文部科学省

平成２８年度理工系プロフェッショナル教育推進委託事業

工学分野における理工系人材育成の在り方に関する調査研究

（情報セキュリティ人材育成に関する調査研究）

成果報告書

平成２９年　３月

学校法人岩崎学園

情報セキュリティ大学院大学

目　次

１．はじめに

１．１ 背景と目的

各大学の学部・大学院のカリキュラムがどの程度産業界のニーズと合っているのか、これらのカリキュラムのどのような点が問題となり得るのかなど、従来の理工系大学教育の問題点の検証等の実施が、理工系大学教育のシステム改革を達成する観点から課題となっている。本調査研究では、理工系大学教育のうち、近年特に早急な人材育成システムの確立が求められている情報セキュリティ分野に焦点を絞り、目指すべき情報セキュリティ人材像を検証・確定し、各大学での人材育成に資することを目的とする。また併せて、モデル・コア・カリキュラムを策定する。

政府機関や重要インフラ事業者等へのサイバー攻撃の激化、個人情報漏えい事案の多発化等、情報セキュリティの確保は国家課題となっており、高等教育機関における人材育成に大きな期待が寄せられている。大学における人材育成を推進していくために、国内外の教育の状況を調査するとともに、情報セキュリティに関する知識体系を整理し、教育現場が参照可能なモデル・コア・カリキュラムを開発する。

大学における各分野の社会的要請にこたえた人材養成のためのカリキュラムは、本来、各大学が独自の理念や特色に基づいて構築すべきものである。

情報科学や情報技術をはじめ科学技術の進歩は著しく、情報セキュリティの確保に貢献するいわゆる情報セキュリティ人材に求められる知識や技能は多様化、高度化しており、限られた大学教育の中で、これらの膨大で変化を続ける知識や技能等を網羅して修得することは困難である。加えて、常に最新の攻撃手法等に関する知識が更新される当該分野においては、学生は、大学を出た後も常に研鑽を続け、将来にわたって社会に貢献していくために必要な基本的な資質と能力を、大学・大学院における教育の段階で身につけておくことが必要となる。

このような状況を踏まえ、本調査研究によって開発するモデル・コア・カリキュラムは、教育内容を精選し、学生が学ぶべき知識や技能等の到達目標をわかりやすく提示することにより、教育内容とレベルを確保することを目指す。

すなわち、情報系をはじめとする理工系の大学・大学院において情報セキュリティに関する教育を実施するにあたって、現時点で学生が修得すべき基本となる教育内容を示すことにより、カリキュラム作成等の参考として提示するものである。

１．２ 調査方法

前述した目的を踏まえ、モデル・コア・カリキュラム策定の参考とするために以下の調査を実施した。

（１）高等教育機関における情報セキュリティに関する教育の現状に関する調査

現在行われている情報セキュリティ教育について、公表されている情報をもとにその定量的な把握を行うとともに、東北地域を例に実際の大学における情報セキュリティ教育の実施状況についてアンケート及びヒアリング調査を実施した。

（２）情報セキュリティに関する人材育成プログラムやカリキュラムの事例収集に関する調査

我が国で大学が関与している情報セキュリティに関する人材育成プログラムやコース、ならびにそれらを構成するカリキュラムについて調査を行った。それぞれの事例について、公表されている情報をもとに概要を整理した上で、うち 5 事例について、実施機関を対象としたヒアリング調査により詳細情報の把握を行った。

（３）諸外国の高等教育機関におけるセキュリティ人材の育成に関する調査

情報セキュリティに関する国としての人材育成の方針や考え方を調査した上で、情報セキュリティ分野で著名な大学等を対象として、特色ある人材育成の取組等に関する教育事例を収集する。なお、海外における情報セキュリティ人材の育成動向については、内閣官房情報セキュリティセンター（現内閣サイバーセキュリティセンター）によって実施された既存調査[1]が存在することから、同調査から把握可能な内容については重ねての調査を回避し、同調査に含まれないながらモデル・コア・カリキュラムの策定上有用と見込まれる事例を対象とした調査を行った。

（４）モデル・コア・カリキュラムに対する産業界の要望に関する調査

産業界において活躍する情報セキュリティ人材が身に付けておくべき知識・スキルとして、産業界においてこれまで検討及びとりまとめが行われ、公表されている内容についての整理・分析を行った。さらに、産業横断サイバーセキュリティ人材育成検討会の協力を得て、大学における情報セキュリティ教育への要望に関するアンケート調査の結果をご提供いただいた。

（５）情報セキュリティ人材育成推進のためのモデル・コア・カリキュラム策定および提言

（１）～（４）の調査結果を参考にするとともに、情報セキュリティ分野のさまざまな有識者の意見を反映させることにより、今後育成すべき情報セキュリティ人材像を検証・確定した。さ

[1] 平成 25 年度情報セキュリティに係る研究開発及び人材育成に関する調査・検討調査報告書
http://www.nisc.go.jp/inquiry/pdf/kenkyu_ikusei_honbun.pdf

らに、我が国の主に情報系の大学・大学院において効果的な人材育成を進めるために必要な学習内容と到達内容等を示すための、複数の区分からなるモデル・コア・カリキュラムを策定した。併せて、同モデル・コア・カリキュラムを教育現場において効果的に活用するための方法に関する提言を行った。

１．３　調査体制

本事業は文部科学省（高等教育局専門教育課）より情報セキュリティ大学院大学への委託により実施された。うち一部の調査については、東北大学、長崎県立大学、みずほ情報総研株式会社の三者への再委託により実施された。

また本調査の実施にあたっては、有識者の知見や大学等における教育の現状をモデル・コア・カリキュラムの策定に反映できるようにするため、次図のように産学の有識者で構成される有識者検討会及び４種類の作業部会からなる会議体を設置し、その調査結果をもとにモデル・コア・カリキュラムの策定を行うこととした。

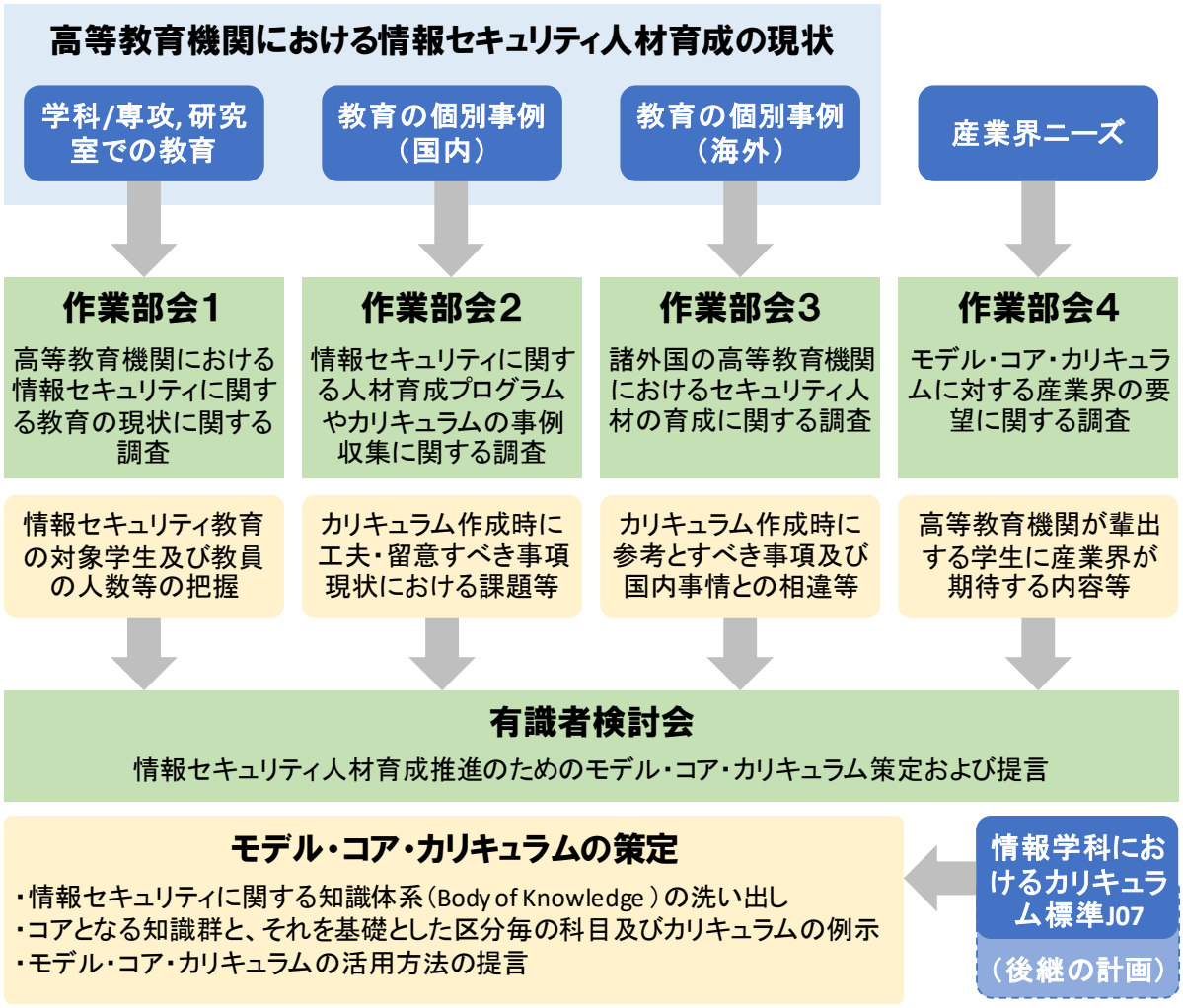

図　1　本調査の全体構成

有識者検討会及び４種類の作業部会の設置に際しては、それぞれの目的に応じて、専門的な知見を有する方にご協力をいただいた。それぞれの構成メンバーを示す。

表 1　有識者検討会委員

氏名	所属・役職等
川村　亨	産業横断サイバーセキュリティ人材育成検討会　事務局
後藤　厚宏	情報セキュリティ大学院大学情報セキュリティ研究科長・教授
砂原　秀樹	慶應義塾大学大学院　メディアデザイン研究科　教授（作業部会2主査）
曽根　秀昭	東北大学　サイバーサイエンスセンター長　教授（作業部会1主査）
田中　英彦◎	情報セキュリティ大学院大学学長・教授
平山　敏弘	特定非営利活動法人日本ネットワークセキュリティ協会教育部会長（作業部会4主査）
宮地　充子	大阪大学大学院　工学研究科　電気電子情報工学専攻　教授（作業部会3主査）

（敬称略・五十音順、◎＝座長）

表 2　作業部会１委員

氏名	所属・役職等
猪俣　敦夫	東京電機大学大学院　未来科学研究科　情報メディア学専攻　教授
下房地　毅	独立行政法人情報処理推進機構　イノベーション人材センター　グループリーダー
曽根　秀昭◎	東北大学　サイバーサイエンスセンター長　教授
高岡　詠子	上智大学　理工学部　情報理工学科　教授

（敬称略・五十音順、◎＝主査）

表 3　作業部会２

氏名	所属・役職等
大久保　隆夫	情報セキュリティ大学院大学　情報セキュリティ研究科　教授
岡村　耕二	九州大学　　情報基盤研究開発センター　先端ネットワーク研究部門　教授
加藤　雅彦	長崎県立大学　情報システム学部　情報セキュリティ学科　教授
砂原　秀樹◎	慶應義塾大学大学院　メディアデザイン研究科　教授
長谷川　長一	株式会社ラック　サイバーセキュリティ事業部　理事

（敬称略・五十音順、◎＝主査）

表 4　作業部会３

氏名	所属・役職等
辰己　丈夫	放送大学 教養学部 教授
橋本　正樹	情報セキュリティ大学院大学 情報セキュリティ研究科 准教授
藤川　和利	奈良先端科学技術大学院大学 総合情報基盤センター 教授
前田　典彦	株式会社カスペルスキー チーフセキュリティエヴァンゲリスト
宮地　充子◎	大阪大学大学院 工学研究科 電気電子情報工学専攻 教授

（敬称略・五十音順、◎＝主査）

表 5　作業部会４

氏名	所属・役職等
川村　亨	産業横断サイバーセキュリティ人材育成検討会 事務局
平山　敏弘◎	特定非営利活動法人日本ネットワークセキュリティ協会 教育部会長
藤本　正代	富士ゼロックス株式会社 パートナー
星　智恵	ネットワンシステムズ株式会社 市場開発本部 ソリューション・サービス企画室
持田　啓司	株式会社ラック FIoTech 本部 ビジネスアーキテクト

（敬称略・五十音順、◎＝主査）

２．情報セキュリティ教育の現状と社会的ニーズ

本章では、前述の目的を踏まえ、高等教育機関における情報セキュリティ教育の現状と、こうした教育に対する社会的ニーズに関して調査した結果を示す。

２．１ 我が国における情報セキュリティ教育の実施状況

モデル・コア・カリキュラムを検討するにあたり、対象となる高等教育機関における情報セキュリティ教育の現状を把握することを目的として、インターネットで公開されている情報に基づく実施状況の量的把握と、実施状況に関する深掘調査の 2 種類の調査を実施した。

２．１．１ 公開情報に基づく実施状況の量的把握

現在行われている情報セキュリティ教育について、公表されている情報をもとにその定量的な把握（教育の受講者数と教員数）を行った。このとき、実施されている教育には次の 3 種類があることから、それぞれに適した方法を用いて実施状況に関する調査を実施している。

(a) 情報セキュリティに関する専門的内容についての教育

学士課程であれば半年以上、修士課程であれば 1 年以上をかけて情報セキュリティ教育に関する専門的な教育を実施するものである。現在の我が国において、情報セキュリティに関するこうした教育は次の 3 種類の方法で受講者向けに実施されていると考えられる。

- 情報セキュリティを専門とする学科や専攻において、学位のためのプログラムを受講
- 情報セキュリティ分野を研究テーマとする研究室において、研究活動を行う過程で専門的な知識やスキルを習得
- enPiT security（SecCap）[2]のような情報セキュリティ分野を対象とする専門教育プログラムへの参加を通じて習得

そこで、こうした専門的内容に関する教育の受講者を把握するため、上記 3 種類の条件を満たす学生数を調査することとした。このうち、第 1 項目については情報セキュリティ大学院大学の情報セキュリティ専攻科の在籍者が該当するが、これらの在籍者は同時に第 2 項目の研究室にも配属されるため、重複を避けるために加算対象外とした。

(b) 情報セキュリティに関する専門的内容の入門的な教育

典型的な例としては、学士課程又は修士課程における半年間の講義 1 科目、またはその一部において、情報セキュリティに関する専門的知識（セキュリティの概念、脅威とその対策技術、暗号やネットワークセキュリティの背景知識など）の入門的内容を学ぶものである。(c)が日常生活上知っておくべき情報セキュリティに関する実用的な知識に重点を置いているのに対し、

[2] https://www.seccap.jp/

専門的知識につながる内容を含むことが特徴である。そのため、こうした科目は学士課程であれば入学 3 年目以降の受講が推奨されている場合が多い。こうした教育の受講者数を把握するため、情報系学科を擁する高等教育機関を中心としてシラバスを検索し、情報セキュリティ教育を行っている科目を選択可能な学生の在籍数を集計することとした。

(c) 情報セキュリティに関するリテラシー教育

学及び日常生活における情報システムやネットワークの利用のために覚えておくべき情報セキュリティリテラシーの教育であって、あらゆる産業分野の業務に従事するためにも必要な基礎知識である。典型的な例としては、学士課程の新入生等を対象に、一定の回数にわたって学内の情報機器やネットワークを活用する際に必要となる情報セキュリティ上の知識について教育するものが該当する。この場合、同じ科目内で情報セキュリティに関する内容以外に、情報倫理や情報機器を使う際のモラル等について教育するものもある。このような教育の受講者数を把握するため、情報セキュリティを扱う教育のうち、新入生等を対象とするものについてシラバスを検索し、当該科目の受講対象となっている学生の在籍数を集計することとした。

（1）情報セキュリティ分野を研究テーマとする研究室と在籍学生数

公開情報をもとに情報セキュリティ教育を行っている研究室を網羅的に抽出するために、以下の 3 種類の条件のいずれかを満たす研究室を対象とした。

- 情報処理学会コンピュータセキュリティ研究会主催による「コンピュータセキュリティシンポジウム 2016 (CSS2016)」[3]の発表者（教員、学生、研究生等の種別を問わない）が開催時に所属していた研究室
- 電子情報通信学会　情報セキュリティ研究専門委員会 （ISEC 研)「暗号と情報セキュリティシンポジウム 2016（SCIS2016）[4]」の発表者（教員、学生、研究生等の種別を問わない）が開催時に所属していた研究室
- 金岡 晃講師（東邦大学）が情報セキュリティ分野への進学希望者向けに公表している情報セキュリティ分野を扱っている研究室のリスト[5]に掲載されている研究室

これらについて集計した結果を表 6 に示す。なお、調査に際して各研究室が扱っている情報セキュリティ分野における研究テーマについても調査を行っている。表に示した研究テーマのカテゴリ名で表象している研究テーマはそれぞれ図 2 のとおりである。複数の分野にまたがると考えられるテーマについては、2 つ以上のカテゴリに該当することとしている。

[3] http://www.iwsec.org/css/2016/
[4] http://www.iwsec.org/scis/2016/
[5] 情報セキュリティ関連の大学研究室 Web サイトをまとめてみた（金岡晃）
https://github.com/akirakanaoka/seclablist

- 暗号：暗号理論及び暗号応用（電子署名、秘密分散、電子透かし、ステガノグラフィ）、暗号プロトコルなど
- 認証：認証手法（人物、機器その他）、認証技術、生体認証（バイオメトリクス）、認証プロトコル、アクセス制御など
- ネットワーク：アクセス制御、ネットワーク経由の脅威と対策、サイバー攻撃対策など
- システム：マルウェア、ハードウェアまたはソフトウェアの脆弱性、セキュリティアーキテクチャ、セキュア OS、アプリケーション実行制御
- データ：データベースセキュリティ、電子署名、秘密分散、デジタルフォレンジック
- マネジメント・ソーシャル：情報セキュリティマネジメント（情報システム、組織その他）、情報セキュリティガバナンス、情報セキュリティ監査、プライバシー保護技術、プライバシー影響評価、セキュリティ経済学（費用対効果分析など）、リスクコミュニケーションなど

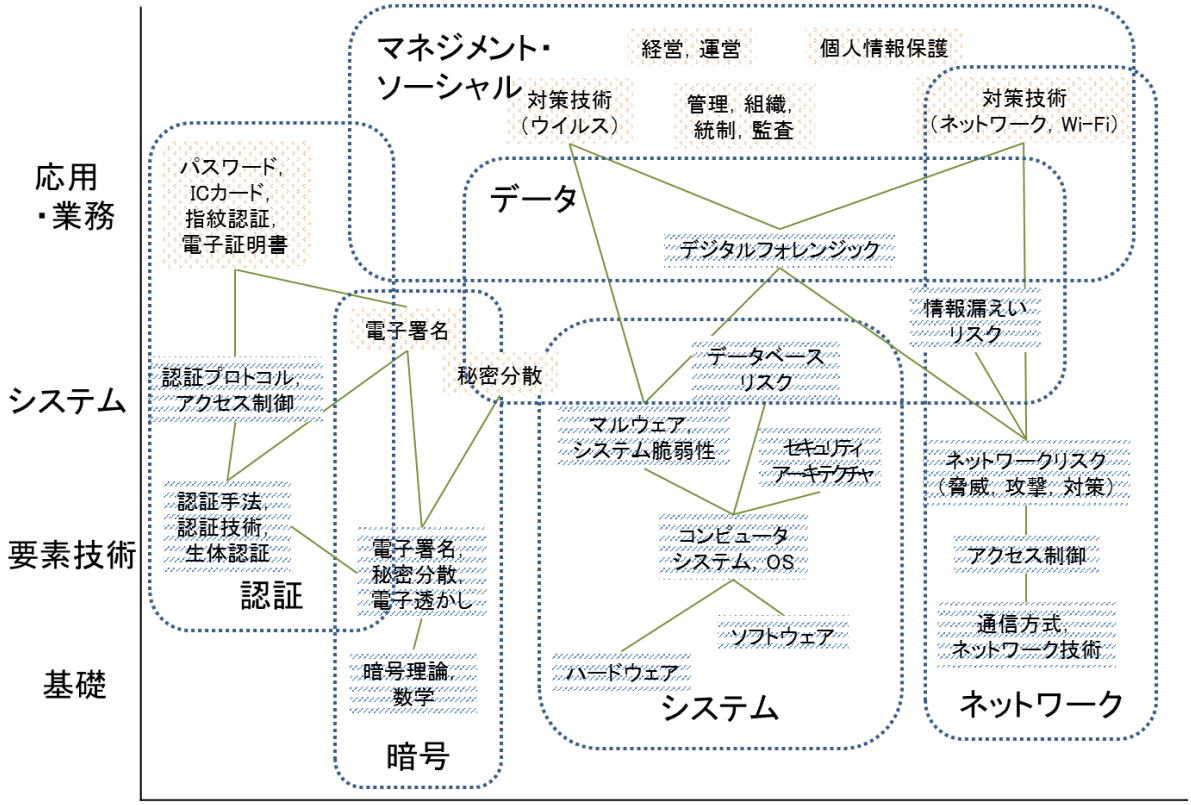

図 2　情報セキュリティ分野の研究テーマ

表 6　情報セキュリティ分野を研究テーマとする研究室と在籍学生数

研究室の分類	研究室数	扱っている研究テーマ毎の該当研究室数						1 年間に輩出される学生数（人）
		暗号	認証	ネットワーク	システム	データ	マネジメント・ソーシャル	
在籍学生情報を公表	87	42	27	34	30	22	14	787.8
在籍学生情報を非公表	47	15	6	23	24	12	10	（425.6）
合計	134	67	33	57	54	34	24	（1213.4）

（注）カッコ内は推計値

このとき、表中に示した「1 年間に輩出される学生数」は各研究室に所属する学生数に関する情報をもとに、次の数式で算出される値である。

1 年間に輩出される学生数 ＝ 学士課程在籍の学生数（4 年生以上）
＋ 修士課程在籍の学生数（学年を問わない）÷2
＋ 博士課程在籍の学生数（学年を問わない）÷3

なお、実際には研究室内で進学することで、社会に輩出しない学生が存在する可能性があるが、メンバーが完全に入れ替わる場合もあり、つねに進学が想定されるとは限らないことから進学による影響は考慮しないこととした。また、大学によっては学部 3 年から研究室に配属されるケースがあるが、学士課程 3 年の学生については在籍学生情報の調査対象としていない。

表中の推計値は、在籍学生情報を公表していない大学を対象に、公表している研究室における 1 研究室あたりの 1 年間に輩出される学生数の平均値と同程度の学生が在籍していることを仮定して推計したものである。在籍学生情報を非公表の研究室には、実際に学生が配属されていない可能性もあるため、実際に研究室で情報セキュリティ分野の専門的教育を受講している学生の数は本項で推計した 1,213.4 人／年よりもやや少ないものと見込まれる。

（2）情報セキュリティ分野を対象とする専門教育プログラムに参加している学生数

調査時点における代表的なプログラムの修了者数を次表に示す。この合計より、平成 27 年度の 1 年間に輩出された学生数の実績合計は 171 名である。

表 7　情報セキュリティ分野を対象とする代表的な専門教育プログラムの修了者数

プログラム名	1 年あたりの修了者数	備考
分野・地域を越えた実践的情報教育協働ネットワーク（セキュリティ分野）（enPiT-Security）	113 人[6]	平成 27 年度実績
トップエスイー[7]	40 名	第 10 期実績 （2015～2016 年度）
東京電機大学 国際化サイバーセキュリティ学特別コース（CySec）[8]	18 人 （5 科目以下の修了者を含めると 33 人）	平成 27 年度実績
合計	171 人	

（3）情報セキュリティに関する科目を受講することが可能な学科等と在籍学生数

情報系を専門とする専攻（大学院修士課程）と学科（学士課程、高等専門学校）とのそれぞれについて、情報セキュリティに関する講義や演習を 1 科目以上受講可能な学生数の調査を実施した。このうち、情報セキュリティ教育を行っている可能性があるが、シラバスからは判断できない学科や専攻における実施状況については、シラバスから判断可能な大学における情報セキュリティ関連科目の実施に関する割合から推計している。科目については内容が情報セキュリティに関するものであっても、科目名にそれが示されていない場合があるため、可能な限りシラバスの講義計画等を通じて把握するように努めた。具体的には次のような科目名において、実際には情報セキュリティに関する内容が扱われている場合がみられた。

＜修士課程＞

- 情報ネットワーク特論
- インターネット工学特論
- データ工学特論
- 情報基盤システム特論
- 情報システム信頼性特論
- 情報メディア論
- 情報環境特論
- 情報システム論演習

＜学士課程＞

- 符号理論

[6] enPiT-Security 本プログラムを受講した修士学生で、所定の単位（共通基礎科目　6 単位以上、演習科目または先進科目　4 単位以上）を取得し、修了認定を受け取った数。他に、部分的に受講した学生や学部生、高専生がいる。https://www.seccap.jp/

[7] トップエスイー http://www.topse.jp/ja/

[8] CySec https://cysec.dendai.ac.jp/

- 情報ネットワーク、コンピュータネットワーク
- ネットワーク・コンピューティング
- コンピュータネットワーク
- ネットワーク技術
- 情報社会及び情報倫理
- 信頼性工学
- 情報機器演習
- 情報工学演習

＜高等専門学校＞

- 情報理論
- 情報工学、電子情報工学
- ソフトウェア工学
- 情報ネットワーク、コンピュータネットワーク
- 情報機器

なお、これらの科目の中には、情報セキュリティ分野以外の内容が主となっているものも含まれるが、情報セキュリティ分野を扱う科目とみなしている。

候補となる学科の選出に際しては、理工学系の学科だけでなく、情報セキュリティに関する教育を行っている可能性のある経営系などの学科を含めた。

調査の結果を表 8に示す。

表 8　情報セキュリティに関する科目を受講することが可能な学科等と在籍学生数

			高等教育機関において情報セキュリティ教育を受講する機会を有する人材数（人／年）		
			大学院修士課程	大学学士課程	高等専門学校
①	候補となる学科等の数		193	313	58
②	①のうち、シラバスから情報セキュリティに関する教育の有無が判断できる学科等の数		175	236	56
③	②のうち、実際に情報セキュリティ教育が行われている学科等の数		157	229	51
④	③のうち、在籍者数が公開されている学科等の数		144	170	51
⑤	③の学科における1学年あたり平均在籍者数の合計（人）		6,615	13,487	2,509
⑥	①と②及び③と④の対比をもとに、有無を判断できない学科等を含めた推計値（人）（＝⑤×①÷②×③÷④）		7,954	24,095	2,598
⑦	進学を考慮した補正（実際に社会に出る人数。ただし博士後期課程への進学は無視する）（人）	下限値	6,615	6,872	1,505
		上限値	7,954	16,142	1,559
⑧	1年間に高等教育機関から輩出される情報セキュリティ教育を受講する機会のあった人材数の合計値（人）	下限値	14,992		
		中間値	20,323		
		上限値	25,654		

表内に示した推計のうち、「進学を考慮した補正」とは、学士課程または高等専門学校において情報セキュリティ教育を受講した学生が社会に出ずに進学することで、輩出される人材数の対象外となることを示している。このとき、高等専門学校の卒業生のうち、40%[9]が進学するものとし、学士課程卒業者については修士課程の推計値相当の人数が進学するものとした。したがって、上表における「1年間に高等教育機関から輩出される情報セキュリティ教育を受講する機会のあった人材数の合計値」には修士課程からの輩出人数の影響を受けない形となっている。

また、上限値と下限値の意味は次の通りである。中間値は両者の平均値である。

- 上限値：情報セキュリティ教育を実施しているかどうかをシラバスから把握できない学科について、把握可能な学科における実施の割合と同様の比率で実施されていると仮定した場合の学科数
- 下限値：情報セキュリティ教育を実施しているかどうかをシラバスから把握できない学科においては情報セキュリティに関する教育がまったく実施されていないと仮定した場合の学科数

この結果、情報セキュリティ教育を受講することが可能な人材は、高等教育機関全体から年間 2 万人程度が輩出されていると見込まれる。ただし、情報セキュリティに関する科目が選択科目の場合は、対象者が選択せず受講していない可能性がある。実際に情報セキュリティに関する科目を受講した人数については、（1）における推計と異なり正確な把握は困難であることに留意する必要がある。

（4）情報セキュリティに関するリテラシー教育を実施している学科等と在籍学生数

情報系学科に限らない大学学士課程を対象に、情報セキュリティに関するリテラシー教育を行っている事例について調査した結果を示す。

① 学士課程において情報セキュリティリテラシー教育を実施している学科等の在籍学生数

シラバスを公開している大学のうち、新入生を対象とするリテラシー教育において情報セキュリティに関する教育を行っている事例について調査したところ、9 つの大学において実施していることが確認された。うち 2 大学については、全学の新入生における必修科目としている。これらの科目を受講可能な学生数を合算すると、8,388 人である（うち 1 大学については受講者数が不明のため合算対象としていない）。

[9] 独立行政法人国立高等専門学校機構の公表資料における「卒業生者全体に対する進学率」の平成 27 年度実績をもとに設定。http://www.kosen-k.go.jp/pdf/gaiyo_H28-singaku.pdf

② 通信制大学において情報セキュリティ教育を実施している学科等の在籍学生数

通信制大学においては時間割による制約が少ないため、幅広い科目が提供されている。この一環として 3 大学において情報セキュリティに関する科目が提供されている。各大学が公表している在籍学生数をもとに、情報セキュリティ関連の科目を受講可能な学生数を合算すると 23,266 人である。他の調査結果と比較して大学数の割に人数が多いが、これらの科目はいずれも選択科目であり、実際の受講者はこれよりもかなり少ないものと見込まれる。

（5）情報セキュリティ分野の大学教員数

情報セキュリティ分野の大学教員数を把握する方法としては、以下の 2 つが想定される。

- （1）で把握した大学研究室の主宰者数をもとに算定する方法
- （3）で把握した大学における講義の担当講師をもとに算定する方法

このうち前者については、1 つの研究室に複数の教員が所属している場合があるため、その分を追加的に把握する必要があるが、（1）の調査を通じて個別の状況の把握が容易である。一方後者については新たにシラバスをもとに全ての担当教員名を洗い出さなければならず、（3）においてシラバスから把握可能な学科・専攻が限られることから十分な精度を確保することが困難である。そこで本調査においては、（1）で教員数を把握する手段として、（1）で把握した研究室を単位として当該研究室に所属する教員数を集計する方法を用いることとした。その結果を次表に示す。

表 9　情報セキュリティ分野の大学教員数

分　類		在籍教員公表研究室分（人）	在籍教員非公表研究室分（人）	合計（人）
教員数		188	47	235
専門分野別	暗号	86	15	101
	認証	62	6	68
	ネットワーク	82	23	105
	システム	70	24	94
	データ	58	12	70
	マネジメント・ソーシャル	30	10	40

（注 1）専門分野の定義は表 6 と同じ
（注 2）調査対象とした教員は教授、准教授、講師、助教であり、特任教員を含む
（注 3）研究室所属教員数を非公表の研究室の教員数は 1 名とみなす
（注 4）複数の専門分野を扱う研究室に所属する教員は全員がすべての専門分野を扱うものとみなす

調査時点において、我が国の大学で情報セキュリティ分野を専門とする教員数は 235 名程度と推計される。また、従来我が国においては世界的な研究者の分布と比較して暗号系の研究者が多いことが特徴と言われてきたが、調査時点においては暗号系も多いながら、ネットワークやシス

テムに関するセキュリティを扱う研究者が増加していることが示されている。

（６）過去の類似調査結果との比較

本調査と同様に、情報セキュリティに関する教育を受講した学生の人数に関する調査を実施した結果が、平成 24 年 4 月に独立行政法人情報処理推進機構（IPA）より「情報セキュリティ人材の育成に関する基礎調査」[10]（以下、「IPA 調査」という。）報告書として公表されている。同報告書において、「情報セキュリティ人材の供給能力に関する調査」として示されている調査結果は、本調査との間で調査方法に若干の相違があるものの、大学等における情報セキュリティ教育の実施状況に関する経年変化を把握する目的で比較対象とすることが可能と考えられる。

次表に IPA 調査報告書における調査結果と、本調査の調査結果とを比較した結果及び調査条件の相違を示す。

表 10　IPA 調査結果との本調査の調査結果の比較

<table>
<tr><th colspan="2">調査項目</th><th>IPA 調査結果</th><th>本調査の調査結果</th><th>条件の相違等</th></tr>
<tr><td rowspan="2">情報セキュリティに関する専門的内容についての教育</td><td>情報セキュリティ分野を研究テーマとする研究室と在籍学生数</td><td>99 研究室
592～1,149 人/年
（約 1,000 人/年）</td><td>134 研究室
788～1,213 人/年</td><td>IPA 調査には情報セキュリティ大学院大学ほかの在籍者数を含まない</td></tr>
<tr><td>情報セキュリティ分野を対象とする専門教育プログラムに参加している学生数</td><td>3 プログラム
1 研究科 1 専攻
129 人/年
（約 130 人/年）</td><td>3 プログラム
171～186 人/年</td><td>IPA 調査には情報セキュリティ大学院大学ほかの在籍者数を含む</td></tr>
<tr><td rowspan="5">情報セキュリティに関する専門的内容の入門的な教育（情報セキュリティに関する科目を受講することが可能な人材数）</td><td>修士課程</td><td>246 専攻
4,250～5,201 人/年</td><td>193 専攻
6,615～7,954 人/年</td><td>（特になし）</td></tr>
<tr><td>学士課程</td><td>348 学科
14,198～18,249 人/年</td><td>313 学科
13,487～24,095 人/年</td><td>（特になし）</td></tr>
<tr><td>高等専門学校</td><td>58 学科
885～1,027 人/年</td><td>58 学科
2,509～2,598 人/年</td><td>（特になし）</td></tr>
<tr><td>合計
（進学を考慮したもの）</td><td>16,664～21,558 人/年
（約 20,000 人/年）</td><td rowspan="2">14,992～25,654 人/年</td><td rowspan="2">IPA 調査は専門学校在籍者を含めた人数</td></tr>
<tr><td>上記合計から専門学校を除いたもの</td><td>14,704～18,836 人/年</td></tr>
</table>

上述の比較より、次の傾向が判読される。

- 情報セキュリティに関する専門的内容についての教育を受講した人材数は、IPA 調査の時点と比較して約 2 割の増加傾向が認められる。ただし、本調査において調査対象研究室の数が大幅に増加している点を考慮する必要がある。これは情報セキュリティをテーマとする研究室が増えたためではなく、本調査のみ金岡講師の調査結果（本報告書 9 ページ参照）をもとに対象研究室を追加していることによる。一方で、既存の情報系研究室において新たに情報

