

**「サイバーセキュリティ人材育成分科会」第1次取りまとめ案に対して提出された意見
及びその意見に対するサイバーセキュリティ人材育成分科会の考え方**

(意見募集期間：令和元年5月11日～同年5月31日)

提出意見：9者

法人：1者（日本ネットワークセキュリティ協会 社会活動部会）

個人：8者（個人A～個人H）

【総論】

| 意見 | 考え方 | 提出意見を踏まえた案の修正の有無 |
|--|--|-------------------------|
| <p>意見1 初等中等教育及び警察組織に対するサイバーセキュリティ人材育成が考慮されるべき。</p> <p>○ 基本的に賛成ですが重要な視点が欠けています。それは、初等中等教育のサイバーセキュリティです。「日本全国に存在する小学・中学・高校のほぼ全ては、従業員ベースで中小企業である」という事実を今回の取りまとめに当てはめた時、危機的な状況であることは即座に理解いただけだと思います。まだ人材があり、規模が大きい大学は整備されつつありますが、高校までは悲惨です。教育現場は、ようやくデジタル教科書が制度として動き始めたように、遅々としながらも教育の情報化は進んでいます。次に来るべきは情報化によって集められた教育データの利活用です。この分野で日本は世界から完全に遅れています。この状況に対する危機感から、日本学術会議でも教育データ利活用分科会 (http://www.scj.go.jp/ja/member/iinkai/bunya/jyoho/index.html) が立ち上がり、同僚も議論されていますが、データの収集元となる教育現場における人材育成はかなり厳しいです。文科省も (http://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1397369.htm) のように努力していますが、厳しいです。教育現場を支える ICT 支援員という立場はありますが、給料は安く、しかし求められる業務の種類の豊富さは半端なく多く、足りていません。</p> <p>今回の取りまとめで、人材が育たない問題を、地域格差の問題や規模の大小に求められていますが、私の考えでは、日本国民が生まれてから最初に教育を与える組織が、サイバーセキュリティに対してあまりにも無知であることも重要と思</p> | <p>初等中等教育の現場等を含め、地域におけるサイバーセキュリティ人材を確保することは重要な課題であり、今後の総務省における取組の参考とさせていただきます。</p> | <p align="center">無</p> |

います。サイバーセキュリティ対策や意識について、負のスパイラルに陥る前にスタート地点がマイナスです。とはいえ、まだ間に合います。まだ学校にデジタル端末は完全に行き渡っていませんので。あと5年くらいが勝負でしょう。

ポイントは2つです。

まず、学校のサイバーセキュリティ対策を教育の問題と片付けず、産業界が取り組むべき根本課題として、省庁を超えて予算を確保することです。現在の文科省の予算では絶対に足りません。

もう1つは、セキュリティ人材のエコシステムに、初等中等教育の現場と、警察組織をしっかりと組み込むことです。学校現場にセキュリティ人材が必要となることで就業機会が全国くまなく増えます。また、生徒に対する情報モラル教育はそれなりに各学校がされていますが、教員に対する情報セキュリティ教育を増やすべきです。ただ、この際にはある程度公的な性格を帯びた組織が受け持つべきでしょう。ベストは警察と考えています。私も関わっている京都府警察のネット安心アドバイザー(教育モラルを主に高校で出前講義、体験学習、しかし最近はやお年寄りも対象が多い)[https://www.pref.kyoto.jp/fukei/anzen/cyber](https://www.pref.kyoto.jp/fukei/anzen/cyber/cyber13.html)

[/cyber13.html](https://www.pref.kyoto.jp/fukei/anzen/cyber/cyber13.html)のような仕組みの整備です。警察組織のサイバーセキュリティ対策も地域によっては遅れているとは聞きます。しかし、セキュリティ人材は現在の警察の業務との相性もいいですから、最初は警察に対してもレクチャーしながら、徐々に警察がコーディネートしていくような形で、これを機会に警察組織のセキュリティ意識を機に高めては良いかと思えます。

