情報通信技術の進展とサイバーセキュリティに関する用語集

A

➢ **Anonymous（アノニマス）**

インターネット上の匿名掲示板やオンラインコミュニティを通じて形成され、政府や企業に対して抗議行動やサイバー攻撃などを行う国際的ハッカー集団のこと。情報の自由に対する脅威とみなしたものに対して大規模な攻撃を行っている。Anonymousは「匿名の」という意味の形容詞。

➢ **APCERT（エーピーサート）**

Asia Pacific Computer Emergency Response Teamの略で、アジア太平洋地域に所在するCSIRT組織のコミュニティのこと。同地域内のCSIRTの間でインシデント対応時における連携、情報共有、共同研究開発、インターネットセキュリティの普及啓発等の活動を行っている。

B

➢ **BCM（主要事項「4.4　災害とセキュリティ対策」を参照）**

Business Continuity Managementの略で、事業継続マネジメントのこと。災害等のリスク発生時に企業が事業を継続するうえでのリスクを特定し、それに対する対応計画を事前に策定するなど一連のマネジメントプロセスで、BCPの上位概念にあたる。

➢ **BCP（主要事項「4.4　災害とセキュリティ対策」を参照）**

Business Continuity Planの略で、事業継続計画のこと。自然災害への対策のみならず、情報セキュリティ対策を含めた形での計画の策定が求められる。経済産業省から2005年に「事業継続計画策定ガイドライン」が発表された。

➢ **BYOD**

Bring Your Own Deviceの略で、企業などで従業員が私物の情報端末などを業務で利用すること。コスト削減などのメリットがあるが、情報漏えい・ウイルス感染などへの対策や、紛失・盗難時の対応などが複雑になることが多い。

C

➢ **CERT/CC（サートシーシー）**

Computer Emergency Response Team/ Coordination Centerの略。Morrisワーム事件を契機に、1988年に米国で設立された世界初のCSIRTであり、カーネギーメロン大学ソフトウェア工学研究所内で運営されている。

➢ **CIO**

Chief Information Officerの略で、最高情報責任者のこと。組織内の情報システムや情報戦略を統括する。

➢ **CISO**

Chief Information Security Officerの略で、最高情報セキュリティ責任者のこと。組織内の情報管理及びその運用を担当し、情報セキュリティを統括する。

➢ **CISSP**

Certified Information Systems Security Professionalの略で、国際的に認められた情報セキュリティプロフェッショナル認証資格のこと。2004年に米国規格協会よりISO/IEC 17024の認証を受け、認定資格試験としての信頼度が高くなった。

➢ **CRYPTREC（クリプトレック）**

Cryptography Research and Evaluation Committees の略で、電子政府推奨暗号（「電子政府推奨暗号リス

ト」を参照）の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討する総務省と経済産業省の共同プロジェクトのこと。

➢ **CSIRT（シーサート）（主要事項「4.3　事故前提のセキュリティ対応体制」を参照）**

Computer Security Incident Response Teamの略。インシデントに対応する組織横断の専門チーム。

➢ **CSMS**

Cyber Security Management Systemの略で、制御システムセキュリティにおけるセキュリティマネジメントシステムのこと。一般財団法人日本情報経済社会推進協会（JIPDEC）が認定組織となり世界に先駆けて認証体制を構築した。

➢ **CSO**

Chief Security Officerの略で、最高セキュリティ責任者のこと。組織のセキュリティ対策を統括する。

➢ **CSSC**

Control System Security Centerの略で、技術研究組合制御システムセキュリティセンターのこと。重要インフラ等の制御システムのセキュリティを確保するため、研究開発、国際標準化活動、認証、人材育成、普及啓発、各システムのセキュリティ検証等を行う技術研究組合として、2012年3月に設立された。

➢ **CYMAT（サイマット）**

CYber incident Mobile Assistant Teamの略で、情報セキュリティ緊急支援チームのこと。NISC内に設置されており、省庁等に対するサイバー攻撃に対して被害拡大防止、復旧、再発防止などのための技術的な支援と助言等を行う。

D

➢ **DCS**

Distributed Control Systemの略で、分散制御システムのこと。大規模なプロセスを、ネットワークで接続された小型の制御装置に分散して制御するシステムで、工場や各種プラントのシステムで利用される。

➢ **DoS攻撃（ドス攻撃）**

DoSはDenial of Serviceの略で、サービス妨害攻撃のこと。標的となるマシンの処理量や通信量を増加させたり、ソフトウェアの脆弱性や設定の不備を悪用したりして、マシンの機能の低下や停止、あるいはネットワークを利用不可能な状態にすることを意図した攻撃。DoS攻撃のうち、ネットワーク上の多数のマシンから一斉に行うものをDDoS（Distributed Denial of Service）攻撃という。

E

➢ **EC**

Electronic Commerceの略で、電子商取引のこと。「電子商取引」を参照。

➢ **EDSA**

正式名称は、ISASecure Embedded Device Security Assurance（EDSA）Certification。ISCIが運営する制御機器（組込み機器）のセキュリティ保証に関する認証制度のこと。日本ではCSSCが国内認証業務を実施している。

➢ **ENCS**

European Network for Cyber Securityの略で、欧州の重要インフラのレジリエンス（回復力）を高めることを任務とする非営利組織のこと。本拠地はオランダのハーグに置かれている。CSSCと覚書を締結し、制御システムのセキュリティ対策の高度化等に関する連携を進めている。

➢ **ENISA（エニーサ）**

European Union Agency for Network and Information Securityの略で、欧州ネットワーク情報セキュリ

ティ庁のこと。EUの機関で、ネットワークセキュリティ及び情報セキュリティに関する予防・対応能力を促進することを任務とする。

F

➢ **FIRST（ファースト）**

Forum of Incident Response and Security Teamsの略で、世界中のCSIRT組織が情報交換やインシデント対応に関する協力を行うことを目的とした非営利国際団体のこと。米国のCERT/CCが中心となって設立された。

G

➢ **GSOC（ジーソック）**

Government Security Operation Coordination teamの略で、政府機関情報セキュリティ横断監視・即応調整チームのこと。NISC内に設置されており、政府機関の情報システムにGSOCセンサーを設置し、攻撃等の脅威を24時間体制で監視している。

I

➢ **ICS-CERT（アイシーエスサート）**

Industrial Control Systems Cyber Emergency Response Teamの略で、米国国土安全保障省の産業制御システムセキュリティを担当する機関のこと。

➢ **IDS**

Intrusion Detection Systemの略で、侵入検知システムのこと。ネットワークあるいはホストへの攻撃や侵入を検出し、管理者への通報を行うシステム。ファイアウォールと組み合わせて、セキュリティをより強固にする目的で使われる。

➢ **IEC**

International Electrotechnical Commissionの略で、国際電気標準会議のこと。電気及び電子技術分野における国際標準の策定を行う国際標準化機関。

➢ **IEC 62443**

制御システムセキュリティに関する国際規格のこと。制御システムに関係する組織としては「装置ベンダ」、「インテグレータ」、「事業者」などがあるが、IEC 62443ではそれぞれに向けた要件が規定されている。

➢ **IETF**

Internet Engineering Task Forceの略で、インターネットで利用されるプロトコル（通信規約）やアーキテクチャ等の技術標準を策定するための民間主導の標準化団体のこと。

➢ **IPA**

Information-technology Promotion Agencyの略で、独立行政法人情報処理推進機構のこと。技術・人材の両面から、日本におけるソフトウェア及び情報処理システムの健全な発展を支えるために設立された経済産業省所管の独立行政法人。1970年の設立当時は特別認可法人情報処理振興事業協会であったが、2004年に独立行政法人化され、現在の名称となった。

➢ **IPS**

Intrusion Prevention Systemの略で、侵入防止システムのこと。IDSの防御機能を強化したもので、不正アクセスを検知すると、その通信を遮断する。

➢ **IPスプーフィング**

攻撃元を隠蔽するために、送信元IP アドレスを詐称し、他の送信元になりすます攻撃手法。サービ

ス妨害攻撃などのために利用される。スプーフィング（Spoofing）とはなりすましのことである。

➢ **ISAC（アイザック）**

Information Sharing and Analysis Centerの略で、重要インフラ等の業界（分野）内でセキュリティに関する情報共有を行うための組織のこと。通信、電力、金融、水道、サプライチェーンなどの分野固有のISACがある。米国で多く設立されているが、日本でもTelecom-ISAC Japanや金融ISACが設立されている。

➢ **ISCI（イスキー）**

ISA Security Compliance Instituteの略（ISAはInternational Society of Automation の略。）で、制御システムに係る規格の標準化活動及び普及啓発活動等を実施する国際的なセキュリティ認証推進組織のこと。

