サイバーセキュリティ人材フレームワーク（案）に関するパブリックコメントの結果一覧

意見のうち、パブリックコメントの対象となる案件についての意見のみ、意見の概要とこれに対する考え方を掲載しています。
取りまとめ都合上、お寄せいただいた意見は適宜要約しています。

No.	御意見要約	回答案
1	本案には賛同するが、日本のサイバー分野は内閣官房、総務省、経済産業省、情報処理推進機構、警察等に所管が分散しており、職務定義や評価基準が接続されていないため、フレームワークを単なる分類表にとどめず、各府省庁の採用・育成・評価・調達要件を必ずマッピングするなど、分散した運用を束ねる統合的な仕組みとして位置づけるべきだ。	本フレームワーク（案）は、人材の役割や技能を整理し、官民における人材確保・育成場面での共通的な指針として位置づけるものであり、関係省庁における取組との相互参照関係を見据え、引き続き連携を進めてまいります。
2	ITSSやSecBoK、NICE等の既存枠組みがある中で、なぜ新たにフレームワークを策定するのか意義が不明確。特に人材分野で実績のある情報処理推進機構ではなく内閣官房国家サイバー統括室が主導する理由を明確に示すべきで、新規創設よりも既存フレームワークの横断整理と統合に注力すべきだ。	本フレームワーク（案）は、ITSSやSecBoK、NICE等を踏まえ、これらと相互参照を図りながら、我が国の実態を踏まえたサイバーセキュリティ人材の役割や技能を汎用的に定義するものです。 国家サイバー統括室がその取りまとめを担うのは、特定分野に偏らず、関係省庁間を横断して総合調整を図るためであり、御指摘の既存のフレームワークとの関係整理や横ぐし確保は重要な課題と認識しておりますので、引き続き、関係省庁等と緊密に連携しながら進めてまいります。
3	新たなフレームワークを策定するのであれば、既存の制度・ガイドラインの整理を先行または並行して行うべきである。継ぎ足し的に増えてきた基準や文書の網羅は現場の負担を増大させており、例えば経済産業省やAISIのガイドライン、日本ネットワークセキュリティ協会（JNSA）のスキルマップとの関係整理も不可欠である。名称変更（NISCからNCOなど）のような用語変更は実質的効果が不明確な一方で混乱を招く可能性がある。新枠組みの追加は学習コストを増やし、攻撃者との非対称性を拡大しかねないため、既存制度を俯瞰・統合できる仕組みとすることが重要である。	本フレームワーク（案）は、新たな制度を追加的に創設するものではなく、既存の各種フレームワークとの相互参照を前提としております。そのため、現場の学習コストを増加させるのではなく、分散して存在する枠組みを俯瞰可能とすることで、むしろ活用の効率化に資するものだと考えています。
4	本案は人材の定義・体系化という点で意義があるが、静的なスキル整理に留まらず、更新責任主体・見直し周期・改訂トリガーを明確化した「継続的更新構造」を包含すべきである。また、インシデント時の初動判断責任、外部報告判断責任、経営層説明責任等と人材レベルを接続し、責任分解構造まで踏み込む必要がある。 さらに、中小企業・地方公共団体でも実装可能な段階的モデルや外部連携モデルを明示し、国際整合性も視野に入れた“運用型フレームワーク”へ進化させるべきである。	本フレームワーク（案）は、技術動向の変化等に応じて継続的に更新することを前提としており、固定的な指針ではなく、環境変化に適応するものとして運用する予定です。 有時と平時における役割の違いや中小企業における最低限必要な機能の考え方、情報処理安全確保支援士をはじめとする外部専門人材との接続の在り方等については、手引き書においてモデル事例を示しながら実務的に解説できるよう検討を進めています。 国際整合性に関しては、本フレームワーク（案）は米国のNICEとの相互参照を可能とする設計であるほか、英国主導の「サイバーセキュリティ人材に関する国際的な連合（ICCSW）」（令和７年１月共同署名）への参画を通じて、国際的枠組みとの連携に向けた議論にも関与しています。
5	経験年数を中心としたレベル定義から、実践的スキルや潜在能力重視へ転換すべきである。プロジェクト実績、競技会参加、コミュニティ活動等を評価軸に組み込むことで、多様な人材参入を促進できる。また、技術職を超えた社会的使命や価値観を示す視点、個人の主体性を尊重する「ジョブ・クラフティング」の考え方、専門職としてのキャリアパスの多様化（マネジメント一辺倒の到達構造の見直し）が求められる。加えて、燃え尽きや離職への対応を含む持続可能な人材マネジメント、ならびに教育に加えて「惹きつけ・採用・定着」までを包含する総合的な人材確保策の充実が必要である。	本フレームワーク（案）のレベル設定は、経験年数による一律の整理ではなく、タスク遂行水準等から総合的に判断するものです。また、マネジメントのみを到達点とするものではありません。その上で、御指摘を踏まえ記載の明確化を図る観点から、レベル３以上について、技術的専門性の高度化や専門領域における主導的役割といった要素を明記する方向で見直します。 その他、「惹きつけ・採用・定着」までを見据えた人材確保の観点も、今後の参考とさせていただきます。
6	本案はレベル4を「最終意思決定責任者」と定義し、各職種においても組織俯瞰や企画立案能力を上位条件に含めているため、実質的に「マネジメント＝専門性の頂点」という設計になっている。 その結果、フォレンジックや研究等の分野における“技術的頂点”が正当に評価されず、管理職にならなければ最高評価に到達できない構造となっている。 ITSSの発想を踏襲した縦型ピラミッド構造が前提にあるように見受けられるが、サイバーセキュリティ分野では卓越した技術力そのものが最高価値であり、管理業務と同一軸で整理することには無理がある。 Technical Track（技術特化型キャリア）を明確に設け、マネジメントに移行せずとも最高レベルに到達できる定義へ再設計すべきである。 また、経験年数を要件化することは年功序列的評価を助長し、優秀な若手の早期登用を妨げる可能性がある。役割ごとの特性に即したレベル再定義が必要である。	本フレームワーク（案）のレベル設定は、タスク遂行水準等から総合的に判断するもので、マネジメントのみを到達点とするものではありません。その上で、御指摘を踏まえ記載の明確化を図る観点から、レベル３以上について、技術的専門性の高度化や専門領域における主導的役割といった要素を明記する方向で見直します。 レベル定義における実務経験の考え方についても、年数による一律の整理ではありませんが、こちらも御指摘を踏まえ記載の明確化を図る観点から、当該年数相当の知識・スキルを有していることを含めて評価する形で整理するよう見直します。
7	ロール・レベル定義は整理されているものの、組織内にどの程度配置すべきかの指標が示されていないため、As-Is／To-Be分析や採用・育成計画への活用が難しい。人材類型の提示にとどめるのではなく、業種・規模別の参考配置モデルや自己評価ツールを整備するなど、実際の人材計画に活用できる形での補足が望まれる（本体に盛り込めない場合は活用ガイドライン等で提示することも考えられる）。 また、レベル要件として実務経験年数を掲げる点については、能力の実態を十分に反映しない可能性がある。スキル習熟度は年数よりも業務内容や経験の密度に依存するため、年数は参考指標にとどめ、業務範囲、役割、成果、資格、研修実績等を含めた総合的な評価の考え方を明確化することが望ましい。あわせて、異動・転職やキャリアチェンジを経た人材も適切に評価され得る仕組みとすることが重要である。	本フレームワーク(案）は、人材類型（役割）と能力水準（レベル）の共通整理を目的とするものであり、特定の配置人数や職位を一律に定めるものではありません。組織規模や特性に応じた活用が可能となるよう、モデル事例等は手引き書で提示する予定です。 レベル定義における実務経験については、年数による一律の整理との考えに基づくものではありませんが、御指摘を踏まえ記載の明確化を図る観点から、当該年数相当の知識・スキルを有していることを含めて評価する記載に修正し、力量も評価できるよう見直します。