【個人A】

| | | |
|---|--|----------|
| <p>意見2 「情報処理安全確保支援士」を「地域で活用する」といった観点での取組を行うことが有益。また、サイバーセキュリティ人材の能力について定義を記載すべき。</p> | <p>情報処理安全確保支援士を含め、地域におけるセキュリティ対策を向上するために活躍が期待される人材や、求められる能力等については、本取りまとめを踏まえ総務省が実施するモデル事業等を通じて検討を深めることが必要であると考えます。</p> | <p>無</p> |
| <p>○ サイバーセキュリティ人材の育成について、既存の仕組みを利用しないことを前提としている点について、直ちに有効な改善策として「情報処理安全確保支援士」の活用を提言したい。</p> <p>なぜならば、「情報処理安全確保支援士」に至る過程として「情報セキュリティマネジメント試験」「ITパスポート試験」と段階的な能力開発が詳細に定義されており、民間における試験対策講座や職場における勉強会といった育成プロセスも十分に成熟していることや、サイバーセキュリティは全世界的な観点で最新の技術的な知見に基づいて取り組む必要があることから、サイバーセキュリティ人材について「地域で育成する」といった観点ではなく、サイバーセキュリティについて既に高度な知見を有していることが国家資格により認定されている「情報処理安全確保支援士」を「地域で活用する」といった観点での取組を行う方が、即効性、有効性、経済性といったあらゆる観点から有益であると考えからである。</p> <p>また、サイバーセキュリティ人材と呼称される存在の能力について定義が記載されていない。これについては、1. 現時点で唯一の国家資格であること 2. 登録状況をWebで確認でき安心して情報セキュリティに関する助言を得られること 3. 定期的な研修が義務付けられており能力が担保されていること の3点から、「今回とりまとめ案に記載したサイバーセキュリティ人材としては情報処理安全確保支援士を想定している」という記載を追加することを提言する。</p> <p>セキュリティ人材として、情報処理安全確保支援士を積極的に活用する取組が必要である。セキュリティ対策においては、情報システムが、交通・水道・電力と並ぶかそれ以上の重要な社会インフラとなっている社会背景を考慮し、まずは公助による確実な支援体制を確立し、自助、共助の仕組みを構築する必要がある。本分科会における検討結果に基づき、「地域」を切り口とした情報処理確保支援士の活用に関するモデル事業を実施し、そのモデル事業を元に全国への横展開を実施するといった、Society5.0時代の持続可能な地域社会の実現に貢献することが期待される。</p> <p style="text-align: right;">【個人B】</p> | | |

| | | |
|--|--|----------|
| <p>意見3 政府主体の活動のみならず、産業界主体の活動の支援を行うことで官産連携施策としてのシナジー効果を生み出すことができると考える。</p> | <p>御指摘のとおり、セキュリティ人材の育成にあたっては、官民で連携して行うことが必要であると考えます。</p> | <p>無</p> |
| <p>○ サイバーセキュリティ人材の不足に関する地域的格差については、産業界としても大きな課題と認識しており、産業界主体での地域におけるセキュリティ人材の裾野の広がりや、底上げを図る活動を行ってきている。政府に置かれては政府主体の活動のみならず、産業界主体の活動の支援を行うことで、官産連携施策としてのシナジー効果を生み出すことができると考える。</p> <p style="text-align: center;">【日本ネットワークセキュリティ協会 社会活動部会】</p> | | |

【1 はじめに】

意見無し

【2 地域のセキュリティを巡る現状・課題】

| 意見 | 考え方 | 提出意見を踏まえた案の修正の有無 |
|---|--|------------------|
| <p>意見4 ISEPA（情報セキュリティ教育事業者連絡会）では地方や中小企業で必要とされているセキュリティ業務の内容や、アウトソーシングが可能な業務の整理を行っているため政府施策として活用されることを要望する。</p> <p>○ JNSA 内の組織「情報セキュリティ教育事業者連絡会（ISEPA）」では、セキュリティ人材の実態調査を行い、実際に地方や中小企業で必要とされているセキュリティ業務の内容や、アウトソーシングが可能な業務の整理を行っている。</p> <p>また、可視化ツールによる適材適所配置の研究等を行っており、潜在的に存在するセキュリティ業務を行える人材を発掘し、地域にとらわれることなく必要とされている組織にマッチングするなどの検討を行っている。漠然とした業務ニーズではなく、職務内容（job description）を明確に示し、それに対して保有するスキルのマッチングを行うことで、今よりも需給のミスマッチは少なくなってくると思われることから、地域におけるセキュリティ人材のシェアリングなどの政府施策にも積極的に活用されることを要望する。</p> <p style="text-align: right;">【日本ネットワークセキュリティ協会 社会活動部会】</p> | <p>御指摘の調査等については、本取りまとめを踏まえて、総務省が実施するモデル事業等において、参考とされることと思われます。</p> | <p>無</p> |