➢ **ISMS（主要事項「4.2　情報セキュリティマネジメントシステム」を参照）**

Information Security Management Systemの略で、情報セキュリティマネジメントシステムのこと。企業や行政機関などの組織において、情報セキュリティの確立、実施、維持、継続的改善によって、その組織の目的を達成するための、一連の必要な要素（組織の構造、役割及び責任、計画、運用など）とされる。

➢ **ISO**

International Organization for Standardization の略で、国際標準化機構のこと。電気及び電子技術分野を除く全産業分野（鉱工業、農業、医薬品等）における国際標準の策定を行う。

➢ **ISO/IEC**

ISO及びIECの両組織が共同で作成した国際規格は、ISO/IEC（番号）という規格番号で表記される。

➢ **ISO/IEC 15408（CC）**

ISO/IEC 15408 Common Criteriaの略で、IT関連製品やシステムの開発、製造、運用に関わるセキュリティ品質を客観的に評価するための国際評価基準のこと。

➢ **ISO /IEC 27000ファミリー**

企業や組織における情報セキュリティマネジメントシステム（ISMS）に関する国際規格のこと。ISO/IEC 27001は組織がISMSを構築するための要求事項を示している。

➢ **ITU-T**

International Telecommunication Union（Telecommunication Standardization Sector）の略で、国際電気通信連合の電気通信標準化部門のこと。ITU-TのStudy Group 17（SG17）がセキュリティ専門委員会であり、関係組織での情報共有と意見交換、セキュリティ標準に関わる普及活動などを行っている。

➢ **ITスキル標準**

IPAが策定している、IT関連サービスの提供に必要とされる能力を明確化・体系化した指標のこと。産学における教育・訓練等における基準を提供しようとするもの。

➢ **ITセキュリティ評価及び認証制度**

JISECを参照。

➢ **ITリテラシー（主要事項「7.2　ITリテラシーと情報倫理」を参照）**

インターネットや各種デバイス等、情報通信技術を使う上での基本的な知識や素養のこと。ITリテラシーの不足により、サイバー犯罪や思わぬトラブルに巻き込まれる可能性がある。

J

➢ **JCMVP**

Japan Cryptographic Module Validation Programの略で、暗号モジュール試験及び認証制度のこと。ISO/IEC 19790:2006（JIS X 19790:2007）に基づく認証制度であり、この制度に基づく認証を取得することにより、セキュリティが確保された暗号モジュールであることを証明できる。

➢ **J-CSIP（ジェイシップ）**

Initiative for Cyber Security Information sharing Partnership of Japanの略で、サイバー情報共有イニシアティブのこと。サイバー攻撃による被害拡大防止のため、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IPAが2011年10月に設置したもの。

➢ **JIPDEC（ジプデック）**

Japan Institute for Promotion of Digital Economy and Communityの略で、一般財団法人日本情報経済社会推進協会のこと。プライバシーマーク制度やISMS適合性評価制度の運営を行っている。

➢ **JISEC**

Japan Information Technology Security Evaluation and Certification Scheme の略で、ITセキュリティ評価及び認証制度のこと。セキュリティ機能の適切性･確実性をISO/IEC 15408に基づいて第三者（認証機関の認定を受けた評価機関）が評価し、その評価結果を認証機関が認証する制度。

➢ **JPCERT/CC（ジェイピーサート／シーシー）**

Japan Computer Emergency Response Team Coordination Centerの略で、コンピュータ緊急対応センターのこと。主に日本国内で発生したコンピュータセキュリティインシデントについて、報告の受付、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを行う。

➢ **J-SOX法（ジェイソックス法）**

「金融商品取引法」（昭和23年法律第25号）の2006年の改正「証券取引法等の一部を改正する法律」（平成18年法律第65号）の中で導入された「財務報告に係る内部統制の強化等に関する制度整備」のこと。同制度により「四半期報告書の提出」、「内部統制報告書の提出」、「確認書の提出」が上場会社等に義務付けられた。同法の名称は、米国のSOX法（Sarbanes–Oxley Act）にちなんで呼ばれている。

➢ **JVN**

Japan Vulnerability Notesの略で、日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的とする脆弱性対策情報ポータルサイトのこと。

M

➢ **Man-in-the-Middle攻撃**

「中間者攻撃」を参照。

N

➢ **NICT**

National Institute of Information and Communications Technologyの略で、独立行政法人情報通信研究機構のこと。情報通信分野を専門とする総務省所管の独立行政法人で、情報通信技術の研究開発の推進、情報通信事業の事業支援を行っている。

➢ **NIPP**

National Infrastructure Protection Planの略で、米国の重要インフラ防護に関する国家インフラ防護計画のこと。法律及び大統領令に基づき、米国国土安全保障省が作成している。NIPPに基づき、通信、電力など18の重要インフラセクター（分野）がそれぞれ個別の計画を作成している。

➢ **NISC（ニスク）（主要事項「5.1.1　日本の情報セキュリティ政策」を参照）**

National Information Security Centerの略で、内閣サイバーセキュリティセンターのこと。2015年1月、サイバーセキュリティ基本法に基づき、内閣官房情報セキュリティセンターから改組された。前身である内閣官房情報セキュリティセンターは、情報セキュリティ対策の中核を担う組織として2005年4月に設立された。情報セキュリティ政策に関する中長期計画の立案やサイバー攻撃に関する情報収集等を

行っている。

➢ **NIST（ニスト）**

National Institute of Standards and Technologyの略で、米国国立標準技術研究所のこと。米国商務省が管轄する機関で、技術指針や政府内における標準や運用基準の策定に務めている。

➢ **NSA**

National Security Agencyの略で、米国国家安全保障局のこと。国防総省傘下の情報機関で、高度な情報通信技術を使って諜報活動を行っている。

P

➢ **P2P（ピアトゥピア、ピーツーピー）**

Peer To Peer（ピアトゥピア、ピーツーピー）の略で、不特定多数のコンピュータを直接接続して情報をやり取りするタイプのシステム提供方式のこと。

➢ **PKI**

Public Key Infrastructureの略で、公開鍵基盤のこと。公開鍵暗号方式を核とした、認証、電子署名、暗号化等を含むセキュリティ確保のための包括的なシステム。

➢ **PLC**

Programmable Logic Controllerの略で、PC及び制御ソフトウェアを組み合わせてプロセスの制御・監視を実行する機器のこと。ビルの制御や組立プラントなどにおいて利用されている。

S

➢ **SIEM（シーム）**

Security Information and Event Managementの略で、集められたログ情報に基づいて、異常があった場合に管理者に通知したりその対策方法を知らせたりする仕組みのこと。

➢ **SLA**

Service Level Agreementの略で、サービスレベル合意書のこと。企業が顧客に提供するサービスの内容や品質のレベルを明確にし、企業と顧客との間であらかじめ合意しておくこと、あるいはそれを明文化した文書や契約のことであり、合意したレベルが達成できなかった場合のルールも含まれる。

➢ **SNS（主要事項「6.2.2　SNSの普及に伴う脅威」参照）**

Social Networking Serviceの略で、ソーシャルネットワーキングサービスのこと。コミュニティ型のウェブサイトで、FacebookやTwitter、LINEなどがある。

➢ **SOC（ソック）**

Security Operation Centerの略。ネットワーク監視の拠点としてリモートからセキュリティ機器を監視し、サイバー攻撃の検出とその対応策のアドバイスを行う機能を持ち、企業等の組織内に設置される。

➢ **SQLインジェクション**

Webアプリケーションの不備をついて、SQL（Structured Query Language）というデータベース用言語を用い、攻撃者がデータベースを外部から不正に操作する行為。サーバ管理者の意図しない命令が入力された場合、個人情報等が不正に取得される可能性がある。

➢ **SSO**

Single Sign-Onの略。「シングルサインオン」を参照。

➢ **Stuxnet（スタックスネット）**

2010年7月に確認された産業制御システムを標的としたマルウェア。イランでは、ウラン濃縮用遠心分離機のPLCが改ざんされ、8,400台もの遠心分離機が稼働不能になったとされる。

T

➢ **TCP/IP**

インターネット等で標準的に用いられる通信プロトコルのこと。TCPとIPの2つのプロトコルで構成され、TCPは接続相手を確認してからデータを送受信することで信頼性の高い通信を実現し、IPは相手を確認せずに通信することで、高速なデータ転送を実現する。

➢ **Telecom-ISAC Japan（テレコムアイザックジャパン）**

正式名称は、一般財団法人日本データ通信協会テレコム・アイザック推進会議。通信事業者の商用サービスの安全かつ安心な運用の確立を目的に、テレコム通信事業者を含む会員が関連情報を共有分析し、業界横断的な問題に対して対策をとる場を提供する団体。

➢ **Tor（トーア）**

The Onion Routerの略で、米国海軍調査研究所（Naval Research Laboratory: NRL）が開発した技術をベースとしたTCP/IPの通信経路を匿名化する技術のこと。

