東海大学紀要情報通信学部
Vol.16,2023,pp.1-5

論文

情報通信学部における情報セキュリティカリキュラムの分析

柿崎 淑郎[*1]，井平 和沙[*2]

Analysis of Information Security Curriculum in the School of Information and Telecommunication Engineering

by

Yoshio KAKIZAKI[*1] and Kazusa IHIRA[*2]

(received on Apr. 21, 2023 & accepted on Jul. 18, 2023)

あらまし

日本では2016年頃から情報セキュリティ人材の不足が指摘されており，官学共に様々なとり組みを行ってきた．東海大学情報通信学部は情報セキュリティ専科ではないものの，情報セキュリティを専門とする教員が複数名在籍しており，国内の大学において特徴的である．本論文では，改組前後の情報通信学部カリキュラムをセキュリティ知識分野人材スキルマップを用いて分析し，それぞれのカリキュラムの特徴を明らかにするとともに，どのような情報セキュリティ教育を行い，どのような情報セキュリティ人材育成に資するかを議論する．

Abstract

In Japan, a shortage of information security personnel has been pointed out since around 2016, and various efforts have been made by both the government and academia. The School of Information and Telecommunication Engineering of Tokai University is not a department specializing in information security, but it has several faculty members specializing in information security, which is unique among universities in Japan. In this paper, we analyze the curricula of the School of Information and Telecommunication Engineering before and after the reorganization using SecBoK2021 to identify the characteristics of each curriculum, and discuss what kind of information security education and what kind of information security human resource development they contribute to.

キーワード：情報セキュリティ，情報セキュリティカリキュラム，情報セキュリティ教育，SecBoK
Keywords: *Information Security, Information Security Curriculum, Information Security Education, SecBoK*

1. はじめに

2018年に公表された総務省の資料[1)]に依れば，2016年時点で情報セキュリティ人材が 13.2 万人不足していると推計されており，2020 年には不足数が 19.3 万人に増加すると見込まれている．また，2020年4月には，新型コロナウイルス感染症の急速な拡大によりロックダウンが発生し，テレワークやデジタル・トランスフォーメーション（DX）が急速に普及した．情報セキュリティ人材が不足していると見込まれる中で，テレワークを急拵えで実施したために，セキュリティ対策が不十分で，従来の境界型防御が機能せず，それらを狙ったサイバー攻撃の増加が問題となった．

情報セキュリティ人材を育成するために，官民連携で様々な取り組みが行われており，情報処理推進機構（IPA）のセキュリティ・キャンプ，情報通信研究機構（NICT）の SecHack365 などが行われている．また，文部科学省採択プログラムである成長分野を支える情報技術人材の育成拠点の形成（enPiT）では，大学院生向けの SecCap を 2014 年から，学部生向けの Basic SecCap を 2016 年から，社会人向けの ProSec を 2017 年から実施しており，文部科学省高度人材養成のための社会人学び直し大学院プログラムに採択された東京電機大学では，2015 年から履修証明プログラムとして国際化サイバーセキュリティ学特別コース（CySec）を実施している．他にも，長崎県立大学では 2016 年に日本で初めてセキュリティ学科を設置，九州大学では 2017 年より全学でのサイバーセキュリティ教育，近畿大学では 2022 年に新設された情報学部情報学科サイバーセキュリティコースが IPA から情報処理安全確保支援士試験の免除対象学科等の認定を受けるなど，各大学では社会のニーズに対応する取り組みが行われている．

日本の多くの理工系大学では，教育課程において情報セキュリティが扱われているものの，計算機科学やネットワークを中心としたカリキュラムの一部に過ぎず，情報セキュリティを中心としたカリキュラムで教育を行っている大学は非常に少ない．筆者らが在籍する東海大学情報通信学部通信ネットワーク工学科（JT）は，情報セキュリティを専門とする教員が複数名在籍しており，情報セキュリティを前面に標榜していない学科としては非常に珍しい存在である．

