株式会社 日立システムズ

SSRC-TR-Vol.11

S.S.R.C.定期
トレンドレポート
Vol.11

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.11

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 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:2012/1/1～2012/3/31

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. 防衛省が対サイバー兵器、攻撃を逆探知し無力化

関連記事	● 防衛省が対サイバー兵器を開発中（スラッシュドットジャパン） http://slashdot.jp/story/12/01/01/1326245/%E9%98%B2%E8%A1%9B%E7%9C%81%E3%81%8C%E5%AF%BE%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E5%85%B5%E5%99%A8%E3%82%92%E9%96%8B%E7%99%BA%E4%B8%AD

2. 苦情寄せた個人の情報、閲覧可能状態に

関連記事	● 苦情寄せた個人の情報、閲覧可能状態に　岐阜県弁護士会(朝日新聞デジタル) http://www.asahi.com/digital/internet/NGY201112280002.html ● 個人情報流出は５７７人分　弁護士のネット掲示板(朝日新聞デジタル) http://www.asahi.com/national/update/0206/TKY201202060512.html

3. 文科省サイトから個人情報流出

関連記事	● 文科省サイトから個人情報流出 中国からサイバー攻撃か(サイエンスポータル) http://scienceportal.jp/news/daily/1201/1201042.html

4. 中国がサイバー戦争への備えを強化、「国民皆兵」体制の確立へ

関連記事	● 中国がサイバー戦争への備えを強化、「国民皆兵」体制の確立へ(レコードチャイナ) http://www.recordchina.co.jp/group.php?groupid=57553

5. 北の外貨稼ぎ、ハッカー派遣など手段多様化

関連記事	● 北の外貨稼ぎ、ハッカー派遣など手段多様化(YOMIURI ONLINE) http://www.yomiuri.co.jp/world/news/20120105-OYT1T00148.htm

6. 「Norton AntiVirus」のソースコードが流出？

関連記事	● Symantec Confirms Norton AV Source Code Exposed(infosec ISLAND) http://infosecisland.com/blogview/19200-Symantec-Confirms-Source-Norton-AV-Code-Exposed.html

7. JAXA の PC がウイルスに感染－物質補給機の情報など漏洩の可能性

プレスリリース	● JAXA におけるコンピュータウイルス感染の発生について(宇宙航空研究開発機構) http://www.jaxa.jp/press/2012/01/20120113_security_j.html ● JAXA がウイルス感染事件の調査結果を報告、機密情報の漏えいは認められず(ITmedia) http://www.itmedia.co.jp/news/articles/1203/27/news062.html

8. サイバー攻撃で２６０人情報流出…北九州市立大

関連記事	● サイバー攻撃で２６０人情報流出…北九州市立大(YOMIURI ONLINE) http://www.yomiuri.co.jp/kyoiku/news/20120113-OYT8T00364.htm?from=os4

9. 工場制御システムがウイルス感染

関連記事	● 工場制御システムがウイルス感染…操業停止も(YOMIURI ONLINE) http://www.yomiuri.co.jp/net/news/20120123-OYT8T00693.htm

10. サイバー攻撃：6 万人対策訓練　霞が関職員、感染 1 割

関連記事	● サイバー攻撃：6 万人対策訓練　霞が関職員、感染 1 割（ITpro） http://itpro.nikkeibp.co.jp/article/COLUMN/20120131/379846/

11. サイバー部隊、反撃可能　自衛隊、１００人態勢

関連記事	● サイバー部隊、反撃可能　自衛隊、１００人態勢(msn 産経ニュース) http://sankei.jp.msn.com/politics/news/120121/plc12012101310000-n1.htm

12. ウイルス作成容疑で初摘発＝無職男を逮捕

関連記事	● ウイルス作成容疑で初摘発＝２８歳無職男を逮捕－大阪府警(時事ドットコム) http://www.jiji.com/jc/zc?k=201201/2012012600464

13. サイバー攻撃で情報流出　化粧品通販１４９３人分

関連記事	● サイバー攻撃で情報流出　化粧品通販１４９３人分(msn 産経ニュース) http://sankei.jp.msn.com/affairs/news/120127/crm12012712030006-n1.htm

14. 農水省に標的型メール、情報漏洩はなし

関連記事	● 農水省に標的型メール、情報漏洩はなし(msn 産経ニュース) http://sankei.jp.msn.com/affairs/news/120202/crm12020220210019-n1.htm

15. 動画サイトで感染１００万人超　京都府警、詐欺容疑で捜査へ

関連記事	● 動画サイトで感染１００万人超　京都府警、詐欺容疑で捜査へ(47NEWS) http://www.47news.jp/CN/201202/CN2012020801002119.html

16. １７万人分の個人情報流出　妊娠・育児サイト

プレス リリース	● 不正アクセスによる会員情報漏えいに対するお詫びとご報告(ベビカム) http://blog.babycome.ne.jp/news.php

17. サイバー犯罪、過去最多　前年比倍増２４２件摘発

関連記事	● サイバー犯罪、過去最多　前年比倍増２４２件摘発(千葉日報ウェブ) http://www.chibanippo.co.jp/c/news/national/68853

18. 「2010 年度 国内における情報セキュリティ事象被害状況調査」報告書を公開

プレス リリース	● 「2010 年度 国内における情報セキュリティ事象被害状況調査」報告書について(IPA) http://www.ipa.go.jp/security/fy22/reports/isec-survey/index.html

19. サイバーインテリジェンスに係る最近の情勢

プレス リリース	● サイバーインテリジェンスに係る最近の情勢(警察庁) http://www.npa.go.jp/keibi/biki3/240301kouhou.pdf

