サイバーセキュリティ人材フレームワークに関する検討会（第１回）議事要旨

1. 日時

令和７年 10 月 14 日（火）10 時 00 分～12 時 00 分

2. 場所

赤坂グリーンクロス　４階会議室

3. 出席者

（委員）

猪俣　敦夫	大阪大学 D3 センター 教授 CISO【座長代理】
川北　陽司	独立行政法人情報処理推進機構（IPA） デジタル人材センター人材プロモーションサービス部 スキルトランスフォーメーショングループ サブグループリーダー
後藤　厚宏	情報セキュリティ大学院大学 教授【座長】
園田　道夫	国立研究開発法人情報通信研究機構（NICT） ナショナルサイバートレーニングセンター長
日暮　拓人	一般社団法人 人材サービス産業協議会 事務局長
平山　敏弘	情報経営イノベーション専門職大学（iU） 教授
和田　昭弘	全日本空輸株式会社デジタル改革推進室 専門部長

（事務局）

飯田　陽一	内閣サイバー官
木村　公彦	国家サイバー統括室統括官
関口　祐司	国家サイバー統括室審議官
中溝　和孝	国家サイバー統括室審議官
仙﨑　達治	国家サイバー統括室参事官

4. 議事録

（１） 開会

＜挨拶：飯田内閣サイバー官＞

おはようございます。内閣サイバー官の飯田です。検討会の開催にあたり、一言ご挨拶します。

我が国のサイバーセキュリティを取り巻く情勢は、非常に厳しい状況にあると考えています。官民ともに対応を強化していかなければなりませんが、それを支える最も重要なもの

が人材です。

また、AI などの進展を考えますと、サイバーセキュリティを担う人材に求められる役割や必要なスキルも、絶えず進化・変化していくものだと認識しております。政府としても、こうした動きにしっかりと対応していきたいと考えています。

本検討会では、サイバーセキュリティを担う人材に求められる役割、知識、スキルを定めた「人材フレームワーク」を策定するための検討をお願いします。

また、これを作成するだけでなく、官民の関係者の皆様がこれを活用し、一丸となって効果的かつ効率的に人材の育成・確保を行っていくための環境整備についても、ぜひご議論いただきたいと考えています。

フレームワークの策定自体はゴールではありません。これを具体的に社会の様々な場面で活用し、それを支える人材にとって魅力的な職場やキャリアパスを明確にしていくことが重要です。それが結果として、多くの優秀な人材がサイバーセキュリティに携わることにつながります。この点が非常に重要ですので、本検討会でもそうした活用場面を想定しながら、皆様にご議論いただきたいと思います。

この検討会は、できるだけオープンに進めたいと考えています。我々の議論が、サイバーセキュリティの関係者や、これからこの分野で活躍したいと願う方々に届くようにしたいです。あわせて、現にサイバーセキュリティに携わっている方々からのご意見も積極的に取り入れてまいります。

目安として、今年度内、来年３月までにフレームワークのコアをまとめたいと考えています。並行して、サイバーセキュリティ戦略の策定状況も見ながら、そこへ必要なインプットもしていきたい所存です。

大変タイトなスケジュールではありますが、フレームワークの策定やその利活用、そして最終的なサイバーセキュリティ人材の育成・確保について、手応えのある政策につながりますよう、委員の皆様には積極的かつ忌憚のないご意見をいただければと存じます。どうぞよろしくお願いいたします。

（２） 議事

(1) サイバーセキュリティ人材フレームワークに関する検討会について

事務局より、配布資料（資料１、資料２及び資料３）に基づき、本検討会の設置根拠、運営要領等について説明があった。

(2) 人材フレームワーク策定及び利活用等の基本的考え方（案）

事務局より、配布資料（資料４）に基づき、人材フレームワーク策定及び利活用等の基本的考え方（案）について説明があり、続く意見交換での発言内容は以下のとおり。

○ ITSS の話がありましたが、特に IPA が実施している情報処理安全確保支援士の資格講習

に注目しています。その講習では、スキルレベルが３から４に上がるあたりで、純粋な技術力だけでなく、いわゆる人と話せる力が評価のポイントになっています。例えば、ログを解析する技術力は当然として、その結果を経営者や上位者等に分かりやすく説明できる能力、つまり、俯瞰的に物事を捉え、それを端的に説明する能力が重視されているのです。

