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

―― 教育機関向け ――

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、教育機関における活用シーン・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、各教育機関におけるカリキュラムや授業の設計等を一律に義務づけるものではありません（各教育機関においては、本手引き書の内容を参考としつつ、教育目的や学生の層など、それぞれの特性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、サイバーセキュリティ人材の育成に関わる教育関係者を主な利用者として想定します。
- 特に、学生に対してサイバーセキュリティに関する教育を実施する教育機関（大学、高等専門学校、専門学校等）の教職員のほか、教育サービスを提供する教育事業者等において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（教育機関向け）」（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

教育機関向け事項

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

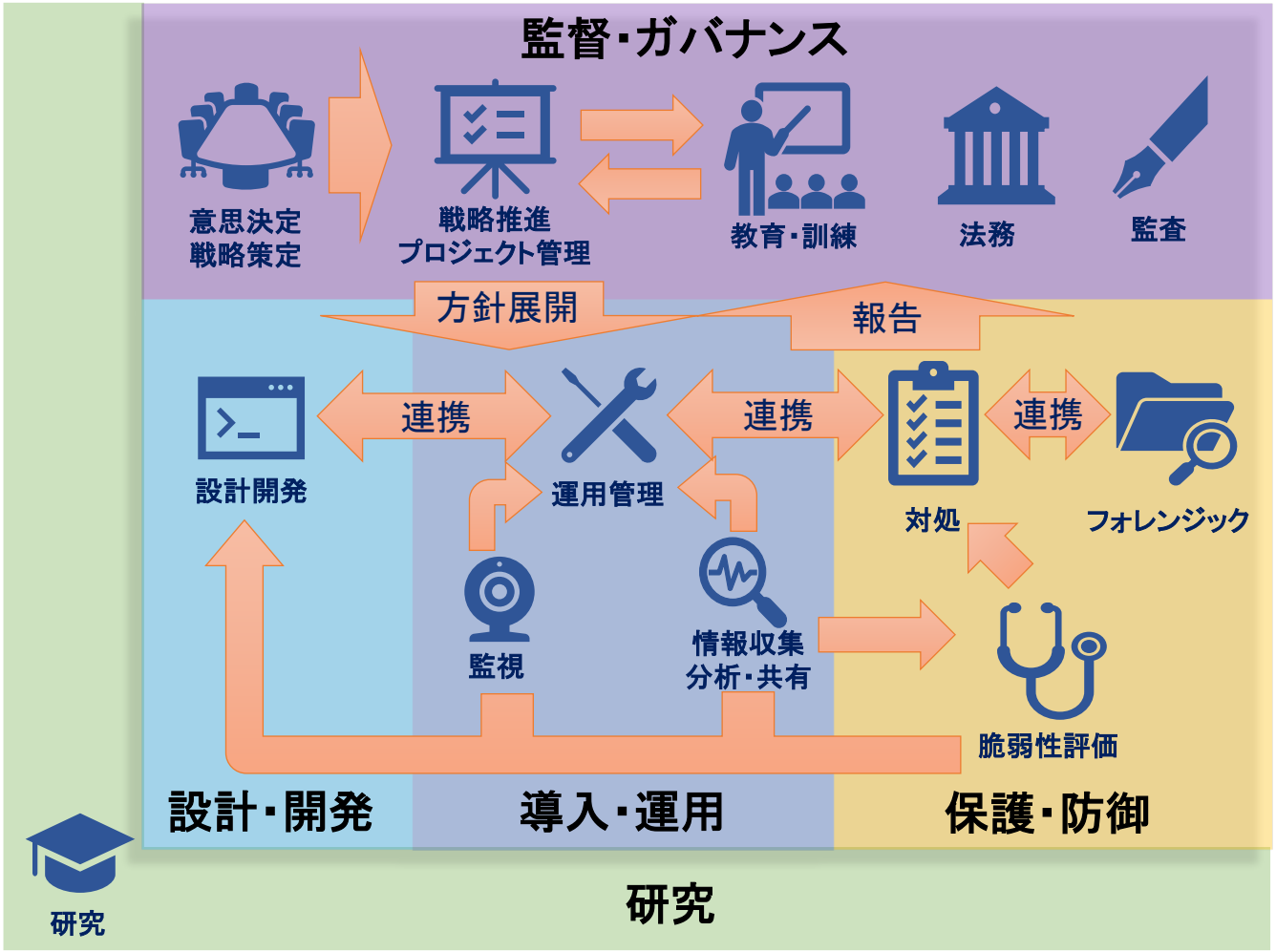
企業等　組織に必要な人材像を明確化し、採用・配置・育成等を計画的に進められる

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 ➢ 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 ➢ NICEフレームワークにおける対応ロール ➢ 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 ➢ 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 ➢ レベル：ITSSを参照した4段階のレベルを定義 ➢ 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)

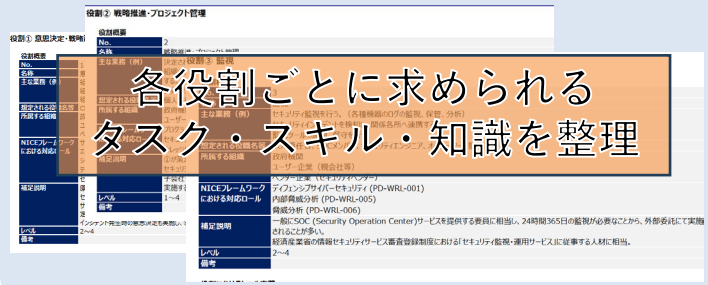
■TKSの考え方

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。 ● 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。 ● 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。 ● 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

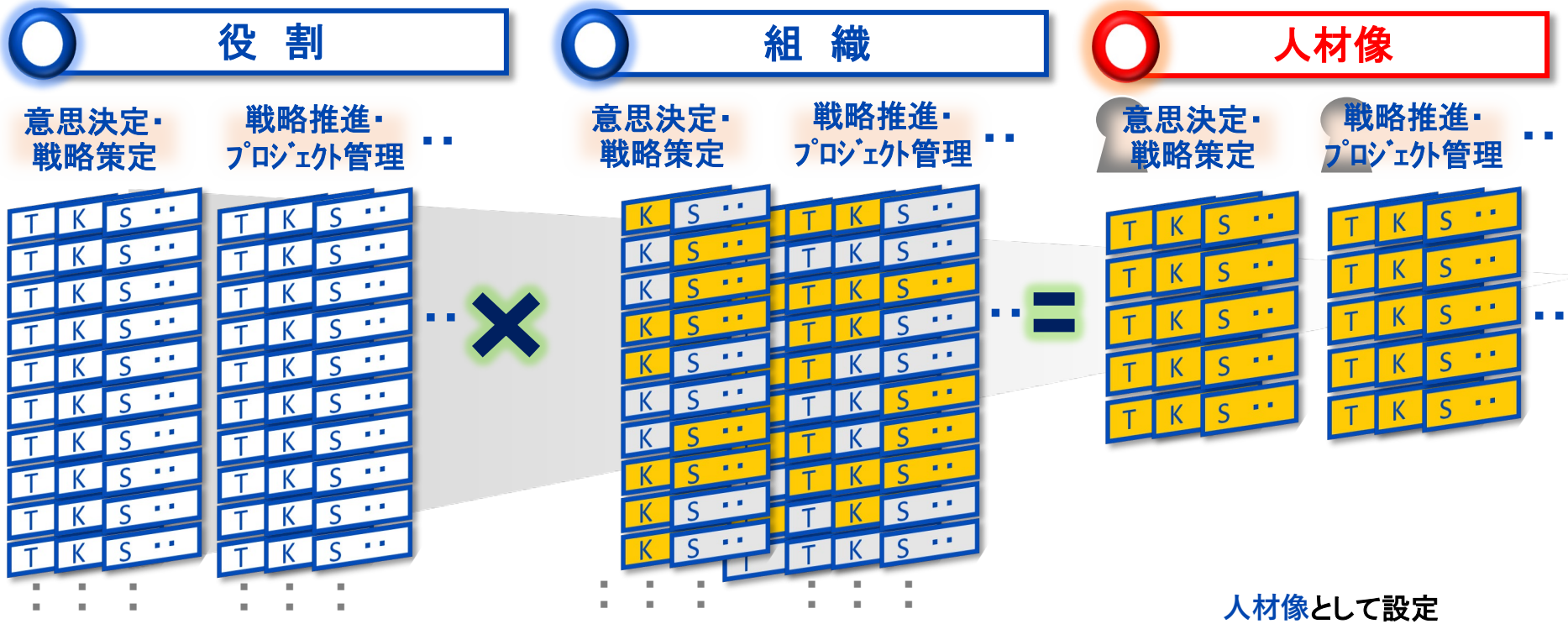
- 手引き書は各対象ごとに「主たる読者の属性」を想定し作成をしているものですが、主たる読者ではない属性の方も参考にしていただけるよう作成しておりますので、以下の対応表を参考にご利用ください。

