中小企業向け

サイバーセキュリティ実践ハンドブック

中小企業も安心！セキュリティ対策で DX を加速

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】

東京都産業労働局

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。

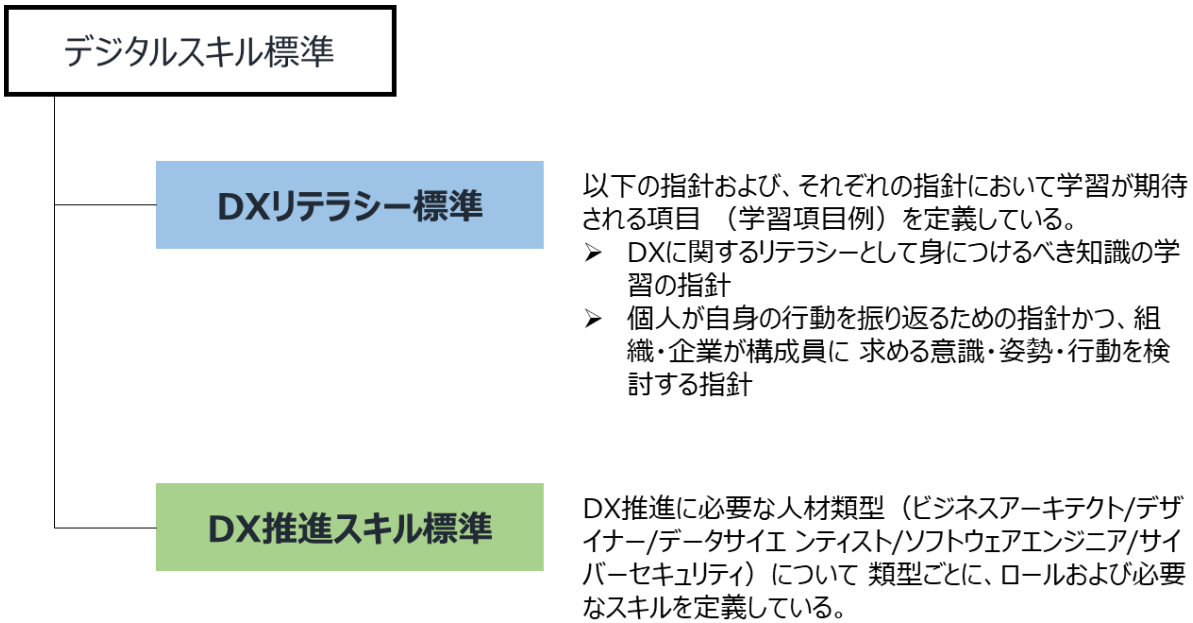


図 86. デジタルスキル標準の構成

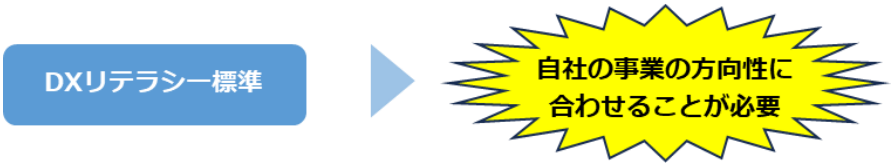
(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

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	https://www.meti.go.jp/policy/it_policy/jinzai/skill_standard/main.html
デジタルスキル標準 ver.1.2（PDF）	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 87. 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>社会の変化</td><td rowspan="5">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>顧客価値の変化</td><td>データを読む・説明する</td><td>ツール利用</td></tr>
<tr><td>競争環境の変化</td><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 rowspan="5"></td><td>データによって判断する</td><td>モラル</td></tr>
<tr><td rowspan="4">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="3"></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 88. 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の欲求の高まり）を知っている	● 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
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	● デジタル技術の活用による競争環境変化の具体的

	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	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	● 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	● データドリブンな判断プロセス

断する	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	● 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	● ネットワークの仕組み（LAN・WAN、通信

	● 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	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ュリティ対策
（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	● 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

	● データ流出の危険性や影響を想像できる	
（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。

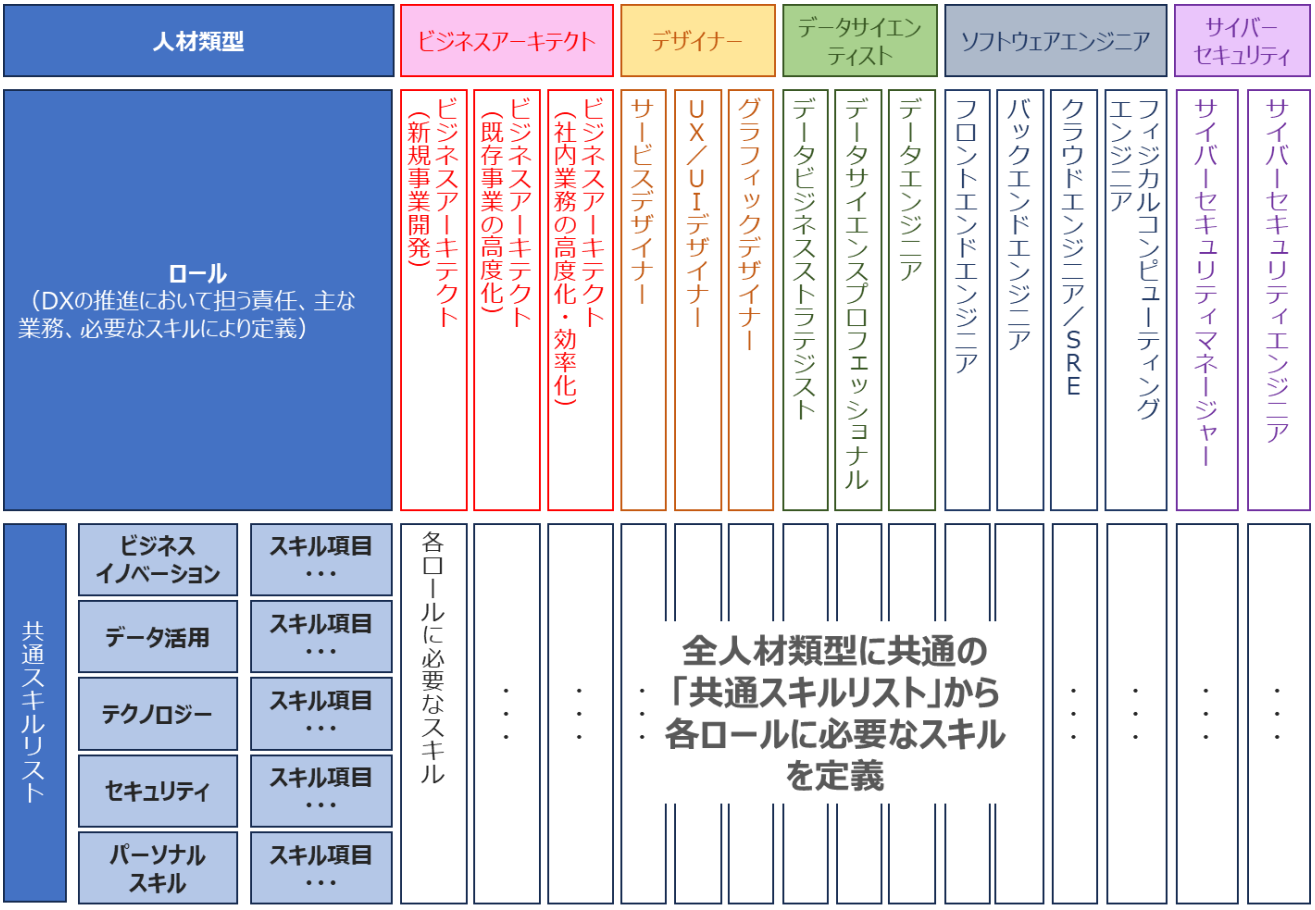


図 89. DX 推進スキル標準の構成

(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。

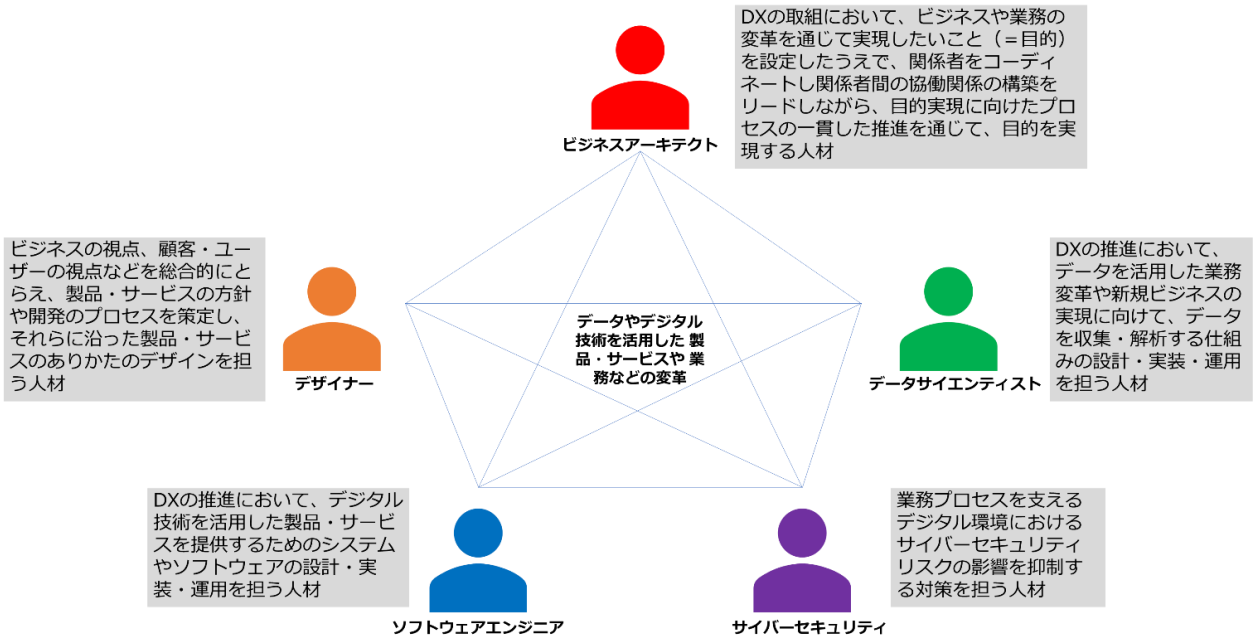


図 90. 人材類型の定義

(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
ソフトウェアエンジニア	フロントエンドエンジニア	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	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

	ニア	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
	セキュリティ技術	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 ● 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	● 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	● 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

			● 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	● 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。

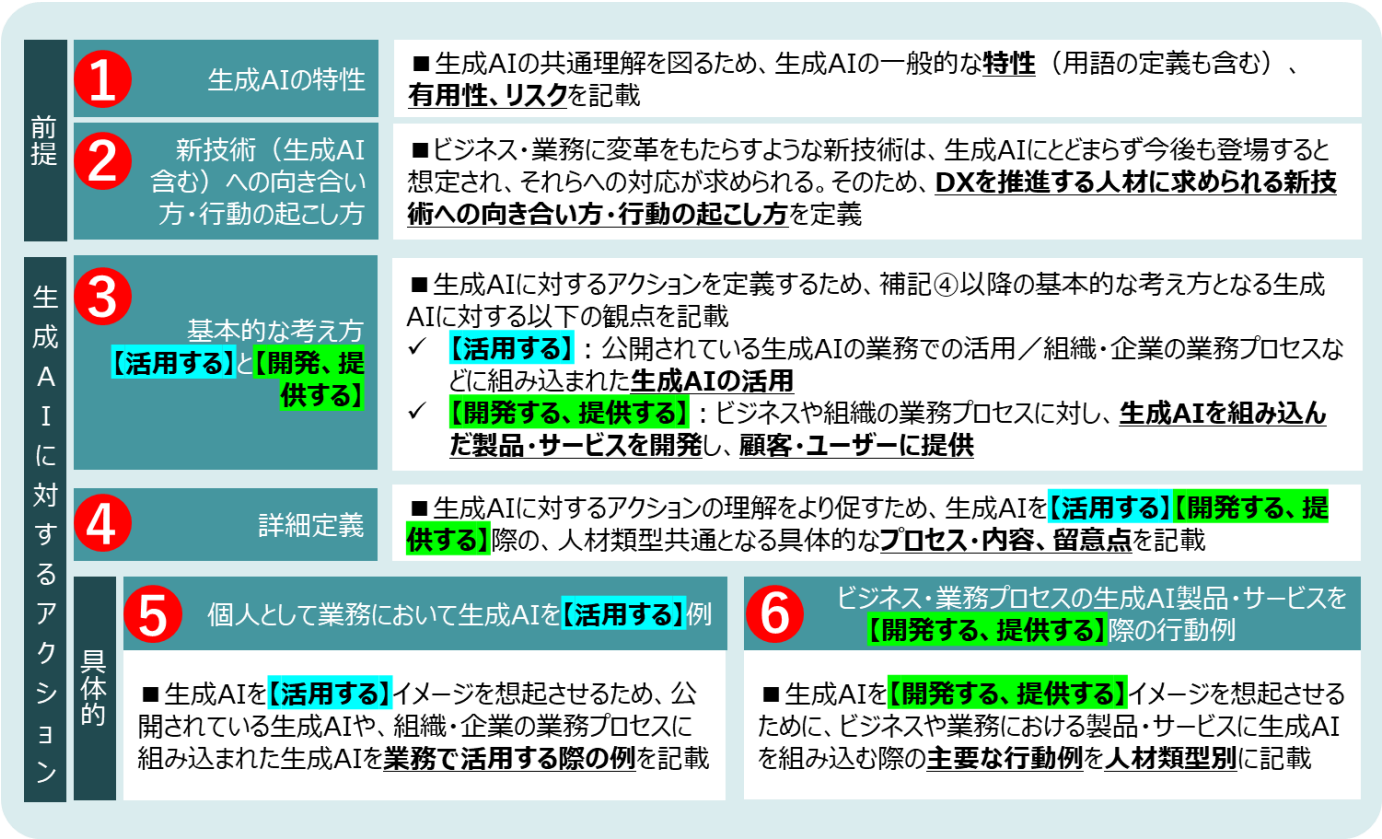


図 91. 生成 AI に関する DX 推進スキル標準

(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。

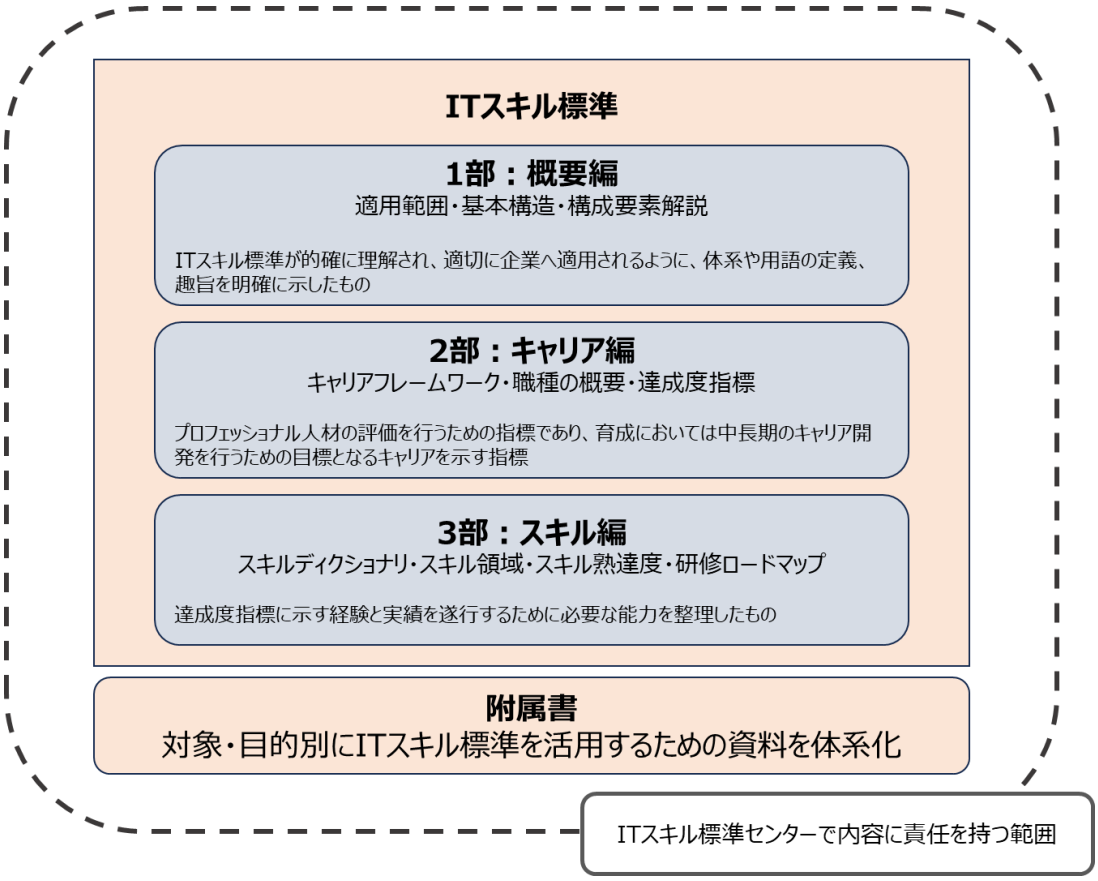


図 92. IT スキル標準の全体構造

(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	https://www.meti.go.jp/policy/it_policy/jinzai/skill_standard/main.html
デジタルスキル標準 ver.1.2（PDF）	https://www.ipa.go.jp/jinzai/skill-standard/dss/ps6vr700000083ki-att/000106872.pdf
IT スキル標準 V3	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/index.html
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。

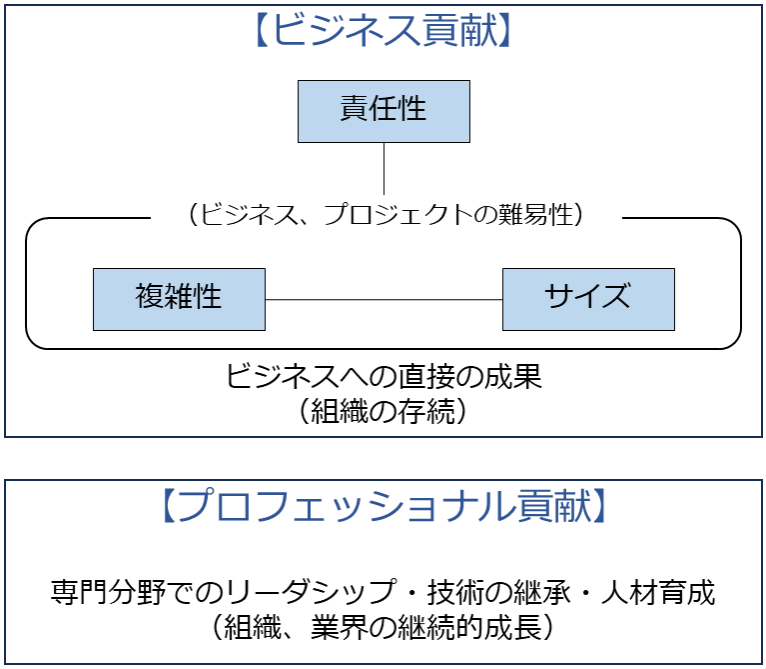


図 93. 達成度指標の構造

(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）	
IPA IT スキル標準 V3	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/index.html
IT スキル標準 V3 2011 2部：キャリア編（PDF）	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	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/index.html
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。

スキルカテゴリー一覧

スキルカテゴリー一覧			
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
		ブロックチェーン	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

詳細理解のため参考となる文献（参考文献）	
IPA ITSS+（プラス）データサイエンス領域	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/data_science.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

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	◎	◎
⑤	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）	
IPA ITSS+（プラス）アジャイル領域	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/agile.html
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

(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

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

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）	
IPA ITSS+（プラス）IoT ソリューション領域	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/iot_solution.html
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。

