令和６年度

中小企業サイバーセキュリティ

社内体制整備事業

第９編　組織として実践するためのスキル・知識と人材育成　【レベル共通】

第22章. サイバーセキュリティ対策を実践するための知識とスキル

章の目的
技術進歩に伴い次々と新しい脅威が生まれている中で、効果的で漏れのないセキュリティ対策を実践していくためには、IT 全般のスキルや知識を持つ人材の育成と確保が重要です。第 22 章では、各種スキル標準のフレームワークをもとに、必要とされる新しいスキルや知識について、体系的に理解することを目的とします。
主な達成目標
◘ 具体的な実施のために必要となる「役割やタスク」「スキルや知識」について、人材育成・人材確保のための各種スキル標準のフレームワークをもとに体系的に理解すること。 ◘ 各種スキル標準のフレームワークをもとに、サイバーセキュリティ対策を実践するために必要なスキルや知識について体系的に理解すること。 ◘ スキルや知識の認定制度と活用方法を理解すること。

22-1. デジタルスキル標準（DSS）

デジタルスキル標準は「DX リテラシー標準」と「DX 推進スキル標準」の 2 つの標準で構成されます。「DX リテラシー標準」は、すべてのビジネスパーソンに向けた指針およびそれに応じた学習項目例を定義しています。「DX 推進スキル標準」は、DX を推進する人材の役割（ロール）および必要なスキルを定義しています。

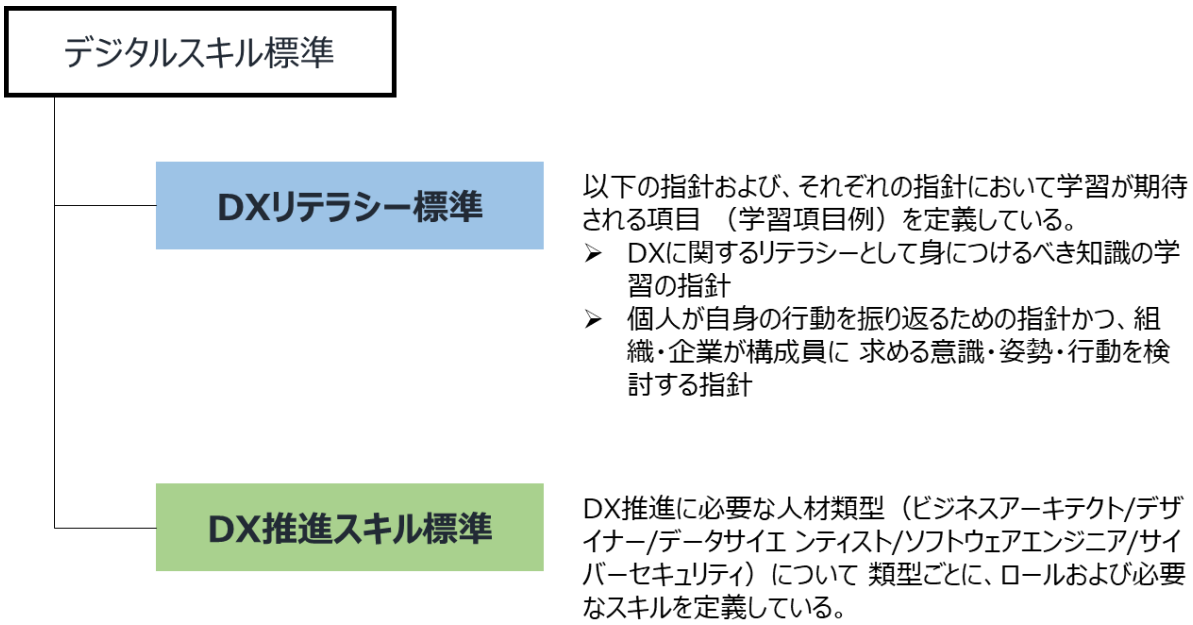


図 85. デジタルスキル標準の構成

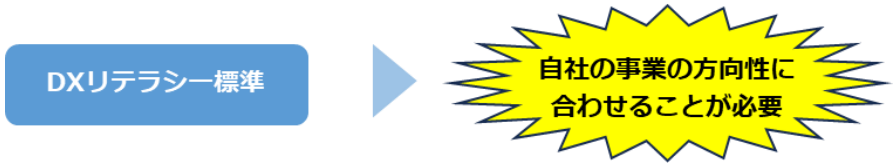
(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

詳細理解のため参考となる文献（参考文献）	
デジタルスキル標準 ver.1.2	https://www.ipa.go.jp/jinzai/skill-standard/dss/ps6vr700000083ki-att/000106872.pdf

22-1-1. DX リテラシー標準（DSS-L）

「DX リテラシー標準」は、すべてのビジネスパーソンが身につけるべきデジタルトランスフォーメーション（DX）に関する基礎的な知識、スキル、マインドセットの学習指針です。企業は、従業員に対して、DX に関するリテラシーを身につけさせるための指針として活用できます。

DX リテラシー標準は、特定の産業や職種、部署などに依存しない汎用性を重視して作成されています。そのため、企業や組織がこれを適用する際には、自身が属する産業や事業の方向性に合わせる必要があります。



DX リテラシー標準は、「標準策定のねらい」「マインド・スタンス」「Why（DX の背景）」「What（DX で活用されるデータ・技術）」「How（データ・技術の利活用方法）」で構成されています。

急速に普及する生成 AI は、各企業における DX の進展を加速させると考えられ、企業の競争力を向上させる可能性があります。あわせて、ビジネスパーソンに求められるスキルも変化し、より重要になる部分もあると想定されます。DX リテラシー標準は上記の状況に対応するため、令和 5 年 8 月に改訂されました。改訂箇所は、下記の図の太文字と下線で示した箇所です。

標準策定のねらい

ビジネスパーソン一人一人がDXに関するリテラシーを
身につけることで、DXを自分事ととらえ、変革に向けて行動できるようになる

Why（DXの背景）

産官学で生成AIの利用が進んでおり、社会環境へ影響を与える可能性があるため、**「社会の変化」**に**人材育成・教育や労働市場の変化等の学習項目例を追加**

What（DXで活用されるデータ・技術）

- ✓ 生成AIは、ビジネスの場で急速に普及・利用されているため、**「AI」**に**生成AIの技術動向や倫理等の学習項目例を追加**
- ✓ 現在の利用状況に鑑み**「ネットワーク」**に**ネットワークの種類、インターネットサービスの学習項目例を追加**
- ✓ 個人や企業等で扱うデータがデジタル技術・サービスに活用されるため、**「データを扱う」**に**活用しやすいデータの入力や整備の手法などの内容・学習項目例を追加**
- ✓ 適切でないデータから生み出される結果は、誤った判断・損害につながり得るため、**「データによって判断する」**に**適切なデータを用いて判断することの重要性などの内容・学習項目例を追加**

How（データ・技術の利活用）

- ✓ 生成AIは、ツールなどの基礎知識や指示（プロンプト）の手法を用いて業務の様々な場面で利用できるため、**「データ・デジタル技術の活用事例」**に**生成AIの活用事例、「ツール利用に生成AIツール概要・利用方法などの学習項目例をそれぞれ追加**
- ✓ 情報漏えいや法規制、利用規約などに正しく対処しながら生成AIを利用することが求められるため、**「モラル」**に**データ流出の危機性等、「コンプライアンス」に法規制や利用規約などの学習項目例をそれぞれ追加**

マインド・スタンス

- ✓ 他項目と比べて**より普遍的な要素を定義**しているため、**生成AI利用においても同様に重要**となる
- ✓ 適切なデータを用いることにより、事実に基づく判断が有効になるため、**「事実に基づく判断」**に**適切なデータ入力の重要性や行動例などを追加**
- ✓ **生成AIをビジネスパーソンとしてのスキルと掛け合わせ生産性向上やビジネス変革などへ適切に利用しようとしていること 、生成AI利用における注意点を理解していること 、生成AI の影響に対して変化をいとわず学び続けること**は、今後、全ビジネスパーソンが身に着けるべきマインド・スタンスとして重要性が増すため、**「生成AI利用において求められるマインド・ス タンス」として既存項目と分けて追加**

図 86. DX リテラシー標準の全体像

(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

項目一覧

<table>
<tr><th>Why（DXの背景）</th><th colspan="2">What（DXで活用されるデータ・技術）</th><th colspan="2">How（データ・技術の利活用）</th></tr>
<tr><td rowspan="4">社会の変化
顧客価値の変化
競争環境の変化</td><td rowspan="4">データ</td><td>社会におけるデータ</td><td rowspan="2">活用事例・利用方法</td><td>データ・デジタル技術の活用事例</td></tr>
<tr><td>データを読む・説明する</td><td>ツール利用</td></tr>
<tr><td>データを扱う</td><td rowspan="3">留意点</td><td>セキュリティ</td></tr>
<tr><td>データによって判断する</td><td>モラル</td></tr>
<tr><td rowspan="5">デジタル技術</td><td>AI</td><td>コンプライアンス</td></tr>
<tr><td>クラウド</td><td colspan="2" rowspan="4"></td></tr>
<tr><td>ハードウェア・ソフトウェア</td></tr>
<tr><td>ネットワーク</td></tr>
<tr><td colspan="5">マインド・スタンス</td></tr>
<tr><td>デザイン思考/アジャイルな働き方</td><td>顧客、ユーザへの共感</td><td colspan="2">常識にとらわれない発想</td><td>反復的なアプローチ</td></tr>
<tr><td>新たな価値を生み出す基礎としてのマインド・スタンス</td><td>変化への適応</td><td>コラボレーション</td><td>柔軟な意思決定</td><td>事実に基づく判断</td></tr>
</table>

図 87. DX リテラシー標準の項目一覧

(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

One Point

DX リテラシー標準の学習方法

IPA が運営する「マナビ DX」という、すべての社会人にとって必須であるデジタルスキルを学べるコンテンツを紹介しているポータルサイトがあります。このポータルサイトでは、DX リテラシー標準の各項目ごとに学習できる講座が掲載されており、DX リテラシーを学ぶことができます。

詳細理解のため参考となる文献（参考文献）	
マナビ DX	https://manabi-dx.ipa.go.jp/

マインド・スタンス

学習のゴール

社会変化の中で新たな価値を生み出すために必要なマインド・スタンスを知り、自身の行動を振り返ることができること。

項目の内容・学習項目

項目	内容	学習項目例
変化への適応	✓ 環境や仕事・働き方の変化を受け入れ、適応するために自ら主体的に学んでいる ✓ 自身や組織が持つ既存の価値観について尊重すべき点を認識しつつ、環境変化に応じた新たな価値観、行動様式、知識、スキルを身につけている	✓ 各自が置かれた環境において目指すべき、具体的な行動や影響例など
コラボレーション	✓ 価値創造のためには、さまざまな専門性を持った人と社内・社外問わずに協働することが重要であることを理解し、多様性を尊重している	
顧客・ユーザーへの共感	✓ 顧客・ユーザーに寄り添い、顧客・ユーザーの立場に立ってニーズや課題を発見しようとしている	
常識にとらわれない発想	✓ 顧客・ユーザーのニーズや課題に対応するためのアイデアを、既存の概念・価値観にとらわれずに考えている ✓ 従来の物事の進め方について理由を自ら問い、より良い進め方がないか考えている	
反復的なアプローチ	✓ 新しい取組や改善を、失敗を許容できる範囲の小さいサイクルで行い、顧客・ユーザーのフィードバックを得て反復的に改善している ✓ 失敗したとしてもその都度軌道修正し、学びを得ることができれば「成	

	果」であると認識している	
柔軟な意思決定	✓ 既存の価値観に基づく判断が難しい状況においても、価値創造に向けて必要であれば、臨機応変に意思決定を行っている	
事実に基づく判断	✓ 勘や経験のみではなく、客観的な事実やデータに基づいて、物事を見たり、判断したりしている ✓ 適切なデータを用いることにより、事実やデータに基づく判断が有効になることを理解し、適切なデータの入力を意識して行っている	

(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

Why（DX の背景）

学習のゴール

人々が重視する価値や社会・経済の環境がどのように変化しているか知っており、DX の重要性を理解している

項目の内容・学習項目例

項目	内容	学習項目例
社会の変化	✓ 世界や日本社会に起きている変化を理解し、変化の中で人々の暮らしをよりよくし、社会課題を解決するためにデータやデジタル技術の活用が有用であることを知っている	✓ メガトレンド・社会課題とデジタルによる解決（SDGs など） ✓ 日本と海外における DX の取組の差、社会・産業の変化に関するキーワード（Society5.0、データ駆動型社会など）
顧客価値の変化	✓ 顧客価値の概念を理解し、顧客・ユーザーがデジタル技術の発展によりどのように変わってきたか（情報や製品・サービスへのアクセスの多様化、人それぞれのニーズを満たすことへ	✓ 顧客・ユーザーの行動変化と変化への対応 ✓ 顧客・ユーザーを取り巻くデジタルサービス

	の欲求の高まり）を知っている	
競争環境の変化	✓ データ・デジタル技術の進展や、社会・顧客の変化によって、既存ビジネスにおける競争力の源泉が変わったり、従来の業種や国境の垣根を超えたビジネスが広がったりしていることを知っている	✓ デジタル技術の活用による競争環境変化の具体的事例

（出典）IPA「デジタルスキル標準 ver.1.2」をもとに作成

What（DX で活用されるデータ・技術）

学習のゴール

DX 推進の手段としてのデータやデジタル技術に関する最新の情報を知った上で、その発展の背景への知識を深めることができる

項目の内容・学習項目例

項目	内容	学習項目例
（データ） 社会におけるデータ	✓ 「データ」には数値に加えて、文字・画像・音声などさまざまな種類があることや、それらがどのように蓄積され、社会で活用されているか知っている	✓ データの種類 ✓ 社会におけるデータ活用
（データ） データを読む・説明する	✓ データの分析手法や結果の読み取り方を理解している ✓ データの分析結果の意味合いを見抜き、分析の目的や受け取り手に応じて、適切に説明する方法を理解している	✓ データの分析手法（基礎的な確率・統計の知識） ✓ データを読む（比較方法・重複など） ✓ データを説明する（可視化・分析結果の言語化）
（データ） データを扱う	✓ デジタル技術・サービスに活用しやすいデータの入力や整備の手法を理解している ✓ データ利用には、データ抽出・加工に関するさまざまな手法やデータベースなどの技術が欠かせない場面があることを理解している	✓ データの入力 ✓ データの抽出・加工（クレンジング・集計など） ✓ データの出力 ✓ データベース（データ

		ベースの種類、構造など）
（データ） データによって判断する	✓ 業務・事業の構造、分析の目的を理解し、データを分析・利用するためのアプローチを知っている ✓ 期待していた結果とは異なる分析結果が出たとしても、それ自体が重要な知見となることを理解している ✓ 分析の結果から、経営や業務に対する改善のアクションを見出し、アクションの結果どうなったかモニタリングする手法を理解している ✓ 適切なデータを用いることで、データに基づく判断が有効となることを理解している	✓ データドリブンな判断プロセス ✓ 分析アプローチ設計 ✓ モニタリングの手法
（デジタル技術） AI	✓ AI が生まれた背景や、急速に広まった理由を知っている ✓ AI の仕組みを理解し、AI ができること、できないことを知っている ✓ AI 活用の可能性を理解し、精度を高めるためのポイントを知っている ✓ 組織/社会でよく使われている AI の動向を知っている	✓ AI の歴史 ✓ AI を作るための手法・技術 ✓ AI の得意分野・限界 ✓ 人間中心の AI 社会原則、ELSI ✓ 最新の技術動向（生成 AI など）
（デジタル技術） クラウド	✓ クラウドの仕組みを理解し、クラウドとオンプレミスの違いを知っている ✓ クラウドサービスの提供形態を知っている	✓ クラウドの仕組み（データの持ち方、データを守るで仕組み） ✓ クラウドサービスの提供形態（SaaS、IaaS、PaaS など） ✓ 最新の技術動向
（デジタル技術） ハードウェア・ソフトウェア	✓ コンピュータやスマートフォンなどが動作する仕組みを知っている ✓ 社内システムなどがどのように作られているかを知っている	✓ ハードウェア（ハードウェアの構成要素、コンピュータの種類） ✓ ソフトウェア（ソフトウェアの種類、プログ

		ラミング的思考） ✓ 企業における開発・運用 ✓ 最新の技術動向
（デジタル技術） ネットワーク	✓ ネットワークの基礎的な仕組みを知っている ✓ インターネットの仕組みや代表的なインターネットサービスを知っている	✓ ネットワークの仕組み（LAN・WAN、通信プロトコル） ✓ インターネットサービス（電子メール） ✓ 最新の技術動向

（出典）IPA「デジタルスキル標準 ver.1.2」をもとに作成

How（データ・技術の利活用）

学習のゴール

データ・デジタル技術の活用事例を理解し、その実現のための基本的なツールの利用方法を身につけた上で、留意点などを踏まえて実際に業務で利用できる

項目の内容・学習項目例

項目	内容	学習項目例
（活用事例・利用方法） データ・デジタル技術の活用事例	✓ ビジネスにおけるデータ・デジタル技術の活用事例を知っている ✓ データ・デジタル技術がさまざまな業務で利用できることを理解し、自身の業務への適用場面を想像できる	✓ 事業活動におけるデータ・デジタル技術の活用事例 ✓ 生成 AI の利用事例
（活用事例・利用方法） ツール利用	✓ ツールの利用方法に関する知識を持ち、日々の業務において、状況に合わせて適切なツールを選択できる	✓ 日常業務に関するツールの利用方法 ✓ 生成 AI の利用方法 ✓ 自動化・効率化に関するデジタルツールの利用方法
（留意点） セキュリティ	✓ セキュリティ技術の仕組みと個人が取るべき対策に関する知識を持ち、安心してデータやデジタル技術を利用できる	✓ セキュリティの 3 要素 ✓ セキュリティ技術 ✓ 個人が取るべきセキ

		ユリティ対策
（留意点） モラル	✓ 個人がインターネット上で自由に情報のやり取りができる時代において求められるモラルを持ち、インターネット上で適切にコミュニケーションできる ✓ 捏造、改ざん、盗用などのデータ分析における禁止事項を知り、適切にデータを利用できる ✓ データ流出の危険性や影響を想像できる	✓ ネット被害・SNS・生成 AI などのトラブルの事例・対策 ✓ データ利用における禁止事項・留意事項
（留意点） コンプライアンス	✓ プライバシー、知的財産権、著作権の示すものや、その保護のための法律、諸外国におけるデータ規制などについて知っている ✓ 実際の業務でデータや技術を利用するときに、自身の業務が法規制や利用規約に照らして問題ないか確認できる	✓ 個人情報の定義と個人情報に関する法律・留意事項 ✓ 著作権・産業財産権・その他の権利が保護する対象 ✓ 諸外国におけるデータ規制 ✓ サービス利用規約を踏まえたデータの利用範囲

(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

22-1-2. DX 推進スキル標準（DSS-P）

DX 推進スキル標準は、人材の種類ごとに必要なスキルの重要度をまとめたものです。人材の種類は、5 つの人材類型（ビジネスアーキテクト/デザイナー/データサイエンティスト/ソフトウェアエンジニア/サイバーセキュリティ）と、その下位区分である 15 のロールに区分されています。一方のスキルは、DX を推進する人材に求められる約 50 のスキルが 5 つのカテゴリ・12 のサブカテゴリに分けられています。このスキルの体系は、すべての人材類型・ロールに共通のものになっており、「共通スキルリスト」と呼ばれています。

