項番	認知順位	認知数(N=544)	表記	説明(概略)	参考:(2016年11月末時点)	追加コメント
Q49-3	1	365	日本年金機構の個人情報流出事故をうけCSIRTの体制強化を勧告	標的型攻撃により日本年金機構から101万人・125万件の年金情報が流出した事故をうけ、内閣官房内閣サイバーセキュリティセンター(NISC)は、サイバーセキュリティ戦略本部長名でCSIRTの体制強化を求める勧告を行った。2015/9/11	http://www.nisc.go.jp/press/pdf/kankoku20150911_press.pdf	NISCによる勧告は、サイバーセキュリティ基本法(平成26年法律第104号)第27条第3項に基づいて行われた。CSIRTは情報セキュリティインシデント対応のためのチームで、「政府機関の情報セキュリティ対策のための統一基準」でも体制の整備等が規定されている。
Q49-9	2	340	Google Chrome、Windows XP/Vistaのサポートが2016年4月に終了	ウェブブラウザー「Google Chrome」において、Windows XP/VistaおよびMac OS X 10.6～10.8のサポートを、2016年3月31日に終了した。2016年4月以降、これらのOSでもGoogle Chromeは動作するが、アップデートやセキュリティ修正は受けられなくなっている。2015/11/11	http://internet.watch.impress.co.jp/docs/news/729989.html	Googleでは、これらのOSについては「既にMicrosoftやAppleから積極的なサポートが提供されてない」ため、サポートを終了すると説明している。なお、Windows Vistaについては、Microsoftによるサポート終了は2017年4月11日の予定。Mac OS Xについては、Appleから明確なサポート期限は示されていない。
Q49-1	3	304	Yahoo!メールで約97万IDの約258万通の新着メールが消失	Yahoo!メールで発生した障害により、約97万件のIDに対して送信された新着メール約258万通が消失した。2015/8/28	http://www.security-next.com/062314	2015/8/28にYahoo!メールでシステム障害が発生し、約10時間にわたりYahoo!メールサービスへアクセスできない状況となった。障害時に切り替えた緊急用システムの不具合により新着メールが消失した。全5000万件のIDのうち、約97万件が影響を受けた。
Q49-2	4	284	不動産店従業員が芸能人の賃貸物件情報をTwitterへ投稿	大手不動産仲介会社の従業員が来店した芸能人の氏名と紹介した賃貸物件の情報をTwitterに書き込み、会社が謝罪文をウェブサイトに掲載した。2016/1/14	http://www.security-next.com/065919	従業員によるSNSへの不適切な書き込みがあとを絶たない。 2015/6/8にはりそな銀行が、従業員による芸能人の来店情報のTwitterへの書き込みを謝罪した。 2016/5/20には帝国ホテルが、従業員による芸能人の来館情報のTwitterへの書き込みを謝罪した。
Q49-8	5	239	暗号化型ランサムウェアのvvvウイルスが日本でも相当数流入	PC内のファイルを閲覧・編集できない形に暗号化し、ファイル復元の身代金を利用者に要求する不正プログラムのランサムウェアが日本国内で流行している。2015年12月にはファイルの拡張子を「.vvv」に変更するvvvウイルスによる攻撃の増加を複数のセキュリティベンダーが検知した。2015/12/15	http://news.mynavi.jp/news/2015/12/15/251/	IPAの「情報セキュリティ10大脅威2016」ではランサムウェアが3位であった。IPAでは2015年6月、2016年1月、4月と繰り返し注意を呼びかけている。 2016年前後よりAndroid端末の画面をロックするランサムウェアも登場し、スマートフォンを狙ったランサムウェアの種類は急増している。
