S.S.R.C.定期
トレンドレポート
Vol.30

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.30

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 2016 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:2016/10/1～2016/12/31

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	● Windows 7 までに DoS 誘発の脆弱性、MS の推奨対策はアップグレード (IT media) http://www.itmedia.co.jp/enterprise/articles/1610/07/news095.html ● Microsoft、10 件の月例セキュリティ情報を公開　新しい更新モデルもスタート (IT media) http://www.itmedia.co.jp/news/articles/1610/12/news057.html ● Windows の設計に起因する攻撃手法「AtomBombing」、セキュリティ企業が発見 (IT media) http://www.itmedia.co.jp/news/articles/1610/31/news056.html ● Windows に未解決の脆弱性、Google が独自方針で情報を公開 (IT media) http://www.itmedia.co.jp/news/articles/1611/01/news068.html ● Microsoft、14 件の月例セキュリティ情報を公開　「緊急」は 6 件 (IT media) http://www.itmedia.co.jp/news/articles/1611/09/news057.html ● カスペルスキー氏、Microsoft の「Defender」特別扱いに“物申す” (IT media) http://www.itmedia.co.jp/news/articles/1611/14/news069.html ● マイクロソフトの新しいセキュリティ更新プログラムガイド「Security Updates Guide」とは (CNet Japan) http://japan.cnet.com/news/service/35092176/ ● Microsoft、12 件の月例セキュリティ情報を公開　IE や Edge に「緊急」の脆弱性 (IT media) http://www.itmedia.co.jp/news/articles/1612/14/news071.html ● 進む Web ブラウザの“Flash 離れ”、Microsoft Edge もブロック拡大へ (IT media) http://www.itmedia.co.jp/news/articles/1612/15/news061.html

2. Apple

関連記事	● Mac のウェブカメラを悪用した傍受の手法が明らかに（CNet Japan） http://japan.cnet.com/news/business/35090175/ ● Apple、「iOS 10.1」で深刻な脆弱性も修正　macOS や watchOS なども（IT media） http://www.itmedia.co.jp/news/articles/1610/25/news055.html ● Apple、Windows 向け iCloud と Xcode の脆弱性を修正（IT media） http://www.itmedia.co.jp/news/articles/1610/28/news060.html ● iOS のバグを試したつもりが緊急電話に DDoS 攻撃。逮捕の少年「アップルのバグ報奨金に応募したかった」（engadget） http://japanese.engadget.com/2016/10/31/ios-ddos/ ● iOS の脆弱性「Trident」を突く「Pegasus」スパイウェアの手法などをセキュリティ企業がレポート（CNet Japan） http://japan.cnet.com/news/service/35091770/ ● iPhone ユーザを狙った不正アプリによるセクストーション被害が発生（IPA） http://www.ipa.go.jp/security/anshin/mgdayori20161110.html ● OS X の IOSurface におけるタスク処理の不備により権限が昇格可能となる脆弱性（Scan Net Security） http://scan.netsecurity.ne.jp/article/2016/12/07/39238.html ● 「iOS 10.2」、iPhone や iPad 向けに公開　計 12 件の脆弱性を修正（IT media） http://www.itmedia.co.jp/news/articles/1612/13/news055.html ● macOS Sierra や Safari、Windows 向け iCloud と iTunes の更新版公開　深刻な脆弱性が多数（IT media） http://www.itmedia.co.jp/news/articles/1612/14/news073.html ● アプリに HTTPS 義務付けの ATS、Apple が実装期限を延期（IT media） http://www.itmedia.co.jp/news/articles/1612/26/news053.html

3. Adobe

関連記事	● Adobe、Acrobat や Flash Player などの更新版を一挙公開 (IT media) http://www.itmedia.co.jp/news/articles/1610/12/news058.html ● 直近「Adobe Acrobat/Reader アップデート」 、実際は 74 件の脆弱性を修正 (Security NEXT) http://www.security-next.com/075117 ● Flash の未解決の脆弱性突く攻撃発生、Adobe が臨時パッチ公開 (IT media) http://www.itmedia.co.jp/news/articles/1610/27/news067.html ● Adobe、Flash Player の更新版リリース　深刻な脆弱性を修正 (IT media) http://www.itmedia.co.jp/news/articles/1611/09/news058.html ● Flash Player の脆弱性突く攻撃を確認、直ちにアップデート適用を (IT media) http://www.itmedia.co.jp/news/articles/1612/14/news072.html

