教育の質を保証するFDの在り方

～ 大学院における情報セキュリティ教育について ～

2010年02月22日
第3回AIIT/KIC FDシンポジウム
パネルディスカッション

情報セキュリティ大学院大学 教授
※　横浜市CIO補佐監
内田　勝也 （ uchidak@gol.com ）

教育の質を保証するFDの在り方

情報セキュリティ大学院大学
アドミッション・ポリシー

アドミッション・ポリシー 博士前期課程

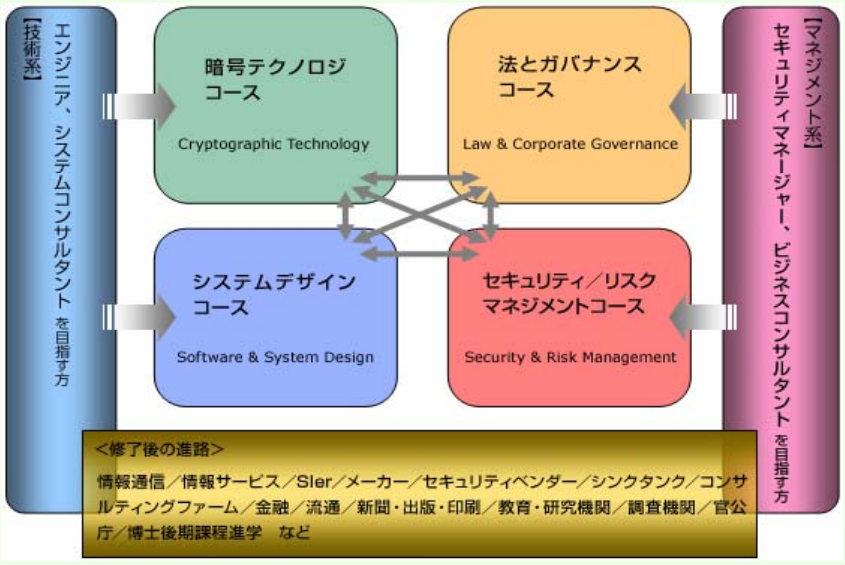
情報科学技術は社会全体に大変大きなインパクトを与え、今後とも社会の中軸を支える重要な技術であると言えます。いまや情報ネットワークシステムは人類共有のインフラストラクチャとしてますます重要な社会的基盤となりつつあります。これにより、生活・経済活動におけるさまざまな利便性が向上する一方、システムの安全性や信頼性に対する脆弱性や情報そのものの暴露、漏洩、改ざんなどのリスクも増大しており、広い視点に立った情報セキュリティの重要性がますます高まっています。しかしながら、これまで既存の大学・大学院においては情報セキュリティに関する教育、研究が体系的になされておらず、当該分野に関する高度な技術、知識、分析能力等を有する人材の不足が深刻な問題となりつつあり、今後の情報社会発展にとって大きな足かせとなり兼ねません。

本大学院大学は、技術、管理・運営、法制度、情報倫理等広範な領域を対象とする学際的総合科学である情報セキュリティについて、それぞれの分野の第一線で活躍する研究者および実務家の力を結集し、高信頼性社会の実現を担う高度で専門的な知識・技術と高い倫理観を備えたプロフェッショナルとして、情報セキュリティにおける技術面での対策を担う情報セキュリティエンジニアと情報セキュリティの運用・管理面でのリーダーとなる情報セキュリティマネージャを養成いたします。

入学者選抜にあたっては、入学後の研究を推進していくうえで必要な基礎学力はもちろんのこと、情報社会に対する倫理観と問題意識、そして、真摯な態度で研究に臨む積極性や主体性を重視いたします。これまでの専門分野に必ずしもとらわれず、新しいテーマに関心があり、さまざまなバックグラウンドを持つ仲間と切磋琢磨しながら、自己実現と社会貢献を目指す方々の入学を希望しています。

