株式会社 日立システムズ

SSRC-TR-Vol.20

S.S.R.C.定期
トレンドレポート
Vol.20

株式会社　日立システムズ

セキュリティリサーチセンタ

© Hitachi Systems, Ltd. 2014. All rights reserved.

S.S.R.C.トレンドトレポート Vol.20

目次

S.S.R.C.
Shield Security Research Center

© Hitachi Systems, Ltd. 2014. 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。

S.S.R.C. Shield Security Research Center

© Hitachi Systems, Ltd. 2014. All rights reserved.

3. トレンドレポート 2014 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:2014/4/1～2014/6/30

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. フィッシング

関連記事	● ゆうちょ銀行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/20140401jpbank.html ● お名前.com 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/onamaecom20140415.html ● [05/01 更新]三井住友カード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/smbc_card20140430.html ● スクウェア・エニックス(FINAL FANTASY XIV)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/square_enix20140508.html ● 三菱東京 UFJ 銀行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/mufg20140610.html ● スクウェア・エニックス（ドラゴンクエスト X）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/square_enix20140611.html ● りそな銀行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/resona20140616.html ● ウェブマネ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/webmoney20140626.html ● 三井住友銀行をかたるフィッシング(フィッシング対策協議会)

© Hitachi Systems, Ltd. 2014. All rights reserved.

	http://www.antiphishing.jp/news/alert/smbc20140627.html ● Amazon ギフト券プレゼントキャンペーンを装ったフィッシング詐欺に注意(Internet Watch) http://internet.watch.impress.co.jp/docs/news/20140618_653910.html ● 大学職員のメールアカウントがフィッシングで詐取 - スパム送信の踏み台に(Security NEXT) http://www.security-next.com/048904 ● 2014/04 フィッシング報告状況(フィッシング対策協議会) https://www.antiphishing.jp/report/monthly/201404.html ● 2014/05 フィッシング報告状況(フィッシング対策協議会) https://www.antiphishing.jp/report/monthly/201405.html ● 2014/06 フィッシング報告状況(フィッシング対策協議会) https://www.antiphishing.jp/report/monthly/201406.html

2. オンラインバンキング被害

関連記事	● ESET、ネットバンキングの不正送金マルウェアに警鐘 - 日本国内で活発化(マイナビニュース) http://news.mynavi.jp/news/2014/04/02/516/ ● 法人向けネットバンキングでも不正送金、シマンテックが注意喚起(日経コンピュータ) http://itpro.nikkeibp.co.jp/article/NEWS/20140410/549842/?top_tl1 ● インターネットバンキングを悪用した不正送金への注意喚起(ラック) http://www.lac.co.jp/security/alert/2014/04/14_alert_01.html ● キヤノン ITS、ネットバンキングの不正送金を目論むウイルスの拡大を確認(マイナビニュース) http://news.mynavi.jp/news/2014/04/14/406/ ● 巧妙化するネットバンキングの不正送金問題 - 法人には倒産リスクも(Security

© Hitachi Systems, Ltd. 2014. All rights reserved.

	NEXT) http://www.security-next.com/048711 ● オンラインバンキングを狙うトロイの木馬: 日本のインターネットユーザーに対して執拗に続く攻撃(Symantec) http://www.symantec.com/connect/ja/blogs-345 ● Android 向けのバンキングマルウェアが急増(Kaspersky) https://blog.kaspersky.co.jp/faketoken-2014q1/

3. MITB 攻撃

関連記事	● 三井住友銀行の不正送金は「MITB 攻撃」、ワンタイムパスワード利用者も被害に(日経コンピュータ) http://itpro.nikkeibp.co.jp/article/NEWS/20140513/556399/

4. Gameover Zeus 摘発

関連記事	● ボットネット型マルウェア「Gameover Zeus」と身代金要求型マルウェア「CryptoLocker」を摘発(McAfee) http://www.mcafee.com/japan/security/mcafee_labs/blog/content.asp?id=1415 ● 国内ＰＣ、２０万台感染か＝不正送金ウイルス－所有者に通知へ・警察庁など(時事ドットコム) http://www.jiji.com/jc/zc?k=201406/2014060300889

5. OpenSSL の脆弱性問題(Heartbleed)

関連記事	● OpenSSL の脆弱性に関する注意喚起 (JPCERT/CC) https://www.jpcert.or.jp/at/2014/at140013.html ● OpenSSL の脆弱性、影響は極めて重大 - パスワードや秘密鍵の流出も(ITmedia) http://www.itmedia.co.jp/enterprise/articles/1404/09/news041.html ● パッチ未適用のサーバーに深刻な脅威となる Heartbleed 脆弱性(Symantec)

© Hitachi Systems, Ltd. 2014. All rights reserved.

