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４回）議事要旨

1. 日時

令和８年３月 27 日（金）14 時 30 分から 16 時 30 分

2. 場所

赤坂グリーンクロス　４階会議室

3. 出席者

（委員）

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
西本　逸郎	株式会社ラック 技術顧問
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
松本　哲也	パナソニックホールディングス株式会社
吉岡　克成	横浜国立大学大学院環境情報研究院/ 先端科学高等研究院 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
斉田　幸雄	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＞

内閣サイバー官の飯田です。開会にあたりまして一言ご挨拶を申し上げます。委員の皆様におかれましては、年度末のご多忙のところ、本検討会にご参加いただきまして誠にありがとうございます。

サイバー攻撃は日々高度化・巧妙化しており、これに対応できる人材の確保・育成が、我が国にとって重要な政策課題となっています。このため、昨年 10 月に本検討会を設置し、サイバーセキュリティ人材に求められる役割や技能を整理した人材フレームワークと、その活用方法を示した手引き書の策定について、委員の皆様に熱心にご議論いただいてまいりました。

本日はいよいよ取りまとめの議論となります。また、２月 17 日から約３週間、フレームワーク案のパブリックコメントを行ったところですが、非常に多くのご意見をいただきました。これらを本日の取りまとめにどのように反映するかについても、ぜひ委員の皆様のご意見を伺いたいと思います。

このフレームワーク、そして手引き書により、各組織におけるサイバーセキュリティ人材の定義が明確になりますので、採用や配置の適正化、教育・訓練のミスマッチの解消、育成すべき重点分野の把握が容易になるものと期待しています。ただし、このフレームワークや手引き書は、策定すれば終わりということではなく、あくまでも出発点ですので、本日の会合では、フレームワークを今後の社会の様々な場面で活用していただくための具体的な方向性や課題についても、ぜひご議論いただきたいと考えており、それをもって今後の取組につなげてまいりたいと考えています。

サイバーセキュリティ人材の確保・育成に向けて、本日も活発なご意見をお願いいたします。どうぞよろしくお願いいたします。ありがとうございました。

（２） 議事

(1) パブリックコメントの実施結果及び対応（案）について

事務局より、配付資料（資料１）に基づき、パブリックコメントの実施結果及び対応（案）について説明があり、座長から各委員に対して意見を求めた。主な発言は以下のとおり。

○ 最後のレベル３、４のところを、エキスパートという言い方で、テクニカルなスキルの突出した方と、マネジメントという形に分けた案を出していただいた。詳細を詰めすぎても際限がないため、まずはこの形で運用を開始するのが適切ではないかと考えます。

パブリックコメントの中で気になったのは、特にテクニカルの方に関して、経験年数が少ないにもかかわらず、才能がある人を適切に評価・登用するための方策が求められていたこと。この点は非常に難しい論点ではありますが、例えば、実際に、中高生の頃から優れた才能を発揮している人材は少なからず存在します。そうした人材をどのように評価するかについて、今回反映するかどうかも含めて、少し気になるところではあったと思いました。

特に、レベル３が４年から 10 年、レベル４は 10 年以上となっていることに違和感を覚

える方もおり、年数を明示すべきかどうかについて数件のコメントが寄せられておりました。そのあたりが少し今、気になったというところです。

○　今回、パブリックコメントの後の取組本当に大変だったと思います。
　年数で区切ることへの懸念は理解できますが、セキュリティは「三場」（火事場、修羅場、土壇場）に「ロック」（ベースとして経営者の揺るぎない意思）とも言われており、このような場面を経験して、本当に実力がついていくほか、本当にベストプラクティスをその場で出せるとか、いうようなところがあるので、経験の蓄積は非常に重要であると考えられます。
　ただ、最近の優秀な若い方々は、シミュレーション的に次々とされているので、一概には言えないところもあります。それでよいのであれば、こちらの方には「相当」ということが書かれているので、「相当する」という表現を用い、見識のある方が判断する運用は、現実的であると考えます。

事務局
○　パブリックコメントを踏まえて、やはり年数を固定的に記載していた点は、まさにおっしゃるようなところで「相当する」という表現に、少し語尾を変えさせていただきます。

○　10 年分に相当する経験を３年程度で積むような優秀な人材も存在し得るという理解でおります。

○　今の論点ですが、例えばレベル４-E というところを見ると、条件として「下記３点のうち２点以上を満たす者」と書かれています。そのうちの②のところで、「コミュニティ活動や対外情報発信等」という文言があります。このあたりを推進する、あるいは推奨するというところで、その才能を捉えるといったものに置き換えられるのではないかと感じました。その点もよく考慮されており、肯定的に評価いたします。

○　まず、現在議論となっているレベルについて、P.３に出ているところですが、私のイメージとしては、レベル３とレベル４の間でエキスパート（E）とマネジメント（M）に分かれているのがよいのではないかと思います。レベル３は独力で業務を遂行できる一人前の段階であるため、この段階で M と E を明確に分けることには疑問があります。レベル３は点線による区分にとどめ、レベル４で明確に E と M に分岐する形が、実践的なイメージの分け方として、一人前になるまでは M と E の両方の素養を備えていることが望ましいと考えます。これが１点目です。
　次に、パブリックコメントを拝見して、SecBoK との関連やプラス・セキュリティに関するご意見が多かった点です。SecBoK だけでなく、様々なフレームワークが存在する中で、今回このサイバーセキュリティ人材フレームワークを NCO として出す際に、既存のフレー

