

関西大学のシラバスから見る情報セキュリティ教育の在り方

著者	河野 和宏
雑誌名	関西大学インフォメーションテクノロジーセンター年報 : ITセンター年報
巻	4
ページ	3-15
発行年	2014-07-01
URL	http://hdl.handle.net/10112/00018823

関西大学のシラバスから見る情報セキュリティ教育の在り方

社会安全学部 河野和宏

1. はじめに

情報機器の高性能化・小型化・低価格化やインターネットの普及により、人々の日常生活においても様々な情報機器が使用され、かつインターネットを通して多種多様なサービスが受けられるようになった。特に、多くの一般人がスマートフォン端末に代表されるモバイル端末を1台以上所有し、これらの端末を常に持ち運ぶようになったことに加え、公共空間でのWi-Fi環境の整備やモバイルルータの普及により屋外のどの場面でもインターネットに接続できるようになった影響は大きく、従来の屋内利用を想定して利用・提供していた情報機器・サービスの環境を大きく変化させることとなった。

例えば、電車等の移動時間や待ち時間に行うことが多い読書一つをとっても、以前までは単行本等の書籍を持ち歩き、それらを読んでいることがほとんどであったが、現在はタブレット端末（もしくはスマートフォン端末）に保存してあるデジタル書籍を読んでいる場面が頻繁に見られるようになった。また、どこにいても所有のモバイル端末をインターネットに接続できるという現代の特徴を活用し、自身がその時に考えたこと・感じたことやその時に撮影した写真等をすぐに投稿し、ほとんどリアルタイムでコミュニケーションを取ることができるマイクロブログサービスのよう、常にインターネットに接続できることを前提としたオンラインサービスがインターネット上で新たに展開されるサービスの主流になりつつある。身近にある情報機器の観点から見ても、扱いに慣れるまで時間がかかる大型のデスクトップパソコンや、パソコンと比較すると性能不足の携帯電話端末から、パソコンとほぼ変わらない性能を有しながら小型であり、かつタッチパネルによる感覚的な操作により、素人でもすぐに扱えるスマートフォン端末・タブレット端末へと変化している。

しかしながら、これらの情報機器・インターネットの目覚ましい普及および発展に対し、それらを利用する上でより一層必要とされる情報セキュリティに対する意識は十分に向上していない現状がある。インターネットでの発信が全世界に向けての発信ということを認識しておらず、Twitter等のマイクロブログでの不用意な書き込みにより発生する情報漏洩や炎上事件は、その最たる例であり、2014年現在でも後を絶たない。インターネットの特性自体は以前から何も変わっていないにもかかわらず、近年になって注目されるほど数多く発生しているのは、誰もが手軽に扱え、種々のインターネットサービスを利用できるスマートフォ

ン端末の普及により、ユーザーが利便性の側面しか捉えず、セキュリティについて何も考えずに行動してしまった結果といえよう。さらに、大学等の公共空間に設置されているデジタル複合機を介した情報漏洩のように、高機能な情報機器やクラウドサービスが利用される結果、ユーザ・管理者双方に知識不足・認識不足が発生し、適切に管理することができず、結果、セキュリティインシデントが発生している点からも、セキュリティに対して未成熟であるといえる。

ここで、人々のセキュリティに対する意識が未だ十分に高くないことをデータから示すために、情報セキュリティインシデントのうち、8割を占める情報漏洩・紛失に焦点を絞って話を進める^[1]。日本ネットワークセキュリティ協会（JNSA）が2003年からインターネット上にて公表している情報セキュリティインシデントに関する調査報告書^[2]によると、2008年以降は毎年1,500件近くの情報漏洩事件が発生していることがわかる。ここで、この件数は、あくまで対外的に公表された事件の件数であることから氷山の一角と考えられ、実際はもっと多いと予想される。漏洩事件にはならなかったヒヤリハットの事例も考慮すると、日常では数えきれないほどのインシデントもしくはインシデントになる一歩手前の状況が発生していると想定される。

さらに、2008年以降の報告書の内容を比較検討すると、情報漏洩の8割が誤操作や管理ミス等の人的要因により発生している点、インターネット経由ではなく、技術的対策が取りにくい紙媒体からの漏洩が約7割を占めている点がわかる^[3]。これはつまり、技術的な対策不足というより、人的要因という、日頃からのセキュリティに対する意識の低さがそのまま情報漏洩に直結していることを示している。

