経済産業省

第 18 回　デジタル時代の人材政策に関する検討会

議事要旨

＜日 時＞　令和 6 年 2 月 1 日(木)13:30～15:00
＜場 所＞　オンライン開催（Teams）
＜出席者＞　三谷座長、有馬委員、石川委員、石原委員、島田委員、田中委員、広木委員
＜ゲスト＞　日本電気株式会社 サイバーセキュリティ戦略統括部 エグゼクティブエキスパート
日本セキュリティオペレーション事業者協議会 代表 武智 洋
株式会社メルカリ セキュリティチーム マネージャ 竹井 悠人
＜オブザーバー＞　関係省庁

1）論点 2（生成 AI が DX 推進を担う専門レベルの人材に与える影響）に関する外部有識者プレゼンテーション①

はじめに、日本電気株式会社 サイバーセキュリティ戦略統括部 エグゼクティブエキスパート、日本セキュリティオペレーション事業者協議会 代表 武智 洋氏よりプレゼンテーションが行われ、その後、以下のような討議が行われた。

- 一般にメンバーシップ制の日本企業でどのようにセキュリティ人材を育てていくかは課題となる。どのようなスキル、ナレッジを持つべきか、日本として基準を持つことが重要。キャリアパスの定義も難しい。企業内の仕組みとして、原則は、同一職は同一賃金ということになるはずであるが、そうはなっていないので、社会的に待遇面での仕組みの浸透を待つ必要もあるかもしれない。
- 経験則ではあるが、コミュニケーションスキルは小中学校でどのように教育されていたかに影響する。その向上に何が必要かについての解は現状持っていない。接しているエンジニアとマネージャーでのコミュニケーションの仕方は異なる。言葉の使い分けの必要がある。
- セキュリティの業務はあまり定型化されていない。セキュリティ対応するなら CSIRT 構築しましょうという大枠の話に留まることが多く、何かが発生した際のプレイブックという風な詳細の業務まで定義されていないことが多い。ITU-T X.1060 のような取組のように業務とオペレーションを定型化した上で分けることができれば、一人でセキュリティに関するすべてを行うのではなく、チームで取り組めるようになる可能性がある。

- 教育者を確保するのは難しい。1つは産業と教育の流動性を高めるための仕組みを作ること。現在、大学は先生が得意な領域しかカバーしていない場合が多い。大学で教えるためには、博士号が必要であることが多く、産業界から異動することはハードルが上がってしまう。
- デジタル人材の引き止め施策としては、優秀な人の賃金をあげるというのがある。一般にマネージャーにならないと給与があがらない仕組みが多い、それでも制度内でインセンティブを与える取組み実施は可能である。
- 一般の企業はセキュリティ人材の確保にアウトソースをうまく活用することにあると考えている。さらに今後は、生成AIによるプログラミング支援ソフトではあらかじめプロンプトが用意されているので、専門性が低くてもある程度カバーできるようになる可能性がある。
- 今後、日本でも警察や防衛でセキュリティ人材を育成ということが言われている。既に海外では軍のセキュリティ業務を担当した人が民間に流れている。警察や防衛のセキュリティ人材が増えることで、今後この流れが日本でも起こる可能性がある。生成 AIにより軽微なインシデントには自動で対応できてしまうようになると、民間では高いレベルの攻撃への対応が経験しにくくなってくる。警察や防衛で、高いレベルの攻撃に対して訓練された人が民間の防衛を担う人材になる可能性はある。
- 特にセキュリティに関しては経験が重要。日本では60歳を超えると嘱託などの扱いにして人材を有効活用できていない。大手ベンダーにいるようなシニア人材の活用が鍵ではないか。
- セキュリティに関わる人材はマニュアル意識が強くなってきているように感じる。マニュアル頼りになると守りの意識が強すぎたり、本質的な倫理観を見失う。リベラルアーツのような広い視点をセキュリティ人材が持つことが重要
- セキュリティ人材の倫理観を高める施策としては、まずは倫理観などのカリキュラムが必要であり、高校や大学の授業に含める必要がある。しかし、技術集団の中では広い視野をもっている人もいれば、技術にしか興味がない人もいるので、それらを分けて評価できることが重要となると考えている。
- 組織運営側からすると、倫理観や責任についても評価に織り込んでいくこと、ジョブディスクリプション、レスポンシビリティーの明確化が効果的。

2）論点 2（生成 AI が DX 推進を担う専門レベルの人材に与える影響）に関する外部有識者 プレゼンテーション②

続いて、株式会社メルカリ セキュリティチーム マネージャ竹井 悠人氏により氏よりプレゼンテーションが行われ、その後、以下のような討議が行われた。

- セキュリティチームの人材流動性は関連部署間での個人の異動や、組織全体のセキュリティ戦略に応じた部門編成による異動等がある。サイバーセキュリティは会社の中で果たす役割は時流に応じて変化する。
- サイバーセキュリティの技術的な教育は外部教材やセキュアコーディング研修をおこなっており、セキュリティへの理解の底上げを試みている。リテラシーを高めるための個人情報保護法に関する e-learning 等も実施している。リテラシーについては特効薬がなく、徐々に高めていく必要がある。
- セキュリティ部門の評価方法の例として、インシデントに対しての貢献度やセキュリティに対する知見のように、知識面、経験面、オーナーシップ等多角的に判断されている。評価者はセキュリティ人材であり、貢献度合いを理解できる状態にすることも重要である。
- セキュリティ人材のキャリアラダーとして、CISO というのがあるが、CISO は情報セキュリティ戦略を経営視点から意思決定する役割となる。一方で開発という観点からは、リサーチ部門におけるリサーチフェローみたいなものがキャリアラダーとして必要となるかもしれない。
- 生成 AI を使うことを前提として、企業が萎縮しないで生成 AI を使っていくことが重要。
- 本質的な理解は重要だが、本質的で無い部分の学び方について、生成 AI が発達することで、プロトコルや細かい専門用語は生成 AI に質問すれば解決してしまうようになると考えている。また、テストケースを書かせる等の機械的な仕事は生成 AI ができるようになると考えている。

以上

＜お問い合わせ先＞
商務情報政策局 情報技術利用促進課
電話：03-3501-1511（内線：3971）