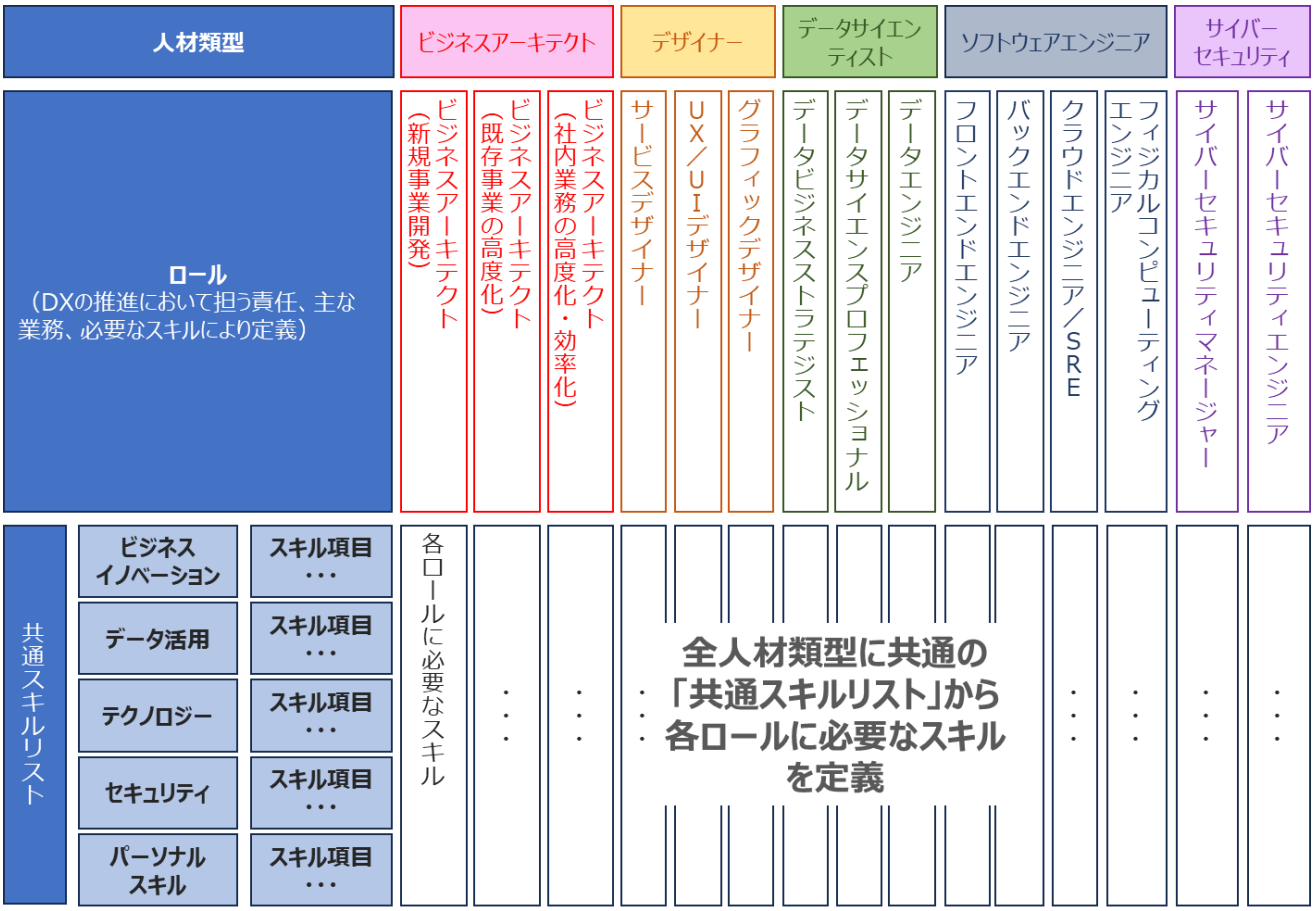


図 88. DX 推進スキル標準の構成

(出典) IPA「デジタルスキル標準 ver1.2」をもとに作成

※５種類の人材類型のうち「サイバーセキュリティ」のみが、人称ではなく対象分野名となっています。

各人材類型のロールと、DX 推進において担う責任は以下の通りです。

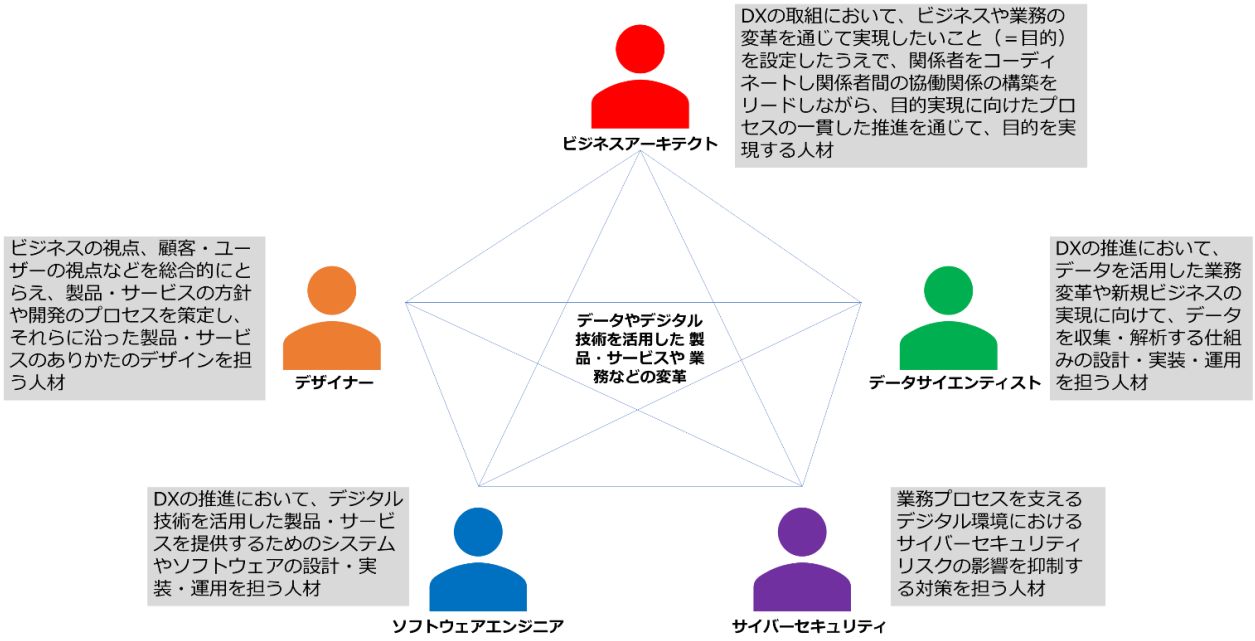


図 89. 人材類型の定義

(出典) IPA「デジタルスキル標準 ver1.2」をもとに作成

人材類型	ロール	DX 推進において担う責任
ビジネスアーキテクト	ビジネスアーキテクト（新規事業開発）	新しい事業、製品・サービスの目的を見出し、新しく定義した目的の実現方法を策定した上で、関係者をコーディネートし関係者間の協働関係の構築をリードしながら、目的実現に向けたプロセスの一貫した推進を通じて、目的を実現する
	ビジネスアーキテクト（既存事業の高度化）	既存の事業、製品・サービスの目的を見直し、再定義した目的の実現方法を策定した上で、関係者をコーディネートし関係者間の協働関係の構築をリードしながら、目的実現に向けたプロセスの一貫した推進を通じて、目的を実現する
	ビジネスアーキテクト（社内業務の高度化・効率化）	社内業務の課題解決の目的を定義し、その目的の実現方法を策定した上で関係者をコーディネートし関係者間の協働関係の構築をリードしながら、目的実現に向けたプロセスの一貫した推進を通じて、目的を実現する
デザイナー	サービスデザイナー	社会、顧客・ユーザー、製品・サービス提供における社内外関係者の課題や行動から顧客価値を定義し製品・サービスの方針（コンセプト）を策定するとともに、それを継続的に実現するための仕組みのデザインを行う
	UX／UI デザイナー	バリュープロポジションに基づき製品・サービスの顧客・ユーザー体験を設計し、製品・サービスの情報設計や、機能、情報の配置、外観、動的要素のデザインを行う
	グラフィックデザイナー	ブランドのイメージを具現化し、ブランドとして統一感のあるデジタルグラフィック、マーケティング媒体などのデザインを行う
データサイエンティスト	データビジネスストラテジスト	事業戦略に沿ったデータの活用戦略を考えるとともに、戦略の具体化や実現を主導し、顧客価値を拡大する業務変革やビジネス創出を実現する
	データサイエンスプロフェッショナル	データの処理や解析を通じて、顧客価値を拡大する業務の変革やビジネスの創出につながる有意義な知見を導出する
	データエンジニア	効果的なデータ分析環境の設計・実装・運用を通じて、顧客価値を拡大する業務変革やビジネス創出を実現する
ソフトウ	フロントエンドエン	デジタル技術を活用したサービスを提供するためのソフト

ェアエンジニア	ジニア	ウェアの機能のうち、主にインターフェース（クライアントサイド）の機能の実現に主たる責任を持つ
	バックエンドエンジニア	デジタル技術を活用したサービスを提供するためのソフトウェアの機能のうち、主にサーバサイドの機能の実現に主たる責任を持つ
	クラウドエンジニア／SRE	デジタル技術を活用したサービスを提供するためのソフトウェアの開発・運用環境の最適化と信頼性の向上に責任を持つ
	フィジカルコンピューティングエンジニア	デジタル技術を活用したサービスを提供するためのソフトウェアの実現において、現実世界（物理領域）のデジタル化を担い、デバイスを含めたソフトウェア機能の実現に責任を持つ
サイバーセキュリティ	サイバーセキュリティマネージャー	顧客価値を拡大するビジネスの企画立案に際して、デジタル活用に伴うサイバーセキュリティリスクを検討・評価するとともに、その影響を抑制するための対策の管理・統制の主導を通じて、顧客価値の高いビジネスへの信頼感向上に貢献する
	サイバーセキュリティエンジニア	事業実施に伴うデジタル活用関連のサイバーセキュリティリスクを抑制するための対策の導入・保守・運用を通じて、顧客価値の高いビジネスの安定的な提供に貢献する

(出典) IPA「デジタルスキル標準 ver1.2」をもとに作成

共通スキルリストの全体像

全人材類型に共通する「共通スキルリスト」は、DX を推進する人材に求められるスキルを 5 つのカテゴリ・12 のサブカテゴリで整理しています。

各カテゴリは 2 つか 3 つのサブカテゴリに分け、1 つ目では主要な活動を、2 つ目以降ではそれを支える要素技術と手法を、大くくりに整理しています。

カテゴリ	サブカテゴリ	スキル項目
ビジネス変革	戦略・マネジメント・システム	ビジネス戦略策定・実行
		プロダクトマネジメント
		変革マネジメント
		システムズエンジニアリング
		エンタープライズアーキテクチャ
		プロジェクトマネジメント

	ビジネス・モデル・プロセス	ビジネス調査
		ビジネスモデル設計
		ビジネスアナリシス
		検証（ビジネス視点）
		マーケティング
		ブランディング
	デザイン	顧客・ユーザー理解
		価値発見・定義
		設計
		検証（顧客・ユーザー視点）
		そのほかデザイン技術
データ活用	データ・AI の戦略的活用	データ理解・活用
		データ・AI 活用戦略
		データ・AI 活用業務の設計・事業実装・評価
	AI・データサイエンス	数理統計・多変量解析・データ可視化
		機械学習・深層学習
	データエンジニアリング	データ活用基盤設計
		データ活用基盤実装・運用
テクノロジー	ソフトウェア開発	コンピュータサイエンス
		チーム開発
		ソフトウェア設計手法
		ソフトウェア開発プロセス
		Web アプリケーション基本技術
		フロントエンドシステム開発
		クラウドインフラ活用
		SRE プロセス
		サービス活用
	デジタルテクノロジー	フィジカルコンピューティング
		そのほか先端技術
		テクノロジートレンド
セキュリティ	セキュリティマネジメント	セキュリティ体制構築・運営
		セキュリティマネジメント
		インシデント対応と事業継続

		プライバシー保護
	セキュリティ技術	セキュア設計・開発・構築
		セキュリティ運用・保守・監視
パーソナルスキル	ヒューマンスキル	リーダーシップ
		コラボレーション
	コンセプチュアルスキル	ゴール設定
		創造的な問題解決
		批判的思考
		適応力

(出典) IPA「デジタルスキル標準 ver1.2」をもとに作成

例として、セキュリティカテゴリの詳細を説明します。

カテゴリ	サブカテゴリ	スキル項目	内容	学習項目例
セキュリティ	セキュリティマネジメント	セキュリティ体制構築・運営	• セキュリティ対策を実施する体制の構築とその維持運営（要員の確保・育成を含む）を円滑に行うためのスキル • 組織としてのセキュリティカルチャーを企業内で醸成する活動を行うためのスキル	• セキュリティ対応組織（セキュリティ統括機能、SOC、xSIRTなど）との連携手順 • サービスや機器のセキュリティ対策に関する組織内の役割と責任の明確化 • 組織におけるセキュリティカルチャーの醸成方法
		セキュリティマネジメント	• 情報、サイバー空間、OT/IoT 環境などのセキュリティマネジメントのプロセスを組織として適切に実施するためのスキル	• セキュリティ関連法制度 • ポリシー、規程、マニュアルなどの整備 • 脅威インテリジェンスの活用を含むリスクの認知 • リスクアセスメント手法

				• セキュリティ要件定義、機能要件としてのセキュリティ機能 • 認証方式の種類・特徴と選定方法 • 情報資産管理、構成管理 • セキュリティ教育・トレーニングと資格・認証制度 • 情報セキュリティ監査の手法
		インシデント対応と事業継続	• 各種リスク（サイバー攻撃、過失、内部不正、災害、障害など）がデジタル利活用におけるセキュリティインシデントとして顕在化した際の影響を抑制し、事業継続を可能とするためのスキル	• デジタル利活用における事業継続 • 事業継続計画の整備と訓練 • インシデント対応と危機管理の連携手順 • 日常および緊急時の情報共有とコミュニケーション
		プライバシー保護	• パーソナルデータ等のプライバシー情報の保護に求められる要件の理解とその実践に関するスキル	• セキュアシステム設計の概要と実践方法 • DevSecOps の考え方と実践方法 • セキュリティ要件およびセキュリティ機能の実現・実装 • IT/OT/IoT デバイスにおけるセキュリティ対策 • クラウドサービスおよびネットワーク機器のセキュリティ機能の概要と設定 • 脆弱性の概念と対策・診断方法
	セキュリティ技	セキュア設計・開発・構築	• デジタルサービス・製品の企画設計を行う際に、サイバー攻撃や各種不正の影響を受けにくくするために遵守すべき基準や要件をもとに設計・開発・構築を行うスキル	• セキュアシステム設計の概要と実践方法 • DevSecOps の考え方と実践方法 • セキュリティ要件およびセキュリティ機能の実現・実装 • IT/OT/IoT デバイスにおけるセ

	術		• デジタルサービス・製品の脆弱性について理解し、診断を適切に実践（委託による実施を含む）するためのスキル	キュリティ対策 • クラウドサービスおよびネットワーク機器のセキュリティ機能の概要と設定 • 脆弱性の概念と対策・診断方法
		セキュリティ運用・保守・監視	• デジタルサービスをセキュアに運用するための保守と対策を適切に実践するためのスキル • セキュリティに関する監視とインシデントの原因究明などを適切に実践するためのスキル	• 脅威情報や脆弱性情報の活用 • モニタリングの方法と観測データの活用 • 運用・監視業務への AI 応用 • インシデント時の影響調査、トリアージ方法 • デジタルフォレンジックサービスの活用

(出典) IPA「デジタルスキル標準 ver1.2」をもとに作成

生成 AI に関する事項

DX を推進するには、新たに登場するデジタル技術がもたらす変化を捉え、それに対応していくことが重要です。ここでは、生成 AI を例にして、DX を推進する人材に求められる新技術への向き合い方、行動の起こし方などを説明します。

急速に進歩・普及する生成 AI は、各企業における DX を加速すると考えられ、企業の競争力に大きな影響を与える可能性があります。生成 AI の活用によって、新規事業の開発、知的労働や知的労働を伴う肉体労働の生産性向上などが期待できる一方、生成 AI 活用による権利侵害・情報漏えい、倫理的な問題などが発生しないよう十分に注意を払う必要があります。

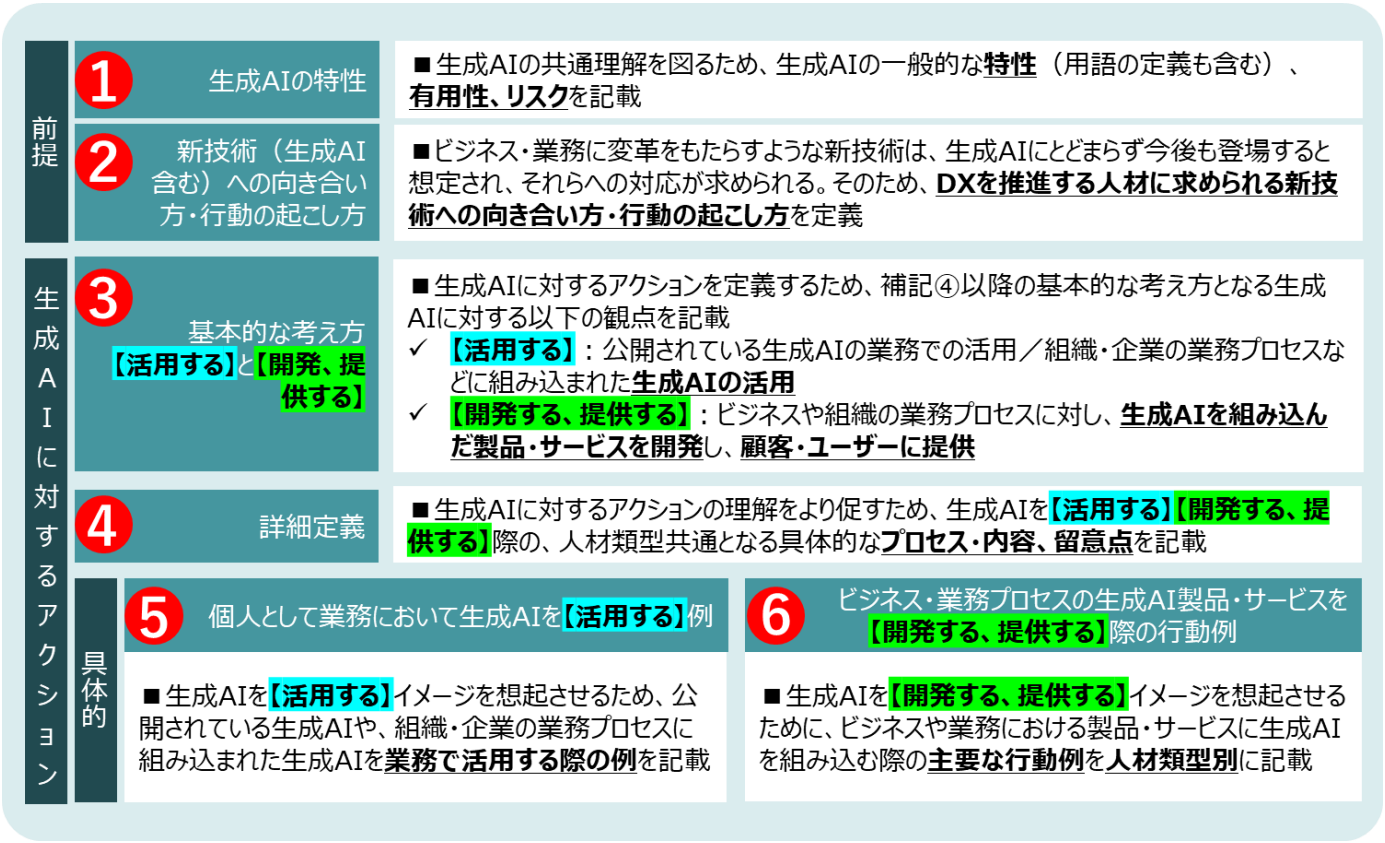


図 90. 生成 AI に関する DX 推進スキル標準

(出典) IPA「生成 AI に関する DX 推進スキル標準の改訂 要旨（2024 年 7 月）」をもとに作成

22-2. IT スキル標準（ITSS）

22-2-1. 概要

IT スキル標準（ITSS）は、IT 分野で必要とされるスキルや知識を体系化し、評価するための指標です。経済産業省が 2002 年に策定し、現在は IPA が管理しています。ITSS は、IT 人材の育成に寄与することを目的としており、企業が共通して使用できるスキル指標を提供することで、キャリアパスの明確化やスキルの標準化に役立っています。

IT スキル標準の全体構成

IT スキル標準は、3 部で構成されます。全体構成の決定に際しては、国際規格や JIS 規格などの様式、記述方法を参考にしています。

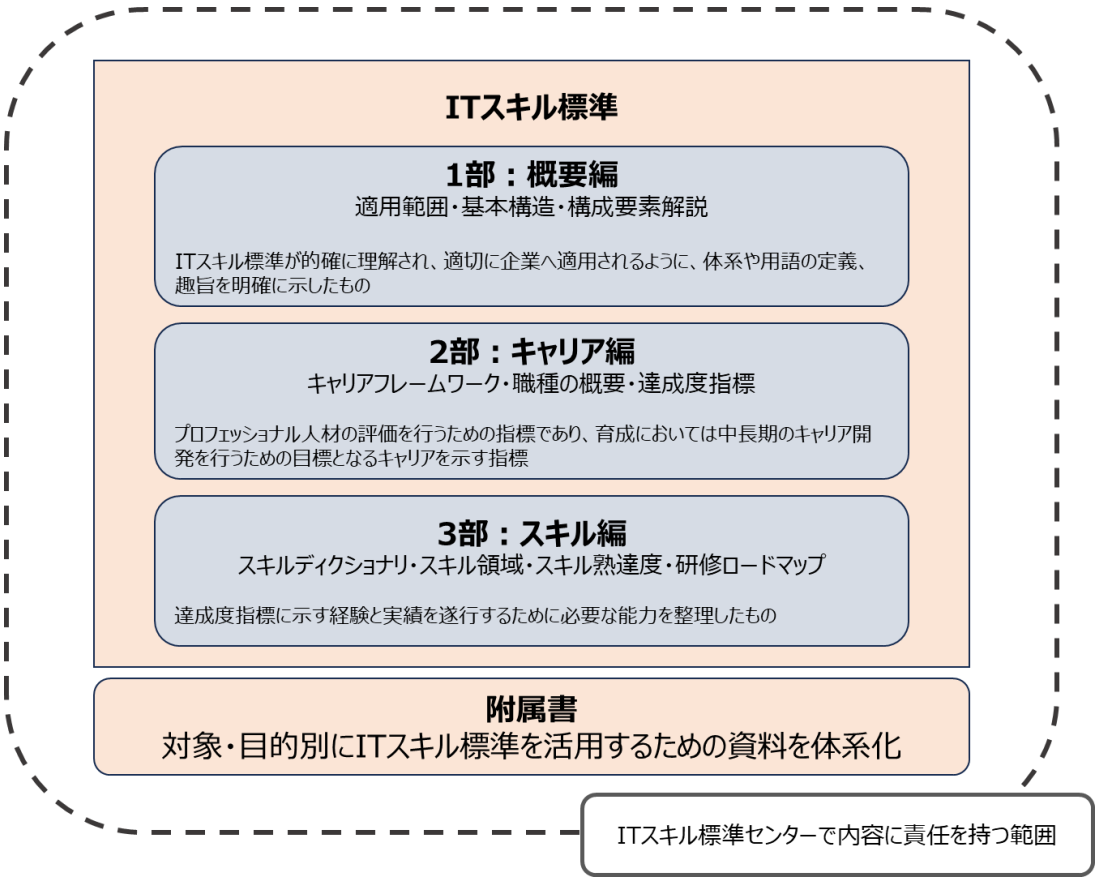


図 91. IT スキル標準の全体構造

(出典) IPA「デジタルスキル標準」をもとに作成

詳細理解のため参考となる文献（参考文献）	
デジタルスキル標準 ver.1.2	https://www.ipa.go.jp/jinzai/skill-standard/dss/ps6vr700000083ki-att/000106872.pdf
IT スキル標準 V3 2011　1 部：概要編	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024840.pdf

22-2-2. キャリア

「２部：キャリア編」では、IT スキル標準の構成要素である「キャリアフレームワーク」、「職種の概要」、「達成度指標」を収めています。IT 人材のレベル評価は、経験と実績に基づく「達成度指標」によって行うことが IT スキル標準の特色です。キャリアフレームワークは横軸に職種区分、縦軸にレベル設定があり、11 の職種と 35 の専門分野を設けています。また、それぞれの専門分野に対応して、各個人の能力や実績に基づく 7 段階の達成レベルを規定しています。キャリア編で定義したのは、プロフェッショナル人材の評価を行うための指標であり、育成においては中長期のキャリア開発を行うための目標となるキャリアを示す指標です。

キャリアフレームワークの職種と専門分野

職種	専門分野
マーケティング	マーケティングマネジメント
	販売チャネル戦略
	マーケットコミュニケーション
セールス	訪問型コンサルティングサービス
	訪問型製品セールス
	メディア利用型セールス
コンサルタント	インダストリ
	ビジネスファンクション
IT アーキテクト	アプリケーションアーキテクチャ
	インテグレーションアーキテクチャ
	インフラストラクチャアーキテクチャ
プロジェクトマネジメント	システム開発
	IT アウトソーシング
	ネットワークサービス
	ソフトウェア製品開発
IT スペシャリスト	プラットフォーム
	ネットワーク
	データベース
	アプリケーション共通基盤
	システム管理
	セキュリティ
アプリケーションスペシャリスト	業務システム
	業務パッケージ

