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
（案）

2012 年　月　日

普及啓発・人材育成専門委員会

目次

１．はじめに.....3

２．情報セキュリティ人材育成プログラムについて.....5
（１）現状と課題.....5
（２）基本的な考え方.....6
（３）具体的な取組.....6

３．情報セキュリティ人材育成施策の課題及び具体施策提言について.....9
（１）企業等の情報セキュリティ担当者.....10
①情報セキュリティ専門家を目指す者の支援.....11
②企業等における情報セキュリティ人材育成の支援.....12
③企業経営層への情報提供等.....15

（２）政府機関等の情報セキュリティ担当者.....20
①組織内 CSIRT 等の設置、サイバーインシデント版の DMAT の育成.....21
②情報セキュリティリスクに確実に対応できる職員の採用・育成.....21
③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.....22
④重要インフラ事業者における人材育成促進.....23

（３）情報セキュリティ産業人材.....25
①企業等における人材の育成支援.....25
②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大学
・大学院教育の強化.....27
③優秀な人材の発掘及び更なる能力向上.....28

（４）先端的な研究者・技術者.....30
①情報セキュリティ研究開発の推進.....30
②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大学
・大学院教育の強化等.....31
③産学官の人材交流と高度な人材に係るコミュニティの形成.....31
④グローバルに活躍できる人材の育成.....32

（５）人材類型を跨ぐ横断的課題等.....33

（５－１）情報セキュリティ人材の基礎的資質を育成する教育の充実……33
①初等中等教育段階における情報セキュリティに関する教育の充実等……33
②大学の共通教育・教養教育における情報セキュリティに関する教育の充実等……34
（５－２）情報セキュリティの専門家育成のための共通課題……35
①産学連携の強化……35
②情報セキュリティに関する事故事例等の有効活用……37
③法律専門家の育成……37

１．はじめに

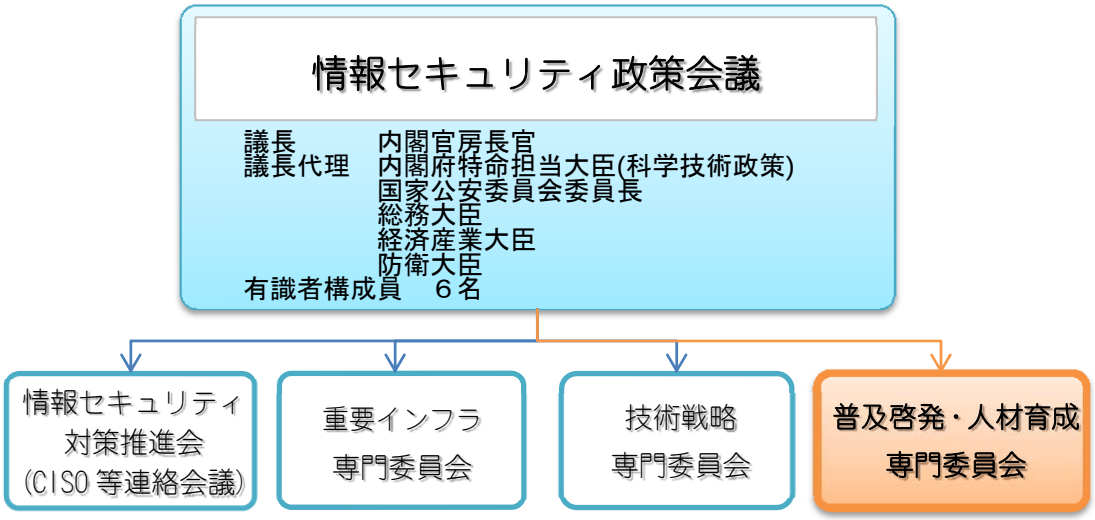
近年、経済活動や社会生活の情報通信技術への依存が高まる中にあって、情報セキュリティ上のリスクは高度化・多様化しており、従来の取組を超えた情報セキュリティの確保が急務となっている。

このような状況を踏まえ、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）及びこれ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）、「情報セキュリティ 2011」（2011 年７月８日）等を策定し、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「情報セキュリティ人材育成プログラム」が策定された。本プログラムは、2011 年度から 2013 年度までを対象とし、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するとともに、未だ不十分な領域について重点化を図っている。

情報セキュリティの普及・啓発については、「情報セキュリティ普及・啓発プログラム」が同時に策定され、情報セキュリティ対策を一般常識として国民全体に定着させるための各種取組を推進することとされている。

また、情報セキュリティの人材育成・確保及び普及・啓発に係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」（以下「専門委員会」という。）が設置された。専門委員会は、両プログラムを踏まえ、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、評価等を行うこととされている。



図表１　普及啓発・人材育成専門委員会の位置付け

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ためには、情報セキュリティ対策を担う人材の育成と、一般国民を主な対象とする普及・啓発の双方を促進する必要がある。情報セキュリティに関する普及・啓発については、普及啓発・人材育成専門委員会の下に「普及啓発・人材育成推進方策検討ワーキンググループ」を設置して検討しているところである。

専門委員会においては、情報セキュリティ人材育成プログラムの内容を踏まえ、情報セキュリティの人材育成施策について、2011 年 11 月から５回にわたって検討を行った。

本報告書はそれらの議論を基に、情報セキュリティ人材育成プログラムで提言されている施策について体系化及び具体化を行い、今後の具体的課題を整理したものである。

２．情報セキュリティ人材育成プログラムについて

はじめに、専門委員会における議論の契機となった情報セキュリティ人材育成プログラムの内容について概説する。

（１）現状と課題

情報セキュリティ人材育成プログラムにおいては、情報セキュリティ人材に関する現状と課題として大きく六つの事項を挙げている。

まず、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と、また、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ことが指摘されている。

次に組織のトップの認識不足である。従来の企業等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と指摘されている。

三つ目として、リスク対応力の脆弱性が挙げられている。東日本大震災の反省などを踏まえ、事業継続リスク等を如何に提言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、リスク対応力の強化を図っていく必要があるとされた。

四つ目として、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）が指摘された。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、その解決は急務だとされている。

