

産学協同によるセキュリティ教育の実践と課題

佐々木良一* 松田剛# 伊藤栄二#

*東京電機大学工学部 #株式会社ヒューコム

*〒101-8457 東京都千代田区神田錦町2-2

E-mail sasaki@im.dendai.ac.jp

あらまし インターネットの普及に伴い増大したセキュリティへの脅威の問題を解決するには人材の確保のための情報セキュリティ教育（以下、単にセキュリティ教育と呼ぶ）が不可欠であるが、2003年時点では、外国と比べ大きく劣る状況にあった。そこで、著者らは民間のセキュリティ教育を行っている機関と協力し、社会人と学生を対象とし、セキュリティ教育を行うことにした。本稿では、東京電機大学と、SEA/J (Security Education Alliance) が協力し、社会人と大学院生を対象として2004年度と2005年度に東京電機大学で行ったセキュリティ教育の実践結果と、今後の課題について述べる。

キーワード セキュリティ 教育 セキュリティ技術者 カリキュラム

Practice and Problems of Information Security Education by Industry-University Cooperation

*Ryoichi Sasaki, #Tsuyoshi Matsuda, #Eiji Itoh

*Tokyo Denki University #HUCOM

*Kanda Nisikicho 2-2, Chiyoda-Ku, Tokyo 101-8457, Japan

E-mail: sasaki@im.dendai.ac.jp

Abstract: To solve a problem of threats to the security that increased with the spread of Internet, information security education is becoming essential. However, in the year 2003, the situation was inferior in comparison with foreign countries. Therefore, authors decided to start the education for members of society and university in cooperation with the security education organization and university. This paper deals with the practice and problems on information security education performed in 2004 and 2005 by SEA/J and Tokyo Denki University.

Key words security, education, security engineer, and curriculum

1. はじめに

インターネットの普及に伴い増大したセキュリティへの脅威の問題を解決するには人材の確保のため情報セキュリティ教育（以下、単にセキュリティ教育と呼ぶ）が不可欠である。一口で、セキュリティ教育といっても、教育対象者や教育の実施者によっていろいろなものがあるが、2003年時点では、いずれも外国と比べ大きく劣る状況にあった。

そこで、佐々木は民間のセキュリティ教育を行っている機関と協力し、社会人と学

生を対象とし、セキュリティ教育を行うことにした。本稿では、東京電機大学と、SEA/J (Security Education Alliance) ⁶⁾ が協力し、社会人と大学院生を対象として2004年度から東京電機大学で行ったセキュリティ教育の実践結果と、今後の課題について述べる。

2. セキュリティ教育の状況 ¹⁾⁻³⁾

2. 1 全体的状況

セキュリティ教育は、図1に示すように多様な教育実施者や、教育対象者が存在す

る。教育実施者としては、職場内で行うもののほかに、専門企業や大学が行うものがある。

筆者らは、経済産業省の情報セキュリティ教育研究会で、セキュリティ教育の現状を調査するとともに、CSO (Chief Security Officer) 補佐クラスに必要な、セキュリティ教育のカリキュラムの提言を行った⁵⁾。その調査段階の、2003 年度の時点では、次のようなことがいえた。

(1) 専門企業による教育を見てみると、米国では、RSA 社や CSI、SANS などの民間組織を中心に充実した教育を実施している。一方、日本では、一部で急速に充実しつつあるがまだまだ玉石混交である。

(2) 大学教育についてみてみると、外国に比べて遅れが目立つ。特に、質的には米国、量的には韓国に比べ遅れている。韓国では学部や大学院に「セキュリティ学科」が誕生し、毎年 1000 人規模の卒業生を送り出し始めている。一方、日本では、ようやく 2004 年 4 月に情報セキュリティ大学院大学が 1 校、開校したところである。一般の情報系大学では、セキュリティ教育を実施していない大学の方が多い。