サイバーセキュリティの議論は、先ほどの米国の事例のように網羅的に扱おうとすると、どうしても技術的な詳細、いわゆるレイヤーの低い部分に注目が集まりがちです。

しかし、実際の活動において組織としての意思決定を進める上では、経営層などに対してきちんと説明し、理解と承認を得ることが不可欠です。したがって、そうしたコミュニケーション能力や説明能力の重要性を積極的に示していく必要があると感じています。

○　利活用の観点から意見を述べます。企業が本当に求めているのは、その技術スキルを持つことを前提とした上で、さらにプロジェクトをリードする力、マネジメント能力、あるいはベンダーと円滑にコミュニケーションを取る能力です。ベンダー側から見れば、顧客企業の上層部にしっかりと提案できるプレゼンテーション能力を持つ人材が求められています。しかし、そうした能力を持つ人材は育成が進んでおらず非常に少ないため、市場では取り合いになり、結果としてスキルと年収が上がっていくという構造が見られます。

したがいまして、このフレームワークにおいて、技術スキルを前提とした上で、マネジメント力やプレゼンテーション力といった能力をどう表現できるかが、一つの鍵になると考えています。その観点から、論点１の「レベル」設定においては、単なる技術スキルのレベル分けよりも、こうしたマネジメント能力などに応じたレベルを設定する方が、最終的な利活用、つまり実際の採用市場において、より効果的に機能するのではないかと感じています。

○　人材像の設定についてですが、日本には中小企業を含め多数の企業があり、多くがサイバーセキュリティを課題と認識しつつも、具体的な対策に苦慮しているのが実情です。そうした中で、活動の指針となるフレームワークを策定することは非常に重要な取組であり、ぜひ進めていきたいと考えています。

このフレームワークは、大企業だけでなく、40 万社ほど存在する中小企業、零細企業まで含めて 200 万社ほどとなりますが、このような企業に対して、幅広くセキュリティ意識を向上させるものでなければなりません。そのためには、既存の業務にプラスアルファの形でセキュリティへの取組が組み込まれるような、現場で実践しやすい形でなければ浸透は難しいでしょう。

例えば、専門職に対し、何をインプットすれば、組織全体のセキュリティが向上するのか。それが業務の一部として明確に定義されることが重要です。そして、そうした「業務にセキュリティを組み込む活動」を考案・推進できるサイバーセキュリティ人材と、それを現場で理解し実行する従業員の双方が機能することで、初めて企業のセキュリティレベルは向上します。サイバー攻撃の主な標的が企業である以上、こうした実践的な取組が不可欠です。

やはり「既存の業務に何をプラスするか」という形でセキュリティ要件が定義されている方が、企業にとっては受け入れやすいものです。

一方で、フォレンジック、捜査、脆弱性評価といった高度な専門家を必要とする企業も存在します。企業によってセキュリティレベル向上のために必要な専門性は異なります。

したがって、資料９ページにあるように、今回策定するサイバーセキュリティフレームワークを「軸」としつつ、各企業が自社の状況に応じて必要な部分を相互参照できる形が理想です。フレームワークができた後、「私たちの会社は、この部分を参照すればよい」とすぐに分かり、職場で活用できるとよいとのイメージを持ちましたので、発言させていただきました。

○　論点①、特にレベル設定についてコメントします。本日の事務局資料で、諸外国の事例ではレベル設定があるものとないものがあるとご説明いただきました。しかし、日本ではITSS（IT スキル標準）が非常に広く使われているという実態がありますので、まずレベルの定義は設けるべきだと考えます。

一方で、まだ先の議論かもしれませんが、資料 18 ページのレベルの「見え方」について懸念があります。これは純粋に表記に関するコメントですが、提示された案ではレベルが０から始まっているようにお見受けします。しかし、ITSS をはじめ日本で使われている多くの標準は１から始まっています。

おそらく、この案のレベル０～３は、ITSS などのレベル１～４に相当するものと読み替えて理解しましたが、このように既存の枠組みと表記が異なると、一見した際に誤解を招く可能性があるのではないかと直感的に感じました。

したがって、レベルの中身もさることながら、その見せ方についても、既存の枠組みと平仄を合わせ、表記や粒度感を統一していくべきではないかと考えます。

○　皆様のお話を聞き、「人材像」という言葉を使うことの弊害について考えました。例えば、米国の NICE フレームワークは個々のワークロールが細かく定義されていますが、これは見方を変えれば、複数のワークロールを組み合わせることで、多様な人材を柔軟に表現できるという利点があります。つまり、個々のスキル要素の組み合わせで人材を捉えやすい構造になっています。

