2 DAX40-06-3_システムの構築に必要なスキル・知識

改版履歴

2021年10月17日
「サイバーセキュリティ対策として考慮すべき事項」をガイドブックにリンク

2020年3月12日 DAX40-01の詳細を分冊化

3 システムを活用したサービスの企画・構築・運用に必要な人材育成

4 はじめに

ITを活用したサービスの実現に関わる企画部門、業務部門、
システム部門が保有すべきスキルと知識。

組織委内で人材を育成、
確保できない場合は、外部に求め、
全体で以下のようなスキルと知識を保有することが望まれる。

4 業務に必要なスキル・知識の習得

5 iコンピテンシ・ディクショナリ（iCD）

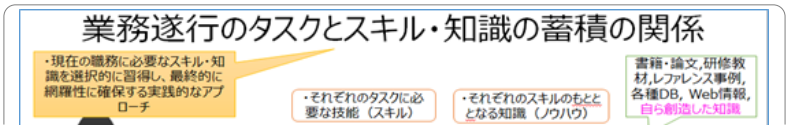
システム開発におけるタスクとスキル・知識を体系的に洗い出したものである。

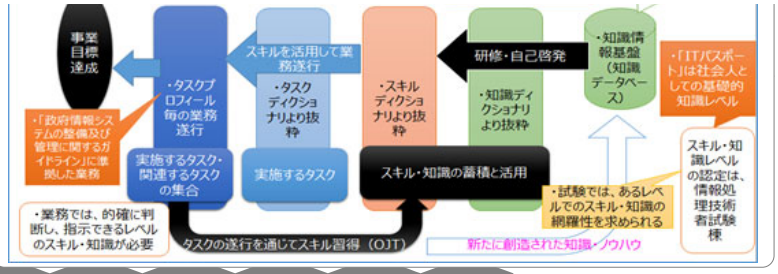
各アーカイブ機関での人材育成

各アーカイブ機関が人材育成について検討する際、事業の内容に合わせて、
「タスクディクショナリ」からタスクを選択することにより、
そのタスクを遂行するために必要なスキル、知識が提示される。タスクを担当する人材は、

そのスキル・知識を絞り込んで習得するようにすることにより、
短期間に効率的に人材育成ができる。

5 業務遂行のタスクとスキル・知識の蓄積のスキーム

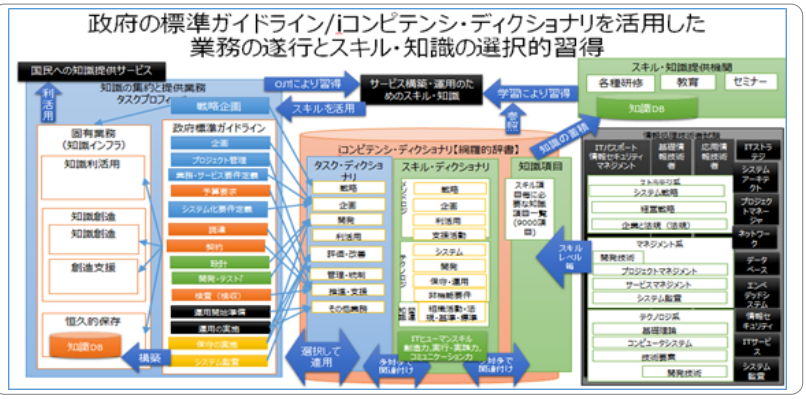




１つのタスクを実施するためには、
様々なスキルが必要であり、１つのスキルは、
経験と様々な知識により身に付く。
現在の職務に必要なスキル・知識を選択的に習得し、
最終的に網羅性に確保する実践的なアプローチが、
iコンピテンシ・ディクショナリの考え方である。

