資料４－３

新・情報セキュリティ人材育成プログラム
（案）

平成２６年　　月　　日
情報セキュリティ政策会議

１．はじめに

本プログラム策定までの経緯

情報通信技術が、経済活動や社会生活において大きな便益をもたらし、さらにはイノベーションの源として一層の普及が進む中にあって、情報セキュリティ上のリスクの深刻化が進行しつつある。このサイバー空間を取り巻く環境の変化は極めて急速であり、また、社会のいたるところにグローバルにつながった情報通信技術が浸透するようになったことによりリスクも急速に拡散している。こうしたリスクへ対応するための情報セキュリティの確保には、質・量ともに従来をはるかに超えた取組が必要であり、それを支える人材の育成・確保が急務となっている。

情報セキュリティ分野の人材育成については、2011 年７月に、情報セキュリティ政策会議において 2011 年度から 2013 年度までの３年間及び中長期的な情報セキュリティに係る人材育成施策の今後の方向性について検討を行い、「情報セキュリティ人材育成プログラム」を決定した。

また、2012 年５月には「情報セキュリティ人材育成プログラムを踏まえた 2012 年度以降の当面の課題等について」を普及啓発・人材育成専門委員会において策定し、企業、政府機関等における情報セキュリティ人材の育成施策の課題及び具体施策提言についてとりまとめを行った。

政府としては、これらに基づき、各種人材育成施策を推進してきたが、近年サイバー空間を取り巻くリスクの深刻化が急激に進展していることや、人材育成は短期的に結果が出る課題ではないことから、現状では未だ十分な成果が出ているとは言い難い。

こうした中、情報セキュリティ政策会議は、国家の安全保障・危機管理、社会経済の発展、国民の安全・安心確保のため、新たな情報セキュリティ戦略として、世界を率先する強靭で活力あるサイバー空間を構築し、「サイバーセキュリティ立国」を実現することを基本的な方針とする「サイバーセキュリティ戦略」を 2013 年６月に決定した。

この中で、人材育成に関しては、産業活性化、研究開発及びリテラシー向上とともに、サイバー空間の創造力・知識力の強化を目指す「活力ある」サイバー空間の構築のための方策の１つと位置付け、情報セキュリティ人材の不足解消に向けた積極的取組として、情報セキ

ュリティ従事者の能力の底上げ、突出した人材の発掘・育成、グローバル水準で活躍できる人材の育成、政府機関等における人材育成等を掲げている。

また、国家安全保障戦略（2013 年 12 月国家安全保障会議決定・閣議決定）においても、サイバー空間の防衛及びサイバー攻撃への対応能力の一層の強化を図ることとしており、セキュリティ人材層の強化などについて総合的に検討を行い、必要な措置を講ずることとしている。

さらに、2013 年 12 月には高度情報通信ネットワーク社会推進戦略本部（IT 総合戦略本部）において「創造的 IT 人材育成方針」が決定された。本方針では、「IT の利便性を享受して生活できる社会の構築と環境の整備」、「日本の IT 社会をリードし世界にも通用する IT 人材の創出」の２つを掲げ、今後、関係府省が取り組むべき具体的計画を検討していくこととしている。

本プログラムは、これらを踏まえて「情報セキュリティ人材育成プログラム」の見直しを行ったものである。基本的に今後３年間（2014 年度から 2016 年度）を対象とし、中長期的課題に対する視点も盛り込んで、今後推進すべき新たな人材育成戦略について取りまとめている。

２．情報セキュリティ人材に関する現状と課題

（１）サイバー空間を取り巻くリスクの深刻化

情報通信技術は、個人や家庭等の私的な空間から社会インフラ等の公的な空間、機器やデバイスの内部まで隅々に行き渡り、経済・生活基盤を支え国家の成長を牽引する存在となっている。このため、これらのシステム、ネットワーク等に障害が発生すれば社会に深刻な影響を及ぼすこととなる。このように、サイバー空間を取り巻くリスクは拡大し続けており、これまで以上に情報セキュリティ対策[1]が重要になっている。

【甚大化するリスク】

情報セキュリティに関する事故については、組織内部の職員等による過失または故意の事故が従来より多数発生しており、内部の情報管理等が引き続き重要な課題であるが、近

[1] 単なるコンプライアンス対策としてだけではなく、組織内のリスク管理の一環として実施される情報セキュリティ対策を指す。

年、外部からのサイバー攻撃のリスクが高まっている。かつてのサイバー攻撃はいたずらや愉快犯的な目的が多かったが、その後、経済目的のものが増加し、最近では、国家機関、防衛産業、重要インフラ事業者等及び研究機関などから機密情報や技術情報等を窃取することが目的とみられる攻撃が発生している。また、重要インフラサービスの提供に影響を与えるような脅威の顕在化も指摘されている。

こうした攻撃の多くは、いわゆる標的型攻撃[2]によると考えられ、情報システム等への内部侵入による被害は、システムの適切な設計や、脆弱性を作りこまないプログラミング、さらに、適切な運用・監視などにより、大幅に低減することが可能であると考えられる。このため、高度な情報セキュリティの専門人材のみならず、情報システム、制御システムなどの様々な分野において、基礎的な情報セキュリティ対策や、情報セキュリティを組み込んだシステム設計などに対応できる人材が求められている。

【拡散するリスク】

あらゆるものがインターネットに接続される時代となりつつあり、サイバー攻撃の対象となり得る機器が我々の身の周りの隅々まで行き渡ることによるリスクの拡散が進行している（図１）。最近では、スマートデバイスやデジタル複合機といった機器からの情報流出、家電製品や防犯カメラといった機器を踏み台としたサイバー攻撃等も発生している。

また、情報系ネットワーク等の外部ネットワークと切り離された独立系システムもサイバー攻撃の対象となっている。例えば、重要インフラの制御系システムに対して、ＵＳＢメモリ等を媒介として不正プログラムを感染させ、インフラのシステムや機器を稼働不能とすることも現実の問題となっている。

このように、情報通信技術が関係する製品・サービスの急速な拡大と、それに伴う情報セキュリティ対策の必要性が拡大する中、情報セキュリティに関わる問題は、単に情報セキュリティの専門家のみによって対応しきれる問題ではなく、IT 製品・サービスをはじめとして制御システムなどの様々な情報通信技術を用いた製品・サービス提供や運用を行う全ての者が一定の知識と能力を身に付け、情報セキュリティの確保に対応することが求められる状況となってきている。

[2] 標的型攻撃：特定の機関や組織のユーザーを狙ったサイバー攻撃のこと。典型例の一つは、標的とした企業の社員等に向けて、関係者や別の社員を装って不正プログラムが添付されたメールを送信する手法。

図１　IT の普及により広がるサイバー空間

こうした状況を踏まえ、「創造的 IT 人材育成方針」においても、「安全・安心に IT を製品・サービスなどに実装する人材」に求められる情報開発基礎力、システム基盤開発力、ソフトウェア開発力、情報サービス実用化力・提供力のいずれにも、情報セキュリティは共通して必要な能力とされたところである。

また、同方針中で、「情報セキュリティに関しては、一般的に、システム開発の下流工程になるほど、システムの脆弱性等を修正する費用は増大するとされているため、上流工程である企画、設計段階に携わる人材にも情報セキュリティの知識、技能が必要とされる」と指摘されているところである。

これらのことから、情報セキュリティを専門とする者のみならず、情報通信技術を用いた製品・サービスの企画、設計段階に携わる技術者等であっても、情報セキュリティに関し必要な基本的知識、能力が求められている。

【グローバルリスク】

世界各国における情報通信技術の利用拡大に伴い、サイバー空間を取り巻くリスクもグローバルに拡大している。サイバー空間には国境がなく、その脅威はボーダレスに波及してくるため、自らが海外に出て行かない場合でも常にグローバルリスクにさらされる状況にある。

例えば、海外において発生した外国政府機関等に対する DDoS 攻撃[3]において、一般個

[3] DDoS（Distributed Denial of Service）攻撃：ネットワークを通じた攻撃手法の一種で、標的となるコンピュータに対して複数のマシンから大量の処理負荷を与えることでサービスを機能停止状態へ追い込む手法。

人の所有する家庭用ＰＣが踏み台となり攻撃サーバに仕立てられた事案が発生したり、海外で企業の営業秘密等の窃取が狙われる標的型攻撃等の問題が顕在化している。また、グローバルなサプライチェーン等におけるひとつの点への攻撃が他の拠点へも影響することが危惧されている。

（２）情報セキュリティのスキルを有する人材の不足

サイバー空間を取り巻くリスクの深刻化に対し、「サイバーセキュリティ戦略」では、政府や重要インフラ、その他の企業等における対策を強力に進めることとしているが、その基盤として情報セキュリティ人材の充実が不可欠である。また、情報セキュリティ人材としては、情報セキュリティ意識の啓発、教育、運用までのマネジメントのスキルや、コンピュータ・ネットワーク防護など多様な領域における理解、実践能力が求められる。しかしながら、こうした情報セキュリティを支える人材については、様々な課題が残されている。

【経営層の情報セキュリティに対する認識上の課題】

今日、多くの企業その他の組織は、その経営・運営戦略の一環として情報システムを利活用しており、戦略遂行上重要な業務や情報を情報システムによって処理している。すなわち、情報通信技術の利活用は、企業において収益の源泉、またその他の組織においても業務の高度化等に資するものであり、営業秘密、機密情報等の重要な情報の保秘や正確さの確保、業務遂行上不可欠な情報システムの運用の維持などは、企業等の戦略上又は事業継続上不可欠な要素である。

