別添８　用語解説

	用　　語	解　　説
A	AI (Artificial Intelligence)	人工知能。昨今、深層学習の登場により、画像解析等の精度が向上し、製品の異常検知やガン診断等、既に幅広い産業分野で応用されているが、近年では、特に生成AIの発展が注目されている。
	AIST (National Institute of Advanced Industrial Science and Technology)	国立研究開発法人産業技術総合研究所（産総研）。経済産業省が所管し、サイバーセキュリティ分野ではセキュリティ強化技術や評価技術、セキュリティ保証スキーム等の研究に取り組んでいる。
	AJCCBC (ASEAN-Japan Cybersecurity Capacity Building Centre)	日ASEANサイバーセキュリティ能力構築センター。2018年９月にタイ・バンコクに設立され、ASEAN 諸国の政府職員及び重要インフラ事業者職員向けの演習等に取り組んでいる。
	APCERT (Asia Pacific Computer Emergency Response Team。エイピーサート)	2003年12月に発足したアジア太平洋地域に所在するCSIRTからなるコミュニティ。アジア太平洋地域におけるCSIRT間の協力関係の構築、インシデント対応時における連携の強化、円滑な情報共有、共同研究開発の促進、インターネットセキュリティの普及啓発活動、域内のCSIRT構築支援等に取り組んでいる。
	AppGoat	脆弱性の概要や対策方法等の脆弱性に関する基礎的な知識を実習形式で体系的に学べる体験学習ツール。
B	BCP (Business Continuity Plan)	緊急事態においても重要な業務が中断しないよう、又は中断しても可能な限り短時間で再開できるよう、事業の継続に主眼を置いた計画。重要インフラのサイバーセキュリティに係る行動計画において、重要インフラ事業者等は、任務保証を実施する観点から、BCPを整備・維持することが必要とされている。なお、BCPのうち情報（通信）システムについて記載を詳細化したものはIT-BCP（ICT-BCP）と呼ばれる。
C	CCRA (Common Criteria Recognition Arrangement)	CC承認アレンジメント。国際標準ISO/IEC15408セキュリティ評価基準（Common Criteria）に基づいて評価・認証された認証国18か国の認証製品を、受入国13か国を含む全てのCCRA加盟国で認証製品として相互に承認する協定。
	CERT (Computer Emergency Response Team。サート)	企業や行政機関等において、情報システム等にセキュリティ上の問題が発生していないか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う体制。CSIRTと同義。
	CISO (Chief Information Security Officer)	最高情報セキュリティ責任者。企業や行政機関等において情報システムやネットワークの情報セキュリティ、機密情報や個人情報の管理等を統括する責任者のこと。なお、「政府CISO」は内閣サイバーセキュリティセンター長が務める。
	CISSMED (Cyber Intelligence Sharing SIG for Medical)	医療分野について、医療情報の有識者を中心に厚生労働省が呼び掛け、他分野のISAC関係者の協力を得つつ、医療分野のISACの前進として2022年度に立ち上げた検討グループ。
	CPSF (Cyber/Physical Security Framework)	（「サイバー・フィジカル・セキュリティ対策フレームワーク」の項目を参照。）
	CRSAシステム (Continuous Risk Sourcing and Action システム)	常時リスク診断・対処システム。組織のセキュリティポリシー等に準拠するために情報システムに導入された必要なコントロール（管理策）に関し、以下３点を実施。①リスク診断：必要なコントロールと実際の状態とのギャップやリスクを可視化、②対処：可視化されたギャップやリスクの是正対応、③常時：ギャップやリスクの可視化と是正対応を継続的に実施。
	CRYPTREC (Cryptography Research and Evaluation Committees)	電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。デジタル庁、総務省及び経済産業省が共同で運営する暗号技術検討会と、NICT及びIPAが共同で運営する暗号技術評価委員会及び暗号技術活用委員会で構成される。
	CSAF (Common Security Advisory Framework)	標準化団体OASIS Openが開発した機械判読可能なセキュリティアドバイザリー標準。動的に変動する製品のセキュリティアドバイザリー情報を効率的に自動処理する目的で開発された。
	CSIRT (Computer Security Incident Response Team。シーサート)	企業や行政機関等において、情報システム等にセキュリティ上の問題が発生していないか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う体制。CERTと同義。

	CTF (Capture The Flag)	専門知識や技術を駆使して、問題の中に隠されたフラグ（＝キーワード）を探し出し、時間内に獲得した合計点数を競うクイズ形式のハッキングコンテスト。
	CVE (Common Vulnerabilities and Exposures)	共通脆弱性識別子。個別製品中の脆弱性を対象として米国政府の支援を受けた非営利団体のMITRE社が採番している識別子。個別製品中の脆弱性に一意の識別番号「CVE識別番号（CVE-ID）」を付与することにより、組織Aの発行する脆弱性対策情報と、組織Xの発行する脆弱性対策情報とが同じ脆弱性に関する対策情報であることを判断したり、対策情報同士の相互参照や関連付に利用したりできる。
	CYMAT (CYber incident Mobile Assistance Team。サイマット)	サイバー攻撃等により機関等の情報システム障害が発生した場合又はその発生のおそれがある場合であって、政府として一体となった対応が必要となる情報セキュリティに係る事象に対して機動的な支援を行うため、内閣官房内閣サイバーセキュリティセンターに設置される体制をいう。
	C&Cサーバ (Command and Control サーバ)	攻撃者がマルウェアに対して指令となるコマンドを送信し、マルウェア感染した端末の動作を制御するために用いられるサーバ。
D	DeltaWall	サイバーセキュリティ対策の鍵となる「自助」、「共助」、「公助」の３つの視点（Delta）と防御（Wall）を指し、金融業界全体のインシデント対応能力の更なる向上を図ることを目的に、金融庁が「金融業界横断的なサイバーセキュリティ演習（Delta Wall）」実施している。
	DFFT (Data Free Flow with Trust)	プライバシーやセキュリティ、知的財産権に関する信頼を確保しながら、ビジネスや社会課題の解決に有益なデータが国境を意識することなく自由に行き来する、国際的に自由なデータ流通の促進を目指す、というコンセプト。2019年１月にスイスで開催された世界経済フォーラム年次総会（ダボス会議）にて、安倍総理（当時）が提唱し、2019年６月のG20大阪サミットにおいて各国首脳からの支持を得て、首脳宣言に盛り込まれた。
