セキュリティ人材育成の課題とアジア太平洋諸国における成功事例

上田　健吾

（受付：2023 年 8 月 4 日　受理：2023 年 8 月 4 日）

1　はじめに

セキュリティ人材育成に関する課題は、日本でもグローバルでも共通している。サイバーセキュリティの専門家の不足、教育とトレーニングの必要性、そして業界と教育機関間のギャップが主な課題として挙げられる。
本稿では、筆者が米国の大学院大学において管轄しているアジア太平洋地域におけるセキュリティ人材育成に関する取り組みを紹介し、課題解決を模索する。

2　セキュリティ人材育成の課題

2. 1　サイバーセキュリティの専門家の不足

(ISC)^2 の調査[1] によると、世界中で 465 万人のセキュリティ人材がいるものの、まだ 343 万人不足していると報告されている。

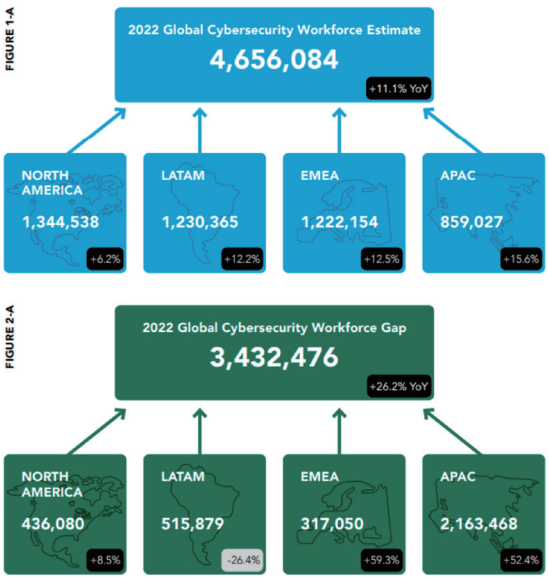

Fig. 1　セキュリティ人材の数と不足人数

SANS Institute

これは全世界的な問題であり、サイバーセキュリティの専門家の需要が供給を上回っている。この問題は日本でもアジア太平洋地域でも顕著で、特に高度なスキルを持つ専門家が不足している。

2. 2　教育とトレーニング

サイバーセキュリティの専門家を育成するためには、専門的な教育と実践的なトレーニングが必要である。しかし、日本ではこれらの教育プログラムがまだ十分に普及していないという課題がある。一方、シンガポールやオーストラリアなどのアジア太平洋地域の一部の国では、政府がサイバーセキュリティ教育を積極的に推進している。

2. 3　業界と教育機関間のギャップ

業界のニーズと教育機関の提供する教育内容との間にはギャップがあり、これが人材不足の環境を悪化させている。日本ではこの問題が特に顕著で、業界のニーズを反映した教育プログラムの開発が求められる。

2. 4　課題解決のアプローチ

日本がこれらの課題に対処するためには、以下のようなアプローチが考えられる。

- 教育機関と業界との連携を強化し、実践的なスキルを提供する教育プログラムを開発する
- サイバーセキュリティのキャリアパスを明確にし、この分野への参入を促す
- 継続的な教育とトレーニングを提供し、既存の専門家のスキルを維持・向上させる

これらのアプローチは、アジア太平洋地域の諸国でも取り組んでいるものであり、各国間での情報共有と協力が効果的な解決策を見つける上で重要となるだろう。

3　アジア太平洋地域における取り組み

3.1　シンガポール

シンガポールでは、シンガポール国立大学 (NUS) がシンガポール政府と共同でサイバーセキュリティ教育と研究のためのセンターを設立した。これは教育、研究、そして業界との協力を通じて、サイバーセキュリティの専門家を育成するための取り組みである。

また、政府がサイバーセキュリティ業界の成長を支援するために、サイバーセキュリティエージェンシー (CSA) を設立し、教育プログラムの開発、業界とのパートナーシップの強化、そして国際的な協力の促進を行っている。

さらに昨年には、CSA は南洋理工大学（NTU）とともにサイバーセキュリティの評価と認証のためのワンストップ施設として機能する国立評価総合センター（NiCE）を発足させた。まさに教育組織と政府と産業界が一体となり、セキュリティ人材の育成を推進していると言えよう。

3.2　オーストラリア

オーストラリアもサイバーセキュリティにおける先進国として様々な政策を取っている。

政府がサイバーセキュリティのスキル向上のために、教育機関と産業界が連携して実践的なスキルを提供するプログラムを開発したり、2020 年のサイバーセキュリティ戦略ではサイバーセキュリティの教育とトレーニングに 1 億 5 千万豪ドルを投じると宣言したりしている。これは、サイバーセキュリティ専門家の供給を増やし、一般的なデジタルリテラシーを向上させるための取り組みである。現在は 2023 年～ 2030 年にかけての戦略についてのディスカッションを行っている。

また、米国や日本、インドをはじめ、様々な諸外国とサイバーセキュリティについての協力体制を構築し、アジア太平洋地域内でのリーダーシップを取っている。

3.3　インド

インド政府は、「National Cyber Security Strategy」を発表し、サイバーセキュリティ専門家の育成を推進している。また、同じく政府がサイバーセキュリティの教育と訓練を提供するための専門機関である「Indian Cyber Crime Coordination Centre」を設立し、国内でのセキュリティ人材育成を牽引している。

そもそもの人口が増加している傾向もあり、その経済規模の拡大に伴い、政策としてセキュリティ対策にも力を入れている。実務的に厳しいセキュリティ制約が課されるケースも散見されるものの、実現のために官民一丸となって取り組んでいる様子が伺える。

3.4　日本

日本でも、政府がサイバーセキュリティ専門家の育成を推進するためにさまざまなイニシアチブを行っている。例えば、内閣サイバーセキュリティセンター (NISC) が「サイバーセキュリティ人材育成方策」を策定し、高等教育機関や専門学校での教育プログラムの開発を推進している。また、いくつかの大学がサイバーセキュリティ専攻を設け、政府主導で産業界との協力も取り付け、専門家育成のための研修プログラムやインターンシップの提供を進めている。

筆者も 2016 年に国立大学にて、社会に出てからすぐに活かせるサイバーセキュリティの実践的な内容を学ぶとともに、理論的背景にある知識も同時に身につけられるような講義を 2 種類作成し教鞭を取ってきたものの、国内ではまだ教育機関で教えられる知識と実際に現場で使える技術に大きなギャップがあるケースが多い。

4　これからのセキュリティ人材育成

上記の通り、日本でも政府機関が主導となり様々な施策が検討されている。すぐにビジネスに結びつく取り組みではないものもあると思うが、多くの企業や教育機関がこれまで以上に取り組みを強化し、より実践的かつ高度なセキュリティ技術を持つ多くのセキュリティ人材を育成できるよう努めたい。

国際的な連携もさらに強化し、国際的にも通用するセキュリティ人材が充足することを期待したい。

参考文献

[1] (ISC)². 2022 Cybersecurity Workforce Study. 2022, https://www.isc2.org/Research/Workforce-Study