S.S.R.C.定期
トレンドレポート
Vol.35

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.35

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 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：2018/1/1～2018/3/31

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	● マイクロソフト、一部 AMD チップ搭載 PC への CPU 脆弱性パッチを一時停止 https://japan.zdnet.com/article/35112915/ (ZDNet Japan) ● MS、ゼロデイ脆弱性の修正含む 1 月の月例パッチを公開 - 公開済み定例外パッチにも注意を http://www.security-next.com/089032 (Security NEXT) ● Windows 8.1 のメインストリームサポートが終了 完全なサポート終了は 2023 年 https://pc.watch.impress.co.jp/docs/news/1100559.html (PC Watch) ● 「Microsoft Office」の脆弱性を悪用するマルウェアが拡散中 https://japan.zdnet.com/article/35113478/ (ZDNet Japan) ● MS、インテルの「Spectre」向けフィックスを無効化する緊急アップデートを公開 https://japan.zdnet.com/article/35113900/ (ZDNet Japan) ● Microsoft、ユーザー脅して購入迫るプログラムを「迷惑プログラム」として削除へ http://www.itmedia.co.jp/enterprise/articles/1802/01/news067.html (ITMedia) ● MS、ブラウザ同梱版「Flash Player」向けに定例外更新 http://www.security-next.com/089956 (Security NEXT) ● Microsoft、2 月の月例セキュリティ更新プログラム公開　計 50 件の脆弱性を修正 http://www.itmedia.co.jp/news/articles/1802/14/news065.html (ITMedia) ● Microsoft、Intel の修正版対策パッチを Windows 10 向けにリリース http://www.itmedia.co.jp/news/articles/1803/02/news061.html (ITMedia) ● 2018 年 3 月のセキュリティ更新プログラム（月例） https://blogs.technet.microsoft.com/jpsecurity/2018/03/14/201803-security-updates/ (Microsoft) ● 「Windows 10」と「7」でマルウェア感染数に大差 https://japan.zdnet.com/article/35116730/ (ZDNet Japan)

2. Apple

関連記事	● Apple、プロセッサ脆弱性「Meltdown」と「Spectre」の対策について説明 http://www.itmedia.co.jp/news/articles/1801/05/news035.html (ITMedia) ● macOS 10.13.2 High Sierra でも実行可能な CPU 脆弱性「Spectre」の PoC が公開される https://applech2.com/archives/20180107-spectre-cve-2017-5753-poc-for-mac.html (APPL Ch.) ● 「macOS」でまたパスワード迂回の不具合 https://japan.cnet.com/article/35112998/ (cnet Japan) ● Mac ユーザーからマルウェア「Fruitfly」が 13 年にわたって何百万枚もの画像やキー入力情報を盗み続けていた http://gigazine.net/news/20180111-fruitfly-damage/ (GIGAZINE) ● Mac を狙う新手のマルウェア、DNS 設定乗っ取られる恐れ http://www.itmedia.co.jp/enterprise/articles/1801/16/news066.html (ITMedia) ● 特定の 1 文字で iPhone/Mac をクラッシュ可能な脆弱性 https://news.mynavi.jp/article/20180220-585563/ (マイナビニュース) ● Mac 狙うマルウェア「Coldroot」、2 年前から活動 https://japan.zdnet.com/article/35114997/ (ZDNet Japan)

3. Adobe

関連記事	● Adobe、「Flash Player」のセキュリティアップデートをリリース http://www.security-next.com/089026 (Security NEXT) ● 「Adobe Flash Player」にゼロデイ脆弱性 Adobe、修正版をリリースへ https://forest.watch.impress.co.jp/docs/news/1104489.html (窓の杜) ● Adobe、ゼロデイ脆弱性を修正した「Adobe Flash Player」v28.0.0.161 を緊急公開 https://forest.watch.impress.co.jp/docs/news/1105256.html (窓の杜) ● Flash ゼロデイ攻撃、北朝鮮攻撃グループ「TEMP.Reaper」が関与 - FireEye 分析 http://www.security-next.com/089920 (Security NEXT) ● 「Adobe Acrobat/Reader」にセキュリティ更新 - 脆弱性 41 件を修正 http://www.security-next.com/090090 (Security NEXT) ● 「Adobe Flash Player」に 2 件の深刻な脆弱性 - 悪用は未確認 http://www.security-next.com/091034 (Security NEXT)

