文系大学における情報セキュリティ人材育成プログラムの考案

片瀬　拓弥

Devising an information security development program at liberal arts universities

Takuya KATASE

要旨

本研究は、文系大学における情報セキュリティ人材育成プログラムとして、第一に情報処理国家試験の取得を目指す科目を大学カリキュラム内に組み入れ、「基礎的な情報セキュリティ教育」を実施することを提案した。第二に「情報セキュリティ教育に関するカードゲーム等を活用したロールプレイング学習」を経た後、「学内 CSIRT の正規メンバーとして学生参加を促す仕組み」を構想した。これらにより、文系大学においても実現可能な情報セキュリティ人材育成プログラムを考案した。

キーワード：情報セキュリティ教育、情報処理国家試験、インシデント、CSIRT、カードゲーム

１．はじめに

2023 年から 2024 年にかけて、ChatGPT を代表格とする生成系 AI の目覚ましい進化により、AI 技術が我々の日常生活やビジネス業務に深く浸透してきている。この大きな変革の中で、サイバーセキュリティの確立は、ますます重要性を増している。特に、企業や組織のデジタルデータがオンラインで共有される環境下では、情報セキュリティの強化は不可欠となっている。サイバー攻撃やデータ漏洩などのセキュリティ侵害は、個人や組織に深刻な被害をもたらし、その対策がますます急務となっている。情報セキュリティ白書（2023）よれば、「2022 年度に観測された世界と日本における情報セキュリティインシデントの発生状況について、サイバー犯罪の件数と被害額は過去 4 年にわたり増加を続け、2022 年の件数は 80 万件と微減したが、被害額は大幅に増加し 103 億ドルとなった」と報告している（図 1）。ここでいう「セキュリティインシデント（security incident）」とは、IT 用語辞典（2023）によれば「情報管理やシステム運用に関して保安上の脅威となる人為的な事象を指す。また、単にインシデントと略される」こともある。よって、「セキュリティインシデント」を「インシデント」と略記する。表 1 に情報セキュリティ白書（2023）に掲載された「情報セキュリティ 10 大脅威 2023 個人・組織向け脅威の順位」を示す。これによると、組織向けの一番の脅威は「ランサムウェアによる被害」となっている。ランサムウェア（ransomware）とは、「ransom（身代金）と software（ソフトウェア）を組み合わせた造語であり、パソコンやサーバー等のシステムをロックすることや、システムに保存されているファイルを暗号化することにより使用不能にするウイルスの総称である。ランサムウェアによって使用不能にしたシステムやファイルを復旧できるようにすることと引き換えに身代金を要求するサイバー攻撃をランサムウェア攻撃と呼ぶ」（情報セキュリティ白書 2023）。そして、このランサムウェア攻撃のインシデント対応は、「標的型攻撃と同様の手口が使用されるため、対応も全体的には標的型攻撃と同様である。標的型攻撃とは、ある特定の企業・組織や業界等を狙って行われるサイバ

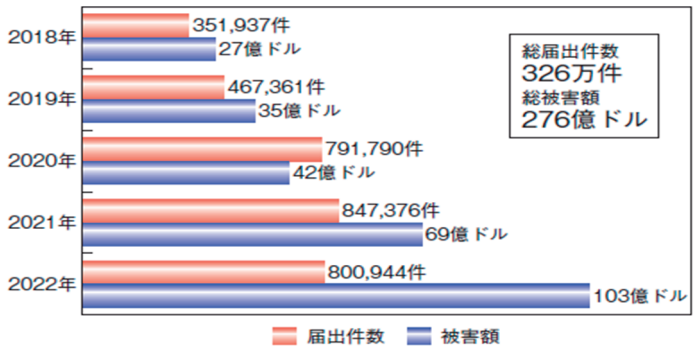

図 1　サイバー犯罪の届出件数と被害額の推移（2018～2022 年）

（出典）情報セキュリティ白書（2023）　FBI Internet Crime Report 2022 を基に IPA 編集版を転載

表 1　情報セキュリティ 10 大脅威 2023「個人」・「組織」向け脅威の順位

「個人」向け脅威	順位	「組織」向け脅威
フィッシングによる個人情報等の詐取	1	ランサムウェアによる被害
ネット上の誹謗・中傷・デマ	2	サプライチェーンの弱点を悪用した攻撃
メールや SMS 等を使った 脅迫・詐欺の手口による金銭要求	3	標的型攻撃による機密情報の窃取
クレジットカード情報の不正利用	4	内部不正による情報漏えい
スマホ決済の不正利用	5	テレワーク等のニューノーマルな働き方を狙った攻撃
不正アプリによるスマートフォン利用者への被害	6	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
偽警告によるインターネット詐欺	7	ビジネスメール詐欺による金銭被害
インターネット上のサービスからの個人情報の窃取	8	脆弱性対策情報の公開に伴う悪用増加
インターネット上のサービスへの 不正ログイン	9	不注意による情報漏えい等の被害
ワンクリック請求等の不正請求による金銭被害	10	犯罪のビジネス化（アンダーグラウンドサービス）