20. 不正ログイン、４％が侵入　警察庁調査、実態把握へ

関連記事	● 不正ログイン、４％が侵入　警察庁調査、実態把握へ(朝日新聞デジタル) http://www.asahi.com/digital/internet/TKY201203100191.html

21. サイバー攻撃の防御力検証施設、宮城に設置へ

関連記事	● サイバー攻撃の防御力検証施設、宮城に設置へ(YOMIURI ONLINE) http://www.yomiuri.co.jp/net/news/20120319-OYT8T00475.htm

22. イカタコウイルス作成者、二審も実刑判決　東京高裁

関連記事	● イカタコウイルス作成者、二審も実刑判決　東京高裁(朝日新聞デジタル) http://www.asahi.com/digital/internet/TKY201203260459.html

23. 感染研ホームページが不正アクセス被害に

プレス リリース	● 感染研ホームページへの不正アクセスについて(国立感染症研究所) http://www0.nih.go.jp/niid/misc/announcement120327.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. 2011 年 12 月のウイルス脅威

プレス リリース	● 2011 年 12 月のウイルス脅威(Dr.WEB) http://news.drweb.co.jp/?i=478&c=1&lng=ja&p=0

2. 2012 年 1 月のウイルス脅威

プレス リリース	● 2012 年 1 月のウイルス脅威(Dr.WEB) http://news.drweb.co.jp/?i=485&c=1&lng=ja&p=0

3. 2011 年のウイルスレビュー

プレス リリース	● 2011 年のウイルスレビュー(Dr.WEB) http://news.drweb.co.jp/?i=484&c=1&lng=ja&p=0

4. 2012 年 2 月のウイルス脅威

プレス リリース	● 2012 年 2 月のウイルス脅威(Dr.WEB) http://news.drweb.co.jp/?i=502&c=1&lng=ja&p=0

5. Android Market にマルウェアが混在 - 感染機器は最大 500 万台

関連記事	● Android Market にマルウェアが混在 - 感染機器は最大 500 万台(マイナビニュース) http://news.mynavi.jp/news/2012/01/31/051/index.html

6. Web カメラでユーザーを盗撮する新たなバックドア

関連記事	● Web カメラでユーザーを盗撮する新たなバックドア(Dr.WEB) http://news.drweb.co.jp/?i=489&c=1&lng=ja&p=0

7. 告発サイトの Cryptome に不正コード、ユーザーがマルウェア感染の恐れ

関連記事	● 告発サイトの Cryptome に不正コード、ユーザーがマルウェア感染の恐れ (ITmedia) http://www.itmedia.co.jp/enterprise/articles/1202/15/news092.html

8. Mac OS X をターゲットにした「Flashback」マルウェアが出現

関連記事	● Flashback Mac Trojan Horse Infections Increasing with New Variant(intego) http://www.intego.com/mac-security-blog/flashback-mac-trojan-horse-infections-increasing-with-new-variant/ ● Flashback Mac Malware Uses Twitter as Command and Control Center(intego) http://www.intego.com/mac-security-blog/flashback-mac-malware-uses-twitter-as-command-and-control-center/

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＜2012.01.10＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.01.10＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20120106/377867/?ST=security

2. チェックしておきたい脆弱性情報＜2012.01.11＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.01.11＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20120106/377868/?ST=security

3. チェックしておきたい脆弱性情報＜2012.01.12＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.01.12＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20120106/377869/?ST=security

4. チェックしておきたい脆弱性情報＜2012.01.17＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.01.17＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20120116/378534/?ST=security

5. チェックしておきたい脆弱性情報＜2012.01.25＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.01.25＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20120124/379165/?ST=security

6. チェックしておきたい脆弱性情報＜2012.02.14＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.02.14＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20120213/381125/?ST=security

7. チェックしておきたい脆弱性情報＜2012.02.22＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.02.22＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20120221/382223/?ST=security

8. チェックしておきたい脆弱性情報＜2012.02.28＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.02.28＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20120221/382224/?ST=security

9. チェックしておきたい脆弱性情報＜2012.03.07＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.03.07＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20120305/384624/?ST=security

10. チェックしておきたい脆弱性情報＜2012.03.14＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.03.14＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20120312/385981/?ST=security

11. チェックしておきたい脆弱性情報＜2012.03.19＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.03.19＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20120312/385982/?ST=security

12. チェックしておきたい脆弱性情報＜2012.03.28＞

プレス リリース	● チェックしておきたい脆弱性情報＜2012.03.28＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20120327/388053/?ST=security

5. 総括

2012 年に入り、サイバー攻撃の脅威が顕著化しています。千葉県警による調査によると、昨年のサイバー犯罪における検挙件数が、前年比およそ 2 倍となる 242 件で、過去最多になっていた[17]事が明らかになった事例があるように、今や地方自治体レベルにおいても注目されるべき事案となっています。

また、制御用システムへのサイバー攻撃対策が注目されています。工場等の制御系システムは、スタンドアローンや閉じたネットワークで運用されることが多く、特殊なシステムを採用している等の理由から、マルウェア感染のリスクは低いと考えられていました。しかし、昨年イランで、「Stuxnet」「Duqu」と呼ばれるマルウェアによって、核燃料施設の産業用制御システムがサイバー攻撃によって稼働不能に陥る深刻な被害が発生し、日本でも自動車等の製造ラインを制御するシステムがマルウェア感染によって一時操業停止に陥る等の大きな被害が発生し始めています。これらの状況を受け、経済産業省では制御系システムのセキュリティ対策を推進するため、国内重要インフラや工場等で仕様されている制御システムのセキュリティを検証するための施設を、宮城県に設置することを決定しました。重要インフラへのサイバー攻撃は、国民生活に大きな影響を及ぼす可能性がある重要な問題であることから、国家として必要な対策を早急に実施することが望まれます。

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