株式会社 日立システムズ

SSRC-TR-Vol.24

S.S.R.C.定期
トレンドレポート
Vol.24

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.24

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 2015 年第 2 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:2015/4/1～2015/6/30

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. 標的型攻撃

関連記事	● メールでマルウェア感染、個人情報約 125 万件が漏洩 –日本年金機構（Security NEXT） http://www.security-next.com/058906 ● 日本年金機構の情報漏えいで、「2 次被害」への注意相次ぐ（セキュリティ通信） http://security-t.blog.so-net.ne.jp/2015-06-08 ● 脆弱性が判明しサイトを一時停止 - 日本年金機構（Security NEXT） http://www.security-next.com/059145 ● 年金機構、初動に甘さ　少なくとも 27 台感染、大半が東京本部　公表に遅れ、事後対応も混乱（IT media） http://www.itmedia.co.jp/news/articles/1506/08/news041.html ● 米政府職員 400 万人分の個人情報流出、中国からサイバー攻撃か（ロイター） http://jp.reuters.com/article/2015/06/05/us-cyber-idJPKBN0OL02R20150605 ● 石油連盟、標的型攻撃でパソコンウイルス感染（IT pro） http://itpro.nikkeibp.co.jp/atcl/news/15/061001940/ ● 石油やガスなどの企業にサイバー攻撃、情報盗む新手のマルウェアが拡大（IT media） htttp://www.itmedia.co.jp/news/articles/1504/01/news054.html ● 東京商工会議所に標的型メール攻撃　個人情報 1 万 2000 件流出の可能性（IT media） http://www.itmedia.co.jp/news/articles/1506/10/news094.html ● 広島県外郭団体で端末 52 台中 5 台がウイルス感染、標的型攻撃メール受信も（IT pro） http://itpro.nikkeibp.co.jp/atcl/news/15/061702030/ ● 上田市が標的型攻撃でウイルス感染、インターネットを遮断（IT pro） http://itpro.nikkeibp.co.jp/atcl/news/15/061602021/

	● 「標的型メール」を仕掛けられるウイルス作成ソフトが横行（産経 WEST） http://www.sankei.com/west/news/150617/wst1506170016-n1.html ● C&C の IP 通知に MS の「TechNet」を悪用 - 「Deputy Dog」の攻撃グループ（Security NEXT） http://www.security-next.com/058530 ● レバノンの政治組織と思われる長期的サイバー攻撃、標的は機密情報か(チェック・ポイント) (Scan NetSecurity) http://scan.netsecurity.ne.jp/article/2015/04/09/36167.html ● パブリッククラウド利用者 17%に被害経験 - 標的型攻撃など（Security NEXT） http://www.security-next.com/058541 ● 「Microsoft Office」よりも「一太郎」が狙われる？ 標的型攻撃の国内動向（TechTarget Japan） http://techtarget.itmedia.co.jp/tt/news/1505/21/news06.html ● 標的型攻撃メールは年間 505 件 - 国内発のメール目立つ（Security NEXT） http://www.security-next.com/058804 ● 企業への標的型攻撃、31 カ月続くケースも（IT media） http://www.itmedia.co.jp/enterprise/articles/1505/28/news062.html ● 企標的型攻撃の”司令塔”、国内で 7 倍に（IT pro） http://itpro.nikkeibp.co.jp/atcl/column/14/346926/041600229/

