株式会社 日立システムズ

SSRC-TR-Vol.18

S.S.R.C.定期
トレンドレポート
Vol.18

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.18

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 2013 年第 4 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:2013/10/1～2013/12/31

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. Adobe、ハッカー侵入による顧客情報漏えい

関連記事	● アドビに不正アクセス--290 万人分の顧客情報が漏えいか（CNET Japan） http://japan.cnet.com/news/business/35038037/ ● 米アドビへのハッカー侵入、当初発表より被害広範囲（ロイター） http://jp.reuters.com/article/topNews/idJPTYE99T00H20131030 ● Adobe から流出したパスワードでの Facebook への不正アクセスが判明（Gigazine） http://gigazine.net/news/20131112-after-adobe-breach/ ● Facebook 社、流出した Adobe のアカウント情報（ID / Password）と同じアカウントを一時停止（Sophos） http://www.sophos.com/ja-jp/press-office/press-releases/2013/11/ns-facebook-locks-accounts-using-same-passwordsemails-on-adobe.aspx ● Adobe ライセンスキー送付を装う詐欺を確認、添付は開かず削除を（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1312/24/news037.html

2. 企業や機関の Web サイト改ざん被害

関連記事	● 神奈川工科大のウェブサイトが改ざん - 閲覧でウイルス感染のおそれ（Security NEXT） http://www.security-next.com/044968 ● ウェブサイトが改ざん被害、閲覧でウイルス感染のおそれ - NTT データ MSE

	(Security NEXT) http://www.security-next.com/044946 ● ドン・キホーテの Web サイトが改ざん被害 - 訪問者はウイルス感染の恐れ（マイナビニュース） http://news.mynavi.jp/news/2013/12/11/066/ ● 弊社 Web サイト改ざんに関するお詫びとご報告（株式会社キーエンス） http://www.keyence.co.jp/PDF/keyence_131220.pdf

3. ネットバンキングに関する不正送金事件

関連記事	● ネットバンキング被害 7 億 6000 万円、予防のウイルス対策を官民連携で（総務省）（So-net セキュリティ通信） http://security-t.blog.so-net.ne.jp/2013-10-22 ● ネットバンキングの情報盗む「BANCOS」が急増、IPA の 3Q 報告書（ITPro） http://itpro.nikkeibp.co.jp/article/NEWS/20131024/513302/ ● 不正送金 日本 インターポールを通じてロシアに捜査協力を要請（The Voice of Russia） http://japanese.ruvr.ru/2013_10_22/123219542/ ● 東ヨーロッパのオンライン銀行を狙う一連の攻撃「Apollo」について（TrendMicro） http://blog.trendmicro.co.jp/archives/8030 ● ネットバンキングに係る不正アクセス被害の防止対策について（警視庁） http://www.keishicho.metro.tokyo.jp/haiteku/haiteku/haiteku428.htm ● ネット銀不正送金、県警初摘発 標的が地方に拡大か（徳島新聞） http://www.topics.or.jp/localNews/news/2013/11/2013_13850816214753.html ● 不正送金、「足跡」隠す手口が巧妙に ネットバンキング（日本経済新聞） http://www.nikkei.com/article/DGXNASDG1101U_Z11C13A1CC1000/ ● ネットバンキング不正送金被害 11.8 億円 1～11 月、最悪時の 4 倍（日本経済新

