S.S.R.C.定期
トレンドレポート
Vol.31

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.31

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 1 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：2017/1/1～2017/3/31

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	● Windows 10 Creators Update で追加されるセキュリティ機能たち（IT media） http://www.itmedia.co.jp/enterprise/articles/1701/10/news022.html ● Microsoft の月例セキュリティ情報は 4 件のみ、うち 1 件が「緊急」（IT media） http://www.itmedia.co.jp/news/articles/1701/11/news063.html ● 「Windows Essentials 2012」の配布とサポートが終了（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/1038422.html ● Microsoft、セキュリティ情報公開の方式を変更　2 月からはサマリー掲載廃止（IT media） http://www.itmedia.co.jp/news/articles/1701/17/news071.html ● 「Windows 7」のセキュリティは時代遅れ、今から移行準備を--独 MS（DZNet Japan） http://japan.zdnet.com/article/35095132/ ● Windows の未解決の脆弱性、次回月例更新プログラムで対処の見通し　危険度評価は引き下げ（IT media） http://www.itmedia.co.jp/news/articles/1702/06/news060.html ● Microsoft、月例セキュリティ更新プログラムの公開を延期（IT media） http://www.itmedia.co.jp/news/articles/1702/15/news062.html ● 「アンチウイルスソフトは死んだ」発言の真意は（IT media） http://www.itmedia.co.jp/enterprise/articles/1702/21/news035.html ● Microsoft の更新プログラム公開延期で相次ぐ未解決の脆弱性、今度は Edge と IE にも（IT media） http://www.itmedia.co.jp/news/articles/1702/27/news095.html ● Microsoft、2 月と 3 月の月例更新プログラムを併せて公開（IT media） http://www.itmedia.co.jp/enterprise/articles/1703/15/news055.html

2. Apple

関連記事	● Mac を狙うマルウェア、何年も前から密かに流通か（IT media） http://www.itmedia.co.jp/news/articles/1701/20/news064.html ● Apple、iOS や macOS Sierra をアップデート　多数の脆弱性を修正（IT media） http://www.itmedia.co.jp/enterprise/articles/1701/24/news059.html ● 「電車で見ず知らずの女性の名前を知る方法」が話題に　iPhone の機能「AirDrop」を悪用（IT media） http://www.itmedia.co.jp/news/articles/1701/30/news060.html ● 「iPhone」アクティベーションロック確認機能の削除はハッキング対策か（CNet Japan） https://japan.cnet.com/article/35095855/ ● Mac などのバックドアを指摘した善意のハッカーJonathan Zdziarski を Apple がセキュリティ部門に雇用（TechTarget） http://jp.techcrunch.com/2017/03/15/20170314apple-hires-security-researcher-jonathan-zdziarski/ ● ハッカー集団が Apple に身代金 10 万ドル要求、ユーザーの端末をリセットすると脅迫（IT media） http://www.itmedia.co.jp/news/articles/1703/23/news067.html ● CIA、Mac や iPhone 狙うマルウェア開発していた――告発サイト WikiLeaks が資料公表（IT media） http://www.itmedia.co.jp/news/articles/1703/24/news056.html ● Apple、脆弱性 84 件を修正した「iOS 10.3」と 127 件修正の「macOS Sierra 10.12.4」、38 件修正の「Safari 10.1」をリリース（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/1051684.html ● Safari から締め出して金銭を要求、iOS のポップアップ悪用する手口が横行（IT media） http://www.itmedia.co.jp/news/articles/1703/29/news072.html

