国家サイバー統括室
National Cybersecurity Office

資料5

サイバーセキュリティ人材フレームワーク（案）の検討状況について

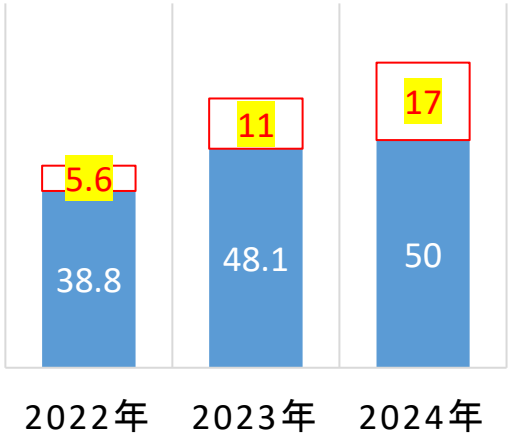
内閣官房 国家サイバー統括室
人材政策班

サイバーセキュリティ人材を取り巻く情勢

- サイバー攻撃の巧妙化・深刻化によりサイバーセキュリティを担う人材の確保・育成は急務。
- 効率的・効果的にサイバーセキュリティ人材の確保・育成を図るため、国家サイバー統括室ではサイバーセキュリティ人材の役割や技能を定義した人材フレームワークの年度内のとりまとめに向け、有識者検討会※2を立ち上げ議論を進めたほか、フレームワーク案のパブリックコメントを実施。

※1　我が国のCS人材数について

米国ISC2（セキュリティの国際的な民間認定団体）による調査によると、必要数・不足数とも増加傾向にある。



（出典）ISC2 Cybersecurity Workforce Study 2022, 2023, 2024

※2　サイバーセキュリティ人材フレームワークに関する検討会について

2025年10月、人材フレームワークに関する議論を進めるため、有識者11名からなる検討会を立ち上げ。

構成員※　（五十音順・敬称略）

- 猪俣　敦夫（座長代理）
  ・・・・・大阪大学D3センター教授 CISO
- 川北　陽司
  ・・・・・独立行政法人情報処理推進機構（IPA）デジタル人材センター 人材プロモーションサービス部スキルトランスフォーメーショングループ サブグループリーダー
- 後藤　厚宏（座長）
  ・・・・・情報セキュリティ大学院大学 教授
- 園田　道夫
  ・・・・・国立研究開発法人情報通信研究機構（NICT）
- 辻　伸弘
  ・・・・・SBテクノロジー株式会社プリンシパルセキュリティリサーチャー
- 西本　逸郎
  ・・・・・株式会社ラック技術顧問
- 日暮　拓人
  ・・・・・一般社団法人 人材サービス産業協議会事務局長
- 平山　敏弘
  ・・・・・情報経営イノベーション専門職大学（iU） 教授
- 松本　哲也
  ・・・・・パナソニックホールディングス株式会社
- 吉岡　克成
  ・・・・・横浜国立大学大学院環境情報研究院/先端科学高等研究院教授
- 和田　昭弘
  ・・・・・全日本空輸株式会社デジタル改革推進室専門部長