8	本フレームワークは、これから学習・参入する人材の視点が弱く、成長目標となる客観的指標が不足している。 情報セキュリティマネジメント試験や情報処理安全確保支援士などの資格は、履歴書にも記載できる客観的評価軸であり、モチベーション向上にも資する。 しかし、情報処理安全確保支援士制度の社会的認知は十分とは言えず、企業人事で適切に評価されないケースもある。将来的には資格保有者の必置化や、難易度を調整した中間資格の新設など、客観的達成指標の整備を検討すべきである。	御指摘のとおり、資格取得は客観的指標として有効であり、学習段階にある方の目標設定や動機付けにも資するものと考えています。情報処理安全確保支援士を含む既存資格・試験との関係整理については、本フレームワーク（案）との接続の在り方を今後検討してまいります。 有資格者の必置化や新資格の創設といった制度的措置については、より中長期的かつ政策的な検討を要する構想であることから、将来的な論点として関係施策の動向も踏まえつつ参考とさせていただきます。
9	本案はITSSとの相互参照を掲げているが、レベル定義の整合性に疑問がある。 特に、レベル3以上でマネジメントを要件とする構造は、ITSSのレベル感（レベル3＝独力遂行、レベル4＝技術チームリーダ相当）と乖離しており、ITSS導入済組織で混乱を招く可能性がある。 また、マネジメント必須の設計では、卓越した技術専門家が上位レベルに到達しにくい。専門職トラックの明示や、レベル3・4定義の見直し（マネジメント固定の緩和）が必要である。 さらに、レベル1の「実務経験2年未満」という条件の意味合いが不明確であり、経験年数を「望ましい」とする現行記載も要件として曖昧である。経験年数を必須条件とするのか、参考情報とするのかを明確化すべきである。	本フレームワーク（案）はITSSとの相互参照を可能とする設計としておりますが、既にITSSを活用している組織に混乱が生じないよう、レベル設定の考え方や対応関係も考慮しています。 その上で、ITSSのレベル３にマネジメント要素は含まれていませんが、本フレームワークでは、有識者検討会においてコミュニケーション力や調整力等を重視すべきとの意見があったことを踏まえ、一定のマネジメント的要素を位置づけています。 また、上位レベルが直ちに管理職を意味するものではありませんが、御指摘を踏まえ記載の明確化を図る観点から、レベル３以上について、技術的専門性の高度化や専門領域における主導的役割といった要素を明記する方向で見直します。 各レベルの実務経験の考え方は、年数により一律の整理ではなく、あくまで目安として記載しているものです。
10	現行案は、上位レベルほどマネジメントや最終意思決定責任を要件としており、「上位＝管理職」と読める構造になっている。その結果、管理を担わない高度専門職の到達点が不明確で、技術力強化や人材育成の目的に逆効果となるおそれがある。 NISTのNICE、ENISAのECSF、SFIA FoundationのSFIA等を踏まえ、レベルは自律性・影響範囲・業務難易度で定義し、管理を必須としない上級専門職の道筋を明示すべきである。また、「最終意思決定」は技術判断とリスク受容を区別して整理する必要がある。	本フレームワーク（案）のレベル設定は、管理職昇進を前提とするものではなく、段階的に影響範囲や責任の広がりを示す考え方です。レベル３・４の「マネジメント」や「最終意思決定」も、職位ではなく業務上の責任・影響度を例示したものです。 しかしながら、「上位＝管理職」との誤解を招き得るとの御指摘を踏まえ記載の明確化を図る観点から、レベル３以上について、技術的専門性の高度化や専門領域における主導的役割といった要素を明記する方向で見直します。
11	国際的には、技術分野の最上位人材を管理職とは分離した専門職として位置付ける制度が一般的であり、国際連携の場面でも高度専門家同士が直接対応することが多い。このため、技術系最上位レベルが明確でない場合、国際的な役割分担や評価基準との不整合が生じる可能性がある。 また、国家安全保障分野では、先端攻撃研究など高度な技術能力が国家防衛力に直結することから、管理職ではない技術トップ人材を最上位として評価する仕組みが整備されている。こうした実態を踏まえ、技術専門職として到達可能な最高レベルを明確化するとともに、マネジメント系とスペシャリスト系の並列的なキャリア構造を整理し、技術成果を重視した評価の考え方を導入することで、国際的枠組みとの整合性を確保することが望ましい。	本フレームワーク（案）のレベル設定は、タスク遂行水準等から総合的に判断するもので、マネジメントのみを到達点とする考えに基づくものではありません。その上で、御指摘を踏まえ記載の明確化を図る観点から、レベル３以上について、技術的専門性の高度化や専門領域における主導的役割といった要素を明記する方向で見直します。 また、国際的なフレームワークとの関係については、既に米国のNICEとの相互参照が可能となるよう設計しており、加えて英国主導の「サイバーセキュリティ人材に関する国際的な連合（ICCSW）」（令和７年１月署名）への参画等を通じて、国際的な議論にも関与しています。
12	レベル3・4がマネジメント前提の定義となっており、脆弱性評価能力と必ずしも一致しない。 実務では、純粋な技術力（侵入可否判断・検出能力）が最も高い人材がレベル2相当の場合もある。 現行案はビジネス・管理寄りで、純粋技術能力の評価が弱い懸念。 防御力確保にはマネジメント以上に高度な実務技術力が重要。 技術重視型の制度設計への見直しを求める。	本フレームワーク（案）のレベル設定は、タスク遂行水準等から総合的に判断するもので、マネジメントのみを到達点とする考えに基づくものではありません。その上で、御指摘を踏まえ記載の明確化を図る観点から、特に上位レベルにおいてマネジメント要素に偏らないよう見直します。とりわけ、脆弱性評価や高度な分析・対処等の専門的技術を要する役割については、技術的専門性や技術的影響力そのものが上位レベルの到達像として適切に位置付けられるよう記載します。

No.	御意見要約	回答案
13	①意思決定・戦略策定のレベル設定について、レベル4の必須条件として組織内での「調整能力」を入れるべき。また、レベル3の条件①は必須とすべき。 CISOについては、「経営レベル」の役職としての位置づけ、「経営層（取締役等）」の責任と権限のもとで、専門的な知識を行使できる必要がある。	本フレームワーク（案）は、各レベルが段階的に能力を拡張する構造としており、レベル４はレベル３で求められる能力を前提に、より広い影響範囲と責任を担う位置付けです。レベル３においても、関係者との会話・説明等を通じたコミュニケーション力や一定のマネジメント要素を含んでおり、その延長としてレベル４では組織横断的な調整や意思決定への関与を想定しています。 CISOについては、経営層の責任と権限の下で専門的知見を発揮する役割の重要性を踏まえ、その位置付けが適切に伝わるよう手引き書において記載します。
14	人材育成の議論は文書作成にとどまり、具体性・実効性が不足している。現場では教育予算が削減されており、方針と実態に乖離がある。フレームワークを作るだけでなく、実際に運用できる体制・予算措置を伴うべき。	御意見として承ります。
15	脆弱性情報は継続的収集が不可欠だが、何をどう集めるべきか判断が難しい。情報収集が属人的になりやすく、特に少人数体制では限界があり、個人スキルなのか、組織的仕組みとして整備すべきかが不明確。 有事対応だけでなく、平時の継続的情報収集（例：SBOM等）を体系的に位置付けるべき。	本フレームワーク（案）では一般的に各組織に求められるタスクを整理しているものであり、具体的な人材像については、各組織の実情や体制等を踏まえて検討されることを想定しています。
