

# 情報セキュリティ人材の育成に向けた検討

～人材育成・資格制度体系化専門委員会における出発点～

平成18年8月30日  
内閣官房情報セキュリティセンター(NISC)

# 本専門委員会における検討項目について

「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)

## 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 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 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。

情報セキュリティ対策に遅れが見られる政府機関における人材の育成・確保方策も含め、我が国全体としての「情報セキュリティ人材」の育成・確保に向けて、包括的な検討を行う。(その一環として、資格制度に関する課題についても洗い出し、体系化を図る。)

## 検討に当たっての基本的な考え方について

### 検討の対象となる「情報セキュリティ人材」の範囲について

1. 本専門委員会においては、「情報セキュリティ人材」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関わる人材を対象にその育成方策を検討することとする。
2. 例えば、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情報セキュリティ・リテラシの向上といった課題については、検討の対象外とする。

### 検討の進め方について(案)

1. 一言に「情報セキュリティ人材」と言っても、どういった人材を指すのか、必ずしも明確でない。また、資格制度の体系化についても、実際に我が国の情報セキュリティ対策の向上につながるような人材の育成・確保につながるような形で課題の整理が行われるべき。
2. したがって、まず、我が国全体の情報セキュリティ対策を支える上で必要となる「情報セキュリティ人材」とはどういった人材なのかについてカテゴライズを行い、
3. その人材カテゴリごとに、
  - ・その人材カテゴリの現状(「質」、「量」など)をどう評価するのか。
  - ・どのような形で育成・確保(供給)がなされているのか(流通モデルの整理)。について検討を行い、それぞれの課題について、必要な対応策を検討することとしてはどうか。
4. 最終的に、人材カテゴリごとに整理された対応策を横断的に俯瞰し、例えば、
  - ・政府機関、企業など情報セキュリティ対策を実施する組織において必要となる対応策
  - ・高等教育機関や資格制度を初めとする育成プログラムの在り方といった形で、対策をまとめることが適当ではないか。

## 「情報セキュリティ人材」のカテゴリについて

我が国全体の情報セキュリティ対策を支える上で必要となる「情報セキュリティ人材」とは、  
どういった人材か。

例えば、下記のような人材が考えられるのではないか。

我が国を代表し、世界をリードする高度・先進的な情報セキュリティ技術の研究開発者

セキュリティ・プロバイダ(Sier、製品ベンダ、コンサル・監査企業等)における人材

ア) 顧客企業に対してセキュリティ製品・サービス・ソリューション等を提供する人材

組織(行政機関(政府・地方公共団体)や企業)において情報セキュリティ対策を実施する人材

ア) 幹部(各省幹部・首長や経営者)

イ) 組織内における情報セキュリティ関係者(CISOや情報セキュリティ担当者 など)

ウ) 一般職員

### ア) 高度・先進的な情報セキュリティ技術の研究開発者の現状について、どのように評価するか。

1. 我が国を代表し、世界をリードする情報セキュリティ技術の研究開発者の現状と、その育成パスをどのように評価するか。  
(例)  
大学院: 東京大学、大阪大学、筑波大学、東京工業大学、北陸先端科学技術大学院大学、奈良先端科学技術大学院大学、慶應義塾大学、中央大学 等  
民間企業: 大手通信企業やベンダーの研究所 等
2. 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、こうした研究者、技術者が安定的に育成され、供給されることが必要であることについて異論はないのではないか。  
(参考)  
技術戦略専門委員会報告書(2005年11月17日) <次ページ参照>
3. 他方で、こうした人材の育成は、資格制度の活用や、短期的な対策で実現されるとは考えにくく、我が国の技術開発全体の長期的視野に立ち、大学院や民間企業等の連携も含めた総合的な戦略の検討が必要ではないか。