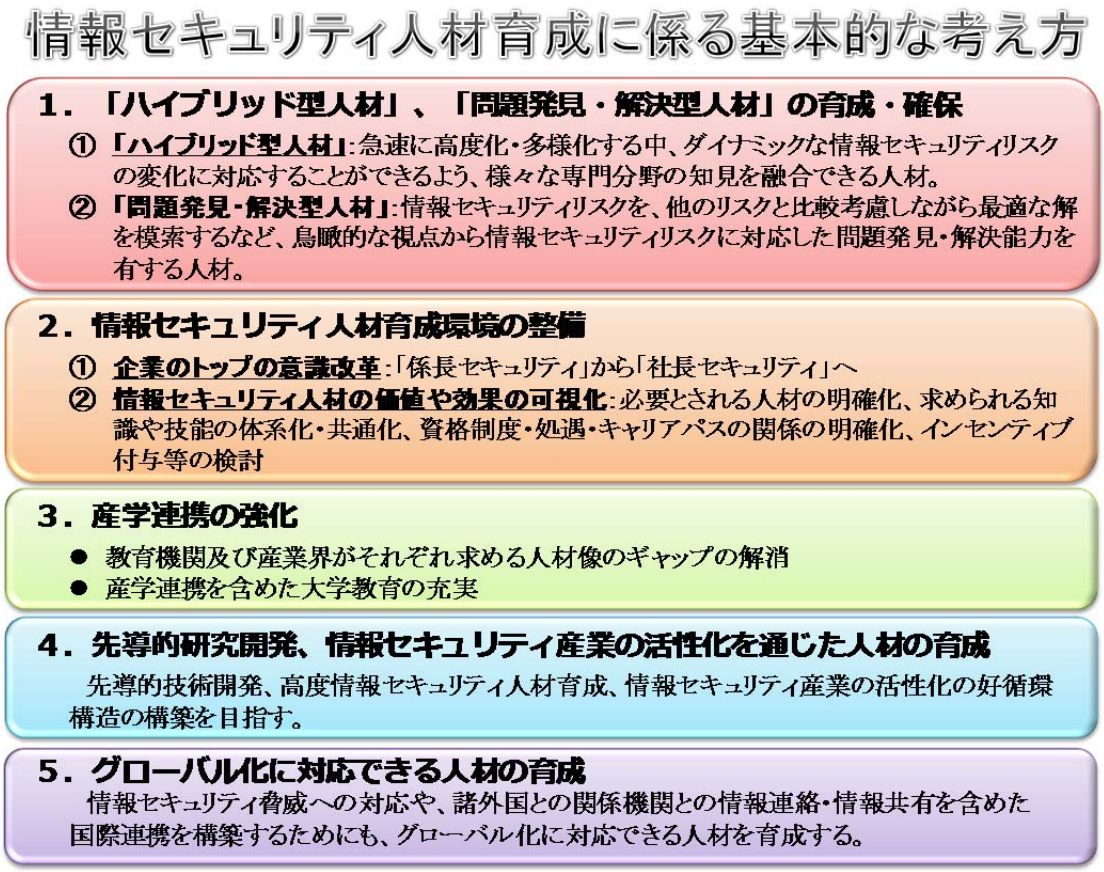
五つ目として、グローバル化に対応した人材の不足が挙げられている。あらゆる分野においてグローバル化が進んだ社会において、日本の情報セキュリティ人材もグローバル化に対応していくことが求められるということである。

最後に、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

しまっていると指摘された。

（２）基本的な考え方

現状と課題を踏まえ、政府として推進すべき人材育成に関する基本方針として、「ハイブリッド型人材」、「問題発見・解決型人材」の育成・確保、情報セキュリティ人材育成環境の整備、産学連携の強化、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、グローバル化に対応できる人材の育成の五つが示された。



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）

（３）具体的な取組

以上の考えに基づき、情報セキュリティ人材育成プログラムでは、具体的な取

組について提言されている。以下に主なものを挙げる。

先端的な情報セキュリティ研究者・技術者等の育成については、「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とされた。

政府機関における人材育成については、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とされた。

企業等における人材育成については、企業等の経営者の意識改革に資する取組として、企業等の経営トップ同士が様々な議論を行う場において意見交換を行うことが有意義であるとされるとともに、全社的な人材育成環境の整備に資する取組として、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キャリアパスの策定・普及の促進及びリカレント教育の実施が有効であるとされた。また、CIO及びCISOを組織内できちんと位置付けていくことが重要であるとされた。

教育機関における人材育成については、大学・大学院教育の充実に資する取組として、「ISS Square」や「IT Keys」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とされるとともに、実務経験学習等実践的な教育の充実に資する取組としては、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こととされた。また、初等中等教育においては、学習指導要領の改訂により、情報セキュリティに関する教育を充実させたところであり、情報セキュリティの動向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とされるとともに、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とされた。

官民連携・産学連携の強化については、産学連携教育のマッチングの促進に資する取組として、国内外の企業等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とされた。実践的な教育体制の確立への協力促進として、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とされた。また、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とされた。

３．情報セキュリティ人材育成施策の課題及び具体施策提言について

専門委員会は、人材育成プログラムを踏まえ、情報セキュリティに関する人材のパターンを大きく四分類（企業等の情報セキュリティ担当者、政府機関のセキュリティ担当者、セキュリティ産業人材、先端的な研究者・技術者）し、必要となる施策を整理した。

これらに加え、全ての情報セキュリティ人材の基礎となる初等中等教育、大学の共通教育の充実や、産学連携の強化等の課題についても、必要な施策を整理している。

施策の整理に際しては､それぞれの人材育成に係る現状と課題を簡単に整理し、それを踏まえて、今後実施すべき施策を提言することとした。括弧内には各施策の責任府省庁を掲げてあり、複数の府省庁が記載されている場合には、それぞれが適切に連携して施策を推進することが期待される。

※情報セキュリティに関する人材の四分類

①企業等の情報セキュリティ担当者

企業等において、自分の組織を守るため、情報セキュリティの脅威に対する対策を講じる人材

②政府機関のセキュリティ担当者

政府機関において、自分の組織を守るため、情報セキュリティの脅威に対する対策を講じる人材

③セキュリティ産業人材

政府機関、企業等情報セキュリティ対策を実施する組織からの発注、委託等を受け、情報セキュリティに関する製品・サービス・ソリューション等をビジネスとして提供する企業等における人材

④先端的な研究者・技術者

情報セキュリティのために必要となる技術や製品､管理手法などについて、主に学術的な研究を目的とした研究者､あるいは先進的な製品の開発者など、我が国全体の情報セキュリティ対策をリードしていく人材

（1）企業等の情報セキュリティ担当者

（現状）

情報セキュリティの確保は、今や全ての企業等が自らの問題として対処すべき課題となっている。しかしながら、独立行政法人情報処理推進機構の調査に対しては、　　（公表後記載予定）が情報セキュリティ対策の人材数若しくはスキル又はその双方が不足していると回答するなど、企業等における情報セキュリティ人材の確保は進んでいない。

今日、多くの企業等の情報システムはそれぞれの企業業務と密接に結び付いた独自の構成となっている。これらのシステムの構築は専門事業者に委ねられることになるが、業務の細部まで情報システムが入り込んでいるため、その構築と運用に際しては当該企業等の実務に精通した者の関与が不可欠である。また、とりわけ緊急時にはシステム上のリスクと経営上のリスクを俯瞰して判断を迫られるなど、情報システムの運用全てについて専門事業者に任せることはできない。

また、これらの情報システムの運用に際しては、システムの機能のみで情報セキュリティを確保することはできない。情報システムを利用する社員一人ひとりが情報セキュリティを適切に確保するよう、社内での情報取扱いに係るルールを定めるとともに、必要な教育訓練を行う等の組織的対応が必要となっている。

このような状況の下、企業等においては、①情報システム部門等において、技術的なセキュリティ対策を理解しシステム管理等を行うスペシャリスト人材と、②総務部門等において、情報セキュリティポリシー策定や情報セキュリティ監査を行う人材等の育成確保が必要となっている。

