2015年　用語

項番	認知順位	認知数（N=437）	表記	意味説明	参考（2015年11月末時点）	追加情報
4	1	299	個人情報保護法改正	個人情報の保護を図りつつ、パーソナルデータの利活用を促進することによる、新産業・新サービスの創出と国民の安全・安心の向上の実現及びマイナンバーの利用事務拡充のために所要の改正を行うもの。	http://www.kantei.go.jp/jp/singi/it2/pd/pdf/gaiyou.pdf	2005年の個人情報保護法施行から10年、2015年9月3日、個人情報保護法を改正する法律が衆議院本会議で可決、成立した。改正法では、「個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする」とし、新たな産業創出や豊かな国民生活に役立つことを明示している。
15	2	193	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。
6	3	176	不正競争防止法改正	営業秘密の保護強化に主眼をおいたものであり、昨年発生したベネッセからの大量の個人情報持ち出し事件をはじめとして、海外メーカへ国内の先端技術の流出が相次いだことをきっかけとして強化されたものである。	https://digitalforensic.jp/2015/07/13/column370/	改正不正競争防止法が2015年7月3日の参院本会議で可決、成立した。 今回の改正では、特に刑罰が強化されていることが特徴である。その為、罰則を定める第21条が大幅に修正・追加されている。 (1)罰金の引き上げ もっとも分かりやすい改正点であるが、営業秘密侵害行為に関する罰金額が引き上げられた。現在は、個人の場合で最高1,000万円、法人の場合で最高3億円であるが、これが個人で2,000万円以下、法人で5億円以下となる。 (2)海外犯への重罰化 (3)犯罪収益の没収 (4)不正開示された情報を取得した者を処罰可能に (5)非親告罪化 (6)未遂罪の追加 (7)海外蔵置のクラウドサーバへの対応 (8)侵害の立証負担の軽減 (9)営業秘密侵害製品の輸出入の禁止 (10)消滅時効の延長
11	4	176	特定個人情報保護委員会	個人番号その他の特定個人情報の有用性に配慮しつつ、その適正な取扱いを確保するために必要な措置を講ずることを任務とする内閣府外局の第三者機関。 特定個人情報の取扱いに関する監視・監督（立入検査、報告徴求、指導、助言、勧告、命令等の権限の行使）、情報保護評価に関すること（指針の策定や評価書の承認）、特定個人情報の保護についての広報・啓発、これらの事務のために必要となる調査・研究及び国際協力等を行う。	http://itpro.nikkeibp.co.jp/article/COLUMN/20140313/543263/?rt=nocnt	個人情報保護法及び番号法が2015年に改正されたことに伴い、2016年1月に個人情報保護全般を取り扱う「個人情報保護委員会」に改組される予定
2	5	170	サイバーセキュリティ基本法	国のサイバーセキュリティに関する戦略や制度、政策等に関する基本方針が定められた法律のこと。2014年11月6日の衆議院本会議において可決、成立した。 基本法では、原則として各行政分野における施策の方針等が定められるため、サイバーセキュリティ基本法は、国のサイバーセキュリティに関する具体的な法制化や政策策定のための指針が定められているという位置づけ。	http://securityblog.jp/words/cybersecurity_basic_act.html	増大するセキュリティ上の脅威に鑑み、政府のサイバーセキュリティに関する役割や責任を明確にし、体制や機能を強化することを目的に成立したのがこのサイバーセキュリティ基本法である。同法は、国に対し「サイバーセキュリティに関する総合的な施策を策定し、および実施する責務を有する」と規定しており、官房長官をトップとした省庁横断の組織としてサイバーセキュリティ戦略本部が設置された。同本部は、セキュリティ戦略の策定や、内閣に対する、行政各部の指揮監督に関する意見具申などを行う。
9	6	146	忘れられる権利	プライバシー保護のための新しい権利の概念。インターネットの発達により、ホームページ上などに各種の個人情報が永年消えずに残るようになった。このことから、適切な期間を経た後にまで情報が残っている場合、これを削除したり消滅させたりできる権能があってしかるべきだとする考え方に基づくもの。	https://kotobank.jp/word/%E5%BF%98%E3%82%8C%E3%82%89%E3%82%8C%E3%82%8B%E6%A8%A9%E5%88%A9-189857	「忘れられる権利」を明確に認めたのは、11年に判決が出たフランス女性らの訴訟である。女性が若き日に撮影したヌード写真が、数十万以上ものホームページに名前と共に転載された。このため、グーグルに対して検索からの削除を求めることを認めた判決。

項番	認知順位	認知数（N=437）	表記	意味説明	参考（2015年11月末時点）	追加情報
