リテラシー教育としてのサイバーセキュリティ

岡村 耕二
九州大学　サイバーセキュリティセンター長　教授

概要：本項では、九州大学のサイバーセキュリティ教育の取り組みについて、平成 29 年度からの必須化に向けて、現在選択科目として開講しているサイバーセキュリティ基礎論を受講している全学部からの様々な学生による講義の感想、小テストの内容、試験の結果などから得た知見や課題を交えながら紹介する。

キーワード：サイバーセキュリティ、教育

1. 九州大学の情報系組織の変遷

九州大学では、大型計算機センターや情報処理教育センターなどの情報関連施設を統合し、2000 年に 4 月に情報基盤センターが設置された。教員と職員を分けた組織形態の歴史も長く、2007 年には学内外への情報サービスを一手に担う組織として情報統括本部が発足し、教員が所属して研究開発と全国共同利用計算サービスを担当する情報基盤研究開発センターと、職員が所属する情報システム部が設置された。

2014 年には、サイバーセキュリティセンター[1] が設置された。サイバー攻撃への対応など、サーバーセキュリティ対策は、情報統括本部で行っている。一方で、サイバーセキュリティセンターでは、まず、人材教育、そして研究と国内外の機関との連携・共同研究を行う役割を持っている。大学のサイバー攻撃対策などには、直接関与しないという立場である。

サイバーセキュリティセンターは、まだ大きな組織ではなく、教授会もないので、人事権もない。私は情報基盤研究開発センターに所属しており、サイバーセキュリティセンターは兼任という形にはなっているが、現在はほぼ 100% サイバーセキュリティセンターの仕事をしている。

2. ICT 整備の歴史とセキュリティインシデント

ICT 整備の歴史は、セキュリティインシデントとの戦いであり、インシデント対策にかかるコストは右肩上がりに増加している。(図 1)

1998 年頃は、web がやや普及して、学生もホームページを自分で作れるようになった。それに伴い、ホームページ上に著作権のあるものを置いて、外部から指摘を受けてしまうことがよくあった。この頃は、著作権侵害を例に、学生に対して情報倫理についての教育をしていた。

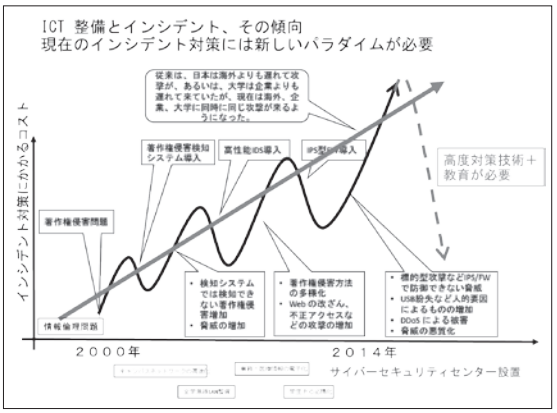

図 1　ICT 整備とインシデント、その傾向

2000 年に入ると、キャンパスネットワークや SINET が高速化し、P2P ソフトを使った本格的な著作権侵害問題が出てきた。これは新聞に載ってしまうこともあり、学生に注意をするだけでは済まなくなった。そこで、P2P フェンダーというツールを使い、九大のアドレスで、著作権侵害が発生していないかをチェックした。これにより、この問題はやや減った。

しかし、その後に、検知システムでは検知できない著作権侵害の問題が増加したため、高性能 IDS を導入した。IDS ではアプリケーションの識別ができるので、P2P の利用など、P2P ファインダーがサポートしていないようなアプリケーション識別がかなりできるようになった。

さらに、Web の改ざんや不正アクセスな

1　http://staff.cs.kyushu-u.ac.jp/ja/index.html

どの攻撃が増加し、問題を検知するだけでなく、止めることも必要になり、IPS 型ファイアウォールを導入した。このように、新たなツールを導入すると効果が出るが、また別のセキュリティインシデントが発生して対応しなければならないということを繰り返しており、年々セキュリティインシデントの件数も増加している。そのため、もう新たな対策製品を買うだけでは対応できなくなっている。今後、このインシデントを大きく減らすためには、もはや、セキュリティ対策の機器を購入していくだけは十分ではなく、なにかパラダイムシフトのようなものが必要である。それが、高度な対策技術の研究と、やはり教育である。

3. サイバーセキュリティ教育の全学必須化

その後も、学生による著作権や倫理に関わるインシデントは減らなかったため、2014 年にトップダウン的にサイバーセキュリティ教育を開始することになった。当時の理事から話があり、私はアメリカでセキュリティ教育が有名なメリーランド大学（UMBC[2]）に調査に行った。その後、九州大学でサイバーセキュリティの全学部教育を開始する方向と、サイバーセキュリティセンターを設置することが決まった。

