S.S.R.C.定期
トレンドレポート
Vol.28

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.28

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 2016 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:2016/4/1～2016/6/30

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. Microsoft

関連記事	● Microsoft サービスでアカウント乗っ取りの問題報告（IT media） http://www.itmedia.co.jp/enterprise/articles/1604/06/news061.html ● MS「Office」、一部パッチが米国時間第 1 火曜日に配布 (CNET Japan) http://japan.cnet.com/news/service/35080958/ ● Microsoft の月例セキュリティ情報公開（IT media） http://www.itmedia.co.jp/news/articles/1604/13/news056.html ● サポートが切れても生き残り続ける Windows XP (マイナビニュース) http://news.mynavi.jp/news/2016/04/12/154/ ● PowerShell、Windows マルウェア開発ツールとして悪用の傾向 (マイナビニュース) http://news.mynavi.jp/news/2016/04/19/197/ ● 3 月に修正された Windows の脆弱性に悪用のおそれ (Security NEXT) http://www.security-next.com/069372 ● Windows Server 2003 の機能を悪用する攻撃、初の確認 (IT media) http://www.itmedia.co.jp/enterprise/articles/1604/28/news074.html ● MS、セキュリティ更新 16 件を公開　一部脆弱性にゼロデイ攻撃も (Security NEXT) http://www.security-next.com/069721 ● 管理不備の「MS SQL Server」狙うアクセスが増加（Security NEXT） http://www.security-next.com/069653 ● Microsoft、安易なパスワードを使用禁止　攻撃にも対抗措置 (IT media) http://www.itmedia.co.jp/enterprise/articles/1605/27/news063.html

	● 外交機関を狙った新たなサイバースパイ組織「Danti」、既存の脆弱性を悪用し、世界中の組織を標的に（Kaspersky） http://www.kaspersky.co.jp/about/news/virus/2016/vir02062016 ● Microsoft の月例セキュリティ情報を公開、「緊急」は 5 件 (IT media) http://www.itmedia.co.jp/news/articles/1606/15/news070.html ● MS の駆除ツール、拡大懸念される不正送金マルウェア「Gozi」に対応 (Security NEXT) http://www.security-next.com/071046

2. Apple

関連記事	● Siri を使ってパスコードをかわされる脆弱性、Apple が修正 (IT media) http://www.itmedia.co.jp/enterprise/articles/1604/07/news063.html ● 暗号化解除をめぐる米法案、司法当局へのバックドア提供を義務付け (IT media) http://www.itmedia.co.jp/news/articles/1604/09/news022.html ● OS X のランサムウェア「KeRanger」が映す、凶悪化するマルウェアの姿 (DZNet Japan) http://japan.zdnet.com/article/35081411/ ● アップル、「iOS 9.3.2」を公開 セキュリティ上の問題などに対処 (CNET Japan) http://japan.cnet.com/news/service/35082697/ ● 「macOS Sierra」の「Safari 10」ブラウザ、「Flash」をデフォルトで無効に (DZNet Japan) http://japan.zdnet.com/article/35084338/

3. Adobe

関連記事	● 更新：Adobe Flash Player の脆弱性対策について（IPA） https://www.ipa.go.jp/security/ciadr/vul/20160406-adobeflashplayer.html ● Adobe Creative Cloud のデスクトップアプリに脆弱性 (Security NEXT) http://www.security-next.com/068843 ● 「Adobe Acrobat/Reader」が脆弱性 92 件を修正 ゼロデイ攻撃は未確認 (Security NEXT) http://www.security-next.com/069713 ● 【速報】Adobe Flash Player の更新が公開　ゼロデイ脆弱性含む 25 件を修正 (Security NEXT) http://www.security-next.com/069828 ● 5 月実施の「Flash Player」更新 実際は 31 件を解消 (Security NEXT) http://www.security-next.com/070689 ● エクスプロイトキットの標的となる脆弱性、上位 10 種は「Flash Player」関連 (Security NEXT) http://www.security-next.com/070932 ● 更新：Adobe Flash Player の脆弱性対策について（IPA） https://www.ipa.go.jp/security/ciadr/vul/20160615-adobeflashplayer.html