16	7	140	IoT	Internet of Things コンピュータなどの情報・通信機器だけでなく、世の中に存在する様々な物体（モノ）に通信機能を持たせ、インターネットに接続したり相互に通信することにより、自動認識や自動制御、遠隔計測などを行うこと。	http://e-words.jp/w/IoT.html	IoE（Internet of Everything） 「ありとあらゆるものが接続されたインターネット」という意味で、モノのインターネットと、人やデータ、情報、ソフトウェアなどが中心の従来からあるインターネットが統合された姿を指す。とはいえ、従来のインターネットとの違いはモノが接続されている点であるため、実際上はIoTとほぼ同義として用いられることが多い。主にCisco Systems社が提唱している用語。
3	8	129	NISC	2015年1月、政府が内閣官房に設置したサイバーセキュリティ関連の組織のこと。前身は、2005年4月に設置された内閣官房情報セキュリティセンター（NISC）。 2015年1月に施行された「サイバーセキュリティ基本法」に基づき、我が国のサイバーセキュリティ戦略を策定する組織として、内閣に「サイバーセキュリティ戦略本部」が設置され、同時に、内閣官房情報セキュリティセンターを改組し「内閣サイバーセキュリティセンター」が設置された。	http://www.nisc.go.jp/about/index.html	NISCの業務 ・　情報システムに対する不正活動の監視・分析 情報通信ネットワーク又は電磁的記録媒体を通じて行われる、行政各部の情報システムに対する不正な活動の監視及び分析。 ・　重大事象の原因究明調査 行政各部におけるサイバーセキュリティの確保に支障を及ぼすおそれがある、重大な事象の原因究明のための調査。 ・　行政各部に対する監査等 行政各部におけるサイバーセキュリティの確保に関し必要な助言、情報の提供その他の援助及びサイバーセキュリティの確保のために必要となる監査。 ・　サイバーセキュリティに関する企画・立案、総合調整 上記の他、サイバーセキュリティの確保に関する施策の企画及び立案並びに総合調整。
8	9	121	サイバー保険	サイバー攻撃による損害を懸念する企業や組織向けの商品。それぞれの保険によってカバーされる詳細な内容は異なるが、基本的には漏えいした情報の損害賠償、他者への業務阻害などに対する損害賠償、インシデントの原因や被害範囲の調査にかかる費用の補償などが組み込まれている。	http://www.daj.jp/news/151023_01/	国内においては、損害保険ジャパン日本興亜、AIU損害保険などが販売している。
13	10	88	やり取り型攻撃	特定の企業や個人を狙ったサイバー攻撃である「標的型攻撃」の一種。攻撃対象にいきなりウイルス添付メールを送信するのではなく、無害のメールで通常のやり取りを何回か行い、ファイル添付のメールが送られても不自然ではない状況を作ってから、ウイルス添付メールを送り付ける。	http://www.nikkei.com/article/DGXMZO7996570R21C14A1000000/	具体的な例としてよく挙げられるのが、商品内容の問い合わせやクレームを装ったもの、あるいは採用窓口などを狙ったものがある。 まず、顧客や取引先のフリをして問い合わせ窓口に質問や苦情の電子メールを送る。そして何度か電子メールでやりとりをしてから、具体的な内容を書いた資料に見せかけて不正プログラムを仕組んだ添付ファイルを送る。 採用窓口を狙った場合は、電子メールで採用状況などを問い合わせたあと、履歴書に見せかけた不正な添付ファイルを送って相手に開かせる。こうした手順を踏むことで、相手が疑いなく添付ファイルを開く可能性を高めている。
12	11	87	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。
18	12	82	M2M	M2M(Machine to Machine) 機械と機械が通信ネットワークを介して互いに情報をやり取りすることにより、自律的に高度な制御や動作を行うこと。	http://e-words.jp/w/M2M.html	M2Mシステムの例としては、工場内での工作機械の集中制御や、自動販売機の在庫状況の遠隔監視、様々な建物に設置されたエレベーターの稼働状況の監視、実際の自動車の走行状況を集約したリアルタイムの渋滞情報、発電所や家庭の配電盤などにセンサーやコンピュータを導入してきめ細かな電力使用料の監視や供給制御を行なうスマートグリッドなどが挙げられる。

項番	認知順位	認知数（N=437）	表記	意味説明	参考（2015年11月末時点）	追加情報
10	13	81	パーソナルデータの匿名化	データに含まれる名前や生年月日、住所といった情報を削除したり、変更を加えたりすることで、個人を特定できないようにすること。 パーソナルデータは、個人の名前や住所、さらには個人の社会経済的属性等、主に民間企業が持つ大量の「個人情報」と認識されており、いわゆる「ビックデータ」の1つと考えることができる。民間企業を中心に、パーソナルデータの利活用が注目されており、営利目的のためのパーソナルデータの販売だけでなく、それをもとにしたさらなるビジネスの可能性が追究されている。そうした状況のなかで、パーソナルデータに含まれる個人情報の保護が、パーソナルデータの提供における重要な論点になっている。	http://www.nii.ac.jp/userdata/results/pr_data/NII_Today/64/p10-11.pdf http://www.kantei.go.jp/jp/singi/it2/pd/	個人情報の保護に関する法律及び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律の一部を改正する法律（H27.9月公布）で以下の点が整備された。 ・利用目的の変更を可能とする規定の整備 ・匿名加工情報に関する加工方法や取扱い等の規定の整備 ・個人情報保護指針の作成や届出、公表等の規定の整備
