

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2回）議事要旨

1. 日時

令和7年12月18日（木）14時00分から16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
辻 伸弘	S B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)

中間 俊英	株式会社ラック イノベーション領域 常務執行役員
仲上 竜太	株式会社ラック イノベーション領域 プロダクト統括部 統括部長
古川 佳和	大阪商工会議所 経営情報センター 次長
長田 悠城	パーソルキャリア株式会社 doda エージェント事業部 IT 部 ゼネラルマネジャー

(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
仙崎 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、会議を始めさせていただければと思います。本日、第2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にお集まりいただき、ありがとうございます。はじめに、開催にあたりまして出席状況をご報告させていただきます。本日はすべての委員にご出席いただいております。

##### (2) 議事

###### (1) ヒアリング

事務局

○ 本日は、3つの異なる企業や団体の方にご参加いただいております。今回検討しておりますフレームワークにつきまして、人材像の検討などに資する具体的事例ですとか、活用場面における課題や示唆などを伺うことを狙いとしております。

1件目は、セキュリティベンダーというお立場から株式会社ラック様。2件目につきましては、中小企業をご支援されているお立場から大阪商工会議所様。3件目につきましては、求人市場といった観点からパーソルキャリア株式会社様にご登壇をいただければというところでございます。それぞれのお立場から取組事例などをご紹介いただくとともに、こちらで検討中のフレームワークに対しまして、現場の目線から見たご意見やご要望などをお伺いできればと考えております。なお、ヒアリングにつきましては、本日に引き続いて、年明けの次回の検討会でも実施する予定でございます。ヒアリングなどからいただいたご意見などを踏まえて、今後の議論の深化につなげてまいりたいと考えております。以上でございます。

###### (ア) 株式会社ラックからのヒアリング

中間 俊英 イノベーション領域 常務執行役員及び仲上 竜太 イノベーション領域 プロダクト統括部 統括部長より別紙1に基づき説明があった。

(イ) 大阪商工会議所からのヒアリング

古川 佳和 経営情報センター 次長より別紙2に基づき説明があった。

(ウ) パーソルキャリア株式会社からのヒアリング

長田 悠城 doda エージェント事業部 IT 部 ゼネラルマネジャーより別紙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。

○ パーソルキャリアにお伺いしたいんですけれども、先ほどグラフを見せていただいて、2023年くらいから2025年という形、約2年でだいぶ増えているというところがよくわかったんですけれども、特にセキュリティエンジニアみたいなのところというのは、0.2%で、情報通信業は7%と先ほどデータがありました。そういうのは似たようなWebエンジニアとか、そういったところからサイバーセキュリティの方に、逆に言うと職能幹旋というか、そういうこともあるんでしょうかね。逆にサイバーセキュリティって、割と学際的というか、いろいろな領域に渡っているんで、他の業種の方も、ある程度上限年収の高いところに移っていくというのは、ありなのかなと思って、そういったところは、何かご支援とかされているのでしょうか。

パーソルキャリア株式会社

○ やはり、アプリケーションの部分でも、セキュリティに絡むところは当然多分にございますし、インフラは先ほど申したとおり、サーバーやネットワーク、クラウド関連でも、いずれでもセキュリティにチャレンジできる、そういうのはございます。そのため、積極的に、こういった市場ニーズが高い職種に対して、職業紹介をしていくということは、本人の希望を踏まえた上ですけれども、積極的に行っております。

また、求人数がこれだけ伸びているということで、やはり今のタイミング、企業様が、本当に人が足りないと言っているんで、個人の方の活躍の余地が大きいですよね。やはりそこで、セキュリティとしての一步目を踏み出すことによって、数年後、大幅なスキルアップであるほか、本人がご希望をされるのであれば、積極的に職種の越境でのご支援というのは、させていただいていますし、できてもいる部分もございます。ありがとうございます。

○ ラックにお伺いしたいと思います。資料1の14ページ、最後のところですが、コンピュータサイエンスを基礎としてということで、皆様のように最前線に実務を重視して、活躍されている組織で、あえて基礎の大事さというところを挙げられているところを、私は逆に興味を持っていました。実務が大事だというのは、どの方もおっしゃっていたこと

だったので。教育法人である組織として、大学専門教育組織の意見も聞いた方が良いというお話もいただいていた、そういうふうな考えになった経緯ですとか、ご経験ですとか、少しお話していただければありがたいです。

#### 株式会社ラック

○ コンピュータサイエンスと書いているのは、これはかなりあえて書いているところがございます。昨今、コンピュータ環境の仮想化が進んでいて、自分でメモリをつけたことがないコンピュータエンジニアが増えてきていると言えるかと思えます。そういった中で、やはり手触りのないコンピュータ環境が最近若手エンジニアの中に見られるようになっており、我々としては、サイバー攻撃に対しては、特に脆弱性への攻撃ですとか、攻撃のパケットのテキストがなぜ通るのかといった部分については、コンピュータのエンジニアリングというか、コンピュータの構造をしっかりと理解していないと、攻撃そのものがなぜ成功するのかというのが理解できないというような状況になっています。

単純にクラウド上でコンフィギュレーションして、プログラムが動いて、何かシステムができたような気になっていると、それだけではサイバーセキュリティはなかなか難しいということもあり、やはり学生時代でのコンピュータカリキュラムの経験ですとか、セキュリティ資格の前に情報処理技術者資格の基本的な部分ですとか、応用的な部分をしっかりと学んでいただくというところについても、我々としては重要視しているというところがございます。ありがとうございます。

