2026 年３月 10 日

内閣官房国家サイバー統括室　御中

一般社団法人全国銀行協会

「サイバーセキュリティ人材フレームワーク（案）」に対する意見について

2026年２月17日付で意見募集のあった標記の件に対する意見を別紙のとおり取りまとめ、提出いたしますので、何卒ご高配賜りますようお願い申しあげます。

以　　上

（別紙）

「サイバーセキュリティ人材フレームワーク（案）」に関する意見

項番	コメント箇所（頁、項番等）	コメント等
1	「サイバーセキュリティ人材フレームワーク（案）について」 4頁 （「サイバーセキュリティ人材が担う役割の全体像」）	現在示されている役割定義（13項目）は、実態に対して不足しています。セキュリティコンサルの立場、ポリシー・ガイドライン・組織規程策定の立場、サイバーセキュリティのリスクを評価する立場などが包含されておらず、実際の役割の範囲とは乖離が見られます。より広い視点での見直しが必要です。
2	「サイバーセキュリティ人材フレームワーク（案）について」 5頁 （「人材フレームワークのレベル設定について」）	レベル4の定義が「最終意思決定責任（＝管理職）」に偏重しており、高度な技術専門性を極めるスペシャリストの到達点が不明確です。 管理責任を担う「マネジメント・トラック」と、高度な技術課題を解決する「テクニカル・トラック」を併記し、両者が同等に評価される設計を明示すべきと考えます。
3	「サイバーセキュリティ人材フレームワーク（案）について」 5頁 （「人材フレームワークのレベル設定について」）	「経験年数」は必ずしも能力を担保する指標ではありません。 例えば、長年業界に身を置きながら実績が伴わない層に対し、最新技術に精通した若手層を過小評価してしまうリスクが懸念されます。 つきましては、年数指標を参考値に留め、具体的なプロジェクト実績、実技スキル、コミュニティへの貢献度といった「成果・能力ベース」の評価軸へシフトすることを提案します。
4	「サイバーセキュリティ人材フレームワーク（案）について」 5頁 （「人材フレームワークのレベル設定について」）	資格ビジネスの形骸化防止と「貢献文化」の醸成の観点が必要ではないでしょうか。 評価指標を特定の資格に固定化した場合、ベンダー主導の「資格・認定取得」のみが重視され、実務上の貢献と乖離する懸念があります。 機密保持を前提としつつ、ブログ、OSSへの寄稿、ISAC等のコミュニティ活動を通じた「外部への知見還元」を、高度人材の重要な評価指標として位置づけるべきです。 開発者コミュニティで機能している「実績に基づく信頼（レピュテーション）」の概念をセキュリティ分野にも導入すべく、組織が専門人材の外部発信を支援・許可するための指針を手引きに盛り込むことを提言します。特に国内外のカンファレンスでの登壇実績などは、組織内に閉じない客観的な専門性を示す指標として高く評価されるべきです。
5	「サイバーセキュリティ人材フレームワーク（案）について」 5頁 （「人材フレームワークのレベル設定について」）	今回のレベル定義にあたり、事業会社のセキュリティ専門組織においてセキュリティ人材が能力を効果的に発揮するためには、ビジネス知識・経験や企画・立案能力だけでは不十分であると考えます。 外部機関や他組織を含むステークホルダーとの折衝、および業務を完遂に導く実務遂行能力までを、高度人材に求められる必須要件としてレベル設定の定義に反映してもよいのではないでしょうか。
6	「サイバーセキュリティ人材フレームワーク（案）について」 5頁 （「人材フレームワークのレベル設定について」）	レベル４では、条件の内「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」および「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」の２点を満たす場合もこれに該当することになっていますが、この条件のみでは、事業会社におけるセキュリティ人材の「トップレベル」としての十分な評価を得るには至らないと考えます。 企画・立案能力に加え、策定した施策が正しい方向性を維持し、考慮不足が生じないよう適切に助言・リードしながら、最終的な完遂まで導く「実行推進能力」こそが、高度人材には不可欠ではないでしょうか。
7	「サイバーセキュリティ人材フレームワーク（案）について」 「サイバーセキュリティ人材フレームワーク（本体案）」 全般	セキュリティ関連業務に従事する人材像に関して、国内においてはJNSAが公開するSecBoKなどがあり、一方で、特にグローバル展開しているような大企業や活躍が国内に閉じない個人などはNICEフレームワークなどの海外との共通指標で捉えられるようにする必要性があるといった状況において、本「サイバーセキュリティ人材フレームワーク」が有効活用されるためには、これらの既存基準・指標とは別に本フレームワークを改めて定義する意義を明確に示す必要があるのではないでしょうか。
8	「サイバーセキュリティ人材フレームワーク（案）について」 「サイバーセキュリティ人材フレームワーク（本体案）」 全般	人材流動性に対応した「ポータブルな実績評価」の仕組み構築が不可欠ではないでしょうか。 例えば、現所属組織でのみ有効な評価指標では、転職などの環境変化のたびにキャリアの継続性が断絶することになり、適正な人材流動化と市場価値に基づく適正な処遇を妨げ、ひいてはサイバーセキュリティ人材の確保・育成の阻害要因となることも懸念されます。 特に個人向け手引書の作成に向けては、細かなタスクリストを固定的に決めるのではなく、評価の「型（インターフェース）」を標準化するアプローチを提案します。役割・難易度・成果を記録する「実績の標準フォーマット」を確立することで、業界全体としてセキュリティ人材を適正に評価・活用できる環境が整うと考えます。
9	「サイバーセキュリティ人材フレームワーク（案）について」 「サイバーセキュリティ人材フレームワーク（本体案）」 全般	個人向け手引書の作成に向けては、細かな知識項目（K）やタスク（T）の確認に終始するのではなく、本フレームワークの役割定義に基づき、自らの実績を客観的に把握し、外的に評価を獲得できる人材の育成を目指すべきです。 特定の組織に閉じない、より高次な視点でのセルフアセスメントが行われるような仕組みが求められます。

以 上