S.S.R.C.定期
トレンドレポート
Vol.26

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.26

目次

1. はじめに ..... - 2 -

2. ご利用条件 ..... - 2 -

3. トレンドレポート 2015 年第 4 四半期度版 ..... - 3 -

3.1. セキュリティトレンド情報 ..... - 3 -

4. 新種ウイルス情報 ..... - 15 -

4.1. 脆弱性情報 ..... - 17 -

5. データからみるサイバー犯罪の傾向 ..... - 20 -

6. 総括 ..... - 22 -

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 2015 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:2015/10/1～2015/12/31

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	● 【注意喚起】 Internet Explorer のサポートポリシーが変更、バージョンアップが急務に（IPA） http://www.ipa.go.jp/security/ciadr/vul/20151215-IEsupport.html ● 旧バージョンの「IE」はどれほど使われている？--サポート終了迫る（ZDNet Japan） http://japan.zdnet.com/article/35075178/ ● MS、「Windows 10」初のメジャーアップデートを提供開始（CNET Japan） http://japan.cnet.com/news/service/35073434/ ● Microsoft、ブラウザセキュリティ強化でドライブバイ攻撃も阻止（IT media） http://www.itmedia.co.jp/enterprise/articles/1512/18/news056.html ● マイクロソフト、中間者（MiTM）手法を用いたアドウェアを禁止へ（CNET Japan） http://japan.cnet.com/news/service/35075450/ ● Windows 10 のメジャーUD で一部 ESET 製品に不具合 - マルウェア対策がオフに（Security NEXT） http://www.security-next.com/064296 ● Microsoft、更新プログラムで Dell の証明書を無効化（IT media） http://www.itmedia.co.jp/enterprise/articles/1512/02/news048.html

2. Apple

関連記事	● Mac OS X 上に望まないアプリケーションをインストールするマルウェア (Dr.Web) http://news.drweb.co.jp/show/?i=957 ● Apple OS X のスクリプトエディタにおいて遠隔から任意のコードが実行されてしまう脆弱性（Scan Tech Report）（Scan NetSecurity） http://scan.netsecurity.ne.jp/article/2015/11/09/37647.html ● OS X の既知脆弱性を狙う攻撃コード - 「Yosemite」以前はゼロデイ状態 (Security NEXT) http://www.security-next.com/064013 ● Apple の「Gatekeeper」が破られる恐れ、マルウェアに利用も（IT media） http://www.itmedia.co.jp/enterprise/articles/1510/01/news130.html ● 新たな iOS マルウエア「YiSpecter」、非脱獄デバイスも攻撃（IT pro） http://itpro.nikkeibp.co.jp/atcl/news/15/100603271 ● ロックされた iPhone のデータ、Apple でも取り出しは不可能（IT media） http://www.itmedia.co.jp/news/articles/1510/21/news137.html ● Apple、独自のルート証明書をインストールする iOS アプリを App Store から削除（財経新聞） http://www.zaikei.co.jp/article/20151012/273445.html

3. Adobe

関連記事	● Flash Player にまたゼロデイ脆弱性、前日の更新で修正されず（IT pro） http://itpro.nikkeibp.co.jp/atcl/news/15/101403383/ ● Apple、セキュリティ上の懸念を理由に広告ブロックアプリの一部を削除（マイナビニュース） http://news.mynavi.jp/news/2015/10/13/146/ ● 12 月修正の「Flash Player」脆弱性が攻撃対象に - 確実にアップデートを（Security NEXT） http://www.security-next.com/065457 ● Flash Player の脆弱性対策情報、今年は 9 月時点で 190 件、すでに昨年 1 年間の 2.5 倍（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/20151026_727485.html ● Flash 更新しない層が 2 割弱、Java では 3 割-IPA 調査（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/20151229_737384.html ● 「Pawn Storm 作戦」で利用された Flash Player の脆弱性、Adobe の緩和策を回避（トレンドマイクロ） http://blog.trendmicro.co.jp/archives/12380 ● アドビ、「Flash Professional」を「Animate CC」に名称変更--HTML5 に軸足（CNET Japan） http://japan.cnet.com/news/service/35074309/