17	14	57	CSMS	CSMS(Cyber Security Management System) 産業用オートメーション及び制御システム（IACS：Industrial Automation and Control System）を対象としたサイバーセキュリティ(注)のマネジメントシステム。	http://www.isms.jipdec.or.jp/csms/index.html	CSMS認証基準 IEC 62443シリーズでは、制御システムセキュリティ実現に活用できる基準の一つであるIACSのためのセキュリティマネジメントシステムとしてIEC 62443-2-1が規格化されている。 このIEC 62443-2-1に基づき、IACS分野のセキュリティマネジメントシステム認証基準として「CSMS認証基準(IEC 62443-2-1:2010)」が策定された。
5	15	53	IDaaS	IDaaS(Identity as a Service) ID管理や認証システムをクラウド上でサービスとして提供する。	http://www.atmarkit.co.jp/ait/articles/1508/07/news034.html	IDaaSは大きく「IDマネジメント機能」と「アクセスコントロール機能」の2つから構成される。 1.IDマネジメント機能（IDM：Identity Management） IDentityやパスワードといったユーザ属性をIdP(Identity Provider)として管理する機能 2.アクセスコントロール機能 「認証」と「認可」
7	16	42	eディスカバリ	eディスカバリ(Electronic discovery、e-discovery) 米国民事訴訟の手続きの一つとしてDiscovery（証拠開示制度）がある。これは陪審審理、裁判官審理の前に訴訟当事者同士が訴訟に関連するすべての資料を自ら収集し、開示する制度のことである。現在、企業に存在する資料のほとんどが電子データで作成されているため、電子データの開示手続をe-Discoveryという。	http://www.sbbit.jp/article/cont1/28807	昨今、価格カルテル（独禁法違反）の摘発や製造物責任訴訟などによって、日本企業が莫大な賠償金額を支払ったり、取り締まりの対象となることが増えている。各種メディアによる報道では、賠償金額や制裁金額の大きさばかり目立つが、直面した企業はそれ以外の対応にも多額のコストと時間を費やしている。特にe-Discovery（電子証拠開示制度）対応は、その中でも大きな割合を占める重要な手続きの1つである。
14	17	33	SIEM	SIEM(Security Information and Event Management) さまざまなネットワーク機器やサーバーから、多様かつ膨大なログを収集して一元管理し、それらを基に不正を検知する新しいセキュリティシステムのこと。	http://itpro.nikkeibp.co.jp/atcl/column/14/494329/051400097/	ファイアウオール、プロキシーサーバー、IDSといったネットワーク・セキュリティ機器、Webサーバーやメールサーバーなどのサーバーから「レシーバー」機能でログを収集し、「データストア」に保存。「アナライザー」機能によって、複数種類のログを組み合わせて分析し不正を検知する。 さまざまなログを分析し、どういう条件のとき不正と見なすか、というルールは、ユーザー企業のシステム環境に大きく依存するので、個別に決める必要がある。しかも、システム環境の変更やサイバー攻撃の変化に合わせて、更新していかなければならない。そのため、IDSよりも不正検知の精度を高められるが、その分、運用の負荷が大きい。
1	18	21	SDx	Software-Defines … ITインフラの論理構成をソフトウェアによって定義・制御する考え方を表したもの。	http://www.sbbit.jp/article/cont1/29935	サーバを対象としたSDC（Software-defined Computing）やストレージを対象としたSDS（Software-defined Storage）、ネットワークを対象としたSDN（Software-defined Networking）、さらにはインフラ全体を包含したSDI（Software-defined Infrastructure）、データセンタを包含したSDDC（Software-defined Datacenter）など、さまざまな領域が対象となっている。