しかしながら我が国の企業等においては、経営層が、情報セキュリティ対策の必要性は感じていても、経営戦略としての取組を積極的に行っているところは多いとは言い難い。情報セキュリティ人材への投資についてもその傾向はみられ、不足解消の取組について６割の企業が何らかの姿勢で取組意向を示しているものの、具体的な取組については特に行っていないという回答が半数近くを占めている。このことから見ても、まだ多くの企業等において、経営層が情報セキュリティに係るビジネスリスクを真に認識し、具体的な行動をとるには至っていないことが分かる。（図２）

また、情報セキュリティ対策を適切に考え、実践できる人材の前提として、情報通信技術に係る基礎的能力を着実に身につけたソフトウェア人材の存在が重要であり、ソフトウ

ェア人材の動向を把握して、我が国の産業界のニーズに対応した人材の育成がなされていることが不可欠であることを認識しておかねばならない。

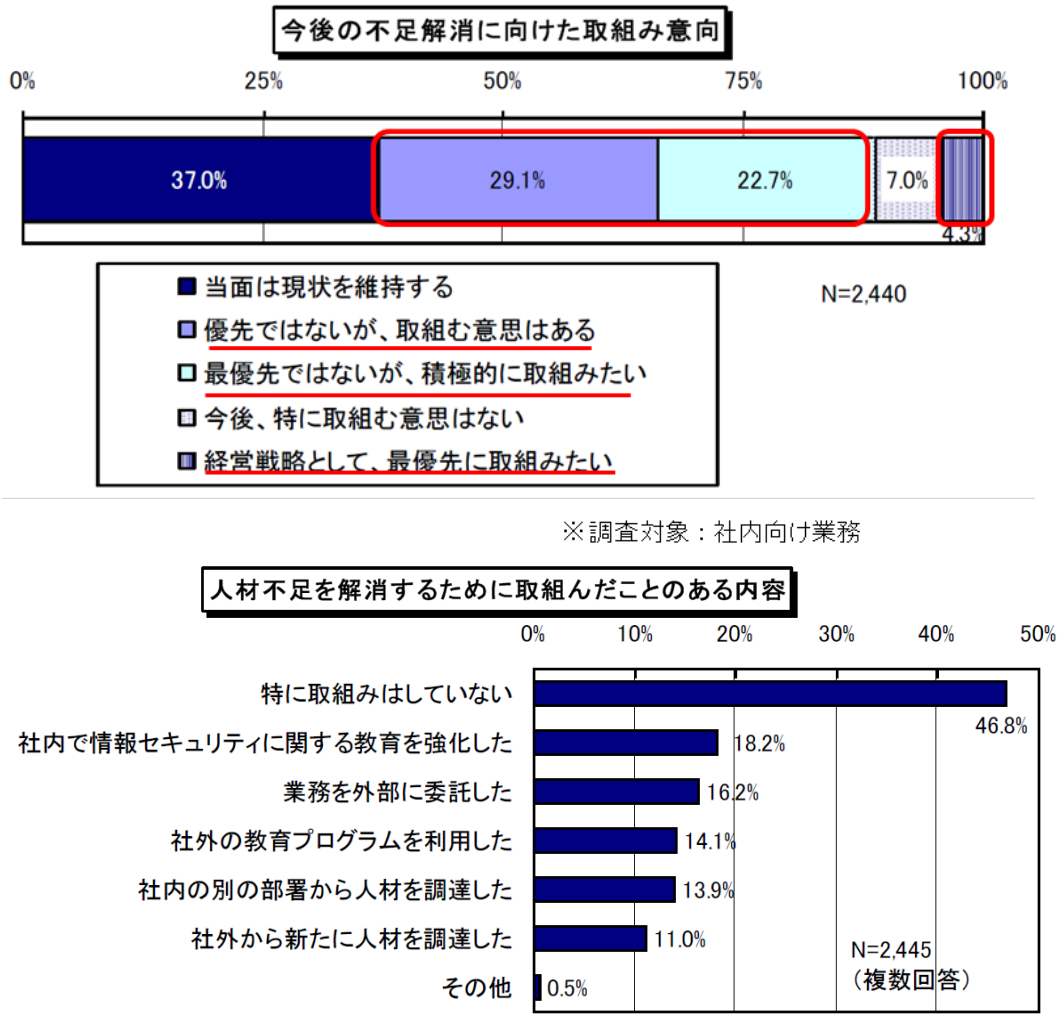

図２　企業等における人材不足解消に向けた取組状況

出典：独立行政法人情報処理推進機構「情報セキュリティ人材の育成に関する基礎調査」2012 年４月

【企業等の実務者層における課題】

我が国の情報システムの多くは、企業・組織等の業務と密接に結び付いたものとなっている。そしてこれらの情報システムの構築や運用は専門事業者（IT ベンダー）に委ねられ、情報セキュリティに関する対策も IT ベンダーに委ねられることも多いが、本来、業務の細部まで入り込んだ情報システムの構築と運用に際しては、ユーザー企業等においても、当該組織等の実務に精通した者の関与が不可欠である。

一方、独立行政法人情報処理推進機構（IPA）の試算によると、「サイバーセキュリティ戦略」において示されているように、国内で情報セキュリティに従事する技術者約 26.5 万人のうち、必要なスキルを満たしていると考えられる人材は 10.5 万人強にとどまり、残りの 16 万人あまりに対しては何らかの教育やトレーニングを行う必要があるとされている。さらに、約８万人が潜在的に不足しているとされており、その解消に向けた取組は、我が国の情報セキュリティ対策に係る水準を確保していく上で急務である。

【高度な専門性及び突出した能力を有する人材の必要性】

情報セキュリティの分野は急激に変化し続けており、日々発生する新たな事案、高度な事案への対処には、一般的な情報セキュリティ従事者の能力の底上げによる質的・量的不足の解消だけでは不十分であり、環境の変化に対応した新たな対策を創ることができる高度な専門性及び突出した能力を有する人材の確保が不可欠である。

これまでも、政府関係機関や大学の事業等において、情報セキュリティ分野を牽引する高度な専門性及び突出した能力を有する人材の発掘・育成に資する取組が進められてきたが、例えば情報セキュリティ（ツール）を数多くの海外の製品・サービスに頼っている現状（図３）等を見ると、我が国の安全保障、産業競争力強化の観点からも、わが国から新たな技術を創出し、それを支える人材を確保するための取組を今後より一層進める必要がある。

高度な専門性等を有する人材の存在は、情報通信に携わる技術者をリードし、また次の世代の情報セキュリティ人材の能力の向上、グローバルな攻撃からの防御、新産業の創出等にも資するものと考えられる。

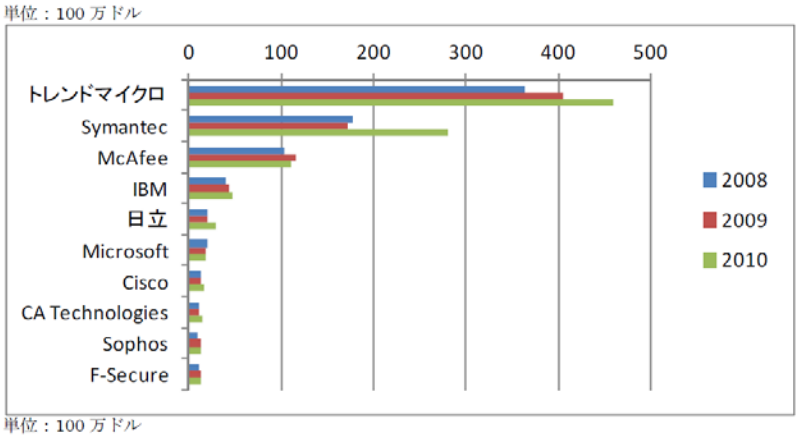

図３　情報セキュリティ（ツール）のベンダ別売上高【日本】
（経済産業省「平成 23 年度企業・個人の情報セキュリティ対策促進事業」調査報告書（2012 年３月））

また、若年層の関心を喚起し、将来の職業としての動機づけにつながるような情報セキュリティ人材が我が国から輩出され、国内外で活躍するようになれば、人材の裾野拡大にも資するものと考えられる。そのためにも、突出した才能が社会に見出され、政府や企業等に登用され研鑽を積んでいけるような環境整備が求められる。

【グローバル水準の人材の必要性】

現在、製造業などを中心に海外での生産、調達、販売等の企業活動のグローバル化が当たり前になりつつあり、新興国等の市場への参入も活発化している。また、流通や小売、金融等の内需型の産業も、国内市場の伸び悩みの中、アジア等の海外における事業展開が活発化している。そのため、企業活動と情報通信技術の一体化が進む中、企業においては、情報通信技術のグローバル化への対応とその対応を担う人材の育成・確保は必要不可欠である。

こうした中、サイバー空間には国境がなく、サイバー攻撃も国を越えて行われることから、サイバー攻撃から我が国、自組織を守るためには、攻撃者の能力を超えて対応できる高い能力がなければ対処できないこととなる。このため、各種人材の育成の課程において、グローバル水準のレベルで活躍できる人材の育成も視野に入れておくことが重要である。

（3）施策の対象分類と検討すべき課題

上記のようなリスクの深刻化と、一方で生じる大幅な人材不足に対処していくためには、人材の供給（育成・発掘）だけでなく、需要（雇用等）に対しても施策を講じて、「人材の好循環」を形成していかなければならない。

