人材育成・資格制度体系化専門委員会報告書

―人は城、人は石垣、人は堀―

２００７年1月２３日
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

目 次

はじめに ・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 1

委員名簿 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 4

第一章 情報セキュリティに係る人材の育成についての基本的考え方
第一節 情報セキュリティに係る人材の育成の必要性 ・・・・・・・ 5
第二節 本委員会における検討の方向性 ・・・・・・・・・・・・・ 8
第三節 本報告書の構成 ・・・・・・・・・・・・・・・・・・・・ 10

第二章 先進的な情報セキュリティ技術・製品及び高度な管理手法の研究・開発者
第一節 具体的な人材像 ・・・・・・・・・・・・・・・・・・・・ 11
第二節 現状と課題 ・・・・・・・・・・・・・・・・・・・・・・ 11
第三節 必要となる人材育成方策 ・・・・・・・・・・・・・・・・ 12

第三章 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提供する企業等における人材
第一節 具体的な人材像 ・・・・・・・・・・・・・・・・・・・・ 16
第二節 現状と課題 ・・・・・・・・・・・・・・・・・・・・・・ 17
第三節 必要となる人材育成方策 ・・・・・・・・・・・・・・・・ 21

第四章 政府機関、企業等の組織において情報セキュリティ対策に係る人材
第一節 具体的な人材像 ・・・・・・・・・・・・・・・・・・・・ 27
第二節 政府機関等における現状と課題、必要となる人材育成方策 ・ 29
第三節 企業等の民間部門における現状と課題、必要となる人材育成方策 39
第四節 留意すべき事項 ・・・・・・・・・・・・・・・・・・・・ 46

第五章 情報セキュリティに係る人材の育成に向けた具体的な取組み
第一節 政府機関における人材の育成に向けた取組み ・・・・・・・ 48
第二節 民間部門における人材の育成に向けた取組み ・・・・・・・ 53
第三節 教育機関に関する取組み ・・・・・・・・・・・・・・・・ 54
第四節 資格制度等に関する取組み ・・・・・・・・・・・・・・・ 56
第五節 各種教育プログラムの体系化について ・・・・・・・・・・ 57

おわりに　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・ 59

本委員会における検討の経緯 ・・・・・・・・・・・・・・・・・・・・ 61

参考

資料

はじめに

ユビキタス情報社会の到来が着実に進行している現在、我が国の社会経済活動や国民生活などあらゆる分野で情報技術（以下、「IT」という。）が、隅々にまで深く浸透しつつある。このように IT への依存度が日々高まってきているなか、IT を完全・安心に活用するための情報セキュリティ対策が焦眉の急を要する問題となっている。

このような状況に対応すべく我が国における情報セキュリティ政策は、2005年４月に内閣官房に情報セキュリティセンターが、同年５月には内閣官房長官を議長とする「情報セキュリティ政策会議」が設置され、国全体としての情報セキュリティ対策強化の中核機関としての活動を開始し、政府横断的かつ本格的な政策推進体制が整った。

その後、同年 12 月には、政府機関における情報セキュリティ対策の実施基準である「政府機関の情報セキュリティ対策のための統一基準」と、我が国の社会経済活動の基盤となる重要インフラ分野における対策実施計画である「重要インフラの情報セキュリティ対策に係る行動計画」が決定され、情報セキュリティ対策の強化が急がれる両分野における対策の枠組みが矢継ぎ早に定められてきたところである。

また、2006 年２月には、上記の政府機関、重要インフラ分野に加え、企業・個人の領域までを含めた我が国初の情報セキュリティに関する国家戦略である「第１次情報セキュリティ基本計画」が決定され、新しい官民連携モデルの構築を目指し、2006 年度から 2008 年度までの３か年における情報セキュリティ政策の明確な道筋が定められた。

さらに、同基本計画の初年度である 2006 年度における実施計画となる「セキュア・ジャパン 2006」も 2006 年６月に決定され、内閣官房をはじめ、各府省庁において、各種施策の展開が図られているところである。

このように、情報セキュリティ政策の積極的な推進が図られる中、同基本計画においては、情報セキュリティ対策の強化が求められる政府機関、重要インフラ、企業、個人という対策実施４領域に加え、これら全分野に跨る課題として、技術戦略の推進、人材の育成・確保、国際連携・協調の推進、犯罪の取締り等、という４つの横断的な情報セキュリティ基盤の形成が求められている。

このうち、人材の育成については、情報セキュリティのみならず、あらゆる分野において課題とされる領域であるが、特に情報セキュリティ対策においては、昨今の政府機関等からの重要情報の漏洩やソフトウェアの設計上の不具合によるシステム障害などの事案からも分かるとおり、他の分野に比べて人的な要素への依存度が高いものと考えられる。

このようなセキュリティ分野における人材の重要性は、何も、情報化がここまで進展した最近になって急浮上してきた考え方ではない。古くは戦国時代の名将・武田信玄が「人は城、人は石垣、人は堀」との言葉を残しており、この名言は、約 450 年を経た現在においても、情報セキュリティ対策強化の根幹が「人」にあることを明示する普遍の真理と考えられる。

こうした認識の下、この度、情報セキュリティ政策会議の下に、情報セキュリティに係る人材の育成方策について幅広く検討を行うための場として、本専門委員会が設置され、2006 年８月から 11 月までの約３ヶ月、全４回に亘って会合を開催し、検討を重ねた。

もとより人材の育成方策については、長期的な視野に立ち、初等中等教育の現場における教育のあり方も含め、国家全体としての育成方策のあり方について検討することが必要となる問題である。
しかしながら、情報セキュリティ対策の向上が喫緊の課題として求められる中、本委員会としては、我が国における現有戦力の速やかな育成を通じた対策レベルの向上を図るため、当面、早期に着手・実行すべき事項について検討を行うという視点に立って検討を行った。

こうした前提の下、本委員会における検討に当たっては、我が国の社会経済活動から学術研究分野に至るまで、当面、およそ情報セキュリティに関わってくると考えられる人材については全て対象として捉え、幅広い範囲の人材について、その現状と課題を検証し、可能な限り必要となる方策について提言すべく、精力的に議論を行ったところである。
４回という限られた時間ながら、本委員会での議論では、各方面の専門家である委員から、多岐に亘り、かつ、多くの示唆に富む意見が示されるとともに、これに基づき活発な議論が行われ、報告書をまとめるに当たっては十分に検討が尽くされたものと確信している。

今回、これら関係者のご知見・ご尽力の下にとりまとめた本報告書は、今後

の我が国の情報セキュリティ政策の「人」の面に関する施策の展開を図る上で極めて有意義なものと考える。ここで、本報告書の作成に多大のご尽力をいただいた関係者各位に深甚なる謝意を表する。

今後、本報告書における提言の内容について、関係省庁や情報セキュリティに係る多くの関係者によって、着実な政策の推進や対策の強化が図られ、我が国の社会経済活動や国民生活などあらゆる分野で IT を安心して利用できる環境の実現に向けた一助となることを期待し、巻頭の言としたい。

2007 年 1 月 23 日
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　委員長
西尾　章治郎

委員名簿

【委員長】

西尾 章治郎	大阪大学大学院教授（文部科学省科学官）

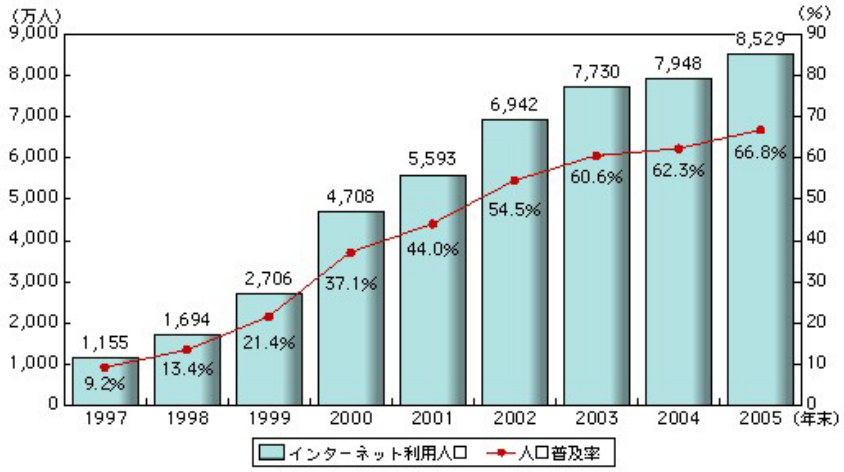
【委員】

有賀 貞一	株式会社 CSK ホールディングス取締役
内田 勝也	情報セキュリティ大学院大学教授
大沢 彰	エヌ・ティ・ティ・コミュニケーションズ株式会社 経営企画部ビジネスモデル推進室 セキュリティ担当部長
筧 捷彦	早稲田大学教授
木内 里美	大成建設株式会社社長室理事情報企画部長
嶋崎 長三	財団法人日本データ通信協会専務理事
関口 和一	日本経済新聞論説委員
田島 優子	弁護士
知地 孚昌	岐阜県総合企画部次長（情報化推進担当）
藤本 正代	富士ゼロックス株式会社シニアマネージャ
真瀬 宏司	株式会社パソナテック取締役会長
松村 博史	独立行政法人情報処理推進機構理事
満塩 尚史	環境省 CIO 補佐官
和貝 享介	監査法人トーマツ

第一章　情報セキュリティに係る人材の育成についての基本的考え方

第一節　情報セキュリティに係る人材の育成の必要性

高度情報通信ネットワーク社会が現実のものとなり、政府機関や企業をはじめとする社会における様々な組織活動や国民生活の多くの場面において、IT 化が急速に進展している（図表１及び２）。



図表１　インターネット利用者数及び人口普及率[1]の動向

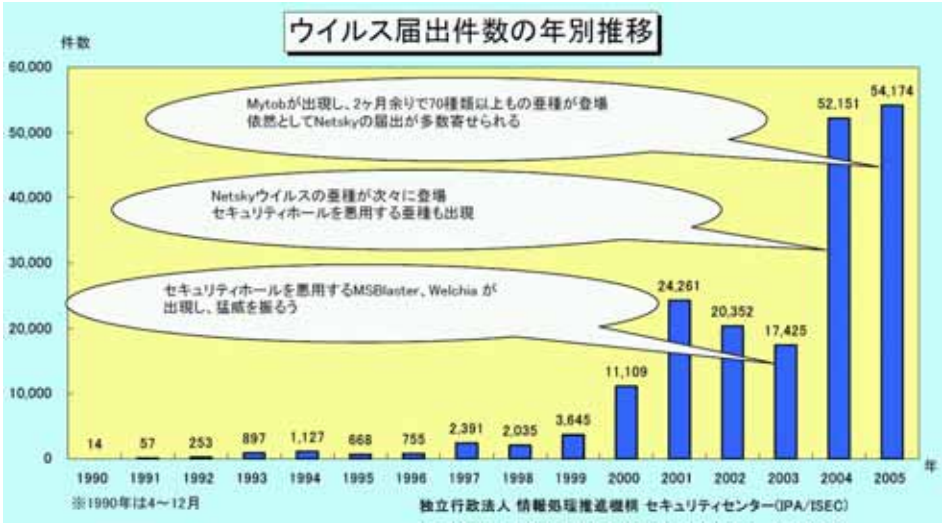
出所：総務省「平成 18 年版 情報通信白書」

図表２　企業におけるインターネット利用の有無

出所：総務省「平成 17 年 通信利用動向調査報告書 企業編」

[1] 過去１年の間に、パソコン、携帯電話、PHS、携帯情報端末、ゲーム機等を通じて利用したインターネットの利用率を指す。

このように、社会全体の IT 化が進展する一方で、高度情報通信ネットワーク社会形成基本法が制定された平成 12 年と比較すると、例えばコンピュータウイルスの届出件数が約 4.9 倍に（図表３）、不正アクセスの届出件数が約 3.6 倍になる（図表４）など、様々な社会経済活動や国民生活において IT を活用する上でのリスク、すなわち情報セキュリティのリスクも急激に増大している。



図表３　コンピュータウイルス届出件数の年別推移

出所：(独)情報処理推進機構「2005 年のコンピュータウイルス届出状況」

図表４　不正アクセス届出件数の年別推移

出所：(独)情報処理推進機構「2005 年コンピュータ不正アクセス届出状況」

こうした中、政府が定めた「第１次情報セキュリティ基本計画」[2]（以下、「基本計画」という。）をはじめとして情報セキュリティ対策の必要性に対する認識も深まりつつあり、政府が進める同計画に基づく様々な施策のほか、企業等の組織などにおいても情報セキュリティの対策が講じられてきている。

組織や個人、さらには国家として何らかの対策を行う場合、その担い手となる人的要素が極めて重要であることは論を待たず、情報セキュリティ対策についても例外ではない。もちろん、適切な情報セキュリティ対策を実施するためには、最先端の技術・製品や、効果的・効率的な組織の管理手法なども必要な要素であるが、これら技術・製品やより高度な管理手法についての研究、あるいはそうした管理手法を実際の組織に適用するには、人による実施・関与が不可欠であり、それぞれの場面に応じた相当のスキルを備えた人材が必要となる。

しかしながら、現時点においては、IT 化の進展のスピードや、これと歩調を合わせるかのように進化･発展する様々な情報セキュリティのリスクに対して、それぞれの場面に応じた相当な能力を備えた人材が十分に確保されている（あるいは、それぞれの場面に対処する人材に対して、十分な能力が確保されている）かというと、心許ないと言わざるを得ない。これは、組織における情報セキュリティ対策をはじめとして、我が国全体として情報セキュリティ対策に着手したばかりの段階であることによるものと考えられる。

こうした中、基本計画に基づく平成 18 年度の実施計画である「セキュア・ジャパン 2006」[3]において、人材育成及び資格制度の体系化に関して検討を行う必要があるとの決定がなされた[4]。本委員会は、これを受け、我が国全体として情報セキュリティ対策を効果的に進めていく上で必要となる人材とはどういった人材か、あるいは、こうした人材に対してどのような能力を求めていくことが必要か、さらにはそうした人材の育成や能力の浸透・醸成を図っていく上で必要となる方策は何か、といった点について検討を行い、可能な限り関係者の指針となるような提言をすることを目指した。

---

[2] 「第１次情報セキュリティ基本計画」（平成 18 年２月２日情報セキュリティ政策会議決定）（参考１参照）

[3] 「セキュア・ジャパン 2006」(平成 18 年６月 15 日情報セキュリティ政策会議決定)

[4] 参考２参照

第二節　本委員会における検討の方向性

前述のとおり、本委員会では、情報セキュリティに係る人材の育成方策等について検討を進めることとしているが、一言で「情報セキュリティに係る人材」といっても、IT 化が進展した現在、情報セキュリティに何らかの形で携わる人材という意味では、行政事務や企業業務をはじめとして、社会経済活動の中でおよそ情報技術に触れる人間であれば、全て含まれると考えることができる。

したがって、我が国全体として情報セキュリティ対策を効果的に進めていく上で必要となる人材の育成方策等を検討するには、「情報セキュリティ職人」とでも呼ぶべき、情報セキュリティを専門的に職務として扱う人材のみを育成することで足りる問題ではない。

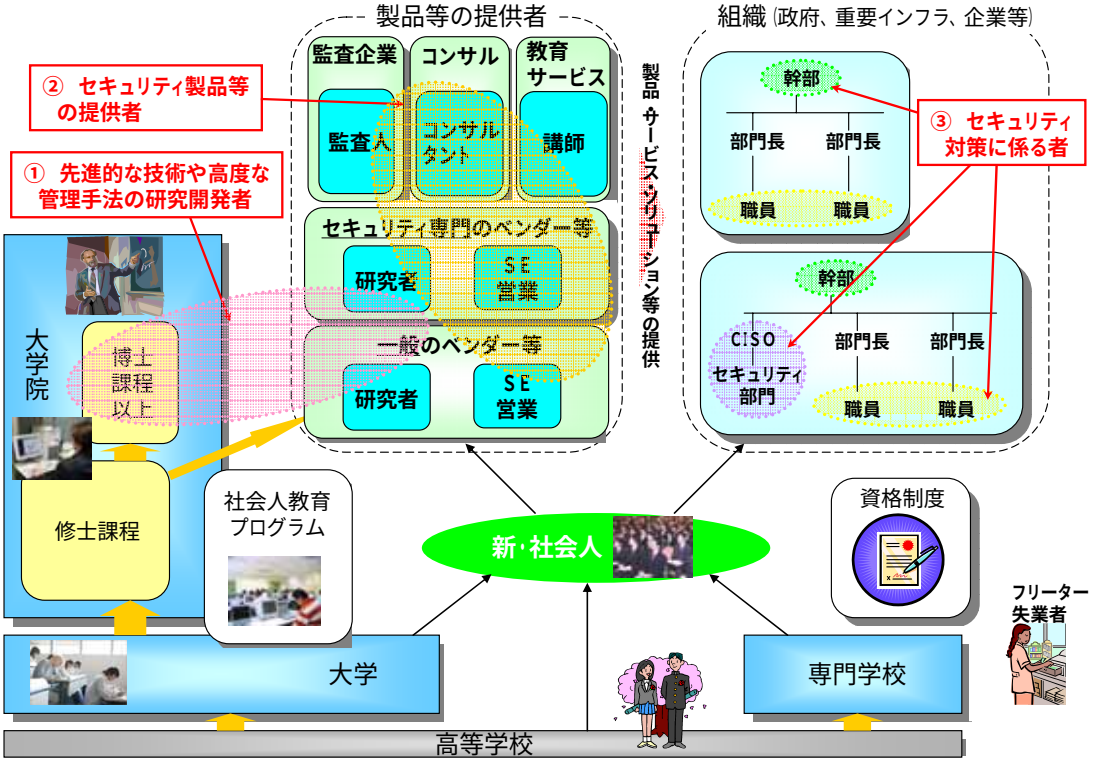
例えば、企業の営業社員であれば、コミュニケーション能力やセールストークのスキルが最も重視されると考えられる。しかしながら、こうした人材であっても、例えばパソコンで顧客情報等を管理していれば、それに伴う情報セキュリティのリスクに対応するための最低限の知識も身につける必要がある。

あるいは、企業における経営者であれば、まずもって経営能力が求められるところに疑いの余地はない。ただ、経営者であっても、企業等の組織における適切な情報セキュリティ対策の推進に当たっては、具体的な経営資源の配置が求められるものであり、そのためには企業経営上必ず存在する情報セキュリティのリスクを明確に認識・理解することが必要となる。

このように、様々な社会経済活動の中で業務を実施する様々なプレーヤーがいる中で、我が国全体として効果的なセキュリティ対策を推進していくためには、情報セキュリティに直接携わる者だけでなく、こうしたあらゆるプレーヤー達の意識や能力（知識、技能等）をどのように確保・向上していくか、といった視点に立って検討を進めることが必要となる。

こうした視点に立ち、本報告書においては、効果的な情報セキュリティ対策を推進する上で関係してくると考えられるプレーヤーとして、大きく
－先進的な情報セキュリティ技術・製品及び高度な管理手法の研究・開発者
－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提供する企業等における人材
－政府機関、企業等の組織において情報セキュリティ対策に係る人材

という３つのカテゴリに分け、それらの人材カテゴリごとに、必要となる対応策の検討を行った（図表５）。



図表５　本報告書における検討のイメージ

その際には、前述のとおり、情報セキュリティに係る人材は多岐に渡り、その育成方策としても、例えば、
－高度な研究の実施
－理論体系の理解
－実習等による技能・実践的手法の習得
－職員研修等によるリテラシーの向上
など様々な手段が考えられることから、育成の対象となる人材やこれに求めるべき能力ごとに、適切な方策を検討することが必要となる。

なお、我が国全体として効果的な情報セキュリティ対策の向上を図っていくためには、小中学校での教育や、一般家庭・個人に向けた啓発など、広く国民一般における知識や意識の向上といったことも必要となってくる。しかしながら、本委員会においては、そこまで対象を広げることとはせず、情報セキュリティに係る人材として、高等教育機関や政府・産業界など、技術の最先端分野や社会組織において情報セキュリティに係る人材を対象にその育成方策を検討することとする。

第三節　報告書の構成

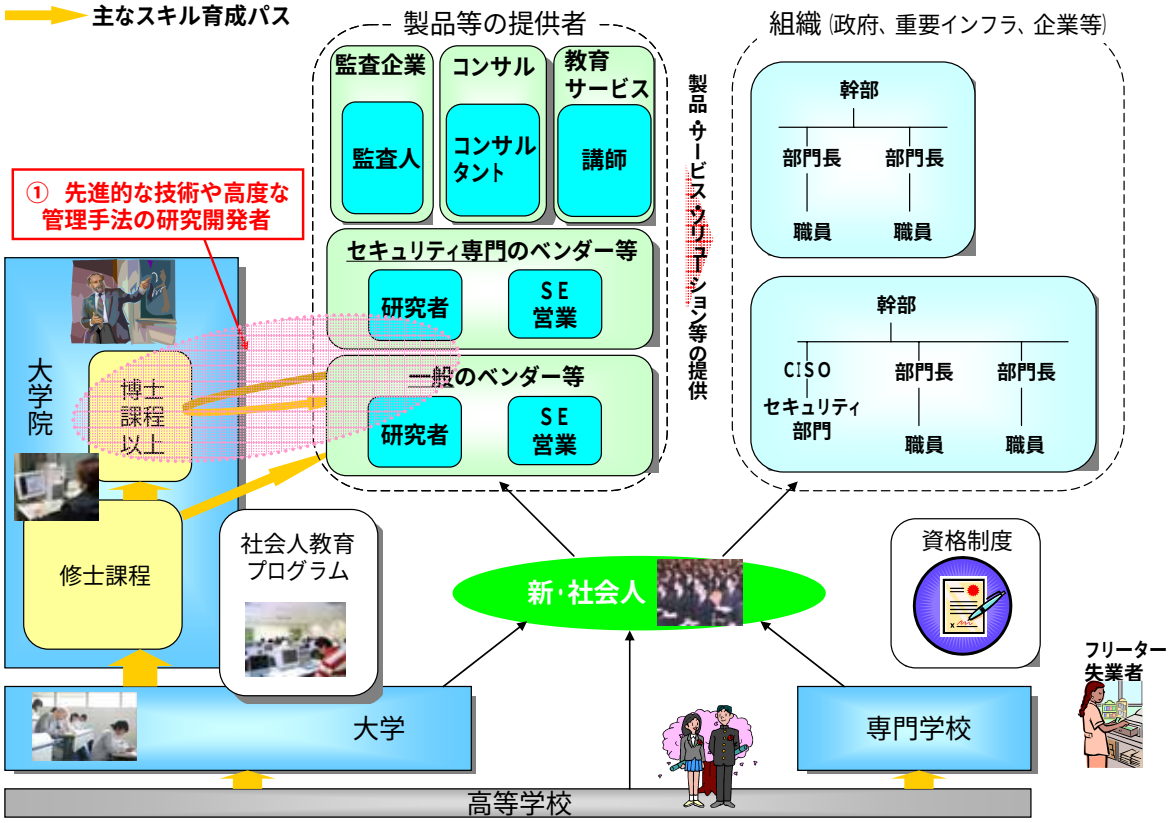
本報告書の構成は以下のとおりである。

まず、第二章から第四章において、前述した人材カテゴリごとに、具体的な人材像、現状と課題、必要となる人材育成方策について検討を行っている。その上で、第五章において、第二章から第四章までの検討を踏まえ、情報セキュリティに係る人材の育成に向けて具体的に実施すべき取組みについて整理を行っている。

第二章　先進的な情報セキュリティ技術･製品及び高度な管理手法の研究･開発者

第一節　具体的な人材像

このカテゴリは、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であり、大きく、技術系の研究・開発者と、管理系の研究・開発者に分けることができる（図表６）。



図表６　第二章における検討のイメージ

第二節　現状と課題

(1)　先進的な情報セキュリティ技術の研究者及び関連製品の開発者

現在、こうした人材は、工学・情報系等の大学院において修士課程を修了した学生が博士課程に進学するか、企業に就職して研究所や開発部門に配属され、

研究や製品開発を行う、あるいは企業研究者が大学院等に派遣されて研究を行うといった形により育成されているのが現状である。

しかしながら、ソフトウェア分野における海外取引額が圧倒的な輸入超過の状況にある[5]など、情報関連分野における我が国の国際競争力は低いといわざるをない。情報セキュリティに関して見ても、市場に流通している製品はほとんどが海外製品であり、研究分野においても暗号など一部の分野を除いて研究水準が高いとは言えない。このため、我が国の技術力の維持向上、国際競争力の強化を図る観点から、セキュリティを含む情報関連分野における研究開発力の一層の強化が求められているところである。

(2) 高度な管理手法の研究者・開発者

従来、我が国においては情報セキュリティに対して暗号技術など技術面などからのアプローチが主となっており、セキュリティ対策を進める上で必須となるこの管理手法の分野における研究・開発の歴史は決して深いものとは言えない。

こうした管理手法について研究・開発を進める大学院大学や米国の有名大学の日本校などが創設されているが、まだ端緒についたばかりとの感がぬぐえないというのが現状である。

第三節 必要となる人材育成方策

真の情報セキュリティ先進国「セキュア・ジャパン」の実現には、我が国全体の情報セキュリティ対策をリードしていくための人材として、こうした最先端の技術の研究者や関連製品の開発者、高度な管理手法に関する研究者等が安定的に育成されていくことが必要である。

他方で、こうした人材は、未開拓の領域を新たに切り開いていくべき人材であり、職場での OJT[6]や、既に体系化された知識や技能を習得する資格制度、社会人教育プログラムといった比較的短期的な育成プログラムで育成方策を論

---

[5] （社）情報サービス産業協会の「2005 年コンピュータソフトウェア分野における海外取引及び外国人就労等に関する実態調査」によると、2004 年におけるソフトウェア輸出額は約 320 億円であるのに対して、輸入額は約 3,646 億円。

[6] On the Job Training：日常業務を通じた教育訓練のこと。

じることは困難である。むしろ、我が国全体の研究開発力・技術開発力の向上といった長期的な視野に立って検討されるべき課題である。

この点、政府においては、「第３期科学技術基本計画」[7]の分野別推進戦略（情報通信分野）の中で、「情報セキュリティ技術の高度化」が盛り込まれ、具体的に以下の２項目が我が国の科学技術政策の重点分野の一つとして位置づけられたことは意義深いものがある[8]。

【課題１】情報セキュリティ技術の高度化

【課題２】技術を補完しより強固な基盤を作るための管理手法の研究

また、文部科学省においては、平成 14 年度から、「大学の構造改革」の一環として、国公私立大学を通じ、優れた研究教育拠点に重点的に支援を行い、世界最高水準の大学づくりを推進することを目的とした「21 世紀 COE プログラム」[9]を実施している。

さらには、その成果を踏まえ、その基本的な考え方を継承しつつ、より重点的な支援により飛躍的な発展を目指す「グローバル COE プログラム」の展開が検討されている。

こうした動きは我が国の研究開発力・技術開発力の向上といった観点から見て歓迎すべき動きであり、引き続き積極的な展開が図られることが求められる。ここで、このような競争的資金の事業の設計・実施に当たっては、単に資金を各大学に配分するといった形ではなく、国公私立を通じた競争的な環境の中で、研究者が大学における研究以外の業務等に追われず、自らの研究に専念できる環境の整備や、国内外の優れた研究機関との連携、海外からの研究者の招聘の促進など、真に我が国の研究開発・技術開発分野における国際的競争力の向上につながるよう、多角的な観点から検討がなされなければならない。

特に、情報セキュリティは、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。このため、情報セキュリティに関する研究開発力の強化・向上のためには、こうした幅広い領域における研究開発力の底上げと、相互の連携を図っていくことが必要となる。

---

7 「第３期科学技術基本計画」（平成 18 年３月 28 日閣議決定）

8 参考３参照

9 http://www.jsps.go.jp/j-21coe/参照

この点、例えば大阪大学情報科学研究科において、国際的かつ学際的視野を有し、世界各国の技術者や研究者らを強いリーダーシップをもって率い、共同研究開発等の国際的連携を成功に導くことを可能にする優秀な人材の育成を目的として、米国カリフォルニア大学サンディエゴ校（UCSD）をはじめとする生命科学との融合領域を重視する拠点的な大学に数ヶ月間に及び学生を派遣するインターシップ制度を確立するといった新たな取組みもなされている。今後は、こうした創意工夫に満ちた研究者育成方策が各大学の自主的な発案により展開されていくことが期待される。

なお、本委員会の中では、中国、インド、韓国、ブラジルなどの諸外国においていわゆるエリート教育政策により高度な IT 人材の育成が図られていることを踏まえ、我が国においても優れた研究・開発者の育成のために、従来の高等教育の枠組みを越えたいわゆるエリート教育政策についても検討すべきではないかという意見も示された。

他方で、この点に関しては、前述の「21 世紀 COE プログラム」等の競争的資金の導入により、各大学院が大学院間や産業分野との連携を図るなど、従来の教育の枠組みを越えた様々な創意工夫を展開するような動きが活発化してきており、こうした状況を踏まえれば、現行の大学院における競争を促進することで、ある程度目的は達成されるのではないかといった指摘も示された。

また、その他にも、

－横並び的な考え方の強い我が国において、従来の教育の枠組みを越えたいわゆるエリート人材を育成し、こうした人材がその他大勢の国民をリードするという国家像に対して国民的合意形成を得ることができるかどうか、慎重な判断を要すること

－従来の教育の枠組みを越えたいわゆるエリート教育の枠組みを新設したとしても、５年程度で成果が出るものではなく 10 年から数十年単位を成果の範囲として捉える必要があること、また、育成した人材の全てが、望まれるエリート人材として確実に育成できる訳ではなく、何十人かに一人、場合によっては成果というべき人材が出ないかも知れないというリスクを認識した上で推進する必要があること

－こうした人材の育成については、単に教育体制の問題だけでなく、これらの高度な教育を受けつつも研究・開発の道に進まなかった人材がビジネスの分野で活躍することができ、高度な研究・開発分野とビジネス分野との循環が促進され、ビジネス分野そのものの質の向上やこれらの人材のビジネスマイ

ンドの向上に繋がるよう、企業における人材採用方針なども含めた社会的な環境の整備も併せて必要になること

といった、様々な論点が示されたところである。

いずれにしても、我が国の将来を担う先端的な人材の育成のあり方については、情報セキュリティ分野に限定して検討するべき問題ではなく、政府において新たに設置された「イノベーション 25 戦略会議」や総合科学技術会議での議論や、第３期科学技術基本計画における科学技術関連の幅広い人材育成に係る方針を踏まえ、関係府省において速やかな対応がなされることが期待される。

第三章　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提供する企業等における人材

第一節　具体的な人材像

このカテゴリは、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（以下「製品等」という。）をビジネスとして提供する企業等における人材であり、大きくは、
－技術系の製品等を提供する企業等における人材
－管理系の製品等を提供する企業等における人材
に大別される。

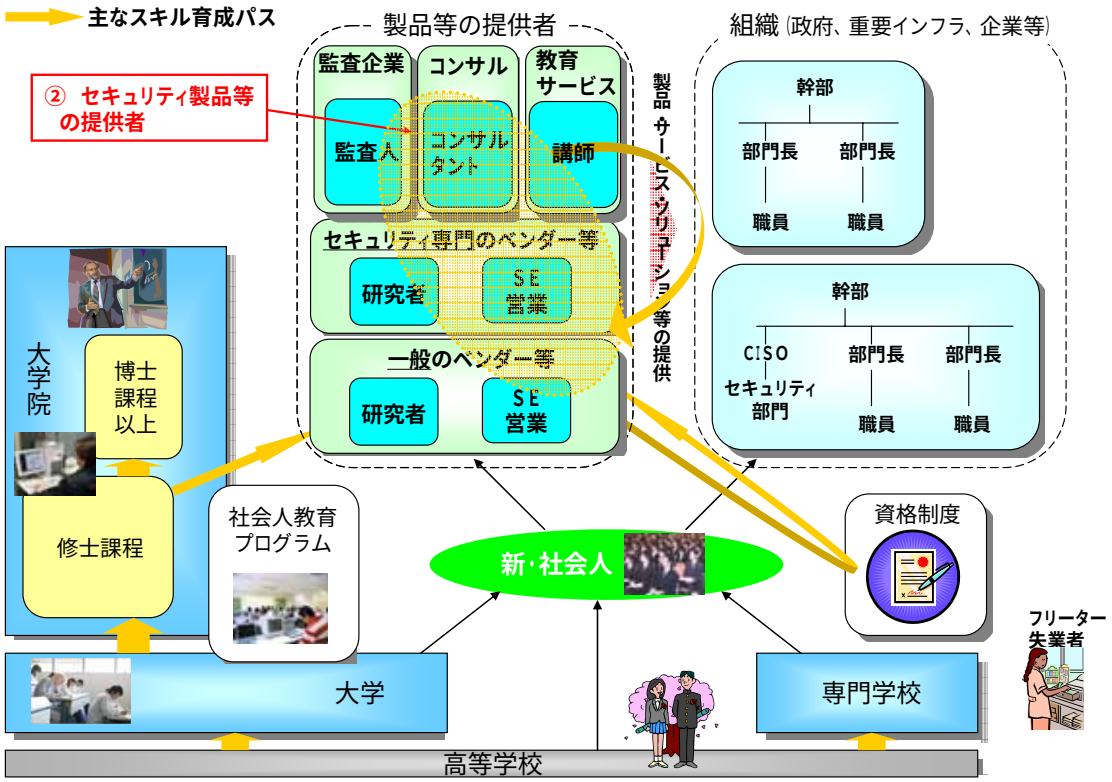
技術系の製品等を提供する企業等における人材としては、セキュリティ製品等を専門的に扱うベンダー[10]やシステムインテグレータ[11]（以下「ベンダー等」という。）における技術者が挙げられるほか、一般のベンダー等、すなわち、セキュリティを専門としないベンダー等も対象として捉えなければならない。これは、セキュリティを専門としないベンダー等であっても、顧客企業等からの依頼を受けて情報システムを提供するものであり、この情報システムに大きなセキュリティ上の欠陥があれば、結果として顧客企業の情報セキュリティ対策に大きな脅威を招来することになるためである。

また、管理系の製品等を提供する企業等における人材としては、コンサルティング会社におけるコンサルタントや情報セキュリティ監査を行う企業において業務に従事する者、顧客企業等の一般社員に対して情報セキュリティ教育を実施する教育サービス企業におけるプログラム設計者などが挙げられる。

これらの人材は、我が国全体としての情報セキュリティ対策レベルの向上に資するため、顧客企業等に対してより品質・信頼性の高い製品等を提供するために必要となる能力の確保が求められる。

---

10 本報告書では、情報技術関連の製品を販売する者を指す。
11 本報告書では、顧客から、情報システムの企画、構築、運用などの業務を一括して請け負う事業を営む者を指す。



図表７　第三章における検討のイメージ

第二節　現状と課題

(1)　技術系の製品等を提供する企業等における人材

ア　セキュリティ製品等を専門的に扱うベンダー等における人材

情報セキュリティ対策を実施する組織にとっては、アンチウイルスソフトウェアなど市場で提供されるセキュリティ製品に対する依存度が一般的に非常に高く、我が国の情報セキュリティ対策の維持・向上のためには、こうした製品の品質・信頼性の確保が非常に重要な要素となってくる。

こうしたセキュリティ製品等を専門的に扱うベンダー等においては、昨今の情報セキュリティ対策需要の急激な高まりを受け、大きく業績を拡大してきている。こうした企業においては、セキュリティそのものを商品としているため、日々情報セキュリティに関する技術や脅威の形態が進化する中で、企業間競争を勝ち抜くため、各社の技術者の育成等を行っているところであり、今後も市場原理の中で人材の育成が行われていくものと期待される。

ただ、その際には、最新の技術動向等について理解することも必要であるが、

普遍的な原理としての情報セキュリティの基礎・本質についても理解をする必要があること、また、第一章でも述べたとおり、情報セキュリティの周辺領域も含めた幅広い事項について知識・技能を習得する必要があることに留意が必要である。

また、過去には、アンチウイルスソフトウェアを製造・販売するセキュリティ専門のベンダーでありながら、配信したパターン・ファイル[12]の不具合により、顧客側のシステムに大規模な障害を引き起こしてしまった例などもあるが、製品等を提供する側の企業においては、万が一にもこうしたトラブルが起こることのないよう、製品の品質管理や、それに必要となる人材の育成や体制の整備の徹底を図ることが求められる。

さらに、ここで例示した企業は、自らの組織における情報セキュリティ対策についても、情報漏洩やシステム障害などを起こしている。これらの問題は、製品等の提供者としての立場に関わってくるものではないが、セキュリティ製品等を専門的に扱うベンダー等は、本来、顧客企業の範となるべきことを踏まえれば、一般の企業以上に、社員の教育や品質管理のための体制の整備を図ることが望まれる。

イ　一般のベンダー等における人材

次に、セキュリティを専門としないベンダー等においては、第一節で述べたとおり、顧客企業等から依頼を受けて情報システムを提供するものであり、この情報システムに大きなセキュリティ上の欠陥があれば、結果として顧客企業等の情報セキュリティに大きな脅威を招来することになる。このため、本来であれば、その技術者に対し、製品等を製造・提供するに当たって必要となる最低限の情報セキュリティに関する能力を身につけることが必要である。

しかしながら、こうした企業においては、Web 技術の普及をはじめとした情報システムのオープン化の流れに伴うプログラミングの汎用化により、セキュアプログラミング技法[13]に対する理解や意識のないプログラマが増加してきており、その結果として、バッファ・オーバーフローなどのセキュリティホールをいくつも抱える脆弱なソフトウェアやそれを搭載するシステムが製造・提供され、社会の様々な場面で運用されているというような事態も招いている。

---

12 アンチウイルスソフトウェアがコンピュータウイルスやワームを検出するために使う、コンピュータウイルス等の特徴を記録したファイルのこと。

13 セキュリティ上の脆弱性を持たないようにプログラミングを行う技法のこと。

このため、こうした一般の（セキュリティを専門としない）ベンダー等における技術者に対しても、例えば、ソフトウェアを開発する技術者にとってのセキュアプログラミング技法や開発したプログラムの脆弱性を点検する製品の活用方法等、製品等を製造・提供するに当たって必要となる最低限の情報セキュリティに関する能力を広く身につけさせるための方策について検討を行う必要がある。

また、最近では、顧客企業等の情報システムがオフィス機器やネットワークと一体化していく中で、オフィス機器ベンダーから派遣されてプリンタなどのオフィス機器の設定・修理等に従事する者や、通信事業者から派遣されて通信回線の設定に従事する者など（以下「フィールド・サービス・エンジニア」という。）が、顧客企業等からの情報セキュリティ対策に関する細かなニーズに対する最初の窓口として各種の相談やニーズに応えつつあるところである。

これらフィールド・サービス・エンジニアの情報セキュリティに関する知識・技能の向上を図ることが、顧客企業等における情報セキュリティ対策の向上に広く繋がるとも考えられる。

ウ　地方において情報セキュリティに関する製品等を提供する企業における人材について

我が国全体を考えた場合、地方において情報セキュリティに関する製品等を提供する企業等における人材及びその能力の確保という点も一つの課題である。現在では、主に需要の規模の問題からセキュリティ専門のベンダー等は東京など大都市圏に集中しており、各地域では、セキュリティに関する最新の製品等の提供を受けることが容易ではない。また、各地域における一般のベンダー等においても、その技術者等にセキュリティに関する最新の知識等を身につけさせようとしても、相応しい教育プログラムの利用機会が乏しいのが現状である。こうしたことから、今後、地方において情報セキュリティに関する製品等を提供する企業における人材とその能力をどう確保していくかという点も大きな課題である。

(2)　管理系の製品等を提供する企業等における人材

ア　情報セキュリティに関するコンサルティングや監査サービスを提供する企業における人材

情報セキュリティに関するコンサルティングや監査サービスを提供する際には、顧客である企業等の組織が実施する情報セキュリティ対策の全般について助言や監査を行うことが不可欠であり、情報セキュリティポリシーといった規程類の策定状況や、顧客組織内の情報セキュリティ対策の体制など、表面的な事項の検査を行うことだけでは十分とはいえない。

したがって、こうしたサービスを提供するにあたっては、コンサルティングや監査に必要不可欠な指導的・批判的な視点・能力を有する人材が必要となるのはもちろんのこと、情報セキュリティに関する最新の技術動向についてもある程度の知識を有する人材が必要となってくると考えられる。また、業務管理の面から各種法令や人事・労務管理の分野に関する知識を有する人材も必要になってくると考えられる。すなわち、情報セキュリティに関するコンサルティングや監査サービスを提供する企業にとっては、こうした幅広い知識等を持つ人材を幅広く、かつ、バランスよく育成・確保することが必要である。

このような状況を踏まえ、民間団体等においては、例えば我が国の情報セキュリティ監査制度に則した標準的な監査手法・監査技術の検討や、監査人の専門的知識などが一定水準以上であることを担保する資格制度の構築などの取組みが行われている。また、倫理的な側面を含め、一定品質以上のコンサルティングや監査サービスを提供するための基本的な知識や実習を行う研修等も実施されている。さらには、大学院等の高等教育機関においても管理手法等に関する教育課程が提供されつつあるところである。

加えて、情報セキュリティに関するコンサルティングや監査サービスの提供に際しては、顧客企業等の事業内容、規模等によって異なってくるニーズに的確に対応する能力も必要である。こういった能力については、実務経験を積み重ねることによって得られる場合が多いことから、各企業等が OJT で対応しているのが実態である。

イ　情報セキュリティ教育ビジネスの拡大について

第四章で述べる日本経団連企業におけるアンケート結果を見ると、顧客企業における人材育成方策として、外部のセキュリティ教育サービスに対する期待も大きい。このため、今後はこうした教育ビジネスの拡大が期待されるとともに、教育サービスを提供する企業には、顧客企業等に対して適切な教育プログ

ラムを提供することが求められる。

第三節　必要となる人材育成方策

(1)　技術系の製品等を提供する企業等における人材について

ア　企業等における社内の計画的な人材育成プログラムの必要性

第二節で述べたとおり、セキュリティ製品等を専門的に扱うベンダー等においては、顧客企業等の情報セキュリティ対策が、その提供する製品等に大きく依存していることを十分に認識し、製品の品質管理や、そのために必要となる人材の育成や体制の整備の徹底を図ることが求められる。

また、一般の（セキュリティを専門としない）ベンダー等においては、その技術者に対して、例えば、ソフトウェアを開発する技術者にとってのセキュアプログラミング技法や開発したプログラムの脆弱性を点検する製品の活用方法等、製品等を製造・提供するに当たって必要となる最低限の情報セキュリティに関する能力を身につけることを推進していく必要がある。

ここで、特に一般のベンダー等においては、目先の利益を追求し、多重階層化の外注構造の中で、内製力を失った技術空洞化現象が起きていており、こうした技術系の製品等を提供する企業において計画的な人材育成プログラムが策定されていない傾向が強い。

このため、これら企業には、情報システムを提供する上での社会的な責任を自覚し、一定の品質・信頼性が確保された製品を提供できるよう、技術者に必要なスキルを整理した上で、各種の資格制度や社会人教育プログラムなどを活用しつつ、計画的に技術系人材の育成を図ることが求められる。

また、先に述べたオフィス機器ベンダーや通信事業者においても、そのフィールド・サービス・エンジニアに対して、資格制度等の各種教育プログラムの活用を通じた情報セキュリティ知識・技能の定着を図ることにより、顧客企業等の現場における情報セキュリティ対策に関する細かなニーズに対応し、広く企業等における情報セキュリティ対策の向上に貢献することが期待される。

イ　教育プログラムの充実について

前述の通り、各企業における計画的な人材の育成が必要となることに加え、こうした企業が人材を育成しようとした場合に、既に企業にいる技術者が社会人教育として実践的にこれらの知識・技能を身につけることや、こうした企業に就職するであろう学生が就職後に即戦力として働けるように、大学課程において同様の知識・技能を身につけることが可能となるような教育プログラムの充実が必要となる。

この点、財団法人等において、社会人等が実践的な技法等を習得できる総務省の補助事業を活用した教育プログラムを展開しているほか[14]、一部の大学において、科学技術振興調整費プロジェクトを活用し、学生と社会人双方の技能向上を目的とした教育プログラムを実施してきており[15]、一定の成果を上げてきている。

特に、後者の中には、社会人と学生が共同でネットワーク等における実践的研修を行う中で、社会人の経験から実際の企業におけるネットワーク現場の課題などについて学生が直接学ぶ機会を持つことができるなど、産学間での有効な情報・知識の交換に繋がった例もある。

ただし、これら大学における教育プログラムについては、既に終了したものもあれば、2008 年度において終了するものもある。このため、国として、引き続き、こうした社会人の実践的な技能研修のプログラムの展開に対する支援が求められる。

具体的には例えば、今年度から文部科学省で実施している、産学連携の下での先導的 IT スペシャリスト育成推進プログラムについて、情報セキュリティ技能への発展を図るといった方策が考えられる。