（出典）情報セキュリティ白書（2023）から転載

一攻撃の一種である。フィッシングメールやウイルスメールを不特定多数の相手に無差別に送り付ける攻撃とは異なり、標的型攻撃は、特定の企業・組織や業界が持つ機密情報の窃取やシステム・設備の破壊・停止といった、明確な目的をもって行われる」（情報セキュリティ白書 2023）。実際、2022 年 6 月に埼玉大学がランサムウェアによる被害を受けたと報告している（埼玉大学 2023）。

IT 用語辞典（2023）によれば、「このようなインシデントが発生した際に行われる被害把握や原因特定、正常な状態への復旧、利害関係者への報告や連絡といった対応業務をインシデントレスポンス（incident response）と称し、これを行うために組織内に設置された部署を CSIRT（Computer Security Incident Response Team/シーサート）という」と解説している。大学も組織である以上、この CSIRT 設置ニーズが高まっているといえる。

2．学校における情報セキュリティ対応

2．1　文部科学省からの情報セキュリティ対応指針

文部科学省（2022a）は、地方公共団体が設置する学校（小学校、中学校、義務教育学校、高等学校、中等教育学校及び特別支援学校）を対象とした教育情報セキュリティポリシーに関するガイドラインを改訂し、各教育委員会・学校に対し情報セキュリティポリシーの策定と運用ルールの見直しを促している。これらの基本理念を要約すると以下の①～⑥になる。

①組織体制を確立すること

学校における情報セキュリティ対策の考え方を確立させるため、情報セキュリティの責任体制を明確にしておくこと。最高情報セキュリティ責任者（CISO：Chief information Security Officer）の設置。

②児童生徒による重要性が高い情報へのアクセスリスクへの対応を行うこと

コンピュータを活用した学習活動の実施など、児童生徒が日常的に情報システムにアクセスする機会があるため、本来は児童生徒が見ることを想定していない重要性が高い情報等にアクセスするリスクを回避すること。

③標的型及び不特定多数を対象とした攻撃等による脅威への対応を行うこと

学校ホームページや教職員によるメールの活用、さらには学習活動におけるインターネットの活用等が行われていることから、地方公共団体のいわゆる行政部局と同様に、標的型及び不特定多数を対象とした攻撃等による脅威に対する対策を講ずること。

④教育現場の実態を踏まえた情報セキュリティ対策を確立させること

成績処理等を自宅で行うことを目的として、教員が個人情報を自宅に持ち帰る場合がある。また、児童生徒が活用する情報システムであっても重要性が高い情報を保持する場合、暗号化等の対策を講ずること。

⑤教職員の情報セキュリティに関する意識の醸成を図ること

学校は、成績や生徒指導関連等の重要性が高い情報を取り扱うことから、研修等を通じて、教職員の情報セキュリティに関する意識の醸成を図ること。

⑥教職員の業務負担軽減及びICTを活用した多様な学習の実現を図ること

情報セキュリティ対策を講じることによって校務事務等の安全性が高まるとともに、教員の業務負担軽減へとつながる運用となるよう配慮すること。

このような状況に対応し、各地方公共団体・教育委員会の情報セキュリティ担当者が無料参加できるCSIRT研修も行われている（CYDER 2023）。この研修は、サイバー攻撃を受けた際の一連のインシデント対応に関し、パソコンを操作しながらロールプレイ形式で体験できる演習となっている。

また、文部科学省（2022b）は、大学を含む高等教育機関に対しても「大学等におけるサイバーセキュリティ対策等の継続的な取り組みについて」という通知を出している。この通知では、①リスク管理体制の構築、②リスクの特定、③リスク対策、④サプライチェーンリスクへの対応、⑤インシデント対応体制（CSIRT 等）の構築、⑥セキュリティ運用の実施、⑦監査等での運用チェックについて、強化改善するように促している。

