# サイバーセキュリティ人材フレームワーク活用の手引き2026

個人（専門人材）向け

国家サイバー統括室
National Cybersecurity Office

令和8年4月3日

# 本書の位置づけ・利用上の留意点等について

## 位置づけ

- 本書は、「サイバーセキュリティ人材フレームワーク」の策定背景・目的、整理概念に加え、専門人材としてキャリア形成を企図する方の活用シーン・方法などを解説した「サイバーセキュリティ人材フレームワーク」の手引き書です。
- サイバーセキュリティ人材フレームワークの理解及び活用を支援することを目的に作成したものであり、目指すべき個人のキャリアを一律に義務づけるものではありません（本手引き書の内容を参考としつつ、自らの適性やキャリア志向に応じて適切に活用してください）。

## 想定利用者

- 本手引き書は、官民においてサイバーセキュリティ対策等に関わる社会人および今後関わることを希望する学生を主な利用者として想定します。
- 特に、サイバーセキュリティ分野において専門人材としてキャリア形成を目指す個人に活用されることを想定しています。

## その他利用上の留意点

### 効力について

- 本手引き書は、法令、契約又は行政処分等の法的根拠となるものではなく、法的拘束力を有するものではありません。
- 本手引き書の内容と法令又は契約等の間に相違がある場合には、法令又は契約等が優先されます。

### 用語及び定義について

- 本手引き書にて記載する用語の定義は、基本的にサイバーセキュリティ人材フレームワークにおける定義に基づくものです。

### 情報の正確性及び更新について

- 本手引き書の内容は、作成時点における情報及び知見に基づくものであり、技術動向等により内容が変更される場合があります。
- 最新の情報については、関係機関が公表する資料等を参照してください。

### 出典の明示について

- 本手引き書を利用する際は下記の例に倣い、出典を記載してください。
- 記載例）
- 出典：国家サイバー統括室「サイバーセキュリティ人材フレームワーク活用の手引き2026（個人（専門人材）向け）」（〇年〇月〇日に利用）

- 本手引き書を編集・加工等して利用する場合は、編集・加工等を行ったことを記載してください。
  なお、編集・加工した資料を、あたかも国（国家サイバー統括室）が作成したかのような態様で公表・利用してはいけません。

### 準拠法と合意管轄について

- 本手引き書の解釈等については、日本法を準拠法とします。
- 本手引き書に関連して生じた紛争については、東京地方裁判所を第一審の専属的合意管轄裁判所とします。

### 免責について

- 国（国家サイバー統括室）は、利用者が本手引き書を用いて行う一切の行為（編集・加工等した情報を利用することを含む。）について何ら責任を負うものではありません。

### その他

- 本利用ルールは、著作権法上認められている引用などの利用について、制限するものではありません。
- 本利用ルールは今後変更される可能性があります。

# 目　次

## 共通事項



## 個人（専門人材）向け事項

# 共　通　事　項

# 1．はじめに（サイバーセキュリティ人材フレームワークとは）

**概要**

サイバーセキュリティを担う人材について、職種別の役割と、それぞれに求められるタスク・知識・スキルを体系的に整理するとともに、能力等に応じたレベルを設定し、官民共通のフレームワークとして設定するものです。

## 策定背景

### 現　状

- 職種ごとの役割やスキルセットが**不十分**
  求められる知識・スキル等が曖昧
- 実務ニーズとサイバーセキュリティ人材の要件との対応関係が不明確

**人材の育成・確保を効果的・効率的に進めるための**
共通基盤が不十分**な状態**

一括りに「サイバー人材」と語られる傾向

### 策定後目指す効果

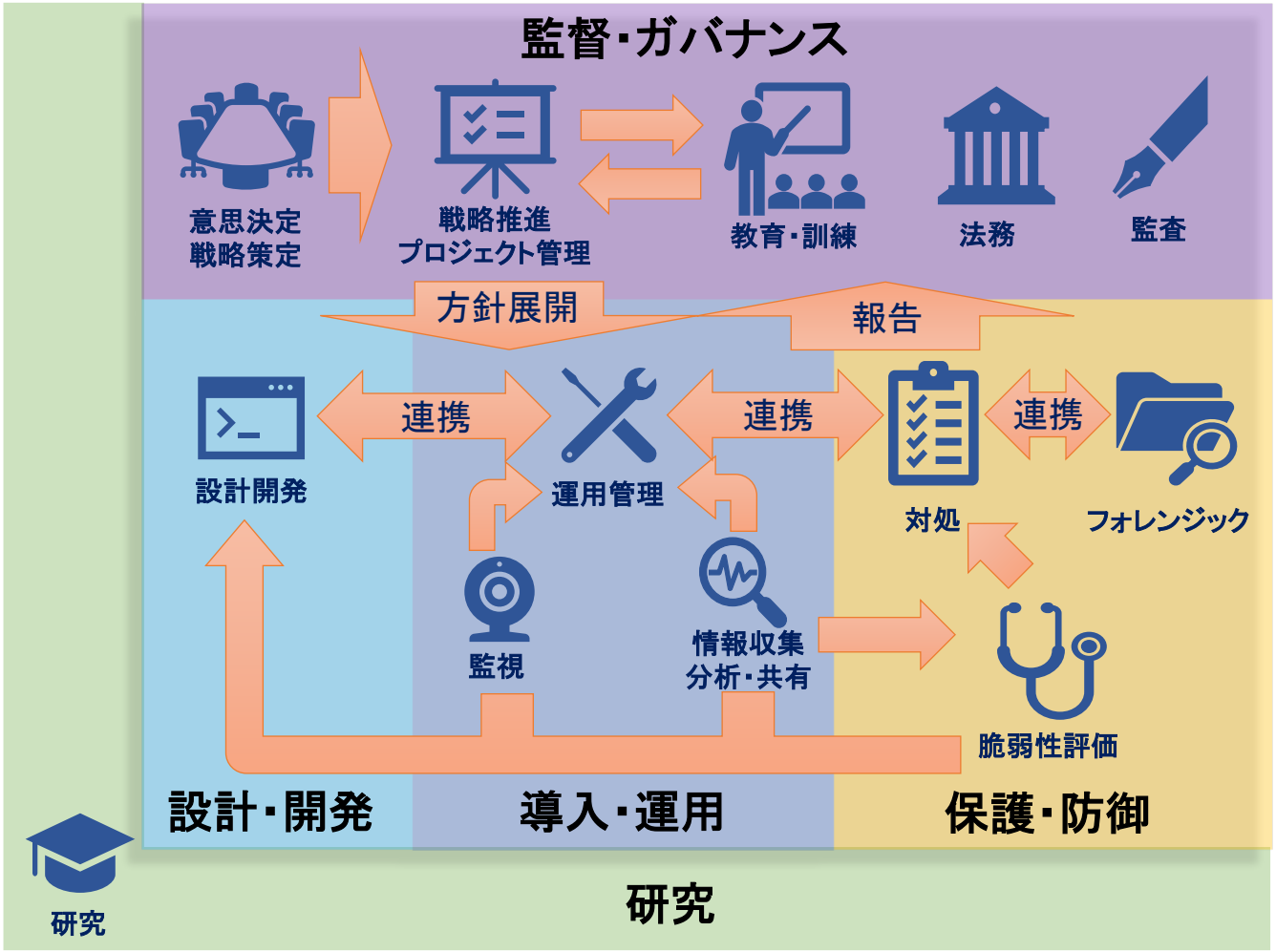
**企業等**　組織に必要な人材像を明確化し、採用・配置・育成等を計画的に進められる

**個人**　役割に応じて求められる知識・スキル等が可視化され、学習やキャリア形成の指針となる

**教育機関等**　ニーズに即したサイバーセキュリティ人材の要件を踏まえ、教育内容やカリキュラムを体系的に企画・設定できる

可視化により、効果的・効率的な人材育成を実現する環境を整備

# サイバーセキュリティ人材が担うべき「役割」の全体像（イメージ）




通報・報告・連絡・相談

外部公的機関等

- 警察
- 個人情報保護委員会
- サイバーセキュリティ関連組織（NCO・IPA・JPCERT/CC等）

# 2．サイバーセキュリティ人材フレームワークの概要

- サイバーセキュリティ人材フレームワーク（Excel）は下表の各要素から構成されます。
- 各役割及び個別のタスク・知識・スキルとNICEフレームワークとの対応関係も明示しています。

| | |
|---|---|
| **各役割の定義シート（①～⑬）** | ● 13の役割を具体的に説明するため、以下の要素で構成<br>➢ 主な業務（例）：その役割で実施する業務内容を示す。タスクの内容をまとめたものに相当<br>➢ NICEフレームワークにおける対応ロール<br>➢ 想定される役職名等：組織において当該役割を担っている人材の主な役職名<br>➢ 補足説明：国内の既存のフレームワークとの対応関係等を示す<br>➢ レベル：ITSSを参照した4段階のレベルを定義<br>➢ 各役割で求められる汎用的なTKS:当該役割を担う人材が行うタスク(T)、及びそのタスクを実施するために必要な知識(K)及びスキル(S) |

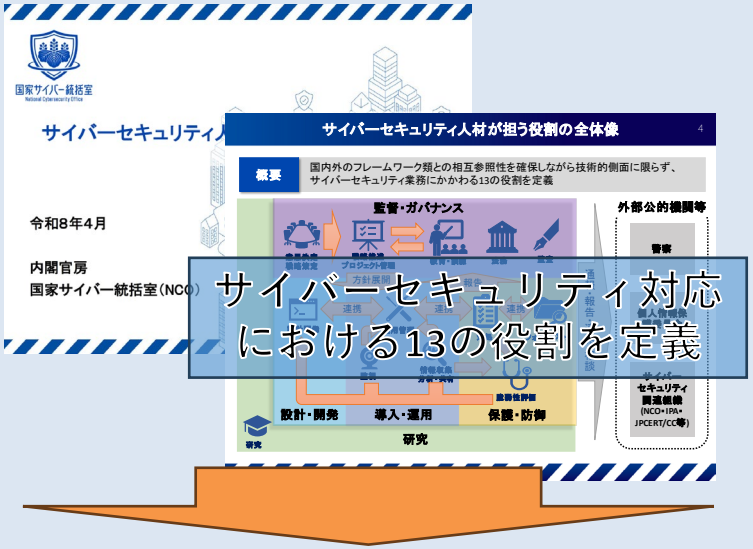
## ■TKSの考え方

| | |
|---|---|
| **タスク(T)** | ● 本フレームワークで役割毎に定義しているタスク(T)とNICEフレームワークv2.1.0におけるタスクとの対応表を示す。<br>● 原則として、本フレームワークで定義している1つのタスクについてNICEフレームワークのタスクが1つ以上対応するが、一部本フレームワーク独自のタスクが存在する。 |
| **知識(K)** | ● 本フレームワークで役割毎に定義している知識(K)とNICEフレームワークv2.1.0における知識との対応表を示す。<br>● 原則として、本フレームワークで定義している1つの知識についてNICEフレームワークの知識が1つ以上対応するが、一部本フレームワーク独自の知識が存在する。 |
| **スキル(S)** | ● 本フレームワークで役割毎に定義しているスキル(S)とNICEフレームワークv2.1.0におけるスキルとの対応表を示す。<br>● 原則として、本フレームワークで定義している1つのスキルについてNICEフレームワークのスキルが1つ以上対応するが、一部本フレームワーク独自のスキルが存在する。 |

# 3．手引き書とは（人材フレームワークとの対応関係等）

本書では、各組織において求められる「役割」を、各組織の規模・特性を踏まえ、タスク・知識・スキルをベースに「人材像」として具体化して説明します。

## ■人材フレームワーク





## ■手引き書(本書)

①：小規模組織

②：大規模組織

13の役割をもとに、組織の個別事情に応じた「人材像」として具体化（例を用いて説明）

③教育機関

人材育成に資する教育コンテンツ等の設計方針などを整理

④-1：個人(専門人材)
④-2：個人
(プラス・セキュリティ)

専門人材/プラス・セキュリティ別のスキル向上に役立つ情報を整理

# 【参考】各手引き書の想定読者一覧

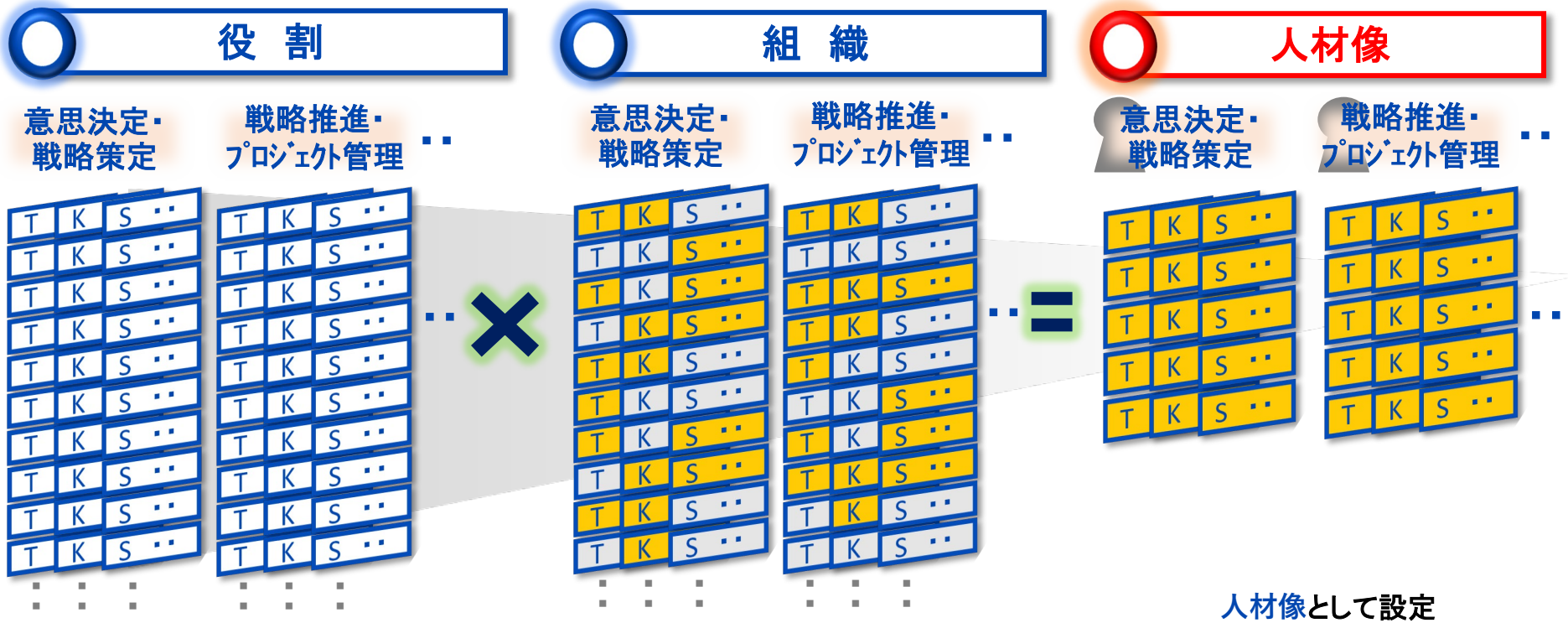
- 手引き書は各対象ごとに「主たる読者の属性」を想定し作成をしているものですが、主たる読者ではない属性の方も参考にしていただけるよう作成しておりますので、以下の対応表を参考にご利用ください。

