S.S.R.C.定期
トレンドレポート
Vol.34

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.34

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 4 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：2017/10/1～2017/12/31

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	● 2017 年 10 月マイクロソフトセキュリティ更新プログラムに関する注意喚起 http://www.jpcert.or.jp/at/2017/at170039.html (JPCERT/CC) ● Windows 10 優先のセキュリティ対策に Google が批判 http://news.mynavi.jp/articles/2017/10/30/windows10report/（マイナビニュース) ● Windows Defender Exploit Guard: 攻撃表面を縮小して次世代型マルウェアに対抗する https://blogs.technet.microsoft.com/jpsecurity/2017/11/01/windows-defender-exploit-guard-reduce-the-attack-surface-against-next-generation-malware/ (Microsoft) ● Microsoft Windows OS において DLL Hijacking により UAC を回避する手法 https://scan.netsecurity.ne.jp/article/2017/11/06/40323.html (ScanNetSecurity) ● Windows 標準のマルウェア対策エンジンに「最悪」の脆弱性、どうしてこうなった？ http://techtarget.itmedia.co.jp/tt/news/1711/07/news03.html (TechTaregt) ● Office の DDE プロトコル悪用の恐れ、Microsoft が対策呼び掛け http://www.itmedia.co.jp/enterprise/articles/1711/14/news042.html (ITMedia) ● 2017 年 11 月のセキュリティ更新プログラム（月例) https://blogs.technet.microsoft.com/jpsecurity/2017/11/15/201711-security-bulletin/ (Microsoft) ● 「Microsoft Office」に 17 年前からの脆弱性が発覚、月例パッチで修正 https://japan.zdnet.com/article/35110497/ (ZDNet Japan) ● 2017 年 12 月のセキュリティ更新プログラム（月例) https://blogs.technet.microsoft.com/jpsecurity/2017/12/13/201712-security-updates/ (Microsoft)

2. Apple

関連記事	● iPhone 7 の Wi-Fi チップセットのファームウェアにコード実行の脆弱性 http://news.mynavi.jp/news/2017/09/29/306/ (マイナビニュース) ● iOS のポップアップを偽装し、Apple ID やそのパスワードを盗み取る PoC が公開される。 https://applech2.com/archives/20171011-ios-password-popup-phishing-poc.html (APPL Ch.) ● 「Mac」向け人気メディアプレーヤー、マルウェアとともに一時配布 https://japan.cnet.com/article/35109176/ (cnet Japan) ● Apple、Wi-Fi の WPA2 に関する脆弱性「KRACK」の情報をアップデートし、4-way ハンドシェイクに関する一部の脆弱性は iPhone 7 以下に影響しないと発表 https://applech2.com/archives/20171105-about-krack-and-impact-ios-devices.html (APPL Ch.) ● 「macOS High Sierra」にパスワードなしでログインできてしまう脆弱性 https://japan.cnet.com/article/35111084/ (cnet Japan)

3. Adobe

関連記事	● Adobe Flash Player の脆弱性対策について(APSB17-32)(CVE-2017-11292) https://www.ipa.go.jp/security/ciadr/vul/20171017-adobeflashplayer.html (IPA) ● 「Flash Player」へのゼロデイ攻撃、「BlackOasis」が関与か - 「FinFisher」感染狙い http://www.security-next.com/086672 (Security NEXT) ● 複数の深刻な脆弱性へ対処した「Adobe Flash Player」のセキュリティアップデート http://www.security-next.com/087566 (Security NEXT) ● 「Adobe Acrobat/Reader」の脆弱性 62 件を解消 - 10 月に EOL 迎えた「同 XI」にも最終更新 http://www.security-next.com/087561 (Security NEXT) ● 「Adobe Flash Player」にセキュリティアップデート - 深刻な脆弱性は含まれず http://www.security-next.com/088356 (Security NEXT)