以上のことから、現在の環境においては、数多くの情報セキュリティインシデントもしくは一歩手前の状況が発生しており、それらの多くはセキュリティに対する人々の意識の低さから発生しているといえる。それでは、なぜ人々はセキュリティ意識が低いままなのであるのか。我々はこの原因の一つとして、大学までの学生時代における情報セキュリティ教育の在り方に課題があると推察する。セキュリティインシデントを発生させてからでは遅いため、スマートフォン端末等の情報端末が既に身近にある高校生・大学生の時からセキュリティについての十分な知識や対策を身につける必要があるものの、高校で行われる情報科目のみでは十分なセキュリティ教育がなされているとはいえない^[3]。加えて、情報科目は1年間での学習であり、かつ大学進学には直接関係がないため、定期的な教育も難しい。大学にいたっては、学習指導要領のような統一された基準もなく、専門的な知識を学ぶということもあり、大学もしくは学部のみで考えても独特のカリキュラムが編成されているため、日本の大学全体としてどのような情報セキュリティ教育がなされているか、そもそも誰も把握できていないという根本的な問題がある^[4]。

そこで本稿では、大学での情報セキュリティ教育がどのように行われているか明らかにするため、まずは総合大学である関西大学を例に調査し、大学での情報セキュリティ教育の在

り方の一端を示す。具体的には、筆者が所属する社会安全学部における情報教育・セキュリティ教育に関する講義内容を紹介した後、関西大学が公開しているシラバス^[5]をもとに、各学部にも所属する学生がどのような情報教育・情報セキュリティ教育を受けているか明らかにする。さらに、文系学部・理系学部や年度といった視点から教育の違いを論究する。なお、学生全体に対する情報セキュリティ教育の実施内容を検証するという観点から、ITを専門とする部署である関西大学インフォメーションテクノロジーセンター（ITセンター）が行う単独の講習会は対象とはしないこととする。

2. 社会安全学部での情報教育・情報セキュリティ教育

筆者は工学部の出身ということもあり、所属する関西大学社会安全学部では、ITに関する講義の一部を担当している。そこで、2014年度に担当する2つの科目の内容から、社会安全学部ではIT全般に対してどのように教育しているかを述べる。

2.1. ITの利活用を目的とした科目

社会安全学部ではITの利活用を目的とし、実際にパソコンを用いてスキルを上達させる実習科目が複数用意されている。2014年度以降の入学生においては、1年次向けで全員必須の実習科目である「IT実習」、2年次向けでより高度なスキルを身につけることができる実習科目である「GIS実習」「統計データ解析実習Ⅰ・Ⅱ」等、複数の選択実習科目が用意されているが、本節では、パソコンを扱う上で最も基本的なスキルを学ぶことができる「IT実習」について、シラバスを参考にしながら説明する。なお、2014年度からカリキュラムが一部変更されており、2013年度以前までの入学生に対しては、「IT基礎実習Ⅰ」、「IT基礎実習Ⅱ」、「IT活用実習Ⅰ」、「IT活用実習Ⅱ」という4つの必須の実習科目が用意されており、受講生は2年間を通して文書作成・データ処理から、専用のソフトを利用したデータベースの構築や統計処理の技術を修得していくこととなっている。

1年次向けの科目「IT実習」は、パソコン・インターネット等を活用して、文書作成、プレゼンテーション、コミュニケーション、データ整理・分析、情報検索などの日常的な作業を行うスキルを身につけることを目的とした実習科目である。本実習科目の目標は次の通りである。

- Microsoft Wordの基本操作ができるようになる。
- Microsoft PowerPointの基本操作ができるようになる。
- Microsoft Excelの基本操作ができるようになる。
- 情報セキュリティや情報倫理、情報検索に関する基礎的知識を修得する。

上記の到達目標を達成するため、表1に示す計15回の内容を、3時間かけて（つまり1限・2限続けて）実施している。また、担当教員だけでは受講者全員に対してきめ細かな指導は難しいため、指導者側一人あたりの学生数が20人になるよう、TA・SAが配属されている。