教育については、2014 年度の後期に選択科目で開講して実績作りをし、翌年の 2015 年度には、教育企画委員会の審議の中で 2017 年度から全学生への教育の必須化が決定された。九州大学は、2017 年度からクォーター制になることが決まっている。クォーター制では、4 学期制になるので、第 1 クォーターでこのような学生の役に立つ科目を行うことも狙いである。

基幹教育院でも科目実施の協議が行われた。基幹教育とは、昔の教養部に相当する基礎教育である。今は 1 年間で、数学や語学、哲学、経済学等様々な科目を実施している。そのため、新たに科目を増やすことは難しかった。そこで、既存の情報系の科目で受講者が減少しつつある科目を整理して、サイバーセキュリティの科目とした。

4. サイバーセキュリティ基礎論

全学生へサイバーセキュリティ教育を行う根拠は、2014 年 11 月に成立したサイバーセキュリティ基本法[3] である。サイバーセキュリティ基本法では、大学でもサイバーセキュリティ対策をし、教育をするように明記されている。これまでは、必要に応じて教育を行うが、学生全員には教育を行っていなかった。

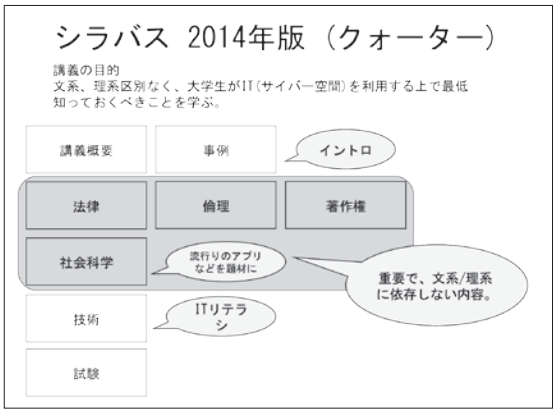

図 2　シラバス 2014 年版

2014 年に講義を開設した際には、クォーター制のため、8 コマで授業を組んだ（図 2）。選択科目であり、様々な学部の学生が受講するため、前半は法律、倫理、そして、法律の中でも重要な著作権の話といった、文系に近い内容とした。また、いわゆる SNS を使って起きるようなトラブルの話やプライバシー、ネットワークの匿名性は実際どうなのか等、学生に身近な例を取り上げている。もちろん、IT リテラシーとして技術の項目も 1 コマ盛り込んでいる。

2015 年度は、15 回の学期制で授業を組んだ。教える内容はあまり増やさず、回数を増やし、それぞれの回で小テストを行い、その合算値で評価を行った。

2016 年度のシラバスが図 3 である。2017 年度からのクォーター制を見越した内容としている。選択科目の講義の第 1 週目は学生が講義を選択する週間なので、受講する学生全員が出席するわけではない。そのため、イントロダクションとして、全体を網羅する話をしている。次の 3 コマは事例の話としている。情報基盤センターの先生からは一般的な話、ヤフー株式会社[4] の方より、企業から見た事例の話、九大病院の先生より、九大病院の事例の話をしてもらっている。

