資料１

情報セキュリティ人材育成に関する論点

情報セキュリティに関する５種類の人材（企業の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、その他一般人）が成長していく過程で講じられる人材育成施策に関する論点は以下の通り。

（1）企業の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、企業における情報セキュリティ人材は、数及びスキルの双方において不足していると言われるなど、確保は進んでいない。

今日、多くの企業の情報システムはそれぞれの企業業務と密接に結び付き、独自の構成となっている。このようなシステムは専門事業者によって構築されるが、システムが業務の細部まで入り組んでいるため、その構築と運用に際しては当該企業の実務に精通した者の関与が不可欠である。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場合も多く、専門事業者に全てを任せることは望ましくない。

また、システムの機能のみで完全な情報セキュリティを確保することはできない。このため、社内での情報取扱いに係るルールを定め、必要な教育訓練を行う等の組織的対応も必要となっている。

このような状況の下、企業においては、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、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、そうでなければ採用後の社内での人材育成が不可欠である。

また、必ずしも収益に直結しない情報セキュリティへの投資や情報セキュリティ人材の育成を推進するためには、企業経営層における情報セキュリティへの理解促進が不可欠である。

以下、それぞれの場合について、対応策をとりまとめる。

①情報セキュリティ専門家を目指す者の支援

（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１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考えられる。専門家を目指す者の将来の不安を少しでも払拭するためには、企業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、平成 23 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、専門家を目指す者の参考になるとともに、②に示す人材育成計画を策定する企業の参考になるものと考えられる。

＜論点＞

○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のではないか。キャリアパスモデルを策定し、普及に努めるべきではないか。

②企業における情報セキュリティ人材確保の支援

（人材育成計画の策定）

企業において情報セキュリティ人材を確保するには、専門知識を持った者を採用するか、採用後に社内で育成していくかになるが、その際には求められる情報セキュリティ人材の将来がある程度明確になっていることが望まれる。企業が求める人材像とその育成過程を具体化することにより、効果的に人材育成できるとともに、応募しようとする者に将来の処遇期待を示すことが可能となる。

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、当該企業が求める人材像を明確にし、その人材像に至る過程で取得すべき資格、予定される研修やリカレント教育、中期的な処遇見通し（キャリアパス）等について、具体的に定められていることが望ましい。また、例えば経理や営業といった他の部門との行き来などについても例示されることがなお望ましい。

人材育成計画は基本的には個々の企業により策定されるものである。しかしながら、情報セキュリティ人材に必要とされる能力は、その策定の際参考とできるモデルプランがあることが望ましい。また、人材育成に関連するスキルとそれに関連する資格・教育プログラムが整理されると、企業における人材育成計画の策定や、組織内外の人材の流動化による適材適所の人材配置等が促進されると考えられる。

＜論点＞

○人材育成計画策定促進

人材育成計画の策定は、企業における効果的な人材育成等に資すると考えられるため、これを促進するような取組が必要ではないか。

○スキル、資格、教育プログラムの整理

企業における人材育成計画策定、効率的人材育成、組織内外の人材流動化による適材適所の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べきではないか。

（多様な教育機会の提供）

セキュリティ人材の育成に際しては、ＯＪＴや企業内研修にとどまらない、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提供されることが望ましい。例えば、一定の勤務経験の後、大学等で集中的に学ぶリカレント教育等は、有効である。

また、多様なインシデントシーンを経験できることが望ましい。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。

平成 18 年度～平成 22 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」の教育拠点において、ＩＴ企業の技術者等の社会人学生の受け入れが行われた（「ISS Square」では平成 22 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。

＜論点＞

○リカレント教育の促進

情報セキュリティに関する基礎的な学習を短期間に集中して授業を開催するなど、体系的な知識の無い社会人が参加しやすいリカレント教育の取組の全国展開を図るべきではないか。

○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をハブとした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べきではないか。

（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における情報セキュリティ対策は、当該企業のみの問題ではない。このため、平成 23 年１月 24 日、内閣官房副長官から各省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、調達仕様書等において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、例えば「実務担当者には、『情報処理の促進に関する法律』（昭和 45 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」こととしている。

