Q45 出来事

項番	認知順位	認知数(N=437)	表記	説明(概略)	参考:(2014年11月末時点)	追加コメント
Q45-21	1	420	Windows XPサポート終了	2014年4月9日(日本時間)をもって、Windows XP、Microsoft Office 2003、Internet Explorer 6 のサポートを終了した。これらに対するセキュリティパッチなども提供を終了した。	http://www.microsoft.com/ja-jp/windows/lifecycle/xp_eos.aspx	Microsoft社では、サポート終了に伴うセキュリティのリスクがあるため、Windows 8、新しいOffice への移行を勧めている。
Q45-9	2	387	他者のパソコンを遠隔操作し、犯罪予告を行った事件	2012年の6月から9月にかけて、インターネット上の掲示板や、官公庁のホームページ上に、襲撃や破壊、大量殺人などの犯行予告が行われ、事件に関与したと思われる数名が逮捕された。その後、全ての逮捕者が、何者かに自分のパソコンを遠隔操作されたりした事が判明し、警察の誤認逮捕も問題となった。	https://kotobank.jp/word/%E9%81%A0%E9%9A%94%E6%93%8D%E4%BD%9C%E4%BA%8B%E4%BB%B6-189777	誤認逮捕された人々は、内部に遠隔操作プログラムが仕掛けられていたソフトウエアを知らずに利用したことや、Webサイトにスクリプトや自動転送(HTTPリダイレクト)を仕込むことによって、閲覧者に意図せず別のWebサイト上で掲示板への書き込みなどを行わせる攻撃手法CSRF(Cross Site Request Forgeries)の被害にあっていた。
Q45-16	3	383	ﾋﾞｯﾄｺｲﾝ取引所であるﾏｳﾝﾄｺﾞｯｸｽ社が倒産	インターネット上の仮想通貨ビットコインの取引所「マウントゴックス」を運営するMTGOX(東京・渋谷)が2014年2月28日、東京地裁に民事再生法の適用を申請し同日受理されたと発表した。	http://www.nikkei.com/article/DGXNASGC2802C_Y4A220C1MM8000/	MTGOXのマルク・カルプレス社長によると、2014年2月初旬、システムの不具合(バグ)を悪用した不正アクセスが発生し、売買が完了しない取引が急増。「バグの悪用により(ビットコインが)盗まれた可能性が高い」と判断した。さらに、2月24日、利用者からの預かり金を保管する預金口座の残高が最大で28億円程度不足も分かった。
Q45-7	4	367	Twitterへの悪ふざけ写真投稿による炎上事件(ﾊﾞｶｯﾀｰとも呼ぶ)	2013年夏、相次ぎ発覚した小売りや外食店での悪ふざけ写真。アルバイト従業員や来店客がツイッターなどに投稿した写真は瞬く間にネット上を駆け巡り、多くの人目にさらされた。「不衛生」「二度と行かない」。一部の消費者からはこんな声も上がり、店舗ブランドが傷つく例も続出した。	http://matome.naver.jp/odai/2137616612852032401	被害を受けた店舗では、閉店に追い込まれたり、倒産に至ったケースもある。Twitterへ投稿した本人は、停学や退学になるケースも見られる。
Q45-13	5	335	元米政府職員ｽﾉｰﾃﾞﾝ氏による政府の盗聴活動の暴露	元米中央情報局(CIA)職員のエドワード・スノーデン(Edward Snowden)氏(29)は、米政府が個人の電話記録やインターネット利用を極秘裏に監視していた事実を暴露した。	http://www.afpbb.com/articles/-/2950073?pid=10897395	NSAが運用する監視プログラムを暴露した勇敢な内部告発者として称賛する声も上がっている。一方で米政府は、同プログラムは米国人をテロから守るために必要な活動だとしており、米議員の多くはスノーデン氏の行為を卑劣な裏切り行為だと非難している。
Q45-14	6	334	InternetExplorerやOpenSSL脆弱性を利用した標的型攻撃を確認	Microsoft 社はInternet Explorer の「脆弱性を悪用しようとする限定的な標的型攻撃を確認しています。」と公表している。OpenSSL脆弱性を発見した、日本のネットワークセキュリティ技術・研究開発企業レピダムでは「標的型攻撃などに利用される可能性は非常に高い」と警告している。	https://www.ipa.go.jp/security/ciadr/vul/20140428-ms.html http://www.itmedia.co.jp/enterprise/articles/1406/06/news034.html	2014 年 10 月 22 日(日本時間)にもMicrosoft 社は「脆弱性を悪用する悪意のある Microsoft PowerPoint ファイルを利用した限定的な標的型攻撃を確認しています。」と公表している。

