

**S.S.R.C.定期  
トレンドレポート  
Vol.9**



*Shield Security Research Center*

**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.トレンドレポート Vol.9

目次

1.	はじめに.....	- 2 -
2.	ご利用条件.....	- 2 -
3.	トレンドレポート 2011 年第 3 四半期度版.....	- 3 -
3.1.	セキュリティトレンド情報.....	- 3 -
3.2.	新種ウイルス情報.....	- 10 -
3.3.	脆弱性情報.....	- 11 -
4.	総括.....	- 12 -



## 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ー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ー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ー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ーのセキュリティアナリストが、月ごと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 3 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:2011/7/1～2011/9/30

#### 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. 米テレビ、FOXニュースの簡易ブログ「ツイッター」がハッキング被害に

関連記事	<ul style="list-style-type: none"><li>● オバマ大統領暗殺のデマ=米保守系TVにハッカー攻撃（時事ドットコム） <a href="http://www.jiji.com/jc/zc?k=201107/2011070400903">http://www.jiji.com/jc/zc?k=201107/2011070400903</a></li></ul>
------	--

##### 2. ソニーミュージックアイルランドのウェブサイトが改ざんされ偽のニュースが掲載

関連記事	<ul style="list-style-type: none"><li>● Hackers plant bogus celebrity stories on Sony Music Ireland website (naked security) <a href="http://nakedsecurity.sophos.com/2011/07/05/sony-music-ireland-hackers/">http://nakedsecurity.sophos.com/2011/07/05/sony-music-ireland-hackers/</a></li></ul>
------	--

##### 3. 警察庁へのサイバー攻撃、中国発が9割である事が明らかに

関連記事	<ul style="list-style-type: none"><li>● 警察庁へのHP攻撃、中国発が9割 中国に捜査協力要請（日本経済新聞） <a href="http://www.nikkei.com/news/headline/article/g=96958A9C93819695E2E4E2E7E78DE2E5E2E5E0E2E3E39191E2E2E2E2">http://www.nikkei.com/news/headline/article/g=96958A9C93819695E2E4E2E7E78DE2E5E2E5E0E2E3E39191E2E2E2E2</a></li><li>● 警察庁のHP閲覧できず サイバー攻撃か 3時間半大量アクセス（msn 産経ニュース） <a href="http://sankei.jp.msn.com/affairs/news/110711/crm11071111180003-n1.htm">http://sankei.jp.msn.com/affairs/news/110711/crm11071111180003-n1.htm</a></li></ul>
------	---

4. マイレージ会員の個人情報が外部から閲覧可能に

関連記事	<ul style="list-style-type: none"> <li>● マイレージ会員の個人情報が外部から閲覧可能に、カード情報も - スカイネットアジア (Security NEXT) <a href="http://www.security-next.com/022323">http://www.security-next.com/022323</a></li> </ul>
------	---

5. 米サイバー防衛戦略が公表

関連記事	<ul style="list-style-type: none"> <li>● Department of Defense Strategy for Operation in Cyberspace <a href="http://www.defense.gov/news/d20110714cyber.pdf">http://www.defense.gov/news/d20110714cyber.pdf</a></li> </ul>
------	--

6. 東芝関連企業サーバが不正アクセス被害に

プレスリリース	<ul style="list-style-type: none"> <li>● 米国グループ会社のサーバに対する不正アクセスについて (東芝) <a href="http://www.toshiba.co.jp/about/press/2011_07/pr_j1601.htm">http://www.toshiba.co.jp/about/press/2011_07/pr_j1601.htm</a></li> </ul>
---------	---

7. イカタコウイルス作成者に実刑判決

関連記事	<ul style="list-style-type: none"> <li>● イカタコウイルス作成者に実刑判決 「器物損壊」認定 (IT media) <a href="http://www.itmedia.co.jp/news/articles/1107/20/news040.html">http://www.itmedia.co.jp/news/articles/1107/20/news040.html</a></li> </ul>
------	--

