国家サイバー統括室
National Cybersecurity Office

資料２

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

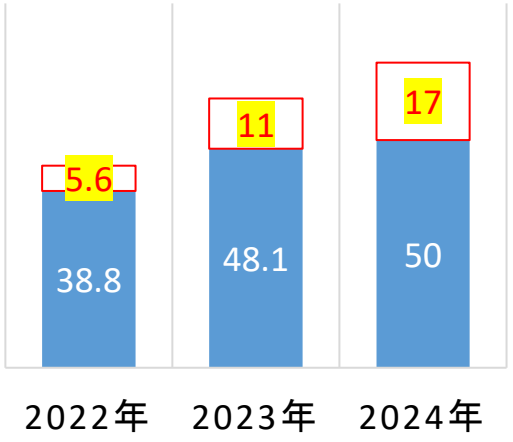
内閣官房 国家サイバー統括室
人材政策班

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育成・確保を図るため、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、現在フレームワーク案のパブリックコメントを進めているところ。

※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
（2026年2月17日（火）～3月10日（火））

諸外国の「人材フレームワーク」の例

- 諸外国ではサイバーセキュリティ人材について、職種（ロール）ごとにT（タスク）K（知識）S（スキル）を定義した人材フレームワークを整備し、人材育成に活用。
- 我が国の実情に沿った官民共通のサイバーセキュリティ人材フレームワークを、諸外国の事例も参考にしつつ策定し、官民一体となって効率的・効果的に人材確保・育成を推進。

✓ 諸外国のフレームワークにおける職種（ロール）数の比較

- 細分化することできめ細やかな人材定義ができる一方、活用場面が限定的な職種も生じる
- 雇用の流動円滑化やミスマッチを防ぐ観点からも、代表的な人材像の定義によるスキルの可視化が必要

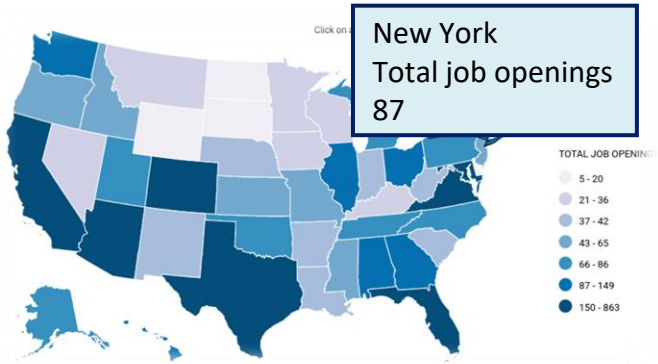
国等	策定年	職種数	LV分
米国	2017年初版、2024年改訂、2025年改訂	41	—
欧州	2022年公開	12	有
カナダ	2023年公開	22	—
豪州	2019年初版、2020年改訂	9	有

✓ フレームワークの活用例（米国）

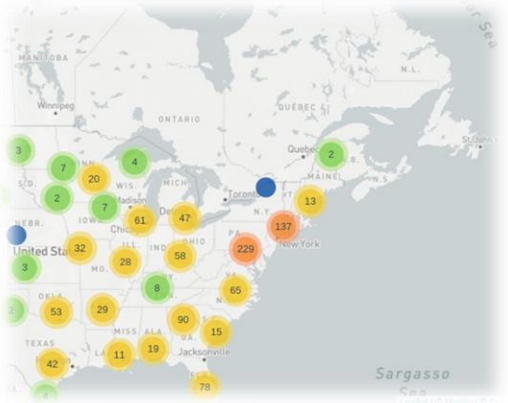
- 米国のCyberseekでは、NICEフレームワークに沿ったサイバーセキュリティ求人情報や教育サービスの検索が可能

（Cyberseek公式サイトにおける表示例）

求人数・採用要件（資格）の可視化



求人数を州単位でマップ表示



プロバイダー（研修事業者・大学等提供者）ごとにトレーニングセンター等の教育機関を地図上に可視化

（米）cyberseek：https://www.cyberseek.org/

（参考）米国 NICEフレームワークの41職種

- 米・国立標準技術研究所（NIST）が策定。
- サイバーセキュリティ分野の人材像を分類（5カテゴリー/41職種）、それぞれに求められるタスク（942）、知識（631）・スキル（538）を整理したもの。
- 産官学共通の枠組みとして、採用、教育等の幅広い場面で活用。