4. Android

関連記事	● 「ZNIU」:脆弱性 Dirty COW を突く Android 端末向け不正アプリを確認 http://blog.trendmicro.co.jp/archives/16031 (トレンドマイクロ) ● Android のユーザー補助サービスを悪用する初のランサムウェア「DoubleLocker」が登場 http://www.atmarkit.co.jp/ait/articles/1710/17/news032.html (@IT) ● Google Play、人気 Android アプリの脆弱性発見に報奨金 1000 ドル http://www.itmedia.co.jp/news/articles/1710/20/news062.html (ITMedia) ● Android を狙い、デバイスをボットネットに組み入れようとするマルウェアが Google Play に出現 https://www.symantec.com/connect/ja/blogs/android-google-play (シマンテック) ● Ramnit: 予想外の場所に今でも出現するワーム https://www.symantec.com/connect/ja/blogs/ramnit-2 (シマンテック) ● スマホに感染、仮想通貨を採掘させるウイルス―Google Play に登場 https://internetcom.jp/203668/crypt-coin-malware-for-android (INTERNET COM) ● チャットアプリ「WhatsApp」の偽物、Google Play で 100 万回以上ダウンロード https://japan.cnet.com/article/35109986/ (cnet Japan) ● 144 個の Google Play アプリに新種の Android マルウェアを発見 http://blogs.mcafee.jp/android-malware-grabos-exposed-millions-to-pay-per-install-scam-on-google-play (マカフィー) ● 「Toast」機能を利用してオーバーレイ攻撃を実行する Android 端末向け不正アプリを Google Play で確認 http://blog.trendmicro.co.jp/archives/16414 (トレンドマイクロ)

5. 情報漏洩

関連記事	● 米ヤフー、３０億件情報流出　全利用者が被害、過去最大規模、不正侵入か http://www.sankei.com/world/news/171004/wor1710040010-n1.html (産経ニュース) ● TOKYO MX、個人情報 37 万件流出か http://www.asahi.com/and_w/interest/entertainment/CORI2098428.html (朝日新聞) ● 医療機関予約システムに不正アクセス　最大６０万人の情報流出か http://www.sankei.com/affairs/news/171011/afr1710110026-n1.html (産経ニュース) ● 5 年前に終了したプリントゴッコ通販サイトに不正アクセス - 顧客情報が流出 http://www.security-next.com/086552 (Security NEXT) ● ＧＭＯインターネット　１万 4600 件余の顧客情報流出 http://www3.nhk.or.jp/news/html/20171030/k10011204001000.html (NHK) ● 「CIA がカスペルスキーに成りすますコードを作成した」と WikiLeaks が新文書「Vault 8」を発表 http://gigazine.net/news/20171110-cia-impersonate-kaspersky-code/ (GIGAZINE) ● ウーバー、5700 万人分個人情報流出の隠蔽発覚　16 年 https://www.nikkei.com/article/DGXMZO23784990S7A121C1EAF000/ （日本経済新聞） ● Imgur、170 万件のアカウント情報流出認める--2014 年にハッキング被害 https://japan.cnet.com/article/35110958/ (cnet Japan) ● ダークウェブに 14 億件の個人データ流出、有名ポルノサイトも https://forbesjapan.com/articles/detail/18912 (Forbes JAPAN)

6. 脆弱性

関連記事	● フラッシュメモリーは「電線の直結」でハッキングし、情報を抜き取れる――米研究グループが発見 https://wired.jp/2017/09/30/sd-card-hack/ (WIRED) ● Dnsmasq に 7 件の脆弱性、Android や Linux など広範に影響の恐れ　パッチ適用を http://www.itmedia.co.jp/enterprise/articles/1710/03/news044.html (ITMedia) ● 脆弱性の悪用を防ぐため Windows アプリケーションの実行は新しいフォルダーで https://www.ipa.go.jp/security/anshin/mgdayori20171003.html (IPA) ● Apache HTTP サーバに存在する脆弱性「OptionsBleed」 http://blog.trendmicro.co.jp/archives/16069 (トレンドマイクロ) ● WPA2 の脆弱性「KRACKs」、ほぼすべての Wi-Fi 通信可能な端末機器に影響 http://blog.trendmicro.co.jp/archives/16162 (トレンドマイクロ) ● Oracle、定例アップデートで 252 件の脆弱性に対応 - 半数弱が「緊急」または「重要」 http://www.security-next.com/086738 (Security NEXT) ● メールソフト多数で「Mailsploit」の脆弱性発覚--スパム対策も回避 https://japan.zdnet.com/article/35111572/ (ZDNet Japan) ● 「Petya」も狙う「MS17-010」の脆弱性、少なくとも 4000 万台弱の未修正端末が稼働 http://www.security-next.com/083205 (Security NEXT) ● Oracle の「Identity Manager」に重大な脆弱性、緊急パッチ公開　すぐに適用を http://www.itmedia.co.jp/news/articles/1710/31/news052.html (ITMedia) ● OpenSSL の複数の脆弱性（CVE-2017-3735, CVE-2017-3736） https://oss.sios.com/security/openssl-security-vulnerability-20171103 (サイオス)