8. ウイルス保管容疑で男逮捕 改正刑法で初摘発

関連記事	<ul style="list-style-type: none"> <li>● ウイルス保管容疑で男逮捕 改正刑法で初摘発 (IT media) <a href="http://www.itmedia.co.jp/news/articles/1107/21/news069.html">http://www.itmedia.co.jp/news/articles/1107/21/news069.html</a></li> <li>● ウイルス作成者が控訴 = 「イカタコ」器物損壊 (時事ドットコム) <a href="http://www.jiji.com/jc/zc?k=201107/2011072800848">http://www.jiji.com/jc/zc?k=201107/2011072800848</a></li> </ul>
------	---

9. AT&T 社内文書の不正入手で契約従業員を逮捕

関連記事	<ul style="list-style-type: none"> <li>● AT&amp;T 社内文書の不正入手で契約従業員を逮捕 (ZDNet Japan) <a href="http://japan.zdnet.com/security/analysis/35005388/">http://japan.zdnet.com/security/analysis/35005388/</a></li> </ul>
------	---

10. NATO 機密文書流出か ハッカー集団が「攻撃」

関連記事	<ul style="list-style-type: none"> <li>● NATO機密文書流出か ハッカー集団が「攻撃」 (msn 産経ニュース)  <a href="http://sankei.jp.msn.com/world/news/110722/erp11072201260000-n1.htm">http://sankei.jp.msn.com/world/news/110722/erp11072201260000-n1.htm</a> </li> </ul>
------	--

11. 迷惑メール送信幫助の疑い アドレス「名簿屋」を初摘発

関連記事	<ul style="list-style-type: none"> <li>● 迷惑メール送信幫助の疑い アドレス「名簿屋」を初摘発 警視庁 (msn 産経ニュース)  <a href="http://sankei.jp.msn.com/affairs/news/110725/crm11072515350019-n1.htm">http://sankei.jp.msn.com/affairs/news/110725/crm11072515350019-n1.htm</a> </li> </ul>
------	---

12. PC がウイルス感染、アカウント情報や個人情報流出の可能性

関連記事	<ul style="list-style-type: none"> <li>● PC がウイルス感染、アカウント情報や個人情報流出の可能性 - 国交省 (Security NEXT)  <a href="http://www.security-next.com/022778">http://www.security-next.com/022778</a> </li> </ul>
------	---

13. 米サイバーセキュリティを担当する最大の請負業者の1つである ManTech International がサイバー攻撃被害に

関連記事	<ul style="list-style-type: none"> <li>● 米政府のサイバーセキュリティ請負業者にハッカー攻撃 (CNet Japan)  <a href="http://japan.cnet.com/news/business/35005745/">http://japan.cnet.com/news/business/35005745/</a> </li> </ul>
------	--

14. 国連や米政府に最大のサイバー攻撃

関連記事	<ul style="list-style-type: none"> <li>● Report on 'Operation Shady RAT' identifies widespread cyber-spying (The Washington Post)  <a href="http://www.washingtonpost.com/national/national-security/report-identifies-wide-spread-cyber-spying/2011/07/29/gIQAoTUmqI_story.html">http://www.washingtonpost.com/national/national-security/report-identifies-wide-spread-cyber-spying/2011/07/29/gIQAoTUmqI_story.html</a> </li> </ul>
------	--

15. 日本全国の銀行ネットバンクが不正アクセス被害に

関連記事	<ul style="list-style-type: none"> <li>● 日本全国の銀行ネットバンクで不正アクセスが相次ぐ（日本経済新聞）  <a href="http://www.nikkei.com/tech/news/article/g=96958A9C93819499E2E1E2E2818DE2E1E2EAE0E2E3E3E2E2E2E2E2;da=96958A88889DE2E4E1E2E5E0E6E2E0E7E2E6E0E2E3E2E2E2E2E2E2">http://www.nikkei.com/tech/news/article/g=96958A9C93819499E2E1E2E2818DE2E1E2EAE0E2E3E3E2E2E2E2E2;da=96958A88889DE2E4E1E2E5E0E6E2E0E7E2E6E0E2E3E2E2E2E2E2E2</a></li> </ul>
------	---