ソフトウェアデベロップメント	基本ソフト
	ミドルソフト
	応用ソフト
カスタマーサービス	ハードウェア
	ソフトウェア
	ファシリティマネジメント
IT サービスマネジメント	運用管理
	システム管理
	オペレーション
	サービスデスク
エデュケーション	研修企画
	インストラクション

(出典) IPA「ＩＴスキル標準Ｖ３ 2011 ２部：キャリア編」をもとに作成

各職種の概要

職種	概要
マーケティング	顧客ニーズに対応するために、企業、事業、製品およびサービスの市場の動向を予測かつ分析し、事業戦略、販売戦略、実行計画、資金計画および販売チャネル戦略などビジネス戦略の企画および立案を実施する。市場分析などを通じて立案したビジネス戦略の投資効果、新規性、顧客満足度に責任を持つ。
セールス	顧客における経営方針を確認し、その実現のための課題解決策の提案、ビジネスプロセス改善支援およびソリューション、製品、サービスの提案を実施し成約する。顧客との良好なリレーションを確立し顧客満足度を高める。
コンサルタント	知的資産、コンサルティングメソドロジを活用し、顧客の経営戦略やビジネス戦略および IT 戦略策定へのカウンセリング、提言、助言の実施を通じて、顧客のビジネス戦略やビジョンの実現、課題解決に貢献し、IT 投資の経営判断を支援する。提言がもたらす価値や効果、顧客満足度、実現可能性などに責任を持つ。
IT アーキテクト	ビジネスおよび IT 上の課題を分析し、ソリューションを構成する情報システム化要件として再構成する。ハードウ

	ェア、ソフトウェア関連技術（アプリケーション関連技術、メソドロジ）を活用し、顧客のビジネス戦略を実現するために情報システム全体の品質（整合性、一貫性など）を保った IT アーキテクチャを設計する。設計したアーキテクチャが課題に対するソリューションを構成することを確認するとともに、後続の開発、導入が可能であることを確認する。また、ソリューションを構成するために情報システムが満たすべき基準を明らかにする。さらに実現性に対する技術リスクについて事前に影響を評価する。
プロジェクトマネジメント	プロジェクトマネジメント関連技術、ビジネスマネジメント技術を活用し、プロジェクトの提案、立上げ、計画、実行、監視コントロール、終結を実施し、計画された納入物、サービスと、その要求品質、コスト、納期に責任を持つ。
IT スペシャリスト	ハードウェア、ソフトウェア関連の専門技術を活用し、顧客の環境に最適なシステム基盤の設計、構築、導入を実施する。構築したシステム基盤の非機能要件（性能、回復性、可用性など）に責任を持つ。
アプリケーションスペシャリスト	業種固有業務や汎用業務において、アプリケーション開発やパッケージ導入に関する専門技術を活用し、業務上の課題解決に関わるアプリケーションの設計、開発、構築、導入、テストおよび保守を実施する。構築したアプリケーションの品質（機能性、回復性、利便性など）に責任を持つ。
ソフトウェアデベロップメント	ソフトウェアエンジニアリング技術を活用し、マーケティング戦略に基づく、市場に受け入れられるソフトウェア製品の企画、仕様決定、設計、開発を実施する。また上位レベルにおいては、ソフトウェア製品に関連したビジネス戦略の立案やコンサルテーションを実施する。開発したソフトウェア製品の機能性、信頼性などに責任を持つ。
カスタマーサービス	ハードウェア、ソフトウェアに関連する専門技術を活用し、顧客の環境に最適なシステム基盤に合致したハードウェア、ソフトウェアの導入、カスタマイズ、保守（遠隔保守含む）、修理を実施するとともに、顧客のシステム基盤

	管理およびサポートを実施する。また IT 施設インフラの設計、構築、導入および管理、運営を実施する。導入したハードウェア、ソフトウェアの品質（使用性、保守容易性など）に責任を持つ。
IT サービスマネジメント	システム運用関連技術を活用し、サービスレベルの設計を行い顧客と合意されたサービスレベルアグリーメント（SLA）に基づき、システム運用リスク管理の側面からシステム全体の安定稼動に責任を持つ。システム全体の安定稼動を目指し、安全性、信頼性、効率性を追及する。またサービスレベルの維持、向上を図るためにシステム稼動情報の収集と分析を実施し、システム基盤管理も含めた運用管理を行う。
エデュケーション	担当分野の専門技術と研修に関連する専門技術を活用し、ユーザーのスキル開発要件に合致した研修カリキュラムや研修コースのニーズの分析、設計、開発、運営、評価を実施する。
共通（レベル 1、2）	担当業務の技術領域に関する基本知識を活用し、上位者の指示の下、あるいは既存の作業標準やガイダンスにしたがい、要求された作業を実施する。自らの担当作業に対する実施責任を持つ。

(出典) IPA「ＩＴスキル標準Ｖ３ 2011 2部：キャリア編」をもとに作成

達成度指標

達成度指標は、実務能力のレベル評価指標として定義したものです。IT スキル標準では、IT 人材のレベル評価は、経験と実績に基づく「達成度指標」によって行います。達成度指標は、ビジネスを成功させる人材を評価する 2 つの貢献に焦点を当てています。「ビジネス貢献」とは、プロジェクトの成功の経験と実績など、ビジネス成果に対する貢献を示します。「プロフェッショナル貢献」とは、専門技術の向上による社内外への貢献、さらに後進育成や技術の継承といったプロフェッショナルとしての貢献を示します。

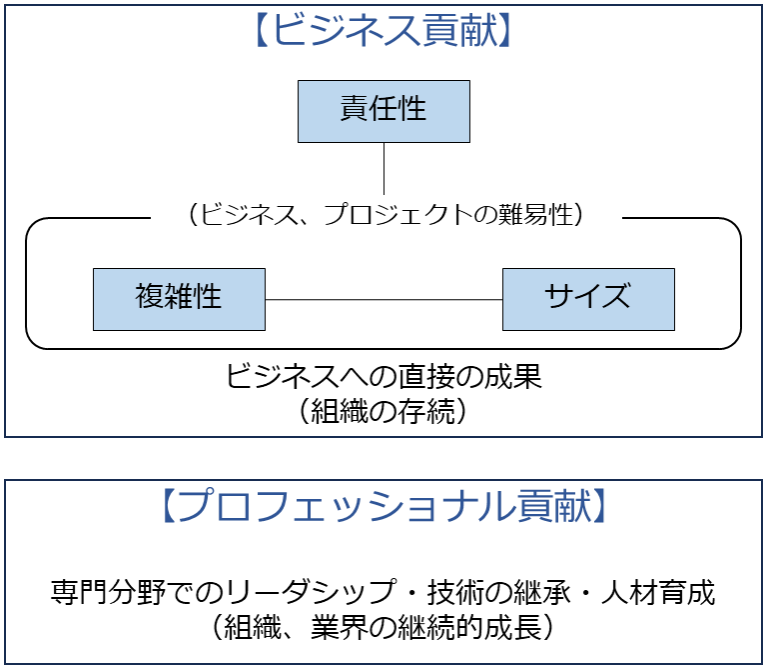


図 92. 達成度指標の構造

(出典) IPA「ＩＴスキル標準Ｖ３ 2011 ２部：キャリア編」をもとに作成

レベル＼要素	ビジネス貢献		プロフェッショナル貢献			
	責任性	実績回数	専門性の発揮度	技術の継承実績		後進育成
7	チームの責任者として他をリード	3 回以上	専門領域に関して他を指導できる高度な専門性保有し、業界をリードしている	5 項以上	☐ 学会、委員会などプロフェッショナルコミュニティ活動 ☐ 著書 ☐ 社外論文掲載 ☐ 社内論文掲載 ☐ 社外講師 ☐ 社内講師 ☐ 特許出願	必須
6		3 回以上	専門領域に関して他を指導できる高度な専門性保有し、業界に貢献している	4 項以上		
5		3 回以上	専門領域に関して他を指導できる高度な専門性保有し、社内に貢献している	3 項以上		
4	チームのリーダー	2 回以上	専門領域に関して高度の専門性保有し、後進を指導している	1 項以上		
3	メンバー	1 回以上	専門領域に関して専門性を保有し、独力で実践している	-		-
2			専門性を踏まえて活動を実施			
1						

(出典) IPA「ＩＴスキル標準Ｖ３ 2011 ２部：キャリア編」をもとに作成

IT スキル標準では、ビジネス貢献とプロフェッショナル貢献の両方が重視されています。IT 人材は、ビジネス貢献、およびプロフェッショナル貢献という達成度指標で定められた基準を同時に満たしていることが必要です。

詳細理解のため参考となる文献（参考文献）	
IT スキル標準 V3 2011　2部：キャリア編	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024842.pdf

22-2-3. スキル

「3 部：スキル編」では、IT スキル標準で定義されているすべてのスキル項目、知識項目を網羅した「スキルディクショナリ」、職種ごとにスキル項目、知識項目を整理した「スキル領域」と「スキル熟達度」、および IT スキル標準に対応して習得すべき研修科目を職種ごとに明示した「研修ロードマップ」を収めています。スキル編は、達成度指標に示す経験と実績を遂行するために必要な能力を整理したものであり、教育や訓練の設計を行う際の指標として活用するものです。

以下の表は、各職種に求められるスキルの中からセキュリティに関連するスキルを抜き出したものです。

各職種に求められるセキュリティに関するスキル	
全職種共通	● プロジェクト・リスク・マネジメント
マーケティング	● 関連法規に関する知識
セールス	● 最新技術動向
コンサルタント	● ビジネスモデルのリスクコントロールの評価 ● 最新ソリューションの動向 ● 情報技術動向の調査
IT アーキテクト	● 関連技術（IT）動向の把握 ● 統合要件の定義 ● インフラストラクチャ要件（主に非機能要件）の定義 ● インフラストラクチャアーキテクチャ設計
プロジェクトマネジメント	● ソフトウェアエンジニアリング ● 最新技術動向 ● セキュリティシステムの実装・検査 ● ネットワーク技術の理解と応用 ● ネットワークシステムの運用、保守、管理 ● リスク・マネジメント計画 ● リスク識別

	● 定性的リスク分析 ● 定量的リスク分析 ● リスク対応計画 ● リスクの監視コントロール
IT スペシャリスト	● 最新技術動向 ● ネットワーク技術の理解と応用 ● インターネット技術 ● セキュリティと個人情報 ● IT 基盤構築プロセス ● システム非機能要件基礎 ● コンプライアンスと法規 ● プラットフォーム要件定義手法 ● プラットフォーム設計手法 ● ネットワークシステムの運用・保守・管理 ● 物理データベースの設計技術 ● データベース関連製品の利用技術 ● データベース開発における重要技術 ● アプリケーション共通基盤要件定義手法 ● アプリケーション共通基盤設計手法 ● セキュリティ方針の策定 ● セキュリティ対策基準の策定 ● セキュリティシステムの計画策定 ● セキュリティシステムの要件定義 ● セキュリティシステムの設計 ● セキュリティシステムの実装・検査 ● セキュリティシステム導入支援 ● セキュリティシステムの運用管理 ● セキュリティ障害（事件事故／インシデント）管理 ● セキュリティの分析 ● セキュリティの見直し（セキュリティシステムの評価と改善） ● 情報セキュリティ監査の実施・支援 ● セキュリティシステムの実装・検査 ● 業界固有のセキュリティ要件・事例 ● コンサルティングの実施 ● セキュリティ技術動向

	● セキュリティと個人情報 ● コンピュータ・フォレンジック（証拠保全追跡）
アプリケーションスペシャリスト	● 最新技術動向 ● ネットワーク技術の理解と応用 ● インターネット技術 ● システム管理手法 ● データベース開発における重要技術 ● アプリケーションセキュリティ ● セキュリティ技術の理解と応用 ● セキュリティ技術動向 ● セキュリティシステムの実装、検査 ● セキュリティとプライバシー
ソフトウェアデベロップメント	● セキュリティシステムの実践、検査 ● セキュリティとプライバシー ● 最新技術動向 ● ネットワーク技術の理解と応用 ● インターネット技術 ● アプリケーションセキュリティ ● 適合すべき標準の選定 ● リスク管理基礎
カスタマーサービス	● 最新技術動向 ● インターネット技術 ● セキュリティとプライバシー ● ネットワーク技術の理解と応用 ● 関連国際標準および関連規格 ● お客様サポート ● 改善提案 ● ストレージ技術 ● データベース技術 ● セキュリティ技術 ● メンテナンスの準備 ● セキュリティ管理
IT サービスマネジメント	● 基準と標準 ● 人材育成

	● 資産管理 ● セキュリティとプライバシー ● システム運用管理手法 ● リスク管理 ● セキュリティ管理 ● インシデント管理 ● 問題管理 ● 変更管理 ● リリース情報 ● 構成管理 ● ネットワークシステム管理 ● セキュリティ技術 ● 最新セキュリティ情報の収集
エデュケーション	● 最新技術動向

(出典) IPA「IT スキル標準 V3 2011 スキルディクショナリ_20120326」をもとに作成

詳細理解のため参考となる文献（参考文献）	
ＩＴスキル標準Ｖ３ 2011 ３部：スキル編	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024844.pdf
IT スキル標準 V3 2011 スキルディクショナリ_20120326	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024846.pdf

22-3. ITSS+（プラス）

ITSS+は、従来の IT スキル標準（ITSS）を拡張し、第 4 次産業革命に向けて求められる新たな領域の新しいスキルをカバーするために策定されました。対象となっている領域は、「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」の 4 つの領域です。

詳細理解のため参考となる文献（参考文献）	
ITSS+（プラス）概要	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/about.html

22-3-1. データサイエンス領域

ITSS+（プラス）の「データサイエンス領域」は、企業などの業務において大量データを分析し、その分析結果を活用するための一連のタスクとそのために習得しておくべきスキルを取りまとめたものです。

タスクは、IPA と「一般社団法人データサイエンティスト協会」スキル定義委員会が協力して策定、見直しを行っています。

スキルは同協会が公開している「スキルチェックリスト」を活用しています。

スキルカテゴリー覧

スキルカテゴリー覧			
データサイエンス力	基礎数学	データエンジニアリング力	環境構築
	データの理解・検証		データ収集
	意味合いの抽出・洞察		データ構造
	予測		データ蓄積
	推定・検定		データ加工
	グルーピング		データ共有
	性質・関係性の把握		プログラミング
	サンプリング		IT セキュリティ
	データ加工		AI システム運用
	データ可視化	ビジネス力	行動規範
	時系列分析		契約・権利保護
	学習		論理的思考
	自然言語処理		着想・デザイン
	画像・映像認識		課題の定義
	音声認識		アプローチ設計

	パターン発見		データ理解
	シミュレーション・データ同化		分析評価
	最適化		事業への実装
			PJ マネジメント
			組織マネジメント

(出典) IPA「データサイエンティスト　スキルチェックリスト　Ver5.00」をもとに作成

データサイエンティストに必要とされるセキュリティに関するスキル（抜粋）

分野	スキルカテゴリ	サブカテゴリ	内容
ビジネス力	行動規範	コンプライアンス	個人情報の扱いに関する法令、そのほかのプライバシーの問題、依頼元との契約約款に基づき、明示されていない項目についても仮名化/匿名化すべきデータを選別できる（名寄せにより個人を特定できるもの、依頼元がデータ処理の結果をどのように保持し利用するのかなどの考慮）
	着想・デザイン	デザイン	プライバシー・バイ・デザインやデータガバナンスの考え方を理解した上で、UI 専門家などと協議し、同意取得やプライバシーに配慮したデータ取得設計ができる
	アプローチ設計	アプローチ設計	データの機密度を考慮した上で、内外の AI サービスに対する活用可否を判断し、入出力データの配置先（クラウドストレージへの配置可否や、社内オンプレ環境におけるセキュリティレベルなど）を設計できる
データエンジニアリング力	IT セキュリティ	基礎知識	セキュリティの 3 要素（機密性、完全性、可用性）について具体的な事例を用いて説明できる
		プライバシー	ハッシュ化、マスキング、k-匿名化、差分プライバシーなどのプライバシー保護の仕組みを理解し適用できる
		攻撃と防御手法	マルウェアなどによる深刻なリスクの種類（消失・漏えい・サービスの停止など）を理解している
			OS、ネットワーク、アプリケーション、データなどの各レイヤーに対して、ユーザーごとのアクセスレベルを設定する必要性を理解している
			DoS 攻撃、不正アクセス、マルウェア感染や内部不正などのセキュリティインシデントが発覚した場合に既存のルールに

			基づき対応できる
			OS、ネットワーク、アプリケーション、データに対するユーザーごとのアクセスレベルを設計できる
			SQL インジェクションやバッファオーバーフロー攻撃の概要を理解し、防止する対策を判断できる
			なりすまし、改ざん、盗聴などのセキュリティ侵害を防御するための対策とセキュリティポリシーを設計し実践できる
			侵入検知システム（IDS）やファイアウォール、エンドポイント対策（EPP/EDR）などを用いて、外部からの不正アクセスを検知、防御、内部侵入後の対策を行う環境を設計できる
			不正メールの検出、不正通信トラフィックの自動遮断、ログからの不正検知など AI を活用したサイバー攻撃などに対する防御ソリューションの有用性と誤検出などのリスクを評価し導入を判断できる
		暗号化技術	暗号化されていないデータは、不正取得された際に容易に不正利用されるおそれがあることを理解し、データの機密度合いに応じてソフトウェアを使用した暗号化と復号ができる
			なりすましや改ざんされた文書でないことを証明するために、電子署名が用いられることを理解している
			公開鍵暗号化方式において、受信者の公開鍵で暗号化されたデータを復号化するためには受信者の秘密鍵が必要であることを知っている
			ハッシュ関数を用いて、データの改ざんを検出できる
			SSH や SSL/TLS などのセキュアプロトコルの概要と必要性を説明できる
		認証	OAuth に対応したデータ提供サービスに対して、認可サーバから取得したアクセストークンを付与してデータ取得用の REST API を呼び出すことができる
			Kerberos 認証と Radius 認証の違いを理解し、それぞれの認証の特徴やユースケースを説明できる
			SAML や OpenID Connect を用いて一度のログインで複数の Web アプリケーションのログイン認証を連携するシングルサインオンの仕組みを設計できる
		ブロックチェ	ブロックチェーン技術を用いてストレージに蓄積されたデー

		ーン	タの安全性と品質を保証するシステムを設計できる
		ゼロトラスト	ゼロトラストの概念を理解し、クラウド利用やリモートワークに対応した情報セキュリティの担保と、データ活用の利便性を両立させる環境をサービスを利用して実装できる

(出典) IPA「データサイエンティスト　スキルチェックリスト　Ver5.00」をもとに作成

詳細理解のため参考となる文献（参考文献）	
データサイエンティスト　スキルチェックリスト　Ver5.00	https://www.datascientist.or.jp/common/docs/skillcheck_ver5.00_simple.xlsx
データサイエンティストのためのスキルチェックリスト／タスクリスト概説	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001ity-att/000083733.pdf

22-3-2. アジャイル領域

ITSS+（プラス）の「アジャイル領域」は、アジャイル開発手法に関するスキルを強化するために設けられた領域です。アジャイル開発は、ソフトウェア開発において変化する要件に柔軟に対応し、顧客満足度の高いサービスを迅速かつ継続的に提供する手法の一つです。重要なのは、関係者全員が自律的に考え、ユーザー価値とビジネス価値の最大化を目指して改善を続けることです。スクラム、XP などさまざまな方法論がありますが、重要なのは仮説検証を繰り返し、失敗から学ぶ姿勢にあります。

「アジャイル領域へのスキル変革の指針」は、アジャイル開発の経験が浅い人や非開発者向けに、アジャイルの背景や必要な学びを説明しています。アジャイル開発の成功には、経営層や事業部門の協力が不可欠です。経営層や事業部門もアジャイルの考え方を理解し、開発に深く関わることが重要です。アジャイル開発に関しては IPA からさまざまなドキュメントを公開されていますが、スキル強化のためには、「アジャイル領域」へのスキル変革の指針として公開されている以下の資料が参考になります。

各資料の概要と想定する読者

①「なぜ、いまアジャイルが必要か？」

-概要：Society5.0 時代になぜアジャイルが必要かを理解します。

Society5.0 時代に直面する問題と従来の問題との違いを踏まえ、いまの時代の問題の解法としてアジャイルが適していることを説明しています。

②「アジャイルソフトウェア開発宣言の読みとき方」

-概要:アジャイル開発のベースにあるマインドセットや原則について理解します。

「アジャイルソフトウェア開発宣言」にある「4 つの価値」と「12 の原則」について検討メンバーの解釈を説明しています。

③「ビジョンとプロダクトの橋渡し」
-概要：いまの時代にプロダクトを価値として届けるために「プロダクト」の責任者に求められる役割を理解します。プロダクト責任者の必要性、役割、振る舞い方について説明しています。

④「アジャイル開発の進め方」
-概要：アジャイル開発のプロセスと開発者の役割について理解します。アジャイル開発プロセスの特徴やチームの特徴、および開発者の学ぶべきスキルについて説明しています。

⑤「アジャイルのさらなる広がり」
-概要：アジャイルの広がりを経営での事例、現場で取組方について説明しています。

◎：主体、〇：共同、△：参考

資料		概要	想定読者			
			経営層	事業部門	開発部門／チーム	情報システム部門
①	なぜ、いまアジャイルが必要か？	Society5.0 時代になぜアジャイルが必要かを理解	◎	◎	◎	◎
②	アジャイルソフトウェア開発宣言の読みとき方	アジャイル開発のベースにある価値観や原則について理解	〇	◎	◎	◎
③	ビジョンとプロダクトの橋渡し	プロダクト責任者の必要性、役割、振る舞い方について理解	〇	◎	〇	〇
④	アジャイル開発の進め方	アジャイル開発のプロセスと開発者の役割について理解	△	〇	◎	◎
①	アジャイルのさらなる広がり	アジャイルの広がりを経営、現場での取組方を例に理解	◎	〇	〇	〇

(出典) IPA「アジャイル領域へのスキル変革の指針」をもとに作成

詳細理解のため参考となる文献（参考文献）	
アジャイル領域へのスキル変革の指針	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001i7c-att/000065571.pdf

22-3-3. IoT ソリューション領域

ITSS+（プラス）の「IoT ソリューション領域」は、IoT 技術の設計、実装、管理に必要なスキルを強化するために設けられた領域です。これは、特に第 4 次産業革命に対応するために必要なスキルセットを提供することを目的としています。主に IT ベンダーとして必要な技術要素や、開発

プロセスなどに焦点を当て、IoT ソリューション開発でのロール（役割）定義や、各ロールにおけるタスクの特徴などについて解説されています。

対象

IoT ソリューション領域へのスキル変革の指針は、以下のような対象者が何を学ぶべきかの羅針盤や、IoT ソリューション領域の特徴の理解などに利用することを想定しています。