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」（平成 24 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しており、今後検討を進める必要がある。

＜論点＞

○資格要件の設定

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継続教育の実効性をいかに確保していくか検討していく必要があるのではないか。

また、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国以外の者に扱わせることを内容とする契約を締結する企業等と同様の取組を促す方策について、実情を勘案の上、広範な検討を行うべきではないか。

③企業経営者の意識改革

企業における情報セキュリティ対応能力を向上させるためには、経営者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、全社的に推進していく必要がある。これまで述べた様々な情報セキュリティに関する企業内での人材育成施策の実施についても、経営者層の理解がなければ実施は困難である。

また、新たな情報通信技術等を活用した様々なサービスが企業等によっ

て開発・提供される中、これらサービス提供者における情報セキュリティの確保も不可欠な課題である。

しかしながら、現状では、未だ経営者層の情報セキュリティに関する認識が十分でない場合も多く、情報システム部門等に任せきりであったりそもそも必要となる経営資源を十分に投入していないケースが少なくない。こういった経営者層の意識を改革していく必要がある。

（企業経営者への訴えかけ）

企業経営者の意識改革のためには、あらゆる機会をとらえて、企業経営者等に訴えかけていくことが重要である。とりわけ、我が国の企業の大半を占める中小企業の経営者の意識改革を重点的に対応することが重要である。

現在、企業の経営者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、経済産業省が「サイバー情報共有イニシアティブ（Ｊ－ＣＳＩＰ）」を開催するとともに、中小企業情報セキュリティ指導者セミナーを開催（全国 25 か所（各会場 50～100 名程度）（平成 23 年度））している。また、経済団体が主催する会議等において政府職員が講演するなどによる情報発信を実施している。これらは必ずしも十分とは言えず、意識改革のために必要とな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。

なお、企業経営者への働きかけに際しては、企業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や、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、より具体的に情報セキュリティ対策を進めることを推奨することが望ましい。

他方、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ことも多く、企業の人事担当、採用担当への訴えかけも必要である。

また、情報セキュリティを理解した経営者を育成する観点から、経営者層育成のために設置されている経営学修士課程等において、情報セキュリ

ティ関連講義を実施されることが期待される。

＜論点＞

○経営者向けセミナーの開催等

情報セキュリティ対策の重要性等について、企業経営層・人事担当・採用担当の理解を深めるべく、経営者向けセミナー等を開催するとともに、経済団体等が開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べきではないか。

○セミナーの実施

中小企業の経営者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実施すべきではないか。

○ＣＩＯ及びＣＩＳＯ

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について、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べきではないか。

○経営学修士課程等における取組の推進

経営学修士課程等において、情報セキュリティ関連講義の実施が重要であることについて、大学院関係者の理解を深めるべきではないか。

（体制整備の義務付け）

一般の調達等において、国の安全に関する重要な情報を扱う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の責任の明確化が求められている。必要に応じてこのような義務付けを行うことは有効である。

＜論点＞

○国の安全に関する重要な情報を扱う企業等との契約における情報セキュリティ対策の促進

（２）政府機関のセキュリティ担当者

（現状）

政府機関においては、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、これを各府省庁がＣＩＳＯのもとで実施することとしている。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い恐れがある。

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とともに、とりわけ小規模組織等の情報セキュリティインシデント対応能力補完措置を講じることとしている。具体的には、各府省庁の情報セキュリティ担当からなり、危機発生時に省庁の壁を越えて事態対処に当たるチーム（以下「事案対処チーム」という。）を組織し、これを有効活用しようとするものである。

①事案対処チームの育成と連携強化

まずは事案対処チームを立ち上げ、必要な人材を早急に育成することが重要である。事案対処チームは各省が連携した組織であるため、組織が円滑に活動するには、参加する各要員が各府省庁のシステムなどについて共通した知識や理解を持っている必要がある。また、実際にインシデントが発生した場合、機動的な対応には各要員の連携が重要であり、同一の研修に参加するなど日ごろの連携体制を維持することが必要である。

