項番	認知順位	認知数(N=367)	表記	説明(概略)	参考:(2013年11月末時点)	追加コメント
Q48-18	1	314	尖閣諸島中国漁船衝突映像流出	2010年11月4日、尖閣諸島における中国漁船衝突事故の状況を撮影したビデオがYouTubeに投稿されており、投稿者として海上保安官が名乗り出た。	http://b.hatena.ne.jp/articles/201011/2041	2010年9月7日に起きた漁船衝突事故。当初は強気の姿勢で中国側船長を逮捕しながら、中国政府からの釈放要求に応じ、衝突時のビデオを公開しようとしない政府の姿勢に不信が高まっていた。
Q48-12	2	298	Yahoo! JAPAN IDの流出(2013年)	5月17日、Yahoo！JAPAN IDを管理しているサーバに外部から不正アクセスを受け、最大2200万件のIDのみが抽出されたファイルが作成されたことが分かったと発表した	http://www.itmedia.co.jp/news/articles/1305/18/news008.html	そのうち148万6000件は暗号化済みパスワードとパスワード再設定用の「秘密の質問」も流出したとみられると発表した。
Q48-15	3	266	遠隔操作ｳｨﾙｽ事件	2012年夏から秋に、犯人がインターネットの電子掲示板を介して、他者のパソコン(PC)を遠隔操作し、これを踏み台として襲撃や殺人などの犯罪予告を行った。	http://www.weblio.jp/content/%E3%83%91%E3%82%BD%E3%82%B3%E3%83%B3%E9%81%A0%E9%9A%94%E6%93%8D%E4%BD%9C%E4%BA%8B%E4%BB%B6	遠隔操作には、WEBサイトの脆弱性や、犯人が自作したトロイの木馬"iesys.exe"が使用され、真犯人の行為で複数の男性が冤罪となったことについて、マスコミ・警察庁OBも問題を指摘している。
Q48-17	4	254	ｽﾏﾎｱﾌﾟﾘによる個人情報流出	特定のアプリをダウンロードしたスマートフォンの電話帳から、電話番号やメールアドレスが流出するなど、スマートフォンを原因とする情報流出事件	http://www.yomiuri.co.jp/otona/life/law/20130108-OYT8T00869.htm	違法ではないが、不用意な情報収集でIT企業が解散に追い込まれる例も出ている。
Q48-5	5	207	偽画面によるﾌｨｯｼﾝｸﾞ詐欺(2012年)	金融機関などからの正規のWebサイトを装い、偽画面への入力を通じて、暗証番号やクレジットカード番号などを不正に詐取する詐欺行為である。	http://e-words.jp/w/E38395E382A3E38383E382B7E383B3E382B0.html	偽画面((真正なサイトでない画面)
Q48-26	6	203	韓国へのｻｲﾊﾞｰ攻撃(2013年3月)	3月20日韓国の放送局や銀行で一斉にシステムがダウンする大規模なサイバー攻撃があり、国家規模で混乱が発生し、放送局では業務復旧までに約9日を要した。	http://news.mynavi.jp/articles/2013/05/27/korea/	パッチマネージメントサーバ(PMS)を乗っ取り、外部の商用サーバからPMS内に悪性コードをダウンロードした。この悪性コードは、アンチウィルスソフトでは検知されなかった。
Q48-16	7	176	「不正ｱｸｾｽ禁止法」改正(2012年)	2000年に施行されたコンピューターの不正利用を禁止する法律で、2012年5月、規制の対象となっていなかったIDやパスワードの不正取得禁止を盛り込んだ改正がされた	http://kotobank.jp/word/%E4%B8%8D%E6%AD%A3%E3%82%A2%E3%82%AF%E3%82%BB%E3%82%B9%E7%A6%81%E6%AD%	不正アクセスの準備行為である他人のIDやパスワードを不正に取得する「フィッシング」などの増加を受けて改訂された。
Q48-19	8	176	Javaの脆弱性(2013年1月)	2013年1月、Java に存在する新たなゼロデイ脆弱性が確認されました。すでに、この脆弱性を利用した不正プログラム(エクスプロイト)は、「Blackhole Exploit Kit (BHEK)」や「Cool Exploit Kit (CEK)」といった攻撃ツールで利用されている。	http://blog.trendmicro.co.jp/archives/6521	特に「REVETON」という「身代金要求型不正プログラム(ランサムウェア)」の亜種を拡散させるために利用されていたことが報告されています。
Q48-7	9	163	ﾌｧｰｽﾄｻｰﾊﾞﾃﾞｰﾀ消失事故(2012年)	レンタルサーバ事業者ファーストサーバが、2012年6月20日―21日に起こした大規模なデータ消失事故	http://www.itmedia.co.jp/news/articles/1208/10/news051.html	第三者委員会による調査報告書によると、担当者がマニュアルを無視し、独自プログラムでシステム更新を行なった際に事故が起きたという。
