資料4

事務局説明資料

令和７年１０月１４日

内閣官房
国家サイバー統括室
人材政策班

人材フレームワーク策定及び利活用等の基本的考え方（案）

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。
- 我が国のサイバーセキュリティ人材の必要数・不足数は増加傾向という民間調査結果※もあることから、効率的・効果的にサイバーセキュリティ人材の育成・確保を図るための取組が必要。

サイバー空間を巡る脅威に対応するため喫緊に取り組むべき事項（令和7年5月29日　サイバーセキュリティ戦略本部決定）

（サイバーセキュリティを支える人的・技術的基盤の強化）

〇官民を通じたサイバーセキュリティ人材の確保・育成

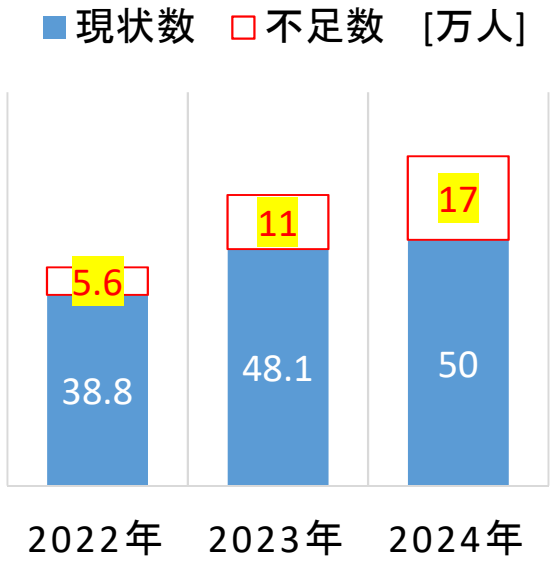
様々な領域において、マネジメントから実務まで、サイバーセキュリティに関して求められる枠割・スキルが多様化しているところ、それを担う人材の育成確保が、官民を通じて急務となっている。

（中略）

我が国全体として効率的・効果的にサイバーセキュリティ人材の育成・確保を図る観点から、（中略）求められる役割・スキル等を整理した官民共通の「人材フレームワーク」策定に向けた議論を開始し、年度内に結論を得る。

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

諸外国の人材フレームワークの動向

諸外国において人材に求められる知識・スキル等を体系的に整理した枠組（フレームワーク）を整備し、産官学における効果的な人材育成・確保に役立てられている。

NICEフレームワーク

国立標準技術研究所（NIST）発行：2017年公開

- ✓セキュリティに必要な人材像を41に分類し、その職務内容、必要な知識、技能※を整理
  - ※　防御側だけでなく、サイバー作戦の計画や実行に関する技能を含む。
- ✓採用・人事（キャリアパスを含む）での活用の他、教育プログラムや資格等の対応関係を整理
- ✓各種データ（人材需給、資格保有等）の作成・分析に活用
- ✓スキルレベルの定義なし

欧州サイバーセキュリティ・スキル・フレームワーク

欧州連合サイバーセキュリティ機関（ENISA）発行：2022年公開

- ✓セキュリティに必要な人材像を12に分類し、その職務内容、求められる知識・技能等を整理
- ✓採用・人事での場面の他、教育プログラムや資格等の対応関係を整理する際に活用
- ✓各種データ（人材需給、スキル保有等）の作成・分析に活用
- ✓スキルレベルの定義あり

カナダ・サイバーセキュリティ・スキル・フレームワーク

カナダサイバーセキュリティセンター（CCCS）：2023年公開

- ✓NICEフレームワークを国内事情を踏まえ簡素化、セキュリティに必要な人材像（専門領域を除く）を22に分類し、その職務内容や求められる知識・技能等を整理
- ✓採用・人事、教育プログラム等への活用を想定
- ✓スキルレベルの定義なし

ASDサイバー・スキル・フレームワーク

豪州通信情報局（ASD）発行：2019年公開

- ✓英国のフレームワーク等を参考に、ASD及び関係政府機関、産業、学術機関向けに、特に専門性の高い9つの人材像を定義し、求められる能力・技能・習熟レベル等を整理
- ✓採用・人事（キャリアパスモデル含む）での活用の他、教育プログラムや資格等の対応関係を整理
- ✓スキルレベルの定義あり

※ 日本国内では、独立行政法人情報処理推進機構（IPA）が策定する「ITスキル標準（ITSS）」や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）が策定する「SecBoK」等がある。

米国 NICEフレームワークの例

- 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人材像）、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