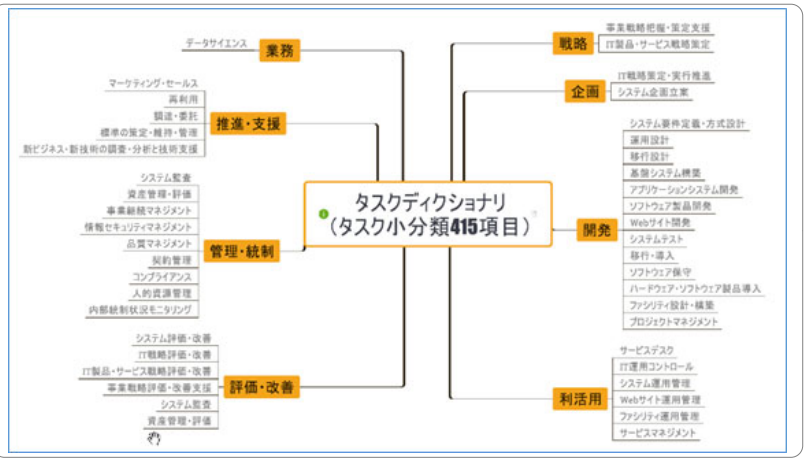
業務を遂行するためには、的確に判断し、
指示できるレベルのスキル・知識が必要であり、
業務に必要なスキル・知識を、
事前に選択的に習得して、
業務を遂行することが望ましいが、
業務を遂行する前に持っていないスキル・知識は、
タスクの遂行を通じて習得（OJT）することで、業務を円滑に進められるようになる。