表1 実習科目「IT 実習」の講義概要（関西大学シラバス^[5]を参考に作成）。

回	講義概要
1	コンピュータの基本操作、インフォメーションシステム、学内 IT 関連サービスの紹介、e-Learning システム CEAS
2	ファイル・フォルダの扱い方、電子メール
3	タイピングの基礎（Word の利用も可）
4	Word の利用（1. 文書作成の基本操作、文書の装飾）
5	Word の利用（2. 図・表の挿入、段組み文書の作成）
6	PowerPoint の利用（1. スライド作成の基本操作）
7	PowerPoint の利用（2. 図形描画とスライドショー）
8	Word の利用（3. 複雑なレイアウト文書の作成）
9	Word の利用（4. Word の便利な機能）、情報セキュリティと情報倫理、情報検索
10	Excel の利用（1. データの入力方法、表の編集・レイアウト）
11	Excel の利用（2. レイアウト、数式の入力、基本的な関数の利用 1）
12	Excel の利用（3. 基本的な関数の利用 2、グラフの作成 1）
13	Excel の利用（4. グラフの作成 2）
14	Word の利用（5. 論文作成法）
15	小テスト（Word, Excel）

IT 実習の進め方としては、担当教員は、関西大学の e-Learning システムである CEAS を用いて、予め全ての資料を公開した後、その配布資料に基づいてパソコンやソフトの各機能を説明し、実際に操作する。教員の画面は、机の中央に置かれている提示用モニタに映しだされているため、受講生はモニタを見て確認し、自分で実際に操作して機能や操作方法を覚えた後、与えられた幾つかの課題をこなすことになる。

与えられた課題は CEAS のレポート機能を用いて提出するが、全ての課題は実習時間内で提出することが原則となっている。これは、他の講義科目・実習科目と異なり、1 回あたり 3 時間という長時間の実習であることから、実習時間内で内容を全て理解することを想定しているためである。そのため、教員による説明や課題において理解できない点があれば、教員・TA・SA が個別に対応し、全員が同じ分量の課題を達成できるよう、進み具合を確認しながら実習を進めている。反対に、課題を早めに終わらせた学生に対しては、追加課題を用意し、残りの実習時間も有意義な時間になるよう、配慮している。

さらに、本実習の終了後、受講生には Active! Mail による「ふりかえりメール」の提出を義務付けている。受講生は、①実習で学習した内容、②実習を受けての質問、③理解しているかどうかを確認するために出題される簡単な問題に対する回答、の 3 つの内容をメールで担当教員まで送信する。担当教員はそのメールを受けて、質問や不正解の回答に対してコメントを付けて返信することにより、学生に必要な情報をフィードバックしている。なお、CEAS の機能を用いても、ふりかえりメールと同様の仕組みをとることができるが、メールで提出させる他の目的として、定期的にメールを送ることにより、社会で「メールを書く」ということはどういうことか理解させ、友達同士でのメールのやり取りには通常存在しない、「相手の名前を書く」「自分の名前を名乗る」等の、一般的なメールのマナーを習慣づけるという目

的もある。

IT 実習の内容を検討すると、ほとんどの時間を IT の利活用に割いており、セキュリティに関する内容は、第9回目の2時間目のみで、ほとんど触れていない状況である。これは、本実習の目的が IT の利活用であることから、仕方がない面があるものの、内容についても、ウイルスやワンクリック詐欺がどのようなものか等、知識の学習となっており、実際の対策に結びついていない可能性がある。また、一般的なりスクの説明となっていることから、大学生も含め、近年の若者が利用しているスマートフォン端末や、Twitter に代表されるマイクロブログサービス等に対するリスクについては説明不足となっている点も否めない。限られた時間内では全てを説明することはできないこと、IT 実習はパソコン・ソフト等の利活用を目的としていることから、例えば Twitter からの情報漏洩や炎上事件等、実際に同年代の大学生が発生させたセキュリティインシデントを説明することにより、利用している情報端末（パソコン・スマートフォン）やサービスに対するリスクを認識させ、最低限必要となる対策を各自が講じることができるよう、本年度から内容を一部変更する予定である。

2.2. 情報セキュリティの理解を目的した科目

社会安全学部において、筆者は学部向けの講義科目「情報セキュリティ論」を担当している。本講義科目では、情報セキュリティの基本的な考え方から始まり、情報に対するリスク（脅威）、そのリスクから情報を保護するための基本技術から応用技術等を、実際のシステムや対策を踏まえながら幅広く説明し、「情報を守る」とは一体どういうことか、正しく理解することを目的としている。その目的を踏まえ、本講義科目の目標は次の通りとしている。

