株式会社 日立システムズ

SSRC-TR-Vol.21

S.S.R.C.定期
トレンドレポート
Vol.21

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.21

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 2014 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:2014/7/1～2014/9/30

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. bash の脆弱性

関連記事	● 「bash」シェルに重大な脆弱性、主要 Linux でパッチが公開(ITmedia) http://www.itmedia.co.jp/enterprise/articles/1409/25/news042.html ● bash シェルの修正パッチは不完全、脆弱性突く攻撃の報告も(ITmedia) http://www.itmedia.co.jp/enterprise/articles/1409/26/news059.html ● bash の Shellshock 脆弱性を利用するボットネットが出現(Slashdot) http://linux.slashdot.jp/story/14/09/27/0446227/ ● bash の脆弱性で Apple がコメント、「デフォルトの OS X は安全」（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1409/29/news042.html ● bash 0day マルウェア感染の「real time」リバースエンジニアリング（0day.jp） http://blog.0day.jp/2014/09/bash-0dayreal-time.html ● 「Shellshock」：どのように被害をもたらすか（トレンドマイクロ） http://blog.trendmicro.co.jp/archives/9974 ● Apple、「bash」の脆弱性「ShellShock」に対応する修正パッチを公開（Security NEXT） http://www.security-next.com/052395

2. LINE

関連記事	● 「LINE」パスワード変更でスタンププレゼント　乗っ取り被害防止で(ITmedia) http://www.itmedia.co.jp/news/articles/1407/04/news064.html ● 韓国による LINE 盗聴疑惑、日本のユーザーはどう対処すべきか(ITpro) http://itpro.nikkeibp.co.jp/article/COLUMN/20140627/567263/ ● 中国で LINE・カカオトーク不通　長期化か(Yahoo) http://headlines.yahoo.co.jp/hl?a=20140713-00000008-yonh-kr ● 仲里依紗、ヒャダイン、薬丸……芸能界でも LINE 乗っ取り被害者続出(Yahoo) http://headlines.yahoo.co.jp/hl?a=20140711-00000017-rbb-ent ● LINE 乗っ取り、警視庁が捜査開始、100 件 650 万円の被害確認(INTERNET Watch) http://internet.watch.impress.co.jp/docs/news/20140722_658990.html ● 台湾政府、政府機関での LINE 利用を禁止へ(Slashdot) http://security.slashdot.jp/story/14/09/24/1958209/

3. ベネッセ情報漏洩

関連記事	● ［速報］ベネッセで「進研ゼミ」などの個人情報約 760 万件漏洩、内部者関与の可能性(ITpro) http://itpro.nikkeibp.co.jp/article/NEWS/20140709/570262/

4. ランサムウェア

関連記事	● ファイル暗号化で「脅迫」するランサムウェア、複数の新種を確認（トレンドマイクロ） http://blog.trendmicro.co.jp/archives/9535 ● NAS を人質に身代金 0.6BTC を要求、ランサムウェア「SynoLocker」の攻撃広がる(INTERNET Watch)

	http://internet.watch.impress.co.jp/docs/news/20140813_662143.html ● ランサムウエアによる攻撃が増加中、ファイルを暗号化するタイプも登場(ITpro) http://itpro.nikkeibp.co.jp/atcl/column/14/277462/073100001/

5. 不正ログイン・アクセス

関連記事	● 無印良品のネットショップで約 2 万件の不正ログイン - 約 422 万回の試行(Security NEXT) http://www.security-next.com/051267 ● 「Suica ポイントクラブ」に 30 万件近いアクセス、不正ログインも確認(ScanNetSecurity) http://scan.netsecurity.ne.jp/article/2014/08/19/34690.html ● 大量不正アクセスで停止の「Suica ポイントクラブ」、10 日ぶりに全面再開(PC Online) http://pc.nikkeibp.co.jp/article/news/20140827/1140603/ ● FW 製品のサポートサイトに不正アクセス - 日立ソリューションズ(Security NEXT) http://www.security-next.com/051899 ● JR 東「My JR-EAST」2 万 1000 アカウントに不正ログイン　サービス停止(ITmedia) http://www.itmedia.co.jp/news/articles/1409/12/news165.html ● 約 1 万件の「リクルート ID」で不正ログイン被害 - 約 3 分の 1 でログイン成功(Security NEXT) http://www.security-next.com/052073 ● 法務省サーバーに不正アクセス　一部情報が流出の可能性(産経) http://www.sankei.com/affairs/news/140922/afr1409220027-n1.html ● 宅配便利用者向けサイト「クロネコメンバーズ」で不正ログイン (Security NEXT) http://www.security-next.com/052325

