資料4

人材像（案）の修正案について

令和７年１２月１８日

内閣官房
国家サイバー統括室
人材政策班

人材像（案）の修正案について

第１回会合における主な御意見

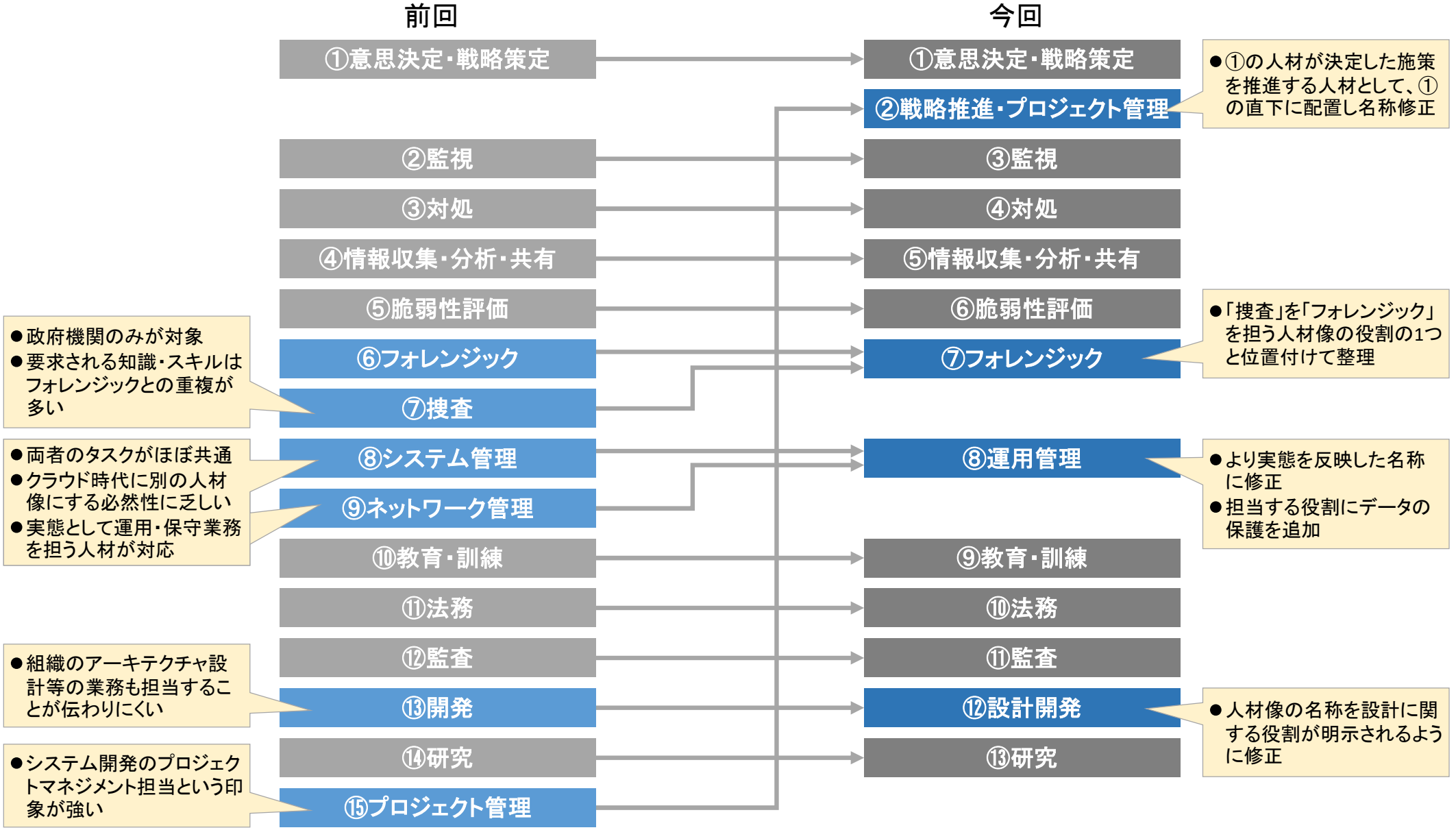
- 「対処」のタスクは単純なインシデント対応にとどまらないはず。
- 「開発」がコーディングに寄りすぎており、もっとアーキテクチャ設計の観点を盛り込むべき。
- サイバースペースインテリジェンスは「情報収集・分析・共有」で収まらない可能性がある。
- NICEのワークロールでは、どこを自動化できそうか、AIで代替できるかの検討が行いやすいが、現状の人材像案では曖昧になってしまう。