[10] https://www.ipa.go.jp/security/fy23/reports/jinzai/

セキュリティを研究テーマとして扱うようになった研究室もあり、研究室及び輩出される学生数が増加傾向にあるのは確かである。

- 情報セキュリティに関する科目を受講することが可能な人材数については、修士課程、学士課程、高等専門学校のいずれも増加の傾向にある。学士課程のみ、人材数の下限値が IPA 調査結果より少なくなっているが、これは本調査における調査対象学科数が IPA 調査よりも少ないことによる。同様の条件は修士課程にも当てはまるが、修士課程では情報セキュリティに関する科目を有する専攻の比率が高まったことにより、増加の影響が顕著に現れている。
- 高等専門学校においても、情報セキュリティに関する科目を受講することが可能な人材数の増加が著しい。IPA 調査以降で定員数の増加や情報系学科の新設などは行われておらず、この増加は情報セキュリティ関連科目を開講する学科の比率が高まったことによるものと考えられる。
- 表中に記載の通り、IPA 調査は情報系専門学校の在籍者も対象としているのに対し、本調査は対象としていない相違がある。専門学校在籍者を含めずに比較した場合、情報セキュリティに関する科目を受講することが可能な人材数は専門的内容についての教育を受講した人材数と同様、平均して約 2 割程度の増加傾向が認められる。

２．１．２ 実施状況に関する深掘調査

モデル・コア・カリキュラムの検討に際し、実施状況の質的把握の観点からアンケート調査及びヒアリング調査を通じて深掘調査を実施した結果を示す。

（１）仮説の設定

調査に先立ち、現在の我が国の大学における情報セキュリティ教育の実施状況に関して、次表の仮説を設定した。

表 11　情報セキュリティ教育の実施状況に関する仮説

仮説1	リテラシー教育でない情報セキュリティ教育が実施されているのは、情報セキュリティ分野を研究テーマとしている教員が在籍している学科がほとんどである。
仮説2	情報セキュリティを専門としている教員が、非常勤講師として他大学で情報セキュリティに関する（リテラシー教育でない）セキュリティ教育を受け持つことはよくある。
仮説3	産業界で情報セキュリティ業務に従事している方が非常勤講師として情報セキュリティ分野の講義や演習を受け持つことは、特別なコース以外ではまだ少ない。
仮説4	情報系学科／専攻に属する学生のうち、情報セキュリティに関する専門科目（情報理論や情報ネットワーク工学などの一部でセキュリティ関連の話題を扱うものは除く）を受講する割合は5

	割程度である。
仮説5	情報セキュリティに関する講義を行っていても、その前提となるネットワーク技術や数学に関する基礎が身についていない学生が多いため、シラバスで予定している内容を講義することが困難なことがある。
仮説6	現在、学生向けに情報セキュリティ教育を行っていない大学は、必要性を感じていないか、必要と感じているが何らかの阻害要因で実施できていない場合に2分される。後者の場合の阻害要因は、既存カリキュラムが満杯で追加困難、教えられる講師の確保が困難、などである。
仮説7	科目名にセキュリティとついていなくても、ネットワーク工学などの講義の一部のコマでセキュリティ関連の内容を教えている場合がある。方法としては、同一の講師がセキュリティも教える場合と、オムニバスでセキュリティに詳しい外部講師・産業界講師等が教える場合の2種類がある。
仮説8	情報倫理に関する講義の中でセキュリティを教えている場合もある。（特に文科系学科、文理融合系学科等）
仮説9	ロボット工学、医療・介護分野など、情報やネットワークのセキュリティが重要な分野では、情報セキュリティ教育の必要性が学科内で認識されている。ただし、実際に実施されているのはごくわずかである。

（2）アンケート及びヒアリング調査の実施

上記の仮説を検証するとともに、高等教育機関における情報セキュリティ教育に関して検討されている方針や直面している課題等を把握することを目的として、東北地域の大学等をサンプルとしてアンケート調査及びヒアリング調査を実施した。東北地域を選定した理由としては、限られた期間内で全国を対象に調査することができなかった一方、東北地域の大学には情報セキュリティ分野を専門とする多くの教員を擁する機関とそうでない機関、総合大学と理工系大学など幅広いバリエーションがあり、作業部会 1 における審議の結果、サンプル調査を行う地域として適切と判断されたことによる。

① アンケート調査

東北地域の高等教育機関のうち、以下の機関から回答を得た。

表 12　アンケート回答機関

分類	総合大学	理工系大学	高等専門学校	合計
国立	5 機関		1 機関	6 機関
公立	1 機関	1 機関		2 機関
私立	3 機関	2 機関		5 機関
合計	9 機関	3 機関	1 機関	13 機関

② ヒアリング調査

①で回答を得た高等教育機関及び追加で依頼した機関の中から、合計 10 機関の協力を得て、訪問形式によるヒアリング調査を実施した。

（3）調査結果に示される状況

アンケート調査の集計結果を質問ごとに整理した結果を示す。

① 情報セキュリティに関する教育の実施状況

回答機関のうち、1 機関を除き情報セキュリティに関する専門科目、または他の科目における一部として情報セキュリティ分野を対象とする教育が実施されている。その科目名と教員の担当状況を次表に示す。ほとんどの科目が学内教員により実施されているが、一部では情報セキュリティ分野を専門としない教員が情報セキュリティ科目を担当している例も見られる。また経営系学科においては、Web システムや情報社会論といった実学的な内容を扱う科目で情報セキュリティをとりあげている点に特徴が示されている。

情報セキュリティに関する専門科目を提供していない大学からは、その理由として「他の科目に比べて必要性が低い」「現状の科目で十分（カリキュラム編成上の都合）」「学内で担当可能教員がいない」といった内容が示されている。

表 13　アンケート回答大学において開講されている情報セキュリティ専門科目

分類	科目名（履修年次）	担当教員	備考
国立	暗号とセキュリティ（4 年）	学内教員	暗号関連が中心
	情報倫理（2 年）	学内教員（専門外）	情報セキュリティに関する専門的内容を含む
国立	情報セキュリティ（3 年）	学内教員	
	情報倫理（2 年・必修）	学内教員	
国立	情報システムの理解と構成	学内教員	
	情報社会と情報倫理	学内教員	
国立	通信工学部 B（3 年）	学内教員	
公立	情報ネットワーク工学（3 年）	学内教員	
	システム科学演習 B（2 年）	オムニバス外部講師	
私立	情報セキュリティ工学（3 年）	学内教員	
	通信ネットワーク	学内教員	
	情報リテラシー	学内教員	
私立	情報セキュリティ（3 年）	学内教員	
	コンピュータネットワーク（3 年）	学内教員	
	コンピュータアーキテクチャ（1 年）	学内教員	
私立	情報ネットワーク（3 年）	学内教員	
	符号とセキュリティ（2 年）	学内教員	

分類	科目名（履修年次）	担当教員	備考
	コンピュータ入門演習（1 年・必修）	学内教員	
私立	Web システム（3 年）	学内教員（専門外）	
	情報セキュリティ（2 年）	学内教員	
	情報倫理（1 年・必修）	学内教員	
私立	情報ネットワーク（3 年）	学内教員	
	情報社会論（2 年）	オムニバス学内教員	
高専	情報セキュリティ（5 年）	学内教員	講演会を別途実施
	技術者倫理（5 年）	オムニバス学内教員	
	情報セキュリティ基礎（4 年）	学内教員	
	ネットワーキング技術Ⅱ（4 年・必修）	学内教員	

② 理工系学部を対象とした情報セキュリティ教育の実施状況

アンケート調査から、総合系大学では国公私立を問わず理工系学部全体としての情報セキュリティ教育の必要性が認識されていることが示されている。しかしながら情報系以外の学科では情報セキュリティを意識した教育は行われていない。私立の単科系の大学では、総合系大学と比較して必要性の認識は低い傾向が見られる。なお、情報系以外の学科向けにコンピュータやネットワークに関連した科目が実施される場合、その中で情報セキュリティに関連する内容が扱われることがあるが、これは意識的に実施されているものではないと回答されている。

③ 全学を対象とした情報セキュリティリテラシー教育の実施状況

アンケート調査の依頼先の多くが理工系学部の担当者であったため、全学における状況が必ずしも把握されていない点に留意が必要であるが、学部を問わず教養科目において情報処理に関する講義や演習等が実施される場合、その一環として情報セキュリティに関するリテラシー教育が行われている。ある程度の規模を有する総合大学においては、学内向けに専用の情報セキュリティリテラシー教材（Web 教材や講習会向け教材）を作成する例も見られる。

④ 情報セキュリティ教育を行う上での課題

情報セキュリティ教育を行う上での課題として、各大学から指摘された内容を以下に抜粋する。学内における必要性に関する認知度の低さが阻害要因となっていることが推測される。

- 実施には全学レベルでの情報セキュリティ教育の重要性が認識される必要がある
- 他の情報科目に比べて専門科目としての学生の必要性・重要性の認知度が低く、受講者が少ない
- ネットワーク技術や数学などに関する前提知識について学生によって理解に差があるため、概念的な説明にとどまりがち

- 担当可能な教員が少ないため、学部全体への教育機会の提供が困難
- 予算的な問題から外部講師を招いての講演実施が困難
- 学科内で電子情報系の科目を幅広く提供するため、情報セキュリティ教育を行う上での前提となるネットワーク技術や数学に関する基礎を十分に身につけてもらうことができない
- 文理融合型学科のため、文科系・芸術系科目の比重が多く、情報セキュリティに限らず情報系の教育が十分にできない

⑤ 要望など

今後の情報セキュリティ教育の普及に向けた要望や提言として、回答された内容の抜粋を以下に示す。

- 「素性のわからない添付ファイルを開かない」といったリテラシー教育は技術者教育とは異なるものであり、セキュリティを確保するにはどうすべきかの理論や方法論がほしい
- 全国的に情報セキュリティ教育の実態が暗号系に特化しており、情報系の教員であっても情報の完全性や可用性を理解していない例がみられる
- 分野や学部・学科に関係なく、情報システムやネットワークを利用するエンドユーザであれば誰でも、情報の本質を捉えた情報セキュリティに関する必要最小限の知識や理解は持つべき
- 学生に対する教育以外に、大学経営層に対する教育も必要
- Web 講義などにより、受講すれば単位を提供するようにすることで充実化が可能なのではないか

（4）仮説の検証結果

（1）に示した仮説について、（2）に示したアンケート調査及びこれを踏まえて実施したヒアリング調査の結果をもとに、仮説の妥当性について検証した結果を示す。

仮説1	リテラシー教育でない情報セキュリティ教育が実施されているのは、情報セキュリティ分野を研究テーマとしている教員が在籍している学科がほとんどである。

地方国立総合系大学においては、情報セキュリティ分野の専門教員のいる大学以外は実施もされていない。専門教育を行っている大学でも、学問体系が確立している“符号”や“暗号”など数理科学に関する科目が情報セキュリティの専門科目として位置づけられており、専門教員も符号や暗号を専門とする教員である。このように、セキュリティ分野の専門教員の専門分野にセキュリティ教育の内容が左右されるケースも目立つ。

また、国立総合系大学をはじめとした従来型の工学部・理工学部に在籍する情報セキュリティ

分野以外の教員は、情報セキュリティ系科目を数理科学に深く入る必要があり、数学をはじめとした基礎学問を系統的にしっかり学んでいないと理解できないものとして捉えているケースが多く、セキュリティの機密性・完全性・可用性の定義など、社会や企業におけるニーズで捉える産業界との間で「情報セキュリティ」という概念自体の捉え方が異なっていることがわかった。

仮説2	情報セキュリティを専門としている教員が、非常勤講師として他大学で情報セキュリティに関する（リテラシー教育でない）セキュリティ教育を受け持つことはよくある。

今回調査した範囲では、仮説に示されているような事例は見受けられない。リテラシー教育に関しては、大学教員が非情報系（看護系大学）のセキュリティリテラシー教育を担当している事例がある。

仮説3	産業界で情報セキュリティ業務に従事している方が非常勤講師として情報セキュリティ分野の講義や演習を受け持つことは、特別なコース以外ではまだ少ない。

今回調査した範囲では、仮説に示されているような産業界教員が非常勤講師を担う事例は見受けられず、ほぼ仮説の通りと思われる。情報系専門学科を有する大学では、社会人向けの短期CTF[11]コースを外資系セキュリティ企業と共同開発し、企業講師が実践演習を担当している事例がある。

仮説4	情報系学科／専攻に属する学生のうち、情報セキュリティに関する専門科目（情報理論や情報ネットワーク工学などの一部でセキュリティ関連の話題を扱うものは除く）を受講する割合は5割程度である。

今回調査対象とした大学は、“電子系と情報系”あるいは“理学系と工学系”が学科の中でまとめて扱われている大学が大多数であった。また、情報セキュリティ分野の専門科目が全員の必修科目となっているのは情報系専門大学のみであり、他は一部必修または選択履修である。情報系と通信系が同一の学科として扱われている大学の場合、情報系の選択者は情報セキュリティ系科目が必修、それ以外は選択となっているなど、仮説で想定した内容に近い事例もみられる。ただし、中小規模の総合系や単科系の大学においては、カリキュラムにおいて理工系学科として情報系かどうかに関わらず画一的な扱いとされている場合が多い。

[11] Capture The Flag の略。原義は陣取りゲーム的なもの一般を意味するが、情報セキュリティ分野では情報システムの模擬環境への攻撃が成功すると正解がわかるようなゲームで得点を競う形式のイベントを指す。米国発祥であるが、現在では世界各地で実施されている。我が国では SECCON（http://www.jnsa.org/seccon/）が代表的である。

仮説5	情報セキュリティに関する講義を行っていても、その前提となるネットワーク技術や数学に関する基礎が身についていない学生が多いため、シラバスで予定している内容を講義することが困難なことがある。

地方国立総合系大学を中心に、符号や暗号など数理科学の視点で情報セキュリティを捉えている教員からは、数学が苦手な学生が多く苦労しているとの回答が得られている。地方私立大においては、暗号化などで数学的な内容を深掘りしてしまうと学生が理解できなくなるという実態を踏まえ、将来的に専門家ではなく一般レベルの社会人に向けた育成を行うという教育目標に合わせ、利用シーンや事例を交えながら学生のレベルに合わせた教育を行おうとする工夫がなされている。一方、情報系専門学科を有する大学からは、専門的な情報セキュリティの前提知識となるオペレーティングシステム（OS）やデータベースに関する講義が３年生や４年生で行われるため、幅広い前提知識が必要となる情報セキュリティの専門教育はできるだけ上級学年に持っていくのが望ましいという意見が示されている。他の大学からも、情報セキュリティを理解する上で不可欠な情報ネットワークの授業が３年生以降であるなど、情報セキュリティ教育を実施する上で前提知識や習得順に関する課題が存在することが指摘されている。

セキュリティ分野を幅広く熟知した大学の教員からは、「学部は基礎寄りの内容を学ぶ場と捉え、大学院は何回も入って良い場とし、実践を含む最新のセキュリティ教育を行うのが理想である」との意見が示されている。

仮説6	現在、学生向けに情報セキュリティ教育を行っていない大学は、必要性を感じていないか、必要と感じているが何らかの阻害要因で実施できていない場合に2分される。後者の場合の阻害要因は、既存カリキュラムが満杯で追加困難、教えられる講師の確保が困難、などである。

教員レベルでは、ほぼ全ての教員が情報セキュリティに関する教育の必要性を感じている。大学経営として必要性が理解されていないという意見がある一方で、大学法人としての中期計画の中で「サイバーセキュリティ教育」が盛り込まれているケースもある。後者の例では全学を対象に従来の情報リテラシー教育から一歩進んだ、本格的なサイバーセキュリティ教育の展開が計画されている。

情報セキュリティ教育の阻害要因としては、既存のカリキュラムが満杯ということもあるが、各大学より「ディプロマ・ポリシーおよびカリキュラム・ポリシーに入らない限りは難しい」との意見が示されている。また、符号暗号を除いた情報セキュリティが既存の学問体系に比べて新しいことや、電子情報系学科においては電子系がメインのため情報セキュリティが入る余地がないことも阻害要因になっている。

情報セキュリティに関する科目新設を教員からのボトムアップで提案することはハードルが高く、トップダウン的に文部科学省や学会等からの通達があると動きやすいとの意見がある。

仮説7	科目名にセキュリティとついていなくても、ネットワーク工学などの講義の一部のコマでセキュリティ関連の内容を教えている場合がある。方法としては、同一の講師がセキュリティも教える場合と、オムニバスでセキュリティに詳しい外部講師・産業界講師等が教える場合の2種類がある。

今回調査した限りでは外部講師・産業界講師が教えるケースは見受けられないが、それ以外はほぼ仮説の通りといえる。教養教育では「情報基礎」、専門教育では「情報ネットワーク」などにおいて、15 コマの中の 3 コマ程度を情報セキュリティ教育に充当している事例が多い。このうち、教養教育では専門の異なる学内教員が分担あるいはオムニバスで対応している例が多く、情報ネットワークに関しては同一教員がセキュリティを含めて教えている例がほとんどである。

情報系専門学科を有する大学や、全学教育に既に取り組んでいる大学を除く一般の地方国立大や私立大学（理工／電子情報が同一学部あるいは学科となっている大学）からは、15 コマの専門教育に対するモデルカリキュラムではなく、既存の教養科目や情報系専門科目の中で 3 コマ程度をセキュリティ教育に充当することを前提としたモデルカリキュラムや教材の確立に期待する声が非常に多い。「国レベルでの模範例などのスライドや動画があると授業に取り込みやすく、国のお墨付きがあれば安心して使える」といった意見も示されている。

仮説8	情報倫理に関する講義の中でセキュリティを教えている場合もある。（特に文科系学科、文理融合系学科等）

文科系学科や文理融合学科という枠ではなく、全学教養科目の情報倫理や情報基礎の中で、数コマを情報セキュリティのリテラシー教育に充当している例が多い。

経営系と情報系学科のみで構成される大学では、「経営情報システム論」などの科目で経営学部がセキュリティマネジメントや情報システムの上流工程などの内容を担当することで相互連携している事例が見られる。総合大学の教員からも、経営と情報の両側面からセキュリティを捉えていく必要性に関する指摘がなされている。

反対に情報系専門大学を有する大学からは、企業等の組織構造を知らない学生にはセキュリティマネジメントは理解できないため実施していないとの回答があり、育成する人材像の違いが回答に反映している可能性がある。

仮説9	ロボット工学、医療・介護分野など、情報やネットワークのセキュリティが重要な分野では、情報セキュリティ教育の必要性が学科内で認識されている。ただし、実際に実施されているのはごくわずかである。

ほぼ仮説の通りである。教員レベルでの情報セキュリティ教育の必要性は認識されているが、既存の学問体系において基礎科目である物理や数学、計算機関連科目などでカリキュラムが満たされてしまっており、現状では科目として情報セキュリティが入る余地がないというのが各大学の実情であると思われる。

２．１．３ 調査結果のまとめ

文献調査及びアンケート・ヒアリング調査をもとに、我が国における情報セキュリティ教育の現状に関する調査を実施した。情報セキュリティに関する専門的内容についての教育の受講者は 1 年あたり 1,200 名弱程度、情報セキュリティに関する科目を受講することが可能な人材数は 1 年あたり 20,000 名程度と試算され、5 年前に IPA が調査した同様の調査と比較して約 2 割の増加が認められる。一方、東北地方を対象に深掘調査を実施したところ、13 機関中 12 機関で何らか情報セキュリティに関する内容を教育しているが、内容が暗号に限定されるなど、産業界が期待するものとは異なるものも多いといった課題も指摘されている。さらに、大学教員はほぼすべてが情報セキュリティ教育の必要性を認識している一方で、大学における教育方針はまちまちであり、結果的に十分な情報セキュリティ教育が実施されない大学が依然として存在する結果を生んでいることが明らかとなった。

２．２ これまでの情報セキュリティ教育に関する取組

モデル・コア・カリキュラム策定のための参考とするため、我が国の大学が関与してこれまでに実施された情報セキュリティ教育に関する取組について調査を行った結果を示す。

２．２．１ 情報セキュリティ教育に関するおもな事例

大学が関与している情報セキュリティに関する人材育成プログラムやコースについて、公表されている情報をもとに概要を整理した結果を示す。

（１）情報セキュリティ分野の人材育成プログラム

学科・専攻やコースとは別に、情報セキュリティ人材育成のためのプログラムとして実施された事例を次表に示す。所定の教育を修了した受講者に対しては、修了認定を行っている事例がほとんどである。

表 14　情報セキュリティ分野の人材育成プログラムの事例

No.	取組の名称	対象とする教育の種類（教育のレベル）	概　要
01	大阪大学 セキュア・ネットワーク構築のための人材育成プログラム（H13～H17）	修了認定（情報系大学院レベル）	文部科学省の助成のもと、講義と実験の組み合わせによりネットワークセキュリティ専門技術者の育成を実施
02	早稲田大学 セキュリティ技術者養成プロジェクト（H13～）	修了認定（情報系学部レベル）	産学連携により産業界の技術者・研究者を講師とする大学院向け講義を実施（学部向け）
03	早稲田大学 セキュリティ技術者養成プロジェクト（H13～）	修了認定（情報系大学院レベル）	産学連携により産業界の技術者・研究者を講師とする大学院向け講義を実施（大学院向け）
04	中央大学 情報セキュリティ・情報保証 人材育成拠点（H15～19） 情報セキュリティ副専攻	修了認定（情報系大学院レベル）	安全なネットワーク構築や脆弱性検出に関する能力開発のための実習システムを導入したほか、米国セキュリティ団体とも連携して体系的教育を実施
05	工学院大学 セキュアシステム設計技術者の育成プログラム（H15～19）	修了認定（情報系大学院レベル）	大学間連携及び産学連携により、情報システムのライフサイクル全般にわたるセキュリティ要件を反映した設計ができる技術者の育成を実施
06	中央大学 電子社会の信頼性向上と情報セキュリティ（21世紀COEプログラム）（H16～19）	研究開発（を通じた人材育成）	社会人学生を企業に在籍のまま博士課程に受け入れ、深い専門性と幅広い視野を持つ人材の育成を実施
07	情報セキュリティ大学院大学ほか 研究と実務融合による高度情報セキュリティ人材育成プログラム（ISS Square）（H20～ 継続中）	修士号及び修了認定（情報系大学院レベル）	先導的ITスペシャリスト育成推進プログラムとして、大学間や産学の壁を超えて潜在力を結集し、情報セキュリティ分野における世界最高水準の人材を育成

No.	取組の名称	対象とする教育の種類（教育のレベル）	概　要
08	奈良先端科学技術大学院大学ほか 社会的ITリスク軽減のための情報セキュリティ技術者・管理者育成（IT Keys）（H20～24）	修了認定（情報系大学院レベル）	先導的ITスペシャリスト育成推進プログラムとして、関西圏を中心とした情報系4大学院および4企業・団体の連携のもと、情報ネットワークの管理・運用の現場でリーダーシップを発揮し活躍できる技術者・実務者を育成
09	情報セキュリティ大学院大学ほか 分野・地域を越えた実践的情報教育協働ネットワーク（セキュリティ分野、enPiT-Security第1期）（H24～継続中）	修士号、修了認定（情報系大学院レベル）	連携大学間の協力のもと、暗号やネットワークなどの技術的な知識から法制度やリスク管理などの社会科学的な知識までバラエティに富んだ講義や演習コース等を通じて、社会・経済活動の根幹にかかわる情報資産および情報流通のセキュリティ対策を技術面・管理面で牽引できる実践リーダーを育成
10	東京電機大学 国際化サイバーセキュリティ学特別コース（CySec）	修了認定（情報系大学院レベル）	双方向ワークショップ形式の演習等を通じて、企業において情報セキュリティ統括責任者（CISO）や上級セキュリティエンジニアを育成
11	東北大学ほか 情報セキュリティ分野の実践的人材育成コースの開発・実施（セキュリティ分野、enPiT-Security第2期）（H28～）	修了認定（情報系学部レベル）	第1期の成果をもとに、学部学生を主対象として、より多くの大学・高専・専門学校や企業の参加のもと、多様な基礎科目・専門科目・先進PBL科目（演習等）の提供を通じて、社会生活、産業、行政の広い分野において活躍するセキュリティ人材を育成
12	国立情報学研究所 トップエスイー	修了認定（情報系大学院レベル）	ソフトウェアエンジニアリングの技術・理論・ツールを使いこなすスーパーアーキテクトを育成する、社会人向けの教育プログラム
13	東京工業大学 野村総合研究所寄附講座「サイバーセキュリティ教育研究共創プログラム」サイバーセキュリティ特別専門学修プログラム	修了認定（情報系大学院レベル）	サイバーセキュリティに関する教育・研究の推進を目的とした連携協定を締結し、サイバー攻撃手法の解析や防御技術に関する研究を行うとともに、産業界講師による関連講義を実施

（2）情報セキュリティ分野を対象とする学科・専攻・コース

学位の対象となる学科・専攻・コースとして情報セキュリティ分野の教育を行っている事例を次表に示す。

表 15　情報セキュリティ分野を対象とする学科・専攻・コースの事例

No.	取組の名称	対象とする教育の種類（教育のレベル）	概　要
14	情報セキュリティ大学院大学 情報セキュリティ研究科	修士号 博士号	情報セキュリティ分野を専門とする研究科として、技術のみならず法学や倫理学といった人文・社会科学諸分野にわたる教授陣により、広い視野に立って問題解決を担う高度な専門技術者、実務家、研究者を育成

No.	取組の名称	対象とする教育の種類（教育のレベル）	概　要
15	長崎県立大学 情報システム学部 情報セキュリティ学科	学士号	学部教育での実践的教育のほか、外部イベントや長期インターンシップ等を通じて社会で即戦力として活躍できる情報セキュリティのプロフェッショナルを育成
16	兵庫県立大学大学院 応用情報科学研究科 応用情報科学専攻 高信頼情報科学コース	修士号 博士号	技術とマネジメントの両方の観点から情報の安全・安心と質を考えることのできる人材を育成(カーネギーメロン大学とのダブルディグリープログラムを提供)

（3）情報セキュリティ分野を対象とする講義・演習等

学士課程または修士課程のカリキュラムを構成する一部科目において、情報セキュリティに関する内容を扱う講義や演習を実施している事例を次表に示す。

表 16　情報セキュリティ分野を対象とする講義・演習等の事例

No.	取組の名称	対象とする教育の種類（教育のレベル）	概　要
17	東京電機大学 情報セキュリティ講座「ネットワークのセキュリティ」	講義・演習（情報系大学院レベル）	特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）との連携により、産業界の講師による実践的演習を実施
18	東京電機大学 情報セキュリティ講座「不正侵入対策の実際」	講義・演習（情報系大学院レベル）	特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）との連携により、産業界の講師による実践的演習を実施
19	早稲田大学 マイクロソフト寄附講座「情報セキュリティ技術」	講義・演習（非情報系を含む学部レベル）	実践的なセキュリティの知識及び技術を習得したコンピュータセキュリティ分野の人材育成を支援するため、マイクロソフトの技術者による講義を実施
20	早稲田大学 NTT寄附講座「サイバー攻撃対策技術の基礎」	講義・演習（情報系学部レベル）	サイバー攻撃対策技術を創出する傑出したサイバーセキュリティ人材の発掘・育成を目的として、NTT技術者が講師を務めるサイバー攻撃対策講座を設置（学部向け）
21	早稲田大学 NTT寄附講座「高度サイバー攻撃対策技術」	講義・演習（情報系大学院レベル）	サイバー攻撃対策技術を創出する傑出したサイバーセキュリティ人材の発掘・育成を目的として、NTT技術者が講師を務めるサイバー攻撃対策講座を設置（大学院向け）
22	岡山理科大学 JNSA連携による遠隔講義「情報セキュリティ」	講義・演習（情報系学部レベル）	JNSA会員企業の技術者が遠隔教育にて理系学部学生に情報セキュリティの基礎について講義
23	北陸先端科学技術大学院大学 NEC寄附講座「サイバーレンジ構成学」	研究開発	サイバーセキュリティに関する最先端の研究活動と人材育成を目的として、サイバー空間の演習環境の構成技術の研究開発とこれを用いた教育プログラムの設計及び教材開発を実施

No.	取組の名称	対象とする教育の種類（教育のレベル）	概　要
24	九州大学 富士通寄附講座「富士通スペシャリスト育成研究部門」	講義・演習（情報系学部レベル）研究開発	サイバーセキュリティ教育に関する研究及びセキュリティ人材育成の加速を目的とした寄附研究部門を設置し、人材育成手法や教材に関する研究開発を行うとともに、研究成果を活用した講座を提供

（４）情報セキュリティ分野を対象とする一般向け講義・演習等

大学が主体的に提供している情報セキュリティに関する一般向け（社会人、学生等）のコース事例を次表に示す。

表 16　情報セキュリティ分野を対象とする一般向けコースの事例

No.	取組の名称	対象とする教育の種類（教育のレベル）	概　要
25	情報セキュリティ大学院大学短期再教育プログラム「実践サイバーレンジ演習」	主に社会人を対象とする自己研鑽向け	大日本印刷株式会社およびその子会社である株式会社サイバーナレッジアカデミーと共同で、インシデントレスポンスのための実習講座（座学とサイバーレンジ演習）を開講
26	情報セキュリティ大学院大学短期再教育プログラム「情報セキュリティ入門講座」	主に社会人を対象とする自己研鑽向け	2015年度にオンライン大学講座gaccoで実施した入門的内容を同一の講師陣によるスクーリング形式の講義として開講
27	情報セキュリティ大学院大学短期再教育プログラム「サイバーセキュリティ技術講座」	主に社会人を対象とする自己研鑽向け	企業等で情報セキュリティを担当している方を対象に、機密情報漏えいなどサイバー攻撃の脅威から企業等を防御するための実践的な知識やスキルを身につけることを目的とした、実習中心の講座
28	情報セキュリティ大学院大学（JMOOC/gacco）情報セキュリティ『超』入門	一般の自己研鑽向け	情報セキュリティ大学院大学によるオンライン大学講座（2015年度）
29	情報セキュリティ大学院大学(JMOOC/gacco)情報セキュリティ初級	一般の自己研鑽向け	情報セキュリティ大学院大学によるオンライン大学講座（2015年度）。以降、官公庁、企業における教育講座として活用されている。

２．２．２ 事例に関する詳細分析

前項に示した事例のうち、モデル・コア・カリキュラムを作成する上で参考になる特徴を有すると考えられる 5 事例について、各実施大学等へのヒアリング調査に基づく詳細分析を行った結果を示す。

（1）事例詳細 1：分野・地域を越えた実践的情報教育協働ネットワーク（セキュリティ分野）（enPiT-Security）

本事例は、我が国の高等教育機関において調査時点で最も大規模に実施されている情報セキュリティ分野の人材育成プログラムである。5 つの連携大学（情報セキュリティ大学院大学、奈良先端科学技術大学院大学、北陸先端科学技術大学院大学、東北大学、慶應義塾大学）を中心にプログラムに参加している大学等がそれぞれ異なる講義を提供し、受講者は開催校への通学または遠隔教育システムを通じて受講する。演習を行う科目については、大学の休暇期間等に集中的に実施される。

本事例における情報セキュリティ教育に関する取組内容の詳細を次表に示す。

表 17　事例詳細 1：分野・地域を越えた実践的情報教育協働ネットワーク（セキュリティ分野）（enPiT-Security）における教育内容の詳細

項目	調査対象事項	調査結果
情報セキュリティ教育の形態		大学院修士課程を主対象とする情報セキュリティ人材育成のためのプログラム（第 2 期からは大学学部等に展開）
対象とする教育レベル		情報系大学院教育（第 2 期は情報系大学学部教育）（専門教育）
教育手法	産学連携教育（講師提供、教材作成、資料提供、等）	・実践教育の実施に向けて、産業界との全国的なネットワークを形成（連携企業 14 社。他にも多数のセキュリティエキスパートが協力） ・産学での実践教育事例の共有、意見交換を行う会合を開催 ・CTF 及び企業インターンシップへの参加を推奨
	実践的教育（PBL、演習、競技形式、等）	・20 を超える短期集中型演習（PBL 演習、セキュリティ技術に関する講義・演習） ・応用学習（最新情報セキュリティ理論と応用、先進ネットワークセキュリティ技術、情報セキュリティ技術特論、セキュア社会基盤論、情報セキュリティ法務経営論）
	ICT 活用（演習環境、遠隔教育、e-ラーニング、等）	・5 大学の連携による幅広いセキュリティ分野の最新技術や知識の体験を通じた習得
具体的な教育の特徴	育成しようとする人材像	社会・経済活動の根幹に関わる情報資産および情報流通のセキュリティ対策を、技術面・管理面で牽引できる実践リーダー
	前提とする知識・スキル	（各大学にて設定）
	修了要件	共通科目（2 単位）・基礎科目（4 単位以上）、実践演習（2 単位）、先進科目（2 単位）を取得した学生を対象に SecCap 認定証を発行（33 ページ図 4 参照）。さらにこれらに加え実践演習と先進科目で 4 単位以上を取得した学生をセキュリティスペシャリスト（SecCap10）に認定。
	対象者の選抜が行われた場合はその方法	（各大学にて実施）
	募集人数、参加人数、修了人数	平成 25 年度の目標育成学生数：60 名→90 名参、65 名を認定 平成 26 年度の目標育成学生数：80 名→109 名参加、84 名を認定 平成 27 年度の目標育成学生数：90 名→129 名参加、113 名を認定 平成 28 年度の目標育成学生数：100 名→146 名参加、130 名を認定
	回数・時間	（大学ごとに設定）
	講義・演習の内容 （H28 年度実績、 32 ページ図 3 参照）	◇ベースラインとしての共通（SecCap 認定の必修）科目 ・情報セキュリティ運用リテラシー ◇基礎科目