※その他、関係省庁等がオブザーバーとしての参加

（これまでの議論の過程等）

第1回（2025年10月14日）
- 人材フレームワーク策定及び利活用等の基本的考え方について

第2回（2025年12月18日）
- 関係者（セキュリティベンダー、商工会議所、人材サービス事業者）からのヒアリング
- 手引き書の基本的考え方について

第3回（2026年2月9日）
- 関係者（人材可視化、高等専門学校、OT）からのヒアリング
- フレームワーク案、手引き書の進捗について

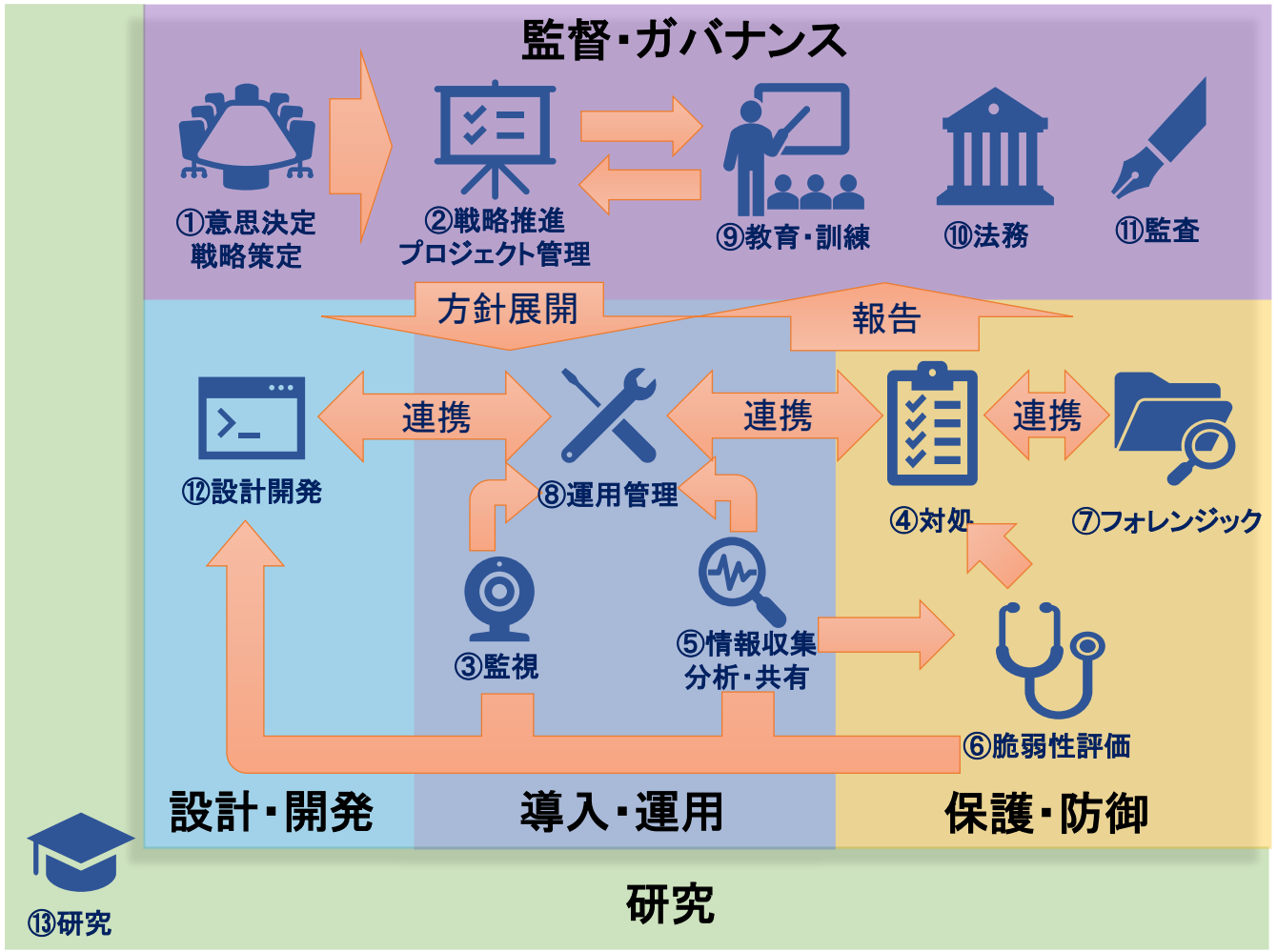
フレームワーク案のパブリックコメント
（期間：2026年2月17日（火）～3月10日（火））

サイバーセキュリティ人材が担う役割の全体像

概要

国内外のフレームワーク類との相互参照性を確保しながら技術的側面に限らず、サイバーセキュリティ業務にかかわる13の役割及び人材の練度等に応じた4段階のレベルを定義

13の役割の全体像



レベルの概要

レベル	レベル定義の概要
4	業務における最終意思決定に責任を負う
3	独力で業務遂行可能であり、マネジメントを行う
2	指示に基づく作業を実施する
1	最低限必要な知識を有する

