SSRC-TR-2010-07

S.S.R.C.定期
トレンドレポート
Vol.4

株式会社　日立情報システムズ

セキュリティリサーチセンタ

初版　2010/07/01

S.S.R.C.トレンドトレポート Vol.4

目次

1. はじめに

S.S.R.C.(Shield Security Research Center)は、株式会社日立情報システムズ 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する予定です。

本文書は、株式会社日立情報システムズ、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、株式会社日立情報システムズ(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 2010 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:2010/04/01～2010/06/30

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. ヤフーの電子メールにハッカー侵入、中国滞在の外国人記者が使用

関連記事	● ヤフーの電子メールにハッカー侵入か、中国滞在の外国人記者が使用（AFP BB News） http://www.afpbb.com/article/environment-science-it/it/2715141/5556035 ● ジャーナリストなどの Yahoo メールアカウントが中国と台湾でハックされたらしい（Cyber law） http://cyberlaw.cocolog-nifty.com/blog/2010/03/yahoo-ef4d.html

2. 京都府警、映画違法配信容疑で逮捕、「Ｐ２Ｐ観測システム」を利用した初の事例

関連記事	● 京都府警、映画違法配信容疑で逮捕。ファイル共有ソフト使いネットに（京都新聞） http://www.kyoto-np.co.jp/article.php?mid=P20100331000217&genre=C1&area=K00

3. IE悪用攻撃は数日で 50 カ国に拡大──未修正の脆弱性(CVE-2010-0806)による危険な実態

関連記事	● IE 悪用攻撃は数日で 50 カ国に拡大──未修正の脆弱性による危険な実態（IT media） http://www.itmedia.co.jp/enterprise/articles/1004/02/news021.html ● Active Exploitation of CVE-2010-0806（Microsoft Malware Protection Center） http://blogs.technet.com/b/mmpc/archive/2010/03/30/active-exploitation-of-cve-2010-0806.aspx

4. マカフィー、「サイバー犯罪とハクティビズム」レポートを発表

プレスリリース	● マカフィー、「サイバー犯罪とハクティビズム」レポートを発表　～増加の一途をたどる組織的なサイバー犯罪や、政治目的のハッキング活動に警鐘～ http://www.mcafee.com/japan/about/prelease/pr_10a.asp?pr=10/04/05-1

5. 情報を盗む「サイバースパイ網」、中国に存在の可能性

関連記事	● 情報を盗む「サイバースパイ網」、中国に存在か（IT media） http://www.itmedia.co.jp/news/articles/1004/07/news025.html ● チベットやインドを監視するスパイ・ネット、政府機関やダライ・ラマ事務所の PC を攻撃（IT pro） http://itpro.nikkeibp.co.jp/article/NEWS/20100407/346764/

6. 国内企業の情報セキュリティ対策実態調査結果を発表

プレスリリース	● マカフィー、「サイバー犯罪とハクティビズム」レポートを発表　～増加の一途をたどる組織的なサイバー犯罪や、政治目的のハッキング活動に警鐘～ http://www.mcafee.com/japan/about/prelease/pr_10a.asp?pr=10/04/05-1

7. 「違法DLでネット切断」法案、英国でも可決

関連記事	● 「違法 DL でネット切断」法案、英国でも可決（IT media） http://www.itmedia.co.jp/news/articles/1004/12/news033.html

8. Word Pressのブログに大量のハッキング被害、不正サイトへ誘導も

関連記事	● Word Press のブログに大量のハッキング被害、不正サイトへ誘導も（IT media） http://www.itmedia.co.jp/news/articles/1004/13/news016.html

9. 米大手企業の最大 88%が「Zeus」ボットネット攻撃の被害に--米調査

関連記事	● 米大手企業の最大 88%が「Zeus」ボットネット攻撃の被害に--米調査（ZDNet Japan） http://japan.zdnet.com/news/sec/story/0,2000056194,20412154,00.htm

10. Google 対中国：第一次サイバー世界大戦

関連記事	● Google 対中国：第一次サイバー世界大戦（japan.internet.com） http://japan.internet.com/busnews/20100416/6.html

11. フィッシング対策ガイドライン 2010 年度版

プレスリリース	● フィッシング対策ガイドライン 2010 年度版（フィッシング対策協議会） https://www.antiphishing.jp/antiphishing_guide.pdf

12. 神奈川県警でサイバーテロ対策本部が発足

関連記事	● 神奈川県警でサイバーテロ対策本部が発足（ポリスチャンネル） http://www.police-ch.jp/news/2010/05/006326.php

