株式会社 日立システムズ

SSRC-TR-Vol.16

S.S.R.C.定期
トレンドレポート
Vol.16

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.16

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 2013 年第 2 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:2013/4/1～2013/6/30

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. 遠隔操作ウイルス事件

関連記事	● 遠隔操作ウイルス事件 - 4/4 (現代ビジネス) http://gendai.ismedia.jp/articles/-/35315 ● 幼稚園襲撃予告で再逮捕へ＝ＰＣ遠隔操作で片山容疑者 警視庁など (時事ドットコム) http://www.jiji.com/jc/c?g=soc_30&k=2013041000028 ● 片山容疑者、公判前整理に＝ＰＣ遠隔操作?東京地裁（ウォール・ストリート・ジャーナル) http://jp.wsj.com/article/JJ11227996960082694559218324072213119747749.html ● 片山容疑者を追起訴へ＝誤認逮捕の幼稚園襲撃予告?ＰＣ遠隔操作・東京地検 （ウォール・ストリート・ジャーナル) http://jp.wsj.com/article/JJ12282921058044743930219898299651669956923.html ● ＰＣ遠隔操作:伊勢神宮爆破予告で再逮捕へ 業務妨害疑い（毎日新聞） http://mainichi.jp/select/news/20130504k0000m040084000c.html ● ＰＣ遠隔操作:雲取山で記憶媒体発見（毎日新聞） http://mainichi.jp/select/news/20130521k0000e040187000c.html ● 検察側、証拠示さず…ＰＣ遠隔操作の公判前整理（Yahoo Japan） http://bylines.news.yahoo.co.jp/egawashoko/20130522-00025135/ ● 遠隔操作、片山容疑者３回目起訴 一貫して無実を主張（47NEWS） http://www.47news.jp/CN/201305/CN2013052901001395.html

	● PC遠隔操作ウィルス事件 「警察の敗北宣言」で見えたIT捜査の稚拙さ（livedoor NEWS） http://news.livedoor.com/article/detail/7761221/

2. 韓国同時多発サイバー攻撃

関連記事	● 韓国への大規模サイバー攻撃の教訓　迫る本当の危機（日本経済新聞） http://www.nikkei.com/article/DGXNASFK0101X_R00C13A4000000/ ● 韓国へのサイバーテロ - 4/10 http://d.hatena.ne.jp/Kango/20130323/1363986809 http://japanese.joins.com/article/354/170354.html?servcode=500&sectcode=510

3. 北朝鮮へのサイバーテロ

関連記事	● 北朝鮮の公式 Twitter アカウントなどもハッキングされ、関連サイトが改ざんされて金正恩第一書記をからかう画像などが掲載された（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1304/05/news035.html ● 攻撃を受けたサイトの一部は運用再開。また、アノニマスは 6 月 25 日に北朝鮮核施設を攻撃することを示唆。 http://news.livedoor.com/article/detail/7577206/ http://news.livedoor.com/article/detail/7576195/ http://news.livedoor.com/article/detail/7574718/ http://japanese.joins.com/article/231/170231.html?servcode=500&sectcode=510 http://sankei.jp.msn.com/world/news/130409/kor13040900380000-n1.htm ● 中国当局が、中国から北朝鮮への観光旅行の取扱いを一時停止するよう指示。 http://www.j-cast.com/2013/04/09172745.html http://zasshi.news.yahoo.co.jp/article?a=20130409-00000332-playboyz-soci http://www.zakzak.co.jp/society/politics/news/20130410/plt1304100711000-n1.htm

	http://sankei.jp.msn.com/world/news/130410/chn13041014130005-n1.htm

4. Kaspersky Lab、Android マルウェアを使用した標的型攻撃を特定

関連記事	● 中国語圏の作者による Android 端末を狙う世界初の深刻な標的型攻撃が発生 ウイグル人活動家のモバイル端末から連絡先リスト、メッセージなどの情報を詐取（Kaspersky） http://www.kaspersky.co.jp/news?id=207585751

5. アプリケーションによって表示される広告を介して拡散する Android 向け偽アンチウイルス

関連記事	● 偽の広告を表示させ、感染しようとする Android マルウェア「Android.Fakealertt」についての注意喚起（Dr.WEB） http://news.drweb.co.jp/?i=620&c=1&lng=ja&p=0

