情報セキュリティ人材育成プログラム（案）

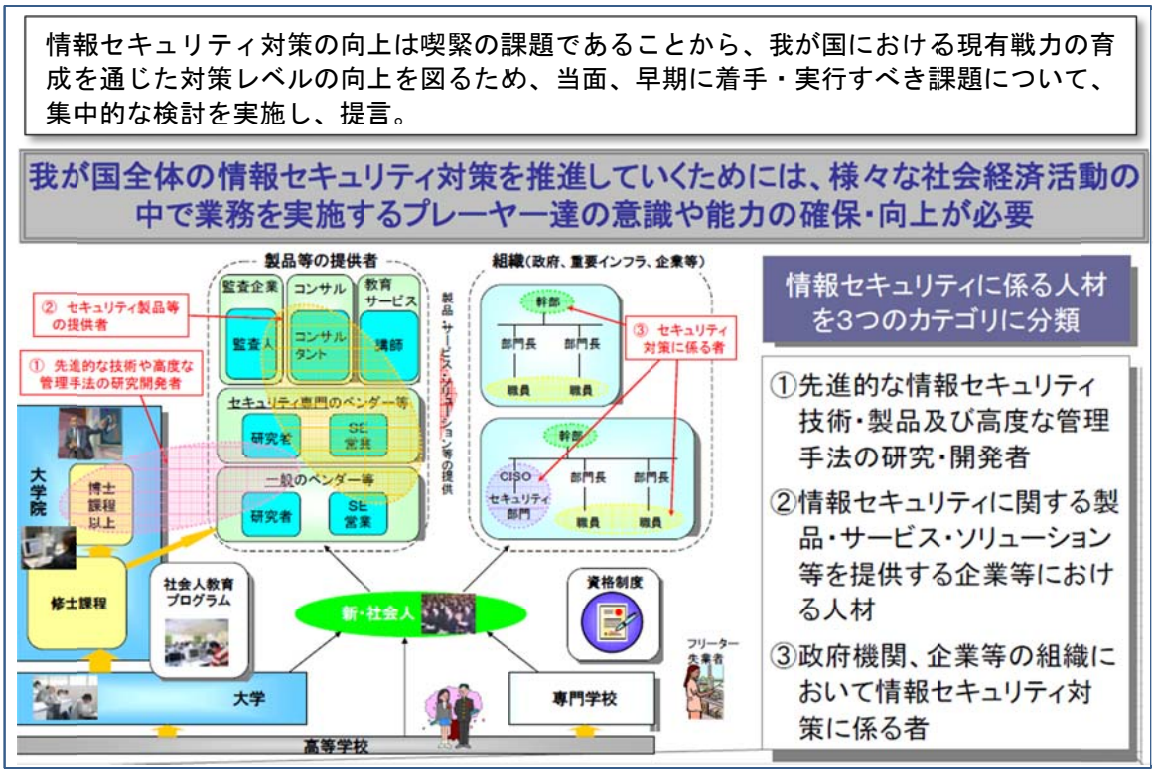
目次

1. はじめに

近年、経済活動や社会生活の情報通信技術への依存が進む中にあって、情報セキュリティ上のリスクの高度化・多様化が進展しつつあり、従来の取組をはるかに超える情報セキュリティの確保が急務である。

このような状況の変化を踏まえ、情報セキュリティ政策会議（議長：内閣官房長官）は、「国民を守る情報セキュリティ戦略」（2010 年 5 月 11 日、以下「情報セキュリティ戦略」という。）及び情報セキュリティ戦略に基づく年度計画である「情報セキュリティ 2010」（2010 年 7 月 22 日、以下「年度計画」という。）を策定し、官民が連携した総合的な情報セキュリティ政策に係る取組を推進している。

情報セキュリティの人材育成については、2006 年に情報セキュリティ政策会議「人材育成・資格制度体系化専門委員会」において議論され、政府機関及び企業等における情報セキュリティ人材における現状と課題及び今後の人材育成方策について「人材育成・資格制度体系化専門委員会報告書」（2007 年 1 月、以下「人材専門委員会報告書」という。）が取りまとめられた。



図表１　「人材育成・資格制度体系化専門委員会報告書」概要

政府としては、人材専門委員会報告書等に基づき、各種人材育成策を実施・推進してきたが、近年の情報セキュリティを取り巻く環境の急激な変化に伴う情報セキュリティリスクは極めて広範かつ多岐にわたってきている。また、グローバル人材を含めた各組織における情報セキュリティ人材の育成についても十分成功しているとは言い難いのが現状である。

このため、情報セキュリティ戦略及び年度計画並びに人材専門委員会報告書等を踏まえた様々な情報セキュリティに係る人材育成策の今後の方向性について検討するとともに、未だ不十分な領域について重点化を図った「情報セキュリティ人材育成プログラム」（以下、「人材育成プログラム」という。）を策定することとした。

また、人材育成プログラムは、今後３年間（2011 年度から 2013 年度）を対象としているが、人材育成は中長期的課題であるので、その視点も盛り込んである。なお、人材育成プログラムの評価等は、後述する「普及啓発・人材育成専門委員会」（仮称）において行い、必要に応じて取組の内容の見直しも実施する。

参考：人材育成と普及啓発の関係

高度な情報通信技術を担う先端的な人材育成と裾野が広い一般国民を主な対象とする普及・啓発施策の双方が相まって、はじめて我が国における情報セキュリティの水準をバランスよく向上させることが可能となる。

人材育成プログラムは、政府機関、企業、教育機関等における情報セキュリティ人材の育成を対象としている。普及・啓発施策については、「情報セキュリティ普及・啓発プロブラム」に基づき推進することとしており、これら両プログラムを共に推進することにより、我が国の情報セキュリティ対策の向上を図ることとする。

