情報処理学会論文誌 Vol.58 No.5 1163–1174 (May 2017)

技術能力に注目した情報セキュリティ教育課程開発のためのカリキュラム分析

孫 英敬[1] 山口 由紀子[2,a)] 嶋田 創[2,b)] 高倉 弘喜[3,c)]

受付日 2016年8月31日, 採録日 2017年2月9日

概要：情報セキュリティへの脅威はますます増加しており，高度な技術を備えた人材を求める声が増大している．それにともない，日本では高等教育機関における情報セキュリティ教育課程を今後拡充していく方針が示されているが，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．そこで我々は，アメリカ国立標準技術研究所の下に設置されている 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情報セキュリティ人材の要求要件ととらえて情報セキュリティ教育過程の開発を目指した研究を行っている．本研究では，NICE において 783 項目に表されている技術能力を 62 種類に分類・集約した．さらに，日本および，セキュリティ教育が進んでいる韓国の大学についてカリキュラムを調査し，NICE 技術能力との相関分析によりカリキュラム分析を行った．

キーワード：セキュリティ，人材育成，技術能力，高等教育，カリキュラム

A Curriculum Analysis for Information Security Curriculum Development Focusing on Technical Competencies

YoungKyung Son[1] Yukiko Yamaguchi[2,a)] Hajime Shimada[2,b)] Hiroki Takakura[3,c)]

Received: August 31, 2016, Accepted: February 9, 2017

Abstract: Threats to information security are increasing rapidly and requests of the human resources who acquire high technology are also increasing. Japanese government announced the new policy to solve this problem by expanding a curriculum of information security at higher education institutions. The curriculum should be practical and provide technical competencies required on actual field. This study aimed at the development of a curriculum by adopting the information security competencies defined by NICE (The National Initiative for Cybersecurity Education) which is a under organization of the American National Institute of Standards and Technology. In this paper, we classified 783 NICE technical competencies into 62 items. Moreover, we investigated the curriculum among Japanese and Korean universities and analyzed them by a correlation analysis with NICE technical competencies.

Keywords: security, human resources development, technical competencies, higher education, curriculum

[1] 名古屋大学情報科学研究科（当時）
Graduate School of Information Science, Nagoya University, Nagoya, Aichi 464–8603, Japan
[2] 名古屋大学情報基盤センター
Information Technology Center, Nagoya University, Nagoya, Aichi 464–8601, Japan
[3] 国立情報学研究所
National Institute of Informatics, Chiyoda, Tokyo 101–8430, Japan
a) yamaguchi@itc.nagoya-u.ac.jp
b) shimada@itc.nagoya-u.ac.jp
c) takakura@nii.ac.jp

1. はじめに

サイバー空間は，個人の日常生活だけではなく，企業の経済活動および役所の行政サービス等，様々な活動の中心となっている．また，クラウドコンピューティングやビックデータ，IoT（Internet of Things）等の新たな情報通信技術の発展によりサイバー空間はますます拡大しており，それに対する人々の依存度も高まっている．これにより，

セキュリティ脅威の発生原因が増加し，保護する資産の識別が困難になり，セキュリティ技術の適用が困難な小型スマート機器が増加する等，情報セキュリティ対策の難しさを増大させる要因となっている．特に社会基盤施設をはじめ，スマートホーム，スマートカー等のあらゆる機器がインターネットに接続される IoT 技術は，既存の情報漏えいや金銭奪取等とはレベルが異なる人の生命まで脅かす致命的で大規模な被害を招く恐れがある．さらに，サイバー攻撃の手口も徐々に巧妙化しているため，防ぐことが非常に困難になっている．

このような状況のもと，高度な技術を備えた情報セキュリティ人材を求める声が増大しているが，情報セキュリティ人材は質も量もまったく足りない状況である．現在日本における情報セキュリティ担当者は 26.5 万人であるが，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であると報告されている [1], [2]．一方，高等教育機関を通じて供給可能な人数は年間およそ 1,000 人であるため，需要と供給のギャップが広がっている．

そこで我々は，現実に即した人材の育成を実現するため，大学における情報セキュリティ学部課程のカリキュラム開発を目指した研究を行っている．本研究では，教育設計（インストラクションデザイン）の原理に基づき，要求分析，設計，開発の 3 段階でカリキュラム開発を行うことを想定し，要求分析および，設計のための既存のカリキュラム分析を行った．要求分析では，アメリカ国立標準技術研究所（National Institute of Standards and Technology, NIST）の下に設置されている NICE（The National Initiative for Cybersecurity Education）が定義した情報セキュリティ技術能力 [3] を要求要件ととらえ，情報セキュリティ人材に必要とされる技術能力の分類を行い，重要度の割当てを行った．また，現在日本と韓国の大学，大学院で行われている情報セキュリティ教育カリキュラムの調査を行った．さらに，要求分析で得られた NICE 技術能力との相関分析による評価手法を提案し，分析を行った．

2. 情報セキュリティ人材の現況と育成

2.1 日本の取り組み

2000 年代に入って全世界的に情報セキュリティ人材に対する需要が増え，人材育成の必要性が認識されはじめた．佐々木らは，セキュリティ教育の対象を職場や役割によって 3 種に大別し，対象別に要求される教育内容をまとめた [4]．また，日本のセキュリティ教育が米国や韓国に比べ遅れていることを指摘し，学部課程の設立と人材育成の重要性を強調した [5]．しかし，それにもかかわらず，2014 年の IPA の調査 [1], [2] によると，現在情報セキュリティ担当者は 26.5 万人で，8 万人不足していることが指摘されている．

表 1 日本における高等教育機関の年間人材供給力
Table 1 The annual number of human resources supplied by higher education institutions in Japan.