16. 全国初、クレジットカード現金化業者逮捕 出資法違反容疑で警視庁

関連記事	<ul style="list-style-type: none"> <li>● 全国初、クレジットカード現金化業者逮捕 出資法違反容疑で警視庁（msn 産経ニュース）  <a href="http://sankei.jp.msn.com/affairs/news/110805/crm11080512430007-n1.htm">http://sankei.jp.msn.com/affairs/news/110805/crm11080512430007-n1.htm</a></li> </ul>
------	--

17. 動画サイトの利用実態調査検討委員会報告書 - 日本レコード協会

関連記事	<ul style="list-style-type: none"> <li>● 「動画サイトの利用実態調査検討委員会」報告書公表（日本レコード協会）  <a href="http://www.riaj.or.jp/release/2011/pr110808.html">http://www.riaj.or.jp/release/2011/pr110808.html</a></li> </ul>
------	---

18. シティカードジャパン、約 9 万人分のカード情報が流出、第三者に売却される

関連記事	<ul style="list-style-type: none"> <li>● 顧客情報の不正売却について（シティカードジャパン）  <a href="http://www.citibank.co.jp/ccsi/ja/notice/20110805_01.html">http://www.citibank.co.jp/ccsi/ja/notice/20110805_01.html</a></li> </ul>
------	--

19. 世界規模で拡散している標的型攻撃「Operation Shady RAT」

関連記事	<ul style="list-style-type: none"> <li>● 世界 14 カ国、72 組織をターゲットにした Operation Shady RAT（マカフィー）  <a href="http://www.mcafee.com/japan/security/mcafee_labs/blog/content.asp?id=1275">http://www.mcafee.com/japan/security/mcafee_labs/blog/content.asp?id=1275</a></li> <li>● New CitiGroup hack shows security 'experts' preaching calm should cut it out (IT WORLD)  <a href="http://www.itworld.com/security/191581/new-hack-citigroup-shows-security-experts-preaching-reason-should-just-cut-it-out">http://www.itworld.com/security/191581/new-hack-citigroup-shows-security-experts-preaching-reason-should-just-cut-it-out</a></li> </ul>
------	---

20. アフラック他、3社の外資系保険会社の個人情報不正転売被害に

<p>プレスリリース</p>	<ul style="list-style-type: none"> <li>● お客さま情報の不正売却について（アフラック） <a href="http://www.aflac.co.jp/news_pdf/20110812.pdf">http://www.aflac.co.jp/news_pdf/20110812.pdf</a></li> <li>● お客様情報の流出について（アメリカンホーム保険） <a href="http://www.americanhome.co.jp/news/20110815.html">http://www.americanhome.co.jp/news/20110815.html</a></li> <li>● お客様情報の不正売却について（メットライフ アリコ） <a href="http://www.metlifealico.co.jp/about/press/2011/110815_2.html">http://www.metlifealico.co.jp/about/press/2011/110815_2.html</a></li> <li>● お客様情報の不正売却につきまして（エース損害保険株式会社） <a href="http://www.ace-insurance.co.jp/CGI/news/view.cgi?mode=detail&amp;seq=0000000267">http://www.ace-insurance.co.jp/CGI/news/view.cgi?mode=detail&amp;seq=0000000267</a></li> <li>● お客様情報の不正売却について（セディナ） <a href="http://www.cedyna.co.jp/info/20110816.html">http://www.cedyna.co.jp/info/20110816.html</a></li> </ul>
<p>関連記事</p>	<ul style="list-style-type: none"> <li>● アリコとエースでも情報流出＝代理店から、4社で計2万5200件（時事ドットコム） <a href="http://www.jiji.com/jc/zc?k=201108/2011081500652">http://www.jiji.com/jc/zc?k=201108/2011081500652</a></li> </ul>