2. 情報セキュリティ人材に関する現状と課題

情報セキュリティ人材の育成についての必要性、重要性は以前と比べ増大しているものの、新たな課題や未だ解消されていない課題も数多く存在するなどギャップが存在する。これらの課題を解消し、効果的、効率的な人材育成を図るための構造的転換が求められる。

(1) ギャップの拡大

① 情報セキュリティ脅威の高度化・多様化に対応できる人材の不足

サイバー攻撃の大規模化・現実化、「新しいタイプの攻撃」の出現、クラウド・コンピューティング、スマートフォン等に対するセキュリティ上の脅威など、**情報セキュリティ上の脅威は、今まで以上に高度化・多様化しているが、このような急激な変化に対応することができる人材が十分に確保できていない。**これらの急激な変化に対応するためには、従来型の受動的な方法ではなく、能動的で信頼の高い（ディペンダブルな）情報システムを構築・運用する必要がある。そのためには、それらのシステムを研究開発、構築、運用できる高度な情報セキュリティ人材の確保が不可欠である。また、これらの高度な情報セキュリティ技術を理解し、効果的に運用できる幅広い情報セキュリティ知識を有する人材も求められている。

② 業種を問わず必要とされる情報セキュリティ人材の不足

あらゆる分野で情報セキュリティに関する知識が必要になっているが、それに対応できる人材が十分ではない。現在の高度情報通信社会は、情報活用の規模や情報伝達のスピードが加速化し、情報通信技術が社会的インフラとして重要な役割を果たし、情報通信技術の活用なくして、社会経済活動や国民生活を営むことができないと言えるほど、情報通信技術への依存度が高まっていると言える。このような傾向は今後も加速化されると予想され、安心・安全な情報通信システムを構築・運用するために不可欠な情報セキュリティ技術の重要性は益々高まっている。

従前であれば、情報セキュリティを扱う人材は非常に限定的であり、他の業種とは別に特別に存在するという認識で良かったが、今や、どの分野の職種においても、情報セキュリティへの認識が必須となっている。

(2) 組織のトップの認識不足

組織のトップが情報セキュリティを戦略的なものとして位置付けている事例は多くなく、情報資産に係るリスクの管理を情報システム部門等の現場の判断に任せている企業も少なくないと考えられる。現場における情報セキュリティ対策が進んでいないことに加え、経営層の意思が明確化されていない。経営層が意思決定を行う際に必要な情報セキュリティ対策の評価がうまくできていないといった、経営層による情報セキュリティ上の統制の欠如という課題も大きいと考えられる。従来の企業の情報セキュリティ対策は、「係長セキュリティ」という言葉に象徴されるように、あまりにも情報システム部門の現場に任せきりであった。これでは、企業としてリスク管理が行えているとは言えない。

最近の事例を見ても、例えば、東日本大震災直後に大規模な情報システムの障害が発生し、その対応を誤ったために、企業幹部の問題にまで発展したケースや、企業の情報システムに不正アクセスが発生し、数十カ国にわたる数千万人の個人情報が流出し、国際的にも大きな議論になっているケースが報道されていることなどを見ても分かるように、今までは現場の情報セキュリティ担当者に任せていれば何とかなると考えられていたが、各企業が情報通信技術を戦略的に活用し、業務のネットワーク化が進展している状況下においては、対応を誤れば、企業の経営問題や経営者の責任にも発展しかねない可能性があることを、組織のトップは認識する必要がある。

(3) リスク対応力の脆弱性

今般の東日本大震災では、我が国のリスク対応力の脆弱性が明らかになった。大震災の反省などを踏まえ、従来のウイルス対策、不正アクセス対策、情報漏えい対策等の狭義の情報セキュリティリスクに加え、状況が変化する中で、事業継続リスク等を如何に低減するかなど広義の情報セキュリティリスクに対して、より広い視野から、リスク・コミュニケーション、リスク・マネジメントなどを通じたリスク対応力の強化を図っていく必要がある。このような広義の情報セキュリティリスクへの対応ができるような人材を育成することが重要である。

また、今回の大震災への対応について様々な問題点も指摘されているが、一方で、新たなメディアであるソーシャル・ネットワーク・サービス（SNS）の活用や情報通信分野におけるボランティア活動など現場力を生かした災害時に大変役立った事例も数多く報告されている。このような献身的な一つ一つの創意工夫を積み重ねていくことにより、リスク対応力も高まると考えられる。

(4) 産学連携の不足（産業界のニーズと教育機関のシーズのミスマッチ）

情報セキュリティ人材の育成については、実践的な教育が不可欠である観点から、産学が連携して育成していくことが求められている。しかし、教育機関が育成を目指す人材と、産業界が求める人材には、求められる資質のギャップが以前から指摘されており、その解決は急務である。教育機関における人材育成については、企業側に直接的なメリットが少なく、企業からの協力が得られにくいという指摘もある。

事業継続性などに関するリスク対応力などをもった人材を育成するには、学部間をまたいだセキュリティとリスクマネジメントを融合したコースなどを設置し、企業でのインターンシップなども積極的に取り入れることも考えられる。

(5) グローバル化に対応した人材の不足

世界的に見て、あらゆる分野においてグローバル化が進み、情報通信産業、情報セキュリティ産業についても国を超えて一層流動化が進んでいる。このような社会において、日本の情報セキュリティ人材もグローバル化に対応していくことが求められている。日本の情報セキュリティ産業が、国際競争力をつけていくためには、初期段階から、グローバルな人材の育成を視野に入れておくことが重要である。

大学での情報セキュリティ教育においても、国外のセキュリティ関連の機関において、インターンシップをできるような制度を積極的に取り入れていくべきである。

(6) 諸外国に大きく遅れる我が国の情報セキュリティ人材育成体制

各国の情報セキュリティ人材の育成体制を見てみると、官民が連携した人材育成、情報セキュリティ技術コンテスト等を通じた人材育成、高等教育機関による独自の人材育成等、様々な体制で情報セキュリティ人材の育成を実施している。しかし、我が国においては、情報セキュリティ人材育成についての認識は高くなく、戦略的分野に係る人材育成であるにもかかわらず、諸外国に大きく遅れてしまっているのが現状である。