御指摘を踏まえた修正案

- 以下の各人材像（案）について名称を含む修正を検討。
  - ✓ **「システム管理」**及び**「ネットワーク管理」**：類似のタスクが多く、クラウド時代に区別の必要性が薄れていることを踏まえ**「運用管理」**として統合し、データ保護の要素を追記
  - ✓ **「開発」**：委員御指摘を踏まえ、**「設計開発」**に名称を変更し、企画設計関連のタスクを追加
  - ✓ **「プロジェクト管理」**：単なるプロジェクト管理でなく、「意思決定・戦略策定」による決定を受けて推進する人材として名称を**「戦略推進・プロジェクト管理」**にするとともに列挙順を**②番目に変更**
  - ✓ **「捜査」**：**「フォレンジック」**における役割の一部として整理
- サイバーセキュリティインテリジェンスについては、今後人材像毎のTKSを具体化する過程において必要に応じてタスクを追加する方向。
- 人材像定義において、NICEのロールとの対応関係を明示することにより、AI代替等の検討等を行いやすくなるよう配慮。

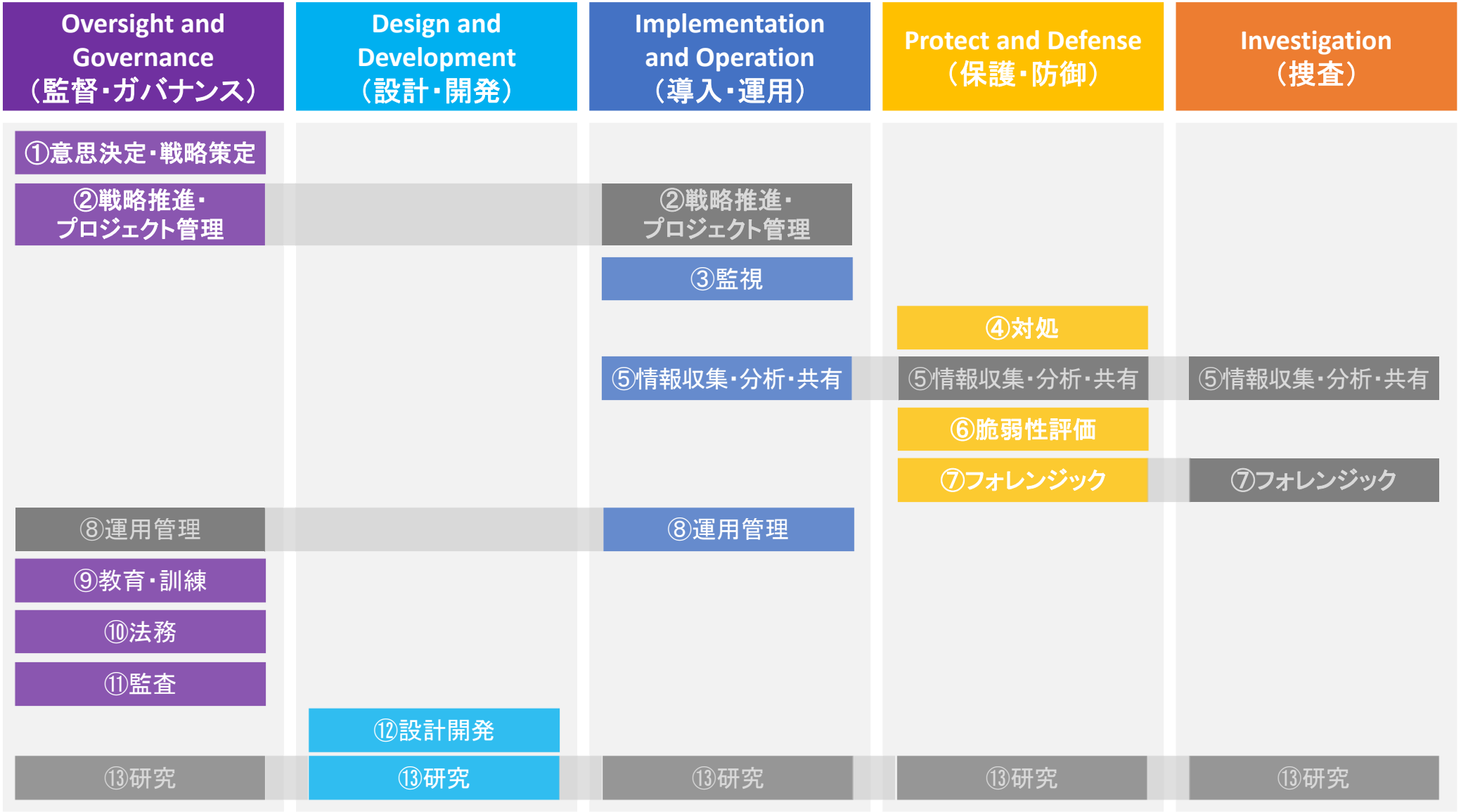
人材像（案）の修正案について

■ 水色で示した人材像を対象に修正（全体で15種類から13種類に変更）



人材像（案）の修正案について

■ NICEフレームワークのカテゴリ別に、13の人材像を整理すれば以下のとおり（グレーは一部含む）。



人材像(案)の修正案(1/13)