これに対し、もし我々のフレームワークが固定的な「人材像」を定義してしまうと、どうしても「その定義に完璧に合致すること」が目標となり、画一的な人材育成につながる懸念があります。

日本人は真面目な気質から、フレームワークで定義された要素を一つ一つ満たすことに注力し、かえって視野が狭くなってしまうかもしれません。しかし実際には、定義された範囲を少しはみ出すようなスキルを持つ人材こそが、様々な場面で活躍し得るのではないでしょうか。例えば、フォレンジックと捜査のスキルは、両方を併せ持つ人材が求められる場

面もあります。そのため、最終的な成果物の公表やプロモーションの段階で、こうした柔軟性や多様性の重要性を伝え、複数のスキル要素を組み合わせることの価値を伝えるような工夫が必要だと考えます。そうしなければ、このフレームワークは画一的で使いにくいものになってしまうのではないかと感じました。

○　技術的な詳細レベルではなく、「人間力」や「コミュニケーションの能力」をどのように捉えるかという点について、事務局のご意見を伺いたいです。事務局案にある「練度」というキーワードは、これらの能力を包含するものなのでしょうか。それとも異なる概念でしょうか。

○　【事務局回答】後の資料を見ていただくと分かるように、内容はスキルに寄っているかもしれません。他方、レベルが上がるにつれて、求められる非スキル要素の度合いが高まっていくというイメージです。

例えば、資料 18 ページのレベル２や３の定義には、「他者に対して説明・指導ができる」といった記述が含まれており、ご指摘の能力を薄くではありますが意識しています。しかし、今いただいたご意見を踏まえると、これらの要素をより明確に打ち出すべきだと感じました。特にレベル３につながると考えています。

○　つまり、概念としては取り組んでいるものの、それをさらに強く打ち出すべきかどうかが今後の議論のポイントですね。承知いたしました。

私個人の観点からは、このフレームワークの「位置づけ」が非常に重要だと考えています。９ページ目にもありますが、国内で様々なフレームワークに関する活動が活性化するのは望ましいことですが、その際に「これは我々のフレームワークのどの部分に対応するのか」という共通言語、つまり目安が必要です。例えば EU のフレームワークは米国の NICE フレームワークに細かく紐づけて分析されていますし、ISC2 のような国際的な業界団体も同様の傾向にあります。したがって、我々も NICE を一つの軸として対応づけを考えるのは正しい方向性だと思います。

ただ、ここで議論になるのは、「NICE は細かすぎないか」という点です。活用しやすさを重視するならば、土台となるフレームワークをあまりに厳密に規定しすぎると、かえって使いづらくなり、融通が利かなくなる恐れがあります。このあたりは経験豊富な委員の皆様も実感されているかと思います。したがって、「共通言語として理解はできるが、細かく縛りすぎない」という、絶妙な落としどころを見つける必要があるでしょう。

さらに、フレームワークを作るだけでなく、活用の手引書や具体的な活用事例を増やしていく活動も並行して行うべきです。例えば、まず政府機関が率先して活用事例を公開すれば、民間企業も「それなら我々も似たようにできる」と、良い参考になるはずです。その際、先ほど述べた「縛りすぎない」フレームワークが、柔軟な活用を促す上で良い落としどころに

なると思います。

○　当然この会は、サイバーセキュリティ人材ということで話しておりますが、もう少し俯瞰して、DX 人材など、俯瞰してみた上で、その中でのセキュリティ人材の重要性を考えるのが良いのではないでしょう。

○　【事務局回答】今日も ITSS などの話も、いろいろな方からいただいておりますので、ぜひ我々も俯瞰して見て心掛けていきたいと思っております。

○　まずこの取組に当たっては、我が国の全体方針や共通理念に沿った議論を進めていくことが重要です。また、今の委員のご質疑とも被るかと思いますが、テクニカルに寄っている感がありますけれども、まずはそのテクニカル面を重視して、第一版というか、初版は策定いただければ良いかと思います。ノームハッキングやマインドハッキングのような、そういったところも考慮する必要があるのではないでしょうか。それから、組織について、メンバーシップ型組織において専門家に活用してもらうためのマネジメントの観点や、あるいは逆に、私としては、これ自身、どちらかというと個人に着目して作っているかと思いますが、個人としてのフレームワークとは別に、チームとしてのロールを意識したフレームワークといったものがあってもよいのではないでしょうか。