２．２　大学のCSIRT組織の現状

このように大学においても情報セキュリティに関するインシデント対応組織（CSIRT）の必要性が高まっている。ここで、国内大学内に明確なCSIRT組織が存在するかどうか、日本シーサート協議会（2023）の加盟会員リスト（全523団体）を調査すると表2のように21校であった。主として、国公立の理工系学部を持つ総合大学に偏りがちであり、多くの私立文系大学の学内組織では、実際のインシデントに十分に対処できる能力を備えていない可能性がある。このような状況では、文系大学生が情報セキュリティの基礎的知識を習得する機会もあまりないのではないかという課題も浮かび上がる。

次に、大学のCSIRT組織に関する先行文献調査を行った。小川（2018）は、全国602校の私立大学の情報セキュリティ担当者に対し、大学CSIRT設置についてアンケート調査を行った。その結果、回答のあった131校の私立大学でCSIRTが設置されているのは、わずか10校のみであり、121校は設置されていないと報告している。一方、青山・三河（2020）は、新潟大学のCSIRT組織を紹介してい

表 2　日本シーサート協議会の加盟会員リスト（大学のみを抜粋）

正式名称	所属組織
Chiba University Cyber Security Incident Response Team	国立大学法人　千葉大学
北海道大学 CSIRT	国立大学法人　北海道大学
海洋大 CSIRT	国立大学法人　東京海洋大学
近畿大学 CSIRT	学校法人　近畿大学
工学院大学情報セキュリティインシデント対応チーム	学校法人　工学院大学
九州工業大学　ネットワークセキュリティ基盤運用室	国立大学法人　九州工業大学
宮崎大学情報セキュリティインシデント対応チーム	国立大学法人　宮崎大学
新潟大学情報セキュリティインシデント対応チーム	国立大学法人　新潟大学
大阪教育大学 CSIRT	国立大学法人　大阪教育大学
岡山大学 CSIRT	国立大学法人　岡山大学
大阪公立大学情報セキュリティインシデント対応チーム	公立大学法人　大阪公立大学
OU-CSIRT	国立大学法人　大阪大学
情報統括本部　九大 CSIRT	国立大学法人　九州大学
静岡大学情報危機対策チーム	国立大学法人　静岡大学
国立大学法人信州大学セキュリティ・インシデント・レスポンス・チーム	国立大学法人　信州大学
島根大学コンピューターセキュリティインシデント対応チーム	国立大学法人　島根大学
東京工業大学 情報システム緊急対応チーム	国立大学法人　東京工業大学
東京電機大学シーサート	東京電機大学総合メディアセンター
学校法人東京女子医科大学 情報セキュリティインシデント対応チーム	学校法人　東京女子医科大学
東京大学情報システム緊急対応チーム	国立大学法人　東京大学
WIDE Incident Response Team	慶應義塾大学（WIDE プロジェクト）

る。この報告では、2016 年度からセキュリティ体制の大幅な見直しと再構築を行い、実働組織として新たに 28 個の部局 CSIRT を導入したとしている。このきめ細かな組織体制により、インシデントに対する初動対応を改善したと報告している。ただし、学生が正規の CSIRT メンバーになることは想定していないと推測される。これらの先行文献を比較すると、一般的に国立大学と私立大学の CSIRT 設置に関する格差は明らかであり、特に私立文系大学の CSIRT 組織の設置は遅れていると推測される。

また、大学の CSIRT 組織による教育研修・訓練実施について、米谷ら（2018）は、香川大学の事例を紹介している。この報告では、医学部附属病院において標的型攻撃によって端末 1 台がウイルスに感染したというインシデント発生に基づき、情報セキュリティ対策の強化の一環として、2016 年に CSIRT 組織を発足させ、訓練・教育・注意喚起・報告受付の各業務を組織化したとしている。さらに、標的型攻撃メール訓練を教職員に行った結果を報告している。ただし、この訓練に学生は参加していないと推測される。中西ら（2018）も、岩手大学における CSIRT 体制の構築について報告しているが、この事例でも学生が正規の CSIRT メンバーとして参加する仕組みは取り入れられていないと推測される。

３．本研究の目的

本研究は、文部科学省からの情報セキュリティ対応指針に基づき、大学においても設置ニーズが高まっているインシデント対応組織（CSIRT）の現状を踏まえ、学内 CSIRT 組織を活用し、その CSIRT の正規メンバーとして学生参加を促す仕組みを構想したい。そのことにより、インシデント対応を体験的に学び、文系大学においても実践可能な情報セキュリティ人材育成プログラムを考案することが目的である。