4. Android

関連記事	● Google、Android の月例セキュリティ情報を公開　深刻な脆弱性が多数存在 (IT media) http://www.itmedia.co.jp/enterprise/articles/1606/07/news064.html ● 97%の Android 端末にルート化の恐れ、深刻な脆弱性 (TREND Micro) http://blog.trendmicro.co.jp/archives/13168 ● グーグル、「Android」セキュリティレポート 2015 年版を公開 課題はパッチの適用（DZNet Japan） http://japan.zdnet.com/article/35081626/ ● 古い Android は「XP 状態」、ランサムウェア感染攻撃を確認 (IT media) http://www.itmedia.co.jp/enterprise/articles/1604/26/news071.html ● Android に 5 年前から存在する脆弱性、履歴データなど窃取の危険性 (マイナビニュース) http://news.mynavi.jp/news/2016/05/07/044/ ● ハッキングされた Android ゲーム内に潜むバンキングトロイの木馬 (Dr. WEB) http://news.drweb.co.jp/show/?i=1020 ● Google、Android の月例セキュリティ情報を公開 (IT media) http://www.itmedia.co.jp/enterprise/articles/1606/07/news064.html

5. 情報漏洩

関連記事	● ［詳報］JTB を襲った標的型攻撃（IT pro） http://itpro.nikkeibp.co.jp/atcl/column/14/346926/061500549/ ● ホームページへの不正アクセスが判明、約 43 万件の個人情報が流出の恐れ (Scan Net Security) http://scan.netsecurity.ne.jp/article/2016/04/22/38400.html ● J WAVE に不正アクセスゼロデイ攻撃で個人情報が流出した可能性 (Security NEXT) http://www.security-next.com/069210 ● B2B 卸の「NETSEA」、約 13 万件の個人情報を流出（IT pro） http://itpro.nikkeibp.co.jp/atcl/news/16/042601241/ ● コマンドインジェクション脆弱性を悪用した不正アクセス攻撃により約 35 万件の個人情報が流出の可能性 (Scan Net Security) http://scan.netsecurity.ne.jp/article/2016/05/04/38437.html ● アンダーグラウンドのハッキングフォーラムから個人情報が流出 (マイナビニュース) http://news.mynavi.jp/news/2016/05/18/081/ ● 米リンクトイン、1 億件超のパスワードを無効化　外部流出の恐れ (REUTERS) http://jp.reuters.com/article/linkedin-password-idJPKCN0YA0HG ● Acer の米通販サイトに不正アクセス、クレジットカード情報が流出 (IT media) http://www.itmedia.co.jp/enterprise/articles/1606/21/news063.html ● 店舗情報 6116 件や会員情報 62 万件の流出があらたに判明 GMO メイクショップ (Security NEXT) http://www.security-next.com/071245

	● 「スパイラル EC」の脆弱性が悪用され「ViVi」通販サイトで会員情報流出、同一プラットフォーム利用の他社で最大 42 サイト約 98 万件に拡大するおそれ (Scan Net Security) http://scan.netsecurity.ne.jp/article/2016/06/24/38628.html ● 学校教育ネットワークに不正アクセス、約 1 万人分の生徒の個人情報が流出 (Scan Net Security) http://scan.netsecurity.ne.jp/article/2016/06/28/38639.html