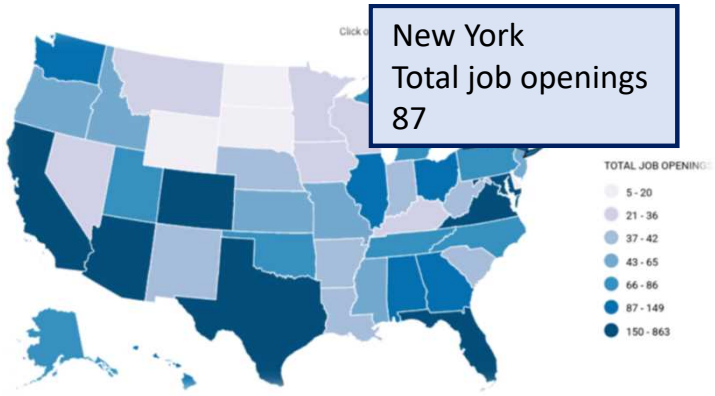
保護・防衛
防衛サイバーセキュリティ
デジタル・フォレンジック
インシデント・レスポンス
インフラ・サポート
内部脅威分析
脅威分析
脆弱性診断
捜査
サイバー犯罪捜査官
デジタル・エビデンス・アナリスト

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）

フレームワークの活用事例（米国「CyberSeek」の例）

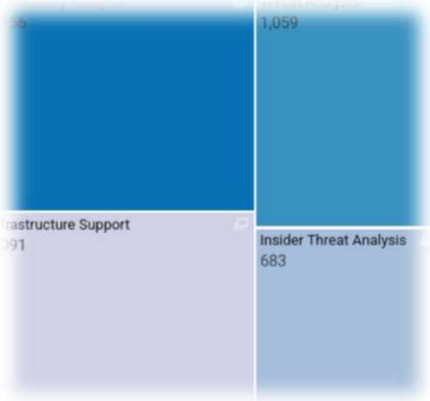
採用情報

✓ **求人数・採用要件（資格）の可視化**

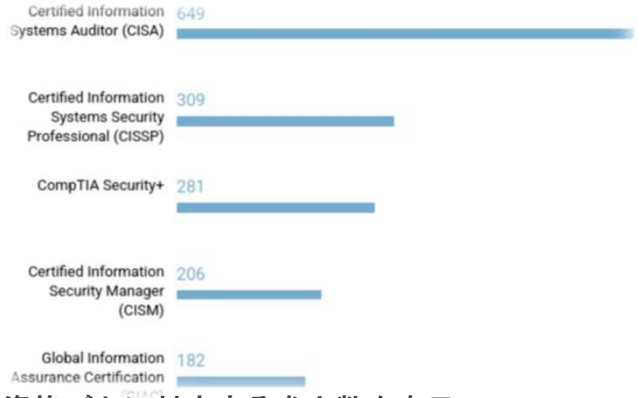


求人数を州単位でマップ表示

NY×パブリックセクター（連邦政府職員）で検索した場合の表示例



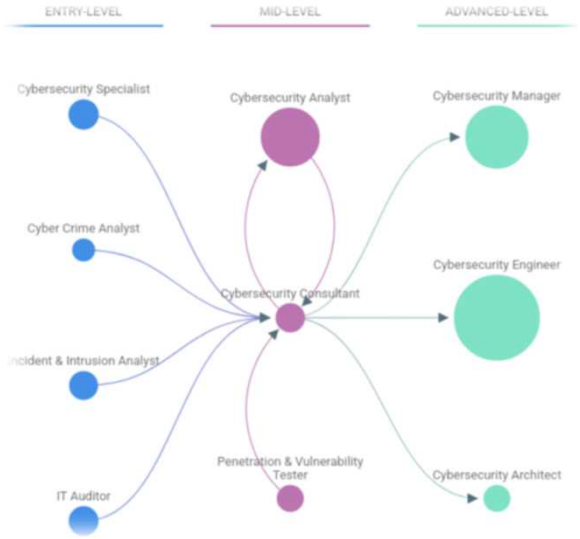
求人数をNICEフレームワークのロールごとに表示



資格ごとに対応する求人数を表示

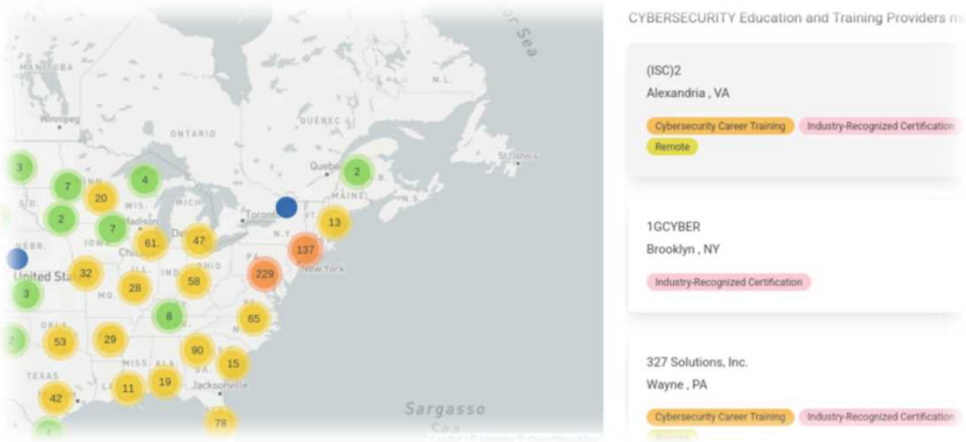
キャリアパス

✓ **キャリアパスの可視化**（3つのレベルに分類）



教育情報

✓ **教育機関の可視化**



諸外国の人材フレームワークの比較

- 人材像を多く設定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人材像も生じる
- 練度の違いをレベルで表現しているフレームワークもある
- これらを踏まえ、我が国のフレームワークは如何にあるべきか

