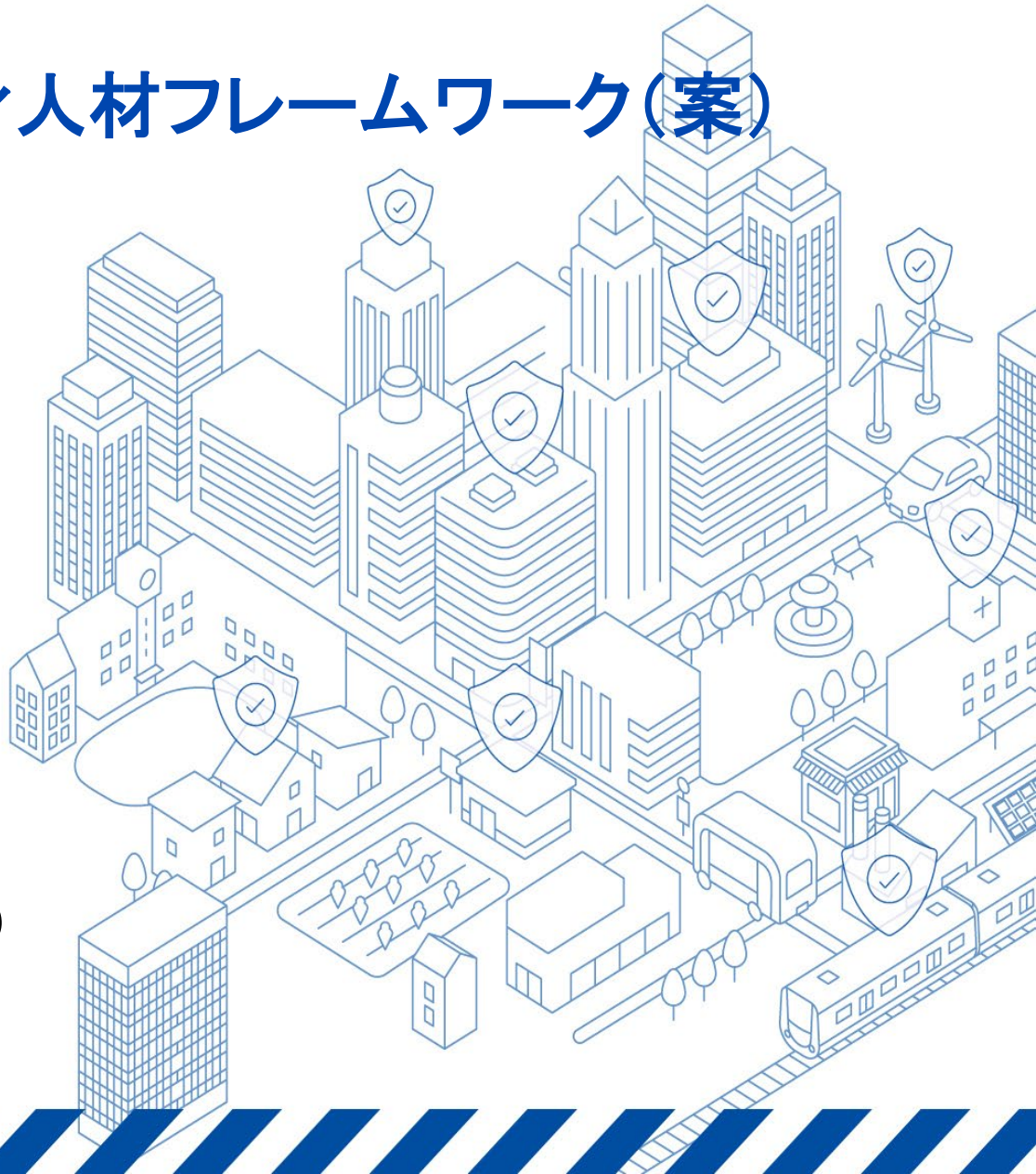
サイバーセキュリティ人材フレームワーク（案）について



令和８年２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。
- 策定にあたっては、令和7年10月に有識者検討会を立ち上げ、議論を進めているところ。
（検討会資料は以下のページから御覧いただけます。https://www.cyber.go.jp/council/csjinzai/index.html）

