平成 22 年度内閣官房
情報セキュリティセンター
委託調査

【概要版】

平成 22 年度 情報セキュリティに係る人材育成・確保及び普及啓発に関する調査・検討

報告書

2011 年3月

株式会社 NTT データ経営研究所

1.　背景／目的

(1)　背景

情報セキュリティ政策会議(2010 年 5 月 11 日)において決定された「国民を守る情報セキュリティ戦略」では、新たな環境変化に対応した情報セキュリティ政策の強化を行うことが定められた。この強化政策では、次の 2 点が示されている。

・ 国民・ユーザ保護の強化として「普及・啓発活動の充実・強化」の取り組み ・ 技術戦略の推進等として「情報セキュリティ人材の育成」の取り組み

上記戦略を受けて「情報セキュリティ 2010(情報セキュリティ政策会議　第 24 回会合決定　同年 7 月 22 日)」では、内閣官房が情報セキュリティの普及・啓発手法の検討と情報セキュリティ人材育成に関する工程表を策定することとなった。

(2)　目的

本調査・検討は、「国民を守る情報セキュリティ戦略」及び「情報セキュリティ 2010」を受けて、「普及・啓発活動の充実・強化」及び「情報セキュリティ人材の育成」の取り組みについて、情報セキュリティ人材を取り巻く現状や課題等についての調査、分析を行ったうえで、今後の情報セキュリティ人材の育成・確保及び普及啓発に関する政策の在り方を明らかにするものである。

本調査・検討では、昨今の情報セキュリティ情勢を踏まえ、各方面からの具体的な課題の検討と、実施すべき人材育成・確保及び普及啓発に関する課題の抽出を行ったうえで、政府が緊急的に取り組むべき課題について、有識者による検討を行う。

本調査・検討は、政府が推進すべき人材育成及び普及啓発に関する施策の立案の起点となることを目的とする。

2.　調査研究の全体像

本調査・検討におけるテーマ（「情報セキュリティの普及啓発の検討」および「情報セキュリティ人材の育成・確保の検討」は、ユーザに対する認知（Awareness）の底上げ・引き上げやサポートの在り方等について、相互に関連したテーマとなっているため、普及啓発と人材の育成・確保の両方を視野に入れる必要がある。これを踏まえて、情報セキュリティ人材の在り方を整理し、テーマの検討を行う。