監督・統治
通信セキュリティ（COMSEC）マネージャー
サイバーセキュリティ・ポリシー・戦略プランナー
サイバーセキュリティ人材マネージャー
サイバーセキュリティ教育カリキュラム開発者
サイバーセキュリティ・インストラクター
サイバーセキュリティ法務アドバイザー
エグゼクティブ・サイバー・リーダーシップ
プライバシー・コンプライアンス・ マネージャー
プロダクト・サポート・マネージャー
プログラム・マネージャー
セキュア・プロジェクト・マネージャー
セキュリティ・コントロール・アセッサー
システム・オーソライザー
システム・セキュリティ・マネージャー
テクノロジー・ポートフォリオ・マネージャー
テクノロジー・プログラム監査人

設計・開発
サイバーセキュリティ・アーキテクト
エンタープライズ・アーキテクト
セキュア・ソフトウェア開発者
セキュア・システム開発者
ソフトウェア・セキュリティ・アセッサー
システム要件プランナー
システム試験・評価者
テクノロジー研究開発者
OTサイバーセキュリティ・エンジニア
導入・運用
データ・アナリスト
データベース・アドミニストレーター
ナレッジ・マネージャー
ネットワーク・オペレーター
システム・アドミニストレーター
システム・セキュリティ・アナリスト
テクニカル・サポート

保護・防衛
防衛サイバーセキュリティ
デジタル・フォレンジック
インシデント・レスポンス
インフラ・サポート
内部脅威分析
脅威分析
脆弱性診断
捜査
サイバー犯罪捜査官
デジタル・エビデンス・アナリスト

人材像	役割（タスク）：44タスクを要求	知識：88知識を要求	スキル：18スキルを要求
システム・セキュリティ・アナリスト	• セキュリティ管理の有効性評価 • 重要なテクノロジー調達用件の特定 • アプリケーション・サイバーセキュリティ・ポリシーの実装 • システム・サイバーセキュリティ・ポリシーの実装 （この他、40タスクが求められている）	• 暗号アルゴリズムに関する知識 • コンピュータネットワークプロトコルに関する知識 • リスク管理プロセスに関する知識 • サイバーセキュリティに関する法規制の知識 （この他、84知識が求められている）	• セキュリティシステム設計を評価するスキル • サプライヤーの信頼性を評価するスキル • 製品の信頼性を評価するスキル • ソフトウェア通信の脆弱性を特定するスキル • ユーザークレデンシャル管理システムを開発するスキル （この他、13スキルが求められている）

