国家サイバー統括室
National Cybersecurity Office

サイバーセキュリティ人材フレームワーク2026

令和8年4月

内閣官房
国家サイバー統括室（NCO）

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。

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

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。

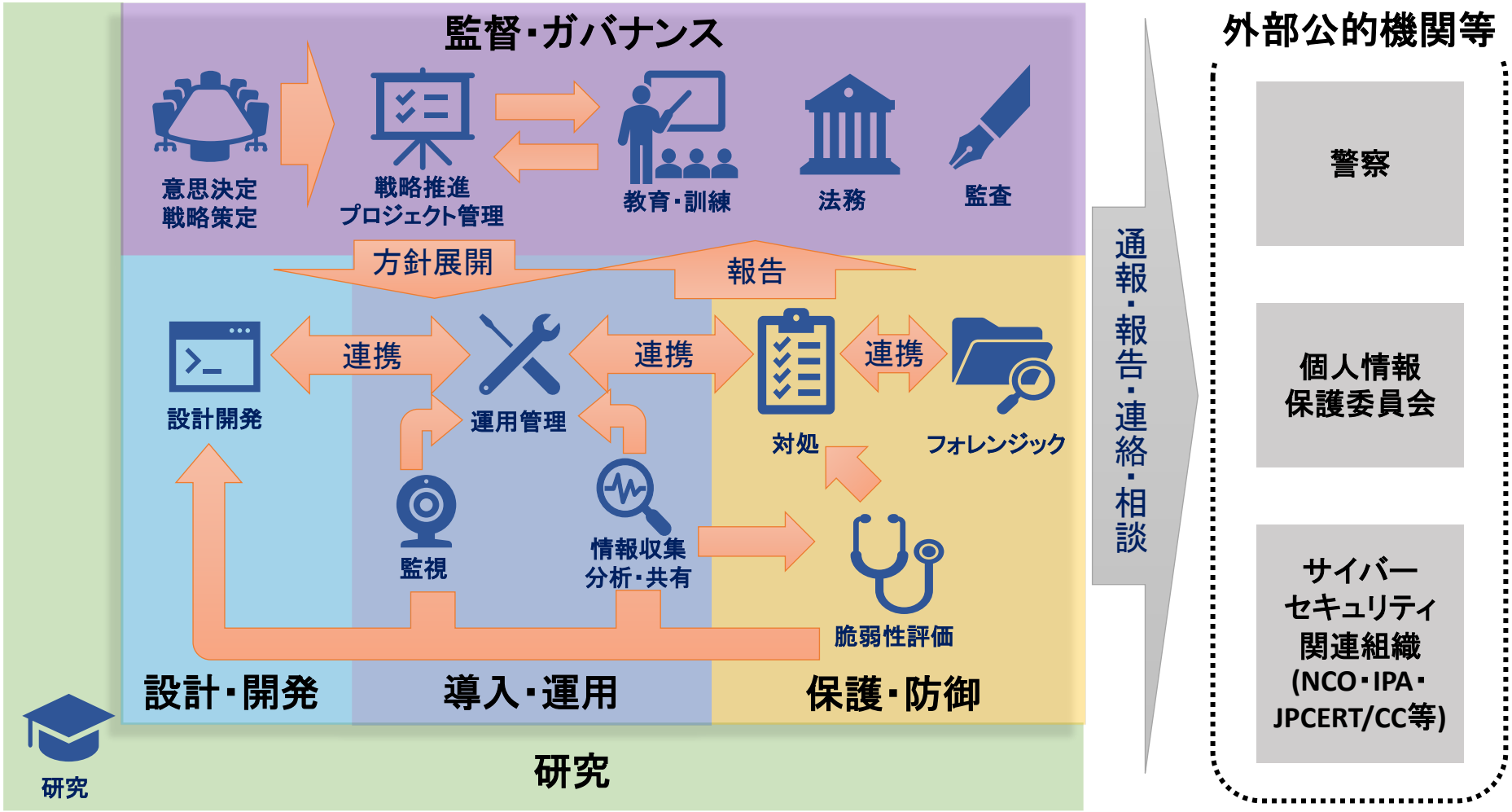
※　特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）が発行するSecBoK
　　産業横断サイバーセキュリティ検討会　人材定義リファレンス　　等

