Q46. 用語

項番	認知順位	認知数（N=437）	表記	意味説明	参考（2014年11月末時点）	追加情報
Q46-4	1	365	ワンタイムパスワード	遠隔地にある端末からネットワークを通じてサーバコンピュータを利用する際に、アクセスしてくる人間が正規のユーザかどうかを検証する認証技術、「使い捨てパスワード」とも呼ばれる。	http://e-words.jp/w/E383AFE383B3E382BFE382A4E383A0E38391E382B9E383AFE383BCE38389.html	毎回異なる文字列になるように設定されており、ユーザが申告したパスワードも毎回異なった文字列としてサーバに送信される。このため、万が一通信経路上でサーバと端末のやり取りを盗み聞きされても、同じパスワードは二度と使えないため、サーバが不正使用されることはない。
Q46-17	2	356	特定秘密保護法案	漏えいすると国の安全保障に著しい支障を与えるとされる情報を「特定秘密」に指定、それを取り扱う人を調査・管理し、それを外部に知らせたり、外部から知ろうとしたりする人などを処罰することによって「特定秘密」を守ろうとする秘密保護法。	http://www.nichibenren.or.jp/activity/human/secret/about.html	2013年12月6日、第185回国会で成立し、同年12月13日に公布。2014年12月10日施行。
Q46-2	3	344	パーソナルデータ	国籍、名前、血液型、生年月日等、個人の固有の情報（個人の行動・状態に関するデータなど）。	http://www.kantei.go.jp/jp/singi/it2/info/h260625_siryou2.pdf#search='%E3%83%91%E3%83%BC%E3%82%BD%E3%83%8A%E3%83%AB%E3%83%87%E3%83%BC%E3%82%BF%E3%81%AE%E5%88%A9%E6%B4%BB%E7%94%A8%E3%81%AB%E9%96%A2%E3%81%99%E3%82%8B%E5%88%B6%E5%BA%A6%E6%94%B9%E6%AD%A3%E5%A4%A7%E7%B6%B1'	パーソナルデータの利活用に関する制度改正大綱では平成25年12月20日に高度情報通信ネットワーク社会推進戦略本部で決定された「パーソナルデータの利活用に関する制度見直し方針」を踏まえた検討に基づき、具体的に個人情報保護関係法令の改正等により措置する内容について、政府として方向性を示している。
Q46-1	4	332	マルウェア	コンピュータウイルス、ワーム、スパイウェアなどの「悪意のこもった」ソフトウェアのこと。“mal-”という接頭辞には「悪の」という意味があり、これとソフトウェアを組み合わせた造語。	http://e-words.jp/w/E3839EE383ABE382A6E382A7E382A2.html	遠隔地のコンピュータに侵入したり攻撃したりするソフトウェアや、コンピュータウイルスのようにコンピュータに侵入して他のコンピュータへの感染活動や破壊活動を行ったり、情報を外部に漏洩させたりする有害なソフトウェアのことを言う。
Q46-15	5	320	マイナンバー法案	全国民に個人番号を付番し、個人を一意に特定することを可能とする「行政手続における特定の個人を識別するための番号の利用等に関する法案（通称：マイナンバー）」。	http://www.itmedia.co.jp/enterprise/articles/1409/04/news013.html	基礎年金番号、介護保険の被保険者番号、自治体内での事務に利用する宛名番号等分野や組織ごとに個人を特定するための番号が存在。そこで複数の機関に存在する個人情報を、同一人の情報に確認できるように、国民1人1人に「個人番号」と呼ばれる番号を付番し、各分野、各機関で横断的に利用することができる「番号制度」である。
Q46-5	6	303	DDoS攻撃	“Distributed Denial of Service attack”の略。複数のネットワークに分散する大量のコンピュータが一斉に特定のネットワークやコンピュータへ接続要求を送出し、通信容量をあふれさせて機能を停止させてしまう攻撃。	http://e-words.jp/w/DDoSE694BBE69283.html	電子掲示板(BBS)等で参加者を募って大勢の攻撃者が意図的に一斉に攻撃を実行する場合とコンピュータや通信機器が攻撃者に乗っ取られ、所有者の知らないうちに攻撃に参加させられてしまう場合がある。複数のDNSの不特定からの問い合わせに応答する機器（オープンリゾルバ）等を利用し攻撃者の送信パケットを増幅し、ターゲットへ輻輳を起こしたりする。
