株式会社 日立システムズ

SSRC-TR-Vol.14

S.S.R.C.定期
トレンドレポート
Vol.14

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.14

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する予定です。

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 2012 年第 4 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:2012/10/1～2012/12/31

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. 遠隔操作ウイルス事件

関連記事	● なりすまし（遠隔操作）ウイルスによる犯行予告事件をまとめてみた。（piyolog） http://d.hatena.ne.jp/Kango/20121008/1349660951 ● ＩＣＰＯ通じドイツなどに捜査協力要請へ　捜査長期化も（産経ニュース） http://sankei.jp.msn.com/west/west_affairs/news/121014/waf12101409230000-n1.htm ● 真犯人による犯行声明メール全文まとめ（Satoru.net） http://d.hatena.ne.jp/satoru_net/20121016/1350397183 ● 「真犯人」は熟練プログラマー？　ウイルスに改良の痕跡、「一から開発」と犯行声明　（産経ニュース） http://sankei.jp.msn.com/affairs/news/121018/crm12101808510007-n1.htm ● プロの開発者が作成か＝高価な専門ツール使用－証拠隠滅の痕跡も、ＰＣ遠隔操作（時事ドットコム） http://www.jiji.com/jc/zc?k=201210/2012101800773 ● なりすまし事件、警察は「完敗」　発信元にたどり着くのは「ほぼ不可能」（ITmedia） http://www.itmedia.co.jp/news/articles/1210/22/news037.html ● 遠隔操作ウイルスの真犯人を守る「Tor（トーア）」の秘密（ASCII.jp） http://ascii.jp/elem/000/000/737/737738/ ● ウイルス解析、全国から選抜チーム　警察庁（日本経済新聞）

	http://www.nikkei.com/article/DGXNASDG3105K_R01C12A1MM0000/ ● 自民党ＨＰに安倍氏脅迫　育児ブログにも子供殺害予告（産経ニュース） http://sankei.jp.msn.com/affairs/news/121106/crm12110614250016-n1.htm ● パソコン乗っ取り『真犯人』報道機関にメール「私の負けです。自殺します」(J-CAST) http://www.j-cast.com/tv/2012/11/14153798.html ● 遠隔操作真犯人の投稿のまとめ＆分析（Satoru.net） http://d.hatena.ne.jp/satoru_net/20121119 ● 遠隔操作の手口公開　警察庁、ネット利用者協力求め（警視庁） http://www.keishicho.metro.tokyo.jp/jiken/jikenbo/enkaku/enkaku.htm

2. インターネットバンキング利用者の金融情報を狙った新たな犯行手口の発生

関連記事	● インターネットバンキング利用者の金融情報を狙った新たな犯行手口の発生について（警察庁） http://www.npa.go.jp/cyber/warning/h24/121026.pdf ● 【重要】不正にポップアップ画面を表示させてゆうちょダイレクトの情報を盗み取ろうとする犯罪にご注意ください（ゆうちょ銀行） http://www.jp-bank.japanpost.jp/direct/pc/drnews/2012/drnews_id000041.html ● ウイルス感染等によるインターネットバンキングの犯罪にご注意ください（三菱東京 UFJ 銀行） http://www.bk.mufg.jp/info/phishing/ransuu.html ● 【重要】不正にポップアップ画面を表示させてインターネットバンキング(SMBCダイレクト)の情報を盗み取ろうとする犯罪にご注意ください（三井住友銀行） http://www.smbc.co.jp/security/popup.html ● フィッシングサイト(詐欺)にご注意ください（四国ろうきん） http://www.shikoku-rokin.or.jp/important/n121024a.php

3. スマホ情報流出アプリ、５人逮捕…９万人感染

関連記事	● スマホ情報流出アプリ、５人逮捕…９万人感染（YOMIURI ONLINE） http://www.yomiuri.co.jp/net/news/mobile/20121030-OYT8T00950.htm

4. ハッカー集団、世界 100 大学の個人情報など 12 万件を暴露　日本の大学名も

関連記事	● ハッカー集団、世界 100 大学の個人情報など 12 万件を暴露　日本の大学名も（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1210/03/news021.html ● 複数の国内大学への不正アクセス事案をまとめてみた。さらに Ghostshell についても調べてみた。（piyolog） http://d.hatena.ne.jp/Kango/20121006/1349524730

5. 共有ソフトで一斉摘発　「パーフェクトダーク」

関連記事	● ファイル共有ソフト「Perfect Dark」利用事犯に係る一斉集中取締りの実施について（警察庁） http://www.npa.go.jp/cyber/warning/h24/121109.pdf ● 共有ソフトで一斉摘発　「パーフェクトダーク」（47News） http://www.47news.jp/CN/201211/CN2012110901001287.html

