株式会社 日立システムズ

SSRC-TR-Vol.15

# S.S.R.C.定期
# トレンドレポート
# Vol.15


**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.15

## 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 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:2013/1/1～2013/3/31

### 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. 遠隔操作ウイルス事件

| | |
|---|---|
| 関連記事 | ● 遠隔操作ウイルス『新春パズル　～延長戦～』の全文&解法（Satoru.net）<br>http://d.hatena.ne.jp/satoru_net/20130105/1357321422<br>● 遠隔操作、犯人の真意は…ネット上から現実空間に　警察や報道機関を翻弄（msn 産経ニュース）<br>http://sankei.jp.msn.com/affairs/news/130107/crm13010707120001-n1.htm<br>● サイバー犯罪、ハッカーの知恵借りる　警察庁（日本経済新聞）<br>http://www.nikkei.com/article/DGXNASDG24019_U3A120C1CR0000/<br>● 遠隔操作犯人容疑者の 2005 年の犯行予告まとめ(Satoru.net)<br>http://d.hatena.ne.jp/satoru_net/20130210/1360461088<br>● 逮捕の３０歳男、平成１７年にも逮捕　大手レコード会社社長らの殺害予告容疑(産経ニュース)<br>http://sankei.jp.msn.com/affairs/news/130210/crm13021009470005-n1.htm |

#### 2. 韓国同時多発サイバー攻撃

| | |
|---|---|
| 関連記事 | ● 3/20 韓国同時多発サイバー攻撃について（3.20 大乱）(セキュリティはたのしいかね？ Part 2)<br>http://negi.hatenablog.com/entry/2013/03/22/123529<br>● 北のサイバー攻撃、経由地の中国当局「黙認」か（YOMIURI ONLINE）<br>http://www.yomiuri.co.jp/world/news/20130322-OYT1T00471.htm?from=main1 |

| | |
|---|---|
| | ● 韓国サイバー攻撃マルウェア検証（FFRI BLOG）<br>http://www.fourteenforty.jp/blog/2013/03/2013-03-22-1.htm<br>● 韓国でのサイバー攻撃で、リモートの Linux Wiper 見つかる（Symantec）<br>http://www.symantec.com/connect/ja/blogs/linux-wiper<br>● 韓国サイバー攻撃・北、ハッカー数千人養成　正恩氏直轄、手口高度化（IT media）<br>http://www.itmedia.co.jp/news/articles/1303/21/news031.html<br>● 2013 年 3 月に発生した韓国へのサイバー攻撃をまとめてみた。（piyolog）<br>http://d.hatena.ne.jp/Kango/20130323/1363986809<br>● 韓国へのサイバーテロ、論理爆弾の仕組みが判明（WIRED）<br>http://wired.jp/2013/03/26/logic-bomb-south-korea-attack/ |

## 3. 農林水産省がサイバー攻撃被害

| | |
|---|---|
| **関連記事** | ● ＴＰＰ関連の機密文書流出？　農水省へのサイバー攻撃で（msn 産経ニュース）<br>http://sankei.jp.msn.com/affairs/news/130101/crm13010122080004-n1.htm<br>● サイバー攻撃で再調査を指示　農相（日本経済新聞）<br>http://www.nikkei.com/article/DGXNASDG0801D_Y3A100C1CC0000/<br>● 農林水産省の TPP 情報等の窃取を目的にしたと思われるウィルス感染(サイバー攻撃)事案をまとめてみた。（piyolog）<br>http://d.hatena.ne.jp/Kango/20130107/1357582614<br>● 農水省で内部情報流出の疑い　大量のデータ通信を確認（47news）<br>http://www.47news.jp/CN/201301/CN2013011101001522.html<br>● 農水省がサイバー攻撃調査の初会合　「全通信記録を徹底検証」（日本経済新聞）<br>http://www.nikkei.com/article/DGXNASFK17044_X10C13A1000000/ |

