講演レポート

実務型セキュリティ人材育成プログラム

砂原秀樹
奈良先端科学技術大学院大学教授

概要：2007 年度の「先導的 IT スペシャリスト育成プログラム」に、奈良先端科学技術大学院大学の「社会的 IT リスク軽減のための情報セキュリティ技術者・実務者育成」が採択された。その計画、プログラムの内容について説明する。

キーワード：情報セキュリティ、人材育成、セキュリティ管理者

1. はじめに

WIDE プロジェクト[1] の発足が 1988 年ですが、当時は現在のセキュリティ状況を予想すらできませんでした。ですが、インターネットを始めた者の一人として、この状況を放置することはできるものではありません。そうした思いから「社会的 IT リスク軽減のための情報セキュリティ技術者・実務者育成」[2] プログラムを、2007 年度の「先導的 IT スペシャリスト育成プログラム」[3] に提案していました。この度、幸いにも採択されることができましたので、その計画等も含めて説明します。

2. セキュリティを巡る状況

セキュリティ管理者が果たすべき役割は多岐にわたり、これを全部実行できる人材はまさにスーパーマンですが、その数は少なく、これは解決しないといけない問題です。

それでは、セキュリティ管理者の日常業務を考えてみましょう。まずサービスを考え、さまざまな検討の末、計算機を導入して、ソフトウェアをインストールして、さまざまな設定を行う必要があります。しかも、サービスは増えこそすれ、減ることはありません。

奈良先端科学技術大学院大学（以下、NAIST と略す）では電子図書館を 12 年程前から運営していますが、そこに入れてあるコンテンツのアクセス権の管理も複雑です。誰に見せてもいいものから、お金を払った人にだけ見せる講座、特定の講義を履修している人だけに見せるものとか、契約ごとに全部違います。また本学の電子図書館は、全授業をビデオアーカイブしていますが、記録した授業を eLearning 教材に仕上げるのは、大変手間のかかる作業です。また本学では分子解析や遺伝子情報の交換などを行っていますが、遺伝子関係は権利関係がものすごく複雑です。

ソフトウェアとして LDAP を例にとると、管理対象や、権限管理、課金管理などを考えていく必要があります。これだけなら、情報科学や情報工学の教育を受けてきた方なら、十分に対応できる内容です。これに対して、組織や人事を関連づける判断は、いわゆる経営的センスが必要になってきます。従って、これまで普通に育てたエンジニアでは対応できないところがでてきます。

さらに個人情報保護法の問題もあります。情報漏洩のケースとして、委託契約先の技術者が、ある情報を見たことを他人に何の気なしに喋ってしまったことがあります。この場合は仕組みだけで解決できる問題ではなくて、ルール作りとか契約まで視野にいれて、取り決めを結んでいく必要があります。

個人情報の漏洩といえば、Winny も社会的に大問題になりましたが、この背景には、自分が当事者であるという意識の欠如があります。ウイルス対策ソフトウェアやスパイ対策ソフトウェアをインストールしていない人は、当たり前のようにいます。先日も、ウイルスに感染したマシンがありましたが、いわゆる外国の危ないサイトにアクセスすることが、どういう意味を持っているのかを理解していないケースでした。今や大学の国際化は当然のことですから、日本生まれでない学生も多いのですが、そういう人たちはバックグラウンドが違いますから、意識がまったく違います。そういう人たちにやってはいけないことを教え諭すのは非常に苦労しますが、これもセキュリティ担当者がやらざるを得ないことが多い状況です。

その反面、過剰反応の問題もあります。ポリシーを作成するときに、十分な知識があれば守るべき線が分かるのですが、不十分なままで作成すると反応が過剰になり、厳格すぎるポリシーになることが多いようです。運用ポリシーを作るのは本当に微妙な作業で、ポ