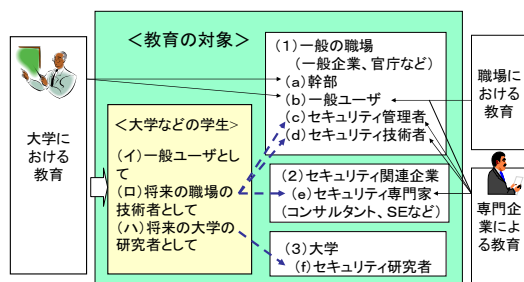


図1 大学および企業における教育

2. 2 東京電機大学の場合³⁾

東京電機大学工学部では、佐々木が赴任した 2001 年よりセキュリティ教育を充実し始めた。その時点において計画したセキュリティに関する講義は次のとおりであった。

(1) 「情報倫理」工学部 1 年-4 年向け (2001 年度より実施)。ユーザ教育用。
(2) 「コンピューティング基盤とセキュリティ」工学部情報メディア学科 4 年生 (2005 年度より実施)。将来の企業内のセ

キュリティ技術者向け。

(3) 「ネットワークセキュリティ特論」工学部大学院修士過程 1 年-2 年 (2001 年度より実施)。将来の企業内のセキュリティ技術者向けおよび将来の大学研究者向け。

大学院についていうと、上記のような 1 講座だけでは、将来の企業内のセキュリティ技術者向けにも、将来の大学研究者向けにも不十分であるという思いが強かった。

3. 産学協同による教育の必要性

上記のような思いと、日本におけるセキュリティ教育の遅れを何とかしたいという思いから、2002 年ごろより大学院教育の充実化に向けた計画を立て始めた。

まず、セキュリティ教育として教えるべき項目の検討を行ったが、その範囲はきわめて広い。それは、対象者によって異なってくるが、全体では図 2 に示すようになるだろうと考えた。

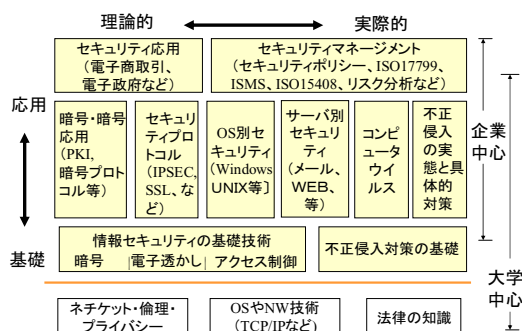


図2 セキュリティ教育の分野

そして、大学院における教育の形態や内容を決定するにあたっては、次のようなことを考えた。

(1) 大学院における教育は、(a) 将来の技術者になるために、直接的に役に立つと共に、(b) 大学でなければならない基礎からの積み重ねを必要とする物にも重点をおく事が必要である。

(2) 役に立つという意味においては、(a) ウイルス対策 (b) 不正侵入の実態と対策 (c) セキュリティプロトコル (d) セキュリティマネジメントなどが必要になる。

(3) 基礎からの積み重ねを必要とするという意味においては、(a) セキュリティ技術の基礎 (暗号技術、電子透かし技術な

ど)や(b)暗号応用技術(電子署名・暗号プロトコルなど)が必要である。

(4)役に立つためには実習・実技形式が不可欠となるが、実習・実技まで含めると、教育の範囲が広く一人の教員での対応は非常に困難である。

(5)一方、大学には社会人の再教育という使命もある。特に、基礎からの積み重ねを必要とする項目については、民間の教育機関だけでは不十分であると考えられる。セキュリティ分野においては、上述したように暗号や電子すかし技術など基礎からの積み重ねを必要とする部分は多い。

(6)そこで、大学が強い分野においては大学の先生が教え、企業が強い分野については企業の技術者が教えることとし、大学院生とともに社会人も教育の対象とすべきであると考えた。

すなわち、産学協同によるセキュリティ教育の実施である。

ここで、社会人もいろいろな人がいるが、将来、セキュリティ管理者として活躍できる人で、その基本技術を習得したい人を想定した。

図2を眺めつつ、教えるべき内容と、それに必要とする時間の検討を行い、最低、3コース必要であり、講義1を「暗号技術とその応用」、講義2を「ネットワークのセキュリティ」、講義3を「不正侵入対策の実際」とするのがよいだろうと思い至った。

4. 産学協同による教育の実践

4. 1 教育開始までの経緯³⁾

このあたりの基本構想は、2003年の2月ごろまでに順調に固まっていた。

このような構想を、2003年の初夏に、SEA/Jの理事長であり、株式会社ヒューコム⁷⁾の社長である井上陽一氏にお話したところ積極的に協力したいというお申し出があった。

この時点から、SEA/J側からヒューコムの宇都孝久氏(故人)なども参加し検討を行い、講義1を大学側が中心になり、講義2と3をSEA/Jが中心になってやることで合意が得られた。その後、一緒に細部を詰めることで、計画が加速した。

