セキュリティを含めた人材の育成

後藤 滋樹
早稲田大学 基幹理工学部情報理工学科 教授

概要：大学は組織としてサイバー攻撃の対策を講じる必要がある。それと同時に大学はセキュリティの教育に注力することが求められている。幸いにも多くの学生がセキュリティ分野に興味を抱いている。また産業界と大学が協力する体制が整備されつつある。

キーワード：サイバー攻撃、セキュリティ教育、人材育成

1. 大学は攻撃され、攻撃する

当然のことながら、大学は外部からの攻撃を受けている。本学も標的型攻撃を受けたことがある。さらに、大学の内部でも問題は起きており、数年前には USB メモリーからトロイの木馬が全学的に学生の間で流行った。最近は DNS amp attack や NTP amp attack も多く、ssh の総当たり攻撃を受けるのは日常茶飯事である。学生が研究のために、攻撃の持続時間を測って統計をとるなど、サイバー攻撃を論文の材料にすることもある。

一方、大学の中から攻撃をしてしまったこともある。PlanetLab[1] はスペックに合ったマシンを大学として提供すると、プロジェクトに加盟する世界中の 700-800 台ものマシンを利用できるインターネット上の実験的なネットワークである。ある時、PlanetLab の本学のノードから米国のデータセンタへのポートスキャンが行われて苦情が寄せられた。調べてみると MIT の学生が行ったことだと判明した。

また、非常勤の先生の PC が踏み台に使われたこともあった。学生と教職員の意識を全学でもれなく高めるような取り組みが大学として必要となった。

サイバーセキュリティ基本法により、大学としては教育だけでなく、組織として対応を取らなければならなくなった。本学では、理事が務める CISO の下に情報セキュリティ委員会があり、その下に学生、教員、職員がいるという体制である。教員は、研究に何々が必要だと主張する向きもあり情報セキュリティ委員会としても一律に規制しにくい。一方、職員組織は一般企業と似ている。事務系が標的型攻撃に狙われる。

1 https：//www.planet-lab.org/

2. 早稲田大学のセキュリティ教育

本学では、寄附講座の形で 2 科目を 2015 年度に新設した。それまでセキュリティの科目がないわけではないが、本格的な科目の誕生である。大学院の科目は、高度な演習を行うので、受講人数を 12 名に制限したが、初年度は 43 人の学生が申込み、希望する生徒全員は授業が受けられなかった。

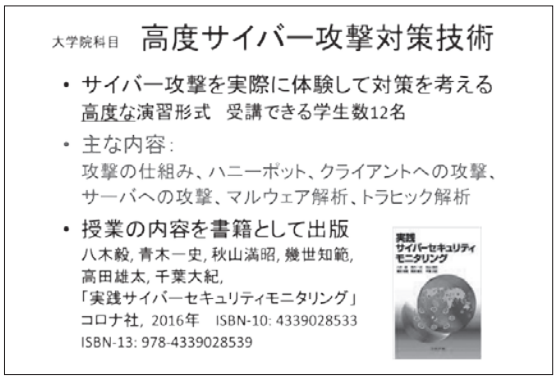

図 1 「高度サイバー攻撃対策技術」講座

高度サイバー攻撃対策技術の講座（図 1）では、当然サイバー攻撃の話をするので、教材を公開できない。そのため、履修の抽選に外れてしまった学生を対象に、本学のラーニングシステムである CourseN@vi 上に、仮想的なクラスを新設して教材を置いた。履修者は、研究室でサーバやネットワーク管理を担当している学生が指導教授から履修するように言われて受講している例が多い。こうなると半ば学生も仕事である。

講座を運営していく上で様々な課題が発生した。一つは、無線 LAN の問題である。受講者は仮想デスクトップで実験環境を利用する。このために有線ネットワークが使える教室を準備したが、無線 LAN で使う学生も多く、アクセスが集中すると遅くなった。

さらに、高度な内容を授業で扱うため、受講者よりもTA（Teaching Assistant）の人数が多い科目となった。TAの大学院生は、前の週に講師と一緒に予習をする。TAは学生に指導できる程度に習熟するので、履修申込で外れた学生がTAをつとめると、TAの学生の方が知識が身につくという皮肉なことが起きている。