ムワークと連携しているという回答はいただいていますが、オールジャパンで取り組んでいるという点を効果的に発信しながら推進していただきたいというのが２点目です。

また、プラス・セキュリティの件に関しましては、SecBoK でも同様ですが、今回の人材フレームワークで示されている開発やプロジェクト管理といった役割については、プラス・セキュリティでもレベル１、２、３と分けており、レベル３の高い人はこちらのセキュリティ人材にも該当する部分があります。そういった点に関連しており、その下のレベルについても人材フレームワークや手引き書で触れられております。専門家だけでなく、DX 等を推進するうえで必要な人材としてのプラス・セキュリティも考慮していること、また 13 の役割との関連性がある旨の回答をいただいた点について、フレームワーク公表時に効果的に発信していただきたいと考えます。

○　私もオールジャパンというのは非常に重要なメッセージだと思います。新たなフレームワークが単に追加されたという印象を与えないよう、ぜひご留意いただきたいと思います。

それから、先ほどの「コミュニティ活動や対外情報発信」のところですが、ここは実務的にも重要だと思っています。非常に高いテクニカルスキルがある人が組織外との交流を持たない場合にリスクが生じる可能性があり、そうした方が適切なコミュニティに参加し、自身のスキルを堂々と発信できることが、健全な形で活躍していただくうえで重要だと考えます。このように、社会と適切にコミュニケーションがとれる方で、かつスキルがある方というのはまことに好ましいと私も思っております。

○　今回 P.３で、マネジメント系とエキスパート系に分けられたという点ですが、IPA が公表しております「デジタルスキル標準」におきましても、同じような粒度感、すなわちサイバーセキュリティの領域ですと、サイバーセキュリティマネージャーとサイバーセキュリティエンジニアという、この２つで同じ粒度感で分けておりますので、親和性が高いと考えております。

また、パブリックコメントや委員の皆様から出ておりますが、年数のところについては非常に難しいと思っております。ただ、パブリックコメントで意見をくださっている、特に年数のところを懸念されている方というのは、とりわけ最前線で活動されている現場の方からのご意見が多いと思われますが、このフレームワークが使われる場面という意味でいうと、当然現場の方もお使いになると思いますが、人事の方、いわゆる人的資源管理等をされる方も当然お使いになるかと思います。その場合、定義が定性的なものだけでは実際の運用が難しくなる可能性もありますので、年数という考え方もやはりある程度あった方が、実際使われる場面、使う側の観点としては、必要かと思いますので、この形で差し支えないと考えております。

○　私はユーザー企業におりますけれども、ユーザー企業においても、人事制度上ではエキスパート系とマネジメント系が同等のランクで分かれておりますので、企業から見て非常に分かりやすい構成であると考えております。

○　現在の定義の箇所への検討になりますが、人材仲介の立場から見ましても、このエキスパート的な分け方とマネジメントという分け方は、実際の募集や採用要件を決めたいというときにも、確認・調整する要素でもありますので、この分け方は非常に明快であると感じました。

また、先ほどお話もありましたとおり、企業側としても人事等が目安に使うというのもありますが、個人の側が目指すときに、マネジメントの道しか示されていないと受け取られてしまう懸念がありますので、この２つに分かれていることは、個人にとっても意義のある構成になったと考えます。加えて、そのスペシャリティを高めていったら、マネジメントのトップクラスと同等に位置づけられるという見せ方も非常に重要であり、人材の育成という観点からも、非常に重要な分け方であったと捉えています。

○　研究者等についても同様ですが、専門分野で、例えばペネトレーションでかなり極めると、一つの専門分野を極めた後、別の分野に移って新たな専門性を磨いていくことがあり、そうした経験を通じて技術者としての視野の広さが養われるため、そうした複数分野にわたる専門性について、何らかの位置づけがあるとよいと考えます。

○　専門性の幅ですね、面積が広くなるという印象でしょうか。現時点で適切な表現を定めることは容易ではありませんが、次回以降の発展形において考慮していきたいと思います。

○　パブリックコメントを踏まえた改訂、ありがとうございます。レベル３、４がマネジメント系とエキスパート系に分かれたことで、非常にわかりやすくなりました。企業の立場からも活用しやすい構成であると考えます。ありがとうございます。

○　非常に好評なコメントをいただけたと思います。

この後、取りまとめの話にもなるかもしれませんが、本日の議論で次のバージョンという言い方が出でているとおり、事務局には、このフレームワークを不断に見直し続けることをお願いしているところです。そういう意味で、本フレームワークをバージョン 1.0 や、人材フレームワーク 2026 と呼称して、次のバージョンが予定されていることを示すのはいかがでしょうか。NICE 等でも、バージョン 1.0、2.0 というのもあれば、年数を入れるものもあります。そういう形で出すと、次があるのだなという印象を持たれるかと思いました。この辺りの打ち出し方について、ご見解をいただければと思いました。