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



人材フレームワークのレベル設定について

ITSS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	**レベル4-M**：業務における意思決定に責任を負う者 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タスクを組織内で適切に実施させるための意思決定及びマネジメントを行うことができる ② 各役割に関する自らの責任に応じた説明や連携を行うために必要となる知識・スキルを有している ③ 組織マネジメント業務に関する10年以上の実務経験に相当する知識・スキルを有する	**レベル4-E**：自らの専門分野を確立し、ハイレベルのプレーヤとして組織内外で認知されている者 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タスク遂行を通じて、高い専門知識・スキルを有する人材として組織内外で認知されている ② 組織内教育や指導、コミュニティ活動や対外情報発信等を通じて組織内外のセキュリティ向上に貢献している ③ サイバーセキュリティに関する10年以上の実務経験に相当する実践的な知識・スキルを有する ※下線部はITSSレベル6以上に相当する部分	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	**レベル3-M**：業務について関連するチームメンバの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タスクについて、チームのマネジメントを通じて遂行することができる ② 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 ③ サイバーセキュリティに関する実践的知識・スキルに加えて、組織マネジメントに関する実務経験相当の知識・スキルを有する	**レベル3-E**：自らの専門領域の業務を独力で遂行可能な者 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タスクを自らが中心となって遂行することができる ② エキスパートとして自身の専門領域に関わる最新情報や動向の習得・活用を行っている ③ サイバーセキュリティに関する4～10年の実務経験に相当する実践的な知識・スキルを有する	レベル3 （独力で遂行可能）
2	**レベル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2～4年の実務経験に相当する実践的な知識・スキルを有する		レベル2 （指導の下で遂行可能）
1	**レベル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 他者の指示及び支援により、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1～2年の実務経験を有する		レベル1 （最低限必要な知識を有する）

役割の詳細：①意思決定・戦略策定

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	ユーザー企業（サプライチェーン）		ベンダー企業（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
	●	●	●	●	●

主な業務（例）	● 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。 ● 組織のシステムのセキュリティ確保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
想定される役職名等	CISO及びその補佐役	
補足説明	● 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対処を担う人材に指示を行う。 ● SecBoKでは「セキュリティ経営、意思決定・戦略策定」、「セキュリティ統括」のロールに対応。 ● 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では、「CISO」、「CRO」、「CIO」、「システム部門責任者」等の役割に対応。	

役割の詳細：②戦略推進・プロジェクト管理

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	ユーザー企業（サプライチェーン）		ベンダー企業（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
	●	●	▲	●	●

主な業務（例）	● 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。 ● 組織のサイバーセキュリティ対策に関するプログラム又はプロジェクトに関して、目標・計画の策定、プログラム/プロジェクト体制の整備、進捗管理、資産・予算管理、委託先管理、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
想定される役職名等	個人情報管理責任者、情報管理者、プロジェクトマネージャー、プロジェクトリーダー　等	
補足説明	● ①意思決定・戦略策定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。明確にプロジェクトとして扱われていない活動も含む。 ● 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。 ● SecBoKでは、「プロジェクト管理」、「社内外調整」のロールに対応。 ● 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では、「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」の役割・担当に対応。	

役割の詳細：③監視

③監視	当該役割を担う人材が所属する組織				
	政府機関	ユーザー企業（サプライチェーン）		ベンダー企業（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
	●	●	―	●	●

主な業務（例）	● 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
想定される役職名等	SOC責任者、SOCメンバー、セキュリティエンジニア、オペレーター、監視担当　等	
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。 ● SecBoKでは「監視・運用」のロールに対応。 ● 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では、「SOC担当」に対応。	

役割の詳細：④対処

④対処	当該役割を担う人材が所属する組織				
	政府機関	ユーザー企業（サプライチェーン）		ベンダー企業（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
	●	●	●	●	●

主な業務（例）	● 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
想定される役職名等	CSIRT責任者、CSIRTメンバー、インシデントハンドラー、セキュリティエンジニア、オペレーター等（一般にCSIRT以外は通常時の業務における役職名で扱われることが多い）	
補足説明	● CSIRTが存在する組織の場合、CSIRTに所属する人材に相当。 ● 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全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。 ● SecBoKでは「対処（インシデントハンドリング）」のロールに対応。 ● 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では、「CSIRT責任者/担当」、「サイバーセキュリティ事件・事故担当」の役割・担当に対応。	

役割の詳細：⑤情報収集・分析・共有

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	ユーザー企業（サプライチェーン）		ベンダー企業（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
	●	●	–	●	●

主な業務（例）	● 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
想定される役職名等	サイバーセキュリティアナリスト、脅威インテリジェンスアナリスト、リサーチャー、セキュリティエンジニア　等	
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。 ● CTEM（Continuous Threat Exposure Management）として、継続的に脅威の検知及びリスクへの対応を行うような取組を含めることも想定される。 ● SecBoKでは「脅威・脆弱性情報収集」のロールに対応。 ● 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では、「SOC担当」に対応。	

