R2-535

世界から見た日本のサイバーセキュリティ人材育成を担う、アカデミー機関の在り方

第三セクター・（株）横須賀テレコムリサーチパーク　技術顧問　　太田　現一郎

1　目的

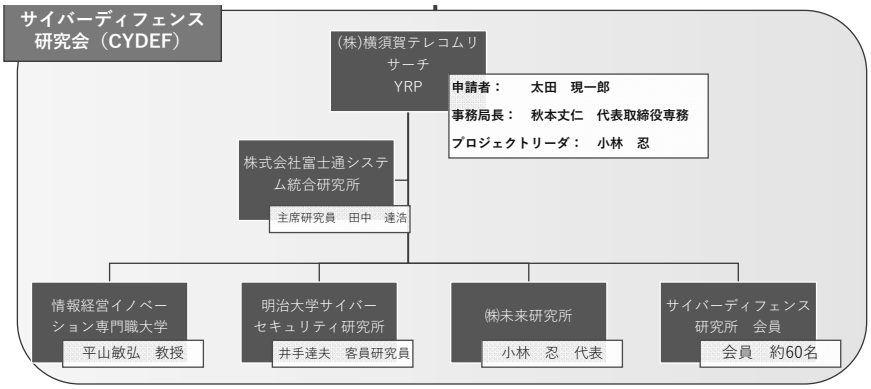
本研究は、各国との比較の上で、日本のサイバーセキュリティ人材の育成上の現状と問題点を明らかにしたものである。欧米と比較し日本のアカデミー機関では、サイバーセキュリティ学問を専門とする学部・学科が非常に少なく、定常的に 20 万人弱の人材が不足している。一方で米国では 2019 年からの 2 年で 18 万人ものサイバーセキュリティ人材を輩出ししている。この様な状況下、サイバーセキュリティ人材育成の観点から、海外との比較の中で、日本の課題を解決に導ける糸口を見出したいと考え、研究に取り組んだ。

2．方法

調査研究の方法としては、横須賀テレコムリサーチパークが、その活動を支援するサイバーディフェンス研究会主催の国際会議にサイバー教育のセッションを設けるとともに、Web 会議を主軸としたヒアリングを中心に、各種参考文献を参照しつつ調査研究を進めた。以下に調査対象と本プロジェクトを推進した実施体制を示す。

【調査対象】

【実施体制】



3. 成果

成果物である報告書は 4 章構成とし、それぞれ日本、欧州、米国の現況を述べ、最後にそれらを分析する章立てとした。

第 1 章において、日本のサイバー人材の現状とその育成に対する取組みについて述べた。そこでは具体的なデータを基にセキュリティ人材不足の多くは、セキュリティ専門家ではなく、プラス・セキュリティ人材であることを明らかにし、その不足を埋めるための様々な取り組みを紹介した。

第 2 章において、欧州のサイバー人材育成のカリキュラムの中から多国間サイバーディフェンス教育訓練プロジェクト（MNCDE&T: Multi National Cyber Education & Training Project）とサイバーセキュリティ研究卓越学術センター（ACE-CSR：Academic Centre of Excellence in Cyber Security Research）を取り上げ、前者は政府（含 EU）及び軍の構成員、後者は大学の研究者・学生に対して、安全保障をも含めた形のサイバーセキュリティ教育が行われていることを明らかにした。

第 3 章において、米国の人材育成ツールの中から、NIST（National Institute of Standards and Technology）の NICE（National initiative for Cybersecurity Education）が規定した Framework を紹介した後、NICE により構築された、就職斡旋ツールである Cyberseek またキャリアアップのための教育サポートシステムである NICCS を紹介した。また前述のサイバーセキュリティ研究卓越学術センター（ACE-CSR：Academic Centre of Excellence in Cyber Security Research）の活動にも似た、国家安全保障局が中心となって運営を行う高等教育カリキュラム、サイバーセキュリティアカデミックエクセレンスセンター（National Centers of Academic Excellence in Cybersecurity（NCAE-C）について触れ、その具体的な教育状況について Norwich University を例にとり説明した。

第 4 章では、これらの事例を分析した。

日本においてはスキル中心でマネジメントの視点が不十分であり、サイバーセキュリティ人材における問題として数と質を挙げ、前者は日本政府の施策の不十分、後者は日本企業の組織体質が原因であるとした。

欧州においては、最上層に当たる安全保障のレイヤーに対する考慮しっかりなされている欧州と、それが欠けている日本の状況が、その教育の差に表れているとした。

米国においては、その事例を通じて、サイバー人材需要の喚起と創生に成功したことがその要因であるとした。その需要喚起を実現するに至った施策が重要であり、「サイバーセキュリティの人材育成を国家プロジェクトと位置付け邁進させる」という大統領令の下、関係する米国政府省庁が有する資産をまとめあげたリーダーシップの有無が日米の差に表れているとした。

4. 考察

研究を通じて、欧米の例に見られたトップダウンアプローチと、日本の例に見られるボトムアップアプローチの差が顕著に表れたと考える。欧米ではサイバーセキュリティに関しては国が

責務を負うミッションと定義付けられ、公の組織によるトップダウンアプローチにて企画・実施・運営がなされているのに対し、日本においては、国としてのあるべき姿は示すものの、基本的には民需に基づいた人材育成を期待するボトムアップ施策を行っている。国民の資産を守るためのサイバーセキュリティ対応には迅速な対処、必要な横連携が必須であり、全体視点とリーダーシップの欠落は時に致命的なものともなりかねない。その意味で、政府がリーダーシップを十分発揮できるような体制を構築していくべきであると考える。

また日本のサイバーセキュリティ人材育成を担うアカデミー機関は、欧米と比べ少ない。この理由は、そこから輩出される人材を受け入れる人材市場が少ないことに起因する。 不足している 20 万人弱のサイバーセキュリティ人材を登用するための施策の前に、人材需要を喚起する施策もまた国のリーダーシップに求められるものである。その上で、求められる人材を育成するための具体的な施策・教育まで言及したかったものの、コロナ禍の許、研究も思うに任せず、最終的にそこまで行きつくことができなかった。これらについては爾後の課題としたい。

サイバーセキュリティは、ネットワークを利用するすべての人が行わなければならないものであることから、その教育対象は世界人口の半数以上となる。本研究で取り上げたものはその中の一部でしかなく、求められる一般性の担保は今後さらに研究を広げていくことで見出すことができればと思料する。