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。

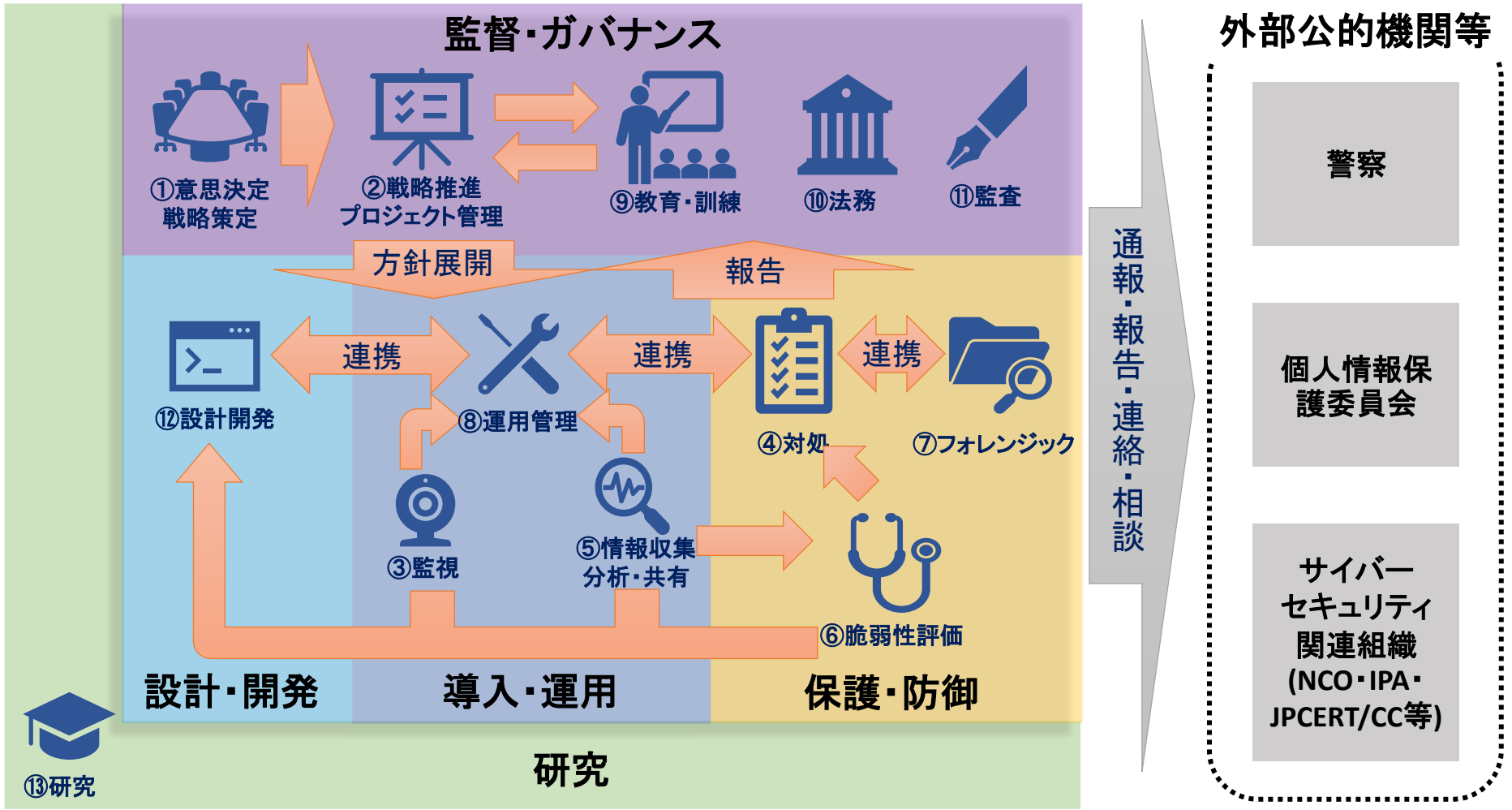
※　特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）が発行するSecBoK
　　産業横断サイバーセキュリティ検討会　人材定義リファレンス　　等