凡例
◎：主たる想定読者
○：自身の業務等に密接にかかわる情報を含むもの
△：業務等において参考となる情報を含むもの

| 読者の所属・属性 / 手引き書 | 小規模組織 | | 大規模組織 | | セキュリティ事業者 | 教育機関 | |
|---|---|---|---|---|---|---|---|
| | マネジメント層 | 担当者 | マネジメント層 | 担当者 | ― | 教員 | 学生 |
| 小規模組織向け | ◎ | ○ | △ | △ | △ | △ | △ |
| 大規模組織向け | ― | ― | ◎<br>(人事担当者含む) | ○ | △ | △ | △ |
| 教育機関向け | △ | ― | △ | ― | ― | ◎<br>(教育事業者含む) | ○ |
| 個人<br>(専門人材) | △ | △ | △ | ◎<br>(セキュリティ担当者) | ○ | ― | ○<br>(セキュリティ分野志望者) |
| 個人<br>(プラス・セキュリティ) | △ | ◎ | △ | ◎<br>(バックオフィス、品質管理者等) | ○ | ― | ○<br>(学部の専門性によらず全学生に有益) |

# 【参考】サイバーセキュリティにおける人材像の概念整理

- フレームワーク本体では、13の「役割」と各役割毎に汎用的なTKSを定義します。
- その上で、各組織において求められる役割を実施する人材の定義をフレームワークをもとに具体化したものを「（各役割の各組織における）人材像」とし、その具体化手順について手引き書にて提示します。



# 4．他の人材フレームワークとの参照関係

本フレームワークと国内の他のフレームワークとの関係は以下の通りです。
必要に応じて他のフレームワークも併せてご参照いただけます。

| | 本フレームワーク | ITSS+（セキュリティ領域） | SecBoK 2025 | 産業横断サイバーセキュリティ研究会 人材定義リファレンス | CSIJサイバーセキュリティ プロフェッショナル人材ロール |
|---|---|---|---|---|---|
| ① | 意思決定・戦略策定 | セキュリティ経営（CISO）<br>デジタル経営（CIO/CDO）<br>企業経営（取締役）<br>事業ドメイン（戦略・企画・調達） | セキュリティ経営、意思決定・戦略策定<br>セキュリティ統括 | CISO、CRO、CIO等<br>システム部門責任者 | |
| ② | 戦略推進・プロジェクト管理 | セキュリティ統括<br>デジタルシステムストラテジー<br>経営リスクマネジメント<br>事業ドメイン（生産現場・事業所管理） | セキュリティ統括<br>プロジェクト管理<br>社内外調整 | サイバーセキュリティ統括<br>ISMS担当<br>個人情報取扱責任者/担当<br>特定個人情報取扱責任者/担当 | |
| ③ | 監視 | セキュリティ監視・運用 | 監視・運用 | SOC担当 | |
| ④ | 対処 | セキュリティ監視・運用 | 対処（インシデントハンドリング） | CSIRT責任者/担当<br>サイバーセキュリティ事件・事故担当 | インシデントハンドラー |
| ⑤ | 情報収集・分析・共有 | セキュリティ調査分析・研究開発 | 脅威・脆弱性情報収集 | SOC担当 | |
| ⑥ | 脆弱性評価 | 脆弱性診断・ペネトレーションテスト | 脆弱性診断・評価 | 運用系サイバーセキュリティ担当 | Web/NW脆弱性診断士<br>情報システムペンテスター<br>IoTデバイス脆弱性診断士<br>IoTシステムペンテスター<br>IoT脆弱性分析士 |
| ⑦ | フォレンジック | セキュリティ調査分析・研究開発 | インシデント調査・分析 | サイバーセキュリティ事件・事故担当 | |
| ⑧ | 運用管理 | セキュリティ監視・運用<br>デジタルプロダクト運用 | システム管理・ネットワーク管理<br>監視・運用 | システム管理者、ネットワーク管理者<br>運用系サイバーセキュリティ担当、他 | クラウドセキュリティプロフェッショナル |
| ⑨ | 教育・訓練 | セキュリティ統括 | 教育・訓練 | サポート教育担当 | |
| ⑩ | 法務 | 法務 | 法務 | | |
| ⑪ | 監査 | セキュリティ監査、システム監査 | 監査 | 監査責任者、監査担当 | |
| ⑫ | 設計開発 | デジタルシステムアーキテクチャ<br>デジタルプロダクト開発 | セキュリティ設計<br>開発 | セキュリティ設計担当<br>構築系サイバーセキュリティ担当、他 | サービス企画におけるリスク分析士<br>クラウドセキュリティプロフェッショナル |
| ⑬ | 研究 | セキュリティ調査分析・研究開発 | | | |

# 個人（専門人材）向け手引き書の全体構成

# 個人（専門人材）向け手引き書2026の全体構成

- サイバーセキュリティ分野で高度な専門性を有する人材としての活躍を目指す個人が、目指すキャリアと現状のギャップを把握し、必要な知識・スキルを効果的に習得していくためのステップと、実際の専門人材のキャリアパス事例を解説します。

## 現状の課題

セキュリティ分野での
キャリア形成についての悩み

- 自分に向いているセキュリティの役割や、次に目指すべきキャリアがわからない
- 目指すキャリアに対して、今の自分に不足している知識・スキルが客観的にわからない
- 不足している知識・スキルを、具体的にどうやって習得すればよいかわからない

**目指すキャリアに必要な要件の可視化と、自律的なキャリア形成・学習の指針が必要**

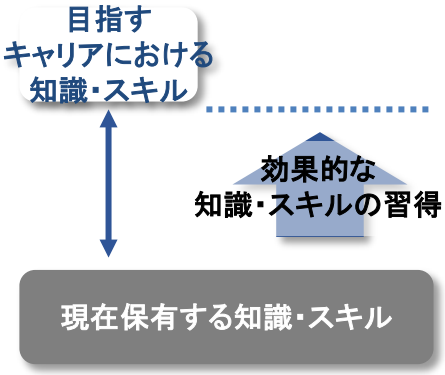
## フレームワークを用いたキャリアの可視化と学習の指針策定

サイバーセキュリティ人材フレームワーク

各役割ごとにタスクから関連する知識・スキルを整理

**【セルフアセスメント】**
フレームワークを活用し、目標とする役割や現在の自分におけるタスク・知識・スキルを可視化

**【学習指針の検討】**
- 抽出したギャップの中から、習得すべき知識・スキルを抽出し、「資格取得」「研修」等の学習指針を検討




**この手引き書で紹介する専門人材の例**
（随時拡充・見直し予定）

実際の専門人材の事例も適宜参照し、目指すキャリアに近しい事例を探してみましょう

**現場技術からのマネジメント・エキスパート**
運用や開発の経験を積みマネジメント・エキスパートへ

**監査・ガバナンス専門家**
監査や法務の専門性を一貫して磨く

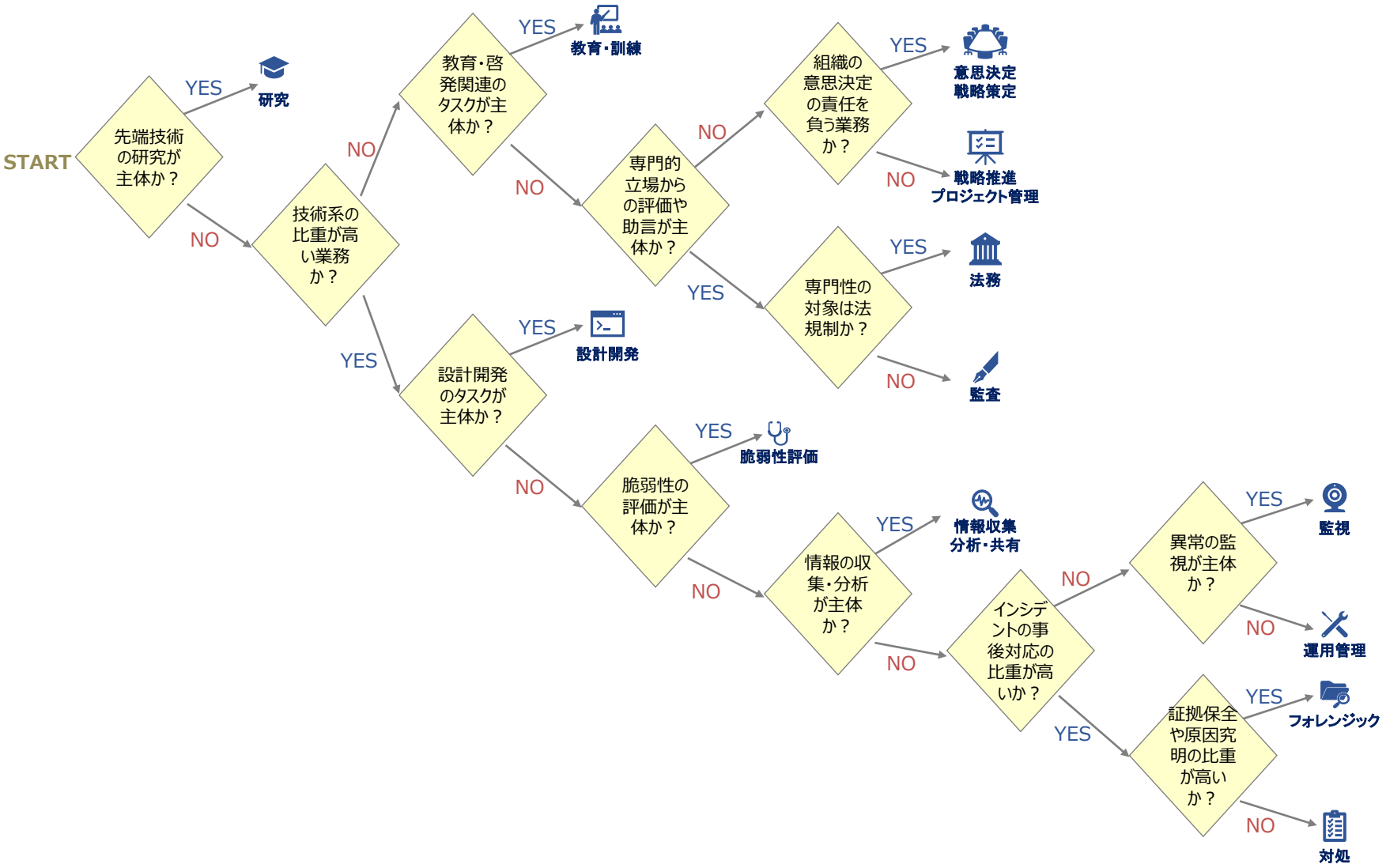
**技術領域のエキスパート深化**
設計・開発を軸に特定技術の専門性を深める

**アカデミアからのエキスパート社会実装**
基礎研究からプロダクト化・経営へと貢献

# セルフアセスメントの方法

# フレームワークで定義する「13の役割」とは

- まずは、サイバーセキュリティ人材のフレームワークにおいて定義される13の役割について、以下フローチャートも参考にしながら、自身の現在の業務に近い役割、あるいは今後目指したいキャリアに近い役割がどれに当てはまるか確認ください。

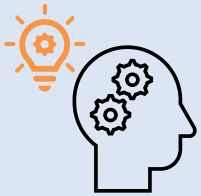


# 目標に応じたセルフアセスメントの位置付け

- 今後のサイバーセキュリティに関するキャリアの目標に応じて、セルフアセスメントの位置付けも変わってきます。ここでは3つの例について、目標に応じたセルフアセスメントの活用方法案を示します。

## 目標例１

**自分の専門としている役割についての知識・スキルのレベルアップをしたい**

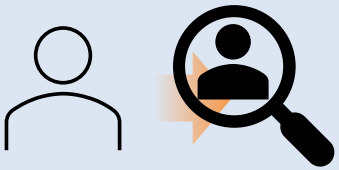


**セルフアセスメントの対象**

担当業務として実施するタスク（今後実施する可能性のあるものも含む）

## 目標例２

**社会で注目されている役割にジョブチェンジしたい**



**セルフアセスメントの対象**

ジョブチェンジの対象となる役割を構成する主要なタスク

## 目標例３

**新たにサイバーセキュリティのキャリアを目指したい**

**セルフアセスメントの対象**

ロールモデルとなるキャリアパスに含まれる複数の役割を構成するタスク

# 目標例１（自分の専門としている役割についての知識・スキルのレベルアップをしたい）

- 現在13の役割のいずれかを担う方については、今後のキャリアパスを職場の上司や先輩に相談する機会があると思いますが、対話がしやすくなる工夫として、フレームワークを用いるのも一案です。

## 例）目標設定・評価面談


担当業務について、タスク「●●」は自信を持って対応できています。

私もそう思います。タスク「〇〇」は、来期以降対応できるよう期待してます。

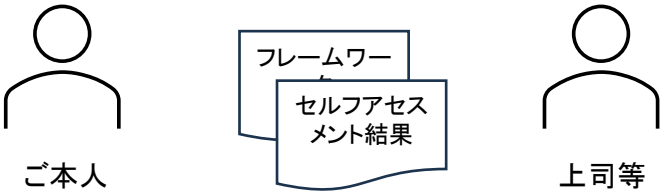
タスク「〇〇」に関連する知識「△△」、およびスキル「△△」の習得を頑張りたいです。

そうですね、加えて将来を見据え、タスク「■■」に関連する知識として整理される「□□」も今から習得していけると望ましいです。

**ポイント**

- 自身の担当業務等を、フレームワークで用いられているキーワードを共通言語として上司と対話できると、レベルアップすべき知識やスキルの明確化が図りやすくなります。
- 上司の方は、フレームワークも参考にしつつ、ご自身の経験と面談者本人の適性等と照らし合わせ、助言ができると望ましいです。

