平成 24 年度
内閣官房情報セキュリティセンター
委託調査

平成 24 年度

情報セキュリティ人材の育成に向けた検討

報告書

（要約版）

2013 年1月

株式会社 NTT データ経営研究所

1. 本調査・検討の概要

1.1. 背景と目的

本事業は、「情報セキュリティ人材育成プログラム[1] 」(2011 年7月8日情報セキュリティ政策会議決定)および「情報セキュリティ人材育成プログラムを踏まえた2012年度以降の当面の課題等について[2]」(2012年5月31日普及啓発・人材育成専門委員会取りまとめ)を踏まえ、情報セキュリティ人材の育成に関する情報を収集するものである。

本調査では、企業および大学に対してヒアリング等を行うことにより、情報セキュリティ人材の育成に関する課題、ニーズ、取り組み事例等を把握することを目的とする。

1.2. 調査内容

情報セキュリティ人材育成に関する課題、情報セキュリティ研究科等の設置・教育に関する企業のニーズ、情報セキュリティ教育に関する大学の教養課程・共通課程に対する企業のニーズ、情報セキュリティ教育に関するＭＢＡ又はＭＯＴ等に対する企業のニーズを把握するため、企業に対するヒアリング等を実施した。

教養課程・共通課程及び情報セキュリティ専門でない研究科において、情報セキュリティの授業を実施している事例、資格試験等を活用した授業を実施している事例、情報セキュリティに関する新たな学位の創設についての意向を把握するため、大学に対するヒアリング等を実施した。

こららの調査をとりまとめ、大学における情報セキュリティ教育の実施に資する大学向け啓発資料案を作成した。

本調査は、情報セキュリティ人材育成に幅広い知見を有する有識者からなる検討会を開始し、当該検討会において、調査結果の分析・検討等を行いつつ調査を進めた。

---

[1] 出典：http://www.nisc.go.jp/active/kihon/pdf/jinzai2011.pdf
[2] 出典：http://www.nisc.go.jp/active/kihon/pdf/jinzai_kadai2012_fix.pdf

2. 企業ニーズ等調査

2.1. 企業のニーズ等

企業のニーズ等は、情報セキュリティ人材タイプを６つに分類したうえで、現状及び課題と、その解決として大学へ求める要望についてＩＴユーザ企業１０社と情報セキュリティ事業を提供している企業１０社を訪問調査し、結果を取りまとめた。

(1) 調査対象　～情報セキュリティ人材の分類

本調査における情報セキュリティ人材の分類は、「情報セキュリティ人材育成プログラムを踏まえた 2012 年度以降の当面の課題等について」（2012 年 5 月 31 日普及啓発・人材育成専門委員会取りまとめ）の分類を踏まえて整理した。

「情報セキュリティ人材育成プログラムを踏まえた 2012 年度以降の当面の課題等について」においては、企業内人材を「企業等の情報セキュリティ担当者」、「情報セキュリティ産業の人材」、「先端的研究者・技術者」に分類されている。本調査においては、この整理を踏まえつつ、企業内におけるを人材配置状況を踏まえ、以下の６タイプに詳細化した。

タイプ１：企業の経営層の人材

情報セキュリティに係る責任者として、CSO（Chief Security Officer）や CISO(Chief Information Security Officer)などが想定される。