3. Adobe

関連記事	● Adobe、Acrobat と Reader のセキュリティアップデートを予告（IT media） http://www.itmedia.co.jp/news/articles/1701/10/news052.html ● Flash Player の更新版、直ちに適用を　Acrobat／Reader の脆弱性も修正（IT media） http://www.itmedia.co.jp/enterprise/articles/1701/11/news059.html ● Windows 用 Chrome 拡張機能「Adobe Acrobat」に XSS の脆弱性（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/1040049.html ● 「Acrobat/Reader」更新の脆弱性対応件数が修正（Security NEXT） http://www.security-next.com/077663 ● Adobe、Flash Player などの脆弱性に対処　直ちに更新を（IT media） http://www.itmedia.co.jp/news/articles/1702/15/news063.html ● MS、定例外の修正パッチを急遽リリース - Adobe Flash Player の脆弱性に対処（Security NEXT） http://www.security-next.com/078785 ● Flash Player の深刻な脆弱性を修正、直ちに更新を（IT media） http://www.itmedia.co.jp/news/articles/1703/15/news056.html

4. Android

関連記事	● 1 月の Android 月例セキュリティ情報公開、94 の脆弱性を修正 (INTERNET Watch) http://internet.watch.impress.co.jp/docs/news/1037705.html ● Kaspersky Lab、Wi-Fi ルーターを狙う Android 向けトロイの木馬「Switcher Trojan」を発見（Kaspersky) http://www.kaspersky.co.jp/about/news/virus/2017/vir10012017 ● Android アプリに大手サービスの「鍵」をハードコード、AWS アカウントにアクセスも（IT media) http://www.itmedia.co.jp/news/articles/1701/18/news065.html ● Twitter アカウントに操作される――Android 版トロイの木馬「Twitoor」の恐怖 (TechTarget) http://techtarget.itmedia.co.jp/tt/news/1701/19/news03.html ● 「Android」を狙う新たなマルウェア--Flash のセキュリティアップデートを偽装 (CNet Japan) https://japan.cnet.com/article/35096674/ ● クルマの遠隔操作 Android アプリ、マルウェアに無防備な実態が判明（IT media) http://www.itmedia.co.jp/news/articles/1702/21/news057.html ● Google Play に 132 本の不正アプリ、開発環境を悪用する手口が浮上（IT media) http://www.itmedia.co.jp/news/articles/1703/03/news072.html ● Google、Android の月例セキュリティパッチ公開、多数の深刻な脆弱性を修正 (IT media) http://www.itmedia.co.jp/enterprise/articles/1703/08/news063.html ● 広告を悪用する Android マルウェア「Chamois」、Google が阻止（IT media) http://www.itmedia.co.jp/enterprise/articles/1703/14/news063.html ● Android 端末の約半数、2016 年中に更新されず（IT media) http://www.itmedia.co.jp/news/articles/1703/24/news059.html

5. 情報漏洩

関連記事	● 米国防総省の下請け企業から 11GB の機密情報が漏洩（マイナビニュース） http://news.mynavi.jp/news/2017/01/05/117/ ● イプサ、不正アクセスの調査結果を公表 - デバッグモードによりカード情報残存（Security NEXT） http://www.security-next.com/077978 ● 「闇ウェブ」の利用者データがハッキングで大量流出（IT pro） http://itpro.nikkeibp.co.jp/atcl/idg/14/481542/020800330/ ● 「SQLi 攻撃」で最大 13 万件の顧客情報が流出 - 日販グループ会社（Security NEXT） http://www.security-next.com/078416 ● １９９２人分流出　制度開始以来最大規模（毎日新聞） http://mainichi.jp/articles/20170217/k00/00e/040/153000c ● 米ヤフー、不正アクセス被害は3200万件--偽造クッキーでログイン（CNet Japan） https://japan.cnet.com/article/35097482/ ● 14 億人の個人情報、迷惑メール業者のバックアップファイルで露呈（IT media） http://www.itmedia.co.jp/news/articles/1703/07/news064.html ● 都税支払サイトからクレカ情報 67.6 万件が流出か - 「Apache Struts 2」の脆弱性突かれる（Security NEXT） http://www.security-next.com/079385 ● 不正アクセスによる個人情報漏洩で GMO-PG に報告を要請 - 経産省（Security NEXT） http://www.security-next.com/079955 ● JINS 通販サイトで個人情報が流出か - 「Apache Struts 2」脆弱性が再度原因に（Security NEXT） http://www.security-next.com/079944