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

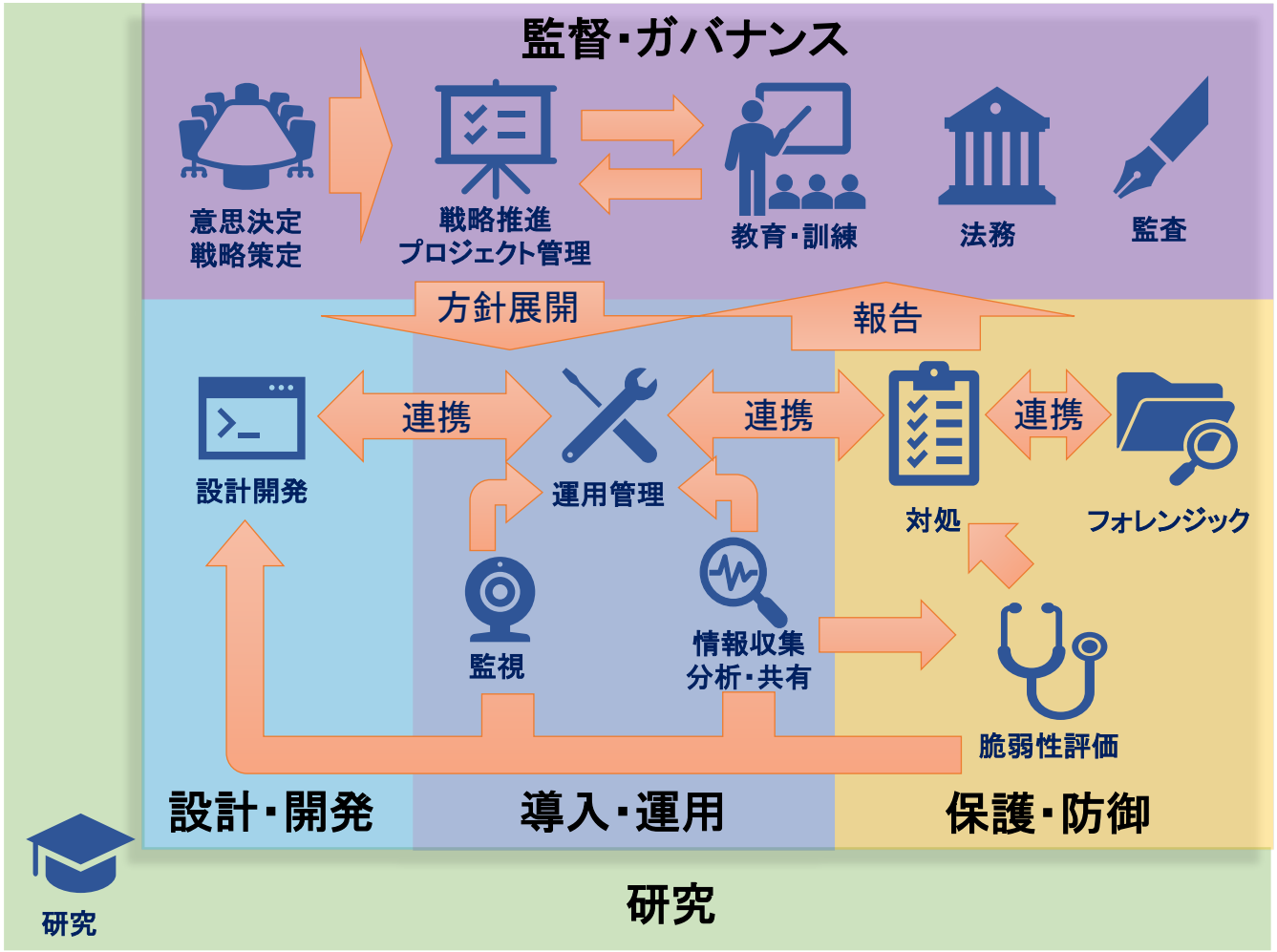
人材フレームワークの位置づけと前提等

位置づけ	**必須事項ではなく、「指針」の位置づけ**	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。
対象範囲	**産官学等幅広い主体による活用を想定**	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。
活用方針	**利用者の実態に応じて柔軟に活用**	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。
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**	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
見直し	**不断の見直しを前提とする**	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