①意思決定・戦略策定	当該役割を担う人材が所属する組織				
	政府機関	民間企業(サプライチェーン)		民間企業(アウトソース先等)	
		親会社等	子会社等	セキュリティベンダー	運用保守事業者
	●	●	●	●	●

おもな役割	● 組織のサイバーセキュリティ戦略やポリシー等を策定する。 ● 組織のサイバーセキュリティに係る予算を確保し、組織体制を構築する。 ● 組織のシステムに対する責任を持つ。	
NICEフレームワークにおける対応ロール	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
	システム認可	OG-WRL-013
	テクノロジーポートフォリオ管理	OG-WRL-015
	セキュリティ管理策評価	OG-WRL-012
補足説明	● CISO及びその補佐役に相当。 ● 原則として外部委託による対応はできず、自組織にて責任を負うべき人材像である。 ● セキュリティポリシー策定等を外部委託にて実施する場合でも、ポリシー策定の責任は自組織で負う必要がある。 ● サプライチェーンのセキュリティ確保において、親会社やサプライチェーンを統括する企業が子会社その他の企業のセキュリティ対策に関する戦略決定を包括的に担う場合もある。 ● インシデント発生時の意思決定も実施し、④を担う人材に指示を行う。	

人材像（案）の修正案（2/13）

②戦略推進・プロジェクト管理	当該役割を担う人材が所属する組織				
	政府機関	民間企業（サプライチェーン）		民間企業（アウトソース先等）	
		親会社等	子会社等	セキュリティベンダー	運用保守事業者
	●	●	▲	–	–

おもな役割	● 決定されたサイバーセキュリティ戦略に基づく取組を推進・管理する。 ● 組織のプロジェクトに関して、目標・計画の策定、プロジェクト体制の整備、進捗管理、資産・予算管理、業務改善等の各種管理業務を実施する。 ● 要員のクリアランス、取り扱う個人情報、機密情報の管理・運用、インシデント発生時の運用ルールを定める。	
NICEフレームワークにおける対応ロール	プログラム管理	OG-WRL-010
	セキュリティプロジェクト管理	OG-WRL-011
	ナレッジ管理	IO-WRL-003
補足説明	● ①が策定したセキュリティ対策に関する施策を実施する役割を担う。 ● セキュリティ対策に関する各種プロジェクト（ISMS運営、対策の導入、全社展開等）を推進するプロジェクトマネージャーに相当する。 ● 子会社・委託先等における“▲”は、自組織に限定したプロジェクトの場合は必要であるが、サプライチェーン全体のプロジェクト等を従たる立場で実施する場合は不要であることを意味する。	

人材像（案）の修正案（3/13）

③監視	当該役割を担う人材が所属する組織				
	政府機関	民間企業（サプライチェーン）		民間企業（アウトソース先等）	
		親会社等	子会社等	セキュリティベンダー	運用保守事業者
	●	●	–	●	–

おもな役割	● セキュリティ監視を行う（各種機器のログの監視、保管、分析）。 ● セキュリティインシデントを検知し、関係各所へ連携する。 ● 監視ツールの運用、保守を行う。	
NICEフレームワークにおける対応ロール	ディフェンシブサイバーセキュリティ	PD-WRL-001
	内部脅威分析	PD-WRL-005
	脅威分析	PD-WRL-006
補足説明	● 一般にSOC（Security Operation Center）サービスを提供する要員に相当し、24時間365日の監視が必要なことから、外部委託にて実施されることが多い。 ● 経済産業省の情報セキュリティサービス審査登録制度における「セキュリティ監視・運用サービス」に従事する人材に相当。	

人材像（案）の修正案（4/13）

④対処	当該役割を担う人材が所属する組織				
	政府機関	民間企業（サプライチェーン）		民間企業（アウトソース先等）	
		親会社等	子会社等	セキュリティベンダー	運用保守事業者
	●	●	●	●	–

おもな役割	● 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。 ● インシデント対応に係る関係機関との連絡・調整等を行う。 ● 組織として実施するインシデントに係る広報等への対応のために必要な情報提供を行う。	
NICEフレームワークにおける対応ロール	インシデントレスポンス	PD-WRL-003
補足説明	● インシデント発生時の対処を担う人材として、組織の規模に関わらずすべての組織において必要な人材であるが、専門的な知識・スキルが必要な内容をセキュリティベンダーの専門人材にて対応する等の役割分担が行われることもある。	