(7) 分野別課題

① 政府機関における人材育成

政府機関における情報セキュリティ人材育成については、これまで情報セキュリティ政策会議において決定・改定された「政府機関の情報セキュリティ対策のための統一基準」（以下、「統一基準」という。）等に基づき、最高情報セキュリティ責任者等の各種責任者・管理者の設置や情報セキュリティ対策に係る教育等の人材育成体制が整備されてきた。

しかし、情報セキュリティに関する高度な能力を有する者の育成には、長期間を要するにも関わらず、多くの機関においては、情報セキュリティ対策を担当する者として、こうした職員が配属されるとは限らない状況にある。また、２～３年以内に人事ローテーションが実施されることから、情報セキュリティ対策の担当者のキャリアパスを構築することが困難とされている。

② 企業における人材育成

今や、ほとんどすべての企業がインターネットを利用する[1]時代になっているが、他方、インターネットや企業内ＬＡＮ等を利用する上での問題点として、「セキュリティ対策の確立が困難」、「ウイルス感染に不安」、「従業員のセキュリティ意識が低い」という理由が挙げられている[2]。

また、インターネットや企業内ＬＡＮ等を利用する企業のほとんどが何らかのセキュリティ対策を実施してはいるが、その対策の状況は、ウイルス対策プログラムの導入といったような従来の対策を実施しているだけというのが現状である。

多くの企業における人材育成については、人材育成戦略を策定するノウハウもなく、日々の OJT の中で能力の向上を図るしかないという現状にある。また、最近は OJT の機会が減少するとともに、情報セキュリティ人材に対する認識があまり高くないため、計画的な人材育成があまり行われておらず、人材育成の機会も十分に確保されていない。

情報通信技術が企業活動に深く浸透し、情報セキュリティリスクへの対応が経営に与える影響が益々増大してきている下で、急速に高度化・多様化し続ける情報セキュリティ上の脅威に対応することのできる人材の育成が求められている。

---

[1] 総務省「平成 22 年通信利用動向調査の結果」平成 23 年 5 月 18 日より「企業のインターネット利用率は、全体で 98.8%」

[2] 総務省「平成 22 年通信利用動向調査の結果」平成 23 年 5 月 18 日
「インターネット、企業内ＬＡＮ等を利用する上での問題点（企業）（複数回答）（平成 22 年末）」

③ 大学院における人材育成

大学院では情報セキュリティに関する高度な専門的研究開発を行うのが中心であるのに対して、産業界では、製品・サービスに組み込むことができる要素技術としての実用的な情報セキュリティ技術が求められる。互いが求める資質が異なることから、学内研究者が産業界へ進むことは困難な状況である。また、研究テーマや、求める人材像の違いから、産業界と学術界とは人材交流や共同研究等が活発にできない状況もある。

④ 大学における教育

大学は、知識の創造・発信拠点として、社会的責任を遂行するに当たり、重要な責務を担っている。また、大学における教育や研究のために、今や情報通信技術は欠かせない存在になっており、情報セキュリティについて共通した認識を持って情報を安全に利活用することが求められている。情報セキュリティというものが、企業人にとって特殊ではなくなりつつあり、広義の情報セキュリティリスクに対応することができる人材が求められているが、このような人材はまだ不足していると考えられる。

また、情報セキュリティの分野は、情報セキュリティに関する専門的な知識に加え、様々な周辺領域に関する知識も必要になるため、自らの専門分野に関する知識を深めるとともに、各分野の専門家と協力・連携を図るといった「コラボレーション力」を充実させることができるような枠組みや教育体制を整備することも重要である。

⑤ 初等中等教育段階における教育

学校教育における情報セキュリティ教育については、平成 10 年の学習指導要領改訂[3]において、コンピュータや情報通信ネットワークの積極的な活用等情報教育の充実が図られ、平成 20 年及び平成 21 年の学習指導要領改訂[4]において、情報モラル[5]に関する指導の充実等も含め、教育の情報化について、情報教育及び教科指導における情報通信技術活用の両面で様々な充実が図られている。

---

[3] 平成 10 年 12 月に小学校及び中学校学習指導要領が、平成 11 年 3 月には高等学校学習指導要領の改訂告示がなされた。具体的には、中学校技術・家庭科（技術分野）で「情報とコンピュータ」を必修とするとともに、高等学校で普通教科「情報」を新設し必履修とするとともに、専門教科「情報」を新設した。

[4] 平成 20 年 3 月に小学校及び中学校の新学習指導要領が、平成 21 年 3 月には高等学校及び特別支援学校の新学習指導要領の改訂告示がなされた。

[5] 「情報モラル」とは、「情報社会で適正に活動するための基となる考え方や態度」

しかし、高性能化してきた携帯電話等を通じたインターネットの利用が急速に普及し、インターネット上での誹謗中傷やいじめ、インターネット上の犯罪や違法・有害情報、個人情報の流出などの問題が発生している社会において、情報セキュリティの確保の重要性が高まっている。

情報化の光と影の影響の両面を十分に理解した上で、情報モラル教育に取り組むことがますます重要となり、特に道徳をはじめ、各教科等での指導を通じて、情報社会における基本的なルールやマナー、情報通信技術の安全な活用等、情報を活用する場面での基本的な考え方や態度を育成することが一層重要になってきている。