6. 脆弱性

関連記事	● Oracle の定例アップデート公開、データベースや Java に深刻な脆弱性 (IT media) http://www.itmedia.co.jp/enterprise/articles/1604/20/news063.html ● シマンテックのメールセキュリティ製品に複数の脆弱性（Security NEXT） http://www.security-next.com/069173 ● 「Apache Struts 2」の脆弱性への攻撃確認、送信元は中国や米国 (Scan Net Security) http://scan.netsecurity.ne.jp/article/2016/05/02/38433.html ● 「OpenSSL」に複数の重大な脆弱性、アップデートを呼びかけ (Scan Net Security) http://scan.netsecurity.ne.jp/article/2016/05/10/38445.html ● WordPress へフォームを設置するプラグインに深刻な脆弱性（Security NEXT） http://www.security-next.com/069938 ● VMware、深刻な脆弱性に対処したアップデートをリリース（Security NEXT） http://www.security-next.com/070022 ● 企業向け「ウイルスバスター」に LAN 環境から攻撃が可能となる脆弱性 (Security NEXT) http://www.security-next.com/070240 ● 無料 Wi Fi スポット検索アプリに複数の脆弱性（Security NEXT） http://www.security-next.com/070412 ● サポート終了「Apache Struts 1」に脆弱性（Security NEXT） http://www.security-next.com/070852

7. サイバー攻撃

関連記事	● 「熊本地震」に便乗するサイバー攻撃へ警戒を 標的型攻撃や詐欺サイトなどに注意（Security NEXT） http://www.security-next.com/068948 ● 世界の金融機関に緊張走る サイバー攻撃マルウエアに識別コード (Bloomberg) https://www.bloomberg.co.jp/news/articles/2016-05-17/O7CB3J6TTDTB01 ● 活発な「Pawn Storm 作戦」、独「キリスト教民主同盟」を標的 (TREND Micro) http://blog.trendmicro.co.jp/archives/13328 ● 韓国空軍サイトにサイバー攻撃（JIJI.COM） http://www.jiji.com/jc/article?k=2016052500190 ● 「イルカ・クジラ漁」標的にサイバー攻撃、アノニマスが“宣戦布告” (IT media) http://www.itmedia.co.jp/business/articles/1604/20/news062.html ● 米軍がＩＳにサイバー攻撃　司令官装い偽指示も　ＮＹＴ紙が報じる (産経ニュース) http://www.sankei.com/world/news/160425/wor1604250011-n1.html

8. ランサムウェア

関連記事	● 病院でランサムウェア感染被害が横行、診療にも支障（IT media） http://www.itmedia.co.jp/enterprise/articles/1604/01/news065.html ● アダルトサイトから感染する Android ランサムウェアが日本に上陸 (マイナビニュース) http://news.mynavi.jp/news/2016/04/05/084/ ● JBoss サーバ経由でランサムウェアに感染させる手口が横行、対応策は？ (IT media) http://www.itmedia.co.jp/enterprise/articles/1604/19/news061.html ● Flash の脆弱性がランサムウェアの拡散に悪用される (日立ソリューションズ 情報セキュリティブログ) http://securityblog.jp/news/20160421.html ● システムを感染させるためにマルウェアが使う PowerShell (McAfee) http://blogs.mcafee.jp/mcafeeblog/2016/05/powershell-b29b.html ● ワーム型ランサムウェア「ZCryptor」が登場 USB メモリなどで拡散 (Security NEXT) http://www.security-next.com/070596 ● 「CryptXXX」が進化、LAN 上の共有フォルダをスキャン データ窃取機能も (Security NEXT) http://www.security-next.com/070734 ● カナダの大学、ランサムウェア感染で約 168 万円の身代金を支払う （IT media） http://www.itmedia.co.jp/enterprise/articles/1606/09/news059.html ● 暗号化型ランサムウェア「JIGSAW」、顧客サポートを開始、支払いを促す (TREND Micro) http://blog.trendmicro.co.jp/archives/13459 ● 新型ランサムウェア出現、“ZIP パスワード”でファイルを人質に（IT media） http://www.itmedia.co.jp/enterprise/articles/1606/28/news071.html