6. POS

関連記事	● POS 端末を狙う新手のマルウェア出現、米国機関がアラート発行（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1408/01/news044.html ● POS システムへの攻撃：正規ソフトの悪用でクレジットカード情報を検証、窃取後はアンダーグラウンド市場で販売(トレンドマイクロ) http://blog.trendmicro.co.jp/archives/9202 ● 新たな POS マルウェア「Backoff」を確認。標的は米国か(トレンドマイクロ) http://blog.trendmicro.co.jp/archives/9605 ● POS 端末を狙うマルウェア、米国で 1000 社以上に感染か(ITmedia) http://www.itmedia.co.jp/enterprise/articles/1408/25/news039.html

7. 標的型攻撃

関連記事	● テンプレートドキュメントを使った標的型攻撃(ITpro) http://itpro.nikkeibp.co.jp/article/COLUMN/20140703/568728/ ● 最大の弱点は「人間」、攻撃者が情報を盗むまでの 6 ステップ(ITpro) http://itpro.nikkeibp.co.jp/article/COLUMN/20140701/567912/ ● 国家レベルの標的型攻撃、製薬業界に照準(ITpro) http://itpro.nikkeibp.co.jp/atcl/column/14/264220/090100009/ ● 巧妙化進む標的型攻撃、対象者を事前調査か - Android 端末もターゲットに(Security NEXT) http://www.security-next.com/052033

8. DDoS

関連記事	● DNS サーバに対する DDoS 攻撃が断続的に発生 - eo 光(Security NEXT) http://www.security-next.com/050154 ● 日本国内のオープンリゾルバを悪用する DDoS 攻撃が発生 - DNS リフレクター攻撃とは異なる手法(Security NEXT) http://www.security-next.com/050711 ● 多様化する「DDoS 攻撃」、国内のホームルーターも踏み台に(ITpro) http://itpro.nikkeibp.co.jp/atcl/column/14/346926/072800020/ ● ソニーの PSN、DDoS 攻撃による接続障害から復旧(CNET Japan) http://japan.cnet.com/news/service/35052853/ ● マルウェア感染による Linux 端末のボット化に注意 - DDoS 攻撃へ悪用されるおそれ(Security NEXT) http://www.security-next.com/051861

9. フィッシング

関連記事	● 7 月のフィッシング報告、前月から 7 割減 - ゲーム関係の攻撃縮小が影響(Security NEXT) http://www.security-next.com/051001 ● Yahoo! JAPAN をかたるフィッシング(2014/08/05) (フィッシング対策協議会) http://www.antiphishing.jp/news/database/yahoojapan20140805.html ● セゾンカードの偽サイトに誘導するフィッシング詐欺メールに注意(INTERNET watch) http://internet.watch.impress.co.jp/docs/news/20140811_661862.html ● 防災科学技術研究所の関連サイトが改ざん - フィッシングの踏み台に(Security NEXT) http://www.security-next.com/051191

	● NTT 西のフレッツ回線名義や ID 騙し取るフィッシング - 追加認証情報が狙いか(Security NEXT) http://www.security-next.com/051853 ● 防災科学技術研究所の関連サイトが改ざん - フィッシングの踏み台に(Security NEXT) http://www.security-next.com/051191 ● 三菱東京 UFJ 銀の利用者狙うフィッシングに注意を(Security NEXT) http://www.security-next.com/052180 ● 一時沈静化した金融機関狙うフィッシングサイトが再度活発に(Security NEXT) http://www.security-next.com/052322

10. 改ざん

関連記事	● グーグルや米ヤフーの偽ドメイン問題、マイクロソフトが対策を発表(ZDNet) http://japan.zdnet.com/security/analysis/35050725/ ● NTT ドコモ利用者狙う偽サイトが出現、見た目もドメイン名も偽装(ITpro) http://itpro.nikkeibp.co.jp/atcl/news/14/072700226/ ● Web サイトの改ざん報告は月平均 400 件、早急な対策実施を(ITpro) http://www.itmedia.co.jp/enterprise/articles/1408/13/news095.html ● 日産の一部サイトが約 2 カ月にわたり改ざん - 外部サイトに誘導(Security NEXT) http://www.security-next.com/051564 ● 指宿市のサイトが不正アクセスで改ざん - 情報漏洩は否定(Security NEXT) http://www.security-next.com/052197