情報システム管理者等のスペシャリストについては一定の深い知識を、また、総務部門等人材については、関連する一定水準以上の知識等をそれぞれ保有している必要がある。このため、いずれの人材についても専門知識等が必要となり、専門知識を持った者を採用するか、採用後に社内において人材を育成することが不可欠となっている。

これら情報セキュリティ人材の育成においては、経営者層の理解が重要である。情報セキュリティは費用対効果が必ずしも明確ではない。加えて、情報セ

キュリティの内容そのものが、専門家ではない経営者にはわかりにくい場合が多い。その結果、人材育成を含む情報セキュリティへの投資が他の経営上の投資に劣後し、十分に行われないことが多い。情報セキュリティ人材の育成を推進するに当たっては、企業経営層等における情報セキュリティへの理解を促進する必要がある。

なお、規模が小さく、セキュリティ上重要な情報を有していないような企業等については､大企業と同程度の対策を実施することは困難であることが多い。中小企業に対しては、このような事情を踏まえた配慮が必要である。

① 情報セキュリティ専門家を目指す者の支援

（横断的キャリアパス・モデルの提示等）

情報セキュリティ人材不足の一つの要因として、情報セキュリティの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いことがあげられる。専門家としての将来の発展性、安定性等の見通しは、職業選択上多くの者が考慮するところであるが、事例も少なく、なかなか実態が分かりにくい。

このような不安を少しでも払拭するために、企業等に採用された場合のキャリアパスを中心に、転職を通じてキャリアアップを図るケースや、学界におけるキャリアパス等も含め、モデルとなる横断的キャリアパスを提示することが望ましい。

独立行政法人情報処理推進機構では､2011 年度中を目途に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・モデルを策定することとしている。事例数に限りはあるものの具体例を積み重ねたものであり、専門家を目指す者や②に示す人材育成計画を策定する企業等の参考になるものと考えられる。

＜今後実施すべき施策＞

〇横断的キャリアパス・モデルの策定及び普及

キャリアパス・モデルの策定は、企業等における情報セキュリティ人材不足の解消に資する。横断的キャリアパス・モデルを策定し、普及に努める。

・独立行政法人情報処理推進機構が策定した情報セキュリティ人材のキャリアパス・モデルの普及に努める（経済産業省）。

② 企業等における情報セキュリティ人材育成の支援

（人材育成計画の策定）

企業等において、情報セキュリティ人材を採用・育成するためには、当該企業等が必要とする情報セキュリティ人材の姿とその将来像をある程度明確化することが望まれる。これにより効果的な人材育成が可能になるとともに、応募しようとする者に将来の処遇期待を示すことができる。

そのような過程を整理したものを「人材育成計画」と呼ぶ。人材育成計画においては、当該企業等が求める役職ごとの人材像、それぞれの段階で取得すべき資格、予定される研修やリカレント教育、経理や営業といった他の部門との行き来を含むキャリアパス、中期的な処遇見通し等について、具体的に定められていることが望ましい。

企業等の情報システムは個々の企業等の業務と密接に結びついていることから、人材育成計画についても、個々の企業等がその業務等を踏まえて策定すべきものである。他方、人材育成過程で習得させるべき情報セキュリティ関連知識・技能やその習得順序等には、企業等の業務内容に係らず共通するものも多い。したがって、情報セキュリティに係る知識・技能とそれに関連する資格・教育プログラムを整理したものや、これらを踏まえた人材育成計画の「モデルプラン」があれば、人材育成計画を作成しようとする企業等の参考になると考えられる。

＜今後実施すべき施策＞

〇人材育成計画策定促進

企業等における「人材育成計画」の策定に資する情報を提供し、効果的な情報セキュリティ人材の育成や採用を促進する。

・独立行政法人情報処理推進機構が策定した情報セキュリティ人材のキャリアパス・モデルの普及に努めること等により、企業等における人材育成計画の策定を促進する（経済産業省、関係府省庁）。

〇スキル、資格、教育プログラム等の整理

・情報セキュリティ関連業務で求められるスキルと関連する資格、教育プログラムを整理して公表する（総務省、経済産業省）。

（多様な教育機会の提供）

情報セキュリティ人材の育成に際しては、情報セキュリティ関連技術が日々急速に進歩していること、及び、とりわけインシデント対応において、一面的な知識や技能ではなく、総合的な判断能力が求められることを踏まえる必要がある。このため、情報セキュリティ人材の育成に際しては、OJT や企業内研修等にとどまらず、幅広い教育機会が提供されることが望ましい。

急速に進歩する技術への十分な対応を可能とするためには日頃の継続的な学習が不可欠であるが､加えて体系的な学習の機会が与えられることが望ましい。例えば、一定の勤務経験の後、大学院等で集中的なリカレント教育が行われることは有効と考えられる。

また、情報セキュリティインシデントに係る実践的な経験の幅を広げる機会が提供されることが望ましい。情報セキュリティに関連する国の機関等は、優秀な人材に最先端の経験を提供させる機会を設けることが望まれる。

2006 年度～2010 年度に実施された「先導的 IT スペシャリスト推進プログラム」では､IT 企業の技術者等が社会人学生として受け入れられた(「ISS Square」では 2010 年度の修了者 45 名のうち 14 名が社会人)。受入数は限られていたものの、その成果には高い評価も得られており、リカレント教育の一つのあり方を示したものと考えられる。

＜今後実施すべき施策＞

〇リカレント教育の促進

情報セキュリティを体系的・集中的に学習するためのリカレント教育の取組を推進する。

・高等教育機関等における社会人学生の受け入れを支援する（文部科学省）。

〇政府機関等による民間セキュリティ人材の一時的受入

政府機関や独立行政法人等において民間セキュリティ人材を一定期間受入れ、情報セキュリティ人材の育成と人材ネットワークの形成を図る。

・政府機関や独立行政法人等がハブとなり産学官のセキュリティ関連業務を交互に経験できる機会を設けることなどにより、幅広いネットワークの形成を図り、情報セキュリティ人材を育成する（関係府省庁）。

（資格要件の設定）

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は、当該企業等のみの問題ではない。このため、2012 年 1 月 24 日、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」においては、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おり、「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若しく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。

このように、情報セキュリティ対策に携わる者に一定の資格要件を設定することは、重要な情報に係る情報セキュリティの確保に資するとともに、企業等における人材育成の目標を設定することにもなる。

情報セキュリティ政策会議に報告された「情報セキュリティ対策に関する官

民連携の在り方について」(2012 年 1 月 19 日　官民連携の強化のための分科会決定）においては、国と調達契約を結んでいない、あるいは調達契約の及ばない「国の安全に関する重要な情報を扱う企業等」に対しても同様の取組方策を検討することとされている。

これらの企業等における取り組みは、情報セキュリティを学んだ人材が活躍する場の拡大に寄与する取組であるため、今後の検討が望まれる。

＜今後実施すべき施策＞

〇資格要件の設定

国の安全に関する重要な情報を扱う調達の情報セキュリティ要件に基づき整備される体制における実務担当者に対し、継続して新たな知識の補充を行うための継続教育のあり方や実効性の確保方策について検討する。

