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３回）議事要旨

1. 日時

令和８年２月９日（月）10 時 00 分から 12 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）

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
辻　伸弘	ＳＢテクノロジー株式会社 プリンシパルセキュリティリサーチャー
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

（ゲストスピーカー）

大槻　晃助	一般財団法人日本サイバーセキュリティ人材キャリア支援協会 （JTAG 財団） 事業部長
高崎　庸一	一般財団法人日本サイバーセキュリティ人材キャリア支援協会 （JTAG 財団） 事務局長
丸山　真佐夫	木更津工業高等専門学校 情報工学科 教授
中野　利彦	株式会社日立製作所 インフラ制御システム事業部 セキュリティエバンジェリスト

小林　英二　　株式会社日立製作所 インフラ制御システム事業部
制御セキュリティ設計部長

（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

事務局

○ それでは定刻となりましたので、第３回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を開催いたします。本日もご多忙のところご出席いただきましてありがとうございます。

本日は全 11 名の委員の皆様にご出席いただいております。ここからの進行につきましては後藤座長にお願いできればと思います。

（2）　議事

(1) ヒアリング

事務局

○ 今回のヒアリングは、今後のフレームワーク策定・活用に向けた課題や示唆を得ることを目的とします。

はじめに、一般財団法人日本サイバーセキュリティ人材キャリア支援協会（JTAG 財団）には、人材の可視化ツールである「VisuMe」などを紹介いただきます。次に、教育場面での活用という観点から木更津工業高等専門学校に、最後に、制御システムのセキュリティと人材育成の観点から株式会社日立製作所に、それぞれ説明をいただく予定です。

（ア）一般財団法人日本サイバーセキュリティ人材キャリア支援協会（JTAG 財団）からのヒアリング

大槻　晃助　事業部長及び高崎　庸一　事務局長より資料１に基づき説明があった。

（イ）木更津工業高等専門学校からのヒアリング

丸山　真佐夫　情報工学科教授より資料２に基づき説明があった。

（ウ）株式会社日立製作所からのヒアリング

中野　利彦　インフラ制御システム事業部セキュリティエバンジェリスト及び小林　英二　インフラ制御システム事業部制御セキュリティ設計部長より資料３に基づき説明があった。

３団体による説明の後、座長から各委員に対して質問や意見を求めた。主な発言は以下のとおり。

○ では、まず私から質問します。はじめにJTAG財団にお伺いしますが、３点ございます。

１点目は、ツールの利用状況や実践状況についてです。実際に利用されている企業からのフィードバックや、具体的な活用方法について改めてご教示ください。

２点目は、個人が情報を入力する頻度についてです。例えば、転職時だけでなく、学習履歴などを日々更新するような、どのようなペースでの利用を想定されていますでしょうか。

３点目として、このツールは個人の利用が主体となるのでしょうか。先ほどのご説明ではチーム単位での活用可能性も示唆されていましたが、特定の事業部門が持つセキュリティスキルの総量を評価するなど、組織単位での利用は可能かお聞かせください。

一般財団法人日本サイバーセキュリティ人材キャリア支援協会（JTAG財団）

○ まず、現在の利用状況ですが、会員企業は十数社で、アクティブユーザー数は二千数百人です。利用頻度は企業によって異なりますが、当財団としては、年に１回程度のアセスメント実施を推奨しています。これにより、業務経験の蓄積や資格取得によるスコアの変化を反映できるためです。また、社員以外での利用例もあります。例えば、外部から人材を採用する際に候補者に実施していただいたり、教育事業者が顧客に対して最適な研修を提案するために活用したりするケースがあり、利用頻度は様々です。以上が１点目と２点目への回答です。

○ 利用状況の調査やフィードバックの収集は、常に実施されているという理解でよろしいでしょうか。

一般財団法人日本サイバーセキュリティ人材キャリア支援協会（JTAG財団）

○ はい。事務局側の運用画面で利用者数などをすべて把握しており、実績として蓄積しています。

○ その実績をもとに、改善点や利用ノウハウも蓄積されていくという理解でよろしいでしょうか。

一般財団法人日本サイバーセキュリティ人材キャリア支援協会（JTAG 財団）
○ はい、そのとおりです。お客様から、使い勝手に関するご意見や機能追加のご要望などを数多くいただいています。

○ 木更津高専にお伺いします。ご説明資料の中で上位１%の突出した人材が示されています。
先日、偶然にも貴校ご出身の非常に優秀な方と、国内で CTF をどのように盛り上げていくかについて話す機会がありました。その際、なぜ木更津高専で優れた人材が育つのか尋ねたところ、「突出した学生がいると、その周りに人が集まり、組織全体のレベルが引き上げられる。いわばアウトライヤーがその世代を牽引していく」というお話がありました。
このような突出した人材は、時に扱いにくさもあるかと存じますが、その良い影響をうまく活用することが重要だと感じます。貴校では、こうした学生をどのように位置づけ、その能力をどのように見ているのでしょうか。

木更津工業高等専門学校
○ ご指摘のとおり、高専には時折、非常に優れた学生が現れます。これは木更津高専に限らず、どの高専でも見られる現象かと認識しています。
木更津高専では、そのようなユニークな学生が現れた際には、通常の授業の枠を超えた対応をしています。教員がうまく導き、セキュリティ分野への興味をさらに深めてもらうため、CTF や企業の勉強会へ参加を促すなどの取組を行っています。そうしますと、クラスメイトなどが関心を持って集まってくる、という良い循環が生まれることがあります。この好循環を全国規模に広げたいと考え、特に優れた学生を対象とした招待制の講習会をトップオブトップス講習会という名称で実施しています。この講習会を通じて、参加学生のスキルを一層高めるとともに、将来有望な学生も一緒に招待し、育成を図っています。
これを毎年継続し、木更津高専の特色として定着させるまでには至っていませんが、今年度はトップレベルの学生たちが中心となり、セキュリティの同好会を通じて後輩を指導するような仕組みを自主的に考えてくれています。この取組がうまく機能していくことを期待しているところです。