教育の質を保証するFDの在り方

情報セキュリティ大学院大学
修士課程コース



- 情報セキュリティ分野と言っても、非常に広範であるが、なかなか理解されない。
- 多くの人たちは、ICT分野の1つだと考えているが、マネジメントや法制度分野が広がっている
- 最近、① 暗号、② コンピュータ、③ ネットワーク、④ マネジメント、⑤ 法制度の5分野と分類している

教育の質を保証するFDの在り方

情報セキュリティ大学院大学
博士前期(修士) 及び博士後期(博士)課程

カリキュラム： 技術・管理運営・法制度・情報倫理を相互に連携、協調させ横断的で創造的な情報セキュリティ教育を目指す

情報セキュリティ輪講Ⅰ	*情報セキュリティ特別講義*	暗号・認証と社会制度	暗号プロトコル
アルゴリズム基礎	数論基礎	暗号理論	計算代数
個人識別とプライバシー保護	インターネットテクノロジ	不正アクセス技法	ネットワークシステム設計・運用管理
セキュアシステム構成論	情報デバイス技術	情報システム構成論	オペレーティングシステム
セキュアプログラミングとセキュアOS	プログラミング	ソフトウェア構成論	セキュリティシステム監査
情報セキュリティマネジメントシステム	**リスクマネジメント**	**セキュアシステム実習**	セキュリティ管理と経営
組織行動と情報セキュリティ	知的財産制度	国際標準とガイドライン	セキュア法制と情報倫理
法学基礎	マスメディアとリスク管理	Presentation for Professionals	統計的方法論
リスクの経済学	統計的リスク管理	情報セキュリティ輪講Ⅱ	特設講義
セキュリティの法律実務	**以上は全て2単位**		
研究指導(6単位)	*プロジェクト研究指導(4単位)*	1年プログラムの場合、研究指導の代わりに、プロジェクト研究指導	

以下は、博士後期(博士)課程

情報セキュリティ特別研究(6単位)	情報セキュリティ博士演習	情報セキュリティ技術特論	情報セキュリティ管理特論

注) 科目名の後ろに単位が記載されていないものは、全て2単位　*赤字* の科目は必修科目

修了要件：

- 博士前期(修士 2年制)課程　年限 = 原則2年　修得単位 = **30単位**以上(含 研究指導6単位)　修士論文
- 博士前期(修士 1年制)課程　年限 = 原則1年　修得単位 = **46単位**以上(含 プロジェクト研究指導4単位)　プロジェクト研究
- 博士後期(博士)課程　年限 = 原則3年　修得単位 = 8単位以上　博士論文

科目履修(最大10単位修得可能)制度も活用されている

博士前期(修士 2年制)では；

- 1年目は平日夜間3日程度と土曜日で、所要単位を取得。(夜間：18:20～19:50、20:00～21:30　土曜日：9:00～16:50)
- 2年目は研究指導(修論作成)を中心にして、卒業を目指している。 社会人で昼間を利用する学生は1、2名程度

博士後期課程：①修業年限：3年以上(教授会が優秀な研究業績者と認めた者は1年以上)　②所要単位：8単位以上
③博士論文審査および最終試験

教育の質を保証するFDの在り方

情報セキュリティ教育の困難さ

情報セキュリティ分野での誤解(都市伝説)

1．2002年7月、当時の米国大統領重要インフラ保護委員会 の副委員長 ハワード・シュミットは、インタビューで、『米国国防総省(DoD)が行った2001年の調査では、**国防総省への攻撃の97～98%の攻撃はパッチ適用をしなかったか**、設定ミスである』と述べている
http://www.govtech.com/gt/articles/18492

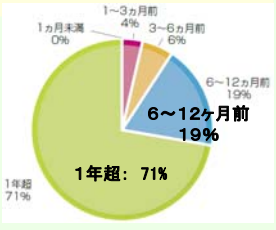
2．情報漏えいの原因

(1) InfoWatchの調査では2006年に世界各国で起きた情報流出事件のうち、1回でもメディアで取り上げられた150件のうち、**過失が77%で、業種や地域による偏りはなく**、大企業や中小企業、政府機関、軍などで流出が発生している
http://www.itmedia.co.jp/news/articles/0702/17/news011.html