その後、佐々木と、蓮尾氏に、経営企画室の田丸健一郎氏を加えた東京電機大学側

のメンバーと、宇都氏、持田啓司氏(大塚商会)、松田のSEA/Jのメンバーがプロジェクトを組み、開講のための準備を進めていった。相談の結果、まず、2004年度と2005年度に実施することとし、各講義の募集人員と受講費用は、表1に示すとおりとした。

表1 募集人員と受講料

	講義名	講師と形態	募集人員
1	暗号技術とその応用	佐々木中心 講義形式	大学院生： 50名以下 社会人： 15名以下 (受講料1万円)
2	ネットワークのセキュリティ	SEA/Jの講師中心 実習中心	大学院生： 15人程度 社会人： 15人程度 (受講料3万円)
3	不正侵入対策の実際	SEA/Jの講師中心 実習中心	大学院生： 15人程度 社会人： 15人程度 (受講料3万円)

講義1, 2, 3を単独で受講できるようにし、修了者には東京電機大学工学専攻主任から修了書を出すことにした。

こうした産学協同の試みは、人材育成基盤の整備を急ぐ行政施策と合致し、検討の過程で経済産業省とNPO日本ネットワークセキュリティ協会(JNSA)⁴⁾の協力が得られた。(JNSAは2005年度からの参画)

募集を開始するに当たっては、社会人に開講をPRするために経済産業省担当官の講演も含めて2004年2月19日(木)にセキュリティ教育に関する無料セミナーを実施した。

このセミナーについては、幸い、マスコミが、実施の案内や、結果の紹介などいろいろな形で扱ってくれた。

このように、講座開設の準備は、比較的順調に進んだが、予想しない次のような問題も生じた。

(1)講義に使うマイクロソフトのOSなどについて、大学全体として、使用契約を結んでいたが、社会人が参加すると、別

契約が必要であることが判明した。このため、別途、お金を払い契約を結ばなければならなかった。

(2) 当初大学のコンピュータやネットワーク環境を全面的に使おうと思っていた。しかし、本講義では、実習の目的上、サーバに管理者権限で入ったり、擬似攻撃を行ったりするため、大学のセキュリティポリシーと整合しないという問題が生じ、環境を独自に追加せざるをえないということになった。

4. 2 2004 年度の実践状況

以上のような経緯を経て、講義が開始された。そのシラバスは、表 2-4 に示すとおりである。

表 2 講義 1：暗号とその応用

2004 年度前期：水曜日 17:30-19:00	
第 1 回	イントロダクション
第 2 回	セキュリティ技術と暗号技術の概要
第 3 回	共通鍵暗号 1 (ストリーム暗号、ブロック暗号の代表である DES)
第 4 回	共通鍵暗号 2 (共通鍵暗号の適用モード、解読方法、鍵管理など)
第 5 回	公開鍵暗号 1 (公開鍵暗号のニーズ、RSA 暗号の具体的方法の説明と実習)
第 6 回	公開鍵暗号 2 (エルガマル暗号、利用形態、攻撃方法)
第 7 回	デジタル署名
第 8 回	PKI 1 (基本的枠組み)
第 9 回	PKI 2 (PKI の相互認証方法や、公開鍵証明書が無効化の手順など)
第 10 回	暗号プロトコル (暗号をベースにした秘密分散法や、マルチパーティプロトコル、グループ署名、多重署名等の方法)
第 11 回	不正コピーの防止技術 (技術の概要、電子透かしなど)
第 12 回	全体のまとめ

表 3 講義 2：ネットワークのセキュリティ

2004 年度前期：水曜日 19:10-20:40	
第 1 回	イントロダクション
第 2 回	ネットワークセキュリティ技術の概要

第 3 回	不正侵入の現状と対策の基礎
第 4 回	ウイルス対策
第 5 回	メール・WEB セキュリティ
第 6 回	クライアント OS セキュリティ対策
第 7 回	セキュリティプロトコル (SSL,IPSEC)
第 8 回	不正侵入と対策技術
第 9 回	アクセス制御
第 10 回	ネットワークセキュリティトータル設計
第 11 回	セキュリティマネージメント
第 12 回	全体まとめ

