株式会社 日立システムズ

SSRC-TR-Vol.37

S.S.R.C.定期
トレンドレポート
Vol.37

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.37

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 3 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：2018/7/1～2018/9/30

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 が「アメリカ中間選挙の候補者をハッカーが狙っている」兆候を発見 https://gigazine.net/news/20180720-microsoft-reveal-midterm-campaing-hacking/ (ギガジン) ● Microsoft Office の脆弱性、バックドアの感染に使われる https://news.mynavi.jp/article/20180730-670512/ (マイナビニュース) ● Microsoft の VBScript にゼロデイ脆弱性、北朝鮮のハッカー集団が悪用か https://gigazine.net/news/20180820-microsoft-vbscript-darkhotel-apt/ (ギガジン) ● VBScript エンジンのメモリ解放後使用（Use After Free）の脆弱性「CVE-2018-8373」により、IE でシェルコードの実行が可能に https://blog.trendmicro.co.jp/archives/19457 (トレンドマイクロ) ● 米保守派団体サイト狙ったロシア系ハッカーを阻止＝マイクロソフト https://jp.reuters.com/article/usa-russia-hackers-idJPKCN1L60QL (ロイター) ● Microsoft、Spectre V3a/4 と L1TF 脆弱性対策の Intel CPU 向けマイクロコード更新を公開 https://forest.watch.impress.co.jp/docs/news/1139097.html (窓の社) ● 7 月の MS 月例パッチが公開、脆弱性 53 件を修正 - 「緊急」は 17 件 http://www.security-next.com/095589 (securitynext) ● MS、8 月の月例パッチ公開 - 脆弱性 2 件でゼロデイ攻撃 http://www.security-next.com/096790 (securitynext) ● MS、月例パッチで脆弱性 62 件を修正 - 「Windows ALPC」のゼロデイ脆弱性に対応 http://www.security-next.com/097872 (securitynext) ● Windows タスクスケジューラのゼロデイ脆弱性、回避策が公開 - 独自パッチも http://www.security-next.com/097556 (securitynext)

2. Apple

関連記事	● Apple、「Boot Camp」向けに脆弱性「KRACK」対策のアップデート http://www.security-next.com/095436 (securitynext) ● Apple、Mac 向けにセキュリティアップデート - 「Safari」最新版も http://www.security-next.com/095515 (securitynext) ● Apple、「iOS 11.4.1」をリリース - 脆弱性 22 件を修正 http://www.security-next.com/095511 (securitynext) ● Apple Watch 初のジェイルブレイク(脱獄)コード「JelbrekTime」がリリースされる https://gigazine.net/news/20180806-apple-watch-jelbrektime/ (ギガジン) ● Kaspersky Lab、サイバー犯罪組織 Lazarus が macOS 向けマルウェアを使用し仮想通貨取引所を攻撃する「AppleJeus」を発見 https://prtimes.jp/main/html/rd/p/000000094.000011471.html (PRTIMES) ● MacAppStore ランキング上位の「Adware Doctor」というアプリにユーザーのブラウザ履歴を収集し中国のサーバーへ送信する機能が発見され、Apple が Store から削除。 https://applech2.com/archives/20180908-adware-doctor-steal-mac-user-browser-history.html (AAPLCh.) ● macOS に未解決の脆弱性、クリック操作偽造の恐れ http://www.itmedia.co.jp/news/articles/1808/14/news041.html (ITmedia) ● Apple、「iTunes 12.9 for Windows」で修正した脆弱性の内容を発表 - CVE 番号ベースで 19 件の脆弱性を修正 https://forest.watch.impress.co.jp/docs/news/1145009.html (窓の社) ● Apple、「macOS Mojave 10.14」をリリース - 脆弱性 8 件に対処 http://www.security-next.com/098223 (securitynext)

3. Adobe

関連記事	● 「Adobe Acrobat/Reader」に複数の深刻な脆弱性 - 7 月 10 日にアップデート予定 http://www.security-next.com/095392 (securitynext) ● 「Adobe Acrobat/Reader」に 51 件の深刻な脆弱性 - あわせて 100 件以上を修正 http://www.security-next.com/095582 (securitynext) ● 「Adobe Acrobat/Reader」に深刻な脆弱性 - パッチ公開は 8 月 14 日を予定 http://www.security-next.com/096697 (securitynext) ● 「Adobe Flash Player」のアップデートがリリース - 脆弱性 5 件を解消 http://www.security-next.com/096775 (securitynext) ● 「Adobe Photoshop CC」に Critical な脆弱性が 2 件、修正版が公開 https://forest.watch.impress.co.jp/docs/news/1139126.html (窓の社) ● 「Adobe Acrobat/Reader」既知脆弱性の実証コードが公開 http://www.security-next.com/098271 (securitynext)