また、現在、各種の情報セキュリティ資格が提供されているが、これらの資格は、いわゆる「情報セキュリティ（技術）のプロフェッショナル」としての資格がほとんどである。そのため、一般のベンダー等の技術者が情報セキュリティに関する最低限の知識を身につけるためにアラカルト的に選択することのできる資格の創設や、一般的なプログラマ資格をはじめ、情報技術に関する一般的な資格において情報セキュリティの要素を追加・拡大することなどが期待される。

---

14 ＜資料１＞参照
15 ＜資料２＞参照

ウ　地方においてセキュリティに関する製品等を提供する企業における人材

我が国全体での情報セキュリティ対策の必要性について考えると、各地域において情報セキュリティに関する製品等を提供する企業等における人材やその能力の確保も大きな課題である。

ここで、セキュリティ製品等を専門的に扱うベンダー等といった企業については、必ずしも各地方における需要規模が大きいとは考えにくいため、その振興方策等を検討するのは容易ではないと考えられる。

他方で、地方においても、地方公共団体や企業など、情報セキュリティ対策を求められる組織は多数存在しており、これらの顧客に対して情報システムの構築等を手がける一般のベンダー等の情報セキュリティに関する知識や技能が、地域における行政サービスや企業活動における品質・信頼性に直結することにもなる。

特に、情報セキュリティ対策は、情報システムを構築して終了するものではなく、その後の定常的な運用の中で常時対応が求められる性質のものであるため、地方公共団体や企業の情報システムの維持管理等に携わる地域に密着したベンダー等には、これら最低限の知識・技能を身につけた人材を育成・確保することが求められる。

この点、現在では、景気の拡大に伴って IT 人材に対する需要も高まる中、地方の大学を卒業した理工系の学生が東京など大都市圏のベンダー等に就職し、各地域のベンダー等が必要な人材を確保することが困難になっている面もある。

こうした中、岐阜県や兵庫県など地方においても、国の補助事業を活用しつつ情報セキュリティに関する技術面や管理面に関する実践的な研修を受けることのできる拠点の整備が進んできており、今後は、こうした拠点における育成プログラムなどを最大限に活用しながら、各地域に密着したベンダー等における人材の情報セキュリティに関する能力の向上が図られることが期待される。

なお、ここで紹介した事例においては、既に他の事業で展開中のカリキュラムを活用して事業展開を行っている[16]。このように、各地方における教育プログラムの実施に当たっては、既存の教育プログラムの成果などを極力活用し、

16 岐阜県の（財）ソフトピアジャパンにおいては横須賀テレコムリサーチパークにおいて展開中のカリキュラムを、兵庫県の（財）ひょうご情報教育機構においては大阪大学で実施された人材育成プログラムのカリキュラムを活用している。

できるだけ低コストで展開されることが望ましい。

また、地域によっては、地方公共団体が主体となって、フリーターや失業者に対する IT スキル育成研修プログラムを設け、カリキュラムの策定から採用に至るまで地元の情報産業界と連携し、フリーター・失業者の雇用対策、地元 IT 産業の育成、労働力の配置転換といった複数の課題を解決するための事業を展開し、一定の成果を上げているところもある。

さらには、人材派遣会社と連携して、資格の取得件数や受講者数といったいわゆるアウトプットの目標だけでなく、結果として実際に IT 企業へ就職した人数などのアウトカムに相当する目標を成果目標として定めた IT 人材育成プログラムを展開している例もある。

このように、具体的な人材の育成方策としては、単に育成拠点といったハードの整備に留まらず、当該拠点において育成された人材が、地元企業や社会のニーズに沿った形で企業への採用に至るといった実効ある施策の展開が期待される。こうした方向に向け、地方公共団体や各地域の情報産業団体、さらには人材の育成や就職に関するノウハウを有する企業など、関係者が知恵を寄せ合いながら、各地域の実情に応じた様々な検討がなされることが望まれる。

エ　その他

なお、本委員会においては、ソフトウェアの安定した品質とその向上を図るためには、知識レベルを問う資格制度に加えて、実務試験等を加味しつつ、これを取得した者でなければ一定のソフトウェア構築をしてはならないという、いわば建築士のような資格制度の導入についても検討すべきではないかという意見が示された。

この点、ソフトウェアサービスが提供されるようになってから数十年が経っている中で、いまだに品質管理や信頼性向上が十分に図られていない現状を踏まえれば、積極的に検討すべきだとする意見がある一方で、大幅な規制強化になることや、外国企業にとっての参入障壁となることに対する懸念、発注者側のユーザ企業の技術レベルの向上を図ることを進めるべき、といった反対の意見も示された。

この問題は、本委員会の役割である人材育成方策というよりは、情報システムやソフトウェアの品質の確保・信頼性の向上といった観点から、必要となる

枠組みはどうあるべきかといった議論の中の一つの方策として検討がなされるべきである。このため、本委員会において結論を示すことは控え、関係者において、前述の指摘事項を踏まえつつ、議論がなされることを待つこととする。

(2)　管理系の製品等を提供する企業等における人材について

ア　情報セキュリティに関するコンサルティングや監査サービスを提供する企業における人材

第二節に述べたとおり、情報セキュリティに関するコンサルティングや監査サービスを提供するにあたっては、幅広い知識・経験のみならず、最新の技術動向に関する知識や顧客企業のニーズに応じた的確な対応能力などの極めて幅広い能力を有する人材をバランスよく育成・確保することが必要である。このため、コンサルティングや監査サービスを提供する企業の人材育成に際しては、企業内等での OJT に加えて、必要に応じて各民間団体等で取り組まれている資格制度、研修等や、大学院等の高等教育機関での教育課程等を活用することが有効であると考えられる。

現時点においては、企業内等での OJT や民間団体等による人材育成に関する取組みが一定程度機能していると考えられるため、これら取組み等の動向を注視していくことが適当であるが、こうした各資格制度や研修等は、情報セキュリティの技術変化や社会変化による監査ニーズの変化に適切に対応していくことが不可欠であるため、その充実に向けた民間団体等の不断の努力が期待される。

なお、米国においては、この種の業務に従事する者同士が交流するためのコミュニティが形成され、能力・知見の向上を目的とした情報交換等が行われており、一定の成果を上げている。我が国においても、関係者における同様のコミュニティの形成が図られつつあり、こうした交流が更に深まり、引き続き活発な情報交換等が行われることが重要であると考えられる。

イ　情報セキュリティ教育サービスを提供する企業等に期待される役割

今後拡大が期待される教育ビジネスにおいては、主に顧客企業の幹部や一般社員向け教育をターゲット・マーケットとして捉えることになると考えられる。このため、そのカリキュラム等の設計に当たっては、幹部向けにリスクの認識・

理解の浸透や、一般社員向けに次章第二節に述べるセキュリティリテラシーの確実な定着を図るという観点が必要不可欠である。なお、その際には、政府機関における情報セキュリティ教育用資料が公開されれば、それを参考にすることも一案として考えられる。

また、こうした外部の教育メニューに期待する企業のニーズをくみ取り、大学院等においても、文部科学省の先導的 IT スペシャリスト育成推進プログラムのように、産学連携を図ることにより、産業界のニーズと大学のシーズを適切にマッチングさせた体系的な教育プログラムを提供することが望まれる。

第四章　政府機関、企業等の組織において情報セキュリティ対策に係る人材

第一節　具体的な人材像

(1)　組織において情報セキュリティ対策に係る人材

このカテゴリは、政府機関や企業など、何らかの業務目的をもって行動する組織において、情報システムを利用している場合に、当該情報システムに起因する情報セキュリティの脅威に対する対策を講じることとなる人材である。

具体的に、こうした組織における情報セキュリティ対策を考える上では、大きく以下の人材を視野に入れて考えなければならない。
－幹部、経営者
－一般職員・社員
－情報セキュリティ対策を担当する者

こうした対策を実施しなければならない組織としては、社会全体の IT 化の進展に伴って、現在では政府機関や地方公共団体、企業などあらゆる組織が関係してきており、例えば政府機関であれば、各府省庁によってその政策・行政目的、規模なども異なり、企業であれば、事業内容や規模などによっても様々である。このため、我が国全体の情報セキュリティ対策を考えた場合、このカテゴリの人材が最も広範囲に渡ると考えられる。

そこでここでは、まずは大きく「政府機関」と「民間部門」に分け、それぞれについて前述の３カテゴリの人材の現状と課題、必要となる人材育成方策について検討を行った（図表８）。

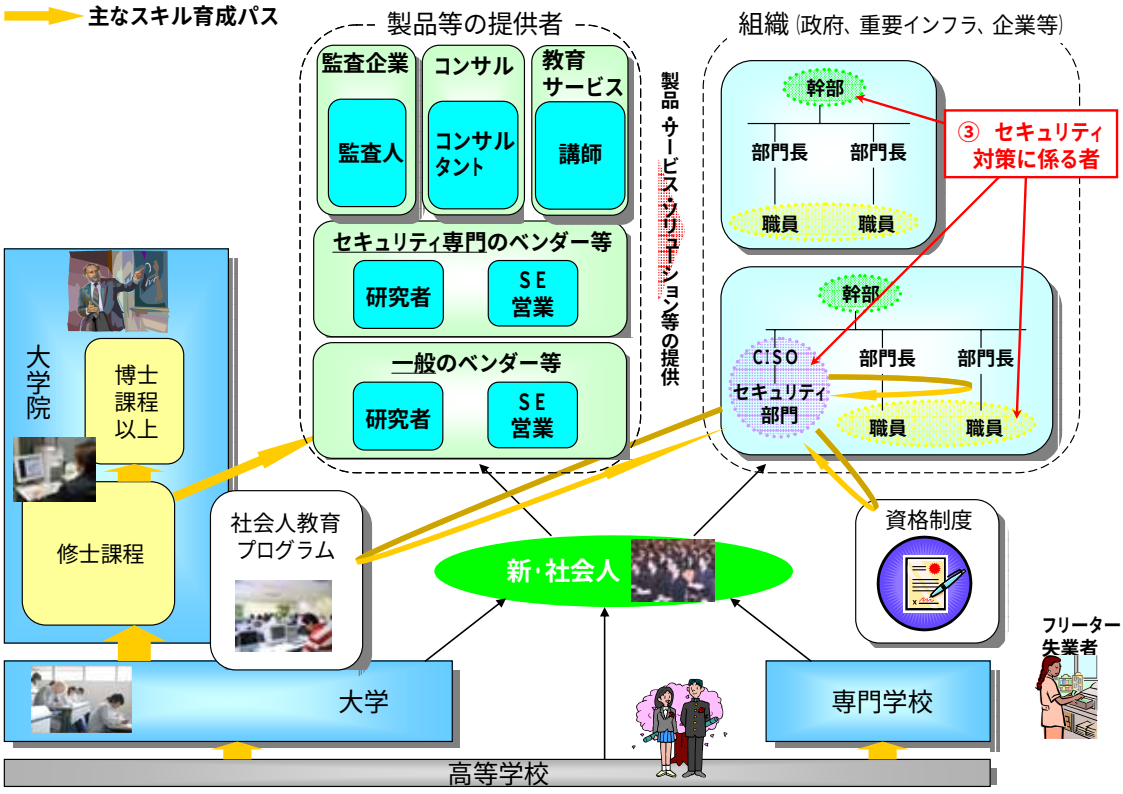
(2)　留意すべき事項

こうした組織における情報セキュリティ対策を実施する上で、考慮しなければならないのは、次の二点である。

第一に、政府機関や企業等の組織は、本来、政策目的の実現や、利益・企業価値の最大化といったことを目標として行動するための組織であり、情報セキュリティ対策のために存在している組織ではない。このため、こうした組織に

対して闇雲に情報セキュリティの必要性を訴えても、一義的には優先度の低い課題としてとらえられてしまうということである。このため、特に各組織の幹部等に対しては、本来の政策目的や企業目的の実現に向けて、なぜ情報セキュリティ対策が必要かということを的確に示す必要がある。

第二に、組織における情報セキュリティ対策は、各企業がそれぞれの顧客や社会との関係といった社会的責務とこれに対するリスクを十分に分析した上で、必要となる製品等を導入すべき問題だという点である。この点、現在では、セキュリティに関する製品等を提供する企業等から一定のパッケージ化された製品等に関する説明を受け、自らの組織における十分なリスク分析等を行うことなく導入する例が多いと推測されるが、こうした対策では、費用をかけても十分な効果に繋がらないということについても留意することが必要である。



図表８　第四章における検討のイメージ

第二節　政府機関等における現状と課題、必要となる人材育成方策

(1)　現状と課題

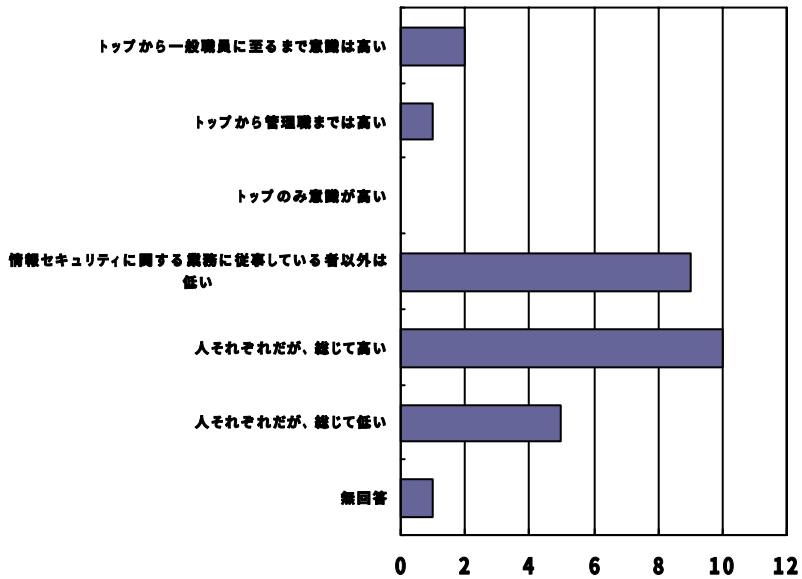
本委員会においては、政府機関における情報セキュリティに係る人材の現状について把握するため、平成 18 年８月から９月にかけ、実態調査を行った。

調査結果の詳細は、＜資料３＞のとおりであるが、大要、以下のとおりである。

（組織における意識の現状）

・組織全体の情報セキュリティに関する意識については、「人それぞれだが、総じて高い」という回答が最も多く、この傾向は、次節で述べる日本経団連の企業アンケートと似ているといえる。しかしながら他方で、セキュリティ意識の高い職員のカテゴリについて見ると、企業においては「トップから一般職員に至るまで意識は高い」との回答が高かった一方で、政府機関においては、「情報セキュリティに関する業務に従事している者以外は低い」の割合が高く、企業に比べると、政府機関においては、幹部をはじめ一般職員の意識は比較的低く、情報セキュリティ担当者のみが意識が高いという状況にあることがうかがえた（図表９）。

＜資料３の Q01、資料４の Q15 の調査結果を参照＞



図表９　情報セキュリティに関する意識の現状

（専任職員・外注職員の配置状況）

・「情報セキュリティに関する業務を専任で担当する職員が配置されている」と回答した府省庁は全体の４割程度であり、２～３名規模の場合が多かった。また、全体の約半数の府省庁が情報セキュリティに関する何らかの業務について、外注要員を活用しているとの回答であった。専任の担当職員（公務員）と外注職員が従事している業務の内容を見ると、前者はセキュリティマネジメントや情報セキュリティ監査などの管理系の割合が高く、後者はネットワークやアプリケーションのセキュリティ、運用・緊急時対応など、技術系の割合が高いことが分かる。

＜資料３の Q02、Q03、Q04、Q05 の調査結果を参照＞

（資格制度の活用について）

・資格制度の活用状況については、調査期間が短かった為、十分な調査が困難であったという事情もあるが、情報セキュリティ業務の担当職員の中に資格取得者（独自資格を含む）を有する府省庁は全体の 1/4 程度であった。また資格取得者を有する府省庁においても人数的には１～２名程度にとどまる。

・資格制度に対する評価としては、「よくわからない、無回答」が圧倒的に多く、政府機関における資格制度活用に対する関心の低さがうかがえる結果となった。

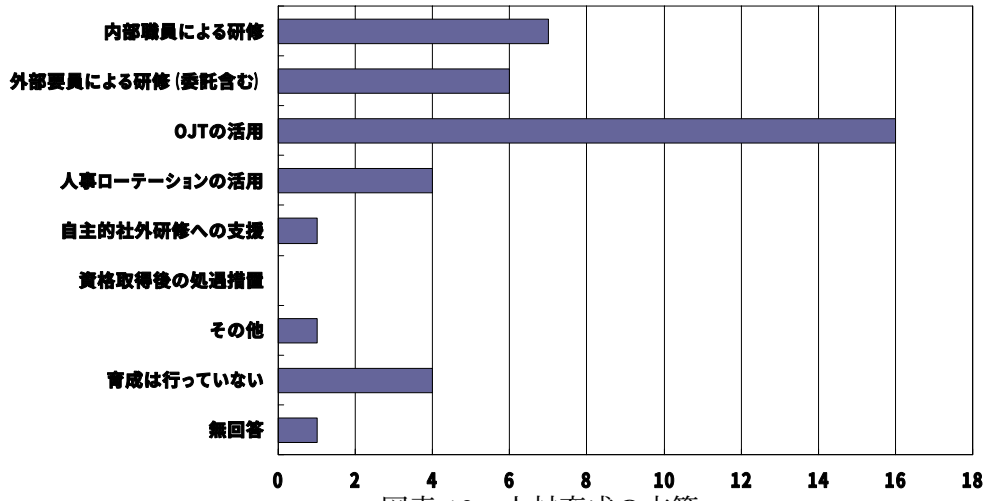
＜資料３の Q06、Q07、Q08、Q09、Q10 の調査結果を参照＞

（人材の育成と確保の状況）

・政府機関における情報セキュリティ人材の育成（内部での育成）の方策としては、圧倒的に「OJT の活用」の割合が高い（図表 10）。

・また、人材の確保（外部からの調達）の方策としては、「業者への外注」への割合が高く、非常勤職員の採用の割合は低い。

＜資料３の Q12、Q14 の調査結果を参照＞

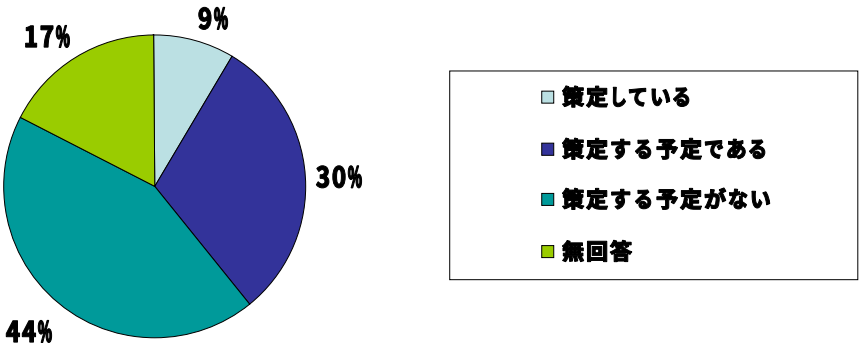


図表 10　人材育成の方策

（人材計画の策定状況）

・こうした状況の中、情報セキュリティ人材の育成・確保のために「人材計画を策定している」又は「策定する予定である」と回答した府省庁は全体の４割程度であった（図表 11）。

＜資料３の Q16 の調査結果を参照＞



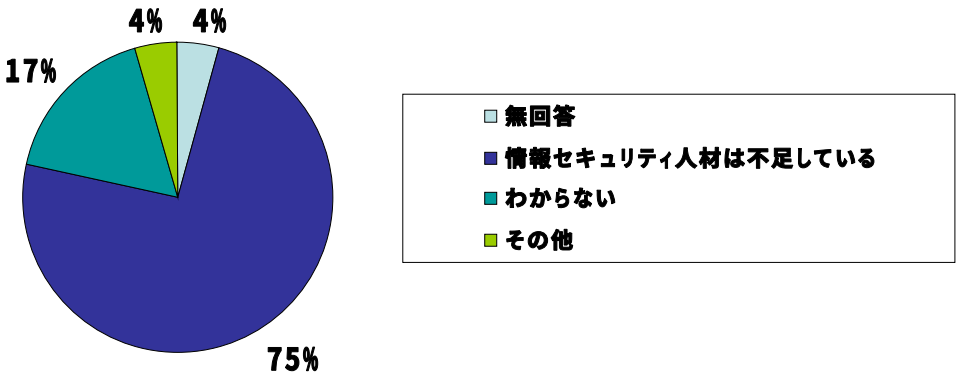
図表 11　明文化された人材計画

（人材の充足感）

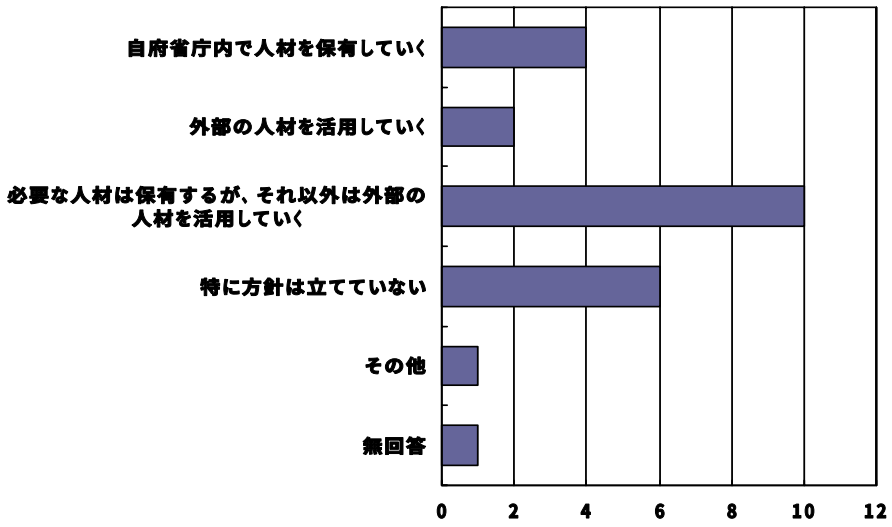
・情報セキュリティ業務を担当する人材の充足感については 3/4 の府省庁が「情報セキュリティ人材は不足している」、1/5 の府省庁が「わからない」との回答であり、充足していると感じている省庁の割合は低い（図表 12）。

・その上で、人材をどのように育成・確保していくかという点については、「必要な人材は保有するが、それ以外は外部の人材を活用していく」の割合が最も高かった。この点、次節で述べる企業アンケートにおいては、「社内における既存の人材を育成する」が 86%と、内部の人材を育成しようとする意向が強く、政府機関においては、企業とは異なり、外部人材の活用に前向きであることがうかがえた（図表 13）。

＜資料３の Q16、Q19 の調査結果を参照＞

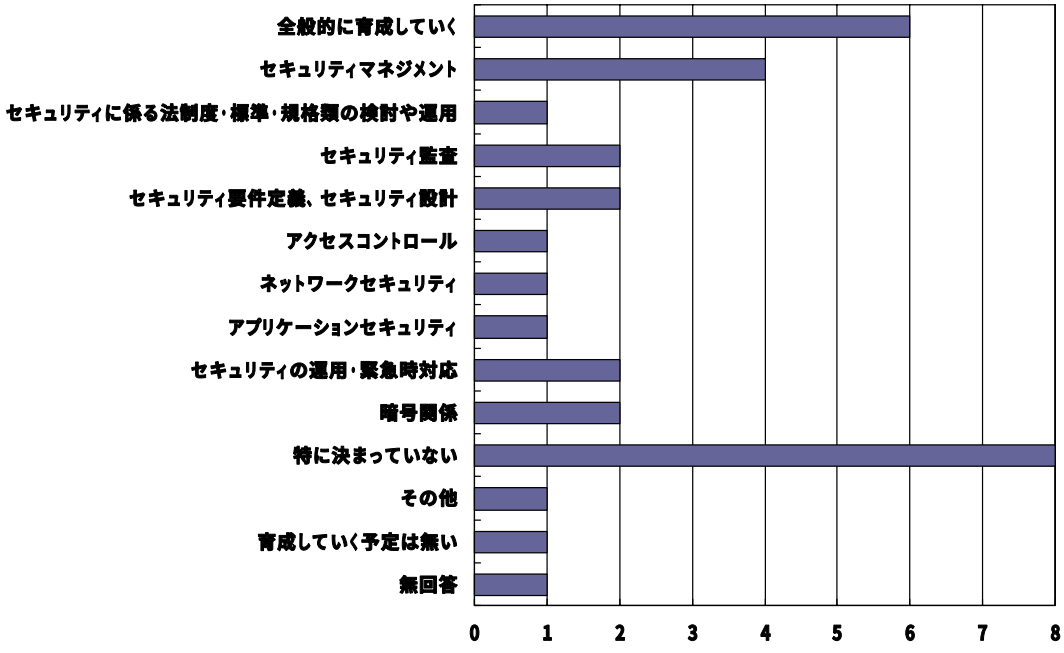


図表 12　人材の育成・確保状況

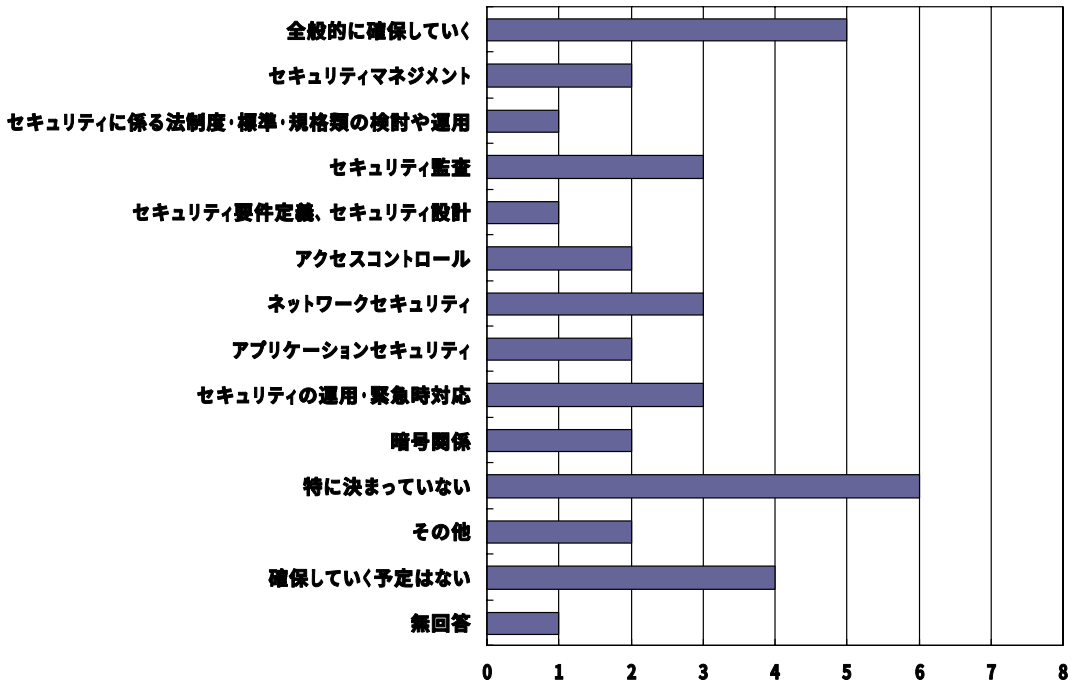


図表 13　人材を育成・確保する上での方針

・情報セキュリティ業務を担当する人材に不足している分野・能力については「全般的に不足している」「わからない」という回答が多く、多くの府省庁で必要な情報セキュリティ人材が明確になっていないことがうかがえる結果となった。
・また、今後、育成又は確保していきたい人材の分野・能力についても、「全般的に育成（確保）していく」「特に決まっていない」の割合が高く、各省庁において、計画的な人材の育成・確保戦略が定められていない実態が浮き彫りになった（図表 14、15）。
＜資料３の Q17、Q21、Q22 の調査結果を参照＞



図表 14　今後、育成していきたい人材の分野・能力



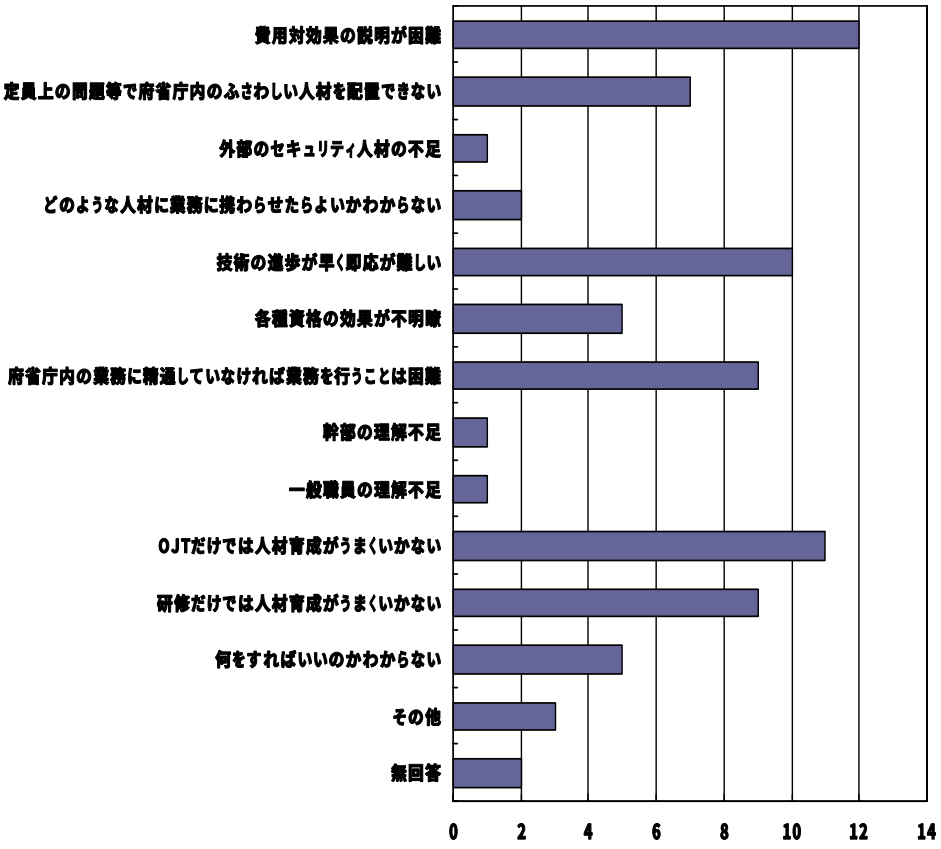
図表 15　今後、確保していきたい人材の分野・能力

（人材を育成・確保する上での課題）

・情報セキュリティ人材を育成・確保する上で「問題となっている事項は無い」と回答した府省庁はゼロであった。

・情報セキュリティ人材を育成・確保する上で問題となっている事項は極めて多岐に渡るが、「費用対効果の問題」「OJT だけではうまくいかない」「技術の進歩が早く即応が難しい」といった意見が多かった（図表 16）。

＜資料３の Q20 の調査結果を参照＞



図表 16　情報セキュリティ人材を育成・確保する上で問題となっている事項

以上を総合すると、政府機関においては、総じて次のように考えられる。

－情報セキュリティに係る人材が不足している。

－にも係わらず、具体的な育成・確保のための戦略が立てられていない。

－また、そうした戦略を立てるためのノウハウもなく、日々の OJT の中で能力の向上を図るしかないというのが現状である。

(2)　政府機関において必要となる人材育成方策

ア　一般職員について

業務を遂行していく上で情報技術の活用が不可欠のものとなったことにより、これを活用する上での情報セキュリティ上の最低限の知識（以下「セキュリティリテラシー」という。）は、コンプライアンスやセクシャルハラスメント対策等と同様に、業務を行う全ての職員が常識やマナーとして身に付けておくべきである。また、自らが所属する組織の定めたセキュリティに関するルール（以下「セキュリティポリシー」という。）については、組織の職員の当然の義務として、これを理解し、遵守することが必要となる。

したがって、一般職員には、高度な IT スキルの習得よりもむしろ、情報技術を活用して業務を実施する上でのセキュリティリテラシーと自らが所属する組織のセキュリティポリシーを理解させるための方策を検討する必要がある。

イ　幹部職員について

組織の情報セキュリティを維持するためには、個々人の能力のみに依存するのではなく、組織全体として情報セキュリティ対策を推進していくことが必要である。これには組織を統治する幹部職員の能動的な関与が必要であることは疑いを得ない。

具体的には、幹部職員は、情報セキュリティのリスクに対応するための組織・体制の構築、必要となる人員・予算・権限等の割り当てを統制していくことが求められるが、このためには、幹部職員に対してリスクを認識・理解させるための方策を検討する必要がある。

ウ　情報セキュリティ対策を担当する者について

一般に組織において情報セキュリティ対策を的確に推進していくためには、組織全体の情報セキュリティを維持する観点から、組織横断的に情報セキュリティマネジメント、情報セキュリティ監査、セキュリティの運用・緊急時対応等の情報セキュリティ対策を担当する者を置くことが望ましい。情報セキュリティ対策を担当する者としては、情報セキュリティ対策を実施する上での責任

者となる最高情報セキュリティ責任者（Chief Information Security Officer; CISO）と実際に情報セキュリティ対策を実施する情報セキュリティ担当者が存在する。情報セキュリティ対策を担当する者に求められる能力としては、「管理系分野」（組織の情報セキュリティを調整し、これを推進できる能力）と「技術系分野」（運用する技術や製品に関する情報セキュリティ対策を実施できる能力）に大別される。また、求められる能力の高度性、専門性には幾つかの段階があると想定できる。

政府機関においては、国民の信託を受け大量の情報を保有し、取り扱っていることから、こうした情報の適正な管理が求められ、一般的には CISO 及び前述した能力を有する情報セキュリティ担当者を置くことが望ましい。

ここで、政府機関において、情報セキュリティ対策を担当する者を内部人材（公務員）の育成により確保すべきか、外部人材の調達により確保すべきか、という点について検討する必要がある。

まず、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い期間を要するにも係わらず、多くの府省庁においては、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。加えて、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を担当する者のキャリアパスを構築することが困難であるという事情がある。

また、市場化テストの導入など公務員の定数の削減が求められる中、公務員としての人的資源は本来携わるべき政策立案等に優先的に割り当てるべきであり、民間の人材を活用することで足りる分野については、可能な限りそのように対処すべきものと考えられる。

以上のような状況を踏まえれば、政府機関において情報セキュリティ対策を担当する者を確保するに当たっては、可能な限り外部人材を活用することが適当と考えられる。政府機関における実態調査においても、各府省庁からは「必要な人材は保有するが、それ以外は外部の人材を活用していく」という回答が最も多い結果となっており、こうした意向にも沿うものである。

ただし、外部人材を活用すればそれでよいというものではなく、こうした外部人材が各府省庁の組織内において十分に能力を発揮し、組織全体としての情報セキュリティ対策の向上に繋がるような取組みをしなければならない。

具体的には、例えば、CISO を補佐する者（CISO 補佐官）として外部専門家を活用する場合には、当該 CISO 補佐官の意見が具体的な改善につながるような組織内での体制の整備等が必要となる。また、アウトソーシングを行う場合にも、アウトソーシング先に全て丸投げするのではなく、府省庁側において、業務に沿った適切なセキュリティサービスの提供を受けるために必要となる最低限の情報セキュリティに関する能力を有する人材を育成する必要があると考えられる。

このように、外部人材の保有する専門的な能力と内部人材の調整力等の有機的な連携を図ることがなければ、外部の専門家等を活用しても、その部分が組織の責任者にとっては「ブラックボックス」となり、結果として実効ある対策の向上に繋がらない可能性があるということに留意が必要である。

なお、外部人材を活用している府省庁が多く存在する一方で、高度な能力を有する情報セキュリティ対策を担当する専任の担当者を育成している府省庁も存在する。このように実際に各府省庁がどのような人材を必要とするか、また、どのように配置するかといった点は、各府省庁の規模や業務特性に応じて必ずしも一定でないと考えられ、例えば、下記のように組織・業務形態が異なる場合は、情報セキュリティ対策を担当する者の役割は異なってくると考えられる。

－機微な情報を扱う組織とその他の組織
－中央省庁と地方支分部局
－一般の行政組織と部隊活動を行う組織

このため、政府機関においては、各府省庁の特性を考慮した上で、必要な情報セキュリティに関する能力を有する情報セキュリティ担当者を育成するための方策を検討する必要がある。

エ　政府全体での育成の取組み

政府機関における情報セキュリティ対策に係る人材については、現時点では、その育成・確保は十分に行われておらず、各府省庁の取組みも手探り状態という状況である。

このため、まずは早急に政府職員における知識・技能の向上を図るための方策について具体的な取組みを検討する必要がある。

ここで、アンケート結果によれば、OJT に依存している府省庁が多いが、こ

れは、実態としては、体系的な対策については検討されないまま、日々の対策業務に忙殺されている傾向を否定できないと考えられる。

このため、一義的に責任を負う各府省庁が抜本的な改善策を執ることにより、情報セキュリティ対策に係る人材の育成・確保を図る必要があるが、その際、政府機関全体としてみた場合には共通化できる育成プログラムも多いと考えられる。

特に、各府省庁における予算の確保が容易ではない中、各府省庁が独自に育成計画を立てることは難しく、また政府全体としてのコスト面から見ても効率的ではないと考えられることから、政府機関全体で育成プログラムを可能な限り共通化していくことが効果的であると考えられる。

以上のような考え方に立ち、第五章第一節において、政府機関における情報セキュリティ対策のための必要となる人材育成のあり方について、詳しく提言を行う。

(3) 地方公共団体において情報セキュリティ対策に係る人材について

地方公共団体においても、住民の個人情報を含む大量の情報を保有し、取り扱っていることから、こうした情報の適正な管理が求められる。このため、政府機関と同様に、一般職員におけるセキュリティリテラシーの浸透とセキュリティポリシーの理解・遵守、幹部職員におけるリスクの認識・理解が必要となるとともに、組織横断的に情報セキュリティ対策を実施する上での責任者となる CISO 及び情報セキュリティ担当者が配置されることが望ましい。

実際、地方公共団体によっては、外部の専門家を CISO 補佐官として採用しつつ、これをサポートする内部の専任の担当者を置き、外部監査の実施や一般職員の研修まで、広く情報セキュリティ対策の実施を手懸けている先進的な団体も存在している。

地方公共団体においても、限られた予算・要員の中で、できるだけ効果的に情報セキュリティ対策に係る人材の育成･確保をすることが必要となってくる。このため、政府機関での取組みや、先進的な自治体における取組みなどを参考にしつつ、それぞれの地域や団体の実情に応じて、適切に対応することが求められる。

第三節　企業等の民間部門における現状と課題、必要となる人材育成方策

(1)　現状と課題

本委員会においては、前節の政府機関に加え、企業における情報セキュリティに係る人材の現状について把握するため、同じく平成 18 年８月から９月にかけ、日本経団連の協力を得て、アンケート調査を実施した。

本アンケート調査は、日本経団連の情報通信委員会の企業に対して実施したものであり、全ての企業の中でも、日本経団連に加盟している比較的大規模な企業であること、また、日本経団連加盟企業の中でも比較的 IT に対する意識の高い企業が回答者の中心となっている。このため、我が国全体の民間部門における実態は、以下の結果よりももう少しレベルが低いものと考えることが妥当と考える。

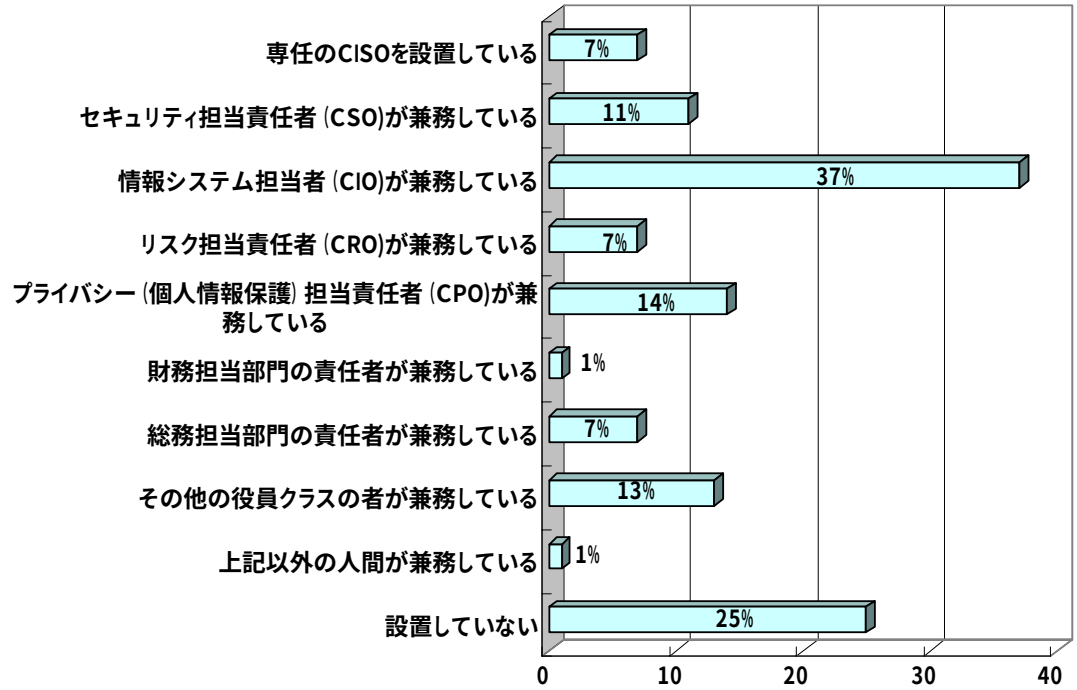
調査結果の詳細は、＜資料４＞のとおりであるが、大要、以下のとおりである。

（情報セキュリティに関する体制の現状）

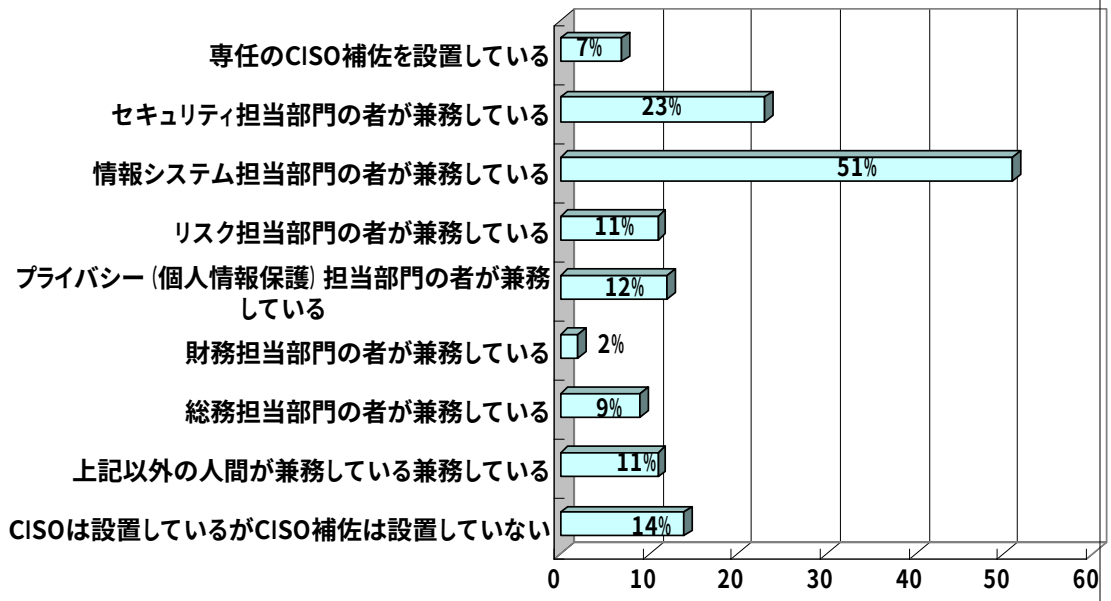
・91%の企業が既にセキュリティポリシーを策定、79%の企業が担当者（担当部門）を設け、そのうちの 82%（全体の 65%）がその役職の権限を越えた枠組みを整えている。また、75%が CISO を設置し（66%は社長・役員クラス）、そのうち 86%が CISO 補佐を設置するなど、情報セキュリティのための体制整備は一定程度進んできていると言うことができる。

・他方で、情報システム担当部門を兼任している CISO を設置している企業の割合が 37%（図表 17）、CISO を置いている企業のうち、情報システム担当部門を兼任している CISO 補佐を設置している企業の割合は 51%となっており（図表 18）、情報セキュリティの担当として情報システム部門の比重が高いことがうかがえる。