## セキュリティ・プロバイダにおける人材について

ア) セキュリティ・プロバイダ(Sier、製品ベンダ、コンサル・監査企業等)における人材の現状について、どのように評価するか。

### 【顧客に対してセキュリティ製品・サービス・ソリューションを提供する人材】

1. 情報セキュリティを「売り」にしている企業において、顧客に対して情報セキュリティに関する製品やサービス、ソリューション等を提供する人材の現状について、どう評価するか。
2. こうした人材の「質」について、どのように評価するか。例えば、
  - ・顧客たる組織のニーズに合わせ、適正なスキルをもった人材を提供できているか。
  - ・「質」の向上が必要とした場合、規制・基準などによる強制的な能力の引き上げや、任意の資格制度を活用した平均的な能力の底上げなど、どのような方法が考えられるか。
3. こうした人材の「量」について、どのように評価するか。例えば、
  - ・今後、日本全国で情報セキュリティ対策が必要となることを見据えると、各地域においてセキュリティ製品・サービス・ソリューションを提供できる人材は十分に確保できているか。
  - ・「量」の拡大が必要とした場合、どのような形で労働力の転換を図ることが考えられるか。
4. こうした人材を育成することを目的とした現在の各種育成プログラムについて、どのように評価するか。  
(例) 社会人を対象とした高等教育機関における実践的プログラム、SE等を想定した資格制度 等

ア) 組織(行政機関(政府・地方公共団体)や企業)において情報セキュリティ対策を実施する人材の現状について、どのように評価するか。

### 【幹部(各省幹部・首長や経営者)】

1. 行政機関や企業における幹部の情報セキュリティ意識をどう評価するか。行政機関と民間企業において、差があるか。また、民間企業の中でも、大企業と中小企業において差があるか。
2. 幹部が意識すべき諸課題のうち、情報セキュリティ対策については、従来から対応が求められていた課題ではなく、特に近年急激にその必要性が高まったこと、技術的知識が求められることや、対策についても体系的な整理がなされてこなかったことなどの理由から、幹部の意識が高まりにくいという傾向があるということはないか。
3. また、「意識」のレベルについて、例えば、「知識として知っている」というレベルと、幹部として人事配置・予算の手当・体制の構築等組織的な対応までリーダーシップを発揮できているというレベルで考えた場合、現状はどのように評価されるのか。

