S.S.R.C.定期
トレンドレポート
Vol.27

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.27

目次

© Hitachi Systems, Ltd. 2016. All rights reserved.

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。

© Hitachi Systems, Ltd. 2016. All rights reserved.

3. トレンドレポート 2016 年第 1 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:2016/1/1～2016/3/31

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。

© Hitachi Systems, Ltd. 2016. All rights reserved.

1. Microsoft

関連記事	● Microsoft、9 件の月例セキュリティ情報を公開　古い IE は最後のアップデート（IT media） http://www.itmedia.co.jp/news/articles/1601/13/news053.html ● Microsoft、2016 年 2 月のセキュリティ情報を公開 計 13 件（IT media） http://www.itmedia.co.jp/news/articles/1602/10/news059.html ● Microsoft、13 件の月例セキュリティ情報を公開　IE と Edge に「緊急」あり（CNET Japan） http://www.itmedia.co.jp/enterprise/articles/1603/09/news059.html ● MS、「Windows 10」を「推奨される」更新プログラムとして提供開始　（ZDNet Japan） http://japan.zdnet.com/article/35077208/ ● Windows 10 初の大型アップデート「Anniversary Update」、今夏提供へ（CNET Japan） http://japan.cnet.com/news/service/35080403/ ● Windows 8、来週で更新サポート終了……「Windows 8.1」へのアップデートを（RBB TODAY） http://www.rbbtoday.com/article/2016/01/08/138520.html ● 1 割弱が旧版 IE を利用 - まもなくサポート終了で危険な状態に（IT media） http://www.security-next.com/065739 ● 「EMET を使って EMET を無効化」、Microsoft が脆弱性に対処　（IT media） http://www.itmedia.co.jp/enterprise/articles/1602/24/news066.html ● Microsoft Windows の WebDAV においてメモリ検証不備により権限昇格または DoS 攻撃されてしまう脆弱性　（Scan NetSecurity） http://scan.netsecurity.ne.jp/article/2016/03/28/38298.html ● Windows PowerShell 規制を回避するトロイの木馬発見　（マイナビニュース） http://news.mynavi.jp/news/2016/01/25/201/

© Hitachi Systems, Ltd. 2016. All rights reserved.

2. Apple

関連記事	● アップル、「iOS 9.2.1」と「OS X 10.11.3」を公開 （CNET Japan） http://japan.cnet.com/news/service/35076466/ ● 複数の Apple 製品の脆弱性に対するアップデート（Scan Tech Report）（Scan NetSecurity） http://jvn.jp/vu/JVNVU97668313/ ● 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 ● 新型の iOS マルウェア出現、設計問題を突き通常端末にも感染（IT media） http://www.itmedia.co.jp/news/articles/1603/17/news065.html ● Apple「Gatekeeper」に迂回の恐れ、パッチでも解決できず？（IT media） http://www.itmedia.co.jp/news/articles/1601/19/news054.html ● ゼロデイ脆弱性の‘発見者’たちを雇って Mac のセキュリティを確保した Apple (TechCrunch) http://jp.techcrunch.com/2016/02/04/20160203apple-beefs-up-its-security-team-by-hiring-zero-day-exploit-team/ ● Apple、FBI 捜査のための iPhone バックドア命令を拒否――自由を脅かすもの (IT media) http://www.itmedia.co.jp/news/articles/1602/17/news152.html

© Hitachi Systems, Ltd. 2016. All rights reserved.

3. Adobe

関連記事	● Adobe Reader および Acrobat の脆弱性対策について (APSB16-02)(CVE-2016-0932 等) (IPA) http://www.ipa.go.jp/security/ciadr/vul/20160113-adobereader.html ● 「Adobe Flash Player」に 22 件の脆弱性　更新は 72 時間以内に (Security NEXT) http://www.security-next.com/066768 ● 「Adobe Acrobat/Reader」向けアップデート、3 月 8 日を予定 - ゼロデイ攻撃は未確認 (Security NEXT) http://www.security-next.com/067529 ● 「Flash Player」のセキュリティ更新が公開　ゼロデイ脆弱性を修正 (Security NEXT) http://www.security-next.com/067755 ● 2015 年下半期は DBD 攻撃が約 1.4 倍に 9 割超が Flash 脆弱性を悪用 (Security NEXT) http://www.security-next.com/067356

© Hitachi Systems, Ltd. 2016. All rights reserved.