4. Android

関連記事	● Google、Android の月例セキュリティパッチ公開、深刻な脆弱性を解決 (IT media) http://www.itmedia.co.jp/news/articles/1610/04/news074.html ● 「Google Play」配信アプリ 400 本超にトロイの木馬型マルウェア (CNet Japan) http://japan.cnet.com/news/service/35089975/ ● Google、Android の月例パッチを公開　「Dirty COW」の脆弱性にも対処 (IT media) http://www.itmedia.co.jp/news/articles/1611/08/news064.html ● Android 向けファームウェアに深刻な脆弱性、米機関は「もはや rootkit」と断言 (IT media) http://www.itmedia.co.jp/enterprise/articles/1611/18/news115.html ● Android マルウェア「Gooligan」横行、100 万超の Google アカウントに不正アクセス（IT media） http://www.itmedia.co.jp/news/articles/1612/01/news066.html ● Google、Android の月例セキュリティパッチを公開　多数の深刻な脆弱性に対処 (IT media) http://www.itmedia.co.jp/enterprise/articles/1612/06/news066.html ● Doctor Web、よく知られた Android デバイスのファームウェア内でトロイの木馬を発見（Dr.WEB） http://news.drweb.co.jp/show/?i=1125 ● 銀行情報を狙う Android マルウェア、世界で被害拡大　ファイルを人質に取る機能も実装（IT media） http://www.itmedia.co.jp/news/articles/1612/20/news051.html

5. 情報漏洩

関連記事	● iOS 向けサードパーティストア「Haima」用ソフトに Apple ID 流出の危険性 (TREND Micro) http://blog.trendmicro.co.jp/archives/13905 ● ハッキング容疑でロシア人の男を逮捕、LinkedIn の大量流出事件に関与か (IT media) http://www.itmedia.co.jp/news/articles/1610/20/news060.html ● 「フラット 35」の顧客情報流出か　勤務先や年収も……メールサーバに不正アクセス、不正な転送設定も (IT media) http://www.itmedia.co.jp/news/articles/1610/27/news075.html ● 新生銀行子会社で情報漏えいの可能性、「未知のマルウェア」と後から判明 (IT media) http://www.itmedia.co.jp/enterprise/articles/1611/08/news119.html ● 米アダルトサイトで 4 億人強の情報流出、日本語ユーザーも 65 万人が被害 (IT media) http://www.itmedia.co.jp/news/articles/1611/15/news058.html ● 米海軍で兵士 13 万人あまりの個人情報が流出 (IT media) http://www.itmedia.co.jp/news/articles/1611/25/news060.html ● 資生堂子会社に不正アクセス、42 万人分の個人情報流出の恐れ　カード情報も (IT media) http://www.itmedia.co.jp/news/articles/1612/02/news115.html ● 米 Yahoo!、新たに 10 億人分のデータ流出判明 (IT pro) http://itpro.nikkeibp.co.jp/atcl/news/16/121503750/ ● LinkedIn 傘下の Lynda.com に不正アクセス　5 万 5000 人のパスワードをリセット (DZNet Japan) http://japan.zdnet.com/article/35093927/

6. 脆弱性

関連記事	● Oracle が定例セキュリティパッチ公開、Java など 253 件の脆弱性を修正（IT media） http://www.itmedia.co.jp/news/articles/1610/19/news062.html ● 「MySQL」のゼロデイ脆弱性、定例パッチで一部修正（Security NEXT） http://www.security-next.com/074904 ● Linux カーネルに脆弱性「Dirty COW」発覚、管理者権限を取得される恐れ（IT media） http://www.itmedia.co.jp/news/articles/1610/24/news044.html ● 「BIND 9」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/1611/04/news053.html ● OpenSSL の更新版公開、DoS の脆弱性を修正（IT media） http://www.itmedia.co.jp/news/articles/1611/11/news058.html ● Tor 匿名解除の攻撃に利用の脆弱性、Firefox や Thunderbird も修正（IT media） http://www.itmedia.co.jp/news/articles/1612/02/news054.html ● デスクトップ向け「Chrome 55」の安定版リリース　HTML5 デフォルト化は延期に（IT media） http://www.itmedia.co.jp/enterprise/articles/1612/03/news037.html ● セキュリティリリース「PHP 7.0.14」「同 5.6.29」が公開（Security NEXT） http://www.security-next.com/076549 ● 「Apache Tomcat 8.5.0」以降に情報漏洩の脆弱性（Security NEXT） http://www.security-next.com/076692 ● Firefox の更新版「50.1」公開、深刻な脆弱性を修正（IT media） http://www.itmedia.co.jp/news/articles/1612/15/news060.html ● 「Ubuntu」デスクトップに深刻なバグ--遠隔からコード実行のおそれ（DZNet Japan） http://japan.zdnet.com/article/35094006/

