

平成18年度「専修学校教育重点支援プラン」成果報告書

事業名	全国初の四年制情報セキュリティ学科における実践教育プログラム体系の開発と実施		
法人名	学校法人河合塾学園		
学校名	トライデントコンピュータ専門学校		
代表者	理事長 河合 弘 登	担当者 連絡先	桜井 裕治(さくらい ゆうじ) TEL:052-735-1605

1. 事業の概要

セキュリティ技術を専門に学ぶ全国初の四年制学科「情報セキュリティ学科」を基本想定とする、実践的な教育プログラムの開発と実証を行った。また、高度セキュリティ人材に要求される広範囲なセキュリティ技術への対応を図るべく、過去の事業試算の活用・拡充も含めた一連の教育体系を具体化することにより、他の専門学校にも適用可能な完備性・完結性の高いモデル的な教育プログラムとすることを目指した。

本事業では、IT企業やユーザ企業におけるセキュリティ人材の実態に関する情報収集と分析を行うと同時に、実務性の高い、ケーススタディ方式を取り入れたセキュリティ運用・管理スキルを習得するためのテキスト教材の制作を行った。更に、テキスト教材を用いた実験的な授業を行い、内容やレベルなどに関する検証を試みた。

2. 事業の評価に関する項目

①目的・重点事項の達成状況

ITと経営の一体化が急速に進む中、企業にとってセキュリティの確立はますます重要な課題となってきた。セキュリティに対する技術的な脅威の多様化や高度化への対策のみならず、個人情報保護法(2005年)や日本版SOX法(2008年)といった法制面からの要請への対応など、セキュリティをめぐる課題は広範であり、今や企業経営そのものに直結している。

このような状況の中、求められているセキュリティ人材とは、である。例えば、平成18年4月に第一回試験が実施された情報処理技術者試験「テクニカルエンジニア(情報セキュリティ)」の想定人材像や、同月1日に公開された『ITスキル標準version2.0』の職種「ITスペシャリスト(専門分野セキュリティ)」の定義などは、このことを明確に示している。

このようなスキルは実務での経験を踏む中で研鑽されるものであり、四年制学科であっても就職時でこの水準に到達させることは困難である。しかしながら、卒業して数年後の目標人材像としてこれを設定し、そこに到達する上で必要となる基盤知識やスキルを四年間のカリキュラムの中で徹底することは十分に可能であると考えられる。かつ、専門学校教育の高度化—高度人材の輩出に資するという狙いに照らしても、このような取り組みを積極的に行うことの意義は大きいはずである。すなわち、卒業直後に活かせる専門性だけに焦点を当てた教育ではなく、数年後のキャリアアップをも視野に収めた体系的なカリキュラムの具体化と提供である。

本事業では、セキュリティエンジニアリングプロセスを横断的にカバーできるスキルを備えたプロフェッショナル、すなわち、セキュリティ要件の分析やアーキテクチャ設計からセキュリティ機能の設計・開発、運用フェーズにおけるセキュリティ管理の支援までを担い得るスペシャリストを人材像を目標とする教育プログラムの研究開発を行った。教育プログラムを適用する対象は、セキュリティ技術を専門に学ぶ全国初の四年制専門課程である「情報セキュリティ学科」(河合塾学園)を基本想定として内容の具体化を図った。教育プログラムの開発作業の完了後には、その一部分について実験的な授業を実証講座という形式で実施し、人材育成プログラムの有効性や今後の課題などについて検証を加えた。また、他の専門学校でも活用可能な完備性の高い四年制課程のモデル的な教育プログラムを目指し、今後の専門学校におけるセキュリティ(IT)教育の高度化に貢献していくことを目的とした。

②事業により得られた成果

昨年度委託事業(区分「新教育領域の開発」)にて開発したカリキュラムの三学年次での使用を目的とするテキスト教材(学生向けテキスト、講師向け指導マニュアル)を企画・制作した。テキスト教材は全体が三部構成(第一章 セキュリティ運用・管理の基礎、第二章 インシデントレスポンス、第三章 定常的なセキュリティ運用・管理)となっており、セキュリティの基礎知識やセキュリティの要素技術などの基本的なスキルを一通り学習した高学年次の学生を対象とした、セキュリティ運用・管理の実践技術を修得させることを狙いとしたものである。

「第一章 セキュリティ運用・管理の基礎」

前提として今まで学習してきた内容である、セキュリティの基礎やサーバ、ネットワークについて再確認するパートとなっている。

「第二章 インシデントレスポンス」

攻撃手法を再確認した後、ケーススタディを用いた学習を行うパートとなっている。実際にログを見て問題を発見し解決方法を探るなど、より実践的な内容となっている。

「第三章 定常的なセキュリティ運用・管理」

運用・管理していくために必要となるツールについての学習を行う。前章のケーススタディを再活用し、管理ツールや可視化ツールについての理解を深める内容となっている。

また、講師向けマニュアルの企画・制作も行い、ケーススタディ実習環境や各学習項目を指導する上でのポイント、説明のための参考情報などを、学生向けテキスト教材の流れに沿った形でまとめた。

