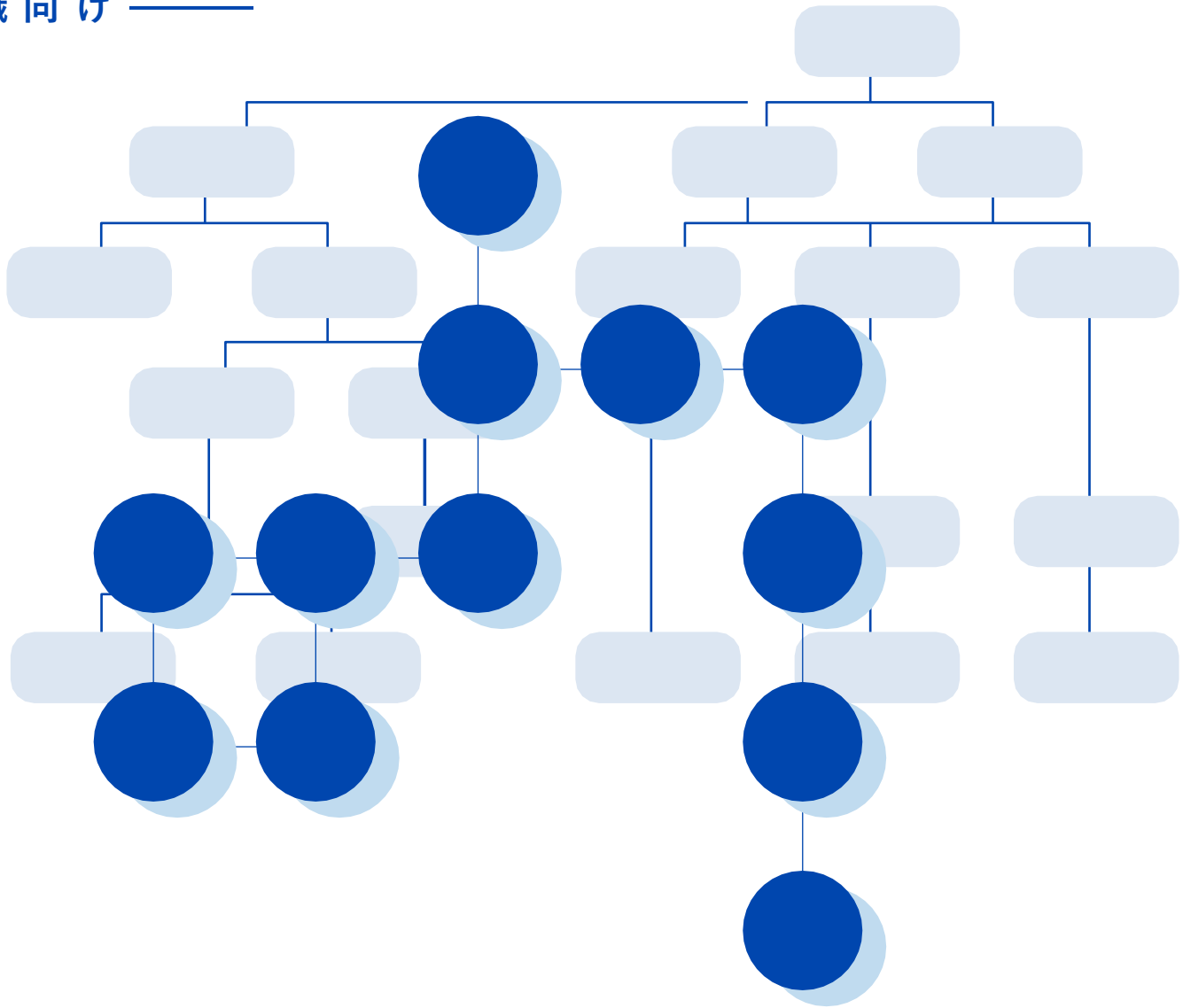
サイバーセキュリティ人材フレームワーク活用の手引き2026

―― 大規模組織向け ――



国家サイバー統括室
National Cybersecurity Office

令和8年4月3日

本書の位置づけ・利用上の留意点等について

位置づけ

- 本書は、「サイバーセキュリティ人材フレームワーク」の策定背景・目的、整理概念に加え、大規模組織における活用シーン・方法などを解説した「サイバーセキュリティ人材フレームワーク」の手引き書です。
- サイバーセキュリティ人材フレームワークの理解及び活用を支援することを目的に作成したものであり、各組織における人材育成、配置等を一律に義務づけるものではありません（各組織においては、本手引き書の内容を参考としつつ、自らの規模・特性に応じて適切に活用してください）。

想定利用者

- 本手引き書は、官民においてサイバーセキュリティ対策等に関わる者を主な利用者として想定します。
- 特に、事業内容が多様で一律の運用が難しい大規模組織を対象に、そのサイバーセキュリティを確保するために人材をどのように採用・配置・育成するのがよいかの検討に関わる方による活用を想定しています。

その他利用上の留意点

効力について

- 本手引き書は、法令、契約又は行政処分等の法的根拠となるものではなく、法的拘束力を有するものではありません。
- 本手引き書の内容と法令又は契約等の間に相違がある場合には、法令又は契約等が優先されます。

用語及び定義について

- 本手引き書にて記載する用語の定義は、基本的にサイバーセキュリティ人材フレームワークにおける定義に基づくものです。

情報の正確性及び更新について

- 本手引き書の内容は、作成時点における情報及び知見に基づくものであり、技術動向等により内容が変更される場合があります。
- 最新の情報については、関係機関が公表する資料等を参照してください。

出典の明示について

- 本手引き書を利用する際は下記の例に倣い、出典を記載してください。
  記載例）
  出典：国家サイバー統括室「サイバーセキュリティ人材フレームワーク活用の手引き2026（大規模組織向け）」（〇年〇月〇日に利用）

- 本手引き書を編集・加工等して利用する場合は、編集・加工等を行ったことを記載してください。
  なお、編集・加工した資料を、あたかも国（国家サイバー統括室）が作成したかのような態様で公表・利用してはいけません。

準拠法と合意管轄について

- 本手引き書の解釈等については、日本法を準拠法とします。
- 本手引き書に関連して生じた紛争については、東京地方裁判所を第一審の専属的合意管轄裁判所とします。

免責について

- 国（国家サイバー統括室）は、利用者が本手引き書を用いて行う一切の行為（編集・加工等した情報を利用することを含む。）について何ら責任を負うものではありません。

その他

- 本利用ルールは、著作権法上認められている引用などの利用について、制限するものではありません。
- 本利用ルールは今後変更される可能性があります。

目　次

共通事項

大規模組織向け事項

共　通　事　項

1．はじめに（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です。

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

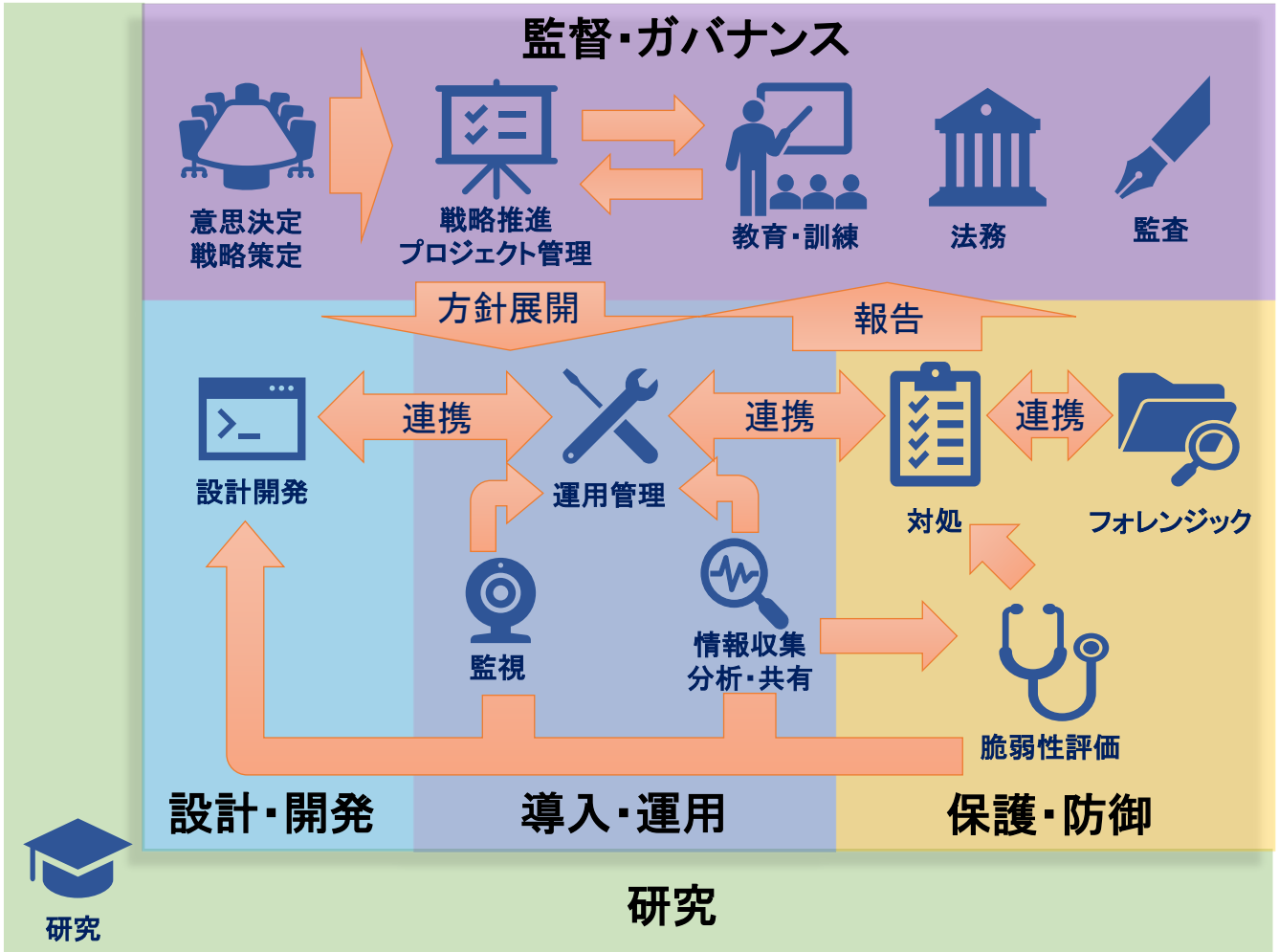
企業等　組織に必要な人材像を明確化し、採用・配置・育成等を計画的に進められる

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

サイバーセキュリティ人材が担うべき「役割」の全体像（イメージ）



通報・報告・連絡・相談

外部公的機関等

- 警察
- 個人情報保護委員会
- サイバーセキュリティ関連組織（NCO・IPA・JPCERT/CC等）

2．サイバーセキュリティ人材フレームワークの概要

- サイバーセキュリティ人材フレームワーク（Excel）は下表の各要素から構成されます。
- 各役割及び個別のタスク・知識・スキルとNICEフレームワークとの対応関係も明示しています。

各役割の定義シート（①～⑬）	● 13の役割を具体的に説明するため、以下の要素で構成 ➢ 主な業務（例）：その役割で実施する業務内容を示す。タスクの内容をまとめたものに相当 ➢ NICEフレームワークにおける対応ロール ➢ 想定される役職名等：組織において当該役割を担っている人材の主な役職名 ➢ 補足説明：国内の既存のフレームワークとの対応関係等を示す ➢ レベル：ITSSを参照した4段階のレベルを定義 ➢ 各役割で求められる汎用的なTKS:当該役割を担う人材が行うタスク(T)、及びそのタスクを実施するために必要な知識(K)及びスキル(S)

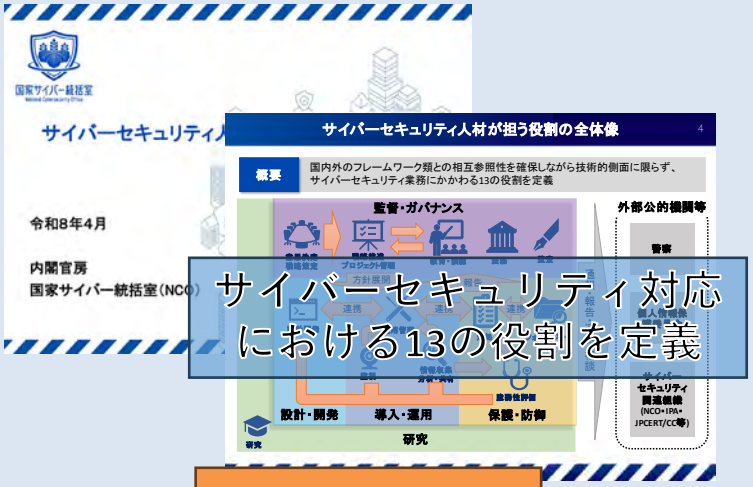
■TKSの考え方

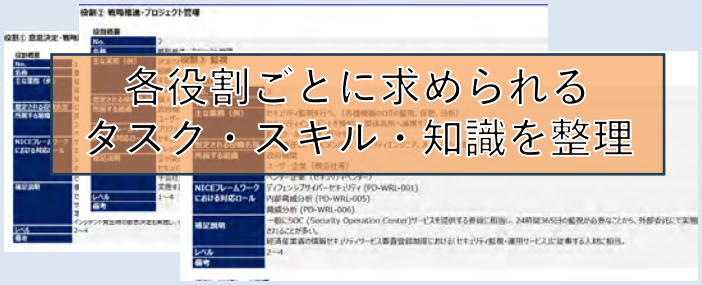
タスク(T)	● 本フレームワークで役割毎に定義しているタスク(T)とNICEフレームワークv2.1.0におけるタスクとの対応表を示す。 ● 原則として、本フレームワークで定義している1つのタスクについてNICEフレームワークのタスクが1つ以上対応するが、一部本フレームワーク独自のタスクが存在する。
知識(K)	● 本フレームワークで役割毎に定義している知識(K)とNICEフレームワークv2.1.0における知識との対応表を示す。 ● 原則として、本フレームワークで定義している1つの知識についてNICEフレームワークの知識が1つ以上対応するが、一部本フレームワーク独自の知識が存在する。
スキル(S)	● 本フレームワークで役割毎に定義しているスキル(S)とNICEフレームワークv2.1.0におけるスキルとの対応表を示す。 ● 原則として、本フレームワークで定義している1つのスキルについてNICEフレームワークのスキルが1つ以上対応するが、一部本フレームワーク独自のスキルが存在する。

3．手引き書とは（人材フレームワークとの対応関係等）

本書では、各組織において求められる「役割」を、各組織の規模・特性を踏まえ、タスク・知識・スキルをベースに「人材像」として具体化して説明します。

■人材フレームワーク





■手引き書(本書)

①：小規模組織

②：大規模組織

13の役割をもとに、組織の個別事情に応じた「人材像」として具体化（例を用いて説明）

③教育機関

人材育成に資する教育コンテンツ等の設計方針などを整理

④-1：個人(専門人材)

④-2：個人
(プラス・セキュリティ)

専門人材/プラス・セキュリティ別のスキル向上に役立つ情報を整理

【参考】各手引き書の想定読者一覧

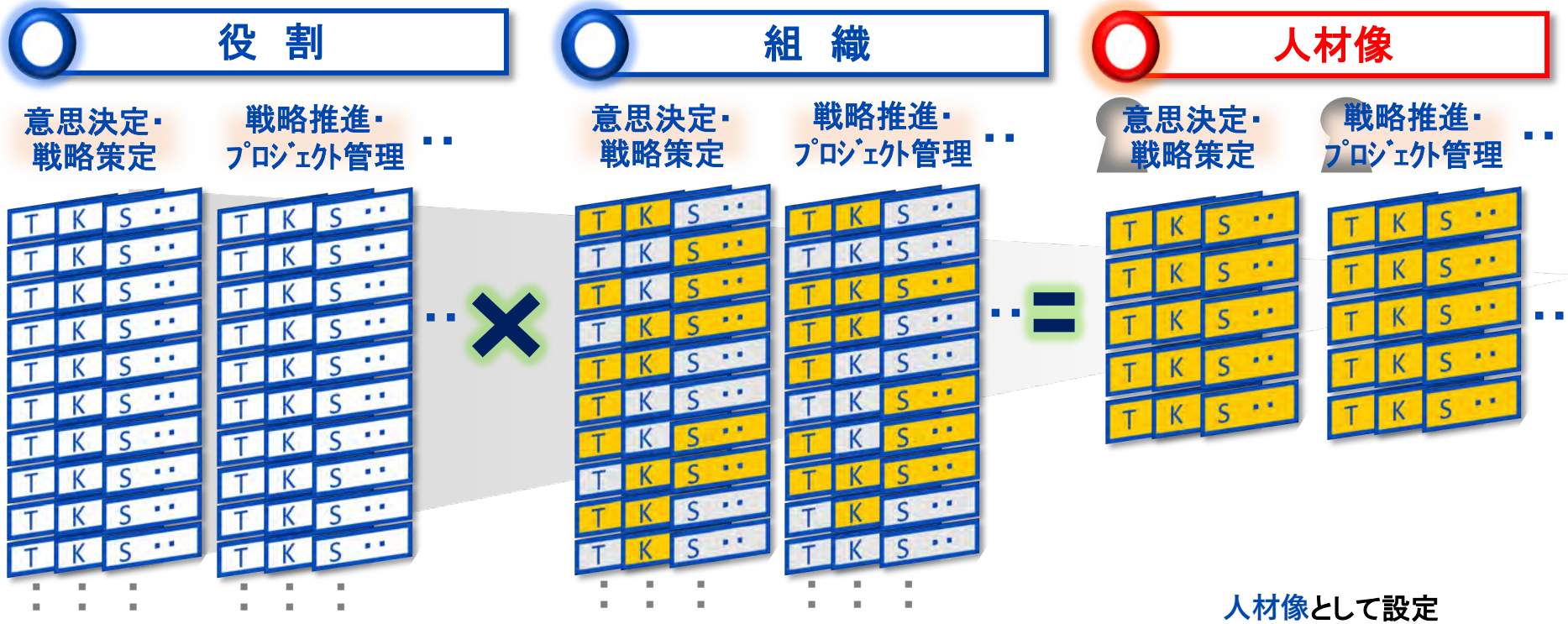
- 手引き書は各対象ごとに「主たる読者の属性」を想定し作成をしているものですが、主たる読者ではない属性の方も参考にしていただけるよう作成しておりますので、以下の対応表を参考にご利用ください。

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)

【参考】サイバーセキュリティにおける人材像の概念整理

- フレームワーク本体では、13の「役割」と各役割毎に汎用的なTKSを定義します。
- 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「（各役割の各組織における）人材像」とし、その具体化手順について手引き書にて提示します。



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、タスク（T）を絞り込み
（イメージ）橙：自組織で対応／灰：外部委託

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

4．他の人材フレームワークとの参照関係

本フレームワークと国内の他のフレームワークとの関係は以下の通りです。
必要に応じて他のフレームワークも併せてご参照いただけます。

	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			

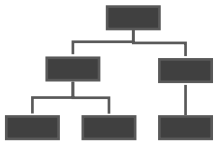
大規模組織向け事項

大規模組織向け手引き書2026の全体構成

- 本手引き書では、大規模組織におけるサイバーセキュリティ人材フレームワークの活用方法について主に以下の4点について解説します。
- 大規模組織においては、それぞれの事業内容やコーポレートガバナンスの特性に応じて、セキュリティガバナンスの体制も異なりますので、本手引き書を通じてセキュリティガバナンス体制の検討や、それらを踏まえた、職務記述書の記載・評価方法をお示しします。

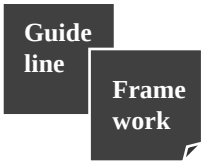
セキュリティガバナンス/セキュリティマネジメントの観点

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

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

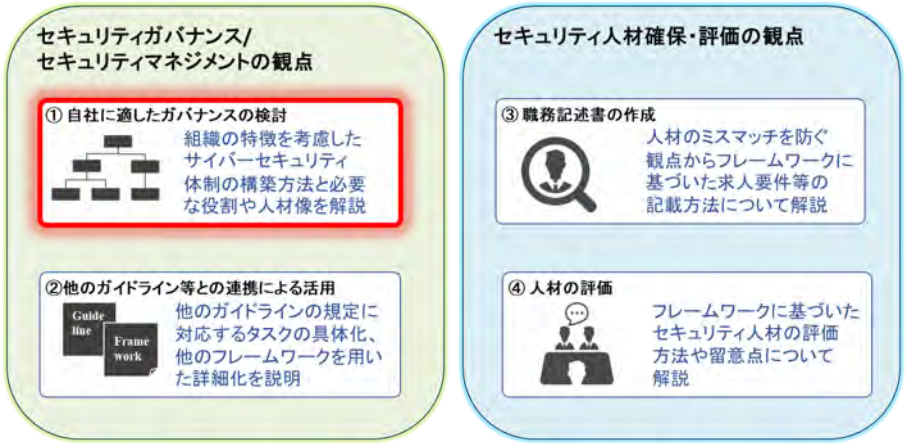
セキュリティ人材確保・評価の観点

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

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



①：セキュリティガバナンス体制の検討

大規模組織におけるサイバーセキュリティガバナンスの必要性

- 大規模企業ならではの課題として、自組織事業に関するコーポレートガバナンスやエンタープライズリスクマネジメントの観点から、サイバーセキュリティのガバナンスをどのように行うべきかが挙げられます。事業内容や組織構造を考慮する必要があり、自組織の特性に応じた検討が求められます。
- 経済産業省が公表している『サイバーセキュリティ経営ガイドラインVer3.0』※では、経営者がCISO等への指示を通じて確実に実施させるべき事項として下表の重要10項目を挙げていますが、同ガイドラインの付録である『サイバーセキュリティ体制構築・人材確保の手引き』では、**CISOがこれらを実践するための組織的な機能として「セキュリティ統括機能」を設置することを推奨**しています。
- 本書では、セキュリティ統括機能における特に人材面での考え方について、フレームワークを用いて説明します。

サイバーセキュリティ経営ガイドラインが規定する 経営者がCISO等への指示を通じて確実に実施させるべき重要10項目	
指示01	サイバーセキュリティリスクの認識、組織全体での対応方針の策定
指示02	サイバーセキュリティリスク管理体制の構築
指示03	サイバーセキュリティ対策のための資源（予算、人材等）確保
指示04	サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
指示05	サイバーセキュリティリスクに効果的に対応する仕組みの構築
指示06	PDCAサイクルによるサイバーセキュリティ対策の継続的改善
指示07	インシデント発生時の緊急対応体制の整備
指示08	インシデントによる被害に備えた事業継続・復旧体制の整備
指示09	ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策
指示10	サイバーセキュリティに関する情報の収集、共有及び開示の促進