- 一般的に使われている情報セキュリティ技術の内容を正しく理解する。

表2 講義科目「情報セキュリティ論」の概要（関西大学シラバス^[5]を参考に作成）。

回	講義概要
1	ガイダンス（情報セキュリティ概論、現代社会の危険性とその実例）
2	情報セキュリティの考え方
3	情報資産に対する脅威①
4	情報資産に対する脅威②
5	情報漏洩の原因及び対策
6	情報セキュリティマネジメントシステム（ISMS）
7	演習：暗号解読を通じたクラッキング体験
8	暗号・署名①：共通鍵暗号
9	暗号・署名②：公開鍵暗号
10	暗号・署名③：デジタル署名
11	ファイアウォール・ルータ・アンチウイルス
12	アクセス制御・認証
13	可用性に対する対策・実用面での対策・その他のセキュリティ対策
14	情報セキュリティの法律
15	体験：実際のセキュリティ技術

- ・日常生活において必要となるセキュリティやリテラシー（知識や能力）を習得する。

以上の目標を達成するため、表2に示す通り、情報セキュリティ全般の内容が理解できる講義内容としつつ、第7回目の講義や第15回目の講義のように、情報セキュリティ技術をより深く理解するための演習・体験を取り入れている。また、本講義科目での学習内容を今後活かすために、ITパスポート試験を含めた、情報処理技術者試験の受験を推奨しており、取り組む学生は多くはないものの、実際に取得している学生も存在する。

IT実習と大きく異なる点は、講義を聴くことにより、情報の保護という観点から必要となる知識を習得する点、多くの講義科目と同様、時間外学習が必要となる点である。本講義の特性上、インターネットの仕組み等の、情報を扱う上で必須となる知識が求められるため、IPアドレスやポート番号等の言葉を知らない等、基礎知識が不足している学生には、あらかじめ事前学習を求めている。また、情報セキュリティ全般を取り扱うことから、講義の分量も多く、第8回から第10回にかけて行われる暗号技術に関する講義にいたっては、数学的な思考力も要求されるため、正確に理解するためには相応の事後学習が要求される。

また、本講義の特徴として、講義内容を暗記する、単なる暗記学習ではなく、学習した内容を実際の対策にも繋げることができるよう、幾つかの工夫を施している。例えば、講義内での閑話休題として、最近発生したセキュリティインシデントを紹介し、発生した背景からその原因、および対策まで、講義内容と絡めて説明したり、第1節で言及したとおり、近年のセキュリティインシデントの多くは情報漏洩であり、その要因は誤操作・管理ミス等に代表される人的要因であることを第5回講義で時間をかけて説明したりすることにより、現実のセキュリティインシデントに対応できるよう講義している。

3. 関西大学のシラバスからみる情報セキュリティ教育の現状と課題

本節では、関西大学で公開されている2013年度のシラバスをもとに、所属する大学生に対してどのような情報セキュリティ教育を実施しているかを調査する。関西大学には、文系学部・理系学部合わせて13学部から構成される総合大学であるため、文系学部（法学部、文学部、経済学部、商学部、社会学部、外国語学部、政策創造学部、人間健康学部、社会安全学部）、理系学部（システム理工学部4学科、環境都市工学部3学科、化学生命工学部2学科、総合情報学部）の大きく2つに学部を分類して検証する¹。さらに、10年前の2003年度における実施状況も調査することにより、時代の変化に応じて、どのように情報リテラシー教育・情報セキュリティ教育が変化したかを検証する。

なお、関西大学では総合大学である特色を活かし、学部間の枠を超えて学生が受講可能な共通教養科目が提供されている。共通教養科目では、一部の学部を除き、自身が興味を持つ科目を受講することにより、学部内だけでは習得できない様々な知識を取得することができ

1 本節で述べる内容の一部は、文献[6]にて報告済みの内容であるが、改めて本稿にて報告する。

る。共通教養科目を調査したところ、情報リテラシーの能力を向上させる科目、情報技術・ネットワーク技術について学習する科目、SNS やマイクロブログ等も含めたメディアリテラシーを学ぶ科目が合わせて 5 科目存在するが、これらは学部が提供する講義科目ではなく、200 以上もある共通教養科目から学生が自由に選択することから、対象外とする。