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。

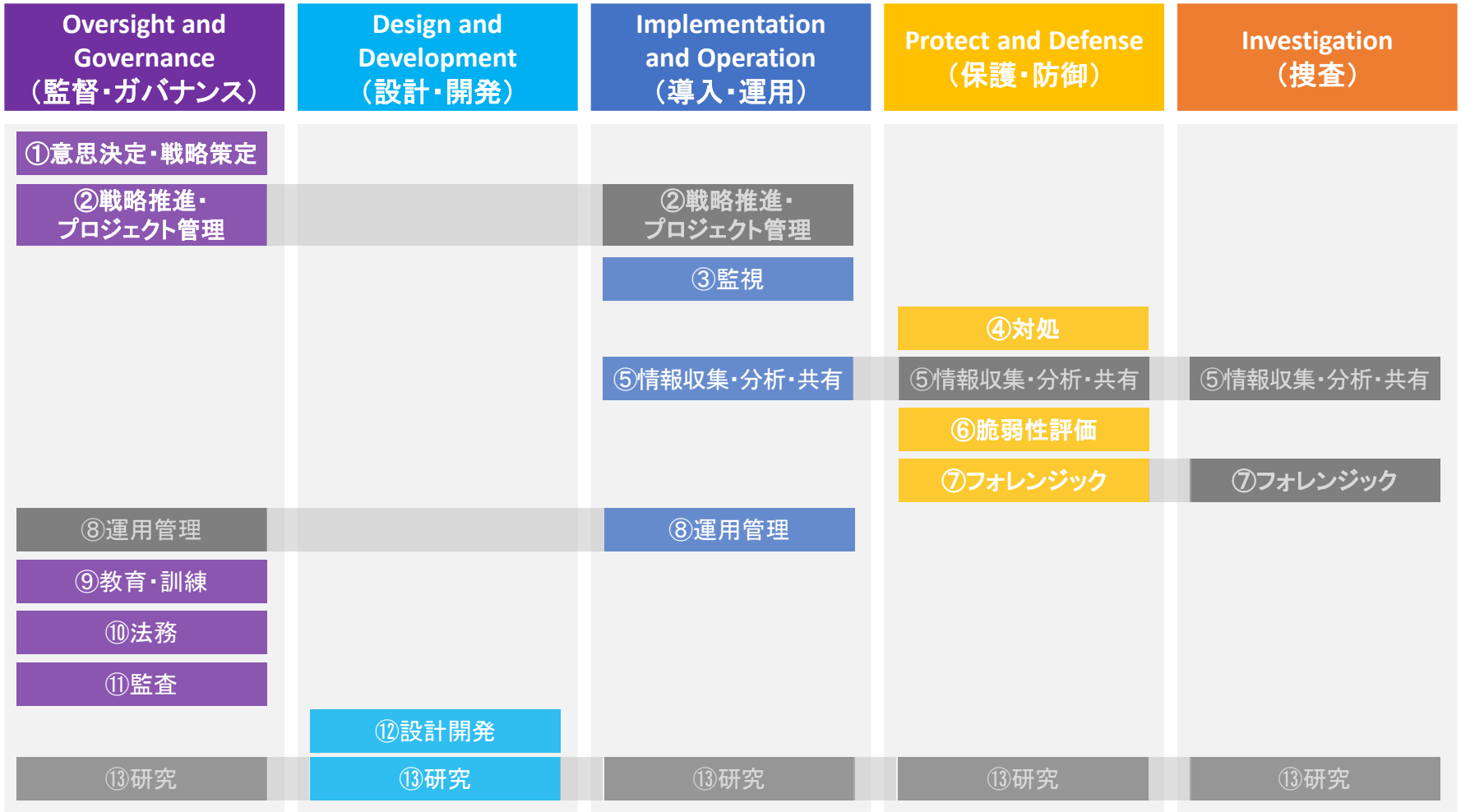
サイバーセキュリティ人材が担う役割の全体像

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**を定義



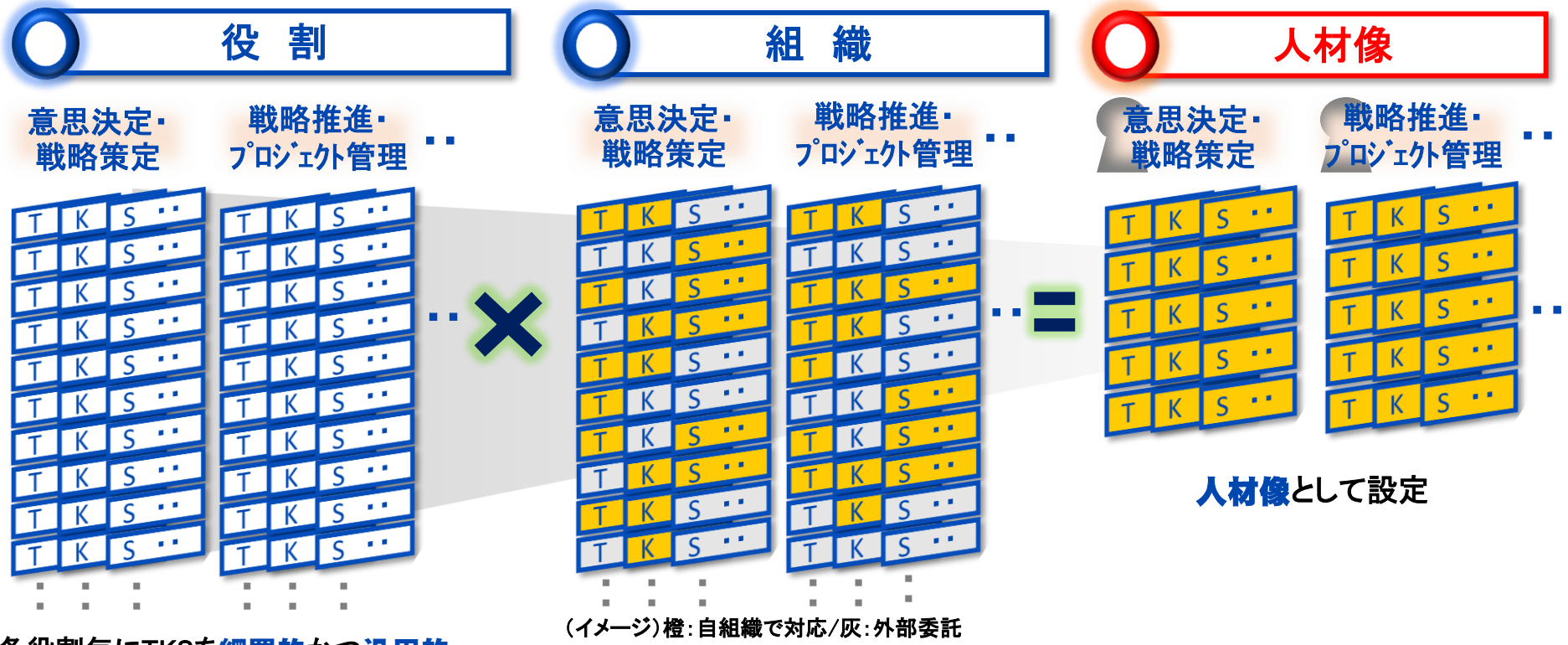
（参考）13の役割とNICEフレームワークのカテゴリとの関係



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

人材フレームワークのレベル設定について

人材の練度等に応じて、ITSS（ITスキル標準）のレベルと相互参照を図りながら、**4段階のレベル**を設定

レベル	人材フレームワークのレベルの定義	対応するITSSレベル
4	**業務における最終意思決定に対して責任を負う者** 条件：下記3点のうち2点以上を満たす者 ① 各役割で定義された知識に加え、業界全体やビジネスに関連する幅広い知識を持っている ② 組織全体を俯瞰して、各役割で定義された知識・スキルの向上を企画・立案することができる ③ サイバーセキュリティに関する実務経験が10年以上が望ましい	レベル4以上 （組織内や業界内等のハイレベルプレーヤ）
3	**業務を独力で遂行可能であり、かつマネジメントを行う者** 条件：下記3点のうち2点以上を満たす者 ① 各役割で定義された知識に基づき、組織内外の連携先と円滑な会話（説明・指導等による管理）ができる ② 各役割で定義されたタスクを実行できる ③ サイバーセキュリティに関する実務経験が4～10年程度が望ましい	レベル3 （独力で遂行可能）