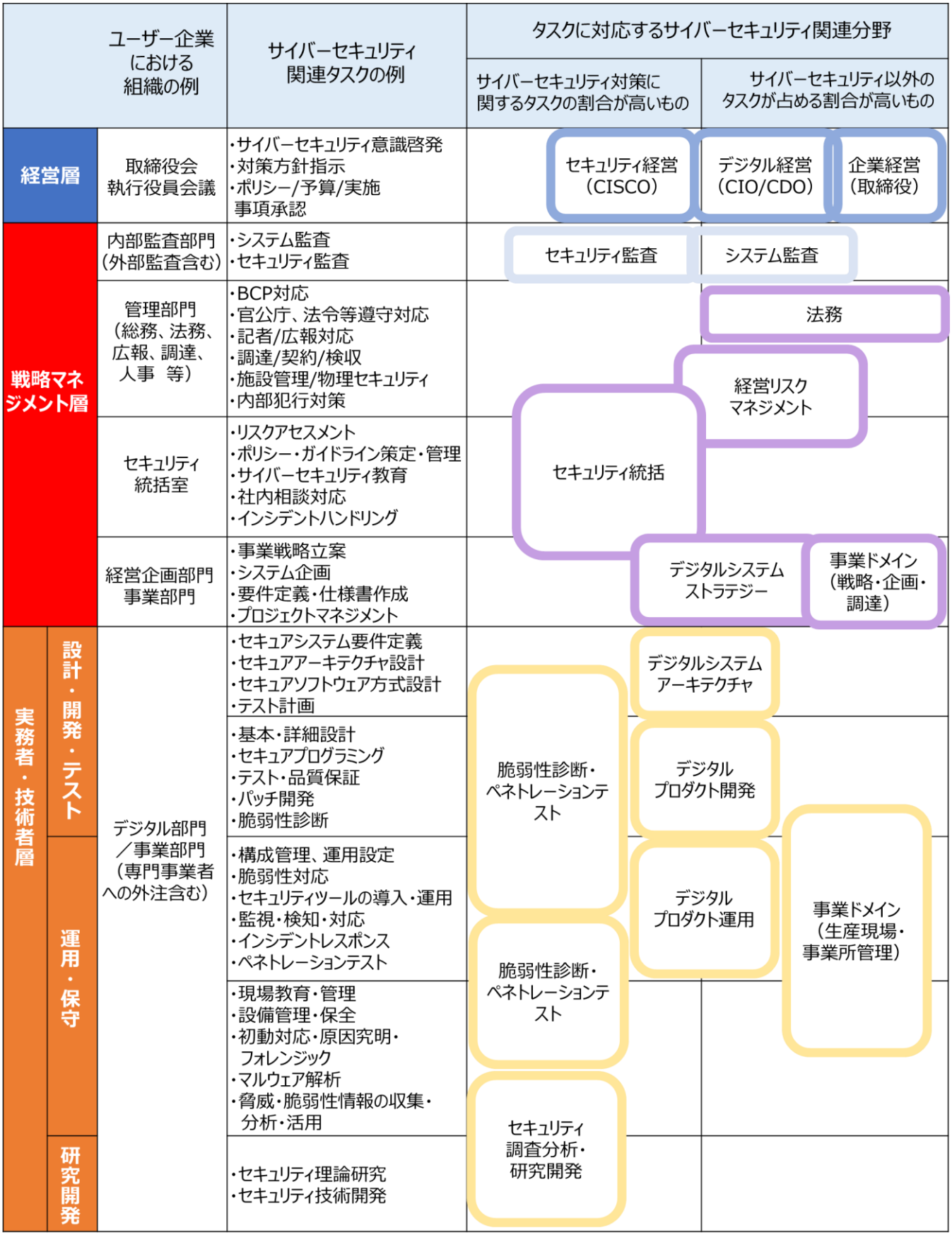


図 94. セキュリティ関連タスクを担う分野の概観図

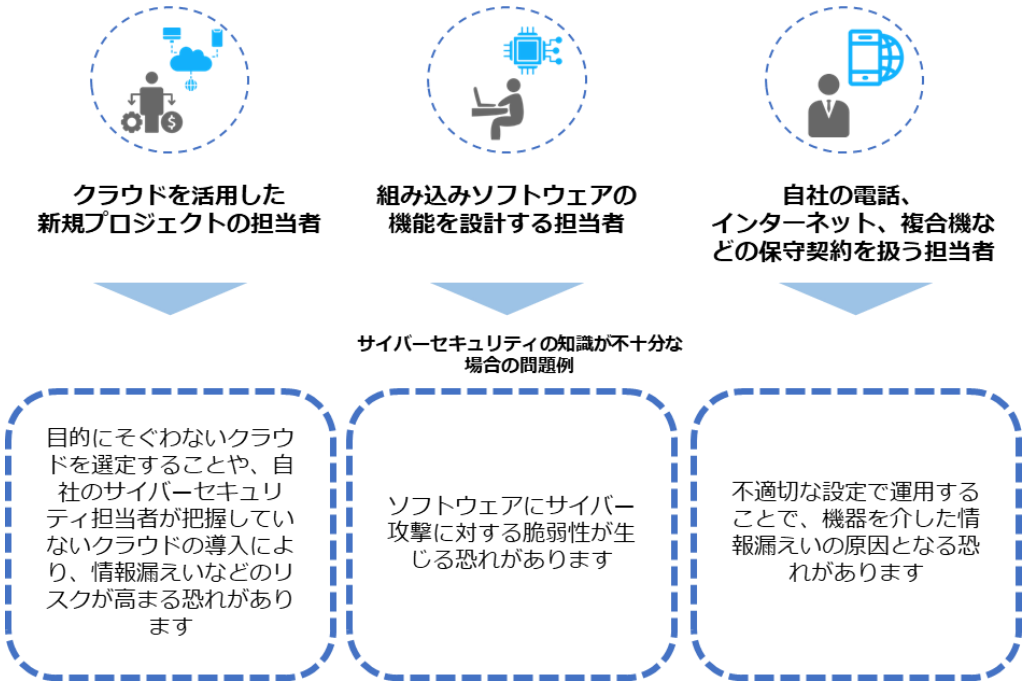
(出典) IPA「ITSS+（プラス）セキュリティ領域」をもとに作成

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。

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/curriculum/

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

NCO(国家サイバー統括室)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、NCO のサイトを参照してください。

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。

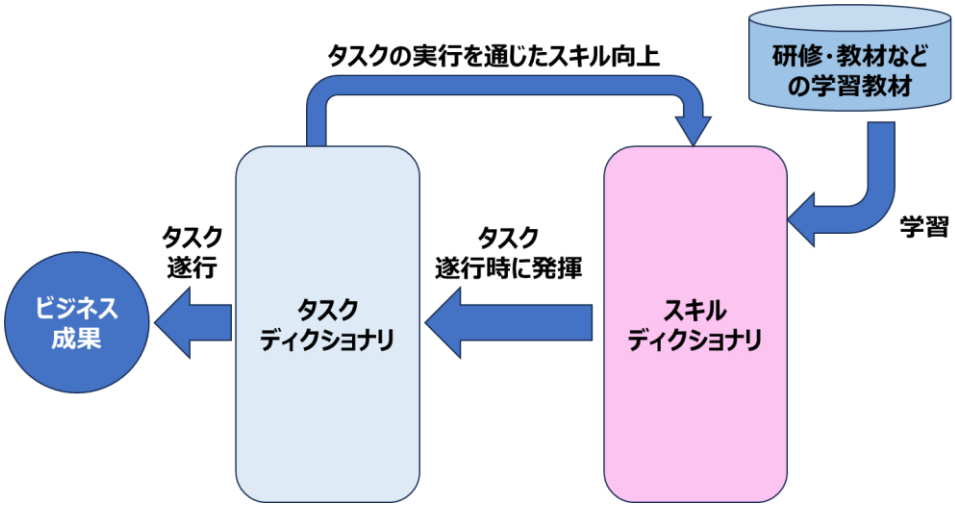


図 95. 業務遂行とディクショナリの働きの関係

(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。

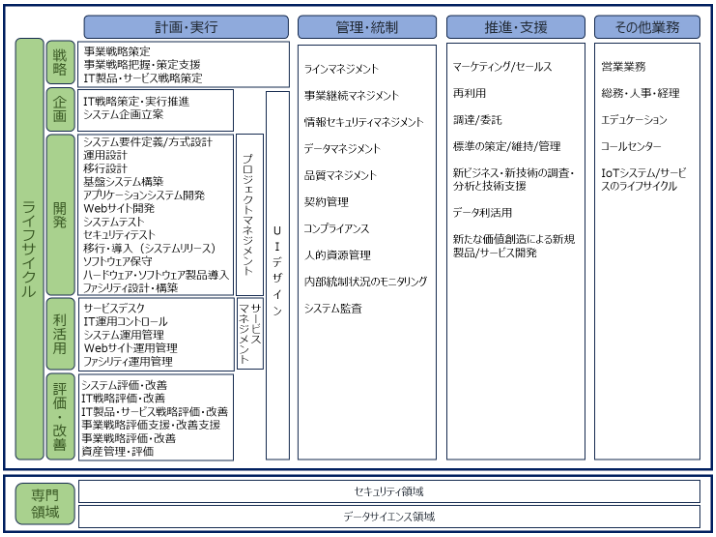
タスクディクショナリを構成する各コンテンツの関係は以下の通りです。

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

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

各タスクの属性情報 （特性、特徴）

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	自社向け情報システム開発・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 96. 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。

