株式会社 日立システムズ

SSRC-TR-Vol.10

S.S.R.C.定期
トレンドレポート
Vol.10

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.10

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 2011 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:2011/10/1～2011/12/31

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. ハッカー集団 Anonymous によるハッキング事例

関連記事	● 米捜査機関の Web サイトに不正アクセス、捜査員らの個人情報が暴露(IT pro) http://www.itmedia.co.jp/news/articles/1112/13/news021.html ● Anonymous claims new Monsanto-related hack(SC MAGAZINE) http://www.scmagazine.com/anonymous-claims-new-monsanto-related-hack/article/218504/ ● 米調査機関サイトに侵入　個人情報でXマス寄付(47NEWS) http://www.47news.jp/CN/201112/CN2011122601000964.html ● ハッカー集団が情報機関の顧客リストを暴露、日本の大手企業名も(IT media) http://www.itmedia.co.jp/enterprise/articles/1112/27/news013.html ● Anonymous による NYSE への DDoS 攻撃 (IIJ) https://sect.iij.ad.jp/d/2011/10/127533.html ● アノニマスが米セントルイス市長サイトに侵入か、反格差デモ支持(REUTERS) http://jp.reuters.com/article/worldNews/idJPJAPAN-24099720111110

2. 衆院にサイバー攻撃　議員のパスワード盗まれる

関連記事	● 衆院サイバー攻撃“ならず者国家”の仕業か…米国は“中国”厳戒(zakzak) http://www.zakzak.co.jp/society/foreign/news/20111025/frn1110251558000-n1.htm ● ３議員のＰＣウイルス感染　サイバー攻撃、確認急ぐ(47news) http://www.47news.jp/CN/201110/CN2011102501000295.html ● 全衆院議員のパスワード盗難か　管理者権限で操作(朝日新聞デジタル) http://www.asahi.com/national/update/1026/TKY201110250740.html ● 全議員のメール盗み見可能に　サイバー攻撃で衆院調査(47news) http://www.47news.jp/CN/201111/CN2011111401000856.html ● パスワード変えた議員は半数以下　衆院サイバー攻撃(朝日新聞デジタル) http://www.asahi.com/national/update/1117/TKY201111170163.html

3. １０台超す参院ＰＣに攻撃か　不正サイトに接続試みる

関連記事	● １０台超す参院ＰＣに攻撃か　不正サイトに接続試みる(朝日新聞デジタル) http://www.asahi.com/digital/internet/TKY201111100674.html ● 全参院議員ＩＤ流出か＝サーバ２台感染－事務局発表(時事ドットコム) http://www.jiji.com/jc/zc?k=201111/2011112100766

4. 外務省にサイバー攻撃　大使館も、一部感染

関連記事	● 外務省にサイバー攻撃　大使館も、一部感染(47news) http://www.47news.jp/CN/201110/CN2011102601000420.html

5. 総務省の複数 PC がウイルス感染

プレスリリース	● 総務省におけるウイルス感染事案(総務省) http://www.soumu.go.jp/menu_news/s-news/01kanbo05_02000040.html

6. 国土地理院にもサイバー攻撃

関連記事	● サーバに対する不正アクセスについて(国土地理院) http://www.gsi.go.jp/johosystem/johosystem65000.html

7. 厚労省サーバがウイルスに感染

関連記事	● 厚労省サーバがウイルスに感染　一時ネット接続を停止(msn 産経ニュース) http://sankei.jp.msn.com/affairs/news/111130/crm11113011290006-n1.htm

8. サイバー攻撃、被害相次ぐ　都道府県の情報システム

関連記事	● サイバー攻撃、被害相次ぐ　都道府県の情報システム(47NEWS) http://www.47news.jp/CN/201111/CN2011110201000452.html

9. 文科省や国土地理院でウェブサイト改ざんが発生

関連記事	● 文科省や国土地理院でウェブサイト改ざんが発生(Security NEXT) http://www.security-next.com/026833

10. ソニー、ネットワークに 9 万件超える不正アクセス

関連記事	● PlayStation®Network 、 “Sony Entertainment Network” 、 Sony Online Entertainment のユーザーアカウントへの第三者の“なりすまし”による不正なサインインの試行について(ソニー株式会社) http://www.sony.co.jp/SonyInfo/News/Press/201110/11-1012/

11. 銀行の第二認証情報を詐取するフィッシング

プレス リリース	● 【注意喚起】銀行の第二認証情報を詐取するフィッシングにご注意ください(2011/10/18)(フィッシング対策協議会) http://www.antiphishing.jp/news/alert/20111018.html

12. 国内の偽造キャッシュカード、盗難キャッシュカードなどを悪用したインターネットバンキング犯罪による被害発生状況および補償状況

プレスリリース	● 偽造キャッシュカード等による被害発生等の状況について(金融庁) http://www.fsa.go.jp/news/20/ginkou/20090318-2.html

