情報セキュリティ人材育成・資格制度について

内閣官房情報セキュリティ政策会議
人材育成・資格制度体系化専門委員会

２００６年８月３０日

情報セキュリティ大学院大学
内田　勝也(uchida@iisec.ac.jp)

事前の質問について

下記事項について、可能な範囲で説明を

1. 学生の概要：専攻の概要と年齢・バックグラウンド(純粋な学生か企業からの派遣か等)、人数、就職状況(希望と実際の就職先)等
2. 情報セキュリティ教育のカリキュラムの概要：授業内容・所要単位、授業形態、時間、講義と技術実践の割合等
3. カリキュラム構築に当たっての考え方：スキル整理や人材ニーズ調査の方法・結果、資格制度との関係、就職への考慮等
4. 情報セキュリティ教育についての学術・研究と就職先のニーズとの関係：企業ニーズとのギャップの有無・内容、解決策
5. 我が国全体としての情報セキュリティ人材の現状と評価：必要とされる(重視される)技能・人材、不足している技能・人材、求められる技能・人材と処遇面のミスマッチ等
6. 情報セキュリティ人材の育成に関連する制度(企業の採用方針・処遇、官民の各種資格制度、教育制度等)に対する評価・要望等：「情報セキュリティ人材の重要性が企業内で評価されていない」、「現存のこの資格・制度は役に立たない・この点を改正すべき」、「こんな制度・資格が欲しい」、その他、企業・資格機関・他の教育機関(他の大学、専門学校等)・行政側に対する評価・要望等
7. その他：高等教育機関の立場から見た情報セキュリティ人材の育成・確保に関しての提言、要望、参考となる事項

はじめに

本学の設立経緯

- 2001年9月11日の米国同時多発テロをTVに見ていた理事長が、日本でも情報セキュリティを専門とする学生を育成する必要を感じ、当時の某総研理事長に大学院の設立の相談をした。
- 某総研理事長は、顧問をしていた林（現 副学長）に対して、大学院設立の支援をして欲しいと依頼した。
- 林は、経済・法律等の分野には明るかったが、全般的な情報セキュリティについては専門外であったため、中央大学 辻井（現 学長）に相談を持ちかけた（辻井は2004年3月で、中央大学を定年退官することになっていた）。
- 当時、辻井は中央大学21thCOEの拠点リーダであり、また中央大学研究開発機構での情報セキュリティ人材育成の代表者であったが、情報セキュリティ専門の大学院を作るのであれば、技術、管理・運用、法制度、倫理等を相互に連携、協調させ横断的で創造的な情報セキュリティの研究・教育を目指す大学院を設立することを考えた。

このような経緯で、2004年4月に情報セキュリティ大学院大学が設立

情報セキュリティ大学院大学の概要

1. 学生の概要：専攻の概要と年齢・バックグラウンド（純粋な学生か企業からの派遣か等）、人数、就職状況（希望と実際の就職先）等

- 8割は社会人（企業派遣と自費が半分程度）
- ベンダーからの学生が大部分。 ユーザ企業からの入学は大半が自費
- 年齢は学部卒から定年後まで。 中心は30台前半
- 今年度は、修士：約80名、後期博士課程（初年度）：14名
- 就職：2006年3月が一期生の卒業で、数名の就職状況。概ね希望通り

2. 情報セキュリティ教育のカリキュラムの概要

- 授業内容・所要単位：次ページ以降に
- 授業形態、時間：
  昼間の授業もあるが、学生は夜間・土曜日を利用している
  夜間・土曜日中心（90分×15回＝2単位、実習は30回=2単位）
- 講義と技術実践の割合等： 必修科目として技術実践はありません
  - **セキュアシステム実習**：防御・攻撃システム環境を構築し、攻撃・防御を実際に行いながら知識・技能を学ぶ 270分×10回
  - **プログラミング**：C言語による実習 90分×15回
  - **ソフトウェア構成論**： Javaの実習 90分×15回
  - **リスクマネジメント、情報セキュリティマネジメントシステム**：ケーススタディ、グループ討議、プレゼンテーション等を含めて行っている 90分×15回
  - **プレゼンテーション技法**：模擬記者会見，プレゼンテーション 90分×15回

	月	火	水	木	金	土
1						
2						
3						
4						
5						
6						

1						
2						
3						
4						
5						
6						

1時限 9:00～10:30 1時限 9:00～10:30
4時限 14:40～16:10 4時限 14:40～16:10
5時限 18:20～19:50 5時限 16:20～17:50
6時限 20:00～21:30