4. Android

関連記事	● URLをクリックするだけで個人情報が抜き取られるAndroidアプリの脆弱性が中国で発覚 https://pc.watch.impress.co.jp/docs/news/1100391.html (PC Watch) ● 新手の Android スパイウェア「Skygofree」、ユーザー監視の高度な機能を実装 http://www.itmedia.co.jp/news/articles/1801/17/news054.html (ITMedia) ● 仮想通貨交換アプリの偽物が Google Play に出現 https://eset-info.canon-its.jp/malware_info/special/detail/180116.html（マルウェア情報局) ● Google、Android アプリのバグ発見に過去最大の報奨金 https://news.mynavi.jp/article/20180123-575118/ (マイナビニュース) ● Facebook の認証情報を窃取する Android 端末向け不正アプリ「GHOSTTEAM」を確認 http://blog.trendmicro.co.jp/archives/16857 (トレンドマイクロ) ● Google、Android の月例セキュリティ情報を公開　計 26 件の脆弱性を修正 http://www.itmedia.co.jp/enterprise/articles/1802/06/news057.html (ITMedia) ● 24 時間で 5000 台の Android 端末に感染して仮想通貨のマイニングを開始するマルウェアが報告される https://gigazine.net/news/20180206-android-devices-mining-botnet/ (GIGAZINE) ● 「Android」版トロイの木馬「AndroRAT」に新しい変種が登場 https://japan.zdnet.com/article/35114729/ (ZDNet Japan) ● 出荷時点で「トロイの木馬」に感染　40 モデル以上の Android デバイスで確認 http://www.itmedia.co.jp/news/articles/1803/05/news116.html (ITMedia) ● 3 月の Android セキュリティ情報公開、Media フレームワークなどに深刻な脆弱性 http://www.itmedia.co.jp/enterprise/articles/1803/06/news060.html (ITMedia)

5. 情報漏洩

関連記事	● 約 24 万人分の個人情報漏えい、米国土安全保障省が明らかに https://japan.zdnet.com/article/35112766/ (ZDNet Japan) ● 九州商船の予約サイトに不正アクセス、会員情報流出の可能性 - 不正ファイルが設置され外部通信 http://www.security-next.com/089021 (Security NEXT) ● 幻冬舎の Web サイト、不正アクセスで個人情報流出の可能性　対象は登録者 9 万人以上 http://nlab.itmedia.co.jp/nl/articles/1801/15/news139.html (ねとらぼ) ● GMO ペパボ「カラーミーショップ」に不正アクセス　クレジットカード情報が流出 http://www.itmedia.co.jp/news/articles/1801/26/news066.html (ITMedia) ● OnePlus のサイトから 4 万人のクレジットカード情報流出、カード不正利用の報告も http://www.itmedia.co.jp/news/articles/1801/22/news058.html (ITMedia) ● ポルシェジャパン、第三者の不正アクセスにより電子メールアドレス計 2 万 8722 件の顧客情報流出を確認 https://car.watch.impress.co.jp/docs/news/1108530.html (Car Watch) ● 米信用情報会社 Equifax の情報流出、さらに米国の 240 万人に影響 https://japan.zdnet.com/article/35115607/ (ZDNet Japan) ● 5000 万人分の個人情報が流出か　フェイスブック　トランプ氏ともつながりある英分析会社、データを不正に取得 https://www.nikkei.com/article/DGXMZO28345660200320180000000/ (日経) ● Walmart 協力企業から 130 万件の顧客情報流出、パスワードも漏洩 https://news.mynavi.jp/article/20180320-601721/ (マイナビニュース)