9. フィッシング

関連記事	● セゾンカードの偽サイトに注意　「暫定的に ID 変更」と不安煽る (Security NEXT) http://www.security-next.com/068757 ● ゆうちょ銀行のフィッシング　「パスワード変更通知」を偽装 (Security NEXT) http://www.security-next.com/068779 ● Apple からの「アカウントがロックされます」偽メールが出回る (Scan Net Security) http://scan.netsecurity.ne.jp/article/2016/05/21/38490.html ● 「個人情報を家族や友人にばらす」 - 金銭要求する脅迫メール (Security NEXT) http://www.security-next.com/070570 ● 電通大に不正アクセス　フィッシングメール 280 万件送信（IT media） http://www.itmedia.co.jp/news/articles/1606/06/news109.html ● ガンホーゲームズを騙るメールに注意、本文に“流失”のミス (Scan Net Security) http://scan.netsecurity.ne.jp/article/2016/06/29/38648.html ● 「OMC Plus」の偽サイトが稼働中 フィッシング攻撃に注意を (Security NEXT) http://www.security-next.com/071525

10. マルウェア

関連記事	● Linux のボットネット「BillGates」による攻撃が激化 (DZNet Japan) http://japan.zdnet.com/article/35080857/ ● 不正送金関与のマルウェアに注意、金融機関のデータベースから痕跡隠す (IT media) http://www.itmedia.co.jp/enterprise/articles/1604/27/news073.html ● Google のアプリ検証機能をすり抜けるトロイの木馬が登場 (マイナビニュース) http://news.mynavi.jp/news/2016/05/19/088/ ● 国内から 23 番ポートへの不正通信が増加　業務用機器がマルウェア感染 (Security NEXT) http://www.security-next.com/070292 ● ネットバンキング狙うマルウェア、前四半期比 2 倍超に 偽日本郵政メールなどで拡散（Security NEXT) http://www.security-next.com/070365 ● Doctor Web からの警告：システムレジストリ内に潜む「ファイルレス」トロイの木馬 Kovter (Dr. WEB) http://news.drweb.co.jp/show/?i=1027 ● 不正送金マルウェア「Gozi」に警戒を 日本語メールや EK 経由で感染 (Security NEXT) http://www.security-next.com/070979

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. 2016 年 4 月のウイルスレビュー

関連記事	● 2016 年 4 月のウイルスレビュー（Dr. WEB） http://news.drweb.co.jp/?i=1011

2. 2016 年 5 月のウイルスレビュー

関連記事	● 2016 年 5 月のウイルスレビュー（Dr. WEB） http://news.drweb.co.jp/?i=1022

3. 2016 年 6 月のウイルスレビュー

関連記事	● 2016 年 6 月のウイルスレビュー（Dr. WEB） http://news.drweb.co.jp/?i=1038

4. 2016 年 4 月のモバイルマルウェア

関連記事	● 2016 年 4 月のモバイルマルウェア（Dr. WEB） http://news.drweb.co.jp/?i=1010

5. 2016 年 5 月のモバイルマルウェア

関連記事	● 2016 年 5 月のモバイルマルウェア（Dr. WEB） http://news.drweb.co.jp/?i=1021

6. 2016 年 6 月のモバイルマルウェア

関連記事	● 2016 年 6 月のモバイルマルウェア（Dr. WEB） http://news.drweb.co.jp/?i=1040

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＜2016.04.04＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.04.04＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/033100107/

2. チェックしておきたい脆弱性情報＜2016.04.11＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.04.11＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/033100108/

3. チェックしておきたい脆弱性情報＜2016.04.18＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.04.18＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/041400109/

4. チェックしておきたい脆弱性情報＜2016.04.26＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.04.26＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/042200110/

5. チェックしておきたい脆弱性情報＜2016.04.28＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.04.28＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/042200111/

6. チェックしておきたい脆弱性情報＜2016.05.19＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.05.19＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/051700112/

7. チェックしておきたい脆弱性情報＜2016.05.23＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.05.23＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/051700113/

