情報セキュリティ教育課程開発のための 国内外の大学比較分析による技術能力分析

孫 英敬† 山口 由紀子†† 嶋田 創†† 高倉 弘喜‡

†名古屋大学 大学院情報科学研究科
464-8601 愛知県名古屋市千種区不老町
qlemf00@net.itc.nagoya-u.ac.jp

††名古屋大学 情報基盤センター
464-8601 愛知県名古屋市千種区不老町
{yamaguchi,shimada}@itc.nagoya-u.ac.jp

‡国立情報学研究所
101-8430 東京都千代田区一ツ橋 2-1-2
takakura@nii.ac.jp

あらまし 情報セキュリティへの脅威はますます増加しており，国家・社会的に高度な技術を備えた人材を求める声が増大している．それに伴い，日本は国家戦略として，今後，高等教育機関における情報セキュリティ教育課程を拡充していく方針を示している．情報セキュリティ教育課程は，実際の現場から要求される技術能力を満たす，現実に即した人材を育成するものでなければならない．そこで本研究では，NICE(The National Initiative for Cybersecurity Education)が定義した情報セキュリティ技術能力を要求要件と捉え，国内外の大学における情報セキュリティ教育課程を分析することによって，技術能力に注目した教育課程開発のための方向性を考察する．

Technical Competency Analysis on Domestic and Foreign Universities for Information Security Curriculum Development

YoungKyung Son† Yukiko Yamaguchi†† Hajime Shimada†† Hiroki Takakura‡

†Graduate School of Information Science, Nagoya University
Furo-Cho, Chikusa-ku, Nagoya, 464-8601, JAPAN
qlemf00@net.itc.nagoya-u.ac.jp
††Information Technology Center, Nagoya University
Furo-Cho, Chikusa-ku, Nagoya, 464-8601, JAPAN
{yamaguchi,shimada}@itc.nagoya-u.ac.jp
‡National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, JAPAN
Takakura@nii.ac.jp

Abstract Threats to information security are increasing rapidly. However, professionals who fight against them are lacking from the viewpoint of both quantity and quality. To solve this problem, the government of Japan announced the new policy to expand a curriculum of information security at higher education institutions. The curriculum needs to be practical and provide technical competencies required on actual field. In this study, we investigate the direction for curriculum development by adopting the information security competency defined by NICE(The National Initiative for Cybersecurity Education) and analyzing the curriculum among domestic and foreign universities.

1　はじめに

情報セキュリティへの脅威はますます増加しており，国家・社会的に高度な技術を備えた人材を求める声が増大している．これに対応するため，各国において様々な教育課程が施行される中，日本では情報セキュリティ人材の質的向上と量的拡大を目指し，国家戦略として，今後，高等教育機関における情報セキュリティ教育課程を拡充していく方針が示されている[1].

しかし，情報セキュリティ教育課程モデルが提示されていないため，学科の開設時に多くの困難が予想される．情報セキュリティ分野は数学的思考やコンピュータ知識等から法律や制度等のセキュリティマネジメントまで全てを網羅する必要がある．また，国家レベルの安全保障問題を解決する学問として実際の現場から要求される技術能力を満たす，現実に即した人材を育成するものであることが必須となる．

そこで本研究では，技術能力に注目した教育課程開発モデルに基づき，NICE(The National Initiative for Cybersecurity Education)が定義した情報セキュリティ技術者に必要とされる知識，スキル，能力等の技術能力[2]を要求要件と捉え，国内外の大学における情報セキュリティカリキュラムを分類し，相関性分析を行うことによって，技術能力の満足度を調べ，効率的な情報セキュリティ教育課程開発のための方向性を模索する．

2　技術能力に注目した教育課程

技術能力に対する研究は 1990 年代から本格的に行われ，様々な定義があるが，OECD は DeSeCo プロジェクト（1997~2003）[1]を通じて，「特定の脈絡の複雑な課題要求を成功的に満たす能力」と定義し，社会構成員の成功的な人生と社会発展に要求される核心技術能力（Key competencies）を提示した[3]．つまり，技術能力に注目した教育課程(Competency based curriculum)とは，社会発展だけでなく，個人の成功的な人生のため，社会から求められる知識やスキル，能力等に基づいて行う教育であると定義できる．情報セキュリティ教育は実践的かつ具体的な実務を反映したものでなければならないため，本教育課程の採用が最も効果的である．技術能力は “generic/core skill”, “general attributes”, “generic/key competence” 等と多様に使われているが，本稿では広い意味で “技術能力(Competency)”と称する．