役割の詳細：⑥脆弱性評価

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	ユーザー企業（サプライチェーン）		ベンダー企業（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
	●	●	–	●	●

主な業務（例）	● 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
想定される役職名等	脆弱性診断士、脆弱性アナリスト、ペネトレーションテスター、セキュリティエンジニア　等	
補足説明	● 脆弱性の有無に関する判断には専門的なスキルが求められるため、自組織内で関連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。 ● SecBoKでは「脆弱性診断・評価」のロールに対応。 ● 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では、「運用系サイバーセキュリティ担当」に対応。	

役割の詳細：⑦フォレンジック

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	ユーザー企業（サプライチェーン）		ベンダー企業（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
	●	●	–	●	●

主な業務（例）	● 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。	
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
想定される役職名等	フォレンジックエンジニア、セキュリティエンジニア　等	
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。 ● SecBoKでは「インシデント調査・分析」のロールに対応。 ● 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では、「サイバーセキュリティ事件・事故担当」に対応。	

役割の詳細:⑧運用管理

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	ユーザー企業(サプライチェーン)		ベンダー企業(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
	▲	●	●	●	●

主な業務(例)

- 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。
- 情報システム及びネットワーク環境についての事業継続計画(BCP)を立案する。
- 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・復旧にあたる。
- 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

想定される役職名等

セキュリティオペレーター、システムオペレーター、セキュリティエンジニア　等

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。
- SecBoKでは「システム管理・ネットワーク管理」のロールに対応。
- 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では、「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」等の役割・担当に対応。

役割の詳細：⑨教育・訓練

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	ユーザー企業（サプライチェーン）		ベンダー企業	大学等教育機関
		親会社等	子会社等		
	●	●	●	教育サービス事業者	●

主な業務（例）	● 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。 ● サイバーセキュリティに関する教育や普及啓発を行う際に用いるコンテンツを作成する。	
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
想定される役職名等	講師、インストラクター、教授、研究員、研修担当　等	
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。 ● SecBoKでは「教育・訓練」のロールに対応。 ● 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では、「サポート教育担当」に対応。	

役割の詳細：⑩法務

⑩法務	当該役割を担う人材が所属する組織			
	政府機関	ユーザー企業（サプライチェーン）		アウトソース先等
		親会社等	子会社等	法律事務所等
	△	●	●	

主な業務（例）	● 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、サイバー・デジタル関連規制・制度等についての助言を行う。 ● 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
想定される役職名等	（サイバー）法務担当、リーガルアドバイザー　等	
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。 ● SecBoKでは「法務」のロールに対応。 ● 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に対応する役割（担当）はなし。	

役割の詳細：⑪監査

⑪監査	当該役割を担う人材が所属する組織			
	政府機関	ユーザー企業（サプライチェーン）		アウトソース先等
		親会社等	子会社等	監査法人等
	▲	●	●	

主な業務（例）	● 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
想定される役職名等	情報セキュリティ監査人、情報セキュリティ監査技術者、セキュリティアセッサー、セキュリティ監査担当　等	
補足説明	● 監査目的に応じて、内部監査と外部監査の2種類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。 ● 政府機関の“△”は政府機関全体の監査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。 ● SecBoKでは「監査」のロールに対応。 ● 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では、「監査責任者」、「監査担当」の役割・担当に対応。	

役割の詳細：⑫設計開発

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	ユーザー企業（サプライチェーン）		ベンダー企業（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
		●	●	●	●

主な業務（例）

- 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

想定される役職名等

セキュリティアーキテクト、セキュリティエンジニア、システムエンジニア、テスター　等

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。
- SecBoKでは「セキュリティ設計」、「開発」のロールに対応。
- 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では、「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」等に対応。

役割の詳細：⑬研究

⑬研究	当該役割を担う人材が所属する組織					
	政府機関	大学等教育機関	ユーザー企業（サプライチェーン）		ベンダー企業（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
	●	●	●	●	●	●

主な業務（例）	● サイバーセキュリティに関する先端技術の研究を行う。 ● 共同研究や技術指導等、研究分野以外の人材と連携し、サイバーセキュリティ分野の課題解決や新たな取組の実現や実用化を支援する。 ● 技術ロードマップを作成する。 ● 研究活動を通じてサイバーセキュリティ分野で高度な知見やスキルを有する人材を育成する。 ● サイバーセキュリティに関する学会やコミュニティ活動に参加する。	
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
想定される役職名等	教授、講師、研究員、R&D担当　等	
補足説明	● SecBoKに対応するロールはなし。 ● 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に対応する役割（担当）はなし。	