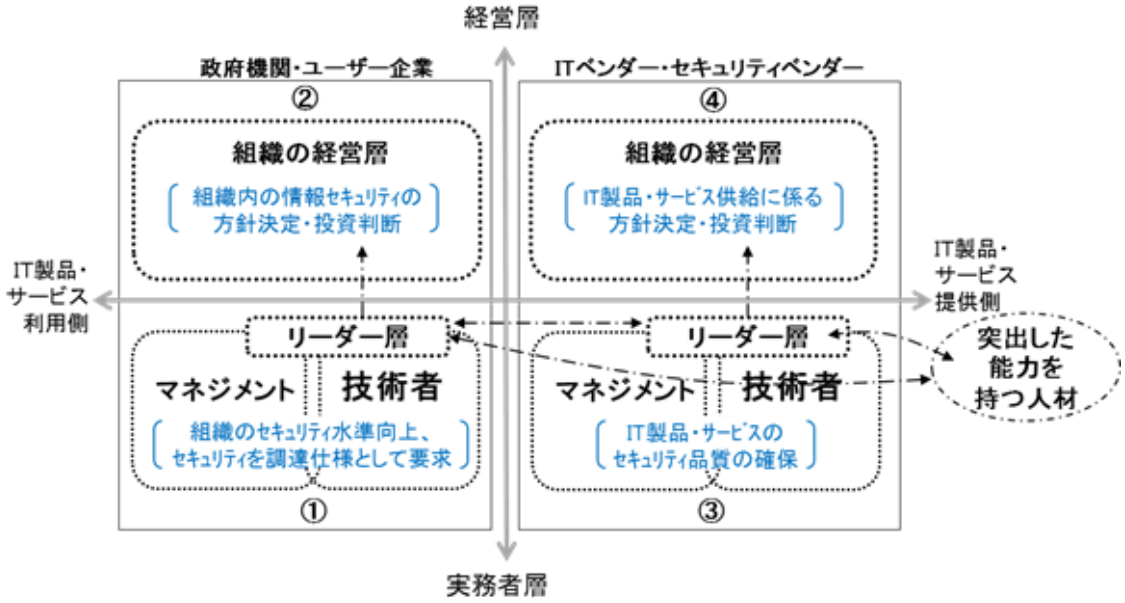

図４　施策の対象分類

例えば、人材の供給の観点では、政府機関・ユーザー企業等が、自組織の情報セキュリティを確保するため、IT 製品・サービスの「利用側の実務者層」（図４①）に、どのような対策が必要かを判断し実行する能力を身につけさせる必要がある。これに対し、「提供側の実務者層」（③）は、利用側の顕在的・潜在的要求に応えるレベルの能力を身につけることが当然必要となる。

一方、人材の需要の観点では、「利用側の経営層」（②）は、情報セキュリティを自組織の経営戦略として認識し、①を適切な処遇で登用することが必要である。同様に、「提供側の経営層」（④）は、必要なサービス・製品の開発・供給の戦略に基づき、③を適切な処遇で登用することが必要である。

加えて、我が国全体の情報セキュリティの水準を向上させるためには、牽引役として突出した能力を持つ人材が、実務者層のリーダーとして活躍したり、経営層と実務者との間のコミュニケーションを促進したり、提供側と利用側の橋渡しをするなど、各場面を行き来して活躍することが必要である。

なお、図１で示した通り、あらゆるものがインターネットに接続されている時代となってきていることから、ここで示す「利用側」とは、単に各組織におけるルーターやサーバ等のいわゆる情報システムの利用に限定するものではなく、各組織の業務の中で扱う IT 製品・サービス全体を捉えてその利用を指すものである。具体的には、金融・電力・水道・ガス・鉄

道等の社会インフラが、そのインフラサービスを提供するに当たって利用しているIT 製品・サービスや、生活家電・自動車・医療設備関連産業等において、埋め込まれる等されて利用しているIT 製品・サービスも含むものである。

このように、各分類の人材が相互に関連しており、人材の供給・需要の双方に課題が存在する中、我が国全体の情報セキュリティの水準を向上させていくためには、産学官による様々な施策を有機的に組み合わせて推進していくことが必要となる。

これらを踏まえ、第３章では、はじめに、人材の需要・供給双方に着目した取組の基本方針と、その具体的方策について述べる。そこでは、経営戦略の一部としての情報セキュリティ対策の啓発や調達における情報セキュリティ要件の設定による経営層の意識改革、層の厚い情報通信に携わる技術者（システムエンジニア、ネットワークエンジニア、プログラマー等）に対し必須能力として情報セキュリティを身につけさせるための取組について記述する。

次に、高度な専門性及び突出した能力を有する人材の発掘・育成に向け必要な取組について述べる。また、グローバル化するサイバー空間の脅威に対応していくため、国内外で研鑽を積みながらグローバル水準で活躍できる人材育成についても記述する。

とりわけ、政府機関においては、その情報及び情報システムを守り、国民生活の安全・安心を担保していくためにも、各府省庁等において情報セキュリティ対策の着実な推進が強く求められており、関連する人材の育成についても自ら率先して取り組むべきであることから、そのための具体的方策について述べる。

さらに、初等中等教育段階における情報通信に関する基礎学力充実、高等教育段階における実践的能力を高める演習の強化、情報セキュリティについて教えることができる人材の育成、情報セキュリティ人材のキャリアパスの提示といった教育機関における課題について記述する。

なお、広く一般国民を対象として情報リテラシーを高める普及啓発の具体的方策については、今後「情報セキュリティ普及・啓発プログラム」の見直しにおいてとりまとめることとする。

３．今後の取組方針

【基本方針】

我が国の情報セキュリティの水準を高めるため、人材の「需要」と「供給」の好循環を形成。

＜需要＞　経営層の意識改革

・情報セキュリティが経営戦略の基盤であることを自ら認識するための取組を推進することを通じ、経営層の意識改革を促し、情報セキュリティに対する投資意欲を喚起して人材の需要を創出する。

・経営層と実務者層との間をつなぐ実務者層のリーダー層が、経営戦略の視点から情報セキュリティに関する課題や方向性を考えコミュニケーションができるよう、経営と情報セキュリティの双方について理解し説明できる能力を育成する環境を整備する。

＜供給＞　人材の「量的拡大」と「質的向上」

・層の厚い既存の情報通信に携わる技術者に、情報セキュリティを必須能力として位置付ける。

・グローバル化する脅威に対応できる高度な人材や突出した能力を有する人材の育成・発掘を推進する。

（１） 経営層の意識改革

①経営戦略の一部としての情報セキュリティ対策の推進

組織等の事業戦略や方針について意思決定をする経営層が、自組織におけるシステムや知的財産、技術等の事業戦略上の意義・重要性をよく認識することは、これらを守る必要性について自律的に考える前提である。その結果、自組織の発展に不可欠なものとして情報セキュリティが意識されることとなり、経営層は情報セキュリティの水準を自組織の要求事項に適合するよう経営資源の投資に努めることとなる。そして深刻化する脅威に対して、情報セキュリティ対策が必要な部署に、必要な人材を適切に配置するニーズが生じてくる。

組織において情報セキュリティをどの水準に設定するかは、本来、各組織の経営・運営戦略上の問題である。すなわち、高度な情報セキュリティ水準を確保し、顧客からの信頼や自組織の情報の安全を高めることに必要な資源を投入するか、リスク受容等の異なる選択を行うかは、他のリスクとのバランスを考慮した上で経営層が決定することとなる。そうした意思決定が、情報セキュリティを取り巻く現状や、それが経営に与える影響を十分認識せずに行われることは適切ではない。経営層に正しく情報が提供され、組織全体としてのリスク管理の一環として適切な経営判断が行われるような環境整備が必要である。

具体的には、情報セキュリティ対策や人材育成の重要性等について企業等の経営層や経営幹部候補者、人事担当を含む経営管理部門を対象とした講習会等を引き続き開催するとともに、経済団体等が主催する会議等、経営層が集まるあらゆる機会をとらえて、経営戦略の一部として情報セキュリティに関する啓発活動を行い、経営層の意識改革を図っていく。

また、政府として積極的に情報セキュリティに関する経営層の意識改革を行う取組の１つとして、政府主催の経営者向けセミナー等の機会を通じて、各業界の経営層に対し、閣僚級や政府高官から直接訴えかける取組も行われているが、こうした取組を引き続き行う。

情報セキュリティに関する問題は、複数の事業領域にわたり、業務における利便性、効率性の阻害要因になることもしばしばあることから、企業経営が複雑化する中で、組織の全体最適化の視点からの情報セキュリティに関する部門横断的な戦略策定、意思決定、実務執行を行うためには、各組織が CISO[4]等を組織内で適切かつ確実に位置付け、責任の明確化が図られることが重要である。事業戦略の中に情報通信技術をどう位置付け活用するかなどを考えられる経営層の意識啓発や、情報セキュリティが事業戦略にどう影響するかなどもしっかりと考え説明できるスキルなどを身につけた CISO をはじめ経営層候補者等の育成に向け、情報通信技術あるいは情報セキュリティ領域と経営関連領域の連携が今後より一層重要になる。そのため、大学院などにおいて情報通信技術の関連のコースと経営学が密接に連携した教育課程を整えるなど必要な知識や経営のスキルを身につけるための環境整備を促していく。

[4] CISO（Chief Information Security Officer（最高情報セキュリティ責任者））：企業において自社の経営理念に合わせて情報セキュリティ戦略を立案、実行する責任者をさす。

また、我が国の企業数の大半を占める中小企業の経営層への情報セキュリティに関する理解の増進は重要である。

現在、具体的な取組として、経済産業省では、中小企業を指導する立場にある者等を対象としたセミナーを実施し、全国に指導者を設置しネットワーク化を図るとともに、中小企業団体等との連携により、当該団体等が主催する情報セキュリティ対策セミナーに協力する取組を実施し、中小企業における情報セキュリティの水準の向上を図っている。また、社内教育に活用できる啓発資料・ツール等を整備し、利用を促進している。さらに、IPA では、情報セキュリティ対策の推進が困難と感じている企業等に対する対策コストの負担の適正化及び対策の推進を目的として、「情報セキュリティ対策ガイドライン」の普及の促進や、攻撃を受けた被害企業へのハンズオン支援[5]等の取組について検討が進んでいる。