本論文では，情報セキュリティを専門とする教員が複数名在籍している東海大学情報通信学部の特徴に着目し，JT のカリキュラムで実施されている教育が，情報セキュリティ人材育成にどのように貢献しているかを，日本ネットワークセキュリティ協会（JNSA）が公表しているセキュリティ知識分野人材スキルマップ（SecBoK）[2)]を参照し，分析する．また，全学改編によって新設された情報通信学部情報通信学科（JE）についても，同様に調査を行い，情報セ

*1 情報通信学部情報通信学科 准教授
Department of Information and Telecommunication Engineering, Associate Professor
*2 情報通信学部通信ネットワーク工学科 卒業生
Department of Communication and Network Engineering, Former Student

キュリティ人材育成に資するカリキュラムであるかを分析する．これらの結果から，両学科のディプロマ・ポリシーおよびカリキュラム・ポリシーに基づいて，どのようなセキュリティ人材の育成が可能であるかを議論する．

2. 関連研究

サイバーセキュリティについてのカリキュラム標準としては，ACM/IEEE/AIS SIGSEC/IFIP の Joint Task Force による CSEC2017[3]がある．CSEC2017 はサイバーセキュリティに特化したカリキュラム標準ではあるが，実際には一般的な情報技術の知識やスキルも必要とされるため, CSEC2017 を包括しているより汎用的なカリキュラム標準として，IT2017[4]や CC2020[5]が採用されることが多い．

これらの国際的なカリキュラム標準を元に，日本の情報専門教育の状況に対応したカリキュラム標準 J17[6]を情報処理学会が策定した．J17 では，コンピュータ科学領域，情報システム領域，ソフトウェアエンジニアリング領域，コンピュータエンジニアリング領域，インフォメーションテクノロジ領域，一般情報処理教育の 6 領域に加えて，情報セキュリティ [7]が策定された．

学術研究においても，情報セキュリティ，サイバーセキュリティに関連するカリキュラム検討や実践の報告が複数ある．孫らの研究 [8]では，情報セキュリティ教育カリキュラムの調査を行い, NICE 技術能力 [9]との相関分析による評価手法を提案し，分析を行っている．分析の結果，日本の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ことが明らかになった．また，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，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た．

3. 情報セキュリティ知識項目 SecBoK

情報セキュリティ知識項目 SecBoK は日本ネットワークセキュリティ協会（JNSA）によって策定され，2003 年から定期的に改訂が行われ，最新版は 2021 年に発表された SecBoK2021[2]（以下，単に SecBoK と略す）である．SecBoK では，米国立標準技術研究所 NIST の SP 800-181（NICE Framework）を参照し，スキル構造とロールを取り入れている．また，SecBoK におけるロールの定義には，日本シーサート協会（NCA）の CSIRT（Computer Security Incident Response Team）人材の定義と確保 [10]に準拠している．SecBoK は，カリキュラム標準 J17[6]の情報セキュリティ領域のカリキュラム標準である J17-CyberSecurity[7]に参照されているので, SecBoK の定義する知識・スキルに基づいてシラバスを作成することが可能である．

SecBoK では，ロールとして，CISO（最高情報セキュリティ責任者），POC（Point of Contact），ノーティフィケーション，コマンダー・トリアージ，インシデントマネージャー・インシデントハンドラー，キュレーター，リサーチャー，セルフアセスメント・ソリューションアナリスト，脆弱性診断士，教育・啓発，フォレンジックエンジニア，インベスティゲーター，リーガルアドバイザー, IT 企画部門，IT システム部門，情報セキュリティ監査人の 16 種が定義されている．また，ロールごとに必要とされている知識・スキルを前提スキル，必須スキル，参考スキルの 3 段階でスコアリングしており，前提スキルなら 1，必須スキルなら 2，参考スキルなら 0.5 を割り当てられている．