16	現行のサイバーセキュリティ人材フレームワークは、役割整理とレベル設定により共通言語化を図る点は評価できるが、最終責任の所在や専門性の保証が制度的に担保されていない。そこで、レベル４相当業務の一部を情報処理安全確保支援士に位置付け、重大インシデントの最終技術判断や経営向け適合意見などを担う責任専門職として明確化すべきである。 あわせて、重要インフラ事業者や大企業に専属または常勤契約の登録支援士配置を段階的に求め、レベル要件（レベル３・４）にも登録支援士を組み込むことで、フレームワークを責任構造を備えた実効的制度へと強化すべきである。小規模組織については外部顧問モデル等で対応する。	本フレームワーク（案）は、人材の役割と技能を整理し、官民共通の参照軸を示すことを目的とするものであり、特定資格への独占業務付与や専属配置の義務化までを制度として定めるものではありません。 一方で、高度専門人材の活用は重要と認識しており、小規模組織向け手引き書では情報処理安全確保支援士等の外部専門家を活用するモデルを示しています。 また、本フレームワーク（案）は資格の有無のみによって人材の能力水準や役割適合性を判断するものではありませんが、国家資格・試験等は高度専門性を客観的に示す指標の一つとなり得ることから、今後の運用や関連施策の検討において、その位置付けを整理してまいります。
17	「脆弱性診断」と「ペネトレーションテスト」を同等に扱うのは適切ではない。前者は弱点の評価、後者は攻撃者視点での実証的攻撃であり、求められる技能が異なるためである。よって、「攻撃シミュレーション（レッドチーム）」を独立した役割として追加することを提案する。	御指摘のとおり、脆弱性診断とペネトレーションテストは手法や求められる技能に違いがあることは認識しておりますが、フレームワーク（案）本体では、役割の過度な細分化を避け、タスク（T)、知識（K)、スキル（S)において汎用的に整理する構成としております。他方、御指摘も踏まえて、手引き書においてそれぞれの位置づけの違い等を解説してまいります。
18	AIが急速に進化しておりセキュリティ人材の補完をしている現状を鑑みると、サイバー人材フレームワークにおいても、人間とAIの役割分担と、その役割分担を前提とした人間が担当すべき事項を明確化すべきではないか。	御指摘のとおり、AIの活用は今後ますます重要になると認識していますが、AIは特定の役割に限定されるものではなく、全ての役割に横断的に関係する要素と考えています。そのため、本フレームワーク（案）では、個別の役割として切り出すのではなく、知識（K）、スキル（S）において、AIの活用能力やAIを前提とした職務遂行力を共通要素として位置づけています。 今後のAI技術の進展状況を踏まえつつ、フレームワーク等に適切に整理・反映してまいります。
19	人材フレームワークの明確化は評価できるが、現状は資格要件が重視され、長年の実務経験やセキュリティ分野の修士・博士学位が十分に評価されにくい面がある。指定校制度等により学位をレベル定義と一定程度連動させる仕組みを設け、多様で高度な人材を活用できる枠組みを検討すべきである。	本フレームワーク（案）は、資格の有無のみに依拠するものではなく、タスク（T)、知識（K)、スキル（S）等に基づき能力を総合的に評価する考え方を採っております。 学位については、カリキュラムと知識（K）、スキル（S）との対応関係を可視化するなど評価手法が確立すれば、御指摘の点も可能になると認識しており、引き続き考慮してまいります。
20	「情報収集・分析・共有」共有後の評価もふくむはずであり表現が長くなるため、「脅威インテリジェンス」とまとめてはどうか。「脆弱性評価」は、ペネトレーションテストなども含まれるところ、ペネトレーションやレッドチームなどはより高度なスキルを要するため、テストごとに分野をわけるか、差別化してはどうか。 その他、SFIAやCMMC等のスキルフレームワークやセキュリティ成熟度モデルとの相互参照、個人用の手引書では具体的に資格試験等との関連付けも検討してほしい。	「情報収集・分析・共有」は、御指摘のとおり評価までを含む活動を想定しており、特定の用語（「脅威インテリジェンス」）に置き換えずとも趣旨は包含されていると考えます。 脆弱性評価とペネトレーションテスト等については、求められる技能に違いがあることは認識しておりますが、他方で、本フレームワーク（案）では、役割の過度な細分化を避け、タスク（T)、知識（K)、スキル（S)において汎用的に整理する構成としております。 また、SFIAやCMMC等との相互参照や資格との対応付け等、今後の検討課題といたします。
21	客観的な指標として利用する観点から、情報処理技術者試験等の合格実績を本フレームワークと紐づけることはできないだろうか。	情報処理技術者試験等の資格試験等との関連付けについては、今後の検討課題とさせていただきます。
22	本フレームワーク案は、サイバーセキュリティ人材に求められる役割・TKSを体系化し、4段階のレベル定義や利用主体別手引きを整備している点で高く評価できる。採用・配置・育成・評価の共通言語として活用可能な有意義な基盤である。 一方で、実務への定着を促すためには以下の具体化が必要である。 ① 役割の兼務を前提としたモデル提示とMust／Betterの二層構造化 ② レベル1～4の客観性向上（Rubric、成果物例、三面評価テンプレート） ③ NICEとの整合に加え、国内研修・資格・実務適用までの学習導線マップの明示 特に小規模組織・自治体向けには、最小限モデル、外部委託のRACI整理、評価制度（Level3・4）との対応関係、LGWAN等の特性反映、委託先管理標準条文の提示が有効である。 さらに、教育機関との地域連携モデルや、個人向けセルフアセスメントツールおよび資格との体系的な学習ロードマップを整備することで、産学官および個人の活用が一層進むと考える。	役割の兼務モデル、レベル1～4の評価方法（考え方・活用例）、小規模組織向けの最小限モデルやセルフアセスメントツールについては、いずれも手引き書において具体的な事例等を示しながら解説する予定です。 なお、資格制度等との具体的な関連付けについては今後の検討課題といたします。 その他の御意見につきましても、今後の具体化・運用設計に当たり、検討課題として整理してまいります。
23	私は個人として迷惑メールの継続的な分析を行ってきた。その結果、攻撃は生活インフラを横断し、日本企業のブランドを騙って国民のクレジット情報等を詐取する組織的犯罪であると認識している。しかし本フレームワーク（案）では、業界横断の攻撃構造を理解する人材像、偽装されやすいブランド特性を分析する視点、報告窓口の設計や不正サイト停止依頼を担う実務能力、国家と民間の情報連携を主導する役割が十分に明確化されていない。 攻撃が生活インフラを横断している現実を踏まえ、 ①生活インフラ横断型の分析人材の明確化、 ②報告窓口設計・運用スキルの明示、 ③国家レベルの情報連携を担う人材の位置付け、 をフレームワークおよび手引き書に反映すべきである。これにより、本案はより実務に即し、国民の安全確保に資する実効性ある基盤となると考える。	御意見として承ります。
24	国際的な事業環境におけるインシデント対応の実務を踏まえ、いくつか提案する。まず、人材要件の整理に当たっては、組織規模だけでなく、取り扱う情報の重要度や域外規制の適用有無などの規制影響度も補助軸として考慮すべきである。 また、米国NICEやEU Cybersecurity Skills Framework、ISO関連規格との対応関係を明示し、国際展開企業における人材育成や評価基盤として活用しやすくすることが望ましい。さらに、多言語調整や本社・現地間の責任分界整理などを含む越境インシデント対応を担う人材像を補足するとともに、レベル4については国際規制対応力や企業価値毀損リスクの評価能力など、経営責任に直結する観点を明示することが望ましい。 これらを補強することで、本フレームワークの国際的な活用可能性が高まると考えられる。	御指摘の情報の重要度や規制影響度を踏まえた人材要件については、フレームワーク上の「戦略推進・プロジェクト管理」や「法務」の役割に包含されるものと考えています。 また、越境インシデント対応を担う人材像等についても、既存の役割の中で包含し得るものと考えていますが、実務上の分かりやすさの観点からの整理については今後の検討課題とします。 国際フレームワークとの関係については、本案は既にNICEと相互参照可能な設計としておりますが、その他の国際的枠組みとの関係性についても、今後必要に応じて整理・明確化を図ってまいります。 レベル4の要件に関する御指摘については、経営責任との関係を含め、運用上の解説の充実に当たり参考とさせていただきます。