○ ラックとパーソルキャリアにお聞きします。ラックへはまず、セキュリティ部門の方、社内の人材育成のところであります。主にセキュリティ部門の方の育成みたいな話かと思うんですけども、多分、ラックの社員の半数程度はセキュリティ部門ではない方もいらっしゃると思いますが、そうした方々のセキュリティに対する取組についてお聞きしたいです。

パーソルキャリアには、今、こちらの方で数字を出していただいたんですけども、アメリカの方で、CyberSeek というサイトがありまして、そちらの方で、セキュリティの求人数というのは、ジョブオープニングで、50 何万件ぐらいとかありますので、それと比べると、正確には分かりませんが、おそらく2桁程度違うなど、doda のお話とは大きな乖離があるように思います。そのところというのは、日本で拾えていないのかとか、実際にそれほど、そんなに人数が大きいのかみたいな、それは、ギャップがあるところについて、お考えあればお聞きしたいということになりますので、以上です。

#### 株式会社ラック

○ セキュリティは、実践も含めてやっているけれども、実際にはどうなんだというところかと思うんですけども、まず、入社してすぐに若手のエンジニアが経験するのは、共通的

なカリキュラムがございまして、当然、そのビジネスマンのところであるんですけども、システム開発を通して、プログラミングですとか、コンピュータがどういうふうに動いているのか等を、Java のプログラミングなど、そのプログラミングを通じて、実践的に体得していただくというところを、共通カリキュラムとして設けております。

その先には、実際にそのものづくりの後に、サイバーセキュリティということで、攻撃の体験ですとか、こういったような SQL インジェクションが、どのように刺さるのかといったようなところも含めて、実際のメンバーにもそういった検証を行い、実際に作るだけではなく、それを守ることを観点としながら、いわゆるシフトレフトですとか、セキュリティ・バイ・デザインという考え方も含めて、システムインテグレーションのメンバーにも、セキュリティをしっかり理解していただいた上で、システムインテグレーション側のメンバーに伸ばしているのは、どちらかということ、プロジェクトマネジメントですとか、そういった開発工程のスキルに、専門性を伸ばしていくとなっております。

○ 今回、こちらの人材フレームワークで、例えば開発のほか、専門性マネジメントみたいなもの、一応人材層としては述べられているので、そういったところに近いようなイメージの育成になりますか。

#### 株式会社ラック

○ あと、やはり PM ですとか、開発工程を踏まえているということも大事なんですけど、やはりセキュリティのボキャブラリーが通じるというのが、非常に言われている会社として重要視はしております。SI だからといって、セキュリティのトレンドですが、トピックについていけなくていいというわけではなく、やはり専門的な攻撃の細かいところまでは分からなくても、自分たちの実践にどういう影響があるのかとか、そういった部分は分かるように今しているかということなんです。

#### パーソルキャリア株式会社

○ まず、国内市場の転職に特化をしている部分なので、グローバルとの求人との差みたいなところを大きくベンチマークしているわけではないです。特徴としては、とはいっても、少しオープンポジションであるほか、少し網羅的に採用しているという部分はあると思います。

セキュリティだけでなく、他のものも含めてなんですけれども、やはり細分化することによって、求人数自体は確かに伸びると思うんですが、そうしてしまうと、最後、お伝えをしたとおり、かなり限定的な方の採用になってしまう。そういったことを避けていくために、多少ジェネラリストを取っていきたいという気持ちもあって、ポジションを少し広めに出していて、求人数自体はなので伸びないという可能性はあると思います。

あとは拾いきれていないというところはあると思っています。実際に企業様から案件を

いただくときも、海外ではこういったような形なのでとか、これだけポジションとか可能性があるよねという話は、特におっしゃられておらず、あくまでも国内の人のパイをどうやって取っていくかというところだけに目を向けているケースは非常に多いため、先ほど海外との比較でいうと、これだけ差があるよということをそもそも知らない人が採用されている、個人・法人ともに多いというのは、事実あるのではないかなと思っています。

○ まずラックの方に聞きたいのが、コミュニケーションとつながるよというのが、すごく気になると思いますが、いろんな取組をされていて、僕はもうずっと学生出た頃から、ラックは国内を代表するセキュリティ会社だと思っていましたが、いろんな取組をした上で、いろんな人材を育成していくことを、どのように効果測定されているか、測定方法で何か教えていただけますか。

#### 株式会社ラック

○ 効果測定なんですけれども、これはなかなか難しいところであると思います。表に出てくるのは、資格の部分だったりとか、どこかで賞を取ってきたり、社内 LT、それから外部のイベントで登壇したりといったようなところで、ある意味、目立つ人というのが出てくるところというのが、第三者から見たときの、こういったスキルアッププログラムの成果として、出てくると思います。ただ、そのような部分には、スキルアッププログラムだけではなくて、個人の研鑽の部分も非常に多く含まれているので、ある意味、個人で研鑽したいという人が、社員相互で受けられるようなプログラムで、お互いに伸びていくということが、効果として出てきていると思います。

やはり我々としても、組織の管理観点で、マネジメントの中で、従業員のスキルをしっかりと把握して、伸ばしていきたいというところが、思いとしてはしっかりあって、先ほどご説明させていただいた、JTAG というのはその一環ではあるんですけれども、必ずしも手触りのあるスキルが計数に現れるかというところ、そこはなかなか難しいところです。ここはやはり、上司の理解ですとか、上司がメンバーのスキル、それから興味の部分をしっかりとりえて、業務にアサインして、それが目標管理としてしっかりと成果につながっていくというところが、マネジメントサイドの腕の見せ所、というところになるかと思っています。

