サイバーセキュリティタスクフォース
サイバーセキュリティ人材育成分科会（第３回）　議事要旨

１　日　時

平成 31 年２月 12 日（火）10:00～12:00

２　場　所

総務省８階　第１特別会議室

３　出席者

（構成員）後藤主査、園田主査代理、稲葉構成員、大高構成員、岡本構成員、武智構成員、手塚構成員、長谷川構成員、水越構成員

（ヒアリング対象者）一般社団法人大田工業連合会淺野氏、国立高等専門学校機構手島氏

（オブザーバー）大能内閣サイバーセキュリティセンター参事官補佐、木村経済産業省サイバーセキュリティ課課長補佐

（総務省）竹内サイバーセキュリティ統括官、泉大臣官房審議官、木村参事官（総括担当）、赤阪参事官（政策担当）、近藤参事官（国際担当）、豊重サイバーセキュリティ統括官室参事官補佐、三木地域情報政策室企画官

４　配付資料

資料３－１　大高構成員提出資料
資料３－２　大田工業連合会提出資料
資料３－３　武智構成員提出資料
資料３－４　国立高等専門学校機構提出資料
参考資料３－１　サイバーセキュリティ人材育成分科会（第２回）議事要旨

５　議事要旨

（１）開　会

（２）議　題

①　前回会合の振り返り

事務局から参考資料３－１に基づき、前回会合の振り返りが行われた。

②　構成員・関係者ヒアリング

大高構成員から資料３－１について、淺野氏から資料３－２について、武智構成員から資料３－３について、手島氏から資料３－４について、それぞれ説明が行われた。

③　意見交換

構成員・関係者ヒアリングの後、意見交換が行われた。主な意見等は次のとおり。

水越構成員：淺野氏の発表に関して、中小企業においては、工場と自宅のネットワーク環境が一体になっているところもあると思うが、実態を把握されているか。また、中小企業の中には、工作機械や生産機器がウイルスに感染していたとしても、生産に影響を与えない限り放っておいても良いと考えているところもあると思うが、実態はどうか。

淺野氏：一点目について、御指摘のとおり、同じ LAN に工場用と自宅用が接続されているという状況は存在する。そのような状況で、UTM（Unified Threat Management）を設置してアクセス可能な情報にフィルタをかけると、例えば、ゲームを禁止する設定にした場合、自宅用でもゲームができなくなってしまうことがある。二点目について、中小企業の意識は正直低く、影響があるかないかでいうと影響はあると思われる。小さな町工場においても、受発注はメールで行い、図面もデータとして扱い、それを生産用のデータに加工して機械を動作させるなど、全て電子情報を扱っており、パソコンや IT なくして町工場の機械はほとんど動かない状況である。したがって、生産機器に問題が発生して生産が止まってしまうと、それを組み込む大手の製品もつくれなくなるという事態も発生し得る。一方で、対策が重要とは思っていながらも対策がとれていない中小企業は多い。

武智構成員：町工場に限らず、OT の世界では、ウイルスに感染していたとしても生産に影響がなければ良いという一面があり、IT 環境のオペレーションとは全く異なる。コストをかけずにどうやっていくかは難しい課題ではあるが、各社の事業に合ったオペレーションをどのように実現できるか、取り組んでいるところ。

手塚構成員：中小企業では、業務用のメールのドメインはプライベートのものと同じものをそのまま使っているか、プライベートのものとは別のものを用意しているか、割合はどの程度か。

淺野氏：業務用とプライベート用でドメインを切り分けているケースが多いが、フリーメールやプロバイダのドメインのメールを業務に用いている会社も感覚としては１～２割程度はいるのではないかと思う。

長谷川構成員：サイバーセキュリティに関するセミナーやイベントを開催しても、なかなか人が集まらない。来る人は決まっていて、公共や重要インフラ、特に地銀、エネルギー系、通信系、交通系ぐらいしか参加しない。人を集めることよりも、必要な企業に必要な情報を届けることが重要であり、例えば働き方改革を切り口に、ICT やセキュリティを絡めるというのも一案。また、

