SSRC-TR-2010-10

S.S.R.C.定期
トレンドレポート
Vol.5

株式会社　日立情報システムズ

セキュリティリサーチセンタ

初版　2010/10/01

S.S.R.C.トレンドトレポート Vol.5

目次

1. はじめに ..... - 2 -
2. ご利用条件 ..... - 2 -
3. トレンドレポート 2010 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. WEBサイト改ざん関連情報 ..... - 8 -
3.3. 新種ウイルス情報 ..... - 11 -
3.4. 脆弱性情報 ..... - 11 -
4. 総括 ..... - 12 -

1. はじめに

S.S.R.C.(Shield Security Research Center)は、株式会社日立情報システムズ 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、株式会社日立情報システムズ、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、株式会社日立情報システムズ(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 2010 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:2010/07/01～2010/09/30

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. 米政府、インフラへのサイバー攻撃発見プログラムを開発＝関係筋

関連記事	● 米政府、インフラへのサイバー攻撃発見プログラムを開発＝関係筋（ウォールストリートジャーナル） http://jp.wsj.com/IT/node_80374

2. アンラボ、昨年の 7.7 サイバーテロ時に感染した ゾンビパソコンからの DDoS 攻撃に関する注意喚起

ニュースリリース	● アンラボ、昨年の 7.7 サイバーテロ時に感染した ゾンビパソコンからの DDoS 攻撃に関する注意喚起（AhnLab） http://www.ahnlab.co.jp/company/press/news_release_view.asp?seq=5036&pageNo=1&news_gu=01

3. 中国の対米サイバー攻撃拠点は海南島の人民解放軍　米機関が断定

関連記事	● 中国の対米サイバー攻撃拠点は海南島の人民解放軍　米機関が断定（msn 産経ニュース） http://sankei.jp.msn.com/world/china/100710/chn1007101939002-n1.htm

4. Dellのサーバ用マザーボードにマルウェアが混入

関連記事	● Dell のサーバ用マザーボードにマルウェアが混入（IT media） http://www.itmedia.co.jp/enterprise/articles/1007/22/news021.html

5. 米民間告発サイト、大量の米軍機密文書を公開

関連記事	● 米民間告発サイト、大量の米軍機密文書を公開（ウォールストリートジャーナル） http://jp.wsj.com/US/Politics/node_85379 ● 公開文書、戦争犯罪の可能性示唆＝ウィキリークス創設者（ウォールストリートジャーナル） http://jp.wsj.com/US/node_85798

6. デジタル複合機の脆弱性に関する調査報告書の公開

プレスリリース	● デジタル複合機の脆弱性に関する調査報告書の公開（IPA） http://www.ipa.go.jp/about/press/20100830.html

7. ATMのハッキングに成功、ハッカーの国際会議「DEFCON」で発表

関連記事	● ATM のハッキングに成功、ハッカーの国際会議「DEFCON」で発表（AFP BB News） http://www.afpbb.com/article/environment-science-it/it/2744837/6033459

8. ヤフオク届いたら「偽物」　同じ出品者、苦情１００件超

関連記事	● ヤフオク届いたら「偽物」　同じ出品者、苦情１００件超（asahi.com） http://www.asahi.com/national/update/0817/TKY201008170385.html

9. もしや新手のテロ？ 空港のコンピューターにトロイの木馬で飛行機が墜落炎上

関連記事	● もしや新手のテロ？ 空港のコンピューターにトロイの木馬で飛行機が墜落炎上（GIZMODO） http://www.gizmodo.jp/2010/08/post_7538.html

10. 米国防総省ネットワークにスパイ侵入

関連記事	● 米国防総省ネットワークにスパイ侵入（ウォールストリートジャーナル） http://jp.wsj.com/US/node_94666

11. Microsoft.com は毎秒 7000～9000 回の攻撃を受けている

関連記事	● Microsoft.com は毎秒 7000～9000 回の攻撃を受けている（/.JP） http://slashdot.jp/security/10/08/31/1136257.shtml

12. 平成 22 年上半期のサイバー犯罪の検挙状況等について

ニュースリリース	● 平成 22 年上半期のサイバー犯罪の検挙状況等について（警視庁） http://www.npa.go.jp/cyber/statics/h22/pdf01-1.pdf

13. 福島の高速バス予約サイトから情報流出　不正利用も

ニュースリリース	● 個人情報の流出についてのお詫び（さくら観光） http://www.489.fm/oshirase5.html ● 9/17 個人情報の流出について 2 次報告 http://www.489.fm/oshirase7.html（さくら観光）
関連記事	● 福島の高速バス予約サイトから情報流出　不正利用も（asahi.com） http://www.asahi.com/digital/internet/TKY201009020149.html