2	**業務において指示に基づく作業を実行する者** 条件：下記3点のうち2点以上を満たす者 ① 各役割で定義された知識の概要に基づき、組織内外の連携先と会話ができる ② 他者の指示により、各役割で定義されたタスクを実行することができる ③ サイバーセキュリティに関する実務経験が2～4年程度が望ましい	レベル2 （指導の下で遂行可能）
1	**業務に対する最低限必要な知識を有する者** 条件：下記3点のうち2点以上を満たす者 ① 各役割で定義された知識のやキーワードを理解し、業務に必要な最低限の会話ができる ② 他者の指示により、各役割で定義されたタスクを実行することができる ③ サイバーセキュリティに関する実務経験が2年未満である	レベル1 （最低限必要な知識を有する）

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	● 小規模組織におけるおけるセキュリティ対策の考え方（役割に基づく体制の一例等） ● モデルケースに基づく活用例　等
② 大規模組織 例：中堅・大企業、政府機関 等	● 担当者を採用するときの職務記述書の作成方法 ● レベルを踏まえた人事評価等にあたっての活用方法　等
③ 教育機関 例：大学、教育事業者 等	● 輩出したい人材像を定めて、知識・スキルを段階的に習得するためのカリキュラムの作り方（作成にあたっての考え方）　等
④−1 個人（専門人材） 例：専門人材、専門人材を目指す学生等	● 専門人材に求められるスキルセットを踏まえたセルフアセスメントの実施方法 ● スキルギャップを埋めるための学習方法　等
④−2 個人（プラス・セキュリティ人材）	● 各役割の概要 ● プラス・セキュリティ人材に求められるスキルセットを踏まえたセルフアセスメントの実施方法 ● スキルギャップを埋めるための学習方法　等