○ まず、私自身も関わっております JTAG 財団について、補足させていただきます。
資料１の９ページにあります VisuMe は、何かを認定するというよりも、大学入試における共通テストのような位置づけと認識しております。これは、個々の人材がどの程度の能力を持つかを可視化するものです。これにより、大学が文系・理系で重視する科目を変えるように、企業側も求める人材像に応じて独自のプロファイルを作成し、育成や採用に活用できる仕組みとなっております。

例えば、本検討会で議論している 13 の人材像についても、それぞれのプロファイルを作成すれば、人材との適合性を測ることが可能と考えられます。一方で、SecBoK が 2025 年に改訂されるなど、追随すべき課題もございます。

これを踏まえ、木更津高専と日立製作所に 1 点ずつ質問があります。

まず木更津高専には、2026 年から開始される「プラス・セキュリティ」の取組についてお伺いします。情報系以外の学生がセキュリティを学ぶことになった際の反応、例えば「なぜ学ぶ必要があるのか」といった疑問の声や、セキュリティ関連の職務への就業意欲など、学生の皆様の意識や感覚について、お分かりになる範囲で教えていただけますでしょうか。

次に日立製作所には、現場部門におけるセキュリティ人材の評価についてお尋ねします。資料３の 12 ページなどを拝見しますと、事業組織側にもセキュリティ担当の方がいらっしゃると存じます。一般的に、IT 部門以外の方が担うセキュリティ業務は人事評価に結びつきにくく、育成が難しいという課題が聞かれますが、貴社では事業組織側の人材に対する人事評価制度がどのようになっているか、お聞かせいただければ幸いです。

木更津工業高等専門学校

○ プラス・セキュリティに関するご質問にお答えします。

導入当初は、教員側にも「セキュリティは専門分野であり自分たちには関係ない」という意識がありました。そのため、まずは教員の意識改革から着手し、現在もその途上にあります。

学生も同様に「セキュリティは情報工学科の学生が学ぶもの」という認識が当初はありましたが、エンジニアであれば誰もが自身の担当分野でセキュリティに関わること、そしてその知識の有無が自ら作るシステムに影響を及ぼすことを、徐々に伝えているところです。

来年度からプラスセキュリティコースの学生を情報工学科以外の 4 学科で各学科 10 名募集しますが、40 名の学生の中からどのような学生が興味を示してくれるかは、実際に始めてみないと分からない状況です。そのため、今後ますます機運を盛り上げていく必要があると認識しています。

企業側から、セキュリティ専門部門に限らず、あらゆるエンジニアにセキュリティ知識が必要であるという要望を求人の形で示していただけると、学生の意識が大きく変わり、ひいては教員の課題意識も高まっていくのではないかと考えております。

株式会社日立製作所

○ 当方では大きく３つの階層で人材を捉えています。まず経営層については、評価が難しいためここでは一旦置いておきます。

次に現場層ですが、ここはスキルレベルというよりも、必要な知識を有しているか、また指定の教育を受けているかといった観点で管理しています。

そして中間の層にあたるセキュリティの専門家については、スキルマップを用いて能力

の達成度を管理し、評価に反映させています。このように、３階層で評価の仕組みを整理し、推進しております。

○ ありがとうございます。そうしますと、現場層の方々については、研修の受講歴を確認するだけでなく、例えば個々人の業務上の役割やミッションの中に、セキュリティに関する項目が明記されているケースもあるのでしょうか。

株式会社日立製作所
○ はい。資料３に記載の PDCA の図で「施策策定/徹底」と示しておりますが、ここで現場部門が実行すべき内容をすべてトップダウンで指示します。
そして、その内容を現場が正しく理解しているかを、ガバナンスの一環として教育や監査を通じて確認します。もし達成できていない場合は、再度指導を行うといった形で、継続的な改善サイクルを回しております。

○ JTAG 財団に対し、２点質問がございます。
１点目は資料の３ページについてです。中央に「トレーニングや学習を提示」とありますが、これは JTAG 財団が独自に提供されているトレーニングなのでしょうか。あるいは、既存の事業者や学校などが提供するトレーニングを斡旋・紹介するものなのでしょうか。この点の実態についてお伺いします。
２点目は５ページについてです。左側に「ブラッシュアップやメンテナンスを迅速に継続させていくために、各指標をモジュール化」と記載があります。こうした指標は、随時ブラッシュアップとメンテナンスが必須であると認識しておりますが、その更新頻度はどの程度を想定されているのでしょうか。先ほど他の委員から SecBoK の更新をトリガーにするというお話がありましたが、それ以外に、世の中のトレンドを反映して独自にアップデートするような、SecBoK 以外のトリガーや頻度に関するお考えがあればお聞かせください。以上２点です。

一般財団法人日本サイバーセキュリティ人材キャリア支援協会（JTAG 財団）
○ まずトレーニングについてご説明します。当方のアセスメントでは、推奨研修が自動的に表示される仕組みを備えています。教育事業者様が自社の研修を登録し、アセスメント結果に合致した場合に表示される機能がありますが、現在は一時的に停止しています。これは、登録事業者様や表示される研修が少なく見劣りがするためです。
今後は登録を促進し、将来的には教育事業者の研修だけでなく、学校のプログラムなども対象に含めることができると考えております。次に指標のブラッシュアップについてです。目標としては年１回の定期的な更新を掲げておりましたが、実際にはこの４年間で１回のメンテナンスにとどまっています。