事務局
○　ありがとうございます。その点については、公表する際に、バージョン番号が低いと未完成な印象を与える可能性があるため、あえてバージョン番号を明示しないという方法もあると考えておりました。そこは例えば 2026 とする等になるかと思います。

○　バージョン番号や年が出ていると、引用する側でも、例えば、自分の会社は 2026 版をベースに社内基準を作った等の言い方もしやすいと思いますので、区分けができると非常に良いという気がいたします。

○　このフレームワークは、既に出ましたように、今後公表に向けて最終の調整をしていただくということで理解しております。今日いただいた意見は、ほぼサポーティブな意見ばかりでしたので、本体については大体このとおりで良いという気がいたします。
　そのうえで、説明の仕方ですね。このフレームワークを出しましたということを、うまくアピールしていただくことを願いしたいのと、今後見直しや運用を積極的に推進していく姿勢を示していただけると良いと考えております。そういうことを含めまして、事務局で整理を進めていただければと思いますが、よろしいでしょうか。

(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
　事務局より、配付資料（資料２）に基づき、(2)　人材フレームワーク及び手引き書の取りまとめ（案）について説明があり、座長から各委員に対して意見を求めた。主な発言は以下のとおり。

○　今の資料の P.４の対応表は非常に重要だと思います。対応表の詳細は個別に確認するとして、このスライドを示すだけでなく、より丁寧に説明する機会を今後設けていただくとよいと思いました。特に、来年度は、このフレームワークや手引き書に基づく啓発活動等が期待されますが、その際に P.３や P.４を用いて適切に説明し、このような使い方をするとよい、詳しくはこちらを参照してほしい、といった取組をぜひお願いしたいと考えております。特に、組織の話と個人の話が交差する部分が非常に重要だと思いますので、その点に関してぜひ期待したいと考えております。

○　今の発言と、ほぼ同じことを言おうと思っておりました。この一覧をまとめていただいたのは素晴らしいです。さらにもう一歩踏み込んで、このような立場の人はこのフレームワークや手引き書をどう読んで、どう活用してもらいたいかという、普及活動の方に入るかもしれませんが、もう一歩歩み寄るようなメッセージ性があると素晴らしいと思いました。
　というのも、現在私は大学におりますので、大学や大学院を卒業・修了して就職活動を行

っている学生もおりますが、セキュリティの研究室にいても、自分のスキルや持っている知識を社会にどう生かしていけるのか、どういうところにニーズがあるのかも含めて、よく分かっていないという学生が非常に多くいます。このような国としてのフレームワークができて、社会から非常に求められていることや、どのようにキャリアアップしていけばよいのかという指針があることは、素晴らしいことだと思っています。

その際、教育機関向けの表を見ると、三角と丸がついており、すべてが対象であるため、すべて読むようにということだとは思いますが、もう少し学生に強く刺さるというか、社会から求められており、自分はこの分野を選びたいという気持ちを導けるような内容があると、非常に素晴らしいと思いました。フレームワークの中でそこまで行うのは難しいかもしれませんが、普及や啓発も含めて、つながるような内容になっていると素晴らしいと思いました。

○ 今の話にも絡むところですが、例えばマネジメント層の◎というところがあり、そこに読んでいただきたいという意図があると思います。例えば、大規模組織向けの P. 6 で言うと、これは経済産業省の「サイバーセキュリティ体制構築・人材確保の手引き」や「サイバーセキュリティ経営ガイドライン」のようなものに絡んでくるため、そこで経営者に読んでほしいという点についてはよいと思います。

一方で、私自身が例えばプラス・セキュリティ人材を広めようとしたときに、様々な企業や区役所等の行政機関の方とお話しすると、IT やセキュリティ分野の方にはその重要性を理解していただけます。しかし、プラス・セキュリティが対象とするのは、IT やセキュリティの専門分野ではなく、ユーザー部門や事業部門の方々です。そういった方々にプラス・セキュリティ人材を育成してほしいとお話しすると、重要性は分かるものの、結局は人事制度や評価に関わってくるため、IT やセキュリティ部門だけでは広められないという話になります。したがって、プラス・セキュリティを広めようとすると、やはり経営者の方にお伝えし、人事評価制度等も絡めて評価していただく必要があります。現状では、ただ現場でセキュリティに詳しい便利な人で終わってしまっているところを、適切に評価する仕組みが必要です。そのため、この表においても、経営層やマネジメント層、例えば人事や総務の方々にも見ていただきたいということが分かるような表にしていただけるとありがたいと思いました。これが 1 点目です。

また、私自身はプラス・セキュリティ研究所というところで、専門のセキュリティ専門家を育てるというよりも、プラス・セキュリティを教育しています。セキュリティや IT 分野に進もうとする学生だけではありませんが、一般的な企業に就職した際に、何を勉強しているのかと聞かれて「セキュリティをやっています」と答えると、意外と評判が良く、興味を持って聞いてくれることが多いようです。そういった点も含めて、専門家を目指す方だけでなく、セキュリティを学べば、セキュリティ分野に進まなくてもどのような場面で活用できるのかという視点が、企業側にとっても気になる部分です。そのため、この表の丸の付け方