国等	フレームワーク名	策定年	人材像数	レベルの定義
米国	NICEフレームワーク	2017年初版、2020年、2025年改訂	41	なし
欧州	欧州サイバーセキュリティ・スキル・フレームワーク	2022年公開	12	あり
カナダ	カナダ・サイバーセキュリティ・スキル・フレームワーク	2023年公開	22	なし
豪州	ASDサイバー・スキル・フレームワーク	2019年初版、2020年改訂	９	あり
我が国における視点（例）	―	―	活用を見据えた適切な数・粒度は如何にあるべきか	練度を表現できるようにしてはどうか

我が国における人材フレームワーク策定及び利活用等の基本的考え方（案）

① 活用を見据えた人材像の設定

- 社会のさまざまな場面での活用を見据え、実用的な人材像の数・粒度を設定。
- 同一の人材像において練度の違いを反映できるよう、レベルの概念を設ける。

② 既存の国内外のフレームワーク類との相互参照性の確保

- （国際的にも著名な）米国のNICEフレームワークを参照の下、我が国の実情を踏まえ、NICEにおけるロールを整理統合し、我が国における人材像およびTKS（Task,Knowledge,Skill）を設定。
- 諸外国の既存フレームワークとの連携も見据え、本年１月に参画した、サイバーの専門家基準に係る国際標準化等を目的とした枠組み「サイバーセキュリティに関する国際的な連合（ICCSW）」とも連携。
- 国内のフレームワーク類（SecBoK等）とも相互参照を図ることで、相互利用の促進や、補完関係を活かした内容の詳細化・最新化等を図る。（P9）

③ フレームワークの性質

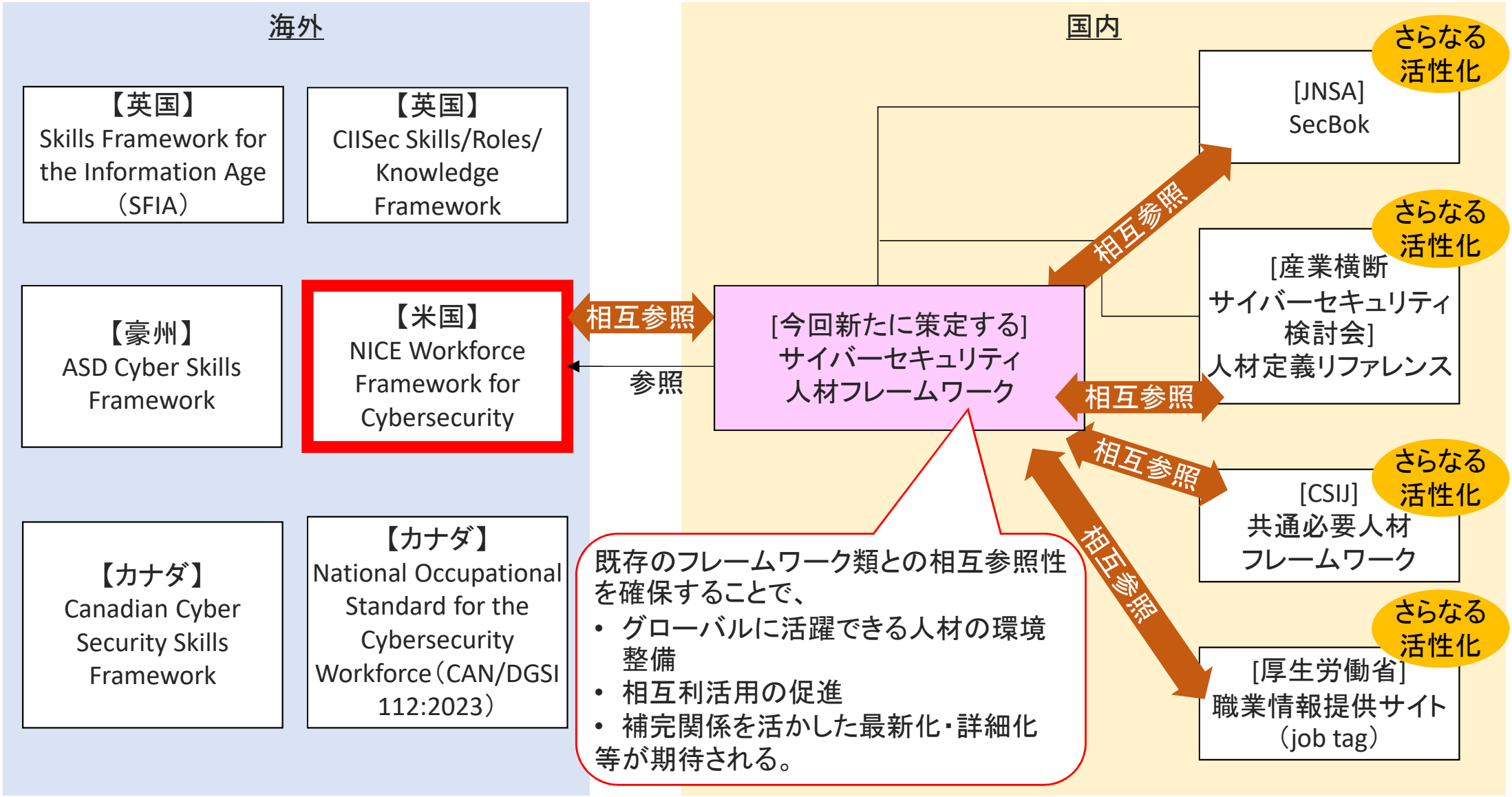
- 画一的な人材育成を目的としたものではなく、フレームワークを参考に、現場の実情を踏まえつつ、個々の状況に応じてカスタマイズして活用するもの。
- 各組織でのフレームワーク活用を支援する手引き書を整備。
- 技術の進展等今後の社会情勢の変化を踏まえ、必要に応じて見直しを図ることとする。

