資料7

情報セキュリティ人材の育成方策について
(議論の方向性)

平成18年9月15日
内閣官房情報セキュリティセンター(NISC)

検討の進め方について（案）

1．「情報セキュリティ人材」として、（前回示したとおり、）例えば、
- 高度・先進的な情報セキュリティ技術の研究開発者
- 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企業等における人材
- 組織において、情報セキュリティ対策を実施する者（幹部、担当者、一般職員）

など、様々な人材が考えられる。

また、人材の「育成」方法としても、
- 高度な研究の実施
- 理論体系の理解
- 実習等による技能の習得
- 周知啓発等による意識の向上

など、様々な手段が考えられる。

2．したがって、前回示したとおり、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」についてカテゴライズを行い、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、それぞれの課題に対して必要な対応策を検討することとしてはどうか。

3．必要な対応策の検討に当たっては、上記のとおり、「育成」方法には様々な手段があることを踏まえ、適切な対応策を検討するべきではないか。

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

「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。

1．育成方策を検討すべき「情報セキュリティ人材」のカテゴリとしては、下記のような人材カテゴリが考えられるのではないか（次頁の図を参照）。

①　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

→次頁の　　部分

②　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）において、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者

→同　　部分

③　組織（政府、重要インフラ、企業等）において、情報セキュリティ対策を実施する者

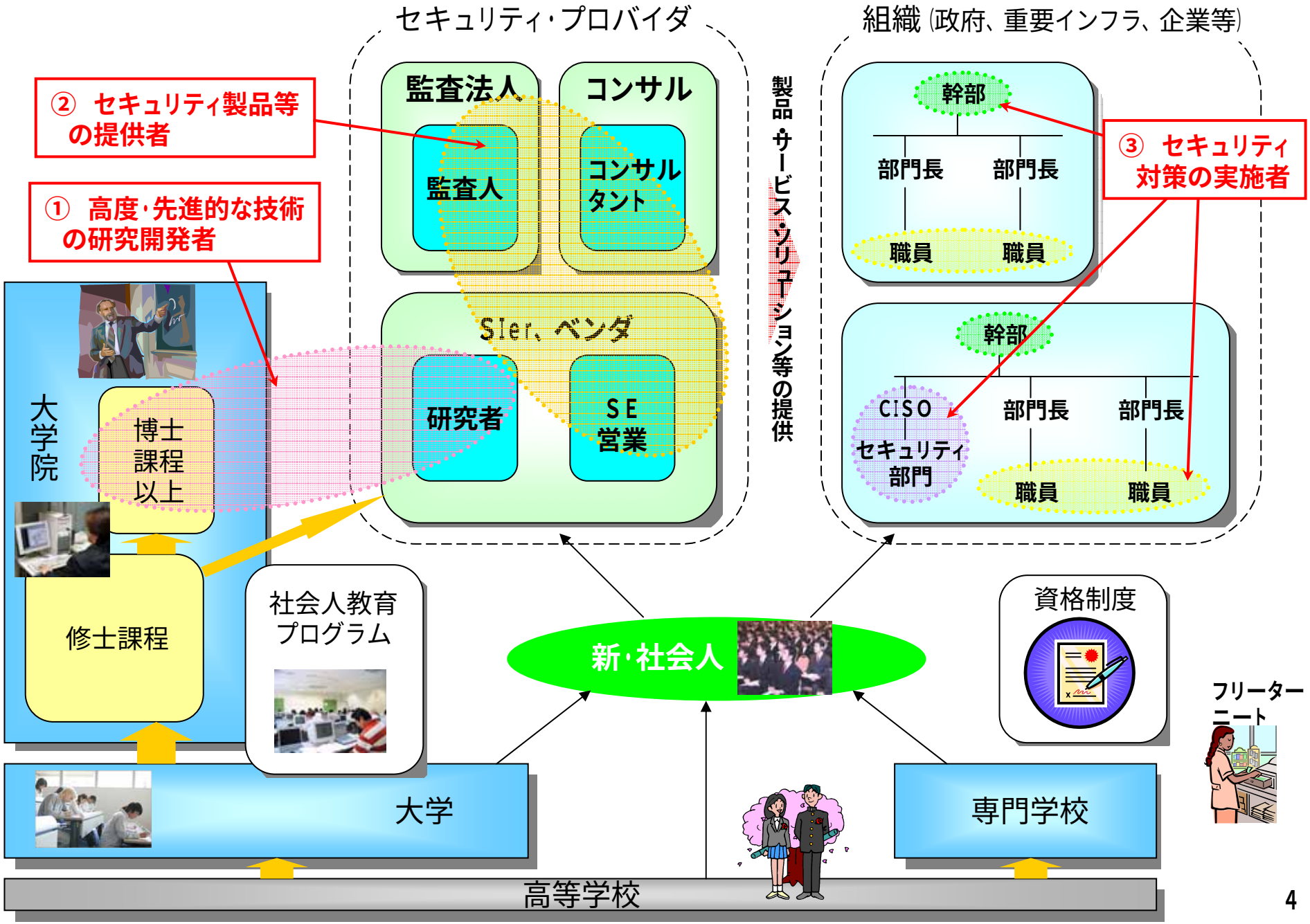
ア）　幹部（各省幹部・首長や経営者）　→同　　部分

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等）　→同　　部分

ウ）　一般職員　→同　　部分

2．その他、カテゴリとして大きく捉えるべき人材はあるか。

育成方策を検討すべき「情報セキュリティ人材」のカテゴリについて（イメージ）



①高度･先進的な技術の研究開発者について

高度・先進的な情報セキュリティ技術の研究開発者の育成メカニズム

主なスキル育成パス

セキュリティ・プロバイダ

監査法人

監査人

コンサル

コンサルタント