4. Android

関連記事	● 新たな「Stagefright」脆弱性--1 件は「Android」端末ほぼすべてに影響（CNET Japan） http://japan.cnet.com/news/service/35071335/ ● 悪質な Android アドウェア、世界 20 カ国で流通（IT media） http://www.itmedia.co.jp/enterprise/articles/1510/08/news048.html ● 「Android」フォンの 87%で脆弱性が放置--ケンブリッジ大調査（ZDNet Japan） http://japan.zdnet.com/article/35071874/ ● Android 端末の 87%に 11 件の脆弱性、英研究者が指摘（プライスウォーターハウスクーパース）（IT media ） http://www.itmedia.co.jp/enterprise/articles/1510/15/news055.html ● root 権限奪取の Android アドウェア、削除ほぼ不可の進化版（IT media） http://www.itmedia.co.jp/enterprise/articles/1511/05/news053.html ● 「Apache Cordova」に複数の脆弱性 - 作成した Android アプリに影響（Security NEXT） http://www.security-next.com/064670

5. 情報漏洩

関連記事	● 米オンライン証券会社にも不正アクセス、460 万人の顧客情報が流出（IT media） http://www.itmedia.co.jp/enterprise/articles/1510/06/news045.html ● 英通信会社 TalkTalk にサイバー攻撃、契約者 400 万人の情報流出の可能性（IT media） http://www.itmedia.co.jp/enterprise/articles/1510/26/news035.html ● 無料 Web ホスティング業者に不正アクセス、1350 万人超の情報流出（IT media） http://www.itmedia.co.jp/enterprise/articles/1510/30/news066.html ● VTech の個人情報流出は 1170 万件、保護者と子どもに被害（IT media） http://www.itmedia.co.jp/enterprise/articles/1512/03/news063.html ● T-Mobile の顧客情報 1500 万件が漏洩（TechCrunch） http://jp.techcrunch.com/2015/10/02/20151001records-of-15-million-t-mobile-customers-swept-up-in-experian-hack/ ● サンリオ、330 万人のユーザー情報流出との報道で調査（REUTERS） http://jp.reuters.com/article/sanrio-idJPKBN0U42PN20151222 ● 約 68 万人の有権者データの流出が判明､インターネット上で閲覧可能な状態に(堺市）（Scan NetSecurity） http://scan.netsecurity.ne.jp/article/2015/12/17/37830.html ● 「シネマイクスピアリ」Web サーバに不正アクセス、2,432 名の個人情報が漏えい(イクスピアリ）（Scan NetSecurity） http://scan.netsecurity.ne.jp/article/2015/12/03/37753.html ● メルマガ配信システムに不正アクセス、アドレス 2000 件が削除 - 那覇市（SNEXT） http://www.security-next.com/063642 ● 東ガス子会社に不正アクセス、顧客情報が漏洩 - 攻撃試行の痕跡は 2012 年から（Security NEXT） http://www.security-next.com/064293