＜資料４の Q12、Q14、Q16、Q20 のアンケート結果を参照＞



図表 17　情報セキュリティ担当責任者（CISO）の設置状況

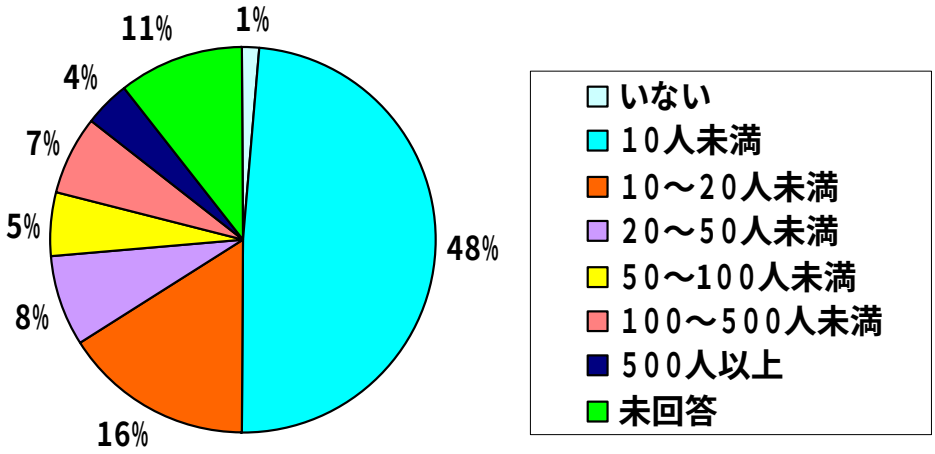


図表 18　CISO 補佐の設置状況

（担当者の現状）

・88%の企業が正社員の担当者がいると回答しているが、専任者がいると回答した企業は 47%に留まっており、兼任者しかいない企業が約半数に上ることが分かった（図表 19）。

＜資料４の Q24（１）（２）のアンケート結果を参照＞



図表 19　情報セキュリティ業務を担当する専任の正社員の数

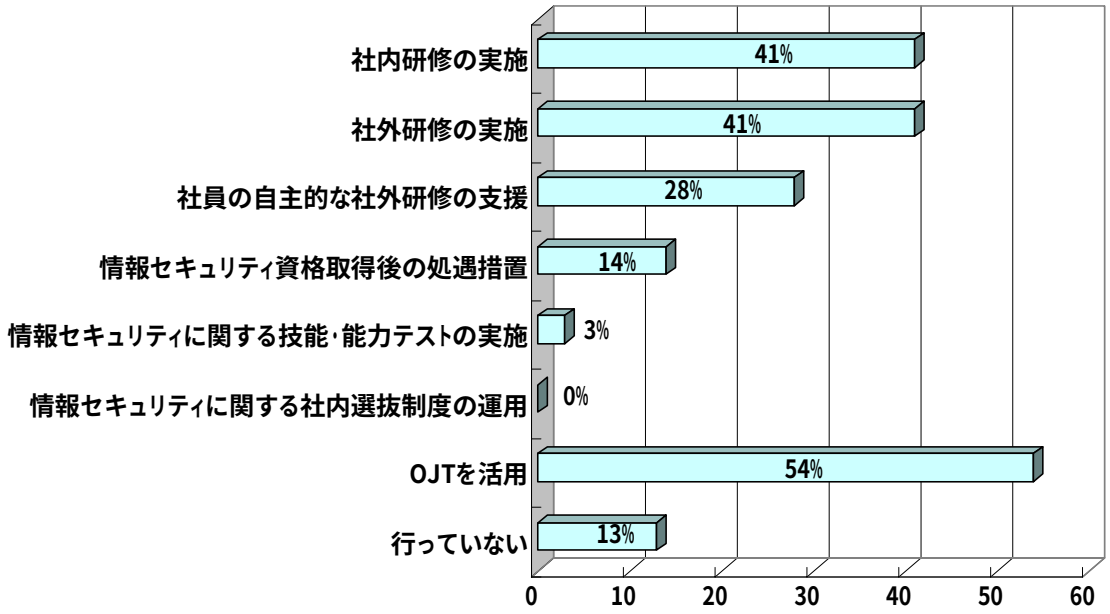
（人材の育成・確保の方策）

・育成方策については、「OJT を活用」が 54%で、「社内研修の実施」と「社外研修の実施」が各々41%でそれに次いだ（図表 20）。

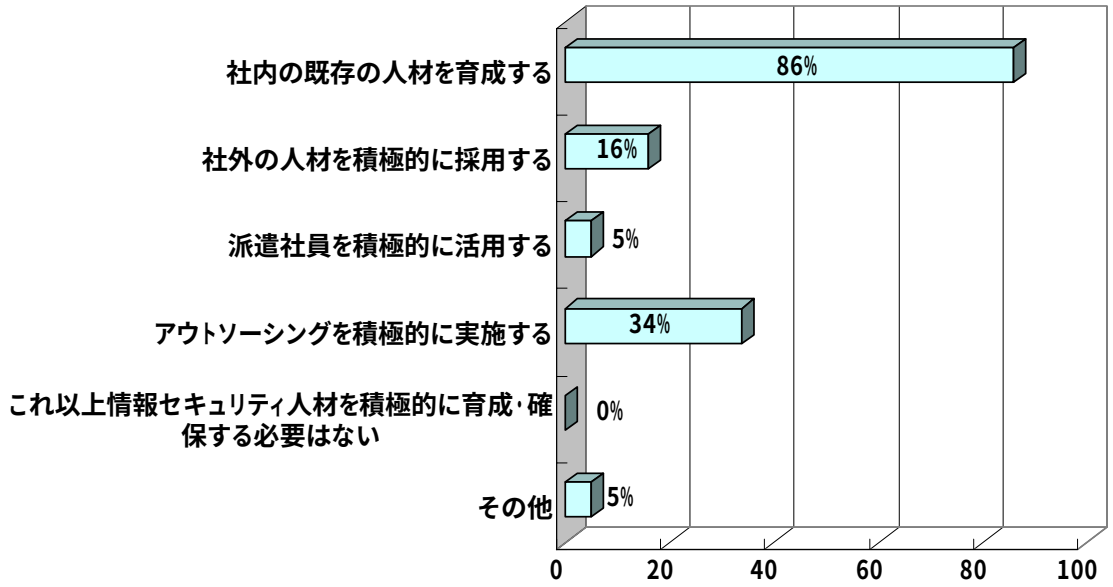
・社外からの確保方策については、75%が実施していない。

・今後の方針としても、「社内の既存の人材を育成する」という回答が 86%と非常に多く、逆に「社外の人材を積極的に採用する」と回答した企業は 16%に留まり、企業においては、内部人材を育成する意向が圧倒的に強いことがうかがえた（図表 21）。

＜資料４の Q28、Q29、Q32 のアンケート結果を参照＞



図表 20　情報セキュリティ人材の「育成」のために実施している方策

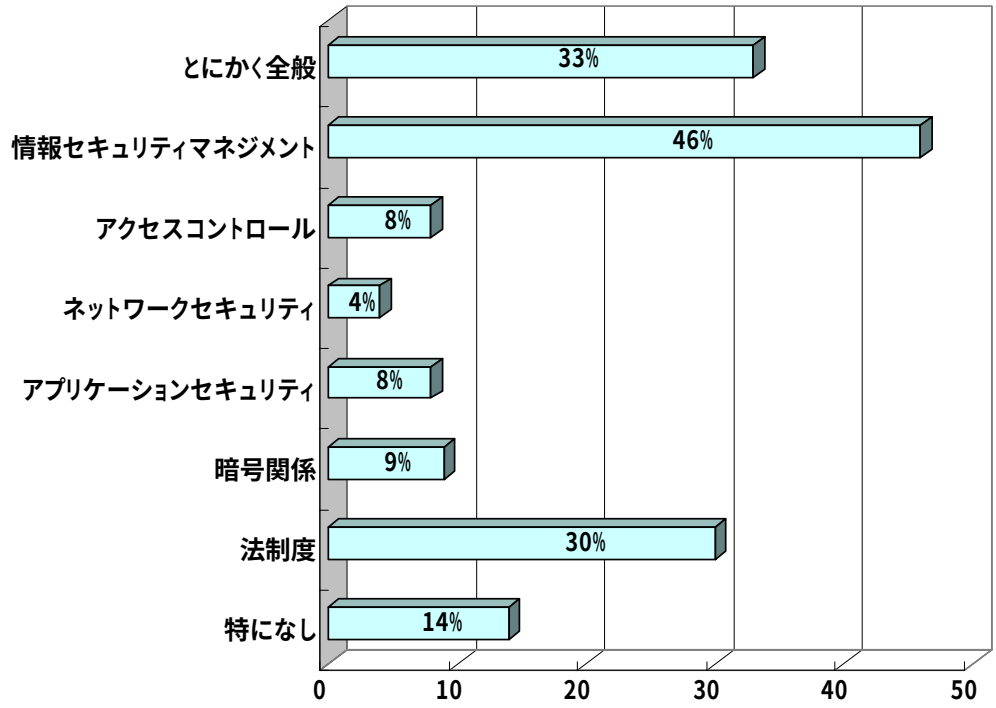


図表 21　情報セキュリティ人材を育成・確保するための今後の方針

（不足している人材の分野・能力）

・不足している情報セキュリティ人材の分野・能力については、「情報セキュリティマネジメント」（46%）という回答が最も多く、次いで「とにかく全般」（33%）、「法制度」（30%）という回答が多かった。全般的に不足していると感じながらも、情報セキュリティマネジメントと法制度の不足感が相対的に高いことが分かった（図表 22）。

＜資料４の Q30 のアンケート結果を参照＞



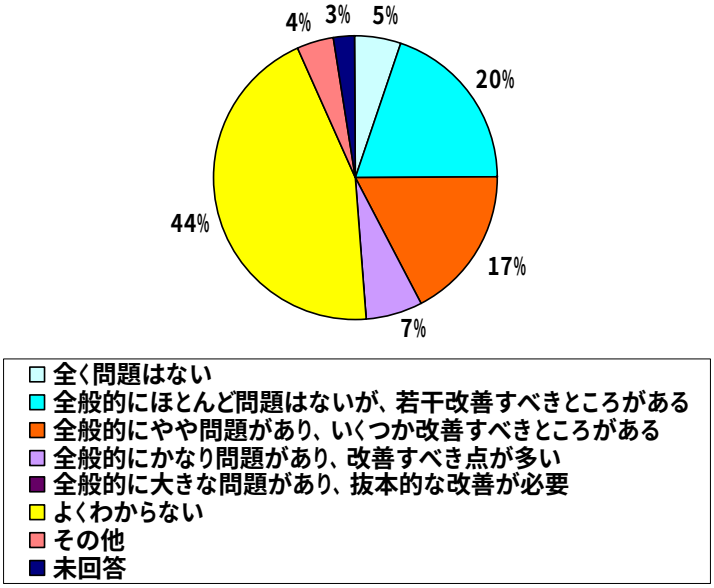
図表 22　社内で不足していると感じる情報セキュリティ人材の分野又は能力

（資格制度について）

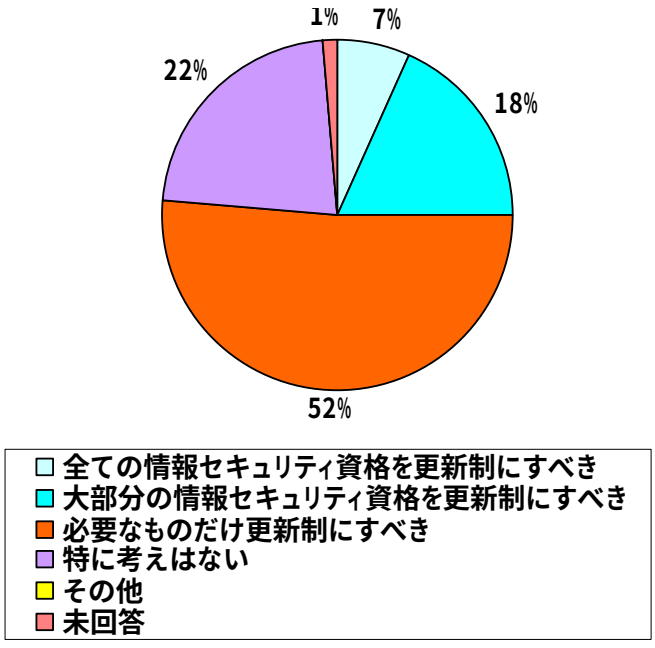
・44%が資格制度について何らかの問題があると感じているが、同時に同程度の割合の企業が「よく分からない」と回答しており、企業の情報セキュリティ担当者が情報セキュリティ資格についてあまり意識していないことが分かった（図表 23）。

・また、更新制については、程度の差はあるものの、76%が更新制を導入すべきという考えを持っていることが分かった（図表 24）。

＜資料４の Q34、Q36 のアンケート結果を参照＞



図表 23　情報セキュリティ資格制度全般に対する評価



図表 24　情報セキュリティ資格の更新制に対する考え方

（情報セキュリティ教育を行う主体について）
・また、教育機関については、「よく分からない」という回答が、専門学校については 78%、大学については 73%、大学院については 77%を占め、企業の担当者がこれら教育機関についてあまり意識していないことが分かった。
＜資料４の Q39、Q41、Q43 のアンケート結果を参照＞

以上を総合すると、以下のことがうかがえる。
－体制の整備や担当者の配置は進んできている一方、
－情報システム部門への依存度が高く、マネジメントや法制度に関する知識が比較的不足している。
－また、資格制度や各種教育機関における教育プログラムについての意識が低く、基本的に OJT による能力の確保が一般的になっている。

(2) 必要となる人材育成方策

ア 一般社員及び幹部

一般社員と幹部に求められる情報セキュリティに関する能力については、政府機関と大きな変わりはない。

すなわち、一般社員であれば、セキュリティリテラシーの浸透と、自らが所属する組織のセキュリティポリシーの理解・遵守が求められ、そのための方策を検討する必要がある。

また、幹部であれば、情報セキュリティのリスクに対応するための組織・体制の構築、必要となる人員・予算・権限等の割り当てを統制していくことが求められ、このため、リスクを認識・理解させるための方策について検討する必要がある。

イ 情報セキュリティ対策を担当する者

企業においても、組織全体の情報セキュリティを維持する観点からは、政府機関と同様に、一般的には組織横断的に情報セキュリティ対策を実施する上での責任者となる CISO 及び情報セキュリティ担当者が配置されることが望まし

い。情報セキュリティ担当者には、後述する「PDCA サイクル」[17]のモニタリング（監視）活動の一環として実施される情報セキュリティ対策の内部監査の担当者を含めて考慮すべきである。

アンケート結果によれば､企業においては情報セキュリティ担当者について、内部人材の育成により対応しようとする意向が 86%と非常に強かった。このこと自体について問題はないと考えられるが、アンケート結果を見ると、人材育成計画を策定している企業がわずか 13%しかなく、「OJT を活用」としている企業が 54%となっているのが実態である。ここで「OJT の活用」の実態は、体系的な人材育成計画がないまま、その人材をある部署で一定期間勤務させるだけとも推察され、現時点においては、企業においても総じて体系的な情報セキュリティに係る人材の育成計画が整備されていないことがうかがえる。

このため、各企業においても、最新の技術や製品情報に関する知識や、実践的な技能を身につけることのできる社外の様々な教育プログラム等を活用しつつ、自らの企業内において情報セキュリティに関する能力を有する人材を計画的に育成していくことが求められている。

なお、企業においても、上で述べたように一般的には CISO 及び情報セキュリティ担当者が配置されることが望ましいが、各企業は本来、利益や企業価値の最大化を目的とする組織であり、全ての企業が、その事業・業務内容や企業形態にもかかわらず、一律に横断的な情報セキュリティのための組織・要員の確保や、人材の育成を行わなければならないということにはならない。

例えば、日本の製造業においては、各製造現場における従事者が自らの業務プロセスを日々見直すという、いわゆるカイゼン運動を実施することにより、製品に関して世界的にも極めて高いレベルでの品質管理を実現してきた例がある。このように、各現場において高いレベルでの業務の管理・改善プロセスが確立している企業組織においては、外形標準的・横断的な統治組織に頼らず、既存の業務プロセスの中に情報セキュリティ対策の手順を入れ込むことによって、情報セキュリティの対策レベルの維持・向上を図ることも一つの形態として考えることができると思われる。

ただし、例えば、
－電子商取引により一般個人の情報を多く取り扱う企業

[17] Plan（計画）・Do（実行）・Check（評価）・Act（改善）サイクルのこと。

－重要インフラ企業[18]に代表されるような、情報システムが停止した場合の顧客や社会への影響が大きい企業

などは、その社会的影響の大きさを踏まえ、組織横断的に対策を実施できる体制・要員を整えて情報セキュリティ対策を実施することが求められる。

また、こうした企業等において情報セキュリティを担当する人材が効果的に理論体系や実践的手法等を身につけることのできる社会人育成プログラムの充実が求められる。このため、CISO や情報セキュリティ担当者が必要とする技術系・管理系の知識や技能について実践的に学ぶ機会を提供する研修プログラム等を実施する大学等に対して、ベンダー等における技術者向けのプログラムと同様に、政策的に支援を行っていくことが必要と考えられる。

以上のような状況を踏まえ、次章において、民間部門における情報セキュリティ対策のための必要となる人材育成のあり方について、詳しく提言を行う。

第四節　留意すべき事項

(1)　対策について主体的に検討できる人材の配置と PDCA サイクルの必要性

組織における情報セキュリティ対策の実施に当たって、まずセキュリティポリシーの策定が行われるのが一般的と考えられるが、中には自らの組織における業務等について十分に分析を行わないまま、外部のコンサルティング企業等から示される形式的なセキュリティポリシーを定めている例が散見される。こうしたセキュリティポリシーでは、組織の誰もが意識に止めず、結果として実効性に乏しいものとなってしまうため、セキュリティポリシーの策定段階から、組織の業務等に通じ、対策について主体的に検討できるような人材の配置が必要である。

それ以上に重要なのが、情報セキュリティ対策の実施に当たっての継続的な改善・見直しのプロセス、いわゆる「PDCA サイクル」の構築である。セキュリティポリシーの策定までは、組織全体としてイベント的に取組みが行われ、幹部をはじめ職員がその時点で意識をするが、策定以後は、ほとんど十分に理

[18] 重要インフラについては、「重要インフラの情報セキュリティ対策に係る行動計画」（平成 17 年 12 月 13 日情報セキュリティ政策会議決定）や「重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針」（平成 18 年 2 月 2 日情報セキュリティ政策会議決定）において、情報セキュリティの確保の観点から専門的人材の育成について既に言及がされている。

解・実行されないという例が多く見られる。また、セキュリティポリシーに基づく対策は実施されているが、環境の変化に応じた見直しがなされないまま、一定の対策がずっと実施されているという例も少なくない。

しかしながら、情報セキュリティ対策は、情報セキュリティのリスクに対する対策であり、リスクに変化が起これば、当然ながら対策にも変更が必要となるものである。したがって、情報セキュリティのリスクを含む環境の変化に柔軟に対応しつつ、対策の着実な運用と質的レベルの維持・向上を図ることが必要であり、それには、単に一時期だけ有能な職員を配置するのではなく、長期的な視野に立った人材の育成・確保や配置についても考えなければならない。

(2) 技術系スキルの必要性

政府機関や一般企業で言えば、技術的なことは全てベンダー等に任せきりになっている企業も多いが、一般的には、こうした組織においても、最低限の技術的事項を理解している人材の配置が必須である。具体的には、発注するに当たって最低限の技術的事項について理解し、業務要件にあった的確な仕様の策定を行い、実際のプロジェクトの進捗管理等の段階においてベンダー等とやりとりをし、更には、システムを導入するに当たっての最低限のチェック（例えばサーバの簡単な脆弱性検査など）のできる人材が必要である。

また、こうした技術系の人材から出される最新の技術動向や製品情報を踏まえた意見・提言を吸い上げ、組織全体の PDCA サイクルの中で反映できるような枠組みについても、併せて構築することが必要である。

第五章　情報セキュリティに係る人材の育成に向けた具体的な取組み

第一節　政府機関における人材の育成に向けた取組み

政府機関における情報セキュリティ対策に係る人材の育成については、前章第二節で述べたとおり、現状を踏まえ、まずは早急に政府職員における知識・技能の向上を図る必要がある。このため、以下では、政府機関における人材育成のため、当面取り組むべきと考えられる事項について提言を行う。

その際、政府職員における知識・技能の向上については、一義的には各府省庁が責任を持って実施すべきであるが、政府機関全体で共通に必要となる育成プログラムについては、可能な限り政府機関全体で共通化し、継続的に推進していくことが効率的である。

ここで、新たな教育の枠組みを開発し、これを実行するためには相当の時間を費やすと考えられ、また、政府全体の情報セキュリティ政策の要となる内閣官房情報セキュリティセンターには人員や予算面での制限もあることから、現在、各府省庁で個別に実施されている既存の情報セキュリティ教育プログラムとの連携・調整を図り、可能な限りこれらを有効に活用していくことが、政府機関における人材育成にあたっての近道であると考えられる。

(1)　一般職員について

セキュリティリテラシーの向上については、第三節で述べるとおり、高等学校における「情報教育」等において一般的な知識として身につけておかれるべきことだが、当面、現在既に政府機関に所属している職員への対応策として、政府機関の職員への研修を徹底することが現実的であると考えられる。なお、セキュリティリテラシーについては､各府省庁の業務特性によらず必要であり、内容にも大きいな違いはないと想定できるため、政府統一的な「セキュリティリテラシー教育プログラム」（仮称）を整備し、全政府職員がこれを定期的に受講できるような枠組みについて検討する必要がある。この際、セキュリティリテラシーに関する教育については、情報システムに関わる教育ではなく、政府職員の人事教育の中に取り入れていくことが求められる。

また、セキュリティリテラシーとは別に、「政府機関統一基準」[19]に基づいて、各府省庁はそれぞれ定めたセキュリティポリシーの浸透を図っていく必要がある。このため各府省庁は、自府省庁のセキュリティポリシーを職員へ理解させるための教育を継続的に実施すべきである。

(2) 幹部職員について

幹部職員にリスクの認識・理解を求めるにあたっては、本来は各組織のリスク及びガバナンスに起因する問題であるため、各組織が独自に分析し、これに対応することが望ましい。しかしながら、政府機関であれば対応しなければならないリスクについて共通となる内容も多いと考えられ、加えて、各府省庁が内部で幹部職員にリスクマネジメントの教育を実施するのは容易ではなく、教育を実施するための枠組みを構築するにも相当の時間を費やすと考えられる。

このため、幹部職員についても政府統一的な「リスクマネジメント教育プログラム」(仮称)を整備すべきである。この際、幹部職員の業務の特殊性を鑑み、職位が変わる等の区切りの段階において、確実に受講できる形態を検討する必要がある。この際、リスクマネジメントに関する教育については、業務全体の最適化の視点から、情報システムに関わる教育ではなく、政府機関の人事教育の中に取り入れていくことが求められる。

(3) 情報セキュリティ対策を担当する者について

ア 情報セキュリティ対策を担当する者の育成について

各府省庁が行政事務を執行していく上で必要となる情報セキュリティ対策を実施するため、情報セキュリティ対策を担当する者に求められる能力には、(一部の府省庁を除いて)共通する部分も多いと考えられる。

こうした各府省庁の業務特性に左右されず必要となる情報セキュリティに関する能力を有する担当者の育成については、従来のように各府省庁が個別に実施するのではなく、可能な範囲で府省庁横断的に育成を推進する方が効率的であると考えられる。このことから、政府統一的な「情報セキュリティ担当者教育プログラム」(仮称)を整備し、これを各府省庁に提示した上で、各府省庁の

[19] 「政府機関の情報セキュリティ対策のための統一基準」(平成 17 年 12 月 13 日情報セキュリティ政策会議決定)

判断においてこれを活用させるための枠組みを構築するべきである。

こうした政府統一的な情報セキュリティ担当者教育プログラムの整備に当たっては、既に各府省庁が実施している教育プログラムを有効に活用していくべきである。例えば、総務省行政管理局が実施している「情報システム統一研修」[20]などと十分に連携・調整を図り、情報セキュリティに関する技術や製品の最新動向等を反映した見直しを行いつつ、政府全体として効果的・効率的なプログラムを組むことが求められる。

その際には、一般に２～３年と比較的短い人事異動のサイクルにおいても、その間で職員が継続的に能力を維持・向上することができるよう配慮することが必要である。このため、情報セキュリティ担当部門に配属された直後の職員向けの研修に加え、例えば半年や１年の業務経験を積んだ職員に対して、より高度なスキルや最新技術の動向などについても学ぶことができるような、継続教育の枠組みについても検討が必要である。

一方、特定の府省庁のみが必要とする、または極めて高度な情報セキュリティに関する能力を有する情報セキュリティ対策を担当する者の育成に関しては、各府省庁がそれぞれの責任において、現在と同様に引き続き推進していくべきである。既に独自の職員訓練プログラムを実施している府省庁においては、こうした既存の訓練機会を最大限に活用しながら情報セキュリティ対策を担当する者への教育を展開していくことも重要である。

その際、こうした人材を必要とする府省庁では一般に極めて重要な情報を保有し、取り扱っていることを踏まえれば、当該府省庁内において教育を実施する際にも、最先端の技術や高度な管理手法についての十分な理解と習得が図られるよう配慮が必要である。また、こうした技術や管理手法に関する教育を受けた者が身につけた知識や技能を、組織内において実践できるような環境作りも必要不可欠である。

イ　外部人材の活用について

前述の通り、政府機関においては、情報セキュリティに係る業務について、外部人材の活用が一般的に行われている。これは、キャリアパスの構築が困難であり、かつ、定員削減を求められている政府機関にあっては、極めて有効な手段の一つと考えられる。

---

[20] 各府省庁の情報化を担う基幹要員等の養成を目的として、国の行政機関等における行政情報システム関係業務等に従事する職員に対して総務省行政管理局が実施する研修。

ここで、外部人材の活用に当たって、CISO 補佐官など情報セキュリティを担当する者としては、CIO 補佐官等に求められる IT や情報システムに関する知識に加えて、リスク分析技術やセキュリティ運用など、情報セキュリティに特化した能力が必要となることに留意が必要である。

また、外部人材の活用に当たっては、こうした人材が各府省庁の組織内において、その能力を最大限に発揮することのできるような環境の整備が必須である。

具体的には例えば、CISO 補佐官については、多くの府省庁において外部専門家を活用しているが、単に「ご意見番」に留め、その意見を具体的な改善につなげることがなければ、効果は乏しいものとなる。このため、こうした外部専門家の意見を組織内で実効的に推進することのできる体制や権限の付与、さらには、組織内部での企画・調整を推進することのできる有能な内部人材（プロパー職員）の配置も必要となる。

また、こうした外部専門家を採用する場合には、単に情報セキュリティに関する技能や知識の有無だけでなく、組織内での円滑な業務推進のため、職員に準じた公務員倫理観やビジネスマナー等を適切に備えていることも確認しておく必要がある。

さらには、こうした人材は、専門的見地から見て、組織の体制・業務などの枠組みについて改善が必要と思われる場合には、幹部等に対してその必要性を説明し、説得することも求められることになる。このためのプレゼンテーション能力、コミュニケーション能力なども必要な能力として確認しておく必要がある。

また、政府機関への実態調査によると、特にセキュリティの運用・緊急時対応やアプリケーション、ネットワーク等の技術的な業務に関して、外部人材を活用しようとする意向が強いが、こうした製品等の提供者の力量を保証し、これを適切に把握するためには、当該者が保有している資格を一つの目安として活用することも有効と考えられる。

ウ　政府機関の内部職員による資格の保有について

前述したような既にスキルを持つ外部人材を活用する一方で、こうした人材

と連携を図りながら組織内における調整等を行う内部職員の育成も必要であり、その手段の一つとして、官民の団体によって運用・提供されている資格制度を活用することも考えられる。しかしながら、資格制度の中には、知識・技能を習得するためのプログラムというよりは、既に知識・技能を有している者が対外的にその事実を示すことのできるよう、一定の枠組みの下で保証するというのが基本的な枠組みになっているもの（レベル判定型の教育プログラム（資格制度））もあるということに留意が必要である。特に、現在の政府機関職員の人材育成に当たっては、担当者等に知識・技能を習得させることが最も重要な課題であるという現状を踏まえれば、既に有している知識・技能を対外的に示す必要性には乏しいと考えられる。

このように考えると、政府機関における情報セキュリティ担当者に対してこうした資格の取得を画一的に促していくよりも、むしろ、既に展開されている、実践的な研修等により知識・技能の定着を図る教育プログラム（訓練・実習型の教育プログラム）を必要に応じて活用しつつ、政府機関の特性を考慮した上での情報セキュリティに係る人材の能力を向上させるための教育プログラムを整備し、この教育プログラムの受講を認定することで、資格に代わるものとして位置付けることが適当ではないかと考えられる。

むしろ、情報セキュリティ対策を担当する者にとっては、一時点においての知識・技能よりも、実際に継続的に対策を行っていく上での知識・技能が重要である。したがって、こうしたプログラムの設計に当たっては、政府機関職員の人事異動サイクルなども考慮に入れつつ、継続的な教育が実施できるような枠組みについて検討する必要がある。

(4) 政府機関における枠組みの構築に向けた検討

以上、政府機関における情報セキュリティ対策に係る人材の育成に向けて取り組むべき事項を示したが、今後、政府内においてこれを具体的に実行するための枠組みについて検討がなされるべきである。

第二節　民間部門における人材育成に向けた取組み

民間部門における情報セキュリティ対策に係る人材の育成についても一般社員､幹部職員､情報セキュリティ担当者に渡って対策を講じていく必要がある。

(1)　一般社員について

一般社員については、政府機関における職員と同様に、セキュリティリテラシーを身につけることが基本となる。このため、各企業は、今後拡大が期待される外部の教育ビジネスなどを活用しつつ、全社員に対して、入社時や一定期間ごとに行われる社員研修等の場の中で、セキュリティリテラシーについて習得できるようなプログラムを設定することが求められる。

(2)　幹部について

幹部に対しては、情報セキュリティのリスクを認識・理解させるための教育が必要となる。

この点、企業によって事業・業務内容や企業形態は多種多様であり、情報セキュリティのリスクも一律ではないため、幹部への教育は、単に外部の教材等を流用するだけでは足りず、個々の企業ごとにリスクを分析した上で、幹部に説明を行っていく必要がある。このような企業ごとのリスクの分析と幹部への説明に当たっては、外部のコンサルティング等を活用しつつも、社内業務等に通じた内部の社員の関与が不可欠である。

(3)　情報セキュリティ対策を担当する者について

情報セキュリティ対策を担当する者について、政府機関においては外部人材を可能な限り活用することを基本としているのに対し、企業においては、内部人材を育成することにより対処しようとする意向が強い。こうした方針自体は何ら否定されるものではないが、この場合、情報セキュリティの基礎や最新の技術動向について、各企業の内部人材が知識・技能として習得し、継続的にこれらの知識・技能を更新していく必要が出てくる。

このため、民間部門においては、情報セキュリティ対策を担当する者について、計画的な育成プログラムを整備することが必要となる。特に、日本経団連加盟企業へのアンケートの結果によると､多くの企業がいまだ OJT による対応が主流となっている。しかしながら、組織全体としての適切な情報セキュリテ

ィ対策の推進を実行する観点からは、情報セキュリティの基礎について十分に理解をした上で、管理面・技術面の双方について、実践的な知識・技能を習得することが必要であり、各種の外部教育プログラムを活用しながら、計画的な担当者の育成計画を策定することが望まれる。

第三節　教育機関等に関する取組み

(1)　大学院等の高等教育機関に関する取組み

大学院等の高等教育機関においては、まず、その「研究機関」としての機能から、我が国の研究開発・技術開発分野の拠点としての役割が求められる。これらの拠点においては、優れた人材を養成することが必要であり、このため、第二章第三節で述べたとおり、政府は「21 世紀 COE プログラム」の充実等を図る一方、各大学院等には、こうした競争的資金を活用するに当たり、研究開発・技術開発力の高い人材の養成に繋がるような柔軟かつ創造的な提案が期待される。

次に、「教育機関」としての機能から、これまで述べたとおり、政府は産学連携による先導的な IT 人材の育成を政策的に推進するとともに、社会人教育プログラム等の提供主体としての役割も期待されていることから、各大学院等には、企業・産業界や他の教育機関等とも連携を図りつつ、企業人の受講にも配慮することが期待される。

(2)　高等学校や大学の一般教養課程における情報セキュリティ教育の必要性

政府機関、企業等における一般職員・社員が必要な能力として、情報セキュリティリテラシーが上げられているが、実際に、人材派遣会社の中には、IT 人材か否かに係わらず、派遣社員として顧客企業に派遣する人材については、全員、事前に情報セキュリティに関する研修を受けさせているという例もある。

このように、情報セキュリティについては、言わば「社会人としてのマナー・常識」になりつつある状況であり、次代の一般職員・社員となる若者達に広く情報セキュリティに関する最低限の知識を身に付けてもらう必要がある。

また、先進的な技術の研究者をはじめとして、第二章から第四章までに述べてきた様々な情報セキュリティに係る人材の全体的なレベルアップを図るため

には、裾野となる国民全体のセキュリティリテラシーの向上を図る必要がある。

この点、既に高等学校において、平成 15 年度から教科「情報」が必履修となっており、情報セキュリティについても、情報モラル教育の１つの要素として指導がなされているところであるが、その内容についてより効果的なものにするなど一層の充実を図ることが求められる。

特に、高校生への教育という面では、日々進化している情報セキュリティの脅威に対する個別の対処策について教えるよりも、むしろ「情報処理やインターネットの仕組み」「情報セキュリティの本質は何か」といった普遍的な基礎・原理について理解・認識を定着させた上で、情報セキュリティに関する実践力を育むことが重要であり、今後の学習指導要領の見直し等に当たっては、こうした観点からの検討が行われることが求められる。

他方で、本委員会で検討を進めているほぼ同時期に、全国の高等学校において、必履修教科である「情報」の時間を他の科目の授業に振り替えていたという、いわゆる未履修の問題が全国的に明らかとなった。このことは、情報教育が次世代を支える高校生にとって必要なものであるという考えに立って教科「情報」が必履修になったことを踏まえれば、看過できる問題ではない。特に、今後世界規模で情報化がさらに進展し、社会経済活動や国民生活のあらゆる分野で IT が活用されると考えられる中で、次代を担う若者達の IT の活用能力は我が国の産業競争力等にも直結してくることから、確実に能力の定着を図る必要があると考えられる。

この問題については、新たに政府に設置された「教育再生会議」や文部科学省などにおいて、セキュリティも含めた情報活用能力の着実な定着を図るという観点に立って、真摯に対応が検討されなければならない。

また、現在では大学の進学率が５割を越えており、大学が新社会人の半数以上の人材を送り出していることに鑑みれば、大学の一般教養課程における情報教育にも更なる役割が期待される。既に各大学においては情報教育が浸透しているが、前述した高等学校での情報に関する教育の充実に加え、大学の一般教養課程においても、学部・学科の別によらず、広く学生に情報セキュリティに関しても高等学校での内容を一層深めた情報処理に関する教育を行うことが期待される。

(3)　メディアが担う教育的機能

メディアは、一般個人に対して直接情報発信をするという機能を持っていることから、一般個人のセキュリティリテラシーの向上に当たって大きな役割を果たすことができる。特に、セキュリティリテラシーが国民各層に広く求められる今日、メディアには、情報セキュリティに関するトピックを積極的に取り扱い幅広く啓発を図るとともに、情報セキュリティに関する重要性について分かりやすく的確に伝えることにより、一般個人のセキュリティリテラシーの向上にさらに寄与することが期待される。

第四節　資格制度に関する取組み

(1)　情報セキュリティ資格の現状

情報セキュリティに係る人材が、必要な能力を身につけ、また、そうした能力を既に身につけていることを対外的に示すための枠組みとして、各種資格制度が存在している。本委員会では、現在運用されている情報セキュリティ資格のうち主なものについて＜資料５＞のとおりとりまとめた。

＜資料５＞の作成に当たっては、基本的に情報セキュリティ専門の資格を対象とし、求められる知識・技能の一部として情報セキュリティに関する知識等を求めている資格については対象外とした。また、ベンダー中立的な資格を対象とし、個々のベンダーが提供する資格は対象外とした。

＜資料５＞にあるとおり、情報セキュリティ資格の中には、経済産業大臣が実施する、いわば官製の「情報処理技術者試験」において、「情報セキュリティアドミニストレータ」と「テクニカルエンジニア（情報セキュリティ）」の二つの試験が提供される一方で、民間の団体等により運営されている資格制度も存在する。また、後者の中には、海外で普及している資格を日本向けに展開したものもあれば、国内の企業によって構築されたものなどもある。さらに、試験への合格のみによって資格が得られるものと、試験への合格に加え、一定の実務経験や倫理規約への同意・遵守など、他の要件を求めるものがある。

(2)　官民の役割を含めた資格制度のあり方について

前述のとおり、情報セキュリティ資格の中には、官民双方のものが併存しており、官製の試験については、官民の適切な役割分担という観点から、その役割について検討をすることが必要となる。

この点、本委員会においては、情報処理技術者試験について、民間による資格制度が運用されている現状を踏まえれば、既に役割を終えたのではないかとの意見も出されたところである。他方で、一般的な知識・技能を汎用化・一般化し、基礎的な知識等の定着を図るという意味で、一定の意義があるのではないか、国策実現の手段として行われている国の試験と商業ベースの民間試験とは自ずと役割は違うはずでないか、といった意見も出されたところである。

情報処理技術者試験については、このような論点も踏まえつつ、市場における人材ニーズの現状や民間の団体において運用されている資格制度の内容・動向、第三章第三節(1)エに述べるソフトウェアの品質の確保・信頼性の向上に関する議論の動向等を踏まえ、官民の適切な役割分担という観点から適宜適切に見直しを図りながら設計・運用されることが必要である。

また、情報セキュリティ分野のうち、管理面の知識等については、それぞれの社会や文化が影響し得る領域であるため、単に技術面だけでなく総合的な資格として考える場合、日本独自の社会や組織文化の特性を踏まえた知識等が求められるかどうかについて検討することが必要である。
このため、主に国内での展開を前提とする資格においてこうした事項が反映されることが期待されるとともに、国際展開を前提として日本において展開している資格においても、必要に応じ、試験内容の柔軟な見直しが図られることが期待される。

(3)　資格制度に係る更新制・継続教育について

＜資料５＞にあるとおり、現在運用されている資格制度の中には、一定の更新制・継続教育の仕組みを導入しているものもある一方で、一度受験して合格した場合には、永久にその資格が認められるものも存在する。

この点、特に情報セキュリティに関する技術動向については、常に日進月歩であることを踏まえれば、少なくともそうした最新の技術動向についての知識や技能に係る資格制度については、一定の更新制・継続教育の枠組みを設けることが必要と考えられる。

第五節　各種教育プログラムに関する体系図について

本委員会では、当初、情報セキュリティに係る人材の育成方策を検討する中の項目として、資格制度の体系化についても検討を行うこととされていた。

ここで､政府機関における実態調査や企業に対するアンケートの結果からは、これら情報セキュリティ対策を実施する組織においては、必ずしも資格制度を深く認識していないこと、また、情報セキュリティ担当者に必要な能力・スキルの確保に当たっては、必ずしも資格制度だけでなく、様々な教育プログラムが存在することから、本委員会においては、資格制度を含め、現在提供されている代表的な教育プログラムについて、体系図として分類・整理を行うこととした。

具体的には、今後、情報セキュリティに係る人材の育成計画を立てようとする者が、比較をしつつその参考とできるような一つの目安として、
－まずは第三章及び第四章において整理した情報セキュリティに係る人材のカテゴリごとに必要とされる能力の整理を行い、
－その上で、それぞれの人材カテゴリごとに、能力の習得等に資すると考えられる各種の教育プログラム（高等教育機関、社会人実践プログラム、資格制度等）について整理を行った。（＜資料６＞参照）

ここで、＜資料６＞は、あくまで「一つの目安」であるということに留意が必要である。例えば企業等においてもその事業規模や事業内容、さらには組織形態や一般的な社員研修の方針などがある中で、この表とは異なる形で人材の育成等が行われることも十分にありえると考えられる。また、表の下段にまとめた各種の教育プログラムについても、本委員会として推奨しようとするものではなく、一つの目安として示しているものに過ぎない。

今後、人材の育成計画を立てようとする者は、自らの組織等においてどのような人材が必要となるかをそれぞれ独自に検討し、＜資料６＞を参考としつつも、自らの組織の実情等も十分に勘案しながら、人材の育成・確保の方策を定めることが望まれる。
また、表の下段にまとめた各種の教育プログラムの提供者は、＜資料６＞をもってみだりに教育プログラムの売り込みをかけることは厳に慎むべきであり、顧客企業等のニーズを十分に踏まえ、適切な対応をすることが求められる。

おわりに

本委員会においては、情報セキュリティに係る人材の育成方策について、包括的に検討を行った。

検討に当たっては、情報セキュリティを専門的に職務として扱う人材のみを対象として捉えるのではなく、我が国全体として情報セキュリティ対策を効果的に進めていくためには、社会経済活動における様々なプレーヤーが情報セキュリティに係ってくるという視点に立ち、可能な限り幅広い人材を対象として、現状と課題を分析し、必要となる対応方策について提言を行った。

特に、本委員会においては、我が国全体の情報セキュリティ対策を考える上で最も広範囲にわたると考えられる政府機関と企業において実際に情報セキュリティ対策に係る人材について、約１月に渡って実態調査・アンケートを実施し、これら組織における人材及びその育成方策が、いまだ不十分であることを浮き彫りにした。

この点に関しては、特に、情報セキュリティ対策の模範を示すべき政府機関について、できるだけ効率的な育成の推進を図るという観点に立って、各府省庁共通の教育プログラムとなる、

－一般職員向けの「セキュリティリテラシー教育プログラム」
－幹部職員向けの「リスクマネジメント教育プログラム」
－情報セキュリティ担当者向けの「情報セキュリティ担当者教育プログラム」

（いずれも仮称）の整備について提言を行った。

また、我が国における情報セキュリティ対策をリードしていくこととなる、先進的な情報セキュリティ技術・製品及び高度な管理手法の研究・開発者についても検討を深め、大学院等の高等教育機関における研究・開発力の向上といった点についても一定の提言を行った。

さらに、情報セキュリティに関する製品等を提供する企業における人材についても、間接的に情報セキュリティに係ってくる一般のベンダー等における人材も含め、幅広くその育成のあり方について提言を行うことができた。

加えて、各カテゴリの人材の育成方策についての検討を通じて、各カテゴリの人材毎に必要とされる能力を整理し、その習得に資すると考えられる各種の教育プログラムについて体系図として分類・整理を行った。

このように、研究機関や政府機関も含めて我が国で情報セキュリティ対策を推進する上で関係してくるであろう幅広い人材について俯瞰し、その現状と課題を整理し、必要な提言を行ったのはおそらく初めてであり、その意味で本報告書は非常に意義深いものと考えている。

今後、政府においては、前述した各府省庁共通の教育プログラムの整備や、大学院等の高等教育機関における競争的資金の拡充等、本報告書において提言を行った具体的な取組みについて、早急に着手することが求められる。

また、企業においても、本報告書の提言を踏まえつつ、経営リスクの一つとしての情報セキュリティに関するリスクについて早期に認識・理解をし、できるだけ早期に効果的な形で情報セキュリティに係る人材の育成・確保を進め、我が国の情報セキュリティ対策の底上げを図ることが期待される。

なお、本報告書においては、我が国全体として情報セキュリティ対策に着手したばかりの現段階における情報セキュリティに係る人材の現状と課題を踏まえて検討・提言を行っているものである。したがって、今後、情報セキュリティに係る人材の広がりや市場の拡大、さらには新たな情報セキュリティのリスクの登場などに伴って、求められる人材・能力や、必要となる対応策についても、当然見直しが必要となる可能性があるという点について留意が必要である。

また、「はじめに」でも述べたとおり、人材育成方策については、本来、長期的な視野に立ち、初等中等教育も含め国家全体としての育成方策のあり方について検討することが必要である。この点、今回の報告書においては、当面、早期に着手・実行すべき事項について検討・提言を行ったが、初等中等教育も含めた長期的な人材育成方策のあり方についても、引き続き検討がなされることを期待したい。

本報告書が、情報セキュリティ対策を実施する上で「人」に係る問題を解決しようとする全ての方々にとって、進むべき方向を検討する上での参考となり、結果として、我が国の情報セキュリティ対策の向上に資することを願ってやまない。

本委員会における検討の経緯

【情報セキュリティ政策会議】

2006年 7月25日 第7回会合
人材育成・資格制度体系化専門委員会の設置について

2006年10月25日 第8回会合
「セキュア・ジャパン 2006」の進捗状況について

【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】

2006年 8月30日 第1回会合
（１）我が国政府の情報セキュリティ問題への取組みについて
（２）情報セキュリティ人材の育成に向けた検討
（３）情報セキュリティ人材・資格制度について
（４）情報セキュリティ人材(高度 IT 人材)の現状と今後の課題
（５）情報処理技術者試験制度について
（６）自由討議