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)

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

手引き書（案）の構成イメージ

手引き書は、利用主体に共通する事項と、主体ごとの固有事項を分けて構成する。

共通事項	
● サイバーセキュリティ人材フレームワークの概要 策定背景及び定義する「役割」の全体像等について ● サイバーセキュリティ人材フレームワーク本体の構成 ● 手引き書の概要 位置づけや手引き書で具体化する「人材像」の概念について　等	
利用主体別固有事項	
① 小規模組織 例：中小企業、小規模自治体 等	● 小規模組織におけるセキュリティ対策の考え方（役割に基づく体制の一例等） ● モデルケースに基づく活用例　等
② 大規模組織 例：中堅・大企業、政府機関 等	● 担当者を採用するときの職務記述書の作成方法 ● レベルを踏まえた人事評価等にあたっての活用方法　等
③ 教育機関 例：大学、教育事業者 等	● 輩出したい人材像を定めて、知識・スキルを段階的に習得するためのカリキュラムの作り方（作成にあたっての考え方）　等
④−1 個人（専門人材） 例：専門人材、専門人材を目指す学生等	● 専門人材に求められるスキルセットを踏まえたセルフアセスメントの実施方法 ● スキルギャップを埋めるための学習方法　等
④−2 個人（プラス・セキュリティ人材）	● 各役割の概要 ● プラス・セキュリティ人材に求められるスキルセットを踏まえたセルフアセスメントの実施方法 ● スキルギャップを埋めるための学習方法　等

① 小規模組織向け手引き書の作成方針案（骨子案）

方針概要

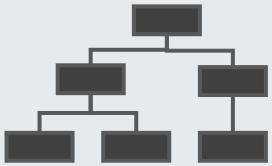
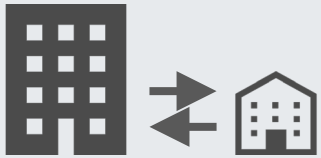
- セキュリティの専門人材を十分に確保することが困難である状況を前提に、必要な体制を可視化した上で、役割分担等を検討し、「人材像」として具体化。
- イメージとして分かりやすく示すため、次の3つのモデルケースにおける活用例を記載。うち【ケース1】を主として説明しつつ、他のケースで異なる対応が必要な場合を示す。

	【ケース１】	【ケース２】	【ケース３】
サイバーセキュリティ対策における悩み	 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」をあまり意識できていなかった。	 取引先から経済産業省の「セキュリティ対策評価制度」への対応を要求されているが、どうすればよいかわからない。	 サイバーセキュリティ対策は代表者が実質一人ですべて対応しているが、やるべきこと（タスク）が何かを把握したい。
想定する企業属性	● 従業員8名 ● 小売業（ネット販売） ● PCは使いこなせるが、セキュリティはよくわからないという従業員が大半。	● 従業員30名 ● 製造業（部品製造） ● 「工場の設備なら慣れているが、PCは苦手」という従業員が多い。 ● 工場はネットに接続していない。	● 従業員2名（代表＋アシスタント） ● サービス業（デザイナー）

② 大規模組織向け手引き書の作成方針案（骨子案）

方針概要

- セキュリティ体制がある程度構築されていることを前提に、より効果的・効率的に人材育成・確保（採用）を行うための活用例を示す。
- レベルに応じた評価に関する内容は大規模組織向けのみで詳細を記載するため、必要に応じ、他の利用主体が参照できるよう、汎用性のあるものとして記載。

自社に適したガバナンスの検討	サプライチェーン委託先管理	職務記述書の作成	人材の評価
			
自社の特徴に相応しいセキュリティガバナンスの体制の考え方例示ともに示す。	委託先において必要最低限のセキュリティ対策を行うために、求められるタスクや教育方法などのノウハウを示す。	人材募集において、ミスマッチを防ぐ観点で、応募者が興味をもつような職務記述書の考え方について示す。	レベルを踏まえた人材の評価にあたって留意すべき内容を示す。