## 例）キャリア面談




今後のキャリアとしては、「●●」と考えています。

イメージとしては、レベル3相当、13の役割のうちの「〇〇」が近いですか？

はい、「〇〇」に加えて、「△△」も良いなと考えており、アセスメントをしてみました。

「3-E」相当のキャリアアップをご想像されていると理解しました。例えばスキル「□□」を伸ばせる「XXXX」プロジェクトに入るのはいかがですか。

**ポイント**

- 将来目指すキャリアを言語化するため、フレームワークに基づいたセルフアセスメントの結果を活用できると望ましいです。
- ただし、必ずしも13の役割のうちのどれかに断定できるものでもありませんので、ご関心ある役割について複数アセスメントをしてみてください。
- 上司の方は、アセスメントの結果をふまえ、知識やスキルの習得方法について助言ができると望ましいです。

# 目標例２（社会で注目されている役割にジョブチェンジしたい）

- 既に同分野で活躍される方も、社会や技術動向等ふまえ、ジョブチェンジを考える機会があると考えます。
- 例えば、国内の求人情報（公開情報ベース）を参考にすると、レベル3相当とされる求人が多く見受けられます。また、レベル3以上では、マネジメント系・エキスパート系とキャリアが分岐することに伴い、求められるTKSも異なってきます。
- こうしたTKSの要求事項の詳細にも留意しつつ、セルフアセスメントを実施できると望ましいです。

| レベル | 人材フレームワークのレベルの定義（抜粋） | |
|---|---|---|
| 4 | レベル4-M<br>業務における意思決定に責任を負う者 | レベル4-E<br>自らの専門分野を確立し、ハイレベルのプレーヤとして組織内外で認知されている者 |
| 3 | レベル3-M<br>業務について関連するチームメンバのマネジメントを行う者 | レベル3-E<br>自らの専門領域の業務を独力で遂行可能な者 |
| 2 | レベル2<br>業務において指示に基づく作業を実行する者 | |
| 1 | レベル1<br>業務に対する最低限必要な知識を有する者 | |

**令和7年度に各種求人サイト上のサイバーセキュリティ関係求人で多く見られる役割及びTKSの例**

| | レベル3-M相当 | レベル3-E相当 |
|---|---|---|
| 役割 | 意思決定・戦略策定、戦略推進・プロジェクト管理、法務　等 | 設計開発、監視、対処（インシデントレスポンス）　等 |
| セルフアセスメント項目（例） | | |
| タスク(T)<br>※定義より共通する性質を抽象化 | 組織のセキュリティ方針・ルールや、プロジェクト計画の立案・策定 | システムに対する適切なセキュリティ設定の設計・実装、および事後対応・復旧措置 |
| | 経営層や関連部署に対するセキュリティリスクや評価結果の報告・説明 | 検知された異常（アラート）やインシデントに対する初期調査および原因究明 |
| 知識(K) | サイバーセキュリティ関連法規・組織内のポリシー・関連計画に関する知識 | サイバー攻撃やサイバーセキュリティの脅威/脆弱性に関する知識 |
| | リスクマネジメントに関する知識 | ネットワークセキュリティに関する知識 |
| スキル(S) | 関係者と適切なコミュニケーションを行うスキル | ハードウェア、ソフトウェア、基幹システム等の性能を把握し、最適な設定を実施するスキル |
| | 今後組織におけるリスクとなり得るサイバーセキュリティ脅威を想定するスキル | ハードウェア、ソフトウェア、基幹システム等の性能を把握し、最適な設定を実施するスキル |
| 備考 | 上流工程経験に加え、マネジメント・PL経験等の企画力も重視。 | クラウド等の最新技術スタック、特定製品知識の深堀りスキルが要求。 |

# 目標例３（新たにサイバーセキュリティのキャリアを目指したい）

- 今後新たにサイバーセキュリティ分野におけるキャリアパスを検討される方は、既にご活躍される専門人材の事例等も参考にいただき、自身の関心に近い役割は何か、考えてみましょう。
- レベルの詳細は大規模組織向け手引き書を参照してください。ここではキャリアの入り口としてどういった事例があり得るか取り上げています。

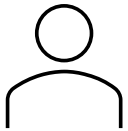
| 専門人材の事例※ | セルフアセスメント項目（例） | |
|---|---|---|
| **現場技術からのマネジメント・エキスパート分岐型**<br>ITシステム全体を広く「運用管理」する立場としてキャリアを開始させ、マネジメント系、エキスパート系のどちらにキャリアの軸を置くか判断するパターン | タスク(T) | システム及びネットワーク機器のアップデート・バックアップの管理 |
| | 知識(K) | ネットワークインフラストラクチャに関する知識 |
| | スキル(S) | ハードウェア、ソフトウェア、基幹システム等を管理するスキル |
| **監査・ガバナンス専門家型**<br>キャリアを通じ一貫して、「監査」「法務」に関する専門性を磨いていくキャリアパターン | タスク(T) | 個人情報管理、コンプライアンス等、法的リスク分析の対象とすべき情報、サービスや、その関連法令・社内規定を取得・整理 |
| | 知識(K) | コンプライアンスおよびプライバシーの原則と実践に関する知識 |
| | スキル(S) | 法的事項や技術的事項を、専門家および非専門家に対して分かりやすく口頭で説明し、理解を促すスキル |
| **技術領域のエキスパート深化型**<br>「設計・開発」を中心とした技術の最前線に身を置き、特定技術の専門性を磨いていくキャリアパターン | タスク(T) | 開発・実装（※初期的なスクリプト作成や自動化等を含む） |
| | 知識(K) | システムとアーキテクチャに関する知識 |
| | スキル(S) | 情報システムのパフォーマンスの低下や、トラブルが発生した場合に、原因を追究し解決するスキル |
| **アカデミアからのエキスパート社会実装型**<br>「研究」領域から始まり、アカデミアの探究を最終的に社会やビジネスへどのように実装するか模索するキャリアパターン | タスク(T) | 自組織内/外におけるサイバーセキュリティに係る課題の把握 |
| | 知識(K) | サイバー攻撃やサイバーセキュリティの脅威/脆弱性に関する知識 |
| | スキル(S) | 研究結果が実用化等の発展可能性を判別するスキル |

※上記パターンは、本書でわかりやすく事例紹介をするための類型であり、実際のキャリアパスはより多様なパターンが想定されます。

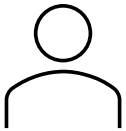
# フレームワークを用いたセルフアセスメントに関する補足

- サイバーセキュリティ人材のフレームワークにおいて定義される13の役割においては、実態として1つの役割に含まれる複数の具体的業務（タスク）が混ざっている場合があります。
- セルフアセスメントにおいては、13の役割に加えて、所属組織あるいは自身のキャリアにおいて実施する必要のあるタスクとは何か、整理するステップも大切にしましょう。

**例）目標例1（目標設定・評価面談）より**



ご本人



上司等

13の役割も参考にした実施タスクの具体化

タスクの達成度の確認 など

目標設定に向けた確認として、当部の担当業務としては、13の役割のうちの「●●」、この中でタスク「〇〇」や「△△」を所掌している理解で合っていますか？

はい、役割は「●●」でそのとおりで、タスクについては「□□」も入ってきます。

承知しました。タスク「〇〇」「△△」「□□」に対する達成状況、および関連する知識・スキルの習得が今年度の評価に関わってくるでしょうか？

そのとおりです。加えて、個人の関心ある領域の専門性を高めていっていただきたいので、その領域についての言語化も、フレームワーク等も活用しながら整理していってください。

分かりました。では具体的に担当業務について、タスク「●●」については…

**ポイント**

- セルフアセスメントについて、目標例1～3いずれにおいても、まずは所属組織あるいは自身のキャリアにおける現状や将来を見据え、実施が求められるタスクは何か、13の役割からさらにブレイクダウンして整理すると、その後の知識・スキルのギャップに関する検討も効果的に進められます。
- 以下の例も参考にしつつ、多様な業務・タスクが関連する役割については、こうした前段の整理も大事にしましょう。

**役割に含まれる具体的業務（例）**

脆弱性評価

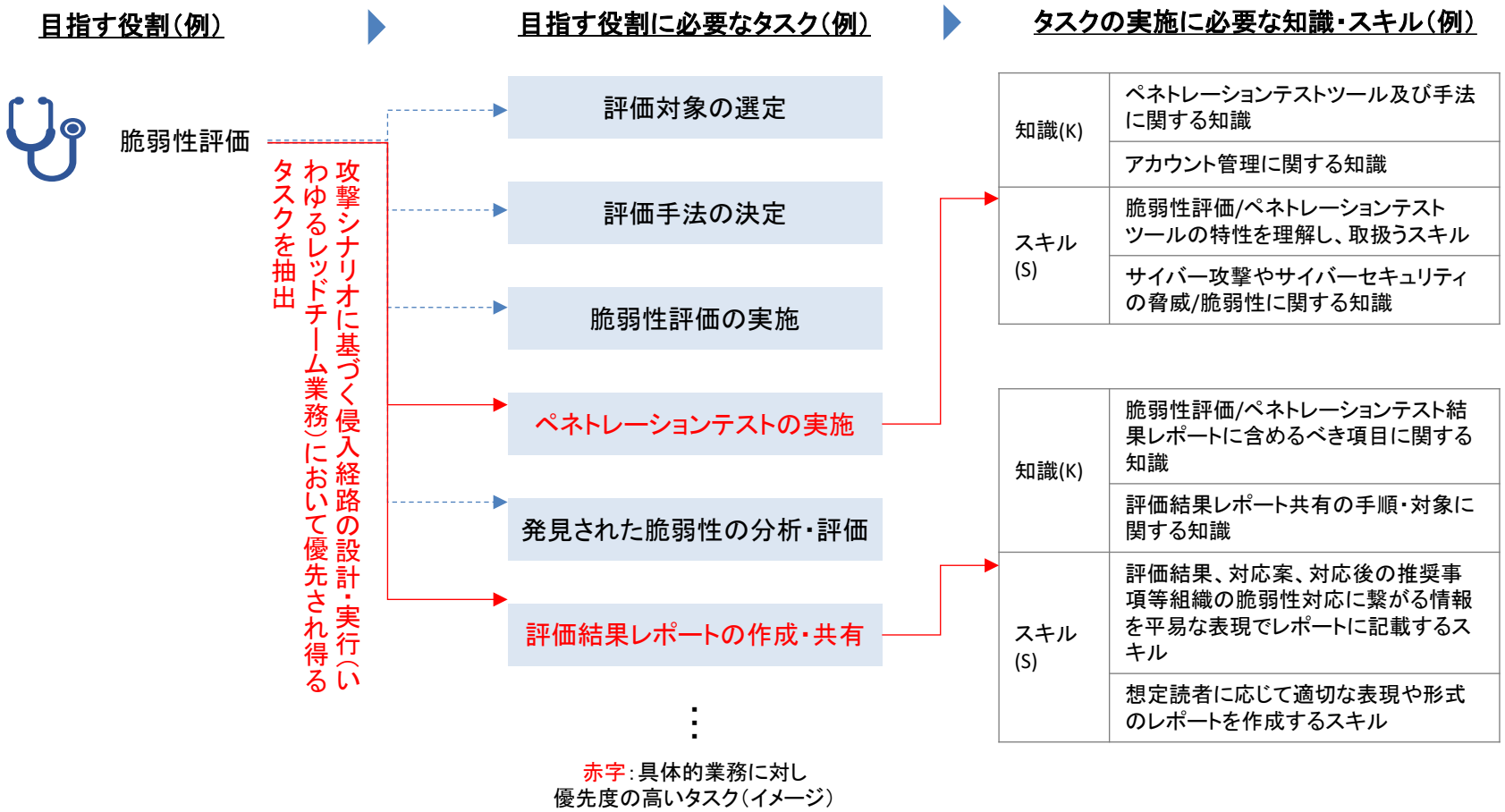
- 攻撃シナリオに基づく侵入経路の設計・実行（レッドチーム）（後述にさらに補足紹介）
- 網羅的に脆弱性を確認
- …

運用管理

- 脆弱性の修正・再発防止（後述にさらに補足紹介）
- アクセス制御やアカウントの管理
- …

# フレームワークを用いたセルフアセスメントに関する補足

- 所属組織あるいは自身のキャリアにおいて実施する必要のあるタスクを整理する際にも、フレームワークを活用してみましょう。
- 例えば、前頁のように脆弱性評価という役割には、「攻撃シナリオに基づく侵入経路の設計・実行（レッドチーム）」「網羅的に脆弱性を確認」といった具体的業務が複数含まれています。
- 具体的業務を遂行する上で優先度の高いタスクを、フレームワークを用い抽出することで、自身のキャリア形成において必要な知識・スキルを整理しやすくなります。




赤字：具体的業務に対し
優先度の高いタスク（イメージ）

# フレームワークを用いたセルフアセスメントに関する補足（例１）

- 役割「脆弱性評価」において、実際の攻撃者と同じ目線で疑似攻撃を行い、組織の検知・対応能力を含めた総合的なセキュリティ水準を検証する「レッドチーム」の職務に関するセルフアセスメント例です。
- ここでは、実際の業務における行動特性をもとに評価します。この役割で技術の専門家を目指す場合、各項目に対して「定められた手順書どおりに実行できるか」「マニュアル外の未知の事象や複雑な技術的課題に対しても、自律的かつ独力で完遂できるか」といった基準で自己評価を行えると望ましいです。

## セルフアセスメントの例

| 区分 | セルフアセスメント項目 | 自己評価 | 自己評価の理由 |
|---|---|---|---|
| タスク(T) | ペネトレーションテストの実施 | ○ | シナリオに基づき、防御機構の回避や内部侵入を伴う高度なテストを独力で完遂できる |
| | 評価結果レポートの作成・共有 | △ | 既存のテンプレートと指示に従い、正確にレポートを作成し共有できる |
| 知識(K) | ペネトレーションテストツール及び手法に関する知識 | × | 未習得 |
| | アカウント管理に関する知識 | ○ | 非定型な設定時にも独力で活用できる知識がある |
| スキル(S) | 脆弱性評価/ペネトレーションテストツールの特性を理解し、取扱うスキル | △ | 上位者の補助の下でツールを操作できる |
| | サイバー攻撃やサイバーセキュリティの脅威/脆弱性に関する知識 | ○ | 実際の攻撃グループ（APT）のTTPsを深く分析し、実戦的なレッドチーム演習に組み込める |

## 評価の基準の考え方
（エキスパート系の場合）

**自律性**

指示やマニュアルに依存せず、自らの専門的知見をもとに独力で業務を完遂できるか。

**タスクの複雑さ**

未知の脅威や高度なアーキテクチャなど、マニュアルでは対応できない技術的・専門的に高度で非定型な課題を解決できるか。

**影響力**

組織内での高度な技術指導、コミュニティでの情報発信や独自研究など、業界や社会の技術水準に対する影響力があるか。

# フレームワークを用いたセルフアセスメントに関する補足（例２）

- 前ページと同様、役割「運用管理」において、自社の環境を最新の脅威から守る「脆弱性の修正・再発防止」等に関連するタスク・知識・スキルを抽出したセルフアセスメント例です。
- 運用管理の現場では、自身で非定型なトラブルを解決する専門性と独力遂行力に加え、チームを指揮し、関係部署と利害調整を行う「組織と人を動かす力」の2つの方向性が存在します。