21. 警察庁のHPへサイバー攻撃 7月、尖閣めぐり中国掲示板で呼びかけ

<p>関連記事</p>	<ul style="list-style-type: none"> <li>● 「小日本のサイトを攻撃して殺します」 7月、尖閣めぐり中国掲示板で呼びかけ（msn産経ニュース） <a href="http://sankei.jp.msn.com/affairs/news/110826/crm11082611330008-n1.htm">http://sankei.jp.msn.com/affairs/news/110826/crm11082611330008-n1.htm</a></li> </ul>
-------------	--



22. 三菱東京 UFJ 銀のネットバンクで不審メールが流通、顧客情報を盗み取る

<p>プレスリリース</p>	<ul style="list-style-type: none"> <li>● 当行を装った不審な電子メール（件名：三菱東京 UFJ 銀行より大切なお知らせです）にご注意ください。（三菱東京 UFJ 銀行） <a href="http://www.bk.mufg.jp/info/phishing/20110825.html">http://www.bk.mufg.jp/info/phishing/20110825.html</a></li> <li>● 三菱東京 UFJ 銀行を装った不審なメールによる不正取引について（三菱東京 UFJ 銀行） <a href="http://www.bk.mufg.jp/news/news2011/pdf/news0906_02.pdf">http://www.bk.mufg.jp/news/news2011/pdf/news0906_02.pdf</a></li> </ul>
<p>関連記事</p>	<ul style="list-style-type: none"> <li>● 三菱東京 UFJ 銀のネットバンクで不審メールが流通、顧客情報を盗み取る（ITpro） <a href="http://itpro.nikkeibp.co.jp/article/NEWS/20110829/367761/">http://itpro.nikkeibp.co.jp/article/NEWS/20110829/367761/</a></li> </ul>

23. ビックカメラネット通販で不正購入 中国人 3 人逮捕 他人のポイント使う

<p>関連記事</p>	<ul style="list-style-type: none"> <li>● ビックカメラネット通販で不正購入 中国人 3 人逮捕 他人のポイント使う（msn 産経ニュース） <a href="http://sankei.jp.msn.com/affairs/news/110829/crm11082911440003-n1.htm">http://sankei.jp.msn.com/affairs/news/110829/crm11082911440003-n1.htm</a></li> </ul>
-------------	--

24. 「平成 22 年度 学校・教育機関の個人情報漏えい事故の発生状況・教員の意識に関する調査」

<p>プレスリリース</p>	<ul style="list-style-type: none"> <li>● 「平成 22 年度 学校・教育機関の個人情報漏えい事故の発生状況・教員の意識に関する調査」（ISEN） <a href="http://school-security.jp/pdf/2010_s.pdf">http://school-security.jp/pdf/2010_s.pdf</a></li> <li>● ISEN、「平成 22 年度 学校・教育機関の個人情報漏えい事故の発生状況・教員の意識に関する調査」を実施（asahi.com） <a href="http://www.asahi.com/business/pressrelease/ATP201109010055.html">http://www.asahi.com/business/pressrelease/ATP201109010055.html</a></li> </ul>
----------------	---

25. セシールの顧客情報 3 万件流出 委託会社が不正売却

プレスリリース	<ul style="list-style-type: none"> <li>● お客様情報の不正売却について（セシール）</li> </ul> <p><a href="http://corp.cecile.co.jp/news/pdf/11-66.pdf">http://corp.cecile.co.jp/news/pdf/11-66.pdf</a></p>
---------	---

26. 米NBCにハッカー攻撃、9.11 米テロ事件の情報を悪用

関連記事	<ul style="list-style-type: none"> <li>● 米NBCにハッカー攻撃、9・11 跡地でのテロ情報流す（CNN）</li> </ul> <p><a href="http://www.cnn.co.jp/tech/30003941.html">http://www.cnn.co.jp/tech/30003941.html</a></p>
------	---