(2) 内閣府国民生活局
「個人情報の保護に関する事業者の取組実態調査」
H19年3月実施。回答数 4,060件(回収率 20.3%)
http://www5.cao.go.jp/seikatsu/shingikai/kojin/20th/20070425kojin2.pdf

漏えい発生原因	回答(%)	
1．従業者の置忘れ、施錠忘れ等の過失	21.3	
2．従業者のインターネット利用上の過失(メール誤送信、HPへの誤掲載等)	8.6	
3．従業者(含 退職者)が盗難にあった(含 車上荒し)	14.2	
4．委託先・運送業者の漏えい等	17.6	61.7
5．サーバ／PCへの攻撃(ハッキング・ウイルス感染)	2.8	
6．従業者の個人情報持出し、売却・譲渡・漏えい等	3.6	6.4
7．原因は未だに不明である	5.4	5.4
8．その他	25.8	25.8
9．無回答	0.7	0.7

3．2008年Verison Businessの調査：　右図「脆弱性によるデータ漏洩／侵害の何ヵ月前に、その脆弱性のパッチが提供されていたか」
http://www.verizonbusiness.com/resources/whitepapers/wp_supplemental-report-specifics-for-the-financial-services-food-beverage-retail-and-tech-services-industries_en_xg.pdf



侵入は、オペレーティングシステムよりもアプリケーションが標的になっており、攻撃の4分の1弱は脆弱性を利用した攻撃。 **攻撃を受けた脆弱性の90%は、その攻撃の6ヶ月以上前にパッチが提供されており、パッチを当てていれば侵入を防止できた**

情報セキュリティ教育の困難さ

ウェブサイト管理者へ：ウェブサイト改ざんに関する注意喚起
一般利用者へ：改ざんされたウェブサイトからのウイルス感染に関する注意喚起

- 閲覧した利用者のパソコンにウイルスを感染させることを狙ったウェブサイトの改ざん事例が発生しているため、ウェブサイト管理者等へ注意を喚起し、ウェブサイトの運用を再度見直すことを推奨します
- 改ざんされたウェブサイトの管理者は、被害者に留まらず、閲覧した利用者のパソコンにウイルスを感染させてしまう加害者となります。このような被害の拡大を防ぐため、ウェブサイトの管理者は、運営しているウェブサイトが改ざんされていないか確認し、ウイルスの“ばらまきサイト”に仕立て上げられないようにしてください

(1) ウェブサイト改ざんの概要と主な原因

- ウェブサイト改ざんの原因として、ftp※のアカウント情報の盗難事例がある。 盗んだ ftp アカウント（ID/パスワード）を使い、正規のユーザになりすまし、改ざんしたページをウェブサーバに公開（アップロード）する
- ftp のアカウント情報を盗む手口は、スパイウェアをターゲットのパソコンに送り込むなどの方法が一般的です

※File Transfer Protocol の略。ネットワークでファイルを転送するためのプロトコル。

- 改ざんされたウェブページには不正なスクリプトが埋め込まれ、そのページを閲覧した一般利用者を、ウイルスが仕掛けられた悪意あるウェブサイトにアクセスさせます。一般利用者が悪意あるウェブサイトを閲覧した場合、利用者のパソコンに脆弱性があると、それを悪用されウイルスに感染させられてしまいます

（抜粋） http://www.ipa.go.jp/security/topics/20091224.html

スパイウェアを送り込まれる原因・・・

- メールに添付されたファイルをクリックしたため
- インターネット経由でダウンロードするフリー・ソフトウェアにバンドルされている
- ポップアップ・ウインドウ、ActiveX技術、Web ブラウザ等のセキュリティ・ホールを利用
- FTPのユーザID/パスワード盗難： 約8,700件 日本企業も