6. 脆弱性

関連記事	● カスペルスキー、自社ウイルス対策ソフトの脆弱性に対処--Project Zero の指摘受け（DZNet Japan） http://japan.zdnet.com/article/35094566/ ● PHP メール送信用ライブラリ「PHPMailer」「SwiftMailer」「zend-mail」に、ほぼ同種の脆弱性（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/1037758.html ● 「BIND 9」に複数の深刻な脆弱性 - キャッシュ DNS サーバに影響（Security NEXT） http://www.security-next.com/077327 ● Oracle Java の脆弱性対策について(CVE-2017-3289 等) (IPA) http://www.ipa.go.jp/security/ciadr/vul/20170118-jre.html ● 内閣官房、マイナポータル環境設定プログラムに脆弱性と公表、再インストール求める（IT pro） http://itpro.nikkeibp.co.jp/atcl/news/17/012300189/?rt=nocnt ● Cisco 製品多数の部品に不具合　18 カ月たつと障害発生、復旧不可能に（IT media） http://www.itmedia.co.jp/enterprise/articles/1702/08/news069.html ● WordPress サイトの改ざん被害は 150 万件超に　「最悪級の脆弱性」（IT media） http://www.itmedia.co.jp/news/articles/1702/13/news045.html ● OpenSSL の更新版公開、危険度「高」の脆弱性に対処（IT media） http://www.itmedia.co.jp/news/articles/1702/17/news056.html ● 昨年末判明の「SKYSEA Client View」脆弱性 - 引き続き攻撃が発生中（Security NEXT） http://www.security-next.com/079300

	● 「Firefox 52」公開、非 HTTPS ページでの入力に警告　NPAPI プラグインは無効化（IT media） http://www.itmedia.co.jp/news/articles/1703/09/news070.html ● 米 Google、デスクトップ向けの「Chrome 57」安定版公開　36 件の問題を修正（IT media） http://www.itmedia.co.jp/news/articles/1703/13/news052.html ● Apache Struts 2 における脆弱性（S2-045、CVE-2017-5638)の被害拡大について（LAC） https://www.lac.co.jp/lacwatch/alert/20170310_001246.html ● Cisco IOS の重大な脆弱性、WikiLeaks 情報で発覚　数百種類のスイッチに影響（IT media） http://www.itmedia.co.jp/news/articles/1703/21/news061.html ● VMware、仮想マシン脱出の脆弱性を修正　Pwn2Own でハッキング実証（IT media） http://www.itmedia.co.jp/news/articles/1703/30/news008.html

7. サイバー攻撃

関連記事	● ハッカー集団 Carbanak のマルウェア、グーグルのサービス悪用—Forcepoint (DZNet Japan) http://japan.zdnet.com/article/35095222/ ● イタリアで発生したハッキング事例：「EyePyramid」（TREND Micro） http://blog.trendmicro.co.jp/archives/14329 ● サイバー犯罪を追い詰める法執行機関との協力：キーロガー「Limitless」の作成者、罪状を認める（TREND Micro） http://blog.trendmicro.co.jp/archives/14345 ● アパホテル予約サイト、1 週間ぶり復旧　「中国人の予約歓迎」「本は撤去しない」(IT media) http://www.itmedia.co.jp/news/articles/1701/25/news064.html ● 全国１８大学、サイト改ざん被害　１２月から１月に集中（朝日新聞） http://www.asahi.com/articles/ASK1T54BFK1TULZU007.html ● 選挙ハッキングをしているのは「秘密結社」か（IT media） http://www.itmedia.co.jp/business/articles/1702/02/news017.html ● 米 Yahoo!のアカウントに不正侵入の可能性、ユーザーに通知（IT media） http://www.itmedia.co.jp/news/articles/1702/16/news059.html ● 韓中外交摩擦がサイバー戦に発展か？（IT pro） http://itpro.nikkeibp.co.jp/atcl/column/14/549762/030700135/ ● 「Apache Struts 2」の脆弱性、一部代替パーサーでも攻撃が成立 (Security NEXT) http://www.security-next.com/079675 ● 国内 2 万台超の端末がマルウェア感染、ドイツで 600 万ユーロの被害を引き起こしたインターネットバンキング不正送金事案で（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/1050987.html

