株式会社 日立システムズ

SSRC-TR-Vol.38

S.S.R.C.定期
トレンドレポート
Vol.38

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.トレンドレポート Vol.38

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 4 四半期版

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：2018/10/1～2018/12/31

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	● マイクロソフトがデジタル版ジュネーブ諸条約"実現に向け「Digital Peace Now」開始" https://japan.zdnet.com/article/35126400/ (ZDNET ジャパン) ● ファイルレス型のマルウェアに対抗--Windows 10 のセキュリティ対策事例 http://japan.zdnet.com/article/35126405/ (ZDNET ジャパン) ● Microsoft 製品の脆弱性対策について(2018 年 10 月) https://www.ipa.go.jp/security/ciadr/vul/20181010-ms.html (IPA) ● マイクロソフト、古い VLC を悪用した攻撃に注意喚起 https://news.mynavi.jp/article/20181112-721410/ (マイナビニュース) ● マイクロソフトの多要素認証サービス、再び障害が発生 https://japan.zdnet.com/article/35129291/ (ZDNET ジャパン) ● Microsoft、ログインシステムの重大バグを修正-2 段階認証の Office アカウントでも乗っ取れた https://jp.techcrunch.com/2018/12/12/2018-12-11-microsoft-login-bug-hijack-office-accounts/ (TechCrunch) ● MS、2018 年最後の月例セキュリティ更新 - 一部脆弱性でゼロデイ攻撃も http://www.security-next.com/100894 (securitynext) ● Microsoft、IE の臨時更新プログラムを公開 攻撃の発生を確認 http://www.itmedia.co.jp/news/articles/1812/20/news063.html (ITmedia) ● 「Windows」にゼロデイ脆弱性、PoC が公開 - 8 月の「ALPC 脆弱性」公表と同一人物 http://www.security-next.com/099305 (securitynext) ● Windows にゼロデイ脆弱性 - ALPC 脆弱性と同一人物が再度調整なしにコード公開 http://www.security-next.com/101276 (securitynext)

2. Apple

関連記事	● Apple、iOS と Windows 向け iCloud の脆弱性を修正 http://www.itmedia.co.jp/news/articles/1810/09/news060.html (ITmedia) ● アリペイ：ハッカーが盗んだアップル ＩＤ使い顧客資金を奪う https://www.bloomberg.co.jp/news/articles/2018-10-11/PGF7AT6TTDS401 （ブルームバーグ) ● Apple、macOS で「QuickTime 7」のサポートを終了」 https://internet.watch.impress.co.jp/docs/news/1147591.html（インターネットウォッチ) ● Apple、「iOS 12.1」をリリース - CVE 番号ベースで 32 件の脆弱性を修正 https://forest.watch.impress.co.jp/docs/news/1150743.html (窓の社) ● iOS メール App におけるサービス運用妨害（DoS）の脆弱性 https://jvn.jp/jp/JVN96551318/ (JVN) ● macOS や iOS など Apple の全 OS に深刻な脆弱性 https://pc.watch.impress.co.jp/docs/news/1151400.html (PC Watch) ● iPhone 上で削除したはずのデータを復元可能な脆弱性が見つかる https://gigazine.net/news/20181115-iphone-hacked-deleted-files/ (ギガジン) ● 「iTunes 12.9.2 for Windows」「iCloud for Windows 7.9」が公開 -8 件の脆弱性を修正 https://forest.watch.impress.co.jp/docs/news/1156932.html (窓の杜) ● Apple、「macOS Mojave 10.14.2」をリリース -機能を強化、不具合や脆弱性の修正も https://forest.watch.impress.co.jp/docs/news/1157052.html (窓の杜)

3. Adobe

関連記事	● 予告より 1 日前倒し、「Adobe Acrobat/Reader」アップデートが公開 - 脆弱性 86 件を修正 http://www.security-next.com/098518 (securitynext) ● Adobe Flash Player の脆弱性（APSB18-39）に関する注意喚起 http://www.jpcert.or.jp/at/2018/at180044.html (JPCERT) ● Adobe Acrobat および Reader の脆弱性（APSB18-40）に関する注意喚起 http://www.jpcert.or.jp/at/2018/at180045.html (JPCERT) ● 「Adobe Flash Player」に深刻な脆弱性 - 定例外アップデートが緊急リリース http://www.security-next.com/100211 (securitynext) ● ゼロデイ脆弱性を修正した「Adobe Flash Player 32」が公開 -攻撃への悪用も確認 https://forest.watch.impress.co.jp/docs/news/1156921.html (窓の社) ● 「Adobe Acrobat/Reader」、脆弱性 87 件に対処 - 当初予定より高い重要度 http://www.security-next.com/100884 (securitynext)