## 4. ７６万人もの個人情報を漏洩させた『全国電話帳』が名前を変え『全国共有電話帳』として復活

| | |
|---|---|
| 関連記事 | ● これはヤバイ！ ７６万人もの個人情報を漏洩させた『全国電話帳』が名前を変え『全国共有電話帳』として復活（I believe in Technology）<br>http://reynotch.blog.fc2.com/blog-entry-413.html<br>● 76 万人の個人情報が流出したアプリ 「全国電話帳」作者に聞く“制作の動機”（EX ドロイド）<br>http://exdroid.jp/d/51215/ |

## 5. トルコの認証局、中間 CA 証明書を誤発行

| | |
|---|---|
| 関連記事 | ● トルコの認証局、中間 CA 証明書を誤発行--グーグルや MS、対応を明らかに（Cnet Japan）<br>http://japan.cnet.com/news/service/35026500/ |

## 6. 世界 271 の銀行にハッキングのアルジェリア人逮捕

| | |
|---|---|
| 関連記事 | ● 世界 271 の銀行にハッキングのアルジェリア人逮捕<br>http://japanese.cri.cn/881/2013/01/08/241s203118.htm |

## 7. 四国電力 個人情報ネット流出

| | |
|---|---|
| 関連記事 | ● 委託業者所有パソコンからの個人情報の流出について（四国電力株式会社）<br>http://www.yonden.co.jp/press/re1301/1180955_1968.html |

## 8. 埼玉と茨城の中学生を補導　サイトに不正アクセス容疑

| | |
|---|---|
| 関連記事 | ● 埼玉と茨城の中学生を補導　サイトに不正アクセス容疑（日本経済新聞）<br>http://www.nikkei.com/article/DGXNASDG2901G_Z20C13A1CC0000/ |

## 9. 栃木県の雨量水位観測システムにサイバー攻撃

| | |
|---|---|
| 関連記事 | ● 栃木県の雨量水位観測システムにサイバー攻撃 - データ改ざんが発生（Security NEXT）<br>http://www.security-next.com/036864 |

## 10. New York Times 紙に不正侵入

| | |
|---|---|
| 関連記事 | ● New York Times 紙に不正侵入、攻撃手法で対策の課題も明らかに（IT media）<br>http://www.itmedia.co.jp/enterprise/articles/1302/01/news036.html<br>● ニューヨークタイムズへのサイバー攻撃から学ぶこと（IT pro）<br>http://itpro.nikkeibp.co.jp/article/COLUMN/20130213/456061/?ST=security |

## 11. UPnP に深刻な脆弱性

| | |
|---|---|
| 関連記事 | ● 数千万台の端末に影響か――UPnP に深刻な脆弱性（Computer World）<br>http://www.computerworld.jp/topics/563/206286 |

## 12. ＡＴＭにスキミング装置　首都圏６カ所、１３０口座被害

| | |
|---|---|
| 関連記事 | ● ＡＴＭにスキミング装置　首都圏６カ所、１３０口座被害（ニュースウェブ）<br>http://blog.livedoor.jp/yoshitaka1215/archives/2453126.html |

## 13. EU が新サイバーセキュリティー規則提案へ

| | |
|---|---|
| 関連記事 | ● EU が新サイバーセキュリティー規則提案へ（ウォールストリートジャーナル）<br>http://jp.wsj.com/article/SB10001424127887324261304578284623571415296.html |

## 14. 米エネルギー省にサイバー攻撃

| | |
|---|---|
| 関連記事 | ● 米エネルギー省にサイバー攻撃　職員の個人情報盗まれる（日本経済新聞）<br>http://www.nikkei.com/article/DGXNASGM05023_V00C13A2EB1000/ |

### 15. サイバー攻撃防御へ　内閣情報政策監を新設

| | |
|---|---|
| 関連記事 | ● サイバー攻撃防御へ　内閣情報政策監を新設（産経ニュース）<br>http://sankei.jp.msn.com/politics/news/130205/plc13020501340001-n1.htm |