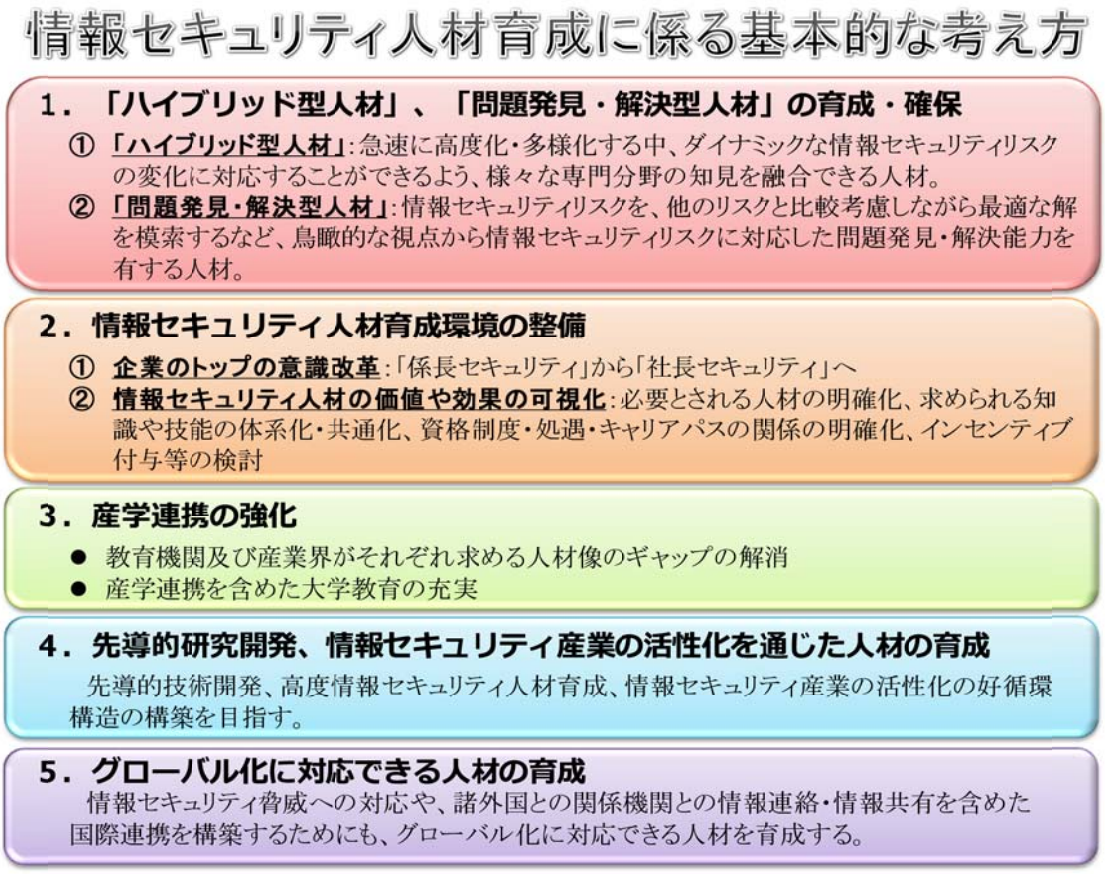
⑥ 教員の指導力について

教員一人ひとりが情報通信技術活用指導力の向上の必要性を理解し、校内研修等を積極的に活用して、自ら研鑽を積むとともに、教育委員会等が各学校の研修に積極的に関わったり、教育委員会等の研修を充実することが必要である。また、平成 22 年３月末時点において公立学校の校務用コンピュータの整備率は、教員１人１台に近づいている。校務の情報化が進展していく中、情報セキュリティの確保は避けて通ることができなくなってきている。

児童・生徒に情報セキュリティを教える立場の教員の情報セキュリティに関する知識及び指導力は必ずしも一様ではないにも関わらず、学校業務の多忙さから情報セキュリティ知識の習得機会が少ないと考えられる。

3. 基本的な考え方

情報セキュリティをめぐる環境の変化や、情報セキュリティの人材育成に係るこれまでの取組や課題を踏まえ、政府として推進すべき人材育成に関する基本方針を以下に示す。



図表２　情報セキュリティの人材育成に係る基本的な考え方（概要）

(1) 「ハイブリッド型人材」、「問題発見・解決型人材」の育成・確保

情報セキュリティ分野において求められる人材の領域は、技術面で言えば、数学、コンピュータ科学、通信工学など、管理面で言えば、経済・経営学、法律、会計学、社会・集団心理学といった周辺領域と密接不可分な関係にある。また、情報セキュリティ対策は、技術的な情報システムの立場からだけで実現できるものではなく、企業の監査業務、法務業務等とも密接に関係する。すなわち、情報セキュリティ分野においては、情報システムや情報セキュリティに関する技術的知見に加え、マネジメントの知見、さらにはリスク管理能力のある人材が求められる。情報通信技術は他の分野に比べ技術革新が著しいため、パラダイムシフトが起こることを前提に今後の技術動向やその影響を把握できる能力を有するとともに情報セキュリティに係る脅威が高度化、多様化する

中、ダイナミックなリスクの変化に対応できる人材が求められている。このように、情報セキュリティ分野においては、一つの分野の専門家ではなく、様々な専門分野の知見を融合できる文理融合型の「ハイブリッド型人材」が求められている。

IT リスクという視点から考えれば、IT リスク対策は、一つの対策だけで完結することは困難であり、様々な対策の組み合わせが不可欠である。また、状況がダイナミックに変化することにより、許容できるリスクレベルも大きく変化するなど、状況が瞬時に激変する中で最適な対応を行うための「ダイナミック・リスク対応」の観点や一つのリスクへの対応が従来存在しなかった新たな別のリスクを引き起こすことがあり、リスクとリスクを比較考慮しながら最適な解を模索するなど、鳥瞰図的な視点で、ダイナミックに変化する情報セキュリティリスクに対応した問題発見・解決能力を有する「問題発見・解決型人材」が求められている。

特に、今般の東日本大震災を踏まえ、リスク・コミュニケーション、リスク・マネジメントなどの重要性が認識されたところであり、我が国全体として、リスク対応能力の強化が求められている。情報セキュリティ分野は、日々、リアルタイムでグローバルに発生するリスクに対応せざるを得ない環境におかれているため、この分野における人材育成の知見は、大規模災害が発生した際にも対応できる人材の育成にも活用できると考えられる。