等についても、そういった点を意識していただけるとありがたいと思います。

○　ありがとうございます。今おっしゃった後半のお話には、私も大賛成です。セキュリティの学科ではない学生向けに、セキュリティを勉強しておくと就職に有利であるというアピールがあってもよいと思います。また、人事や採用担当の方に向けては、そういった人材を採用すれば、プラス・セキュリティ人材として会社全体にとって有利になるというアピールがあるとよいと思いました。そういう意味では、この表の右下の部分ですかね。学生のプラス・セキュリティについては、法学部や商学部、経済学部の方々に対しても、これをやっておくとよいということが、丸のところに表現されているとよいと思います。

事務局
○　括弧書き等で少し添えるような形で検討したいと思います。

○ あと、それをどこかで適切に説明していただけるとよいという気がします。
それに関係して、プラス・セキュリティのところで、専門の方はレベル３以上という感じで出ていましたが、レベル１というような言い方があまり出ていなかったかと思います。本体の方ですが、レベル１でも全く問題なく、それを適切に持っていると非常に価値があるというような言い方で、プラス・セキュリティをアピールしていただくのもよいのではないかという気がしました。

○　関連する観点からですが、この大規模組織向け手引き書について見る際に、P.18 にパターンがあるのですが、CSIRT のみ書かれています。前回は制御システムにおける人材育成に関する事例の紹介もあり、OT セキュリティの重要性が高まっています。また、最近でいうと、欧州サイバーレジリエンス法（EU CRA）への対応があり、PSIRT（Product Security Incident Response Team）が必須となっています。そういったところの表現がされていないのは、何か理由があるのでしょうか？
もう一つ、先ほどの P.４に関しましては、学生の話もありましたが、逆に企業から言うと、生産技術の人間や、製品やサービス等の開発の人間、その他、品質の人間に、やはりここを読んでプラス・セキュリティを学んでほしいと思います。例えば製品であれば品質というキーワードでセキュリティを見ますので、品質の人間もセキュリティを勉強してほしいですし、当然、コードを書いている人間もやってほしいです。それから OT で言うと、生産技術という観点もありますので、そうした観点を多次元的に盛り込むと資料が煩雑になるとは思いますが、そういう形でぜひプラス・セキュリティの部分についても読ませられればよいと思いました。企業から言うと、プラス・セキュリティで言うと、品質、開発、または生産技術というところにも、ぜひ読んでもらえる、あるいは読ませるようなことができたらと思いました。

事務局
○　ご質問の点についてですが、文献から引用してきたものをアレンジしてよいのかどうかという懸念があり、あくまで我々としては、既存の様々な取組を人材という目線で具体化していく際の導入としてこれを使用しています。そのため、オリジナルをアレンジするという意味で、「オリジナルを一部改変」といった表現にするのがよいかと考えております。

○　そのような表現は様々あるため、ここを見た瞬間に、おそらく IT 部門しか見ないような気がいたします。先ほども申し上げましたが、生産技術や品質、設計開発の担当者には、そのような部分が見えなくなってしまいます。IT システムの開発については、CSIRT とあり、特に IT 部門と書かれているため、見るとは思いますが、そこがフレームワークから引用されたとは分かるものの、やはり気になります。

○　よく「○○をベースに加筆した」という言い方で記載しますので、そのような言い方で注釈を付ければよいのではないでしょうか。

○　「サイバーセキュリティ体制構築・人材確保の手引き」も入っていたため、少し補足いたします。
　その表を作成した経緯というわけではありませんが、従来の SecBoK も同様でした。SecBoK を作成したのが 2016 年頃であったため、やはり CSIRT がかなり意識されており、前回の SecBoK も CSIRT の人材に近い役割のような形になっていました。それをそのまま使用したわけではありませんが、当時はやはりコンピュータといえば CSIRT という意識で作成したため、CSIRT と表現されています。何らかのインシデントレスポンスの別のチームであれば、現在では CSIRT やコンピュータだけでなくてもよいという形なのかなと、お聞きして思いました。もしかしたら CSIRT という箇所は変えずに、「インシデントのレスポンスチームです」くらいの形で一部改変してしまうというのが、一つのやり方かなと思いました。

○　５、６年前の状況では IT 部門が中心であったため、そこは新しくアップデートしていくことが重要だと思います。図を作成するのはかなり大変でしょうけれども、少し工夫していただければと思いました。

○　先ほどの１点目の議題のところにもありましたが、例えば他のフレームワークとの連携といった形からすると、そのような記載が大規模組織向けの手引き書の方には書かれていますが、おそらく本体の方にはあまり触れられていないのではないかと思います。パブリックコメントへの対応が十分に反映されていないのではないかという疑問が生じる可能性

があります。公表物全体で網羅されていること、または参照先を明示する形式とする等、表現の工夫が必要ではないかと考えております。

それから、今回の参考資料として、参考資料３-１から３-５までそれぞれありますが、これはいつ頃公表されるのでしょうか。わかりやすく記述されておりますので、早期に公開することが望ましいと考えます。

