参考資料

「トップガンも含めたサイバー人材の育成・活用についての一考察」

2016 年 9 月 5 日

一般社団法人サイバーリスク情報センター理事　則房雅也

動機

2011 年に複数日本企業が同時に大規模なサイバー攻撃を受けたことで、サイバー攻撃の存在が一般に知られることになり、有効な対策の実現が急がれるようになった。その後 2 年ほど経ったころ、対策への取り組みにさほど進捗が無いことに気づき、その原因を調べた。行きついた原因は「人材がいない」である。サイバーセキュリティを扱える人材がいないため、具体的に何も進まないという、社員隅々にまでインターネット、IT 利用が浸透した世界トップを行く日本企業からまさかの指摘を受けた。

2020 年までの人材育成シミュレーションと課題を指摘（図 1）し、その後 3 年経った 2015 年でもさほど事態の改善は見られなかった。この間、政府組織に対するサイバー攻撃が増えて被害が続出し、政府周辺でサイバーセキュリティが最優先取り組み課題の一つとなった。それにもかかわらず、ほとんどの企業でサイバーセキュリティ人材の育成や採用は進めておらず、期待と現実のギャップが拡大している。今でも（求めるスキルを備えた）サイバーセキュリティ人材を提供できるところは見当たらない。人材育成は簡単には解けない課題と考えざるを得ない。

人材不足のまま 2020 年を迎えると多くの予測が現実となる。これまでとはレベルの異なる量と質のサイバー攻撃がやってきて、これまでにない多くの企業、政府組織、あるいは個人にまで破壊的な被害が広がることになる。かなり現実的な危機として見えてきた。一企業で人材育成・維持への課題は解けない。多くの関係者が協力し、社会全体で人材を育成し共有し活用する仕組み（以下、エコシステム）を構築しなければならない [1)]。本ホワイトペーパーでは、なぜ今エコシステムが必要なのか、実現できたなら何を得られるのか、をわかりやすく説明する。

取り組み内容の重複を避けかつ一貫性、整合性を保てる、時間と投資を無駄にしない人材育成を、産官学の協力で行う柱としてエコシステムが位置づけられることを期待する。

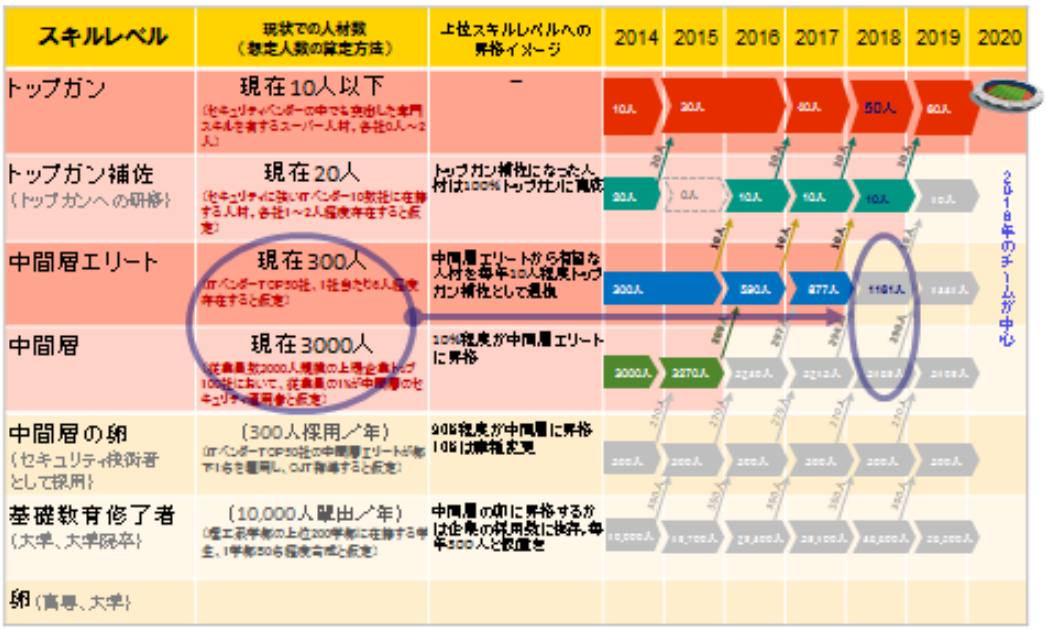

図１　人材育成を指摘したシミュレーション*

はじめに

サイバーセキュリティ人材不足の課題検討は、オープンガバメントコンソーシアム(以降、OGC)で始めた[2)]。守れなかったサイバー攻撃を目にしたのに、多くの企業が従来テーマの範囲で取り組もうとしたからである。エコシステムの考え方（図 2）は、サイバーセキュリティの専門家を目指す人材の裾野を広げて、新しい時代の企業活動を守ることに活躍してもらおうと考え、政府、教育機関側に多数のサイバーセキュリティ人材の育成を提言するためにまとめた。産業横断サイバーセキュリティ人材育成検討会（以降、XS 人材検討）は、経団連サイバーセキュリティ懇談会の政府提言をきっかけに 2015 年に発足した。提言には多くの重要な指摘を含んでいたが、実行に移そうとすると、そんな人材はここにいない、と言われて行き詰ってしまう。