セキュリティや ICT 業界の人からの講演や研修だけでは、参加者も資料を持ち帰って終わりで、次に続かない。コミュニティの形成につながるイベントを行ったり、ワークショップ形式で双方向に学ぶことのできる研修やイベントを継続的に行うことで、少しずつ必要な人に必要な情報が届けられるようになる。

また、CTF などのセキュリティ関係のコンテストにおいて、大学生に比べ、高専生の意欲の高さを常々感じている。高専生は、もともと情報系や電子工学系等を専門にやりたいという学生が多く、好きで意欲的に学習しているように感じる。好きで自発的、自律的にやっている学生に対して、いかに時期や状況に合った機会を与えるかが重要。一方、好きでない学生には、CTF のような機会があることを知ってもらい、意欲を高めることが重要。大学や高専にある学習環境を公共機関や企業が常設で持つということは困難であり、産学連携でそのような学習環境を活用することも重要。

後藤主査：「OT」は一つのキーワードになる。中小企業の場合、生産設備などの OT と直接関わる。高専においても、機械や建築を学び OT 分野で今後活躍するだろう学生がセキュリティも学んでいる。自治体においても、水道のようなインフラサービスが多く存在するが、その担当者のセキュリティ意識や教育などはどのような状況か。

大高構成員：自治体では、水道、下水道、ゴミの処理・焼却が３大制御系。その中でも特に、下水道は止まるとすぐに市民生活に大きな影響を及ぼすことから、非常に重要な、止めてはいけない制御系である。

下水道の制御系の管理は、インターネットにつないでいないため、かえって安心だと思いこんでしまっている職員もいるが、データの収集や情報の投入を行うこともあり、また、オペレーションをする人のヒューマンエラー等、リスクがあるということを認識することは非常に重要。さらに、ポンプ場をはじめ、市内に張り巡らされたネットワークも存在し、専用線で監視やコントロールをしており、支障があると人的に対応できるものとできないものがあるため、そのセキュリティはしっかり対応する必要があり、リスクアセスメントを行いながら、どのような対応が必要か検討しているところ。

制御系のセキュリティには、物理的なテロと、サイバーセキュリティとの境目があいまいであるという難しさがあるが、人的対応が必要となる部分もあるので、セキュリティ対策が必要であることを制御系の人にも意識してもらうことが重要。

稲葉構成員：スタート時の誰も人材がいないときに、どのように人材を育成するかは難しい点と思うが、藤沢市ではどのような体制で取り組まれたか。

また、人材を外から連れてくるにしても、中で育成するにしても人件費が必要になるが、市議会の予算承認が必要になるところ、普段の市民の生活において必要性を実感してもらいにくい、セキュリティに対して予算を割くこ

とについて、藤沢市ではどうやって説得したかを教えていただきたい。

大高構成員：１点目について、インターネットが社会に浸透するのに伴い、情報セキュリティということも言われるようになり、セキュリティポリシーを作成し、セキュリティポリシーに基づく安全管理措置を進めていく中で、職員の中で学び合いながらセキュリティ人材を育てていった。

セキュリティについて、内部監査を行うと、セキュリティをやっていたら仕事にならないと嫌がられた時代もあったが、セキュリティの必要性を全員で考え、だんだん理解されてくると、セキュリティにも取り組まなくてはならないという意識が芽生えてくる。そうすると、今度は、セキュリティと利便性のバランスに困っているという相談を受けるようになる。セキュリティは、利便性をある程度確保しないと守ってもらえない世界であり、現場の人たちのことを考えて、守れないレベルの厳しいセキュリティにするのではなく、ルールづくりやツールの導入など、セキュリティを守ってもらうための手段を考えることを通じて、セキュリティに関するスキルが伸びるということの繰り返しで、人材が育ってきた。職員が職員を教えるという場も非常に多く設けており、人に教えるということがスキルアップにつながる。

２点目について、セキュリティの必要性を経営層に、自治体でいえば、財政課、市長、副市長にどれだけ理解してもらうかが非常に大切で、議会への説明は、どんなに良い事業に取り組んでも、住民から信頼されなければ立ち行かないので、セキュリティが必要であるということをしっかりと説明することが必要。また、セキュリティ委員会という組織を立ち上げている。その会議において承認を得れば、市長、副市長のいる場で承認を得られた決定事項として推進しやすくなるので、こうした体制づくりも必要。どんなに人的対策をとっても、守られないことがあるという事実を突きつけて予算確保をするなど、説得できる材料をそろえることも非常に重要。