	聞) http://www.nikkei.com/article/DGXNASDG1204W_S3A211C1CR8000/

4. 相次ぐ企業サイトへの不正ログイン

関連記事	● 「PR Newswire に不正アクセス、企業のプレスリリースが悪用される恐れ http://blog.prnewswire.com/2013/10/16/customer-security-announcement-2/ http://www.itmedia.co.jp/enterprise/articles/1310/18/news053.html ● 「EC ナビ」の 2 万 8452ID で不正ログイン - ポイントの不正利用は確認されず (株式会社 VOYAGE GROUP) http://voyagegroup.com/news/press/2013/495/ ● セブンネットショッピング　不正アクセスのお知らせとお詫び（株式会社セブンネットショッピング) http://company.7netshopping.jp/2013/10/pc_apology.html ● 【e オリコサービス】不正アクセスについて（株式会社オリエントコーポレーション) http://www.orico.co.jp/information/20131108.html ● 賃貸住宅入居者向けサイトに不正アクセス - クラウド DB 運営会社の顧客情報漏洩が原因（Secuirty NEXT) http://www.security-next.com/044410 ● Apple 情報サイトにハッキング被害、ユーザー情報が流出（ITmedia) http://www.itmedia.co.jp/enterprise/articles/1311/14/news042.html ● GitHub に「総当たり」攻撃、安易なパスワードが破られる（ITmedia) http://www.itmedia.co.jp/enterprise/articles/1311/21/news045.html ● OMC カードの会員サイトに不正ログイン - ポイントの不正交換が発生 (Secuirty NEXT) http://www.cedyna.co.jp/info/20131118.html ● 不正アクセスを受けてログイン制限を実施 - シティーカード（Security NEXT)

	http://www.citibank.co.jp/ccsi/ja/notice/20131216.html ● 信州大：個人情報７８２２人分流出　不正アクセス受け（毎日新聞） http://sp.mainichi.jp/select/news/20131203k0000e040245000c.html ● 「リスト型アカウントハッキングによる不正ログインへの対応方策について（サイト管理者などインターネットサービス提供事業者向け対策集）」の公表（総務省） http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000063.html

5. モバイルデバイスを狙う不正アプリの増加

関連記事	● Google Play で流通する模倣アプリ - 個人情報窃取が目的か（Security NEXT） http://www.security-next.com/044268 ● 電話番号を狙う不審な Android アプリ、韓国ユーザー向けも Google Play 上に多数発見（McAfee） http://www.mcafee.com/japan/security/mcafee_labs/blog/content.asp?id=1380 ● 脆弱性を悪用してアンチウイルスから逃れる新たな Android 向けトロイの木馬（Dr.WEB） http://news.drweb.co.jp/show/?i=680&lng=ja&c=1 ● スマートフォンユーザーを狙うフィッシングとマルウェアの複合型攻撃（Symantec） http://www.symantec.com/connect/ja/blogs-315 ● デジタル署名の信頼揺らぐ？　高度な Android マルウェアが急増（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1312/09/news063.html ● 不審な Android アプリさらに 15 種、謎の目的で Google アカウント ID を外部送信（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/20131218_628289.html ● スマホやタブレットを狙った APT 攻撃が増加中（ITPro） http://itpro.nikkeibp.co.jp/article/IDG/20131219/525907/

6. 日本発の情報セキュリティ国際会議「CODE BLUE」

関連記事	● 「CODE BLUE」は、国内・アジアの人材の国際会議への発表の場および海外との交流の場を日本発で提供することを目的として設立された。 http://scan.netsecurity.ne.jp/article/2013/10/23/32765.html http://www.atpress.ne.jp/view/41548

7. 米国および英国政府による諜報活動に関して

関連記事	● NSA、携帯電話の位置情報を世界的規模で収集か（CNET Japan） http://japan.cnet.com/news/society/35040946/ ● Microsoft もサービス暗号化強化を発表 ― 「政府による違法アクセスは APT 攻撃」（ITmedia） http://www.itmedia.co.jp/news/articles/1312/05/news123.html ● アップルなど米 8 社、個人情報収集の管理強化をオバマ大統領に要請（ロイター） http://jp.reuters.com/article/topNews/idJPTJE9B800T20131209 ● 米英の情報機関、ネットゲームに「潜入」してテロ監視か（CNN） http://www.cnn.co.jp/tech/35041140.html ● NSA、監視対象の追跡にブラウザのクッキーを利用か（CNET Japan） http://japan.cnet.com/news/society/35041268/ ● NSA の通話記録メタデータ収集、違憲の可能性 - 米連邦地裁（CNET Japan） http://japan.cnet.com/news/society/35041492/