7. サイバー攻撃

関連記事	● 最史上最大級の DDoS 攻撃に使われたマルウェア「Mirai」公開、作者が IoT を悪用（IT media） http://www.itmedia.co.jp/news/articles/1610/04/news046.html ● 米 DNS サービスに大規模 DDoS 攻撃で米国で Twitter や Spotify が長時間ダウン（IT media） http://www.itmedia.co.jp/news/articles/1610/22/news024.html ● テレビにもサイバー攻撃　画面が停止し「罰金払え」の画面　国内 300 件以上ウイルス検知（IT media） http://www.itmedia.co.jp/news/articles/1610/31/news066.html ● インドの支払システムへの攻撃で 300 万のデビット カードが危険に～「私達のせいではありません！」 日立ペイメントサービス社は ATM 情報漏えいを否（Scan Net Security） http://scan.netsecurity.ne.jp/article/2016/11/15/39170.html ● たった 1 台のノート PC でもサーバーをダウンさせられる脅威の「BlackNurse」（Gigazine） http://gigazine.net/news/20161115-blacknurse/ ● サンフランシスコ市営鉄道の駅のシステムや電光掲示板に不正にアクセス、約 810 万円を要求（Scan Net Security） http://scan.netsecurity.ne.jp/article/2016/11/29/39213.html ● 「Ameba」に PW リスト攻撃 - 3754 万回に及ぶ試行で 59 万 ID に不正ログイン（Security NEXT） http://www.security-next.com/076191 ● ロシアの情報工作懸念　米、サイバー攻撃への「報復」警告　独仏も選挙介入警戒（日本経済新聞） http://www.nikkei.com/article/DGXLASGM17H8J_X11C16A2FF8000/

8. ランサムウェア

関連記事	● 悪質な WSF を添付したメールでランサムウェア拡散図る例が急増--シマンテック（DZNet Japan） http://japan.zdnet.com/article/35090596/ ● 新しいエクスプロイトキット「Bizarro Sundown EK」を確認。「LOCKY」に誘導（TREND Micro） http://blog.trendmicro.co.jp/archives/13998 ● ルータを狙う「JITON」でクレジットカード漏えい、ランサムウェア被害へ（DZNet Japan） http://japan.zdnet.com/article/35091792/ ● 自分の顔写真で「犯罪者情報」と……身代金要求ウイルス、スマホで急増　顔を勝手に撮影も（IT media） http://www.itmedia.co.jp/news/articles/1611/14/news061.html ● 2016 年 10 月から継続して確認される巧妙な日本語メールと頒布されるランサムウェアを解析（TREND Micro） http://blog.trendmicro.co.jp/archives/14066 ● ワーム機能を持つ安価な暗号化型ランサムウェア「Stampado」（DZNet Japan） http://japan.zdnet.com/article/35092699/ ● ランサムウェア、クリスマス商戦に便乗　偽配送メールに警戒を（Security NEXT） http://www.security-next.com/076028 ● 画像でマルウェアに感染させる「ImageGate」攻撃、ランサムウェア拡散に使用か（IT media） http://www.itmedia.co.jp/enterprise/articles/1611/27/news031.html

	● 解析情報：「CERBER」、データベースファイルの暗号化機能を追加 (TREND Micro) http://blog.trendmicro.co.jp/archives/14102 ● 偽の MS サポート技術者への料金支払いを促すランサムウェアが登場 (DZNet Japan) http://japan.zdnet.com/article/35093198/ ● 米サンフランシスコ市交通局で被害、ランサムウェア「HDDCryptor」を解析 (TREND Micro) http://blog.trendmicro.co.jp/archives/14122 ● 「ファイルを取り戻したければ、誰か 2 人を感染させろ」――ランサムウェアに新手の手口（IT media） http://www.itmedia.co.jp/news/articles/1612/13/news059.html