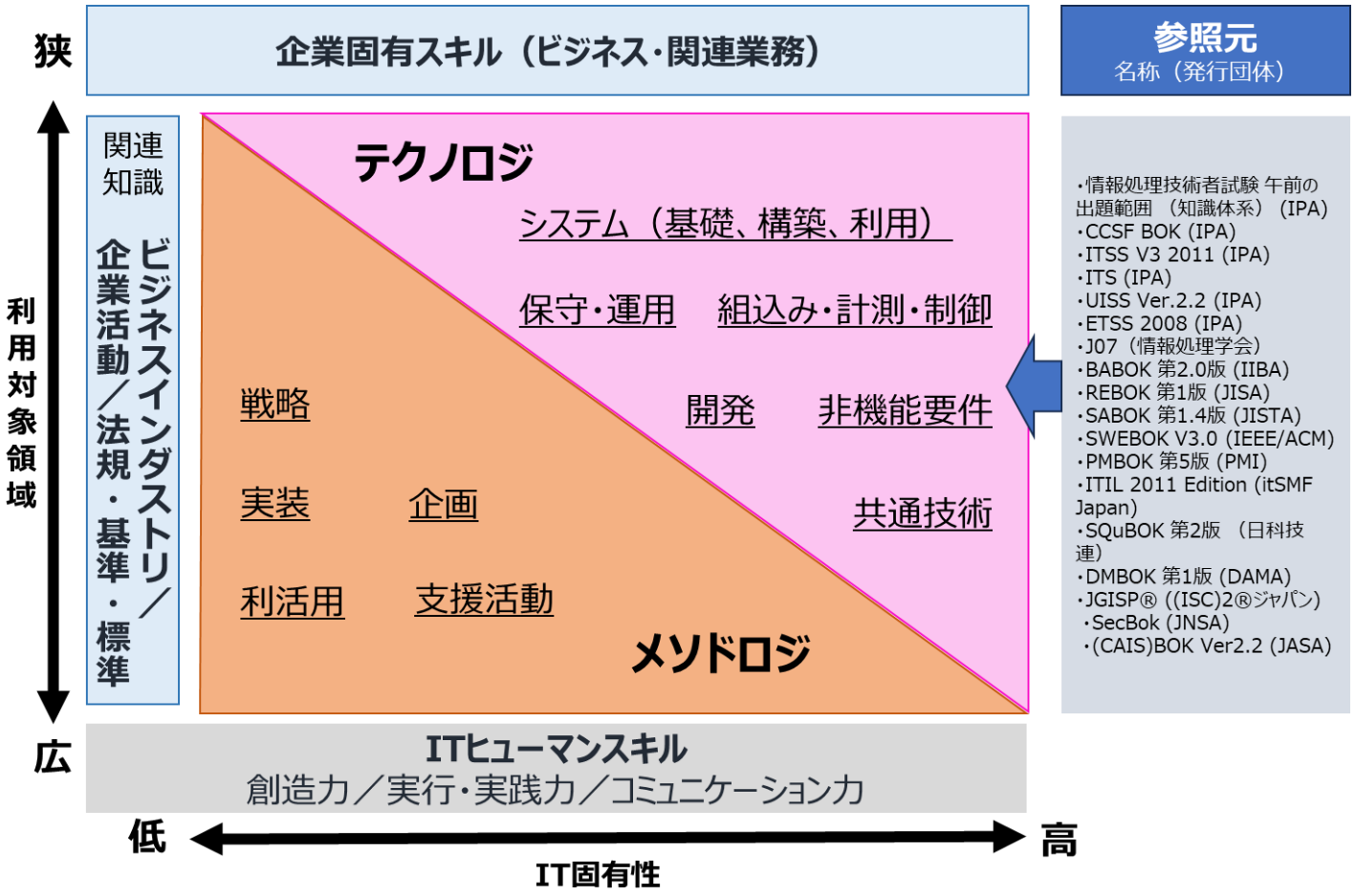


図 97. スキルディクショナリの構成
(出典) IPA「i コンピテンシディクショナリ解説書」をもとに作成

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

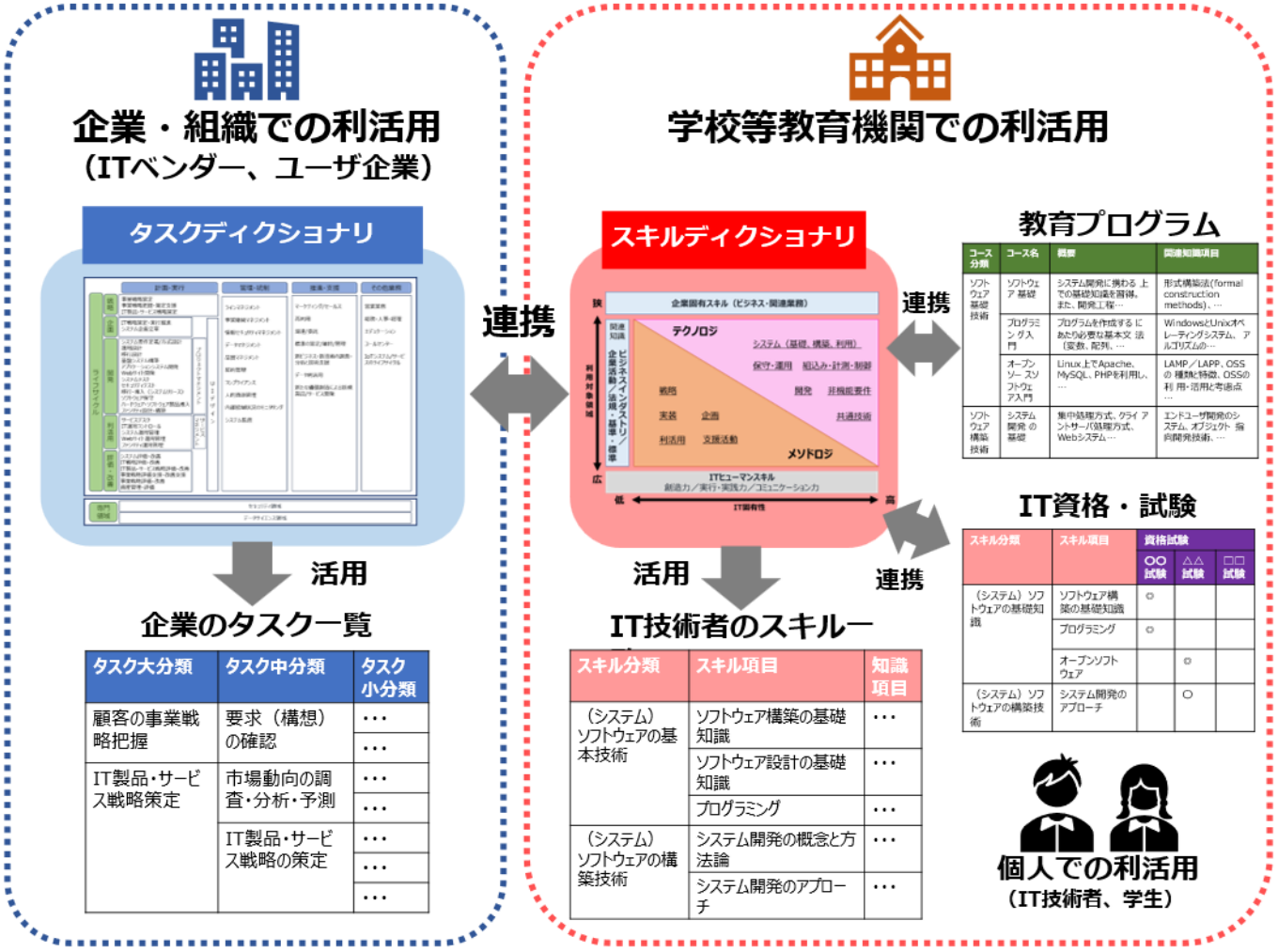


図 98. i コンピテンシ ディクショナリ（iCD）の利活用形態

(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。

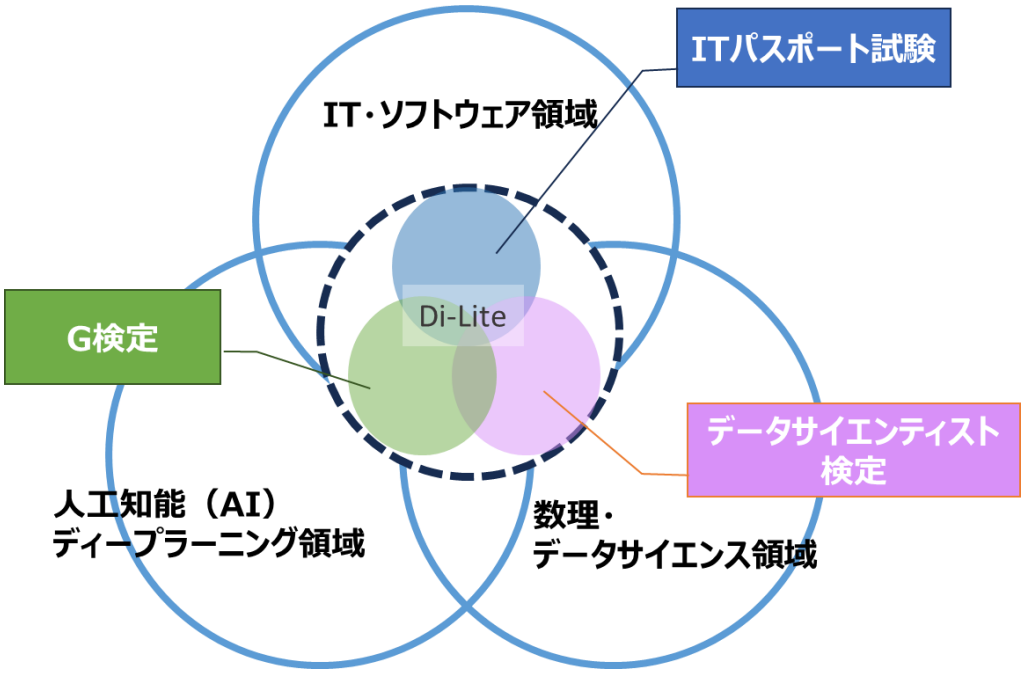


図 99. Di-Lite の 3 つの領域
(出典) デジタルリテラシー協議会「Di-Lite とは」をもとに作成

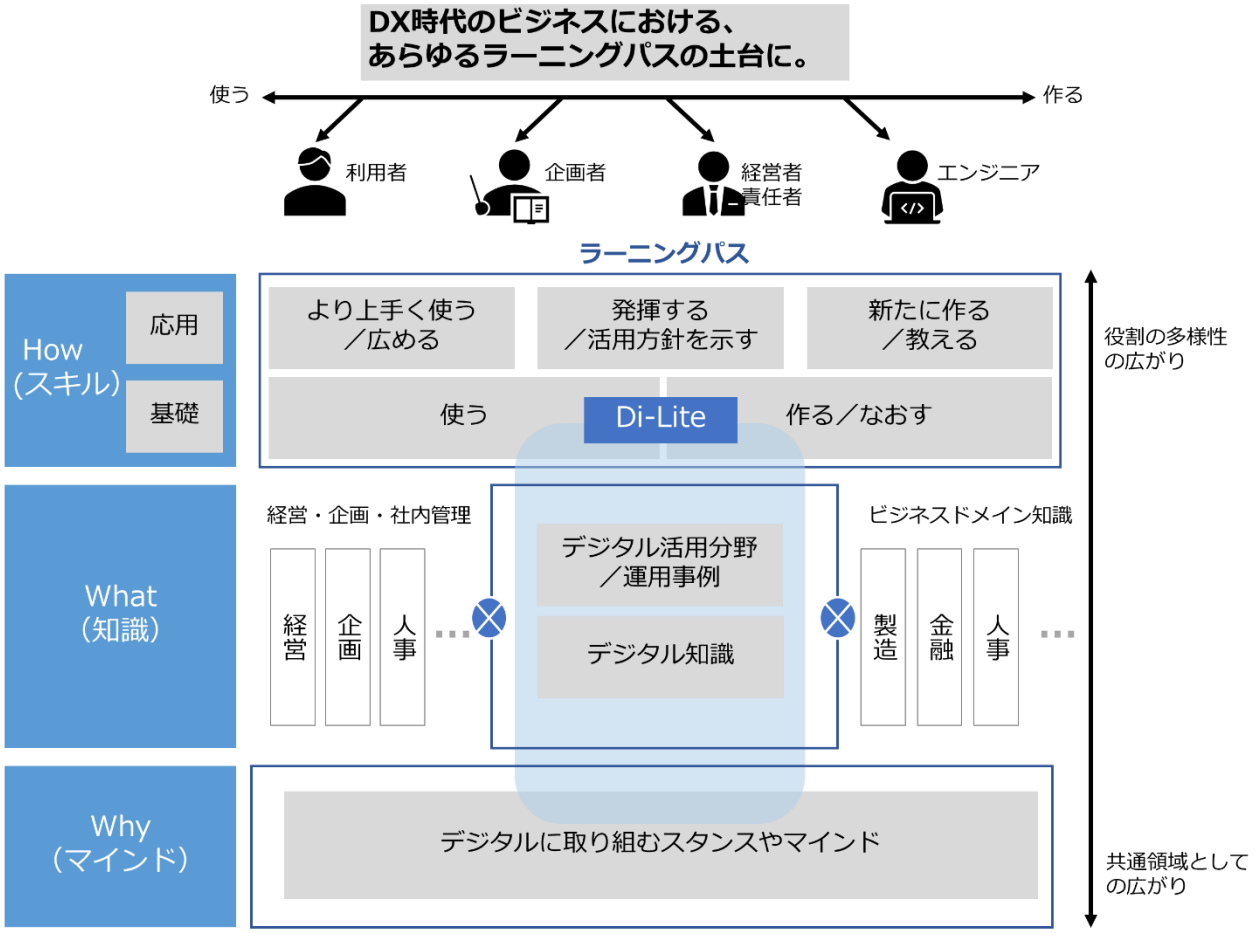


図 100. デジタルリテラシー・スキルフレームワーク

(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

① **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

② **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

③ 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 試験内容・出題範囲	https://www3.jitec.ipa.go.jp/JitesCbt/html/about/range.html
IT パスポート試験シラバス（Ver.6.4）	https://www.ipa.go.jp/shiken/syllabus/nl10bi0000007sxy-att/syllabus_ip_ver6_4.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
データサイエンスカ★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カ★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
ビジネスカ★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、「22-3-1.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/#
G 検定の試験範囲（シラバス）と例題	https://www.jdla.org/certificate/general/#general_No03

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。

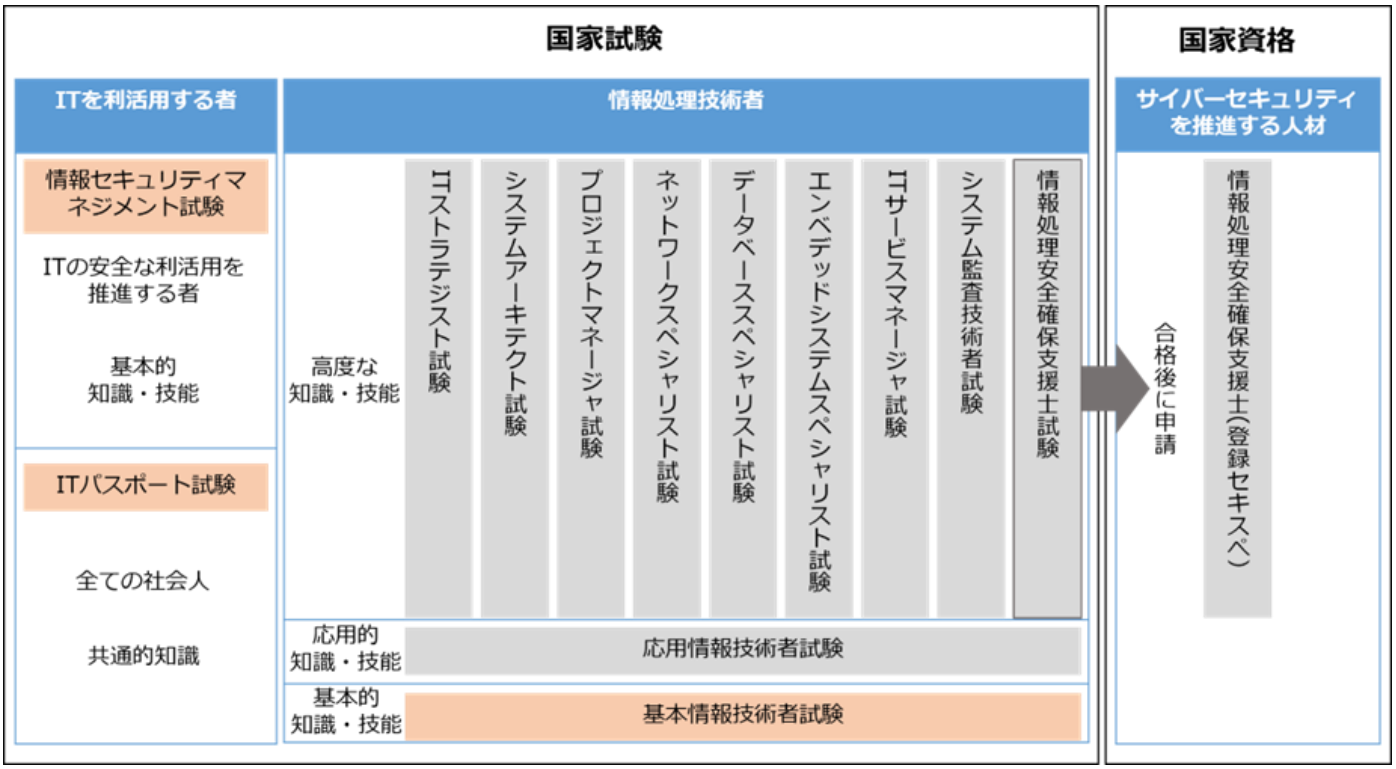


図 101. IT ヒューマンスキル概念図

(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、「23-1-1. 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）	
IPA 試験要綱・シラバスについて	https://www.ipa.go.jp/shiken/syllabus/gaiyou.html
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

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、「23-1-1. 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®とは	https://japan.isc2.org/cissp_about.html
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

第24章. 各種人材育成カリキュラム

章の目的
第 24 章では、知識やスキルを備えた人材の育成・確保に向けて、関係機関が公表しているセキュリティ関連のカリキュラム内容を把握することを目的とします。紹介するカリキュラム内容は、具体的な実施計画や実施内容を検討する際の参考資料となります。

主な達成目標
◘ 「プラス・セキュリティ知識補充講座 カリキュラム例」のカリキュラム内容を理解すること ◘ 「IT スキル標準モデルカリキュラム」のカリキュラム内容を理解すること ◘ デジタルスキル習得に関する講座を紹介する「マナビ DX」について概要と活用方法を理解すること

24-1. プラス・セキュリティ知識補充講座 カリキュラム例

「プラス・セキュリティ知識補充講座」は、国家サイバー統括室（NCO）が提供するプログラムで、特に経営層やデジタルトランスフォーメーション（DX）を推進する部課長向けに設計されています。この講座は、企業内外のセキュリティ専門人材との協働を円滑に行うために必要な知識を補充することを目的としています。

具体的には、以下のように経営層向けとデジタル化推進部門の部課長級マネジメント層向けの 2 つのカリキュラムで構成されています。

- 経営層
  企業のセキュリティリスクに対する理解を深め、経営判断に役立つ知識を提供。
- デジタル化推進部門の部課長級マネジメント層
  業務や製品・サービスのデジタル化を推進する役割を担う部門の管理職向けに、セキュリティリスク管理やデジタル化に伴うセキュリティ対策を強化する知識を提供。

理想とする目標

経営層（必ずしも DX を担当している部署の担当役員などではなく、経営層全体）

- サイバーセキュリティに関する動向が自社のコーポレートリスクに与える影響を的確に把握できる。
- 上記の影響を踏まえ、自社のセキュリティ体制構築・投資の決定・指示を的確に実行できる。
- 万一のインシデント発生時に、的確に経営判断を行い、指示をできる。

業務、製品・サービスのデジタル化を推進する部門のマネジメントを担う部課長級

- サイバーセキュリティに関する動向が自社の担当する事業・自部署に与える影響を的確に把握できる。
- 上記の影響を踏まえつつ、自部署で実施されている対策の現状を理解できる。
- 上記について、経営層が的確な経営判断をできるよう、自ら説明・報告できる。
- 上記を実施するために、社内（情報システム部門など）・社外（ベンダーなど）と、円滑にコミュニケーションできる。

（出典）NISC「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

このカリキュラムは、企業内研修のプログラムを策定する際に参考にできるよう設計されており、対象別の目標・到達レベルは以下の通りです。

カリキュラム受講後の到達レベルは、以下の表の「中」のレベルを想定しています。つまり、専門家との意見交換ができるレベルを目指したものとなっています。

	理解	コミュニケーション	評価・分析	判断
高	自らの役割に必要な知識を概ね網羅的に習得し、理解している	自ら把握すべきことを洗い出し、専門家を含む適切な対象者に回答を求めることができる	脅威や脆弱性が自組織に及ぼす影響を評価できる	自らの知識のみで、自組織での対応に関する適切な判断ができる
中	**自らの役割に必要な知識の全体像を把握した上で、その一部について理解していることを自覚している**	**専門家との意見交換ができる**	**脅威や脆弱性がどのように自組織に影響を及ぼすのかを理解できる**	**専門家の判断について、根拠を理解して合意を与えることができる**
低	サイバーセキュリティ関連文書に用いられる用語の意味を理解している	専門家からの説明を概ね理解することができる	脅威や脆弱性とは何かを理解している	自らの知識のみでは判断に関与することが困難

カリキュラム例の構成は以下の通りです。

	経営層向け	部課長級向け
目標	● サイバーセキュリティが自社のコーポレートリスクに与える影響の把握 ● 影響を踏まえた自社のセキュリティ体制構築・投資の決定・指示 ● インシデント発生時の適切な経営判断・指示	● サイバーリスクが自部署に与える影響理解 ● 自部署で実施されている対策の現状理解 ● 上記の経営層への報告 社内外とのコミュニケーション
時間設定	7.5時間（集合講習3時間＋オンデマンド4.5時間（うち必須3時間））	11時間（集合講習4.5時間＋オンデマンド6.5時間（うち必須5.5時間））
留意点	● 経営会議及び対外対応として実際に起こり得るケースから逆算 ● 各コマのインプット項目では、部課長級向けから内容を限定・変更	● 部署内会議やベンダー管理で実際に起こり得るケースから逆算 ● 既存のスキルなどフレームワーク（SP800-181等）と紐付けを実施
1.基礎知識	① デジタルインフラの基本（30分）◇ ② デジタル技術の基盤とリスク（30分）◇ ③ デジタル環境のコストと運用責任（30分）◇	① デジタルインフラ入門（20分）◇ ② サイバーセキュリティに関する用語の意味（20分）◇ ③ デジタル環境の管理や責任に関するキーワード（20分）◇ ① デジタルインフラの要点（30分）◆ ② デジタル技術の基盤とリスク（30分）◆ ③ デジタル環境のコストと運用責任（30分）◆
2.脅威と対策	① サイバー攻撃手法とそのトレンド（30分）◆ ② 脅威への対策（30分）◆ ③ 事例紹介（実際のサイバー攻撃事例の紹介、サイバー攻撃のデモンストレーション など）（30分）★	① サイバー攻撃手法とそのトレンド（30分）◆ ② 脅威への対策（30分）◆ ③ 事例紹介（実際のサイバー攻撃事例の紹介、サイバー攻撃のデモンストレーション など）（30分）★ ④ 演習1：脅威と対策における“悪い見本”から学ぶ（60分）★
3.投資	① コーポレートリスクとしてのサイバーセキュリティ（コンプライアンスを含む）（30分）◆ ② 体制構築・人材確保（30分）◆ ③ 演習1：各種対策の費用、損失想定、確率値から必要な投資を検討（70分）★	① サイバーセキュリティのリスクマネジメントの特徴（30分）◆ ② 対策における費用と損失の考え方（30分）◆ ③ リスクマネジメントのケーススタディ（30分）★ ④ 演習2：自部署リスクとその対応策を洗い出し、リスク管理部門などへ説明（60分）★
4.SHとの関係	① インシデント対応における経営層の役割（30分）◆ ② 通常時の備えと情報開示の在り方（30 分）◆ ③ インシデント対応と情報開示の事例から学ぶ（30分）★ ④ 演習2：インシデント発生時の模擬記者会見（50分）★	① インシデント対応プロセスとその準備（30分）◆ ② 通常時の備えとインシデント情報の取扱上のポイント（30分）◆ ③ インシデント対応と情報開示の事例から学ぶ（30分）★ ④ 演習3：インシデント発生時の社内外連絡（60分）★
5.関係法令	-	① サイバーセキュリティに関する国内法令とその読み方（20分）◆ ② サイバーセキュリティに関する基準・規格など（20分）◆ ③ サイバーセキュリティに関するガイドラインなど（20分）◆

★：集合講習での開催が推奨されるもの（受講必須）

◆：オンライン・オンデマンド形式での実施を想定（受講必須）

◇：オンライン・オンデマンド形式での実施を想定（受講任意）

(出典) NISC「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

24-1-1. 経営層向けカリキュラム例

経営層向けカリキュラム例を紹介します。カリキュラムは、４単元で構成されます。

経営層向け第１単元	
名称	1.基礎知識

	『デジタルシステムとサイバーセキュリティの概要』
目標	● デジタルシステムとそのサイバーセキュリティ対策に関して経営層として次のような場面において適切な判断を行う上で、どのようなことを予め知っておくべきなのかの自覚を促す。 ➢ 担当者による提案についての、自社のニーズ、競争力、コストなどの面からの妥当性 ➢ 新たな施策に伴うリスクとその抑制策の妥当性
到達レベル	● 関係者とのコミュニケーションにおいて用いられる概念と用語について、コミュニケーションに支障の無い程度の理解を得る。

経営層向け第 2 単元	
名称	**2.脅威と対策** **『サイバー空間における脅威と対策』**
目標	● 脅威および脆弱性とその対策に関する理解を通じて、サイバー空間における主要な脅威を事業上のリスクとして適切に把握できるようになる。
到達レベル	● 現在のデジタル環境では脆弱性による影響をゼロにできず、最新の脅威につねに対処していく必要があることを理解し、対策をしなかった場合の自社での被害想定ができるようになる。

経営層向け 第 3 単元	
名称	**3.投資** **『サイバーセキュリティと投資対効果』**
目標	● どのような場合にサイバーセキュリティリスクが企業価値の毀損を生じさせるのかを理解し、それを防ぐために日常でサイバーセキュリティ対策としてどのような投資などの方策を行うべきかに関して適切な判断を行えるようになる。
到達レベル	● 自社におけるサイバーセキュリティリスクを特定し、対応の優先順位付けや対処方針の選定を行うとともに、その実現に必要な体制構築や人材確保・育成に関する指示を行えるようになる。 ● セキュリティ対策の担当者から提示されるセキュリティ対策案について、経営層として妥当性に関する判断を下せるようになる。

(出典) NCO「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

経営層向け 第 4 単元	
名称	**4.ステークホルダーとの関係** **『サイバーセキュリティと企業価値』**
目標	● サイバーセキュリティインシデントの発生時の適切な対応について理解した上で、企業価値を損なわないためにあらかじめ備えておくべきことを自社の事情に応じてイメージできるようになる。
到達レベル	● 自社におけるインシデント対応を含むサイバーセキュリティ対策に関する取組方針について、対外的に説明や意見交換ができるレベルの理解に到達する。

カリキュラム例の詳細については、「付録：プラス・セキュリティ知識補充講座カリキュラム例の詳細」に記載しています。

詳細理解のため参考となる文献（参考文献）	
NCO プラス・セキュリティ知識	https://security-portal.nisc.go.jp/dx/plussecurity.html
プラス・セキュリティ知識補充講座 カリキュラム例	https://security-portal.nisc.go.jp/dx/pdf/plussecurity_curriculum.pdf

24-1-2. 部課長級向けカリキュラム例

部課長級向けカリキュラム例を紹介します。カリキュラムは、5 単元で構成されます。

部課長級向け 第 1-1 単元	
名称	**1.基礎知識** **『デジタルシステムとサイバーセキュリティの概要（初級編）』**
目標	● デジタル化を推進する部門のマネジメントを担う部課長として中級編の目標に到達するために必要となる、最低限の基礎知識を習得する。
到達レベル	● デジタルシステムとインターネットおよびそれらのセキュリティ対策において用いられる最低限の知識を習得する。

部課長級向け 第 1-2 単元	
名称	**1.基礎知識** **『デジタルシステムとサイバーセキュリティの概要（中級編）』**
目標	● デジタル化を推進する部門のマネジメントを担う部課長として次のような場面において適切な判断を行う上で、どのようなことを予め知っておくべきなのかの自覚を促す。 ➢ 担当者による提案についての、自社のニーズ、競争力、コストなどの面からの妥当性

	➢ 新たな施策に伴うリスクとその抑制策の妥当性
到達レベル	● デジタルシステムとサイバーセキュリティに関する用語と概念について、第 2 単元目以降の学習を行うために予め習得しておくべきレベルに到達させる。具体的には、対象とする用語と概念を用いて、デジタルシステムやサイバーセキュリティ対策に関するソリューションを提供するベンダーとの実用的な対話に支障の無い程度の理解を得ることにする。

部課長級向け 第 2 単元	
名称	**2.脅威** **『サイバー空間における脅威と対策』**
目標	● 脅威および脆弱性とその対策に関する理解を通じて、サイバー空間における主要な脅威を事業上のリスクとして適切に把握できるようになる。
到達レベル	● 現在のデジタル環境では脆弱性による影響をゼロにできず、最新の脅威につねに対処していく必要があることを理解し、対策をしなかった場合の自社での被害想定ができるようになる。

部課長級向け 第 3 単元	
名称	**3.投資** **『サイバーセキュリティとリスク対応』**
目標	● 自部署におけるサイバーセキュリティリスクのマネジメントに必要となる概念と、具体的なアクションについて理解する。
到達レベル	● 部署におけるサイバーセキュリティリスクを特定し、対応の優先順位付けや対処方針の選定を行うとともに、その実現に必要な体制や要員の確保・育成を行えるようになる。 ● 担当者や社外ベンダーから提示されるセキュリティ対策案について、組織として妥当性に関する判断を下せるようになる。

部課長級向け 第 4 単元	
名称	**4.ステークホルダーとの関係** **『サイバーセキュリティ対応における社内外連携』**
目標	● デジタル化を推進していく際のサイバーセキュリティ対策、運用時のインシデントへの適切な対応について理解した上で、その効果を担保するために実施すべき情報開示や連絡の内容と効果的な方法について理解し、実践できるようになる。

到達レベル	● 自部署に係るサイバーセキュリティ対策に関する社内外のコミュニケーション（情報収集、協議、エスカレーションなど）について、実用レベルで実施できる。

部課長級向け 第 5 単元	
名称	**5.関連法令** **『サイバーセキュリティに関する法制度』**
目標	● サイバーセキュリティ対策で関連する法律、基準、ガイドラインなどについて、実用上支障が無い程度の理解を得る。
到達レベル	● デジタル化に関連する取組の中で、遵守すべき法律、基準、ガイドラインなどを意識することができる。

