株式会社 日立システムズ

SSRC-TR-Vol.19

S.S.R.C.定期
トレンドレポート
Vol.19

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.19

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 2014 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:2014/1/1～2014/3/31

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。

1. GOM Player のアップデートに偽装したマルウェア感染被害

関連記事	● 正規のソフトウェアのアップデートで、不正なプログラムが実行される事案について（株式会社ラック） http://www.lac.co.jp/security/alert/2014/01/23_alert_01.html ● GOM Player の更新機能を悪用したマルウェア（Kaspersky） http://blog.kaspersky.co.jp/malware-abuses-gom-player/ ● Adobe から流出したパスワードでの Facebook への不正アクセスが判明（Gigazine） http://gigazine.net/news/20131112-after-adobe-breach/ ● 医師ＰＣがウイルス感染＝患者情報漏えいか - 国立がんセンター（時事ドットコム） http://www.jiji.com/jc/zc?k=201402/2014020600217 ● 「Backdoor.Win32.Miancha.*」の技術情報（Kaspersky） http://blog.kaspersky.co.jp/malware-abuses-gom-player-2/ ● 「もんじゅ」PC のウイルス感染経路、「GOM Player」のアップデートと断定（Security NEXT） http://www.security-next.com/046925 ● マルウェア（ウイルス）感染に関するお詫びと調査結果のご報告（株式会社グレテックジャパン） http://www.gomplayer.jp/player/notice/view.html?intSeq=300

2. 相次ぐ Web サイト改ざん被害

関連記事	● OpenSSL の Web サイトに改ざん被害、ソースコードは無事（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1401/07/news031.html ● Web サイトの改ざんが 1 年で 6000 件超　事後対応の体制作りが急務（ITPro） http://itpro.nikkeibp.co.jp/article/COLUMN/20140110/529283/ ● 3 カ月弱にわたりサイト改ざん、閲覧でウイルス感染のおそれ - 三輪そうめん山本（Security NEXT） http://www.security-next.com/046570 ● サイト改ざんの影響について（株式会社ヤマレコ） http://www.yamareco.com/modules/diary/67-detail-67764 ● はとバスＨＰが改ざん　閲覧者７万５千人ウイルス感染の可能性も（msn 産経ニュース） http://sankei.jp.msn.com/affairs/news/140226/dst14022614110003-n1.htm ● 西日本新聞のＨＰ改ざん＝無関係サイトに誘導（時事ドットコム） http://www.jiji.com/jc/zc?k=201403/2014032000349 ● IE のゼロデイ攻撃が日本国内にも波及 - 今すぐ回避策を（So-net セキュリティ通信） http://security-t.blog.so-net.ne.jp/2014-02-26

3. KADOKAWA の Web サイト改ざん、フィッシングメールの踏み台として悪用

関連記事	● 日本の大手出版社の Web サイトが Gongda 悪用ツールキットに利用される（Symantec） http://www.symantec.com/connect/ja/blogs/web-gongda ● 怪しくないサイトも危ない！　KADOKAWA のサイトで一時マルウェア感染の恐れ（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/20140117_631154.html ● 角川の Web サイト改ざん事件で明らかになった“ハッカーの狙いは日本人

	(ITPro) http://itpro.nikkeibp.co.jp/article/COLUMN/20140123/531704/?ST=security ● 「KADOKAWA」サーバに不正侵入、フィッシングメールの踏み台にされた恐れ サイト閉鎖（ITmedia） http://www.itmedia.co.jp/news/articles/1403/23/news011.html ● ［続報］KADOKAWA への不正アクセス、大手銀行を装うフィッシングが目的 (ITPro) http://itpro.nikkeibp.co.jp/article/NEWS/20140324/545503/?ST=security

4. 企業サイトへの不正ログイン事件

関連記事	● パスワードリスト攻撃再び、「Potora」で不正ログイン被害 323 件（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/20140121_631596.html ● 「GOM Player」などの会員サービスに不正ログイン攻撃 - 未登録の場合は勝手に会員登録（Security NEXT） http://www.security-next.com/045840 ● @nifty、会員情報 165 件分が不正閲覧、使い回しパスワードが原因か（Internet WATCH） http://internet.watch.impress.co.jp/docs/news/20140124_632249.html ● ファッション通販サイトに不正ログイン攻撃 - 最大 2 万 4000 件のクレカ情報を不正取得か（Security NEXT） http://www.security-next.com/46047 ● JAL マイレージ Web サイトに不正アクセス、約 2700 万人にパスワード変更を依頼 http://itpro.nikkeibp.co.jp/article/NEWS/20140203/534282/ https://www.jal.co.jp/info/jmb/140203.html http://www.itmedia.co.jp/enterprise/articles/1402/04/news135.html