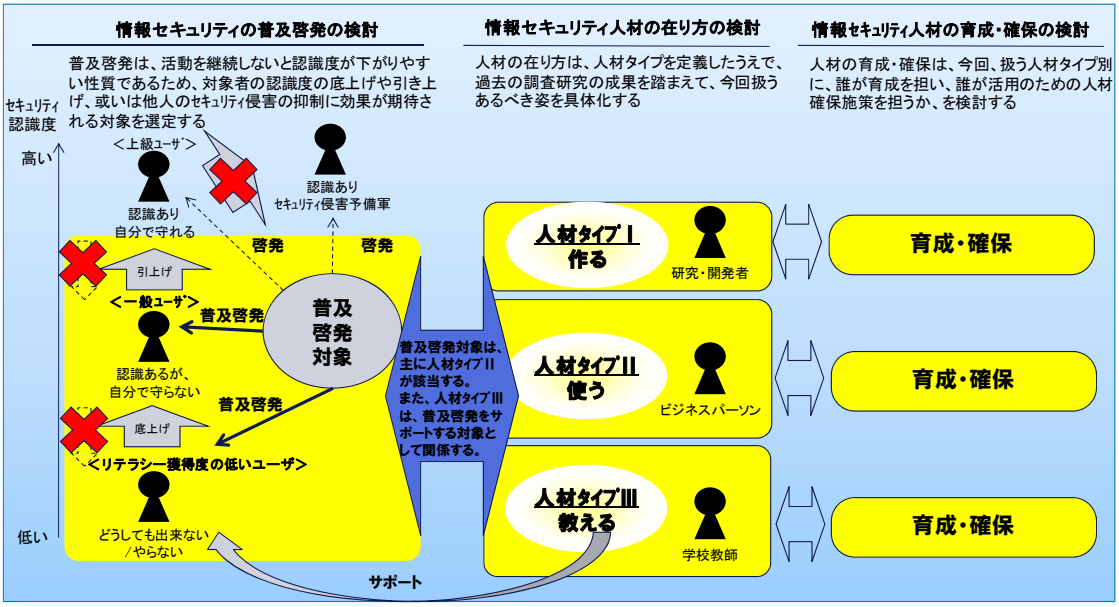


図 1 調査研究の全体像

3.　情報セキュリティの普及啓発

3.1.　普及啓発の必要性

IT 及び IT を利用したサービス（以下、IT サービス）は、日々進化を続け社会に新たな変革をもたらしている。IT の進化及び IT がもたらす変革は、従来のセキュリティ上の課題を解決する一方で、別の課題を新たに発生させている。このように情報セキュリティには解決しなければならない課題が時間とともに移り変わる「Moving Target」と呼ばれる特徴がある。そのため、時間とともに変わる情報セキュリティ上のリスクからユーザが自らの身を守る知識を身につけられるよう、情報セキュリティの普及・啓発を継続的に行う必要がある。

IT サービスの仕組みは様々な技術や仕掛けを複合的に利用していることから、その仕組みが変化すればリスクも変化する。しかし、ユーザはそこで利用されている仕組みを理解せずにサービスを享受するため、ユーザはその仕組みが持つリスクによって被害を受ける可能性がある。したがって、時代に応じたサービスごとの仕組みの理解について、継続的な普及啓発が必要である。

一方で、仕組みは個々のサービスによって異なるが、便利なモノにはリスクが伴うという情報セキュリティの本質は、全てのサービスに共通する。このようなリスク認識をユーザが持てば、新しい IT サービスを利用する都度、ユーザ自身が自発的に注意を払うことが期待できる。このことから、情報セキュリティの本質を教えるという普遍的な普及活動が必要となっている。

以上を踏まえて本調査・検討では情報セキュリティの普及啓発の意義を以下のとおり定義する。

「IT サービスの仕組みと情報セキュリティの本質の両方を国民（ユーザ）に啓発することによって、ユーザがセキュアな行動様式を持ち、IT サービスの変化に自発的に対応できるようになること」

その上で、普及啓発の対象毎に課題を整理した後、どのような施策を打っていくべきかを検討した。なお、検討の過程において、普及啓発の対象を以下の通り整理した。また、普及啓発のための基盤の整備も必要であるとの議論があったため、この対象に加えて、施策としては、基盤についても整理している。

- ホームユーザ（若年層）
- ホームユーザ（成人層）
- ビジネスユーザ
- 基盤

3.2.　普及啓発の施策

本節では、普及啓発の対象毎に、課題と解決の方向性を示す。本節に記載する方向性は、今後さらに施策として具体化する際の参考となる。

3.2.1. ホームユーザ（若年層）

私的用途に IT サービスを利用する者のうち、小学校・中学校・高等学校就学中の者を対象とする若年層を取り巻く IT サービスの利用及び普及啓発の現状は、リスク及び IT サービスの仕組みの認識不足及び教える側である学校教師のリテラシー・知識不足が認められる。

このため、若年層向け情報セキュリティの普及啓発では、若年層の生活圏として中心的な場である学校と家庭に焦点をあてて、「普及啓発の必要性」で整理した情報セキュリティの本質と IT サービスの仕組みについて教育することを検討する。このとき、危険なものには近づかないことに偏りすぎた教育は IT 利用そのものを阻害する可能性があるため、ケーススタディに基づいた情報セキュリティの本質を教えることが有効と考える。そのうえで、発達段階に応じた教材・手法を用いる必要がある（下図②）。

併せて、若年層に情報セキュリティを教える側の学校教師や保護者のリテラシーや知識を高める必要がある（下図①及び③）。

このような考えに沿って、若年層向け情報セキュリティの普及啓発は、「情報安全教育」の枠組みに組み込むことによって、教育の現場に過度な負荷をかけないよう配慮する。そのうえで、学校教師・保護者・校長等学校組織の長に対する普及啓発と、現場での教育を支えるための教材・ツールの提供を検討する。