また，1145 の知識・スキルを定義し，知識分野として，00 基礎, 01IT･セキュリティ基礎, 02IT ヒューマンスキル，03 セキュガバナンス，04 セキュマネジメント，05 ネットセキュリティ，06 システムセキュリティ，07 セキュア設計構築，08 セキュリティ運用，09 暗号・認証・署名，10 サイバー攻撃手法，11 インテリジェンス，12 デジタルフォレンジクス，13 サイバー捜査，14 セキュリティ人材育成，15 法・制度・標準，16 ビジネススキル，17 関連領域に分類している．知識・スキルのレベルは，低（概ね経験 3 年未満でも対応可能），中（経験 3 年以上または関連する演習・トレーニング受講者なら対応可能），高（経験 10 年以上または高度な研修受講を前提とする専門実務経験者または「突出した人材」なら対応可能）の 3 段階に加え，ペンディング（レベル付けの対象外）を合わせた，4 段階のレベル付けがなされている．

4. 情報通信学部のカリキュラム分析

本稿執筆時点において, 改組前の JT, 改組後の JE には，情報セキュリティあるいはサイバーセキュリティに関する教員が複数名在籍している．セキュリティ専科の学科ではないにもかかわらず，1 つの学科にセキュリティを専門とする教員が複数名在籍しているのは, 国内の大学において，珍しい状況である．

学科のカリキュラムは，カリキュラム・ポリシーに従って, 在籍教員の専門性が活かされた構成となることが多い．セキュリティ専科の学科ではないのであれば，セキュリティに隣接する学問分野に立脚し，その中に情報セキュリティ教育が配置されているはずである．

JE は 2022 年に改組され，米国計算機学会（ACM）と米国電気電子学会（IEEE）が定めた情報技術の国際標準カリキュラム IT2017[4]に準拠してカリキュラムが作成された．IT2017 では，Essential IT domains として 10 領域，Supplemental IT domains として 9 領域を定めており，いずれの領域にもサイバーセキュリティが含まれている．Essential IT domains は全体の 40%を占めているが，その中でも，Cybersecurity Principles (ITE-CSP)は 6%で最も高い比率となっており，サイバーセキュリティは最重要視されている．そのため，IT2017 に準拠した JE のカリキュラムもセキュリティが重視されていることが予想される．

本章では，JT と JE それぞれのカリキュラムが，情報セキュリティ教育において，どのような位置づけで，どのような人材育成に資するかを, SecBoK に照らして分析する．

4.1 分析方法

各学科のカリキュラムによって，どのような情報セキュリティ教育が行われているかを分析するために，各学科のカリキュラムから区分 IV 主専攻科目を分析対象とする．JT は既に完成年度を迎えており，各授業科目のシラバスが存在しているが，JE は完成年度を迎えていないため，すべての授業科目のシラバスが存在しておらず，授業科目の概要しか参照する文書がない．本来であれば，シラバス内の授業の目標，テーマ，キーワード，授業要旨または授業概要，授業計画を利用することで，より厳密性と精度の高い分析が可能と見込まれるが，JT と JE で分析結果を比較可能とするため，シラバスがない授業科目については授業科

目の概要を用い，シラバスがある授業科目についてはシラバス内の授業要旨または授業概要を分析に用いることとした．

分析は以下の手順で行う．

（1） 授業科目ごとにシラバスから授業要旨または授業概要，あるいは授業科目の概要を抽出する．
（2） 抽出した文字列に対して，形態素解析を行い，名詞のみを抽出する．なお，名詞が連続する場合は，結合する．
（3）抽出した名詞から，調査に不適切な用語を取り除き，調査対象語とする．
（4） SecBoK の各知識・スキルにおける小項目に，調査対象語が含まれるかどうかを，全ての授業科目で調査する．

分析は Ubuntu 22.04.2 上の Python 3.10.6 で行い，形態素解析には Janome 0.4.2 を使用した．

4.2 ロールに対する適合度の分析

本分析では，各授業科目がそれぞれのロールで必要とされているスキルをどの程度充足しているかを分析する．3 章で説明したように，SecBoK では 16 種のロールが定義されている．分析手順 4 で得られた結果と，ロールごとに必要とされている知識・スキルがどの程度一致しているかを調べ，各授業科目がロールごとに必要とされている知識・スキルをどの程度充足しているかを調べ，ロールに対する適合度を求める．本論文では紙面の都合上，授業科目ごとに求めた適合度を集約し，カリキュラム全体で評価する．

分析結果を Table 1 に示す．Table 1 より，JE よりも JT の方が多くのロールに対して適合度が高いが，その差はいずれも大きくはない．

Table 1 Conformity to Rolls.