9. フィッシング

関連記事	● LINE をかたるフィッシング（フィッシング対策評議会） https://www.antiphishing.jp/news/alert/line_20161031.html ● 2016/10 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/201610.html ● 2 段階で情報をだまし取る「偽 Amazon」に注意 - サインインしたように見せかけクレカ情報を追加要求（Security NEXT） http://www.security-next.com/075515 ● ハンゲーム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/hangame_20161114.html ● 「発送」「お届け」を装った佐川急便の偽メールに注意 - 問い合わせが増加（Security NEXT） http://www.security-next.com/075822 ● Apple 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/apple_20161201.html ● 2016/11 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/201611.html ● Yahoo! JAPAN をかたる「至急!!!お客様 ID 危険検出」メールに注意、ウイルス感染の恐れ（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/1035653.html ● [更新] 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_20161222.html ● 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_20161226.html

10. マルウェア

関連記事	● 韓国で流行した新手の不正送金マルウェアが国内上陸 - 不正送金被害も (Security NEXT) http://www.security-next.com/074499 ● マイクロソフト「Security Essentials」を装う新マルウェア「Hicurdismos」が登場（CNet Japan） http://japan.cnet.com/news/business/35091046/ ● クレジットカードや金融機関関連の情報を窃取する「Ursnif」に注意 (Scan Net Security) http://scan.netsecurity.ne.jp/article/2016/11/01/39114.html ● IoT ボットネットを構築する新たなマルウェアが発見される（DZNet Japan） http://japan.zdnet.com/article/35091518/ ● 「添付写真について」というウイルス付きメールが拡散中、警視庁が Twitter で「早期警戒情報」を出して注意呼び掛け（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/1028684.html IOC の信頼性の低下、メモリ常駐型マルウェアの出現（Scan Net Security） https://scan.netsecurity.ne.jp/article/2016/11/24/39207.html ● Gatak：医療機関を集中的に狙うマルウェア（Symantec） https://www.symantec.com/connect/ja/blogs/gatak-0 ● 新しい「Mirai」、ルータを狙うポート 7547 への攻撃が示す今後の脅威 (TREND Micro) http://blog.trendmicro.co.jp/archives/14108 ● ATM マルウェアの新ファミリ「Alice」を確認（TREND Micro） http://blog.trendmicro.co.jp/archives/14189

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. 2016 年 10 月のウイルスレビュー

関連記事	● 2016 年 10 月のウイルスレビュー（Dr. WEB） http://news.drweb.co.jp/?i=1104

2. 2016 年 11 月のウイルスレビュー

関連記事	● 2016 年 11 月のウイルスレビュー（Dr. WEB） http://news.drweb.co.jp/?i=1117

3. 2016 年 12 月のウイルスレビュー

関連記事	● 2016 年 12 月のウイルスレビュー（Dr. WEB） http://news.drweb.co.jp/?i=1129

4. 2016 年 10 月のモバイルマルウェア

関連記事	● 2016 年 10 月のモバイルマルウェア（Dr. WEB） http://news.drweb.co.jp/?i=1103

5. 2016 年 11 月のモバイルマルウェア

関連記事	● 2016 年 11 月のモバイルマルウェア（Dr. WEB） http://news.drweb.co.jp/?i=1116

6. 2016 年 12 月のモバイルマルウェア

関連記事	● 2016 年 12 月のモバイルマルウェア（Dr. WEB） http://news.drweb.co.jp/?i=1128

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＜2016.10.03＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.10.03＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20161003.html

2. チェックしておきたい脆弱性情報＜2016.10.11＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.10.11＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20161011.html

3. チェックしておきたい脆弱性情報＜2016.10.17＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.10.17＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20161017.html

4. チェックしておきたい脆弱性情報＜2016.10.24＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.10.24＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20161024.html

5. チェックしておきたい脆弱性情報＜2016.10.31＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.10.31＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20161031.html

6. チェックしておきたい脆弱性情報＜2016.11.07＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.11.07＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20161107.html

