項番	認知順位	認知数(N=429)	表記	説明(概略)	参考:(2017年11月末時点)	追加コメント
Q46-9	1	237	匿名加工情報	「匿名加工情報」とは、個人情報を個人情報の区分に応じて定められた措置を講じて特定の個人を識別することができないように加工して得られる個人に関する情報であって、当該個人情報を復元して特定の個人を再識別することができないようにしたものをいう。	個人情報の保護に関する法律についてのガイドライン(匿名加工情報編)平成28年11月(平成29年3月一部改正)個人情報保護委員会	
Q46-24	2	215	ディープラーニング(深層学習)	音声の認識、画像の特定、予測など人間が行うようなタスクを実行できるようにコンピューターに学習させる手法です。ディープ・ラーニングでは、人間がデータを編成して定義済みの数式にかけるのではなく、人間はデータに関する基本的なパラメータ設定のみを行い、その後は何層もの処理を用いたパターン認識を通じてコンピューター自体に課題の解決方法を学習させます。	https://www.sas.com/ja_jp/insights/analytics/deep-learning.html#deepworld	ディープラーニングは機械学習の中の手法の一つ。従来の機械学習と異なり、ニューラルネットワークを何層も重ね、データ分析、学習能力を強化したもの。
Q46-8	3	195	WAF	WAF(Web Application Firewall) 外部ネットワークからの不正アクセスを防ぐためのソフトウェア(あるいはハードウェア)であるファイアーウォールの中でも、Webアプリケーションのやり取りを把握・管理することによって不正侵入を防御することのできるファイアウォールのことである。	http://www.sophia-it.com/content/WAF	WAFの特徴としては、従来のファイヤーウォールがネットワークレベルで管理していたことに対して、WAFはアプリケーションのレベルで管理を行う、といった点を挙げることができる。SQLインジェクションやクロスサイトスクリプティング、強制ブラウジングといった要求に対して、「攻撃」と見なして拒絶することができる。
Q46-20	4	194	ブロックチェーン	ブロックチェーン(Blockchain) 仮想通貨のビットコインを支える技術で、取引情報を分散管理する仕組み。 すべての取引情報をネットワーク上のコンピュータで共有しているため、1台のコンピュータで障害が発生しても継続して使用できる。また、改ざんされにくいという特徴がある。	http://itpro.nikkeibp.co.jp/atcl/keyword/14/463081/111600115/	銀行間取引にブロックチェーンを使用する実証実験が国内で相次いで行われている。みずほフィナンシャルグループ、三井住友銀行、三菱UFJフィナンシャル・グループの3大メガバンクとデロイトトーマツ グループによる実証実験が2016年1月から9月にかけて行われた。
Q46-19	5	191	CSIRT	CSIRTは、Computer Security Incident Response Teamの略で、サイバー攻撃などのセキュリティインシデントに対処するための組織の総称。 インシデント関連情報、脆弱性情報、攻撃予兆情報の収集や分析、インシデント対応の方針や手順の策定などを行う。	http://www.nca.gr.jp/outline/	CSIRTの役割は「消防」にたとえられる。CSIRTがあることでサイバー攻撃やウイルス感染などのセキュリティインシデントへの迅速で適切な対応が可能となり、被害を最小限に抑えることができると期待されている。 CSIRTは組織内や組織外の関係者と連携して巧妙化・複雑化するサイバー攻撃への対応にあたる。

項番	認知順位	認知数(N=429)	表記	説明(概略)	参考:(2017年11月末時点)	追加コメント
Q46-12	6	187	Apache Struts2の脆弱性	世界的に最も普及しているWebサーバ(HTTPサーバ)ソフトウェアのApache。普及しているがゆえに、脆弱性が発見されると大きな問題となる。2017年3月に公表された脆弱性は、ファイルをアップロードする時に使う機能「Jakarta Multipart parser」にあった。 第三者がこの脆弱性を突くHTTPリクエストを送信すると、StrutsのWebアプリケーションを実行するサーバー上で任意のコードが動かせてしまう。つまり、悪意のあるプログラムでも実行できてしまう。	https://itpro.nikkeibp.co.jp/atcl/column/14/346926/032100893/	