5 iコンピテンシ・ディクショナリ（iCD）を活用した業務の遂行とスキル・知識の選択的習得



5 タスクディクショナリ

タスクの種類を網羅的に辞書化したものが「タスクディクショナリ」



スキルディクショナリ

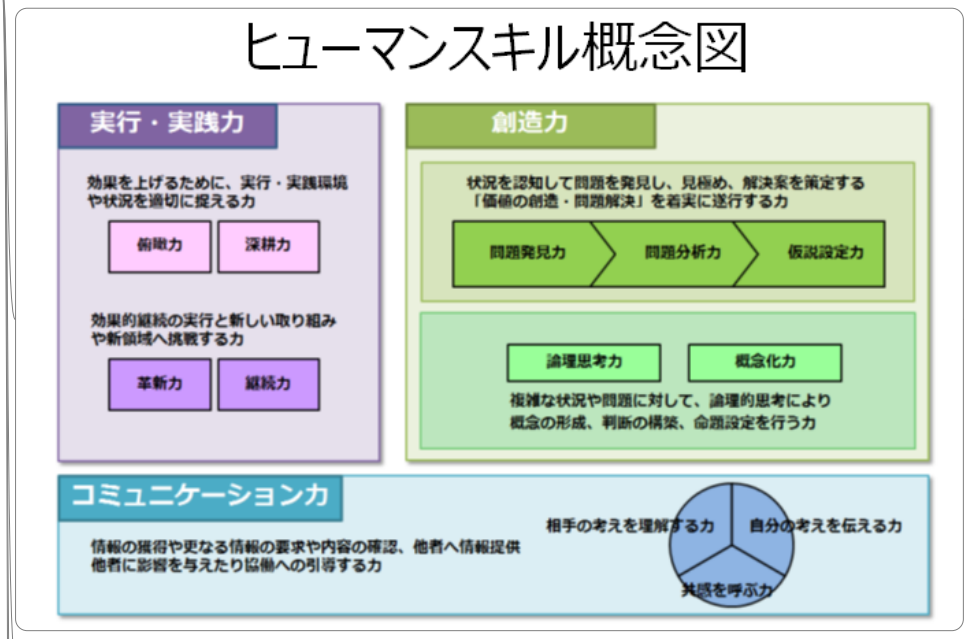
スキルの種類を網羅的に辞書化したもの「スキルディクショナリ」

①ビジネス活動の様々な手法、
方法のスキルとして「メソドロジ」、

②IT関連技法などのスキルとして「テクノロジ」

③対象となる業務を進めるための関連知識や
業務固有のスキルとして「関連業務知識」、

④ IT
に関するタスクを実行する際に必要となる実行力・実践力、創造力、
コミュニケーション力等のスキルとして「ITヒューマンスキル」。



実行力・実践力

俯瞰力・深耕力・革新力・継続力

効果を上げるために、
実行・実践環境や状況を適切に捉える力

効果的継続の実行と新しい取り組みや新領域へ挑戦する力

創造力

問題発見力・問題分析力・仮説設定力・論理思考力・概念化力

状況を認知して問題を発見し、見極め、
解決案を策定する「価値の創造・問題解決」を
着実に遂行する力

複雑な状況や問題に対して、
論理的思考により概念の形成、
判断の構築、 命題設定を行う力

コミュニケーション力

自分の考えを伝える力・相手の考え方を理解する力・共感を呼ぶ力

情報の獲得や更なる情報の要求や内容の確認、他者への情報提供、
他者に影響を与えたり、協働への引導する力

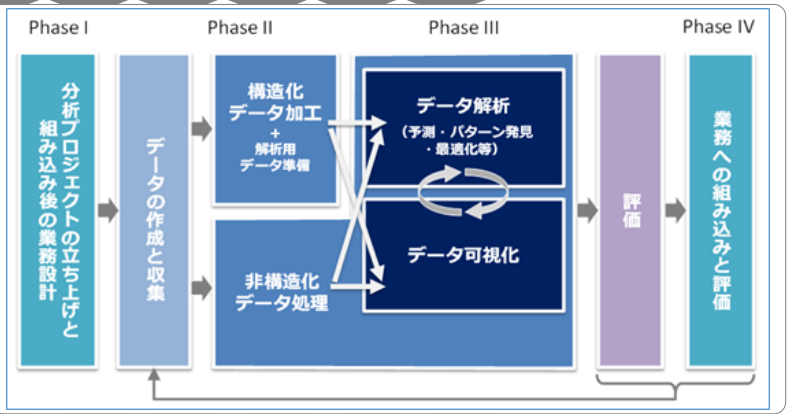
5 知識ディクショナリ

様々なスキルに必要となる知識を網羅的に辞書化したものが、「知識ディクショナリ」

5 データサイエンス領域でのタスクとスキル

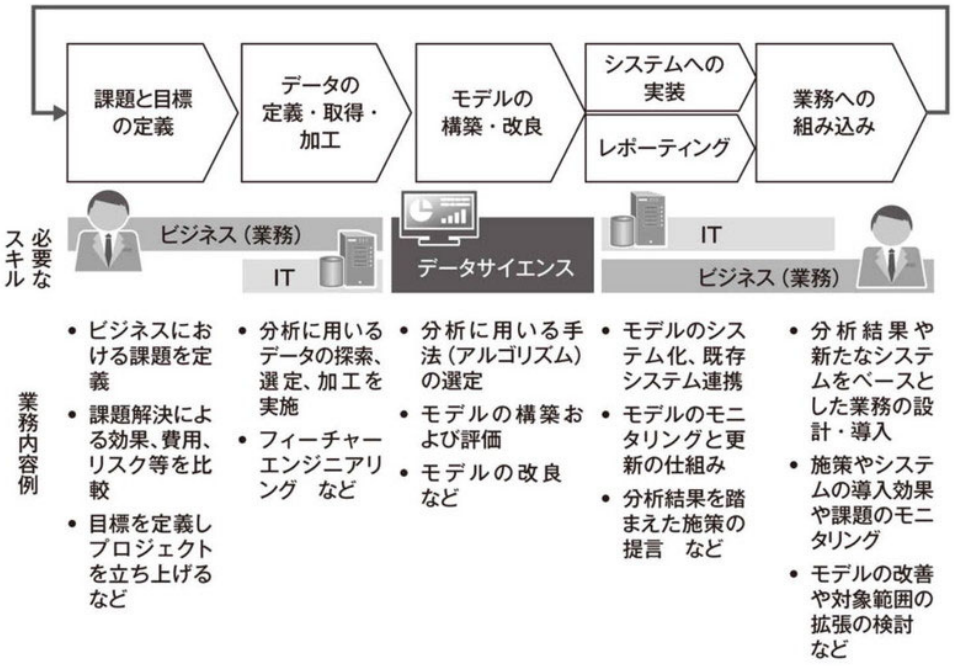
第4次産業革命に対応した新スキル標準（ITSS+）として、「セキュリティ領域」とともに、
「データサイエンス領域」に関して、
大量データを分析し、
その分析結果を活用するための一連のタスクとそのために習得しておくべきスキルカテゴリ、
タスク構造が網羅的示されている。

システム部門ではなく、
業務部門のタスクとして、業務設計、
データの作成と収集、 構造化データ加工、
解析用データ準備、データの準備、
データ解析、データ可視化、
非構造化データ処理、評価、
業務への組み込みと評価の工程が定義されている。