リシーを守ために、どの技術を使って、どう運用していくと、一番バランスが良いのか、なかなか分からないわけです。かといって、厳しくしすぎると、今度は誰も使わないシステムになり、さらに穴ができる結果になります。ですから管理者のスキルが非常に重要になってきます。素晴らしい管理者のつくった組織は、住みやすい環境がつくれますが、管理者の能力が下がるほど、過剰反応をする傾向にあります。

15 年ぐらい前までは、外側から内側に向かう攻撃を監視していればよかったのですが、最近は、内側にも敵がいます。学外へ持っていってウイルスに感染したパソコンを、平然と研究室のネットワークにつないでいる人がいます。あと、寮や宿舎にネットワークのある大学は大変です。寮はまだ何とかなりますが、本当に大変なのは大学宿舎です。住んでいる教職員の方たちにどんなに言い含めても、そこの子どもまではなかなか手が回りません。またプライベートスペースですので女性の方もいらっしゃいますから、セクハラとかも考えないといけません。

ネットワークの監視を行うために、いろいろなツールを使いこなす必要があります。MRTG から始まって tcpdump、それから最近はサンプリングといいますが、8,000 パケットに 1 個とか、16,000 パケットに 1 個ぐらい取ってきて、それをチェックしながら通信状態の把握をしています。これも、あまねく監視していると、プライバシーの侵害だといってくる人がいますので、「こういう理由に基づいて、こういうツールを皆さんの通信を監視することに使っています。従って、問題がないことを認識して行動してください」と、学内のあちらこちらで言わないといけません。そうしないと勝手なことをやっているといわれて、大変な問題になります。

それから、IDS や IPS などありますが、これは買ってきて導入すればそれで済むと思っている人たちが多いようです。しかし、これを使いこなすためには、どのパターンを対象にして、どのようにチェックするかとか、パターンのアップデートをどうするかなど、新しく自分たちで考えながら運用していかねばなりません。

このように、道具の使い方から始まって、ポリシーを作る経営センス、それから、どんどん新しくなる法律を解釈して、対処方を考えていかなければいけないし、まったくセキュリティが分かっていない人に教育までしなければなりません。それから、技術だけ分かればいいわけではなくて、法律や倫理も理解している必要があります。

3. 実務型セキュリティ人材育成プログラムの概要

セキュリティをやっている人間は、大体が法律や経営などは不得手なのですが、それではセキュリティ管理者の役割を果せないことをこれまで説明してきました。さらにとても大切なことは、こうした仕事は 1 人でできるものではなく、仲間が必要だということです。そうすると仲間を見つけるプロセスを、うまく作ってやらなければなりません。これからお話をするプログラムの基本的なポイントです。

2006 年度の「先導的 IT スペシャリスト育成プログラム」はソフトウェアエンジニア育成をテーマにしていて、大阪大学が主導して関西圏の大学をまとめました。2007 度の同プログラムはセキュリティがテーマになり、本来なら京都大学が取りまとめるところなのですが、いろいろなご相談をしている中で、内閣官房セキュリティ補佐官 2 名を加えて NAIST が頭に立つようにいっていただきました。そうした経緯から、「社会的 IT リスク軽減のための情報セキュリティ技術者・実務者育成」というプログラムを作らせていただき、NAIST が申請大学となり、京都大学、大阪大学、北陸先端科学技術大学院大学（以下、JAIST と略す）に連携大学に入っていただきました。

今年度の「先導的 IT スペシャリスト育成プログラム」には、セキュリティ技術の研究者育成という目的も入っていたのですが、やはり実務者育成に集中することにしました。大学院を修了した若者が、すぐに各大学や各組織の、CSO、CIO、CSIO といったような立場になれるとは思いませんが、それを補佐するような立場になれるような人材を作ろうという趣旨です。今まで説明をしてきた通り、セキュリティ対策の立案から実行までをできる人を育成することを考えています。ソフトウェアの設定や使い方などもしますが、やっぱりやりたいことは、エンジニアリング、法律、政策、経営、倫理といったようなことを理解した上で、セキュリティポリシーを作ること、それからシステムデザインをすること、インシデントが発生したときにその対策を取ることができること、を考えています。

