中間報告書　別紙 1

日本企業における人材不足と産学官連携による対策の必要性

1.0 版

2016/01

1　サイバーセキュリティ人材の現状・課題

2011 年発覚したサイバー攻撃を契機に、サイバーセキュリティが日本社会の重要課題と認識され、サイバー人材不足が喫緊の課題であると認識された。IPA による調査では、情報セキュリティに従事する技術者は約 23 万人（内 14 万人がスキル不足)、不足人材数は約 2.2 万人と報告したが、改定して、現在はそれぞれ 26.5 万人（内 15.9 万人)、約 8.2 万人としている。

2020 年東京オリンピック・パラリンピック競技大会では、競技周辺、関係組織、開催都市に対する大規模・連続的なサイバー攻撃が見込まれる。昼夜を問わない同時多発的な攻撃に競技期間中対処し続けるためには、少数の有識者に依存するのではなく、交代要員も含めた十分な体制構築が必要である。個社毎で対応できる話ではなく、産業界として、業種にとらわれず企業間で連携できる仕組みが求められる。

この体制構築に向けたシミュレーション（付録１　オープン・ガバメント・コンソーシアム）によると、2018 年までに実働部隊・中間層を増やすことが鍵とされ、企業内の IT 経験者の活用等の短期的な対策と、2020 年以降を見据えた大学での人材育成の必要性等の長期的な対策が主張されている。また、トップガン人材育成に向けた OJT 環境や講師の不在が仮題とされている。

（http://www.nisc.go.jp/security-site/spc/wg/dai01/pdf/01shiryou0203.pdf）

ユーザー企業では、セキュリティ人材候補となる IT 人材の母集団が少ないため、人材の確保・維持は更に困難である。比較的多くのセキュリティ人材を抱える ICT 企業・セキュリティ企業と連携し、アウトソースする部分と自社で部分を見極める必要がある。(付録２)。

サイバーセキュリティ人材の候補者を育成する環境を、一企業で提供することは困難と言える。企業間の連携、産学の連携、産官の連携、海外との連携など、産業界として、日本国として、人材育成・レベルアップ、本人への動機づけ、活躍できる産業の創出と拡大、育成支援側への参画(指導者、投資家)など、エコシステム(付録３)を整え、人材と利潤が循環する仕組みを考えてゆく必要がある。（http://ogc.or.jp/archives/1726）

過去、IT 黎明期にはソフトウェア人材の不足が同規模で起こった。この時、産学官の労力で課題を提起し取り組んだ結果、人材育成に加え IT 産業の拡大にもつながった。唯一の反省は、ラリー・ペイジやマーク・ザッカーバーグに代表される、クリエイティブ人材の育成が成し得なかったことである。

2　産業界の状況

欧米と比べ、日本企業におけるサイバーセキュリティに対する経営層の関心度はまだ不十分である。サイバー攻撃を自分の問題と捉えていない、または、サイバーセキュリティを IT テーマと捉えている日本企業が多い。しかしながら、これでは近年のサイバー攻撃には十分に対抗できない。標的型攻撃に代表されるように、サイバー攻撃は複雑・巧妙化し続けており、企業の存続に関わるような被害をもたらし得る（付録４）。従来のセキュリティ対策とは根本的に異なり、単なる IT テーマではなく、経営の重要課題として取り組むべきである。

臨機応変に攻撃を変えてくる相手に対しては、人智を集め臨機応変に対応するしかない。高いスキルを持った人材の必要性はここにある。

しかしながら、4.1 でも述べたように、人材不足は深刻であり、特にユーザー企業では人材の確保・維持が困難である。さらに、人事ローテーションのため経験が蓄積しにくく、対応能力は手薄になってゆく。これは雇用システムの異なる欧米では起こりにくい、日本で固有の問題と言える。