- 既存の IT システム開発に携わっているが、これから IoT ソリューション開発に取り組もうとするエンジニア
- すでに IoT ソリューション開発を実施しており、今後のキャリアや強みとする分野を考えようとしているエンジニアなど

(出典) IPA「IoT ソリューション領域へのスキル変革の指針 2021 改訂版」をもとに作成

ドキュメント構成

IoT ソリューション領域のドキュメントは、「①IoT ソリューション領域へのスキル変革の指針」、「②タスクリスト」、「③参考文献」の 3 部構成になっています。

① IoT ソリューション領域へのスキル変革の指針：
IoT ソリューション領域にこれから取り組もうとする方やスキルチェンジをしようとする技術者などに対して、当該領域の特徴や、活躍するロール（役割）、必要なタスクの概要などを説明しています。

② タスクリスト：
IoT ソリューション領域の仕事を行う上で具体的な業務をタスクとして定義し、大分類・中分類・小分類の階層に分解して示したものです。また、それぞれについてロール（役割）が主に担うタスクについても示しています。

③ 参考文献：
IoT ソリューション領域の仕事を行う上で参考となる書籍や公表資料などを示したものです。

(出典) IPA「IoT ソリューション領域へのスキル変革の指針 2021 改訂版」をもとに作成

詳細理解のため参考となる文献（参考文献）	
IoT ソリューション領域へのスキル変革の指針 2021 改訂版	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001i0x-att/000065568.pdf

22-3-4. セキュリティ領域

ITSS+（プラス）の「セキュリティ領域」は、企業のセキュリティ対策に必要なスキルと知識を体系化し、評価するための枠組みです。この領域は、特にサイバーセキュリティの脅威に対応するために設計されています。「セキュリティ領域」では、企業のセキュリティ対策に必要となるセキ

ュリティ関連業務のまとまりを 17 分野に整理しています。それぞれの分野に求められるセキュリティ知識、スキルの概要を理解することで、セキュリティ体制の構築時と人材育成・配置などに活用することができます。また、セキュリティ専門人材のみならず、セキュリティ以外の業務を生業としている人材の「学び直し」の指針として用い「プラス・セキュリティ人材」を育成できます。（セキュリティを専門としない事業部門、管理部門などの人材で、セキュリティ領域の知識・スキルを身につけた人材を、「プラス・セキュリティ人材」と呼んでいます）。

次の図は、セキュリティ関連タスクを担う分野の概観図です。

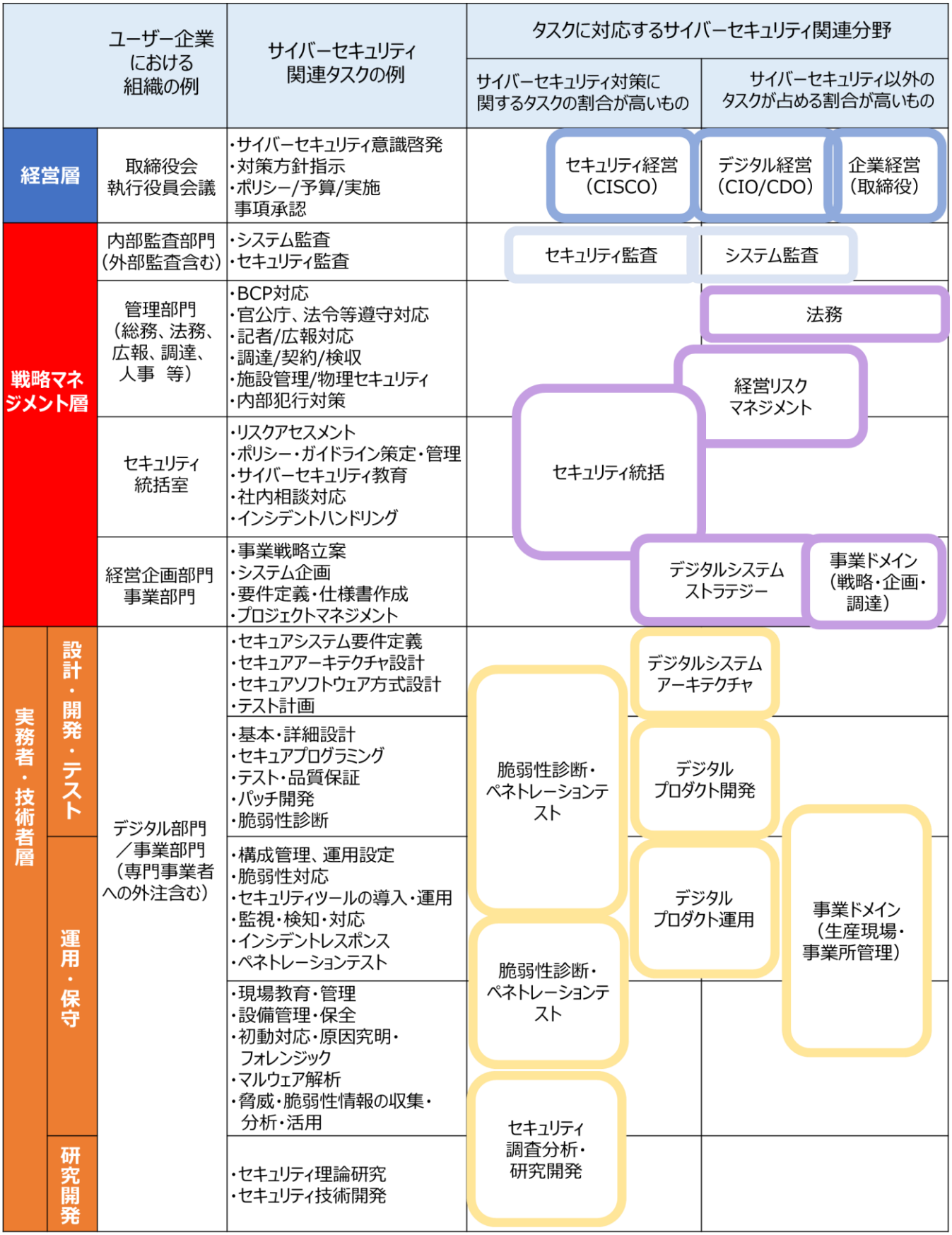


図 93. セキュリティ関連タスクを担う分野の概観図

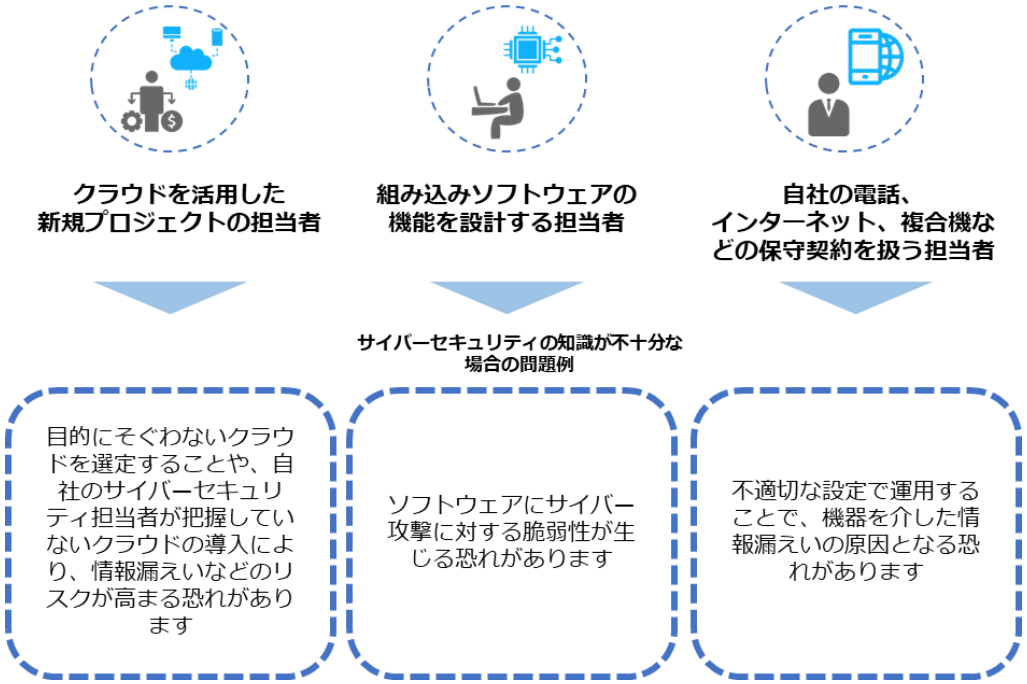
(出典) IPA「ITSS+（プラス）セキュリティ領域」をもとに作成

詳細理解のため参考となる文献（参考文献）	
サイバーセキュリティ体制構築・人材確保の手引き	https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf

プラス・セキュリティ

プラス・セキュリティとは
自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること、あるいは身につけている状態のこと

企業は、デジタルトランスフォーメーションの推進と並行してサイバーセキュリティへの対策が求められています。この状況の中、経営層をはじめ、法務や広報といった、必ずしも IT やセキュリティに関する専門知識や業務経験を有していない人も「プラス・セキュリティ」知識を習得することが重要です。なぜなら、デジタルトランスフォーメーションが進む中、サイバーセキュリティ担当部署だけでは、サイバーセキュリティ対策への対処が難しい状況になっているためです。そのため、サイバーセキュリティ対策が不十分な場合、インシデントが生じる可能性がある業務を担っている人材には、業務に必要なセキュリティに関する知識・スキルを身につけてもらう必要があります。



プラス・セキュリティ人材の育成

プラス・セキュリティの知識を身につける方法として、主に試験・資格を活用したり、教育プログラムを受けたりする方法があります。ここでは、具体例も含めて紹介します。

試験・資格の活用

各分野の人材がプラス・セキュリティの知識を身につける方法の 1 つとして、試験や資格の活用が挙げられます。資格を活用することの利点は、特定の役割や業務を担うために必要なスキルを効率よく習得できることです。

（例）

情報セキュリティマネジメント試験

【対象】企業の戦略マネジメント層や実務者層のサイバーセキュリティ担当者

【内容】本試験は、情報セキュリティマネジメントの計画・運用・評価・改善を通して組織の情報セキュリティ確保に貢献し、脅威から継続的に組織を守るための基本的なスキルを認定するものです。

教育プログラム・コミュニティ活動の活用

NISC（内閣サイバーセキュリティセンター）は、経営層、管理職、一般従業員ごとにそれぞれ初級、中級、上級で難易度が分けられたプラス・セキュリティ知識を補充できる研修、セミナー、講義などを紹介しています。

（例）

実践的サイバー防御演習「CYDER」(NICT)

【対象】各組織の情報システム担当者や CSIRT 要員

【難易度】初学者から準上級者

【内容】実際にマルウェア感染などのサイバー攻撃を受けた場合の対処能力の向上を図ることを目的としています。被害の対処をベンダーなど外部委託先に任せている場合であっても、被害発生時に委託先がどのような作業を実施しているかを予め理解・把握しておくことで、円滑なインシデント対応につながります。

実践サイバー演習「RPCI」（NICT）

【対象】経営層、管理職、一般従業員（特に、CISO、CSIRT 管理者、CSIRT メンバー、インシデントが発生した際の対応に携わる方、情報システムの管理・運用・調達・企画・開発に携わる方に向いています）

【難易度】中級～上級

【内容】本番に近いリアルな環境でのインシデント対応を行う演習です。擬似的に発生させたサイバー攻撃に CSIRT としてチームで対処します。実際の対応に近い体験をすることで、多くの気づきや学びを得ることができます。

そのほかについては、NISC のサイトを参照してください。

詳細理解のため参考となる文献（参考文献）	
実践的サイバー防御演習「CYDER」(NICT)	https://cyder.nict.go.jp/
実践サイバー演習「RPCI」(NICT)	https://rpci.nict.go.jp/
目的や所属・役割から選ぶ施策一覧	https://security-portal.nisc.go.jp/

22-4. i コンピテンシ ディクショナリ（iCD）

i コンピテンシ ディクショナリ（iCD）は、組織において IT を利活用するビジネスに求められる業務（タスク）と、それを支える IT 人材の能力や素養（スキル）を「タスクディクショナリ」、「スキルディクショナリ」として体系化したものです。具体的には、タスクとスキルをそれぞれ辞書のように参照できる形で構成立ててまとめています。i コンピテンシ ディクショナリを辞書として使用することで、従業員は、自身の業務に必要なスキルを把握できます。組織は目的に応じた人材育成や業務改善・効率化に活かすことができます。

i コンピテンシ ディクショナリ（iCD）に関する重要なポイント

i コンピテンシ ディクショナリ（iCD）において、重要なことは考え方です。タスクやスキルについては、デジタルスキル標準を参照することが大切です。

i コンピテンシ ディクショナリ（iCD）は、網羅的なタスク、スキル、知識の「辞書」として今後も有用ではありますが、デジタルスキル標準（DSS）と重複する部分が多く、デジタルスキル標準（DSS）の方が最新情報であるためです。

22-4-1. i コンピテンシ ディクショナリ（iCD）の考え方

i コンピテンシ ディクショナリは、企業、組織および IT 技術者が、人材育成やスキル向上に関わる施策を効率的に立案・推進し、成果を上げるための道具として有用です。

i コンピテンシ ディクショナリは、「タスクディクショナリ」と「スキルディクショナリ」で構成されています。仕事やスキルを構造的に表現して、必要に応じて取捨選択することで、企業や組織のあるべき姿や人材育成のための施策を、根拠を持って効率的に推進できます。

業務遂行における各ディクショナリの働きと関係は以下の通りです。

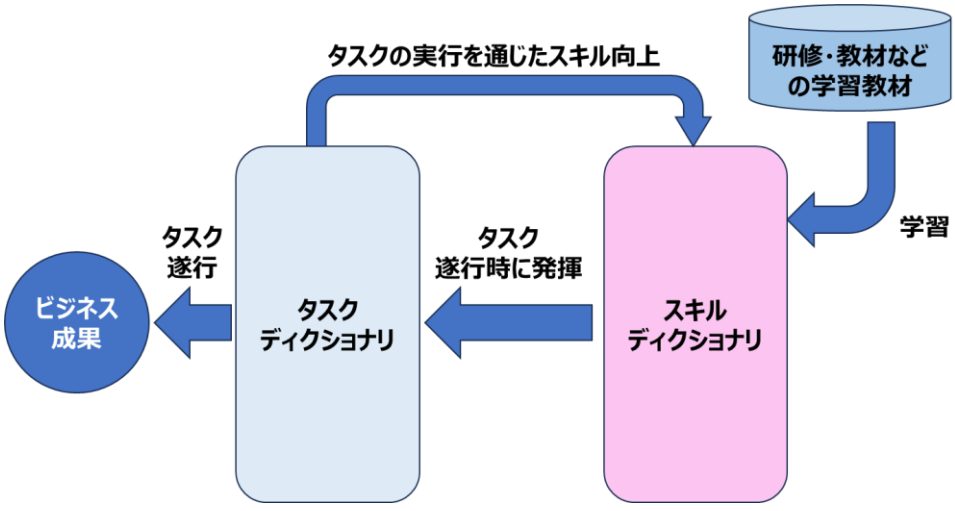


図 94. 業務遂行とディクショナリの働きの関係

(出典) IPA「i コンピテンシ ディクショナリ解説書」をもとに作成

「タスクディクショナリ」の考え方

タスクディクショナリの広範囲で網羅的なタスク群を参照し、自社・自組織のビジネスモデル、経営戦略や事業計画、および現状の業務に基づいて取捨選択することで、あるべき自社・自組織のタスクを定められます。

タスクを定めることにより、どのような能力を持つ人材がどのくらい必要かを明らかにでき、現状とのギャップも明確となり、効果的な人材育成施策を立案・実施することができます。また、組織の最適化や人員の最適配置など、人材育成に留まらない活用が可能です。

タスクディクショナリには、「タスクディクショナリ構成図」、「タスクプロフィール」が含まれており、自タスクを策定する際の参考情報として利用することを想定しています。

タスクディクショナリを構成する各コンテンツの関係は以下の通りです。

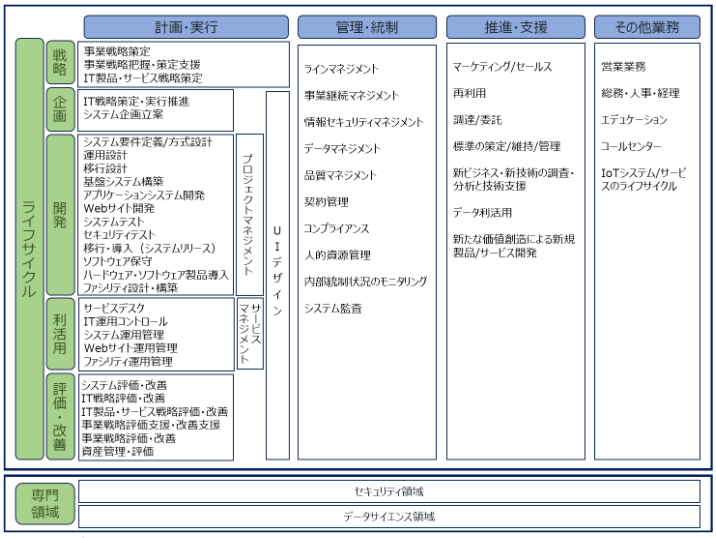
タスクディクショナリの全体像

タスク一覧

タスク大分類コード	タスク大分類	タスク中分類コード	タスク中分類	タスク小分類コード	タスク小分類	評価項コード	評価項目
ST01	事業戦略策定	ST01.1	事業環境の分析	ST01.1.1	経営方針の確認	ST01.1.1.1	自社の基本理念・ビジョン・方針を理解する
						ST01.1.1.2	新たな事業計画を立案するにあたり、経営方針や経営陣の思いを確認、共有する
						ST01.1.1.3	事業で達成すべき目標を定めるために、企業目標を把握する
				ST01.1.2	外部環境の分析	ST01.1.2.1	マクロ環境（自社を取り巻く産業や業界）の変化の要因を調査、把握する
						ST01.1.2.2	自社が所属する業界や自社製品・サービスの市場規模および今後の見通しを調査、把握する
						ST01.1.2.3	競合他社の市場シェア、収益性、動向を調査、把握する
				ST01.1.3	内部環境の分析	ST01.1.3.1	自社の組織体制、現状人員数、配置状況を把握する
						ST01.1.3.2	自社の収益性、安全性、生産性等の財務状況を把握する
						ST01.1.3.3	自社の製品やサービスの売上高、利益率、ライフサイクル上のポジションを把握する
						ST01.1.3.4	調達、生産、物流、サービス等の自社業務の一連の流れを把握する
						ST01.1.3.5	事業管理のために必要な情報が自社内のどこに、誰によって、どのように管理されているか把握する

各タスクの属性情報（特性、特徴）

タスクディクショナリ構成図



※タスクディクショナリの把握と保守（タスク追加・更新時の整理）のためのコンテンツ

タスクプロフィール

タスクプロフィール種別	タスクプロフィール種別の説明	タスクプロフィールグループ	タスクプロフィールコード	タスクプロフィール	タスクプロフィールの説明
ビジネスタイプ別	組織の立場（ユーザ、ベンダ）や業態によって必要なタスクを識別するもの。 ◎：必要なタスク ○：必要だが、他部門やアウトソースへの委託等が可能なタスク	-	A-010-010	自社向けシステム開発・保守・運用	自社向けシステムの開発・保守・運用を担う部門（IT/非IT企業の情報システム部門）に関連するタスク
			A-010-020	システム受託開発	アプリケーションシステムおよび基盤システムの受託開発を担う企業に関連するタスク
			A-010-030	ソフトウェア製品開発	ソフトウェア製品の企画・開発・販売を担う企業に関連するタスク
			A-010-040	組込みソフトウェア開発	組込みソフトウェアの開発を担う企業に関連するタスク
			A-010-050	Webサイト構築・運用	顧客のWebサイトの構築および運用を担う企業に関連するタスク
			A-010-060	システム運用サービス（運用業務受託）	顧客のシステム運用業務を受託して実施する企業に関連するタスク
			A-010-070	システム運用サービス（データセンタ運営）	自社のデータセンタ施設を持ち、顧客のシステム運用業務を受託して実施する企業に関連するタスク
			A-010-080	ITコンサルティング	ITコンサルティング（戦略、企画）を担う企業に関連するタスク