セキュリティインシデントは自分 1 人で解決できるものではなく、いわゆる交渉事が必要になります。そちらからこの攻撃が来てい

ます、だから、これはこういうふうに直してもらいたいのですが、どうすればいいでしょうかという話を、先方としなければなりません。これは、理工系学部出身者には、苦手な分野だと思いますが、今求められているのはこういうことです。それと同時に、やはり表面上の技術だけでなく、背景となるメカニズムや技術を理解していることが必要です。だからこそ大学院でやる意味があるのだと思います。そういった人材育成を目標に掲げてプログラムをデザインしてきました。

実践的セキュリティエンジニアを育てたいのですが、そのためにまず基礎となる知識、これはいわゆる情報科学工学系の大学院ではすでに教えていることですが、ネットワーク技術や、セキュリティ技術、情報理論に代表されるようなものをきっちり体系化して教えることが、ポイントです。だからこそ情報工学の大学院の中に、このコースを作ったのです。それと同時に、法律、経営、政策といったような分野の理解、組織連携、さらに最新情報の収集といったことができるように、弁護士や公認会計士であるとか、企業経営者、政府政策系の方、そういった専門家の方々に来ていただいて突っ込んだ議論をしていただきます。

机上の学習だけでは、本当にインシデントに遭った場合に、対応できません。これには、やはり経験がものをいうもので、やはり毎日パケットをのぞき込んでいて、これは危険だと感じたら、その対策を予防的に張るということが必要になってきます。そこで、経験的知識といっていますが、実際にいろいろなインシデントを経験することが必要で、危機対応能力、それから、実践能力、それから、インシデントが起きたときに、何を証拠として取っておいて、フォレンジックスとかいいますけども、それを人に見せて、それで交渉事を進めていくかっていったようなことを含めて、ちゃんと対象をつくっていくということをしようと思いました。

このプログラムにさまざまな組織が関わります。NAIST と JAIST は、セキュリティインシデントのための、いろいろな基礎的研究基盤や実習基盤を作ってきましたので、その辺りを担います。それから、大阪大学と京都大学は関西地区の大学として、日本のインターネットの構築の推進力の一部を担ってきた実績があります。

それから、京都大学の上原哲太郎先生が中心になって若い芽を育てている NPO 法人情報セキュリティ研究所[4]、独立行政法人通信機構研究機構（以下、NICT と略す）北陸リサーチセンター[5]、それからセキュリティインシデントが発生したときに報告された情報の管理を行っている JPCERT/CC[6] にも協力していただきます。それから、現場の状況を見てほしいと思いますので、いろいろな交渉の末、NTT コミュニケーションズ株式会社にもご協力をいただけることになりました。そんなことで、全部で 8 つの組織がかかわってスタートをすることになっています。さらにサイバー関西プロジェクト[7] という、関西でインターネットの推進をやってきたグループとも意見交換をしてきました。こうしたことから、プログラムを推進する要素は揃ってきたと思います。

プログラムに携わるメンバーですが、NAIST には情報セキュリティ補佐官の山口英先生がいます。それから、大阪大学には中村先生、東野輝夫先生を初めとする方々がいらっしゃいます。それから、京都大学は岡部寿男先生を筆頭に、高倉弘喜先生、上原哲太郎先生が関わります。それから、JAIST からは、日本の暗号技術の権威である宮地充子先生に入っていただきます。もう 1 人の情報セキュリティ補佐官である篠田陽一先生には、NICT 北陸リサーチセンターの立場から携わっていただきます。それから、NPO 法人情報セキュリティ研究所からは上原先生を初めとする方々、そして JPCERT/CC からは代表理事の歌代和正さんに客員教授になっていただく予定です。最後になりますが、NTT コミュニケーションズは OCN 事業の方々に主として関わっていただく予定です。