④ 策定後の利活用等（P10）

- 官民問わず、自組織のサイバーセキュリティ人材の定義に活用。
- 求人（採用）や評価、配置、キャリアパスの可視化等人材マッチングに係る様々な場面で活用。
- フレームワークを軸に、大学等の高等教育や職業訓練、社会人の能力開発や高度専門人材の育成に至るまで、様々な育成施策を有機的に連携させ、体系的かつ継続的な学びの環境を整備。

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）



人材フレームワークの利活用例

1. 人材定義の推進

人材フレームワークにおける人材定義（TKS）や手引書を参照し、各組織で必要となるサイバーセキュリティ人材の定義を明確化

- 専門知識や実践スキルを備えた高度人材の育成・確保
- 政府機関等の中核的な対処人材の育成への活用
- 研修や演習の充実・強化等の育成施策、政府人材の官民交流や外部の高度専門人材を登用する仕組みの効率的・効果的な運用

2. 人材のマッチング

人材の需要・供給状況や教育・訓練機関の情報の網羅的かつ一元的な可視化

- キャリアパスを可視化し、人材を活用しようとするさまざまな組織等における採用・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
- 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等、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

3. 教育・訓練への活用

さまざま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

- 資格試験の合格や実践的演習の修了等といった成果と、人材像・レベルとの関連付けを推進し、人材のスキル可視化につなげる
- 職業訓練において、参加者に応じた必要な知識・スキルが習得可能なカリキュラムを設計

「人材像」の呼称（案）

■ 既存のフレームワーク類ではさまざまな呼称が用いられているところ、本検討会では「人材像」を用いている。

	採用しているフレームワーク	定義・背景等	名称採用のメリット	名称採用のデメリット
人材像	ITSS（METI） 統合セキュリティ人材モデル （NEC・日立・富士通）	–	ITSSで古くから使われており、なじみがある。	部分的な兼務者を「人材像」で表現すると多くのケースで不自然になる。
人材類型 職種	共通キャリアスキルフレームワーク （IPA）	7種類の「人材類型」の中に複数の「職種」を定義。	「職種」は実際に存在するものであれば、人材側から見るとわかりやすい。	部分的な兼務者を「職種」で表現すると多くのケースで不自然になる。
人材類型 ロール	DX推進スキル標準（DSS-P）	5種類の「人材類型」の中に複数の「ロール」を定義。	兼務が多く見込まれるDX担当者を表象する名称として違和感がない。	メンバーシップ雇用主体の国内で「ロール」という概念があまり認知されていない。
分野	ITSS+（セキュリティ領域） （METI、IPA）	プラス・セキュリティを考慮した場合、人材像とするのが適切でないため、あえて「分野」として定義。	「分野」は専任・兼務のいずれも実態を表象する名称として違和感がない。	従事する人材を表象する概念であることが伝わりにくい。
タスクプロフィール	iCDタスクディクショナリ （IPA→iCDA）	ビジネスタイプ、開発対象などからタスクを参照する切り口を表す。	業務で求められるタスクのまとまりとして正確な表現である。	一般になじみがない用語であり、わかりにくい。
職種	iCDスキルディクショナリ （IPA→iCDA）	代表的な職種を表す。	「職種」は実際に存在するものであれば、人材から見るとわかりやすい。	部分的な兼務者を「職種」で表現すると多くのケースで不自然になる。
役割（担当） 担当職	人材定義リファレンス（産業横断サイバーセキュリティ研究会）	「担当職」は管理職以外の担当者に相当。経営層・管理職等は「役割」で表現。	「担当」は専任・兼務のいずれも実態を表象する名称として違和感がない。	「担当」は一時的なニュアンスが強く、中長期での育成との親和性に難がある。
ロール（役割）	SecBoK（JNSA）	NICEが「Work roles」を用いていることに準拠。	NICEとの親和性が高く、兼務を表象する名称としても違和感がない。	メンバーシップ雇用主体の国内で「ロール」という概念があまり認知されていない。
Work roles	NICE cybersecurity workforce framework	–	–	–