2. サイバー攻撃

関連記事	● 富山大にサイバー攻撃　サーバーのパスワード単純なまま（朝日新聞 DIGITAL） http://www.asahi.com/articles/ASH625DS6H62UUPI001.html ● サイバー攻撃対策「５年後に１万人」　NTT、４倍増へ（朝日新聞 DIGITAL） http://www.asahi.com/articles/ASH6B432WH6BULFA00Q.html ● 世界女子カーリング大会のサイトが改ざん ・ 閲覧でマルウェア感染の可能性（Security Next） http://www.security-next.com/056070 ● 豪空港サイトが改ざん＝「イスラム国」支持声明（時事ドットコム） http://www.jiji.com/jc/c?g=int_30&k=2015041200286 ● 慶大研究室ＨＰに弁護士殺害予告　何者かが改ざんか（朝日新聞 DIGITAL） http://www.asahi.com/articles/ASH614K4SH61UTIL02D.html ● 飛行中の旅客機制御システムに不正侵入か　ＦＢＩが捜査（CNN.co.jp） http://www.cnn.co.jp/usa/35064629.html ● パスワード一元管理の LastPass にハッキング、情報流出も（IT media） http://www.itmedia.co.jp/enterprise/articles/1506/16/news050.html ● TV 放送にパスワードが映り TV 局が速攻でハッキングされる（Gigazine） http://gigazine.net/news/20150413-hacked-during-tv-interview/ ● 米保険会社から 110 万人の個人情報流出、DB に不正アクセス（IT media） http://www.itmedia.co.jp/enterprise/articles/1505/22/news051.html ● 米国で納税者アカウントに不正アクセス、10 万人に被害　（IT media） http://www.itmedia.co.jp/enterprise/articles/1505/27/news046.html ● 日本動物園水族館協会にサイバー攻撃　飼育員情報が流出（朝日新聞 DIGITAL） http://www.asahi.com/articles/ASH5W3HC8H5WUTIL006.html ● サイバー攻撃に狙われる医療機関、患者情報の流出状況は？（IT media） http://www.itmedia.co.jp/enterprise/articles/1505/12/news042.html

3. フィッシング

関連記事	● フィッシング対協、Facebook ページで学習教材を公開（Security NEXT） http://www.security-next.com/059760 ● 「イ左川急便」名乗るフィッシング - 不正サイトへ誘導か（Security NEXT） http://www.security-next.com/059830 ● フィッシング、2 月に再び増加 - 昨年末と同水準に（Security NEXT） http://www.security-next.com/057314 ● みずほ銀行をかたるフィッシング（フィッシング対策協議会） https://www.antiphishing.jp/news/alert/mizuho20150520.html ● 三井住友銀利用者狙うフィッシング - メール本文はわずか 1 文（Security NEXT） http://www.security-next.com/058575 ● ゆうちょ銀装うフィッシング - 「アカウントの凍結」などと不安煽る（Security NEXT） http://www.security-next.com/058425 ● 新生銀行を装った詐欺メール・詐欺サイトについてのご注意（新生銀行） http://www.shinseibank.com/info/news150421_secure.html ● 【注意喚起】SMS(ショートメッセージサービス)で誘導される銀行のフィッシングサイトにご注意ください（2015/06/16）（フィッシング対策協議会） http://www.antiphishing.jp/news/alert/_sms_20150616.html ● セゾン Net アンサーをかたるフィッシング （2015/05/25）（フィッシング対策協議会） http://www.antiphishing.jp/news/alert/saison20150525.html ● 暗号化通信を盗聴可能にする攻撃、日本のネットバンクを標的に（IT media） http://www.itmedia.co.jp/enterprise/articles/1504/13/news124.html ● 2015 年 1Q のネットバンク不正引出、法人被害は沈静化（Security NEXT） http://www.security-next.com/058838

	● 警視庁、日本標的の不正送金ウイルス「無力化作戦」に乗り出す　ボットネット特定し対策（IT media） http://www.itmedia.co.jp/news/articles/1504/10/news094.html ● 2015/03 フィッシング報告状況（フィッシング対策協議会） http://www.antiphishing.jp/report/monthly/201503.html ● 2015/04 フィッシング報告状況（フィッシング対策協議会） http://www.antiphishing.jp/report/monthly/201504.html ● 2015/05 フィッシング報告状況（フィッシング対策協議会） http://www.antiphishing.jp/report/monthly/201505.html