Q48-22	10	155	農林水産省へのｻｲﾊﾞｰ攻撃	農林水産省は2013年5月、同省へのサイバー攻撃で2012年1月から4月にかけ5台のパソコンから合計124点の行政文書が流出した可能性があることを明らかにした。	http://itpro.nikkeibp.co.jp/article/NEWS/20130525/479521/	分析が十分に行われず、「情報流出の可能性は低い」との誤った認識が共有された。
Q48-9	11	153	AdobeReaderの脆弱性(2013年2月)	Adobe Reader"および"Adobe Acrobat"シリーズの旧バージョンに存在したゼロデイ脆弱性で、セキュリティ情報(APSB13-07)で対応された。	http://www.forest.impress.co.jp/docs/news/20130221_588722.html	任意コードの実行を許す恐れのあるメモリ破損の脆弱性(CVE-2013-0640)とバッファーオーバーフローの脆弱性(CVE-2013-0641)が存在した。
Q48-10	12	149	住基ﾈｯﾄの大規模障害(2013年3月)	自治体にある住民基本台帳システムと住基ネットを接続する「コミュニケーションサーバー」のハードウエアとOSを231の自治体で更新した際に発生した大規模障害。	http://itpro.nikkeibp.co.jp/article/NEWS/20130403/468302/	住民基本台帳ネットワークシステム(住基ネット)が利用できなくなる障害が発生した。原因が、データベース(DB)に情報を書き込む際の文字コードの誤り(文字化け)にあった。
Q48-1	13	136	gooIDへの不正ﾛｸﾞｲﾝ要求(2013年)	2013年4月、NTTレゾナント社のサービス「gooID」に対して、特定IPアドレスから不正なログインの試みを検知したと発表し、3万アカントをロック対応し、PW変更を依頼した。	http://itpro.nikkeibp.co.jp/article/NEWS/20130403/468462/	他社サービスから流出したID/パスワードのセットリストをgooIDシステムに対して試行している可能性、その後10万アカントに対応と追加記事、被害について(最終) http://pr.goo.ne.jp/detail/1703/
Q48-6	14	109	Evernoteﾕｰｻﾞ情報流出(2013年)	Evernoteが、暗号化されたパスワードを含むユーザー情報への不正アクセスを検知したとして、約5000万人に上る全ユーザーのパスワードをリセットした。	http://www.itmedia.co.jp/enterprise/articles/1303/03/news004.html	Evernoteのようなクラウドにデータを保存するサービスもデータを書き換えられる恐れがある。
Q48-13	15	105	NTTﾃﾞｰﾀ委託職員偽造ｶｰﾄﾞ事件	2012年11月、NTTデータの銀行データベースで、内部の人間(委託社員)が顧客情報を抜き取り、偽造キャッシュカードを作成して現金を盗んだ事件である。	http://www.yomiuri.co.jp/net/security/goshinjyutsu/20121130-OYT8T00931.htm	京都府警によれば、8銀行16口座から計約2000万円が引き出されたのを確認している..
Q48-3	16	99	AnonymousによるopJapan(2012年)	2012年6月に起きた日本の政府や組織を狙った「Anonymous」によるサイバー攻撃で、一部Webサイトが書き換えられたり、一時閲覧しづらい状態に陥ったりした。	http://www.itmedia.co.jp/enterprise/articles/1207/03/news108.html	違法ダウンロードの刑事罰化や日本音楽著作権協会(JASRAC)が中心となって導入をすすめる違法アップロードを監視するISPモジュールについて抗議している模様 (http://matome.naver.jp/odai/2134072361520387901)
Q48-11	17	82	JINSｵﾝﾗｲﾝｼｮｯﾌﾟｸﾚｶ情報流出	2013年4月、眼鏡ブランド「JINS」通販サイトからクレジットカード情報が流出した事件で、流出した顧客数は当初最大1万2036人としていたが最大2059人だったと発表した。	http://www.itmedia.co.jp/news/articles/1304/10/news115.html	バックドアプログラムが設置され、第三者のサーバにクレジットカード情報が転送されるようアプリケーションプログラムの改ざんが行われた形跡を確認した。
Q48-8	18	79	Apacheの不正ﾓｼﾞｭｰﾙを用いた改竄	トレンドマイクロは2013年3月、ウェブサーバー「Apache」不正モジュールを使った改ざん被害が国内外で報告されていると注意を呼びかけた。	http://internet.watch.impress.co.jp/docs/news/20130319_592299.html	PayPalをかたるフィッシングメールによる攻撃の被害報告が連日寄せられ、攻撃者がこれに続く新たな攻撃手法(改ざんサイトを発端とする攻撃)準備を進めているようだと推測している。