項目	調査対象事項	調査結果
		・各大学の既存科目から複数指定 ◇実践力を高める実践セキュリティ演習を開催 ・情報セキュリティ演習（理論系） ・セキュリティ基礎演習（技術系） ・ネットワーク・セキュリティ技術演習（技術系） ・Web アプリケーション検査と脆弱性対策演習（技術系） ・デジタル・フォレンジック演習（技術系） ・CTF 入門と実践演習（技術系） ・CTF 実践演習（技術系） ・無線 LAN セキュリティ演習（技術系） ・システム攻撃・防御演習（技術系） ・システム侵入・解析演習（技術系） ・リスクマネジメント演習（技術系） ・インシデント体験演習（技術系） ・IT 危機管理演習（技術系） ・ハードウェアセキュリティ演習（技術系） ・ネットワーク・セキュリティ演習（技術系） ・インシデント対応と CSIRT 基礎演習（社会科学系） ・組織経営とセキュリティマネジメント演習（社会科学系） ・事業継続マネジメント演習（社会科学系） ◇実践力を補強するための統合的な先進科目 ・最新情報セキュリティ理論と応用（理論系） ・情報セキュリティ技術特論（技術系） ・先進ネットワークセキュリティ技術（技術系） ・セキュア社会基盤論（社会科学系） ・情報セキュリティ法務経営論（社会科学系）
	参加教員数	72 名（H28 年度）
	講師用資料等の作成方法	（各大学にて調整）
評価の仕組み	評価方法	①「情報技術人材育成のための実践教育ネットワーク形成事業委員会」による中間・最終評価 ②enPiT 外部評価委員による評価 ③enPiT-Security アドバイザー委員による助言 ④アンケートによる受講生満足度評価
	評価者 （平成 28 年度）	①enPiT 事業委員会７名（阿草 清滋（南山大）、碓井 誠（オピニオン）、木内 里美（オラン）、重木 昭信（ミライト）、谷口 秀夫（岡山大）、玉井 哲雄（法政大）） ②enPiT 外部評価委員会6名（大島信幸（IPA）、國井秀子（芝浦工大）、筧捷彦（早稲田大）、佐々木良一（東京電機大）、菊池純男（日立）、角田千晴（JUAS）） ③enPiT-Security アドバイザー委員6名（近澤武（三菱電機）、江崎浩（東京大）、田中俊昭（KDDI 総研）、富永哲欣（NTT）、下村正洋（JNSA）、花田径子（岡崎女子大）） ④enPiT-Security 受講生
	客観性を担保するための工夫	外部評価委員会等、種々様々のアドバイス等
質の確保や特色を出すための具体的な工夫や仕組み	カリキュラム設計の意図・背景	実践セキュリティ人材育成に向けて、共通に必要な基礎知識学習、幅広いセキュリティ分野の最新技術や知識を具体的に体験を通して習得できる実践演習、および応用力を高める学習からなるバラエティに富んだカリキュラムを提供。
	教養教育、専門基礎教育、専門教育の間の接続に関する工夫	・SecCap コースが重点をおく実践的な技術演習を受講するために非情報系知識や人文系知識を背景として持つハイブリッド人材に向け入門講座を開設。慶應義塾大学と情報セキュリティ大学院大学の二拠点で開講した。また、東北大学では演習科目「ネットワーク・セキュリティ実践」を非情報系の学生が受講し易い講座内容とし、新規に参加大学に加わった２校から非

項目	調査対象事項	調査結果
		情報系の学部生を受け入れた
	情報セキュリティ分野ではないが、情報セキュリティに関する専門教育を行う上で必要な知識を事前に習得してもらうために実施した調整・工夫等	・自習用教材を配信。 ・講義や演習による理解度向上の程度と受講生から見た難易度を把握するため、各講義や演習でアンケートを実施し、講師へのフィードバックを行う等、講義・演習の改善を図った。
	学生指導に際し、カリキュラム構成の観点から配慮すべき事項	情報セキュリティ・エンジニアとして身に付けるべきセキュリティ技術の基礎力として、OS、ソフトウェア、ネットワークなどのセキュアな構成技術、およびマルウェア対策に関する広範な知識・技術を習得するため、共通科目「情報セキュリティ運用リテラシー」を開講。
	産学連携の際の役割分担、具体的連携内容に関する工夫、配慮が必要であった事項	NTT、IBM、NEC、ネットワンシステムズに連携企業として参画いただき、夏季に開講する集中型の実践セキュリティ演習（ネットワークセキュリティ技術演習、Web アプリケーション検査と脆弱性対策演習、デジタルフォレンジック演習）と、後期開講の先進科目（応用学習）である先進ネットワークセキュリティ技術の実践的な教材開発や演習指導、企業見学等に協力いただいた。
	実施の結果、学生の関心が高かった内容、低かった内容	インシデント対応の現場見学（IBM SOC. NTT 東日本の NOC）、実践セキュリティ演習等、関心が高かった。
	前年度実施経緯を踏まえた見直しや、受講者側からの評価や意見・要望を通じた改善	Web アプリケーション検査演習の演習環境（サーバに対するより現実的な脆弱性の組込）の強化。

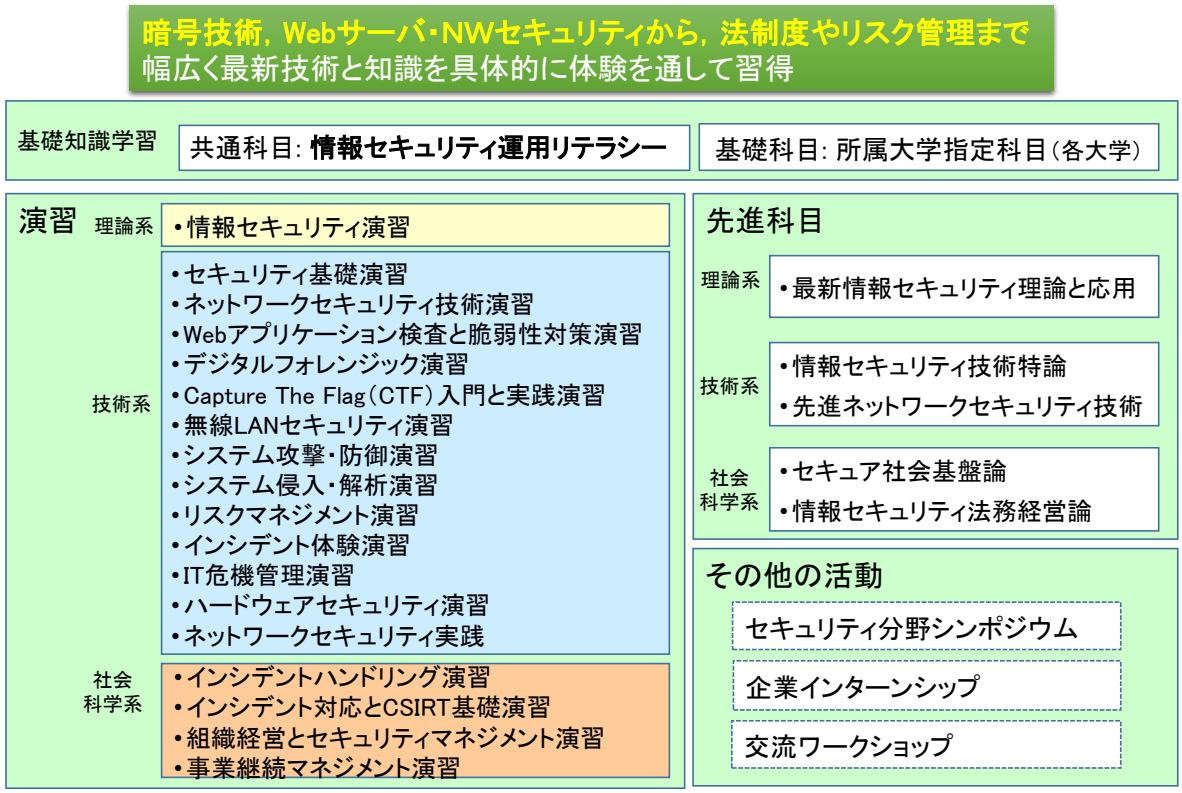

図 3　enPiT Security（SecCap）カリキュラム（平成 28 年度）

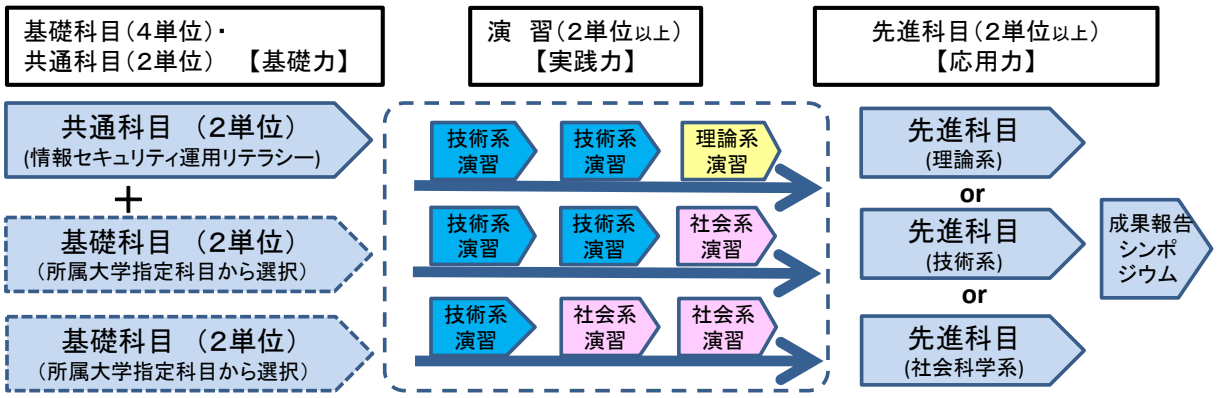

図 4　enPiT Security（SecCap）修了認定の仕組み

（2）事例詳細 2：長崎県立大学 情報システム学部 情報セキュリティ学科

本事例は、大学学士課程において我が国で初めて情報セキュリティ教育を対象として設置された学科である、長崎県立大学情報システム学部情報セキュリティ学科における教育内容を対象とするものである。学士課程教育であることから、情報セキュリティ分野の基礎となる数学的知識や計算機及びネットワークの基盤技術から、様々な専門分野までの教育を 4 年間で行うために工夫が試みられている。

本事例における情報セキュリティ教育に関する取組内容の詳細を次表に示す。

表 18　事例詳細 2：長崎県立大学情報システム学部情報セキュリティ学科における教育内容の詳細

項目	調査対象事項	調査結果
情報セキュリティ教育の形態		情報セキュリティ人材育成のためのコース（大学学部）
対象とする教育レベル		情報系大学学部教育（専門教育、専門基礎教育）
教育手法	産学連携教育（講師提供、教材作成、資料提供、等）	・企業インターンシップを実施。 ・そのほか、長崎県のサイバーセキュリティ研究会と各種の連携を実施。
	実践的教育（PBL、演習、競技形式、等）	・1年次から「情報技術演習」「情報セキュリティ演習」を実施（これらはそれぞれ IT パスポート試験、情報セキュリティマネジメント試験の合格を目指すもの）。 ・CTF、セキュリティキャンプ等への参加を推奨。 ・産業界出身教員の個人的な人脈を活用することで、外部の有識者からアドバイスを得ることはある。
	ICT 活用（演習環境、遠隔教育、e-ラーニング、等）	・演習環境を構築し、2017 年 1 月にリリース予定（インターネットトラフィックのキャプチャやマルウェアの捕獲ができる）。演習環境の日常的な運用は学内情報システム室が行う。演習環境を用いた県内企業との共同研究等も予定。 ・情報処理技術者試験向けの CBT を提供し、学生が自分のアカウントでリハーサルを行える。
具体的な教育の特徴	育成しようとする人材像	情報セキュリティ学科では、情報セキュリティ全般にわたる広い視野と知識を備え、情報セキュリティのプロフェッショナルとして活躍できる人材（情報セキュリティに関する知識や技術を有し、企業や行政などの情報セキュリティ分野で活躍できる人材）を育成する。
	前提とする知識・スキル	高等学校を卒業または同等以上の学力
	修了要件	情報セキュリティ学科では以下の能力等を有し、所定の単位を修得した者に学士（情報セキュリティ学）の学位を授与する: 1. 情報セキュリティ分野において活躍するための基本的な知識や技術 2. 情報技術者として必要なネットワーク、データベース、OS、プログラミング、システム開発等に関する知識や技術 3. 高度情報化社会における諸問題を自ら発見し、解決する能力
	対象者の選抜が行われた場合はその方法	個別学力検査（一般入試）、面接・小論文（特別選抜）
	募集人数、参加人数、修了人数	40 名（一般入試（前期 20 名、後期 8 名）、特別選抜（推薦）12 名）。
	回数・時間	セキュリティ専門科目（必須 11 科目、選択 10 科目）
	演習の内容	・IT パスポート試験、情報セキュリティマネジメント試験の合格を目指した演習の実施（実施中） ・情報システム学部の教員による、学部共通科目としての各種演習（来年度以降実施） ・情報セキュリティ学科の教員による、学科専門科目としての各種演習（再

項目	調査対象事項	調査結果
		来年度以降実施）
	講師用資料等の作成方法	・担当教員が作成。
評価の仕組み（受講者による評価を除く）	評価方法	大学・県の評価審議会による評価。教員評価は研究・社会貢献・学内運営・教育の軸で行われる。
	評価者	
	客観性を担保するための工夫	
質の確保や特色を出すための具体的な工夫や仕組み	カリキュラム設計の意図・背景	情報セキュリティ学科では、教育目標を実現するため、以下のような方針に基づき教育課程を編成： 1. 情報技術者として身につけておくべき知識や技術を修得させるため、学部共通科目して情報数理や IT 技術に関する基本的な科目を配置する。 2. セキュリティに関する知識を深めるため、学科専門科目として情報セキュリティ技術とセキュリティマネジメントに関する科目を配置する。 3. 専門知識を修得しながら、コミュニケーション能力、課題解決能力及び協働する力を身につけさせるため、演習科目を配置する。 4. それまでに学んだ全てを統合し、課題の設定・調査・分析・考察・解決法の提案等の能力を涵養するため、卒業論文の作成を課す。
	教養教育、専門基礎教育、専門教育の間の接続に関する工夫	・専門科目については「手を動かす」機会を増やすことで理解度を高める。
	情報セキュリティ分野ではないが、情報セキュリティに関する専門教育を行う上で必要な知識を事前に習得してもらうために実施した調整・工夫等	・自主的に勉強しようとする、やる気のある学生をできるだけサポートする。学生のコミュニティの中にできる人材がいれば、周りの学生もそれにつられて底上げが図られる効果が期待できる。 ・外部のイベントや勉強会への参加を推奨する。 ・情報分野の必要な知識を習得するようカリキュラムを組んでいる
	学生指導に際し、カリキュラム構成の観点から配慮すべき事項	・低学年を対象とする共通科目については他学部の受講生も対象になることから、わかりやすい内容とする必要がある。 ・情報系の知識は入学時の差が大きい。学生の興味や関心は、大学入学前にどのような経験をしているかに依存する。
	産学連携の際の役割分担、具体的連携内容に関する工夫、配慮が必要であった事項	（これまでのところ未実施）
	実施の結果、学生の関心が高かった内容、低かった内容	・学部学生にとって、マネジメント系の内容は実務経験がないこともあって理解が難しい。 ・技術系の科目については、学生の関心を引きつける工夫は比較的容易。 ・セキュリティ学科を志望した学生であるので、セキュリティに関する内容への関心は高い。
	前年度実施経緯を踏まえた見直しや、受講者側からの評価や意見・要望を通じた改善	（本年度開設のため情報無し）

（3）事例詳細 3：情報セキュリティ大学院大学 情報セキュリティ研究科（修士課程）

本事例は、機関そのものが情報セキュリティ人材育成を目的としている情報セキュリティ大学院大学における、修士課程の教育課程を対象とするものである。

本事例における情報セキュリティ教育に関する取組内容の詳細を次表に示す。

表 19　事例詳細 3：情報セキュリティ大学院大学 情報セキュリティ研究科（修士課程）における教育内容の詳細

項目	調査対象事項	調査結果
情報セキュリティ教育の形態		情報セキュリティ人材育成のためのコース（大学院修士課程）
対象とする教育レベル		情報系大学院教育
教育手法	産学連携教育（講師提供、教材作成、資料提供、等）	・産業界で活躍する専門家を客員教授、連携教授として任用し、実践的内容の講義・演習を実施。
	実践的教育（PBL、演習、競技形式、等）	・enPiT-Security プログラムの併修が可能。
	ICT 活用（演習環境、遠隔教育、e-ラーニング、等）	リアルタイム受講への補完的位置づけとしてのオンデマンド受講等
具体的な教育の特徴	育成しようとする人材像	・エンジニア、システムコンサルタント、アナリスト（技術系：情報セキュリティに関する確かな専門知識と広い視野を備え、セキュアなシステム・プロダクトの設計、開発、構築、提案ができる技術者や、技術面のコンサルティングを担う専門家） ・セキュリティマネージャー、ビジネスコンサルタント（マネジメント系：情報セキュリティに関する総合的な知識を持ち、社会の変動要因や制約条件を踏まえて適正なリスク分析・評価を行い、企業・組織における実効性のある政策提言や人間系セキュリティ対策を担うリーダー）
	前提とする知識・スキル	基本的な IT やコンピュータに関する知識を有することが望ましいが必須条件ではない
	修了要件	（2 年制プログラム） 修業年数 2 年以上（教授会が優れた研究業績を上げたと認めた者については1年以上）、かつ所要単位数：30 単位以上、かつ修士論文審査および最終試験に合格。 （1 年制プログラム） 準修業年限として 1 年以上在学し、研究科が定める授業科目について 46 単位以上修得し、必要な研究指導を受けたうえ、特定の課題についての研究成果の審査及び最終試験に合格
	対象者の選抜が行われた場合はその方法	一般入試：面接（プレゼンテーション含む）および志望理由書、学業成績、小論文等出願書類審査を総合して行う。 社会人入試：面接（プレゼンテーション含む）および研究計画書等出願書類審査を総合して行う。
	募集人数、参加人数、修了人数	4 月入学 2 年制 40 名（ほかに 1 年制、10 月入学にて若干名）
	回数・時間	必修 4 科目、選択 44 科目
	講義・演習の内容 （H28 年度実績から一部抜粋）	・セキュリティ監査 保証型の情報セキュリティ監査に着目して、企業でまず、助言型監査によって問題点を把握して、改善して保証をうけられる準備を行う。次に、保証を受ける事業について言明を作成する。外部監査人は、言明をベースに保証型監査を実施する。このような監査のフローを体験し、監査報告書を策定する。トレーニングと演習を通じて実践的な能力を身につける。また、講義履修と併せて、NPO 日本セキュリティ監査協会が認定する公認情報セ

項目	調査対象事項	調査結果
		キュリティ監査人（補）の受験資格が得られる。 ・情報セキュリティ運用リテラシー 本科目は、夏季の特設実習の基礎となるセキュリティ技術、および、実社会の最前線の技術動向について学ぶオムニバス形式の講義である。前期は 4 回（各 2 コマ）の講義によって、特設実習（セキュリティ実践Ⅰ）の受講に必要な基礎知識を学ぶ。後期は 4 回（各 2 コマ）の講義にて、産業社会の最前線で活躍している外部講師をまねき、特設実習を通して体験的に学習したセキュリティ技術が実社会にどのように役立っているかについて知見を深める。更に、将来に向けて取り組むべきセキュリティ技術について、現状の課題分析をベースに検討する。 ・ハッキングとマルウェア解析 ハッキングおよびマルウェア解析の基礎能力の習得を目的としたもので、前半はハッキングに、後半はマルウェア解析に焦点をあてて実施する。具体的に、ハッキングでは情報収集、脆弱性識別、エクスプロイト、パスワード解読、マルウェア（トロイの木馬，バックドア，ウィルス，ワーム）による攻撃および盗聴の基礎を学び、グループワークも行う。マルウェア解析では、マルウェアの概要と作成、ハニーポットによるマルウェア収集、表層解析、アセンブラの基礎とプログラミング、バイナリファイルの構成、動的および静的解析、アンチ解析技術を修得する。 ・先進ネットワークセキュリティ技術 実社会での活動事例をベースに、特設実習（セキュリティ実践ⅠまたはⅡ）にて体験を通して習得したネットワークセキュリティ技術の実社会での役割と今後の技術展望や課題について学ぶことにより、先進ネットワークセキュリティ技術について理解し応用力を深める。実社会での事例としては、企業組織や官庁・自治体の内部で活動するネットワークセキュリティ事故対応チーム（CSIRT）と、セキュリティベンダー等が提供するセキュリティオペレーションセンター（SOC）サービスを取り上げ、社会における役割と今後の課題について学ぶ。更に、セキュリティ最新事情やマルウェア解析などの最新技術動向について、現場の最前線で活躍する講師によるオムニバス形式の講義により、応用力を高める。 ・セキュア社会基盤論 情報セキュリティに関する法律、経済、経営その他の社会基盤に関する基礎的な知識を習得すると同時に、情報セキュリティにかかわる具体的な問題を解決するための手法を、実際のインシデントに基づくケースやデータベースを利用しながら習得することをねらいとする。情報資産が入っているパソコンの盗難、個人情報の漏洩、プライバシーにかかわる情報の利活用などの具体的なインシデントや事例を想定し、これらに対してどのような法律の規定が適用され、先行事例に対してどのような判決が下されたのか、どのような原因があると考えられるのか、どのようなリスクがありどのようにマネジメントすることが可能か等について、各受講者が実際に調査したりデータ分析を行ったりする演習形式も取り入れ、取るべき対処の方法を具体的に立案する能力を習得していく。 ・サイバーセキュリティ先端特論 サイバーセキュリティに関する先端的な内容について、前半部分の回では組み込み・制御技術のセキュリティやロボット・AI のセキュリティ等の技術問題を中心として取り上げる。後半部分の回では、情報による安全保障、テロ対策、国際関係、サイバー防衛等の問題を取り上げる。なお各領域の専門家をゲストとして招聘することを予定している。 ・セキュリティ実践Ⅰ 技術系、理論系、社会科学系のセキュリティ実践演習モジュールから 2 単位相当分を選択して受講するものである。受講者は、自らが目指す産業界

項目	調査対象事項	調査結果
		が求めるマルチタレント型のセキュリティ人材に向けて、受講する実践演習モジュールを主体的に選択する。 ・セキュリティ実践Ⅱ 特設実習（セキュリティ実践Ⅰ）を既に受講した者または受講見込みの者が、更に 2 単位相当分を選択し、受講するもの。 ・Windows セキュリティ Windows の基本的なセキュリティ機能を学ぶとともに、ハンズオン実習を通じて Windows に対する攻撃と防御を体験することにより、Windows システムを安全に運用・管理するための技能を習得することを目的とする。
	講師用資料等の作成方法	（原則として各講師による）
評価の仕組み	評価方法	各界の有識者からなるアドバイザリーボードを設置し、研究動向並びに教育効果に対する助言・示唆を得てポテンシャルの向上と活性化を図っている。
	評価者 （H28 年度）	縣 公一郎（早稲田大）、猪﨑 哲也（沖電気工業）、石川 明（日立ソリューションズ）、江坂 忠晴（パナソニック）、木谷 強（NTTデータ）、工藤 義一（富士通エフサス）、國井 秀子（芝浦工業大）、黒川 雅夫（神奈川県）、後藤 滋樹（早稲田大）、坂内 正夫（NICT）、佐々木 良一（東京電機大）、佐々倉 秀一（NTTコミュニケーションズ）、篠原 弘道（NTT）、庄司 信一（日本電気）、関口 和一（日本経済新聞社）、土屋 大洋（慶應義塾大）、堤 和彦（三菱電機）、富田 達夫（IPA）、西田 直人（東芝）、服部 桂（朝日新聞社）、森永 公紀（日本放送協会）、渡辺 巧教（横浜市）
	客観性を担保するための工夫	多様な立場にある評価者の委嘱。
質の確保や特色を出すための具体的な工夫や仕組み	カリキュラム設計の意図・背景	情報セキュリティに関する技術や知識は、独立した分野ではなく IT 関連の総合科学の上に成立、すなわち、基礎科学分野の論理数学や電磁気学などから始まって、 コンピュータ、オペレーティングシステム、ソフトウェア、ネットワーク、通信プロトコル、アクセス制御、 運用技術、管理手法、組織論、法律、更には倫理まで、関係する分野は多岐にわたる。これを踏まえて、情報セキュリティに関する教育研究領域を、「技術」「管理運営」「法制度」「情報倫理」の 4 つの観点から捉え、カリキュラムを編成。
	教養教育、専門基礎教育、専門教育の間の接続に関する工夫	情報セキュリティ全般に渡る広い視野と見識を備え、リーダーとして現場における問題解決を担う高度な専門人材を育成するために、以下の 4 つのコースフレームを 2016 年 10 月よりリニューアルした（39 ページ図 5 参照）。 ・数理科学コース：情報セキュリティに関わる、数理的な諸問題を深く理解し、よりよい解決を見出すことで、より効率的でより強力な情報セキュリティを実現するための基盤構築を目指す。講義による知識習得にとどまらず、少人数のセミナーや個別指導を通じて学習・研究を進める。 ・システム・デザインコース：企業・研究機関等で研究開発、ソフトウェア・システム・製品の開発、システムコンサルティング、新事業の立案・企画業務などに従事されている方、あるいは従事することを目指している方を対象とし、OS、ソフトウェア、ネットワーク、システム設計・運用管理などの IT システム技術、およびそれらの安全でセキュアな構成法に関する広範な知識・技術を習得する。さらに、セミナーや個別指導を通じて得られた知識と技術を統合する実践能力を身につける。また、経営管理や法制度等の周辺領域の知識を身につけることで、セーフティ＆セキュリティビジネスの推進に必要な幅広い視野を養う。 ・サイバーセキュリティとガバナンスコース：分析能力を有する専門人材、および、企業や政府自治体においてサイバー攻撃対処を担う SOC/CSIRT 組織を構築・運用するマネージャ人材を育成する。本コースではデジタル・フォレンジックやネットワーク等、サイバーセキュリティの先端技術とともに、実社会におけるサイバー攻撃対処で必要となるセキュリティ関連法制や国

項目	調査対象事項	調査結果
		際動向等の知識を習得することにより、総合的な対処能力を身につける。 ・セキュリティ/リスクマネジメントコース：IT のリスクが重要になる中、リスクを特定して、組織のリスクから情報を適切に保護・管理し、組織の機会につなげるリスクマネジメントを実践する。また、経営者の観点からセキュリティ戦略策定、セキュリティ対策の投資、効果測定、監査などのリスクガバナンスを実践する。リスク分析や対策のマネジメンのみならず、ガバナンスを構築し実践できる人材を育成する。
	情報セキュリティ分野ではないが、情報セキュリティに関する専門教育を行う上で必要な知識を事前に習得してもらうために実施した調整・工夫等	多様なアカデミックバックグラウンドを持つ学生を受け入れることを前提に、博士前期課程においては、それぞれが自身の研究テーマや問題意識に応じて、情報セキュリティに関する高度な知識を学際的に学べるようにするとともに、基礎知識の習得と最新動向の把握にも配慮したカリキュラム編成を実施。より具体的には、暗号、インターネット、情報システム、ソフトウェアなどのセキュリティ関連技術、情報科学、リスク評価、マネジメント理論、組織のガバナンスのあり方、情報モラル、社会制度・法制度等にかかる科目群を情報セキュリティという観点から分野横断的に配置。
	学生指導に際し、カリキュラム構成の観点から配慮すべき事項	（研究科を通じて一様ではないため省略）
	産学連携の際の役割分担、具体的連携内容に関する工夫、配慮が必要であった事項	ISS スクエア（情報セキュリティ大学院大学、中央大学、国立 情報学研究所他、企業・研究機関 11 社の産学連携による高度情報セキュリティ人材育成プログラム。暗号・認証、ネットワーク、システム、ソフト ウェア、マネジメント、法制・倫理までトータルにカバーされた講義群、インターンシップや見学会、企業現場の実務家によるオムニバス講義）
	実施の結果、学生の関心が高かった内容、低かった内容	（研究科を通じて一様ではないため省略）
	前年度実施経緯を踏まえた見直しや、受講者側からの評価や意見・要望を通じた改善	（研究科を通じて一様ではないため省略）

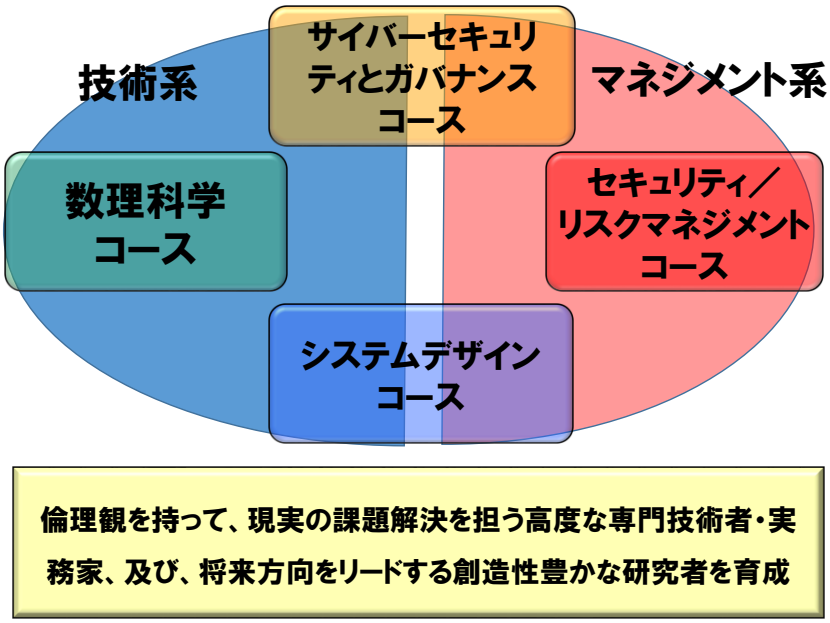

図 5　情報セキュリティ研究科（修士課程）における４つのコース

（4）事例詳細 4：九州大学サイバーセキュリティセンター 富士通スペシャリスト育成研究部門

本事例は、産学連携のもとで情報セキュリティ分野における最新の動向に関する研究開発及び教育を行うための体制（寄付講座）を構築した九州大学サイバーセキュリティセンターを対象とするものである。

本事例における情報セキュリティ教育に関する取組内容の詳細を次表に示す。

表 20　事例詳細 4：九州大学サイバーセキュリティセンター 富士通スペシャリスト育成研究部門

項目	調査対象事項	調査結果
情報セキュリティ教育の形態		情報セキュリティ人材育成のための講義・演習等
対象とする教育レベル		情報系／非情報系大学学部教育（専門教育／教養教育）
教育手法	産学連携教育（講師提供、教材作成、資料提供、等）	富士通寄附講座として講座の運営費用を企業が負担。富士通は教育には直接関与しないが、月１回ミーティングを開催し、同社のセキュリティ担当者からアドバイスを受けている。
	実践的教育（PBL、演習、競技形式、等）	受講生を 2～3 人で構成されるチームに分け、チーム単位で毎回演習を実施。
	ICT 活用（演習環境、遠隔教育、e-ラーニング、等）	演習用 IoT デバイスとして、ビデオカメラによる定点観測システムを想定し、「Web カメラ」＋「Raspberry Pi」＋「Wi-Fi アダプター」による環境を利用。
具体的な教育の特徴	育成しようとする人材像	セキュリティを考慮した「ものづくり」ができる人材を育成する。「ものづくり」にはハードウェア開発などを含む。
	前提とする知識・スキル	プログラミング、ネットワーク、ハードウェアなどの情報科学の基礎的な知識があると理解がしやすい。
	修了要件	期末に実施する試験による。
	対象者の選抜が行われた場合はその方法	なし
	募集人数、参加人数、修了人数	10 名程度（平成 28 年度。講師 1 人で演習に対応できる人数として想定）。受講生として大学学部4年レベルを想定していたが、総合科目としての扱いのため実際には学部1年の受講もある。受講生の半数は工学部電気情報工学科の学生で、それ以外は様々な学部・学科から来ている。
	回数・時間	平成 28 年度後期開講、1 回 90 分全 15 回。
	演習の内容	IoTを用いたシステムのセキュリティについて、ハンズオンによる演習をしながら学ぶ。実際の IoT システムにおいて、IoT デバイスからのデータの収集とデータベースでの管理が重要なポイントなので、それらの脆弱性や攻撃の手法などを教えるとともに、攻撃を避けるためにどのような対策をすればよいかの演習を行っている。
	講師用資料等の作成方法	担当講師（金子晃介准教授）が過去の知見をもとに作成。
評価の仕組み	評価方法	効果測定（選択式試験）を実施。
	評価者	担当講師による。
	客観性を担保するための工夫	講義開始時と終了時、受講者と対照群に対してそれぞれ試験を実施し、教育効果を定量的に測定する。
質の確保や特色を出すための具体的な工夫や仕組み	カリキュラム設計の意図・背景	・近年の電気情報工学科の演習において、実際に手を動かして学ぶ経験が減っており、ソフトウェアなど高いレイヤーでの教育が主体となっている。ハードウェアに近いところでの演習を行うことを通じて、技術がわかる人材を育成したい。 ・学部学生にセキュリティ分野の専門知識を習得してもらうには限界があるが、学生が社会人となり、業務を行う中で「これは大学で学んだあのこと

項目	調査対象事項	調査結果
		か」と思い出してもらえればよい。全員の役に立つわけではないだろうが、セキュリティ業務に携わることになったときに役立ててもらえるようにすることが我々の役目と考えている。
	教養教育、専門基礎教育、専門教育の間の接続に関する工夫	・セキュリティ関連科目を増やしたくても、現在の工学部学生のカリキュラムはぎっしり埋まっており、新たに科目を追加することはできない。そこで既存科目の名称や内容を変えてセキュリティに関する内容を追加することで、必要な知識を習得してもらうことを考えている。
	情報セキュリティ分野ではないが、情報セキュリティに関する専門教育を行う上で必要な知識を事前に習得してもらうために実施した調整・工夫等	・総合科目として実施しているため、前提知識について具体的な指定ができていない。現状では個別の演習課題ごとに必要な知識を習得してもらっている。
	学生指導に際し、カリキュラム構成の観点から配慮すべき事項	・学生の理解度からすれば、今回の演習で対象としている定点観測システムにデータベースシステムが利用されているとは想像もつかない。よってWeb カメラ、無線 LAN、データベースの SQL など個別の脆弱性などを教えるに先立ってシステムの全体像を示し、理解を促すようにしている。 ・学生にはゲーム感覚で楽しんでもらえるように工夫している。学習内容そのものを面白くするアイデアはないが、試験を選択式や正誤問題にするほうが学生の意欲は高まるようだ。
	産学連携の際の役割分担、具体的連携内容に関する工夫、配慮が必要であった事項	・当面は企業の参加を想定せず、九州大学を主体に運営の予定。
	実施の結果、学生の関心が高かった内容、低かった内容	（10 月開講のため、現時点では不明）
	前年度実施経緯を踏まえた見直しや、受講者側からの評価や意見・要望を通じた改善	・今年度の評価結果をもとに改善を予定。
その他	情報セキュリティ教育をとりまく環境など	・本講座の成果は、大学で開催する中高生向けの市民講座などでも活用予定。 ・社会人向けのリカレント教育の必要性は理解しているが、現状でチャネルがないためできていない。実施に向けて、彼らが何を学びたいかについて考える必要がある。 ・現在工学部ではエネルギー分野に注力しており、エネルギーインフラとセキュリティは密接な関係にあることから、今後何らかの協力を行うことになると考えている。 ・本講座が先行することになったが、来年度以降、産業横断サイバーセキュリティ人材育成研究会活動と整合をとり、我々のこれまでの成果を取り込んでもらったり、同成果物で示されているような人材の育成に取り組んだりなどの方向性を探っていきたい。 ・CTF やセキュリティキャンプの活用は計画している。いずれもこれまでの九大生の参加は少ないので、学内 CTF を行った上でキャンプへの応募を促すなど、学生への働きかけを行っていく。関連するサークル活動との連携なども考えたい。