(出典) NCO「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

カリキュラム例の詳細については、「付録：プラス・セキュリティ知識補充講座カリキュラム例の詳細」に記載しています。

詳細理解のため参考となる文献（参考文献）	
NCO プラス・セキュリティ知識	https://security-portal.nisc.go.jp/dx/plussecurity.html
プラス・セキュリティ知識補充講座 カリキュラム例	https://security-portal.nisc.go.jp/dx/pdf/plussecurity_curriculum.pdf

24-2. IT スキル標準モデルカリキュラム【IT スキル標準 V3（レベル 1)】

IT スキル標準（ITSS）については、22 章で説明しましたが、各種 IT 関連サービスの提供に必要とされる知識やスキルを体系化した指標であり、産学における IT サービス・プロフェッショナルの教育・訓練などに有用な「ものさし」（共通枠組）を提供しようとするものです。

IT スキル標準は、11 の職種と 35 の専門分野を設け、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。

「IT スキル標準モデルカリキュラム」は、IT スキル標準のレベル 1～3 を目指す人向けのカリキュラムとして IPA から公開されているものですが、ここではレベル 1 向けのモデルカリキュラムを紹介します。

このカリキュラムは、職業人として備えておくべき、情報技術に関する共通的な基礎知識を修得することを目指す社会人や学生を対象としたカリキュラムであり、研修ロードマップをもとに、具体的な研修コースを設計･実施する際に参考となる情報がまとめられています。このモデルカリキュラムを履修することにより、IT スキル標準のレベル 1 に相当する知識を修得することができます。

IT スキル標準モデルカリキュラムの構成

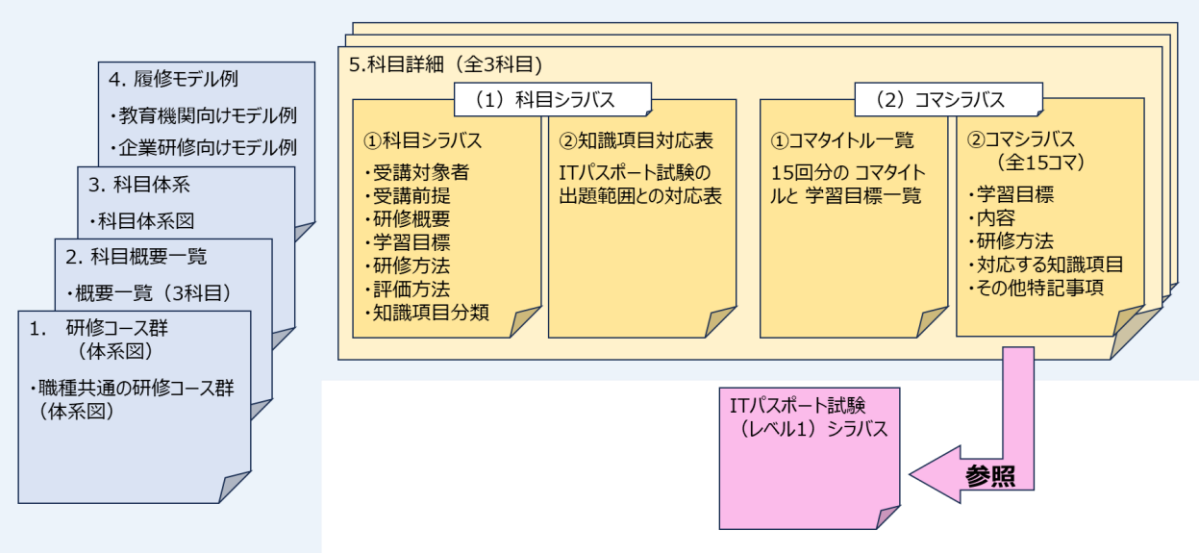


図.102 「IT スキル標準モデルカリキュラムの構成」

(出典) IPA「IT スキル標準モデルカリキュラム－レベル 1 を目指して－」をもとに作成

IT スキル標準のレベル 1 モデルカリキュラム（科目概要一覧）

対象人材	① 本格的な就業経験のない学生 ② IT に関する基本的な知識を持たない社会人
対象場面	① 企業：IT 系企業を含め企業などの内定者の入社前研修など ② 教育機関：情報系、非情報系のすべての学部、学科における教育。ただし、情

	報系専門学科においては一般教養課程における教育
特徴	● 特定の製品や分野に偏らない知識と体系的なパーソナルスキルを修得できます。 ● IT パスポート試験の出題範囲と整合し、科目およびコマシラバスごとに知識項目との対応が明らかになっているので、「IT パスポート試験（レベル 1）シラバス」と併用することでより一層の研修効果を図ることができます。

このカリキュラムでは「IT 基本 1」コース群に含まれるコース「IT 入門」と「パーソナルスキル入門」に対応する科目が策定されています。

科目名	概要	受講対象者／受講前提	構成	時間
IT 入門（1）	「IT 基本 1」コース群の 1 つとして、ストラテジおよびマネジメント分野の基本的かつ普遍的な知識の修得を目的とする。具体的には、企業における経営戦略と担当業務の関連、システム開発のライフサイクル、プロジェクトマネジメント、サービスマネジメントおよびシステム監査などの知識を学習する。	IT スキル標準のレベル 1 を目指す者/前提科目は特にないが、高校卒業程度の知識を有していること	90 分×15 回	22.5h
IT 入門（2）	「IT 基本 1」コース群の 1 つとして、テクノロジ分野の基本的な知識の修得を目的とする。具体的には、情報のデジタル化とアルゴリズム、ハードウェア、ソフトウェア、ネットワーク、データベースおよびセキュリティに関する基本的な知識を学習する。	IT スキル標準のレベル 1 を目指す者/「IT 入門（1）」を修了していること、または同等の知識を有していること	90 分×15 回	22.5h
パーソナルスキル入門	パーソナルの領域に関して職業人として基本的な要件である、チームワークに基づくリーダーシップ、コミュニケーションの基本（書く、話す、聞く、考える）、プレゼンテーションの基本、論理展開（問題解決）法の基本、基本的なビジネスマナー、更に IT を活用する上で求められるパーソナルスキルの概要などを学習する。	IT スキル標準のレベル 1 を目指す者/前提科目は特にないが、高校卒業程度の知識を有していること	90 分×15 回	22.5h

(出典) IPA「IT スキル標準モデルカリキュラム－レベル 1 を目指して－」をもとに作成

IT 入門（1）

科目シラバス

科目	IT 入門（1）
職種	職種共通
レベル区分（対象者）	IT スキル標準のレベル 1 を目指す者
受講前提	前提科目は特にないが、高校卒業程度の知識を有すること
学習目標	職業人として IT（情報技術）の基本的な知識を活用し、上位者の指導の下、業務の分析と解決およびシステム化の支援を行うことができる
研修・教育方法	講義、演習
修得スキルの評価方法	講義終了後の受講レポート、定量アンケート、知識確認テスト、演習問題の取組状況を総合的に判断して評価を行う
カリキュラム構成	1 コマ 90 分×15 回（総時間：22.5 時間）
知識項目分類	【分野】ストラテジ系 【大分類】 1.企業と法務 【中分類】 1 企業活動 2 法務 2.経営戦略 【中分類】 3 経営戦略マネジメント 4 技術戦略マネジメント 5 ビジネスインダストリ 3.システム戦略 【中分類】 6 システム戦略 7 システム企画 【分野】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 9 ソフトウェア開発技術 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 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 12 システム監査

(出典) IPA「IT スキル標準モデルカリキュラム－レベル 1 を目指して－」をもとに作成

コマタイトルの例については、「付録：IT スキル標準レベル 1 コマタイトル一覧」に記載しています。

IT 入門（2）

科目シラバス

科目	IT 入門（2）
職種	職種共通
レベル区分（対象者）	IT スキル標準のレベル 1 を目指す者
受講前提	「IT 入門（1）」を修了していること、また同等の知識を有していること
学習目標	職業人として IT（情報技術）の基本的な知識を活用し、上位者の指導の下、業務の分析やシステム化の支援や情報の活用ができる
研修・教育方法	講義、演習
修得スキルの評価方法	講義終了後の受講レポート、定量アンケート、知識確認テスト、演習問題の取組状況を総合的に判断して評価を行う
カリキュラム構成	1 コマ 90 分×15 回（総時間：22.5 時間）
知識項目分類	【分野】テクノロジ系 【大分類】 7 基礎理論 【中分類】 13 基礎理論 14 アルゴリズムとプログラミング 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 16 システム構成要素 17 ソフトウェア 18 ハードウェア 9 技術要素 【中分類】 19 ヒューマンインタフェース 20 マルチメディア 21 データベース 22 ネットワーク 23 セキュリティ

(出典) IPA「IT スキル標準モデルカリキュラム－レベル 1 を目指して－」をもとに作成

コマタイトルの例については、「付録：IT スキル標準レベル 1 コマタイトル一覧」に記載しています。

パーソナルスキル入門

科目シラバス

科目	パーソナルスキル入門
職種	職種共通
レベル区分（対象者）	IT スキル標準のレベル 1 を目指す者
受講前提	前提科目は特にないが、高校卒業程度の知識を有していること
学習目標	職業人としての基本的なパーソナルスキルの知識を活用し、上位者の指導の下、チームメンバーとして、業務活動に参加することができる
研修・教育方法	講義、グループ演習
修得スキルの評価方法	講義終了後の受講レポート、定量アンケート、知識確認テスト、演習問題の取組状況を総合的に判断して評価を行う
カリキュラム構成	1 コマ 90 分×15 回（総時間：22.5 時間）

(出典) IPA「IT スキル標準モデルカリキュラム－レベル 1 を目指して－」をもとに作成

コマタイトルの例については、「付録：IT スキル標準レベル 1　コマタイトル一覧」に記載しています。

詳細理解のため参考となる文献（参考文献）	
IT スキル標準とは -ものさしとしてのスキル標準	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/itss2.html
IT スキル標準モデルカリキュラム－レベル 1 を目指して－	https://www.ipa.go.jp/archive/jinzai/skill-standard/itss/qv6pgp000000buc8-att/000024802.pdf

24-3. マナビ DX

マナビ DX は、経済産業省と IPA が運営するデジタル人材育成のためのプラットフォームで、デジタルスキル習得に関する講座を紹介するポータルサイトになっています。デジタルスキルを学んだことのない人から、実践的なデジタル知識・スキルを身につけたい人まで、それぞれに適した講座を紹介してくれます。

紹介されている講座

マナビ DX で紹介されている講座には以下のような特徴があります。

- **厳選された信頼できる講座**
  デジタルスキル標準（DSS）などのスキル標準への対応を経産省・IPA が審査し、合格した講座のみが掲載されています。
- **種類が豊富**
  講座はさまざまなパートナーから提供されており、デジタルリテラシーや基本的な IT スキルを学ぶための講座から実際のビジネスシーンで役立つ実践的なスキルを習得するための講座まで幅広い講座が掲載されています。
- **受講料支援のある講座も掲載**
  講座には無料のものと有料のもの（受講料が必要なもの）がありますが、一部の講座では受講料の補助が受けられるものもあります。
- **リスキリングにも活用**
  リスキリングに重要なデジタルスキル習得をはじめる方に最適な初学者向け講座も提供されています。

「マナビ DX」には多くの講座が掲載されています。その一部を紹介します。

- **デジタルリテラシー講座**
  - IT パスポート試験対策：IT の基本知識を学ぶための講座
  - データサイエンス入門：データ分析の基礎を学ぶための講座
  - AI 活用入門：人工知能の基本概念とその応用方法を学ぶための講座
- **デジタル実践講座**
  - AI データ活用実践コース：Web 開発の基礎から AI 技術の応用までを学ぶ講座
  - IT エンジニア総合コース：フロントエンドからバックエンド、さらに AI 技術までを網羅する講座
  - AI×IoT エンジニア育成コース：Web 開発、AI、IoT 技術を統合的に学ぶ講座
- **サイバーセキュリティ関連講座**
  - SaaS 担当者のためのセキュリティコース

クラウドサービスを利用する際に必要となる情報セキュリティの基礎知識とクラウドサービスにおけるリスク分析手法を学ぶ講座

- サイバーセキュリティ技術者育成コース
  サイバーセキュリティ技術を習得するための実践的な高度技術を基礎から体系的に学ぶ講座
- インターネットセキュリティ技術（実習編）
  インターネット上のさまざまな脅威について学習し、組織において必要となるセキュリティ対策技術を、実習を通して習得する講座
- 攻撃手法概論
  サイバーセキュリティにおける代表的な攻撃手法の概要とその特徴について学ぶ講座
  （サイバー攻撃からシステムや情報資産を保護するために、まずは攻撃手法の概要を学びたい方におすすめです。）

- **特定のスキルに特化した講座**
  - ゼロから始める AI エンジニア講座セット：AI の知識ゼロから E 資格の取得を目指すセット講座
  - IoT エンジニア育成コース A：Web 開発の基礎から IoT 技術までを学ぶ講座

マナビ DX では、スキル標準のレベル定義をもとに 1～4 のレベルに分けて掲載しています。講座レベルは、検索結果や講座ページで確認することができます。

講座レベルは下の表を確認してください。

マナビ DX の講座レベル

レベル 4	**DX 推進スキル標準・ITSS・ITSS+** 一つまたは複数の専門を獲得したプロフェッショナルとして、専門スキルを駆使し、業務上の課題を発見と解決をリードするレベル。プロフェッショナルとして求められる、経験の知識化とその応用（後進育成）に貢献する。
レベル 3	**DX 推進スキル標準・ITSS・ITSS+** 要求された作業をすべて独力で遂行するレベル。専門を持つプロフェッショナルを目指し、必要となる応用的知識・技能を有する。
レベル 2	**DX 推進スキル標準・ITSS・ITSS+** 要求された作業について、上位者の指導の下、その一部を独力で遂行するレベル。プロフェッショナルに向けて必要となる基本的知識・技能を有する。
レベル 1	**DX リテラシー標準** 要求された作業について、上位者の指導を受けて遂行するレベル。プロフェッショナルに向けて必要となる基本知識・技能を有する。

(出典) マナビ DX「マナビ DX での学び方」をもとに作成

マナビ DX での学び方

Point1 キーワードやカテゴリで検索可能

キーワードや「学習できるスキル」や「目指すロール」、「リテラシー講座」といったあらかじめ定義されたカテゴリから講座を探すことができます。

- キーワードから探す
  どの画面でも、ヘッダーからキーワードで検索することが可能です。具体的なキーワードや講座名があればここから検索してください。また、トレンドキーワードを集めた「注目ワード」を利用することもできます。
- スキルやロールから探す
  トップページの「3 つのカテゴリ（リテラシー講座・学習できるスキル・目指すロール）」から講座を絞りこむことができます。これらのカテゴリはデジタルスキル標準に準拠しています。
- マナビ DX オススメから探す
  具体的なキーワードやカテゴリが想像できない場合は、マナビ DX オススメの視点から講座を選ぶことも可能です。

Point2 自分の「お気に入り」や「学習プラン」の作成が可能

マナビ DX にログインすると、講座を記録することができます。

- 「お気に入り」への登録
  学習してみたい講座、気になる講座があれば、「お気に入り」に登録することが可能です。
- 「学習プラン」による計画的な学習の実現
  学習したい講座を見つけたら、「学習プラン」を活用し、計画的な研修受講や受講実績を管理することをお勧めします。「学習プラン」は学習したい講座の登録、学習の進捗、研修の受講実績を管理することができ、計画的、継続的な自己研鑽を実現することができます。

Point3 講座は「デジタルスキル標準（DSS）」と紐付け

「デジタルスキル標準（DSS）」を理解し活用しましょう

マナビ DX に掲載されている講座は、「デジタルスキル標準（DSS）」に紐づけされています。「デジタルスキル標準（DSS）」を活用し、目指すキャリアや習得したい知識・スキルから次の講座を探し、段階的に学習していくことができます。

- 「デジタルスキル標準（DSS）」にはすべてのビジネスパーソンを対象にデジタル技術を理解して活用するスキル（デジタルリテラシー）をまとめた「DX リテラシー標準（DSS-L）」と、高い専門性を持って組織の中で DX を推進するために必要な役割と知識・スキルをまとめた「DX 推進スキル標準（DSS-P）」があります。

- 「デジタルスキル標準（DSS)」を使って、デジタル社会の中でビジネスパーソンに求められている知識・スキルや企業や組織の DX の推進において必要な人材を理解し、自分に必要とされている知識やスキルを整理しましょう。ビジネスパーソンとして必要な知識や習得すべきスキルを、あるいは自分が目指したい人材像や実際の業務を描きながら、現在の自分の強み、弱みを棚卸し、なりたい自分に必要な知識や習得すべきスキルを整理し、学び続けることで、さらなる自己研鑽につなげることができます。

デジタル人材に関する政策や最新テクノロジー情報を知りましょう

学びの継続はとても重要です。ぜひ、マナビ DX の機能を存分に活用し、「もっと知りたい」「もっとスキルアップしたい」を実現するために、計画的、継続的に学ぶことで、自分自身をますます成長させていきましょう。

Point4 最先端の新技術にも対応

デジタルの分野は新しいテクノロジーが次々と出現、進歩していくため、常に最新情報をキャッチし、継続して学び続けることがとても重要です。学び続けることで、更なる自己研鑽をしていきましょう。

- 受講したい研修が見つかったら、講座詳細から、講座提供事業会社のサイトへ進み、研修を申し込みの上、研修を受講しましょう。

（出典）マナビ DX「マナビ DX での学び方」をもとに作成

One Point

デジタル人材育成に関する支援制度から講座を探す方法

マナビ DX では経済産業省を始め、各省庁におけるデジタル人材育成に関する個人、事業者様向けの支援制度を紹介しています。また、第四次産業革命スキル習得講座（経済産業省)、教育訓練給付制度（厚生労働省)、人材開発支援助成金（厚生労働省）などと連携した講座があります。

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
デジタル人材育成政策のご紹介	https://manabi-dx.ipa.go.jp/gov_assist

第25章. スキルと知識を持った人材育成・人材確保方法

章の目的
第 25 章では、カリキュラムなどを活用し、チェンジマインド、リスキリングも含めた実施計画および教育・研修の実施内容の作成方法を理解することを目的とします。カリキュラムごとに、実践方法を例示します。

主な達成目標
◘ 「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに、教育・研修の実施内容および実施計画を作成する手順を理解すること ◘ 「IT スキル標準」をもとに、教育・研修の実施内容および実施計画を作成する手順を理解すること ◘ 「デジタルスキル標準」をもとに、教育・研修の実施内容および実施計画を作成する手順を理解すること

25-1. 「プラス・セキュリティ」の実施計画例

セキュリティに詳しくない人に加えて、既にセキュリティを担当している人も、新しい技術を学び、考え方を最新にしていくことが必要です。技術は常に進化しており、過去の対策や古い考え方では、最新のサイバー攻撃に対応することが難しいためです。昨今は AI を使った新しい攻撃手法が増加しており、昔のスキルや知識だけでは十分に対応することは困難です。この章の前半では、「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに、教育・研修の実施内容および実施計画を解説します。

この章の後半ではリスキリングに有効と考えられるカリキュラムを例にして、リスキリングのための研修実施計画の策定について解説します。現在、AI や自動化などの新しい技術の導入が進んでいますが、これによって従来の仕事が変化し、新しいスキルが必要になります。中長期でみれば AI などの新技術の普及によって、一部の職業は消滅し、新しい職業が生まれることになるでしょう。そうした変化の中で、個人が市場で競争力を維持するためには、リスキリングを通じて最新の技術や知識を習得し、変化に対応できる能力を高めることが重要です。リスキリングを成功させるためには、チェンジマインド（変革思考）を持つことが非常に重要です。チェンジマインドとは、変化を受け入れ、柔軟に対応する考え方を意味します。リスキリングには新しい知識やスキルを習得するための柔軟な思考が不可欠です。考え方を柔軟に変え、具体的な目標を設定するとともに、信頼できる教材やカリキュラムを選んで、自分にあった学習方法を見つけることが、リスキリング成功の秘訣だと言ってよいでしょう。この章では関係機関が公表しているカリキュラムを参考に、セキュリティに関する学習方法を例示します。