6. サイバー攻撃

関連記事	● ソウル地下鉄にハッキング　北朝鮮のサイバー攻撃か（朝日新聞 DIGITAL） http://www.asahi.com/articles/ASHB54D14HB5UHBI011.html ● 「イスラム国」がアメリカの電力会社にハッキング（TV asahi） http://news.tv-asahi.co.jp/news_international/articles/000060748.html ● 対南サイバー攻撃毎日１００万件…北朝鮮の非対称威嚇（中央日報） http://japanese.joins.com/article/267/208267.html ● 米政府、JP モルガンなど狙ったサイバー攻撃で 3 人を起訴（CNET Japan） http://japan.cnet.com/news/business/35073397/ ● 2015 年 3Q の DDoS 攻撃は 23%増 - 半数がネットゲーム狙い（Security NEXT） http://www.security-next.com/065071 ● イラン、ＮＹ郊外のダムをサイバー攻撃　情報収集目的？（Security NEXT） http://www.sankei.com/world/news/151222/wor1512220012-n1.html ● 2015 年 3Q の DDoS 攻撃は 23%増 - 半数がネットゲーム狙い（Security NEXT） http://www.security-next.com/065071 ● 新たな「BackStab」攻撃の研究結果を公開、日本でも 218 件の攻撃を確認（パロアルトネットワークス）（Scan NetSecurity） http://scan.netsecurity.ne.jp/article/2015/12/25/37866.html ● 日経サイトにサイバー攻撃「ＤＤｏＳ攻撃」か　閲覧不安定「アノニマス」関与の可能性も（産経ニュース） http://www.sankei.com/affairs/news/151111/afr1511110040-n1.html ● 北欧の捕鯨国が､アノニマスに攻撃された（東洋経済 ONLINE） http://toyokeizai.net/articles/-/94499 ● 不正アクセス 他人ＦＢ侵入容疑　男逮捕、７００人ＩＤ盗む？　警視庁、初の立件（毎日新聞） http://mainichi.jp/articles/20151110/dde/041/040/019000c

7. 脆弱性

関連記事	● WinRAR に脆弱性報告、遠隔操作される恐れ（IT media） http://www.itmedia.co.jp/enterprise/articles/1510/01/news097.html ● Windows 版 Python に意図しない DLL ファイル読み込む脆弱性（Security NEXT） http://www.security-next.com/063055 ● 航空業界向け Datalex 製ソフトに脆弱性 - すでに修正済み（Security NEXT） http://www.security-next.com/063095 ● Apache HTTP Server の mod_headers モジュールにおけるディレクティブを回避される脆弱性（JVN） http://jvndb.jvn.jp/ja/contents/2013/JVNDB-2013-006321.html ● アバストにおけるディレクトリトラバーサルの脆弱性（JVN） http://jvn.jp/jp/JVN25576608/ ● Oracle Java の脆弱性対策について(CVE-2015-4835 等) (IPA) http://www.ipa.go.jp/security/ciadr/vul/20151021-jre.html ● NTP に脆弱性、システム時刻を変更される恐れ（IT media） http://www.itmedia.co.jp/enterprise/articles/1510/23/news052.html ● 2015 年 3Q の脆弱性届出は 213 件 - ソフトとサイトいずれも増加（Security NEXT） http://www.security-next.com/063762 ● Java ライブラリに脆弱性、主要ミドルウェア全てに影響（IT media） http://www.itmedia.co.jp/enterprise/articles/1511/10/news053.html ● PowerDNS の権威 DNS サーバに DoS 攻撃のおそれ（Security NEXT） http://www.security-next.com/064279 ● 攻撃サイトへの誘導、国内から 170 万件超 - 正規サイト経由が 8 割超（Security NEXT） http://www.security-next.com/064422

	● 脆弱性攻撃サイト誘導元の 8 割が「汚染された正規サイト」（ZDNet Japan） http://japan.zdnet.com/article/35073836/ ● Zoho のファイアウォール管理製品に複数の脆弱性（Security NEXT） http://www.security-next.com/064723 ● BIND 9 に DoS 攻撃受ける恐れ - 異常終了する脆弱性が判明（Security NEXT） http://www.security-next.com/065246 ● VMware、Apache Commons Collections 関連の脆弱性を修正（IT media） http://www.itmedia.co.jp/enterprise/articles/1512/21/news039.html ● 脆弱性が未修正の「Joomla！」狙う攻撃が増加 - 1 日あたり 1 万 6600 件（Security NEXT） http://www.security-next.com/065534 ● Juniper 製品のバックドア用パスワード公開、SANS が警戒レベル引き上げ（IT media） http://www.itmedia.co.jp/enterprise/articles/1512/22/news056.html

