項番	認知順位	認知数（N=367）	表記	意味説明	参考（2013年11月末時点）	追加情報
Q49-5	1	268	ﾜﾝﾀｲﾑﾊﾟｽﾜｰﾄﾞ	One Time Password（OTP）：認証のために1回しか使えない「使い捨てパスワード」のこと	http://www.atmarkit.co.jp/aig/02security/onetimepassword.html	トークンと呼ばれるワンタイムパスワード生成器が使われ、サーバ との時刻同期を利用して暗証番号と時刻の組み合わせから、一見ランダムな10桁程度の数字を生成して使う方式が一般的である。
Q49-2	2	256	BCP	事業継続計画（Business Continuity Plan）、災害などリスクが発生したときに重要業務が中断しないこと、万一の場合でも、目標復旧時間内に重要な機能を再開させリスクを最低限にするように準備しておく戦略的な計画。	http://www.weblio.jp/content/BCP	(内閣府）中央防災会議では、2015年度までの10年間に、大企業の全てと中小企業の半数以上の設定を目標としている。
Q49-22	3	250	ﾏｲﾅﾝﾊﾞｰ法案可決(2013年)	社会保障・税の共通番号法は5月24日に成立した。国民一人ひとりに番号をふり、年金などの社会保障と納税を1つの個人番号で管理する新制度が2016年1月から始まり、給付申請などの行政手続きが大幅に簡素化される。	http://www.nikkei.com/article/DGXNASFS2400E_U3A520C1MM0000/	個人情報の漏洩や第三者による悪用のおそれもあるため、政府は悪用を防ぐため、行政機関を監視・監督する「特定個人情報保護委員会」を設け、情報管理を徹底するなど対策を急ぐ。
Q49-32	4	230	Android向けｳｨﾙｽ	Android OSを搭載したスマートフォンやタブレットなどに感染するコンピューターウイルスで、Windows OSを標的にするウイルスと同様のものが流通している。	http://kotobank.jp/word/Android	密かに侵入しデータの消去や外部のコンピューターを攻撃する「トロイの木馬」、個人情報などを第三者に送信する「スパイウエア」、外部からの遠隔操作を可能とする「ボット」などが有名である。
Q49-25	5	227	Apache（Apache HTTP Server）	最も人気の高いWebサーバソフトウェアの一つ。1995年に開発が始まり、UNIX系OSを中心に幅広い人気を獲得した。フリーソフトウェアとして無償で公開され、ボランティアのプログラマたちの手によって長年開発が続けられている。	http://e-words.jp/w/Apache.html	NCSA（米国立スーパーコンピュータ応用研究所） httpdの細かいバグを修正したり新しい機能を追加するためのパッチ(patch)集として公開されていたが、途中から単体のWebサーバソフトとして公開された。
Q49-17	6	224	Office365	マイクロソフトのクラウドサービスで,BPOS(Microsoft Business Productivity Online Suite)という名称でExchange Onlineに始まり、2011年にOffice 365と名称を変え改良と機能拡張を経て現在に至っている。	http://news.mynavi.jp/series/365/001/	基本的にはメールサービス、インスタントメッセージングサービスに、公開Web サイト、オンライン会議、ドキュメント共有、そしてMicrosoft Office(Office 365 ProPlus)を加えたサービス群である。
Q49-20	7	205	Anonymous	匿名(Anonymous=アノニマス)で活動する国際的ハッカー集団。政府や企業に対する抗議活動の手段として、DDoS攻撃(分散型サービス拒否攻撃)によって、インターネット上の特定のサーバーをアクセス不能にしたり、サーバーに侵入し、データの改ざんや流出を行ったりする。	http://kotobank.jp/word/%E3%82%A2%E3%83%8E%E3%83%8B%E3%83%9E%E3%82%B9	2013年11月、和歌山県太地町のイルカ追い込み漁に抗議し、同町や同県、国の省庁など22のウェブサイトにサイバー攻撃を仕掛けると声明を出した。
Q49-15	8	198	WEP	Wired Equivalent Privacy の略であり、無線通信における暗号化技術で、送信されるパケットを暗号化して傍受者に内容を知られないようにすることで、有線通信と同様の安全性を持たせようとしている。	http://e-words.jp/w/WEP.html	秘密鍵暗号方式の一つで、IEEE 802.11bのセキュリティシステムとして採用されている。
