株式会社 日立システムズ

SSRC-TR-Vol.22

S.S.R.C.定期
トレンドレポート
Vol.22

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.22

目次

1. はじめに ..... - 2 -
2. ご利用条件 ..... - 2 -
3. トレンドレポート 2014 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 ..... - 14 -
4.1. 脆弱性情報 ..... - 16 -
5. データからみるサイバー犯罪の傾向 ..... - 19 -
6. 総括 ..... - 21 -

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 2014 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:2014/10/1～2014/12/31

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. ソニーピクチャーズ

関連記事	● ソニーピクチャーズにサイバー攻撃か、米メディアが報道（IT pro） http://itpro.nikkeibp.co.jp/atcl/news/14/112602024/ ● ソニーピクチャーズへのサイバー攻撃、北朝鮮が関与か（IT pro） http://itpro.nikkeibp.co.jp/atcl/news/14/120102067/ ● ソニー・ピクチャーズがサイバー攻撃に反撃、盗まれた情報の流通を妨害（IT media） http://www.itmedia.co.jp/news/articles/1412/12/news051.html ● 盗まれたソニーの電子証明書によって署名されたマルウェアで一騒動（Slashdot） http://security.slashdot.jp/story/14/12/15/0610251/ ● ソニー・ピクチャーズへの大規模なサイバー攻撃を教訓に緊急提言（Scan NetSecurity） http://scan.netsecurity.ne.jp/article/2014/12/24/35461.html

2. ShellShock

関連記事	● 次々に発覚する bash の脆弱性、最新のパッチ適用を（IT media） http://www.itmedia.co.jp/enterprise/articles/1410/06/news038.html ● 「bash」の脆弱性狙う攻撃が継続中 - 「Webmin」もターゲットに（Security NEXT） http://www.security-next.com/052684 ● bash の脆弱性への攻撃、13 日間で 53,000 件以上を観測（Scan NetSecurity） http://scan.netsecurity.ne.jp/article/2014/10/10/34976.html ● 【脆弱性】「Shellshock」攻撃、1 日あたり平均 6.1 件（Security NEXT） http://www.security-next.com/052750 ● 「Shellshock」攻撃でサーバがマルウェア感染 - 大阪府立産業技研（Security NEXT） http://www.security-next.com/053281 ● 米ヤフー、「Shellshock」脆弱性によるハッカー攻撃の指摘受け回答（CENT Japan） http://japan.cnet.com/news/service/35054771/

3. スマートフォン

関連記事	● Android 版「Yahoo！ボックス」に脆弱性 - 中間者攻撃のおそれ（Security NEXT） http://www.security-next.com/052524 ● Android のメモリカードデータを消去し通信をブロックする「荒らし」トロイの木馬（Dr. WEB） http://news.drweb.co.jp/show/?i=787&lng=ja&c=1 ● 香港のデモ隊をスパイする Android トロイの木馬（Dr. WEB） http://news.drweb.co.jp/show/?i=788&lng=ja&c=1 ● 韓国のユーザを狙った Android 端末向け不正アプリを追跡（トレンドマイクロ） http://blog.trendmicro.co.jp/archives/10302

	● スマホを狙うマルウェア、「PUA」「トロイの木馬」で全体の 95%を占める（Scan NetSecurity） http://scan.netsecurity.ne.jp/article/2014/11/13/35207.html ● Android ファームウェアに潜むマルウェア（Dr. WEB） http://news.drweb.co.jp/show/?i=804&lng=ja&c=1 ● Android 不正アプリによる RFID プリペイドカード改ざんが南米で発生（トレンドマイクロ） http://blog.trendmicro.co.jp/archives/10432 ● '個人情報や金銭を盗む Android マルウェア（Dr. WEB） http://news.drweb.co.jp/show/?i=811&lng=ja&c=1 ● 中国企業の Android スマホにバックドア、セキュリティ企業が発見（IT media） http://www.itmedia.co.jp/enterprise/articles/1412/18/news045.html ● App Store の偽アプリ：iPhone／iPad 利用者を狙う詐欺行為を確認 トレンドマイクロ） http://blog.trendmicro.co.jp/archives/10058 ● 不正サイトの検知数が上昇 - iPhone6 便乗詐欺も（Security NEXT） http://www.security-next.com/052862

