605.html

11. チェックしておきたい脆弱性情報＜2017. 06.12＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.06.12＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170612.html

12. チェックしておきたい脆弱性情報＜2017. 06.19＞

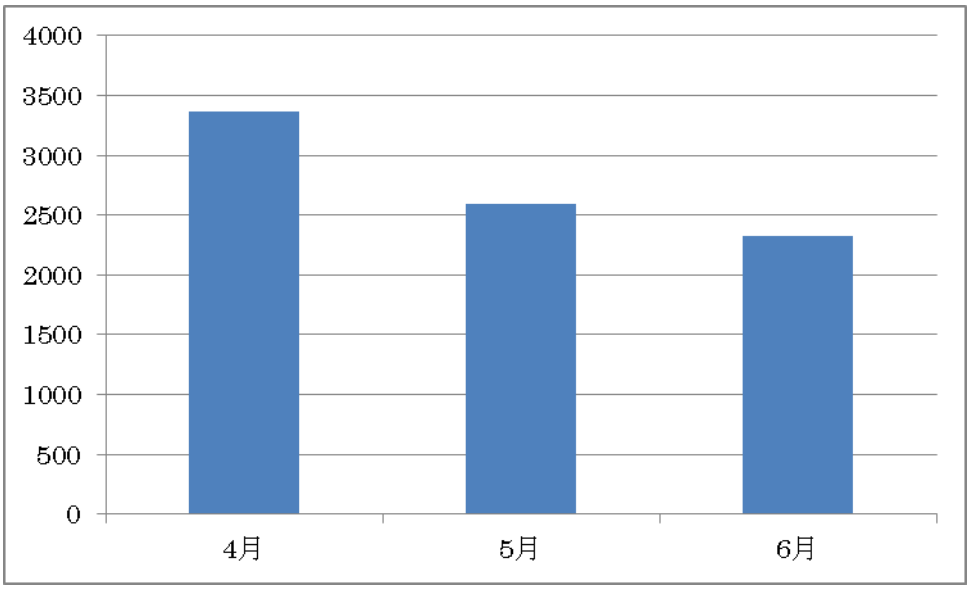
プレス リリース	● チェックしておきたい脆弱性情報＜2017.06.19＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170619.html

13. チェックしておきたい脆弱性情報＜2017. 06.26＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.06.26＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170619.html