2 http://umbc.edu/

3 http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g18601035.htm

4 http://docs.yahoo.co.jp/

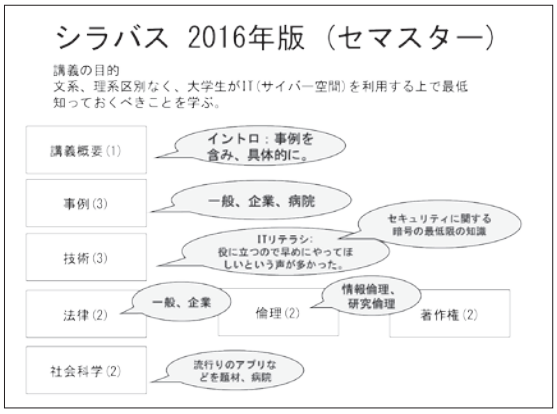

図 3　シラバス 2016 年版

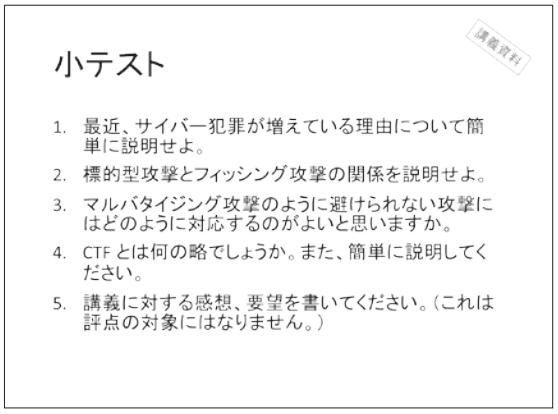

図 4　小テスト（1）

サイバーセキュリティ基礎論ルーブリック

		A	B	C	D	F
知識・理解（３０点満点）	講義の内容について正しく理解している。（３０点満点）	十分に理解できている。（２７～３０点）	理解できている。（２４～２６点）	ある程度理解できている。（２１～２３点）	一部のみ理解できている。（１８～２０点）	全く理解できていない。（０～１７点）
専門的技能（３０点満点）	サイバーセキュリティに関する専門的な知識について正しく理解している。（３０点満点）	十分に理解できている。（２７～３０点）	理解できている。（２４～２６点）	ある程度理解できている。（２１～２３点）	一部のみ理解できている。（１８～２０点）	全く理解できていない。（０～１７点）
汎用的技能（３０点満点）	講義で得た知識を応用して自分の生活に役立たせることができる。（３０点満点）	十分にできる。（２７～３０点）	できる。（２４～２６点）	ある程度理解できる。（２１～２３点）	一部のみ理解できる。（１８～２０点）	全くできない。（０～１７点）
態度・志向性（１０点満点）	講義スライド以外の事項を自ら調べて学習している。（１０点満点）	十分に学習している。（９～１０点）	学習している。（８点）	ある程度学習している。（７点）	一部のみ学習している。（６点）	全く学習していない。（０～５点）

図 5　ルーブリック

2014 年度の授業アンケートで、IT リテラシーの話はかなり役に立つので早くやってほしいという意見があったため、講義の前半に行うことにした。ここでは、コンピューターネットワークの話、無線ネットワークの話と暗号技術の話をしている。法律、倫理、著作権、社会科学についても、それぞれ 2 コマ分を取っている。

5.　評価について

第 1 回目の導入の講義の後に行った小テストの問題が、図 4 である。学生にとっては、あまり簡単ではない問題となっているが、このような問題を出題しているのには、理由がある。

九州大学では、平成 19 年度より GPA 制度[5]を導入した。GPA（Grade Point Average）制度とは、それまでの、優・良・可・不可の 4 段階評価を、A・B・C・D・F の「5 段階評価」とする国際的な成績評価システムである。そして、学習到達状況についての評価基準をより明確にするためにルーブリックを作っている（図 5）。

サイバーセキュリティ基礎論では、授業全体について理解できているか、専門的な知識が理解できているか、また、知識を応用して役立たせることができるか、自分でも調べられるようになっているかというそれぞれの項

5　https://www.kyushu-u.ac.jp/ja/education/class/learning/gpa/

目で、どの程度理解できているかによって評価している。

そのため、図 4 の小テストの問題は、ルーブリックの項目に対応した問題になっている。1 問目は、授業で話した内容であり、2 問目はやや専門的な内容を問う問題である。3 問目は、この授業を受けて身に付いたことを応用して答える問題である。そして 4 問目では、授業では教えていないが、学生はパソコンを持ってきているので、調べて答える問題を出題した。

授業アンケートを実施したところ、1 ケ月前までは高校生だった学生からは、やはり授業のスライドを見て分からない問題は出さないでほしいという意見が非常に多かった。さらに、選択式の問題にしてほしいという意見も多かった。これは、キーボードを打つのが遅くて試験時間の 20 分間では回答ができない学生が意外と多くいることもわかった。そういった意見も参考にしながら、講義の準備をしていった。

6. 授業の内容

実際に起きた事件を事例として取り上げると、学生にも分かりやすいと思い、ベネッセの個人情報流出事件[6] 等を授業でも取り上げていた。しかし、学生からは、具体的な事例よりも、もう少し一般的な話の方がいいという意見もあった。

ガイダンスでは、様々な学部の学生が受講することもあり、何故、サイバーセキュリティのことが、今、問題になっているかという説明もしている。つまり、攻撃をする技術が金儲けとして成功してしまったため、さらに高度な攻撃技術が開発され、それを防御する技術開発・ビジネスも急増して、一つのビジネスとして加速し続けているということである。

学生に、標的型攻撃やフィッシング攻撃という言葉を聞いたことがあるか、と問うが、ほとんど手が上がらない。それぞれの特徴や仕組みを説明しても、深くは理解できないかもしれないが、このような用語があることを知れば、メディア等で話題になった際に目に留まるだろう。そういったきっかけになればいいと考えている。