### 16. 外務省にサイバー攻撃

| | |
|---|---|
| 関連記事 | ● 外務省にサイバー攻撃、「国民の権利が侵害されるおそれ」がある情報など約 20 通流出の疑い(IT pro)<br>http://itpro.nikkeibp.co.jp/article/NEWS/20130206/454501/<br>● 外務省の 2013 年 2 月の情報流出事案をまとめてみた。（piyolog）<br>http://d.hatena.ne.jp/Kango/20130207/1360246175 |

### 17. 米ＦＲＢがハッカー被害

| | |
|---|---|
| 関連記事 | ● 米ＦＲＢがハッカー被害＝銀行幹部の情報流出かーメディア報道（時事ドットコム）<br>http://www.jiji.com/jc/zc?k=201302/2013020600412 |

### 18. 米大統領、サイバー攻撃防衛強化に向けた大統領令に署名

| | |
|---|---|
| 関連記事 | ● 米大統領、サイバー攻撃防衛強化に向けた大統領令に署名（ロイター）<br>http://jp.reuters.com/article/worldNews/idJPTYE91C02820130213 |

### 19. 旧朝銀系信組が流出隠蔽

| | |
|---|---|
| 関連記事 | ● 旧朝銀系信組が流出隠蔽　顧客情報数万件　１８年確認、金融庁公表せず（産経ニュース）<br>http://sankei.jp.msn.com/affairs/news/130221/crm13022107250001-n1.htm |

### 20. サイバー攻撃の「手口」集約　経産省、データベース整備

| | |
|---|---|
| 関連記事 | ● サイバー攻撃の「手口」集約　経産省、データベース整備（Sankei Biz）<br>http://www.sankeibiz.jp/macro/news/130225/mca1302250815007-n1.htm |

### 21. 米ＮＢＣサイトにサイバー攻撃か

| | |
|---|---|
| 関連記事 | ● 米ＮＢＣサイトにサイバー攻撃か、フェイスブックはアクセス遮断（ロイター）<br>http://jp.reuters.com/article/topNews/idJPTYE91L00620130222 |

### 22. AFP ツイッターでハッキング、シリア政府支持派が犯行声明

| | |
|---|---|
| 関連記事 | ● AFP ツイッターでハッキング、シリア政府支持派が犯行声明（AFP BB News）<br>http://www.afpbb.com/article/environment-science-it/it/2931417/10360865 |

### 23. 企業ＨＰから情報漏えい　一部投資家、売買で利益

| | |
|---|---|
| 関連記事 | ● 企業ＨＰから情報漏えい　一部投資家、売買で利益（産経ニュース）<br>http://sankei.jp.msn.com/affairs/news/130314/crm13031410140002-n1.htm |

### 24. 米政府機関の脆弱性データベースがマルウェア感染でダウン

| | |
|---|---|
| 関連記事 | ● 米政府機関の脆弱性データベースがマルウェア感染でダウン（IT media）<br>http://www.itmedia.co.jp/enterprise/articles/1303/15/news035.html |

### 25. JINS の不正アクセスによるカード情報流出、7 件の不正利用を確認

| | |
|---|---|
| 関連記事 | 不正アクセス（JINS オンラインショップ）に関する調査報告（中間報告）（JINS）<br>http://www.jins-jp.com/info.pdf<br>● 不正アクセス（JINS オンラインショップ）に関する調査結果（最終報告）（JINS）<br>http://www.jins-jp.com/info.html |

## 26. 中２男子を書類送検　「アメーバピグ」不正アクセス容疑

| | |
|---|---|
| 関連記事 | ● 中２男子を書類送検　「アメーバピグ」不正アクセス容疑（スポニチ）<br>http://www.sponichi.co.jp/society/news/2013/03/19/kiji/K20130319005429850.html |

## 27. Kaspersky、Android を狙った初の標的型攻撃発生を報告

| | |
|---|---|
| 関連記事 | ● Kaspersky、Android を狙った初の標的型攻撃発生を報告（IT media）<br>http://www.itmedia.co.jp/enterprise/articles/1303/27/news034.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. ２０１２年１１月の世界のマルウェアランキングを公開

| | |
|---|---|
| プレス<br>リリース | ● マルウェアランキング（世界のランキング）（ESET）<br>http://canon-its.jp/product/eset/topics/malware1211.html |