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	―	―	◎ (人事担当者含む)	○	△	△	△
教育機関向け	△	―	△	―	―	◎ (教育事業者含む)	○
個人 (専門人材)	△	△	△	◎ (セキュリティ担当者)	○	―	○ (セキュリティ分野志望者)
個人 (プラス・セキュリティ)	△	◎	△	◎ (バックオフィス、品質管理者等)	○	―	○ (学部の専門性を問わない)

【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） デジタル経営（CIO/CDO） 企業経営（取締役） 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 セキュリティ統括	CISO、CRO、CIO等 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 デジタルシステムストラテジー 経営リスクマネジメント 事業ドメイン（生産現場・事業所管理）	セキュリティ統括 プロジェクト管理 社内外調整	サイバーセキュリティ統括 ISMS担当 個人情報取扱責任者/担当 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 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 情報システムペンテスター IoTデバイス脆弱性診断士 IoTシステムペンテスター 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 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 監視・運用	システム管理者、ネットワーク管理者 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 デジタルプロダクト開発	セキュリティ設計 開発	セキュリティ設計担当 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 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			

教 育 機 関 向 け 事 項

教育機関向け手引き書2026の全体構成

- 企業と教育機関の間にある「求める人材像」の認識ギャップ（言葉の壁）を解消するため、人材フレームワークを共通言語として活用します。本手引き書では、フレームワークの「役割」等を共通言語として明確化したニーズをもとに、具体的な学習項目へと落とし込み、カリキュラムへ反映させるためのステップを解説します。

現状の課題

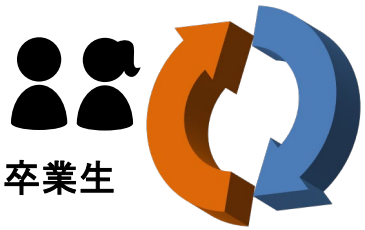
企業のニーズ

（例）
- 現場でログを見て判断できる人材が欲しい
- インシデント発生時に初動対応できる即戦力が欲しい
- クラウドセキュリティが分かる人材が欲しい
- 地場の製造業のセキュリティの運用ができる人材が欲しい

教育カリキュラム設計者

- ニーズやトレンドの情報を断片的に得ることはできるが、粒度がまちまちであったり、共通的な指標がないため、カリキュラム設計が難しい
- より正確に社会のニーズを把握するために共通言語となる仕組みが必要

フレームワークを用いた産学の対話



STEP1
【企業からの「役割」等を用いたニーズの明確化】
人材フレームワークの13の役割を用いて、企業が求める人材像を明確化

STEP2
【知識・スキルの特定】
- 知識の例：サイバー攻撃手法、クラウド基盤知識
- スキルの例：SIEMツールの操作、ログからの予兆検知

教育機関の実践

①特定した知識・スキルをもとに、現状のシラバスとのギャップを分析
知識の例：最新の攻撃トレンド」「クラウド固有の仕様」「業界特有のコンプライアンス」
スキルのギャップの例：「ツール操作」「ログ分析の実践」「インシデント時の判断（トリアージ）」

②特定したギャップをもとにセキュリティ教育を充足させる対策を検討
対策の例：既存科目の内容アップデート、演習科目の新設、インターンシップ、外部演習プログラム（分野別実践演習の開発・実施基盤「CYROP」等）の活用。

セキュリティ人材に関する社会のニーズ

学生時代にセキュリティを学習する意義

ポイント　社会においてセキュリティは不可欠な素養となっています

- 情報技術の発展や我が国の安全保障を取り巻く情勢より、セキュリティの重要性は年々高まっています。
- セキュリティはもはや他人事ではなく個人のリテラシー向上が不可欠であり、企業も、将来社員となる学生に最低限の素養を求めています。
- サイバーセキュリティの日本全体の基礎力向上及び専門人材の育成のために、教育機関の重要性は高まっています。

セキュリティの重要性の高まり

Political

- 社会のデジタル化に伴い、サイバー空間の安全確保が社会機能の維持に直結
- 個人情報保護やデータプライバシーに関する法規制が世界的に厳格化

Economic

- 中小企業や関連会社を踏み台にするサプライチェーン攻撃が多発
- セキュリティ人材の採用コストや維持コストが上昇

Social

- 消費者のデータプライバシーに対する意識が高まっている
- 人の心理的な隙や行動のミスにつけ込む攻撃（フィッシング詐欺やビジネスメール詐欺）が巧妙化

Technological

- 生成AIの普及により、攻撃者はより自然なフィッシングメールの作成等が容易に。
- 工場設備（OT）、医療機器、家電、自動車など、あらゆるものがネットにつながり、サイバー攻撃の対象が拡大

教育機関でセキュリティを学ぶ有効性

- 学生時代からセキュリティに触れる機会を増やすことで、セキュリティに関連する職業へのキャリアを提示し、社会全体のセキュリティ対応力の底上げにつなげる。

- どのような職種であれ、企業のPCやデータを扱う以上、セキュリティ知識は必須スキル。
- 悪意がなくても、知識不足による設定ミスや情報持ち出しが、企業に億単位の損害を与える可能性がある。

- セキュリティの脅威が高まる中で、身近な脅威から自分自身を守るスキルが不可欠となっている。
- 「AIに情報を入力する際のリスク」など、新しい技術を安全に使いこなすリテラシーを早期に身につける必要がある。

セキュリティの多様な活躍の場とその魅力

- セキュリティの仕事は技術職だけに留まりません。法律、経営、教育、監査など、文系・理系を問わず多様なバックグラウンドが活きる13の役割が存在します。もちろん、高度な技術力を活かした活躍のパスもあります。
- 現在の専攻や興味が出発点となり、多様な専門家へと成長できるキャリアの例を提示します。

出発点	将来的な活躍の例	魅力
文系・社会科学系 **（法学、経営学、経済学、教育学 など）** 文系専攻等の出身の方にも多様な活躍の場があります	 ルール作りや監査からスタートし、現場の専門家と経営層を繋ぐプロジェクトマネージャー（PM）を経て、ゆくゆくは企業の経営方針に直接関わるCISO（最高情報セキュリティ責任者）等へと成長するケースがあります。	専門用語を経営層等に分かりやすく翻訳する橋渡しとして、技術とビジネスの境界を埋める重要な役割を担います。実務の現場からは、「若手のうちから経営層に直接事業のリスクを説明し、改善を促す機会がある」「ルールをただ押し付けるのではなく、関係者を巻き込みながら組織を強化していく過程に大きなやりがいを感じる」といった声が聞かれます。
理系・情報系 **（情報工学、計算機科学、データサイエンス など）** 技術を極めるパスはもちろん、経営に活かすパスもあります	 社会のデジタル基盤の安全を根底から支えるプロダクトアーキテクトや、サイバー犯罪の証拠を解析するフォレンジック等の専門家として道を切り拓くほか、技術の価値を抽象化して政策や経営に活かせる専門家を目指すことも可能です。	社会のITインフラを安全に作り上げるほか、システムの弱点を見つけ出す「ペネトレーションテスター」や、未知の脅威を解明する「研究者」として活躍します。実務の現場からは、「緊張感と達成感がある」「ゲームの裏技や手品を見つけたようなワクワク感がある」と語られ、最先端の技術を社会実装していく知的好奇心が満たされる仕事です。
理系・その他 **（機械工学、電子工学、数理科学 など）** 最新技術を使いこなす、社会や組織のキーパーソンになれます	 組織をサイバー攻撃から守る実務経験を積み、複数の領域を横断的に理解してAI等の最新技術を使いこなす「ジェネラリスト」や、現場を指揮するリーダーへとステップアップするケースがあります。	企業や組織のネットワークを日々「監視・運用管理」し、異常を検知する「SOC」や、いざという時に被害を最小限に食い止める初動対応を行う「CSIRT」等があります。実務の現場からは、「トラブルを鎮静化した際に他部署から深く感謝される」という声や、「『サイバー空間』で自社や社会の基盤を守る最前線のやりがいがある」といった声が上がっています。