4. Android

関連記事	● Google、Android の月例セキュリティ情報を公開　Nexus 向けのパッチ配信（IT media） http://www.itmedia.co.jp/enterprise/articles/1602/02/news054.html ● Google、Android の月例セキュリティ情報公開　新たなメディア処理の脆弱性も（IT media） http://www.itmedia.co.jp/news/articles/1603/08/news053.html ● Google、Android 向けパッチを開発、Linux の未解決の脆弱性に対応（IT media） http://www.itmedia.co.jp/enterprise/articles/1601/22/news065.html ● Android 端末の 66%に影響？Linux カーネルの脆弱性で割れる意見（TechTarget Japan） http://techtarget.itmedia.co.jp/tt/news/1602/04/news06.html ● Android 搭載のスマートテレビ、不正アプリによりバックドア型不正プログラムに感染（TREND MICRO） http://blog.trendmicro.co.jp/archives/12762 ● Android 利用者のネットバンク情報狙う「Asacub」（Security NEXT） http://www.security-next.com/066992 ● Android に新手のマルウェア、端末を遠隔操作される恐れ（IT media） http://www.itmedia.co.jp/news/articles/1602/16/news059.html ● 「Android」を狙うマルウェアの「GM Bot」--ソースコードがオンラインに流出（CNET Japan） http://japan.cnet.com/news/service/35078304/ ● ファームウェアおよび有名企業の提供するアプリを狙う新たな Android 向けアドウェア（Security NEXT） http://news.drweb.co.jp/show/?i=995

© Hitachi Systems, Ltd. 2016. All rights reserved.

5. 情報漏洩

関連記事	● 米 Time Warner Cable の加入者情報が流出、32 万人に影響も（IT media） http://www.itmedia.co.jp/news/articles/1601/08/news068.html ● 江崎グリコの EC サイトに不正アクセス　個人情報 8 万 3000 件流出か（IT media） http://www.itmedia.co.jp/news/articles/1603/07/news094.html ● Tweepie からアカウント情報 5.5 万件が流出　不正ログイン攻撃に悪用される（Security NEXT） http://www.security-next.com/067727 ● FBI と DHS、職員の個人情報が大量流出か（CNET Japan） http://japan.cnet.com/news/business/35077573/ ● 三菱東京 UFJ 銀の利用者情報流出、調査結果を発表（Security NEXT） http://www.security-next.com/065701 ● 通販サイト DB に不正アクセス、カード情報が流出　セキュリティコードも（Security NEXT） http://www.security-next.com/066582 ● ゴルフ情報メディア「ALBA.Net」に不正アクセス 個人情報が流出（Security NEXT） http://www.security-next.com/067293 ● 2015 年 8 月に不正アクセス、クレカ情報が流出か　ネットマーケ支援業者（Security NEXT） http://www.security-next.com/067549 ● DDoS 攻撃対策会社がハッキングされ顧客情報が流出（THE ZEROONE） https://the01.jp/p0002082/ ● アークン、なりすましが不正アクセスの原因 全取締役を処分 （Security NEXT） http://www.security-next.com/066967 ● 北大のサーバが外部と不正通信 - 情報流出の可能性（Security NEXT） http://www.security-next.com/065840

© Hitachi Systems, Ltd. 2016. All rights reserved.