### 2. ２０１２年１１月の日本のマルウェアランキングを公開

| | |
|---|---|
| プレス<br>リリース | ● マルウェアランキング（日本のランキング）（ESET）<br>http://canon-its.jp/product/eset/topics/malware1211_jp.html |

### 3. 新コンピューターウイルス「レッド・オクトーバー」を特定、露社

| | |
|---|---|
| 関連記事 | ● 新コンピューターウイルス「レッド・オクトーバー」を特定、露社（AFP BB News）<br>http://www.afpbb.com/article/environment-science-it/it/2920662/10105984<br>● 大規模サイバースパイ活動「Red October」、Java エクスプロイトも使用（Computer World）<br>http://www.computerworld.jp/topics/563/206122<br>● カスペルスキー研究所がサイバー・スパイ網を摘発（ロシア NOW）<br>http://roshianow.jp/science/2013/01/20/40961.html |

### 4. 中国で Android マルウェアが流行、過去最大のボットネットを形成か

| | |
|---|---|
| 関連記事 | ● 中国で Android マルウェアが流行、過去最大のボットネットを形成か（IT pro）<br>http://www.itmedia.co.jp/enterprise/articles/1301/25/news085.html |

## 5. 2012 年のウイルスレビュー

| | |
|---|---|
| プレス<br>リリース | ● 2012 年のウイルスレビュー（DR.WEB）<br>http://news.drweb.co.jp/?i=603&c=1&lng=ja&p=0 |

## 6. ２０１２年１２月の世界のマルウェアランキングを公開

| | |
|---|---|
| プレス<br>リリース | ● マルウェアランキング（世界のランキング）（ESET）<br>http://canon-its.jp/product/eset/topics/malware1212.html |

## 7. ２０１２年１２月の日本のマルウェアランキングを公開

| | |
|---|---|
| プレス<br>リリース | ● マルウェアランキング（日本のランキング）（ESET）<br>http://canon-its.jp/product/eset/topics/malware1212_jp.html |

## 8. 2013 年１月のウイルス脅威

| | |
|---|---|
| プレス<br>リリース | ● 2013 年１月のウイルス脅威（DR.WEB）<br>http://news.drweb.co.jp/?i=606&c=1&lng=ja&p=0 |

## 9. ２０１３年１月の世界のマルウェアランキングを公開

| | |
|---|---|
| プレス<br>リリース | ● マルウェアランキング（世界のランキング）（ESET）<br>http://canon-its.jp/product/eset/topics/malware1301.html |

## 10. ２０１３年１月の日本のマルウェアランキングを公開

| | |
|---|---|
| プレス<br>リリース | ● マルウェアランキング（日本のランキング）（ESET）<br>http://canon-its.jp/product/eset/topics/malware1301_jp.html |

## 11. 2013 年 2 月のウイルス脅威

| | |
|---|---|
| プレス<br>リリース | ● 2013 年 2 月のウイルス脅威（DR.WEB）<br>http://news.drweb.co.jp/?i=612&c=1&lng=ja&p=0 |

## 12. DHL を装ったマルウェアの登場

| | |
|---|---|
| プレス<br>リリース | ● DHL を装ったマルウェアの登場（SOPHOS）<br>http://www.sophos.com/ja-jp/press-office/press-releases/2013/03/ns-a-dhl-delivery-which-is-nothing-but-malware.aspx |

### 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＜2013.01.11＞

| | |
|---|---|
| プレス<br>リリース | ● チェックしておきたい脆弱性情報＜2013.01.11＞<br>http://itpro.nikkeibp.co.jp/article/COLUMN/20130109/448526/?ST=security |

2. チェックしておきたい脆弱性情報＜2013.01.15＞

| | |
|---|---|
| プレス<br>リリース | ● チェックしておきたい脆弱性情報＜2013.01.15＞<br>http://itpro.nikkeibp.co.jp/article/COLUMN/20130109/448527/?ST=security |