Rolls	JT	JE	Difference (absolute)
CISO	86%	85%	0.31%
POC	77%	82%	5.37%
Notification	78%	81%	2.63%
Commander and Triage	83%	82%	0.57%
Incident managers and Incident handlers	84%	79%	5.79%
Curator	82%	79%	2.50%
Researcher	83%	79%	4.49%
Self Assessment and Solution Analyst	87%	85%	2.29%
Vulnerability Assessor	87%	83%	3.86%
Education and Awareness	60%	70%	10.11%
Forensic Engineer	83%	81%	1.62%
Investigator	79%	80%	1.31%
Legal Advisor	78%	74%	3.83%
IT Planning Department	82%	82%	0.42%
IT Systems Department	89%	88%	1.43%
Information Security Auditor	79%	83%	3.41%

4.3 知識分野に対する充足度の分析

本分析では，各授業科目が SecBoK で定義されている知識・スキルをどの程度充足しているかを知識分野ごとに分析する．3 章で説明したように，SecBoK では 1145 の知識・スキルを 18 の知識分野に分類している．分析手順 4 で得られた結果と，知識分野ごとに定義されている知識・スキルをどの程度充足しているかを授業科目ごとに調べ，知識分野に対する充足度を求める．本論文では紙面の都合上，授業科目ごとに求めた充足度を集約し，カリキュラム全体で評価する．

分析結果を Table 2 に示す．Table 2 より，知識分野の充足度は，JT よりも JE の方が高い．また，いくつかの知識項目において，JT と JE の差は大きくなっている．

Table 2 Sufficiency for Knowledge Fields.

Knowledge Fields	JT	JE	Difference (absolute)
00Basics	89%	81%	8.11%
01IT & Security Basics	83%	88%	4.17%
02IT Human Skill	92%	96%	4.17%
03Security Governance	100%	100%	0.00%
04Security Management	97%	100%	3.03%
05INetwork security	91%	88%	2.94%
06Systems Security	97%	97%	0.00%
07Secure design and construction	93%	93%	0.00%
08Security Operation	84%	87%	2.63%
09Cryptography, Authentication and Signature	100%	79%	21.43%
10Cyber Attack Techniques	85%	68%	17.07%
11Intelligence	77%	83%	6.40%
12Digital Forensics	85%	76%	9.09%
13Cyber Investigation	50%	75%	25.00%
14Security Personnel Training	76%	94%	17.65%
15Laws, Institutions and Standards	74%	81%	7.41%
16Business Skills	75%	82%	7.02%
17Related Areas	88%	85%	3.04%

5. 考察

本章では，4 章の分析結果から，JT および JE のカリキュラムがどのような情報セキュリティ人材育成に資するかを考察する．また，両学科のディプロマ・ポリシーおよびカリキュラム・ポリシーを参照し，カリキュラムにおける情報セキュリティの位置づけを議論する．

5.1 JT と JE の比較

まず，JT と JE のロールにおける違いを考察する．Table 1 より，多くのロールにおいて JT と JE の差は大きくない．

JT が JE よりも適合度が高いロールは，差が大きい順に，

インシデントマネージャー・インシデントハンドラー，リサーチャー，脆弱性診断士である．インシデントマネージャーは，インシデントハンドラーに指示を出し，インシデントの対応状況を把握し，対応履歴を管理するとともにコマンダーへ状況を報告するロールである．インシデントハンドラーは，インシデントの処理を行い，セキュリティベンダーに処理を委託している場合には指示を出して連携し，管理を行うロールである．リサーチャーは，セキュリティイベント，脅威情報，脆弱性情報，攻撃者のプロファイル情報，国際情勢の把握，メディア情報などを収集し，キュレーターに引き渡すロールである．脆弱性診断士は，アプリやインフラに脆弱性があるか，検査，診断を行い，評価するロールである．これらの結果から，JT は JE よりもテクニカルなセキュリティ人材に適したカリキュラムであることがわかる．