8. ランサムウェア

関連記事	● 世界で被害総額 3 億ドル以上というランサムウェアを分析（Scan NetSecurity） http://scan.netsecurity.ne.jp/article/2015/11/04/37619.html ● Web サーバを攻撃する Linux 上のランサムウェアが出没、身代金は 1 ビットコイン（TechCrunch） http://jp.techcrunch.com/2015/11/07/20151106linux-ransomware-is-now-attacking-webmasters/ ● LINE で「身代金要求型ウイルス」を販売、容疑の少年を再逮捕（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/20151124_732059.html ● ランサムウェア「CryptoWall」に新手の亜種、2 段階攻撃で拡散（IT media） http://www.itmedia.co.jp/enterprise/articles/1512/04/news057.html ● 「.vvv」ウイルスの被害と対策。強制暗号＝ランサムウェアが、サイト表示＝広告だけで感染してしまう（YAHOO!ニュース） http://bylines.news.yahoo.co.jp/mikamiyoh/20151206-00052167/ ● 「vvv ランサムウェア」は Flash 脆弱性で感染、「Angler EK」で拡散 - カスペが分析（Security NEXT） http://www.security-next.com/064949 ● 「vvv ウイルス」ばらまき型メールが 12 月 8 日以降増加、警視庁も「添付ファイル開かないで」と注意呼び掛け（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/20151211_735005.html ● 12 月のランサムウェア感染、Web サイト経由は WordPress の脆弱性を悪用? (マイナビ ニュース) http://news.mynavi.jp/news/2015/12/24/498/ ● 過去 1 年に 8.1%がマルウェア感染 -「ランサムウェア」被害は 0.3%（IT media ） http://www.security-next.com/065471

9. フィッシング

関連記事	● 金融庁をかたるフィッシング（2015/10/16）（フィッシング対策協議会） https://www.antiphishing.jp/news/alert/fsa_20151016.html ● J:com をかたるフィッシング（フィッシング対策協議会） https://www.antiphishing.jp/news/alert/jcom_20151020.html ● みずほ銀の偽サイトへ誘導するフィッシング SMS（Security NEXT） http://www.security-next.com/063796 ● OMC カード利用者狙うフィッシング - 会員向けサイトを偽装（Security NEXT） http://www.security-next.com/064115 ● ジャパンネット銀行の偽サイトに注意 - 中国語含む SMS で誘導（Security NEXT） http://www.security-next.com/064222 ● 住信 SBI ネット銀行をかたるフィッシング（2015/11/30）（フィッシング対策協議会） https://www.antiphishing.jp/news/alert/sbi_20151130.html ● はまぎん装うフィッシングに注意 - 他行攻撃の文面を使い回し（Security NEXT） http://www.security-next.com/064863 ● ゆうちょ銀行装うフィッシング - 複数パターンで攻撃（Security NEXT） http://www.security-next.com/065195 ● 「マイナンバーが漏洩した」「交付できない」と騙す詐欺メールに注意（Security NEXT） http://www.security-next.com/064252

10. マルウェア

関連記事	● Linux ユーザーを脅かす Rekoobe トロイの木馬（Dr.WEB） http://news.drweb.co.jp/show/?i=955 ● Hyatt の決済システムでマルウェア感染、またもホテルで発覚（IT media） http://www.itmedia.co.jp/enterprise/articles/1512/25/news068.html ● Linux マルウェアの DDoS 攻撃、アジアに集中砲火（IT media） http://www.itmedia.co.jp/enterprise/articles/1509/30/news137.html ● IoT のセキュリティを強化するマルウェア「Linux.Wifatch」--シマンテックが報告（ZDNet Japan） http://japan.zdnet.com/article/35071416/ ● バンキングマルウェア「SHIFU」を検知・防御できたことを検証（FFRI）（Scan NetSecurity） http://scan.netsecurity.ne.jp/article/2015/10/15/37492.html ● 「Magento」利用の EC サイトに不正なコード、マルウェア感染の踏み台に（IT media） http://www.itmedia.co.jp/enterprise/articles/1510/20/news049.html ● FAX 受信通知や企業名を騙るメールを複数検知、30 件でマルウェアを DL（日本 IBM）（Scan NetSecurity） http://scan.netsecurity.ne.jp/article/2015/10/30/37591.html ● MySQL サーバへのマルウェア注入攻撃に注意 - DDoS 攻撃の踏み台に（Security NEXT） http://www.security-next.com/064062 ● 感染したコンピューターへのアクセスを可能にするトロイの木馬（Dr.WEB） http://news.drweb.co.jp/show/?i=942 ● 大手ホテルの POS 端末にマルウェア、米国やハワイの Sheraton などに影響（IT media） http://www.itmedia.co.jp/news/articles/1511/24/news049.html