「プラス・セキュリティ知識補充講座 カリキュラム例」の内容を実施するための手順を例示します。

前提条件

中小企業を対象とし、セキュリティ専門家は社内に存在しない。

1.目標の明確化

単元の目標と、到達レベルを明確にします。（以下の表は、部課長級向けの第 3 単元（投資『サイバーセキュリティとリスク対応』）の場合です）

目標
自部署におけるサイバーセキュリティリスクのマネジメントに必要となる概念と、具体的なアクションについて理解する。
到達レベル
● 部署におけるサイバーセキュリティリスクを特定し、対応の優先順位付けや対処方針の選定を行うとともに、その実現に必要な体制や要員の確保・育成を行えるようになる。

● 担当者や社外ベンダーから提示されるセキュリティ対策案について、組織として妥当性に関する判断を下せるようになる。

(出典) NCO「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

2.学習方法の検討

カリキュラム内容を学習するための方法を検討します。例えば以下のようなものが挙げられます。

- 専門家の活用
  サイバーセキュリティの専門家や、企業向けにトレーニングサービスを提供する企業を活用して学習します。中小企業に対応できる柔軟なサポートを提供するサービスを優先的に検討することが重要です。例えば、企業のセキュリティ状況に応じたカスタマイズされた研修プログラムを依頼したり、専門家によるワークショップを依頼したりすることが効果的です。
- オンライン学習の活用
  無料や低価格で利用できるオンライン学習プラットフォームを使って、従業員がセキュリティの基礎を学べるようにします。例えば、セキュリティに関する基礎コースを受講できるオンライン学習サイト（例：マナビ DX など）があります。従業員が自分のペースで学習できるため、業務の合間を利用して学びやすいことがメリットです。
- 内部研修の実施
  外部講師を招かず、社内の IT リテラシーが高い従業員が中心となり、セキュリティの基本を他の従業員に教える研修を行います。例えば、社内の担当者が「パスワードの強化方法」や「メールのフィッシング対策」といった実践的な内容を教えることで、全体のセキュリティ意識を高められます。社内の状況に即した内容で実施できるため、企業全体でスムーズに学習が進む点が特徴です。

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

3.受講者の準備

受講者によってデジタル・ネットワーク技術、サイバーセキュリティに関する知識に差があると考えられます。以下のような方法によって受講の要否を判断することが大切です。

	方法の種類	概要	利点（○）・欠点（×）
①	セルフチェックに基づく受講者判断	「○○について説明できる」といったチェック項目のリストを提供し、「はい」が一定比率以上の場合は、当該項目の受講を省略できる。	○ 動画に比べると準備コストが少なく済む × チェック項目が多くなると受講者にとって判断に要する負担が増大する
②	理解度テストによ	受講者の理解度を確認する４択	○ 提示した方法の中で、最も厳

	る判定	問題を出題し、一定以上の得点を得た受講者は当該項目の受講を省略できる。	密な判定が可能 × カリキュラムの冒頭で「得点が低いので要受講」を示すのは受講意欲を下げる恐れがある
③	動画視聴に基づく受講者判断	受講者は次ページに示すシナリオの動画を視聴し、理解度十分（同様の場面で適切な判断が可能）と判断した場合は当該項目の受講を省略できる。	○ 受講者にとっては軽い負担で適切な判断を行うことが可能で利便性に優れる × 動画教材の作成にコストがかかる 事前の目的設定が重要
④	（判断支援手段を提供しない）	各項目を受講するか否かを受講者による判断に委ねてしまう。	○ 判断用教材の準備が不要 × 基礎知識不十分なまま集合講習に参加する受講者が生じる可能性がある

(出典) NCO「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

そのほか、受講の可否を判断する手段として以下のものが挙げられます。

- 事前アンケートの実施
  セキュリティ知識レベルを把握するために、セルフチェック形式のアンケートを実施します。このアンケートでは、日常的に利用されるデジタルツールやセキュリティ用語の理解度を確認します。アンケートの結果をもとに、カリキュラムを受講する対象者を決定します。部門のマネジメント層で、実際にセキュリティ対応に関与する可能性のあるメンバーを中心に選びます。

4.カリキュラムの実施

カリキュラム内容の実施方法を例示します。（以下は、部課長級向けの第 3 単元（投資『サイバーセキュリティとリスク対応』）の場合です）

- オンライン研修の実施
  オンデマンド形式で提供される次の事項を学習します。
  - サイバーセキュリティのリスクマネジメントの特徴（オンデマンド・30 分）
  - 対策における費用と損失の考え方（オンデマンド・30 分）

  この段階では、サイバー攻撃の基礎やリスク管理の基本概念について学びます。
- 集合講習の実施
  集合講習で提供される次の事項を学習します。

➢ リスクマネジメントのケーススタディ（集合講習：30 分）

集合形式の講習では、講師が具体的なサイバー攻撃事例を紹介し、効果的なセキュリティ対策を解説します。また、参加者同士でディスカッションを行い、演習を通じて理解を深めます。

- 演習の実施

  演習 2：自部署リスクとその対応策を洗い出し、リスク管理部門などへ説明（集合講習：60 分）

  演習では、リスク対応策のシミュレーションを行い、サイバーセキュリティにおける投資の費用対効果を検討します。参加者は自社に最も適したリスク対応策を模索し、チームで発表を行います。

5.結果の評価と報告

カリキュラム実施後に評価と報告を行います。

- 結果のフィードバック

  集合講習後、各部門に対して研修の成果をフィードバックします。各部門が現状のセキュリティ対策を見直し、改善点を明確にします。

- 最終報告書の作成

  すべての受講者の意見や研修結果を反映した最終報告書を作成し、経営層に提出します。この報告書は、今後のセキュリティ体制の強化に向けた重要な資料となります。

6.ガントチャートの作成

上記の手順を実施するためのガントチャートを作成することで、進捗状況の管理が容易になります。

ステップ	タスク	サブタスク	期間	担当者	備考
ステップ 1：カリキュラム目標の確認と調整	1. カリキュラム目標の確認	1.1 カリキュラム内容の確認	2 日	プロジェクトリーダー	単元の目的と目標を確認
		1.2 経営層との初回ミーティング	1 日	プロジェクトリーダー、経営層	経営層との合意形成
		1.3 フィードバックの反映	2 日	プロジェクトリーダー	ミーティングの結果を反映
		1.4 最終合意の取得	2 日	プロジェクトリーダー	経営層からの最終承認
ステップ 2：外部パートナーの選定	2. セキュリティベンダーの選定	2.1 セキュリティベンダーリストの作成	3 日	人事部、セキュリティ担当	ベンダー候補をリスト化

		2.2 ベンダーとの初期打ち合わせ	3日	人事部、セキュリティ担当	各ベンダーに要件を共有
		2.3 ベンダー提案の評価	4日	人事部、セキュリティ担当、経営層	提案内容の評価と比較
		2.4 ベンダーの選定	2日	人事部、経営層	最終決定を行い、承認
		2.5 契約の準備と締結	2日	人事部、法務担当	契約書の準備と締結
ステップ3：受講者の準備	3. 事前アンケートの実施	3.1 アンケート内容の設計	2日	人事部、セキュリティコンサルタント	セルフチェックリストの作成
		3.2 アンケートの配布	1日	人事部	受講対象者へ配布
		3.3 回収と結果の分析	3日	人事部	アンケート結果を集計し分析
		3.4 受講者リストの確定	1日	人事部、セキュリティ担当	受講者リストを最終確定
ステップ4：カリキュラムの実施	4. オンライン研修の実施	4.1 オンライン教材の準備	4日	セキュリティコンサルタント	オンデマンド形式の教材準備
		4.2 学習スケジュールの通知	1日	人事部	受講者にスケジュールを周知
		4.3 受講者の進捗確認	7日	人事部	受講進捗の確認とフォロー
		4.4 オンライン研修の完了	2日	受講者、セキュリティコンサルタント	オンライン研修を終了
	5. 集合講習の実施	5.1 講師の手配	2日	セキュリティコンサルタント	集合講習を担当する講師を確定
		5.2 集合講習の準備	3日	講師、サポートスタッフ	教材、演習の準備
		5.3 集合講習の実施	1日	受講者、講師	集合講習で事例紹介と演習実施
		5.4 演習の実施	1日	受講者、講師	投資効果分析やリスク対応策を検討
ステップ5：結果の評価と報告	6. 結果のフィードバックと報告	6.1 フィードバックの整理	3日	各部門マネージャー	受講者からフィードバックを収集

		6.2 改善提案の作成	3 日	各部門マネージャー	改善提案を作成
		6.3 改善提案の実行計画作成	2 日	各部門マネージャー	提案に基づいたアクションプランを策定
	7. 最終報告書の作成	7.1 報告書の初稿作成	3 日	プロジェクトリーダー	研修結果をもとに報告書を作成
		7.2 報告書のレビュー	2 日	各部門マネージャー、経営層	レビューとフィードバック
		7.3 報告書の最終版作成	2 日	プロジェクトリーダー	最終報告書を経営層に提出

タスク	サブタスク	期間	担当者	2024年2月							
				1日	2日	3日	4日	5日	6日	7日	8日
1. カリキュラム目標の確認	1.1 カリキュラム内容の確認	2日	プロジェクトリーダー								
	1.2 経営層との初回ミーティング	1日	プロジェクトリーダー、経営層								
	1.3 フィードバックの反映	2日	プロジェクトリーダー								
	1.4 最終合意の取得	2日	プロジェクトリーダー								

タスク	サブタスク	期間	担当者	2024年2月												
				9日	10日	11日	12日	13日	14日	15日	16日	17日	18日	19日	20日	21日	22日
2. セキュリティベンダーの選定	2.1 セキュリティベンダーリストの作成	3日	人事部、セキュリティ担当														
	2.2 ベンダーとの初期打ち合わせ	3日	人事部、セキュリティ担当														
	2.3 ベンダー提案の評価	4日	人事部、セキュリティ担当、経営層														
	2.4 ベンダーの選定	2日	人事部、経営層														
	2.5 契約の準備と締結	2日	人事部、法務担当														

タスク	サブタスク	期間	担当者	2024年2月							3月
				23日	24日	25日	26日	27日	28日	29日	1日
3. 事前アンケートの実施	3.1 アンケート内容の設計	2日	人事部、セキュリティコンサルタント								
	3.2 アンケートの配布	1日	人事部								
	3.3 回収と結果の分析	3日	人事部								
	3.4 受講者リストの確定	1日	人事部、セキュリティ担当								

タスク	サブタスク	期間	担当者	2024年3月													
				2日	3日	4日	5日	6日	7日	8日	9日	10日	11日	12日	13日	14日	15日
4. オンライン研修の実施	4.1 オンライン教材の準備	4日	セキュリティコンサルタント														
	4.2 学習スケジュールの通知	1日	人事部														
	4.3 受講者の進捗確認	7日	人事部														
	4.4 オンライン研修の完了	2日	受講者、セキュリティコンサルタント														

タスク	サブタスク	期間	担当者	2024年3月							
				16日	17日	18日	19日	20日	21日	22日	23日
5. 集合講習の実施	5.1 講師の手配	2日	セキュリティコンサルタント								
	5.2 集合講習の準備	3日	講師、サポートスタッフ								
	5.3 集合講習の実施	1日	受講者、講師								
	5.4 演習の実施	1日	受講者、講師								

タスク	サブタスク	期間	担当者	2024年3月							
				24日	25日	26日	27日	28日	29日	30日	31日
6. 結果のフィードバックと報告	6.1 フィードバックの整理	3日	各部門マネージャー								
	6.2 改善提案の作成	3日	各部門マネージャー								
	6.3 改善提案の実行計画作成	2日	各部門マネージャー								

タスク	サブタスク	期間	担当者	2024年4月							
				1日	2日	3日	4日	5日	6日	7日	8日
7. 最終報告書の作成	7.1 報告書の初稿作成	3日	プロジェクトリーダー								
	7.2 報告書のレビュー	2日	各部門マネージャー、経営層								
	7.3 報告書の最終版作成	2日	プロジェクトリーダー								

ガントチャート作成後の流れ

以下の 3 つのポイントに焦点を当てることで、ガントチャートを活用したプロジェクト管理が効果的に行え、カリキュラム内容のスムーズな実施につながります。

- 進捗確認とスケジュール管理
  プロジェクトが計画通りに進んでいるかを定期的に確認し、スケジュールに遅れが生じた場合には迅速に対策を講じます。
- リソースの効率的な活用と調整
  限られたリソースを最大限に活用し、必要に応じて適切に調整することで、プロジェクトのスムーズな進行をサポートします。
- リスクの早期特定と対応策の準備
  プロジェクトに潜むリスクをあらかじめ特定し、問題が発生する前に対応策を準備しておくことで、予期しないトラブルにも迅速に対応できる体制を整えます。

25-2. 「リスキリング」「チェンジマインド」の実施計画例

25-2-1. 「IT スキル標準」の実施計画例

IT スキル標準レベル 1「IT 入門（2）」をもとに実施計画を作成する手順を説明します。

1.目標の明確化

学習目標を明確にします。

学習目標
職業人として IT（情報技術）の基本的な知識を活用し、上位者の指導の下、業務の分析やシステム化の支援や情報の活用ができる。

(出典) IPA「IT スキル標準モデルカリキュラム－レベル 1 を目指して－」をもとに作成

2.目標達成に必要な作業を洗い出す

カリキュラムの知識項目を確認し、学ぶ必要がある項目を整理します。

	タイトル	学習目標	対応する知識項目（大分類）―（中分類）
第 1 回	オリエンテーション、コンピュータ上での情報表現	数値や文字情報をコンピュータ上で表現する方法と用語を説明できる。	● 基礎理論 － 基礎理論 ● 技術要素 － マルチメディア
第 2 回	プログラミングの役割	アルゴリズムとプログラミングとの関係を説明できる。	● 基礎理論 － アルゴリズムとプログラミング
第 3 回	コンピュータの種類と構成する装置	コンピュータを構成する装置と役割を説明できる。	● コンピュータシステム － ハードウェア ● コンピュータシステム － コンピュータ構成要素
第 4 回	ソフトウェアの種類と役割	ソフトウェアの種類と役割を説明できる。	● コンピュータシステム － ソフトウェア
第 5 回	システム処理形態と処理方式	システムの処理形態と処理方式の用語を説明できる。	● コンピュータシステム － システム構成要素
第 6 回	前半のまとめ	前半の講義のまとめを行う。	-
第 7 回	マルチメディアとヒュ	マルチメディアの種類と	● 技術要素 － ヒューマ

	ーマンインタフェース	ヒューマンインタフェースの基本的な用語を説明できる。	ンインタフェース ● 技術要素 – マルチメディア
第 8 回	ネットワーク技術の活用①	インターネットの仕組みと通信サービスの特徴を説明できる。	● 技術要素 – ネットワーク
第 9 回	ネットワーク技術の活用②	通信網と通信プロトコルに関する用語を説明できる。	● 技術要素 – ネットワーク
第 10 回	データベースの技術①	データベースのモデル化と正規化の方法を説明できる。	● 技術要素 – データベース
第 11 回	データベースの技術②	データベースの表操作の方法を説明できる。	● 技術要素 – データベース
第 12 回	情報セキュリティ対策①	セキュリティ対策に関する基本的な用語を説明できる。	● 技術要素 – セキュリティ
第 13 回	情報セキュリティ対策②	セキュリティ対策に関する基本的な用語を説明できる。	● 技術要素 – セキュリティ
第 14 回	後半のまとめ	後半の講義のまとめを行う。	-
第 15 回	まとめ	これまでの講義内容を総括する。	-

(出典) IPA「IT スキル標準モデルカリキュラム – レベル 1 を目指して – 」をもとに作成

3.学習内容の詳細化

各回で行う内容を具体的に決めます。例として第 13 回で行う内容は、以下の通りです。

第 13 回 情報セキュリティ対策②（講義 70 分＋演習 20 分）	
学習目標	セキュリティ対策に関する基本的な用語を説明できる。
内容	1．技術的なセキュリティ対策 （1）個人認証技術の種類と特徴 ● ID、パスワード ● コールバック ● デジタル署名

	● 生体認証技術 （2）暗号化技術の種類と特徴 ● 公開鍵暗号方式の仕組み ● 秘密鍵暗号方式の仕組み （3）不正侵入・コンピュータウイルス対策 ● 入退出管理 ● アクセス管理、機密管理 ● ファイアウォール・コンピュータウイルスの種類と対策 （4）演習問題【セキュリティの種類と対策】 2．そのほかの情報セキュリティ対策 （1）個人情報の漏えい （2）情報セキュリティポリシー （3）責任と権限の明確化 （4）情報セキュリティマネジメントシステム（ISMS）
研修・教育方法 （予定時間）	講義 70 分 演習 20 分
対応する知識項目	＜共通キャリア・フレームワークの大分類／中分類との対応＞ 技術要素－セキュリティ

（出典）IPA「IT スキル標準モデルカリキュラム－レベル 1 を目指して－」をもとに作成

カリキュラムをもとに、学習内容を具体的にします。

具体的な学習内容（例）

1.技術的なセキュリティ対策

（1）個人認証技術の種類と特徴

個人認証は、システムやネットワークへのアクセスを管理するための基本的な技術です。以下の主要な技術を説明します。

- ID、パスワード
  最も一般的な認証方法。ID で個人を特定し、パスワードで本人確認を行います。ただし、パスワードの漏えいリスクや、短い・単純なパスワードの使用がセキュリティの脆弱性となりがちです。
- コールバック
  電話やメッセージを使用して本人確認を行う方法。例えば、ログイン時にワンタイムパスワードを送信し、そのパスワードを使用してログインする方法などが含まれます。二要素認証（2FA）の一部として利用されることも多いです。

- デジタル署名
  公開鍵暗号方式を利用して、データの改ざんや成りすましを防ぐ技術。電子的な書類やメールの送信者が本人であることを証明する際に使用されます。
- 生体認証技術
  指紋、顔認証、虹彩認証など、生体的な特徴を利用して個人を特定します。高いセキュリティを実現できますが、技術の精度やプライバシー問題が課題となることもあります。

（2）暗号化技術の種類と特徴

情報を保護するために、データの暗号化は重要です。主に以下の 2 つの暗号化方式があります。

- 公開鍵暗号方式
  暗号化と復号に異なる鍵（公開鍵と秘密鍵）を使用する方式です。公開鍵で暗号化されたデータは対応する秘密鍵でのみ復号可能であり、安全な通信に使われます。
- 秘密鍵暗号方式
  暗号化と復号に同じ鍵を使用する方式。公開鍵暗号に比べて高速で、VPN や Wi-Fi のセキュリティなどに使用されますが、鍵の管理が課題となります。

（3）不正侵入・コンピュータウイルス対策

ネットワークやシステムに対する攻撃を防ぐための対策です。

- 入退出管理
  システムや施設への物理的・論理的なアクセスを制限し、許可された者のみがアクセスできるようにする対策です。カードキーや生体認証が使用されます。
- アクセス管理、機密管理
  特定の情報にアクセスできるユーザーや権限を設定し、無許可のアクセスを防ぎます。これにより、社内のデータ流出や情報漏えいを防ぎます。
- ファイアウォール
  ネットワーク間の不正な通信を防ぐための装置またはソフトウェア。パケットフィルタリングやプロキシ機能などを使用し、外部からの攻撃を防ぎます。
- コンピュータウイルス対策
  ウイルス対策ソフトウェアの導入や、定期的なアップデート、メール添付ファイルの検査など、ウイルス感染を防ぐための措置が取られます。

（4）演習問題【セキュリティの種類と対策】

実際の状況を想定したシナリオを使い、各種セキュリティ対策がどのように適用されるかを検討します。

例：新しいウェブサービスを公開する際、どのような認証・暗号化技術を導入すべきかを考察

する問題。

2. そのほかの情報セキュリティ対策

（1） 個人情報の漏えい

個人情報の漏えいリスクに対する対策として、データの暗号化、アクセス権限の制限、適切なバックアップの実施が重要です。また、外部とのデータ共有には必ずセキュリティ対策を講じ、セキュアなチャネルを使用することが推奨されます。