また、クラウドシステムを活用し、中小企業等に対し統一して情報セキュリティ対策を講じる仕組みも登場している。政府としてもその安全・安心な利用等について、ガイドラインの策定・普及を通じて実務担当者に対する支援を行っていく。

このような取組を通じ、組織の規模や業態等に応じ、経営層等にきめ細かく必要な情報を提供し、意識改革を促していく。

近年、中小企業等に対し、災害等の発生時における事業継続計画（BCP）とその前提となるリスク管理の体制を評価する動きが見られ、BCP 策定企業向けの融資制度を提供している金融機関も見られる[6]。こうした動きに対応して、情報セキュリティについても、可用性[7]の観点などを含めて事業継続に必要な要素のひとつとして認識されるような取組を積極的にすべきである。そのため、IT-BCP を含む BCP の策定と、その前提となるリスク分析の方法論を検討し、企業や組織への導入を図ると共に、それを担える人材育成の重要性に対する経営層の共通認識を醸成していくための取組を後押ししていく方策を官民で連携して行っていく。

これらの取組に加え、経営層が経営・運営戦略上のリスクをステークホルダーに対して説明する一環として、情報セキュリティに係る取組の説明も重要である。その結果、経営層が

---

[5] 現場に出て活動しながら行う支援活動や教育訓練のこと

[6] 中小企業 BCP ガイド（平成 20 年３月 中小企業庁）
（http://www.chusho.meti.go.jp/bcp/download/bcp_guide.pdf）

[7] 可用性：認可されたエンティティ（団体等）が要求したときに、アクセス及び使用が可能である特性

より一層、自社の情報セキュリティ対策に目を向けることも期待される。このため、例えば、上場企業におけるサイバー攻撃によるインシデントの可能性等について、米国の証券取引委員会（SEC[8]）における取組[9]等を参考にしつつ、事業等のリスクとして投資家に開示することの可能性を検討し、結論を得る。その際、関連情報の共有など開示するインセンティブを促すための仕組みの在り方についても併せて検討し、結論を得る。

また、開示する情報の正確性などを確保するために、情報セキュリティ監査・格付けの必要性の理解を一層広げる取組が求められる。さらに、形式的でなく実質的な内容の監査が行われるよう、適切な基準の整備・見直しを含め、監査方法の継続的な検討が重要である。加えて、監査等の妥当性の保証も重要であり、情報セキュリティ監査等を行う人材の育成、資格制度の適切な活用等も必要となる。こうした人材の育成は企業等の経営層の意識啓発のみならず、我が国の情報セキュリティ水準の向上にも資すると考えられることから、監査等を実施する者の常日頃からのスキルアップ（最新の情報の提供など）、行動規範の確立、監査制度の整備充実について引き続き取り組む。

具体的には、IT 技術知識を保有する技術者に、監査人資格取得のための研修等を通じて監査技術知識を習得させること、あるいは、特定サービスや特定保護目的（標的型攻撃対策等）のための標準監査技法や監査ツールを用いた実習を受けさせること等の監査実務教育を推進し、外部監査のみならず内部監査の質的向上に資する。

②実務者層のリーダー層に対する組織内部におけるコミュニケーション能力の強化

情報セキュリティに関わる実務者等のうちリーダー層については、経営層との間で情報セキュリティに対する共通理解を醸成するとともに、実務者層と経営層の双方が情報セキュリティの課題や方向性を共有し互いにコミュニケーションを図っていけるよう、組織内部で自らコーディネーターとなることが重要である。こうした人材には、組織の経営層の役割等を理解し、経営層との調整や各種組織判断への接続（縦の橋渡し）が出来る能力や経験が求められる。

こうした者が、経営戦略の視点も理解しつつ組織内の考え方を変革していけるような経営戦略と情報通信技術の利活用、情報セキュリティと事業リスクとの関係などを分析し、伝え

[8] Securities and Exchange Commission
[9] SEC “CF Disclosure Guidance: Topic No. 2, Cyber security”
（http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm）

ていくコミュニケーション能力などの向上を図る場などの環境整備も必要である。例えば、産業界において、経営企画とそのためのビジネスフロー、システム要件の検討といったテーマを与えてグループで一定期間の合宿等により集中的に討議し、成果を発表するといった集中セミナーの開催などの施策を推進する。

これらの結果、経営者等が、情報セキュリティ対策について、やむを得ず捻出するコストとしてではなく、自組織の製品・サービスの品質を高めるために必要なツールであり、経営戦略と一体の投資であるという認識が一層広く普及していくことを目指し、情報提供や情報開示等の環境整備を行っていく。

③調達における情報セキュリティ要件の設定

ある製品・サービスの利用側である顧客が、情報セキュリティ対策を講じるために調達の際に受注企業等に品質として情報セキュリティを要求することは、受注企業における情報セキュリティの水準の向上を意識させる強い動機付けとなる。

「サイバーセキュリティ戦略」においても、政府調達等における情報セキュリティ水準の一層の向上が記載されていることから、政府自らが、率先して、政府調達においてより高い情報セキュリティを要件化していく。

また、民間企業等におけるシステム等の調達においても、より一層高い情報セキュリティ要件が設定されれば、企業等の経営層の情報セキュリティに対する投資意欲が喚起され、波及効果として人材の登用・処遇向上が進むことが期待される。

現状、政府は、国の安全に関する重要な情報を扱う企業等における情報セキュリティ対策について、2012 年１月、内閣官房副長官から各府省庁大臣官房長等に対して発出された「調達における情報セキュリティ要件の記載について」に基づき、各府省庁が国の安全に関する重要な情報を国以外の者に扱わせることを内容とする契約を行う際には、調達仕様書等で情報セキュリティを確保するための体制の整備を求めることとしている。また、同通知では「実務担当者には、『情報処理の促進に関する法律』（1970 年法律第 90 号）に基づき行われる情報処理技術者試験のうち、情報セキュリティに関する資格を有する者又は同等の知識及び技能を有することを自ら証明できる者を含むこととし、当該者については、継続して新たな知識の補充を行うことに配慮する」こととされている。

こうした取組を一層強化するため、「政府機関の情報セキュリティ対策のための統一基準（2014 年３月改定予定）」においても、情報システムの開発・運用等を外部委託する際に、再委託先も含め、委託先企業の従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）などを確認することとしている。その際、最新の技術を習得しているかを確認することが重要であるため、例えば、情報セキュリティに係る情勢の変化に対応できているかを測る方法として、「直近３年程度以内の情報セキュリティスペシャリスト試験に合格している者」のように、資格要件に情報処理技術者試験の合格年度の記載を求めるといったことが考えられる。また、今後その運用にあたっては、単に資格、研修実施等の有無を確認するのではなく、例えば、納入物の品質管理の手続を情報セキュリティに係る検査・監査能力を有する者が行ったかどうかなど、それぞれの局面において妥当な能力を有する者が携わったかについての確認の可能性について更なる検討をしていくことが求められる。

なお、情報セキュリティ品質の向上のために、情報セキュリティに係る検査・監査や評価が行われる場合、それを担う者の能力の確保・向上は不可欠である。能力を担保できる資格の活用や、研修の実施等により、それを達成することが必要である。

このような政府調達での要件設定を通じた情報セキュリティ品質の向上の取組は、情報セキュリティの重要性についての認識を広げることとなる。同様に、一般の民間企業等同士の契約においても情報セキュリティの要件化が進めば、我が国全体の情報セキュリティの水準が高められ、情報セキュリティ人材の需要も増加するものと期待される。

（2）必須能力としての情報セキュリティ

情報セキュリティ従事者の量的・質的不足の解消に向けた取組は急務であり、情報セキュリティ人材について相当数の需要が喚起されるとともに、その需要に見合う素養を有する技術者の育成が強く求められる。一方、大学等の高等教育機関から輩出される情報セキュリティの専門知識の教育を受けた人材の数は、現状では年間 0.1 万人程度[10]と限られている。約 16 万人の質的不足、約 8 万人の量的不足を解消するには、大学等における専門教育の拡充のみならず、現在国内に約 80 万人[11]の規模を有すると推計される既存のシステムエンジニ

[10] 情報セキュリティ人材の育成に関する基礎調査（２０１２年４月　IPA）
[11] 「IT 人材白書 2013」(IPA)の IT スキル標準の職種別人材数推計結果（IT 提供側）に示された IT スキル標準職種別人材数のうち、IT アーキテクト、プロジェクトマネジメント、IT スペシャリスト、アプリケーションスペ

ア、ネットワークエンジニアやプログラマー等の情報通信に携わる技術者に対し、情報セキュリティのスキルを向上させていくための取組が必要である。

このため、企業等では情報セキュリティ人材の育成として以下のような方策に取り組むことが重要である。また、政府も、こうした取組を支援するため、サイバー攻撃の事例の情報共有やその情報をもとにしたケースの作成、教材・教育プログラムへの展開等に積極的に取り組んでいく。

①情報通信に携わる技術者が情報セキュリティを基礎能力として身につけるための取組

情報システムの設計・開発・運用の要であり、情報セキュリティについても実務者として担当することが期待される人材のボリュームゾーンでもある情報通信に携わる技術者に対し、企業内や教育機関等において実践的な教育が行われ、システムの設計段階から情報セキュリティ対策を織り込む「品質としての情報セキュリティ」の必要性をベンダー、ユーザーの双方が共有し、情報セキュリティのスキルが不可欠であるという共通認識を形成することが重要である。