人材の分類	推定供給人数
情報セキュリティに関する研究を習得	1,000 人
うち 専門教育コースを修了	130 人

このように人材の需要と供給のギャップが広がっている最も大きな原因は，佐々木らが文献 [4], [5] で指摘していたとおり，高等教育機関の数が少ないことがあげられる．**表 1** に示すように高等教育機関を通じて供給可能な人数は年間およそ 1,000 人にすぎない [1]．その中でも，大学院，大学，高専，専門学校において情報セキュリティに関して専門的で体系的な教育を受けた専門コースを修了する者は 130 人にすぎず，多くは大学院，大学の研究室での論文作成等において，情報セキュリティに関する研究を行った者である．そのため，教育課程においては関連授業がほとんど開講されていないため，情報セキュリティに関する幅広い専門知識を身に付けることが難しい状況である．

現在日本の大学における情報セキュリティ専門教育機関としては，大学院では情報セキュリティ大学院大学，学部では 2016 年度から開設された長崎県立大学情報セキュリティ学科が唯一である．そのほかに，一般大学において，情報学研究科等の大学院修士課程に文部科学省の人材育成プログラム（ISS Square，IT Keys，enPiT-Security）を加えて人材を養成している．

ISS Square は，大学間や産学の連携を通じて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するためのプログラムとして，大学と企業，研究機関 11 社が参加している．育成する人材像は「高度な情報セキュリティ実践リーダー」，「高度情報セキュリティ研究・開発者」を目指しており，所属研究科の履修単位とは別に 20 単位を追加に履修するように定めている[*1]．

IT Keys は，情報セキュリティ分野における世界最高水準の人材育成拠点の形成を目的とし，関西圏を中心とした 4 大学院および 4 企業・団体が参加している．このコースは公的機関や企業等において情報セキュリティ対策実施の責任者となる最高情報セキュリティ責任者，および実際に対策を立案し，その実行を指示する情報セキュリティ担当者の育成を目標にしている．修了要件は 12 単位であり，講義等の教育課程に企業と団体も積極的に参加している[*2]．

enPiT は，最先端の情報技術を実践的に活用できる人材育成のためのプログラムとして，クラウドコンピューティング，セキュリティ，組み込みシステム，ビジネスアプリケーションの 4 つの分野に分けており，そのうち

[*1] http://iss.iisec.ac.jp/
[*2] http://it-keys.naist.jp/

表 2 韓国における情報セキュリティ学科数
Table 2 The number of information security departments in Korea.

	大学	大学院	短大	合計
学科数	36	32	8	76
在籍生数	5,701	1,241	568	7,510
2014 年度卒業生数	435	281	110	826

enPiT-Security は 5 つの参加大学が協力して開講する「産業界が求める実践セキュリティ人材の育成」コースである．修了認定単位は 10 単位としている[*3]．

これらの人材育成プログラムに参加している大学は次のとおりである．

ISS Square 情報セキュリティ大学院大学，中央大学，東京大学

IT Keys 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-Security 奈良先端科学技術大学院大学，東北大学，慶應義塾大学，情報セキュリティ大学院大学，北陸先端科学技術大学院大学

2.2 韓国の取り組み

韓国では 1998 年から情報セキュリティ専門教育課程が設置されはじめ，2003 年には 7 大学と 15 大学院で情報セキュリティ教育が本格的に行われた．2010 年代に入ってからは，長期的な教育計画の樹立や教育課程の検証，一般人向けの教育拡大等に対する研究が始まった [6], [7]．しかし，依然として，社会から要求される技術能力の詳細が明確に把握されていないため，大学の教育課程と実際の現場との間でどういう分野でどのくらいの差があるのか認識することが困難な状況にある．

韓国は 2013 年，発源地が北朝鮮と推定される，放送/金融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 月 20 日，6 月 25 日）を受けたことをきっかけに，「国家サイバー安保総合対策（2013.7）」を発表し，2017 年までの 5 年間で最精鋭の情報セキュリティ専門家 5,000 人養成を目標に取り組んでいる [8]．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，2014 年時点において，4 年制大学に 36 学科，大学院に 32 専攻，短大に 8 学科の合計 76 が設置されており，在籍数と 2014 年の卒業生数は**表 2** のとおりである [8]．

しかしながら，韓国情報保護振興院（Korea Internet & Security Agency, KISA）が発表した「情報セキュリティ人材需給実態調査及び分析展望結果報告書（2014.12）」[9] によると，韓国の情報セキュリティ人材数は 94,224 人であり，そのうち，再教育が必要な初心者レベルの人材は 27,274 人で全体の 27.5%を占めていると推定されている．

[*3] http://www.enpit.jp/

表 3 韓国における情報セキュリティ人材数と不足数
Table 3 The numbers of the information securities human resources and the human resources lacking.

	2014 年	2015 年	2016 年	2017 年
供給	3,646	3,392	4,106	4,368
不足	13,020	15,945	19,094	22,449

また，この報告書によると，現在韓国の情報セキュリティ人材はおよそ 13,000 人が不足しており，正規教育機関（大学・大学院）および公共/民間教育機関を通じた供給人数を毎年増やしていっても需要の増加率には及ばず，2017 年になると，不足人数は 22,449 人に達すると予測されている（**表 3**）．

2.3 米国での取り組み

サイバーセキュリティ先進国であるアメリカ合衆国（以下，米国）における情報セキュリティ人材育成は，主に教育機関に対する認定プログラム制度および学生に対する奨学金制度により進められている．特に，全米科学財団（National Science Foundation）による Cybercrops® [*4]は，National Security Agency による Center of Academic Excellence in Information Assurance Education/Cyber Defense（CAEIA/CD）[*5]で認定された教育機関等で学ぶ学生に対する奨学金制度であり，現在 62 の大学等の教育機関で運用されている．この制度では，奨学金を受けた学生に対して，卒業後に政府機関（連邦，州，地元）での勤務を義務付けており，政府機関における情報セキュリティ人材を確保している．

さらに米国では，教育機関での教育とは別に，認定資格の取得が重要なアイテムとなっている．なかでも ISC（International Information Systems Security Certification Consortium）による CISSP（Certified Information Systems Security Professional）[*6]の信頼度が高く，情報セキュリテイ関連の求人では，CISSP の資格保有が条件となっている場合が多い．

このような状況においても，2015 年の状況で 20 万 9 千人の情報セキュリティ人材が不足しており[*7]，情報セキュリティ人材育成ためのさらなるアクションプランが示されている[*8]．

[*4] https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504991
[*5] https://www.nsa.gov/resources/educators/centers-academic-excellence/
[*6] https://www.isc2.org/cissp/default.aspx
[*7] https://www.commerce.gov/news/secretary-speeches/2014/12/remarks-commerce-secretary-penny-pritzker-training-americas
[*8] https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

2.4 日本における問題点と対策

企業において情報セキュリティを担う人材の育成についての主な悩みとしては「スキルアップが難しい」,「専門性の高い人材の育成方法が分からない」,「専門性が高いが,スキルの幅が広がらない」等があげられている．以下に企業のセキュリティ担当者に対するヒアリング結果をあげる [2], [10].