	● 中国におけるコンピューターウイルス感染率が再び上昇傾向、2014 年調査で 63.7%、携帯端末では 31.5%（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/20151008_724728.html ● 改ざん Xcode 使用アプリ、米国や日本企業にも侵入（IT media） http://www.itmedia.co.jp/enterprise/articles/1511/05/news054.html ● 金融機関を狙う「Dyre」マルウェア、「Windows 10」と「Edge」ブラウザも標的に（ZDNet Japan） http://japan.zdnet.com/article/35073797/ ● 不正送金に悪用できるウイルス保管容疑、中２男子を逮捕（朝日 DIGITAL） http://www.asahi.com/articles/ASHC42TZ3HC4UTIL003.html ● iOS のバックアップデータを盗む BackStab 攻撃発生、日本でも確認（IT media） http://www.itmedia.co.jp/enterprise/articles/1512/08/news136.html ● 新たな iOS マルウェア出現、非脱獄版にも感染（IT media） http://www.itmedia.co.jp/enterprise/articles/1510/06/news044.html ● もう「iPhone だから安全」ではない、誰にでも感染し得る iOS 向けマルウエアの脅威（IT pro） http://itpro.nikkeibp.co.jp/atcl/column/15/040800083/102100028/

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. 2015 年 10 月の世界の月間マルウェアランキングを公開

プレス リリース	● マルウェアランキング(世界のランキング) (ESET) http://canon-its.jp/product/eset/topics/malware1510.html

2. 2015 年 10 月の日本の月間マルウェアランキングを公開

プレス リリース	● マルウェアランキング(日本のランキング) (ESET) http://canon-its.jp/product/eset/topics/malware1510_jp.html

3. 2015 年 10 月のウイルスレビュー

関連記事	● 2015 年 10 月のウイルスレビュー (Dr. WEB) http://news.drweb.co.jp/?i=938

4. 2015 年 11 月のウイルスレビュー

関連記事	● 2015 年 11 月のウイルスレビュー (Dr. WEB) http://news.drweb.co.jp/?i=954

5. 2015 年 12 月のウイルスレビュー

関連記事	● 2015 年 12 月のウイルスレビュー (Dr. WEB) http://news.drweb.co.jp/?i=966

6. 2015 年 10 月の Android マルウェア

関連記事	● 2015 年 10 月の Android マルウェア (Dr. WEB) http://news.drweb.co.jp/?i=939

7. 2015 年 11 月の Android マルウェア

関連記事	● 2015 年 11 月の Android マルウェア（Dr. WEB） http://news.drweb.co.jp/?i=953

8. 2015 年 12 月の Android マルウェア

関連記事	● 2015 年 12 月の Android マルウェア（Dr. WEB） http://news.drweb.co.jp/?i=967

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＜2015.10.06＞

プレス リリース	● チェックしておきたい脆弱性情報＜2015.10.06＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/100400080/

2. チェックしておきたい脆弱性情報＜2015.10.13＞

プレス リリース	● チェックしておきたい脆弱性情報＜2015.10.13＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/100400081/

3. チェックしておきたい脆弱性情報＜2015.10.19＞

プレス リリース	● チェックしておきたい脆弱性情報＜2015.10.19＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/101500082/

4. チェックしておきたい脆弱性情報＜2015.10.26＞

プレス リリース	● チェックしておきたい脆弱性情報＜2015.10.26＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/101600083/