SIer、ベンダ

研究者

SE
営業

製品・サービス・ソリューション等の提供

組織（政府、重要インフラ、企業等）

幹部

部門長　部門長

職員　職員

幹部

CISO　部門長　部門長

セキュリティ部門

職員　職員

① 高度・先進的な技術の研究開発者

大学院

博士課程以上

修士課程

社会人教育プログラム

新・社会人

資格制度

フリーター
ニート

大学

専門学校

高等学校

高度・先進的な情報セキュリティ技術の研究開発者について

① 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．現在、こうした人材は、工学系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、企業の研究所等に就職して研究を続ける、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はないか（前頁の図を参照）。

（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。

3．　他方で、こうした人材の育成は、職場でのＯＪＴや、資格制度･社会人教育プログラムといった短期的な対策で対応を論じることは無理であり、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はないか。

4．　この点、「第３期科学技術基本計画」（平成１８年３月２８日閣議決定）の分野別推進戦略（情報通信分野）において、「情報セキュリティ技術の高度化」が盛り込まれており、総合科学技術会議や文部科学省のイニシアティブによる積極的な政策展開が期待されるところ、「研究機関」としての大学院等の高等教育機関への支援策の必要性やその具体策など、本委員会として提言することはあるか。

②セキュリティ製品等の提供者について

セキュリティ製品等の提供者の育成メカニズム（イメージ）

主なスキル育成パス

② セキュリティ製品等の提供者

セキュリティ・プロバイダ

監査法人

コンサル

監査人

コンサルタント

Sier、ベンダ

研究者

SE 営業

製品・サービス・ソリューション等の提供

組織（政府、重要インフラ、企業等）

幹部

部門長　部門長

職員　職員

幹部

CISO　部門長　部門長

セキュリティ部門

職員　職員

大学院

博士課程以上

修士課程

社会人教育プログラム

新・社会人

資格制度

フリーター

ニート

大学

専門学校

高等学校

② 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。

1．現在、こうした人材は、主に、
① 顧客に製品・サービス・ソリューション等を提供する業務の中で、ＯＪＴ的にスキルを習得する
② 大学や民間の実践的な社会人教育プログラムによるスキルを習得する
③ 資格取得によってスキルを習得する
といった形により育成されているのが現状ではないか（前頁の図を参照）。