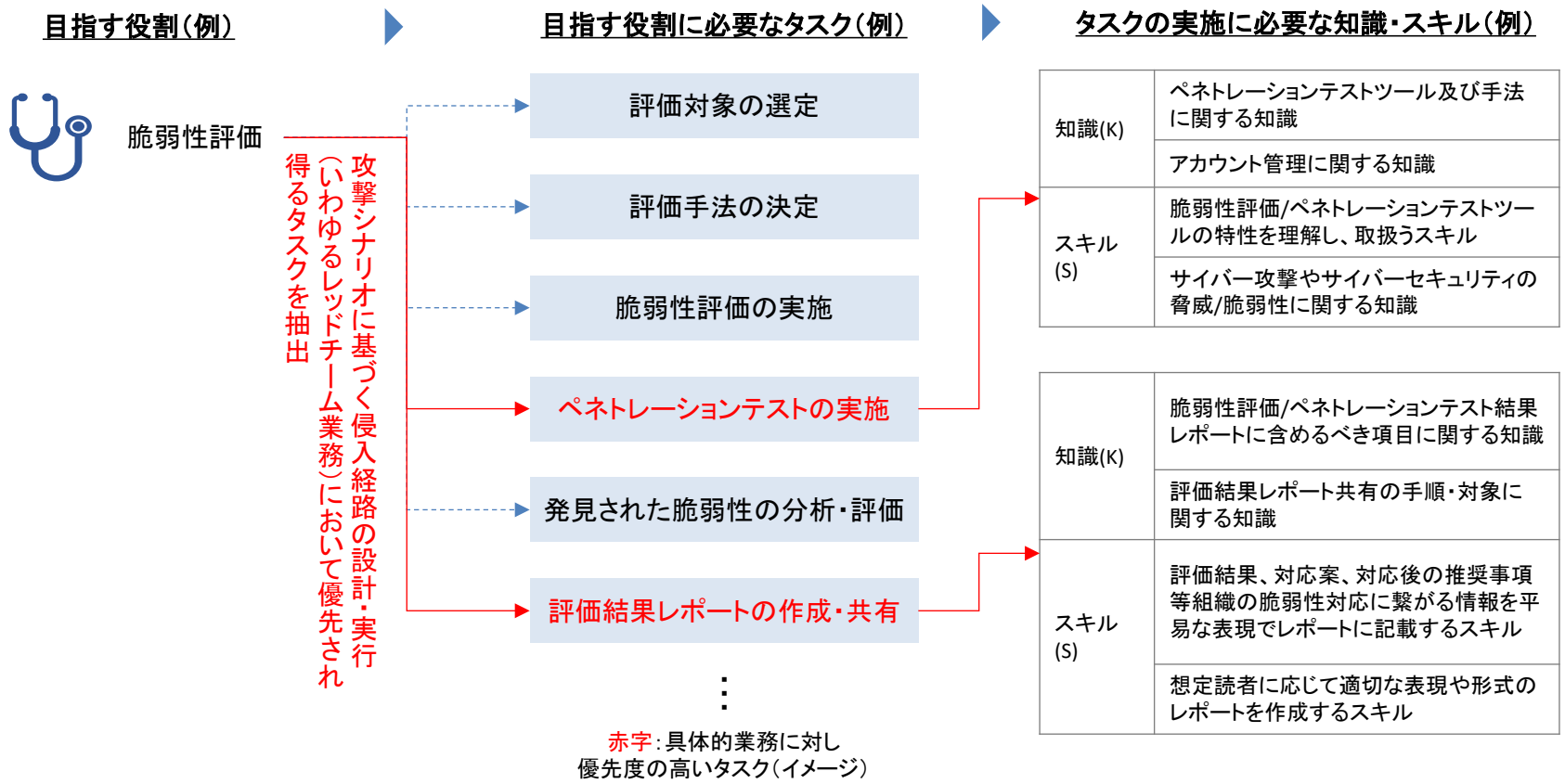
セキュリティ人材に関する社会のニーズ

- 企業からの「○○ができる人材が欲しい」というニーズは、多くの場合「タスク」に基づいています。産学の対話において、企業側からフレームワークの「役割」や「タスク」を用いて人材ニーズが提示されることを前提に、教育機関はそれらをもとに「教育すべき知識・スキル(KS)」へ逆引きするアプローチが有効です。

教育機関の得意領域	企業の実務のニーズに即した教育	マネジメント系の教育	セキュリティ専門人材・情報系人材の教育
	例 製造業の多い地域の高専	例 法学部や経営学部を有する文系大学等	例 就職率向上を目指す情報系専門学校・大学等
社会のニーズの把握	**製造業企業と対話** • 制御システム(OT)のことがわかる人材が欲しい • セキュリティ対策を求められているが、現場で対応できる人がいない 等	**企業の管理部門と対話** • 個人情報保護法やGDPRなどの法規制対応が急務 • セキュリティポリシーの策定、従業員への教育を企画できる人材が欲しい等	**SIerの求人の把握** • プラス・セキュリティの素養を持つ人材が欲しい • 即戦力として、ログを見てインシデントの予兆に気づける人材が欲しい 等
	フレームワークを活用し、企業のニーズに基づき役割とタスクを明確化		
自校で育成するターゲットの検討	**安定稼働を守るOTセキュリティ現場担当者** 役割:⑧運用管理、④対処 タスク(T):OTシステムの維持管理を行う、異常発生時にエスカレーションなどの初動対応を行う	**法的知見と調整力で組織を支える人材** 役割:⑩法務、⑨教育・訓練 タスク(T):コンプライアンス、契約管理、社内ルールの策定・推進	**インシデントに対応できるシステムエンジニア** 役割:⑧運用管理、③監視、④対処 タスク(T):クラウド領域での設計・設定・維持、SOCやインシデント対応の初動
	フレームワークを活用し、特定したタスク(T)から必要な知識・スキルを逆引き		
自校が育成する人材の定義	**知識** • 制御システムの知識 • OTセキュリティの概要	• サイバーセキュリティの法規 • リスクマネジメントの理論	• クラウドサービスの知識 • ネットワークの理解
	スキル • ネットワークのトラブル解決 • インシデント時のエスカレーション	• 契約書の読解・作成スキル • 関係部署やベンダーとのコミュニケーションスキル	• ログ分析スキル • クラウド環境でのセキュリティ設定
	レベル • 現場で手順書に従って確実に対応できるレベル2相当。	• 専門用語を理解し、専門家(エンジニア・弁護士)と橋渡しができるレベル2～3相当	• 実務において指示を受けながら作業を完遂できるレベル2以上