従来、どちらかと言えば、情報セキュリティ分野は、技術に詳しい人材を求める傾向にあったが、情報セキュリティが安心、安全な情報通信技術を支える基盤的な技術に位置づけられ、各企業が情報通信技術への依存度を高め企業経営、企業戦略などとも密接に関係する環境下においては、技術の視点のみで人材を育成するのでなく、「バイブリッド型人材」、「問題発見・解決型人材」に焦点を当てた人材育成を図ることが極めて重要である。

(2) 情報セキュリティ人材育成環境の整備

① 企業のトップの意識改革

―「係長セキュリティ」から「社長セキュリティ」へ[6]―

組織のトップは、「情報セキュリティ対策は、情報システム部門の現場に任せておけばよい（「係長セキュリティ」）」という発想から脱却すべきである。

企業経営者として、企業のリスク管理は、自らの問題であると認識しているが、情報セキュリティ対策については、企業経営者のマターではない

[6] 林紘一郎「情報セキュリティ総合科学　第２号」~係長セキュリティから社長セキュリティへ：日本的経営と情報セキュリティ~2010 年 11 月, http://www.iisec.ac.jp/proc/vol0002/iisec_proc_002_p001.pdf

という認識が大半である。しかしながら、企業活動の主要な部分は、情報通信技術に依存しており、そのリスク対策が情報セキュリティと捉えると情報セキュリティ対策は、経営の根幹にかかわる問題である。自社の有する技術情報等の知的財産を守り、高い競争力を維持し、企業を成長させていくためにも、情報セキュリティの確保・維持は、企業経営上のかなめとなる。また、情報セキュリティがリスク対策である以上、それは全社的に費用対効果を最適化するものであり、他の経営意思決定と何ら異なるものではない。さらに、情報セキュリティ対策は、経営全般のガバナンスと責任の在り方（内部統制、コンプライアンス、品質管理、環境適応、企業の社会的責任）などと整合的かつ統制の取れたものでなければならない。

以上のことを踏まえると、昨今の状況変化は、情報セキュリティ対策について、まさに「社長セキュリティ」が求められていると言える。このことは、情報セキュリティの課題のところでも述べた、最近発生した民間企業の大規模な情報システム障害や大規模な個人情報の流出事案などへの対応を見るまでもない。

情報セキュリティ対策を推進するためには、トップから現場の職員に至る全ての社員がリスク管理意識を共有し、それを支えるモラルとモチベーションを持てる環境を醸成することが重要である。

また、情報セキュリティの確保に関わるガバナンスを円滑化させるために、現場や現場の管理者などとトップとの意思疎通をより活性化するための人材育成も重要である。

「社長セキュリティ」の確立は、従来、企業における情報セキュリティ人材育成の課題とされていた、ⅰ）処遇と連動できていない、ⅱ）就業満足度やモチベーションの向上を図ることが難しい、といった課題の解決にも寄与すると考えられる。このことは、情報セキュリティに従事する者の社会的地位の向上など、情報セキュリティを魅力ある職業として位置づけることにも貢献する。

② 情報セキュリティ人材の価値や効果の可視化

少子高齢化の進展による人材の確保の困難化や厳しい勤務環境の指摘があることなどを踏まえ、産業界、企業が求める情報セキュリティ人材の明確化や効果の可視化を図ることが重要である。大多数の企業においては、情報セキュリティに関して求められる知識や技能が体系化、共通化されておらず、各個人レベルでのスキル保有に留まっているとの問題点がある。

資格制度や各種教育プログラムについては、2007 年の人材専門委員会報告でも指摘されているように、その見直しを引き続き図る必要があるが、資格制度、処遇、キャリアパスの関係を明確に位置づけることが情報セキ

ュリティ人材の確保を図る上で重要である。また、情報セキュリティ人材育成に関するインセンティブ付与（情報セキュリティ人材の評価、優遇制度など）について検討する必要がある。

(3) 産学連携の強化

教育機関が育成を目指す人材と、産業界が求める人材には、求める資質のギャップが以前から指摘されており、その解決は急務である。また、産学連携を含めた大学教育については、従前より実践的な情報セキュリティ教育の不足が指摘されてきた。これらの課題を解決するため、平成 18 年度から文部科学省の施策である「先導的 IT スペシャリスト育成推進プログラム』が始まり、それに基づき、平成 19 年度に、「ISS Square」（情報セキュリティ大学院大学、中央大学、東京大学)、「IT Keys」（奈良先端科学技術大学院大学、北陸先端科学技術大学院大学、大阪大学、京都大学）が、研究と実務を融合し、大学間や産学の壁を超えて潜在力を結集し、情報セキュリティ分野における世界最高水準の人材を育成するためのプログラムとして採択された。

大学名	プロジェクト名称	プロジェクト概要
・奈良先端科学技術大学院大学 ・京都大学 ・大阪大学 ・北陸先端科学技術大学院大学	IT Keys 社会的ITリスク軽減のための情報セキュリティ技術者・管理者育成	民間・公共の各種組織において情報セキュリティ対策の立案遂行を主体的に実施しうる人材の育成を目標とし、組織管理技法および情報システムの総合リスク対策技術を体系的に習得するために関西圏を中心とした情報系4大学院により連携型教育コースを設ける。社会人を積極的に受け入れ、団体・企業からの招聘講師による最新動向を反映した講義および実践的演習を通じ、即戦力となりうる実務者を養成する。
・情報セキュリティ大学院大学 ・東京大学 ・中央大学	ISS Square 研究と実務融合による高度情報セキュリティ人材育成プログラム	情報セキュリティ大学院大学、中央大学、東京大学、NII、NICTと企業8社の産学連携による研究と実務を融合したプログラムにより、高度情報セキュリティスペシャリストを養成する。講義・実習とも充実した科目群による情報セキュリティに関する幅広い知識と高い実践力を備えたリーダー人材と、産学連携による高度かつオープンな研究会活動を通じて醸成される本質的な問題解決能力を備えた高度研究開発人材とを育成する。