CISO

ガバナンスに関する悩み

- 自社の組織ガバナンスにあったセキュリティリスク管理体制を構築したいが、各体制ごとにどういった人材が求められるのかがわからない
- 限られたセキュリティスキルを有する人材に最大限活躍していただくためには、どういった体制を構築すべきかがわからない
- CISOを支える人材としてどういった人材を確保すべきかがわからない

必要となる取組

- 組織の特徴にあったセキュリティ統括機能を設置
- フレームワークを参照し、必要となるタスクを担う人材を配置

※ サイバーセキュリティ経営ガイドラインが規定している内容及びセキュリティ統括機能の詳細については、次の資料を参照してください。
サイバーセキュリティ経営ガイドライン Ver3.0 及び **サイバーセキュリティ経営ガイドライン付録F サイバーセキュリティ体制構築・人材確保の手引き**（経済産業省）
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

フレームワークの役割と重要10項目との対応

- サイバーセキュリティ経営ガイドラインが規定する重要10項目を実践する際は、セキュリティガバナンスを担う「意思決定・戦略策定」及び「戦略推進・プロジェクト管理」の各役割を中心として、次のような対応となります。

経営者がCISO等への指示を通じて確実に実施させるべき重要10項目		意思決定・戦略策定	戦略推進・プロジェクト管理	その他の役割※
指示1	サイバーセキュリティリスクの認識、組織全体での対応方針の策定	● 各種方針の策定	● 個別プロジェクトの立案	–
指示2	サイバーセキュリティリスク管理体制の構築	● 体制の構築	● 体制の運用管理	–
指示3	サイバーセキュリティ対策のための資源（予算、人材等）確保	● 予算案の作成・配賦	● 人員・予算等の執行管理	● 【教育・訓練】人材の確保・育成
指示4	サイバーセキュリティリスクの把握とリスク対応に関する計画の策定	● 計画案の作成・承認	● 計画の執行管理	● 【情報収集・分析・共有】関連情報の収集 ● 【監査】リスクアセスメントの実施
指示5	サイバーセキュリティリスクに効果的に対応する仕組みの構築	● 計画案検討・承認 ● 対策状況確認	● 各プロジェクトの推進・管理	● 【監視】異常の継続的監視 ● 【情報収集・分析・共有】関連情報の情報収集 ● 【脆弱性評価】脆弱性診断の定期実施 ● 【運用管理】対策システム等の運用・保守 ● 【設計開発】対策システム等の設計開発 ● 【研究】先端技術の研究
指示6	PDCAサイクルによるサイバーセキュリティ対策の継続的改善	● 計画の検討・承認 ● 実施状況確認 ● 改善案の検討・承認	● PDCAサイクル管理	● 【監査】対策状況の監査 ● 【教育・訓練】人材の評価
指示7	インシデント発生時の緊急対応体制の整備	● 緊急対応体制の検討・指示	● インシデント対応に関するプロジェクト管理	● 【対処】インシデント対応準備、発生時対応
指示8	インシデントによる被害に備えた事業継続・復旧体制の整備	● 事業継続・復旧体制の検討・指示	● 事業継続・復旧に関するプロジェクト管理	● 【対処】インシデントからの復旧対応 ● 【フォレンジック】証拠保全、原因分析
指示9	ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策	● サプライチェーン対策の検討・指示	● 調達管理 ● 委託先管理	● 【法務】サプライチェーン関連のコンプライアンス対応
指示10	サイバーセキュリティに関する情報の収集、共有及び開示の促進	● 意思決定に必要な情報の収集指示、共有 ● 対外情報開示	● 関係機関との連携	● 【情報収集・分析・共有】関連情報の収集・共有

セキュリティ統括機能に含まれるタスク

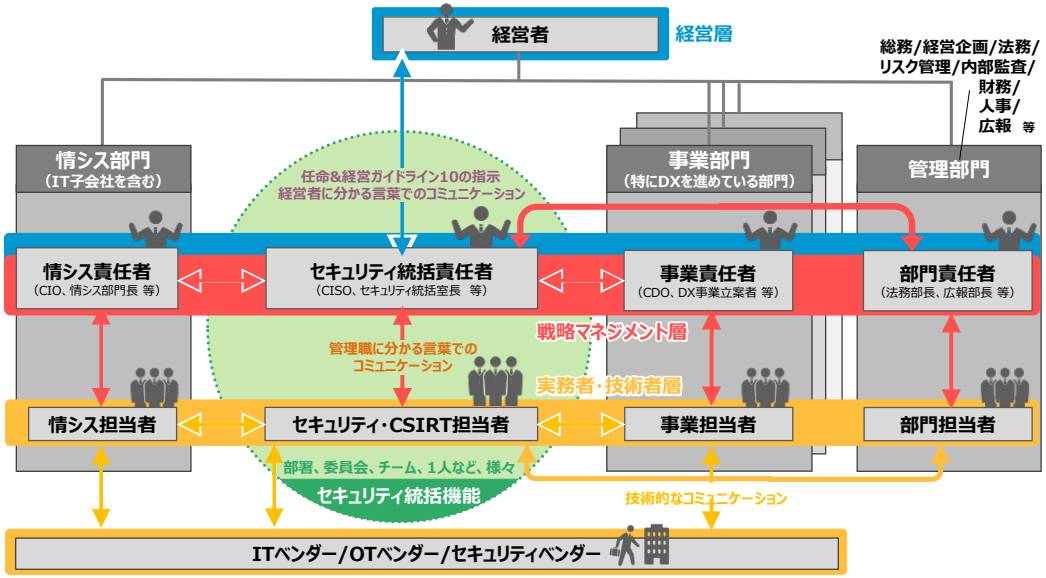
セキュリティ統括機能に含まれる可能性のあるタスク（組織の方針に依存）

※大規模組織におけるセキュリティ対策は、統括機能による「方針の決定（本書）」と、現場の個人による「業務での実践」が揃って初めて機能します。現場の実務担当者（専門人材、プラス・セキュリティ人材）の目線で求められるタスクやスキルについては、『**個人（専門人材）向け手引き書**』『**個人（プラス・セキュリティ）向け手引き書**』もご参照ください。

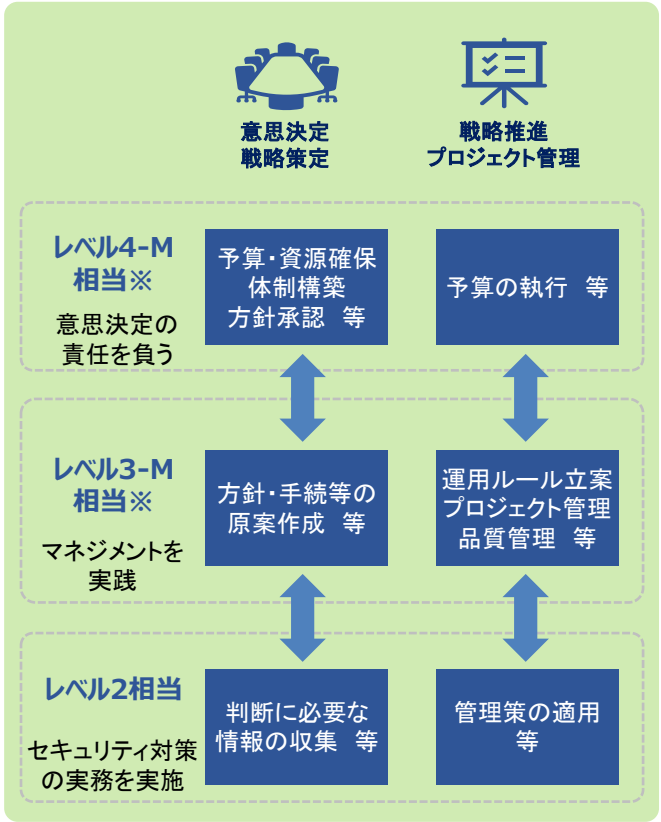
セキュリティ統括機能とは？

- 「セキュリティ統括機能」とは、企業におけるリスクマネジメント活動の一部として、セキュリティ対策及びセキュリティインシデント対応について、CISOや経営層による意思決定や、事業部門におけるセキュリティ対策の検討及び実施について、専門的な知見や経験をもとにサポートする機能のことを指します。
- 「セキュリティ統括」という言葉からは経営層に近いところで活動する印象を受けますが、実際にはフレームワークの「意思決定・戦略策定」や「戦略推進・プロジェクト管理」で規定されているタスクのうち、実務者層が行うようなものも受け持っているなど、その実装方法に応じて実務レイヤーも含めた形で組織階層を横断したセキュリティ対策を受け持つ場合もあります。

セキュリティ統括機能のイメージ



セキュリティ統括機能のタスク例



図の出典： サイバーセキュリティ経営ガイドライン付録F サイバーセキュリティ体制構築・人材確保の手引き（経済産業省）
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

※ セキュリティ対策の実務は、レベル2の担当者のほか、レベル3-E（独力での専門的実務遂行）やレベル4-E（高度な専門知識に基づく実務・指導）を担う人材も実施します。

セキュリティ統括機能をどのように実現するのがよいか（1/3）

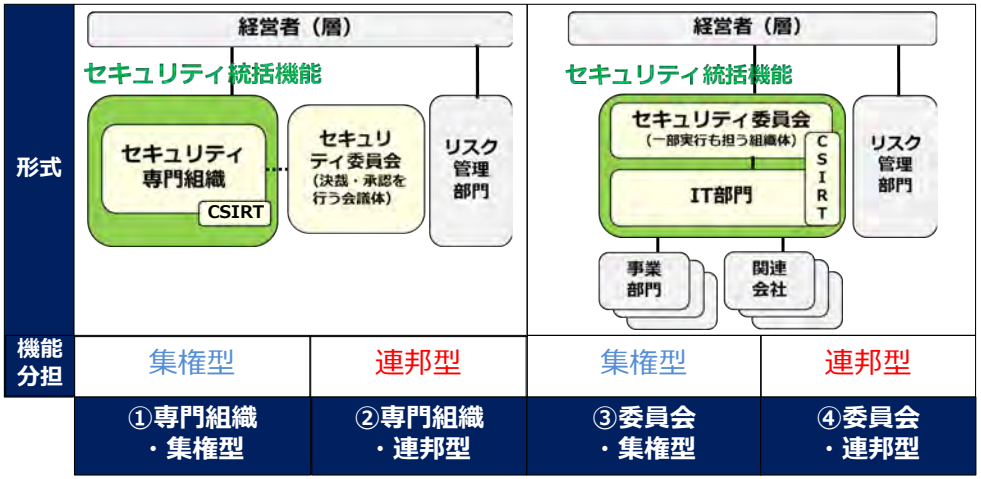
ポイント 組織の特性に応じたセキュリティ統括機能の組織形態と機能分担を検討します

- 『サイバーセキュリティ体制構築・人材確保の手引き』では、過去に大規模組織を対象とする調査結果に基づき、セキュリティ統括機能について、その「組織形態」と「機能分担」の方法に関する違いをもとに次の4つの類型に整理しています。
- 自組織の特徴に合った組織形態及び機能分担を選ぶ必要があるため、次ページ以降でその判別方法を説明します。

セキュリティ統括機能の組織形態
- **専門組織型：** セキュリティ統括機能を、セキュリティ統括室等の独立した部門や、情報システム部門の中のセキュリティチームなどの専門組織が担う
- **委員会型：** 事業部門・管理部門・情報システム部門・関連会社等からなるセキュリティ委員会が一部の実行機能も担い、その下に情報システム部門が位置づけられ、全社的なガバナンスを行う

セキュリティ統括機能の機能分担
- **集権型：** 全社で統一されたサイバーセキュリティ対策のルールに基づき、一元的に管理
- **連邦型：** サイバーセキュリティ対策のうち、全社システムは一カ所で統括、各事業部門・関連会社固有のシステムは各々が担当

セキュリティ統括機能の４類型※

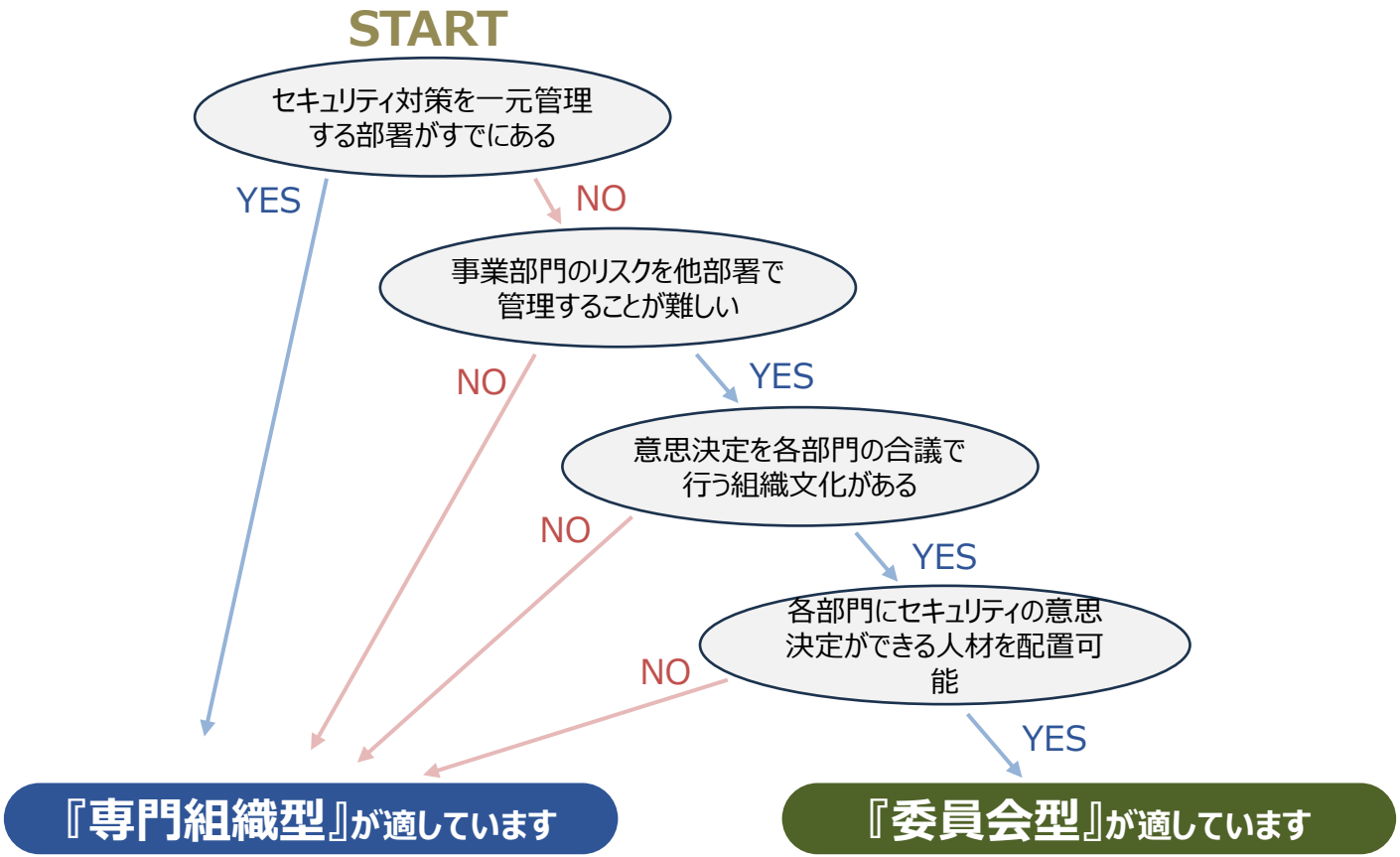


【補足】
近年、製造業では、IT関連インシデントを対象としたCSIRTに加えて、製品セキュリティに対応するPSIRT(Product Security Incident Response Team)や、製造設備に対応するFSIRT(Factory Security Incident Response Team)に重点をおいたセキュリティ統括機能を用意する企業が増えています

※一般社団法人日本情報システム・ユーザー協会（JUAS）：「平成30年度サイバーセキュリティ経済基盤構築事業（企業におけるサイバーセキュリティ体制の構築及び戦略マネジメント層の育成に関する実態調査）」（2019年3月）（現在は国立国会図書館のデジタルコレクションにて閲覧可能）
https://dl.ndl.go.jp/pid/14460066

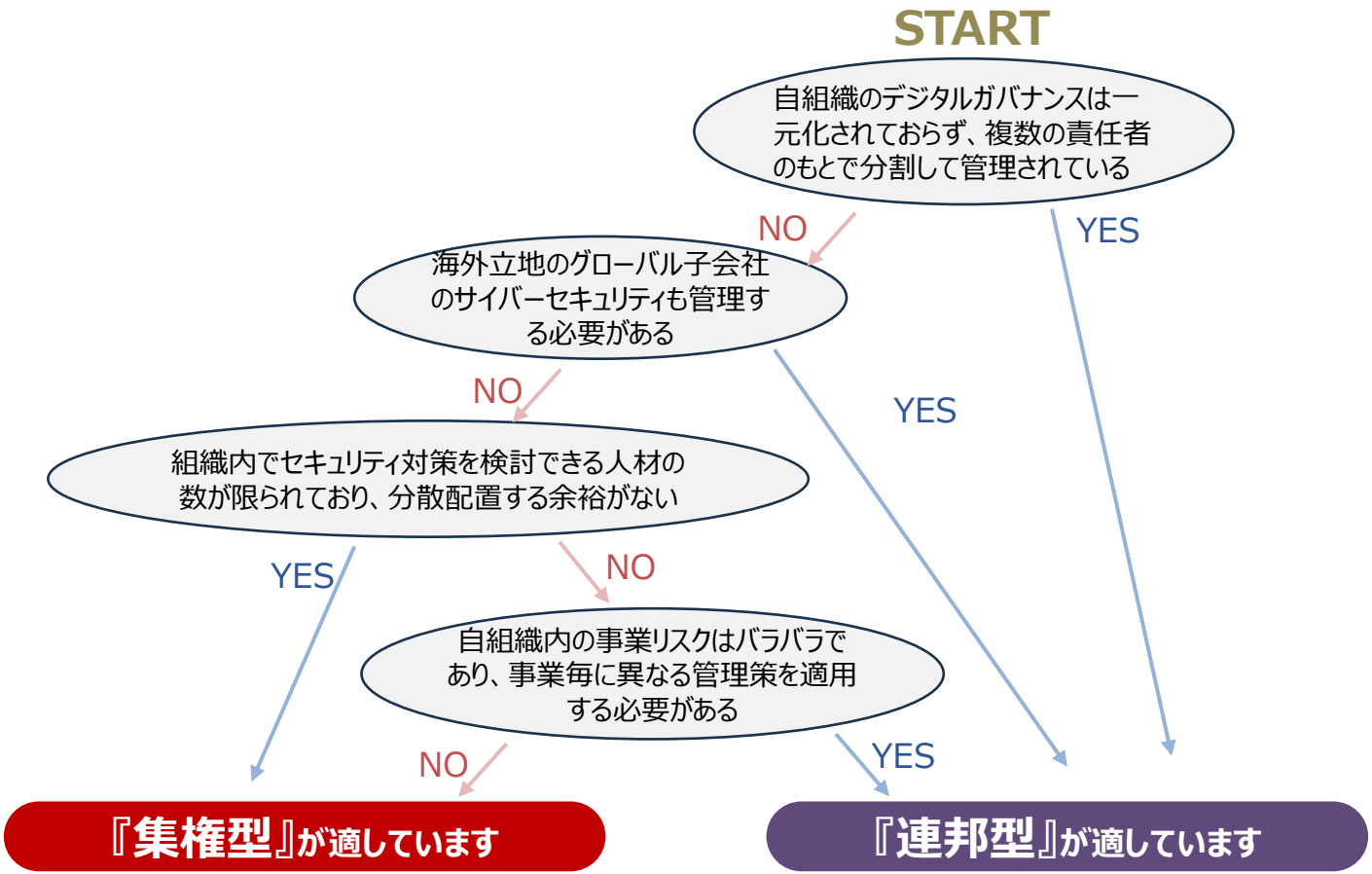
セキュリティ統括機能をどのように実現するのがよいか（2/3）

- 初めに、セキュリティ統括機能の組織形態として、「専門組織型」と「委員会型」のどちらが自組織に適しているかの判定のための簡易判定チャートを示します。
- 本表はあくまで参考であり、自組織にとって最適な形態が判定結果と異なる可能性もあることにご留意ください。

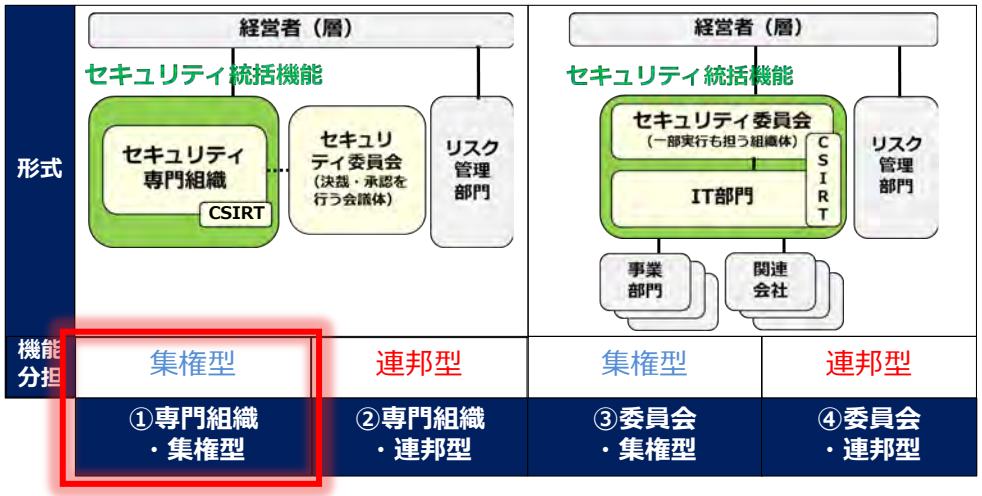


セキュリティ統括機能をどのように実現するのがよいか（3/3）

- 次に、セキュリティ統括機能の機能分担として、「集権型」と「連邦型」のどちらが自組織に適しているかの判定のための簡易判定チャートを示します。
- 本表はあくまで参考であり、自組織にとって最適な形態が判定結果と異なる可能性もあることにご留意ください。

