

平成18年11月30日
内閣官房情報セキュリティセンター (NISC)

高度情報通信ネットワーク社会推進戦略本部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報告書(案)の
パブリックコメントの募集について**

1. 人材育成・資格制度体系化専門委員会について

人材育成・資格制度体系化専門委員会(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))は、情報セキュリティに関する人材の育成及び資格制度の体系化に係る事項について調査検討を行うために、情報セキュリティ政策会議(議長:内閣官房長官)の下に設置され、専門家・実務家を集め、本年8月30日から4回に渡って会合を開催し、検討を重ねてきました。(委員名簿については、別紙1をご参照下さい。)

本委員会における検討の成果として、「人材育成・資格制度体系化専門委員会報告書(案)」を取りまとめましたところ、本報告書案に対して広く意見を求めるべくパブリックコメントを募集することとなりましたので、本日、本報告書案を公表し、パブリックコメントの募集を開始します。

人材育成・資格制度体系化専門委員会におけるこれまでの検討の経緯については、(<http://www.nisc.go.jp/conference/seisaku/training/index.html>)をご参照下さい。

2. 人材育成・資格制度体系化専門委員会報告書(案)について

(1)「人材育成・資格制度体系化専門委員会報告書(案)」の全体像(別紙2参照)

本報告書案においては、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、企業等において情報セキュリティ対策の実施に係る人材
- 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いました。

(2)人材育成のための主な具体的方策

本報告書案に示された人材育成のための主な具体的方策は以下のとおりです。

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

- 長期的視野からの積極的施策の展開
 - ・「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
 - ・周辺領域も含めた研究開発力の底上げと相互の連携
- 先端的な人材の育成のあり方
 - ・「イノベーション25戦略会議」や「総合科学技術会議」での議論等への期待

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

- 技術系の製品等を提供する企業等において必要となる人材の育成方策
 - ・セキュリティ専門ベンダー等における人材の育成や体制の整備の徹底
 - ・一般のベンダー等の技術者に対し、セキュアプログラミング技法等最低限の情報セキュリティに関する能力を身に付けることを推進
 - ・産学連携の取組みを中心とした教育プログラムの充実
 - ・地域に密着したベンダー等の人材の育成に向けた各地域における検討
- 管理系の製品等を提供する企業等において必要となる人材の育成方策
 - ・知識・経験、最新の技術動向やニーズへの対応能力など幅広い能力を有する人材をバランスよく育成・確保
 - ・各民間団体の資格制度・研修や高等教育機関での教育課程等の活用
 - ・同業種の者同士のコミュニティの形成
 - ・体系的な教育プログラムの提供

政府機関、企業等において情報セキュリティ対策の実施に係る人材

- 政府機関において必要となる人材育成方策
 - ・政府統一的な教育プログラムの整備
 - 「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 >
 - ・特定府省庁において必要となる高度な能力を有する人材の確実な育成
- 企業等において必要となる人材の育成方策
 - ・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
 - ・OJTに頼らず各種の外部教育プログラムを適切に活用
 - ・情報セキュリティ担当者育成計画の策定

教育機関等に関する取組み

- 「21世紀 COE プログラム」等の活用に当たっての柔軟かつ創造的な提案
- 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
(教科「情報」の未履修問題に関する対応の検討)

資格制度に関する取組みと教育プログラムの体系化

- 官民の適切な役割分担という観点に立った情報処理技術者試験の見直し
- 最新の技術動向についての知識や技能に関する更新制・継続教育の枠組みの必要性
- 人材の育成計画の目安となる必要な能力と各種教育プログラムに関する体系図の提示(別紙3参照)

3. パブリックコメントの募集について

本報告書案の内容は、広く意見を募集すべきものであることから、本専門委員会の第4回会合においてパブリックコメントの募集を行うことが決定されました。

パブリックコメントの募集は本日より約1ヶ月間受け付けます。

パブリックコメントの募集は、内閣官房情報セキュリティセンター(NISC)ホームページ(<http://www.nisc.go.jp/>)において実施します。

【本件に関する問い合わせ先】

内閣官房情報セキュリティセンター

川野参事官補佐、川口主査

電話 03-3581-3768(センター代表)

「情報セキュリティ政策会議」は、平成17年5月30日のIT戦略本部決定によって設置されました(<http://www.nisc.go.jp/press/pdf/050530seisaku-press.pdf>)。