人材像（案）の修正案（5/13）

⑤情報収集・分析・共有	当該役割を担う人材が所属する組織				
	政府機関	民間企業（サプライチェーン）		民間企業（アウトソース先等）	
		親会社等	子会社等	セキュリティベンダー	運用保守事業者
	●	●	–	●	–

おもな役割	● 組織内外の情報セキュリティに関する情報を収集する（脅威ハンティング等、脅威の能動的な探索の実施を含む）。 ● 収集した情報の分析を実施する。 ● 分析した結果を管理及び共有する。	
NICEフレームワークにおける対応ロール	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
	内部脅威分析	PD-WRL-005
	脅威分析	PD-WRL-006
	ナレッジ管理	IO-WRL-003
補足説明	● 脆弱性情報の収集及び脅威インテリジェンスに相当するタスクを含む。 ● 中小企業では収集した情報から自組織への影響を適切に判断できるスキルを有する人材の確保が困難な場合も多いと想定される。この場合、セキュリティ対策が実施された外部のSaaSサービスを利用すること等により、この役割を担う人材を割り当てない対応も考えられる。	

人材像（案）の修正案（6/13）

⑥脆弱性評価	当該役割を担う人材が所属する組織				
	政府機関	民間企業（サプライチェーン）		民間企業（アウトソース先等）	
		親会社等	子会社等	セキュリティベンダー	運用保守事業者
	●	●	–	●	–

おもな役割	● ソフトウェアやシステム、ネットワーク等を対象に脆弱性診断・ペネトレーションテストを行い、脆弱性がないか評価する。	
NICEフレームワークにおける対応ロール	脆弱性分析	PD-WRL-007
補足説明	● 自組織内で脆弱性評価を行うスキルを有する人材を確保できない場合には外部委託による対応が可能である。 ● 経済産業省の情報セキュリティサービス審査登録制度における「脆弱性診断サービス」及び「ペネトレーションテストサービス」に従事する人材に相当。	

人材像（案）の修正案（7/13）

⑦フォレンジック	当該役割を担う人材が所属する組織				
	政府機関	民間企業（サプライチェーン）		民間企業（アウトソース先等）	
		親会社等	子会社等	セキュリティベンダー	運用保守事業者
	●	●	–	●	–

おもな役割	● サイバーセキュリティインシデントが発生した際に、デジタルデータの証拠保全対象を判断し、適切なツールで証拠保全を行う。 ● 証拠保全の対象としたデジタルデータを分析し、人材像「対処」と連携し、セキュリティインシデントを調査・報告する。 ● 司法執行権を有する政府機関がサイバー犯罪に対する捜査を行う。	
NICEフレームワークにおける対応ロール	デジタルフォレンジック	PD-WRL-002
	サイバー犯罪捜査	IN-WRL-001
	デジタル証拠解析	IN-WRL-002
補足説明	● 適切な証拠保全や原因調査等には専門的なスキルが要求されることから、一般の企業等では自社で当該業務を担う人材を有さず、外部委託により対応することが多い。 ● 経済産業省の情報セキュリティサービス審査登録制度における「デジタルフォレンジックサービス」に従事する人材に相当。	

人材像（案）の修正案（8/13）

⑧運用管理

当該役割を担う人材が所属する組織				
政府機関	民間企業（サプライチェーン）		民間企業（アウトソース先等）	
	親会社等	子会社等	セキュリティベンダー	運用保守事業者
▲	●	－	－	●

おもな役割

- 組織の要請に応じ、要件定義・仕様の策定時における開発部署への助言・所要の意見提出を行う。
- 組織で扱うデータを適切に保護するためのアクセス制御、認証及びバックアップ等の管理策を実施する。
- 情報インフラ設備等の運用・保守に係る作業内容等を記載した運用・保守計画書を作成する。
- 運用・保守計画書に沿って、情報インフラ設備等の運用・保守業務を実施する。
- 情報システム及びネットワーク環境におけるセキュリティの設定等ネットワークの安全性を担保し、不審な兆候の検知時やインシデント発生時には関係各所と連携し、対処に当たる。
- 情報システム及びネットワーク環境の運用終了時は、機器の廃棄、データの消去等を適切に行う。

NICEフレームワークにおける対応ロール

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-002
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
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

補足説明

- 実態としてはセキュリティ対策のみを担う担当者を割り当てるのではなく、情報システム等の運用保守担当者がセキュリティ対策も担う形での実施が想定される。
- 政府機関の“▲”は一部機関において組織内で運用管理が実施される場合を想定する。

人材像（案）の修正案（9/13）

⑨教育・訓練	当該役割を担う人材が所属する組織				
	政府機関	民間企業（サプライチェーン）		民間企業（アウトソース先等）	
		親会社等	子会社等	セキュリティベンダー	運用保守事業者
	●	●	●	●	–