人材フレームワークの位置づけと前提等

位置づけ	必須事項ではなく、「指針」の位置づけ
対象範囲	産官学等幅広い主体による活用を想定
活用方針	利用者の実態に応じて柔軟に活用
他のフレームワークとの関係性	相互参照を図りながら活用
見直し	不断の見直しを前提とする

体制整備等にあたり、一律の履行を求めるものではなく、利用主体の取り組みを支援するための「指針」である。

国・地方公共団体・民間企業、教育関係機関等、産官学を問わず、幅広い主体における活用を想定。

各利用主体が、組織の規模・特性、職務内容等に応じて、変更・修正をして、柔軟に活用することを想定。

主な利用主体別にフレームワークの活用例等をまとめた「手引き書」を併せて策定。

既存の国内外の人材フレームワーク（※）等との相互参照性を確保することで、利用場面や利用主体の特性に応じた補完関係や発展的な活用を促進する。

※　特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）が発行するSecBoK
　　産業横断サイバーセキュリティ検討会　人材定義リファレンス　　等

技術動向や社会情勢の変化を踏まえ、必要に応じ見直しや改訂を行う。

手引き書（案）の構成イメージ

手引き書は、利用主体に共通する事項と、主体ごとの固有事項を分けて構成する。

共通事項	
● サイバーセキュリティ人材フレームワークの概要 策定背景及び及び定義する13の「役割」の全体像等について ● サイバーセキュリティ人材フレームワーク本体の構成 ● 手引き書の概要 位置づけや手引き書で具体化する「人材像」の概念について　等	
利用主体別固有事項	
① 小規模組織 例：中小企業、小規模自治体 等	● 必要な役割の割り当てや自組織で担う機能と外部委託する機能を整理 ● 従業員規模に応じた体制モデル等の提示 ● 限られた人員の中での育成方法や外部支援の活用方法の整理
② 大規模組織 例：中堅・大企業、政府機関 等	● 集権型・委員会型等の体制形態とセキュリティガバナンス機能の整理 ● 採用時の職務定義書作成や役割に基づく人材配置の考え方 ● レベルに基づく評価等人材マネジメント視点での活用例
③ 教育機関 例：大学、教育事業者 等	● フレームワークを産学で共有する共通言語として活用する考え方 ● 短期（教育事業者）と中長期（大学等）の人材育成の役割の違いを踏まえたカリキュラム設計の考え方 ● 既存の好事例の紹介による教育プログラム設計に資する参考情報の提示
④−1 個人（専門人材） 例：専門人材、専門人材を目指す学生等	● フレームワークに基づくセルフアセスメントの実施方法 ● 複数の役割間の移行など、多様なキャリアパス間の提示
④−2 個人（プラス・セキュリティ人材）	● セルフアセスメントによる基礎スキルの確認と能力向上の方向性整理 ● 小規模組織の体制モデルを踏まえた、兼務人材として担う役割・業務の理解

人材フレームワークの普及により、人材確保・育成・活躍が進む姿の実現に向けて

- 人材フレームワークを軸に、求人情報、教育・訓練、資格試験・演習等の情報を関連付けて、我が国における 効率的・効果的なサイバーセキュリティ人材の確保・育成を図る。（サイバーセキュリティ戦略）
- その実現に向けて、当面は、事業者等の協力の下、フレームワークや手引きの実践による効果検証を蓄積。
- 重要インフラ事業者にも活用に向けて取り組んでいただくべく、行動計画等への反映（参照関係の確立）を進める。
- ユースケースも踏まえた拡大方策を講じていくなど、段階的な普及方策を検討。