6. 脆弱性

関連記事	● 「Windows」と「Samba」に深刻な脆弱性「Badlock」（Security NEXT） http://www.security-next.com/068242 ● 「Angler EK」が 1 月に修正された「Silverlight」の脆弱性を悪用（Security NEXT） http://www.security-next.com/067132 ● 脆弱性「DROWN」、非推奨の SSLv2 に存在することが確認される。HTTPS サーバ全体の 3 分の 1 に影響（TREND MICRO） http://blog.trendmicro.co.jp/archives/12950 ● OpenSSH に脆弱性、秘密鍵流出の恐れ（IT media） http://www.itmedia.co.jp/enterprise/articles/1601/15/news059.html ● 「IKE プロトコル」が DDoS 攻撃に悪用されるおそれ 9 倍に増幅されるケースも（Security NEXT） http://www.security-next.com/067340 ● 「Joomla！」脆弱性を突かれスパム送信の踏み台に - 藤沢市関連サイト（Security NEXT） http://www.security-next.com/066075 ● 国内のウェブサイトに SQL インジェクションの脆弱性 （JVN） http://jvn.jp/ta/JVNTA99929369/ ● メールを開いていないのに感染：Outlook の脆弱性（Kaspersky） https://blog.kaspersky.co.jp/bad-badwinmail/9879/ ● PHP に複数の脆弱性 - アップデートが公開（Security NEXT） http://www.security-next.com/066018 ● Java のダウンロードプロセスに脆弱性、Windows ユーザーは入れ替えを（IT media） http://www.itmedia.co.jp/enterprise/articles/1602/09/news058.html ● 2015 年 4Q の脆弱性登録は 1619 件 - 「IE」190 件で最多（Security NEXT） http://www.security-next.com/066362

© Hitachi Systems, Ltd. 2016. All rights reserved.

7. サイバー攻撃

関連記事	● 山口県の外国人向け観光情報サイトに不正アクセス　(Security NEXT) http://www.security-next.com/068246 ● 復旧したばかりの厚労省ＨＰにまたサイバー攻撃　２日連続、３回目（産経ニュース） http://www.sankei.com/affairs/news/160126/afr1601260049-n1.html ● 北朝鮮サイトが一時閲覧不能　サイバー攻撃か（YAHOO JAPAN） http://headlines.yahoo.co.jp/hl?a=20160216-00000071-yonh-kr ● 京都動物愛護センターのサイトが改ざん　閲覧でマルウェア感染のおそれ(Security NEXT) http://www.security-next.com/067349 ● イスラエル電力公社、大規模なサイバー攻撃で「マヒ状態」に（IT media） http://www.itmedia.co.jp/enterprise/articles/1601/28/news060.html ● サイバー攻撃倍増　昨年５４５億件　防犯カメラからも発信（産経ニュース） http://www.sankei.com/affairs/news/160221/afr1602210005-n1.html

© Hitachi Systems, Ltd. 2016. All rights reserved.

8. ランサムウェア

関連記事	● 「Locky ランサムウェア」が国内外で猛威 マクロを有効化させる巧妙手口も (Security NEXT) http://www.security-next.com/067037 ● 日本語表示に対応したモバイル版ランサムウェアを初確認、既に国内でも被害 (TREND MICRO) http://blog.trendmicro.co.jp/archives/13041 ● 進化する「Teslacrypt」、既知の脆弱性でセキュリティ製品の検知を回避 (Security NEXT) http://www.security-next.com/067890 ● 偽のウインドウで管理者権限を奪う Android ランサムウェア - シマンテック (マイナビ ニュース) http://news.mynavi.jp/news/2016/02/01/262/ ● トロイの木馬送り込み、勝手にユーザーのマシンに入り込むマルウェア (ASCII) http://ascii.jp/elem/000/001/137/1137734/ ● 新暗号型ランサムウェア「PETYA」、MBR を上書きして PC へのアクセス不能に (TREND MICRO) http://blog.trendmicro.co.jp/archives/13106 ● WordPress や Joomla サイトの改ざん相次ぐ、ランサムウェアへ誘導 (IT media) http://www.itmedia.co.jp/enterprise/articles/1602/23/news061.html ● Neutrino Exploit Kit 経由で侵入するランサムウェア、TeslaCrypt (McAfee Blog) http://blogs.mcafee.jp/mcafeeblog/2016/03/neutrino-exploi-e39a.html ● Mac を狙うランサムウェア、正体が判明 (IT media) http://www.itmedia.co.jp/news/articles/1603/10/news068.html ● ランサムウェア感染メール、1 週間で 20 万件 国内検知の半数超 (Security NEXT) http://www.security-next.com/067834

© Hitachi Systems, Ltd. 2016. All rights reserved.