また、今後の成長分野（例えば、「日本再興戦略」（2013 年６月閣議決定）によれば、ビッグデータ、農業、社会インフラ、健康・医療等）において必要となる情報通信技術を信頼性の高いものとするためには、情報セキュリティに配慮したものづくりやサービスづくりが不可欠である。我が国の競争力強化の観点からも、情報通信に携わる技術者が情報セキュリティのスキルを身につける必要があると考えられる。

このため、企業等が提供する製品やサービスの品質の一要素として情報セキュリティが位置付けられるよう、企業向けセミナーの開催等を通じて、企業等の技術者に対し、関係各省や業界団体等の各主体がより積極的な教育・啓発活動を推進する。

加えて、急速に進歩する技術への十分な対応を可能とするため、日頃の継続的な学習だけでなく、体系的な学習の機会が与えられることが求められる。例えば、一定の勤務経験の後、大学院等の教育機関で集中的なリカレント教育を受けられる等の仕組みが有効である。こう

シャリスト、ソフトウェアデベロップメントの総数の合計に、IT 利用側の IT 人材推計結果を加え算出したもの。

した教育を希望する者が受講しやすい環境整備について、産学官が連携して推進していく。

さらに、組織内で情報セキュリティについて教える能力を有する人材の育成も重要である。情報セキュリティを始め情報通信技術の基礎的内容を教えるためのカリキュラム・教材を準備し、必要とする機関に提供する取組もあることから、そうしたものも有効に活用しつつ、指導者の確保を図っていくことが重要である。また、既に多くの企業等で、e-ラーニング等により情報セキュリティの基礎を学習する取組が行われているが、それらの内容、質の向上も重要であり、より実践的な知識が得られるよう、後述するサイバー攻撃の事例共有、ケースを基にした教材等も活用しつつ、学習教材の見直し、改善を行っていくことが求められる。

特に、情報セキュリティ、ひいては情報通信技術全体において、あらゆるものの動作に関わるソフトウェアの設計・開発を担う人材の育成は急務である。例えば、システムを設計する際、近年では汎用のソフトウェアに頼ることが多くなり、技術者自らがソフトウェアを作成しその仕組みを理解していることは稀になりつつある。つまり、ソフトウェアのブラックボックス化が進行している。このため、不具合が生じた際にもオリジナルのソフトウェアベンダーに依存せざるを得ない状況が生じている。

一方で、日本の制御システムの中核ソフトウェアにおいては、現在も既成のＯＳではなく独自のＯＳで開発されたものが残っており、制御システムの細かな動きまで国内の技術者が構築したものによって制御されてきた。しかし、近年、こうした技術を支えてきた技術者が第一線から退く時期に差し掛かっていることから、制御システムの基盤技術を次世代に受け継いでいくことが重要である。

こうした状況を踏まえ、基盤としてのソフトウェア人材の充実のためにも、例えば第一線から退いた技術者が教育機関等において再び教える立場として活躍できるようにする取組を進めるなど、情報通信技術全体を支えるソフトウェアの設計・開発を担う人材を育成するための教育プログラムや、我が国がこれまで培ってきた基盤技術を次世代に受け継いでいくための環境整備について、産学官で連携して推進していく。

②情報セキュリティ能力の評価基準・資格等の整備

情報セキュリティ人材の能力を評価し、それを組織内での業務・処遇等に反映させていくため、情報セキュリティに関する資格試験やスキルを評価する基準、教育プログラムの整備

等を政府として進めていく必要がある。

情報セキュリティ人材に求められるスキルは対象となる人材の担当業務領域や役割によっても大きく異なることから、スキル標準の改善・活用等を通じ、必要とされる能力・知識を明確化していくことが重要である。

この点、現在 IPA は共通キャリア・スキルフレームワーク（CCSF）[12]の情報セキュリティ人材に関する能力・知識を最新化して公開しているが、民間企業等が育成の重要性を認識し、主体的にこの活用を促進するための取組を推進する。

その上で、企業側は社員に対し、それぞれの業務において求められるスキルセットについてスキル標準を参考に明示し、スキル習得状況について客観的に示せるよう後述する資格等を活用して「見える化」を図り、また、従業者の新規採用や昇進等において必要なスキルを身につけていることを提示できるように資格等の意味・活用方法などを示していくことが求められる。

また、教育機関で育てる人材のレベルと企業が必要とする人材のレベルを明確に双方が認識できる仕組みが重要であり、大学、高等専門学校等の教育機関においては、企業のニーズも取り込んだ形で、企業との連携による教育プログラム等を検討することが求められる。

IPA の情報処理技術者試験については、基礎的な知識を問う試験である「IT パスポート」から、情報セキュリティの高度な専門性を問う「情報セキュリティスペシャリスト」まで各種の試験が、数多くの企業や教育機関などで幅広く活用されており、社会に定着した試験となっている。各試験区分では、昨今の情報セキュリティの重要性の一層の高まりを踏まえ、2014 年度春期以降の試験から出題構成を見直し、情報セキュリティ分野に関する出題比率を増加させるなど、情報セキュリティに関する出題の強化・拡充が図られたところである。

情報通信技術を取り巻く環境が急激に変化している中で、情報処理技術者試験では引き続き最新の技術動向等を踏まえた出題が求められる。また、情報セキュリティに対する実践的能力を常に評価・担保できる試験、資格・認証制度として位置付けられるよう、例えば海外の民間資格のように合格後に継続教育を設けるとともに、情報セキュリティ人材の能力を認証する等、試験制度に関する在り方についての検討を進める。また、それに先駆け、政府や

[12] 高度 IT 人材を育成・評価するため、IT に関する各職種で共通の評価尺度として利用できるよう定義された枠組みのこと。IT スキル標準（ITSS）、組込みスキル標準（ETSS）、情報システムユーザースキル標準（UISS）の共通の参照モデルに位置付けられるとともに、情報処理技術者試験は CCSF に準拠して設計・実施されている。

企業においては情報処理技術者試験の合格年次で判断することや、同試験では合否のみでなく結果を点数でも表示されることから、繰り返し受験することを促すなどの取組が重要である。

また、情報セキュリティの分野は進歩が著しい分野であり、情報セキュリティ技術者として求められる能力・知識も進歩していくことから、資格等の整備においては常に最新の情報を身につけられるような教材や習得の場などの環境整備を行っていくことも重要である。

さらに、情報セキュリティの分野において優秀な人材を集めるためには、幅広く人材を集める必要があることから、一時的に仕事を辞めざるをえなかったり、一定期間の休職が必要となったりする有能な人材についても再び活用していく仕組みが望まれるが、能力の「見える化」が図られることは、再就職、転職などの際の指標として有効であると考えられる。加えて、資格の整備とともに職場環境の整備も必要であり、上述の資格制度の検討の課程で、情報セキュリティの資格を有している者へのインセンティブの在り方や、職場環境に関する意識の啓発も行っていくことを検討していく。

③情報セキュリティのスキル向上のための実践的取組の実施

ア．サイバー攻撃の事例共有、ケースを基にした教材等の開発

サイバー攻撃に対する防御を行うためには、実際にどのような手口でサイバー攻撃が行われ、それに対してどのような防御を行ったらいいかといった実践的な知識の蓄積が重要である。このため、過去に発生した情報セキュリティに関する事故事例等を教材として活用することには大きな効果がある。実際の事故等が発生した際に迅速かつ適切に対処できる情報セキュリティ人材を育成し、ひいては我が国の情報セキュリティの水準を高めていく観点からは、これらが高等教育の場、企業内の人材育成の場を含めて有効活用されることが望ましい。

そこで、行政機関等が入手した情報セキュリティに係る事案情報、不正プログラム情報や、行政機関自らが感知した事案情報、もしくは捜査機関内で集約・分析している事案情報等について、情報提供者の秘密保持や捜査上の秘密等に配慮し、関係者の同意等を得た上で、学習教材として活用される方法の検討を進める。また、そうした事例研究、情報共有を行うコミュニティ等の環境整備についても国及び関係機関から率先して推進する。

具体的には、個々のサイバー攻撃について、特徴的な事例を分析してケース（ビジネススクールで用いられるようなケーススタディに基づく教材のように、実際に起きた事故等を分析・研究し、討議等の題材として活用できる形にしたもの）を作成し、そのケースを題材として、技術者等が対処法（防御手法、攻撃手法も含む）について自ら考え、対策を検討できるような実践的な学習教材・教育プログラムを政府関連機関、教育機関等で連携して作成していく。その際、多くの者が取り組みやすいシミュレーション形式のコンテンツの開発等も行っていき、クラウド技術なども活用しつつ、幅広い立場の技術者や教育関係者が利用できるようにすることが重要である。その際、特に、攻撃手法等を学んだ技術者等がそれを悪用しないよう倫理教育も併せて行うことが重要である。

イ．教材等を利用した情報セキュリティ教育、訓練等の実施

情報セキュリティについて学習する技術者に対し、そのための教育、訓練の場を提供することは重要である。その際の学習教材として、上記の種々のサイバー攻撃の事案の教育現場での活用につなげていくことが有用と考えられる。そのため、上記教材に対応したカリキュラムやマニュアル等を整備し、教材が教育機関、企業等で活用されるよう連携を図るとともに、実際の教育を通して見つかった改善点等を教材の見直しに随時反映させていくことが必要である。

また、実際のサイバー攻撃を想定した実践的演習について、総務省では、標的型攻撃へのインシデントレスポンス等について、「実践的サイバー防御演習（CYDER[13]）」を官公庁、企業等のLAN管理者等を対象に2013年度から実施している。今後さらに実際の攻撃手法などをよく把握の上、実際の運用環境に近い環境での実践的な演習を引き続き推進することが求められる。

経済産業省では、技術研究組合制御システムセキュリティセンターにおいて、制御セキュリティテストベッドを活用した制御システム技術者やユーザー企業に対する訓練や演習を行っている。こうした施設を有効に活用し、実践的な教育・演習を通じた人材の育成が引き続き必要である。