4. Android

関連記事	● Google、2018 年 10 月の Android セキュリティ情報を公開 フレームワーク関連の脆弱性に対処 http://www.itmedia.co.jp/enterprise/articles/1810/02/news057.html (ITmedia) ● 35 種類もの Android 向け偽装ウイルス対策アプリが発見される https://eset-info.canon-its.jp/malware_info/trend/detail/181018.html (キヤノン IT ソリューションズ) ● 継続する 5555/TCP ポート宛攻撃通信と ADB が有効化された脆弱な Android エミュレータについて https://blog.nicter.jp/2018/10/android-5555/ (NICTOR BLOG) ● Android の 2018 年 11 月セキュリティ情報が発表 - 任意コードが実行されてしまう脆弱性 https://forest.watch.impress.co.jp/docs/news/1151825.html (窓の社) ● Android/TimpDoor : モバイルデバイスをバックドアに変えるプロキシ型マルウェア https://blogs.mcafee.jp/android-timpdoor-backdoor (マカフィー) ● Android の 2018 年 12 月セキュリティ情報が発表 -メディアフレームワークに深刻な脆弱性 https://forest.watch.impress.co.jp/docs/news/1156503.html (窓の杜) ● Android 端末向け不正アプリ「XLOADER」と「FAKESPY」に類似点、中国のサイバー犯罪集団「Yanbian Gang」とのつながりを示唆 https://blog.trendmicro.co.jp/archives/19928 (トレンドマイクロ) ● 決済アプリから金を奪い取る悪質アプリ、アンドロイドで発見 https://forbesjapan.com/articles/detail/24442 (Forbes)

5. 情報漏洩

関連記事	● 聖教新聞通販サイトから個人情報 18 万件が流出か - 偽決済画面でクレカ情報の詐取も http://www.security-next.com/098808 (securitynext) ● Facebook の情報流出、影響は約 3000 万人-被害の詳細や経緯は https://japan.cnet.com/article/35126967/ (CNET ジャパン) ● 香港キャセイ航空で乗客データ流出 940 万人に影響か http://www.afpbb.com/articles/-/3194587 (AFPBBNews) ● 25 万人分の個人情報売りに　英航空大手から流出 https://www.nikkei.com/article/DGXMZO37733780U8A111C1000000/（日本経済新聞） ● マリオットの情報流出、5 億人に影響の恐れ--米でデータ保護関連法求める声も https://japan.cnet.com/article/35129495/ (CNET ジャパン) ● 任天堂グッズ販売 Web サイトへ 4 ヶ月にわたり不正アクセス、カード情報が流出（エディットモード） https://scan.netsecurity.ne.jp/article/2018/12/10/41710.html (scannetsecurity) ● 情報流出問題相次ぐ Facebook、今度は 680 万人の写真流出の恐れ http://japan.zdnet.com/article/35130196/ (ZDNET ジャパン) ● ベーシック、不正アクセスで約 40 万件の顧客情報が流出した可能性 https://japan.cnet.com/article/35130441/ (CNET ジャパン) ● 増え続けるデータ漏洩、漏洩数は 1 インシデント当たり 480 万件に到達 https://news.mynavi.jp/article/20181012-705099/ (マイナビニュース)

