

パブリックコメントの実施結果及び 対応(案)について

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に係るパブリックコメントの状況について

- 令和8年2月17日(火)から3月10日(火)までの**22日間**、パブリックコメントを実施。
- **50者から56件**の意見が寄せられ、特にレベル設定について、実態を踏まえた定義の明確化を求める意見が中心。
- これを踏まえ、**レベル3以上を「マネジメント系」と「エキスパート系」に整理する**方向で見直しを行う。

意見の カテゴリ (整理)

- ① レベル定義・区分に関する意見**
 - 上位レベル＝マネジメントのみ、という印象
 - 技能を極めた専門家の位置付けが弱い 等
- ② フレームワークの構造・記載に関する意見**
 - 表現が抽象的で実務イメージが湧きにくい
 - 役割とタスクの関係がやや分かりにくい 等
- ③ 活用方法に関する意見**
 - 採用・配置等における実装方法が見えにくい 等
- ④ 教育・資格制度との連携に関する意見**
 - 教育カリキュラムや研修体系との接続
 - 既存資格や認定制度との関係整理 等
- ⑤ 他のフレームワークの相互参照に関する意見**
 - 既存の国内外フレームとの対応関係 等

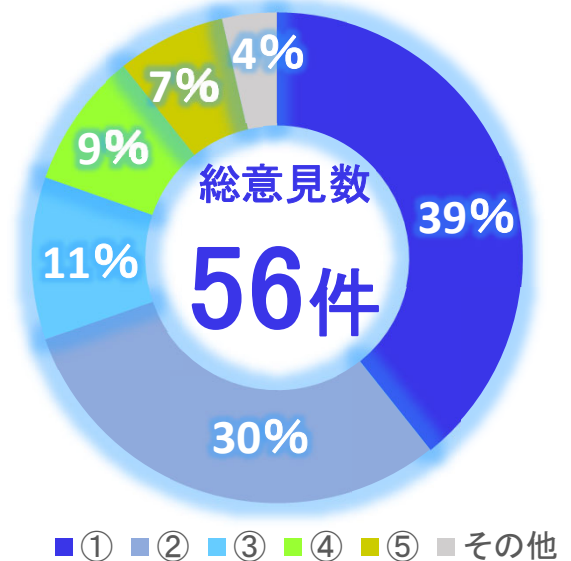
22件

17件

6件

5件

4件



うち提案意見

- **技術分野の専門性を踏まえたレベル設定(区分の新設等)としてはどうか。**
- **役割・タスクの定義について、内容や範囲が明確になるよう細分化して整理してはどうか。**
- **組織規模に応じた実践方法や外部専門家との連携を前提とした運用モデルを提示してはどうか。**
- **資格制度や研修等の取組とフレームワークの関係を整理してはどうか。**

対応

(1)レベルの見直し

上位レベルの在り方や専門性の位置付けに関する意見を踏まえ、レベル3以上を「マネジメント系」と「エキスパート系」の二系統に整理する方向で見直しを行う。

(2)手引き書等への反映

活用方法の具体化や教育・資格制度との連携に関する提案も踏まえ、フレームワークの実務での活用を念頭に、手引き書等において具体化・補足を図る。

※意見内訳は大きな分類
※複数区分にまたがる場合も、いずれからの区分(主論点)に分類

(参考)見直し前のレベル設定(第3回検討会)

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	<p>業務における最終意思決定に対して責任を負う者</p> <p>条件: 下記3点のうち2点以上を満たす者</p> <ol style="list-style-type: none">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ー)
3	<p>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</p> <p>条件: 下記3点のうち2点以上を満たす者</p> <ol style="list-style-type: none">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	<p>業務において指示に基づく作業を実行する者</p> <p>条件: 下記3点のうち2点以上を満たす者</p> <ol style="list-style-type: none">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	<p>業務に対する最低限必要な知識を有する者</p> <p>条件: 下記3点のうち2点以上を満たす者</p> <ol style="list-style-type: none">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)

パブリックコメントを踏まえたレベルの見直し(案)

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 (赤文字箇所が第三回検討会からの変更点)

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	<p>レベル4-M : 業務における意思決定に責任を負う者</p> <p>条件: 下記3点のうち2点以上を満たす者</p> <ul style="list-style-type: none"> 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 	<p>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</p> <p>条件: 下記3点のうち2点以上を満たす者</p> <ul style="list-style-type: none"> ① 各役割で定義されたタスク遂行を通じて、高い専門知識・スキルを有する人材として組織内外で認知されている ② 組織内教育や指導、コミュニティ活動や対外情報発信等を通じて組織内外のセキュリティ向上に貢献している ③ サイバーセキュリティに関する10年以上の実務経験に相当する実践的な知識・スキルを有する ※下線部はITSSレベル6以上に相当する部分 	<p>レベル4以上 (組織内や業界内等のハイレベルプレーヤ)</p>
3	<p>レベル3-M : 業務について関連するチームメンバーのマネジメントを行う者</p> <p>条件: 下記3点のうち2点以上を満たす者</p> <ul style="list-style-type: none"> 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 	<p>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</p> <p>条件: 下記3点のうち2点以上を満たす者</p> <ul style="list-style-type: none"> ① 各役割で定義されたタスクを自らが中心となって遂行することができる ② エキスパートとして自身の専門領域に関わる最新情報や動向の習得・活用を行っている ③ サイバーセキュリティに関する4~10年の実務経験に相当する実践的な知識・スキルを有する 	<p>レベル3 (独力で遂行可能)</p>
2	<p>レベル2 : 業務において指示に基づく作業を実行する者</p> <p>条件: 下記3点のうち2点以上を満たす者</p> <ul style="list-style-type: none"> 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 		<p>レベル2 (指導の下で遂行可能)</p>
1	<p>レベル1 : 業務に対する最低限必要な知識を有する者</p> <p>条件: 下記3点のうち2点以上を満たす者</p> <ul style="list-style-type: none"> 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 		<p>レベル1 (最低限必要な知識を有する)</p>