教育課程の開発モデルとして最も一般的に使われるのは「ADDIE モデル」で，分析(Analysis)，設計(Design)，開発(Development)，運営（Implementation），評価（Evaluation）の 5 段階となっており，各段階の頭文字を取って名付けられた．技術能力に注目した教育課程の開発プロセスは，この「ADDIE モデル」に基づいて図 1 のように行われる[4].

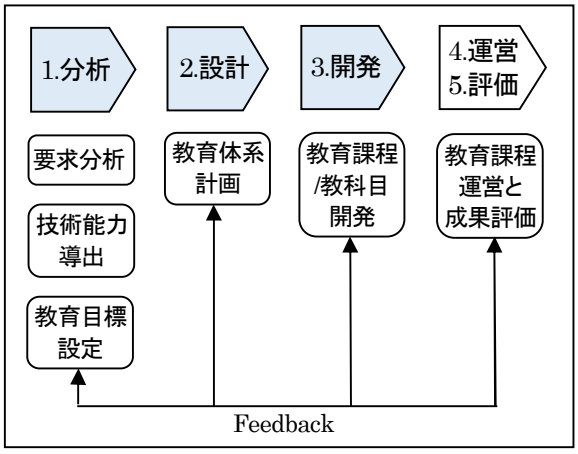

図 1. 教育課程開発プロセス[4]

分析とは，国家や社会，専門家及び学習者からの要求を分析することによって，必要な技術能力を導出し，教育目標を設定する段階である．設計では，導出した技術能力に応じて科目を分類し，科目別の授業タイプやレベル等を定義する．第 3 段階の開発では，学科で教える全ての科目を学年及び学期により体系化し，最終の教育課程モデルを提示する．運営と評価は開発した教育課程を実際に実施したのちに行うものであるため，本研究の対象外とする．

[1] 急変する現代社会に適切に対応できるように教育目標を再確立するために OECD が行った研究

3　要求分析

3.1　NICE の技術能力の採用

高度な人材を養成するためには，社会からの要求を正確に把握し，必要な技術能力を満たせるようにするのが最も重要である．本研究では，教育課程開発プロセスの第 1 段階である要求分析として，NICE(National Initiative for Cybersecurity Education)から提示された技術能力を適用する．NICE は情報セキュリティ教育を担当する米国の国家機関として，サイバーセキュリティの基盤を構築するために 20 以上の米連邦省庁と機関，及び多数の公共機関と民間組織と共同で National Cybersecurity Workforce Framework を開発した．これは，情報セキュリティ職務分野を 7 個のカテゴリと 31 個の細部項目に分け，各細部項目に必要とされる技術能力（Knowledge, Skills, Ability）を定義している[2]．その一部を表 1 に示す．

表 1. NICE のサイバーセキュリティ技術能力

カテゴリ(7 個)	細部項目(31 個)	技術能力 (62 種, 783 個)
情報セキュリティ製品，及びシステム開発	ソフトウェア開発，情報セキュリティエンジニアリング	脆弱性評価
		コンピュータ言語
		⋮
	⋮	⋮
監督と開発	戦略計画と政策開発	脆弱性評価
		刑法
	⋮	⋮
⋮	⋮	⋮

3.2　NICE 技術能力の順位付け

次に，大学のカリキュラムを分類し NICE 技術能力との相関性を分析するため，各細部項目に求められる技術能力 783 項目を 62 種類に分類しなおした．この 62 種類の技術能力の重要度を抽出するため，細部項目での出現回数により順位づけを行った．この結果の一部を表 2 に示す．例えば，3 位となった脆弱性評価という技術能力は 783 項目うちの 49 項目に出現している．重複する回数が多ければ多いほど，一番多く要求される重要な技術能力と見なし，このような方法で全ての技術能力に対する順位付けと，後の節で引用できるように参照番号付けを行った．その結果の一部を表 2 に示す．1 位は「情報システム/ネットワークセキュリティ」，2 位はネットワーク基礎知識である「インフラ設計」，次は「情報保証/セキュリティマネジメント」と「脆弱性評価」，「コンピュータネットワークディペンデンス」等の順に位置づけられた．なお，同一順位の技術能力があったため，順位は 1 位から 25 位となった．