	DDoS (Distributed Denial of Service)	分散型サービス不能攻撃。（DoSの項目を参照。）
	DoS (Denial of Service)	サービス不能攻撃。特定のサーバに対して一度に大量のデータを送出し、通信路やサーバの処理能力をあふれさせるものや、サーバやアプリケーションの脆弱性を悪用して機能を停止させるものがある。なお、複数の攻撃元から行われるDoS攻撃をDDoS攻撃という。
	DNS (Domain Name System)	ドメイン名とIPアドレスを対応付けて管理するシステム。
	DNSSEC (DNS Security Extensions)	DNSに対し、データ作成元の認証やデータの完全性を確認できるように仕様を拡張するもの。DNSSECによってデータの偽装を検知することが可能となる。これにより、 DNSキャッシュポイズニング(DNSサーバの脆弱性を利用して偽の情報をDNSサーバへ記憶させ、 そのDNSサーバを使用するユーザに対して影響を与える攻撃)のような攻撃を防ぐことができる。
	DX (Digital Transformation)	将来の成長、競争力強化のために、新たなデジタル技術を活用して新たなビジネスモデルを創出・柔軟に改変すること。
E	Emotet	主にメールの添付ファイルを感染経路としたマルウェア（不正プログラム）の一つ。Emotetに感染すると、感染端末からの情報漏えいや、他のマルウェアの感染といった被害に遭う可能性がある。
	eシール (Electronic seal)	電磁的記録に記録された情報（電子データ）に付与された又は論理的に関連付けられた電子データであって、次の要件のいずれにも該当するものをいう。 一 当該情報の出所又は起源を示すためのものであること。 二 当該情報について改変が行われていないかどうかの確認ができるものであること。 また、個人名の電子署名とは異なり、使用する個人の本人確認が不要であり、領収書や請求書等の経理関係書類等のような迅速かつ大量に処理するような場面において、簡便にデータの発行元を保証することが可能。
	e-ネットキャラバン	一般財団法人マルチメディア振興センターが運営している、インターネットの安心・安全な利用のために、保護者・教職員等向け及び小学生～高校生向けに実施する啓発・ガイダンス。総務省及び文部科学省支援のもと、保護者や学校の教職員、児童生徒を対象とするインターネットの安心・安全な利用に向けた啓発活動（全国規模で行う出前講座）を実施している。

F	FIRST (Forum of Incident Response and Security Teams)	各国のCSIRTの協力体制を構築する目的で、1990年に設立された国際協議会であり、2024年４月現在、世界107の官・民・大学等718の組織が参加している。
G	G7 (Group of Seven)	主要７か国（仏、米、英、独、日、伊、加（議長国順））首脳会議。
	G20 (Group of Twenty)	G7各国に加え、欧州連合（EU）、亜、豪、ブラジル、中、印、インドネシア、メキシコ、韓、露、サウジアラビア、南アフリカ、トルコ（アルファベット順）の首脳が参加して毎年開催される国際会議。
	GIGAスクール構想	Society5.0時代を生きる全てのこどもたちの可能性を引き出す、個別最適な学びと協働的な学びを実現するため、児童生徒の１人１台端末と、学校における高速大容量の通信ネットワークを一体的に整備する構想。
	GSOC (Government Security Operation Coordination team。ジーソック)	24時間365日、政府横断的な情報収集、攻撃等の分析・解析、政府機関への助言、政府関係機関の相互連携促進及び情報共有等の業務を行うため、内閣官房内閣サイバーセキュリティセンターに設置される体制をいう。なお、GSOCには、政府機関を対象とした「第一GSOC」と独立行政法人及び指定法人を対象とした「第二GSOC」がある。
H	HPKI (Healthcare Public Key Infrastructure)	保健医療福祉分野の公開鍵基盤。医療現場において、公的資格の確認機能を有する電子署名や電子認証を行う基盤。
I	icat	サイバーセキュリティ注意喚起サービス。IPAを通じ、ソフトウェア等の脆弱性に関する情報がタイムリーに発信されている。
	ICT (Information and Communications Technology)	情報通信技術。
	iLogScanner	ウェブサーバのアクセスログから攻撃と思われる痕跡を検出するためのツール。ウェブサイトのログを解析することで攻撃の痕跡を確認でき、一部の痕跡については攻撃が成功した可能性の確認が可能。
	IoC (Indicator of Compromise)	セキュリティ侵害インジケータ。システムに対する攻撃発生やどのようなツールが使われたかなどを明らかにする手がかりとなる情報。
	IoT (Internet of Things)	あらゆる物がインターネットを通じてつながることによって実現する新たなサービス、ビジネスモデル、又はそれを可能とする要素技術の総称。
	IoTセキュリティ・セーフティ・フレームワーク	経済産業省において、IoT 機器に求められる機能の要求を明確化するとともに、フィジカル空間とサイバー空間のつながりの信頼性確保の考え方を整理したもの。
	IPA (Information-technology Promotion Agency)	独立行政法人情報処理推進機構。ソフトウェアの安全性・信頼性向上対策、総合的なIT人材育成事業（スキル標準、情報処理技術者試験等）とともに、情報セキュリティ対策の取組として、コンピュータウイルスや不正アクセスに関する情報の届出受付、国民や企業等への注意喚起や情報提供等を実施している独立行政法人。
	IPアドレス (Internet Protocol address)	インターネットやイントラネットなど、IPネットワークに接続されたコンピュータや通信機器等に割り振られた識別番号。これらのうち、インターネットに接続された機器に割り当てられるIPアドレスで、世界中でひとつしかないアドレスをグローバルIPアドレスという。
	ISAC (Information Sharing and Analysis Center)	サイバーセキュリティに関する情報収集や、収集した情報の分析等を行う組織。分析した情報はISACに参加する会員間で共有され、各々のセキュリティ対策等に役立てられる。
	ISMAP (Information system Security Management and Assessment Program)	政府情報システムのためのセキュリティ評価制度（通称イスマップ）。政府情報システムにおけるクラウドサービスのセキュリティ評価制度として2020年度に制度運用を開始。
	ISMAP-LIU (ISMAP for Low-Impact Use)	ISMAPの枠組みのうち、リスクの小さな業務・情報の処理に用いるSaaSサービスを対象にした仕組み。

	ISO (International Organization for Standardization)	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国際標準化機関。