（５）事例詳細５：東京電機大学 国際化サイバーセキュリティ特別コース（CySec）

本事例は、東京電機大学が社会人向けに開講している履修証明プログラムである国際化サイバーセキュリティ特別コース（CySec）を対象とするものである。情報セキュリティ関連業務を担当する社会人が必要とするマネジメント関連の知識を提供することに特徴を有する。

本事例における情報セキュリティ教育に関する取組内容の詳細を次表に示す。

表 21　事例詳細５：東京電機大学 国際化サイバーセキュリティ特別コース（CySec）における教育内容の詳細

項目	調査対象事項	調査結果
情報セキュリティ教育の形態		情報セキュリティ人材育成のためのプログラム（社会人向け履修証明プログラム）
対象とする教育レベル		社会人学び直し
教育手法	産学連携教育（講師提供、教材作成、資料提供、等）	最前線で活躍する産業界講師による講義・演習指導
	実践的教育（PBL、演習、競技形式、等）	双方向対話型ワークショップ形式の演習と、 座学ワークショップを合わせて実施
	ICT 活用（演習環境、遠隔教育、e-ラーニング、等）	・演習用ノート PC 持参を前提 ・CISSP 受験対策のビデオ教材を配信（受講生は自宅でも試聴可）
具体的な教育の特徴	育成しようとする人材像	経営・運営・折衝・監査等も先導可能な高度サイバーセキュリティ専門家の養成（最高情報セキュリティ責任者（CISO）または上級セキュリティエンジニア）
	前提とする知識・スキル	・学部卒業程度の情報セキュリティに関する基礎知識 ・ネットワーク、OS、セキュリティ関連技術に関する学部卒業レベルの知識(1PF) ・分散処理、コンピュータネットワーク、TCP/IP およびセキュリティ関連技術に関する学部卒業レベルの知識(2CD) ・UNIX 系 OS の操作への習熟(2CD) ・プログラミング経験(2CD) ・アセンブリに関する知識(x86) (2CD) ・基本的なプログラミング能力、基礎的な HTML/DB の知識(6DD)
	修了要件	受講開始から 4 年以内に、以下の 6 科目 120 時間以上の学習プログラム（履修証明プログラム）を提供し、修得した者に履修証明書を発行: 「サイバーセキュリティ基盤」(1PF) 「サイバーディフェンス実践演習」(2CD) 「セキュリティインテリジェンスと心理・倫理・法」(3IN) 「デジタル・フォレンジック」(4DF) 「情報セキュリティマネジメントとガバナンス」(5MG) 「セキュアシステム設計・開発」(6DD)
	対象者の選抜が行われた場合はその方法	面接（動機のほか、どの程度の経験・スキルを有しているかも尋ねている）
	募集人数、参加人数、修了人数	10 名程度（2016 年度後期。ただし定員を厳密に制限しているわけではない）
	回数・時間	通常開講では夜間時間（18 時 10 分以降）に週 2 コマ、集中開講では指定した土曜日に 3 コマで実施
	演習の内容	双方向対話型ワークショップ形式の演習と、 座学ワークショップを合わせて実施。

項目	調査対象事項	調査結果
	講師用資料等の作成方法	各講師に任せている。ただし教科書に基づく講義よりもディスカッションが中心となることが多い。
評価の仕組み	評価方法	評価委員会を設置。
	評価者	外部評価者（林　紘一郎（情報セキュリティ大学院大学）、申　吉浩（兵庫県立大）、久保山　哲二（学習院大学）、下村　正洋（JNSA）、辻　ゆかり（情報セキュリティ大学院大学）、神吉　敏雄（MBSD））
	客観性を担保するための工夫	大学院相当のセキュリティ科目としての質の確保と、社会人が学ぶ価値のあるものという2つの観点から教育内容についてのディスカッションを定期的に実施している。
質の確保や特色を出すための具体的な工夫や仕組み	カリキュラム設計の意図・背景	法律・倫理など制度的枠組みに関する理解や、攻撃者の意図や行動に関する洞察、 企業におけるコンプライアンスを実現するためのガバナンスなど、幅広くかつ高度な能力を育成。
	教養教育、専門基礎教育、専門教育の間の接続に関する工夫	（社会人学び直し向けのため対象外）
	情報セキュリティ分野ではないが、情報セキュリティに関する専門教育を行う上で必要な知識を事前に習得してもらうために実施した調整・工夫等	・授業の開始前や資料の末尾などに「参考資料」を示すことで、このレベルの内容を把握していることを前提に進める旨を明らかにしている。受講生はこうした情報を参考に事前学習を行う。 ・社会人向けには学力試験ができないので、どの程度の知識を有しているかを客観的に把握できない。どのような人をターゲットにどのようなレベルの授業を行うかを明確にすることは、教える側、学ぶ側の双方のために必要。
	学生指導に際し、カリキュラム構成の観点から配慮すべき事項	・初年度に専門科目の講義を英語で行ったところ、受講生が理解できなかったため、翌年度は英語の教材を用いて日本語で講義する形に見直している。 ・社会人は熱心に質問するため、質問時間を十分に確保してあっても超過することがあり、その場合は時間通りに終了したい学生にとっては不利益となってしまう。
	産学連携の際の役割分担、具体的連携内容に関する工夫、配慮が必要であった事項	・社会人学び直し向け講座で提供するカリキュラムのうち、大学教員が独自に教えられるものは暗号やネットワークセキュリティなど技術に特化したものが中心であり、脅威やリスク分析に関して教えられるのは教科書的な内容に限られてしまう。産業界講師の参加は必須であり、そうした現場の話を聞くことで大学教員における授業もより実践的な内容にすることができている。
	実施の結果、学生の関心が高かった内容、低かった内容	・職場で必要とする知識を学ぶ目的で、事前知識が必ずしも十分でない状態で出願する人が多い。一方で、どの受講者も情報システムとネットワークに関する知識は習得しており、ネットワークセキュリティの基礎を教える必要は無い。 ・本学でしか提供していない内容（セキュリティインテリジェンスと心理・倫理・法、情報セキュリティマネジメントとガバナンス等）への関心が高く、演習などでもそうしたテーマで盛り上がっている。こうした知見は企業にとっての貴重なノウハウであり、一般に社外に出したがらない傾向がある。そうした内容を実体験を踏まえて聞けるので、受講者にとっての価値が高いのではないか。 ・具体的に手を動かして学べる演習科目の評価は総じて高い。
	前年度実施経緯を踏まえた見直しや、受講者側からの評価や意見・要望を通じた改善	・受講者アンケートの結果を踏まえて、受講生にとって既知の内容などについては翌年のカリキュラムで見直している。 ・幅広い知識を扱う講義が多いので、より深く学びたい、という要望がある。
その他	社会人学び直し向けのモデル・コア・カリキュラムを作成する上でのアドバイス	・受講者の目的に応じて、何にフォーカスするのかいくつかのコースを分ける必要がある。セキュリティに関するすべてを教えるのは現実的ではない。「これだけを知っておけば十分」というものはない。 ・大学発の講座というのは実態に即しておらず、大学という仕組みを使って産業界で学び合う場であるととらえたほうがよい。特定の一企業が主導し

項目	調査対象事項	調査結果
		てもうまくいかないが、大学が主導することで企業も協力しやすいという面がある。 ・産業界講師を確保するには、彼らが何を魅力と感じているかを考える必要がある。講師経験という肩書きが組織内で有利になる場合もあれば、「自分しか知らない知識」を世の中に発信する機会として活用したい、あるいは自分の代わりになる人材を育てたいと思っていることもある。セキュリティ業界の特徴として、ある分野で秀でている人は、学歴や所属に関係なく業界のトップで活躍しているので、能力があることをアピールできる場の提供は、セキュリティ業界において求められていることなのではないか。

「分類」欄凡例:■＝公開情報、※＝当該機関による情報提供、☆＝ヒアリング調査

２．２．３ 調査結果のまとめ

我が国の大学が関与してこれまでに実施された情報セキュリティ教育に関する取組として、27の事例について調査を行い、うち 5 事例についてヒアリング調査を通じた深掘調査を実施した。モデル・コア・カリキュラムが対象とする学士課程、修士課程及び社会人学び直しのそれぞれについて先行する事例が存在しており、実践的教育や産学連携等の実施を通じて産業界が求める人材を育成するための工夫が講じられている。

２．３ 海外における情報セキュリティ教育の動向

海外における情報セキュリティに関する国としての人材育成の方針や考え方の事例とともに、情報セキュリティ分野で著名な大学等を対象として、特色ある人材育成の取組等に関する教育事例について調査した結果を示す。

２．３．１ 公開情報に基づく事例調査

（１）情報セキュリティに関する国としての人材育成の方針や考え方

① 米国

米国では、サイバーセキュリティに関するスキルを備えた人材が官民において大幅に不足している現状を踏まえ、米国を支えるサイバーセキュリティ人材の育成戦略として、2010 年に NICE（National Initiative for Cybersecurity Education）[12]を発表した。これは、サイバーセキュリティ人材の育成を国家課題として、連邦政府機関（国立標準技術研究所（NIST）を中心とする 20 省庁）が協力して教育プログラムを提供することを定めたものである。教育関連では、国立科学財団（NSF）と教育省の主導で、サイバーセキュリティに関連したプログラムを、義務教育、高等教育、職業訓練プログラムにわたって提供することとしている。

このほか、2015 年 3 月に IT 分野のエンジニアの育成のための教育と雇用環境の整備を目的とする TechHire Initiative[13]がオバマ大統領より公表された。この中でサイバーセキュリティはネットワーク運用やプロジェクトマネジメントと並ぶ重要な職種として例示され、大学のみならず、産業界が認定したトレーニングプログラムやブートキャンプ、高度なオンラインコース等でも学ぶ機会を提供することが提唱されている。

大学等を対象とする取組として注目されるのは、政府機関や軍で活躍する人材の育成を目的とした“National Centers of Academic Excellence in Information Assurance / Cyber Defense / Cyber Operation”の指定である。情報保証、サイバー防衛またはサイバーオペレーションに関する教育または研究を行っている教育機関のうち、一定の基準を満たしているものを国家安全保障局（NSA）と国土安全保障省（DHS）が指定する。この指定を受けた教育機関で学ぶ学生は、次の２種類の奨学金を申し込むことができる。

- Federal Cyber Service: Scholarship for Service（CyberCorp）：全米科学財団（NSF）と人事局（OPM）が提供するもの
- Information Assurance Scholarship Program：国防総省（DoD）が提供するもの

これらの奨学金では、大学等の教育機関で必要となる授業料のほか、宿舎や教科書代に加えて給付金も支給される。一方、奨学金を受けた学生には夏期に政府機関で行われるインターン

[12] http://csrc.nist.gov/nice/
[13] https://www.whitehouse.gov/issues/technology/techhire

シップへの参加と、卒業後一定期間にわたる連邦政府または軍における勤務が義務づけられており、給与面で民間に及ばない政府機関が情報セキュリティに関する専門教育を受けた人材を確保するための手段として位置付けられている。

2017 年 3 月時点で情報セキュリティ分野に関するこうした“National Centers of Academic Excellence”に指定されている大学の数と、うちサイバー防衛分野における対象として提示されている教育・研究テーマの一覧を以下に示す。

表 22 “National Centers of Academic Excellence in Information Assurance / Cyber Defense / Cyber Operation”指定機関数

National Centers of Academic Excellence 指定の種類	教育期間	機関数
情報保証に関する教育	4 年	34
	2 年	11
サイバー防衛に関する教育	4 年	134
	2 年	42
情報保証に関する研究		7
サイバー防衛に関する研究		68
サイバーオペレーション		16
上記のいずれか 1 つ以上に指定されている機関数の合計		222

表 23 「サイバー防衛分野」における対象テーマ

サイバー操作	セキュア組込みシステム
データ管理システムのセキュリティ	セキュアモバイルテクノロジー
データセキュリティ解析	セキュアなソフトウェア開発
デジタルフォレンジクス	セキュアな通信
ヘルスケアのセキュリティ	セキュリティインシデント解析と対応
産業制御システム（SCADA）のセキュリティ	セキュリティポリシー開発とコンプライアンス
ネットワークセキュリティアドミニストレーション	システムセキュリティアドミニストレーション
ネットワークセキュリティエンジニアリング	システムセキュリティエンジニアリング
セキュアクラウドコンピューティング	

② 欧州連合（EU）

EU では、2013 年 2 月に“Cyber Security Strategy of the European Union”[14]を公表し、この中で「サイバーレジリエンスの構築」の一環として情報セキュリティ人材の育成の必要性を提示している。これに基づく具体的なアクションとして、EU におけるネットワーク及び情報セキュリティに関する専門機関である ENISA が 2014 年 10 月に"Roadmap for NIS education programmes in Europe”[15]を公表した。これらをもとに、EU 域内では情報セキュリティ人材育成に関して、2016 年末時点において次のような取組が行われている。

- EU 域内の大学等で提供されている NIS（ネットワーク及び情報セキュリティ）関連コースのマッピングと公表
- 既存のトレーニングコースと NIS 業務の市場ニーズとのギャップの調査
- “The European Cyber Security Challenge”の開催（CTF に類似した競技。2016 年は 10 か国 100 名が参加）
- 一般向け啓発用クイズの公表
- ベストプラクティスの共有

また、ENISA では加盟国各国でのサイバーセキュリティ戦略策定を支援しており、この一環としての教育訓練プログラム策定に際し、目的と代表的なタスクを次のように掲げている。

＜教育訓練プログラムの目的＞

- 既存の情報セキュリティ業務担当者の運用能力を強化する
- 学生がサイバーセキュリティ領域に参加するよう働きかけるとともに、同領域で活動するための準備に資する
- 情報セキュリティにおける産学間の連携を促進する

＜代表的なタスク＞

- 各国における情報セキュリティ教育訓練プログラムの立ち上げ
- 産業界の重要ポストで働く人材のセキュリティスキルの認証支援
- 情報セキュリティに関する責任を負う役割とそこで求められる教育的背景に関する一覧の作成
- 大学のカリキュラムへの情報セキュリティコースの追加（コンピュータサイエンスだけでなく、必要性に応じた他の専門領域も対象）
- サイバーセキュリティ分野を教育するスキルを有する認定された専門家の登録制度の構築

[14] http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
[15] https://www.enisa.europa.eu/publications/roadmap-for-nis-education-programmes-in-europe

③ 英国

英国では、2011 年 11 月に“The UK Cyber Security Strategy”[16]を公表し、その中で政府・民間の双方において情報セキュリティ人材が不足しており、これを踏まえた育成の必要性を掲げている。2016 年に公表された同戦略の annual report[17]においては、過去 5 年間の取組の成果（実施予定を含む）として、人材育成関連では以下の事項が示されている。

- 義務教育から中等教育を対象とするサイバーセキュリティ教材の開発と教員向け研修を実施
- 計算機及びディジタル関連の教員資格へのサイバーセキュリティ関連知識の統合
- GCHQ（政府通信本部）等の実習生を対象としたサイバーセキュリティ関連トレーニングの実施
- サイバー侵入アナリストほか、250 以上のサイバーセキュリティ関連の役割を規定
- コンピュータサイエンスと関連コースで学ぶ学生に期待されるサイバーセキュリティ分野のスキルと知識に関して産学官共同にてフレームワークを定義（各大学はこのガイドラインをもとに 2016-17 年にコースを更新予定）
- 次世代の専門家育成を目的として、学部学生を対象にサイバーセキュリティ分野の専門教育を行う“Cyber First”制度を設立
- コンピュータサイエンスまたは関連コースを学ぶ学部学生を対象とするサイバーセキュリティに関するメンタリングとサイバーキャンプを開催
- コンテスト形式の“Cyber Security Challenge UK”を継続開催

2016 年に公表された“National Cyber Security Strategy 2016-2021”[18]では、2021 年に向けて上記の内容に加え次の内容に取り組むことが示されている。

- スキルギャップを埋めるための産官学によるアドバイザリグループの創設
- 14～18 歳を対象とした放課後や夏期スクールによるサイバーセキュリティスペシャリスト育成教育の実施
- エネルギー、金融及び輸送業界における実習生向けトレーニングの実施
- 高いポテンシャルを持つと見込まれる労働者向けのサイバーセキュリティに関する再訓練
- サイバーセキュリティスペシャリストにおけるスキルギャップを埋めるために、大学が担う役割の策定
- 政府におけるサイバーセキュリティに関する方針策定等を担う人材を対象とする国家資格の創設

[16] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
[17] https://www.gov.uk/government/publications/the-uk-cyber-security-strategy-2011-2016-annual-report
[18] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

- 政府と軍をまたがるサイバーセキュリティ分野のセンターオブエクセレンスとしてのサイバー防衛アカデミーの創設
- 初等から大学院レベルにわたる、教育内容へのサイバーセキュリティ及びディジタルに関するスキル開発の取り込み

④ フィンランド

フィンランドは 2013 年 1 月に自国のサイバーセキュリティ戦略として“Finland's Cyber Security Strategy”[19]を公表した。同戦略において、人材育成は社会全体のコンピテンスを高める手段として重視されている。サイバーセキュリティに関する教育は、初等から高等までの教育機関で行うべきものであるとともに、研究開発とイノベーションによるサイバーセキュリティ分野のソリューション開発を促すことも重視されており、こうしたイノベーションへの投資もサイバーセキュリティ分野の人材育成の一環として示されている。

同戦略の実施プログラムでは、国際競争の中でコンピテンスを獲得するために、異なる業種・役割の機関が連携・共同して取り組むべきことが強調されている。具体例として、フィンランドにおけるイノベーション都市プログラムである INKA において、サイバーセキュリティをテーマとしているユヴァスキュラ（Jyväskylä）市において、自治体、州、学術機関、企業（スタートアップ企業、外資系企業を含む）が連携することで、新たなビジネスや国際的な競争優位性を形成することが期待されている。

⑤ イスラエル

イスラエルは近隣の国家の支援を得ることが困難という地政学的な理由により、世界的にも最も早い時期（90 年代後半）からサイバーセキュリティに相当するリスクを認識し、2000 年代初頭には重要インフラのサイバーセキュリティに関するポリシーを策定した。現在は 2011 年 8 月に公表された“Advancing National Cyberspace Capabilities”をもとに同年創設された政府機関 National Cyber Bureau[20]を中心として、サイバーセキュリティに関する施策が実施されている。同機関が行うタスクとして、人材育成関連では次の事項が打ち出されている。

- 専門機関におけるサイバー空間とスーパーコンピューティングに関する研究開発の推進
- サイバー空間に関する国としての教育計画と賢明な利用に関する立案
- サイバー空間における脅威とその対策についての一般向け啓発の推進・強化
- サイバー空間の脅威に関する一般向けの警告と情報（防衛策の実践を含む）の提供
- イスラエルのサイバー産業の振興

---

19 http://www.defmin.fi/en/publications/strategy_documents/finland_s_cyber_security_strategy
20 http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/default.aspx

• 海外の関連機関との連携の推進

（２）情報セキュリティ人材のスキルを測定・評価するための指標

① 米国

上述の NICE のもとで、“Cybersecurity workforce framework” が規定されている。これは、次表に示す 6 種類の職種カテゴリについて、業務を構成するタスクとタスクの実施に必要な知識（Knowledge)・スキル（Skill)・能力（Ability）をそれぞれとりまとめたものである。

表 24　NICE Cybersecurity workforce framework における職種カテゴリ分類

	職種カテゴリ	カテゴリの定義
Ⅰ	セキュアな供給 Security Provision	システム開発の各プロセスに関わる、セキュアな IT システムの構想、設計及び構築
Ⅱ	運用・保守 Operate and Maintain	効果的かつ効率的な IT システムの性能とセキュリティ要件を確保するために必要なサポート、管理及び保守
Ⅲ	保護・防衛 Protect and Defend	IT システム内部やネットワークへの脅威の検知、分析及び被害の緩和
Ⅳ	捜査 Investigate	IT システム、ネットワーク及び電子証跡に関するサイバー攻撃・犯罪への対応
Ⅴ	運用・情報収集 Collect and Operate	インテリジェンス活動に用いられるサイバーセキュリティ情報の高度な収集
Ⅵ	分析 Analyze	サイバーセキュリティ情報の有効性についての高度なレビュー及び評価
Ⅶ	監督と開発 Oversight and Development	サイバーセキュリティ活動を効果的に実施できるようにするためのサポート

米国連邦政府ではこれをもとに、情報セキュリティ分野で次のような「ロールモデル」を策定し、人材の募集や研修に活用している。

- システム運用プロフェッショナル
- データアドミニストレータ
- 計算機ネットワーク防御スペシャリスト
- デジタルフォレンジックとインシデントレスポンスアナリスト
- 情報セキュリティ監査人
- 情報システムセキュリティオフィサー
- 情報システムセキュリティマネージャー
- 情報セキュリティアーキテクト
- リスク・脆弱性アナリスト
- ソフトウェアディベロップメント

• 情報システムセキュリティエンジニア
• 戦略計画・ポリシー開発プロフェッショナル
• CISO（最高情報セキュリティ責任者）

② 欧州連合（EU）

参加各国の IT スキル標準等を相互参照するためにフレームワークとして、2008 年に“European e-Competence Framework”（e-CF）が策定されている。これをもとに、欧州標準化委員会（CEN）が“European ICT Professional Profiles”[21]として 23 種類の職種を定義の上公表しており、うち以下の２種類が情報セキュリティ関連の専門職種に該当する。

• ICT セキュリティマネージャー
• ICT セキュリティスペシャリスト

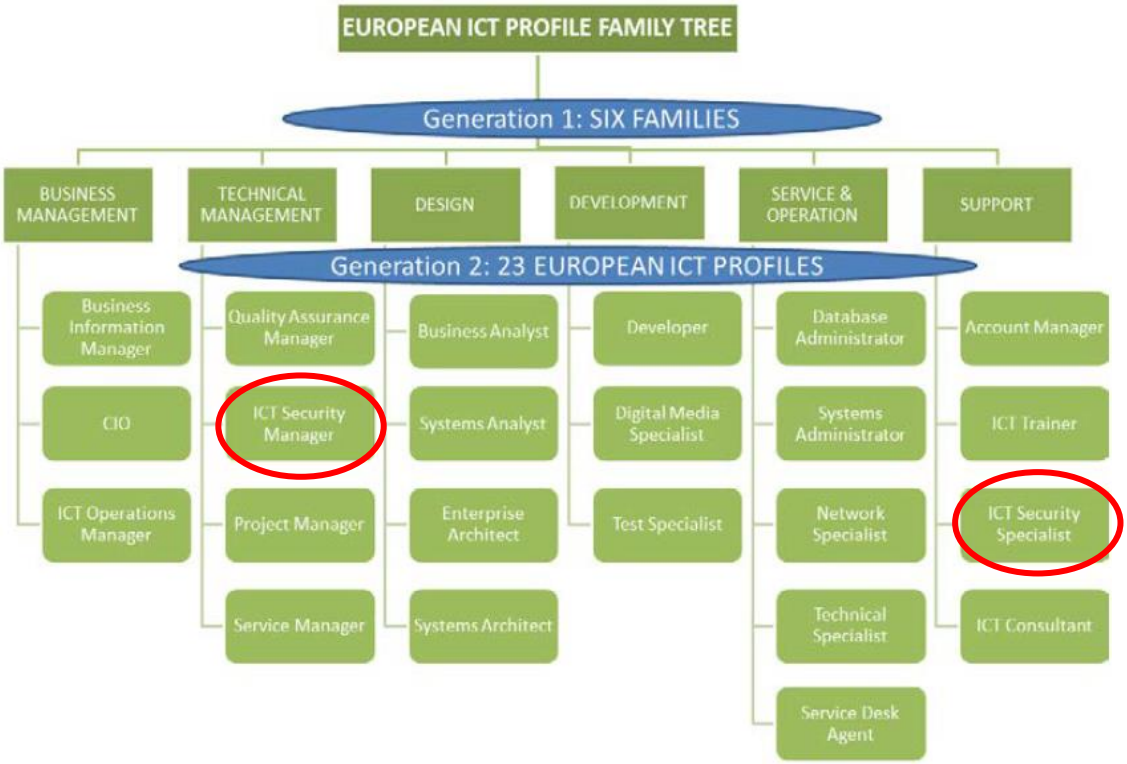

図 3　European ICT Professional Profiles の構造図

③ 英国

情報システムに関する管理業務と作業を対象に、必要とされるスキルと責任レベルを明確化

[21] ftp://ftp.cen.eu/CEN/Sectors/List/ICT/CWAs/CWA%2016458.pdf

することを目的として、SFIA（Skills Framework for the Information Age）が SFIA Foundation によって公表されている。最新版は 2015 年 6 月に公表された第 6 版である。SFIA では情報システムに関する業務を 6 種類のカテゴリに分類し、7 段階のスキルレベルに応じて役割のマッピングを行っている。情報セキュリティ専門の役割として、以下の 3 種類のカテゴリに合計 7 種類の役割が割り当てられている。e-CF で定めるレベルとの互換性はないが、対応関係表を提供することで便宜が図られている。

- 戦略とアーキテクチャ
  - 情報セキュリティ
  - 情報保証
- 展開及び運用
  - セキュリティ管理
  - 侵入テスト
  - インシデント管理
- スキル及び品質
  - 安全性評価
  - デジタルフォレンジック

（3）情報セキュリティ人材の資格・認定制度

国際的に運用されている制度が多いことから、運用団体ごとに整理する。

① International Information Systems Security Certification Consortium（(ISC)²）

- CISSP（Certified Information Systems Security Professional）

  情報セキュリティの専門家を認定することを目的とした資格であり、ISC²が定める情報セキュリティ分野を対象とする Common Body Knowledge（CBK）の 10 分野を理解していることを前提に、業務経験や倫理規約への合意等をもとに認定を行う。情報セキュリティ分野の採用時の条件として最も活用されることが多い資格とされ、2015 年 3 月時点で是世界各国に 97,000 名以上の資格保持者を有する。

- SSCP（Systems Security Certified Practitioner）

  情報セキュリティを専門としていない人材を対象に、情報セキュリティの専門家や経営者と情報セキュリティに関するコミュニケーションを図ることができる能力を認定することを目的とした資格である。米国国防総省における昇任条件等での活用例もある。

- SSLCP（Certified Secure Software Lifecycle Professional）

ソフトウェアの要件定義から保守・破棄に至るすべてのライフサイクルを対象とするセキュリティ対策に関する知識要件を有することを認定する、ソフトウェア開発におけるセキュリティ対策に携わる者を対象とする資格である。

② Information System Audit and Control Association（ISACA）

• CISA（Certified Information Systems Auditor：公認情報システム監査人）

情報システムの監査及びセキュリティ、コントロールに関する高度な知識、技能及び経験を有する専門家であることを認定する資格であり、5 年程度の実務経験を有することが前提となっている。

• CISM（Certified Information Security Manager：公認情報セキュリティマネージャー）

情報セキュリティ分野のうち、マネジメント系に特化した資格であり、セキュリティガバナンス、コンプライアンス、インシデント管理等を対象とする。

③ SANS Institute

• GIAC（Certified Information Systems Security Professional）

情報セキュリティの分野において必要な知識やスキルを、当該個人が有していることを証明することを目的とする資格であり、対象とする専門分野（セキュリティ管理、フォレンジックス、マネジメント、監査、ソフトウェア、法制度）に応じて多くの試験区分が設けられており、さらに基礎（Essential）区分がある。実務経験を求めていない点が特徴である。

④ The Computing Technology Industry Association（CompTIA）

• CompTIA Security+

セキュリティエンジニアの基本レベルのスキル及び知識を有することを認定する資格であり、ネットワーク、暗号技術、業務・組織運営におけるセキュリティに関する知識と改善能力、問題解決能力を問う試験が用いられている。

⑤ The International Association of Privacy Professionals（IAPP）

• CIPP（Certified Information Privacy Professional）

情報のプライバシー管理に関する資格認証を行うものであり、法規制、プライバシーの概念、データの扱いなどを対象とする。プライバシーに関する非営利組織 IAPP が運営しており、現時点で日本語での案内はないが、日本国内での CBT 方式での試験も実施されて

いる。

（4）情報セキュリティ教育を対象とするカリキュラム等（自組織向けを除く）

① The Institute of Electrical and Electronics Engineers, Inc.（IEEE）

現在策定中の“Computer Engineering Curricula 2016”において、計算機工学を学ぶ学部学生向けのカリキュラムのガイドラインを作成しており、この中で「情報セキュリティ」科目案が提示されているほか、他科目のシラバスにおいてもセキュリティに関する内容を扱うことを求めている。

表 25　CE-SEC “Information Security”（全 20 回）

CE-SEC-1	歴史と概要（2 回）
CE-SEC-2	関連するツール、標準、技術的制約（2 回）
CE-SEC-3	データセキュリティと完全性（1 回）
CE-SEC-4	脆弱性：技術的要素と人間的要素（4 回）
CE-SEC-5	資源保護のモデル（1 回）
CE-SEC-6	共通鍵暗号と公開鍵暗号（3 回）
CE-SEC-7	メッセージ認証符号（1 回）
CE-SEC-8	ネットワークとウェブセキュリティ（3 回）
CE-SEC-9	認証（1 回）
CE-SEC-10	トラステッドコンピューティング（1 回）
CE-SEC-11	サイドチャネル攻撃（1 回）

２．３．２ ヒアリング調査による深掘調査

前述の事例のうち、情報セキュリティ分野で著名な３大学を対象に、内容の深掘のためのヒアリング調査を実施した結果を示す。

（１）ロンドン大学ロイヤルホロウェイ校（英国）

① ロンドン大学ロイヤルホロウェイ校情報セキュリティグループについて

ロンドン大学ロイヤルホロウェイ校情報セキュリティグループ（以降 ISG と表記）ISG は、1992 年に世界で初めて情報セキュリティを学問として大学のプログラムに取り入れたことで世界的に知られている。英国内においては、情報セキュリティ研究・教育の主導的役割を担い続けており、国策との関わりも非常に深い組織である。

② カリキュラム作成時のリファレンスや意識した資格等

GCHQ によるサイバーセキュリティ MSc の認定制度がある[22]。しかし、この認定制度は制度設計時に ISG 古参の教員が中心的役割を果たしたこともあり、そもそも ISG のカリキュラムがベースとなっている。したがって、GCHQ による認定制度のリファレンスが ISG カリキュラムであり、逆もまた同様と言える。なお、2016 年 5 月の段階で、英国内大学院の 8 コースがフル認定(内 2 が ISG)を、12 コースが仮認定(内 1 が ISG)を取得済みである[23]。

③ カリキュラム構成上、実践力養成のためにしている工夫

オプション講座の Software Security と Security Testing Theory and Practice，Digital Forensics は、各々チュートリアルとハンズオンで構成されている。ただし、いずれの科目も成績評価が困難であり、課題となっている。現状では、ハンズオン系の講座は現状上記のみであるが、増強への要請が年々高まっている。

④ 産業界や官公庁とどのように協力しているか

第一に、ハンズオン系講座への講師派遣を依頼している。専任の教員は主に基礎理論を担当し、実践力が重要となるハンズオンは、多数の修了生を含む現職の専門家が担当することが多い。第二に、カリキュラム委員会への協力・助言を依頼している。ISG では、3-4 年毎に、カリキュラム委員会によるカリキュラムの更新を行っている。また、カリキュラムの更新に備えて、多数の修了生を中心に、学術界有識者や産業界上級職者へのヒアリングを定期的に実施している。

---

[22] Education and research - NCSC Site: https://www.ncsc.gov.uk/education-research
[23] GCHQ-certified degrees - NCSC Site: https://www.ncsc.gov.uk/information/gchq-certified-degrees

（２）ユヴァスキュラ大学（フィンランド）

① ユヴァスキュラ大学情報科学学部サイバーセキュリティ学科について

ユヴァスキュラ大学情報科学学部サイバーセキュリティ学科（以降 CyberSec と表記）は、フィンランドのサイバーセキュリティ戦略の中核を担っている。これまでの具体的な活動例を次表に示す。

表 26 The Cyber Security evolution in the University of Jyväskylä

期間	プロジェクト
2009-2010	Basics of the Cyber Security education research report
2011-2012	Central Finland ICT-strategy, Central Finland Security Program, Cyber Security Theme courses
2013	Finland's Cyber Security Strategy, INKA Cyber Security Program, Cyber Security Theme courses
2014	Finland's Cyber Security Strategy Implementation, INKA Cyber Security Programme Implementation, Cyber Security of Science Program, Cyber Security Doctral Program, ICT 2023 programme: Information Security, Cyber Trust Program
2015-2017	Finland's Cyber Security Strategy evaluation, Cyber Security Education development: PD, MBA, International Cyber Security cooperation, New Cyber Security research programs, IBM Watson Academic Initiative

② CyberSec におけるサイバーセキュリティ教育の内容について

Postgraduate と Doctoral レベルのコースがある．2017 年 5 月にサイバーセキュリティ教育プログラムの改変を行う予定で、これに向けて英語版シラバスも準備済。CyberSec には、Cyber Security Technology Profile と Cyber Security Management Profile の２プロファイルがある。各プロファイルともに、"Mandatory Courses"、"Theme Courses"、"Master's Thesis"、"Secondary Subject Studies"、"Optional Studies"から構成され、これに加えて、Technology Profile には"Project Studies"が、Management Profile には"Optional elective courses"がある。なお、現時点では、非専門家(学部生)向けの講座はない。カリキュラム作成時のリファレンスや意識した資格等は特に存在せず、学生は、フィンランドのサイバーセキュリティ関連ノウハウの蓄積に資するテーマで修士論文を書く。

CyberSec で開講している講義科目名は以下の通りである。

- Society and Information Security

- Cyber world and Security
- Anomaly Detection
- Cyber World and International Law
- Introduction to cyber conflict
- Cyber defence strategy analysis
- Advanced Anomaly Detection
- Advanced Persistence Threat
- Operating system security 1
- Operating system security 2
- Software Security
- Cyber Attack and it's protection
- System vulnerabilities
- Information Security Management
- Advanced Course on Information Security Management
- Information privacy
- Network Security
- Requirements Engineering

③ 産業界や官公庁との協力について

ユヴァスキュラ大学は、サイバーセキュリティの MSc と PhD プログラムを持つフィンランドで唯一の大学であり、フィンランドのサイバーセキュリティエコシステム内で重要な役割を担っている。このエコシステムは、150 以上のアクティブな企業と 2000 以上の組織拠点からなる。