2． まず、SIerやベンダーなど、主に「IT」や「技術」を売りするセキュリティ・プロバイダにおける、ＳＥなどの人材を育成する上での課題は何か。

① 例えば、現在は、アプリケーションプログラムにおけるセキュリティ配慮のレベルに開きがあり、情報システムの全体的な信頼性確保という観点からは、セキュリティ専門のＳＥだけでなく、アプリケーションを開発するＳＥが広くセキュア・プログラミングなどの技法について理解するような方策について検討する必要があるのではないか。

② また、情報システムの品質確保という観点から、ＳＥ等の人材に求めるべきことはあるか。
例えば建築士のように、法律による規制を導入することにより、人材の質の向上が図られるのではないかといった意見もあるが、以下のような点を踏まえ、どう考えるか。
・業界における開発プロセスの標準化が遅れていること。
・ITを活用する上での大きな規制強化となり、社会全体としてのコストがかかること。
・技術革新が激しい中で、行政が適正な規制の運用をできるか疑問なしとしないこと。
・そもそも、本委員会の目的である「人材育成」を図るために規制を導入するということ自体、疑問なしとしないこと。

セキュリティ製品等の提供者について

③　また、こうした人材に係る各種育成プログラムについてどのように評価するか。

（関連すると思われる主な育成プログラム）

高等教育機関：中央大学（情報セキュリティ・情報保証　人材育成拠点）
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）
情報セキュリティ大学院大学、カーネギーメロン大学日本校　等

その他の教育機関：横須賀テレコムリサーチパーク、ひょうご情報教育機構、ソフトピアジャパン　等

資格制度：テクニカル・エンジニア（情報セキュリティ）
NISM（サーバセキュリティ実践、不正アクセス監視実践）
CSPM（Technical）
CISSP
GIACs（GCFW、GCIA、GCIH、GCWN、GCUX、GSNA、GCFA）　等

④　例えば、以下のような論点を踏まえ、メリット・デメリットや有効な活用方策についてどう考えるか。
・特に、上記①の論点から見た場合、アプリケーションを開発するＳＥ等のセキュア・プログラミングへの理解度を保証する資格等はあるか。
・教育機関については、社会人に配慮した週末・夜間のみ、あるいは数日間程度の短期間のみといったものから、一年から二年に渡って通学が必要となるものがあるが、どう評価するか。
・資格制度の中には、実機を用いた実習等があるものとないもの、更新制があるものとないものがあるが、どう評価するか。　等

セキュリティ製品等の提供者について

3． 次に、コンサルティング企業や監査企業など、主に「マネジメント」や「監査」を売りにするセキュリティ・プロバイダにおける、コンサルタントや監査人などの人材を育成する上での課題は何か。