これからのデジタルアーカイブの構築は、
ビッグデータやAIを活用が必須であり、
各アーカイブ機関の業務部門が中心となって
「データサイエンス領域」のタスク工程に沿って確実に進め、
業務への適用を評価していくことが重要であり、
業務部門での人材育成、
人材確保が課題となる。

図表1　一般的なデータ分析の業務の流れ



（出所）野村総合研究所

4 網羅的なスキル・知識レベルの確認

5 情報処理技術者試験によるスキル・知識の網羅性の評価認定

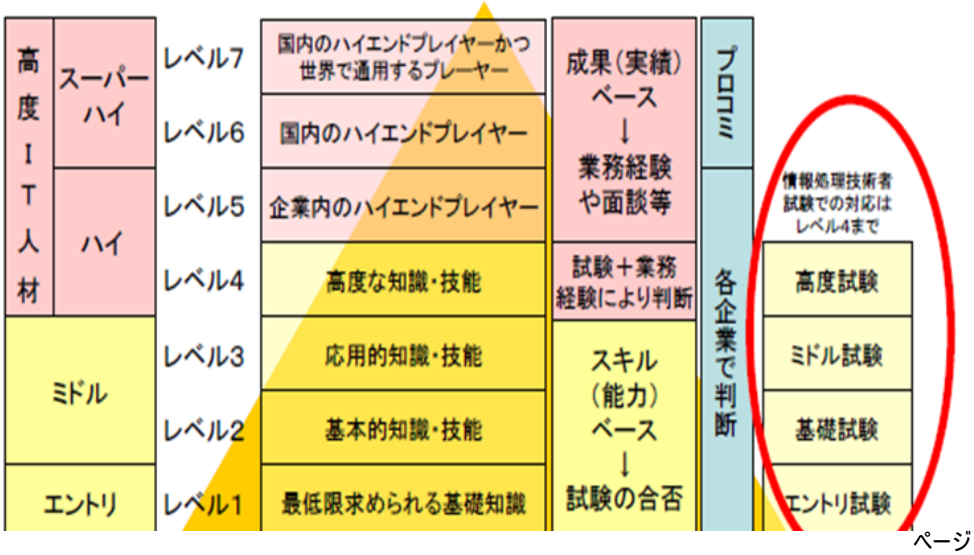
専門分野においては、
分野毎に網羅的な知識の習得状況評価する

応用分野においては、
IT関連全般の知識の理解度を評価する

基礎分野においては、
IT関連全般の用語の意味の理解度を評価する

業務を通じての知識習得では網羅的な知識は得られないため、
合格するためには業務以外での学習が必要

5 共通レベル定義



レベル７

社内外にまたがり、テクノロジやメソドロジ、
ビジネス変革をリードするレベル。

市場への影響力がある先進的なサービスやプロダクトの創出を
リードした経験と実績を持つ世界で通用するプレーヤ。

レベル６

社内外にまたがり、テクノロジやメソドロジ、
ビジネス変革をリードするレベル。

社内だけでなく市場から見ても、
プロフェッショナルとして認められる経験と実績を持つ国内のハイエンドプレーヤ。

レベル５

社内において、テクノロジやメソドロジ、
ビジネス変革をリードするレベル。

社内で認められるハイエンドプレーヤ。

レベル４

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、
業務上の課題の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