25	本案は現状の組織実態を整理した構成となっている一方で、指針として求められる「目指すべき専門性の姿」が十分に示されていないと考える。特に役割8「運用管理」に多数のNICEロールが集約されている点については、将来的な細分化の方向性と段階的ロードマップを明示すべきである。また、役割6「脆弱性評価」と役割12「設計開発」における評価機能の重複整理や、OTサイバーセキュリティの位置づけの明確化についても検討結果を示すことを求める。	本フレームワーク（案）は、サイバーセキュリティ人材に求められる役割や技能を汎用的に整理するものであり、過度に細分化しない方針で整理しております。 役割⑧「運用管理」の構成、役割⑥「脆弱性評価」と役割⑫「設計開発」における評価機能の整理については、役割ごとに観点が異なるものと認識しています。OTサイバーセキュリティの位置づけについては、役割間の重複や過度な細分化を避ける観点から包括的に整理しております。
26	本フレームワークは、表の構成上、マネジメント人材のみが高レベルに到達できる設計となっており、管理職に進まないスペシャリスト人材は実質的にレベル２にとどまる内容に見える。これは、民間企業における多様なキャリアパス確保の観点や、専門人材の海外流出が指摘される現状を踏まえると課題である。 他フレームワークとの「相互参照」も、実質的には対応表の提示にとどまり、スペシャリスト人材を適切に評価・位置付ける仕組みにはなっていない。 資料全体ではなく本体の表のみが参照される可能性を踏まえ、管理職に進まない専門人材のキャリアパスも明確に示されるよう、フレームワーク本体の表構成を見直すべきである。	レベルについては、管理職のみが上位レベルに到達することを意図したものではありません。その上で、御指摘を踏まえ記載の明確化を図る観点から、レベル３以上について、技術的専門性の高度化や専門領域における主導的役割といった要素を明記する方向で見直します。 技術分野のエキスパートのような高度専門人材を含む多様なキャリアパス等については、手引き書等において今後具体化を図ってまいります。

No.	御意見要約	回答案
27	ユーザー企業（ビジネス側部門）において現場と高度専門人材を橋渡しする「プラス・セキュリティ人材」を本フレームワークの中核ロール（いわば第14のロール）として明記し、その認定要件として「ITパスポート」「情報セキュリティマネジメント（SG）」「データマネジメント（仮称）」の3区分合格を条件とする名称独占の国家資格を創設すべきである。 本フレームワークで示される13のロールは供給側の専門人材としては網羅的であるが、日本の脆弱性の本質は専門家不足以上に、ユーザー企業側のビジネス人材における基礎的リテラシーの不足にある。サプライチェーン攻撃に対して高度資格者を大量配置することは現実的ではなく、現場業務を理解しつつ専門家へ適切にエスカレーションできる人材層の厚みこそが不可欠である。 2027年度の新試験制度で整備される試験区分を組み合わせて資格化すれば、新たな試験開発コストを抑制しつつ既存制度の価値を高めることができる。さらに名称独占資格とすることで、企業内の配置・昇進基準と直結させやすくなり、リスキリングの実効性と労働市場の流動化を促進できる。 このような人材をフレームワーク上に明確に位置づけることにより、13の専門ロールを実装面で接続する結節点が形成され、本フレームワークの実効性と日本全体のサイバーセキュリティレジリエンスの底上げにつながる。	本フレームワーク（案）においては、いわゆる「プラス・セキュリティ人材」に相当する機能は、既存の複数の役割の中に包含されております。 また、本フレームワーク（案）は特定の資格創設を前提とするものではなく、国家資格・試験等は人材の客観的指標の一つとして活用し得るものであり、今後の運用や活用施策の検討の中で参考にさせていただきます。
28	サイバーセキュリティ人材の評価の高度化と、国内外で通用する共通基盤の確立の観点から3点を提言する。 1. 実務経験年数要件の廃止 レベル判定における「実務経験年数」の一律要件を削除し、実務上の成果・責任に基づく能力評価へ転換すべき。 2. 国内外標準との整合確保 国内標準である IPA 所管のITSSとの互換性を確保しつつ、国際標準である SFIA Foundation が策定するSFIA 9を参照し、国内外で通用する体系へ再編すべき。 3. 高度人材層の細分化 「レベル4以上」を一括りにせず、技術アーキテクトやリーダー人材を適切に評価できる多層的な構造へ拡張すべき。	レベルの定義における実務経験については、年数による一律の整理を意図したものではありません。その上で、御指摘を踏まえ記載の明確化を図る観点から、当該年数相当の知識・スキルを有していることを含めて評価する形で整理するよう見直します。あわせて、上位レベルの在り方についても見直しを行い、レベル３以上について、技術的専門性の高度化や専門領域における主導的役割といった要素を明記する方向で見直します。 国内外標準との整合についても留意しつつ、今後の運用や活用施策の検討の中で参考にさせていただきます。
29	SecBoKとの補完関係や具体的な活用方法について、本フレームワークとどちらを主軸として活用する想定なのかなど、関係整理の考え方を明確にすべきである。 また、レベル設定における「サイバーセキュリティに関する実務経験」が何を指すのかを明確化し、レベル判定のばらつきを防ぐ考え方を示す必要がある。さらに、一部の役割でレベルが「2〜4」とされている設計意図を示すとともに、専門人材とプラス・セキュリティ人材のレベル判定の考え方や、資格・研修とロール／レベルとの関係についても整理して示すことが望ましい。	SecBoKとの関係については、知識体系としてのSecBoKと本フレームワーク（案）が相互補完的に活用されるよう既にロールの整理等を行っています。SecBoKを既に活用している主体においては、従来の取組を尊重しつつ柔軟に参照していただき、これまで活用していない主体においては本フレームワーク（案）を導入時の共通言語として活用することを想定しています。 また、「実務経験」について本フレームワーク（案）ではあくまで標準系を示すものであり、各組織の特性等に応じて具体化が図られるものと認識しておりますが、御指摘は今後の検討課題といたします。 専門人材とプラス・セキュリティ人材のレベル定義は共通の考え方に基づくものとしており、資格・研修とロール／レベルとの関係については、今後手引き書等において整理を検討してまいります。
30	日本のサイバーセキュリティ上の課題は専門人材の不足だけでなく、ユーザー企業のビジネス人材における基礎的なセキュリティリテラシーの不足にあるため、既存制度を活用した人材育成の仕組みを強化すべき。具体的には、 ・情報セキュリティマネジメント試験（SG）合格者を、プラス・セキュリティ人材の中核として本フレームワーク上に位置づけること（例：第14のロールとして定義） ・SG合格者の配置をSECURITY ACTION（二つ星）要件と連動させるなど、組織内での活用を促す仕組みを設けること ・SG合格者をデジタルスキル標準（DSS）のサイバーセキュリティマネージャーや情報処理安全確保支援士（SC）へ段階的に育成する制度的接続を整備すること など、既存制度（SG、SECURITY ACTION、DSS、SC）を連携させ、ユーザー企業側のプラス・セキュリティ人材を体系的に育成・活用する仕組みを構築すべき。	御指摘のとおり、ユーザー企業側のビジネス人材のセキュリティリテラシー向上や、いわゆるプラス・セキュリティ人材の育成は重要な課題であると認識しています。本フレームワークにおいても、専門人材に加え、各業務分野でセキュリティを理解し実践する人材の重要性を踏まえて整理しています。 一方で、本フレームワーク（案）はサイバーセキュリティ人材に求められる役割や技能を汎用的に整理することを主な目的としており、特定の資格制度や試験制度を前提として役割を定義することは想定していません。御提案のような既存制度との具体的な連携の在り方については、今後の人材育成施策の検討に当たっての参考とさせていただきます。