（2008.2.27 http://www.finjan.com/Pressrelease.aspx?id=1868&PressLan=1819&lan=3）

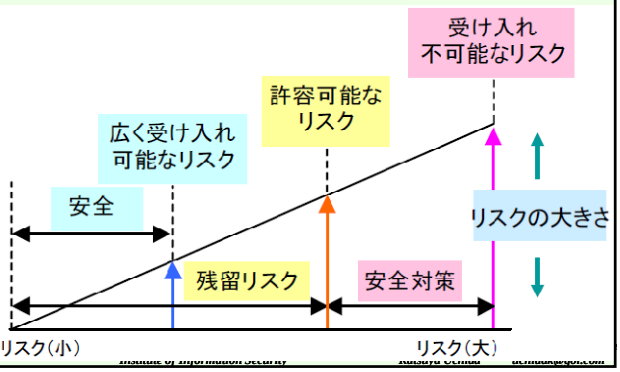
教育の質を保証するFDの在り方

情報セキュリティ教育の困難さ

安全と安心 (1)

- 安全を“絶対に事故が起きないこと”と解釈している人がいるが，これは間違いである。無論，絶対に事故が起きないことは理想ではあるが，これは，「何もしない」こと以外，確実な実現は不可能だからである。「何かする」以上，安全を脅かす何かは必ず存在する。問題はその何かを人知を尽くしてコントロールすることにある。
- 具体的には，リスクという考え方が必要となる。機械やシステムの分野では，絶対安全はあり得ないとして，安全は，「人への危害または損傷の危険性が，許容可能な水準に抑えられている状態」（ISO8402：品質管理及び品質保証－用語の定義），または，「受け入れ不可能なリスクが存在しないこと（受け入れることの出来ないリスクからの開放）」（ISO/IECガイド51：規格に安全面を導入するためのガイドの定義）と定義されている。安全が絶対安全を意味しているのではなく，“常に危険性（リスク）は残されており，それが許容可能，または受け入れ可能なもののみになっていること”としている。ガイド51 の安全の定義にはリスク(risk)という用語があり，安全はリスクを経由して定義されている。

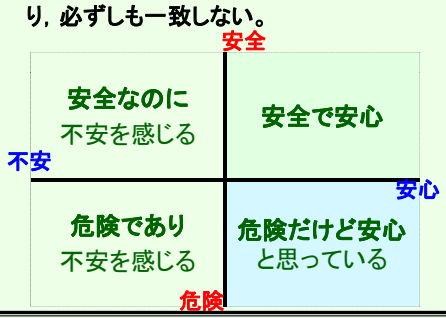
ISO8402の定義にある「人への危害または損傷の危険性」とは，リスクのことで，リスクとは，「危害の発生する確率及び危害のひどさの組み合せ」と定義されている。ここで“組み合せ”とは，危害の発生確率の大きさと危害の大きさとの両方を勘案して，リスクの大きさを決めることを意味し，発生確率が大きいほど，また危害が大きいほど，リスクは大きく設定しなければならない。



情報セキュリティ教育の困難さ

安全と安心 (2)

- 安全は，科学技術，社会技術の問題として論理的に，客観的に，数量的に評価される試みが行われている。リスクという概念が用いられ始めたのは，このためと考えられる。安全は科学技術や社会技術として実現させることを通して，客観性を重んじる方向を目指して発展してきている。しかし，安全の定義にリスクの概念が用いられ，リスクには危害のひどさという主観的な面が含まれており，また，安全目標には価値観が含まれているので，安全をすべて客観的に，技術的に取り扱うことは困難。
- 一方，安心は主観的に判断され，個人によって大きく異なる。人間の心理に深く根ざしている。
  安心について，人が知識・経験を通じて予測している状況と大きく異なる状況にならないと信じていること，自分が予想していないことは起きないと信じ何かあったとしても受容できると信じていること
  安心は，“信頼する”という人間の心と強く関係している。
- 安全の反対は危険であるが，安心の反対概念は，心配，ないしは不安であろう。安全であることは安心に大きく貢献するはずであるが，安全であっても安心できない例，逆に安心しているが実は安全でない例もあり，必ずしも一致しない。