手引き書の位置づけ・概要

- フレームワークを実務で活用するための指針として「手引き書」を作成
- 利用主体別（小規模組織・大規模組織、教育、専門人材、プラス・セキュリティ）に分冊形式で整理
- 共通事項と利用主体別固有事項に分けて構成

全体構成（概要）

詳細は参考資料（各冊子）参照

共通事項

- フレームワークの全体像や手引き書の使い方・留意点等を整理し、全体を俯瞰

記載内容

- □ 人材フレームワーク/手引き書とは
- □ 他の人材フレームワークとの参照関係

利用主体別事項

1. 小規模組織向け

- □ 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. 大規模組織向け

- □ 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. 教育機関向け

- □ 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. 個人向け（専門人材）

- □ 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. 個人向け（プラス・セキュリティ）

- □ 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

【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活用いただくことも想定しております。

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)	○	―	○ (学部の専門性によらず全学生に有益)

1.小規模組織向け手引き書2026の全体構成

- 小規模組織に共通するセキュリティ対策の課題の解決を、条件に応じた3種類のケースを通じて説明します。
- タスクの割り当てに関する説明を通じて、フレームワークの役割は一人で担うことを前提としたものではなく、複数の人材に割り当てて分担可能であるということを理解できます。

多くの小規模組織に共通する課題認識：

- 組織内でサイバーセキュリティ専任の人材を確保することが難しい
- サイバーセキュリティ対策として何をすればよいのかわからない

小規模組織におけるセキュリティ対策の基本的な考え方

	ケース1：A社（オンライン小売業・従業員数8名）	ケース2：B社（製造業・従業員数20名）	ケース3：C社（サービス業・従業員数2名）
悩み	サイバーセキュリティ対策はこれまで外部業者に任せており、「自組織でやるべきこと」を意識できていない。	社内にデジタルリテラシーを備えた人材がほとんどいない。	1人でやるべきことが何かがわからない。
解決方策	**以下のステップを通じた無理のないセキュリティ体制の実現** STEP1 自組織で担うべき役割の明確化 STEP2 各自への「タスク」の割り当て STEP3 必要な「知識・スキル」の自己評価 STEP4 「知識・スキル」の習得方法の決定・実施	**委託活用で確保した2年間で担当者育成** STEP1 マネージドセキュリティサービスの利用で当面の安全確保 STEP2 人選の上、約2年間をかけ担当者を育成 STEP3 タスクを割り当て	**組織的な対策を省いて対応** STEP1 監視・対処等の機能を内包するクラウドサービスを利用 STEP2 必要なタスクを絞り込んだ上で代表者が対応

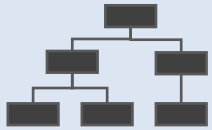
2.大規模組織向け手引き書2026の全体構成

- 大規模な組織ならではの課題解決にフレームワークを活用する事例として、組織のガバナンス、他のガイドラインとの連携、人材の採用及び評価について取り上げるとともに、そのプロセスにおいてフレームワークを構成する役割、タスク、知識、スキル、レベルの各要素の使い方を説明します。

経済産業省
「サイバーセキュリティ体制構築・人材確保の手引き」（第2.0版）

参照

① 自社に適したガバナンスの検討



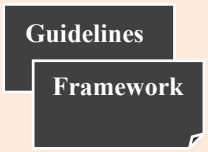
組織の特徴を考慮したサイバーセキュリティ体制の構築方法と必要な役割や人材像を解説します。

サイバーセキュリティリスクのガバナンスはコーポレートガバナンスの形態に合わせることが重要

自社の特徴に応じた人材配置

②他のガイドライン等との連携による活用

他のガイドラインの規定に対応するタスクの具体化、他のフレームワークを用いた詳細化を説明します。



外部の要求事項に合わせるだけでなく、フレームワークで規定する役割・知識・スキルをより詳細に定義することが可能

取引先等からの要求への対応

フレームワークの活用による課題解決

知識・スキルの不足を可視化

③ 職務記述書の作成

人材のミスマッチを防ぐ観点からフレームワークに基づいた求人要件等の記載方法について解説します。

求人側と求職者側がフレームワークを通じて役割や能力についての認識を共有することで採用時のミスマッチを防止

モチベーション向上

④ 人材の評価

フレームワークに基づいたセキュリティ人材の評価方法や留意点について解説します。

目標設定やキャリアパスの計画等の取り組みを通じて人材のモチベーション向上や組織的な人材育成を実現

3.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

卒業生　社会ニーズ

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。

4-1.個人（専門人材）向け手引き書2026の全体構成

- サイバーセキュリティ分野で高度な専門性を有する人材としての活躍を目指す個人が、目指すキャリアと現状のギャップを把握し、必要な知識・スキルを効果的に習得していくためのステップと、実際の専門人材のキャリアパス事例を解説します。