13. 米グーグル、無線ＬＡＮの個人データを誤収集

関連記事	● 米グーグル、無線ＬＡＮの個人データを誤収集（ウォールストリートジャーナル） http://jp.wsj.com/IT/node_61126 ● グーグル、Wi-Fi ネットワークの通信情報を誤って収集--Street View 撮影用車両で（CNET Japan） http://japan.cnet.com/news/media/story/0,2000056023,20413470,00.htm ● グーグルがストビューカーで勝手に収集していたデータ、重要なパスワードやメール本文も含まれると判明！（ギズモード） http://www.gizmodo.jp/2010/06/post_7223.html

14. ドイツではパスワードを設定していない無線LANが罰金対象になりうる

関連記事	● ドイツではパスワードを設定していない無線LANが罰金対象になりうる（スラッシュドットジャパン） http://slashdot.jp/security/article.pl?sid=10/05/17/0556216

15. 富士火災や富士生命の顧客リストが外部流出

プレスリリース	● お客様情報紛失に関するお詫びと弊社への金銭要求に関するご報告について（富士火災海上保険株式会社） http://www.fujikasai.co.jp/news/attach/100518.pdf
関連記事	● 富士火災や富士生命の顧客リストが外部流出 - 金銭要求の投書で判明（Security NEXT） http://www.security-next.com/012589.html

16. 米国防総省が、メリーランド州フォートミード基地にサイバー司令部を設置

関連記事	● Lynn Notes Cyber Command's Significance（DEPARTMENT OF DEFENSE） http://www.defense.gov/news/newsarticle.aspx?id=59295

17. 図書館ＨＰにアクセス３万３千回　業務妨害容疑で男逮捕

関連記事	● robots.txtに従わず、図書館ＨＰにアクセス３万３千回　業務妨害容疑で男逮捕（サーバ管理者日誌） http://www.nantoka.com/~kei/diary/?201005c#T201005262 ● マスコミ報道だけでは分からない岡崎図書館事件（Libra hack） http://librahack.jp/

18. Webブラウザのタブがいつの間にか詐欺サイトに – タブナッピング攻撃

関連記事	● Web ブラウザのタブがいつの間にか詐欺サイトに、新手の攻撃を実証（IT media） http://www.itmedia.co.jp/news/articles/1005/26/news031.html

19. 人間をコンピューターウイルスに感染させる初の実験

関連記事	● 人間をコンピューターウイルスに感染させる初の実験、英研究者が自身の体で（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/20100527_369790.html

20. サイバー犯罪対策における国際情勢

関連記事	● サイバー犯罪対策における国際情勢（McAfee） http://www.mcafee.com/japan/security/mcafee_labs/blog/cooperation-grows-in-fight-against-cybercrime.asp

21. Unlha32.dll等開発停止、LHA書庫の使用中止呼びかけ

関連記事	● Unlha32.dll等開発停止、LHA書庫の使用中止呼びかけ（スラッシュドットジャパン） http://slashdot.jp/~Claybird/journal/508709

22. Winny違法利用者への警告メールが本格始動

プレスリリース	● メールによる注意喚起活動（CCIF） http://www.ccif-j.jp/activity.html#1
関連記事	● 「確信犯があぶり出される」Winny 違法利用者への警告メールが本格始動（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/20100610_373278.html

23. 韓国政府サイトに大規模なサイバー攻撃、中国経由

関連記事	● 韓国政府サイトに大規模なサイバー攻撃、中国経由（AFP BB News） http://www.afpbb.com/article/environment-science-it/it/2734844/5863452

24. イランがインターネット警察創設

関連記事	● イランがインターネット警察創設へ「危険な兆候を排除」（CNN） http://cnn.co.jp/world/AIC201006170012.html

25. 各国の「サイバー戦」軍備

関連記事	● 各国の「サイバー戦」軍備（人民網） http://j.people.com.cn/94474/7029531.html

3.2. WEB サイト改ざん関連情報

当期間確認された WEB サイト改ざん（Gumblar 被害等）に関する情報は以下の通りです。

1. 神戸市関連サイト「こうべ環境未来館」が改ざん被害に

ニュースリリース	● ホームページのウイルス感染について（神戸市） http://www.city.kobe.lg.jp/other/100401.html
関連記事	● 神戸市関連サイト「こうべ環境未来館」が改ざん被害 - 原因は「Gumblar」亜種（Security NEXT） http://www.security-next.com/012357.html