【3 地域におけるセキュリティ人材育成に向けた方策】

| 意見 | 考え方 | 提出意見を踏まえた案の修正の有無 |
|--|---|------------------|
| <p>意見5 地域におけるセキュリティファシリテーターについて、他制度等との整合性を取るべき。また、関係省庁と連携を行うべき。</p> <p>○ 地域におけるセキュリティファシリテーターの育成ですが、同様な事が経済産業省(IPA)で情報セキュリティプレゼンター制度が試みられています。この制度の活用状況がどの程度であるか判りませんが、最近では情報処理安全確保支援士を積極的に活用しようとしている動きがあります。また、営業的なセンスのあるスキルを持った人材としてITコーディネータ制度がありますこれらの制度との整合性を取るべきではないでしょうか。</p> <p style="text-align: right;">【個人C】</p> <p>○ 現場部門の情報セキュリティ管理者として、部門のセキュリティ管理スキルを身に付けた情報セキュリティマネジメント試験、約7万人の合格者を都市部の民間企業はもとより、規模の小さな中小企業が多い地方においても、セキュリティを担う戦略マネジメント層人材として、企業の採用選考や従業員の処遇において有効に活用していくことを総務省・経済産業省・NISCが緊密な連携の下で推奨してはどうか。</p> <p>全ての社会人が持つべきITリテラシーについての基準を策定するとともに、ITパスポート試験を拡充してITリテラシーを認定するためのITパスポート4.0試験を実施し、各省庁の省益を超えて挙国一致で最大限に同試験を活用してはどうか。民間企業等において情報漏えい等の被害が発生しており、セキュリティ人材を育成することは急務である。地域力を結集、活用してセキュリティ人材の裾野を広げ、底上げすることにおいては、企業の業務担当者としての情報セキュリティリテラシー、全てのビジネスパーソンに基礎的ITリテラシーが備わることで人材育成に資するのではないか。研修機会の偏在についても現在、民間教育事業者・大学・団体等で開講されている、ITパスポート試験の対策講座は42講座(通信講座を含む)あり、問題には当たらない。</p> <p>IPAにおいて、インターネットを活用して調査した結果地方の中小企業で</p> | <p>地域におけるセキュリティファシリテーターの育成については、既存の取組を含め、関係省庁と密接に連携して取り組むことが必要であると考えます。</p> | <p>無</p> |

は十分にセキュリティ体制が構築されていないといった組織体制の偏在についても、ITリテラシースタンダード1級、ITSSとの対比でITパスポート4.0の合格者であるならば、事業運営上の先端IT活用の企画提案・システム部門等との実務的な調整等や情報セキュリティの知識、リスク対応までを含めて事業部門の立場でリードするレベルとある。受験機会が頻繁にあるITパスポート4.0の最大活用によって、ファシリテーターは古い知識ではなく最新の知識を習得していることが必要という要件にも対応できる。就業機会の偏在、地域においてセキュリティに関する雇用の受け皿が無い課題は、事業運営上の付加価値創出を先導できる人材としての、職務の広がり、事業部門のリーダークラスとしての昇進、その他のキャリアアップ実現について等、企業の採用選考や従業員の処遇においてAI、ITリテラシー1級に関する能力の反映を促すことでITパスポート4.0を国家が後押ししていくことで解決に繋がっていくのではないか。

利用者側において情報技術に関する一定の知識・技能をもつ者であり、担当する業務の情報化を利用者の立場から推進する初級システムアドミニストレータ試験、約50万人の合格者が存在する。合格した者の中には、履歴書に記載しただけで資格を休眠させている者なども一定数、存在しているだろうと推察する。これらの中には、結婚などにより企業を退職した者も含んで考える。総務省が経済産業省と緊密な連携を組んで、初級シスアド人材に対して、情報セキュリティ人材への転換を促していくために、リカレント教育プログラムを総務省が策定し、試験なり講習を行って情報セキュリティ人材として認定する仕組みを整えてはどうか。総務省と経済産業省の緊密な連携の下、初級シスアド試験50万人の合格者をターゲットとして、リカレント教育を施したならば、地域におけるセキュリティファシリテーターの育成にも資するのではないか。