① こうした人材に係る各種育成プログラムについてどのように評価するか。

（関連すると思われる主な育成プログラム）

高等教育機関：情報セキュリティ大学院大学、カーネギーメロン大学日本校　等

その他教育機関：横須賀テレコムリサーチパーク、ひょうご情報教育機構、ソフトピアジャパン　等

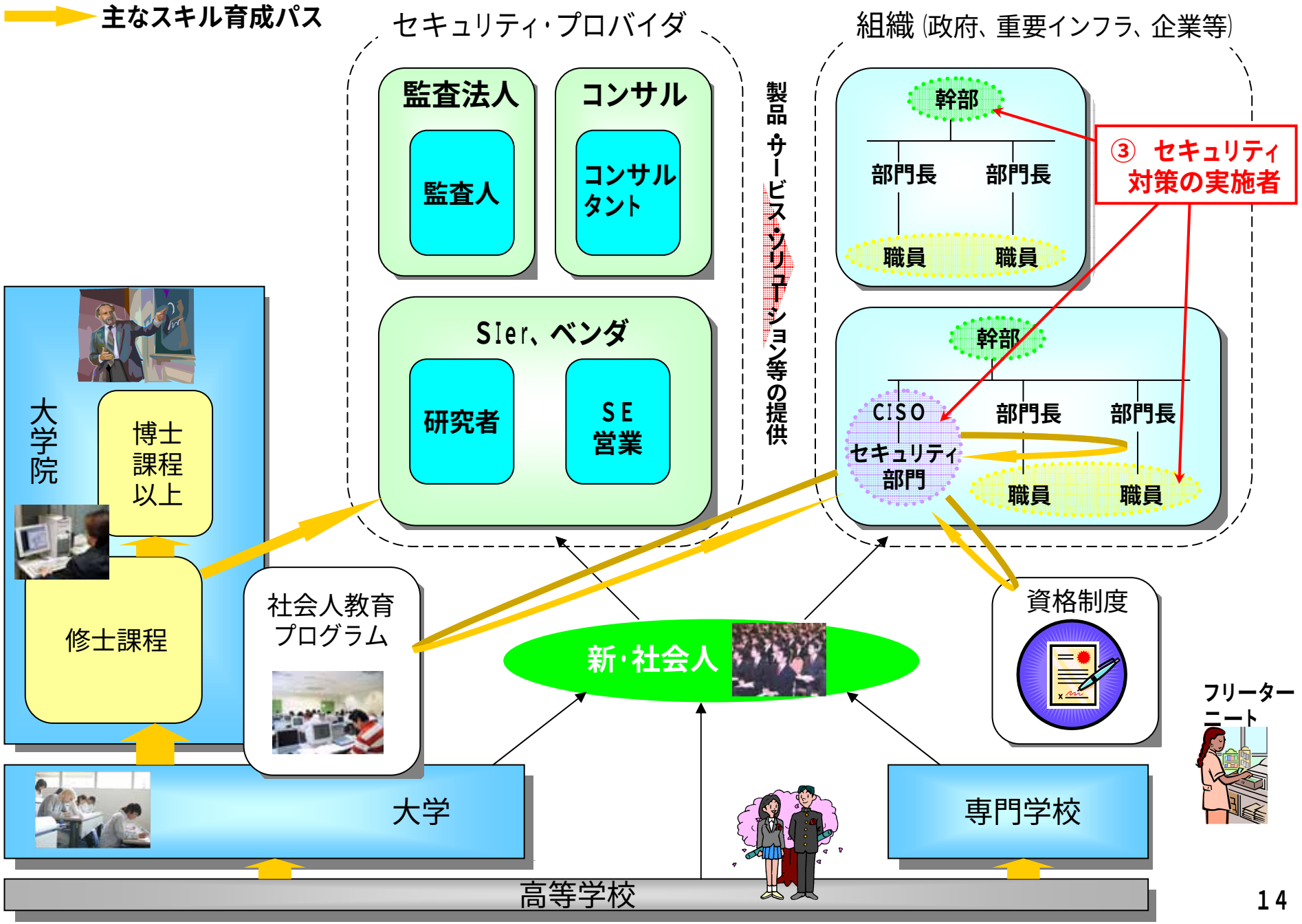
資格制度：情報セキュリティアドミニストレータ
NISM（セキュリティポリシー実践、セキュリティ監査実践）
CSPM（Management）
CISSP
CISM、CISA
CAISs（CAIS-Lead Auditor、CAIS-Auditor、CAIS-Assistant、CAIS-Associate）
GIACs（GSEC、GISF、GSAE、G7799、GSLC、GCSC、SANS+S、GSIP）　等

② 例えば、以下のような論点を踏まえ、メリット・デメリットや有効な活用方策についてどう考えるか。
・教育機関については、社会人に配慮した週末・夜間のみ、あるいは数日間程度の短期間のみといったものから、一年から二年に渡って通学が必要となるものがあるが、どう評価するか。
・資格制度の中には、演習等があるものとないもの、実務経験を問うものがあるものとないもの、更新制があるものとないものがあるが、どう評価するか。　等