４．情報セキュリティ人材育成プログラム

４．１　基礎的な情報セキュリティ教育

本研究では、まず、基礎的な情報セキュリティ教育のカリキュラム構成を検討する。2023 年度現在、本学の情報系基礎科目は、情報基礎演習、情報活用演習、情報科学の 3 科目となっている。演習 2 科目については、情報リテラシー教育として、Word、Excel のスキル習得が主目的となっている。一方、情報科学は、後述の IT パスポート試験や類似情報検定の受験を想定した授業内容となっている。しかし、現在のカリキュラム構成の課題は、実践的な情報セキュリティ教育を実施する前段階に留まっていることにある。よって、本研究では、さらに踏み込んだカリキュラム構成を検討したい。そこで、独立行政法人情報処理推進機構（以下、IPA）主催の国家試験（IPA 2023a）である IT パスポート試験、情報セキュリティマネジメント試験、基本情報技術者試験に着目する。これらの資格は、学生にとって情報技術の知識基盤を構築できる上に、就職活動時において、国家資格として履歴書の資格欄に記載できることから、学生にとっても資格取得のメリットが大きいと考えられる。

①IT パスポート試験（以下、IP 試験）

IP 試験は、IT を利活用する全ての社会人・学生を対象としており、情報技術の初歩的知識を評価するレベル 1 の情報処理国家試験である。この試験に合格するために必要な学習時間の目安は「100～200 時間」といわれている（TAC 2023）。一方、著者の指導経験からすると効率的学習を行えば、約 50 時間程度の学習で取得可能と考えている。また、試験方式は、2011 年から CBT（Computer Based Testing）方式となり、2023 年では年間を通じて随時受験可能である。合格率は、概ね 50％前後となっている（IT パスポート試験 2023）。

②情報セキュリティマネジメント試験（以下、SG 試験）

SG 試験は、業務で個人情報を取り扱う者、業務・管理部門で情報管理を担当する者、外部委託先に対する情報セキュリティ評価・確認を行う者、情報セキュリティ管理の知識・スキルを身に付けたい者、IP 試験合格からステップアップしたい者が主対象となっており、情報セキュリティに関する広範な知識を評価するためのレベル 2 の情報処理国家試験である。この試験に合格するために必要な学習時間の目安は「100～200 時間」といわれている（TAC 2023）。一方、著者の指導経験からすると、IP 試験合格程度の知識があれば、約 50 時間程度の追加学習で取得可能と考えている。また、試験方式は、IP 試験同様に 2020 年から CBT 方式となり、2023 年では年間を通じて随時受験可能である。2023 年（CBT 方式）の合格率（IPA 2023b）は、概ね 70％前後となっている。

③基本情報技術者試験（以下、FE 試験）

FE 試験は、IT を活用したサービス、製品、システム及びソフトウェアを作る人材に必要な基本的知識・技能をもち、実践的な活用能力を身に付けたい者、主にプログラマーやシステムエンジニアなどの ICT 関連企業や部門に勤めている人などを主対象としたレベル 2 の情報処理国家試験である。IT

業界では「IT エンジニアの登竜門」として認識されており、特に大手のシステム開発会社では入社後に合格が義務付けられていることもある。この試験に合格するために必要な学習時間の目安は「200〜400 時間」といわれている（TAC 2023）。一方、著者の指導経験からすると、IP 試験合格程度の知識があれば、約 100 時間程度の追加学習で取得可能と考えている。また、試験方式は、IP 試験同様に 2023 年から CBT 方式となり、年間を通じて随時受験可能である。2023 年（CBT 方式）の合格率（IPA 2023c）は、概ね 50％前後となっている。

さて、IPA（2023d）が公開している IP 試験、SG 試験、FE 試験のシラバス内容の比較を巻末付表に示す。この付表は、IP 試験シラバス Ver6.3、SG 試験シラバス Ver4.0、FE 試験シラバス 9.0 に基づいている。これらの試験の学習項目は、テクノロジー系、マネジメント系、ストラテジー系の 3 つの分野に大別されており、文系大学生のような IT 初学者が、情報処理国家試験の資格取得という具体的目標を持って、基礎的な情報セキュリティ知識を身につけるために適していると考える。