※タスクディクショナリの把握と活用（タスクの選択、役割の定義など）のためのコンテンツ

図 95. タスクディクショナリの構成

(出典) IPA「i コンピテンシディクショナリ解説書」をもとに作成

「スキルディクショナリ」の考え方

スキルディクショナリは、IT 技術者個人が、スキルディクショナリからスキル項目を選択して、現状把握やスキル向上目標を設定するために利用できます。

タスクディクショナリとの連係情報を利用して、そのスキルが、どのタスクの遂行に有効なのかを判断する使い方もできます。

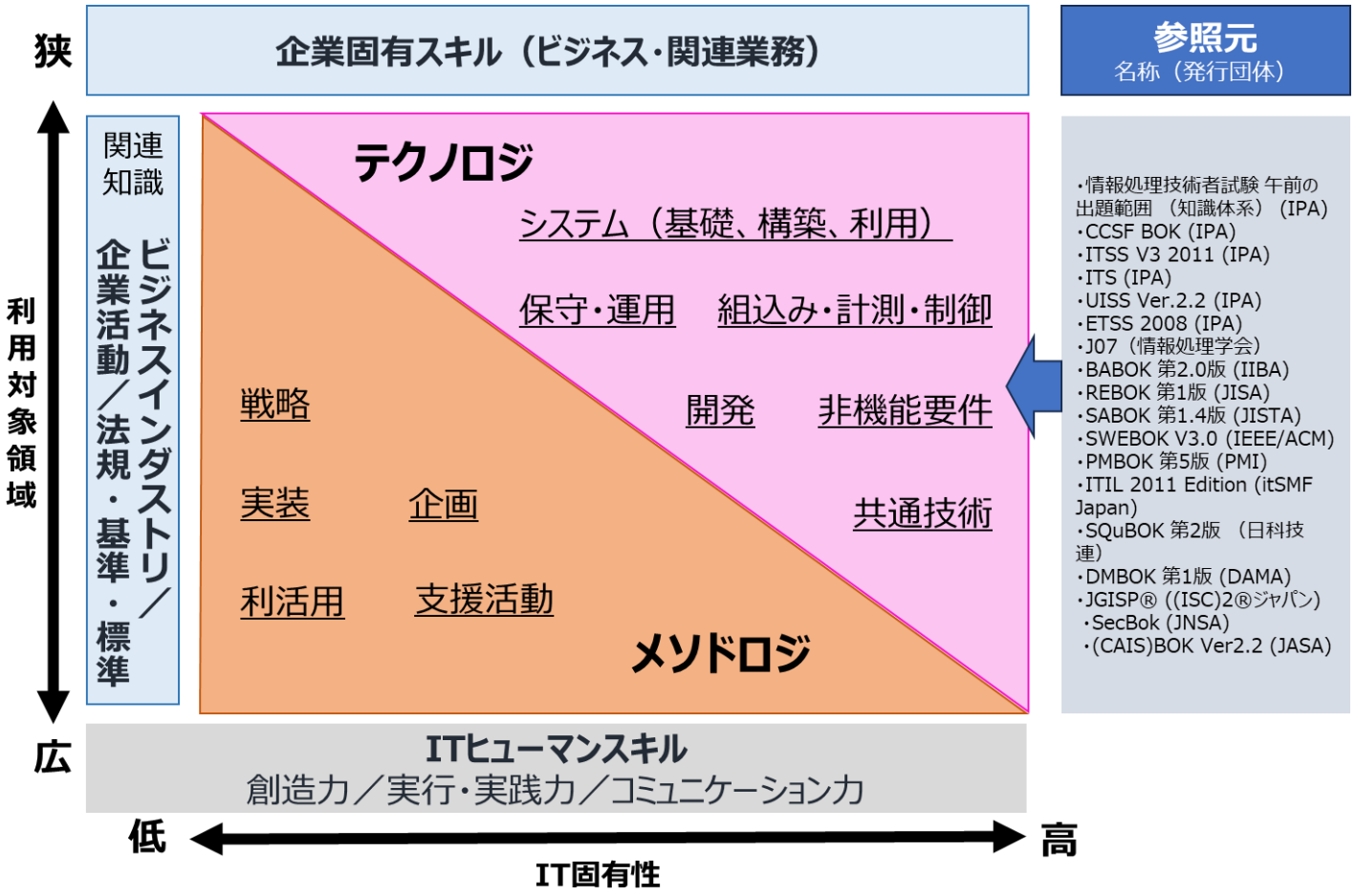


図 96. スキルディクショナリの構成

(出典) IPA「i コンピテンシディクショナリ解説書」をもとに作成

各項目の詳細は以下の通りです。

システム（基礎、構築、利用）
✓ ソフトウェア技術
✓ データベース技術
✓ ハードウェア技術
✓ Web システム技術
✓ プラットフォーム技術
✓ ネットワーク技術
保守・運用

- ✓ IT サービスマネジメント業務管理技術
- ✓ IT サービスオペレーション技術
- ✓ システム保守・運用・評価
- ✓ 障害修理技術
- ✓ 施工実務技術
- ✓ ファシリティ設計技術
- ✓ サポートセンター基盤技術

組込み・計測・制御

- ✓ 組込み技術（基礎、構築、利用）
- ✓ ディジタル技術
- ✓ ヒューマンインターフェース技術
- ✓ マルチメディア技術
- ✓ グラフィック技術
- ✓ 計測・制御技術

開発

- ✓ システムアーキテクティング技術
- ✓ システム開発管理技術

非機能要件

- ✓ 非機能要件（可用性、性能・拡張性）
- ✓ セキュリティ技術（基礎、構築、利用）

共通技術

- ✓ IT 基礎
- ✓ ナレッジマネジメント技術

戦略

- ✓ 市場機会の評価と選定
- ✓ マーケティング
- ✓ 製品・サービス戦略
- ✓ 販売戦略
- ✓ 製品・サービス開発戦略
- ✓ システム戦略立案手法
- ✓ コンサルティング手法
- ✓ 業務動向把握手法

企画

- ✓ システム企画立案手法

✓ セールス事務管理手法
✓ 要求分析手法
✓ 非機能要件設計手法
実装
✓ アーキテクチャ設計手法
✓ ソフトウェアエンジニアリング手法
✓ カスタマーサービス手法
✓ 業務パッケージ活用手法
✓ データマイニング手法
✓ 見積り手法
✓ プロジェクトマネジメント手法
利活用
✓ サービスマネジメント
✓ サービスの設計・移行
✓ サービスマネジメントプロセス
✓ サービスの運用
支援活動
✓ 品質マネジメント手法
✓ リスクマネジメント手法
✓ IT ガバナンス
✓ 資産管理手法
✓ ファシリティマネジメント手法
✓ 事業継続計画
✓ システム監査手法
✓ 標準化・再利用手法
✓ 人材育成・教育・研修
✓ 情報セキュリティ

(出典) IPA「i コンピテンシディクショナリ解説書」をもとに作成

i コンピテンシ ディクショナリ（iCD）の利活用の形態

i コンピテンシディクショナリは、以下の 3 種類の活用形態を利用対象者別に想定しています。

- 企業・組織での利活用
- 個人での利活用
- 学校等教育機関での利活用

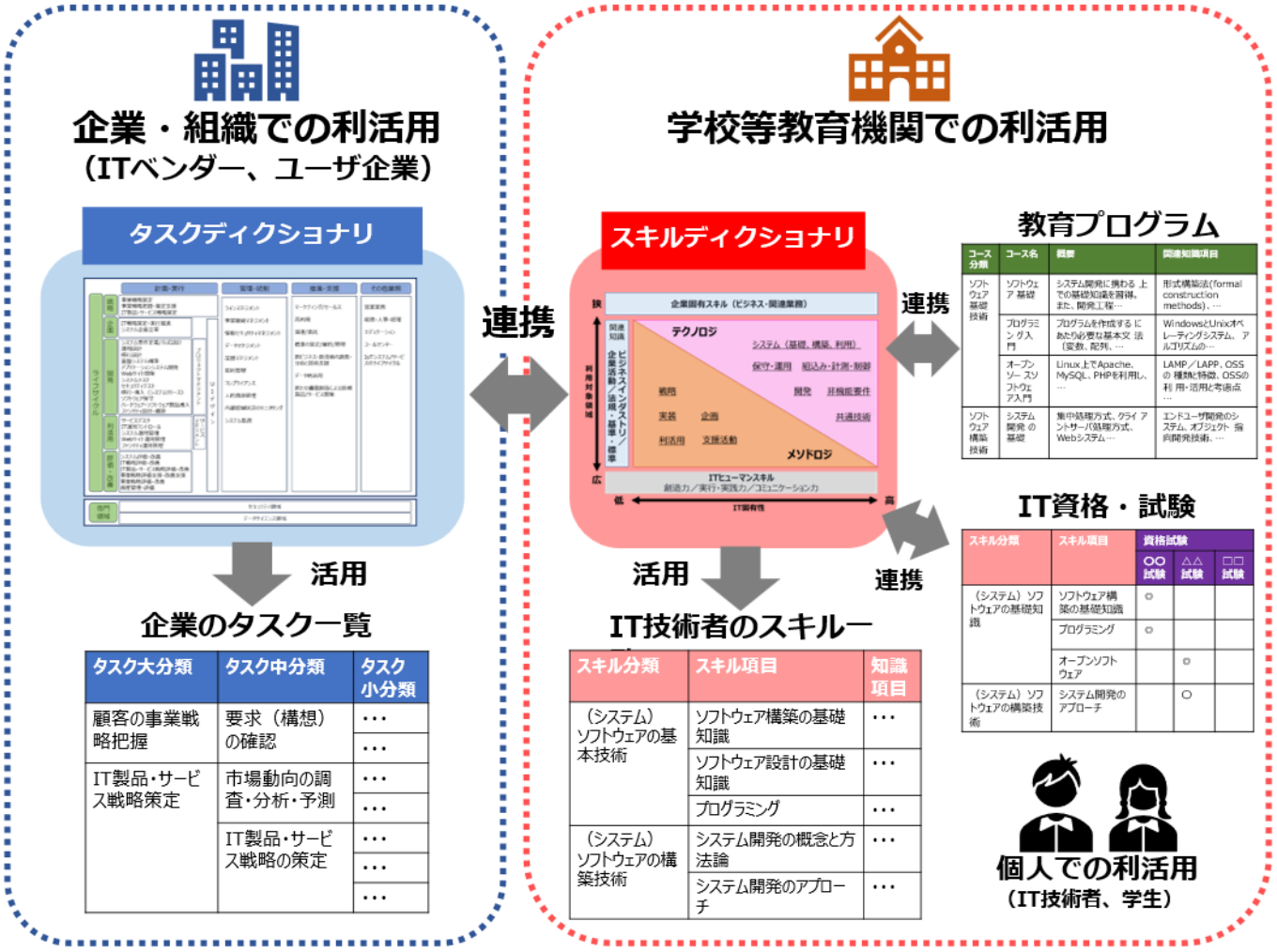


図 97. i コンピテンシ ディクショナリ（iCD）の利活用形態

(出典) IPA「i コンピテンシディクショナリ解説書」をもとに作成

第23章. 人材の知識とスキルの認定制度

章の目的
第 23 章では、IT およびデジタル人材のスキル、知識の認定制度と活用方法を理解することを目的とします。認定制度は、従業員一人一人に IT や情報セキュリティの知識を身につけてもらうための有効な手段となります。

主な達成目標
◘　スキルや知識の認定制度と活用方法を理解すること。

23-1. Di-Lite

「Di-Lite」とは、デジタルリテラシー協議会が定義する、すべてのビジネスパーソンが持つべきデジタル時代の共通リテラシーのことです。具体的には、以下の 3 つの領域に関するスキルや知識を指します。

① IT・ソフトウェア領域：基本的な IT スキルやソフトウェアの使用方法
② 数理・データサイエンス領域：データ分析や統計の基礎知識
③ 人工知能（AI）・ディープラーニング領域：AI 技術やディープラーニングの基礎知識

これらのスキルを身につけることで、デジタル時代におけるビジネスの効率化や競争力の向上が期待されています。学習すべき範囲は、「IT パスポート試験」「G 検定」「データサイエンティスト検定」の 3 つの試験のシラバス範囲になります。

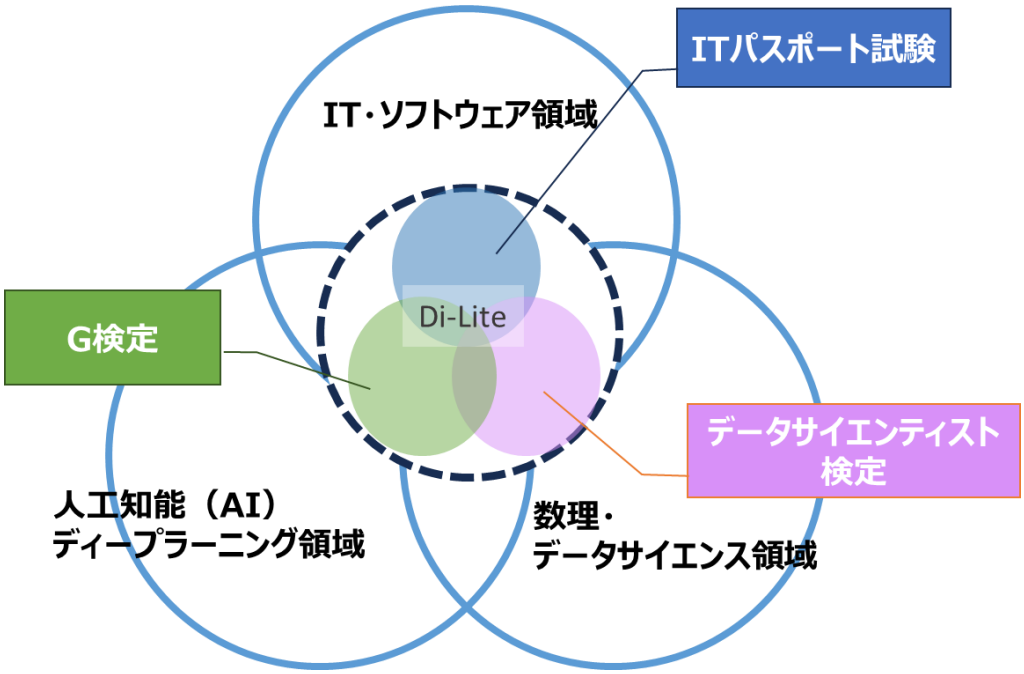
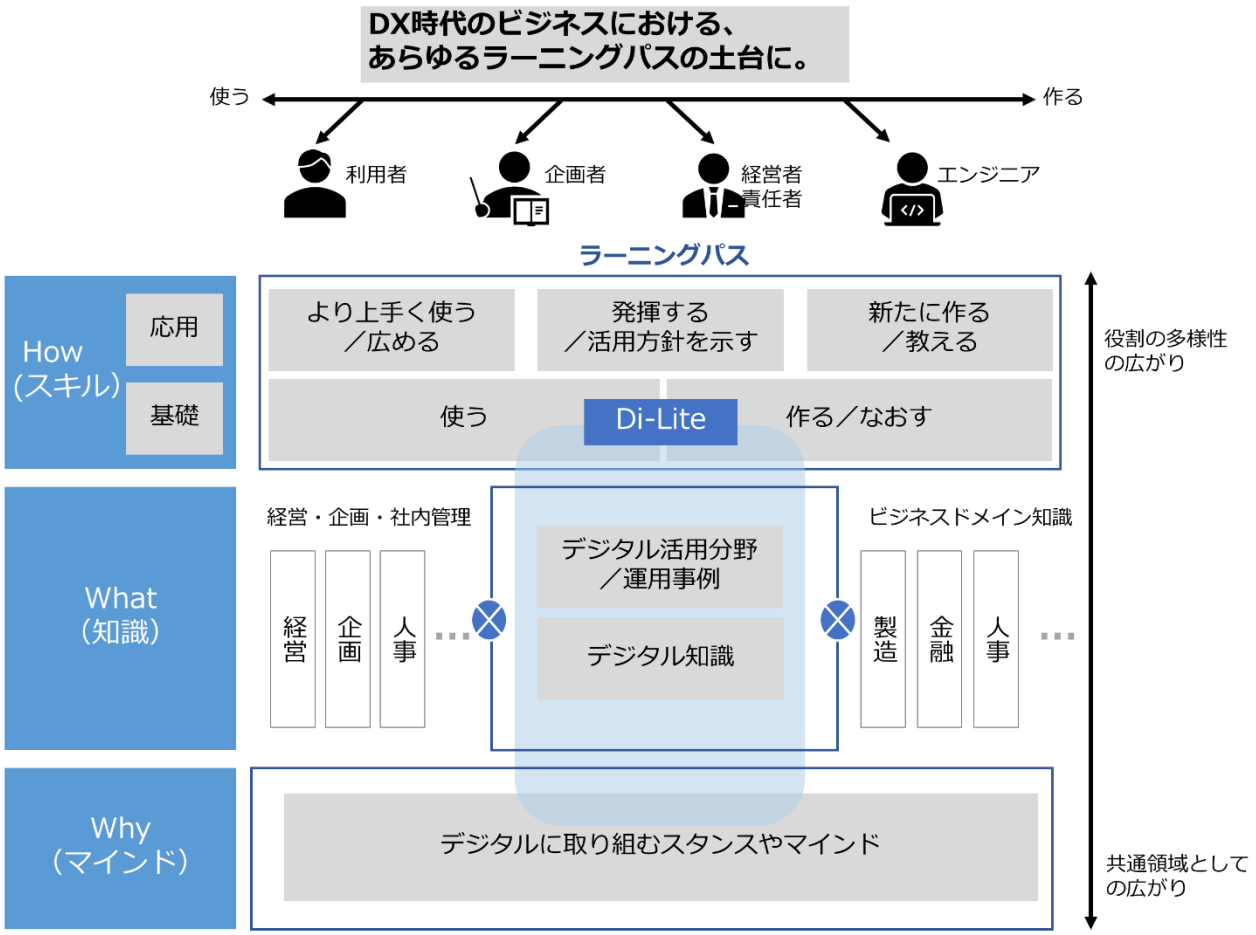


図 98. Di-Lite の 3 つの領域
(出典) デジタルリテラシー協議会「Di-Lite とは」をもとに作成



当協議会が、2021年4月時点で考え方を整理した「デジタルリテラシー・スキルフレームワーク」です。
今後協議を進める中で、更新される場合がございます。

図 99. デジタルリテラシー・スキルフレームワーク

(出典) デジタルリテラシー協議会「Di-Lite とは」をもとに作成

DX 推進パスポート

「IT パスポート試験」、「DS 検定 リテラシーレベル」、「G 検定」の 3 試験の合格数に応じて、デジタルバッジが発行されます。3 試験のうちいずれか 1 種類の合格者には「DX 推進パスポート 1」、いずれか 2 種類に合格すると「DX 推進パスポート 2」、3 つすべてに合格すると「DX 推進パスポート 3」のデジタルバッジが発行されます。

DX 推進パスポートのデジタルバッジ

DX パスポート 3	「IT パスポート」「データサイエンティスト検定」「G 検定」のすべてに合格
DX パスポート 2	「IT パスポート」「データサイエンティスト検定」「G 検定」のいずれか 2 つに合格 【デジタルバッジ発行のパターン】

	①　「IT パスポート」と「データサイエンティスト検定」に合格 ②　「IT パスポート」と「G 検定」に合格 ③　「データサイエンティスト検定」と「G 検定」に合格
DX パスポート 1	「IT パスポート」「データサイエンティスト検定」「G 検定」のいずれか 1 つに合格 【デジタルバッジ発行のパターン】 ①　「IT パスポート」に合格 ②　「データサイエンティスト検定」に合格 ③　「G 検定」に合格

(出典) デジタルリテラシー協議会「Di-Lite」をもとに作成

詳細理解のため参考となる文献（参考文献）	
Di-Lite	https://www.dilite.jp/

23-1-1. IT ソフトウェア領域

Di-Lite の 3 つの領域のうち「IT ソフトウェア領域」における学習範囲「IT パスポート試験」のシラバスについて全体像を説明します。

IT パスポート試験のシラバスは、情報処理技術者試験の一部として、幅広い IT 知識を評価するために設計されています。シラバスは「ストラテジ系」「マネジメント系」「テクノロジー系」の 3 つの主要な領域に分かれています。

IT パスポート（IP）

対象者	職業人およびこれから職業人となる者が備えておくべき、IT に関する共通的な基礎知識を持ち、IT に携わる業務に就くか、担当業務に対して IT を活用していこうとする者

シラバスの全体像は以下の通りです。

ストラテジ系
大分類 1：企業と法務 **中分類 1：企業活動** ✓　経営・組織論 ✓　業務分析・データ利活用 ✓　会計・財務

中分類 2：法務

- ✓ 知的財産権
- ✓ セキュリティ関連法規
- ✓ 労働関連・取引関連法規
- ✓ その他の法律・ガイドライン・情報倫理
- ✓ 標準化関連

大分類 2：経営戦略

中分類 3：経営戦略マネジメント

- ✓ 経営戦略手法
- ✓ マーケティング
- ✓ ビジネス戦略と目標・評価
- ✓ 経営管理システム

中分類 4：技術戦略マネジメント

- ✓ 技術開発戦略の立案・技術開発計画

中分類 5：ビジネスインダストリ

- ✓ ビジネスシステム
- ✓ エンジニアリングシステム
- ✓ e-ビジネス
- ✓ IoT システム・組込みシステム

大分類 3：システム戦略

中分類 6：システム戦略

- ✓ 情報システム戦略
- ✓ 業務プロセス
- ✓ ソリューションビジネス
- ✓ システム活用促進・評価

中分類 7：システム企画

- ✓ システム化計画
- ✓ 要件定義
- ✓ 調達計画・実施

マネジメント系

大分類 4：開発技術

中分類 8：システム開発技術

- ✓ システム開発技術

中分類 9：ソフトウェア開発管理技術

- ✓ 開発プロセス・手法

大分類 5：プロジェクトマネジメント

中分類 10：プロジェクトマネジメント

- ✓ プロジェクトマネジメント

大分類 6：サービスマネジメント

中分類 11：サービスマネジメント

- ✓ サービスマネジメント
- ✓ サービスマネジメントシステム
- ✓ ファシリティマネジメント

中分類 12：システム監査

- ✓ システム監査
- ✓ 内部統制

テクノロジー系

大分類 7：基礎理論

中分類 13：基礎理論

- ✓ 離散数学
- ✓ 応用数学
- ✓ 情報に関する理論

中分類 14：アルゴリズムとプログラミング

- ✓ データ構造
- ✓ アルゴリズムとプログラミング
- ✓ プログラム言語
- ✓ その他の言語

大分類 8：コンピュータシステム

中分類 15：コンピュータ構成要素

- ✓ プロセッサ
- ✓ メモリ
- ✓ 入出力デバイス

中分類 16：システム構成要素

- ✓ システムの構成
- ✓ システムの評価指標

中分類 17：ソフトウェア

- ✓ オペレーティングシステム
- ✓ ファイルシステム
- ✓ オフィスツール
- ✓ オープンソースソフトウェア

中分類 18：ハードウェア

✓ ハードウェア（コンピュータ・入出力装置）

大分類 9：技術要素

中分類 19：情報デザイン

✓ 情報デザイン

✓ インタフェース設計

中分類 20：情報メディア

✓ マルチメディア技術

✓ マルチメディア応用

中分類 21：データベース

✓ データベース方式

✓ データベース設計

✓ データ操作

✓ トランザクション処理

中分類 22：ネットワーク

✓ ネットワーク方式

✓ 通信プロトコル

✓ ネットワーク応用

中分類 23：セキュリティ

✓ 情報セキュリティ

✓ 情報セキュリティ管理

✓ 情報セキュリティ対策・情報セキュリティ実装技術

(出典) IPA「IT パスポート試験シラバス」をもとに作成

「技術要素」に含まれる「情報セキュリティ」について抜粋して詳細に説明します。

情報セキュリティ

1. 情報セキュリティの概念

- 情報セキュリティの基本的な概念と目的

2. 情報資産

- 企業における情報資産の代表的な種類として、顧客情報、営業情報、知的財産関連情報、人事情報などがあること

3. 脅威と脆弱性

- 情報セキュリティの代表的な脅威の種類と基本的な対処法
- セキュリティインシデントが発生しやすくなる要因である脆弱性

① **人的脅威の種類と特徴**
② **技術的脅威の種類と特徴**
③ **物理的脅威の種類と特徴**
④ **脆弱性**
⑤ **不正のメカニズム**

4. 攻撃手法

- 情報システム、組織および個人への外部からの不正な行為と手法、およびそれらへの対策の概要

情報セキュリティ管理

1. リスクマネジメント

- リスクマネジメントは、リスクの特定・分析・評価・対応という流れで実施されること
- 事故などが発生した際に対処するために、対応マニュアルの整備や教育・訓練などの準備が必要であること

2. 情報セキュリティ管理

- 情報セキュリティ管理の必要性と情報セキュリティマネジメントシステム（ISMS：Information Security Management System）の考え方