表 4 講義 3：不正侵入対策の実践

2004 年度後期：水曜日 19:10-20:40	
第 1 回	イントロダクション
第 2 回	セキュリティマネージメント
第 3 回	ウイルス対策
第 4 回	Windows セキュリティ
第 5 回	UNIX セキュリティ
第 6 回	セキュリティプロトコル
第 7 回	ソフトウェア開発とセキュリティ
第 8 回	不正侵入と対策技術 1 (IDS の構築、検出実習)
第 9 回	不正侵入と対策技術 2 (アクセス制御、NAT、FW 等)
第 10 回	ケーススタディ
第 11 回	情報セキュリティと法律
第 12 回	全体のまとめ

講義 1 と講義 2 を前期に実施し、講義 3 を後期に実施した。

講義 1 は予定通り佐々木が、講義 2 は SEA/J (ヒューコム) の近藤裕朗氏が、講義 3 は、同じく SEA/J (ヒューコム) の伊藤が行った。

2, 3 の講義は、実機演習をベースにしたより実践的な教育スタイルでありその学習目標は、様々なインシデントに対応できる応用力の醸成というのが特徴である。

最終的な、受講者は以下に示すとおりである。

	社会人	学生	合計
講義 1	13	35	48
講義 2	17	13	30
講義 3	13	17	30

社会人は複数の講義を受講した人が多く、実質の人数は、男子 19 名、女子 3 名、合計 22 名であった。また、平均年齢は、40.3 才で、最高年齢は 59 才、最低年齢は 27 才あった。ネットワークやセキュリティ関連業務の人は少なく、教養として勉強してみたいと言う人もいた。

講義 1 は応募者全員を採用した。講義 2,3 には、大学院生は、2 倍以上が応募し、社会人も採用人員よりやや多い人数が応募した。講義 2,3 は書類審査後、抽選をする形で、最終受講者をきめた。

試験の成績については、講義 1 については学生と社会人でほとんど差がなくいずれも良くできていた。数学の基礎さえあり、きちんと講義を聴いていれば、理解できる内容だったからであると考えられる。

講義 2, 3 については、社会人の中には非常に良くできていた人もいるが、平均すると学生の方が 5 点ぐらい良かった。社会人の中にはネットワークやコンピュータに関する知識が不十分な人もいて、セキュリティ以前の部分で、苦労があったように見られる。

4. 3 2005 年度の実践状況

2005 年度は、講義 1 は佐々木が、講義 2 と 3 については伊藤が実施した。

それぞれの受講者は以下のとおりである。

	社会人	学生	合計
講義 1	4	11	15
講義 2	13	17	30
講義 3	11	19	30

社会人の参加者がやや減ったのは、事前にセミナーを行うなどの PR 活動の不足の可能性が高い。講義 1 の学生の受講者が減ったのは、前年、修士の 1 年生 2 年生が応募し全員受講許可したため 2005 年度は修士の 1 年しか受講希望者が残っていなかったためと考えられる。

なお、社会人は前年に比べかなり若返り、平均年齢は 30 歳台であった。前年に比べ、ネットワーク関連業務やセキュリティ関連業務についている人が多いのが特徴であった。一方、ネットワークの知識があまりない人もごく少数ではあるがやはりいた。

講義 2 と 3 については前年度の反省を踏

まえ以下のようなことを行った。

(1) 「端末の基本操作ができる」「TCP/IP を理解している」等の前提条件が満たされていないため、講義では操作部分、講義内容の理解で遅れる受講者が見られた。このため受講生のスキル（または経験）のバラつきを想定し、講義の前提知識となる部も一部教えた。また、期に一回ずつ土曜日に、補習を行い遅れの取戻しを図った。

(2) 前年度は不正アクセスの技術内容（攻撃側）が中心であったが、攻撃への対策原理、対策作業についての理解度が低い受講生が見られた。攻撃手法とは、対策（または管理者）側の技術の素養がなければ、有効性、原理、対策を理解させることが難しい。

よって対策（または管理者）側の対策として、公開サーバの設計、構築、運用をカリキュラムに含めた。この結果、攻撃が成功する際の対策不備（原因）を理解した上で、対策技術の実施を行うことができ、理解度が上がったと思われる。

(3) 限られた時間（90/回）内で効率よく業務経験を積ませるために、遠隔に常時接続可能なサーバ環境を構築し、講義と平行して随時学習できる新しい講義形態の実践を試みた。