よって、基礎的な情報セキュリティ教育プログラムとして、IP 試験の学習範囲を網羅できる科目を大学 1 年次、SG 試験の学習範囲を網羅できる科目を大学 2〜3 年次、FE 試験の学習範囲を網羅できる科目を大学 2〜3 年次に、それぞれ系統的に配置することが考えられる。ただし、各試験の学習範囲に対応した科目が最低でも 1 科目ずつ配置されることが望ましいが、大学カリキュラムの構成上、難しいこともある。その場合、別の情報系科目の自習課題として、各試験の学習範囲を e ラーニングで補うことも考えられる。実際、これらの情報処理国家試験を大学カリキュラムに組み入れた事例について、インターネット検索により「IP 試験　大学シラバス」、「SG 試験　大学シラバス」、「FE 試験　大学シラバス」というキーワードを使って調査するといくつかの大学のシラバス例を見つけることができる。

４．２　学生の学内 CSIRT への参加方法

「基礎的な情報セキュリティ教育」を経た後、第一に学内 CSIRT 参加前の準備教育プログラムとして、「カードゲーム等を活用したロールプレイング学習」を実施することを提案したい。もちろん、情報セキュリティ知識だけでなく、パソコンやネットワーク機器を使った実機演習（ネットワーク実習やアクセスログ解析など）も必要である。しかし、文系大学ということに焦点化すると、大学カリキュラムの構成上も、このような実機演習科目を相当数配置することは難しい。そこで、大学 3 年次から 4 年次に配属される専門セミナー（いわゆるゼミ活動）、または、学生サークルや委員会等の活動として、ロールプレイング学習と実機演習を組み入れることは可能と考える。そこで、本研究では、特に文系大学生でも学習ハードルが低いと推測される「カードゲーム等を活用したロールプレイング学習」に着目した。ロールプレイング学習では、実際のインシデントを想定した「役割」と「場面」を具体的に設定する。「役割」は、CSIRT 内の役割（ロール）を指し、「場面」は、実際のインシデントケースを想定する。ここで、情報セキュリティ教育に関するカードゲーム等の一覧を表 3 に示す。いずれも、情報セキュリティの初学者向けに教育目的で開発されたゲームであり、文系大学生にも気軽に CSIRT 組織の役割や機能を学べるものと推測される。このような「情報セキュリティ教育に関するカードゲーム等を活用したロールプレイング学習」により、学内 CSIRT に参加前の模擬体験を行い、参加モチベーションや情報セキュリティ知識への一段の向上が図れるものと考える。

第二に、具体的な学内 CSIRT への参加方法を構想したい。実際、学内 CSIRT へ学生参加を促す事例が一部の私立理工系大学で挙げられている（TDU-CSIRT 2017）。この中の学生参加例としては、①学生チームによるセキュリティ関連機器のパトロール、②学生による Web サイト用のセキュリティ解

表 3　情報セキュリティ教育に関するカードゲーム等の一覧

ゲーム名称	ゲーム内容	開発組織名
ABCSIRT 30 分で学ぶ はじめてのインシデント対応	プレイスタイル：チーム対抗戦 プレイ人数：2〜4 名 プレイ時間：20〜30 分 学習効果：CSIRT の流れや、主な役割が学べる	中核人材育成プログラム 卒業プロジェクト 第 3 期生 （IPA 2023e)
GAME OF CSIRT 防ぐ、でもやられる、ならば対処する	プレイスタイル：個人またはチーム対抗戦 プレイ人数：2 名または 2 チーム プレイ時間：15〜20 分 学習効果：サイバー攻撃に対して必要な対応が学べる	中核人材育成プログラム 卒業プロジェクト 第 3 期生 （IPA 2023e)
マルウェアスイーパー 協力と決断力でパンデミックを阻止せよ	プレイスタイル：チーム連携 プレイ人数:：4 名 プレイ時間：20〜30 分 学習効果：CSIRT 連携の大切さを体感できる	中核人材育成プログラム 卒業プロジェクト 第 3 期生 （IPA 2023e)
攻撃者視点の獲得を目的としたボードゲーム：Cyber Attacker Placement	プレイ人数：3 人〜4 人 プレイ時間：45 分〜1 時間 学習効果：攻撃者を疑似体験することでセキュリティ対策の重要性を学ぶ。	中核人材育成プログラム 卒業プロジェクト 第 6 期生 （IPA 2023e)
セキュリティ専門家 人狼（通称：セキュ狼）	プレイ人数：3〜20 人 プレイ時間：20〜60 分 学習効果：インシデント対応に焦点を当てており、CSIRT としてのチーム連携や問題解決方法を学ぶ。	JNSA 教育部会 ゲーム教育ワーキンググループ JNSA（2023）
Malware Containment	プレイ人数：4〜5 人 プレイ時間：30〜60 分 学習効果：CSIRT メンバーとして、情報分析を行うことでインシデント対応の問題解決力を向上させる。	JNSA 教育部会 ゲーム教育ワーキンググループ JNSA（2023）