活用場面	試行段階（ユースケースの発掘）	普及段階（拡大方策の実施）	目指す姿
体制整備	●手引き書①の実践 ● 中小企業	重フラ事業者においても、まずはフレームワークと実際の体制との対応をとるなど積極的な活用によってユースケースを蓄積	限られた人員の中で担うべき役割・タスクを明確化し、選択と集中による効率的なスキル向上により、サイバーセキュリティ対策を強化
採用・配置	●手引き書②の実践 ● セキュリティ担当 ● 人材サービス事業者	利活用の一層の促進に向けて、ユースケースの蓄積を踏まえたフレームワーク等の見直しを行うとともに、必要な仕組みの検討を含め、官民連携の下で取組を推進	組織が求める人材の定義をフレームワークに沿って理解可能なものとすることで、採用や配置時のミスマッチを解消
教育・訓練	●手引き書③の実践 ● 教育機関 ● 教育・訓練事業者		フレームワークに沿って個人や社会のニーズが可視化されることにより、要請に沿った教育・訓練メニューの強化・提供
キャリア形成	●手引き書④の実践 ● 学生 ● 専門人材		社会ニーズの可視化により、CS人材として目指すべきキャリアが明確化され、自身が保有するスキル・知識とのギャップ分析等により、積極的・継続的なスキル向上を実施

参　考

III. 目的達成のための施策
3. 我が国のサイバー対応能力を支える人材・技術に係るエコシステム形成

（1）効率的・効果的な人材の育成・確保

経済社会のデジタル化が進展する中で、サイバー攻撃は一層複雑化・巧妙化の一途を辿り、あらゆる分野でサイバーセキュリティを担う人材の確保・育成が急務となっている。このため、人材フレームワークを軸に、様々な施策を有機的に連携させながら効率的・効果的な人材育成を進める。

① 人材フレームワークの整備と効果的な運用

サイバーセキュリティ分野における人材の確保・育成を効果的に推進するためには、多様な職務ごとに、必要な知識・スキル等を体系的に整理した人材フレームワークを速やかに策定し、社会の様々な場面で活用されることが重要である。これにより、企業や行政機関、大学・教育機関等が**サイバーセキュリティ人材像の共通理解の下、より効果的かつ計画的な育成や採用等が可能**となる。

フレームワーク策定に当たっては、我が国の官民における対処体制を念頭に実用性の高い内容とした上で、国内外の既存フレームワークや職業分類等との整合を図ることで、人材が国内外を問わず活躍できる環境の整備を目指す。

フレームワークの整備後は、その人材定義に基づき、人材の需要・供給状況や教育・訓練機関の情報を網羅的かつ一元的に可視化し、国内の人材動向を俯瞰できる仕組みづくりのために、官民協働して取り組む。これにより、キャリアパスを可視化し、**人材を活用しようとする様々な組織における採用・配置等の場面を通じ、人材のマッチングやキャリア形成支援の質と効果を一層向上**させていく。