【参考】フレームワークを用いたタスク・知識・スキルの絞り込み方法の補足

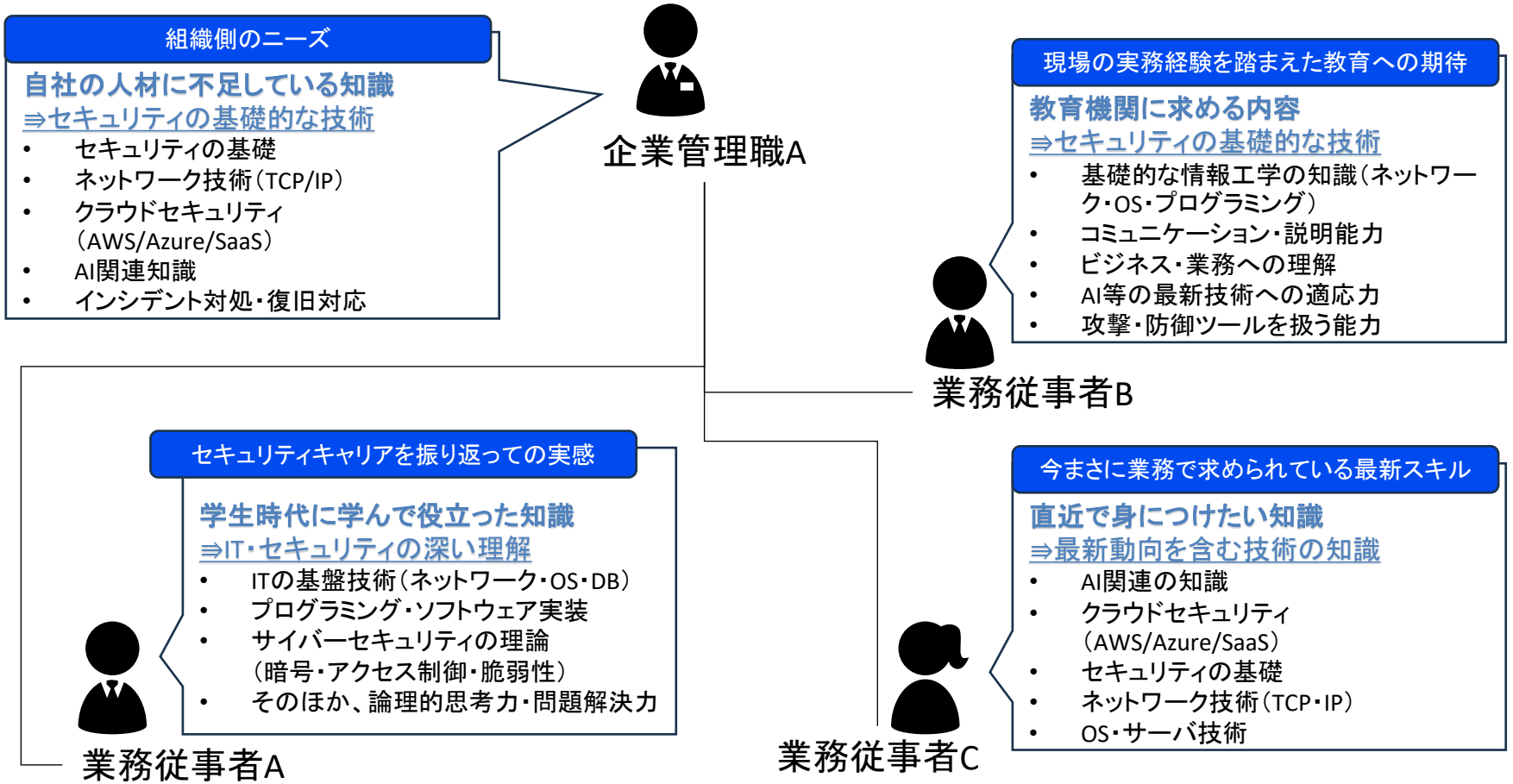
- 選定した役割から、フレームワークを活用したタスクの特定及び特定されたタスクに紐づく知識・スキルの抽出が可能です。
- 例えば、脆弱性評価という役割には、「攻撃シナリオに基づく侵入経路の設計・実行（レッドチーム）」「網羅的に脆弱性を確認」といった具体的業務が複数含まれています。
- 具体的業務を遂行する上で優先度の高いタスクを、フレームワークを用い抽出することで、それらのタスクを遂行するために必要な知識・スキルを整理しやすくなります。



社会に出てから役立つ実感のある知識・スキル

- 企業や業務従事者へのアンケートから、社会に出て実際に求められ、役立つと感じられている知識・スキルの傾向が明らかになっています。
- 特定の専門分野だけでなく、セキュリティやITの基盤技術から、最新動向への適応力、ビジネスへの理解まで、幅広い知識のニーズが高まっています。

13の役割に汎用的に必要な知識・スキルが求められています



※企業管理職・業務従事者向けのアンケートをもとに作成

カリキュラムを作るための考え方

カリキュラムを作るための考え方

- 社会のニーズに応えるカリキュラム設計の4ステップを提示します。
- 育成したい「役割」と必要な「知識・スキル(KS)」を特定し、既存の講義内容とのギャップを可視化することで、新規科目の検討や外部連携の必要性を判断できます。

STEP1 自校が育成したい人材をフレームワークの「役割」から選択※

STEP2 選んだ役割に必要な「知識・スキル」をフレームワークからリストアップ※

STEP3 既存の講義内容とKSのギャップを特定

STEP4 不足しているKSを特定し、新規科目や外部連携の必要性を判断

Sample Case

ガバナンス人材

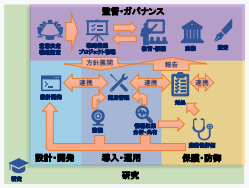
①意思決定 戦略策定 ②戦略推進 プロジェクト管理 ⑪監査

情報系の専門家

⑫設計開発 ⑦フォレンジック ④対処

リテラシーを持つ人材

全役割の前提



役割② 戦略推進・プロジェクト管理

K(知識)

プロジェクト資金の調達方法に関する知識
調達先のリスクの特定、評価に関する知識
サプライチェーンの構造と運用に関する知識
調達する機器の選定基準とその評価に関する知識
調達時に遵守すべき法令や規制に関する知識
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
サイバーセキュリティ上のリスク管理の原則と実務に関する知識
プロジェクト管理ツールの使用に関する知識
プロジェクトスコープや計画の変更に関する知識
組織が提供するサービスのリスクやパフォーマンス管理に関する知識
プロジェクトに必要な職務要件とスキルセットに関する知識
チームビルディング活動の実施に関する知識
メンバーのモチベーションエンゲージメントを高める方法に関する知識
最終成果物や報告書の作成に関する知識
プロジェクト評価とレビューに関する知識
プロジェクトに係る文書の整理とアーカイブに関する知識
次ステップの計画の立案に関する知識
インシデント対処に関する知識
外部AIサービスを利用する場合の情報[illegible]に関する知識
AIが生成した情報の取り扱いにおいて[illegible]すべき事項に関する知識
セキュリティ対策目的でAIを利用する[illegible]遵守すべき事項に関する知識

S(スキル)

通常時及びインシデント発生時の運用[illegible]ルを策定するスキル
組織目標や戦略を分析し、プロジ[illegible]を立案するスキル
サプライヤー評価と選定基準を調達プ[illegible]用するスキル
プロジェクトにおいて発生した契約事項[illegible]スキル
調達先のリスクを分析し、判断するスキ[illegible]
組織のサイバーセキュリティ水準を満た[illegible]の要件を決定するスキル
法律や規制の要求事項を調達プロセスに[illegible]ル
遵守すべき法令やプライバシー上の要求事[illegible]に適用させるスキル
プロジェクトで活用している技術の性能を監視[illegible]
プロジェクトにおける各業務が組織の求めるセキ[illegible]会しているか監視、分析するスキル
プロジェクトの進行状況を把握し、必要に応じて調[illegible]
必要な変更を承認し、計画に反映するスキル
組織が提供するサービスの水準や品質を監視、分析するスキル
顧客が求めるサービス水準を分析するスキル
フィードバックをもとにサービス改善を行うスキル
プロジェクトに必要な職務要件を基にメンバーを選定、採用するスキル
プロジェクトメンバーに対する情報伝達スキル
プロジェクトメンバーの意見への傾聴スキル
[illegible]築・改善や報酬を利用してチームビルディング[illegible]維持するスキル
[illegible]成果、費用[illegible]主要なステークホルダー[illegible]与する
[illegible]フォーマンス[illegible]評価するスキル
[illegible]整理・アーカイブ[illegible]や成果物[illegible]スキル
成果を分析し、次プロジェクトの計画を立案するスキル
関係部署と連携し、インシデント対処を行うスキル
関係者と適切なコミュニケーションを行うスキル
議論のファシリテーションを行うスキル
組織内外のステークホルダーと連携するスキル