Q45 出来事

項番	認知順位	認知数(N=437)	表記	説明(概略)	参考:(2014年11月末時点)	追加コメント
Q45-8	7	296	Googleｸﾞﾙｰﾌﾟで共有していた官公庁の情報が誰でも閲覧可能になっていた事案	環境省、復興庁、農林水産省、国土交通省において、省庁内や外部関係組織との連絡や情報共有にGoogleグループのサービスを利用し、その内容が、誰でも閲覧可能な状態に放置されていた。	http://www.jnsa.org/secshindan/secshindan_7.html	実際にGoogleグループのサービスを利用していた職員の情報保護に関する意識の低さの問題があげられる。同時に、組織としては職員に対して便利で安全なサービスを提供できていない問題があると思われる。
Q45-1	8	285	米国から中国に「ｻｲﾊﾞｰ攻撃による窃盗行為を止めるように」と強い要請を行った事案	2013年7月にワシントンで開催された「米中戦略経済対話」において、米国の副大統領から中国政府に対し「サイバー攻撃による窃盗行為を止めるように」強い要請がなされたと報じられた。	http://business.nikkeibp.co.jp/article/opinion/20140722/268984/?rt=nocnt	この要請からも、米国政府が、サイバー空間における機密情報の窃盗に頭を悩ませている様子が窺える。また、影響は、情報システムの枠だけに留まらず、国家間の外交問題に発展している。
Q45-5	9	264	ｲﾝﾀｰﾈｯﾄﾊﾞﾝｷﾝｸﾞの不正送金被害が発生。2013年の被害額は約14億円と報道発表（警察庁調べ）	警察庁は2014年1月30日、2013年中のネットバンキングにおける不正送金の発生状況を公表した。それによると、口座の預金を勝手に送金されて盗まれる事件は1315件発生し、被害総額は約14億600万円で過去最悪だった。	http://itpro.nikkeibp.co.jp/article/NEWS/20140203/534107/	警察庁によると、ネットバンキングユーザーの預金が不正送金される事件が急増している。2011年は165件で被害額が約3億800万円、2012年は64件で被害額が約4800万円だったが、2013年は6月以降に急増。過去最悪の被害件数および被害額になった。尚、2014年上半期（1月～6月）の発生件数は1254件、被害額は約18億5200万円で、1件あたりの被害額は約148万円。
Q45-15	10	260	百度の文字変換ｱﾌﾟﾘ「Baidu IME」「Simeji」が、ﾕｰｻﾞｰの入力内容を同社へ無断送信していた事案	ネットエージェントは2013年12月26日、中国Baiduの日本法人バイドゥが無償配布しているPC向け日本語IME「Baidu IME」とAndrid向け日本語IME「Simeji」を使って入力された文字列が、ユーザーに無断で外部のサーバに送信されているという解析結果を明らかにした。	http://www.itmedia.co.jp/news/articles/1312/26/news055.html	ユーザーが設定画面でログ送信をオフにしたり、「クラウド入力」をオフにしていても、変換した文字列や端末名、使用中のアプリ名が、国内にあるサーバに送信されていることが分かった。パスワードなど半角入力のみの場合は送信されない。クレジットカード番号や電話番号なども、変換しない限り送信されない。
Q45-18	11	245	JR東日本のSuica履歴販売に対しﾌﾟﾗｲﾊﾞｼｰ問題の指摘	JR東日本が、交通系ICカード「Suica」の乗降履歴を日立製作所に販売した。国土交通省がヒアリングに乗り出したことを機に、新聞やテレビは「事前説明がなかったのは問題」と一斉に報道。それを受けて利用者からも「勝手に売るな」「気持ち悪い」などの批判が噴出した。	http://www.sbbit.jp/article/cont1/26628	要因は、Suica履歴の販売について、JR東日本が利用者に事前説明をしていなかった点である。利用規約にはSuica履歴の販売、譲渡について記載はなく、規約の変更も行わなかった。文書などによる利用者への告知もなかった。販売したデータの具体的な中身についての説明も不十分だった。
Q45-20	12	224	ISO/IEC27001規格が改定	情報セキュリティマネジメントシステム（ISMS）評価認定制度の基となっている国際規格「ISO/IEC27001」が2013年10月に改訂された。既存ISMS取得組織は2年以内に対応が必要である。	http://www.isms.jipdec.or.jp/ikou/27001_2013/ISO_IEC_27001_2013_transition_outline.pdf	ISO/IEC27001の規格そのものの見直しと、リスクに関する用語や考え方の規格であるISO31000やISO Guide73との整合やISO Guide83の採用など、“ISO/IEC27001の規格に影響を与える他の規格との整合”が図られた。既存ISMS取得組織は2年以内（2015年10月まで）に対応が必要である。