27. 三菱重にサイバー攻撃

関連記事	<ul style="list-style-type: none"> <li>● 三菱重工、国内 11 拠点でウイルス感染の事実を公表、「機密情報流出は確認されず」（ITpro）</li> </ul> <p><a href="http://itpro.nikkeibp.co.jp/article/NEWS/20110919/368887/">http://itpro.nikkeibp.co.jp/article/NEWS/20110919/368887/</a></p> <ul style="list-style-type: none"> <li>● 三菱電機、川崎重工も形跡、I H I にもサイバー攻撃（Searchina）</li> </ul> <p><a href="http://news.searchina.ne.jp/disp.cgi?v=2011&amp;d=0920&amp;f=national_0920_369.shtml">http://news.searchina.ne.jp/disp.cgi?v=2011&amp;d=0920&amp;f=national_0920_369.shtml</a></p> <ul style="list-style-type: none"> <li>● 三菱重工を含む防衛産業 8 社が標的型攻撃の被害に、Trend Micro が分析（INTERNET Watch）</li> </ul> <p><a href="http://internet.watch.impress.co.jp/docs/news/20110920_478766.html">http://internet.watch.impress.co.jp/docs/news/20110920_478766.html</a></p> <ul style="list-style-type: none"> <li>● 三菱重工サイバー攻撃と標的型メール（YOMIURI ONLINE）</li> </ul> <p><a href="http://www.yomiuri.co.jp/net/security/goshinjyutsu/20110922-OYT8T00985.htm">http://www.yomiuri.co.jp/net/security/goshinjyutsu/20110922-OYT8T00985.htm</a></p>
------	---

28. 標的型メール攻撃事案の把握状況について - 警察庁

プレスリリース	<ul style="list-style-type: none"> <li>● 標的型メール攻撃事案の把握状況について（警察庁）</li> </ul> <p><a href="http://www.npa.go.jp/keibi/biki5/hyotekigata.pdf">http://www.npa.go.jp/keibi/biki5/hyotekigata.pdf</a></p>
---------	---

### 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. vsftpd 2.3.4 に含まれたバックドアに関する検証レポート

関連記事	<ul style="list-style-type: none"><li>● vsftpd 2.3.4 に含まれたバックドアに関する検証レポート (NTT データ先端技術株式会社) <a href="http://security.intellilink.co.jp/article/vulner/110706.html">http://security.intellilink.co.jp/article/vulner/110706.html</a></li></ul>
------	---

#### 2. 一部の Web サイトに不正な iframe タグが埋め込まれる

関連記事	<ul style="list-style-type: none"><li>● 一部の Web サイトに不正な iframe タグが埋め込まれる (IBM Tokyo SPC Report) <a href="https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/injection_20110728?lang=ja">https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/injection_20110728?lang=ja</a></li></ul>
------	---

#### 3. マスターブートレコードに感染するマルウェアがまた流行

関連記事	<ul style="list-style-type: none"><li>● MBR 感染型がまた流行か (図解付き) (Symantec ブログ) <a href="http://www.symantec.com/connect/blogs/mbr-1">http://www.symantec.com/connect/blogs/mbr-1</a></li></ul>
------	---

#### 4. Android 2.3 にて、root レベルで感染するマルウェア

関連記事	<ul style="list-style-type: none"><li>● GingerMaster Is First Malware To Utilize A Root Exploit On Android 2.3 (dark READING) <a href="http://www.darkreading.com/authentication/167901072/security/news/231500422/gingermaster-is-first-malware-to-utilize-a-root-exploit-on-android-2-3.html">http://www.darkreading.com/authentication/167901072/security/news/231500422/gingermaster-is-first-malware-to-utilize-a-root-exploit-on-android-2-3.html</a></li></ul>
------	---

#### 5. リモートデスクトップ経由で感染を広げる新手のウイルス「Morto」出現

関連記事	<ul style="list-style-type: none"><li>● リモートデスクトップ経由で感染を広げる新手のウイルス「Morto」出現 (So-net セキュリティ) <a href="http://www.so-net.ne.jp/security/news/view.cgi?type=2&amp;no=2663">http://www.so-net.ne.jp/security/news/view.cgi?type=2&amp;no=2663</a></li></ul>
------	---