○　このフレームワークは、策定の目的や想定する利用者をわかるようにすべきです。

○　【事務局回答】後ろのページで図化したようなものをお示ししておりますので、大体このような人をイメージしているというところは、やっているつもりではありますが、そのあたりはしっかりしていきたいと思います。

○　人材像の設定について、いわゆる「名は体を表す」ではありませんが、つけたネーミングとやっている仕事が、はっきり分かるようにしてほしいです。それから、人材について、雇う側と雇われる側、育てる側と育てられる側といった双方があると思いますが、片務的ということではなく、共創的でなければならないのではないでしょうか。また、企業側が欲しい人材と、人材側がなりたい人材にギャップがあるのであれば、そういったところを調べる必要があるのではないでしょうか。また、これは委員の皆様のご意見と被りますが、やはり、技術的なスキルだけでなく、コミュニケーションやプレゼンテーションスキルについても考慮があると良いです。

○　人材像の粒度やレベル設定については、提示いただいたものぐらいが限界であり、数としてはこれ以上増やさないほうがよいかと思います。また、相互参照性について、複数の委

員からのご意見のとおり、この新しく作るフレームワークで細々なところまで決めるのではなく、例えば知識については SecBoK があるので、そこに紐づけるのはどうでしょうか。

○ 海外との相互参照という点について、国内外、特に海外でフレームワークを策定している団体等との間で協議等が進んでいるのでしょうか。

○ 海外からも参照されることを目標にしたいです。

○ 性質に関わる点で、事例についてです。そういった事例をやはり手引書に書いてはどうでしょうか。

○ 大企業や中小企業をイメージしたときの役割の割り振りや、インソース、いわゆる直営でやるか、アウトソースするかという点の参考にできるようになると良いです。

○ 利活用についてですが、キャリアパス、キャリアプランといったものを示せると良いです。あるいは、このフレームワークを作った後のプロモーションが大切です。

○ 人材像の呼び方について、人材像なのかロールなのかを、いずれにしても明らかにしないと混乱してしまう可能性があります。

○ 同じく人材像の呼び方について、人材像で良いのではないでしょうか。

○ 同じく人材像の呼び方について、機能や役割の方が日本では受け入れられやすいのではないでしょうか。

(3) 人材像の設定（案）

事務局より、配布資料（資料４）に基づき、人材像の設定（案）について説明があり、続く意見交換での発言内容は以下のとおり。

○ 昨今のインシデントを見て、日本はインシデント対応に非常に脆弱だと感じています。これまで、いわゆるディフェンス、つまり常時監視といった対策には力を入れてきました。しかし、ランサムウェアのような非常にシンプルな攻撃によって、甚大な被害を受けています。

その背景には、事故が起きても、毎日のニュースで見ているにもかかわらず、それを他人事として捉え、「自分ごと」になっていないという問題があります。誰もが攻撃を受けることを前提として、対策に取り組む必要があります。

その上で、先ほど注目されていた「対処」が極めて重要になります。本当にインシデントが起きたとき、社長や経営者といったトップがいかに即座に先頭を切ってリーダーシップを発揮できるかが問われます。情報セキュリティマネジメントシステム ISMS にも書かれているように、これは技術ではなくリーダーシップの問題です。しかし、その部分を安易に外部委託に任せようとする傾向があります。私たちは、「オフェンシブセキュリティ」という言葉もありますが、インシデントが起きることを前提とした視点で人材を育成していかなければなりません。ここが日本の本当に弱い部分だと感じます。

そして、先ほどの既存のフレームワーク類との相互参照性の確保に関連して、一つ参考になるのが、ISC2 の CISSP における知識体系（CBK）と、その中にある 8 つのドメインという考え方です。この 8 つのドメインは世界的な標準であり、米国や英国、その他の国でも通用するため、これをベースにした内容は国際的にも通用します。その中では「対処」についても定義されています。

これを完全に模倣するのではなく、参考にしつつ、日本の組織や文化に合わせて変換する形で記述していけば、先ほどお話のあった「たすきがけ」のような相互参照が即座に可能になるのではないかと考えています。

○　各人材像と役割について、不足があるかどうかという点で、現状の案は非常に網羅的にカバーされていると感じています。しかしその一方で、「開発」などの掘り下げ方に少し気になる点があります。