6. 三菱重工でもウイルス感染

関連記事	● 当社業務用パソコンのウイルス感染について（三菱重工） http://www.mhi.co.jp/notice/notice_121130.html ● JAXA と三菱重工のウイルス感染インシデントをまとめてみた。（piyolog） http://d.hatena.ne.jp/Kango/20121203/1354549095 ● ハッカー集団が NASA や国防総省などの情報流出を公言、JAXA の名も（ITmedia） http://www.itmedia.co.jp/news/articles/1212/11/news029.html

7. ウェブシャークで 10 万件弱の個人情報が流出

関連記事	● ウェブシャークで 10 万件弱の個人情報が流出、実被害も - 経産省が報告求める (Security NEXT) http://www.security-next.com/034883 ● ウェブシャーク、カード情報 98 件へのアクセスを確認 - 事情説明メールで混乱も (Security NEXT) http://www.security-next.com/034975

8. DVD リッピング禁止、違法 DL に刑罰も～改正著作権法が一部施行

関連記事	● 今日から DVD リッピング禁止、違法 DL に刑罰も～改正著作権法が一部施行 (INTERNET Watch) http://internet.watch.impress.co.jp/docs/news/20121001_561966.html

9. 政府がサイバー攻撃対策に 250 億円

関連記事	● 政府がサイバー攻撃対策に 250 億円 (ITpro) http://itpro.nikkeibp.co.jp/article/COLUMN/20120924/424663/?top_tl1

10. 米国へのサイバー攻撃、3 年間で 2 倍に 調査結果

関連記事	● 米国へのサイバー攻撃、3 年間で 2 倍に 調査結果 (AFP BB News) http://www.afpbb.com/article/disaster-accidents-crime/crime/2906659/9655985?ctm_campaign=txt_topics

11. 新生銀 ATM にスキミング機器、暗証番号も盗撮

関連記事	● 新生銀 ATM にスキミング機器、暗証番号も盗撮 - 海外で 600 万円以上の不正出金（Security NEXT） http://www.security-next.com/036087

12. マスターカードに偽装した日本語のフィッシングサイトが急増

関連記事	● マスターカードに偽装した日本語のフィッシングサイトが急増（ITmedia） http://www.itmedia.co.jp/pcuser/articles/1212/19/news125.html

13. スマホ情報流出で逮捕の５人を釈放、東京地検

関連記事	● スマホ情報流出で逮捕の５人を釈放、東京地検（産経ニュース） http://sankei.jp.msn.com/affairs/news/121121/crm12112101060000-n1.htm

14. ファイル共有…サーバー管理者を初摘発

関連記事	● ファイル共有…サーバー管理者を初摘発　「うたたね」利用で仙台の男　徳島県警（産経ニュース） http://sankei.jp.msn.com/affairs/news/121210/crm12121014190011-n1.htm

15. 読売新聞社員のアドレス悪用される

関連記事	● 読売新聞社員のアドレス悪用される　不正メール５０万通（朝日新聞） http://www.asahi.com/digital/internet/TKY201212110632.html

16. 丸井のＡＴＭでスキミング

関連記事	● 丸井のＡＴＭでスキミング　海外で 550 人分不正利用（日本経済新聞） http://www.nikkei.com/article/DGXNASDG07083_Y2A201C1CC0000/?dg=1

17. POS 端末を狙うマルウェア、40 カ国に感染広げる

関連記事	● POS 端末を狙うマルウェア、40 カ国に感染広げる（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1212/14/news034.html

18. 退職社員らが不正アクセス、情報漏えい

関連記事	● 退職社員らが不正アクセス、情報漏えい　ジブラルタ生命保険（日本経済新聞） http://www.nikkei.com/article/DGXNZO48189210Y2A101C1CC1000/

19. 双子の男子高校生が不正アクセス容疑　他人のパスワードでゲーム

関連記事	● 双子の男子高校生が不正アクセス容疑　他人のパスワードでゲーム（産経ニュース） http://sankei.jp.msn.com/affairs/news/121116/crm12111614460017-n1.htm

20. 中学生３人が不正アクセス容疑

関連記事	● 中学生３人が不正アクセス容疑　北海道警、書類送検（日本経済新聞） http://www.nikkei.com/article/DGXNASDG0100H_R01C12A2000000/

21. フィッシング容疑初摘発　大阪の中３男子書類送検

関連記事	● フィッシング容疑初摘発　大阪の中３男子書類送検（産経ニュース） http://sankei.jp.msn.com/affairs/news/121205/crm12120514200014-n1.htm