4. 脆弱性

関連記事	● 秀丸エディタにおけるバッファオーバーフローの脆弱性（JVN） http://jvn.jp/jp/JVN58784309/ ● 深刻な脆弱性に対応した「WordPress 4.2.2」が公開 即時更新を推奨（Security NEXT） http://www.security-next.com/058178 ● フィルタリング製品が不正なルート証明書を使用 - 秘密鍵が漏洩（Security NEXT） http://www.security-next.com/057878 ● YouTube にビデオを削除されてしまう脆弱性、Google が即修正（IT media） http://www.itmedia.co.jp/enterprise/articles/1504/02/news044.html ● 「BGA32.DLL」に脆弱性、使用停止を、「QBga32.DLL」では最新バージョンで修正（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/20150519_702645.html ● 脆弱性取り扱いのガイドライン 2015 年版を公開、経産省告示の改正を反映(IPA、JPCERT/CC)（Scan NetSecurity） http://scan.netsecurity.ne.jp/article/2015/05/25/36448.html ● 産業制御システムで使用される PLC の脆弱性を標的としたアクセスの観測について（警察庁セキュリティポータル） http://www.npa.go.jp/cyberpolice/topics/?seq=16382

5. ゼロデイ攻撃

関連記事	● Adobe が Flash の緊急パッチを公開、ゼロデイ攻撃も発生（IT media） http://www.itmedia.co.jp/enterprise/articles/1506/24/news053.html ● 2014 年のゼロデイ脆弱性は 24 件 - ゼロデイ期間が前年比 15 倍に（Security NEXT） http://www.security-next.com/057659 ● 「Duqu 2.0」が標的型サイバー攻撃に利用したゼロデイ脆弱性「CVE-2015-2360」の解析（トレンドマイクロ） http://blog.trendmicro.co.jp/archives/11710

6. POS

関連記事	● 決済カード情報を盗む新手の POS マルウェア、スパムメールで感染拡大（IT media） http://www.itmedia.co.jp/news/articles/1505/27/news045.html ● 米国のホテルやサービス業を狙う POS マルウェア「MalumPoS」を確認（トレンドマイクロ） http://blog.trendmicro.co.jp/archives/11640 ● POS システム狙う RAM スクレイパーが増加、Verizon がデータ漏洩／侵害の年次（INTERNET Watch） http://internet.watch.impress.co.jp/docs/column/security/20150506_700636.html ● POS マルウェア「FighterPOS」、ブラジルで 2 万件以上のクレジットカード情報を窃取（トレンドマイクロ） http://blog.trendmicro.co.jp/archives/11301

7. マルウェア

関連記事	● マルウェア攻撃への投資、平均リターン率は 1425% (スラド) http://security.srad.jp/story/15/06/17/1942238/ ● ステガノグラフィを利用する不正プログラム、米国の医療関連企業を中心に感染を確認（ZDNet Japan） http://blog.trendmicro.co.jp/archives/11799 ● 複合機の通知を偽装したメールがマクロ型不正プログラムを頒布、日本でも被害 (トレンドマイクロ) http://blog.trendmicro.co.jp/archives/11776 ● 欧州当局、マルウェアを呼び込むボットネットを摘発　世界で感染も拡大（IT media） http://www.itmedia.co.jp/news/articles/1504/13/news040.html ● オープンソース SSH クライアント「PuTTY」、トロイの木馬版が見つかる--データ窃盗の恐れ（ZDNet Japan） http://japan.zdnet.com/article/35064727/ ● サイト閲覧でマルウェア感染か、情報流出は確認されず - 新潟県（Security NEXT） http://www.security-next.com/059714 ● 九州歯科大の PC にマルウェア - 警察からの指摘で判明（Security NEXT） http://www.security-next.com/059914 ● 米英などの情報機関、「Android」スマホのハッキングを過去に計画--米報道 (CNET) http://japan.cnet.com/news/society/35064876/

8. ランサムウェア

関連記事	● ランサムウェアが世界で猛威、感染で 1 万ドルの被害も（IT media） http://www.itmedia.co.jp/enterprise/articles/1506/25/news047.html ● スパムメール型のランサムウェアがイタリアとスペインのユーザを標的に（セキュアブログ） http://blog.f-secure.jp/archives/50748550.html ● 活発化する「Crypto ランサムウェア」（トレンドマイクロ） http://blog.trendmicro.co.jp/archives/11739 ● パッチ提供までの遅延を狙うゼロデイ攻撃、悪質なランサムウェアが増加(シマンテック) (Scan NetSecurity) http://scan.netsecurity.ne.jp/article/2015/04/16/36203.html ● 脅迫するランサムウェア、日本や韓国への攻撃を本格始動（IT media） http://www.itmedia.co.jp/enterprise/articles/1504/24/news135.html ● 「 パソコン内のファイルを人質にとるランサムウェアに注意！ 」 メッセージが流暢な日本語になるなど国内流行の懸念（IPA） http://www.ipa.go.jp/security/txt/2015/06outline.html ● 身代金ウイルスの被害を多数確認、Windows や Flash の脆弱性を突いて感染（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/20150526_703863.html