4． 情報セキュリティの製品・サービス・ソリューション等を提供する人材の「量」についてどう評価するか。
・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、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」の確保が必要とした場合、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。

③セキュリティ対策の実施者について

セキュリティ対策を実施する者の育成メカニズム（イメージ）



セキュリティ対策の実施者（幹部）について

③ 組織（政府、重要インフラ、企業等）において情報セキュリティ対策を実施する者のうち、幹部の現状について、どのように評価するか。

1．**幹部については**、情報セキュリティの観点のみならず、組織のリーダーとしての資質、企業価値の最大化等の観点から選ばれるものであり、情報セキュリティ対策を実施する者としての「育成」としては、**その意識付けを行うというのが本筋ではないか**。

2．この点、日本経団連の企業に行ったアンケートの結果を見ると、
① 情報セキュリティポリシーの策定率：９１％
② 社長・役員クラスのＣＩＳＯの配置：６６％
③ 担当者（担当部門）の設置：７９％、そのうち役職の権限を越えた枠組みの付与：８２％（全体の６５％）
など、情報セキュリティ対策が進んでいるところを見ると、**企業において、情報セキュリティ対策に「着手する」というレベルでの対処は進みつつある**と言える。
政府機関においても、「政府機関統一基準」が決定されたことに伴い、省庁ごとのセキュリティポリシーの制定、最高情報セキュリティ責任者（ＣＩＳＯ）、最高情報セキュリティアドバイザー（ＣＩＳＯ補佐）の設置とこれに基づいた情報セキュリティ**対策の実施が進められているところ**である。

3．**ただ、他方で**、同アンケートによれば、
① ＣＩＳＯ補佐は情報システム部門の担当者が兼務：５１％
② 不足していると感じる人材の分野・能力：「とにかく全般」３３％、「マネジメント」４６％、「法制度」３０％
など、現状においては、**情報システム部門等に依存している割合が高く、マネジメントの観点からのセキュリティ対策の人材の育成・確保・配置が進んでいない**と推察される。
また、ＣＩＳＯやＣＩＳＯ補佐が兼務である場合に、当該業務を担当することに追加的処遇を与えている企業は一社もなく、いわばリスクに対応した適切な体制の構築や人的処遇もできているとは言えない状況とも考えられる。

セキュリティ対策の実施者（幹部）について

4．また、政府機関における実態調査においては、情報セキュリティに関する意識の現状について、「情報セキュリティに関する業務に従事している者のみ意識が高い」の回答が企業に比べて高く、幹部を含めた組織全体への意識向上が民間企業ほどまでに図られていないと懸念される。

5．このため、我が国全体の情報セキュリティ対策を着実に推進するに当たっては、各省庁の幹部や会社社長などの意識向上を図ることが必要であるが、他方で、こうした層の人材が、情報セキュリティの理論体系や技術要素などまで理解する必要はなく、主には、

・組織として、情報セキュリティに関するどのような「リスク」があるのか

・そのリスクを最小化するには、単に情報システム部門に任せただけでは足りず、例えば、
　ー総務・機密管理・人事部門等と一体となった組織の構築
　ー組織横断的な権限の付与
　ー新たな課題についての知識・技能を得るための職員の育成　など
　に、トップ・ガバナンスとして取り組む必要があること

などを認識させることが、必要なのではないか。

6．こうした幹部への意識向上を図るためには、どのような枠組みが必要と考えられるか。
（論点の例）
・基本は、各組織のリスク及びガバナンスの問題なので、各組織の中で分析・説明が行われるべき問題。
・政府機関に対するＮＩＳＣの関わり方
・経済団体や業界団体等におけるトップ・セミナー　等

セキュリティ対策の実施者（情報セキュリティの担当者）について

③ 組織（政府、重要インフラ、企業等）において情報セキュリティ対策を実施する者のうち、情報セキュリティの担当者（CISO、担当者等）の現状について、どのように評価するか。