	● 「ランサムウェア」脅威がモバイルへも拡大中（TREND MICRO） http://blog.trendmicro.co.jp/archives/13055 ● オンライン上に公開されたランサムウェアのコードを悪用。情報共有は適切な範囲と方法の選択が重要（TREND MICRO） http://blog.trendmicro.co.jp/archives/12785 ● Bitdefender、ランサムウェアに対抗する無償ツールを公開（Security NEXT） http://www.security-next.com/068436

© Hitachi Systems, Ltd. 2016. All rights reserved.

9. フィッシング

関連記事	● 楽天銀行をかたるフィッシング（2016/01/04）（フィッシング対策協議会） http://www.antiphishing.jp/news/alert/_rakutenbank20160104.html ● ハンゲームをかたるフィッシング（2016/01/04）（フィッシング対策協議会） http://www.antiphishing.jp/news/alert/_hangame20160104.html ● 三井住友銀行をかたるフィッシング（2016/01/22）（フィッシング対策協議会） https://www.antiphishing.jp/news/alert/smbc_20160122.html ● セゾン Net アンサーをかたるフィッシング（フィッシング対策協議会） http://www.antiphishing.jp/news/alert/saison_20160318.html ● 米国で所得税申告の時期を狙ったフィッシングメールが急増（フィッシング対策協議会） http://www.antiphishing.jp/news/entry/_20160224_mynabi.html ● フィッシング攻撃はますます激化--その実態は（ZDNet Japan） http://japan.zdnet.com/article/35077223/ ● 米国と英国の組織の 84% がスピアフィッシング攻撃を受けているとの調査結果（フィッシング対策協議会） http://www.antiphishing.jp/news/entry/_20160122_itbusinessedge.html ● 2 月はフィッシング報告が倍増 - 98%が金融機関ターゲット（Security NEXT） http://www.security-next.com/067428

© Hitachi Systems, Ltd. 2016. All rights reserved.

10. マルウェア

関連記事	● 複数のデジタル証明書を使って検出をすり抜けるマルウェアが出現（Symantec） http://www.symantec.com/connect/ja/blogs/malware-being-signed-multiple-digital-certificates-evade-detection-0 ● 不正送金マルウェア「URLZone」が日本に本格上陸か（Security NEXT） http://www.security-next.com/066529 ● POS マルウェア「FighterPOS」、ワーム機能を追加（TREND MICRO） http://blog.trendmicro.co.jp/archives/12935 ● 偽日本郵政メールで不正送金マルウェアに感染　「Racuten」にも注意（Security NEXT） http://www.security-next.com/067068 ● 複合機偽装メールで国内被害も発生した「Dridex」、勢い収まらず（Security NEXT） http://www.security-next.com/067044 ● 自己防衛機能装えた新手の情報窃取マルウェア「USB Thief」（Security NEXT） http://www.security-next.com/068175 ● 跡を残さず破壊する「ファイルレス」マルウェアの恐怖（TechTarget） http://techtarget.itmedia.co.jp/tt/news/1603/15/news03.html ● 国内初の“POS マルウェア”被害確認か、ホテルチェーンのハイアット、東京・箱根など国内 4 ホテルで感染の疑い、クレジットカード情報が漏えい（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/20160115_739230.html ● 3500 超の正規サイトに不正コード - 閲覧によるマルウェア感染なく情報収集目的か）（Security NEXT） http://www.security-next.com/066211 ● バングラデシュ中銀の盗難被害、ハッカーはマルウエアで侵入か　（REUTERS） http://jp.reuters.com/article/usa-fed-bangladesh-malware-idJPKCN0WD2C9

© Hitachi Systems, Ltd. 2016. All rights reserved.