2006年 9月15日 第2回会合
（１）資格制度運営団体ヒアリング
（２）地方自治体における情報セキュリティ人材の確保について
（３）日本経団連アンケート結果報告
（４）政府機関実態調査結果報告
（５）討議

2006年10月13日 第3回会合
人材育成・資格制度体系化専門委員会報告書骨子（案）についての検討

2006年11月16日 第4回会合
人材育成・資格制度体系化専門委員会報告書（案）についての検討

＜参考一覧＞

参考１：「第１次情報セキュリティ基本計画」
参考２：人材育成等に関する「セキュア・ジャパン 2006」関連記述抜粋
参考３：「第３期科学技術基本計画」及び「分野別推進戦略」における情報セキュリティ関連抜粋

「第1次情報セキュリティ基本計画」
－今後3年間の重点政策－

○全主体が適切な役割分担を果たす「新しい官民連携モデル」の構築に向けて、今後３年間、政府は「第１次情報セキュリティ基本計画」に基づき、各種対策を強化。

	政府機関・地方公共団体	重要インフラ	企業	個人
役割	情報セキュリティ対策の「ベストプラクティス」へ	国民生活・社会経済活動の基盤としての安定供給の確保	市場に評価される情報セキュリティ対策の実施	IT社会の担い手としての意識の向上
今後３年間の主な重点政策①（４領域）	◆政府機関統一基準に基づいた 各省庁の評価 ◆ サイバー攻撃等への緊急対応能力の強化	◆ 情報共有・分析機能の整備 ◆ 重要インフラ連絡協議会の設置 ◆ 分野横断的な演習、相互依存性解析の実施	◆政府調達における入札条件の整備 ◆ 情報セキュリティ監査等第三者評価制度の活用推進 ◆ コンピュータウィルス等への対応体制の強化	◆ 情報セキュリティ教育の推進 ◆「情報セキュリティの日」の創設等広報啓発の強化 ◆ ユーザーフレンドリーなサービスの提供等の環境整備
【個別設計図】	政府機関統一基準	重要インフラ行動計画	各省庁による施策	各省庁による施策

今後３年間の主な重点政策②（横断的事項）

情報セキュリティ技術戦略の推進
◆政府が活用することを前提とした技術開発実施
◆「グランドチャレンジ型」技術開発の推進

情報セキュリティ人材の育成確保
◆ 多面的・総合的能力を有する実務家の育成
◆ 情報セキュリティの資格制度を体系化

国際連携・協調の推進
◆ 国際的な安全・安心の基盤づくりへの貢献
◆ 我が国発の国際貢献

犯罪の取締り、権利利益の保護救済
◆ サイバー犯罪の取締り強化及び関連基盤整備
◆ サイバー空間の安全性向上のための技術開発

参考１

参考2

人材育成等に関する「セキュア・ジャパン2006」関連記述抜粋

1　情報セキュリティに関する資格制度の体系化について

p.33　第3章　第2節　②　情報セキュリティに関する資格制度の体系化

ア）情報セキュリティに関する資格制度の体系化等のための検討（内閣官房、総務省、文部科学省及び経済産業省）

高い能力を有する情報セキュリティ技術者、各組織における最高情報セキュリティ責任者（CISO）、情報システム運用受託者、各組織の情報システムの運用担当者、情報システム利用者等それぞれに応じた適切なスキルについて関係府省庁間で連携を図りつつ検討を行い、情報セキュリティに関わる技術者等にとってキャリアパスとなるための情報処理技術者試験をはじめとする情報セキュリティに関する資格制度の体系化について、その基本方針及び具体策を2006年中に示す。

2　政府機関における情報セキュリティ人材の育成・確保について

p.12　第2章　第1節　⑤　政府機関における人材育成

ア）政府職員の人材育成に係る検討（内閣官房及び全府省庁）

政府として情報セキュリティ対策を一体的に進めていくための政府職員の人材育成について検討し、政府全体として戦略的に人材育成を行うための基本方針及び具体策を2006年度に示す。

イ）緊急対応能力に係る人材育成手法の検討（内閣官房）

IT障害への緊急対応に係るノウハウを収集し、各政府機関の人材育成へ反映させる方法について検討し、政府全体として戦略的に人材面での緊急対応能力強化を推進するための基本方針及び具体策を2006年度中に策定する。

ウ）情報セキュリティに関する資格保有率向上に係る検討（内閣官房及び全府省庁）

政府機関の情報システム管理部門における、情報処理技術者試験等の資格保有状況等について調査するとともに方向性について検討し、資格保有率の向上に資する具体策を2006年度に示す。

3　政府機関以外の分野での情報セキュリティ人材の育成・確保について

p.47　第5章　第3節　横断的な情報セキュリティ基盤の底上げ

イ）情報セキュリティ教育者、専門家等に係る人材育成・訓練（内閣官房、総務省、文部科学省及び経済産業省）

情報セキュリティ教育者、専門家等に係る人材育成・訓練の機会を増加させるとともに、これらの者の重要性を社会全体が認識し、職業上の地位と評価が確保されるようなキャリアパスの構築に向けた戦略を検討する。

第３期科学技術基本計画　閣議決定：３月２８日、以下関係部分（抜粋）

参考３

第１章　基本理念
３．科学技術政策の理念と政策目標
（１）第３期基本計画の理念と政策目標
第２期基本計画期間中において、国民が最も身近に科学技術への不安を感じるとともに期待が強いのは、健康と安全の問題である。この間、ＳＡＲＳ（重症急性呼吸器症候群）、ＢＳＥ（牛海綿状脳症）、鳥インフルエンザ等国境を越えた感染症の発生、これらも契機とした食の安全性に関する不信感の高まり、花粉症等免疫疾患の深刻化、地震・津波・台風等による大規模自然災害や列車事故等の大規模事故の発生、米国同時多発テロ以来複雑化した国際安全保障環境、情報セキュリティに対する脅威の増大、依然として厳しい治安情勢等、国の持続的な発展基盤である安全と安心を脅かす事態が次々と生じた。その一方で、細胞・分子レベルでの進歩が著しい生命科学による画期的な治療法、予防医学や食の機能性を活用した健康な生活の実現、地震等の自然災害、事故・犯罪等に対する先端科学技術の最適な活用など、健康と安全を守る科学技術への期待は高まっている。
このような状況を受け、子どもから高齢者まで国民を悩ます病を克服し、誰もが生涯元気に暮らせる社会を実現すること、さらには国家・社会レベルから生活者の暮らしに至るまで、安全が誇りとなり世界一安全と言える国を実現することを科学技術政策の目標に位置付ける。

第２章　科学技術の戦略的重点化
２．政策課題対応型研究開発における重点化
（１）「重点推進４分野」及び「推進４分野」
第２期基本計画において、国家的・社会的課題に対応した研究開発の中で特に重点を置き、優先的に資源を配分することとされたライフサイエンス、情報通信、環境、ナノテクノロジー・材料の４分野については、次のような観点から、引き続き基本計画においても、特に重点的に研究開発を推進すべき分野（「重点推進４分野」という。）とし、次項以下の分野内の重点化の考え方に基づきつつ優先的に資源配分を行う。

分野別推進戦略　総合科学技術会議決定：３月２２日、以下関係部分（抜粋）

Ⅱ　情報通信分野
２．重要な研究開発課題
（４）セキュリティ及びソフトウェア領域
① セキュリティ領域
我が国の国民生活・経済活動のあらゆる場面においてＩＴが深く利用されるようになった現在、我が国の社会経済活動の持続的発展と国際競争力の維持という観点からＩＴ基本法にいう「高度情報通信ネットワークを安心して利用可能」な環境とすることが求められている。この環境を実現するに当たり、(a) 急速に拡大するＩＴ利活用に、情報セキュリティ技術の開発が対応できていない、(b) 既存の情報セキュリティ技術の限界を補完する組織・人間系の管理手法とのバランスを欠いているとの問題がある。
これを解決するためには、(a) そもそもの情報セキュリティ技術の高度化を図ると同時に、(b) 開発された情報セキュリティ技術が実環境で効果的・効率的に運用されるため組織・人間系の管理手法の高度化の両面からの取組が必要である。
以上のことから、広範な研究開発投資が必要であり、その中でも特に以下の研究開発課題が重要である。
【課題１】情報セキュリティ技術の高度化
【課題２】技術を補完しより強固な基盤を作るための管理手法の研究

３．戦略重点科学技術
（１）選択と集中の戦略理念
③　全ての国民がＩＴの恩恵を実現できる社会の実現
(c) 安全・安心の具現化に資する情報通信システム技術の研究開発の推進
近年、社会経済活動の基盤機能を提供する、いわゆる重要インフラにおけるＩＴ利用の拡大が著しい。情報セキュリティ政策会議によって２００６年２月に決定された「第１次情報セキュリティ基本計画」では、重要インフラにおける情報通信機能を利用した構成要素の安全性確保は喫緊の課題であるとの認識に基づき、このための研究開発強化は必要不可欠であるとしている。このため「第１次情報セキュリティ基本計画」等に述べられた、安全・安心な社会基盤を形成する取組遂行に必要な科学技術の研究開発を広く実施する。
具体的には、安全・安心なデジタル情報の流通・加工・共有を可能にする情報通信インフラの構築・運用・管理に資する基盤技術ならびに統合化技術の研究開発を実施する。
また、重要インフラを含む、超大規模グローバル社会システムの設計・運用管理を可能にする基盤技術ならびに統合化技術の研究開発を実施する必要がある。
さらに、ＩＴが普遍化した環境を前提として、認証基盤などの新たに生まれてくる重要インフラの社会への組込みを行う実施戦略の設計、ＩＴを最大限活用するための社会システムデザイン研究の強化も併せて実施する。
【戦略重点科学技術１０】世界一安全・安心なＩＴ社会を実現するセキュリティ技術

⑩ 世界一安全・安心なIT社会を実現するセキュリティ技術
情報セキュリティ政策会議によって2006年2月に決定された「第1次情報セキュリティ基本計画」において指摘されているように、重要インフラにおける情報通信機能を利用した構成要素の安全性確保は喫緊の課題であり、このための研究開発強化は必要不可欠である。また、世界有数のブロードバンド大国となった我が国では、IT利用に不安を感じる個人を限りなくゼロにし、安心してITを利用できる環境を整備するという社会及び国民のニーズに迅速に対応することが不可欠である。このため、(1)③(c)で述べた観点から、ネットワーク領域の【課題5】利用者の要求に応じたデペンダブルなセキュアネットワーク、【課題6】幅広い利用者が使いやすい情報通信ネットワーク、セキュリティ領域の【課題1】情報セキュリティ技術の高度化、【課題2】技術を補完しより強固な基盤を作るための管理手法の研究が重要である。したがって、これらの研究開発課題の中核部分を戦略重点科学技術として選定する。

4．推進方策
(2) 各論
④ セキュリティ及びソフトウェア領域
(a) セキュリティ領域
IT依存度が急激に高まるなか、各重要インフラでは、サイバー攻撃、システム障害、人為的ミス及び災害等あらゆる脅威から情報通信機能を利用した活動の安全性ならびに安定的供給を確保することが最優先の課題となっている。そのため、情報セキュリティ技術を構成している多種多様な基礎技術、関連技術の高度化を含めた研究開発強化は必須である。
また、利用者が安全であると認識し、安心して各種情報の伝達や、その加工及び共有等を行える社会を実現するためには、世界最高水準の安全・安心な情報通信インフラを構築する必要がある。さらに、重要インフラを含む次世代ネットワーク環境を視野に入れた環境を実現するために必要となる各種基盤技術及び、それらの統合化技術に関する研究開発を実施する必要がある。
さらに、ITの利用・活用が進展し普遍化した環境を見据え、認証基盤などを国民生活・社会経済活動へスムーズに組み込むための実施戦略の設計として、新たな技術の普及によるIT社会の変化を捉え、必要となる社会制度の整備や、技術の普及戦略を開発する、いわゆる社会システムデザイン研究の強化も併せて実施するべきである。

別表1　重要な研究開発課題の詳細（情報セキュリティ関係部分の抜粋）

別表1 重要な研究開発課題の詳細
1．ネットワーク領域
【課題5】利用者の要求に応じたデペンダブルなセキュアネットワーク
○障害の検知及びネットワーク犯罪の自動検出・回復・予防
○デペンダブルな課金、認証、NW管理
○デペンダブルなネットワーク・オペレーション・システム
○テストベッドによる信頼性、安全性の向上
【課題6】幅広い利用者が使いやすい情報通信ネットワーク
○次世代ネットワークにおける新規アプリケーションの創出とその利用
○テストベットによるキラーアプリケーションの試行育成
○オンデマンドサービスネットワーク構築技術
○利活用の高度化を体系的に推進するサービス構築・提供技術(サービスサイエンス)
○ユニバーサルコミュニケーション技術
・言語の壁を越えるユニバーサルコミュニケーション
・障害者が使いやすいネットワーク

4．セキュリティ及びソフトウェア領域
4．1　セキュリティ領域
【課題1】情報セキュリティ技術の高度化
○脆弱性を無くす高信頼ソフトウェア開発環境構築のための研究開発
例えば、脆弱性を作り込んでしまわないための言語及びその処理系の開発、プログラム開発環境などの統合的な開発、ISO15408 などの高信頼システム開発手法の積極活用を達成するための技術
○ユビキタス環境やGRID環境といった先進的な大規模分散処理環境におけるセキュリティ技術の確立
例えば、資源や処理ノードが大規模分散している環境での安全なデータアクセスとデータ処理の基盤環境作り
○安全なシステムアーキテクチャとOSに係る研究
例えば仮想実行環境を実現する仮想マシン（アダプティブ・セキュア・マシン）技術を使ったセキュリティ管理環境の構築。
○次世代 Trusted Computing 情報基盤技術及び高信頼情報処理アーキテクチャの研究
○情報の長期間保存技術に関する研究
○攻撃遮断技術に関する研究
○脅威分析、脆弱性情報共有技術に関する研究
○情報セキュリティ評価技術に関する研究
【課題2】技術を補完しより強固な基盤を作るための管理手法の研究
○ITに起因するリスクアセスメントに係る研究
○高信頼性組織デザインについての研究
○重要な情報を守るための情報管理技術の確立

＜資料一覧＞

資料１：財団等が実施している情報セキュリティ関連教育プログラムについて【資 1～資 4】
資料２：高等教育機関における主な情報セキュリティ関連教育プログラムについて【資 5～資 11】
資料３：政府機関の実態調査の結果【資 12～資 33】
資料４：日本経団連加盟企業に対するアンケートの結果【資 34～資 75】
資料５：主な情報セキュリティ資格について【資 76～資 82】
資料６：情報セキュリティに係る人材に求められる能力と各種教育プログラムの体系図について【資 83～資 89】

財団等が実施している情報セキュリティ関連教育プログラムについて

	政府施策との関連	概　要	設置経緯
(株)横須賀テレコムリサーチパーク	総務省 情報通信人材研修事業費補助金	■特徴 大規模なネットワークシステムを摸した研究設備を用いた実践中心の研修により、実践的保守・運用スキルの習得及び情報セキュリティマネジメントの実践対応能力の向上を図る。 ■コースの概要 **○座学中心コース（２日間）** ・**「技術レイヤ」向け基礎コース**：①IRRRT（注）の実践を可能とする技術者に必要な基礎知識を習得する。②「管理レイヤ」人材とともにインシデントレスポンスチームのメンバーとして働くために必要最小限のマネジメント的知識に関する知識を習得する。 ・**「管理レイヤ」向け基礎コース**：①IRRRT の実践を可能とする管理者に必要な基礎知識を習得する。②「技術レイヤ」人材と一緒に「システム実習中心コース」を受講するために必要最低限の技術的知識を習得する。 （注）IRRRT：発生したインシデントを迅速に検知し、関係部署と連携を図り的確に処理し、被害を最小限にとどめるとともに、安全にシステム・サービスを回復する一連の処理体系 **○システム実習中心コース（３日間）** ・**イントラ・エクストラネットコース**：イントラ・エクストラネットシステムを対象とした実習中心コース、 ・**Web ビジネスサイトコース**：Web システムを対象とした実習中心のコースで、特にｅコマース系のシステム管理者のインシデントレスポンスに対する対処方法を習得する。 **■受講対象者** **○IRRRT の実践が可能な技術レイヤ人材**：情報セキュリティ業務系管理者、システム管理者、ネットワーク管理者へ技術的助言ができる技術者 **○IRRRT の実践が可能な管理レイヤ人材**：情報セキュリティマネジメントにおいて、各関連部署との	H17 年度：開講

資料１

注）本資料は、現在実施されている情報セキュリティ関連教育プログラムのうち、主なものについて調査し単純に列挙したものであり、本委員会としてこれらの教育プログラムを特に推奨しようとするものではない。

		連携をとったり、技術レイヤ人材に対しても的確な指示やマネジメント的助言ができる業務系管理技術者 **■定員及び受講料** **受講料　40 万円／人** 各コース（座学中心コース２日間、システム実習コース３日間）※ ※　座学中心コースの各レイヤ向けコースとシステム実習コースの各コースは、それぞれ自由に組み合わせ受講することができます。 **定員　約 600 名／年(各コース合計)** **■補助金額** 203,995 **千円**	
(財)ひょうご情報教育機構	同上	■特徴 大型計算機環境再現装置により、民間企業等の典型的な大規模ネットワーク環境を構築し、情報セキュリティ侵害事案を主体とした実践的カリキュラムを策定することにより、受講者のレベル・スキルに応じ、基礎からネットワーク管理運用技術者向けの高度なレベルの階層研修を実施。 **■コースの概要** **○共通コース（初級）（２日間）** ・情報セキュリティ総括基礎講座：情報セキュリティ侵害と攻撃、情報セキュリティマネジメント、セキュリティインシデント　等 ・情報セキュリティ管理及び監査基礎講座：情報セキュリティマネジメントシステムの概要、ISMS 適合評価制度と構築のポイント、情報セキュリティ監査　等 ・モバイルセキュリティ基礎講座：モバイルコンピューティング、無線 LAN セキュリティ対策　等 **○基礎コース（中級）（14 日間）** ・座学（６回）：セキュリティとプライバシー、情報セキュリティ監査、法制（個人情報保護法、プロバイダ責任制限法）　等 ・実践（８回）：ソフトウェアの脆弱性、侵入解析の基礎　等	H18 **年度：開講**

		○**応用コース**（上級）（14 日間） ・座学（６回）：サイバー犯罪・サイバーテロ、情報セキュリティインシデントと対策技術の動向、法制（電子商取引法、知的財産法）　等 ・実習（８回）：侵入されたシステムの解析、システムへの攻撃と防御　等 ■**受講対象者** ○**共通コース**：一般的な SE として最低限の知識と実務経験を有している者 ○**基礎コース**：専門的・実践的な知識と実務経験を有している者 ○**応用コース**：高度な知識と実務経験を有している者※ ※応募資格：①UNIX 又は LINUX サーバの構築・運用の経験を有すること ②企業、行政、大学等のネットワーク運用管理者の経験を有すること ■**定員及び受講料** **共通コース（初級）：各講座 15 名、受講料３万円** **基礎コース（中級）：10 名程度、受講料 40 万円** **応用コース（上級）：10 名程度、受講料 40 万円** ■**補助金額** 75,516 **千円**	
(財)ソフトピアジャパン	同上	■特徴 典型的な企業内ネットワークとインターネット環境を仮想的に構築し、インシデントを擬似的に発生させることにより、受講者がこれに対応するための業務面及び技術面双方における対応手順を習得。これにより、組織内での体系的セキュリティマネジメントの実践対応能力の向上を図る。 ■**コースの概要** ○**テクニカル系** ・**セキュリティテクニカルコース**(2 日間)：インシデントに対し発生を迅速に検知し、的確に対処して、被害を最小限にとどめ、安全にサービスを回復させることができる現場対応能力・応用力を持つ人材を育成。	H18 **年度：開講**

		・セキュリティテクニカル実践コース（５日間）：情報セキュリティ業務系管理者や、システム管理者、ネットワーク管理者に対して技術的助言ができる技術者を育成。 **〇マネジメント系** **・セキュリティマネジメントコース**（２日間）：不正アクセス手法・対策・防御法、情報セキュリティマネジメント、インシデントレスポンスの基礎等を学び情報セキュリティマネジメントのための手法やＰＤＣＡの設計ができる人材を育成。 **・セキュリティマネジメント実践コース**（５日間）：マネジメント的な立場でのインシデントレスポンスを体得するとともに、マネジメント実装のための手順、ポリシー策定を中心としたスキルを習得し、各関連部署との連携や的確な指示や助言ができる業務系管理者を育成。 **■受講対象者** **〇テクニカル系**：システム・ネットワーク管理の知識・技術を有する中級・上級クラスのシステム管理者・技術者、ネットワーク管理者・技術者、及びその補佐をする者 **〇マネジメント系**：組織の情報セキュリティマネジメントの実施推進者及びその予定がある者。PDCAサイクルの運用・検査を行う実務担当者 ■　定員及び受講料 480 **名／年(各コース合計)** **テクニカル系** **・セキュリティテクニカルコース：**84,000 **円** **・セキュリティテクニカル実践コース：**210,000 **円** **マネジメント系** **・セキュリティマネジメントコース：**84,000 **円** **・セキュリティマネジメント実践コース：**210,000 **円** **■補助金額** 88,463 **千円**	

注）本資料は、現在実施されている情報セキュリティ関連教育プログラムのうち、主なものについて調査し単純に列挙したものであり、本委員会としてこれらの教育プログラムを特に推奨しようとするものではない。

高等教育機関における主な情報セキュリティ関連教育プログラムについて

教育機関名	機関の位置づけ/政府施策との関連	カリキュラムの概要	学生数/卒業者数	設置経緯/実績
中央大学	**大学院**	■カリキュラムの名称等 **大学院理工学研究科** ■カリキュラムの目的･内容 **情報工学専攻において、情報セキュリティに関する講義・研究を実施。** **また、H15 年度からは、「電子社会・情報セキュリティ副専攻」を開設。本副専攻では、情報セキュリティの向上には、技術的対策に併せて、管理運営・システム監査、法的遵守などの面からの総合的対策が不可欠との視点に立ち、工学系科目に加えて、社会系科目を設け、技術者でありながらも、総合的な広い視野をもってセキュリティマネジメントに当たることのできる人材を育成している。** ■実技･実習について **特になし（実技については、人材育成拠点プログラムで習得可能）** ■学費 817,800 **円（入学金：**240,000 **円、在学料：**535,800 **円、実験実習料** 42,000 **円）**	H15 **修士** 11 H16 **修士** 19 H17 **修士** 4 **合計** 34 **名**	H15 **年度：開設**
情報セキュリティ大学院大学	**大学院大学**	■カリキュラムの名称等 **情報セキュリティ研究科 情報セキュリティ専攻 修士課程** ■カリキュラムの目的･内容 **セキュアなシステム・プロダクトの開発、設計、構築ができる技術者である「情報セキュリティエンジニア」、組織のセキュリティレベルを維持･向上することで差別化による競争優位を創出するリーダーとなる「情報セキュリティマネージャ」の育成を目的とした大学院大学で、以下の３つの修了要件からなる。** ・博士前期課程（2 年制）	**○毎年の学生数** **定員** 49 **名** **○修了者数** H17 **年度** **修士：**21 **名**	H16.4 **博士前期課程開講** H18.4 **博士後期課程開講**

資料２

注）本資料は、現在実施されている情報セキュリティ関連教育プログラムのうち、主なものについて調査し単純に列挙したものであり、本委員会としてこれらの教育プログラムを特に推奨しようとするものではない。

		原則２年以上、30 単位以上、修士論文審査・最終試験 ・博士前期課程（1 年制） １年以上、46 単位以上、リサーチペーパー ・博士後期課程 原則 3 年以上、8 単位以上、博士論文審査・最終試験 ■実技･実習について **・セキュアシステム実習：防御・攻撃システム環境を構築し、攻撃を防御を実際に行いながら知識・技能を学ぶ　90 分×3 限×10 回** **・プログラミング：C 言語による実習　90 分×15 回** **・ソフトウェア構成論：Java の実習　90 分×15 回** **・リスクマネジメント、情報セキュリティマネジメントシステム、：ケーススタディ、グループ討議、プレゼンテーション等を実施** **・プレゼンテーション技法：模擬記者会見、プレゼンテーション** ■学費 **【2 年制コース】** **初年度 1,500 千円（次年度以降 1,200 千円）** **（入学金 300 千円、授業料 1,000 千円、施設設備費 150 千円、実習費 50 千円）** **【1 年制コース】** **2,300 千円** **（入学金 300 千円、授業料 1,800 千円、施設整備費 150 千円、実習費 50 千円）** **【博士課程後期】** **初年度 1,300 千円（次年度以降 1,000 千円）** **（入学金 300 千円、授業料 800 千円、施設整備費 150 千円、実習費 50 千円）**		
カーネギーメロン大学日本校	**文部科学大臣の指定を受けた「外国の大学院の修士課**	■カリキュラムの名称等 **情報セキュリティ研究科修士課程（MSIT-IS）** **（米国 Carnegie Mellon University の Master of Science）**	**○毎年の学生数** **10 名程度** **○在学者数**	H17.8 **開講**

	程を有する教育施設」（外国大学院日本校）	■カリキュラムの目的･内容 企業組織等の CISO、コンサルタント、教育者や研究者など、技術と経営・政策の双方に通用する情報セキュリティの高度人材を育成する。 期間：1 年 4 ヶ月（1 学期 4 ヶ月×4 学期） 修了に必要な単位：144 単位（必修科目 60 単位、選択科目 48 単位、プロジェクト 36 単位） ■実技･実習について マネジメントに関する科目では、企業の CISO になったとの想定の下、ネットワークからの攻撃など様々な状況を付与した際に、どのように判断し対応すべきかといった演習等を実施。 また、科目ごとに、グループワーク等による研究プロジェクトが課され、チームとして課題に取り組み、実用的なシステム開発などを実施。システム設計に関するプロジェクトでは、実際に企業で利用されているシステムやネットワークの脆弱性を分析し、改善提案を実施する。 ■学費（H17 年度実績） 登録料：100 ドル（約 1.1 万円） 授業料：約 696 万円（1 学期あたり 15,800 ドル（約 174 万円）） 教材費：実費	9 名	
中央大学	平成 15 年度科学技術振興調整費・新興分野人材養成	■カリキュラムの名称等 「情報セキュリティ・情報保証　人材育成拠点」 ■カリキュラムの目的･内容 学生や社会人を対象に、主に実践教育を中心とした情報セキュリティ技術者を育成（Windows 等の OS セキュリティ、セキュアプログラミング、SANS 講座等）。 ■実技･実習について	H15　40 H16　213 H17　264 合計　517 名	H15 年度：開講 H19 年度：終了予定

注）本資料は、現在実施されている情報セキュリティ関連教育プログラムのうち、主なものについて調査し単純に列挙したものであり、本委員会としてこれらの教育プログラムを特に推奨しようとするものではない。

		ハンズオン形式での実践多数。 ■学費 無料		
工学院大学	平成 15 年度科学技術振興調整費・新興分野人材養成	■カリキュラムの名称等 技術者能力開発センター（CPD センター） 「セキュアシステム設計技術者育成プログラム」 ■カリキュラムの目的･内容 特に社会人を中心に、ライフサイクル全般にわたるセキュリティ要件を上流行程に組み込み設計できる技術者を産学連携で養成するプログラム。体系的な基礎知識を得るための講義と、実務的知識を得るための PBL（Project Based Learning;課題解決型学習）からなる。 （平成 17 年度実績） 期間：5 月中旬～11 月末、土曜日 6 時間 講義科目数：24＋特別講義 4、総時間：168 時間 ■実技･実習について 受講生を 7～8 人のグループに分けて、実際の企業から提示される課題に対して先進的システムを提案する PBL を実施。 ■学費 実費（入学金、授業料等はなし）	○毎年の学生数 定員 40 名 ○修了者数実績 （H18 は受講者数） H15 年度　0 名 H16 年度　43 名 H17 年度　41 名 H18 年度　46 名	H15 年度：開講準備 H16 年度：開講 H19 年度：終了予定
中央大学	平成 14 年度 21 世紀 COE プログラム	■カリキュラムの名称等 「電子社会の信頼性向上と情報セキュリティ」 ■カリキュラムの目的･内容 情報セキュリティの中心的技術である暗号などを基礎として、電子社会を支える要素技術、高信頼性ネットワークシステム、電子行政・電子ビジネスのための電子	高度な研究者を育成するプログラムであり、修了者数等を把握しているものではない。	H14 年度：開設 H18 年度：終了予定

注）本資料は、現在実施されている情報セキュリティ関連教育プログラムのうち、主なものについて調査し単純に列挙したものであり、本委員会としてこれらの教育プログラムを特に推奨しようとするものではない。

		社会システムに関する高度な研究者の育成を目的とした研究拠点プロジェクト。 ■実技･実習について 高度な研究者を育成するものであり、実技を習得することを目的としていない。 ■学費 高度な研究者を育成するものであり、このプログラムのための学費がある訳ではない。		
大阪大学	H13 年度科学技術振興調整費・新興分野人材養成	■カリキュラムの名称等 サイバーメディアセンター、情報系専攻 「セキュア・ネットワーク構築のための人材育成プログラム」 （Secure Net プログラム） ■カリキュラムの目的･内容 情報系専攻大学院生・学部学生、社会人などを対象に、以下の２つのコースを設け、特に応用コースに重点を置いたカリキュラムにより、ネットワーク運用現場での即戦力となるような人材の育成を目指す。 ・「基礎コース」（講義） …情報セキュリティに関する一般的な知識の習得 ・「応用コース」（実習） …「基礎コース」を習得した学生を対象に、実運用ネットワークにおける運用経験（OJT）を積むための演習 また、委託先の日本電気株式会社によるセキュリティ監査を通じて、実習技能の検証と処理能力の向上、評価を図ることとされている。 ■実技･実習について 「応用コース」において、実運用ネットワークとして「大阪大学キャンパスネットワーク（ODINS）上での演習を実施する。	○修了者数実績 H13 社会人 4 博士 3 修士 6 H14 社会人 15 博士 7 修士 8 H15 社会人 16 博士 2 修士 6 H16 社会人 20 博士 4 修士 4 H17 社会人 23 博士 2 修士 12 延べ 132 名	H13 年度から「基礎コース」を開始 H14 年度以降､「基礎コース」と「応用コース」を実施 H17 年度に終了（財団法人ひょうご情報教育機構「情報通信セキュリティ人材育成センター」に継承）

		■学費 **無料**		
早稲田大学	H13 **年度科学技術振興調整費・新興分野人材養成**	■カリキュラムの名称等 **理工学部コンピュータ・ネットワーク工学科** **「セキュリティ技術者養成プロジェクト」** ■カリキュラムの目的･内容 **学部学生向けおよび大学院学生向けに以下の３つの講座を開設。** ①「ネットワークセキュリティ設計」（学部生対象）半期【H14 年度～】 …情報セキュリティに関する基本的な知識の習得 （注）H14～17 年度までの講座名は「ネットワークセキュリティ基礎」 ②「情報セキュリティ特論（A)」（大学院学生対象）半期【H14～16 年度】 …最先端のセキュリティ技術の状況の理解とその弱点等を習得 ③「情報セキュリティ特論（B)」（大学院学生対象）半期【H14～16 年度】 …セキュリティをめぐる法律的、社会的側面について習得 **平成 16 年度からは、Microsoft 社と連携して、体系的な Windows のコンピュータセキュリティ技術カリキュラムも開設。** ④「リアルタイム 3D グラフィックスプログラミング」【H16 年度～】 ⑤「プロジェクト管理」【H16 年度～】 ⑥「情報セキュリティ技術 A」【H16 年度～】 ⑦「オペレーティングシステム実装論 A」【H16～17 年度】 ■実技･実習について **上記④の講座については、プログラミング実習を実施。** ■学費 (理工学部･大学院理工学研究科としての学費) **【学部・初年度】**	○**例年の受講者数** **①約 50 名** **②約 20～25 名** **③約 20～25 名** **④約 35 名** **⑤約 110 名** **⑥約 100 名** **⑦約 100 名** ○**累積受講者数** **（H14～17 年度）** **①約 200 名** **②約 70 名** **③約 70 名** **④約 70 名** **⑤約 220 名** **⑥約 200 名** **⑦約 200 名**	H13 **年度：開講準備** H14 **年度：開講** H16 **年度：**Microsoft **社との連携講座開講**

		1,678 千円 （入学金 290 千円、授業料 1,069 千円、施設費 235 千円、実験実習料 84 千円） 【理工学研究科・初年度】 1,198.5 千円 （入学金 260 千円、授業料 704 千円、施設費 150 千円、実験演習料 84.5 千円）		
東京電機大学		■カリキュラムの名称等 大学院工学研究科「情報セキュリティ講座」 ■カリキュラムの目的･内容 東京電機大学が SEA/J と連携し、学生と社会人の両方に役立つことを目的として、理論的部分から実際的部分、基礎的部分から応用的部分まで広く学ぶことができるよう、以下の３つの講座を実施。 ①「暗号とその応用」（12 回：東京電機大学担当） ②「ネットワークのセキュリティ」（12 回：SEA/J 担当） ③「不正侵入対策の実際」（12 回：SEA/J 担当） ■実技･実習について ②・③の講座においては、実際に公開サーバの構築・運用を行うとともに、インシデントレスポンスの技術を学ぶ。 ■学費 社会人受講生は、①は 10 千円、②・③は各 30 千円	○毎年の学生数 社会人は各講座 15 名 ○受講者数実績 H16 年度 ①院生 35 名 社会人 13 名 ②院生 16 名 社会人 17 名 ③院生 15 名 社会人 13 名 H17 年度 ①院生 12 名 社会人 13 名 ②学生 17 名 社会人 17 名 ③学生 17 名 社会人 13 名	H16 年度、H17 年度の２年間実施

注）本資料は、現在実施されている情報セキュリティ関連教育プログラムのうち、主なものについて調査し単純に列挙したものであり、本委員会としてこれらの教育プログラムを特に推奨しようとするものではない。

資料3

政府機関の実態調査の結果

＜概要＞

調査目的　　：政府機関における情報セキュリティに関する人材の育成・確保状況を調査するため。

調査期間　　：2006 年 8 月 16 日～9 月 1 日

回答者　　：各府省庁の情報セキュリティ対策を主幹する部門、又は情報システム統括部門、もしくはそれに準ずる部署において、情報セキュリティに関する業務に携わる者

回答形式　　：任意回答、回答できない部分は無回答または不明として回答。

結果の取扱い：個別府省庁名の公表はしない、また、評価の対象とはしない。

＜アンケート用紙＞・・・・・・・・・・・・・・・・・・・・・・・・・・・・-資 13-

＜アンケート結果＞・・・・・・・・・・・・・・・・・・・・・・・・・・・・-資 23-

情報セキュリティに関する人材育成･確保に関するアンケート

府省庁名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

部局課係名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

１．本アンケートの回答者

このアンケートは、府省庁の組織全体としての情報セキュリティに関する人材の育成・確保と資格制度の取得状況に関する現状の把握、及び問題点の全体像を把握することを意図しています。

各府省庁の情報セキュリティ対策を主管する部門、又は情報システム統括部門、もしくはそれに準ずる部署の方にご回答をお願いいたします。なお、数字を伴わない府省庁の状況に関する質問については、ご担当者様の主観に基づいたご回答で構いません。

２．本アンケートの対象範囲

本アンケートにおいては、貴府省庁の本省、外局（※地方支分部局、特別の機関、施設等機関は除きます）における情報セキュリティに関する人材育成・確保の状況についてご回答いただきたく、お願いいたします。

３．本アンケートに対する回答の方法

質問項目をお読みいただき、該当する選択肢のチェックボックスを塗りつぶしてください。

（記入例）

■ 情報セキュリティに関する業務を専任で担当する職員がいる　２人

なお、人数や金額等、数字を答えるものについては、はっきりした数字がわからなければ、大まかな数字で結構です。なお、いただきましたご回答に対して誤解を避けるためにも、特に必要な場合には注釈を付け加えていただきたくお願いいたします。

現在の情報セキュリティ管理体制

Q01　貴府省庁内における職員の情報セキュリティ意識について、教えて下さい。（あてはまるものをすべて選んでください。）

- □ トップから一般職員に至るまで、情報セキュリティ意識は高い
- □ トップから管理職クラスまでは意識が高いが、それより下になると意識は低い
- □ 意識が高いのは、トップまでである
- □ 情報セキュリティに関する業務に従事している者以外は、意識は低い
- □ 人によって意識の高さはまちまちだが、総じて意識は高い
- □ 人によって意識の高さはまちまちだが、総じて意識は低い

Q02　貴府省庁には情報セキュリティに関する業務を担当する職員（外注要員は含みません）はいますか。（あてはまるものをすべて選んでください。なお、専任の担当者がいる場合は、お手数ですがその人数もご回答ください。正確に把握していなければ、概数で結構です。）

- □ 情報セキュリティに関する業務を担当する職員はいない
- □ 情報セキュリティに関する業務を兼務で担当する職員がいる
- □ 情報セキュリティに関する業務を専任で担当する職員がいる　＿＿人

Q03　Q02 で「情報セキュリティに関する業務を専任で担当する職員がいる」と回答された組織の方に伺います。担当者の方は、具体的にはどのような分野の業務に従事されていますか。（あてはまるものをすべて選んでください。）

- □ 情報セキュリティマネジメント（セキュリティポリシー構築、情報資産管理、リスクマネジメント、人員計画、体制構築、BCM 等）
- □ 情報セキュリティに係る法制度・標準・規格類（ISMS、ISO/IEC15408 等）の検討や運用
- □ 情報セキュリティ監査
- □ セキュリティ要件定義、セキュリティ設計
- □ アクセスコントロール（アクセス権限管理、認証）

□ ネットワークセキュリティ（ファイアウォール、侵入検知等）
□ アプリケーションセキュリティ（サーバアプリケーション、OS 等）
□ セキュリティの運用・緊急時対応（ID マネジメント、パッチ管理、ウイルス・不正アクセス対応等）
□ 暗号関係（暗号、PKI、電子署名等）
□ その他（　　）

Q04　貴府省庁内の情報セキュリティに関する業務を担当する外注要員はいますか。（あてはまるものをすべて選んでください。なお、担当者がいる場合は、お手数ですがその人数もご回答ください。正確に把握していなければ、概数で結構です。）

□ 情報セキュリティに関する業務を担当する外注要員はいない
□ 情報セキュリティに関する業務を担当する外注要員がいる
　　人

Q05　Q04 で「情報セキュリティに関する業務を担当する外注要員がいる」と回答された組織の方に伺います。担当者の方は、具体的にはどのような分野の業務に従事されていますか。（あてはまるものをすべて選んでください。）

□ 情報セキュリティマネジメント（セキュリティポリシー構築、情報資産管理、リスクマネジメント、人員計画、体制構築、BCM 等））
□ 情報セキュリティに係る法制度・標準・規格類（ISMS、ISO/IEC15408 等）の検討や運用
□ 情報セキュリティ監査
□ セキュリティ要件定義、セキュリティ設計
□ アクセスコントロール（アクセス権限管理、認証）
□ ネットワークセキュリティ（ファイアウォール、侵入検知等）
□ アプリケーションセキュリティ（サーバアプリケーション、OS 等）
□ セキュリティの運用・緊急時対応（ID マネジメント、パッチ管理、ウイルス・不正アクセス対応等）
□ 暗号関係（暗号、PKI、電子署名等）
□ その他（　　）

情報セキュリティに関する各種資格制度の取得状況と評価・要望等

Q06　Q02でお答えいただいた情報セキュリティに関する業務を担当する職員の中で、以下の資格を持っている方は何名いますか（あてはまるものをすべて選んでください。なお、資格取得者がいる場合は、お手数ですがその人数もご回答ください。正確に把握していなければ、概数で結構です。）

	専任担当者	兼務担当者
□ 情報セキュリティアドミニストレータ	____ 人	____ 人
□ テクニカルエンジニア（情報セキュリティ）	____ 人	____ 人
□ NISM の情報セキュリティ資格	____ 人	____ 人
□ セキュリティ監査人関連資格（システム監査技術者、CISA、公認システム監査人等）	____ 人	____ 人
□ 公認情報セキュリティマネージャー	____ 人	____ 人
□ 情報セキュリティ検定	____ 人	____ 人
□ CIW の情報セキュリティ資格	____ 人	____ 人
□ CompTIA の情報セキュリティ資格	____ 人	____ 人
□ SANS の情報セキュリティ資格	____ 人	____ 人
□ CISCO の情報セキュリティ資格	____ 人	____ 人
□ Oracle の情報セキュリティ資格	____ 人	____ 人
□ Microsoft の情報セキュリティ資格	____ 人	____ 人
□ Sun Micro の情報セキュリティ資格	____ 人	____ 人
□ その他の情報セキュリティ資格		
（資格名：	____ 人	____ 人）
（資格名：	____ 人	____ 人）
（資格名：	____ 人	____ 人）
（資格名：	____ 人	____ 人）

Q07　現在提供されている、各種の情報セキュリティ資格制度全般（Q06 参照）に対する評価を以下から選んで下さい。（あてはまるものを１つ選んでください。）

□ 全く問題ない
□ 全般的にほとんど問題はないが、若干改善すべきところがある

□ 全般的にやや問題があり、いくつか改善すべきところがある
□ 全般的にかなり問題があり、改善すべき点が多い
□ 全般的に大きな問題があり、抜本的な改善が必要
□ よく分からない
□ その他（　　）

Q08　Q07 で「やや問題がある」、「かなり問題がある」、「大きな問題がある」と回答された方に伺います。
情報セキュリティ資格制度全般について改善すべき点を教えて下さい。

（　　）

Q09　情報セキュリティ資格の更新制に対する考え方を以下から選んで下さい。（あてはまるものを１つ選んでください。）

□ 全ての情報セキュリティ資格を更新制にすべき
□ 大部分の情報セキュリティ資格を更新制にすべき
□ 必要なものだけ更新制にすべき
□ 特に考えはない
□ その他（　　）

Q10　現存の個別の情報セキュリティ資格で役に立たないと思うものや改善が必要だと思うものがあれば、具体的資格の名称と改善すべき点を教えて下さい。

（　　）

情報セキュリティ人材の育成・確保手法

Q11　貴府省庁内で情報セキュリティ人材（情報セキュリティ業務担当者及び今後情報セキュリティ業務を担当する予定の者）を育成・確保するための計

画等（明文化されたもの）を策定していますか。（あてはまるものを１つ選んでください。）

- □ 策定している（策定時期：＿＿＿＿＿＿＿＿）
  → 当該計画等の概要が分かるものを添付いただけると幸いです。
- □ 策定していないが今後策定する予定である
- □ 策定していないし今後策定する予定もない

Q12 情報セキュリティ人材を貴府省庁内にて「育成」（府省庁内の既存の人材を育成）するために、現在貴府省庁で実施している方策を以下から選んで下さい。（あてはまるものをすべて選んでください。）

- □ 内部職員による研修の実施
- □ 外部の要員による研修（外部委託研修も含む）の実施
- □ ＯＪＴの活用
- □ 人事ローテーションの活用
- □ 職員の自主的な社外研修への支援（資格取得のための金銭的補助や勤怠優遇等）
- □ 情報セキュリティ資格取得後の処遇措置（基本給の上昇、報奨金等）
- □ 情報セキュリティ人材の「育成」は行っていない
- □ その他（　　）

Q13 情報セキュリティ人材を「育成」（府省庁内の既存の人材を育成）するために、現在貴府省庁で年間にかかっている予算額はいくらですか。

- □ 500 万超
- □ 100 万～500 万
- □ 50 万～100 万
- □ 50 万未満
- □ 不明

Q14 情報セキュリティ人材を「確保」（外部から調達）するために、現在貴府省庁で実施している方策を以下から選んで下さい。（あてはまるものをすべて選んでください。）

□ 情報セキュリティに関する知識や経験を有する職員を採用する
□ 情報セキュリティに関する知識や経験を有する職員を非常勤職員等として採用する
□ 情報セキュリティに関する知識や経験を有する業者に外注する
□ 他府省庁や関連組織の情報セキュリティに関する知識や経験を有する職員に協力を依頼する（出向者も含む）
□ 情報セキュリティ人材の「確保」は行っていない
□ その他（　　）

Q15　情報セキュリティ人材を「確保」（外部から調達）するために、現在貴府省庁で年間にかかっている予算額はいくらですか。

□ 1000 万超
□ 500 万～1000 万
□ 100 万～500 万
□ 100 万未満
□ 不明

今後の方針と課題

Q16　貴府省庁における現在の情報セキュリティ人材の育成･確保状況について教えて下さい。（あてはまるものを１つ選んでください。）

□ 情報セキュリティ人材は特に不足していない
□ 情報セキュリティ人材は不足している
□ わからない

Q17　Q16 で「情報セキュリティ人材は不足している」と回答された方に伺います。貴府省庁において不足していると感じる情報セキュリティ人材の分野又は能力を以下から選んでください。（あてはまるものをすべて選んでください。）