[13] CYber Defense Exercise with Recurrence

我が国は、情報セキュリティの専門家が所属する組織を変えながらキャリアパスを形成していく欧米とは異なり、情報セキュリティの専門家でなかった者が、組織内の人事異動等により情報セキュリティの担当となることもあることから、そうした担当者が短期間で情報セキュリティを学べる教材・プログラムが必要とされている。そうした中で、アクティブラーニングやPBL[14]（問題解決型授業）などの体験型の学習方法は有用であるとの指摘がある。こうした手法は、ジェネラリストと専門家との間のスムーズな人事交流にも資するものと考えられることから、その普及を促していくことが必要である。

（3）高度な専門性及び突出した能力を有する人材の発掘・育成

日々変化する新たな事案や高度な事案に対応し、情報セキュリティ分野を牽引するような高度な専門性を持った人材や、突出した能力を有する人材が不可欠である。一方で、そのような人材を発掘・育成するためには、画一的な教材・教育プログラムだけではなく、テストベッドを用いた先端的な研究開発を通じた人材育成や、能力の開花に結び付く場を設ける等の成長支援も必要である。

①高度な専門性を持った情報セキュリティ人材育成のための高等教育の強化

情報セキュリティの専門人材には、高度で幅広い知識や特殊な能力が求められる。大学等における高等教育ではそのための基礎となる教育が実施される必要があるが、現状、全ての分野で十分な教育ができる教員を単独で揃えることのできる教育機関は極めて限られている。このような状況下にあっては、まずは複数の大学が連携して体制を整えることが有効である。また、情報セキュリティ分野は実践が重要であることから、産学連携もあわせ進めることが望ましい。

文部科学省の「情報技術人材育成のための実践教育ネットワーク形成事業（enPiT[15]）」においては、大学や産業界が全国的なネットワークを形成し、実際の課題に基づく課題解決型学習等の実践的な教育により、実践的な情報セキュリティ能力を有する人材の育成を進めている。こうした、高度な人材育成のための複数の大学間、大学と産業界との連携のための施策を引き続き推進する。

---

[14] Problem Based Learning
[15] Education Network for Practical Information Technologies

また、情報セキュリティに関する研究科等を大学・大学院に設置する取組は、企業等へ専門的な能力を有した即戦的な人材を供給する取組として有効と考えられる。今後、人材の需要と供給の好循環を形成していくためには、こうした高等教育機関に対し、国や産業界等の需要者が求める人材像を示していくことが重要であり、高度な専門性を持った人材の採用等について政府としても率先して取り組んでいくことが求められる。

高等専門学校等においては、基礎と実践的な技術力を融合させた教育を行っており、情報工学科等では、ハードウェアとソフトウェアの基礎的な力をしっかりと身につけた上で、実践的な情報システムの開発能力を備える技術者の育成を目標としたモデルコアカリキュラムの導入を進めており、その中でも情報セキュリティは学習項目として取り上げられているところである。今後、カリキュラムの導入促進を通じて、各学校において、最低限の能力基準の確保に向けた検討が引き続き行われることが期待される。

また、経営戦略の一部としての情報セキュリティ対策の推進（（１）①）において示した実務者層のうちリーダー層については、経営層と実務者層の間をつなぐ役割を果たすことが考えられるが、これらの者の育成に関し、米国や韓国等においては、情報セキュリティを専門としつつ、様々な専門分野の知見や組織経営等に必要な知識を併せ持ち、俯瞰的な視点でサイバー空間を取り巻くリスクに対応していける人材が高等教育機関から輩出されている。さらに、そうした人材が政府機関、民間企業等を行き来しながら研鑽を積み、情報セキュリティの分野を牽引している例もある。そのような総合的な能力と豊富な経験を有し、世界に打って出られるような人材の育成や、官民を横断して人材が循環する仕組みの構築についても、今後我が国が情報セキュリティの分野で国際的プレゼンスを高めていくためにチャレンジすべき課題であり、具体的な検討を進める。

②最先端の分野で活躍する突出した人材の発掘及び更なる能力向上

情報セキュリティ分野に限らず、最先端の分野で活躍する突出した能力を持つ人材は、通常の教育では育成が難しい。このような人材に対しての取組は、その能力に注目した発掘や、国内外の優秀な技術者等と切磋琢磨して能力の開花に結び付く場を設けることが重要である。

現在、IPA において、将来の IT 産業の担い手になり得る優れた若い人材の発掘と育成のた

め、初等中等教育段階を含めた 22 歳以下の学生・生徒に対して、IT 業界の第一線で活躍中のトップエンジニアを講師として招聘し、情報セキュリティなどに関する高度な教育プログラムである「セキュリティ・キャンプ」事業を 2004 年から開催しているところである。

また、情報通信技術を駆使してイノベーションを創出することのできる独創的なアイデアと技術を有するとともに、これらを活用する優れた能力を持つ、突出した若い逸材（スーパークリエータ）を発掘育成することを目的とした「未踏事業」を 2000 年度より行っている。事業の実施にあたっては、独創性を積極的に評価するために、ソフトウェア関連分野における優れた能力と実績を持つ人材をプロジェクトマネージャー（PM）として任用し、独自の眼力による提案内容の審査、開発テーマの選定、クリエータへの指導・助言、開発の進捗管理、開発結果の評価等を行っている。

さらに、一組織では対応が困難で、社会的な被害拡大が懸念される深刻なサイバー攻撃を受けた組織に対し、通常活動への復帰・再発防止に向けた対応支援を行う「サイバーレスキュー隊（仮称）」を、IPA が 2014 年度より開始する予定である。そこでは、サイバー攻撃被害の封じ込めという短期的課題に対応するとともに、同隊において若手を含む突出した技術を持つ人材を採用し、トレーナーの指導の下、OJT でマネジメント能力を養うことで、リーダー層を担う人材を輩出していくことも目指している。

加えて、特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）では、日本の情報セキュリティ技術者の育成を目的とし、チームに分かれて攻撃と防御の２つの立場で能力を競い合う競技イベントである「SECCON」を開催している。

このような事業やコンテストなどの仕組みを通じ、情報セキュリティを守ることの重要性や倫理を指導しつつ、必要な能力の開発や人材の発掘を引き続き産学官が連携して推進していく。また、発掘された人材等が実社会でその能力を活かせるようにしていくことが重要であり、こうした事業やコンテスト等を通じて育成すべき人材像の明確化に向け、関係省庁や企業が連携する方策も、今後検討していくべき課題である。

なお、多くの若年層が情報セキュリティの分野に関心や憧れを抱くことは、こうした優秀な人材の発掘のみならず、人材の裾野を広げ、我が国の情報セキュリティ水準自体を底上げすることにもつながる。さらに、そのようにして社会的な認知が高まることは、企業等で情報セキュリティ人材が活躍する場面が増えることにもつながる。このため、社会、とくに若年層に訴求できるよう、情報セキュリティの分野で活躍するトップ人材などをテーマにした

コンテンツを、普及しやすいメディア等を活用しつつ啓発していくことにつき検討を進める。

（4）グローバル水準の人材の育成

企業の活動を始めとするあらゆる分野において、グローバル化が進むとともに、サイバー攻撃も国を越えて行われる。こうしたサイバー攻撃から我が国を守るためには、攻撃者の能力を超える、つまりグローバル水準の能力がなければ対処できないこととなる。

ここで、グローバル水準の人材とは、単に語学力が優れていることのみを意味せず、グローバルなサイバー攻撃に十分に対応しうる能力[16]や国際会議等における内容面での交渉能力などを有し、専門分野において世界に通用する最先端の知識・能力を備えた人材を指している。これらの能力は、海外で活躍する人材のみならず、国内において活躍する人材にも求められるものである。

こうしたグローバル水準の人材の育成については、まずは大学等教育機関において最新の国際動向等を踏まえた積極的な人材育成が実施されるよう、国内外の大学、企業等と連携してカリキュラム改善に努めていくことが望ましい。また、例えば、情報セキュリティに関する実務経験を有する国内外の人材を交えた講義・演習等も、グローバル水準の人材育成に資すると考えられる。続いて、そのような教育を受けた人材が互いに切磋琢磨して能力を高めていくとともに、次世代の人材を育てる立場となっていくような人材育成の好循環が実現することが望まれる。さらに、そうした人材が企業及び政府機関等において積極的に雇用されることで、わが国の情報セキュリティ水準の向上につながることが期待される。

グローバル水準の人材を育成するためのカリキュラム改善の一例として、2013 年には、経済産業省の「産学連携評価モデル・拠点モデル実証事業」の下で、グローバルな現場で活躍できる情報セキュリティ人材の育成を目標とした、大学・大学院における教育・研究プロジェクトが発足している。

また、グローバル水準の人材を育成するためには、できるだけ多くの国際的な体験や情報共有が必要である。各国機関との連携、国際会議への参加や留学の支援、我が国での国際会議の開催、現在国内で開催されている競技イベントを国際レベルで行うこと等を通じ、海外の優秀な技術者等と切磋琢磨しながら研鑽を積む場を増やしていくことが有効と考えられる。このため、政府としてもトップレベルの人材を集めた国際会議、競技イベント等に対し積極

[16] 例えば、新たな攻撃方法の課題を設定しそれに対処できる能力。

的に応援していく。

例えば、米国国立標準技術研究所（NIST[17]）や韓国インターネット振興院（KISA[18]）との情報交換や、インシデント対応に係る官民組織の国際的な集まりであるFIRST[19]への参加等に引き続き取り組む。加えて、海外各国の攻撃対応窓口機関（CSIRT[20]）との間で脅威情報を共有し、共同対処を行う枠組みの構築に向けた検討も進めていく。このような場を積極的に活用し、最新の防御・攻撃に係る技術トレンドの共有、国籍を超えた情報交換・交流の場の提供、共同研究・事業連携の促進及びリクルートの機会提供、国際的コミュニティの形成などの面で、情報セキュリティ人材が互いに切磋琢磨する環境を構築する。