＜論点＞

○CSIRT 要員の育成等

政府機関においては、インシデントに機動的に対応するために、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こととしているため、それを担う組織内 CSIRT 要員を早急に育成する必要があるのではないか。

○事案対処チーム要員の育成

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事案対処チームを早急に設立すべきではないか。

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対応を行っている。しかしながら、昨今、情報セキュリティリスクが一層高まってきたことを踏まえると、情報セキュリティの担当者についても、一定程度の知見を持った職員が配置されることが必須である。

これに対応するためには、一定程度の知見を持った者を採用する方法や、採用後の人事ローテーションにおいて同一の者が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。また、内部人材の活用のみならず、官民の人事交流により、外部から優秀な人材を活用する工夫も考えられる。

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。

＜論点＞

○人事ローテーションの工夫

各府省庁の情報セキュリティ担当者同士で人事ローテーションを行うといった工夫が必要ではないか。

○優秀な人材の活用及び排出

内部人材の活用のみならず、官民の人事交流により、外部から優秀な人材を活用する工夫も考えられるのではないか。

○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をハブとした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べきではないか。

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

組織内の情報セキュリティを向上させるためには、システムや担当者のみの能力の向上だけでは不十分であり、個々の職員全員の意識や能力の向上が必要である。そのため、採用時の試験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、高度情報セキュリティ人材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情報セキュリティ人材の育成を行っているところである。

政府職員全体の情報セキュリティ意識の啓発と能力の更なる底上げのためには、政府機関を取り巻く状況や研修効果等を踏まえた教育訓練の充実強化を図っていくことが必要である。また、国家公務員は情報セキュリティに関する素養が求められるため、適切な人材を国家公務員に採用する観点から、公務員試験において、情報セキュリティ関係の出題は効果的であると考えられる。

＜論点＞

○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

国家公務員は情報セキュリティに関する素養が求められることから、公務員試験において、情報セキュリティ関係の出題を行うべきではないか。

政府機関を取り巻く状況や研修効果等を踏まえた教育訓練の充実強化を図るべきではないか。

（３）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。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必ずしも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。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が不可欠であるが、複数の要因を統合して判断できる能力も重要である。このような能力確保のためには多様な経験が必要であり、一の企業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求められる能力は、必ずしも教育等で得られない先天的なものがあり、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実践的スキルを有する人材の育成支援

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。

情報セキュリティ分野は実践が重要であることから、産学官の最先端の分野で情報セキュリティに関する業務を多数経験した人材が数多く輩出され

ることにより、我が国のセキュリティレベルが向上すると考えられる。

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振興機構等が優秀な人材受け入れ、研究機関への受け入れを通じて人材育成を進めることにより、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。

また、企業のセキュリティ担当者と同様、リカレント教育も重要である。学生時代に学習した内容について、実践的な経験を持ちながら再度学び直すことにより、情報セキュリティに関する一歩進んだ理解が可能となり、一層の能力の向上が図られるだろう。

＜論点＞

○キャリアパスモデルの普及、人材育成計画策定促進

キャリアパスモデルの策定は、企業における人材育成計画策定促進に寄与することが期待される。独立行政法人情報処理推進機構が策定したモデルの利用促進等を通じて、企業におけるキャリアパスや人材育成計画の策定を促進すべきではないか。

○スキル、資格、教育プログラムの整理

企業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べきではないか。

○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、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振興機構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ことが期待されるのではないか。

○リカレント教育の促進

ISS Square 等で実施されたリカレント教育の枠組みを参考に、専門的知識を持った者の学び直しに資するようなリカレント教育の取組の全国展開を図るべきではないか。

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。

今後、情報セキュリティに関する講座が拡大され、大学・大学院における教育体制が充実することを期待する。既に情報セキュリティに関する研究科等の設置、ひいては「情報セキュリティ技術経営」等の学位の授与を検討する動きもあるが、企業へ即戦力を供給する取組、情報セキュリティ産業人材育成のモデルの普及、情報セキュリティ人材の社会的地位向上という観点から、有効ではないかと考えられる。