（2） 情報セキュリティポリシー

企業や組織が、情報資産をどのように保護するかを明確に定めた規程やガイドラインを「情報セキュリティポリシー」と呼びます。これにより、従業員全員がセキュリティの重要性を理解し、一貫した対策を講じることができます。

（3） 責任と権限の明確化

セキュリティ対策においては、誰がどのような責任を持ち、どのような権限を持つのかを明確にすることが不可欠です。これにより、インシデント発生時の対応がスムーズに進行し、迅速な問題解決が可能となります。

（4） 情報セキュリティマネジメントシステム（ISMS）

ISMS は、企業や組織がセキュリティ管理をシステム的に行うためのフレームワークです。国際規格である ISO/IEC 27001 に準拠して、リスクの評価、管理、改善を繰り返すことで、継続的なセキュリティ強化を図ります。

4.学習方法の選定

カリキュラム内容を学習するための方法を検討します。学習方法を例示します。

- オンライン学習（e ラーニングなど）の利用

無料や低価格で利用できるオンライン学習プラットフォームを活用します。例えば、「マナビ DX」などで、以下のような内容を学びます：

  - パスワードや生体認証技術、暗号化技術の基礎について解説したレッスン
  - 不正アクセス対策やウイルス対策の基本を学べる動画やレッスン
  - 情報セキュリティポリシーや ISMS の基本をカバーする初心者向けのレッスン

- 実践的な演習を取り入れた社内研修

社内で、実際に手を動かして学べる簡単な演習を実施します。例えば、以下のような内容を取り入れます：

- パスワード管理や二要素認証の設定について、従業員が自分で試すハンズオン研修
- 簡単なファイアウォールの設定やアクセス管理の仕組みを学べる実践的な演習
- セキュリティ対策の演習問題の実施

これらの実施により、従業員がすぐに実務に役立てられるスキルを身につけられます。

- 社内ディスカッションと情報共有

定期的に社内でセキュリティに関する話し合いや情報共有の場を設け、従業員同士で意見交換を行います。例えば以下のような事項を取り上げます。

- 個人情報保護やセキュリティポリシーに関する業務上の注意点や実践方法について
- ISMS をどのように社内で実践するか、基本的な導入手順や活用方法についてディスカッションを行います。学んだ内容を業務にどのように適用できるかを従業員同士で考えることで、実践的な理解を深め、セキュリティ対策を現場で活かせるようになります。

5.学習の進行と進捗管理

学習を開始し、週次または月次で進捗報告を行います。各セッションの進行状況を確認し、従業員が計画に遅れを取っている場合は、すぐに調整を行います。さらに、定期的なテストや確認を設定し、理解度やスキルの定着度を把握します。

6.フィードバック収集とフォローアップの実施

従業員からのフィードバックを定期的に収集し、内容が難しすぎる、または簡単すぎる場合には、カリキュラムの内容を調整します。さらに、トレーニング終了後も、従業員が学んだことを実際の仕事で活用できているかを確認し、必要に応じて追加のサポートや新しい学習計画を提供します。

25-2-2. 「デジタルスキル標準」の実施計画例

「デジタルスキル標準」は、DX に関する基礎的な知識やスキル・マインドを身につけるための指針としての「DX リテラシー標準」と、DX を推進する人材を育成・採用するための指針としての「DX 推進スキル標準」の 2 種類で構成されています。

DX リテラシー標準

DX リテラシー標準では、あらゆるビジネスパーソンに求められる知識・スキルが定義されています。学習項目のうち、「How – セキュリティ」を学ぶための手順を例示します。

1.学習内容の検討

学習する内容を明確にします。「How – セキュリティ」で定義されている内容は以下の通りです。

(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

How – セキュリティの内容

セキュリティ技術の仕組みと個人がと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。

- データやデジタル技術に対して徒に不安を感じることなく、適切に利用するためには、情報を守る仕組みを知ることが求められる。
- 企業が用意する環境・対策に加えて、個人もセキュリティ対策を行う必要性とその方法を理解する必要がある。

学習項目例は以下の通りです。

学習項目例

- セキュリティの 3 要素
  - ✓ 機密性
  - ✓ 完全性
  - ✓ 可用性
- セキュリティ技術
  - ✓ 暗号
  - ✓ ワンタイムパスワード
  - ✓ ブロックチェーン
  - ✓ 生体認証
- 情報セキュリティマネジメントシステム（ISMS）
- 個人がとるべきセキュリティ対策
  - ✓ ID やパスワードの管理
  - ✓ アクセス権の設定
  - ✓ 覗き見防止
  - ✓ 添付ファイル付きメールへの警戒
  - ✓ 社外メールアドレスへの警戒

(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

学習内容を具体的にします。

具体化した学習内容（例）

セキュリティの 3 要素

- 機密性
  情報を許可された人だけがアクセスできる状態を保つこと。例えば、パスワードや暗号化によってデータを保護します。
- 完全性

情報が正確で、改ざんや破壊されていない状態を維持すること。例えば、ハッシュ関数を使ったデータ検証により、データの一貫性を確保します。

- 可用性
  情報やシステムに必要なときにアクセスできる状態を維持すること。例えば、サーバの冗長化やデータバックアップにより、障害発生時も業務を継続できるようにします。

セキュリティ技術

- 暗号
  暗号は、データを「鍵」を使って別の形に変える技術です。この変えられたデータは、正しい「鍵」を持っている人だけがもとの形に戻せる仕組みです。
- ワンタイムパスワード
  一度限り有効な使い捨てのパスワード。時間制限や一回の使用で無効になるため、パスワードが盗まれても再利用されるリスクが低いです。
- ブロックチェーン
  取引データを分散型の台帳に記録する技術。ブロックチェーンは変更が困難で、データの透明性と信頼性を高めるために使用されます。
- 生体認証
  ユーザーの身体的特徴（指紋、顔、虹彩など）を使用して本人確認を行う技術。これにより、なりすましのリスクを減らします。
- 情報セキュリティマネジメントシステム（ISMS）
  組織が情報セキュリティを計画的に管理・運営するための仕組み。ISO 27001 がその基準として有名で、リスクアセスメント、セキュリティ方針の策定、従業員の教育などが含まれます。

個人がとるべきセキュリティ対策

- ID やパスワードの管理
  複雑なパスワードを使用し、使い回しを避ける。パスワードマネージャーを活用することも推奨されます。
- アクセス権の設定
  必要最低限のアクセス権限を設定し、不要な権限を持たないようにする。例えば、共有フォルダへのアクセス権限を適切に管理することが重要です。
- 覗き見防止
  公共の場所で作業する際に、画面を覗かれないように注意する。プライバシーフィルターなどの物理的な対策も効果的です。
- 添付ファイル付きメールへの警戒
  信頼できない送信者からの添付ファイルは開かない。特に.exe ファイルやスクリプトファ

イルは注意が必要です。

- 社外メールアドレスへの警戒
  社外からのメールにはフィッシングや詐欺のリスクが伴うことが多いため、注意深くメールの内容やリンクを確認することが重要です。

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
【ほぼ 15 秒アニメ】子ブタと学ぼう！情報セキュリティ対策のキホン	https://www.ipa.go.jp/security/anshin/measures/start.html

2.学習方法の選定

社内研修や、オンライン学習（e ラーニングなど）を利用することも有効です。

3.学習計画の策定

社内研修を実施するための計画を例示します。

学習計画の例

研修期間と目的

期間：半日～1 日（1 セッションあたり 30 分～1 時間）

目的：基本的なセキュリティ知識を学び、実務でのリスクを軽減できるレベルにする。

研修プログラム例

1 日目：セキュリティの基本

内容：セキュリティの 3 要素（機密性、完全性、可用性）の基本説明。

方法：簡単なプレゼンテーションと事例紹介を活用し、各自が自身の業務におけるセキュリティの問題点を考えます。

2 日目：セキュリティ技術の紹介

内容：暗号化、ワンタイムパスワード、生体認証の基本説明。

方法：専門的な用語を避け、従業員が使い慣れている技術やツールを例に出すことで、日常にどう活かせるかを具体的に説明します。

3 日目：個人がとるべきセキュリティ対策

内容：パスワード管理、メールの警戒、物理的なセキュリティの基本説明。

方法：従業員が今すぐできる行動に絞り、具体的な行動リストを共有します。例えば、「今日から自分のパスワードを強化する」「メールのリンクをクリックする前に URL を確認する」といった実践的な対策を提案します。

計画策定のポイント

- 実践的かつシンプルな内容にする

研修内容は理論に加えて、実際に業務で活かせる具体的な行動を中心に設計します。複雑な専門用語や技術的な話は避け、従業員がすぐに実践できる対策を説明することが重要です。
例：パスワードを複雑に設定し、パスワード管理ツールを使う方法を教える、メールの不審な点を見分けるチェックリストを提供する。

- 短時間で集中できるセッション構成
  研修は 30 分～1 時間と短く区切り、1 回のセッションで 1 つのテーマに集中するように構成します。従業員の負担を減らし、重要な内容を確実に理解してもらうために、セッションごとに焦点を絞ることが大切です。
  例：1 回目は「パスワード管理」、2 回目は「不審メールへの対応」といった具合に、テーマを分けて短い時間で進める。
- 実施後のフォローアップを重視
  研修が終わった後も、理解度や実践状況を確認する仕組みを取り入れることが重要です。例えば、定期的なチェックリストの確認や簡単なクイズで知識の定着を図ります。
  例：研修後に「パスワードを強化しましたか？」などのフォローアップメールや、理解度を測るクイズを実施することで、日常的に意識を高める。

4.学習の実施

計画をもとに、学習を実施する際のポイントを挙げます。

- 参加者の理解度に合わせた進行
  参加者のセキュリティに対する知識の違いを考慮し、初心者にも分かりやすい言葉を使い、ゆっくり進めることが大切です。難しい言葉や専門用語は避けて、具体的な例を使いながら説明しましょう。
  例：「パスワード管理がなぜ重要か」を説明する際に、複雑な理論ではなく、「簡単なパスワードは悪意のある人に推測されやすい」という形で、わかりやすく説明します。

- 実際の行動を取り入れる
  理論に加えて、実際にやってみる活動を含めることで、参加者が実務にどう活かすかを学べるようにします。実際に手を動かしてみることで、学んだ内容が現実の業務に結びつきやすくなります。
  例：「不審なメールをどう判断するか」を学んだ後、実際にその場でメールを確認してもらう時間を作り、すぐに対策を実行する体験をさせます。

5.フィードバックの収集とフォローアップ

研修後の確認・フォローアップ・フィードバックは、参加者の理解度を深め、セキュリティ意識を継続的に高め、次回の研修をより効果的にするために重要です。

ポイントを３つ紹介します。

- 理解度の確認

  研修内容がしっかりと理解されているかを確認するため、簡単なテストやクイズを実施します。これにより、参加者がどの程度理解しているか、また補足が必要な部分があるかを把握できます。

  例：「今日学んだセキュリティ対策を実際にどのように実施するか」を問う簡単な質問や選択式のテストを実施します。

- フォローアップと定期的な確認

  研修が終わった後も、継続してセキュリティ意識を高めるために、定期的に復習資料を送ったり、重要なポイントをリマインドするメールを配信したりします。日常的にセキュリティ意識を保つ仕組みを作ることが大切です。

  例：毎月１回「パスワードを更新していますか？」や「不審なメールに注意しましょう」といった確認メールを送ります。また、定期的にセキュリティ対策のチェックリストを共有し、従業員が自主的に対策を実践しているか確認します。

- フィードバックの収集

  研修後に参加者からのフィードバックを収集し、研修内容や進行方法についての改善点を把握します。これにより、次回の研修がより効果的なものになります。

  例：「研修で学んだことは役に立ちましたか？」「今後、さらに知りたいセキュリティの内容はありますか？」といった簡単なアンケートを実施し、感想や要望を集めます。

DX 推進スキル標準

「人材類型：サイバーセキュリティ」の「サイバーセキュリティマネージャー」の育成の例を紹介します。「サイバーセキュリティマネージャー」に必要なスキルを身につけるための教育・研修の実施計画を例示します。

人材類型	サイバーセキュリティ
ロール	サイバーセキュリティマネージャー
DX の推進において担う責任	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
主な業務	● 新規ビジネスにおけるデジタル活用を通じて生じるサイバーセキュリティ、セーフティ、プライバシー保護に関するリスクを評価する ● リスクとリターンのバランスを踏まえ、サイバーセキュリ

	ティリスクの影響を抑制するための戦略や、対策の実施体制を検討する ● サイバーセキュリティリスク抑制のための対策の実施状況の管理や監査を行う ● 事業実施に用いているデジタル環境で発生するサイバーセキュリティインシデントへの対応を行う
必要なスキル（高い実践力と専門性が必要のみ抜粋）	カテゴリ：セキュリティ サブカテゴリ：セキュリティマネジメント スキル項目 ● 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

(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

スキルの詳細は以下の通りです。

「セキュリティマネジメント」サブカテゴリーの構造
● 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、および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適切に実施するためのスキル ● 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 ● プライバシー保護 パーソナルデータなど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

上記のスキルを身につけるための実施計画を例示します。

1. 現状分析と目標設定

(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

現状分析

従業員の現在のセキュリティ知識とスキルを評価します。簡単なテストやアンケートでセキュリティに関する理解度を測定し、各自の強みや弱みを把握します。

テストの例は以下の通りです。

セキュリティに関する理解度テストの例

セキュリティ体制構築・運営

Q1. セキュリティ体制を効果的に構築し、維持運営するために最も重要な要素は次のうちどれですか？

a. セキュリティ体制を継続的に見直し、必要に応じて改善するプロセスを設ける

b. セキュリティソフトウェアを定期的にアップデートする

c. IT 部門の従業員だけでセキュリティ体制を構築し、他の従業員には任せない

d. 外部ベンダーにすべてのセキュリティ対策を委託する

答え：「a. セキュリティ体制を継続的に見直し、必要に応じて改善するプロセスを設ける」

解説：セキュリティ体制の構築や運営は、一度設けたら終わりではなく、常にリスクや組織の変化に応じて見直し、改善することが求められます。従業員の育成や全員が参加するセキュリティカルチャーの醸成も重要です。

セキュリティマネジメント

Q2. セキュリティマネジメントのプロセスで、最も重要な「リスクアセスメント」とは何ですか？

a. セキュリティソフトウェアの更新スケジュールを確認すること

b. 会社のセキュリティ予算を決定すること

c. 企業が直面するセキュリティリスクを評価・分析すること

d. セキュリティインシデントの発生回数を計測すること

答え：「c. 企業が直面するセキュリティリスクを評価・分析すること」

解説：リスクアセスメントは、組織の脅威や脆弱性を特定し、どのようなリスクが最も重大であるかを評価するプロセスです。

インシデント対応と事業継続

Q3. サイバー攻撃が発生した場合に、最初に行うべき対応はどれですか？

a. 影響を受けたシステムを速やかにオフラインにする

b. すぐに新しいセキュリティソフトウェアをインストールする

c. メディアにインシデントを報告する
d. インシデントの原因を調査するためのチームを編成する

答え：「a. 影響を受けたシステムを速やかにオフラインにする」
解説：サイバー攻撃を受けた場合、被害の拡大を防ぐために、まず影響を受けたシステムを隔離することが重要です。

プライバシー保護
Q4. プライバシー保護の観点から、企業が顧客の個人情報を処理する際に最も重要な点は何ですか？
a. データの物理的な保存場所を定期的に変更する
b. データ処理の目的を明確にし、顧客からの同意を得る
c. データを自動で削除するソフトウェアを購入する
d. 顧客にデータ処理の手続きを詳細に説明する

答え：「b. データ処理の目的を明確にし、顧客からの同意を得る」
解説：プライバシー保護法において、データ処理の目的を明示し、事前に顧客の同意を得ることは最も基本的かつ重要な要件です。

スキル習得目標の設定

身につけさせたいスキル（セキュリティ体制構築、セキュリティマネジメント、インシデント対応、プライバシー保護など）を明確にし、何をいつまでに習得するか具体的な目標を設定します。

目標設定の例

1. セキュリティ体制構築・運営
目標：
3 ヶ月以内に、基本的なセキュリティポリシーを策定して社内に共有し、従業員全員が日常業務においてそのポリシーを実践できるようにする。

2. セキュリティマネジメント
目標：
3 ヶ月以内に、主要なセキュリティリスクを把握し、それに基づいた簡単なリスク評価（例えば、データバックアップやアクセス権管理）を実施できるようにする。

3. インシデント対応と事業継続
目標：
3 ヶ月以内に、インシデント発生時の基本的な対応フロー（インシデントの報告、初期対応、関係者への連絡）を整備し、従業員がそのフローに従って行動できるようにする。

4. プライバシー保護

目標：
3 ヶ月以内に、顧客データや個人情報の取り扱いに関する基本的なガイドラインを策定し、従業員がデータ保護の基本的な手順を実践できるようにする。

2. 学習計画の作成

目標を達成するための計画を作成します。

計画作成のポイント

- シンプルで実践的な内容にする（即実践できるスキルを重視）
  複雑な理論よりも、日常業務で使えるシンプルなスキルを学ばせます。フィッシング対策やパスワード管理など、すぐに役立つ内容を中心にして、従業員がすぐに行動に移せるようにします。
- 段階的な進行と定期的なフィードバック（進捗を段階的に確認し、小さな成功を積み重ねる）

すべてを一度に学ばせるのではなく、段階ごとに小さな成功体験を積み重ねるプランにします。定期的に進捗を確認し、フィードバックを与えて次のステップに進める形にします。

計画作成の例

1. セキュリティ体制構築・運営

目標：3 ヶ月以内に、基本的なセキュリティポリシーを全従業員に共有し、日常業務において実践できるようにする。

第 1 週 - 第 2 週

セキュリティポリシーの作成

インターネット上で公開されている無料のセキュリティポリシーテンプレートを活用し、パスワード管理やフィッシング対策を含むシンプルなポリシーを作成します。

ツール例：NIST や中小企業向けサイバーセキュリティポリシーの無料リソースを利用。

第 3 週 - 第 4 週

社内で簡単な説明会を開催

経営者や IT 担当者がリーダーとなり、30 分程度の説明会を開催し、セキュリティポリシーの内容を簡単に説明します。

クイズやディスカッション形式で理解を深めます。

第 5 週 - 第 6 週

実践トレーニング

タスク： USB デバイスの管理と紙資料の処理に関する簡単な演習を実施。

内容

- USB デバイスの管理：従業員が USB メモリなどを使用する際、デバイスを適切に取り扱い、安全にデータを移動・管理する方法を実演。

例：外部デバイスを使う際のリスクや、使用後のデバイスの安全な保管方法を学びます。

- 紙資料の取り扱い：紙ベースの情報管理について、重要な資料の廃棄方法（シュレッダーの使用）や、デスクの片付け（クリアデスク）の実践演習を行います。
  例：印刷された重要書類をどのように処理すべきかを実際に体験させます。

第 7 週 - 第 12 週

簡単な社内チェックとフィードバック

月に 1 度、従業員がセキュリティポリシーを実践できているか簡単なチェックを行い、必要に応じて改善フィードバックを行います。

2. セキュリティマネジメント

目標：3 ヶ月以内に、主要なセキュリティリスクを把握し、簡単なリスク評価を実施できるようにする。

第 1 週 - 第 2 週

主要なリスクのリストアップ

経営者と IT 担当者がリーダーとなり、事業に関連するリスク（データ漏えい、内部不正、機器故障など）をリストアップし、シンプルなリスク評価シートを作成します。

第 3 週 - 第 4 週

データバックアップの実施指導

各部門で定期的に重要データのバックアップが行われるように指導し、クラウドストレージを利用してデータ保護を強化します。

第 5 週 - 第 6 週

アクセス権限の簡単な見直し

各部門で使用しているファイルやシステムに対して、必要な人だけがアクセスできるよう、アクセス権限を見直します。特別なシステムがない場合は、共有フォルダの権限設定を調整。