■ 論点①：活用を見据えた人材像の設定（P8①）
- 諸外国のフレームワークも踏まえつつ、我が国として使いやすいものとするための実用的な人材像の数・粒度、レベル設定はいかにあるべきか

■ 論点②：既存の国内外のフレームワーク類との相互参照性の確保（P8②）
- NICEフレームワークを参照しつつ、内外の各種フレームワーク類との「ハブ」的な位置づけを目指す考え方（P8）は妥当か

■ 論点③：フレームワークの性質（P8③）
- 記載した内容で抜けている視点はないか

■ 論点④：策定後の利活用等（P8④）
- P9に記載した内容含め、抜けている視点はないか

■ 論点⑤：「人材像」の呼称について（P11）
- 他の呼称含め、妥当な呼称はないか

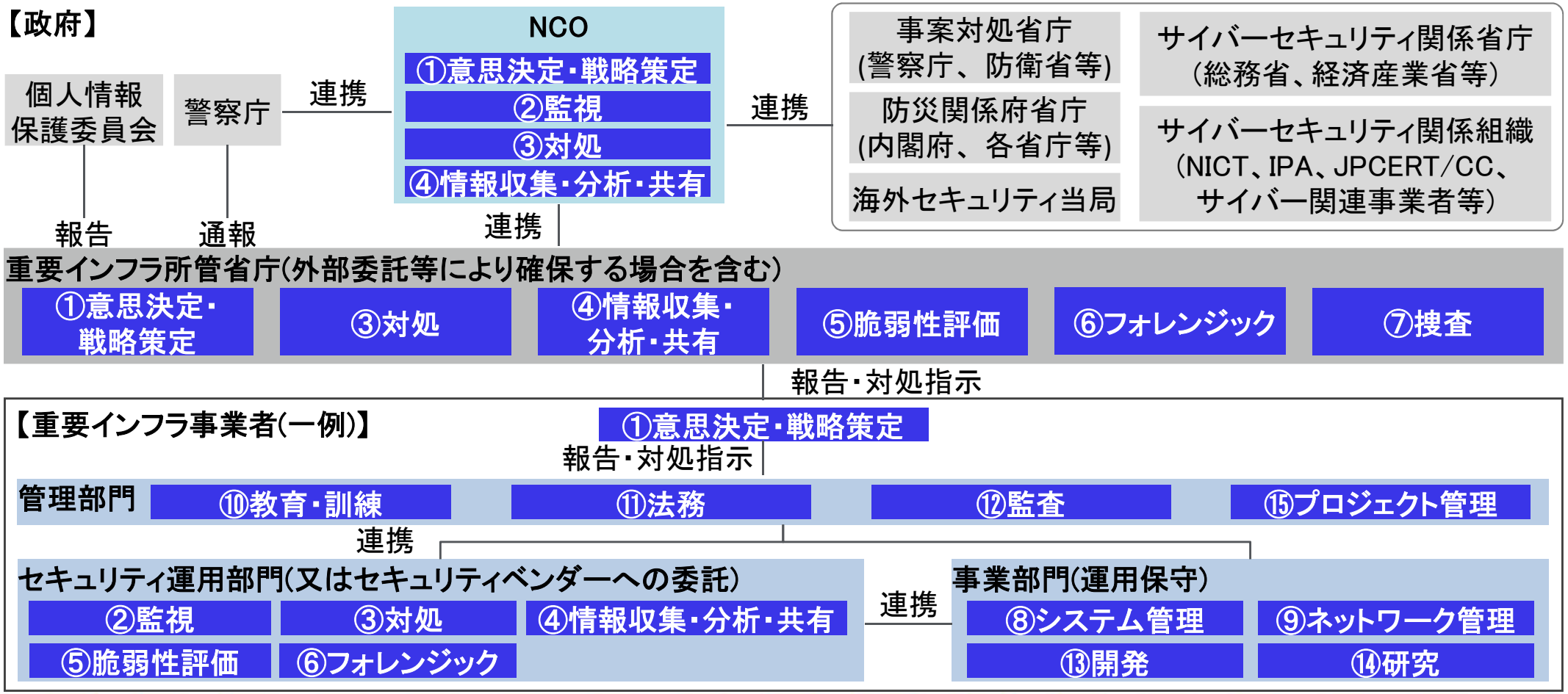
人材像の設定（案）

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、15の人材像を設定。
- 人材像ごとに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。
- これらの人材像は自組織の人材に限らず、外部委託等で確保する場合も想定する。