Q49-24	9	158	SLA	ｻｰﾋﾞｽの提供者と委託者（顧客）との間で契約を行う際に、提供するサービス内容と範囲、品質に対する要求（達成）水準を明確にし、それが達成できなかった場合のルールを含めて、あらかじめ合意しておくこと。	http://www.itmedia.co.jp/im/articles/0507/03/news005.html	service level agreement / サービスレベル・アグリーメント / サービスレベルに関する合意 / サービス品質保証契約と言う。
Q49-18	10	152	資産管理ｻｰﾊﾞ	社内にある大量のパソコンやサーバー、プリンター、ネットワーク機器、ソフトウエアといった「IT資産」を統合的に管理するシムテムサーバである。必要なセキュリティパッチが適用されているかの管理を含む。	http://it-trend.jp/words/itshisan	韓国大規模サイバー攻撃の手口は国内で60%程度のシェアを誇るアンラボ社製品の各社に設置された資産管理サーバを乗っ取り、そこにmalwareを仕込んだと言われている。
Q49-4	11	121	2要素認証（2段階認証）	2-factor authentication ：2つの認証方式を併用して精度を高めた認証方式のこと	http://e-words.jp/w/2E38395E382A1E382AFE382BFE8AA8DE8A8BC.html	認証方式は、ID/パスワードなど対象者の知識を利用したもの、USBトークンやスマートカードなど対象者の持ち物を利用したもの、バイオメトリクスなど対象者の身体の特徴を利用したものの3方式がある。
Q49-3	12	93	CGI版PHPの脆弱性	2012年5月に発表された脆弱性：PHP（(Hypertext Preprocessor)のCGIラッパーに問題があり、リモートから文字列を送り込むことで、PHPのソースコードを閲覧されたり、Webサーバの権限で任意のコードを実行される恐れがある。	http://www.atmarkit.co.jp/news/201205/10/php543.html	PHPは、WEB開発等で広く使われているオープンソースの汎用スクリプト言語です。CGIとは Common Gateway Interface の略称で、WEBサーバーと外部実行プログラムの間のインターフェイス仕様・機構のこと、ラッパーは関数等を渡すプログラム機能名
Q49-16	13	91	SIP	Session Initiation Protocol の略であり、VoIPを応用したインターネット電話などで用いられる、通話制御プロトコルの一つ。1999年3月に発表された規格。	http://e-words.jp/w/SIP.html	転送機能や発信者番号通知機能など、同様のプロトコルと比べて公衆電話網に近い機能を備え、接続にかかる時間も短くなっている。各端末に割り当てられるアドレス形式が電子メールアドレスの形式に近い。
Q49-1	14	74	SpyEye	SpyEyeとは、感染したクライアントPCから銀行の口座情報やクレジットカード情報を盗み出すウイルス。オンラインバンキングに関連する情報を盗み出す以外にも、バックドア機能やキーロガーなど様々な機能が搭載されていることから非常に危険なウイルスとして知られている。	http://itpro.nikkeibp.co.jp/article/COLUMN/20110612/361290/	2011年4月18日頃、日本IBMの東京セキュリティー・オペレーション・センター（東京SOC）ではSpyEyeと呼ばれるウイルスに感染したクライアントPCの増加を検知した。
Q49-26	15	64	WSUS2更新ﾌﾟﾛｸﾞﾗﾑ(KB2734608)	Windows Server Update Services 3.0 Service Pack 2 用(Windows8等）の更新プログラム (KB2734608)	http://support.microsoft.com/kb/2734608/ja	WSUS 通信チャネル強化プログラム（2720211） を、確実に更新するための対応
Q49-11	16	58	61398部隊	中国人民解放軍の総参謀部の傘下にある電子情報などを担当する部隊。この部隊には数百人から数千人の隊員が所属し、上海の浦東新区の12階建てのビルなどを拠点にしている。	http://d.hatena.ne.jp/keyword/61398%C9%F4%C2%E2	「APT1」というグループによる大規模なサイバー攻撃が、米国Mandiant社などから疑われている。