9. Microsoft

関連記事	● Windows XP サポート終了から 1 年も、依然多くのユーザーが利用（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/20150413_697447.html ● Flash と Windows の脆弱性を突くコンボ攻撃発生、Windows の脆弱性は未解決（IT media） http://www.itmedia.co.jp/enterprise/articles/1504/21/news037.html ● Microsoft、「Spartan」ブラウザの脆弱性報告に報奨金を進呈（IT media） http://www.itmedia.co.jp/enterprise/articles/1504/23/news058.html ● Windows Server 2003 サポート終了目前　それでも移行が遅れる理由（IT media） http://www.itmedia.co.jp/enterprise/articles/1505/20/news045.html ● Windows 10 ではホームユーザーへの月例更新が廃止され、更新プログラムは随時配布に（スラド） http://security.slashdot.jp/story/15/05/05/2121228/

10. Adobe

関連記事	● 2011 年に確認済の脆弱性「CVE-2011-2461」が抱えるリスク（トレンドマイクロ） http://blog.trendmicro.co.jp/archives/11245 ● Adobe、「Reader/Acrobat」の脆弱性 34 件を修正 - パッチ適用優先度を引き上げ（Security NEXT） http://www.security-next.com/058342 ● 5 月の UD で修正された「Flash Player」脆弱性の悪用を確認 - 緩和策の回避も（Security NEXT） http://www.security-next.com/058796 ● Adobe、メジャーUD「Photoshop CC 2015」で脆弱性 4 件を修正（Security NEXT） http://www.security-next.com/059560

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. 2015 年 4 月の世界の月間マルウェアランキングを公開

プレス リリース	● マルウェアランキング(世界のランキング) (ESET) http://canon-its.jp/product/eset/topics/malware1504.html

2. 2015 年 4 月の日本の月間マルウェアランキングを公開

プレス リリース	● マルウェアランキング(日本のランキング) (ESET) http://canon-its.jp/product/eset/topics/malware1504_jp.html

3. 2015 年 5 月の世界の月間マルウェアランキングを公開

プレス リリース	● マルウェアランキング(世界のランキング) (ESET) http://canon-its.jp/product/eset/topics/malware1505.html

4. 2015 年 5 月の日本の月間マルウェアランキングを公開

プレス リリース	● マルウェアランキング(日本のランキング) (ESET) http://canon-its.jp/product/eset/topics/malware1505_jp.html

5. 2015 年 4 月のウイルスレビュー

関連記事	● 2015 年 4 月のウイルスレビュー (Dr. WEB) http://news.drweb.co.jp/?i=867

6. 2015 年 4 月の Android マルウェア

関連記事	● 2014 年 4 月のモバイル Android マルウェア (Dr. WEB) http://news.drweb.co.jp/?i=866

7. 2015 年 5 月のウイルスレビュー

関連記事	● 2015 年 5 月のウイルスレビュー (Dr. WEB) http://news.drweb.co.jp/?i=874

8. 2015 年 5 月の Android マルウェア

関連記事	● 2014 年 5 月のモバイル Android マルウェア (Dr. WEB) http://news.drweb.co.jp/?i=875

9. 2015 年 6 月のウイルスレビュー

関連記事	● 2015 年 6 月のウイルスレビュー (Dr. WEB) http://news.drweb.co.jp/?i=889

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＜2015.04.07＞

プレス リリース	● チェックしておきたい脆弱性情報＜2015.04.07＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/040300050/

2. チェックしておきたい脆弱性情報＜2015.04.13＞

プレス リリース	● チェックしておきたい脆弱性情報＜2015.04.13＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/040300052/