表 2. NICE 技術能力の順位付け

番号	技術能力	順位
1	情報システム/ネットワークセキュリティ	1
2	インフラ設計(ネットワーク基礎)	2
3	情報保証/セキュリティマネジメント	3
4	脆弱性評価	
5	コンピュータネットワークディペンデンス	4
6	オペレーティングシステム	5
7	刑法/制度/倫理	6
8	コンピュータ/ディジタルフォレンジックス	7
9	最新の技術動向	
10	ソフトウェアテストと評価	8
11	システムライフサイクル	
12	システムテストと評価	
13	コンピュータ言語	9
14	アイデンティティマネジメント	
15	リスクマネジメント	10
16	インシデントマネジメント	11
17	論理システム設計	12
18	ネットワーク管理	
19	テレコミュニケーションズ	
20	暗号学/暗号アルゴリズム	13
21	データ管理	
22	契約/調達	14
23	セキュリティ(PII, PCI, 電子商取引/支払いシステム)	
24	要求分析(ISO/IEC 国際ガイドラインと標準規格)	15
25	システムインテグレーション	
26	コンピュータとエレクトロニクス	16
27	情報技術性能評価	
28	コンフィギュレーション管理	17
29	情報技術アーキテクチャ	
30	ソフトウェアエンジニアリング	
31	データベースマネジメントシステム	18
32	数学/数学的思考	
33	ソフトウェア開発	
34	知識マネジメント	19
35	エンクリプション(著作権保護システム/技術)	20
36	エンタープライズアーキテクチャ	
37	モデリングとシミュレーション	
38	組織意識	
39	フォーレンジック	21
40	ハードウェア	

41	エンベデッドコンピュータ	22
42	ヒューマンファクター(ヒューマンインタフェース，バイオ)	
43	情報システムセキュリティサーティフィケーション	
44	Reasoning(情報処理，科学的方法の使用)	
45	Teaching Others	
46	ウェブ技術	
47	データベースアドミニストレーション	23
48	ハードウェアエンジニアリング	
49	政府と法学	
50	PIA(個人情報影響評価)	24
51	コンピュータ活用スキル	
52	外部意識	
53	オブジェクトテクノロジー	
54	プロジェクト管理	
55	容量マネジメント	25
56	インターナルコントロール(CMMI)	
57	マルチメディア技術	
58	オーラルコミュニケーション	
59	政治常識	
60	公共安全とセキュリティ	
61	品質保証	
62	サーベイランス	

4 各国の教育課程設計分析

図1の第3段階である設計は，導出した技術能力により教科目を体系化する過程である．そのため，現在行われている大学における情報セキュリティ教育課程が NICE 技術能力，すなわち，社会からの要求をどれ程満たしているか，技術能力別にどういう科目を教えているかを調べることによって，今後の教育課程開発の方向性を導くことができる．

そこで本節では，情報セキュリティ人材育成のための日本と韓国における取り組みや大学現況を調べ，表2の技術能力により各大学の情報セキュリティ教科目を分類し，科目数を数え技術能力の順位を付ける．順位付けを行ったのち，Spearman の順位相関係数を用いて NICE 技術能力順位との相関性を導出し各国の設計を比較分析する．Spearman の順位相関係数は，順位データから求められる変数間の相関程度を表す指標であり，相関関係数 r_s は −1と1の間の値を持つ．±1に近いほど相関性が高く，0 に近いほど低くなる(変数の順位が完全に反対であれば −1)．変数間の相関性の程度を判断する基準は次の通りである．

表 3. 相関性判断基準

相関係数	相関性程度	相関係数	相関性程度
±0.9 以上	とても高い	±0.2~0.4 未満	低い
±0.7~0.9 未満	高い	±0.2 未満	ほぼなし
±0.4~0.7 未満	多少高い		