Q49-10	17	47	RAT	Back OrificeやSubSevenに代表されるリモートからコントロールが可能なトロイの木馬プログラムの総称である。	http://itpro.nikkeibp.co.jp/word/page/10005030/	Remote Administration Tool, 又はRemote Access Trojan の略である。
Q49-23	18	44	ﾗﾝｻﾑｳｪｱ	マルウェア（悪意のあるソフトウェア）の一種で、ユーザーのデータを「人質」にとり、データの回復のために「身代金」（ransom）を要求するソフトウェアのことである。	http://www.sophia-it.com/content/%E3%83%A9%E3%83%B3%E3%82%B5%E3%83%A0%E3%82%A6%E3%82%A7%E3%82%A2	トロイの木馬としてパソコン内部に侵入し、勝手にファイルを暗号化したり、パスワードを設定したりして、正常にデータにアクセスできないようにしてしまう。
Q49-27	19	41	幽霊ﾄﾞﾒｲﾝ名	ghost domain names(幽霊ドメイン名)は、上位ドメインの管理者が削除したはずのドメインが利用可能なまま残るというDNSの脆弱性のことで、2012年2月に発表された。	http://securityblog.jp/words/5402.html	本来であれば名前解決が不可能になるはずのドメイン名が、委任情報の削除後も長期にわたって使用可能な状態になるよう仕向けることができる。脆弱性(CVE-2012-1033)
Q49-31	20	41	Flashback	2011年9月に発見された、MACを狙ったトロイの木馬型ウイルスである。	http://blog.trendmicro.co.jp/archives/5066	Adobe Flashプレイヤーのロゴを使い、Flashのインストラーを装って侵入し、Flashbackをインストール後、Macに保存されたユーザー名とパスワードを探し出すマルウエアである。
Q49-7	21	37	弱い暗号鍵の無効化(KB2661254)	Microsoftは2013年02月、長さが 1024 ビット未満である弱い RSA 暗号キーの使用をブロックする 主な Windows を対象とした更新プログラム (KB 2661254) を公開した。	http://support.microsoft.com/kb/2661254/ja	RSA暗号とは、桁数が大きい合成数の素因数分解問題が困難であることを安全性の根拠とした公開鍵暗号の一つ。RSAは発見者3名の名前から取った。
Q49-28	22	37	APT	APT（Advanced Persistent Threat）は標的型攻撃の一種に分類されるサイバー攻撃である。2011年頃から国内で標的型攻撃の脅威が注目され始めたことに伴い、このキーワードが登場する機会も増えた。	http://itpro.nikkeibp.co.jp/article/Keyword/20120717/409401/	標的型攻撃は組織の特定部門や特定の個人をターゲットにして、個人情報や機密情報を盗み出す攻撃で、手口としてマルウエアを添付したメールを送り付け、個人情報や機密情報を盗み出そうとするものが多い。
Q49-14	23	33	ｴｸｽﾌﾟﾛｲﾄｷｯﾄ	複数のエクスプロイトコード（セキュリティ上の脆弱性を攻撃するためのプログラム）をパッケージ化して、様々な脆弱性攻撃に対応できるようにしたプログラムのことである。	http://www.sophia-it.com/content/%E3%82%A8%E3%82%AF%E3%82%B9%E3%83%97%E3%83%AD%E3%82%A4%E3%83%88%E3%82%AD%E3	新しく発見された脆弱性への攻撃プログラムなどが随時追加されていくことで、さまざまな場面に対して攻撃を仕掛けることが可能
Q49-12	24	29	OAuth	オープンプロトコルであり、デスクトップ、モバイル、Webアプリケーションなどにセキュアなｱﾌﾟﾘ認可(authorization) の標準的手段を提供する。	http://ja.wikipedia.org/wiki/Oauth	あらかじめ信頼関係を構築したサービス間で、ユーザの同意のもとに、セキュアにユーザの権限を受け渡しする「認可情報の委譲」のための仕様である。
Q49-8	25	27	Open Resolver	オープンリゾルバは、外部の不特定の IP アドレスからの再帰的な問い合わせを許可している DNS（キャッシュ）サーバのこと、国内外に多数存在し、大規模な DDoS 攻撃の踏み台として悪用されているとの報告がある。	http://www.jpcert.or.jp/pr/2013/pr130002.html	DNSキャッシュサーバは自らが管理するドメインがなく、ネットワーク内のクライアントからの問い合わせを受けてインターネット上のドメイン名 やIPアドレスの探索を行い、結果を返答する。