7. チェックしておきたい脆弱性情報＜2016.11.14＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.11.14＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20161114.html

8. チェックしておきたい脆弱性情報＜2016.11.21＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.11.21＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20161121.html

9. チェックしておきたい脆弱性情報＜2016.11.28＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.11.28＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20161128.html

10. チェックしておきたい脆弱性情報＜2016.12.05＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.12.05＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20161205.html

11. チェックしておきたい脆弱性情報＜2016.12.12＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.12.12＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20161212.html

12. チェックしておきたい脆弱性情報＜2016.12.19＞

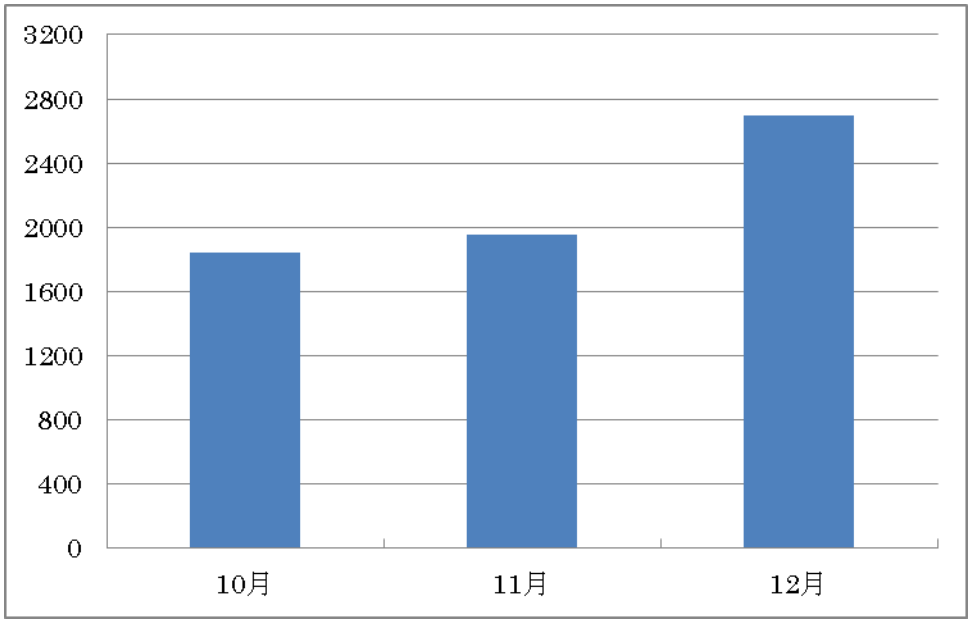
プレス リリース	● チェックしておきたい脆弱性情報＜2016.12.19＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20161219.html

13. チェックしておきたい脆弱性情報＜2016.12.26＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.12.26＞ http://www.hitachi.co.jp/hirt/publications/csirt/memo20161226.html