①　日本固有の雇用システムと人事ローテーション

新規雇用の中心は大卒採用で、この時点で文系人材が中心の業種に理系人材は入らない。IT 依存率の高い企業であっても、IT が本業でないなら、本業に必要な人材の雇用が優先される。IT＝省コストなので、IT 部門＝省コスト部門と扱われがち。つまり、少ない人数で多くを扱うのが IT 技術者の宿命となる。このような条件下、未経験の技術習得、広範囲で複雑な話題を扱うサイバーセキュリティを、余暇でマスターすることは不可能と言える。

終身雇用と人事ローテーションはキャリアパスと切り離せない。複数の組織と事業を経験することで、より大きな組織と事業の管理者になれる。ローテーションから外れて管理者としてのキャリアパスはない。ジェネラリスト向きの仕組みが出来上がっており、その中のスーパージェネラリストがより上位に登用される。

これを前提に、雇用時には適用性、柔軟性が重視されがちである。セキュリティしかやらないという人材の雇用機会は中途採用、というのが実情である。両者を許容するキャリアパスを構築した企業はまだない。旧態前とした企業風土では、内部から自己変革が起こることも難しい。

② 人事制度との不適合

組織をまたがる人事ローテーションは中間管理職になった後に多く、若いうちは、最初に所属した部署を異動することはない。OJD が人材育成の手段だった時は有効だったが、急速に事業が変化し、技術が推移する昨今、社内人材の固定化は変化に追従する足かせとなっている。社内専門家制度、社内採用制度など、いろいろな試みが行われているが、企業文化として根付くのは難しく、効果が継続するまでには至っていない。

サイバーセキュリティ技術者、管理者のように、従来の職種、人材像にはない新しいタイプの人材を増やそうにも、高い潜在能力がありながら現職、現組織に縛られて、育成機会を必要な時に与えられないというジレンマがある。

大卒新規雇用の基準はジェネラリスト中心で、スペシャリスト指向の採用は中途採用になるが、そもそもサイバーセキュリティ人材が市場に流動するほど多くない現状では、いずれの採用もうまく機能することはない。

③ ユーザー企業と ICT 企業それぞれの課題

これまでの説明でも分かるように、IT 従事を望む成績優秀な理系人材は、その多くが大手 ICT 企業に入ることになり、ユーザー企業にはほとんど入らない。また IT バブル時代の崩壊以降、IT 従事を嫌う成績優秀な理系人材の数も少なくない。

サイバーセキュリティ人材の適切な育成対象候補はこれらの理系人材である。これらの候補者を動機付けし、活躍できる環境を整えることが、人材確保・維持につながる。

2020 オリンピック開催期間中とその前後、もっとも深刻なサイバー攻撃や被害を受けるのは開催開場以上に、日本の企業だと考えられる。昼夜を問わない攻撃を、現状の人材で何件扱えるか、と考えると簡単なことではない。そう考えると、一社で何とかできる話とは思えなくなる。産業界として、業種にとらわれず企業間で連携できる仕組み、2020 年に向かっての取り組み方を検討すべきと言える。

3　産学官の連携の必要性

“世界中のセキュリティベンダー社員数より攻撃者数の方が多い現状では、セキュリティベンダーが手を組まないで攻撃者に勝てる道理はない”、と主張した CEO がいた。より深刻な状況下の日本においては、産学官総力をかけて考える契機でもある。

産学官それぞれでないとできないことは少なくない。しかしサイバー攻撃に対しては、それぞれで出来ることをしているだけでは問題解決につながらない。奇しくも、一向に減らず繰り返される攻撃と被害で、これが証明された形になっている。業種を超えた(産業横断)連携、産と学の連携、産と官の連携の仕方を考え、それぞれの効果が全体に回る社会システムにしてゆかなければならない。2020 年を考えると、日本全体で一致団結してサイバー攻撃に取り組む体制を築くことが今求められている。