全てのスキル指標と、業務経験年数に応じた基礎スコアといった入力指標を全面的に見直すことは、大変な作業となります。JTAG 財団の活動は委員の皆様のボランティアに支えられており、この運営体制では限界があるのが実情です。

しかし、SecBoK を基準としている以上、その改定への対応は必須であると認識しており、現在 JNSA と協議を進めているところです。

○ ご説明いただいた３者の皆様に、順番に質問いたします。

まず JTAG 財団への質問です。先ほど他の委員からもご意見がありましたが、個人単位だけでなくチームや部門単位で可視化できる機能があれば、人事部門や現場での活用範囲が広がるのではないかと考えられます。そうした機能の追加を期待いたします。また、テンプレート登録の機能について、どのようなものか改めてご説明いただけますでしょうか。例えば、理想の人材像をテンプレートとして設定できれば、予算獲得のきっかけにもなり得ると感じました。

次に、木更津高専にお伺いします。時間の都合上１点に絞ります。「トップ人材」として育成された卒業生が、その後どのような分野で活躍されているか、具体的な事例があればお教えください。

最後に、日立製作所への質問です。「セキュリティ統括」の役割について、これは現場と経営幹部をつなぐハブのような機能と理解してよろしいでしょうか。もしそうであれば、この役割を担う人材に必要なスキルはどのようなものでしょうか。

また、高度な調整能力が求められると考えられますが、そのような人材の育成方法や、育成の成果をどのように測定されているかについてお聞かせいただければ幸いです。

一般財団法人日本サイバーセキュリティ人材キャリア支援協会（JTAG 財団）

○ 画面を共有しながらご説明します。

チーム向けの管理者機能として「グループアセスメント」という機能があり、選択した対象者全員の状況を一覧で確認することが可能です。サンプルプロファイルについては、現在は個人の業務のみ登録されていますが、今後はチーム用のサンプルプロファイルも作成して実装する予定です。この作業は JNSA 内の JTAG ワーキンググループで進めており、完成次第、当財団でシステムに登録します。このように、プロファイル登録は自社の業務に合わせて設定できるようになっています。

JTAG 財団が提供するサンプルプロファイルは、あくまで一般的な理想像です。それとは別に、各企業様が自社の特定の業務に合わせた形で、独自にプロファイルを設定できる機能も備わっています。例えば、セキュリティ担当のレベルを「ジュニア」と設定するなど、管理者機能を用いて、自社の業務に応じたスコアを自由に登録できます。個人の業務登録だけでなく、例えば「自社の CSIRT チームとして、特定のスキルをこのレベルで保有している必要がある」といったチーム全体の要求レベルを登録し、比較することも可能です。これに

より、グループアセスメント機能を用いて、現在の構成人員で要求レベルを満たしているかどうかが一目で把握できます。

また、人員の入れ替えシミュレーションなど、チーム編成の検討にも活用いただけると考えております。採用活動においては、求める人材のスキルレベルを明確に提示できます。

しかしながら、自社の各業務に対して必要なスキルと、その具体的なレベルを定義できている企業は、実際にはほとんどないのが現状ではないでしょうか。この点が、当財団の現在の大きな課題です。機能は提供しているものの、それを活用できる企業が少ないため、今後は啓発活動にも力を入れていく必要があると認識しています。

各企業において、職務ごとに必要なスキルとそのレベルが論理的に整理される文化が醸成されることを期待しております。以上です。

木更津工業高等専門学校

○ 卒業生の進路についてですが、大学などに進学する学生も多く、最終的な就職先を完全に追跡できていないのが実情です。把握している範囲では、必ずしもセキュリティ専門の企業に就職しているわけではないという感触です。

ネットワーク関連やクラウド関連の企業に進み、セキュリティのスキルが何らかの形で活かせる職種に就いているという印象があります。セキュリティに秀でた学生が、必ずしもセキュリティ分野のみに関心があるわけではありません。新しいことや先端的なことであれば何にでも興味を持つ学生も多いため、最終的にセキュリティ分野を選択するとは限らないのが現状です。

一方で、セキュリティコースを設置している高知高専では、当校と比較してセキュリティ関連企業へ就職する学生が多いという印象です。ただし、トップレベルの学生が必ずしもそちらに進んでいるわけではありません。当校としては、セキュリティを学んだ学生がそのスキルを存分に活かしてくれることを願っています。データとしてお示しすることはできませんが、以上が当方の所感です。

株式会社日立製作所

○ 「セキュリティ統括」についてですが、ご指摘のとおり、ハブとしての役割を担っているとご理解いただいて差し支えありません。

その実態は、事務局と、企業を横断する会議体で構成されています。役員から現場の部門まで、各層から人選されたメンバーで会議体を構築しています。したがって、資料では「組織」と記載していますが、実質的には事務局とこの会議体を指します。

運営については、会議体の中に制御、セキュリティ、IT の各専門家や、現場を熟知した担当者がいるため、彼らを中心に議論を進めています。ただし、当初はセキュリティの専門家が不足していたため、現在は ICSCoE の卒業生が中心的な役割を担っています。9 期生までで十数名に上る卒業生が、専門家として参画しています。