	ISO/IEC JTC 1/SC 27	情報セキュリティ、サイバーセキュリティ、プライバシー保護の分野を対象に、国際規格を策定するISO/IEC JTC 1 配下の分科委員会。 https://www.iso.org/committee/45306.html　参照。
	ISP (Internet Service Provider)	インターネット接続事業者。
	ITSS+	第４次産業革命に向けて求められる新たな領域の“学び直し”の指針。従来のITスキル標準（ITSS)が対象としていた情報サービスの提供やユーザ企業の情報システム部門の従事者のスキル強化を図る取組みに活用されることを想定しており、「データサイエンス領域」「アジャイル領域」「IoTソリューション領域」「セキュリティ領域」について策定している。
	ITU (International Telecommunication Union)	国際電気通信連合。国際連合の専門機関の一つ。国際電気通信連合憲章に基づき無線通信と電気通信分野において各国間の標準化と規制を確立することを目的とする。
	ITU-T (International Telecommunication Union Telecommunication Standardization Sector)	ITUの電気通信標準化部門。
	IT調達申合せ	IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ。政府機関等において特に防護すべき情報システム・機器・役務等に関する調達の基本的な方針及び手続について、関係省庁で申し合わせた（取り決めした）もの。
	IWWN (International Watch and Warning Network)	サイバー空間の脆弱性、脅威、攻撃に対応する国際的な取組の促進を目的とした会合。
J	JC3 (Japan Cybercrime Control Center)	一般財団法人日本サイバー犯罪対策センター。産学官連携によるサイバー犯罪等への対処のため、日本版NCFTA（サイバー空間における脅威への対処を目的として米国で発足した非営利団体）として設立された。
	JISEC (Japan Information Technology Security Evaluation and Certification Scheme)	国内外の政府調達のためのセキュリティ要件の評価認証制度。IT関連製品のセキュリティ機能の適切性・確実性を、セキュリティ評価基準の国際標準であるISO/IEC 15408に基づいて第三者（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。
	JISP (Japan cyber security Information Sharing Partnership。ジスプ)	サイバーセキュリティ対策を政府が積極的に支援する官民連携の取組。民間団体、地方公共団体、政府関係組織、情報セキュリティ関係機関等が、サイバーセキュリティに関する脅威情報、インシデント情報等をワンストップで共有でき、参加組織からの要請に応じて助言及び対処支援調整を行うパートナーシップ。2019年４月から2020年東京オリンピック/パラリンピック競技大会のサイバーセキュリティの取組として運用を開始し、2022年４月から、サイバーセキュリティ協議会の枠組みの中での取組として活動を継承した。社会経済を支えるサービスを提供する組織を対象に加え、社会全体のサイバーセキュリティの確保に向け、持続的なサイバーセキュリティ対策の推進を目的としている。
	JPCERT/CC (Japan Computer Emergency Response Team/Coordination Center)	インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデントについて、日本国内のサイトに関する報告の受付、対応の支援、発生の状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行っている機関。特定の政府機関や企業からは独立した組織として、日本における情報セキュリティ対策活動の向上に積極的に取り組んでいる。1996年10月に「コンピュータ緊急対応センター」として発足。
	JST (Japan Science and Technology Agency)	国立研究開発法人科学技術振興機構。知の創出から研究成果の社会還元とその基盤整備を担う国内の中核的組織。新たな科学知識に基づく創造的な革新的技術のシーズ（新技術シーズ）を創出することを目的として戦略的創造研究推進事業を推進しており、CREST・さきがけ・ERATO・ACT-X等のプログラムがある。

	JVN (Japan Vulnerability Notes)	JPCERT/CCとIPAが共同で管理している脆弱性対策情報提供サイト。
	JVN iPedia	IPAが運営する脆弱性情報データベース。
L	LAN (Local Area Network)	企業内、ビル内、事業所内等の狭い空間においてコンピュータやプリンタ等の機器を接続するネットワーク。
	LGWAN (Local Government Wide Area Network)	総合行政ネットワーク。地方公共団体の組織内ネットワークを相互に接続する行政専用ネットワークであり、安全確実な電子文書交換、電子メール、情報共有及び多様な業務支援システムの共同利用を可能とする電子自治体の基盤。
	Living Off The Land攻撃 (LOTL攻撃)	システム内寄生攻撃。ネットワーク機器の脆弱性の悪用等により初期侵入を行った後、従来から行われているマルウェアを用いたサイバー攻撃とは異なり、システム内に組み込まれている正規の管理ツール、コマンド、機能等を用いて、認証情報の窃取、システム情報の収集等の活動を行う。
M	Mejiro	JPCERT/CCが提供するインターネットリスク可視化サービス。インターネット上のリスク要因に関するデータを収集し、国・地域別の指標を計算して可視化している。
	MOU/NDA (Memorandum Of Understanding/Non-Disclosure Agreement)	覚書及び秘密保持契約。
	MyJVN API	ウェブを通じてJVN iPediaの情報を利用するためのソフトウェアインタフェース。MyJVN が提供する API を利用して様々な脆弱性対策情報を取得し、脆弱性対策情報を利用したサイトやアプリケーションを開発することが可能となる。
N	NEDO (New Energy and Industrial Technology Development Organization)	国立研究開発法人新エネルギー・産業技術総合開発機構。
	NICT (National Institute of Information and Communications Technology)	国立研究開発法人情報通信研究機構。情報通信技術分野の研究開発を基礎から応用まで統合的な視点で実施するとともに、産学官で連携し研究成果の社会還元等を行う独立行政法人。
	NICTER	無差別型サイバー攻撃の大局的な動向を把握することを目的としたサイバー攻撃観測・分析システム。ダークネットと呼ばれる未使用のIPアドレスを大規模に観測している。
	NII (National Institute of Informatics)	国立情報学研究所。大学共同利用機関法人 情報・システム研究機構に属する研究所。情報学という新しい学問分野での「未来価値創成」を目指す、我が国唯一の学術総合研究所として、ネットワーク、ソフトウェア、コンテンツなどの情報関連分野の新しい理論・方法論から応用までの研究開発を総合的に推進している。