要求された作業を全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

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。

ITを活用した業務の構築・運用に携わるために
必要となる基本的知識・技能を有する。

レベル１

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。

ITを利用する社会人の常識としての基本的知識・技能を有する。

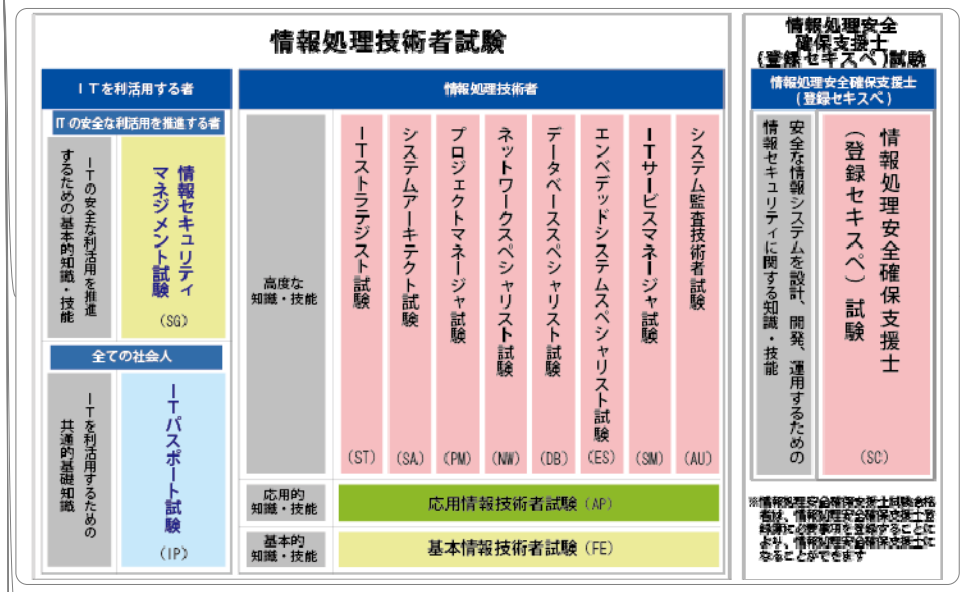
5 分野

専門分野【レベル4以上】においては、
分野毎に網羅的な知識の習得状況を評価する

応用分野【レベル3】においては、
IT関連全般の知識の理解度を評価する

基礎分野【レベル2】においては、
IT関連全般の用語の意味の理解度を評価する

5 情報処理技術者試験



ITパスポート試験（レベル1） IPA

情報処理技術者試験のレベル１で、
社会人の常識とされる..職業人が共通に備えておくべき情報技術に関する基礎的な知識をもち、情報技術に携わる業務に就くか、
担当業務に対して情報技術を活用していこうとする者が持つべき、
スキルと知識を備えているかを評価する。

出題範囲は網羅的であるが、
内容は用語の意味を知っていればいい程度。

基本情報技術者試験（レベル2） IPA

情報セキュリティマネジメント試験（レベル2） IPA

応用情報技術者試験（レベル3） IPA

ITストラテジスト試験（レベル4） IPA

3 サイバーセキュリティ対策として考慮すべき事項と必要なスキル・知識

4 総論

サイバーセキュリティの被害に遭った場合、
組織の存立が危ぶまれる事態になりえることを自覚する
・世の中で起こっているセキュリティ被害を対岸の火事だと思っている経営者、
ITは導入しているにも関わらず

セキュリティ対策のための費用はないとして
対策に後ろ向きの経営者、
最も重要な情報にアクセスする権限を持ちながら、
セキュリティに関しての意識の低い経営者。
これらの経営者が最大のセキュリティリスク

国は、大企業のみならず、中小企業も、
「サイバーセキュリティ経営ガイドライン」を参照することを求めている

【参考】「中小企業向けサイバーセキュリティ対策の極意」を引用

東京都が中小企業の経営者向けに、
サーバーセキュリティ対策として認識すべきことを
イラストを交えてまとめたもの

経営者が認識すべきことであるが、
それを認識させるためにも、
担当者が理解していることが重要

4 【参考】企業経営のためのサイバーセキュリティの考え方の策定について【NISC】

5 基本方針－サイバーセキュリティは、より積極的な経営への「投資」へ－

グローバルな競争環境の変化

ITの発展によるビジネスの変革が、
消費者向けのビジネスから企業間取引へと拡大

サイバー空間と実空間の融合がさらに進み、
チャンスもリスクも一層増大

⇒サイバーセキュリティをやむを得ない「費用」でなく、積極的な経営への「投資」と位置づけ、
企業としての「挑戦」と、
それに付随する「責任」として取り組むことが期待される