3. 個人情報保護

- 個人情報保護の必要性、法律やプライバシーマーク制度などの取組の目的

4. 情報セキュリティ組織・機関

- 不正アクセスによる被害受付けの対応、再発防止のための提言、情報セキュリティに関する啓発活動などを行う情報セキュリティ組織・機関の役割、および関連する制度

5. 各種の基準・ガイドライン

- コンピュータウイルス対策基準、コンピュータ不正アクセス対策基準、システム管理基準などが、情報システムに関する規範として利用されていること

情報セキュリティ対策・情報セキュリティ実装技術

1. 情報セキュリティ対策の種類

- 情報セキュリティ対策としての人的・技術的・物理的セキュリティ対策の基本的な考え

方

② 人的セキュリティ対策

- 人的セキュリティ対策の種類
- 身近な業務における基本的な対策の実行

③ 技術的セキュリティ対策

- 技術的セキュリティ対策の種類
- 身近な業務における基本的対策の実行

④ 物理的セキュリティ対策

- 物理的セキュリティ対策の種類
- 組織のルールにしたがった行動の実行

2. 暗号技術

- 情報セキュリティを維持するために必要な暗号技術の基本的な仕組み、暗号化アルゴリズム、暗号強度などの特徴

3. 認証技術

- 認証の必要性、脅威を防止するためにどのような認証技術が用いられるかの概要
- それぞれの認証技術によって何が証明できるかの概要

4. 利用者認証

- 利用者認証のために利用される技術の種類、特徴

5. 生体認証（バイオメトリクス認証）

- 利用者確認に利用される技術の 1 つである生体認証技術の種類、特徴

6. 公開鍵基盤

- 公開鍵基盤の基本的な仕組みと特徴

7. アプリケーションソフトウェア・IoT システムのセキュリティ

- アプリケーションソフトウェア、IoT システム、IoT 機器のセキュリティの対策の種類、特徴

(出典) IPA「IT パスポート試験シラバス」をもとに作成

詳細理解のため参考となる文献（参考文献）	
IT パスポート試験シラバス	https://www.ipa.go.jp/shiken/syllabus/nq6ept00000014eh-att/syllabus_ip_ver6_3.pdf

23-1-2. 数理・データサイエンス領域

Di-Lite の 3 つの領域のうち「数理・データサイエンス領域」における学習範囲である「データサイエンティスト検定」のシラバスについて全体像を説明します。

データサイエンティストとは、データサイエンス力、データエンジニアリング力をベースにデータから価値を創出し、ビジネス課題に答えを出すプロフェッショナルです。データサイエンティストに求められるスキルセットはデータサイエンス力・ビジネス力・データエンジニアリング力とされ、検定においても 3 つの領域の力を図ります。

データサイエンティスト検定（リテラシーレベル）

対象者	• データサイエンティスト初学者 • これからデータサイエンティストを目指すビジネスパーソン

試験範囲（3 つの領域）

領域	内容
データサイエンス力★1	線形代数基礎、微分・積分基礎、集合論基礎、統計数理基礎、洞察、性質・関係性、推定・検定、アソシエーション分析、因果推論、データ確認、俯瞰・メタ思考、データ理解、サンプリング、データクレンジング、データ加工、特徴量エンジニアリング、方向性定義、軸だし、データ加工、表現・実装技法、意味抽出、回帰・分類、統計的評価、機械学習、深層学習、時系列分析、クラスタリング、ネットワーク分析、レコメンド、自然言語処理、画像認識、映像認識、音声認識、大規模言語モデル
データエンジニアリング力★1	システム企画、システム設計、アーキテクチャ設計、クライアント技術、通信技術、データ抽出、データ収集、データ構造の基礎知識、テーブル定義、DWH、分散技術、クラウド、フィルタリング処理、ソート処理、結合処理、前処理、マッピング処理、サンプリング処理、集計処理、変換・演算処理、データ出力、データ展開、データ連携、基礎プログラミング、拡張プログラミング、AI サービス活用、アルゴリズム、分析プログラム、SQL、IT セキュリティの基礎知識、攻撃と防御手法、暗号化技術、認証、AutoML、MLOps、AIOps、プロンプトエンジニアリング、生成 AI のコーディング支援
ビジネス力★1	ビジネスマインド、データ･AI 倫理、コンプライアンス、MECE、構造化能力、言語化能力、ストーリーライン、ドキュメンテーション、説明能力、AI 活用検討、KPI、スコーピング、データ入手、分析アプローチ設計、生成 AI 活用、統計情報への正しい理解、ビジネス観点での理解、意味合いの抽出･洞察、評価･改善の仕組み、契約、権利保護、プロジェクト発足、リソースマネ

	ジメント、リスクマネジメント

（出典）データサイエンティスト協会 「データサイエンティスト検定 リテラシ－レベルとは」をもとに作成

※データサイエンティストに求められるスキルについては、「22-4-1.データサイエンス領域」で説明します。

詳細理解のため参考となる文献（参考文献）	
データサイエンティスト検定 リテラシ－レベルとは	https://www.datascientist.or.jp/dscertification/what/

23-1-3. AI・ディープラーニング領域

Di-Lite の 3 つの領域のうち「AI・ディープラーニング領域」における学習範囲「G 検定」のシラバスについて全体像を説明します。

G 検定（ジェネラリスト検定）

対象者	• ビジネスの関わるすべての方

G 検定の試験範囲（シラバス）

技術分野
人工知能とは 人工知能の定義、人工知能分野で議論される問題 **人工知能をめぐる動向** 探索・推論、知識表現とエキスパートシステム、機械学習、ディープラーニング **機械学習の概要** 教師あり学習、教師なし学習、強化学習、モデルの選択・評価 **ディープラーニングの概要** ニューラルネットワークとディープラーニング、活性化関数、誤差関数、正則化、誤差逆伝播法、最適化手法 **ディープラーニングの要素技術** 全結合層、畳み込み層、正規化層、プーリング層、スキップ結合、回帰結合層、Attention、オートエンコーダ、データ拡張 **ディープラーニングの応用例** 画像認識、自然言語処理、音声処理、深層強化学習、データ生成、転移学習・ファインチューニング、マルチモーダル、モデルの解釈性、モデルの軽量化 **AI の社会実装に向けて**

AI プロジェクトの進め方、データの収集・加工・分析・学習 **AI に必要な数理・統計知識**
法律倫理分野
AI に関する法律と契約 個人情報保護法、著作権法、特許法、不正競争防止法、独占禁止法、AI 開発委託契約、AI サービス提供契約 **AI 倫理・AI ガバナンス** 国内外のガイドライン、プライバシー、公平性、安全性とセキュリティ、悪用、透明性、民主主義、環境保護、労働政策、そのほかの重要な価値、AI ガバナンス

(出典) 日本ディープラーニング協会「G 検定とは」をもとに作成

G 検定の試験範囲のうち、セキュリティに関する箇所を抜粋して説明します。

AI 倫理・AI ガバナンス	
11.安全性とセキュリティ	
• 安全性に関する論点の所在と代表的な事例を理解している • セキュリティ上の課題としてどのような攻撃などが存在しているのか理解している • 安全性やセキュリティの課題への対応手段を理解している	Adversarial Attack（Adversarial Examples)、セキュリティ・バイ・デザイン、データ汚染、データ窃取、モデル窃取、モデル汚染

(出典) 日本ディープラーニング協会「G 検定 試験出題範囲（シラバス 2024)」をもとに作成

詳細理解のため参考となる文献（参考文献）	
G 検定とは	https://www.jdla.org/certificate/general/#general_No03
G 検定の試験範囲（シラバス）と例題	https://www.jdla.org/certificate/general/#

23-2. 情報処理技術者試験

個人や組織が安全で効果的な IT の活用を進めるためには、IT 業界や IT 職種に限らず、IT を利用する側のすべての人々が IT や情報セキュリティに関する知識を持つことが必要です。また、デジタルトランスフォーメーション（DX）の進展に伴い、IT やセキュリティに関する専門知識や業務経験がない人々にとっても、企業内外でセキュリティの専門人材と協力する機会が増加しています。このような協力関係を築くためにも、IT や情報セキュリティに関する知識を習得しておくことが望まれます。従業員一人一人に IT や情報セキュリティの知識を身につけてもらうための有効な手段の一つが、情報処理技術者試験の受験です。情報処理技術者試験に合格するには、IT リテラシーおよび情報セキュリティに関する基礎知識を習得する必要があるからです。組織全体で従業員一人一人のセキュリティ意識を高めることは、組織の安全な運営に不可欠です。また、組織内のセキュリティ専門人材不足の問題の解消にも役立ちます。まずは情報処理技術者試験の全体像を紹介します。

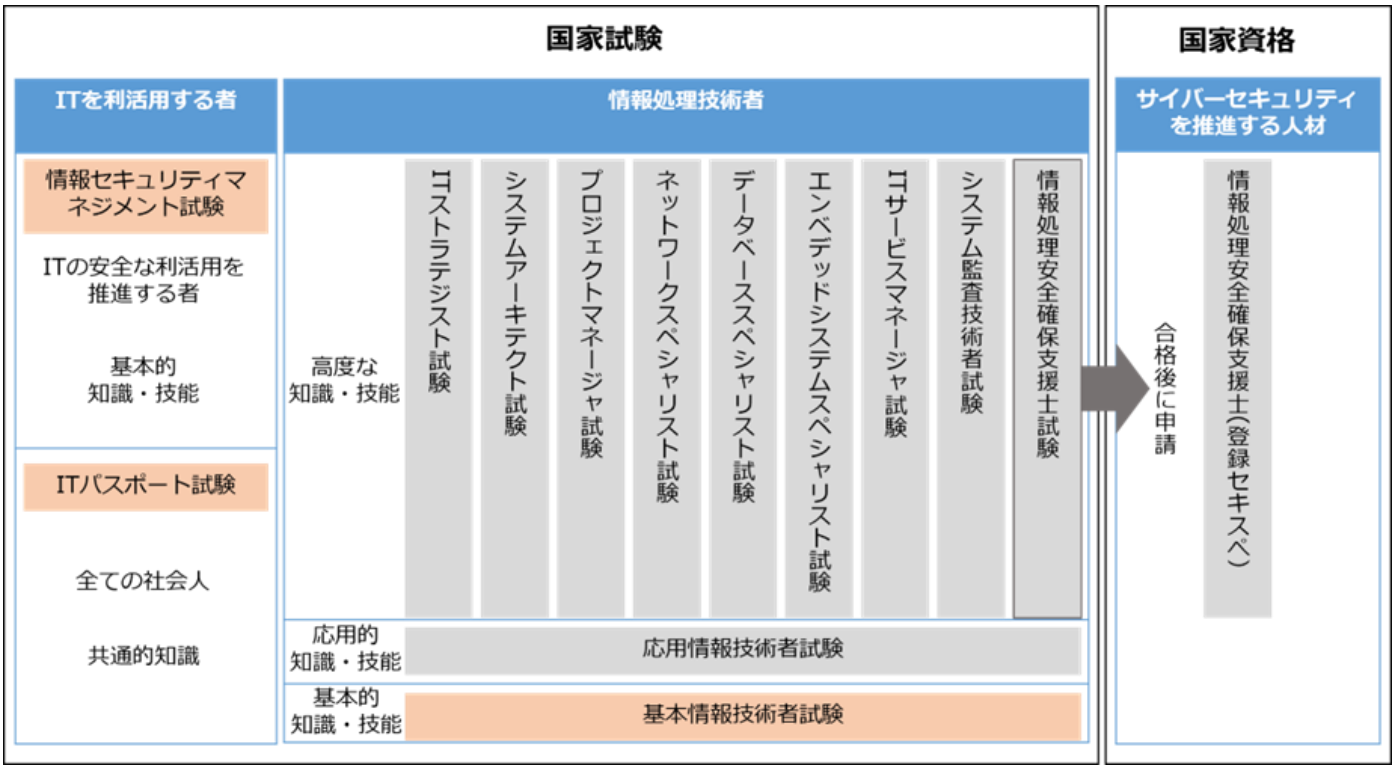


図 100 IT ヒューマンスキル概念図

(出典) IPA「情報処理技術者試験・情報処理安全確保支援士試験　試験要綱」をもとに作成

各試験の出題分野の全体像を以下の表に示します。

※IT パスポート試験については、「22-2-1. IT ソフトウェア領域」を参照してください。

出題分野 ＼ 試験区分			情報セキュリティマネジメント試験（参考）	基本情報技術者試験（科目 A）	応用情報技術者	高度試験・支援士試験	
						午前Ⅰ（共通知識）	午前Ⅱ（専門知識） 情報処理安全確保支援士試験
テクノロジー系	基礎理論	基礎理論		○2	○3	○3	
		アルゴリズムとプログラミング					
	コンピュータシステム	コンピュータ構成要素					
		システム構成要素	○2				
		ソフトウェア					
		ハードウェア					
	技術要素	ユーザーインターフェース					
		情報メディア					
		データベース	○2				○3
		ネットワーク	○2				◎4
		セキュリティ	◎2	◎2	◎3	◎3	◎4
	開発技術	システム開発技術		○2	○3	○3	○3
		ソフトウェア開発管理技術					○3
マネジメント系	プロジェクトマネジメント	プロジェクトマネジメント	○2				
	サービスマネジメント	サービスマネジメント	○2				○3
		システム監査	○2				○3
ストラテジ系	システム戦略	システム戦略	○2				
		システム企画	○2				
	経営戦略	経営戦略マネジメント					
		技術戦略マネジメント					
		ビジネスインダストリ					
	企業と法務	企業活動	○2				
		法務	◎2				

注記 1：○は出題範囲であることを、◎は出題範囲のうちの重点分野であることを表す。

注記 2：2、3、4 は技術レベルを表し、4 が最も高度で、上位は下位を包含する。

(出典) IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

上記の表の「セキュリティ」分野の内容を詳細に説明します。

大分類	中分類	小分類	知識項目例
技術要素	セキュリティ	情報セキュリティ	情報の機密性・完全性・可用性、多層防御、脅威、マルウェア・不正プログラム、脆弱性、不正のメカニズム、攻撃者の種類・動機、サイバー攻撃（SQL インジェクション、クロスサイトスクリプティング、DoS 攻撃、フィッシング、パスワードリスト攻撃、標的型攻撃、AI を悪用した攻撃ほか）、暗号技術（共通鍵、公開鍵、秘密鍵、RSA、AES、ハイブリッド暗号、ハッシュ関数ほか）、認証技術（デジタル署名、メッセージ認証、タイムスタンプほか）、利用者認証（利用者 ID・パスワード、多要素認証、パスワードレス認証、アイデンティティ連携（OpenID、SAML）ほか）、生体認証技術、公開鍵基盤（PKI、認証局、デジタル証明書ほか）、政府認証基盤（GPKI、ブリッジ認証局ほか）など
		情報セキュリティ管理	情報資産とリスクの概要、情報資産の調査・分類、リスクの種類、情報セキュリティリスクアセスメントおよびリスク対応、情報セキュリティ継続、情報セキュリティ諸規程（情報セキュリティポリシーを含む組織内規程）、ISMS、情報セキュリティ管理策（組織的管理策、人的管理策、物理的管理策、技術的管理策）、情報セキュリティ組織・機関（CSIRT、SOC（Security Operation Center）、エシカルハッカーほか）、コンピュータ不正アクセス対策基準、コンピュータウイルス対策基準、PCI DSS など
		セキュリティ技術評価	ISO/IEC 15408（コモンクライテリア）、JISEC（IT セキュリティ評価および認証制度）、JCMVP（暗号モジュール試験および認証制度）、CVSS、脆弱性検査、ペネトレーションテストなど
		情報セキュリティ対策	情報セキュリティ啓発（教育、訓練ほか）、組織における内部不正防止ガイドライン、マルウェア・不正プログラム対策、ランサムウェア対策、不正アクセス対策、情報漏えい対策、アカウント管理、ログ管理、脆弱性管理、入退室管理、アクセス制御、侵入検知/侵入防止、検疫ネットワーク、携帯端末（携帯電話、スマートフォン、タブレット端末ほか）のセキュリティ、クラウドサービスのセキュリティ、IoT の

			セキュリティ、AI を使ったセキュリティ技術、AI そのものを守るセキュリティ技術、セキュリティ製品・サービス（ファイアウォール、WAF、DLP、SIEM ほか）、デジタルフォレンジックスなど
		セキュリティ実装技術	セキュアプロトコル（IPsec、SSL/TLS、SSH、WPA3 ほか）、認証・認可技術（SPF、DKIM、SMTP-AUTH、OAuth、DNSSEC ほか）、セキュア OS、ネットワークセキュリティ、データベースセキュリティ、アプリケーションセキュリティ、コンテナセキュリティ、セキュアプログラミングなど

（出典）IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

詳細理解のため参考となる文献（参考文献）	
情報処理技術者試験 情報処理安全確保支援士 試験要綱	https://www.ipa.go.jp/shiken/syllabus/nq6ept00000014lt-att/youkou_ver5_3.pdf

セキュリティに関する知識やスキルを身につけるためには、以下の試験が推奨されます。

- IT パスポート
- 情報セキュリティマネジメント試験
- 基本情報技術者試験
- 応用情報技術者試験
- 情報処理安全確保支援士試験

上記の試験に焦点を当て、各試験について説明します。
※IT パスポート試験については、「22-2-1. IT ソフトウェア領域」を参照してください。

23-2-1. 情報セキュリティマネジメント試験

対象者	情報システムの利用部門にあって、情報セキュリティリーダーとして、部門の業務遂行に必要な情報セキュリティ対策や組織が定めた情報セキュリティ諸規程（情報セキュリティポリシーを含む組織内諸規程）の目的・内容を適切に理解し、情報および情報システムを安全に活用するために、情報セキュリティが確保された状況を実現し、維持・改善する者。

業務と役割	情報システムの利用部門において情報セキュリティが確保された状況を実現し、維持・改善するために、次の業務と役割を果たします。 ① 部門における情報資産の情報セキュリティを維持するために必要な業務を遂行します。 ② 部門の情報資産を特定し、情報セキュリティリスクアセスメントを行い、リスク対応策をまとめます。 ③ 部門の情報資産に関する情報セキュリティ対策および情報セキュリティ継続の要求事項を明確にします。 ④ 部門の業務の IT 活用推進に伴う情報システムの調達に際して、利用部門として必要となる情報セキュリティ要求事項を明確にする。また、IT 活用推進の一部を利用部門が自ら実現する活動の中で、必要な情報セキュリティ要求事項を提示します。 ⑤ 業務の外部委託に際して、情報セキュリティ対策の要求事項を契約で明確化し、その実施状況を確認します。 ⑥ 部門の情報システムの利用時における情報セキュリティを確保します。 ⑦ 部門のメンバーの情報セキュリティ意識、コンプライアンスを向上させ、内部不正などの情報セキュリティインシデントの発生を未然に防止します。 ⑧ 情報セキュリティインシデントの発生またはそのおそれがあるときに、情報セキュリティ諸規程、法令・ガイドライン・規格などに基づいて、適切に対処します。 ⑨ 部門または組織全体における情報セキュリティに関する意見・問題点について担当部署に提起します。
活用方法	① 部門の情報セキュリティマネジメントの一部を独力で遂行できます。 ② 情報セキュリティインシデントの発生またはそのおそれがあるときに、情報セキュリティリーダーとして適切に対処できます。 ③ IT 全般に関する基本的な用語・内容を理解できます。 ④ 情報セキュリティ技術や情報セキュリティ諸規程に関する基本的な知識を持ち、部門の情報セキュリティ対策の一部を独力で、または上位者の指導の下に実現できます。 ⑤ 情報セキュリティ機関、他の企業などから動向や事例を収集し、部門の環境への適用の必要性を評価できます。

(出典) IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

23-2-2. 基本情報技術者試験

対象者	IT を活用したサービス、製品、システムおよびソフトウェアを作る人材に必要な基本的知識・技能を持ち、実践的な活用能力を身につけた者。
業務と役割	上位者の指導の下に、次のいずれかの役割を果たします。 ① 組織および社会の課題に対する、IT を活用した戦略の立案、システムの企画・要件定義に参加します。 ② システムの設計・開発、汎用製品の最適組み合わせ（インテグレーション）によって、利用者にとって価値の高いシステムを構築します。 ③ サービスの安定的な運用の実現に貢献します。
活用方法	① IT 全般に関する基本的な事項を理解し、担当する活動に活用できます。 ② 上位者の指導の下に、IT 戦略に関する予測・分析・評価に参加できます。 ③ 上位者の指導の下に、システムまたはサービスの提案活動に参加できます。 ④ 上位者の指導の下に、システムの企画・要件定義に参加できます。 ⑤ 上位者の指導の下に、情報セキュリティの確保を考慮して、システムの設計・開発・運用ができます。 ⑥ 上位者の指導の下に、ソフトウェアを設計できます。 ⑦ 上位者の方針を理解し、自らプログラムを作成できます。

(出典) IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

23-2-3. 応用情報技術者試験

対象者	IT を活用したサービス、製品、システムおよびソフトウェアを作る人材に必要な応用的知識・技能を持ち、高度 IT 人材としての方向性を確立した者。
業務と役割	独力で次のいずれかの役割を果たします。 ① 組織および社会の課題に対する、IT を活用した戦略の立案、システムの企画・要件定義を行います。 ② システムの設計・開発、汎用製品の最適組み合わせ（インテグレーション）によって、利用者にとって価値の高いシステムを構築します。 ③ サービスの安定的な運用を実現します。

活用方法	① 経営戦略・IT 戦略の策定に際して、経営者の方針を理解し、経営を取り巻く外部環境を正確に捉え、動向や事例を収集できます。 ② 経営戦略・IT 戦略の評価に際して、定められたモニタリング指標に基づき、差異分析などを行うことができます。 ③ システムまたはサービスの提案活動に際して、提案討議に参加し、提案書の一部を作成できます。 ④ システムの企画・要件定義、アーキテクチャの設計において、システムに対する要求を整理し、適用できる技術の調査が行うことができます。 ⑤ 運用管理チーム、オペレーションチーム、サービスデスクチームなどのメンバーとして、担当分野におけるサービス提供と安定稼動の確保が行うことができます。 ⑥ プロジェクトメンバーとして、プロジェクトマネージャ（リーダー）の下でスコープ、予算、工程、品質などの管理ができます。 ⑦ 情報システム、ネットワーク、データベース、組込みシステムなどの設計・開発・運用・保守において、上位者の方針を理解し、自ら技術的問題を解決できます。

(出典) IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

23-2-4. 各分野スペシャリスト試験

各分野スペシャリスト試験については、概要を説明します。

IT ストラテジスト試験（ST）

対象者	高度 IT 人材として確立した専門分野を持ち、企業の経営戦略に基づいて、ビジネスモデルや企業活動における特定のプロセスについて、情報技術（IT）を活用して事業を改革・高度化・最適化するための基本戦略を策定・提案・推進する者。