4. DDoS

関連記事	● DDoS 攻撃が大規模化、100Gbps 超の攻撃が 3 カ月間で 17 件発生 - Akamai 報告（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/20141024_672910.html ● ファイナルファンタジー XIV のゲームサーバ群が DDoS 攻撃を受けていたと発表（Scan NetSecurity） http://scan.netsecurity.ne.jp/article/2014/11/23/35271.html ● RSA 幹部がサイバー犯罪のサービス化を指摘、DDoS 攻撃は 1 時間 8 ドル（IT pro） http://itpro.nikkeibp.co.jp/atcl/news/14/120502147/ ● ソニー攻撃、今度は米国の PlayStation Network がダウン――DDoS か(IT media) http://www.itmedia.co.jp/news/articles/1412/09/news050.html ● DDoS 攻撃:大量データ送りダウン 闇サイトに代行業者（毎日新聞） http://mainichi.jp/select/news/20141230k0000m040088000c.html

5. 不正ログイン・アクセス

関連記事	● 後を絶たない不正ログイン - 今年の被害総数 79 万件に（So-net） http://security-t.blog.so-net.ne.jp/2014-10-02 ● AT&T の従業員が顧客情報に不正アクセス（IT media） http://www.itmedia.co.jp/news/articles/1410/07/news047.html ● バリューコマース、不正ログインを受け個人情報が流出（情報漏洩ニュース） http://blog.livedoor.jp/antitheft/archives/1791760.html ● ＯＣＮに不正アクセスした疑い 中国籍の会社員を逮捕（朝日新聞） http://www.asahi.com/articles/ASGD930X3GD9UTIL004.html ● ICANN に不正アクセス、ユーザー情報が流出（IT media） http://www.itmedia.co.jp/enterprise/articles/1412/18/news046.html

6. 改ざん

関連記事	● 愛媛県武道館のＨＰ改ざん アダルトサイトへ誘導（47NEWS） http://www.47news.jp/CN/201410/CN2014100201001798.html ● 産経新聞、健康情報サイトを閉鎖 - 不正アクセスによる改ざんの可能性（Security NEXT） http://www.security-next.com/053237 ● 技術評論社サイトが改ざん被害　フィッシング原因でサーバ OS を入れ替えられる（IT media） http://www.itmedia.co.jp/news/articles/1412/08/news144.html ● 同一詐欺グループで 7 万件のドメイン取得 - 正規サイト改ざんで SEO（Security NEXT） http://www.security-next.com/054793 ● 「シリア電子軍」の Web ハッキング、Gigya のドメイン情報改ざんが原因（IT media） http://www.itmedia.co.jp/news/articles/1411/28/news059.html ● 水飲み場攻撃で狙われた日本バスケ協会のサイトが再び改ざん被害（Security Next） http://www.security-next.com/054211

7. フィッシング

関連記事	● Facebook を騙る英語のフィッシングサイトを確認、注意を呼びかけ（Scan NetSecurity） http://scan.netsecurity.ne.jp/article/2014/10/08/34957.html ● 三菱東京 UFJ 銀行のフィッシング攻撃が再発 - 「アカウントを凍結」で不安煽る（Security NEXT） http://www.security-next.com/052960 ● 「ドラゴンクエスト X」利用者から共通アカウントや OTP を騙し取るフィッシング（Security NEXT） http://www.security-next.com/053173 ● アカウントやカード情報狙うフィッシング横行、銀行とゲームが標的に（So-net） http://security-t.blog.so-net.ne.jp/2014-10-30 ● 減少傾向だったフィッシング、10 月に再び増加（Security NEXT） http://www.security-next.com/054544

8. POS

関連記事	● 米小売チェーンから再びカード情報流出か、POS マルウェア感染の疑い（IT media） http://www.itmedia.co.jp/news/articles/1410/22/news045.html ● 新しい POS マルウェアを確認。クリスマス商戦が狙いか（トレンドマイクロ） http://blog.trendmicro.co.jp/archives/10453 ● ロシアのアンダーグラウンドで確認された POS マルウェア「LusyPOS」（トレンドマイクロ） http://blog.trendmicro.co.jp/archives/10544