5 基本的な考え方

二つの基本的認識

＜①挑戦＞サイバーセキュリティは、
利益を生み出し、
ビジネスモデルを革新するものであり、
新しい製品やサービスを創造するための戦略の一環として考えていく

＜②責任＞全てがつながる社会において、
サイバーセキュリティに取り組むことは社会的な要求・要請であり、
自社のみならず社会全体の発展にも寄与する

三つの留意事項

＜①情報発信による社会的評価の向上＞

「セキュリティ品質」を高め

品質向上に有効な経営基盤の一つとして
セキュリティ対策を位置付けることで
企業価値を高めることが必要。

そのような取組に係る姿勢や方針を情報発信することが重要。

＜②リスクの一項目としてのサイバーセキュリティ＞

提供する機能やサービスを全うする（機能保証）という観点から、
リスクの一項目としてのサイバーセキュリティの視点も踏まえ、リスクを分析し、
総合的に判断。

経営層のリーダーシップが必要。

＜③サプライチェーン全体でのサイバーセキュリティの確保＞

サプライチェーンの一部の対策が不十分な場合でも、
自社の重要情報が流出するおそれあり。

一企業のみでの対策には限界があるため、
関係者間での情報共有活動への参加等が必要。

4 サイバーセキュリティ対策として考慮すべき事項

5 ガイドブック『中小企業向けサイバーセキュリティ対策の極意』

『中小企業向けサイバーセキュリティ対策の極意』Ver.2.1（EPUB版:44.2MB）

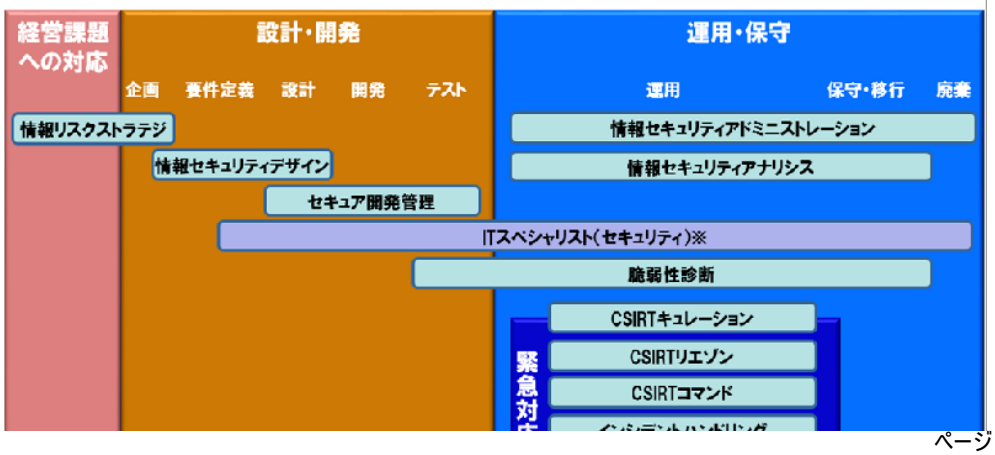
MISSION3
経営者は事前に何を備えればよいのか？

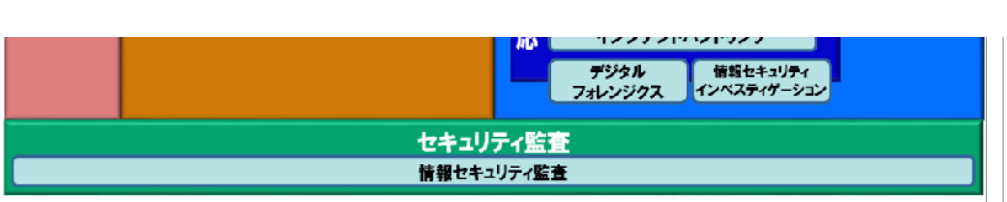
INFORMATION
6-6：DX時代に不可欠な人材の確保
（Ver.2.05:2021.9.3更新）

4 サイバーセキュリティ対策に必要なスキルと知識

5 情報システムのライフサイクルに応じた各セキュリティ専門分野の対象フェーズの分類

情報システムのライフサイクルに応じた各セキュリティ専門分野の対象フェーズの分類





5 セキュリティ領域のスキル標準「ITSS+」【2017年6月5日】

専門的なセキュリティ業務の役割の観点により、経営課題への対応から設計・開発、運用・保守、セキュリティ監査における13の専門分野を具体化

新たに創設された国家資格「情報処理安全確保支援士(登録セキスペ)」が想定する業務を包含

5 専門分野【詳細】

情報リスクストラテジ

自組織または受託先における業務遂行の妨げとなる情報リスクを認識し、その影響を抑制するための、組織体制の整備や各種ルール整備等を含む情報セキュリティ戦略やポリシーの策定等を推進する。
自組織または受託先内の情報セキュリティ対策関連業務全体を俯瞰し、アウトソース等を含むリソース配分の判断・決定を行う。