対して，JE が JT よりも適合度が高いロールは，差が大きい順に，教育・啓発，POC，情報セキュリティ監査人である．教育・啓発は，社内のリテラシーの向上，底上げのための教育及び啓発活動を行うロールである．POC は，社外向けでは JPCERT コーディネーションセンター，内閣サイバーセキュリティセンター（NISC），警察，監督官庁，日本シーサート協議会（NCA），他 CSIRT（Computer Security Incident Response Team）等との連絡窓口，社内向けでは IT 部門調整担当社内の法務，渉外，IT 部門，広報，各事業部等との連絡窓口となり，情報連携を行うロールである．情報セキュリティ監査人は，情報セキュリティに係るリスクのマネジメントが効果的に実施されるよう，リスクアセスメントに基づく適切な管理策の整備，運用状況について，基準に従って検証又は評価し，もって保証を与えあるいは助言を行うロールである．これらの結果から，JE は JT よりもコミュニケーターや調整役に適したカリキュラムであることがわかる．

次に, JT と JE の知識分野における違いを考察する. Table 2 より，いくつかの知識分野において，差が大きくなっている．

JT が JE よりも充足度が高い知識分野は，差が大きい順に，09 暗号・認証・署名，10 サイバー攻撃手法，12 デジタルフォレンジクスである. これらの結果から, JT は JE よりも情報セキュリティの基礎的な技術やプリミティブな知識の充足度が高いことがわかる．

対して，JE が JT よりも充足度が高い知識分野は，差が大きい順に，13 サイバー捜査，14 セキュリティ人材育成，15 法・制度・標準である．これらの結果から，JE は JT よりも分野横断的，境界領域的な知識の充足度が高いことがわかる．

5.2 JT のカリキュラム

本節では，これまでの分析結果を JT のディプロマ・ポリシーおよびカリキュラム・ポリシーに照らして，さらに詳細に分析する．

JT のディプロマ・ポリシーは以下の通りである．

・『知識・理解』 急速に発展する通信ネットワーク技術に柔軟に対応できる基礎学力と先端技術の知識を有している．
・『汎用的技能』 国境を越える技術である通信ネットワークを通して国際社会の発展に貢献できる，独創的で先端的な技術開発力を有している．
・『態度・志向性』 通信ネットワークの利便性と危険性を理解し，通信ネットワーク基盤の諸課題を総合的に把握し解決することができる．

このディプロマ・ポリシーに基づいて，カリキュラム・ポリシーでは,「通信系科目」,「ネットワーク系科目」,「ソフトウェア系科目」に分類した専門科目群と，それらに共通する「基幹科目」を段階的に学修出来るようにカリキュラム・マップを構成している．5.1 節で示したように, JE に対して JT の特徴が現れている知識分野は，09 暗号・認証・署名，10 サイバー攻撃手法，12 デジタルフォレンジクスである．それぞれに寄与度が高い授業科目は，暗号理論，情報通信セキュリティ入門, 通信ネットワーク入門であった．これらの科目の担当教員は，いずれもセキュリティ専門の教員であり，カリキュラム・マップによれば，いずれも「ネットワーク系科目」に属している．つまり，JT の情報セキュリティ教育はネットワークに立脚したセキュリティであることがわかる．