9. ランサムウェア

関連記事	● 9 月以降、国内でランサムウェアが増加傾向（Security NEXT） http://www.security-next.com/052706 ● YouTube 上の偽広告からランサムウェア感染へ誘導、主に米国で被害（トレンドマイクロ） http://blog.trendmicro.co.jp/archives/10094 ● 人質ファイルを 1 つ解放するランサムウエア「CoinVault」（IT pro） http://itpro.nikkeibp.co.jp/atcl/column/14/264220/120400022/ ● 2014 年 3Q にマルウェア総数が 3 億件を突破 - 新種のランサムウェアが大幅増（Security NEXT） http://www.security-next.com/054483 ● ランサムウェア「REVETON」、従来の手法に新たな感染経路を追加して感染拡大（トレンドマイクロ） http://blog.trendmicro.co.jp/archives/10579 ● 日本語対応ランサムウェア「法律違反、30 万円払え」と脅迫（Security NEXT） http://www.security-next.com/054605 ● 日本でも感染報告、急増中の脅迫ウイルス「Crowti」に注意（PC Online） http://pc.nikkeibp.co.jp/article/news/20141104/1146705/

10. 情報漏洩

関連記事	● JPMorgan へのサイバー攻撃、7600 万世帯と 700 万社の情報が流出（IT media） http://www.itmedia.co.jp/enterprise/articles/1410/03/news042.html ● 米で相次ぐマルウェアのカード情報流出、今度は大手チェーン 2 社から（IT media） http://www.itmedia.co.jp/news/articles/1410/14/news034.html ● Dropbox のアカウント情報約 700 万件が流出？　Dropbox はシステム侵害を否定（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/20141014_671192.html ● 通販サイトでカード情報 2 万 2000 件が流出 - セキュリティコードも（Security NEXT） http://www.security-next.com/053582 ● 1500 人分の ID を中国に販売　プロキシサーバ運営 2 社、無線ルータから流出(IT media) http://www.itmedia.co.jp/news/articles/1411/21/news061.html ● 共同通信社の業務用 PC2 台がマルウェア感染 - 顧客情報流出の可能性（Security NEXT） http://www.security-next.com/054502 ● 米郵政公社にサイバー攻撃、職員 80 万人の個人情報が流出か（IT media） http://www.itmedia.co.jp/enterprise/articles/1411/11/news044.html

11. Apple

関連記事	● 香港の民主派活動にサイバー攻撃？　iOS の高度なマルウェア出現（IT media） http://www.itmedia.co.jp/enterprise/articles/1410/02/news036.html ● 発見された新たな Mac OS X ボットネット（Dr. WEB） http://news.drweb.co.jp/show/?i=784&lng=ja&c=1 ● 中国の iCloud ユーザーを狙ったサイバー攻撃、中国政府が関与か（IT　pro） http://itpro.nikkeibp.co.jp/atcl/news/14/102201550/ ● 「iMessage」を狙ったスパムが急増--セキュリティ企業（CENT Japan） http://japan.cnet.com/news/business/35055690/ ● OS X Yosemite に脆弱性、管理者がパスワードなしで root 権限を得られる？（Slashdot） http://security.slashdot.jp/story/14/11/04/0824241/ ● OS X を狙うマルウェアの詳細判明、Apple 対策に不安の声も（IT　media） http://www.itmedia.co.jp/enterprise/articles/1411/06/news049.html ● 非“脱獄”の iOS にも感染するマルウェア現る、中国で大量流通（IT　media） http://www.itmedia.co.jp/enterprise/articles/1411/07/news051.html ● iOS 端末を狙う「WireLurker」、Windows を経由するバージョンも発見される（CNET Japan） http://japan.cnet.com/news/service/35056342/ ● iOS デバイス上の正規アプリを不正アプリに置き換える攻撃手法の詳細が明らかに（Slashdot） http://apple.slashdot.jp/story/14/11/13/0351206/ ● 脱獄済み iOS 狙う RAT 亜種が登場、非公式アプリストアで拡散（Security NEXT） http://www.security-next.com/054647 ● 動画サイト経由でアドウェアが拡大 - 標的は Mac OS X　（Security NEXT） http://www.security-next.com/053439