・国の契約相手方の情報セキュリティを確保するための体制における実務担当者について、継続して新たな知識の補充を行うための実効的な方策について検討する（内閣官房、関係府省庁）。

国と調達契約を結んでいない、あるいは調達契約の及ばない「国の安全に関する重要な情報を扱う企業等」に対し、国の安全に関する重要な情報を扱うことを含む契約を締結する企業等に対し求める情報セキュリティ要件と同様の取組を促す方策について、実情も勘案の上、検討を行う。

・調達契約を結んでいない、あるいは調達契約の及ばない「国の安全に関する重要な情報を扱う企業等」に対する情報セキュリティの確保方策について検討を行う（内閣官房、関係府省庁）。

③ 企業経営層への情報提供等

企業等における情報セキュリティ向上のためには、経営層が自社における情報セキュリティ対策の重要性を認識し、これを全社的に推進していくことが望まれる。情報セキュリティは専門的との意識を持つ経営層も多いが、それゆえ、その重要性を経営層が理解しないと必要な投資が行われなくなる。情報セキュリティ人材の育成推進の観点からも、企業経営層等における情報セキュリティへの理解を促進する必要がある。

また、企業等は自社自身の情報セキュリティだけでなく、自社のサービス利用者の情報セキュリティにも深く意を払わなければならない。近年、新たに開発される多様な情報通信サービスの中には、利用者のプライバシーや情報セキュリティに対する配慮が行き届かないものも見受けられる。経営層は、自社が提供するサービスの利用者に対する情報セキュリティの確保についても、理解を深める必要がある。

企業等において情報セキュリティの水準をどの水準に設定するかは、本来、企業等の経営上の問題である。すなわち、高度なセキュリティ水準を確保し、顧客からの信頼や自社の情報の安全を高めるか、異なる選択を行うかは、経営層が決めることである。しかしながら、企業経営層等が、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意思決定することは、適切ではない。企業経営層等に関連する情報を提供し、適切な判断が行われるよう努める必要がある。

（企業経営層等への情報提供）

企業経営層等における情報セキュリティに関する認識を高めるためには、あらゆる機会をとらえて、企業経営層等に訴えかけていく他ない。とりわけ、我が国の企業の大半を占める中小企業の経営層への訴えかけを重点的に進めることが重要である。

経済産業省では「情報セキュリティガバナンス導入ガイドライン」（2009 年 6 月 30 日）を公表するなどして、企業経営層等が責任とリーダーシップを持って情報セキュリティ対策を推進するよう取り組んでいる。また、企業等の経営層同士が情報セキュリティに関する様々な意見を交換できる場として、「情報セキュリティガバナンス協議会」（2012 年４月設立予定）の活動を支援するとともに、中小企業向け情報セキュリティ指導者育成セミナーを開催（全国 25 か所（各会場 30～80 名程度）（2011 年度））している。この他、内閣官房や関係省庁職員が、経済団体等が主催する会議等において積極的に講演するなどして情報発信している。

このように取組が重ねられてはいるが、必ずしも十分とは言える状況にない。企業経営層等に必要な情報を提供し理解を得る取組には際限がないが、地道な

努力を続けることが重要である。

企業経営層等への働きかけに際しては、人材育成計画の策定、産学連携等を通じたセキュリティ人材の確保・育成が重要であることを訴えかけることが重要である。また、企業等の内に情報セキュリティの責任者（CISO 等）を設置し、当該組織の情報セキュリティに係る司令塔として機能させること、サイバー攻撃や標的型攻撃メールを想定した訓練を行うことなど、具体的な情報セキュリティ対策に関する推進方策に言及することが望ましい。

なお、例えば、情報システム関連部門では情報セキュリティに強い学生の採用を希望しているにも関わらず、実際の求人に反映されていない場合があることを踏まえ、企業経営者等への働きかけとともに、人事担当、採用担当にも働きかけることが望ましい。

情報セキュリティ対策が経営上の重要課題となっていることから、経営学修士課程等における情報セキュリティ関連講義の開設、情報セキュリティに関する研究科の設置、「情報セキュリティ技術経営」等の学位授与等を検討する動きがある。このような取組の促進を図るとともに、企業経営層等に対して、これらの関連情報についても提供していくことが望ましい。

＜今後実施すべき施策＞

〇経営層向けセミナーの開催等

情報セキュリティ対策の重要性、情報セキュリティ人材育成の重要性、産学連携による人材育成の取組状況、情報セキュリティに関する研究科や学位に関する大学の取組状況等について、企業等の経営層・人事担当・採用担当の理解を深めるべく、経営層向けセミナー等を開催するとともに、経済団体等が主催する会議も活用するなど、あらゆる機会をとらえて普及啓発を行う。

・企業等の経営層、人事担当、採用担当等を対象としたセミナー等を開催するとともに、経済団体等が主催する会議も活用するなど、あらゆる機会をとらえて普及啓発を行う（内閣官房、総務省、経済産業省、文部科学省）。

・「情報セキュリティガバナンス協議会」の活動を支援する（経済産業省）。

〇セミナーの実施

中小企業の経営層や情報セキュリティ指導者向けに、わかりやすい情報セキュリティ対策を提示する。

・中小企業向け情報セキュリティ指導者セミナーを引き続き開催する（経済産業省）。

〇表彰等の実施

企業等の経営層の意識改革のためには、人材育成計画や産学連携などについて優れた取組を行っている企業等を表彰することによってインセンティブを与える。

・情報セキュリティ確保の観点から、優れた取組を行っている企業等について引き続き表彰する（総務省）。

〇CISO 等の設置促進

情報セキュリティ対策を推進する上で重要な役割を果たす CISO に求められる役割・能力を整理し、企業等の理解を深めるとともに設置を促進する。CISO が設置されておらず、CIO、CRO が設置されている企業等には、これらの役職の者による CISO の兼務や、CISO の新設を促進する。

・情報セキュリティを推進する観点から、CISO に求められる役割・能力を整理し、CISO の設置の普及等に努める（経済産業省）。

（体制整備の確保）

国の安全に関する重要な情報を扱う企業等については、「調達における情報セキュリティ要件の記載について」において、各府省庁が契約を締結する際には、契約の相手先に情報セキュリティを確保するための体制整備と経営者責任の明確化を求めることとされている。企業等における取組を加速する上で、このように要件を課すことは有効である。

情報セキュリティ政策会議に報告された「情報セキュリティ対策に関する官民連携の在り方について」（2012 年 1 月 19 日）においては、国と調達契約を結んでいない、あるいは調達契約の及ばない「国の安全に関する重要な情報を扱う企業等」に対する同様の取組方策を検討することとされている。