NICE フレームワークでは、「アーキテクチャ」というワークロールの中で「開発」が定義され、設計や改善可能性といった業務が説明されています。これに対し、本フレームワークの案には、新しいものを創造し、世の中にないもので課題解決を図る、あるいは発明するといった、創造的な人材の要素が欠けているように感じます。

今までに存在しないものを創り出し、世の中の課題解決に貢献するような人材像を示すべきだと考えます。それが独立した人材像になるか、既存の定義に説明を加える形になるかは検討が必要ですが、その視点が抜けている点が気になりました。

もう一点、同様の観点からですが、サイバーセキュリティの重要性を「啓発する」人材も必要です。現在は行政がその役割を担うことが多いですが、それだけでは限界があります。啓発コンテンツを作成するなど、現実に即した活動を行う役割や機能も、フレームワークのどこかに定義されると良いでしょう。

そうした人材がいれば、このフレームワークが現場でどのように活用されるかを具体的なストーリーとして描くことができ、手引書以上のプラスアルファの価値を持つ活用例を示せるようになります。そのような人材という視点も盛り込めると良いと考えます。

○サイバーセキュリティの課題は「他人事」と捉えたり、「自分の仕事ではない」とシステム担当者に任せきりにしたりする、いわゆる「マインドセット」に起因する脆弱性が大きい

と感じています。
一方で、ご提示いただいたフレームワーク案を拝見しますと、主に「スキルセット」を中心に構成されているとお見受けしました。そこでご提案ですが、特定の人材像に限定するのではなく、全ての役割に共通する横串の要素として、この「マインドセット」を定義してはいかがでしょうか。
DX においても、多くの方が「自分は関係ない」という他人事の姿勢であり、まずはそのマインドを醸成することから始めています。サイバーセキュリティにおいても同様に、このフレームワークの中に、そうした当事者意識を持つためのマインドセットに関する定義を加えていただけると、非常に効果的だと考えます。

○ 既存のフレームワーク類との相互参照性の確保について、このフレームワークをハブとして参照先として機能させるにあたり、リスキリングサービスとして活用したり、各企業が教育・採用に活用しやすくしたりするためには、まず「ハブとなる新フレームワーク」と「参照先となる国内の既存フレームワーク」との役割分担を明確に定義することが重要ではないかと認識しています。
一般企業が求めるニーズと、SIer やセキュリティベンダーといったサービス提供側が求める人材像やスキルセットは異なります。さらに、それは大手企業と中小企業とでも異なります。例えば、「大手／中小」と「ベンダー／一般企業」を縦横の軸として４象限で整理してみると、それぞれの立場で求められる要件の違いが明確になるのではないでしょうか。
このように、立場によるニーズの違いと、ハブと参照先の位置づけを整理することで、ハブとなるべきこのフレームワークで「何を定義するのが最適か」が定まりやすくなると感じました。

○ 企業や立場によって求められる人材やスキルレベルは異なります。新しい法律ができても、一企業だけではサイバーディフェンスは完結しません。ですから、このハブの中で「自社の立ち位置はここだ」ということが見えてくるようになれば良いです。
大企業と中小企業でできることとできないことがある点、またアメリカと日本の企業文化の大きな違いは考慮すべきです。関連人材を全て自社で抱える米国企業と、アウトソースを活用する日本企業とでは、求められる人材要件が大きく異なります。
こうした状況を踏まえると、やはり意思決定や戦略策定を担う層が重要になります。トップである経営層はもちろんですが、その次の層、つまり意思決定をサポートする人材が極めて重要です。それは企業の組織によって、IT 部門、総務部門、企画部門など様々でしょう。
そのような企業の方々が、自社のサイバーセキュリティをどのように進めていくかという全体像を描けるよう、具体的な事例を交えながら指針を示すことができれば、議論は大きく進展するのではないでしょうか。

○　14 ページの図に示された 15 の分類について、具体的な視点から申し上げると、この分類の中身はまだまだ練る必要があると感じています。

一つは、先ほど他の委員からご指摘のあった「対処」の点です。経営層も含めた対処能力を考えると、これはレジリエンスの話になります。米国エグゼクティブ向けの" Cyber Resilience by Design: The Executive's Guide to Managing a Cyberattack "という本では社長がどうあるべきか、対処の項目として「顧問弁護士がサイバーインシデントに強いか確認せよ」という点から始まっています。さらに、広報・マスコミ戦略をどうするかといった内容が続き、それを分解して部下に役割を担わせているか、という点がガイドブックに書かれています。そこまでを含めた「対処」だと考えると、現在の案とは相当イメージが異なってきます。