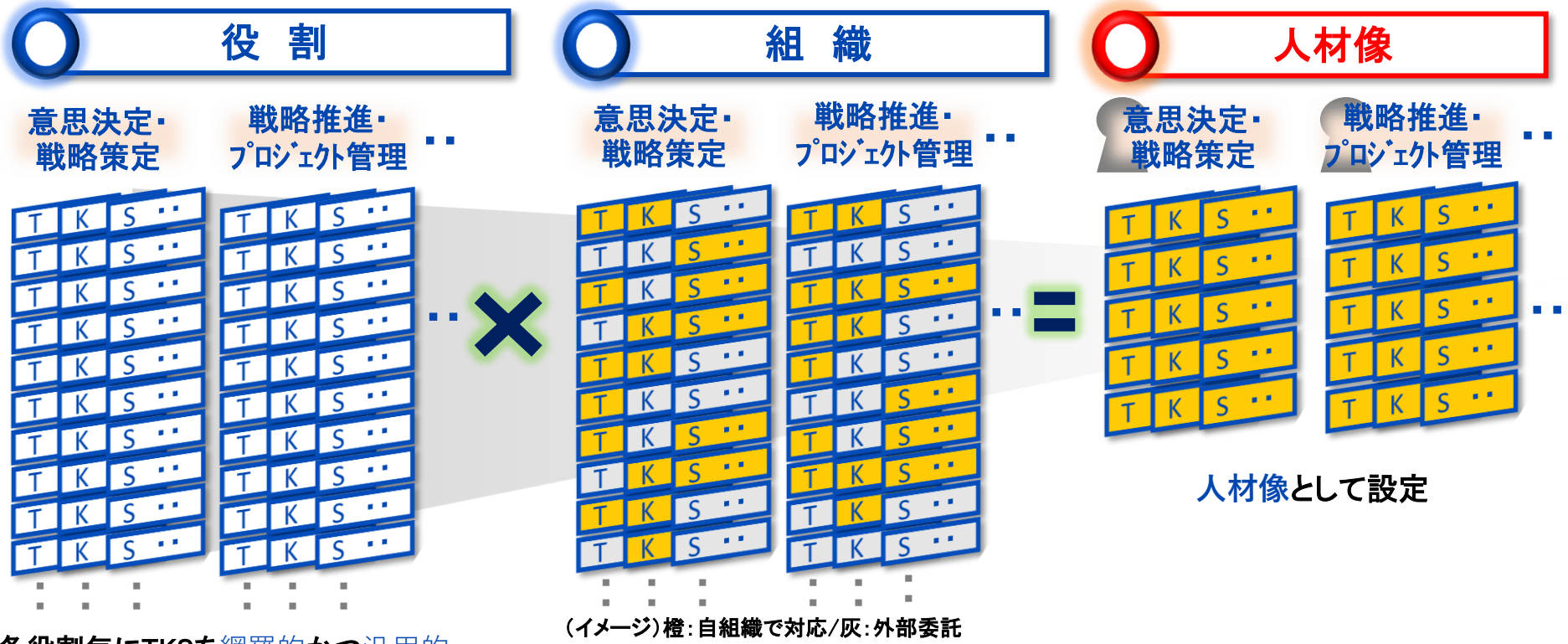
様々な主体によって行われる教育・訓練について、フレームワークとの関連付けを強化する。具体的には、資格試験の合格や実践的演習の修了等といった成果と、フレームワークにおける人材像・レベルとの関連付けを推進し、参加者のスキルの可視化を促進できる仕組みとするとともに、教育・訓練のカリキュラム設計にも活用する。政府においては、政府デジタル人材のスキル認定制度と連携を図るなど、フレームワークを基盤として適切な評価制度の整備や人材の適正配置を促進する。

これらの取組を通じて、多様な人材が社会で必要とされる場面で力を発揮する環境を整えることで、**様々な現場で得られた知見や経験が人材を通じて有機的に循環**することになり、社会全体のセキュリティ水準の持続的強化にもつながる。

サイバーセキュリティにおける人材像の概念整理

概要

- フレームワーク本体において、サイバーセキュリティ人材が担う13の「役割」を示したうえで、役割毎に汎用的なタスク(T)、知識(K)、スキル(S)を定義する。
- 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「(各組織における各役割の)人材像」とし、その具体化手順について手引き書にて提示する。