現状の課題

セキュリティ分野での
キャリア形成についての悩み

- 自分に向いているセキュリティの役割や、次に目指すべきキャリアがわからない
- 目指すキャリアに対して、今の自分に不足している知識・スキルが客観的にわからない
- 不足している知識・スキルを、具体的にどうやって習得すればよいかわからない

目指すキャリアに必要な要件の可視化と、自律的なキャリア形成・学習の指針が必要

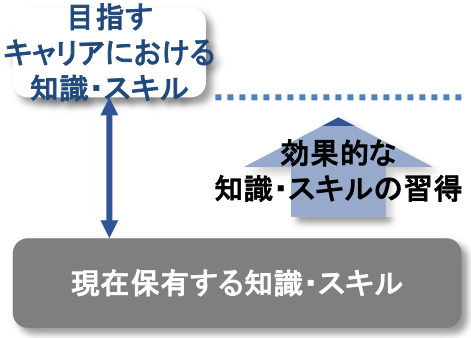
フレームワークを用いたキャリアの可視化と学習の指針策定

サイバーセキュリティ人材フレームワーク

各役割ごとにタスクから関連する知識・スキルを整理

【セルフアセスメント】
フレームワークを活用し、目標とする役割や現在の自分におけるタスク・知識・スキルを可視化

【学習指針の検討】
- 抽出したギャップの中から、習得すべき知識・スキルを抽出し、「資格取得」「研修」等の学習指針を検討



この手引き書で紹介する
専門人材の例
（随時拡充・見直し予定）
実際の専門人材の事例も適宜参照し、目指すキャリアに近しい事例を探してみましょう

現場技術からのマネジメント・エキスパート
運用や開発の経験を積みマネジメント・エキスパートへ

監査・ガバナンス専門家
監査や法務の専門性を一貫して磨く

技術領域のエキスパート深化
設計・開発を軸に特定技術の専門性を深める

アカデミアからのエキスパート社会実装
基礎研究からプロダクト化・経営へと貢献

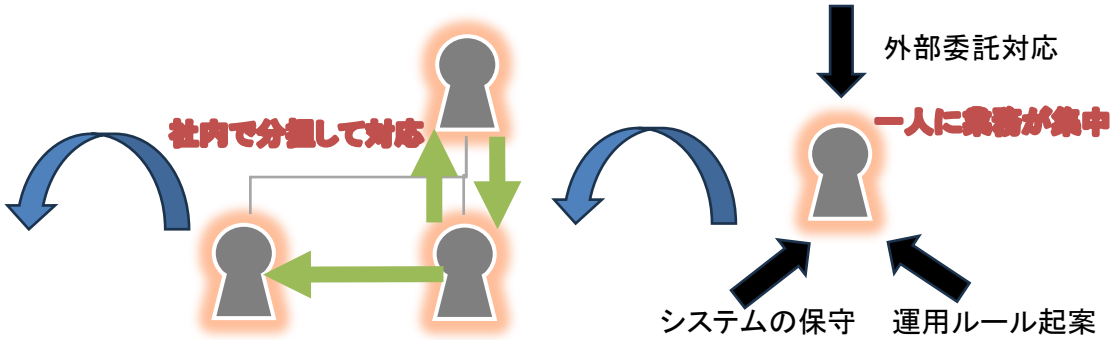
4-2.個人（プラス・セキュリティ）向け手引き書2026の全体構成

- バックオフィス(経理・総務・人事等)や営業等、サイバーセキュリティを専門業務としない個人が、自身の本来業務に関連して必要となるセキュリティ知識・スキル(プラス・セキュリティ)を特定し、効果的・効率的に習得・実践していくためのステップを解説します。

担当者の困りごと

現場担当
- 新しいクラウドサービス(SaaS)を業務で使いたいが、セキュリティリスクがわからない

バックオフィス担当
- 委託先の管理や契約時のセキュリティチェックをどう行えばよいか不安
- インシデント発生時に、専門部署へどう報告・連携すればよいかわからない