平成2005年8月31日

安全・安心な社会構築への安全工学の果たすべき役割

日本学術会議 人間と工学研究連絡委員会安全工学専門委員会

http://www.scj.go.jp/ja/info/kohyo/pdf/kohyo-19-t1034-1.pdf

「事故前提社会」とは、事故が有り得るから諦めて事前予防に向けた対策を行なわないとか、どのような被害にあっても、それは仕方ないものであると諦めさせるとかいうことを意味するものでは決してない。

2008年6月19日
情報セキュリティ政策会議「次期情報セキュリティ基本計画に向けた第1次提言」

なぜ、「事故前提社会」という言葉を使わなければならないのだろうか？
「安全・安心な社会」の方が分かり易いし、前向きな感じがするのだが。

講座：情報セキュリティマネジメントシステム

1. 授業のねらい

情報セキュリティは、技術、管理・運用、法制度の三位一体の対応が大切であるが、管理・運用面で重要な役割を果たすものとして情報セキュリティマネジメントシステム（ISMS）がある。企業・組織における情報セキュリティの総合的な管理体制の確立を目指すものであり、また、この管理システムに基づいた適合性評価制度は国内だけでなく、国際的な推進がなされている。情報セキュリティ管理体制を構築するために必要な考え方について総合的な観点から学習する。

2. 授業計画

講義形式での授業を中心とするが、グループでの討論、プレゼンなども計画

1) オリエンテーション（講義の概要、目標、評価方法など）
2) 企業・組織と情報セキュリティ
3) 情報セキュリティマネジメントシステムの歴史、背景
4) セキュリティ実施基準
   (1)セキュリティ基本方針、情報セキュリティのための組織
5) (2)資産の管理
6) (3)人的資源のセキュリティ、物理的及び環境的セキュリティ
7) (4)通信及び運用管理
8) (5) アクセス制御
9) (6) 情報システムの取得、開発及び保守
10) (7) 情報セキュリティインシデントの管理
11) (8) 事業継続管理、順守
12) 監査
13) 経営者の責任とマネジメントレビュー
14) PDCAサイクル
15) 情報セキュリティマネジメントシステム認証制度

3. 教科書

特に指定しない。

4. 参考書

（財）日本情報処理開発協会（JIPDEC）が、「情報セキュリティマネジメント適合評価制度」について多くの資料を作成している。（URL: http://www.isms.jipdec.jp/ ）これらを参考に使用する。　その他の参考文献、URLなどには適宜紹介する。

5. 関連科目

なお、企業等での勤務経験があることが望ましい。企業・組織での勤務経験がない受講生については、後期での選択が望ましい。

6. 成績評価の方法

教育の質を保証するFDの在り方　講座：情報セキュリティマネジメントシステム

授業評価：コメント（その１）

- 授業内容が講義だけでなく、考えたりディスカッションをする時間があったので内容に興味を持つ事ができました。 情報セキュリティ方針のプレゼン発表は一番最初だったという事もあり少し大変でした。 会社ではISMSを取得していないため、ISMSの概念について学ぶ機会が得られて非常に良かったです
- ISMSを客観的に学ぶことができて、とても有意義な授業でした。ありがとうございました
- 当初はISMS適合評価制度に関する講義だと思ではなくセキュリティマネジメントとして幅広い内部分が多く、非常に有意義な授業でした
- 大変、参考になる内容が多かったと思います。 疑問としては、実際にどのようにして実践するかというのがあります（自分のテーマでもあります）
- 当初は固い授業を想像していたが、予想に反し、楽しくISMSについて学べました。授業を受けて、自社のセキュリティマネジメントシステムやISMS自体の問題も見えてきました。 得た事を業務に活かしていきたいと思います。 ありがとうございました
- 情報セキュリティポリシーを作成して発表する演習は、色々な人の考えを知ることができて面白かった