説ブログ記事の執筆、③学生が研究で開発したツール等の活用と研究へのフィードバック、であった。その後の活動記録を調査すると、「埼玉県警察と自治会学生 CSIRT 委員会（通称：学生 CSIRT）が合同で体験型サイバーセキュリティセミナーを開催した（東京電機大学 2023）」との Web ブログ記事を見つけることができた。一方、国内の文系大学事例は、文献及び Web 調査では発見できなかった。

さて、一般的なインシデント対応フローを示すと以下となる。ステップ①：事前準備、ステップ②：検知・報告、ステップ③：応急処置、ステップ④：調査、ステップ⑤：通知・公表、ステップ⑥：恒久対応、ステップ⑦：再発防止・事後対応、これらのステップ中において、学生参加が可能なフローを考えると、まずは「ステップ①：事前準備」と「ステップ⑦：再発防止・事後対応」に焦点化できる。なぜなら、インシデント発生時のリアル対応（ステップ②から⑥）は、機密情報管理の観点から参加ハードルが高いからである。一方、「ステップ①」は、インシデント発生時に備え、定期的なインシデント対応訓練やセキュリティ教育を実施する仕組み作りなどに学生参加を促せる。東京電機大学

（2023）の事例は、これに当たる。さらに「ステップ⑦」は、インシデント対応後の再発防止策を整理したり、根本的原因を追求したりすることに学生参加を促せる。ここでは必要に応じて、機密情報を除去した上で「アクセスログ」等を解析させ、インシデント報告書や再発防止案を書かせることも可能であろう。さらに機密情報に関する倫理規定を策定し、学生及びその保護者に対して機密保持に関する誓約書提出を課した上で学内 CSIRT のインシデント対応（ステップ②から⑥を含む）を教職員と共に実践するインターンシップ等も考えられる。このように「基礎的な情報セキュリティ教育」及び「情報セキュリティ教育に関するカードゲーム等を活用したロープレイング学習」を経た上で、学内 CSIRT の活動自体を情報セキュリティ人材育成プログラムの一環として位置づけることにより、情報関連の教育リソースが比較的少ない文系大学においても実現可能な構想と考える。

５．まとめ

本研究は、文部科学省からの情報セキュリティに関する対応指針に基づき、大学においても設置ニーズが高まっているインシデント対応組織（CSIRT）の現状を踏まえ、文系大学における情報セキュリティ人材育成プログラムとして、第一に情報処理国家試験の取得を目指す科目を大学カリキュラム内に組み入れ、「基礎的な情報セキュリティ教育」を実施することを提案した。第二に「情報セキュリティ教育に関するカードゲーム等を活用したロールプレイング学習」を経た後、「学内 CSIRT の正規メンバーとして学生参加を促す仕組み」を構想した。これらにより、文系大学においても実現可能な情報セキュリティ人材育成プログラムを考案した。ただし、私立文系大学では、学内 CSIRT 組織自体が設置されていないケースも多々あると考えられる。まずは、学内 CSIRT の設置を早急に進め、その後、考案したプログラムを実践し、その有効性を検証することが今後の課題である。

引用・参考文献

青山茂義・三河賢治（2020）「大学 CSIRT 体制に対する考察と新潟大学への部局 CSIRT の適用」『学術情報処理研究』, 24(1), 116-125.

CYDER（2023）「Cyber Defense Exercise with Recurrence：実践的サイバー防御演習）」『国立研究開発法人情報通信研究機構（NICT）』 https://cyder.nict.go.jp/course/ （2023/12/27 参照）

FBI（2022）「Internet Crime Report 2022」『米国連邦捜査局（Federal Bureau of Investigation）』

IPA（2023a）「試験情報>試験の概要>試験のメリット」『IPA 独立行政法人 情報処理推進機構』https://www.ipa.go.jp/shiken/about/index.html （2023/12/27 参照）

IPA（2023b）「試験情報>統計情報>統計情報（情報セキュリティマネジメント試験）」『IPA 独立行政法人 情報処理推進機構』https://www.ipa.go.jp/shiken/reports/toukei_sg.html（2023/12/27 参照）