	NII-SOCS (NII Security Operation Collaboration Services)	NIIの事業の１つで、大学間連携に基づく情報セキュリティ体制の基盤構築を指す。大学間連携に基づきサイバーセキュリティ人材を養成すると同時に、攻撃検知・防御能力の研究成果を適宜適用することで、国立大学法人等におけるサイバーセキュリティ基盤の質の向上を図るとともに、サイバーセキュリティ研究の推進環境と、全ての学術研究分野に対する安心・安全な教育研究環境を提供するための研究開発等を進めている。
	NISC (National center of Incident readiness and Strategy for Cybersecurity)	内閣サイバーセキュリティセンター。サイバーセキュリティ戦略本部の事務の処理を行い、我が国におけるサイバーセキュリティの司令塔機能を担う組織として、2015年１月９日、内閣官房情報セキュリティセンター（National Information Security Center）を改組し、内閣官房に設置された。センター長は、内閣官房副長官補（事態対処・危機管理担当）が務めている。
	NIST (National Institute of Standards and Technology)	アメリカ国立標準技術研究所。
	NOTICE (National Operation Towards IoT Clean Environment)	サイバー攻撃に悪用されるおそれのあるIoT機器をNICTで調査し、当該機器の利用者への注意喚起を行う取組。

O	OS (Operating System)	多くのアプリケーションソフトが共通して利用する基本的な機能を提供し、コンピュータシステムを管理する基本ソフトウェア。
	OSS (Open Source Software)	ソフトウェアのソースコードが無償で公開され、利用や改変、再配布を行うことが誰に対しても許可されているソフトウェア。
	OT (Operational Technology)	システムを運用するための技術。
P	PJMO (Project Management Office)	プロジェクトを推進する組織。
	PoC (Proof of Concept)	概念実証。
	PP (Protection Profile)	IT製品のセキュリティ上の課題に対する要件をCC（国際規格）に従って規定したセキュリティ要求仕様。主に調達要件として用いられる。
	PSIRT (Product Security Incident Response Team)	企業において、製品を利用する顧客に関わるインシデント対応を主たる機能とする組織。
Q	Q-LEAP	「光・量子飛躍フラッグシッププログラム」。経済・社会的な重要課題に対し、量子科学技術（光・量子技術）を駆使して、非連続的な解決（Quantum leap）を目指す研究開発プログラム。
R	RPKI (Resource Public-Key Infrastructure)	リソースPKI（PKI:公開鍵基盤）。IPアドレスやAS番号といった、アドレス資源の割振りや割当てを証明するためのPKIを指す。
	RMF (Risk Management Framework)	リスク管理枠組み。米国防省の最新のセキュリティ基準を参考に、防衛省・自衛隊の情報システムに導入された。
S	SBOM (Software Bill of Materials)	ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リスト。
	SCAP (Security Content Automation Protocol)	情報セキュリティに関わる技術面での自動化と標準化を実現する技術仕様。
	SINET (Science Information NETwork)	日本全国の大学、研究機関等の学術情報基盤として、国立情報学研究所(NII)が構築、運用している情報通信ネットワーク。
	SIP (cross-ministerial Strategic Innovation promotion Program)	戦略的イノベーション創造プログラム。内閣府総合科学技術・イノベーション会議が司令塔機能を発揮して、府省の枠や旧来の分野を越えたマネジメントにより、科学技術イノベーション実現のために創設した国家プロジェクト。国民にとって真に重要な社会的課題や、日本経済再生に寄与できるような課題に取り組み、基礎研究から実用化・事業化（出口）までを見据えて一気通貫で研究開発を推進する。
	SNS (Social Networking Service)	社会的ネットワークをインターネット上で構築するサービス。
	SOC (Security Operation Center)	セキュリティ・サービス及びセキュリティ監視を提供するセンター。
	Society5.0	狩猟社会、農耕社会、工業社会、情報社会に続く、人類史上５番目の新しい社会。新しい価値やサービスが次々と創出され、社会の主体たる人々に豊かさをもたらしていく。（出典：未来投資戦略2017（平成29年６月９日閣議決定））
	SSDF (Secure Software Development Framework)	米国NISTが策定した「ソフトウェアの脆弱性を軽減するためのソフトウェア開発者向けの手法をまとめたフレームワーク」。各手法は４つに分類され、手法を実践するためのタスクが体系化されている。各手法の実践により、脆弱性を低減するとともに、未対処のまま悪用された場合の影響を軽減し、脆弱性の再発を防ぐ根本原因に対処可能となる。
	STARDUST （スターダスト）	NICTにおいて研究開発している、高度かつ複雑なサイバー攻撃に対処するため、政府や企業等の組織を模擬したネットワークに攻撃者を誘い込み、攻撃者の組織侵入後の詳細な挙動をリアルタイムに把握することを可能とするサイバー攻撃誘引基盤。

T	TSUBAME	JPCERT/CCが運営するインターネット定点観測システム。インターネット上に観測用センサーを分散配置し、セキュリティ上の脅威となるトラフィックの観測を実施。得られた情報はウェブサイト等を通じて提供されている。
	TTP	Tactics, Techniques and Proceduresの略で、サイバー攻撃者の振る舞いである戦術、技術及び手順を指す。
U	URL	Uniform Resource Locator（ユニフォーム・リソース・ロケータ）アドレス。インターネット上において情報が格納されている場所を示すための住所のような役割を果たす文字列。
V	VPN (Virtual Private Network)	インターネット等の公衆回線網上で、認証技術や暗号化等の技術を利用し、保護された仮想的な専用線環境を構築する仕組み。
	VRDA フィード (Vulnerability Response Decision Assistanceフィード)	ユーザが脆弱性への対応判断を行う際に必要となる脆弱性の脅威を把握するための情報を、基準となる分析項目とそれら項目に対応する分析値として取りまとめ、定型データフォーマットで表現して配信するもの。
5	5G	第５世代移動通信システム。2015年９月、ITUにおいて、5Gの主要な能力やコンセプトをまとめた「IMTビジョン勧告（M.2083）」が策定され、その中で、5Gの利用シナリオとして、「モバイルブロードバンドの高度化（eMBB：enhanced Mobile BroadBand）」「超高信頼・低遅延通信（URLLC：Ultra-Reliable and Low Latency Communications）」「大量のマシーンタイプ通信（mMTC：massive Machine Type Communications）」の３つのシナリオが提示されており、主な要求条件として、「最高伝送速度 20Gbps」「１ミリ秒程度の遅延」「100万台/㎢の接続機器数」が挙げられている。