○ 分かりました。目立つ人だけが評価されるというのは、縁の下の力持ちの人たちが輝けないというのは、避けたほうがいいかなと思っています。結局、この人がいくら稼ぐようになるのか、いくら稼ぐ人を取りまとめることができるのかというのを、明確に示すような人事制度の部分でも、必要かなと思いました。はい、ありがとうございます。

大阪商工会議所に聞かせていただきたいんですが、中小企業に対して実証事業をされていたと思うんですけれども、その時の 30 社中 30 社が何かしらの攻撃被害になっていて、5 社が通信を繰り返し、C2 とかの通信を繰り返していたと思うんですが、これはどれくら

いのインパクトがあるものだったのか、示すことができますか。例えば、被害額はどれくらいになるのか、対応費用はどれくらいなのかというところまでは、トレースはされていないですか。

大阪商工会議所

○ そこまでトレースしていません。うちのところは何も起きてなかったと思われていたのが何か起きていた事実が分かったということと、あとは、30社中で30社すべてで何かが起きていたというのが、やっぱり一番大きいところかなというところですか。

○ 何社に1社がサイバー攻撃の被害、ランサムや被害を受けていますけれども、目にする機会が多いのですが、どれくらい費用がかかるのか、放置した場合に自社にどれだけの損失があるのかというところまで伝えることができたほうが、特に大阪の皆さんに刺さると思いますか。

大阪商工会議所

○ よく分かります。実際に5社もそうなんですけど、結局、被害がなかったというか、被害が起きていたことが分からなかったんで、この企業の方々の認識としては、被害はゼロだったということなんですよ。そういったところが実証実験によって、分かったことによって「ありがとう」のひとことで終わります。その被害の額は正直見えないんですよ。

○ パーソルキャリアにお伺いさせてください。資料3の7ページのサービスのご紹介のところなんですけれども、こちら、御社では大分類というところで15職種や、あるいは中分類の13職種、セキュリティであれば2つとして、細分化されているとお話いただいたと思います。これはどういう基準、どういうポリシーに基づいて、区別をされて、分けられているのかお伺いしたいなと思いました。

というのが、例えば、いわゆる国内外の基準、NICEフレームワークであるほか、国内であればIPA基準とかをベースにして作られたのか、あるいは求人市場に存在する求人数とかを分析して、上から多い順に並べた結果なのか、どういう基準で作られたのかお伺いしたいです。

ご質問の意図といたしましては、本来、国内外の基準だったり今回NCOが作ろうとされているフレームワークであったり、求人市場での利活用を想定して作られているはずですが、先ほど申し上げた2パターンの後者（市場の求人数を分析）であった場合に、実態としてこれらが現場で使われていないとなると、意味がないのではないかと危惧します。この場合、どういう基準であれば使いやすいかといった観点で質問させてください。よろしくお願いたします。

パーソルキャリア株式会社

○ もちろん、各種、世の中にあるフレームワークであるほか、何かしらのデータや区分ということは参考にしているものはございます。ただ、それだけに準拠しているというよりは、登録をされる個人のお客様が分かりやすいかどうかというのは重要視しております。

結局、専門家ではない個人の方々が、ご自身が自分の職種は何ですかと問うときに、それが分かりやすくなかったら、あまり意味がないとなってしまいますので、世の中にいる個人の方が、パッと見たときには、自分はこれではないかと思えるような、遊びというか、余白を設けて設定をしているということはありません。

また、こちらに関しては、何か新しいものが出てきたから、すぐに変更をかけている、定期的に職種分類を変えているということはありません。そこについては、職種が新しくできていく、消えていくということが多分に起きている時代であるため、都度更新していくことが、どうしても難しいということもあります。もう一点、我々dodaとして展開させていただいておりますが、他の職業紹介の同じ生業をしているサービスも、世の中に多分展開しているため、他社のカテゴリの部分であるほか、dodaだけがこうあるべきだとやっても仕方がないというところがあるので、人材紹介事業全体のところである程度の基準に揃っていくということが、現状であると思います。活用されるという観点でいうと、やはりそのフレームワークを使っていくのは、人材紹介の立場からすると、個人のお客様、ないし法人のお客様になってくるので、やはりその個人、法人の実際に利用される方の立場に立ったときに、分かりやすいのかであるほか、その意味合いが把握できるのかという観点、そこを組み込んでいくというのは、絶対的に必要かなと考えております。

○ さらに聞かせていただいて恐縮なんですけれども、他の事業者様と暗黙の了解で似たような粒度感になっていくとおっしゃったと思いますが、やはりそれは、いわゆるデファクトスタンダード的な形で皆さん共通でお使いになっているベースとなるものがあるのか、あるいは、各事業者様それぞれが独自に分類を進めた結果として、皆さん同じような粒度感になっているというのが実態ということになりますでしょうか。

○ 全体でいうと、まず共通の何かがある、もの差があるかという、ないです。これは各社が、求職者から見たときの分かりやすさというところから、積み上げていって分類をしていました。例えば、私が紹介をやっていた最初の頃の98年とか2000年ぐらいの頃というのは、エンジニアって社内SEという括りと、SIerというシステムエンジニアという括りしかなかったんです。これが徐々にインターネットになってWeb化されていったときに、初めてどうやらメインフレームの話とオープンは違うねと分かれていき、オープンもWeb化していっているのだから違うという話で、分類を増やしていっています。世の中の職種の定義が増えていったのに合わせて増えていったというのが経緯です。なので、結構各社が、これが求職者・求人者としゃべっていて分かりやすいものから、どちらかという分類を組み上