□ 情報セキュリティマネジメント（セキュリティポリシー構築、情報資産管理、リスクマネジメント、人員計画、体制構築、BCM 等）

□ 情報セキュリティに係る法制度・標準・規格類（ISMS、ISO/IEC15408等）
□ 情報セキュリティ監査
□ セキュリティ要件定義、セキュリティ設計
□ アクセスコントロール（アクセス権限管理、認証）
□ ネットワークセキュリティ（ファイアウォール、侵入検知等）
□ アプリケーションセキュリティ（サーバアプリケーション、OS 等）
□ セキュリティ運用・緊急時対応（ログ、パッチ管理、ウイルス・不正アクセス対応等）
□ 暗号関係（暗号、PKI、電子署名等）
□ その他（　　）
□ 全般的に不足している。

Q18　今後育成・確保したい必要な情報セキュリティ人材のイメージを教えて下さい。（あてはまるものをすべて選んでください。）

□ 府省庁の情報セキュリティを企画・立案する者
□ 情報システムの開発や運用にあたって、利用者と開発者間で情報セキュリティ面からの検討や調整等を行う者（ベンダの選定等を含む）
□ 情報セキュリティ機能を開発・実装する者
□ 情報セキュリティ機能を運用する者
□ 情報セキュリティ技術に関する調査・研究を行う者
□ 府省庁の情報セキュリティの維持状況を監視・検査する者
□ その他（　　）

Q19　貴府省庁において情報セキュリティ人材を育成・確保する上での方針を以下から選んで下さい。（あてはまるものをすべて選んでください。）

□ 可能な限り自府省庁内で情報セキュリティ人材を保有していく
□ 可能な限り外部の情報セキュリティ人材を活用していく
□ 必要な情報セキュリティ人材は府省庁内部で保有するが、それ以外については外部の人材を活用していく
□ 特に方針は立てていない
□ 情報セキュリティ人材を積極的に育成・確保する考えはない
□ その他（　　）

Q20 情報セキュリティ人材を育成・確保していくうえでの障害になっていると思われる問題点があれば教えてください。（あてはまるものをすべて選んでください。）

- □ 特に障害になっている問題点はない
- □ 府省庁内（予算担当部門等）への費用対効果の説明が困難
- □ 定員上の問題等で、府省庁内にふさわしい人材がいてもなかなか情報セキュリティ部門に配置できない
- □ 外部の情報セキュリティ人材が不足（採用したい人材や派遣して欲しい人材がいない等）
- □ 府省庁内・外を問わずどのような人材に情報セキュリティ業務に携わらせたらよいかわからない
- □ 技術の進歩が早すぎて即応が難しい
- □ 各種資格の効果が不明瞭である
- □ 府省庁内の業務に精通していなければ情報セキュリティ業務を行うことが困難である
- □ 幹部の理解不足
- □ 一般職員の理解不足
- □ ＯＪＴだけでは人材育成がうまくいかない
- □ 研修だけでは人材育成がうまくいかない
- □ 何をすればいいのかわからない
- □ その他（　　）

Q21　今後貴府省庁で「育成」（府省庁内の既存の人材を育成）していくことを検討している情報セキュリティ人材の分野又は能力を以下から選んで下さい。（あてはまるものをすべて選んでください。）

- □ 情報セキュリティマネジメント（セキュリティポリシー構築、情報資産管理、リスクマネジメント、人員計画、体制構築、BCM 等）
- □ 情報セキュリティに係る法制度・標準・規格類（ISMS、ISO/IEC15408 等）
- □ 情報セキュリティ監査
- □ セキュリティ要件定義、セキュリティ設計
- □ アクセスコントロール（アクセス権限管理、認証）

□ ネットワークセキュリティ（ファイアウォール、侵入検知等）
□ アプリケーションセキュリティ（サーバアプリケーション、OS 等）
□ セキュリティ運用・緊急時対応（ログ、パッチ管理、ウイルス・不正アクセス対応等）
□ 暗号関係（暗号、PKI、電子署名等）
□ その他（　　）
□ 全般的に「育成」していく
□ 「育成」していく予定はない
□ 特に決まっていない

Q22　今後貴府省庁で「確保」（外部から調達）していくことを検討している情報セキュリティ人材の分野又は能力を以下から選んで下さい。（あてはまるものをすべて選んでください。）

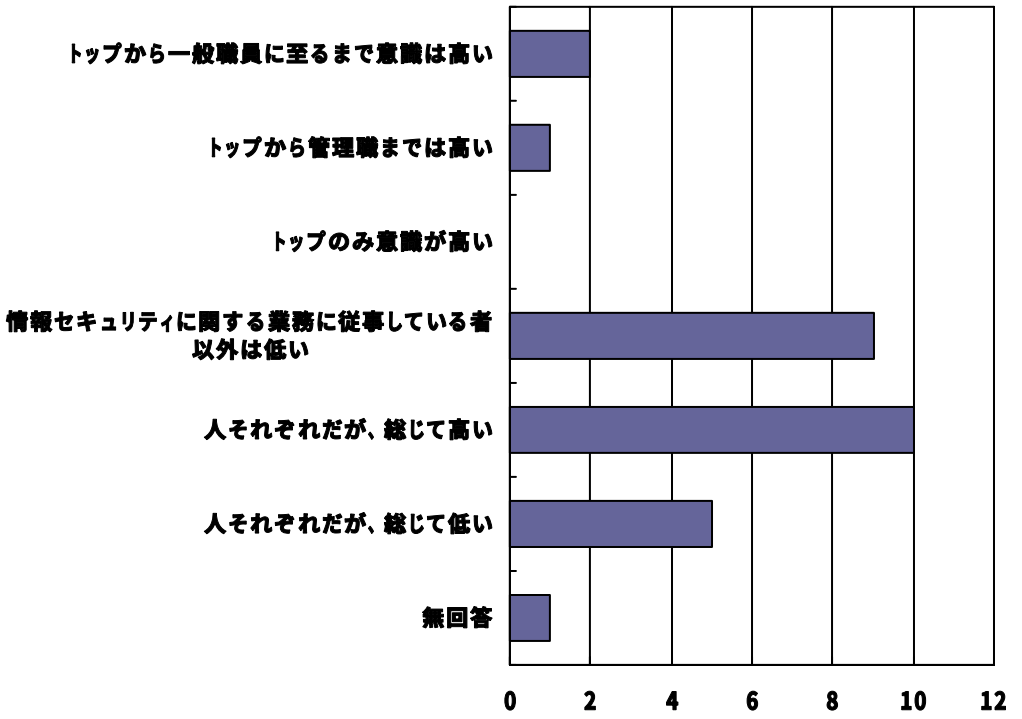
□ 情報セキュリティマネジメント（セキュリティポリシー構築、情報資産管理、リスクマネジメント、人員計画、体制構築、BCM 等）
□ 情報セキュリティに係る法制度・標準・規格類（ISMS、ISO/IEC15408 等）
□ 情報セキュリティ監査
□ セキュリティ要件定義、セキュリティ設計
□ アクセスコントロール（アクセス権限管理、認証）
□ ネットワークセキュリティ（ファイアウォール、侵入検知等）
□ アプリケーションセキュリティ（サーバアプリケーション、OS 等）
□ セキュリティ運用・緊急時対応（ログ、パッチ管理、ウイルス・不正アクセス対応等）
□ 暗号関係（暗号、PKI、電子署名等）
□ その他（　　）
□ 全般的に「確保」していく
□ 「確保」していく予定はない
□ 特に決まっていない

以上

お疲れ様でした

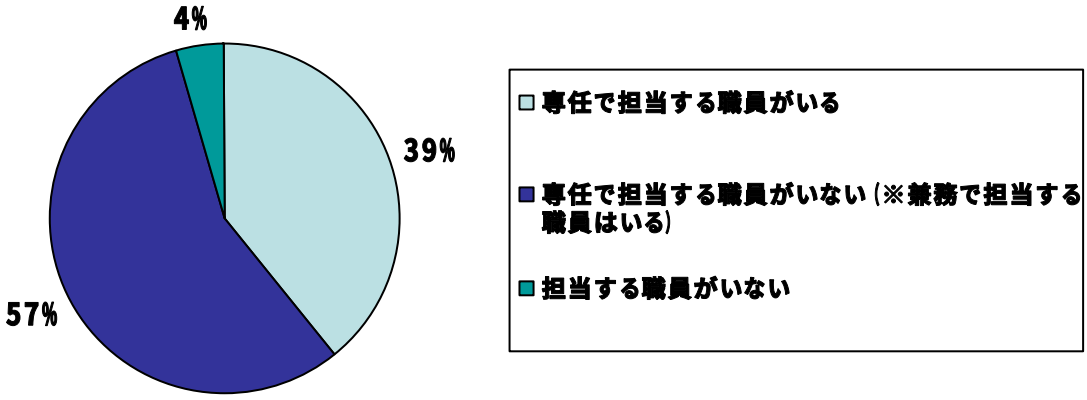
＜アンケート結果＞

Q01　情報セキュリティに関する意識の現状



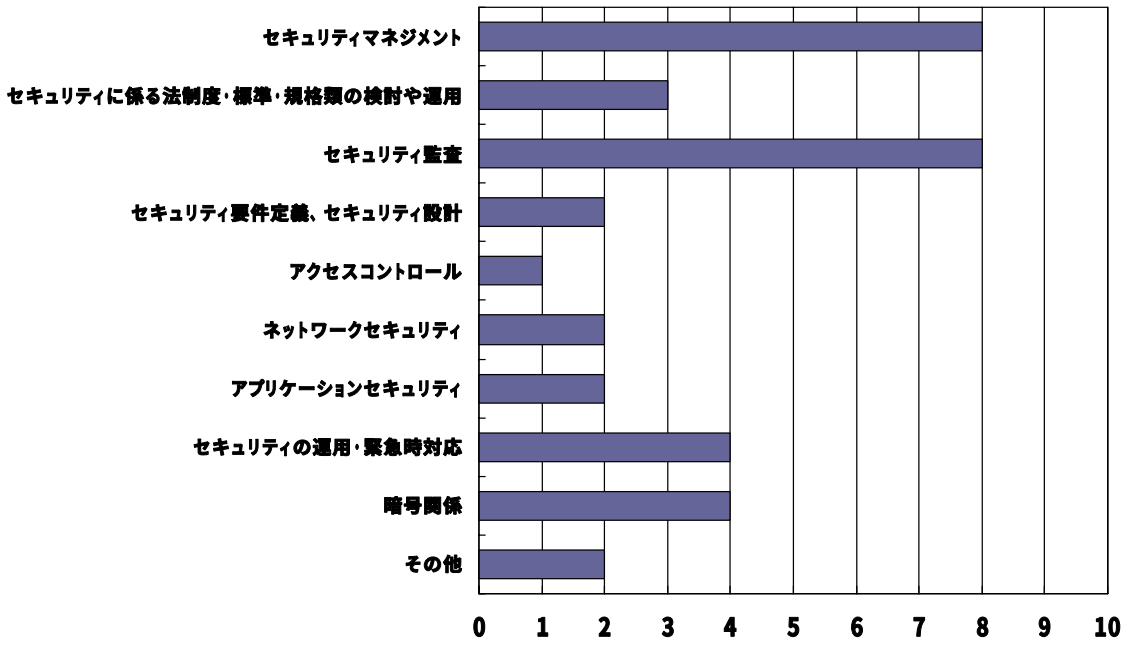
（有効回答：23府省庁、複数回答可能項目）

Q02　情報セキュリティ専任職員の配置状況



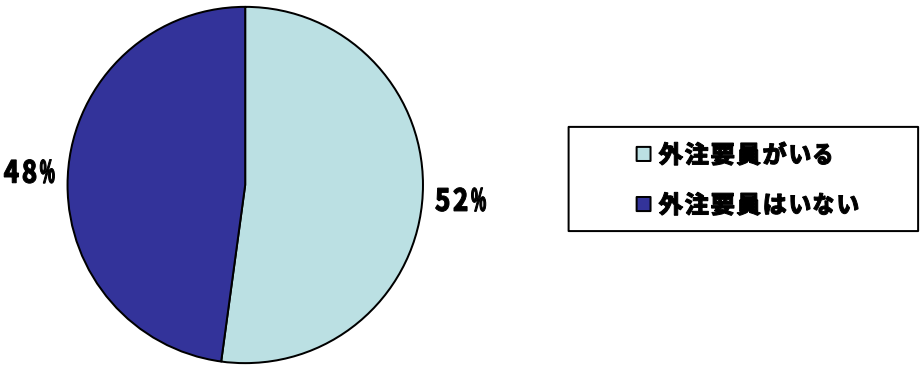
（有効回答：23府省庁）

Q03　専任職員が従事している業務の内容



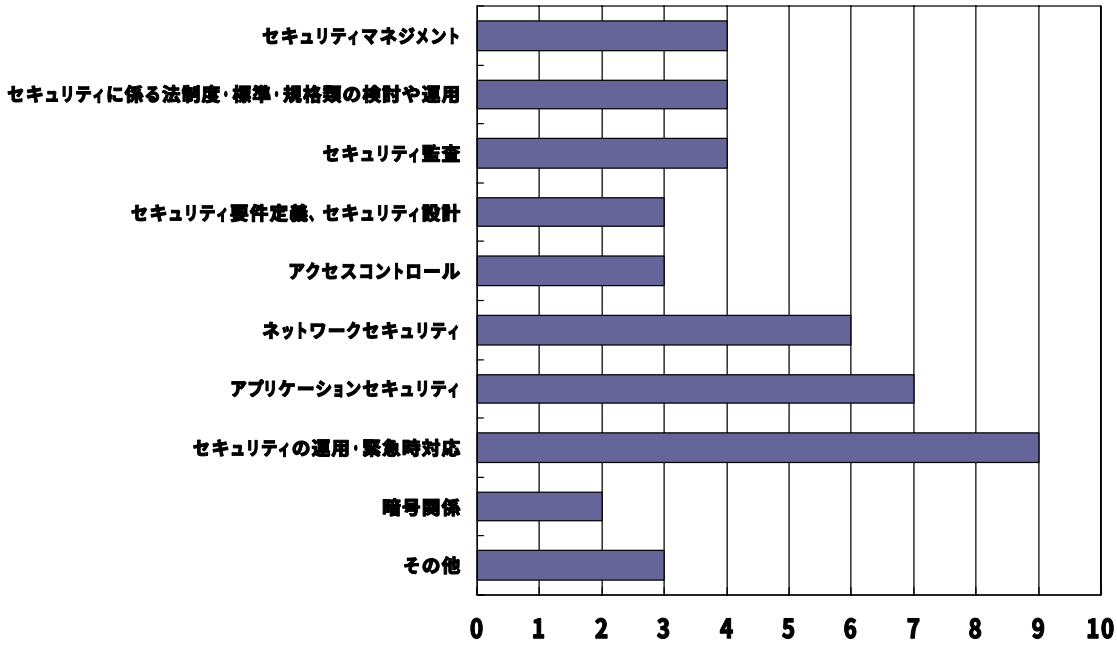
（有効回答：9府省庁、複数回答可能項目）

Q04　外注要員の配置状況



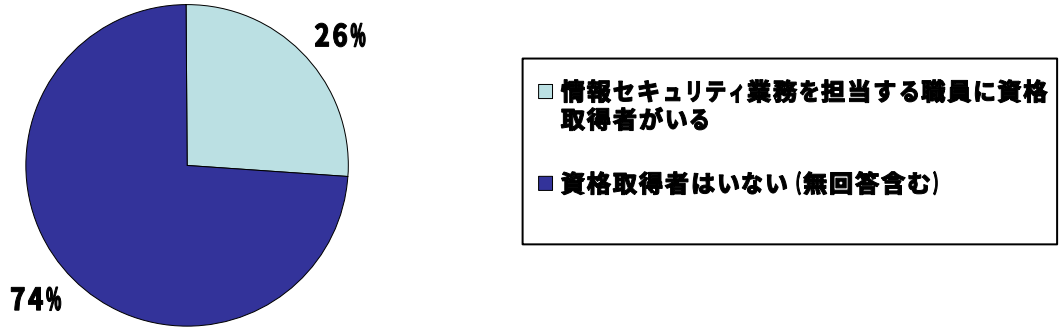
（有効回答：23府省庁）

Q05　外注要員が従事している業務の内容



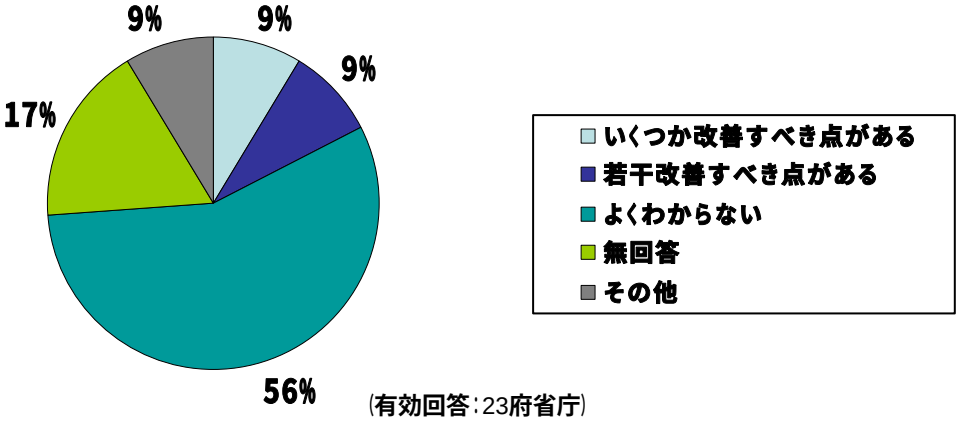
（有効回答：12府省庁、複数回答可能項目）

Q06　情報セキュリティ資格の取得者



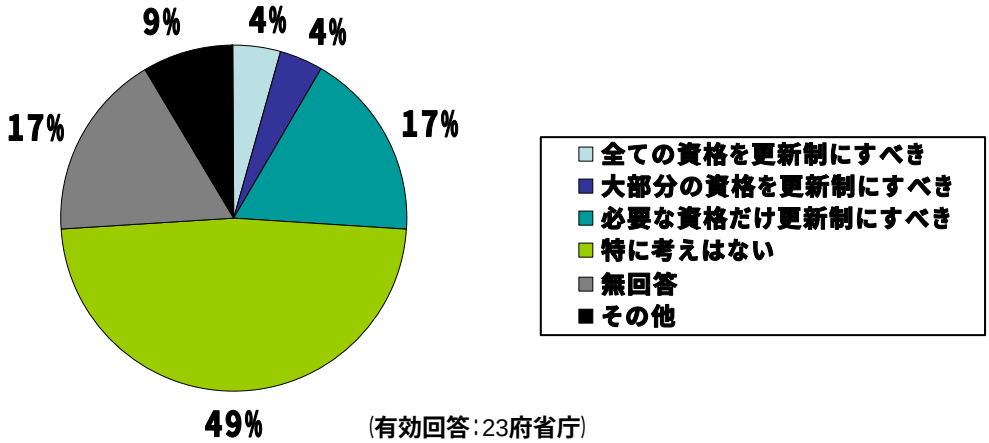
（有効回答：23府省庁）

Q07　資格制度に対する考え方



（有効回答：23府省庁）

Q09　更新制度に対する考え方



（有効回答：23府省庁）

Q08、10　資格制度に対する評価・問題点

資格制度に対する評価・問題点について自由回答を求めた所、実業務に従事する担当者の意見として一部の府省庁から以下のような回答があったため、これを列記する。

○　情報セキュリティは実践、実務面が重視されるため、より有用な位置付けを目指すために、公的資格については民間資格との間で位置付けを見直すべき。

○　資体系的かつ網羅的な情報セキュリティ対策のカリキュラムの欠如。

○　IT スキル標準（開発側、利用者側）と資格制度のマッピングの必要性。

○　保有資格と組織内のスキル評価の困難性、資格取得インセンティブの欠如。

○　日進月歩で進むセキュリティ対策に対応した資格の必要性（更新制等）。

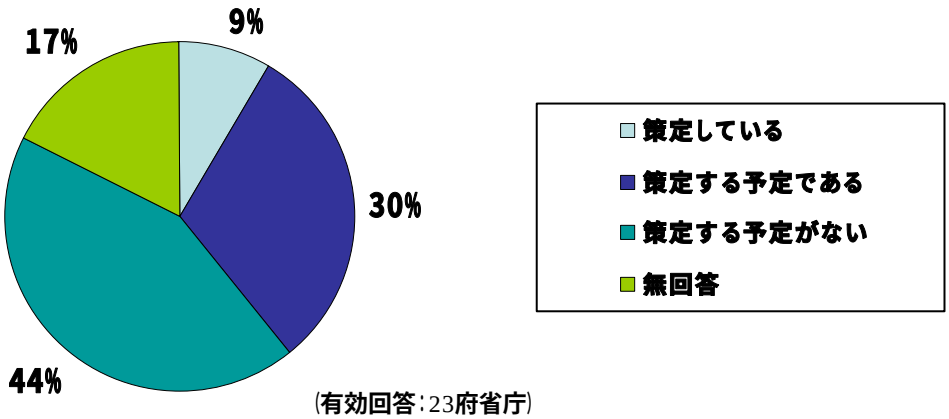
○　公的資格とベンダ資格の整合性。

○　主務官庁が複数にまたがっているためか、公的資格の付与機関が多すぎる。

○　資格制度が乱立し、どれを選択すれば良いのかわかりにくい。技術系、マネジメント系各分野別に整理が必要。

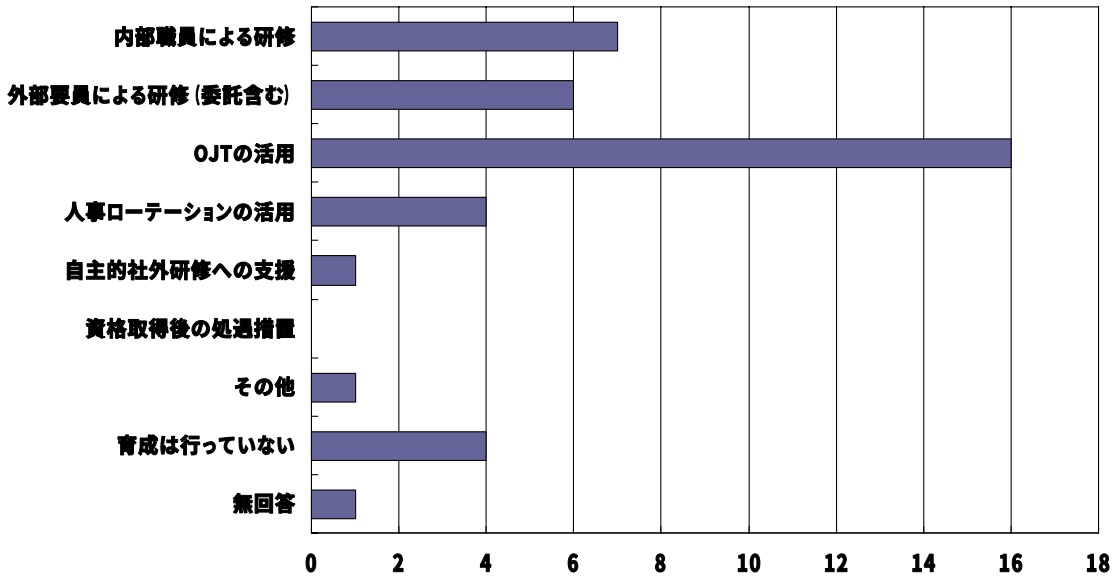
○更新制になった場合、資格取得意欲が損なわれる懸念がある。

Q11　明文化された人材計画



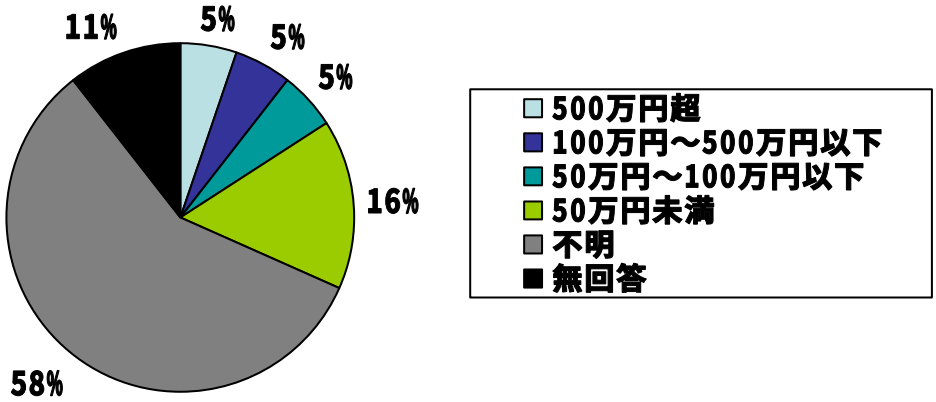
（有効回答：23府省庁）

Q12　人材育成の方策



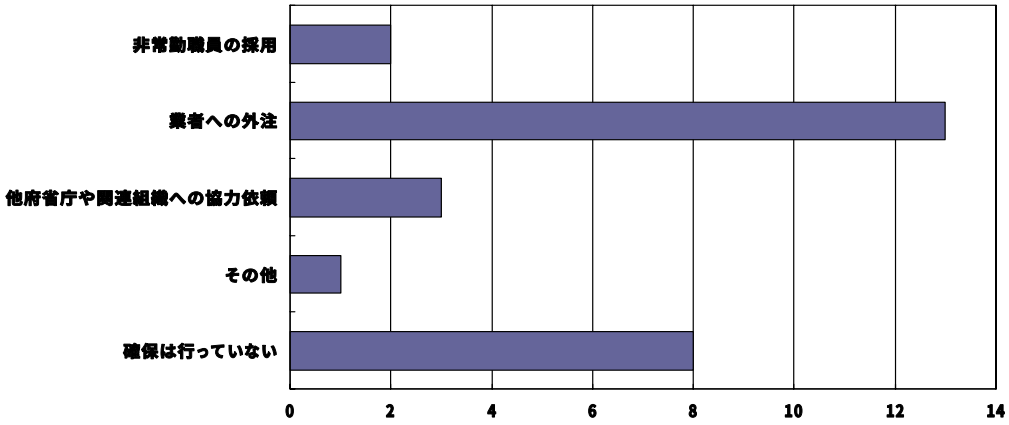
（有効回答：23府省庁、複数回答可能項目）

Q13　人材育成のための予算



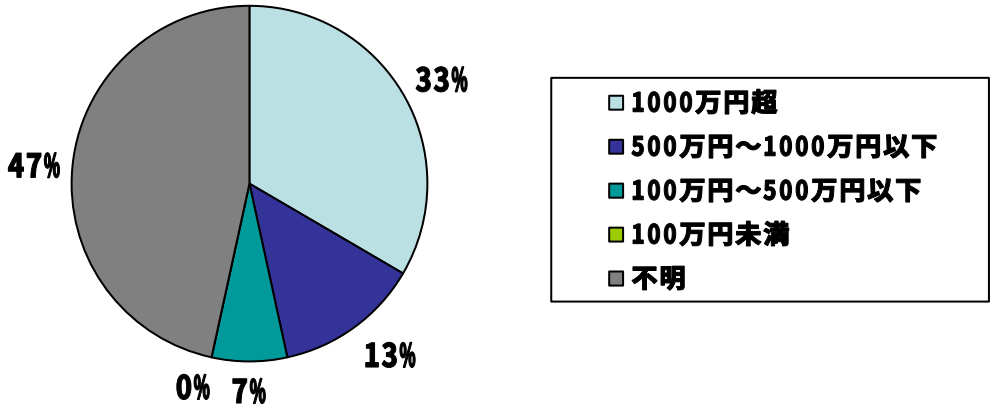
（有効回答：19府省庁）

Q14　人材確保の方策



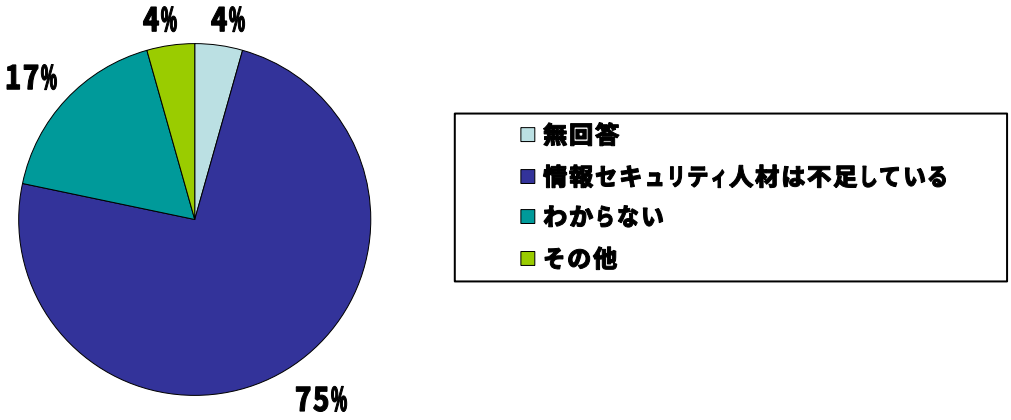
（有効回答：23府省庁、複数回答可能項目）

Q15　人材確保のための予算



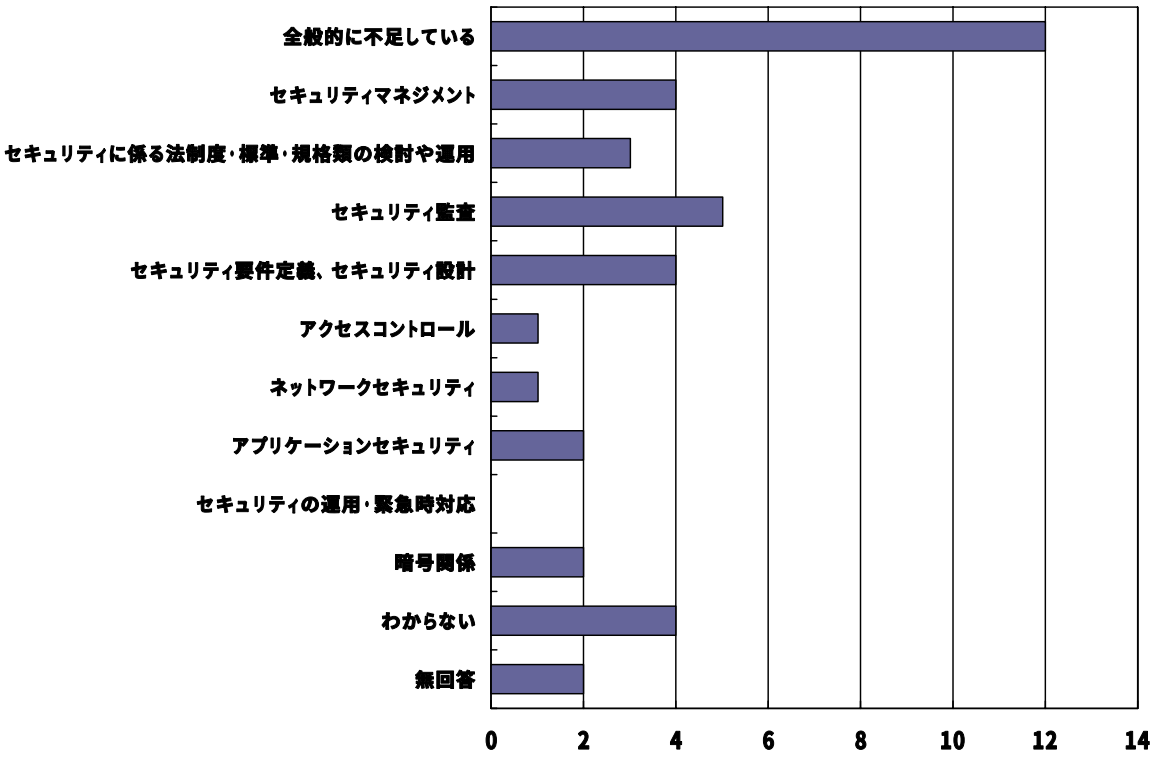
（有効回答：15府省庁）

Q16　人材の育成・確保状況



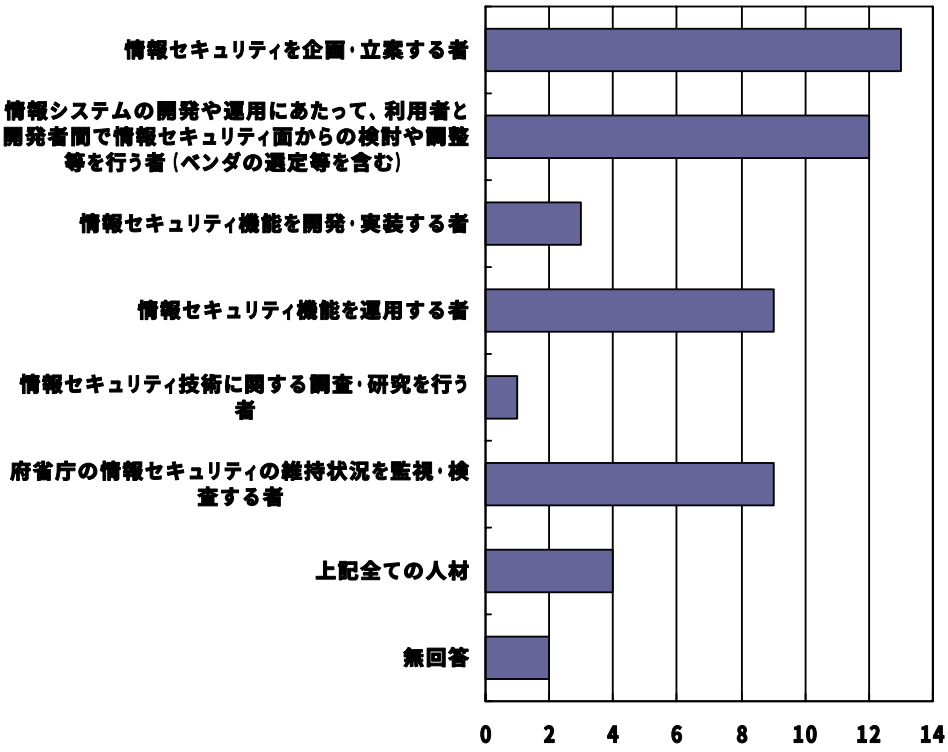
（有効回答：23府省庁）

Q17　不足している人材の分野・能力



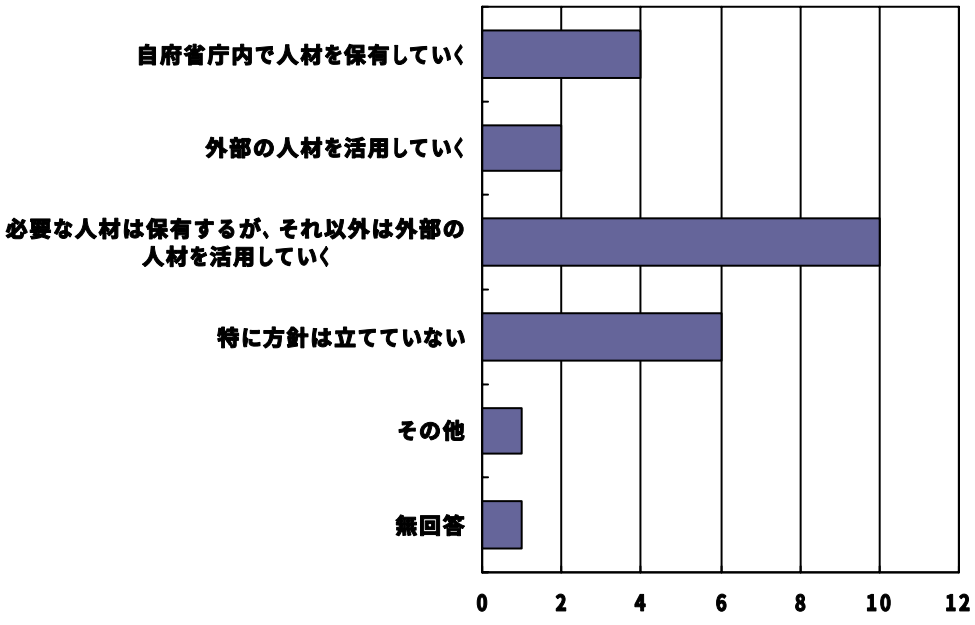
（有効回答：23府省庁、複数回答可能項目）

Q18　求められる情報セキュリティ人材のイメージ



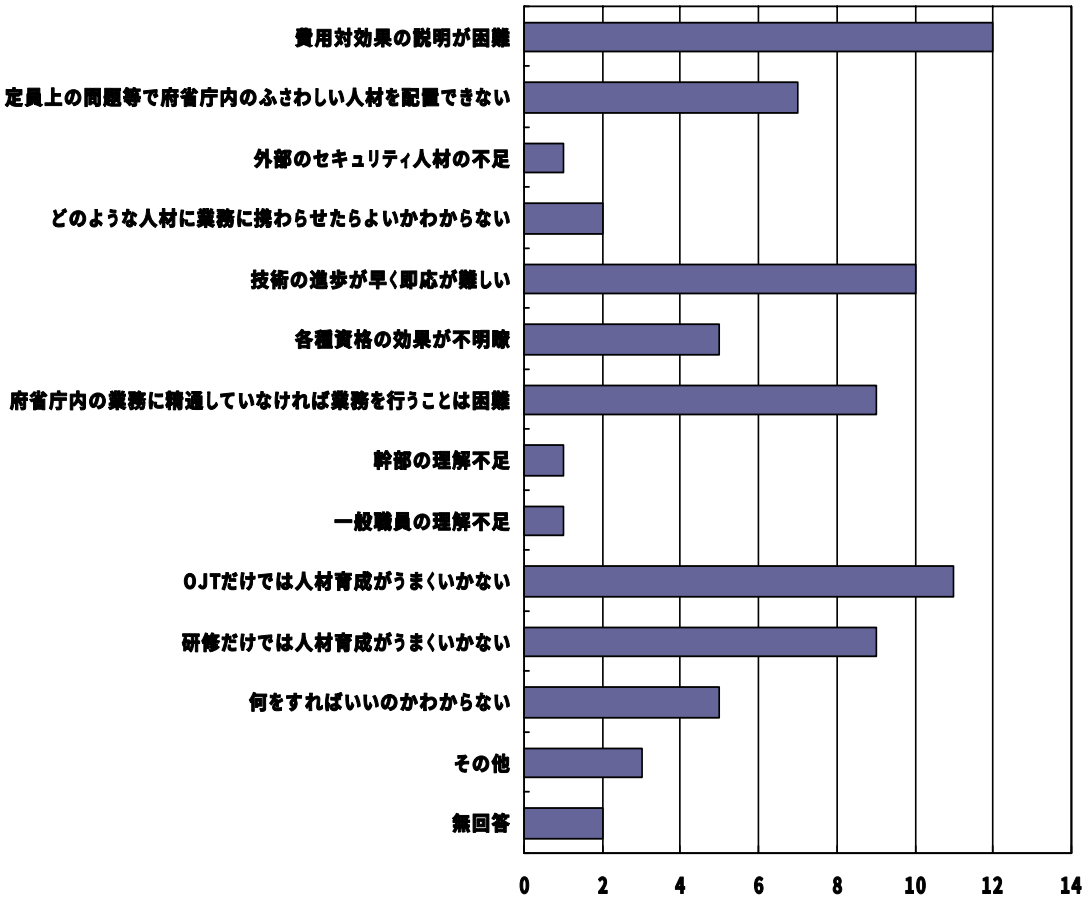
（有効回答：23府省庁、複数回答可能項目）

Q19　人材を育成・確保する上での方針



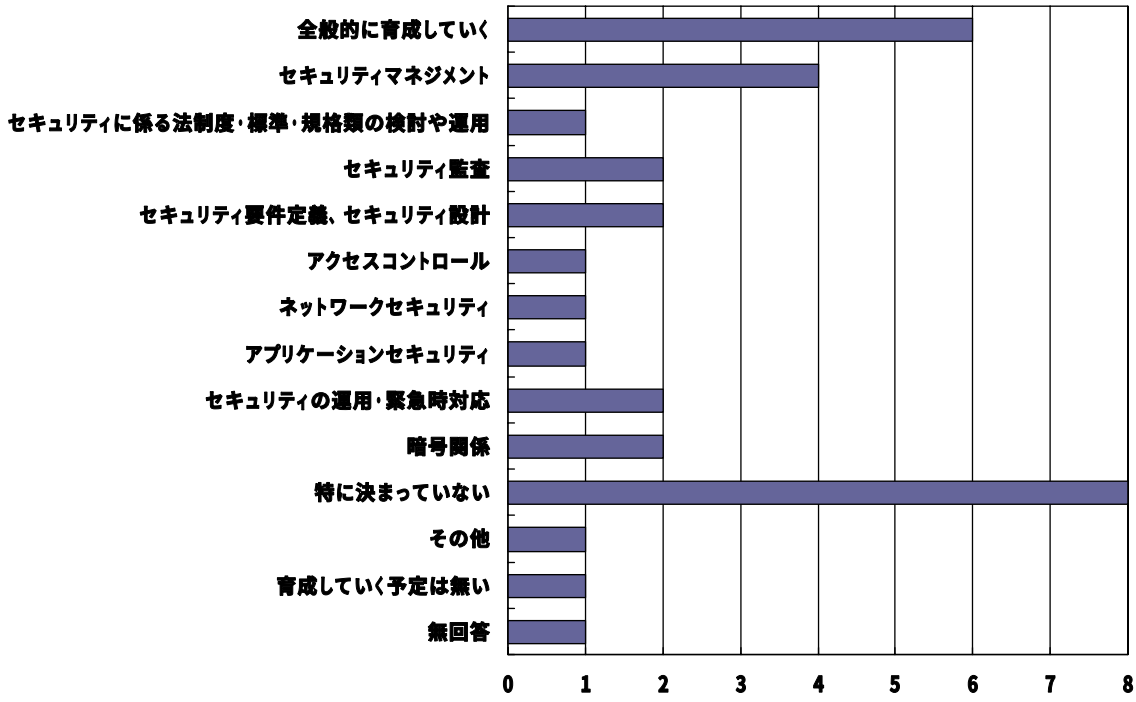
（有効回答：23府省庁、複数回答可能項目）

Q20　情報セキュリティ人材を育成・確保する上で問題となっている事項



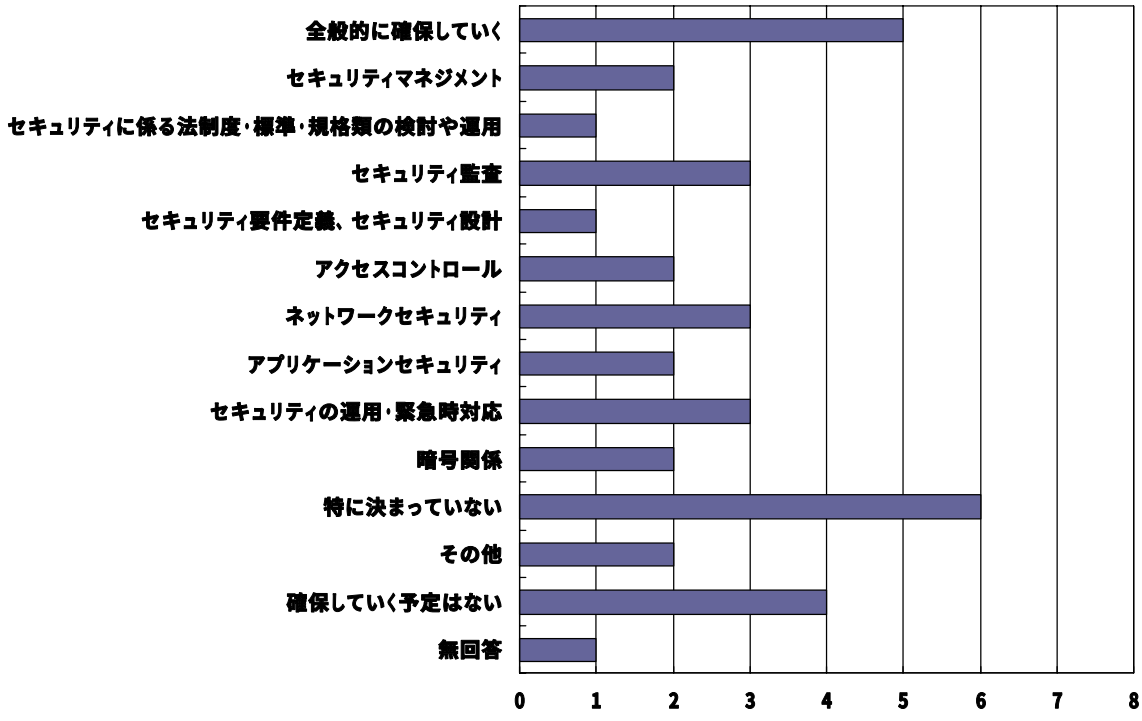
（有効回答：23府省庁、複数回答可能項目）

Q21　今後、育成していきたい人材の分野・能力



（有効回答：23府省庁、複数回答可能項目）

Q22　今後、確保していきたい人材の分野・能力



（有効回答：23府省庁、複数回答可能項目）

資料4

日本経団連加盟企業に対するアンケートの結果

＜アンケート概要＞

調査目的　　：企業における情報セキュリティ人材の現状等について調査するため
調査期間　　：２００６年7月２５日～9月１１日
対象　　：日本経団連「情報通信委員会」所属の２１７企業・団体の情報セキュリティ対策担当者
有効回答数　：７６企業・団体
回答形式　　：任意回答、不明部分は未回答又は不明として計上
結果の取扱い：個別企業名は公表の対象としない