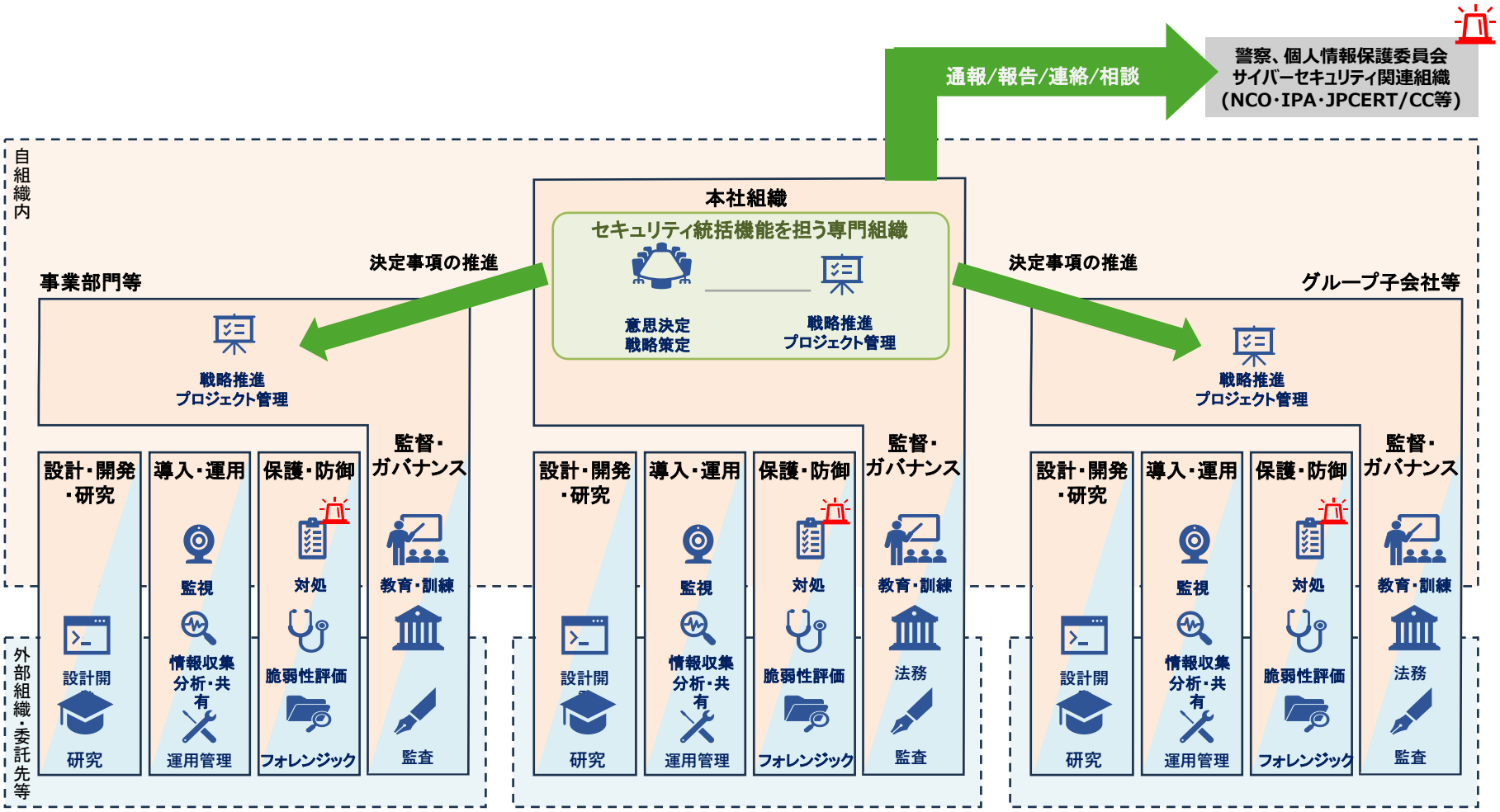


専門組織・集権型


形式
機能分担
経営者（層）
セキュリティ統括機能
セキュリティ専門組織
CSIRT
セキュリティ委員会（決裁・承認を行う会議体）
リスク管理部門
経営者（層）
セキュリティ統括機能
セキュリティ委員会（一部実行も担う組織体）
IT部門
CSIRT
リスク管理部門
事業部門
関連会社
集権型
連邦型
集権型
連邦型
①専門組織・集権型
②専門組織・連邦型
③委員会・集権型
④委員会・連邦型

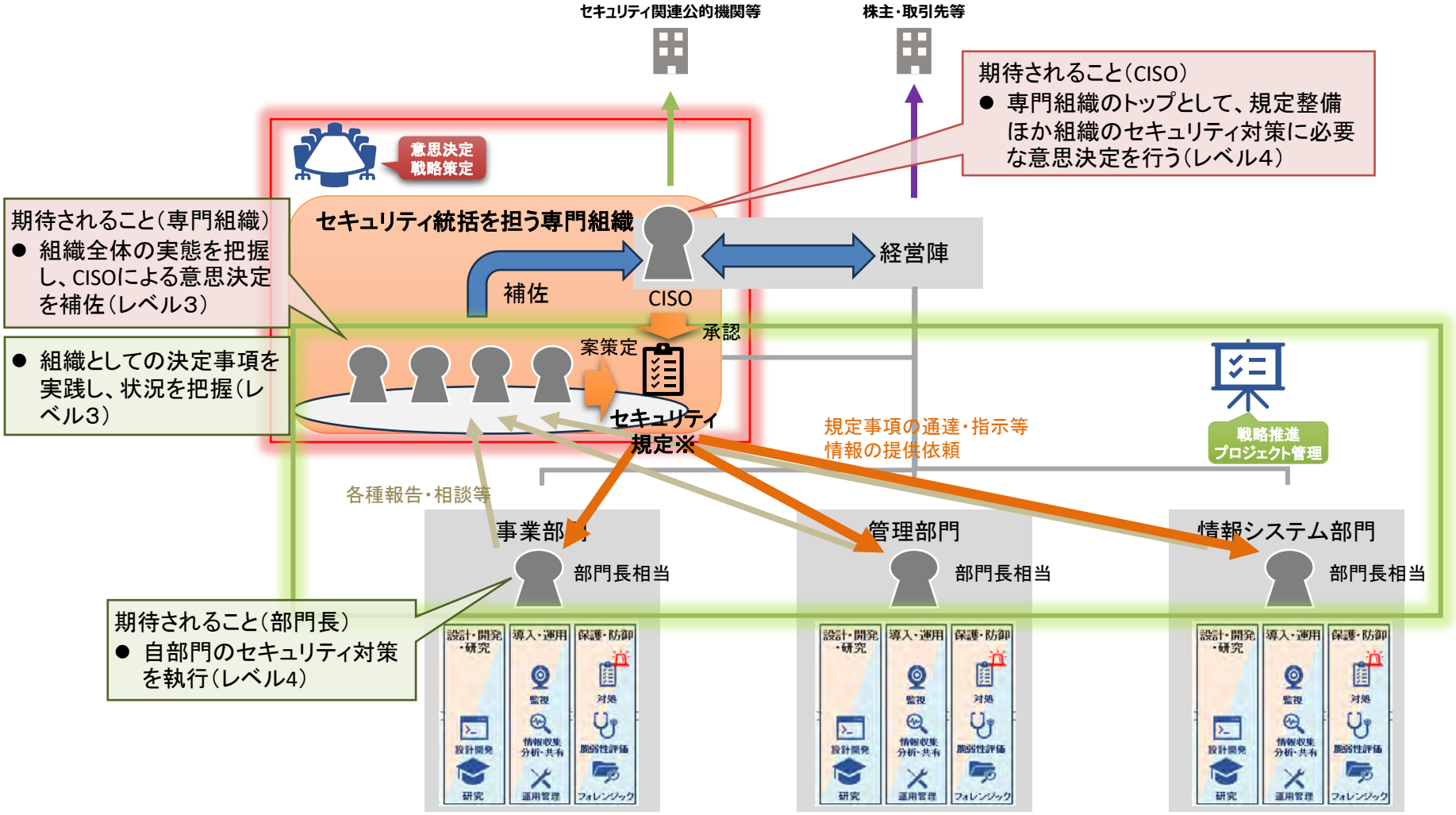
「専門組織・集権型」のガバナンス体制の基本的な考え方

- 「専門組織・集権型」のセキュリティ統括機能をフレームワークの役割定義を用いて表現すると次のようになります。
- 「専門組織・集権型」の特徴は、ガバナンスの専門人材を社内の1部署に集中配置することであり、このような専門性を有する人材数が限られている組織に適しています。



「専門組織・集権型」のガバナンス体制における主な役割の割り当て

- 本類型を採用した組織において、フレームワークの定める「意思決定・戦略策定」及び「戦略推進・プロジェクト管理」の役割をどこが担うかを以下に示します。
- セキュリティ統括を担う専門組織では、セキュリティ方針やそれを踏まえた具体的なセキュリティ規定までを一気通貫で定め、各部門ではその執行を担います。（図中※印）



「専門組織・集権型」のガバナンス実施において必要なタスク（セキュリティ統括を担う専門部署）

- 本類型を採用した組織において、CISOは専門組織の支援を得ながら、組織全体のサイバーセキュリティリスクを認識した上で、必要となるセキュリティ対策について指示を行います。

意思決定
戦略策定

期待されること：
- 規定整備ほか組織のセキュリティ対策に必要な意思決定及び指示をすべて専門組織が行う（担当者がCISOを補佐することで実施）

タスク	知識・スキル		知識・スキルをブレイクダウンしたもの	必要レベル	
				CISO	担当者
● サイバーセキュリティに関する意思決定・戦略策定に必要な情報を把握する ● サイバーセキュリティに関する監査とその結果に基づく見直しを実施する	**経営・組織運営、自組織の戦略に関する知識**	→	**自組織で行っている業務に関する知識**	4	3
			自組織で行っている業務で扱う情報に関する知識	4	3
	リスクマネジメントに関する知識	→	リスクマネジメントに関する知識	4	3
	サイバーセキュリティの最新技術や傾向に関する知識		**業務内容毎のサイバーセキュリティリスクに関する知識**	4	3
		→	**サイバーセキュリティリスクへの対策の種類とその効果、影響等に関する知識**	3	3
	組織のシステムやネットワークの基本原則や構造に関する知識	→	自組織で利用しているデジタル機器やサービス（クラウドを含む）に関する知識	3	3
	サイバーセキュリティに関する組織全体の構造と機能に関する知識	→	自組織におけるサイバーセキュリティリスクに関する目標や許容範囲に関する知識	3	3
	組織のポリシー等の策定および意思決定に係る手続に関する知識	→	**組織のポリシー等の策定および意思決定に係る手続に関する知識**	4	3
	今後組織におけるリスクとなり得るサイバーセキュリティ脅威を想定するスキル	→	**今後組織におけるリスクとなり得るサイバーセキュリティ脅威を想定するスキル**	3	3
	組織目標と体制を評価するスキル	→	**収集された情報をもとに、目標と体制の妥当性を評価するスキル**	4	3
	関係者と適切なコミュニケーションを行うスキル	→	**業務担当者との間で適切な対策実施に関する調整を行うスキル**	4	3

水色セル：当該ガバナンス類型において特に重要度が高く、優先的に習得・評価することが望ましい知識・スキル
黄色セル：担当範囲（組織全体）のサイバーセキュリティリスク対策の責任を負うことから、重要となる知識・スキル

「専門組織・集権型」のガバナンス実施において必要なタスク（各部門）

- 本類型を採用した組織において、各部門ではセキュリティ統括機能は担わず、専門組織において規定された手続等を執行する業務が中心となります。

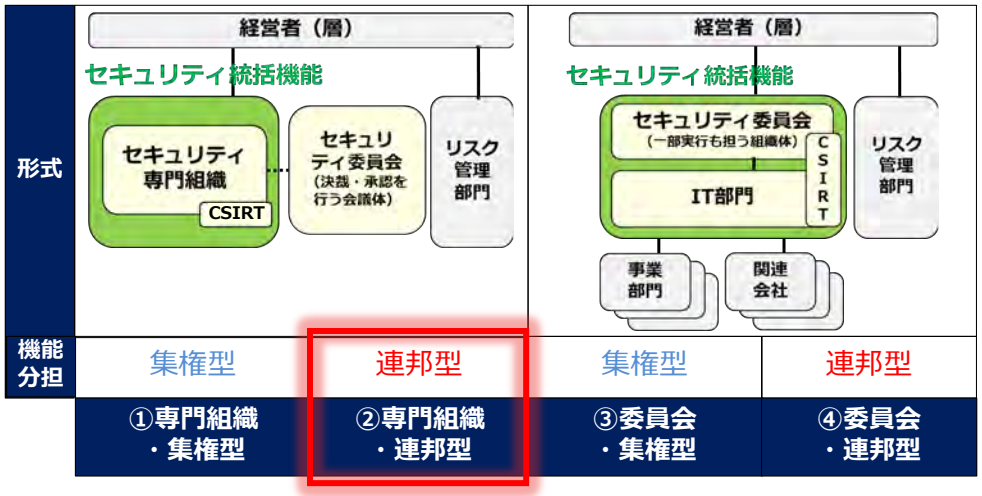
意思決定
戦略策定

期待されること：
- 自部門のセキュリティ対策を執行
- 意思決定が必要な場合は、セキュリティ統括を担う専門部署に相談して指示に従う

タスク	知識・スキル		知識・スキルをブレイクダウンしたもの	必要レベル	
				部門長	担当者
● サイバーセキュリティに関する意思決定・戦略策定に必要な情報を把握する ● サイバーセキュリティに関する監査とその結果に基づく見直しを実施する	**経営・組織運営、自組織の戦略に関する知識**	→	**自組織で行っている業務に関する知識**	3	3
			自組織で行っている業務で扱う情報に関する知識	3	3
	リスクマネジメントに関する知識	→	**リスクマネジメントに関する知識**	3	3
	サイバーセキュリティの最新技術や傾向に関する知識		業務内容毎のサイバーセキュリティリスクに関する知識	3	3
		→	サイバーセキュリティリスクへの対策の種類とその効果、影響等に関する知識	3	3
	組織のシステムやネットワークの基本原則や構造に関する知識	→	自組織で利用しているデジタル機器やサービス（クラウドを含む）に関する知識	3	3
	サイバーセキュリティに関する組織全体の構造と機能に関する知識	→	自組織におけるサイバーセキュリティリスクに関する目標や許容範囲に関する知識	3	3
	組織のポリシー等の策定および意思決定に係る手続に関する知識	→	組織のポリシー等の策定および意思決定に係る手続に関する知識	3	3
	今後組織におけるリスクとなり得るサイバーセキュリティ脅威を想定するスキル	→	今後組織におけるリスクとなり得るサイバーセキュリティ脅威を想定するスキル	3	3
	組織目標と体制を評価するスキル	→	収集された情報をもとに、目標と体制の妥当性を評価するスキル	3	3
	関係者と適切なコミュニケーションを行うスキル	→	**業務担当者との間で適切な対策実施に関する調整を行うスキル**	3	3

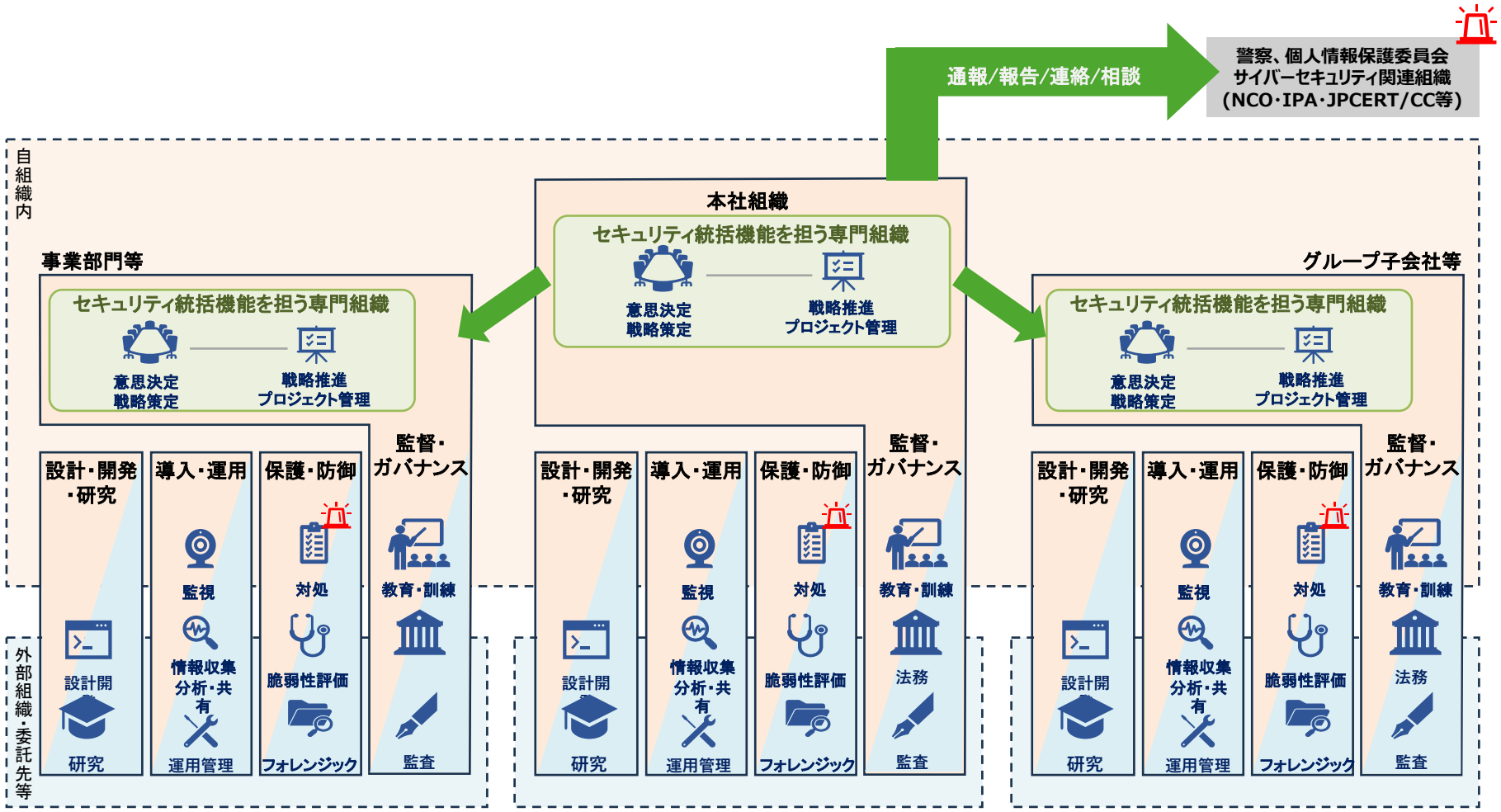
水色：当該ガバナンス類型において特に重要度が高く、優先的に習得・評価することが望ましい知識・スキル

専門組織・連邦型


形式
機能分担
経営者（層）
セキュリティ統括機能
セキュリティ専門組織
CSIRT
セキュリティ委員会
（決裁・承認を行う会議体）
リスク管理部門
経営者（層）
セキュリティ統括機能
セキュリティ委員会
（一部実行も担う組織体）
IT部門
CSIRT
リスク管理部門
事業部門
関連会社
集権型
連邦型
集権型
連邦型
①専門組織・集権型
②専門組織・連邦型
③委員会・集権型
④委員会・連邦型

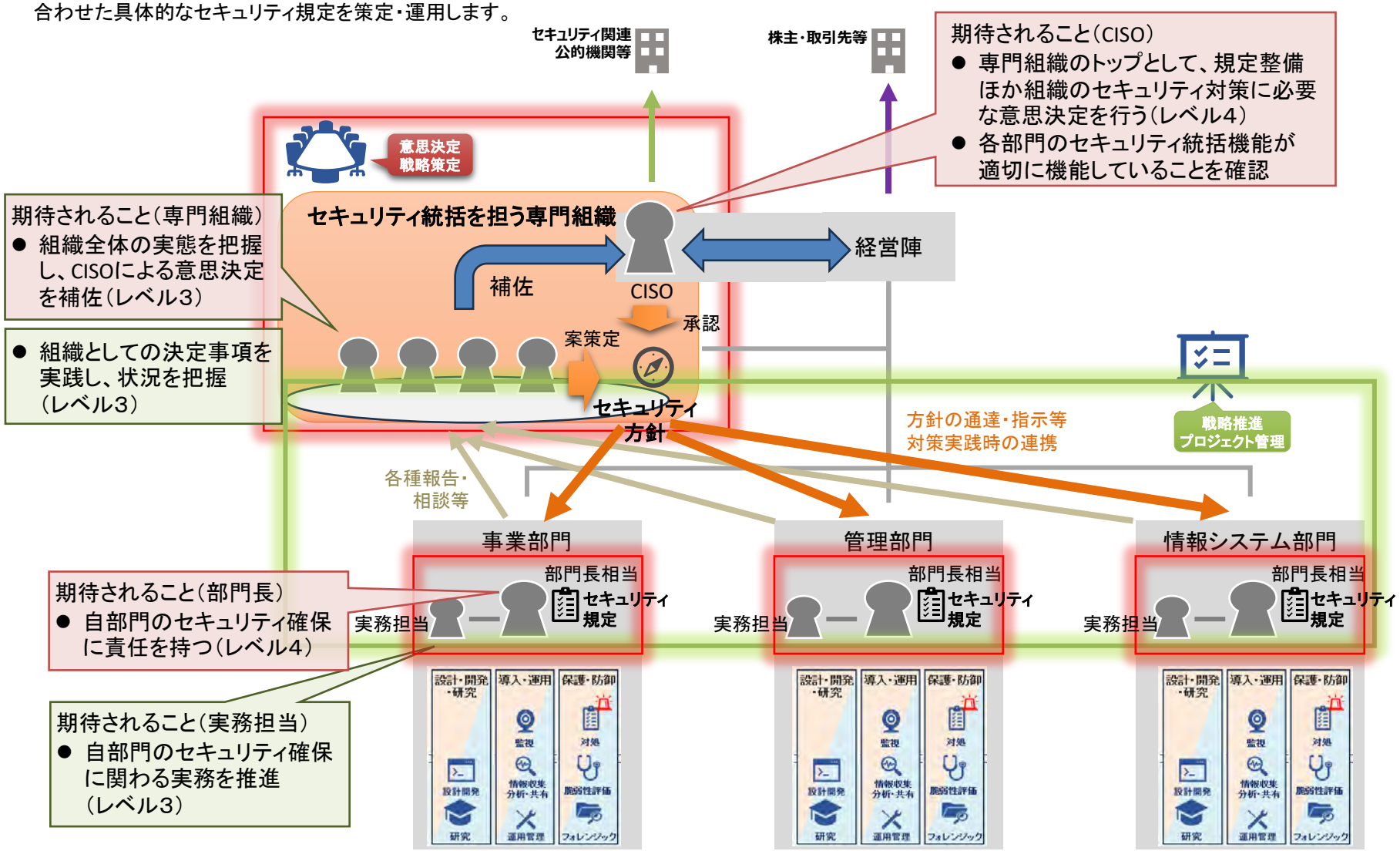
「専門組織・連邦型」のガバナンス体制の基本的な考え方

- 「専門組織・連邦型」のセキュリティ統括機能をフレームワークの役割定義を用いて表現すると次のようになります。
- 「専門組織・連邦型」の特徴は、セキュリティ統括機能を担う専門組織が社内に複数存在することであり、部門特有の事情を反映したガバナンスが可能となる一方で、組織間での対策状況の確認や調整が必要となります。