(出典) IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

IT ストラテジスト試験は、経営戦略に基づいて IT 戦略を策定し、IT を高度に活用した事業革新、業務改革、および競争優位を獲得する製品･サービスの創出を企画･推進して、ビジネスを成功に導く CIO や CTO、IT コンサルタントを目指す方に最適な試験です。

システムアーキテクト試験（SA）

対象者	高度 IT 人材として確立した専門分野を持ち、IT ストラテジストからの提案を受けて、情報システムを利用したシステムの開発に必要となる要件を定義し、それを実現するためのアーキテクチャを設計し、開発を主導する者。

(出典) IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

システムアーキテクト試験は、システム開発の上流工程を主導する立場で、豊富な業務知識に基づいて的確な分析を行い、業務ニーズに適した情報システムのグランドデザインを設計し完成に導く、上級エンジニアを目指す方に最適な試験です。

プロジェクトマネージャ試験（PM）

対象者	高度 IT 人材として確立した専門分野を持ち、組織の戦略の実現に寄与することを目的とするシステム開発プロジェクトにおいて、プロジェクトの目的の実現に向けて責任を持ってプロジェクトマネジメント業務を単独でまたはチームの一員として担う者。

(出典) IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

プロジェクトマネージャ試験は、プロジェクトを取り巻く環境変化やステークホルダの多様な要求に柔軟に対応しながら、プロジェクトを確実に成功に導くマネージャを目指す方に最適な試験です。

ネットワークスペシャリスト試験（NW）

対象者	高度 IT 人材として確立した専門分野を持ち、ネットワークに関係する固有技術を活用し、最適な情報システム基盤の企画・要件定義・開発・運用・保守において中心的な役割を果たすとともに、固有技術の専門家として、情報セキュリティを含む情報システムの企画・要件定義・開発・運用・保守への技術支援を行う者。

(出典) IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

ネットワークスペシャリスト試験は、ネットワークの固有技術からサービス動向まで幅広く精通し、目的に適合した大規模かつ堅牢なネットワークシステムを構築し運用できるネットワークエン

ジニアやインフラ系エンジニアを目指す方に最適な試験です。

データベーススペシャリスト試験（DB）

対象者	高度 IT 人材として確立した専門分野を持ち、データベースに関係する固有技術を活用し、最適な情報システム基盤の企画・要件定義・開発・運用・保守において中心的な役割を果たすとともに、固有技術の専門家として、情報システムの企画・要件定義・開発・運用・保守への技術支援を行う者。

(出典) IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

データベーススペシャリスト試験は、企業活動を支える膨大なデータ群を管理し、パフォーマンスの高いデータベースシステムを構築して、顧客のビジネスに活用できるデータ分析基盤を提供するデータベース管理者やインフラ系エンジニアを目指す方に最適な試験です。

エンベデッドシステムスペシャリスト試験（ES）

対象者	高度 IT 人材として確立した専門分野を持ち、IoT を含む組込みシステムの開発に関係する広い知識や技能を活用して、市場動向・関連業界の動向を踏まえて最適な組込みシステムの事業戦略や製品戦略を策定し、ハードウェアとソフトウェアの要求仕様の策定、および要求仕様に基づいた組込みシステムの設計・構築・製造を主導的に行う者。

(出典) IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

エンベデッドシステムスペシャリスト試験は、スマート家電、自動運転などあらゆるモノがつながる IoT が進展する中で、新たな機能を実現するために、ハードウェアとソフトウェアを適切に組み合わせたシステムの企画・開発を推進し、必要な機能・性能・品質・セキュリティなどを確保する、組込み・IoT 系のフルスタックエンジニアを目指す方に最適な試験です。

IT サービスマネージャ試験（SM）

対象者	高度 IT 人材として確立した専門分野を持ち、サービスの要求事項を満たし、サービスの計画立案、設計、移行、提供および改善のための組織の活動および資源を、指揮し、管理する者。

(出典) IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

IT サービスマネージャ試験は、顧客ニーズを踏まえ、日々の継続的改善を通じて安全性と信頼性の高い IT サービスを最適なコストで安定的に提供し、IT 投資効果を最大化できる IT サービスマネージャを目指す方に最適な試験です。

システム監査技術者試験（AU）

対象者	高度 IT 人材として確立した専門分野を持ち、高い倫理観の下、監査対象から独立かつ客観的な立場で、情報システムや組込みシステムを総合的に検証・評価して、監査報告の利用者に情報システムのガバナンス、マネジメント、コントロールの適切性などに対する保証を与える、または改善のための助言を行う者。

(出典) IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

システム監査技術者試験は、情報システムに係るリスクを分析し、コントロールを評価・検証することによって、組織体の目標達成に寄与し、利害関係者に対する説明責任を果たす監査人や情報システム責任者などを目指す方に最適な試験です。

23-2-5. 情報処理安全確保支援士試験

対象者	サイバーセキュリティに関する専門的な知識・技能を活用して企業や組織における安全な情報システムの企画・設計・開発・運用を支援し、また、サイバーセキュリティ対策の調査・分析・評価を行い、その結果に基づき必要な指導・助言を行う者。
業務と役割	情報セキュリティマネジメントに関する業務、情報システムの企画・設計・開発・運用におけるセキュリティ確保に関する業務、情報および情報システムの利用におけるセキュリティ対策の適用に関する業務、情報セキュリティインシデント管理に関する業務に従事し、次の役割を主導的に果たすとともに、下位者を指導します。 ① 情報セキュリティ方針および情報セキュリティ諸規程（事業継続計画に関する規程を含む組織内諸規程）の策定、情報セキュリティリスクアセスメントおよびリスク対応などを推進または支援します。 ② システム調達（製品・サービスのセキュアな導入を含む）、システム開発（セキュリティ機能の実装を含む）を、セキュリティの観点から推進または支援します。 ③ 暗号利用、マルウェア対策、脆弱性への対応など、情報および情報システム

	の利用におけるセキュリティ対策の適用を推進または支援します。 ④ 情報セキュリティインシデントの管理体制の構築、情報セキュリティインシデントへの対応などを推進または支援します。
活用方法	① 情報システムおよび情報システム基盤の脅威分析に関する知識を持ち、セキュリティ要件を抽出できます。 ② 情報セキュリティの動向・事例、およびセキュリティ対策に関する知識を持ち、セキュリティ対策を対象システムに適用するとともに、その効果を評価できます。 ③ 情報セキュリティマネジメントシステム、情報セキュリティリスクアセスメントおよびリスク対応に関する知識を持ち、情報セキュリティマネジメントについて指導・助言できます。 ④ ネットワーク、データベースに関する知識を持ち、暗号、認証、フィルタリング、ロギングなどの要素技術を適用できます。 ⑤ システム開発、品質管理などに関する知識を持ち、それらの業務について、セキュリティの観点から指導・助言できます。 ⑥ 情報セキュリティ方針および情報セキュリティ諸規程の策定、内部不正の防止に関する知識を持ち、情報セキュリティに関する従業員の教育・訓練などについて指導・助言できます。 ⑦ 情報セキュリティ関連の法的要求事項、情報セキュリティインシデント発生時の証拠の収集および分析、情報セキュリティ監査に関する知識を持ち、それらに関連する業務を他の専門家と協力しながら遂行できます。

(出典) IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

23-3. 国際セキュリティ資格

各情報処理技術者試験で培った IT 知識は、国際セキュリティ資格の学習の基礎となります。また、相乗効果の観点から国際セキュリティ資格の学習を通じて、各情報処理技術者試験の知識を深められたり、より高度な IT ポジションへのキャリアアップが期待できたりします。

CISSP（Certified Information Systems Security Professional）

対象者	情報セキュリティ分野での専門知識と経験を持っている者。
業務と役割	ISC2 が認定を行うベンダーフリー・カントリーフリーの情報セキュリティの専門家資格です。CISSP には、情報セキュリティにおける理論やメカニズムを理解することに加えて、その知識を体系的かつ構造的に整理し、状況に応じた適切な判断を行うための、合理的かつ実践的な「知識」と「理解度」があることを証明します。
活用方法	ANSI(米国規格協会)より、ISO/IEC17024 の認証を受けた厳正な資格開発、運用、運営、維持に加え、米国国防総省のキャリアパスにおいて取得が義務付けられている資格の 1 つにも認定されており、CISSP は知識と実務経験を兼ね備えた、常に最新の知識を持った情報セキュリティプロフェッショナルであることを証明します。

(出典) ISC2「CISSP 8 ドメインガイドブック」をもとに作成

CISM（Certified Information Security Manager）

対象者	主に情報セキュリティガバナンス、プログラムの開発と管理、インシデント管理、およびリスク管理の専門知識を持っていることを証明することを希望する者。
業務と役割	CISM は、情報セキュリティマネジメントの知識と経験を認定する国際的資格であり、日本語名称を『公認情報セキュリティマネージャ』と呼称します。ISACA により、2002 年に資格制度が創設され、2003 年度より試験が開始されました。情報セキュリティマネジメントのチームプレイヤーからリーダーへ、ステップアップしたい方に最適な認定資格です。

活用方法	CISM は、企業・団体などの情報セキュリティプログラムに係る、マネジメント、設計、監督を行う、以下のプロフェッショナルの方をフォーカスしています。 ● セキュリティマネージャ（Security managers） ● 最高情報セキュリティ責任者（CISO）や最高戦略責任者（CSO）をはじめとする ● セキュリティ担当役員（Security directors） ● セキュリティ担当役職者（Security officers） ● セキュリティコンサルタント（Security consultants） ● コンプライアンス、リスク、プライバシー担当役職者・マネージャ

(出典) ISACA 東京支部ホームページをもとに作成

CISA(Certified Information Systems Auditor)

対象者	企業などで運用されている情報システムの信頼性・安全性などの検証・評価を行う際に高いスキルを持って対応できると証明することを希望する者。
業務と役割	CISA とは"Certified Information Systems Auditor"の略称であり、「公認情報システム監査人」とも呼ばれています。ISACA（情報システムコントロール協会）が認定する国際的な資格であり、情報システムを監査する者の能力と専門性を証明します。
活用方法	IT/情報システム監査人、コントロール、保証および情報セキュリティの専門家としてのキャリア育成に役立ちます。

(出典) ISACA 東京支部ホームページをもとに作成

詳細理解のため参考となる文献（参考文献）	
CISSP 8 ドメインガイドブック	https://japan.isc2.org/files/MAR-CISSP_Guidebook-JP-RB-2023.pdf
ISACA 東京支部	https://www.isaca.gr.jp

引用文献

デジタルスキル標準 ver.1.2

https://www.ipa.go.jp/jinzai/skill-standard/dss/ps6vr700000083ki-att/000106872.pdf

生成 AI に関する DX 推進スキル標準の改訂 要旨（2024 年 7 月）

https://www.ipa.go.jp/jinzai/skill-standard/dss/about_dss-p.html

Di-Lite とは

https://www.dilite.jp/

G 検定とは

https://www.jdla.org/certificate/general/

G 検定の試験範囲（シラバス）と例題

https://www.jdla.org/certificate/general/#

IT スキル標準 V3 2011　1 部：概要編

https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024840.pdf

IT スキル標準 V3 2011　2 部：キャリア編

https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024842.pdf

IT スキル標準 V3 2011 スキルディクショナリ_20120326

https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024846.pdf

データサイエンティスト　スキルチェックリスト　Ver5.00

https://www.datascientist.or.jp/common/docs/skillcheck_ver5.00_simple.xlsx

アジャイル領域へのスキル変革の指針

https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001i7c-att/000065571.pdf

IoT ソリューション領域へのスキル変革の指針 2021 改訂版

https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001i0x-att/000065568.pdf

ITSS+（プラス）セキュリティ領域

https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/security.html

i コンピテンシディクショナリ解説書

https://www.icda.or.jp/wp-content/uploads/2021/03/iCD_guidebook-1.pdf

情報処理技術者試験・情報処理安全確保支援士試験 試験要綱

https://www.ipa.go.jp/shiken/syllabus/nq6ept00000014lt-att/youkou_ver5_3.pdf

CISSP 8 ドメインガイドブック
https://japan.isc2.org/files/MAR-CISSP_Guidebook-JP-RB-2023.pdf
ISACA 東京支部
https://www.isaca.gr.jp

参考文献

デジタルスキル標準 ver.1.2

https://www.ipa.go.jp/jinzai/skill-standard/dss/ps6vr700000083ki-att/000106872.pdf

マナビ DX

https://manabi-dx.ipa.go.jp/

Di-Lite

https://www.dilite.jp/

IT パスポート試験シラバス

https://www.ipa.go.jp/shiken/syllabus/nq6ept00000014eh-att/syllabus_ip_ver6_3.pdf

データサイエンティスト検定 リテラシーレベルとは

https://www.datascientist.or.jp/dscertification/what/

G 検定とは

https://www.jdla.org/certificate/general/#general_No03

G 検定の試験範囲（シラバス）と例題

https://www.jdla.org/certificate/general/#

IT スキル標準 V3 2011　1 部：概要編

https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024840.pdf

IT スキル標準 V3 2011　2 部：キャリア編

https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024842.pdf

IT スキル標準 V3 2011 スキルディクショナリ_20120326

https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024846.pdf

IT スキル標準Ｖ 3　2011　3 部：スキル編

https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024844.pdf

ITSS+（プラス）概要

https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/about.html

データサイエンティスト　スキルチェックリスト　Ver5.00

https://www.datascientist.or.jp/common/docs/skillcheck_ver5.00_simple.xlsx

データサイエンティストのためのスキルチェックリスト／タスクリスト概説

https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001ity-att/000083733.pdf

アジャイル領域へのスキル変革の指針
https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001i7c-att/000065571.pdf
IoT ソリューション領域へのスキル変革の指針 2021 改訂版
https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001i0x-att/000065568.pdf
サイバーセキュリティ体制構築・人材確保の手引き
https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf
実践的サイバー防御演習「CYDER」(NICT)
https://cyder.nict.go.jp/
実践サイバー演習「RPCI」（NICT）
https://rpci.nict.go.jp/
目的や所属・役割から選ぶ施策一覧
https://security-portal.nisc.go.jp/
情報処理技術者試験 情報処理安全確保支援士 試験要綱
https://www.ipa.go.jp/shiken/syllabus/nq6ept00000014lt-att/youkou_ver5_3.pdf
CISSP 8 ドメインガイドブック
https://japan.isc2.org/files/MAR-CISSP_Guidebook-JP-RB-2023.pdf
ISACA 東京支部
https://www.isaca.gr.jp

■AI

Artificial Intelligence の略。

「AI（人工知能）」という言葉は、昭和 31 年に米国の計算機科学研究者ジョン・マッカーシーが初めて使った言葉。昭和 25 年代後半から昭和 35 年代が第一次 AI ブーム、昭和 55 年代が第二次 AI ブーム、現在は平成 20 年代から始まる第三次 AI ブームである（近年の大規模言語モデルなどの登場を契機に、第 4 次 AI ブームに入ったとの見方もある）。「AI」に関する確立した定義はないが、人間の思考プロセスと同じような形で動作するプログラム、あるいは人間が知的と感じる情報処理・技術といった広い概念で理解されている

■BCP

Business Continuity Plan（事業継続計画）の略。企業が災害やテロ攻撃などの緊急事態に直面した際に、被害を最小限に抑え、企業の存続に関わる最も重要な事業を継続または早期復旧するための計画

■CSIRT（シーサート）

Computer Security Incident Response Team の略。コンピュータセキュリティにかかる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、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動を行う

■DDoS 攻撃（ディードスこうげき）

Distributed Denial of Service Attack の略。攻撃者が複数のコンピュータを操作し、標的となるコンピュータに対して同時に大量の問い合わせを送ることにより、過剰な負荷をかけてサービスを利用できなくする攻撃手法

■DFFT

Data Free Flow with Trust の略。日本が提案したコンセプトであり、ビジネスや社会的な課題を解決するために、データの国際的な自由な流れを促進すると同時に、プライバシー、セキュリティ、知的財産権に対する信頼を確保することを目指している

■EDR

Endpoint Detection and Response の略。パソコンやスマートフォン、サーバなどのエンドポイントにおける不審な動作を検知し、迅速な対応を支援するソリューション。従来のツールやソリューションでは防げなかった未知のマルウェアや不正アクセスを検知し被害の拡大を防止する

■eKYC

electronic Know Your Customer の略称。オンラインで完結可能な本人確認方法のこと

■G ビズ ID

行政手続きなどにおいて手続きを行う法人を認証するための仕組み。1 つの ID・パスワードで本人確認書類なしにさまざまな政府・自治体の法人向けオンライン申請が可能になる

■ICSCoE 中核人材育成プログラム

平成 29 年 4 月に独立行政法人情報処理推進機構（IPA）内に設置された産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence, ICSCoE）

が実施している人材育成プログラム。制御技術（OT：Operational Technology）と情報技術（IT）の両方の知識・スキルを有し、社会インフラ・産業基盤へのサイバーセキュリティリスクに対応できる人材の育成を目的としている

■ICT

Information and Communication Technology の略。IT（情報技術）に加えて、コンピュータやスマートフォンなどを用いて行うコミュニケーションを実現する技術（通信技術）を含んでいる

■IDS

Intrusion Detection System の略。不正アクセスや異常な通信を検知して管理者に通知するシステムのこと。IPS と異なり、不正アクセスや異常な通信をブロックする機能はない

■IoT（アイ・オー・ティー）

Internet of Things の略。日本語では「モノのインターネット」。インターネットにコンピュータやセンサー、カメラ、産業機械、家電などさまざまな「モノ」が接続され、データを収集したり、相互に情報をやり取りしたりする概念や仕組み、技術のこと

■IPS

Intrusion Prevention System の略。不正侵入防止システムとも呼ばれるセキュリティ確保の仕組み。

IPS は、異常を検知した場合、管理者に通知するに加えて、その通信を遮断する

■IP アドレス

コンピュータをネットワークで接続するために、それぞれのコンピュータに割り振られた一意になる数字の組み合わせ。 IP アドレスは、127.0.0.1 のように 0～255 までの数字を 4 つ組み合わせたもので、単にアドレスと略されることがある。 現在主に使用されているこれら 4 つになる数字の組み合わせによるアドレス体系は、IPv4（アイ・ピー・ブイフォー）と呼ばれている。また、今後情報家電などで大量に IP アドレスが消費される時代に備えて、次期規格として、IPv6（アイ・ピー・ブイシックス）と呼ばれるアドレス体系への移行が進みつつある。なお、IPv6 では、アドレス空間の増加に加えて、情報セキュリティ機能の追加などの改良も加えられている

■ISAC

Information Sharing and Analysis Center の略。業界内での情報共有・連携を図る組織のこと。国内では、金融や交通、電力、ICT などの分野に ISAC がある。ICT-ISAC では、ICT 分野の情報セキュリティに関する情報（インシデント情報を含む。）の収集・調査・分析を行っている

■ISMS

Information Security Management System の略称。情報セキュリティを確保するための、組織的、人的、運用的、物理的、技術的、法令的なセキュリティ対策を含む、経営者を頂点とした総合的で組織的な取組。組織が ISMS を構築するための要求事項をまとめた国際規格が ISO/IEC 27001（国内規格は JIS Q 27001）であり、審査機関の審査に合格すると「ISMS 認証」を取得できる

■ISP

個人や企業などに対してインターネットに接続するためのサービスを提供する事業者

のこと。ユーザーは ISP と契約し、回線を用いて ISP が運営するネットワークに接続することで、インターネット上のサーバなどへアクセスできる

■IT リテラシー

コンピュータやインターネットをはじめとする情報技術（IT）を適切に活用する基礎的な知識や技能

■JPCERT/CC

日本におけるセキュリティインシデントなどの報告の受付け、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、技術的な立場から行っている組織。政府機関や企業などから独立した中立の組織として、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

■JVN

Japan Vulnerability Notes の略。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対策情報を提供する、脆弱性対策情報ポータルサイトのこと

■KPI

Key Performance Indicator の略。目標・戦略を実現するために設定した具体的な業務プロセスをモニタリングするために設定される指標（業績評価指標：Performance Indicators）のうち、特に重要なもの

■LockBit2.0

「Your files are encrypted by LockBit」というメッセージを表示させ、身代金を要求するマルウェア（ランサムウェア）。感染するとファイルが暗号化され、拡張子が「.LockBit」に変更される

■MAC アドレス

Media Access Control address の略。隣接する機器同士の通信を実現するためのアドレスのこと。ネットワーク機器や PC、ルータなどについている固有の識別番号で、一般的に 12 桁の 16 進数で「00-00-00-XX-XX-XX」などと表される

■NISC

National center of Incident readiness and Strategy for Cybersecurity の略。内閣サイバーセキュリティセンターの略称。サイバーセキュリティに関する施策の立案や実施、行政各部の情報システムに対するセキュリティ対策の強化を担当

■NIST サイバーセキュリティフレームワーク（CSF）

米国政府機関の重要インフラの運用者を対象として誕生し、防御に留まらず、検知・対応・復旧といった、インシデント対応が含まれている。日本においても、今後普及が見込まれる

■RPA

Robotic Process Automation の略。定型的な業務をソフトウェアのロボットにより自動化すること

■NTP

Network Time Protocol の略。あらゆる機器の時刻情報を同期するためのプロトコル（通信規約）のこと。時刻情報を配信するサーバと、時刻合わせを行うクライアント間、およびサーバ間の通信方法を定めている

■PII

Personally Identifiable Information の略。「個人を特定できる情報」と訳されるこ

とが多いが、実際には個人を特定するために使用される情報のこと。個人と 1 対 1 に紐づいているマイナンバー、メールアドレス、携帯電話番号、銀行口座番号に加えて、氏名、生年月日、住所、勤務先などの情報も PII に含まれる

■PJMO

Project Management Office の略。プロジェクトの進捗管理やタスク管理などを行う組織のこと。プロジェクト管理を行うチームや担当者を指す。

例えば、プロジェクト管理を行うチームは、情報システム部門の担当者に加え、実務部門の担当者、調達担当者、業務委託先が決定した後はその担当者も含めた体制で構成する

■PMO

Project Management Office の略。（企業組織やプロジェクト規模によっては、Program Management Office、Portfolio Management Office とも呼ばれる。）組織全体のプロジェクトを横断的に管理する体制を指す。

政府ガイドラインでの PMO は、府省全体の管理となっているが、一般企業においては、企業全体のプロジェクトの管理と読み替えられる。

PJMO が個々のプロジェクト計画を定めるのに対し、PMO は全プロジェクトについて、横断的に管理・支援を行う（例：計画、予算、執行管理、PJMO 支援など）

■RFI

Request For Information の略。情報提供依頼のこと。発注者が依頼をする候補となるシステム開発会社に対して、技術情報や製品情報の提供を依頼すること