フレームワークをもとに知識・スキルをリストアップ

知識・スキルを確認

既存の授業で不足する知識・スキルを特定

②戦略推進 プロジェクト管理

【知識】
- セキュリティ法規・リスク・インシデント対応およびAI活用の原則
- プロジェクトの計画・予算・評価および組織・人材管理のノウハウ

【スキル】
- プロジェクトの計画・予算・進捗を統括し成果を報告する能力
- 関係者との連携・交渉およびチームの採用・意欲向上を図る能力

対応策例

AIをプロジェクトマネジメントに活用する企業担当者を招聘

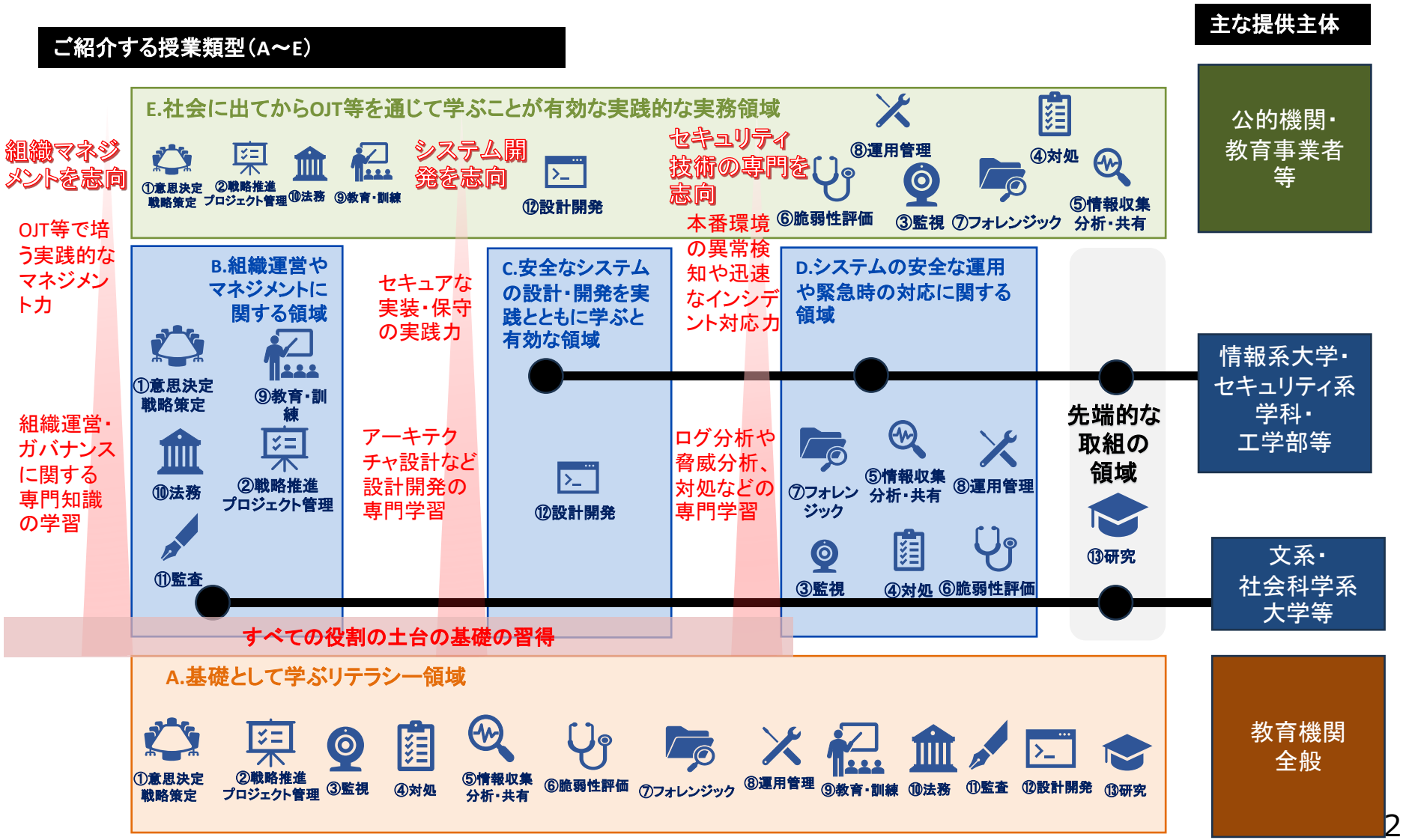
課題解決型プロジェクト学習でチームでの連携を学ぶ

Point
本手引き書P.16で述べた企業との対話を通じて把握した社会のニーズも踏まえ、対応の優先度をつけましょう。

※⑥脆弱性評価などについては、役割の特定後にタスク(T)の絞り込みを実施した上で、知識・スキル(KS)を特定することが望ましい場合があります。例えば、脆弱性評価の役割においては、「レッドチーム的な評価」なのか「脆弱性診断」なのかといった観点でタスクの絞り込みを行うことで、より適切な教育プログラムの設計につながります。

手引き書で考え方をご紹介する授業類型

- 13の役割に求められる要素を、学部や学科、提供する研修等のサービスの特性に応じてカリキュラムへ組み込みやすくするため、大きく4つの「授業類型」に整理しました。次頁以降で授業設計の考え方を紹介します。



A. 基礎として学ぶリテラシー領域

ポイント　プラス・セキュリティへの教育の手引きは、まず本頁をご覧ください

- 全学生が社会人として必要な「セキュリティ・リテラシー」を身につけるための授業設計の例です。
- 多くの役割に共通する基礎的な知識・スキルを抽出し、教養科目等で最新トピックや身近な事例と絡めて学習させることが有効です。

複数の役割において共通的に求められる知識・スキル

知識(K)	スキル(S)
• リスクマネジメントに関する知識 • 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 • 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 • 外部AIサービスを利用する場合の情報保護に関する知識 • AIが生成した情報の取り扱いにおいて留意すべき事項に関する知識 • セキュリティ対策目的でAIを利用する際に考慮すべき事項についての知識	• 関係者と適切なコミュニケーションを行うスキル • 組織内外のステークホルダーと連携するスキル • 想定読者に応じて適切な表現や形式のレポートを作成するスキル • 議論のファシリテーションを行うスキル • 通常時及びインシデント発生時の運用ルールを策定するスキル

既存の授業の工夫例

Point 1　学習する内容

- プライバシー保護等の基本的なルールを学習してもらう
- サイバーセキュリティの脅威や脆弱性に関する基礎知識を学習してもらう
- 生成AI等の最新のトピックと絡めて、技術者倫理（ELSI）やAI利用時のモラル等と合わせて学習してもらう

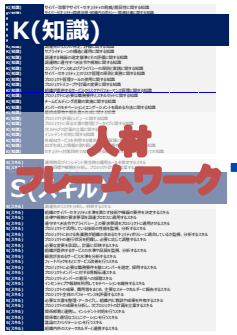
Point 2　学習の工夫

- 教養科目や教員養成科目として、多くの学生が受講する授業に組み込む
- ICTを教える授業に組み込む
- トラブル等の身近な事例と合わせて教える

※本手引き書はセキュリティ領域を中心に記載しています。カリキュラム設計の際は、学習の前提となる『ITの基礎知識（OSやネットワーク等）』が不足しないよう併せてご留意ください。