演習用のツールのインストールは時間がかかる。それを事前に済ませておくか、どこまでをお膳立てするかが難しい。料理教室に例えると、鍋を開けたらもう半分できているというのでは、料理教室でありえるのか。

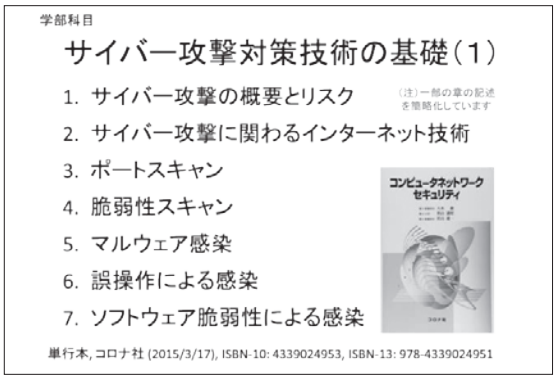

図2 「サイバー攻撃対策技術の基礎」講座

学部では、サイバー攻撃対策技術の基礎という科目を実施している（図2）。学部では100名を定員として履修を募集した。これまで類似の科目がなかったためか、初年度は150名の申込があった。

学生の感想を聞くと、難しい内容だが興味があるという反応だった。複数の新聞社から授業の取材があり、企業からの見学もあったので、履修した学生も社会に期待されているという手応えを感じたのではないか。

3. 今後の課題

他の大学でも同様の取組みが始まっている。1つの大学ですべてをカバーするのは限界があるので、横の連携やさらに産学官の連携を始めている。

情報の共有も課題である。たとえば研究用のデータとなる、悪意のあるblack dataは国際的にもいろいろなサンプルがあり、日本の情報処理学会でもMWSという仕組みがある。ところが、研究をするためには技術を検証する必要がある。個人情報や通信の機密で保護されている普通のwhite dataへのアクセスは非常に難しく、自分の周辺のデータしか使えない。

セキュリティの研究成果を共有するためには、データや研究の手法の詳細を書かないとよく分からない。国際会議で学生が表彰されると、詳細な問い合わせが来ることがある。

国際協力も不可欠である。ミサイルとサイバー攻撃は、近距離の方が遠距離よりも成功率が高い。ウイルスは近くのネットワークに拡散する。ある国の中でも、DoS attackを受けている。たとえばCNNICというJPNICの兄弟組織が攻撃を受けた例が、中国語では公開されている。

4. セキュリティ教育の効果

セキュリティ教育への関心の高まりにより、産業横断サイバーセキュリティ人材育成検討会[2]が始まっている。

セキュリティの理解のためには、情報通信の広範な知識が必要であり、大学の必修科目を習得していない学生は、サイバー攻撃の授業を受けても理解できないだろう。敷居が高いが、ある意味では教育的でもある。社会の要請では、現在のセキュリティ人材では将来の展開に向けて不十分だという。そもそも技術者の人数が大幅に不足している。

やはり問題となるのは、情報共有である。コンピューターウイルスという言い方は、もともと人間の病気が元になっている。例えば、エボラ出血熱の場合、病気に罹ると仲間外れにされたりする。家族が患者を隠したり、村単位で隠してしまうことがあり、実態が把握できなかった。現在のサイバーセキュリティは、これに近いところがある。サイバー攻撃にあっても、意図的に隠すまでではないが、

2 http://cyber-risk.or.jp/

積極的には発表をしない。あるいは、実は感染しているのに気がついていないこともある。コンピュータやネットワークに携わるわれわれは、こういうものに十分教訓を得て、時代に相応しく情報共有をやらないといけないだろう。

〈参考〉
八木毅，秋山満昭，森達哉，針生剛男，後藤滋樹，「産学連携によるサイバーセキュリティ教育分野の確立」信学技報，vol. 115, no. 81, ICSS2015-10, pp. 51－56, 2015年6月.