- はてな、不正ログインの可能性を公表……登録情報確認を呼びかけ

http://www.rbbtoday.com/article/2014/02/24/117151.html

http://hatena.g.hatena.ne.jp/hatena/20140224/1393211701

- mixi に不正ログイン 370 件　身に覚えのない mixi ゲームに登録される (ITmedia)

http://www.itmedia.co.jp/news/articles/1402/25/news132.html

- mixi に不正ログイン 1 万 7000 件　身に覚えのない「つぶやき」投稿（ITmedia）

http://www.itmedia.co.jp/news/articles/1402/28/news154.html

- 「My SoftBank」で不正アクセス、344 件の顧客情報が漏洩（ITPro）

http://itpro.nikkeibp.co.jp/article/NEWS/20140228/540325/

- 不正ログイン（リスト型攻撃）相次ぐ - なりすまし投稿や不正購入の被害も (So-net セキュリティ通信)

http://security-t.blog.so-net.ne.jp/2014-03-07

- ドラクエ X の便利ツールアプリで不正ログイン - ワンタイムパス設定呼びかけ (マイナビニュース)

http://news.mynavi.jp/news/2014/03/08/040/

- @wiki でメアドなどの個人情報が流出 - 全登録ユーザーが対象に

http://news.mynavi.jp/news/2014/03/09/093/

http://internet.watch.impress.co.jp/docs/news/20140309_638779.html

- ＡＮＡマイル、不正交換被害　６５万円分奪われる

http://www.asahi.com/articles/ASG3C0FBQG3BUTIL06C.html

http://www.security-next.com/047109

- Suica ポイントサービスのウェブサイトに大量アクセス（レスポンス）

http://response.jp/article/2014/03/18/219406.html

- JCB に不正ログイン、T ポイントへの交換を悪用（YOMIURI ONLINE）

http://www.yomiuri.co.jp/it/security/goshinjyutsu/20140327-OYT8T00506.html

5. 企業からの顧客情報漏えい

関連記事	● 「EC カレント」など通販サイトで個人情報最大 9 万 4359 件漏洩、カード不正利用被害も http://www.nikkei.com/markets/ir/irftp/data/tdnr2/tdnetg3/20140130/8i9ajw/1401201401300096076.pdf http://itpro.nikkeibp.co.jp/article/NEWS/20140131/533850/?ST=security ● 光文社、不正アクセス被害でクレジットカード情報 1,160 件が流出の可能性（RBB Today） http://www.rbbtoday.com/article/2014/03/04/117479.html ● 会員専用サイトに不正アクセス、個人情報 5000 件が流出 - ベリタス（Security NEXT） http://www.security-next.com/047278 ● Forbes のパスワード、流出（Kaspersky） http://blog.kaspersky.co.jp/forbes-passwords-leak/ ● １億人超の個人情報流出　韓国大手カード３社（msn 産経ニュース） http://sankei.jp.msn.com/world/news/140112/kor14011216490004-n1.htm ● Snapchat、ユーザー情報流出問題で謝罪 - アップデートを公開（CNET Japan） http://japan.cnet.com/news/service/35042343/ ● ドイツで約 1600 万人分のアカウント情報流出 - 海外メディアの報道（ITPro） http://itpro.nikkeibp.co.jp/article/NEWS/20140122/531482/?top_nhl

6. モバイルアプリを利用して出会い系サイトに誘導する手口

関連記事	● “出会えない系サイト”の罠　「電池長持ち」アプリで連絡先抜き取り、出会い系に登録させる手口（ITmedia） http://www.itmedia.co.jp/news/articles/1402/05/news047.html ● メッセンジャーアプリ「LINE」の人気に便乗するスパムメール、出会い系 Web サイトへ誘導（Trend Micro）

	http://blog.trendmicro.co.jp/archives/8649 ● 「LINE」を騙り出会い系サイトに誘導するスパムメールに注意喚起（情報セキュリティブログ） http://securityblog.jp/news/20140304.html