5.3 JE のカリキュラム

同様に，JE についても詳細に分析する．

JE のディプロマ・ポリシーは以下の通りである．

・『知識・理解』 高度情報化社会が要求する情報通信の多様な先端技術に柔軟に対応できる基礎・専門知識．
・『汎用的技能』 グローバル社会の中で活躍できる英語能力と，多様化する価値観を受容できるコミュニケーション力を持ち，先端的情報通信技術を利活用して，社会に生じる様々な問題に対して他分野との協働により解決を目指すことができる“コーディネート力”と実践的専門能力．
・『態度・志向性』 通信ネットワークの利便性と危険性を理解し，通信ネットワーク基盤の諸課題を総合的に把握し解決することができる．

このディプロマ・ポリシーに基づいて，カリキュラム・ポリシーでは,「学系共通科目」,「情報通信学基幹専門科目」,「情報通信学基幹 : 自己発展科目」, 高年次にはより専門性の高い 4 つの科目群である「先端的データ処理」,「プラットフォーム・デザイン」,「総合情報システム」,「マネジメントシステム」を設定している．5.1 節で示したように，JT に対して JE の特徴が現れている知識分野は，13 サイバー捜査, 14 セキュリティ人材育成, 15 法・制度・標準である．それぞれに寄与度が高い授業科目は，スマート社会と人間行動，プロジェクト実習 2，エッジ・コンピューティングであった．本稿執筆時点の担当教員の予定によれば，プロジェクト実習 2 は担当教員が 12 名おり，内 2 名がセキュリティ専門の教員である．他 2 科目についてはセキュリティが専門ではない教員が担当である．このように，JE のカリキュラムにおいては，授業科目の概要に情報セキュリティに関連するキーワードが含まれているものの，必ずしもセキュリティの専門家が教授するとは限らない. そのため，充足度が高い知識分野だとしても，適切かつ十分な情報セキュリティ教育が実施されるかは不透明である．

また, 5.1 節より, JE が JT よりも適合度が高いロールは，教育・啓発，POC，情報セキュリティ監査人であり，ディプロマ・ポリシーが示す“コーディネート力”はまさに養成する人材像と一致しているといえる．

5.4 SecBoK の問題点

SecBoK は NIST の NICE Framework（SP 800-181 Rev.1）[9]を参照し，NICE Framework のロール（NICE ロール）に基づいて SecBoK のロールが作成されている．しかしながら，NICE Framework には，SecBoK のロール以外にも多数のロールが定義されている．NICE Framework では，SECURELY PROVISION (SP)， OPERATE and MAINTAIN (OM)， OVERSEE and GOVERN (OV), PROTECT and DEFEND (PR), ANALYZE (AN)， COLLECT and OPERATE (CO)， INVESTIGATE (IN)の 7 つのカテゴリーにロールを分類している．SecBoK と NICE ロールの対応関係を NICE Framework のカテゴリーで評価した結果を Table 3 に示す．Table 3 より，OV，IN の対応度は高いが，SP，CO の対応度は著しく低い．SP には，Software Developer，Enterprise Architect，Security Architect，Systems Developer といった，システム開発者，ソフトウェア開発者に関係する重要なロールが含まれているが，SecBoK には含まれていない．そのため，このようなロールを養成するカリキュラムの場合，SecBoK では正しく評価することができない．

このように，SecBoK では CSIRT に関するロールが多く定義されているが，CSIRT 関連以外のセキュリティ人材は，SecBoK では評価することができない．

しかしながら，実際に不足が問題となっているセキュリティ人材は，概ね CISO，SOC (Security Operation Center)，CSIRT であり，実態と乖離しているわけではない．例えば，サイバー攻撃の監視を行う SOC やインシデント発生時の事後対応を行うフォレンジックエンジニアなどは，中小企業が自社で雇用し続けることは困難であるため，セキュリティベンダーにアウトソースすることが現実的である．一方で，インシデント対応に必要となる POC やインシデントハンドラーは，自組織内で雇用を必要とするロールであると考えられる．そのため，SecBoK が定義するロールは，日本が現在必要としているセキュリティ人材を如実に表しており，育成すべき重要なロールであるといえる．

Table 3 Comparison of NICE rolls and SecBoK rolls.