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した上で、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	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	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 ● 人材サービス事業者（採用）		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

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。

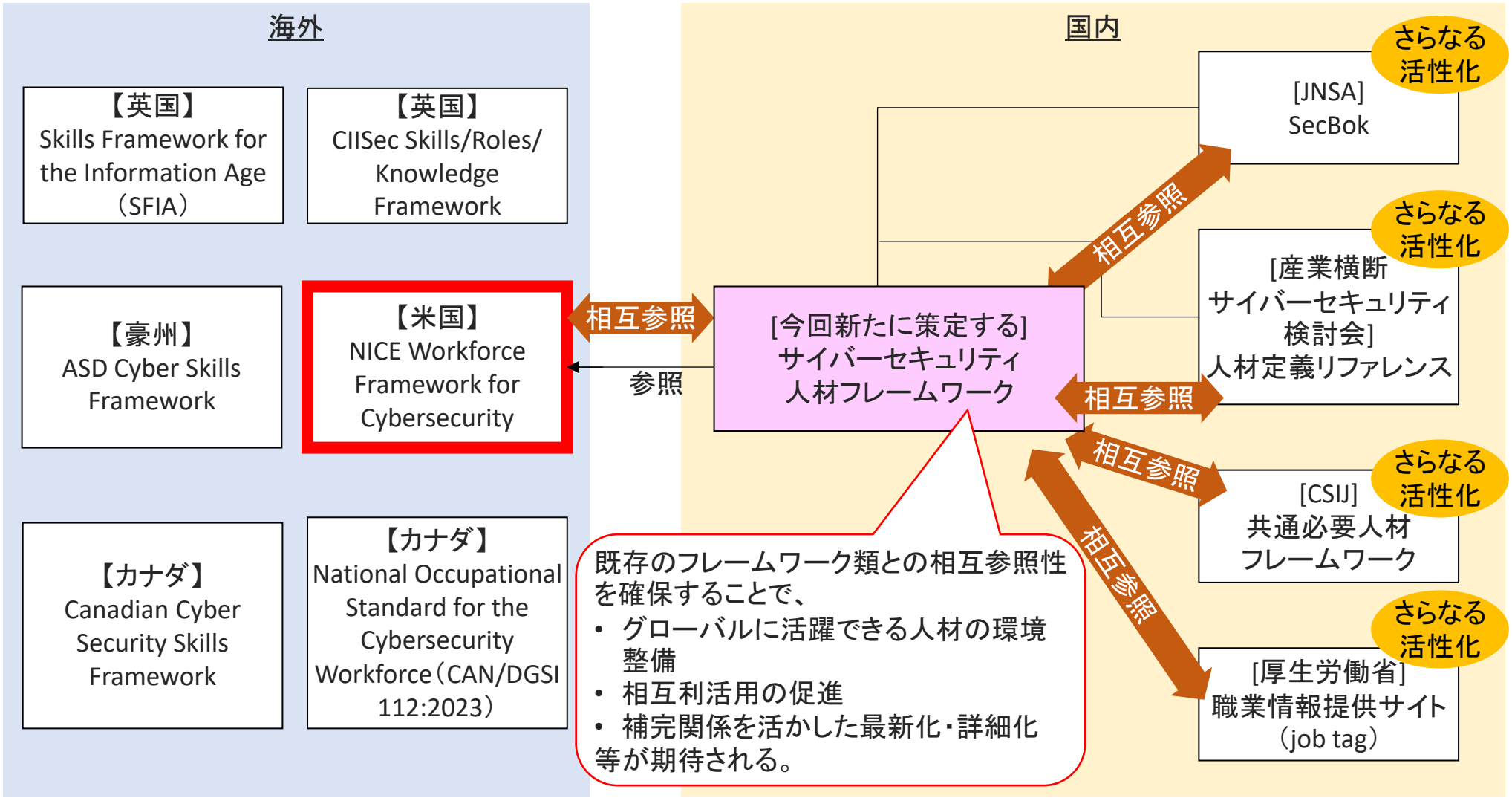
様々な主体によって行われる**教育・訓練について、フレームワークとの関連付けを強化**する。具体的には、**資格試験の合格や実践的演習の修了等といった成果と、フレームワークにおける人材像・レベルとの関連付け**を推進し、参加者のスキルの可視化を促進できる仕組みとするとともに、教育・訓練のカリキュラム設計にも活用する。政府においては、**政府デジタル人材のスキル認定制度と連携**を図るなど、フレームワークを基盤として適切な評価制度の整備や人材の適正配置を促進する。