7. NTP を悪用した DDoS 攻撃の発生

関連記事	● ntpd の monlist 機能を使った DDoS 攻撃に関する注意喚起（JPCERT/CC） https://www.jpcert.or.jp/at/2014/at140001.html ● NTP を利用する DDoS リフレクション攻撃に対する対策（Trend Micro） http://blog.trendmicro.co.jp/archives/8437 ● 悪用される時刻同期（NTP）サーバー、新手の DDoS 攻撃で“加害者”になるおそれも（ITPro） http://itpro.nikkeibp.co.jp/article/COLUMN/20140122/531463/ ● NTP 増幅攻撃で“史上最大規模”を上回る DDoS 攻撃発生（@IT） http://www.atmarkit.co.jp/ait/articles/1402/12/news140.html ● 「NTP 増幅」手法の DDoS 攻撃、もっと強大化する恐れも（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1403/13/news069.html

8. ネットショップを標的としたクレーム偽装メール被害

関連記事	● ウイルス:ネットショップ宛てにメール　商品クレーム偽装（毎日新聞） http://mainichi.jp/select/news/20140309k0000e040161000c.html ● 情報を盗み出すトロイの木馬に狙われたオンラインストア http://www.symantec.com/connect/ja/blogs-342 http://itpro.nikkeibp.co.jp/article/NEWS/20140312/543123/?ST=security

9. 金融機関を装うフィッシング攻撃が断続的に発生

関連記事	● 再び三菱東京 UFJ 銀行をかたるフィッシングメール、丁寧な日本語へと進歩

	(INTERNET Watch) http://internet.watch.impress.co.jp/docs/news/20131227_629408.html ● 三菱東京ＵＦＪかたる偽メール、年明けから出回る（日本経済新聞） http://www.nikkei.com/article/DGXNASFK2102A_R20C14A1000000/ ● 日本国内で特定銀行を狙う集中的なフィッシングサイト作成を確認（Trend Micro） http://blog.trendmicro.co.jp/archives/8678 ● 日本年金機構をかたる迷惑メール出回る - 「FX 口座」勧誘に誘導（So-net セキュリティ通信） http://security-t.blog.so-net.ne.jp/2014-01-30 ● 日本年金機構、職員になりすました架空年金制度案内のメールに注意喚起 http://blog.livedoor.jp/antitheft/archives/1756906.html http://www.nenkin.go.jp/n/data/service/0000016803mPFdSVzrc5.pdf

10. 検索サイトの広告を悪用した偽のフィッシングサイト

関連記事	● ご用心！！　京都銀行のインターネットバンキング画面に偽サイト（msn 産経ニュース） http://sankei.jp.msn.com/west/west_affairs/news/140218/waf14021820260040-n1.htm ● 広告を悪用したフィッシングで正送金被害発生 - その手口と防止策（So-net セキュリティ通信） http://security-t.blog.so-net.ne.jp/2014-02-25 ● ヤフーの偽サイト広告、新たに名古屋銀行と WebMoney で表示（ITPro） http://itpro.nikkeibp.co.jp/article/NEWS/20140226/539645/?ST=security

11. 被害の増加が懸念されるリベンジポルノ

関連記事	● リベンジポルノ特命委設置＝自民（時事ドットコム） http://www.jiji.com/jc/zc?k=201402/2014021300546

	● 自ら裸を撮影４２％＝児童ポルノ過去最悪 - スマホ普及が背景・警察庁（時事ドットコム） http://www.jiji.com/jc/zc?k=201403/2014030600229 ● 金もうけに悪用、リベンジポルノ募るサイト続々（朝日新聞） http://www.asahi.com/articles/ASG3N2HV3G3MUHBI01L.html

12. Bitcoin 取引所の Mt.GOX が民事再生手続き

関連記事	● ビットコインの Mt.Gox がアクセス不能 - 大手 6 社が共同声明（ITmedia） http://www.itmedia.co.jp/news/articles/1402/25/news139.html ● ビットコイン取引停止、仮想通貨の「リーマン騒動」の様相も（The Wall Street Journal） http://jp.wsj.com/article/SB10001424052702304380304579405861735800566.html ● Bitcoin 取引所の Mt.GOX が民事再生手続き、490 億円相当の Bitcoin がほぼ消失（ITPro） http://itpro.nikkeibp.co.jp/article/NEWS/20140228/540326/?ST=security