5. チェックしておきたい脆弱性情報＜2015.11.10＞

プレス リリース	● チェックしておきたい脆弱性情報＜2015.11.10＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/110500084/

6. チェックしておきたい脆弱性情報＜2015.11.13＞

プレス リリース	● チェックしておきたい脆弱性情報＜2015.11.13＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/110700085/

7. チェックしておきたい脆弱性情報＜2015.11.16＞

プレス リリース	● チェックしておきたい脆弱性情報＜2015.11.16＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/110700086/

8. チェックしておきたい脆弱性情報＜2015.11.30＞

プレス リリース	● チェックしておきたい脆弱性情報＜2015.11.30＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/112600087/

9. チェックしておきたい脆弱性情報＜2015.12.03＞

プレス リリース	● チェックしておきたい脆弱性情報＜2015.12.03＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/112900088/

10. チェックしておきたい脆弱性情報＜2015.12.07＞

プレス リリース	● チェックしておきたい脆弱性情報＜2015.12.07＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/112900089/

11. チェックしておきたい脆弱性情報＜2015.12.17＞

プレス リリース	● チェックしておきたい脆弱性情報＜2015.12.17＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/121500090/

12. チェックしておきたい脆弱性情報＜2015.12.18＞

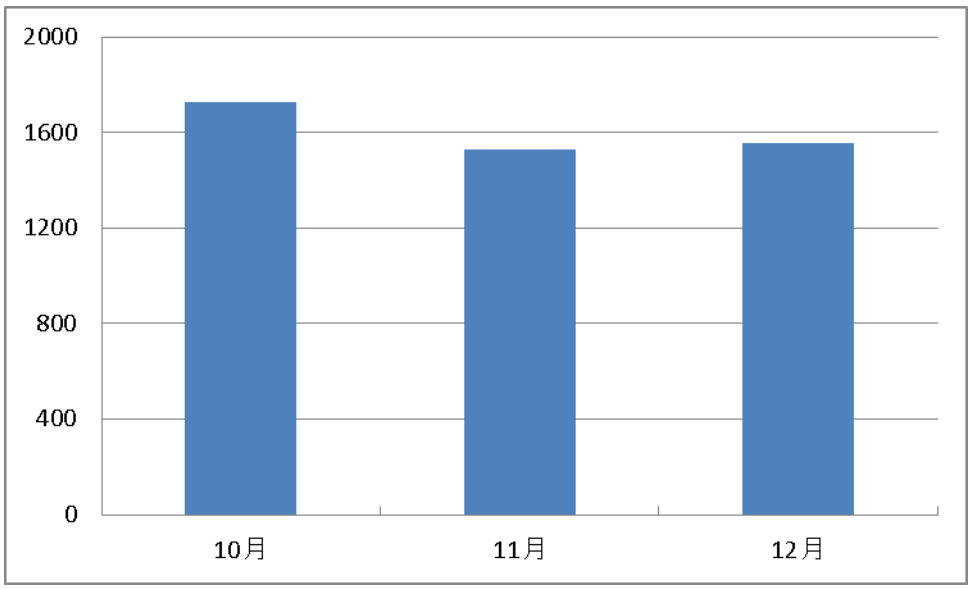
プレス リリース	● チェックしておきたい脆弱性情報＜2015.12.18＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/121500091/

13. チェックしておきたい脆弱性情報＜2015.12.22＞

プレス リリース	● チェックしておきたい脆弱性情報＜2015.12.22＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/121500092/