	http://www.symantec.com/connect/ja/blogs/heartbleed ● 脆弱性「Heartbleed」、モバイルアプリにも影響(Trend Micro) http://blog.trendmicro.co.jp/archives/8945 ● OpenSSL の脆弱性で初の被害、カナダや英国で発覚(ITmedia) http://www.itmedia.co.jp/news/articles/1404/15/news035.html ● バンドルされた OpenSSL ライブラリ、モバイルアプリおよび Android4.1.1 に脆弱性「Heartbleed」の影響を与えることを確認(Trend Micro) http://blog.trendmicro.co.jp/archives/8961 ● Tor ノードに OpenSSL の脆弱性、通信内容の平文流出も(ITmedia) http://www.itmedia.co.jp/enterprise/articles/1404/18/news046.html ● OpenSSL 脆弱性攻撃の被害、ついに現実に……三菱 UFJ ニコス、会員 894 名の情報が漏えいか(RBB TODAY) http://www.rbbtoday.com/article/2014/04/21/119072.html ● OpenSSL 脆弱性対策の「致命的なミス」、秘密鍵を変更せず(ITmedia) http://www.itmedia.co.jp/enterprise/articles/1405/12/news038.html ● 終わりが見えない Heartbleed 攻撃、新たな手口で無線 LAN が危ない(TechTarget) http://techtarget.itmedia.co.jp/tt/news/1406/16/news05.html ● OpenSSL の脆弱性、いまだに悪用可能な Web サイトが相当数存在(ITmedia) http://www.itmedia.co.jp/enterprise/articles/1406/17/news038.html

© Hitachi Systems, Ltd. 2014. All rights reserved.

6. Apache Struts2 と Apache Struts1 の脆弱性問題

関連記事	● 更新：Apache Struts2 の脆弱性対策について(CVE-2014-0094)(CVE-2014-0112)(CVE-2014-0113)(IPA) http://www.ipa.go.jp/security/ciadr/vul/20140417-struts.html ● Apache Struts2（2.3.16、S2-020 の修正版）に対するゼロディを弊社エンジニアが発見いたしました。(三井物産セキュアディレクション) http://www.mbsd.jp/news20140422.html ● サイト構築ソフトに欠陥　官公庁などサイバー攻撃の恐れ(日本経済新聞) http://www.nikkei.com/article/DGXNASDZ240HW_U4A420C1EA2000/

7. リスト型攻撃

関連記事	● ニコニコ動画に不正ログイン約 22 万件が発覚 - 17 万円分のポイント不正使用も(マイナビニュース) http://news.mynavi.jp/news/2014/06/13/263/ ● はてなに約 160 万回の不正ログイン試行、Amazon ギフト券交換 3 件は阻止(日経コンピュータ) http://itpro.nikkeibp.co.jp/article/NEWS/20140623/566043/ ● 「Ameba」で不正ログイン被害 3 万 8280 件、またパスワードリスト攻撃(INTERNET Watch) http://internet.watch.impress.co.jp/docs/news/20140624_654903.html ● 3 週間で 50 万件超の不正ログイン、「リスト型攻撃」が止まらない(日経コンピュータ) http://itpro.nikkeibp.co.jp/article/COLUMN/20140624/566362/

© Hitachi Systems, Ltd. 2014. All rights reserved.

8. Windows XP のサポートが 4 月 9 日に終了

関連記事	● サポート終了後の Windows XP 対応策(エフセキュア) http://blog.f-secure.jp/archives/50725039.html ● 地方公共団体の XP 使用率は 13.0%　約 26 万 5000 台が稼働中――総務省調査(ITmedia) http://www.itmedia.co.jp/news/articles/1404/14/news061.html ● 米国国税庁も「Windows XP」有料サポートを契約(WIRED) http://wired.jp/2014/04/15/windows-xp-laggard-will-pay-microsoft/ ● パロアルトネットワークスが Internet Explorer に存在する重大な脆弱性 21 件を特定(インターネットコム) http://internetcom.jp/busnews/20140612/5.html ● Windows XP の脆弱性は必ず狙われる(日経コンピュータ) http://itpro.nikkeibp.co.jp/article/COLUMN/20140612/563463/

9. POS への攻撃

関連記事	● 先週の注目ニュース：POS 端末のリスク、各社の月例パッチなど(Kaspersky) http://blog.kaspersky.co.jp/news-points-of-sale-under-attack/ ● 実は安全ではない「POS レジ」 サイバー犯罪者が好んで狙う理由は(TechTarget) http://techtarget.itmedia.co.jp/tt/news/1406/19/news07.html ● POS システムや仮想通貨を狙う攻撃が増加(Trend Micro) http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20140512053131.html ● ＜ＰＯＳ＞ウイルスまん延　レジと一体、カード情報危険に(Yahoo) http://headlines.yahoo.co.jp/hl?a=20140630-00000045-mai-soci

© Hitachi Systems, Ltd. 2014. All rights reserved.