6. 脆弱性

関連記事	● セキュリティアップデート「Firefox 62.0.3」がリリース - 深刻な脆弱性 2 件を修正 http://www.security-next.com/098566 (securitynext) ● バージョン管理システム「Git」に任意コード実行の脆弱性、修正版が公開 https://forest.watch.impress.co.jp/docs/news/1146869.html (窓の杜) ● “VMware”シリーズの仮想化製品に未修正の脆弱性 - VMware が回避策を案内 https://forest.watch.impress.co.jp/docs/news/1147079.html (窓の杜) ● Oracle、Java やデータベースなど 301 件の脆弱性を修正 速やかに適用を http://www.itmedia.co.jp/news/articles/1810/17/news074.html (ITmedia) ● MIT、プロセッサ性能を犠牲にせず「Meltdown/Spectre」脆弱性を解決する新手法 https://pc.watch.impress.co.jp/docs/news/1148962.html (PC Watch) ● 「Firefox 63」公開 トラッキングの防止機能追加、危険度最高を含む 15 件の脆弱性に対処 http://www.itmedia.co.jp/news/articles/1810/24/news071.html (ITmedia) ● 「Apache Struts」のアップロード機能に深刻な脆弱性 - リモートよりコード実行のおそれ http://www.security-next.com/099681 (securitynext) ● JPCERT/CC のログ可視化ツールにコードインジェクションなど複数脆弱性 - 修正版がリリース http://www.security-next.com/099785 (securitynext) ● 「VirtualBox」にゼロデイ脆弱性 -ロシアのセキュリティ研究者が“GitHub”で明らかに https://forest.watch.impress.co.jp/docs/news/1152373.html (窓の杜) ● 「Spectre」「Meltdown」関連で新たに 7 件の脆弱性 http://www.itmedia.co.jp/news/articles/1811/15/news059.html (ITmedia)

7. サイバー攻撃

関連記事	● 銀行サイバー攻撃、関与の北朝鮮精鋭ハッカー集団を特定 米企業 http://www.afpbb.com/articles/-/3192045 (AFPBBNews) ● ロシアが「見境ない」サイバー攻撃、英国など非難声明 https://www.cnn.co.jp/tech/35126579.html (CNN) ● 防衛装備庁、サイバー攻撃受ける https://this.kiji.is/427749858595570785 (共同通信社) ● 「一国のほぼすべての銀行が顧客データ盗難の被害にあう」という衝撃のサイバー攻撃が発生 https://gigazine.net/news/20181107-almost-pakistani-banks-stolen-data/ (ギガジン) ● 豪企業を狙った中国のサイバー攻撃が急増、知財窃盗目的で 調査 http://www.afpbb.com/articles/-/3198461 (AFPBBNews) ● 独当局、ロシアのハッカー集団によるサイバー攻撃検知 https://jp.reuters.com/article/germany-cyber-russia-idJPKCN1NZ0EE (ロイター) ● Quora、約 1 億人に影響のサイバー攻撃　該当者にはメールで通知済み http://www.itmedia.co.jp/news/articles/1812/04/news075.html (ITmedia) ● 米共和党にサイバー攻撃 https://this.kiji.is/442784882596381793 (共同通信社) ● 米海軍の下請け業者などにサイバー攻撃か http://www.news24.jp/articles/2018/12/15/10411862.html (日テレ NEWS24) ● 中国のサイバー攻撃、12 カ国に被害 米司法省発表 https://www.nikkei.com/article/DGXMZO39229080R21C18A2000000/ (日本経済新聞) ● 「APT10」によるサイバー攻撃に強い懸念、各国の発表を支持（NISC） https://scan.netsecurity.ne.jp/article/2018/12/25/41776.html (scannetsecurity)

8. ランサムウェア

関連記事	● ボットネットによる拡散機能を備えた暗号化型ランサムウェア「Viro」を確認 https://blog.trendmicro.co.jp/archives/19664 (トレンドマイクロ) ● ランサムウェア「GandCrab」に無料の復号ツール - 被害者は推計 50 万人 http://www.security-next.com/099368 (securitynext) ● ランサムウェア「GandCrab」対応復号ツール、100 万ドル超の被害回避 - Bitdefender 報告 https://japan.zdnet.com/article/35127946/ (ZDNET ジャパン) ● ランサムウェアで病院や公共機関を脅迫、米司法省がイラン人 2 人の起訴を発表 http://www.itmedia.co.jp/news/articles/1811/29/news085.html (ITmedia) ● 中国で 10 万台以上のコンピューターがデータを暗号化するランサムウェアに感染、「WeChat で 1800 円払え」と要求 https://gigazine.net/news/20181206-wechat-payment-ransomware-infect-china/ (ギガジン)