今すぐ活用できる現役およびすぐ集めて育成開始できる候補のほとんどは企業に属している。学生や公務員ではない。企業数の多さで全体として人数が多そうに見えるが、個人またはごく少人数であちこちに分散している実態がある。サイバー攻撃対応力は無いに等しい。2020 年までに対応力を劇的に強化するには、分散する力を集結させ、訓練し、共有できることが鍵である。人材のほとんどを抱える産業界は、実はエコシステムのコアに位置する。産業界で人材が増えれば、周囲の組織の対応力も向上する。XS 人材検討では、参加企業および官学と横断的な連携をとり、エコシステム実現を目標にして、まず産業界でサイバーセキュリティ人材を増やしレベルアップすることを最初の取り組みとした[3)]（図 3)。

XS 人材検討では、参加企業が少なくとも 2020 年に一定レベルで対応が取れるように、人材育成に関する検討結果の実行・実装までイニシャティブを取って行ってゆく。新たな参加企業、取り組み範囲の広がりが得られれば、2020 年により広く社会に対し重要な役割を果たせることになる。

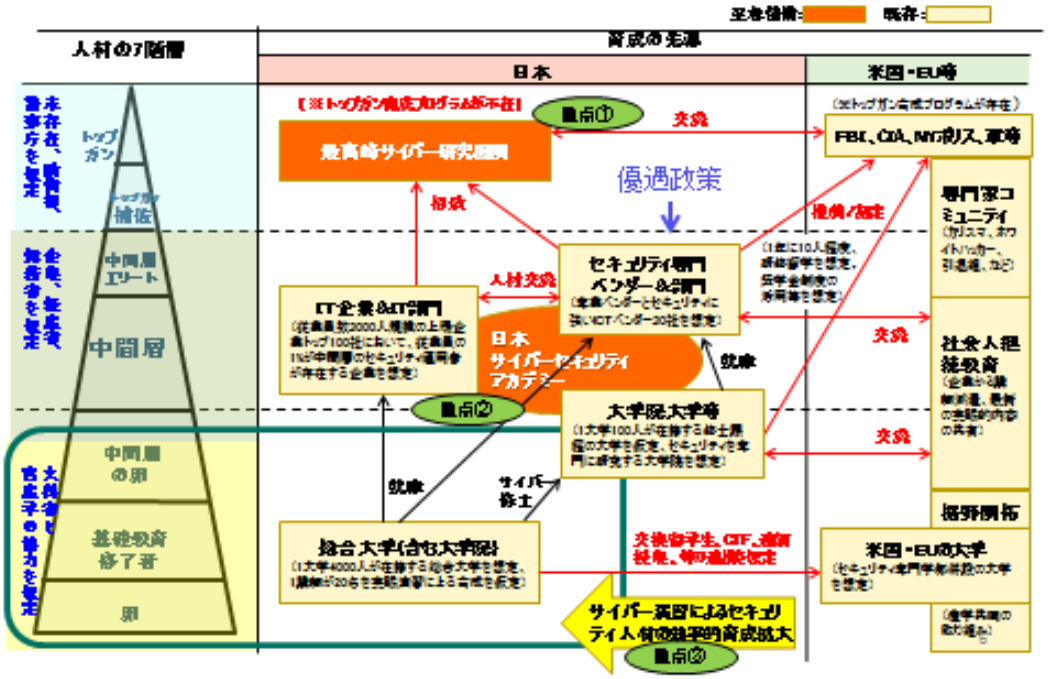

図２　個人のキャリアパスから見たエコシステム**

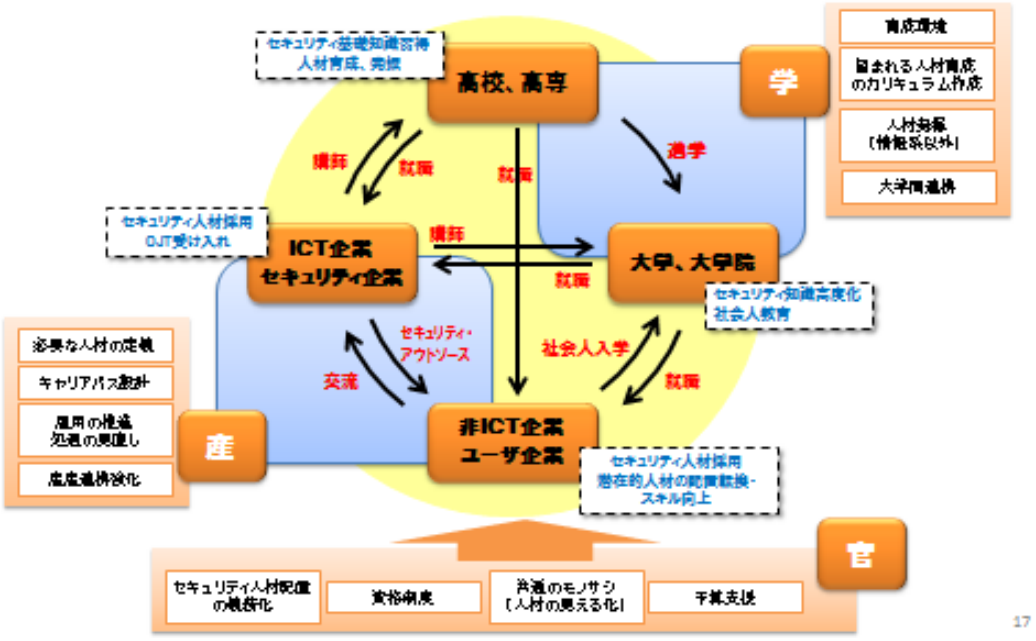

図３　産官学の協力から見たエコシステム***

業種や企業ごとで内部の人材構成が異なる

XS 人材検討である事実が明らかになった。育成候補者の所在が業種で異なり、同業種

でも企業ごとに違いがある、ということである。ICT 企業には IT やインターネットに精通した人材が多いが、ユーザ企業（以降、非 ICT 企業）では少ない。非 ICT 企業では、IT への適性が見いだされた人が途中から IT 業務を担当することになる（図 4－1)。また、技術者の多い非 ICT 企業でも、事業領域の技術者が中心で IT 技術者にするためではない（図 4－2)。これらの企業では、担当職務を本来業務から IT 業務へと、途中で役割変更、職種転換している。

サイバー攻撃は IT やインターネットを駆使するため、これらの技術に精通した人材が育成対象として望ましい。ICT 企業では一度の役割変更、職種転換でサイバーセキュリティ人材候補となるが、非 ICT 企業では極めて小さい母集団から二度目の役割変更、職種転換が必要で、実施機会は事実上ほとんどない。

サイバー攻撃対応を行う CSIRT（Cyber Security Incident Response Team）設置を考える企業は多い。ICT 企業では人材母集団（図中の黄色部分）が大きく、チーム作りと維持は難しくない。多くの非 ICT 企業では、チームを作っても維持が困難になる。時間とともに弱体化し、いざというときに機能しない。両企業間の協力で困難は乗り切れるはずだが、要件の相互理解などが不足し、今のところ現実解には至っていない。