人材育成に関しては、テーマごとのディスカッションを通じて知識を深め、各部門から参加しているメンバーがその学びを自部門に持ち帰り展開するという枠組みで進めています。さらに、訓練のループを回すことも重要です。実際に発生するインシデントを事例として、既存のルールやプロセスに問題はなかったか、不足していた知識やスキルは何か、そしてそれをどう確保していくかを検討し、組織全体のレベルアップを図っています。

○ ご説明いただいた３者の皆様に質問です。AI をはじめとする技術革新の速度が増しており、教育内容を継続的に更新する必要性が高まっていると考えられます。この点について、既に対応されていること、あるいは今後対応を検討されていることがありましたらご教示ください。

一般財団法人日本サイバーセキュリティ人材キャリア支援協会（JTAG 財団）
○ 難しいご質問です。
AI については、複数の教育事業者様が既に取り組まれていると認識しています。JTAG 財団の取組に関しましては、人材の可視化を AI で実現したいという議論が常々ございます。人物像の把握なども、AI が適切な情報量を見定めてくれるようになるのではないかと考えています。これを教育分野に応用できれば理想的ですが、実現可能かどうかはまだ分かりません。しかし、その可能性には期待しております。

○ ご質問は、AI のような新たなニーズや求められる教育スキルに対して、対応が可能かどうかという趣旨と理解いたしました。

一般財団法人日本サイバーセキュリティ人材キャリア支援協会（JTAG 財団）
○ はい。システム的には、内容を入れ替えることで対応可能な設計になっています。しかし、現時点ではまだ実施しておりません。

木更津工業高等専門学校
○ ご質問は、最後のスライドに深く関連しますので、もし可能でしたら表示をお願いできますでしょうか。
ご指摘のとおり、教育内容は継続的に、かつ高い頻度で更新する必要があり、その指針として業界が示すような枠組みを活用したいと考えています。当方では、人材フレームワークを活用して企業ニーズを把握し、それを MCC および MCC Plus の改定指針とすることを検討しています。最後のスライドにあります教育認定制度も、そうした目的で活用できるものと認識しています。
具体的な取組としましては、企業のエンジニアや研究者といった外部講師を招聘し、最新動向を反映した講義を組み立てることを意識しております。また、内部教員の育成も重要視

しており、教員コミュニティを育て、勉強会などを通じて研鑽する機運を高めています。さらに、企業のエンジニアの方々と月１回の学習会を開催するなど、最新動向に対応できる体制づくりを進めています。しかしながら、学校組織はカリキュラムの改定に時間を要するという性質があり、迅速な対応は非常に大きな課題であると認識しています。

株式会社日立製作所
○ AI の応用については、基本的には積極的に活用していくという流れになっています。
AI が出力した結果が制御システムや事業に与える影響や、その正当性については、利用者側が責任をもって判断します。
一方で、委託できる業務は積極的に AI に任せるという方針です。全社的には、AI に関する情報を共有する組織があり、そこでは良い事例なども共有されています。しかし、AI の進歩は極めて速く、制御システムの進歩速度とは大きな差があるため、そのギャップをどのように埋めて活用していくかを調整しながら進める必要があります。以上です。

○ 大学でも、セキュリティ特化ではありませんが、グループでのシステム開発の演習の科目において、従来、１か月の仮想プロジェクトとして実施していた内容が、AI 利用で数時間～数日程度で出来てしまうという内部検証結果が出まして、内容の練り直しをせざるを得ないということがございました。セキュリティオペレーションや脆弱性検証などでも AI 利活用が進むと思いますので、その観点でご質問させていただきました。

○ 日立製作所に質問させていただきます。木更津高専にはコメントとなります。
まず日立製作所への質問ですが、「制御システムとして何をすべきか」という点についてです。ご説明の中で示された「セキュリティ統括」という役割の方は、セーフティの領域も担当範囲に含まれるのでしょうか。もし担当範囲が異なる場合、制御システムの扱いにおいては、セーフティとセキュリティは常に一体として対応されている、という理解でよろしいでしょうか。
次に、木更津高専へのコメントです。「プラス・セキュリティ」人材の育成において、８割を目標に企業と連携されている点は素晴らしい取組であると認識しております。当方が代表を務める産業横断サイバーセキュリティ研究会でも、過去に「セーフティープラス・セキュリティ」をテーマにした教育ビデオを制作した経緯があり、こうした地に足のついた活動は非常に有益であると感じております。

株式会社日立製作所
○セーフティに関しましては、入社以来、徹底して教育が行われています。現在は、そのセーフティの考え方にセキュリティをどのように組み込むかという観点での教育を進めている状況です。結果としてセーフティとセキュリティは一体として教育を実施していること

になります。

○ 私からは JTAG 財団と日立製作所へ質問です。

まず JTAG 財団にお伺いします。先ほどから議題となっている利用状況や利用頻度に関連する内容です。資料１の９ページにあるグループアセスメント機能は、求人や採用における雇用仲介の観点からも非常に優れた仕組みであると拝見しました。この機能によって、組織内で不足している人材や求める人材像が可視化され、具体的な対話につながることが期待されます。現状では、まだ活用の初期段階にあると認識していますが、この活用を促進するための具体的な取組や今後のアクションがあればお教えください。

次に、日立製作所にお伺いします。スキルレベルの定義、訓練計画への落とし込み、評価までの一連のサイクルについてです。このサイクルにおけるスコアの基準やレベル設定はどのように決定し、それをどのようにして組織知として反映させているのでしょうか。この仕組みは、VisuMe の今後の参考にもなると考えられますので、詳しくお聞かせいただきたいです。