このような取り組みは、情報セキュリティを学んだ人材が活躍する場の拡大

に寄与する取組であるため、今後の検討が望まれる。

＜今後実施すべき施策＞

〇体制整備の確保

国と調達契約を結んでいない、あるいは調達契約の及ばない「国の安全に関する重要な情報を扱う企業等」に対し、国の安全に関する重要な情報を扱うことを含む契約を締結する企業等に対し求める情報セキュリティ要件と同様の取組を促す方策について、実情も勘案の上、検討を行う。

・調達契約を結んでいない、あるいは調達契約の及ばない「国の安全に関する重要な情報を扱う企業等」に対する情報セキュリティの確保方策について検討を行う（内閣官房、関係府省庁）。

（２）政府機関等の情報セキュリティ担当者

（現状）

政府においては、各機関が守るべき情報セキュリティ水準を統一基準群として示し、これに準拠する取組を各府省庁が CISO のもとで実施している。各府省庁の CISO は官房長等が充てられているが、これをサポートする人材として、最高情報セキュリティアドバイザーが置かれ、平常時はもちろん、緊急時に的確な対処が行われるようにしている。

システムの運用は必ずしも専門家が充てられず、通常の人事ローテーションの中で２～３年周期で交代することが多い。情報セキュリティに関して全くの素人が着任する場合もある。とりわけ規模の小さい組織の場合、情報セキュリティ担当が一名であったり、他の業務を兼務したりしている場合がある。このように、専門的な能力の獲得が不十分となったり、業務上の重要な情報が引き継がれなかったりする恐れがある。

昨今の情報セキュリティ上のリスクの高まりを受け、政府では各府省庁の危機管理能力の向上に努めることとし、体制の強化を図っている。まずは、各府省庁が情報セキュリティに係る危機発生時において機動的に対処するための機能（以下「組織内 CSIRT 等」という。）を保有するとともに、これを補完すべく危機発生時に府省庁の壁を越えて機動的に支援できるサイバーインシデント版の DMAT（Disaster Medical Assistant Team 災害急性期に活動できる機動性をもったトレーニングを受けた医療チーム）（以下「サイバーインシデント版の DMAT」という。）を編成し、これを有効活用することが必要であると思われる。

情報セキュリティは、システム担当者の努力のみで確保できるものではない。政府の情報システムを利用する全職員が基本的な情報セキュリティに関する知識を獲得する必要がある。

このため、政府では多様な訓練等を実施しているが、これらを継続し充実させていくことが不可欠である。

また、国に準じた情報セキュリティの確保が求められる重要インフラ事業者においても、積極的な情報セキュリティ人材の育成が行われることが重要である。

① 組織内 CSIRT 等の設置、サイバーインシデント版の DMAT の育成

まずは各府省庁において組織内 CSIRT 等を整備するなどして、標的型攻撃等に関する対策を遺漏なく継続的に実施するとともに、サイバーインシデント版の DMAT を立ち上げ、必要な人材を育成することが重要である。

＜今後実施すべき施策＞

〇CSIRT 要員の育成等

各府省庁において組織内 CSIRT 等を整備すべく要員を育成する。

・CSIRT 等の要員に求められる知識・技能を有する人材を育成するため、能力に応じた段階的かつ計画的な研修プログラムの制度設計の構築を行う（内閣官房）。

〇サイバーインシデント版の DMAT の育成

CSIRT 等の要員の確保が困難な府省庁や、大規模なインシデント等により政府として迅速かつ的確に対応すべき事態が発生した際に、他の府省庁の CSIRT 等の要員による支援を可能とするサイバーインシデント版の DMAT の設立及びその要員の育成について検討を行う。

・サイバーインシデント版の DMAT の設置に向け、府省庁間の協力のルール作り、内閣官房情報セキュリティセンターの調整機能の整備、その要員の育成について検討を行う（内閣官房）。

② 情報セキュリティリスクに確実に対応できる職員の採用・育成

現在、各府省庁においては、政府機関の情報セキュリティ対策のための統一基準群に基づき、最高情報セキュリティアドバイザーを設置し、情報セキュリティに関する専門的な見地からの助言等を行っている。しかしながら、昨今の情報セキュリティ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、情報セキュリティ担当者については、今後、採用及び人事ローテーションにおいて特別の配慮を行うことが望ましい。具体的には、職員採用後の人事ローテーションにおいて、特定の者には長い期間情報セキュリティを担

当することでその能力を向上させるなどの工夫が必要と考えられる。

その際、特定の府省庁で継続的に業務に当たるのではなく、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、①のサイバーインシデント版の DMAT 立ち上げと相まって政府一体となった情報セキュリティ確保体制の構築を進めることが望ましい。また、独立行政法人等においてより専門的な業務に携わることで能力の開発向上を図るとともに、情報セキュリティ関係者間の人的ネットワークを構築することが望ましい。

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も図られるべきである。

なお、情報セキュリティに携わる人材の採用等に際しては、扱われる情報の重要性やシステムリスクを踏まえたセキュリティの確保にも配慮することが重要である。

＜今後実施すべき施策＞

〇人事ローテーションの工夫

・各府省庁等の情報セキュリティ担当部署と内閣官房情報セキュリティセンターで人事交流を行うなど、職員の希望も踏まえつつ、情報セキュリティ担当者が長い間情報セキュリティに係る業務に携われるよう、人事ローテーションの工夫を検討する（関係府省庁）。

〇優秀な外部人材の活用

・官民の人事交流等により情報セキュリティに係る外部人材を活用する人事のあり方を検討する（関係府省庁）。

〇政府機関や独立行政法人等をハブとしたセキュリティ人材のネットワーク形成

・政府機関や独立行政法人等がハブとなり産学官のセキュリティ関連業務を交互に経験できる機会を設けることなどにより、幅広いネットワークの形成を図り、情報セキュリティ人材を育成する（関係府省庁）。

③ 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

情報セキュリティ向上に際しては、システムや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向上が必要である。そのため、採用時において情報セキュリティについての素養を確認することや、採用後には常に研修・訓練を実施していくことが必要である。

現在、警察庁、防衛省等において、高度な情報セキュリティ人材の育成に向けた訓練が実施されている。また、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、標的型不審メール攻撃訓練を実施するなど、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。各府省等は、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。このような訓練等を発展継続することが重要である。

また､国家公務員には情報セキュリティに関する素養が必要であることから、公務員採用時において、情報セキュリティに関する素養を確認することも効果的と考えられる。

＜今後実施すべき施策＞

〇訓練・研修の充実

政府機関を取り巻く状況や研修効果等を踏まえた訓練･研修の充実強化を図る。

・本年度の訓練結果等を踏まえてプログラムの充実を図る等し、職員教育や対処訓練を実施する（内閣官房）。

・政府職員に対する採用時の合同研修において情報セキュリティに係る内容を盛り込むなど教育機会の付与に努める（内閣官房､人事院）。

〇公務員採用時における情報セキュリティ関連素養の確認

・国家公務員採用に際して情報セキュリティに関する素養の確認に努めるよう、関係府省庁に対し要請する（内閣官房）。

④ 重要インフラ事業者における人材育成促進

重要インフラとは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活・社会経済活動の基盤であり、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。