13. 深刻化するオンラインバンキングの不正送金被害

関連記事	● 不正送金被害が過去最悪ペース、2014 年 2 月までに 6 億円の被害（ITPro） http://itpro.nikkeibp.co.jp/article/NEWS/20140314/543828/?ST=security ● 2013 年の被害額は 14 億円～全銀協がネットバンキング犯罪対策特設サイト開設（So-net セキュリティ通信） http://security-t.blog.so-net.ne.jp/2014-03-26

14. 政府がサイバー攻撃の大規模訓練、全省庁が参加

関連記事	● 政府が、２０２０年の東京五輪を見据え、急増するサイバー攻撃に備えて大規模な訓練を実施（ロイター） http://jp.reuters.com/article/technologyNews/idJPTYEA2G0A720140318

15. 国家安全保障局が発足　情報一元化、縦割り打破へ

関連記事	● 国家安全保障会議（日本版 NSC）の事務局となる国家安全保障局が、発足（日本経済新聞） http://www.nikkei.com/article/DGXNASFS07008_X00C14A1MM0000/

16. 世界規模でインフラを狙った攻撃確認

関連記事	● エネルギーセクターを狙ったサイバー攻撃（ITPro） http://itpro.nikkeibp.co.jp/article/COLUMN/20140121/531203/ ● インフラ狙いのサイバー攻撃急増、データセンターやモバイルインフラが標的に（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1401/30/news031.html

17. Windows XP サポート終了問題

関連記事	● －Windows XP のセキュリティに関する企業ユーザ意識調査－ Windows XP 利用企業の IT 管理者、約半数がサポート終了後も業務利用意向あり（Trend Micro） http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20140109021807.html?cm_re=news-_-corp-_-press ● Windows XP を使った ATM が 95％も存在し、更新が間に合わないおそれ（Gigazine） http://gigazine.net/news/20140120-atm-upgrade-windows-xp/ ● 「ウィンドウズＸＰ」サポート切れの 4 月 9 日、700 万台以上のＰＣがサイバー攻撃の標的に（ダイアモンド・オンライン） http://diamond.jp/articles/-/49854 ● 3 月時点で 46%の企業が XP 利用、半数以上が今後も利用 - 「不自由しない」6 割（Security NEXT） http://www.security-next.com/047396

18. ＩＤ盗まれメール大量送信　つくば、生物研など被害

関連記事	● 茨城県つくば市の農業・食品産業技術総合研究機構と農業生物資源研究所は、メールの送受信に必要なＩＤなどが盗まれ、研究員らのメールアカウントを使って大量の不審なメールが発信されたと発表（日本経済新聞） http://www.nikkei.com/article/DGXNASDG2103U_R20C14A1CC1000/

19. WordPress の 16 万サイトが「Pingback」機能を利用され、攻撃の踏み台に

関連記事	● WordPress の 16 万サイトが大規模攻撃の踏み台に、「Pingback」機能悪用（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1403/13/news036.html

20. Twitter のスパムツイート、スパム DM 拡散

関連記事	● Twitter 上での「スパムツイート」や「スパム DM」の拡散に注意（情報セキュリティブログ） http://securityblog.jp/news/20140213.html ● 止まらない Twitter スパム！今度は「この画像分かる？」で 1 万 5000 人が被害（ITPro） http://itpro.nikkeibp.co.jp/article/COLUMN/20140213/536387/?ST=security

21. 横浜銀行元委託先社員　カード偽造・不正利用事件

関連記事	● 横浜銀データでカード偽造　容疑の委託先社員逮捕　2400万円を不正に引き出し（日本経済新聞） http://www.nikkei.com/article/DGXNASFS0403W_U4A200C1MM8000/ ● 「対策を打つ前にやられた」、NTT データが横浜銀行データ不正取得事件について釈明（ITPro） http://itpro.nikkeibp.co.jp/article/NEWS/20140205/534910/?ST=security

22. ソチオリンピックを題材とした標的型攻撃

関連記事	● Darkmoon による標的型攻撃で餌に使われた、ソチオリンピックに対するテロの脅威（Symantec） http://www.symantec.com/connect/ja/blogs/darkmoon

23. Microsoft を狙ったハッキング行為が相次いで発生

関連記事	● Microsoft ブログや Twitter が乗っ取り被害、「シリア電子軍」が声明（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1401/14/news056.html ● Microsoft、今度は Office ブログにハッキング被害（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1401/22/news038.html ● Microsoft、サイバー攻撃でファイルを盗まれたと発表（ITmedia） http://www.itmedia.co.jp/news/articles/1401/27/news050.html