一般財団法人日本サイバーセキュリティ人材キャリア支援協会（JTAG 財団）

○ グループアセスメント機能は提供しておりますが、現状、本格的に活用されている会員企業はまだ少ない状況です。活用に向けた試みの中で、いくつかの課題が見えてきました。

一つは、組織の全従業員を対象にアセスメントを実施すると、グラフの線が多数表示されてしまい、かえって見づらくなるという点です。より本質的な課題として、チームとしてどのようなスキルレベルバランスが必要かをユーザー企業側で定義することが難しい点が挙げられます。当サービスは主に CSIRT を想定していますが、例えば自社の CSIRT が業務を遂行するために、どのスキルがどのレベルで必要なのかという基準を策定することが、コンサルタント等の支援なしでは困難なのが実情です。

この背景には、各企業が自社の業務やタスクを遂行するために必要なスキルとそのレベルを明確に定義できていないという現状があると考えています。そのため、機能の活用促進には、まずその前提となる業務分析やスキル定義の重要性を啓発していく必要があり、それが当方の課題であると認識しています。一方で、人材採用の領域では、会員である人材サービス会社の１社が、この機能の活用を試みています。応募者にアセスメントを実施するには運用面やコンプライアンス面での障壁がありますが、スキル面でのマッチング精度が非常に分かりやすくなるという利点があります。スキルだけで人材を評価できるわけではありませんが、こうした活用の動きは出てきております。

株式会社日立製作所

○ ご質問の取組は、社内だけでなく、二次請けの協力会社の従業員の皆様にも対象を広げて実施しています。

レベル設定やカテゴリ分けの基本的な枠組みは、開始当初にCSSC（制御システムセキュリティセンター）で理事長を務められている東北大学の高橋先生にご相談しながら構築しました。ただし、企業によってスキルのレベル差が大きいため、この枠組みを画一的に適用するのではなく、まず雛形を提示した上で、対象となる事業者様と対話し、各社の実情に合わせて内容を見直すという手順を踏んでいます。その上で具体的なレベルと目標を設定し、どの組織にどのレベルの確認を行うかを決定し、スパイラルアップを図るという進め方です。この手法により、各社に合わせた柔軟な対応を可能にしています。

例えば、取組の初期段階にある企業様の場合、少しずつ達成可能な目標を設定し、段階的にレベルを引き上げていきます。一方で、先進的な企業様に対しては、より難易度の高いレベルを設定するという対応をしています。

○ はじめにJTAG財団に３点質問いたします。１点目は、ご説明のツールがセキュリティ専門家を対象としたものか、あるいはユーザー企業のIT部門に対して「プラス・セキュリティ」を教育するものかという点です。

２点目は、QMSにおける力量管理といった目的での活用は可能かという点になります。

３点目は、資料１の８ページでDRがITスキル領域に含まれていますが、BCPの観点からサイバーBCP はどのように扱われているかについてお伺いします。次に、日立製作所にご質問です。セキュリティ統括組織は、制御システムを対象としたものでしょうか。それとも情報システムやプロダクトも含む全社的な組織なのでしょうか。もし対象範囲が異なる場合、制御システム部門との関係性についてもご説明をお願いいたします。

一般財団法人日本サイバーセキュリティ人材キャリア支援協会（JTAG財団）

○ VisuMeは、スキル可視化の基盤としてITスキルを据えています。サービス名は「VisuMe for Digital Security」であり、その名のとおりデジタルセキュリティに特化して機能を強化したアセスメントツールという位置づけです。そのため、IT スキルのみを測定することも可能ですが、全体の３分の１をセキュリティ領域が占めているため、求める粒度によってはセキュリティ分野の比重が大きいと感じられるかもしれません。

○ ユーザー企業では IT 人材が担う領域は広いものの、セキュリティ業務は社外に委託する傾向が見られます。そうした中で、IT 人材に対してセキュリティの知見を付与していくことの意義について確認したい、という趣旨の質問です。

一般財団法人日本サイバーセキュリティ人材キャリア支援協会（JTAG財団）

○ ご指摘の点こそ、当方が最も目指しているところです。一般的なIT人材が、より積極的にセキュリティ関連業務へ参画していくことを促したいと考えています。

次に２点目のご質問ですが、本ツールは力量管理や人事考課にも利用できます。しかし、

従業員への過度な圧力となり軋轢を生む可能性があるため、当方としてはその用途を強く推奨しておりません。一方で、HR システムにスキル指標をスコアとして API 連携させるような活用は有効だと認識していますが、現状ではまだ実現できていない状況です。

３点目のサイバーBCP については、当然ながら BCP の評価項目として含まれています。サイバーBCP に関連する業務経験を積むことで、スコアが向上する設計になっています。

株式会社日立製作所

○ ご質問のセキュリティ統括組織は、特定の部門向けではなく、全社を対象範囲としています。組織の構成ですが、各部門から人材を集めて組織体や会議体を構築し、運営していくのが一般的です。制御システム部門との関係については、同部門の担当者もこの統括組織に参画し、共に議論を進めています。そのため、現場の実情にそぐわない要求が一方的に下されることはありません。

一方で、事業継続の観点から実行すべき施策は、この組織で十分に検討した上で経営層の承認を得てから、各現場へ展開するプロセスを構築しています。

○ ベースとなる専門分野、例えばコンピューター科学に非常に強い人材もいれば、哲学や論理学といった分野に強みを持つ人材もいます。

後者のような人材がセキュリティ分野で大きく成長する可能性があるという話はよく聞きます。知人には、最初からセキュリティを専攻するのではなく、学部で哲学、論理学、物理、法律などを学んでからの方が良いと主張する者もいます。これには納得できる部分もありますが、実現は容易ではないという側面もあるでしょう。本日のご発表は、セキュリティ人材がプラスアルファでどのようなスキルを身につけるべきか、また、高専で育成されるような即戦力に近い人材の能力を可視化し教育するという点で、非常に分かりやすく、有益なツールや考え方であると認識しました。