げていったものが、大手はおおむね揃っている状態であり、結果的に似たようなものになっています。物差しとしては必要なので、求人者・求職者としゃべるときに、こういうフレームワークがあって、例えば、分かりやすく、こういう資格がある人のこのレベルの人が欲しいんだよと言われると、ああそうだねと言って分かりやすくなるので、どのような人がターゲットなのかは分かりますが、「遊びをあえて残した」というお話のとおり、厳密に定義したスキルセットの人材を求められることはありません。結果的に「こういう人でもいい」「ここまでなら許容できる」といったやり取りが発生するため、厳密化すればするほどミスマッチするという可能性が出てくるので、ここの話になっているというところです。

○ 大阪商工会議所にお伺いしたいんですけども、(資料2)最後のページ、絵に描いた餅でクスッと笑われたというのが、非常に我々は反省しないといけないなと思っています。最後のところに、やっぱり窓口となるような人材が必要ということが書かれているんですけども、じゃあ成功というか、うまくいっているお会社というのは、相談の窓口というのは、どういった形で置かれているのかとか、もう少し具体的な事例というか、教えていただきたいと思います。

#### 大阪商工会議所

○ ちょっと今日の資料にはありませんが、私どもがこのアンケートを取ったときの項目のひとつに、例えばセキュリティに関して、最初に窓口としてどこに相談に行くのかという設問がございました。さて、どこでしょうとなったときに、一番トップは、やはり出入り業者なんです。私どもみたいな商工会議所だったり、IPA だったり、警察とかいう公的機関は非常に少ないといったような事情でございます。とはいえ、どこであっても窓口となるような人や場所があるだけで全然違うかなと思っていて、何もなくて、どこに相談したらいいかわからない、というのが一番困るなと思っています。

○ パーソルキャリアに少々ご質問なんですけれども、(資料3)スライドの10枚目のところで、doda 登録における IT 技術者は5%で、セキュリティエンジニアは2.0%であるんですけども、これは実際に存在する数の割合からすると乖離があって、IT 技術者の方がだいぶ流動性が高いのかなと推測するんですけども、実際、IT エンジニアって、昨今、生成 AI が出てきて、いろいろコード作れるなど、そういう話も結構出ているので、そういう意味では、AI の影響によって、例えば、要件定義など設計フェイズに近い職に転換するような意図が見られるとか、そういう傾向があるのか、その辺あたりの知見があれば、ご教示いただければと思うんですけども、いかがでしょうか。

パーソルキャリア株式会社

○ AI 技術が台頭してきたことによって、個人側のご希望の志向性の変化などがあるかという感じですかね。はい。それは間違いなくございます。まず、ご質問からずれてしまうことなんです、このセキュリティエンジニア 0.08%という結果は、あくまでもセキュリティエンジニアとして登録をしているものだけをピックアップしています。なので、他の部分でいうと、サーバーエンジニアやネットワークエンジニア、ないしは社内 SE の中、ないしは IT コンサルの中にもセキュリティ知見を豊富に持っている、世に一般に言うセキュリティエンジニアに該当される方は、おそらく含まれていると思われま。ただ、ではそのコアスキルって何なのかとなった時に、自分はサーバーのところが強いのねとか、やはり事業会社の中の IT 部門をやっていて、セキュリティだけではなくて、その他のすべての IT 戦略の部分を書いているので、という登録がある部分がございます。なので、純度としてはこの数字になるという形なんです、世の中に 0.08%しかいないかと言われると、もう少し引き上がるかなとまず思っただけだと良いかなと思っっています。

AI 等々の台頭、新しい技術の登場によって、個人の志向性の変化が出てくるかというのは、これはもう日々感じているところなので、やはり何かしら転職をされたい、キャリアを考えたいと思われる場合というのは、何か不安であったりだとか、ご懸念があるということになってくるので、自分の仕事が奪われるかもしれないという部分だとか、このままだと、給料がどんどん上がらなくなるかもしれないとか、立場を脅かされるかもしれないというような、少々こう、切迫感のようなところを起点に志向性が動いていって、考えも変わっていったりとか、キャリア選択を、職業選択をされる方も多分でございます。そのため、昔よりもさらに AI が出てきたことによって、それを加速しているかなと思っっています。ご回答になってますでしょうか。

○ であれば、セキュリティという条件の良いお仕事も選択肢にあるよ、と勧めると、多数がそちらに転換する、ということはあるのでしょうか。

パーソルキャリア株式会社

○ セキュリティどうですかという話をご提案すると、個人の方がそれになびくかどうかですかね。どれだけやはりセキュリティニーズが高いかであるほか、チャンスがあるよという話を伝え、個人の方が不安に思っていることを、いかにワクワク感を持っていただくか、自分のキャリアや仕事に誇りとワクワク感を持っていただくか、この転換点を作ることが、世の中の就業人口の人たちが豊かに働いていくことになると思っっています。そのため、それはセキュリティのほか、世の中から求められているものになったときのワクワク感を想像させる、そのチャンスは積極的にやりたいなと思っっています。