8. 海賊版販売サイトへのアクセスを抑止する取り組み

関連記事	● 海賊版 DVD 販売サイト見ようとしたら PC に注意表示・遮断する取り組みが始まる（INTERNET Watch） http://internet.watch.impress.co.jp/docs/news/20131205_626463.html ● 海賊版販売サイトへのアクセスを抑止する取り組みに参画（BB ソフトサービス株式会社）

	http://www.bbss.co.jp/company/news/2013/news_20131206.html

9. 復讐代行サイトに端を発した事件

関連記事	● 復讐代行サイト：運営者を名誉毀損容疑で逮捕　全国初（毎日新聞） http://sp.mainichi.jp/select/news/20131024k0000m040107000c.html ● 「復讐サイト」で互いのストーカー行為に協力　２７歳の女歯科医ら逮捕（msn 産経ニュース） http://sankei.jp.msn.com/affairs/news/131128/crm13112813130008-n1.htm ● 闇サイト　３人で“交換ストーカー”か（NHK ニュース） http://archive.is/apeeo

10. Facebook アカウント乗っ取り被害

関連記事	● IPA、Facebook の"乗っ取り被害"に注意喚起 - 「安易に友達承認しないで」 http://www.ipa.go.jp/security/txt/2013/11outline.html http://news.mynavi.jp/news/2013/11/02/108/

11. フランスの機関から不適切に発行されたデジタル証明書

関連記事	● Google ドメイン用の不正証明書が発行される、各社が失効措置へ（ITmedia） http://www.itmedia.co.jp/news/articles/1312/10/news036.html ● Microsoft、不正な証明書失効の更新プログラムを Windows XP 向けにも提供（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1312/16/news030.html

12. 複合機のセキュリティ設定不十分から、内部文書が誰でも閲覧可能に

関連記事	● 住民票・答案…複合機の蓄積データ、公開状態に（YOMIURI ONLINE） http://www.yomiuri.co.jp/kyoiku/news/20131107-OYT8T00445.htm

	● IPA がオフィス機器のセキュリティに関する注意喚起、「管理者パスワード変更を」（ITPro） http://itpro.nikkeibp.co.jp/article/NEWS/20131111/517225/ ● 複合機からの情報漏洩が相次ぐ　サーバーと同様の対策が必要（ITPro） http://itpro.nikkeibp.co.jp/article/COLUMN/20131122/519972/

13. 脱原発団体にサイバー攻撃 33 団体に計 253 万通の一斉メール

関連記事	● 反原発や脱原発を訴える全国の市民団体に９月中旬から１１月上旬にかけて大量のメールが一斉に送りつけられ、少なくとも３３団体に２５３万通以上届いた。（朝日新聞） http://www.asahi.com/articles/TKY201311090612.html

14. 個人情報抜き取る不正アプリ販売の疑い　ＩＴ会社社長ら逮捕

関連記事	● 不正個人情報抜き取る不正アプリ販売の疑い　ＩＴ会社社長ら逮捕　３７００万人分か（msn 産経ニュース） http://sankei.jp.msn.com/affairs/news/131205/crm13120510210005-n1.htm

15. 日本における水飲み場型攻撃を確認

関連記事	● 日本における水飲み場型攻撃に関する注意喚起（ラック） http://www.lac.co.jp/security/alert/2013/10/09_alert_01.html ● 「IE」に新たなゼロデイ攻撃--高度なターゲット化が特徴（CNET Japan） http://japan.cnet.com/news/service/35039771/ ● 本格的に日本を襲い始めた APT（エフセキュア） http://blog.f-secure.jp/archives/50715372.html ● 「IE の新しい脆弱性を突く攻撃は、標的型なのに継続的に攻撃しない」、ファイア・アイが説明（ITPro） http://itpro.nikkeibp.co.jp/article/NEWS/20131115/518206/