14. 「裏サイト」パトロール始動　奈良県教委、民間業者に委託　悪質書き込みを削除

関連記事	● 「裏サイト」パトロール始動　奈良県教委、民間業者に委託　悪質書き込みを削除（msn 産経ニュース） http://sankei.jp.msn.com/region/kinki/nara/100904/nar1009040211004-n1.htm

15. 再度活発化するConfickerワーム

関連記事	● 再度活発化する Conficker ワーム（McAfee Labs Blog） http://www.mcafee.com/japan/security/mcafee_labs/blog/jp_conficker-warm.asp

16. サイバー攻撃…中国語に改ざん

関連記事	● 徳島２町村のＨＰ、サイバー攻撃…中国語に改ざん（YOMIURI ONLINE） http://www.yomiuri.co.jp/net/news/20100922-OYT8T00486.htm ● 山口大のＨＰ改ざん、中国語で「日本の豚」（YOMIURI ONLINE） http://www.yomiuri.co.jp/kyoiku/news/20100922-OYT8T00167.htm ● 【中国人船長釈放】中国からのサイバーテロ？　神戸の団体ＨＰ改竄（msn 産経ニュース） http://sankei.jp.msn.com/affairs/crime/100925/crm1009251949017-n1.htm

17. イランの原子力発電所のシステムがウイルスに感染

関連記事	● イランの原子力発電所のシステムがウイルスに感染（ウォールストリートジャーナル） http://jp.wsj.com/World/Europe/node_108794

18. イカタコウイルスを作成＝魚介類画像にファイル改変－会社員逮捕・警視庁

関連記事	● イカタコウイルスを作成＝魚介類画像にファイル改変－会社員逮捕・警視庁（時事ドットコム） http://www.jiji.com/jc/zc?k=201008/2010080400222

19. 顧客クレジットカード情報流出　ネット宅配で 1 万 2 千件

ニュースリリース	● お客様情報の取扱いに関するお詫びとご報告（NEO BEAT） http://www.neobeat.co.jp/news/detail_20100804.php
関連記事	● 「プロのハッカー集団 の犯行」　ネットスーパーの情報盗難（47news） http://www.47news.jp/news/2010/08/post_20100813173203.html

20. 福島の高速バス予約サイトから情報流出　不正利用も

関連記事	● 福島の高速バス予約サイトから情報流出　不正利用も（asahi.com） http://www.asahi.com/digital/internet/TKY201009020149.html ● 調査であらたに約 1160 件が判明し流出件数が 17 万 755 件に - さくら観光（Security NEXT） http://www.security-next.com/015161

21. 「Faith」通販サイトに不正アクセス、カード情報 7 万 4,048 人分流出

ニュースリリース	● 当社子会社における不正アクセスによるお客様情報流出に関するお詫びとお知らせ（MCJ） http://www.mcj.jp/ir/irnews/2010/pdf/0927_01.pdf

3.2. WEB サイト改ざん関連情報

1. 公式サイトとニュースサイトが改ざん被害 – 大阪デジタルコンテンツビジネス創出協議会

関連記事	● 公式サイトとニュースサイトが改ざん被害 – 大阪デジタルコンテンツビジネス創出協議会（Security NEXT） http://www.security-next.com/012983

2. 運営サイトがSQLインジェクションで改ざん – ホビージャパン

関連記事	● 運営サイトが SQL インジェクションで改ざん – ホビージャパン（Security NEXT） http://www.security-next.com/013171

3. 不正アクセス被害で閲覧者にウイルス感染のおそれ – リム情報開発

関連記事	● 不正アクセス被害で閲覧者にウイルス感染のおそれ – リム情報開発（Security NEXT） http://www.security-next.com/013838

4. Tシャツ販売サイトが改ざん - 閲覧でウイルス感染のおそれ

関連記事	● T シャツ販売サイトが改ざん - 閲覧でウイルス感染のおそれ（Security NEXT） http://www.security-next.com/013880

5. 運用サーバに不正アクセス、漏洩や改ざんは発生せず – 丸紅インフォテック

関連記事	● 運用サーバに不正アクセス、漏洩や改ざんは発生せず – 丸紅インフォテック（Security NEXT） http://www.security-next.com/014139

6. 北九州市の情報サイトが改ざん – 誘導先は閉鎖されており実質被害なし

関連記事	● 北九州市の情報サイトが改ざん – 誘導先は閉鎖されており実質被害なし（Security NEXT） http://www.security-next.com/014118