24. トルコ政府による Twitter 遮断措置

関連記事	● Twitter 禁止のトルコ、Twitter やグーグルがユーザーに対抗手段を提供--SMS 利用や無料 DNS（CNET Japan） http://japan.cnet.com/news/business/35045534/

25. 日本発信の情報セキュリティ国際会議「CODE BLUE」、第一回目の開催

関連記事	● 日本発の情報セキュリティ国際会議「CODE BLUE」開催 http://codeblue.jp/ http://internet.watch.impress.co.jp/docs/news/20140217_635552.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. 2013 年 12 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/malware1312.html

2. 2013 年 12 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/malware1312_jp.html

3. 2014 年 1 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/malware1401.html

4. 2014 年 1 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/malware1401_jp.html

5. 2014 年 2 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/malware1402.html

6. 2014 年 2 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/malware1402_jp.html

7. 2013 年 12 月のウイルス脅威

関連記事	● 2013 年 12 月のウイルス脅威（Dr.WEB） http://news.drweb.co.jp/?i=701&c=2&lng=ja&p=0

8. 2014 年 1 月のウイルス脅威

関連記事	● 2014 年 1 月のウイルス脅威（Dr.WEB） http://news.drweb.co.jp/show/?i=710&c=9

9. 2014 年 2 月のウイルス脅威

関連記事	● 2014 年 2 月のウイルス脅威（Dr.WEB） http://news.drweb.co.jp/show/?i=717&lng=ja&c=2

10. Tor（匿名通信システム）を利用するマルウェアの増加

関連記事	● Tor を利用する 64 ビット版「ZBOT」、セキュリティ製品の回避手法を向上（Trend Micro） http://blog.trendmicro.co.jp/archives/8388 ● Tor を利用するマルウエアが増加（ITPro） http://itpro.nikkeibp.co.jp/article/COLUMN/20140210/535786/?ST=security ● Tor を使用する悪性アプリ（アンラボ） http://www.ahnlab.co.jp/securityinfo/blog.asp

11. POS 端末を狙うマルウェア、引き続き世界各国に感染拡大

関連記事	● POS 端末に「チューバッカ」感染、世界 11 カ国で被害（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1402/03/news031.html ● レジや POS を狙うマルウェア（Kaspersky） http://blog.kaspersky.co.jp/ram-scrapers-and-other-point-of-sale-malware/ ● 最近気になるメモリ上の情報を狙った POS マルウェア（エフセキュア）

	http://blog.f-secure.jp/archives/50722457.html

12. Bitcoin 等の仮想通貨採掘を狙ったマルウェアの拡散

関連記事	● Bitcoin をマイニングする新たな Trojan.Mods (Dr.WEB) http://news.drweb.co.jp/show/?i=698&lng=ja&c=2 ● 「ビットコイン」発行ソフトを勝手にダウンロードさせるサイバー攻撃、日本に集中　被害 6000 件以上（ITmedia） http://www.itmedia.co.jp/news/articles/1402/17/news037.html ● 身代金として Bitcoin を要求するランサムウェア「BitCrypt」（アンラボ） http://www.ahnlab.co.jp/securityinfo/blog.asp?seq=176 ● Mac 上の電子通貨を盗む Trojan.CoinThief (Dr.WEB) http://news.drweb.co.jp/show/?i=711&lng=ja&c=4 ● ビットコインを不正取得、ウイルス「ポニー」が大量拡散（ロイター） http://jp.reuters.com/article/topNews/idJPTYEA1N09320140224 ● Mt.Gox からの情報流出に見せかけた、Bitcoin を盗むマルウェア（Kaspersky） http://blog.kaspersky.co.jp/analysis_of_malware_from_the_mtgox_leak/ ● 10 カ国語で「ビットコイン払え」、新たな“脅迫ウイルス”出現（ITPro） http://itpro.nikkeibp.co.jp/article/NEWS/20140327/546704/?bpnet

13. 画像データを装ったマルウェア

関連記事	● メタデータに埋め込まれたマルウエア（ITPro） http://itpro.nikkeibp.co.jp/article/COLUMN/20140106/528062/?ST=security ● オンライン銀行詐欺ツール「ZBOT」、画像に環境設定ファイルを隠ぺい（Trend Micro） http://blog.trendmicro.co.jp/archives/8681 ● トロイの木馬の亜種、「迷彩型ゼウス」が出現（インターネットコム） http://internetcom.jp/busnews/20140306/3.html