また、米国では競技イベントである「DEFCON CTF[21]」に世界各地から情報セキュリティの専門家が集い、競技を通じてお互いの能力向上を図っているのを参考に、グローバルにトップレベルの専門家が参加し、グローバルに見てトップ水準の者と議論でき、比較することのできる国際的な会議等の開催を支援していくなどを通じて、研鑽を積む場を増やしていくことが有効と考えられることから、各種競技イベントなどにおいて海外からの参加者の招聘や参加資格を開放するなどの取組を促していく。

（５）政府機関等における人材育成

我が国の情報セキュリティの水準を向上させるため、とりわけ、政府機関等は自ら率先して人材育成に積極的に取り組んでいくことが重要である。このため、情報及び情報システムに係るセキュリティ水準の一層の向上を図るとともに、システム担当者の能力の底上げや幹部の情報セキュリティに対する理解の増進を、引き続き着実に推進する。

今後のサイバー攻撃等への対処体制の充実・強化に向け、必要な情報セキュリティ人材を政府自ら確保していくための人材の育成・登用等に係る具体的取組について記載する。

①サイバー空間を取り巻くリスクに対応できる職員の採用・育成

昨今のサイバー空間を取り巻くリスクの一層の高まりを踏まえ、日常的にシステム運用等

[17] National Institute of Standards and Technology
[18] Korea Internet & Security Agency
[19] Forum of Incident Response and Security Teams
[20] Computer Security Incident Response Team
[21] Capture The Frag

に携わる情報セキュリティ担当者についても、一定の専門的知見を持った職員が配置される必要が生じている。

このため、CISO アドバイザーのみならず各職員においても、CISO を実質的に補佐できる体制を充実させるととともに、情報セキュリティ担当者については、採用及び人事ローテーションにおける特別の配慮や、情報セキュリティ専門事業者等との積極的な官民交流等について、2012 年6月、内閣官房副長官から各府省庁大臣官房長等に対して発出された「各府省庁情報セキュリティ担当者に係る人材育成等について」に基づき、引き続き積極的に取り組んでいく。

また、情報セキュリティ担当者に対しては、自組織内のシステムでトラブルが発生したことにつき負の評価がされるというのでなく、システムを適切に管理し、トラブルを未然に防止し何も起こらなかったことについて、それを成果として高い人事評価に繋げるといった、政府内での情報セキュリティに対する意識改革も必要である。

さらに、情報セキュリティに関する知見を深め、情報セキュリティ関係の資格の取得を促進するためにも、情報セキュリティ関係の資格を有している職員に対するインセンティブについても検討していく。

特定の府省庁で継続的に業務にあたるのではなく、他府省庁や内閣官房等において同種の事務に携わることで、経験を広げるとともに、各府省庁の情報セキュリティ担当者間で協力してサイバー攻撃に対応していくことも重要となる。このため、2012 年6月に国の機関等において大規模なサイバー攻撃等により政府として一体となって迅速・的確に対応すべき事態等が発生した際に、機関の壁を越えて連携し、被害拡大防止等について機動的な支援を行う「情報セキュリティ緊急支援チーム（CYMAT[22]）」が発足した。CYMAT においては、政府一体となった対応が必要となる情報セキュリティに係る事象に対応できる人材を養成・維持するため、定期的な研修、訓練の実施等を行っている。このような政府一体となった情報セキュリティ確保体制がより強固なものとなるよう、今後さらに連携を強めていくこととする。

内閣官房情報セキュリティセンター（NISC）では、現在、組織内での研修、CYMAT を

[22] CYber incident Mobile Assistance Team

通じた職員の能力向上を行っているが、今後とも、サイバー攻撃に関するインシデントの情報等の集約、国内外の情勢の分析、技術動向の分析が可能な内部人材の育成・採用を進めていく。また、現在行われているリスク評価の取組についても、その結果を人材育成に反映していくこととする。

加えて、2015 年度を目途として、「サイバーセキュリティ戦略」で示されているように、NISC については、その機能強化の取組として、専門職員の採用や育成等の人事管理による人材の確保など、組織体制を整備することとしているが、NISC 自身も高度な情報セキュリティ人材のキャリアパスのひとつになるよう更なる取組を推進するなど、政府機関全体として内部人材の活用のみならず、官民の人事交流等により、外部の優秀な人材の有効活用を引き続き行っていく。こうした専門人材の育成・登用は、求められる人材像を社会に示し、情報セキュリティ人材に関する需要の呼び水にもなりうることから、政府として率先して進めることとする。

将来的には、米国や韓国のように情報セキュリティの専門家が、政府、民間企業、研究機関、教育機関の各機関で経験を積みつつ、総合的な情報セキュリティ人材としてのスキルを上達させていくようなキャリアパスが形成されることが望まれる。

なお、各府省庁では、情報セキュリティに係る事案が発生した際、迅速かつ適切に対処するための体制として、CSIRT の整備を２０１２年度末までに終えているが、標的型メール攻撃等を受けた際にその被害を最小限にとどめ、迅速かつ適切に対応できるよう、大規模サイバー攻撃事態などの発生を想定した各省庁の CSIRT 関係者による対処訓練を実施する。

また、法務省においては、検察官及び検察事務官が、複雑・巧妙化するサイバー犯罪に適切に対処するため、捜査上必要とされる知識と技能を習得できる研修を全国規模で実施し、捜査能力の充実を図る取組が行われているほか、警察庁においては、人材育成等による取締り等の体制を強化するとともに、サイバー防犯ボランティアの結成及び育成や活動の支援を強化している。安全で安心なサイバー空間の醸成に向けては、こうしたサイバー犯罪対策のための人材育成の強化も必要不可欠であることから、今後も着実に推進する。

②政府職員全体の情報セキュリティ意識の啓発と研修・訓練の実施

情報セキュリティの向上に際しては、情報システムやそれを扱う担当者の能力向上を図るだけでは不十分であり、職員全員の意識や能力の底上げが必要である。そのため、政府機関において、常に研修・訓練を実施してスキル向上に努めることが必要である。

現在、内閣官房では、政府職員を対象とした教育用教材の作成・配布や各種研修カリキュラムにおいて情報セキュリティに関するプログラムを盛り込む他、情報セキュリティに係る認識の共有と更なる知識・技能の向上を図っている。また、各府省庁等は、内閣官房による上記支援等も活用しながら情報セキュリティ人材の育成を行っている。今後も、このような実践的な訓練等を、環境の変化に合わせて都度見直しを行いつつ、継続していく。

また、政府職員全体の情報セキュリティ意識の啓発と能力の底上げのための施策として、前掲の「各府省庁情報セキュリティ担当者に係る人材育成等について」（平成２４年６月）の中で、国家公務員採用時の面接においても、情報セキュリティに関する素養の確認等を行うよう要請がなされている。これを踏まえ、政府においても採用面接時に IT パスポートや情報セキュリティに関する資格の有無を確認するなど、政府の情報セキュリティ人材育成のために様々な取組が実施されており、これらを引き続き着実に行っていく。

③重要インフラ事業者等における人材育成

重要インフラは、その機能が停止、低下又は利用不可能な状態に陥った場合に、我が国の国民生活・社会経済活動に多大な影響を及ぼすおそれがあるため、重要インフラ事業者等において必要となる情報セキュリティの確保が図られるよう、組織内でより積極的に人材育成が図られることが望ましい。

具体的に、重要インフラ事業者等においては、「重要インフラの情報セキュリティ対策に係る第３次行動計画」（２０１４年３月改定予定）に基づき、システムの構築・運用及びリスク源の評価とそれに基づく方針の策定・実行に必要な人材を、一種の経営資源として継続的に確保していくことが求められる。また、内閣官房においては、重要インフラ所管省庁と協力し、「分野横断的演習」を改善しつつ引き続き実施するほか、重要インフラの情報セキュリティに関する広報公聴活動や国際連携及び規程類の整備を通じて、重要インフラ事業者の意識啓発や能力向上等の人材育成に関して必要な支援を行う。

（６） 教育機関における情報通信技術教育の充実等

①初等中等教育段階における情報通信技術に関する教育の充実

初等中等教育段階では、2003 年度から高等学校で情報科が必履修教科として設置され、2008 年の学習指導要領改訂において、情報セキュリティに関する内容を充実したところである。情報科では、情報及び情報手段を活用するための知識、技能や科学的な考え方を習得し、社会の中で情報及び情報技術が果たしている役割や影響を理解させることで、社会の情報化の進展に主体的に対応できる能力と態度を育てることが目標とされている。この趣旨を踏まえた上で、高等学校における情報セキュリティに関する教育を着実に推進する。

また、2008 年に改訂した小学校及び中学校の学習指導要領においては、発達段階に応じ各教科等の指導を通じて、情報セキュリティも含む情報モラルの育成のための学習活動を充実したところであり、引き続き、情報モラルに関する教育を着実に推進することが重要である。

さらに、情報セキュリティの基本となる情報通信技術の学習では、コンピュータの原理、コンピュータプログラムなどの基礎などについて学ぶことや関心を喚起することも重要である。2008 年の学習指導要領改訂では、中学校「技術・家庭」技術分野において、プログラミングを含めた情報通信技術に関する学習内容の充実を図ったところであり、引き続き、初等中等教育段階からのプログラミング等に関する教育等を積極的に推進する。