＜論点＞

○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を継続して実施するとともにその成果を全国的に展開することが重要ではないか。

○研究科等の設置支援

全国的な展開にあたっては、情報セキュリティを学ぶことができる場を増やす必要があり、このためには情報セキュリティに関する研究科等の設置の推進が重要ではないか。

○学位授与

一部の大学では「情報セキュリティ技術経営」等の学位の授与を検討する動きもあるが、企業へ即戦力を供給する取組、情報セキュリティ産業人材育成のモデルの普及、情報セキュリティ人材の社会的地位向上という観点から、有効ではないか。

③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

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インセンティブ付与に関する取組も重要である。

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。

＜論点＞

○表彰等の実施

優秀な人材の確保及び能力向上のためには、優秀な人材を発掘し、更なる能力向上に向けた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であり、上記の取組を継続・発展して実施していくことが期待されるのではないか。

ハッキングコンテストなどの情報セキュリティに関するコンテスト開催

も有効ではないか。

（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、我が国の情報セキュリティ分野の国際的な産業競争力確保において不可欠である。また、情報セキュリティの確保が国家安全保障とも結びつく重要課題であることから、国内に高い水準の研究者を有することが必須である。

先端的な研究者・技術者の育成に際しては、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る。基礎教育の課題は（３）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。他方、研究開発環境の確保のためには、研究開発資金の重点化、集中化等が必要となる。

①情報セキュリティ研究開発の推進

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て、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ことが重要である。

情報セキュリティ政策会議において、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。この戦略に掲げた４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４重要分野についての研究開発を推進する中で先端的研究者・技術者の育成を図っている。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。

＜論点＞

○研究開発戦略の推進

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はないか。

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

「（３）セキュリティ産業人材」において提言した、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も、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。

＜論点＞
○複数大学や産業界の連携協力による大学・大学院教育
○研究科等の設置支援
○学位授与

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、最先端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し、最先端の技術者・研究者として活躍できることが望ましい。

また、高度な情報セキュリティに係る能力が生かされるためには、そのような能力を有する者が切磋琢磨できる、健全なコミュニティの形成が望ましい。

このため、例えば、政府機関や関係する独立行政法人に産官学の“とんがった“人材を結集させ、“とんがった“人材を輩出する中心的な役割を果たすことが期待される。

＜論点＞
○内閣官房情報セキュリティセンター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、独立行政法人情報処理振興機構、独立行政法人情報通信研究機構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ことが期待されるのではない

か。

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り、国際会議への参加や日本への招致、海外留学等の取組の推進をすることも必要である。

＜論点＞

○国際会議への参加等

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り、国際会議への参加や日本への招致、海外留学等の取組の推進をすることも必要ではないか。

（５）全てのセキュリティ人材育成に共通する課題等について

（現状）

情報化が進んだ現代日本社会においては、情報セキュリティの専門家以外であっても、情報セキュリティに関する基礎的な知識を持っていることが必要である。

また、大学・大学院において情報工学や情報セキュリティを専攻しておらずとも、企業や行政機関等において情報セキュリティ担当としての役割を果たすことが求められることがあり、その際、大学の共通教育・教養教育や初等中等教育において、情報セキュリティを学習したバックグラウンドは非常に有益である。

このため、大学の共通教育・教養教育や初等中等教育において、情報セキュリティの教育を充実する必要がある。

①初等中等教育段階における情報セキュリティ教育の充実

セキュリティ人材の育成は、大学・大学院生の育成、社会人の育成が中心となるが、情報セキュリティに関する教育は高等学校卒業後に初めて始まるのではなく、将来のセキュリティ人材育成という観点からは初等中等教育段階の教育も重要である。初等中等教育段階では、「情報」の科目が必修化されたところであり、発達段階に応じた情報セキュリティに関連する教育を確実に実施する必要がある。