Q49-9	26	27	pharming詐欺	ユーザーに気づかれないようにして金融機関などを装った偽のWebサイトに誘導し、不正に個人情報や暗証番号などの情報を得ようとする、ネット詐欺の手口のことである。	http://www.sophia-it.com/content/%E3%83%95%E3%82%A1%E3%83%BC%E3%83%9F%E3%83%B3%E3%82%B0	フィッシングは電子メールを通じて虚偽の情報を届け偽サイトに誘導するが、ファーミングはより直接的である。農業（farming）をもじった「pharming」と名づけられた。
Q49-13	27	25	ﾊｸﾃｨﾋﾞｽﾄ	サイバー犯罪に関する用語で、社会的・政治的な主張を目的としたハッキング活動（ハクティビズム）を行う者のことである。	http://www.sophia-it.com/content/%E3%83%8F%E3%82%AF%E3%83%86%E3%82%A3%E3%83%93%E3%82%B9%E3%83%88	自分たちの主張を声明として発表したり、政治的に敵対する政府や企業へ攻撃したりするために、敵方のサーバーをダウンさせたり、Webサイトを改竄したり、機密情報を盗んだりといったサイバー攻撃を行う。
Q49-29	28	24	Stuxnet	2010年にイランを中心とする中東各地域で発見された、標的型攻撃を行うマルウェアの通称である。イランの原子力施設の制御システムをダウンさせたことで知られる。	http://www.sophia-it.com/content/Stuxnet	ドイツのシーメンスが開発した産業用機器の制御システムを攻撃対象として、物理的な機器破損・稼動停止を引き起こした初めてのマルウェアであると言われている。
Q49-33	29	20	Need to Knowの原則	“情報を必要な人だけに開示する”考え方を、「Need to Knowの原則」という。情報セキュリティの基本だが、なかなか徹底できていない。	http://itpro.nikkeibp.co.jp/free/TIS/keitai/20040716/147358/	Need to Knowの原則を徹底するには、認証の基本情報であるIDと、そのIDから参照できる情報とのマッピングとを厳密に管理する必要がある。

項番	認知順位	認知数（N=367）	表記	意味説明	参考（2013年11月末時点）	追加情報
Q49-21	30	16	J-CSIP	2011年10月重工、重電等、重要インフラで利用される機器の製造業者を中心に情報共有と早期対応の場として、サイバー情報共有イニシアティブ（J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan ）が発足。	http://www.ipa.go.jp/security/J-CSIP/	経済産業省の協力のもと公的機関であるIPAが、情報ハブ（集約点）の役割として、参加組織間で情報共有を行い、高度なサイバー攻撃対策に繋げていく。
Q49-19	31	14	Gauss	2012年8月、レバノンの銀行から情報を収集することを焦点にしたFlameに似たウイルスが発見された。	http://blog.trendmicro.co.jp/archives/5761	コンピュータに関連する情報から、オンライン銀行やソーシャル・ネットワーキング・サービス（SNS）、Eメール、インスタントメッセンジャ（IM）などの個人情報の収集を行う。
Q49-30	32	12	ﾀｯﾌﾟｼﾞｬｯｸ攻撃	特別に細工された「トースト通知」と呼ばれるアプリのポップアップウィンドウをタップさせるようユーザに促す攻撃で、Android端末に潜む未知の脅威を利用している。	http://blog.trendmicro.co.jp/archives/6482	Android OS を搭載した端末における「User Interaction（UI）」のコンポーネントに存在する特定の脆弱性を利用します。
Q49-6	33	8	Shamoon(W32.Disttrack)	2012年8月に、サウジアラビアのある企業をターゲットにした標的型攻撃で利用されたマルウェアであり、MBR(マスターブートレコード)を上書きすると言われおり、感染後はOSを起動することができなくなる恐れがある。	http://xploitr.blogspot.jp/2012/08/shamoonw32disttrack.html	最大級の脅威と紹介しているサイトもある。