➢ **TPM**

Trusted Platform Moduleの略で、ハードウェアベースのセキュリティ基盤を提供するセキュリティモジュール（セキュリティチップ）のこと。チップメーカーやPCメーカーからなる標準化団体Trusted Computing Group（TCG）によって仕様が規定されている。

V

➢ **VPN**

Virtual Private Networkの略で、仮想プライベートネットワークのこと。インターネットその他の公衆回線を、暗号化技術などを用いて仮想的に組織内ネットワークのように利用できるサービスのこと。

W

➢ **WikiLeaks（ウィキリークス）**

各国の政治や企業活動などに関する機密情報を公開するためのウェブサイト。匿名性が維持された状態で運営されており、匿名通信ツールによって投稿者が身元を知られたり通信の監視を受けたりせずに投稿することができる。

ア

➢ **アイデンティティ管理（主要事項「1.3.2　認証・アイデンティティ管理」を参照）**

認証に使われる、IDやパスワード等の情報を適切に管理する技術のこと。第三者に情報が漏れた場合、なりすましや不正アクセス被害を受ける可能性が高まる。

➢ **アクセス制御（主要事項「1.3.3　アクセス制御」を参照）**

正当なユーザ等にはネットワークや情報及び情報システムにアクセスすることを認め、不当な主体のアクセスは拒否する制御のこと。情報資産の重要性に応じて適切に設定する必要がある。

➢ **アドウェア**

Advertising-Supported Softwareの略で、広告を表示するソフトウェア又はアプリケーションの総称。それ自体としては必ずしも不正とはいえないが、ユーザにとっては迷惑と判断される行為を執拗に行うことからグレーゾーンのプログラム（グレーウェア）に分類される。

➢ **アノニマス**

Anonymousを参照。

➢ **暗号（暗号化）（主要事項「1.3.1　暗号（暗号化）」を参照）**

一定の規則に基づいてデータを変換することでデータの機密性や完全性を守るための手法。コン

ピュータや通信、インターネットサービスの安全性を担保するための基盤となる技術。

➢　**暗号危殆化**

暗号の安全性レベルが低下した状態、又はその影響により暗号アルゴリズムが組み込まれているシステムなどの安全性が脅かされる状況。

➢　**暗号モジュール試験及び認証制度**

JCMVPを参照。

➢　**アンチウイルスソフト**

コンピュータをウイルスから防御するためのソフトウェアのこと。ウイルス対策ソフトとも呼ばれる。ウイルスに関する特徴が記されたパターンファイルに基づき、コンピュータに侵入したウイルスを検知、除去する。

➢　**違法コピー**

著作権を侵害する、あるいは使用許諾契約に反する形でソフトウェアをコピーすること。正規品を購入せず、インターネットオークションやファイル共有ソフトなどから海賊版を入手してインストールすることも違法コピーにあたる。不正コピーともいう。

➢　**インシデント**

サービスやシステムの障害、ヒューマンエラー、不正行為、偶発的な事故、意図的な攻撃等、事業活動又は情報セキュリティを損ねる可能性のある事象の総称。

➢　**インターネット上の違法・有害情報（主要事項「5.2.6　インターネット上の違法情報・有害情報」を参照）**

インターネット上の違法情報はインターネット上に掲載すること自体が違法となる情報（児童ポルノ画像、わいせつ画像、覚醒剤等規制薬物の販売に関する情報等）、有害情報は違法情報には該当しないが、犯罪や事件を誘発するなど公共の安全と秩序の観点から有害な情報のこと。

➢　**インターネットバンキング（主要事項「6.2.5　不正送金」を参照）**

インターネットを介して銀行の取引サービスを行うこと。近年、不正送金事件が多発し大きな被害を生んでおり、各金融機関はセキュリティ対策として、ワンタイムパスワードなどの導入を行っている。

➢　**インフォメーションハイディング（Information Hiding）（主要事項「1.3.5　インフォメーションハイディング」を参照）**

「情報を隠す」セキュリティ技術の総称。代表的な例として、秘匿通信を目的としたステガノグラフィと著作権管理、情報誘導、改ざん検出などを目的とした電子透かしがある。

➢　**ウィキリークス**

WikiLeaksを参照。

➢　**ウイルス（主要事項「1.2.2　マルウェア」を参照）**

標的となるファイルやプログラム、コンピュータ等に自分自身のコピーを複製（感染）するように設計されているマルウェア。ファイルを開く、プログラムを実行するなどのユーザの操作をきっかけとして、有害なコードが実行される。

➢　**ウイルス検知**

コンピュータ中に侵入している、あるいは侵入しようとしているウイルスを発見し、ユーザにその情報を知らせること、及びその機能。

➢　**営業秘密管理指針**

経済産業省が作成する指針で、企業が「不正競争防止法」（平成5年法律第47号）による保護を受けられるような、営業秘密の管理方法等を解説したもの。

➢　**炎上**

不祥事や不注意又は不適切なインターネット上の書込み等を契機として注目を集め、インターネット

のサイトやコメント欄などに大量に非難や中傷のコメントが書き込まれる状態。

➢ **オープンデータ政策（主要事項「5.1.3　オープンデータ政策」を参照）**

オープンデータ（機械で判読可能なデータ形式で、二次利用が可能な利用ルールで公開されるデータ）の利活用等の促進を目的とした国や地方自治体の政策。

カ

➢ **海賊版**

著作権や著作隣接権などを侵害している製品や商品のこと。アジア地域から来るものが多いが、知財保護、取締体制が異なるために個々の摘発は技術的、時間的に難しく、結果的に侵害行為は後を絶たない。

➢ **仮想プライベートネットワーク**

VPNを参照。

➢ **学校裏サイト**

特定の学校に関する掲示板サイト。その学校の公式ホームページなどとは異なり、関係者（大抵は在校生）が許可を得ずに開設している。学校や学校関係者に関する噂などが匿名で書き込まれ、いじめの温床になっているとされる。

➢ **可用性**

情報セキュリティの3つの理念のうちの一つ。許可された者が必要なときにいつでも情報にアクセスできるようにすることを意味する。

➢ **監視（主要事項「1.3.4　監視」を参照）**

ネットワークや各種ネットワークサービスについて異常を迅速に発見するために行う。監視カメラなどを使って物理的に人や物の出入りを監視する方法に加え、サーバやネットワーク機器などに対する「ハードウェア監視」、「サービス監視」、「ネットワーク監視」などがある。

➢ **完全性**

情報セキュリティの3つの理念のうちの一つ。保有する情報が正確であり、完全である状態を保持することを意味する。

➢ **機能安全**

付加的に導入された電子機器（コンピュータ等）を含んだ装置が、正しく働くことによって実現される安全性のこと。対比される言葉は「本質安全」で、製品やシステムの危険源そのものを取り除くか危害の大きさを低減させることによって安全を確保する方策のこと。

➢ **機密（性）情報**

許可された者だけがアクセスできる情報。企業内機密情報とは、企業を維持・存続させるために必要な経営情報、研究開発情報、人事情報などのことで、営業秘密と同義で用いられる場合が多い。

➢ **機密性**

情報セキュリティの3つの理念のうちの一つ。情報へのアクセス（閲覧など）が許可された者に限定されていることを意味する。

➢ **共通鍵暗号**

暗号化と復号化に同じ鍵（共通鍵）を用いる暗号技術。一般に公開鍵暗号方式に比べて処理が高速に行えるという長所がある。

➢ **金融ISAC**

高度化するサイバー攻撃に対抗するため、金融機関間でサイバーセキュリティに関する情報を共有するために設立された一般社団法人。

➢ **組込みシステム（主要事項「3.3　組込みシステム」を参照）**

産業機器や家電製品などの機器に組み込まれ、機器の制御を行う目的に専用化されたコンピュータシ

ステムのこと。組込みシステムのセキュリティに関する、ガイドライン作成や普及啓発はIPA等により実施されている。

➢　**クラウド（主要事項「2.3　クラウドのセキュリティ」を参照）**

データやソフトウェアをネットワーク経由で提供するサービスのこと。サービスの性質上、サーバ内のデータ消失や意図しない対象とデータが共有されるといったリスクがある。

➢　**クラウドセキュリティ（主要事項「2.3　クラウドのセキュリティ」を参照）**

クラウド特有のセキュリティのこと。クラウドセキュリティの向上のため、経済産業省が「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」を、総務省は「クラウドサービス提供における情報セキュリティ対策ガイドライン」を公表している。

➢　**クラウド情報セキュリティ管理基準**

経済産業省が2012年に公表した「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」を踏まえ、クラウド事業者が行うべき事項を整理したもの。

➢　**クラッカー（Cracker）**

コンピュータに不正に侵入し、システムやデータを破壊、改ざんする等の行為を行う者のこと。

➢　**グレートファイアウォール**

GFW（Great Firewall）、又は金盾などと呼ばれる、中国政府によるインターネット検閲システム。特定の海外サイトのアクセスや反政府的な書込みといった行為を監視している。