31	レベル4については、役割を問わず責任を担うレベルであることを明確にすべき。あわせて、日本企業では高度なサイバーセキュリティ人材が十分に評価されず海外企業へ流出する例もあるため、CISO・CTO等の専門人材がCEOと同等又はそれ以上の価値を持ち得ることを示すなど、高度専門人材の位置づけを明確化すべき。	レベル4については、特定の職位や職員を指すものではなく、各役割において高度な専門性を発揮しつつ重要な判断や責任を担うレベルを想定して整理しているものです。いただいた御意見は、高度専門人材の位置づけや評価の在り方の観点から、今後の参考とさせていただきます。各組織のガバナンス体制に応じたCISOの位置づけについては、手引き書において記載してまいります。
32	各役割のレベル設定が一本道のキャリアを前提とし、上位レベルでマネジメント要素が強く求められる構造となっているため、技術や技能を高める専門職のキャリアが評価されにくい可能性がある。技術系役割については、専門性を高めるキャリアとマネジメント系キャリアを分けるなど、複線的なキャリアパスの整理が望ましい。 また、レベル定義が一律の構造となっており、役割ごとの実態が十分に反映されていない可能性があることから、役割の特性に応じたレベル設定やキャリア形成の考え方を示すことが望ましい。さらに、知識・スキルの評価方法が明確でない点や、人材像がイメージしにくい点についても、評価の指針や具体的な職務例を示すなどの補足が必要である。	本フレームワーク（案）のレベルにおいて、専門性の向上とマネジメントの双方のキャリアを想定しており、必ずしも単一のキャリアパスを前提とするものではありません。その上で御指摘も踏まえ記載の明確化を図る観点から、技術的専門性の高度化や専門領域における主導的役割といった要素を明記する方向で見直します。 また、その具体的な活用については各組織の実態に応じて柔軟に対応いただくものと考えております。 役割の特性に応じたレベル設定については、今後、事例の蓄積を踏まえて検討していくべき課題だと認識しています。 知識・スキルの評価方法や具体的な人材像についても、手引き書等の中でその一例を示してまいりますが、御指摘の内容も参考にさらなる充実を図ってまいります。
33	本フレームワーク案について、いくつか改善を提案する。まず、レベル定義において実務経験年数の比重が大きく、若手の高い能力を有する人材や他分野からの転職者が上位レベルに到達しにくい可能性があるため、年数要件の位置付けを見直し、成果や資格等も含めた柔軟な評価基準とすることが望ましい。 また、13の役割を前提とした構成は中小企業・小規模組織では現実的でない場合もあることから、簡易版や役割の優先順位、規模別の活用モデルを示すなどの配慮が必要である。加えて、AI等の技術進展を踏まえた内容の具体化や、フレームワークの陳腐化を防ぐための定期的な見直しの仕組みを明確化することも重要である。 さらに、企業で活用されている国内外のセキュリティ資格との関係を整理し、ロール・レベルとの対応関係を示す資料を提示するとともに、監視・対処・情報収集など実務上兼務されることの多い役割について、具体的な役割の組み合わせ例を示すことが望ましい。	レベルの定義における実務経験の考え方について、年数による一律の整理ではなく、業務内容や成果等も踏まえた総合的な判断を想定しており、年数は参考目安として位置付けています。 また、中小企業での活用については役割の兼務を前提としており、組織規模別の手引き書で具体的な活用方法を示す予定です。AI等の技術進展への対応やフレームワークの見直しについては、今後の運用状況を踏まえ検討してまいります。 既存資格との関係整理や役割の組み合わせ例についても、今後の検討の参考とさせていただきます。
34	レベル3を「マネジメントを行う者」、レベル4を「最終意思決定に責任を負う者」と定義している点について、技術専門職であっても管理職や意思決定権限を持たなければ最高レベルとして評価されない構造となっており、技術専門職の評価が相対的に低くなる可能性があるとの指摘。 また、米国のテクニカルパス（インディビデュアル・コントリビューター）や、National Institute of Standards and Technology の NICE Framework、および Information-technology Promotion Agency が策定した IT Skill Standard では、必ずしも管理職であることを上位レベルの要件としていないことを踏まえ、技術専門職としてのキャリアパスや能力評価の在り方について再検討すべき。	レベル定義については、ITSS等の既存の枠組みも参考としつつ、これまでの有識者検討会における議論を踏まえ、各役割において求められる責任や役割の広がりを整理したものです。本フレームワーク（案）におけるレベルは、特定の職位や人事制度を前提とするものではなく、技術的専門性を含めた能力発揮の在り方を整理する観点から設定しています。その上で、御指摘を踏まえ記載の明確化を図る観点から、技術的専門性の高度化や専門領域における主導的役割といった要素を明記する方向で見直します。
35	レベル4を「業務における最終意思決定に責任を負う者」とする組織ベースの要件は、ITSSが示す「専門分野を確立し課題解決をリードするレベル」という定義や、技術専門職の実態と必ずしも整合しない。高度な技術力を有する専門人材が役職や最終意思決定権限の有無により適切に評価されない可能性があるため、技術的リーダーシップや複雑課題の解決等の成果・能力ベースの観点を中心とした定義への見直しを求める。	レベル４における組織において重要な判断や責任を担う役割に関する定義については、ITSSの考え方も参考としつつ、これまでの有識者検討会における議論を踏まえ、サイバーセキュリティ分野において求められる役割や実務の実態を考慮して本フレームワーク（案）において独自に整理しているものです。その上で、御指摘も踏まえ記載の明確化を図る観点から、技術的専門性の高度化や専門領域における主導的役割といった要素を明確に位置づける方向で見直しを行います。
36	レベル3について、ITSSでは「独力で作業を遂行できる能力」を指すにもかかわらず、本案では「マネジメントを行う者」等の要件を課しており整合していないため、マネジメント要件の削除又はITSSとの対応関係の説明の見直しを求める。	レベル3におけるマネジメント要素については、ITSSの考え方も参考としつつ、これまでの有識者検討会における議論を踏まえ、サイバーセキュリティ分野において求められる役割や実務の実態を考慮して本フレームワーク（案）独自に整理しているものです。他方、御指摘も踏まえ、技術的専門性の高度化や専門領域における主導的役割といった要素を明確に位置づける方向で見直しを行います。
37	本フレームワーク案は、従来の人材フレームワークと比べて実用性が高く、全体として賛同する。その上で、いくつか改善を提案する。 まず、レベル4の「最終意思決定に責任を負う者」という表現は曖昧であるため、善管注意義務などの具体例を付記し責任範囲を明確化することが望ましい。また、「実務経験」についてもTKSとの関係が分かる形で具体化する必要がある。 さらに、中小規模組織では役割の兼務が多いため、兼務しやすい役割の組み合わせや兼務すべきでない役割を整理した手引き書の整備が望まれる。加えて、役割4（対処）には「インシデント手順書の作成」をタスクとして追加すること、役割12（設計開発）は将来的な設計と開発の分割も視野に整理することが考えられる。 あわせて、記述の整合性確認を行うとともに、TKSの評価方法としてテストやデジタルバッジ等の活用を検討し、既存フレームワークに加えてECSFとの対応関係も整理することで、実務活用性と国際整合性を高めることが望ましい。	レベル4の定義の明確化や実務経験の具体例の提示、TKSの評価方法に関する御意見については、フレームワークの実務的な活用の観点からの御指摘として受け止め、今後の運用や見直しの検討の参考とさせていただきます。 役割④「対処」におけるインシデント手順書の作成については、本フレームワークではタスクを過度に細分化しない整理としていることから、既存のタスクの中で包含して整理しております。 役割の兼務に関する御指摘については、中小規模の組織において役割を兼務する場合があることも踏まえ、実務での活用を想定した手引き書の中で、可能な範囲で反映いたします。 その他、ECSFとのマッピングに関しても反映を検討するとともに、個別のTKSの評価方法等についても今後の検討課題といたします。表記揺れについては、御指摘を踏まえ記載の整合を図るよう修正いたします。