自身の業務とセキュリティの接点を明確にし、必要なタスク・知識・スキルを理解することが必要

STEP1

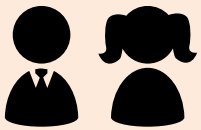
【自身の業務とタスク(T)の紐づけ】

日常業務やインシデント時の関わり方から、フレームワーク上の「タスク」を抽出・特定

STEP2

【知識・スキルの特定】
- 知識の例：個人情報保護法等の法規、リスクマネジメント
- スキルの例：アカウント・IDの適切な管理、専門家とのコミュニケーション

個人の実践(セルフアセスメントと学習)



① 目標と現状のギャップ分析(セルフアセスメント)

抽出した知識・スキルをもとに、「業務で求められる目標レベル」と「現在の自分のレベル」を比較し、優先的に補強すべき要素を客観的に把握。

②ギャップを埋めるための学習計画と実践

対策の例：情報セキュリティマネジメント試験等の資格取得を通じた体系的な学習、CYDER、プレCYDERなどの実践的な研修の受講、社内ルールの再確認など。

詳細は人材フレームワーク（本体）参照

（参考）国内の人材フレームワーク類との対応関係

	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			

（参考）諸外国の人材フレームワーク類との対応関係(1/2)

	本フレームワーク	欧州 (ECSF) 【12プロファイル】	グローバル/英国等 (SFIA 9) 【セキュリティ特化は7、IT全般で70以上】	英国 (UK CSC) 【15スペシャリズム】
①	意思決定・戦略策定	Chief Information Security Officer (CISO)	Security leadership, strategy and management	Cyber Security Management
②	戦略推進・プロジェクト管理	(該当なし) ※Cybersecurity Risk Managerと一部重複	(該当なし) ※Project delivery practitioners等の役割で代替	Cyber Security Governance & Risk Management
③	監視	Cyber Incident Responder ※対処に包含	Security operations	Network Monitoring & Intrusion Detection
④	対処	Cyber Incident Responder	Incident management practitioners	Incident Response
⑤	情報収集・分析・共有	Cyber Threat Intelligence Specialist	(該当なし) ※Security operations等に内包	Cyber Threat Intelligence
⑥	脆弱性評価	Penetration Tester	Penetration testing practitioners、Vulnerability analysis practitioners	Vulnerability Management、Security Testing
⑦	フォレンジック	Digital Forensics Investigator	(該当なし) ※Incident management practitionersに内包	Digital Forensics
⑧	運用管理	Cybersecurity Implementer	Security operations	Secure Operations、Identity & Access Management
⑨	教育・訓練	Cybersecurity Educator	Learning & development (L&D) practitioners、Teaching practitioners 等（IT全般）	(該当なし)
⑩	法務	Cyber Legal, Policy & Compliance Officer	Security risk management, audit and compliance ※一部内包	Data Protection & Privacy
⑪	監査	Cybersecurity Auditor	Security risk management, audit and compliance	Cyber Security Audit & Assurance
⑫	設計開発	Cybersecurity Architect、Cybersecurity Implementer	Security architecture practitioners	Secure System Architecture & Design、Secure System Development、Cryptography & Communications Security
⑬	研究	Cybersecurity Researcher	(該当なし)	(該当なし) ※Cryptography & Communications Security等に一部内包