### 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. DNS サーバの BIND9 に DoS 攻撃を受ける深刻な脆弱性が発覚

関連記事	<ul style="list-style-type: none"> <li>● (緊急) BIND 9.x の脆弱性を利用したサービス不能 (DoS) 攻撃について (JPCERT/CC) <a href="http://jprs.jp/tech/security/2011-07-05-bind9-vuln-remote-packet-auth-and-recurs.html">http://jprs.jp/tech/security/2011-07-05-bind9-vuln-remote-packet-auth-and-recurs.html</a></li> </ul>
------	--

#### 2. Firefox の nsTreeRange オブジェクトにおけるメモリ破壊の脆弱性(CVE-2011-0073)に関する検証レポート

関連記事	<ul style="list-style-type: none"> <li>● Firefox の nsTreeRange オブジェクトにおけるメモリ破壊の脆弱性 (CVE-2011-0073) に関する検証レポート (NTT データ先端技術株式会社) <a href="http://security.intellilink.co.jp/article/vulner/110714.html">http://security.intellilink.co.jp/article/vulner/110714.html</a></li> </ul>
------	--

#### 3. phpMyAdmin にて任意のコードを実行可能な脆弱性 (CVE-2011-2505, CVE-2011-2506) に関する検証レポート

関連記事	<ul style="list-style-type: none"> <li>● phpMyAdmin にて任意のコードを実行可能な脆弱性 (CVE-2011-2505, CVE-2011-2506) に関する検証レポート (NTT データ先端技術株式会社) <a href="http://security.intellilink.co.jp/article/vulner/110729.html">http://security.intellilink.co.jp/article/vulner/110729.html</a></li> </ul>
------	--

#### 4. PHP5.3.7 の crypt 関数に致命的な脆弱性

関連記事	<ul style="list-style-type: none"> <li>● PHP5.3.7 の crypt 関数に致命的な脆弱性(Bug #55439) (徳丸浩の日記) <a href="http://blog.tokumaru.org/2011/08/php537cryptbug-55439.html">http://blog.tokumaru.org/2011/08/php537cryptbug-55439.html</a></li> </ul>
------	--

#### 4. 総括

今期は、国内著名企業を標的とした攻撃事例が相次ぎました。中でも、防衛関連企業を標的とした「標的型メール攻撃<sup>22</sup>」が報道でもクローズアップされており、何者かによる防衛情報の盗み見など、国家規模が想定される攻撃が話題となっております。この「標的型メール攻撃」は、実際に標的企業に存在、もしくは認識のある人物などの情報を騙り送信されており、表面的には何の害もないように見えるメールの添付ファイルなどを閲覧する事で対象 PC がウイルス感染し、そこを踏み台として企業システム内の情報を盗み見たり、窃取されてしまいます。攻撃には既知の脆弱性などが悪用されていますが、ウイルス対策ソフトやアップデート措置の有無に関わらず、ソーシャルエンジニアリングを用いた手法が取られており、ふとした隙間を突いて、システムが攻撃者の支配下に置かれてしまいます。こうしたことにより、一部企業では、社員に対して害のない偽メールを送信して、実際にどの位の割合で感染する可能性があるかどうかなどを検証する企業もあり、セキュリティピックとしても今後継続して注目すべき事例となっております。現代のサイバー犯罪者は、あくまでも秘かに標的ネットワークに侵入して悪意のある行為を働くというのが主流となっており、実際の被害の有無に関わらない継続的なセキュリティ教育や対策が必要となってきています。

また、外資系保険企業からの個人情報不正転売事件<sup>20</sup>が相次ぎました。これは、関連企業の元従業員が情報を第3者に不正転売した事から明らかになっており、内部から流出する個人情報に対するセキュリティ対策も再度強化される必要があります。

# 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>