あ	アクセス制御	情報等へのアクセスを許可する者を制限等によりコントロールすること。
	アタックサーフェスマネジメント	政府機関等の情報システムをインターネット上から組織横断的に常時評価し、脆弱性等の随時是正を促す取組。
	暗号資産	中央銀行や政府機関によって発行された通貨でないが、取引、貯金、送金等に使用可能な、通貨価値をデジタルで表現したもの。 資金決済に関する法律（平成21年法律第59号）第２条第５項においては、以下のように定義されている。 ① 物品を購入し、若しくは借り受け、又は役務の提供を受ける場合に、これらの代価の弁済のために不特定の者に対して使用することができ、かつ、不特定の者を相手方として購入及び売却を行うことができる財産的価値（電子機器その他の物に電子的方法により記録されているものに限り、本邦通貨及び外国通貨並びに通貨建資産を除く。次号において同じ。）であって、電子情報処理組織を用いて移転することができるもの。 ② 不特定の者を相手方として①と相互に交換を行うことができる財産的価値であって、電子情報処理組織を用いて移転することができるもの。
い	インシデント	中断・阻害、損失、緊急事態又は危機になり得る又はそれらを引き起こし得る状況のこと（ISO22300）。IT分野においては、システム運用やセキュリティ管理等における保安上の脅威となる現象や事案を指すことが多い。
	インターネットの安全・安心ハンドブック	サイバーセキュリティに関する普及啓発活動の一環としてNISCが公開しているハンドブック。サイバーセキュリティに関する基本的な知識を紹介し、誰もが最低限実施しておくべき基本的なサイバーセキュリティ対策を実行してもらうことで、更に安全・安心にインターネットを利活用してもらうことを目的に制作された。サイバー空間の最新動向や、今特に気を付けるべきポイント等を踏まえ、2023年１月にVer.5.00として改訂。
か	完全性	情報に関して破壊、改ざん又は消去されていないこと（Integrity）。
	カウンターインテリジェンス	外国の敵意ある情報活動を無効にするための防諜活動。
く	クラウドサービス	事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。クラウドサービスの例としては、SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）等がある。

	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	総務省において、2014年４月策定。クラウドサービス利用の進展状況等に対応するため、クラウドサービス提供事業者が留意すべき情報セキュリティ対策に関するガイドライン。2018年７月に第２版を公表し、クラウド事業者のIoTサービスリスクへの対応に関する内容を追加。また2021年９月に第３版を公表し、クラウドサービスにおける責任分界の在り方や国際規格等との整合性を踏まえた内容に改定。
	クラウド・バイ・デフォルト原則	システム導入時に、クラウドサービスの利用を第一候補として、その検討を行う。
こ	コマンド実行（コマンドインジェクション）	オペレーティングシステムのコマンドを不正に実行できてしまう脆弱性及び攻撃手法。
	コンティンジェンシープラン	重要インフラ事業者等が重要インフラサービス障害の発生又はそのおそれがあることを認識した後に経営層や職員等が行うべき初動対応（緊急時対応）に関する方針、手順、態勢等をあらかじめ定めたもの。
さ	サイバーインテリジェンス	情報通信技術を用いた諜報活動。
	サイバー攻撃	一般的には、インターネットやコンピュータ等を悪用することにより、情報の窃取等を行うこととされる。サイバーセキュリティ基本法第２条では「情報通信ネットワーク又は（中略）記録媒体（中略）を通じた電子計算機に対する不正な活動」が例示されている。また、2013年に策定されたサイバーセキュリティ戦略（2013年６月情報セキュリティ政策会議決定）では、「情報通信ネットワークや情報システム等の悪用により、サイバー空間を経由して行われる不正侵入、情報の窃取、改ざんや破壊、情報システムの作動停止や誤作動、不正プログラムの実行やDDoS攻撃（分散サービス不能攻撃）等」とされている。
	サイバーセキュリティ	コンピュータ、ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていること。サイバーセキュリティ基本法第２条では、「この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（略）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（略）が講じられ、その状態が適切に維持管理されていることをいう。」とされている。
	サイバーセキュリティ意識・行動強化プログラム	サイバーセキュリティ普及啓発について、産学官民の関係者が円滑かつ効果的に活動し、有機的に連携できるよう、2019年１月24日にサイバーセキュリティ戦略本部にて決定。
	サイバーセキュリティお助け隊サービス	相談窓口、システムの異常の監視、緊急時の対応支援、簡易サイバー保険など中小企業のサイバーセキュリティ対策を支援するサービス。
	サイバーセキュリティ関係機関	重要インフラのサイバーセキュリティに係る行動計画における関係主体の一つ。国立研究開発法人情報通信研究機構（NICT）、独立行政法人情報処理推進機構（IPA）、一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）、一般財団法人日本サイバー犯罪対策センター（JC3）。
	サイバーセキュリティ基本法	サイバーセキュリティに関する施策を総合的かつ効率的に推進するため、基本理念を定め、国の責務等を明らかにし、戦略の策定その他当該施策の基本となる事項等を定めた法律。2014年11月12日公布・一部施行、2015年１月９日完全施行。
	サイバーセキュリティ協議会	政府機関等のPCがランサムウェア「WannaCry（ワナクライ）」に感染した事案を踏まえ、2018年12月に成立したサイバーセキュリティ基本法の一部を改正する法律に基づき、2019年４月１日に、官民の多様な主体が相互に連携し、サイバーセキュリティに関する施策の推進に係る協議を行うために組織されたもの。本協議会は、官民又は業界を問わず多様な主体が連携し、サイバーセキュリティの確保に資する情報を迅速に共有することにより、サイバー攻撃による被害を防ぎ、また、被害の拡大を防ぐことなどを目的としている。2022年４月１日には、JISPを統合し、機能の充実強化を図っている。
	サイバーセキュリティ経営ガイドライン	経済産業省及びIPAの共同により策定されている、大企業及び中小企業（小規模事業者を除く）のうち、ITに関するシステムやサービス等を供給する企業及び経営戦略上ITの利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するためのガイドライン。2015年12月にVer1.0を策定、2017年11月にVer2.0に改訂。