3.1. 文系学部における情報リテラシー教育・情報セキュリティ教育の現状

各文系学部で提供されている情報リテラシーおよび情報セキュリティに関する科目の実施状況をまとめた結果を表 3 に示す。なお、表 3 において、「学部」は学部名を、「PC 利用の実習科目」は情報の利活用のためにパソコン・ソフトを利用する実習科目があるかどうかを、「セキュリティに関する内容（実習科目）」はセキュリティに関する何らかの内容が実習内であるかどうかを、「情報に関する講義科目」はパソコンやインターネット等を含め、情報に関連した講義があるかどうかを、「セキュリティに関する内容（講義科目）」は、前述の講義科目において何らかのセキュリティに関する内容を講義しているかどうかを表す。さらに、「情報セキュリティを対象とした科目」は、情報の保護を目的とし、情報セキュリティ自体を対象とした講義科目が存在するかどうかを表す（この科目と判断した場合は、「情報に関する講義科目」には含めないものとする）。各項目における有無は、「○」「×」で表し、判断が難しい一部の科目・内容については、「△」で表す。なお、シラバスの内容で判断しているため、各実習科目、講義科目において、実際にセキュリティに関する内容を扱っているかどうかは調査の対象外としている。

表 3 より、ほとんどの文系学部において、パソコンおよびソフトを活用する実習が実施されている（9 学部のうち 8 学部）ことがわかるが、多くの実習科目では、Microsoft Word や Excel に代表される、オフィスソフトを用いた文書作成・データ処理等の、利活用に重点が置かれており、セキュリティ対策について、シラバス上では触れられていない場合も見ら

表 3 関西大学の文系学部における情報に関する実習科目・講義科目の実施状況。

学 部	PC 利用の実習科目	セキュリティに関する内容 (実習科目)	情報に関する講義科目	セキュリティに関する内容 (講義科目)	情報セキュリティを対象とした科目
法 学 部	○	×	○	○	×
文 学 部	○	○	○	○	×
経 済 学 部	○	○	△	×	×
商 学 部	○	○	○	○	×
社 会 学 部	○	×	○	○	×
外 国 語 学 部	○	○	×	×	×
政策創造学部	○	×	×	×	×
人間健康学部	× ^[注1]	×	×	×	×
社会安全学部	○	○	△	△	○

[注 1] 人間健康学部では、共通教養科目の「基礎からの情報処理」が実習科目に相当すると考えられるが、本文中にある通り、共通教養科目のため対象から外している。

れた。また、実習内で実施されているセキュリティ対策の内容についても、ネチケット等の簡単な内容であることがほとんどであり、情報セキュリティに関する具体的な内容の記載は見られなかった。これは、第2節で述べた通り、実習の目的がITの利活用であり、かつ時間の制約があることから、具体的な内容まで含めることは極めて難しいためといえる。

文系学部間での違いを考察すると、表3から、情報に関する講義科目を開講する・しないで大まかに分類することもできるが、これらの開講する実習科目・講義科目の内容をより精査すると、データベースシステムの構築やHTMLによるホームページ作成、データ分析等の、選択実習科目をより多く提供し、パソコン・ソフトを利用した情報の利活用能力を向上させようとしているのか、反対に倫理や法律、ネットワークやメディアに関する講義を通して情報全般に対する教育を提供し、間接的に情報セキュリティに必要な知識を習得させようとしているのか等、情報リテラシー教育・情報セキュリティ教育の方針の違いを明確に確認することができた。特に、後者の場合、例えば情報ネットワークに関する講義科目の一つの講義内容として、情報セキュリティの一大テーマである暗号や認証を取り扱う等、情報セキュリティに関する何らかの内容を教えているケースが多く見られた。

情報セキュリティ全般を体系立てて取り扱う講義に関しては、一学部を除いて存在していない。これは、文系学部という性質上、理系の側面が強い情報セキュリティに関する内容を担当できる教員が少ないこと、加えて、先程述べたとおり、情報の利活用に重点をおくか、情報を扱う科目内における一つのテーマとして、情報セキュリティの一部を扱うかのどちらかの方針に従って教育しているためと推測される。