10. 偽 Flash Player

関連記事	● Flash Player の偽更新メッセージに注意　悪意あるプログラムのインストール誘導(ITmedia) http://www.itmedia.co.jp/news/articles/1406/19/news124.html ● ネット広告から Flash Player を偽装するアドウェアへの誘導、日本から 1 万 7 千件以上のアクセスを確認(Trend Micro) http://blog.trendmicro.co.jp/archives/9335

11. CDNetworks 改ざん

関連記事	● CDNetworks の改ざん、エッジサーバーからのアップロード機能を悪用か(日経コンピュータ) http://itpro.nikkeibp.co.jp/article/NEWS/20140605/561702/ ● CDNetworks のウイルス被害、認証サーバーを介さずに直接改ざん(日経コンピュータ) http://itpro.nikkeibp.co.jp/article/NEWS/20140619/565342/

S.S.R.C.
Shield Security Research Center

© Hitachi Systems, Ltd. 2014. 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. 2014 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/malware1403.html

2. 2014 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/malware1403_jp.html

3. 2014 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/malware1404.html

4. 2014 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/malware1404_jp.html

5. 2014 年 3 月のウイルス脅威

関連記事	● 2014 年 3 月のウイルス脅威（Dr.WEB） http://news.drweb.co.jp/?i=726&c=1&lng=ja&p=1

6. 2014 年 4 月のウイルス脅威

関連記事	● 2014 年 4 月のウイルス脅威（Dr.WEB） http://news.drweb.co.jp/?i=732&c=1&lng=ja&p=0

© Hitachi Systems, Ltd. 2014. 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＜2014.3.20＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.3.20＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140319/544482/

2. チェックしておきたい脆弱性情報＜2014.3.24＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.3.24＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140319/544483/

3. チェックしておきたい脆弱性情報＜2014.04.02＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.04.02＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140401/547443/

4. チェックしておきたい脆弱性情報＜2014.04.07＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.04.07＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140401/547444/

5. チェックしておきたい脆弱性情報＜2014.04.17＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.04.17＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140415/550844/

6. チェックしておきたい脆弱性情報＜2014.05.13＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.05.13＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140509/555763/

© Hitachi Systems, Ltd. 2014. All rights reserved.

7. チェックしておきたい脆弱性情報＜2014.05.14＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.05.14＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140509/555764/

8. チェックしておきたい脆弱性情報＜2014.05.16＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.05.16＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140512/556183/

9. チェックしておきたい脆弱性情報＜2014.05.22＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.05.22＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140520/558102/

10. チェックしておきたい脆弱性情報＜2014.05.28＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.05.28＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140526/559403/

Shield Security Research Center

11. チェックしておきたい脆弱性情報＜2014.05.30＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.05.30＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140526/559404/

12. チェックしておきたい脆弱性情報＜2014.06.10＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.06.10＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140606/562344/

© Hitachi Systems, Ltd. 2014. All rights reserved.

13. チェックしておきたい脆弱性情報＜2014.06.12＞

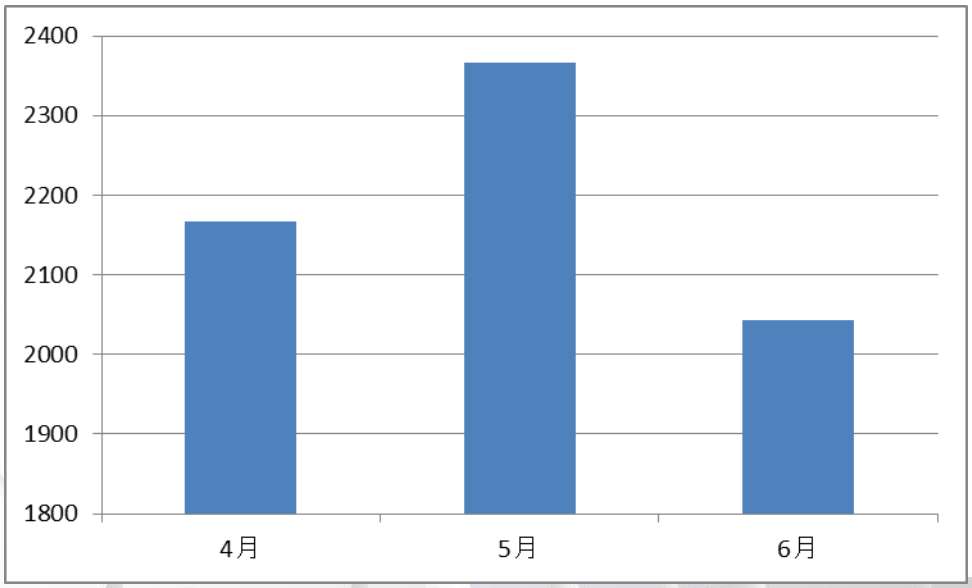
プレス リリース	● チェックしておきたい脆弱性情報＜2014.06.12＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140606/562347/