8. ランサムウェア

関連記事	● セキュリティ甘い「MongoDB」狙ったランサム攻撃が発生中（Security NEXT） http://www.security-next.com/077192 ● 4 種類のランサムウェア復号ツールをあらたに公開 – Avast (Security NEXT) http://www.security-next.com/077684 ● ロサンゼルスの単科大学がランサムウェアの身代金 300 万円を支払う (THE ZERO ONE) https://the01.jp/p0004179/ ● 高級ホテルでランサムウェア被害、宿泊客を部屋から閉め出し（IT media） http://www.itmedia.co.jp/news/articles/1701/31/news068.html ● ワシントンの防犯カメラにランサムウェア、ストレージの 7 割が感染　映像記録できない状態に（IT media） http://www.itmedia.co.jp/news/articles/1701/31/news067.html ● Netflix を「タダ見」できると誘引、実はランサムウェアを拡散（TREND Micro） http://blog.trendmicro.co.jp/archives/14390 ● 偽のランサムウェアで脅して身代金を要求、被害の実態は？--英調査 (DZNet Japan) https://japan.zdnet.com/article/35095582/ ● ランサムウェアで重要インフラが人質に取られる可能性--米大学が実験 (DZNet Japan) https://japan.zdnet.com/article/35096704/ ● 「TorrentLocker」が再び活発化、拡散手段を変えヨーロッパ主要国を攻撃対象に (TREND Micro) http://blog.trendmicro.co.jp/archives/14583 ● ランサムウェア「Cerber」が進化、機械学習利用のセキュリティツールから検出回避--トレンドマイクロ（DZNet Japan） https://japan.zdnet.com/article/35098898/

9. フィッシング

関連記事	● [更新] NEXON をかたるフィッシング（フィッシング対策評議会） http://www.antiphishing.jp/news/alert/nexon_20170113.html ● Amazon をかたるフィッシング（フィッシング対策評議会） http://www.antiphishing.jp/news/alert/amazon_20170131.html ● 2017/01 フィッシング報告状況（フィッシング対策評議会） http://www.antiphishing.jp/report/monthly/201701.html ● PayPal をかたるフィッシング（フィッシング対策評議会） http://www.antiphishing.jp/news/alert/paypal_20170203.html ● 「こんにちはクライアント」　Apple かたるフィッシングメールに注意 (IT media) http://www.itmedia.co.jp/news/articles/1702/07/news108.html ● 「Google Play」の日本語フィッシングサイト事例、SMS での誘導を確認 (TREND Micro) http://blog.trendmicro.co.jp/archives/14462 ● MyJCB をかたるフィッシング（フィッシング対策評議会） http://www.antiphishing.jp/news/alert/jcb_20170220.html ● 2017/02 フィッシング報告状況（フィッシング対策評議会） http://www.antiphishing.jp/report/monthly/201702.html ● [更新] LINE をかたるフィッシング（フィッシング対策評議会） http://www.antiphishing.jp/news/alert/line_20170316.html ● [更新] マイクロソフトをかたるフィッシング（フィッシング対策評議会） http://www.antiphishing.jp/news/alert/microsoft_20170317.html ● セゾン Net アンサーをかたるフィッシング（フィッシング対策評議会） http://www.antiphishing.jp/news/alert/saison_20170317.html ● ウェブマネーをかたるフィッシング（フィッシング対策評議会） http://www.antiphishing.jp/news/alert/webmoney_20170324.html