情報セキュリティデザイン

「セキュリティバイデザイン」の観点から情報システムのセキュリティを担保するためのアーキテクチャやポリシーの設計を行うとともに、これを実現するために必要な組織、ルール、プロセス等の整備・構築を支援する。

セキュア開発管理

情報システムや製品に関するリスク対応の観点に基づき、機能安全を含む情報セキュリティの側面から、

企画・開発・製造・保守などにわたる情報セキュリティライフサイクルを統括し、対策の実施に関する責任をもつ。

脆弱性診断

ネットワーク、OS、ミドルウェア、アプリケーションがセキュアプログラミングされているかどうかの検査を行い、診断結果の評価を行う。

情報セキュリティ

組織としての情報セキュリティ戦略やポリシーを

具体的な計画や手順に落とし込むとともに、
対策の立案や実施（指示・統括）、
その見直し等を通じて、
自組織または受託先における情報セキュリティ対策の具体化や実施を統括する。また、
利用者に対する情報セキュリティ啓発や教育の計画を立案・推進する。

情報セキュリティアドミニストレーション

組織としての情報セキュリティ戦略やポリシーを
具体的な計画や手順に落とし込むとともに、
対策の立案や実施（指示・統括）、
その見直し等を通じて、
自組織または受託先における情報セキュリティ対策の具体化や実施を統括する。
また、
利用者に対する情報セキュリティ啓発や教育の計画を立案・推進する。

情報セキュリティアナリシス

情報セキュリティ対策の現状に関するアセスメントを実施し、
あるべき姿とのギャップ分析をもとにリスクを評価した上で、
自組織または受託先の事業計画に合わせて導入すべきソリューションを検討する。
導入されたソリューションの有効性を確認し、
改善計画に反映する。

CSIRTキュレーション

情報セキュリティインシデントへの対策検討を目的として、セキュリティイベント、
脅威や脆弱性情報、 攻撃者のプロファイル、
国際情勢、
メディア動向等に関する情報を収集し、
自組織または受託先に適用すべきかの選定を行う。

CSIRTリエゾン

自組織外の関係機関、 自組織内の法務、
渉外、IT部門、広報、
各事業部等との連絡窓口となり、
情報セキュリティインシデントに係る情報連携及び情報発信を行う。
必要に応じてIT部門とCSIRTの間での調整の役割を担う。

CSIRTコマンド

自組織で起きている情報セキュリティインシデントの全体統制を行うとともに、
事象に対する対応における優先順位を決定する。
重大なインシデントに関してはCISOや経営層との情報連携を行う。
また、
CISOや経営者が意思決定する際の支援を行う。

インシデントハンドリング

自組織または受託先におけるセキュリティインシデント発生直後の初動対応
（被害拡大防止策の実施）や被害からの復旧に関する処理を行う。
セキュリティベンダーに処理を委託している場合には指示を出して連携する。
情報セキュリティインシデントへの対応状況を管理し、
CSIRTコマンドのタスクを担当する者へ報告する。

デジタルフォレンジクス

悪意をもつ者による情報システムやネットワークにを対象とした活動の証拠保全を行うとともに、消されたデータを復元したり、
痕跡を追跡したりするためのシステム的な鑑識、精密検査、 解析、 報告を行う。

情報セキュリティインベスティゲーション

情報セキュリティインシデントを対象として、
外部からの犯罪、 内部犯罪を捜査する。
犯罪行為に関する動機の確認や証拠の確保、

次に起こる事象の推測などを詰めながら論理的に捜査対象の絞り込みを行う。

情報セキュリティ監査

情報セキュリティに係るリスクのマネジメントが効果的に実施されるよう、
リスクアセスメントに基づく適切な管理策の整備、運用状況について、
基準に従って検証又は評価し、
もって保証を与えあるいは助言を行う。

3 次世代図書館サービスでの人材育成･確保

4 はじめに

AIが人間の能力を超える日は決して近くはない。今後10年は、
まずは人間に不足している労働力を補完し、
労働力を省力化することにより、
既存の業務効率･生産性を高めることである。