6. 不正アクセス:ＨＰ改ざん容疑の少年を逮捕…京都府警

関連記事	● Tor を使い、他人の HP に不正アクセスしたとして、神奈川県在住の未成年が逮捕（毎日新聞） http://mainichi.jp/select/news/20130425k0000e040199000c.html

7. 不正ライブラリが組み込まれた Android アプリが Google Play 上に 32 件 - 偽広告 SDK を装った攻撃か

関連記事	● 4 件の開発者アカウントを通じて配布されており、ダウンロード回数は、200 万回から最大で 900 万回に及ぶと見られる（Security NEXT） http://www.security-next.com/039598

8. 複数の銀行で９千万円被害　ネットバンキング不正事件

関連記事	● 利用者のパソコンの多くは、送金などをする際に本人確認のため銀行からパソコンのメールアドレスに送られてくる「ワンタイムパスワード」を盗み取る新タイプのウイルスに感染していた http://www.tokyo-np.co.jp/s/article/2013042401002172.html http://tumblr.tokumaru.org/post/48803296783/new-virus-steals-one-time-password

9. スマホ向け認証・決済サービス「mopita」、5450 アカウント不正ログイン被害

関連記事	● 不正ログインが行われていたのは 4 月 18 日 2 時 24 分から 19 日 15 時 55 分までの期間（エムティーアイ） http://www.mti.asia/?p=17449

10. ＡＰ通信ハッキング、シリア情報相が「電子軍」の犯行を否定

関連記事	● 訪問先のロシア・モスクワで記者会見した情報相は、アサド大統領を支持するシリア電子軍が、今回のハッキングを行うことは考えられないと述べた（ロイター） http://jp.reuters.com/article/worldNews/idJPTYE93O00H20130425?feedType=RSS&feedName=worldNews

11. ３月の大規模サイバー攻撃、スペインで容疑者を逮捕

関連記事	● スペイン警察によれば、容疑者は３５歳のオランダ国籍の男だという http://www.cnn.co.jp/tech/35031466.html http://japan.internet.com/webtech/20130328/8.html

12. LivingSocial にサイバー攻撃--アカウント 5000 万件以上に影響か

関連記事	● LivingSocial によると、不正にアクセスされたデータには、一部ユーザーの氏名、メールアドレス、誕生日のほか、暗号化されたパスワード（「ハッシュ化」して「ソルティング」されたパスワード）が含まれているという（CNET Japan） http://japan.cnet.com/news/service/35031431/

13. Yahoo！JAPAN に不正アクセス　最大 2200 万 ID が流出した恐れ

関連記事	● Yahoo！JAPAN ID を管理しているサーバが不正アクセスを受け、最大 2200 万件の ID が流出した可能性（ITmedia） http://www.itmedia.co.jp/news/articles/1305/18/news008.html

14. 農水省の内部文書１２４点流出か　サイバー攻撃調査委

関連記事	● 同省の規定で機密レベルは３段階あり、流出した可能性があるのは、レベルが２番目に高い文書８５点と最も低い文書３９点だった http://www.maff.go.jp/j/press/kanbo/hisyo/pdf/130524_1-02.pdf http://www.asahi.com/national/update/0525/TKY201305240456.html

15. 「イモトの WiFi」のグローバルデータ、不正アクセスでカード情報 11 万件流出　セキュリティコードや住所も

関連記事	● 10 万件以上のユーザーのクレジットカード情報やセキュリティコード、住所などが流出 http://www.xcomglobal.co.jp/info http://www.itmedia.co.jp/news/articles/1305/27/news131.html

16. 市職員が住民情報システムから個人情報を不正取得 - 加古川市

関連記事	● 兵庫県加古川市において、職員が職務権限を利用して不正に住民情報を取得し、外部へ漏洩していたことがわかった（Security NEXT） http://www.security-next.com/040307

17. 桃山学院大のサイトが不正アクセスにより改ざん - 情報収集目的か

関連記事	● 桃山学院大学は、同大のウェブサイトが不正アクセスにより改ざんされたと発表した。ウイルス感染や情報流出などの被害は確認されていないという（Security NEXT） http://www.security-next.com/040268