Q45 出来事

項番	認知順位	認知数(N=437)	表記	説明(概略)	参考:(2014年11月末時点)	追加コメント
Q45-2	13	202	JAL・ANAﾏｲﾚｰｼﾞが、不正ｱｸｾｽによりﾎﾟｲﾝﾄを不正利用された事件	2014年2月3日、日本航空（JAL）は運営する「JALマイレージバンク（JMB）」サイトへの不正ログインが判明し、JMB会員になりすました第三者がマイルを特典に交換するトラブルが多数発生していたことを発表した。同年3月17日、全日空（ANA）の「ANAマイレージクラブ」で不正アクセスが発生、マイルが盗まれる被害が発生したと発表された。	http://security.slashdot.jp/story/14/02/04/0846219/	「JALマイレージバンク」の問題点として、ログインには数字7桁もしくは9桁の「マイレージ番号」を使用し、またパスワードは数字6桁でアルファベットなどを含めることができないという同サイトの仕様が挙げられていた。「ANAマイレージクラブ」は、数字10桁の会員番号と数字4桁のパスワードを使用しており、数字4桁のパスワードの危険性はかねてから指摘されていた。
Q45-3	14	140	PC内のﾃﾞｰﾀをﾛｯｸし身代金を要求するﾗﾝｻﾑｳｪｱの感染拡大（CryptoLockerなど）	ランサムウェアに感染すると、コンピュータが使用できなくなったと通告するメッセージが表示され、解除するためと称して「罰金」の支払いを要求される。米国土安全保障省（DHS）傘下のUS-CERTが2013年7月31日、Webサイトに掲載した情報を更新して注意を呼びかけた。	http://www.itmedia.co.jp/enterprise/articles/1308/02/news031.html	もし感染した場合でも、相手に要求されるままに金を払ってはいけないとUS-CERTは助言し、信頼できるセキュリティ専門家に相談してマルウェアを削除するか、HDDをフォーマットしたうえでOSを再インストールするよう促している。
Q45-19	15	139	ｱﾄﾞﾋﾞｼｽﾃﾑｽﾞへの不正ｱｸｾｽにより、ｸﾚｼﾞｯﾄｶｰﾄﾞ番号を含む3800万人の顧客情報が流出	米Adobe Systemsが、現地時間2013年10月3日に不正アクセスを受け、ユーザーの名前とID、暗号化したパスワード、暗号化したクレジットカード/デビットカード番号、有効期限などのデータに攻撃者がアクセスしたことが分かったと発表した。	http://itpro.nikkeibp.co.jp/article/IDG/20131031/515124/	Adobe Systems社から流出したユーザー名とハッシュ化されたパスワードのデータ1億5000万件がネット上に公開されたのは10月第4週の後半だった。このファイルのリンクはさまざまなサイトに掲載された。その1つがAnonNews.orgで、これを見た調査報道記者のBrian Krebs氏がファイルを発見した。
Q45-6	16	121	ﾊﾟｰｿﾅﾙﾃﾞｰﾀ利活用に向けた法制の見直し	2015年に予定される個人情報保護法改正に関連して、政府では「パーソナルデータ」の利活用に向けた制度の整備が検討されている。	http://www.soumu.go.jp/main_content/000305738.pdf	個人に関連するデータ（パーソナルデータ）の利活用については、現行の個人情報保護法の運用状況や、プライバシーに対する社会的な意識の高まりなどから、大綱では「利活用の壁」を生じさせる「グレーゾーン」の存在と、「個人の権利利益の侵害」を未然に防止することを課題に挙げられている。
Q45-12	17	118	「ウイルス対策」を騙ったｱﾌﾟﾘで電話帳ﾃﾞｰﾀが約3,700万人分抜き取られた事件	Android向けアプリ「安心ウイルススキャン」はセキュリティ対策をうたいながら実際にはユーザーの電話帳データを抜き取り、外部サーバに送信する悪質なアプリであった。	http://www.itmedia.co.jp/news/articles/1307/24/news089.html	運営する出会い系サイトへ誘導するスパムメールを送信したとして、千葉県警は2013年7月24日、特定電子メール法違反などの疑いで東京都内のIT関連会社社長の男（50）ら9人を逮捕した。
Q45-4	18	79	不正ｱｸｾｽにより、米ﾀｰｹﾞｯﾄ社が4000万枚のｶｰﾄﾞ情報搾取被害	米ディスカウントストア大手ターゲット社は、感謝祭前日の2013年11月27日から12月15日までの19日間に同社店舗で顧客が利用したクレジットカードおよびデビットカード最大4000万枚の情報がハッカー攻撃により流出したことを明らかにした。	http://jp.reuters.com/article/topNews/idJPTYE9BI07Y20131219	カード保持者の氏名、カード番号、使用期限、3桁のセキュリティコードの流出の疑いが発生。アナリストによると、同社への影響としては販売の減少が予想されるほか、カード会社からセキュリティ対策の不備などに絡む請求を受ける可能性が高い。