「第一章 環境構築」

実習の概要や環境構築に関する説明を行い、実習前に準備すべき点についてまとめている。

「第二章 実習の解説」

ネットワークの問題、メールサービスの問題、Webサービスの問題、不正侵入について、問題の実行、回答、解決方法について問題ごとにまとめている。

「第三章 IDS導入後の問題発生」

IDS導入環境の確認、IDS導入環境でのインシデントについて説明を行っている。

③今後の活用

本校においては、四年制学科の三年次教材として来年度活用する予定。また、実施協力校においても使用を検討している段階である。また、専門学校にとどまらず、企業の新人研修等にも役立てられるよう、成果報告会出席者に対しても教材を配布した。

④次年度以降における課題・展開

実証講座受講者やオブザーバのアンケート結果からは、本教材の活用にあたっては、教員の確保と実習環境の確保が課題であるとの回答が得られた。また、現在の学科やコースとの整合性についても考える必要があるとの意見もあった。

3. 事業の実施に関する項目

①ニーズ調査等

企業サイドが現在どのようなセキュリティ人材を必要としているのかを具体的かつ詳細なレベルで把握し、その結果を教育プログラムの内容に反映することするために企業におけるセキュリティ人材のニーズ調査を行った。また、開発・運用側のエンジニアが対象となっている情報処理技術者試験新試験区分「テクニカルエンジニア(情報セキュリティ)」に関する情報収集も行った。

企業におけるセキュリティ人材のニーズ調査は、訪問ヒアリング方式(一部郵送アンケート方式)にて、名古屋を中心に、その他各委員の所属校のエリアも候補として行った。回答企業数は15社で、企業の基本情報、人材採用・育成、インターンシップなど、全22問の調査項目とした。本事業でのテーマでもあるセキュリティ運用管理の実践的教育に関する質問では、全ての企業が必要性を感じるとの回答が得られた。

情報処理技術者試験新試験区分「テクニカルエンジニア(情報セキュリティ)」調査は、公的ドキュメント(出題範囲、スキル標準、統計情報など)、過去の出題、一般書籍(対策本、解説書など)、関連Webサイト上の情報などから情報を収集し、整理を行った。

試験内容や傾向、応募者の状況(実績)など、多面的な情報の収集を通して、

- ・ 目標資格(のひとつ)とすることは妥当であろうか
- ・ モデルカリキュラムの構成要素として組み入れることは可能かなどといった考察を行うことを主眼とした。

②テキスト教材の開発

昨年度委託事業(区分「新教育領域の開発」)にて開発したカリキュラムの三学年次での使用を目的とするテキスト教材(学生向けテキスト、講師向け指導マニュアル)を企画・制作した。テキスト教材の内容は、以下に列記するように大きく3つのパートから構成されている。

1) セキュリティ運用・管理の基礎

セキュリティの基礎を振り返り、サーバ運用の管理、情報の必要性、ネットワークの情報、サーバ情報の解析など、かつて学習したことの再確認を行う。

2) インシデントレスポンス

実際に発生しているインシデントから問題を見つけ出し、解決方法を探ることを、ケーススタディを用いてより実践的な学習を行う。

3) 定常的なセキュリティ運用・管理

定常的に運用・管理するために管理ツールや可視化ツールによる運用・管理方法を学習する。ツールを用いて改めてケーススタディに取り組むことで、より一層理解を深める。

本教材は、セキュリティの基礎知識やセキュリティの要素技術などの基本的なスキルを一通り学習した高学年次の学生を対象者に、セキュリティ運用・管理の実践技術を修得させることを狙いとしている。

また、講師向けマニュアルの企画・制作も行い、ケーススタディ実習環境や各学習項目を指導する上でのポイント、説明のための参考情報などを、学生向けテキスト教材の流れに沿った形でまとめた。

1) 環境構築

実習の概要や環境構築に関する説明を行い、実習前に準備すべき点についてまとめている。

2) 実習の解説

ネットワークの問題、メールサービスの問題、Webサービスの問題、不正侵入について、問題の実行、回答、解決方法について問題ごとにまとめている。

3) IDS導入後の問題発生

IDS導入環境の確認、IDS導入環境でのインシデントについて説明を行っている。

③実証講座

実施の狙いは、開発したテキスト教材の内容やレベル・題材の妥当性、テキストの体裁や構成などの評価を行うことである。

開発したテキスト教材は全体が三部構成(第一章 セキュリティ運用・管理の基礎、第二章 インシデントレスポンス、第三章 定常的なセキュリティ運用・管理)となっているが、実証講座ではその中の一部分を取り出す形で実験的な授業を行うこととした。具体的には、テキスト教材の「第二章 インシデントレスポンス」の部分に関する講義とケーススタディ及び「第三章定常的なセキュリティ運用・管理」の講義を行う内容の授業を実施した。

対象は、教える側の視点から評価を行うために、実施委員としてプロジェクトに参加している専門学校教員とした。

受講後、教材のレベルや内容、題材の妥当性などについてアンケートをおこなった。セキュリティの運用管理の実践をテーマとする技術教育の必要性は、受講者全員が「必要である」と感じていた。

④その他

開発したテキスト教材はケーススタディ方式にて制作しており、実際に発生させたインシデントから、自ら問題を発見し解決方法を探るといった、より実践的な構成となっている。環境設定や、指導ポイントについても講師マニュアルにまとめられているので、本校だけではなく、他の専門学校や企業でも活用可能な教材となっている。