一企業を超えて活躍できる人材の育成・維持を目指すエコシステムは、上場企業の 90%を越える非 ICT 企業にこそ有用性が高い。

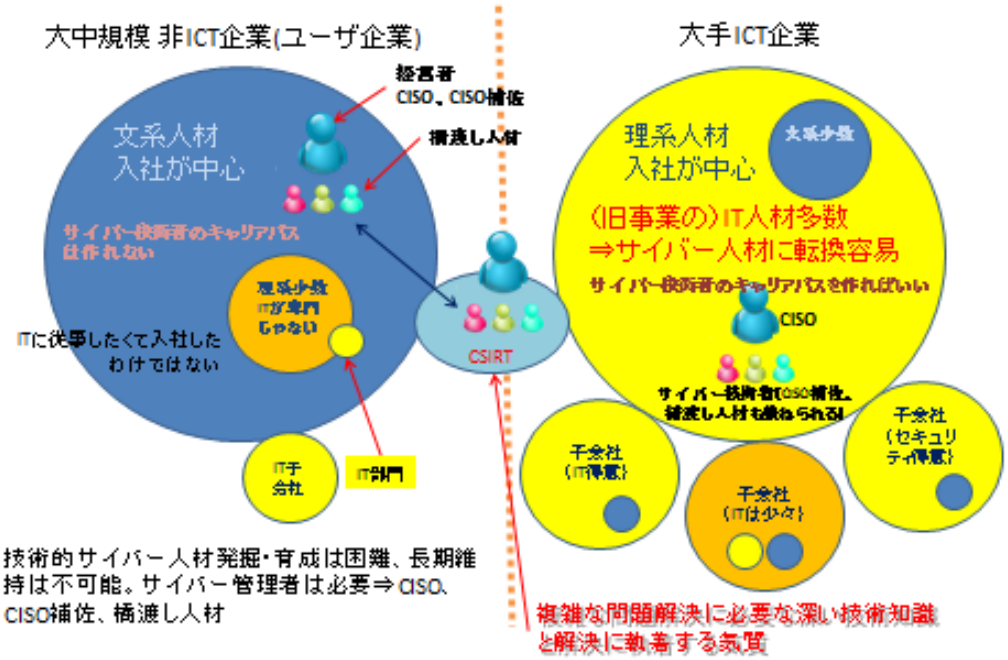

図 4－1　技術系人材が少ない企業****

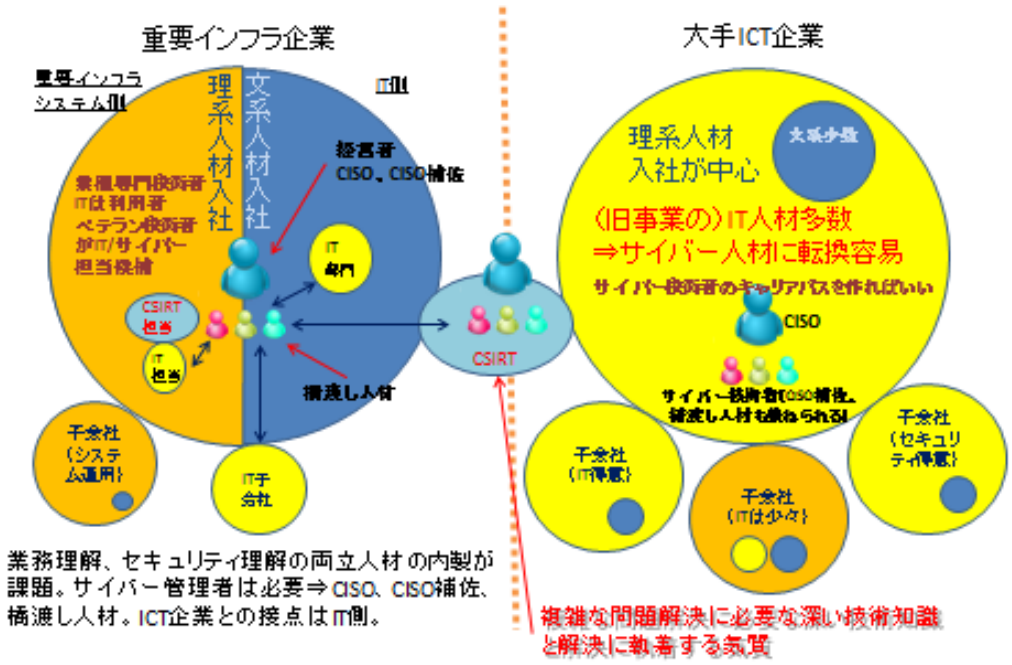

図 4－2　技術系人材は多くても IT 人材は少ない企業****

人材の育成・維持にエコシステムが不可欠な背景

人材育成のもっとも重要な要件は、育成した人材が最大限活躍できること。たとえば、大学で育成した人材は求める職に就けること、採用企業は機会を提供し続けることである。企業内で育成を考えると、候補者は現在他の仕事をしており、役割変更、配置転換が必要になる。候補者に機会が与えられること、配置転換が柔軟に行えること、が不可欠となる。今後、多くの企業で CISO 設置が義務づけられ、CISO 業務遂行組織（たとえば CISO 統括室）や実行力のあるスタッフの確保が必要になる、これが社内人材配置転換のきっかけにもなる。

最小限であっても専任組織作りは必要で、これまで多くの企業で、本業を持つ優秀なマネージャや技術者が、サイバーセキュリティ担当を空き時間で兼任している。定期人事異動がある度に、二つの業務を担当できる後継者は見つからず、サイバー攻撃対応の方が弱体化の一途をたどる。サイバー攻撃に形だけの対応体制は長続きしない、作業量は増え、かつ高い質が求められる時代に入った。危機管理、財務、知財のような、専門性と目的が明確な組織である。

サイバー攻撃が発生すると作業が急に増え、動くべき人も増える。必要な人材を十分確保してある企業は少ない。育成候補者、育成手段を持たないところは急場を凌ぐ体制も準備できない。アウトソーシングなど代替案の急な実行が不可欠になる。

活躍する場と同様に重要な要件がキャリアパスの提供である。旧型人材用に最適化された人事制度が多く、サイバーセキュリティ人材だけの特別扱いは難しい。これを回避し