○ 大阪商工会議所の件ですが、(資料 2) 3 ページのところ、取引先で攻撃があつて被

害を受けた場合に、取引先の賠償を請求するのは 47%で、取引を止める・停止が 29%ということがある一方、過去に発生した大手自動車メーカーに関するサイバー被害については、発注元の自動車会社の幹部が現地へ赴き支援を表明したような、ああいうような動きもあったりして、現実的に中小企業自身が自衛すべきと言いつつも、やはり現実的に 100%はならないです。その中で、どういうふうなことをすれば、やはり中小企業としてやるべきことはやるけれど、それでも事件が発生した場合に、どういうふうな人材がどういうふうに動いていかなきゃいけないのか、というのは非常に重要なと思うんですが、そのあたりで何かお考えがあるでしょうか、という、何かヒント及び悩み等はございますか。

#### 大阪商工会議所

○ このアンケートを取ったときと今とかなり問題意識というのは違ってきていると思っております。このときは確かにこの 47%が、損害賠償するぞと言いながら、これとは別にサプライチェーン上にある上位の企業にヒアリングをしたことがあるのですが、その企業が取引先に対してセキュリティのチェックリストをつけてくださいと求めたときに、100 点満点で 30 点でしたと。では 30 点だったらどうするのかといったときに、やめるんですかと言っても、やめられないんですよ。ではそこを引き上げるのに、どうすればいいんですか。それは自助努力ですか。それとも何か協力するんですかとなったときに、結局、協力せざるを得なくなるんですよ。このようなサプライチェーンにおける被害があった場合も、自社で、例えばこれを取引やめることによって、むしろ自分たちも被害というよりも本当に商売としてうまくいかなくなってしまう現状もわかっていて、今後はむしろみんなで一緒に対策を考えましょうと。この際、まさに国が取り組んでいることかと思うんですが、みんなで一緒に対策を考える、というように持っていけないといけないと思っています。もしも、同様のアンケートを取ったらとしたら、47%が、損害賠償するぞ、という数字が減っていることを期待したいと思っています。

○ 2つ目なのですが、今のお話を受けても、いざというときの、自助・共助・公助、特に共助、サイバーセキュリティってどのようにやっているかって非常に課題だと思うんですが、こういう人材の観点では、好機になるかもしれないなどは期待をしております。2つ目なんですが、最近、AI 関係が非常に活発になって、1つの課題としては、キャリアラダー、つまりキャリアパスの階段が消滅し、喪失してしまうという問題です。

普段、いつもであれば新人で入って、この業務をやって、これを覚えて、次に行くという部分から、AI にやらせればよいということで、そのあたりをトレーニングする場所がなくなっているという問題。これは逆に言うと、企業サイドからすると、やはり効率で求めると、そのようにせざるを得ないなどというのがあると思うんですが、一方、パーソルキャリアのようなところは、人の需給の動向がいろいろ出てくると思うわけです。まだまだそこまで至っていないところには、キャリアパスを、先ほどの 24 歳の方のポテンシャルの部分で転職

をされたというようにもあったように、そのあたりを埋めていくような、そういうような動きですとか、お考えですとか、そのあたりはお聞かせいただけますでしょうか。

パーソルキャリア株式会社

○ 確かに AI をはじめとして、オペレーションの部分が大きく変わっていくことや、育成の体制が変わっていくことは、感じている部分があります。一方で、「人は不要である」といったニーズはほぼ出ていないのですね。要は確かに若年層のところの育成部分のコストはかかりますし、確かにそのような部分は、AI に置き換えることによって、人材費を削減することもできると思いますが、やはりどこの企業も人が欲しいという状態にはなっているんです。それは人でしかできないことであるほか、絶対にシステムや AI に置き換えられない部分が残っていくと、企業も含めて我々も思っているからです。確かに世の中の変化として、どこの年齢、年収、キャリアケースのページでご支援をしていくかということは、今後考え続けなければならないなとは思いますが、例えばそれが若年層の方のキャリアパスがなくなるので、そこを非注力として、中堅のところの即戦力人材に触れようとか、あまりそういうことは考えていないので、これはどこの紹介会社もしっかりとセグメントを分けて、若年層は若年層なり、今のやり方のご支援のスタイルがある人たちというのを、少し細分化するような形で、ご支援方法を確立していく方向が強いかなどは思います。

○ 何でそういうふうに思ったかという、先ほどの大阪商工会議所のお話の絵に描いた餅の話なんですけど、やはり絵に描いた餅を実体のあるものにするためには、そのような人が動いていかなきゃいけないって、現実、中小企業のそのようなことがお金になるかどうかは別として、一番勉強になることは事実ですよ。なので、本来であれば年層及びリタイヤをされるような方のセカンドキャリアパスなんかは、プラス・セキュリティの部分でつないでいくというような発想というのは、非常に重要な観点かなと思いますし、一番おそらく爆速で身につくのではないかと思います。そのため、何かそのような仕掛けというんですかね、何か誘導も何かできるといいなと思いました。

○ 質問なんですけど、ユーザー企業側とベンダー側とでは、やはり同じ項目であったりしても、求められる内容やスキルが少々変わってくるんじゃないかなと思ってまして、その辺の見分け方などをどのように捉えているのでしょうか。一つのエンジニア枠には括られないのではないかなとも思いますが、その辺りのご見解はありますか。

パーソルキャリア株式会社

○ おっしゃるとおり、括られないです。全然違う。やはりその事業者側のユーザーサイドか、それを受注しているか、それを受けているかという、商流も IT の場合だとございまして、アプリのエンジニアだとしても、上流なのか、中流か、下流なのかという、工程の差も