3. チェックしておきたい脆弱性情報＜2015.04.22＞

プレス リリース	● チェックしておきたい脆弱性情報＜2015.04.22＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/041900054/

4. チェックしておきたい脆弱性情報＜2015.04.27＞

プレス リリース	● チェックしておきたい脆弱性情報＜2015.04.27＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/041900055/

5. チェックしておきたい脆弱性情報＜2015.05.13＞

プレス リリース	● チェックしておきたい脆弱性情報＜2015.05.13＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/051000057/

6. チェックしておきたい脆弱性情報＜2015.05.15＞

プレス リリース	● チェックしておきたい脆弱性情報＜2015.05.15＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/051000058/

7. チェックしておきたい脆弱性情報＜2015.05.19＞

プレス リリース	● チェックしておきたい脆弱性情報＜2015.05.19＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/051000059/

8. チェックしておきたい脆弱性情報＜2015.06.03＞

プレス リリース	● チェックしておきたい脆弱性情報＜2015.06.03＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/052900062/

9. チェックしておきたい脆弱性情報＜2015.06.08＞

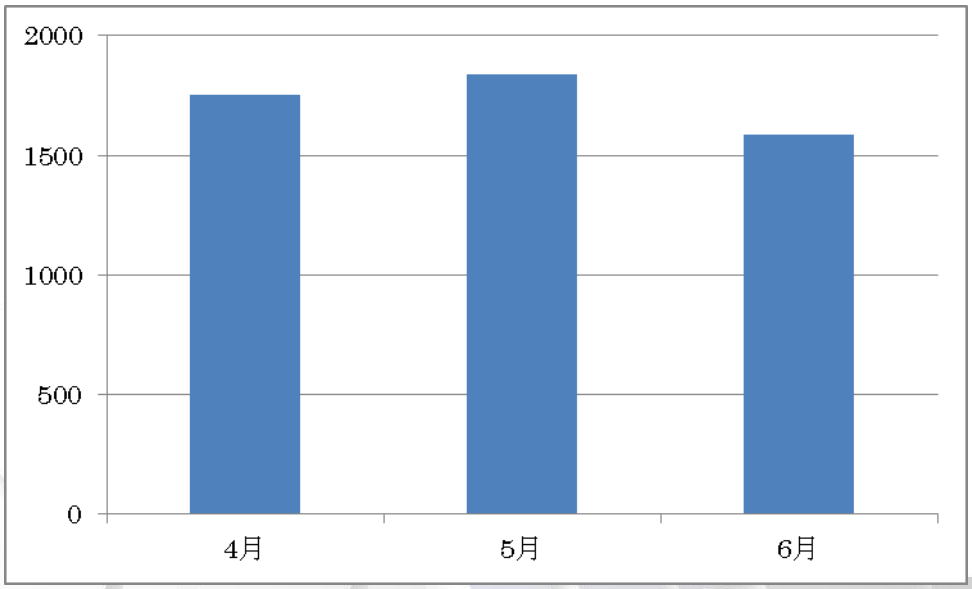
プレス リリース	● チェックしておきたい脆弱性情報＜2015.06.08＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/053100063/

10. チェックしておきたい脆弱性情報＜2015.06.15＞

プレス リリース	● チェックしておきたい脆弱性情報＜2015.06.15＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/053100064/