てすべてをアウトソーシングするわけにもいかず、サイバーセキュリティ人材を活躍させるキャリアパスの構築は、企業でこれから長く取り組むことになる課題である。

エコシステムに対する２つの立ち位置

「育成した人材が最大限活躍できること」が重要であると前述したが、人材育成の仕方に関する議論は多いが、個人をどう効果的に活躍させるかという議論は少ない。誰のためのエコシステムであるべきか、この問いには２つの答えを示さねばならない。

1. 育成される側のためには、グローバルに通用する個人へとレベルアップするキャリアパスが示されること（図 2）

訓練された攻撃者と対峙するには、守備側が攻撃者と同等のスキルを保有しなければならない。一人で守れないものなら、チームとして個人の不足を補う、内製チームで守れないものなら、外部のスキルを活用する。現実には、日常業務の遂行と平行して長時間訓練に参加する余裕はなく、高いレベルが必要になるほど、実践を通したスキルアップ、短期間で焦点を絞った高度な訓練をこなすことが求められる。図 2 の主要なポイントは以下の通り。

① IT やインターネットなどの基本は教育機関で履修し終える

非 ICT 企業でセキュリティ技術者の教育は難しい、さらに基本も知らないのでは最低必要な技術者の確保まで難しい。ICT 企業でしか育成機会が作れないという制限は大きい。

② 産官学で実戦の場が数多く提供され、できる限り多様な実践経験を積める

アウトソース、出向、共同研究、分析、結果の共有など、あらゆる参加方法で実践環境が共有される。たとえば、日本サイバーセキュリティアカデミーのような仕組みで。

③ 海外トップ機関への参加機会が作られる

演習、研修、留学、共同研究など、いろいろな参加方法で US や EU での最先端訓練への参加機会が提供される。国家間レベルの協力関係が元にあるのが、成果を広く共有する点で望ましいが、教育機関間、政府組織間の個別関係の下でも効果は期待できる。