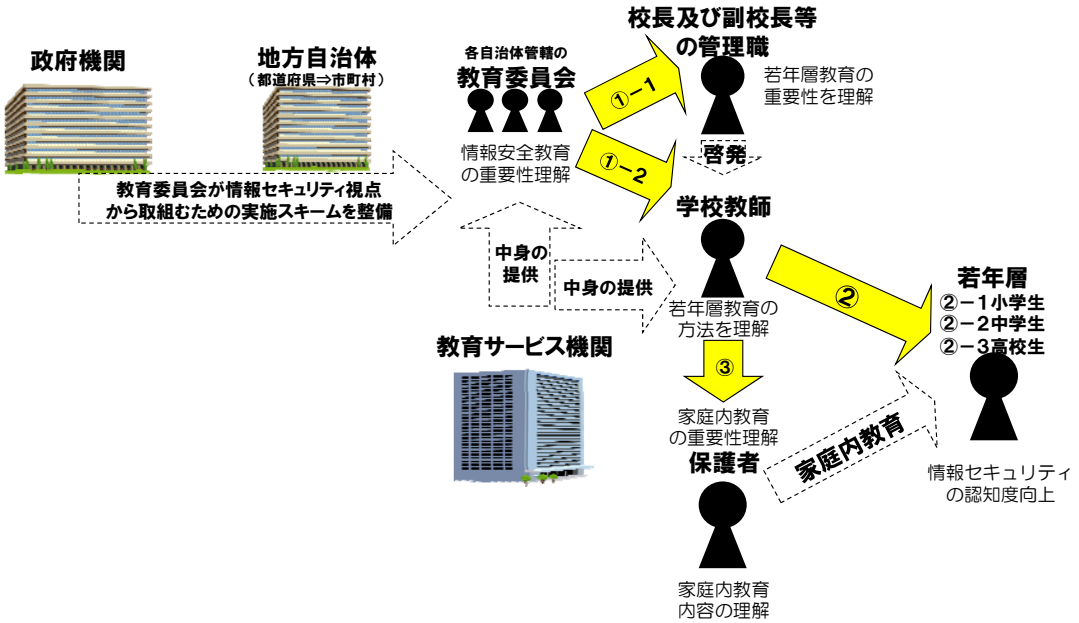


図 2 若年層向け取り組みの全体概要

3.2.2. ホームユーザ（成人層）

私的用途に IT サービスを利用する者のうち、ホームユーザ（若年層）以外の成人層を取り巻く IT サービスの利用及び普及啓発の現状は、構成する年齢構成等が幅広く、IT 習熟度や IT サービスの利用頻度も多岐にわたるため、IT リテラシーや仕組みの理解にばらつきが認められる。

このため、成人層向け情報セキュリティの普及啓発では、情報セキュリティに関するリテラシー獲得度の低いユーザ及びある程度の獲得度はあるが、自分自身を守るまでのリテラシーを獲得していないユーザに焦点をあて、国内全域における上述の対象に対して「3.1. 普及啓発の必要性」で整理した情報セキュリティの本質と IT サービスの仕組みについて、リテラシーや知識が獲得できるよう取り組むことを考える。

成人層のなかにはどんなに普及啓発を行っても理解できない、理解しようとしない「永遠の初心者」とされる対象者も存在すると考えられるが、このような対象者もリテラシー獲得度の低いユーザとして扱い、普及啓発によって「永遠の初心者」を解消することを目指す。

このような考え方に沿って、成人層向け情報セキュリティの普及啓発は、リテラシー獲得度合いの低いユーザ及び一般ユーザとの接点を重視して国内全域での教育・普及啓発機会を提供可能とすることを検討する（下図①及び②）。