「専門組織・連邦型」のガバナンス体制における主な役割の割り当て

- 本類型を採用した組織において、フレームワークの定める「意思決定・戦略策定」及び「戦略推進・プロジェクト管理」の役割をどこが担うかを以下に示します。
- なお、本類型においては、セキュリティ統括を担う専門組織（本社）がセキュリティ方針までを定め、各事業部門等ではその方針を踏まえ、自部門の事業実態に合わせた具体的なセキュリティ規定を策定・運用します。



「専門組織・連邦型」のガバナンス実施において必要なタスク（セキュリティ統括を担う専門部署）

- 本類型を採用した組織において、CISOは専門組織の支援を得ながら、組織全体のサイバーセキュリティリスクを認識した上で、各部門のセキュリティ統括機能と連携しつつ、必要となるセキュリティ対策について指示を行います。

意思決定
戦略策定

期待されること:
- 組織のセキュリティ対策に関する方針策定等の意思決定を専門組織が行う（担当者がCISOを補佐することで実施）
- 必要に応じて、各部門のセキュリティ統括機能を支援する

タスク	知識・スキル		知識・スキルをブレイクダウンしたもの	必要レベル	
				CISO	担当者
● サイバーセキュリティに関する意思決定・戦略策定に必要な情報を把握する ● サイバーセキュリティに関する監査とその結果に基づく見直しを実施する	**経営・組織運営、自組織の戦略に関する知識**	→	**自組織で行っている業務に関する知識**	4	3
			自組織で行っている業務で扱う情報に関する知識	4	3
	リスクマネジメントに関する知識	→	リスクマネジメントに関する知識	4	3
	サイバーセキュリティの最新技術や傾向に関する知識		業務内容毎のサイバーセキュリティリスクに関する知識	4	3
		→	サイバーセキュリティリスクへの対策の種類とその効果、影響等に関する知識	3	3
	組織のシステムやネットワークの基本原則や構造に関する知識	→	自組織で利用しているデジタル機器やサービス（クラウドを含む）に関する知識	3	3
	サイバーセキュリティに関する組織全体の構造と機能に関する知識	→	**自組織におけるサイバーセキュリティリスクに関する目標や許容範囲に関する知識**	3	3
	組織のポリシー等の策定および意思決定に係る手続に関する知識	→	**組織のポリシー等の策定および意思決定に係る手続に関する知識**	4	3
	今後組織におけるリスクとなり得るサイバーセキュリティ脅威を想定するスキル	→	**今後組織におけるリスクとなり得るサイバーセキュリティ脅威を想定するスキル**	3	3
	組織目標と体制を評価するスキル	→	**収集された情報をもとに、目標と体制の妥当性を評価するスキル**	4	3
	関係者と適切なコミュニケーションを行うスキル	→	**業務担当者との間で適切な対策実施に関する調整を行うスキル**	4	3

水色：当該ガバナンス類型において特に重要度が高く、優先的に習得・評価することが望ましい知識・スキル

「専門組織・連邦型」のガバナンス実施において必要なタスク（各部門）

- 本類型を採用した組織において、各部門は自部門に関するセキュリティ統括機能を担います。そのため、意思決定に責任を負うために必要なレベルの習得が求められます。

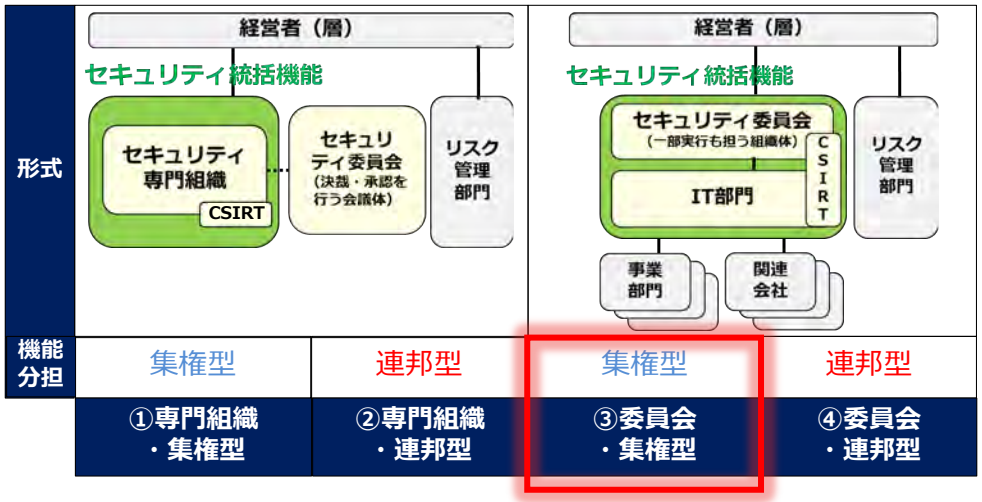
意思決定
戦略策定

期待されること:
- 自部門のセキュリティ統括機能を担い、セキュリティ確保に責任を持つ

タスク	知識・スキル		知識・スキルをブレイクダウンしたもの	必要レベル	
				部門長	担当者
● サイバーセキュリティに関する意思決定・戦略策定に必要な情報を把握する ● サイバーセキュリティに関する監査とその結果に基づく見直しを実施する	**経営・組織運営、自組織の戦略に関する知識**	→	**自組織で行っている業務に関する知識**	4	3
			自組織で行っている業務で扱う情報に関する知識	4	3
	リスクマネジメントに関する知識	→	リスクマネジメントに関する知識	4	3
	サイバーセキュリティの最新技術や傾向に関する知識		**業務内容毎のサイバーセキュリティリスクに関する知識**	4	3
		→	**サイバーセキュリティリスクへの対策の種類とその効果、影響等に関する知識**	3	3
	組織のシステムやネットワークの基本原則や構造に関する知識	→	自組織で利用しているデジタル機器やサービス（クラウドを含む）に関する知識	3	3
	サイバーセキュリティに関する組織全体の構造と機能に関する知識	→	自組織におけるサイバーセキュリティリスクに関する目標や許容範囲に関する知識	3	3
	組織のポリシー等の策定および意思決定に係る手続に関する知識	→	組織のポリシー等の策定および意思決定に係る手続に関する知識	4	3
	今後組織におけるリスクとなり得るサイバーセキュリティ脅威を想定するスキル	→	今後組織におけるリスクとなり得るサイバーセキュリティ脅威を想定するスキル	3	3
	組織目標と体制を評価するスキル	→	**収集された情報をもとに、目標と体制の妥当性を評価するスキル**	4	3
	関係者と適切なコミュニケーションを行うスキル	→	**業務担当者との間で適切な対策実施に関する調整を行うスキル**	4	3

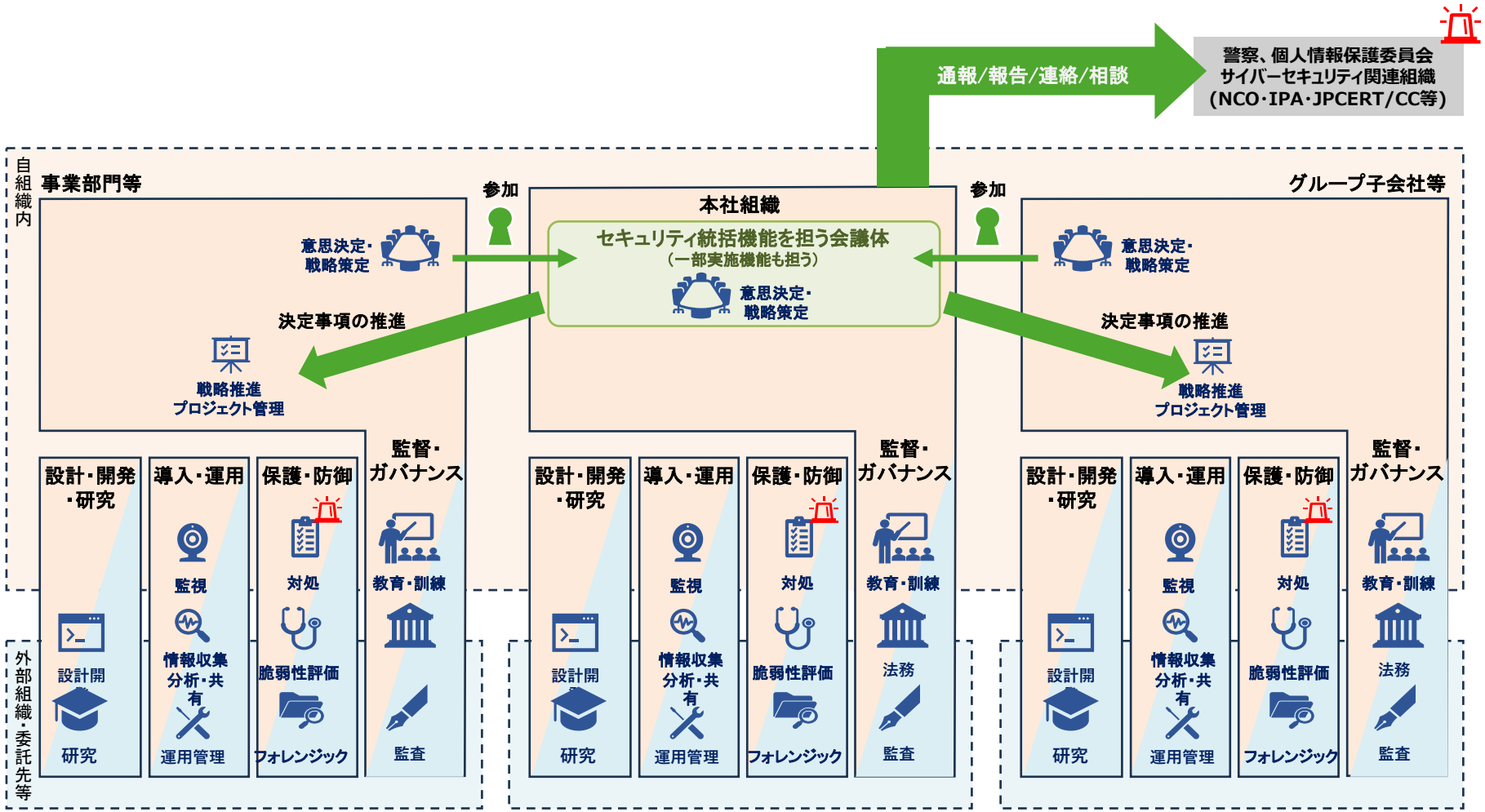
水色セル：当該ガバナンス類型において特に重要度が高く、優先的に習得・評価することが望ましい知識・スキル
黄色セル：担当範囲（自部門）のサイバーセキュリティリスク対策の責任を負うことから、特に重要となる知識・スキル

委員会･集権型


形式
経営者（層）
セキュリティ統括機能
セキュリティ専門組織
CSIRT
セキュリティ委員会（決裁・承認を行う会議体）
リスク管理部門
経営者（層）
セキュリティ統括機能
セキュリティ委員会（一部実行も担う組織体）
IT部門
CSIRT
リスク管理部門
事業部門
関連会社
機能分担
集権型
連邦型
集権型
連邦型
①専門組織・集権型
②専門組織・連邦型
③委員会・集権型
④委員会・連邦型

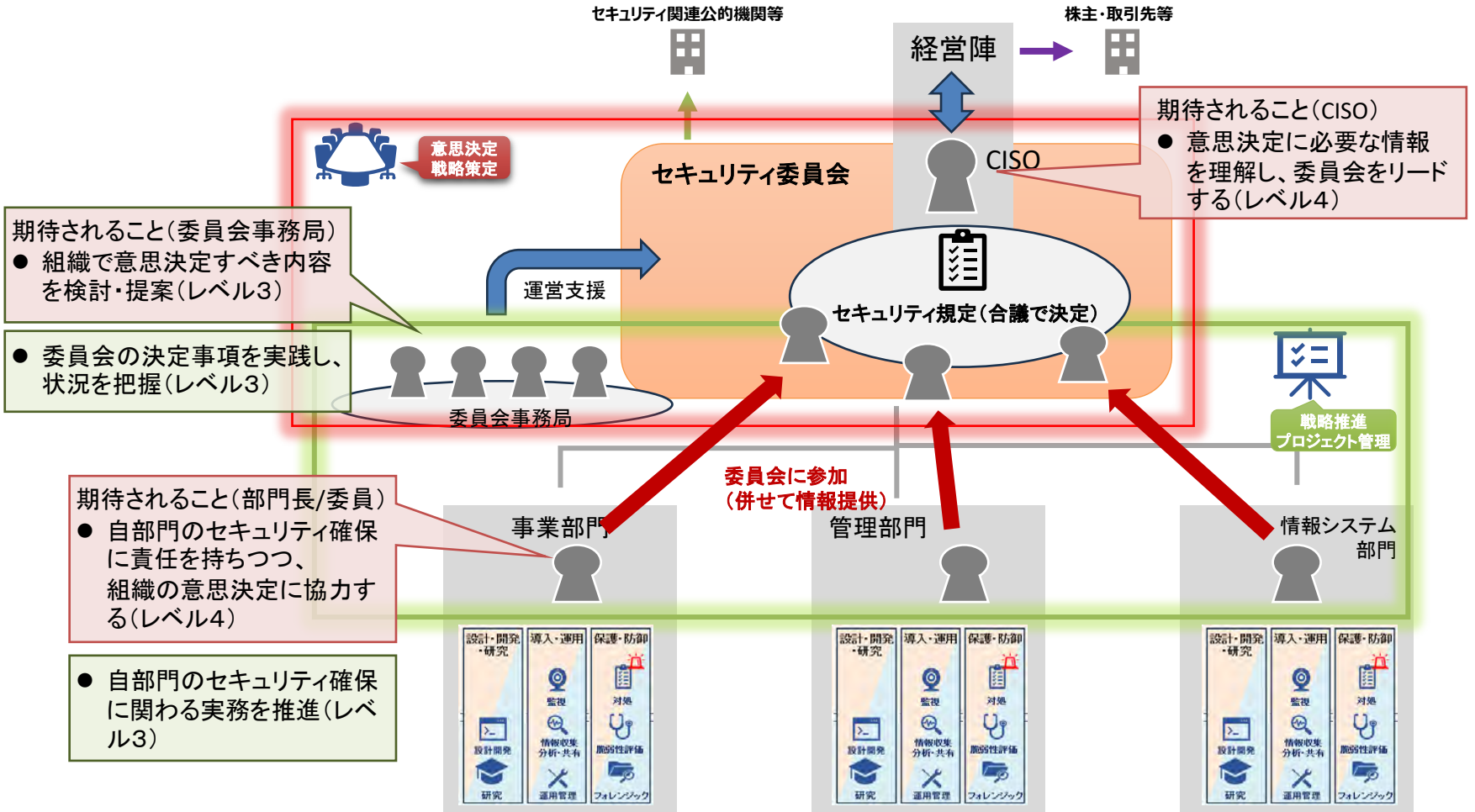
「委員会・集権型」のガバナンス体制の基本的な考え方

- 「委員会・集権型」のセキュリティ統括機能をフレームワークの役割定義を用いて表現すると次のようになります。
- 「委員会・集権型」の特徴は、ガバナンスに関する意思決定が主要部署間での合議によって行われる一方、実践に関しては組織横断的に統一された形で行われることです。



「委員会・集権型」のガバナンス体制における主な役割の割り当て

- 本類型を採用した組織において、フレームワークの定める「意思決定・戦略策定」及び「戦略推進・プロジェクト管理」の役割をどこが担うかを以下に示します。
- 本類型においては、セキュリティ委員会での合議を通じてセキュリティ方針を決定し、その方針に基づく具体的なセキュリティ規定は全社統一の形で策定されます。各部門は当該規定に基づき、自部門のセキュリティ対策を執行します。



「委員会・集権型」のガバナンス実施において必要なタスク（委員会）

- 本類型を採用した組織において、CISOは各部門からの委員の意見を調整しつつ、意思決定に向けた合意形成をリードします。
- 委員会事務局は、CISOを補佐するため、組織全体のリスク判断に必要な情報を把握し、委員会で決定した規定を各部門に通知します。

意思決定
戦略策定

期待されること:
- 組織内のセキュリティ対策に関する方針策定に必要な情報を集約し、委員会での審議を通じて意思決定を行う

タスク	知識・スキル		知識・スキルをブレイクダウンしたもの	必要レベル	
				CISO	事務局
● サイバーセキュリティに関する意思決定・戦略策定に必要な情報を把握する ● サイバーセキュリティに関する監査とその結果に基づく見直しを実施する	**経営・組織運営、自組織の戦略に関する知識**	→	**自組織で行っている業務に関する知識**	4	3
			自組織で行っている業務で扱う情報に関する知識	4	3
	リスクマネジメントに関する知識	→	リスクマネジメントに関する知識	4	3
	サイバーセキュリティの最新技術や傾向に関する知識		**業務内容毎のサイバーセキュリティリスクに関する知識**	4	3
		→	**サイバーセキュリティリスクへの対策の種類とその効果、影響等に関する知識**	3	3
	組織のシステムやネットワークの基本原則や構造に関する知識	→	自組織で利用しているデジタル機器やサービス（クラウドを含む）に関する知識	3	3
	サイバーセキュリティに関する組織全体の構造と機能に関する知識	→	自組織におけるサイバーセキュリティリスクに関する目標や許容範囲に関する知識	3	3
	組織のポリシー等の策定および意思決定に係る手続に関する知識	→	**組織のポリシー等の策定および意思決定に係る手続に関する知識**	4	3
	今後組織におけるリスクとなり得るサイバーセキュリティ脅威を想定するスキル	→	**今後組織におけるリスクとなり得るサイバーセキュリティ脅威を想定するスキル**	3	3
	組織目標と体制を評価するスキル	→	収集された情報をもとに、目標と体制の妥当性を評価するスキル	4	3
	関係者と適切なコミュニケーションを行うスキル		**業務担当者との間で適切な対策実施に関する調整を行うスキル**	4	3
		→	**会議体による合意形成のスキル**	4	ー

水色セル：当該ガバナンス類型において特に重要度が高く、優先的に習得・評価することが望ましい知識・スキル
黄色セル：担当範囲（組織全体）のサイバーセキュリティリスク対策の責任を負うことから、特に重要となる知識・スキル
紫色セル：委員会型のガバナンス実施において重要な知識・スキル

「委員会・集権型」のガバナンス実施において必要なタスク（各部門）

- 本類型を採用した組織において、本社機能のセキュリティ委員会の構成員を兼ねる部門長は、「専門組織・連邦型」の部門長のように自部署のセキュリティ対策のみを把握すればよいのではなく、組織全体の意思決定に必要な知見を備える必要があります。

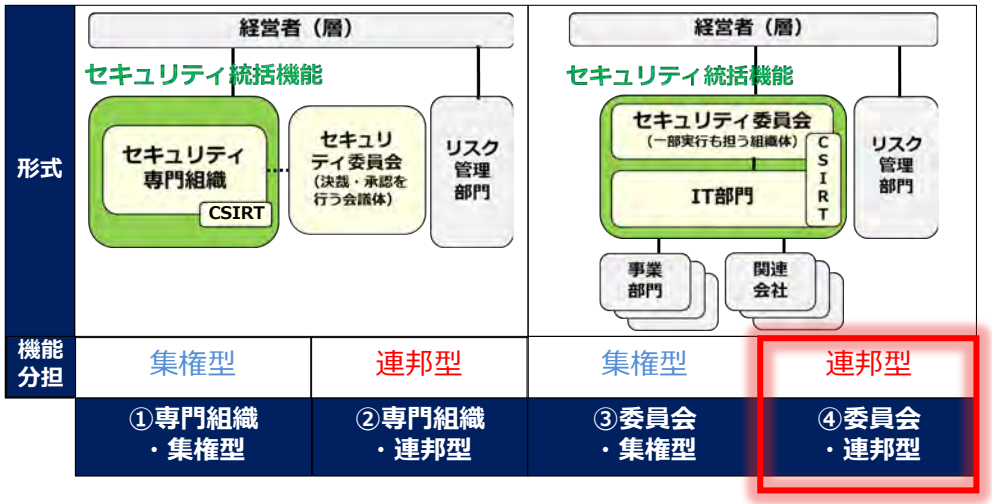
意思決定
戦略策定

期待されること:
- 委員としてのセキュリティ統括機能への参加を通じた、組織全体の意思決定への協力（自部署の条件の反映のほか、有用なプラクティスの共有）

タスク	知識・スキル		知識・スキルをブレイクダウンしたもの	必要レベル	
				部門長	担当者
● サイバーセキュリティに関する意思決定・戦略策定に必要な情報を把握する ● サイバーセキュリティに関する監査とその結果に基づく見直しを実施する	**経営・組織運営、自組織の戦略に関する知識**	→	**自組織で行っている業務に関する知識**	4	3
			自組織で行っている業務で扱う情報に関する知識	4	3
	リスクマネジメントに関する知識	→	**リスクマネジメントに関する知識**	4	3
	サイバーセキュリティの最新技術や傾向に関する知識	→	**業務内容毎のサイバーセキュリティリスクに関する知識**	4	3
			サイバーセキュリティリスクへの対策の種類とその効果、影響等に関する知識	3	3
	組織のシステムやネットワークの基本原則や構造に関する知識	→	自組織で利用しているデジタル機器やサービス（クラウドを含む）に関する知識	3	3
	サイバーセキュリティに関する組織全体の構造と機能に関する知識	→	自組織におけるサイバーセキュリティリスクに関する目標や許容範囲に関する知識	3	3
	組織のポリシー等の策定および意思決定に係る手続に関する知識	→	**組織のポリシー等の策定および意思決定に係る手続に関する知識**	4	3
	今後組織におけるリスクとなり得るサイバーセキュリティ脅威を想定するスキル	→	今後組織におけるリスクとなり得るサイバーセキュリティ脅威を想定するスキル	3	3
	組織目標と体制を評価するスキル	→	収集された情報をもとに、目標と体制の妥当性を評価するスキル	4	3
	関係者と適切なコミュニケーションを行うスキル	→	**業務担当者との間で適切な対策実施に関する調整を行うスキル**	4	3
			会議体による合意形成のスキル	4	―