【個人D】

| | | |
|---|---|----------|
| <p>意見6 公的機関や自治体において情報処理安全確保支援士を任用条件とする「情報セキュリティ専門監」を新設し、地域におけるセキュリティファシリテーターとして活動させるべき。</p> | <p>セキュリティファシリテーターに求められるスキルや資格等については、本取りまとめを踏まえて総務省が実施するモデル事業等を通じて検討を深めることが適当であると考えます。</p> | <p>無</p> |
| <p>○ <P13> 「地域の中核企業やリーダーが中心となって」という記載があるが、地域の中核企業も少子高齢化による人材不足に直面しており、また、地方になればなるほど取引関係の密度が上がることから、「取引関係に関わらず」といった発想は、実態と乖離した無責任な提言であると考えます。これに対して、各地域に公的な産業振興センターが設立されているが、そういった公的機関や、県及び政令市の情報政策部門と産業振興部門を統括する形での「情報セキュリティ専門監（情報処理安全確保支援士を任用条件とする）」の設置を促し、公的機関が中核となって地域全体のセキュリティ対策を底上げする、といった考え方の方が現実的であり地域の企業の参加も容易なのではないか。よって、本部分については以下のとおり修正することを提言する</p> <p>「このようなコミュニティを構築するためには、県及び政令市の情報政策部門と産業振興部門の連携又は既存の産業振興センターを活用し、それぞれに情報処理安全確保支援士を任命要件とする「情報セキュリティ専門監」職を必置化し、地方公共団体が中心となって地域全体のセキュリティ対策を底上げすることが必要ではないか。」</p> <p><P15> P13に関する意見と同様に「民間任せ」ではなく、「地方公共団体が責任をもって」「情報処理安全確保支援士」による体制を構築することが必要であると考えます。よって、各提言についてそれぞれ以下の内容に変更することを提言する。</p> <ol style="list-style-type: none"> 1. そのような活動を県及び政令市に設置した情報処理安全確保支援士であることを任用要件とする「情報セキュリティ専門監」を中核として責任をもって展開できるよう、県及び政令市に対して、情報処理安全確保支援士の所属状況の調査を行うとともに、調査結果を基にモデル事業実施に必要な体制及び人事上の措置を講ずることを指示する。 2. 県及び政令市において「情報セキュリティ専門監」に任命されたものについて、着手できる団体から順次ファシリテーターとして育成するためのモデル事業を実施する。 3. ファシリテーターは古い知識ではなく最新の知識を習得していることが必要 | | |

であり、最新情報を常にアップデートすることが地域での信頼を得るためにも重要である。このため、最新の知識の習得と継続的な研修が義務付けられている情報処理安全確保支援士を、地域における Society5.0 における中心的役割を果たす人材として、支援する政策を立案する。

<P16> 中小企業 1 社で…複数の企業が共同でシェアすることができるのではないかとあるが、利害が対立する中小企業間でのシェアというのは困難であり、当初から中立的立場を要求される公的機関に設置するほうが合理的であると考えられる。よって、以下により修正することを提言する。

1. 企業等において必要なセキュリティ対策の優先度に応じて、大勢の整備や設備の導入など、組織として講じるべき措置について助言等を行うことができる「情報セキュリティ専門監」制度を県及び政令市において整備し、その責任において担当監を責任者とした部門自ら、又は地域ごとの情報処理安全確保支援士とのマッチングを行い、複数の中小企業でシェアするためのモデル事業を実施する。
2. モデル事業の成果を全国的に横展開することで、情報処理安全確保支援士が在職していない県及び政令市において、「情報セキュリティ専門監」を必置化することにより資格取得又は有資格者の採用を促進し、地域におけるサイバーセキュリティに関する組織態勢の底上げを図る。

漠然とした「セキュリティ人材」との連携といった定義では、能力・資質に課題がある連携体制になることが予想されるため、以下の内容を追記することを提言する。

「情報処理安全確保支援士により構成されている、情報処理安全確保支援士会（設立準備中）と地方公共団体の連携を促進することにより、拡大するセキュリティリスクに対応できる体制の構築を図る。」