9. フィッシング

関連記事	● 日本など 14 カ国の大学を狙う大規模攻撃 - 論文 DB 装うフィッシングで知的財産を標的に http://www.security-next.com/099256 (securitynext) ● 大学 Web メール狙うフィッシング増加、独自のデザインも模倣（IPA） https://scan.netsecurity.ne.jp/article/2018/11/01/41563.html (scannetsecurity) ● Kaspersky Lab、米英など 16 か国で大学の認証情報を狙ったフィッシング詐欺を検知 https://www.kaspersky.co.jp/about/press-releases/2018_vir06112018（カスペルスキー） ● 3D セキュア（本人認証サービス）の認証情報を詐取することを目的としたフィッシング（2018/11/09） http://www.antiphishing.jp/news/alert/3dsecure_20181109.html（フィッシング対策協議会） ● Gmail に差出人を空欄にできるバグ「Ghost Emails」 - フィッシング攻撃などで悪用のおそれ http://www.security-next.com/100400 (securitynext) ● 学生がフィッシング被害、迷惑メール約 29 万件の踏み台に - 新潟大 http://www.security-next.com/100745 (securitynext) ● Gmail や Yahoo!メールの 2 段階認証を無効化するフィッシング詐欺が横行している https://gigazine.net/news/20181214-iranian-phisher-bypass-2fa-protection/（ギガジン） ● 乗っ取られた日本のサーバからフィッシングメール送信 https://news.mynavi.jp/article/20181217-740889/ (マイナビニュース)

10. マルウェア

関連記事	● 「TRITON」マルウェア利用の ICS 攻撃にロシアの国有研究機関が関与か -FireEye 報告 http://japan.zdnet.com/article/35127532/ (ZDNET ジャパン) ● Windows の正規機能 WMIC および CertUtil を利用しブラジルのユーザを狙うマルウェアを確認 https://blog.trendmicro.co.jp/archives/19759 (トレンドマイクロ) ● マルウェア「Emotet」に大きな変化、電子メールメッセージを大量収集 http://japan.zdnet.com/article/35128040/ (ZDNET ジャパン) ● ロシアの仮想通貨マイニングマルウェア WebCobra を発見 https://blogs.mcafee.jp/webcobra-malware-uses (マカフィー) ● 国際的慈善団体のウェブサイトに仮想通貨マイニング・マルウェア、サイバーセキュリティ企業が検知 https://jp.cointelegraph.com/news/cybersecurity-firm-detects-cryptojacking-malware-on-make-a-wish-foundation-website (コインテレグラフ) ● Linux サーバに焦点を絞ったマルウェア「Mirai」登場、大規模 DDoS の可能性 https://news.mynavi.jp/article/20181125-728709/ (マイナビニュース) ● Linux を狙う仮想通貨発掘マルウェアを確認、ルートキットを利用し活動を隠ぺい https://blog.trendmicro.co.jp/archives/19844 (トレンドマイクロ) ● 流行マルウェア「EMOTET」の内部構造を紐解く https://www.mbsd.jp/blog/20181225_2.html (三井物産セキュアディレクション)

11. その他

関連記事	● 爆破予告とセクストーション詐欺の関連性 https://gblogs.cisco.com/jp/2018/12/talos-bitcoin-bomb-scare-associated-with/ (CISCO) ● 10 月も継続した「セクストーション」スパム、総被害額は 1,000 万円を突破か https://blog.trendmicro.co.jp/archives/19824 (トレンドマイクロ) ● 「アダルトサイト閲覧」で脅す脅迫メールに新展開、ランサムウェアを配布 https://securitynews.so-net.ne.jp/news/sec_00011.html (So-net) ● セクストーション詐欺の分析 https://gblogs.cisco.com/jp/2018/11/talos-anatomy-of-sextortion-scam/ (CISCO) ● 「アダルトサイト経由のハッキング」で脅す詐欺メール、12 日間で 250 万円を詐取か https://blog.trendmicro.co.jp/archives/19682 (トレンドマイクロ)

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 10 月のウイルスレビュー

関連記事	● 2018 年 10 月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=12898

2. 2018 年 11 月のウイルスレビュー

関連記事	● 2018 年 11 月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=12965

3. 2018 年 12 月のウイルスレビュー

関連記事	● 2018 年 12 月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=13030

4. 2018 年 10 月のモバイルマルウェア

関連記事	● 2018 年 10 月のモバイルマルウェア（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=12914

5. 2018 年 11 月のモバイルマルウェア

関連記事	● 2018 年 11 月のモバイルマルウェア（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=12967

6. 2018 年 12 月のモバイルマルウェア

関連記事	● 2018 年 12 月のモバイルマルウェア（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=13028

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 ＜2018.10.01＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.10.01＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20181001.html