4.1 日本の取り組み

4.1.1 人材育成の現況

2014 年 IPA の調査[5][6]によると，日本の情報セキュリティ担当者は 26.5 万人である．しかし，そのうち必要なスキルを満たしていると考えられる人材は 10.5 万人にとどまり，残りの 16 万人に対しては何らかの教育やトレーニングが必要だと報告されている．また，8 万人が不足しているとされているが，高等教育機関を通じて供給可能な人数は，年間およそ一千人だけであり，その中においても専門コースを修了する人は 130 人に過ぎない．つまり，高等教育機関で行われている情報セキュリティ教育は，社会からの要求を質的にも量的にも満たしていない状況である．

大学における情報セキュリティ専門教育機関としては情報セキュリティ大学院大学が唯一であり，一般大学の場合は，独自の大学院課程(情報科学研究科等)に文部科学省の人材育成プログラム(ISS スクェア，ITKeys，enPiTーセキュリティ等)を加えて人材を養成している．人材育成プログラムは大学間や産学の連帯を通じて社会から求められる高度な人材の育成を目標にしており，各プログラムに参加している大学は次の通りである．

- ISSスクェア：情報セキュリティ大学院大学，中央大学，東京大学
- ITKeys：奈良先端科学技術大学院大学，京都大学，大阪大学，北陸先端科学技術大学院大学
- enPiT：奈良先端科学技術大学院大学，東北大学，情報セキュリティ大学院大学，慶應義塾大学，北陸先端科学技術大学院大学

さらに，学部課程としては初めて長崎県立大学が来年から情報セキュリティ学科を開設する予定で，カリキュラムを公開している．

4.1.2 教科目分類と技術能力分析

ここでは前述した情報セキュリティ大学院大学，長崎県立大学，人材育成プログラム，そして人材育成プログラムに参加している大学の学部と大学院課程の情報セキュリティ教科目に対し 62 種の技術能力への対応付けを行い，科目数が多い順にそれぞれの技術能力順位を付けた．その結果の一部を表 4 に示す．

表 4. 技術能力による教科目分類結果

NICE 技術能力	情報大	長崎県立大	ITKeys	…
情報システム/ネットワークセキュリティ	1	3	2	…
インフラ設計	5	3	1	…
情報保証/セキュリティマネジメント	2	4	-	…
⋮	⋮	⋮	⋮	…

順位付けを行ったのち，Spearman の順位相関係数を使って NICE 技術能力との相関性を導出した．分析を行った結果，表 5 に示すように，情報セキュリティ大学院大学の順位相関係数は 0.543 として NICE 技術能力と多少高い相関性があることが分かった．人材育成プログラムにとっても相関係数が各 0.432，0.486，0.433 で多少高い相関性があった．したがって，情報セキュリティ大学院大学と人材育成プログラムは，実際の現場からの要求をある程度満たしていると考えられる．長崎県立大学の場合は 0.163 として NICE 技術能力との相関性がほぼなかったが，学部課程はコンピュータ言語や数学等の基礎科目も重視するためにそれらの比率が高い反面，NICE 技術能力は活用スキルに重点を置いてカリキュラムに組み込まれているため，相関性が低くなってしまったと考える．

次に，一般大学における情報セキュリティ教育コースの適合性を測ってみるために，各人材育成プログラムに参加している大学から一つを選択して大学自体の学部課程と大学院課程に加え人材育成プログラムを運営した場合(ISS スクェア+東京大学，ITKeys+大阪大学，enPiT+東北大学)を想定し，NICE との相関関係を分析した．その結果，変数間の比較可能なデータ数である N(度数)は，人材育成プログラ