38	監視や情報収集・分析を支えるSIEM等の監視・分析基盤の設計・構築・実装に関する役割が現行案では明確でないため、監視・分析業務と区別した上で、基盤整備に関する業務を既存役割内で明示する、又は独立した役割として位置づけるべき。	組織におけるSIEM等の監視・分析基盤の設計・構築に関する御指摘について、　組織ごとの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という観点では「戦略推進・プロジェクト管理」の役割に包含されるものと考えております。 他方、サービスとしてのSIEM等の設計・開発という観点では、セキュリティ事業者等が担う位置づけとして「設計開発」や「運用管理」において包含しうるものと考えております。 いただいた点を踏まえて、フレームワークを活用する組織特性を踏まえて、これらの対応関係がより分かりやすくなるよう、手引き書等における記載の明確化について今後の検討の参考とさせていただきます。

No.	御意見要約	回答案
39	本フレームワークは、官民共通のサイバーセキュリティ人材基盤として重要であり、13の役割と4段階のレベル、NICE等との相互参照を整理している点を評価する。役割名の見直しや組織規模別の手引き書の整備、既存フレームワークとの整合性確保も適切である。 その上で、能動的サイバー防御に関する政策との関係を明示し、フレームワークがその基盤となる位置付けを示すことが望ましい。また、日本固有の脅威事例や組織実態を踏まえた役割の具体化を手引き書で示すとともに、兼務を前提とした役割設計や官民連携を含む日本固有の設計思想を整理することで、国際的参照価値を高めることができる。 さらに、社会的意義や4段階レベルに基づくキャリアパスを明確化することで、人材志望者の関心喚起にもつながると考えられる。	御指摘の能動的サイバー防御や国家安全保障分野の施策との関係については、本フレームワークの直接の対象範囲とはしておりませんが、裾野が広がることで当該分野へも貢献することを期待しています。 また、各役割の具体的な活用イメージや、志望者にとってのキャリアパスの可視化、教育機関等での活用については、実務での理解を促進する観点から、今後の手引き書の見直し等において可能な範囲で反映することを検討いたします。 あわせて、役割設計の考え方や本フレームワークの位置づけについても、利用者にとって理解しやすい形で示すよう、今後の整理の参考とさせていただきます。
40	本フレームワークの知識項目（K）は、リスク管理やツール運用等は整理されている一方で、攻撃の成立原理を理解するための基盤的なコンピュータサイエンス知識（OS、ネットワーク、コンピュータアーキテクチャ等）の位置づけが十分に明確ではないと考える。 脅威分析、インシデント対処、脆弱性評価、設計開発等を実効的に担うためには、①OS・ネットワーク等の基礎技術、②SBOM等を含むソフトウェア構造理解、③AIやシークレット管理等の新たな攻撃対象に関する知識といった技術基盤を体系的に整理し、役割④、⑤、⑥、⑫、⑬等の知識・スキルに段階的に位置づけるべきである。 また、各レベルに応じた理解の深度を明確化するとともに、役割1において制度・政策に関する知識を補強するなど、ツール操作やポリシー理解にとどまらず、技術原理に基づき脅威を分析・判断できる人材育成の観点からフレームワークを整理すべきである。	本フレームワーク（案）における知識（K）及びスキル（S）は、NICEと相互参照可能な設計で、サイバーセキュリティ人材に求められる能力を汎用的に整理したものです。御指摘のOS、ネットワーク、コンピュータアーキテクチャ等の基盤的な知識については、「対処」、「脆弱性評価」、「設計開発」等を担う上で前提となる基礎的知識として位置付けられるものと考えておりますが、当該考え方の整理については教育向け手引き書で記載してまいります。 また、AIに関する知識や技術については、特定の役割に限定するのではなく、関連する役割全般において必要となる要素として整理しております。 役割に共通して求められる能力の水準については、レベル定義の中で整理しているところであり、役割①「意思決定・戦略策定」においては、制度・政策やガバナンスに関する知識も含めて整理しております。 御指摘の技術原理に基づき脅威を分析・判断できる人材育成の観点や、技術動向を踏まえた知識の整理の在り方については、今後のフレームワークの運用や見直しを検討する際の参考とさせていただきます。
41	サイバーセキュリティを取り巻く情勢が厳しさを増す中、人材育成・確保を目的とした本フレームワークの策定は時宜を得たものであり、その趣旨に賛同する。 他団体のフレームワークとの参照関係の整理や教育プログラムとのマッピング、各省庁間の連携強化、プラス・セキュリティ人材として持つべき意識の具体例の提示など、実務で活用しやすい形での継続的な取組を期待する。 また、将来的に本分野で世界をリードできる人材育成の指針となるよう、役割ごとの具体的な業務イメージの普及啓発を進めるとともに、例えば情報処理安全確保支援士の活躍場面を役割と対応付けて示すなど、国内施策と連携した活用を進めるべきである。	他団体のフレームワークとの参照関係の整理や教育プログラムとのマッピング、各省庁間の連携、プラス・セキュリティ人材として求められる意識の具体化、役割ごとの業務イメージの明確化等については、本フレームワークの実効的な活用を進める上で重要であると考えております。これらの点については、手引き書等において、活用イメージや具体例を示すことも含め、関係機関とも連携しながら普及・活用を進めてまいります。 情報処理安全確保支援士の活躍場面については、小規模組織向け手引き書において記載しております。
42	本フレームワークは国際的な枠組みを参照して役割やTKSを整理している点は評価できるが、各国フレームワークが前提としている脅威環境認識や政策体系が明示されておらず、フレームワークの根本的な前提条件が欠落していると考える。 サイバー空間における攻撃側の構造的優位性、攻撃者と防御者の能力・資源の非対称性、完全防御の不可能性（侵害前提）、脅威環境の継続的変化といった前提を明示しなければ、TKSは単なるチェックリストとして理解され、未知の脅威に対応できる人材育成基盤として十分に機能しないおそれがある。 このため、フレームワーク冒頭に脅威環境認識を整理したセクションを設けるとともに、各役割の補足説明やレベル定義において脅威環境との関係を明確化するなど、役割やTKSの必要性を説明できる構造とすべきである。 また、NICE等との対応関係についても、各国の政策体系や前提条件の違いを踏まえて整理することが望ましい。	本フレームワーク（案）は、我が国を取り巻く情勢を踏まえて、サイバーセキュリティ人材に求められる役割や技能を汎用的に整理したものであり、このため、特定の脅威認識や政策体系を詳細に示すものではありません。 御指摘については、今後の人材育成を進めるにあたり、社会全体としてどの分野に重点を置くべきか検討する上での参考とさせていただきます。
43	本フレームワークの各役割・スキルレベルについて、既存の国家資格・試験制度との対応関係を整理すべきである。 我が国では、情報処理推進機構が実施する情報処理技術者試験や情報処理安全確保支援士制度等、既に人材育成基盤となる資格制度が存在している。これらとの関係が明確でない場合、教育機関や企業における人材育成方針が分かりにくくなる可能性がある。 このため、フレームワークの役割・スキルレベルと既存資格制度との対応関係を整理し、教育機関、企業、受験者にとって活用しやすい体系とすべきである。	情報処理推進機構が実施する情報処理技術者試験や情報処理安全確保支援士制度を含む既存制度との関連付けについては、今後のフレームワークの普及・活用を進める中で、整理を進めていくことを検討してまいります。