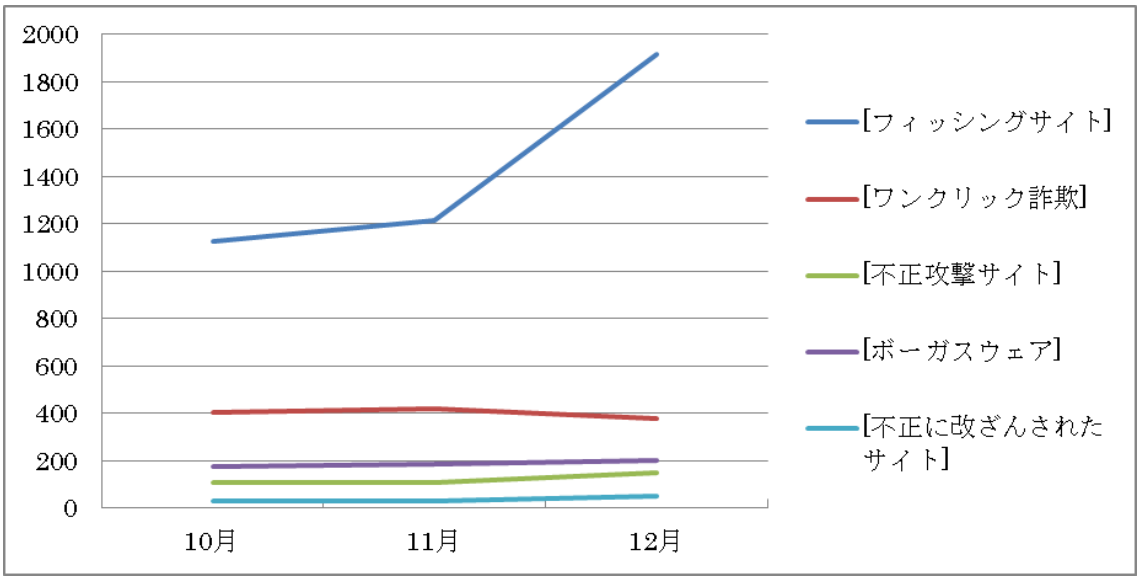
5. データからみるサイバー犯罪の傾向

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サイバー犯罪の傾向を以下に示します。



「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(2016 年 10 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、過去 1 年の平均である 2000 件と比較すると 10 月、11 月は 2000 件で変わらず横ばいに推移していますが、12 月は 700 件近く増加した 2700 件となっております。フィッシングサイトの項目で、過去 1 年の平均である 1200 件と比較すると、12 月は 700 件近く増加した 1900 件となっており過去 1 年で最高の件数となっております。これは、金融機関、オンラインゲーム等をかたるフィッシングに加え、11 月末に LINE、12 月に Apple をかたるフィッシングの報告が再び増えていることが原因です。このように利用者の多いサービス業者をかたるフィッシングメールの報告が増えており、今後も利用者の多いサービス業者をかたるフィッシングが増える可能性があります。フィッシングメールかどうか判断に迷う場合や不審な内容がある場合、各サービス事業者の問い合わせ窓口等に連絡することを推奨いたします。

6. 総括

今期は、ネットワークカメラや家庭用ルータ等の IoT 機器を狙った「Mirai」と呼ばれるマルウェアを悪用した DDoS 攻撃が流行しました。Mirai は、初期設定で使用されるユーザ名とパスワードを利用して IoT 機器をスキャン、ログインできた機器に感染し、DDoS 攻撃を行う踏み台として悪用されています。Mirai は、ソースコードがインターネット上に公開されており、世界中で Mirai によると推定される被害が報告されています。10 月 21 日に米 DNS サービスを提供している Dyn が Mirai に感染した推定 10 万台の IoT 機器を悪用した DDoS 攻撃を受け、サービスを利用する Twitter、Spotify、Reddit、Netflix 等が約 6 時間利用できなくなりました。対処法として、Mirai はメモリにのみ存在することから、感染したデバイスの電源を切ることで削除されます。また、IoT 機器はパスワードが初期設定の状態であると感染しやすいので、パスワードを強固なものに変更することで感染を防ぐことができます。Mirai に感染し知らない間に攻撃者の攻撃に加担しないためにも、家庭内の IoT 機器の設定を確認することを推奨いたします。

前期に引き続き、今期もランサムウェアによる被害が多く報告されています。ランサムウェアは感染した PC 上のファイルを暗号化し、攻撃者はファイルの復元することを引き換えに金銭を払えと脅してきます。主な感染経路は、ばらまき型のメールの添付ファイルを開くことや、改ざんしたサイトをアクセスさせ、ソフトウェアの脆弱性を利用して、PC 内にマルウェアをダウンロードさせるドライブバイダウンロード攻撃により感染します。ドライブバイダウンロード攻撃の際に、ソフトウェアの脆弱性を突く攻撃を行えるツールのことを Exploit Kit と呼びます。9 月中旬から「Rig Exploit Kit」によるドライブバイダウンロード攻撃が増加傾向にあります。この背景としては、これまで主流だった「Angler Exploit Kit」や「Neutrino Exploit Kit」が活動を停止したことがあげられます。このように、1 つの Exploit Kit が活動停止してもすぐに他の Exploit Kit が利用されてしまい攻撃は止まりません。対処法としては、ランサムウェアの被害から自身の PC を守るために、定期的なデータのバックアップや、ソフトウェアを最新の状態にアップデートすることを推奨いたします。また、ランサムウェアの種類を特定することで、種類やバージョンによっては、復号ツールが公開されている場合もあります。

株式会社　日立システムズ

〒141-8672 東京都品川区大崎 1-2-1

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

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