- セキュリティ担当者については，セキュリティを専攻していた人材をターゲットとした採用募集を行ってほしい．
- セキュリティに特化した業務でなくても，すべての者に情報セキュリティに関する基礎的なリテラシが必要．大学において教養科目として学習しておいてほしい．
- セキュリティ担当者として育成するためには教育コストがかかりすぎる．
- セキュリティ分野は人手が急激に必要となっており，大学において基礎的な知識を幅広く修得した人材が求められている．

これらの結果から，現在日本の情報セキュリティ教育は企業を中心に行われており，高等教育機関における教育課程は社会からの要求を満たしていないということが分かる．

これに対応するため，日本政府は人材の量的拡充と質的向上を目指し，国家戦略として，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 [11]．また，最近では単に情報セキュリティの現場の実務を担う人材だけでなく，その「実務者層」と組織の「経営層」との間にたって，経営方針に基づくサイバーセキュリティ対策実践，および，実務課題をふまえた経営戦略が提示できる「橋渡し人材層」の必要性が認識されつつある [12].

このように，人材の量的充足が急務な状況にあるが，社会からの要求に適切に対応した人材育成が行われなければ，人材の質需給のギャップは依然として存在する恐れがある．そこで本研究では，求められる技術を備えた現実に即した人材の育成を目標に，技術能力に注目した情報セキュリティ学部課程のカリキュラム開発のための，要求分析と既存カリキュラムの調査・分析を行った．

3. 技術能力に注目したカリキュラム設計と分析

3.1 カリキュラム開発

カリキュラム開発は，教育が目指す領域を定義し，それを実現するために必要な授業構成を設計することで実現される．しかしながら，カリキュラムを構成する領域や教育内容を表現する要素が定まっていない場合には，設計も困難な作業となる．

これに対して，情報専門教育の分野では，情報処理学会がカリキュラム標準 J07 を策定し，公開している [13]．J07

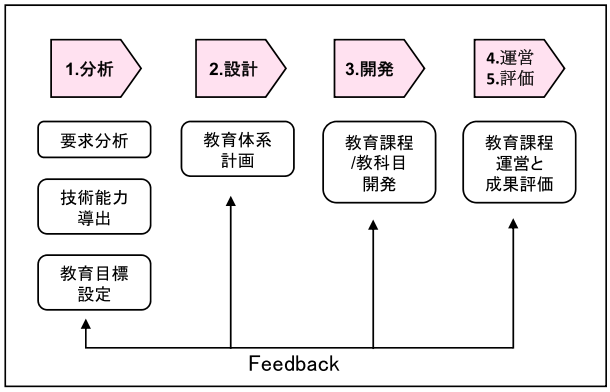

図 1 ADDIE モデルによる教育課程開発プロセス
Fig. 1 Curriculum development process by ADDIE model.

では，カリキュラムを構成する知識項目集（ISBOK）と教育目的・学習内容を記述したラーニングユニット（LU）を定義している．カリキュラムの設計では，複数の LU から構成される科目を定義し，これらを組み合わせることでコース全体の設計を行うことが可能であり，標準的なカリキュラムも提示されている．

一方で，医学・看護学等のスキルの習得が重要な要素となっている教育分野では，インストラクションデザインという概念を導入したカリキュラム開発も行われている．本研究では，現実社会に求められている技術能力を備えた人材育成のため，インストラクションモデルによるカリキュラム開発を想定し，要求分析を行うとともに，カリキュラム設計に必要な既存カリキュラムの調査・分析を行った．

本研究では，インストラクションデザインとして「ADDIE モデル」を参考した．ADDIE モデルは，分析（Analysis），設計（Design），開発（Development），運営（Implementation），評価（Evaluation）の 5 段階で構成されており，各段階の頭文字をとって名付けられている．ADDIE モデルでは，これら 5 段階のプロセスで実施される（**図 1**）．本研究では，5 段階の構成において，まず要求分析の段階として，情報セキュリティ人材に求められる要求要件の定義となる技術能力の分析を行い，さらに，設計の段階として，既存のカリキュラムの調査・分析を行った．

3.2 カリキュラム分析

設計されたカリキュラムに対する分析・評価は，実際の講義を通じて行われるものであるが，時間がかかるうえに定量的な評価が難しい．そこで，シラバス文書に対するデータ解析手法を用いた分析も行われている．

野澤らは，シラバスの文書から抽出した用語に対してクラスタリングを行うことで，カリキュラムの類似性を分析するシステムを構築し，9 大学 10 学科のカリキュラム分析を行った [14]．また，関谷らはシラバス文書に対して確率的言語モデルに基づいたカリキュラムマップを生成し，3.1 節で述べた J07 カリキュラムの 1 つである J07-CS を標

準として，いくつかの大学のカリキュラムとの比較を行った [15].

これらはカリキュラムを可視化することで現在使われている大学のカリキュラムの分析・評価を支援するものである．一方で，産業界からの要求と大学のカリキュラムとの相関関係を分析・評価することで，今後のカリキュラム改善に反映させるための研究も行われている [16]．本研究では，インストラクションデザインの分析段階で得られた情報セキュリティ人材に求められる技術能力と大学のカリキュラムとの相関関係を分析することで，現行の情報セキュリティ教育の状況について考察する．

4. 要求分析

4.1 NICE 情報セキュリティ技術能力

2.3 節で述べたように，米国においては CISSP 資格の保有が情報セキュリティ求人の条件となっており，この CISSP 資格試験で示されている技術能力が社会に求められている情報セキュリティ人材に必要な技術能力となっている．また，アメリカ国立標準技術研究所（National Institute of Standards and Technology, NIST）の下に設置されている NICE（The National Initiative for Cybersecurity Education）が開発している「National Cybersecurity Workforce Framework」（以下，NICE 技術能力）も広く使われている．日本においては，日本ネットワークセキュリティ協会（以下，JNSA）が「セキュリティ知識分野（SecBoK）人材スキルマップ」[*9] を編纂し，情報セキュリティ関連の職種別に求められる技術能力を示している．

CISSP 資格は，米国内にとどまらず今や世界的な情報セキュリティ資格となってきており，2017 年 1 月 16 日現在，163 カ国，11 万人以上が資格を取得している [*10]．資格試験で求められる技術能力は，8 カテゴリに分類して示されている．各カテゴリに対する重みも示されており，技術能力の重要度ととらえることができる．一方で，CISSP では受験資格として 5 年の実務実績が求められており，技術能力には大学教育では習得できないものも多々含まれている．

JNSA では，2003 年から情報セキュリティに関する業務に携わる人材が習得すべき技術能力を体系的に整理したスキルマップを作成しており，社会人向けの教育コースの設計に多く利用されている．2016 年版では，各職種で求められる技術能力が，NICE 技術能力に準拠して構成されている．