1．政府機関における情報セキュリティ対策のための体制の在り方、人材育成方策についてどのように考えるか。

2．一般に情報セキュリティを確保するためには、組織横断的な権限を有する専任のCISOやセキュリティ担当部門を設置することが望ましいと言われるが、実際に設置することが適当・必要かどうか、また、そうした職員をどういった形で確保するかといった点については、各政府機関の
・責務
・規模、体制
などによって、考え方が異なってくるのではないか。
（例）中央省庁と地方支分部局、部隊活動を行う組織と一般の行政組織、機微な情報を扱う機関とその他の機関　等

3．また、人材の状況について見ると、政府機関実態調査の結果、概ね以下のとおりであった。
・4割程度の省庁が情報セキュリティの専任職員を置いており、その業務としては、マネジメント、監査などの回答が多く、職員は省内調整等に比較的重点を置いていることがうかがえる。
・他方、約半数の省庁で外注要員も活用しており、セキュリティの運用・緊急時対応、アプリケーション・ネットワークセキュリティなどの活用が多く、技術的な業務については外部への依存度が高い。
・育成方策としては「OJT」、確保方策としては「外注」が多かった。
・求められる人材イメージとしては、「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当たって、利用者と開発者間で情報セキュリティの面から検討や調整等を行う者」が多かった。

政府機関における情報セキュリティの担当者について

4．今後の方針については、以下のとおりであった。

・約3／4の省庁で人材の不足感があるものの、今後の方針は「全般的に確保」「特に決まっていない」など、人材の育成戦略が明確になっていない状況。

5．このため、政府全体として、情報セキュリティに係わる人材をどう育成するか、その枠組みについて早期に検討することが必要ではないか。

6．その際には、例えば、以下のような事項について配慮が必要ではないか。

・政府機関によって、あるべき体制や人材の育成・確保の在り方も異なる点。

・一般的に2～3年で人事異動が行われ、情報セキュリティ担当としてのキャリアパスを構築することが困難な点。

・総務省行政管理局がこれまでに行ってきている「情報システム統一研修」との連携・調整。

・既に独自の職員訓練プログラムを持っている組織における、既存の訓練機会の活用・連携。

・各省庁の人材育成に関するＮＩＳＣの関わり方　等

セキュリティ対策の実施者（情報セキュリティの担当者）について

③ 組織（政府、重要インフラ、企業等）において情報セキュリティ対策を実施する者のうち、情報セキュリティの担当者（CISO、担当者等）の現状について、どのように評価するか。

1．次に、民間部門における情報セキュリティ対策のための体制の在り方、人材育成方策についてどのように考えるか。

2．体制の在り方について、一般に情報セキュリティを確保するためには、組織横断的な権限を有する専任のCISOやセキュリティ担当部門を置くことが望ましいと言われるが、例えば、民間企業についても、
・電子商取引等により一般個人の情報を多く取り扱う企業と、小売りを行わない製造業等の企業
・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と、そうでない企業
などによって、考え方が異なってくるのではないか。

3．また、人材育成方策について、日本経団連のアンケートの結果、民間企業においては、情報セキュリティ人材を確保するため、「内部人材の育成」による意向が強い。
・「育成するための方策」・・・OJT54%、社内研修41%、社外研修41%
←→外部から「確保するための方策」・・・「行っていない」75%
・今後の方針・・・「社内の既存の人材の育成」86%、←→「社外の人材を採用」16%
・人材派遣会社からのヒアリングでも、セキュリティに関する派遣等の活用は少ない模様。

4．その上で、アンケートでは、企業が抱える課題として以下のような課題が挙げられている。
・「費用対効果が分からない」38%、「社内にふさわしい人材がいても配置できない」41%、
「社内の業務に精通していなければ情報セキュリティは困難」34% など
・不足していると感じる人材の分野・能力：「とにかく全般」33%、「マネジメント」46%、「法制度」30%