11. 情報漏洩

関連記事	● 法人顧客の従業員情報が流出した可能性、原因調査中 - NTT ドコモ(Security NEXT) http://www.security-next.com/051934 ● Gmail アドレスとパスワード約 500 万件が流出か(ITmedia) http://www.itmedia.co.jp/news/articles/1409/11/news043.html ● JAL マイレージ会員の個人情報流出　最大 75 万件　社内 PC にマルウェア、遠隔操作か(ITmedia) http://www.itmedia.co.jp/news/articles/1409/24/news165.html ● マルウェア感染で顧客情報約 2.1 万件が外部サーバへ - JAL (Security NEXT) http://www.security-next.com/052369 ● ｉＣｌｏｕｄがハッキング被害？　米女優ヌード写真拡散(朝日) http://www.asahi.com/articles/ASG9130WGG91UHBI00C.html ● セレブ写真流出は標的型攻撃が原因――Apple が調査結果を発表(ITmedia) http://www.itmedia.co.jp/news/articles/1409/03/news038.html ● Apple のクック CEO、セキュリティ対策方針を表明――セレブ写真流出で(ITmedia) http://www.itmedia.co.jp/enterprise/articles/1409/09/news051.html ● 「iCloud」ヌード写真流出拡大、新たに 26 人　Apple の対策効かず　捜査も難航か(ITmedia) http://www.itmedia.co.jp/news/articles/1409/25/news049.html

12. ネットバンキング

関連記事	● C 法人ネットバンキングを狙う電子証明書窃取攻撃を解析(トレンドマイクロ) http://blog.trendmicro.co.jp/archives/9417 ● オンラインバンキングの不正送金被害、法人向け対策も加速へ(@IT) http://www.atmarkit.co.jp/ait/articles/1407/22/news037.html ● ネットバンキング不正送金、企業被害の実態(読売) http://www.yomiuri.co.jp/it/security/goshinjyutsu/20140725-OYT8T50279.html ● 日本のオンラインバンキングを狙う「Trojan.Snifula」の新種が出現--シマンテックが警告(ZDNet) http://japan.zdnet.com/security/analysis/35051519/ ● ネットバンキングを狙う「VAWTRAK」が急増 - 検出 8 割が国内(Security NEXT) http://www.security-next.com/051433

13. Microsoft

関連記事	● マイクロソフト、一部製品のサポート終了期限案内を強化--「Windows 7」など(CNET Japan) http://japan.cnet.com/sp/allaboutms/35050573/ ● 「IE」へのパッチ提供、2016 年 1 月から最新版のみに - ブラウザ利用環境の確認を(Security NEXT) http://www.security-next.com/051284 ● XP 終了で慌てている間に、ジワジワ迫る「Vista」と「IE8」の寿命(ITmedia) http://www.itmedia.co.jp/pcuser/articles/1408/25/news084.html ● 次期 OS「Windows 9」に便乗するサイバー犯罪者 - マルウェアや情報詐取に注意(Security NEXT) http://www.security-next.com/051730

14. パスワード強度

関連記事	● ANA マイレージクラブに「英数字 8～16 けた」の新パスワード　数字 4 けたから強化(ITmedia) http://www.itmedia.co.jp/news/articles/1408/18/news129.html ● 危なすぎる数字だけのパスワード、JAL と ANA がユーザー認証を強化(ITpro) http://itpro.nikkeibp.co.jp/atcl/column/14/346926/090100042/

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. 2014 年 7 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/malware1407.html

2. 2014 年 7 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/malware1407_jp.html

3. 2014 年 8 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/malware1408.html

4. 2014 年 8 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/malware1408_jp.html

5. 2014 年 7 月のウイルス脅威

関連記事	● 2014 年 7 月のウイルス脅威（Dr.WEB） http://news.drweb.co.jp/?i=765&c=1&lng=ja&p=1

6. 2014 年 8 月のウイルス脅威

関連記事	● 2014 年 8 月のウイルス脅威（Dr.WEB） http://news.drweb.co.jp/?i=781&c=1&lng=ja&p=0

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＜2014.07.04＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.07.04＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20140703/568729/

2. チェックしておきたい脆弱性情報＜2014.07.16＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.07.16＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/071400001/