B.組織運営やマネジメントに関する領域

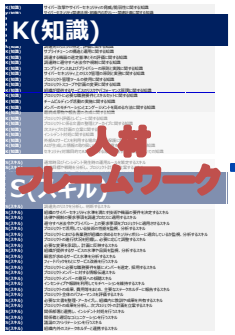
- 文系・社会科学系の学生等に向けて、組織運営やマネジメントの観点からセキュリティを学ぶための授業設計例です。
- 「意思決定・戦略策定」や「法務」「監査」などの役割に必要な知識・スキルを、関連法規やプロジェクト管理、リスクマネジメント等の既存の学習内容と結びつけることで実践的な素養を養います。



役割	①意思決定 戦略策定	②戦略推進 プロジェクト管理	⑨教育・訓練	⑩法務	⑪監査
知識	• 経営・組織運営、自組織の戦略 • リスクマネジメントおよびサイバーセキュリティ関連法規・ポリシー	• プロジェクト管理ツール、スコープ変更、予算管理 • サイバーセキュリティ上のリスク管理の原則と実務	• 教育計画、カリキュラムの立案および管理 • 指導技術や受講者の学習評価	• サイバーセキュリティおよびプライバシー関連法規・ポリシー • 法的リスクに対する分析・評価手法	• 監査プロセス、基準、倫理規定 • ポリシー、法規制、システム構成 • 監査ツール及び評価手法
スキル	• 組織目標と体制を評価し、水準を予測するスキル • ステークホルダーと連携し、コミュニケーションを行うスキル	• プロジェクト計画を立案するスキル • 関係者と適切なコミュニケーションを行い、ファシリテーションを行うスキル	• 教育計画やカリキュラムを策定 • 教材を開発または選定し、受講者の学習を指導・ファシリテートするスキル	• 関係者へのヒアリング等を通じて法的リスクを分析するスキル • 法的文書を作成して説明するスキル	• 監査計画を作成し、基準に基づき監査項目を設定するスキル • 管理策の実施状況やログ等を適合性を評価するスキル
既存の教育カリキュラム例	• ITパスポート試験の対策 • 企業経営の学習 • プロジェクトマネジメントやサイバーセキュリティ政策の学習	• プロジェクトマネジメントについての学習 • ITパスポート試験の対策 • 内部統制やISMSの学習	• 教育方法や指導方法についての学習	• 不正アクセス禁止法やGDPR等の関連法規の学習 • サイバー犯罪についての学習	• 監査や内部統制、法規等に関する学習 • 経営やマネジメントに関する学習

C.安全なシステムの設計・開発を実践とともに学ぶと有効な領域

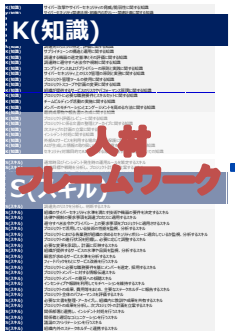
- 情報系や工学系の学生に向けて、システムやソフトウェアの安全な設計・開発を行うための授業設計例です。
- 「設計開発」や「脆弱性評価」などの役割に求められるタスクのうち、開発ライフサイクルの各フェーズ（要件定義・設計、実装・開発、テスト、リリース・運用保守）に関連するタスクを絞り込んだ上で、プログラミングやシステム構築の授業において、セキュリティ要件を組み込んだ実践的な演習等を取り入れることが考えられます。



役割	⑫設計開発 タスクをもとに細分化	要件定義・設計	実装・開発	テスト / リリース・運用保守
知識	• 組織のシステムのサイバーセキュリティの課題 • 要件定義書、基本・詳細設計書に記載すべき項目 • クラウドやOT環境の脅威と対策に関する知識	• コーディング、統合、内部デプロイ等実装に関する知識 • AI開発において考慮すべきセキュリティに関する知識	• テスト手法及び手順に関する知識 • 情報システムに対する攻撃に関する知識	• リリースの手順に関する知識 • 情報システムの変更管理に関する知識 • 情報システムの障害や復旧方法に関する知識
スキル	• システム上のセキュリティ課題を整理し、要件定義書に明確化するスキル • 要求を満たすためシステムへ実装するセキュリティ機能を具体化するスキル	• 設計書の要求を満たすセキュアなプログラムを作成、又は既成品を選定・実装するスキル • セキュア設計構築においてAIを適切に活用するスキル	• システムの特性からテスト手法を決定し、テスト計画書を作成するスキル • テストを実施し、結果を評価して改善活動を行うスキル	• 実装する機能を現場と調整の上、段階的にリリース・実装するスキル • システムに不具合等が発生した際に対応し、アップデート等の変更作業を行うスキル
既存の教育カリキュラム例	• 「監査」や「運用時のリスク管理」の視点を取り入れたアーキテクチャ設計・システム評価	• 暗号理論やアルゴリズム教育とセットにしたセキュアプログラミング演習 • Webアプリ開発を通じた実装実習	• 攻撃者視点を知るためのCTF形式演習 • システムに対する実践的な脆弱性診断・ペネトレーションテスト	• Webサーバやクラウド環境を用いたシステムのデプロイ・保守演習

D.システムの安全な運用や緊急時の対応に関する領域

- 情報系の学生等に向けて、システムの安全な運用やインシデント対応を担うための授業設計例です。
- 「監視」や「対処」「運用管理」などの役割に求められる知識・スキルに基づき、実際のツール操作やログ分析、インシデント対応の疑似体験等を授業に組み込むことが有効です。



役割	③監視	④対処	⑤情報収集分析・共有	⑥脆弱性評価	⑦フォレンジック	⑧運用管理
知識	• ツール（監視、ログ収集・分析）及びその手法に関する知識 • セキュリティログ（システムログ等）に関する知識	• インシデント対処活動の手順や手法 • インシデント評価、トリアージ • リスク／脅威の評価	• サイバー攻撃やサイバーセキュリティの脅威/脆弱性 • 情報収集及び分析のツール、手法	• 脆弱性評価/ペネトレーションテストツール及び手法 • 脆弱性の一般的な評価基準	• フォレンジック対応のプロセス、必要なツール等 • データ保全・分析のツール、手法及びプロセス	• ネットワーク及びシステムセキュリティ • クラウドサービスの種類と責任分界 • アクセス制御
スキル	• システムやネットワーク等を監視し侵入を検出 • ログから、機器障害か不正アクセスかを判別	• 事業継続を目的に何の対応を優先すべきかを判断 • 関係各所に指示を与える	• 信頼できる情報源を特定し、関連する情報を収集 • 情報を元にリスク分析を行い、組織に影響のある脅威を特定	• シナリオを元にテストを行う • 脆弱性の深刻度や影響を元に重大度をスコアリングし優先度を付けるスキル	• データの機密性、完全性等を損ねず保全 • データを分析し、機器で行われた操作や不正行為を特定	• アクセス制御を実施し、正しい制御かを確認 • ハードウェア、ソフトウェア等に適切なセキュリティ対策を設定
既存の教育カリキュラム例	• ハニーポットを用いた攻撃の検知演習 • SIEMツール等を用いたトラフィック・ログ分析演習	• CSIRTを想定したインシデント対応演習 • 外部実践プログラム（SecCap等）やCTFを取り入れたハンズオン	• OSINTを活用した最新の脅威情報の収集と分析レポート作成 • 経済安全保障やサイバー犯罪等、脅威動向のケーススタディ	• 攻撃手法の理論と実践を組み合わせたペネトレーションテスト演習 • CTFを活用した脆弱性発見の実践	• デジタル証拠の保全・抽出を行うデジタルフォレンジック演習 • サイバー犯罪捜査や刑法等と紐づけた法的・技術的調査	• サーバ、OS、ネットワーク、ファイアウォール（FW）等の構築とアクセス制御の実習

E.社会に出てからOJT等を通じて学ぶことが有効な実践的な実務領域

- 本領域は、人材育成における「学習の3層構造」のうち、最上位となる第3層（実践・実務領域）に位置づけられます。大学や高専等で身につけた「第1層：一般的なリテラシー」や「第2層：専門的・技術的な基礎力」をベースに、実際の業務現場で求められる実践的なタスク遂行能力を養います。主に、社会人向けにスポット的な教育を提供する教育事業者や、企業内のOJTが担う領域です。