7. サイバー攻撃

関連記事	● アマゾン傘下の Whole Foods に不正アクセス--決済カード情報が狙われる https://japan.cnet.com/article/35108089/ (cnet Japan) ● ビジネスプロセス詐欺（Business Process Compromise、BPC）の事例と対策 http://blog.trendmicro.co.jp/archives/16037 (トレンドマイクロ) ● 米証券取引委　　企業情報開示システムへの不正アクセスでさらなる被害 https://www.bloomberg.co.jp/news/articles/2017-10-03/OX89K76JIJUO01 (Bloomberg) ● IoT マルウェア「Satori」攻撃発生、アジアに感染集中か--ワーム型で拡大 https://japan.zdnet.com/article/35111546/ (ZDNet Japan) ● ロシア　ＮＡＴＯ兵士携帯をハッキングか http://www3.nhk.or.jp/news/html/20171007/k10011171031000.html (NHK) ● 金正恩氏暗殺含む米韓作戦計画が流出か　昨年９月、北朝鮮のハッキングと推定 http://www.sankei.com/world/news/171010/wor1710100032-n1.html (産経ニュース) ● イラン政府の関与が疑われる諜報活動グループ「APT33」が韓国を狙った理由 https://the01.jp/p0005877/ (the ZERO/ONE) ● F35 戦闘機の情報、豪防衛業者から盗まれる 中国ハッカーか http://www.afpbb.com/articles/-/3146446 (AFP) ● スウェーデンの交通機関が DDoS 攻撃を受け運航不能に陥る https://the01.jp/p0005941/ (the ZERO/ONE) ● 電力会社や重要インフラ狙うサイバー攻撃の実情--US-CERT レポート https://japan.zdnet.com/article/35109320/ (ZDNet Japan) ● Bitcoin マイニングの NiceHash、ハッキングで数千万ドルを失う https://jp.techcrunch.com/2017/12/08/2017-12-06-nicehash-hack/ (TechCrunch)

8. ランサムウェア

関連記事	● ランサムウェア脅威は継続、「サービスとしてのサイバー犯罪」台頭--ユーロポール報告 https://japan.zdnet.com/article/35108073/ (ZDNet Japan) ● ランサムウェアに身代金を支払ってしまった病院、対策に“正解”はあるのか？ http://www.itmedia.co.jp/enterprise/articles/1710/04/news012.html (ITMedia) ● UAC 回避機能を複数搭載したランサムウェア「HkCrypt」 https://www.mbsd.jp/blog/20171012.html (三井物産セキュアディレクション) ● 「LOCKY」と「FAKEGLOBE」、2 つのランサムウェアを交互に拡散するスパムメール送信活動を確認 http://blog.trendmicro.co.jp/archives/16089 (トレンドマイクロ) ● 暗号化しないランサムウェア「ShinigamiLocker」と、スクリーンロッカー／偽ランサムウェアの脅威 https://www.mbsd.jp/blog/20171018.html (三井物産セキュアディレクション) ● エクスプロイトキット「Magnitude EK」が韓国を対象に暗号化型ランサムウェア「MAGNIBER」を拡散 http://blog.trendmicro.co.jp/archives/16190 (トレンドマイクロ) ● 「Bad Rabbit」ランサムウェアの感染拡大、ロシアなどで報告--「Petya」亜種か https://japan.zdnet.com/article/35109298/ (ZDNet Japan) ● 日本企業を狙うランサムウェア「鬼」、ファイル暗号化して痕跡を消去 http://www.itmedia.co.jp/enterprise/articles/1711/01/news074.html (ITMedia) ● 新種のランサムウェア「GIBON」が拡散中 https://japan.zdnet.com/article/35109955/ (ZDNet Japan) ● 身代金を支払うその前に、対ランサムウェア復号ツール http://techtarget.itmedia.co.jp/tt/news/1712/27/news01.html (TechTarget)