このエコシステムに含まれる組織例は以下の通りである。

- Air Force Academy
- Air force Command Finland
- JAMK Unifersity of Applied Sciences
- Finish Defence Forces CS Agency, Cyber Division
- Finish Defence Forces Intelligence Agency
- Valtori, Government ICT Centre
- ERILLISVERKOT, State Security Networks Ltd.
- AIRBUS, DEFENCE & SPACE
- descom
- digia

- Relator
- IXONOS
- FUJITSU
- MAGISTER
- KILOSOFT
- SPARTA
- FICONIC

（3）ベングリオン大学（イスラエル）

①　イスラエルの情報セキュリティ教育について

イスラエルにおける情報セキュリティ教育に関して、ベングリオン大学に対してヒアリング調査を行った結果を以下に示す。

- イスラエルではあらゆる学生は 18 歳になると 3 年間の兵役に行くことを義務付けられている。従って、日本を含む先進国であれば大学等で高等教育を受ける年代を、イスラエルの若者は軍人として過ごす。他国と高等教育について比較するのであれば、イスラエルの場合はこの前提に留意する必要があろう。
- イスラエルの若者に対する高等教育は、兵役中に行われる。中でもサイバーセキュリティに関する高等教育は、いわゆるサイバー攻撃を専門とする 8100 部隊、諜報を専門とする 8200 部隊、衛星通信等無線傍受を専門とする 9000 部隊等で実施されている。これらサイバーセキュリティ関連部隊に配属される若者は、事前の知能検査で非常に優秀な成績をおさめたトップレベル人材であり、イスラエルの兵役システムでは、はじめにパイロット特性をもつものが空軍に、知能検査優秀者がサイバーセキュリティ関連部隊に選抜される。
- また、さらにごく一部の若者について、兵役につくことを遅らせ、特別な英才教育を施すことが行われており、サイバーセキュリティ向けの最上位のプログラムは、タルピオットと呼ばれている。タルピオット・プログラムに選抜されるのは、毎年 18 歳になる若者約 100,000 人のうちで 50 人のみである。これらの若者には物理学とコンピュータサイエンスの英才教育が施される。また、次点のサイバーセキュリティ向けプログラムに、プサゴットもある。プサゴット・プログラムには、毎年約 200 人が選抜され、選抜された若者に対しては徴兵を延期し、その後の 4 年間で二つの学位(物理学と電気工学またはコンピュータサイエンスと電気工学)を取得させる。

② ベングリオン大学について

ベングリオン大学（BGU）は、テルアビブ大学、イスラエル工科大学、エルサレム工科大学

等と共に、イスラエルのサイバーセキュリティ研究・教育の一翼を担っている。BGU は、イスラエル南部の都市ベエルシェバにあり、ここでは、軍のサイバー研究施設や研究開発特区、イスラエル国家サイバー局のオペレーションセンター等を集積する「サイバースパーク」が建設途上にある。BGU でのサイバーセキュリティ研究・教育は、研究や教育に利用する素材やデータのみならず、学生や教職員がサイバースパーク内を頻繁に流動することで、常に最新・最先端の内容を維持できるように設計されている。

BGU でのサイバーセキュリティ教育の特徴は、サイバースパークを通じた流動的で柔軟かつ実践的な研究・教育であり、産業界と、防衛を主とする政府組織と連携することで、イスラエルが国家として推進するサイバーエコシステムの核となっている。このサイバーエコシステムの中には、上述したイスラエル軍の各サイバー関連部隊も含まれており、全てのサイバー関連部隊がサイバースパーク内または近隣に大規模な研究拠点を構えている。このような背景の中での BGU の重要な役割のひとつは、兵役を終えたサイバー関連部隊の技術者を学生として受け入れ、彼らが自身のノウハウをビジネス化する手助けをすることにある。従って、BGU は、上述したテルアビブ大学等他の大学と比べると、基礎的・学術的な研究や教育よりも実用化を大前提とする応用的な研究を主体とする大学であると言える。例えば、BGU のサイバーセキュリティ修士課程コースがスタートしたところであるが、これはイスラエル人向けのコースではなく(イスラエル人向けの教育は上述した通り)、イスラエルの持つサイバーセキュリティ教育ノウハウを外国人向けにカスタマイズしてビジネス化した意味合いもある。

２．３．３ 調査結果のまとめ

諸外国の高等教育機関における情報セキュリティ人材の育成動向について調査を行った。米国、EU（フィンランドを含む)、英国、イスラエルのそれぞれにおいて、大学を巻き込んだ形で情報セキュリティ人材に関する政府機関主導の育成プログラムが存在する。あわせて、情報セキュリティ人材のスキルを測定・評価するための指標が提供されており、国をまたがるものとしては EU 参加国向けの European ICT Professional Profiles、民間資格の CISSP（Certified Information Systems Security Professional）などが活用されている。情報セキュリティ分野で顕著な 3 大学を対象とする深掘調査では、大学への講師派遣をはじめとする産学官連携が工夫されている様子が示された。

２．４ 大学における情報セキュリティ教育に対する産業界からの要望

文献調査及びアンケート調査をもとに、モデル・コア・カリキュラムに対する産業界からの要望に関する調査を行った結果を示す。

２．４．１ これまでの調査における産業界から大学への要望

過去に実施された情報セキュリティ人材を対象とする調査として、最新の事例を示す。

① IT 人材白書（独立行政法人情報処理推進機構）[24]

毎年 IT 人材に関するアンケート調査（IT ベンダ、ユーザ企業、教育機関を対象）を実施しており、その結果を掲載している。情報セキュリティ人材を対象とする項目もあり、産業界の現状において人材不足の傾向にあることが示されている。2016 年版における調査項目のうち、「産業界が教育機関に対して最も重視してほしいと考えている技術分野」として取り上げられている調査結果を次図に示す。

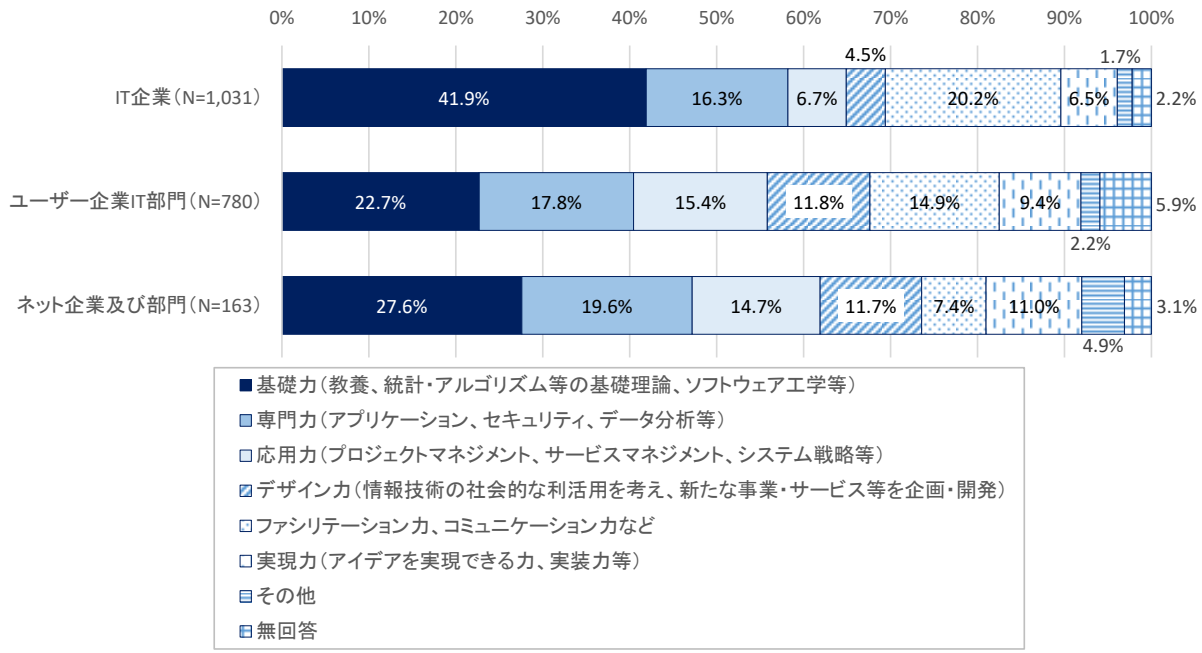

図 4　産業界が教育機関に対して最も重視してほしいと考えている技術分野[25]

これによれば、IT 企業は基礎力への期待が圧倒的に高く、次いでファシリテーション力、コミュニケーション力が続き、情報セキュリティ分野を含む専門力は 3 番目に多い回答となっている。こうした背景として、IT 企業では専門的な知識やスキルについては社内での育成が前提なっており、教育機関には企業が教えにくい基礎力やファシリテーション、コミュニケーショ

[24] PDF 版は右サイトより無料でダウンロード可能：https://www.ipa.go.jp/jinzai/jigyou/about.html
[25] IT 人材白書 2016（独立行政法人情報処理推進機構 IT 人材育成本部, 2016 年発行）の図表 5-1-22 よりデータを引用

ンなどの能力育成に期待していることが推測される。一方、ユーザ企業の IT 部門やネット企業及び部門においては、専門力への期待も相対的に大きく、基礎力に次いで 2 番目の位置を占める。これらの企業においては、IT 企業と比較して自社での育成機能が十分でなく、専門性を身につけた人材を外部から確保するニーズが高いことがうかがえる。

② IT ベンチャー等によるイノベーション促進のための人材育成・確保モデル事業（経済産業省）[26]

自社向けの情報セキュリティ対策業務に従事する人材と、社外向け情報セキュリティ対策業務に従事する人材の調査時点における人材数と不足数の推計を行っている。これによれば、自社向けに従事している情報セキュリティ人材の数は約 24 万人、社外向けに従事している情報セキュリティ人材の数は約 9,400 人と推計され、自社向け人材の不足数は 3～22 万人と見積もられている。

２．４．２ 情報セキュリティ分野の専門家が産業界で活躍するために必要なスキル

産業界において作成された情報セキュリティ人材が備えるべきスキルに関する複数の情報源をもとに、情報セキュリティ分野の専門家が産業界で活躍するために必要なスキルの一覧をとりまとめた結果を示す。

（１）情報セキュリティ人材が備えるべきスキルに関する情報源

情報セキュリティ人材が備えるべきスキルを示した情報源として、本調査では以下の 3 種類を扱うこととした。

① 産業横断サイバーセキュリティ人材育成検討会報告書[27]

産業横断サイバーセキュリティ人材育成検討会は、今後大幅な不足が見込まれるサイバーセキュリティ人材（サイバー空間におけるセキュリティ対策を実践できる人材）の確保（育成と雇用）に向け、重要インフラ分野を中心とした日本の企業が結集し協力し合い一丸となって取り組むことを目的として 2015 年 6 月に発足した。本項に示す報告書は同検討会における第一期の成果である、日本企業（特にユーザ企業）の組織構造とセキュリティ業務との関係に関する実態把握と、主に産業界共通の情報システム部門領域を対象とした人材定義の成果をとりまとめ、2016 年 9 月に公表したものである。うち付録 D において、「産業横断 人材定義リファレンスに基づくスキルマッピング」として、こうした取り組みの成果物である業務に関する要求知識と業務区分に基づく人材の定義を、iCD[28]におけるスキルディクショナリにマッピングした形式で公表している。

---

[26] http://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_fullreport.pdf
[27] http://cyber-risk.or.jp/sansanren/index.html
[28] i コンピテンシディクショナリの略。独立行政法人情報処理推進機構（IPA）が IT 関連に限らない企業活動に求められるタスク（業務）とスキル（能力）をそれぞれディクショナリと呼ばれる表形式に体系化した資料として公表しているもの。右のサイトよりダウンロード可能：https://icd.ipa.go.jp/icd/

② セキュリティ知識分野（SecBoK）人材スキルマップ 2016 年版[29]

特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）が、産学官における情報セキュリティ分野の有識者で構成される会議体での検討結果をもとに、情報セキュリティ業務の現場の感覚をもとに、現在最も不足している情報セキュリティ人材に関する 16 種類の役割に求められる知識項目を整理して 2016 年 4 月に公表したものである。知識項目の整理体系は、米国の国立標準技術研究所（NIST）にて作成された NICE Cybersecurity Workforce Framework がベースとなっており、米国における情報セキュリティの現場で必要とされる知識やスキル、能力に関する項目が盛り込まれている。本調査の実施に際しては、同協会の協力を得て、SecBoK と iCD におけるタスクディクショナリとの対応関係を整理した資料を提供いただいた。

③ 情報処理安全確保支援士試験シラバス[30]及び資格更新研修カリキュラム

国家資格「情報処理安全確保支援士」制度は、サイバーセキュリティに関する専門的な知識・技能を活用して企業や組織における安全な情報システムの企画・設計・開発・運用を支援し、また、サイバーセキュリティ対策の調査・分析・評価を行い、その結果に基づき必要な指導・助言を行う人材の育成と確保を目的として、2016 年に創設された。情報処理安全確保支援士試験のシラバスは、こうした資格取得を目指す人材が備えるべき知識・技能の細目を示すものである。また「情報処理安全確保支援士」は、3 年毎の資格更新となっており、それに伴い年に 1 回の遠隔演習と、3 年に 1 回の集合研修が義務づけられているため、その講習体系および講習資料も参考資料として大いに役立つものである。

（２）必要なスキルの抽出方法

（１）に示した 3 種類の情報源をもとに、次の手順にて抽出を行った。

- 産業横断サイバーセキュリティ人材育成検討会のスキルマッピング及び SecBoK では、いずれも iCD のタスクとの対応関係を示していることから、情報セキュリティ人材が実施できるようになるべきタスクを iCD のタスクディクショナリをベースにとりまとめ、iCD が提供する連係表より求められるスキルに変換した。
- 情報処理安全確保支援士のシラバスについては、IPA がスキルとの対応表を提供していることから、これを用いて必要となるスキルを抽出し、前項の結果との和集合により情報セキュリティ分野の専門家が産業界で活躍するために必要なスキルの一覧をとりまとめた。

この手順を次図に示す。

[29] http://www.jnsa.org/result/2016/skillmap/
[30] https://www.jitec.ipa.go.jp/1_13download/syllabus_sc_ver1_0.pdf

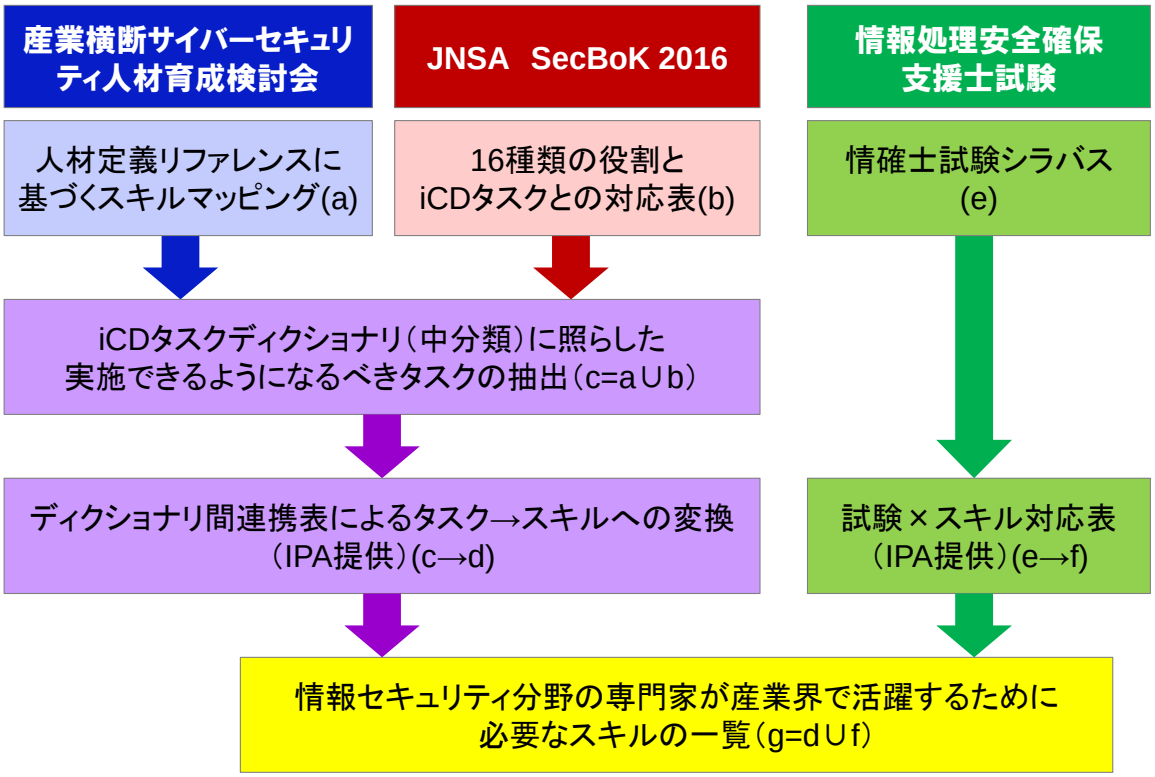

図 5　必要なスキルの抽出手順

（3）抽出結果

（2）の手順により、次表に示すスキルが抽出された。なお、ここに示す内容のすべてが大学における教育に求められるわけではなく、産業界における業務経験等を通じて習得することが適切なものも含まれる。

表 27　情報セキュリティ分野の専門家が産業界で活躍するために必要なスキルの一覧

メソドロジ	戦略	市場機会の評価と選定 製品・サービス戦略 システム戦略立案手法
	企画	システム企画立案手法 要求分析手法 非機能要件設計手法
	実装	アーキテクチャ設計手法 ソフトウェアエンジニアリグ手法 カスタマーサービス手法 データマイニング手法 見積り手法 プロジェクトマネジメント手法
	利活用	サービスマネジメント サービスの設計・移行 サービスのマネジメントプロセス サービスの運用

	支援活動	品質マネジメント手法 リスクマネジメント手法 IT ガバナンス 資産管理手法、 ファシリティマネジメント手法 事業継続計画 システム監査手法、 標準化・再利用手法 人材育成・教育・研修 情報セキュリティ チェンジマネジメント手法
テクノロジ	システム	ソフトウェアの基礎技術 ソフトウェアの構築技術 ソフトウェアの利用技術 データベースの基礎技術 データベースの構築技術 データベースの利用技術 プラットフォームの基礎技術 プラットフォームの構築技術 プラットフォームの利用技術 ネットワークの基礎技術 ネットワークの構築技術 ネットワークの利用技術 クラウドコンピューティングの基礎技術 クラウドコンピューティングの構築技術 クラウドコンピューティングの利用技術
	開発	システムアーキテクティング技術 システム開発管理技術、
	保守・運用	IT サービスマネジメント業務管理技術 IT サービスオペレーション技術 システム保守・運用・評価 障害修理技術 ファシリティ設計技術、 サポートセンター基盤技術
	非機能要件	非機能要件（可用性、性能・拡張性、運用・保守性、移行性） セキュリティの基礎技術 セキュリティの構築技術 セキュリティの利用技術
	組込み・計測・制御	組込みの基礎技術、組込みの利用技術 ヒューマンインターフェース技術 計測・制御技術
	共通技術	IT 基礎
関連知識		ビジネスインダストリ 企業活動 法規・基準・標準

２．４．３ 産業界へのアンケート調査結果

産業横断サイバーセキュリティ人材育成検討会の協力を得て実施された、同検討会会員企業を対象とする情報セキュリティ人材の育成に関して大学に期待する内容についてのアンケート調査の結果を示す。同検討会会員企業へのアンケート調査における質問項目は次表の通りである。

表 28　アンケート調査における質問項目

(1)「突出した知識・能力を有する人材」のためのカリキュラム策定に向けて
① 我が国が必要とするセキュリティ人材像
② 大学や大学院での教育に期待する内容
(2)「情報セキュリティ関連業務を専任する人材」のためのカリキュラム策定に向けて
① 自社での必要性と必要人数、充足状況
② 業務で担う役割の種類について、現状または意見
③ 業務で必要となる知識・スキル・コンピテンシーについて、現状または意見
④ 育成に関する役割分担（自社で行う部分、大学・大学院に期待する部分）
(3)「情報セキュリティ関連業務を専任としない人材」のためのカリキュラム策定に向けて
① 業務で担う役割の種類について、現状または意見
② 業務で必要となる知識・スキル・コンピテンシーについて、現状または意見
③ 現在の人材における知識・スキル・コンピテンシーの充足状況
④ 情報セキュリティ分野の知識・スキル・コンピテンシーに関して大学に期待する内容
(4) 採用・雇用の観点について
① キャリアパスに関する意見
② ジョブローテーションに関する現状または意見
③ 採用やリクルートのシーンで必要となる、人材を表現する言葉や指標
④ 採用やリクルート、キャリアパス、人材育成の問題における地方の活用

以下、調査結果を要約したものを示す。

（１）「突出した知識・能力を有する人材」のためのカリキュラム策定に向けて

① 我が国が必要とするセキュリティ人材像

得られた回答において、情報セキュリティ技術に関して突出した能力を求める意見は皆無であった。代わりに次のような能力に優れた人材への期待が示されている。

- ネットワーク、データベース、OS など、多岐に渡る幅広い知識を有する人材
- 習得した知識を活用して、状況に応じた対策・解決策を考えられる人材
- 語学力とコミュニケーション能力のある人材
- 所属組織の内外から信頼される人材

- 高い倫理観と強い正義感、愛国心を持っていて犯罪や社内外での不正行為を起こすことのない、安心して採用できる人材

また、人材像を定めるに際して、国内外の人材像定義との整合性の確保や合意形成を求める意見も示されている。

② 大学や大学院での教育に期待する内容

即戦力を求める意見と、大学ならではの教育に期待する意見に分かれている。前者の例として、次のような要望が示されている。

- 理論と実践（演習）とのバランスの確保
- 技術的な内容とマネジメント的な内容のバランスの確保
- グローバルな最新情報の収集や国内外の実務者によるレクチャーを交えた実践的構成
- 現場で必要となるチームワークや体力を培うような訓練

一方、後者に相当する要望としては、次のようなものが示されている。

- セキュリティと経済、セキュリティと心理といった企業がなかなか手を出せない基礎的な研究につながる基盤的な教育
- 法学や経営学の基礎など、セキュリティの周辺領域の知識に関する教育
- IT 系以外の経済学部・経営学部などで情報セキュリティ教育を行うことで、そうした人材がセキュリティ分野以外の業務に従事している際のセキュリティ業務への巻き込み（体制構築への協力など）を容易にする

（２）「情報セキュリティ関連業務を専任する人材」のためのカリキュラム策定に向けて

① 自社での必要性と必要人数、充足状況

アンケート調査に回答した企業はいずれも大企業であるが、情報セキュリティ分野の専門技術者の充足度については不足していると回答した企業から、充足済と回答した企業まで幅広く分かれる結果となった。サンプル数が少ないながら、全体的に見ると不足と回答する企業が多く、今後専門的な人材の確保に取り組むことが示されており、情報セキュリティ専門人材の採用ないし育成が強化される傾向にあることが示されている。

② 業務で担う役割の種類について、現状または意見

情報セキュリティ人材が担う役割として、以下が示されている。

- 情報セキュリティ機能の設計や対策実施に関する企画業務
- 情報セキュリティポリシーの作成、教育、内部監査を含む内部統制

- 社内 SOC[31]の担当者（情報セキュリティに係る技術動向等情報収集を含む）
- 社内 CSIRT[32]の担当者（インシデントハンドリング対応等を含む）
- ペネトレーションテストの実施または委託管理
- セキュリティ団体への参画、及び社会・業界へのセキュリティ普及活動

③ 業務で必要となる知識・スキル・コンピテンシーについて、現状または意見

情報セキュリティに関する専門的業務に従事する人材に必要となる知識・スキル・コンピテンシーとして示された内容は次の通りである。いずれも学士課程や修士課程において育成目標としているレベルを上回るものと見込まれ、これらを卒業・修了した人材が直ちに情報セキュリティ分野の専門性が求められる現場で活躍できるわけではないことがわかる。

- CISSP（2.3.1 参照）レベルの知識
- 脅威情報をもとにした影響分析・対応策検討をスピード感を持って実行できる能力
- 情報セキュリティに関する幅広い知識と、システム構築・運用やインシデント対応等の経験によるスキル、及び全体を俯瞰し自律的に行動できるコンピテンシー
- セキュリティ専門の技術だけではなく、情報技術一般や、法学・経営学などの知識も必要

④ 育成に関する役割分担（自社で行う部分、大学・大学院に期待する部分）

情報セキュリティ人材の育成に際し、自社の業務に直結する内容に関しては、当然ながら自社で教育することが示されている。一方で大学・大学院に期待する内容としては、次のような内容が挙げられている。

- 基礎的な部分の教育
- セキュリティ技術者としての基盤に関する内容
- 基礎・基盤、理論面での教育、実験環境を用いた体験型学習
- 業務改革の事例を通じて、対策の実施にどの程度費用がかかるかなどの感覚を学んできてもらえるとよい

（3）「情報セキュリティ関連業務を専任としない人材」のためのカリキュラム策定に向けて

① 業務で担う役割の種類について、現状または意見

情報セキュリティ関連業務を専任としない人材の扱いについては、回答企業ごとに内容が異

[31] Security Operation Center（セキュリティオペレーションセンター）の略。情報セキュリティ対策を目的とした情報システムやネットワークの監視や制御、関連情報の収集等を行う。CSIRT の一部として機能させる場合と、独立して機能させる場合の両方がある。

[32] Computer Security Incident Response Team（コンピュータセキュリティインシデント対応チーム）の略。情報システムやネットワークにおける情報セキュリティインシデントが発生した際に、状況確認、関係機関や組織内の連絡、被害発生や拡大の防止のための対策実施の判断などを行うためのチームを指す。

なる結果となっている。役割として挙げられているものを以下に示す。

- 部署毎の情報セキュリティポリシーの徹底及びインシデント対応
- CSIRT における指揮命令、報告・連絡、教育・訓練等
- 情報セキュリティにおける管理系業務

② 業務で必要となる知識・スキル・コンピテンシーについて、現状または意見

①と同様、回答企業ごとに内容が異なる傾向が見られる。

- ベンダ等の外部専門家とコミュニケーションが取れるレベルでの IT 及びセキュリティの基礎知識
- 自社のセキュリティポリシーに基づいたリスクアセスメントや、必要な機能に関する要件定義などを自社のあるべき姿や状況に照らして自ら行うことができる能力
- 全社を巻き込む取組・企画を行うための企画力（課題解決力）・プロジェクト推進力・コミュニケーション能力
- サイバーセキュリティの脅威に対する正確な意識と動機付け
- 情報管理、文書管理の精度向上に繋げられる知識

③ 現在の人材における知識・スキル・コンピテンシーの充足状況

（2）①と同様、充足状況は回答企業毎に異なり、全体的には不足と考える企業が多いものと認められる。

④ 情報セキュリティ分野の知識・スキル・コンピテンシーに関して大学に期待する内容

（2）と共通の回答がある一方、現場とコミュニケーションを図るための手段は現場で育成するしかないので大学には期待しないとの回答も示されている。

- 倫理的、基礎・理論面での意識・知識
- CISO やインシデントハンドラーといった役割を想定した実践的な教育
- 基礎的な部分の教育

（4）採用・雇用の観点について

① キャリアパスに関する意見

情報セキュリティ人材のキャリアパスに関しては、現状において各社とも確立していないことを示唆させる内容となっている。

- ユーザ企業内でセキュリティだけでキャリアパスを完結させることは困難であり、ICT 企業やセキュリティベンダに入社し、ユーザ企業へ出向し実践的な経験をキャリアパス上の

必須なステップとすることが早道に思える

- ゼネラリスト育成志向の強い採用・育成をしてきた一般企業にとってはセキュリティ専門人材に限らず、専門人材のキャリアパスをどうするかという視点で検討が必要
- セキュリティの担当としてある程度までキャリアップできる枠組みと、いろいろな部署を渡り歩く様な経験とを組み合わせたキャリアパスを作れると良い
- 国内の各事業者が共通の人材像を共有することが、キャリアパス形成の前提
- 業界で「セキュリティエンジニアの成功事例」を作ることも必要

② ジョブローテーションに関する現状または意見

情報セキュリティ分野の専門技術者においてもジョブローテーションは必要との意見が主流であるが、その方法は確立されていないことが回答より示唆される。

- 一定割合でのジョブローテーションは行っているが、都度他組織との調整事項であり、キャリアパスとして確立されていない
- セキュリティを踏まえた企画や設計を行うことにより、見直しなどのムダな業務を抑制するだけでなく、セキュリティマインドをもった人が広範囲に存在しそれぞれの部署で周囲を啓発することによって、組織全体のセキュリティレベルを高めることになると思われることから、一般の技術者もセキュリティ業務を経験してほしいと考えている
- 現在はゼネラリストの育成にむけたジョブローテーションがメインとなっており、今後は専門人材のキャリアパスを検討すると同時にジョブローテーションについても検討が必要
- 優秀な技術者ほど業務に固定されがちで現実的には難しい
- セキュリティは現場を知らないと的確な対策がわからないため、ジョブローテーションを通じて現場を知る必要がある

③ 採用やリクルートのシーンで必要となる、人材を表現する言葉や指標

下記回答に示されているとおり、採用やリクルートにおいて重視されている事項は回答企業ごとに異なることがわかる。

- 採用（採用者の実力値）の指標になるのはやはり取得資格（CISSP、情報処理安全確保支援士、情報セキュリティマネジメントなど）
- 採用に際しては「セキュリティ対策（防御）を通じて会社を守り、価値を高める」ということをアピールすべき
- ベンダ系、ユーザ系（マネジメント系、技術系）などの枠組みによって要求される情報セキュリティ人材は異なるので、体系的に分けた上で定義するのが良い
- 情報セキュリティ専門人材育成のためのキャリアパスに沿ってジョブローテーションを実

施するのであれば、そのことは採用時点で伝えなければ、採用のミスマッチにつながる

- 技術に対する好奇心が強くないとこの仕事には向かないので、情報セキュリティ技術者を採用する際には、必ず「コンピュータは好きですか」と聞いている

④ 採用やリクルート、キャリアパス、人材育成の問題における地方の活用

今回の回答企業はいずれも東京に拠点を置く企業であるため、地方企業の当事者としての回答は得られなかったが、地方向けの対策が必要であることについては概ね共通した認識となっている。

- セキュリティ人材が必要なのは地方の企業でも同様だが、情報セキュリティ人材は東京に偏在している
- 地方企業にもそれなりに IT 人材はいるので、情報セキュリティ人材に育成する教育機会を地方でも増やしていくことは有効
- 地方の人材に対するチャンスを作らないと難しい
- 地方では情報セキュリティ人材を育成する余裕がないと見込まれるので、都心部で育成された人材のローテーションや、人材の共同利用のような発想も必要かもしれない

２．４．４ 調査結果のまとめ

文献調査及びアンケート調査をもとに、モデル・コア・カリキュラムに対する産業界の要望についての調査を実施した。情報セキュリティの現場で直ちに必要となるような知識やスキルに関する要望よりも、基礎力・ファシリテーション力・コミュニケーション力などへの期待のほか、経済や心理との関係など、企業が手を出しにくい学問分野に関する教育に期待する意見が示されている点が特徴的である。こうした傾向をもとに、産業横断サイバーセキュリティ人材育成検討会、特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）、情報処理安全確保支援士試験シラバスをもとに産業界で必要とされるスキルを表 29 のように整理した。

表 29　産業界で用いられる指標（知識項目とスキル分類）

記号凡例： 緑色は[産]*及び[情]*で求めているスキル 水色縦線は[産]*のみで求めているスキル			iコンピテンショナリディクショナリのスキル分類												
			メソドロジ					テクノロジ							関連知識
			戦略	企画	実装	利活用	支援活動	システム	開発	保守・運用	非機能要件	組込み・計測・制御	共通技術	
SecBoK2016 知識項目	基礎	工学基礎												
		ICT 基礎		■	■			■	■	■	■	▨	▨	
		ビジネス基礎	■		▨	■	■							▨
	セキュリティ専門分野	セキュリティ基礎									■			
		セキュリティガバナンス					■							
		セキュリティマネジメント	■			■	■				■			
		ネットワークセキュリティ						■			■			
		システムセキュリティ		■				■	■		■			
		セキュアシステム設計・構築		■	■			■	■		■			
		セキュリティ運用			■	■	■	■		■	■			
		暗号・認証・電子署名									■			
		サイバー攻撃手法									■			
		デジタルフォレンジック									■			
		法・制度・標準				■	■				■			▨

＊［産］産業横断サイバーセキュリティ人材育成検討会「人材定義リファレンスに基づくスキルマッピング」が求めるスキル
［情］情報処理安全確保支援士試験シラバスにおける要求される知識に対応するスキル

３．大学における情報セキュリティ教育のためのモデル・コア・カリキュラム

本章では第２章における調査結果をもとに、現在の我が国の大学が情報セキュリティ教育を実施する際にカリキュラム作成の参考となるような、モデル・コア・カリキュラムの案を例示する。

３．１ モデル・コア・カリキュラムの定義

本章で提示するモデル・コア・カリキュラムの目的、作成方針などについて解説する。

３．１．１ モデル・コア・カリキュラムの目的

第２章に示した通り、我が国の高等教育機関における情報セキュリティ教育は、産業界からのニーズが示される一方で、学内での必要性の認識不足や教員の不足などの理由により、これまで積極的に取り組まれていなかった。しかしながら現状調査に示されているように、情報系学科では情報セキュリティに関する専門科目または既存科目の中で何らかの情報セキュリティに関する内容を扱う事例が見られるほか、文科系学部等を含む幅広い学部の新入生等を対象とした情報セキュリティリテラシー教育を行っている事例も見られるようになっている。一方で、深掘調査からは情報セキュリティに関する内容であっても、暗号など特定の分野に偏っているとの指摘や、リテラシー教育は技術者育成とは切り離して考えるべきとの意見も示されており、現在の大学における情報セキュリティ教育は、必ずしも産業界をはじめとする社会のニーズに対応したものになっていないことが見込まれる。そこで、こうした状況の改善を図るため、本調査では以下の各項を目的としてモデル・コア・カリキュラムの作成を行う。

- 産業界におけるニーズを反映した、情報セキュリティ分野に関して大学で教育すべきコアとなる内容の提示
- 多様な例示を通じた大学における情報セキュリティ教育の実施方法に関する解説の提供
- モデル・コア・カリキュラムを通じた産学間での情報セキュリティ分野の知識・スキルに関する共有の強化