おもな役割	● 組織のサイバーセキュリティ人材に係る育成・確保の方針を策定する。 ● サイバーセキュリティ人材に対する教育の計画、実施、評価を実施する。	
NICEフレームワークにおける対応ロール	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
補足説明	● 企業規模を問わず、教育・訓練を担当する人材は必要となる。講師や教材作成等を外部委託することは可能。 ● セキュリティ担当者が担う方法と、人事部門の研修担当者等が担う方法の両方が想定される。	

人材像(案)の修正案(10/13)

⑩法務	当該役割を担う人材が所属する組織				
	政府機関	民間企業(サプライチェーン)		民間企業(アウトソース先等)	
		親会社等	子会社等	セキュリティベンダー	運用保守事業者
	▲	●	●	●	–

おもな役割	● 組織に対して、情報セキュリティに関する事項(個人情報保護等)に関連する法令等の助言を行う。 ● 組織及び従業員のコンプライアンス意識を向上させ、社内ルール等の管理を行う。	
NICEフレームワークにおける対応ロール	サイバーセキュリティに関する法的助言	OG-WRL-006
	プライバシーコンプライアンス	OG-WRL-008
補足説明	● 一般的には組織内の法務担当者がサイバーセキュリティに関する関連業務を担当する形での実施が想定される。 ● 政府機関の“▲”は政府機関全体の法務機能において当該役割を担う人材が存在することを示す。	

人材像（案）の修正案（11/13）

⑪監査	当該役割を担う人材が所属する組織				
	政府機関	民間企業（サプライチェーン）		民間企業（アウトソース先等）	
		親会社等	子会社等	セキュリティベンダー	運用保守事業者
	–	●	●	●	–

おもな役割	● 運用管理から独立した立場から、組織やシステムを対象とするリスク評価を行う。 ● 情報セキュリティ監査及びシステム監査を行う。 ● 情報セキュリティ監査及びシステム監査後の改善計画の作成・助言、改善活動の実施・助言を行う。	
NICEフレームワークにおける対応ロール	技術プログラム監査	OG-WRL-016
	セキュリティ管理策評価	OG-WRL-012
補足説明	● 監査目的に応じて、内部監査と外部監査の方法を使い分けることが想定される。 ● 経済産業省の情報セキュリティサービス審査登録制度における「情報セキュリティ監査サービス」に従事する人材に相当。	

人材像(案)の修正案(12/13)

⑫設計開発	当該役割を担う人材が所属する組織				
	政府機関	民間企業(サプライチェーン)		民間企業(アウトソース先等)	
		親会社等	子会社等	セキュリティベンダー	運用保守事業者
	●	●	–	–	●

おもな役割	● 新規又は更新するサービス・製品案の検討にあたり、望ましいアーキテクチャとその潜在的なリスクを想定した上で、リスクへの対処のために備えるべきセキュリティ機能の設計を行う。 ● 整理した内容を元に、情報システム等の要件定義、設計、開発、テスト、評価を行い、サービス・製品等を実用化する。 ● 「セキュリティ・バイ・デザイン」の考え方に則り、システム開発の企画段階からセキュリティを実装する。 ● 自組織で発見された脆弱性に対する修正プログラムを作成する。	
NICEフレームワークにおける対応ロール	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
補足説明	● 情報システム・サービスの設計開発の一連のプロセスのうち、企画段階を担う人材から最終テストを担う人材までを含む。	

人材像(案)の修正案(13/13)

⑬研究	当該役割を担う人材が所属する組織				
	政府機関	民間企業(サプライチェーン)		民間企業(アウトソース先等)	
		親会社等	子会社等	セキュリティベンダー	運用保守事業者
	●	●	–	●	●