修士課程での授業

- 前期・後期の授業分布
- ダブルトラックは少ない
  前期：1コマ、後期：4コマ
- 研究指導は火曜日5・6限だが、指導教員による
- 平日3、4日程度、土曜日の出席で修了可能

情報セキュリティ人材育成・資格制度について

情報セキュリティ大学院大学
修士課程

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

	授業科目名	履修区分	単位数	修了に必要な単位数
専門基礎	情報デバイス技術	選択	2	8
	プログラミング	選択	2	
	インターネットテクノロジ	選択	2	
	アルゴリズム基礎	選択	2	
	数論基礎	選択	2	
	セキュア法制と情報倫理	選択	2	
	セキュリティ管理と経営	選択	2	
	プレゼンテーション技法	選択	2	
	情報セキュリティ輪講Ⅰ	必須	2	
	研究指導	必須	6	6

	授業科目名	履修区分	単位数	修了に必要な単位数
専門	計算代数	選択	2	16
	暗号理論と電子認証	選択	2	
	暗号プロトコル	選択	2	
	個人識別と個人情報保護	選択	2	
	情報システム構成論	選択	2	
	オペレーティングシステム	選択	2	
	セキュリアシステム構成論	選択	2	
	セキュリアシステム実習	選択	2	
	ソフトウェア構成論	選択	2	
	セキュリアプログラミングとセキュリアOS	選択	2	
	不正アクセス技法	選択	2	
	ネットワークシステム設計・運用管理	選択	2	
	セキュリティシステム監査	選択	2	
	情報セキュリティマネジメントシステム	選択	2	
	セキュリティの法律実務	選択	2	
	リスクマネジメント	選択	2	
	セキュア社会制度論	選択	2	
	情報セキュリティ輪講Ⅱ	選択	2	
	情報セキュリティ特論	必須	2	

■ 修了要件

以下の3つの条件を全て満たすこと

- 修業年限：2年以上
- 所要単位：30単位以上
  - 専門基礎科目 8単位以上（含必修2単位）
  - 専門科目 16単位以上（含必修2単位）
  - 研究指導 6単位
- 修士論文など
  - 修士論文及び最終試験

上記は、修士2年コースの例で、多くの学生は、

- **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**

修士1年コースは、修士論文の代わりに課題研究（リサーチペーパー作成）を行い、所要単位は46単位以上

後期博士課程：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

情報セキュリティ人材育成・資格制度について

情報セキュリティ大学院大学
情報セキュリティ管理者（CISO）コース

コース概要： 2007年4月開講予定

対象者	企業、自治体等で、3年以上の勤務経験を有し、コンピュータの知識があることが望ましい。CISO（情報セキュリティ管理者）を目指す人を対象
研修期間	4月～7月 及び 10月～2月初（約4ヶ月 年2回開講予定）
育成目標	• 企業や自治体において、情報セキュリティを統括して考えることのできる管理職（役員補佐）の育成を目指し、経営トップに情報セキュリティ政策を具申できる知識・能力を持った者を目指す • 大規模なセキュリティインシデント発生時に、経営者を補佐し、関連部門を統括して対応できる人材の育成 • 1つの企業・組織で通用するだけなく、他の企業・組織でも通用する経営的な専門知識を持った情報セキュリティ専門家の育成を目指す • 情報セキュリティの理論（座学）だけでなく、実践に対する知識・経験を持つ者を目指す。　実践講座の履修は必須 • 個人としての知識・技術だけでなく、プロジェクトマネジメントができる情報セキュリティ管理者の育成を行う
科目受講	• 受講科目の内、選択4科目以上、必修1科目を選択する • 特別講座「① プロジェクトマネジメント講座」及び、「② セキュリティ基礎講座」は履修が望ましい。但し、既に資格を取得している場合は不要 • 選択科目は6科目を越えない範囲で入学期間の翌期間まで履修できる
修了条件	• 選択科目：　4 科目以上 • 必修科目：　1 科目 • 本学の実施するCISO資格試験に合格した者 または SANS GIAC（GSEC）またはCISSP 資格合格者
受講科目	必須 セキュアシステム実習 選択 セキュリティ管理と経営、セキュリティの法律実務、セキュア法制と情報倫理、セキュア社会制度論、暗号・認証と社会制度、プレゼンテーション技法、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、セキュリティシステム監査、個人識別と個人情報保護、インターネットテクノロジー 特別講座：① プロジェクト・マネジメント　② セキュリティ基礎講座（CISSP／GIACの内容）
修了資格等	• 情報セキュリティ管理者（CISO）資格を授与 • 大学院授業については、科目選択を行ったものとし、単位を付与し、大学院へ入学した場合、最大10単位までは履修済みとみなす。（選択科目、必修科目の合計で10単位まで）