３．１．２ モデル・コア・カリキュラムの作成方針

前述の目的を踏まえ、本調査では次の方針のもとでモデル・コア・カリキュラムの作成を行うこととする。

（１）モデル・コア・カリキュラムの位置付け

現状において、我が国の高等教育機関において実施される情報セキュリティ教育に関してどのような内容を、どのレベルで教えるべきかについての、標準やコンセンサスなどは存在しない。第２章で示したように、産業界からのニーズも、IT 企業とそれ以外では異なった傾向を示すなど、一律ではない。そこで、モデル・コア・カリキュラムは情報セキュリティ教育に関する“標準”を

示すのではなく、“サンプル”を例示するとの位置付けで提供するものとし、コアとして提示する内容を含めて大学が柔軟に採否を判断できるようにする。

（２）育成する人材像

モデル・コア・カリキュラムの対象は、情報セキュリティ分野の専門人材に限定するのではなく、「他の技術分野を専門とするが、情報セキュリティも理解している人材」を対象とする育成についても考慮する。具体的には情報系以外の理工系の学生を想定するが、保健医療福祉やデザインなど、専門分野に取り組む上で情報セキュリティ対策が密接に関わる分野の学生についても考慮に含めることとする（後述の例示②にて対応）。

また、理工系、文科系等を問わず、大学新入生等を対象とする情報セキュリティリテラシー教育については、専門人材育成の対象ではないが、大学において確実に需要があり、かつこの段階で適切な情報セキュリティ教育を行うことは、社会における情報セキュリティの確保において大きな効果をもたらすと期待されることから、例示の対象に含めることとする（例示①にて対応）。

これらに含まれない文科系専門教育等向けのカリキュラム展開については本調査の対象外としている。なお、情報セキュリティ分野は、マネジメント系・法律系・社会系分野と密な関係があり、２章の事例詳細３に示す情報セキュリティ大学院大学には、それらに対応する大学院修士課程カリキュラムが用意されている。このため、文科系の情報セキュリティ専門分野で活躍する人材育成に向けた学士課程や社会人学び直しにおけるカリキュラムを含めた具体的な検討は今後の作業である。

（３）例示するカリキュラムの粒度

情報セキュリティ分野を専門としない教員が参照することが見込まれるものについては、便宜のために科目ごとに教育する内容に関する説明を行う。

一方、情報セキュリティ専門人材を育成する学科向けなど、情報セキュリティ分野を専門とする教育が参照することが前提のカリキュラムについては、自明の内容と見込まれることから詳細の説明を省くものとする。

（４）他の標準との対応

モデル・コア・カリキュラムに基づくカリキュラム作成に際して、他の標準や産業界で求められている知識・スキルとの対応関係を容易に確保できるようにするため、以下の配慮を行う。

①「情報学科におけるカリキュラム標準 J07」[33]との整合

モデル・コア・カリキュラムにて例示する科目名を「情報学科におけるカリキュラム標準 J07」

[33] https://www.ipsj.or.jp/12kyoiku/J07/J0720090407.html

（以下、「J07」という。）で提供されているモデルカリキュラムのものと一致させる。だし J07 には以下の５種類があり、それぞれ BoK（Body of Knowledge）の構成も異なるため、情報セキュリティ関連の内容が充実している CS、IS、IT が定める内容を優先しつつ調整することとする。

- CS（Computer Science：コンピュータ科学領域）
- IS（Information System：情報システム領域）
- SE（Software Engineering：ソフトウェアエンジニアリング領域）
- CE（Computer Engineering：コンピュータエンジニアリング領域）
- IT（Information Technology：インフォメーションテクノロジ領域）

② 企業が求める人材とのマッチングを容易とするための工夫

以下の 2 点により、企業が求める教育を受講しているかどうかの判断を容易にする。

ア）企業が活用している資格や BoK などとのマッピングの提供

以下が定める知識やスキル項目との対応がわかるような情報提供を行う。

- 産業横断サイバーセキュリティ人材育成検討会 人材定義リファレンス（2.4.2 参照）
- 情報処理安全確保支援士シラバス（2.4.2 参照）
- セキュリティ知識分野（SecBoK）人材スキルマップ 2016 年版（2.4.2 参照）

イ）演習科目の明示

実践能力重視の観点から、シラバスにおける演習科目を明示する。

（５）知識項目の洗い出し

モデル・コア・カリキュラムで扱うべき知識項目について、J07 の定める知識体系をベースに整理した結果を次表に示す。例示するカリキュラムに掲載する科目名のうち、下表の内容と一致させることが可能なものについては、極力一致させることとする。

表 30　モデル・コア・カリキュラムで扱う知識項目の分類

情報セキュリティ専門分野	前提となる知識項目（例）	応用領域の知識項目（例）
暗号	数学（代数幾何学ほか）、 アルゴリズムの基礎	電子署名
認証	通信、情報管理	認証とアクセス制御
ネットワーク セキュリティ	通信、ネットワークコンピューティング、 Web システムとその技術	認証とアクセス制御
システム セキュリティ	コンピュータアーキテクチャ、 オペレーティングシステム、 ソフトウェア工学、	脆弱性、 情報セキュリティサービス、 ソフトウェアセキュリティの実現、

情報セキュリティ専門分野	前提となる知識項目（例）	応用領域の知識項目（例）
	アルゴリズムとデータ構造、 プログラミング言語、 アプリケーション計画、 情報システム設計、 システムの実装とテスト戦略	セキュリティと高信頼化、 形式手法
データセキュリティ	アルゴリズムとデータ構造、 情報管理、データベース	フォレンジック
情報セキュリティ マネジメント、 ソーシャル分野他	情報管理、 情報システム管理、 組織理論一般、経済学、 社会的視点と情報倫理	情報保証と情報セキュリティ、 コンピュータ犯罪、 プライバシーと市民的自由

（６）育成すべき人材ごとの方針案

以下①～③それぞれを対象とするモデル・コア・カリキュラムの例示を行うにあたり、本調査における人材ごとの教育方針を示す。

① 情報セキュリティ専門人材育成向け

第２章にて把握された産業界ニーズによれば、「情報セキュリティのみに詳しい人材」の需要はあるが少なく、情報系の基盤技術に関する知識を有していることへの期待が高いことから、情報系の幅広い知識・スキルを有する人材として育成するためのカリキュラムとなるように配慮する。一方で、基盤技術に関する学習は情報セキュリティを学ぶ者にとって不可欠であるにもかかわらず、初学者に退屈に感じられやすいことが懸念され、詰め込みによるモチベーション低下も予想される。情報セキュリティ分野は CTF（Capture The Flag、本報告書の 22 ページ脚注参照）競技などにも見られるように、学習した基礎知識を活かす機会が豊富という特徴を有することから基盤技術の知識習得の動機付けとして活用できるような演習の設定等の工夫を行う。

② 情報セキュリティを専門としない学生向け

大半の理工系学部３年においては、カリキュラムに新たに情報セキュリティ系科目を追加する余裕がないことから、以下の２つの方法のいずれかの採用を前提に、双方についてのモデル・コア・カリキュラムを提供することとする。

ア）可能な範囲で最大限の専門教育を行う場合

情報セキュリティ系１科目と休暇期間中の集中演習を組み合わせたカリキュラムとする。これは enPiT 2 / Basic SecCap で計画されているものを参考に提供する。

イ）無理のない範囲で可能な教育を行う場合

必要最低限と考えられる内容をコアとして定めた上で、情報セキュリティ系１科目、それが難しい場合は既存科目の一部で必要最低限のセキュリティに関する教育を実施する。

③ 社会人の学び直し向け

社会人のニーズに応じて、３種類のモデル・コア・カリキュラムを提供する。いずれも講義と演習の組合せにて実施を想定する。

ア）短期（２週間程度）集中コース

情報セキュリティ分野のうちある特定のテーマについて手早く学びたい現役 IT 技術者を対象に教育を実施する。

イ）中期（３～６か月程度）コース

情報セキュリティ分野のうち特定の知識領域について学びたい現役 IT 技術者を対象に教育を実施する。

ウ）長期（１年程度）コース

情報セキュリティ分野について体系的に学びたい現役 IT 技術者を対象に、修士課程１年向けの内容に相当する教育を実施する。

３．２ モデル・コア・カリキュラムの構成

３．１における検討をもとに、本調査では次表と図に示す 10 種類のモデル・コア・カリキュラムの例示を行う。

表 31　モデル・コア・カリキュラムの構成案

区分	例示ごとの定義	育成しようとする情報セキュリティ人材像	対象者（凡例参照）		
			専門人材	技術者	一般
区分1 学士課程４年間で卒業し社会に出ることを想定した区分	①一般教養としての情報セキュリティに関する講義を対象とするもの	日常の社会生活を営む上で必要なセキュリティに関する知識を備えた人材	○	○	◎
	②学士課程卒業後就職を予定している広く理工系に近い学生を対象とするもの	情報セキュリティに関する基礎的な知識を備えた人材（セキュリティ分野への就職は前提としない）	○	○	○
	③情報セキュリティを専門とする学科等を対象とするもの	情報セキュリティに関する基礎的な知識・経験と意識を備えた人材（セキュリティ分野への就職は前提としない）	○	○	△
区分2 学士課程４年間＋修士課程２年間の６年間の課程を経て社会に出ることを想定し、リテラシー教育が終了した学生（主に学部3年～修士1年）を想定した区分	④修士課程に進学予定の情報系学士課程の学生を対象とするもの	情報セキュリティを本格的に学ぶ上で必要となる基盤的知識を習得した人材	◎	○	－
	⑤情報セキュリティに関する単独の科目を対象とするもの	情報セキュリティに関する基本的な知識を備えた人材（セキュリティ分野への就職は前提としない）	△	○	○
	⑥専門とは別に情報セキュリティを学ぶコース等を対象とするもの	習得した知識・実践的経験を自らの専門分野のセキュリティ対策に活かせる人材	△	◎	－
	⑦情報セキュリティを専門とする専攻等を対象とするもの	情報セキュリティに関する専門的な知識と実践的な経験、及び意識を備えた人材（セキュリティの専門性をある程度発揮できる環境への就職等を想定）	◎	○	－
区分3 情報セキュリティに関して体系的に学び直したいと考える現役IT技術者（就職後10～15年程度（30代中～後半）の技術者）を想定した区分	⑧短期（２週間程度）集中コース	習得した情報セキュリティに関する実践的知識・経験を自らの業務に活かせる人材	○	◎	○
	⑨中期（3～6ヶ月程度）コース	習得した情報セキュリティに関する実践的知識・経験を自らの業務に活かせる人材	○	◎	△
	⑩長期（1年程度）コース	習得した情報セキュリティに関する実践的知識・経験を自らの業務に活かせる人材	◎	△	－

凡例：専門人材＝情報セキュリティ分野を専門とする人材、
技術者＝情報セキュリティを理解する技術者やマネージャ、一般＝一般の社会人
◎＝主たる育成対象、○＝育成対象、△＝条件により活用可能、－＝対象外

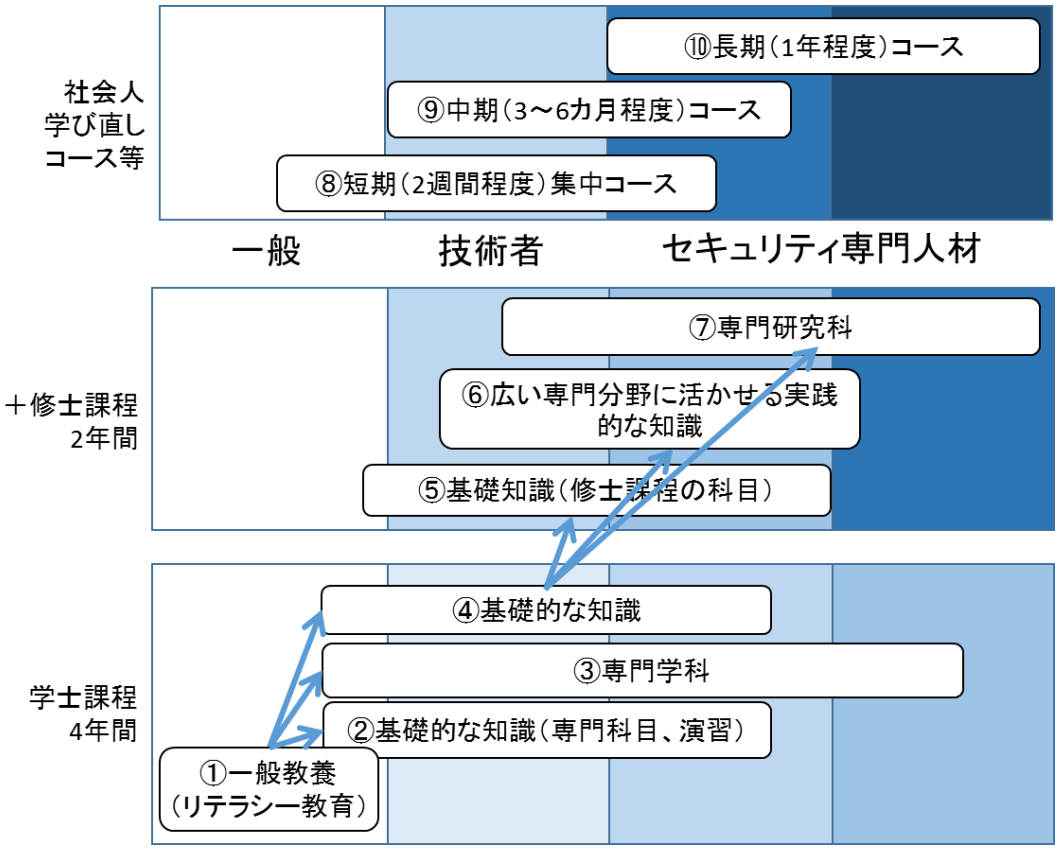

図 6　モデル・コア・カリキュラム 10 例示の位置づけ

各区分における例示の選定に関する考え方を以下に示す。

（１）区分１：学士課程４年間で卒業し社会に出ることを想定した区分

前述の通り、大学新入生等を対象とする情報セキュリティリテラシー教育は専門人材育成の対象ではないが、大学において確実に需要があり、かつこの段階で適切な情報セキュリティ教育を行うことは、社会における情報セキュリティの確保において大きな効果をもたらすと期待されることから、モデル・コア・カリキュラムの例示の１つとして設定する（例示①）。

一方、情報セキュリティ分野の専門知識を習得するには、あらかじめ数学や情報通信ネットワーク、コンピュータアーキテクチャ、プログラミング言語等の知識が必要であり、情報系の学士課程において典型的なカリキュラムにおいてそうした条件が整うのは 4 年次に近い時期となってしまい、卒業研究との関係で誰もが受講するような科目とするのが難しい状況にある。そこで、モデル・コア・カリキュラムでは次の２種類の例示により、産業界等で求められる情報セキュリティ分野の専門知識を有する人材の育成を図ることとする。

- 情報セキュリティ分野に関して等しく専門性を深めるのでなく、受講者の関心などに応じた特定の領域に絞った上で、夏期休暇期間等に集中的に実施するなどの工夫により、既存カリ

キュラムとの両立を図る（例示②）。

- 専門分野として情報セキュリティのみを扱う学科を構成し、3～4 年次に情報セキュリティ専門科目を集中的に学習するために必要な基礎知識を 1～2 年次で学ぶようなカリキュラム構成とする（例示③）。これは調査時点において、長崎県立大学情報システム学部情報セキュリティ学科においてのみ取り組まれている内容であり、同学科におけるカリキュラム構成を参考としている。

（２）区分２：学士課程４年間＋修士課程２年間の６年間の課程を経て社会に出ることを想定し、リテラシー教育が終了した学生（主に学部３年～修士１年）を想定した区分

（１）と異なり、情報セキュリティに関する専門科目を大学院修士課程において学ぶことを前提とすると、比較的ゆとりをもってカリキュラムを構成することが可能である。

修士課程進学を前提としたとき、学士課程 3～4 年次においては情報セキュリティ分野の専門知識を理解するために必要となる、情報通信ネットワークの基盤技術や、計算機技術を構成するコンピュータアーキテクチャやプログラミング言語、データベースなどについて学ぶことが望ましい。しかしながら前述のように、基盤技術に関する学習は情報セキュリティを学ぶ者にとって不可欠であるにもかかわらず、初学者にとっては退屈と感じられやすいことが懸念される。このとき、学士課程の期間中でも情報セキュリティ分野の専門的な演習科目等を受講することで、この分野の面白さを実感してもらうとともに、受講者にとって今後の学習意欲を高めるような動機付けとなれば理想的である。そこで、例示②のカリキュラムと同様の科目構成で修士課程進学を前提とする学士課程 3～4 年次向けのカリキュラムを作成する（例示④）。

一方、修士課程向けのカリキュラムとしては、まず小規模なものとして、情報セキュリティ以外の分野を専攻する修士課程在籍者を対象に、1 科目で情報セキュリティ分野に関する最低限の専門知識を提供するようなカリキュラムを示す（例示⑤）。

続いて、同様に情報セキュリティ分野以外を専攻する受講者を対象に、例示⑤よりもさらに多くの情報セキュリティ分野の専門知識・スキルを得ようとする場合に適したカリキュラム案を示す（例示⑥）。これは現行の enPiT Security / SecCap のプログラムに基づく取り組みと重複する内容であり、同プログラムで得られた知見を反映して作成している。

最後に、情報セキュリティ分野を専門とする専攻向けのカリキュラムを示す（例示⑦）。これは、情報セキュリティ大学院大学情報セキュリティ研究科における実践を通じた知見を反映したものである。

（３）情報セキュリティに関して体系的に学び直したいと考える現役ＩＴ技術者（就職後１０～１５年程度（３０代中～後半）の技術者）を想定した区分

社会人の学び直し向けのカリキュラムを例示するには、あらかじめ彼らのニーズを把握しておく必要がある。具体的には、次のような２種類のニーズが想定される。

- 情報セキュリティ分野の特定の１領域について、手早く学びたい
- 最新の情報セキュリティ分野について、体系的に学びたい

まず前者の場合、入門講座であれば半日～１日で完結させることも可能であるが、専門教育を前提とした場合、１日あたりの講義・演習時間の割り当て方法にもよるが、２週間程度が必要と見込まれる。そこで、２週間で特定のテーマについて集中的に学習するための短期コースのカリキュラムの例示を行うこととする（例示⑧）。

続いて、例示⑧に示した短期のコースを組み合わせることによる派生的な中期コース（３～６ヶ月）の例示を行う（例示⑨）。当該例示において詳細を説明するように、こうした組み合わせを提示するためには実施する大学等において情報セキュリティ分野の十分な教育リソース（教員、教材、演習環境等）が必要となるため、多くの大学で適用可能とはいえないが、社会人ニーズへの対応方法の例示として示すものである。

最後に、１年間程度で体系的な専門教育を行うための長期コースに関するカリキュラムの例示を行う（例示⑩）。これは修士課程１年向けの教育内容に相当する。

３．３ 各モデル・コア・カリキュラムの内容

各モデル・コア・カリキュラムとして例示する内容についての詳細を示す。なお、各例示の説明において、特に断りのない限り、講義または演習１科目は 4～6 ヶ月間にわたって１コマ 90 分×15 コマ程度で構成されるものと仮定する。

３．３．１ 例示①：一般教養としての情報セキュリティに関する講義を対象とするもの

（１）概要

本カリキュラムの概要を次表に示す。

表 32　例示①概要

大学における情報セキュリティ教育のためのモデル・コア・カリキュラム　例示①		
情報セキュリティリテラシー教育向け		
種別		科目シラバス
想定する受講者		学士課程の新入生（１年次・学部問わず）
受講者の知識･スキル		普通科高校卒業程度の知識・スキルを想定する
育成する人材像		日常の社会生活を営む上で必要となる情報セキュリティに関する知識を備え、適切な判断ができる人材
到達目標	コア部分	以下の５点について理解する。 ①情報セキュリティをなぜ考える必要があるか ②情報倫理と著作権に関して遵守すべき事項 ③代表的な脅威がもたらす影響と対策のための技術や仕組み ④情報セキュリティに関する法律や制度 ⑤情報社会においてセキュリティとして留意すべきこと
	コア以外を含むカリキュラム全体	（コア部分と同じ内容の詳細化）
関連科目との関係		・本科目受講に先立って受講しておくべき科目はなし ・リテラシー科目として以下の①②のいずれかの指定を推奨： ①全学生必修 ②情報処理関連の演習または情報セキュリティ専門科目の受講には本科目の単位取得を要件とする
実施方法		講義またはeラーニング教材自習

（２）科目構成例

３コマ程度の講義で上記のコア部分①から⑤について理解する科目構成例を次表に示す。この科目例では、技術の仕組みや制度の詳細を解説するのではなく、受講生にとって身近な事例を使って問題意識を高めることを狙う。また、サイバー攻撃などについてはパソコン等で実施可能な簡単なデモンストレーションによって、その脅威を実感できるようにする。

表 33　科目構成例

回数	講義内容	解　説
1	情報セキュリティの必要性	現代社会が直面する情報セキュリティ課題と社会経済活動における情報セキュリティの重要性を理解するために、大学や日常生活におけるアカウントやパスワード管理の役割を例に情報セキュリティの現状の課題について考える。続いて、実社会におけるサイバー攻撃の脅威と要因、およびサイバー攻撃対策に必要な対策の考え方について学ぶ。
2	脅威と対策技術	コンピュータやインターネットを狙うサイバー攻撃の仕組みをデモストレーションをまじえて具体的に解説する。パソコンの乗っ取りと遠隔操作、ネットワークや Web サービスを妨害する DDoS（分散型サービス不能攻撃）等の事例を取り上げ、それぞれについて、対策技術の概要を学ぶ。また、情報セキュリティの基盤技術として、暗号化技術の役割と仕組みをわかり易く解説する。
3	関連法律･制度と社会的問題	情報セキュリティを取り巻く法律や制度の中から、企業活動や日常生活に関わりの深いものを取り上げ、その基本的な考え方を解説する。企業活動の役割と責任の観点から、プライバシーと個人情報保護の法律、サイバー犯罪防止のためのコンピュータウイルスと不正アクセスに関する法律について学ぶ。また、企業活動に関わりの深い標準やガイドラインとして情報セキュリティマネジメントシステム(ISMS)などを例に取り上げ、その役割を解説する。最後に、大学の場を例にとって、情報倫理と著作権に関して遵守すべき事項を確認する。

（3）適用条件

本カリキュラムは、以下の３種類の実施方法が想定され、それぞれ適用条件が異なる。

① リテラシー教育を目的とする講義形式で行う場合

学内情報システムやネットワーク等の環境を利用する上であらかじめ理解しておくべき内容に関する講義として行う場合、教育内容は自ずと利用上のルール的なものに力点が置かれるものとなる。対象となる環境に特化した内容にすることも考えられる。再履修を前提とした不合格を想定せず、試験のレベルも平易なものが想定される。

② 自習型 e ラーニング形式で行う場合

①の内容を講義形式でなく、学生に自習式の e ラーニング教材を受講させ、付属のテストに合格することで修了とするものである。e ラーニング教材の構成は、内容ごとに区分するのが望ましく、本カリキュラムのコアとして示した内容をもとに 5 回分程度で構成することが想定される。

③ 他の科目の一部に含める形で行う場合

情報系科目の一部として教育を行う場合、内容はリテラシー的なものであっても、位置づけは情報系基礎科目となることから、①②よりも学術的な観点から教育内容を定めることが望ましい。

（４）産業界で用いられる指標等との対応

本カリキュラムで受講可能な科目と産業界で用いられるスキル分類との対応関係を次表に示す。

表 34　産業界で用いられる指標との対応（例示①）

記号凡例: ◎=演習を伴う実践的専門教育 〇=座学中心の専門教育 ◇=基礎的/入門的教育 ★=状況に応じてケースバイケース ※=習得済が受講の前提 緑色は[産]*及び[情]*で求めているスキル 水色縦線は[産]*のみで求めているスキル			iコンピテンショナリディクショナリのスキル分類												
			メソドロジ					テクノロジ							
			戦略	企画	実装	利活用	支援活動	システム	開発	保守・運用	非機能要件	組込み・計測・制御	共通技術	関連知識
SecBoK2016 知識項目	基礎	工学基礎												
		ICT 基礎		■	■			■	■	■	■	▨	▨	
		ビジネス基礎	■		▨	■	■							▨
	セキュリティ専門分野	セキュリティ基礎									◇			
		セキュリティガバナンス					■							
		セキュリティマネジメント	■			◇	◇				★			
		ネットワークセキュリティ						■			◇			
		システムセキュリティ		■				■	■		◇			
		セキュアシステム設計・構築		■	■			■	■					
		セキュリティ運用			■	◇	◇	■		■	◇			
		暗号・認証・電子署名									◇			
		サイバー攻撃手法									★			
		デジタルフォレンジック									■			
		法・制度・標準				◇	◇				◇			▨

＊［産］産業横断サイバーセキュリティ人材育成検討会「人材定義リファレンスに基づくスキルマッピング」が求めるスキル
［情］情報処理安全確保支援士試験シラバスにおける要求される知識に対応するスキル

（５）実施上の工夫点

受講生として新入生を対象としていることもあり、リテラシー教育の必要性について関心が得られない場合も多いと見込まれる。情報セキュリティに関するルールを逸脱した場合に被る被害やペナルティについての説明を必要に応じて交えることで、受講者にとって自らの問題であると実感してもらえるように工夫すべきである。

３．３．２ 例示②：学士課程卒業後就職を予定している理工系学生等を対象とするもの

（１）概要

本カリキュラムの概要を次表に示す。

表 35　例示②概要

大学における情報セキュリティ教育のためのモデル・コア・カリキュラム　例示②		
就職を予定している学士課程在籍者を対象とする情報セキュリティ分野の実践講座向け		
種別		科目シラバス
想定する受講者		学士課程で卒業を予定しており、セキュリティに関する知識を得たいと考える3～4年次在籍者（理工系学生やＩＴ技術の利用者となる学生）
受講者の知識･スキル		理工系教養科目＋情報リテラシー教育を想定する
育成する人材像		産業界で必要となる情報セキュリティ分野に関する基礎的な知識を身につけた人材（セキュリティ分野への就職は前提としない）
到達目標	コア部分	受講者の志望業界で求められる次のような情報セキュリティに関する知見を習得し、実務に活用できるようにする。 （例１）工学系（非情報）：制御システムのセキュリティ対策技術 （例２）保健医療福祉系：個人・機微情報の管理手法 （例３）芸術系：作品の脆弱性対策及び著作権保護
	コア以外を含むカリキュラム全体	（コア部分に同じ）
関連科目との関係		・本科目受講に先立って受講しておくべき科目を設定しないが、受講する学生の前提知識に応じて、以下の内容に関する教育を推奨する。 ①情報とデジタルデータの概念 ②コンピュータとして総称することが可能な機器の概念
実施方法		講義及び演習

（２）科目構成例

次表の科目構成例は、既存の情報系学科の講義と演習を基礎科目とし、それに加える形で、情報セキュリティの専門科目の講義と演習を受講することによって、受講者の就職先の業界で求める情報セキュリティに関する知見を習得し、実務に活用できるようにすることを狙うものである。このため、専門科目の講義と演習には多様性があり、大学毎に特色のある科目を受講生に提供することを想定している。

なお、次表の科目構成例は、実践的なセキュリティ人材育成プログラムとして、平成 28 年度から大学の学部学生を主対象として始まった Basic SecCap[34]コースで提供が予定されている科目に基づいている。本コースは、平成 29 年度から 10 以上の連携大学で開講され、周辺の参加大学からも受講できるようになる予定である。

[34] https://www.seccap.jp/basic/

表 36　科目構成例

学年	講　義	演　習　等
基礎科目	コンピュータシステム、基礎数学、情報理論、アルゴリズムとデータ構造、情報論理学、コンピュータアーキテクチャ、オペレーティングシステム、データベース、ソフトウェア工学、コンパイラ、システムプログラム、コンピュータネットワーク、情報セキュリティ、数値解析、リスクマネジメント、情報法制度、テクニカルライティング	プログラミング基礎演習、 プログラミング実践演習
専門科目	セキュリティ総論 A（倫理、評価、運用） セキュリティ総論 B（暗号基礎から応用） セキュリティ総論 C（暗号、ウィルス、ITリスク） セキュリティ総論 D（システム基礎から制度） セキュリティ総論 E（物理レベルからアプリケーションレベルまで）	セキュリティ基礎演習 ログ解析演習 クラウド・セキュリティ演習 インシデントレスポンス演習 サイバープログラミング演習 サイバーディフェンス基礎演習 CSIRT 基礎演習

表 37　専門科目の講義例

講義名	解説
セキュリティ総論 A	• セキュリティリテラシー • セキュリティ攻撃の事例 • セキュリティ防御の事例 • プログラムのセキュリティリスク • ネットワークのセキュリティリスク • 暗号技術と実利用例 • 情報セキュリティポリシー • 情報セキュリティ対策体制 • 情報倫理 • まとめと試験
セキュリティ総論 B	• 数理モデルから紐解く暗号理論 • 代数学から構築する実践セキュリティ技術 • 実用化暗号の安全性評価と実装演習 • Python によるマルウェア解析 • IoT 機器とサイバーセキュリティ • セキュリティ技術の標準化
セキュリティ総論 C	• イントロダクション • コンピュータウイルス • アクセス管理技術 • 暗号の概要 • 共通鍵暗号 • 公開鍵暗号 • デジタル署名と PKI • 暗号プロトコル • 個人情報漏洩対策

講義名	解説
	• 不正コピー対策 • セキュリティポリシーと ISMS • ICT システムの運用とセキュリティ • デジタルフォレンジック • IT リスクの考え方 • 考査と解説
セキュリティ総論 D	• ネットワークシステムの基礎 • 情報数学基礎 (暗号，ハッシュ) • サイバーセキュリティの考え方 • インシデント対応技術 • 情報監査 • パーソナル情報とセキュリティ • CSIRT と運用
セキュリティ総論 E	• イントロダクション、暗号の歴史と概要 • 暗号数学 • 共通鍵暗号とデータ暗号化/公開鍵暗号と認証技術 • 暗号計算の SW/HW 実装 • SW/HW 実装に対する工夫と安全性評価 • 階層型通信プロトコルモデル • データリンク層セキュリティ • ネットワーク層セキュリティ • トランスポート層セキュリティ • アクセス制御 • メモリ脆弱性 • 侵入検知 • マルウェア検知 • マルウェア解析

表 38　専門科目の演習例

講義名	解説
情報ネットワーク演習	インターネットを構築するには、パソコン、スイッチ、ルータなどのネットワーク機器を接続し、ネットワークとして動作させるための適切な情報を設定しなければならない。本演習では、ルータ設定をおこない、インターネットがどのように構築されているのかをイメージする。さらに構築したネットワーク上にセキュアなWebサーバを立て、サーバへのトラヒック監視を行うことにより、ネットワークセキュリティの重要性について基本から学ぶ。
クラウドセキュリティ基礎演習	クラウドサービスの開発から提供までの工程と実装時のセキュリティマネジメントを学び IDC(インターネット・データセンター)上への模擬システムの展開をテーマとしたクラウドサービスのセキュリティ要件と運用要件の抽出を行い、クラウドサービス提供に係る実践的なセキュリティの考え方を身につけることを目標とする。

講義名	解説
インシデントハンドリング演習	セキュリティインシデントを体感できるワークショップ（ボード ゲーム形式）を実施し、サイバーセキュリティにおける経営層（CIO/CISO など）の在り方、CSIRT に必要とされる人材像、現場における対応事例などを学ぶ。更に、演習を踏まえインシデントハンドリングを適切に実施するための仕組みについてグループで考察し発表する。

（３）適用条件

受講者の属性（情報系学科、情報系以外の理工系学部、その他学部）によって背景知識が大きく異なるため、これに配慮したカリキュラムとする。

（４）産業界で用いられる指標等との対応

本カリキュラムで受講可能な科目と産業界で用いられるスキル分類との対応関係を次表に示す。

表 39　産業界で用いられる指標との対応（例示②）

記号凡例： ◎=演習を伴う実践的専門教育 〇=座学中心の専門教育 ◇=基礎的/入門的教育 ★=状況に応じてケースバイケース ※=習得済が受講の前提 緑色は[産]*及び[情]*で求めているスキル 水色縦線は[産]*のみで求めているスキル			iコンピテンショナリディクショナリのスキル分類												
			メソドロジ					テクノロジ							関連知識
			戦略	企画	実装	利活用	支援活動	システム	開発	保守・運用	非機能要件	組込み・計測・制御	共通技術		
SecBoK2016 知識項目	基礎	工学基礎									※				
		ICT 基礎						◎	〇	◇	※				
		ビジネス基礎													
	セキュリティ専門分野	セキュリティ基礎									◎				
		セキュリティガバナンス													
		セキュリティマネジメント				◇	◇				〇				
		ネットワークセキュリティ						◎			◎				
		システムセキュリティ		◇				◎	◇		◎				
		セキュアシステム設計・構築		◇	◇			◇	◇		◇				
		セキュリティ運用			◇	〇	〇	〇		◇	〇				
		暗号・認証・電子署名									〇				
		サイバー攻撃手法									〇				
		デジタルフォレンジック									◇				
		法・制度・標準				◇	〇				◇				◇

＊［産］産業横断サイバーセキュリティ人材育成検討会「人材定義リファレンスに基づくスキルマッピング」が求めるスキル
［情］情報処理安全確保支援士試験シラバスにおける要求される知識に対応するスキル

（５）実施上の工夫点

本カリキュラムの対象人材は「成長分野を支える情報技術人材の育成拠点の形成（セキュリティ分野）」（enPiT Security 2 / Basic SecCap）プログラムにおける想定と近く、同プログラムのスキーム等の活用は有効である。

３．３．３ 例示③：情報セキュリティを専門とする学科等を対象とするもの

（１）概要

本カリキュラムの概要を次表に示す。

表 40　例示③概要

大学における情報セキュリティ教育のためのモデル・コア・カリキュラム　例示③		
情報セキュリティ分野を専門とする学科向け		
種別		カリキュラム
想定する受講者		情報セキュリティを専門とする学科の学生（1～4年次）
受講者の知識･スキル		普通科高校卒業程度の知識・スキルを想定する。
育成する人材像		情報セキュリティに関する基礎的な知識･経験と意識を身につけた人材（セキュリティ分野への就職は前提としない）
到達目標	コア部分	情報セキュリティ上の主要な脅威と対策について理解するとともに、情報セキュリティ分野の代表的な要素技術について、演習等を通じてそれぞれの原理と活用方法を習得する。
	コア以外を含むカリキュラム全体	（コア部分に同じ）
関連科目との関係		学科内で体系的に整備する。
実施方法		講義及び演習、卒業論文