Q49-12	6	205	レノボ社ThinkPadシリーズに外部への個人情報送信疑惑	レノボ社が販売するThinkPadおよびThinkCentre、ThinkStationシリーズにおいて、外部へ個人情報を送信しているとの疑惑が報じられた。2015/11/24	http://thehackernews.com/2015/09/lenovo-laptop-virus.html	「Lenovo Customer Feedback Program 64」というソフトウェアがタスクスケジューラに登録・自動実行されるようになっていた。「This task uploads Customer Feedback Program data to Lenovo」という説明が付けられていた。 この報道を受けて、レノボ社は「プリインストールアプリの利用動向について、製品の品質向上などを目的に一部利用情報の収集を実施しているが、収集データから個人やデバイスを特定できない」と釈明する声明を発表した。
Q49-7	7	174	ポップアップがサイト閲覧のみで表示されるゼロクリック詐欺の登場	ウェブサイトの閲覧中に会員登録完了のポップアップ画面を表示し、高額の料金を請求するゼロクリック詐欺の登場について、シマンテックが公式ブログで警告した。2016/1/26	http://news.mynavi.jp/news/2016/01/27/562/	ウェブサイト内のボタンのクリックでポップアップ画面を表示するのがワンクリック詐欺であるが、ウェブサイトの自動遷移(リダイレクト)によってクリック操作なしでポップアップ画面を表示するタイプの攻撃が登場している。高額の料金を請求するもののほかPCがウイルスに感染したとしてサポートへの電話を促すものもあり、2016年6月にIPAが注意を呼びかけている。
Q49-4	8	158	標的型サイバー攻撃相談件数が前年比6倍に増加	2015年度上半期(2015年4月～9月)にIPAの標的型サイバー攻撃特別相談窓口に寄せられた相談は246件で、2014年の同時期と比べて6倍であった。2015/10/26	https://www.ipa.go.jp/security/J-CRAT/index.html	IPAでは標的型サイバー攻撃を受けた際に、専門的知見を有する相談員が対応する「標的型サイバー攻撃特別相談窓口」を設置している。 日本年金機構の個人情報流出があった2015年6月以降に相談件数が大幅に増加した。相談件数は、2015年度下期が291件、2016年度上期が269件となっている。
Q49-11	9	141	Baidu社のAndroid用SDKにバックドア機能や不正プログラムを確認	トレンドマイクロ株式会社が、中国の検索エンジン「百度」(Baidu)のソフトウェア開発キット(SDK)「Moplus」に、バックドア機能が備わっていることを発表した。同社は、Moplus SDKを利用した不正プログラムをすでに確認しているとして、約1億人のAndroidユーザーが影響を受けたとみられ、警鐘を鳴らしている。2015/11/6	http://internet.watch.impress.co.jp/docs/news/729567.html	「百度」(Baidu)本社は、「Moplus SDKに関するすべての脆弱性に迅速に対応し、10月30日までに修正を完了した。Moplus SDKを利用しているすべてのサードパーティー開発者に対しても通知を行った。我々はあくまで今回の問題を『脆弱性』だと認識しており、意図的に実装した『バックドア』ではない。」と声明を発表している。

Q49 出来事

項番	認知順位	認知数(N=544)	表記	説明(概略)	参考:(2016年11月末時点)	追加コメント
Q49-13	10	138	AndroidOS 9億5千万台のスマホに影響をあたえる脆弱性が発覚	Androidに遠隔からでも端末を乗っ取れる深刻な脆弱性 " Stagefright " Exploitが発見された。Android搭載端末の電話番号さえ分かれば、不正なMMSメッセージ(MultipleMessageServiceメッセージ)を送り付けて被害者が知らないうちに端末を制御できてしまうという極めて深刻な脆弱性であった。2015/7/28	http://www.itmedia.co.jp/enterprise/articles/1507/28/news049.html	脆弱性はAndroid OS側の動画再生エンジンにあり、バージョン2.2(Froyo)以降のAndroidに存在していることから、Androidの95%に当たる9億5000万台に影響が及ぶと試算されている。Googleは直ちに修正パッチをメーカーやキャリア向けに公開し、ユーザーへの配信(修正パッチの適用)を促している。