4. Android

関連記事	● Android 月例セキュリティ情報公開、複数の深刻な脆弱性に対処 http://www.itmedia.co.jp/enterprise/articles/1807/03/news068.html (ITmedia) ● Android 狙う情報窃取アプリ、SMS で拡散 - 銀行アプリを偽物に置換 http://www.security-next.com/095424 (securitynext) ● Google Play で配信されたスパイウェア「Android/FoulGoal.A」にイエローカード！ https://blogs.mcafee.jp/google-play-users-risk (マカフィー) ● ステルス機能備えた Android アドウェア「MobiDash」に注意 https://news.mynavi.jp/article/20180725-668914/ (マイナビニュース) ● Google、Android の月例セキュリティ情報を発表 -リモートコード実行などを修正 https://forest.watch.impress.co.jp/docs/news/1137180.html (窓の社) ● Android が狙われる「Man-in-the-Disk」攻撃--SD カード経由でスマホに不正侵入 https://japan.cnet.com/article/35124146/ (CNET ジャパン) ● Android 端末の ADB ポートが「Mirai」の亜種「Satori」の拡散に利用されていることを確認 https://blog.trendmicro.co.jp/archives/19433 (トレンドマイクロ) ● Google、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/news/articles/1809/05/news063.html (ITmedia) ● 決済時の認証情報を盗むマルウェア、「Google Play」上のアプリで検出 https://japan.zdnet.com/article/35122354/ (ZDNET ジャパン)

5. 情報漏洩

関連記事	● IPA、情報漏洩の防止マニュアルを拡充 -「Windows 10」「Office 2016」などの解説を追加 https://forest.watch.impress.co.jp/docs/news/1141453.html (窓の社) ● 日本ネットワークセキュリティ協会／情報流出発覚に平均 100 日／情報漏洩時の対応セミナー開催 https://www.bci.co.jp/netkeizai/article/4305 (日流ウェブ) ● Mozilla、情報漏洩をチェックできる「Firefox Monitor」提供開始 https://japanese.engadget.com/2018/09/26/mozilla-firefox-monitor/ (engadget) ● マーケティング企業のデータベースサーバから 1100 万件の個人情報が流出 https://japan.zdnet.com/article/35125806/ (ZDNET ジャパン) ● British Airways の情報流出、Ticketmaster 事件のハッカーグループが関与か https://japan.zdnet.com/article/35125475/ (ZDNET ジャパン) ● 監視アプリの「mSpy」が数百万人分の顧客情報を流出、3 年で 2 度目の大規模漏えい https://gigazine.net/news/20180905-mspy-leaks-millions-sensitive-records/ (ギガジン) ● 中国の大手ホテル Huazhu 1 億 3000 万人の宿泊客情報が流出か http://www.itmedia.co.jp/news/articles/1808/30/news067.html (ITmedia) ● SNS の個人情報 30 億件流出 現地 IT 企業トップ首謀 https://www.sankeibiz.jp/macro/news/180829/mcb1808290500001-n1.htm (産経)

6. 脆弱性

関連記事	● Oracle、四半期定例パッチをリリース - 脆弱性 334 件を修正 http://www.security-next.com/095793 (securitynext) ● 続報：IoT ボット「VPNFilter」に感染したデバイスで 19 件の脆弱性を確認 https://blog.trendmicro.co.jp/archives/19349 (トレンドマイクロ) ● 「Knot Resolver」に脆弱性 - DNS キャッシュポイズニングのおそれ http://www.security-next.com/096476 (securitynext) ● 「Samba」に 5 件の脆弱性 - 制御奪取や情報漏洩のおそれ http://www.security-next.com/096817 (securitynext) ● 「パスワードマネージャー」に脆弱性、プロセス間通信を悪用される恐れ http://www.atmarkit.co.jp/ait/articles/1808/20/news038.html (@IT) ● Apache Struts 2 におけるリモートコード実行に関する脆弱性（CVE-2018-11776）（S2-057）についての検証レポート http://www.intellilink.co.jp/article/vulner/180830.html (NTT データ先端技術株式会社) ● 深刻な脆弱性に対処した「Ghostscript 9.24」が前倒しで公開 - アップデートを強く推奨 http://www.security-next.com/097720 (securitynext) ● 「FragmentSmack」脆弱性、80 を超えるシスコ製品に影響 https://japan.zdnet.com/article/35126193/ (ZDNET ジャパン) ● Linux カーネルに脆弱性「Mutagen Astronomy」、PoC が公開 - 「RHEL」「CentOS」に影響 http://www.security-next.com/098324 (securitynext) ● 「Apache Struts 2」の脆弱性、クリプトジャッキング攻撃の標的に--Linux マシンに影響 https://japan.zdnet.com/article/35125178/ (ZDNET ジャパン)