図表３　先導的 IT スペシャリスト育成推進プログラム（平成 19 年度採択拠点）

文部科学省「「平成 19 年度先導的 IT スペシャリスト育成推進プログラム」採択状況」平成 19 年 9 月

予算措置は、平成 22 年度で終了したが、この取組は、我が国の高度情報セキュリティ人材を育成するためのモデルとなる取組であり、人材育成が中長期的な課題であることを踏まえれば、この成果を単発のプロジェクトの成果として捉えるのではなく、永続性をもった取組にすることが我が国において世界最高水準の情報セキュリティ人材を育成するためにも極めて重要である。本プロジェクトは、産学連携のベストプラクティスでもあり、何らかの形で予算措置がなされることを期待する。

(4) 先導的研究開発、情報セキュリティ産業の活性化を通じた人材の育成

「情報セキュリティ研究開発戦略」において指摘されているように、クラウド・コンピューティングやスマートフォンなどの情報セキュリティ上の課題や「新しいタイプの攻撃」の発生など情報セキュリティの脅威は、高度化・多様化しており、これらに対応するためには、新たに「能動的で信頼性の高い（ディペンダブルな）情報セキュリティ」（ニュー・ディペンダビリティ）に係る研究開発を、世界を先導する形で推進していく必要がある。

このような研究開発を推進するには、高度な情報セキュリティ人材が必要であり、この分野で先導的な研究開発成果が得られれば、我が国の情報通信産業や情報セキュリティ産業の国際競争力強化やグローバル展開にも貢献できる。先導的技術開発、高度情報セキュリティ人材育成、情報セキュリティ産業の活性化の好循環構造が構築できるよう積極的に取り組む必要がある。

(5) グローバル化に対応できる人材の育成

我が国の企業のグローバル化は進展しており、オフショアばかりではなく、海外展開を図る企業も増加している。企業の海外拠点との間の神経系とも言える情報通信ネットワークは不可欠であり、それを支える情報セキュリティに対するニーズも高まっている。また、情報セキュリティの脅威の視点からは、サイバー攻撃やコンピュータウィルスは、国境とは無関係に発生しており、これらに的確に対応するためには、諸外国の関係機関との情報連絡、情報共有など国際的な連携が不可欠である。また、情報セキュリティ技術にも、国境は存在しないため、グローバルな視点でその動向を把握する必要があることは言うまでもない。この傾向は益々加速化すると予想されることから、グローバル化に対応できる情報セキュリティ人材の育成は急務である。

4.　具体的な取組

(1) 「普及啓発・人材育成専門委員会」（仮称）等の設置

情報セキュリティの人材育成･確保を専任とする司令塔機能を明確化するため、「情報セキュリティ政策会議」の下に、新たに「普及啓発・人材育成専門委員会」（仮称）を設置し、情報セキュリティに関する普及啓発、人材育成施策について、助言、評価等を行う。「普及啓発・人材育成専門委員会」（仮称）は、以下の点を参考に助言、評価等を行う。

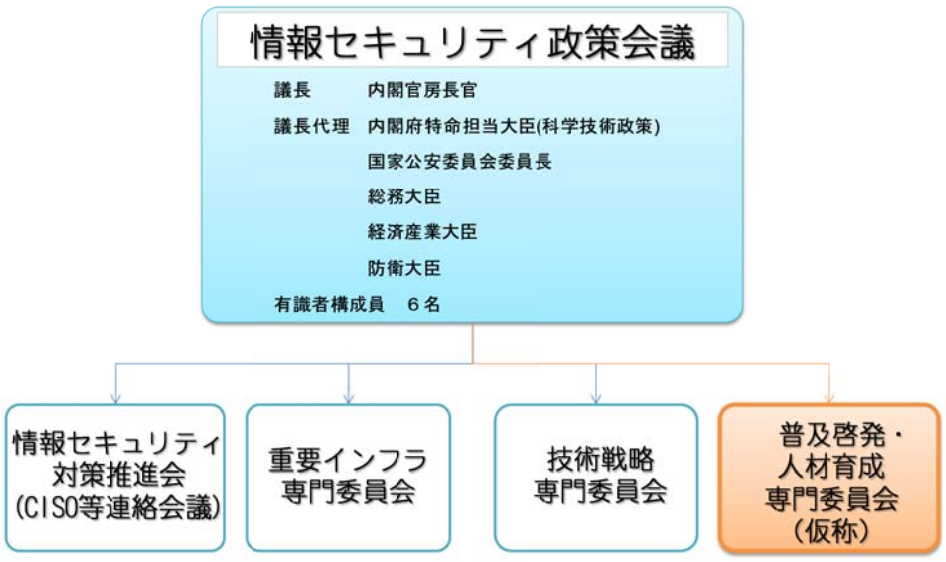
ⅰ）人材育成プログラムの具体的な取組が、「３．基本的な考え方」で示した「ハイブリッド型人材」、「問題発見・解決型人材」の育成などに資する取組になっているかの検証を行う。

ⅱ）人材育成プログラムについて、政府機関、企業、教育機関別に進捗状況をフォローする。十分な進捗が見られない場合は、その原因や解決方策などについて議論し、必要に応じ、助言などを行う。