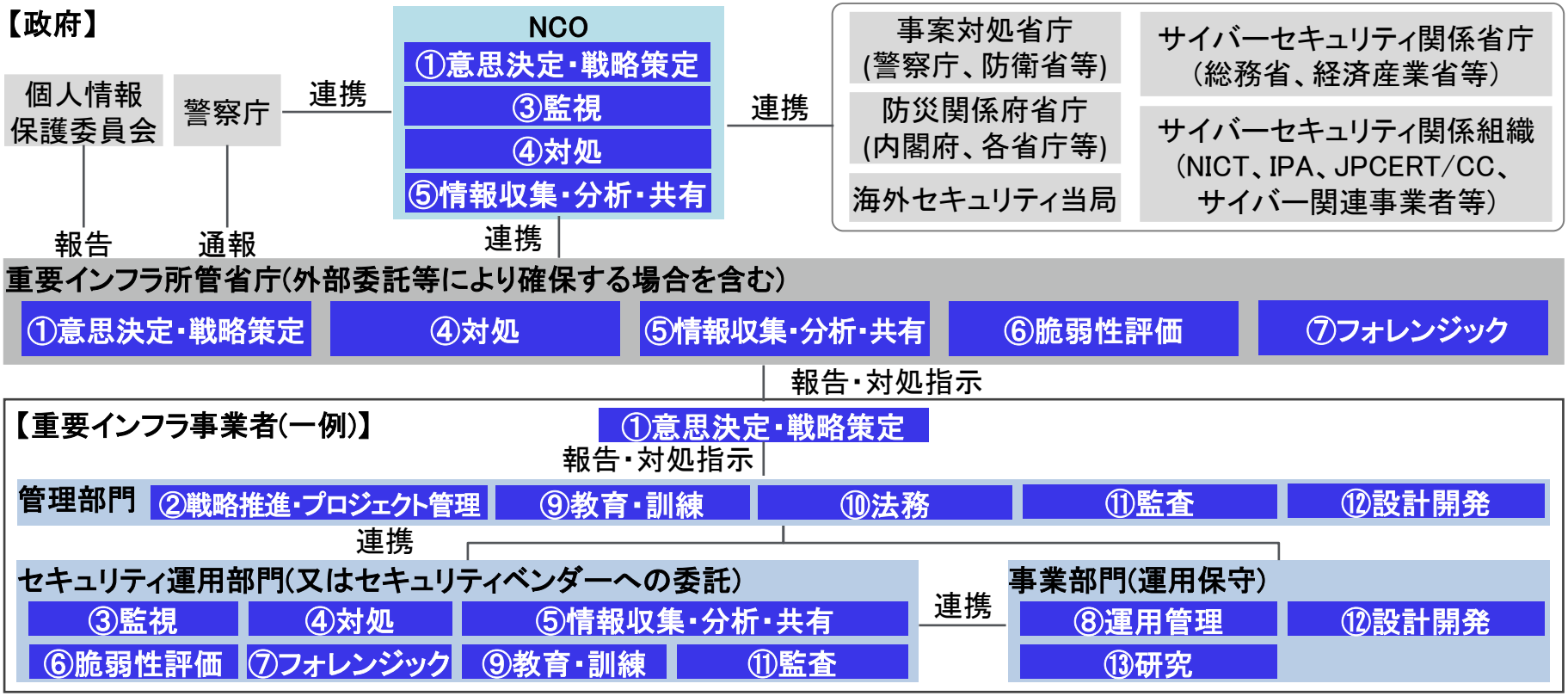
（参考）諸外国の人材フレームワーク類との対応関係(2/2)

	本フレームワーク	加国 (カナダ / DGSI)【コア22ロール】	シンガポール (SSG) 【ICT全体123 / うちセキュリティ15】	豪州 (ASD) 【9ロール】
①	意思決定・戦略策定	Chief Information Security Officer (CISO)	Chief Information Security Officer (CISO)	(該当なし) ※Operations Coordinatorが一部内包
②	戦略推進・プロジェクト管理	Information System Security Officer (ISSO)	Cyber Risk Manager、Cyber Risk Analyst	Operations Coordinator
③	監視	Cybersecurity Operations Analyst、Cybersecurity Operations Technician	Security Operations Manager、Security Operations Analyst	Intrusion Analyst
④	対処	Information Systems Security Manager - Cybersecurity Operations、Cybersecurity Incident Responder、OT incident responder	Incident Investigation Manager、Incident Investigator	Incident Responder
⑤	情報収集・分析・共有	Cyber Threat Intelligence Analyst、Supply Chain Security Analyst	Threat Analysis Manager	Cyber Threat Analyst
⑥	脆弱性評価	Vulnerability Assessment Analyst、Penetration Tester、Security Testing and Evaluation Specialist	Vulnerability Assessment and Penetration Testing Manager、Vulnerability Assessment and Penetration Testing Analyst	Penetration Tester、Vulnerability Assessor
⑦	フォレンジック	Digital Forensics Analyst	Forensic Investigation Manager、Forensic Investigator	Malware Analyst
⑧	運用管理	Identity & Access Management (IAM) Support Specialist、Encryption / Key Management Support Specialist	Associate Security Analyst	(該当なし)
⑨	教育・訓練	(Adjacent roles) Cyber Instructor 等	(該当なし)	(該当なし)
⑩	法務	Data Privacy Specialist / Privacy Officer、(Adjacent roles) Cyber Legal Advisor	(Data Protection トラック) Group Data Protection Officer、Data Protection Officer	(該当なし)
⑪	監査	Information Security (IS) Auditor	(IT Audit トラック) IT Audit Manager、IT Auditor	Cyber Security Advice and Assessment
⑫	設計開発	Security Architect、Security Engineer / Technologist、Secure Software Assessor、Operations Technology Systems Analyst、Information Systems Security Developer、Security Automation Engineer/Analyst	Security Architect、Senior Security Engineer / Security Engineer	Cyber Security Advice and Assessment
⑬	研究	Cryptographer / Cryptanalyst	(該当なし)	Vulnerability Researcher