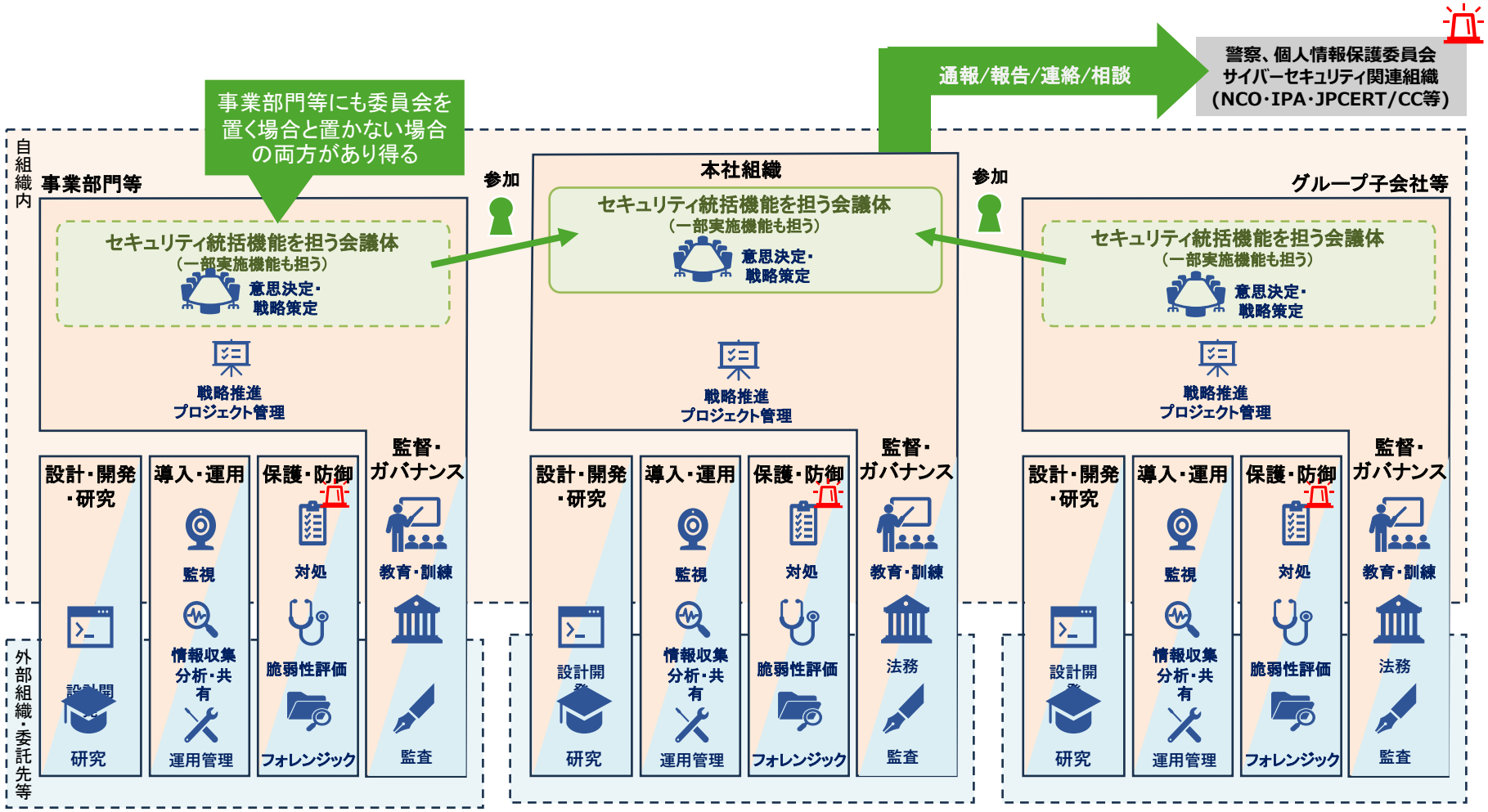
水色セル：当該ガバナンス類型において特に重要度が高く、優先的に習得・評価することが望ましい知識・スキル
紫色セル：委員会型のガバナンス実施において重要な知識・スキル

委員会・連邦型


形式
経営者（層）
セキュリティ統括機能
セキュリティ専門組織
CSIRT
セキュリティ委員会（決裁・承認を行う会議体）
リスク管理部門
経営者（層）
セキュリティ統括機能
セキュリティ委員会（一部実行も担う組織体）
IT部門
CSIRT
リスク管理部門
事業部門
関連会社
機能分担
集権型
連邦型
集権型
連邦型
①専門組織・集権型
②専門組織・連邦型
③委員会・集権型
④委員会・連邦型

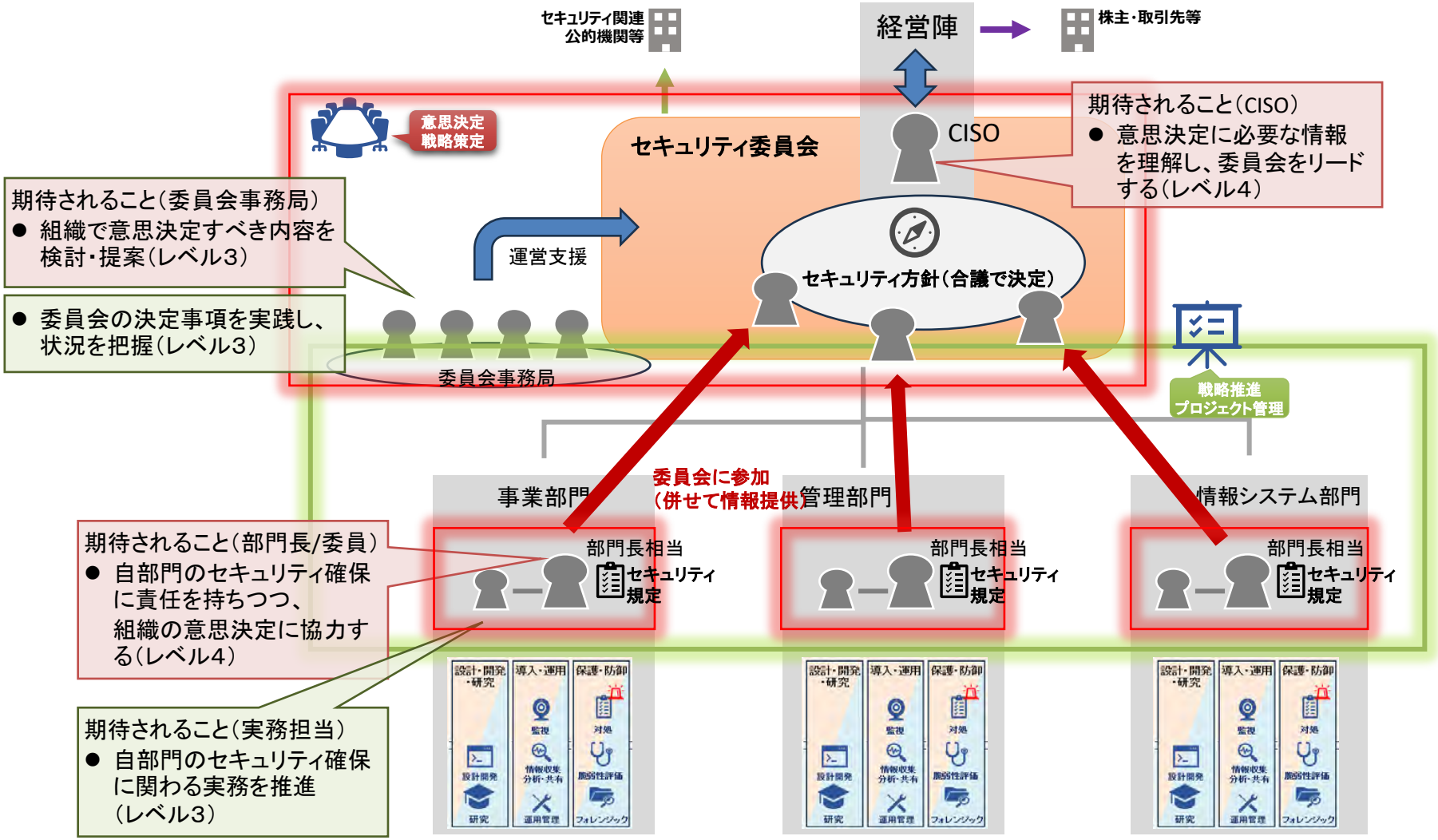
「委員会・連邦型」のガバナンス体制の基本的な考え方

- 「委員会・連邦型」のセキュリティ統括機能をフレームワークの役割定義を用いて表現すると次のようになります。
- 「委員会・連邦型」の特徴は、「委員会型」に起因する合議の必要性と「連邦型」に起因する複数の専門組織の設置の両面の特徴を併せ持つことであり、4つの類型の中でガバナンスを受け持つ人材数が最も多く必要となります。



「委員会・連邦型」のガバナンス体制における主な役割の割り当て

- 本類型を採用した組織において、フレームワークの定める「意思決定・戦略策定」及び「戦略推進・プロジェクト管理」の役割をどこが担うかを以下に示します。
- 本類型においては、セキュリティ委員会での合議を通じてセキュリティ方針を決定し、各事業部門等ではその方針を踏まえ、自部門の事業実態に合わせた具体的なセキュリティ規定を策定・運用します。



「委員会・連邦型」のガバナンス実施において必要なタスク（委員会）

- 本類型を採用した組織において、CISOは各部門からの委員の意見を調整しつつ、意思決定に向けた合意形成をリードします。

意思決定
戦略策定

期待されること：
- 組織内のセキュリティ対策に関する方針策定に必要な情報を集約し、委員会での審議を通じて意思決定を行う

タスク	知識・スキル		知識・スキルをブレイクダウンしたもの	必要レベル	
				CISO	事務局
● サイバーセキュリティに関する意思決定・戦略策定に必要な情報を把握する ● サイバーセキュリティに関する監査とその結果に基づく見直しを実施する	**経営・組織運営、自組織の戦略に関する知識**	→	**自組織で行っている業務に関する知識**	4	3
			自組織で行っている業務で扱う情報に関する知識	4	3
	リスクマネジメントに関する知識	→	リスクマネジメントに関する知識	4	3
	サイバーセキュリティの最新技術や傾向に関する知識		業務内容毎のサイバーセキュリティリスクに関する知識	4	3
		→	サイバーセキュリティリスクへの対策の種類とその効果、影響等に関する知識	3	3
	組織のシステムやネットワークの基本原則や構造に関する知識	→	自組織で利用しているデジタル機器やサービス（クラウドを含む）に関する知識	3	3
	サイバーセキュリティに関する組織全体の構造と機能に関する知識	→	自組織におけるサイバーセキュリティリスクに関する目標や許容範囲に関する知識	3	3
	組織のポリシー等の策定および意思決定に係る手続に関する知識	→	**組織のポリシー等の策定および意思決定に係る手続に関する知識**	4	3
	今後組織におけるリスクとなり得るサイバーセキュリティ脅威を想定するスキル	→	**今後組織におけるリスクとなり得るサイバーセキュリティ脅威を想定するスキル**	3	3
	組織目標と体制を評価するスキル	→	**収集された情報をもとに、目標と体制の妥当性を評価するスキル**	4	3
	関係者と適切なコミュニケーションを行うスキル		**業務担当者との間で適切な対策実施に関する調整を行うスキル**	4	3
		→	**会議体による合意形成のスキル**	4	―

水色セル：当該ガバナンス類型において特に重要度が高く、優先的に習得・評価することが望ましい知識・スキル
紫色セル：委員会型のガバナンス実施において重要な知識・スキル

「委員会・連邦型」のガバナンス実施において必要なタスク（各部門）

- 本類型を採用した組織において、本社機能のセキュリティ委員会の構成員を兼ねる部門長は、自部署のセキュリティ対策と組織全体の意思決定の責任を負うことから、全社のCISOに近い知識・スキルが必要となります。

意思決定
戦略策定

期待されること:
- 自部門のセキュリティ統括機能を担い、セキュリティ確保に責任を持つ
- 委員としてのセキュリティ統括機能への参加を通じた、組織全体の意思決定への協力（自部署の条件の反映のほか、有用なプラクティスの共有）

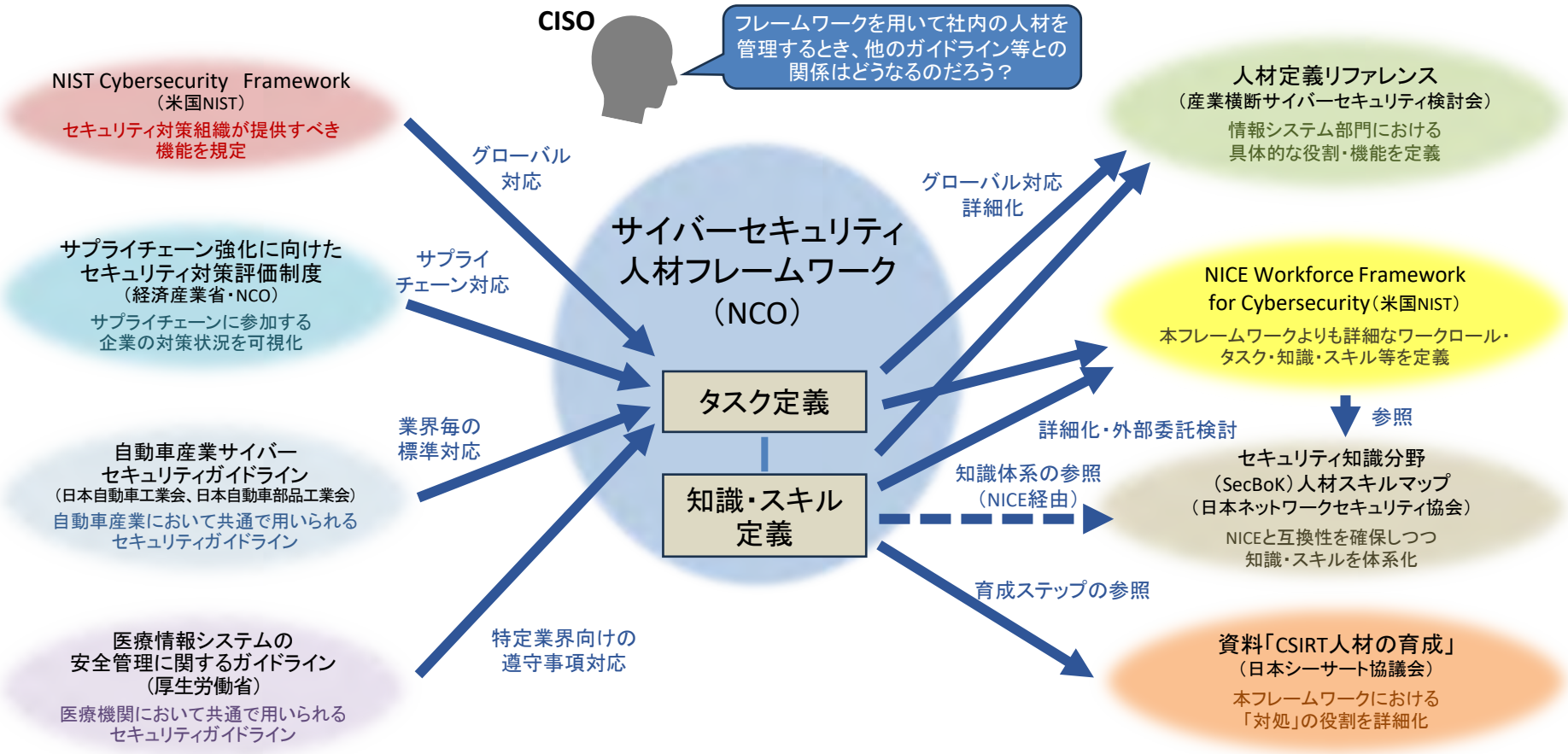
タスク	知識・スキル		知識・スキルをブレイクダウンしたもの	必要レベル	
				部門長	担当者
● サイバーセキュリティに関する意思決定・戦略策定に必要な情報を把握する ● サイバーセキュリティに関する監査とその結果に基づく見直しを実施する	**経営・組織運営、自組織の戦略に関する知識**	→	**自組織で行っている業務に関する知識**	4	3
			自組織で行っている業務で扱う情報に関する知識	4	3
	リスクマネジメントに関する知識	→	**リスクマネジメントに関する知識**	4	3
	サイバーセキュリティの最新技術や傾向に関する知識		**業務内容毎のサイバーセキュリティリスクに関する知識**	4	3
		→	**サイバーセキュリティリスクへの対策の種類とその効果、影響等に関する知識**	3	3
	組織のシステムやネットワークの基本原則や構造に関する知識	→	自組織で利用しているデジタル機器やサービス（クラウドを含む）に関する知識	3	3
	サイバーセキュリティに関する組織全体の構造と機能に関する知識	→	自組織におけるサイバーセキュリティリスクに関する目標や許容範囲に関する知識	3	3
	組織のポリシー等の策定および意思決定に係る手続に関する知識	→	組織のポリシー等の策定および意思決定に係る手続に関する知識	4	3
	今後組織におけるリスクとなり得るサイバーセキュリティ脅威を想定するスキル	→	今後組織におけるリスクとなり得るサイバーセキュリティ脅威を想定するスキル	3	3
	組織目標と体制を評価するスキル	→	**収集された情報をもとに、目標と体制の妥当性を評価するスキル**	4	3
	関係者と適切なコミュニケーションを行うスキル		**業務担当者との間で適切な対策実施に関する調整を行うスキル**	4	3
		→	**会議体による合意形成のスキル**	4	ー

水色セル：当該ガバナンス類型において特に重要度が高く、優先的に習得・評価することが望ましい知識・スキル
黄色セル：担当範囲（自部門）のサイバーセキュリティリスク対策の責任を負うことから、特に重要となる知識・スキル
紫色セル：委員会型のガバナンス実施において重要な知識・スキル

他のガイドライン等との連携による活用

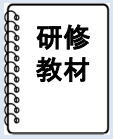
大規模組織を対象とするサイバーセキュリティ関連ガイドライン等の例

- ここでは、フレームワークを他のガイドラインやフレームワークと組み合わせて活用する方法として、他のガイドラインに準拠するためのタスクの具体化と、組織内での分担や教育の検討を目的として知識・スキルの詳細化に利用可能な外部のガイドライン等を示します。



目的に応じた利用例

- フレームワークを様々な目的に活用するためには、フレームワークを他のフレームワークやガイドライン等と組み合わせて用いることが有効です。前ページの図に示したとおり、外部ガイドライン等との連携方法は「タスクの具体化」「内製/外部委託の切り分け」「育成ステップの把握」「知識体系の参照」など多様であり、以下ではそれぞれの代表的なユースケースについて説明します。

	目　的	参照するガイドライン等の例	目的を達成するためのアプローチ
Case 1	『サプライチェーン強化に向けたセキュリティ対策評価制度』への対応に必要なタスクを各担当に割り当てたい 	**『サプライチェーン強化に向けたセキュリティ対策評価制度』関連資料**（経済産業省）	同制度の要求事項をもとに、フレームワークが規定するタスクの内容をブレイクダウンして担当に割り当て **➔ 本手引き書43ページ参照**
Case 2	サイバーセキュリティ対策に関して社内の人材で対応できないタスクを割り出した上で、外部委託で対応したい 	**人材定義リファレンス**（産業横断サイバーセキュリティ検討会）	「セキュリティオペレーション アウトソーシングガイド」を用いて対応する外部サービスを把握 **➔ 本手引き書44ページ参照**
Case 3	CSIRT要員を中心に、役割に応じた人材の教育方法を知りたい 	**資料「CSIRT人材の育成」**（日本シーサート協議会）	フレームワークとの対応付けを整理して、CSIRT業務等の人材育成ステップを把握 **➔ 本手引き書45ページ参照**
Case 4	社内研修用教材の作成にあたり、対象となる知識・スキルを体系的に整理したい 	**セキュリティ知識分野（SecBoK）人材スキルマップ**（日本ネットワークセキュリティ協会）	NICEフレームワークを介して知識カテゴリを参照し、研修教材の体系的整理に活用 **➔ 本手引き書46ページ参照**

Case1: 要求事項をもとにフレームワークのタスクの内容をブレイクダウン

- フレームワークを活用している組織が「サプライチェーン強化に向けたセキュリティ対策評価制度」の自己評価を行おうとするとき、同制度の要求事項をフレームワークのタスクと対応付けた上で、具体的な内容にブレイクダウンして各担当に割り当てることができます。

	フレームワークのタスク	タスクをブレイクダウン	「サプライチェーン強化に向けたセキュリティ対策評価制度」の★3の要求事項（抜粋）
意思決定・戦略策定	通常時のほか、緊急時や復旧時を含むサイバーセキュリティ対応体制を構築する	▶	✓ セキュリティ推進活動を担当する部署、役員及び従業員を決定し、責任及び権限を割り当てること。
	サイバーセキュリティに関する戦略、方針、規定等を策定又は承認する	▶	✓ 守秘義務のルールを策定し、遵守させること。 ✓ 自社のセキュリティ対応方針を策定し、周知すること。
戦略推進・プロジェクト管理	プロジェクトで使用する機器等の調達及びサプライチェーン管理	▶	✓ 取引先と自社とのビジネス又はシステム上の関係を把握すること。 ✓ 自社の機密情報の取扱い方法を、共有先との間で明確にすること。 ✓ セキュリティインシデント発生時の他社との役割及び責任を明確にすること。
監視	対象システムや機器等からログを収集	▶	✓ ネットワーク上の適切な場所でネットワーク接続及びデータ転送を監視すること。
対処	インシデント対処準備	▶	✓ セキュリティインシデントへの対応手順、対応体制等を定めること。 ✓ 事業上重要なシステムについて、事業継続の要件に沿う復旧に必要な準備を行うこと。
運用管理	構成管理及び変更管理	▶	✓ 情報機器、OS及びソフトウェアに関する情報を把握すること。 ✓ ネットワークに関する情報を把握するための仕組みを整備すること。 ✓ 情報機器、OS及びソフトウェアの安全な構成を確立し、維持すること。
	通常時・インシデント又は通信障害発生時の運用ルールの起案	▶	✓ 自社の機密情報を扱う外部情報サービスを管理すること。 ✓ 機密区分に応じた情報の管理ルールを定め、それに基づく管理を行うこと。
	ユーザーアカウント・権限管理	▶	✓ ユーザID の発行・変更・削除の手続を定め、適切に運用すること。 ✓ 管理者IDの発行・変更・削除の手続を定めること。 ✓ パスワード設定に関するルールを定め、周知すること。 ✓ パスワードの管理に関するルールを定め、周知すること。
	アクセス制御方針の作成及び方針に基づいたアクセス制御の実行	▶	✓ アクセス権の管理ルールを定めること。
	システム及びネットワーク機器のアップデート・バックアップの管理	▶	✓ 適切なバックアップを行うこと。 ✓ 情報機器、OS及びソフトウェアへのセキュリティパッチ及びアップデートの適用に係る手続を策定し、実行すること。
	システム及びネットワーク機器に対する初期設定の実施	▶	✓ パソコン及びスマートデバイスにはロック制御を行うこと。 ✓ システムをマルウェア感染から保護すること。 ✓ 内外のネットワークを適切に分離し、境界部分を防護すること。
教育・訓練	教育・訓練の実施	▶	✓ セキュリティインシデント発生時の対応に関する教育・訓練を行うこと。
設計開発	設計	▶	✓ システム及び情報の重要度に応じて認証の強度及び実装方法を決定すること。