次に、他の委員からご指摘のあった「開発」についてです。14 ページの図では「開発」が右下にありますが、重要インフラ事業者における開発をアーキテクチャの観点から考えると、これは「①経営判断」の横に位置すべきものです。電力会社や通信会社において、システムのセキュリティ設計はどうあるべきか。BCP や地政学リスクまで含めたアーキテクチャがあり、それを分解していくのが本来の姿です。しかし、この図では「開発」が最終工程のコーディング担当者のように描かれてしまっています。実際、NICE フレームワークではサイバーセキュリティアーキテクチャやエンタープライズアーキテクチャが冒頭に来ており、その点の感覚がずれていると感じます。

もう１つ細かい点ですが、NICE フレームワークの５つのカテゴリーに対応させていますが、実はこれは最新版の構成です。初版には「サイバースペースインテリジェンス」と「サイバースペースエフェクト」が含まれていました。これらは国防用語であったため NICE から別のフレームワークに移管されましたが、米国としてはその概念を保持しています。日本において、特に OSINT 能力を含む「サイバースペースインテリジェンス」を除外し、「情報収集・分析・共有」の項目に含めるだけで良いのか、このあたりも再検討すべきだと考えます。このように、15 の分類の中身はまだ議論の余地があると思います。

とは言いつつも、私はこの 14 ページの図自体は非常によいと考えています。なぜなら、今回の新法案で最も重視されている「官民連携」を端的に表しているからです。政府機関と重要インフラ事業者が、どのような人材と能力を発揮し合って対処していくのかを、この図を基に具体的に議論できます。この事例に合わせた分析は非常に価値があります。

さらに、リボルビングドア、つまり官民の人材交流の際にも、どのような人材が行き来するのかという議論にこのフレームワークが活用できるため、非常に良い実例です。

したがって、細かい中身は議論していくべきですが、この実例を軸に詳細を詰めていくことは非常に有効です。その検討結果を提示することで、民間側は「それなら自社ではこう解釈できる」と応用でき、事案対処省庁も「これは参考になる」と活用する可能性があります。ですから、このページを徹底的に議論していくことが非常に有益ではないかと考えます。これに合わせて 15 の分類を見直し、それが実例と合っているか、政府と重要インフラ事業者の連携がこれでうまくいくか、という点を確認することが有益です。

○ NICE フレームワークの細かさについてです。確かに非常に細かく、それが使いづらさにつながるというイメージがありますが、背景には、アメリカやオーストラリアで自動化が進んでいるという現状があります。オペレーションレベルのタスクは自動化や標準化によって人材不足がシステムで補われており、その一方で、意思決定に近い層の人材は相変わらず不足しています。ただ、その層に関しても CISO に関する書籍が多数出版されるなど、広範なタスクやミッションに言及したコンテンツが充実しています。

そうした視点で NICE フレームワークのワークロールを見ると、「この部分は自動化できそうだ」「ここは生成 AI で代替できるかもしれない」といった点が比較的わかりやすい構造になっています。

これに対し、今回ご提示いただいた人材像の役割説明では、そのあたりが少し曖昧で、どこに自動化などの新しい技術を組み込む余地があるのかが見えづらいと感じました。

NICE をそのまま模倣することが正解とは思いませんが、私たちのフレームワークも、「将来的には生成 AI に置き換わる可能性のある部分」や、「生産性向上によって重要度が相対的に下がる役割」といった将来の変化を意識できるような説明になっていると、より良いものになるのではないでしょうか。

○ 人材フレームワークについて他の団体と同様、我々日本ではボランティア精神による活動を行っていますが、各国は国を挙げて人材フレームワークを策定しており、国内の既存フレームワーク類がなかなか対抗できないと感じていました。

そうした中、今回 NCO が国としてこのような形で人材フレームワークの策定を表明してくださったことで、ぜひとも日本としてのしっかりとした人材フレームワークをこの委員会を通じて作っていきたいと強く望んでいます。

そして、これまでは NICE など海外のフレームワークを参照して日本のものを作る、という流れが人材に関して続いていましたが、今回は、日本が作った人材フレームワークを各国が参照してくれるようなものを作っていきたいという思いがあります。