44	魅力的なキャリアパスの提示や企業のサイバーセキュリティ対策の向上という目的に照らすと、新たなフレームワークを策定するよりも、既存の枠組みの活用促進や広報強化を優先すべきではないかとの意見である。 SecBoK2025など既存フレームワークの活用や、日本ネットワークセキュリティ協会との連携による普及、ロールモデルの発信やセキュリティ分野の魅力発信、さらにサイバーセキュリティお助け隊の広報強化等を進める方が効果的ではないかとしている。 また、新たなフレームワークを策定する場合には、目的達成度を客観的に評価できる指標や基準を事前に設定し、定期的に効果測定を行うなど、運用面での検証・見直しの仕組みを整備すべきであるとしている。	既存のフレームワークとの関係性については重要と認識しており、SecBoK2025 との参照関係については、本フレームワーク（案）の検討に当たり既に整理しております。今後も既存の取組との関係性を踏まえつつ、実際の活用状況や効果を見ながら継続的な見直しを行ってまいります。
45	本フレームワーク案について、役割定義、レベル設定及び評価方法等の見直しを求める。 13の役割ではセキュリティコンサルティングやリスク評価等の実務が十分に包含されていない可能性があるほか、レベル定義が管理職中心となっており高度な技術スペシャリストの到達点が不明確であるため、マネジメントと技術専門の双方のキャリアパスを示すべきと考える。 また、評価に当たっては経験年数や資格のみではなく、実績・技術力やコミュニティ活動等も考慮すべきである。	御指摘の役割の整理については、本フレームワーク（案）における既存の役割の中で一定程度包含され得るものと考えております。 また、レベル設定における経験年数は、一律の整理ではなく、あくまで参考となる目安として示しているものです。評価に当たっては、各組織の特性等に応じ、実務経験や成果、能力等を踏まえて総合的に判断されることが重要であると認識しております。加えて、コミュニティ活動等を通じた貢献や、関係者との調整を含め業務を遂行する能力といった要素についても、検討会での議論を踏まえ本フレームワーク（レベル）において考慮しており、評価への活用については手引き書でその一例をお示しします。 上位レベルの在り方については、御指摘を踏まえ記載の明確化の観点から、技術的専門性の高度化や専門領域における主導的役割といった要素を明記する方向で見直します。
46	本フレームワーク案の策定には賛同するが、技術や脅威環境の変化が速いことを踏まえ、行政主導の定期的見直しだけでは海外標準や実務ニーズとの乖離が生じる可能性があると考える。そのため、産学官のフィードバックを取り込む継続的かつ自律的な更新メカニズムを組み込み、複数年予算による安定的な運用体制の下でフレームワークを継続的に進化させる仕組みが必要であると考える。	御指摘のとおり、サイバーセキュリティを取り巻く技術動向や脅威環境の変化は速く、今後、産学官の関係者からの知見や実務からのフィードバックも踏まえつつ、必要に応じて見直しを行い、その充実を図ってまいります。
47	本フレームワーク案の方向性には概ね賛同するが、経営・戦略レベルの役割や実務タスクの定義に一部不足があると考える。具体的には、経営層によるサイバーセキュリティ戦略やBCPの策定などの戦略的タスク、設計段階におけるセキュリティ要件定義（Shift Left）、サプライチェーン管理を含む運用管理タスク、サイバーインテリジェンス分析能力の体系的整理などを補強すべきと考える。 また、本フレームワークの対象にセキュリティ製品開発者を含める場合には、製品設計・開発に関するタスクの位置付けについても整理が必要であると考える。	経営・戦略レベルの役割や実務タスクについては、本フレームワーク（案）における役割②「戦略推進・プロジェクト管理」や役割⑧「運用管理」等の中で、サイバーセキュリティ戦略の策定や事業継続の観点も含め整理しています。また、設計段階でのセキュリティ確保やサプライチェーンを含む運用管理、サイバーインテリジェンスに関する活動についても、各役割のタスクの中に包含して整理しています。 セキュリティ製品の設計・開発に関する業務についても、役割⑫「設計開発」の中に包含して整理しています。
48	役割番号の付け方に体系性がなく直感的に理解しづらいため、同一カテゴリに属する役割が把握しやすいよう番号の整理を行う必要がある。 レベル定義における実務経験年数をサイバーセキュリティ全体で整理している点について、役割ごとの経験年数も考慮しなければ人材配置や採用時にミスマッチが生じる可能性があることから、役割ごとの経験も加味した整理が必要である。 レベル1の条件である「サイバーセキュリティに関する実務経験が2年未満」という定義では下限が示されておらず条件として機能しにくいため、一定の下限を設けるなどの見直しが必要である。 スキル項目に高度な内容と汎用的な内容が混在しているため、レベル1～4に対応してタスク・知識・スキルを整理するなど、レベルとの対応関係が分かる形での整理が望まれる。 役割1「意思決定・戦略策定」と役割2「戦略推進・プロジェクト管理」の区分が分かりづらいため、役割の違いが明確になるよう名称や整理の見直しが必要である。	御指摘の役割番号の整理については、フレームワーク全体の分かりやすさの観点から、今後の見直しに当たっての参考とさせていただきます。 レベル定義における実務経験の考え方については、年数による一律の整理ではなく、当該年数相当の知識・スキルを有していることを含めて評価する形で整理するよう見直します。 レベル1の経験年数の下限に関する御指摘については、初学者も含めた幅広い人材の参画を想定している点も踏まえつつ、今後の運用状況も見ながら検討してまいります。 タスク・知識・スキルとレベルとの対応関係の整理については、フレームワークの活用のしやすさの観点から、今後の運用や改善の中で参考とさせていただきます。 なお、役割1と役割2の異なりについては一定の整理を行っているところですが、大規模組織向け手引き書においてより詳細に記載してまいります。
49	サイバーセキュリティ人材について役割・タスク・知識・スキルを体系的に整理し、官民共通の指針として可視化しようとする方向性自体には意義があると考える。一方で、本案は主として組織における人材育成や専門人材の輩出、業務に付加して知識を習得する就業者を中心に構成されており、全世代の国民を対象とした基礎的なサイバーセキュリティ理解の底上げという観点が十分に示されていないように感じる。 デジタル化が社会全体に広がる中で、サイバーセキュリティは専門人材や若年層のみが重点的に学ぶ分野ではなく、年齢や就業状況を問わず国民全体に必要な生活基盤であると考える。家庭で契約や管理を担う世代や高齢者、離職中の者、地方在住者なども含め、幅広い層が対象となるような視点が必要である。 そのため、本フレームワーク又は手引き書において、国民全体を対象とした基礎的な区分を明確に位置付け、学校教育に加えて社会人の学び直しや高齢者向け支援、地域拠点等での学習機会なども含めた段階的なモデルを示すことが望ましいと考える。専門人材の育成と併せて、国民全体の基礎的な防御行動の底上げを図る視点を持つことが重要である。	本フレームワーク（案）では、専門人材に加え、本来業務に加えてサイバーセキュリティの知識・スキルを身に付ける「プラス・セキュリティ」の考え方も概念として盛り込んでいます。 また、プラス・セキュリティ人材の育成や活用を念頭に置いた手引き書の作成も進めているところであり、御指摘の国民全体の基礎的な理解の向上という観点についても、今後の取組を進める上で参考とさせていただきます。

No.	御意見要約	回答案