そこで質問ですが、IT 分野の経験者に限らず、今後セキュリティ人材として育成すべき「原石」をどのように発掘し、育てていくべきか、この点についてご意見があればお聞かせください。

一般財団法人日本サイバーセキュリティ人材キャリア支援協会（JTAG 財団）

○ 人材の資質としては、好奇心とセンスが当初から最も重要であると認識しています。潜在的な適性については、当財団として、傾向分析や統計分析を通じて明らかにしていきたいと考えています。

例えば、10 万人規模のデータが集まれば、「特定の行動特性を持つ人材は、特定のセキュリティ業務に適性がある」といった相関関係が見出せる可能性があります。個人の思考様式なども含め、分析によって適性の違いが明らかになるのではないかと期待しています。

木更津工業高等専門学校

○ 高専は実践的な技術教育を重視する教育機関であるため、哲学のような幅広い教養分野は、どちらかといえば弱い側面があります。しかしその反面、学生一人ひとりの興味の対象が多様であり、それを許容する自由な校風がございます。

実際に、情報工学科以外の学生がセキュリティ分野に強い関心を示すことも珍しくありません。企業で活躍されている高専卒業生の中にも、専門外の学科から異なる業界を経て、セキュリティ分野にたどり着いた方がいらっしゃいます。

こうした状況から、高専教育の中で、いかに学生の将来につながる多様な学びの機会を提供できるかが課題であると認識しています。現時点で「こうすればよい」という明確な答えを提示することは難しいですが、以上が当方の所感です。

株式会社日立製作所

○ 専門家以外の人材にセキュリティの知見を「付与する」という考え方に同意します。特に事業部門の従業員にいかにセキュリティマインドを植え付けるかは、非常に重要なポイントだと認識しています。演習を通じてインシデントを実際に体感させ、対策を怠った場合に何が起こるのか、それが事業にどのような影響を与えるのかを理解してもらうことで、意識改革を促すアプローチが有効です。

こうした背景から、事業部門向けの教育カリキュラムと、セキュリティ専門家向けのカリキュラムは、全くの別物として設計すべきだと考えています。専門家育成に関しては、本日お話があったような専門知識の習得はもちろんのこと、当社の例では、外部専門家からご協力を得たり、セキュリティの専門家を対象としたカンファレンスへ社員を派遣したりすることを通じて、知見の蓄積を進めています。

○ 一点補足ですが、先ほど高専の教育についてご謙遜がありましたが、当方の大学院大学で実施している特待生入試において、高専出身の学生が数学などの基礎学力で極めて優秀な成績を収め、授業料免除を勝ち取る事例が複数あります。このことからも、高専の基礎教育は大変素晴らしいものであると認識しております。

それでは、予定の時刻となりましたので、本日のヒアリングは以上で終了といたします。ご登壇者の皆様におかれましては、ご多忙の中、誠にありがとうございました。改めて感謝申し上げます。ゲストの皆様は、これにてご退室ください。ここで５分程度の休憩に入ります。

(2) 人材フレームワーク及び手引き書（案）の進捗状況について

事務局より、資料４及び別紙に基づき、人材フレームワーク及び手引き書（案）の進捗状況について説明があり、座長から各委員に対して質問や意見を求めた。主な発言は以下のとおり。

○ 以前のレビューでもコメントした内容と一部重複しますが、いくつか意見を述べさせていただきます。

第一に、採用担当者の視点からの活用方法です。現場から特定のスキルを持つ人材を求められた際に、それがどの人材像や役職名に該当するのかを逆引きできる仕組みがあると、より活用しやすくなると考えられます。

第二に、小規模組織向けの活用法についてです。自組織で人材を確保することが困難な事業者が多いため、委託先に対して本フレームワークを用いて求める人材像を明示し、適切な人材が配置されているかを確認するといった使い方が考えられます。第三に、資格との関連付けです。13 の人材像と各種資格を関連付け、「この人材像にはこの資格があると望ましい」といった情報があれば有用です。

一方で、各種資格を全て取得したとしても、13 の人材像を網羅できるのかという点には若干の懸念が残ります。最後に、これは細かい点ですが、手引き書のモデルケースで用いられている「X 社」という名称は、著名な企業名と重複するため、別の表記に変更することが望ましいと考えます。

○ 同感です。特に、発注者と受託者の関係における活用が重要であると認識しています。本フレームワークの重要な役割は、採用者と被採用者間のみならず、発注者と受託者間の円滑な意思疎通を可能にする「標準言語」としての機能にあると考えられます。

現状では、発注者側が委託先の人材能力を確認する能力に欠け、問題が生じているケースが少なくありません。そのため、手引き書には、発注者側の能力向上に資するような活用イメージを盛り込むことが有効です。

また、受託者側にとっても、自社にどのような人材がいるかを具体的にアピールできるという利点も期待できるため、標準言語としての活用を推進することが望まれます。

○ ３点ございます。

１点目は、省庁が示すセキュリティ関連の評価制度との連携についてです。大学や病院といった現場では、省庁の評価基準が曖昧で、具体的にどのように指導すればよいか苦慮する場面があります。本フレームワークが、そうした各省庁の基準と整合性を図る形で活用されるよう、今後の協力をお願いしたいと考えています。