ⅲ）様々な資格制度や教育プログラムがあることから、それぞれの効果について可能な範囲で検証し、必要に応じ、改善策などについて、助言などを行う。

ⅳ）資格制度、キャリアパス、処遇等との関係について、必要に応じ、可能な範囲で検証を行う。

ⅴ）情報セキュリティを巡る環境変化を踏まえた施策の見直しや新たな施策について提言を行う。



図表４　「普及啓発・人材育成専門委員会」（仮称）の位置付け

(2) 先端的な情報セキュリティ研究者・技術者等の育成

我が国全体の情報セキュリティ水準の向上や情報セキュリティ分野の国際競争力の強化を図るためには、世界を先導することができる先端的な情報セキュリティ研究者・技術者を多数育成する必要がある。これは、大学院教育の充実や様々な研究機関での研究開発の方向性などとも密接に関係するが、世界に通用する日本発の技術や、産業界の製品やビジネスに結びつくような大学発の技術について研究開発していく観点からも、科学技術基本計画とよく連携を図りながら、今回取りまとめられた「情報セキュリティ研究開発戦略」を戦略的に推進する中で、先導的な研究者・技術者を育成することが重要である。

また、研究開発戦略を官民が連携して推進し、クラウド・コンピューティング、スマートフォン、IPv6、SNS などにおける情報セキュリティ上の課題を解決できる新たな技術開発及びその普及促進や、サイバーセキュリティ研究テストベッド等を活用した有機的な人材ネットワークの構築を通じて、新たな情報セキュリティ対策を推進できる高度な人材の育成に貢献する。

(3) 政府機関における人材育成

政府機関においては、昨今の情報セキュリティに係る問題意識や技術的・環境的な変化に対応し、最高情報セキュリティ責任者による情報セキュリティ対策の取組の理解及び把握に資する新たな基本方針として、「政府機関の情報セキュリティ対策のための統一規範」（以下、「統一規範」という。）を情報セキュリティ政策会議において決定したところである。

この統一規範等に基づき、政府職員に対して、人材育成施策を計画的かつ着実に推進していくことが重要である。具体的には、政府職員向けの統一的な教育プログラムの充実や教育教材のひな形の充実、標的型メール攻撃に係る教育訓練等を実施することで、政府職員における情報セキュリティに関する知識の習得とその向上を支援する。

(4) 企業における人材育成

① 企業経営者の意識改革

企業の情報セキュリティ対策については、「係長セキュリティ」から企業のトップ自らが判断する「社長セキュリティ」への抜本的な転換を図る必要がある。そのための一助として、海外の事例を含め、企業経営上の情報セキュリティ対策に関する成功事例や失敗事例を共有できる仕組みを構築することは有意義である。また、企業の経営トップ同士が様々な議論を行う場において、企業のリスク管理の観点から情報セキュリティ対策の在り方や人材育成方策などをテーマとして取り上げ、意見交換を行うこと

も有意義である。

② 全社的な人材育成環境の整備

企業等における、情報セキュリティ人材の育成の方針等を定めた人材育成計画や明確なキャリアパスの策定、普及を促進する。ⅰ）求められる人材像、ⅱ）資格制度・教育プログラム、ⅲ）キャリアパス、ⅳ）処遇（評価体系）等の関係が明確になれば、企業内における人材育成も促進される。

人材育成計画を立案する者は、自らの組織において、どのような人材が必要になるかを検討し、人材に求められる能力と教育プログラムなどを参考としながら、人材育成計画を定めることが望まれる。また、企業内の各組織において求められる情報セキュリティ人材像を明確にし、その情報セキュリティ人材に求められる知識や技能を体系化、共通化することが重要である。業務改革、システム改革と並行して、情報セキュリティ要件を見直し、それを担える人材を育成する必要がある。

また、情報セキュリティ人材育成計画については、内外を問わず、ベストプラクティスを収集、分析、共有することが有効である。さらに、人材を育成するにあたっては、一定の評価体系に沿った処遇を行うプロフェッショナル制度の導入等も有用である。なお、情報セキュリティを巡る環境変化や企業戦略に応じて人材育成計画のレビューを行う必要があることは言うまでもない。

情報セキュリティ技術が個人レベルでのスキルの保有とならないよう、体系だった知識を習得させるために、社会人学生として改めて高等教育機関等で学び直すリカレント教育を実施することも有効である。

③ ＣＩＯ、ＣＩＳＯの任命等

CIO[7]、CISO[8]は、情報セキュリティに関する最終的な意思決定権限を持つ者であり、組織の情報リスクの概況把握と許容リスクレベルの決定、情報セキュリティ対策のためのリソース調達と割り当て、情報セキュリティの管理状況のモニタリングと改善指示などを行う。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。今後、益々、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、CIO、CISO を組織内

[7] 「CIO」とは、Chief Information Officer（情報システム統括役員）の略称で、企業における情報通信技術の導入、利活用に関するすべての最終責任を負っている役員をいい、企業において自社の経営理念に合わせて情報化戦略を立案、実行する責任者をさす。

[8] 「CISO」とは、Chief Information Security Officer（最高情報セキュリティ責任者）の略称で、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。

できちんと位置付けていくことが重要である。

また、情報セキュリティの脅威が、今後ますますグローバル化、高度化、複雑化するということを踏まえると、民間企業において「情報セキュリティ保険」といった制度も他の制度を参考としながら、検討されることも一案である。

④ 重要インフラ事業者

重要インフラ事業関係者の情報セキュリティ基盤の強化のために、分野横断的演習や訓練及びセミナー等を通じ、高度な情報セキュリティ知識を有する人材の育成に積極的に取り組むとともに、その状況を関係者間で共有するよう努める。

⑤ 中小企業

中小企業における高度な情報セキュリティを確保するため、中小企業を指導する立場にある者等を対象とした「中小企業情報セキュリティ指導者セミナー」等を実施する。

(5) 教育機関における人材育成

教育機関における人材育成についても、「ハイブリッド型人材」、「問題発見・解決型人材」の育成・確保に重点を置いた取組が望まれる。例えば、学部を超えた連携や、大学を超えた連携、産学連携などが望まれるとともに、知識伝授型だけではなく、学生自らが問題を発見し問題解決を行う方式を積極的に採用していくことが期待される。