④ トップガン排出を目指す官学研究活動へ、企業の研究参加機会を提供

企業内の母集団は小さいが、トップガンを目指せるキャリアパスを示し、企業内トップから更にレベルアップする動機を与える。現状、トップガンを排出する研究機関はないので、この設立検討も必要。

⑤ 社会人継続教育の提供

IT やインターネットなど基本教育は①の範囲。最先端(攻撃)の内容、実践的な内容、最新インシデント対応演習、攻撃を生む社会情勢、サイバー犯罪、国際法などが実践的キャリアパス開発に貢献する。

2. 育成推進側、活用側のためには、産官学で協力し、育成目標人数と育成手法が整えられ、期待した人材像の育成成果が予測できること（図 3）

欧米で産官学間の人材流動性は高い。国境を越えた人材登用も容易である。人材の流動性は人材育成にも大きなメリットがある。流動性の低い日本では、産での経験がない人が、産が必要とする内容（たとえば、実践的内容）を教えにくい。高度な内容ほど要求に応えにくい。そのため、まず教えられる人を育成する、という話が出てくる。テーマがサイバー攻撃だと、産のどこにも訓練に使える実践の現場などない。早く「教えられる人」を確保するには工夫がいる。近年欧米でも人材不足が指摘されるが、教える人はいるが期待する速さで育成できない、と言っているようである。

どこでも単純に解決できていない話なので、産官学が率直な意見を交換し、人材育成の実行に障害となる課題をすばやく解くことである。

① 産業界が求める人材を定義し、これを教育機関に提供する

やはり産業界で多くの人材が活躍できて大きな効果が得られる。多くの企業がサイバーセキュリティ人材として雇用しキャリアパスの出発点を明確にする。基礎教育を企業内で省略できることも、次のパスに早く移るために重要である。

② 企業内での継続教育要件を定義し、これを教育機関に提供する

考慮すべき要件が２つある。一つ目は、現役人材のレベルアップ、二つ目は、候補人材の配置転換を助ける教育である。前者は現業を行いながらになるので時間制限が大きい。短時間で必要な教育だけ受けられることが条件となる。後者は基礎力の再確認も含め、妥当な期間の集中教育が必要である。企業がこれらを加速する制度が導入されるとよい。もう一つ考えられる要件がある。転職によるキャリア開発を助ける教育だが、この費用負担をする企業は少ない。中途採用の動機を与える、スキル獲得を保証する教育、生活の補助、企業に動機を持たせる制度などが導入されるとよい。

③ 企業の上位レベル人材間の交流、レベルアップ機会の提供

XS 人材育成で行っている勉強会は、基本レベルの情報交換、人材交流を実現している。これを企業内で活躍する上位レベルのサイバーセキュリティ人材を対象に行うイメージである。企業人を対象にした MBA プログラムが参考になりそうである。

④ 産官学で協力し、トップガンの要件、活躍の場を提供する

一企業の IT 環境でサイバー攻撃を経験しても、グローバルで発生するさまざま

なサイバー攻撃に対応できるようにはならない。一企業で提供できる実習環境の限界である。トップガンと呼んでよい人材は、グローバルで発生する攻撃に精通し、一組織（企業、政府組織など）を越えて活動し、関わる組織をいずれも守るために行動し、問題に対応しているときは利益より守ることを優先して行動する。ビジネスで行動しにくいが、ビジネス抜きでは続かない。産官学の協力で、複数の帽子をかぶれるなど、工夫がいる。

エコシステムによって得られるメリット

エコシステムと言っても、これまで述べてきたように、実現すべきことは山のようにある（図 6)。時間と費用を無駄にする取り組みは避けなければならない。イスラエルや米国では、すでにエコシステムを実現している[4]。おそらく、北朝鮮や中国でも、世界最大規模のサイバーセキュリティ従事者を保有しており、内容は異なるがエコ効果の得られる人材育成と維持システムができていると思われる。サイバーセキュリティ人材の育成に取り組んでいる国は他にも少なくない。時間とともに人材面で成果が現れるに違いない。日本は産官学の協力を密にし、他の国より早く最先端レベルに追い付き、国内課題としてではなく、グローバル課題としてサイバーセキュリティを語れるようにならなければならない。

エコシステムで追及すべき目標は「雇用と産業の創出」である。前述の国々では、サイバーセキュリティがビジネスの一要件として浸透している。これまで指摘してきた内容も、「雇用と産業の創出」に結びつけなければ長続きしない。2020 年を目標にいろいろなビジネスが動いている。2020 年以降も継続、伸長するビジネスはあり、2020 年は将来のビジネスを検証する場になるはずである。