Q45 出来事

項番	認知順位	認知数(N=437)	表記	説明(概略)	参考:(2014年11月末時点)	追加コメント
Q45-17	19	72	ﾛﾘﾎﾟｯﾌﾟﾚﾝﾀﾙｻｰﾊﾞｰが管理する8,438ｳｪﾌﾞｻｲﾄが改ざん被害	2013年8月下旬に、レンタルサーバー「ロリポップ！レンタルサーバー」で、ブログ管理ソフト「WordPress」を利用したWebサイトが8438件、改ざんされた。	http://itpro.nikkeibp.co.jp/article/Active/20140213/536447/	ロリポップレンタルサーバを提供しているpaperboy&co.(現GMOペパボ株式会社)は2013年8月30日19:13に説明をアップデートした。WordPressのプラグインやテーマの脆弱性を悪用されて不正侵入を受けた上で、「当社のパーミッションの設定不備を利用」されたことが原因であると明記している。
Q45-11	20	64	ﾋﾟｻﾞｰﾗ、ﾏﾂｷﾖの公式ｱﾌﾟﾘを騙る偽ｱﾌﾟﾘがAppStoreで提供された事案	偽アプリはそれぞれ、ピザーラのピザ注文サイトに接続「pizza-la For iPhone」、マツモトキヨシ通販サイト「e!マツモトキヨシHD」「e!マツモトキヨシ For iPhone2.0」に接続し正常に注文もできる。	http://www.itmedia.co.jp/news/articles/1401/16/news090.html	実際に会員登録や注文もできるようだが、どこかに通信を中継されている可能性もある。「App Store」のアプリ審査は厳しいことで有名だが、インターネット上には、著作権などの権利に関するチェックが甘いとの指摘がある。
Q45-10	21	53	米国で100Gbpsのﾄﾗﾌｨｯｸが絶え間なく9時間継続観測、史上最大のDDoS攻撃発生	この攻撃が観測されたのは2013年9月24日。被害にあった組織の名称は公表されていない。攻撃対象となったWeb サイトはクラウドセキュリティベンダー Incapsula によって保護されていた。	http://internetcom.jp/webtech/20131002/4.html	この攻撃で注目すべき点は、「DNS リフレクター攻撃(トラフィックが30倍にまで「増幅」される)」と呼ばれる攻撃手法が使われていないこと。これは、攻撃者自身が100 Gbps のバンド幅を保有していることを意味している。このバンド幅は安いものではない。