Categories	NICE [rolls]	SecBoK [rolls]	Sufficiency [%]
SP	11	1	9%
OM	7	3	43%
OV	14	11	79%
PR	4	2	50%
AN	7	1	14%
CO	6	0	0%
IN	3	3	100%

5. おわりに

本論文では，全学改編前後の東海大学情報通信学部のカリキュラムについて，情報セキュリティ教育の観点から，SecBoK を用いて分析を行った．

全学改編前の JT では，ネットワークに立脚した情報セキュリティ教育となっており，特にテクニカルなセキュリティ人材育成に適したカリキュラムであった．また，知識分野の適合度に寄与している授業科目は，情報セキュリティに関連する専門科目であり，集中的に効率よく教育が行われていることが分かった．

一方，全学改編後の JE では，国際標準カリキュラム IT2017 を用いてカリキュラム作成が行われたことが，分析結果からも明らかであった．JT との比較において，JE は分野横断的，境界領域的な知識分野の充足度が高くなっており，全学改編の構想が分析結果にも表れている．また，JE のディプロマ・ポリシーに挙げられている“コーディネート力”は，適合度の高いロールからも見て取ることができ，養成する人物像とカリキュラムは一致していた．しかしながら，IT2017 に従ってカリキュラムが作成されているものの，実際にその科目を教授する者の専門性が必ずしも適合しておらず，適切かつ十分な情報セキュリティ教育が実施されるかは不透明である．

今後の展望としては，国内唯一の情報セキュリティ学科を有す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，IPA の情報処理安全確保支援士試験免除対象学科等の認定を受けている近畿大学情報学部情報学科のカリキュラムを分析し，東海大学情報通信学部情報通信学科との比較を行い，それぞれの特長を明らかにしたい．

参考文献

1) 総務省，“我が国のサイバーセキュリティ人材の現状について，”https://www.soumu.go.jp/main/content/000591470.pdf, 2018.（閲覧日：2023 年 4 月 9 日）
2) 日本ネットワークセキュリティ協会，“セキュリティ知識分野（SecBoK）人材スキルマップ 2021 年版，”https://www.jnsa.org/result/skillmap/，2021.（閲覧日：2023 年 4 月 9 日）
3) ACM/IEEE/AIS SIGSEC/IFIP，“CSEC2017 Curricular Guidelines，”https://cybered.hosting.acm.org/wp/，2017.（閲覧日：2023 年 4 月 9 日）
4) ACM/IEEE-CS，“Information Technology Curricular Gudelines − IT2017，”https://it2017.acm.org/，2017.（閲覧日：2023 年 4 月 9 日）
5) ACM/IEEE-CS，“Computing Curricula 2020: Paradigms for Global Computing Education，”https://dl.acm.org/doi/book/10.1145/3467967, 2020.（閲覧日：2023 年 4 月 9 日）
6) 情報処理学会，“カリキュラム標準 J17，”https://www.ipsj.or.jp/annai/committee/education/j07/curriculum_j17.html，2018.（閲覧日：2023 年 4 月 9 日）
7) 情報処理学会，“カリキュラム標準 情報セキュリティ J17-CyberSecurity，”https://www.ipsj.or.jp/annai/committee/education/j07/ed_j17-CyberSecurity.html，2018.（閲覧日：2023 年 4 月 9 日）
8) 孫英敬，山口由紀子，嶋田創，高倉弘喜： 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，情報処理学会論文誌，Vol. 58，No. 5，pp. 1163–1174，2017.
9) NIST，“Workforce Framework for Cybersecu- rity (NICE Framework), SP 800-181 Rev.1，”https://doi.org/10.6028/NIST.SP.800-181r1，2020.（閲覧日：2023 年 4 月 9 日）
10) 日本シーサート協議会，“CSIRT 人材の定義と確保 (Ver.2.1)，”https://www.nca.gr.jp/activity/imgs/recruit-hr20201211.pdf，2020.（閲覧日：2023 年 4 月 9 日）