■SASE（サシー）

Secure Access Service Edge の略。令和元年に提唱されたゼロトラストセキュリティを実現する方法の 1 つで、IT 環境のネットワークの機能とセキュリティの機能をクラウドサービス上で統合して提供するサービス、また、その考え方・概念

■SBOM（エスボム）

Software Bill of Materials の略。ソフトウェアを構成する要素を一覧できるリストのこと。SBOM は、ソフトウェアの構成要素の名称やバージョン情報、開発者、依存関係などの情報を含む。SBOM は、ソフトウェアのリスクを把握・管理するのに役立つ

■SDP

Software-Defined Perimeter の略。ゼロトラストを実現するための仕組みで、すべての通信をチェックおよび認証する。VPN は、ネットワーク接続前に一度だけ認証を行うのに対し、SDP は、ユーザーの情報（デバイス、場所、OS など）など複数の要素からネットワーク接続前、接続中、接続後で検証と認証を行う

■SECURITY ACTION

中小企業自らが、情報セキュリティ対策に取り組むことを自己宣言する制度

■SLA

Service Level Agreement の略。サービス提供者と利用者の間で結ばれるサービスの品質に関して合意する契約のこと。サービスを提供する事業者が利用者に対して、どの程度の品質を保証できるのかを明示したもの

■Society5.0

日本が目指すべき未来社会

の姿として、平成 28 年に閣議決定された「第 5 期科学技術基本計画」において内閣府が提唱した概念。サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）で、狩猟社会、農業社会、工業社会、情報社会の次にくる社会として位置づけられている

■SSL/TLS

Web サーバと Web ブラウザとの通信において、データを暗号化して送受信する仕組みのこと。これにより、通信の途中で情報の盗聴・改ざんや、なりすましを防ぐことができる。過去には SSL が使われていたが、脆弱性が発見されたため、TLS（v.1.2 以降）への移行が進んでおり、今では SSL は使われなくなってきている。しかし、歴史的経緯で SSL の用語が広く普及しているため、本テキストでは「SSL/TLS」と表記する

■SWG

Secure Web Gateway の略。社内と社外のネットワーク境界で通信を中継する役割を持っている。また、やり取りしているデータを分析し、悪意のあるデータを遮断することによりセキュアな通信環境を実現

■VPN（Virtual Private Network）

Virtual Private Network の略。インターネット上で安全性の高い通信を実現するための手法。通信データを暗号化し、送信元から送信先までの通信を保護することにより、盗聴やデータの改ざんを防ぐ。VPN（Virtual Private Network）を使用することによって、ユーザーは物理的に独立した専用線で通信しているかのような安全な通信を行うことができる

■WAF（ワフ）

Web Application Firewall の略。 従来のファイアウォールが、IP アドレスとポート番号で通信を制御していたことに対して、Web アプリケーションの脆弱性を狙うサイバー攻撃を防ぐことを目的として、アプリケーションレベルで通信を制御（分析・検知・遮断）するファイアウォールのこと

■WAN

Wide Area Network の略。広義には、広い地域をカバーするネットワークのことで、インターネットとほぼ同義の言葉として使われる。

一方、狭義には、物理的に離れた場所にある LAN（オフィスのフロアや建物内など狭いエリアで構築されたネットワーク）同士を接するネットワークを指し、特定のユーザーしかアクセスできない。このプライベートな WAN を構築する場合には、通信事業者に依頼する必要がある

■アクセス制御

特定のデータやファイル、コンピュータ、ネットワークにアクセスできるユーザーを制限する機能のこと

■アセスメント

システムや運用環境などを客観的に調査・評価すること。現在の利用状況を把握することにより、システムの再構築や運用改善の参考情報となる

■暗号化

データの内容を変換し、第三者には、内容を見ても解読できないようにすること

■アンダーグラウンドサービス

合法ではない非公式な活動が行われるオンラインの闇市場やコミュニティでサイバー攻撃を目的としたツールなどを販売しているサービス

■イベントログ

コンピュータシステムに起こった出来事や、行われた操作などを時系列に記録したデータのこと

■インターネットバンキング

インターネットを利用して銀行との取引を行うサービスのこと。銀行の窓口や ATM に出向かなくても、スマートフォンやパソコンなどを使って、いつでも利用可能な時間帯に振り込みや残高照会などの取引を行うことができる

■ウイルス定義ファイル（パターンファイル）

セキュリティソフトウェアがマルウェアを検出するための定義情報が入ったファイル。実世界でいえば顔写真つきの手配書のようなもの

■エンティティ

個人、組織、団体、コンピュータシステム、通信機器など、多様な実体のこと

■エンドポイントデバイス

ネットワークに接続して、ネットワークを介して情報を交換するデバイス（パソコン、プリンタ、スキャナ、スマートフォン、仮想マシン、サーバ、IoT デバイスなど）

■改ざん

文書や記録などのすべてまたは一部に対して、無断で修正・変更を加えること。IT 分野では、権限を持たない者が管理者に無断でコンピュータにアクセスし、データの書き換え・作成・削除などをする行為

■可用性

許可された者だけが必要なときにいつでも情報や情報資産にアクセスできる特性

■完全性

参照する情報が改ざんされていなく、正確である特性

■機密性

許可された者だけが情報や情報資産にアクセスできる特性

■脅威インテリジェンス

サイバー攻撃などの脅威への対応を支援することを目的として、収集・分析・蓄積された情報のこと。一部の産業では、企業横断的にこうした情報（インテリジェンス）を共有する活動が行われている

■供給者

組織に対して、製品・サービスを供給する企業または個人のこと。製品の場合、PC やサーバ、通信機器などがある。サービスの場合、クラウドサービス、インターネット接続サービス、業務の委託、物流、教育などがある

■クラッキング

悪意を持って情報システムに侵入し、データの改ざん・機密情報の盗み出し・サーバ攻撃・情報システムの破壊などの行為

■クリーンインストール

すでにインストールされている OS を削除した上で、新しく OS を再インストールする方法のこと。記憶領域にあるデータはすべて消去されるので、データはバックアップから復元する必要がある

■限定提供データ

不正競争防止法で次のように定義されている。「業として特定の者に提供する情報として電磁的方法（電子的方法、磁気的方法その人の知覚によっては認識することができない方法をいう。次項において同じ。）により相当量蓄積され、および管理されている技術上または営業上の情報（秘密として管理されているものを除く。）をいう。」

■個人情報保護委員会

個人情報の有用性を考慮しながらも、個人の権利や利益を保護するために、個人情報の適切な取扱いを確保することを任務とする、独立性の高い行政機関（組織的には内閣府の外局）。個人情報保護法およびマイナンバー法に基づき、個人情報の保護に関する基本方針の策定・推進や個人情報などの取扱いに関する監視・監督、認定個人情報保護団体に関する事務などの業務を行っている

■コーディング

プログラミング言語でソースコードを書くこと

■コンパイル

プログラミング言語で書かれたプログラムを機械語に変換する作業

■サイバー攻撃

インターネットを通じて、別の企業や組織、ときに国家を攻撃する行為の総称。対象は、個人が所有するパソコンやスマートフォンから、企業のサーバやデータベース、国の重要インフラまでさまざまである。デジタル社会となった現代では、インターネット空間をサイバー空間と呼ぶ。サイバー空間において、敵対する国家、企業、集団、個人などを攻撃する行為やその防御をサイバー戦争と呼ぶこともある。

■サイバーセキュリティお助け隊サービス制度

「サイバーセキュリティお助け隊サービス」は、中小企業のセキュリティ対策に不可欠な各種サービスをワンパッケージにまとめた、民間事業者による安価なサービス。独立行政法人情報処理推進機構（IPA）は中小企業向けセキュリティサービスが満たすべき基準を設定しており、同基準を充足するサービスに「お助け隊マーク」を付与し、同サービスの普及促進活動を行っている

■サイバーセキュリティ戦略

組織や企業がセキュリティに関する目標を達成するための計画やアプローチ

■サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

単純なサイバー空間（仮想空間）におけるセキュリティ対策から、サイバー空間とフィジカル空間（現実空間）のそれぞれにおけるリスクを洗い出し、そのセキュリティ対策を整理するためのフレームワーク

■サプライチェーン

製品やサービスの供給に関わる一連のプロセスのこと。具体的には、原材料や部品の調達、生産、物流、販売など、製品やサービスが最終的に消費者に届くまでの流れを指す。サプライチェーンは、製造業者、卸売業者、小売業者などが協力して構築される

■サポートユーティリティ

情報システムを運用する施設の稼動に不可欠な設備やライフライン、公共インフラのこと。ISO/IEC 27002:2022

では、サポートユーティリティの例として、電気、通信サービス、給水、ガス、下水、換気、空調を挙げている

■シャドーIT

従業員が業務に使用する IT 機器やサービスのうち、企業が把握していないものを指す。具体的には、普段プライベートで使用しているオンラインストレージといったクラウドサービス、個人所有のデバイスなどで、組織の許可なく業務に利用しているもの

■磁気データ消去装置

ハードディスクに強力な磁気を照射することで、ハードディスク内の磁気記録領域に記録されている情報を破壊する装置のこと。短時間で効率よく、大量のハードディスクのデータを完全に消去できる

■ジャーニーマップ

一人のユーザーが目的を達成するための道のり（プロセス）を表に表したもの。

カスタマージャーニーマップともいう

■情報資産

営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報

■情報セキュリティ事象

情報セキュリティ上よくない、システムやサービス、ネットワークの状態のこと。

情報セキュリティ事象の中でも、事業運営を危うくしたり、情報セキュリティを脅かしたりする可能性が高いものは、セキュリティインシデントに分類される

■情報セキュリティの 3 要素「CIA」

情報セキュリティの 3 つの要素、機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）の頭文字をとって「CIA」と呼ぶ

■真正性

情報セキュリティマネジメントの付加的な要素で、利用者、プロセス、システム、情報などが、主張どおりであることを確実にする特性のこと。真正性を低下させる例としては、なりすまし行為などがある

■信頼性

システムが実行する処理に欠陥や不具合がなく、想定した通りの処理が実行される特性

■スクリーンセーバ

離席時に PC の画面の内容を盗み見されることを防ぐ機能のこと。PC に対して一定時間ユーザーによる操作がなかった場合、自動的にアニメーションや写真などを表示し、作業中の情報を見せないようにする

■スクリーンロック

デバイスの誤動作や勝手に操作されることを防ぐための機能。スクリーンロック画面になっているときはパスワードやロックパターンの入力、指紋や顔の認証をしなければ解除することができない

■脆弱性

情報システム（ハードウェア、ソフトウェア、ネットワークなどを含む）におけるセキュリティ上の欠陥のこと

■脆弱性診断

システムや機器などにおいて、セキュリティ上の欠陥がないか診断すること

■責任追跡性

情報資産に対する参照や変

更などの操作を、どのユーザーが行ったものかを確認することができる特性

■セキュリティインシデント

セキュリティの事故・出来事のこと。単に「インシデント」とも呼ばれる。例えば、情報の漏えいや改ざん、破壊・消失、情報システムの機能停止またはこれらにつながる可能性のある事象などがインシデントに該当

■セキュリティ・キャンプ

情報セキュリティに関する高度な技術と倫理に関する講習・演習を行う合宿。審査に通過した 22 歳以下の学生・生徒が対象。次代を担う情報セキュリティ人材を発掘・育成するために、独立行政法人情報処理推進機構（IPA）と（一財）セキュリティ・キャンプ協議会が実施している

■セキュリティホール

情報システムにおけるセキュリティ上の欠陥のこと。「脆弱性」とほぼ同義であるが、セキュリティホールは、ソフトウェアの設計上のミスやプログラムの不具合によって発生するセキュリティ上の脆弱性のみを指す場合がある

■セキュリティポリシー

企業や組織において実施する情報セキュリティ対策の方針や行動指針のこと。社内規定といった組織全体のルールから、どのような情報資産をどのような脅威からどのように守るのかといった基本的な考え方、情報セキュリティを確保するための体制、運用規定、基本方針、対策基準などを具体的に記載することが一般的

■ゼロデイ攻撃

OS やソフトウェアに存在する脆弱性が公開された後、修正プログラムや回避策がベンダーから提供されるまでの間に、その脆弱性を悪用して行われるサイバー攻撃のこと

■ゼロトラスト

従来の「社内を信用できる領域、社外を信用できない領域」という考え方とは異なり、社内外を問わず、すべてのネットワーク通信を信用できない領域として扱い、すべての通信を検知し認証するという新しいセキュリティの考え方

■ソフトウェアライブラリ

プログラムにおいてよく利用される機能を切り出し、再利用しやすいようにまとめたもので、プログラム作成のための部品のこと。ライブラリを利用することで、1 から作る必要がなくなり、効率的に開発を行うことができる

■ソリューション

問題や課題を解決するための具体的な解決策や手段を指す。ある特定の課題やニーズに対して提供される解決方法やアプローチのことを指すことが一般的で、ビジネスシーンにおけるソリューションの意味とは「顧客が抱える問題や課題を解決すること」

■ダークウェブ

特別な手法でないとアクセスできない、匿名性の高い非公開の Web サイトのこと。漏えいした個人情報や機密情報、危険な商品、クラッキングツールなど、違法なものが取引されている

■多要素認証

多要素認証は、サービス利用時において利用者の認証を行うために、3 つの要素（①利用者だけが知っている情報②利用者の所有物③利用者の生体情報）のうち、少なくとも 2

つ以上の要素を組み合わせて認証する安全性が高い認証方法。例えば、利用者が知っている情報としてはパスワード、利用者の所有物としては、スマートフォンの電話番号を用いたメッセージ認証、利用者の生体情報としては指紋認証や顔認識などがある。また、近年では FIDO2 と呼ばれる、デバイスを使用したパスキーによる認証により、パスワードレスでの認証が広まっている

■データサイエンス

数学、統計、人工知能などの技術を用いて、大量のデータを解析し、ビジネスに有益な知見を抽出すること

■データマスキング

個人情報や機密情報が含まれるデータを扱う際に、特定の部位のみを無意味な符号（アスタリスク「※」など）に置き換える処理のこと。もとのデータの一部を秘匿化し、個人や機密情報を識別できないようにすることで、データ分析やテストデータなどに利用可能とする

■デジタル化

紙などで管理されてきた情報（非デジタル情報）をデジタル化するデジタイゼーション（digitization）と、デジタル技術を用いてビジネスプロセスを自動化・合理化するデジタライゼーション（digitalization）がある。音楽ビジネスでいえば、アナログ記録のレコードを CD（コンパクトディスク）にすることがデジタイゼーション、音楽をダウンロード販売することがデジタライゼーションである

■デジタル情報

0、1、2 のような離散的に（数値として）変化する量で表現できる情報のこと。一般的にコンピュータ内部では「0」と「1」の 2 進数で表現されている。デジタル情報は劣化することがなく、整理・検索が容易であるという特徴がある

■デプロイ

実行ファイルをサーバ上に配置することで、ユーザーが利用できるようにすること

■トラフィック

通信回線やネットワーク上で送受信される信号やデータ、データ量のこと

■内部監査

内部の独立した監査組織が業務やシステムの評価、監査、アドバイスを行う活動である。情報セキュリティマネジメントシステム（ISMS）に関する国際規格である ISO27001 の監査では、ポリシーや規定、手順に適合し、各情報資産が確実に守られているか確認する

■ハウジングサービス

データセンターのラック（サーバを収容する鍵のついた棚）とサーバに接続する回線や電源を貸し出すサービスのこと。自社が所有しているサーバを、物理的にセキュリティが強固なデータセンターに設置し、運用できるため、セキュリティを強化できるメリットがある

■ビジネスインパクト分析

災害など不測の事態によって業務やシステムが停止した場合に、会社の事業に与える影響度を評価すること。BCP（事業継続計画）を立てる上で実行する必要がある

■ビジネスメール詐欺

攻撃者がビジネス用のメールを装い、企業の担当者をだまして、不正送金や機密情報の流出などの原因となる攻撃。BEC（ベック）Business Em

ail Compromise とも略される

■ビッグデータ

全体を把握することが困難な程、膨大な規模のデータ群

■否認防止性

システムに対する操作・通信のログを取得や本人に認証させることにより行動を否認させないようにする特性

■標的型攻撃

機密情報を盗み取ることなどを目的として、特定の個人や組織を狙った攻撃。業務関連のメールを装ったウイルスつきメール（標的型攻撃メール）を、組織の担当者に送付する手口が知られている。従来は府省庁や大手企業が中心に狙われてきたが、最近では地方公共団体や中小企業もそのターゲットとなっている

■標的型メール攻撃

特定の個人や組織を標的にしたフィッシング攻撃の一種。一般のフィッシング攻撃とは異なり、業界ニュースや社内情報といった情報を利用するため、業務上のメールと見分けがつかない内容や、業務で付き合いがある人物の名前で送られることもある

■ファイアウォール

本来は「防火壁」のことだが、情報セキュリティの世界では、外部のネットワークからの攻撃や不正なアクセスから企業や組織のネットワークやコンピュータ、データなどを守るためのソフトウェアやハードウェアを指す。パソコンの OS に付随しているもの、セキュリティソフトウェアについているもの、専用のハードウェアになっているものなど形態はさまざまである

■ファイル共有ソフト

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したソフトウェアのこと。不特定多数でファイルを共有するソフトは、自動的にファイルを送受信する仕組みであるため、ウイルスの感染によって、公開したくないファイルがインターネットに流出するトラブルなどが多く発生している。不特定多数でファイルを共有するファイル共有ソフトは、使用を禁止する必要がある

■不正アクセス

利用権限を持たない悪意のあるユーザーが、企業や組織で管理されている情報システムやサービスに不正にアクセスすること。不正アクセスにより、正規の個人情報の窃取やデータの改ざんや破壊などの危険がある。日本では、平成12年2月に施行された不正アクセス行為の禁止などに関する法律（不正アクセス禁止法）により、法律で固く禁じられている

■踏み台

不正侵入の中継地点として利用されるコンピュータのこと。他人のコンピュータに侵入するときに、直接自分のコンピュータから接続すると、接続元の IP アドレスによって、犯人が特定されてしまう可能性がある。そこで、いくつかのコンピュータを経由してから、目的のコンピュータに接続することにより、犯人が自分のコンピュータを探しにくくする。このように、現実的な被害はないけれども、不正侵入の中継地点としてのみ利用されるコンピュータのことを踏み台と呼ぶ

■フォレンジック

犯罪捜査における分析や鑑識を意味する言葉。サイバー

セキュリティの分野で使われる「フォレンジック」とは、セキュリティ事故が起きた際に、端末やネットワーク内の情報を収集し、被害状況の解明や犯罪捜査に必要な法的証拠を明らかにする取組を指す。「デジタル・フォレンジック」や「コンピュータ・フォレンジック」などと呼ばれる

■ブラックマーケット

広義には、不法な取引が行われる市場を指す。不正に入手した個人情報などを売買するインターネット上の市場（闇市）

■フレームワーク

フレームワーク（サイバーセキュリティフレームワーク）とは、マルウェアやサイバー攻撃などさまざまなセキュリティ上の脅威から、情報システムやデータを守るために、システム上の仕組みや人的な体制の整備を整える方法を「ひな型」としてまとめたもの

■プロキシ

クライアントとサーバの中間で、両者の通信を中継する役割を担うサーバのこと。

プロキシは、クライアントからのリクエストやサーバからの応答をすべて把握することが可能なため、詳細な通信内容をログとして記録したり、Web サーバから送られてきたコンテンツをチェックし、不正なコードやマルウェアが含まれていないかをチェックしたりできる

■ブロックチェーン

複数のコンピュータを使用し、分散的にデータをブロック単位にまとめて鎖（チェーン）のように記録する、オープンな分散型台帳。ビットコインなどの暗号資産に使われている仕組み

■ベストプラクティス

何かを行う方法や工程、その実践例の中で、ある基準にしたがって最も優れていると評価されたもののこと。実績や経験に基づいて確立された成功例や良い成果をもたらす方法論

■ペルソナ分析

理想とする顧客像を具体化し、典型的なユーザーのプロファイル分析をすること

■ベンダーロックイン

ソフトウェアの機能改修やバージョンアップ、ハードウェアのメンテナンスなど、情報システムを使い続けるために必要な作業を、それを導入した事業者以外が実施することができないために、特定の事業者（ベンダー）を利用し続けなくてはならない状態のこと

■マルウェア

パソコンやスマートフォンなどのデバイスやサービス、ネットワークに害を与えたり、悪用したりすることを目的として作成された悪意のあるソフトウェアの総称。コンピュータウイルスやワームなどが含まれる

■ミラサポコネクト

ビッグデータを活用して事業を伸ばしたい中小企業を応援するための「ミラサポコネクト構想」をもとにした、行政、支援者、民間事業者に分散して保有されているデータ（法人情報、決算情報、経営カルテなど）を連携し、経営課題解決に資する支援を提供するための、官民データ連携基盤

■ミドルウェア

OS とアプリケーションの中間に位置するソフトウェア

のこと。アプリケーションが業務に関する処理を行う際、データベースやサーバのやり取りをミドルウェアが担うことで複雑な処理を行うことができる

■無線 LAN

LAN は Local Area Network の略。物理的なケーブルを使わず、電波を利用してネットワークに接続する仕組み。この無線 LAN を通じて、コンピュータはインターネットなどのネットワークにアクセスすることができる

■無停電電源装置

UPS とも呼ばれる。停電が起きてしまったときに電気を一定時間供給し続けるための装置のこと。パソコンやハードディスク、サーバなどを予期せぬ停電から守れる

■ユーティリティプログラム

コンピュータで、システムの運用を支援するプログラムのこと。具体的には、記憶媒体間のデータ転送、ファイルの複写・削除・整理などの処理を行うためのプログラムのこと。システムおよびアプリケーションによる制御を無効にすることのできるものもある

■ランサムウェア

悪意のあるマルウェアの一種。パソコンなどのファイルを暗号化し利用不可能な状態とし、解除と引き換えに被害者から身代金（ransom）を要求する

■リスクアセスメント

企業や組織が持つ情報資産に対するリスクの分析・評価を行うプロセスのこと。具体的には情報資産の特定、脅威と脆弱性の特定と評価、リスクの分析と評価を行う。リスク評価の結果、許容できるもの以外は何らかのセキュリティ対策を講じる必要がある

■リスク評価

組織やプロジェクトにおける特定されたリスクに対して、重要度や影響度を評価するプロセス

■リモートデスクトップ接続

パソコン、タブレット、スマートフォンなどのデバイスを使用して、遠隔地から特定のパソコンに接続する方法