そこで本研究では，情報セキュリティ人材に求められる要求要件として NICE 技術能力を採用することとした．NICE 技術能力は米国の情報セキュリティ人材を育成し，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，および多数の公共機関と民間組織が共同で開発したものである．2010 年から開発が始まり，2011 年に完成した後も毎年アップデートされている．なお，本研究では 2013 年度版を参照した [*11]．NICE 技術能力では，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（知識，スキル，能力）を定義している．その一部を**表 4** に示す．

NICE 技術能力では，31 項目の細部項目のそれぞれについて対応している情報セキュリティに関する職種の例があげられている．単に情報セキュリティの実務担当者だけでなく，Chief Information Security Officer（CISO）や Chief Information Officer（CIO）等，情報セキュリティに関わる様々な階層の職種に求められる技術能力が示されており，日本が今後必要となる「橋渡し人材」の育成にも対応可能な要求要件であると考える．

4.2 情報セキュリティ技術能力の分類と順位付け

表 4 に示した NICE 技術能力では，31 項目の各細部項目において求められる技術能力の総数は 783 個となっている．本研究では，この 783 個の技術能力について，整理・分類を行い，62 種類に集約した．

本研究では，62 種類に集約した技術能力について，異なる細部項目に出現する回数が多いほど，多様な職務分野で多く要求される重要な技術能力と見なし，出現回数順に順位付けを行った．たとえば，「脆弱性評価」という技術能力は，783 個のうち 49 回出現していた．このような方法で 62 種類の技術能力に対する順位付を行い，参照番号を付けた．この結果を**表 5** および **表 6** に示す．

5. 情報セキュリティ教育課程分析

5.1 日韓の教育課程設計調査

本研究では，日韓の大学・大学院におけるセキュリティ教育のカリキュラムが NICE で求められている技術能力を備えた人材育成に対応しているのかを評価するための調査・分析を行った．なお，米国の大学のカリキュラムについては単位制をとっており，日韓の学科制と異なり教科目が特定できないため，今回の分析の対象外とした．

日本については，情報セキュリティ大学院大学と長崎県立大学，2.1 節で述べた情報セキュリティ人材育成プログラムとそれに参加している大学（情報科学科等）のカリキュラムについて調査した．

韓国では表 2 に示したように，高等教育機関に全部で 76 の情報セキュリティ教育課程が情報科学科とは別に開設されている．本研究では，このうちサイバー警察や国防学科等の特殊学科やカリキュラムを公開していない教育機関，および，教育期間が短く幅広く専門的な内容の教育が難しい短大を除いて，22 大学（**表 7**）と 19 大学院（**表 8**），あ

[*9] http://www.jnsa.org/result/2016/skillmap/
[*10] https://www.isc2.org/member-counts.aspx
[*11] http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_for_printing.pdf

表 4 NICE 技術能力の構成
Table 4 National Cyber Security Workforde Framework.

カテゴリ（7 項目）	細部項目（31 項目）	技術能力
セキュリティ製品およびシステム開発	情報認証コンプライアンス	情報システム/ネットワークセキュリティ
		リスクマネジメント
		情報認証
		⋮
	ソフトウェア認証	脆弱性評価
	セキュリティエンジニアリング	情報認証
		⋮
	⋮	⋮
運営およびメインテナンス	システム管理	情報システム/ネットワークセキュリティ
		インフラ設計
		⋮
	⋮	⋮
保護および防御	インシデント対応	情報システム/ネットワークセキュリティ
		⋮
	⋮	⋮
サイバー捜査	デジタルフォレンジック	コンピュータフォレンジック
		⋮
	⋮	⋮
監督および開発サポート	戦略計画/ポリシ開発	刑法
		⋮
	⋮	⋮
情報収集および解読	サイバーオペレーション	未公開
	⋮	

表 5 NICE 技術能力の順位付け
Table 5 Order of technical competencies by appearace counts.

No.	技術能力	出現回数
1	情報システム/ネットワークセキュリティ	63
2	インフラ設計	54
3	情報認証	49
4	脆弱性評価	49
5	コンピュータネットワークディフェンス	45
6	オペレーティングシステム	32
7	刑法	24
8	コンピュータフォレンジックス	23
9	最新技術動向	23
10	ソフトウェアテストと評価	21
11	システムライフサイクル	21
12	システムテストと評価	21
13	コンピュータ言語	19
14	アイデンティティマネジメント	19
15	リスクマネジメント	18
16	インシデントマネジメント	17
17	論理システム設計	15

わせて 41 大学のカリキュラムを調査した．

これらの大学において，技術能力が備わった人材の育成がなされているかどうかを評価するため，本研究では，各大学のカリキュラムの各教科目について 62 種類の NICE 技術能力への対応付けを行った．対応付けにおいては，各教科目にたいして 1 つの NICE 技術能力への対応付けを行った．教科目には複数の技術能力の習得を目指した科目もあるが，シラバスを参照し最も適した技術能力への対応付けを行った．

対応付けの例として**表 9** に長崎県立大のカリキュラムについて技術能力への対応付けを行った結果を示す．表 9 において，参照番号 1 の「情報システム/ネットワークセキュリティ」技術能力については，3 科目が対応していた．なお，長崎県立大では 2 年次以降のシラバスが公開されていないため，科目名による対応付けを行った．

5.2 相関分析

大学・大学院のカリキュラムでは，限られた開講時間数の中で 62 種類に及ぶ NICE 技術能力のすべてを満たすこ

表 6 NICE 技術能力の順位付け（続き）
Table 6 Oder of technical competencies by appearace counts (cont.).