3.2. 理系学部における情報リテラシー教育・情報セキュリティ教育の現状

各理系学部で提供されている情報リテラシーおよび情報セキュリティに関する科目の実施状況をまとめた結果を表3に示す。なお、表3と同様、表4において、「学部・学科」は学部名および学科名を、「PC利用の実習科目」は情報の利活用のためにパソコン・ソフトを利用する実習科目があるかどうかを、「セキュリティに関する内容（実習科目）」はセキュリティに関する何らかの内容が実習内であるかどうかを、「情報に関する講義科目」はパソコンやインターネット等を含め、情報に関連した講義があるかどうかを、「セキュリティに関する内容（講義科目）」は、前述の講義科目において何らかのセキュリティに関する内容を講義しているかどうかを表す。さらに、「情報セキュリティを対象とした科目」は、情報の保護を目的とし、情報セキュリティ自体を対象とした講義科目が存在するかどうかを表す（この科目と判断した場合は、「情報に関する講義科目」には含めないものとする）。各項目における有無は、「○」「×」で表す。

表4より、全ての理系学部において、パソコンおよびソフトを利用した実習を実施していることがわかるが、文系学部と同様、利活用に重点が置かれており、セキュリティに関する内容は半数の学部で含まれておらず（10学部・学科中、5学部・学科が実施）、文系学部

表4 関西大学の理系学部における情報に関する実習科目・講義科目の実施状況。

学部・学科	PC 利用の 実習科目	セキュリティ に関する内容 (実習科目)	情報に関する 講義科目	セキュリティ に関する内容 (講義科目)	情報セキュリ ティを対象と した科目
システム理工学部 数学科	○	○	○	○	○
システム理工学部 物理・応用物理学	○	×	×	×	×
システム理工学部 機械工学科	○	×	○	×	×
システム理工学部 電気電子情報工学科	○	○	○	○	○
環境都市工学部 建築学科	○	×	×	×	×
環境都市工学部 都市システム工学科	○	○	○	○	×
環境都市工学部 エネルギー・環境工学科	○	×	×	×	×
化学生命工学部 化学・物質工学科	○	○	×	×	×
化学生命工学部 生命・生物工学科	○	×	×	×	×
総合情報学部	○	○	○	○	○

以上に実施されていないことがわかる。これは、文系学部で行われる実習科目では、情報リテラシー能力の向上を目的としてインターネットやメールの利用に関する内容を実施しており、その実習中において、情報倫理やネチケット、マナー等、情報セキュリティに関する内容を扱っていたが、理系学部（工学部）の実習科目では、「モノ・ソフトを作る」という工学部の性質から、プログラミングの習得やアルゴリズムの理解・構築、シミュレーションを目的としている場合が多く、一般の情報リテラシー能力を向上させる実習とは異なるためである。

さらに、表4より、情報に関する学部・学科を除けば、多くの学部・学科において、シラバス上では情報セキュリティに関連した講義・演習科目を提供していないことがわかる。この理由として工学系の学部においては、カリキュラムがそれぞれの学部・学科の内容に特化しており、内容も極めて専門性が高くなるためであると考えられる。反対に、総合情報学部のように、情報を専門に扱う学部・学科においては、情報セキュリティだけでなく、情報全般に関して多岐にわたる実習・講義科目を提供しているといえる。

3.3. 過去における情報セキュリティ教育の実施状況

前節までは学部ごとの違い、特に文系学部、理系学部の違いにより、情報教育・情報セキュリティ教育に違いがあるかどうかを調査したが、本節では、約10年前である2003年度の提供科目をもとに、当時の情報教育・情報セキュリティ教育を把握し、現在の教育と比較検討する。調査方法としては、現時点では関西大学で公開されているシラバスシステムを元に、以前の講義科目や内容を検索することも可能であるが、利用するデータベースが最新年度に

表5 2003年度における関西大学での情報に関する実習科目・講義科目の実施状況。

学部	PC 利用の 実習科目	情報に関する 講義科目	情報セキュリティを 対象とした科目
法学部・法律学科	○	○	×
法学部・政治学科	○	○	×
文学部	—	—	—
経済学部	○	△	×
商学部	○	△	×
社会学部	○	○	×
工学部・機械工学科	○	△	×
工学部・機械システム工学科	○	△	×
工学部・電気工学科	○	○	×
工学部・電子工学科	○	○	×
工学部・化学工学科	○	×	×
工学部・応用化学科	○	×	×
工学部・先端マテリアル工学科	○	×	×
工学部・システムマネジメント工学科	○	○	×
工学部・都市環境工学科	△	×	×
工学部・建築学科	○	△	×
工学部・生物工学科	○	×	×
総合情報学部	○	○	△