12. Microsoft

関連記事	● Windows シェルにも bash に似た脆弱性か（IT media） http://www.itmedia.co.jp/enterprise/articles/1410/07/news048.html ● 【Sandworm】「Windows OLE」にゼロデイ攻撃が 1 年以上 - 容易に悪用可能で拡大注意(Security NEXT) http://www.security-next.com/052837 ● マイクロソフト、10 月のセキュリティ更新プログラムで一部ユーザーに不具合(ZDNet Japan) http://japan.zdnet.com/security/analysis/35055380/ ● MS の一部更新プログラムに不具合 - ハングアップのおそれ（Security Next） http://www.security-next.com/054425 ● Exchange Server の更新プログラムに不具合、一部を配信停止（IT media） http://www.itmedia.co.jp/news/articles/1412/12/news050.html

13. ネットバンキング

関連記事	● 法人のネットバンク被害が拡大 - 地銀被害が主要行を上回る（Security NEXT） http://www.security-next.com/053127 ● 韓国の銀行を狙うオンライン銀行詐欺ツール、C&C サーバへの経路に Pinterest を利用（トレンドマイクロ） http://blog.trendmicro.co.jp/archives/10587

14. ゼロデイ攻撃

関連記事	● 「Windows OLE」に脆弱性、ゼロデイ攻撃が発生中 - 「Sandworm」とは別物（Security NEXT） http://www.security-next.com/053031 ● 一太郎へのゼロデイ攻撃作戦「CloudyOmega」は 2011 年から - 国内組織の情報窃取狙い（Security NEXT） http://www.security-next.com/053651 ● Xbox Live や PSN に続く攻撃、今度は Tor が標的に（IT media） http://www.itmedia.co.jp/enterprise/articles/1412/29/news023.html

15. ドメイン名ハイジャック

関連記事	● 正規サイトから他サイトに誘導「ドメイン名ハイジャック」 日経電子版など被害（IT media） http://www.itmedia.co.jp/news/articles/1411/06/news123.html

16. Wi-Fi

関連記事	● ホテルの Wi-Fi を使ったら情報が盗まれていた――「ダークホテル」の驚愕手口（IT media） http://www.itmedia.co.jp/news/articles/1412/12/news054.html

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. 2014 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/malware1410.html

2. 2014 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/malware1410_jp.html

3. 2014 年 10 月のウイルス脅威

関連記事	● 2014 年 10 月のウイルス脅威（Dr. WEB) http://news.drweb.co.jp/?i=802&c=1&lng=ja&p=1

4. 2014 年 10 月のモバイル脅威

関連記事	● 2014 年 10 月のモバイル脅威（Dr. WEB) http://news.drweb.co.jp/?i=805&c=1&lng=ja&p=1

5. 2014 年 11 月のウイルス脅威

関連記事	● 2014 年 11 月のウイルス脅威（Dr. WEB) http://news.drweb.co.jp/?i=812&c=1&lng=ja&p=0

6. 2014 年 11 月のモバイル脅威

関連記事	● 2014 年 11 月のモバイル脅威（Dr. WEB) http://news.drweb.co.jp/?i=818&c=1&lng=ja&p=0

7. 2014 年 12 月のウイルス脅威

関連記事	● 2014 年 12 月のウイルス脅威（Dr. WEB） http://news.drweb.co.jp/?i=820&c=1&lng=ja&p=0

8. 2014 年 12 月のモバイル脅威

関連記事	● 2014 年 12 月のモバイル脅威（Dr. WEB） http://news.drweb.co.jp/?i=819&c=1&lng=ja&p=0

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＜2014.10.02＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.10.02＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/092900019/?ST=security

2. チェックしておきたい脆弱性情報＜2014.10.06＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.10.06＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/092900020/?ST=security

3. チェックしておきたい脆弱性情報＜2014.10.09＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.10.09＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/100700022/?ST=security/

4. チェックしておきたい脆弱性情報＜2014.10.10＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.10.10＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/100700023/?ST=security

5. チェックしておきたい脆弱性情報＜2014.10.28＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.10.28＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/102700025/?ST=security

6. チェックしておきたい脆弱性情報＜2014.10.30＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.10.30＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/102700026/?ST=security