情報セキュリティ人材育成・資格制度について

ご質問に関するもの

3．カリキュラム構築に当たっての考え方

- スキル整理や人材ニーズ調査の方法・結果：**個人的には、以下の事柄等が大きな影響があった**
  - 1998年6月、NetSec'98 基調講演で、Purdure大学のEugene Spaffordは、「いわゆるハッカーを雇う必要はない。**我々の大学の学生は、ハッカーに対して優とも劣らない**」と発言で、米国のセキュリティ教育に興味を持った
  - 2000年10月、米国**SANS**主催「Firewall講座」（5日間）に参加。 講師のレベルの高さ、受講者数（約500名：全体では2,000名程度？）に愕然（http://www.sans.org/）
  - 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%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.net/magazine/sup_story.phtml?id=18492
  - 2003年8月に始めた中央大学 情報セキュリティ人材育成で考えていたことを大学院で適用したかった
    http://www.mext.go.jp/a_menu/kagaku/chousei/unyo/saitaku/15/03061901/002/066.pdf
    http://www.mext.go.jp/b_menu/houdou/17/12/05122703/011/006.htm
- 資格制度との関係：**国内における特定の資格制度は考えていなかった**
  - マネジメントやネットワーク技術者に対しては、SANS等の米国のシステムの良さと日本の特徴（法制度、企業風土等）を取り入れたものを構築する必要があると思っていた
  - 但し、短期で行うものは、資格制度を考えたいと思っていた。
    ・基礎（入門でなく）、・プロジェクトマネジメント、・ネットワーク実践（セキュアシステム実習）
- 就職への考慮等：**マネジメント系に学部学生を受けいれる可能性は少ないと判断していた**
  - 社会人学生の割合が高いと考え、学生が就職する可能性は少ない。
    ⇒ 15％以下：2006年3月 3人、 2007年3月 6人程度

情報セキュリティ人材育成・資格制度について

ご質問に関するもの

4．情報セキュリティ教育についての学術・研究と就職先のニーズとの関係

- 企業ニーズとのギャップの有無・内容
  - 企業とのギャップはある。 ギャップ以前の問題（必要性を感じていない？）かも知れない
  - 国内の企業・官庁・自治体等で、プロフェッショナルとして認められるのは、「医者、弁護士、会計士」等であり、情報システム、情報セキュリティ分野を同等な仕組みを考えられない限り、ギャップを埋めることは不可能ではないかと考えている
  - あるいは、企業等の管理職・役員を「プロフェッショナル」であるという考え方が一般的になれば可能性はあるかも知れない
  - 開校前に、マスコミ等から、これほど多くの学生が必要なのかと言われた。 「**証券アナリスト**」や「**マスコミで情報セキュリティ専門記者**」になる卒業生がいても良いのではないかと思っている
- 解決策：**単純な解決策はないと考えている。 真のプロフェッショナルを育成することが解決策では**

例1：某自治体でのプール事故 ⇒ ここからでも情報セキュリティ分野の教訓は得られる
- 受託事業者（含 監視員）の問題
- 市側の問題
- 文部科学省（全国一斉点検の指示）の問題

例2：2005年6月：価格比較サービス大手のサイトの不正アクセスをした留学生の自宅から押収したパソコンに、利用者のメールアドレスなどの個人情報計約9万件が保管されていることが判明。**サイトの欠陥**をつき、外部から不正な命令を入力しデータベースを直接操作する「**ＳＱＬインジェクション**」を使用。攻撃用ソフトは、中国語のインターネットサイトから入手
- 企業・組織の情報セキュリティ担当者であれば、この事件から学ぶことは多いはずだが

情報セキュリティ人材育成・資格制度について

ご質問に関するもの

5．我が国全体としての情報セキュリティ人材の現状と評価

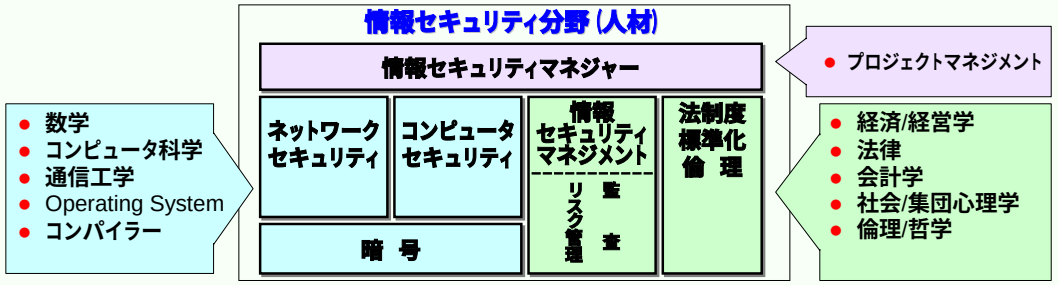
- 必要とされる（重視される）技能・人材
  - 必要な人材は、非常に広範囲になっている。
- 不足している技能・人材
  - 情報セキュリティの全ての分野