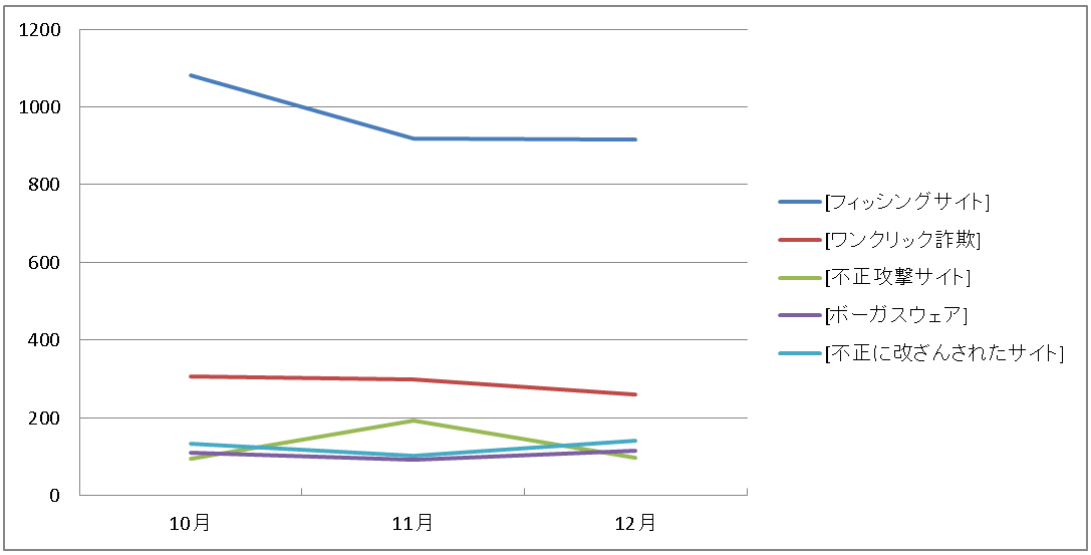
5. データからみるサイバー犯罪の傾向

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(2015 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を見ると前期と比較して全体的に減少していることがわかります。脅威別検知数のフィッシングサイトの検知数が他月より多いのは偽ブランド品のフィッシングサイトが多く検知されたからです。脅威別検知数について他の項目の推移を見てみると、不正攻撃サイト以外は殆ど横ばいであり、不正攻撃サイトは特定サイトへの多数の検知があったことから 11 月が増加しています。

6. 総括

今期は 拡張子が(.vvv)であることから vvv ウイルスと呼称されるランサムウェア「TeslaCrypt」が大きな騒ぎとなりました。このランサムウェアは、自身のパソコンだけでなく外部ストレージやネットワークドライブのファイルを暗号化し、復号するには身代金が必要だと脅してきます。このようなランサムウェアは以前から存在していましたが、Web サイトの広告を見るだけで感染されるといった噂が流れたことで大きな騒ぎとなりました。実際の感染経路はメールの添付ファイルやドライブバイダウンロードを使われていました。ランサムウェア対策としては、インストールしているソフトウェアを最新にすることや、アンチウイルスソフトの導入と最新の定義ファイルに保つこと、不審な添付ファイルを実行しないこと、ネットワーク接続していないストレージへの定期的なバックアップをすることが挙げられます。ランサムウェアはパソコン内の大切なデータを使用不可能にする危険性があります。そのため前述の対策を推奨いたします。

Microsoft 社の Internet Explorer(IE)のサポートポリシーが変更になり 2016 年 1 月 12 日(米国時間)を過ぎると使用している OS でサポートされる、最新版の IE だけが技術サポートとセキュリティ更新を受けられることになりました。サポート終了後のソフトウェアを利用し続けると新たな脆弱性に対して根本的な対策を行うことが出来なくなります。各 OS に対する最新の IE(*1)を確認し最新版へのアップデートを推奨いたします。IE7,8 が社内システム等に必要なため最新版へ更新できない場合、IE11 では「エンタープライズモード」(*2)による IE7,8 の動作エミュレートで互換性を保つことが可能です。

また、12 月の Windows Update では Outlook2010 がセーフモードで起動するという不具合がありました。毎月ある Windows Update を行う際はパッチに関する情報収集や検証環境を利用した動作確認をしてからアップデートすることを推奨いたします。

(*1) Internet Explorer のサポートポリシーが変わりました。(Microsoft)

https://www.microsoft.com/japan/msbc/Express/ie_support/

(*2) エンタープライズ モードとは (Microsoft)

https://technet.microsoft.com/ja-jp/library/dn640687.aspx

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