更に、
既存の業務の提供する価値（品質や顧客満足度など）を高め、
これまでに存在しなかった新しい価値をもった業務を 創出することは容易に想像できる。

今後の人材として、AI等の活用を想定し、
新しい業務に取組む意欲や満足度を高めることが重要である。

4 AIの活用が一般化する時代における重要な能力

ルーティンワーク、 マニュアル化された仕事は、

アルバイト、非常勤、外部委託、
そして人工知能に置き換わる。そのような時代に、人が持つ重要な能力は、情報収集能力、課題解決能力、
論理的思考などの業務遂行能力である。

企画発想力や創造性、 語学力や理解力、
表現力などの基礎的素養と、
チャレンジ精神や主体性、行動力、
洞察力などの人間的資質を発揮できることが重要である。

また、円滑な業務の遂行のためには、
コミュニケーション能力やコーチングなどの対人関係能力が、今まで以上に必要になる。

4 業務担当の役割と資質

図書館等のデジタルアーカイブ機関での、
資料の収集、 組織化、 保存、 提供の業務、
レファレンスサービス、
予測調査等の業務のうち、
マニュアルに沿って行ってきた業務はもとより、
自ら習得してきた文献等の知識、
調べ方のスキルに基づいて、
事実を提供するサービスは、
AIシステムを活用し、
AIシステムにより自動的に提示する情報の評価、
補正する業務に移行していくことが必然となる。

自ら事実を知識として保有しその知識を提示する能力ではなく、
AIシステムを活用して外部にある知識を併せて、
新たな知識として付加価値を付けた知識を提示する能力が求められる。

- 選書
- 関連付けに必要な典拠類の構築
- 情報に関する基本情報付け（メタデータ付与）
- 情報に関する付加価値情報付け
- 情報間の関連付け
- 分類・主題情報の付与
- レファレンス

数年後、
機械学習が一般化され特別でなくなった次に特別な価値を持つのは、
ディープラーニングに可能な限り早く取り組み、
知見を積み、
自組織に必要になるデータを理解し、
少しでも早くそのデータの蓄積を始めることが大事である。

4 新しい役割分担

5 概要

従来は、事業戦略部門、業務部門、
システム部門等に分かれて、
サービスを構築し運用してきた。近年、
システムライブラリアンというシステムに詳しいライブラリアンの必要性が謳われてきたが、

今後は、①ビジネスの旗振り役、
②ディープラーニングの技術者、
データサイエンテイスト、
③モデルを組み込んだシステムを作るエンジニア、④ビジネスとエンジニア、
データサイエンテイストの橋渡し役のような分類で、
図書館等のデジタルアーカイブ機関が保有する情報をビッグデータとして、
如何にして知識として蓄積し活用していくかを調整する「ビジネスとエンジニア、
データサイエンティストの橋渡し役」が重要になる。

5 ビジネスの旗振り役

ビジネスの旗振り役は、組織のCEO、
CIOクラスであり、社会動向、
市場動向を踏まえて戦略的に事業計画を策定する役割を担う。しかしながら、
急速な社会の変化に対応して的確な判断ができる経営層が少なく、
またデジタル変革の時代に組織が保有する情報の重要性を
認識するCDO的な役割を持つ人材が経営層にいないのも現状である。

そのような状況において、
この役割を補佐役として、
常に社会動向と利用者ニーズを把握し、
実質的にマネジメントするビジネスの旗振り役が重要な役割を果たす人材が重要である。

5 ビジネスとエンジニア、
データサイエンテイストの橋渡し役

橋渡し役は、
既存の組織にはない役割であり、
ITとAIの技術を理解しながらビジネスとつないでいく人で、AIの機能モジュールは、
AI関連機関よりライブラリが整備され、
多種多様なAPIが提供されたりされているため、自らアルゴリズムを設計、
開発する必要はない。

どうビジネスに生かすかを描き、
AIを活用したプロジェクトをマネジメントできる人材が求められる段階になってきた。

2 AI時代のシステム開発手法

ウォータフォールとアジャイル

2 AI時代に必要なスキル・知識

AI時代のタスク

構築・運用に必要な役割と、
必要な技能・知識

必要な能力

技術の習得方法