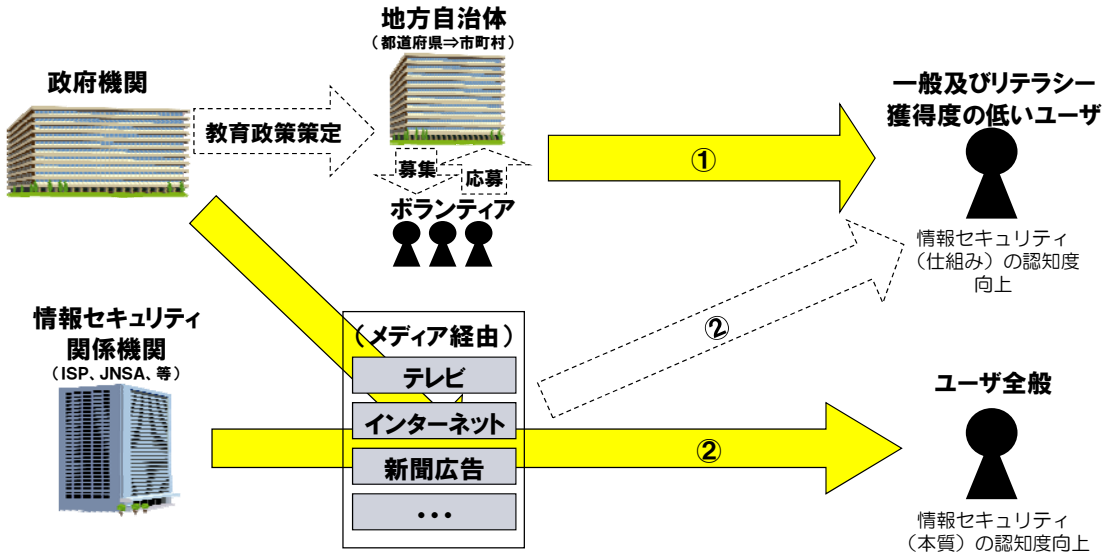


図 3 成人層向け取り組みの全体概要

3.2.3. ビジネスユーザ

ビジネス用途に IT サービスを利用する者であるビジネスユーザを取り巻く IT サービスの利用及び普及啓発の現状は、企業規模の大小を問わず勤務先企業経営者の情報セキュリティに関する認識に大きく左右される。従業員は経営者の方針に基づく企業ガバナンスに従って、情報セキュリティを意識した企業活動を行う。その結果、従業員が情報漏えい等の不祥事を起こした場合は、経営者が責任を負う。

そこで、ビジネスユーザ向けには、企業ガバナンスが機能することを前提として、企業方針への強い影響力を持った経営者及び部門長に焦点をあて、情報セキュリティの取り組みの重要性・必要性を啓発することが必要となる。

例えば、ポイントカード発行時に顧客の個人情報を直接扱うようなスーパーマーケットや美容院等の店頭において、正社員や契約社員の他に派遣社員やアルバイト・パート従業員が配置されている場合がある。こういった非正規雇用の従業員に対する社内の情報セキュリティ教育が行き届いていないために、情報漏えい事故等を発生させる事象が現場の実態として見受けられる。経営層への啓発においては、非正規雇用の従業員についても正社員と同等の情報セキュリティ教育が必要であることを訴求する必要がある。