当然ある。あと開発等とインフラも含めて、技術領域も全く異なってくるため、それを一括りにして、アプリがインフラだというのは少々雑ですし、それだけではマッチングがなされないとは思っています。なので、どう見立てているかということ、我々の場合ですと、法人と個人で、専任で分けていますので、法人の場合に言うと、例えばセキュリティの中だったとしても、それが CSIRT のところなのかだったりとか、ガバナンスの体制のところを突き詰めたいのかだったりだとか、SOC なのかだったりとか、そういうフォレンジックなのかとか、何のセキュリティのところを求めたいですかということも、実際にヒアリングと対話で埋めていく、その内容の解像度を極めて高めた上で、求人内容に落とし込んでいくという、入り口は同じエンジニアかもしれないけれども、求人詳細やその補足で埋めていくという形になります。

個人に関しても、やはり職種のヒアリング、ただ個人の方が自分が何をやっているかということと言語化するのが結構難しかったりするので、オープンとクローズドでも当てていって、これはできるのかできないのかであったりだとか、どの高さまで対応ができるのかということ、経歴のヒアリングだけではなくて、業務内容のヒアリングをして、スキルセットを見立てていくという形だと思います。ただ、これは大きな問題としては、求人営業マンのスキルにかなり寄ってくるんですね。属人的になってしまっている、その抽出力が極めて高い人間は解像度が高まりますし、そうではない場合というのは、荒いまま出てしまうため、アンマッチが起きるとい形になるので、ここは少々属人的、個力に担保されているというのが、大きな課題と捉えていますので、今後少々埋めていきたいなと、チャレンジしていきたいなと思っているところですが、見立ての方法はこのようにやっています。

## (2) 人材像（案）の修正案及び手引き書（案）の基本的な考え方について

事務局より、配布資料（資料4・5）に基づき、人材像（案）の修正案及び手引き書（案）の基本的な考え方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。

○ それでは質疑に入ります。今後のスケジュールや進め方、ヒアリングの予定、フレームワークをとりまとめる予定など、事務局より簡単に教えていただけますか。

### 事務局

○ 検討会自体が全体で4回の開催をイメージしておりまして、今回2回目ということでございます。今回と次回の会議で、ヒアリングもさせていただきつつ、内容もだんだんブラッシュアップを進めていくというところまで進めていければと考えております。第3回（次回）の会議では、特にパブリックコメントにかけるフレームワーク案を、次回の会議で取りまとめたいと考えております。なので基本的には、今回13の人材像の取扱説明書のようなもの

をお出ししましたけれども、そこに TKS まで付いたものが、フレームワークそのものになると思いますし、多分それだけパブリックコメントされても、多分よく分からないと思います。そのため、少しこれをこうしていくという、少し文章化したようなものも添えた上で、パブリックコメントをするのかなとは考えておりますので、次回の会議で、フレームワークそのものであるほか、これをこういうふうに使っていきたいとか、そのようなものが伝わるような文章なんかも、ご覧いただくようなイメージで考えております。

この図でいうところの、第3回と第4回の間にはパブリックコメントが入っていて、そのパブリックコメントの内容を踏まえて、野心的な目標としては、年度内に第4回の会議を行いまして、この会議としては、フレームワーク案のようなところは、このような形で、というようところまで、取りまとめていくというのが、当局の考えでございます。

○ 手引き書については、最終版の手前の段階、つまり活用をサポートする手引き書（案）までは出しましょうということですね。その目標に向けて皆様からのコメントをお願いします。例えば、第3回に向けて、こういう作業をしていただくと良いのではないかなど、いかがでございましょうか。

○ すみません、今のご指摘からずれてしまうかもしれないですけども、先に申し上げます。議論が、実務者が足りないという目の前の問題、どう解決するかというところに、まだすごく強く意識されていると感じております。やはりフレームワークは、長期的な視野で活用できるものであってほしいという思いがありますので、長期的に見た場合には、中核的なセキュリティ技術に関わる人材が、我が国のどこで作れるかということも、すごく大事だと思っております。特に AI 技術が進んで、オペレーションもどんどん変わってくるときに、そこを追従できる人材がいないと、結局、外国の技術を使うなど、そのような話が出てきてしまう。

先ほど、パーソルキャリアのお話で、24 歳の方が、即業務経験があって、年収が 110 万円上がってよかったという話があったんですけども、あの事例を詳しく見ると、海外製品の輸入販売を行う商社となっていて、結局、海外が儲かっているところで、それを販売している業務ということになっているので、技術のコアなところに関わっているわけではないという、そんな見方もできてしまうかなと思いました。ですので、私も研究室で学生が卒業するときに、みんなセキュリティ関係の業務に就くわけではない。どうしてかと、特に創造性が高く能力が高い学生ほど、そうではない傾向がある気がしてしまっていて、将来性を感じられないといえますか、この資料を見ますと、研究開発とか高度な人材が活躍しそうな、というのが見えてこないところを、すごくよく感じておりまして、学生がこのフレームワークを見て、セキュリティ人材として生きていきたいなと思えるようなものになっていると良いなということを申し上げたいと思います。

○ 個人的には、別の角度でも表現できる気もしますが、そこは対応したいと思います。

○ 第1回から第2回にかけて、いろいろと中身を、1回目の部分と見比べながら、いろいろ気づきが出てきているんですけども、私の立場からすると、やはりユーザー企業の観点で、どうすべきなのかということコメントしておきたいと思います。