➢　**クレジットカード番号情報等の不正取得**

クレジットカード番号が登録されたサービスやシステムに対する不正アクセスや、スキミング（カメラや小型読み取り機で不正にカード情報を読み取ること）等によって不正にクレジットカード番号を取得すること。「割賦販売法」（昭和36年法律第159号）でクレジットカード番号の不正な提供や取得に対する刑事罰を規定している。

➢　**クロスサイトスクリプティング**

入力欄のあるウェブサイトで、入力した内容をそのままブラウザに送り返してしまうような仕組みを備えた場合の危険性が指摘された脆弱性のこと。ブラウザ上で悪意のスクリプト（プログラム）が実行されてしまう可能性がある。

➢　**刑事訴訟法**

昭和23年法律第131号。刑事訴訟に関する手続について定めたもの。2011年（平成23年）の改正で、電気通信回線で接続している記録媒体からの複写、記録命令付差押え、電磁的記録に係る記録媒体の差押えの執行方法、保全要請に関する規定、電磁的記録に係る記録媒体についての差押状の執行を受ける者等に対する協力要請等を新設。

➢　**景品表示法**

正式名称は「不当景品類及び不当表示防止法」（昭和37年法律第134号）。消費者が自主的かつ合理的に商品・サービスを選択できるよう、商品やサービスの品質、内容、価格等を偽って表示を行うことを規制するとともに、過大な景品類の提供を防ぐために景品類の最高額を制限する法律。

➢　**刑法**

明治40年法律第45号。電磁的公正証書原本不実記録罪、電磁的記録不正作出罪、電子計算機損壊等業務妨害罪、電子計算機使用詐欺罪、電磁的記録毀棄罪の処罰等を定めたもの。2011年（平成23年）の改正で、不正指令電磁的記録に関する罪や電子計算機損壊等業務妨害罪の未遂罪等を新設。

➢　**公開鍵暗号**

暗号化時には公開鍵、復号時には秘密鍵という異なる鍵を用いる暗号方式。秘密鍵無しでは復号が計算的に不可能（＝膨大な時間がかかる）という特性を持つ。認証、電子署名など、多様な用途に利用されている。

➢ **国際協調（主要事項「5.3.1　国際協調」を参照）**

政府の情報セキュリティ政策会議において、国際連携・共助に関する我が国の基本方針及びそれに基づく重点取組分野等を整理した「サイバーセキュリティ国際連携取組方針」が策定されている。また、人権、民主主義、法の支配等の分野で国際社会の基準策定を主導する欧州評議会が中心となってサイバー犯罪条約が作成され、当初、日本・米国・欧州の主要国30か国が署名した。

➢ **国際的相互承認**

協定に合意した国の間で相互に通用する認証のこと。例えばISO/IEC 15408は、欧米6か国7機関で構成されるCCプロジェクトによって開発された共通基準（Common Criteria: CC）に基づき国際的相互承認が行われている。

➢ **国際電気標準会議**

IECを参照。

➢ **国際標準化機講**

ISOを参照。

➢ **個人情報保護法（主要事項「5.2.2　個人情報保護」を参照）**

正式名称は「個人情報の保護に関する法律」（平成15年法律第57号）。個人の権利と履歴を保護するための法律で、同法では個人情報を所有する事業者に対する義務や対応を定めている。

➢ **国家安全保障会議**

日本の安全保障に関する重要事項を審議する機関として内閣に設置。「4大臣会合」（内閣総理大臣、内閣官房長官、外務大臣、防衛大臣）を中核として、外交及び安全保障に関する諸課題について、戦略的観点から日常的、機動的に議論を実施。いわゆる日本版NSC。

➢ **国家安全保障会議（米）**

英語ではNational Security Council（NSC）。米国で外交及び安全保障に関する政策や戦略の検討を行う大統領直属の諮問機関。

➢ **子どもとサイバー犯罪（主要事項「6.2.3　子どもとサイバー犯罪」を参照）**

スマートフォンやインターネット接続可能な携帯ゲーム機などの普及により、子どもたちがインターネットを利用できる環境が広がるとともに、子どもたちがサイバー犯罪の被害者や加害者になるケースが増えている。

サ

➢ **サービスレベル合意書**

SLAを参照。

➢ **最高情報責任者**

CIOを参照。

➢ **最高情報セキュリティ責任者**

CISOを参照。

➢ **サイバー演習（主要事項「4.5　サイバー攻撃に備えた実践的演習」を参照）**

情報システムのインシデント発生を想定したシナリオを設定し、必要に応じて対応又は判断・対応について議論することで、情報システムにおけるインシデント対応体制・手順や、情報システムやサービスの稼働継続に関わる手順・規程に関して、実行可能性の確認や課題抽出を行うもの。対応の習熟度を高めるために行われる訓練とは異なる。

➢ **サイバー空間における安全保障（主要事項「5.3.2　サイバー空間における安全保障」を参照）**

安全保障上の主要課題となっているサイバー攻撃に関して、サイバー空間の防護及びサイバー攻撃への対応能力の強化等により、国の安全保障を万全とすること。日本では、2014年3月に自衛隊の専門部

隊として「サイバー防衛隊」が発足した。外務省は日米同盟の強化の観点から日米サイバー対話を開催している。

➢　**サイバー（防衛）軍（米）**

英語名称はUnited States Cyber Command（USCYBERCOM）。米国戦略軍に設置されたサイバー攻撃、サイバー戦を担当する統合部隊。

➢　**サイバー攻撃（主要事項「1.2.3　不正アクセス・サイバー攻撃」を参照）**

マルウェア感染やコンピュータ及びネットワークに対する侵入・改ざん、サービス運用妨害などの攻撃。以前は愉快犯によるものが多かったが、金銭目的や政治的なアピールを目的としたものに変化しており、国家によるサイバー攻撃も増加している。

➢　**サイバーストーカー**

何度もメールを送りつけるなど、ネットワークを利用して執拗につきまとう者をいう。掲示板サイトを使って誹謗中傷をしたり、何らかの手段で住所などを割り出したりして、物理的なストーカー行為に発展することもある。

➢　**サイバーセキュリティ基本法**

平成26年法律第104号。日本のサイバーセキュリティ施策を推進するために、サイバーセキュリティ戦略・基本的施策を規定し、内閣にサイバーセキュリティ戦略本部を設置するもの。NISCについては法制化することを明記している。

➢　**サイバーセキュリティ戦略本部**

2015年1月、サイバーセキュリティ基本法の施行に伴い、内閣に設置された日本政府における情報セキュリティ政策の最高決定機関。情報セキュリティ政策会議の決定事項及び検討事項等は同本部に引き継がれた。

➢　**サイバーセキュリティ法案（米）**

2011年から2012年にかけて、サイバー攻撃に関する情報を政府や企業間で共有することを可能とする法案が米国連邦議会に複数提出され、下院において可決されたものの、いずれも上院で否決され、成立には至らなかった。

➢　**サイバー戦争**

コンピュータネットワーク上で行われる国家間・組織間の戦争。敵対する国家や組織にサイバー攻撃を仕掛け、サイトの改ざん、ネットワークサービスの妨害、機密情報の窃取等を行う。

➢　**サイバーテロ**

重要インフラの基幹システムに対して行われる電子的攻撃、又は電子的攻撃による可能性が高いもので、社会基盤の混乱を目的とする実力行使。

➢　**サイバー犯罪（主要事項「6.2.1　サイバー犯罪の発生状況」を参照）**

コンピュータやインターネット等のネットワークを利用して行われる犯罪の総称。国内ではコンピュータ・電磁的記録対象犯罪及び不正指令電磁的記録に関する罪、ネットワーク利用犯罪、不正アクセス禁止法違反の3つの類型に分類される。

➢　**サイバー犯罪条約**

正式名称は「サイバー犯罪に関する条約」（平成24年条約第7号）。サイバー犯罪に対する世界初の国際条約で、2001年11月に日米欧の主要国を含む30か国が署名した。日本では、2012年11月から効力が発生。

➢　**サイバー防衛隊**

24時間体制で防衛省・自衛隊のネットワークの監視及びサイバー攻撃発生時の対処を実施するとともに、サイバー攻撃に関する脅威情報の収集、分析、調査研究等を行う組織。

➢ **サイバーポリス（主要事項「5.2.4　サイバー犯罪とその対策」を参照）**

警察庁が平成10年に「ハイテク犯罪対策重点推進プログラム」の中で提示したハイテク犯罪対策体制の総称のこと。各都道府県警察がハイテク犯罪捜査体制を強化するためにプロジェクトを立ち上げ、警察庁では情報技術の解析や警察官の知識や技能向上の教育を行う。