（２）科目構成例

表 41　科目構成例（仮）

学年	講義（共通科目を除く）	演習等
1年次	情報数学、情報理論、微分積分学、代数幾何学、確率統計学、電磁気学、情報リテラシー、コンピュータアーキテクチャ、オペレーティングシステム、プログラミング基礎、情報社会	プログラミング基礎演習
2年次	数値解析、無線通信工学、暗号理論、データ構造とアルゴリズム、コンピュータネットワーク、情報管理（データベース）、情報セキュリティ概論、ソフトウェア工学、リスクマネジメント、情報法制度、テクニカルライティング	プログラミング実践演習、 情報システム演習
3年次	ネットワークセキュリティ、認証とアクセス制御、セキュアプログラミング、プロジェクトマネジメント、情報セキュリティマネジメント、デジタルフォレンジックス、不正アクセス技法、プライバシー保護とディジタル著作権管理	サーバ構築･運用実践演習、 ネットワークセキュリティ実践演習、 企業インターンシップ
4年次	セキュリティ運用とインシデントレスポンス、脆弱性管理、情報セキュリティ監査	インシデント対応演習、 卒業研究

（３）適用条件

３～４年次の専門科目は情報セキュリティに関する科目中心で構成可能とする。また、情報セキュリティ分野の専門性を備えた教員を確保することを前提とする。なお教育の所属については学内に限る必要はなく、外部講師や産業界講師でも差し支えない。

（４）産業界で用いられる指標等との対応

本カリキュラムで受講可能な科目と産業界で用いられるスキル分類との対応関係を次表に示す。

表 42　産業界で用いられる指標との対応（例示③）

記号凡例： ◎=演習を伴う実践的専門教育 ○=座学中心の専門教育 ◇=基礎的/入門的教育 ★=状況に応じてケースバイケース ※=習得済が受講の前提 緑色は[産]*及び[情]*で求めているスキル 水色縦線は[産]*のみで求めているスキル			iコンピテンショナリディクショナリのスキル分類												
			メソドロジ					テクノロジ							関連知識
			戦略	企画	実装	利活用	支援活動	システム	開発	保守・運用	非機能要件	組込み・計測・制御	共通技術	
SecBoK2016 知識項目	基礎	工学基礎									○	○	○	
		ICT 基礎		◎	◎			◎	◎	◎	◎	◎	◎	
		ビジネス基礎				○	○							◎
	セキュリティ専門分野	セキュリティ基礎									◎			
		セキュリティガバナンス												
		セキュリティマネジメント				○	○				○			
		ネットワークセキュリティ						◎			○			
		システムセキュリティ						◎	○		○			
		セキュアシステム設計・構築			○			◎	○		○			
		セキュリティ運用			○	○	○	○		○	○			
		暗号・認証・電子署名									○			
		サイバー攻撃手法									◎			
		デジタルフォレンジック									○			
		法・制度・標準				◇	○				○			◇

＊［産］産業横断サイバーセキュリティ人材育成検討会「人材定義リファレンスに基づくスキルマッピング」が求めるスキル
［情］情報処理安全確保支援士試験シラバスにおける要求される知識に対応するスキル

（５）実施上の工夫点

情報セキュリティを専門とする職種への就職を希望する学生と、その他職種を希望する学生の双方の要望に応えるカリキュラムとする必要がある。基盤技術については情報セキュリティへの応用に特化しない形で教育することが望ましい。一方で選択科目において、情報セキュリティサービスベンダに勤務する方を講師とする講座を設けたり、脆弱性検査やデジタルフォレンジック技術などを専門的に学ぶ講義や演習を設けたりすることが考えられる。

３．３．４ 例示④：修士課程に進学予定の情報系学士課程の学生を対象とするもの

（１）概要

本カリキュラムの概要を次表に示す。

表 43　例示④概要

大学における情報セキュリティ教育のためのモデル・コア・カリキュラム　例示④		
進学予定の情報系学士課程在籍者を対象とする情報セキュリティ分野の実践講座向け		
種別		科目シラバス
想定する受講者		修士課程でセキュリティを学びたいと考える学士課程3～4年次在籍者
受講者の知識・スキル		理工系教養科目＋情報リテラシー教育を想定する
育成する人材像		情報セキュリティを本格的に学ぶ上で必要となる基盤的知識を習得した人材
到達目標	コア部分	情報セキュリティ分野の要素技術（網羅的でなく部分的でよい）の習得を通じて対策の重要性と脅威に応じた対策方法について理解する。
	コア以外を含むカリキュラム全体	（コア部分に同じ）
関連科目との関係		・本科目受講に先立って受講しておくべき科目を設定しないが、受講する学生の前提知識に応じて、以下の内容に関する教育を推奨する。 ①情報とデジタルデータの概念 ②コンピュータとして総称することが可能な機器の概念
実施方法		講義及び演習

（２）科目構成例

本カリキュラムにおける科目構成例は、例示②に準じるものとする。

表 44　科目構成例

学年	講義	演習等
基礎科目	コンピュータシステム、基礎数学、情報理論、アルゴリズムとデータ構造、情報論理学、コンピュータアーキテクチャ、オペレーティングシステム、データベース、ソフトウェア工学、コンパイラ、システムプログラム、コンピュータネットワーク、情報セキュリティ、数値解析、リスクマネジメント、情報法制度、テクニカルライティング	プログラミング基礎演習、 プログラミング実践演習
専門科目	セキュリティ総論 A（倫理、評価、運用） セキュリティ総論 B（暗号基礎から応用） セキュリティ総論 C（システム基礎から制度）	セキュリティ基礎演習 ログ解析演習 クラウド・セキュリティ演習 インシデントレスポンス演習 サイバープログラミング演習 サイバーディフェンス基礎演習 CSIRT 基礎演習

（３）適用条件

例示②に準じる。

（４）産業界で用いられる指標等との対応

例示②に準じる。

（５）実施上の工夫点

本例示における教育内容は例示②と実質的に同じである。ただし、進学を前提とした受講者を対象としているので、演習等の実施に際して受講者が今後さらなる学習の必要性を実感できるような課題設定の工夫を行うことが望ましい。

３．３．５ 例示⑤：情報セキュリティに関する単独の科目を対象とするもの

（１）概要

本カリキュラムの概要を次表に示す。

表 45　例示⑤概要

大学における情報セキュリティ教育のためのモデル・コア・カリキュラム　例示⑤		
修士課程在籍者を対象とする情報セキュリティ分野の単独科目向け		
種別		科目シラバス
想定する受講者		情報セキュリティ以外の分野を専攻する修士課程在籍者等
受講者の知識･スキル		理系大学卒業程度の知識・スキルを想定する
育成する人材像		情報セキュリティに関する基本的な知識を備えた人材 （セキュリティ分野への就職は前提としない）
到達目標	コア部分	産業界で技術者として活躍する際に知っておくべき情報セキュリティの考え方について、主要な脅威とその対策に関する技術的背景知識を通じて理解する。
	コア以外を含むカリキュラム全体	コア部分の知識の種類を拡張した形で、より幅広い脅威や対策技術について理解する。
関連科目との関係		・修士課程において前提とする科目等はなし。
実施方法		講義（演習を含めても可）

（２）科目構成例

次表の二つの科目構成例は、情報セキュリティ以外の分野を専攻する修士課程在籍者を対象としている。

科目構成例（１）は、IT を利用する企業等において実践知識として役立つことに重点を置いた構成となっており、社会人学生の多い大学院にも適する。また、社会人の学び直しにおいても利用できる内容である。

一方、科目構成例（２）は、学部において情報セキュリティに関する講義を受ける機会が無かった（または少なかった）学生が、情報セキュリティに関する基本的な知識を備えることに適した科目構成としている。

表 46　科目構成例（１）

回数	講義内容	解説
1	情報セキュリティ基礎知識	情報セキュリティの基本的な概要を学び、現在社会が直面する情報セキュリティ課題と企業活動におけるセキュリティの重要性を理解するために実社会におけるサイバー攻撃の脅威と要因、およびサイバー攻撃対策に必要な考え方について学ぶ。サイバー攻撃への対策では、技術的・物理的な対策から人的・組織的対策まで総合的に取り組むことの重要性を学ぶ。

回数	講義内容	解説
2	情報セキュリティを支える暗号技術の基礎と応用(1)	暗号技術の基礎として、共通鍵暗号、ハッシュ関数、公開鍵暗号とその応用である電子署名と PKI について学ぶ。
3	情報セキュリティを支える暗号技術の基礎と応用(2)	インターネットで重要な相手認証の概要と暗号技術や実装技術の評価の重要性について学ぶ。また、アルコリズムだけでなく暗号化技術を実装したハードウェやソフトウェアの評価の重要性について学ぶ。
4	ネットワークを守る認証技術とシステム技術(1)	「なりすまし」を防ぐために用いられる認証技術や「なりすまし対策」について紹介し、その効果を理解する。多要素認証、多ルート認証、認証に関わる TIPS を紹介。
5	ネットワークを守る認証技術とシステム技術(2)	不正なネットワーク接続を防御するための要素技術を学ぶ。不正なアクセスからネットワークを守る認証技術、アクセス制御技術と対応するアプライアンス機器の概要を学ぶ。また、広く利用が普及している無線 LAN とスマートフォンのセキュリティ対策についても学ぶ。
6	企業の情報ネットワークシステムのセキュリティ	企業の情報ネットワークのセキュリティ課題と対応する防御技術としてネットワークの仮想化、侵入検知技術、セキュリティ管理業務と支援システムについて学ぶ。
7	ソフトウェアのセキュリティ課題と対策	ソフトウェアに潜む脆弱性について学ぶ。マルウェアの侵入の手口となるバッファオーバーフローを例に攻撃の仕組みや OS やシステム・ソフトウェアによる対策技術の概要について学ぶ。
8	情報セキュリティマネジメントのフレームワーク(1)	情報セキュリティマネジメントにおける事故事例から情報セキュリティマネジメントの重要性とそのフレームワーク（PDCA サイクル）について学ぶ。
9	情報セキュリティマネジメントのフレームワーク(2)	情報セキュリティに関連する国際標準とガイドラインの概要とソフトローの役割について学ぶ。また、情報セキュリティに関連する認証制度の概要として ISMS 適合性評価制度の概要について学ぶ。
10	情報セキュリティのリスクマネジメントとリスクコントロール(1)	情報セキュリティマネジメントにおけるリスクマネジメント手法の概要を学びリスクの分析方法、リスクの評価方法について事例をベースに学ぶ。
11	情報セキュリティのリスクマネジメントとリスクコントロール(2)	リスクコントロールの具体例として物理的な対策（耐震対策、入退管理、バックアップ拠点等）、人的・組織的な対策（教育訓練、機密保持契約、誓約書、管理体制等）、そして技術的な対策（セキュリティ機器の設計、導入、運用等）について学ぶ。
12	情報セキュリティの関わる法律の基礎知識(1)	最新のセキュリティ関連の法律について焦点を当てサイバーセキュリティ基本法、不正アクセス禁止法などセキュリティに関係する主要な法律の内容について学ぶ。

回数	講義内容	解説
13	情報セキュリティの関わる法律の基礎知識(2)	個人情報保護法やプロバイダ責任制限法などネットワークの上での権利・利益を保護し、それが侵害されたときの対応に関係する法律の概要を学ぶ。また情報セキュリティに関係して理解しておくことが望ましい法律についても学ぶ。
14	Web データベース・クラウドのセキュリティと CSIRT(1)	事例をベースに Web アプリケーションに潜む脆弱性、攻撃の仕組みと被害、有効なセキュリティ対策について学ぶ。また、企業情報システムを例にデータベース、Web、電子メール、クラウドに関わる脅威と被害、および必要なセキュリティ対策について総合的に学ぶ。
15	Web データベース・クラウドのセキュリティと CSIRT(2)	企業組織における CSIRT の役割とサイバーセキュリティに関わる国際的な取り組みとして国際的な連携活動や情報共有の取り組みについて学ぶ。

表 47　科目構成例（2）

回数	講義内容	解説
1	情報におけるリスクとは	IT における情報とは何であり、情報セキュリティ事故が自分自身を含む社会全体に対して多大な影響を与える可能性があることを事例を通じて理解できることを目標とする。また、情報セキュリティにおける攻撃方法とその対策についての概要を学ぶ。
2	インターネット概説＆Webシステム概要	・インターネットの発展と情報セキュリティ ・クロスサイトにまたがる情報セキュリティ脅威 ・SQL インジェクション ・その他の脅威
3	ネットワーク基礎技術	・伝送方式と特徴 ・TCP/IP ネットワーク ・アドレッシング ・経路制御 ・無線ネットワーク
4	ネットワークリスク	・単一障害点、ボトルネック ・相互接続 ・なりすまし、権限の取得・昇格 ・侵入・攻撃（DoS/DDoS 攻撃、バックドア等）
5	Webサーバーシステムリスク	・Web システムにおける情報セキュリティ ・ネットワークセグメント毎のセキュリティレベル ・Web システム企業標的の不正アクセス ・一般人が対象にされるソーシャルエンジニアリング攻撃
6	Webアプリケーションへの脅威	・Web アプリケーションの仕組み ・脆弱性の原理と対策（SQL インジェクション）

回数	講義内容	解説
		・Web アプリケーションのライフサイクルとセキュリティ
7	映画に学ぶ情報セキュリティ基礎技術	・セキュリティ初心者でも理解しやすい内容として、映画で見るハッキングの基礎技術（ソーシャルハッキング、スキャニング、バックドア、スニッフィング、ウォードライビング等）について説明を実施
8	IT技術まとめ	・インターネット初期のころのセキュリティ対策 ・現在のインターネットとセキュリティ ・IT 技術とセキュリティ
9	オペレーティングシステムおけるセキュリティ	・オペレーティングシステムとは ・OS のセキュリティリスク ・OS のセキュリティ対策 ・保守と運用
10	認証とアクセス制御	・認証とアクセス制御（認可）とは ・認証技術 ・アクセス制御方法
11	システム運用管理リスク	・電子メールのセキュリティ対策技術 ・運用管理における対策技術
12	情報セキュリティ運用と管理	・個人としてのセキュリティ ・組織としてのセキュリティ ・コンピュータ管理者としてのセキュリティ
13	BYODにおけるセキュリティの脅威と防御策	・BYOD、その脅威と対策について ・身近な情報端末における脅威と対策について
14	事業継続リスク概説	・Business Continuity:BC とは ・リスク管理、事業継続計画、災害対策の定義と相互関係 ・直下型地震への対応
15	情報リスク管理総括	・情報リスク管理・セキュリティ総まとめ

（３）適用条件

情報セキュリティ分野を専門とする教員が講師を務めることが望ましいが、セキュリティ分野を専門としない情報系専攻の教員等による実施等も考慮した内容とする。

（４）産業界で用いられる指標等との対応

本カリキュラムで受講可能な科目と産業界で用いられるスキル分類との対応関係を次表に示す。

表 48　産業界で用いられる指標との対応（例示⑤）

記号凡例： ◎=演習を伴う実践的専門教育 〇=座学中心の専門教育 ◇=基礎的/入門的教育 ★=状況に応じてケースバイケース ※=習得済が受講の前提 緑色は[産]*及び[情]*で求めているスキル 水色縦線は[産]*のみで求めているスキル			iコンピテンショナリディクショナリのスキル分類												
			メソドロジ					テクノロジ							関連知識
			戦略	企画	実装	利活用	支援活動	システム	開発	保守・運用	非機能要件	組込み・計測・制御	共通技術	
SecBoK2016 知識項目	基礎	工学基礎									※			
		ICT 基礎				※	※	※			※			
		ビジネス基礎												
	セキュリティ専門分野	セキュリティ基礎									〇			
		セキュリティガバナンス					◇							
		セキュリティマネジメント				◇	〇				〇			
		ネットワークセキュリティ						◇			〇			
		システムセキュリティ		◇				◇			〇			
		セキュアシステム設計・構築		◇				◇						
		セキュリティ運用				◇	〇	◇			〇			
		暗号・認証・電子署名									〇			
		サイバー攻撃手法									〇			
		デジタルフォレンジック									◇			
		法・制度・標準				◇	〇				◇			◇

＊［産］産業横断サイバーセキュリティ人材育成検討会「人材定義リファレンスに基づくスキルマッピング」が求めるスキル
［情］情報処理安全確保支援士試験シラバスにおける要求される知識に対応するスキル

（５）実施上の工夫点

情報セキュリティ分野の関連領域は数学、工学、法学、社会学等幅広く、すべての領域において専門性を発揮できる教員はいないと考える必要がある。領域ごとに参考資料を準備し、教員による講義資料作成に活用してもらえるようにすることが望ましい。

３．３．６ 例示⑥：専門とは別に情報セキュリティを学ぶコース等を対象とするもの

（１）概要

本カリキュラムの概要を次表に示す。

表 49　例示⑥概要

大学における情報セキュリティ教育のためのモデル・コア・カリキュラム　例示⑥		
修士課程在籍者を対象とする情報セキュリティ専門講座等向け		
種別		科目シラバス
想定する受講者		専門とは別に情報セキュリティを学ぼうと考える修士課程在籍者等
受講者の知識・スキル		理系大学卒業程度の知識・スキルを想定する
育成する人材像		習得した知識･実践的経験を自らの専門分野のセキュリティ対策に活かせる人材
到達目標	コア部分	産業界で技術者として活躍する際に知っておくべき情報セキュリティの考え方について、脅威の特徴や対策に用いられる要素技術に関する専門的内容を座学と演習の組み合わせを通じて理解する。
	コア以外を含むカリキュラム全体	コア部分の知識の種類を拡張した形で、より幅広い脅威や対策技術について理解する。
関連科目との関係		以下について十分な知識を有することを前提とする。 ・コンピュータネットワーク（TCP/IP、無線LAN） ・コンピュータアーキテクチャ ・オペレーティングシステム（Windows及びUNIX系） ・プログラミング言語（C言語、アセンブラ）
実施方法		講義及び演習

（２）科目構成例

表 50　科目構成例（コア部分のみ実施）

講座例	おもな内容	解説
情報セキュリティの基盤技術と知識（必須科目）	情報セキュリティの基礎 クラウドにおけるセキュリティ問題 インターネットにおける様々なリスクと対策 アセンブラ基礎 デジタルフォレンジックの基礎 情報セキュリティに関する法律 リスクマネジメントとペネトレーションテスト 情報セキュリティに対する政府の考え方	情報セキュリティ分野の専門科目の講義や演習に参加する上であらかじめ習得しておくべき知識について網羅的に学ぶ。
最新情報セキュリティ理論と応用（講義形式・選択科目）	楕円曲線暗号方式の理論と実装 脅威分析技術 セキュアプログラミング技術 システム管理保護技術 関連技術（OS アクセス制御、PKI、リバースエンジニアリング等）	情報セキュリティ分野の最新技術に関する理論的背景と応用事例について学ぶ。

講座例	おもな内容	解説
セキュリティ PBL 演習（集中合宿による演習形式、選択科目）	無線 LAN セキュリティ演習 システム攻撃・防御演習 リスクマネジメント演習 インシデント体験演習 IT 機器管理演習 ハードウェア・セキュリティ演習 システム侵入・解析演習	情報セキュリティ分野で実際に活用されている脅威への対策について、その要素技術と活用方法を具体的な演習を通じて学ぶ。

（3）適用条件

本カリキュラムは情報セキュリティ分野の基盤技術に関して学習済みであることを前提としている。表 50 の必須科目「情報セキュリティの基盤技術と知識」はこれらの基盤技術に関する教育を補うものであり、すべての受講者に十分な知識があるとみなせる場合は内容を軽減ないし必須としないことも可能である。

（4）産業界で用いられる指標等との対応

本カリキュラムで受講可能な科目と産業界で用いられるスキル分類との対応関係を次表に示す。

表 51　産業界で用いられる指標との対応（例示⑥）

記号凡例: ◎=演習を伴う実践的専門教育 ○=座学中心の専門教育 ◇=基礎的/入門的教育 ★=状況に応じてケースバイケース ※=習得済が受講の前提 緑色は[産]*及び[情]*で求めているスキル 水色縦線は[産]*のみで求めているスキル			iコンピテンショナリディクショナリのスキル分類												
			メソドロジ					テクノロジ							関連知識
			戦略	企画	実装	利活用	支援活動	システム	開発	保守・運用	非機能要件	組込み・計測・制御	共通技術	
SecBoK2016 知識項目	基礎	工学基礎									※			
		ICT 基礎		※	※			※	※	※	※			
		ビジネス基礎												
	セキュリティ専門分野	セキュリティ基礎									◎			
		セキュリティガバナンス					◎							
		セキュリティマネジメント	○			○	◎				◎			
		ネットワークセキュリティ						◎			◎			
		システムセキュリティ		◎				◎	○		◎			
		セキュアシステム設計・構築		○	○			◎	○		◎			
		セキュリティ運用			○	◎	◎	◎		○	◎			
		暗号・認証・電子署名									◎			
		サイバー攻撃手法									◎			
		デジタルフォレンジック									◎			
		法・制度・標準				○	○				○			○

＊[産] 産業横断サイバーセキュリティ人材育成検討会「人材定義リファレンスに基づくスキルマッピング」が求めるスキル
[情] 情報処理安全確保支援士試験シラバスにおける要求される知識に対応するスキル

（５）実施上の工夫点

本カリキュラムの対象人材は「分野・地域を越えた実践的情報教育協働ネットワーク（セキュリティ分野）」（enPiT Security / SecCap）プログラムにおける想定と近く、同プログラムのスキーム等の活用は有効である。

３．３．７ 例示⑦：情報セキュリティを専門とする専攻等を対象とするもの

（１）概要

本カリキュラムの概要を次表に示す。

表 52　例示⑦概要

大学における情報セキュリティ教育のためのモデル・コア・カリキュラム　例示⑦		
情報セキュリティを専門とする専攻科向け		
種別		カリキュラム
想定する受講者		情報セキュリティを専門とする専攻科の学生
受講者の知識･スキル		理系大学卒業程度の知識・スキルを想定する
育成する人材像		情報セキュリティに関する専門的な知識と実践的な経験、及び意識を備えた人材とし、セキュリティの専門性をある程度発揮できる環境への就職等を想定する
到達目標	コア部分	産業界で技術者として活躍する際に知っておくべき情報セキュリティの考え方について、脅威の特徴や対策に用いられる要素技術に関する専門的内容を座学と演習の組み合わせを通じて体系的に理解する。
	コア以外を含むカリキュラム全体	コア部分の知識の種類を拡張した形で、より幅広い脅威や対策技術について体系的に理解する。
関連科目との関係		専攻内で体系的に整備する。
実施方法		講義及び演習、修士論文

（２）科目構成例

表 53　科目構成例

学年	講義	演習等
理論系	暗号理論、暗号･認証と社会制度、アルゴリズム基礎、数論基礎、計算代数、統計的方法論	
技術系	暗号プロトコル、インターネットテクノロジ、不正アクセス技法、ネットワークシステム設計･運用管理、セキュアシステム構成論、情報デバイス技術、情報システム構成論、オペレーティングシステム、セキュアプログラミングとセキュアOS、ソフトウェア構成論、ペネトレーション技法、統計的リスク管理、個人識別とプライバシー保護	プログラミング実習、 セキュアシステム実習、 ネットワークセキュリティ技術演習、 Webアプリケーションと脆弱性対策演習、 デジタルフォレンジック演習
マネジメント系	情報セキュリティマネジメントシステム、セキュリティシステム監査、セキュリティ管理と経営、リスクマネジメント、組織行動と情報セキュリティ、セキュア法制と情報倫理、法学基礎、知的財産制度、国際標準とガイドライン、セキュリティの法律実務、リスクの経済学、マスメディアとリスク管理	インシデント対応とCSIRT基礎演習、 組織経営とセキュリティマネジメント演習、 事業継続マネジメント演習
その他	情報セキュリティ特別講義	情報セキュリティ輪講 修士論文

（３）適用条件

本カリキュラムは大学院修士課程における独立した専攻として設計しており、情報セキュリティ分野の専門性を備えた教員を確保することを前提とする。なお、教員の所属は学内に限らず、外部講師や産業界講師を活用することでも差し支えない。

（４）産業界で用いられる指標等との対応

本カリキュラムで受講可能な科目と産業界で用いられるスキル分類との対応関係を次表に示す。

表 54　産業界で用いられる指標との対応（例示⑦）

記号凡例: ◎=演習を伴う実践的専門教育 〇=座学中心の専門教育 ◇=基礎的/入門的教育 ★=状況に応じてケースバイケース ※=習得済が受講の前提 緑色は[産]*及び[情]*で求めているスキル 水色縦線は[産]*のみで求めているスキル			iコンピテンショナリディクショナリのスキル分類												
			メソドロジ					テクノロジ							関連知識
			戦略	企画	実装	利活用	支援活動	システム	開発	保守・運用	非機能要件	組込み・計測・制御	共通技術	
SecBoK2016 知識項目	基礎	工学基礎									※	※	※	
		ICT 基礎		※	※			※	※	※	※	※	※	
		ビジネス基礎	※		※	※	※							※
	セキュリティ専門分野	セキュリティ基礎									◎			
		セキュリティガバナンス					◎							
		セキュリティマネジメント	◎			◎	◎				◎			
		ネットワークセキュリティ						◎			◎			
		システムセキュリティ		◎				◎	◎		◎			
		セキュアシステム設計・構築		◎	◎			◎	◎		◎			
		セキュリティ運用			◎	◎	◎	◎		◎	◎			
		暗号・認証・電子署名									◎			
		サイバー攻撃手法									◎			
		デジタルフォレンジック									◎			
		法・制度・標準				○	◎				◎			○

＊[産] 産業横断サイバーセキュリティ人材育成検討会「人材定義リファレンスに基づくスキルマッピング」が求めるスキル
[情] 情報処理安全確保支援士試験シラバスにおける要求される知識に対応するスキル

（５）実施上の工夫点

（３）に示したように、独立した専攻を対象としており、カリキュラム編成上の制約は少ないものと思われる。

３．３．８ 例示⑧：社会人学び直し向け短期（２週間程度）集中コース

（１）概要

本カリキュラムの概要を次表に示す。

表 55　例示⑧概要

大学における情報セキュリティ教育のためのモデル・コア・カリキュラム　例示⑧		
社会人学び直し:短期(２週間程度)集中コース向け		
種別		科目シラバス
想定する受講者		情報セキュリティの学び直しをしたい現役IT技術者（30代中～後半）
受講者の知識･スキル		産業界で情報系業務に従事している技術者を想定する
育成する人材像		習得した情報セキュリティに関する実践的知識･経験を自らの業務に活かせる人材
到達目標	コア部分	下記テーマについて、業務遂行に必要な知識を習得する。 （テーマ例） ・組織における標的型攻撃対策 ・ソフトウェアの設計・開発段階におけるセキュリティ対策 ・情報セキュリティマネジメントと情報セキュリティ監査 ・CSIRT運営 ・デジタルフォレンジック
	コア以外を含むカリキュラム全体	（コア部分と同じ）
関連科目との関係		以下の領域のうち、当該コース内容を理解する上で必要なものについて基本的な知識を有することを前提とする（募集要項等で明示） ・コンピュータネットワーク（TCP/IP、無線LAN） ・コンピュータアーキテクチャ ・オペレーティングシステム（Windows及びUNIX系） ・プログラミング言語（C言語、アセンブラ）
実施方法		講義及び演習

（２）科目構成例

CSIRT 構築と運営を担う技術者の育成のため、CSIRT 構築の手引き、ネットワークと Web アプリケーションの検査、デジタルフォレンジックの演習を組み合わせた 9 日間の集中コースの例を表 56～表 58 に示す。それぞれのコースは単独でも受講できる内容としている。

(1) CSIRT 構築の手引き　(2 日間)

(2) ネットワークと Web セキュリティ技術演習　（3 日間）

(3) デジタルフォレンジック演習（4 日間）

表 56　科目構成例(1)：CSIRT 構築の手引き

コース内容	企業組織などでインシデント対応を担う企業内 CSIRT の基本的な役割と活動の考え方、企業を脅かす攻撃とその防御策について学ぶコース。セキュリティインシデント対応の基本的なプロセス、および対応時に用いられる技術について、解説と演習を通して習得するほか、組織内でのインシデント対応組織（CSIRT）の立上げと運用、および CSIRT 連携の進め方についてケーススタディを通して学ぶ。また、現実に起きている攻撃手法のデモや Web サーバのログ解析演習を通して、サイバー攻撃によるインシデントの実例について学ぶ。

回数	講義内容	解説
1～4 （1 日）	CSIRT 基礎と実践	• 企業におけるセキュリティリスクへの取組の基本、事故前提の活動、CSIRT の役割、CSIRT の活動例 • CSIRT ケーススタディ • CSIRT インシデントハンドリングの基本 • CSIRT インシデントハンドリングの基礎演習実
5～8 （1 日）	CSIRT 技術演習	• 導入解説、最近のサイバーセキュリティ動向、攻撃手法のデモ • 代表的な Web サーバ（Apache）のログの解説、ログ解析演習 1（URL デコード）、ログ解析演習 2（SQL インジェクション）と解説 • 攻撃手法のデモ（Gumblar またはシェル奪取）、ログ解析演習 3（ブルートフォース）、ログ解析演習 4（ディレクトリトラバーサル）と解説 • 攻撃手法のデモ（クロスサイトスクリプティング）、ログ解析演習 5（クロスサイトスクリプティング）と解説、IDS/IPS 概説、まとめ

表 57　科目構成例(2)：ネットワークと Web セキュリティ技術演習

コース内容	Web サーバ、メールサーバ等の設置・運用に際して必要となる基礎的なセキュリティ技術の習得を狙いとして、検査ツールを利用したサーバに対するポートスキャン検査演習と脆弱性検査演習を行うとともに、発見された脆弱性を是正するための対策演習を行い、結果を報告書にまとめる演習を実施する。Web サーバの構築や運用に必要となる Web アプリケーションセキュリティ検査の知識及び技術を習得し、独力で Web アプリケーションセキュリティ検査を実施し、その結果に応じて必要な対処を提案できる基礎スキルを身につけることを狙いとする。具体的には、脆弱性を持つ Web サーバが設置された環境を利用し、主要な検査項目の演習を集中して行うとともに、対策の提案を含む検査結果報告書をまとめる演習を実施する。

回数	講義内容	解説
1～4 （1 日）	ネットワークセキュリティ技術	• オリエンテーション • ネットワークセキュリティ検査の概要 • ポートスキャン検査演習（nmap） • 脆弱性検査ツールの使用方法と脆弱性検査演習（Nessus） • 発見された脆弱性への対策演習と効果の確認 • 検査結果報告書作成と発表 • まとめ
5～12 （2 日）	Web アプリケーション検査	• オリエンテーション • Web アプリケーション検査の流れ • 入力パラメータの事前調査演習 • 入力検査演習 • セッション検査演習 • 強制ブラウジング検査演習 • 脆弱性対策の概説 • 検査結果報告書の作成とまとめ

表 58　科目構成例(3)：デジタルフォレンジック演習

コース内容	インシデント発生後の対処に必要となるデジタルフォレンジック技術の基礎を習得することを狙いとする。具体的には、デジタルフォレンジックの基礎知識・技術の解説、Windows 端末の解析で共通的に実施される基本的な作業に関する解説と実習、企業におけるインシデントを想定した本格的な解析演習を集中して行うとともに、結果を報告書にまとめる演習を実施する。

回数	講義内容	解説
1～4 （1日）	デジタルフォレジックの基礎	• オリエンテーション • デジタルフォレンジックとは • デジタルフォレンジックに必要な知識と作業の流れ • 各種オープンソース解析ツールの使い方
5～8 （1日）	予備演習：Windows パソコン利用者が行った操作を知り、その痕跡を調査	• ファイルシステムのタイムスタンプ • レジストリ • イベントログ • Web アクセス履歴 • USB デバイス接続履歴、等
9～16 （2日）	解析演習：ある企業からの情報漏えいの原因、影響範囲等を解析	• 情報漏えいの原因となった不正アクセス等の解析 • 情報漏えい経路の解析 • 不正アクセスに伴う影響範囲の解析、等 • 解析結果報告書の作成 • 振り返り：解析対象パソコンで起きていたことの解説

（3）適用条件

期間は必要な講義・演習数等に応じて調整することになる。

（4）産業界で用いられる指標等との対応

本カリキュラムで受講可能な科目と産業界で用いられるスキル分類との対応関係を次表に示す。

表 59　産業界で用いられる指標との対応（例示⑧）

記号凡例： ◎=演習を伴う実践的専門教育 〇=座学中心の専門教育 ◇=基礎的/入門的教育 ★=状況に応じてケースバイケース ※=習得済が受講の前提 緑色は[産]*及び[情]*で求めているスキル 水色縦線は[産]*のみで求めているスキル			iコンピテンショナリディクショナリのスキル分類												
			メソドロジ					テクノロジ							関連知識
			戦略	企画	実装	利活用	支援活動	システム	開発	保守・運用	非機能要件	組込み・計測・制御	共通技術	
SecBoK2016 知識項目	基礎	工学基礎									※	※	※	
		ICT 基礎		※	※			※	※	※	※	※	※	
		ビジネス基礎	※		※	※	※							※
	セキュリティ専門分野	セキュリティ基礎									※			
		セキュリティガバナンス					★							
		セキュリティマネジメント	★			★	★				★			
		ネットワークセキュリティ						★			★			
		システムセキュリティ		★				★	★		★			
		セキュアシステム設計・構築		★	★			★	★		★			
		セキュリティ運用			★	★	★	★		★	★			
		暗号・認証・電子署名									★			
		サイバー攻撃手法									★			
		デジタルフォレンジック									★			
		法・制度・標準				★	★				★			★

＊[産] 産業横断サイバーセキュリティ人材育成検討会「人材定義リファレンスに基づくスキルマッピング」が求めるスキル
[情] 情報処理安全確保支援士試験シラバスにおける要求される知識に対応するスキル

（５）実施上の工夫点

これまで社会人向け講座等を実施していない大学等で行う場合、まず短期のものから開始することが現実的と考えられる。実施方法の詳細については４．２．５に示す。

３．３．９ 例示⑨：社会人学び直し向け中期（３～６ヶ月程度）コース

（１）概要

本カリキュラムの概要を次表に示す。

表 60　例示⑨概要

大学における情報セキュリティ教育のためのモデル・コア・カリキュラム　例示⑨		
社会人学び直し：中期（３～6ヶ月程度）コース向け		
種別		科目シラバス
想定する受講者		情報セキュリティの学び直しをしたい現役IT技術者（30代中～後半）
受講者の知識・スキル		産業界で情報系業務に従事している技術者を想定する
育成する人材像		習得した情報セキュリティに関する実践的知識・経験を自らの業務に活かせる人材
到達目標	コア部分	下記の複数テーマに関する業務遂行に必要な知識を習得し、複合的な領域で構成される業務や脅威への対策に関する能力を得る。 （テーマ例） ・組織における標的型攻撃対策 ・ソフトウェアの設計・開発段階におけるセキュリティ対策 ・情報セキュリティマネジメントと情報セキュリティ監査 ・CSIRT運営 ・デジタルフォレンジック
	コア以外を含むカリキュラム全体	（コア部分と同じ）
関連科目との関係		以下の領域のうち、当該コース内容を理解する上で必要なものについて基本的な知識を有することを前提とする（募集要項等で明示） ・コンピュータネットワーク（TCP/IP、無線LAN） ・コンピュータアーキテクチャ ・オペレーティングシステム（Windows及びUNIX系） ・プログラミング言語（C言語、アセンブラ）
実施方法		講義及び演習