＜アンケート用紙＞・・・・・・・・・・・・・・・・・・・・・・・・・・・・-資 35-

＜アンケート結果＞・・・・・・・・・・・・・・・・・・・・・・・・・・・・-資 49-

情報セキュリティに関する人材育成･確保に関するアンケート

以下の質問にご回答いただきたく、お願いいたします。

選択肢から選ぶものについては、（複数選択可）と記載してある設問を除き、1 つだけ回答をお選び下さい。

なお、数字を答えるものについては、はっきりした数字がわからなければ、大まかな数字で結構です。

また、本アンケートにおいては、御社として社内で保有する情報を管理するための情報システムやネットワーク、社内体制等についてご回答いただきたく、お願いいたします（御社が商品として提供するＩＴ関連機器や顧客から委託等を受けて実施するセキュリティポリシーの策定等については、対象外として下さい)。

会社名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

基礎的事項

Q01　御社の業種を以下から選んで下さい。

1．通信・情報処理・メディア
2．金融・証券・保険
3．電力・運輸・エネルギー
4．商社・流通・卸・小売
5．医療・福祉・教育・研究機関・その他のサービス業
6．製造業（加工組立型産業）
7．製造業（生活関連産業）
8．製造業（基礎素材型産業）
9．建築・土木・不動産
10．その他（　　）

Q02　御社の従業員数は何人ですか。

____ 人

Q03　御社の平成 17 年度の年間売上高はいくらですか。

____ 円

Q04　御社の年間の情報システム関連予算額はいくらですか。

____ 円

Q05　御社の PC の保有台数は何台ですか（リースを受けているもの等も含めて下さい）。

____ 台

Q06　御社のサーバの保有台数は何台ですか（リースを受けているもの等も含めて下さい）。

____ 台

Q07　御社にＩＴ関連業務（社内の情報システムの構築・運用管理等）を担当する方は何人いますか。

正社員　　____ 人（うち専任者　____ 人）
正社員以外　____ 人（うち専任者　____ 人）

Q08　御社の情報システムの管理・運用体制はどのようになっていますか。

1．全て自社で行っている
2．一部外部に委託している
3．完全に外部に委託している
4．社内システム・ネットワークはない
5．その他（　　）

Q09　電子商取引への取組み状況を教えて下さい。

1．BtoB（企業間）の電子商取引に取り組んでいる
2．BtoC（消費者向け）の電子商取引に取り組んでいる
3．BtoB と BtoC の両方の電子商取引に取り組んでいる
4．電子商取引には取り組んでいない
5．その他（　　）

現在の情報セキュリティ管理体制

Q10　社内の情報資産について、全て把握していますか。

1．全ての情報資産を把握している
2．ほとんどの情報資産を把握している
3．一部の情報資産を把握している
4．ほとんど情報資産は把握できていない

Q11　把握している情報資産について、十分なリスク分析（不正アクセス、社員・委託業者の過失による情報漏えい、物理的脅威等）はできていますか。

1．把握している全情報資産について、十分なリスク分析ができている
2．一部の情報資産については、十分なリスク分析ができている
3．ほとんどの情報資産について、十分なリスク分析はできていない

Q12　社内の情報セキュリティポリシーは策定されていますか。

1．策定している
2．今後策定する予定
3．策定していないし、今後策定する予定もない
4．その他（　　）

Q13　Q12 で１又は２と回答された方に伺います。
情報セキュリティポリシーの策定や見直しの体制はどのようになっていますか。

1．全て自社で行っている
2．外部のコンサルティングを受けつつ、自社で行っている

3．一部外部に委託している
4．完全に外部に委託している
5．その他（　　）

Q14　御社の情報セキュリティについて、社内における体制・権限等はどのようになっていますか。

1．担当者（担当部門）を設け、その役職の権限の範囲で実施することとなっている
2．担当者（担当部門）を設け、その役職の権限を越えた枠組み（社長に直訴できる、社内各部門に勧告を行える、社内横断的な委員会を運営する等）を整えている
3．担当者（担当部門）は設けず、情報セキュリティに関する委員会等を設置し、各部門が責任を持って措置することとしている
4．その他（　　）

Q15　社内における情報セキュリティ担当者**以外**の職員の情報セキュリティ意識について、教えて下さい。（1～5までのうち一つと、必要に応じて6又は7をご回答下さい）

1．トップ、役員クラスから社員に至るまで、情報セキュリティ意識は高い
2．トップ、役員クラスから管理職クラスまでは意識が高いが、それより下になると意識は低い
3．トップ、役員クラスから部長クラスまでは意識が高いが、それより下になると意識は低い
4．意識が高いのは、トップ、役員クラスまでである
5．情報セキュリティ担当者以外は、意識は低い
6．人によって意識の高さはまちまちだが、総じて意識は高い
7．人によって意識の高さはまちましだが、総じて意識は低い

Q16　情報セキュリティ担当責任者（CISO）を設置していますか。（1．と 10. を除き複数回答可）

1．専任の CISO を設置している
2．セキュリティ担当責任者（CSO）が兼務している

3．情報システム担当責任者（CIO）が兼務している
4．リスク担当責任者（CRO）が兼務している
5．プライバシー（個人情報保護）担当責任者（CPO）が兼務している
6．財務担当部門の責任者が兼務している
7．総務担当部門の責任者が兼務している
8．その他の役員クラスの者が兼務している
9．上記以外の人間が兼務している
10．設置していない

Q17　Q16 で１～９と回答された方に伺います。
　情報セキュリティ担当責任者（CISO）の方はどのようなクラスの方ですか。

1．社長
2．役員級
3．部長級（役員を除く）
4．課長級
5．その他（　　）

Q18　Q16 で２～９と回答された方に伺います。
　情報セキュリティ担当責任者（CISO）を兼務している方の全業務のうち、情報セキュリティ担当責任者としての業務は何%ぐらいですか。

＿＿ %

Q19　情報セキュリティ担当責任者（CISO）が当該業務を担当することによる追加的処遇（手当て等）はありますか。ある場合はどんな措置ですか。

1．ある（追加的処遇の内容：　　）
2．ない

Q20　CISO 補佐を設置していますか。（１．と９．を除き複数回答可）

1．専任の CISO 補佐を設置している
2．セキュリティ担当部門の者が兼務している

3．情報システム担当部門の者が兼務している
4．リスク担当部門の者が兼務している
5．プライバシー（個人情報保護）担当部門の者が兼務している
6．財務担当部門の者が兼務している
7．総務担当部門の者が兼務している
8．上記以外の人間が兼務している
9．設置していない

Q21　Q20 で１～８と回答された方に伺います。
CISO 補佐の方はどのようなクラスの方ですか。

1．役員級
2．部長級（役員を除く）
3．課長級
4．課長代理、補佐級
5．課長代理、補佐級よりも下
6．その他（　　）

Q22　Q20 で２～８と回答された方に伺います。
CISO 補佐を兼務している方の全業務のうち、CISO 補佐としての業務は何%ぐらいですか。

____ %

Q23　CISO 補佐が当該業務を担当することによる追加的処遇（手当て等）はありますか。ある場合はどんな措置ですか（手当て等)。

1．ある（追加的処遇の内容：　　）
2．ない

Q24　御社に情報セキュリティ業務を担当する方は何人いますか。

正社員　　____ 人（うち専任者　____ 人）
正社員以外　____ 人（うち専任者　____ 人）

Q25　Q24 でお答えいただいた正社員の情報セキュリティ業務担当者のうち、次の資格を持っている方は何名いますか（正確に把握していなければ、概数で結構です。また、各資格の級による区別はいただかなくて結構です）。

1．情報セキュリティアドミニストレータ　＿＿ 人（うち専任者　＿＿ 人）
2．NISM の情報セキュリティ資格　＿＿ 人（うち専任者　＿＿ 人）
3．セキュリティ監査人関連資格　＿＿ 人（うち専任者　＿＿ 人）
4．公認情報セキュリティマネージャー　＿＿ 人（うち専任者　＿＿ 人）
5．情報セキュリティ検定　＿＿ 人（うち専任者　＿＿ 人）
6．CIW の情報セキュリティ資格　＿＿ 人（うち専任者　＿＿ 人）
7．CompTIA の情報セキュリティ資格　＿＿ 人（うち専任者　＿＿ 人）
8．SANS の情報セキュリティ資格　＿＿ 人（うち専任者　＿＿ 人）
9．CISCO の情報セキュリティ資格　＿＿ 人（うち専任者　＿＿ 人）
10．Oracle の情報セキュリティ資格　＿＿ 人（うち専任者　＿＿ 人）
11．Microsoft の情報セキュリティ資格　＿＿ 人（うち専任者　＿＿ 人）
12．Sun Micro の情報セキュリティ資格　＿＿ 人（うち専任者　＿＿ 人）
13．その他の情報セキュリティ資格
（資格名：　＿＿ 人（うち専任者　＿＿ 人））
（資格名：　＿＿ 人（うち専任者　＿＿ 人））
（資格名：　＿＿ 人（うち専任者　＿＿ 人））
（資格名：　＿＿ 人（うち専任者　＿＿ 人））
（資格名：　＿＿ 人（うち専任者　＿＿ 人））

Q26　Q24 でお答えいただいた正社員以外の情報セキュリティ業務担当者のうち、次の資格を持っている方は何名いますか（正確に把握していなければ、概数で結構です。また、各資格の級による区別はいただかなくて結構です）。

1．情報セキュリティアドミニストレータ　＿＿ 人（うち専任者　＿＿ 人）
2．NISM の情報セキュリティ資格　＿＿ 人（うち専任者　＿＿ 人）
3．セキュリティ監査人関連資格　＿＿ 人（うち専任者　＿＿ 人）
4．公認情報セキュリティマネージャー　＿＿ 人（うち専任者　＿＿ 人）
5．情報セキュリティ検定　＿＿ 人（うち専任者　＿＿ 人）
6．CIW の情報セキュリティ資格　＿＿ 人（うち専任者　＿＿ 人）
7．CompTIA の情報セキュリティ資格　＿＿ 人（うち専任者　＿＿ 人）
8．SANS の情報セキュリティ資格　＿＿ 人（うち専任者　＿＿ 人）

9．CISCO の情報セキュリティ資格　　＿＿ 人（うち専任者　＿＿ 人）
10．Oracle の情報セキュリティ資格　　＿＿ 人（うち専任者　＿＿ 人）
11．Microsoft の情報セキュリティ資格　　＿＿ 人（うち専任者　＿＿ 人）
12．Sun Micro の情報セキュリティ資格　　＿＿ 人（うち専任者　＿＿ 人）
13．その他の情報セキュリティ資格
（資格名：　　＿＿ 人（うち専任者　＿＿ 人））
（資格名：　　＿＿ 人（うち専任者　＿＿ 人））
（資格名：　　＿＿ 人（うち専任者　＿＿ 人））
（資格名：　　＿＿ 人（うち専任者　＿＿ 人））
（資格名：　　＿＿ 人（うち専任者　＿＿ 人））

情報セキュリティ人材の育成・確保方策

Q27　御社内で情報セキュリティ人材(情報セキュリティ業務担当者及び今後情報セキュリティ業務を担当する予定の者）を育成・確保するための計画等（明文化されたもの）を策定していますか。

1．策定している（策定時期：　　）
→当該計画等の概要が分かるものを添付いただけると幸いです。
2．策定していないが今後策定する予定
3．策定していないし今後策定する予定もない

Q28　情報セキュリティ人材を「育成」（社内で育成）するために、現在御社で実施している方策を以下から選んで下さい。（複数回答可）

1．社内研修の実施
2．社外研修（外部委託研修も含む）の実施
3．社員の自主的な社外研修への支援（資格取得のための金銭的補助や勤怠優遇等）
4．情報セキュリティ資格取得後の処遇措置（基本給の上昇、報奨金等）
5．情報セキュリティに関する技能・能力テストの実施
6．情報セキュリティに関する社内選抜制度の運用
7．ＯＪＴを活用
8．行っていない
9．その他（　　）

Q29　情報セキュリティ人材を「確保」（社外から調達）するために、現在御社で実施している方策を以下から選んで下さい。（複数回答可）

1．情報セキュリティ専門の正社員を新卒採用
2．情報セキュリティ専門の正社員を中途採用
3．情報セキュリティ専門の派遣社員を確保
4．行っていない
5．その他（　　）

今後の方針と課題

Q30　現在社内で不足していると感じる情報セキュリティ人材の分野又は能力を以下から選んで下さい。（複数回答可）

1．とにかく全般
2．情報セキュリティマネジメント（情報資産管理、リスク分析、体制・計画構築等）
3．アクセスコントロール（アクセス権限管理、認証）
4．ネットワークセキュリティ（ファイアウォール、侵入検知等）
5．アプリケーションセキュリティ（サーバアプリケーション、OS 等）
6．暗号関係（暗号、PKI、署名）
7．法制度（法律等）
8．特になし

Q31　今後確保したい必要な情報セキュリティ人材のイメージを教えて下さい。

（　　）

Q32　情報セキュリティ人材を育成･確保するための今後の方針を以下から選んで下さい。（複数回答可）

1．社内の既存の人材を育成する

２．社外の人材を積極的に採用する
３．派遣社員を積極的に活用する
４．アウトソーシングを積極的に実施する
５．これ以上情報セキュリティ人材を積極的に育成・確保する必要はない
６．その他（　　）

Q33　情報セキュリティ人材を育成･確保するための障害になっていると思われる要因を以下から選んで下さい。（複数回答可）

１．株主・社内（財務部門等）への費用対効果の説明が困難
２．費用対効果がわからない
３．社内にふさわしい人材がいてもなかなか情報セキュリティ部門に配置できない
４．社外の情報セキュリティ人材が不足（採用したい人材や派遣して欲しい人材がいない等）
５．社内・社外を問わずどのような人材に情報セキュリティ業務に携わらせたらよいかわからない
６．技術の進歩が早すぎて即応が難しい
７．各種資格の効果が不明瞭
８．社内の業務に精通していなければ情報セキュリティ業務を行うことが困難
９．幹部の理解不足
10．一般社員の理解不足
11．ＯＪＴだけでは人材育成がうまくいかない
12．研修だけでは人材育成がうまくいかない
13．何をすればいいのかわからない
14．その他（　　）

情報セキュリティ人材の供給側に関する各種制度の評価・要望等

Q34　現在提供されている、各種の情報セキュリティ資格制度全般（Q25 参照）に対する評価を以下から選んで下さい。

１．全く問題ない
２．全般的にほとんど問題はないが、若干改善すべきところがある

３．全般的にやや問題があり、いくつか改善すべきところがある
４．全般的にかなり問題があり、改善すべき点が多い
５．全般的に大きな問題があり、抜本的な改善が必要
６．よく分からない
７．その他（　　）

Q35　Q34 で３～５と回答された方に伺います。
情報セキュリティ資格制度全般について改善すべき点を教えて下さい。

（　　）

Q36　情報セキュリティ資格の更新制に対する考え方を以下から選んで下さい。
１．全ての情報セキュリティ資格を更新制にすべき
２．大部分の情報セキュリティ資格を更新制にすべき
３．必要なものだけ更新制にすべき
４．特に考えはない
５．その他（　　）

Q37　現存の個別の情報セキュリティ資格で役に立たないと思うものや改善が必要だと思うものがあれば、具体的資格の名称と改善すべき点を教えて下さい。

（　　）

Q38　情報セキュリティ人材の教育を行う主体として最も重要だと思うものを以下から選んで下さい。

１．専門学校
２．大学
３．大学院
４．情報セキュリティ教育を行うことを業務とする企業

５．その他（　　）

Q39　専門学校における情報セキュリティ人材の教育に対する評価を以下から選んで下さい。

１．全く問題ない
２．ほとんど問題はないが、若干改善すべきところがある
３．やや問題があり、いくつか改善すべきところがある
４．かなり問題があり、改善すべき点が多い
５．大きな問題があり、抜本的な改善が必要
６．よく分からない
７．その他（　　）

Q40　Q39 で３～５と回答された方に伺います。
　専門学校における情報セキュリティ人材教育について改善すべき点を教えて下さい。

（　　）

Q41　大学における情報セキュリティ人材の教育に対する評価を以下から選んで下さい。

１．全く問題ない
２．ほとんど問題はないが、若干改善すべきところがある
３．やや問題があり、いくつか改善すべきところがある
４．かなり問題があり、改善すべき点が多い
５．大きな問題があり、抜本的な改善が必要
６．よく分からない
７．その他（　　）

Q42　Q41 で３～５と回答された方に伺います。
　大学における情報セキュリティ人材教育について改善すべき点を教えて下さい。

（　　）

Q43　大学院における情報セキュリティ人材の教育に対する評価を以下から選んで下さい。

1．全く問題ない
2．ほとんど問題はないが、若干改善すべきところがある
3．やや問題があり、いくつか改善すべきところがある
4．かなり問題があり、改善すべき点が多い
5．大きな問題があり、抜本的な改善が必要
6．よく分からない
7．その他（　　）

Q44　Q43 で３～５と回答された方に伺います。
　大学院における情報セキュリティ人材教育について改善すべき点を教えて下さい。

（　　）

Q45　情報セキュリティ人材の育成･確保について行政が果たしている役割に対する評価を以下から選んで下さい。

1．全く問題ない
2．ほとんど問題はないが、若干改善すべきところがある
3．やや問題があり、いくつか改善すべきところがある
4．かなり問題があり、改善すべき点が多い
5．大きな問題があり、抜本的な改善が必要
6．よく分からない
7．その他（　　）

Q46　Q45 で３～５と回答された方に伺います。

　情報セキュリティ人材の育成・確保に関して行政が果たしている役割について改善すべき点を教えて下さい。

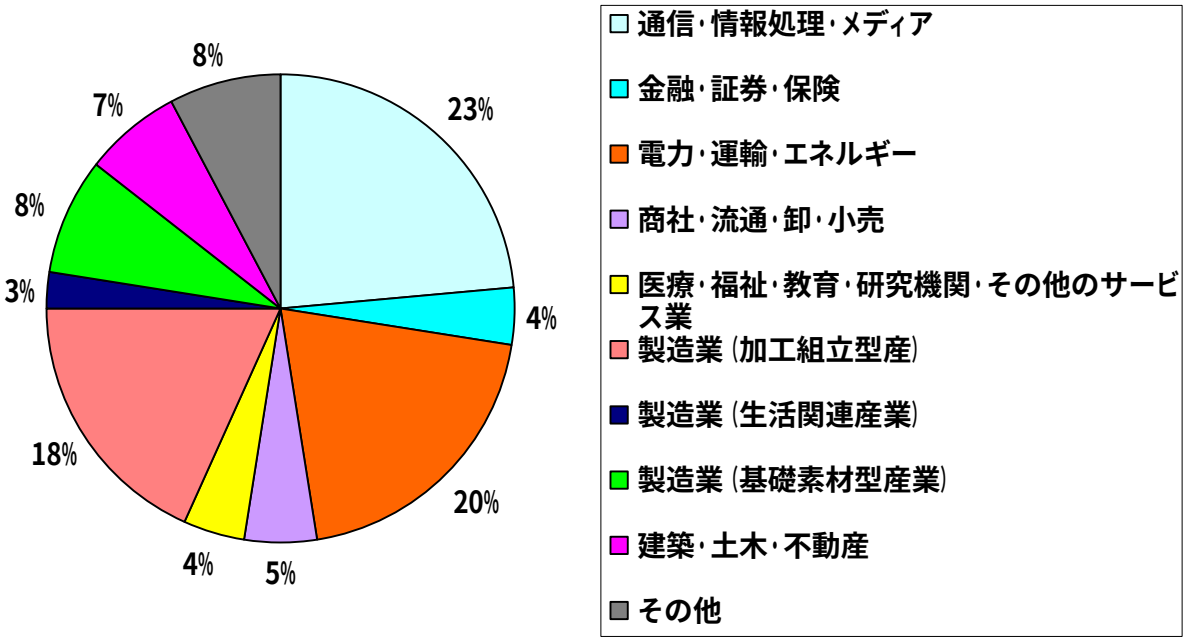
（　　）

Q47　その他、企業における情報セキュリティ対策の現場の立場から見た情報セキュリティ人材の育成・確保に対しての提言、要望、参考となる事項等ありましたら教えて下さい。