6. 脆弱性

関連記事	● IoT デバイスも対象、“現代的な”CPU の脆弱性「Meltdown」と「Spectre」 http://monoist.atmarkit.co.jp/mn/articles/1801/05/news062.html (MONOist) ● ウェブブラウザのパスワードマネージャーにユーザー情報を盗み出される脆弱性 https://gigazine.net/news/20180103-browser-flaw-steal-password/ (GIGAZINE) ● CPU 脆弱性対策パッチによる性能への影響、インテルがベンチマーク公開 https://japan.cnet.com/article/35113055/ (cnet Japan) ● Western Digital の NAS に固定パスワードのバックドア発見 https://news.mynavi.jp/article/20180110-569689/ (マイナビニュース) ● Oracle WebLogic Server に脆弱性攻撃--仮想通貨の発掘を狙う https://japan.zdnet.com/article/35113186/ (ZDNet Japan) ● 「BIND 9」にリモートより攻撃可能な脆弱性 - DoS 攻撃受けるおそれ http://www.security-next.com/089228 (Security NEXT) ● インテルの CPU 脆弱性対策パッチによる再起動の問題、新世代チップでも https://japan.cnet.com/article/35113389/ (cnet Japan) ● 「Electron」アプリに任意コードの実行を許す脆弱性　「Slack」や「Skype」に影響 Windows のみ、Mac/Linux には脆弱性の影響なし https://forest.watch.impress.co.jp/docs/news/1103480.html (窓の杜) ● シスコ「ASA」にリモートコード実行と DoS の脆弱性、至急適用を呼びかけ https://scan.netsecurity.ne.jp/article/2018/02/14/40591.html (ScanNetSecurity) ● 2 月 21 日ごろより「memcached」狙うアクセスが増加 - 悪用報告も http://www.security-next.com/090544 (Security NEXT) ● Intel、修正版対策パッチのリリース状況一覧を公開 http://www.itmedia.co.jp/enterprise/articles/1803/01/news064.html (ITMedia) ● Drupal、極めて重大な脆弱性を修正　直ちに対応を http://www.itmedia.co.jp/enterprise/articles/1803/29/news064.html (ITMedia)

7. サイバー攻撃

関連記事	● 北朝鮮、仮想通貨採掘でハッキング　韓国チームが分析 https://www.nikkan.co.jp/articles/view/00456415 (日刊工業新聞) ● 平昌五輪関連機関にサイバー攻撃 https://this.kiji.is/322651923956335713 (共同通信) ● コインチェック、ＮＥＭ約５８０億円分が不正に外部送金 https://www.sankei.com/affairs/news/180126/afr1801260067-n1.html (産経) ● 国立研究開発法人産業技術総合研究所に対する不正なアクセスに関する事案について http://www.aist.go.jp/aist_j/news/announce/au20180213.html (産総研) ● 4000以上の政府系サイトで閲覧者に対して仮想通貨マイニングを行わせるスクリプトが埋め込まれていたことが判明 https://gigazine.net/news/20180213-government-websites-hacked-for-mining/ (GIGAZINE) ● GitHub に過去最大級の DDoS 攻撃　Akamai の協力により約 8 分で復旧 http://www.itmedia.co.jp/news/articles/1803/02/news065.html (ITMedia) ● 1.7Tbps 規模の攻撃を確認、DDoS は「テラビット攻撃の時代」へ http://www.itmedia.co.jp/news/articles/1803/07/news065.html (ITMedia) ● 個人情報流出３０８万件　サイバー攻撃で８２組織から http://www.tokyo-np.co.jp/article/national/list/201804/CK2018040102000122.html (東京新聞)

8. ランサムウェア

関連記事	● NTT データ、社内システムが「WannaCry 2.0」亜種に感染するも駆除完了と公表 http://itpro.nikkeibp.co.jp/atcl/news/17/012202996/ (日経 xTECH) ● 偽の暗号通貨「SpriteCoin」で誘惑、ランサムウェア配布 https://japan.zdnet.com/article/35113599/ (ZDNet Japan) ● ランサムウェア攻撃者が身代金要求でビットコインを避ける動き?--その理由とは https://japan.zdnet.com/article/35113557/ (ZDNet Japan) ● ランサムウェア開発者のライフスタイル：メールインタビュー結果 https://scan.netsecurity.ne.jp/article/2018/01/25/40535.html (ScanNetSecurity) ● メールのばらまき型攻撃や WannaCry が定着、日本は突出 https://japan.zdnet.com/article/35113796/ (ZDNet Japan) ● ユーザーの 7 割はランサムウェア被害を知らず https://japan.zdnet.com/article/35114202/ (ZDNet Japan) ● 「No More Ransom」プロジェクト：ベルギー連邦警察がランサムウェア「Cryakl」の復号キーを公開 http://www.kaspersky.co.jp/about/news/virus/2018/vir23022018 (カスペルスキー) ● 2017 年の国内検出ランサムウェア、6 割が「WannaCrypt」 http://www.security-next.com/090622 (Security NEXT) ● ランサムウェアで身代金を払うと本当にデータは戻ってくる？ https://internet.watch.impress.co.jp/docs/yajiuma/1110904.html (Internet Watch) ● 約 5 万ドルの身代金：米アトランタ市、ランサムウェア攻撃で障害発生 http://www.itmedia.co.jp/news/articles/1803/23/news066.html (ITMedia) ● ボーイングに「WannaCry」ランサムウェア被害と報道 - 影響は限定的 https://japan.cnet.com/article/35116877/ (cnet Japan)