事務局

○　我々のフレームワークがあり、海外のフレームワークや日本の既存のものがどのようにつながっているかということについて、従前の会議で説明していた概念図のようなものを素材として入れているほか、参考資料２では、P.27、P.28 あたりで一応対応関係表のようなものはつけておりまして、このあたりで接続関係は表現しているつもりでした。素材としては含めておりましたが、概念的な位置づけを示す図を導入部分にも掲載するとよいのではないかと、ご意見を伺いながら感じたところでございます。

もう１点、公表時期についてですが、フレームワーク単体での公表では不十分であると考えておりますので、なるべく同時に出したいと思っております。ボリュームはありますが、まずは細部の修正等もあるかと思いますが、これも同時に、かつ速やかに出せるように努めたいと考えております。

○　最初にオールジャパンのようなお話をさせていただきましたが、大規模組織向けの手引き書について、相互参照の関係図としてはこの図でよいと思います。NICE を含め様々なフレームワークが記載されておりますので、この相互参照図の形よりも、日本国内のフレームワークを取りまとめつつ、海外のフレームワークとの接続窓口となっているという形にしていただくほうが、オールジャパンとして出て、NCO の人材フレームワークが国内の取りまとめ役としての位置づけを持つという形になると考えます。

事務局

○ この図は参照関係の流れが正確に表現されておりますので、NICE を各フレームワーク共通の基盤としているため、参照関係を辿ると NICE に戻るという、その点が図の両側に表れる構成となっております。そのため、フレームワークの位置づけを説明するためには、こちらの図が適切ではないかと考えます。

○ ガイドラインとの連携という文脈に限らず、今回のフレームワークの位置づけとしては、国内の代表的なフレームワークとして示す形が適切ではないかと考えます。

事務局

○　こちらの図がその目的にふさわしいと考えております。具体的な参照関係を示す場合

には、先ほどの詳細な図のような形式になりますので、大規模組織向けの手引き書のような感じになるのかなと思っており、少し違うなと思われるかもしれませんが、実際の参照関係の流れについては、別途把握できる必要があると考えます。

○　この部分についてはシンプルな図のほうが適切ではないかと考えます。過度に詳細な参照関係を示すと、かえって利用者の混乱を招く可能性があるためです。

○　手引き書の内容は非常に充実しており、それぞれの対象にとってわかりやすいものであるため、対象別の取りまとめを出していただいたのは非常によかったと思っています。
　私自身は、これを企業に向けて、あるいは個人の、例えば転職活動をしている人に向けてといったことをイメージしながら見ていたのですが、個人向けの手引き書が専門人材向けとプラス・セキュリティ人材向けに分かれたことで、かなり使いやすくなったと考えております。IT 人材の方が目指す方向を検討する際や、自身の現在のスキルレベルを確認する際に活用するほか、あるいは観点は異なりますが、人材サービス事業者として求職者や企業に対応する担当者がセキュリティを理解するためにも、非常にわかりやすい資料であると感じました。

○ そのお立場では全ての手引き書を参照する必要がありますが、担当ごとにぜひお願いしたいと思います。

○　個人向け手引き書に出てくるセルフアセスメントについて、私の理解が合っているかをお伺いしたいのですが、「アセスメント」という用語からは、試験等が連想されます。他方で、参考資料３-４を手元で拝見しますと、現状（as is）の測定というよりも、目標（to be）に向けた学習指針の検討に活用するものであるという認識です。例えば、13 の役割のうち、その方がどれを目指すのか、あるいはどの職に就いているのかを特定したうえで、それを伸ばすための学習ロードマップとして、将来に向けた活用を意図して「セルフアセスメント」と記載されているものと理解しておりますが、この理解で合っておりますでしょうか。

事務局
○　活用の仕方は人によって異なる部分もあると思いますが、私の理解としては、前回ご説明いただいた VisuMe のような形でスキルを可視化して、目指すところのレーダーチャートとの差分を見出し、そこを埋めるために何をすればよいかを考えるような活動をイメージしています。ただし、ロードマップとの関係については、整理が十分でないところがあります。

○　フレームワークに基づくアセスメントツール等の提供は、現時点では予定されていな

いということでしょうか。

事務局
○ 次の議題である資料３および資料４に関連する内容になりますが、スキルの可視化を進め、ギャップを把握して学びを増進する活動へとつなげていくような、フレームワークに準拠したツールが必要だと考えております。必ずしも事務局自身が提供するのではなく、外部の提供者がフレームワークに準拠した形で提供するということでもよいと考えておりますが、そうしたものを利活用できる環境を作っていけないかと考えているのが現在の状況です。そのような仕組みの整備が必要であると認識しております。

○ テストを受けて自分のスキルマップを確認するという活動と表裏一体の関係になると考えます。
それでは、資料２につきましても様々なアドバイスやコメントが出ましたので、可能な範囲で反映していただき、今後さらに見直しや充実を図っていただきたいと思います。事務局にはご負担をおかけいたしますが、よろしくお願いいたします。

