資料2

人材フレームワーク及び手引き書の取りまとめ（案）について

国家サイバー統括室
National Cybersecurity Office

令和８年３月２７日

内閣官房
国家サイバー統括室
人材政策班

サイバーセキュリティ人材フレームワークの策定趣旨・位置づけ

策定趣旨

- サイバー脅威の高度化・複雑化が進む中、組織の規模や業種に関わらず、必要な人材を確保・育成することが重要
- 一方、各組織において必要な役割や技能を整理し育成等役立てられる共通的な指針が十分に整備されていない現状
- このため、必要な役割や技能を体系的に整理した「サイバーセキュリティ人材フレームワーク」を策定し、より効果的・効率的に人材確保・育成を推進するための環境整備を図る。

位置づけ・性質

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。

期待される効果

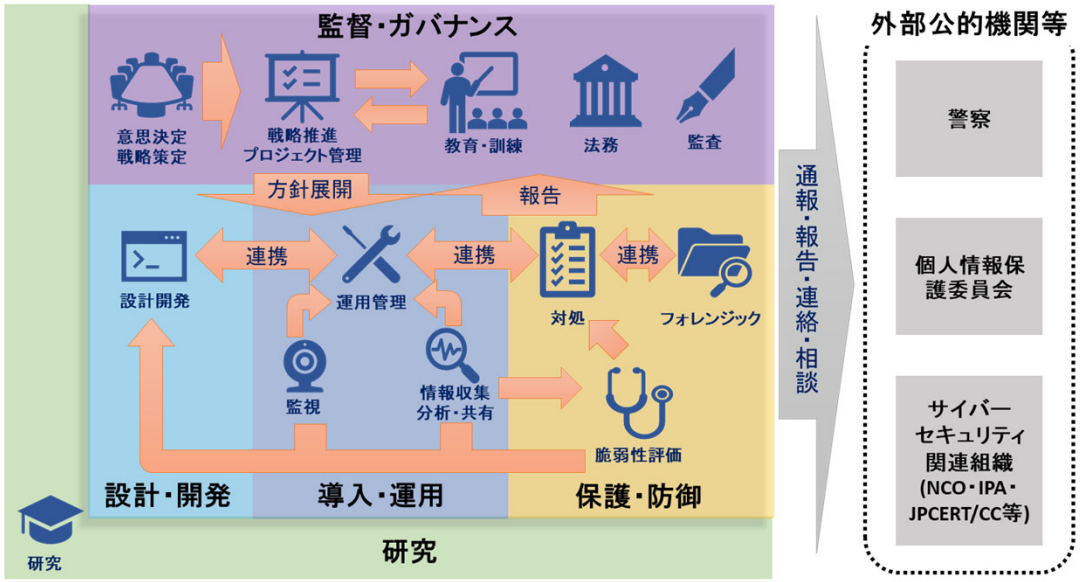
体制整備	必要なセキュリティ機能・役割の整理による組織内の体制整備の明確化等
採用・配置・評価	採用要件の具体化によるミスマッチの解消やスキルレベルに基づく適切な人材配置・評価の実施等
教育・訓練	産学で共有可能な共通言語の提供による社会的ニーズを踏まえた教育内容の充実
キャリア形成	目指すキャリアと現状のギャップの把握による必要な知識・スキルの効果的な習得