7. サイバー攻撃

関連記事	● Web サイトへのサイバー攻撃に備えて 2018 年 7 月 http://www.jpcert.or.jp/newsflash/2018071801.html (JPCERT コーディネーションセンター) ● Check Point、2018 年中期のサイバー攻撃動向発表 https://news.mynavi.jp/article/20180718-663713/ (マイナビニュース) ● ロシアのサイバー攻撃集団「Sandworm Team」が日本の物流企業を標的に、FireEye が観測 https://internet.watch.impress.co.jp/docs/news/1133817.html (インターネットウォッチ) ● シンガポール史上最悪のサイバー攻撃、国家が関与か 専門家指摘 http://www.afpbb.com/articles/-/3183289 (AFPBBNews) ● 米ロ会談前、中国からフィンランドへサイバー攻撃 http://news.nicovideo.jp/watch/nw3695920 (ニコニコニュース) ● ERP を狙うサイバー攻撃が激増、壊滅的な被害招く恐れも http://www.itmedia.co.jp/news/articles/1807/26/news060.html (ITmedia) ● 標的型サイバー攻撃キャンペーン「BLACKGEAR」が再登場、ソーシャルメディアを悪用し C&C サーバ情報を隠ぺい https://blog.trendmicro.co.jp/archives/19332 (トレンドマイクロ) ● サイバー攻撃者が狙うのは企業の人事部門--ベライゾン報告書 http://japan.zdnet.com/article/35123417/ (ZDNET ジャパン) ● 電気通信事業者によるサイバー攻撃対処案 - パブコメ実施 http://www.security-next.com/097033 (securitynext) ● サイバー攻撃、民間で情報共有＝迅速対処へ基盤整備－総務省 https://www.jiji.com/jc/article?k=2018082801161 (JIJI) ● 日本狙ったサイバー攻撃に注意、巧みな Word 文書で感染狙う https://news.mynavi.jp/article/20180917-693069/ (マイナビニュース)

8. ランサムウェア

関連記事	● ランサムウェアとマイニング両方の機能を持ち効率的な攻撃を選ぶウイルスが登場 https://gigazine.net/news/20180706-virus-desides-mining-or-ransomware/ （ギガジン） ● 下火になったランサムウェア、それでも警戒を解くべきでない理由 http://japan.zdnet.com/article/35122071/ (ZDNET ジャパン) ● ランサムウェア「GandCrab」が v4 にアップデート、暗号化がより高速に https://japan.zdnet.com/article/35122299/ (ZDNET ジャパン) ● 標的型ランサムウェア「SamSam」の被害、約 6 億 7000 万円に https://japan.zdnet.com/article/35123375/ (ZDNET ジャパン) ● ランサムウェアが航空産業の製造システムコンピューターに侵入 https://eset-info.canon-its.jp/malware_info/special/detail/180807.html（キヤノン IT ソリューションズ） ● イランのハッカー：ビットコインランサムウェアを開発、サイバーセキュリティ専門家が警告 https://coinpost.jp/?p=40399 (コインポスト) ● 新種のランサムウェア「KeyPass」キャンペーン、20 カ国以上で被害--Kaspersky https://japan.zdnet.com/article/35124049/ (ZDNET ジャパン) ● 新しく確認された暗号化型ランサムウェア「PRINCESS EVOLUTION」が RaaS 利用者を募集 https://blog.trendmicro.co.jp/archives/19418 (トレンドマイクロ) ● オバマ前米大統領の画像を用いるランサムウェア http://japan.zdnet.com/article/35125033/ (ZDNET ジャパン)