下図に示した様な人材が、情報セキュリティ分野で必要とされているが、足りている感じはない

- 求められる技能・人材と処遇面のミスマッチ等
  - 情報セキュリティ分野は技能（技術能力）だけではなく、マネジメント能力等も必要と考えている
  - 処遇面以前に、情報セキュリティをプロフェッショナルなものと考えられているかが疑問
  - 「技能 = プロフェショナル」であるとすれば、どの分野でも昔も今もプロは常に足らない

不幸の始まり！

- 情報セキュリティのある分野の専門家が他の分野を詳しいとは限らない
- しかし、情報セキュリティに詳しくない人は、情報セキュリティは1つの分野だと思っている



情報セキュリティ人材育成・資格制度について

ご質問に関するもの

- **情報セキュリティ人材の育成に関連する制度**
  - 企業の採用方針・処遇： 情報セキュリティ人材の重要性が企業内で評価されていない
    - ITC業界等のベンダーでは少し理解されてきたが、ユーザ部門はまだまだという感じがする
  - 官民の各種資格制度、教育制度等に対する評価・要望等、現存のこの資格・制度は役に立たない・この点を改正すべき
    - 資格保持期間を有期にし、継続教育を取り入れて欲しい
    - 一部の資格制度では「質より量を」重視する改正（悪？）が行われているが、自殺行為では？
    - 受験者、有資格者の多寡を評価基準にしないで欲しい（予算措置等に問題があるとの話を聞くが）
  - こんな制度・資格が欲しい

- **その他** 企業・資格機関・他の教育機関（他の大学、専門学校等）・行政側に対する評価・要望等
  - 高等教育機関の立場から見た情報セキュリティ人材の育成・確保に関しての提言
  - 要望、参考となる事項
    - **個人に対する奨学金／減税制度を考えて欲しい**
      現在、本学に通学している社会人学生の内、私費で通学している者がいる
      学習意欲は高いが、学費等で苦労している。 奨学金／減税を考えて欲しい
    - **セキュリティ減税を行う企業には、自社内のポータルに利用可能教育機関等のURL等を掲載**することを積極的に推進して欲しい

政府、NICTや自治体に一定期間勤務で返済不要の奨学金制度等
米国はこの制度がある

情報セキュリティ人材育成・資格制度について

参考： 影響を受けた情報セキュリティ関連

1970年代後半 1980年代前半	米系銀行にて　データセンター運営を行っており、米系銀行の安全対策に関与 内部統制部で、システム監査、業務監査に従事
1993年～現在 1998年6月	米国CSI（Computer Security Institute）の国際会議に毎年参加 NETSEC'98 基調講演で、Purdure大学のEugene Spaffordは、「いわゆるハッカーを雇う必要はない。我々の大学の学生は、ハッカーに対して優とも劣らない」と発言。米国のセキュリティ教育に興味を持った
1998～2000年	情報セキュリティを体系的に学べないか考え、主に米国の大学／大学院等のウェブ等を調査
2000年10月	米国SANS主催「Firewall講座」（5日間）に参加。 講師のレベルの高さ、受講者数（約500名：全体では2,000名程度？）に愕然（http://www.sans.org/）
2001年4月	「情報セキュリティ事典」（共立出版）で編集委員に。また、 企業の技術者・管理者教育を２００１年末に執筆（刊行は２００３年７月）
2002年6月	２００２年６月：日本セキュリティマネジメント学会 全国大会にて、「技術者・管理者向け情報セキュリティ教育試案」の報告を行った（2003年4月 同学会誌 査読論文に採録）。
2002年10月	中央大学２１世紀COE「電子社会の信頼性向上と情報セキュリティ」開始。 事業推進者（総論：情報セキュリティ総合科学の概念形成、コンピュータセキュリティ、情報セキュリティーマネジメント）に
2003年前期	中央大学 理工学研究科（修士） 副専攻にて「Network Security」講座担当（参照：セキュリティ教育）
2003年8月	中央大学 研究開発機構「情報セキュリティ・情報保証人材育成」（文部科学省 科学技術振興調整費） http://www.mext.go.jp/a_menu/kagaku/chousei/unyo/saitaku/15/03061901/002/066.pdf http://www.mext.go.jp/b_menu/houdou/17/12/05122703/011/006.htm
2004年4月 2006年4月	情報セキュリティ大学院大学開校 修士課程（ISMS、セキュアシステム実習、リスクマネジメントを講義） 後期博士課程開講