実践・実務領域の例

タスクに必要な知識・スキルを学習

	実務とマネジメント	現場の実践的運用	プラス・セキュリティ
役割	①意思決定 戦略策定 ②戦略推進 プロジェクト管理	⑧運用管理 ③監視 ④対処	⑧運用管理 ⑨教育・訓練 ⑩法務
タスク	組織全体のルール策定や、外部委託先の管理、インシデント発生時の事業継続判断を実施	システムの安定稼働を担う担当者が、日々の運用の中で異常を検知し、有事の際に迅速な初動対応を行う	契約手続、法的対応、対外発表や、日々の業務データ・IT機器の適切な管理を通じて、情報漏えいリスクに対処
	• インシデントの初期評価等 • 外部委託先の選定、委託内容の調整、ベンダーの報告書の評価 • コミュニケーションおよび折衝	• アラート監視による不審な兆候の検知と、関係部署への正確な報告 • システムやネットワークにおける不審なイベント・インシデントの検知	• IT機器や外部サービスの調達から運用終了に至るまでの安全管理 • 適切なアカウント管理・アクセス制御 • 秘密保持契約等締結、リスクの評価
知識	• 商用サイバーセキュリティサービスやベンダーの得意分野に関する知識 • 組織のサイバーセキュリティ体制における、各部門の機能及び役割分担に関する実務知識	• 各種セキュリティログの実践的な読み方と意味の理解 • インシデント対処の具体的な手順と、自組織における運用ルールに関する知識	• アカウント管理やアクセス制御の手法など、データセキュリティの管理 • IT機器・システムのライフサイクルにおいて生じるセキュリティリスク • サイバーセキュリティ関連法規や外部への報告フロー等
スキル	• 自組織内/外から収集した初期調査の速報をもとに、事業継続を目的として優先順位を判断 • 調達先（委託先）のセキュリティリスクを実務的な観点から分析し、許容可能かを判断するスキル	• 分析・監視ツールを操作し、異常や不審なイベントを検知するスキル • ログの挙動から不正アクセス等のサイバー攻撃を正確に判別するスキル • インシデント検知時に手順通りに迷わず迅速に対処・報告を実施	• アカウント・IDやアクセス権を管理 • 関係文書や対象サービス利用規約等を正確に理解・評価するスキル • 法的事項や技術的事項について専門家との橋渡しとなり、関係者と適切にコミュニケーションを行うスキル

学年ごとの学習事項の考え方

- 教育機関における学習カリキュラムは、学生の学年や習熟度に合わせて段階的に設計することが重要です。
- いきなり高度な専門領域から始めるのではなく、基礎的な「リテラシー」からスタートし、段階的に「技術」や「ガバナンス」の専門知識・スキルを積み上げていくことが重要です。

基礎的な知識・スキルを学習

専門的な学習

リテラシー※

- リスクマネジメントに関する知識
- 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
- 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
- 外部AIサービスを利用する場合の情報保護に関する知識
- AIが生成した情報の取り扱いにおいて留意すべき事項に関する知識
- セキュリティ対策目的でAIを利用する際に考慮すべき事項についての知識

※リテラシーの学習にあたっては、前提となる『ITの基礎知識（OSやネットワーク等）』が不足しないよう併せてご留意ください。

1st step

多くの役割に含まれる知識・スキルを学習

技術

- 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 等

ガバナンス

- リスクマネジメント
- 関係者と適切なコミュニケーションを行うスキル
- 通常時及びインシデント発生時の運用ルールを策定するスキル

2nd step

特定の役割に固有の知識・スキルを学習

技術

- ペネトレーションテストツール及び手法に関する知識
- 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

ガバナンス

- 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
- 対外的に提出する法的文書を作成するスキル等

カリキュラムの設計に役立つ参考情報

- カリキュラム作成時は、目的や学生の層に応じて既存の文書等も活用可能です。各授業類型で参考になる情報を下表に整理しました。
- ご紹介した授業類型にあわせ、知識・スキルの具体的な授業への落とし込みにぜひご参照ください。

	A. 基礎として学ぶリテラシー領域	B.組織運営やマネジメントに関する領域	C.安全なシステムの設計・開発を実践とともに学ぶと有効な領域	D.システムの安全な運用や緊急時の対応に関する領域	E.社会に出てからOJT等を通じて学ぶことが有効な実践的な実務領域	研究
情報処理学会 カリキュラム標準（J17等） 一般社団法人情報処理学会	J17が定める6つの情報専門領域（CS, IS, CE, SE, IT, GE）とSecBoKの各知識項目との対応表を提示。「一般教育」「セキュリティ基礎」「セキュリティ専門」の3レベルに応じた科目モデルや、既存カリキュラムを整理するためのテンプレートを記載					
モデルコア カリキュラム 一般社団法人情報処理学会			MCC（Model Core Curriculum：モデルコアカリキュラム）として到達目標を定義し、創造性・デザイン能力・汎用的技能などの基盤的資質を定義。教育高度化指針「MCC plus (COMPASS 5.0)」内で、サイバーセキュリティ等のスキルセットを定義			
大学における情報セキュリティ教育のためのモデル・コア・カリキュラム 文部科学省	対象者別（学士課程の一般教養、理工系、情報系、修士課程、社会人学び直しの短期/中期/長期など10区分）に、到達目標とカリキュラム構成例（講義・演習内容）を例示。各科目が産業界の指標（SecBoK、iCD、情報処理安全確保支援士）のどのスキルを満たすかの対応表を整理					
Center of Academic Excellenceのリソース 米国 国家安全保障局(NSA) 国土安全保障省(DHS/CISA)	CAE-CDで学位に応じたKnowledge Units (KUs) の要件を整理し、ハンズオン演習の実施などの評価基準が記載。	CAE-CDで学位レベルに応じたKnowledge Units (KUs) のマッピング要件を整理し、カリキュラムにおけるハンズオン演習の実施などの評価基準が記載。				CAE-Rでサイバーセキュリティ研究機関としての評価基準等を記載
医療分野における持続可能な情報セキュリティ人材育成と継続的雇用・配置・キャリア形成等に関する提言 安全な地域医療の継続性確保に資する医療機関における情報セキュリティ人材の育成と配置に関する研究班	Group C 人材向けカリキュラム 医療情報セキュリティの基本（日常業務での基礎的対策、トラブル時の初期対応など）を全職員向けのリテラシーとして定義。	Group A・B 人材向けカリキュラム 情報セキュリティマネジメント、医療情報関連法令・ガイドライン、IT-BCPの策定、組織的な体制構築や人材育成の手法を定義。		Group A・B 人材向けカリキュラム インシデント発生時の適切な初動対応、侵入検知・防御技術、サイバー攻撃の脅威と脆弱性対応等、実践的な運用・対応スキルを定義。		

SecBoK（セキュリティ知識分野）を活用した知識・スキルの詳細化

- 本フレームワークで定義している知識・スキルをより具体的な教育内容へ落とし込む際、JNSA（日本ネットワークセキュリティ協会）が公表している「セキュリティ知識分野（SecBoK）人材スキルマップ2025年版」を活用することが有効です。
- SecBoKは、本フレームワークと同じくNICEフレームワークとの対応関係を有しており、NICEのTKS-IDを介して本フレームワークの知識・スキル項目とSecBoKの約1,200の詳細項目を相互参照することが可能です。
  カリキュラム設計において、フレームワークの知識・スキル項目をもとに「何を教えるか」の大枠を決めた後、SecBoKのカテゴリ分類を参照して具体的な授業内容・教材の設計に活用できます。