このような攻撃の種類については、流行があるので、違う攻撃が出てくれば、教える内容も変わってくるだろう。

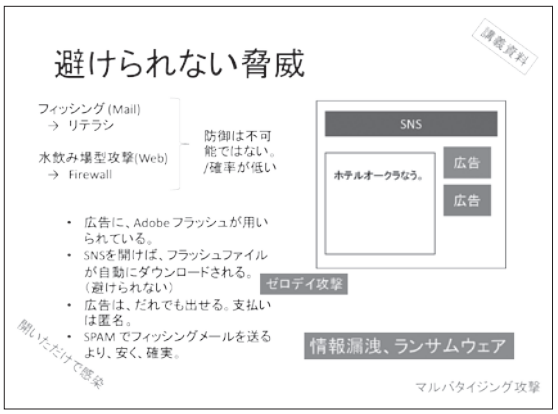

図 6　避けられない脅威

図 6 では、避けられない脅威として、ランサムウェアやマルバタイジング攻撃等について説明している。SNS のあるページを開いただけで感染する仕組みを、コンピュータのネットワークの仕組みを全く知らない一年生に、しかも 10 分ほどで説明するのは、かなり難しいが、このようなイメージの図を作って説明している。

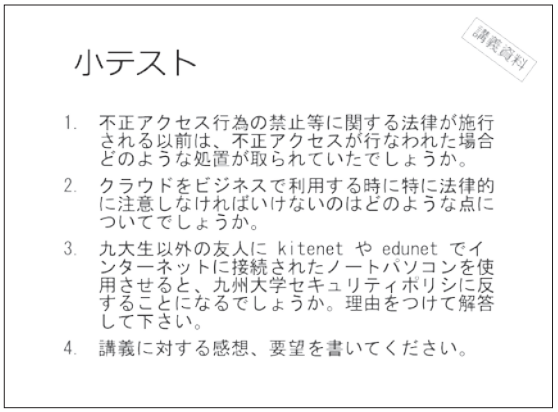

図 7　小テスト（2）

毎回の講義の終わりに実施している小テストが図 7 である。小テストの設問は、授業を聞いていれば概ねわかるような問題を設定している。設問 2 では、クラウドをビジネスで利用する時に特に法律的に注意する点を考えさせている。これは、クラウドサービスというものは、実態がどこにあるかわからないものであるが、何か問題が起きた時には、物理的にデータを保存している機器が設置されている国の法律の元で裁かれることが多い。そのため、クラウドをビジネスで利用する際には、サービスの内容だけでなく、物理的に機

6　http://www.benesse.co.jp/customer/bcinfo/01.html

器が設置されている場所がどこなのか、コピーやバックアップが第三国に持っていかれないかなどについても注意してサービスを選択する必要があると教えている。

設問3には「九大生以外の友人にkitenet[7]やedunet[8]でインターネットに接続されたノートパソコンを使用させると、九州大学セキュリティポリシーに反することになるでしょうか。」という問いを設定している。九大では、全学共通IDとパスワードで出席ができるようになっている。しかし、友人に自分のIDとパスワードを教えて代理出席をしている学生がいるらしく、情報統括本部から対策をしたいと相談を受けての設問であった。授業を通じて、自分のIDとパスワードを他人に教えてはいけないことや、他大学の友人が遊びに来た時に、九大のネットワークを絶対に貸してはいけないということを教えている。また、九大セキュリティポリシーや倫理規定を読むように指導している。

関連する法律についての説明もしている。1987年にコンピュータ犯罪に関する記載が刑法に入った。学生は19歳前後なので、1987年は生まれる前の話になる。そのため、1987年に世の中で起きたことや、NECのPC-98というコンピュータが流行って、10人程で順番に使っていたことや、データの改ざんやコンピュータを使った犯罪が起こるようになったことを歴史に即して話をしている。

1999年に施行された、不正アクセス禁止法[9]についても取り上げている。ふざけてでも、他人のIDを盗むことや、他人のIDでログインをすると、法律で裁かれることになるということを教えている。

そして、大学のセキュリティに関する規定についても紹介している。セキュリティポリシーや情報倫理規定があるが、これまでは、学生に対してそれを説明する機会がなかった。必修科目があれば、このような規定の存在や内容についても説明したいと考えている。

7. 2017年度からの必須化に向けて

2017年度からの必須化に向けてのシラバスは、図8を予定している。内容はこれまでとほぼ同じだが、各項目がほぼ1コマずつになる。ITリテラシーの話と著作権の項目は2コマを予定している。