各役割毎にTKSを網羅的かつ汎用的に定義

組織特性に応じて、自組織で確保すべき役割やTKSを絞り込み

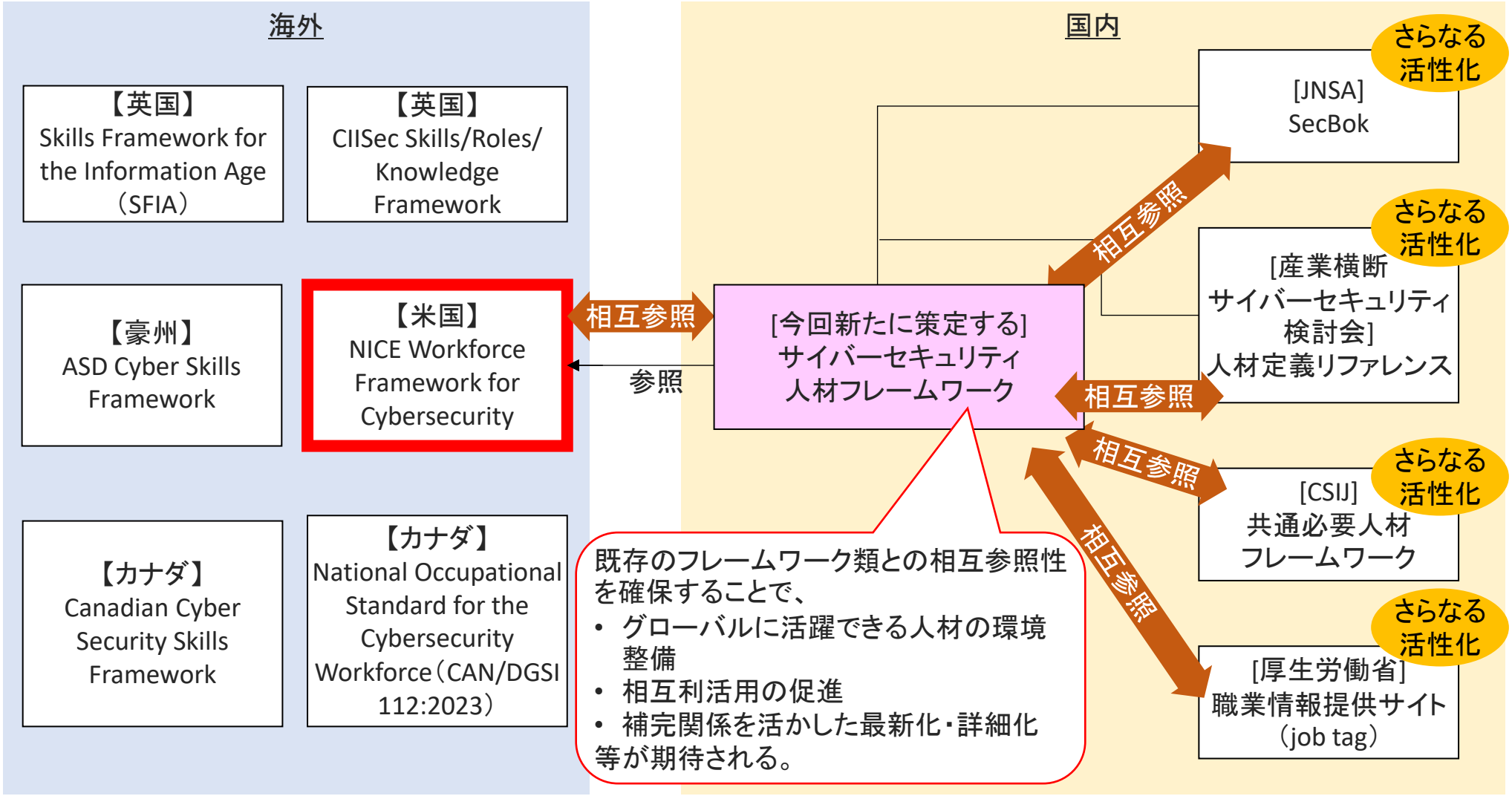
手引き書では、モデルケースをもとに、人材像の設定方法を提示

フレームワーク本体

手 引 き 書

国内外のフレームワーク類との関係性（イメージ）

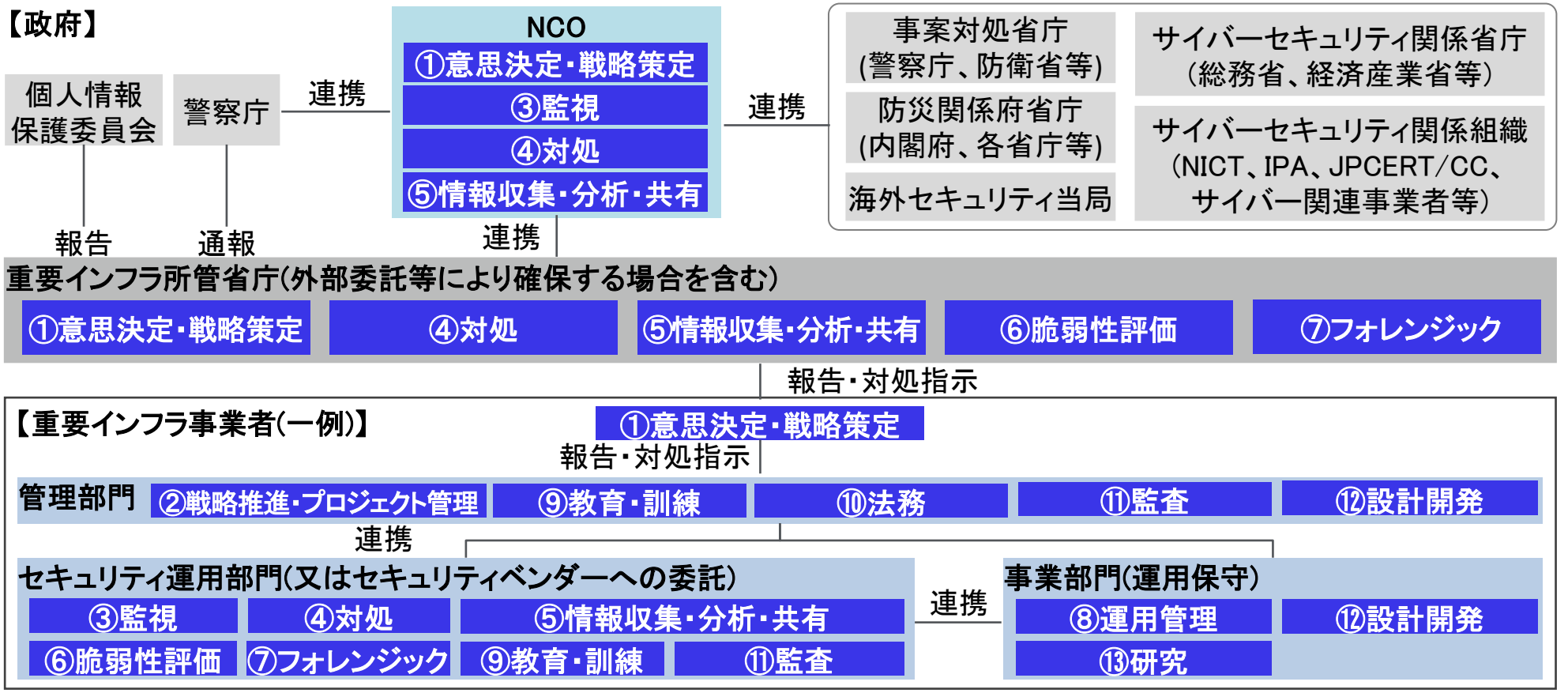
（国内外の既存のフレームワークとの相互参照イメージ）



役割の設定（案）（例：重要インフラ事業者向け対処体制）