① 大学院教育の充実

世界最先端の情報セキュリティ人材の育成を目指した「ISS Square」や「IT Keys」のような取組は、産学連携、大学間連携、高度情報セキュリティ人材の育成、国際競争力の確保のそれぞれの観点からも非常に価値のあるものであり、このような成功事例を正しく評価し、引き続き継続、発展させていくことが極めて重要である。また、情報セキュリティに特化した大学院における高度な専門性を有する人材の育成や、文理融合型の情報セキュリティ・リスクマネジメントコースなどを開設し、産業界と連携を図りつつ、社会人教育プログラムの充実を図る必要がある。

企業経営や組織運営などにおけるリスク管理も含めた広義の情報セキュリティという基本概念をベースに、マネジメントと技術を理解できる高度専門職業人を育成するために、経済学、経営学などと情報通信工学、情報セキュリティ工学等の両面に関する理論と実務教育のバランスに配慮

した体系的なカリキュラムの確立や、学部新卒者や企業人など背景の異なる学生の多様なニーズに配慮した教育内容の充実を図ることが望ましい。

② 大学教育における情報セキュリティ教育の充実

実社会に出た時に、情報セキュリティに関する意識を持っていることは重要であり、各大学の自主的な判断により、大学の共通教育・教養教育の中で、情報セキュリティ教育を受ける機会を確保することも考えられる。このためにも、情報倫理などの科目を通じ、情報セキュリティに関する最低限の教育を実施することを奨励する。また、教育教材や学習ツール等の充実を図るとともに、情報セキュリティだけではなく、リスク・マネジメントの概念や知的財産やプライバシーなど幅広く学ぶことができる環境を構築することも一案である。

なお、情報処理関連学科においては、情報セキュリティ脅威の高度化、広範化等に対応することができるよう、大学間連携による教員体制の充実や、教材の充実・普及を図る。また、グローバルに活躍できる情報セキュリティ人材を育成していく観点から、諸外国と相互理解の増進や人的ネットワークの形成を促進していくためにも、学部学生時代から海外の学会やインターンシップ等への参加の機会を設けることも有用である。

③ 実務経験学習等実践的な教育の充実

情報セキュリティの分野は、単なる情報セキュリティの知識の習得のみならず、実務経験が必要となることが多いため、産学連携の観点からも、実務経験学習を充実させたり、企業人講師に授業してもらうなどの取組を充実させるなど、より実践的な教育を行う。

④ 初等中等教育における情報セキュリティ教育の充実

初等中等教育段階において、平成 20 年及び平成 21 年の学習指導要領の改訂により、共通科目「情報」をはじめとする教科等において、発達段階に応じた情報セキュリティに関連する教育を充実させたところである。その際、情報セキュリティの動向等に合わせた内容について教育していくことが重要である。

⑤ 教員への情報セキュリティ研修の充実

教職員の受講する研修において、情報セキュリティについて学ぶことができるような研修の体制を整備する。また、情報教育担当者連絡会議等を通じ、児童生徒に適切な教育を実施することができるよう、最新の情報セキュリティの動向について周知する。

(6) 官民連携・産学連携の強化

① 産学連携教育のマッチングの促進

産業界と教育機関のニーズのマッチングを促進するためにも、産学双方が互いのメリットを明示し理解することで、教育機関は企業の協力を得つつ、卒業後グローバルマーケットで活躍できるような実践力を備えるための教育を推進、継続する。その際、「ISS Square」や「IT Keys」の取組を参考にする。また、国内外の企業におけるインターンシップ制度を積極的に活用することも有用である。

② 実践的な教育体制の確立への協力促進

実践的な情報セキュリティ教育の確立に向け、産学が連携し、共同の教育カリキュラムの設計、企業人講師の派遣、企業人、大学教員、学生の交流を強化する等の協力体制を強化する。また、情報セキュリティ分野の産業とそれ以外の産業間における人材交流の活発化も期待される。

③ 情報セキュリティ・コンテスト等の活用

情報セキュリティについて、多大な貢献を果たした個人・企業等を表彰したり、諸外国で実施されているような情報セキュリティ・コンテストを実施し、その成績優秀者に対して奨学金を授与するという取組も国内外でみられる。高度な情報セキュリティ人材を確保する観点やグローバルに活躍できる人材を育成する観点からも、インセンティブ措置や全国規模の情報セキュリティ・コンテストの在り方について検討する。

④ 政府機関における就業経験機会の推進

情報セキュリティ分野に興味を有する学生に対する就業経験を提供する観点から、技術系行政官を採用している政府機関等において、既存のインターンシップにかかる取組等を活用しつつ、情報セキュリティに関連する部署でのインターン学生の受入れ等の推進に努める。

(7) 国際連携の強化

情報が国境を越えて自由に流通する昨今、各国が連携して情報セキュリティ政策を推進することが不可欠である。ビジネス環境や経済活動の情報通信基盤が急速にグローバル化する中、我が国の国際競争力の強化を図りつつ、他国と連携していくことが重要である。

特に、ASEAN との関係では、内閣官房情報セキュリティセンターにおいて、2009 年から連携枠組みを通じ、様々な分野において連携強化を図ってきており、情報セキュリティの人材育成においては、2010 年より「日・ASEAN 情報セキュリティ研修」や「日・ASEAN 政府ネットワークセキュリティワークショップ」等を通じ、ASEAN における情報セキュリティ人材の育成を実施しているが、今後も引き続き、当該取組を更に強化、充実させていく。

また、情報セキュリティ人材の育成については、欧米諸国等においても推進されており、各国において高等教育機関の教育プログラムや技術コンテスト等、様々な活動が実施されている。グローバル化に対応した人材を育成していくためにも、国内のみの活動だけではなく、ベストプラクティスの共有や、具体的な協力分野等について検討していくことが望まれる。

国境を超える脅威などに対抗するためには、一国での対策では効果が薄く、国際的な連携を持った情報セキュリティ施策を展開することが必要である。そのため、サイバー攻撃事案などに対し、国際連携を通じた人材の育成を図ることが重要である。