9. フィッシング

関連記事	● あなたの Apple ID に岐阜から不審なログインが!? 偽のアカウント修復サイトに誘導するフィッシングメールが拡散中 https://internet.watch.impress.co.jp/docs/news/1087564.html (INTERNET Watch) ● 楽天カードをかたるウイルスメールが拡散中、件名「口座振替日のご案内」など https://internet.watch.impress.co.jp/docs/news/1087879.html (INTERNET Watch) ● Amazon をかたるフィッシング https://www.antiphishing.jp/news/alert/amazon_20171026.html (フィッシング対策協議会) ● 「アカウントで利用規約違反」と不安煽る偽 Amazon に注意 http://www.security-next.com/087022 (Security NEXT) ● 2017/12 フィッシング報告状況 http://www.antiphishing.jp/report/monthly/201712.html (フィッシング対策協議会) ● フィッシングや不正請求を体験可能!? スマホ向け疑似体験サイトが公開中 https://is702.jp/news/2232/ (トレンドマイクロ) ● bitFlyer をかたるフィッシング https://www.antiphishing.jp/news/alert/bitflyer_20171106.html (フィッシング対策協議会) ● 「フィッシングはデータ漏えいより危険」--グーグル調査 https://japan.zdnet.com/article/35110269/ (ZDNet Japan) ● Apple ID のセキュリティ質問のニセ設定ページに誘導(フィッシング対策協議会) https://scan.netsecurity.ne.jp/article/2017/12/18/40440.html (ScanNet Security)

10. マルウェア

関連記事	● Facebook の「いいね」を偽装するマルウェアが活発化 http://pc.watch.impress.co.jp/docs/news/1083063.html (PC Watch) ● 仮想通貨発掘へ手口を変えた「RETADUP」の亜種、南米の政府やエネルギー産業を狙う http://blog.trendmicro.co.jp/archives/16064 (トレンドマイクロ) ● 情報を盗むマルウェア「FormBook」、感染メールが各国で流通　日本でも確認 http://www.itmedia.co.jp/news/articles/1710/10/news044.html (ITMedia) ● CCleaner で懸念されるコマンド アンド コントロール https://gblogs.cisco.com/jp/2017/10/talos-ccleaner-c2-concern/ (CISCO) ● ボットネット「Necurs」、攻撃者にエラーレポート返送--攻撃を「品質向上」か https://japan.zdnet.com/article/35109036/ (ZDNet Japan) ● こっそり仮想通貨をマイニングする侵入者たち https://the01.jp/p0005920/ (the ZERO/ONE) ● 銀行情報を狙うマルウェア「Ursnif」、日本での活動が再び活発に http://www.itmedia.co.jp/news/articles/1710/27/news060.html (ITMedia) ● Linux サーバを狙うマルウェア「Ebury」の新バージョンが発見 http://news.mynavi.jp/news/2017/11/01/050/ (マイナビニュース) ● IoT 機器を狙うボット「Reaper」、数百万台のネットワーク機器に感染 http://blog.trendmicro.co.jp/archives/16282 (トレンドマイクロ) ● 北朝鮮のマルウェア「Volgmer」、米当局が IP アドレスなど公表 http://www.itmedia.co.jp/enterprise/articles/1711/16/news060.html (ITMedia)

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 10 月のウイルスレビュー

関連記事	● 2017 年 10 月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=11552

2. 2017 年 11 月のウイルスレビュー

関連記事	● 2017 年 11 月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=11611

3. 2017 年 12 月のウイルスレビュー

関連記事	● 2017 年 12 月のウイルスレビュー（Dr. WEB） https://news.drweb.co.jp/show/review/?lng=ja&i=11676

4. 2017 年 10 月のモバイルマルウェア

関連記事	● 2017 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=11554

5. 2017 年 11 月のモバイルマルウェア

関連記事	● 2017 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=11613

6. 2017 年 12 月のモバイルマルウェア

関連記事	● 2017 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=11673

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 ＜2017.10.02＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.10.02＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20171002.html

2. チェックしておきたい脆弱性情報＜2017.10.09＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.10.09＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20171009.html