16. 「銀行強盗」が相次ぐ仮想通貨：被害額も巨額に

関連記事	● 「銀行強盗」が相次ぐ仮想通貨：被害額も巨額に （WIRED.jp） http://wired.jp/2013/11/28/bitcoins-skyrocketing-value-ushers-in-era-of-1-million-hacker-heists/ ● Bitcoin の急騰で仮想銀行強盗が増加（Symantec） http://www.symantec.com/connect/de/blogs/bitcoin-2 ● 日本でも約 3000 台の感染が確認された脅威 「ビットコイン発掘不正プログラム」とは（Trend Micro） http://blog.trendmicro.co.jp/archives/8271 ● ビットコイン価格高騰で、関連不正プログラムやウォレット窃取の被害拡大（Trend Micro） http://blog.trendmicro.co.jp/archives/8324 ● 仮想通貨:ビットコイン急成長　各国当局が動向注視（毎日新聞） http://mainichi.jp/select/news/20131224k0000m020125000c.html ● ビットコイン:麻薬取引などに悪用の恐れ　米に賛否（毎日新聞） http://mainichi.jp/select/news/20131224k0000m020126000c.html

17. 企業を装う「安全確認」メールに注意

関連記事	● 電子書危険な「安全確認」メールに注意、標的をゲームから銀行に変更（フィッシング）（セキュリティ通信） http://security-t.blog.so-net.ne.jp/2013-11-25 ● 11 月の国内フィッシング事情：「安全確認」メールが標的を拡大 http://security-t.blog.so-net.ne.jp/2013-12-26

18. 未成年の犯行によるネット関連犯罪事件

関連記事	● １８歳がフィッシング用サイト…開設で初の逮捕 （YOMIURI ONLINE）

	http://ceron.jp/url/www.yomiuri.co.jp/national/news/20131016-OYT1T01479.htm ● 岡山の高１がウイルス作成容疑　他人のＩＤ入手、書類送検（47NEWS） http://www.47news.jp/CN/201311/CN2013111301002092.html ● オンラインゲームで不正アクセス容疑の４少年書類送検　今市署と県警（47NEWS） http://www.47news.jp/localnews/tochigi/2013/11/post_20131120164630.html ● 不正アプリで男子高生ら書類送検　電子書籍をダウンロード（千葉日報） http://www.chibanippo.co.jp/newspack/20131204/169103 ● ウイルス送り付け中学生送検（NHK ニュース） http://archive.is/XJ3qX ● コンピューターウイルスの提供などで５少年摘発　神奈川県警（msn 産経ニュース） http://sankei.jp.msn.com/region/news/131211/kng131211161300001-n1.htm

19. 百度の IME、中国製の日本語入力ソフトが入力情報を無断送信

関連記事	● 日本語入力ソフトのオンライン機能に注意、企業の重要情報が外部に送信される恐れ（ITPro） http://itpro.nikkeibp.co.jp/article/NEWS/20131217/525422/?ST=security&P=1 ● 百度の IME、中国製の日本語入力ソフトが入力情報を無断送信　パスワードなども（ハフィントンポスト） http://www.huffingtonpost.jp/2013/12/25/baidu-ime_n_4502142.html ● 中国百度が IME 入力情報送信問題で見解を発表、「Simeji はバグでログ誤送信」（ITPro） http://itpro.nikkeibp.co.jp/article/NEWS/20131226/527369/ ● 「Simeji」が入力ログ無断送信バグを修正　「クラウド変換」は初期設定でオフに（ITmedia） http://www.itmedia.co.jp/news/articles/1312/27/news036.html

20. Target、100 万件超の顧客カード情報流出

関連記事	● 米小売大手で 100 万件超のカード情報流出か、過去最大規模になる恐れ（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1312/19/news039.html ● Target から流出のカード情報、闇市場で大量流通（ITmedia） http://www.itmedia.co.jp/news/articles/1312/24/news038.html ● Target のカード情報流出でフィッシング詐欺発生（ITmedia） http://www.itmedia.co.jp/news/articles/1312/26/news036.html

21. 総務省によるマルウェア対策支援プロジェクト「ACTIVE」実施

関連記事	● 総務省は、「官民連携による国民のマルウェア対策支援プロジェクト（プロジェクト名：Advanced Cyber Threats response InitiatiVE　略称「ACTIVE」）」を平成 25 年 11 月 1 日(金)から実施します。(総務省) http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000059.html