【個人B】

| | | |
|--|---|----------|
| <p>意見7 既存のセキュリティ関連団体が多く存在し地域におけるセキュリティファシリテーターの育成を目指した活動が行われているため、これらの民間団体への活動支援が行われることを要望する。</p> | <p>本取りまとめを踏まえて総務省が実施するモデル事業等の実施にあたっては、民間での既存の取組も参考にしながら、行うことが必要であると考えます。</p> | <p>無</p> |
| <p>○ JNSA をはじめとする産業界におけるセキュリティ関連団体はすでに多く存在し、地域ごとに人材育成の支援を行ってきている。JNSA では産学連携により岡山理科大をはじめとする高等教育機関向けに遠隔授業による支援や、高専機構との連携などによる高等教育機関向けの育成支援を行ってきている。また、JNSA 以外の団体でも、「草の根サイバーセキュリティ運動全国連絡会 (Grafsec)」や「セキュリティ対策推進協議会 (SPREAD)」といった、特に地域におけるセキュリティファシリテーターの育成を目指した活動が行われているため、これらのすでに行われている民間団体への活動支援が行われることを要望する。</p> <p>【日本ネットワークセキュリティ協会 社会活動部会】</p> | | |
| <p>意見8 複数の企業で共同して退職者等の副業を活用する形では、個々の企業に対するサービスの提供が希薄となり、十分な効果が発揮されないのではないか。</p> | <p>中小企業では、一社でセキュリティの専門家を雇うことができない場合が多いことから、複数の企業で共有して専門家を活用する場合であっても、個々の企業にとって十分に効果が発揮されることとなるようなモデル事業を実施することが必要であると考えます。</p> | <p>無</p> |
| <p>○ 3(2)についてですが、複数の企業で共同し、更に退職者等の副業を活用したのでは、個々の企業に対するサービスの提供が薄くなりすぎ、十分なサービスの提供ができないおそれがあると思います。</p> <p>【個人E】</p> | | |
| <p>意見9 「情報処理安全確保支援士」と、その育成に関するエコシステムを含めた「人材活用」での施策を講じるべき。</p> | <p>意見2に対する考え方とおおり。</p> | <p>無</p> |
| <p>○ <P21> 全体的に「公助」の観点が抜け落ちているとともに、情報処理安全確保支援士を育成することによる社会全体の情報セキュリティ人材育成事業に対して「蛇足」のページとなっているように見受けられます。例えば、情報セキュリティ分野においては「情報処理安全確保支援士」があり、その前段階としての「情報セキュリティマネジメント試験」があり、さらに入門編としての「IT パスポート試験」という形で、人材育成については既に整備が完了しており、高等教育機関での学習により情報処理安全確保支援士の一部試験免除制度といったエコシステムも形成されています。よって、総務省においては「人材育成」ではなく、既に存在する「情報処理安全確保支援士」と、その育成に関するエコシステムを含めた「人材活用」での施策を講じられるべきだと考えます。これらのことから、本ページは</p> | | |

全て削除することが望ましいと考えます。

県及び政令市に情報処理安全確保支援士を任命要件とする「情報セキュリティ専門監」を設置し、そこが中心となって地域の情報処理安全確保士会との連携により、地域全体で面的にサイバーセキュリティの関心を高めることが求められる。そのうえで、サイバーセキュリティに関心を持った個別の中小企業等が「情報セキュリティ専門監」や「情報処理安全確保支援士」と連携しながら、効率的にセキュリティ対策に取り組む仕組みの構築が求められる。また、こうした取り組みが地域に根付き自走するためには、各地域の「情報セキュリティ専門監」を中心とした部門が下支えしつつ、情報処理安全確保支援士が活躍できるエコシステムの形成が求められる。

【個人B】

【4 むすび】

| | | |
|---|-----------------------|----------|
| <p>意見10 Society5.0の推進のためには情報処理安全確保支援士の活用が必須。 十分な雇用機会が無く市場規模の小さい地方の現状を踏まえると、実現性に乏しい民間による活動を前提とするのではなく、県及び政令市を中心的存在として活動を拡大していく方策を採用すべき。</p> | <p>意見6に対する考え方のおり。</p> | <p>無</p> |
| <p>○ <P22> Society5.0の推進のためには情報処理安全確保支援士の活用が必須であり、その活用方法を確立することが不可欠であると考え。また、十分な雇用機会が無く市場規模の小さい地方の現状を踏まえると、実現性に乏しい民間による活動を前提とするのではなく、県及び政令市を中心的存在として活動を拡大していく方策を採用すべきである。</p> <p style="text-align: right;">【個人B】</p> | | |