IPA（2023c）「試験情報>統計情報>統計情報（基本情報技術者試験）」『IPA 独立行政法人 情報処理推進機構』https://www.ipa.go.jp/shiken/reports/toukei_fe.html（2023/12/27 参照）

IPA（2023d）「試験情報>試験要綱・シラバス>試験要綱・シラバスについて」『IPA 独立行政法人 情報処理推進機構』https://www.ipa.go.jp/shiken/syllabus/gaiyou.html（2023/12/27 参照）

IPA（2023e）「デジタル人材の育成>産業サイバーセキュリティ>中核人材育成プログラム>中核人材育成プログラム 卒業プロジェクト」『IPA 独立行政法人 情報処理推進機構』https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/index.html（2023/12/27 参照）

IT パスポート試験（2023）「IT パスポート試験>公開情報>統計情報」『株式会社日立ソリューションズ・クリエイト』https://www3.jitec.ipa.go.jp/JitesCbt/html/openinfo/statistics.html （2023/12/27 参照）

IT 用語辞典（2023） https://e-words.jp/w/セキュリティインシデント.html（2023/12/27 参照）
JNSA（2023）「JNSA 教育部会 ゲーム教育ワーキンググループ」『日本ネットワークセキュリティ協会』https://www.jnsa.org/edu/secgame/ （2023/12/27 参照）
情報セキュリティ白書（2023）「進む技術と未知の世界：新時代の脅威に備えよ」『独立行政法人情報処理推進機構（IPA）』
米谷雄介・後藤田中・小野滋己・青木有香・宮﨑凌大・八重樫理人・藤本憲市・林敏浩・今井慈郎・最所圭三（2018）「香川大学での標的型攻撃メール訓練の導入と改善点の検討」『学術情報処理研究』, 22(1), 54-63.
文部科学省（2022a）「教育情報セキュリティポリシーに関するガイドライン」（令和 4 年 3 月一部改訂）」『文部科学省』
文部科学省（2022b）「大学等におけるサイバーセキュリティ対策等の継続的な取り組みについて（通知）」『文部科学省 4 文科高第 367 号令和 4 年 6 月 22 日』
中西貴裕・福岡誠・金野哲士・田頭徹・鈴木健之・田口慎・大内慎也・木村優太・加治卓磨・川村暁（2018）「岩手大学における持続可能な情報セキュリティインシデント対応体制の構築」『学術情報処理研究』, 22(1), 44-53.
日本シーサート協議会（2023）『一般社団法人 日本コンピュータセキュリティインシデント対応チーム協議会』 https://www.nca.gr.jp/member/（2023/12/27 参照）
小川賢（2018）「私立大学情報セキュリティ担当者の CSIRT に関するアンケート調査」『神戸学院大学経営学論集』, 15(1), 93-107.
埼玉大学（2023）「ニュース一覧>本学の情報システムへの不正アクセスについて」『埼玉大学 HP』 https://www.saitama-u.ac.jp/news_archives/2023-0207-1206-9.html （2023/12/27 参照）
TAC（2023）「よくあるご質問>情報処理・パソコン>情報処理>各試験の学習時間はどれくらいかかりますか？」『資格の学校 TAC』 https://faq.tac-school.co.jp/support/list/web/knowledge1111.html（2023/12/27 参照）
TDU-CSIRT（2017）「東京電機大学における CSIRT 活動 講演資料」『サイバーセキュリティシンポジウム 2017 in TDU』https://www.csirt.dendai.ac.jp/csirt/public-information/ （2023/12/27 参照）
東京電機大学（2023）「ニュース一覧>埼玉県警察と学生が合同で体験型サイバーセキュリティセミナーを開催」『東京電機大学 HP』https://www.dendai.ac.jp/news/20230523-01.html（2023/12/27 参照）

SUMMARY

This study proposed the implementation of "basic information security education" as an information security human resource development program at liberal arts universities, firstly, by incorporating courses aiming to obtain the National Examination for Information Processing into the university curriculum. Secondly, after "role-playing learning using card games and other methods related to information security education," I proposed a "mechanism to encourage students to participate as regular members of the university's CSIRT.