このような考え方に沿って、ビジネスユーザ向け情報セキュリティの普及啓発は、経営者及び部門長に焦点をあてた普及啓発の施策を検討する（下図①）。

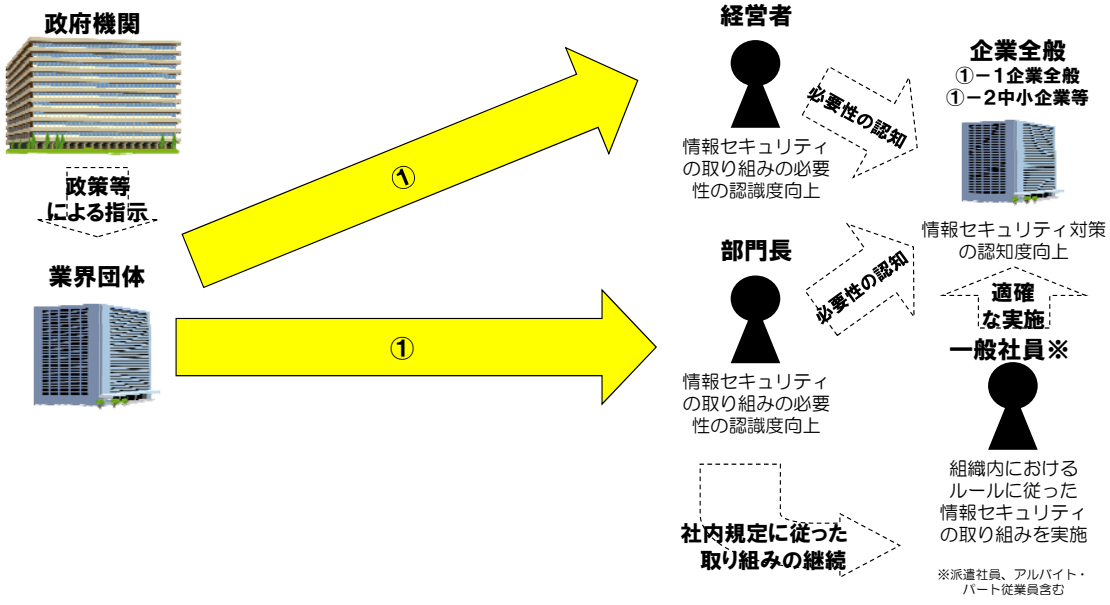


図 4 ビジネスユーザ向け取り組みの全体概要

3.2.4. 基盤

IT サービスを利用する者のセキュリティ意識に直接的・間接的に影響を及ぼす周辺環境である基盤については、安全安心な IT 利用が自発的に促進される仕組みが必要となる。

具体的には、情報セキュリティ対策の実施状況をユーザが自身のサービス選択基準として判断できる環境整備などが考えられる（下図①及び②）。このような環境があれば、企業の情報セキュリティ対策への取り組みが品質向上や事業利益につながるため、企業が積極的に情報セキュリティ対策に取り組むことが期待できる。

また、ユーザの相談窓口として連絡・相談先の明確化や普及啓発の取り組み効果を確認して改善を図るいわゆる PCDA サイクルを機能させるための効果測定の仕組みも考慮する（下図③及び④）。

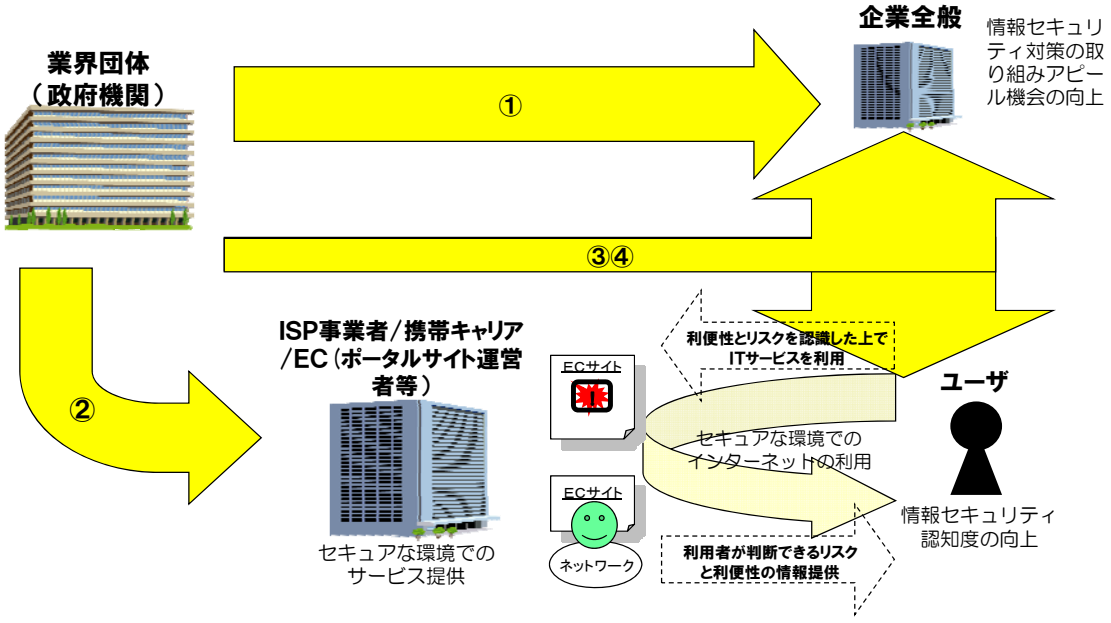


図 5 基盤における取り組みの全体概要

4.　情報セキュリティ人材の育成確保

4.1.　人材の必要性

本節では情報セキュリティ人材の必要性について、情報活用と社会環境の観点から整理する。

（1）　情報活用と情報セキュリティ

今日、企業活動においては、膨大なデータを分析・処理してビジネスに還元する情報活用が IT の利用によって効率的・効果的に行われているかつ、社会活動のあらゆる場面で情報が活用されるようになった。これらの情報活用には、情報を取り扱う以上必ず情報セキュリティのリスクが伴っている。そのため、例えば、電子化された大規模な名簿がインターネット上に流出した場合の甚大な被害のように、情報活用に関係する情報セキュリティのリスクの顕在化は、これまで以上に広範囲かつ拡大する傾向にある。