9. フィッシング

関連記事	● 仮想通貨フィッシング　闇サイト「仕掛け」売買　価格 800 円、素人も参戦 http://www.itmedia.co.jp/news/articles/1807/03/news044.html (ITmedia) ● 仮想通貨狙った「フィッシング」日本語版上陸「ビットフライヤー」の偽メールも　巧妙手口が続々 http://www.itmedia.co.jp/news/articles/1807/05/news059.html (ITmedia) ● 2018/07 フィッシング報告状況 https://www.antiphishing.jp/report/monthly/201807.html（フィッシング対策協議会) ● B2B を狙うフィッシングが急増か、国内企業が注意喚起--米 BEC 被害額は 1 兆円以上 https://japan.zdnet.com/article/35123972/ (ZDNET ジャパン) ● 「クラウド時代の認証情報」を狙いフィッシング詐欺が急増、2018 年上半期の脅威動向を分析 https://blog.trendmicro.co.jp/archives/19461 (トレンドマイクロ) ● 2018/08 フィッシング報告状況 https://www.antiphishing.jp/report/monthly/201808.html（フィッシング対策協議会) ● 「WordPress」の認証情報を詐取するフィッシングメールを確認、データベース更新を促し偽ログインページへ誘導 https://internet.watch.impress.co.jp/docs/news/1141625.html（インターネットウォッチ) ● 2018/09 フィッシング報告状況 https://www.antiphishing.jp/report/monthly/201809.html（フィッシング対策協議会)

10. マルウェア

関連記事	● この新しいマルウェアは Windows のクリップボードを乗っ取り、暗号通貨アドレスを書き換える https://jp.techcrunch.com/2018/07/04/2018-07-03-new-malware-highjacks-your-windows-clipboard-to-change-crypto-addresses/ (TechCrunchJapan) ● 認証情報など盗むマルウェア「Smoke Loader」に新たな感染手法 http://japan.zdnet.com/article/35121987/ (ZDNET ジャパン) ● マルウェアの共闘: Emotet と Trickbot をプッシュするマルスパム https://www.paloaltonetworks.jp/company/in-the-news/2018/unit42-malware-team-malspam-pushing-emotet-trickbot (パロアルトネットワークス) ● 勢いを増す仮想通貨マイナー https://blog.kaspersky.co.jp/cryptominers-almost-double/20675/ (カスペルスキー) ● トロイの木馬 Rakhni：攻撃は暗号化か、マイニングか https://blog.kaspersky.co.jp/rakhni-miner-cryptor/20733/ (カスペルスキー) ● 日本人を標的とした仮想通貨マイニングマルウェアの攻撃数 1 カ月あたり最大 310 万件超を記録 - Avast 発表 https://press.avast.com/ja-jp/avast-crypto-mining-malware-trend-in-line-with-bitcoin-value (avast) ● 2018 年 7 月 マルウェアレポート https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1807.html (キヤノン IT ソリューションズ) ● 2018 年 8 月 マルウェアレポート https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1808.html (キヤノン IT ソリューションズ)

11. その他

関連記事	● 【注意喚起】偽口座への送金を促す“ビジネスメール詐欺”の手口（続報） https://www.ipa.go.jp/security/announce/201808-bec.html (IPA) ● ビジネスメール詐欺の損害は 125 億ドル超に--FBI 調査 https://japan.zdnet.com/article/35122577/ (ZDNET ジャパン) ● 「ビジネスメール詐欺に関する実態調査 2018」を発表 ～約 4 割がビジネスメール詐欺の攻撃を受けた経験あり～ https://www.trendmicro.com/ja_jp/about/press-release/2018/pr-20180814-01.html (トレンドマイクロ) ● 日本語の使用が確認された「ビジネスメール詐欺」、その背景に迫る https://blog.trendmicro.co.jp/archives/19654 (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 7 月のウイルスレビュー

関連記事	● 2018 年 7 月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=12725

2. 2018 年 8 月のウイルスレビュー

関連記事	● 2018 年 8 月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=12803

3. 2018 年 9 月のウイルスレビュー

関連記事	● 2018 年 9 月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=1286

4. 2018 年 7 月のモバイルマルウェア

関連記事	● 2018 年 7 月のモバイルマルウェア（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=12723

5. 2018 年 8 月のモバイルマルウェア

関連記事	● 2018 年 8 月のモバイルマルウェア（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=12809

6. 2018 年 9 月のモバイルマルウェア

関連記事	● 2018 年 9 月のモバイルマルウェア（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=12859