50	能力評価における経験年数要件について、技術の進展が早い分野では経験年数の長さが必ずしも能力を担保するものではないと考える。そのため、タスク遂行実績や資格、脆弱性報告の実績等を踏まえた経験年数に依存しない「ポートフォリオ型評価」の導入を検討することが望ましい。 また、13の役割や多数のTKSは、小規模組織にとっては理解や活用の負担が大きい可能性があると考える。そのため、情報処理推進機構（IPA）の「中小企業の情報セキュリティ対策ガイドライン」との接続を強化し、中小企業が自社で取り組むべき事項を簡潔に判断できる小規模組織向けの要約版やチェックリストを整備することが望ましい。 さらに、インシデント対応においては技術的復旧だけでなく、法的リスクや広報、ブランド毀損等も踏まえた経営判断としてのトリアージ能力をより明確に位置付けることが重要であり、エンジニアと経営層の共通言語として機能するよう整理することが望ましい。	御指摘の能力評価における経験年数の考え方については、経験年数による一律の整理ではなく、当該年数相当の知識・スキルや実務能力を有していることを含めて評価する趣旨で整理しています。 また、TKSの数が多く小規模組織にとって活用が難しいのではないかとの御指摘については、小規模組織向けの手引き書において、御指摘のガイドラインを参照しつつ、モデル事例等を踏まえながら優先順位の考え方や具体的な取組の進め方を解説することとしております。 さらに、インシデント対応においては、関係部署との連携や組織としての対応の進め方も重要であることから、こうした観点についても手引き書の中で一部触れており、実務における活用の参考となるよう示しています。
51	現案の13の役割は各専門領域を機能別に整理した点では有用である一方、これらを横断的に統合し、組織全体として最適な意思決定につなげる役割が十分に位置付けられていないと考える。各役割が細分化されることで組織のサイロ化が進み、平時のガバナンスや有事の意思決定に支障が生じる可能性がある。 そのため、技術と経営を横断してリスクを統合的に扱う人材として、技術的リスクを経営の言語に翻訳し、経営判断を現場の統制に落とし込む多層的な翻訳能力や、各専門領域の活動を全体最適の観点から調整する機能を明確に位置付ける必要があると考える。 また、インシデント発生時に断片的な技術情報を統合し、経営判断につながる形で意思決定を支援する統合機能についても、専門職能として整理することが望ましい。これらの能力はCISOのみに限られるものではなく、組織の各レイヤーにおいて必要となるため、独立した役割として定義するか、あるいは高度専門職に共通する要件として明確に位置付けることが必要であると考える。	御指摘のとおり、サイバーセキュリティに関する取組を効果的に進めるためには、各専門領域の取組を横断的に調整し、「橋渡し」の役回りも重要な観点だと認識しています。 本フレームワーク（案）においては、役割①「意思決定・戦略策定」や役割②「戦略推進・プロジェクト管理」等において、関係者との調整や組織横断的な取組の推進といった要素を位置付けており、こうした役割の中で御指摘のような機能も一定程度包含されるものと考えています。 いただいた御指摘については、今後フレームワークの理解を深めるための手引き書の作成や活用事例の整理等を進める中で、参考とさせていただきます。
52	技術者が技術者として専門性を高めながらキャリアや処遇を向上させていくキャリアパスが十分に示されていないと感じており、欧米のように技術職のままキャリアやポスト、報酬が向上していく事例を示すことが必要であると考える。 また、提示されているExcel様式の使い方や企業における具体的な活用方法が分かりにくく、どのように自社の人材不足の状況を把握すればよいのかが理解しにくいと感じる。 さらに、人材評価の基準が定性的であるため適切な評価が可能か懸念があり、セキュリティの専門知識を持たない人事担当者でも活用できるよう、具体的な事例や判断の参考となる基準を示すことが望ましいと考える。	御指摘の技術者のキャリアパスに関する点については、本フレームワーク（案）においても、専門性を高めながらキャリアを形成していくことの重要性を踏まえ、レベルの上位段階においてマネジメント志向のキャリアと技術専門職としてのキャリアの双方を想定した整理が明確となるよう記載を見直します。 また、活用方法については、各組織の状況や目的に応じて柔軟に活用されることを想定しており、具体的な活用のイメージについては手引き書等において事例を示していますが、引き続き改善に努めてまいります。 さらに、人材の評価についても、本フレームワーク（案）は一律の評価基準を定めるものではなく、各組織の実情や人事制度等に応じて柔軟に活用されることを想定しています。御指摘の点については、今後の活用に向けての参考とさせていただきます。
53	本フレームワークが企業における人材の確保・配置・育成に実務的に活用できるかという観点から評価しており、特に育成・評価の指標として有用であることや、自組織に不足している人材像を定義し採用要件として示せることが重要であると考える。 監視業務の例では、インシデント初動対応やエスカレーション判断に関わるため、各レベルにおいて最低限求められる知識を一定程度明示することが望ましいと感じている。「有識者の指示により実行できる」といった表現のみでは、必要な知識を十分に持たない人材でも役割を満たしているように見える可能性がある点を懸念している。一方で、レベル差を主に経験年数で整理する考え方であれば一定程度理解できるとも考える。 また、自組織の不足人材の把握に当たっては、手引き書の構成イメージ自体は有用と評価しているものの、実際の運用では自己申告的な整理となる可能性もあり、具体化の仕方によっては評価や整理が難しくなるのではないかと感じている。	各レベルにおいて最低限求められる知識を明確に整理することについては、組織の規模やシステム環境、業務内容等によって必要となる知識の範囲が大きく異なるため、一律に示すことは難しい面があると考えています。このため、本フレームワーク（案）では一定の抽象度を持たせた整理とし、各組織の実情に応じて柔軟に活用されることを想定しています。 また、人材の把握や評価についても、各組織の人事制度や運用に応じて活用されることを想定しており、御指摘の点も今後の活用の参考とさせていただきます。
54	本フレームワークの方向性自体は支持するが、実効性を高める観点からいくつかの点を指摘する。 まず、現行案は情報システムを主対象として設計されており、OT・組込み・製品セキュリティを担う人材像が十分に位置付けられていないと考える。製品開発事業者においては、製品開発実務を前提としたセキュリティ対応や製品ライフサイクル全体のリスク管理、国際規制・標準への対応が求められることから、少なくとも役割12「設計開発」の補足説明や手引き書において、OT・組込み・製品セキュリティ人材の位置付けを明確化する必要があると考える。 また、レベル4が最終意思決定責任を負う者として整理されている点について、管理職への移行を前提としたキャリア構造となり、技術専門職が十分に評価されにくくなる可能性を懸念している。そのため、手引き書において、技術専門職と管理職が並立するキャリアモデルや、管理職に一定の技術理解を求めるモデルなど、組織が自らの実情に応じて参照できるキャリアパスの例を示すことが望ましいと考える。 さらに、セキュリティ人材の内製化と外部リソース活用の関係についても整理が必要であると考える。手引き書において、自組織で担うことが望ましい機能と外部リソースで補完可能な機能の考え方を示すとともに、本フレームワークを外部人材やサービスの評価基準として活用できる具体的な例を提示することが有用であると考える。	御指摘のOT人材については、役割⑧「運用管理」や役割⑫「設計開発」に包含されると考えており、実態としては各組織においてそれぞれのタスク（T）、知識（K）、スキル（S）を詳細化する中で、各組織の業務特性に応じ具体的な対象領域を含めて定義され、活用されることを想定しています。 また、技術専門職のキャリアパスに関する御指摘については、レベル4の位置付けを含め、上位レベルの区分の在り方について見直します。 セキュリティ人材の内製化と外部リソース活用の関係については、各組織の実情に応じた役割分担の考え方や活用の方向性を、手引き書において示していくこととしています。御指摘の点も今後の整理の参考とさせていただきます。