(3) 人材フレームワークの今後の利活用に向けて
事務局より、配付資料（資料３・４）に基づき、(3) 人材フレームワークの今後の利活用に向けてについて説明があり、座長から各委員に対して意見を求めた。主な発言は以下のとおり。

○ それでは、ただいまご説明のありました今後の進め方について、来年度からフレームワークをどのように普及させていくのか、また次のバージョンや拡大をどう考えていくのかということですので、ぜひ皆様から様々なご意見やアドバイス、ご提案をお願いいたします。

○ 全体として良い成果物が仕上がりつつあると考えておりますので、まずは周知・普及が重要だと考えております。資料の１点目に書かれておりますが、セキュリティ分野の業界団体だけではなく、例えば経団連や商工会議所等を通じて、企業に直接、人材育成の重要性を普及していくのがよいのではないかと思っております。昨今、様々な事故もありましたし、AI を用いた攻撃も出てきている中で、2025 年は転換点となり、企業の関心が高まってきております。このタイミングでしっかりと企業に向けて、サイバーセキュリティ人材の重要性を伝えていくのがよいと思っておりますので、そうした発信経路をぜひご活用いただきたいと考えます。
また、最後の６点目の話になるかもしれませんが、現在は国主導で進んでおりますが、何年間でどこまで達成するのかという目標を明確にし、その後どうするのかということもセ

ットで考えていかないと、この活動が突然停止するという事態になりかねません。出口戦略も含めて、将来的に民間に移管するのであればどのように進めるのかといった点も、早めに検討しておく必要があると思います。

○　資料４の３ポツ目にある「政府における各種方針との一体化」というところは、私が一番重要であり、期待しているところです。今回のフレームワークは NCO が策定しており、企業向けに限定されるものではありませんが、企業や産業界向けという印象を持たれがちです。例えば、市区町村の行政機関に説明に伺うと、「それは経済産業省の考え方であり、当方は総務省のガイドラインに従う必要があります」といった反応が返ってくることがあります。病院であれば厚生労働省、大学であれば文部科学省のガイドラインに従うという対応になりがちです。しかし、NCO が主導する政府統一の考え方であり、オールジャパンの取組であるという文脈の中で、この人材フレームワークがあり、これが必要だからやっていきましょうという流れを作っていただけると、省庁間の縦割りによる障壁を解消することができます。そのため、例えば次回以降、これをどのように広めていくかという議論の際に、各省庁の人材育成担当者にもご参加いただき、合意形成を図りながら普及を進めるアプローチも必要ではないかと考えます。ぜひご検討いただきたく、協力できることがあれば対応いたしますので、オールジャパン体制での普及のあり方についてご検討いただきたいと思っております。

○ 非常に大事なポイントだと思います。先ほど他の委員からご提案のあった業界団体等への広範な周知と、政府関係機関への働きかけは、並行して進めていく必要があると考えております。

例えば、最近の調達要件では、情報処理安全確保支援士や CISSP の資格を持っている人材が必要であるとありますが、そうした要件の中に、NCO のフレームワークにおける特定の役割やレベルに該当する人材という記載が盛り込まれると、政府内でも共通認識となりますし、それを見た民間の方々も関心を持ち、学んでいただけるきっかけになると思います。セキュリティ専門人材に限らず幅広い人材が対象であるということを、いかに認識していただくかが重要であると感じました。

○　先ほどの資料３において、オレンジ色で示された部分がまさに我々の立場に該当するものと理解しておりました。実際に人材仲介の立場から見ますと、先ほどのご議論のとおり、業界団体を通じて、特に求人を行う企業側のニーズが明確になることが非常に重要です。これはいわば鶏と卵の関係ですが、採用したいと言っていただけないところに、セキュリティの重要性を訴えても、紹介可能なセキュリティ人材が不足している場合、対応が困難になります。明確なニーズがあってこそ、採用方法や組織体制に関する具体的な議論が生まれますので、まずは企業の皆様にサイバーセキュリティ人材の必要性を理解していただくための

周知が重要であると考えております。
　人材サービス事業者の立場としては、そのニーズに適切に対応できるよう、本フレームワークを活用していくことになりますので、各業界団体を通じた会員企業への周知といった取組は、並行して進めていくべき一つの方向性であると考えております。

○　資料４の６ポツのところに関連して申し上げます。CyberSeek というものがありますが、私は従来詳しくなかったのですが、現在、CyberSeek 自体の米国の運用や、どのような形でデータが最適化されているか、どのように使われているかという点を調査されようとしていると伺いました。CyberSeek は大規模な仕組みではありますが、我が国としても目指すべきモデルの一つであると考えますので、米国の実態についてもぜひ調査を進めていただきたいです。調査結果を共有いただければ幸いです。

事務局
○　今年度実施しているのですが、どこまで踏み込んだ調査が可能かという状況です。

○　こちらも継続的に実施していただきたいと考えます。
　また、英国においても産業界との連携がかなり進んでおりますので、比較調査を実施していただくとよいのではないかと考えます。官民でエキスパートを評価し、適切な専門家を見つけるためのポータルサイトが整備されているようです。企業がそのポータルを通じて適切なアドバイザーを見つけることができる仕組みとなっているとのことです。