このため、重要インフラ事業者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、関係省庁が取組むべき対策等を「第二次行動計画」(2009 年 2 月 3 日）としてとりまとめその推進を図っている。その中で、人材育成については、内閣官房が「分野横断的演習等を通じた、高度な情報セキュリティ人材の育成」に取り組むこととされている。

今後、重要インフラ事業者において、より積極的に人材育成が図られることが望ましい。（１）②（企業等における情報セキュリティ人材育成の支援）に掲げられた施策はもとより、（２）①（組織内 CSIRT 等の設置)、②（情報セキュリティリスクに確実に対応できる職員の採用・育成)、③（職員の情報セキュリティ意識の啓発と能力の底上げ）に掲げられた施策に準じた取組や、各セプター内で横断的に実施する研修プログラムの検討等が推進されることが望ましく、政府は積極的な支援・助言を行うべきである。

＜今後実施すべき施策＞

〇重要インフラ事業者における人材育成の促進

・重要インフラ事業者において、組織内 CSIRT 等の設置、情報セキュリティリスクに確実に対応できる職員の採用・育成、職員の情報セキュリティ意識の啓発と能力の底上げ等、政府に準じた取組を推進する（内閣官房、関係府省庁）。

・各セプター内で横断的に実施する研修プログラムを検討する（内閣官房、関係府省庁）。

〇人材育成計画策定促進

〇スキル、資格、教育プログラム等の整理

〇リカレント教育の促進

〇政府機関等による民間セキュリティ人材の一時的受入

（３）情報セキュリティ産業人材

（現状）

企業や政府機関等における情報セキュリティ対策は、情報セキュリティサービスやソリューション等を提供するセキュリティ産業なくして成り立たない。また、国家安全保障確保の観点からも、情報セキュリティ産業は極めて重要である。情報セキュリティ確保に係る企業等の関心が高まりセキュリティ産業への需要が増加する中、当該産業における人材の育成が急務である。

しかしながら、セキュリティ産業を職業として選択した場合、どのようなキャリアパスが存在するのかが必ずしも明らかでない。このため、将来への不安感もあり当該分野に十分な数の優秀な人材が集まっていない。

また、セキュリティ産業を支える人材を輩出すべき高等教育機関も、十分な体制がとられていない。一つの大学で情報セキュリティの専門家を育成するために必要な全ての単位を提供できる機関は限られている。

セキュリティ産業といっても、セキュリティ・サービス・プロバイダ、システム・インテグレータ、セキュリティ監査等とその領域は多様であり、求められる人材もそれぞれの領域により異なっている。いずれにおいても、まずは特定領域の専門家として自立できる人材を育成することとなるが、中期的には複数の要因を統合し、これらをモデル化して判断できる能力も重要になる。

このように専門家として高い能力が求められる情報セキュリティ産業人材の育成に際しては、多様な経験が必要であり、一企業等を超えた人材育成措置が必要となっている。

これらに加え、セキュリティ産業人材には、その職に適したセンスのようなものが必要であり、これを見出すことが求められる。現状、我が国においてはそのような機会は必ずしも多く設けられていない。

① 企業等における人材の育成支援

セキュリティ産業人材の育成についても、企業等のセキュリティ担当者と同様、キャリアパス・モデルの策定、人材育成計画の策定、スキル、資格、教育

プログラムの関係の整理が重要である。また、リカレント教育も重要である。

多様な経験としては、例えば、複数の企業が相互に一定期間情報セキュリティ人材を出向させ合う等、企業間の人材交流が行われることが考えられる。また、内閣官房情報セキュリティセンター、独立行政法人情報通信研究機構、独立行政法人産業技術総合研究所、独立行政法人情報処理推進機構等が優秀な人材受け入れ、人材育成を進めることが考えられる。継続的に実施することで、これらの機関に産官学の優秀な人材が集結し、人材を輩出することが期待される。

＜今後実施すべき施策＞

〇キャリアパス・モデルの普及、人材育成計画策定促進

セキュリティ人材の確保のため、キャリアパス・モデルを示しその普及に努める。企業等における人材育成計画策定を促進する。

・独立行政法人情報処理推進機構が策定した情報セキュリティ人材のキャリアパス・モデルの普及に努めること等により、企業等における人材育成計画の策定を促進する（経済産業省、関係府省庁）。

〇スキル、資格、教育プログラムの整理

企業等における人材育成計画策定、効率的人材育成、適材適所における人材配置等の促進のため、様々な業務で求められるスキルとそれに関連する資格・教育プログラムを整理する。

・情報セキュリティ関連業務で求められるスキルと関連する資格、教育プログラムを整理して公表する（総務省、経済産業省）。

〇リカレント教育の促進

社会人が専門的知識を深めることに資するようなリカレント教育の取組を充実する。

・高等教育機関等における社会人学生の受け入れを支援する（文部科学省）。

〇内閣官房情報セキュリティセンターや独立行政法人等を活用した人材育成

内閣官房情報セキュリティセンターや独立行政法人等に産官学の優秀な人材を結集させ、優秀な人材を輩出する中心的な役割を果たす方策を検討する。

・内閣官房情報セキュリティセンター、独立行政法人情報通信研究機構、独立行政法人産業技術総合研究所、独立行政法人情報処理推進機構が優秀な人材を輩出する中心的機能を果たすことを目標として、関係機関との連携を強化するための連絡会を開催する（内閣官房、総務省、経済産業省）。

② 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大学・大学院教育の強化

セキュリティ産業人材には、高度で幅広い知識や特殊な能力が求められる。大学・大学院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大学・大学院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、産学連携も合わせ進めることが望ましい。

文部科学省の「先導的 IT スペシャリスト推進プログラム」においては、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、複数大学や産業界の連携協力による教育が実施されるとともに、教育カリキュラムや教材の開発が進められてきた。同プログラムは着実に実績を残しており、このような事業の継続と拡大が望まれる。

また、前述した情報セキュリティに関する研究科等を設置する取組は企業等へ即戦力を供給する取組として有効と考えられる。情報セキュリティに関する研究科等の設置や講座の拡大は、大学の自主的な判断に基づき行われるものであるが、今後、大学・大学院におけるこれらの教育体制が充実することを期待する。

＜今後実施すべき施策＞

〇複数大学や産業界の連携協力による大学・大学院教育

複数の大学や産業界が連携協力した教育の継続及びその成果の全国的展開を支援する。

・複数大学や産学連携による高度で実践的な教育活動の支援を行う

（文部科学省）。

〇情報セキュリティに関する研究科等

情報セキュリティに関する研究科等が設置されることを推進する。

・情報セキュリティに関する研究科等の設置に資するよう、情報セキュリティに関する最新の情報を大学等に対し積極的に提供する（内閣官房、総務省、経済産業省、文部科学省）。

③ 優秀な人材の発掘及び更なる能力向上

セキュリティ産業において最先端の分野で活躍する人材には、教育では得られない特殊な能力を持っていることが求められると言われている。このような人材の発掘及び更なる能力向上のための取組も重要である。