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 ＜2018.07.02＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.07.02＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180702.html

2. チェックしておきたい脆弱性情報＜2018.07.09＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.07.09＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180709.html

3. チェックしておきたい脆弱性情報＜2018.07.16＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.07.16＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180716.html

4. チェックしておきたい脆弱性情報＜2018.07.23＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.07.23> http://www.hitachi.co.jp/hirt/publications/csirt/memo20180723.html

5. チェックしておきたい脆弱性情報＜2018.07.30＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.07.30＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180730.html

6. チェックしておきたい脆弱性情報＜2018.08.06＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.08.06＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180806.html

7. チェックしておきたい脆弱性情報＜2018.08.13＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.08.13＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180813.html

8. チェックしておきたい脆弱性情報＜2018.08.20＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.08.20＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180820.html

9. チェックしておきたい脆弱性情報＜2018.08.27＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.08.27＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180827.html

10. チェックしておきたい脆弱性情報＜2018.09.3＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.09.03＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180903.html

11. チェックしておきたい脆弱性情報＜2018.09.10＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.09.10＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180910.html

12. チェックしておきたい脆弱性情報＜2018.09.17＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.09.17＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180917.html

13. チェックしておきたい脆弱性情報＜2018.09.24＞

プレス リリース	● チェックしておきたい脆弱性情報＜2018.09.24＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20180924.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7月～9月)を図2に示します。

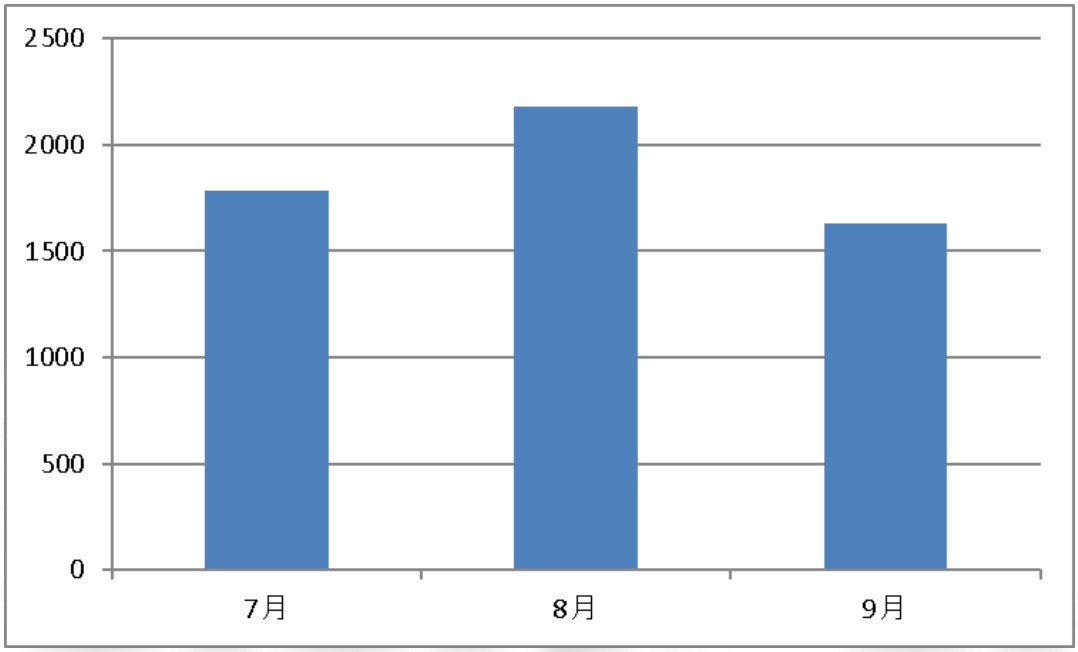

図1 「危険な可能性」と判断されたウェブサイトの件数

(*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/)