２点目は、ステップ２の「各自へのタスクの割り当て」についてです。特に中小企業においてタスクを割り当てることは困難な場合が多いため、この点に関する具体的な例示や、実践を後押しするような支援があると有効と考えられます。

３点目は、人事的な視点の導入です。役割の中に、キャリアパスの策定や人事異動による能力開発といった視点を含めることは、組織として持つべき重要な能力を明確にする上で不可欠です。これを考慮いただくことで、フレームワークの内容がより充実し、深みが増す

と考えられます。

○ ご指摘は、本フレームワークが策定された後には、各省庁の基準において、これを基に人材を確保するよう明記していただくなど、指針として活用されるべきという趣旨と理解いたしました。

事務局
○ ご指摘の点についてお答えします。
まず各省庁との連携については、ご期待のとおり、本フレームワークが省庁と民間の双方で誤解なく理解できる共通の指針として活用されることが、その役割であると認識しています。
次にタスクの割り当てに関しましては、事例が非常に細かく見えるかもしれませんが、これは特定の個人へ業務が集中することを避け、組織内で可能な限り業務を分担するという思想に基づき作成しています。実務において、事例のように広範かつ均等な分担が常に可能とは限りませんが、作成にあたってはそうした意図を反映させております。

○ 先ほど高等専門学校におけるセキュリティ教育に関するお話がありましたが、本フレームワークは大学においても活用できるものであることが期待されます。
大学は専門分野が多岐にわたるため、一部の専門学科を除き、一つの大学で網羅的にセキュリティ教育を行うことは難しいと考えられます。そのような状況でも、各大学が自身の強みのある分野で、本フレームワーク上のどの役割を担えるのかが明確になるような構成が望ましいです。今後、大学間の連携や再編が進む中で、互いに不足する部分を補い合う際にも参考となるフレームワークとなることが求められます。

○ 事前の説明内容を短期間で反映いただき、ありがとうございます。申し上げた内容がかなり反映されていると認識していますが、３点ほど意見を述べさせていただきます。
まず１点目は、４ページの図についてです。ユーザー企業の IT 部門に相当する「設計・開発」と「導入・運用」の領域に、いかにセキュリティを組み込むかが重要です。現状の図では、「設計・開発」から「導入・運用」への連携が中心に見えますが、「セキュアバイデザイン」の観点からは、下段にある専門家ラインの「情報収集分析・共有」、「監視」、「脆弱性評価」が、「設計・開発」や「導入・運用」と密に連携することが不可欠と考えられます。この連携を明確に示すため、太い矢印を追加することを提案します。
２点目は、22 ページの「運用管理」についてです。こちらには BCP の観点も盛り込んでいただきたいです。
３点目は、「法務」の役割に関してです。対象を法律に限定せず、ソフトローや業界規制も考慮することが求められます。特に、個人情報保護法だけでなく、欧州のサイバーレジリ

エンス法（EU CRA）や AI 法、データ法といったサイバー・デジタル関連の法令を例示し、「サイバー」というキーワードを明確に打ち出していただきたいです。

○　３点意見を述べます。

１点目は、手引き書の 12 ページに関連する内容です。小規模事業者の多くは、「設計開発」や「導入運用」、「防御」といった役割を自組織で担うのではなく、外部に委託します。その際に重要となるのは、委託先を適切に評価し管理する能力です。これは「プラス・セキュリティ人材」が担うべき役割とも重なるため、小規模事業者がプラス・セキュリティ人材を活用して外部委託を行うという視点も、検討に加えていただければと考えます。

２点目は、本フレームワークの普及に関する提案です。本書は非常に有用ですが、セキュリティ対策に不慣れな小規模事業者にとっては、その分量が導入の障壁となる懸念があります。そこで普及策として、情報処理安全確保支援士が本書の解説者となり、事業者が自ら実施できない部分を業務として担うといった連携モデルの構築を検討していただきたいです。支援士の活用という観点からも有益と考えられます。

３点目は、７ページで示されているレベル設定についてです。今回はレベル４までが対象となっていますが、将来的にはレベル５、６、７といった高度人材、特にマネジメントや戦略を担う人材の育成・評価が課題となります。今回のフレームワーク策定にあたっても、その将来的な展開を見据えた検討が行われることを期待します。

事務局

○　まず情報処理安全確保支援士の活用に関してですが、手引き書 22 ページの図において、その点を一部意図しております。小規模組織では、経営者がサイバーセキュリティに関する高度な判断を単独で行うことが難しい場面も想定されます。そこで、外部の相談先を確保し、不足する知見やスキルを補いながら対策を進めるという考え方を、この図で表現しています。

次に、レベル５、６、７についてです。現時点では、まず人材の裾野を広げることに注力しており、その先に高度人材の育成があると想定しています。ご指摘の点も踏まえ、今後の検討課題として認識しております。

○ 以前の意見交換の際にも申し上げましたが、手引き書が特に重要であると考えています。手引き書に示されたモデルケースに自組織が明確に当てはまらない場合に、どのケースを参考にすればよいかを判断するための手掛かりが、様々な箇所に盛り込まれていると望ましいです。

一例として、資料４（別紙）の 34 ページに記載されている他の組織への展開例が挙げられます。この中で、デジタルスキルが不十分な従業員が多い企業を想定した「ケース２」のように、各ケースのポイントとなる部分が示されていますが、こうした記述をさらに充実さ