➢ **サプライチェーンセキュリティ**

サプライチェーン内におけるセキュリティを確保すること。なお、サプライチェーンとは、製品やサービスを生産し、移動して、サプライヤから顧客に供給するための組織、人、活動、情報及び資源のつながりを意味する。

➢ **産業用ネットワーク**

産業プラントや工場の中で動く製造装置や加工機、組立装置などをつなぐネットワークのこと。一般的に利用されているLANの規格であるイーサネット（Ethernet）をベースにした通信技術を活用する動きが活発化してきている。

➢ **事業継続計画**

BCPを参照。

➢ **児童ポルノ**

写真や電磁的記録媒体など、18歳未満の者に関する（主に性的な）描写をしたもののこと。「児童買春、児童ポルノに係る行為等の規制及び処罰並びに児童の保護等に関する法律」（いわゆる「児童ポルノ禁止法」。平成11年法律第52号）に定められている。

➢ **重要インフラ攻撃（主要事項「1.2.5　重要インフラに対する攻撃」を参照）**

電力、水道、通信、金融、交通などの社会の基盤を提供する重要インフラへのサイバー攻撃は増加している。国内ではNISCや情報セキュリティ関係省庁、CSSC等が重要インフラの防護のために取組を行っている。

➢ **重要インフラの情報セキュリティ対策に係る行動計画（主要事項「1.2.5　重要インフラに対する攻撃」を参照）**

電力、水道、通信、金融、交通などの代替が著しく困難な重要インフラのセキュリティ対策を強化するため、2005年12月に情報セキュリティ政策会議によって決定された計画。2014年5月19日には、「重要インフラの情報セキュリティ対策に係る第3次行動計画」が決定されている。

➢ **証拠保全**

裁判などで用いるための証拠を確保、保存すること。民事訴訟では重要書類を確保するためには証拠保全（「民事訴訟法」（平成8年法律第109号）第234条以下）という手続きを行い、証拠を手元に確保することが極めて重要となる。

➢ **商標法**

昭和34年法律第127号。商標を保護することにより、商標を使用する者の業務上の信用を維持するとともに、消費者の利益を保護することを目的とする。商標登録、審査、商標権等について規定している。

➢ **情報処理技術者試験**

「情報処理の促進に関する法律」（昭和45年法律第90号）第7条に基づき実施される、情報処理に関して必要な知識及び技能を問う国家試験。情報技術の背景として知るべき原理や基礎となる知識・技能について、幅広く総合的に評価する。試験事務は経済産業省から委託を受けたIPAが実施する。

➢ **情報処理推進機構**

IPAを参照。

➢ **情報セキュリティ（主要事項「1.1　情報セキュリティの基礎」を参照）**

情報セキュリティとは、JIS Q 27000:2014（ISO/IEC 27000:2014）によって情報の機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）を維持することと定義されている。この3 つの理念をまとめて、

頭文字をとって情報セキュリティにおける「CIA」と略される。

➢　**情報セキュリティ格付**

企業や組織が取り扱う技術情報、営業機密、個人情報について、そのセキュリティのレベルを示す指標のこと。マネジメントの成熟度、情報漏えい防止策の強度、コンプライアンスへの取組などを審査し、17段階の符号で表す。日本では株式会社アイ・エス・レーティングが格付を実施している。

➢　**情報セキュリティガバナンス（主要事項「4.1　企業の情報セキュリティに対する取組」を参照）**

社会的責任にも配慮したコーポレート・ガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること。

➢　**情報セキュリティ監査**

情報セキュリティにかかわるリスクのマネジメントが効果的に実施されるための監査。リスク評価に基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査人が独立かつ専門的な立場から検証又は評価して、保証の付与や助言を行う。

➢　**情報セキュリティ管理基準**

組織体が効果的な情報セキュリティマネジメント体制を構築し、適切な管理策を整備・運用するための実践的な規範として、経済産業省が定めた基準（平成20年経済産業省告示第246号）。情報セキュリティマネジメントにおける管理策のための国際標準規格であるISO/IEC 27001:2005（JIS Q 27001:2006）を基にしている。

➢　**情報セキュリティ緊急支援チーム**

CYMATを参照。

➢　**情報セキュリティ研究開発戦略（主要事項「7.3　セキュリティ研究開発体制」を参照）**

情報セキュリティ政策会議は2014年7月に「情報セキュリティ研究開発戦略（改定版）」を決定。サイバー攻撃の検知防御能力の向上や、社会システム等を防護するためのセキュリティ技術の強化等の研究開発推進方針を示している。

➢　**情報セキュリティ政策会議（主要事項「5.1.1　日本の情報セキュリティ政策」を参照）**

内閣の高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）の下に日本の情報セキュリティに関する問題の根幹に関する事項を決定する母体として設置された。情報セキュリティ政策に関する基本戦略の策定、情報セキュリティ政策の事前・事後評価、情報セキュリティ対策に関わる政府統一的な安全基準の策定を担っていた。サイバーセキュリティ基本法等に基づき、情報セキュリティ政策会議の決定事項及び検討事項等はサイバーセキュリティ戦略本部に引き継がれた。

➢　**情報セキュリティ対策推進会議**

情報セキュリティ政策会議に設置され、関係行政機関の最高情報セキュリティ責任者等相互の緊密な連携の下、政府機関における情報セキュリティ対策の推進を図る。

➢　**情報セキュリティ認証（主要事項「2.1　情報セキュリティに関する国際基準・認証」を参照）**

情報セキュリティの観点から、情報技術に関連した製品及びシステムが適切に設計され、その設計が正しく実装されているかを第三者が評価及び認証する仕組み。

➢　**情報セキュリティマネジメントシステム適合性評価制度**

ISMSを参照。

➢　**情報窃取**

個人情報やクレジットカード情報、組織内の機密情報などを密かに盗み取ること。脆弱性を狙ったサイバー攻撃による情報窃取が近年増加している。

➢　**情報通信研究機構**

NICTを参照。

➢ **情報保証**

機密性、完全性、可用性などを確保することによって、情報及び情報システムを保護及び防御する手段のこと。情報保証はシステムの信頼性と戦略的リスク管理を目的とする。

➢ **情報倫理**

情報通信社会において必要とされる道徳やモラルのこと。情報モラルや情報マナーとも呼ばれる。

➢ **情報漏えい**

障害、事故、人為的ミス、不正行為、マルウェア（不正プログラムやウイルス等）により、PCやサーバで管理していた情報がユーザの意図に反して外部に流出すること。

➢ **シングルサインオン（Single Sign-On: SSO）**

利用するシステムごとにパスワード入力等のユーザ認証を必要とせず，一度だけの認証で複数システムを利用できる仕組み。

➢ **侵入検知システム**

IDSを参照。

➢ **スクリプトキディ（Script Kiddy）**

インターネット等で公開されている既存のクラッキングツールを使用して不正アクセスを試みる、初心者クラッカーに対する呼称。

➢ **スタックスネット**

Stuxnetを参照。

➢ **ステガノグラフィ（Steganography）**

情報を別のデータ（画像・動画・音楽など）の中に埋め込み、第三者に情報の存在を気づかれずに当該情報を通信・伝達する技術。

➢ **ステルスマーケティング**

ある特定の商品の宣伝であることを、消費者に隠して行う宣伝や広報活動のこと。有名人に依頼してブログで商品を宣伝してもらう手法など、インターネットを利用したステルスマーケティングが近年増加している。

➢ **スパイウェア**

コンピュータ利用者の個人情報を、密かに収集して外部へ送信するプログラムのこと。一般のウイルス対策ソフトでは検出されない場合も多く、その発見と駆除には専用のスパイウェア対策ソフトが用いられる。

➢ **スパムメール**

不特定多数のユーザに対し、承認を得ずに送られる迷惑メール。送信元を隠すため、セキュリティの弱いメールサーバが不正に利用されることがある。

➢ **スマートグリッド**

電力インフラと通信インフラを融合させた次世代のエネルギー供給システムのこと。通信技術を利用した制御により、電力の需要と供給のバランスを取ることで、エネルギーの有効利用と、送電ロスの低減や電力の安定供給が期待されている。

➢ **スマートフォン依存（主要事項「6.2.4　ネット依存・スマホ依存」を参照）**

インターネットの利用時間をコントロールできないネット依存のうち、特にスマートフォンによるインターネット利用やコミュニケーションに深く依存してしまうこと。

➢ **スマートフォンのセキュリティ（主要事項「2.2　スマートフォンのセキュリティ」を参照）**

スマートフォンやタブレット端末などの携帯端末の利用が広まる中「不正アプリ」によるプライバシー情報や機密情報の漏えいが問題視されているほか、架空請求や不正送金などの被害も発生している。この状況を踏まえ内閣官房や総務省では、ガイドラインを公開している。