企業のサイバーレジリエンスの底上げをするためには、圧倒的に多いユーザー企業のレベルを上げていく必要があるんだろうとっております。先ほど少々大阪商工会議所の話もありましたけれども、やはり、ユーザー企業とベンダー企業で、分業をしているという実態は、見落としてはいけないところです。ここの1から15も、先ほど私も質問しましたが、ユーザー企業で求められるところと、ベンダーで求められるところって、若干やはり違うんだろうなというところもあります。同じ、①から⑩に関してです。あと、予算だったり権限だったり、あとはその全体のリスクマネジメントの中からの役割というようなことを少々意識して考えるべきかなとっておりますので、例えば、本当に設計、開発においては、セキュア・バイ・デザインだとか、セキュアコーディングということユーザー企業はちゃんとできているか確認する必要があります。しかし、実際にベンダーがしていたら、そこで実施するという、まさにエンジニアリングの世界が必要になるというようなことでございますので、少々そういう意識を持った上で、見ていかないと、せっかくいいフレームワークを作っても、見落とすことになるなとっております。そのようなものを考えると、例えば、ERPパッケージを入れるのであれば、セキュリティ要件をちゃんと、要件とか仕様でまとめるのはユーザー企業かもしれない、その実装のほか、それを実現するという、エンジニア部門は、ベンダーとか、クラウドだったら、クラウドが全部セキュリティの準備はあるけれども、それをどう使うかというのは、ユーザーの責任なわけなので、このようなところを、少し大雑把さがないような形で、資料がまとめられるといいかなと、意見を述べさせていただきます。

○ まず、人材像の修正案で、13 の人材像について、説明にある「何々相当」というのは、非常に分かりやすくいいなと思ったんですが、その後には書いてないという、13 分の1にしか書いてなくて、NICE フレームワークに対する対応ロールというはあるものの、実際それって何て呼ばれている仕事なのかなというのが、あまり示されていないなというのがあります。そのため、これがあると非常にイメージもしやすく、この職種であるというようなものが、実際に紐づくといいかなと思いました。あとは、文章を出すときに、セキュリティの人材、ユーザー企業であったとしても、ベンダーであったとしてもそうなんですけど、いろんな人材募集のページとかサイトとか見てみると、自分が応募できるのかと思えるような、ざっくりしたものがやはり多すぎます。

先ほど、パーソルキャリアの方に説明いただいた中には、もちろんミスマッチをなくすために、間口を広げているというのは、あるんじゃないかなと思うものの、意外と人事と現場

がミスコミュニケーションしていて、欲しい人材が明確になっていないというのがあるんじゃないかなと、僕は思っているんです。そのため、このような文書が、分割形式で利用者目線で使いやすいかというのが、利用者目線というのは、現場と人事が人を求めるのを出すときに、相互理解を深めて、こういう人材が欲しいんだというのは、はっきり言える。間口を広げつつも、自社に必要な人材を明確にし、「こういう人が自社にいる」「こういう人はいない」といった認識を共通言語として持てるものを目指すのが、一つ観点としていいんじゃないかなと思いました。

こういう分けがあるところで、中小企業になると、これ全部揃えられるどころか、一人すら用意できないということがあるかと思います。理想論になってしまうのかもしれないですけど、ここまでは最低限用意できたほうがいいですよ、とか。ここから外はもう外にお願いするしかないという状況を、ある程度示すことができればいいかなと思いつつも、そのような中小でこいつを抱えることを、そもそも諦めてしまうという観点も、一つあるんじゃないかなと思うんですよ。では、それではどういうふうを守っていこうかというのは、この議論ではないのかもしれませんが、そういう範囲にも及ぶ必要があるんじゃないかなと思いました。

○ アメリカとの差のような話にも少々つながるんですけども、そもそも日本のジョブ、求人票と言われているものがやはり曖昧なんですよ。なので、サイバーセキュリティ、セキュリティという言葉自体が求人票に浮かび上がらないので、多分拾われていないというのが現実だと思っています。

そこはなぜという、やはり今おっしゃっていただいた、現場の人が求めている話を、例えば我々のような紹介会社に発注するときは、人事が説明しています。でも人事の人はエンジニアの人ではなかったりするので、説明ができない。といったときの物差しになってくるというのは、すごく大事なことだと我々は思います。この手引き書の方に、例えばこの1から4をやったときに、これ、雇用仲介事業者向けってないんですけども、なくていいと思っています。なぜなら大事なのは、この1番とか2番の企業のユーザーが理解しているほか、求職者の自分のエンジニアの人材が、それができると言えるという理解が、物差しとして浸透していくことによって、逆に我々がそれを引き出していけば、求人にどんどん変わっていくと思います。その視点は非常に大事ななと思っています。

そのときに、この人材像の修正案の中の、上にどこに所属するか、のようなところを入れていただいているんですけども、せっかくこれがあるので、逆に言うとさっきおっしゃっていた、ユーザー側とベンダー側というところの役割の違いのようなのを、主な役割が補足に少々入れられると、より理解が進む使い方になるんじゃないかなと思っていました。

○ 私もユーザー企業側なんですけれども、この13の分類を見たときに、やはり一番多いのは、この⑧の運用管理のところと、設計開発のところだと思うんです。その他のところっ