14. Dendroid — Android を狙う新たなトロイの木馬

関連記事	● Android 版 RAT から枝分かれした Dendroid (Symantec) http://www.symantec.com/connect/ja/blogs/android-rat-dendroid ● Android を狙った新たなトロイの木馬 (Dr.WEB) http://news.drweb.co.jp/show/?i=718&lng=ja&c=4

15. ATM を狙うマルウェア

関連記事	● ATM を狙う Trojan.Skimer.19 (Dr.WEB) http://news.drweb.co.jp/?i=714&c=1&lng=ja&p=0 ● ATM を狙うマルウェア、携帯メールで現金引き出す (ITmedia) http://www.itmedia.co.jp/news/articles/1403/26/news037.html ● ATM への SMS 送信で現金を引き出すサイバー犯罪者の巧妙な手口 (Symantec) http://www.symantec.com/connect/ja/blogs/atm-sms

16. FireEye が SMS や電話をブロックする新種の Android マルウェアを確認

関連記事	● FireEye が SMS や電話をブロックする新種の Android マルウェア 6 種を確認し、注意を呼びかけている。 (情報漏えいニュース) http://blog.livedoor.jp/antitheft/archives/1757076.html

17. Android を狙った初のブートキットに 35 万台が感染

関連記事	● このトロイの木馬は、感染したデバイスのメモリ内に潜み、OS 起動の早い段階で自身を起動させてブートキットとして動作する。 (Dr.WEB) http://news.drweb.co.jp/show/?i=705&lng=ja&c=1

18. Linux サーバ 2 万 5000 台にマルウェアが感染、攻撃加担の実態も

関連記事	● 過去 2 年で 2 万 5000 台以上のサーバが Linux を狙うマルウェアの「Ebury」に

	感染し、Web トラフィックのリダイレクトやマルウェアの大量送信に使われていたことが判明した。（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1403/20/news040.html

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＜2014.1.8＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.1.8＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140107/528187/?ST=security

2. チェックしておきたい脆弱性情報＜2014.1.9＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.1.9＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140107/528193/?ST=security

3. チェックしておきたい脆弱性情報＜2014.01.23＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.01.23＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140121/531206/?ST=security

4. チェックしておきたい脆弱性情報＜2014.01.28＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.01.28＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140127/532449/?ST=security

5. チェックしておきたい脆弱性情報＜2014.02.06＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.02.06＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140205/534562/?ST=security

6. チェックしておきたい脆弱性情報＜2014.02.10＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.02.10＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140205/534563/?ST=security

7. チェックしておきたい脆弱性情報＜2014.02.12＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.02.12＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140210/535784/?ST=security

8. チェックしておきたい脆弱性情報＜2014.02.25＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.02.25＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140224/538592/?ST=security

9. チェックしておきたい脆弱性情報＜2014.02.27＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.02.27＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140224/538595/?ST=security

10. チェックしておきたい脆弱性情報＜2014.03.03＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.03.03＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140224/538597/?ST=security

11. チェックしておきたい脆弱性情報＜2014.03.12＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.03.12＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140311/542611/?ST=security

5. 総括

今期、特に注目のトピックは、企業の会員向けWebサイトへの不正ログイン事件が多発したことです。不正ログインの手口は、多くの場合、パスワードリスト攻撃(攻撃者が、取得済のユーザIDやパスワードといったアカウント情報を使って、別のWebサイトでのログインを試みるもの)であると見られています。このような攻撃によって、アカウント情報が閲覧されるだけでなく、無断投稿、コンテンツの不正購入、ポイントの換金や現金不正利用等の被害が発生しました。同様の攻撃がこれまでも確認されているにもかかわらず、不正ログインが後を絶たない理由としては、利用者側でのセキュリティ対策意識が依然として低いという現状がうかがえます。

航空会社のマイレージ会員専用サイトへの不正ログイン事件に関しては、不正ログインの一因として、パスワード設定の仕様が旧来のままで、英数字を混合できないうえに、JALの場合は数字6桁、ANAの場合は数字4桁という制約が存在することも報道され、問題視されました。利用者にとっては、同一パスワードを使い回ししない、脆弱なパスワードを使用しないといったパスワード設定の基本を見直し、徹底することが常に望まれます。また、企業側においても、セキュリティ対策を考慮したシステム設計と、今回のような既知の攻撃に対しての対応として、システム改修を都度検討することが今後も一層求められます。

S.S.R.C.

Shield Security Research Center

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