民間部門における情報セキュリティの担当者について

5．上記を踏まえると、情報セキュリティという性質上、基本的に企業は内部人材の育成によってセキュリティ担当者を確保しようと考えているが、現時点では情報システム担当に依存している面が多く、組織全体のリスク・マネジメントとしての体制構築までに至っているとは言い難い状況。

6．こうした中で、CISOや担当部署を設けて対策を実施すべき企業においては、どのような人材の育成方策が必要・適当か。

7．また、そこまで対策が必要ではないと考えられる企業においては、どのような人材の育成方策が必要・適当か。

8．重要インフラ企業について、どのように考えるか。行動計画や「安全基準等策定に当たっての指針」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言及されているが、どのように取り組むべきか。
例えば、個々の職員のスキルという面から見て、対応を求めるべきことがあるか。

9．こうした人材に係る各種育成プログラムについて、どう評価するか。

（関連すると思われる主な育成プログラム）

高等教育機関：情報セキュリティ大学院大学、カーネギーメロン大学日本校　等

その他教育機関：横須賀テレコムリサーチパーク、ひょうご情報教育機構、ソフトピアジャパン　等

資格制度：情報セキュリティアドミニストレータ
NISM（セキュリティポリシー実践）
CSBM、CSPM（Management）
CISSP
CISM、CISA、CAISs、
GIACs（GSEC、GISF、GSLC、GCSC、SANS+S、GSIP）等

セキュリティ対策の実施者（情報セキュリティ担当者）について

③ 組織（政府、重要インフラ、企業等）において情報セキュリティ対策を実施する者のうち、一般職員の現状について、どのように評価するか。

1．情報セキュリティ対策の実施に当たっては、セキュリティ・プロバイダによる適正な製品・サービスの提供や、組織における適切なセキュリティ管理体制も必要であるが、他方で、営業やサポートなども含め、**ITやセキュリティ以外の業務に携わる全ての職員における対策能力の向上が不可欠**ではないか。

2．事務局がヒアリングを行った人材派遣会社の例によると、IT業務か如何に係わらず、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り、言わば、**「社会人としてのマナー・常識」になりつつある**とも考えられるのではないか。

3．この点、個人情報保護法の施行などに伴って一般職員の意識も向上しつつあると考えられるが、全ての職員に対して、具体的なリスクと自らの責任、さらにはそのために必要となる手順等について効率的に理解を浸透させるため、政府機関や各企業においては、**社内・社外の研修プログラム等を活用しつつ、一般職員向けの情報セキュリティ・リテラシ教育を進めることが求められる**のではないか。
　具体的な教育に当たっては、一般職員の平常業務の遂行に当たって過度な負担とならないよう配慮をしつつも、計画的な教育が浸透するよう、各組織が保有する情報システムの重要度や、取り扱う情報の重要性などに応じて、適切な教育計画を構築することが必要ではないか。

4．　他方、現在は個々の企業が個別に研修等により対応しているのが一般的であろうが、上記のとおり、「社会人としてのマナー・常識」になりつつあるとも考えられることを踏まえれば、次代の「一般職員」となるべき若者達に広くその意識を植え付けるという観点から、例えば、**高等学校の「情報教育」や、大学における一般教養的な教育の一環として、情報セキュリティについても教育することが適当ではないか。**

資格制度の体系化・教育プログラムの在り方について

資格制度の体系化・育成プログラムの在り方について

1．人材カテゴリごとに、主に関連する育成プログラムを整理すると、例えば、次頁の図（削除）のように体系化できるが、どう評価するか。

2．大学院等の高等教育機関に何を期待するか。「研究機関」としての大学院等と、社会人等をはじめとする「教育機関」としての大学院等とで、在り方について議論はあるか。

3．資格制度は、試験のみのものから数年間に渡る実務経験などを問うもの、実機等を用いた実習等があるものやないもの、テクニカル系とマネジメント系など、多岐にわたっているが、これら資格制度をどう評価するか。