Q48-4	19	75	秋田市個人情報流出事故(2012年)	2012年8月、秋田市の市町合併当時の水道関連のお客様情報と河辺松渕市営住宅の入居者情報を含むデータが、インターネット上に流出した事件である。	http://leak00.p-kin.net/Entry/723/	原因は、合併当時のデータ移動作業にあたり、一時使用した個人パソコンのデータが消去されずに残っていたものが、ウイルス感染により流出したものと考えられる。
Q48-14	20	64	NewYorkTimesへの攻撃(2013年)	社内ネットワークが2012年9月末から4カ月にわたって、中国からサイバー攻撃を受けた。温首相に関する記事の情報提供者を特定することと見られる。	http://wired.jp/2013/02/05/new-york-times-hacked/	2013年10月 – 内戦の続くシリア軍が米国のメディアであるNew York Times紙のWebサイトを乗っ取る事件が(再度)起きた。
Q48-24	21	58	AP通信のTwitterﾊｯｷﾝｸﾞ	2013年4月、AP通信のTwitterがハッキング被害を受け、「爆発で大統領が負傷」のデマ流した事件	http://www.itmedia.co.jp/enterprise/articles/1304/24/news034.html	APは直後に同社のアカウントが乗っ取られたと説明している
Q48-28	22	51	米国報告書「弾力的軍事ｼｽﾃﾑ及び先進的ｻｲﾊﾞｰ脅威」の発表(2013年3月)	米国国防総省の国防科学委員会は、138ページの報告書に、ハッキングに対して「核兵器での攻撃を抑止力とする」という趣旨のことが書かれている。	http://www.gizmodo.jp/2013/03/post_11811.html	米国政府はすでにサイバー攻撃はバーチャルのみならずリアルな被害をもたらす戦争行為と見なすことを表明している。
Q48-2	23	33	攻撃者による不正国際IP電話発信	IP-PBXなどのソフトウエアやハードウエアでの設定の問題やセキュリティ対策のぜい弱性を利用することによる「なりすまし」や「乗っ取り」利用すること。	http://www.jaipa.or.jp/topics/?cat=23	IP/PBX: IP電話端末の回線交換を行なう装置およびソフトウエア
Q48-27	24	30	ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略最終案の策定	2013年6月、サイバー攻撃リスクが深刻化してきている状況を踏まえ、「サイバーセキュリティ立国」の実現を目指し、内閣府が2015年度まで3年間の国家戦略を取りまとめた	http://internet.watch.impress.co.jp/docs/news/20130611_603193.html	サイバー犯罪対策のための産官学連合、「サイバー防衛隊」(仮称)の新設など
Q48-25	25	27	My JR-EASTへの不正ﾛｸﾞｲﾝ要求	JR東日本は2013年4月17日、会員サービスサイト「My JR―EAST」に不正アクセスがあり、会員97人の個人情報が書かれたページに侵入された可能性があると発表	http://www.nikkei.com/article/DGXNASDG1703U_X10C13A4CR8000/	特定のIPアドレスから、サイトログイン画面に短時間で約2万6千件の要求があった。個人ページ侵入の可能性がある会員に対し、ロック対応し、パスワードなどの変更を求めた。会員数約350万人。
Q48-23	26	22	Flame(Flamer)の脅威(2012年)	非常に高機能(情報とデータの収集)な脅威で、悪質な機能が巧妙に隠された複数のコンポーネントを使用し、この脅威の標的は、東ヨーロッパと中東に集中している。	http://www.symantec.com/ja/jp/outbreak/?id=flamer	Flamer は、内部コードの複雑さにおいて Stuxnet や Duqu に匹敵します。資金力の高い集団が、東ヨーロッパと中東を標的として作成したものと考えられる。
Q48-21	27	16	ｺﾈｸﾄﾌﾘｰによるｱｶｳﾝﾄ無断取得	FacebookやTwitterアカウントを無断で取得し、利用者が閲覧したページに対しGoogle Analyticsの埋め込み等(ユーザー数の把握のためと説明)を行なっていたと謝罪した。	http://internet.watch.impress.co.jp/docs/news/20111207_496423.html	無料でインターネット接続サービスを提供する代わりに、利用者の閲覧ページ中に飲食店の情報などを表示する公衆無線LANサービスを提供している。
Q48-20	28	7	Operation Ababil	複数の米国大手銀行・金融機関(バンカメ、NYSEなど)が2012年9月から断続的にかなり大規模な DDoS攻撃を受けた事件。	http://d.hatena.ne.jp/ukky3/20130121/1358775092	"Innocence of Muslim"というエジプト系アメリカ人の監督が撮影した反イスラムをテーマとした映画が発端とされ、現地語予告編がYou-tubeで公開されて加熱し、2013年夏まで断続的に攻撃が続いている。