➢　**スマートメーター**

通信機能を持つことで電力やガスなどの使用量を細かく把握し、使用量を制御可能にしたメーター。

➢　**制御システム（主要事項「3.1　制御システム」を参照）**

センサやアクチュエータなどのフィールド機器、コントローラ、監視・制御用に用いるサーバやクライアントPC などをネットワークで接続したシステム。製造業の工場・プラントのほか、電力、ガス、水道、通信、石油化学プラントなどの重要インフラで監視・制御に使われている。

➢　**制御システムセキュリティ国際基準・認証（主要事項「3.2　制御システムセキュリティに関する国際基準・認証」を参照）**

制御システムやマネジメントシステムが、制御システムのセキュリティ基準に適合しているかを認証する仕組み。

➢　**制御システムセキュリティセンター**

CSSCを参照。

➢　**脆弱性（主要事項「1.2.1　脆弱性とその取扱い」を参照）**

ソフトウェア等において機能や性能を損なう原因となり得る欠陥や設定の不備。一般にサイバー攻撃では、攻撃対象のソフトウェアやハードウェアの脆弱性を悪用することが多い。

➢　**青少年インターネット環境整備法**

正式名称は「青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律」（平成20年法律第79号）。青少年にとって有害な情報が数多く流通しているインターネットの状況に対し、対策を実施するためにできた法律。

➢　**政府統一基準（主要事項「5.1.2　政府機関の情報セキュリティ対策」を参照）**

正式名称は「政府機関の情報セキュリティ対策のための統一基準」。日本の政府機関全体の情報セキュリティ水準の向上を目的に、各府省庁の情報セキュリティ対策の整合化・共通化を促進するために策定される統一基準。

➢　**セキュリティ・キャンプ**

日本発で世界に通用する若年層の情報セキュリティ人材を発掘・育成するため、産業界、教育界から結集した講師によって実施されるキャンプ・勉強会のこと。年1回の全国大会と、年数回実施される地方大会がある。

➢　**セキュリティ教育**

インターネットや情報システムを利用するあらゆるユーザに対して、対象と目的に沿った情報セキュリティに関する教育を行うこと。

➢　**セキュリティ人材（主要事項「7.1　セキュリティ人材育成」を参照）**

情報セキュリティの技術的な研究を行う研究者や、情報セキュリティ関連製品・サービスを開発する企業の人材、情報システムを利用する企業や組織における情報セキュリティの担当者等、組織において情報セキュリティ対策や推進にかかわる人材の総称。

➢　**セキュリティ対策コスト**

セキュリティ製品やセキュリティサービスを導入するための費用。一般に、情報資産の価値と導入する製品・サービスの費用対効果、運用負荷とのバランスを考えて決定する。

➢　**セキュリティ投資**

ITリスクを回避、あるいはそれに対応するために予算を投じること。セキュリティに投資したからといって業務効率や顧客サービスが向上しない場合もあり、投資判断は一般的なIT投資の手法とは異なる考え方が必要となる。

➢　**セキュリティ・バイ・デザイン**

情報システムの企画・デザイン段階から情報セキュリティに配慮した設計を行うこと。

➢ **セキュリティプロトコル**

暗号アルゴリズムを応用して認証や秘匿化、改ざん防止等のセキュリティ機能を提供する通信規約。用途（インターネット、電子メール等）や暗号化方式により、SSL、IPSEC、PGP等様々なセキュリティプロトコルが存在する。

➢ **セキュリティホール**

OSやソフトウェアのバグや設定ミス等、情報セキュリティ上の欠陥となる不具合のこと。ソフトウェアのバグの場合、発見後配布されるセキュリティパッチを直ちに適用し、セキュリティホールを塞ぐことが重要となる。

➢ **セキュリティポリシー**

情報の機密性や完全性、可用性を維持していくために規定される、組織の方針や行動指針をまとめたもの。

➢ **セキュリティ要求仕様**

情報システムの構築又はソフトウェアの構築を外部委託により行う場合、調達者が求めるセキュリティ要件を正確に伝えるために作成するもの。

➢ **セプターカウンシル（CEPTOAR Council）**

NISCの重要インフラ対策グループにおいて、分野を超えた情報共有の充実に向けて各セプターにより構成される協議会。セプター（CEPTOAR）とはCapability for Engineering of Protection, Technical Operation, Analysis and Responseの略で、重要インフラ分野ごとに整備された情報共有・分析機能をもつグループのこと。

➢ **ゼロデイ（攻撃）**

ソフトウェア製作会社などがコンピュータの基本ソフト（Operating System: OS）やアプリケーションの脆弱性に対応するパッチを提供する前の脆弱性（ゼロデイ脆弱性）を悪用して行う攻撃の総称。

➢ **ソーシャルエンジニアリング**

サイバーセキュリティにおいては、人間の心理的な隙や行動のミスに付け込み、不正に情報を入手する手段の総称。例として管理者や社員、取引先等になりすましてパスワードを聞き出す、ごみ箱からパスワードが書かれたメモをあさるなどの行為がある。

タ

➢ **耐タンパー（Tamper Resistant）**

暗号化鍵・復号鍵をはじめとする秘密情報や秘密情報の処理メカニズムを外部から不当に観測・改変することや秘密情報を処理するメカニズムを不当に改変することが極めて困難であること。

➢ **多層防御（Defense in Depth）**

何枚もの防衛壁を設置するように複数のセキュリティ保護対策を組み合わせて実施すること。

➢ **中間者攻撃（Man-in-the-Middle攻撃）**

通信を行っている当事者間に悪意を持った第三者が割り込み、不正を行う攻撃のこと。

➢ **著作権法**

昭和45年法律第48号。著作物などに関する著作者等の権利を保護するための法律。2012年に改正され、違法ダウンロード刑事罰化に係る規定が整備された。

➢ **出会い系サイト**

見知らぬ人と出会うことを目的としたウェブサイトのこと。身元や素性を偽って登録することが可能なことから、モラルの低下も懸念され、特に若年層が巻き込まれる犯罪の温床になっているとの指摘もある。

➢　**出会い系サイト規制法**

正式名称は「インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律」（平成15年法律第83号）。出会い系サイトの利用に起因する児童買春その他の犯罪から児童を保護し、児童の健全な育成に資することを目的としている。

➢　**デジタルコンテンツの著作権（主要事項「5.2.3　デジタルコンテンツと著作権保護」を参照）**

ウェブサイト上のコンテンツやデジタルデータは著作権保護の対象であり、著作権者の権利を尊重した利用が求められる。近年コンテンツのデジタル化が進み、デジタルコンテンツを提供する新しいサービスが次々と生まれる中で、デジタルコンテンツの著作権保護の在り方が議論されている。

➢　**デジタルネイティブ**

物心がつく頃にはインターネットやパソコンが普及していた環境で育った世代のこと。概ね1990年代半ば以降に生まれた世代を指す。

➢　**デジタルフォレンジック（Digital Forensics）**

コンピュータセキュリティインシデントの原因究明や証拠発見などを行うために、機器や電子データを分析すること及びその技術的手法のこと。

➢　**電子商取引（主要事項「6.2.6　電子商取引にかかわるトラブル」を参照）**

インターネットや専用ネットワーク等、電子的手段を介して行われる商取引のこと。電子商取引の市場規模が拡大する一方で、様々な消費者問題が発生している。

➢　**電子証明書**

ユーザが利用するサーバや公開鍵が本物であることを保証する電子的な証明書のこと。認証局と呼ばれる第三者機関によって発行される。

➢　**電子署名**

暗号技術の応用の一つとして電子的な文書やデータの真正性を保証するためのもの。公開鍵暗号が用いられる。

➢　**電子透かし**

画像や動画、音楽などのマルチメディアデータの中に、通常の視聴では判別できないような形で著作権情報などを埋め込む技術の総称。

➢　**電子政府推奨暗号リスト**

CRYPTRECにより安全性及び実装性能が確認された暗号技術のリスト。政府機関が暗号化又は電子署名を導入する場合には、やむを得ない場合を除き、電子政府推奨暗号リストに記載された暗号を採用することになっている。

➢　**電子マネーのリスク（主要事項「6.2.7　電子マネーのリスク」を参照）**

近年普及する様々な電子マネーによる決済にかかわるリスク。電子マネーを発行する運営会社が破綻すると現金から交換した電子マネーの価値がなくなったり、アカウントの乗っ取りにより不正に利用されるなどのリスクもある。

➢　**特定商取引法**

正式名称は「特定商取引に関する法律」（昭和51年法律第57号）。通信販売や電話勧誘販売等の消費者トラブルが生じやすい取引類型を対象に、事業者が守るべきルールや、クーリング・オフ等の消費者を守るルールを定めたもの。

➢　**特定電子メール法**

正式名称は「特定電子メールの送信の適正化等に関する法律」（平成14年法律第26号）。利用者の同意を得ずに広告、宣伝又は勧誘等を目的とした電子メールを送信する際の規定を定めた法律。