18. 阪急阪神百貨店サイトに不正アクセス - 個人情報流出の恐れ

関連記事	● 発表によると、最大で 2382 件の利用者情報(氏名、住所、電話番号、生年月日、性別、メールアドレス、セキュリティワード)が閲覧された可能性がある http://www.hanshin-dept.jp/hshonten/notice/onlineshop.html/ http://news.mynavi.jp/news/2013/05/29/290/

19. 玩具通販「ハピネット・オンライン」に不正アクセス、カード番号など不正閲覧

関連記事	● 不正に閲覧された可能性のある顧客情報は、氏名、住所、電話番号、生年月日、性別、メールアドレス、クレジットカード番号と有効期限。最大 9609 人のユーザー情報が不正に閲覧された可能性があり、うち最大 3909 人はクレジットカード情報が閲覧された可能性がある http://www.happinetonline.com/ http://internet.watch.impress.co.jp/docs/news/20130603_602053.html

20. 政府機関や軍事産業を狙うマルウェアスパイ、日本など 40 カ国 350 組織に被害

関連記事	● Kaspersky Lab によると、世界の大手企業や政府機関などがマルウェア「NetTraveler」に感染している（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1306/06/news030.html

21. Android 史上「最も高度なマルウェア」、Kaspersky Lab が報告

関連記事	● このマルウェアの複雑さと、未解決の脆弱性を多数悪用しているという特徴は、ほかの Android マルウェアよりも、Windows マルウェアに近いと Kaspersky は指摘する（ITmedia） http://www.itmedia.co.jp/news/articles/1306/10/news028.html

22. 米フェイスブック、６００万人の個人情報漏れ

関連記事	● ソーシャル・ネットワーキング・サービス（ＳＮＳ）最大手の米フェイスブックは２１日、システムの不具合で、過去１年間に利用者約６００万人の電話番号や電子メールアドレスが他の利用者に漏れていたと発表（YOMIURI ONLINE） http://www.yomiuri.co.jp/net/news0/world/20130622-OYT1T00814.htm

23. Android 端末を人質に取る“偽”ウイルス対策アプリが出現

関連記事	● 偽のウイルススキャンを実行し、端末をロックしてしまう悪質アプリが見つかったという（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1306/24/news021.html

24. 神奈川県二宮町のサイトが改ざん - 閲覧でウイルス感染のおそれ

関連記事	● 神奈川県二宮町のウェブサイトが、何者かの不正アクセスにより改ざんされ、閲覧によりウイルスへ感染する可能性があったことがわかった（Security NEXT） http://www.security-next.com/041172

25. Opera Software、19 日に同社の社内ネットワークが攻撃を受けたことを発表

関連記事	● 短時間「Opera」の自動更新機能を使ってマルウェアが配布された恐れ http://www.forest.impress.co.jp/docs/news/20130627_605503.html https://www.st.ryukoku.ac.jp/~kjm/security/memo/2013/06.html#20130627_opera http://www.sophos.com/ja-jp/press-office/press-releases/2013/06/ns-opera-breached-certificate-stolen.aspx

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 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/malware1302.html

2. 2013 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/malware1302_jp.html

3. 2013 年 3 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/malware1303.html

4. 2013 年 3 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/malware1303_jp.html

5. 2013 年 4 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/malware1304.html

6. 2013 年 4 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/malware1304_jp.html

7. 2013 年 5 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/malware1305.html

8. 2013 年 5 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/malware1305_jp.html

9. 2013 年 3 月のウイルス脅威

関連記事	● 2013 年 3 月のウイルス脅威（Dr.WEB） http://news.drweb.co.jp/?i=614&c=1&lng=ja&p=0

10. 2013 年 4 月のウイルス脅威

関連記事	● 2013 年 4 月のウイルス脅威（Dr.WEB） http://news.drweb.co.jp/?i=623&c=1&lng=ja&p=0

11. 2013 年 5 月のウイルス脅威

関連記事	● 2013 年 5 月のウイルス脅威（Dr.WEB） http://news.drweb.co.jp/?i=628&c=1&lng=ja&p=0

12. 韓国へのサイバー攻撃および新たな 2 つの Android アドウェア亜種に関する新情報も公表

関連記事	● フォーティネットの FortiGuard 脅威動向調査チーム、今四半期最大の脅威は Bitcoin を狙う ZeroAccess ボットネットであることを報告（Fortinet） http://www.fortinet.co.jp/press_releases/130415.html