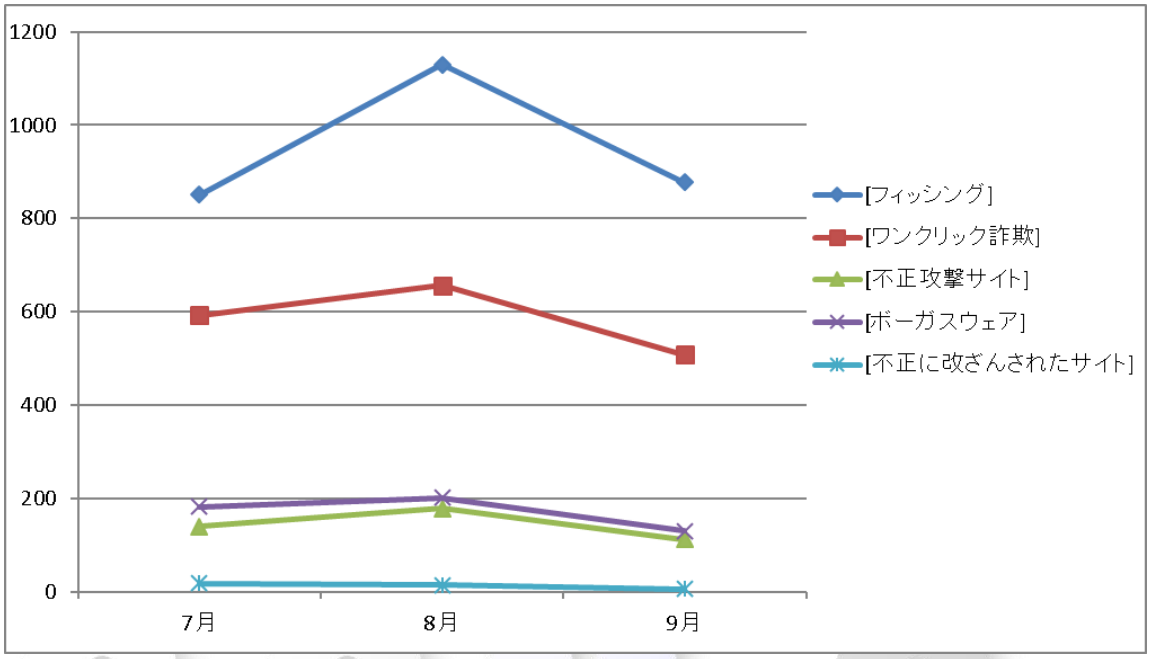

図 2 脅威別検知数の月別推移(2018 年 7 月～9 月)

7 月～9 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 1900 件でした。8 月は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が増加し、約 1100 件に上りました。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)、本四半期のフィッシングの総数は減少傾向にあります。LINE を用いたフィッシングが 2017 年 3 月頃から.cn ドメインで稼働していましたが、8 月中旬より.cn 以外のドメインで稼働するようになり報告数が増えています。LINE を用いたフィッシングについて、引き続き注意が必要です。

(*2)フィッシング対策協議会 2018/09 フィッシング報告状況

(https://www.antiphishing.jp/report/monthly/201809.html)

6. 総括

本四半期において、経営幹部や取引先などになりすましたメールにより、金銭や情報をだまし取るビジネスメール詐欺(BEC)に関するニュースが多数発表されました。7 月には、日本語を用いたビジネスメール詐欺の事例が初めて確認されました。FBI によると 2018 年 5 月までのビジネスメール詐欺による被害の累計は、全世界で 7 万 8617 件、損害額は 125 億ドル以上とのことです。また、トレンドマイクロによる調査の結果、セキュリティ管理部門及び社内 IT 担当部門、経理の幹部担当者 1030 人のうち、約 4 割が同種のメールを受信した経験があると回答しています。今後、日本語を用いたビジネスメール詐欺の増加し、日本国内における被害の増加が想定されますので、従業員への注意喚起等、ビジネスメール詐欺への対策を講ずることを推奨します。

また、仮想通貨に係るサイバー犯罪、サイバー攻撃に関するニュースが多数発表されました。7 月にはマイニングマルウェアとランサムウェアの両方の機能を備え、標的によって攻撃手法を選択するマルウェアが発見されました。カスペルスキーによると、2018 年に入りマイニングマルウェアの検出数がランサムウェアを抜き、最も検出数の多いマルウェアとなったとのことです。9 月には公開されて間もない「Apache Struts 2」の脆弱性を悪用し、ウェブサイトにアクセスした機器が、意図せずに仮想通貨のマイニングを行うように仕向ける、クリプトジャッキング攻撃が確認されています。今後、仮想通貨の取得を目的としたサイバー犯罪、攻撃の更なる増加が予想されます。マイニングマルウェア等、仮想通貨の取得を目的とした犯罪、攻撃は、発覚を遅らせるためにファイルレス型のマルウェアを用いるなど、発見することが困難な点が特徴となりますので、公開された情報を参考に、対策を講ず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

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

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