13. 大阪市水道局、マンションの暗証番号など個人情報流出を発表

プレスリリース	● 民間共同住宅におけるお客さまデータ等の流出について(水道局) http://www.city.osaka.lg.jp/suido/page/0000143890.html

14. Facebook のパスワードが 1 万件以上流出の恐れ、真偽は未確認

関連記事	● Over 10,000 Facebook account details hacked and published(countermeasures) http://countermeasures.trendmicro.eu/over-10000-facebook-account-details-hacked-and-published/

15. 戦闘機資料がサーバ移動　三菱重工へのサイバー攻撃

関連記事	● 戦闘機資料がサーバー移動　三菱重工へのサイバー攻撃(msn 産経ニュース) http://sankei.jp.msn.com/affairs/news/111024/crm11102414450013-n1.htm

16. 職員室のＰＣから児童ポルノ公開容疑　北海道の小学教諭

関連記事	● 職員室のＰＣから児童ポルノ公開容疑　北海道の小学教諭(朝日新聞デジタル) http://www.asahi.com/edu/news/HOK201110240001.html

17. Nasdaq のコンピュータシステムがハッキング被害に

関連記事	● Hackers spy on corporate directors via Nasdaq(Dispatch) http://www.dispatch.com/content/stories/business/2011/10/21/hackers-spy-on-corporate-directors-via-nasdaq.html

18. 仮装空間「アメーバピグ」で詐欺や盗み、子供ら被害

関連記事	● 【アメーバピグ】被害(オンラインゲーム詐欺情報局) http://gamesagi.com/board_g.cgi?mode=res&no=78

19. サイバー攻撃、２４時間で監視　防衛省が企業に義務付け

関連記事	● サイバー攻撃、２４時間で監視　防衛省が企業に義務付け(47NEWS) http://www.47news.jp/CN/201111/CN2011111401000939.html

20. 韓国の「メイプルストーリー」会員情報 1320 万件が流出

プレス リリース	● ネクソン子会社における個人情報漏洩について(NEXON) http://www.nexon.co.jp/jp/content/Support/Notice.aspx?no=119794

21. 警察庁、著作権法違反容疑での一斉摘発を実施

プレス リリース	● 全国 47 都道府県警察によるファイル共有ソフト等を使用した著作権法違反事件の一斉集中取締りの実施について(警察庁) http://www.npa.go.jp/cyber/warning/h23/111201_1.pdf

22. フリー無線 LAN「ConnectFree」は個人情報収集機か？

プレス リリース	● お客様情報の取得に関するお詫びとご説明(コネクトフリー株式会社) http://connectfree.jp/_p/connfree/files/CF_12_05.html

23. 違法ダウンロード処罰へ法案

関連記事	● 違法ダウンロード処罰へ法案＝自公(時事ドットコム) http://www.jiji.com/jc/zc?k=201112/2011120701034

24. オランダの CA 認証局である Gemnet がハッキング被害に

関連記事	● Dutch certificate authority reportedly hacked after access gained through PHP MyAdmin(SC MAGAZINE) http://www.scmagazineuk.com/dutch-certificate-authority-reportedly-hacked-after-access-gained-through-php-myadmin/article/218672/

25. Share 違法利用者に警告メール、権利者団体などが 12 月から

プレス リリース	● Share を悪用して著作権侵害を行っているユーザに、啓発メール送付を開始(ファイル共有ソフトを悪用した著作権侵害対策協議会) http://www.ccif-j.jp/news_20111213.html

26. 音楽ファイルの不正アップローダー9 名の氏名等の開示を命じる判決

プレス リリース	● 音楽ファイルの不正アップローダー9 名の氏名等の開示を命じる判決下る(一般社団法人　日本レコード協会) http://www.riaj.or.jp/release/2011/pr111214.html

27. 北朝鮮総書記死去のニュースに便乗した標的型メール

関連記事	● 北朝鮮総書記死去のニュースに便乗した標的型メールを確認(IBM Tokyo SOC Report) https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/targeted_attack_20111220?lang=ja ● 韓国、金正日総書記の死亡でサイバー危機注意警報発令(ZDNet Japan) http://japan.zdnet.com/security/analysis/35012230/ ● 金正日氏死去に便乗したスパムメールを確認。脆弱性の悪用も(Trend Labs Security Blog) http://blog.trendmicro.co.jp/archives/4682

28. Winny 開発者、金子勇氏の無罪が確定

関連記事	● Winny 開発者、金子勇氏の無罪が確定(マイナビニュース) http://news.mynavi.jp/news/2011/12/21/054/

29. 「アメーバ」に不正アクセス　５万人が退会状態

関連記事	● 「アメーバ」に不正アクセス　５万人が退会状態(47NEWS) http://www.47news.jp/CN/201112/CN2011122501001674.html

30. 史上最大の個人情報流出事件＝流出件数は１億件に迫る―中国

関連記事	● 史上最大の個人情報流出事件＝流出件数は 1 億件に迫る―中国(KINBRICKS NOW) http://kinbricksnow.com/archives/51764388.html