2. NPO支援施設のサイトが改ざん被害に

関連記事	● NPO 支援施設のサイトが改ざん、ウイルス感染のおそれ - 埼玉県（Security NEXT） http://www.security-next.com/012374.html

3. 理化学機器販売会社のウェブサイトが改ざん被害に

ニュースリリース	● 株式会社レスカ社ホームページに関するお詫びとお知らせ（株式会社レスカ社） http://www.rhesca.co.jp/main/company/info201003.html
関連記事	● 理化学機器販売会社のウェブサイトが「Gumblar 亜種」により改ざん（Security NEXT） http://www.security-next.com/012390.html

4. 日本マーケティング・サイエンス学会サイトが改ざん被害に

関連記事	● 「Gumblar」亜種で 2 週間にわたり改ざん状態に - 日本マーケティング・サイエンス学会（Security NEXT） http://www.security-next.com/012398.html

5. 大阪のシステム開発会社サイトが改ざん被害に

ニュースリリース	● 【お詫び】ホームページ改ざん被害について（デジタルアソシエーション株式会社） http://www.digital-as.co.jp/newstopics/2010/04/post-8.html
関連記事	● 「Gumblar」亜種感染でサイトが改ざん - 大阪のシステム開発会社（Security NEXT） http://www.security-next.com/012394.html

6. ダンス関連NPOが運営する複数サイトが改ざん被害に

関連記事	● ダンス関連 NPO が運営する複数サイトが改ざん - 閲覧でウイルス感染のおそれ（Security NEXT） http://www.security-next.com/012416.html

7. 日本インターンシップ協会サイトが改ざん被害に

ニュースリリース	● コンピュータウィルス感染に関するお詫びとお願い（日本インターシップ推進協会） http://www.jipc.or.jp/news/100407.html
関連記事	● 「Gumblar」による改ざんで閲覧者にウイルス感染のおそれ - 日本インターンシップ協会（Security NEXT） http://www.security-next.com/012418.html

8. 北海道開発局サイトが改ざん被害に

関連記事	● 北海道開発局の PC にウイルス感染のおそれ - サイトも緊急停止に（Security NEXT） http://www.security-next.com/012445.html

9. サイバーガジェットサイトが改ざん被害に

ニュースリリース	● サイバーガジェットからホームページに関する報告とお詫び（サイバーガジェット） http://home.cybergadget.co.jp/news/trouble20100416.html
関連記事	● サイト改ざんで閲覧者に「Gumblar」亜種感染のおそれ - サイバーガジェット（Security NEXT） http://www.security-next.com/012446.html

10. ユニフレームサイトが改ざん被害に

ニュースリリース	● 弊社ホームページに関するお詫びとお知らせ（ユニフレーム） http://www.uniflame.co.jp/news/100420.htm
関連記事	● 「Gumblar」亜種によりサイトの全ページが改ざん - アウトドア用品メーカー（Security NEXT） http://www.security-next.com/012463.html

11. プロ野球選手 田口壮さんの公式サイトが改ざん被害に

関連記事	● プロ野球選手 田口壮さんの公式サイト改ざん被害 - 無題なブログ(べつになんでもないこと) http://puppet.asablo.jp/blog/2010/04/26/5043561 ● 「日本人プロ野球選手のオフィシャルサイト」改ざん事例に対する分析（トレンドマイクロ） http://blog.trendmicro.co.jp/archives/3458

12. ケイダッシュステージサイトが改ざん被害に

関連記事	● オードリーの公式サイトがGENOウイルスに感染！サイト一時閉鎖！（秒刊SUNDAY） http://www.yukawanet.com/archives/2613669.html

13. 広島県信用組合サイトが改ざん被害に

プレスリリース	● 当組合ホームページに関するお詫びとお知らせ（広島県信用組合） http://www.hiroshima-kenshin.co.jp/topics/pdfH22/20100428owabi.pdf
関連記事	● 広島信組のウェブサイトが「Gumblar」亜種で改ざん（Security NEXT） http://www.security-next.com/012515.html

14. 多摩農林サイトが改ざん被害に

プレスリリース	● 弊社ウェブサイトをご覧になった皆様へのお詫びとお願い（株式会社多摩農林） http://www.tamanorin.co.jp/index2.php
関連記事	● サイト制作会社の PC が「Gumblar」感染、改ざんが発生 - 山林管理会社（Security NEXT） http://www.security-next.com/012505.html