プログラムの内容は、図 1 の通りになっています。まず基礎科目群は、各大学で持っているネットワークあるいは様々な分野の情報関係の基礎理論の授業を受けていただきます。これは 2 科目 4 単位と書いてありますが、それでは少し物足りないので、さらに積極的に受講してもらう予定です。次の先進科目群は、全部必修になっていて、いわゆる法律系、政策、倫理といったところの専門家の方々から学んでいただく、そして最新情報をまとめた知識を学んでいただきます。最後の実践科目は 4 科目 4 単位になっていて、実際にセキュリティインシデントを体験する実習をやります。

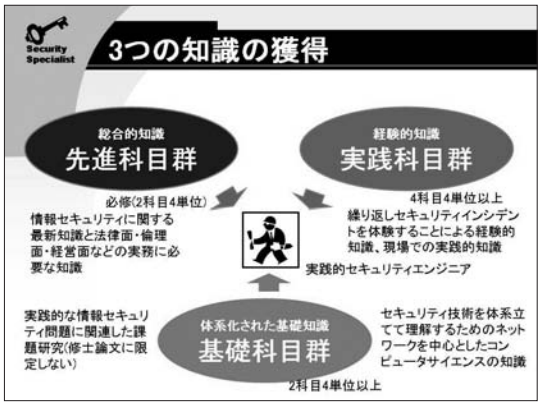

図 1.　3 つの知識の獲得

例えばどんな授業があるかというと、NAIST では基礎科目として図 2 のような授業を受けてもらいます。

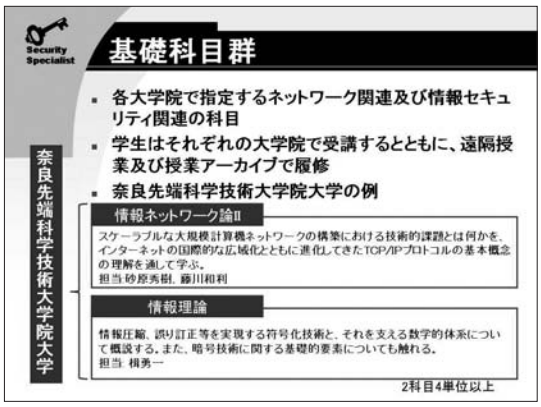

図 2.　基礎科目群

それから、先進科目群に関しては、人的ネットワークをちゃんとつくるということが非常に重要だと思っていて、必修科目は半数以上を集合形式で講義をする考えです。このために、大阪大学の中之島センターやキャンパスプラザ京都など交通の便のいい場所を使っています。この 4 つの大学は先生同士の交流はありますが、学生同士の交流は多くないと思いますので、授業を通して、他大学の先生方や学生と顔見知りになるよう期待しています。先進科目群の具体的内容は図 3 の通りで、「情報セキュリティ運用リテラシー」というのが、倫理や法律といった授業で、「最新情報セキュリティ特論」が最新情報を学んでもらうものです。

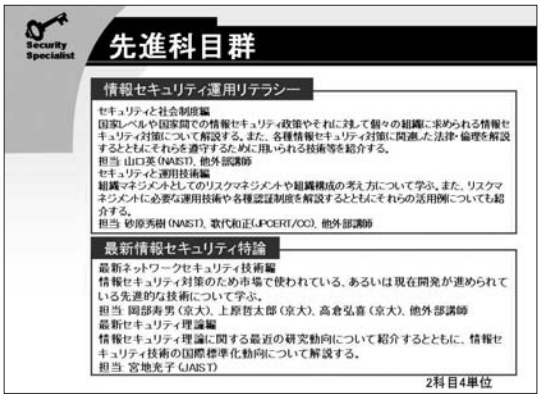

図 3.　先進科目群

さらに実践科目群は、合宿形式になる予定ですが、いろいろな環境を使ってセキュリティインシデントを体験します。それと同時に、NTT コミュニケーションズにインターンシップに行ってもらいます。特に重要視するのは現場勘です。セキュリティやネットワークの管理をしていると分かるのですが、これは危険だという時には、だいたい勘が働きます。そこを養成することを考えています。