No.	技術能力	出現回数
18	ネットワーク管理	15
19	テレコミュニケーションズ	15
20	暗号学/暗号アルゴリズム	14
21	データ管理	14
22	契約/調達	13
23	電子商取引データセキュリティ	13
24	要求分析（ISO/IEC 国際標準規格）	11
25	システムインテグレーション	11
26	コンピュータとエレクトロニクス	10
27	情報技術性能評価	10
28	コンフィギュレーション管理	9
29	情報技術アーキテクチャ	9
30	数学/数学的思考	8
31	ソフトウェアエンジニアリング	9
32	データベースマネジメントシステム	8
33	ソフトウェア開発	8
34	知識マネジメント	7
35	エンクリプション（著作権保護技術）	6
36	エンタープライズアーキテクチャ	6
37	モデリングとシミュレーション	6
38	組織意識	6
39	フォレンジックス	5
40	ハードウェア	5
41	エンベデッドコンピュータ	4
42	ヒューマンファクター	4
43	情報システムセキュリティ認証	4
44	推論手法	4
45	教育技能	4
46	ウェブ技術	4
47	データベースアドミニストレーション	3
48	ハードウェアエンジニアリング	3
49	政府と法学	3
50	個人情報影響評価	3
51	コンピュータ活用スキル	2
52	外部意識	2
53	オブジェクトテクノロジー	2
54	プロジェクト管理	2
55	容量管理	1
56	インターナルコントロール	1
57	マルチメディア技術	1
58	オーラルコミュニケーション	1
59	政治常識	1
60	作戦セキュリティ	1
61	品質保証	1
62	サーベイランス（ハッキング手法）	1

とは不可能である．また，NICE 技術能力には，多くのカテゴリで共通な能力もあれば専門的分野に限定される能力もある．大学教育は情報セキュリティの特定の職種の教育コースではないため，共通的な技術能力に対する比重が重い方が望ましい．

表 7 カリキュラムを調査した大学（韓国）
Table 7 The universities which investigated a curriculum (Korea).

	大学名		大学名
1	建陽大学	12	祥明大学
2	京畿大学	13	ソウル女子大学
3	京東大学	14	誠信女子大学
4	慶一大学	15	世宗大学
5	高麗サイバー大学	16	世宗サイバー大学
6	大邱カトリック大学	17	順天郷大学
7	大田大学	18	崇実サイバー大学
8	東明大学	19	又石大学
9	東新大学	20	中部大学
10	木浦大学	21	漢陽サイバー大学
11	培材大学	22	湖西大学

表 8 カリキュラムを調査した大学院（韓国）
Table 8 The graduate schools which investigated a curriculum (Korea).

	大学院名
1	KAIST 情報セキュリティ大学院
2	建國大学情報通信大学院
3	京畿大学一般大学院
4	慶北大学一般大学院
5	高麗大学情報セキュリティ大学院
6	科学技術聯合大学院大学
7	南ソウル大学
8	大田大学一般大学院
9	東國大学國際情報大学院
10	木浦大学一般大学院
11	祥明大学一般大学院
12	成均館大学情報通信大学院
13	世宗サイバー大学情報セキュリティ大学院
14	順天郷大学一般大学院
15	崇實大学情報科学大学院
16	亞洲大学情報通信大学院
17	延世大学情報大学院
18	忠北大学一般大学院
19	湖西大学一般大学院

本研究では，NICE 技術能力について，62 種類に集約するとともに，Framework 全体おける出現回数による順位付けを行った．本研究ではこの順位を人材育成における重要度ととらえ，重要度の高い技術能力に対する教科目が多く開講されているほど，NICE 技術能力に対応したカリキュラムになっていると評価することとした．

そこで，各大学のカリキュラムについて NICE 技術能力との対応付けを行い，その結果に対して相関分析による評価を行った．相関係数の導出においては，大学のカリキュラムは科目数，技術能力は出現数と評価値が異なるため，評価値そのもので相関関係を分析するのは適切ではない．

表 9 長崎県立大カリキュラムの技術能力への対応付け
Table 9 Correlating the subjects with technical competencies (Nagasaki Pref. Univ.).

技術能力	対応する教科目	科目数
情報システム ネットワーク セキュリティ	セキュリティシステム構築と運用 情報セキュリティ演習 情報セキュリティ	3
コンピュータ言語	マークアップ言語 プログラミング基礎演習 プログラミング応用演習 セキュアプログラミング技法	4
デジタル フォレンジック	コンピュータ フォレンジクス	1
数学的思考	情報数学，情報理論， 微分積分学，統計演習 オペレーションリサーチ	5
⋮	⋮	⋮

そこで本研究では双方の評価値に基づいて順位付けを行い，Spearman の順位相関係数による評価を行った．

Spearman の順位相関係数は，式 (1) により求められる．

$$r_s = 1 - \frac{6\sum d_i^2}{N^3 - N} \tag{1}$$

$$d_i^2 = \sum_{i=1}^{N} (R(x_i) - R(y_i))^2$$

ここで，N はデータ対の数（度数），$R(s_i)$，$R(y_i)$ は評価値 x_i，y_i の順位である．すなわち，順位相関係数 r_s は，各項目について順位差 d_i の 2 乗を度数で補正した値となる．

しかし，今回各大学のカリキュラムと技術能力の対応付けを行ったところ，科目数が同数になる技術能力が多数存在した．Spearman の順位相関係数は，同順位がある場合は式 (2) により求められる．

$$r_s = \frac{T_x + T_y - \sum d_i^2}{2\sqrt{T_x T_y}} \tag{2}$$

$$T_x = \frac{N^3 - N - \sum (t_i^3 - t_i)}{12}$$

$$T_y = \frac{N^3 - N - \sum (t_j^3 - t_j)}{12}$$

ここで，N は度数，t_i，t_j は各順位において同順位を構成するデータの数である．式 (2) では，個々の項目の順位差 d_i を，同順位を構成する項目数により補正して相関係数 r_s を求めている．

また，各大学のカリキュラムでは，技術能力で分類した結果が 62 種類の技術能力の一部についてしか対応していない．そこで，相関分析を行う大学のカリキュラムごとに，対応している技術能力の項目のみを抽出して相関分析を行った．

まず，カリキュラムについて 62 種類の技術能力への対応付けを行い（**図 2**），カリキュラムと対応がある技術能力のみを抽出して相関分析を行う．**図 3** にその過程を示す．

参照番号	出現回数	科目数
1	63	7
2	54	1.5
3	49	4
4	49	
5	45	2
6	32	2
7	24	4
8	23	
9	23	1
10	21	
11	21	
12	21	
13	19	2
14	19	1
15	18	4
16	17	
17	15	
18	15	0.5
19	15	
20	14	1
…	…	…

図 2 技術能力と科目の対応付け
Fig. 2 An example of correlating the subjects with technical competencies.

参照番号	出現回数	NICE順位	ti^3-ti	科目数	科目数順位	tj^3-tj
1	63	1		7	1	
3	49	3		4	3	
7	24	6		4	3	24
15	18	10		4	3	
32	8	15.5		3	5	
5	45	4		2	7	
6	32	5		2	7	24
13	19	8.5		2	7	
2	54	2		1.5	9	
9	23	7		1	14.5	
14	19	8.5	6	1	14.5	
20	14	12		1	14.5	
24	11	13		1	14.5	
29	9	14		1	14.5	
33	8	15.5	6	1	14.5	990
35	6	17		1	14.5	
40	5	18		1	14.5	
52	2	19		1	14.5	
58	1	20		1	14.5	
18	15	11		0.5	20	

図 3 相関係数算出手順
Fig. 3 Calculation procedure of the correlation coefficient.