Q46-18	7	229	リベンジポルノ	恋人や配偶者と別れたあと、リベンジ「復讐」を目的として、以前撮影した相手の猥褻な画像や動画、個人情報をインターネット上などに公開することを意味する語。	http://www.weblio.jp/content/%E3%83%AA%E3%83%99%E3%83%B3%E3%82%B8%E3%83%9D%E3%83%AB%E3%83%8E	特に米国で盛んに行われており、女性に精神的苦痛を与えるとして問題視されてきた。2013年10月に、米国カリフォルニア州で初めてリベンジポルノを禁止する法律が制定、違反者には懲役最大6か月と1000ドルの罰金が課せられる。
Q46-7	8	207	ゼロデイ攻撃	ソフトウエアのセキュリティーホールが発見された際、その情報や対策が広く告知される前に、そのセキュリティーホールを悪用したコンピューターウイルスが出回るなどの攻撃を受けた状態。セキュリティーホールの情報公開と攻撃に日にちが空かないことから「ゼロデイ“Zero Day”」と呼ばれる。	https://kotobank.jp/word/%E3%82%BC%E3%83%AD%E3%83%87%E3%82%A4%E6%94%BB%E6%92%83-183193	ソフトウエア開発企業・団体は研究者らからセキュリティーホールの報告を受けても対応策が整うまで情報公開を遅らせることがあるが、その間に情報が漏えいして攻撃を受ける可能性があるというリスクがある。

Q46. 用語

項番	認知順位	認知数（N=437）	表記	意味説明	参考（2014年11月末時点）	追加情報
Q46-3	9	147	ランサムウェア	トロイの木馬型のコンピュータウイルスの一種で、感染したコンピュータが正常に利用できないよう「人質」に取り、復元のために代価の支払いを要求するソフトウェア。“ransom”は「身代金」の意。	http://e-words.jp/w/E383A9E383B3E382B5E383A0E382A6E382A7E382A2.html	ランサムウェアがコンピュータに感染すると、パスワードを入力しないと利用できないようコンピュータをロックしたり、ファイルを暗号化して読み取れないようにしてしまう。そして、犯人に「身代金」を支払えば復元する旨のメッセージが出現する。
Q46-6	10	145	ブルートフォース攻撃	暗号の解読やパスワードの割り出しなどに用いられる手法の一つ。割り出したい秘密の情報について、考えられるすべてのパターンをリストアップし、片っ端から検証する方式。「総当たり攻撃」とも言う。英名の“brute force”の原義は「力づく」。	http://e-words.jp/w/E7B78FE5BD93E3819FE3828AE694BBE69283.html	秘密の情報が数字4桁など短く単純ならばコンピュータで自動的にすべての組み合わせを調べるのは容易だが、使える文字の種類や長さが増えるに従ってある程度以上に複雑な情報はこの方法では現実的に割り出すことはできない。
Q46-13	11	140	Apache Struts2の脆弱性	Webアプリケーションフレームワーク“Apache Struts 2”の最新版バージョン2.3.16.1に脆弱性が未だ残っている。Apache Struts 2には、外部からクラスローダーを操作されてしまう脆弱性（CVE-2014-0094）が存在。悪用されればWebサーバー内の情報を盗み取られたり、特定ファイルを操作されたり、Webアプリケーションを一時的に使用できない状態になる場合がある。攻撃者が操作したファイルにJavaコードが含まれている場合、任意のコードが実行される恐れもある。	http://www.atmarkit.co.jp/ait/articles/1404/24/news172.html	2014年4月24日、株式会社ラック（東京都千代田区）によると、Webアプリケーションフレームワーク「Apache Struts 2」に存在するものと似た脆弱性が、既にサポートの終了している「Struts 1」にも存在していると指摘し注意を呼び掛けている。
Q46-11	12	135	ショルダーハッキング	ソーシャルエンジニアリングの一つで、対象者がパスワードなどを入力する際のキー操作や画面を盗み見て、機密情報を盗み出す手口。「肩越しに盗み見る」という意味でこのように呼ばれる。	http://securityblog.jp/karuta/133.html	ショルダーハッキングの他にも、オフィスから出る書類のゴミからパスワードや手がかりとなる個人情報の記されたメモを探し出したり、ネットワークの利用者や顧客になりすまして電話で管理者にパスワードの変更を依頼して新しいパスワードを聞き出す、といった様々な手口がある。