① 産学官それぞれでないとできないこと

産はもっとも多くの人材を内部に抱えている。学にも人材候補は多いが、在籍期間が高々6 年に対し、企業で前線に在籍する期間を 20 年とすれば、はるかに多くの実践的人材が企業内にいるはずである。人材の無駄遣いをしてはいないか、各企業で再考する必要がある。仮に無駄遣いが見つかったとき自浄力がすぐ働くか、これには大いに疑問が残る。前節で述べた旧事業環境に適した人事システムが立ちはだかり、変革を断行できる経営者は極めて少ない。これは大企業に特に共通する課題である。

この共通課題を解くには官の力が必要である。法制化、指導、ガイドライン、金銭的動機づけなど、鞭だけにならず飴を抱合せた施策で、動きたくても動けない企業を動かさなければならない。

学に期待したいことは、社会人教育プログラムによる企業人材の継続的レベル向上である。サイバー攻撃のような新しい技術、実践テーマになると、各企業が内部で講師を用意することは不可能にちかい。講師の育成や教材開発から手掛けるのでは、どの企業も動けない。大学がこの役割を引き受けるのが現実的だが、企業はなかなか最初の一歩を踏み出せない。コスト、効果、時間、いずれも不確定だからである。産学で努力はしつつも、産学の動きを後押しする官の施策は不可欠である。

② 効果が循環するエコシステム

前述の施策を個別に実行するのでは、日本全体で一致団結してサイバー攻撃に取り組む、長く継続する一貫性ある活動とならない。産学官が課題を共有し、施策を実行する必要がある。

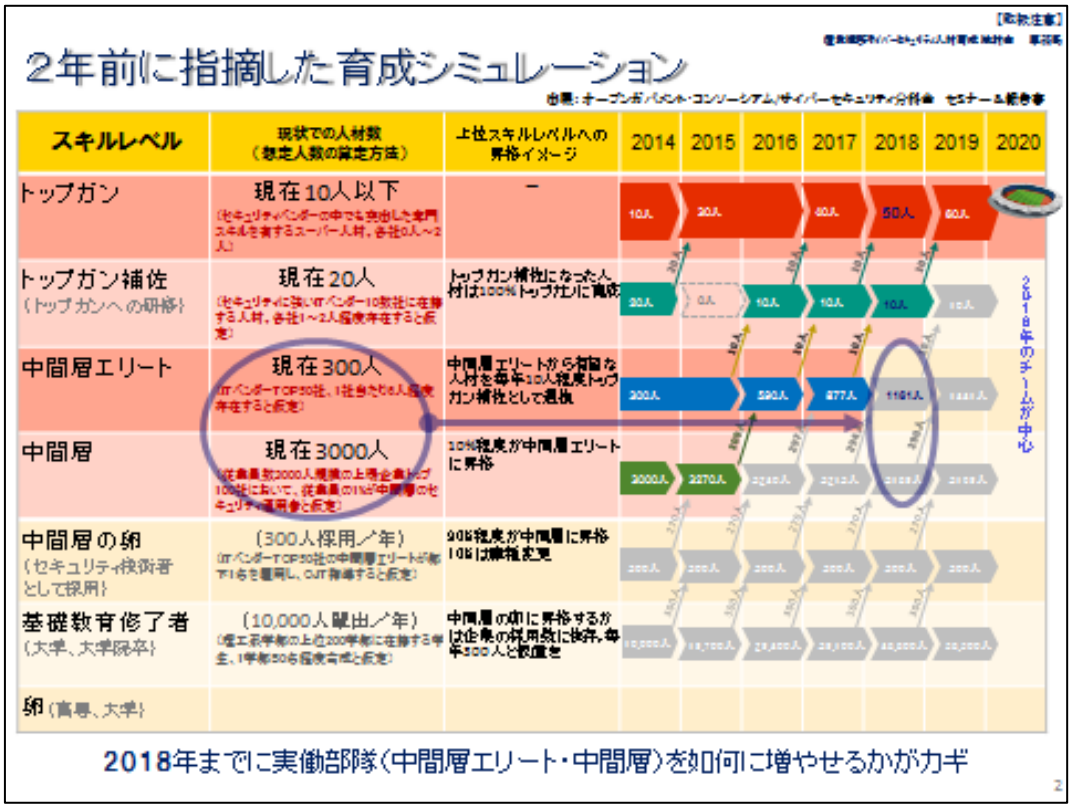
ここでは、育成される人材を中心に考えることが重要で、初心者から最高峰までを目指せるキャリアパスを示さねばならない。産学官の役割はこれを支えて実現することで、そのために一企業を越えた人材活用、海外との交流など、人材を効果的に育成、維持する環境整備が不可欠である。