その結果、講義の学習（前準備、復習）を講義時間に制約を受けることなく進めることができ効率良くサーバ構築、管理という業務経験をつむことができたと考えられる。

(4) 前年以上に、「教える」よりも「経験させる」部分を増やした。講義で学んだ対策作業が、「いざサーバ構築」という時に実践できない人が多かったことや、効果測定において応用問題を出すと解けないことに対応するためである。

(5) 重点化をできるだけ心がけた。講義 3 については「ソフトウェア開発とセキュリティ」をはずしインシデントレスポンスに関する時間を増大した。

試験の成績については、講義 1 については前年と同様に、学生と社会人でほとんど差がなく、ごく一部の人を除いては、いずれも良くできていた。

講義 2, 3 については、全体的に理解度が進んでいたように思う。社会人の中には

非常に良くできていた人が少なくない一方、やはりついていけない人もいて、平均すると学生とほぼ同じぐらいの点であった。

5. 感想と今後の課題

2年間各講義で受講者にアンケートを行った。アンケート結果は以下のとおりである。その結果は、表5に示すとおりであり、以下のようなことが言える。

- (1) 一般に、受講者の満足度は高い。
- (2) 2004年度に比べ2005年度の満足度があがっている。

表5 アンケート結果

		講義1		講義2		講義3	
		2004年	2005年	2004年	2005年	2004年	2005年
理解度	十分理解	45%	41%	29%	40%	29%	39%
	だいたい理解	50%	59%	55%	46%	65%	56%
	あまり理解できず	5%	0%	13%	13%	6%	6%
	ほとんど理解できず	0%	0%	3%	2%	0%	0%
目標達成度	十分達成	44%	59%	23%	40%	27%	33%
	だいたい達成	55%	35%	64%	53%	67%	47%
	達成困難	1%	5%	12%	7%	6%	17%
	達成不可能	0%	0%	1%	0%	0%	3%

このように、今回のセキュリティ教育講座は、効果があったといってよいであろう。著者らもいろいろなノウハウを得ることができた。

また、社会人がいて、一緒に講義を受けることで、学生が、現実のニーズを知るとともに、刺激を受け、積極的に講義に取り組むようになったのが印象的であった。

一応、2年間で予定どおり、産学協同のセキュリティ教育講座を終えることとした。これは、大企業を中心に社内の技術者に対するセキュリティ教育も普及してきていることや、セキュリティ教育を提供している会社が増えてきていることによる。

また、東京電機大学では、今まで大学院でやってきた内容のかんりの部分を、学部で実施するように計画中である。ここでは、今回の講座の実施により大学側に蓄積されたノウハウを生かし、大学独自で実施していきたいと考えている。

今回得られたノウハウを経済産業省やJNSAらとも協力し、他の大学や中小企業のセキュリティ教育の普及に生かして行くのが今後の課題であると考えている。

6. 終わりに

本講座を企画し始めた2002年ごろに比べると、日本のセキュリティ教育も、ずいぶん良くなってきていると考えている。大学においても、セキュリティ教育が充実しつつあり、情報セキュリティ大学院大学も誕生した。また、大企業を中心に社内の技術者に対するセキュリティ教育も普及してきている。

しかし、まだセキュリティ教育を行っていない情報系大学も多く、中小企業や、一般住民に対するセキュリティ教育は不十分である。

一応、2年間で予定どおり、産学協同のセキュリティ教育講座を終えるが、このノウハウを、経済産業省とも協力し、大学や民間のセキュリティ教育の普及に生かしていきたいと考えている。

最後に、この教育の実現と運用に協力いただいた多くの方々に深謝申し上げる。

参考文献

- 1) 佐々木良一、板津守昭「情報セキュリティ教育の現状と将来に関する考察」情報処理学会、CSS2003、2003年10月
- 2) 佐々木良一「大学院情報セキュリティ講座—東京電機大学の場合」Cyber Security Management Vol. 5, No.57, July 2004
- 3) 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、信学技報 SITE 2004年10月
- 4) NPO 日本ネットワークセキュリティ協会 (JNSA)
URL <http://www.jnsa.org/>
- 5) 「情報セキュリティ教育に関する調査報告書」2004年
<http://www.meti.go.jp/policy/netsecurity/downloadfiles/edu-report.pdf>
- 6) SEA/J
URL <http://www.sea-j.net>
- 7) 株式会社ヒューコム
URL <http://www.hucom.co.jp>