9. フィッシング

関連記事	● クレカ会社を装うフィッシング相次ぐ――MUFG カード、クレディセゾン、楽天カード http://security-t.blog.so-net.ne.jp/2018-01-23 (So-net) ● Apple をかたるフィッシングメール、18 万通以上を確認 https://internet.watch.impress.co.jp/docs/news/1102837.html (Internet Watch) ● フィッシング多発、アカウント不正利用で「キャリア決済」被害相次ぐ http://security-t.blog.so-net.ne.jp/2018-02-06 (So-net) ● 全国銀行個人信用情報センター」装う偽サイトに注意 - 「自宅に直接伺う」との記載も http://www.security-next.com/089961 (Security NEXT) ● フィッシング攻撃に注意、「ビジネスメール詐欺」の攻撃手口を分析 http://blog.trendmicro.co.jp/archives/17003 (トレンドマイクロ) ● Experty の ICO を狙うフィッシング詐欺--1600 万円相当の Ethereum が盗まれる https://japan.cnet.com/article/35113899/ (cnet Japan) ● Office 365 ユーザー、パスワード窃取詐欺の標的に https://news.mynavi.jp/article/20180306-594737/ (マイナビニュース) ● フィッシングの標的は仮想通貨の認証情報にシフト https://japan.zdnet.com/article/35116453/ (ZDNet Japan)

10. マルウェア

関連記事	● ファーウェイ製ルータの脆弱性を狙う「Satori」ボットネットのコードが公開 https://japan.zdnet.com/article/35112718/ (ZDNet Japan) ● 仮想通貨マイニング PC のウォレットアドレスを書き換えて採掘コインを根こそぎ奪う恐るべきマルウェア「Satori Coin Robber」 http://gigazine.net/news/20180120-satori-coin-robber/ (GIGAZINE) ● 政府機関などを狙うハッキング集団「Turla」がマルウェアを巧妙化 https://japan.zdnet.com/article/35113539/ (ZDNet Japan) ● 産業システムを狙うマルウェア「TRITON」--ゼロデイ脆弱性を利用 https://japan.zdnet.com/article/35113469/ (ZDNet Japan) ● 多方面に触手を伸ばす Necurs ボットネット https://gblogs.cisco.com/jp/2018/01/talos-the-many-tentacles-of-necurs-botnet/ (シスコ) ● 1 月マルウェアランキング、先月に続き仮想通貨マイナーが第 1 位 https://news.mynavi.jp/article/20180220-585333/ (マイナビニュース) ● 6 年以上もこっそりとルーターを介して拡散していたマルウェア「Slingshot」が特定される https://gigazine.net/news/20180313-slingshot-apt-through-router/ (GIGAZINE) ● 「Meltdown」「Spectre」を狙うマルウェアサンプル、大量に発見 https://japan.cnet.com/article/35114230/ (ZDNet Japan) ● 他人の PC で仮想通貨を勝手に採掘するマルウェア「Coinhive」の衝撃 https://forbesjapan.com/articles/detail/19534 (Forbes JAPAN) ● マルウェア「Zyklon」、Microsoft Office の脆弱性を悪用して拡散 https://news.mynavi.jp/article/20180119-573169/ (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1月のウイルスレビュー