Q46-21	7	170	フィンテック	フィンテック(Fintech)は、金融を意味する「ファイナンス(Finance)」と、技術を意味する「テクノロジー(Technology)」を組み合わせた造語。 金融とITを融合した従来にない新しいサービス。	http://www.fujitsu.com/jp/group/fri/businesstopics/fintech/definition/	2016年5月25日の参議院本会議でフィンテック法案(改正銀行法案関連と改正資金決済法案)が可決された。今後フィンテックの普及が加速すると見られている。 改正銀行法には、仮想通貨交換業に係る法制度の整備などが盛り込まれている。
Q46-18	8	122	SOC	SOC(Security Operation Center) ネットワークやサーバのセキュリティアラートを統合的に監視し、サイバー攻撃の検出、分析、通知、対応策のアドバイスなどを行う。	http://securityblog.jp/words/soc.html	CSIRTがインシデントの対応に重点を置くのに対して、SOCはインシデントの検知に重点を置いている。 従来は、情報システム部門等がシステムやネットワークの管理を行いながら監視を行っていたが、高度化するサイバー攻撃への対応に高い専門性が求められることと、頻発するサイバー攻撃に適切に対処する必要があることから専門組織としてSOCが設けられるようになった。
Q46-4	9	117	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のことである。 ダークネットは未使用のIPアドレスであり、通常はダークネットに対してパケットが送信されることはほとんどない。しかし実際には、ダークネット上で相当数のパケットが観測されるという。	https://www.weblio.jp/content/ダークネット	
Q46-10	10	104	公認情報セキュリティ監査人資格制度	経済産業省が施行した「情報セキュリティ監査制度」に基づき、特定非営利活動法人日本セキュリティ監査協会(JASA)が情報セキュリティ監査人を認定する制度。	http://www.jasa.jp/qualification/about.html	情報セキュリティ監査を公正・公平に実施するため、監査人に求められる知識・経験・技術に応じて、「公認情報セキュリティ主任監査人」「公認情報セキュリティ監査人」「情報セキュリティ監査人補」「情報セキュリティ監査アソシエイト」の4つの資格を認定する。
Q46-2	11	99	MITB攻撃	MITB(Man in the Browser) PCに感染したウイルスがWebブラウザとサーバの通信を傍受して乗っ取り、一部を改ざんするサイバー攻撃。 オンラインバンキングのログイン後、ユーザに気づかれずに不正送金を行う。	http://securityblog.jp/words/790.html	正規のオンラインバンキングサイトにユーザが正規の認証プロセスでログインした後、ウイルスがブラウザを乗っ取りデータを改ざんして不正送金を行う。通信の暗号化や認証の強化で防ぐのは難しく、銀行側もユーザ側も間のウイルスによって不正が行われていることに気づきにくい。
Q46-23	12	90	SMB v1の脆弱性	SMBv1とはSMB バージョン1.0のことで、Windows 2000のころから使われている古いファイル共有プロトコルである。そしてWannaCryが悪用したMS17-010の他、MS16-114のようにしばしば脆弱性が見つかっている。	http://www.atmarkit.co.jp/ait/articles/1705/17/news043_3.html	Windows Vista, Windows Server 2008からSMB V2も実装され、Windows 8.1, Windows Server 2013R2以降では、SMB V1を削除して機能を無効化することも可能。

項番	認知順位	認知数(N=429)	表記	説明(概略)	参考:(2017年11月末時点)	追加コメント
Q46-17	13	89	CISA	CISAとは情報システムの監査および、セキュリティ、コントロールに関する高度な知識、技能および経験を有するプロフェッショナルとてISACA(The Information SystemsAudit and Control Association, Inc. 情報システムコントロール協会)が認定する国際資格。日本語では「公認情報システム監査人」と称する。	https://cisa.jp.net/	