また、情報活用に内在するリスクに対して適切に対処するためには、情報活用と情報セキュリティは不可分な関係となっている。

高度情報活用社会への進展に伴い、今日では、情報セキュリティリスクへの対応が様々な場所で求められるようになっている。したがって、情報活用をするうえでは、その情報セキュリティを担う人材が必要になってくる。

（2）　社会環境と情報セキュリティ

我が国は米国ほどの訴訟社会ではないことから、情報セキュリティリスクの顕在化による負の影響を、企業を取り巻く他のリスクと比較して、コンプライアンスの対象として認識されにくい環境にある。これらの状況を背景として、情報セキュリティ対策の商品やサービスの需要も欧米と比較すると少なく、我が国では情報セキュリティ分野が産業化されているとは言い難い状況にある。

このことから我が国は情報セキュリティ人材のニーズが認識されにくい社会環境を背景として、情報セキュリティ分野に特化した人材は職業として成立しにくい傾向にある。

加えて、我が国では終身雇用制度を採用する企業が大半であるため、資格や専門性という観点では、人材が流動化しにくい社会環境である。そのため、情報セキュリティ人材という専門職が成立しにくいと考えられる。

このような我が国の雇用環境を考慮すると、一人の人材が全てのリスクに対応できる情報セキュリティのスペシャリストを育成するというよりも、特定の分野ではなく複数の分野においてある一定以上の知識や技術を持ち、高度に専門的な問題はスペシャリストに相談できるようなゼネラリスト的な企業人材を育成するなかで、情報セキュリティの知識を習得させるということが求められる。したがって、我が国で求められる情報セキュリティ知識の特徴としては、特定の分野に閉じるのではなく、複数の分野を視野に入れた全域性ある情報セキュリティ知識領域であると考えられる。

4.2.　人材の育成確保の対象

本節では、情報セキュリティ人材が担う役割を整理した後、どの様な人材が求められるのかを整理した。その上で、人材育成確保の対象として、情報セキュリティ技術・知識を作る、使う、教えるという３つの側面を踏まえて、人材像を設定する。

4.2.1. 情報セキュリティ技術を作る

情報活用と情報セキュリティは不可分な関係にあるため､情報活用に利用される IT にも、情報セキュリティ技術が組み込まれることが求められる。また、国際競争力を獲得するためには、そこに組み込まれる情報セキュリティ技術にも国際競争力が求められることになる。

そこで、この分野の研究者は国際競争力を持った実用的な情報セキュリティ技術を確保する研究開発力を持つことが必要である。このことは同時に、我が国がサイバーテロ等の脅威に対抗する技術を保有することにもつながる。

人材タイプⅠ（高度セキュリティ人材）の人材像

国際競争力がある実用的な情報セキュリティ技術の研究開発力を持つ、高度セキュリティ人材と定義する。具体的な人材像としては、実用的な情報セキュリティ技術を研究テーマとする企業内研究者を想定する。

加えて、取り扱っている研究テーマという観点からは同じく確保が求められるということと、大学卒業後の進路として企業内研究者の候補となり得るため、大学内で同様の領域を研究テーマとする学者も対象とする。

4.2.2. 情報セキュリティ技術・知識を使う

企業活動を始めとする経済活動において、業務の効率化や企業競争力獲得のためには、情報セキュリティに配慮した情報活用が求められる。この情報活用の進展に伴いIT部門だけでなく、企業内の他の業務を行う一般的な人材が、情報セキュリティについて意識を持つことを求められることが多くなった。

このことから、自身の業務に関する業務知識やスキルに加えて、実用的な情報セキュリティ知識を持つことが情報活用を安全に行うためには必要である。

人材タイプⅡ（ビジネスパーソン）の人材像

IT部門以外の業務担当者が、自身の業務知識やスキルに加えて、実用的な情報セキュリティ知識を持つ人材と定義する。

具体的な人材像は、これまで情報セキュリティ知識を活用することの中心にいたIT部門や総務部門ではなく、フロント業務や財務や会計等のバックオフィスの担当者を想定する。