③ 教育機関向け手引き書の作成方針案（骨子案）

方針概要

既存のカリキュラム指標などを基礎としながら、現在実務で活躍しているセキュリティ人材へのアンケートなどを通じて社会ニーズ等を踏まえた教育関係者によるカリキュラム・シラバス等の検討に資する次のような考え方を示す。

- 教育機関が企業と人材フレームワークを共通言語として対話等することで、社会の人材ニーズを把握する考え方を示す。
- 上記の可視化を踏まえて、教育機関等においてはどういった人材を育成していくべきか、また、それらを実現するためにどういった教育カリキュラムの設計が必要となるかという点について、考え方を示す。
- 教育カリキュラム等の設計において、自組織での教育リソースを踏まえて、不足するより専門的な要素を補うための一つの事例として、外部講師の招聘なども含めたより実践的なカリキュラム設計に関する工夫の一例を示す。

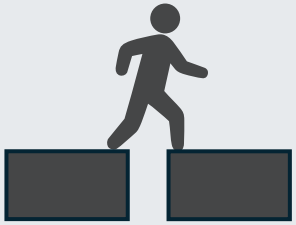
	セキュリティ人材に関する社会のニーズ	カリキュラムを作るための考え方	学ぶべき内容を充足するための工夫例
項目	 セキュリティ人材のニーズの種類や傾向	 サイバーセキュリティに関するカリキュラムを設計する際の考え方や参考情報	 自組織のリソースを踏まえた、より専門的なカリキュラム構築のための工夫
具体的内容	● 教育機関が企業と人材フレームワークを共通言語として対話等することで、社会の人材ニーズを把握する考え方	● 既存のカリキュラム指針等や、左記社会ニーズを踏まえた、カリキュラム設計に関する考え方	● 不足している専門領域に対する外部講師の活用や選定の考え方 ● 他大学や企業、地域コミュニティ等との連携による教育リソースの補完の案

④-1 個人（専門人材）向け手引き書の作成方針案（骨子案）

方針概要

今後サイバーセキュリティの専門人材として活躍したい人材への参考情報として、次のような内容を示す。

- セルフアセスメントを踏まえて、明らかとなるスキルギャップについて、現場で実践されている学習方法や経験の積み方（OJT、競技会等）による解消方法の事例を示す。
- 専門人材の実経験に基づき、職種や学びのつながりを示すキャリアパス事例を参考情報として示す。

	セルフアセスメントの方法	スキルアップとキャリア形成のアプローチ	専門人材の例（本手引書の対象）
項目	 目指す役割に応じて、自身の現状を客観的に評価する観点を整理する	 不足している能力を補うための具体的なアクションプラン	 専門人材のモデルケース
具体的内容	● フレームワークを用いて自身の役割を把握する方法 ● ツールを活用した自己採点の例	● モデルとなる専門人材が実践してきた学習方法や経験の積み方の一例（OJT、競技会等）	● 高度技術者、マネジメント層、研究者等の多様なキャリアの事例

④-2 個人（プラス・セキュリティ）向け手引き書の作成方針案（骨子案）

方針概要

本来業務にプラスして、習得することが望ましい知識・スキルについて、既存のツール等を活用して確認・習得する方法を提示する。

- 自身の業務において付加的に求められるタスクとスキルを例示する。
- 小規模・大規模組織向け手引き書が企業（組織）目線であったのに対し、本手引き書はプラス・セキュリティ人材に焦点を当て、個人の主体的な取組を促す「人」目線でまとめる。

	業務に付加すべきセキュリティ知識・スキル	セルフアセスメントと学習方法
項目	 プラスセキュリティ人材の職務イメージ	 自身の現状評価の方法と学習プランの立て方
具体的内容	● 本来業務（総務、営業、経理等）を遂行する上で、プラスして求められるセキュリティ知識・スキルの例	● アセスメントで不足と評価した項目の学習方法 ● 各種既存資格の活用例

詳細は【別紙】サイバーセキュリティ人材フレームワーク（本体案）参照