に基づいて検索しているため、正確ではない。そこで、過去のインターネット上のホームページを保存してあるサービス「Internet Archive」^[7]を参考にしながら、提供科目を調査する。

2003年度の入学生に対して各学部で提供されている情報リテラシーおよび情報セキュリティに関する科目の実施状況をまとめた結果を表5に示す。表5における項目は、パソコン等を利用する実習科目があるかどうか、情報に関する講義科目があるかどうか、およびセキュリティ全般を体系的に取り扱う科目があるかどうか、という3つであり、各項目における有無は、「○」「×」で表し、判断が難しい科目がある場合には「△」で表す。なお、表3および表4にある、各実習科目・講義科目の内容にセキュリティに関する内容を扱っているかどうかの項目は、表5には存在しない。これは、今回の調査では2003年時点で公開されていた各学部のホームページに記載されているカリキュラムを参考にしているが、具体的な講義・実習内容は記載されておらず、関西大学のシラバスシステムにおいても、先程述べたとおり、利用するデータベースが最新年度に基づいているため、2003年時点での各学部でのカリキュラムは検索可能でも、検索した結果得られる各科目の講義・実習内容は最新年度のものとなっており、2003年におけるシラバスの内容を確認することができないためである。また、文学部においては、専門科目のうち必修科目しか掲載されておらず、選択科目が不明であったため、対象外としている。

表5のうち、法学部から社会学部までは文系学部であり、工学部、総合情報学部は、理系学部であるが、表3および表4と比較すると、情報教育自体は10年前であっても同じ傾向で

あり、PC を利用した実習はどの学部でも実施されていることがわかる。実施内容についても、実習名が2013年度と大きく変わっていないことから、内容自体も大きく変わっておらず、文系学部での実習は基本的にはインターネットおよびオフィスソフトの利用方法等の一般的な情報リテラシー能力の向上を目的とした実習科目であり、理系学部はそれらに加えて、プログラミングの習得等を目的とした実習科目であると推測される。

具体的な実習内容・講義内容がわからず、単純な比較は難しいが、注目すべき点は、2003年時点では、情報セキュリティ全体を取り扱う講義科目は存在していないという点である。総合情報学部においても、2003年度から現在まで「情報と倫理」という講義科目が提供されていることは確認できたが、2013年度に開講されている「情報セキュリティ論」という、情報セキュリティ自体を取り扱った講義科目は、科目名称を見る限り存在していない（前者の講義があるため、表5中では「△」表示としている）。そのため、10年前においては、現在以上に情報の利活用のための知識の習得やスキルアップに焦点が当てられていたのではないかと推察される。

3.4. シラバスの比較から見える情報セキュリティ教育の課題

以上までの調査結果を元に、情報教育・情報セキュリティ教育の現状の課題をまとめ、今後、どのように情報セキュリティ教育があるべきかを検討する。

文系学部・理系学部共通して言えることは、情報の利活用や情報処理能力のスキルアップに焦点が当てられており、情報の保護という観点はさほど重要視されていないということである。情報セキュリティを扱う科目自体は、一般ユーザーにおける実際の対策面のみに限れば、情報セキュリティに関する深い知識は必要ないため必須ではないものの、情報の利活用を推し進めるのであれば、その前提となる、情報を適切に扱い、保護するための最低限の知識を修得しなければならない。そのため、文系学部においては、ほとんどの学部で採用されている、パソコンやオフィスソフトの利活用を学習する、情報リテラシーに関する実習科目において、ネチケット等以上の、一般ユーザーが近代のリスクに対応可能な情報セキュリティに関する知識およびそれらリスクに対する具体的な対策法を実習内容に含める必要がある。

理系学部についても、同様のことが言えるが、文系学部以上に情報セキュリティに関する教育を実施しておらず、ネチケット等の最も初歩的な内容でさえ、シラバス上では実施されていない場合も見られた。つまり、様々な場面で情報機器を触り、データを扱う機会が多いであろう理系（工学系）学部の学生のセキュリティ対策は個々の意識によるということを示しており、学生間で大きく差が現れる可能性があるといえる。実験データの取扱い等、普段から重要な情報を扱っていることから、全体として、一定水準のセキュリティレベルを保つためにも、文系学部と同様、必修科目として実施されることが多い実習系の科目において、リスクへの具体的対策も含めた情報セキュリティに関する十分な教育を実施すべきであるといえる。

