

資料4

先導的情報セキュリティ人材
育成推進委員会(第1回)

H19.4.23

人材育成・資格制度体系化専門委員会 報告書概要

2007年2月2日

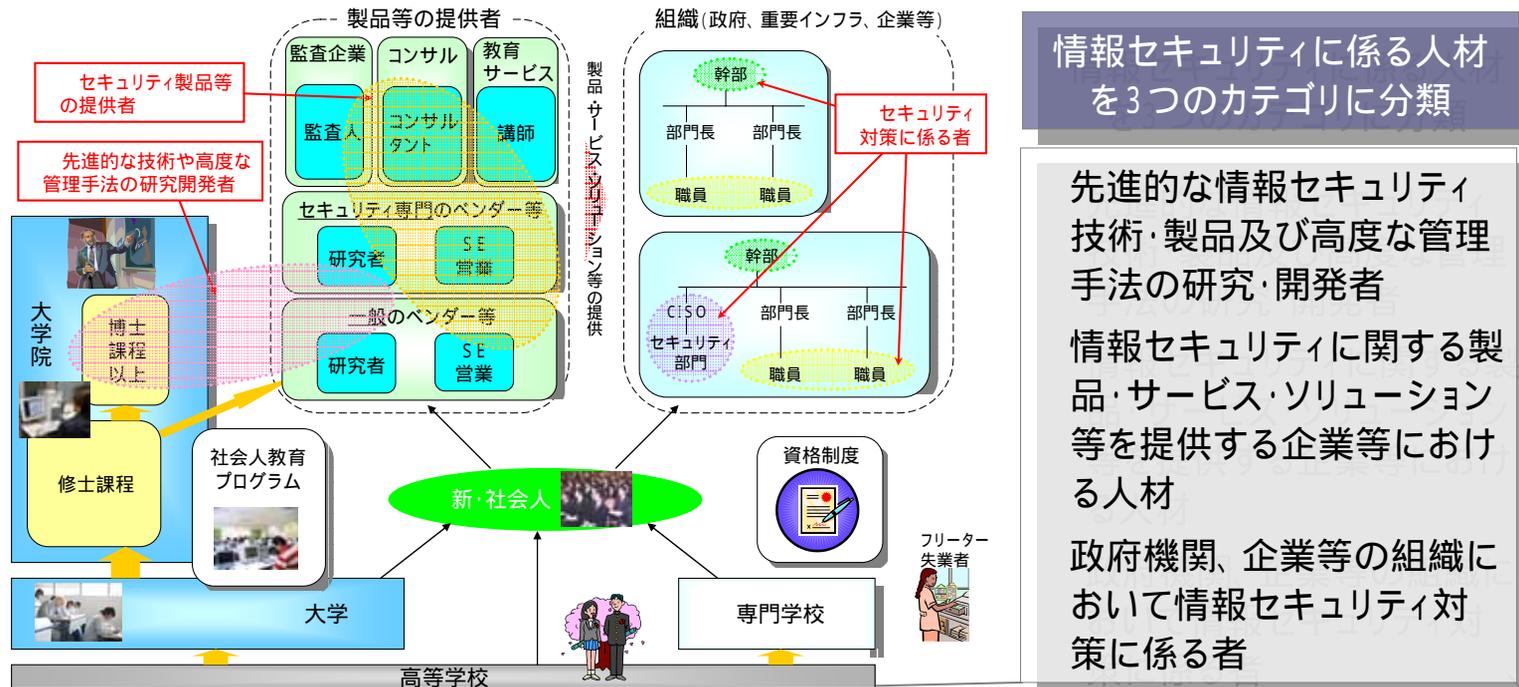
内閣官房情報セキュリティセンター(NISC)

本委員会における検討の進め方

本来、人材育成は長期的視野に立って、初等中等教育の現場における教育のあり方も含め、国家全体として育成方策のあり方を検討することが必要。

しかしながら、情報セキュリティ対策の向上は喫緊の課題であることから、我が国における**現有戦力の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・実行すべき課題**について、集中的な検討を実施し、提言

我が国全体の情報セキュリティ対策を推進していくためには、様々な社会経済活動の中で業務を実施するプレイヤー達の意識や能力の確保・向上が必要



各人材カテゴリごとに、現状・課題を分析し、必要な対応策の検討を実施

先進的な技術や高度な管理手法の研究開発者

- 研究者等の安定的な育成のためには、我が国全体の研究開発力・技術開発力の向上という**長期的視野からの積極的施策の展開**が必要。
 - 「第3期科学技術基本計画」の分野別推進戦略における「情報セキュリティ技術の高度化」
 - 「21世紀COEプログラム」の「グローバルCOEプログラム」への展開
- 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、**周辺領域における研究開発力の底上げと相互の連携**が重要。
 - 各大学における創意工夫に満ちた研究者育成方策の展開
 - 「イノベーション25戦略会議」や「総合科学技術会議」における議論