タイプ２：企業の総務部門等の人材

主な役割としては、セキュリティポリシの策定や情報セキュリティ監査、セキュリティマネジメントの推進等の担当者が想定される。

タイプ３：ユーザ人材

企業における情報システムの利用者

タイプ４：企業における情報システムの部門等の人材

社内の情報システムの開発・保守・運用の担当や技術的なセキュリティ対策を理解し、サイバー攻撃などの検知・監視またはインシデント対応等の担当者が想定される。

タイプ５：情報セキュリティサービスに関連する製品やサービスを提供する人材

セキュリティ関連製品・サービスの開発・提供等を行う担当者が想定される。

タイプ６：先端的研究者・技術者

企業のなかで先端的な研究や開発行う担当者が想定される。

(2) 企業のニーズ等のまとめ

企業のニーズ等は、情報セキュリティ人材タイプ毎の主な現状及び課題と、その解決として大学へ求める要望について以下の通りまとめた。

①全タイプ共通（タイプ３ユーザ含む）

現状及び課題	大学への要望
○情報セキュリティに関するモラルや作法は必須であるが、欠けている人が多い。（金融 A 社） ○PC やスマホ等の自分が使う IT 機器ぐらいは適切に管理すべきであるが、できない人が多い。（鉄道 D 社、情報通信 E 社、運輸 I 社） ○情報セキュリティに関するモラルや作法は、継続的に学習しなければ身につかない。（航空 C 社、宅配 J 社） ○あらゆる分野で、情報セキュリティに配慮した行動が求められている。専攻している分野に関連するセキュリティについては、大学時代に学習して欲しい。 （ベンダーL 社、R 社、セキュリティ関連 T 社）	【教養課程】 ○IT 及びインターネットの基本的な仕組みを理解したうえで、情報セキュリティモラル、情報セキュリティリテラシーを学べる講義を行って欲しい。最近のインシデント事例も取り上げて欲しい。（金融 A 社、航空 C 社、鉄道 D 社、情報通信 E 社、オフィス機器製造・販売 G 社、サービス業 H 社、宅配 J 社、ベンダーL 社, M 社、P 社、R 社、セキュリティ関連 T 社） 【専門課程】 ○文系理系に関係なく、専攻している分野に関連するセキュリティ問題を講義、ゼミ、ワークショップで取り上げて欲しい。（オフィス機器製造・販売 G 社、サービス業 H 社、ベンダー L 社、M 社、R 社、セキュリティ関連 N 社、T 社、有識者 X 氏）

②人材タイプ１　経営層

現状及び課題	大学への要望
○情報セキュリティ事故は経営に重大な影響を与えていることからもわかるように、情報セキュリティは極めて重要な経営課題である。(オフィス機器製造・販売 G 社、ベンダーM 社、セキュリティ関連 T 社) ○情報セキュリティ対策を実施するためには、人・物・金の適切な配分が必要であり、情報セキュリティ対策に対する経営層の理解は必要不可欠。 （オフィス機器製造・販売 G 社、ベンダーM 社、セキュリティ関連 T 社） ○情報セキュリティ対策について、業務と IT の両面から適切に判断できる人材が不足している。（金融 A 社）	【MBA・MOT】 ○情報セキュリティに関する法令・ガイドラインや技術知識等をバランス良く学べる講義や事例研究等により、企業経営における情報セキュリティ投資の必要性・価値を理解できるような教育を実施して欲しい。 (電気通信 B 社、鉄道 D 社、オフィス機器製造・販売 G 社、サービス業 H 社、宅配 J 社、セキュリティ関連 T 社)

③人材タイプ２　総務部門等の人材

現状及び課題	大学への要望
○大学等の専攻に関係なく、情報セキュリティポリシー策定、インシデント対応、情報セキュリティ監査等の業務を担当。そのような業務を行うためには、IT やセキュリティの基礎が必要。（金融 A 社、情報通信 E 社、宅配 J 社、ベンダーO 社） ○業務に根差した情報セキュリティポリシー策定やインシデント対応には、セキュリティ関連法制について体系的な基礎知識が必要。一方、情報セキュリティ関連法令は多岐にわたり、OJT や独学で習得することが困難。（金融 A 社、鉄道 D 社、情報通信 E 社）	【教養課程】 ○IT 及びインターネットの基本的な仕組みを理解したうえで、情報セキュリティモラル、情報セキュリティリテラシーを学べる講義を行って欲しい。最近のインシデント事例も取り上げて欲しい。（金融 A 社、航空 C 社、鉄道 D 社、情報通信 E 社、オフィス機器製造・販売 G 社、サービス業 H 社、ベンダーL 社、M 社、P 社、R 社、情報セキュリティ関連 T 社） 【専門課程】 ○情報セキュリティ関連法制について、体系的に学べる講義を実施して欲しい。 （金融 A 社、情報通信 E 社）