抽出された各項目について，出現回数による順位付け（NICE 順位）と科目数による順位付けを行う．なお，本研究では同順位となる項目数が多いため，順位は平均順位を算出した．

次に，式 (2) により相関係数を求めるため，算出した各順位の値について $t_i^3 - t_i$ および $t_j^3 - t_j$ を算出する．図 3 では科目数順位に従って整列させているため項目が離れているが，NICE 順位については 8.5 位および 15.5 位がそれぞれ 2 項目ずつあった．最後に式 (2) により相関係数 r_s の算出を行う．

r_s は，-1 から 1 の値をとり，± 1 に近いほど相関性が高く，0 に近いほど低くなる．順位がまったく同じであれば 1，完全に反対であれば -1 となる．相関係数 r_s による相関関係の評価は，データ数等により変動するが，おおむね以下のとおりである [17]．

$|r_s| < 0.3$ 相関関係なし
$0.3 \leq |r_s| < 0.5$ やや相関関係あり
$0.5 \leq |r_s| < 0.7$ 強い相関関係あり

なお，本研究においては，要求要件である NICE 技術能力とカリキュラムの間に負の相関関係があっても意味がないため，0 以下の値については 0 と同等に評価することとした．また，今回の相関係数算出においては，大学によって NICE 技術能力に対応する教科目数が異なるため，度数 N も評価指標に加えた．相関係数の算出において，技術能力に対応した教科目の種類（度数）が極端に少ない場合でも，科目数による順位が NICE 技術能力の順位と合致していると相関係数が高くなってしまう．そのため，相関係数と度数による総合的な評価が必要となる．

6. カリキュラム分析

6.1 カリキュラム分析：日本

日本の大学における情報セキュリティ教育課程と NICE 技術能力間の相関係数を導出した結果を**表 10** に示す．

情報セキュリティ大学院大学の相関係数は 0.54 であり，NICE 技術能力と強い相関があることが分かった．3 つの人材育成プログラムも同様に相関係数が各 0.43，0.49，0.43 となり，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，NICE 技術能力に対応したカリキュラム編成となっていることが分かった．

しかしその一方で，度数 N が少なく，取得できる技術能力が少ないという結果になった．情報セキュリティ大学院大学および 3 つの人材育成プログラムは，2 年制や単位数が限定された追加のプログラムであるため，そもそも科目数が少ない．そのため満たす技術能力の数が少ないのは当然であり，少ない科目数の中で効率的に技術能力が習得できるカリキュラムが構成されていることが分かった．

一方，長崎県立大学情報システム学部情報セキュリティ学科は，相関係数が 0.16 となり NICE 技術能力との相関性はほぼないという結果になったが，より多くの技術能力（27 種）を満たしていた．これは，学部課程はコンピュータ言語や数学等の基礎科目の比率が高いが，NICE 技術能力は活用スキルの順位が高いため，相関性が低くなったと思われる．また，4 年制であるため科目数が多く，満たせる技術能力の数が大学院に比べて多くなったと考えられる．このように，学部教育においては，背伸びしすぎて専門的なものに偏るより，基礎を固めて大学院へつなぐような教育であることが望ましい．長崎県立大学のカリキュラムについては，今後大学院のカリキュラムと合わせた評価が必要になると考える．

次に，一般大学における情報セキュリティ教育コースの技術能力との相関を分析するために，各人材育成プログラムに参加している大学から 1 つを選択して当該大学の学部課程と大学院課程に加え，人材育成プログラムを修了した場合のカリキュラムについて NICE 技術能力との相関分析を行った．各人材育成プログラムに対して選択した大学は，ISS Square＋東京大学，ITKeys＋大阪大学，enPiT-Security＋東北大学である．その結果を**表 11** に示す．

その結果，度数は人材育成プログラムのみの場合の 12〜23 種から 32〜34 種に増加し，より多様な技術能力に対する教育がなされていることが分かった．しかし一方で，NICE 技術能力に該当しない一般教養等の科目を除外したにもかかわらず，相関係数はそれぞれ 0.33，0.11，0.32 となり，著しく低下した．これは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，情報セキュリティ関連科目が編成されておらず，順位が低い技術能力に対応した電子情報/信号処理，数学/統計，ハードウェア工学等の教科目が上位となり，相関性が低くなったと考えられる．

6.2 カリキュラム分析：韓国

韓国については，表 7 と表 8 に示した，22 大学と 19 大学院について NICE 技術能力との相関係数を算出した．その結果の一部を**表 12** と**表 13** に示す．

それぞれの大学のカリキュラムの NICE 技術能力との相関係数は，最低の 0.02（祥明大学）から最高の 0.76（京東大学）までのバラツキがあった．度数 N は，大学によって少ない場合で 15 種，多い場合で 28 種を満足していた．大学院では −0.16（南ソウル大学，本研究では 0 と評価）から 0.91（祥明大学）までバラツキがあった．

日本の場合と同様に，NICE 技術能力に対する相関性は学部課程より大学院課程の方が高かった．特に，祥明大学の場合，学部課程の相関係数は 0.02 で調査した大学のうち一番低い相関係数となったが，大学院課程においては 0.91 と相関係数が高くなり，調査した大学院のうち NICE 技術能力との相関性が最も高かった．祥明大学の学科の教育目

表 10 カリキュラムと技術能力の相関分析（日本）
Table 10 Correlative analysis of a curriculum and the technical competencies (Japan).

	情報セキュ大	長崎県立大	ISS Square	IT Keys	en PIT
相関係数	0.54	0.16	0.43	0.49	0.43
度数	19	27	23	14	12

表 11 学部・大学院課程を含めたカリキュラムの相関分析
Table 11 Correlative analysis of a curriculum including a department and a graduate school course.

	ISS Square ＋東京大	IT Keys ＋大阪大	enPiT ＋東北大
相関係数	0.33	0.11	0.32
度数	34	32	32

表 12 カリキュラムの相関分析（韓国・大学）
Table 12 Correlative analysis of a curriculum (Universities in Korea).