せていただくことで、より実践的な手引きになると考えられます。

○ 事前のご説明の際などに指摘させていただいた点が反映されており、感謝いたします。
今回ご提示いただいた資料のうち、小規模組織向け手引き書の 12 ページなどに示されている考え方は、非常に重要であると認識しています。特に「戦略推進・プロジェクト管理」の役割が重要です。「意思決定・戦略策定」は CIO などが担うことが多いと考えられますが、それに助言する「セキュリティ統括」の機能は、業種業態や重要インフラといった事業領域の多様性にかかわらず、各社に必ず置くべきものであり、アウトソースできない中核的な役割であると認識しています。
もし導入に迷う企業があれば、まず自社にこの「セキュリティ統括」機能を設置し、そこを起点として、業種や自社の特性に応じて必要な機能を取捨選択していく、という手引き書の活用方法を促してはいかがでしょうか。その意味で、「セキュリティ統括」という役割に焦点を当てた記述を盛り込むことも有効と考えられます。

○ 内容については、皆様が示された方向で進めることに異論はありません。
加えて、フレームワーク自体の運用ルールを定めることが重要です。例えば、JTAG 財団からもご意見があったように、メンテナンスの時期や更新の条件などを明確にした運用ルールのシートを一枚用意しておかなければ、策定後に内容が陳腐化し、活用されなくなる恐れがあります。そのための準備も進めておくべきだと考えます。

○ 繰り返しになるのですが、技術思考から組織運用という視点からの人材育成への流れにすることが大切であり、今回のケーススタディとして設定された話として、自組織、組織外、連携という視点でのコミュニケーション前提の取組にしていくというのは分かりやすいと思います。事故が起きてからの焦っての対応から、平時こその準備、ここに教育が活きてきます。

○ 資料６ページに示された概念整理の図について意見を述べます。
「役割」と「組織」を掛け合わせて「人材像」を定義するという考え方は優れたものですが、先ほどの JTAG 財団からのコメントにもあったように、この掛け算の要素である「組織」の特性を明確に定義できる企業は多くないのが実情ではないでしょうか。この点については、多くの方が同様の認識をお持ちだと推察します。したがって、手引き書は、各企業が自組織の状況をこの図に当てはめて整理できるよう支援する内容でなければならないと考えます。今後の手引き書の見直しにあたっては、この掛け算の式を成立させるための説明となっているか、という観点でご確認いただけると幸いです。
時間が超過しておりますので、事務局におかれましては、本日いただいた多くの意見を踏まえて、修正をご検討いただけますようお願いいたします。

(3) パブリックコメント（案）について

事務局より、資料５に基づき、パブリックコメント（案）について説明があった。

○ 一点確認させてください。パブリックコメントとして公開されるのは、本資料のどの部分になるのでしょうか。

事務局

○ 手引き書については、直接の意見募集対象ではございません。対象となるのは、本資料で申しますと、

○ ３ページ目以降が対象で、手引き書は対象外である点は理解しました。ただ、手引き書を今後用意する予定がある、ということ自体は周知されるのでしょうか。

事務局

○ 資料５ページに記載の活用方針の中で、手引き書を策定する旨を明記しております。また、先ほどご意見があった点にも関連しますが、今後の方向性として、不断の見直しを前提とするといった方針も記載しています。

○ 手引き書の具体的なイメージまでは示されない、という理解でよろしいでしょうか。

個人的には、手引き書のイメージが少しでもあると、より良い意見が集まるのではないかと考えております。委員の皆様はいかがお考えでしょうか。

今回の検討会では幅広く議論を重ねてきましたが、パブリックコメントで公開されるのは、主に 13 の役割を定義したフレームワーク本体になるかと存じます。意見を寄せる方々には、細部についてのご指摘だけでなく、これをどのように活用したいか、あるいはどのように役立ちそうかといった、活用方法に関するご意見をいただくことが非常に重要です。そのために、何か参考になる情報を示すべきではないか、という点についてご意見があればお聞かせください。

○ 手引き書の目次案だけでも示すのが良いのではないでしょうか。

○ 現状、手引き書の目次はありませんね。目次を示すとすれば、どのような内容が考えられますか。

事務局

○ 本日の資料で活用例としてお示しした５ページほどのスライドがありましたが、例えば

そのような内容が該当すると考えております。

○ 参照資料として、ぜひその方向で検討したいと思います。

飯田内閣サイバー官
○ 確認ですが、本日の資料は公表されるという認識でよろしいでしょうか。もし公表されるのであれば、その公表資料全体をご覧いただいた上で、このような内容を盛り込んでほしい等ご意見をいただく形で良いのではないでしょうか。

事務局
○ はい。公表する会議資料への参照を促し、それと連動させる形でご意見をいただく、という方向で進めたいと存じます。

○ 皆様、よろしいでしょうか。
それでは、パブリックコメントについては、本日議論したとおり、公表される本会議の資料を参照いただくことで活用のイメージを持っていただき、その上でご意見をいただくという方向で進めることといたします。

（3） 閉会
事務局
○ パブリックコメントにつきましては、本日いただいたご意見を反映して手続きを進めてまいります。
会議資料の公表については、この場限りのものを除き、必要な調整と確認を経た上で、後日ウェブサイトに公開する予定です。
今後の予定ですが、パブリックコメント期間を経て、年度内にもう一度、最終回となる検討会を開催いたします。時期は３月下旬頃を想定しており、現在、個別にご日程を調整させていただいております。詳細が決まり次第、改めてご連絡いたします。最終回では、パブリックコメントの結果を踏まえた最終的な取りまとめについてご議論いただく予定です。
以上をもちまして、第３回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を閉会いたします。本日は長時間にわたり、誠にありがとうございました。

以上