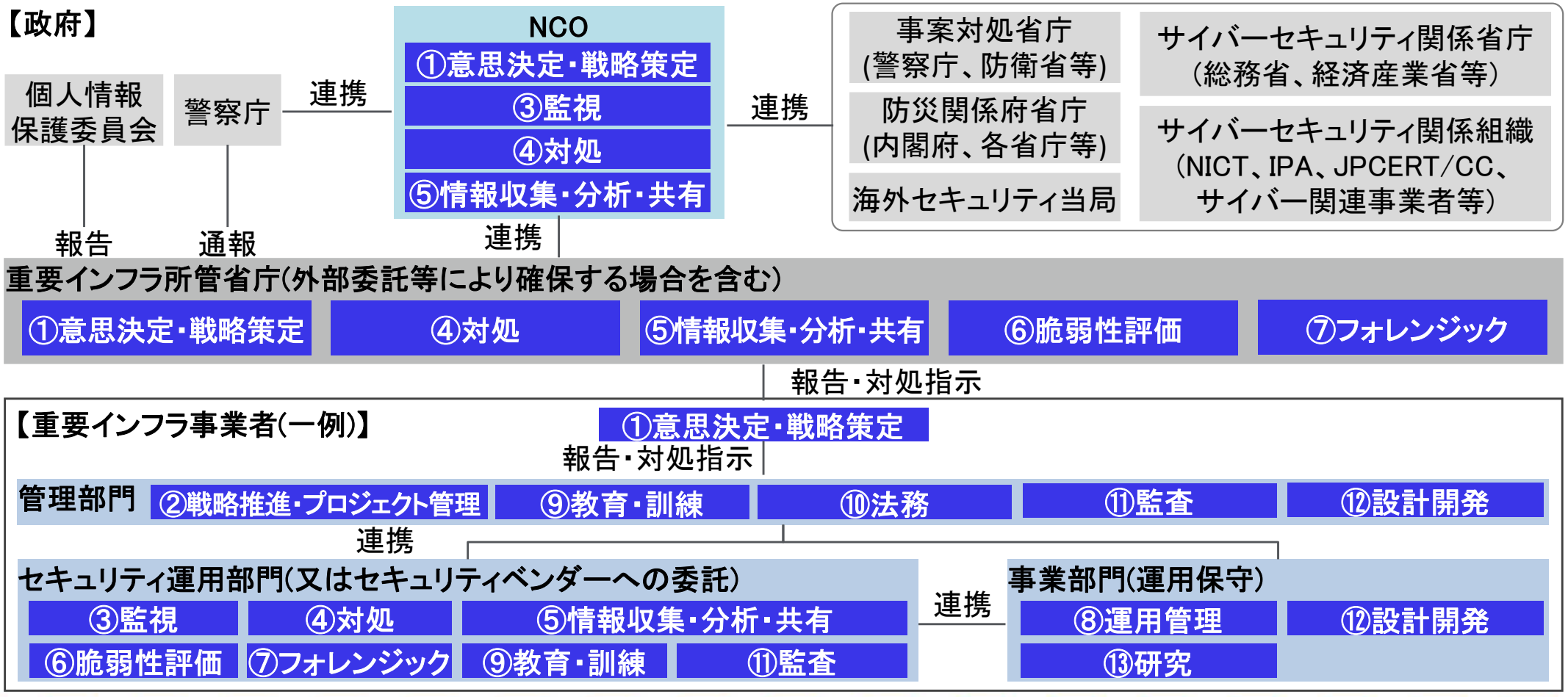
おもな役割	● サイバーセキュリティに関する先端技術の研究を行う。 ● 研究結果を人材像「開発」と連携し、新たな課題の解決に向けた実用化を進める。 ● 技術ロードマップを作成する。	
NICEフレームワークにおける対応ロール	技術研究開発	DD-WRL-008
補足説明	● 研究に関する役割を担う組織として、上表のほか大学等の教育機関が含まれる。	

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。
- 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。