8. チェックしておきたい脆弱性情報＜2016.05.26＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.05.26＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/051700114/

9. チェックしておきたい脆弱性情報＜2016.06.21＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.06.21＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/062000116/

10. チェックしておきたい脆弱性情報＜2016.06.23＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.06.23＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/062000117/

11. チェックしておきたい脆弱性情報＜2016.06.28＞

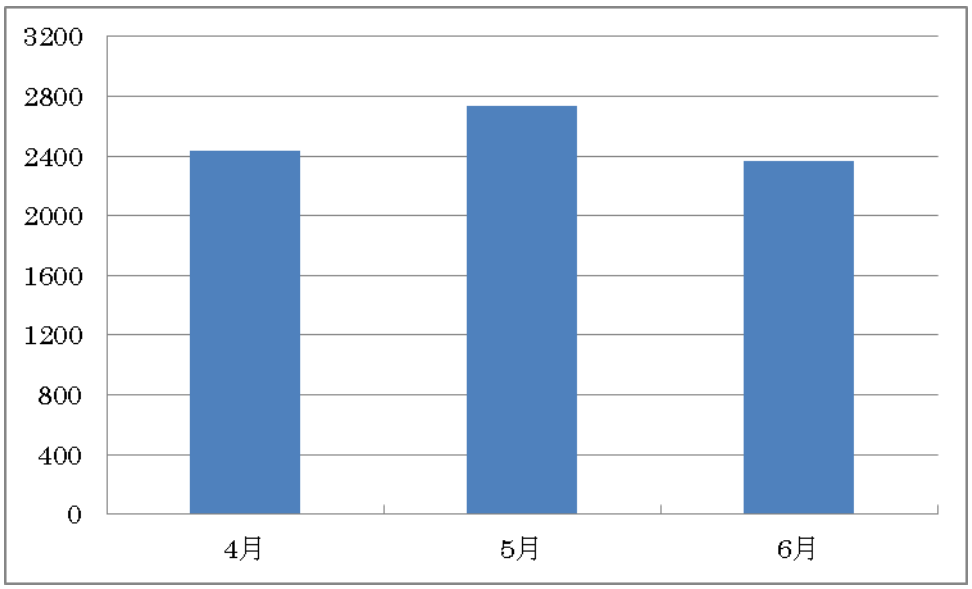
プレス リリース	● チェックしておきたい脆弱性情報＜2016.06.28＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/062000118/

12. チェックしておきたい脆弱性情報＜2016.06.30＞

プレス リリース	● チェックしておきたい脆弱性情報＜2016.06.30＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/062000119/