表 5. 大学のカリキュラムと NICE 技術能力との相関係数

		NICE	情報セキュリティ大	長崎県立大	ISS スクェア	ITKeys	enPiT	ISS +東京大	ITKeys +大阪大	enPiT +東北大
NICE	相関係数	1.000	.543	.163	.432	.486	.433	.326	.110	.318
	N(度数)	62	19	27	23	14	12	34	32	32
情報大	相関係数	−	1.000	.171	.789	.224	.492	.712	.432	.296
	N(度数)	−	19	13	19	8	6	19	14	12
長崎県立大	相関係数	−	−	1.000	.328	.526	−.026	.562	.533	.481
	N(度数)	−	−	27	13	10	9	19	17	19
ISS スクェア	相関係数	−	−	−	1.000	.335	.626	.775	.469	.372
	N(度数)	−	−	−	23	9	6	23	17	14
ITKeys	相関係数	−	−	−	−	1.000	.546	.328	.651	.240
	N(度数)	−	−	−	−	14	7	12	14	12
enPiT	相関係数	−	−	−	−	−	1.000	.693	.029	.662
	N(度数)	−	−	−	−	−	12	8	7	12
ISS +東京大	相関係数	−	−	−	−	−	−	1.000	.590	.731
	N(度数)	−	−	−	−	−	−	34	25	25
ITKeys +大阪大	相関係数	−	−	−	−	−	−	−	1.000	.504
	N(度数)	−	−	−	−	−	−	−	32	23
enPiT +東北大	相関係数	−	−	−	−	−	−	−	−	1.000
	N(度数)	−	−	−	−	−	−	−	−	32

ムのみによる 12~23 個から 32~34 個まで増加し，より多様な技術能力を満たすことが分かった．各大学の教育課程は情報科学や電子情報学を専攻としているため，電子情報/信号処理，数学/統計，ハードウェア工学等が上位となり，多様なエンジニアを養成していた．しかし，NICE 技術能力のどこにも該当していない科目を除外したにもかかわらず，いずれも人材育成プログラムのカリキュラムのみによる相関よりも相関係数が低くなり，情報セキュリティ人材を育成するためのカリキュラムにとっては，適していないことが明らかになった．

また，人材育成プログラムは大学院生を対象にした追加カリキュラムのため，負担を感じる院生から敬遠される事例もあり，輩出できる人材の数も少ない．さらに，分析結果のように，現在の情報科学や電子情報学課程は時間と労力に比べ情報セキュリティ人材を育成するのには限界がある．したがって，人材の質的・量的拡大のためには情報セキュリティ学部課程の開設が急務であり，人材育成プログラムを生かした上に情報セキュリティ分野の特徴や社会からの要求をもっと反映したカリキュラムの開発が必要とされる．

4.2 韓国の取り組み

4.2.1 人材育成の現況

情報セキュリティ産業実態調査(韓国知識情報保安産業協会，2014.12)によると，情報セキュリティ関連産業に従事している人材は，およそ 10 万人であり，そのうち情報セキュリティ業務を担当している人材は，3 万 6 千人とされている．しかし，再教育が必要な初心者レベルの人材が 1 万 4 千人で全体の 40.7%を占めており，中級以上の人材は 2 万 2 千人と把握されている．韓国は 2013 年，発源地が北朝鮮と推定される，放送/金融圏および国家の主要機関を対象にした 2 度の大規模なサイバー攻撃(3.20，6.25)を受け，「国家サイバー安保総合対策（2013.7）」を発表し，2017 年まで 5 年間最精鋭の情報セキュリティ専門家(K-Shield)5 千人養成を目標に取り組んでいる．

韓国の高等教育機関における情報セキュリティ教育課程は，1990 年代から設置され始め，2000 年代に入って本格化された．2014 年基準，4 年制大学に 36，大学院に 32，短大に 8，全部で 76 個学科が設置されており，在籍生数と年間輩出人数は表 6 の通りである[7]．

表 6. 韓国情報セキュリティ大学現況

	4 年制大学	大学院	2 年制短大	合計
学科数	36	32	8	76
在籍生数	5,701	1,241	568	7,510
年間卒業生数（2014 年）	435	281	110	826

それ以外に，KISA（韓国インターネット振興院）では，潜在力のある人材を発掘するため，2006 年から全国の大学の情報セキュリティ課外活動を支援し，地域別セミナーやワークショップ，実習教育，研究支援等を行っている．現在，41 個大学における 45 課外活動，約 1，500 人を支援している[7]．

4.2.2 教科目分類と技術能力分析

調査対象は表 6 の 4 年制大学と大学院であるが，大学の場合はサイバー警察学科(5)やサイバー国防学科(4)等の特殊な学科は除外し，カリキュラムを公開している 22 大学を調査した．特に，高麗大学のサイバー国防学科は，上位 1%のエリートサイバーセキュリティ専門将校を養成するために国防部が共同で作った採用条件型契約課程として，細部カリキュラムは機密にしている．