Q46-13	14	87	RSA Conference	世界的なセキュリティのイベント。 年1回、アメリカのほかヨーロッパやアジアで開催され、セキュリティに関する講演、企業による展示会、CTF(Q50-5参照)が行われる。 幅広い分野のセキュリティの専門家や様々な業種の企業の関係者が参加している。	https://japan.emc.com/microsites/japan/techcommunity/learn/foundation/rsa-qa3.htm	1991年に暗号やインターネットセキュリティに関する情報交換の場としてアメリカで開催されたのがはじまり。 2016年のアジアでは、2016年7月20日～22日にシンガポールで開催された。
Q46-3	15	86	エクスプロイト	エクスプロイト(exploit)とは、スクリプト、あるいはプログラムの1つで、コンピュータ関連においてソフトウェアやハードウェアの脆弱性を利用し、悪意を持った行為のために書かれたものである。	https://it-words.jp/w/E382A8E382AFE382B9E38397E383ADE382A4E38388.html	エクスプロイトは、英語で偉業・手柄・功績を意味する単語。クラッカーの間ではそれをスラングとして用いていた。
Q46-1	16	84	セキュリティレジリエンス	セキュリティに対する回復力、耐久性 レジリエンス(resilience) 〔病気・不幸・困難・苦境などからの〕回復力、立ち直る力、復活力 「脆弱性 (vulnerability) 」の反対の概念	https://dictionary.goo.ne.jp/ej/70899/meaning/m0u/Resilience/ https://eow.alc.co.jp/search?q=vulnerability	
Q46-14	17	83	Security Intelligence	Security Intelligence(セキュリティ・インテリジェンス) システムや機器が出力する大量のデータを収集、分析することでセキュリティを総合的に捉える考え方。	http://it-words.jp/w/E382BBE382ADE383A5E383AAE38386E382A3E382A4E383B3E38386E383AAE382B8E382A7E383B3E382B9.html	従来のウイルス対策ソフトやファイアウォールが連携を考慮しないポイントのセキュリティ対策であったのに対し、様々なデータを一元的に収集し相関関係を分析することで、組織内部に潜む脅威を可視化する。 標的型攻撃のような個々の対策の隙を突く攻撃のリスクを減らすことが可能になる。
Q46-16	18	59	Bug Bounty(バグ発見報奨)	Bug Bounty Program(バグバウンティプログラム) 自社のソフトウェアに存在する脆弱性を見つけ報告した発見者に報奨金を支払う制度。 Google、Microsoft、Facebook、LINE、サイボウズなどが実施している。	http://business.nikkeibp.co.jp/atcl/report/15/061700004/040600092/?rt=nocnt	外部のセキュリティ研究者に脆弱性を指摘してもらうことで、セキュリティ問題の早期解決、サービスや品質の向上が可能になる。 企業側は少ないコストでセキュリティ向上を図ることができる。
Q46-7	19	56	SIEM	SIEM (Security Information and Event Management) さまざまなシステムや機器のログを一元的に管理し、異常や不正を検知するセキュリティシステム。 サーバ、ネットワーク機器、セキュリティ関連機器、アプリケーションなどから収集したログ情報を組み合わせて分析し、異常や不正を検知する。	http://itpro.nikkeibp.co.jp/atcl/column/14/494329/051400097/	従来、不正検知には主にIDS(不正侵入検知システム)が用いられてきた。しかしIDSでは、不正だと思われるパケットを検知したときに、ウイルス対策ソフトやサーバのログを併せて分析することで、不正検知の精度を高める、ということができなかった。 SIEMでは、収集したログを一元管理・分析することで、IDSよりも不正検知の精度を高められる。しかし、「どういう条件のとき不正と見なすか」の基準は、組織のシステム環境に大きく依存し、なおかつシステム環境の変更やサイバー攻撃の変化に合わせて更新する必要があるため、運用の負荷が大きいというデメリットもある。