知識（K）項目の相互参照の例

本フレームワークの知識項目	SecBoK 2025 大項目	SecBoK 2025 中項目	SecBoK 2025 小項目
インシデント対処活動の手順や手法に関する知識	08_セキュリティ運用	5_インシデント対応	インシデント対応の原則と実践に関する知識
			インシデントレスポンスツールと技術に関する知識
			インシデントハンドリングツールと技術に関する知識
	15_法・制度・標準	0_総論	サイバーセキュリティのポリシーと手順に関する知識
	17_関連領域	1_ICT > 11_システム運用	ビジネス継続性とディザスタリカバリ (BCDR) のポリシーと手順に関する知識
アカウント管理に関する知識	04_セキュリティマネジメント	1_ポリシー策定	アカウント作成のポリシーと手順に関する知識
			パスワードポリシーと手順に関する知識

スキル（S）項目の相互参照の例

本フレームワークのスキル項目	SecBoK 2025 大項目	SecBoK 2025 中項目	SecBoK 2025 小項目
関係者と適切なコミュニケーションを行うスキル	02_IT ヒューマンスキル	1_コミュニケーション力	社内外のステークホルダーとの関係構築に関するスキル
			社内外のステークホルダーと協力するスキル
			技術スタッフとのコミュニケーションに関するスキル
			外部組織とのコミュニケーションに関するスキル
			社内外のステークホルダーとのコミュニケーションに関するスキル
議論のファシリテーションを行うスキル	02_IT ヒューマンスキル	1_コミュニケーション力	小グループでのディスカッションを円滑に進めるスキル
			グループディスカッションを円滑に進めるスキル

学ぶべき内容を充足するための工夫例

セキュリティ人材が知識を習得した方法

- 学生が現場の即戦力となるには、知識・スキル（KS）の特性に応じた学習手法の選択が重要です。
- 育成したい役割に合わせ、「手を動かす演習」や「協働学習」「勉強会」など、最適な方法を取り入れてください。

Point

身につける知識・スキルに適した手段の選択が重要

【知識・スキルの獲得手段※】
- 社内研修・勉強会
- 社内のOJT・実業務での経験
- 外部の有料研修・トレーニング
- 書籍等の学習・資格取得
- 社外コミュニティ・勉強会への参加

セキュリティ業務従事者

学習手法	効果的な役割	効果的な知識（K）・スキル（S）の例
手を動かした演習	③ 監視 ⑥ 脆弱性評価 ⑦ フォレンジック ⑧ 運用管理	• ツールを用いたシステム監視と侵入検知 • 脆弱性評価ツールの取扱い • 脅威シナリオに基づく脆弱性の実証検証 • 完全性を保ったフォレンジックデータ保全 • システム脆弱性の修正作業 • 通信機器等のインストールと設定
協働学習	② 戦略推進・プロジェクト管理 ④ 対処 ⑨ 教育・訓練 ⑪ 監査	• 関係者との適切なコミュニケーション • 関係部署と連携したインシデント対処 • 関係各所への対処・復旧作業の明確な指示 • 議論のファシリテーション • プロジェクトメンバーの意見への傾聴 • 受講者の学習指導とファシリテーション • 目的に応じたインタビューの実施
勉強会での演習	① 意思決定・戦略策定 ⑤ 情報収集・分析・共有 ⑩ 法務 ⑬ 研究	• インシデント発生時の経営的意思決定の知識 • セキュリティ方針・目標の策定と組織設計 • 収集情報を基にしたリスク分析と脅威特定 • 組織内の法的リスク分析と明確化 • 法的リスクのスコアリングと対応の優先順位付け • 先行研究の調査と未解明事項の導出

※業務従事者向けのアンケートをもとに作成

学ぶべき内容を充足するための工夫

- 座学だけでは知識・スキルの網羅が難しい場合、実践的な演習やシミュレーションの導入が効果的です。
- 仮想空間（レンジ）を用いた攻防演習や、プロジェクト型学習（PBL）、実務家による現場視点の講義など、各役割の特性に合わせた具体的な工夫例を紹介します。

カテゴリ	工夫の内容・手法	概要・事例	該当する役割
技術力・実装力の育成	**仮想空間での演習**	仮想空間(レンジ)での攻防や攻撃再現を通じ、脆弱性原理と対処を習得	③ 監視 ④ 対処 ⑥ 脆弱性評価
	OT・制御システム実機演習	模擬プラント等を用い、ITとは異なる制御系特有のセキュリティを学習	⑧ 運用管理
運用・開発の実践	**PBL・システム実装**	チームによるセキュアな設計・実装や、課題解決プロジェクトの実践	⑫ 設計・開発
	擬似インシデント対応	ログやシナリオを用い、予兆検知から復旧までの実務のフローを体験	③ 監視 ④ 対処 ⑦ フォレンジック
戦略・マネジメントの実務寄りの学習	**実務家による講義**	現場の意思決定、法制度、経済安保を学習	① 意思決定・戦略策定 ⑤ 情報収集・分析・共有
	マネジメント内部統制シミュレーション	ISMS構築、リスク評価、監査計画など、組織統治とガバナンスを学習	⑨ 教育・訓練 ⑪ 監査 ② 戦略推進・プロジェクト管理

外部人材による講義が有効な役割と事例

- 最新動向や高度な実務スキルを学生に提供するためには、産学連携や外部専門家の活用が非常に有効です。
- 経営層やプロジェクト管理者による「実務家の講義」や、セキュリティベンダー等が提供する「仮想空間での演習」など、外部リソースを活用することで、習得しやすい役割と知識・スキルが存在します。

産学連携・教育機関の連携が多く行われる役割

実務家の講義

知識	スキル
• インシデント発生時における組織経営・運営上の意思決定に関する知識 • 経営・組織運営、自組織の戦略に関する知識 • サプライチェーンの構造と運用に関する知識	• 組織内外のステークホルダーの意向及び能力を評価するスキル • 法令や規制等を評価し、組織への影響を特定するスキル • 関係文書や対象サービス等を法的観点から正確に理解するスキル

仮想空間での演習

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 • 脆弱性評価ツール及び手法に関する知識 • ペネトレーションテストツール及び手法に関する知識	• 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 • 評価/テストで収集した情報を整理し、情報の正確性を分析することで、具体的な脆弱性を特定するスキル

外部人材の講義によって習得可能な知識・スキルの例

外部人材の探し方と連携の工夫

- 外部人材を招く際は、立地や企業との関係性など自校の強みや特性を活かした連携が重要です。
- 教育機関の類型に応じた外部連携の工夫例を提示します。

	教育機関の類型	対応内容
強みや特性を活かす	卒業生を通じた企業との連携が強い	インターン等の活動の一環として、サイバーセキュリティに関する企業の検討を行う
	地元にセキュリティ人材が活躍する企業がある	地元のサイバーセキュリティを担う企業と連携し、産業界講師による講演を行ったり、学生にインターンの機会を設ける
	近隣に多くの大学等が立地している	近隣のサイバーセキュリティの学科を持つ大学等と連携し、共同で演習を実施することで負担を軽減
弱みを補う	実践的な教育を行える人材が不足	地域のセキュリティコミュニティ【地域SECUNITY】※1と連携し、実践経験を有する人材に講師を依頼したり、学生の参加を促す
		SECCON※2ほか、多くの学生が参加するセキュリティイベントを紹介し、オンライン/オンサイトのイベント参加を通じて関心を高めてもらう
	大都市から離れた立地	セキュリティの専門人材は東京近郊に集中している実態があり、連携企業からオンラインの遠隔講義を実施

※1 地域SECUNITY紹介ページ https://www.meti.go.jp/policy/netsecurity/secunity.html
※2 SECCON https://www.seccon.jp/

おわりに／参考情報

- 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。
- フレームワーク本体や関連機関の教育ガイドライン、ツール等のリンク集として、カリキュラム検討にご活用ください。

- 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（プラス・セキュリティ向け）」（P. 25～31）
  - TKSの振り返り（セルフアセスメント）を行った上で、資格取得や研修の受講等で知識・スキルを補うための考え方に言及していますが、E.社会に出てからOJT等を通じて学ぶことが有効な実践的な実務領域に関連しています。

- 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（専門人材向け）」専門人材のキャリアパス例
  - 専門人材のモデルケースごとに、現在も活躍される専門人材の実体験についてご紹介しています。