3. チェックしておきたい脆弱性情報＜2017.10.16＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.10.16＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20171016.html

4. チェックしておきたい脆弱性情報＜2017.10.23＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.10.23＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20171023.html

5. チェックしておきたい脆弱性情報＜2017.10.30＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.10..30＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20171030.html

6. チェックしておきたい脆弱性情報＜2017.11.06＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.11.06＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20171106.html

7. チェックしておきたい脆弱性情報＜2017.11.13＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.11.13＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20171113.html

8. チェックしておきたい脆弱性情報＜2017.11.20＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.11.20＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20171120.html

9. チェックしておきたい脆弱性情報＜2017.11.27＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.11.27＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20171127.html

10. チェックしておきたい脆弱性情報＜2017.12.04＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.12.04＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20171204.html

11. チェックしておきたい脆弱性情報＜2017.12.11＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.12.11＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20171211.html

12. チェックしておきたい脆弱性情報＜2017.12.18＞

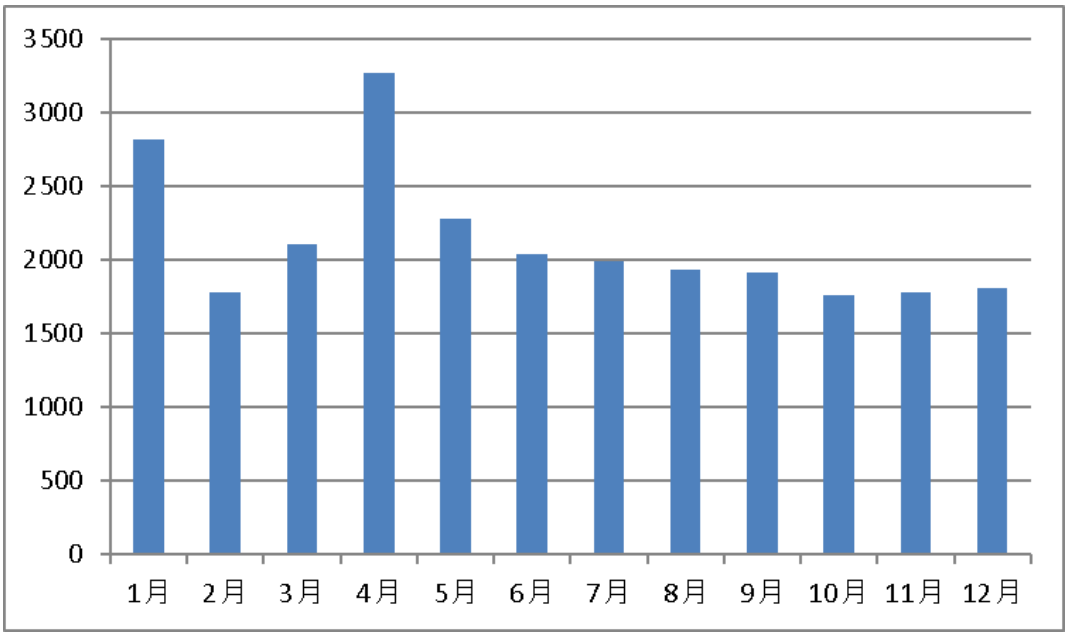
プレス リリース	● チェックしておきたい脆弱性情報＜2017.12.18＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20171218.html

13. チェックしておきたい脆弱性情報＜2017.12.25＞

プレス リリース	● チェックしておきたい脆弱性情報＜2017.12.25＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20171225.html