項番	認知順位	認知数（N=429）	表記	説明(概略)	参考:(2017年11月末時点)	追加コメント
Q46-15	20	46	EDR（Endpoint Detection and Response）	EDR（Endpoint Detection and Response） 端末の挙動（システムアクティビティ）を記録し、その調査・解析によって脅威侵入の原因や経路、影響範囲を割り出す仕組みのこと。 標的型サイバー攻撃が高度化するる中で、早期解決のため注目されている。	https://www.infosec.co.jp/column/EDR%EF%BC%88Endpoint%20Detection%20and%20Response%EF%BC%89%E3%81%A8%E3%81%AF%EF%BC%9F.html	近年は、標的型サイバー攻撃などによって、標的組織用に個別化された攻撃が仕掛けられ、攻撃によって端末に「未知の脅威」が侵入するリスクが常に存在する。これらの潜在脅威や侵入原因などを調べ上げる能力が弱ければ、被害拡大のおそれが強まることが背景となって、近年はEDR製品に注目が集まっている。
Q46-11	21	40	OWASP	OWASP（Open Web Application Security Project） ウェブアプリやウェブサービスのセキュリティの促進を目的とした共同研究や関連活動を行う非営利団体。 フリーでオープンな形でのツール・ドキュメントの提供や、定期的な国際的会議等による研究・啓蒙活動を実施している。	https://www.owasp.org/index.php/Japan	代表的なプロジェクトとしてはOWASP Top 10がある。これは、3年に1度公開される、ウェブアプリケーションにおける重要な脆弱性やその脆弱性を作りこまないようにする方法などを示したドキュメントであり、組織のウェブアプリケーションのセキュリティ要件として、「OWASP Top 10に掲載されている脆弱性に対応できていること」を定めているところも多い。
Q46-5	22	37	CTF	CTF(Capture The Flag) セキュリティ技術の競技。パケット分析、プロトコル解析、システム管理、プログラミング、暗号解読などの知識や技能を競い合う。 問題を解くと「Flag」が得られるクイズ形式と相手のサーバに「Flag」を立てる攻防戦形式のCTFがある。 CTFを通して防御、解析、攻撃技術を実践的に学ぶことができ、セキュリティ人材を発掘・育成する場として活用する動きがある。	http://www.jnsa.org/seccon/	毎年ラスベガスで開催される世界最大規模のセキュリティの会議DEFCONでのCTFが有名。日本でも経済産業省、警察、IPA等が後援するSECCONが毎年開催されている。
Q46-6	23	33	eディスカバリ	eディスカバリ(Electronic discovery、e-discovery) アメリカにの電子証拠開示制度で、民事訴訟における電子的に保存されている情報の証拠開示手続きのこと。	http://www.sbbit.jp/article/cont1/28807	eディスカバリでは、企業に存在するすべての電子データから訴訟に関係する電子データを収集し提出する必要がある。しかし、企業内に存在する電子データ量は膨大であり、訴訟関連の情報だけを漏れなく把握することは簡単ではない。また、電子データは容易に情報を更新できるため、誤った扱いをすると証拠として認められず、削除・隠蔽の疑いによりペナルティを課されて訴訟に不利に働くこともある。 昨今の民事訴訟では、弁護士や証拠保管者（Custodian）に対応する時間に加え、eディスカバリ対応に費やすコストも大きくなって
Q46-22	24	29	FIDO	FIDO（Fast IDentity Online） 生体認証やジェスチャー認証などを利用した多要素認証のこと。 パスワードに代わる新しい認証技術の一つとして期待されている。	http://k-tai.watch.impress.co.jp/docs/column/keyword/759872.html	現状では、インターネットを通してパスワードで認証を行っているが、FIDOによる認証では、デバイスによる個人の認証と、オンラインサーバによるデバイスの認証を分離して行う。 このようにFIDOの特徴として、ユーザー視点では「パスワードを憶えなくて済む」こととと、「個人認証に用いる認証情報そのものはネットワーク上に流れず、サーバ上から漏れることもない」ということがある。