Keywords : Information Security education, National Examination for Information Processing, Security Incident, CSIRT, Card Game

付表　IP 試験、SG 試験、FE 試験のシラバス比較表（■部分：学習項目）

分野	大分類	中分類	項目	IP	SG	FE
テクノロジ系	基礎理論	基礎理論	離散数学	■	／	■
			応用数学	■	／	■
			情報に関する理論	■	／	■
			通信に関する理論	／	／	■
			計測・制御に関する理論	／	／	■
		アルゴリズムとプログラミング	データ構造	■	／	■
			アルゴリズムとプログラミング	■	／	■
			プログラム言語	■	／	■
			その他の言語	■	／	■
	コンピュータシステム	コンピュータ構成要素	プロセッサ	■	／	■
			メモリ	■	／	■
			入出力デバイス	■	／	■
			バス	／	／	■
			入出力装置	／	／	■
		システム構成要素	システムの構成	■	■	■
			システムの評価指標	■	■	■
		ソフトウェア	オペレーティングシステム	■	／	■
			ファイルシステム	■	／	■
			オープンソースソフトウェア	■	／	■
			オフィスツール	■	／	／
			開発ツール	／	／	■
			ミドルウェア	／	／	■
			ハードウェア	■	／	■
	技術要素	情報デザイン	情報デザイン	■	／	／
			インターフェイス設計	■	／	／
		ユーザーインターフェイス	ユーザーインタフェイス技術	／	／	■
			UX/UIデザイン	／	／	■
		情報メディア	マルチメディア技術	■	／	■
			マルチメディア応用	■	／	■
		データベース	データベース方式	■	■	■
			データベース設計	■	■	■
			データ操作	■	■	■
			トランザクション処理	■	■	■
			データベース応用	／	■	■
		ネットワーク	ネットワーク方式	■	■	■
			通信プロトコル	■	■	■
			ネットワーク応用	■	■	■
			データ通信と制御	／	■	■
			ネットワーク管理	／	■	■
		セキュリティ	情報セキュリティ	■	■	■
			情報セキュリティ管理	■	■	■
			情報セキュリティ対策・情報セキュリティ実装技術	■	■	■
			セキュリティ技術評価	／	■	■
	開発技術	システム開発技術	システム開発技術（IP：マネジメント系に分類）	■	／	／
			システム要件定義・ソフトウェア要件定義	／	／	■
			設計	／	／	■
			実装・構築	／	／	■
			統合・テスト	／	／	■
			導入・受入れ支援	／	／	■
			保守・廃棄	／	／	■
		ソフトウェア開発管理技術	開発プロセス・手法（IP：マネジメント系に分類）	■	／	■
			知的財産権適用管理	／	／	■
			開発環境管理	／	／	■
			構成管理・変更管理	／	／	■
マネジメント系	プロジェクトマネジメント	プロジェクトマネジメント	プロジェクトマネジメント	■	■	■
			プロジェクトの統合	／	■	■
			プロジェクトのステークホルダ	／	■	■
			プロジェクトのスコープ	／	■	■
			プロジェクトの資源	／	■	■
			プロジェクトの時間	／	■	■
			プロジェクトのコスト	／	■	■
			プロジェクトのリスク	／	■	■
			プロジェクトの品質	／	■	■
			プロジェクトの調達	／	■	■
			プロジェクトのコミュニケーション	／	■	■
	サービスマネジメント	サービスマネジメント	サービスマネジメント	■	■	■
			サービスマネジメントシステム／計画・運用	■	■	■
			ファシリティマネジメント	■	■	■
			パフォーマンス評価と改善	／	■	■
			サービスの運用	／	■	■
		システム監査	システム監査	■	■	■
			内部統制	■	■	■
ストラテジー系	システム戦略	システム戦略	情報システム戦略	■	■	■
			業務プロセス	■	■	■
			ソリューションビジネス	■	■	■
			システム活用促進・評価	■	■	■
			システム化計画	■	■	■
			要件定義	■	■	■
			調達計画・実施	■	■	■
	経営戦略	経営戦略マネジメント	経営戦略手法	■	／	■
			マーケティング	■	／	■
			ビジネス戦略と目標・評価	■	／	■
			経営管理システム	■	／	■
			技術開発戦略の立案・技術開発計画	■	／	■
		ビジネスインダストリ	ビジネスシステム	■	／	■
			エンジニアリングシステム	■	／	■
			e-ビジネス	■	／	■
			IoT システム・組込みシステム	■	／	／
			民生機器	／	／	■
			産業機器	／	／	■
	企業と法務	企業活動	経営・組織論	■	■	■
			会計・財務	■	■	■
			業務分析・データ利活用	■	■	■
		法務	知的財産権	■	■	■
			セキュリティ関連法規	■	■	■
			労働関連・取引関連法規	■	■	■
			その他の法律・ガイドライン・情報倫理	■	■	■
			標準化関連	■	■	■