【その他】

| | | |
|---|------------------------------------|----------|
| <p>意見 11 サイバーセキュリティ人材として、外国人高度人材を活用すべき。</p> | <p>いただいた御意見については、参考とさせていただきます。</p> | <p>無</p> |
| <p>○ サイバーセキュリティ対策におけるセキュリティ人材の不足は、日本国での低レベルな「高等専門学校、大学、大学院」等で、教育を導入し、日本国での人材の育成を施行して行くと、無駄な財政コストが掛かるので、私は反対です。例えばですが、約1パーセントの「天才(ジェニーパーソン)」と約99パーセントの「凡人(オーディナリーパーソン)」を「区別(セパレーション)」して行くべきです。セキュリティ人材の育成では、「学歴(エデュケーション)」等の要因では、無い状態で、「経験及び実績(キャリア)」の方が重要視される事と、私は考えます。</p> <p>具体的には、セキュリティ人材の「解決案(ソリューション)」では、「5G(第5世代)、IoT(インターネットオブシングス)、AI(人工知能)」における「外国人高度人材(高度外国人人材)」での「大学院修士号及びそれと同等の経歴を持つ者(マスター以上)」を導入すれば、解決する事と、私は考えます。</p> <p>日本国は、約99パーセントの「凡人(オーディナリーパーソン)」を「増加(インクリース)」し、約1パーセントの「天才(ジェニーパーソン)」を「削減(ディクリース)」して来たので、日本国が自分で招いた構造なので、日本国における国家主権及び国民主権での「責任(リスボンサビリティ)」が有り、日本国における社会構造での「問題(プログラム)」で、自業自得での国家の構造と、私は考えます。</p> <p>例えばですが、日本国における「STEAM(科学、技術、工学、芸術、算数及び数学)」の構造では、男性が約50パーセントで有り、女性が約10パーセントで有ると、私は思います。日本国における「STEAM」での対策では、中高年女性及び高齢者女性が約50パーセントに到達する迄には、1世代が約20年として、女性の「STEAM」を導入する事では、「約2世代(約40年)」を必要と成るので、日本国における女性の「STEAM」では、時既に遅しの手遅れの状態と、私は思います。</p> <p>要約すると、垂直思考での付加価値の高い構造に対し、平行思考での効率性を上げる為に無駄を削ぎ落とし、垂直思考での生産性を向上させる構造が望ましい構造と、私は考えます。例えばですが、「哲学(フィロソフィー)及び算数(エレメンタリーマスマテック)」から成る「倫理観(モラルフィロソフィー)」及び「科学技術(サイエンステクノロジー)」では、「人類(スピーシス)」が外付けに着けて来た構造では、「狩猟時代(ハンティング)、農耕時代(ファーミング)、産業時代(インダストリー)、情報技術時代(IT)、人工知能時代(AI)、宇宙居住時代(スペースコロニー)」の構造と、私は考えます。</p> | | |

要するに、付加価値の低い構造では、「狩猟構造(ハンティング)及び農耕構造(ファームング)」では、質より量での「マンパワー(人力)」による「共同体(コミュニティー)」の人材育成が基本と思いますが、付加価値の高い構造では、「産業構造(インダストリー)、情報技術構造(IT)、人工知能構造(AI)、宇宙居住構造(スペースコロニー)」では、量より質での「機械(マシーン)」による「個人体(個人パーソナル)」の人材育成が基本と、私は思います。「解決案(ソリューション)」では、人材育成では、高度化する程に「量より質」の追求が必要と、私は考えます。サイバーセキュリティ対策でのセキュリティ人材の育成では、「人工知能(AI)及び宇宙居住(スペースコロニー)」の構造に対し、「焦点(フォーカス)」を描くと、情報の付加価値の高い人材が必要と成ります。「皮肉(アイロニー)」にも、人材育成では、「現実的(リアル)」な構造では、肉体は、「人間(ヒューマン)」の身体能力で、「頭脳(ブレイン)」は、「チンパンジー(猿)」では、不良品で有り、「目標的(ターゲット)」な構造では、肉体は、「チンパンジー(猿)」の身体能力で、「頭脳(ブレイン)」は、「天才(ジェニー)」では、優良品で有ると、私は考えます。

○ サイバーセキュリティ対策における構造を明確にするべきと、私は考えます。

例えばですが、「センサー技術、ネットワーク技術、デバイス技術」から成る「GPS(サイバーフィジカルシステム)」の導入により、「ゼネコン(土木及び建築)、船舶、鉄道、航空機、自動車、産業機器、家電」等が融合される構造と、私は考えます。