XS 人材育成の取り組みは雇用の創出を先導している。産業の創出は今後の課題になるが、人材はあらゆる点で要となる。産業の創出に着目すべき点がいくつかある。

- IT であれ OT (Operational Technology)であれ、高額投資して開発したシステムの維持管理コストは限界まで削減済みである。その結果、維持管理を行う運用保守チームにサイバー攻撃対応力はない（図 5)。この周辺に、CISO や CSIRT が設置されようとしている。脆弱である実態が明らかになるだろうが、守りの体制が十分になるわけではない。高度な対応力を外部に求める必要が出てくる。
- グローバル市場で企業活動を進める上でサイバーセキュリティは外せない。人材の獲得と維持、特に維持は日本より現地の方がはるかに難しい。日本で人材が増えるに従い、対策準備も問題対応も日本で行えるようになる。この方が、結局、事業損失の回避やコスト削減にもなるはずである。
- 不法に利益を得たい輩が利益源を保有する企業にインターネットでつながれば、サイバー攻撃は起こり、サイバー犯罪に至ってしまう。現状、ほとんどの企業は犯

罪に至って法執行機関がのりだしてから、結局事後処理にコストをかけることしかできない。この状況に誰もが不満で、サイバー攻撃を予知し、事前に攻撃に備える方向に技術開発などが進んでいる。この攻守の均衡を保つ事業機会がすぐに来る。

- IoT (Internet of Things)など新しい IT とインターネットの世界が構築されつつある。インターネットが出現した 1990 年と違い、今では専業化の進んだ組織犯罪体制がインターネット上に出来上がっている。IoT が新しいと言っても、利用者にとっての話で、技術者から見ると従来の延長でしかない。高度な攻撃技術を蓄積した犯罪組織なら、少しの研究で簡単に IoT システムへの侵入も破壊も可能となる。インターネット上に IoT の次が現われても、おそらく同じことになる。今のインターネットが存在する限り、これは変わらない。

こういうところでもサイバーセキュリティ人材の活躍の場は多い。ICT 企業だけがサイバーセキュリティ技術者の活躍の場ではない状況がすぐに来る。

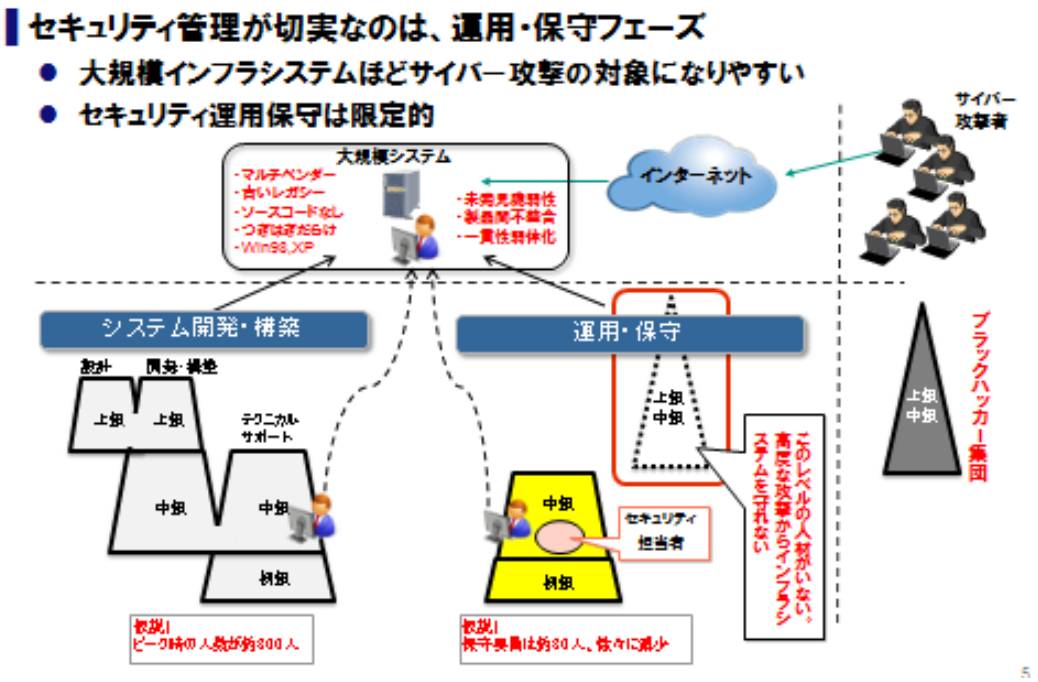

図 5　重要インフラシステムの運用課題*****

どのような機会が新たに現れようが、一組織内の現保有人材や体制だけでサイバーセキュリティに取り組んで、効果を得るのは困難になる一方と言える。この状況は長く変わることはない。事業継続を重視した内部の管理体制は強化した上で、インシデントを扱う技術などは外部の力を導入しつつ、必要な内部人材の育成を着実に進め、どうやっても内

部で解決しない部分は、早く割り切ってエコ効果を得られる外部との新しい協力体制作りを検討し、実行に移すことが重要である。特定企業だけ動いて社会的な効果が得られることはないので、産官学で協力し社会システムとして、この動きを加速させることが必要と言える。産官学が協力して動かした社会システムなら、社会のインフラとして 2020 年以降も機能し続けることができる。