セキュリティ製品等の提供者

- ◆ **技術系の製品等を提供する企業等における人材**
 - **品質の管理**やそのために**必要な人材の育成**や**体制整備の徹底**、各種の教育プログラムを活用した**計画的な人材育成**が必要。
 - 人材の少ない地方においても、**地域の関係者による育成方策の検討**が必要。
- ◆ **管理系の製品等を提供する企業等における人材**
 - コンサルティングや監査サービス等に従事する者同士が、能力・知見を向上させるために**情報交換**を行い、**交流するためのコミュニティの形成**が望まれる。

政府機関・企業等においてセキュリティ対策に係る者

一般職員・社員

- セキュリティリテラシーの浸透
- 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

幹部

- 事業・業務内容、企業形態に応じたリスクの認識・理解

情報セキュリティ対策に係る者

- 組織横断的な対策を実施するCISO、担当者の配置(政府機関)
- 事業・業務内容、企業形態に応じたCISO、担当者の配置(企業等)
- 情報セキュリティの基礎や最新の技術動向の習得

政府機関における具体的育成への取り組み

- **政府統一的な教育プログラムの整備(「政府機関セキュリティ教育3点セット」)**
 - 「セキュリティリテラシー教育プログラム」(仮称) < 一般職員向け >
 - 「リスクマネジメント教育プログラム」(仮称) < 幹部職員向け >
 - 「情報セキュリティ担当者教育プログラム」(仮称) < セキュリティ担当者向け >

企業等における具体的育成への取り組み

- 全社員を対象としたセキュリティリテラシー習得プログラムの設定
- 幹部に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の実施
- 情報セキュリティ対策を担当する者の計画的な育成(OJT依存からの脱却)

大学院、大学、高等学校等の教育機関について

◆ 大学院等の高等教育機関

- 「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、柔軟かつ創造的な研究者育成方策を期待。
- 「教育機関」としての機能から、産業界等と連携を図りつつ、社会人教育プログラム等の提供を期待。

◆ 高等学校及び大学の一般教養課程

- 今や**情報セキュリティ**は「**社会人としてのマナー・常識**」。
 - 高等学校の教科「情報」の一層の充実
 - 大学の一般教養課程における情報教育 高校の内容を一層深めた教育の実施

資格制度に関する取組みと教育プログラムの体系化

- 官製の「**情報処理技術者試験**」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**適時適切に見直しが必要**。
- 資格制度に係る更新制・継続教育の必要性
- 人材の育成計画の目安となるよう、体系図を提示。(次頁)

各人材に求められる能力と各種教育プログラムの体系図

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
セキュリティテラシー									
所属する組織のセキュリティポリシー									
管理系分野	マネジメント技術	C	C	A	A	-	-	-	-
	リスク分析技術	C	C	A	A	-	-	-	-
	情報セキュリティポリシーの策定	C	C	A	A	-	-	-	-
	情報セキュリティ監査	C	C	B	A	-	-	-	-
	関連知識	C	C	A	A	-	-	-	-
	法令・規格	C	C	A	A	-	-	-	-
	事業継続経営(BCP/BCM)	C	C	A	A	-	-	-	-
	リスクコミュニケーション	C	C	A	C	-	-	-	-
	費用対効果	C	C	A	B	-	-	-	-
	人員計画	C	C	A	B	-	-	-	-
	教育・訓練	C	C	A	B	-	-	-	-
	物理セキュリティ	C	C	A	B	-	-	-	-
	調達管理	-	-	-	-	-	-	-	-
	プロジェクトマネジメント	A	B	B	C	-	-	-	-
セキュリティ運用	A	B	B	B	-	-	-	-	
技術系分野	セキュリティアーキテクチャ	A	B	B	B	-	-	-	-
	ネットワークインフラセキュリティ	A	B	B	C	-	-	-	-
	セキュアプログラミング技法	A	B	C	C	-	-	-	-
	セキュリティプロトコル	A	B	B	B	-	-	-	-
	認証	A	B	B	C	-	-	-	-
	アクセス制御	A	B	B	C	-	-	-	-
	PKI	A	B	B	C	-	-	-	-
	暗号	A	B	B	C	-	-	-	-
	電子署名	A	B	B	C	-	-	-	-
	不正コピー防止・電子透かし	A	B	B	C	-	-	-	-
	ファイアウォール	A	B	B	C	-	-	-	-
	侵入検知	A	B	B	C	-	-	-	-
	ウイルス	A	B	B	C	-	-	-	-
	不正アクセス手法	A	B	B	C	-	-	-	-
全般	A	B	B	C	-	-	-	-	
アプリケーションセキュリティ	Web	A	B	B	C	-	-	-	-
	電子メール	A	B	B	C	-	-	-	-
	DNS(Domain Name System)	A	B	B	C	-	-	-	-
OSセキュリティ	Unix, Linux	A	B	B	C	-	-	-	-
	Windows	A	B	B	C	-	-	-	-
	TrustedOS	A	B	B	C	-	-	-	-
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	-
		-	Y R P ソフトピア・Tec ひょうご	-	-	-	-	Y R P ソフトピア・Tec ひょうご	Y R P 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

(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

- 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
- 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
- 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/ty16/reports/skillmap/index.html>)を基に検討を実施した。

(注)「セキュリティテラシー」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。