参考資料２－１

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１回）　議事要旨

１　日　時

平成 30 年 12 月 25 日（火）10:00～11:30

２　場　所

総務省 10 階　第１会議室

３　出席者

（構成員）後藤主査、園田主査代理、大高構成員、岡本構成員、武智構成員、手塚構成員、水越構成員、与儀構成員

（ヒアリング対象者）中部電力株式会社澤井氏・宮地氏、NRI セキュアテクノロジーズ株式会社渡部氏

（オブザーバー）三木地域情報政策室企画官、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

４　配付資料

資料１－１　「サイバーセキュリティ人材育成分科会」開催要綱（案）
資料１－２　我が国のサイバーセキュリティ人材の現状について
資料１－３　中部電力ヒアリング資料（配付資料なし・投影のみ）
資料１－４　NRI セキュアテクノロジーズヒアリング資料
参考資料　「サイバーセキュリティタスクフォース」開催要綱

５　議事要旨

（１）開　会

竹内サイバーセキュリティ統括官から挨拶。

（２）議　題

①　開催要綱について

事務局から資料１－１に基づき、本分科会の主査については、サイバーセキュリティタスクフォースの安田座長から後藤構成員を主査として、また、本分科会の主査代理については、後藤主査から園田構成員を主査代理として、それぞれ指名されている旨の報告があり、開催要綱（案）について承認された。

② 我が国のサイバーセキュリティ人材の現状について
事務局から資料１－２について、説明が行われた。

③ ヒアリング対象者からのプレゼンテーション
澤井氏・宮地氏から資料１－３について、渡部氏から資料１－４について、それぞれ説明が行われた。

④ 意見交換
事務局からの説明及びヒアリング対象者からのプレゼンテーションの後、意見交換が行われた。主な意見等は次のとおり。

武智構成員：Secure SketCH に登録している企業の規模はどの程度か。
渡部氏：売上高で言うと数十億円以上の中堅クラスの企業が中心であり、数億円規模の中小企業は少ない。
武智構成員：企業の規模の違いによって、とるべき施策に差異が生じる点についても議論すべき。
岡本構成員：中部電力のプレゼンを聞き、コミュニティやフェイス・トゥ・フェイスでコミュニケーションすることの重要性を再認識。企業は、サイバーセキュリティ対策に取り組む際、同業他社の動きを特に注視している。取引先に迷惑をかけないという観点でサイバーセキュリティ対策を促すことも必要。また、情報セキュリティ対策とサイバーセキュリティ対策の整理も必要。今までは、標的型メール対策や USB の取扱いなどの情報セキュリティ対策に取り組んできたが、東京 2020 オリンピック・パラリンピック競技大会や IoT 機器の増加への対応といった観点では、サイバーセキュリティ対策として違った取組も必要かもしれない。検討事項案のうち若手セキュリティ人材の育成について、IT パスポートのような資格試験はサイバーセキュリティの勉強のきっかけの一つになる。
与儀構成員：中部電力のプレゼンのうち、活動に必要な資金や人材が不足しているといった課題は、継続的に改善できる仕組みや仕掛けが必要。フェイス・トゥ・フェイスでコミュニケーションすることが必要との発表に関連して、我が国においても、例えば日本 CSIRT 協議会など、サイバーセキュリティに関するコミュニティはそれなりに形成されている一方で、顔ぶれが変わらないという課題があり、若手にどうやって知識やスキルを移行し、コミュニティを仕切る力を渡していくか考える必要がある。また、地域においてコミュニティを主導していくファシリテーターのような人材の育成にも留意が必要。例えば脆弱性の診断やサーバーのログを見る力といった基礎的なセキュリティのスキルを押さえた上で演習に参加することが重要。
手塚構成員：中部電力からのプレゼンにもあったとおり、ボストンでは、自分た

ちの都市を守るために、企業や業界団体だけでなく、全てのステークホルダーが一緒になって、自衛団のような発想で ACSC という地域のサイバーセキュリティを確保するための取組を行っている。我が国でも、地域ごとの自主的な取組が必要であるという観点から、様々なステークホルダーが一緒になって、人材育成を行う考え方を地域でどのように醸成するか検討すべき。

園田主査代理：地方では学習の機会がないという現状がある。例えば、通勤時間などに学習できるオンライン学習コンテンツを用意することも検討してはどうか。

水越構成員：中部電力のプレゼンを聞き、演習シナリオを自分たちで作ることは、自分たちのサービスに対する攻撃側からの視点を学ぶ機会になり、有意義と感じた。また、演習を継続的に行うことを通じて他事業者とのコミュニケーションができるということも重要。中部電力の取組には愛知県警も協力していることについて、愛知県警が協力することになった経緯や愛知県警以外の県警とは今後どのように関わっていく予定か、お聞かせ願いたい。

澤井様：愛知県警で立ち上げていた協議会の会員だった縁もあり、愛知県警にも協力してもらうこととなった。他県警について、岐阜県警はオブザーバーで参加している。警察同士での横連携も強化され始めていると聞いている。

大高構成員：地方公共団体においては、マイナンバー制度の開始に伴い、インターネット環境が分離され、非常にセキュアな環境が構築された反面、サイバーセキュリティに対する脅威への認識が弱くなっており、サイバーセキュリティに対する人材が育ちにくい状況。人材育成の対象を明確にすることが非常に重要。また、マルウェア解析のような高度なスキルを持った人材だけでなく、組織の中でサイバーセキュリティ対策を浸透させるための人材育成も重要。自治体では J-LIS を中心に情報共有がされており、J-LIS では、情報セキュリティ関係のセミナー、CSIRT の構築の仕方、訓練ツール、セキュリティニュースといった情報が提供されているところ、そのようなセミナーに参加できるのは、ある程度規模の大きい自治体に限られる。小さな組織をどうやって底上げし、セミナーや演習に参加できるスキルを身につけさせるか、今年度発足した自治体の CSIRT 協議会においても検討していく予定。

⑤　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