## セルフアセスメントの例

| 区分 | セルフアセスメント項目 | 自己評価 | 自己評価の理由 |
|---|---|---|---|
| タスク(T) | システム内又はネットワーク機器内で発見された脆弱性の修正 | ○ | 未知のエラーに対しても、独力で修正作業を完遂できる |
| | 再発防止策の検討と実装 | ○ | 関係部署との利害調整を主導し、対策を組織に実装させている |
| 知識(K) | 情報システムの脆弱性の修正方法に関する知識 | ○ | 修正の影響範囲を見極め、チームや他部署へ指示・説明ができる |
| | ネットワークの脆弱性に関する知識 | ○ | 知識をもとに、チーム内への対策指示やマネジメントができる |
| スキル(S) | ハードウェア、ソフトウェア、基幹システム等に適切なセキュリティ対策を設定するスキル | × | 未習得 |
| | ネットワークのトラブルの原因を追究し、ネットワークを再構築するスキル | ○ | ビジネス影響を踏まえて対応を判断し、全社的な復旧指揮をとれる |

## 評価の基準の考え方（マネジメント系の場合）

**自律性**

組織の課題を自ら見つけ、他者（チーム・他部署）を動かして自律的に業務を推進・管理できるか。

**タスクの複雑さ**

ビジネスへの影響、予算、部門間の利害など、組織的・人的要因が絡む複雑な課題を整理し、意思決定や調整ができるか。

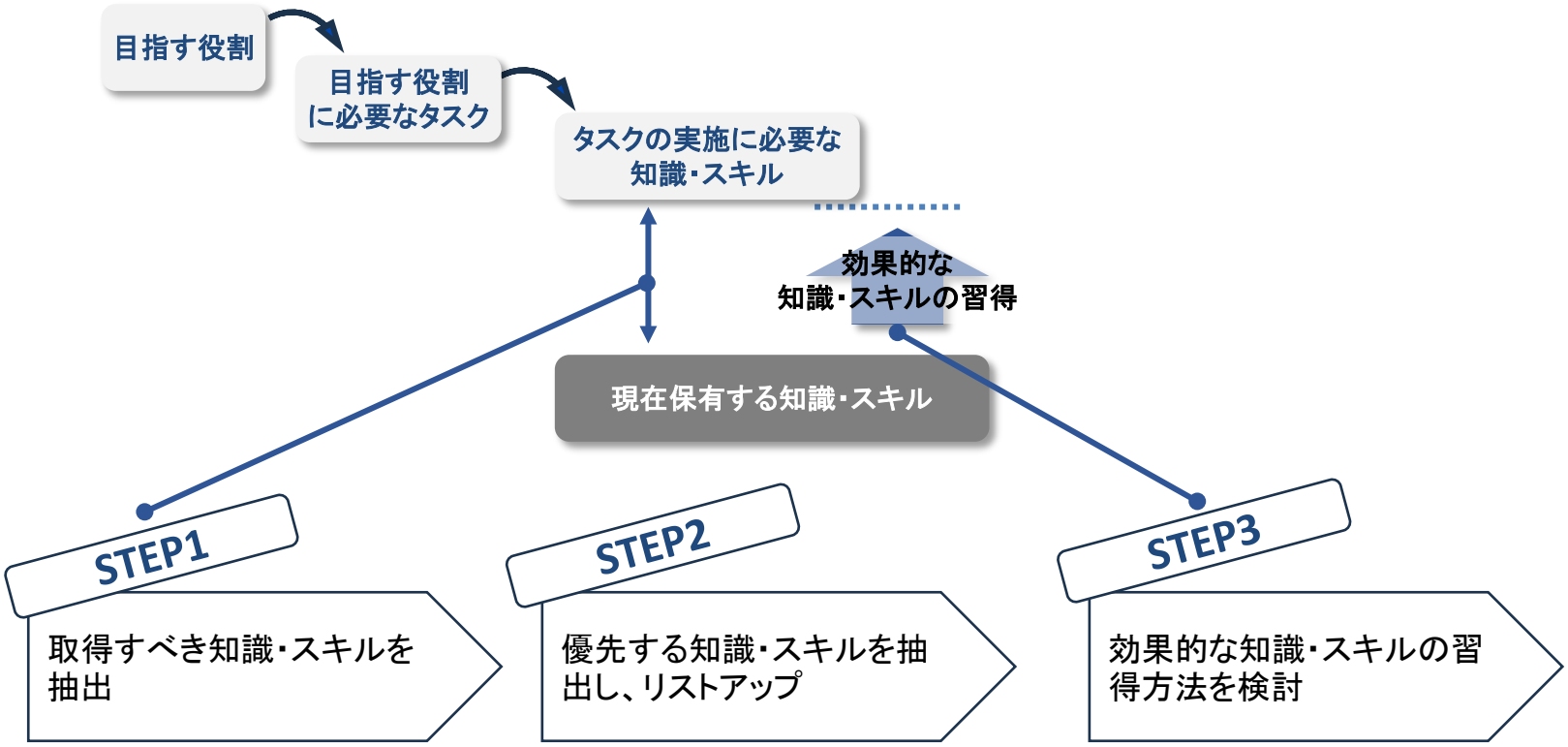
**影響力**

チームの育成、関係部署の意識向上、経営層の意思決定支援など、組織内部の体制やビジネスに対する影響力があるか。

# スキルアップとキャリア形成のアプローチ

# スキルアップとキャリア形成のアプローチ（全体像）

- セルフアセスメントを通じ整理された現状をふまえ、目指すキャリアを実現するための知識・スキル取得を軸にしたキャリア形成の考え方を示します。
- 不足する知識・スキルを抽出し、業務上のニーズ等も踏まえて優先順位をつけた上で、社内研修や外部セミナーなど具体的な補完方法を決定・実行していくプロセスとなります。




セルフアセスメントを通じ整理された知識・スキルの現状と、フレームワークにより整理された目指す役割に必要な知識・スキルの**差分を整理**しましょう

抽出された知識・スキルの差分のうち、**「社会情勢の変化」「所属組織における方針・要望」「自身の関心」**に応じ、取得するものの優先度をつけましょう

優先度の高い知識・スキルの習得に向けて、具体的なアクションプランを検討しましょう。主に、**「資格取得」「研修」「OJT等実務」「コミュニティ活動」**が考えられます。

# 効果的な知識・スキルの習得方法

- 知識・スキルの習得方法については、後述でご紹介する専門人材の実際のキャリア事例でのご経験もふまえ、大きく4つに大別して紹介します。
- なお、ご紹介する方法はあくまでも推奨であり、読者の皆様に適した方法を選んでいただく際の情報としてご参照ください。

## 関連する資格の取得

特定の組織や環境に依存しない「体系的で普遍的な基礎概念」「法規制・コンプライアンスの原則」「客観的な評価・監査のフレームワーク」など、実務の土台として獲得すべき知識を中心に習得できます。

＜該当すると考えられる主な知識・スキル＞
サイバーセキュリティの基本原則と実践に関する知識、リスクマネジメントに関する知識、監査プロセスに関する知識、組織の抱えるシステム上におけるサイバーセキュリティの課題に関する知識、インシデント対処に関する知識　など

モデル人材の声

「資格で学ぶ概念により、情報資産を守るという基本知識や、現場のエンジニアと対話できる概念・言語が獲得できました」

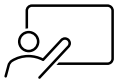
## OJT等の実務を通じた習得

資格や研修では習得しづらい、「現場固有のシステム環境や構成等への適応力」「イレギュラーへの対応力」「関係者との折衝力」など、実務遂行に必要な知識・スキルを習得できます。

＜該当すると考えられる主な知識・スキル＞
自組織におけるサイバーセキュリティに関する規程類に関する知識、組織のシステムやネットワークの基本原則や構造に関する知識、一連のインシデント対処で生じた情報を活用しインシデントの原因を究明するスキル　など

モデル人材の声

「現場特有のノウハウは、現地で紐解き教わっていく領域だと考えています。現場のベテラン（有識者）に積極的に教えを請う姿勢を重視していました。」



## 研修の受講

独学では習得しづらい最新の専門技術や実践的手法、特定製品・ツールの深い仕様理解など、外部の高度な知識・スキルを習得できます。

＜該当すると考えられる主な知識・スキル＞
セキュリティログ（システムログ、アプリケーションログ等）に関する知識、インシデント対処を実施するスキル、脅威シナリオを元に脆弱性評価/ペネトレーションテストを行い脆弱性の有無を明らかにするスキル、情報収集ツールの特性を理解し組織の目的に合った最適なツールを選定するスキル　など

モデル人材の声

「新しい技術や調査手法を学ぶ際は、研修形式の方が頭に残りやすかったです」

## コミュニティ活動への参加

自組織の実務だけでは視野が狭くなりがちなこともふまえ、「他社の最新動向」「業界の標準化の視座」「トップ層とのネットワーキング」など、組織の枠を超えた広がりを持つ知識・スキルを習得できます。

＜該当すると考えられる主な知識・スキル＞
サイバー攻撃やサイバーセキュリティの脅威/脆弱性に関する知識、学会やコミュニティ活動への参加（タスク）、業界標準に応じて情報を分類するスキル　など

モデル人材の声

「会社の仕事だけでは伸びないと考えています。コミュニティに入って勉強会に出ることでアンテナが高まった感覚があります。」

# 効果的な知識・スキルの習得方法（資格の紹介）

- 資格取得を通じては、特定の組織や環境に依存しない「体系的な基礎概念」「法規制・コンプライアンス」「客観的な評価基準」に関する知識・スキルの習得が期待されます。
- フレームワークで定義される知識を網羅的にカバーされる資格としては、「情報処理安全確保支援士」が挙げられますが、カバーしきれない知識・スキルについては別の資格取得をご検討ください。

### ①意思決定・戦略策定

＜役割に関係する主なTKS例＞
- リスクマネジメントに関する知識
- 組織のサイバーセキュリティに係る方針や目標を策定し、組織設計を行うスキル
- サイバーセキュリティに関する戦略、方針、規定等を策定又は承認する

### ⑩法務

＜役割に関係する主なTKS例＞
- コンプライアンスおよびプライバシーの原則と実践に関する知識
- サイバーセキュリティ関連法規・組織内のポリシー・関連計画に関する知識

### ⑪監査

＜役割に関係する主なTKS例＞
- 監査プロセスに関する知識
- 監査対象に対する個別の監査結果を踏まえ、セキュリティ要件への適合性を総合的に評価するスキル

### ⑧運用管理

＜役割に関係する主なTKS例＞
- ネットワークインフラストラクチャに関する知識
- ハードウェア、ソフトウェア、基幹システム等に関する知識

### 情報処理安全確保支援士（最新シラバス※より関連する主な事項を例示）

- 情報セキュリティリスクアセスメント
- 情報セキュリティリスク対応
  など

- コンプライアンス管理（個人情報保護法等の法令やガイドラインの知識等）
- 情報セキュリティ諸規程の策定
  など

- 情報セキュリティ監査（監査のプロセス、関連文書、監査証拠に関する知識等）
  など

### その他資格でカバーが期待される知識・スキル（例）

- サイバーセキュリティに関する戦略、方針、規定等を策定又は承認する

**CISMなど**

- 監査対象に対する個別の監査結果を踏まえ、セキュリティ要件への適合性を総合的に評価するスキル

**システム監査技術者など**

- ハードウェア、ソフトウェア、基幹システム等に関する知識

**クラウドサービスやOSベンダーが実施する試験など**

※独立行政法人情報処理推進機構（IPA）情報処理安全確保支援士試験（レベル4）シラバス https://www.ipa.go.jp/shiken/syllabus/nq6ept00000014ir-att/syllabus_sc_ver2_1.pdf （2026年3月5日閲覧）

# 効果的な知識・スキルの習得方法（研修の紹介）

- 研修受講を通じては、独学や社内のOJTでは経験しづらい「最先端の攻撃手法の検証」や「特定の高度ツールの取扱手法」など、外部の高度な知識・スキルの習得が期待されます。
- なお、公的機関の提供する研修もありますのでご参照ください。

### ④対処

OSINT等の専門研修を受講し、日々のインシデント調査業務に直接活用しています。

＜役割に関係する主なTKS例＞
- インシデント対処を実施するスキル
- インシデント対処に関する知識

### ⑥脆弱性評価

ゼロデイ脆弱性の発見手法、実践的なペネトレーションテストにおける攻撃シナリオの設計方法等について習得しました。

＜役割に関係する主なTKS例＞
- 脅威シナリオを元に脆弱性評価/ペネトレーションテストを行い、脆弱性の有無を明らかにするスキル
- 脆弱性評価/ペネトレーションテストツールの特性を理解し、取扱うスキル

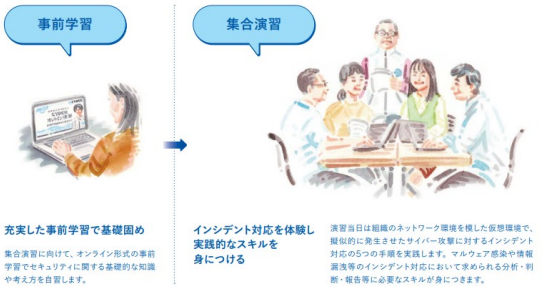
### ⑦フォレンジック

インシデントハンドリングにおける高度な解析・対応手法を習得しました。

＜役割に関係する主なTKS例＞
- フォレンジック対応のプロセスから対象機器の仕様の理解、必要資材の調達、ツール準備等を行うスキル
- フォレンジック対応のプロセス、必要なツール等に関する知識

## 実践的サイバー防御演習「CYDER」

NICT（情報通信研究機構）が提供する実践的サイバー防御演習「CYDER」は、実際の組織ネットワークを模した環境で、サイバー攻撃の検知・分析・初動対応・復旧までを体験的に学ぶ演習プログラムです。標的型攻撃やマルウェア感染などを想定し、実務に直結する対応力の向上を目的としています。
行政機関や民間企業等のセキュリティ人材を想定し、受講者の経験や役割に応じて、基礎から実践まで複数のコースを用意し、攻撃対応の判断力・技術力を段階的に習得できる構成となっています。（学生の方は受講できません）




※国立研究開発法人情報通信研究機構（NICT）「コース案内」 https://cyder.nict.go.jp/course/index.html （2026年3月10日閲覧）