22. ＮＥＣやＮＴＴなど、サイバー防衛で連携　会員に対策助言

関連記事	● ＮＥＣとＮＴＴ、三井物産の情報システム子会社は企業へのサイバー攻撃を防ぐ民間組織「サイバーリスク情報センター」を設立した。　（日本経済新聞） http://www.nikkei.com/article/DGXNASDD270Q0_X21C13A1TJ0000/

23. 国と民間企業によるサイバー犯罪への取り組み

関連記事	● 国とインフラ事業者がサイバー対策訓練（NHK ニュース） http://archive.is/tRuI5 ● ALSOK と警視庁、サイバー犯罪捜査で協定締結（RBB TODAY） http://www.rbbtoday.com/article/2013/11/12/113808.html ● サイバー犯罪対策で官民組織　政府、東京五輪に向け戦略（日本経済新聞）

	http://www.nikkei.com/article/DGXNASDG1000Z_Q3A211C1CR0000/

24. 警視庁機動サイバー班が発足

関連記事	● 警視庁機動サイバー班が発足＝署支援し、捜査力向上へ（時事ドットコム） http://www.jiji.com/jc/zc?k=201310/2013100100943 ● サイバー補導端緒、買春容疑の男逮捕／県警が初（四国新聞） http://www.shikoku-np.co.jp/kagawa_news/social/20131112000240 ● ＜サイバー補導＞本格始動　ネット上で「下着買って」、書き込みから本人に対面（毎日新聞） http://archive.is/pky8l

25. 被害拡大、リベンジポルノ

関連記事	● リベンジポルノやプライバシーのネット拡散をどう止める？ - 表現の自由か、法規制か（ハフィントンポスト） http://www.huffingtonpost.jp/2013/10/13/revengeporn_n_4093699.html ● とんだ坂本龍馬　元交際相手に「裸の写真をばらまく」（スポーツニッポン新聞） http://www.sponichi.co.jp/society/news/2013/12/08/kiji/K20131208007159840.html ● 「リベンジポルノ」サイト運営と恐喝の疑いで男を逮捕　米（CNN） http://www.cnn.co.jp/tech/35041245.html ● リベンジポルノ:被害拡大　元交際相手の裸の写真、ネットに流出　「親しくても撮らせないで」（毎日新聞） http://mainichi.jp/shimen/news/m20131219ddm041040104000c.html

26. 個人情報保護法改正の動き

関連記事	● Suica の乗降履歴事例を引き合いに、法制度改正求める声相次ぐ（ITPro） http://itpro.nikkeibp.co.jp/article/NEWS/20131029/514706/ ● ビッグデータに不安…保護法改正、政府が検討会（YOMIURI ONLINE）

	http://www.yomiuri.co.jp/net/news0/national/20131109-OYT1T00674.htm ● 政府、ビッグデータ対策急ぐ　第三者機関で監視案（朝日新聞） http://www.asahi.com/articles/TKY201311220737.html ● 政府、ビッグデータ活用へ法整備決定（日経新聞） http://www.nikkei.com/article/DGXNASFS20009_Q3A221C1EB1000/ ● 個人情報保護法の見直し方針固まる　「非特定情報」の扱いを柔軟化（ITPro） http://itpro.nikkeibp.co.jp/article/COLUMN/20131220/526244/

27. 季節のイベントを悪用するフィッシング詐欺

関連記事	● ハロウィンに便乗した”世にも恐ろしい”アンケート詐欺を確認（Trend Micro） http://blog.trendmicro.co.jp/archives/8035 ● クリスマスを狙うフィッシングにご用心（Symantec） http://www.symantec.com/connect/ja/blogs-320

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. 2013 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/malware1308.html

2. 2013 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/malware1308_jp.html

3. 2013 年 9 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/malware1309.html

4. 2013 年 9 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/malware1309_jp.html

5. 2013 年 10 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/malware1310.html

6. 2013 年 10 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/malware1310_jp.html

7. 2013 年 11 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/malware1311.html

8. 2013 年 11 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/malware1311_jp.html

9. 2013 年 9 月のウイルス脅威

関連記事	● 2013 年 9 月のウイルス脅威 (Dr.WEB) http://news.drweb.co.jp/?i=678&c=1&lng=ja&p=0

10. 2013 年 10 月のウイルス脅威

関連記事	● 2013 年 10 月のウイルス脅威 (Dr.WEB) http://news.drweb.co.jp/show/?i=683&lng=ja&c=2