➢　**特定秘密保護法**

正式名称は「特定秘密の保護に関する法律」（平成25年法律第108号）。我が国の安全保障に関する情

報のうち特に秘匿することが必要であるものの保護に関し、必要な事項を定めたもの。特定秘密の漏えいを防止し、国と国民の安全を確保することを目的とする。

➢ **トラステッドコンピューティング（主要事項「1.3.6　トラステッドコンピューティング」を参照）**

CPUと独立したハードウェアベースのセキュリティ基盤を構築することによりシステムの高信頼性を担保する仕組みであり、この仕組みを実現するセキュリティチップが、PCの多くに搭載されている。

➢ **トロイの木馬**

ウイルスの一種。自分自身をシステムに必要なファイルなどに見せかけて動作する。システム情報や個人情報を詐取したりバックドアを作ったりするが、自己増殖はしない。

ナ

➢ **内閣官房情報セキュリティセンター**

NISCを参照。

➢ **内閣サイバーセキュリティセンター**

NISCを参照。

➢ **内部統制**

コンプライアンス（法令遵守）の確保、財務報告の信頼性の確保及び業務の効率化を目的として、企業が業務を適正かつ効果的に遂行するため、社内に構築・運用される体制及びプロセスのこと。

➢ **内部不正（主要事項「4.6　内部不正対策」を参照）**

情報セキュリティ対策においては、外部からのサイバー攻撃だけでなく、甚大な被害を生む可能性が高い内部不正も想定する必要がある。特にシステムを熟知している者による犯行の場合は、被害規模が甚大になる危険性が極めて高い。

➢ **なりすまし**

ネットワーク上で他人のふりをすること。他人のパスワードやCookie（Webブラウザに保存された利用者識別情報）を使う、電子メールの発信アドレスを詐称する、偽のウェブサイトを作るなどにより行われ、なりすまされた人が被害を受ける可能性がある。

➢ **日・ASEAN情報セキュリティ政策会議**

情報セキュリティ分野において、日本とASEAN諸国との国際的な連携・取組を強化することを目的とした会議。安心・安全なビジネス環境や情報通信ネットワークの構築、サイバーセキュリティ能力の強化等について取り組んでいる。

➢ **日米サイバー対話**

日米間において、サイバーに関する脅威情報の交換、国際的なサイバー政策についての連携、サイバー戦略の比較、重要インフラに対する共通の脅威に対抗するための取組や計画における協力等について議論している。

➢ **日本版NCFTA**

日本版National Cyber-Forensics & Training Allianceの略で、一般財団法人日本サイバー犯罪対策センター（Japan Cybercrime Control Center: JC3）のこと。産学官が保有する持つサイバー空間の脅威への対処経験等を蓄積・共有するとともに、警察による捜査権限のより効果的な行使脅威への対応を可能とする新たな連携の枠組みとして2014年11月に運用を開始した。

➢ **日本版SOX法**

「J-SOX法」を参照。

➢ **認証（主要事項「1.3.2　認証・アイデンティティ管理」を参照）**

通信相手に認証主体が本物であることを証明する手法で、証明したい種類の違いにより、ユーザ認証、クライアント認証、メッセージ認証などがある。現在は、パスワード認証方式が一般的である。

➢　**ネットいじめ**

携帯電話やパソコンを用いて、掲示板サイト、メール、SNSなどを通じて特定の人間の悪口や誹謗中傷を行うこと。対面のコミュニケーションと比較して、意思疎通が難しくエスカレートしやすい傾向がある。

➢　**ネット依存（主要事項「6.2.4　ネット依存・スマホ依存」を参照）**

インターネットの利用時間をコントロールできずに、これがないといらだちや不安感等を覚え生活への支障をきたすこと。

➢　**ネット検閲（主要事項「5.2.5　外国におけるネット検閲」を参照）**

インターネット上の情報に対して政府機関等の公権力が強制的に表現内容を調査し取り締まることを指す。海外のウェブサイトへのアクセスの制限や特定のキーワードに対するブロッキング、反政府的なサイトの摘発などインターネット上の情報に対する検閲が行われているとされる。

➢　**ネット詐欺**

電子メールやウェブサイトなどを利用した詐欺行為のこと。何らかの方法でウェブサイトに誘い込み、ウェブサイトを訪問した人に対して、脅迫めいた手口で料金の振り込みなどを迫る。

➢　**ネット選挙（主要事項「5.1.4　インターネットを利用した選挙」を参照）**

インターネット等を利用した選挙運動のこと。日本では2013年5月に施行された「公職選挙法の一部を改正する法律」（平成25年法律第10号）により、ウェブサイトやSNS、電子メール等を利用した選挙運動が解禁された。

➢　**ネット盗聴**

ネットワーク上に流れる通信中のデータやネットワークにつながれたコンピュータのデータを不正な手段を用いて盗み取ること。

➢　**ネットワーク検疫**

コンピュータを組織のLANに接続する前に、LANとは隔離されて存在する検査専用のネットワークに接続し、マルウェア感染の有無やセキュリティ対策の状況を確認するもの。

➢　**ネットワークフォレンジック（Network Forensics）**

ネットワーク内を流れる全ての通信データを取得し、過去に発生した事象に対する証拠の保全や不正アクセスの追跡を行うことができる仕組み、及びその技術的手法のこと。

➢　**ネットワークログ**

ネットワーク機器等において、ネットワーク上を流れるデータや他のネットワーク機器との間で交わされるメッセージの内容などを記録したもの。

ハ

➢　**ハートブリード（Heartbleed）**

2014年4月に発覚した、オープンソースの 暗号通信プログラムである「OpenSSL」の特定のバージョンにおける深刻な脆弱性。悪用されると、ウェブサーバのメモリ内データが読み取られ、結果として個人情報が流出するおそれがある。

➢　**バイオメトリクス（Biometrics）**

人間の身体的な特徴や特性を利用して個人を認証する方式。暗証番号やパスワードといった従来の認証方式と比較して、紛失、盗難、偽造のリスクが少ないという特長がある。

➢　**パスワードリスト攻撃**

不正アクセス攻撃の一種で、攻撃者がサイト等から不正に入手したID とパスワードの組合せを使って、他のサイトへのログインを試みる攻撃のこと。

➢　**ハッカー（Hacker）**

コンピュータやネットワークに非常に詳しい人のこと。それらの知識を悪用して不正アクセスや破壊

行為を行う者を表すクラッカーと同じ意味で使用されることもある。

➢ **ハッキング**

高度なコンピュータ技術を利用して、システムを解析したり、プログラムを修正したりする行為のこと。 本来は悪い意味を持つ言葉ではなかったが、現在は不正にコンピュータを利用する行為全般のことをハッキングと呼ぶことが増えている。

➢ **バックアップ・リカバリ**

重要なデータを損失から守ること、及び過去のデータを保存すること。公的機関や企業が取り扱うデータには、法律などによって一定期間保持することが決められているデータもある。

➢ **バックドア**

攻撃者がサーバ等への侵入後、再侵入のために設置する裏口。侵入用アカウントの作成、既存サービスのプログラムの書換え等がバックドアの設置にあたる。

➢ **ハッシュ関数（Hash Function）**

入力されたデータに対応する固定長の小さなデータ（ダイジェスト）を出力する関数。同一のダイジェストとなる、異なる入力データを作成するのは非常に困難であるという特徴を有する。メッセージの正確性を保つ目的で広く利用されている。

➢ **パッチ**

ソフトウェアの不具合が見つかった場合に配布される、不具合部分を修正するプログラムのこと。ソフトウェアを全て入れ替えることなしに問題のある箇所のみを修正することができる。メーカーのウェブサイトなどで提供される。

➢ **バッファオーバーフロー**

バッファ（入力データを一時的に保存するメモリ領域）の長さを越えるデータを送りこむことによって、以降の領域のデータを破壊し動作不能にしたり、外部から送り込んだプログラムを実行させたりする攻撃。

➢ **ビッグデータ（主要事項「2.4　ビッグデータ」を参照）**

大容量のデジタルデータのこと。ビッグデータの特徴としては、多量性、多種性、リアルタイム性がある。ビジネス利用が進む反面、個人に関するデータ（パーソナルデータ）を含むデータの取扱に留意する必要がある。

➢ **秘密保護（主要事項「5.2.1　秘密保護」を参照）**

秘密として管理されている情報を保護すること。我が国における主な秘密保護関連法としては、特定秘密保護法、不正競争防止法などがある。

➢ **標的型攻撃（主要事項「1.2.4　標的型攻撃」を参照）**

特定の企業や組織を狙ったサイバー攻撃。代表的な手口としては、受信者が関心を持つような件名や内容で電子メールを送りつけることによって、受信者が添付ファイルを開き、メール本文中に記載されたURL にアクセスしたりすることで、マルウェアに感染させる。