10. マルウェア

関連記事	● Cookie ヘッダーを用いて C&C サーバとやりとりするマルウェア ChChes (JPCERT) https://www.jpcert.or.jp/magazine/acreport-ChChes.html ● Google スプレッドシートを悪用してマルウェア制御、サイバー攻撃の手口が進化 (TechTarget) http://techtarget.itmedia.co.jp/tt/news/1702/02/news03.html ● マルウェアをメモリに隠す「目に見えない」攻撃手法が登場--140 以上の組織が被害に（DZNet Japan） https://japan.zdnet.com/article/35096314/ ● 人気の高いプラグインのフリをする JavaScript ベースマルウェア発見 (マイナビニュース) http://news.mynavi.jp/news/2017/02/11/117/ ● Windows で動作する「Mirai 拡散マルウェア」 - 中国語環境で作製 (Security NEXT) http://www.security-next.com/078917 ● Kaspersky Lab、データを破壊する新しいマルウェア「StoneDrill」を発見 (Kaspersky) http://www.kaspersky.co.jp/about/news/virus/2017/vir10032017 ● 新しい Linux マルウェア、CGI の脆弱性を利用（TREND Micro） http://blog.trendmicro.co.jp/archives/14577 ● ネットバンキングを狙う「DreamBot」が猛威　今すべき対策は（IT media） http://www.itmedia.co.jp/enterprise/articles/1703/22/news034.html ● Windows 上のアンチウイルスソフトをマルウェアに変えるゼロデイ脆弱性 (DZNet Japan) https://japan.zdnet.com/article/35098558/

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 1 月のウイルスレビュー

関連記事	● 2017 年 1 月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?i=11128

2. 2017 年 2 月のウイルスレビュー

関連記事	● 2017 年 2 月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?i=11187

3. 2017 年 3 月のウイルスレビュー

関連記事	● 2017 年 3 月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?i=11231

4. 2017 年 1 月のモバイルマルウェア

関連記事	● 2017 年 1 月のモバイルマルウェア（Dr. WEB） https://news.drweb.co.jp/show/review/?i=11125

5. 2017 年 2 月のモバイルマルウェア

関連記事	● 2017 年 2 月のモバイルマルウェア（Dr. WEB） https://news.drweb.co.jp/show/review/?i=11189

6. 2017 年 3 月のモバイルマルウェア

関連記事	● 2017 年 3 月のモバイルマルウェア（Dr. WEB） https://news.drweb.co.jp/show/review/?i=11233

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＜2017.01.02＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.01.02＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170102.html

2. チェックしておきたい脆弱性情報＜2017.01.09＞

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/memo20170109.html

3. チェックしておきたい脆弱性情報＜2017.01.16＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.01.16＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170116.html

4. チェックしておきたい脆弱性情報＜2017.01.23＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.01.23＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170123.html

5. チェックしておきたい脆弱性情報＜2017.01.30＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.01.30＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170130.html

6. チェックしておきたい脆弱性情報＜2017.02.06＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.02.06＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170206.html

7. チェックしておきたい脆弱性情報＜2017.02.13＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.02.13＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170213.html

8. チェックしておきたい脆弱性情報＜2017.02.20＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.02.20＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170220.html

9. チェックしておきたい脆弱性情報＜2017.02.27＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.02.27＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170227.html

10. チェックしておきたい脆弱性情報＜2017.03.06＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.03.06＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170306.html

11. チェックしておきたい脆弱性情報＜2017.03.13＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.03.13＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170313.html