（出典）経済産業省「「サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針」（SCS評価制度の構築方針）を公表しました」をもとに作成
https://www.meti.go.jp/press/2025/03/20260327001/20260327001.html

Case2: 自社の人材で対応不可のタスクについての外部委託を検討

- 産業横断サイバーセキュリティ検討会ではいわゆるユーザー企業の情報システム部門が保有すべきサイバーセキュリティ対策機能を定義するだけでなく、それらの機能を組織内の人材で提供することが不可能な場合の外部委託に関する情報提供をしています。これをフレームワークのタスクのうち対応できないものの外部委託の検討に活用する例を以下に示します。

フレームワークの役割とタスク		サイバーセキュリティ対策機能を実現する業務例	アウトソーシングの内容（●◆★は提供主体の違いを示す：右記参照）
脆弱性評価	脆弱性評価の実施	脆弱性診断（導入時・運用時）	脆弱性診断サービス、テスト計画策定支援★
運用管理	システム及びネットワークの管理業務に対する評価及び改善策の実施	セキュリティ対策関連の製品・サービスの選定及び実装支援	基幹・業務システムごとのセキュリティ製品適合性調査● セキュリティ製品　他社との適合性情報提供◆ セキュリティサービス　セキュリティ対応◆ セキュリティ製品評価★ セキュリティサービス評価★
	ユーザーアカウント・権限管理	Active Directory管理 シングルサインオン管理	設定変更実務● シングルサインオン関連　製品・サービス情報提供◆ 多要素認証関連　製品・サービス情報提供◆ 認証におけるセキュリティ対策支援★
	事業継続計画（BCP）の立案	ICT環境における事業継続計画の策定	システム冗長化　企画立案● リスク評価・リスク分析★ BCP／BCM 策定★
	システム及びネットワーク機器のアップデート・バックアップの管理	パッチ適用時の評価テスト	構築・運用システム　パッチ適用● パッチ管理サービス提供◆ サイバー攻撃情報提供、パッチ情報提供★
	ユーザーからの問合せに対するサポート	社内のICTリテラシー向上のためのユーザー支援	ユーザーサポート● コールセンターサービス◆
教育・訓練	教育・訓練の実施	リスク対応教育の企画・計画・実施	研修企画・実施・報告●
設計開発	設計	セキュア構築設計の企画立案 要件定義及基本設計におけるセキュアデザイン	システム構築　セキュリティ対応● 要件定義・基本設計・詳細設計● セキュア構築設計　レビュー★

●：構築・運用委託先インテグレーター
◆：製品・サービスベンダー
★：セキュリティ専門事業者

自社の人材で対応不可のタスクについての外部委託仕様の検討に活用が可能

（出典）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』セキュリティオペレーションアウトソーシングガイド https://cyber-risk.or.jp/cric-csf/report/

Case3: CSIRT業務に関する人材育成ステップの把握

- 日本CSIRT協議会（NCA）ではCSIRT業務に従事する広義の人材を対象として7種類の役割を定義し、それぞれの育成方法を説明しています。
- 下表のようにフレームワークと区分方法は若干異なりますが、対応する役割の参照を通じてそれぞれの担当者の育成にNCAの資料を活用することが可能です。

フレームワークの役割定義	『CSIRT人材の育成』Ver1.0で定義されている役割の例	
意思決定・戦略策定	連絡・全体統括	● 経営者、関係者とのコミュニケーション
戦略推進・プロジェクト管理	セキュリティマネジメント	● 情報セキュリティガバナンスの取組みを維持 ● 情報資産管理、ISMS運用 ● BCP、災害対策の実践
監視	情報収集/情報分析（SOC/監視）	● SOC/監視システムと業務の設計/構築/導入/運用/維持 ● アラート分析、影響評価、関係者連絡、レポート作成
対処	連絡・全体統括	● トリアージを含めた指示、他部署と連携した事案対応
情報収集・分析・共有	インシデント対応	● インシデント対応作業の実行（他役割と連携） ● インテリジェンスを含めたリスク判断の実施
	情報収集/情報分析（SOC/監視）	● 脅威情報の収集、活用
脆弱性評価	脆弱性管理/診断	● 脆弱性管理ルールの運用 ● 脆弱性診断の請負
フォレンジック	フォレンジック	● データ収集、解析/抽出、分析、報告
運用管理	開発/開発支援	● セキュリティソリューションの維持管理
教育・訓練	セキュリティマネジメント	● 情報セキュリティ教育の実施、改善
法務		● コンプライアンス管理
監査		● リスクアセスメント
設計開発	脆弱性管理/診断	● 自社製品・サービスの脆弱性対応
	開発/開発支援	● セキュリティ要件定義、基本設計、設計開発者支援 ● セキュリティ機能構築、維持管理、ガイドライン整備

『CSIRT人材の育成』Ver1.0で示されている「インシデント対応」を担う人材の育成ステップ

基礎教育の修了者
基礎教育を終え、役割別の共通教育も終えたインシデント対応の新規配属者が、さらに学習や経験を通じてインシデント対応の役割、業務内容を把握する。共通教育で行った、一般的なセキュリティ事象、攻撃手法などの詳細の理解、自社システムに関するネットワーク構成、サーバー構成などの構成の深い知識、自社の構成に関するセキュリティ的な防御機器、役割を具体的な作業をイメージして深く理解する。

ステップアップ

担当役割の初心者
データの流れを整理することにより、より深い知識を身に着け、インシデント対応のOJTを通じて経験を積む。上位職が支援すればインシデント対応戦略に基づいた対応タスクの作成や対応ができるようになる。

ステップアップ

担当役割の見習い
実践、訓練を通じて、知識、経験を慣熟させる。一般的な業務に関しては独り立ちし、戦略の策定に基づいたタスクの作成やインシデント対応を該当部門と協力してできるようになる。

（出典）一般社団法人日本コンピュータセキュリティインシデント対応チーム協議会『CSIRT人材の育成』Ver1.0をもとに作成
https://www.nca.gr.jp/activity/training-hr.html

Case 4: NICEフレームワークを介した知識カテゴリの参照

- フレームワークでは米国のNICEフレームワークで定義されているタスク・知識・スキルとの対応関係を整理しており、NICEとの対応関係を有する他のフレームワーク等の相互参照が可能です。
- 以下では、同様にNICEと対応関係にある日本ネットワークセキュリティ協会（JNSA）でのセキュリティ知識分野（SecBoK）人材スキルマップにおける知識・スキルのカテゴリ区分を参照するための例を示します。これは学習教材を作成する際のカテゴリとして活用が可能です。

フレームワークの知識項目抜粋	NICE ID	左記項目に対応するNICEの知識項目（参考訳）	SecBoK 2025 ID	SecBoK 2025のカテゴリ分類		
				分野	大項目	中項目
インシデント対処活動の手順や手法に関する知識	K0677	サイバーセキュリティのポリシーと手順に関する知識	841	15_法・制度・標準	0_総論	–
	K0709	事業継続性と災害復旧（BCDR）のポリシーと手順に関する知識	1096	17_関連領域	1_ICT	11_システム運用
	K0724	インシデントレスポンスの原則と実践に関する知識	467	08_セキュリティ運用	5_インシデント対応	–
	K0725	インシデントレスポンスツールと技術に関する知識	471	08_セキュリティ運用	5_インシデント対応	–
	K0726	インシデントハンドリングツールと技術に関する知識	472	08_セキュリティ運用	5_インシデント対応	–
リスクマネジメントに関する知識	K0675	リスクマネジメントプロセスに関する知識	924	16_ビジネススキル	5_リスクマネジメント	–
	K0721	リスクマネジメントの原則及び実践に関する知識	33	01_IT・セキュリティ基礎	2_セキュリティ基礎	00_総論
	K0734	リスクマネジメントフレームワーク (RMF) 要求事項に関する知識	925	16_ビジネススキル	5_リスクマネジメント	–
	K0735	リスクマネジメントモデル及びフレームワークに関する知識	926	16_ビジネススキル	5_リスクマネジメント	–
	K0835	リスクアセスメントの原則及び実践に関する知識	162	04_セキュリティマネジメント	7_リスク管理	–
	K0920	リスクマネジメントのポリシー及び手順に関する知識	360	07_セキュア設計構築	2_セキュリティ要件定義	–
	K1031	リスク軽減のツール及び手法に関する知識	164	04_セキュリティマネジメント	7_リスク管理	–
	K1076	リスクスコアリングの原則及び実践に関する知識	932	16_ビジネススキル	5_リスクマネジメント	–
	K1078	リスクアセスメントのツール及び手法に関する知識	163	04_セキュリティマネジメント	7_リスク管理	–
	K1208	リスク受容と文書化に関する知識	923	16_ビジネススキル	5_リスクマネジメント	–

本フレームワーク本体で知識の一覧として記載されているもの

NICE IDをキーとしてSecBoK2025から抽出

学習教材

1. 基礎分野
   - 1.1 ICT基礎
   - 1.2 セキュリティ基礎
   - 1.2 法・制度・標準
   - 1.1 ビジネススキル
2. セキュリティ分野
   - 2.1 セキュリティマネジメント
   - 2.2 セキュア設計構築
   - 2.3 セキュリティ運用

SecBoKのカテゴリをもとに
学習教材の体系を整理可能

（出典）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）
セキュリティ知識分野（SecBoK）人材スキルマップ2025をもとに作成
https://www.jnsa.org/result/skillmap/


セキュリティガバナンス/
セキュリティマネジメントの観点
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
②他のガイドライン等との連携による活用
Guide line
Frame work
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
セキュリティ人材確保・評価の観点
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
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

職務記述書の作成

セキュリティ人材の求人における前提条件の理解

ポイント　求人におけるサイバーセキュリティ分野の特徴を把握します

- 本項ではサイバーセキュリティ分野の求人を行う際に用いる職務記述書の作成にあたり、フレームワークをどのように活用するのがよいかについて説明します。
- それに先立ち、サイバーセキュリティ分野の特徴や人材市場の動向を踏まえ、求人に際して留意すべきポイントとして、次の3点を示します。

1 即戦力の人材確保は困難のため、求人において求める要件の優先度の検討が必要

現在、サイバーセキュリティ人材の需給バランスが需要側に大きく偏っているため、経験や専門性を有し、即戦力となるような理想的人材の応募を得ることは容易ではありません。求める要件について優先度を整理し、入社後に習得可能な知識・スキルと、入社時点で必ず保有してほしい知識・スキルや経験を区別した上で、優先度の高い要件に絞って作成する必要があります。

2 厳しい秘密保持が求められる業務の経験については詳しく問えない場合がある

厳格な秘密保持が必要な業務では、退職後も一定期間の守秘が義務づけられていることが一般的です。よって応募してきた人材との面接において、具体的な業務経験を説明してもらえないことがあります。職務記述書の作成にあたっては、このような場合を考慮して、業務で用いた知識やスキルなど、説明可能と思われる内容を要件にするなどの工夫が求められます。

なお、このような場合の具体的な対応方法として、P.54～P.57の「応募要件」欄の「保有知識・スキル」の項目において、業務経験そのものではなく、業務で活用した知識やスキルの保有を要件とする方法を示しています。

3 求人側と応募側でのミスマッチが生じやすくなっている

フレームワークは人材をとりまく共通言語としての活用を目指していますが、その背景にはこれまでサイバーセキュリティに関する技術や脅威、制度等における定義や用語がセキュリティ関係者の間でもまちまちであったことがあり、歴史の長い他分野と比較してコミュニケーション上のミスマッチが生じやすくなっています。採用後に双方で認識の齟齬が生じないように誤解の解消に努める必要があります。

人材採用におけるミスマッチの例

ポイント　職務記述書のどのような内容がミスマッチを生じさせるのかを理解します

- サイバーセキュリティ人材採用における、求人側・応募側のミスマッチ例と対策案を以下に例示します。
- なお、これ以外にも「リモート可とあったのに実質毎日客先往訪」などのミスマッチもありますが、サイバーセキュリティに限った話題でないものは省略しています。

例1

求人側：【職種】セキュリティエンジニア
【仕事内容】
・自社設備のセキュリティ対策実施
・セキュリティインシデント対応
・脆弱性診断　他

応募側：セキュリティのスキルアップをしたくて入社したのに、仕事の大半は非セキュリティのIT保守だった。転職したい・・・

ミスマッチを防ぐための対策案
一般的な企業ではセキュリティ業務しか担当しない人材よりも、何らかの兼務をしている人材のほうが多くなっています。兼務前提であることを隠すよりも、セキュリティのスキルアップのための研修受講支援等でアピールするほうが有効です。

例2

求人側：【休日】年間125日
【勤務時間】平日9:30～18:00
（これ以外の記載なし）

応募側：アラートの度に深夜でも対応が必要。職務記述書の内容は「何事もなければ」の話だった・・・

ミスマッチを防ぐための対策案
サイバーセキュリティ業務の性質上、時間外対応が避けられないものもあるので、その明示は必要です。時間外の緊急対応があっても代休等で労働時間を所定時間内に収める制度があることを示すことで応募側も安心できます。

例3

求人側：【職種】ISMSマネージャー
【応募要件】
・情報セキュリティマネジメントの知識
・セキュリティ担当者の経験

全社のISMSのマネジメントをお願いしたいが、能力的に無理そうだ・・・

応募側：情報セキュリティマネジメント試験に合格しているし、自部署のセキュリティ担当もやっていたし、大丈夫そうだ！

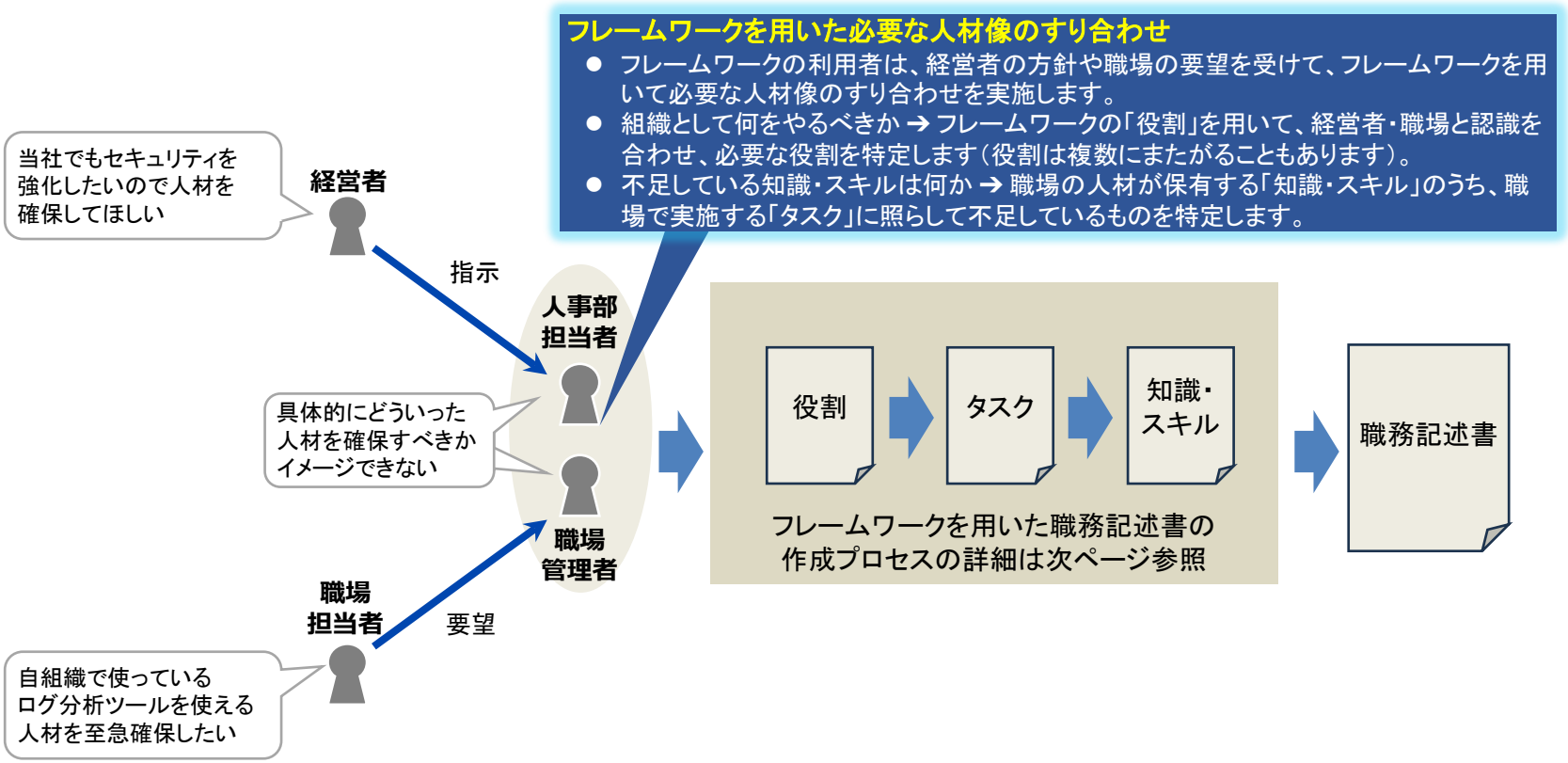
ミスマッチを防ぐための対策案
サイバーセキュリティの業務は多様であり、「セキュリティ担当者」のみでは業務を特定したことにならず、具体化が必要です。また、「情報セキュリティマネジメントの知識」についても、具体的に情報セキュリティマネジメントにおける適合性判断やマネジメントレビュー対応等と示すことで目的に則した求人が可能となります。

これらを踏まえて、次ページ以降で職務記述書の具体的な記載方法を説明します。

職務記述書作成の下準備

ポイント 職務記述書の作成に先立ち、フレームワークを使うのに必要となる情報を集めます

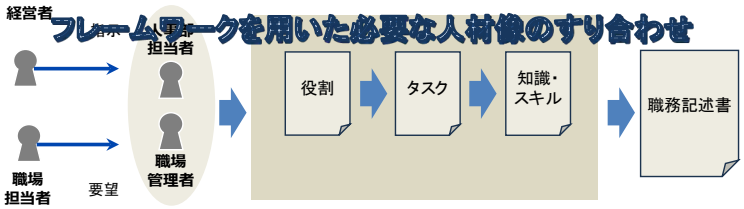
- セキュリティに詳しくない経営者などは、フレームワークで定義している13種類の役割とそれに応じた専門性があることを認識せず、「セキュリティ人材」として一括して求人すればよいと考えていることがあります。
- 一方、現場からは即効性から「特定のツールが使える人材が欲しい」という要望しか出してこない場合もあります。
- これらの要望をそのまま職務記述書に反映しても応募者に適切なメッセージが伝わらず、ミスマッチが生じかねません。サイバーセキュリティ分野の求人を行う場合、どの役割やタスクに関するものかを確認した上で、それが応募者に伝わるような内容とする必要があります。