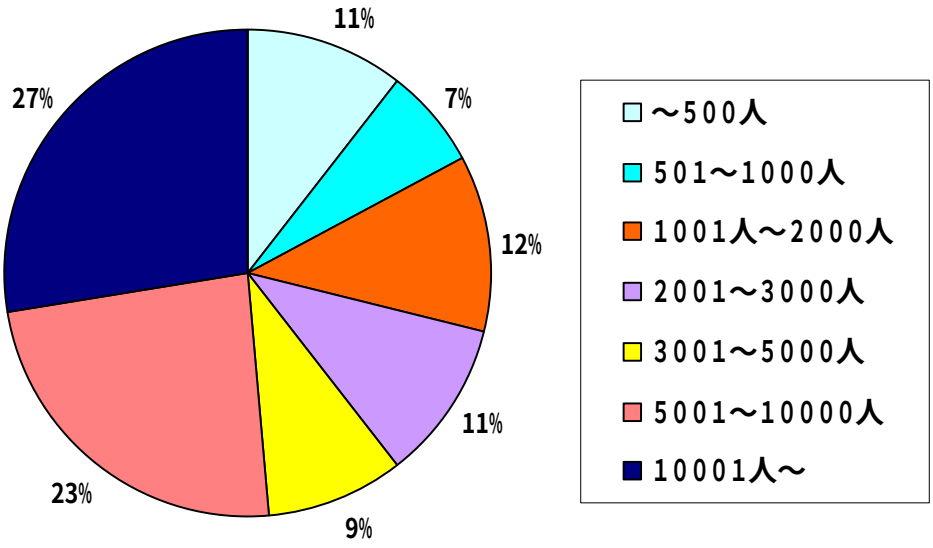
（　　）

＜アンケート結果＞

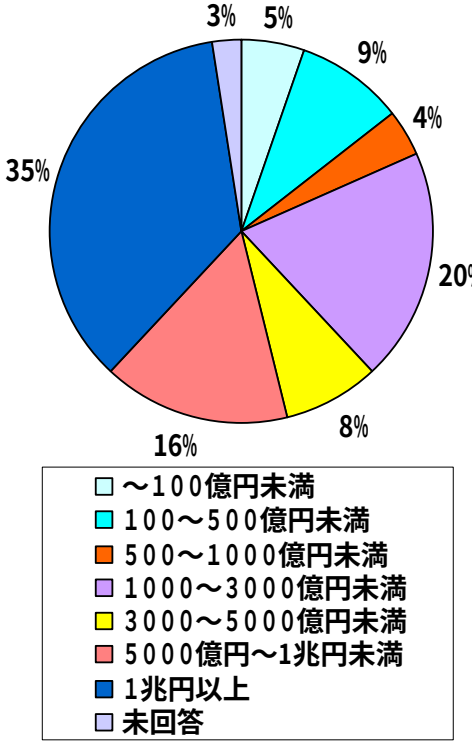
Q01　業種の分類



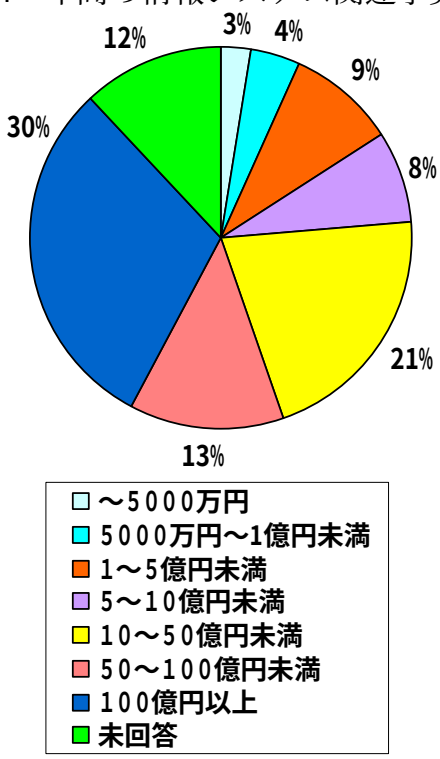
Q02　従業員数



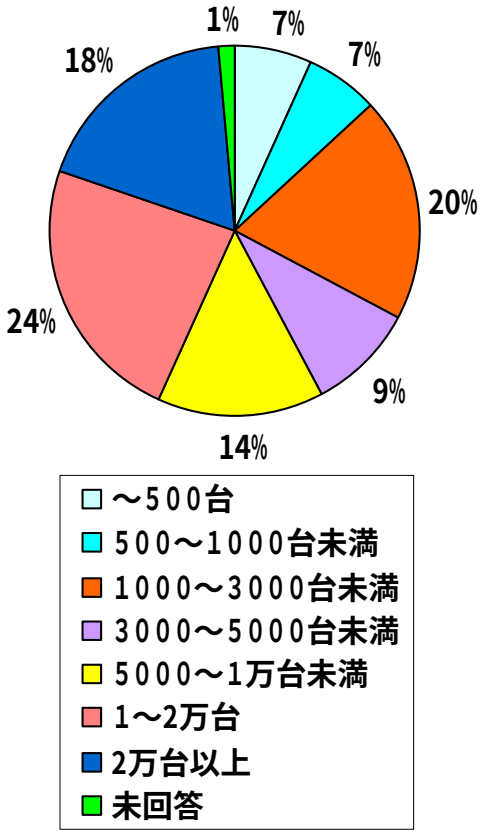
Q03　平成 17 年度の年間売上高



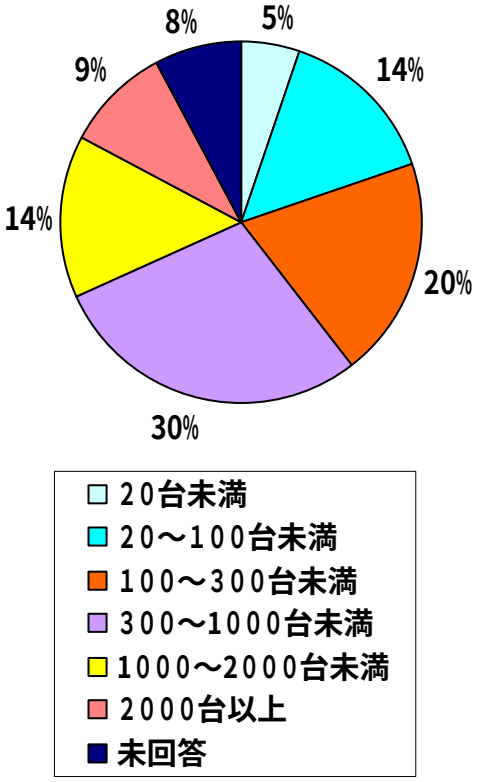
Q04　年間の情報システム関連予算額



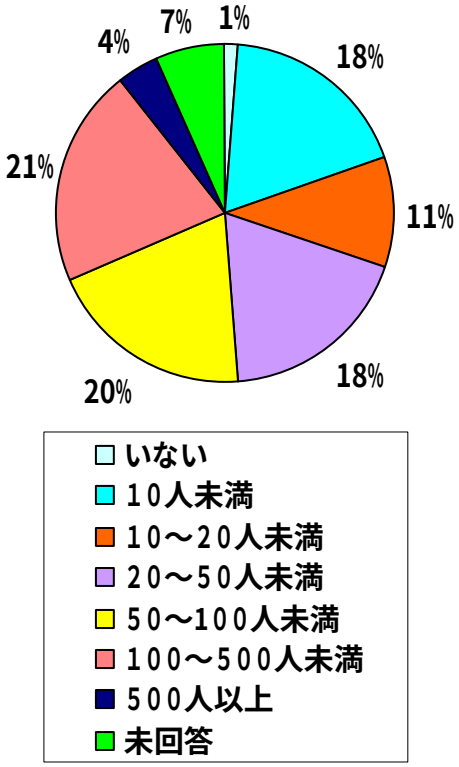
Q05　PC の保有台数



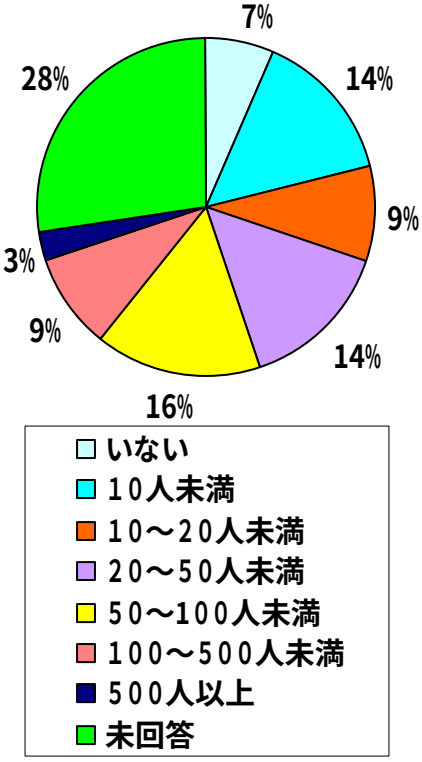
Q06　サーバの保有台数



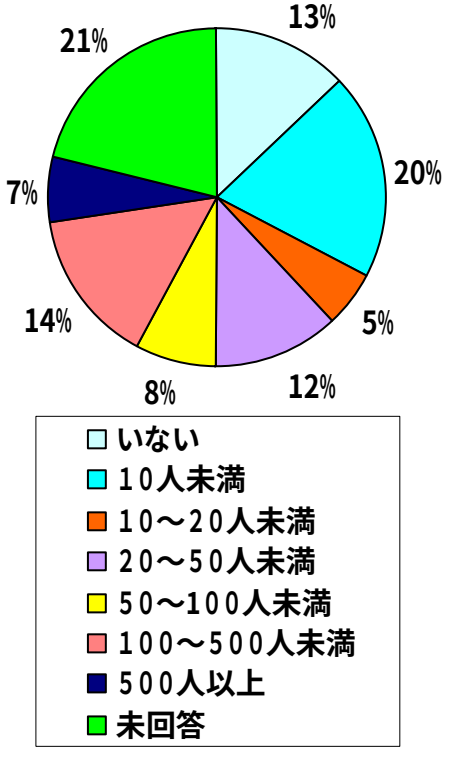
Q07(1)　IT 業務担当正社員数



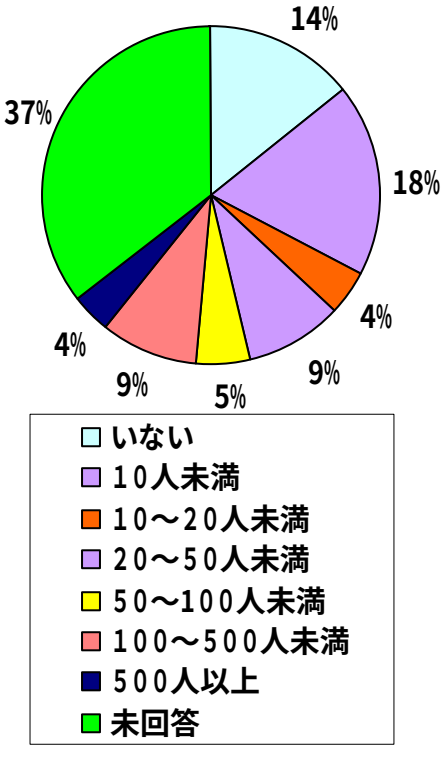
Q07(2)　IT 業務専任正社員数



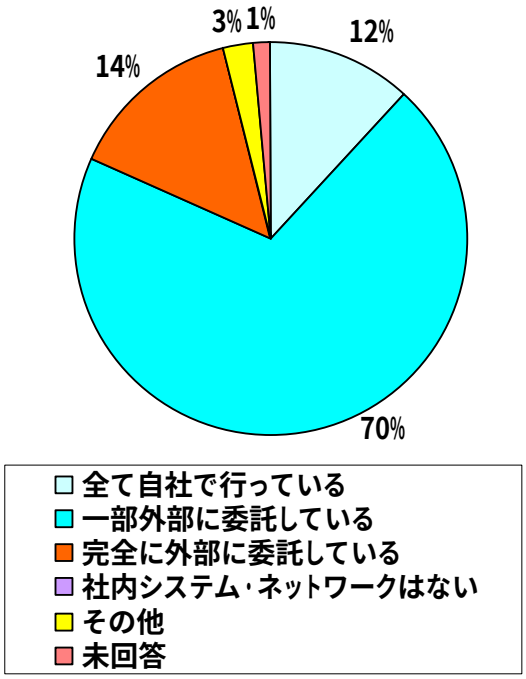
Q07(3)　IT 業務担当非正社員数



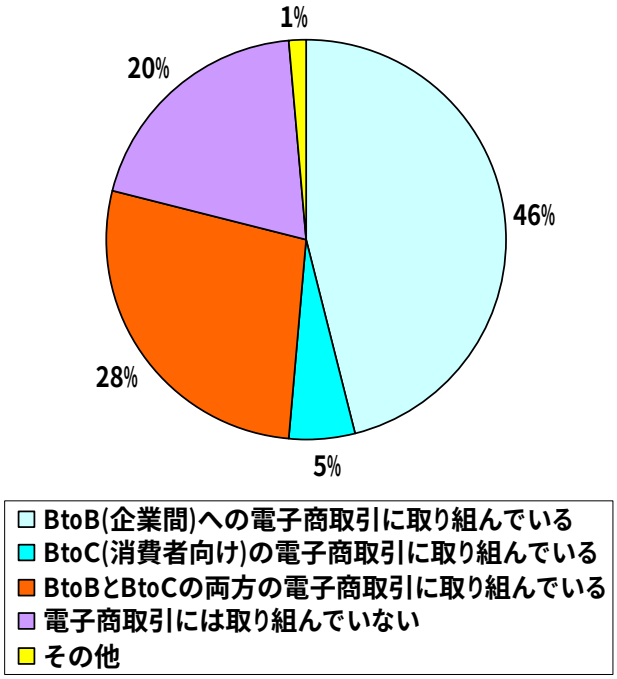
Q07(4)　IT 業務専任非正社員数



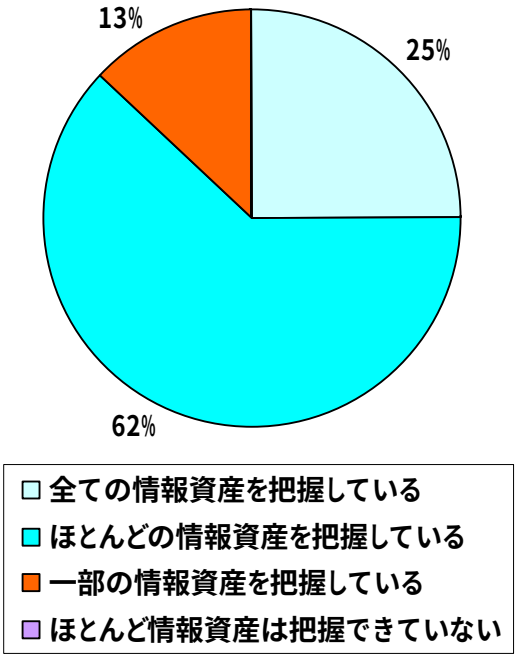
Q08　情報システムの管理・運用体制



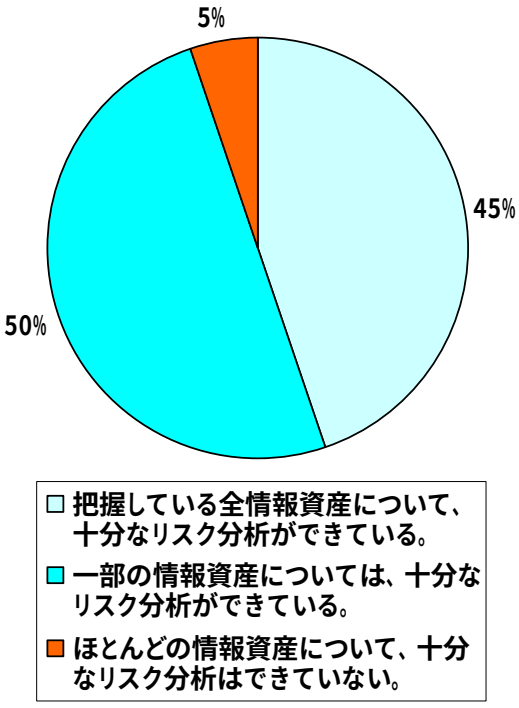
Q09　電子商取引への取組み状況



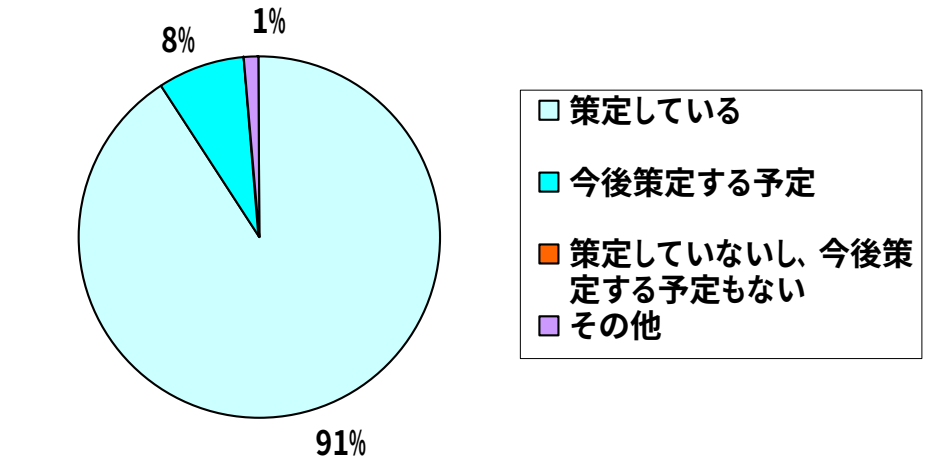
Q10　社内の情報資産の把握状況



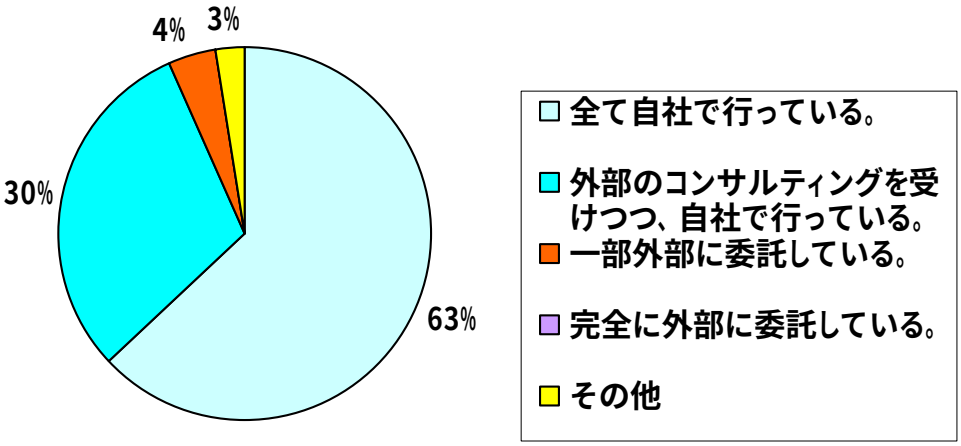
Q11 情報資産のリスク分析状況



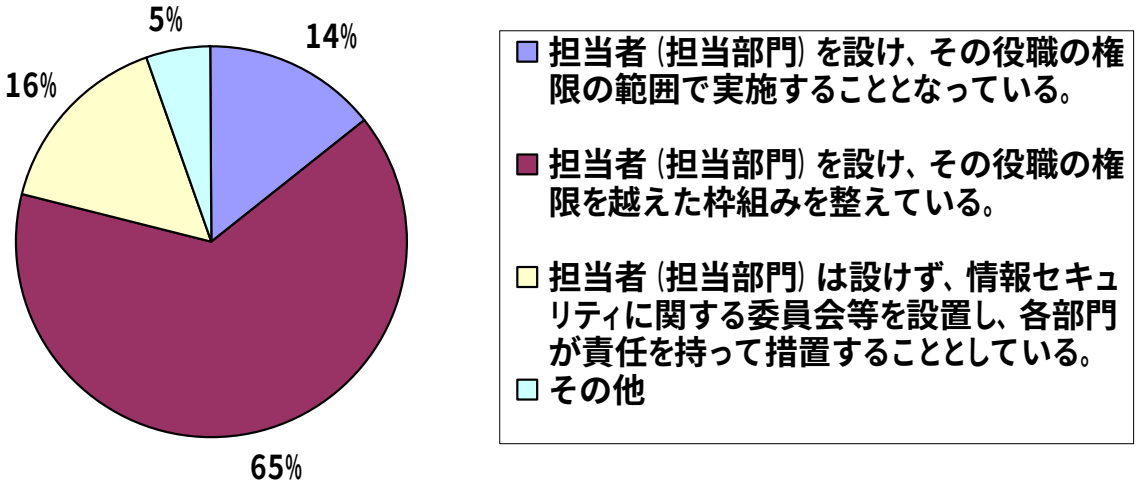
Q12　情報セキュリティポリシーの策定



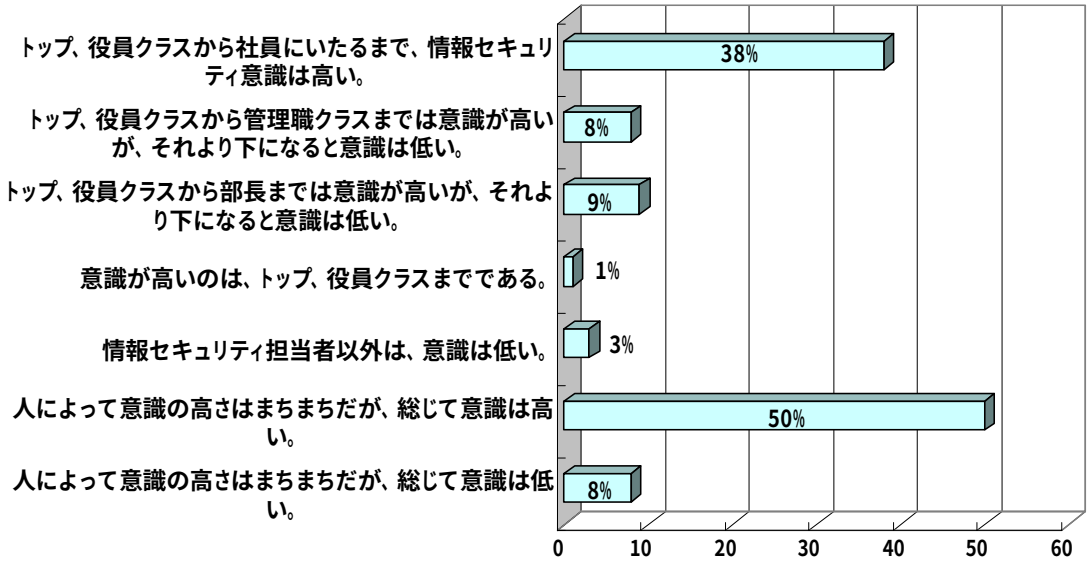
Q13　情報セキュリティポリシーの策定・見直し体制



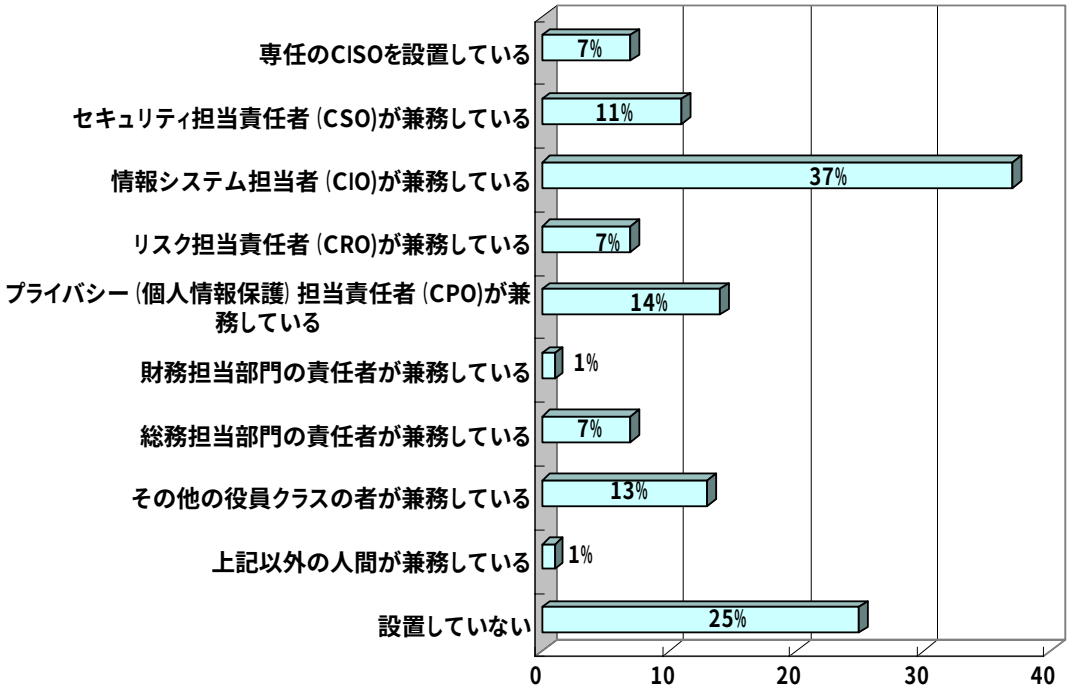
Q14　情報セキュリティに関する社内の体制・権限等



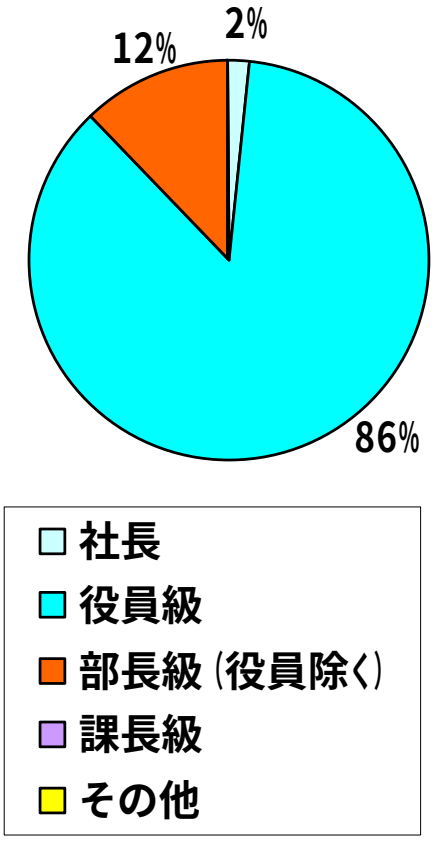
Q15　情報セキュリティ担当者以外の社員の情報セキュリティ意識



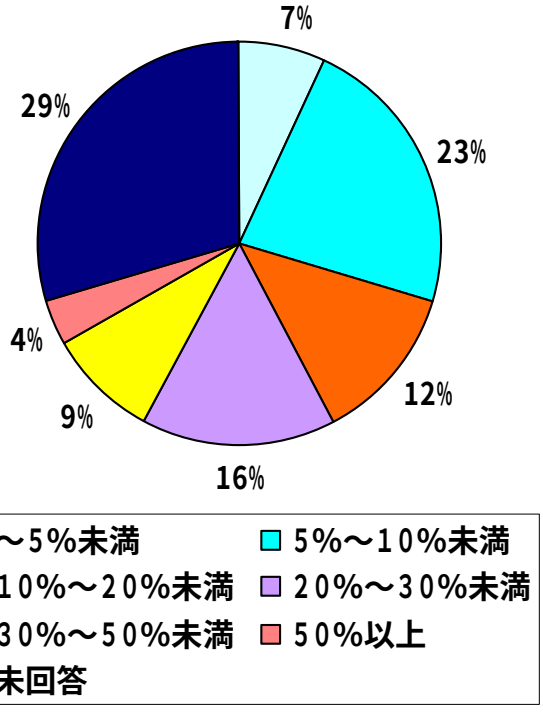
Q16　情報セキュリティ担当責任者(CISO)の設置状況



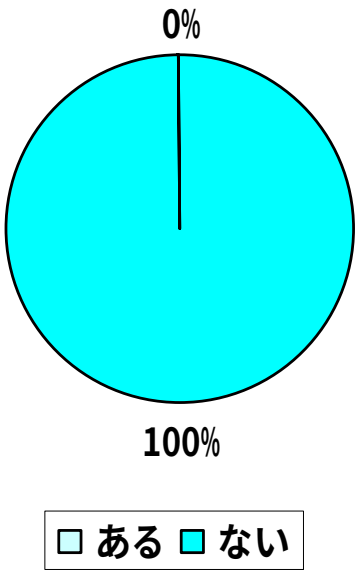
Q17　CISO のクラス



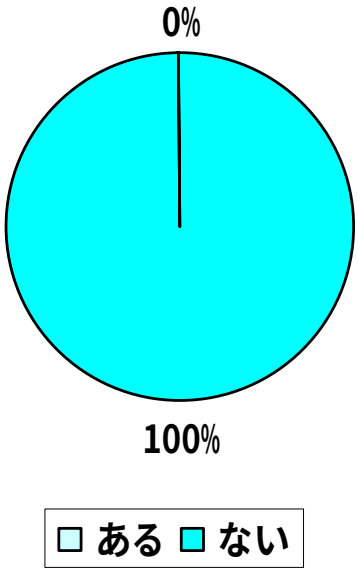
Q18　CISO としての業務の割合



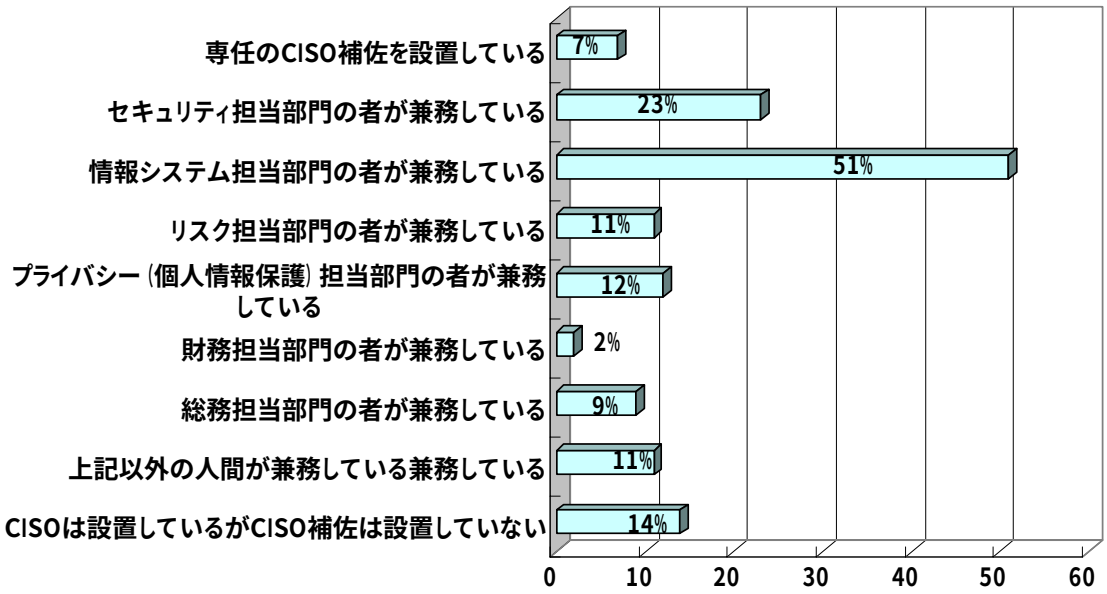
Q19　CISO への追加的処遇の有無



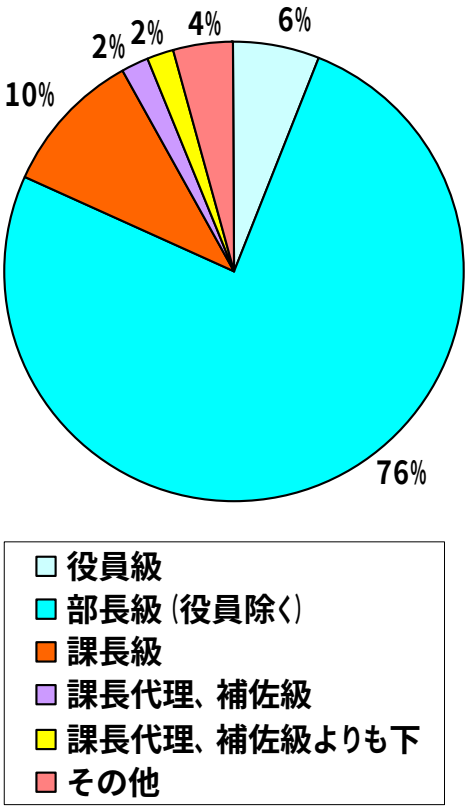
Q23　CISO 補佐への追加的処遇の有無



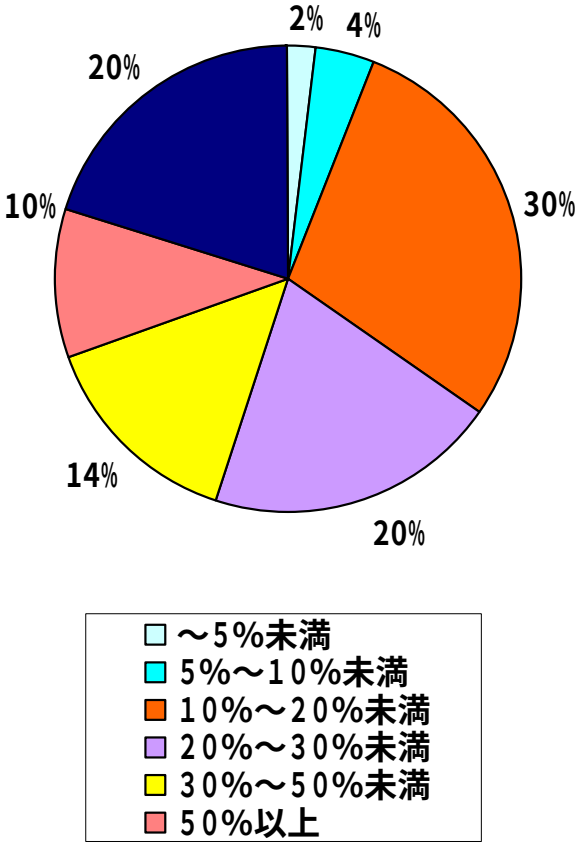
Q20　CISO 補佐の設置状況



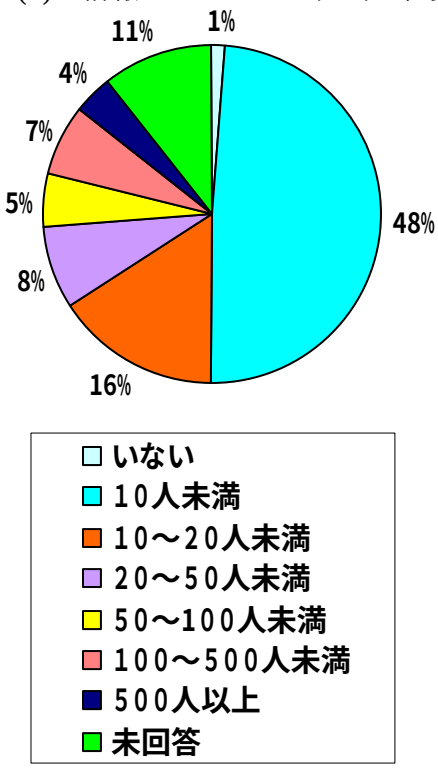
Q21　CISO 補佐のクラス



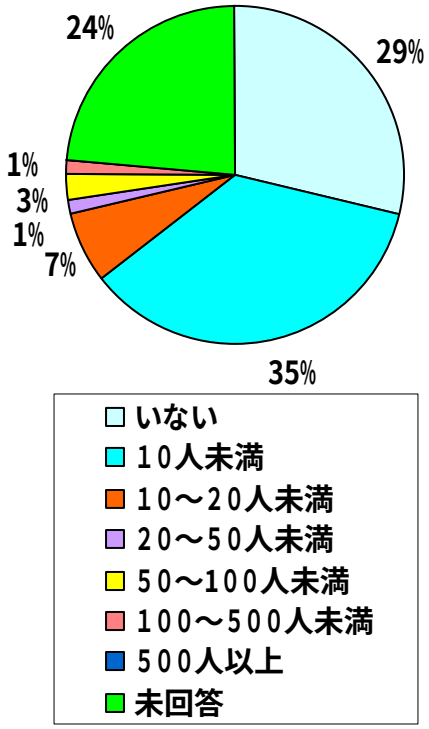
Q22　CISO 補佐としての業務の割合



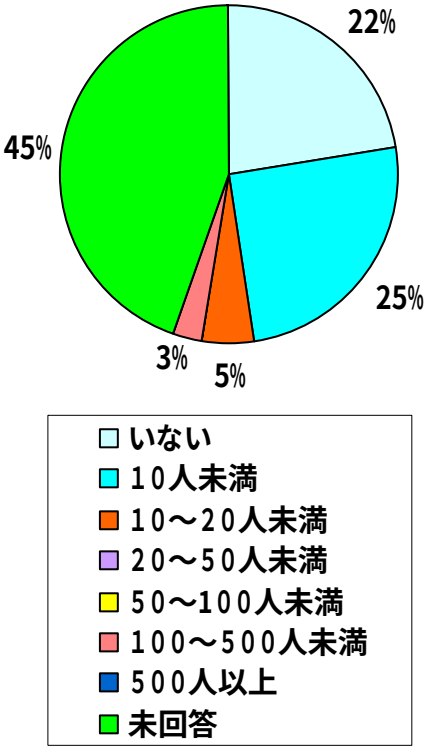
Q24(1)　情報セキュリティ担当正社員数



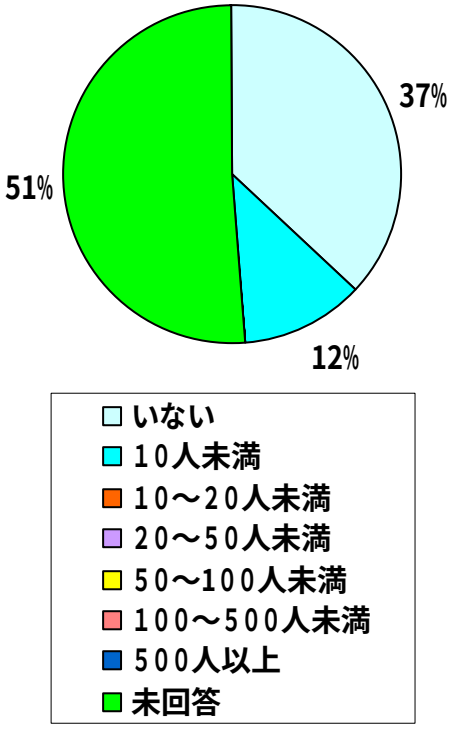
Q24(1)　情報セキュリティ担当非正社員数



Q24(3)　情報セキュリティ専任正社員数

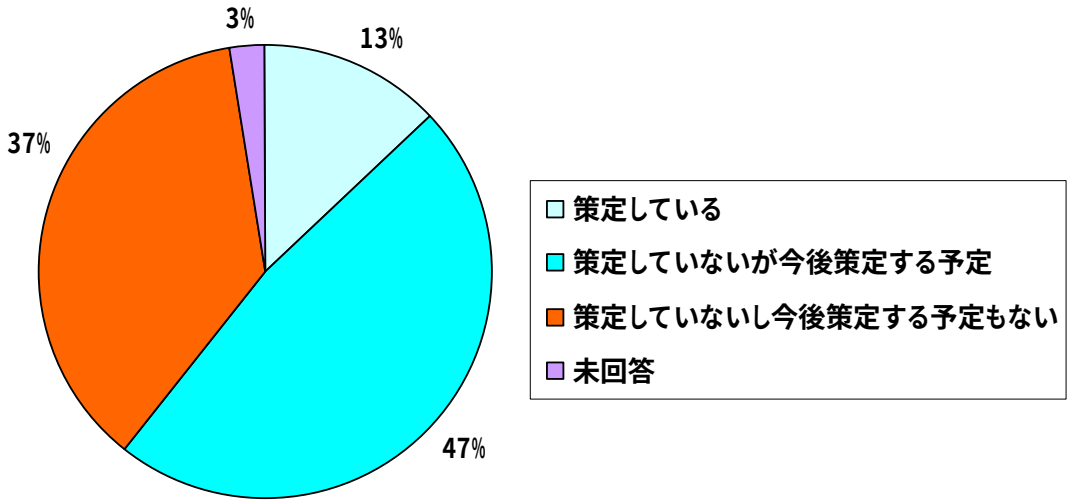


Q24(4)　情報セキュリティ専任非正社員数

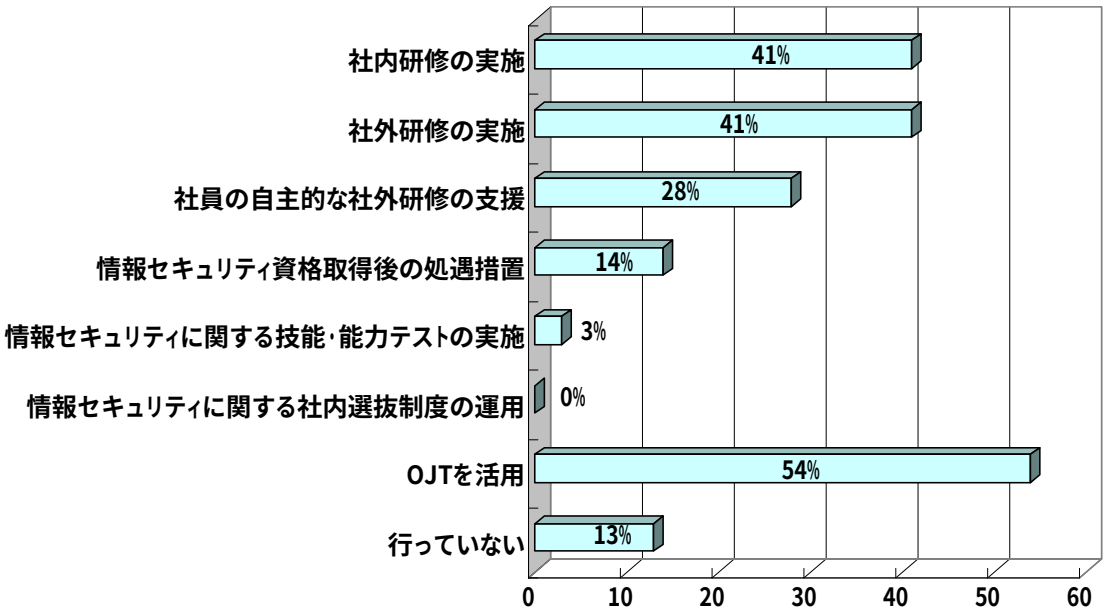


※Q25 及びQ26 についてはほとんど有効な回答が得られなかったため割愛

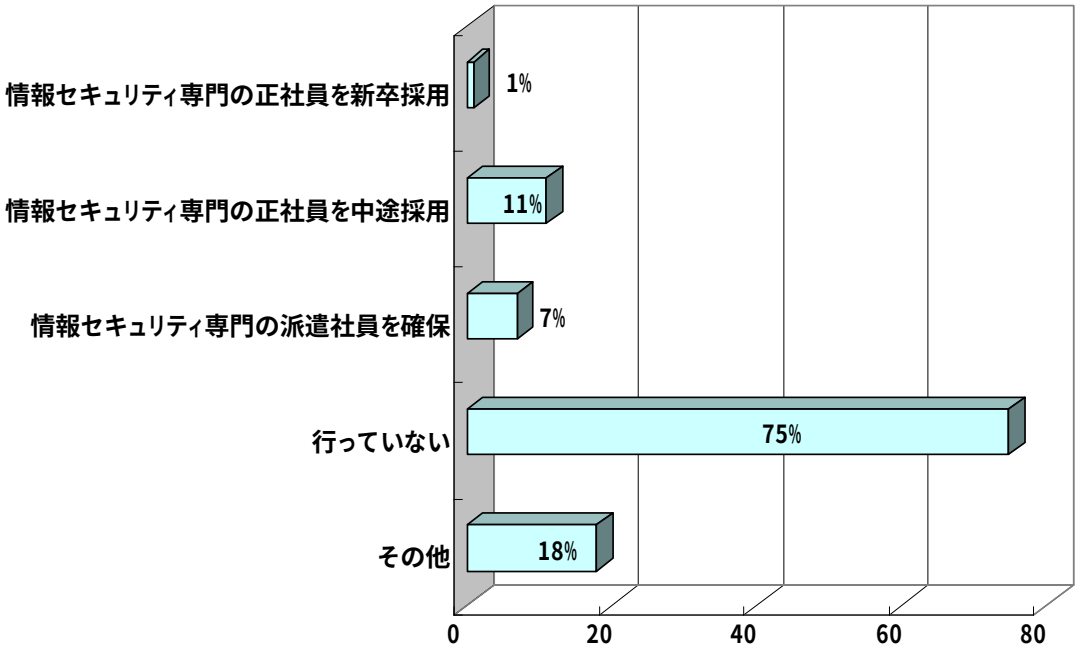
Q27　情報セキュリティ人材を育成・確保するための計画等の策定状況



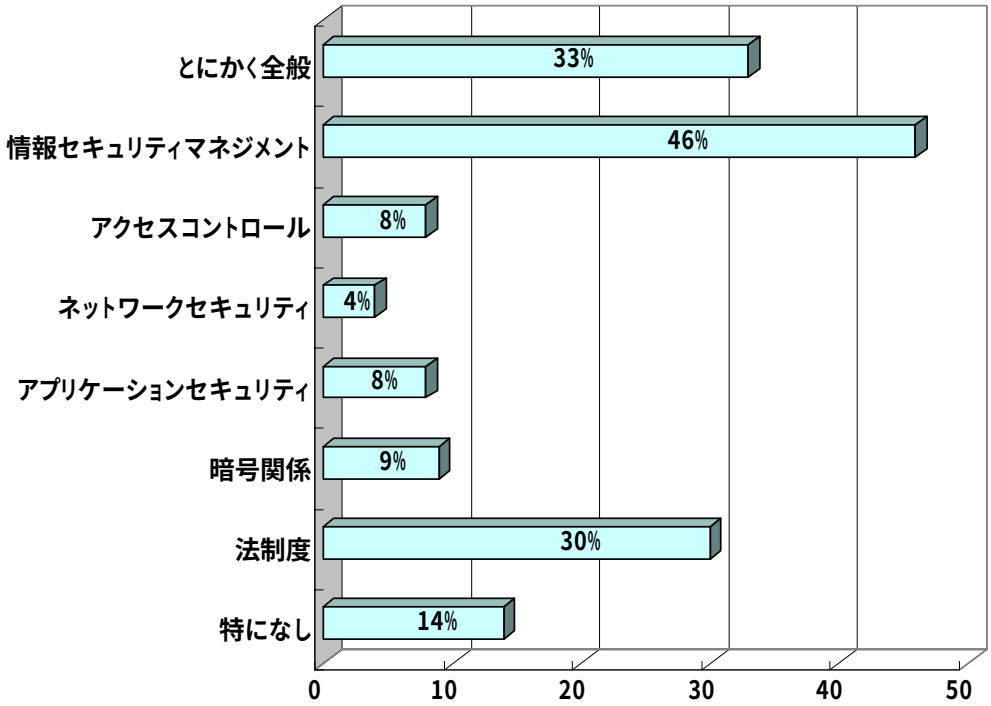
Q28　情報セキュリティ人材の「育成」のために実施している方策



Q29　情報セキュリティ人材の「確保」のために実施している方策



Q30　社内で不足していると感じる情報セキュリティ人材の分野又は能力



Q31　今後確保したい情報セキュリティ人材のイメージ

マネジメント能力を有する人材を求める回答

○　情報セキュリティマネジメントについての専門家
　①設計、構築、運用等の技術に関わる専門家
　②教育、推進等の管理に関わる専門家

○　セキュリティ技術の知識を有し、情報セキュリティマネジメントの企画・実行・推進ができる人材

○　人材はマネジメントに専門化した人材と、セキュリティに関する各種の技術に特化した人材の、スキルの２極化が進むと思われる。

○　技術・法制度全般にわたって情報セキュリティ全体を掌握できた上で業務プロセス改革のＰＤＣＡサイクルを回すことができる人材

○　情報セキュリティ施策の立案、社内への展開・監査業務を行うことができる人材

○　情報セキュリティマネジメントにおいて、グローバルに統一のとれた活動を推進できる人材

○　情報セキュリティ管理のＰＤＣＡサイクル運用を推進していく人材

○　セキュリティに対する制度的知識を基本要件として具備し、その上で、現場の状況、運用実態を理解して、実効のある施策を展開していける人材

○　情報セキュリティマネジメント分野と技術的セキュリティ分野（アクセスコントロール、ネットワークセキュリティ、アプリケーションセキュリティ等）の両方に精通した人材

○　的確なリスクマネジメントを行い、それによって得られる優先順位に従って、限られた社内資産をリスク回避への投資と分配する眼を持つ人材

○　情報セキュリティマネジメントのできる人材

○　ＩＴ、内部統制を理解できる人材

社内業務への適応力を有する人材を求める回答

○　当社業務の特性にマッチした対応策を企画・実行できる人材

○　情報セキュリティ専門知識より、社内業務への適切な適用を判断できる人材を社内に育成したい

○　事業特性を考慮したリスク分析ができる人材

○　事業規模・目的に合ったセキュリティ対策の立案・実施ができる人材

○　適用対象業務並びにそこへの適用に際しての問題点を理解することができ、バランス感を持った解決策の提示・推進を行うことができる人材

○　自社にとって適切なＩＴ技術の評価・選択ができる人材

○　リスク分析ができ、コストを意識しつつ有効な施策を考え、社内に効果的効率的に施策を展開できる人材

○　組織における調整能力の高い人材

○　情報セキュリティ関連の新技術を理解でき、関連法令、社内ルールに詳しく、これらを分かりやすく説明するための資料作成能力及び説明・相談のためのコミュニケーション能力を持った人材

法制度に関する知識を有する人材を求める回答

○　最新の法令・社会の動向・技術動向を見据えて、セキュリティポリシーの実施手順の見直しを行うことができる人材

○　今後、情報セキュリティ関連の法制度が整備されてくることに対応し、法律や条令への対応ができる知識を持った人材。

○　広範囲で正確な知識（法務）を持ち、システム開発やNW設定の経験を持つ人材

○　情報システムと法務の両方の知識・経験がある人材

○　法制度、様々な基準類を理解しかつ社内の情報システムを理解できる人材。または、これらの知識が万全でなくとも、危機管理意識が高く、複眼思考で質問力が高くかつ全体を俯瞰する力のある人材

○　情報セキュリティ関連の新技術を理解でき、関連法令、社内ルールに詳しく、これらを分かりやすく説明するための資料作成能力及び説明・相談のためのコミュニケーション能力を持った人材（再掲）

情報セキュリティ技術を有する人材を求める回答

○　情報セキュリティに関する専門技術的なスキルを有し、実際の作業を遂行することができる人材

○　情報セキュリティ技術全般をバランス良く取得した人材

○　テクニカルな分野に精通している人材

○　ＩＳＭＳ、ＩＴＩＬに準拠したノウハウで構築された環境をサービスとして利用することを前提として評価・設計ができる人材

○　データ削除の痕跡の調査を行うことができる能力を保有する人材

○　人材はマネジメントに専門化した人材と、セキュリティに関する各種の技術に特化した人材の、スキルの２極化が進むと思われる。（再掲）

＜グローバルな対応力を有する人材を求める回答＞

○　英語ができる人材

○　グローバル対応できる人材

○　海外拠点の情報セキュリティ対策を任せられる人材

その他の回答

○　事業戦略と技術戦略両面からセキュリティを検討することができる人材

○　情報セキュリティのみに特化はしないものの、情報システム全般を理解し、かつ、経営や業務についても精通している人材

○　役員クラスの人材

○　セキュリティに関する問題点把握と対処方法提言の能力を有する人材

○　業務そのものは外注するので、委託先と調整できるレベルの総合的知識を有する人材

○　技術的な専門性は必要に応じ外部専門家を活用することを前提として、社内には、それらを評価し、全社展開を企画できる人材

○　企業内の情報セキュリティニーズ・優先度と外部の脅威を把握し、バランス良い施策をタイムリーに実施できる人材。

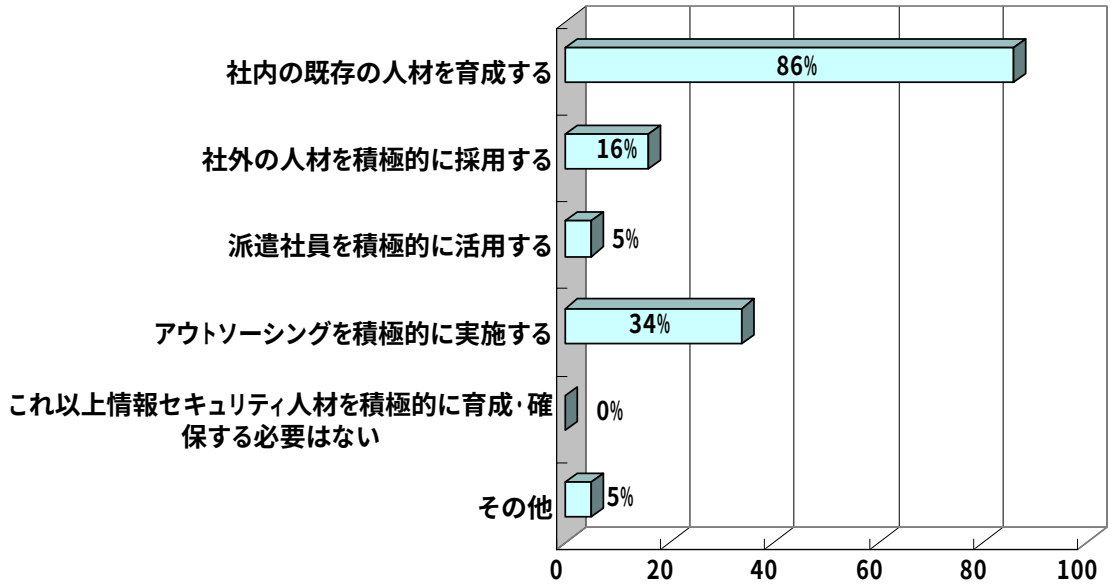
○　ビジネスニーズを理解できる人材

○　少人数による迅速な対応ができる人材

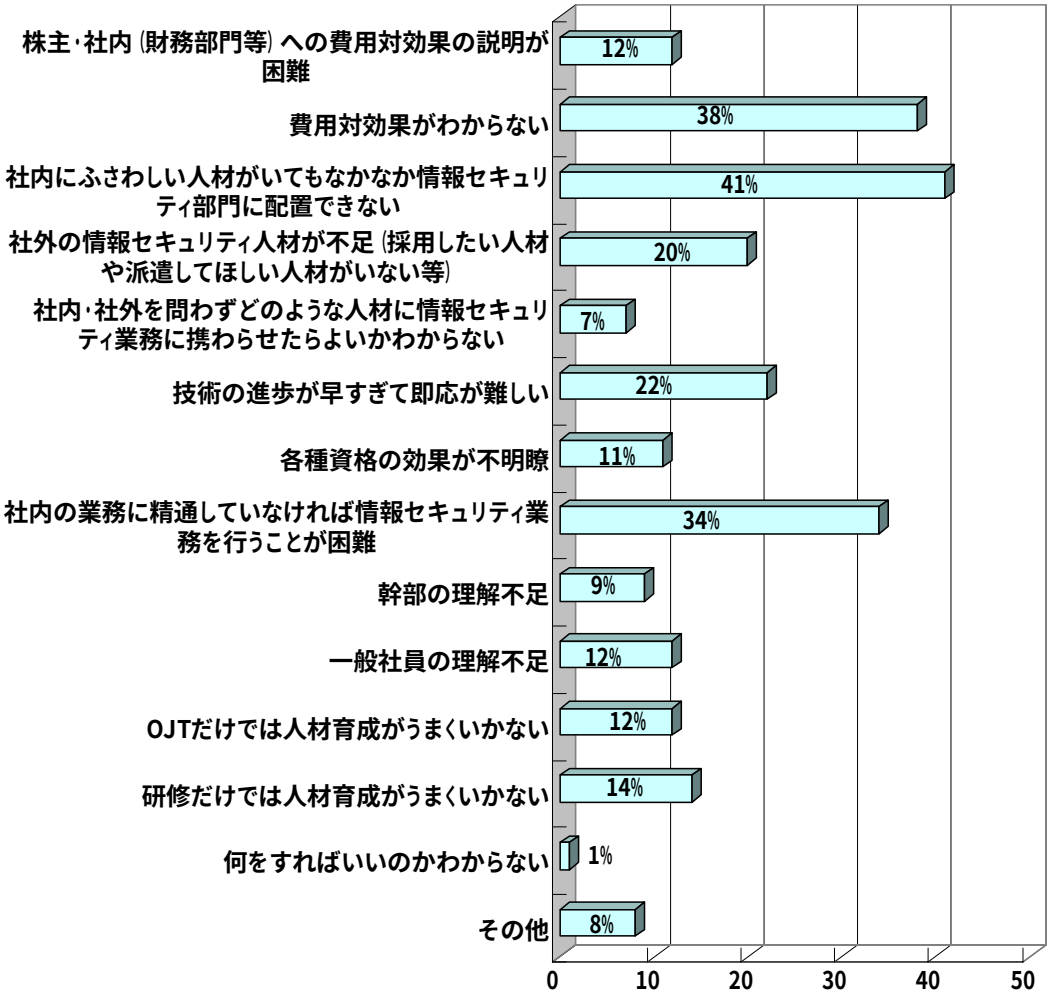
○　役所、役割に応じた情報セキュリティの知識・能力を社員各人が備えていること。

○　情報資産管理におけるリスク分析ができる人材

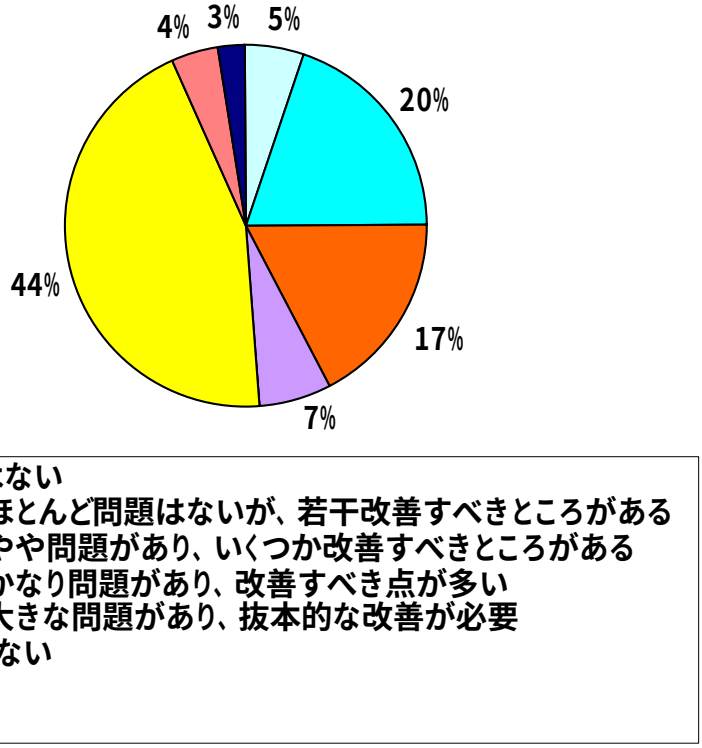
Q32　情報セキュリティ人材を育成・確保するための今後の方針



Q33　情報セキュリティ人材を育成・確保するための障害になっている要因



Q34　情報セキュリティ資格制度全般に対する評価



Q35　資格制度全般についての改善点

資格制度の乱立・重複等について指摘する回答

○　資格の種類が多すぎる。

○　資格制度がベンダーごとに乱立しているため、ＣＤＰに盛り込みにくい。例えば経済産業省制定のものなどに一本化した方が良い。

○　重複感がある。

○　多種の資格制度が乱立し、何が必要で適性かが不明確。体系の整備を望む。

○　各資格の適用範囲が問題。

○　似たような資格が多すぎる。

○　主務官庁が複数にまたがっているためか、公的資格の付与機関が多すぎる。

○　資格制度が乱立し、どれを選択すれば良いのかわかりにくい。技術系、マネジメント系各分野別に整理が必要。

実務との乖離について指摘する回答

○　業務実施資格との乖離、資格の効力の明確化。

○　学問の域を出ていない感がある。制度はツールとしては有効かもしれないが、社内における実行との間にはかなりの距離感がある。

○　総じてインフラ中心の情報セキュリティ認証のため、システム開発・保守領域・ＩＴ以外の情報セキュリティのノウハウを評価する仕組みが不足している。

○　「資格＝能力」とは必ずしもなっていない。資格をとったからといって仕事ができるとの納得感が必ずしも得られない。即ち、実務に直接役立つものになっていない。

○　実践的な教育が不足している。

○　資格の持つ価値が定量的に見えない。基準に合ったサービスを認定するほうが現実的ではないか。

○　セキュリティ技術、法制度の知識を問うことが主になっているが、本来はサイバー攻撃から実際に守る実践力を問うべき。

その他の回答

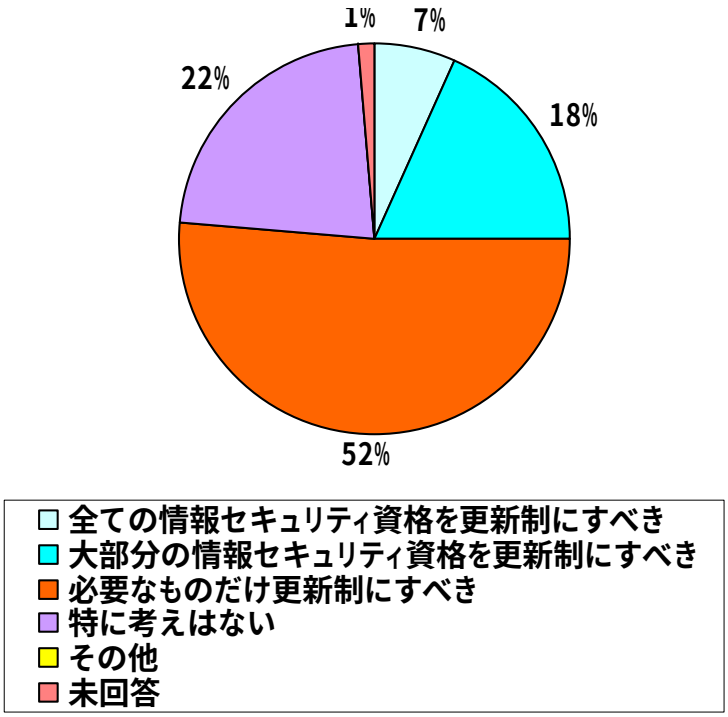
○　全体的に維持更新が大変である。(時間的にも金銭的にも)

○　一般ユーザ企業として、技術の概要についての知識は必要であるが、より経営的観点から捉えるべき問題としていくべきである。

○　費用さえ出せば取得可能なものが多い。

○　技術面が重視されすぎ、システム環境やリソース関連への知識取得のモチベーションが低い。

Q36　情報セキュリティ資格の更新制に対する考え方



Q37　個別資格についての改善点

○　ベンダー系の情報セキュリティ資格は、個別の要素技術に特化しすぎであり、国による資格に個別の要素技術も取り入れるなど一本化を図った方が良い。また、セキュリティ対策の実施者だけでなく、監査や内部統制の観点からモニタリングする視点も盛り込んだ方が良い。

○　全て。特にメーカー名のついた資格はメーカーの売上げの一部としかなってないと思われ、全く不要。

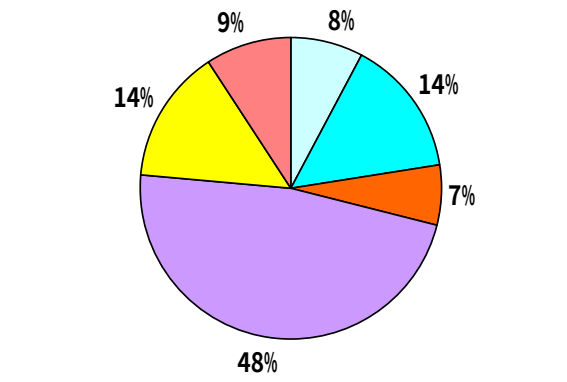
○　実態的にあまり意味のない継続教育要件が要求されている資格は見直した方が良い。

○　情報セキュリティ監査人は他の資格との重複感がある。

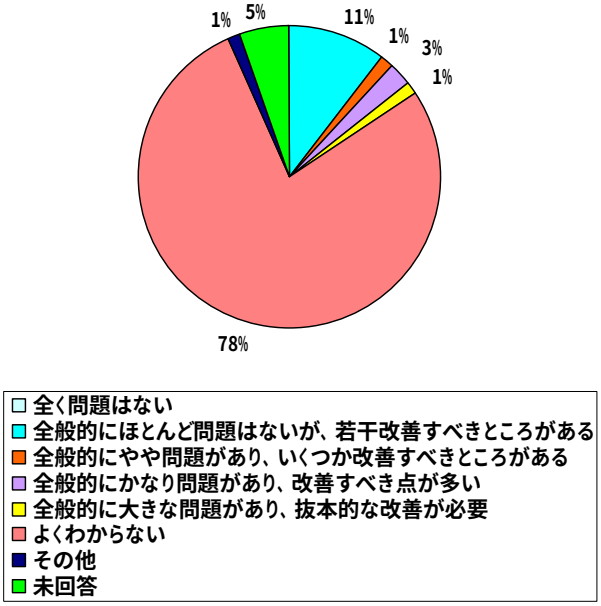
○　具体的資格名は挙げられないが、単にセキュリティ技術、法制度等の知識を問うだけだと役に立たない。

○　情報セキュリティ分野は技術的に日進月歩であり、有資格者のモチベーションが高ければまだしも、そのあたりを確認する為にも更新制など確認をしなければ、国ベースで必要な人材を育成出来ているか否かもわからない。

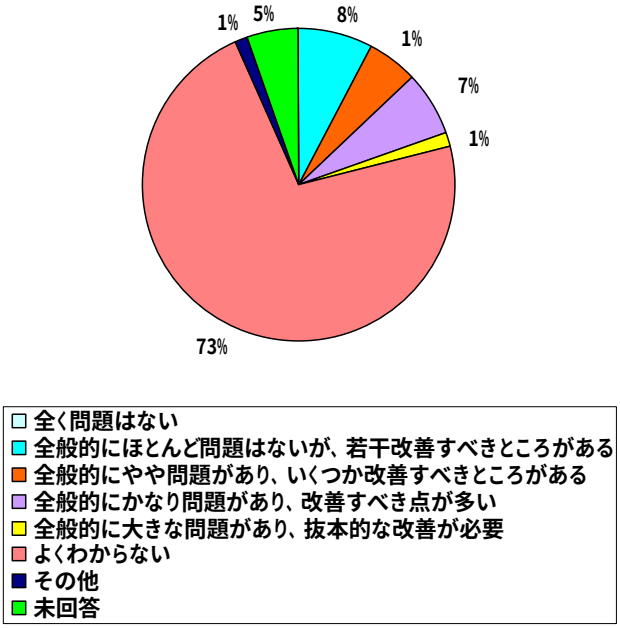
Q38　教育を行う主体で最も重要なもの



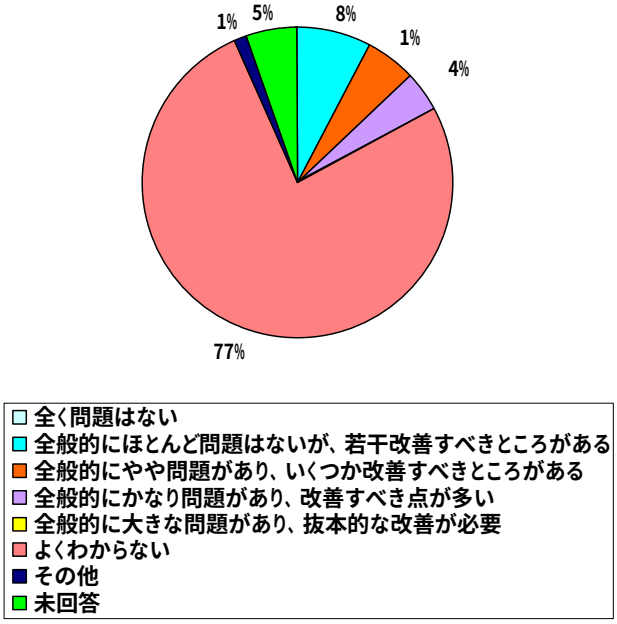
Q39　専門学校に対する評価



Q41　大学に対する評価



Q43　大学院に対する評価



Q40　専門学校についての改善点

○　知識の教育に偏っている感があり、社内における実行との間にはかなりの距離感がある。

○　ツールの使い方が中心のところがあり、その場合、情報セキュリティの基本的考え方、本質の教育が不足している可能性がある。

Q42　大学についての改善点

○　理論や技術が中心となり、実践的なスキル、実践力が不足する可能性がある。社会に出てから磨くという考え方もあると思うが。

○　指導教授自身が、現場・実社会との距離感があるのではないかとの危惧がある。

○　大学の教育課程として情報セキュリティ教育が組み込まれているかが疑問。実践的な場面との乖離があるように思える。

○　学問に重点が置かれている点。

○　基礎から体系的な教育ができていない。

○　大学・大学院で育成すべき人材として、セキュリティ対策技術・ツールに詳しい者と、ＩＴ環境面からそれを如何に応用するかというコンプライアンス面も含めて詳しい者が必要だと思う。両面でのアプローチが少し弱いのではないか。