3. チェックしておきたい脆弱性情報＜2014.07.17＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.07.17＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/071400004/

4. チェックしておきたい脆弱性情報＜2014.07.18＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.07.18＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/071400005/

5. チェックしておきたい脆弱性情報＜2014.07.23＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.07.23＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/071800006/

6. チェックしておきたい脆弱性情報＜2014.07.24＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.07.24＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/071800007/

7. チェックしておきたい脆弱性情報＜2014.07.28＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.07.28＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/072300008/

8. チェックしておきたい脆弱性情報＜2014.08.27＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.08.27＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/082500010/

9. チェックしておきたい脆弱性情報＜2014.08.28＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.05.22＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/082500013/

10. チェックしておきたい脆弱性情報＜2014.08.29＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.08.29＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/082500015/

11. チェックしておきたい脆弱性情報＜2014.09.19＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.09.19＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/091800016/

12. チェックしておきたい脆弱性情報＜2014.09.22＞

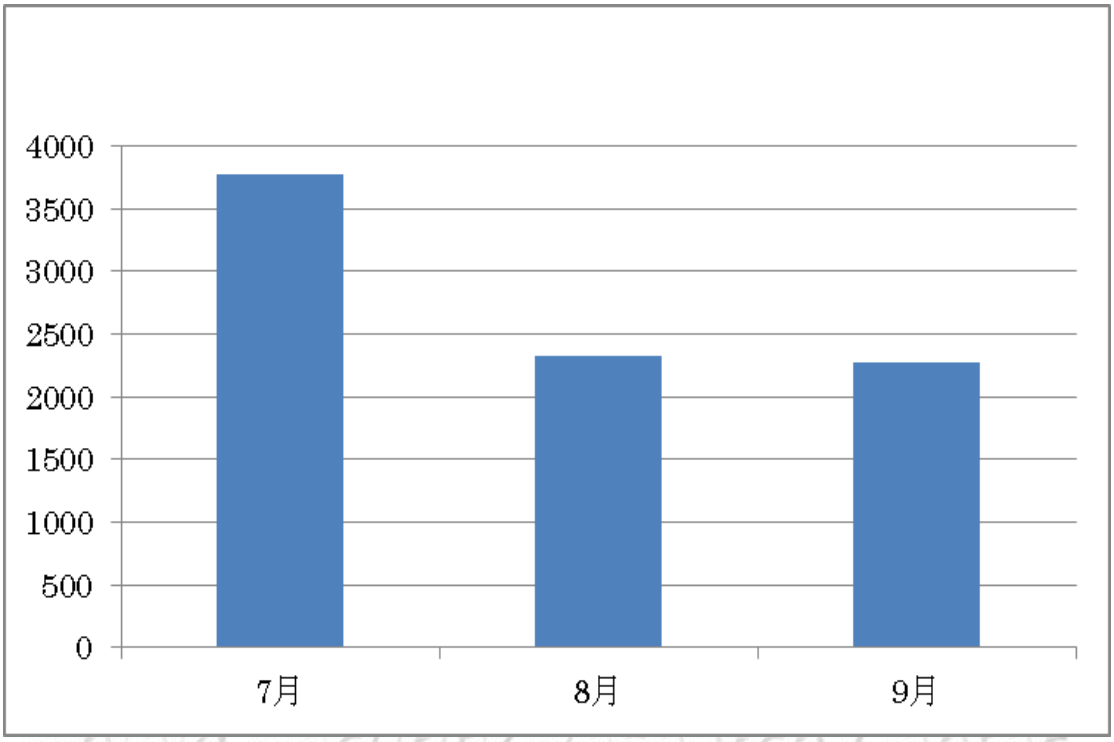
プレス リリース	● チェックしておきたい脆弱性情報＜2014.09.22＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/091800017/

13. チェックしておきたい脆弱性情報＜2014.09.30＞

プレス リリース	● チェックしておきたい脆弱性情報＜2014.09.30＞ http://itpro.nikkeibp.co.jp/atcl/column/14/268561/092900018/