同様のエコシステムを持つ国はいくつかある。イスラエルでは、優秀な高校生の選抜、

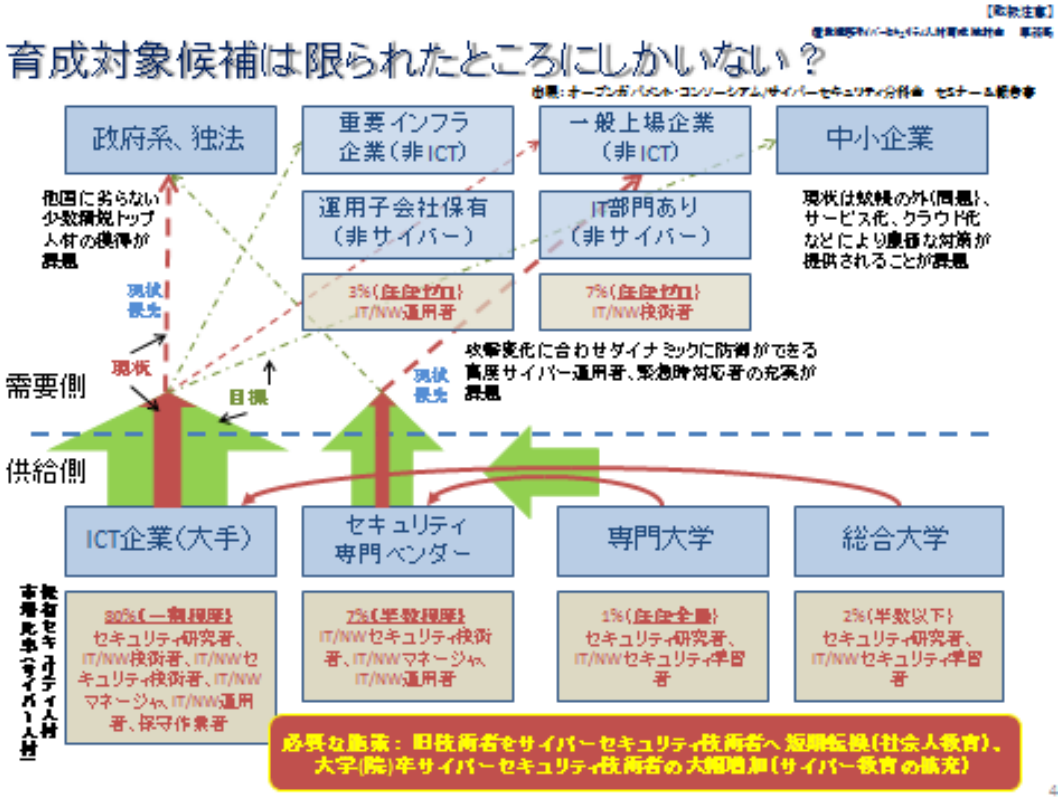
兵役義務に合わせたサイバー部隊への配属、退役後の起業プログラム、起業成功者による後進支援、投資家ネットワーク、失敗しても再挑戦できる起業など、社会のあちこちでサイバー人材が成功する仕組みができている。米国では膨大な防衛予算を背景に、防衛企業が中心となって人材育成が行われている。全米数千校の高校生を対象にしたパトリオットプログラムなどである。起業と成功を手助けするベンチャーファンドなど、すでに出来上がった社会インフラがある。