て、そんなに人はいないだろうと思いますし、個々のページを見ても、NICE フレームワークにおける対応ロールというのは、両方で非常に多いということもありますので、私はそれをプラス・セキュリティという言い方をしています。インフラ系は、開発や運用を行う人材の中にセキュリティの専門家がいるんですけども、システム系にはセキュリティの専門家があまりいない中で、プラス・セキュリティと言ったときに、企業として、これ手引き書の②の中で、システム開発に携わっている業務プロセス企画やアプリ開発やデータベース構築などの人間に、どのようにフレームワークを適用するか、どのような人を求めないといけないかのような視点を、ぜひ入れていただきたいと思います。企業としては、システム系の人材は本当にボリュームが多いので、そういう考え方も必要だろうと思います。その他のところで、そんなに大企業といえども、10人も20人も当然いるわけではありませんけれども、システム系は桁違いでいます。そのため、ぜひそれは⑧⑨などという中、もう少し広くてもいいし、この後ろにもう少しサブカテゴリがあるのかというところも、ぜひ手引き書の中に、組み込めればいいかなと思っています。

○ 新分類について、やはり一つ研究というところが、少しだけ伴っているというか、分かれていたんですけども、これが非常に網羅的に、いろんなところで分散しているというのは、非常によくなったかなと思っています。我々のところも卒論の時期で、今学生たち大変な時期なんですけれども、今の学生はびっくりするくらいに、AI を活用して、コードも実はAI に聞きながら書いている。だから自分のスキルを持ちつつ、多分私たちが想像する以上に、このAI そのものをうまく活用している世代になっているので、この子たちが2年後に、実は現場に来るというところで、私自身はこのAI 進化というところ、特に2030年、2035年といったときに、10年後というところであれですけども、5年後ぐらい先になったときに、この手引き書が本当にどのような形で意味を持つのかというところは、やはり考える必要があるのかなと思っています。何が言いたいかというと、残念ながらと言うと語弊がありますが、結局それだけの活用できる人材があっても、私のところの学生も、なぜか外資系のコンサルばかり行ってしまう。魅力があるかどうかというよりは、そのゴールというところが、どうしてもお金になるのかわからないですけども、サイバーセキュリティに関するキャリアラダーが見えにくくなっているのかなと思います。だからやはり若い人たちにとっては、魅力的に見える世界でしか見えてこないというところは、私たちの課題なのかなと思っています。そのため、このような手引き書は、もちろん現状でそういうような体制のところも大事ですけども、若い人たちに対して、一つの指針になるようなものになっていく必要があるんだろうなと感じます。

○ 資料4の21ページのレベルのところですかね、こちら、前は、今回からお見せさせていただいた点、趣旨ご理解いただきまして、ご提案ありがとうございます。こちら、非常に細かい点なんですけれども、レベル3の②のところの表現なんですけれども、「全て」取

得しているという表現は厳しいとっております。前回の資料で、TKS の例ですかね、③対象の TKS の例とかを見ると、13 のスキルと書いてあるんですけども、この 13 のスキル、全ての項目/要件を満たしていないと、レベル 3 ないしレベル 4 じゃないですとになってしまうと、スキルセットの偏り次第では、本来であればレベル 3 ないしレベル 4 の最前線で活動されている方が、レベル 3 未満と評価されてしまう懸念があります。特に人事部門とかでこういうのが使われる場合、人的資源管理とかで使われると思うんですけども、そのときには、評価されるべき人が評価されなくなってしまう懸念が若干あるかなと思います。ただし資料では 3 点のうち 2 点以上満たせば良いものとしてカバーできるようにはなっているので、他の 2 点で柔軟に運用できると思うんですけども、この「全て」というのは、やはり厳しいと思いましたので、「おおむね」とか、少々緩い表現が適切と考えます。結論として、「全て」という表現は回避していただけるとよいかなと思います。

○ ありがとうございます。まだまだたくさんあると思います。

最後に私も一つ申し上げたいと思います。やはり、フレームワークと手引き書、どこまでフレームワークでどこからが手引き書かは微妙と思いました。形だけであれば、フレームワークは今のものでも十分良いと。どう使うかという手引き書がより大事だと思っています。本来、先ほどあったように、広く即戦力を集めたい。それから、長期的に育てたい。いろいろな施策をやらなきゃいけないわけです。そのような施策に、フレームワークをどう使うんだというところの観点が大事になっていると思います。ユーザー企業にとっての手引き書はどうかとか、ベンダー企業はどうかとか、ラックのように専門会社だったらどうかかなどです。それから、研究開発で長期的に、私共共通ですけど、学部や大学院で人材を育成するときに、どういうことをやっていけばいいのかという、長期的な観点の枠組みの手引き書も本来は欲しいわけです。全部を一気に作れないと思いますが、それを順次作っていくぞというメッセージを出すことが大事だと思います。それから、次にその手前に必要なのは、今回、中小企業向けの記述はありますが、その他の業種向けはまだありませんので、バリエーションをもっと増やしてもいいと思います。

最初の例は NCO 向けの手引き書であれば適切だと思います。NCO 向けなので研究開発がないのは当然でございます。では大学にとっての手引き書はどうか。これらを順に作りながら、対応する手引き書を作っていくというところを、少しでも進めていただきたいと思います。

最後に少々細かい話になりましたので、このようなことに関しては、メールなどで事務局宛てに出させていただいて、次回につなげていくという形にさせていただきたいと思います。

(3) 閉会

事務局

○ 本日の会議資料及び議事概要につきましては、前回と同様に、国家サイバー統括室ホームページに公開させていただく予定です。次回の会議でございますけれども、2月中旬頃と考えておりますけれども、引き続き、関係事業者様からのヒアリングと、パブリックコメント案についての議論を予定しております。詳細は別途調整させていただきます。以上をもちまして、本日の会議を終了いたします。どうもありがとうございました。

以上