（参考）活用例①：重要インフラ事業者向け対処体制

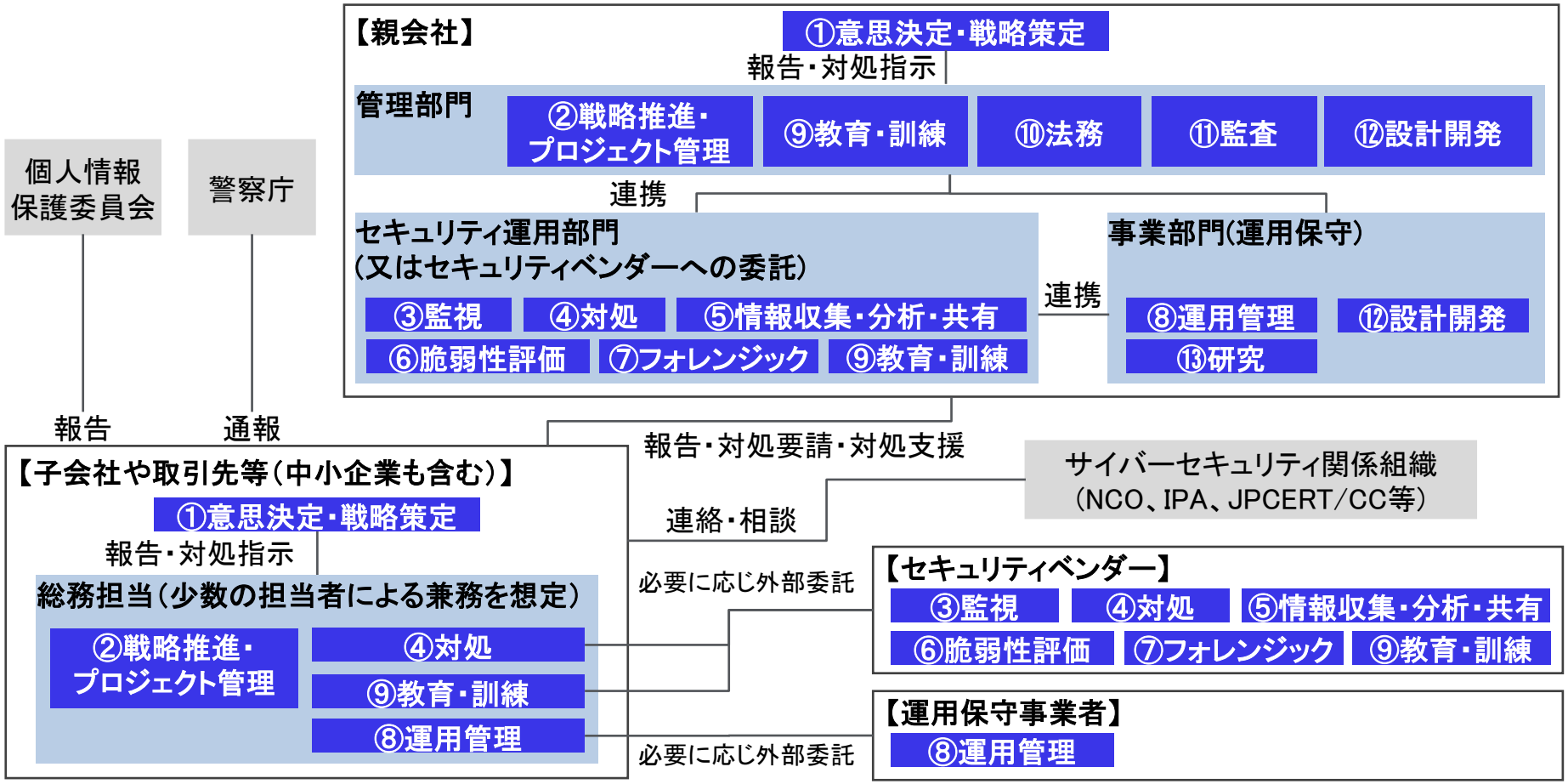
- 重要インフラ企業がサイバー攻撃を受けた状況において、官民が連携して事案対処を行う場面（下図）において求められる役割から、13の人材像を設定。
- 役割ごとにT（タスク）、K（知識）、S（スキル）を定義の上、4段階にレベル分け。

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②：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③：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。