Q46-8	13	134	水飲み場型攻撃	“Watering hole attack（water holing）”EMCコーポレーションのセキュリティ部門であるRSAセキュリティにより2012年に発表されたコンピュータの攻撃手法である。攻撃者をライオン、攻撃対象ユーザーが普段アクセスするウェブサイトを水飲み場に見立て、ライオンが獲物を待ち伏せすることになぞらえた言葉。	http://itpro.nikkeibp.co.jp/article/COLUMN/20140205/534763/?ST=attack	攻撃は、次の3段階で構成される。①攻撃対象ユーザーが普段アクセスしているウェブサイトを推測または観測により特定する②攻撃対象ユーザーがアクセスした際にマルウェアをユーザに気付かれないようにソフトウェアなどをダウンロードさせる（ドライブバイダウンロード）するよう、特定したウェブサイトを改ざん③攻撃対象ユーザーが改ざんされたウェブサイトアクセスにより、ユーザーのコンピュータにマルウェアが導入される。
Q46-14	14	121	CMSの脆弱性	“Content management system”の略。“CMS”は、ウェブコンテンツを構成するテキストや画像などのデジタルコンテンツを統合・体系的に管理し、配信など必要な処理を行うシステムの総称。2014年に入り、ウェブサイト改ざんの被害が急増。要因の1つとして、CMSの脆弱性が悪用され、改ざんが行われる。	https://www.ipa.go.jp/security/topics/alert20130913.html	IPAの脆弱性届出窓口には、攻撃に悪用された実例のあるCMS「WordPress」「Movable Type」について、古いバージョンがウェブサイトで使い続けられている届出が、6月から9月上旬までの約3ヶ月間で42件であった。
Q46-10	15	116	アカウントリスト型ハッキング	他社のWebサービスなどから流出したアカウント（ユーザーIDとパスワード）のリスト使って、別のWebサービスに対して不正ログインを試みるサイバー攻撃	http://itpro.nikkeibp.co.jp/article/COLUMN/20140625/566582/	リスト型アカウントハッキングは、「リスト型攻撃」「リスト攻撃」「パスワードリスト攻撃」「アカウントリスト攻撃」などとも呼ばれる。2013年末ごろから、総務省が発表資料などでリスト型アカウントハッキングという名称を使っているため、Webサービス提供者なども、この名称を使うようになっている。Webサービスごとにユーザーidとパスワードを使い分けていれば、不正にログインされにくくなる。
Q46-12	16	113	ペネトレーションテスト	コンピュータやネットワークのセキュリティ上の弱点を発見するテスト手法の一つで、システムを実際に攻撃して侵入を試みる手法。	http://e-words.jp/w/E3839AE3838DE38388E383ACE383BCE382B7E383A7E383B3E38386E382B9E38388.html	ネットワーク接続された情報システムが外部からの攻撃に対して安全かどうか、実際に攻撃手法を試しながら安全性の検証を行う。不正に侵入できるかどうかだけでなく、DoS（サービス拒否）攻撃にどれくらい耐えられるかを調べたり、侵入された際にそこを踏み台にして他のネットワークを攻撃できるかどうかなどを調べる場合もある。

Q46. 用語

項番	認知順位	認知数(N=437)	表記	意味説明	参考 (2014年11月末時点)	追加情報
Q46-23	17	108	エシュロン(Echelon)	アメリカ合衆国を中心に構築された軍事目的の通信傍受システム。フランス語で梯子の段を意味する語“echelon”に由来。	http://www.itmedia.co.jp/enterprise/articles/1108/06/news002.html	アメリカ国家安全保障局(NSA:National Security Agency)主体で運営と欧州連合等が指摘しているがアメリカ合衆国連邦政府自身が認めたことはない。敵性国家や敵性団体から漏れる電波を傍受したり、時には直接通信線を盗聴で情報を収集していると言われている。
Q46-16	18	94	ライフログ	生活“Life”の記録をデジタルなデータに残すこと。また、その残されたデータそのもの。総務省ワーキンググループでは「パソコンや携帯端末などで取得・蓄積された活動記録(行動履歴)情報」。	https://kotobank.jp/word/%E3%83%A9%E3%82%A4%E3%83%95%E3%83%AD%E3%82%B0-189035	ウェブ訪問先やアクセス記録、電子商取引の決済履歴、位置情報の3点をあげている。広義には、個人の起床時間や睡眠時間、移動場所や移動距離、食事のデータ、読書経歴や音楽再生の記録など。