人材育成・資格制度体系化専門委員会委員名簿

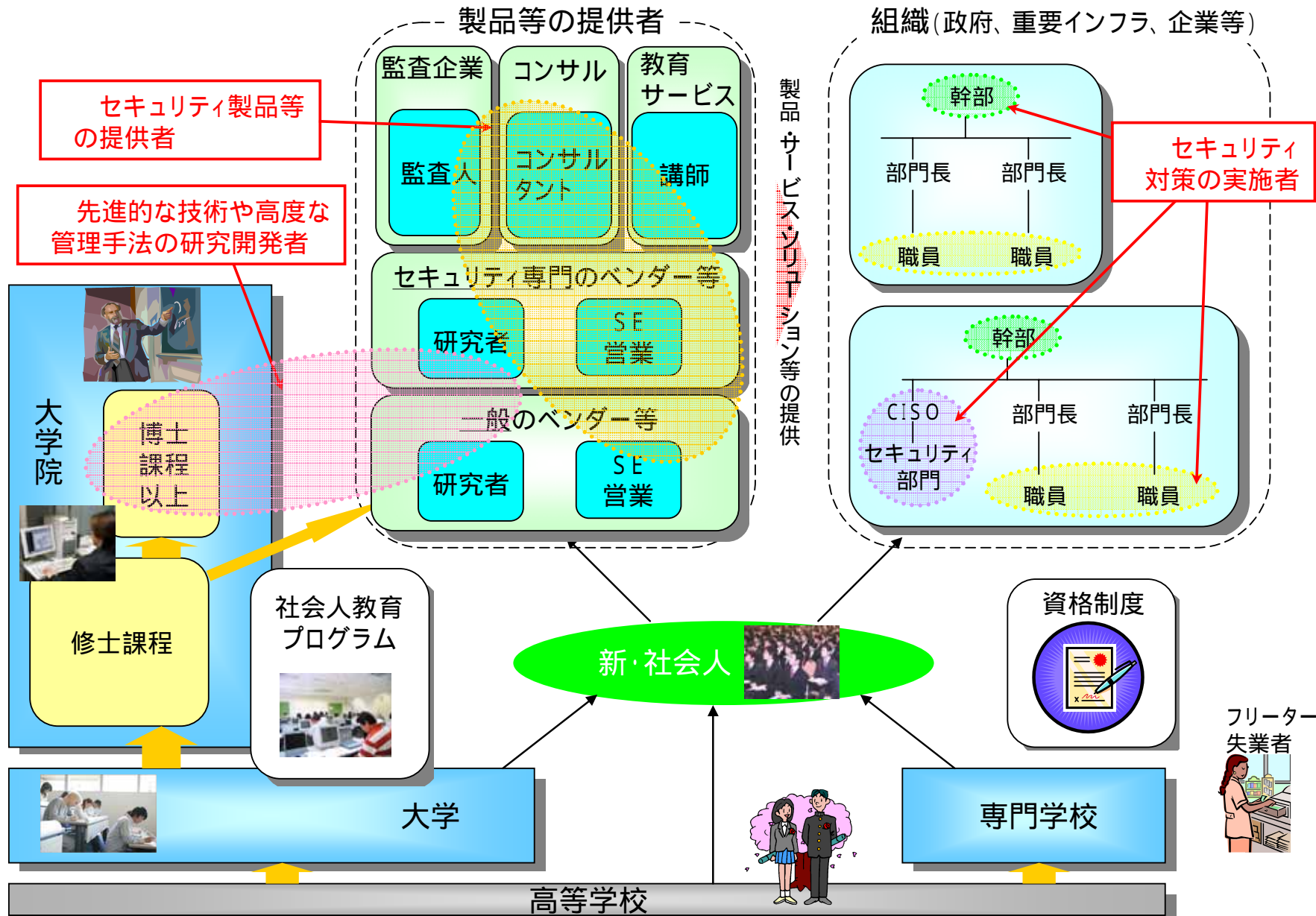
【委員長】

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助教授
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
笥 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

「人材育成・資格制度体系化専門委員会報告書(案)」における検討のイメージ



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の実施に係る人材			
		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	-	-	-	-
	ファイアーウォール	A	B	B	C	-	-	-	-
	ウイルス・侵入等対策技術	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	-	-	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の実施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
- 組織において情報セキュリティ対策を実施していく上で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。