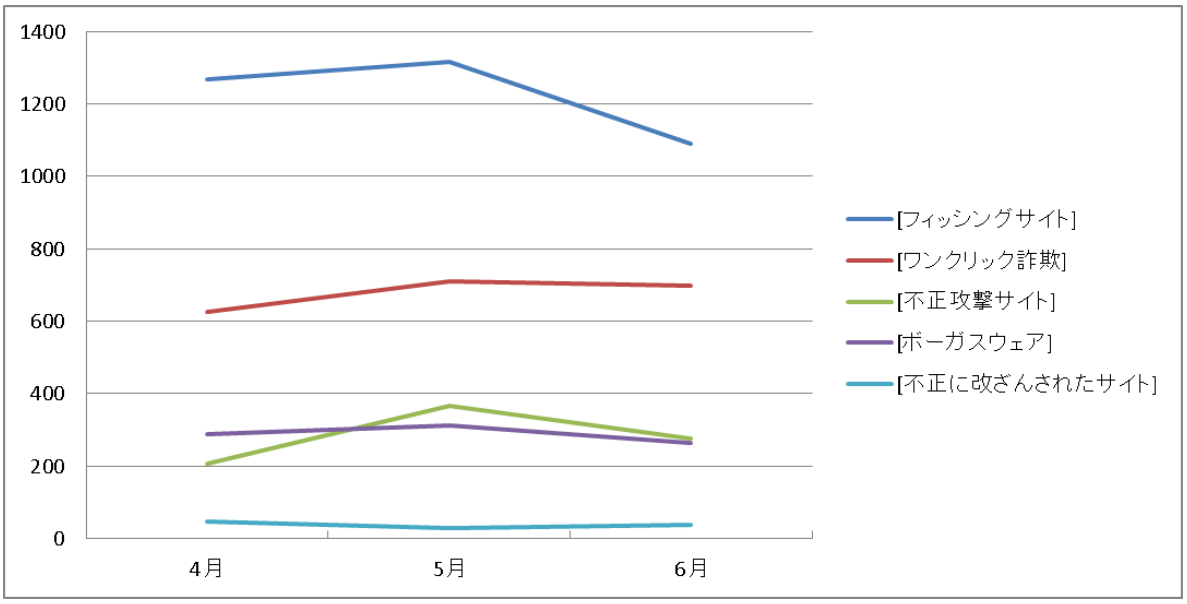
5. データからみるサイバー犯罪の傾向

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(2016 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は、前期の平均と比較すると 4 月と 6 月は 400 件、5 月は 800 件近く増えております。これは、脅威別検知数の月別推移におけるワンクリック詐欺の項目で前期の平均と比較すると、今期の平均は 400 件近く増加していることが原因です。毎期のワンクリック詐欺の項目では、動画サイトが多く検出されています。特に、今期に増加したワンクリック詐欺の大半が、特定の動画サイトを用いる傾向にありました。また、不正攻撃サイトの項目で前期の平均と比較すると、4 月は 100 件、5 月は 300 件、6 月は 200 件近く増加していることも原因です。不正に改ざんされたサイトとボーガスウェアについては、前期から変わらずほぼ横ばいに推移しています。

6. 総括

今期はJTBが不正アクセスによって793万人の個人情報を流出させた可能性があるとして世間を賑わせました。これは、JTBの子会社であるi.JTBの社員が標的型攻撃メールの添付ファイルを開封し、ウイルス感染したことが発端でした。受信した標的型攻撃メールは極めて巧妙であり、過去に取引した企業のメールアドレスになりすましていました。メール自体は、件名に「航空券控え　添付のご連絡」で本文もあり、航空券のeチケットのPDFファイルが添付している、ごく普通の問い合わせメールのようでした。JTBは会見発表した6月14日の時点で、情報流出の事実は確認されておらず、個人情報を悪用された報告もないとしています。2015年に起こった日本年金機構の個人情報流出から、大企業や中堅企業ではセキュリティ対策を強化しています。しかし、本事件のような近年の標的型攻撃メールは非常に巧妙であり、攻撃を完全に防ぐのは難しいです。今後、企業では標的型攻撃を受けても感染を最小限にするシステムや、ウイルスを早急に検知するシステムの導入が重要となります。

前期に引き続き、今期もランサムウェアによる被害が多く報告されています。ランサムウェアは感染したPCのOSの起動をロックおよび、ファイルを暗号化し、元に戻すことと引き換えに身代金を要求してきます。4月には、「Anglet Exploit Kit」などを用いて感染する「cryptXXX」が出現しています。「cryptXXX」は、改ざんされたWebサイトや不正広告を経由して、PCの脆弱性を突き感染します。「cryptXXX」に感染すると、ファイル名に「.crypt」や「.cryp1」などの拡張子が追加されファイルが暗号化します。その後、デスクトップの壁紙やブラウザにファイルを暗号化したことや身代金の支払い方法を表示してきます。ランサムウェアは、身代金を支払っても、データが返ってくる保障はありません。したがって、一度感染するとデータの復旧が非常に困難です。自身のPCやサーバをサイバー攻撃から守るために、データのバックアップおよび、PCやサーバを常に最新の状態にアップデートすることを推奨いたします。

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