7. 赤十字社のサイト、再びマルウェア攻撃の標的に

関連記事	● 赤十字社のサイト、再びマルウェア攻撃の標的に（japan.internet.com） http://japan.internet.com/webtech/20100816/11.html

8. 8月はWebサイト改ざん被害が多発

関連記事	● 8月は Web サイト改ざん被害が多発（Security.GS.MAGAZINE） http://www.security.gs/magazine/security/2010/08/25/story_3146/

9. 山梨県芸術文化協会のサイトが改ざん - 閲覧でウイルス感染おそれ

関連記事	● 山梨県芸術文化協会のサイトが改ざん - 閲覧でウイルス感染おそれ（Security NEXT） http://www.security-next.com/014513

10. 金沢大付高ＨＰ改ざん、中国からアクセス千回超

関連記事	● 金沢大付高ＨＰ改ざん、中国からアクセス千回超（YOMIURI ONLINE） http://www.yomiuri.co.jp/kyoiku/news/20100916-OYT8T00327.htm

11. 宝生能楽堂のサイトがウイルス被害 - 更新用PCから感染

関連記事	● 宝生能楽堂のサイトがウイルス被害 - 更新用 PC から感染（Security NEXT） http://www.security-next.com/015000

12. 住宅リフォーム会社のサイトが改ざん - 閲覧でウイルス感染のおそれ

関連記事	● 住宅リフォーム会社のサイトが改ざん - 閲覧でウイルス感染のおそれ（Security NEXT） http://www.security-next.com/015083

13. 山口大のＨＰ改ざん、中国語で「日本の豚」

関連記事	● 山口大のＨＰ改ざん、中国語で「日本の豚」（YOMIURI ONLINE） http://www.yomiuri.co.jp/kyoiku/news/20100922-OYT8T00167.htm

14. 徳島２町村のＨＰ、サイバー攻撃…中国語に改ざん

関連記事	● 徳島２町村のＨＰ、サイバー攻撃…中国語に改ざん（YOMIURI ONLINE） http://www.yomiuri.co.jp/net/news/20100922-OYT8T00486.htm

3.3. 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. ヘルプファイルに感染する新種のマルウェアに要注意

関連記事	● ヘルプファイルに感染する新種のマルウェアに要注意（McAfee Labs Blog） http://www.mcafee.com/japan/security/mcafee_labs/blog/be-careful-on-help-files.asp

2. 日本におけるガンブラー攻撃とその対策

ニュースリリース	● 日本におけるガンブラー攻撃とその対策（G DATA） http://gdata.co.jp/press/archives/2010/09/post_93.htm

3. バッファロー製ポータブルWi-Fiルーターにウイルス混入

関連記事	● バッファロー製ポータブル Wi-Fi ルーターにウイルス混入（ケータイ Watch） http://k-tai.impress.co.jp/docs/news/20100910_393024.html

3.4. 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. Twitter の XSS の脆弱性を悪用した攻撃が発生

関連記事	● 「マウスオーバーの」問題についての全容（twitter ブログ） http://blog.twitter.jp/2010/09/blog-post_22.html

2. Microsoft Windows のショートカットファイルの処理に脆弱性

関連記事	● Microsoft Windows のショートカットファイルの処理に脆弱性（JVN） http://jvn.jp/cert/JVNVU940193/

4. 総括

中国漁船と日本海保船が衝突した問題に起因して、日本国内の、関連すると推測された複数のサイトが改ざん被害に遭っています。問題の余波は未だ衰えておらず、アンダーグラウンドでのサイバー攻撃が今後も発生する可能性も指摘されています。

昨今のトレンドとして、サイバー攻撃というものが過去にも増してマスコミなどにも取り上げられるようになってきています。諸外国の産業インフラを狙ったと推測されているマルウェア「Stuxnet（スタクスネット）」の出現や、日本国内ウェブサーバへの不正アクセスなど、私達の知らないところで、常にサイバー攻撃が発生している時代になりつつあります。事実、先日発生した Google などへのサイバー攻撃には各国に拡散していたウイルス感染 PC がボットネットとなり、一斉にサイバー攻撃を仕掛けたなど、問題がエンドユーザにまで及んでいる事は明白です。セキュリティの重要性が今一度再認識されている今、セキュリティソフトの適用やその他セキュリティ対策措置を再確認し、サイバー攻撃に悪用されない事が望まれるでしょう。

株式会社　日立情報システムズ

〒141-8672 東京都品川区大崎 1-2-1

http://www.hitachijoho.com

http://www.shield.ne.jp