22 大学のカリキュラムを前と同じ方法で分類し大学それぞれの順位付を行ったものと技術能力別すべての大学の科目を総合して付けた順位を NICE 技術能力と比較した結果の一部を表 7 に示す．全体科目の相関係数は 0.476 として NICE と多少高い相関性があり，22 大学の中で一番相関性の高かったのは京東大学で，相関係数は 0.763 であった．

大学院は，32 ヶ所のうち，19 ヶ所を調査した．大学院の場合，情報セキュリティ専門大学院(高麗大，延世大等 4 ヶ所)，一般大学院の情報セキュリティ学科(京畿大，成均館大等 13 ヶ所)，

表 7. 韓国情報セキュリティ大学(院)の相関係数

		NICE	大学全体	建陽大	京東大	…	NICE	大学院全体	KAIST	祥明大	
NICE	相関係数	1.000	.476	.263	.763	…	1.000	.523	.546	.914	…
	N	62	53	23	17	…	62	44	11	10	…
大学全体	相関係数	-	1.000	.128	.747	…	-	1.000	.481	.804	…
	N	-	53	23	17	…	-	44	11	10	…
建陽大	相関係数	-	-	1.000	-.066	…	-	-	1.000	.447	…
	N	-	-	23	11	…	-	-	11	5	…
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

学際間協同課程(全南大, 慶北大等 5 ヶ所)等の形態で運営されており, 企業と連帯した採用条件型契約学科も開設されていた. これらの相関性分析の結果は, 表 7 のように, 全体科目は 0.523 として大学全体の 0.476 より高く, 祥明大学情報セキュリティマネジメント学科は 0.914 で, 最も高い相関性があった. この学科の教育目標は,「技術的対策だけでなく, セキュリティマネジメント, 政策等の専門知識を備えた融合型人材, 経験を通した現場密着型専門家を育成する」となっており, 工学理論や数学等の理論的科目を最小化し, 応用やマネジメント科目を中心に編成されていた.

4.3 国家別教科目の技術能力分析

前の結果を基に日本と韓国における情報セキュリティ教育の傾向について考察する. 大学で行われるすべての情報セキュリティ教科目を総合し, NICE 技術能力と比較した. 日本の場合, 一般大学を除いて情報セキュリティ大学院大学と長崎県立大学, そして人材育成プログラムのみを対象とし, 韓国は 22 大学と 19 大学院の教科目を全部合わせて結果を求めた(表 8). NICE 技術能力 62 種のうち, 日本は 40 種, 韓国は 55 種を満たしており, 相関係数は各 0.554 と 0.463 として両国とも多少高い相関性があった.

両国ともに教育されている科目について, 差異を調査した. 62 種の技術能力に対する両国の教科目の密度を図 2 のグラフで示す. 表 2 に載せたように, 技術能力は順位の高い順に 1 から 62 番まで番号付けしており, 両国とも 32 番より上位の NICE 技術能力を中心にカリキュラムが編成されていることがわかった.

表 8. 国家別技術能力相関係数

		NICE	日本	韓国
NICE	相関係数	1.000	.554	.463
	N	62	40	55
日本	相関係数	.554	1.000	.418
	N	40	40	40
韓国	相関係数	.463	.418	1.000
	N	55	40	55

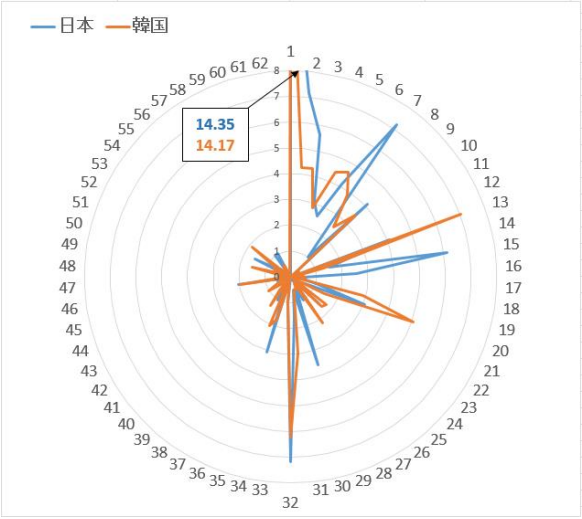

図 2. NICE 技術能力に対する科目密度

両国いずれかで行われている教科目のうち, 教科目密度が 2%以上異なる技術能力を図 3 に示す. コンピュータ言語分野を除いては, 全体的に日本の方の密度が高く, 特にリスクマネジメントやインシデントマネジメント, 情報テクノロ