12. チェックしておきたい脆弱性情報＜2017.03.20＞

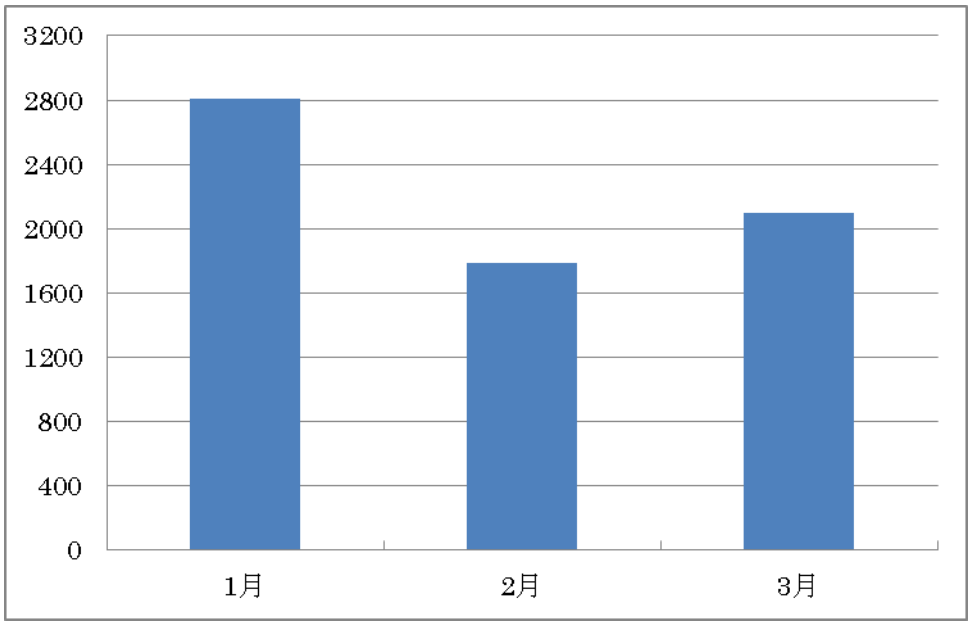
プレス リリース	● チェックしておきたい脆弱性情報＜2017.03.20＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170320.html

13. チェックしておきたい脆弱性情報＜2017.03.27＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.03.27＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20170327.html

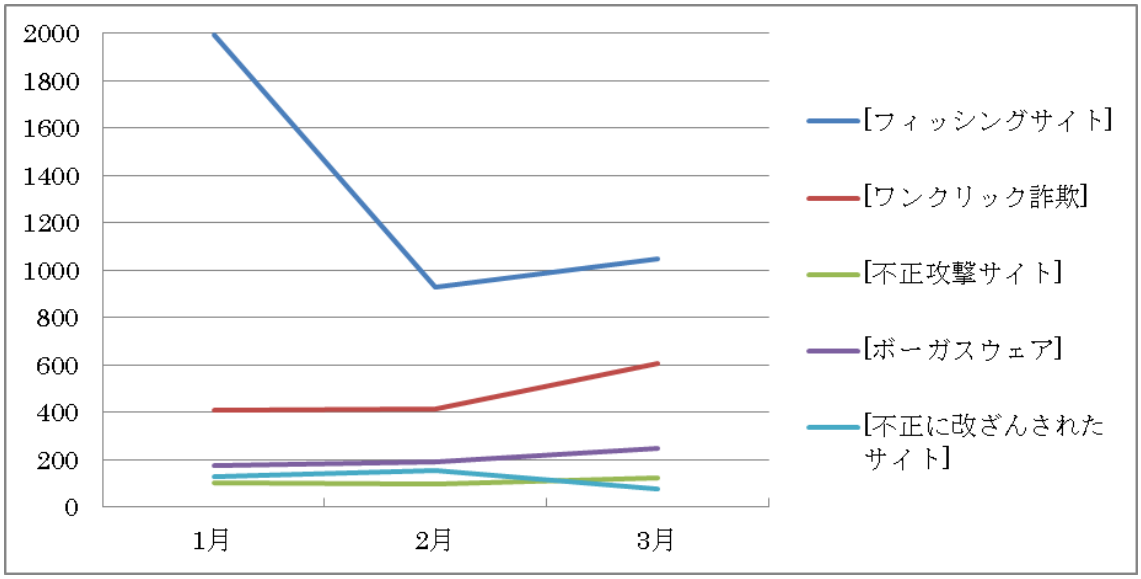
5. データからみるサイバー犯罪の傾向

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 1 月～3 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、過去 1 年の平均である 2100 件と比較すると 1 月は前期の 12 月に引き続き 2800 件と多くなっています。2 月、3 月には過去 1 年の平均である 2100 件を下回っています。