講義の限界かも知れません。 実践的なコースを作るとか、審査員コースに参加するとか考えられる

教育の質を保証するFDの在り方　講座：情報セキュリティマネジメントシステム

授業評価：コメント（その２）

- いくつかの会社（様々な職種）の情報セキュリティ基本方針が見られる（比較できる）と興味深いと思いました。 ISMSを全てわからない状態で受講したので、全体的なこと、キーポイントの両方を学ぶことができ、良かったです
- 演習や発表が、今思いますと、とても勉強になりました。 実際に授業で話を聞いていても、実践にすぐに活かすことが難しいとも今日の演習で感じました。 ISMSをこのように一から学ぶ機会がなかったので、今までISMSに思っていた疑問が解決されて良かったと感じています。 先生の授業、とても楽しかったです
- 反面教師的事例が多かったように感じました。 ISMSを正しく扱っている例を多目に取り入れていただけるとよかったかと思いました
- 情報セキュリティポリシーの作成と発表、ディスカッションが非常に有意義でした。本講義により「ISMSとはどういうものか」と言うことがよく理解できた。 最終課題は何を注意すべきかを改めて考えることができた
- ありがとうございました
- ISMSだけでなく、ISMSに対する考え方のようなものが含まれていて良かったです
- 考え方が勉強になった

情報セキュリティ分野（ISMS、リスクマネジメント等）の授業について

- PBLをやるには、学生の情報セキュリティの知識が十分でなく、知識の偏りが起こる心配をしている（やり方を考えることで解決できるかも知れないが）
- コマシラバスも考えていない ⇒ 毎回（半期毎）に講義資料の見直しは行っており、10～30%程度の改訂を行っている
- ISMS授業では、講義だけでなく、以下のようなことも行っている
  - セキュリティポリシーを各自作成し、プレゼンで、他学生から質問・コメントを受ける（全員）
  - 4～6名程度の複数チームで、ある企業の「プレスリリース」をみて、何があったかを推測させる
  - VTRを視聴させ、① 最も印象に残った内容（事件等）を3つ以上、② 内容的におかしいと思ったこと、③ 理解できなかったこと／単語、を提出させ、後日簡単な解説を行う
-

教育の質を保証するFDの在り方　講座：情報セキュリティマネジメントシステム

情報セキュリティ分野（ISMS、リスクマネジメント等）の授業について

- ISMS推進現場で発生している共通的な問題・課題等を述べるとともに、その解決方法等も解説
  - 2年に1回、ISMS認証取得事業所に対して、調査を行っており、そこからの情報
  - ISMS審査判定委員会（委員長）での課題・問題等について、一般化している
- 実務的な要素が多いため、社会人経験のない学生は少し苦労している
- 属人的な要素が多いと感じている
  - 日々、進歩がある分野では属人的にならざるを得ないと考えている
  - 他の教員に授業内容の評価をして貰うことの難しさもある

ロ 研究室学生について

- 研究指導（修論・輪講等のため）の時間は、積極的に発言を求め、学生に上下関係はなく、議論を勧めている
- ISMS認証取得事業所調査（2年に1回）、 情報セキュリティ調査（1年1回）等のセキュリティ調査では研究室学生が中心に全ての内容について実施している

ありがとうございました

ご質問・コメントがございましたら ・・・・

電子メールでのご質問・コメントはいつでもどうぞ

情報セキュリティ大学院大学
（http://www.iisec.ac.jp/）

教授 内田 勝也

uchidak@gol.com
http://www.uchidak.com/

本資料は、http://www.uchidak.com/ に保存します

本資料は、個人の見解であり、所属組織の考えではありません

（2010年3月末にて、情報セキュリティ大学院を定年退官します）