関連記事	● 2018年1月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=11707

2. 2018年2月のウイルスレビュー

関連記事	● 2018年2月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=11746

3. 2018年3月のウイルスレビュー

関連記事	● 2018年3月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=11797

4. 2018年1月のモバイルマルウェア

関連記事	● 2018年1月のモバイルマルウェア（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=11710

5. 2018年2月のモバイルマルウェア

関連記事	● 2018年2月のモバイルマルウェア（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=11744

6. 2018年3月のモバイルマルウェア

関連記事	● 2018年3月のモバイルマルウェア（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=11800

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 ＜2018.01.08＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.01.08＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180108.html

2. チェックしておきたい脆弱性情報＜2018.01.15＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.01.15＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180115.html

3. チェックしておきたい脆弱性情報＜2018.01.22＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.01.22＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180122.html

4. チェックしておきたい脆弱性情報＜2018.01.29＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.01.29> http://www.hitachi.co.jp/hirt/publications/csirt/memo20180129.html

5. チェックしておきたい脆弱性情報＜2018.02.05＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.02.05＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180205.html

6. チェックしておきたい脆弱性情報＜2018.02.12＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.02.12＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180212.html

7. チェックしておきたい脆弱性情報＜2018.02.19＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.02.19＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180219.html

8. チェックしておきたい脆弱性情報＜2018.02.26＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.02.26＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180226.html

9. チェックしておきたい脆弱性情報＜2018.03.05＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.03.05＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180305.html

10. チェックしておきたい脆弱性情報＜2018.03.12＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.03.12＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180312.html

11. チェックしておきたい脆弱性情報＜2018.03.19＞

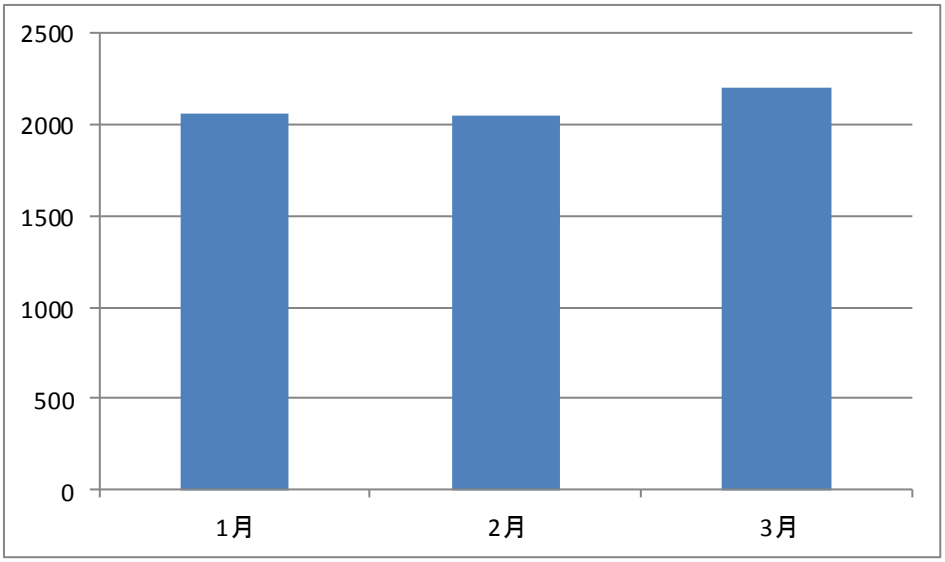
プレス リリース	● チェックしておきたい脆弱性情報＜2018.03.19＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180319.html

12. チェックしておきたい脆弱性情報＜2018.03.26＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.03.26＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180326.html