7. チェックしておきたい脆弱性情報＜2014.11.11＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.11.11＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/111000027/?ST=security

8. チェックしておきたい脆弱性情報＜2014.11.28＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.11.28＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/112600029/?ST=security

9. チェックしておきたい脆弱性情報＜2014.12.01＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.12.01＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/112600030/?ST=security

10. チェックしておきたい脆弱性情報＜2014.12.08＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.12.08＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/120300032/?ST=security

11. チェックしておきたい脆弱性情報＜2014.12.10＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.12.10＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/120300033/?ST=security

12. チェックしておきたい脆弱性情報＜2014.12.15＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.12.15＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/120300034/?ST=security

13. チェックしておきたい脆弱性情報＜2014.12.19＞

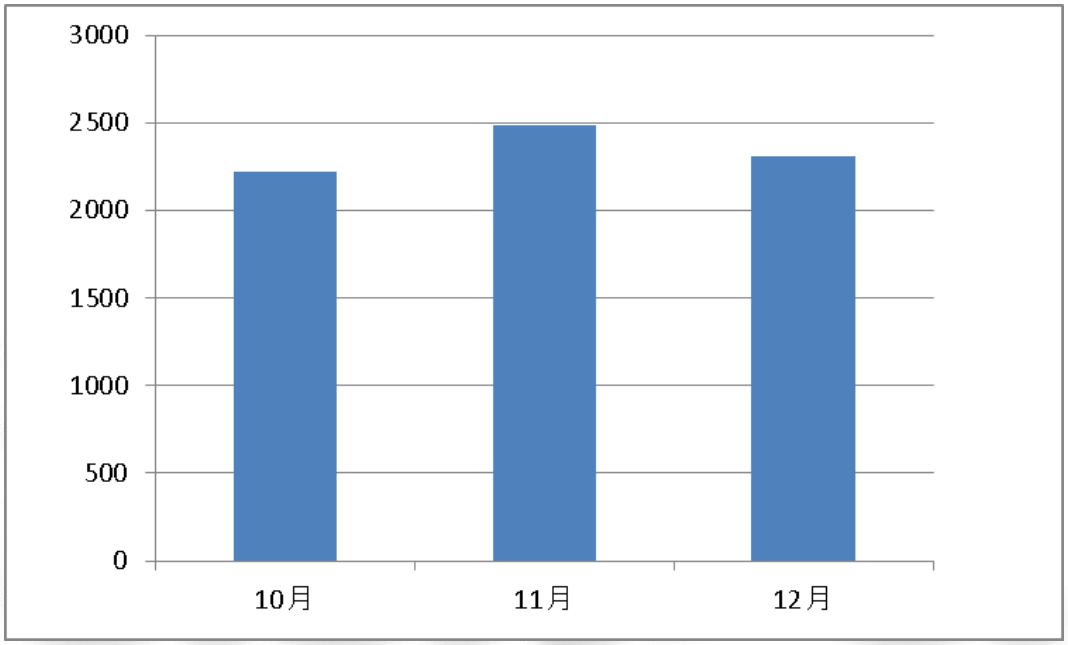
プレス リリース	● チェックしておきたい脆弱性情報＜2014.12.19＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/121800035/?ST=security

14. チェックしておきたい脆弱性情報＜2014.12.24＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.12.24＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/121800036/?ST=security