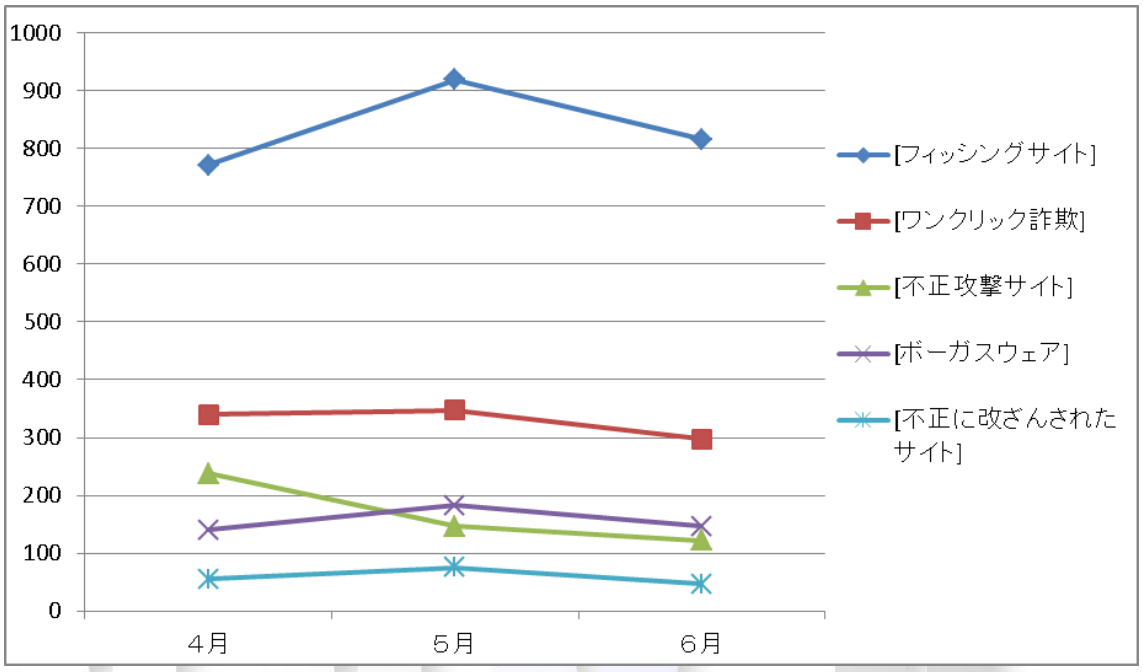
5. データからみるサイバー犯罪の傾向

インターネットユーザがウェブサイトの安全性を確認できるウェブサイトセキュリサービス*のデータをもとにしたサイバー犯罪の傾向を以下に示します。



「危険な可能性」と判断されたウェブサイトの件数

* 株式会社セキュアブレインが提供する無料ウェブセキュリティサービス「gred でチェック」(http://check.gred.jp/)



脅威別検知数の月別推移(2015 年 4 月～6 月)

今期の「危険な可能性」と判断されたウェブサイトの件数を見ると 2000 件以下となっており、前期と比べて大幅な増加や減少は見受けられませんでした。また、脅威別検知数の月別推移によると不正攻撃サイトは、2015 年第 1 四半期(1 月:137 件、2 月:230 件、3 月:194 件)と比較し今期は減少傾向となっています。また、フィッシングサイトは銀行を標的としたものが多発したことから 5 月に増加していることが見受けられます。

6. 総括

今期は日本年金機構の年金個人情報流出事件が 125 万件の個人情報を流出させたとして世間を騒がせました。これは、職員の一人が受信したメールの添付ファイルを開封し、ウイルスに感染したことが発端でした。個人情報が流出した原因は、規定されていた運用形態と異なり個人情報データをインターネットに接続された PC にコピーして作業を行っていたからです。また、感染が発覚した後の対応も遅く被害が深刻化したと報道されています。さらに、流出した 125 万件のデータのうち 55 万件にはパスワードが未設定であったことも問題視されています。本事件では、業務上の利便の為に規定されていた運用形態をとっていなかったことが大きな被害に繋がりました。各社、規定されている運用形態を現場が守れているかどうかの再確認が求められます。

また、同じ個人情報の流出事件として米政府職員の個人情報 400 万件が流出する事件がありました。こちらの事件では、流出した個人情報の多さもさることながら流出した情報の重要性から年金機構の流出事件よりも深刻ではないかという声もありました。流出した中でも問題視されているのは国家の機密情報に触れる人物の身元を調査した質問票です。これが流出する事によって、様々な標的型攻撃の的になる危険性があります。

次に、PC などのデータを勝手に暗号化して金銭を要求するランサムウェアの感染が日本でも目立ってきました。ランサムウェアは 2014 年に欧米地域で感染を広げており年末には日本語で脅迫文を表示するタイプが出現していました。さらに、最近では流暢な日本語も用いられているため注意が必要です。

日本年金機構の事件を始めとしたセキュリティ事故を完全に防ぐことは困難です。そのため、セキュリティ事故を起こしてしまった場合の対策が求められます。

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