サイバーセキュリティ月間	重点的かつ効果的にサイバーセキュリティに対する取組を推進するため、2010年より毎年２月に実施してきた「情報セキュリティ月間」を、2015年から、２月１日～３月18日に期間を拡大したもの。月間の期間中、各種啓発主体と連携し、サイバーセキュリティに関する普及啓発活動を集中的に実施。
サイバーセキュリティ戦略	我が国のサイバーセキュリティ政策に関する国家戦略であり、政府は、サイバー空間そのものが量的に拡大・質的に進化するとともに、実空間との融合が進み、あらゆる国民、セクター、地域等において、サイバーセキュリティの確保が必要とされる時代（Cybersecurity for All）が到来したという状況を踏まえ、2020年代はじめの今後３年間に取るべき諸施策の目標や実施方針を国内外に明確に示すことにより、共通の理解と行動の基礎となるもの。
サイバーセキュリティ戦略本部	2015年１月９日、サイバーセキュリティ基本法に基づき内閣に設置された。我が国における司令塔として、サイバーセキュリティ戦略の案の作成及び実施の推進、国の行政機関等における対策の実施状況に関する監査、重大事象に対する原因究明のための調査等を事務としてつかさどる。本部長は、内閣官房長官。
サイバーテロ対策協議会	警察とサイバー攻撃の標的となるおそれのある重要インフラ事業者等との間で構成する組織。全国の都道府県に設置されており、サイバー攻撃の脅威や情報セキュリティに関する情報共有のほか、サイバー攻撃の発生を想定した共同対処訓練やサイバー攻撃対策セミナー等の実施により、重要インフラ事業者等のサイバーセキュリティや緊急対処能力の向上に努めている。
サイバーセキュリティ対策情報開示の手引き	民間企業にとって参考となり得る情報開示の実例等をまとめたもの。総務省に設置したサイバーセキュリティタスクフォース下の「情報開示分科会」にて検討を進め、2019年６月に公表。
サイバーセキュリティ対処調整センター	東京大会のサイバーセキュリティに係る脅威・事案情報を収集し、関係機関等に提供するとともに、関係機関等における事案対処に対する支援調整を行う組織として、2019年４月に設置。2022年４月から、サイバーセキュリティ協議会の枠組みの中で、JISPの運営事務局として活動を継承している。
サイバーセキュリティネクサス（CYNEX）	NICTが2021年にサイバーセキュリティ分野における産学官の結節点となることを目指し設立した組織。多種多様なサイバーセキュリティ関連情報を大規模集約した上で、横断的かつ多角的に分析し、実践的かつ説明可能な脅威情報を生成するための基盤を構築するとともに、生成された脅威情報を必要とする関係機関に継続的に提供している。また、当該基盤を活用し、国産セキュリティ技術を機器製造事業者や運用事業者が検証できる環境を構築している。
サイバーニュースフラッシュ(CyberNewsFlash)	JPCERT/CCのウェブサイトにあるコラム。情報収集・分析・情報発信を行っている早期警戒グループのメンバーが、脆弱性やマルウェア、サイバー攻撃などに関する情報を掲載している。
サイバーハイジーン	インターネットの利用環境など、ICT環境を健全なセキュリティ状態に保っておくこと。
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（通称ブダペスト条約）。サイバー犯罪に効果的かつ迅速に対処するために国際協力を行い、共通の刑事政策を採択することを目的とする条約。
サイバー・フィジカル・セキュリティ対策フレームワーク	サイバー空間とフィジカル空間を高度に融合させることにより実現される「Society5.0」における新たなサプライチェーン（バリュークリエイションプロセス）全体のサイバーセキュリティ確保を目的として、産業に求められるセキュリティ対策の全体像を整理したもの。経済産業省に設置した産業サイバーセキュリティ研究会WG1の下で検討を進め、2019年４月にVersion 1.0を策定。
サイバーフォースセンター	警察庁に設置。サイバー攻撃の予兆・実態把握、標的型メールに添付された不正プログラム等の分析を実施するほか、事案発生時には技術的な緊急対処の拠点として機能する。
サイバーレンジ	サイバー攻撃や防御の演習を行うために電子計算機上に特別に構築する仮想空間。
サプライチェーン	一般的には、取引先との間の受発注、資材の調達から在庫管理、製品の配達まで、いわば事業活動の川上から川下に至るまでのモノや情報の流れのこと。これらに加えてさらに、ITにおけるサプライチェーンでは、製品の設計段階や、情報システム等の運用・保守・廃棄を含めてサプライチェーンと呼ばれることがある。

	サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）	情報セキュリティ対策が強固とはいえない中小企業を対象にサイバー攻撃やそれに起因する大企業等への被害が顕在化してきており、大企業のみならず、サプライチェーンを構成する地域の中小企業であっても、サイバー攻撃の脅威にさらされているという状況を踏まえ、産業界が一体となって中小企業を含むサプライチェーン全体でのサイバーセキュリティ対策の推進活動を進めていくことを目的として、2020年11月１日に設立。
	サプライチェーン・リスク	従来のサプライチェーン・リスクは、自然災害等、何らかの要因からサプライチェーンに障害が発生し、結果として事業の継続に支障を来すおそれがあるというリスクを主に想定していた。ITにおける新たなサプライチェーン・リスクとしては、サプライチェーンのいずれかの段階において、サイバー攻撃等によりマルウェア混入・情報流出・部品調達への支障等が発生する可能性も考慮する必要がある。また、サプライチェーンのいずれかの段階において、悪意のある機能等が組み込まれ、機器やサービスの調達に際して情報窃取・破壊・情報システムの停止等を招く可能性についても想定する必要がある。
	産業サイバーセキュリティ研究会	経済産業省において設置された研究会。我が国の産業が直面する、深刻度を増しているサイバーセキュリティの課題を洗い出し、関連政策を推進していくため、産業界を代表する経営者、インターネット時代を切り開いてきた学識者等から構成される。
し	事業継続計画	（BCPの項目を参照。）
	実践的サイバー防御演習（CYDER）	総務省がNICTを通じ実施しており、国の機関、指定法人、独立行政法人、地方公共団体及び重要インフラ事業者等の情報システム担当者等を対象とした体験型の実践的サイバー防御演習。
	重要インフラ事業者	重要インフラのサイバーセキュリティに係る行動計画における関係主体の一つ。重要インフラ分野に属する事業を行う者のうち、同行動計画の「別紙１　対象となる重要インフラ事業者等と重要システム例」の「対象となる重要インフラ事業者等」欄において指定するもの及びその組織する団体並びに地方公共団体。 「重要インフラ事業者等」とは重要インフラ事業者及びその組織する団体並びに地方公共団体をいう。 現在、「情報通信」、「金融」、「航空」、「空港」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」、「医療」、「水道」、「物流」、「化学」、「クレジット」、「石油」及び「港湾」の計15分野を指定。 また、上記を所管する金融庁、総務省、厚生労働省、経済産業省及び国土交通省を重要インフラ所管省庁という。
	重要インフラ専門調査会	我が国全体の重要インフラ防護に資するサイバーセキュリティに係る事項について、調査検討を行うため、サイバーセキュリティ基本法施行令（平成26年政令第400号）第２条の規定に基づいて設置される会議体であり、委員は内閣総理大臣が任命する。