この人材像は、自身の業務についての専門性を高く持つことと情報セキュリティの知識を持つことに加えて、他の業務における情報セキュリティ上のリスクを理解したうえで、適切な対処が可能となるような情報セキュリティに関する気づきや洞察力が求められる。

4.2.3. 情報セキュリティ技術・知識を教える

インターネット利用の低年齢化が進み、若年層でもITサービスを頻繁に利用する状況となっている。このような状況では、若年層もサービスに内在するリスクを知ったうえで、これらに適切に対処できるように、情報セキュリティの知識を習得している必要がある。そのため、若年層に対して情報セキュリティ教育を適切に実施できるレベルの知識を習得していることが必要である。

人材タイプⅢ（学校教師）の人材像

若年層に対して情報セキュリティ教育を適切に実施できる知識・スキルを習得した人材と定義する。

具体的な人材像は、学校の現場におけるITや情報に関する教育を行う学校教師を想定する。

4.3. 育成確保の施策

本節では、育成確保の対象毎に、課題と解決の方向性を示す。本節に記載する方向性は、今後さらに施策として具体化する際の参考となる。

4.3.1. 課題解決の方向性

（1）人材タイプⅠ（高度情報セキュリティ人材）

国際競争力がある実用的な情報セキュリティ技術の研究開発力を持つ、高度セキュリティ人材である人材タイプⅠを取り巻く育成確保の現状は、実用的な情報セキュリティ技術の研究開発力が不足していることと、産業界と学界における研究テーマの分断が認められる。また、我が国の情報セキュリティの研究開発活性化と安心・安全な ICT 環境の獲得のために、総合科学技術会議においては、「情報セキュリティ技術開発」がグランドチャレンジ型テーマとして設定されている。

このため、人材タイプⅠの育成確保の施策では、産業界と学界が共通して実用的な研究テーマに取り組むことによって、このようなテーマに取り組める人材を学界から産業界へ輩出して行くことが必要であると考えられる。しかし、こうしたテーマへの取り組みのためには、産業界との人材の交流によるニーズの共有が求められるにもかかわらず、このような交流が自然と行われる環境にもない。その結果、実用的な研究テーマを担える人材も自然発生的には現れないという悪循環に陥っている。

そこで、人材タイプⅠの育成確保については、国際競争力ある実用的な情報セキュリティ技術力を有する研究者を確保するために、産学連携した協働の取り組みと人材を発掘する仕組み等を確立するような方向性が有効であると考える。

（２）人材タイプⅡ（ビジネスパーソン）

IT 部門以外の業務担当者が、自身の業務知識やスキルに加えて、実用的な情報セキュリティ知識を持つ人材である人材タイプⅡを取り巻く育成確保の現状は、実務における情報セキュリティ知識の活用の高まりが確認されるにもかかわらず、情報セキュリティ知識の学習機会等の不足が認められる。例えば、これまで IT 利用が少なかった商品企画や顧客管理作業のような業務においても IT 利用が進んできたため、個人情報の漏えいを始めとした情報セキュリティ事故につながることがある。このため、情報セキュリティ知識を踏まえた業務の遂行が IT 部門以外の業務担当者においても求められている。このような状況のなか、企業では、経営者の情報セキュリティの重要性に関する理解や育成に投入できる経営資源の大小等によって、人材育成に独自に費用をかけて取り組んでいる。その結果、人材育成の取り組みは企業ごとに差が生じるとともに、実務の場面で活用が求められる情報セキュリティ知識を獲得するための汎用的な学習方法や機会の提供も十分とはいえない状況にあると考えられる。

このため、人材タイプⅡの育成確保の施策では、ビジネスパーソンが限られた時間やコストのなかで、自身の業務領域以外の知識を得る手段が求められる。このためには、大学への通学や資格取得の勉強といった学習方法以外の方法で、知識獲得の手段や機会を提供する必要がある。また、ビジネスパーソンに求められる自身が専門とする業務領域以外の知識については、情報セキュリティに関する深い知識が求められているわけではない。そのため、他の業務領域での情報セキュリティの具体的事例の共有や他領域の専門家との情報セキュリティに関する議論等から得られる気づきや洞察といった汎化されたレベルの知識を、業種や職種が異なる人材との交流を通じて短時間で習得することが、負荷や効率性の観点から有効であると考えられる。