④人材タイプ４　情報システム部門等の人材

現状及び課題	大学への要望
○IT ユーザー企業であっても、情報セキュリティの専門家と対等に会話ができる情報セキュリティ人材が必要。（金融 A 社、情報セキュリティ関連 K 社、T 社） ○インシデント等に対応する組織（ＣＥＲＴ）に配属できる人材が、質と量の両面から不足している。（鉄道 D 社、ベンダーL 社、O 社） ○体力のない IT ユーザー企業では、社内で情報セキュリティ人材を育成するのが困難になりつつある。（航空 C 社、有識者 V 氏） ○OJT や独学で知識を身につけた情報セキュリティ担当者は、自らの知識に穴があることを懸念している。（航空 C 社、有識者 V 氏） ○セキュリティの技術は、知識だけでなく、現場で求められる技術を把握しながら、経験と共に体得する実践力が重要。（金融 A 社、ベンダーO 社） ○情報セキュリティのことしかやらない人材は処遇が難しいため、情報セキュリティ以外の業務にも対応できる順応性が必要である。 （金融 A 社、ベンダーL 社、P 社、R 社）	【専門課程（情報関係）】 ○基本的な技術知識を学んだ後に、体系的な情報セキュリティ教育を一通り行って欲しい。（航空 C 社、オフィス機器製造・販売 G 社、ベンダーL 社、M 社、情報セキュリティ関連 T 社） 【専門課程（セキュリティ）】 ○現場で求められる技術を把握するため、演習、インターンシップ、企業との共同研究などによる現場経験をさせて欲しい。（金融 A 社、ベンダーO 社、有識者 U 氏、V 氏、W 氏） ○情報セキュリティだけではなく、幅広く対応できる人材を育成して欲しい。（金融 A 社、鉄道 D 社、情報通信 E 社、情報セキュリティ関連 T 社）

⑤人材タイプ５　情報セキュリティサービスやソリューション等を提供する人材

現状及び課題	大学への要望
○高まるｻｲﾊﾞｰ脅威やｸﾗｳﾄﾞ・ｾｷｭﾘﾃｨなどの新しい環境に対応できる実践力をもった人材が不足。（ベンダーL 社） ○自動車、情報家電、複合機等の組込みｿﾌﾄ開発やﾌﾟﾗﾝﾄ等の制御系ｼｽﾃﾑ開発において、ｾｷｭﾘﾃｨ対策を検討できる人材が不足。（自動車関連 F 社、オフィス機器製造・販売 G 社、ベンダーO 社） ○OJT や独学で知識を身につけた情報ｾｷｭﾘﾃｨ担当者は、自らの知識に穴があることを懸念。（航空 C 社、有識者 V 氏） ○ｾｷｭﾘﾃｨの技術は、知識だけでなく、現場で求められる技術を把握しながら、経験と共に体得するという実践力が重要。 （金融 A 社、ベンダーO 社） ○情報ｾｷｭﾘﾃｨは幅広い技術領域に跨がるﾃｰﾏであるが、情報ｾｷｭﾘﾃｨの専門家は視野が狭いことが多い。（情報セキュリティ関連 S 社、Q 社） ○情報ｾｷｭﾘﾃｨのことしかやらない人材は処遇が難しいため、情報ｾｷｭﾘﾃｨ以外の業務にも対応できる順応性が必要。（金融 A 社、ベンダーL 社、P 社、R 社）	【専門課程（理工系）】 ○情報関係以外の専門課程においても、各専門分野に関連するセキュリティ問題を講義で取り上げて欲しい。（オフィス機器製造・販売 G 社、ベンダーL 社，M 社、セキュリティ関連 T 社） 【専門課程（情報関係課程）】 ○基本的な技術知識を学んだ後に、体系的な情報セキュリティ教育を一通り行って欲しい。（航空 C 社、オフィス機器製造・販売 G 社、ベンダーL 社，M 社、情報セキュリティ関連 T 社） ○組込みソフトのセキュリティ対策を理解するため、模擬体験型演習機の活用を検討して欲しい。（自動車関連 F 社） 【専門課程（セキュリティ）】 ○現場で求められる技術を把握するため、演習、インターンシップ、企業との共同研究などによる現場経験をさせて欲しい。 （金融 A 社、ベンダーO 社、有識者 U 氏、V 氏、W 氏） ○情報セキュリティだけではなく、幅広く対応できる人材を育成して欲しい。（鉄道 D 社、情報通信 E 社、情報セキュリティ関連 T 社）