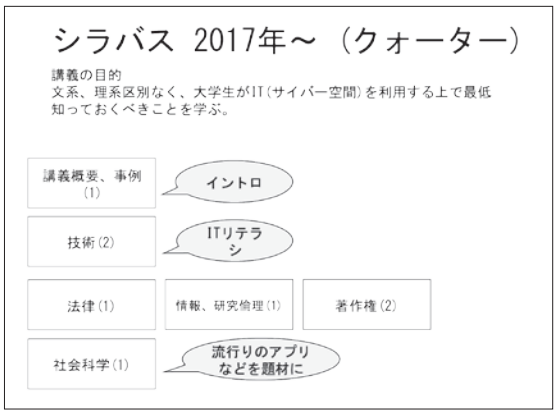

図8　シラバス2017年～

一般的なサイバーセキュリティ教育に用いる科目構成を挙げたものが図9である。サイバーセキュリティの講義のカリキュラムの内容がどの程度網羅しているかを表している。暗号技術や電子署名とPKI、不正プログラム対策や情報セキュリティポリシー、プライバシー保護、法制度は講義に盛り込んでいる。しかし、バイオメトリック認証やデジタルフォレンジック、セキュリティ評価等については、基礎教育では難しいと考え、触れていない。

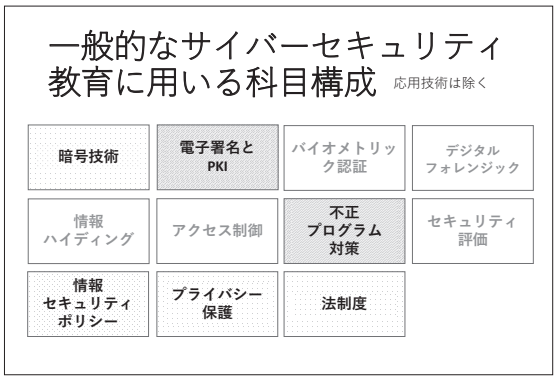

図9　一般的なサイバーセキュリティ教育に用いる科目構成

講義を受講した学生がどの程度のスキルを身に着けられるかを、IPAが定めている7段階のITスキル標準[10]と照らし合わせてみると、レベル1のITパスポートのセキュリティに関する部分は習得できているのではないかと考えている。

7　https://www.nc.kyushu-u.ac.jp/
8　http://ecs.kyushu-u.ac.jp/?page_id=1016
9　http://law.e-gov.go.jp/htmldata/H11/H11HO128.html
10　https://www.ipa.go.jp/jinzai/itss/itss7.html

8. 評価について

平成 26 年度の後期から開講したが、初めの受講者はわずか 38 名だった。過去問がないために学生から倦厭されたのではないかと考えている。しかし、平成 27 年度の後期には 115 名になり、平成 28 年度の前期は 220 名の受講があった。そして、平成 28 年度前期までに歯学部以外、すべての学部から学生が受講している。

評価のテストについて、平成 26 年度は、受講者が少なかったこともあり、期末のペーパー試験で行った。受講者数が増えたこともあり、翌年度からは、Moodle を使ったオンライン試験で 4 択問題に変えた。平成 28 年度は、期末試験は実施せず、毎回 Moodle を使った小テストをするようにした。やはり、記述式は学生からの評判が悪く、採点の評価も難しいため、最近は 4 択問題にしている。

9. 今後の展望

九州大学では、現在、1 学年が 2,600 名なので、150 から 180 名の教室を利用して、平成 29 年度からは 15 クラスの開催を予定している。教員は 8 名で担当する予定である。

試験については、e ラーニングシステムを使って、選択式の問題で行う予定である。これまでの 2 年間で試験問題については蓄積されているので、それらを参考に行っていく。

今後の課題としては、二点が挙げられる。一つは、講義の評価である。全学的に行った教育の成果として、九州大学の学生が本当にセキュリティに強くなったことを何らかの方法で証明することが課題である。一つの方法として、講義を受講する前と後にテストを行い、その点数の結果で評価することが考えられる。

課題のもう一つは、英語での授業である。九州大学では、定員約 300 名の外国人を対象とした学部を新設する予定である。そのため、英語で授業をする必要がある。法律用語等をどうすべきかが課題だ。

これまで 2 年間の講義を行ってきた実績の積み重ねと、学生のフィードバックにより、平成 29 年度からの全学生へのサイバーセキュリティ教育の必須化に向けて、準備が整いつつある。