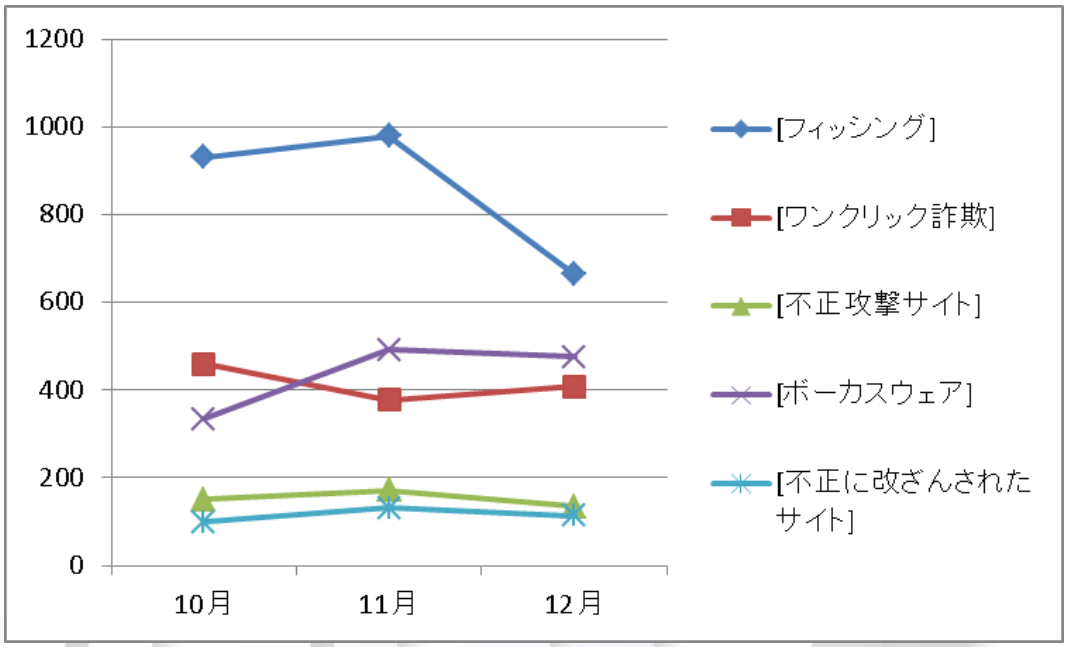
5. データからみるサイバー犯罪の傾向

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（2014 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、悪質な URL の件数は 2200 件から 2500 件の間で推移しています。月別で、悪質な URL 件数の大幅な増加や減少は見受けられませんでした。また、サイバー犯罪の傾向としては、9 月には減少傾向であったフィッシングの件数は 10 月に入り再び増加しました（前月 30%増）。こちらは、2014/12/16 付の Security Next の記事「減少傾向だったフィッシング、10 月に再び増加」においても言及されています。11 月も同様な水準でしたが、12 月に入り件数は減少しました(前月 32%減)。更に、10 月から 11 月にかけてボーカスウェアの件数は増加しましたが(前月 47%増)、一方でワンクリック詐欺の件数は減少しました(前月 18%減)。

6. 総括

今期はソニー傘下のソニーピクチャーズがサイバー攻撃を受け、世間を騒がせました。調査によって北朝鮮が今回のサイバー攻撃に関与しているとの報道が流れましたが、真相は明らかとなっていません。今回の攻撃では、サイバー攻撃によりコンピュータが乗っ取られ、内部データを搾取されたとのことです。北朝鮮では、約 3000 人のハッカーから成るチームが結成されていると伝えられています。今回発生した大規模なサイバー攻撃を教訓として、今後の企業がどのような対策を取るのか注目されています。

次に、Android スマートフォンを狙った攻撃が数多く報告されました。正規のアプリを装いユーザにインストールさせることで、個人情報や金銭を盗むマルウェアが出回りました。また、これまでマルウェア感染の危険性が低いと考えられていた iOS においても、マルウェア感染の報告が確認されました。スマートフォンのセキュリティに対するユーザの意識は低く、アンチウィルスソフトの導入率も低い傾向にあります。今後、更にスマートフォンに対するサイバー攻撃の増加が予想されますので注意が必要です。

また、DDoS 攻撃に関する報告もありました。DDoS 攻撃を代行する業者がアンダーグラウンドで横行しており、1 時間 8 ドルと安価で使用可能であるため、自ら資源を持たない人物でも攻撃が可能となっています。高校一年生がゲーム会社の運営に不満を抱き、このようなサービスを利用することで、ゲーム会社のサーバに攻撃を仕掛け、機能を低下させた事件もありました。これらの攻撃の踏み台になったと考えられる機器の種類の約８７％はルータであり、内部プログラムのアップデートや設定によって防止できるケースがあるため、メーカーのサイト等で確認を取られることを推奨します。

マイクロソフトの月例パッチにおいて 2 回(10 月、12 月)不具合が発生し、パッチの再配布などもありました。サーバ管理者などは、最新のパッチに不具合が無いかを十分確認する必要があります。

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