# 効果的な知識・スキルの習得方法（OJT等実務の紹介）

- OJT等実務を通じては、資格や研修では身につけづらい「現場固有のシステム環境や構成等への適応力」「イレギュラーへの対応力」「関係者との折衝力」といった知識・スキルの習得が期待されます。
- 特に、フレームワークにて定義されるスキルの大半は、実務を通じ習得されることが多いと考えられます。

②戦略推進・プロジェクト管理

- 顧客との要件定義や報告書説明の実務から折衝力を習得しました。
- 顧客への提案や見積作成等の業務を通じ、プロジェクト推進力を獲得しました。

＜役割に関係する主なTKS例＞
- 組織目標や戦略を分析し、プロジェクト計画を立案するスキル
- プロジェクトの進行状況を把握し、必要に応じて調整するスキル
- 関係者と適切なコミュニケーションを行うスキル

③監視

- 重大インシデント時のログ調査は、業務を通じて時間をかけて習熟していくことが大事と考えています。
- 実務において、クエリの組み直しの経験も行い、スキルを習得しました。

＜役割に関係する主なTKS例＞
- 分析ツールを使用してログ分析を実施するスキル
- ツールの設定値を見直し、適切な設定値に変更するスキル
- アラートの監視・調査・分析から不審な兆候を検知し、関係部署へ報告・通報

⑫設計開発

- 研究部署でのシステム実装やクラウド上の開発環境における実務を通じて実装スキルを習得しました。
- 多様な現場でDevSecOps（開発プロセスへのセキュリティ組み込み）を実践し技術を磨きました。

＜役割に関係する主なTKS例＞
- 新たなプログラムを作成、又は既成品を選定し、システムに実装するスキル
- コーディング、統合、内部デプロイ等実装に関する知識

# 効果的な知識・スキルの習得方法（コミュニティ活動の紹介）

- コミュニティ活動を通じては、視野を広げるため「他社・他業界の最新動向」「業界の標準化・ルールメイキングの視座」「トップ層とのネットワーキング」を獲得することが期待されます。
- 公的なコミュニティの場として、全国各地に「地域SECUNITY」※もありますので、関心ある方は活動内容の詳細や参加方法等をご確認ください。

### ⑤情報収集・分析・共有

研究会や勉強会に所属し、社内外の有識者とネットワーキングや情報交換を行っています。

＜役割に関係する主なTKS例＞
- サイバー攻撃やサイバーセキュリティの脅威/脆弱性に関する知識
- 議論のファシリテーションを行うスキル

### ⑨教育・訓練

自分以外に講師として選出された日本のトップエンジニアや研究者と育成ノウハウを共有しています。

＜役割に関係する主なTKS例＞
- 教育計画、課程およびカリキュラムを策定するスキル
- 教育・訓練を受講する組織のセキュアな組織運営をするための情報収集、管理、対処等について教育するスキル

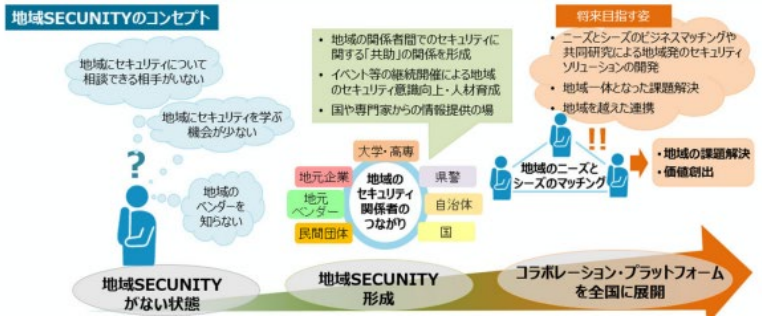
### ⑬研究

学術研究活動を通じ博士号取得を目指しています。また、コミュニティを通じ転職活動も行いました。

＜役割に関係する主なTKS例＞
- 立案した仮説を調査に基づいた実験などを通し、検証するスキル
- 研究の目的や具体的な研究内容、研究手法等を記載した研究計画書を作成するスキル
- ネットワークに対する攻撃に関する知識

## 地域SECUNITY

- 経済産業省では、地域の民間企業、行政機関、教育機関、関係団体等が、セキュリティについて語り合い、「共助」の関係を築くコミュニティ活動を、「地域SECUNITY」と命名しています。
- （閲覧時点の情報では）北海道から沖縄まで、全国各地に「地域SECUNITY」がありますので、関心ある方は、お近くを拠点とするコミュニティを覗いてみましょう。




※ 地域SECUNITY紹介ページ　https://www.meti.go.jp/policy/netsecurity/secunity.html（2026年3月5日閲覧）

# 役立つリンク集・用語集

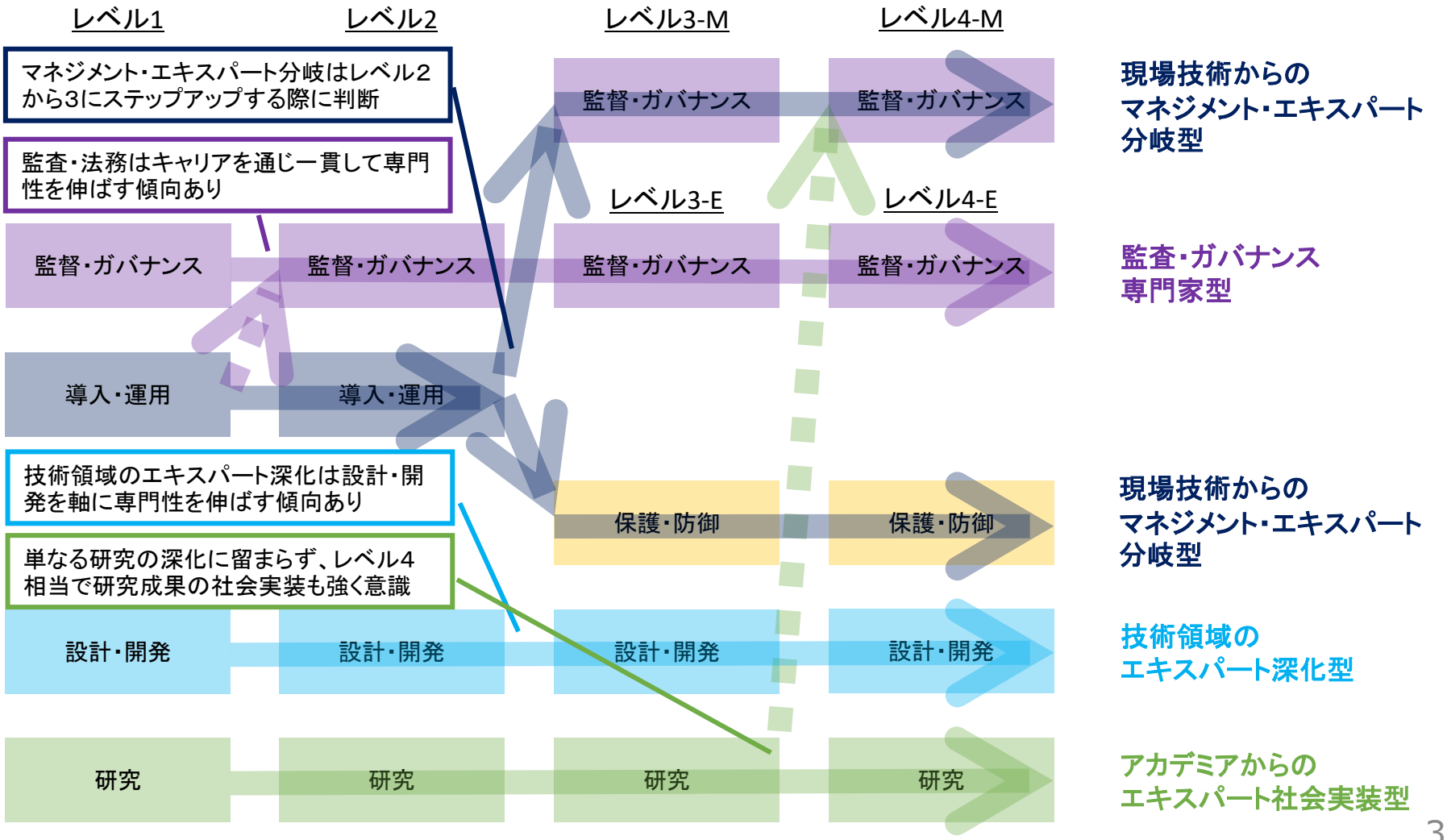
- サイバーセキュリティの専門人材を目指すにあたって、本手引き書と併せて活用できる関連資料をご紹介します。
- サイバーセキュリティ人材フレームワークの本体や、経済産業省やIPAが公表するガイドライン、ツール等のリンク集として自身のキャリアを考える際にご活用ください。

- 国立研究開発法人情報通信研究機構（NICT）「コース案内」（https://cyder.nict.go.jp/course/index.html）
  - 必要なセキュリティ知識を短時間で学習する、実践的サイバー防御演習「CYDER」についてご案内しています。
- 独立行政法人情報処理推進機構「セキュリティインシデント対応机上演習教材」（https://www.ipa.go.jp/security/sec-tools/ttx.html）
  - 一般企業（中小企業）と医療機関の2種類を対象として、実際にセキュリティインシデントが発生した場合を想定した演習教材についてご案内しています。
- 独立行政法人情報処理推進機構「情報処理安全確保支援士試験（レベル4）シラバス」（https://www.ipa.go.jp/shiken/syllabus/nq6ept00000014ir-att/syllabus_sc_ver2_1.pdf）
  - フレームワークで定義される知識を網羅的にカバーされる資格として、ご参照ください。
- 経済産業省「地域SECUNITY」（https://www.meti.go.jp/policy/netsecurity/secunity.html）
  - 地域の民間企業、行政機関、教育機関、関係団体等が、セキュリティについて語り合い、「共助」の関係を築くコミュニティ活動として、ご案内しています。

# 専門人材の例

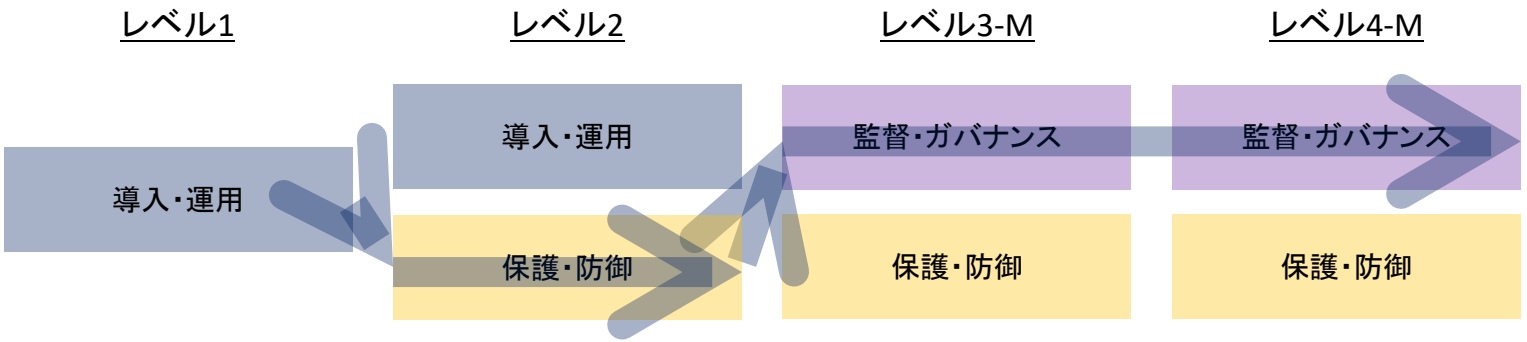
# 専門人材のキャリアパス事例（モデルケース）

- ここからは、実際に過去に知識・スキルギャップを埋めるキャリアを経験され、現在も活躍される専門人材の実体験についてご紹介いたします。
- 実際のキャリアパスはより複雑なパスを通りますが、今回は本書でわかりやすく事例紹介をするため、4パターンの類型化をしており、次頁より各パターンに相当する専門人材の事例を順に掲載をしています。



# 事例1：現場技術からのマネジメント・エキスパート分岐型A（①意思決定・戦略策定）

- ITシステムの運用保守という現場の最前線からキャリアをスタートし、脆弱性診断やセキュアなシステム設計（DevSecOps）の実務を経て専門性を拡大。現在はセキュリティアドバイザリ事業を立ち上げ、経営・戦略的な視点から顧客組織を導く意思決定の役割へと飛躍されています。




**知識・スキルの取得**

| レベル1 | レベル2 | レベル3-M | レベル4-M |
|---|---|---|---|
| SESでの現場経験によるIT基礎概念の習得と運用 | 顧客要件に基づく自律的な診断実務と自社システム開発 | 診断内製化の指導、DevSecOps実装、ISMS体制構築 | 経営者としての戦略的助言、大学等での体系的なセキュリティ教育 |
| • 高度情報処理技術者試験や認定脆弱性診断士などの資格学習から体系的な「概念」を習得 | • DevSecOpsを推進する立場として、現場の開発エンジニアの苦労を理解し、彼らと円滑に調整・合意形成する経験を通じ、マネジメントの基礎固めを実施 | • 中小企業の経営者と直接対峙する中で、事業継続を最優先としつつリスクマネジメントを行う現実的な提案力・組織設計スキルを実践から習得 | |

**役割（主）**

運用管理　脆弱性評価　戦略推進・プロジェクト管理　意思決定・戦略策定

**役割（副）**

情報収集・分析・共有　脆弱性評価　教育・訓練　監査　対処　設計開発

# 事例1：現場技術からのマネジメント・エキスパート分岐型A（①意思決定・戦略策定）

- 資格学習で体系的な「概念」を身につけつつ、多様な現場目線での「実践知」を吸収することが、ITインフラ運用から経営層を支えるポジションへ飛躍する際の重要な知識・スキル取得方法となっています。

## キャリアシフト時に習得した主な知識・スキル

ポイント　レベル2から3にてマネジメント系知識・スキル習得

※下線部の知識・スキルがポイントと関連

### レベル1～2

運用管理～脆弱性評価へのシフト

| TKS | シフト時に新たに習得・拡大 |
|---|---|
| 知識 | • サイバーセキュリティの基本原則と実践に関する知識<br>• サイバー攻撃やサイバーセキュリティの脅威/脆弱性に関する知識 |
| スキル | • 脆弱性評価/ペネトレーションテストツールの特性を理解し、取扱うスキル<br>• 組織のサイバーセキュリティ環境・目的にあった脅威シナリオを元に脆弱性評価/ペネトレーションテストを行い、脆弱性の有無を明らかにするスキル |