3. チェックしておきたい脆弱性情報＜2013.01.22＞

| | |
|---|---|
| プレス<br>リリース | ● チェックしておきたい脆弱性情報＜2013.01.22＞<br>http://itpro.nikkeibp.co.jp/article/COLUMN/20130121/450629/?ST=security |

4. チェックしておきたい脆弱性情報＜2013.01.31＞

| | |
|---|---|
| プレス<br>リリース | ● チェックしておきたい脆弱性情報＜2013.01.31＞<br>http://itpro.nikkeibp.co.jp/article/COLUMN/20130129/452665/?ST=security |

5. チェックしておきたい脆弱性情報＜2013.02.07＞

| | |
|---|---|
| プレス<br>リリース | ● チェックしておきたい脆弱性情報＜2013.02.07＞<br>http://itpro.nikkeibp.co.jp/article/COLUMN/20130206/454563/?ST=security |

6. チェックしておきたい脆弱性情報＜2013.02.12＞

| | |
|---|---|
| プレス<br>リリース | ● チェックしておきたい脆弱性情報＜2013.02.12＞<br>http://itpro.nikkeibp.co.jp/article/COLUMN/20130207/454961/?ST=security |

7. チェックしておきたい脆弱性情報＜2013.02.19＞

| | |
|---|---|
| プレス<br>リリース | ● チェックしておきたい脆弱性情報＜2013.02.19＞<br>http://itpro.nikkeibp.co.jp/article/COLUMN/20130218/456663/?ST=security |

8. チェックしておきたい脆弱性情報＜2013.03.11＞

| | |
|---|---|
| プレス<br>リリース | ● チェックしておきたい脆弱性情報＜2013.03.11＞<br>http://itpro.nikkeibp.co.jp/article/COLUMN/20130307/461501/?ST=security |

9. チェックしておきたい脆弱性情報＜2013.03.12＞

| | |
|---|---|
| プレス<br>リリース | ● チェックしておきたい脆弱性情報＜2013.03.12＞<br>http://itpro.nikkeibp.co.jp/article/COLUMN/20130310/462082/?ST=security |

10. チェックしておきたい脆弱性情報＜2013.03.13＞

| | |
|---|---|
| プレス<br>リリース | ● チェックしておきたい脆弱性情報＜2013.03.13＞<br>http://itpro.nikkeibp.co.jp/article/COLUMN/20130310/462083/?ST=security |



11. チェックしておきたい脆弱性情報＜2013.03.21＞

| | |
|---|---|
| プレス<br>リリース | ● チェックしておきたい脆弱性情報＜2013.03.21＞<br>http://itpro.nikkeibp.co.jp/article/COLUMN/20130319/464321/?ST=security |

12. チェックしておきたい脆弱性情報＜2013.03.26＞

| | |
|---|---|
| プレス<br>リリース | ● チェックしておきたい脆弱性情報＜2013.03.26＞<br>http://itpro.nikkeibp.co.jp/article/COLUMN/20130325/465562/?ST=security |

## 5. 総括

前回より注目トピックとなっていた遠隔操作ウイルス事件の容疑者と見られる人物が逮捕されました。情報によると、容疑者は、以前にネット掲示板を通じて仙台市の女児の殺害予告を書き込んだとして、宮城県警に 17 年 10 月に脅迫容疑で逮捕、同年 11 月には、大手レコード会社社長に対する殺害予告もしたとして再逮捕されていました。本レポート執筆時点で、容疑者は容疑を否認していますが、勾留は続いています。今後も、本事件の経過が注目されます。

また、日本国内省庁へのサイバー攻撃、世界を股にかけ、271 行もの銀行にハッキングしていたハッカーの逮捕、大規模サイバースパイ活動「Red October」の発見、韓国への同時多発サイバー攻撃等、今期も注目すべきトピックが複数明らかになりました。サイバースパイやサイバー戦争等のキーワードが既に一般化される中、アンダーグラウンドハッカーらの活動も活発になっています。ハッカーは、その活動媒体を世間の動向に合わせて変えてきます。昨今ではスマートフォンを標的とした攻撃も明らかになっていますので、ネットライフの利便性の増加と比例したセキュリティ対策が必要になってきているのかもしれません。

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