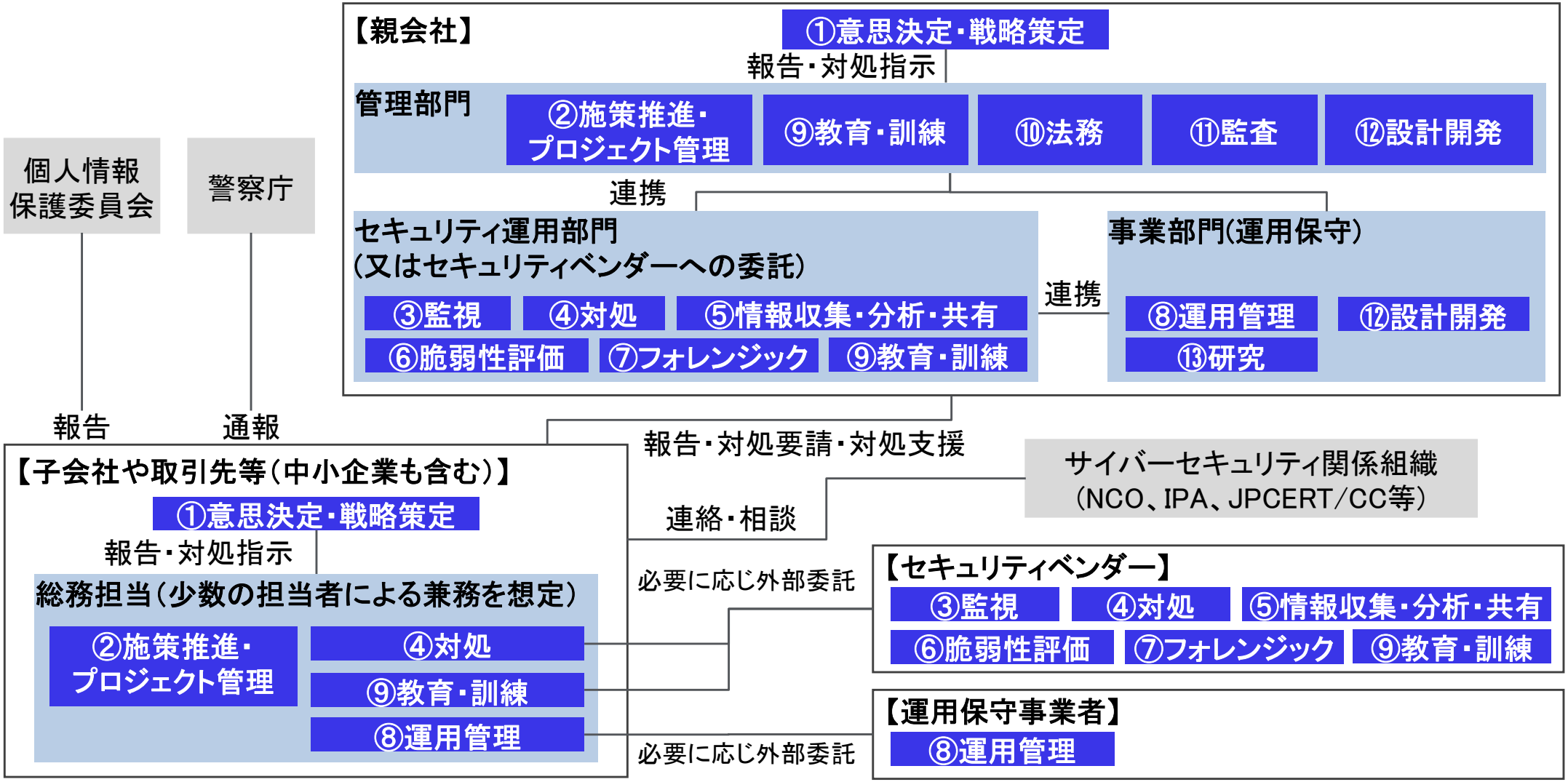
① 意思決定・戦略策定　② 施策推進・プロジェクト管理　③ 監　視　④ 対　処　⑤ 情報収集・分析・共有　⑥ 脆弱性評価