### レベル2～3-M

脆弱性評価～戦略推進・PJ管理へのシフト

| TKS | シフト時に新たに習得・拡大 |
|---|---|
| 知識 | • コーディング、統合、内部デプロイ等実装に関する知識<br>• システムとアーキテクチャに関する知識 |
| スキル | • 関係者へヒアリングを行い、システム上のサイバーセキュリティにおける課題を整理するスキル<br>• 実装する機能を現場との調整の上段階的に実装するスキル |

### レベル3-M～4-M

戦略推進・PJ管理～意思決定・戦略策定へのシフト

| TKS | シフト時に新たに習得・拡大 |
|---|---|
| 知識 | • コンプライアンスおよびプライバシーの原則と実践に関する知識<br>• リスクマネジメントに関する知識 |
| スキル | • 今後組織におけるリスクとなり得るサイバーセキュリティ脅威を想定するスキル<br>• 組織のサイバーセキュリティに係る方針や目標を策定し、組織設計を行うスキル |

## キャリア通じ重要な知識・スキル

**複雑な事象の「構造化」と「言語化」スキル**

- ロジカルシンキングを用い、セキュリティの専門的でわかりづらい部分を分解・整理し、経営層や初学者に「翻訳」して伝えるコミュニケーション能力。
- 外部講師を招いた月1回の社内研修を半年間継続し、培われたもの。

**「逆T字型」のスキルスタックと継続的なキャッチアップ**

- 自分の専門領域（縦の軸）を深めつつ、他の領域（横の軸）を広く浅く知るスタンス。
- AIの進化等で陳腐化しないよう、被害レポートからの脅威分析など、日々生きた情報を収集・分析する姿勢。

**コミュニティ活用と着実なリレーション構築**

- 現場特有のノウハウ（方言）は資格のみでは学べないため、現場の有識者から積極的に学ぶ姿勢。
- コミュニティに自ら飛び込み、他者の知見を吸収する行動力。

# 事例2：現場技術からのマネジメント・エキスパート分岐型B（④対処）

- Web系アプリの全工程開発からキャリアを始め、長年にわたるCSIRT現場での対応と継続的な技術研鑽により、高い技術的専門性を発揮し若手を牽引するシニアエキスパートへと飛躍されています。


**知識・スキルの取得**

| レベル2 | レベル3-E | レベル4-E |
|---|---|---|
| Webアプリ上流工程対応と短期間の脆弱性診断実務 | Webアプリ全工程開発、SIEM導入、CSIRT現場対応とチーム運営 | 技術を極めるシニアエキスパート、大学等での研究・教育活動 |
| • サーバ構築など全工程を実践<br>• 「自宅サーバを立てて運用」といった自己学習により、業務以外でも知見を得る習慣をつける | • 手順書レベルを超えた「定型クエリではないログ分析」や「フォレンジック」等の高度な技術ギャップに対しては、自ら手を動かしたり社外勉強会に参加<br>• 「経営層と対話するためのコミュニケーション力・話術・姿勢」の不足解消 | |

**役割(主)**

| レベル2 | レベル3-E | レベル4-E |
|---|---|---|
| 運用管理 | 対処 | 対処 |

**役割(副)**

| レベル2 | レベル3-E | レベル4-E |
|---|---|---|
| 脆弱性評価 | 戦略推進・プロジェクト管理<br>運用管理<br>脆弱性評価 | 教育・訓練 |

# 事例2：現場技術からのマネジメント・エキスパート分岐型B（④対処）

- CTFなどの自己学習や高度な資格研修で体系的な知見を補完しつつ、CSIRTの最前線で着実に実践知を蓄積することが、アプリ開発から現場を牽引する際の重要な知識・スキル習得方法となっています。

## キャリアシフト時に習得した主な知識・スキル

ポイント　自己学習等を通じエキスパート系を一貫して志向

※下線部の知識・スキルがポイントと関連

レベル2～3-E

設計開発～対処へのシフト

| TKS | シフト時に新たに習得・拡大 |
|---|---|
| 知識 | • セキュリティログ（システムログ、アプリケーションログ等）に関する知識<br>• サイバー攻撃やサイバーセキュリティの脅威/脆弱性に関する知識 |
| スキル | • 分析ツールを使用してログ分析を実施するスキル<br>• ツールの設定値を監視対象や目的に応じた設定にするスキル |

レベル3-E～4-E

対処における専門性深化

| TKS | シフト時に新たに習得・拡大 |
|---|---|
| 知識 | • フォレンジック対応のプロセス、必要なツール等に関する知識 |
| スキル | • インシデントの概要、自組織内/外への影響、復旧見込を速やかにとりまとめ、組織のCISO、経営層に報告するスキル<br>• 一連のインシデント対処で生じた新たな情報や外部からの情報を活用し、インシデントの原因を究明するスキル |

## キャリア通じ重要な知識・スキル

**未知の領域を恐れず試行する仮説検証力**

- 新しい技術や難解なログ分析に直面しても、座学に留まらず、自宅環境や無料ツールを使って実際に手を動かして検証する自律的な学習姿勢が重要

**正常と異常を見極める実践的状況判断力**

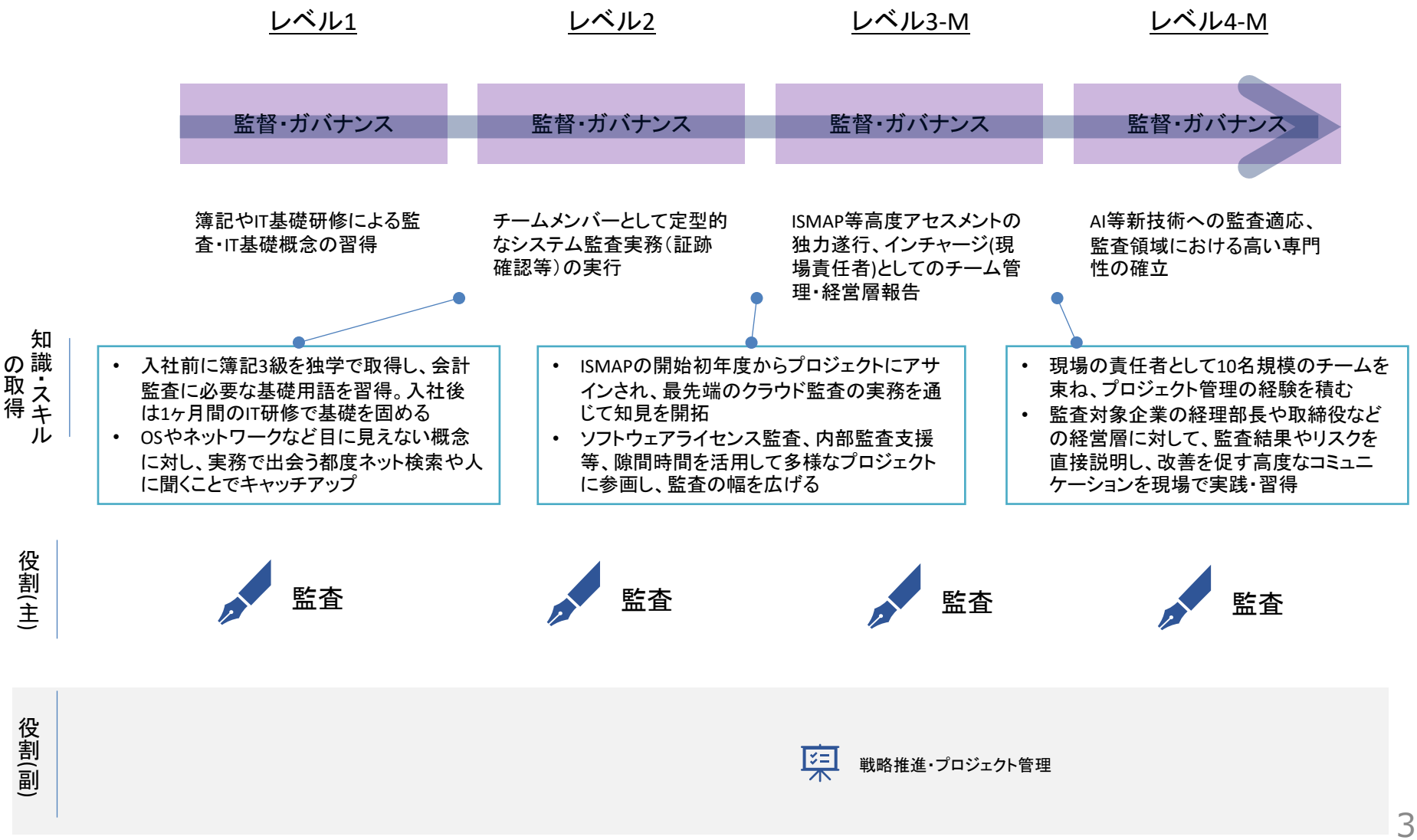
- インフラ構築の経験に裏打ちされた「システムのあるべき姿」の理解に基づいた、適切かつ正確なログ分析のスキル

**相手を引き出し組織を回す対人関係・傾聴力**

- 1on1で相手の意見を引き出すスタンスや、「一人で頑張りすぎず周りを巻き込む」というマインドセットが、属人化を防ぎ、組織全体のセキュリティ活動を安定させるように貢献

# 事例3：監査・ガバナンス専門家型A（⑪監査）

- システム監査の現場からキャリアを始め、高度なセキュリティ監査の独力遂行や経営層への報告経験を重ねて専門性を深化し、現在は最新技術に対する監査への適応も視野に入れ、組織のガバナンス向上を支える専門家として活躍されています。



# 事例3：監査・ガバナンス専門家型A（⑪監査）

- 独学や研修での基礎固めを土台に、最先端のプロジェクトでの実践や経営層との対話を通じて、自身の専門領域にセキュリティの知識・スキルを段階的にプラスするアプローチが考えられます。

## キャリアシフト時に習得した主な知識・スキル

ポイント　業務や研修を通じ、一貫して監査に関する専門性を向上

※下線部の知識・スキルがポイントと関連

### レベル1～2

監査における専門性深化
（基礎習得）

| TKS | シフト時に新たに習得・拡大 |
|---|---|
| 知識 | • 監査プロセス<br>• 監査基準 |
| スキル | • 管理策の実施状況やプロセスを分析し、セキュリティ要件の適合性を判断 |

### レベル2～3-E

監査における専門性深化
（多様なセキュリティ監査経験）

| TKS | シフト時に新たに習得・拡大 |
|---|---|
| 知識 | • 監査における国際標準等やベストプラクティス<br>• クラウドサービスの種類と責任分界 |
| スキル | • 監査対象に対する個別の監査結果を踏まえ、セキュリティ要件への適合性を総合的に評価<br>• 国際標準等やベストプラクティスへの適合性を評価 |

### レベル3-E～4-E

監査における専門性深化
（意思決定の支援に資する専門性獲得）

| TKS | シフト時に新たに習得・拡大 |
|---|---|
| 知識 | • 監査報告書に関する知識 |
| スキル | • 関係者と適切なコミュニケーションを行う<br>• プロジェクトの進行状況を把握し、必要に応じて調整 |

## キャリア通じ重要な知識・スキル

**関係者とのコミュニケーションを通じ監査報告書を作成・共有するスキル**

- ソースコードの不具合を直すことではなく、発見された不備やリスクについて、ITの専門家ではない経理部長や取締役などの経営層に対し、「事実を正しく伝え、なぜ対処が必要か理解してもらい、改善に向けて動いてもらう」ための高度な説明・折衝力。

**監査における国際標準等やベストプラクティスへの適合性を評価するスキル**

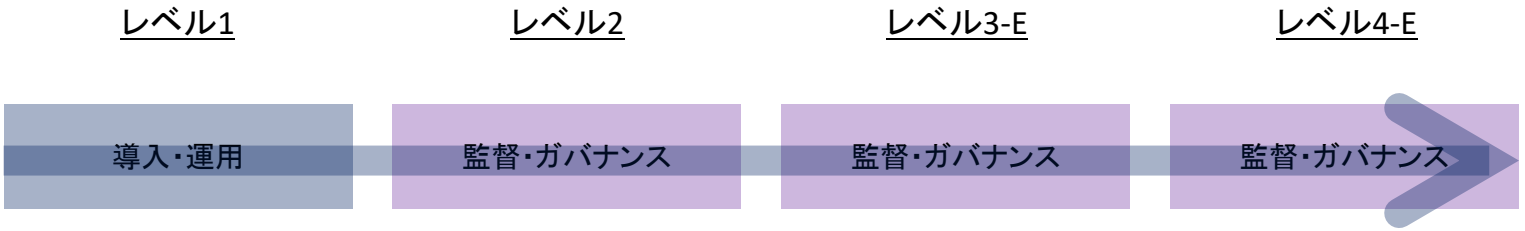
- 特定のシステム構成に留まらず、クラウド（ISMAP）やサプライチェーン、さらには昨今のAI利用リスクなど、次々と登場する新しい技術や制度に対し、監査・アセスメントの評価軸を適用し、都度学びながら評価を完遂する適応力。

**管理策の実施状況やプロセスを分析し、監査とその結果に基づく見直しを実施するスキル**

- 監査（保証）における「事実確認とギャップ分析（アセスメント）」のスキルを土台とし、そこで得た事実関係をもとに、内部監査の代行やセキュリティ評価支援といった形で、顧客の改善に向けたアドバイザリへと価値を拡張していく応用力。

# 事例4：監査・ガバナンス専門家型B（⑩法務）

- IT法務やCSIRT窓口を経て組織のガバナンス推進を統率し、「法務」の専門性をベースに技術と経営を繋ぐトランスレーターとして活躍していくキャリアパスです。




| | レベル1 | レベル2 | レベル3-E | レベル4-E |
|---|---|---|---|---|
| | 事務・総務業務、IT調達等を通じたビジネス・社会人基礎の習得 | IT法務、CSIRTの実務運用および調整窓口を経て、啓発活動など実務を通じた自律的な習得 | 社内全体のデジタルガバナンス推進、プライバシー保護の独力遂行・マネジメント | 経営・技術・法務のトランスレーターとしての意思決定、社会のルール形成に向けた研究・政策提言 |
| 知識・スキルの取得 | • ビジネスキャリア検定、ITパスポート等を取得し、ITと法務の基礎概念を学習<br>• 自らエンジニアの部署に身を置き、日常会話やトラブル対応を共に経験することで、彼らの用語や価値観のニュアンスを肌で学ぶ | • ISMS研修や個人情報保護監査人等を取得し、プライバシー保護とガバナンスの専門性を強化。ビジネスマネジャー検定でマネジメントの土台も構築<br>• 社外の専門家コミュニティに積極的に入り込み、他者事例や業界標準を吸収 | • 現場の実践経験を経営法学の観点から体系化し、修士（経営法）を取得。経験則に留まらない学術的知見を実務に還元し、本質的解決に導くアプローチを修得。<br>• セキュリティを信頼基盤と再定義し、制度やUI設計等による「信頼の可視化」を推進。 | |
| 役割(主) | 運用管理 | 法務 | 法務 | 法務 |
| 役割(副) | 対処 | 戦略推進・プロジェクト管理<br>対処 | 研究 | |