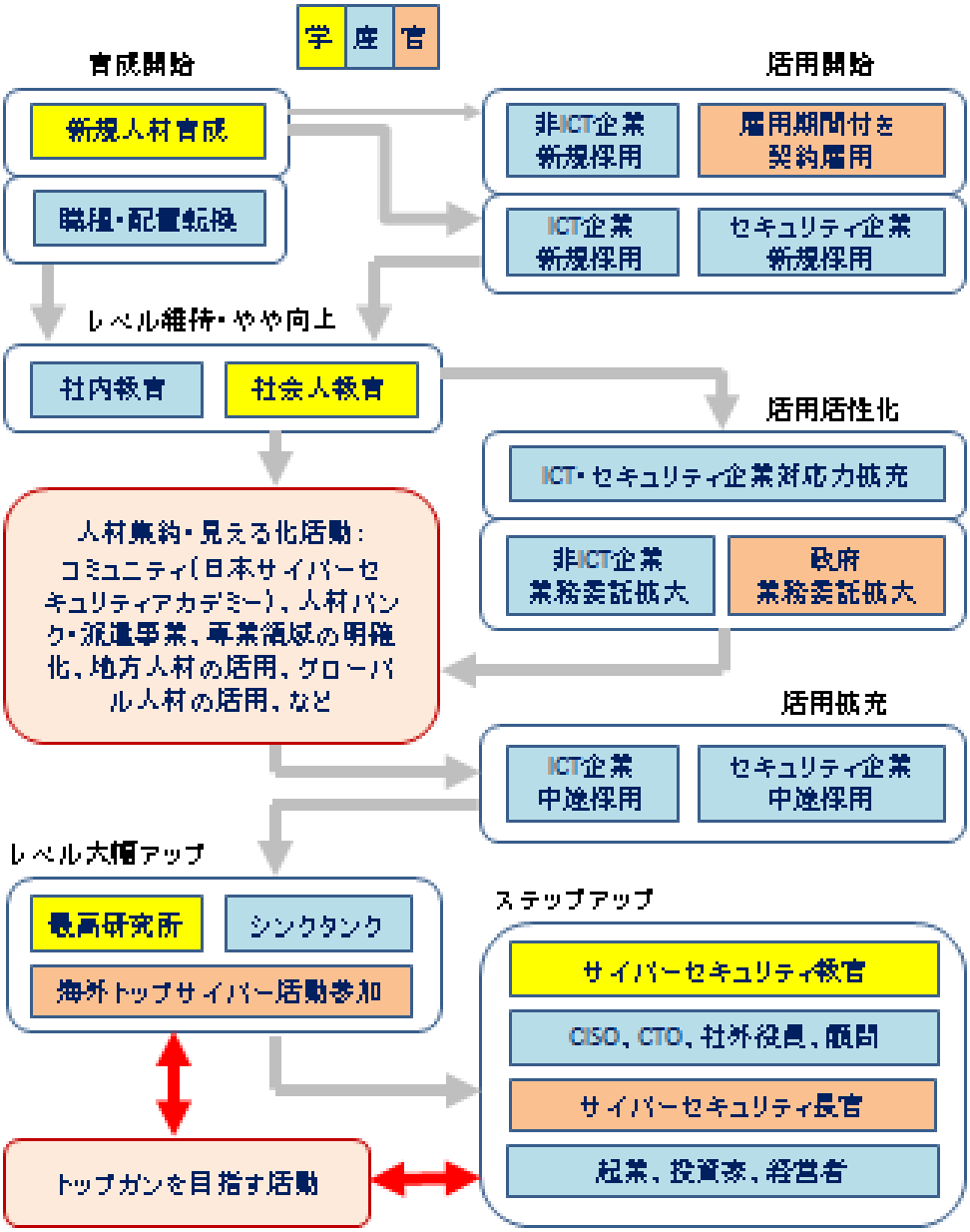

図 6　エコシステムでのキャリアパス例******

参考文献

1）http://cyber-risk.or.jp/sansanren/2.bessi_1_1.0.pdf

2）http://ogc.or.jp/article/1726

3）http://cyber-risk.or.jp/sansanren/index.html

4）“イスラエルのエコシステム、“破壊的” ベンチャー生み出す”、日経コンピュータ、ITPro(http://itpro.nikkeibp.co.jp/atcl/column/14/092900078/093000001/)

補足説明

*) 図１　人材育成を指摘したシミュレーション

トップガン（GOO 国語辞典）：米国空軍士官学校の最優秀の卒業生。転じて、ある分野・社会のトップクラスの人。

ここでは、ホワイトハッカーをトップガンとは捉えていない。単独攻撃を一人のホワイトハッカーが対応することは理解できるが、多数の攻撃者による組織的攻撃に対して一人のホワイトハッカーが対応することは想定していない。組織的攻撃は同時多発的に複数個所で発生する。2011 年の攻撃でも、同時期に複数企業に対して行われた。これまでは、企業間の連携も情報共有もなく、同業者が攻撃を受けていても知らないまま自分も攻撃を受け、どの企業も対応が後手に回り一様に被害を受けてしまっている。個々の企業には優秀なセキュリティ担当がいたと考えると、優秀な担当がいても一組織の中で動くのでは攻撃は防げない、と結論づけられる。