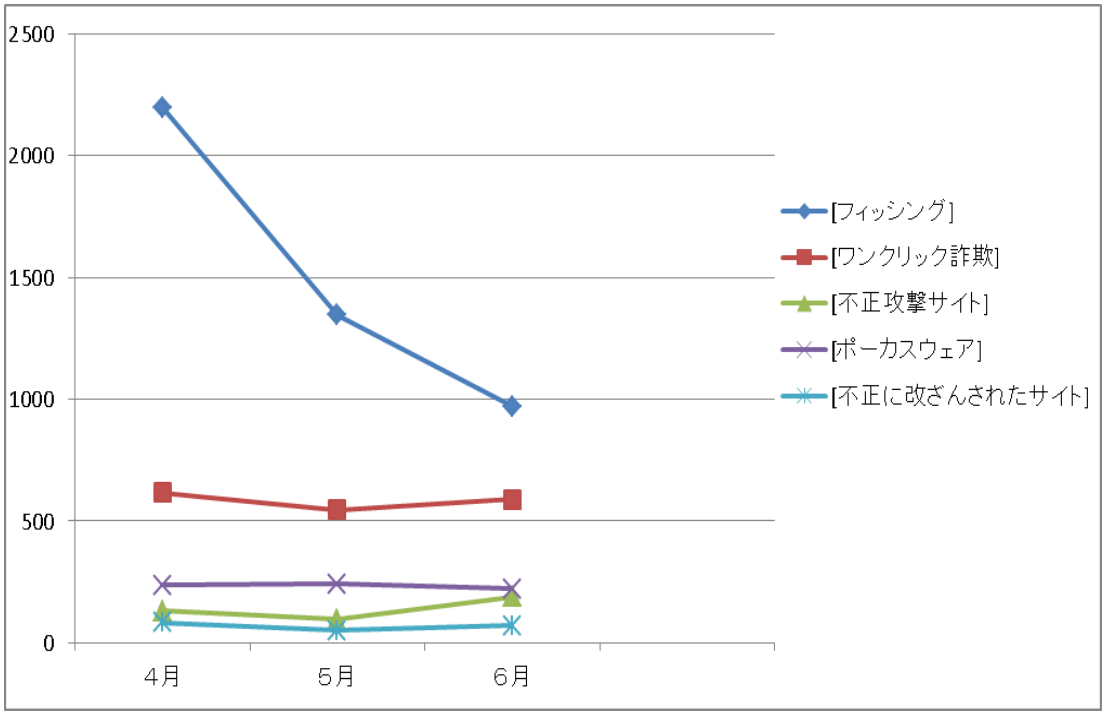
5. データからみるサイバー犯罪の傾向

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(2017 年 4 月～6 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、2016 年の平均である 2100 件と比較すると 4 月は 3300 件と約 1000 件上回っています。その後の 5 月から 6 月にかけて減少傾向にありますが、依然として過去 1 年の平均件数より多い状態が続いています。

フィッシングサイトの項目では、過去 1 年で最高の件数となった 1 月の 2000 件を上回り、4 月に 2200 件を記録しましたが、その後は減少傾向にあります。6 月には 1000 件と過去 1 年を下回る件数となっています。これは、3 月から増加していたマイクロソフトをかたるフィッシングが 4 月を機に減少したことが原因と考えられます。しかし、依然として Apple や LINE をかたるフィッシングは多く報告されており、金融機関や仮想通貨サービス業者をかたったものも報告されています。いずれもアカウントの不正利用の不安を煽り、個人情報の入力を促す手口です。

なお、フィッシングメールは週末を狙って送信される傾向にあるため、週末や週初めは特に注意が必要です。

6. 総括

今期も、前期より引き続き Apache Struts2 の脆弱性を狙った攻撃が発生しています。4 月には、チケット販売大手ぴあが運営を受託するバスケットボールリーグのチケット販売サイトとファンクラブ受付サイトが、Apache Struts2 の脆弱性を悪用した不正アクセスを受け、クレジットカード情報を含む個人情報約 15 万件が流出した可能性があることが判明しました。また、この事案が原因とみられるクレジットカードの不正利用が数十件発生しています。6 月には、同じ脆弱性を悪用した不正アクセスにより、国土交通省の「不動産取引価格アンケート回答サイト」に悪意のあるプログラムが仕込まれ、アンケート結果や登記情報など、合わせて最大約 20 万件流出した可能性があります。

5 月には、ランサムウェア「WannaCry」の感染が拡大し始め、述べ 159 か国 30 万台以上のコンピューターに感染しました。「WannaCry」はファイルを暗号化、復号する代わりに身代金を要求する従来のランサムウェアの機能に加え、ネットワーク経由で感染活動を行うワームとしての機能も有していることが今回の大規模感染に繋がったものと考えられます。

「WannaCry」の感染機能は Windows SMB 1.0 サーバの脆弱性を悪用するもので、インターネット上に公開されたアメリカ安全保障局が開発したとされる攻撃ツール「EternalBlue」を利用したとされています。今後も同攻撃ツールを利用し、情報を窃取するなどの新たな機能を備えたマルウェアが出現する可能性があります。実際に、6 月には「WannaCry」と同じ攻撃ツールを利用するランサムウェアである、「NotPetya」がウクライナを中心に感染が広がり、同国のインフラなどに大きな被害を出しました。その後も感染は拡大し、65 か国で感染が確認されています。

上記のサイバー攻撃事例で悪用された Apache Struts2、Windows SMB サーバの脆弱性は、いずれも大規模な感染や攻撃発生以前に修正プログラムが公開されています。マルウェアの感染やサイバー攻撃を防ぐためにも修正プログラムを早期に適用し、脆弱性対策を徹底することを推奨します。

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