○　法的あるいは知的財産の観点もわかる人材の育成。

Q44　大学院についての改善点

○　教育内容が情報技術に偏重している気がする。会社の中で情報セキュリティを保つためには、様々な業務改革を自ら推進していく能力が問われるが、そういった面の教育が手薄だと思う。

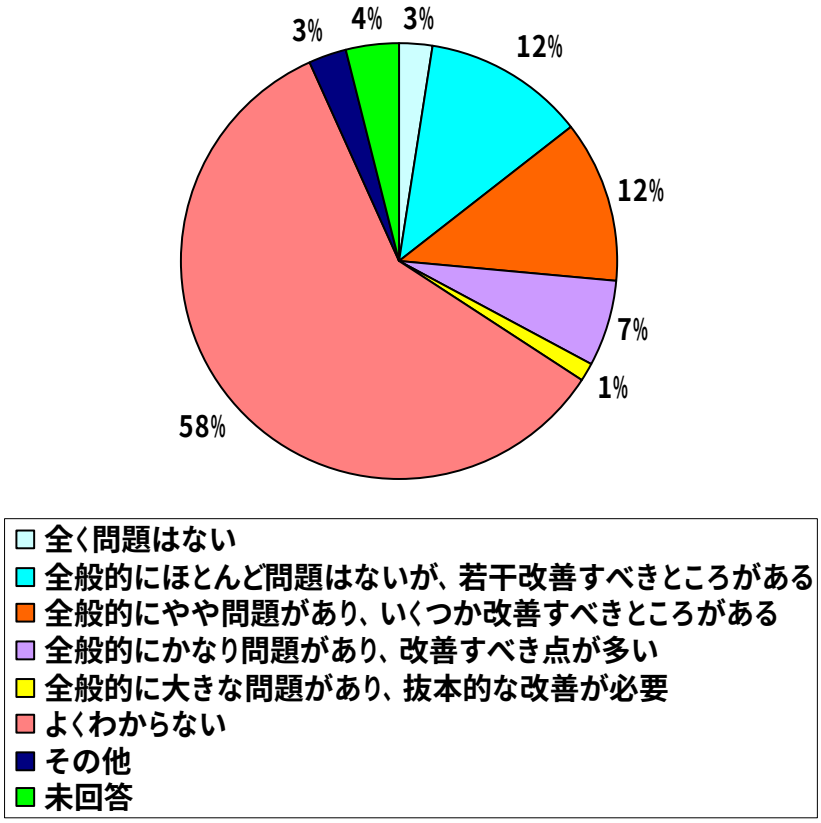
○　実践面との乖離があるように思える。

○　学問に重点が置かれている点。

○　一般の大学院でセキュリティ人材にフォーカスした教育が少ない。

○　コースそのものが少ないと思う。また、教えることが出来る人材も少ないのではと思う。

Q45　行政が果たしている役割に対する評価



Q46　行政の役割に対する改善点

法制度・フレームワーク・ガイドライン等の整備に関する回答

○　人材育成のフレームワークの明確化

○　人材育成等を含めた情報セキュリティ対策における行政としての方針を法制化することにより、国としての役割をより明確にすべきである。

○　資格制度の体系整理と企業として何が必要かのガイドライン整備を望む。

○　企業や団体が備えるべきセキュリティレベルとして、企業規模や業種別に、分野や必要人員数等、ある程度の指針を示していただきたい。

○　ベンダーサイドとユーザサイドに分け、ユーザ企業として必要な人材育成カリキュラムを整備して欲しい。

○　情報技術の開示・普及について一層の改善が必要と思われる。その上で、一般企業（中小～大企業まで）において、何処まで施すべきなのかといったガイドラインを徹底して欲しい。

その他の回答

○　情報セキュリティ施策の重要性について、社会的認識をより高めてもらうことで、人材の育成・確保の重要性が高まると考える。

○　資格、制度の整備だけでなく、情報セキュリティの必要性を社会に認識させ、それを担う人材の社会的地位を上げる施策の強化が必要だと思う。

○　資格制度は整備されているが、他に実務経験者の大学受入支援制度の導入が望まれる。

○　情報セキュリティ確保の必要性の積極的な広報及び資格制度のみならず、実践に即した人材育成のための教育やその費用の助成をお願いしたい。

○　実務に役立つ資格とすること。（作業スキルレベルの資格、プランニングあるいはコンサルティングレベルの資格のいずれも）

○　学校、企業、社会に対して、積極的に指導、支援、補助等を行うべきである。

○　情報セキュリティ人材として、ＩＳＯ１５４０８のようにセキュリティ対策技術の専門家と、いかにツールを応用・適用するかという２種類があると思う。Ｗｉｎｎｙを使わないようにという国からの指導は、後者になると考えるが、両面での一層の指導・提言をお願いする。

○　公的資格の設立は意味がないのではないか。

○　各省庁の役割を一本化して欲しい。（経済産業省、内閣官房など）

Q47　その他要望等

ベストプラクティス・ガイドライン・法制度の整備等に関する回答

○　米国 SOX 法など内外の法制度に則した、タイムリーかつ実効的な政策を期待する。

○　今後出てくる日本版ＳＯＸ法やシステム監査基準と、情報セキュリティとの整合性をとったガイドラインを出して欲しい。

○　ベンダーサイド、ユーザサイドの役割などを明確に区別したガイドラインを作って欲しい。

○　各省庁からのガイドラインが多すぎるので一本化して欲しい。
　例：個人情報保護法の経済産業省、総務省など

○　情報セキュリティに関する法制度の拡充

○　人材育成の前に、情報セキュリティ確保に関する具体的基準やベストプラクティスを整備する必要がある。

○　各企業（海外含め）で発生している事件・事故の事例を原因と対策を含め開示して欲しい。

公的機関による支援等に関する回答

○　情報セキュリティの現場は、技術動向の変化、新たな脅威の出現のスピードが早く、知識・経験がすぐに陳腐化する。そのため、制度的技術確保のための制度的支援を希望する。

○　国内全体のセキュリティレベルを底上げするという方針に沿い、企業への人材育成のための助成金制度等、具体的な施策が必要。

○　補助金制度

○　不正アクセスやサイバーテロなどを仕掛けてくる側の技術、情報、ツールなどのレベルが上がってきており、守る側の対応が追いつかない状況になっている。
　各企業が独自に対応するのではなく、効果的で実用的な対応技術やその適用に必要な人材を公的機関が育成する制度が望まれる。

教育機関による取組みに関する回答

○　専門学校・大学・大学院の人材教育が、会社で役に立つものとはとうてい思えない。ほとんどの場合、再教育が必要。一般的な知識としては意味があるのかもしれない。とにかく、現在は「セキュリティ」をキーワードとして儲け主義的な活動が世の中に溢れているので、そういったものを一度掃除して欲しい。

○　企業のおける情報セキュリティ人材は不足しており、入社する以前にある程度のセキュリティに関する知識・常識を身につけるよう、高校～大学のカリキュラムに組み込む等の施策を進めていただきたい。

○　企業により対応の力の入れ具合が異なる。学生のときからカリキュラムに取り入れるべき。

○　昨年より自宅パソコンからＷｉｎｎｙなどのファイル交換ソフトを悪用したウイル

スにより個人情報や機密情報等の漏洩事件が多発している。特に学生の利用により被害が拡大している。

情報を活用する者として最低限の知識や意識付けが必要であるため、事件概要・問題点、防衛策などを題材とした授業を中学又は高校で教育するようにしてセキュリティレベルの底上げをして欲しい。

資格制度に関する回答

○　資格の効果がわかるような第三者評価が欲しい。

○　企業における育成体制及び公的な資格制度を適切に組み合わせ、その成果（結果）が評価に結びつくよう、推進することが重要。

その他の回答

○　情報セキュリティ対策は情報システムの立場からだけで実現するものではない。企業内の監査業務、法務業務等と密接に関係する必要がある。

セキュリティの技術とルールの実行を確保する体制や権限との整合のとれた組織作りを担える人材の育成・確保が重要である。

○　ビジネスを遂行する上でパートナー（協力会社）との連携が必須であり、パートナーの情報セキュリティも高める必要がある。中小・零細企業では人材を独自に育成することはかなり厳しい。発注元として各社が諸施策を打っていると思うが、そういう企業へのセキュリティ対策をサポートする人材や組織の整備が必要ではないだろうか。

○　情報セキュリティだけしかできない人材は価値が低い。

業務改革、システム改革ができた上で、情報セキュリティもできる人を育てる工夫が必要。

○　セキュリティ責任者の社会的地位向上等、魅力ある職業としての位置づけをつくる企業を超えた社会全体の活動が必要。

○　実際のセキュリティ対策では、リスクの大きさ、対策コスト、利便性の低下等、複数の要素を考慮して、現実的な施策を実施していく必要がある。そのため情報セキュリティ人材には、法制度や各種基準類の理解とシステム開発・運用に関する知識を広

範囲にバランスよく習得することが求められる。
　また、情報セキュリティ対策は、トップから現場職員に至る全ての社員が危機管理意識、それを支えるモラルとモチベーションを持てるようになることが最も重要。

○　予防（防止）策を有効なものとするための十分な要員の配置が確保される必要がある。

○　日本全体に言えることだと思うが、ＩＴは仕事や生活を充実させていくためのツールのひとつであり、仕事上ではそろばんや電卓と同様に利用する人次第であるという主体的認識が薄いと感じる。若い世代はわからないが、特に中高年に「専門家がやってくれるもの」という意識が強く、結果として、情報セキュリティの意識についても主体性がない。時節柄、重要なものという認識はあるだろうが、社会のルールだから守るという受身の意識である。その様な意識の持ち主は主体的ではないので、責任感もなく、何かあれば専門家の責任とする傾向にある。情報セキュリティの管理責任者は日々この様な壁と戦っている。一個人としての主体性がないのは国民性なのか。国やマスコミ、知識人にこの様な風土を変えていく努力を期待する。

○　セキュリティ脅威は企業毎に異なるものではないと思う。国と産業界が協力して、情報共有・共通対応をしていくことが効率的と考える。

○　広く海外の知識・技術等を常に取り入れ、活用していけるような人材の育成を期待する。

主な情報セキュリティ資格について（その1）

略称	SU	SV
正式名称	情報セキュリティアドミニストレータ	テクニカルエンジニア（情報セキュリティ）
主催者	(独)情報処理推進機構	同左
想定する人材 ・スキル項目	企業等の組織における情報セキュリティ対策、管理責任者 【スキル項目（出題範囲）】 （午前の試験） ・コンピュータシステム ・システムの開発と運用 ・ネットワーク技術 ・セキュリティと標準化 ・情報化と経営 ・監査 （午後の試験） ・情報セキュリティシステムの企画・設計・構築に関すること ・情報セキュリティの運用・管理に関すること ・情報セキュリティの技術・関連法規に関すること	情報システムの設計・構築・運用において、情報セキュリティ技術の専門家として、情報セキュリティ機能の開発を推進又は支援する者 【スキル項目（出題範囲）】 （午前の試験） ・コンピュータシステム ・システムの開発と運用 ・ネットワーク技術 ・データベース技術 ・セキュリティと標準化 （午後の試験） ・情報セキュリティシステムの企画・設計・構築に関すること ・情報セキュリティの運用・管理に関すること ・情報セキュリティ技術・関連法規に関すること ・開発の管理に関すること
取得方法等	試験（4 択式 55 問＋記述式 4 問（3 問回答）＋記述式 2 問（1 問回答））	試験（4 択式 55 問＋記述式 4 問（3 問回答）＋論述式 2 問（1 問回答））
実習等の有無	なし	なし
更新制の有無	なし	なし
受験者/取得者数	受験者数　127,461 人（H13～17 年度） 合格者数　16,034 人（同上）	受験者数　18,128 人（H18 年度） 合格者数　1,227 人（同上）
受験費用	5,100 円	5,100 円

注）本資料は、現在運営されている情報セキュリティ資格のうち、主なものについて調査し単純に列挙したものであり、本委員会としてこれらの資格を特に推奨しようとするものではない。
また、資格の中には「公認」「Certified」という語が付されているものがあるが、これらは、各資格の運営団体が付けた名称であり、本委員会として「公認」等しようとするものではない。

主な情報セキュリティ資格について（その2）

略称	NISM	CISSP
正式名称	ネットワーク情報セキュリティマネージャー	Certified Information Systems Security Professional
主催者	NISM 推進協議会 （(社)電気通信事業者協会、情報通信ネットワーク産業協会、(社)テレコムサービス協会、(社)電波産業会、(社)日本インターネットプロバイダー協会、(財)日本データ通信協会、(社)情報通信技術委員会）	(ISC)² ジャパン
想定する人材 ・スキル項目	情報通信ネットワークの運用に携わる者（通信キャリア、ネットワークを利用するサービス事業者及びそれらの機器を開発・製造するメーカーなど） 【総合スキル】 ①ネットワークセキュリティ基礎 ②ネットワークセキュリティ実践 【専門スキル】 ③サーバセキュリティ実践 ④不正アクセス監視実践 ⑤セキュリティポリシー実践 ⑥セキュリティ監査実践	企業等の組織における情報セキュリティ関連業務に従事する実務家・専門家（情報セキュリティ及びシステム担当役員・管理職・担当者、関連製品・サービスの営業職、コンサルタント、エンジニア等）。 【スキル項目：CBK(Common Body of Knowledge)】 ・アクセス制御 ・アプリケーションセキュリティ ・事業継続と災害復旧計画 ・暗号学 ・情報セキュリティとリスクマネジメント ・法律、規制、コンプライアンス、捜査 ・運用セキュリティ ・物理（環境セキュリティ） ・セキュリティアーキテクチャと設計 ・通信とネットワークのセキュリティ
取得方法等	①講義＋試験（2 日） ②③④講義・実習・演習＋試験（3 日） ⑤⑥講義・演習＋試験（2 日）	・認定試験（4 択式 250 問、日英併記）に 700/1000 ポイント以上で合格 ・CBK10 ドメインのうち、少なくとも一分野における 4 年以上（大卒は 3 年以上）の「プロフェッショナルとしての」経験（無作為に行われる監査あり） ・倫理規約への同意　等
実習等の有無	実機を用いた実習、演習あり	なし（上記のとおり 4 年等の実務経験は必要）
更新制の有無	2 年ごとの更新制あり	3 年更新（認定維持料 12,000 円と 120 ポイントの継続教育単位取得が必要）
受験者/取得者数	受講者数　新規 1,554 人　更新　466 人（H13～17 年度） 取得者数　新規 1,545 人　更新　465 人（同上）	取得者数　570 名以上（全世界で 43,000 名以上）
受験費用	①63,000 円、②157,500 円、③④168,000 円 ⑤⑥73,500 円（いずれも会員価格）	68,250 円 （5 日間のセミナーを受けて受験する場合は 630,000 円）

注）本資料は、現在運営されている情報セキュリティ資格のうち、主なものについて調査し単純に列挙したものであり、本委員会としてこれらの資格を特に推奨しようとするものではない。
また、資格の中には「公認」「Certified」という語が付されているものがあるが、これらは、各資格の運営団体が付けた名称であり、本委員会として「公認」等しようとするものではない。

主な情報セキュリティ資格について（その3）

略称	CSBM	CSPM(Technical)	CSPM(Management)
正式名称	情報セキュリティ技術認定・基礎コース (Certified Security Basic Master)	同左・応用コース（テクニカル編） (Certified Security Professional Master of Technical)	同左・応用コース（マネジメント編） (Certified Security Professional Master of Management)
主催者	SEA/J　(Security Education Alliance / Japan)		
想定する人材 ・スキル項目	セキュリティに関係する初級技術者及びシステム関係企業の従業員 【スキル項目】 ・ネットワークセキュリティ基礎 ・攻撃手法 ・ファイアウォール ・不正侵入検知システム ・暗号・認証 ・PKI ・セキュリティプロトコル ・ウィルス ・クライアントセキュリティ ・権限とデータ管理 ・セキュリティ運用 ・情報セキュリティポリシー ・関連法規	システム/セールスエンジニア、情報システム管理者、IT コンサルタント 【スキル項目】 ・セキュリティ対策の考え方 ・脅威とその対策 ・OS の要塞化（Windows） ・OS の要塞化（Linux） ・DNS サーバーへのセキュリティ対策 ・メールサーバーへのセキュリティ対策 ・Web サーバーへのセキュリティ対策 ・ファイアウォール導入設計 ・IDS による侵入検知 ・VPN 導入設計 ・PKI の利用	情報システム管理者、セキュリティ監査員、法務担当 【スキル項目】 ・情報セキュリティとはなにか ・情報セキュリティの構成要素 ・脅威と脆弱性 ・情報セキュリティマネジメント ・リスクの概念 ・リスク分析の概要 ・詳細リスク分析 ・リスクマネジメント ・情報セキュリティポリシーの概要 ・情報セキュリティポリシーの策定 ・情報セキュリティ監査制度
取得方法等	講義＋試験（2 日）	講義、実習＋試験（3 日）	講義、演習＋試験（2 日）
実習等の有無	なし	実機を用いた実習あり	グループ演習あり
更新制の有無	なし	なし	なし
受験者/取得者数	受験者数　2,981 人 合格者数　2,666 人	受験者数　422 人 合格者数　299 人	受講者数　456 人 合格者数　235 人
受験・受講料等	99,750 円（受験のみの場合は 15,750 円）	204,750 円（受験のみの場合は 15,750 円）	141,750 円（受験のみの場合は 15,750 円）

注）本資料は、現在運営されている情報セキュリティ資格のうち、主なものについて調査し単純に列挙したものであり、本委員会としてこれらの資格を特に推奨しようとするものではない。
また、資格の中には「公認」「Certified」という語が付されているものがあるが、これらは、各資格の運営団体が付けた名称であり、本委員会として「公認」等しようとするものではない。

主な情報セキュリティ資格について（その4）

略称	CISA	CISM
正式名称	公認情報システム監査人 Certified Information Systems Auditor	公認情報セキュリティマネージャ Certified Information Security Manager
主催者	ISACA 東京支部	
想定する人材 ・スキル項目	企業等の組織の情報システムやセキュリティのコントロール（統制）に係わる組織で業務を担当する者や、これを評価（監査）する者。 【スキル項目】 ・情報システム監査のプロセス ・IT ガバナンス ・システムとインフラストラクチャのライフサイクル管理 ・IT サービスの提供と支援 ・情報資産の保護 ・災害復旧と業務継続	企業等の組織の情報セキュリティを管理、設計、監督する個人。具体的には、情報セキュリティマネージャ、セキュリティ担当役員・担当役職者、セキュリティコンサルタントなど。 【スキル項目】 ・情報セキュリティガバナンス ・リスク管理 ・情報セキュリティプログラム管理 ・情報セキュリティ管理 ・対応管理（レスポンスマネジメント）
取得方法等	・CISA 試験に 25～99 のうち 75 以上のスコアで合格 ・最低 5 年間の情報システム監査、コントロール（管理）、セキュリティ分野のいずれかの実務経験を有すること ・倫理規約の遵守	・CISM 試験に 25～99 のうち 75 以上のスコアで合格 ・情報セキュリティに関する 5 年以上の経験を有し、そのうち 5 ドメイン中の 3 ドメイン以上から、3 年以上のセキュリティマネジメントの経験を有すること ・倫理規約の遵守
実習等の有無	なし（上記のとおり 5 年の実務経験は必要）	なし（上記のとおり 5 年の実務経験は必要）
更新制の有無	1 年で 20CPE、かつ、3 年で 120CPE 以上の継続教育 維持手数料の支払い（US＄40（会員）、US＄60（非会員））	1 年で 20CPE、かつ、3 年で 120CPE 以上の継続教育 維持手数料の支払い　（US$40（会員）、US$60（非会員））
受験者/取得者数	受験者数　東京会場で 1,100 名/年 取得者数　1,067 名（全世界で 34,361 名）本年 7 月 6 日現在	受験者数　約 100 名/年 取得者数　約 104 名（全世界で 5,231 名）本年 7 月 6 日現在
受験・受講料等	US＄340（会員）、US＄460（非会員）	US＄340（会員）、US＄460（非会員）

注）本資料は、現在運営されている情報セキュリティ資格のうち、主なものについて調査し単純に列挙したものであり、本委員会としてこれらの資格を特に推奨しようとするものではない。
また、資格の中には「公認」「Certified」という語が付されているものがあるが、これらは、各資格の運営団体が付けた名称であり、本委員会として「公認」等しようとするものではない。

主な情報セキュリティ資格について（その5）

略称	CAIS-Lead Auditor	CAIS-Auditor	CAIS-Assistant	CAIS-Associate
正式名称	**公認情報セキュリティ主任監査人** Certified Auditor for Information Security-Lead Auditor	**公認情報セキュリティ監査人** Certified Auditor for Information Security-Auditor	**情報セキュリティ監査人補** Certified Auditor for Information Security-Assistant	**情報セキュリティ監査アソシエイト** Certified Auditor for Information Security-Associate
主催者	**特定非営利活動法人　日本セキュリティ監査協会（JASA）**			
想定する人材 ・スキル項目	**情報セキュリティ監査チームのリーダとなる者**	**監査計画の立案、監査の実施、報告書の作成など、監査を実質的に担当する者。経験を積んで** CAIS-Lead Auditor **を目指す。**	OJT **として監査に参加する者。監査経験を積んで** CAIS-Auditor **を目指す。**	**監査チームの要請により専門知識に基づく助言を行う者**
取得方法等	**・情報通信技術分野での** 4 **年以上の業務経験、うちセキュリティ関連分野で** 2 **年以上の業務経験。（**CISM、CISSP、SU、SV **で代替可）。** **・監査に関する協会認定研修を修了すること。** **・協会認定トレーニングを修了すること。** **・倫理基準遵守の誓約。** **・過去** 3 **年以内に最低** 4 **回延べ** 20 **日間の監査実施経験（うち** 2 **回以上は助言型監査又は保証型監査）があること。** **・過去** 2 **年以内に最低** 3 **回延べ** 15 **日間は、上位の監査人の指導の下で、監査チームリーダとしての経験があること。** **・面接審査を受けること。**			**・専門分野（分野は問わない）での** 3 **年以上の業務経験を有すること、又は代替する資格を保有すること。** **・監査に関する協会認定研修を修了すること。** **・倫理基準遵守の誓約。**
実習等の有無	**トレーニングの中で演習あり（また、上記のとおり実務経験が必要）**			**なし（上記のとおり実務経験は要）**
更新制の有無	1 **年ごとに更新手数料が必要となるほか、**3 **年間で協会が定めたプログラムを一定程度こなすことが必要。**			
受験者/取得者数	**取得者　約** 60 **人**	**取得者　約** 90 **人**	**取得者　約** 100 **人**	**取得者　約** 90 **人**
受験・受講料等	**登録料　申請** 30 **千円＋登録** 10 **千円** **受講料・受験料　**310 **千円等** **維持手数料　**15 **千円**	**登録料　申請** 10 **千円＋登録** 10 **千円** **受講料・受験料　**310 **千円** **維持手数料　**15 **千円**	**登録料　申請** 10 **千円＋登録** 10 **千円** **受講料・受験料　**310 **千円** **維持手数料　**15 **千円**	**登録料　申請** 5 **千円＋登録** 5 **千円** **受講料・受験料　**95 **千円等** **維持手数料　**5 **千円**

注）本資料は、現在運営されている情報セキュリティ資格のうち、主なものについて調査し単純に列挙したものであり、本委員会としてこれらの資格を特に推奨しようとするものではない。
また、資格の中には「公認」「Certified」という語が付されているものがあるが、これらは、各資格の運営団体が付けた名称であり、本委員会として「公認」等しようとするものではない。

主な情報セキュリティ資格について（その6）

略称	GIAC
正式名称	Global Information Assurance Certification
主催者	SANS Institute
想定する人材 ・スキル項目	**企業等の組織において情報システム管理や情報セキュリティ管理を担当する者、情報セキュリティに関する技術的案業務を企業等の組織内において専門的に行う者、情報セキュリティに関する業務を事業として提供するベンダの者** **【主な試験の種類とそれに対応するトレーニングコース】** • GSEC(SANS Security Essentials Bootcamp) • GCFW(Firewalls, Perimeter Protection, and VPNs) • GCIA(Intrusion Detection In-Depth) • GCIH(Hacker Techniques, Exploits and Incident Handling) • GCWN(Securing Windows) • GCUX(Securing Unix/Linux) • GSNA(Auditing Networks, Perimeters & Systems) • GCFA(System Forensics, Investigation and Response) • GISF(Intro to Information Security) • GSAE(IT Security Audit Essentials) • G7799(SANS 17799 Security and Audit Framework) • GSLC(SANS Security Leadership Essentials For Managers) • GCSC(Security Consultant) • SANS +S Training Program for the CISSP Certification Exam • GSIP(Secure Internet Presence – LAMP)
取得方法等	Web **による試験（多肢選択式、**100 **問×２回、各回** 70 **点以上で合格）【**6 **日間のトレーニングコース受講後に受験するのが一般的】**
実習等の有無	**なし**
更新制の有無	4 **年ごとに再受験が必要**
受験者/取得者数	**受験者数　のべ約** 200 **名（**H15～18.6**）** **取得者数**　30 **名程度（**GSEC **の日本語受験のみ。他の英語受験の試験と合わせると** 50 **人程度。全世界で** 12,876 **名）**
受験･受講料等	34,000 **円（**6 **日間のトレーニングコースは、約** 40 **万円程度）**

注）本資料は、現在運営されている情報セキュリティ資格のうち、主なものについて調査し単純に列挙したものであり、本委員会としてこれらの資格を特に推奨しようとするものではない。
また、資格の中には「公認」「Certified」という語が付されているものがあるが、これらは、各資格の運営団体が付けた名称であり、本委員会として「公認」等しようとするものではない。

主な情報セキュリティ資格について（その7）

略称	Security＋	CSA	ASA
正式名称	CompTIA 認定資格　Security+	公認システム監査人 (Certified Systems Auditor)	システム監査人補 (Associate Systems Auditor)
主催者	The Computing Technology Industry Association(CompTIA)	特定非営利活動法人　日本システム監査人協会（SAAJ）	
想定する人材 ・スキル項目	顧客のセキュリティ環境の理解・改善を要するカスタマエンジニア、フィールドサポート、システムエンジニアコールセンター、インストラクタ、など 【スキル項目】 　セキュリティ技術業務における、顧客側の環境の理解と最適な環境へ導く能力を評価 ・セキュリティの一般概念 ・コミュニケーションセキュリティ ・インフラストラクチャセキュリティ ・暗号技術の基本 ・業務・組織面でのセキュリティ	情報セキュリティを含むシステム監査を実施する監査人団の責任者	責任者の指揮の下、情報セキュリティを含むシステム監査を実施できる者
取得方法等	試験（CBT／問題文や穴埋め問題に適する正答を一つまたは複数選択する問題や、図やテキストを正しい場所へドラッグ＆ドロップする形式など／制限時間 90 分／100 問／100～900 のスコア形式　764 スコア以上）	・システム監査人補と同等の知見を持っていること。 ・小論文及び面接試験による必要な資質と実務経験の審査を受け、合格すること。	・システム監査技術者試験合格者と同等の知見を持っていること。 ・「継続教育を受ける旨」の宣誓書を提出すること。
実習等の有無	なし	なし	なし
更新制の有無	なし	３年ごとの更新制あり（一定時間以上の教育の受講が継続要件）	
受験者/取得者数	非公開	660 人/459 人(H15～18 年度)	373 人/371 人(H15～18 年度)
受験･受講料等	28,984 円（会員価格あり）	52,500 円	10,500 円

注）本資料は、現在運営されている情報セキュリティ資格のうち、主なものについて調査し単純に列挙したものであり、本委員会としてこれらの資格を特に推奨しようとするものではない。
　　また、資格の中には「公認」「Certified」という語が付されているものがあるが、これらは、各資格の運営団体が付けた名称であり、本委員会として「公認」等しようとするものではない。

資料6

情報セキュリティに係る人材に求められる能力と各種教育プログラムの体系図について

1. 概要

本資料では、情報セキュリティに係る人材の育成計画を立てようとする者が、比較をしつつその参考とできるような一つの目安として、

－第三章及び第四章において整理した情報セキュリティに係る人材のカテゴリごとに必要とされる能力の整理を行い、

－その上で、それぞれの人材カテゴリごとに、能力の習得等に資すると考えられる各種教育プログラムについて整理を行った。

なお、第二章において整理した人材カテゴリ、すなわち、先進的な情報セキュリティ技術・製品及び高度な管理手法の研究・開発者については、未開拓の領域を新たに切り開いていくべき人材であり、既に体系化された知識や技能を習得することによる育成方策を論じることは困難であることから、この検討の対象からは外している。

2. 体系図の構成

本体系図においては、各列において第三章及び第四章において整理した情報セキュリティに係る人材を並べ、各行においては、これら人材に求められる能力の項目と、各種教育プログラムの大まかな分類を並べている。そして、人材カテゴリごとに、後述の凡例に従って求められる能力を示すとともに、その能力の習得等に資すると考えられる具体的な教育プログラムをまとめている。

これにより、情報セキュリティに係る人材の育成計画を立てようとする者は、育成しようとする人材にどのような能力が必要となり、そのためにどのような教育プログラムがあるのかが、分かりやすく理解できることとなる。

(1) 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提供する企業等における人材に求められる能力についての凡例

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（以下、「製品

等」という）を提供する企業等における人材は、顧客企業等に対してより品質・信頼性の高い製品等を提供するために必要となる能力の確保が求められる。この前提に基づいて、以下のとおり能力についての凡例を設定した。

Ａ：情報セキュリティ対策に直結する製品等の製造・開発・提供に直接携わる者として、関連する先端的な技術・製品や高度な管理手法について熟知し、これらを製品等の中で活用・実装し、提供できる能力
Ｂ：情報セキュリティ対策に関係する、
・ 技術系の製品等の製造・開発・提供に携わる中で、情報セキュリティの要求事項を理解し、製品等の中で実装・提供できる能力
・ 管理系の製品等の提供に携わる中で、技術系の製品等や専門外の管理系の手法や製品等についても相当程度理解し、顧客に助言等できる能力
Ｃ：情報セキュリティに関する製品等を製造・開発・提供する上で知識として身に付けておくべき能力

(2) 政府機関、企業等の組織において情報セキュリティ対策に係る人材に求められる能力についての凡例

政府機関、企業等の組織において情報セキュリティ対策に係る人材は、組織の情報セキュリティを維持するために必要となる情報セキュリティ対策に係る能力の確保が求められる。この前提に基づいて、以下のとおり能力についての凡例を設定した。

α：提供される製品等に関する知識・技能を含め情報セキュリティ対策の目的やその手法について深く理解し、組織における直接の担当者としてこれを主導的に活用し、実践できる能力
β：提供される製品等に関する知識・技能を含め情報セキュリティ対策の目的やその手法について一定程度理解し、組織において外部人材等の専門能力を有する者と連携しつつ、これを活用し、実践できる能力
γ：組織における情報セキュリティ対策に係る知識として身に付けておくべき能力
－：特に業務上必須とはされない能力

(3) 情報セキュリティに関する教育プログラム・資格制度の凡例

情報セキュリティに係る人材の育成にあたって、資料１、資料２、資料５に

示す各種の教育プログラムについて、以下のとおり略称を設定した。
　なお、下記教育プログラムの中には、「公認」「Certified」という語が付されているものがあるが、これらは、各運営団体が付けた名称であり、本委員会として「公認」等しようとするものではない。

（ア）レベル判定型の教育プログラム

① 国が実施している教育資格試験制度（情報処理技術者試験）

教育プログラムの名称	表中の略称
テクニカルエンジニア（情報セキュリティ）	SV（IPA）
情報セキュリティアドミニストレータ	SU（IPA）

② 民間団体が運営している教育資格制度

教育プログラムの名称	表中の略称
Certified Information Systems Security Professional	CISSP
公認情報システム監査人（Certified Information Systems Auditor）	CISA
公認情報セキュリティマネージャ （Certified Information Security Manager）	CISM
CompTIA 認定資格　Security＋	CompTIA
公認システム監査人（Certified Systems Auditor）、システム監査人補(Associate Systems Auditor)	SAAJ

（イ）訓練・実習型の教育プログラム

① 高等教育機関

教育プログラムの名称		表中の略称
情報セキュリティ大学院大学		
	情報セキュリティ研究課情報セキュリティ専攻修士課程	iisec
	CISO コース	iisec・CISO
中央大学		
	21 世紀 COE プログラム・電子政府の信頼性向上と情報セキュリティ	中央大・COE
	副専攻、情報セキュリティ・情報保証・人材育成拠点	中央大・拠点/副

工学院大学（技術者能力開発センター・セキュアシステム設計技術者育成プログラム）	工学院大
カーネギーメロン大学　日本校（情報セキュリティ研究課修士課程）	CMU

② 財団等が実施している教育プログラム

教育プログラムの名称		表中の略称
（株）横須賀テレコムリサーチパーク ・座学中心コース（技術レイヤ向け基礎コース、管理レイヤ向け基礎コース） ・システム実習中心コース（イントラ・エクストラネットコース、Web ビジネスコース）		YRP
（財）ソフトピアジャパン		
	テクニカルコース、テクニカル実践コース	ソフトピア・Tec
	マネジメントコース、マネジメント実践コース	ソフトピア・Mgt
（財）ひょうご情報教育機構 ・共通コース ・基礎コース ・応用コース		ひょうご

③ 教育資格制度

教育プログラムの名称	表中の略称
情報セキュリティ技能認定・基礎コース（Certified Security Basic Master）	CSBM
情報セキュリティ技能認定・応用コース（テクニカル編）（Certified Security Professional Master of Technical）	CSPM・Tec
情報セキュリティ技能認定・応用コース（マネジメント編）（Certified Security Professional Master of Management）	CSPM・Mgt
公認情報セキュリティ主任監査人（CAIS-Lead Auditor）、公認情報セキュリティ監査人（CAIS-Auditor）、情報セキュリティ監査人補（CAIA-Assistant）	JASA
Global Information Assurance Certification	

【技術系トレーニング】 • GSEC(SANS Security Essentials Bootcamp) • GCFW(Firewalls, Perimeter Protection, and VPNs) • GCIA(Intrusion Detection In-Depth) • GCIH(Hacker Techniques, Exploits and Incident Handling) • GCWN(Securing Windows) • GCUX(Securing Unix/Linux) • GCFA(System Forensics, Investigation and Response)	SANS･Tec
【監査・コンサル系トレーニング】 • GSEC(SANS Security Essentials Bootcamp) • GSNA(Auditing Networks, Perimeters & Systems) • GSAE(IT Security Audit Essentials) • G7799(SANS 17799 Security and Audit Framework) • GCSC(Security Consultant)	SANS･Mgt
【マネジメント系トレーニング】 • GSEC(SANS Security Essentials Bootcamp) • GSLC(SANS Security Leadership Essentials For Managers)	SANS･TOP
GSEC(SANS Security Essentials Bootcamp)	SANS･Ess

3. 体系図を使用するにあたっての留意事項

本体系図を使用するにあたっての留意事項は、以下の通りである。

(1) 各カテゴリの人材に求められる能力の確保について

本体系図の各人材カテゴリにおいて求められる能力は、必ずしも一人の人材が全てをカバーしなければならないものではないことに留意が必要である。例えば、

・一般のベンダーやシステムインテグレータにおいて、複数の人材がチームとして携わるプロジェクトを組む場合には、チーム内のメンバーが各々に能力を備え、チーム全体として必要な能力の項目がカバーされていれば問題ないと考えられる。

・組織によって、「経営者」と、「CISO」や「CISO を補佐する者」と、「管理系分野の担当者」の役割分担の枠組みは様々であり、それぞれの組織によって、どの者に「α」の能力を求めていくのかについてはまちまちであると考えられる。

(2) 情報セキュリティに係る人材に必要な能力の凡例について

本体系図において必要とされている能力の凡例についても、あくまで「一つの目安」であるということに留意が必要である。例えば、技術系の製品等を提供する企業等における人材の「一般」について、技術系分野に関する能力が「B」とされているが、

- 外部ネットワークと接続する大規模な業務システムの開発プロジェクト等であれば、その中に技術系分野に関して「A」の能力を有する人材が必要となると考えられる。
- 他方、小規模な開発プロジェクトに開発要員（例えばプログラマ）として参加する担当者に、技術系分野の全項目について「B」を求める必要はないのではないとも考えられる。

(3) 一般職員・社員に求められる「セキュリティリテラシー」と「所属する組織のセキュリティポリシー」について

「セキュリティリテラシー」とは、本文の第四章第二節(2)アにおいて定義されているとおり、「情報技術を活用していく上での情報セキュリティ上の最低限の知識」である。したがって、体系図においては、求められる能力の中の「管理系分野」や「技術系分野」に分類される個々の能力について全て「－（特に業務上必須とはされない能力）」とされているが、「セキュリティリテラシー」に含まれるべき最低限の知識まで不要としているものではないことに留意が必要である。

また、「セキュリティポリシー」は、情報セキュリティに関して組織内で定められるルールのことを意味しており、一般的には明文化されたセキュリティポリシーが策定されていると考えられるが、仮に「セキュリティポリシー」と名のつく明文化された規程類がない場合においても、文書などの情報の管理やIT 機器の使用に関する規則など、実質的にセキュリティポリシーに相当する組織内ルールがある場合には、これを理解・遵守することが求められるものである。なお、情報セキュリティのリスクがあるにもかかわらず、セキュリティポリシーが定められていない組織においては、本文の第四章第四節(1)に示す考え方に沿って、早急にセキュリティポリシーの策定が求められることは、言うまでもない。

(4) 各種教育プログラムについて

各種教育プログラムについても、各プログラムの内容が最も適合していると考えられる人材カテゴリの欄に記載しているものであり、それ以外の欄においても一定程度効果があるプログラムも存在すると考えられる。

また、本体系図に掲載しなかったプログラムの中でも、能力の習得に効果があるプログラムも存在すると考えられる。

情報セキュリティに係る人材に求められる能力と各種教育プログラムの体系図【平成18年11月時点】

求められる能力		情報セキュリティに係る人材								
大分類	小分類	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提供する企業等における人材				政府機関、企業等の組織において情報セキュリティ対策に係る人材				
		技術系の製品等を提供する企業等における人材		管理系の製品等を提供する企業等における人材		幹部、経営者	一般職員社員	情報セキュリティ対策を担当する者		
		セキュリティ専門	一般	セキュリティコンサルティング	セキュリティ監査			CISO又はCISOを補佐する者	技術系分野	管理系分野
セキュリティリテラシー						α	α	α	α	α
所属する組織のセキュリティポリシー						α	α	α	α	α
管理系分野	マネジメント技術	C	C	A	A	γ	-	α	β	α
	リスク分析技術	C	C	A	A	γ	-	α	β	α
	情報セキュリティポリシーの策定	C	C	A	A	γ	-	α	β	α
	情報セキュリティ監査	C	C	B	A	γ	-	α	β	α
	関連知識	C	C	A	A	γ	-	α	β	α
	法令・規格	C	C	A	A	α	-	α	β	α
	事業継続経営（BCP/BCM）	C	C	A	A	α	-	α	β	α
	リスクコミュニケーション	C	C	A	C	α	-	α	β	β
	費用対効果	C	C	A	B	α	-	α	β	β
	人員計画	C	C	A	B	α	-	α	β	β
	教育・訓練	C	C	A	B	γ	-	α	β	α
	物理セキュリティ	C	C	A	B	γ	-	α	β	α
	調達管理					γ	-	α	β	α
	プロジェクトマネジメント	A	B	B	C	-	-	α	α	β
	セキュリティ運用	A	B	B	B	-	-	β	α	β
技術系分野 情報セキュリティ基本技術	セキュリティアーキテクチャ	A	B	B	B	-	-	β	α	γ
	ネットワークインフラセキュリティ	A	B	B	C	-	-	β	α	γ
	セキュアプログラミング技法	A	B	C	C	-	-	β	α	γ
	セキュリティプロトコル	A	B	B	B	-	-	β	α	γ
	認証	A	B	B	C	-	-	β	α	γ
	アクセス制御	A	B	B	C	-	-	β	α	γ
	PKI	A	B	B	C	-	-	β	α	γ
	暗号	A	B	B	C	-	-	β	α	γ
	電子署名	A	B	B	C	-	-	β	α	γ
	不正コピー防止・電子透かし	A	B	B	C	-	-	β	α	γ
ウイルス・侵入等対策技術	ファイアーウォール	A	B	B	C	-	-	β	α	γ
	侵入検知	A	B	B	C	-	-	β	α	γ
	ウイルス	A	B	B	C	-	-	β	α	γ
	不正アクセス手法	A	B	B	C	-	-	β	α	γ
アプリケーションセキュリティ	全般	A	B	B	C	-	-	β	α	γ
	Web	A	B	B	C	-	-	β	α	γ
	電子メール	A	B	B	C	-	-	β	α	γ
	DNS(Domain Name System)	A	B	B	C	-	-	β	α	γ
OSセキュリティ	Unix、Linux	A	B	B	C	-	-	β	α	γ
	Windows	A	B	B	C	-	-	β	α	γ
	TrustedOS	A	B	B	C	-	-	β	α	γ
レベル判定型の教育プログラム		-	SV（IPA） CompTIA	CISM CISSP	CISA SAAJ	-	-	SU（IPA） CISM CISSP	-	SU（IPA） CISM CISSP
訓練・実習型の教育プログラム		iisec 中央大・COE CMU	iisec 中央大・拠点/副 工学院大 CMU	iisec CMU	-	-	-	iisec・CISO CMU	中央大・拠点/副 工学院大	-
		-	YRP ソフトピア・Tec ひょうご	-	-			-	YRP ソフトピア・Tec ひょうご	YRP ソフトピア・Mgt ひょうご
		SANS・Tec	CSPM・Tec NISM SANS・Ess	SANS・Mgt	JASA			SANS・TOP	CSBM CSPM・Tec SANS・Ess	CSPM・Mgt

(1) 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提供する企業等における人材に求められる能力の凡例

- **A** 情報セキュリティ対策に直結する製品等の製造・開発・提供に直接携わる者として、関連する先端的な技術・製品や高度な管理手法について熟知し、これらを製品等の中で活用・実装し、提供できる能力
- **B** 情報セキュリティ対策に関係する、
  - 技術系の製品等の製造・開発・提供に携わる中で、情報セキュリティの要求事項を理解し、製品等の中で実装・提供できる能力
  - 管理系の製品等の提供に携わる中で、技術系の製品等や専門外の管理系の手法や製品等についても相当程度理解し、顧客に助言等できる能力
- **C** 情報セキュリティに関する製品等を製造・開発・提供する上で知識として身に付けておくべき能力

(2) 政府機関、企業等の組織において情報セキュリティ対策に係る人材に求められる能力の凡例

- **α** 提供される製品等に関する知識・技能を含め情報セキュリティ対策の目的やその手法について深く理解し、組織における直接の担当者としてこれを主導的に活用し、実践できる能力
- **β** 提供される製品等に関する知識・技能を含め情報セキュリティ対策の目的やその手法について一定程度理解し、組織において外部人材等の専門能力を有する者と連携しつつ、これを活用し、実践できる能力
- **γ** 組織における情報セキュリティ対策に係る知識として身に付けておくべき能力
- **－** 特に業務上必須とはされない能力

(注) 本体系図を使用するにあたっては、前述する留意事項を必ず参照すること。
(注) 必要な能力については、IPA（独立行政法人 情報処理推進機構）の作成したスキルマップ（http://www.ipa.go.jp/security/fy16/reports/skillmap/index.html）を基に検討を実施した。
(注)「セキュリティリテラシー」「所属する組織のセキュリティポリシー」「調達管理」は、対策の実施者として必要な能力であるため、「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提供する企業等における人材」においては対象外とした。