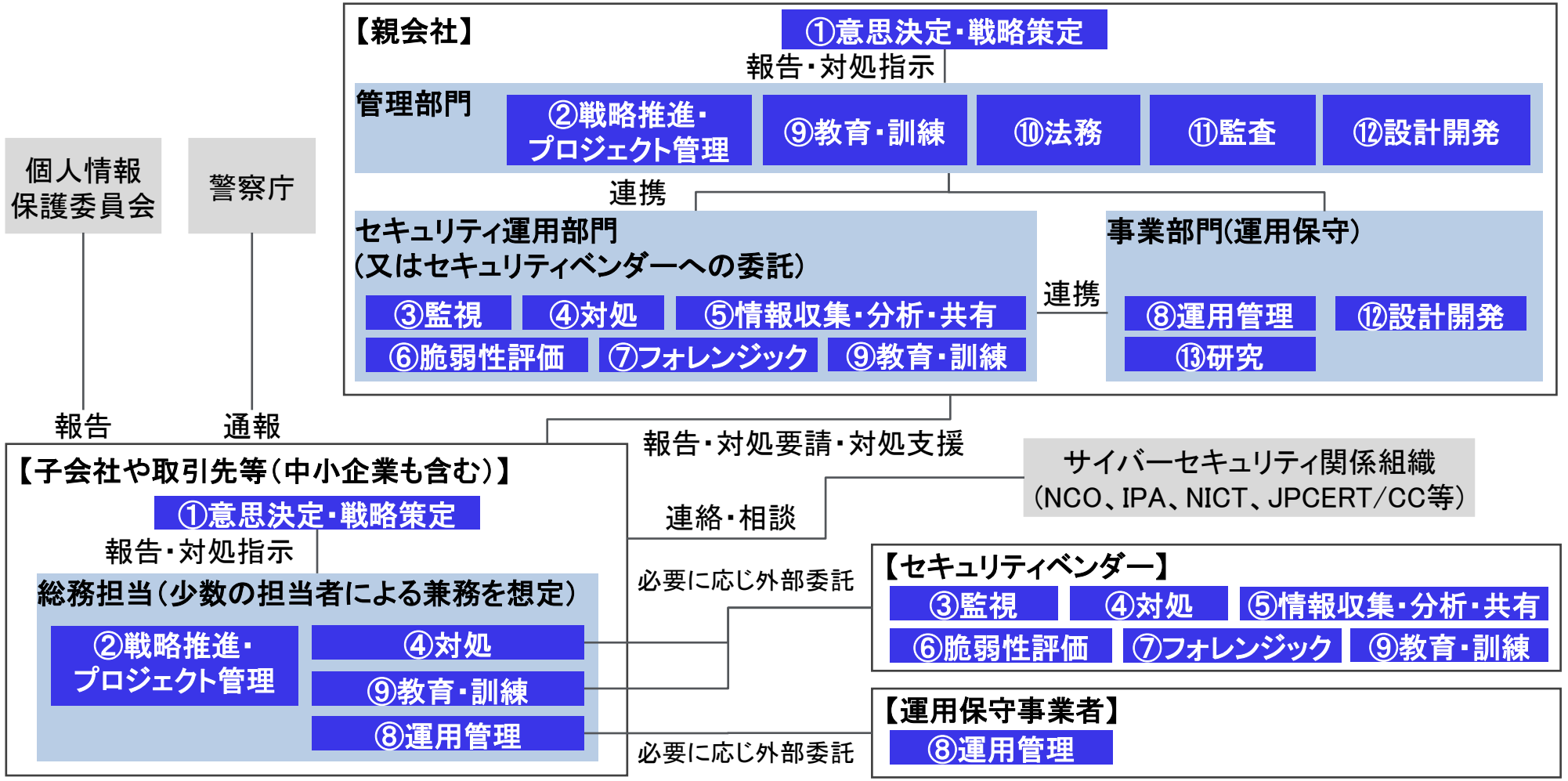
- 重要インフラ企業がサイバー攻撃を受けた状況において、官民が連携して事案対処を行う場面（下図）で求められる13の人材像を設定。
- 役割ごとにT（タスク）、K（知識）、S（スキル）を定義の上、４段階にレベル分け。

① 意思決定・戦略策定　② 戦略推進・プロジェクト管理　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　⑨ 教育・訓練　⑩ 法　務　⑪ 監　査　⑫ 設計開発　⑬ 研　究



（参考）活用例①：サプライチェーン関係者間の連携

- サプライチェーン上の子会社や取引先等の中小企業が、サイバー攻撃によりサービスや製品等に多大な影響を受けた場合（サプライチェーン全体に被害が発生）に、想定される対処体制を検討。
- サプライチェーン上の親会社やセキュリティベンダーと連携しつつ対処にあたる場面を想定。



（参考）活用例②：中小企業

- 中小企業がサイバー攻撃により多大な影響を受けた場合に想定される対処体制を検討。
- 中小企業では総務担当等本来は別業務を本務とする者が、複数の役割を兼務し、セキュリティベンダー等と連携しながら対処にあたる場面を想定。