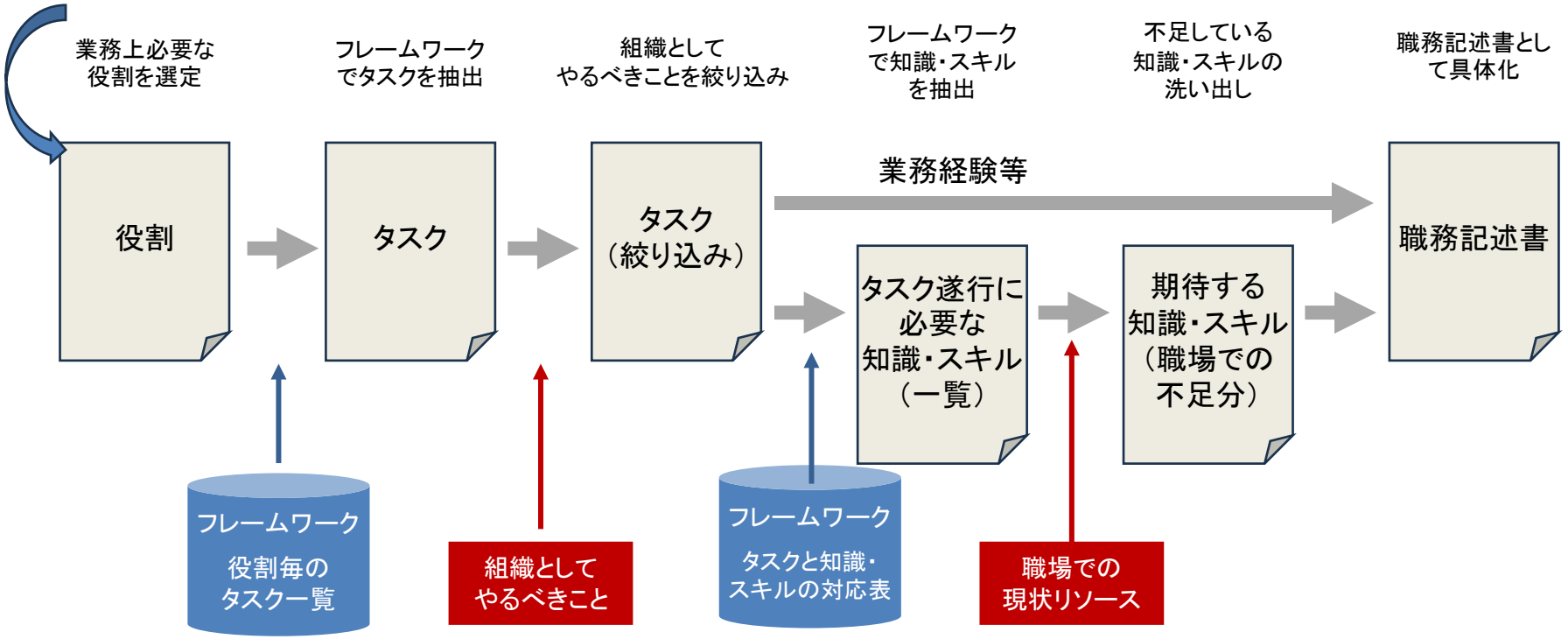


職場の現状をもとに職務記述書に書くべき内容を具体化

ポイント フレームワークを用いて、タスク・知識・スキルの項目を職務記述書に具体化します

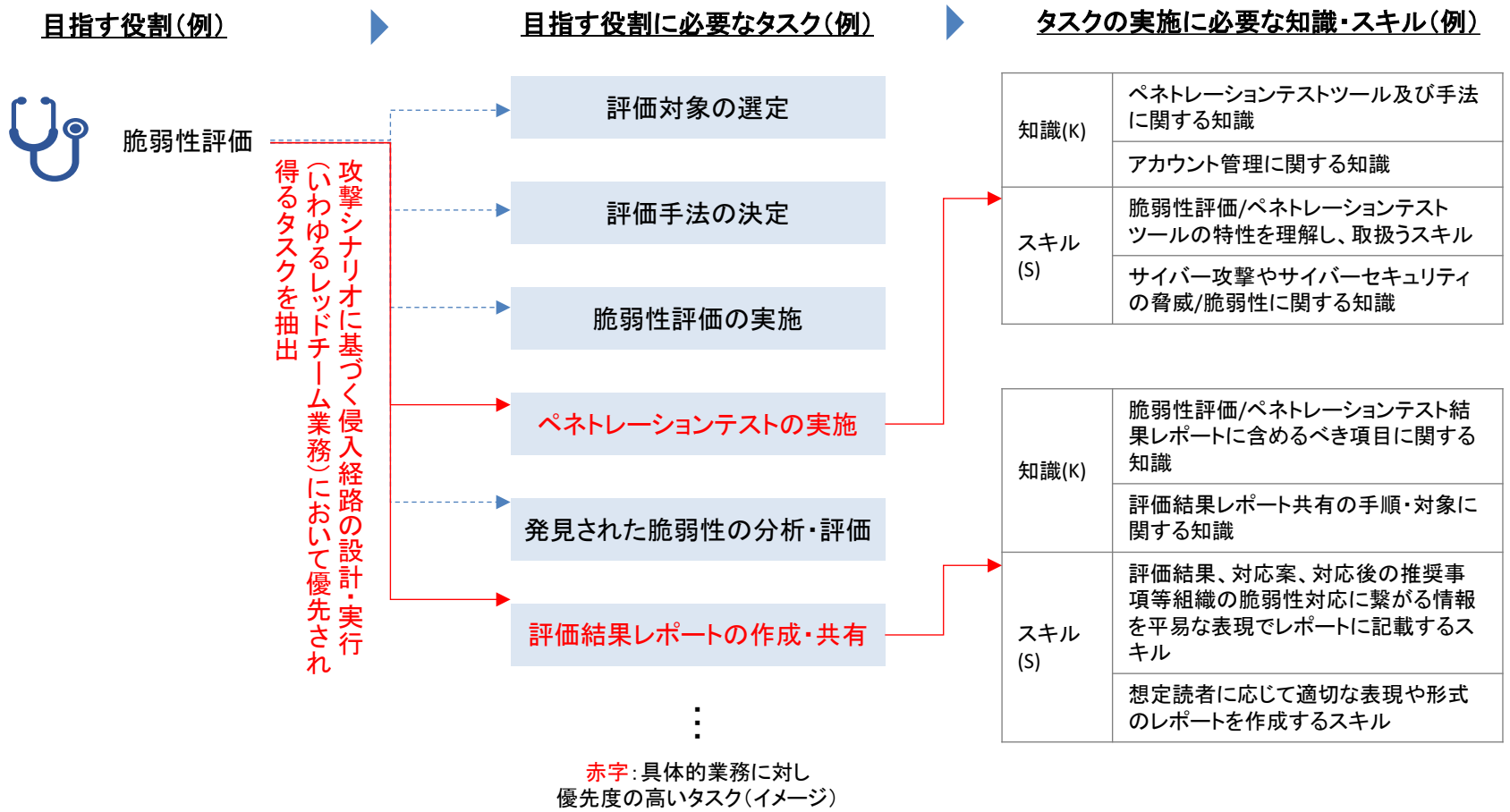
- 職場の現状をもとに、フレームワークを用いて求人したい内容を職務記述書に書くべき内容を具体化するステップを以下に示します。
- 具体的なフレームワークを用いたタスクの絞り込み及び知識・スキルの抽出方法は次ページを参照してください。





【参考】フレームワークを用いたタスク・知識・スキルの絞り込み方法の補足

- 選定した、業務上必要な役割を踏まえて、フレームワークを活用したタスクの特定及び特定されたタスクからの知識・スキルの抽出方法を示します。
- 例えば、脆弱性評価という役割には、「攻撃シナリオに基づく侵入経路の設計・実行（レッドチーム）」「網羅的に脆弱性を確認」といった具体的業務が複数含まれています。
- 具体的業務を遂行する上で優先度の高いタスクを、フレームワークを用い抽出することで、それらのタスクを遂行するために必要な知識・スキルを整理しやすくなります。



赤字：具体的業務に対し
優先度の高いタスク（イメージ）

フレームワークのTKSを活用した職務記述書の作成に向けた考え方

ポイント　職務記述書の作成にあたり、フレームワークの内容が活用可能です

- 本節では、フレームワークが定義するタスク（T）・知識（K）・スキル（S）を活用し、精度の高い職務記述書を作成する方法を説明します。
- 職務記述書を作成する際には、どの役割のTKSを起点にするか、またどのレベルの人材を求めるか（マネジメント系 / エキスパート系）によって、フレームワークの参照方法が異なります。以下では、代表的なパターンを示します。

パターン	求めるレベル	役割の参照方法	適するケース	本書での例示
パターン1	**Lv4-M / Lv3-M** （マネジメント系）	「①意思決定・戦略策定」「②戦略推進・プロジェクト管理」を中心に参照	セキュリティ統括機能のコアメンバーや、ガバナンスを担う人材の確保	作成例案（1）
パターン2	**Lv3-E / Lv4-E** （エキスパート系）	「④対処」「③監視」「⑤情報収集・分析・共有」等の技術系役割を中心に参照	CSIRT・SOC等で高度な技術的判断を独力で行える人材の確保	作成例案（2）
パターン3	**Lv2 → Lv3-E育成前提** （ポテンシャル採用）	「⑥脆弱性評価」「⑧運用管理」等から入社時点の必須K・Sを絞り込み、将来担ってほしいTを明示	即戦力の確保が困難な場合に、育成前提でポテンシャルのある人材を確保	作成例案（3）
パターン4	**Lv3-M / Lv3-E** **（複数役割兼務）**	複数の役割のTKSを横断的に統合	人員が限られ、一人で複数役割を兼務する必要がある場合	作成例案（4）

作成例案（1）：ガバナンス・戦略企画を担う人材

- 大規模組織におけるセキュリティ統括機能（専門組織や委員会等）のコアメンバーとして、経営層に近い視点でセキュリティ戦略を推進する人材の求人例です。
- フレームワークにおける役割「①意思決定・戦略策定」「②戦略推進・プロジェクト管理」を担うことを想定しています。

STEP 1 役割とレベルからタスクの選定

項目	内容
参照する役割	①意思決定・戦略策定 / ②戦略推進・プロジェクト管理
求めるレベル	**Lv3-M**（チームのマネジメントを通じて業務を遂行）以上
レベル設定の理由	CISOを補佐し、組織全体の実態を把握してセキュリティ戦略を立案・推進できる人材が必要

フレームワークの役割「①意思決定・戦略策定」「②戦略推進・プロジェクト管理」から、担当してほしい業務に対応するタスクを選定します。

タスク

- サイバーセキュリティに関する戦略、方針、規定等を策定又は承認する
- サイバーセキュリティに関する監査とその結果に基づく見直しを実施する
- サイバーセキュリティ対策に必要な予算や人員等のリソースを確保する
- 外部委託やサプライチェーンにおけるサイバーセキュリティ対策を統括する
- サイバーセキュリティに関する意思決定・戦略策定に必要な情報を把握する
- サイバーセキュリティ戦略に沿ったプロジェクトの立案

STEP 2 タスクに紐づくK・Sの抽出

選定したタスクの遂行に必要な知識・スキルをフレームワークから抽出し、Lv3-M以上で求められる行動特性を踏まえて応募要件を設定します。

知識 スキル

抽出した知識・スキル	Lv3-Mで期待される行動特性
サイバーセキュリティに係る業界の指標や法律等の規制要件に関する知識	規制動向をもとに組織への影響を評価し、ポリシー改定を主導可能
経営・組織運営、自組織の戦略に関する知識	組織全体を俯瞰し、独力で戦略立案と予算確保が完遂できる
リスクマネジメントに関する知識	最新の脅威動向や事業リスクを分析し、実効性のある戦略を立案できる
組織のサイバーセキュリティに係る方針や目標を策定し、組織設計を行うスキル	関連部署との利害調整を主導できる
関係者と適切なコミュニケーションを行うスキル	経営層や他部門と円滑に調整・折衝できる
組織目標と体制を評価するスキル	収集された情報をもとに、目標と体制の妥当性を評価できる

STEP 3 職務記述書への具体化

具体化したTKSを職務記述書に落とし込みます

項目	記載内容
職種	サイバーセキュリティ戦略・企画担当（セキュリティ統括部門）
FWにおいて該当する役割	**①意思決定・戦略策定、②戦略推進・プロジェクト管理（Lv3-M）**
仕事内容	• グループ全体のサイバーセキュリティ戦略・ロードマップの策定および推進 • セキュリティガバナンスの強化（関連規程の策定・見直し、遵守状況のモニタリング） • 経営層へのセキュリティリスク状況の報告およびIT投資提言 • サプライチェーンや外部委託先を含めたセキュリティリスク評価
応募要件（業務経験）	• 事業会社の情報システム部門またはセキュリティ専門組織における、セキュリティ戦略策定や企画・推進業務の経験（目安3年以上） • ITインフラ構築等のプロジェクトにおけるリーダーまたはマネジメント経験
応募要件（保有知識・スキル）	• 情報セキュリティ関連のフレームワーク（NIST CSF、ISMS等）に関する知識 • ITインフラ（ネットワーク、サーバー、クラウド等）全般に関する基本的な知識 • 経営層や他部門、外部ベンダーなど多様なステークホルダーと円滑に調整・折衝を行うコミュニケーションスキル
応募要件（保有資格）	情報処理安全確保支援士、CISSP、CISM、CISA等のセキュリティ関連資格があれば尚可
勤務形態・休暇等	フレックスタイム制、週〇日の在宅勤務可能
待遇・福利厚生等	資格取得支援制度、報奨金制度 外部の専門研修・カンファレンス参加費用の全額補助

作成例案（2）：CSIRT・インシデント対応を担う人材

- 大規模組織において、実際に発生するサイバー攻撃の脅威からシステムを守り、緊急時の際の司令塔となる専門技術人材の求人例です。
- フレームワークにおける役割「③監視」「④対処」「⑤情報収集・分析・共有」を担うことを想定しています。

STEP 1 役割とレベルからタスクの選定

項目	内容
参照する役割	④対処 / ③監視 / ⑤情報収集・分析・共有
求めるレベル	Lv3-E（自らの専門領域の業務を「独力」で遂行）以上
レベル設定の理由	未知の事象にも自律的に状況を判断し、被害範囲を特定・対処できる人材が必要

フレームワークの役割「④対処」「③監視」「⑤情報収集・分析・共有」から、担当してほしい業務に対応するタスクを選定します。

タスク

- インシデントの可能性検知及び初動対応
- インシデント対応に係る関係部署への対応措置の指示
- インシデント対応に係る関係部署への復旧措置の指示
- アラートの監視・調査・分析から不審な兆候を検知し、関係部署へ報告・通報
- 情報の収集 / 情報の分析
- インシデントに対する初期調査の実施
- 発生したインシデントの原因究明調査

STEP 2 タスクに紐づくK・Sの抽出

選定したタスクの遂行に必要な知識・スキルをフレームワークから抽出し、Lv3-E（独力での専門的実務遂行）で求められる行動特性を踏まえて要件を設定します。

知識 スキル

抽出した知識・スキル	Lv3-Eで期待される行動特性
インシデント対処活動の手順や手法に関する知識	マニュアル外の未知の事象に対しても、自律的に状況を判断できる
サイバー攻撃やサイバーセキュリティの脅威/脆弱性に関する知識	新たな脅威情報を自ら分析し、未知の脅威に対する検知ロジックを策定できる
ツール（監視、ログ収集・分析）及びその手法に関する知識	提供された情報に加え、自ら分析してツール設定を最適化できる
自組織内/外のサイバーセキュリティ関係各所にインシデントに対する対処作業及び復旧作業を明確化し、指示を与えるスキル	独力でインシデント対応の全工程を指揮できる
機器障害か、不正なアクセスや悪意のある侵入であるかことを判別するスキル（トリアージ）	未知のアラートに対しても自律的にトリアージ判断を下せる

STEP 3 職務記述書への具体化

具体化したTKSを職務記述書に落とし込みます

項目	記載内容
職種	CSIRTリードエンジニア（サイバーセキュリティインシデント対応）
FWにおいて該当する役割	③監視、④対処、⑤情報収集・分析・共有（Lv3-E）
仕事内容	• 社内CSIRTの中核メンバーとして、セキュリティインシデント発生時の初動対応、影響調査、復旧に向けた対応のリード、SOC等からのエスカレーション対応およびログ分析。セキュリティインシデント対応マニュアル・フローの整備と、定期的な対応訓練（演習）の企画・実施 • 最新の脅威インテリジェンス情報の収集と社内への注意喚起・対策立案
応募要件（業務経験）	• CSIRTやSOCなどでのセキュリティインシデント対応、またはログ監視・分析の実務経験（目安3年以上） • ネットワーク、サーバー（Windows/Linux）、クラウド等のITインフラの設計・構築または運用保守の実務経験
応募要件（保有知識・スキル）	• インシデントハンドリングや各種ログ分析に関する専門的な知識 • 緊急時に冷静に状況を把握し、関係各所へ的確に指示・連携ができる判断力とコミュニケーションスキル
応募要件（保有資格）	• 情報処理安全確保支援士、CISSP、CEHなどの資格保有であれば尚可
勤務形態・休暇等	• 所定労働時間外の緊急インシデント発生時は、輪番制でのエスカレーション・緊急対応が発生する可能性があります（代休取得制度や深夜対応手当等のサポートあり）
待遇・福利厚生等	• 高度なセキュリティ技術研修（SANS等）の受講費補助

作成例案（3）：脆弱性評価エンジニア（育成前提）

- 即戦力の確保が困難な場合に、入社時点ではLv2（指示下での実行）相当の人材を採用し、入社後の育成によりLv3-E（独力での専門的実務遂行）を目指す求人例です。
- フレームワークにおける役割「⑥脆弱性評価」を担うことを想定しています。

STEP 1 役割とレベルからタスクの選定

項目	内容
参照する役割	⑥脆弱性評価
求めるレベル	Lv2（定められた手順に従い、正確に業務を実行できる）だが、将来はLv3-E（自律的に脆弱性を評価し、独力で診断・報告できる）を目指す
レベル設定の理由	脆弱性診断の即戦力人材の市場獲得が困難なため、IT基盤の知識とセキュリティへの関心を持つ人材を育成前提で採用

入社時点で担当するタスクと、育成後に担ってほしいタスクを区分して示すことで、応募者にキャリアパスを伝えます。

タスク

- 脆弱性評価の実施
- 評価結果レポートの作成・共有
- 発見された脆弱性の分析・評価
- ペネトレーションテストの実施
- 評価対象の選定
- 評価手法の決定

STEP 2 タスクに紐づくK・Sの抽出

入社時点で必ず保有してほしいK・Sと、入社後に習得可能なK・Sを区分します。

知識 スキル

抽出した知識・スキル	入社時必須	入社後習得
組織内の関連計画、対象システム、機器の構成要素やセキュリティに関する知識	—	○
脆弱性評価ツール及び手法に関する知識	○（基本操作レベル）	○（高度な活用）
ペネトレーションテストツール及び手法に関する知識	—	○
脆弱性の一般的な評価基準に関する知識	○（CVSSの基本理解）	○（実践的な活用）
脆弱性評価/ペネトレーションテストツールの特性を理解し、取扱うスキル	○（独力での活用）	○（独力での活用）
組織の環境・目的にあった脅威シナリオを元に評価を行い、脆弱性の有無を明らかにするスキル	—	○
特定された脆弱性毎に深刻度、影響の大きさ等を元に重大度をスコアリングし、対応の優先順位を付けるスキル	○	○

STEP 3 職務記述書への具体化

具体化したTKSを職務記述書に落とし込みます

項目	記載内容
職種	セキュリティエンジニア（脆弱性診断）※育成枠
FWにおいて該当する役割	**⑥脆弱性評価** **（採用時はLv2とするが、職務経験等を通じてLv3-Eとなることを期待する）**
仕事内容	〈入社後まず担当する業務〉 • 手順書に基づく自社システム・ネットワークの定期脆弱性スキャンの実施 • 診断結果レポートの作成補助 〈スキル習得後に担当する業務〉 • 脆弱性の分析・優先度付けおよび修正対応の推進 • ペネトレーションテストの計画策定・実施 • 評価対象の選定および評価手法の決定
応募要件（業務経験）	• ITインフラ（ネットワーク、サーバー等）の構築・運用経験（1年以上） ※脆弱性診断の実務経験は不問
応募要件（保有知識・スキル）	〈必須〉 • TCP/IP、DNS、HTTP等のネットワークプロトコルに関する基礎知識 • 脆弱性スキャンツール（Nessus、OpenVAS等）の基本的な操作経験 • CVSS（共通脆弱性評価システム）の基本的な理解 〈歓迎〉 • Webアプリケーションの開発・運用経験 • CTF（Capture The Flag）等のセキュリティ競技への参加経験
応募要件（保有資格）	• 情報処理安全確保支援士、CompTIA Security+等があれば尚可
勤務形態・休暇等	• 診断実施時は夜間・休日作業あり（振替休日制度あり）
待遇・福利厚生等	• 資格取得支援制度（合格報奨金あり） • 入社後1年間のメンター制度あり

作成例案（4）：セキュリティ運用リーダー（監視・運用管理・教育訓練を兼務）

- 人員が限られる組織において、複数の役割を一人の人材が兼務する必要がある場合の求人例です。
- フレームワークにおける役割「③監視」「⑧運用管理」「⑨教育・訓練」を横断的に担うことを想定しています。

STEP 1 役割とレベルからタスクの選定

項目	内容
参照する役割	③監視 / ⑧運用管理 / ⑨教育・訓練
求めるレベル	Lv3-E（監視・運用の技術的業務を独力で遂行）かつ Lv3-M（チームの教育・指導を通じてセキュリティ水準を向上）
レベル設定の理由	技術的な実務遂行と組織内の人材育成の両方を担える人材が必要

3つの役割からタスクを統合し、重複・類似を整理した上で1つの職務として定義します。

タスク

③監視	アラートの監視・調査・分析から不審な兆候を検知し、関係部署へ報告・通報、ログ分析、ツールの選定・設定
⑧運用管理	構成管理及び変更管理、システム及びネットワーク機器のアップデート・バックアップの管理、システム内又はネットワーク機器内で発見された脆弱性の修正、通常時・インシデント又は通信障害発生時の運用ルールの起案
⑨教育・訓練	教育・訓練の実施、教材又は啓発コンテンツの企画・設計・開発、結果の評価分析と改善

STEP 2 タスクに紐づくK・Sの抽出

3つの役割のK・Sを集約し、優先度の高い知識・スキルを抽出します。

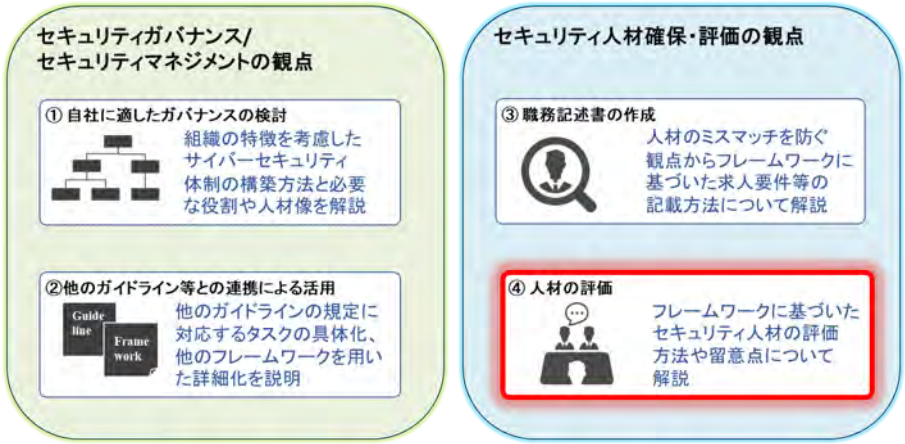
知識 スキル

抽出した知識・スキル	優先度
ツール（監視、ログ収集・分析）及びその手法に関する知識	高
構成管理に関する知識	高
情報システムの脆弱性の修正方法に関する知識	高
指導技術に関する知識	中
教育計画、課程およびカリキュラムの立案および管理に関する知識	中
ツールを使用してシステムやネットワーク、データベース等を監視し、侵入を検出するスキル	高
分析ツールを使用してログ分析を実施するスキル	高
情報システムの脆弱性を修正するスキル	高
関係者と適切なコミュニケーションを行うスキル	高
教材を開発または選定するスキル	中
受講者の学習を指導・ファシリテートするスキル	中