# 事例4：監査・ガバナンス専門家型B（⑩法務）

- 基礎資格の取得や社外コミュニティでの知見吸収、技術の現場に深く身を置き、実務に即した知見を得ることで、法務・ビジネスの専門性にセキュリティの実践知を融合させるアプローチが考えられます。

## キャリアシフト時に習得した主な知識・スキル

ポイント　法務としての専門性を軸に、知識・スキルを拡大

※下線部の知識・スキルがポイントと関連

レベル1～2

運用管理～法務へのシフト

| TKS | シフト時に新たに習得・拡大 |
|---|---|
| 知識 | • サイバーセキュリティ関連法規・組織内のポリシー・関連計画 |
| スキル | • 関係者と適切なコミュニケーションを行う<br>• 自組織における法的文書に関し、記載すべき項目やルールに則り作成 |

レベル2～3-E

法務における専門性深化
（多様なセキュリティ監督経験）

| TKS | シフト時に新たに習得・拡大 |
|---|---|
| 知識 | • コンプライアンス、プライバシーの原則と実践<br>• 法的リスクに対する分析・評価手法、プロセス |
| スキル | • 業界の自主規制等の要求事項を評価し、組織への影響を特定<br>• 法的リスク分析を行い、組織内の法的リスクを明らかにする |

レベル3-E～4-E

法務における専門性深化
（多様なセキュリティ監督経験）

| TKS | シフト時に新たに習得・拡大 |
|---|---|
| 知識 | • サイバーセキュリティに係る業界の指標や法律等の規制要件<br>• インシデント発生時における組織経営・運営上の意思決定 |
| スキル | • 専門家および非専門家に対して分かりやすく口頭で説明し、理解を促す<br>• インシデントの原因を分析し、方針や戦略に組み込む |

## キャリア通じ重要な知識・スキル

**法的リスク分析の評価結果を経営層等へ分かりやすく説明するスキル**

- 非エンジニアリング領域からの参入であることを逆手に取り、高度な技術用語や複雑な法規制をビジネス言語に翻訳し、経営層や現場双方の納得感を引き出して意思決定を円滑にする力。

**サイバーセキュリティに関する関係者と適切なコミュニケーションを行うスキル**

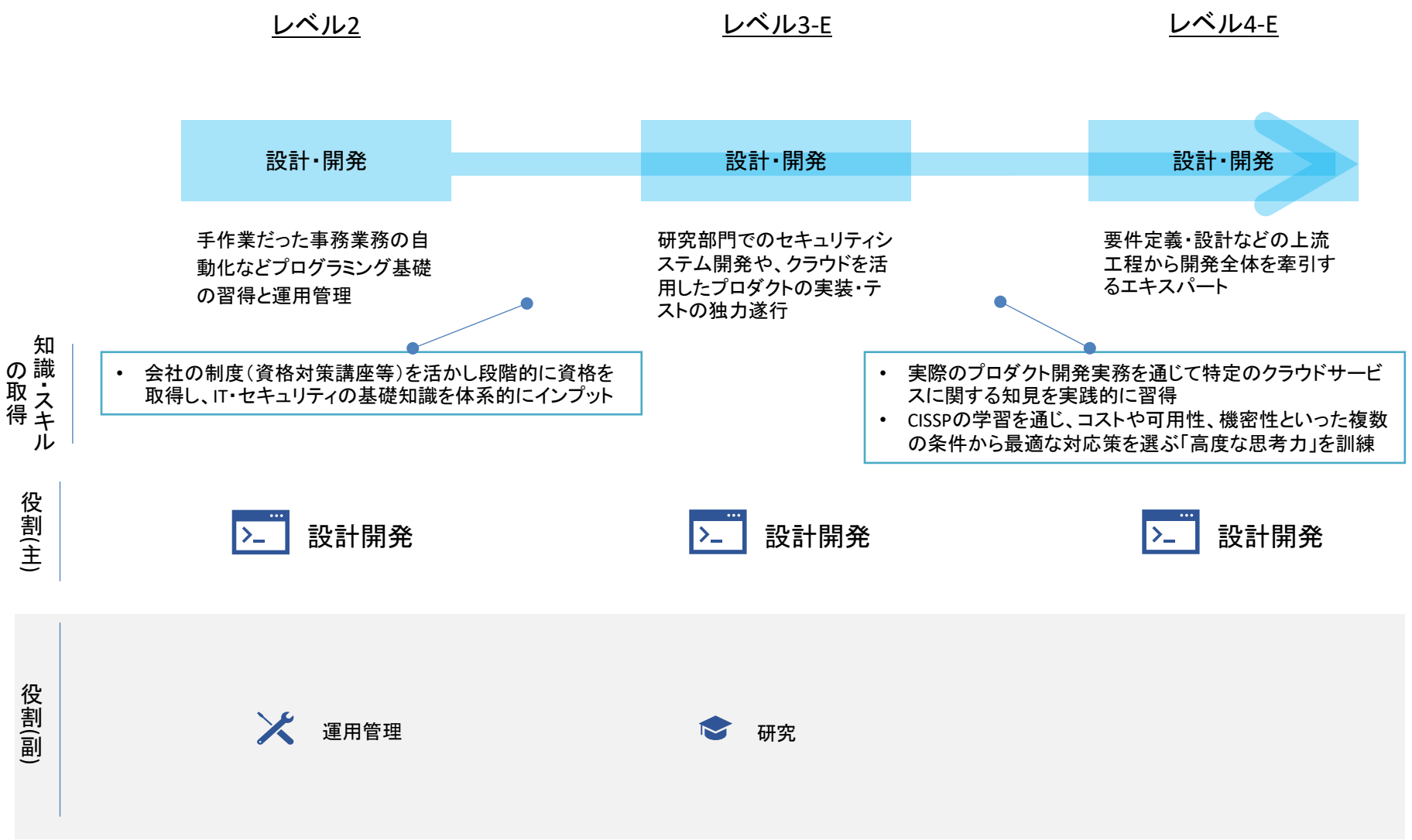
- 上流工程での理想的な企画立案に留まらず、エンジニアと協働し、現場の専門性や背景を深く理解することで、「ルールを押し付ける法務」ではなく「ビジネスを共に前進させるパートナー」として機能する対人スキル。

**コンプライアンスの原則を実践し、サイバーセキュリティに関する戦略、方針、規定等を策定するスキル**

- セキュリティやプライバシー対応を単なるコストや制約と捉えず、顧客からのデジタルトラストを獲得するための源泉と位置づけ、企業競争力を高めるための制度や枠組みを実装する力。

# 事例5：技術領域のエキスパート深化型A（⑫設計開発）

- 事務職（マクロ開発）からスタートし、独学と実務でプログラミングやインフラ技術を習得して、自社セキュリティプロダクトの設計・開発を牽引するスペシャリストへと深化しようとされています。



# 事例5：技術領域のエキスパート深化型A（⑫設計開発）

- 分からないことを放置せずに自己学習を怠らないことで、事務業務でのマクロ開発を皮切りに、独学と実務で技術を習得することが重要と考えられます。

## キャリアシフト時に習得した主な知識・スキル

ポイント　レベル3以降の特定クラウドサービスに関する専門性の深化

※下線部の知識・スキルがポイントと関連

レベル2～3-E

設計開発における専門性深化
（開発実務、研究活動を実施）

| TKS | シフト時に新たに習得・拡大 |
|---|---|
| 知識 | • コーディング、統合、内部デプロイ等実装に関する知識<br>• サイバーセキュリティの基本原則と実践に関する知識 |
| スキル | • 新たなプログラムを作成、又は既成品を選定し、システムに実装するスキル |

レベル3-E～4-E

設計開発における専門性深化
（特定技術に関する専門性や資格の習得）

| TKS | シフト時に新たに習得・拡大 |
|---|---|
| 知識 | • クラウドサービスの種類と責任分界に関する知識<br>• 組織の抱えるシステム上におけるサイバーセキュリティの課題に関する知識 |
| スキル | • 新たなプログラムを作成、又は既成品を選定し、システムに実装するスキル<br>• 実装する機能を現場との調整の上段階的に実装するスキル |

## キャリア通じ重要な知識・スキル

**未経験から技術を吸収する「地道な自己学習」スキル**

- 分からないことを放置せず自らリスト化して調査・学習する姿勢。これがプログラミング技術やクラウド技術の習得など、全フェーズでの技術的成長を支える強力なエンジンとなっている。

**有識者からの「ヒアリング・吸収力」とコミュニケーション**

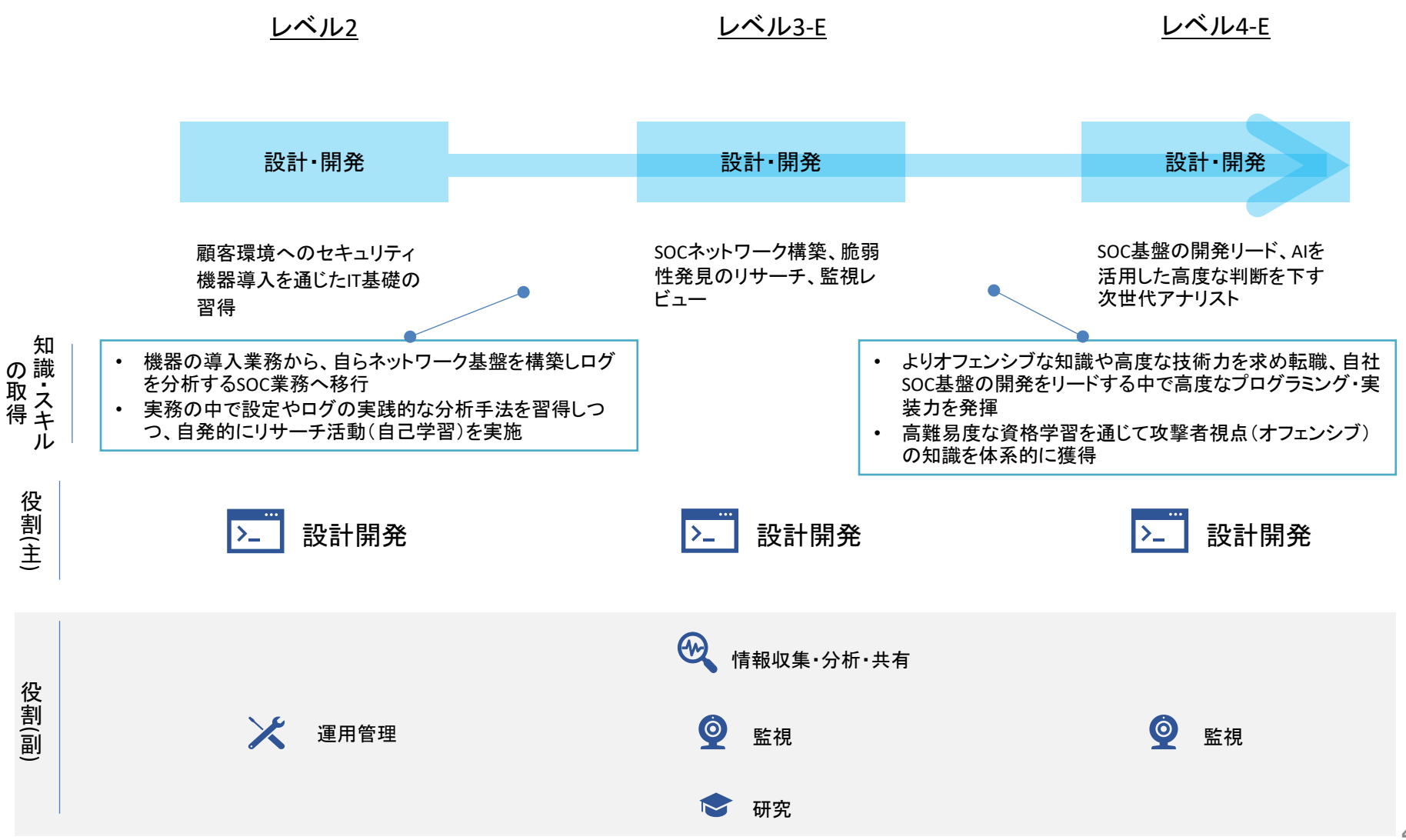
- 社内に多くいるスペシャリストとの日々の会話を通じて自然に知識を吸収するように心がける。
- 社内システムの開発においては他部署メンバーからのフィードバック（「便利」「使いやすい」等）を直接受け取り、モチベーションとシステム品質を向上に活かす。

**状況に応じた「ロジカルな思考・最適解の選択」スキル**

- CISSPの学習等を通じて培った、複数の制約条件の中から最適なアプローチを論理的に導き出す思考力であり、今後、実装担当から上流工程（設計・要件定義）をリードする立場を目指す上で、最も核となるスキルとして機能することが期待。

# 事例6：技術領域のエキスパート深化型B（⑫設計開発）

- セキュリティ機器の運用やSOC監視から、自発的な脆弱性リサーチや自社SIEM基盤の開発へと技術を深掘りしていく、高度な監視・設計開発の専門家としてのキャリアを歩まれています。



# 事例6：技術領域のエキスパート深化型B（⑫設計開発）

- AIとの共存、コミュニティ活動への積極的参加等、飽くなき技術探究心を大切にすることが、脆弱性に関する検証や自社SIEM基盤の開発といった技術を深掘りするキャリアパスの一助となっています。

## キャリアシフト時に習得した主な知識・スキル

ポイント　実務経験および自己学習を通じSOC基盤開発をリードできる技術者へ

※下線部の知識・スキルがポイントと関連

レベル2～3-E

設計開発における専門性深化
（ログ分析の実務の経験蓄積）

| TKS | シフト時に新たに習得・拡大 |
|---|---|
| 知識 | • セキュリティログ（システムログ、アプリケーションログ等）に関する知識<br>• サイバー攻撃やサイバーセキュリティの脅威/脆弱性に関する知識 |
| スキル | • 分析ツールを使用してログ分析を実施するスキル<br>• ツールの設定値を監視対象や目的に応じた設定にするスキル |

レベル3-E～4-E

設計開発における専門性深化
（資格学習等も通じた専門性高度化）

| TKS | シフト時に新たに習得・拡大 |
|---|---|
| 知識 | • コーディング、統合、内部デプロイ等実装に関する知識 |
| スキル | • 新たなプログラムを作成、又は既成品を選定し、システムに実装するスキル<br>• 脆弱性評価/ペネトレーションテストツールの特性を理解し、取扱うスキル |