具体的には、「電波規格(エレクトリカルウェーブスペック)」の事例が有ります。(ア)「通信衛星回線(サテライトシステム)」における「トランスポンダー(中継器)」から成るポート通信での「DFS(ダイナミックフレカンシーセレーション)」の構造。(イ)「電話回線(テレコミュニケーション)」における基地局制御サーバーから成る「SIPサーバー(セッションイニテエーションプロトコル)」の構造。(ウ)「インターネット回線(ブロードバンド)」におけるISPサーバーから成る「DNSサーバー(ドメインネームシステム)」の構造。(エ)「テレビ回線(ブロードキャスト)」における「通信衛星回線、電話回線、インターネット回線」の構造。

具体的には、「通信規格(トランスミッションスペック)」の事例が有ります。(ア)「3G(第3世代)」における「GPS(グローバルポジショニングシステム)」から成る「3GPP(GSM方式及びW-CDMA方式)」の構造。(イ)「4G(第4世代)」における「LTE(ロングタームエボリューション)」から成る「Wi-Fi(ワイアーレスローカルエリアネットワーク)」の構造。(ウ)「5G(第5世代)」での「NR(New Radio)」における

| | | |
|--|-----------------------|----------|
| <p>「VPN(バーチャルプライベートネットワーク)」の構造。</p> <p>具体的には、「情報技術(IT)」及び「人工知能(AI)」の事例があります。(ア)クラウドコンピューティングでは、「ビッグデータ(BD)」から成る「データベース(DB)」を導入した、ITネットワークの構造。(イ)エッジコンピューティングでは、Web上での「URL(ユニフォームリソースロケータ)」における「HTML(ハイパーテキストマークアップラングエッジ)」から成る「HTTP(ハイパーテキストトランスファープロトコル)」での「API(アプリケーションプログラミングインターフェイス)」を融合し、「HTTPS(HTTP over SSL/TLS)」を導入した、AIネットワークの構造。</p> <p>要約すると、「サイバー空間(情報空間)」では、「SDN/NFV」での「仮想化サーバー(メールサーバー、Webサーバー、FTPサーバー、ファイルサーバー)」から成る「リレーポイント(中継点)」における「VPN(バーチャルプライベートネットワーク)」の構造と、私は考えます。「フィジカル空間(物理空間)」では、「AP(アクセスポイント)」の構造と、私は考えます。</p> <p>要するに、「サイバーセキュリティー人材」における育成では、日本国での財政コストが掛かるので、「外国人高度人材(高度外国人材)」での「大学院修士号及びそれと同等の経歴を持つ者(マスター以上)」を導入する事で、解決する事と、私は考えます。厚生労働省の管轄における「ハローワーク(職業安定所)」の「水準(レベル)」に対し、「外国人高度人材(高度外国人材)」を「基準(スタンダード)」に改革する事が必要と、私は考えます。</p> <p style="text-align: right;">【個人F】</p> | | |
| <p>意見 12 サイバーセキュリティー人材は必要。</p> | <p>賛同の御意見として承ります。</p> | <p>無</p> |
| <p>○ サイバーセキュリティー人材は必要だと思う。</p> <p style="text-align: right;">【個人G】</p> | | |
| <p>意見 13 概要としてはこれでよいのではないかと。</p> | <p>賛同の御意見として承ります。</p> | <p>無</p> |
| <p>○ 概要としてはこれでよいのではないかと思われた。意見は以上である。</p> <p>人材育成を外れて意見を行うと、現在の企業のWebセキュリティ担当者などは、例えばSMBCダイレクト(https://direct.smbc.co.jp/aib/aibgsjs5001.jsp 等。TLSv1.0までの対応、暗号スイートは低セキュリティなものばかり。)に見られるような、セキュリティについて問題あると思われる状況がある場合において、報告・通告があった様な事態にちゃんと対応を行うようにしていく必要があると考</p> | | |

える。そうしないと、いくら市民の目が企業を監視し、セキュリティ問題の存在とその是正にういての通告が行われるようになっても、結局甲斐無しという事になってしまうのであるが、それではせっかくの人材育成も効果が薄くなってしまいうので、人材育成に加えて、情報セキュリティの実務担当者(達)において、(通告等により認知されるに至った)実際に存在する問題事態への対処を、進んで行っていく様な空気の醸成が行われていく事を求めたい。

【個人H】