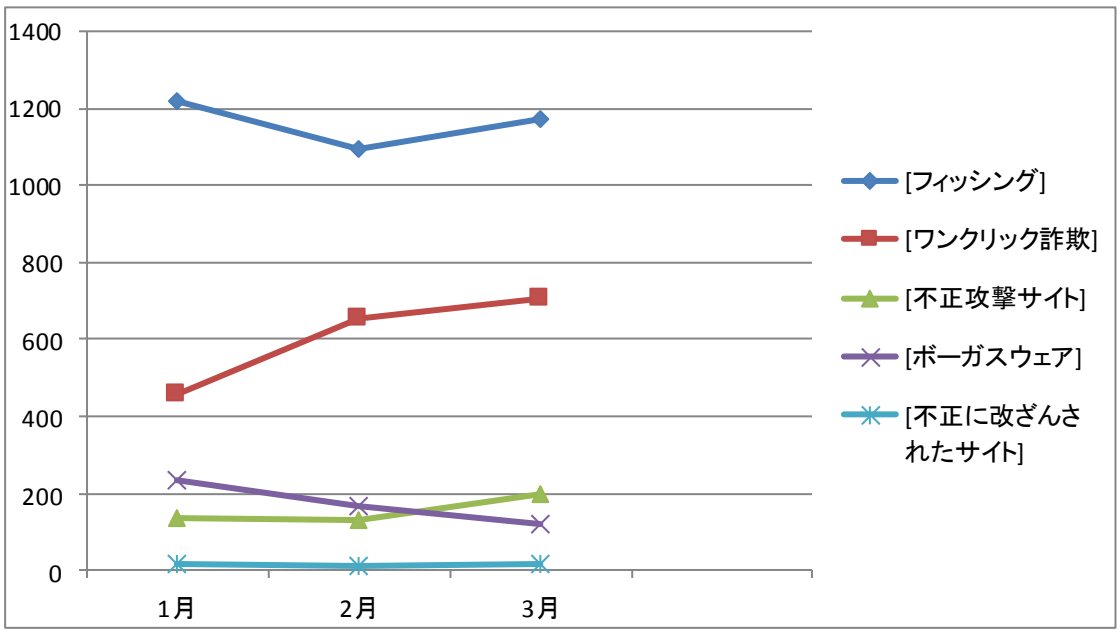
5. データからみるサイバー犯罪の傾向

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 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月平均で約 2100 件でした。過去 1 年の月平均である 2100 件と同水準となりました。

今期はワンクリック詐欺サイトの検知数が増加を続け、3 月は 704 件と 1 月の 458 件から 66%増加しました。一方、ボーガスウェアの検知数は減少傾向にあり、3 月は 118 件と 1 月の 233 件から 50%減少しました。不正攻撃サイトは 2 月の 129 件から 3 月は 196 件と検知数が 50%増加しています。

また、フィッシングの送信元として Netflix などのサブスクリプションサービスや、スマートフォンゲームで実際に行われているキャンペーンを装ったものが現れており(*1)、騙されないようより一層の注意が求められます。

(*2) https://www.antiphishing.jp/report/monthly/201802.html フィッシング対策協議会

6. 総括

前期から、仮想通貨を対象としたサイバー攻撃が流行しており、仮想通貨取引所のアカウント情報,、ウォレット情報、仮想通貨を採掘させるための計算資源などがマルウェアやフィッシングにより狙われています。特に、不正なスクリプトをウェブサイトに挿入し、閲覧者の計算資源を仮想通貨の採掘に利用するクリプトジャッキングと呼ばれる攻撃が多数発生し、Google は仮想通貨の広告と Chrome の拡張機能における仮想通貨の採掘機能の禁止を発表しました。1 月には日本の大手仮想通貨取引所、Coincheck が外部から不正アクセスを受け、580 億円分の仮想通貨が流出する事件も発生しています。仮想通貨に関連したサイバー攻撃は仮想通貨の相場と連動することが予想されるため、今後も継続して注意を払う必要があります。

脆弱性に焦点を当てると、1 月初めには CPU の投機的実行プロセスにおける脆弱性 Meltdown、Spectre が発覚しました。攻撃には対象のシステムにログインする必要があるものの、その影響範囲の広さに注目が集まりました。これに対して Intel が公開した修正パッチにより CPU の計算能力低下やシステムの再起動問題が発生したため、システム管理者はパッチ適用可否の判断に迫られました。正しい判断を下すためには、修正パッチを適用する場合、適用しない場合それぞれのリスクを評価する能力が求められます。

また、3 月には分散型メモリキャッシュシステム memcached の脆弱性を利用したリフレクション攻撃により、GitHub や米国のサービスプロバイダに対し最大 1Tbps を超える DDoS が発生しました。このように、攻撃が容易な脆弱性の放置は自身の機器やネットワークを侵害されるだけでなく、外部への攻撃に利用されてしまう恐れがあるため必ず対応を行ってください。

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