11. 2013 年 11 月のウイルス脅威

関連記事	● 2013 年 11 月のウイルス脅威 (Dr.WEB) http://news.drweb.co.jp/show/?i=695&lng=ja&c=4

12. アンチウイルスソフトを装うマルウェアの拡散

関連記事	● アンチウイルスベンダーを装ったスパム。適用を促されたセキュリティパッチは、Zbot/Zeus マルウェア (Sophos) http://www.sophos.com/ja-jp/press-office/press-releases/2013/11/ns-spam-from-an-antivirus-company-its-zeus-malware.aspx ● 偽のウイルス対策ソフトウェア更新通知がマルウェアを拡散 (Symantec)

	http://www.symantec.com/connect/ja/blogs-317 ● ソフトウェアのアップデート装うウイルス拡散、日本人もターゲットに（So-net セキュリティ通信） http://security-t.blog.so-net.ne.jp/2013-11-27 ● 著名セキュリティ企業を装って偽パッチを送り付ける手口に注意（Security NEXT） http://www.security-next.com/044873 ● Android Tapsnake モバイルスケアウェア: 偽ウイルス対策アプリを宣伝する広告（Symantec） http://www.symantec.com/connect/ja/blogs/android-tapsnake

13. ランサムウェア「CryptoLocker」、世界的に蔓延

関連記事	● ランサムウェア「CryptoLocker」、オンライン銀行詐欺ツール「ZBOT」を経てコンピュータに侵入（Trend Micro） http://blog.trendmicro.co.jp/archives/8017 ● CryptoLocker に関する緊急アラート（Sophos） http://www.sophos.com/ja-jp/press-office/press-releases/2013/11/ns-cryptolocker-urgent-alert.aspx ● 恐怖のランサムウェア、CryptoLocker (Kaspersky) http://blog.kaspersky.co.jp/cryptolocker-is-bad-news/ ● 日本でも急増する「身代金型ウイルス」被害　「東京五輪」が標的に!? (ITmedia) http://www.itmedia.co.jp/news/articles/1312/06/news045.html ● ランサムウェア「CryptoLocker」の新しい亜種を確認、USB ワーム活動による感染拡大を狙う（Trend Micro） http://blog.trendmicro.co.jp/archives/8355

14. ブラウザロック型のランサムウェア

関連記事	● 大規模なマルバタイジング攻撃に続くブラウザロック型のランサムウェア (Symantec) http://www.symantec.com/connect/ja/blogs-325

15. マルウェア「Ramnit」が高機能化

関連記事	● マルウェア「Ramnit」が高機能化 - FTP ネットワーク構築する亜種も (Security NEXT) http://www.security-next.com/044081

16. 銀行を狙うバンキング型トロイの木馬の新種「Neverquest」

関連記事	● トロイの木馬 Neverquest：多数の銀行がターゲットに (Kaspersky) http://blog.kaspersky.co.jp/neverquest-trojan-built-to-steal-from-hundreds-of-banks/ ● オンラインバンキングを狙うトロイの木馬、危険な新種の Neverquest は古い同族の進化形 (Symantec) http://www.symantec.com/connect/ja/blogs/neverquest

17. ATM を感染させる Trojan.Skimer.18

関連記事	● ATM を感染させるバックドアはこれまでにも確認されていますが、世界中で広く使用されているデバイスを標的としたものとしては Trojan.Skimer.18 が初めてとなります。 (Dr. WEB) http://news.drweb.co.jp/show/?i=697&lng=ja&c=1

18. SAP ユーザを狙うバックドア「BKDR_SHIZ.TO (Gamker)」を確認

関連記事	● SAP ユーザを狙うバックドア「BKDR_SHIZ.TO」、Bitcoin ウォレットなども攻撃対象に (Trend Micro) http://blog.trendmicro.co.jp/archives/8183