➢ **ファイアウォール**

セキュリティを高める目的で、ネットワークの内部と外部の境界に設置する装置。通信を監視し、許可されない通信を遮断する。パケットフィルタリングとアプリケーション・ゲートウェイの2種類の方式がある。

➢ **ファイル交換（共有）ソフト**

複数の利用者によるネットワークでのファイルのやり取りを可能にするソフトウェア。ファイルの交換は、P2P（ピアトゥピア、ピーツーピー）で実行される。違法なデータがやり取りされ著作権を侵害することもあり、社会問題になっている。

➢　**ファジング（Fuzzing）**

検査対象のソフトウェア製品に「ファズ（Fuzz）」と呼ばれる問題を引き起こしそうなデータを大量に送り込み、その応答や挙動を監視することで脆弱性を検出する検査手法。

➢　**フィッシング**

実在するクレジットカード会社や金融機関などを装った内容のメールを無作為に発信して、メールの受信者に偽のウェブサイトにアクセスするように仕向け、個人情報を騙し取る行為のこと。

➢　**フィルタリング**

ウェブサイト上の違法・有害情報へのアクセスを制御するために、受信者側でこれらの情報を受信するかどうかを選択すること。

➢　**フェアユース（Fair Use）**

著作権のある著作物に関して、その保護期間中であっても公正な使用であれば著作権の侵害に該当しないとする規定。米国では著作権法第107条において規定されている。日本でも、「日本版フェアユース」の導入が検討されている。

➢　**不正アクセス（主要事項「1.2.3　不正アクセス・サイバー攻撃」を参照）**

正規のアクセス権を持たない者が、ソフトウェアなどの脆弱性などを利用して不正にシステムやネットワークへのアクセス権を取得し、利用すること。

➢　**不正アクセス禁止法**

正式名称は「不正アクセス行為の禁止等に関する法律」（平成11年法律第128号）。不正アクセス行為や、不正アクセス行為につながる識別符号の不正取得・保管行為、不正アクセス行為を助長する行為等を禁止する法律。

➢　**不正アプリ（スマートフォン）**

携帯電話のシリアル番号やカード情報、電話番号、アカウント情報などをユーザの意図に反して収集するアプリケーションのこと。スマートフォン向けの不正アプリはモバイルマルウェアとも呼ばれる。

➢　**不正競争防止法**

平成5年法律第47号。業者間の公正な競争の促進及びこれに関する国際約束の実施を通して、国民経済の健全な発展を目的とする法律。商品等表示の混同や営業秘密の侵害等に関する民事的・刑事的措置について明記。

➢　**（ネット）不正送金**

インターネットバンキングのIDやパスワードを盗むなどして、預貯金が別口座に不正に送金されること。被害件数、一件当たりの金額も大幅に増えてきている。

➢　**プライバシー（主要事項「6.1.1　パーソナルデータ」を参照）**

法令上で定義されていないが、個人の私生活等、一般に公開されたくない情報のことを指す場合が多い。厳密には個人情報とは異なる概念である。

➢　**プライバシーマーク**

個人情報保護法よりさらに厳格な要件を定めた個人情報保護に関するガイドラインであるJIS Q 15001に適合した個人情報管理体制をとっている事業者を認定する制度のこと。

➢　**ブラックハット（Black Hat）**

情報セキュリティの専門家であるジェフ・モス（Jeff Moss）を創立者とするコンピュータセキュリティの国際会議。攻撃者の視点から見た最新の攻撃方法や脆弱性、ハッキングツールやセキュリティツール等について発表が行われる。

➢　**プロトコル（Protocol）**

機器の間で正確に信号やデータ、情報を相互に伝達するために、事前に決められた手順や規約の集合のこと。通信規約や通信手順ともいう。

➢ **プロバイダ責任制限法**

正式名称は「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」（平成13年法律第137号）。特定電気通信による情報の流通によって権利の侵害があった場合に、プロバイダ等の損害賠償責任の制限及び発信者情報の開示を請求する権利を定めたもの。

➢ **米国国立標準技術研究所**

NISTを参照。

➢ **ポートスキャン**

外部ネットワークから対象サーバに信号を送り、サーバへのアクセスの可否、サーバで用いられているプログラムの種類や脆弱性などについて調査すること。攻撃者等が、外部からの侵入や攻撃の可否を調べる目的で、不正アクセスやサイバー攻撃に先立って行われることが多い。

➢ **ボットネット（Botnet）**

攻撃者の命令に基づき動作するプログラム（ボット）に感染したコンピュータ及び攻撃者の命令を送信する指令サーバ（ボット指令サーバ）からなるネットワークをいう。攻撃者の命令により大量のスパムメールの送信やDoS（Denial of Service）攻撃などを行う。

➢ **ホワイトハッカー**

ネットワークやコンピュータに関する高度な知識や技術を持つ者を意味する「ハッカー」のうち、特にその技術を善良な目的に活かす者のこと。

➢ **ホワイトリスト**

あらかじめ登録された情報に基づき、通信や実行などの動作を許可する方式又は許可する対象を登録したリストのこと。一方、危険な対象を登録し、これを排除する方式をブラックリストと呼ぶ。通信のフィルタリングやアプリケーションの実行制御に利用される。

マ

➢ **マイナンバー制度**

「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」（いわゆる「番号法」。平成25年法律第27号）に基づくもの。住民票を有する全ての国民に対して番号を付し、社会保障、税、災害対策の分野で効率的に情報を管理する制度。行政の効率化、国民の利便性向上、公平かつ公正な社会を実現する社会基盤として位置づけられる。

➢ **マルウェア（主要事項「1.2.2　マルウェア」を参照）**

悪意のコード又は悪意のソフトウェアと呼ばれ、利用者の同意を得ずにコンピュータ等にインストールされ（感染）、利用者が意図しない有害な行為を行うプログラムの総称。

➢ **水飲み場型攻撃**

攻撃対象とするユーザが普段アクセスするウェブサイトにコンピュータウイルスを埋め込み、サイトを閲覧しただけでコンピュータウイルスに感染するような罠を仕掛ける攻撃方法。水飲み場に集まる動物を狙う猛獣の攻撃になぞらえている。

➢ **身代金要求ウイルス**

マルウェアの一種で、ユーザのコンピュータ内にある任意のファイルを暗号化し、暗号化を解除する見返りとして金銭を要求する不正なソフトウェアのこと。ランサムウェアとも呼ばれる。

➢ **メールフィルタ**

迷惑メールを取り除く機能のこと。 統合セキュリティ対策ソフトや一部の電子メールソフトに装備されている。

ラ

➢　ランサムウェア

「身代金要求ウイルス」を参照。

➢　リスク開示

投資判断などにつながる経営上のリスクを企業等から開示すること。リスク管理やコンプライアンスへの取組を積極的に開示することで、企業の信頼性の向上が期待できる。情報セキュリティに関するリスク開示の例として政府機関や企業による「情報セキュリティ報告書」の公開が挙げられる。

➢　リスクコミュニケーション

リスクのより適切なマネジメントのために、利害関係者が対話・共考・協働を通じて、多様な情報や情報の解釈の共有を図る活動のこと。ただし、リスクコミュニケーションの概念に関しては、個人や専門分野によって理解の方向性や力点が異なっており、必ずしも統一的定義はない。

➢　リスクマネジメント

組織を取り巻く様々なリスクに統一的に取り組むマネジメントであり、組織の状況を確定した上で、リスクアセスメントの一連のプロセス（リスクの特定、分析、評価）、リスク対応、モニタリング、レビューのPDCAを実施する。

➢　リベンジポルノ

復讐や嫌がらせ目的で、元交際相手等の性的な画像や動画を本人の同意なくインターネット上等で不特定多数に公開すること。

➢　量子暗号（Quantum Cryptography）

光子の量子的性質を利用して、盗聴されていないことが絶対に保証された情報を送受信者に供給する暗号方式。第三者が盗聴すると、盗聴を検知することができる。通信速度が遅いため、秘密鍵の送信などに用いることが想定されている。

➢　レジリエンス（Resilience）

日本語では回復力と訳される。インシデント等の事象に対して、あらかじめ準備を行ったり、対応について計画したりすることで、迅速かつ適切な復旧を行うことができる能力。

ワ

➢　「忘れられる権利」（主要事項「6.1.2 「忘れられる権利」」を参照）

個人のデータの削除を求める権利。2010年に欧州委員会で初めて掲げられ、欧州の新たなデータ保護の枠組みとなるEUデータ保護規則案においても、その理念が尊重されている。「忘れられる権利」にかかわる司法判断が国内外で下され、議論が高まっている。

➢　ワンタイムパスワード

本人認証を行うためのパスワードを毎回変更する方式。パスワードは時刻等によって生成され、万が一盗聴されたとしても再利用できず高い安全性を確保できる。