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



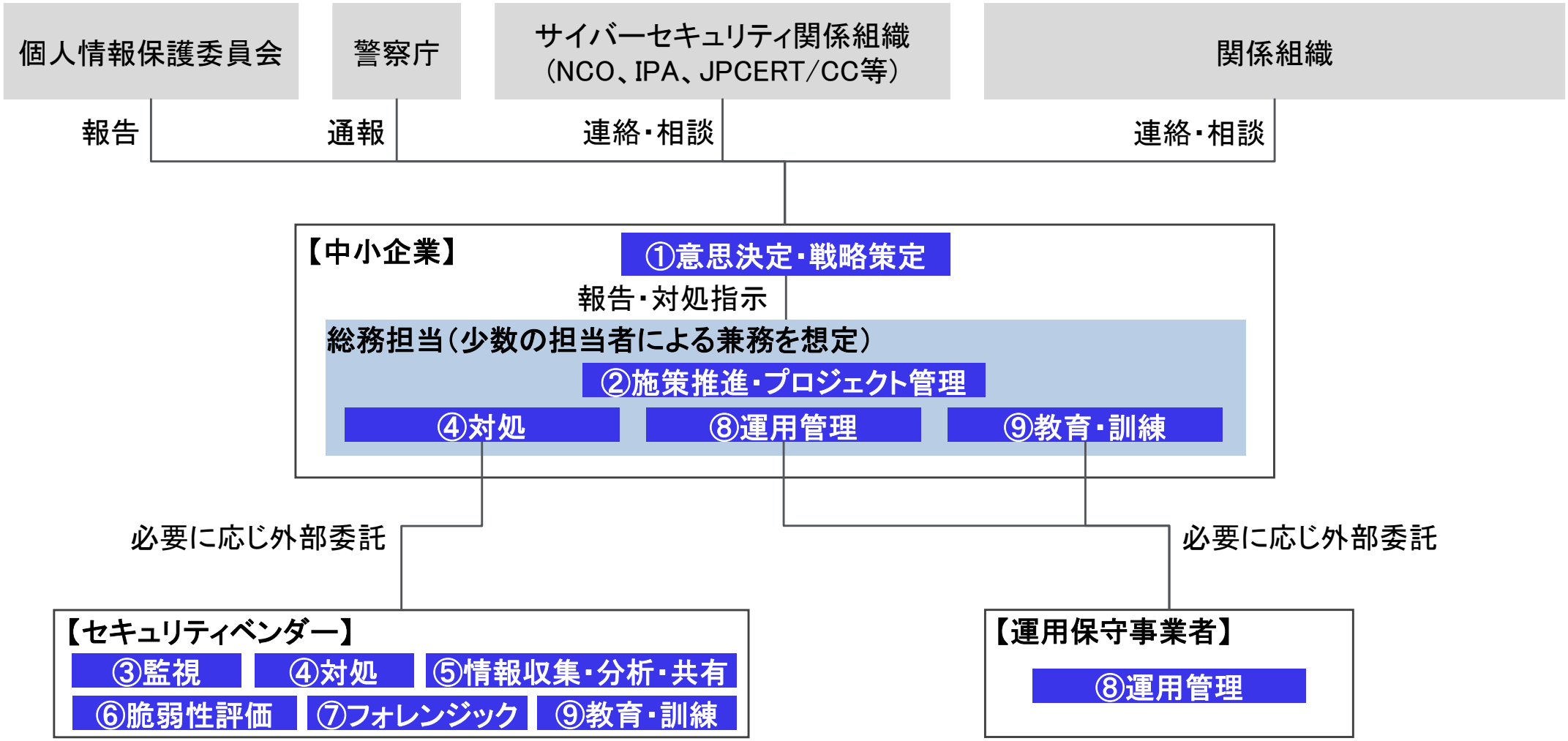
（参考）活用例①：サプライチェーン関係者間の連携

- 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。



（参考）他の人材フレームワークとの対応関係

	本フレームワーク	ITSS+（セキュリティ領域）	SecBoK	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）	CISO	CISO、CRO、CIO等 システム部門責任者	
②	施策推進・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）	IT企画部門 POC ノーティフィケーション	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		SOC担当	
④	対処	セキュリティ監視・運用	コマンダー、トリアージ、 インシデントハンドラー、 インシデントマネージャー	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	キュレーター、リサーチャー セルフアセスメント、 ソリューションアナリスト	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	脆弱性診断士	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	フォレンジックエンジニア インベスティゲーター	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	IT企画部門 ITシステム部門	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・啓発	サポート教育担当	
⑩	法務	法務	リーガルアドバイザー		
⑪	監査	セキュリティ監査、システム監査	情報セキュリティ監査人	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	IT企画部門 ITシステム部門	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			

本フレームワークにおけるレベルの設定について

レベル設定についての主な御意見

■ 前回検討会での意見及び有識者ヒアリングにおいて次の指摘がなされている。

前回検討会での意見	● 無理にレベル分け等をすると、分かりにくいものになるのではないか。 ● レベルを示す数値による見え方を既存のもの（ITSS等）に合わせるべき。 ● 高度な人材像について入りこむと迷走の懸念があり、別途検討でよい。
有識者ヒアリングでの意見	● NICEフレームワークではレベル定義を行っておらず、コンピテンシーの概念を用いることを前提としている。 ● レベル分けを行おうとすると、評価基準の設定や評価者の確保が課題となる。ぶれなく評価できるか運用面の課題が大きい。

御指摘を踏まえた検討案

- □ 日本型雇用（メンバーシップ型）において、人材の配置やキャリア等の扱いにおいて経験やスキルのレベルを考慮するニーズがあることを踏まえ、次ページに示す４段階のレベルを設定。
- □ ITSSのレベルと（次ページで示す案のとおり）相互参照を図る。
  ※ ITSSとの相互参照を図るため、レベル設定を「０～３」から「１～４」へ改め、各レベルの定義も更新
- □ 採用、配置、育成、評価等のあらゆる場面における、人材像×レベルの活用例については手引き書に記載。

ITSSレベルとの対応イメージ（案）

レベル	人材像レベルの定義	対応するITSSレベル
4	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 13人材像いずれかの業務における実務経験は10年以上が望ましい	レベル4 （組織内のハイレベルプレーヤ）
3	責任：当該業務を独力で遂行可能であり、加えて下位者に対する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「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 13人材像いずれかの業務における実務経験は4～10年が望ましい	レベル3 （独力で遂行可能）
2	責任：当該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「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 13人材像いずれかの業務における実務経験は2～4年程度が望ましい	レベル2 （指導の下で遂行可能）
1	責任：当該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「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 13人材像いずれかの業務における実務経験が2年未満	レベル1 （最低限必要な知識を有する）

人材像見直し案に関してご議論いただきたい点

■ **論点①**：人材像定義の妥当性について（P1～20参照）
- ご意見いただきたいポイント：
  - 人材像定義の見直しを通じて、前回検討会にて御指摘いただいた課題の改善が図られているか。
  - P17～19で示すフレームワークの活用例により、重要インフラ防御に関する官民連携、サプライチェーンセキュリティ、中小企業のセキュリティ対策等を担う人材の配置や役割分担が適切に表現できているか。

■ **論点②**：レベルの取扱いについて（P21～22参照）
- ご意見いただきたいポイント：
  - 本フレームワークにおけるレベルの取扱は、P21、22に示した事務局案でよいか。