こうした情報通信技術に関する教育を引き続き推進し、より一層、情報処理に必要な論理的な思考力や情報通信技術の原理についての理解を促すようなものとなることが求められる。

②高等教育段階における実践的能力を高める演習の強化

大学、高等専門学校等において、情報系技術者として必要な情報通信技術の実践力をより一層高めていくことが望まれる。特に情報セキュリティは、情報通信技術を含むコンピュータサイエンスを駆使する具体的な応用分野であることから、将来の優れた情報系技術者を育てるのに最も適した課題の１つであることに注目すべきである。この方針については、「創造的 IT 人材育成方針」において「高等教育機関の情報系教育における実践力の強化と、実践力の基盤となる理論・基礎の習得が望まれる。」と記載されたところである。実践力を高めるための具体的施策として、各高等教育機関において、講義型授業に加え演習を拡充していくことや、産学連携による産業界の動向を踏まえたより実践的な教育が望まれる。

また、情報を専門分野とする大学や学部においては、大学入学者が入学後の専門的な教育

に円滑に接続できるよう、それぞれのアドミッション・ポリシー（入学者受入方針）の下、入学者選抜において入学志願者の高等学校段階において育成された情報処理に必要な論理的な思考力や情報通信技術の原理についての理解の達成度を適切に評価することが望ましい。

加えて、企業においては、情報系教育を受けた学生の基礎知識、実践力の強化を促すべく、採用時の基本的な知識・能力の確認等を促す。例えば、それぞれの職業に求められるスキル標準を示すことや、資格制度の活用などが考えられる。

③情報セキュリティに関する教員の養成

初等中等教育機関において、情報セキュリティに関する学習活動が一層充実するためには、指導にあたる教員の能力が十分であることが必要である。そのためには、各都道府県及び政令指定都市等の主として情報教育担当の指導主事等を通じて、教員一人ひとりが情報セキュリティに関しても引き続き指導力の向上に努める必要がある。「創造的 IT 人材育成方針」においては、全ての教員に「教員の情報活用指導力」を高めるための積極的な取組が必要とされたところであり、情報セキュリティについてもその一環としてさらなる指導力の向上が望まれる。また、児童・生徒を取り巻くインターネット等の環境の変化は急速であることから、産業界等の民間の協力を得て最新の動向に対応することも必要である。

高等教育機関においても、各大学等の自主的な判断により情報セキュリティに関する教育が実施されているが、例えば大学の共通教育・教養教育の教育カリキュラム作成者の情報セキュリティに対する認識が十分でないと考えられることに加え、専門性のある教員が多くないこと等が指摘されている。このため、教育機関で育成する人材のレベルの明確化と併せて、そうした人材を育成する教員にとって必要となるスキル育成の場や教員向けの教材等についても、例えば博士号の有無等の学歴等にとらわれることなく、民間の能力の活用や、一線を退いた技術者等が活躍できる環境整備も含め、産学官が相互に連携しながら検討を進めていく必要がある。

④情報セキュリティ人材のキャリアパス提示

学生等が情報セキュリティの分野に興味を持ち、情報セキュリティを将来の職業として考えた場合に、専門家としてどのようなキャリアパスが存在するのかが明らかでなく、専門家としての将来の発展性、安定性等といったことの見当がつかないことが、情報セキュリティ人材の不足の一つの要因として指摘されている。

このため、IPA では、活躍中の情報セキュリティ人材へのインタビュー調査を基にキャリアパスモデルを策定して公表し、情報セキュリティの専門家を目指す者への参考資料を提供するなどの取組を行っている。

また、JNSA においては、将来情報セキュリティ技術を活かして活躍したいと考えている学生に対して、情報セキュリティ業界の魅力を感じられるような就労体験の機会を提供することを目的とし、企業におけるインターンシップを支援する事業を実施している。

今後あらゆる成長分野において必要とされる情報通信技術に付随して情報セキュリティも必要とされることを考えると、情報通信に携わるための基盤的知識として、いわば横串としての情報セキュリティ技術の知見を有した技術者の育成が必要である。このことから、情報セキュリティの専門家だけでなく、情報通信に携わる技術者全体において、情報セキュリティの知識を習得することを前提とした人材の育成、キャリアパスの提示が必要である。

具体的には、図４（９ページ）に示した各層の人材像等は以下のとおりである。

ＩＴ製品・サービス提供側における実務者層のリーダー層の場合、ＩＴ製品・サービス及びサービスを実現するシステムの企画・設計・開発・運用などの各段階において、利用側のニーズや利用者が置かれている状況、コストなどを把握・理解し比較衡量できる能力が期待されるとともに、実務者層を取りまとめたり経営層に適切に提案できることが求められる。また、実務者層は情報セキュリティを基礎能力として身に着け、具体的にこれらを実現していけるスキルを有することが期待される。

他方、ＩＴ製品・サービス利用側における実務者層のリーダー層の場合、組織内外の関係部門の業務や情報の流れなどを把握し、業務の高度化等の一環としてシステム化や運用をするときに、実務者層をとりまとめて、業務遂行上のリスクのひとつとして情報セキュリティに関する要求事項などをＩＴ製品・サービス提供側に対して示したり、経営層に事業戦略等の観点から説明できるといった能力が期待される。また、実務者層は情報セキュリティについて理解でき日々の運用やシステムの利用などができることが期待される。

経営層にあっては、事業戦略の検討・執行にあたって、情報通信技術をどのように利活用し、その際の事業上のリスクの一環として、インシデントの発生防止及び発生した際の対応において、情報セキュリティがどのように位置づけられるのか、どのような事業戦略等をも

っていけばよいのかといったことを考えられる基礎的な能力を持つことなどが考えられる。

そして、情報通信に携わる技術者が情報セキュリティを必須能力として定着させていくこと、さらに、経営学をはじめ法律学や心理学などの多様な知見を身につけて行くことにより、情報通信に携わる技術者であって情報セキュリティ技術者でもある者が組織内で経営層となっていくキャリアパスや、情報セキュリティ技術を究めて高度な専門家として活躍することが期待される。その際、経営と情報通信技術や情報セキュリティに関する戦略的思考力や、経営層との間のコミュニケーション能力を有する者に着目していくことが重要である。

４．まとめ

本プログラムでは、2013 年６月に策定した「サイバーセキュリティ戦略」を踏まえ、情報セキュリティ人材の量的・質的不足の解消等の各種課題の解決に向けて、これまで各省の情報セキュリティ人材育成施策の中心となっていた突出した人材の発掘・育成などに加え、経営層の意識改革、経営戦略の一部としての情報セキュリティ対策の推進、調達における情報セキュリティ要件の設定、情報通信に携わる技術者の必須能力としての情報セキュリティ、技術者に情報セキュリティを意識させるための取組、情報セキュリティ能力の評価基準・資格等の整備及びサイバー攻撃の事例・ケースを基にした教材等を用いた情報セキュリティのスキル向上のための実践的取組の実施等についての今後の方針、施策を示した。

また、高度な専門性及び突出した能力を有する人材の発掘・育成を引き続き進めるとともに、グローバル水準の人材の育成、政府機関等における人材育成、教育機関における情報通信技術教育の充実についても検討を行い、今後の方針、施策を示している。

一方で、例えば、情報セキュリティ人材の質的・量的不足は明らかとされているものの、具体的にどのような分野、能力の人材が不足とされているかの実態はあいまいな点も多いことから、今後、ここで掲げた施策の実施結果を調査把握することが必要であり、施策の進捗状況を示す指標（例えばソフトウェア人材、ソフトウェア産業動態の統計の充実など）の整備等を行い、その結果を踏まえた施策の不断の見直しを行っていくことが重要である。

また、人材の能力に係る評価基準・資格等にあっては、社会で実際に求められる人材像につながるものであるべきであり、今後、それに向けて産学官が密接に連携して検討を進めていくことが重要である。

また、２０２０年に東京でオリンピック・パラリンピックが開催されることとなり、国際的にも、我が国の情報通信技術の利活用能力やサイバー攻撃に対する防御能力を高めることが求められており、それを支える情報セキュリティ人材の育成は今後ますます必要となってくると考えられる。

なお、人材育成は短い期間で完結するものではなく、長期的に取り組まなければならない課題である。特に、情報セキュリティに関する人材育成を行うために必要な環境づくりとしては、情報通信全般の幅広い知識、教育をはじめ他分野における各種制度、今後の我が国の

産業における情報通信技術の活用、最終的には日本の社会全般の制度・意識等様々な事項と関連して横断的取組が必要なものである。

このため、政府としては産学官の関係機関、関係者が共通の認識、意識をもって、情報セキュリティという観点のみならず、環境の変化に留意しつつ、他の関連施策とも連携して、総合的に積極的な施策を推進していくこととする。

具体的には、情報セキュリティ政策会議が策定する年度計画において、本プログラムに基づき推進する各施策と担当省庁の明確化を行い、情報セキュリティ人材の好循環に向けた需要と供給の両面から施策を進めていく。また、各取組の進捗状況等について、情報セキュリティ政策会議及びその下の専門部会等において毎年度評価を行い、必要な施策の見直しを行う等のフォローアップを実施し、それらの評価結果については毎年度の年次報告書で公開する等、PDCA サイクルを確立する中で施策の「見える化」を進めていき、国民視点の評価及び施策の推進を図っていく。

また、民間企業等においても、リスク管理のひとつとして情報セキュリティが捉えられれば、経営層とコミュニケーションをする人材を含めた情報セキュリティ人材の需要の顕在化、ひいては企業等のリスク管理を行う経営層としてのキャリアパス構築にもつながることが期待される。

これらの取組により、人材の需要と供給の好循環が創出され、我が国の情報セキュリティ水準のさらなる向上が実現されることを強く期待する。