	重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書	重要インフラのサイバーセキュリティに係る行動計画に基づき、「安全基準等策定指針」で定めたリスクアセスメントや情報共有を行う際の手順を具体的に示したもの。
	重要インフラのサイバーセキュリティに係る安全基準等策定指針	重要インフラのサイバーセキュリティに係る行動計画に基づき、重要インフラサービスの安全かつ持続的な提供を図る観点から、「安全基準等」において規定が望まれる項目を整理・記載し、重要インフラ事業者や重要インフラ所管省庁の「安全基準等」の策定・改定を支援することを目的とするもの。
	重要インフラのサイバーセキュリティに係る行動計画	安全で安心な社会の実現には、官民の緊密な連携による重要インフラのサイバーセキュリティの確保が必要であり、基本的な枠組みとして、政府と重要インフラ事業者等との共通の行動計画を推進してきた。重要インフラの情報セキュリティに係る第４次行動計画（平成29年４月18日サイバーセキュリティ戦略本部決定）を見直し、同行動計画における有効な取組は継続しつつ、組織統治の一部としてサイバーセキュリティを組み入れ、組織全体で対応すること、また重要インフラを取り巻く脅威の変化に対応するため、将来の環境変化を先取りし、サプライチェーンを含めてリスクを明確化し対応することなどを盛り込んだもの。
	情報セキュリティインシデント	望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。（JIS Q 27000:2019）

す	スマートシティセキュリティガイドライン	総務省が安全・安心なスマートシティの推進のため、スマートシティの構築・運営におけるセキュリティの考え方やセキュリティ対策を取りまとめ公表しているガイドライン。2024年に「スマートシティセキュリティガイドライン（第3.0版）」として改定された。
せ	政府情報システムのためのセキュリティ評価制度	（ISMAPの項目を参照。）
	セキュアバイデザイン	IT 製品（特にソフトウェア）が、設計段階から安全性を確保されていること。前提となるサイバー脅威の特定、リスク評価が不可欠。
	セキュアバイデザイン・セキュアバイデフォルトに関する文書	米国サイバーセキュリティ・インフラ安全庁（CISA）等が策定した文書。我が国は2023年10月、当該文書の改訂に当たり、共同署名したことを公表。主な内容は、ソフトウェア作成業者がユーザのセキュリティ強化のために特に講じることが求められる項目をリストアップしたもの。技術の進歩が早い分野であることから、その内容の適切性については政府側が産業界と継続的に適切な対話を重ねて改善を図っていく、という旨も明記されている。
	セキュアバイデフォルト	ユーザ（顧客）が、追加コストや手間をかけることなく、 購入後すぐにIT 製品（特にソフトウェア）を安全に利用できること。
	セキュリティ・バイ・デザイン	（セキュアバイデザインの項目を参照。）
	積極的サイバー防御	サイバー関連事業者等と連携し、脅威に対して事前に積極的な防御策を講じること。サイバーセキュリティ基本法の目的の一つである「国民が安全で安心して暮らせる社会の実現」に係る取組の実施方針として掲げられたもの。
	セプター	重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。Capability for Engineering of Protection, Technical Operation, Analysis and Response の略称(CEPTOAR)。2005年以降順次構築が進められ、2024年３月末現在、15分野で21セプターが活動。
	セプターカウンシル	各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う。政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体。
	ゼロトラストアーキテクチャ	利便性を保ちながら、クラウド活用や働き方の多様化に対応するため、ネットワーク接続を前提に利用者やデバイスを正確に特定、常に監視・確認する次世代のネットワークセキュリティ環境のことで、「内部であっても信頼しない、外部も内部も区別なく疑ってかかる」という「性悪説」に基づいた考え方でセキュリティを確保する。
そ	ソーシャルエンジニアリング	人間の心理的な隙や行動のミスにつけ込み、ネットワークに侵入するために必要となるパスワードなどの重要な情報を、情報通信技術を使用せずに盗み出す方法。
	ソフトウェアタスクフォース	経済産業省において平成31年４月にサイバーセキュリティ対策フレームワークを策定。同フレームワークに基づくセキュリティ対策の具体化・実装を促進するため、検討すべき項目ごとに焦点を絞ったタスクフォースを設置している。OSSを含むソフトウェア管理手法等については、ソフトウェアタスクフォースにおいて検討されている。
た	大規模サイバー攻撃事態等	国民の生命、身体、財産若しくは国土に重大な被害が生じ、若しくは生じるおそれのあるサイバー攻撃事態又はその可能性のある事態。例えば、サイバー攻撃により、人の死傷、重要インフラサービスの重大な供給停止等が発生する事態。
	多層防御	システム内に複数の防御層を設置することで、さまざまな種類のサイバー攻撃から機密情報などを守る。具体的には、以下の３つの領域において対策を行う。 ・ 入口対策（社内ネットワークへのウイルスの侵入・不正アクセスなどの脅威を未然に防ぐ対策） ・ 内部対策（脅威となる存在の侵入を阻止できなかった場合などに、被害の拡大を防止する対策） ・ 出口対策（機密情報や個人情報などの外部漏洩を阻止するための対策）
ち	地域SECUNITY	地域のセキュリティの関係者（公的機関、教育機関、地元企業、地元ベンダー等）が集まりセキュリティについての相談や意見交換を行うためのセキュリティコミュニティ。“SECURITY”と“COMMUNITY”を組み合わせた造語。
	中小企業の情報セキュリティ対策ガイドライン	情報セキュリティ対策に取り組む際の、(1)経営者が認識し実施すべき指針、(2) 社内において対策を実践する際の手順や手法をまとめたもの。
て	ディレクトリトラバーサル	アクセスされることを想定していない非公開情報が保存されているファイル（ディレクトリ）に不正な手段でアクセスすることを指す。パストラバーサルとも。

	デジタル社会の実現に向けた重点計画	デジタル社会の形成が、我が国の国際競争力の強化及び国民の利便性の向上に資するとともに、急速な少子高齢化の進展への対応その他の我が国が直面する課題を解決する上で極めて重要であることに鑑み、我が国経済の持続的かつ健全な発展と国民の幸福な生活の実現に寄与することを目的とし、デジタル社会の形成のために政府が迅速かつ重点的に実施すべき施策に関する基本的な方針を定める計画。2023年６月７日に閣議決定。
	デジタル田園都市国家構想総合戦略	内閣官房デジタル田園都市国家構想実現会議事務局において、まち・ひと・しごと創生総合戦略を抜本的に改訂し、デジタル田園都市国家構想を実現するために、各府省庁の施策を充実・強化し、施策ごとに2023年度から2027年度までの５か年のKPI（重要業績評価指標）とロードマップ（工程表）を位置づけた総合戦略。
	デジタルトランスフォーメーション	（DXの項目を参照。）
	デジタルフォレンジック	不正アクセスや機密情報漏えい等、コンピュータ等に関する犯罪や法的紛争が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称。