そこで人材タイプⅡの育成確保については、業務担当者が自身の保有する業務知識に加えて、情報セキュリティに関する気づきや洞察を習得する機会を提供するために、業種や職種が異なる人材同士の交流機会の場を作るような取り組みを検討する。

（３）人材タイプⅢ（学校教師）

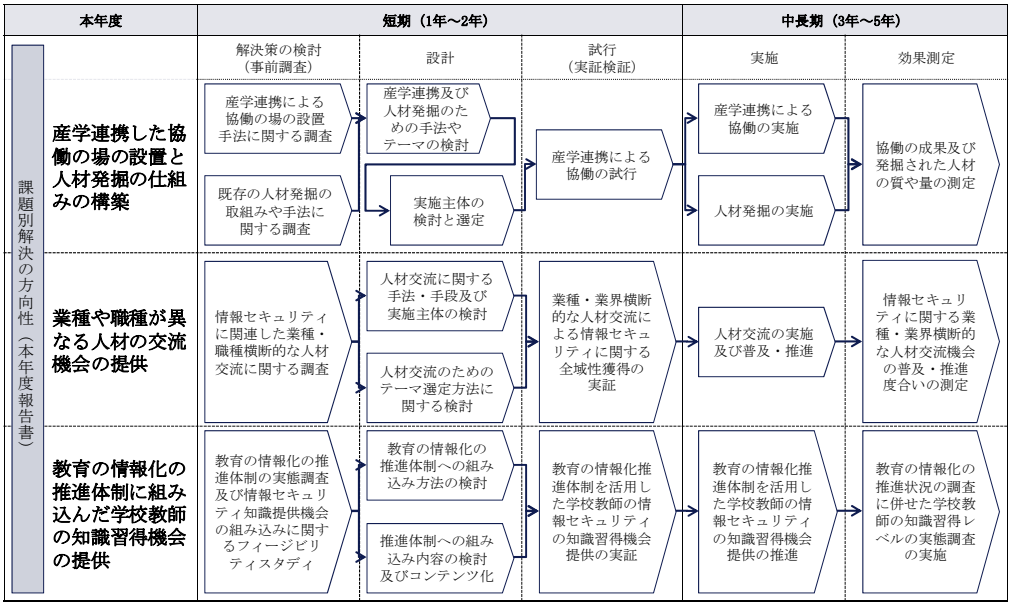
若年層に対して情報セキュリティ教育を適切に実施できる知識・スキルを習得した人材である人材タイプⅢと取り巻く育成確保の現状は、新学習指導要領に対応した「教育の情報化に関する手引」のなかで、学校における情報化の推進体制に基づいた取り組みを文部科学省が平成 22 年に新たに定めているが、学校教師の IT スキル・リテラシーはまだ不足している状況にあることが認められている。

このため、人材タイプⅢの育成確保の施策では、特別枠の時間を用いて習得機会の提供を行うのではなく、学校教師の本来業務の一環として習得機会を設けることが新たな負荷がかからない仕組みにつながるため、望ましいと考えられる。
現在、文部科学省によって、推進されている学校の情報化では、教育委員会と学校が連携した教育の情報化の推進体制が整備されつつある。そこでは、教育委員会が学校 CIO(校長、副校長、教頭)を指導・支援することになっており、加えて ICT 支援員が学校教師のサポートを行うことになっている。

そこで、人材タイプⅢの育成確保については、上記推進体制における教員サポートを通じて情報セキュリティ知識の提供を行うことによって、学校の情報化という本来業務の一環として学校教師向けに情報セキュリティ知識の習得機会を組み込むことが有効であると考える。

4.3.2. 工程表

課題解決の方向性を今後さらに施策として具体化する際の工程表案を以下に示す。



短期的には、政府が本年度の報告書に記載されている課題に応じた解決の方向性に沿った解決策の検討を行う。解決策の検討は、事前調査として具体的に施策の期間や規模に着目して実現可能性、効果の発現性等を把握する。事前調査を受けて、各課題の優先順位付け等に従い、施策ごとに実施概要等の設計を行う。設計した実施概要等は、試行による実証検証で効果等を確認の上確定する。

中長期的には、確定した実施概要に基づいて各施策が実施され、効果測定により取り組み成果を確認する。

今後は、本年度の調査検討から得られた課題解決の方向性ごとに、一連の検討、設計や各施策の実施と効果検証を行っていくことが望まれる。