15. アパレル通販サイトが改ざん被害に

プレスリリース	● niko and...オンラインストアに関するお詫びとお知らせ（トリニティアーツ） http://www.nikoand.jp/nikoand_info0510.html
関連記事	● アパレル通販サイトが Gumblar 亜種で改ざん - トリニティアーツ（Security NEXT） http://www.security-next.com/012547.html

16. 「神戸ファッション美術館」のサイトが改ざん被害に

関連記事	● 「神戸ファッション美術館」のサイトが「Gumblar」亜種で改ざん（Security NEXT） http://www.security-next.com/012557.html

17. 源吉兆庵サイトが改ざん被害に

プレスリリース	● 弊社ホームページ改ざんに関するお詫び（源吉兆庵） http://www.kitchoan.jp/what/100515.html
関連記事	● ウェブサイトが改ざん、閲覧でウイルス感染のおそれ - 源吉兆庵（Security NEXT） http://www.security-next.com/012577.html

18. 複数のマラソン関連サイトが改ざん被害に

関連記事	● 複数のマラソン関連サイトが改ざん、閲覧者にウイルス感染のおそれ（Security NEXT） http://www.security-next.com/012573.html

19. ルコックスポルティフサイトが改ざん被害に

プレスリリース	● ホームページの不正アクセスに関するお詫びと対応のお知らせ（ルコックスポルティフ） http://www.descente.co.jp/important/100514.html
関連記事	● 止まらぬサイト改ざん：訪問の心あたりはありませんか～新規告知サイト 8 件（So-net） http://www.so-net.ne.jp/security/news/view.cgi?type=2&no=2237

20. エムエムネットサイトが改ざん被害に

関連記事	● ウェブサイトが改ざん被害、閲覧者にウイルス感染の可能性 - 医療機関コンサル会社（Security NEXT） http://www.security-next.com/012613.html

21. 大阪市都市型産業振興センターサイトが改ざん被害に

関連記事	● 大阪市都市型産業振興センターのロボット関連サイトが改ざん（Security NEXT） http://www.security-next.com/012625.html

22. ラッセルサイトが改ざん被害に

関連記事	● 「Gumblar」亜種によるサイト改ざん、閲覧者にウイルス感染のおそれ - ゲームソフト会社（Security NEXT） http://www.security-next.com/012617.html

23. ジェイ・エス・エスサイトが改ざん被害に

関連記事	● サイトのトップページが改ざん被害、閲覧でウイルス感染のおそれ - 警備会社（Security NEXT） http://www.security-next.com/012630.html

24. ロータス 21 サイトが改ざん被害に

関連記事	● 「Gumblar」亜種によりサイトの一部ページが改ざん - ロータス 21（Security NEXT） http://www.security-next.com/012634.html

25. フラワーショップJANE PACKERおよびLa Coloristeのサイトが改ざん被害に

関連記事	● サザビーリーグ子会社のフラワーショップサイトが相次いで改ざん（Security NEXT） http://www.security-next.com/012660.html

26. 田島ルーフィングサイトが改ざん被害に

関連記事	● 「Gumblar」亜種感染でサイトのトップページが改ざん - 田島ルーフィング（Security NEXT） http://www.security-next.com/012675.html

27. キャラアニ.comサイトが改ざん被害に

関連記事	● SQL インジェクションでサイト改ざん、個人情報の漏洩は否定 - キャラアニ.com（Security NEXT） http://www.security-next.com/012752.html

28. 日本ワムネットサイトが改ざん被害に

関連記事	● 「Gumblar」亜種によるサイト改ざん、閲覧にウイルス感染のおそれ - 日本ワムネット（Security NEXT） http://www.security-next.com/012784.html

29. 米Lenovoサイトが改ざん被害に

関連記事	● 米 Lenovo のサポートサイトが改ざん、閲覧でウイルス感染のおそれ - 国内向けサイトには影響なし（Security NEXT） http://www.security-next.com/012802.html

30. 野村リビングサポートサイトが改ざん被害に

関連記事	● 顧客情報含む書類を通勤途中に紛失 - 野村不動産グループ会社（Security NEXT） http://www.security-next.com/012854.html

3.3. 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. Googleなどを狙う攻撃コードが流出、McAfeeが警戒を呼びかけ

ニュースリリース	● Windows Mobile Terdial Trojan makes expensive phone calls (Graham Cluley's blog) http://www.sophos.com/blogs/gc/g/2010/04/10/windows-mobile-terdial-trojan-expensive-phone-calls/
関連記事	● 国際電話を悪用する携帯マルウェア出現、Windows Mobile を狙う（IT media） http://www.itmedia.co.jp/news/articles/1004/12/news008.html