トップガンへの期待は、この打開であり活動範囲は組織に閉じない。ホワイトハッカーや各組織のトップ技術者をまとめ、適切な指示をだして攻撃を食い止める、少なくとも被害の拡大は阻止する、ことを役割とする。各組織でトップの技術者でも、一組織に閉じて活動する限りトップガンではない。技術レベルがホワイトハッカーでも、これは変わらない。企業内のシステム環境に責任を持つ IT 部門のトップ技術者はトップガンではない。

SOC で作業する技術者やアナリストが、複数企業を攻撃から守るように動くと、トップガンよりにいると考える。被害が出ることがわかっていて手を打たない、被害が出始めたことがわかって拡大を止めない、という動き方はトップガンではない。トップガンならば、使えるものは全て使って被害を止めるか最小限にとどめることを達成する。この結果で資格が評価される。トップガンに言い訳や弁解は許されない。

トップガン補佐は、一匹狼のホワイトハッカー、企業 IT 部門の中間層エリート、サイバーセキュリティ研究者など。トップガン直下でそれぞれの役割を果たす。トップガンは、責任、権限、能力、範囲などとても重く、他とは大きな差がある。補佐はトップガンの責任や権限を代行する立場にはない。

中間層エリートは、企業内でトップのサイバーセキュリティ技術者、管理者である。トップガン補佐として、トップガンの組織横断活動を支える役割も果たす。

**) 図 2　個人のキャリアパスから見たエコシステム

教育機関の教育を修了した個人が、トップガンまで到達したいと望んだなら、そこまでのキャリアパスが存在し、キャリアアップにチャレンジする機会が必ず与えられる、ことが重要であり必須と言える。企業に入った後でも同じ。パスは一通りではなく、後戻りもやり直しも可能で、それがキャリアアップにチャレンジする機会を妨げることはない。それぞれのキャリアパスは違って構わない。

日本サイバーセキュリティアカデミーは、柔軟なキャリアパス設計、キャリアアップ時期、それぞれのペースでの実行を行いやすくする。そのために、最新情報や技術の習得、再教育機会を得ることができ、ここは企業と教育機関とで運営される。

最高峰サイバーセキュリティ研究機関は、企業では持ちきれないので、産官学共同で設置、運用維持を検討するのが望ましい。

***) 図 3　産官学の協力から見たエコシステム

このテーマは実行し続けることが重要で、産官学が協力する上で難しい点でもある。個人のキャリアパスで考えると、大学在籍から社会で現役を退くまで 40 年はある。これから毎年 2000 人卒業生をだし（仮に 1 大学 100 人、20 大学から）、市場で 5 万人維持すると仮定すると、5 万人到達まで 25 年、単純計算しても 65 年継続するシステムをデザインしておく必要がある。実際にはこうならないが、長く機能し続けるシステムにする必要性があることは事実で、関係者に徹底しておきたい。攻撃は常に高度化し続けるとすると、体制はともかく社会人継続教育の内容は 65 年間進化し続けないといけない。

****) 図 4－1　技術系人材が少ない企業

****) 図 4－2　技術系人材は多くても IT 人材は少ない企業

ICT 企業の中に、実際にサイバーセキュリティ人材に転換可能な潜在人材がここまで多くいるかは疑問が残るが、理解しやすくデフォルメするとこうなる。

ここで注意すべきは、攻撃者以上の努力とスキルアップを日々しておかないと、攻撃を受けたら時間の問題で被害が出てしまう、ということである。CISO と CSIRT の設置は、設置で問題が解決することはなく、解決へのスタート位置にようやく立てる、ということである。

IT 技術者の少ない、ましてやサイバーセキュリティ技術者がほぼいない非 ICT 企業で、どんな CSIRT を持つべきか、よく検討した方が良い。教科書通りに作ってもおそらく長続きしない。

*****) 図 5　重要インフラシステムの運用課題

大規模システムの開発に、何百人もの設計者や開発者がかかったと言われても違和感はない。新規システムだと最新技術を導入するため、もっとも優秀な設計者、開発者が参画する。とても高額である。システムが完成すると保守フェーズになり、運用手順はマニュアル化され基本誰でも行えるようになる。年を経るごとに運用コストは削減され、運用者も入れ替わる。システムの無停止運転が第一優先の時はこれで目的を果たせたが、サイバー攻撃からシステムを守るという目的なら、あまりに脆弱な体制と言える。

本体の専用システムの仕様は第三者に把握されにくいが、昔と違い、その周りを取り巻く装置やソフトは汎用品に依存するようになっている。これらは簡単に攻撃できる。かつ、こういった汎用品の運用はベンダーに依存しており、専用システムの運用管理チームで十分取り扱えないことも多い。裏口を組み込まれていてもわからない。

******) 図 6　エコシステムでのキャリアパス例

トップガンが十分生まれる社会システムにたどり着くまでの道のりは長い。遠くても、育成を開始しなければ何も生まれてこない。長期的には大学の役割が重要だが、2020 年までの短期間を考えると、企業の役割がとても大きい。企業内の人材を、職種・配置転換してサイバーセキュリティ人材を増やさなければならない。ここが新しい産業を起こせるか、起こした産業が大きくなるかのカギになる。サイバーセキュリティという領域では、この先しばらくは人材が中心の産業になるからである。ここを産官学の関係者が理解し協力し合うことが不可欠である。