人材フレームワークの基本構造

13の役割 × タスク　知識　スキル / レベル

13の役割に基づき、タスク(T)、知識(K)、スキル(S)を汎用的に整理するとともに、4段階のレベルを設定

役割　全体像



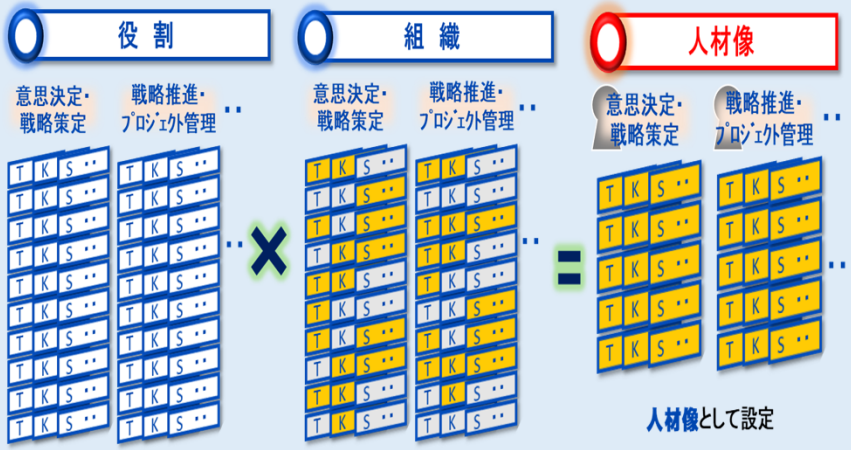
レベル　概要

- タスクの難易度や求められる知識・スキルに応じた4段階のレベルをITSSとの整合性を図りながら設定
- 上位レベル(3以上)では、高度専門性を担うエキスパートと、組織等を統括するマネジメントを区分

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の遂行を通じて、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	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す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）

役割と人材像の関係性

- フレームワーク本体において、サイバーセキュリティ人材が担う13の「役割」を示したうえで、役割毎に汎用的なタスク(T)、知識(K)、スキル(S)を定義
- 各組織において役割を実施する人材の定義を具体化したものを「人材像」とし、その具体化手順について手引き書にて提示



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、専門個人・プラスセキュリティ人材）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）向け

- □ 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、以下の対応表を
参考にご活用いただくことも想定する。

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)	△	◎	△	◎	○	―	○

1.小規模組織向け手引き書の全体構成

- 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

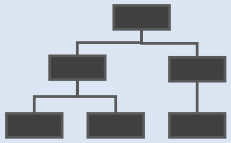
2.大規模組織向け手引き書の全体構成

- 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。

Guidelines
Framework

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

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

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。

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

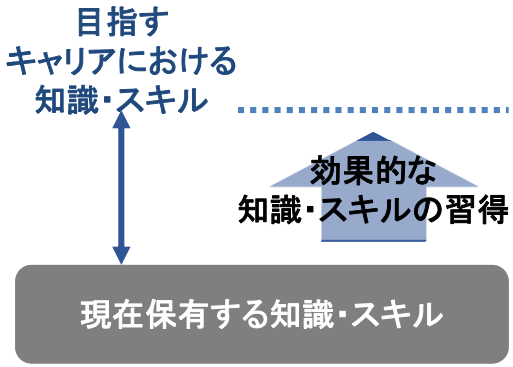
フレームワークを用いたキャリアの可視化と学習の指針策定

セルフアセスメント
（フレームワークに準拠）

役割・タスクを選択すると、関連する知識・スキルが表示

【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

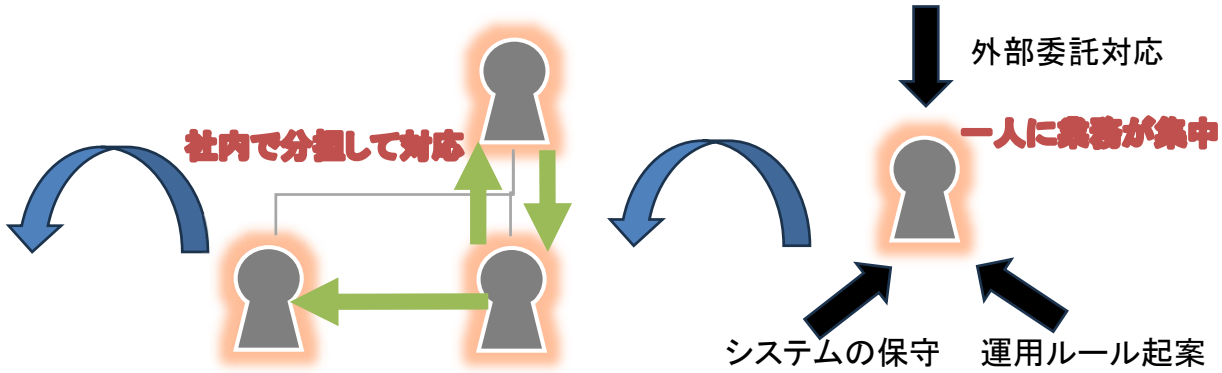
4-2個人（プラス・セキュリティ）向け手引き書の全体構成

- バックオフィス(経理・総務・人事等)やIT開発・運用等のサイバーセキュリティの専門業務ではない個人が、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

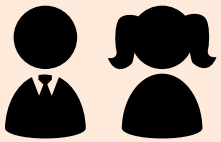
【自身の業務とタスク（T）の紐づけ】

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。