どの国を見ても同じシステムはない。共通するのは、サイバー人材が尊重され、成功するために何度も挑戦できることである。日本の人材育成・維持エコシステムも、日本の事情に合い運用可能なものを考えるべきだと思うが、中心に置くべきは育成される人材であり、ここは明確に社会で認識されなければならない。

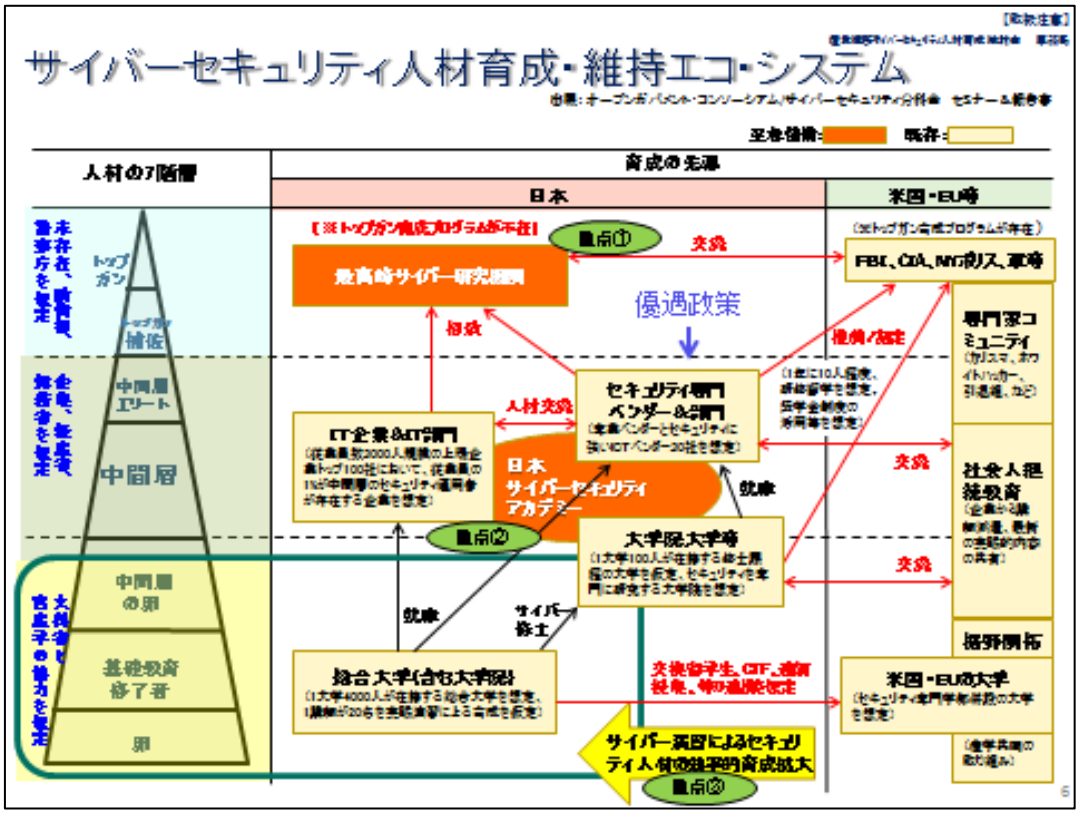
付録 1



付録 2



付録 3



付録 4

Difference between Traditional vs. Cyber

	Traditional	2010 In Japan	Cyber
Important subjects	Virus/malware, Private/confidential Information leakage		All of traditional items, and PLUS Targeted Cyber Attacks
Attackers	Inside (Amateur)		outside (Professional)
Peculiarity	Low skill, easy to detect		Very high skill, hard to detect and always invisible
Motive	Mistakes, sometimes by dissatisfied		Nationalism, business for profits
Detection	Reported by employees		Not noticed for many months
Frequency	Often once		Revisit endlessly
Damage	Sufferer pays		Business suspended
Occurrence	Controllable		Un-controllable