2. チェックしておきたい脆弱性情報＜2018.10.08＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.10.08＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20181008.html

3. チェックしておきたい脆弱性情報＜2018.10.15＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.10.15＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20181015.html

4. チェックしておきたい脆弱性情報＜2018.10.22＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.10.22> http://www.hitachi.co.jp/hirt/publications/csirt/memo20181022.html

5. チェックしておきたい脆弱性情報＜2018.10.29＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.10.29＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20181029.html

6. チェックしておきたい脆弱性情報＜2018.11.05＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.11.05＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20181105.html

7. チェックしておきたい脆弱性情報＜2018.11.12＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.11.12＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20181112.html

8. チェックしておきたい脆弱性情報＜2018.11.19＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.11.19＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20181119.html

9. チェックしておきたい脆弱性情報＜2018.11.26＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.11.26＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20181126.html

10. チェックしておきたい脆弱性情報＜2018.12.03＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.12.03＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20181203.html

11. チェックしておきたい脆弱性情報＜2018.12.10＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.12.10＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20181210.html

12. チェックしておきたい脆弱性情報＜2018.12.17＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.12.17＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20181217.html

13. チェックしておきたい脆弱性情報＜2018.12.24＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.12.24＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20181224.html

14. チェックしておきたい脆弱性情報＜2018.12.31＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.12.31＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20181231.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ティサービス(*1)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図1に、脅威別検知数の月別推移(2018年)を図2に示します。

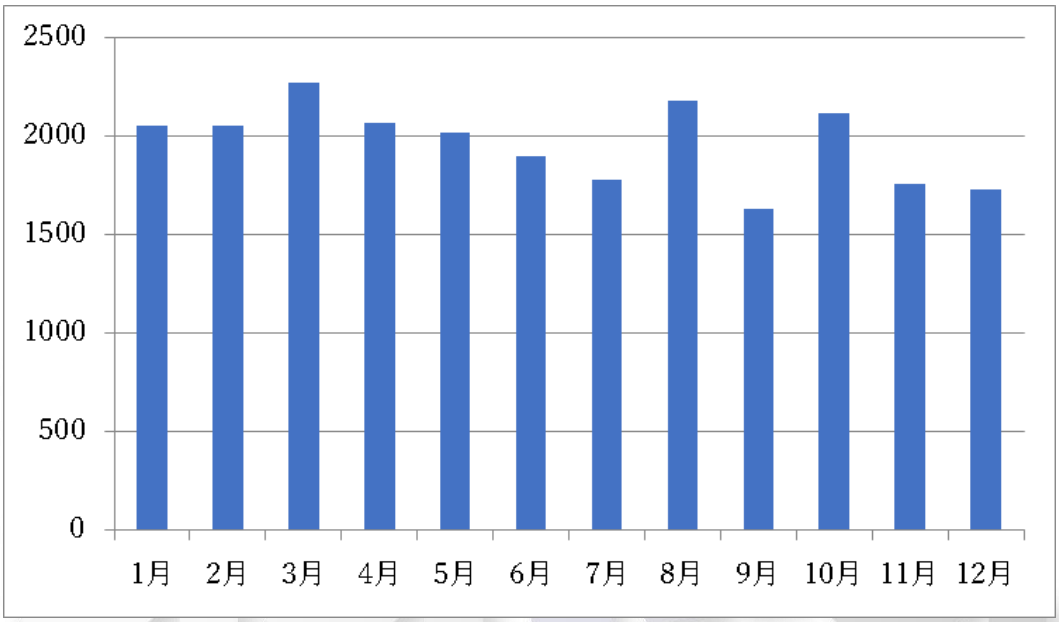

図1 「危険な可能性」と判断されたウェブサイトの件数(2018年)

(*1)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/)