STEP 3 職務記述書への具体化

具体化したTKSを職務記述書に落とし込みます

項目	記載内容
職種	セキュリティ運用リーダー（監視・運用管理・社内教育）
FWにおいて該当する役割	③監視、⑧運用管理、⑨教育・訓練（Lv3-EかつLv3-M）
仕事内容	〈監視・運用業務（約60%）〉 • SIEM等の監視ツールを用いたセキュリティアラートの監視・分析・エスカレーション • セキュリティ運用ルールの策定・見直し 〈スキル習得後に担当する業務〉 • 社内向けセキュリティ教育・啓発コンテンツの企画・開発・実施 • インシデント対応訓練の企画・ファシリテーション • 教育効果の評価・改善
応募要件（業務経験）	• SOCまたは情報システム部門でのセキュリティ監視・運用業務の経験（目安3年以上） • ・サーバー・ネットワーク機器のパッチ管理・構成管理の実務経験
応募要件（保有知識・スキル）	〈必須〉 • SIEM、EDR等のセキュリティ監視ツールの運用・ログ分析スキル • OS・ミドルウェアのパッチ適用、脆弱性修正に関する知識と実施スキル • 技術的な内容を非専門家にもわかりやすく説明できるコミュニケーションスキル 〈歓迎〉 • 社内研修の講師経験、教育コンテンツの企画・開発経験 • Ansible等の構成管理ツールの活用経験
応募要件（保有資格）	• 情報処理安全確保支援士、CompTIA Security+、LPIC等があれば尚可
勤務形態・休暇等	• 監視業務に関して、月〇回程度の夜間・休日のオンコール対応あり（手当支給、代休取得制度あり）
待遇・福利厚生等	• 資格取得支援制度（合格報奨金あり） • 外部セキュリティカンファレンス参加費補助


セキュリティガバナンス/
セキュリティマネジメントの観点
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
②他のガイドライン等との連携による活用
Guide line
Frame work
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
セキュリティ人材確保・評価の観点
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
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

人材の評価

セキュリティ人材の評価における特殊性

ポイント　評価に先立ち、サイバーセキュリティ分野の特殊性を理解します

- 本項ではサイバーセキュリティ対策業務に従事している人材を対象とする評価の考え方について解説します。
- サイバーセキュリティ人材を評価する際、次の4点は他の人材の評価と比較して特徴的であり、十分に考慮する必要があります。

1 「インシデントが起きなかったこと」が成果

営業成績とは異なり、セキュリティは「何事も起きなかった」ことが最大の成果であり、インシデントに備えるために何をしていたかを評価する仕組みが必要です。「セキュリティインシデントが発生せず、対処の機会がなかったため活躍が不十分」といった評価を行うことは不適切です。

一方で、インシデントが起きた場合に自動的に低評価とすることも不適切であり、原因を切り分けて評価する必要があります。

2 最新の技術や脅威に対応できているか

サイバーセキュリティ分野は技術や脅威の動向変化が速く、ある人材が過去に達成した優れた業績が今でも有効とは限りません。

人材の評価項目の選定にあたっては、最新の動向に対応するためにどのような取組を実施し、その成果が得られているかを評価できるようにする必要があります。

3 円滑なコミュニケーションへの努力を評価

サイバーセキュリティ対策の対象が組織における事業活動である以上、セキュリティ人材と経営層、事業関係者等とのコミュニケーションは欠かせません。

「専門知識がなくてもわかりやすいレポート」「経営層の疑問を解消できるように回答」などの取組は、サイバーセキュリティの技術を磨く観点とは異なりますが、セキュリティ人材に求められる重要なスキルが発揮された成果であり、高く評価すべきものです。

4 実績内容が機密扱いであることも考慮

サイバーセキュリティ対策の性質上、評価対象の人材が実際にどのような活動をしたかが重要機密扱いとなる場合があります。重要機密を人事評価資料に記載してしまうとそのデータベース自体も重要機密として保護しなければならなくなります。対象者本人が自己アピールできない結果、評価が不利になるのではモチベーション低下につながるため、そのような不利益が生じない評価の仕組みを検討する必要があります。

評価対象とすべき項目案と重み付けの考え方

ポイント 組織の業務内容や特徴を踏まえて評価項目や重み付けを決定します。

- 前ページの特殊性を考慮しつつ、サイバーセキュリティ人材をどのように評価するかは組織の業務内容や特徴を踏まえて評価の対象とする項目を設定する必要があります。
- また、評価項目や評価における重み付けはセキュリティ人材の担当業務の内容によっても変わってきます。

評価のポイント

Point 1

フレームワークは、組織特有のリスクやシステム環境、業界固有の規制（ガイドライン等）を完全に網羅することは不可能

▶ 標準フレームワークをベースとしつつ、自社のビジネス要件や役割の特性に合わせて独自の評価指標を重ね合わせるアプローチが現実的かつ効果的

Point 2

数千もの膨大なタスクや知識・スキル（TKS）をすべて網羅的にテスト・評価することは、時間的にも労力的にも非現実的

▶ 役割ごとに「事業への直結度」等の観点で重み付けを行い、TKSを現実的な範囲に絞り込むことが重要

Point 3

「その業務を何年経験したか」や「現在の役職」といったキャリアレベルと、実際の能力（真の実務遂行能力）は必ずしも一致しない

▶ 単純な経験年数ではなく、「どれだけ自律的にタスクを遂行できるか」「どれほど複雑な課題に対応できるか」といった具体的な行動特性を基準にすべき

評価項目の設定の例

マネジメント・企画系（組織全体の方向性決定や他部署との調整が主）

分類	評価項目の具体例	評価基準の例
方針・企画の立案 **【重み大】**	事業目標に沿ったサイバーセキュリティ戦略・予算計画を立案し、経営層の承認を得る	**(Lv3)** 組織全体を俯瞰し、独力で戦略立案と予算確保が完遂できる。 **(Lv4)** 最終的な意思決定に責任を持ち、ビジネスリスクを踏まえた判断ができる。
調整・コミュニケーション	セキュリティ施策の導入にあたり、影響を受ける事業部門と折衝し、合意形成を図る	**(Lv2)** 上長のサポートを得て、関係部門と必要な情報共有・調整ができる。 **(Lv3)** 事業部門の業務影響を理解し、自律的に利害調整ができる。
最新動向の適用	法規制（個人情報保護法改正等）や業界ガイドラインの変更を自社のポリシーに反映する	**(Lv2)** 指示に基づき、既存ポリシーの改定作業を実行できる。 **(Lv3)** 規制動向をもとに組織への影響を評価しポリシー改定を主導可能。

技術・実務遂行系（インシデントへの対応や技術的な調査が主）

分類	評価項目の具体例	評価基準の例
実務遂行・初動対応 **【重み大】**	自社の監視ツール（SIEM等）のアラートから不審な兆候を検知し、手順書に従いトリアージを実施する	**(Lv2)** 定められた手順書に沿って、正確にトリアージと初期対応を実施できる。 **(Lv3)** マニュアル外の未知の事象に対しても、自律的に状況を判断し被害範囲を特定できる。
最新脅威・技術への適応	最新の攻撃手法（ランサムウェア等）の情報を収集し、監視ルールや検知シグネチャをアップデートする	**(Lv2)** 提供された情報をもとに、既存のツール設定を変更できる。 **(Lv3)** 新たな脅威情報を自ら分析し、未知の脅威に対する新たな検知ロジックを策定・実装できる。
報告・コミュニケーション	実践的な演習（CTF参加など）を通じたスキルアップ	**(Lv2)** 学習計画に沿って技術を習得し、実務で検証環境を構築できる。 **(Lv3)** 習得した高度な技術をチーム内で共有し、後進の技術指導ができる。

評価におけるレベルの扱い

ポイント　組織内での評価において、フレームワークのレベルを目標設定に活用します。

- フレームワークでは、下表のような4種類のレベルを設定しています。
- サイバーセキュリティの専門分野はフレームワークで13種類の役割に分類されているように多様であり、すべての役割で高いレベルを保有するような人材は存在しません。むしろ、各役割についてレベルを用いて自己評価することを通じて、人材の専門性を表現することができるとも言えます。
- 人材育成におけるレベルの活用については次のページで説明します。

レベルはマネジメント系だけではなく、技術系のキャリアパスも想定しています。

分類・役割	評価対象となるTKSの例示	Lv1 （最低限の知識・補助）	Lv2 （指示下での実行）	Lv3 （独力遂行 / チーム指揮）	Lv4 （高度専門/意思決定）
【技術系】 役割： ⑥脆弱性評価	[Task] 脆弱性評価の実施 [Knowledge] 脆弱性評価ツール及び手法に関する知識 [Skill] 組織の環境・目的にあった脅威シナリオを元に評価を行い、脆弱性の有無を明らかにするスキル	【支援下での補助】 脆弱性評価の基本用語を理解し、上位者の支援や指示のもとで、評価ツールの補助的な操作やスキャン実行を行うことができる。	【手順の遵守】 マニュアルや既存のツール・手順書に従い、対象システムに対する脆弱性スキャンを正確に実行し、結果を報告できる。	**【Lv3-E：独力で遂行】** 自律的にシステムの構成やロジックを分析し、ツールでは検知できない脆弱性を手動診断等で独力で特定・評価できる。	**【Lv4-E：ハイレベル】** 最新の攻撃手法を用いた高度なペネトレーションテスト等を主導し、未知の脆弱性を発見・実証して、組織や業界のセキュリティ向上に貢献する。
【マネジメント系】 役割： ① 意思決定・戦略策定	[Task] セキュリティに関する戦略、方針、規定等を策定又は承認する [Knowledge] リスクマネジメントに関する知識 [Skill] 組織の方針や目標を策定し、組織設計を行うスキル	【基礎理解と補助】 セキュリティ戦略や方針に関する基本的な用語を理解し、先輩や上位者のサポートを受けながら情報収集等の補助を行う。	【定型的な作成】 上位者の指示や既存のテンプレートに基づき、セキュリティ規定等の改定案のドラフトを正確に作成できる。	**【Lv3-M：調整と立案】** 最新の脅威動向や事業リスクを分析し、関連部署との利害調整を主導して、実効性のある戦略やポリシーを立案・展開できる。	**【Lv4-M：意思決定と責任】** 組織全体のリスクとビジネスのバランスを踏まえて、全社的なセキュリティ戦略・ポリシーを最終承認し、その結果に責任を負う。

評価に先立つ目標設定の考え方

- 人材育成の観点から、サイバーセキュリティに関する知識・スキルの向上に関する目標設定を期初に行い、期末にその評価を行う場合のポイントは次のとおりです。
  - ✓ あらかじめ対象者と上長による面談等を通じて、目標設定内容を合意する
  - ✓ 目標とする内容（役割とレベル等）については、組織としての育成方針と本人の指向との整合がとれるものとする
  - ✓ 目標設定時点で、その達成に向けた組織による支援（研修費用負担等）と本人の学習計画等を具体的に検討する

Point

評価基準

年数や役職だけでは不十分

技術や脅威の進化が激しいサイバー領域では経験年数等だけでは実務能力を測れない。

自律性	マニュアルや指示待ちか（Lv2）、独力で完遂できるか（Lv3）
タスクの複雑	定型的な業務か、非定型で複雑な事案に対応できるか
影響力	自己完結か、他者を指導・リードして組織に貢献できるか

Point

技術・マネジメントの複線

技術の専門家が存在

技能を極めた専門家（エキスパート）のキャリアも存在します。

Lv4-M **組織内での適切な実施のための意思決定・マネジメント**	**Lv4-E** **高い専門知識を有し、組織内外への技術的指導や情報発信で貢献**
Lv3-M **チームのマネジメントを通じて業務を遂行**	**Lv3-E** **自らの専門領域の業務を「独力」で遂行**

客観的な目標設定のステップ

ステップ①
ギャップの可視化

フレームワークで定義された役割ごとの「タスク・知識・スキル（TKS）」のリストを用い、「現在の保有スキル」と「目標とする役割・レベル」の差分を洗い出します。

ステップ②
育成方針のすり合わせ

洗い出したギャップをもとに、本人が「マネジメント（M）」と「エキスパート（E）」のどちらのキャリアを目指すかという志向と、組織のニーズを面談ですり合わせます。

ステップ③
学習計画と支援の確約

ギャップを埋めるための具体的なアクション（OJT、CTF等の実践演習、資格取得等）を計画し、組織側は研修費用の負担や業務時間の配分等の「支援」を提供します。

評価項目の例

- 評価項目の例として、「対処」の役割を担う人材を評価する際の評価項目とレベルを示します。

	考え方	留意点
タスク（T）	フレームワークのタスク定義に「自社の対象システム」や「自社のプロセス」を補い、「その業務を実際に経験したか・実績があるか」を問う項目にする。	組織の業務内容に応じて、項目の採否（取捨選択）、修正、追加
知識（K）	フレームワークの知識定義に「自社の対象システム」や「自社のプロセス」を補い、「その業務を実際に経験したか・実績があるか」を問う項目にする。	座学や資格取得による「学習内容の定着度」を測る指標として活用
スキル（S）	フレームワークのスキル定義に「自社の対象システム」や「自社のプロセス」を補い、「その業務を実際に経験したか・実績があるか」を問う項目にする。	スキル単体で評価するのではなく、フレームワークで設定した「レベル定義」と組み合わせて、「どの程度の達成度・自律性で実践できるか」を測る

TKSの区分	フレームワーク本体の定義例	自社向けの評価チェックリストへの変換例（具体的・実務的）
タスク（T）	インシデントに対する初期評価・トリアージ	**【業務実績】** 自社のインシデント対応マニュアル（手順書）に基づき、SOCからのアラートに対する初期評価とトリアージを実施した経験（実績）があるか。
知識（K）	インシデントの評価、トリアージに関する知識	**【学習・説明能力】** 自社のトリアージ基準（影響度・緊急度の定義）と、誤検知（フォールス・ポジティブ）を除外するための基礎的な用語・仕組みを**他者に説明できるか。**
スキル（S）	自組織内/外のサイバーセキュリティ関係各所より収集した初期調査結果をもとに事業の継続を目的に何の対応を優先すべきかを判断するスキル	**【自律性・達成度（レベル判定と結合）】** 収集した調査結果から、ビジネス影響（事業継続）を考慮した対応の優先順位を判断できるか。 ・**Lv2**：上司のサポートやマニュアルの範囲内で判断できる。 ・**Lv3-E**：未知の事象でも、自律的・独力で影響を評価し判断できる。

キャリア形成における評価の活用

- 人材のもつ「強み」や「興味」を活かしたキャリア形成を行い、組織のサイバーセキュリティ対策のコアとなる人材として育成するのに評価を活用することができます。
- 人材本人における成長の実感や高く評価されていると感じることは、人材の離職防止にも有効です。

	組織のコアとなる人材	全役割共通	インシデント対応業務	技術・脅威対応業務
役割	育成にかける時間軸が長く、身につけるべき視野が広い	本人の「強み」や「興味」を活かし、客観的な評価が重要	何も起きなかったこと（インシデント未発生）」が最大の成果。	当初の計画通りに進めることに固執すると、目前の重大なリスクへの対応が遅れる
考慮事項	**育成スパンに応じたアプローチの使い分け**	**目標設定に対する達成状況の評価**	**業務の特殊性を考慮した計画と評価**	**状況変化に伴う柔軟な見直し**
ポイント	【長期育成】現在の役割だけでなく、将来目指す別の役割のTKSを提示し、ギャップを埋める計画を立てる。 【短期促成】網羅性を捨て、直近で必要な「コアとなるTKS」のみに絞り込んで集中的に育成・評価する。	期初にフレームワークの「TKS」と「レベル定義（自律性など）」を用いて目標との差分を客観的に設定し、期末にはそのTKSが目標レベルの行動特性を満たして習得できたかを評価する。	インシデントが発生しなかった場合、「対処」等の実践タスク(T)の評価項目を、「未然に防ぐための備え（脅威情報の収集や演習の企画等）」のタスク(T)に読み替えて評価できるよう、評価シートをカスタマイズする。	期中に新たな脅威が発生した場合、当初設定したタスク(T)の完遂にこだわらず、フレームワークから新たな脅威対応に必要な知識(K)やスキル(S)を抽出し、目標を柔軟に再設定・評価する。

フレームワークの項目をチェックリストとして活用する場合の考え方

- フレームワークが定義する役割毎の知識・スキル項目をキャリア評価におけるチェックリストとして活用する場合の考え方を説明します。

なぜフレームワークをカスタマイズしてチェックリスト化するのか

組織の実態への適合

フレームワークの定義は汎用的であり、自組織固有のビジネス要件やシステム環境を完全には網羅できない

評価の現実性と効率化

フレームワークに定義された膨大な項目をすべて網羅的に評価しようとすることは、時間的にも労力的にも非現実的である

客観性と納得感の向上

抽象的な表現のままでは評価者の主観が混じるため、客観的に自己評価・他者評価が可能な状態にする必要があるため。

どの知識・スキルが自組織に必要なのか

各役割のTKSを確認

各役割に対して定義されている「タスク(T)」「知識(K)」「スキル(S)」の項目をまず確認

「コア項目」を絞り込み

すべてのTKSを対象とするのではなく、自組織の要件や最新の脅威動向に照らし合わせて、優先的に取り組むべき「コアとなる重要なタスク・知識・スキル」に現実的な範囲で絞り込んだ項目群を抽出

どのようにチェックリスト化し、評価に活用するのか

STEP1

自社の業務に応じた項目のカスタマイズ

フレームワークの項目をそのまま流用するのではなく、組織の業務内容や対象システムに応じて、項目の採否、修正、追加を行う。

STEP2

項目の「自己評価可能な状態」への具体化

「○○に関する知識(リスクマネジメント等)」等の項目を、「自社の業務プロセスに沿って流れを説明できるか」等、達成状況を自己評価できる行動指標に変換

STEP3

「レベル定義」との組み合わせによる評価

スキル(S)単体で「できる／できない」を評価するのではなく、フレームワークの「レベル定義」と組み合わせて、達成度(自律性と複雑さ等)で評価する。

評価における資格制度の活用

- セキュリティ人材の評価にサイバーセキュリティ関連資格の取得や更新を活用する場合のポイントを示します。
- 多くの企業において、スキルアップの手段として資格取得者への報奨金の支払い等のインセンティブが提供されています。ただし、資格取得が目的となってしまうことのないよう、人材のヒューマンリソースマネジメントの観点から、資格取得を通じてどのような知識・スキルが習得されたかを管理できるようにすることを検討すべきです。
- 資格・検定制度の活用については、個人（専門人材）向けの手引き書もご参照ください。

資格取得の考え方

現在地の把握（レベルとTKSの判定）	フレームワークのレベル定義（Lv1～Lv4）と、自己の業務に関連するTKS保有状況をチェックし、現在のレベルを客観的に把握する。
不足しているTKSの抽出	目標とする役割や上位レベルに進むために「何が足りないか（知識・スキル）」を特定する。
資格の選定と学習の実施	不足しているTKSを体系的に学ぶため、各資格試験のシラバスとフレームワークの知識(K)・スキル(S)を紐づけ、学習計画の目標（マイルストーン）に設定する。
評価への組み込み	資格取得をもって「対応する知識(K)を習得済み」として客観的に評価する（最新の動向への追従を確認するため、合格時期や有効期限も合わせて管理）。

組織でセキュリティを担う人材の具体例

例
管理部門のセキュリティ兼務担当

例
セキュリティ対策の実務を担当

例
セキュリティガバナンスの統括担当

人材タイプ・役割	現在のレベルと状況	資格の例	証明される能力
② バックオフィス担当（プラス・セキュリティ人材） ※役割：⑩法務、⑪監査	**【Lv1未満～Lv1】** ITの専門家ではないが、SaaSの調達や委託先管理、個人情報保護の業務を担う。	**ITパスポート試験（IP）** **情報セキュリティマネジメント試験（SG）**	**【Lv1～Lv2の確実な習得】** • コンプライアンスおよびプライバシーの原則と実践に関する知識 • 外部委託先管理等の業務現場におけるリスクアセスメントの知識
③ セキュリティ専任者（専門人材） ※役割：④対処、⑥脆弱性評価	**【Lv2：指示下での実行】** 未知の脅威の分析や、自律的な原因究明が独力で完遂することが課題。	**情報処理安全確保支援士（RISS）** **CISSP（認定情報システムセキュリティプロフェッショナル）**	**【Lv3-E（エキスパート）への到達】** • 情報システムの脆弱性を自律的に評価する知識・スキル • インシデントの初期評価から復旧指示までを独力で遂行する能力
④ マネジメント層（専門・統括人材） ※役割：①意思決定・戦略策定	**【Lv3-M：チーム指揮】** 現場の指揮はできるが、経営層とビジネスリスク（事業継続）の観点で対話し、全社的なガバナンスを効かせる知見が不足。	**情報処理安全確保支援士（RISS）** **CISSP（認定情報システムセキュリティプロフェッショナル）**	**【Lv4-M（意思決定・責任）の証明】** • 組織全体のセキュリティガバナンスとリスク管理の知識 • 情報セキュリティプログラムの策定と予算・リソース配分の能力

おわりに／参考情報

- 本手引き書と併せて活用できる関連資料をご紹介します。
- フレームワーク本体や関連機関のガイドライン等のリンク集として、自組織のセキュリティガバナンス体制や人材確保の検討にご活用ください。

- 経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0 及び サイバーセキュリティ経営ガイドライン付録F サイバーセキュリティ体制構築・人材確保の手引き」
  （https://www.meti.go.jp/policy/netsecurity/mng_guide.html）
  - 本手引き書では、大規模組織におけるセキュリティガバナンスの検討の出発点として、同ガイドラインが規定する「経営者がCISO等への指示を通じて確実に実施させるべき重要10項目」を参照しています（P.14～15等）。また、付録Fで推奨される「セキュリティ統括機能」の設置について、その組織形態と機能分担の4類型（専門組織型／委員会型×集権型／連邦型）に基づく体制検討の方法を解説しており、フレームワークの役割定義を用いて各類型に必要な人材像を具体化しています（P.16～39等）。
- 経済産業省「サプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針（案）」
  （https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/20251226_report.html）
  - 本手引き書のCase1（P.43）では、同制度の要求事項をもとに、フレームワークが規定するタスクの内容をブレイクダウンして各担当に割り当てる方法を解説しています。フレームワークを活用しながら同制度への対応を進める際の具体的な手順をお示ししていますので、サプライチェーン対策の検討にご活用ください。
- 一般社団法人日本情報システム・ユーザー協会（JUAS）:「平成30年度サイバーセキュリティ経済基盤構築事業（企業におけるサイバーセキュリティ体制の構築及び戦略マネジメント層の育成に関する実態調査）」（2019年3月）（現在は国立国会図書館デジタルコレクションにて閲覧可能）
  （https://dl.ndl.go.jp/pid/14460066）
  - 本手引き書で解説しているセキュリティ統括機能の4類型（専門組織型／委員会型×集権型／連邦型）は、本調査における大規模組織を対象とした実態調査の結果に基づき整理されたものです（P.17等）。自組織に適したガバナンス体制を検討する際の背景情報としてご参照ください。