また、「情報」の授業が確実に実施されたとしても、教員の能力が十分でなければその効果は十分には発揮しない。教員の能力向上に関する対策としては、各都道府県及び指定都市で指導的立場である情報教育担当指導主事等に対して情報教育担当者連絡会議等を開催し、教育現場における情報セキュリティ等の普及・啓発を行うとともに、「情報セキュリティ月間」において、文部科学省関連機関における情報セキュリティ対策の一環として「情報セキュリティセミナー」を開催し、普及・啓発を行っているところではあるが、まだなお教員の能力は十分ではなく、教員の能力の向上が求められる。

＜論点＞

○情報セキュリティ教育の実施

大学・大学院における育成や社会人の育成を効率的に行うためには、初等中等教育段階で情報セキュリティを学習したバックグラウンドが重要ではないか。

○教員等の能力の向上

教員の能力の向上について、引き続き、教員及び教員を志望する者への情報セキュリティ研修等の充実を図っていくことが必要である。また、初等中等教育における情報セキュリティ教育の向上のみならず、学校の情報セキュリティを確保するためには、学校 CIO の情報セキュリティ対策に対する意識向上が必要ではないか

○大学入試等における出題

初等中等教育では、大学入試等に対応するための教育が優先される傾向にある。初等中等教育で情報セキュリティを確実に学ばせるためには、例えば「情報」が大学入試において取り上げられることが有効ではないか。

②大学の共通教育・教養教育の中での情報セキュリティ教育の充実

大学の共通教育・教養教育においては、各大学の自主的な判断により情報セキュリティ教育が実施されている。積極的な取組として、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を導入し、資格試験合格によって単位を認定している大学等（約１５校）が挙げられる。

しかし、総じて、大学の共通教育・教養教育における情報セキュリティ教育は、「情報」の科目が必履修となっている初等中等教育段階と比べ、実施されていることが少ないと考えられる。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、教えられる教員がいないことなど様々な理由があると思われるが、これを解消する必要がある。

＜論点＞

○情報セキュリティに関する最新情報の提供

大学の共通教育・教養教育における情報セキュリティ教育の実施を推進するため、各大学における情報セキュリティ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の提供が必要ではないか。

○資格試験等の活用

わかりやすい目標を設定し学生の関心を高めたり、適切な教員が不足している大学でセキュリティに関する講義を実施するためには、資格試験合格によって単位を取得させたり、資格に関する学習プログラムを導入するような取組も有効であると考えられ、このような取組が拡大していくことが期待されるのではないか。

③産学連携の強化

大学等において情報セキュリティに関する教育を行う際には、知識のみではなく、実践的な教育が必要不可欠であり、実践的な教育を実施するためには、企業人講師の活用やインターンシップの実施など、産学が連携して教育を実施することが求められる。このような観点から「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、産業界と連携した実務家教員による講義等が実施されるとともに、実践的なインターンシップが実施された。

また、産業界と教育界が協力した授業や教材について、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、データベース化を行い公開中である。引き続き、産学連携の取組を積極的に推進するとともに、すでに実施された取組を全国展開することが必要である。

＜論点＞

○情報セキュリティの実践的教育

すでに実施されている産学が連携した教育を継続して実施していくとともに、今後はこれらの成果を踏まえ、産と学とが協力し、自発的に連携していくことが期待されるのではないか。

○インターンシップの推進

インターンシップについては、上記の取組の成果を教育機関及び産業界に紹介することなどを通じて、更なるインターンシップの推進を行っていくことが重要ではないか。

○データベースの活用

産学が連携した取組を全国的に展開するためには、国立情報学研究所等が作成したデータベースを大学等が活用することが有用ではないか。

④情報セキュリティに関する事故事例等の活用

情報セキュリティ担当が、急速に進歩する技術を効率的に学習し、また、情報セキュリティ事故を未然に防止する観点等から、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学習教材として活用することは効果があると考えられる。情報セキュリティ事故に関する情報については、行政機関や独立行政法人等へ集約されるスキームがあり、これらの集約された情報を、情報提供者等に配慮し、学習教材として提供されることが期待される。

＜論点＞

○情報セキュリティに関する事故事例等の共有化の検討

行政機関や独立行政法人等へ集約される情報セキュリティに関する事故事例等を、情報提供者等に配慮し、学習教材として提供することを検討すべきではないか。