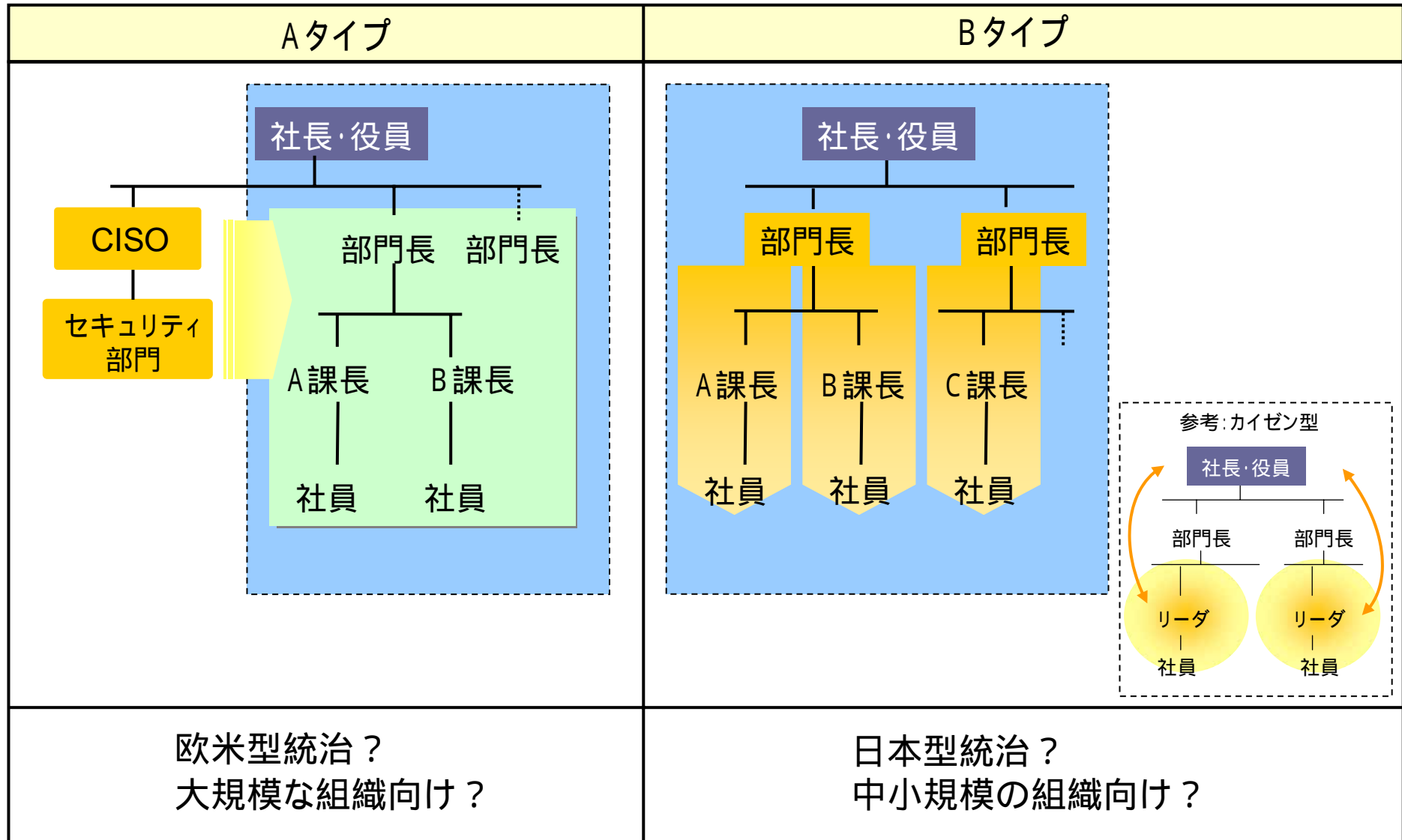


イ) 組織(行政機関(政府・地方公共団体)や企業)において情報セキュリティ対策を実施する人材の現状について、どのように評価するか。

### 【情報セキュリティ対策のための体制】

1. 組織において情報セキュリティ対策を徹底するために適当・可能な体制はどのようなものか。  
<次ページ参照>
2. 例えば、
  - 2～3年で人事異動が進む組織(政府など)
  - ある程度のキャリアパスの構築が可能な大企業
  - セキュリティのため(だけ)の人材確保・体制構築が容易ではない中小企業など、組織の性質や規模などに応じて、どのように考えることができるか。

# 組織における情報セキュリティ対策のための体制イメージ



イ) 組織(行政機関(政府・地方公共団体)や企業)において情報セキュリティ対策を実施する人材の現状について、どのように評価するか。

### 【「Aタイプ」体制におけるCISO・CISO補佐官(以下、「CISO等」という。)]】

1. 現在、CISO等として、どのような人材が配置されているか。その人材は、どのように育成・確保されているのか。  
(組織内部の人材を育成しているのか、外部から採用しているのか。あるいはCISOは内部人材とし、CISO補佐官は外部能力を活用しているのか。)
2. CISO等の育成・確保のためには、どのような育成プログラムが必要・適切か。内部育成と外部採用の場合で考え方が異なるのではないか。  
この点、CISO等を育成することを目的とした各種育成プログラムについて、どのように評価するか。  
(例) CISO等の育成プログラムを提供する高等教育機関、CISO等を想定した資格制度 等

### 【「Aタイプ」体制における情報セキュリティ担当部門の職員】

1. 行政機関や企業における情報セキュリティ担当部門の職員について、どのように評価するか。
2. 情報セキュリティ担当部門の職員の在り方(具体的に配置すべき人材)について、どのように考えるか。一般論として、情報システム担当者(部署)任せになってはいないか。
3. 内部人材と外部能力の活用について、どのように考えるか。
4. セキュリティ担当者を育成・確保するための育成プログラムについて、どのように評価するか。  
(例) 情報セキュリティ担当者を想定した資格制度 等

イ) 組織(行政機関(政府・地方公共団体)や企業)において情報セキュリティ対策を実施する人材の現状について、どのように評価するか。

### 【「Bタイプ」体制における各部門の情報セキュリティ担当職員】

1. 各部門において情報セキュリティ対策を実施する場合に、各部門の情報セキュリティ担当職員として、どのようなスキルが求められるか。
2. こうした職員が短期間で情報セキュリティの本質を理解し、最低限必要なスキルを身につけるためには、どのような育成プログラムが考えられるか。  
(例) 社会人を対象とした高等教育機関における実践的プログラム、担当者を想定した資格制度 等

ウ) 組織(行政機関(政府・地方公共団体)や企業)において情報セキュリティ対策を実施する人材の現状について、どのように評価するか。

### 【一般職員】

1. 一般職員の情報セキュリティ・リテラシについて、どのように評価するか。
2. 一般職員の情報セキュリティ・リテラシを向上させるため、現在、どのような対策が取られているか。また、今後、どのような対策を取ることが必要・適当か。
3. 例えば、企業等の組織が個々に研修等を行うことが適当か。ITが社会経済活動のあらゆる面に普及していることを考えれば、社会人になる以前の問題として取り組むことは考えられないか。