	京畿大	京東大	木浦大	培材大	誠信女子大	祥明大	世宗サイバー大	…
相関係数	0.54	0.76	0.35	0.28	0.59	0.02	0.60	…
度数	15	17	26	28	16	18	24	…

表 13 カリキュラムの相関分析（韓国・大学院）
Table 13 Correlative analysis of a curriculum (Graduate Schools in Korea).

	高麗大	南ソウル大	木浦大	延世大	湖西大	祥明大	世宗サイバー大	…
相関係数	0.32	−0.16	0.53	0.22	0.68	0.91	0.67	…
度数	25	13	21	17	7	10	13	…

表 14 日韓のカリキュラムの比較（一部）
Table 14 Comparison of a curriculum of Japan and Korea (part).

参照番号	技術能力	日本		韓国		密度差
		科目数	密度（%）	科目数	密度（%）	
1	情報システム/ネットワークセキュリティ	28	14.35	195	14.17	0.18
2	インフラ設計	14	7.17	59	4.27	2.9
3	情報認証	11	5.64	59	4.27	1.37
4	脆弱性評価	6	3.07	39	2.82	0.25
5	コンピュータネットワークディフェンス	5	2.56	61	4.42	1.86
6	オペレーティングシステム	8	4.1	64	4.63	0.53
7	刑法	14	7.17	53	3.87	3.3
8	コンピュータフォレンジックス	2	1.02	35	2.57	1.55
⋮	⋮	⋮	⋮	⋮	⋮	⋮
62	サーベイランス	0	0	3	0.21	0.21
	合計	195	100	1,379	100	-

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」というもので，まさに「橋渡し人材」を育成し，その先の「経営層」へのキャリアパスをも意識したカリキュラムとなっている．そのため，大学院課程では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る．

韓国の学部課程と大学院課程では，大学によって技術能力との相関にバラツキが大きかった．これは，大学ごとにある分野に特化した独自のカリキュラムを備えているためであるといえるが，一方では標準的なカリキュラムが決まっていないことによるともいえる．さらに，祥明大学のように学部課程と大学院課程が連携している場合も考慮する必要があることが分かった．

6.3 全体的評価

5.1 節の結果を利用して日本と韓国における情報セキュリティ教育全体の傾向について評価した．日本については，情報セキュリティ大学院大学，長崎県立大学，および人材育成プログラムのカリキュラム全 195 科目を対象とし，韓国については 22 大学と 19 大学院の教科目をすべて合わせた全 1,379 科目を対象とした．日韓では科目数に大きな差があるため，科目密度により比較することにした．**表 14** に結果の一部を示す．

日韓ともに NICE 技術能力において最も出現回数が多い参照番号 1 の「情報システム/ネットワークセキュリティ」技術能力の密度が最も高く，おおむね重要な技術能力の科目密度が高いことが分かった．また，全 62 種類の技術能力のうち，両国双方で教育されているものが 40 種，韓国でのみ行われているものが 16 種，両国いずれでも教育されていないものが 6 種あった．

表 14 について，技術能力の参照番号（1〜62）に対する日韓の教科目密度をグラフで表した（**図 4**）．両国とも 32 番より参照番号が上位の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分かった．表 5 に載せたように，技術能力の参照番号は出現頻度の高い順に付けていることから，両国とも技術能力を備えた人材育成のための教育が行われていることが分かった．

図 4 から参照番号 1 のほかに 13（コンピュータ言語），31（数学/数学的思考）が高い科目密度となっていることが分かる．これらの科目は，多くの大学において基礎科目として開講されいるため，密度が高くなったと考えられる．また，「システムライフサイクル」「システムテストと評価」は，技術能力としては 11 位と高い順位であるが，日韓と

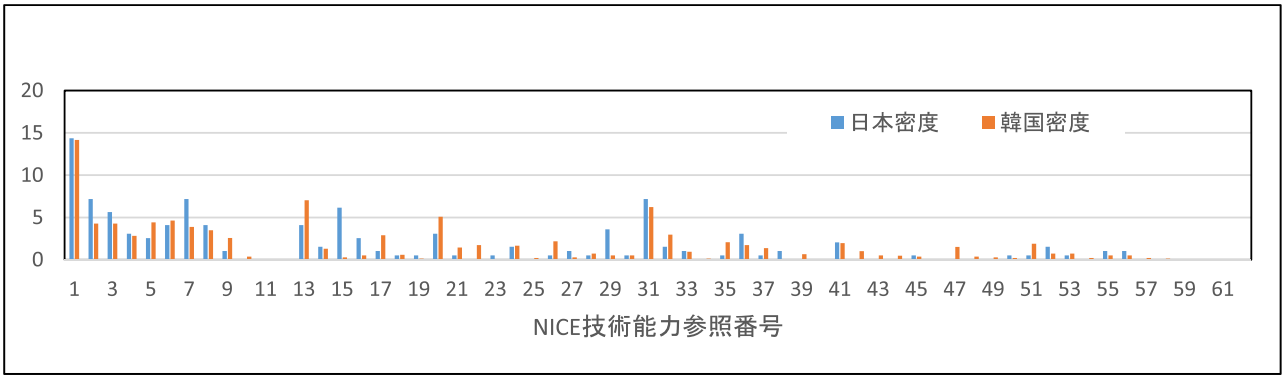

図 4 技術能力の科目密度分布
Fig. 4 Subject density distribution on the technical competencies.

もにそれに対応する科目が開講されていない．これらの技術能力が大学教育にはそぐわない分野であるためと考えられる．

7. おわりに

近年，サイバーセキュリティへの脅威がますます増加しており，これに対応できる優秀な情報セキュリティ人材を育成するため，各国において様々な取り組みが行われている．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，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．

一方，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から法律や制度，マネジメントまですべてを網羅し，実際の現場から要求される技術能力を備えた人材育成が望まれている．さらに，自動化が進みつつある対策技術[*12]を適宜取り込む等，柔軟性も要求される．

このような状況において，本研究では，現実に即した人材の育成を行うカリキュラム開発を目標として，要求分析と設計のための既存カリキュラムの調査・分析を行った．要求分析では，NICE 技術能力を社会からの要求要件ととらえて，NICE において 783 項目に表されている技術能力を 62 種類に分類・集約し，技術能力の重要度付与を行った．さらに，日本と韓国において現在行われているセキュリテイ教育課程の調査を行い，NICE 技術能力との相関分析により評価を行った．