S.S.R.C.
Shield Security Research Center

© Hitachi Systems, Ltd. 2014. 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。

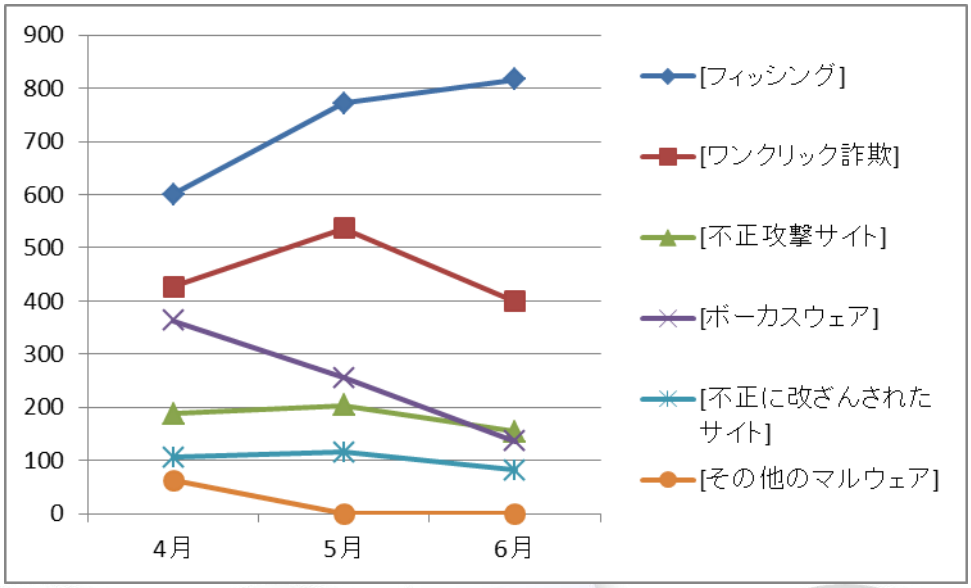


「危険な可能性」と判断されたウェブサイトの件数

Shield Security Research Center

* 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. 2014. All rights reserved.



脅威別検知数の月別推移(2014 年 4 月～6 月)

今期のサイバー犯罪の傾向としては、フィッシングの報告件数が増加傾向にあります。金融機関や、オンラインゲームの運営をかたるフィッシングが特に増加しています。他にもギフト券プレゼントキャンペーンを装って電子マネーを狙うものや、ドメイン名登録サービスをかたったものなども発生しています。

フィッシングメールついては、違和感の無い文面のものも現れています。その一方で稚拙なフィッシングメールも存在しますが「システム更新のため、認証しないとアカウントが使用できなくなる」、「メールアドレスを確認してください」などと言う内容は共通しており、ユーザにクリックを促す内容になっています。

© Hitachi Systems, Ltd. 2014. All rights reserved.

6. 総括

今期は影響範囲の大きい脆弱性が複数発見され、世間を騒がせました。回避策は比較的早期に公開されましたが、根本対策となるものが公開されるまでに多少時間がかかりました。また、現在も対策されていないサーバが多数あると言われています。

その脆弱性は、OpenSSL の脆弱性と Apache Struts の脆弱性です。

Heartbleed とよばれる OpenSSL の脆弱性は、OpenSSL のサーバの秘密鍵や利用者のセッション・クッキーやパスワードを盗み出せる脆弱性でした。基本的な対策はコンパイルオプションでハートビート機能を無効にするか、脆弱性を修正したバージョンへの更新となっています。また、データが盗み出された痕跡が残らないことから、盗まれた可能性があることを前提とした対応が求められ、秘密鍵の再発行が推奨されています。現在も対策されていないサイトが非常に多いとされており注意が必要です。

もう一つの Apache Struts の脆弱性は、ウェブアプリケーションの動作権限内で、情報の窃取や特定ファイルの操作、また Java コードが含まれている場合、任意のコードが実行される可能性があります。この脆弱性は、2013 年 4 月にサポートが切れた Apache Struts1 も影響を受けるものでしたが、開発元から修正版が提供されず問題になりました。Apache Struts1 は、Apache Struts2 との互換性がないため、容易にアップグレードが行えず、脆弱性を修正できていないサーバが多く見受けられました。サポート切れのソフトウェアを使い続けることのリスクが浮き彫りになりました。

これらの脆弱性の問題の経緯を踏まえて、再度、管轄下のサーバが対策できているかの確認を行う事を推奨いたします。

© Hitachi Systems, Ltd. 2014. 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. 2014. All rights reserved.