Q50. 用語

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
Q50-3	1	441	個人情報保護法改正	ビッグデータの利活用促進と個人情報の定義のグレーゾーン解消を背景に、個人情報保護法の改正が2015年9月3日に衆議院本会議で可決、成立した。全面施行は、2017年5月30日とすることが2016年12月20日に閣議決定した。	http://www.ppc.go.jp/personal/preparation/	改正法では、匿名加工情報の規定が新設された。 生体認証データなどの特定の個人の身体の一部をデータ化した符号は「個人識別符号」として個人情報として取り扱うことが明確化された。 保有する個人情報の件数が5000件を超えない小規模事業者は「個人情報取扱事業者」に該当しないとする要件が廃止され、ほぼすべての事業者が個人情報保護法に基づいた個人情報の取り扱いが必要となる。
Q50-9	2	431	不正アクセス禁止法	コンピュータのネットワークを介した不正利用を禁止する法律。 他人のIDやパスワード使用したコンピュータの不正使用、OSやアプリケーションの脆弱性を利用した攻撃によってアクセス権限のないコンピュータを不正に使用する行為、データやプログラムの改ざん行為を禁止している。	http://www.atmarkit.co.jp/ait/articles/0401/01/news130.html	システム管理者は、システムが不正アクセスに遭わないよう適切な管理措置を講じる必要があると規定されている(努力義務)。
Q50-4	3	391	標的型攻撃	特定の組織を狙って行われるサイバー攻撃。 組織の機密情報を盗むのが主な目的。 メールの添付ファイルやウェブサイトを利用してPCをウイルスに感染させ、そのPCを遠隔操作し組織内の情報を盗み出すなどする。	http://www.lac.co.jp/anti-apt/guidebook/chapter1/category1.html	標的型攻撃の手口は年々巧妙化・多様化しており、関係者や外部からの問合せを装ってメールを送り、受信者が気づかずにメールや添付ファイルを開くよう仕向けている。添付ファイルを使わずメール内のリンクでウイルスに感染させる攻撃もある。
Q50-23	4	342	ウェアラブル機器	ウェアラブル機器は、服のように身につけて使用するコンピュータで「ウェアラブル端末」とも呼ばれる。 腕時計型やメガネ型のウェアラブル機器が国内外の企業から相次いで発表されている。	http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/html/nc141330.html	ウェアラブル機器には、医療機器や健康促進のため機器として、位置情報、歩行の距離、高度、体温、心拍数、運動や活動などの健康状態を記録するものなどがある。 今後大きく普及すると期待されているが、個人の行動情報などプライバシーに関わるデータの取り扱いへの配慮などが課題となっている。
Q50-19	5	177	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。
Q50-12	6	171	Wordpressの脆弱性	ブログ作成の無料ソフトウェアWordPressの深刻な脆弱性に対する修正が2016年5月に公開された。 WordPress以外のソフトウェアについても脆弱性は頻繁に報告されている。利用者は、使用するソフトウェアに関する情報に注意し、最新版へのアップデートを適宜行う必要がある	http://www.itmedia.co.jp/enterprise/articles/1605/10/news070.html	Wordpressは、オープンソースのコンテンツ管理システムのソフトウェアである。2016年、6月、7月、10月にもWordPress用プラグインの複数の脆弱性に対して、注意喚起がIPAによる注意喚起が行われている。 http://www.ipa.go.jp/security/vuln/documents/
Q50-8	7	169	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。
Q50-21	8	145	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。
Q50-24	9	142	機械学習	機械学習はAI(人工知能)のアプローチのひとつ。 大量のデータをコンピュータが反復的に学習し、そこに潜む規則性やパターンを見つけ出すこと。 ビッグデータの解析を機械学習で行い、ショッピングサイトのおすすめ商品を表示するなど、様々なサービスで利用されている。	http://www.sas.com/ja_jp/insights/analytics/machine-learning.html	ハードウエアの低コスト化、コンピュータの処理能力の高度化により、機械学習の技術が飛躍的に向上している。 多くの機器がインターネットに接続され、大量のデータが集まるようになり、利用が加速している。 ディープラーニングは機械学習のひとつ。

Q50. 用語

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
Q50-18	10	119	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。
Q50-20	11	117	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。
Q50-10	12	111	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。
Q50-2	13	82	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。
Q50-13	14	67	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。
Q50-1	15	63	スタックスネット	スタックスネット(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。 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と言われ、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する。	http://www.sophia-it.com/content/Stuxnet	イランの原子力施設では1000台近くの遠心分離機がStuxnetの侵入を受けて稼動停止に陥った。2015年12月には、ウクライナの発電所のシステムが別のマルウェアを使ったサイバー攻撃を受け、数時間にわたって停電した。このように、サイバー攻撃の対象は一般的なITシステムだけでなく、産業用制御システム(ICS:Industrial Control Systems)にも拡大している。
Q50-14	16	63	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。
Q50-16	17	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。

Q50. 用語

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
Q50-7	18	57	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。
Q50-17	19	48	CISSP	CISSP認定資格 アメリカに本社がある(ISC)^2(ISCスクエア International Information Systems Security Certification Consortium)が開発・認定を行っている情報セキュリティ・プロフェッショナル認証資格。 世界的に通用するセキュリティの資格。	https://www.isc2.org/japan/cissp_about.html	セキュリティ資格で初めてISO17024を取得し、世界各国で97,000名以上(2015年3月現在)がCISSP認定資格を保持している。世界各国の多くの企業において、CISSP認定資格取得が情報セキュリティ関連業務従事者の必須事項とされているほど、評価の高い認証資格である。 受験資格として、「最低4年以上のフルタイムでのセキュリティ業務経験」を必要としており、継続的に学習を続けないと、資格を喪失してしまう点が特徴的である。
Q50-6	20	38	eディスカバリ	eディスカバリ(Electronic discovery、e-discovery) アメリカにおける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おり、企業経営における大きなリスクであると認知され始めている。 アメリカで訴訟を起こされれば日本企業も対象となり、製品の輸出などアメリカで事業を展開する日本企業は知っておく必要がある。
Q50-15	21	35	EDR(Endpoint Detection and Response)	EDR(Endpoint Detection and Response) エンドポイントである端末の挙動(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、影響範囲を迅速に割り出す仕組みのこと。	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。
Q50-22	22	32	FIDO	FIDO(Fast IDentity Online) パスワードに代わる新しい認証技術のひとつで、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。	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。
Q50-11	23	31	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。
Q50-5	24	28	CTF	CTF(Capture The Flag) セキュリティ技術の競技で、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.insa.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。