## キャリア通じ重要な知識・スキル

**与えられた仕事の枠を超えて技術を探求する「自走力・リサーチ力」**

- 会社の業務や指示されたことだけをこなすのではなく、自発的にリサーチプロジェクトを立ち上げたり、未知の技術を自分で調べて検証したりする姿勢を重視している。

**外部知見を吸収する「コミュニティ活用」スキル**

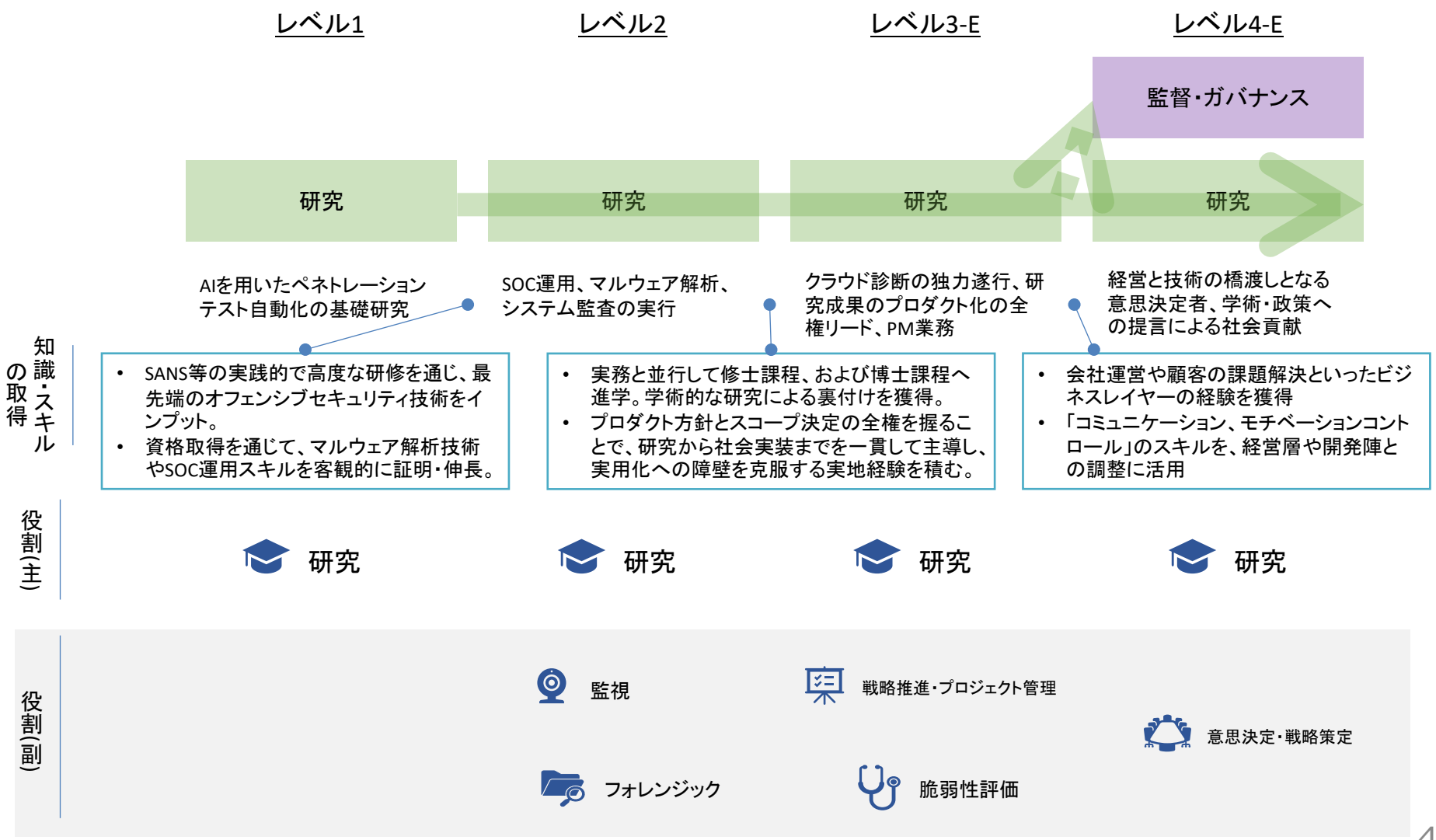
- 社内にとどまらず、勉強会コミュニティに定期的に参加し、他社や他業界のアンテナが高いエンジニアと情報交換を行うことで、最新の脅威動向や技術トレンドをキャッチアップしている。

**AI時代を見据えた「AIとの共存・活用」スキル**

- AIがログの一次分析やサマライズを行う時代において、AIの出力を鵜呑みにせず、技術的根拠に基づいて人間が最終的な高度判断を下すスキルを重視している。

# 事例7：アカデミアからのエキスパート社会実装型A（⑬研究）

- 基礎研究からキャリアをスタートし、組織での実務を経て研究成果のプロダクト化を主導した後、経営と技術の橋渡しとして顧客課題の解決を牽引していくキャリアパスです。



# 事例7：アカデミアからのエキスパート社会実装型A（⑬研究）

- 実務に直結する専門技術のインプットと学術的な探求を並行させながら、事業収益やリソースを意識したビジネス現場での折衝経験を重ね、多角的な視点を獲得するアプローチが考えられます。

## キャリアシフト時に習得した主な知識・スキル

ポイント　研究成果のプロダクト化・社会実装に向けた、実装力・推進力の獲得

※下線部の知識・スキルがポイントと関連

### レベル1～2

研究を通じた専門性深化
（資格取得を通じた伸長）

| TKS | シフト時に新たに習得・拡大 |
|---|---|
| 知識 | • サイバー攻撃やサイバーセキュリティの脅威/脆弱性に関する知識 |
| スキル | • 機器で行われた操作等を評価し、サイバー攻撃や不正行為を特定するスキル |

### レベル2～3-E

研究を通じた専門性深化
（監視・フォレンジックの実務を通じた伸長）

| TKS | シフト時に新たに習得・拡大 |
|---|---|
| 知識 | • 研究計画書に含めるべき項目<br>• サイバーセキュリティの研究領域における情報源 |
| スキル | • 立案した仮説を調査に基づいた実験などを通し、検証<br>• 脅威シナリオを元に脆弱性評価/ペネトレーションテストを行い、脆弱性の有無を明らかにする |

### レベル3-E～4-E

研究を通じた専門性深化
（研究成果を社会へ還元）

| TKS | シフト時に新たに習得・拡大 |
|---|---|
| 知識 | • コーディング、統合、内部デプロイ等実装<br>• プロジェクト管理ツールの使用 |
| スキル | • 基本、詳細設計書で定められている要求を満たす機能を備えた新たなプログラムを作成、又は既成品を選定し、システムに実装<br>• プロジェクトの進行状況を把握し、必要に応じて調整 |

## キャリア通じ重要な知識・スキル

**意思決定・戦略策定を支援する情報把握に資するスキル**

- 高度な技術の深化に留まらず、その技術が持つ意味を抽象化し、経営層や政策決定者などの非専門家に対して「ビジネスや社会にとっての価値」として翻訳・提案し、意思決定に繋げる力を身に付ける。

**プロジェクトの進行状況を把握・調整し、開発・実装を主導するスキル**

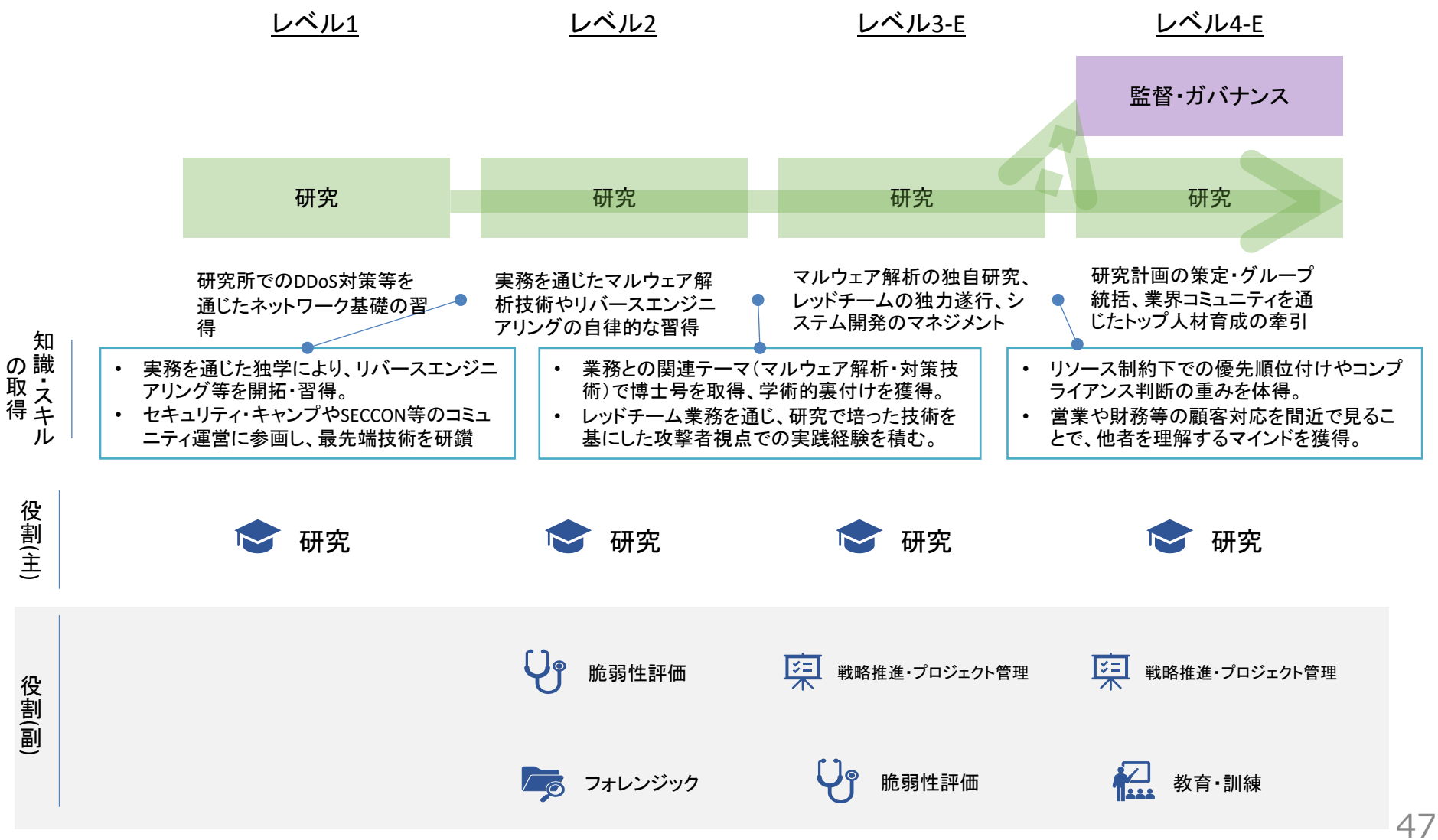
- 学術的な研究成果を論文で終わらせず、自らがプロダクト方針やスコープ決定の全権を握ることで、実装から社会実装までの接続（死の谷の克服）を一気通貫で主導・管理する推進力を習得する。

**ペネトレーションテスト等の実践と、研究結果に基づく新方式の提案の並行推進**

- 座学だけでなく研修などのハンズオンを通じた実践的な実地経験をベースにしつつ、修士・博士課程への進学や政府委員会等を通じて学術的裏付けとマクロな提言力を獲得している。

# 事例8：アカデミアからのエキスパート社会実装型B（⑬研究）

- セキュリティ技術の研究開発から出発し、現場での実践やコミュニティ活動、事業部門でのマネジメントを経て、高い専門性とビジネス視点を併せ持つ研究者として活躍されています。



# 事例8：アカデミアからのエキスパート社会実装型B（⑬研究）

- 研修や資格取得を通じた高度な実務技術の習得と、大学院での学術的な裏付けを両立させつつ、プロダクト開発や組織運営の実地経験を積むことでギャップを解消してこられています。

## キャリアシフト時に習得した主な知識・スキル

ポイント　研究成果のビジネス化・予算獲得により注力

※下線部の知識・スキルがポイントと関連

### レベル1～2

研究を通じた専門性深化
（マルウェア解析等実務を経験）

| TKS | シフト時に新たに習得・拡大 |
|---|---|
| 知識 | • セキュリティログ（システムログ、アプリケーションログ等）に関する知識<br>• 監査プロセスに関する知識 |
| スキル | • 情報システムの監視において検知ツールを使用して異常を検知するスキル |

### レベル2～3-E

研究を通じた専門性深化
（研究と実装の実務を経験）

| TKS | シフト時に新たに習得・拡大 |
|---|---|
| 知識 | • ペネトレーションテストツール及び手法に関する知識<br>• 脆弱性の一般的な評価基準 |
| スキル | • 脆弱性評価特性を理解し、取扱う<br>• 組織のサイバーセキュリティ環境・目的にあった脅威シナリオを元にテストを行い、脆弱性の有無を明らかにする |

### レベル3-E～4-E

研究を通じた専門性深化
（学会やコミュニティ活動等の活動注力）

| TKS | シフト時に新たに習得・拡大 |
|---|---|
| 知識 | • 経営・組織運営、自組織の戦略<br>• サイバーセキュリティに係る予算管理とコスト評価 |
| スキル | • 法的事項や技術的事項を、専門家および非専門家に対して分かりやすく口頭で説明し、理解を促す<br>• 社内外のステークホルダーの意向及び能力を評価 |

## キャリア通じ重要な知識・スキル

**技術的事項を非専門家に対して分かりやすく口頭で説明し、予算計画の立案・調達に繋げるスキル**

- 高度な研究成果を技術領域に留めず、文系中心の経営層や営業、財務といった非専門家に対して「どのような価値やビジネスインパクトがあるか」を相手の立場を想像して分かりやすく翻訳し、研究予算の獲得やビジネス化に繋げる力を身に付ける。

**研究テーマ・目的を決定し、脅威に関する知見に基づき仮説を検証するスキル**

- 学生時代の「遊び感覚（仕組みへの知的好奇心）」から出発した技術探求を、レッドチーム業務等で得たリアルな現場の脅威感と結びつけ、社会の被害を抑えるための「実効的な対策技術の研究開発」へと昇華させる力を身に付ける。

**学会やコミュニティ活動への参加と、サイバーセキュリティに関する啓発・教育の実施**

- セキュリティ・キャンプやコミュニティに身を投じ、トップエンジニア同士で最新手法を磨き合うと同時に、社会全体の人材不足解消を自らの使命と捉え、日本のトップ人材育成を牽引する高い視座と影響力を習得。

©National Cybersecurity Office. 