	テストベッド	システム開発時に、実際の使用環境に近い状況を再現することが可能な試験用環境又は試験用プラットフォームの総称。
	電子署名	電子文書に付加される電子的な署名情報。電子文書の作成者の本人性確認や、改ざんが行われていないことを確認できるもの。
と	統一基準群	国の行政機関、独立行政法人及び指定法人の情報セキュリティを確保するため、これらのとるべき対策の統一的な枠組みについて定めた一連のサイバーセキュリティ戦略本部決定文書等のこと。「政府機関等のサイバーセキュリティ対策のための統一規範」、「政府機関等のサイバーセキュリティ対策の運用等に関する指針」、「政府機関等のサイバーセキュリティ対策のための統一基準」（令和５年７月４日サイバーセキュリティ戦略本部決定）及び「政府機関等の対策基準策定のためのガイドライン」（令和５年７月４日内閣官房内閣サイバーセキュリティセンター決定）。
	トラストサービス	データの改ざんや送信元のなりすまし等を防止する仕組みであり、電子署名やタイムスタンプ等がこれに当たる。
	トラストを確保したDX推進サブワーキンググループ報告書	「データ戦略推進ワーキンググループの開催について」（令和３年９月６日デジタル社会推進会議議長決定）第４項の規定に基づき、トラストを確保したデジタルトランスフォーメーションの具体的な推進方策を検討するため、令和３年10月25日、データ戦略推進ワーキンググループの下にサブワーキンググループが設置された。本サブワーキンググループの検討結果、構成員及びオブザーバーからの主要な意見、今後の方向性が報告書としてまとめられている。（2023年２月廃止）
な	内閣サイバーセキュリティセンター	（NISCの項目を参照。）
	ナショナルサート機能	深刻なサイバー攻撃に対し、情報収集・分析から、調査・評価、注意喚起の実施及び対処と、その後の再発防止等の政策立案・措置に至るまでの一連の取組を一体的に推進するための総合的な調整を担う機能。
	ナショナルサイバートレーニングセンター	2017年４月、実践的なサイバートレーニングを企画・推進する組織としてNICTに設置されたもの。
に	日米サイバー対話	サイバー空間を取り巻く諸問題についての日米両政府による包括対話（第１回：2013年５月、第２回：2014年４月、第３回：2015年７月、第４回：2016年７月、第５回：2017年７月、第６回：2018年７月、第７回：2019年10月、第８回：2023年５月）。
	任務保証	企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、このような「任務」を着実に遂行するために必要となる能力及び資産を確保すること。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方。
は	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。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もあるが、本来は悪い意味の言葉ではない。そのような悪意のある行為は、本来はクラッキングという。
	パッチ適用	ソフトウェアにアップデートを配布して適用するプロセス。
	犯罪インフラ	犯罪を助長し、又は容易にする基盤のことを指す。基盤そのものが合法なものであっても、犯罪に悪用されている状態にあれば、これも犯罪インフラに含まれる。

ひ	ビッグデータ	利用者が急激に拡大しているソーシャルメディア内のテキストデータ、携帯電話・スマートフォンに組み込まれたGPS（全地球測位システム）から発生する位置情報、時々刻々と生成されるセンサーデータなど、ボリュームが膨大であるとともに、従来の技術では管理や処理が困難なデータ群。
	標的型攻撃	特定の組織や情報を狙って、機密情報や知的財産、アカウント情報（ID、パスワード）などを窃取又は組織等のシステムを破壊・妨害しようとする攻撃。標的型攻撃の一種として特定のターゲットに対して様々な手法で持続的に攻撃を行うAPT（Advanced Persistent Threat）攻撃がある。
ふ	ファジング	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	実在の金融機関、ショッピングサイトなどを装った電子メールを送付し、これらのホームページとそっくりの偽のサイトに誘導して、銀行口座番号、クレジットカード番号やパスワード、暗証番号などの重要な情報を入力させて詐取する行為のこと。
	フィッシング対策協議会	フィッシングに関する情報収集・提供、注意喚起等の活動を中心とした対策を促進することを目的として、2005年４月28日に設立された協議会。
	不正アクセス	ID・パスワード等により利用が制限・管理されているコンピュータに対し、ネットワークを経由して、正規の手続を経ずに不正に侵入し、利用可能とする行為のこと。
	不正プログラム	情報システムを利用する者が意図しない結果を当該情報システムにもたらすプログラムの総称。
	プラス・セキュリティ知識	経済社会のデジタル化に伴い、企業内外のセキュリティ専門人材との協働を行うに当たって必要となる知識として、時宜に応じてプラスして習得すべき知識。
	ブルートフォース攻撃	パスワードやユーザIDを総当たりで検証する攻撃。
へ	ペネトレーションテスト	情報システムに対する侵入テストのこと。インターネットに接続されている情報システムに疑似的な攻撃を実施することによって、実際に情報システムに侵入できるかどうかの観点から、サイバーセキュリティ対策の状況を検証し、改善のために必要な助言等を行う。
ま	マイナポータル	マイナンバー制度の導入に併せて新たに構築した、国民一人ひとりがアクセスできるポータルサイト。具体的には、自己情報表示機能、情報提供等記録表示機能、お知らせ機能、各種ワンストップサービス等を提供する基盤であり、国民一人ひとりが様々な官民のオンラインサービスを利用できる。また、API連携により、国、地方公共団体及び民間のオンラインサービス間のシームレスな連携を可能にする基盤。
	マイナンバー	日本国内に住民票を有する全ての方が一人につき１つ持つ12桁の番号のこと。外国籍でも住民票を有する方には住所地の市町村長から通知される。マイナンバーは行政を効率化し、国民の利便性を高め、公平、公正な社会を実現するための社会基盤。
	マネジメント監査	サイバーセキュリティ対策を強化するための監査。
	マルウェア	不正かつ有害な動作を行う、悪意を持ったソフトウェア（malicious software）。
ら	ランサムウェア	データを暗号化して身代金を要求するマルウェア。身代金を意味する「ランサム」と、「マルウェア」を組み合わせた造語。ランサムウェアの例として、2017年に世界的に流行した「WannaCry」等がある。
り	リスクアセスメント	サイバーセキュリティの確保のため、状況を想定することで発生が予想される危険源や危険な状態を特定し、その影響の重大さを評価し、それに応じた対策を事前に実施することで、安全性を高めること。
	リスクマネジメント	組織が担う「任務」の内容に応じて、リスクを特定・分析・評価し、リスクを許容し得る程度まで低減する対応をしていくこと。サイバー空間に本質的にある不確実さから、不可避的に導かれる観点。
	量子暗号通信	量子特有の性質（盗聴を確実に検知可能）を用いた暗号通信。
れ	レジリエンス	サイバーインシデントが発生した際に、その影響を最小化し、早急に元の状態に戻す仕組みや能力、耐性のこと。