3.2. 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. 2011 年 10 月のウイルス脅威

プレス リリース	● 2011 年 10 月のウイルス脅威(Dr.WEB) http://news.drweb.co.jp/?i=444&c=1&lng=ja&p=0

2. 2011 年 11 月のウイルス脅威

プレス リリース	● 2011 年 11 月のウイルス脅威(Dr.WEB) http://news.drweb.co.jp/?i=459&c=1&lng=ja&p=0

3. PDF ファイルにより感染する新たなマルウェア

プレス リリース	● New wave of 'PDF malware' seen(GMA News) http://www.gmanetwork.com/news/story/238310/scitech/new-wave-of-pdf-malware-seen

4. ZeuS を仕掛ける「バンキングスパム」

プレス リリース	● ZeuS を仕掛ける「バンキングスパム」が欧州で拡散中(G DATA) http://sv20.wadax.ne.jp/~gdata-co-jp/press/archives/2011/11/zeus.htm

5. Android マーケットに 30 個以上のマルウェア

プレス リリース	● Android マーケットに 30 個以上のマルウェア(Dr.WEB) http://news.drweb.co.jp/?i=454&c=1&lng=ja&p=0

3.3. 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. チェックしておきたい脆弱性情報＜2011.10.03＞

プレス リリース	● チェックしておきたい脆弱性情報＜2011.10.03＞(IT pro) http://itpro.nikkeibp.co.jp/article/COLUMN/20111003/370021/?rt=nocnt

2. チェックしておきたい脆弱性情報＜2011.10.12＞

プレス リリース	● チェックしておきたい脆弱性情報＜2011.10.12＞(IT pro) http://itpro.nikkeibp.co.jp/article/COLUMN/20111010/370421/

3. チェックしておきたい脆弱性情報＜2011.10.18＞

プレス リリース	● チェックしておきたい脆弱性情報＜2011.10.18＞(IT pro) http://itpro.nikkeibp.co.jp/article/COLUMN/20111017/370861/

4. チェックしておきたい脆弱性情報＜2011.10.25＞

プレス リリース	● チェックしておきたい脆弱性情報＜2011.10.25＞(IT pro) http://itpro.nikkeibp.co.jp/article/COLUMN/20111024/371259/

5. チェックしておきたい脆弱性情報＜2011.11.08＞

プレス リリース	● チェックしておきたい脆弱性情報＜2011.11.08＞(IT pro) http://itpro.nikkeibp.co.jp/article/COLUMN/20111106/372541/

6. チェックしておきたい脆弱性情報＜2011.11.15＞

プレス リリース	● チェックしておきたい脆弱性情報＜2011.11.15＞(IT pro) http://itpro.nikkeibp.co.jp/article/COLUMN/20111114/374446/

7. チェックしておきたい脆弱性情報＜2011.11.24＞

プレス リリース	● チェックしておきたい脆弱性情報＜2011.11.24＞(IT pro) http://itpro.nikkeibp.co.jp/article/COLUMN/20111122/374804/

8. チェックしておきたい脆弱性情報＜2011.11.29＞

プレス リリース	● チェックしておきたい脆弱性情報＜2011.11.29＞(IT pro) http://itpro.nikkeibp.co.jp/article/COLUMN/20111128/375123/

9. チェックしておきたい脆弱性情報＜2011.12.12＞

プレス リリース	● チェックしておきたい脆弱性情報＜2011.12.12＞ (IT pro) http://itpro.nikkeibp.co.jp/article/COLUMN/20111205/375560/

10. チェックしておきたい脆弱性情報＜2011.12.20＞

プレス リリース	● チェックしておきたい脆弱性情報＜2011.12.20＞ (IT pro) http://itpro.nikkeibp.co.jp/article/COLUMN/20111219/376900/

4. 総括

衆議院のネットワークなど、国内省庁をターゲットにした標的型メール攻撃が相次いで確認されました。この攻撃は、メールの添付ファイルを開くことで感染するタイプの攻撃で、標的に対してメールを開かせるような巧妙な細工がされていることが明らかになっています。中でも、3 月に発生した東日本大震災に関連した内容を騙るものがあり、攻撃者が日本国内を意図的に標的にしていたということが窺えます。この攻撃に対し、システム上での対策はさることながら、送信者も標的が騙されるようなアドレスになりすましている可能性もあることから、一番の対策方法は、標的となるユーザのセキュリティ意識の高さが最も有効となるという点が、昨今の情報セキュリティの重要性の高さを感じさせます。

ハッカー集団 Anonymous の台頭など、2012 年に向けて、サイバー攻撃が国家や企業にとって最もクリティカルな攻撃方法となりつつある今、情報セキュリティ対策が前提となった企業運営やネットライフが望まれます。

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.hitachijoho.com

http://www.shield.ne.jp