フィッシングサイトの項目で、1 月は過去 1 年で最高の件数となった 12 月の 1900 件を 100 件上回る 2000 件となっています。これは、12 月に引き続き 1 月は LINE、マイクロソフト、オンラインゲームなどをかたるフィッシングがそれぞれ増えていることが原因です。2 月、3 月には、過去 1 年の平均である 1200 件を下回る 1000 件になっています。これは、LINE や Apple をかたるフィッシングが減少していることが原因です。しかし、依然としてマイクロソフトをかたるフィッシングや新たにウェブマネー関連サービスのアカウント窃取を狙うフィッシングが報告されているので、今後も注意が必要です。また、ワンクリック詐欺の項目で、1 月、2 月は 400 件となっていますが、3 月は 600 件に増加しています。毎期、ワンクリック詐欺で報告されるのは、動画サイトが中心になっており、3 月に増加したワンクリック詐欺の多くも、特定の動画サイトが悪用される傾向にありました。

6. 総括

今期は 3 月から Apache Struts2 の脆弱性を悪用した攻撃による、不正アクセスの被害が多く報告されています。きっかけは、3 月 7 日に公開された「Jakarta Multipart parser のファイルアップロード処理に起因する、リモートで任意のコードが実行される脆弱性(CVE-2017-5638)」でした。Apache Struts2 とは、Web アプリケーションを簡単に構築できるフレームワークのことであり、Jakarta Multipart parser は、Apache Struts2 がクライアントのリクエストを処理する際に使用されるプログラムのことです。本脆弱性を悪用して不正なリクエストを送信することで、サーバ上で任意のコマンドを実行できてしまうというものです。被害状況として JETRO(日本貿易振興機構)サイトでは、一部情報を削除されメールアドレスを含むログ情報 2 万 6708 件、GMO ペイメントゲートウェイでは、クレジットカード情報が 67 万 6290 件流出した可能性があります。他にも複数の Web サイトが不正アクセスの被害に遭っており、現在も攻撃は続いています。サーバ管理者は身に覚えのないコマンドの実行やプロセスの停止、ファイルのダウンロードなどが行われていないかの確認をするとともに、Apache Struts2 およびインストールしているソフトウェアを管理し、最新バージョンにアップデートすることを推奨します。

2016 年後半から定期的に確認されていた日本語スパムメールが拡散する事例が、1 月より再び確認されています。この日本語スパムメールは、国内ネット銀行の利用者を狙う「URSNIF」や「DreamBot」と呼ばれるマルウェアに感染させることが目的です。メールの件名には、「請求書」や「注文書」など利用者を騙そうとする文言が使われています。感染手口としては、受信したメールの添付ファイルに、「.js」拡張子のスクリプトファイルや「.doc」拡張子のマクロ入り文書ファイルなどが含まれており、スクリプトファイルやマクロを実行してしまうと、外部サイトへ接続し「URSNIF」や「DreamBot」をダンロードして自動的に実行することで感染します。これらのマルウェアに感染した状態で国内ネット銀行を利用すると ID およびパスワードが窃取され、不正送金の被害につながる可能性があります。利用者は日本サイバー犯罪対策センター(JC3)(*1)などが注意喚起している情報を参考に、セキュティ対策の見直しをお勧めします。

(*1)日本サイバー犯罪対策センター 注意喚起情報(https://www.jc3.or.jp/info/heads-up.html)

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