第 7 週 - 第 12 週

リスク評価結果の共有

各部門が実施したリスク評価の結果を簡単な報告書としてまとめ、全体会議で共有します。大きなリスクに対する対応策を検討し、全従業員に対策を通知。

3. インシデント対応と事業継続

目標：3 ヶ月以内に、インシデント発生時の基本的な対応フローを整備し、従業員が対応できるようにする。

第 1 週 - 第 2 週

シンプルなインシデント対応フローを作成

報告から初期対応、上司や関係部署への連絡までのシンプルなフローを作成します。例えば、チャットやメールで報告する際のフォーマットを準備。

第 3 週 - 第 4 週

インシデント対応説明会

全従業員に対して、インシデント対応フローの説明会を開催し、実際のシナリオを使って報告の練習を行います。

第 5 週 - 第 6 週

インシデント対応シミュレーション

簡単なインシデント（例えば、ウイルス感染やデータ損失）を想定したシミュレーションを実施し、従業員がフローに従って報告・対応できるかを確認します。

第 7 週 - 第 12 週

定期的なチェックと改善

週に 1 度、インシデントが発生した場合の報告フローをチェックし、問題がないかを確認し、必要に応じてフローを改善します。

4. プライバシー保護

目標：3 ヶ月以内に、顧客データや個人情報の取り扱いガイドラインを策定し、従業員が実践できるようにする。

第 1 週 - 第 2 週

シンプルなガイドライン作成

法令（個人情報保護法）を参照しつつ、データの収集、保存、破棄に関する基本的な手順をガイドラインとして作成。データの最小限の収集や、不要なデータの定期的な削除方法などを明確にします。

第 3 週 - 第 4 週

従業員向けガイドラインの共有

ガイドラインを全従業員に配布し、短い説明会を通じてデータ保護の基本的な考え方を共有します。

第 5 週 - 第 6 週

データ保護の実践

従業員が日常業務の中で、顧客データの取り扱いやアクセス権の管理を実際に行えるよう指導し、定期的なデータ監査を行います。

第 7 週 - 第 12 週

フォローアップと改善

ガイドラインが遵守されているか、簡単なチェックリストを作成し、各部門で確認します。問題点があればすぐに改善策を検討し、再度周知します。

作成した計画をガントチャートにすることで、進捗管理が容易になったり、スケジュール管理が容易になったりするため、効率的に学習を進めることができます。

「セキュリティ体制構築・運営」のガントチャート作成例

タスク ID	タスク名	担当者	開始日	終了日	前提条件	リソース	依存関係	成果の確認ポイント
1	セキュリティポリシーの作成	IT 部門	2024/1/5	2024/1/17	なし	NIST テンプレート	なし	セキュリティポリシー作成完了
2	セキュリティポリシーのレビューと最終化	IT 部門	2024/1/18	2024/1/19	セキュリティポリシーの作成完了	内部リソース	タスク ID 1	ポリシー最終化
3	社内向けセキュリティポリシー説明会の準備	総務部	2024/1/22	2024/1/26	ポリシーがレビューされていること	プレゼンテーション資料、共有スペース	タスク ID 2	説明会準備完了
4	社内向けセキュリティポリシーの説明会開催	総務部	2024/1/29	2024/2/2	説明会準備完了	参加者、プレゼンテーション資料	タスク ID 3	説明会開催完了
5	USB デバイス管理演習	IT 部門	2024/2/5	2024/2/9	なし	USB メモリ	なし	演習完了
6	紙資料処理演習	総務部	2024/2/13	2024/2/19	USB デバイス管理演習完了	シュレッダー、チェックリスト	タスク ID 5	演習完了
7	セキュリティポリシーの実践状況チェック	IT 部門	2024/2/20	2024/3/4	なし	チェックリスト	なし	ポリシー実践確認完了
8	フィードバックと改善提案の作成	IT 部門	2024/3/5	2024/3/25	チェック完了	フィードバックフォーム	タスク ID 7	改善提案完了

タスク名	担当者	開始日	終了日	2024年1月				2024年2月				2024年3月			
				第1週	第2週	第3週	第4週	第1週	第2週	第3週	第4週	第1週	第2週	第3週	第4週
セキュリティポリシーの作成	IT部門	2024/1/5	2024/1/17	■	■										
セキュリティポリシーのレビューと最終化	IT部門	2024/1/18	2024/1/19			■									
社内向けセキュリティポリシー説明会の準備	総務部	2024/1/22	2024/1/26			■									
社内向けセキュリティポリシーの説明会開催	総務部	2024/1/29	2024/2/2				■								
USBデバイス管理演習	IT部門	2024/2/5	2024/2/9					■							
紙資料処理演習	総務部	2024/2/13	2024/2/19						■						
セキュリティポリシーの実践状況チェック	IT部門	2024/2/20	2024/3/4							■	■				
フィードバックと改善提案の作成	IT部門	2024/3/5	2024/3/25									■	■	■	■

ガントチャート作成のポイント

- タスクを具体的に分解する
  プロジェクト全体を小さな作業単位（タスク）に分け、それぞれが具体的で実行可能な内容にします。
  例：「セキュリティポリシー作成」「説明会の準備」など
- 依存関係とスケジュールを設定する
  各タスクの実行順序と、前のタスクが完了しないと次に進めない場合の依存関係を明示します。
  また、各タスクの開始日と終了日を設定し、全体のスケジュール管理ができるようにします。
  例：「ポリシー作成が終わってから説明会準備を開始」
- 成果物（完了条件）を明確にする
  各タスクの完了を確認するための成果物や基準を設定し、進捗状況を評価しやすくします。
  例：「セキュリティポリシーの最終版完成」「説明会が無事に開催された」

これら 3 つのポイントを押さえることで、WBS がシンプルかつ効果的なものになります。

3.学習計画の周知と実施準備

- 従業員への周知
  作成した学習計画を全従業員に共有し、学習目標、内容、進め方について説明します。従業員が学習計画の重要性を理解し、積極的に参加できるように動機づけることが大切です。

- 学習環境の整備
  e ラーニングの導入や、教材、トレーニング資料の準備を整えます。もし外部講師や専門家を招く場合は、そのスケジュールを確保しておきます。
- 担当者の配置とサポート体制の構築
  プランの進行を管理する担当者を設定し、従業員の学習をサポートする体制を整えます。質問や問題が発生した際にすぐに対応できる窓口を作ることも重要です。

4.学習の実行

- スケジュールに従ってトレーニングを進行
  作成したカリキュラムやスケジュールに沿って、トレーニングを開始します。各セッションやモジュールが順調に進んでいるかを確認し、必要に応じて進行を調整します。
- 進捗報告の仕組みの導入
  定期的に学習進捗を確認し、例えば週次または月次の進捗報告会を設けて従業員に学習の進捗状況を報告させることは有効です。これにより、モチベーションを維持し、計画の遅れを早期に発見できます。

5.フィードバックと進捗管理

- 定期的なチェックポイントを設定
  学習プランが順調に進んでいるか確認するために、定期的に学習内容のテストや確認を行います。これにより、理解度の確認と学習の定着を測定できます。
- 従業員からのフィードバック収集
  トレーニングの内容や進め方について、従業員からフィードバックを収集します。もし内容が難しすぎる、もしくは簡単すぎる場合には、カリキュラムの調整を検討します。

6.学習プランの調整

- 進捗に応じたプランの見直し
  進捗状況やフィードバックに基づき、学習プランを柔軟に調整します。例えば、理解が進んでいる分野はスピードアップし、苦手な部分には追加トレーニングを提供するなど、個々の従業員のニーズに合わせた調整が必要です。
- モチベーション向上施策
  成果が見えにくい段階では、従業員のモチベーションが下がる可能性があります。そのため、小さな成功体験や報酬（例えば、社内での称賛や学習ポイントによるインセンティブ）を設定し、モチベーションを維持します。

7.成果の評価とフィードバック

- 成果の測定とフィードバックの提供
  学習が一通り終了したら、最終的なテストや評価を行い、どの程度スキルが習得されたかを確認します。各従業員に対して個別のフィードバックを行い、今後の改善点やさらなる学習の方向性を示します。
- 学習効果の測定
  学習による効果がどの程度業務に反映されているかも重要です。例えば、セキュリティインシデントの減少や、従業員のセキュリティ対応能力の向上が確認できれば、学習プランが効果的であったと判断できます。

8.フォローアップと継続学習

- 継続的な学習計画の策定
  セキュリティは常に進化しているため、1 度の学習プランで終わるのではなく、継続的な学習計画を策定します。例えば、最新のサイバーセキュリティ脅威に対応するための定期的なアップデートや新しいツールの習得を含めた継続学習が必要です。
- 従業員の定着度合いのモニタリング
  学習内容が業務の中でどの程度実践されているかをモニタリングします。セキュリティインシデント対応やセキュリティガイドラインの実施状況を確認し、従業員が習得したスキルを日常的に活用しているか否かを把握します。

これらのステップを通じて、作成した学習プランが効果的に実行され、従業員が必要なスキルを確実に習得することができます。特に、進捗管理とフィードバックの提供を徹底し、学習の定着を促すことが成功の鍵です。

編集後記

第 9 編では、組織としてサイバーセキュリティ対策を実践するためのスキルや知識、そしてそれらを備えた人材の育成について紹介しました。本編では、経営層から現場のマネジメント層に至るまで、それぞれの役割に応じた教育プログラムやカリキュラムの具体例を取り上げ、企業が持続的なセキュリティ体制を築くための実践的な指針を提供しています。特に、デジタル時代において求められるスキル標準や人材育成の重要性を強調し、セキュリティリスクの管理や対応において、適切な判断を行うための知識の習得が不可欠であることを解説しています。

さらに、変化の速いこの領域では、リスキリングの取り組みが重要です。従業員が新たな知識やスキルを継続的に学ぶことで、組織全体のセキュリティ対応力が高まり、急速に進化する脅威に柔軟に対応できるようになります。リスキリングを通じて、個々のスキルをアップデートしながら、組織としても最新のセキュリティ標準に適応できる体制を整えることが、今後の競争力強化につながります。

本編で紹介したカリキュラムや講座は一つの例です。業種、企業規模などによって合わない場合もあります。状況に合わせて内容を取捨選択し、自社にあった教育プログラムを作成していただくことで、より効果的・効率的に人材育成が可能です。紹介したカリキュラムを参考に自社のご状況を踏まえたカリキュラム作成、講座の選定をお勧めします。

本編で学んだ内容を活用し、各自が組織のセキュリティを高めるための一歩を踏み出していただければと思います。

引用文献

デジタルスキル標準ver.1.2（PDF）

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/#general_No03

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
プラス・セキュリティ知識補充講座 カリキュラム例
https://security-portal.nisc.go.jp/dx/pdf/plussecurity_curriculum.pdf
ITスキル標準モデルカリキュラム –レベル 1を目指して–
https://www.ipa.go.jp/archive/jinzai/skill-standard/itss/qv6pgp000000buc8-att/000024802.pdf
マナビDXでの学び方
https://manabi-dx.ipa.go.jp/how

参考文献

デジタルスキル標準

https://www.meti.go.jp/policy/it_policy/jinzai/skill_standard/main.html

デジタルスキル標準ver.1.2（PDF）

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（Ver.6.4）

https://www.ipa.go.jp/shiken/syllabus/nl10bi0000007sxy-att/syllabus_ip_ver6_4.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/

G検定の試験範囲（シラバス）と例題

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

ITスキル標準V3

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

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Ｖ３ 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

ITSS+（プラス）データサイエンス領域

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

IPA ITSS+（プラス）IoTソリューション領域

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

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/curriculum/

ITパスポート試験 試験内容・出題範囲

https://www3.jitec.ipa.go.jp/JitesCbt/html/about/range.html

IPA 試験要綱・シラバスについて

https://www.ipa.go.jp/shiken/syllabus/gaiyou.html

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®とは

https://japan.isc2.org/cissp_about.html

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

プラス・セキュリティ知識

https://security-portal.nisc.go.jp/dx/plussecurity.html

プラス・セキュリティ知識補充講座 カリキュラム例

https://security-portal.nisc.go.jp/dx/pdf/plussecurity_curriculum.pdf

ITスキル標準とは -ものさしとしてのスキル標準

https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/itss2.html

ITスキル標準モデルカリキュラム－レベル 1を目指して－

https://www.ipa.go.jp/archive/jinzai/skill-standard/itss/qv6pgp000000buc8-att/000024802.pdf

デジタル人材育成政策のご紹介

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

【ほぼ15秒アニメ】子ブタと学ぼう！情報セキュリティ対策のキホン

https://www.ipa.go.jp/security/anshin/measures/start.html

■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。

22-1-1、22-1-2、22-3-1、23-1、23-1-2、23-1-3、23-2、24-3、25-1

■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。

22-3-4、23-2

■CVSS

Common Vulnerability Scoring System の略。情報システムの脆弱性に対するオープンで汎用的な評価手法のこと。ベンダーに依存しない共通の評価方法を提供している。CVSS を用いると、脆弱性の深刻度を同一の基準の下で定量的に比較できるようになる。ベンダー、セキュリティ専門家、管理者、ユーザなどの間で、脆弱性に関して共通の言葉で議論できるようになる。

23-2

■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。

22-3-1

■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。

22-3-1

■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。

22-1-2、22-3、22-3-3、23-1-1、23-2、23-2-4、24-3、25-2-2

■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。
23-1-1、23-2、25-2-1、25-2-2

■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。
23-2、25-1

■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。
21-1-5、23-1-2

■NCO
National Cybersecurity Office の略。国家サイバー統括室の略。2025 年 5 月に成立したサイバー対処能力強化法および同整備法を受け、内閣サイバーセキュリティーセンター（NISC）を改組し、同年 7 月 1 日、内閣官房に設置された。サイバーセキュリティ戦略本部の事務局として、サイバーセキュリティの確保に関する総合調整の役割を担う。
22-3-4、24-1

■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。
22-2-2

■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。
22-1-1、22-3-2

■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。
22-3-1、23-2

■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。
25-2-1

■WAF（Web アプリケーションファイアウォール）
Web Application Firewall の略で、「Web アプリケーションの脆弱性を悪用した攻撃」から Web サイトを保護する

セキュリティ対策。Web サーバーの前段に設置して通信を解析・検査し、攻撃と判断した通信を遮断することで、Web サイトを保護する。
23-2

■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。
22-1-1

■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。
23-2

■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。
22-3-1、23-1-2、25-2-1、25-2-2

■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。
22-1-1、22-3-1、25-2-1、25-2-2

■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。
22-2-2、22-3-1、22-4-1、23-2、25-2-2

■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。
22-3-1、23-2、25-2-2

■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。
22-3-1、23-2、25-2-2

■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。
22-1-2

■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。
23-1-2

■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。
22-1-2、22-3-1、22-3-4、23-2、24-3、25-1、25-2-2

■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。

23-1-1、23-2、23-2-1、
24-3、25-2-1

■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。

22-1-2、22-2-2、23-2-4、
23-2-5、25-2-2

■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。

22-1-2、23-1-1、23-2、
23-2-5、24-1、24-1-1、
24-1-2、25-2-1、25-2-2

■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。

22-1-2、22-3-1、23-1-1、
23-2-1、23-2-5、24-1-1、
25-2-2

■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。

22-3-1、23-2、23-2-1、
25-2-1、25-2-2

■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。

22-3-1

■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」

22-2-2、22-2-3、22-3-1、
23-1-1、24-1-2、

■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。

23-2

■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。

22-1-2、22-3、22-3-1、
23-1、23-1-2、24-3

■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
22-1-2、24-1、24-1-2、24-2

■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。
22-3-1

■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。
23-2

■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。
22-3-1、23-2、25-2-1

■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。
22-1-2、22-2-3、23-2

■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。
22-3-1、23-1-1、23-2、25-2-1

■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。
22-2-2、25-2-1

■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。

25-2-1

■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。

22-3-1、25-2-2

■ペネトレーションテスト

ネットワークに接続されたシステムの安全性を検証するテスト手法。すでに知られているサイバー攻撃手法を使って実際にシステムに侵入や攻撃を試みることで攻撃耐性を確認する。

23-2

■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。

22-3-1、22-3-4、23-2、23-2-5

■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。

23-2

■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

22-1-2、25-2-2

■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

25-2-2

経営層向けカリキュラム

経営層向け第１単元	
名称	**1.基礎知識** **『デジタルシステムとサイバーセキュリティの概要』**
目標	● デジタルシステムとそのサイバーセキュリティ対策に関して経営層として次のような場面において適切な判断を行う上で、どのようなことを予め知っておくべきなのかの自覚を促す。 ➢ 担当者による提案についての、自社のニーズ、競争力、コストなどの面からの妥当性 ➢ 新たな施策に伴うリスクとその抑制策の妥当性
到達レベル	● 関係者とのコミュニケーションにおいて用いられる概念と用語について、コミュニケーションに支障の無い程度の理解を得る。
時間設定・実施方式	1 時間 30 分（オンデマンド・省略可能）
①デジタルインフラの基本（30 分）	ビジネスで用いられるデジタルアーキテクチャの構成要素とその意味について概説する。受講者の負担軽減の観点から、まとめて学習するほうがよい内容を適宜集約する。 a) デジタルサービスの提供に用いられるハードウェアの概要 b) OS、ミドルウェア、アプリケーション、クラウドの概念説明 c) IT/OT/IoT の違い、クラウド/オンライン会議の仕組み d) デジタルビジネスの主要プレイヤー
②デジタル技術の基盤とリスク（30 分）	デジタル環境の利便性の代償としてシステムトラブルやサイバーセキュリティインシデントがあり、それぞれリスクに応じた対策が用意されているが、一般に対策の効果を高めるほど、利便性又はコストに影響が及ぶ関係にあることを説明する。 a) ソフトウェアと脆弱性 b) インターネットの仕組み c) デジタルリスクとその対策に関する技術的概念
③デジタル環境のコストと運用責任（30 分）	デジタル基盤を快適に利用している中で、どこにどのように費用がかかっているのかについて、課金方法の種類を含めて説明する。また、トラブルが生じたときのベンダーとの責任分界点や、事業継続計画の必要性について説明する。 a) インターネットを安全に利用するための費用 b) デジタルサービスの約款 c) インシデント時の事業継続

経営層向け第２単元	
名称	**2.脅威と対策** **『サイバー空間における脅威と対策』**
目標	● 脅威および脆弱性とその対策に関する理解を通じて、サイバー空間における主要な脅威を事業上のリスクとして適切に把握できるようになる。
到達レベル	● 現在のデジタル環境では脆弱性による影響をゼロにできず、最新の脅威につねに対処していく必要があることを理解し、対策をしなかった場合の自社での被害想定ができるようになる。
時間設定・実施方式	1 時間 30 分（オンデマンド 60 分、集合講習 30 分）
①サイバー攻撃手法とそのトレンド（オンデマンド・30 分）	サイバーセキュリティリスクをもたらす脅威について、誰がどのように影響を及ぼすのかの概要を説明した上で、現在のトレンドから、今後自社にどのようなインパクトを及ぼす脅威が見込まれるのかを、具体的な被害事例を交えて説明する。 a) おもな攻撃手法 b) 脅威の関係主体と攻撃の動向 c) 最新の脅威
②脅威への対策（オンデマンド・30 分）	脅威による影響を抑制する手段としてどのようなものがあるか説明する。第３単元において自社事業の内容に応じたリスクへの対応方法を扱うことを踏まえ、その前提となる基本的な考え方の理解に重点を置く。 a) 対策の具体的な運用方法 b) 対策実施上の留意点
③事例紹介（集合講習・30 分）	①②をオンデマンド教材によって行うことへの補強として、具体的にリスクが発現したケースについて被害と対策の事例を紹介し、対策が期待通りに行かないのはどのような場合かなど、実践的な内容を説明する。 • ケース紹介（例：工場停止の影響） • ゲストスピーカーによる説明（例：当事者視点でのインシデント経過の説明） • デモンストレーション（例：ランサムウェア感染のデモ）