	● 米国の確定申告システムにマルウェア攻撃、阻止に成功（IT media） http://www.itmedia.co.jp/enterprise/articles/1602/12/news097.html ● 欧州メインのスパム攻撃、日本向けに手口変更で拡大の恐れ（IT media） http://www.itmedia.co.jp/enterprise/articles/1602/01/news106.html ● C&C サーバの情報を ISP に提供することでマルウェア感染を低減する取組（総務省）（Scan NetSecurity） http://scan.netsecurity.ne.jp/article/2016/02/29/38169.html ● 年金機構サイバー攻撃の類似ウイルス、１１団体感染か（朝日新聞 DIGITAL） http://www.asahi.com/articles/ASJ124RGVJ12UTIL00G.html ● バイドゥが配布した開発キットに危険なバックドアが見つかる（IT pro） http://itpro.nikkeibp.co.jp/atcl/column/14/277462/122500042/

© Hitachi Systems, Ltd. 2016. All rights reserved.

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 1 月のウイルスレビュー

関連記事	● 2016 年 1 月のウイルスレビュー（Dr. WEB） http://news.drweb.co.jp/?i=979

2. 2016 年 2 月のウイルスレビュー

関連記事	● 2016 年 2 月のウイルスレビュー（Dr. WEB） http://news.drweb.co.jp/?i=991

3. 2016 年 3 月のウイルスレビュー

関連記事	● 2016 年 3 月のウイルスレビュー（Dr. WEB） http://news.drweb.co.jp/?i=1001

4. 2016 年 1 月のモバイルマルウェア

関連記事	● 2016 年 1 月のモバイルマルウェア（Dr. WEB） http://news.drweb.co.jp/?i=980

5. 2016 年 2 月のモバイルマルウェア

関連記事	● 2016 年 2 月のモバイルマルウェア（Dr. WEB） http://news.drweb.co.jp/?i=990

6. 2016 年 3 月の Android マルウェア

関連記事	● 2016 年 3 月のモバイルマルウェア（Dr. WEB） http://news.drweb.co.jp/?i=1000

© Hitachi Systems, Ltd. 2016. All rights reserved.

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＜2016.01.13＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.01.13＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/011100094/

2. チェックしておきたい脆弱性情報＜2016.01.15＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.01.15＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/011100095/

3. チェックしておきたい脆弱性情報＜2016.01.19＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.01.19＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/011100096/

4. チェックしておきたい脆弱性情報＜2016.02.04＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.02.04＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/020200097/

5. チェックしておきたい脆弱性情報＜2016.02.08＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.02.08＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/020200098/

6. チェックしておきたい脆弱性情報＜2016.02.15＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.02.15＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/021000099/

© Hitachi Systems, Ltd. 2016. All rights reserved.

7. チェックしておきたい脆弱性情報＜2016.02.18＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.02.18＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/021000100/

8. チェックしておきたい脆弱性情報＜2016.03.07＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.03.07＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/030300101/

9. チェックしておきたい脆弱性情報＜2016.03.14＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.03.14＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/030300102/

10. チェックしておきたい脆弱性情報＜2016.03.23＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.03.23＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/032200103/

11. チェックしておきたい脆弱性情報＜2016.03.25＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.03.25＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/032200104/

12. チェックしておきたい脆弱性情報＜2016.03.28＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.03.28＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/032200105/