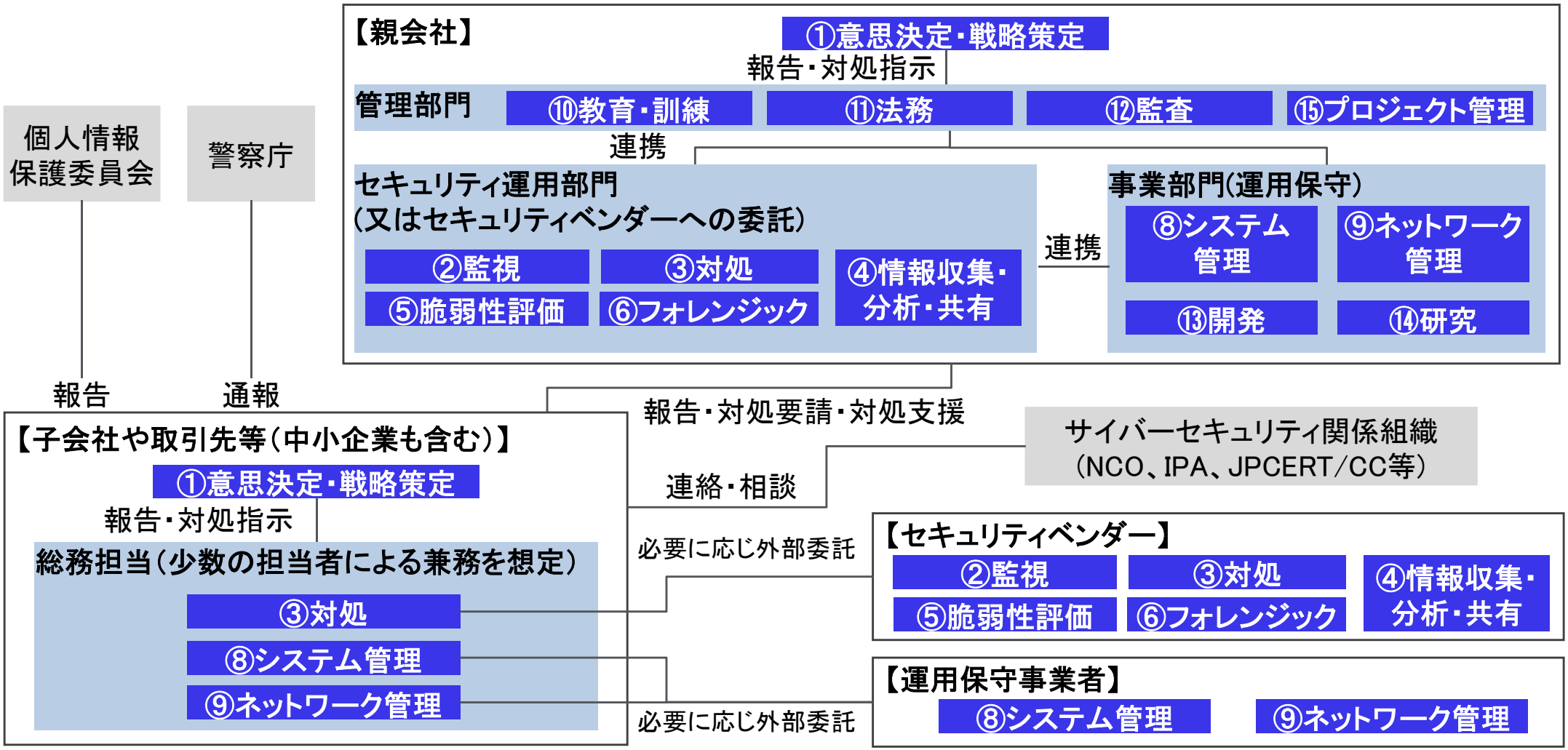
① 意思決定・戦略策定　② 監　視　③ 対　処　④ 情報収集・分析・共有　⑤ 脆弱性評価　⑥ フォレンジック　⑦ 捜　査　⑧ システム管理