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。

参　考

国内外のフレームワーク類との関係性（イメージ）

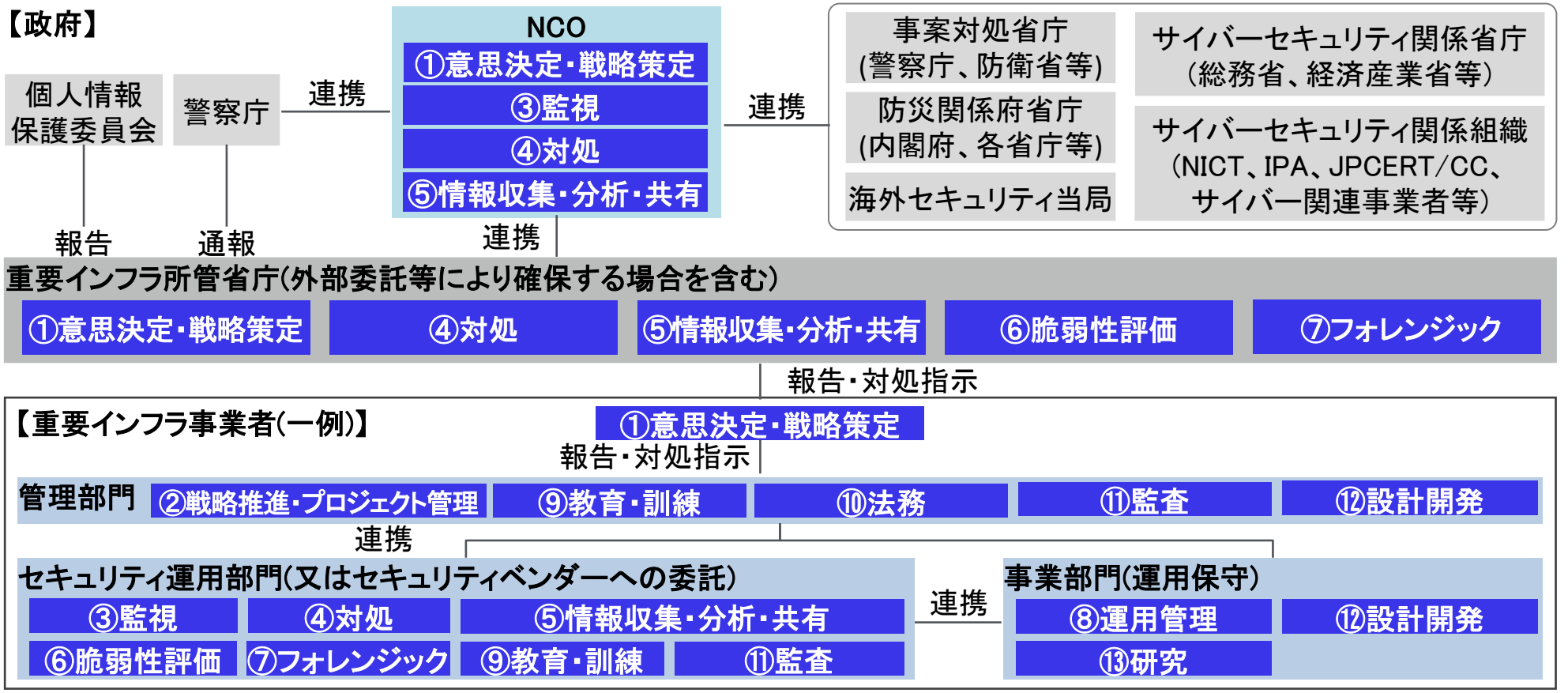
（国内外の既存のフレームワークとの相互参照イメージ）



人材像の設定（案）（例：重要インフラ事業者向け対処体制）