22. ウイルス使い、ＩＤ不正取得＝少年２人を書類送検

関連記事	● ウイルス使い、ＩＤ不正取得＝少年２人を書類送検－秋田県警（時事ドットコム） http://www.jiji.com/jc/zc?k=201212/2012121100425

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. ２０１２年８月の世界の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/malware1208.html

2. ２０１２年８月の日本の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/malware1208_jp.html

3. 2012 年９月のウイルス脅威

プレス リリース	● 2012 年９月のウイルス脅威（Dr.WEB） http://news.drweb.co.jp/?i=566&c=1&lng=ja&p=0

4. 高度なスパイ機能のマルウェア「miniFlame」見つかる、標的型攻撃に使用か

関連記事	● 高度なスパイ機能のマルウェア「miniFlame」見つかる、標的型攻撃に使用か（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1210/16/news024.html

5. ２０１２年９月の世界の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/malware1209.html

6. ２０１２年９月の日本の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/malware1209_jp.html

7. 2012 年 10 月のウイルス脅威

プレス リリース	● 2012 年 10 月のウイルス脅威（Dr.WEB） http://news.drweb.co.jp/?i=579&c=1&lng=ja&p=0

8. ２０１２年 10 月の世界の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/malware1210.html

9. ２０１２年 10 月の日本の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/malware1210_jp.html

10. 2012 年 11 月のウイルス脅威

プレス リリース	● 2012 年 11 月のウイルス脅威（Dr.WEB） http://news.drweb.co.jp/?i=589&c=1&lng=ja&p=0

11. データを消去する新手のマルウェア

プレス リリース	● データを消去する新手のマルウェア、イランで発見（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1212/18/news035.html

12. Autorun ワーム、ユーザをだます手口で再び感染急増

関連記事	● Autorun ワーム、ユーザをだます手口で再び感染急増（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1212/03/news024.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＜2012.10.03＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.10.03＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20121001/426546/?ST=security

2. チェックしておきたい脆弱性情報＜2012.10.09＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.10.09＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20121004/427503/?ST=security

3. チェックしておきたい脆弱性情報＜2012.10.23＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.10.23＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20121021/431301/?ST=security

4. チェックしておきたい脆弱性情報＜2012.10.30＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.10.30＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20121029/433141/?ST=security

5. チェックしておきたい脆弱性情報＜2012.11.01＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.11.01＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20121029/433142/?ST=security

6. チェックしておきたい脆弱性情報＜2012.11.06＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.11.06＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20121105/434841/?ST=security

7. チェックしておきたい脆弱性情報＜2012.11.16＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.11.16＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20121113/436943/?ST=security

8. チェックしておきたい脆弱性情報＜2012.11.20＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.11.20＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20121113/436944/?ST=security

9. チェックしておきたい脆弱性情報＜2012.12.04＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.12.04＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20121127/440066/?ST=security

10. チェックしておきたい脆弱性情報＜2012.12.06＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.12.06＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20121203/441589/?ST=security

11. チェックしておきたい脆弱性情報＜2012.12.10＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.12.10＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20121204/441741/?ST=security

12. チェックしておきたい脆弱性情報＜2012.12.25＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.12.25＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20121221/445981/?ST=security

13. チェックしておきたい脆弱性情報＜2012.12.26＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.12.26＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20121221/446024/?ST=security

5. 総括

今期の注目すべきトピックとして、まず遠隔操作ウイルス事件が挙げられます。この事件がどのようなものかというと、ウイルスに感染させられたPCのコントロールが何者かによって奪われ、そのPCを経由してネット掲示板等に脅迫まがいの書き込みをさせられるといった事件です。所謂、「なりすまし」とも称され、情報セキュリティの中でも注目されている手法です。この事件は、報道はもとより、テレビの番組でも特集が組まれ、真犯人と称される人物の動向に日本中が注目しています。この、真犯人が何故こういった行動を起こしたかの動機は、正確には不明ですが、真犯人は「警察・検察を嵌めて、醜態を晒させたかった」といった趣旨の文章を、不特定多数に送り付けています。

この行為によって真犯人の犯行に無意識に加担させられたユーザは複数に上り、それぞれ無実の罪を着せられる等、苦渋の思いをされました。

今後、サイバー犯罪が巧妙になるにつれて、無意識に犯罪に加担させられる可能性も十分にありますので、ネット掲示板等に張られているリンクは不用意にクリックしない等、一歩先を読んだ対策が望まれます。

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