⑨ ネットワーク管理　⑩ 教育・訓練　⑪ 法　務　⑫ 監　査　⑬ 開　発　⑭ 研　究　⑮ ﾌﾟﾛｼﾞｪｸﾄ管理



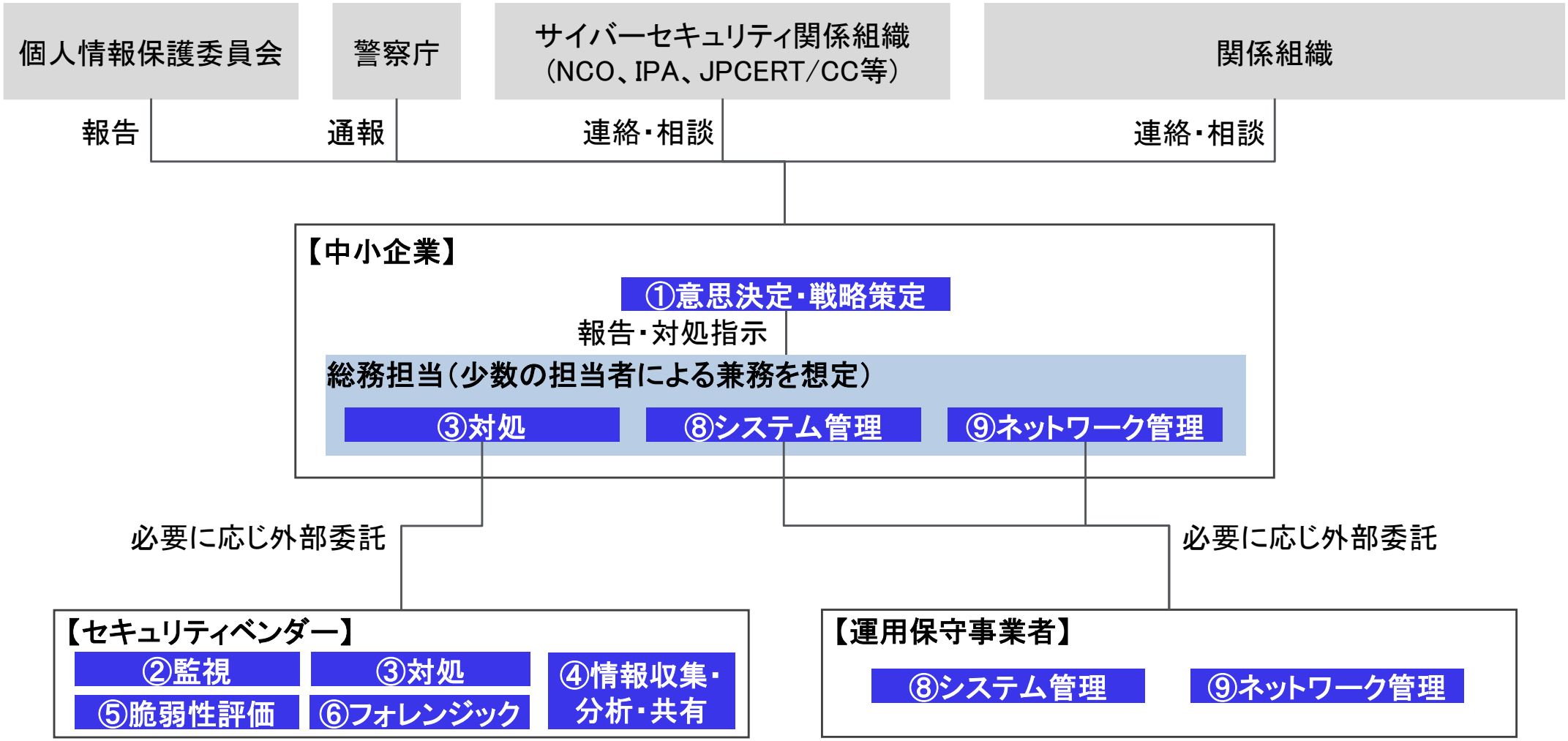
（参考）活用例①：サプライチェーン関係者間の連携

- 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。



人材像及びタスク・知識・スキル（TKS）の例（③対処のケース）

人材像 ③対処　**役割** サイバーセキュリティインシデント発生時、影響の拡大を防止すると共に、発生したインシデントに対する調査、分析、評価、復旧を行う。

タスク（T）：11タスクを設定	知識（K）：10知識を設定	スキル（S）：13スキルを設定
インシデント対処準備（情報収集、注意喚起、対応マニュアル作成、CSIRT訓練の実施等）	インシデント対処活動の手順や手法に関する知識	自組織が所有する機器の仕様の理解（アクセス制御リスト、ネットワーク監視ツール等）、必要資材の調達、チーム編成、基本的なツールの準備等を行い、事業活動の継続を第一としたインシデント対処のプロセスを策定するスキル
インシデントの報告受領	組織のサイバーセキュリティ体制、役割に関する知識	インシデントを検知した自組織内/外のサイバーセキュリティ関係部署から報告を受け、インシデント対応が必要か否かを判断するスキル
初動対応時におけるインシデントの速報の報告（CISO、経営層）	インシデント速報の報告手順・対象に関する知識	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
（この他、8タスクを設定）	（この他、7知識を設定）	（この他、10タスクを設定）

人材像レベル（案）

- 本フレームワークを採用や育成等のさまざまな場面で活用できるよう、人材像のレベルを責任や経験年数、知識・スキルの成熟度に基づき、4段階のレベルに定義。
- 他方、組織規模や対処レベルに応じてレベル設定を調整する必要があるとも考えられる（後述）。