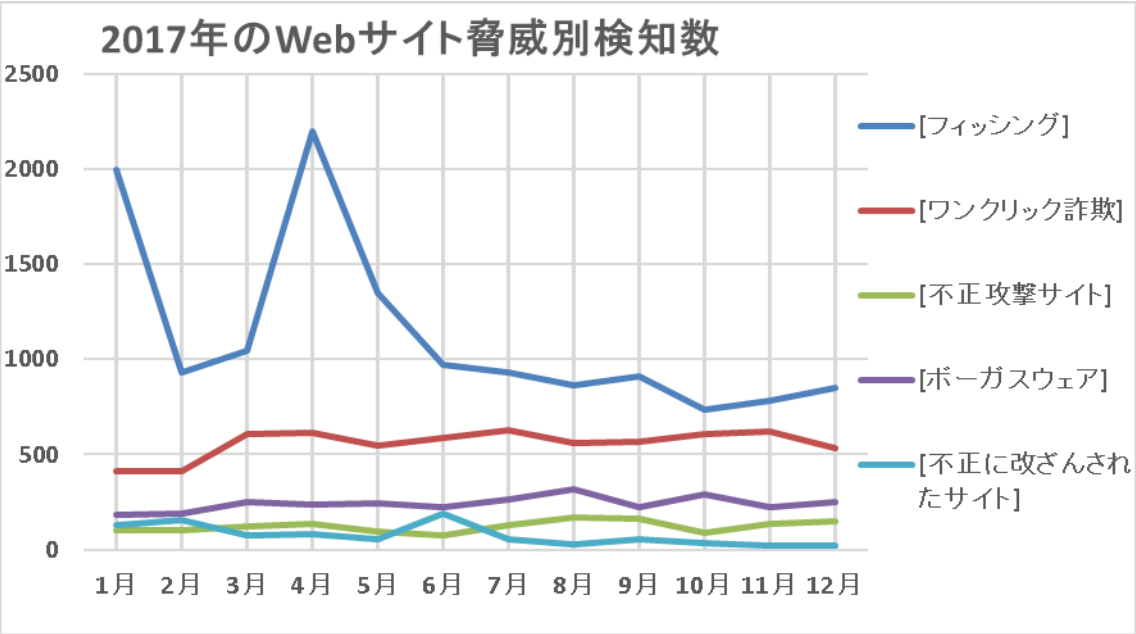
5. データからみるサイバー犯罪の傾向

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(2017 年 1 月～12 月)

* 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～12 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 1780 件でした。過去 1 年の月平均である 2100 件と比較すると、18%減少しています。

ワンクリック詐欺サイトは、10 月、11 月と大きな変化はありませんでしたが、12 月は前月比 16%減少しています。

フィッシングサイトは、10 月には 9 月の 911 件から 738 件と 23%と大きく減少しましたが、その後は増加に転じ、12 月には 850 件と前期の月平均 900 件に近い数字になりました。フィッシングメールは、昨今の仮想通貨の流行に伴い仮想通貨交換所を装ったケースも発生していますので、注意が必要です。(*1)　また、年間を通してフィッシングサイトは検知数を維持しており、メールからアクセスした Web サイトに不審な点を覚えた場合は URL を確認したり、URL から Web サイトの安全性を検査するサービスの利用を推奨します。

(*1)http:/www.antiphishing.jp/report/monthly/201712.html (フィッシング対策協議会)

6. 総括

11 月には、大規模な情報漏えいの発覚が続きました。まず、米 Yahoo から 30 億件分という過去最大規模の個人情報漏えいが発覚しました。これは 2013 年に同社ネットワークに不正侵入された際に流出したとみられています。また、Imgur からは 170 万件のアカウント情報が 2014 年に漏えいしていたことが発覚しました。同社はセキュリティ研究者からの連絡を受け、24 時間以内にパスワードリセットやユーザ、社外への広報などの対応を取りました。一方、Uber は 2016 年に発生した不正アクセスによる 5700 万件の個人情報漏えいを隠ぺいしていたと公表しました。企業などのブランドイメージを保護するためには、情報漏えい自体を防ぐ対策だけでなく、漏えいが起こってしまった後の対応も同等以上に重要です。

今期は脆弱性に関しても大きなニュースがありました。KRACK と名付けられた、WPA2 の脆弱性を突いた攻撃手法です。世界で広く利用されているプロトコルの脆弱性ですので、発表当初は大変注目されましたが、攻撃条件が複雑で遠隔からは攻撃することができないと判明したため、注目度に反して危険性はあまり高くありませんでした。その一方で、Adobe Flash Player に対して発生したゼロデイ攻撃(CVE-2017-11292)に関しては、対応に追われたシステム管理者の方も多かったでしょう。このように、脆弱性の危険度を評価する際には、攻撃が発生しているか、攻撃コードが公開されているか、自組織が攻撃された場合の予想被害などが重要なポイントとなります。脆弱性が公表された際には、以上の点で情報収集を行い、優先順位をつけた脆弱性対策を推奨します。

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