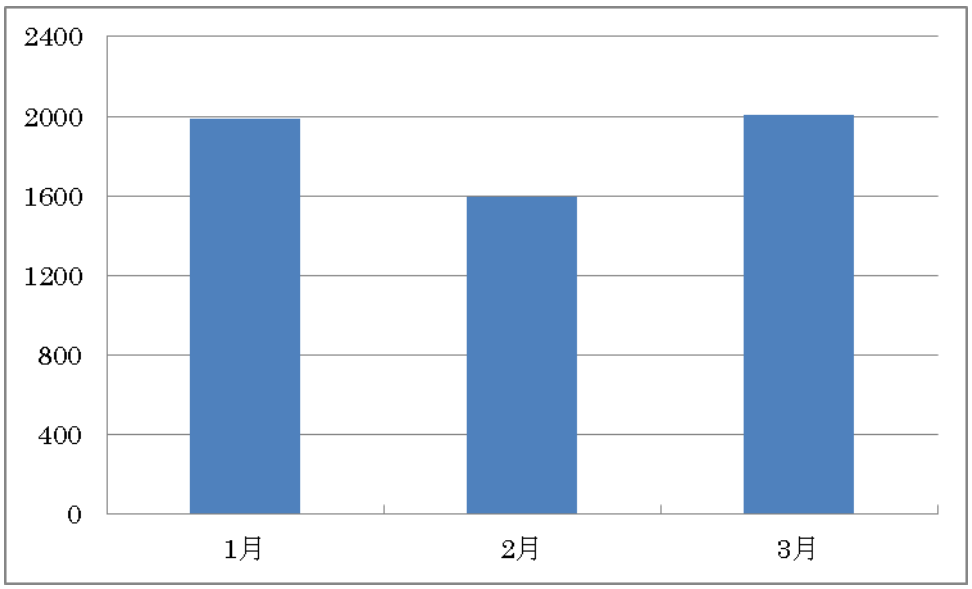
13. チェックしておきたい脆弱性情報＜2016.03.30＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.03.30＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/032200106/

© Hitachi Systems, Ltd. 2016. All rights reserved.

5. データからみるサイバー犯罪の傾向

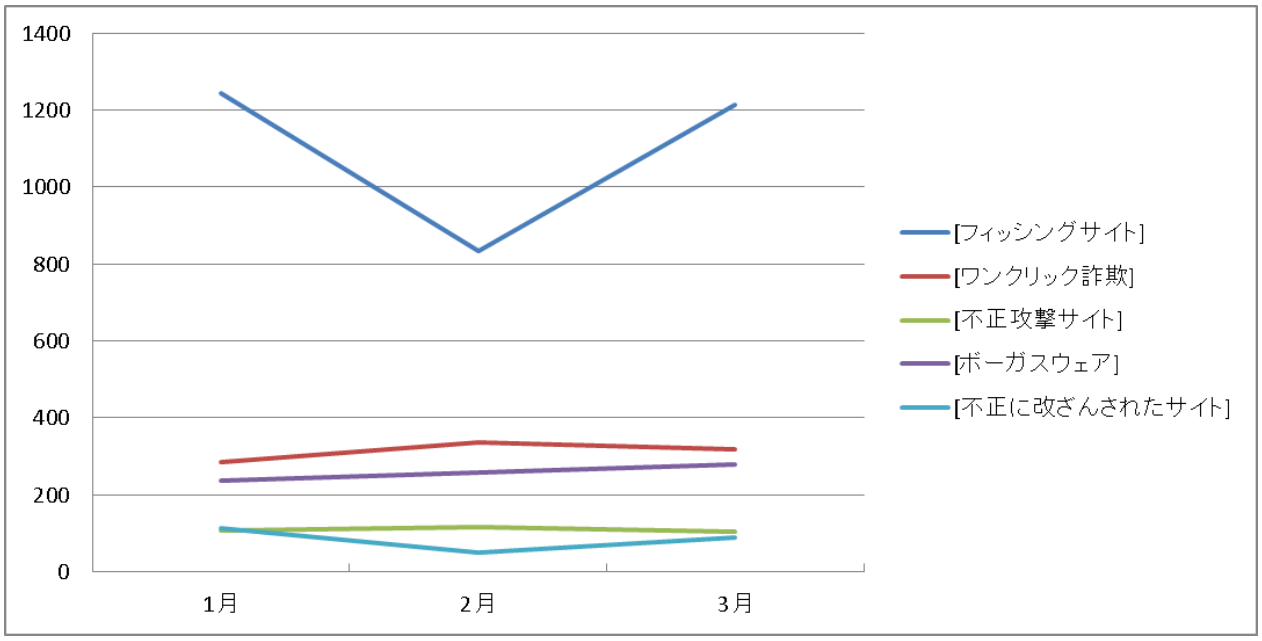
インターネットユーザがウェブサイトの安全性を確認できるウェブサイトセキュリサービス*のデータをもとにしたサイバー犯罪の傾向を以下に示します。



「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/)

© Hitachi Systems, Ltd. 2016. All rights reserved.