レベル	人材像レベルの定義
3	責任：当該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「当該人材像」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「当該人材像」で定義されたスキルについて、チーム全体のスキルアップを計画することができる ③ 15人材像いずれかの業務における実務経験が10年以上である
2	責任：当該業務において下位者に対するマネジメント及び該当領域における重要な情報を上位者へ報告する責任を負う者 条件：下記3点のうち2点以上を満たす者 ①「当該人材像」で定義された知識について、他者に対して説明・指導ができる程度の理解をしている ②「当該人材像」で定義されたスキルをすべて習得している ③ 15人材像いずれかの業務における実務経験が4～10年である
1	責任：当該業務において割り当てられた指示に基づく作業を実行する責任を負う者 条件：下記3点のうち2点以上を満たす者 ①「当該人材像」で定義された知識の概要やキーワードを理解している ② 他者の指示により、「当該人材像」で定義されたスキルを活用することができる ③ 15人材像いずれかの業務における実務経験が1～3年である
0	責任：新卒や未経験入社の者

NICEフレームワークとの関係

NICEフレームワークのワークロールを紐付け、相互参照を図る。

人材像	NICEフレームワークのワークロール名	ワークロールID
①意思決定・戦略策定	サイバーセキュリティポリシーと計画	OG-WRL-002
	エグゼクティブサイバーセキュリティリーダーシップ	OG-WRL-007
	システム認証	OG-WRL-013
	テクノロジーポートフォリオ管理	OG-WRL-015
	セキュリティコントロール評価	OG-WRL-012
②監視	脅威分析	PD-WRL-006
	ディフェンシブサイバーセキュリティ	PD-WRL-001
③対処	インシデントレスポンス	PD-WRL-003
④情報収集・分析・共有	データ分析	IO-WRL-001
	ディフェンシブサイバーセキュリティ	PD-WRL-001
	脅威分析	PD-WRL-006
	ナレッジ管理	IO-WRL-003
⑤脆弱性評価	脆弱性分析	PD-WRL-007
⑥フォレンジック	デジタルフォレンジック	PD-WRL-002
⑦捜査	サイバー犯罪捜査	IN-WRL-001
⑧システム管理	製品サポート管理	OG-WRL-009
	システムセキュリティ管理	OG-WRL-014
	データベース管理	IO-WRL-02
	システム管理	IO-WRL-005
	システムセキュリティ分析	IO-WRL-006
	技術的サポート	IO-WRL-007
	インフラストラクチャサポート	PD-WRL-004
⑨ネットワーク管理	通信セキュリティ（COMSEC）管理	OG-WRL-001
	ネットワーク運用	IO-WRL-004
	製品サポート管理	OG-WRL-009

人材像	NICEフレームワークのワークロール名	ワークロールID
⑩教育・訓練	サイバーセキュリティ人材管理	OG-WRL-003
	サイバーセキュリティカリキュラム開発	OG-WRL-004
	サイバーセキュリティ指導	OG-WRL-005
⑪法務	サイバーセキュリティ法的助言	OG-WRL-006
	プライバシーコンプライアンス	OG-WRL-008
⑫監査	技術プログラム監査	OG-WRL-016
	セキュリティコントロール評価	OG-WRL-012
⑬開発	サイバーセキュリティアーキテクチャ	DD-WRL-001
	エンタープライズアーキテクチャ	DD-WRL-002
	セキュアなソフトウェア開発	DD-WRL-003
	セキュアなシステム開発	DD-WRL-004
	ソフトウェアセキュリティ分析（ソフトウェアセキュリティ評価）	DD-WRL-005
	システム要件計画	DD-WRL-006
	システムテストと評価	DD-WRL-007
⑭研究	技術研究開発	DD-WRL-008
⑮プロジェクト管理	プログラム管理	OG-WRL-010
	セキュアなプロジェクト管理	OG-WRL-011
	ナレッジ管理	IO-WRL-003

人材像設定（案）に関しご議論いただきたい点

■ 論点①：人材像定義やレベル設定の妥当性
- ご意見いただきたいポイント：
  - 提示した体制、人材像（役割、タスク、知識、スキル、レベル）が国内のさまざまな業種・場面等に適用可能か（汎用性）
  - 現場の実態に照らし、主要な人材像の設定に不足がないか
  - 組織規模や対処レベルに応じてレベル設定を調整する必要があるか（セキュリティベンダや大企業におけるレベル3と一般企業におけるレベル3は同じか）（P18）
  - 専門知識や実践スキルを備えた高度な人材像（例：「脅威ハンティング」等）の検討要否

■ 論点②：兼務実態への対応（P15、16参照）
- ご意見いただきたいポイント：
  - 兼務人材は社会全体では非常に多く存在すると考えられるところ、本フレームワークを使い、どのように推進することが妥当か

（案1）今後策定する手引書等に複数の人材像を組み合わせた兼務人材の設定方法を「ひな形」的に例示する

（案2）兼務者の人材像を15の人材像とは別にフレームワーク内に設定する

■ 論点③：セキュリティ専門人材だけでなくプラス・セキュリティ人材の育成・確保
- ご意見いただきたいポイント：
  - プラス・セキュリティ人材の育成・確保にフレームワークを活用するための方策