（２）科目構成例

企業の CSIRT 組織の構築および CSIRT のチームメンバ人材の育成を想定した科目構成例を表 61 に示す。この構成例では、座学主体の基礎講義 3 科目、応用科目 2 科目とハンズオン主体の演習科目（社会人学び直し向け短期集中コースの科目例と同じ）を 3～6 か月程度で学ぶことにより、受講する社会人が所属する企業の CSIRT の中核メンバとして活動するために役立つ能力を得ること目標としている。基礎講義と応用講義は、それぞれ 1 コマ（90 分）ずつの開講を予定しているが、演習科目は、演習の効率面から、2 日から 3 日程度の単位で集中開講とすることが望ましい。

表 61　科目構成例

科目	講義名・コマ数	解説
基礎講義 1	セキュアシステム構成論・15 コマ（各 90 分）	• 情報セキュリティ概論 • さまざまな事例から見るシステムの脆弱性 • 情報システムに到達する不正経路という視点で「セキュアな情報システムとは何か」ついて考察 • セキュリティポリシーという視点で、情報システム全体の構成要素について見ていくことで、セキュアなシステムをどのように構成するか整理する
基礎講義 2	セキュアプログラミングとセキュア OS・15 コマ（各 90 分）	• ソフトウェアの脆弱性 • 設計レベルの問題と実装レベルの問題 • バッファオーバーフロー攻撃の仕組みと防御策 • Web アプリケーションの脆弱性 • 隔離実行、サンドボックス • セキュア OS とアクセス制御
基礎講義 3	ネットワークシステム設計・運用管理・15 コマ（各 90 分）	• ネットワーク設計のための理論（待ち行列理論、トラヒック理論、グラフ理論、信頼性理論） • ネットワークサービス • VLAN と VPN • 企業ネットワーク構築と運用管理の概要 • ネットワークセキュリティ対策技術 • 仮想ネットワーク技術とクラウド、SDN
基礎講義 4	インターネットテクノロジ・15 コマ（各 90 分）	• インターネットの生い立ちと発展の経緯、標準化 • ネットワークアーキテクチャ、ネットワークトポロジ、ネットワークの分類 • LAN 技術（イーサネット、衝突制御、誤り制御、フロー制御） • 無線 LAN、ダイヤルアップ接続 • IP アドレス、アドレス変換、アドレス解決、IPv4 パケット • ルーティング • TCP と UDP、再送制御、輻輳制御 • DHCP、DNS、FTP

科目	講義名・コマ数	解説
		• WWW、電子メール、P2P ファイル交換 • セキュリティプロトコル（IPsec、SSL） • 監視・管理（ICMP、SNMP） • IPv6（IPv6 パケット、IPv4 からの移行） • IP 電話（SIP、音声品質） • QoS（Intserv、Diffserv、キューイング） • マルチキャスト
演習	CSIRT 構築と運営 （詳細は表 56～表 58 参照）	• CSIRT 構築の手引き (2 日間・8 コマ・各 90 分) • ネットワークと Web セキュリティ技術演習 （3 日間・12 コマ・各 90 分） • デジタルフォレンジック演習（4 日間・16 コマ・各 90 分）
応用講義 1	ハッキングとマルウェア・15 コマ（各 90 分）	• 偵察とソーシャルエンジニアリング • スキャンと脆弱性識別 • システムハッキング • トロイの木馬，バックドア，ウィルス，ワーム • スニッファ • マルウェアの概要と作成 • マルウェア解析環境構築、マルウェア収集、表層解析 • アセンブラの基礎とプログラミング • バイナリファイルの構成 • 動的解析、静的解析、アンチ解析技術
応用講義 2	組織行動と情報セキュリティ・15 コマ（各 90 分）	• 組織の定義と組織行動論の枠組み • モチベーションと組織への貢献 • 組織コミットメントと組織の成果 • 集団のダイナミクス • リーダーシップの役割 • 組織文化の概念と機能、形成と変革 • 組織学習：不完全な組織学習をもたらす要因 • 意思決定のバイアス • 意思決定の課題と改善 • 危機管理組織のマネジメント

科目	講義名・コマ数	解説
		• 企業事故･不正行動の事例研究 • 組織変革の立案と策定

（３）適用条件

期間は必要な講義・演習数等に応じて調整することになる。

（４）産業界で用いられる指標等との対応

例示⑧に準じる。

（５）実施上の工夫点

本カリキュラムは、情報セキュリティ分野に関するさまざまな領域の専門的知識を備えた人材を多数擁する高等教育機関での実施を前提とする。

上記の基礎講義や応用講義をコンパクトに実施する場合は、例示⑤で示した科目構成例（１）を活用することも検討に値する。

３．３．１０ 例示⑩：社会人学び直し向け長期（１年程度）コース

（１）概要

本カリキュラムの概要を次表に示す。

表 62　例示⑩概要

大学における情報セキュリティ教育のためのモデル・コア・カリキュラム　例示⑩		
社会人学び直し：長期（１年程度）コース向け		
種別		カリキュラム
想定する受講者		情報セキュリティの学び直しをしたい現役IT技術者（30代中～後半）
受講者の知識・スキル		産業界で情報系業務に従事している技術者を想定する
育成する人材像		習得した情報セキュリティに関する実践的知識・経験を自らの業務に活かせる人材
到達目標	コア部分	産業界で技術者として活躍する際に知っておくべき情報セキュリティの考え方について、脅威の特徴や対策に用いられる要素技術に関する専門的内容を座学と演習の組み合わせを通じて体系的に理解する。
	コア以外を含むカリキュラム全体	コア部分の知識の種類を拡張した形で、より幅広い脅威や対策技術について体系的に理解する。
関連科目との関係		以下の領域について基本的な知識を有することを前提とする（募集要項等で明示） ・コンピュータネットワーク（TCP/IP、無線LAN） ・コンピュータアーキテクチャ ・オペレーティングシステム（Windows及びUNIX系） ・プログラミング言語（C言語、アセンブラ）
実施方法		講義及び演習

（２）科目構成例

表 63　科目構成例（仮）

学年	講義	演習等
理論系	暗号理論、暗号・認証と社会制度、アルゴリズム基礎、数論基礎、計算代数、統計的方法論	
技術系	暗号プロトコル、インターネットテクノロジ、不正アクセス技法、ネットワークシステム設計・運用管理、セキュアシステム構成論、情報デバイス技術、情報システム構成論、オペレーティングシステム、セキュアプログラミングとセキュアOS、ソフトウェア構成論、ペネトレーション技法、統計的リスク管理、個人識別とプライバシー保護	プログラミング実習、 セキュアシステム実習、 ネットワークセキュリティ技術演習、 Webアプリケーションと脆弱性対策演習、 デジタルフォレンジック演習
マネジメント系	情報セキュリティマネジメントシステム、セキュリティシステム監査、セキュリティ管理と経営、リスクマネジメント、組織行動と情報セキュリティ、セキュア法制と情報倫理、法学基礎、知的財産制度、国際標	インシデント対応とCSIRT基礎演習、 組織経営とセキュリティマネジメント演習、 事業継続マネジメント演習

	準とガイドライン、セキュリティの法律実務、リスクの経済学、マスメディアとリスク管理	
その他	情報セキュリティ特別講義	情報セキュリティ輪講

（３）適用条件

受講者のニーズや大学側のポテンシャルに応じて、期間やカリキュラム内容を削減する可能性について考慮することが望ましい。

（４）産業界で用いられる指標等との対応

本カリキュラムで受講可能な科目と産業界で用いられるスキル分類との対応関係を次表に示す。

表 64　産業界で用いられる指標との対応（例示⑩）

記号凡例： ◎=演習を伴う実践的専門教育 〇=座学中心の専門教育 ◇=基礎的/入門的教育 ★=状況に応じてケースバイケース ※=習得済が受講の前提 緑色は[産]*及び[情]*で求めているスキル 水色縦線は[産]*のみで求めているスキル			iコンピテンショナリディクショナリのスキル分類												
			メソドロジ					テクノロジ							関連知識
			戦略	企画	実装	利活用	支援活動	システム	開発	保守・運用	非機能要件	組込み・計測・制御	共通技術		
SecBoK2016 知識項目	基礎	工学基礎									※	※	※		
		ICT 基礎		※	※			※	※	※	※	※	※		
		ビジネス基礎	※		※	※	※								※
	セキュリティ専門分野	セキュリティ基礎									※				
		セキュリティガバナンス					★								
		セキュリティマネジメント	★			★	★				★				
		ネットワークセキュリティ						★			★				
		システムセキュリティ		★				★	★		★				
		セキュアシステム設計・構築		★	★			★	★		★				
		セキュリティ運用			★	★	★	★		★	★				
		暗号・認証・電子署名									★				
		サイバー攻撃手法									★				
		デジタルフォレンジック									★				
		法・制度・標準				★	★				★				★

＊［産］産業横断サイバーセキュリティ人材育成検討会「人材定義リファレンスに基づくスキルマッピング」が求めるスキル
［情］情報処理安全確保支援士試験シラバスにおける要求される知識に対応するスキル

（５）実施上の工夫点

社会人にとっては受講負荷が大きいため、修士課程と同レベルの内容を課す場合であっても負荷軽減について配慮することが望ましい。また、講義内容等を理解する上で必要となる基盤技術に関する知識は受講者において偏りがあるのが一般的であるので、以下のような工夫を行うこと

が求められる。

- 予め受講者を対象にアンケートを実施し、下記の各技術に関する経験や理解度などを尋ねる：
  －コンピュータの構造、オペレーティングシステムの機能、ソフトウェアの動作原理
  －TCP/IP に基づく通信原理、ルータ、スイッチ等の役割、無線 LAN の仕組み
  －プログラミング言語、アセンブラ言語による開発経験
- 講義を実施する際の受講者との会話を通じて内容を調整する（少人数での実施の場合）

４．モデル・コア・カリキュラムの活用方法に関する提言

本章では、前章に示したモデル・コア・カリキュラムを高等教育機関において活用するための方法について例示するとともに、今後の情報セキュリティ教育のあり方についての提言を行う。

４．１ モデル・コア・カリキュラム活用の効果

高等教育機関における情報セキュリティ教育において、モデル・コア・カリキュラムを活用することで、次の効果が得られるものと期待される。なお、以下では大学での応用を例として示すが、高等専門学校等においても同様の活用が可能である。

（１）大学におけるカリキュラム検討負荷の軽減

学科・専攻において情報セキュリティ教育に関連するカリキュラムを策定する際、モデル・コア・カリキュラムを参考とすることで、大学において教育内容に盛り込むべき内容の抽出や絞り込みを行う負荷を大幅に軽減させることができる。

（２）情報セキュリティ教育に関する大学間での単位互換制度の導入などの容易化

モデル・コア・カリキュラムに準拠した科目を設定することで、他大学からどのような内容を行っているかの把握が容易となる。これをもとに、複数の大学間で単位互換制度を実施している場合、モデル・コア・カリキュラムに準拠した情報セキュリティに関する科目をその対象にすることで、情報セキュリティ関連科目の実施が困難な大学においても情報セキュリティ教育の導入が可能となるなどの効果が期待できる。

（３）モデル・コア・カリキュラムによる学内教員の育成促進

２．１．２に示したように、調査時点において高等教育機関で実施されている情報セキュリティ教育は、必ずしも産業界が期待する内容になっていない。これは、一部の教員が情報セキュリティという分野を暗号等を主体とした数学の派生的な応用領域ととらえていることに原因がある。そこで、モデル・コア・カリキュラムを提示し、教育すべき内容を具体的に示すことで、教員を対象とした FD（Faculty Development）の効果が期待できるものと考えられる。

（４）モデル・コア・カリキュラムを産業界と共有することによる産業界講師の活用促進

（３）に示した効果のほか、学外の産業界講師の活用においても効果が期待できる。モデル・コア・カリキュラムが公表されていることで、産業界で活躍する技術者は、予め大学で教育すべき内容について検討したり、教材の準備をしたりすることが可能となる。この結果、大学からの講師依頼に企業が対応できるケースが増加し、産業界講師の活用が促進される効果が期待できる。

（５）産業界の期待に近い形での情報セキュリティ教育を行うことによる就職活動への効果

産業界からのニーズを反映したモデル・コア・カリキュラムに基づく情報セキュリティ教育を行っていることを大学がアピールすることで、企業等はその大学の卒業生が業務を遂行する上で必要となる情報セキュリティ分野の知識を有する人材であると判断することができ、就職活動等にプラスに作用することが期待される。

４．２ モデル・コア・カリキュラムの活用イメージ

第３章に示した 10 種類のモデル・コア・カリキュラムをもとに、実際に大学等でこれらを活用するイメージを示す。

４．２．１ 活用例１：全学向け情報セキュリティ教育の導入

情報セキュリティ分野のリテラシー教育に相当するものであり、情報系ないし理工学系に限らず導入する価値のあるものである。学士課程新入生を対象とした 1 年次での実施を前提としており、実施に当たっては、受講者の前提知識なしで理解可能なように工夫する必要がある。

カリキュラムの構成については、３．３．１に示したものをそのまま適用することで実施可能である。

４．２．２ 活用例２：情報系学科における情報セキュリティ関連科目の見直し

第２章に示したように、現在の情報系学科において、多くの大学が何らかの形で情報セキュリティに関する教育を行っている。しかしながら、こうした内容は産業界が求める内容に一致するとは限らず、モデル・コア・カリキュラムにおいて例示する内容に照らした見直しを行うことは有効である。３．３．２に示す例示②は、情報系学科に限らずに広く理工系学生等を対象としているが、表 37 の専門科目の講義例は、情報系学科における情報セキュリティ関連科目の見直しに役立つと期待する。また、例示②は「成長分野を支える情報技術人材の育成拠点の形成（セキュリティ分野）」の第 2 期である enPiT Security2 / Basic SecCap（学部生を主対象）プログラムに準拠しているため、同プログラムに参加することで実現することができる。

４．２．３ 活用例３：情報系修士課程における情報セキュリティ系科目の追加

情報系の修士課程 1 年次は学士課程 3 年次と比較して、カリキュラム編成上でやや余裕があると見込まれることから、新規の選択科目を追加することも可能と考えられる。そこで、以下のいずれかの方法で情報セキュリティ分野を指向しない情報系の修士課程在籍者に、情報セキュリティに関する基本的な知識を学ぶ機会を提供する。

① 案１：講義科目１科目を追加

モデル・コア・カリキュラムの例示⑤をベースに構成する。可能であれば講義を 13 回程度に圧縮し、2 回程度産業界で活躍する方が実際に取り組んでいる情報セキュリティ対策等についての講演を入れることで、受講者への刺激を高めることも考えられる。当該シラバスの構成案を次表に示す。

表 65　シラバス構成案

科目名	情報セキュリティ対策特論		
対象年次	修士課程1年次	開講時期	後期
概要	現在、情報系のあらゆる業務において情報セキュリティ対策を避けて通ることはできず、進化する脅威に日々対応する必要にも迫られている。一方で、情報セキュリティにおける脅威と対策に関する基本的な考え方を理解しておけば、新たな脅威への対策を考えたり、対策漏れを検討したりすることが容易になり、情報系業務を担う上での利点は大きい。本科目はこうした背景を踏まえ、社会で直面する情報セキュリティ上の主要な脅威とその対策のための技術や仕組みについて、情報系の技術者として理解しておくべき内容を説明するものである。さらに、実際に産業界で情報セキュリティ対策に取り組んでいる方をお招きし、対策を怠った場合の影響の大きさや理解しておくべきポイントについての講演を行う。		
到達目標	開発系、運用系等の情報系業務を担う上で把握しておくべき情報セキュリティに関する脅威と対策の基本的な考え方と、対策が機能する技術的背景について理解する。		
他科目との関係	必須科目は定めないが、以下について予め理解しておくことが望ましい。 ・コンピュータの構成（CPU、メモリ等）とオペレーティングシステムの役割 ・アプリケーションソフトウェアの動作原理 ・TCP/IP に基づくネットワーク通信の基本的動作		
方法	講義		

回数	講義内容	解説
1	情報セキュリティの基礎	情報セキュリティの基本的な概要を学び、現在社会が直面する情報セキュリティ課題と企業活動におけるセキュリティの重要性を理解するために実社会におけるサイバー攻撃の脅威と要因、およびサイバー攻撃対策に必要な考え方について学ぶ。サイバー攻撃への対策では、技術的・物理的な対策から人的・組織的対策まで総合的に取り組むことの重要性を学ぶ。
2	情報セキュリティマネジメントのフレームワーク（1）	情報セキュリティマネジメントにおける事故事例から情報セキュリティマネジメントの重要性とそのフレームワーク（PDCA サイクル）について学ぶ。
3	情報セキュリティマネジメントのフレームワーク（2）	情報セキュリティに関連する国際標準とガイドラインの概要とソフトローの役割について学ぶ。また、情報セキュリティに関連する認証制度の概要として ISMS 適合性評価制度の概要について学ぶ。
4	特別講演（1）	ソフトウェア開発現場における情報セキュリティ対策についての産業界講師による講演

5	情報セキュリティを支える暗号技術の基礎と応用	暗号技術の基礎として、共通鍵暗号、ハッシュ関数、公開鍵暗号とその応用である電子署名と PKI について学ぶ。
6	情報セキュリティのリスクマネジメントとリスクコントロール（1）	情報セキュリティマネジメントにおけるリスクマネジメント手法の概要を学びリスクの分析方法、リスクの評価方法について事例をベースに学ぶ。
7	情報セキュリティのリスクマネジメントとリスクコントロール（2）	リスクコントロールの具体例として物理的な対策（耐震対策、入退管理、バックアップ拠点等）、人的・組織的な対策（教育訓練、機密保持契約、誓約書、管理体制等）、そして技術的な対策（セキュリティ機器の設計、導入、運用等）について学ぶ。
8	特別講演（2）	情報システムの運用現場における情報セキュリティ対策についての産業界講師による講演
9	ネットワークを守る認証技術とシステム技術	なりすましや不正なネットワーク接続を防御するための要素技術を学ぶ。「なりすまし」を防ぐために用いられる認証技術、不正なアクセスからネットワークを守る認証技術、アクセス制御技術と対応するアプライアンス機器の概要を学ぶ。また、広く利用が普及している無線 LAN とスマートフォンのセキュリティ対策についても学ぶ。
10	情報セキュリティの関わる法律の基礎知識（1）	最新のセキュリティ関連の法律について焦点を当てサイバーセキュリティ基本法、不正アクセス禁止法などセキュリティに関係する主要な法律の内容について学ぶ。
11	情報セキュリティの関わる法律の基礎知識（2）	個人情報保護法やプロバイダ責任制限法などネットワークの上での権利・利益を保護し、それが侵害されたときの対応に関係する法律の概要を学ぶ。また情報セキュリティに関係して理解しておくことが望ましい法律についても学ぶ。
12	企業の情報ネットワークシステムのセキュリティ	企業の情報ネットワークのセキュリティ課題と対応する防御技術としてネットワークの仮想化、侵入検知技術、セキュリティ管理業務と支援システムについて学ぶ。
13	ソフトウェアのセキュリティ課題と対策	ソフトウェアに潜む脆弱性について学ぶ。マルウェアの侵入の手口となるバッファオーバーフローを例に攻撃の仕組みや OS やシステム・ソフトウェアによる対策技術の概要について学ぶ。
14	Web データベース及びクラウドシステムのセキュリティ	事例をベースに Web アプリケーションに潜む脆弱性、攻撃の仕組みと被害、有効なセキュリティ対策について学ぶ。また、企業情報システムを例にデータベース、Web、電子メール、クラウドに関わる脅威と被害、および必要なセキュリティ対策について総合的に学ぶ。
15	CSIRT とインシデント対応	企業組織における CSIRT の役割とサイバーセキュリティに関わる国際的な取り組みとして国際的な連携活動や情報共有の取り組みについて学ぶ。

② 案２：講義と集中演習を追加

モデル・コア・カリキュラムの事例⑥をベースに、座学による講義１科目と夏期休暇期間中の演習を導入する。事例⑥は「成長分野を支える情報技術人材の育成拠点の形成（セキュリティ分野）」（enPiT Security / SecCap）プログラムに準拠しているため、同プログラムに参加す

ることで実現することができる。

４．２．４ 活用例４：非情報系の修士課程における情報セキュリティ教育の強化

４．２．３では情報系の修士課程学生を対象に情報セキュリティ教育を実施する場合について説明した。一方、現代社会において情報セキュリティに関する知見は情報系に限らず、他分野を専攻する学生にとっても有用であることから、こうした他専攻向けの選択科目として提供することも考えられる。この場合、４．２．３と比較して情報系の基盤的な知識が不十分な場合が多いと見込まれることから、それを補うような科目構成とする必要がある。当該シラバスの構成案を次表に示す。

表 66　シラバス構成案

科目名	情報システムセキュリティ特論		
対象年次	修士課程1年次	開講時期	後期
概要	現在、あらゆる産業において情報システムやネットワークが活用されており、同時にその情報セキュリティ対策も欠かせなくなっている。情報セキュリティは、対象となる脅威に応じて適切な対策を講じなければ意味をなさず、企業や社会に大きな損害をもたらす恐れがあり、情報セキュリティ対策に関する基本的な考え方を理解しておくことの効果はきわめて大きい。本科目はこうした背景を踏まえ、社会で直面する情報セキュリティ上の主要な脅威とその対策のための技術や仕組みについて、産業界で担う役割に応じて理解しておくべき内容を説明するものである。		
到達目標	産業界で情報システムやネットワークを利活用・管理する際に把握しておくべき情報セキュリティに関する脅威と対策の基本的な考え方と、対策が機能する技術的背景について理解する。		
他科目との関係	必須科目は定めないが、以下について予め理解しておくことが望ましい。 ・コンピュータの仕組みに関する基本的な理解（ハードウェア、OS、アプリケーションなど） ・インターネットや学内 LAN に関する基本的な理解		
方法	講義		

回数	講義内容	解説
1	情報セキュリティの基礎	情報セキュリティの基本的な概要を学び、現在社会が直面する情報セキュリティ課題と企業活動におけるセキュリティの重要性を理解するために実社会におけるサイバー攻撃の脅威と要因、およびサイバー攻撃対策に必要な考え方について学ぶ。サイバー攻撃への対策では、技術的・物理的な対策から人的・組織的対策まで総合的に取り組むことの重要性を学ぶ。
2	コンピュータの仕組み	情報セキュリティに関する学習に際し理解しておくべきコンピュータアーキテクチャ、オペレーティングシステムの役割、アプリケーションソフトウェアの動作の仕組み等について学ぶ。

3	インターネットや LAN の仕組み	情報セキュリティを学ぶ上で理解しておくべきネットワーク上の知識として、TCP/IP に基づく通信の原理、ルータやスイッチなどネットワーク機器の役割、無線 LAN 等について学ぶ。
4	情報セキュリティマネジメントのフレームワーク（1）	情報セキュリティマネジメントにおける事故事例から情報セキュリティマネジメントの重要性とそのフレームワーク（PDCA サイクル）について学ぶ。
5	情報セキュリティマネジメントのフレームワーク（2）	情報セキュリティに関連する国際標準とガイドラインの概要とソフトローの役割について学ぶ。また、情報セキュリティに関連する認証制度の概要として ISMS 適合性評価制度の概要について学ぶ。
6	情報セキュリティを支える暗号技術の基礎と応用	暗号技術の基礎として、共通鍵暗号、ハッシュ関数、公開鍵暗号とその応用である電子署名と PKI について学ぶ。
7	情報セキュリティのリスクマネジメントとリスクコントロール（1）	情報セキュリティマネジメントにおけるリスクマネジメント手法の概要を学びリスクの分析方法、リスクの評価方法について事例をベースに学ぶ。
8	情報セキュリティのリスクマネジメントとリスクコントロール（2）	リスクコントロールの具体例として物理的な対策（耐震対策、入退管理、バックアップ拠点等）、人的・組織的な対策（教育訓練、機密保持契約、誓約書、管理体制等）、そして技術的な対策（セキュリティ機器の設計、導入、運用等）について学ぶ。
9	ネットワークを守る認証技術とシステム技術	なりすましや不正なネットワーク接続を防御するための要素技術を学ぶ。「なりすまし」を防ぐために用いられる認証技術、不正なアクセスからネットワークを守る認証技術、アクセス制御技術と対応するアプライアンス機器の概要を学ぶ。また、広く利用が普及している無線 LAN とスマートフォンのセキュリティ対策についても学ぶ。
10	情報セキュリティの関わる法律の基礎知識（1）	最新のセキュリティ関連の法律について焦点を当てサイバーセキュリティ基本法、不正アクセス禁止法などセキュリティに関係する主要な法律の内容について学ぶ。
11	情報セキュリティの関わる法律の基礎知識（2）	個人情報保護法やプロバイダ責任制限法などネットワークの上での権利・利益を保護し、それが侵害されたときの対応に関係する法律の概要を学ぶ。また情報セキュリティに関係して理解しておくことが望ましい法律についても学ぶ。
12	企業の情報ネットワークシステムのセキュリティ	企業の情報ネットワークのセキュリティ課題と対応する防御技術としてネットワークの仮想化、侵入検知技術、セキュリティ管理業務と支援システムについて学ぶ。
13	ソフトウェアのセキュリティ課題と対策	ソフトウェアに潜む脆弱性について学ぶ。マルウェアの侵入の手口となるバッファオーバーフローを例に攻撃の仕組みや OS やシステム・ソフトウェアによる対策技術の概要について学ぶ。
14	Web データベース及びクラウドシステムのセキュリティ	事例をベースに Web アプリケーションに潜む脆弱性、攻撃の仕組みと被害、有効なセキュリティ対策について学ぶ。また、企業情報システムを例にデータベース、Web、電子メール、クラウドに関わる脅威と被害、および必要なセキュリティ対策について総合的に学ぶ。
15	CSIRT とインシデント対応	企業組織における CSIRT の役割とサイバーセキュリティに関わる国際的な取り組みとして国際的な連携活動や情報共有の取り組みについて学ぶ。

４．２．５ 活用例５：社会人学び直しコースの設置

これまで社会人向け講座等を実施していない大学等で行う場合、まず短期のものから開始することが適切である。モデル・コア・カリキュラムでは２週間のプログラムを例示しているが、内容によってはさらに短期の集中講義とすることも可能である。受講者の参加形態に応じて、次の２種類の実施方法が想定される。

① 夜間と土曜日のみで開催

座学を中心とする講座に適するが、土曜日を活用することで演習の実施も可能である。参加者は通常の業務に支障のない形で参加することができるが、反面集中開催が困難なため、概ね１ヶ月以上の設定で実施することになる。

夜間と土曜日で開催する場合、夜間課程をもたない大学等においては通常のカリキュラムとの調整は容易であるが、夜間や土曜日の教員の確保への配慮が必要となる。

② 平日の午前・午後にまたがる集中開催

平日１日に４コマを連続して実施するもので、時間を要する演習等を伴う講座に適する。最短２日間（8コマ）程度から設定することができる。

実施上の配慮に関しては①と逆になり、教員の確保に関しては問題が少ないが、実施場所の確保に際して他のカリキュラムとの調整が必要となる。

４．３ 今後の活用の方向性

モデル・コア・カリキュラムを活用した高等教育機関における情報セキュリティ教育について、今後の方向性に関する提言を行う。

４．３．１ 「社会で役に立つ人材の育成」という観点からの情報セキュリティ教育の意義

教育の本質は「社会で役に立つ人材の育成」にある。第１章で示した通り、情報セキュリティに関する知識やスキルを習得することが産業界で活躍するにあたってのキーファクターとなっている現在、高等教育機関が情報セキュリティ教育の役割を担うことは、社会における高等教育機関の使命を果たすことでもある。情報セキュリティ分野を正しく理解するためには、暗号の基盤となる数学的知識、コンピュータやインターネットの動作原理などの工学的知識、個人情報保護法や不正アクセス禁止法などの法律的知識、さらにサイバー攻撃に関わる国際情勢など、さまざまな学問領域にまたがる知を総合する必要があり、こうした知を擁する高等教育機関に対する社会の期待は大きい。

さらに、社会生活や産業経済において情報セキュリティ分野が関わる脅威は日々増加・深刻化しており、その対策にも間断なき取組が求められている。今回策定されたカリキュラムやシラバスについても永続的に有効なものとみなさず、社会のニーズに応じて適宜更新を図っていくことで、人材育成の効果もより高まるものと期待される。

４．３．２ 幅広い対象に向けた情報セキュリティ教育の必要性

本調査では、情報セキュリティ分野を専門とする人材向けだけでなく、学士課程、修士課程それぞれの幅広い対象に向けた複数のモデル・コア・カリキュラムを提示している。前項で示したように、情報セキュリティ分野は複数の学問領域にわたり、教育対象となる知識項目が非常に多いことが特徴的である。その一方で、学生が各々の学問に取り組む中で情報セキュリティ分野の学習に割ける時間には限界があり、産業界ほか社会における活躍の場に応じて、情報の安全な管理や相手を認証するための方法、インシデントへの対応の考え方など、ニーズにあった教育を行う必要がある。各高等教育機関においては、育成しようとする人材像ごとの情報セキュリティ教育のありかたについて十分に検討することが求められる。

また、本調査では学士課程、修士課程、社会人の学び直しの３種類に適した情報セキュリティ教育の方法を示しているが、これらの教育はそれぞれ独立したものではなく、相互の作用が期待できるものである。社会人学び直しの受講者における関心を把握し、それを学士課程や修士課程のカリキュラムに反映することで実用性を高めたり、修士課程向けの演習において学生がつまずきやすい内容を把握した上で社会人向けの短期講座を開講したりなど、教育の質を高めるための工夫を行っていくことが望ましい。

４．３．３ 国際的に通用する情報セキュリティ教育の実施

モデル・コア・カリキュラムの策定に際しては、海外における情報セキュリティ教育の実施状況やそこで用いられている知識項目等の分析結果を反映している。JNSA によって策定された SecBoK は米国で策定された知識・スキル項目に基づいているが、日本国内向けに編集するに際して我が国の業務慣行上必要となる知識やスキルの追加を行っている。このように、我が国における情報セキュリティ対策を考えるにあたっては日本におけるビジネス等の事情を反映する必要があり、そうした事情を反映した対策技術の研究開発においては国内に立地する高等教育機関ならではの活躍も期待される。その一方で、サイバー攻撃には国境がなく、今後社会全体で国際水準の対策を講じることができなければ国力の低下を招く恐れがある。高等教育機関においてはこうした状況を踏まえ、国際的に通用する情報セキュリティ教育の維持・発展のため、モデル・コア・カリキュラムを活用していくことが求められる。

４．３．４ 教科書の整備等と連動させることによる普及の促進

本調査はモデル・コア・カリキュラムをもとにカリキュラムの例示を行うことを目的としているため、提示しているカリキュラム内の科目で用いる教科書等の指定は行っていないが、モデル・コア・カリキュラムの内容に連動した教科書を作成することにより、高等教育機関における実践もより容易になるものと見込まれる。ただし、情報セキュリティの分野は脅威及び対策技術のいずれも変化が激しく、情報系の他の領域（コンピュータアーキテクチャ、プログラミング言語、データベースシステム等）と比較すると高頻度で教科書の更新が必要になる。移動体通信の領域などは同様に変化が激しいため、こうした領域における教科書の更新頻度等を参考に、教育内容の見直しについて検討することが考えられる。

５．おわりに

これまで、大学における情報セキュリティの専門教育は、大学での教育基盤がしっかりとしている暗号理論とその応用技術に関するものが主体であった。一方、産業界では、他国と比較しても普及が進んだ情報セキュリティマネジメント（ISMS）の認証取得に向けた PDCA サイクルによる組織改善活動と、そのための社会人教育に重心があったと言える。これに対し、実社会ではサイバーセキュリティに係る脅威が増大し、企業の IT システムや社会インフラに対するサイバー攻撃を検知・防御する技術を開発・運用するセキュリティ技術者や、インシデント時に即応する CSIRT メンバーとなるセキュリティ専門人材等への実社会ニーズが高まってきた。結果として、我が国は、大学教育と実社会ニーズ間のギャップ、および、企業組織活動（社会人教育やキャリアパス）と実社会ニーズ間のギャップという、二つの人材育成ギャップの課題に直面していると言える。もちろん、大学および企業の一部は先駆的に、実社会ニーズに即応できるセキュリティ専門人材の育成を進めており、本調査報告では、それらの取組みをモデル・コア・カリキュラムとして取りまとめた。特に、大学や大学院等の高等教育機関における教育は、その所属学生のみならず、既に企業などで実務に携わっている社会人の学び直し教育にも貢献できるはずである。

本調査で取り上げている先駆的なカリキュラムでは、

- 実社会でのセキュリティ課題を事例とした教育
- コンピュータやネットワーク等のシステム技術と結びついた教育
- IT 技術のみならず、セキュリティを取り巻く法制度、組織マネジメントなどの社会科学系の科目を含めた総合科学としての教育
- 多様なハンズオン主体の演習
- 大学内だけでなく、産業界の専門家の協力を得た講義や演習

などが充実しつつあることは高く評価でき、今後も引き続いて充実と拡大を進めるべきである。一方、今後のセキュリティ専門人材教育において強化すべきは、本格的な IoT 時代に向けたセキュリティ教育である。脆弱性を持たない完璧なシステムを作ることは現実的ではないが、これは設計時や開発時においてセキュリティを疎かにして良いことを意味しない。部品レベルから社会システムに至るまで、設計時・開発時におけるセキュリティ対策（所謂　Security-by-Design）の強化が必要である。特に、自動車の自動走行やロボットの実用化が進む IoT 社会においては、これまで製品開発で重視されてきた安全設計（Safety Design）とセキュリティ設計の両立が重要となる。これは情報セキュリティ専門人材育成に向けた次ステップのモデル・コア・カリキュラムに向けた課題と言えよう。

文部科学省
平成28年度理工系プロフェッショナル教育推進委託事業
工学分野における理工系人材育成の在り方に関する調査研究
（情報セキュリティ人材育成に関する調査研究）
成果報告書

平成29年　3月

学校法人岩崎学園
情報セキュリティ大学院大学

〒221-0835 横浜市神奈川区鶴屋町 2-14-1
TEL: 045-311-7784　https://www.iisec.ac.jp