Q46-20	19	91	SDN	“Software Defined Networking”の略。コンピュータネットワークを構成する通信機器を単一のソフトウェアによって集中的に制御し、ネットワークの構造や構成、設定などを柔軟に、動的に変更することを可能とする技術の総称。	http://e-words.jp/w/SDN.html	ネットワークの装置の配置や配線などの物理的構成とはある程度独立に、目的に応じて複数の仮想的なネットワークを構築することや、そのようにして構築されたネットワークである。
Q46-19	20	62	@police	警察庁による情報提供ウェブサイト。サイバー犯罪やサイバーテロの未然防止及び被害の拡大防止を図ることを目的に、ネットワーク・セキュリティに関する様々な情報を提供している。	http://www.npa.go.jp/cyberpolice/	全国の警察施設のインターネット接続点にセンサーを設置し、その観測結果から「インターネット治安情勢」を定期的に公表する「インターネット定点観測」を2003(平成15)年より公開している。グラフは毎時20分頃に更新され、インターネットにおける各種攻撃状況の変化、ワーム発生等を把握する基礎資料として活用されている。
Q46-9	21	55	MITB攻撃	“Man In The Browser”の略。Webブラウザーで銀行の手続きを実行するオンラインバンキングの情報を盗聴したり、不正送金を実行したりする攻撃。サーバ側からは不正を判断しにくく、攻撃全体でみるとウェブブラウザー内に第三者が居て、サーバとの通信やブラウザ上の表示を操作しているように見える事からこの名前が付いた。	http://itpro.nikkeibp.co.jp/atcl/keyword/14/260922/071400001/	攻撃者はウイルスを使って偽の画面を作り出し、不正操作に必要な情報を入力させたり、通信の内容を改ざんして不正送金を実行したりすること。ウイルスがオンラインバンキングの利用を検知すると、キーボードの入力情報や画面ショットを外部に送信して、IDやパスワードを盗み出す。
Q46-21	22	52	ZeuS	“Zbot”は、銀行口座や各種ログイン情報といったユーザーの個人情報を不正に収集するトロイの木馬型マルウェアのこと。“ZeuS”は、この“Zbot”を簡単に作成することができるツール、またはそのツールから作られた不正プログラムのことで、「Zbotファミリー」と呼ばれることもある。	http://securityblog.jp/words/812.html	感染すると、パソコン内の個人情報やキーボードの入力操作情報などを悪意ある犯罪者に詐取されたり、ボットネットとしてZbotを拡散するために悪意ある犯罪者にパソコンを不正に操られたりする可能性がある。セキュリティ対策企業では、「ZeuS/Zbot」を「Koobface」「Ilomo/Clampi」などとともに「三大危険ボットネット」と位置づけているところもある。
Q46-22	23	43	ダークネット	インターネット上で到達可能なIPアドレスのうち、特定のホストコンピュータが割り当てられていないアドレス空間。	http://www.sophia-it.com/content/%E3%83%80%E3%83%BC%E3%82%AF%E3%83%8D%E3%83%83%E3%83%88	情報通信研究機構は、ダークネット上を流れるパケットの主な種類として①マルウェアが感染対象を探査するためのスキャン②マルウェアが感染対象の脆弱性を攻撃するためのエクスプロイトコード(「脆弱性(セキュリティホール)を攻撃するために作成された簡易なプログラムの総称」)③送信元IPアドレスが詐称されたDDoS攻撃を被っているサーバからの応答、としている。
Q46-24	24	39	k匿名性	個人に関する情報(パーソナルデータ)に対して、他の情報との照合から個人の特定を防ぐための手法の一つ。あるデータにおいて、準識別子の組み合わせが必ず「k」個以上存在する性質を「k匿名性」という。	http://jpn.nec.com/press/201311/20131112_01.html	パーソナルデータの内、組み合わせにより個人の特定に繋がる可能性のある情報(準識別子)を複数のレコードにわたり元の値と関連付く共通の値に加工し、共通の値に加工されたレコード数が「k」個以上になることを保証する。