19. POS 端末を狙うマルウェア、40 カ国に感染広げる

関連記事	● 世界 40 カ国の小売り店やホテル、飲食店などの POS 端末が、クレジットカード情報を狙うマルウェアの標的になっているという。（ITmedia） http://www.itmedia.co.jp/enterprise/articles/1212/14/news034.html

20. リモートアクセス型トロイの木馬「クリープウェア」

関連記事	● クリープウェア：誰かに見られているかもしれない（Symantec） http://www.symantec.com/connect/ja/blogs-323 ● 引き続き Web カメラには警戒を（Symantec） http://www.symantec.com/connect/ja/blogs/web-9

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＜2013.10.02＞

プレス リリース	● チェックしておきたい脆弱性情報＜2013.10.02＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20130930/507756/?ST=security

2. チェックしておきたい脆弱性情報＜2013.10.07＞

プレス リリース	● チェックしておきたい脆弱性情報＜2013.10.07＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20130930/507757/?ST=security

3. チェックしておきたい脆弱性情報＜2013.10.22＞

プレス リリース	● チェックしておきたい脆弱性情報＜2013.10.22＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20131021/512283/?ST=security

4. チェックしておきたい脆弱性情報＜2013.10.25＞

プレス リリース	● チェックしておきたい脆弱性情報＜2013.10.25＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20131021/512284/?ST=security

5. チェックしておきたい脆弱性情報＜2013.11.06＞

プレス リリース	● チェックしておきたい脆弱性情報＜2013.11.06＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20131104/515703/?ST=security

6. チェックしておきたい脆弱性情報＜2013.11.08＞

プレス リリース	● チェックしておきたい脆弱性情報＜2013.11.08＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20131104/515704/?ST=security

7. チェックしておきたい脆弱性情報＜2013.11.11＞

プレス リリース	● チェックしておきたい脆弱性情報＜2013.11.11＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20131104/515705/?ST=security

8. チェックしておきたい脆弱性情報＜2013.11.27＞

プレス リリース	● チェックしておきたい脆弱性情報＜2013.11.27＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20131125/520504/?ST=security

9. チェックしておきたい脆弱性情報＜2013.11.29＞

プレス リリース	● チェックしておきたい脆弱性情報＜2013.11.29＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20131125/520505/?ST=security

10. チェックしておきたい脆弱性情報＜2013.12.18＞

プレス リリース	● チェックしておきたい脆弱性情報＜2013.12.18＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20131216/525002/?ST=security

11. チェックしておきたい脆弱性情報＜2013.12.19＞

プレス リリース	● チェックしておきたい脆弱性情報＜2013.12.19＞ http://itpro.nikkeibp.co.jp/article/COLUMN/20131216/525005/?ST=security

5. 総括

今期は、利用者の危機意識を煽るかたちでの攻撃が目立ちました。まず、企業を装った偽の安全確認メールによるフィッシング詐欺です。企業や公的機関の管理するサイトへの不正アクセス発生等を理由に顧客にメールを送信し、偽サイトに誘導してログインさせようとする手口、入力フォーム型のメールに入力させる手口、メールの返信を要求する手口と、情報詐取を試みる様々な手法が確認されました。次に、ウイルス対策ソフトのアップデートを装ったマルウェアの配布が挙げられます。セキュリティベンダを名乗り、ウイルス対策ソフトの更新といった名目で更新プログラムに見せかけたマルウェアをメールで送り付け、利用者自身にインストールを実行させようとする事例が頻繁に確認されています。こうした手口が発見された当初は、英文によるメールが多かったものの、昨年11月末頃には日本語によるメールも確認されています。攻撃者は、セキュリティベンダ各社が注意を呼び掛けている「CryptoLocker」といった実際のマルウェアを明記するなどして、早急に更新するよう促します。

前述のどちらの手法も、利用者の防衛意識を悪用する非常に巧みなやり口です。企業や公的機関から本物らしい通知を受け取ったとしても、記載されているURLをクリックしたり、添付ファイルを開いたりせず、まずは、当該組織の公式サイトから告知があるかどうか確認する、組織に問合せを行う、といった対策が常に望まれます。

株式会社 日立システムズ

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.hitachi-systems.com/index.html

http://www.shield.ne.jp/ssrc/index.html