⑥人材タイプ６　先端的研究者・技術者

現状及び課題	大学への要望
○クラッキング技術やその解析技術等を試しながら、セキュリティ技術の知識を高めることが重要。（電気通信 B 社）	【専門課程（セキュリティ）】 ○演習、企業との共同研究などにより、実践的な研究者を育成して欲しい。（金融 A 社、電気通信 B 社、ベンダーO 社、情報セキュリティ関連 Q 社、T 社、有識者 U 氏）
○特化した領域を研究していることから、応用が利かないという印象がある。 （ベンダーP 社、情報セキュリティ関連 S 社）	○社会実態に適したユースケースを想定できる人材を育成して欲しい。 （金融 A 社、ベンダーL 社、R 社）

3. 大学実態等調査

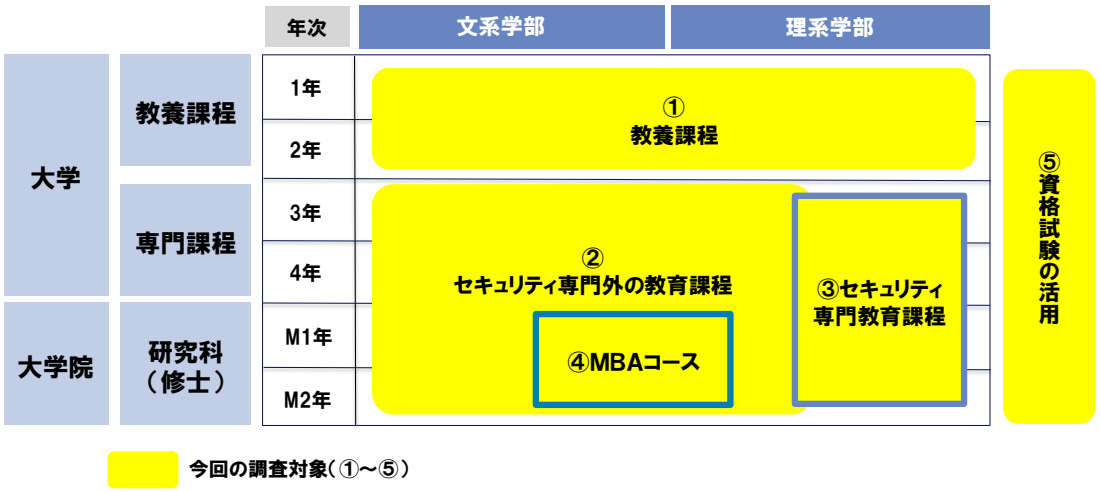
3.1. 調査対象

大学における実態等の調査を行うにあたり、まず、調査対象となる教育課程分類と調査対象選定の考え方を整理した。その整理を踏まえ、、調査項目について有益な情報収集が期待できる大学を調査先として選定した。

(1) 調査対象　～大学調査の対象となる教育課程

調査は、理系学部、文系学部に関わりなく、①教養課程、②セキュリティ専門外の教育課程、③セキュリティ専門教育課程、④MBA コースの４つの教育課程を対象に行う。この分類に加えて、情報セキュリティ資格試験を活用した取組みが見受けられることから、⑤資格試験の活用、も調査対象とした。

図表 1　調査対象の教育課程



(2) 大学の取り組み実態

各大学の情報セキュリティ教育への主な取組みを教育課程等の区分に分けて示す。

図表 2　調査先大学名

教育課程等の区分	大学・学部名	主な取り組みの特徴
①教養課程	山口大学 （全学部：文系・理系含む７学部）	必修科目として、「情報セキュリティ・モラル」（１単位）、「情報リテラシー演習」（１単位）を開講。
	東京電機大学 （情報環境学部）	必修科目として、「情報倫理」（２単位）を開講。
②セキュリティ専門外の教育課程	東京大学 （工学部）	３、４年生の選択科目として、「情報セキュリティ」（２単位）を開講。
	慶應義塾大学 （総合政策学部、環境情報学部）	４年生の選択科目として、「情報セキュリティ・マネジメント」（２単位）を開講。
	法政大学 （理工学部）	２年生の選択必修科目として、「セキュリティ概論」（２単位）、４年生の選択科目として「セキュアシステム開発」（２単位）を開講。
	公立はこだて未来大学大学院 （システム情報科学研究科）	選択科目として、「情報セキュリティ特論」（２単位）を開講。
	中央大学 （商学部）	３、４年生の選択科目として「情報セキュリティ論」（２単位）、「情報セキュリティ技術論」（２単位）を開講。
③セキュリティ専門教育課程	電気通信大学 （情報理工学部総合情報学科）	ネットワークセキュリティ、ソフトウェアセキュリティ、コンテンツセキュリティ等のセキュリティ関連講義を幅広く開講。
④MBA コース	中央大学 （戦略経営研究科）	選択科目として「ネットワーク時代のセキュリティとガバナンス」（２単位）を開講。
	青山学院大学 （国際マネジメント研究科）	選択科目として「情報セキュリティ」（２単位）を開講。