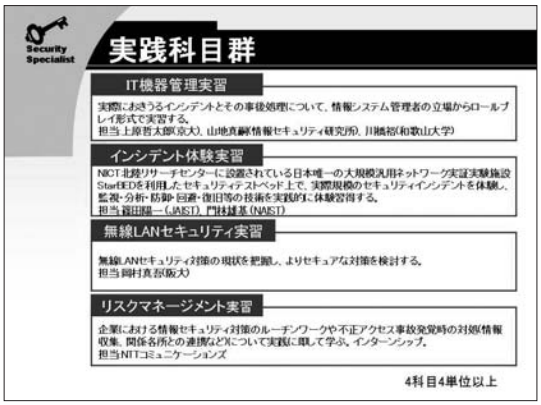

図 4.　実践科目群

授業環境としては、ポイントは 2 つあります。1 つ目は、NAIST の電子図書館にこのプログラムで使われるすべての授業コンテンツを収めることで、それはコースウェア化して、共有していく予定です。ですから、これは復習に使うだけではなく、授業評価であるとか、外部からの評価を得て改善に使っていくといったことを考えています。

2 つ目は、NICT 北陸リサーチセンターの StarBED 大規模ユビキタスシステムエミュレータという装置を、実体験型実習プログラムで使っていくことです。これは日本唯一の施設で、約 800 台のノードと、約 2,000 のポートを持っており、これを組み合わせるこ

とにより自由自在にネットワークを組むことができます。さらに、各ノードには仮想計算機環境が用意してあり、1 ノード当り 10 ノード弱のエミュレーションができるようになっています。そうすると 7,000 から 6,000 ノード位のネットワークを作ることができるわけです。サポートツールがだいぶ出来上がってきておりますので、ネットワークが本当に壊れていく様子を、この環境の中で実験をしていくことでスキルアップを図ろうと考えております。

2007 年度からスタートした事業ですが、今年度は準備期間ですので、カリキュラムやコースウェアを開発したり、大学間の契約とかを行っている最中です。けれども、2008 年 4 月からこのプログラムを実施します。プログラム全体で 4 年間ですので、教育自体を実施するのは 3 年間となる予定です。

原則として、各大学院の博士課程前期あるいは修士課程の学生を対象にする予定ですが、社会人の方々の受け入れも考慮しています。とはいえ、実習機材の関係から全体で 20 名程度が限界と思います。本来このカリキュラムは 1 年間で完了することで決定していますが、2 年あるいは 3 年かけて履修できるような配慮はしていこうと思います。

このプログラムを履修することにより何ができるようになるかというと、実践的実習等によって経験と勘を付けることです。技術的なことだけではなくて、法律、経営、政策、倫理といった知識を獲得し、ちゃんと実践できるような人を育てるということです。それから、ここが一番重要だと思うのですが、プログラムを公開して、広報を積極的にしていく予定で、そういうことをしながら評価等をいただきながら更なる改善を目指していきたいと思います。

4. 最後に

本当に重要なことは、人的ネットワークを作っていくことです。かつてインターネットを作った人間のネットワークができたのと同じように、セキュリティ人材のネットワークをこれからつくっていくことを求めているところです。

参考 URL 等

1) WIDE プロジェクト
http://www.wide.ad.jp/
2) 「先導的先導的 IT スペシャリスト育成推進プログラム」採択拠点
http://it-keys-naist.jp/
3) 先導的 IT スペシャリスト育成プログラム
http://www.mext.go.jp/b_menu/houdou/19/09/07091306.htm
4) NPO 情報セキュリティ研究所
http://www.riis.or.jp/
5) NICT 北陸リサーチセンター
http://www2.nict.go.jp/q/q262/3105/
6) JPCERT/CC
http://www.jpcert.or.jp/
7) サイバー関西プロジェクト
http://www.ckp.or.jp/

注記

本稿は 2007 年 11 月 16 日開催の CAUA 第 6 回合同研究分科会における講演内容を、CAUA 事務局が文章にまとめたもので、文責は CAUA 事務局にあります。