本研究による評価手法の結果，大学院のカリキュラムは技術能力との相関があるものの，単位数が少ないため対応する技術能力数が少ないという結果となり，妥当な評価結果が得られた．また，韓国の大学の事例では，学部課程では相関が低いカリキュラムが編成されている一方で，大学院では相関が高い編成となっているものがあり，学部・大学院全体での評価が必要であることも分かった．調査した大学・大学院全体の教科目の科目密度による分析では，日韓ともに重要な技術能力に対応した科目が多く開講されており，おおむね社会の要求に応えうるカリキュラムになっていることが分かった．

[*12] Cyber Grand Challenge
https://www.cybergrandchallenge.com/

参考文献

[1] IPA（独立行政法人情報処理推進機構セキュリティセンター）：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（オンライン），入手先 ⟨http://www.ipa.go.jp/files/000040646.pdf⟩（参照 2015-11-12）．
[2] IPA（独立行政法人情報処理推進機構セキュリティセンター）：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（オンライン），入手先 ⟨http://www.ipa.go.jp/files/000014184.pdf⟩（参照 2015-11）．
[3] NICE (The National Initiative for Cybersecurity Education): The National Cybersecurity Workforce Framework (online), available from ⟨http://csrc.nist.gov/nice/framework/⟩ (accessed 2014-09).
[4] 佐々木良一，杉立 淳：情報セキュリティ教育の現状と今後，電子情報通信学会技術研究報告，技術と社会・倫理，SITE2002-33, Vol.102, No.656, pp.1–6 (2003).
[5] 佐々木良一：東京電機大学における情報セキュリティ教育，電子情報通信学会技術研究報告，技術と社会・倫理，SITE2004-14, Vol.104, No.392, pp.7–12 (2004).
[6] Kim, D.-W., Chai, S.-W. and Ryou, J.-C.: A Study on Domestic Information Security Education System, *Journal of the Korea Institute of Information Security and Cryptology*, Vol.23, No.3, pp.545–559 (2013)（韓国語）.
[7] Lim, W. and Ahn, S.: *A Study on Improvements of the Information Security Department via the Curriculum Analysis*, Vol.17, No.6, pp.71–80, Korea Association of Computer Education (2014)（韓国語）.
[8] KISA (Korea Internet & Security Agency): 2015 국가정보보호백서（2015 国家情報セキュリティ白書）（オンライン），入手先 ⟨isis.nic.or.kr/ebook/download_pdf/2015.pdf⟩（参照 2015-01）．
[9] KISA (Korea Internet & Security Agency): 2014 년 정보보호 인력수급 실태조사 및 분석전망 결과보고서（2014 年情報セキュリティ人材需給実態調査及び分析展望結果報告書）（オンライン），入手先 ⟨http://www.msip.go.kr/cms/www/open/go30/info/info_4/info_41/_icsFiles/afieldfile/2015/12/03/2014%EB%85%84%20%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%20%EC%9D%B8%EB%A0%A5%EC%88%98%EA%B8%89%20%EC%8B%A4%ED%83%9C%EC%A1%B0%EC%82%AC%20%EB%B0%8F%20%EB%B6%84%EC%84%9D%EC

%A0%84%EB%A7%9D%20%EA%B2%B0%EA%B3%BC%EB%B3%B4%EA%B3%A0%EC%84%9C.pdf〉（参照 2015-01）.
[10] IPA（独立行政法人情報処理推進機構セキュリティセンター）：IT のスキル指標を活用した情報セキュリティ人材育成ガイド—情報セキュリティ上の脅威から企業を護るために—（オンライン），入手先 〈https://www.ipa.go.jp/files/000039528.pdf〉（参照 2015-12）.
[11] NISC（内閣サイバーセキュリティセンター）：「サイバーセキュリティ人材育成総合強化方針（仮称）」に向けた検討事項について（オンライン），入手先 〈http://www.nisc.go.jp/conference/cs/jinzai/dai01/pdf/01shiryou04.pdf〉（参照 2015-12）.
[12] NISC（内閣サイバーセキュリティセンター）サイバーセキュリティ戦略本部：サイバーセキュリティ人材育成総合強化方針（オンライン），入手先 〈http://www.nisc.go.jp/active/kihon/pdf/jinzai_kyoka_hoshin.pdf〉（参照 2016-07-28）.
[13] 情報専門学科カリキュラム標準 J07，情報処理 2008 年 7 月，Vol.49, No.7, pp.719–774 (2008).
[14] 野澤孝之，井田　正，芳鐘冬樹，宮崎和光，喜多　一：シラバスの文書クラスタリングに基づくカリキュラム分析システムの構築，情報処理学会論文誌，Vol.46, No.1, pp.289–300 (2005).
[15] 関谷貴之，松田源立，山口和紀：LDA と Isomap を用いた計算機科学関連カリキュラムの分析，情報処理学会論文誌，Vol.54, No.1, pp.423–434 (2013).
[16] Kim, M.-J., Lee, H., Song, S.-J. and Yoo, J.: Analysis of the Curriculum of Departments of Information Security in Universities and Comparison with Industrial Needs in Korea, *Journal of Industrial and Intelligent Information*, Vol.2, No.3, pp.164–168 (2014).
[17] 種子田重彦：統計学，成分堂 (1985).

孫 英敬

2004 年徳成女子大学日語日文学科卒業．2015 年名古屋大学大学大学院情報科学研究科修士課程修了．同年大韓民国陸軍 3 士官学校人文社会学処第 2 外国学科講師．日本語教育に従事．

山口 由紀子　（正会員）

1983 年名古屋工業大学情報工学科卒業．1985 年名古屋大学大学院情報工学研究科修士課程修了．（株）富士通研究所．1991 年名古屋大学大型計算機センター助手．2002 年同大学情報連携基盤センター助手．2009 年同大学情報基盤センター助教．ネットワーク運用技術，セキュリティに従事．電子情報通信学会会員．

嶋田 創　（正会員）

2004 年名古屋大学博士（工学）．同年名古屋大学研究員．2005 年京都大学特任助手．2009 年奈良先端科学技術大学院大学准教授．2013 年名古屋大学准教授．計算機アーキテクチャとネットワークの研究に従事．IEEE，電子情報通信学会各会員．

高倉 弘喜　（正会員）

1990 年九州大学工学部卒業．1992 年九州大学大学院修士課程修了．1995 年京都大学大学院博士後期課程修了．米国イリノイ州立大学訪問研究員，奈良先端科学技術大学院大学助手，京都大学講師，助教授（准教授），名古屋大学教授を経て，2015 年国立情報学研究所教授．サイバーセキュリティ，高機能ネットワークの研究に従事．博士（工学）．電子情報通信学会，システム制御情報学会，地理情報システム学会，ACM 各会員．