経営層向け 第３単元	
名称	**3.投資** **『サイバーセキュリティと投資対効果』**

目標	● どのような場合にサイバーセキュリティリスクが企業価値の毀損を生じさせるのかを理解し、それを防ぐために日常でサイバーセキュリティ対策としてどのような投資などの方策を行うべきかに関して適切な判断を行えるようになる。
到達レベル	● 自社におけるサイバーセキュリティリスクを特定し、対応の優先順位付けや対処方針の選定を行うとともに、その実現に必要な体制構築や人材確保・育成に関する指示を行えるようになる。 ● セキュリティ対策の担当者から提示されるセキュリティ対策案について、経営層として妥当性に関する判断を下せるようになる。
時間設定・実施方式	2 時間 10 分（オンデマンド 60 分、集合講習 70 分）
①コーポレートリスクとしてのサイバーセキュリティ（オンデマンド・30 分）	サイバーセキュリティリスクは他のコーポレートリスクとどのように異なるかを、対応方法を通じて理解する。受講者がリスクマネジメントそのものの考え方や保険の仕組みなどは理解していることを前提に、②以降の説明で必要となる概念を確認する。 a) サイバーセキュリティリスクのアセスメント b) リスクへの対応方法 c) 関連法制度とコンプライアンス
②体制構築・人材確保（オンデマンド・30 分）	各種公表資料を参考に、企業の特徴に応じた体制や人材確保・育成に関する考え方を理解する。 a) サイバーセキュリティ対策に関する機能と役割の考え方 b) 外部委託の考え方 c) サイバーセキュリティ体制の構築 d) サイバーセキュリティ対策に従事する人材の確保・育成
③演習 1：各種対策の費用、損失想定、確率値から必要な投資を検討（集合講習：70 分）	サイバーセキュリティ対策における費用対効果分析の基本的な考え方について、事例を踏まえて説明する。受講者 3～4 名で 1 チームを構成し、具体例を想定した上で、ゲーム形式で各種対策の費用、損失想定、確率値から必要な投資を検討し、トータルコストの最小化を競う。

経営層向け 第 4 単元	
名称	**4.ステークホルダーとの関係** **『サイバーセキュリティと企業価値』**
目標	● サイバーセキュリティインシデントの発生時の適切な対応について理解した上で、企業価値を損なわないためにあらかじめ備えておくべきことを自社の事情に応じてイメージできるようになる。

到達レベル	● 自社におけるインシデント対応を含むサイバーセキュリティ対策に関する取組方針について、対外的に説明や意見交換ができるレベルの理解に到達する。
時間設定・実施方式	2 時間 20 分（オンデマンド 60 分、集合講習 80 分）
①インシデント対応における経営層の役割（オンデマンド・30 分）	サイバーセキュリティインシデントの対応プロセスにおいて、経営層がどの場面でどのようにかかわるのが適切なのかを理解する。 a) インシデントに備える b) インシデント対応プロセス
②情報開示の在り方（オンデマンド・30 分）	サイバーセキュリティ対策を適切に実施していることを取引先や社会に伝えることにより、企業価値の維持・向上を図る方法について理解する。 a) サイバーセキュリティに関する情報開示の考え方 b) サイバーセキュリティが企業価値に及ぼす影響
③インシデント対応と情報開示の事例から学ぶ（集合講習：30 分）	①②をオンデマンド教材によって行うことへの補強として、インシデント対応と情報開示の事例を紹介し、当初の見通しと異なる状況が生じた場合の適切な対応方法等、実践的な内容を説明する。
④演習 2：インシデント発生時の模擬記者会見（集合講習：50 分）	受講者 3～4 名で 1 テーブルとして、経営者役の 1 名が、マスメディアや企業の広報部門等で記者会見対応に関する経験を有するスタッフが演じるインタビュア役から、自社でのインシデント発生に関する模擬記者会見を行う。

(出典) NCO「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

部課長向けカリキュラム

部課長級向け 第 1-1 単元	
名称	**1.基礎知識** **『デジタルシステムとサイバーセキュリティの概要（初級編）』**
目標	デジタル化を推進する部門のマネジメントを担う部課長として中級編の目標に到達するために必要となる、最低限の基礎知識を習得する。
到達レベル	● デジタルシステムとインターネットおよびそれらのセキュリティ対策において用いられる最低限の知識を習得する。
時間設定・実施方式	1 時間（オンデマンド・省略可能）
①デジタルインフラ入門（20 分）	ビジネスで用いられるデジタルアーキテクチャの構成要素について、基本的な用語の意味を理解する。

	a) デジタルサービスの提供に用いられるハードウェアの紹介 b) OS、ミドルウェア、アプリケーション、クラウドの用語説明 c) IT/OT/IoT がそれぞれ意味するもの
②サイバーセキュリティに関する用語の意味（20 分）	「セキュリティは難しい」という印象を与える背景として、「脆弱性」など日常で用いられないさまざまな用語が用いられることから、よく用いられるサイバーセキュリティ用語の意味の説明を通じて理解を深める。なお、サイバーセキュリティ用語を説明する上で必要となる、ソフトウェアやネットワークに関する用語についても併せて説明する。 a) ソフトウェア開発と脆弱性 b) インターネットの仕組み c) デジタルのリスクに関する諸概念
③デジタル環境の管理や責任に関するキーワード（20 分）	インターネットを通じたサービスなどの提供主体と責任に関する用語について説明する。 a) デジタルビジネスの提供者に関する用語 b) 管理と責任の所在

部課長級向け 第 1-2 単元	
名称	**1.基礎知識** **『デジタルシステムとサイバーセキュリティの概要（中級編）』**
目標	デジタル化を推進する部門のマネジメントを担う部課長として次のような場面において適切な判断を行う上で、どのようなことを予め知っておくべきなのかの自覚を促す。 ● 担当者による提案についての、自社のニーズ、競争力、コストなどの面からの妥当性 ● 新たな施策に伴うリスクとその抑制策の妥当性
到達レベル	● デジタルシステムとサイバーセキュリティに関する用語と概念について、第 2 単元目以降の学習を行うために予め習得しておくべきレベルに到達させる。具体的には、対象とする用語と概念を用いて、デジタルシステムやサイバーセキュリティ対策に関するソリューションを提供するベンダーとの実用的な対話に支障の無い程度の理解を得ることにする。
時間設定・実施方式	1 時間 30 分（オンデマンド・必須）
①デジタルインフラの要点（30 分）	ビジネスで用いられるデジタルアーキテクチャの構成要素とその意味について概説する。 a) デジタルサービスの提供に用いられるハードウェアの構成要素 b) OS、ミドルウェア、アプリケーション、クラウドなどの概念説明

	c) IT/OT/IoT の違い、クラウド/オンライン会議の仕組み d) デジタルビジネスの主要プレイヤーの役割
②デジタル技術の基盤とリスク（30 分）	デジタル環境の利便性の代償としてシステムトラブルやサイバーセキュリティインシデントがあり、それぞれリスクに応じた対策が用意されているが、一般に対策の効果を高めるほど、利便性又はコストに影響が及ぶ関係にあることを説明する。 a) ソフトウェア開発と脆弱性 b) デジタルリスクとその対策に関する技術的概念
③デジタル環境のコストと運用責任（30 分）	デジタル基盤を快適に利用している中で、どこにどのように費用がかかっているのかについて、課金方法の種類を含めて説明する。また、トラブルが生じたときのベンダーとの責任分界点や、事業継続計画の必要性について説明する。 a) インターネットを安全に利用するための費用 b) デジタルサービスの約款 c) インシデント時の事業継続

部課長級向け 第 2 単元	
名称	**2.脅威** **『サイバー空間における脅威と対策』**
目標	脅威および脆弱性とその対策に関する理解を通じて、サイバー空間における主要な脅威を事業上のリスクとして適切に把握できるようになる。
到達レベル	● 現在のデジタル環境では脆弱性による影響をゼロにできず、最新の脅威につねに対処していく必要があることを理解し、対策をしなかった場合の自社での被害想定ができるようになる。
時間設定・実施方式	2 時間 30 分（オンデマンド 60 分、集合講習 90 分）
①サイバー攻撃手法とそのトレンド（オンデマンド・30 分）	サイバーセキュリティリスクをもたらす脅威について、誰がどのように影響を及ぼすのかの概要を説明した上で、現在のトレンドから、今後自社にどのようなインパクトを及ぼす脅威が見込まれるのかを、具体的な被害事例を交えて説明する。 a) おもな攻撃手法 b) 脅威の関係主体と攻撃の動向 c) 最新の脅威
②脅威への対策（オンデマンド・30 分）	脅威による影響を抑制する手段としてどのようなものがあるか説明する。第 3 単元において自社事業の内容に応じたリスクへの対応方法を扱うことを踏まえ、その前提となる基本的な考え方の理解に重点を置く。 a) 対策の具体的な運用方法

	b) 対策実施上の留意点
③事例紹介（集合講習：30 分）	①②をオンデマンド教材によって行うことへの補強として、具体的な脅威と対策の事例を紹介し、対策が期待通りに行かないのはどのような場合かなど、実践的な内容を説明する。<デモンストレーションの実施についても検討>
④演習 1：脅威と対策における“悪い見本”から学ぶ（集合講習：60 分）	受講者 3～4 名で 1 テーブルとして、仮想の企業が実施する脅威への不適切な事前準備（リスク評価、資産管理、パッチ適用、従業員教育など）に関する動画（8 分程度）を視聴し、どこに問題があるかを理由と共に指摘し合う。なお、本ディスカッションでは問題の抽出のみにとどめ、対策方法には踏み込まない。

部課長級向け 第 3 単元	
名称	**3.投資** **『サイバーセキュリティとリスク対応』**
目標	自部署におけるサイバーセキュリティリスクのマネジメントに必要となる概念と、具体的なアクションについて理解する。
到達レベル	● 部署におけるサイバーセキュリティリスクを特定し、対応の優先順位付けや対処方針の選定を行うとともに、その実現に必要な体制や要員の確保・育成を行えるようになる。 ● 担当者や社外ベンダーから提示されるセキュリティ対策案について、組織として妥当性に関する判断を下せるようになる。
時間設定・実施方式	2 時間 30 分（オンデマンド 60 分、集合講習 90 分）
①サイバーセキュリティのリスクマネジメントの特徴（オンデマンド・30 分）	サイバーセキュリティリスクは他のコーポレートリスクとどのように異なるかを、対応方法を通じて理解する。 a) サイバーセキュリティにおけるリスクの特徴 b) リスクへの対応方法 c) サイバーセキュリティ対策に関する機能と役割の考え方
②対策における費用と損失の考え方（オンデマンド・30 分）	費用をかけてサイバーセキュリティ対策を実施しても、インシデントが生じない場合の効果が見えにくい。その場合に「何も対策をしていなければ」といった仮定により想定される損失額を試算し、妥当性を評価する方法について理解する。 a) サイバーセキュリティインシデントによる損失 b) 発生確率の考え方 c) 費用と効果のバランス
③リスクマネジメントのケーススタディ	①②をオンデマンド教材によって行うことへの補強として、具体的なリスク対応体制の事例を紹介し、発生確率や被害の大きさに関する仮定の

（集合講習：30 分）	置き方によってどのように分析結果が変化するかなど、実践的な内容を説明する。
④演習 2：自部署リスクとその対応策を洗い出し、リスク管理部門などへ説明（集合講習：60 分）	受講者 3～4 名で 1 チームを構成し、各参加者はあらかじめ自業種のビジネスモデルと想定するリスクについて整理したものを持ち寄る。それを他の参加者でサイバーセキュリティリスクがどのようなところにあるかを、第 3 単元の内容をもとに相互に指摘する。それについて、第 3 単元で学習したリスクの低減策のうち、どれを適用すべきかを②の内容を踏まえて受講者で議論。1 クール 12～15 分＋講師の講評で構成。

部課長級向け 第 4 単元	
名称	**4.ステークホルダーとの関係** **『サイバーセキュリティ対応における社内外連携』**
目標	デジタル化を推進していく際のサイバーセキュリティ対策、運用時のインシデントへの適切な対応について理解した上で、その効果を担保するために実施すべき情報開示や連絡の内容と効果的な方法について理解し、実践できるようになる。
到達レベル	● 自部署に係るサイバーセキュリティ対策に関する社内外のコミュニケーション（情報収集、協議、エスカレーションなど）について、実用レベルで実施できる。
時間設定・実施方式	2 時間 30 分（オンデマンド 60 分、集合講習 90 分）
①インシデント対応プロセスとその準備（オンデマンド・30 分）	サイバーセキュリティインシデントの対応プロセスの一連の流れを理解する。 a) インシデントに備える b) インシデント対応プロセス
②インシデント時の情報の取扱上のポイント（オンデマンド・30 分）	即応性や要求されるインシデント発生時に、社内関係者や取引先との間でどのような情報のやりとりが必要になるか、そのために予め準備しておくことは何か、確実性を含む情報をどのように取り扱うべきかなどについて理解する。 a) インシデント時に提供すべき情報の種類と流れ b) 不確実性を含む情報の取扱い
③インシデント対応と情報開示の事例から学ぶ（集合講習：30 分）	①②をオンデマンド教材によって行うことへの補強として、インシデント対応と情報開示の事例を紹介し、当初の見通しと異なる状況が生じた場合の適切な対応方法など、実践的な内容を説明する。
④演習 3：インシデント発生時の社内外	受講者 3～6 名で 1 テーブルとして、社内関係者や取引先の役割を演じる受講者に対し、所管部署の事業を通じて発生したインシデントに関す

連絡（集合講習：60 分）	る情報を伝え、不満や混乱を生じさせないためにはどのような点に留意すべきかを工夫する。あらかじめ講師側にてインシデントのシナリオを作成しておき、被害状況や SOC から提供される情報を時間経過に応じて小出しの形で提供する。小出しする方法はカードに記載して提示、あるいはオンライン会議システムのチャット機能で提供するなど工夫してよい。最終的に、判断が適切に行えていたか否かを自己評価し、講師側の評価と対比する。

部課長級向け 第 5 単元	
名称	**5.関連法令** **『サイバーセキュリティに関する法制度』**
目標	サイバーセキュリティ対策で関連する法律、基準、ガイドラインなどについて、実用上支障が無い程度の理解を得る。
到達レベル	● デジタル化に関連する取組の中で、遵守すべき法律、基準、ガイドラインなどを意識することができる。
時間設定・実施方式	1 時間（オンデマンド・必須）
①サイバーセキュリティに関する国内法令とその読み方（20 分）	サイバーセキュリティ対策の企画・実践に従事する要員が留意すべき法令と具体的な解釈の方法について、『サイバーセキュリティ関係法令 Q&A ハンドブック』の活用を前提に紹介する。 a) サイバーセキュリティ対策において留意すべき法令 b) 『サイバーセキュリティ関係法令 Q&A ハンドブック』の活用
②サイバーセキュリティに関する基準・規格など（20 分）	サイバーセキュリティ対策を実践する上で留意すべき国際基準や規格などについて紹介する。 a) サイバーセキュリティに関する基準・規格など
③サイバーセキュリティに関するガイドラインなど（20 分）	企業がサイバーセキュリティ対策を実践する上で活用が有益なガイドライン・フレームワークなどを紹介する。 a) サイバーセキュリティに関するガイドライン・フレームワークなど

(出典) NCO「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

IT 入門（1）

タイトル	学習目標
オリエンテーション、情報化の変遷と代表的な情報システムの特徴	情報化の変遷と代表的な情報システムの特徴を説明できる。
業種別、業務別の代表的なシステムの概要	企業の組織と利用されている業種別、業務別の代表的なシステムの概要を説明できる。
企業活動と企業会計の基本用語	企業活動の成果を評価するための、会計の基本用語を説明できる。
情報化戦略を策定するために必要な基本用語	経営目標から情報化戦略を策定するために必要な、基本的な用語を説明できる。
情報システム戦略の目的と考え方	企業の事業戦略を受けて、情報システム戦略と全体システム化計画策定に必要な手順と用語が説明できる。
業務要件定義と解決策の検討	情報システム戦略を受けて、自部門の業務課題を分析して、業務要件を定義する代表的な手法と用語を説明できる。
企業規範と身近な法律用語	企業の規範、社会・職場で必要となる身近な法律の用語を説明できる。
前半のまとめ	これまでのストラテジ系科目全体の講義のまとめを行う。
ソフトウェア開発プロセスの作業概要と手順	業務要件をもとに、システム要件の定義から稼働までの作業手順と作業項目の用語を説明できる。
代表的なソフトウェア開発手法の概要	代表的な開発手法に関する目的と概要を説明できる。
情報化におけるプロジェクトの種類とプロジェクト遂行の手順	情報化におけるプロジェクトの種類とプロジェクト計画の立案、開発管理、プロジェクトの完了までの手順と用語を説明できる。
システム運用に関する基本用語	IT サービスマネジメントの意義と目的、サービスマネジメントの全体像とシステム運用に関する用語を説明できる。
システム監査の種類と必要性	情報システムの信頼性、安全性、効率性の向上のために行う、システム監査の必要性および監査の種類と用語を説明できる。
後半のまとめ	これまでのマネジメント系科目全体の講義のまとめを行う。
まとめ	これまでの講義内容を総括する。

(出典) IPA「IT スキル標準モデルカリキュラム－レベル 1 を目指して－」をもとに作成

IT 入門（2）

タイトル	学習目標
オリエンテーション、コンピュータ上での情報表現	数値や文字情報をコンピュータ上で表現する方法と用語を説明できる。
プログラミングの役割	アルゴリズムとプログラミングとの関係を説明できる。
コンピュータの種類と構成する装置	コンピュータを構成する装置と役割を説明できる。
ソフトウェアの種類と役割	ソフトウェアの種類と役割を説明できる。
システム処理形態と処理方式	システムの処理形態と処理方式の用語を説明できる。
前半のまとめ	前半の講義のまとめを行う。
マルチメディアとヒューマンインタフェース	マルチメディアの種類とヒューマンインタフェースの基本的な用語を説明できる。
ネットワーク技術の活用①	インターネットの仕組みと通信サービスの特徴を説明できる。
ネットワーク技術の活用②	通信網と通信プロトコルに関する用語を説明できる。
データベースの技術①	データベースのモデル化と正規化の方法を説明できる。
データベースの技術②	データベースの表操作の方法を説明できる。
情報セキュリティ対策①	セキュリティ対策に関する基本的な用語を説明できる。
情報セキュリティ対策②	セキュリティ対策に関する基本的な用語を説明できる。
後半のまとめ	後半の講義のまとめを行う。
まとめ	これまでの講義内容を総括する。

(出典) IPA「IT スキル標準モデルカリキュラム－レベル 1 を目指して－」をもとに作成

パーソナルスキル入門

タイトル	学習目標
オリエンテーション、職業人に求められるパーソナルスキル	本科目の学習目標や進め方を理解する。職業人として企業で求められるパーソナルスキルの概要を説明できる。
ビジネスマナーの基本①	職業人としてお客様や組織から信頼を得るために必要なビジネスマナーの基本動作が行える。
ビジネスマナーの基本②	職業人として適切な電話対応、報告／連絡／相談、顧客対応が行える。
コミュニケーションの基本（2WAY）①	職業人として求められる基本的な 2WAY コミュニケーションの知識を活用して傾聴やインタビューができる。
コミュニケーションの基本（2WAY）②	職業人として求められる基本的な 2WAY コミュニケーションの知識を活用して、上司への業務報告やチームの合意形成ができ

	る。
コミュニケーションの基本（情報伝達）	職業人として求められる基本的な情報伝達の知識を業務に活用できる。
コミュニケーションの基本（情報伝達）文書編①	職業人が現場で実践するビジネス文書の基本的な作成方法を説明できる。
コミュニケーションの基本（情報伝達）文書編②	職業人として求められる高品質なビジネス文書の作成方法を理解し、正確でわかりやすいビジネス文書を作成できる。
コミュニケーションの基本（情報伝達）プレゼンテーション編①	職業人が現場で実践する情報伝達としての基本的なプレゼンテーション方法を説明できる。
コミュニケーションの基本（情報伝達）プレゼンテーション編②	職業人が現場で実践する情報伝達としての高品質な情報伝達としての基本的なプレゼンテーション方法を説明できる。
コミュニケーションの基本（情報整理・分析・検索）①	職業人が現場で実践する基本的なコミュニケーションマネジメントを説明できる。
コミュニケーションの基本（情報整理・分析・検索）②	職業人として求められるコミュニケーションマネジメントの知識を活用して円滑な会議を進められる。
リーダーシップの基本	職業人に求められるリーダーシップ基本と原則を説明できる。
ネゴシエーションの基本	職業人に求められるネゴシエーションの基本と原則を説明できる。
まとめ	これまでの講義内容を総括する。

(出典) IPA「IT スキル標準モデルカリキュラム－レベル 1 を目指して－」をもとに作成

東京都産業労働局