大高構成員：高専での人材育成に関して、データを分析してウイルスの種類やセキュリティホールを見つけるといった技術的にレベルの高い人材の育成や、セキュリティの必要性を働きかける人材の育成といったように、育成する人材像は種類が様々あるが、現状、どのようなキャリアパスに、どのくらいの割合の人材が輩出されているか。

手島氏：高専においては、現状、技術者の 20%をＩＴ技術者として、80%を電力や水道等のインフラ系や化学といった OT も含むユーザー系に輩出している。

セキュリティ教育に関しては、高専の特徴として、中学を卒業してすぐの学生に教えることができる早期教育のメリットを生かし、全高専生に対してセキュリティへの意識付けからスタートしている。建設系の学科の学生に対しては IT やセキュリティの授業はどうしても少なくなってしまっているが、情報系の学科の学生に対しては、できるだけセキュリティやネットワークに関する教育を厚くしていこうと、それぞれの学校において取り組んでいる。

また、特にセキュリティに特化する学科として、高知高専にセキュリティコースを開設している。一方で、セキュリティのトップ人材は、高専内部だけで育てることは困難であり、できるだけ外部の IT ベンダ、セキュリティベンダ、自治体等の協力を得ながらトップ人材を育てる環境をつくることが、トップ人材向けの教育には必要。

大高構成員：高専におけるセキュリティの教育の内容が、中小企業へセキュリティの重要性を浸透させることに役立てば良い。また、最近、小学生がウイルスを作成するという事例もあるため、高専における早期教育を利活用できるとよい。

武智構成員：セキュリティに関心のない層に対して、どうリーチするかが非常に重要な課題。大田区での取組においても、現状ではセミナーの出席率があまり高くないが、関心がもともとないわけではないので、コストをかけ、反復して取り組んでいかないと、中小企業の自助努力だけに頼るのは難しい。

淺野氏：セミナーを開催してもなかなか人が来ないという点については、対策することによって受注が増えるとかコストが削減できるとか、逆に対策をしないと受注の輪から外れるといった、費用対効果を示すのが一番わかりやすいのではないかと考えている。リテラシーの向上のための声かけをしていくことで、実践的かつ効果的な施策になっていく。

岡本構成員：関心のない層へのリーチという点については、長谷川構成員から、経営課題と絡めるのが良いのではないかという話があったが、働き方改革や売上げ向上というワードもだんだん飽きられてきてしまうので、どのようなワードが良いか、引き続き検討していくことが必要。集合型のセミナーには数に限りがあるので、動画の活用にも取り組んでいる。セキュリティに関して IPA が作ったドラマ仕立ての動画を地方で流した際、「こんなことが起きているのか」「そもそも標的型攻撃とは何だかよくわかっていなかった」というような反応もあった。１分、２分の短い動画を用意し、様々な場面で少しずつ流していくことも検討している。

園田主査代理：そもそもどのような脅威があるかというのを可視化しなければ、脅威に気づかないのではないか。例えば、ブロードバンドルーターでも攻撃検知ができ、実際にどのようなリスクが発生しているのかを可視化できれば良い。また、コンテンツメーカーをもっと作ることも重要。高専機構の専門分野別教材には、各分野に非常によく根付いた形のリスクとそれに対する対策が記載されているが、さらに、最新のリスクや脅威を専門的な知識を基にうまく実装する仕組みにしていくと、現場にもっとその知識が行き渡る。

手塚構成員：自治体、中小企業、教育機関それぞれの分野ごとの教育体系の議論があったが、それらを地域におけるマルチステークホルダーによる人材育成のエコシステムの形成という、横串の観点で捉えることも必要。例えば、高専の卒業生が中小企業に就職して、その人たちがそれぞれの企業で教育して

いくというようなエコシステムを、地域に根差した形でどう形成していくか、検討していく必要がある。

④　その他

事務局から、次回の日程について説明があった。

（３）閉会

以上