○　今後の取組として、拡大に向けたご提案もいただければと思います。例えば先ほども AI の話が出ていましたが、レベル 4-E やレベル 4-M に該当する人材にとっても、AI の活用方法は現在大きく変化しております。最前線の人材が AI をどのように活用しているかという現状に加え、将来像についても検討していく必要があると考えます。
　それから逆に、先ほどからプラス・セキュリティというお話がありましたが、AI 秘書や AI エージェントとして機能する様々なサービスが登場してくると考えられます。そうした AI に対するセキュリティ要件はどうなのかといった話が出てくるかもしれません。そうなると、AI 固有の課題もますます重要性を増してまいりますが、将来的な AI の影響をどのように捉えていくかは、大変重要な論点であると考えます。
　先ほど他の委員から専門性の幅を持たせるというお話もございました。非常に重要なご指摘だと思います。加えて、技術スキルの幅に限らず、最近ダブルメジャーという言い方をしているのですが、一例を挙げますと、近年、大企業の法務部門には弁護士資格を有するプロフェッショナルが在籍し、活躍しております。昨今の状況から言うと、そうした方がサイバーセキュリティを理解していなければ、昨今の事案に適切に対応することが困難です。サイバーセキュリティが経営問題として顕在化した際に、経営者が法的な対応について相談

できる人材がいないという事例が報告されております。
　実際に私の大学でそのようなセミナーを実施いたしました。法務部門の方を招き、テクニカルなハンズオン経験の重要性について議論する機会を設けました。そのようなことも求めると、本当に幅を広げるのは当然として、さらにダブルメジャーとして、例えば医師免許を有しつつサイバーセキュリティにも精通しているといった人材が、トップレベルでは次第に必要になってくると考えます。そうした点についても、将来を見据えて今から準備を進めておくことが望ましいと考えております。

○　以前、IPA において「山脈型人材」という概念を提唱しておりました。複数の専門領域でそれぞれ高い能力を持つ人材を指すものです。また、ガートナーでは「バーサタイリスト」という概念が提唱されており、それに近い考え方ではないかと想起いたしました。

○　はい、まさにおっしゃるとおりです。
　来年度も本検討会が継続されるとのことですので、引き続き検討を深めてまいりたいと思います。

○　この点については、社内でも議論しているところですが、現在、知識とスキルについては、基本的には AI で対応可能です。詳細な知識は AI に蓄積されているため、いかに適切に引き出すかということと、スキルの面では AI エージェントの活用が進んでおります。
　そうすると、我々が対応しなければならないのは、AI にどこまで任せられて、その内容について適切に評価ができるということと、実行した結果に対して責任を負えるということです。この２点が非常に重要になっていきます。先ほどお話しした三場ですね。「三場」に「ロック」ですね。「ロック」も「意思（いし）」であるとか、様々な意味をこじつけていろいろ作ったりしていたのですが、そうした場面での判断力を養うことが重要です。プラス・セキュリティ人材にとっても、AI の適切な活用は重要な要素になると考えます。
　別の観点ですが、最近の事案を見ると、攻撃側の速度が著しく向上しております。そのような状況では、デジタル化を安全に進めることが困難であるため、サイバーセキュリティ分野こそ、率先して AI を活用する必要があります。こうしたメッセージは社内外に広く発信していくべきであると考えますが、フレームワークの発信において、こうしたメッセージも含めてもよいのではないかと考えております。

○　将来的な話というよりも、比較的現実的な観点から申し上げますと、資料４の４番のところで、いろいろな資格や研修プログラムと、このフレームワークがどのように結びついているのかというところが、現状、当面は各提供主体による公表というふうに書いてあり、これは現段階ではやむを得ないことと理解しておりますが、基本的には提供主体が自己評価してということですが、記載のとおり、客観性の高い評価の仕組みが重要になると考えます。

フレームワークと資格・研修プログラムとの関連付けが適切に行われ、必要なスキルや知識をどこで習得できるかが明確に分かる仕組みの構築が、実務上重要であると考えますが、資料に記載のとおりではありますが、改めてこの仕組みづくりの重要性を強調しておきたいと考えます。

もう一点、繰り返しになりますが、周知・普及啓発について、少子化で大学や専門学校に入学する学生も減っていきますので、セキュリティ人材の確保を実現するためには、入学段階および卒業・就職の段階において、学生に対して訴求力のあるメッセージを発信できるとよいと考えます。効果が顕在化するまでには相当の時間を要すると思われますので、早期に活動を開始することで、数年後にはセキュリティ分野を選択する学生が増加することが期待されます。

○ ありがとうございます。他はよろしいでしょうか。

それでは、ただいまの第３の議題では、たくさんのご意見をいただきました。「サイバーセキュリティ人材フレームワークの利活用や改善に向けた今後の課題（案）」、この部分につきましては、おそらくこれが来年度のアクションプランというか、何をやっていくかという土台だと思いますので、本日の議論を踏まえ、私、座長一任で事務局と相談しながら取りまとめるかたちでよろしいでしょうか。ありがとうございます。それではそのように進めさせていただきます。