現在、独立行政法人情報処理推進機構において、将来の IT 産業を担う若年層に対し、情報セキュリティを中心として IT 化実現のための技術的な目標と高い技術習得への励み、及び安全かつ信頼性の高い IT 化の進展について正しい知識を与えることを目的にセキュリティ＆プログラミングキャンプを実施している。また、ソフトウェア関連分野において、独創的なアイディア、技術を有し、これらを活用していく能力を有する優れた個人を発掘育成する「未踏 IT 人材発掘・育成事業」を実施している。優秀な人材の確保及び能力向上のためには、このようなインセンティブを与える取組を行うことが引き続き重要と考えられる。

このような教育的なプログラムに加え、コンテストなどの仕組みを通じた人材発掘も有効と考えられる。情報セキュリティを守ることの重要性を指導しつつ必要な能力の開発や人材の発掘を行う方法を検討する必要がある。

＜今後実施すべき施策＞

〇表彰等の実施

優秀な人材を発掘し、更なる能力向上を図る。

・セキュリティキャンプについて、更なる充実を図る（経済産業省）。

・「未踏 IT 人材発掘・育成事業」を引き続き実施する（経済産業省）。

・情報セキュリティ確保の観点から多大な貢献を果たした個人・企業等を表彰する（総務省、経済産業省）。

コンテスト開催等により人材を発掘する。

・情報セキュリティ人材が実践的技能を競えるような競技会等の開催について検討する（総務省、経済産業省）。

・競技会等において優秀な成績を残した者の雇用促進につながる普及啓発について検討する（総務省、経済産業省）。

（４）先端的な研究者・技術者

（現状）

先端的な研究開発能力の確保は、情報セキュリティ分野における我が国の国際的な産業競争力確保において不可欠であり、また、国家安全保障とも結びつく重要課題である。

しかしながら、市場に流通している情報セキュリティ関連製品の大部分が海外製であるなど、この分野における我が国の国際競争力は高くない。また、その結果として、国家の重要システムにも外国製品を使わざるを得ず、国家安全保障上の課題もある。

先端的な研究者・技術者の育成に際しては、専門課程における基礎教育の充実と、発展的研究を支える研究開発環境が不可欠であり、これらの充実を図る必要がある。

また、先端的な研究者は先端的な研究者に育てられるという。高度な情報セキュリティの専門家が集い、意見交換・切磋琢磨できるコミュニティが形成されることが望ましい。

① 情報セキュリティ研究開発の推進

情報セキュリティに係る先端的な研究者・技術者を育成すべく情報セキュリティ分野への研究開発資金の重点的配分を促す際には、中長期的に我が国全体として情報セキュリティに関する研究開発をどのように進めていくかについての計画を定め、それを国全体として戦略的に推進していく中で、人材を育成していく必要がある。

情報セキュリティ政策会議は、2011 年度～2015 年度を対象とした「情報セキュリティ研究開発戦略」（2011 年７月８日）を策定した。研究開発戦略では、四つの重要分野における 12 テーマ及び東日本大震災を踏まえた四つの重点分野を掲げており、これらについて研究開発を推進する中で先端的研究者・技術者の育成を図ることが適切である。

引き続き「情報セキュリティ研究開発戦略」に沿った研究開発を着実に推進

することにより、先端的研究者・技術者の育成を進めていくことが重要である。

＜今後実施すべき施策＞
〇研究開発戦略の推進
・「情報セキュリティ研究開発戦略」に沿った研究開発を引き続き着実に推進することにより、先端的研究者・技術者の育成を進める（内閣官房、総務省、経済産業省、文部科学省、防衛省）。

② 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大学・大学院教育の強化等

専門課程における基礎教育の充実に係る課題は（３）②の「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大学・大学院教育の強化」で述べた課題と共通している。（３）②で提言した、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大学・大学院教育の強化、優秀な人材の発掘及び更なる能力向上のためのインセンティブ措置に関する取り組みについて、先端的な研究者・技術者を育成という観点から推進していくことが重要である。

＜今後実施すべき施策＞
〇複数大学や産業界の連携協力による大学・大学院教育
〇情報セキュリティに関する研究科等

③ 産学官の人材交流と高度な人材に係るコミュニティの形成

高度な情報セキュリティ人材は、先端的な技術とそれを適用する複雑な現実システムの双方を理解できる必要がある。このため、高度な情報セキュリティ人材の育成に際しては、産学官の最先端の分野で情報セキュリティに関する様々な業務を経験することが望ましい。

これらの人材が、産学官の主要な機関で経験を積むことができるよう、内閣官房や独立行政法人が場を提供し、合わせて高度な情報セキュリティ人材の健全なコミュニティが形成されるよう配意する。

＜今後実施すべき施策＞

〇内閣官房情報セキュリティセンターや独立行政法人等を活用した人材育成

内閣官房情報セキュリティセンターや独立行政法人等に産官学の優秀な人材を結集させ、優秀な人材を輩出する中心的な役割を果たす。

・内閣官房情報セキュリティセンター、独立行政法人情報通信研究機構、独立行政法人産業技術総合研究所、独立行政法人情報処理推進機構が優秀な人材を輩出する中心的機能を果たすことを目標として、関係機関との連携を強化するための連絡会を開催する（内閣官房、総務省、経済産業省）。

④ グローバルに活躍できる人材の育成

情報セキュリティの課題はネットワークでつながった国際的課題であり、先端的研究の推進には国際的な視点を持った人材が必要である。

グローバルな視点で物事を考えられるような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をする必要がある。国際会議への参加や留学を支援するとともに、我が国への国際会議招致を推進することも有効と考えられる。

＜今後実施すべき施策＞

〇国際会議への参加支援等

・国際会議への参加支援や我が国への国際会議招致を推進し、グローバルに活躍できる人材の育成を行う（関係府省庁）。

（５）人材類型を跨ぐ横断的課題等

（５－１）情報セキュリティ人材の基礎的資質を育成する教育の充実

（現状）

情報化が進んだ現代社会においては、あらゆる世代においてコンピュータやスマートフォンといった情報通信機器の利用が進展している。小学生が家庭でこれらの機器を利用することも珍しくなく、初等中等教育段階から、その利活用に係る知識とともに、自らを守る最低限の情報セキュリティの知識を授け実践させることが求められている。

また、企業実務等においても一層複雑・大規模な情報通信システムが幅広く使用されており、情報セキュリティに関する基礎知識は、その利活用に係る知識と相まって、いまや社会人には必須のものとなっている。

このため、初等中等教育において、情報セキュリティの教育を充実していく必要がある。また、大学においても、各大学の自主的な判断により、共通教育・教養教育の中で、情報セキュリティに関する教育を受ける機会が確保されることが期待される。

① 初等中等教育段階における情報セキュリティに関する教育の充実等

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、2009 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、情報及び情報技術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推進する。

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、指導に当たる

教員の能力が十分である必要がある。そのためには、各都道府県及び指定都市等の主として情報教育担当の指導主事を通じて、教員一人ひとりが情報セキュリティに関する指導力の向上に努める必要がある。