13. Kaspersky Lab、Android マルウェアを使用した標的型攻撃を特定

関連記事	● 中国語圏の作者による Android 端末を狙う世界初の深刻な標的型攻撃が発生 ウイグル人活動家のモバイル端末から連絡先リスト、メッセージなどの情報を詐取（Kaspersky） http://www.kaspersky.co.jp/news?id=207585751

14. 札幌市:観光情報サイトが新種ウイルス感染…閉鎖続く

関連記事	● 札幌市のホームページの観光情報サイト「ようこそさっぽろ」が新種ウイルスに感染し、２週間以上閉鎖が続いている。（毎日新聞） http://mainichi.jp/select/news/20130621k0000m040041000c.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＜2013.04.03＞

プレス リリース	● チェックしておきたい脆弱性情報＜2013.04.03＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20130401/467643/?ST=security

2. チェックしておきたい脆弱性情報＜2013.04.09＞

プレス リリース	● チェックしておきたい脆弱性情報＜2013.04.09＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20130408/469101/?ST=security

3. チェックしておきたい脆弱性情報＜2013.04.23＞

プレス リリース	● チェックしておきたい脆弱性情報＜2013.04.23＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20130422/472544/?ST=security

4. チェックしておきたい脆弱性情報＜2013.05.01＞

プレス リリース	● チェックしておきたい脆弱性情報＜2013.05.01＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20130426/474101/?ST=security

5. チェックしておきたい脆弱性情報＜2013.05.08＞

プレス リリース	● チェックしておきたい脆弱性情報＜2013.05.08＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20130507/474924/?ST=security

6. チェックしておきたい脆弱性情報＜2013.05.13＞

プレス リリース	● チェックしておきたい脆弱性情報＜2013.05.13＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20130507/474932/?ST=security

7. チェックしておきたい脆弱性情報＜2013.05.28＞

プレス リリース	● チェックしておきたい脆弱性情報＜2013.05.28＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20130527/479681/?ST=security

8. チェックしておきたい脆弱性情報＜2013.05.31＞

プレス リリース	● チェックしておきたい脆弱性情報＜2013.05.31＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20130527/479962/

9. チェックしておきたい脆弱性情報＜2013.06.06＞

プレス リリース	● チェックしておきたい脆弱性情報＜2013.06.06＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20130604/482161/

10. チェックしておきたい脆弱性情報＜2013.06.10＞

プレス リリース	● チェックしておきたい脆弱性情報＜2013.06.10＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20130604/482163/?ST=security

11. チェックしておきたい脆弱性情報＜2013.06.17＞

プレス リリース	● チェックしておきたい脆弱性情報＜2013.06.17＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20130613/484849/?ST=security

5. 総括

今期は、不正アクセスによるWebサイト改ざん、ID、パスワード、クレジットカード番号等を含む個人情報の流出事件が多発しました。流出した情報は、最近流行のパスワードリスト攻撃（他の情報源から事前入手したID、パスワードの組み合わせで不正アクセスを試す攻撃）に用いられる危険性が懸念され、利用者側の自衛策として、複数のサイト及びサービスでパスワードの使い回しをしないことが望まれます。

また、Android端末を標的としたモバイルマルウェアも目立ってきており、偽アンチウィルスソフトの他、Androidの脆弱性を悪用したマルウェア、悪意を持ったコードを含む不正ライブラリをアプリ開発者に利用させることで、一見無害なアプリにマルウェアを忍ばせる等、手口が巧妙化しています。アプリ開発者が悪意を持って不正なライブラリを組み込んだのか、不注意で組み込んでしまったのか経緯は不明ですが、Androidアプリの開発において、サードパーティ製のライブラリを組み込む際には細心の注意を払う必要があります。

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