議論になっている NICE フレームワークは非常に細かいため、それをどう整理・集約するかが重要です。しかし、集約しすぎて分かりにくくなっては本末転倒です。その点で、今回ご提示いただいた 15 分類は、ある程度良い組み合わせになっていると感じます。

ただ、この 15 分類の中にも、セキュリティのコアの凄い人材と、いわゆる「プラス・セキュリティ」人材的なところとでは、いくつか重さが変わってくると思います。その違いを、どのように皆さんに分かりやすく示していくかが今後の課題だと考えています。

○ 今のお話にあったように、国としてこのフレームワークにしっかり責任を持つという姿勢を、ぜひ発信いただきたいです。実際にセキュリティの世界は常に変化しており、NICE にしてもバージョンアップを重ねています。このフレームワークも、NCO が直接関わるか

は別として、その旗振りのもとで、継続的に維持・管理し、発展させていく仕組みづくりについても、ぜひ検討いただければと思います。

○　1から15の人材像はフラットではなく濃淡や色分けがあり、「エンジニアリング系」と「マネジメント系」のように性質が異なるため、同じグループとして扱うのではなく、緩いカテゴライズをすると分かりやすくなるのではないでしょうか。

○　15の分類については、総論として汎用性があり妥当な設定であるとしつつ、どのような定義や設定をしても不足は生じるため、むしろその不足を補うためのカスタマイズ方法などを手引書で示すべきではないでしょうか。また、資料18ページに記載の大企業と中小企業におけるレベル３の調整については、無理に行う必要はないのではないでしょうか高度な人材像の設定については、過度に追求すると迷走する可能性もあるため、別途検討とすることで良いのではないでしょうか。中小企業やサプライチェーンにおける兼務の実態、例えば役割３、８、９ですけれども、こちらについては、現実的な兼務例をガイドラインなどで提示するのは効果的ではないでしょうか。一方で、職責分離の原則に反するような兼務は不可である旨も、ガイドラインなどで謳うべきです。

○　このフレームワークでプラス・セキュリティまで取り扱うことについては、経済産業省が進めるデジタルスキル標準など、他の取組と連携していくのが良いのではないでしょうか。

(4) 今後のスケジュール

事務局より、配布資料（資料５）に基づき、今後のスケジュールについて説明があり、続く意見交換での発言内容は以下のとおり。

○　具体的には、パブリックコメントの期間はどのようになりますか。

○　【事務局回答】第３回と第４回の間に、任意のパブリックコメントを実施し、広くご意見を伺いたいと考えております。

○　パブリックコメントの対象はフレームワーク本体で、手引書は並行して検討を進める、という整理でしょうか。手引書を作成する方針そのものについては、パブリックコメントの際に明示していく、という理解でよろしいですか。

○　【事務局回答】狭義のフレームワークだけでは機械的な印象になってしまうため、その対象範囲や前書きなども含め、見せ方を工夫したいと考えております。

（３） 閉会

＜挨拶：木村統括官＞

統括官の木村です。本日は初回から非常に熱心にご議論いただき、また、多くの重要なご指摘をいただきましたこと、改めて御礼申し上げます。

冒頭にもお話がありましたが、政府内では現在、年内の策定を目指して新しいサイバーセキュリティ戦略に関する議論を別の場で進めております。本検討会でいただいたご議論も、その戦略にしっかりと盛り込めるよう、事務方として取り組んでまいります。

本検討会の検討状況は、冒頭に飯田サイバー官からも話があったように、できる限りオープンに進めてまいります。ご議論にもあったとおり、様々な場面で多くの方々にご活用いただけるようなものに作り込んでいく必要があると考えています。その意味で、先ほどのスケジュールにもありましたように、サイバーセキュリティに関わる様々なお立場の方々のご意見をヒアリングの形で積極的に取り入れ、検討をさらに深めていければと考えております。

今回の主たる議題は人材フレームワークの策定ですが、それをいかに利活用していただくか、という点も重要です。手引書に関するお話もありましたが、そうした点もしっかりと議論していただくとともに、我々も議論を深めていきたいと考えております。また、このフレームワークは一度作って終わりではなく、状況に応じて発展させていくべきものです。そのことを念頭に置きながら、議論を進めていければと考えております。

委員の皆様におかれましては、引き続きご指導を賜りますようお願い申し上げます。簡単ではございますが、閉会のご挨拶とさせていただきます。引き続きよろしくお願いいたします。

以上