⑤資格試験の活用	沖縄大学	２年から４年の選択科目、「情報とシステムⅠ」、「情報とシステムⅡ」（各２単位）の講義を通じて、情報処理技術者試験のレベル１（入門レベル）にあたる「IT パスポート試験」のテクノロジ分野における出題範囲の多くを網羅した授業を展開。
	早稲田大学 （MNC[3]）	選択科目として「CompTIA Security+ 入門」（２単位）の講義を開講。
	青山学院大学	「IT パスポート試験」を活用した講座を開設。
	文教大学	「IT パスポート試験」を活用した講座を開設。
	東京家政大学	「IT パスポート試験」を活用した講座を開設。
	獨協大学	「IT パスポート試験」を活用した講座を開設。
	帝京大学	「IT パスポート試験」を活用した講義を開設。
	羽衣国際大学	「IT パスポート試験」を活用した講義を開設。
	奈良産業大学	「IT パスポート試験」を活用した講義を開設。
	長岡大学	「IT パスポート試験」を活用した講座を開設。

[3] MNC:メディアネットワークセンター、の略。早稲田大学では、MNC を設置し、全学共通副専攻（ソフトウェア学、等）習得に向けた履修科目を提供。

4. 大学向け啓発資料案

企業ニーズ等調査及び大学実態等調査を踏まえて、大学における情報セキュリティ教育の実施に資する大学向け啓発資料案を以下の基本的考え方に基づき作成した。

4.1. 啓発資料案作成における基本的考え方

啓発資料案は大学関係者が自校において情報セキュリティ教育に取組む重要性を認識することを促すと共に、新たに情報セキュリティ教育に取組む際の参考となりうる大学の事例を紹介することを目的として作成した。

このため、啓発資料案の読み手は、情報セキュリティ教育に取組んでいない大学のカリキュラム策定関係者である教職員を想定しており、学生向けの資料ではない。

また、情報セキュリティ教育に取組む重要性を認識することを促す資料であるため、具体的な情報セキュリティ講座の開設等のカリキュラム設計情報は提供しない。

4.2. 啓発資料案構成

啓発資料案の構成は、作成目的を踏まえ、以下の 6 章構成としている。

1 章　情報セキュリティを巡る状況
2 章　インシデント事例及びその影響
3 章　情報セキュリティ人材の重要性
4 章　企業における課題と大学への要望
5 章　大学における情報セキュリティ教育事例
6 章　まとめ

1 章では社会環境として、情報セキュリティに係る実態を統計的資料に基づいて紹介したうえで、2 章では、インシデント及びその発生による影響について事例を活用して紹介している。

3 章では、上記への対応として、情報セキュリティ人材が企業において重要であることを統計資料及び企業担当者へのインタビュー等から示している。

4 章では、企業調査及び検討会での議論を踏まえ、企業における課題及び大学への要望をまとめている。

5 章では、上記 4 章で整理した大学への要望を受ける形で、教育課程（教養課程、専門課程等）ごとに大学の情報セキュリティ教育事例を記載している。

最後に、啓発資料案で紹介した内容を踏まえ、6 章では、企業の情報セキュリティ人材確保に係る課題と大学の取組みを要約している。

4.3. 活用方法

啓発資料案は、読み手である大学関係者が情報セキュリティ教育の実施を検討する際の参考資料となることを意図している。

カリキュラムの設計に向けては、本資料の 5 章に掲載した大学の取組みが参考になる。

4.4. 啓発資料案

啓発資料「大学における情報セキュリティ教育の重要性について（案）」は、別紙として添付する。

以上