Q49-5	11	135	全国初の無線LANただ乗りによる電波法違反容疑で逮捕者	他人が設置した無線LANルーターに無断で接続するただ乗りにより初の逮捕者がでた。容疑者は電波法の上限を超える電波を出力できる不正な無線LANルーターを使い、電波を解析し暗号強度の低いWEPの暗号を解読していた。2015/6/12	http://itpro.nikkeibp.co.jp/pc/atcl/trend/15/1000241/072200006/	事件をうけてIPAでは一般家庭での無線LAN利用についての注意喚起を2015年6月に行った。無線LANがただ乗りされ犯罪に利用された場合、無線LANの所有者に嫌疑がかかることもあり、AESなど強度の高い暗号方式を利用することが求められる。
Q49-6	12	123	複数のマスメディアでゼロデイ攻撃により個人情報が流出	2016/4/20から4/21に日本テレビ、J-WAVE、栄光ゼミナールのウェブサイトが不正アクセスをうけ個人情報が流出した。不正アクセスは、OSコマンドインジェクションのゼロデイ攻撃によるものであった。2016/4/20	http://www.security-next.com/071987	ゼロデイ攻撃とは、修正プログラムが提供される前の脆弱性を悪用して行われる攻撃である。2016年10月にはAdobeFlashPlayerの脆弱性を悪用するゼロデイ攻撃が確認されている。
Q49-15	13	80	2015年9月米中サイバーセキュリティ合意でサイバー戦争回避	2015年9月25日、アメリカを訪問していた中国の習近平国家主席とオバマ大統領が首脳会談を行い、その中で「米中では相互にサイバー攻撃を行わない」ことで合意した。2015/9/25	http://itpro.nikkeibp.co.jp/atcl/news/15/102003436/	今回合意では、主に経済分野での情報窃取や諜報などを対象としたサイバー攻撃である。米中両国が相互にサイバー攻撃を行わないことで合意したが、攻撃対象は米中両国の相互への攻撃であり、日本や他国へのサイバー攻撃を行わないとは述べておらず、日本や他国を踏み台にして、相手国のサイバースペースへ侵入・サイバー攻撃をしかけることは可能である。実際、2015年10月19日、セキュリティ会社の米CrowdStrike社が米中首脳会談から3週間のうちに、中国の攻撃グループが複数の米国企業にサイバー攻撃を仕掛けたことを確認したと発表した。
Q49-10	14	60	Gmailで、暗号化されていないメールに警告アイコン表示機能が追加	2016年2月9日、米Google「Safer Internet Day」にちなみ、新しいセキュリティ機能を公開した。その1つとして、暗号化されていないメールを受信したり、送信先のメールサービスがTLS暗号化をサポートしていない場合、Gmailで鍵がはずれたアイコンが表示されるようになった。認証されていない差出人によるメッセージを受信した場合、プロフィール写真やロゴが表示される場所に、クエスチョンマークが表示される。2016/2/9	http://news.mynavi.jp/news/2016/02/10/595/	またその他にも、Googleアカウントのセキュリティ設定を管理できる「Security Checkup」。Googleアカウントにログインすると、アカウント復旧情報や接続されている端末、アカウント権限、2段階認証プロセスの設定などが、このツール上で確認できる。
Q49-14	15	26	米国で普及しているガレージドア用リモコンに脆弱性が発覚	2015年6月4日、著名なセキュリティリサーチャーのSamy Kamkar氏が、米国で普及しているガレージドア用リモコンに脆弱性があることを発見したと発表した。2015/6/4	https://blog.kaspersky.co.jp/security-year-2015/10012/	この脆弱性をつくと、通信をのっとってガレージドアが操作される可能性がある。リモコンの通信で使用されている暗号の鍵を破るには、総当たり攻撃で30分程度かかるが、ソフトウェアのバグを突くことで10秒程度まで短縮できる検証結果をSamy Kamkar氏は示しており、製造元・ユーザ共に注意を呼びかけている。