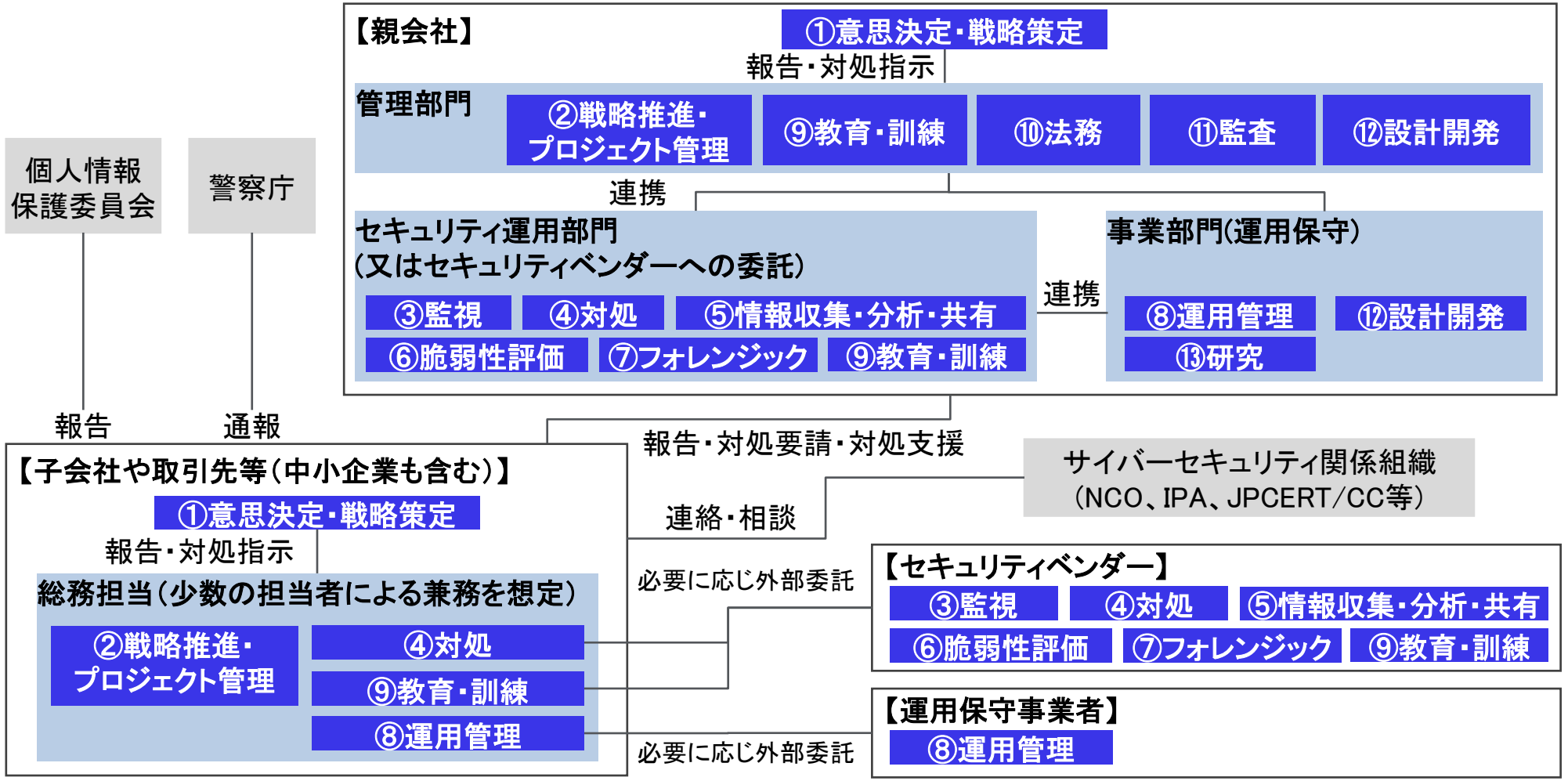
- 重要インフラ企業がサイバー攻撃を受けた状況において、官民が連携して事案対処を行う場面（下図）において求められる役割から、13の人材像を設定。
- 役割ごとにT（タスク）、K（知識）、S（スキル）を定義の上、4段階にレベル分け。

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。