本日いただいたご意見を踏まえ、今後の展開を見据えた整理を進めてまいります。以上で、本日予定していた全ての議事は終了いたしました。本検討会では、今年度４回にわたり、サイバーセキュリティ人材フレームワークの在り方等について闊達にご議論いただきました。本日、フレームワークと手引き書について、取りまとめの段階を迎えることができました。本日の議論を通じて繰り返し指摘されましたとおり、フレームワークと手引き書は、今後の活用や実践を通じて、試行錯誤を重ねながら磨き上げていくことが重要であり、その意味で、本日の取りまとめは出発点であると認識しております。第１回の冒頭で申し上げたとおり、成長するフレームワークとして発展させていくため、引き続きご協力をお願いいたします。

委員の皆様には、それぞれの専門的なお立場から多くの貴重なご意見をいただきましたことに、改めて御礼申し上げます。そのうえで、今後はフレームワークの周知・啓発にぜひご協力いただくとともに、引き続き本取組に対しご知見を賜りますようお願いいたします。

それでは、進行を事務局にお返しいたします。

○　最後に一点よろしいでしょうか。サイバーセキュリティ人材フレームワークの策定にあたっては、サイバーセキュリティ戦略への反映が大きな目的の一つであったと理解しております。今回策定されたフレームワークは、サイバーセキュリティ戦略にどのような形で反映されるのでしょうか。

事務局

○ サイバーセキュリティ戦略についてですが、資料３の P.３をご覧ください。12 月に閣議決定されまして、そちらの中に入れさせていただいております。

時系列で申し上げますと、12 月にサイバーセキュリティ戦略が閣議決定されており、その中で今後フレームワークを策定して推進していく旨が記載されております。戦略上は概括的な記載にとどまっておりますので、今後さらに具体化しながら進めてまいりたいと考えております。この程度の粒度ですので、より肉付けや詳細化をしながら進めていければと考えております。

飯田内閣サイバー官

○ 戦略は５年程度の期間を念頭に策定しており、これまでの検討会でのご議論を踏まえ、戦略に反映することができました。今回フレームワークと手引き書が完成し、これからどのように利活用を実践していくかについては、戦略の実施計画のようなものになると考えております。今後、年次計画を策定する中で、各年度の取組内容を具体化し、戦略の着実な実施、およびフレームワーク・手引き書の実践に向けて、しっかりとフォローアップしてまいりたいと考えております。

また、現在、成長戦略において国内投資等に関する様々な議論が行われておりますが、分野横断的な人材課題としてサイバーセキュリティも重要であり、そのサイバーセキュリティを支える人材も当然重要です。そのため、成長戦略として、今年の骨太の方針につなげていくことや、予算的な裏付けを取っていくことにつながっていくわけですが、そうした形で取組を加速させることも検討してまいりたいと考えております。

（３） 閉会

＜挨拶：木村統括官＞

統括官の木村でございます。閉会にあたり、一言ご挨拶させていただきます。委員の皆様、先生方におかれましては、昨年の 10 月に本検討会を立ち上げて以降、お忙しい中、様々な専門的な知見に基づいて活発なご議論をいただきまして、心より御礼申し上げます。おかげさまで、本日、サイバーセキュリティ人材フレームワーク、そして手引き書の取りまとめというゴールが見えてきたと思っております。

ただ、策定自体が本当のゴールではないということは、先ほどから何度もお話が出ているかと思います。今後、手引き書と併せて、フレームワークが様々な主体において活用されるユースケースを着実に蓄積していくこと、そしてそのために周知・普及啓発をしっかりと行っていくことが重要だと考えております。もちろん我々もしっかりと取り組んでまいりますが、委員の皆様におかれましても、ぜひそれぞれのフィールドで積極的に活用し、普及にご協力いただきますようお願い申し上げます。そのうえで、官民における共通的な言語として、人材フレームワークの内容が活用され、人材の確保・育成がより効率的かつ効果的に進

んでいくことを期待しております。

また、今後の活用状況を踏まえながら、必要な見直しを継続的に行っていかなければならないと考えておりますので、その点につきましても、引き続き来年度以降もご支援をお願いできればと思っております。もちろん、使ってみて見直すというのも当然であり、現在のものをブラッシュアップする中では、最後の方でも少し話が出ましたが、様々な状況変化という意味で、AI の活用といった新しい状況が次々と出てきているのも間違いない事実です。ここはある意味、人材の議論をさせていただいた場でもありますが、日本政府全体で見れば、先ほど成長戦略の話も飯田サイバー官の方からありましたが、その中でも当然 AI の話は取り上げられています。AI のセキュリティという議論も、ここ数か月で非常に熱が入ってきている状況にあります。したがいまして、そういった状況もしっかりと、見直す際の人材フレームワーク 2026 等の中にも適切に入れ込んでいくことが重要であると考えております。

今後も引き続き取り組んでいくことではありますが、ひとまず本日は取りまとめということで、一つの区切りのタイミングであると存じます。これまでのご尽力に改めて感謝申し上げますとともに、利活用のフェーズに移行しながら、引き続き本検討会において連携しながら議論を深めてまいりたいと考えておりますので、引き続きどうぞよろしくお願いいたします。誠にありがとうございました。

以上