また、大学入学志願者の情報科に関する基礎的な学習の達成の程度の判定や、初等中等教育において情報セキュリティに関する教育・学習の充実を促すためには、例えば、高等学校における情報科の教育内容の実態等を十分に見極めつつ、大学入学志願者の約７割が受験する大学入試センター試験において、情報科を出題教科とすることについて、大学及び高等学校関係者等の意見を十分に聴取しながら、検討することが望ましい。

＜今後実施すべき施策＞

〇初等中等教育段階における情報に関する教育

・学習指導要領の改訂等を踏まえ、発達段階に応じ、情報セキュリティを含む情報モラルに関する教育を積極的に推進する（文部科学省）。

〇初等中等教育における教員等の ICT 活用指導力の向上等

・初等中等教育に携わる全ての教員並びに教育委員会及び学校の全ての管理職等の情報セキュリティに関する基本的な知識を含む ICT 活用指導力の向上を目指した取組が地方公共団体等において進められるよう、各地域で情報教育を推進する中核的な役割を担う指導主事、リーダー的教員等を対象とした研修や指導方法等に関する情報交換の機会の提供等を検討する（文部科学省）。

〇大学入試センター試験における情報科の出題に係る検討

高等学校の必履修教科である情報科について、大学入試センターが出題教科とすることを検討するよう大学入試センターに要請する。

・高等学校の教育の実態や大学及び高等学校関係者の意見を踏まえながら、大学入試センター試験において情報科を出題教科とすることについて検討するよう大学入試センターに要請する（文部科学省）。

② 大学の共通教育・教養教育における情報セキュリティに関する教育の充実等

大学の共通教育・教養教育では、各大学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、現状、その数は多くない。その理由は必ずしも明確でないが、大学の共通教育・教養教育の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低いことに加え、そもそも教えられる教員がいないこと等があげられている。

大学の共通教育・教養教育における情報セキュリティに関する教育の重要性を踏まえ、各大学において情報セキュリティに関する教育が実施されるよう、努める必要がある。例えば情報セキュリティに関する最新動向を大学に情報提供することにより、認識を高める試みが考えられる。

情報セキュリティを教えることができる教員が存在しない場合、資格試験合格によって単位を認定することが考えられる。例えば、独立行政法人情報処理推進機構の認定資格である IT パスポート試験の合格により単位を認定している大学（約 30 校）や CompTIA の情報セキュリティに関する認定資格プログラム合格によって単位を認定している大学等（約 15 校）があり、このような情報も併せ提供することが考えられる。

また、情報セキュリティ対策が経営上の重要課題となっていることから、経営学修士課程等における情報セキュリティ関連講義の開設等を検討する動きがある。このような取組についてもその促進を図ることが重要である。

＜今後実施すべき施策＞

〇情報セキュリティに関する最新情報の提供

大学における情報セキュリティに関する教育の実施に資するような情報セキュリティに関する最新情報を提供する。その一環として、大学の自主的な判断に基づく情報セキュリティに係る資格試験合格による単位認定の導入、資格に関する学習プログラムの導入、経営学修士課程等における情報セキュリティ関連講義の実施等の検討に資する情報を提供する。

・情報セキュリティに関する最新情報を大学等に対し積極的に提供する（内閣官房、総務省、経済産業省、文部科学省）。

（５－２）情報セキュリティの専門家育成のための共通課題

① 産学連携の強化

情報セキュリティの専門家には、体系的な知識を有するとともに、それを複雑な現実のシステムに適用できる実践力が求められる。このため、大学等における情報セキュリティに関する教育において、実践的な教育プログラムが提供されることが望ましい。

実践的な教育においては、企業人講師の活用やインターンシップの実施など、産学の連携が不可欠である。これまで、「先導的 IT スペシャリスト推進プログラム」及び「IT 人材育成強化加速事業」において、産業界から派遣された実務家教員が講義等を行うとともに、産業界から実践的なインターンシップの場が提供される等したが、このような取組が広がることが望ましい。

また、産業界と教育界が協力して作成された情報セキュリティに係る実践的教材が、国立情報学研究所（約 200 コンテンツ）及び独立行政法人情報処理推進機構（約 130 コース）において、データベース化・公開されている。このようなデータベースが拡充整備され、大学等で有効に活用されることが望ましい。

＜今後実施すべき施策＞

○情報セキュリティに関する教育における産学連携の促進

情報セキュリティに関する教育における産学連携を拡充・促進する。

・産学連携による実践的教育活動の実施を支援する（経済産業省、文部科学省）。

○インターンシップ及び PBL（Project Based Learning 課題解決型学習）等の推進

産学連携によるインターンシップや PBL の機会提供を促進する。

・産学連携により実践的教育を推進する体制の構築や、インターンシップや PBL の実施を支援する（文部科学省）。

・実践的インターンシップモデルに基づき、企業等と大学・学生のマッチングの支援を行う（経済産業省）。

○データベースの拡充及び活用促進

国立情報学研究所等が作成したデータベースの大学等における活用を促進する。

・産業界と教育界が協力して作成された授業や教材のデータベースを拡充するとともに、その利用促進を図る（経済産業省、文部科学省）。

② 情報セキュリティに関する事故事例等の有効活用

実践的な教育の一環として、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。高度な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水準を高めていく観点からは、これらが有効活用されることが望ましい。

事故事例等は企業等の社会的評価の低下に繋がる可能性や、セキュリティ確保の観点等から隠されることが多いが、一定期間が経過した後、セキュリティ上の問題はなくなることも多い。

行政機関等に提供された情報セキュリティ事故に関する情報について、情報提供者の秘密保持等に配慮した上、学習教材として提供される方法の検討を進めるべきである。

＜今後実施すべき施策＞

〇情報セキュリティに関する事故事例等の共有化の検討

・独立行政法人情報処理推進機構等に集約される情報セキュリティに関する事故事例等について、情報提供者等に配慮し、学習教材として提供する手法について検討する（内閣官房、経済産業省、関係府省庁）。

③ 法律実務家の育成

情報通信分野において技術革新が著しく進展し、これを活用した多種多様な新たなサービスが提供開始されることにより、情報セキュリティが侵害等された場合、これまでにない法律上の問題が発生する可能性が高まっている。

また、多くの情報通信サービスは事実上国境に関係なく提供されており、情報通信サービスや情報セキュリティに係る法律上の問題については、国際的な法的枠組みや他国の法律等も踏まえた対応が必要となっている。

しかしながら、現状、我が国においてこれら情報通信や情報セキュリティに

精通した法律の実務家は限られている。情報通信分野が我が国の社会経済の基盤であるのみならず、産業の国際競争力や国家安全保障と深く結びついていることも踏まえ、法律実務家の育成も焦眉の課題である。

＜今後実施すべき施策＞

○情報セキュリティに詳しい法律家の育成

内閣官房等において弁護士を雇用する等し、情報セキュリティに詳しい司法関係者の育成を図る。

・外部人材を活用する等して情報セキュリティ分野をリードし得る司法関係者の育成を図る（関係府省庁）。