また、第2.1節でも指摘したが、近年は情報機器一つとっても、大学生が身近になっている機器は、パソコンからスマートフォン端末になっており、インターネット環境もクラウド環境へと大きく転換しつつある。そのため、特に学生全員が受講する可能性が高い実習科目で提供する情報セキュリティに関する内容も、その変化に対応していかなくてはならないが、シラバスから読み取ることができる内容では、十分な対応はできていない。実際に、2013年度の実施内容をみても、多くの場合、ネチケット等の内容のため、現代の状況を考慮した内容にはなっていなかった。この問題は、2013年度の内容をそのまま2003年度の内容としても見ても、利用するソフトのバージョンの違いを除けば、特に問題ないということからも、指摘できるであろう。情報機器の発展やインターネット環境・サービスの進展は、日進月歩であり、数年経つと、大幅に変化している可能性が高いことから、情報セキュリティに関する内容については、毎年のマイナーチェンジだけでなく、数年間ごとの大幅なバージョンアップを実施する必要があると結論付ける。

4. おわりに

本稿では、関西大学のカリキュラムから、文系学部・理系学部における情報教育・情報セキュリティ教育の現状を調査し、今後の教育の在り方を検討した。現在の関西大学での情報教育においては、主にPCの利活用による情報活用力の向上に目的があり、情報セキュリティに関する内容はそれほど気を配られていないことを明らかにし、多くの学生が履修する実習系の科目において、少なくとも情報を利用する上で必要となる最低限の知識を習得し、現代の環境に合わせたセキュリティ対策を実施することが可能な実習内容を提供する必要があることを指摘した。本稿からの結果は関西大学に限定しての結果といえるが、筆者の経験上、学生時代においても同様の内容であったことから、おそらくどの大学においても傾向は一緒であると類推され、情報を活用する力だけでなく、その前提となる、情報を適切に扱う力を向上させる必要があるといえる。

なお、本来であれば、これらの教育は、大学だけでなく、高校における教育内容も含めて考慮すべきであるが、高校における情報教育においても、文献^{[6][8]}で指摘している通り、大学と同様、情報の利活用に力を割いていたり、個人情報漏洩に代表される現在のセキュリティインシデントに対応できていなかったりする。高校までは文科省からの学習指導要領に基づいて一定の内容を教えられていることから、大学においては、科目「情報」における情報全般に関する教育内容を確認後、大学で教える内容を精査する等、高校からの教育に連続性を持たせた枠組みを構築することも重要であると考えられる。

最後に、大学および学部におけるカリキュラムの関係上、専門科目内の実習科目・講義科目では時間を割くことが難しい場合や、適切な内容を提供できない場合もあると想定される。その対応の一つとして、今回は調査の対象外としたが、関西大学のITを管理するITセンターにおいては、パソコンの入門講座に始まり、オフィスソフトや画像作成・編集ソフトに対

するリテラシー能力の向上を目的とした講座、さらにはインターネットセキュリティに関する講座も提供しているため、これらの講座の受講を学部として推奨し、受講させることにより、現代のリスクに対応できるだけの最低限の知識を身につけさせることも有効な手段であるといえる。

文 献

- [1] 独立行政法人情報処理推進機構、“情報セキュリティ白書2013、” 2013年9月1日。
- [2] NPO 日本ネットワークセキュリティ協会、“情報セキュリティインシデントに関する調査報告書、” <http://www.jnsa.org/>、2014年2月1日アクセス。
- [3] 河野和宏（分担執筆），“事故防止のための安全学——被害軽減をめざす分析と実践に繋ぐ提言、” 第8章 情報漏洩の事例から考えるセキュリティ対策、関西大学社会安全学部編、ミネルヴァ書房、2013年3月25日。
- [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年。
- [5] 関西大学シラバスシステム、“<http://jmss3.jm.kansai-u.ac.jp/search/SyllabusBridge>、” 2014年2月1日アクセス。
- [6] 河野和宏、“高等教育機関における情報セキュリティ教育に関する一検討、” 2014年暗号と情報セキュリティシンポジウム（SCIS2014）、2B1-4、6ページ、2014。
- [7] Internet Archive、“<http://archive.org/web/web.php>、” 2014年2月1日アクセス。
- [8] 山根敬登、河野和宏、“教科書「社会と情報」からみる情報セキュリティ教育の現状と問題点、” 電子情報通信学会2014年総合大会、D-15-27、p. 166、2014。