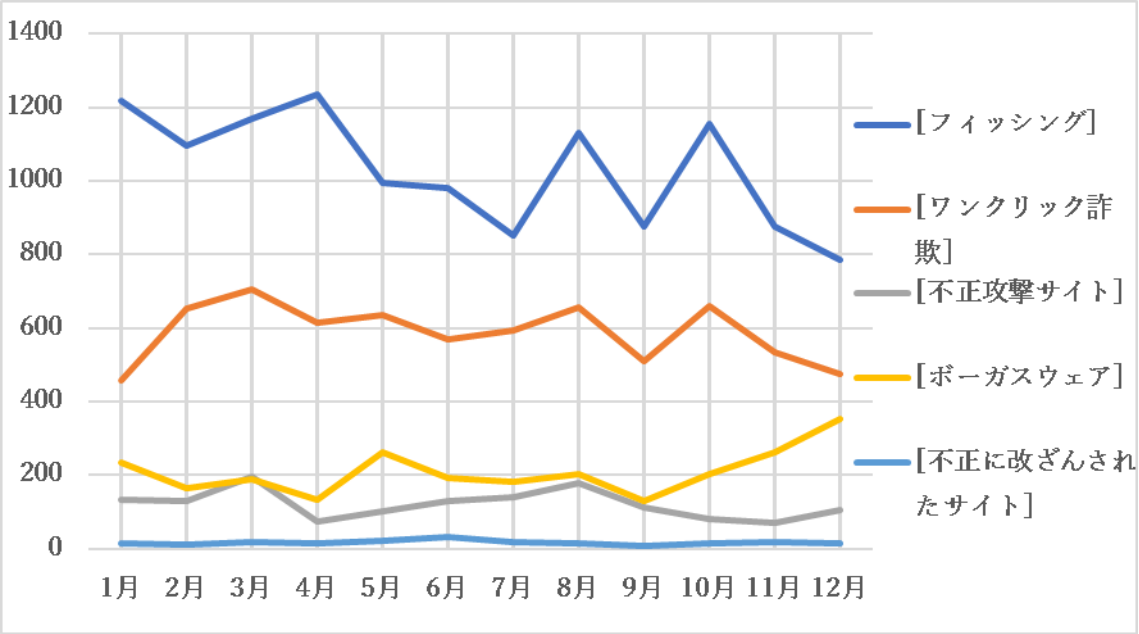

図 2 脅威別検知数の月別推移(2018 年)

10 月～12 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 1870 件でした。2018 年の月平均である約 1960 件と比較すると、5%減少しています。フィッシングの可能性があると判断されたウェブサイトの件数は 10 月に増加し、約 1160 件に上りました。その後、11 月と 12 月にはフィッシングサイトの検知数は減少しております。また、本四半期ではボーガスウェアの検知数増加を確認しております。

フィッシング対策協議会が公開したレポートによると(*2)、フィッシング報告件数は 10 月に減少したものの、本四半期を通して増加傾向にあります。仮想通貨を要求する脅迫メールやプレゼントが当選したと偽り料金がかかるサービスへ登録させる当選詐欺の報告が増えています。

(*2)フィッシング対策協議会 2018/12 フィッシング報告状況

(https://www.antiphishing.jp/report/monthly/201812.html)

6. 総括

本四半期には、「アダルトサイトの閲覧した際に撮影した動画を流布する」と脅し金銭を要求する脅迫メールを送り付ける、セクストーション(性的脅迫)に関するニュースが多数発表されました。この性的脅迫メールでは信憑性を高めるために受信者が実際に使用していると考えられるパスワードを記載する手法も確認しています。そのうえ、日本語での性的脅迫メールの大量送信は 2018 年 10 月に 12 回行われ、約 5 万 2,000 通が拡散されました。その結果、9 月中旬にこの手法が登場してから 10 月末日までに総被害額が 1000 万円を突破しました。また 12 月には、動画を撮影した証拠と偽ってランサムウェア「GandCrab」に感染させようとする手法も確認されています。今後、手口が巧妙化し、日本国内における被害の増加が想定されます。

12 月の初めに、大手ホテルチェーンの Marriot から約 5 億人分の個人情報が漏洩したと発表がありました。調査結果によると Marriot 傘下の Starwood のネットワークに対し 2014 年から不正なアクセスがあったとのことです。また、漏洩した情報は約 1 億 7,000 万人の名前と住所、メールアドレスといった基本情報、3 億 2,700 万人は基本情報に加えて電話番号やパスポート番号などとなっています。本四半期には、キャセイ空港から 940 万人の個人情報、Facebook から 680 万人の写真の流出が確認されています。このような情報漏洩事故を発生させた場合には経済的損失だけでなく、社会的信用を失い企業イメージを損なってしまいます。そのため、情報漏洩を防ぐ対策と漏洩した際の二次災害を防ぐことが重要となります。

株式会社　日立システムズ

〒141-8672 東京都品川区大崎 1-2-1

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

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