脅威別検知数の月別推移(2016 年 1 月～3 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、前期と比較すると 1 月と 3 月は 400 件近く増えております。これは、脅威別検知数の月別推移におけるフィッシングサイトの項目で 1 月と 3 月が、前期および 1 月と比較して検知数が大きく増加していることが原因です。しかしながら、広告の多い動画サイト、正規の URL と酷似した偽サイトが多く検知されているという傾向に変化はありませんでした。

また、フィッシングサイト以外の検知については前期から変わらずほぼ横ばいに推移しています。3 月には Adobe Flash Player のゼロデイ脆弱性情報がありましたが不正攻撃サイトとして Adobe Flash Player を攻撃するサイトも検知しております。

© Hitachi Systems, Ltd. 2016. All rights reserved.

6. 総括

今期は、影響範囲が広い脆弱性として「Badlock」(*1)と「DROWN」(*2)が発見されました。「Badlock」は Windows と Samba に影響する脆弱性で、悪用されるとトラフィックの盗聴やプロトコルのダウングレード攻撃、セッションの乗っ取り攻撃が可能です。この脆弱性は幸いなことに、攻撃者が簡単には悪用できないためそれほど深刻なものではありませんでした。また、「DROWN」は SSL/TLS プロトコルを使った通信の暗号化にある脆弱性で、悪用されると暗号化を解除されて通信内容を傍受される危険性があります。この脆弱性は全 HTTPS の 33%ものサイトが影響を受け、SSLv2 をサポートしているだけで攻撃が可能になります。サーバの運用者はこれらの脆弱性を有していないか確認し、有しているのであれば該当するソフトウェア等の早急なアップデートを推奨いたします。

先期に引き続き、今期もランサムウェアによる被害が多く報告されております。ランサムウェアは感染すると PC 内のファイルを勝手に暗号化し、金銭を支払うように脅してきます。また、一度暗号化されてしまうと自力で元の状態に戻す事は非常に困難です。今期の特徴的なランサムウェアとしては、マスターブートレコード(MBR)を上書きして OS を起動できなくする”PETYA”や、日本語表示するモバイル型ランサムウェアなどがありました。ランサムウェアは 2014 年に流行した CryptoLocker から、ネットワーク上の共有ファイルを暗号化させる機能や、今回の MBR を上書きする機能など年々機能の幅を広げています。さらに、ターゲットも Windows だけなく Mac や Android が狙われるなど拡大しているため、ユーザーはランサムウェアに対して正しい知識を身に着け対策を行う必要があります。対策については、IPA(*3)や JPCERT/CC(*4)などを参照してランサムウェアに対して正しい対策を行う事を推奨いたします。

近年マルウェアによる被害やサイバー攻撃などが増えておりますが、サーバ運用者やユーザーはこういったセキュリティの情報に対して敏感になり、常に最新のセキュリティ情報を収集することが自身のサーバや PC を守ることに繋がります。

© Hitachi Systems, Ltd. 2016. All rights reserved.

(*1) The DROWN Attack

https://drownattack.com/top-sites.html

(*2) Badlock Bug

http://badlock.org/

(*3) 「ランサムウェア感染被害に備えて定期的なバックアップを」

～組織における感染は組織全体に被害を及ぼす可能性も～

https://www.ipa.go.jp/security/txt/2016/01outline.html

(*4) ランサムウエア感染に関する注意喚起

https://www.jpcert.or.jp/at/2015/at150015.html

© Hitachi Systems, Ltd. 2016. All rights reserved.

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

© Hitachi Systems, Ltd. 2016. All rights reserved.