2. 暴露系ウイルス(kenzero/kenzo)

ニュースリリース	● 暴露系ウイルス(kenzero/kenzo)について（ネットエージェント） http://forensic.netagent.co.jp/kenzero.html
関連記事	● ファイル共有ソフトで拡大するあらたな暴露ウイルスで個人情報漏洩や金銭被害が多発（Security NEXT） http://www.security-next.com/012344.html ● Kenzero が海外でも話題に（Cyber Law） http://cyberlaw.cocolog-nifty.com/blog/2010/04/kenzero-8010.html

3.4. 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

1. Java Deployment Toolkit の脆弱性を悪用したゼロディ攻撃

関連記事	● Java Deployment Toolkit の脆弱性を悪用したゼロディ攻撃を観測（TOKYO SOC Report） https://www-950.ibm.com/blogs/tokyo-soc/entry/javaws-201004?lang=ja ● Java の脆弱性を突く攻撃発生、歌詞サイトで悪用（IT Media） http://www.itmedia.co.jp/news/articles/1004/15/news034.html

2. シスコ製Wi-Fi装置に脆弱性

関連記事	● セキュリティ研究者ら、シスコ製 Wi-Fi 装置の脆弱性を説明--Black Hat カンファレンスで（CNET Japan） http://japan.cnet.com/news/sec/story/0,2000056024,20412307,00.htm

3. 危険度の高いPDF攻撃が 1 割以上出現

関連記事	● 危険度の高い PDF 攻撃が 1 割以上出現（G DATA） http://gdata.co.jp/press/archives/2010/05/pdf1.htm

4. Unlha32.dll等開発停止、LHA書庫の使用中止呼びかけ

関連記事	● Unlha32.dll等開発停止、LHA書庫の使用中止呼びかけ（スラッシュドットジャパン） http://slashdot.jp/~Claybird/journal/508709

5. Windows のヘルプとサポートセンタに脆弱性

関連記事	● Windowsのヘルプとサポートセンタの脆弱性（CVE-2010-1885）デモ（n） http://n.pentest.jp/?p=810 ● Windows のヘルプとサポートセンタの脆弱性（CVE-2010-1885）に関する検証レポート（NTT データ・セキュリティ株式会社） http://www.nttdata-sec.co.jp/article/vulner/pdf/report20100615.pdf ● Windows のヘルプとサポート センターの脆弱性を悪用する攻撃（Tokyo SOC Report） https://www-950.ibm.com/blogs/tokyo-soc/entry/mshelp0day_20100625?lang=ja

4. 総括

Gumblar やその亜種による Web サイト改ざんやマルウェア感染の被害が継続して報告されています。被害の報告数は減少傾向にありますが、未だ感染したまま放置されている PC や Web サイトが多く残っており、引き続き注意が必要な脅威となっています。

昨今の脅威増加の背景には、収益を生み出すビジネスとして、サイバー犯罪がアンダーグランドで確立されている事が要因として挙げられます。利益が得られる以上、サイバー犯罪者はどのような手段を用いてでもユーザをウイルスに感染させようとします。その感染及び攻撃方法は多岐に渡り、上記サイト改ざん方法とは別に、迷惑メールを利用した方法（スパム行為）、正規サイトに似せた偽サイトを作成しユーザを騙して、個人情報を搾取する方法（フィッシング詐欺）、ウイルスに感染したとの偽のポップアップを表示させ、偽のウイルス対策ソフトを購入させようと脅す方法（スケアウェア）等があります。このようにユーザを感染させると、攻撃者は次にその感染 PC を悪用して、例えば感染 PC が接続されている LAN 内の別のデバイスに感染して感染経路を増やたり（ワームウイルス）、攻撃者が管理する感染 PC 群（ボットネット）を構築し、別のサイバー攻撃を行ったり、感染 PC より搾取したサイト ID やパスワード情報を悪用して正規サイトに不正アクセスして、不正に商品を売買したりします。

このような被害にあわないためにも、各ベンダから提供されている修正プログラムの適用やウイルス対策ソフトのバターンアップデートなどの基本的なセキュリティ対策を継続して確実に行うことが重要です。

株式会社　日立情報システムズ

〒141-8672 東京都品川区大崎 1-2-1

http://www.hitachijoho.com

http://www.shield.ne.jp