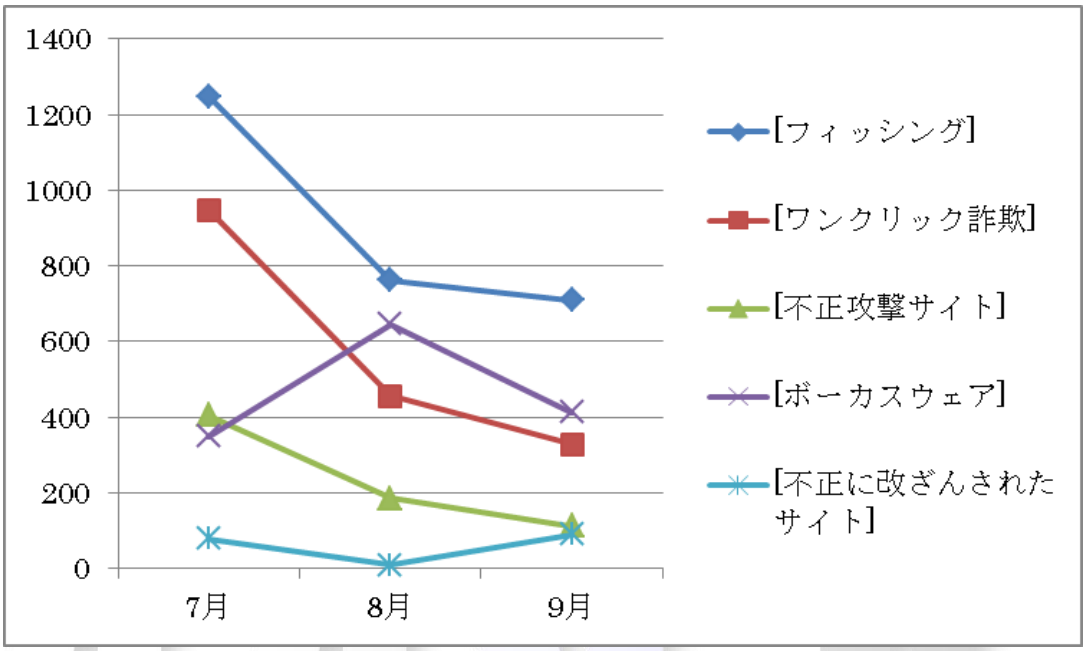
5. データからみるサイバー犯罪の傾向

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(2014 年 7 月～9 月)

今期のサイバー犯罪の傾向としては、7 月にフィッシングとワンクリック詐欺が数多く報告されました。これらは、2014 年第 2 四半期度に発生した金融機関や、オンラインゲームの運営をかたるフィッシングの影響が未だに残っていためだと考えられます。8 月、9 月とフィッシングとワンクリック詐欺ともに減少傾向にあります。8 月に入ると、ボーカスウェアが増加傾向にありますが、その他の攻撃に関しては減少傾向にあります。9 月は不正に改ざんされたサイトの増加が確認されました。

総括

今期は Shellshock と呼ばれる影響範囲の大きい脆弱性が発見され、世間を騒がせました。本脆弱性は、Bash における環境変数の処理における問題です。特定のアプリケーションやソフトウェアでは、Bash 経由で環境変数を操作するため、リモートで攻撃が可能となる場合があります。特に、Bash をシステムシェルとして設定されている場合には注意が必要です。Bash をシステムシェルとして設定されている OS が多く存在するため、Heartbleed を上回る影響力があるとも言われています。また、現在も対策されていない OS が多数あるため十分な注意が必要です。

次に、LINE に不正ログインされアカウントが乗っ取られたユーザから、他のユーザへ、電子マネーをだまし取る詐欺の被害が相次ぎました。弱い強度のパスワードを用いる、モバイル端末だけではなく PC からのアクセスも許可していたため、攻撃者にアカウントを騙し取られてしまいました。LINE は対策として PIN コードの義務付けを行いました。その後も、Gmail アドレスとパスワードの流出、JAL の個人情報流出、iCloud 上のデータ流出などに代表される情報流出の事件が数多く報告されました。それに伴い、今後は企業側も不正ログイン・アクセス対策の更なる強化を実施いていくことが予想されます。既に、ANA マイレージクラブでは、これまで使用していた数字 4 桁のパスワードから「英数字 8 - 16 けた」の新パスワードに変更するなど、対策を行っている企業もあります。

また、これまでと同様に標的型攻撃、DDoS 攻撃、フィッシング、POS などにおいても新たなマルウェアが発見され、引き続き被害が報告されていますので、十分注意する必要があります。

これらの脆弱性やサイバー攻撃の経緯を踏まえて、再度、管轄下のサーバ対策ができているか、パスワード強度が適切であるかなどの確認を行う事を推奨いたします。

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