ジアーキテクチャ等の密度が高かった．韓国は学部の割合が高いためコンピュータ言語等の基礎知識科目が多くなるが，それでもセキュアコーディングを含め，Web/Visual/Socket/.NET/GUI/プログラミング等多様に構成されていた．

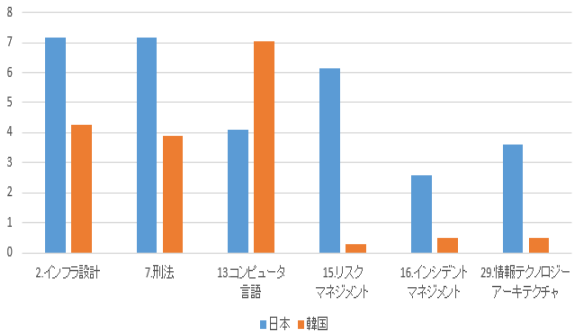

図 3. 両国間差のある技術能力

また，韓国でのみ行われている技術能力は電子商取引や電子支払いシステムに関するセキュリティ，知識マネジメント等 15 種であった．なお，前者のセキュリティについては，調査した 41 大学(大学院)のうち，24 ヶ所で行われており，科目密度は 1.7%であった．

両国いずれでも行われていない技術能力はソフトウェアテストと評価，ハードウェア，Teaching Others(学習者のレベルを測定し適合した教育を行えるスキル)，公共安全とセキュリティ 等 7 種であるが，これらは，あまりにも細分化したり逆に範囲が広すぎたりして一つの科目に編成することが困難な技術能力であった．1 学部課程で満たせる技術能力(表 5，表 7 での N)は最大 28 種で，62 種の技術能力を全部満たすのは現実的に不可能であることを考慮し，教育課程開発の時は類似した技術能力を併合し数を減らすのもよい方法である．

5 おわりに

本研究は国内大学における情報セキュリティカリキュラムを調べ，Spearman の順位相関係数を用いて NICE 技術能力との相関性分析を行った．その結果，幅広い知識や基礎知識科目を中心に編成された学部課程よりセキュリティ専門プログラムや大学院課程の方が技術能力との相関性が高いことが明らかになり，両国間科目編成の差も確認することができた．しかし，セキュリティも分かる組み込みエンジニアのような人材も必要になってくるので，そういう観点からの尺度が必要となる．

今回は要求要件として米国の NICE 技術能力を採用したが，国内の環境にもっと適合した「情報セキュリティ強化対応スキル指標」に基づいた調査も必要である．

今後は米国や英国の情報セキュリティ学部教育課程を調べ，データマイニング手法を用い，必修/選択科目・単位・学期編成等を抽出することによって情報セキュリティ教育課程組成補助モデルを開発する予定である．

参考文献

[1] NISC, “「新・情報セキュリティ人材育成プログラム」の推進”, http://www.nisc.go.jp/active/kihon/pdf/jinzai2014.pdf

[2] NICE, “The National Cybersecurity Workforce Framework”, http://csrc.nist.gov/nice/framework/

[3] OECD(2003), Definition and selection of competencies: Theoretical and conceptual foundations(DeSeCo), http://www.oecd.org/education/skills-beyond-school/definitionandselectionofcompetenciesdeseco.htm

[5] 韓国建陽大学国策事業教育課程開発評価チーム,“Competency Based Curriculum 開発マニュアル”

[5] IPA, “情報セキュリティ人材不足数等に関する追加分析について”, http://www.ipa.go.jp/files/000040646.pdf.

[6] IPA, “情報セキュリティ人材の育成に関する基礎調査_調査報告書”, http://www.ipa.go.jp/files/000014184.pdf.

[7] KISA, “国家情報セキュリティ白書 2015”