Eugene Spafford：「UNIX & インターネットセキュリティ」の著者。１９８８年の「インターネットワーム」事件の対応をした一人（ACM「The Worm Story」で、"Crisis and Aftermath"を執筆）

NETSEC'98：（http://www.gocsi.com/）：米国コンピュータセキュリティ団体CSI主催の国際会議・展示会。毎年6月開催、2006年で16回目。
11月開催のAnnual Conf. & Exhibitionは2006年で33回目。

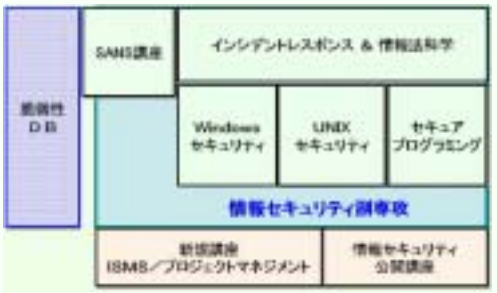
情報セキュリティ人材育成・資格制度について

参考：情報セキュリティ人材育成

技術者・管理者向け情報セキュリティ教育試案
（2002年6月　日本セキュリティ・マネジメント学会　全国大会）

メインフレーム時代、「システムプログラマー」がどこのユーザにもいたのだが・・・

中央大学「情報セキュリティ・情報保証人材育成」
（2003年8月～2008年3月 文部科学省 科学技術振興調整費）



参考：情報セキュリティの特質

情報セキュリティと安全工学

- 安全工学では、原則として「内部・外部を含めて意図的な脅威」は考えない
- 情報セキュリティでは、意図的脅威も考える必要がある

情報セキュリティの製品・サービス

- 大分部の製品・サービスは「対症療法的」であり、「根本療法的」なものほとんどない
  インシデントが起こってて始めて、その対応を行う仕組み
  例：アンチウイルスソフト、侵入検知システム（IDS）

コンピュータ／ソフトウェア科学

- ソフトウェア技術から「根本療法的」な解決方法への試みは始まっているが
  例：「社会基盤としてのセキュアコンピューティングの実現方式の研究」（2000～2004 東大米澤教授Gr）
  「セキュリティ開発ライフサイクル」マイクロソフト社
- システム開発ライフサイクル（SDLC）を考えた情報セキュリティ対策
  例：元米国大統領重要インフラ保護委員会委員長、Howard Schmidtは、2005年10月のSecureLondon 2005会議で、「多くの大学では、安全なプログラムを書く教育が行われていない。使い勝手、拡張性、管理の容易性等を教えているが、セキュリティについての教育が行われていない」と述べている。

特に、アプリケーションシステム開発者やオープンソース等に関係する技術者は、
セキュアなシステム開発が要求される・・・

参考：情報セキュリティ カリキュラム

情報セキュリティ教育

1	Introduction: Role of security, Types of security, Definitions
2	Classification Schemes, Access Control
3	Formalisms: Information flow, Protection Models
4	Policy: Risk Analysis, Policy Formation, Role of audit and control
5	Formal policy models
6	Cryptography: Cipher methods, Key management, digital signatures
7	Authentication and Identity
8	System Design principles. TCB and security kernel construction, Verification, Certification issues
9	System Verification
10	Network Security. Distributed cooperation and commit. Distributed authentication issues. Routing, flooding, spamming. Firewalls
11	Audit Mechanisms
12	Malicious Code: Viruses, Worms, etc.
13	Intrusion Detection and Response
14	Vulnerability Analysis
15	Physical threats, operational security, Legal and Societal Issues

Purdue大学（Computer Science、Master）の「Information Security」シラバス　講義資料、参考資料等全てインターネットで公開

1	What Is Information Security?
2	Type of Attacks
3	Hacker Techniques
4	Information Security Services
5	Legal Issues in Information Security
6	Policies
7	Management Risk
8	Information Security Process
9	Information Security Best Practices
10	Firewalls
11	Virtual Private Networks
12	Encryption
13	Intrusion Detection
14	UNIX Security Issues
15	Windows 2000/Windows 2003 Security Issues
16	Internet Architecture
17	E-Commerce Security Needs
18	Wireless Security

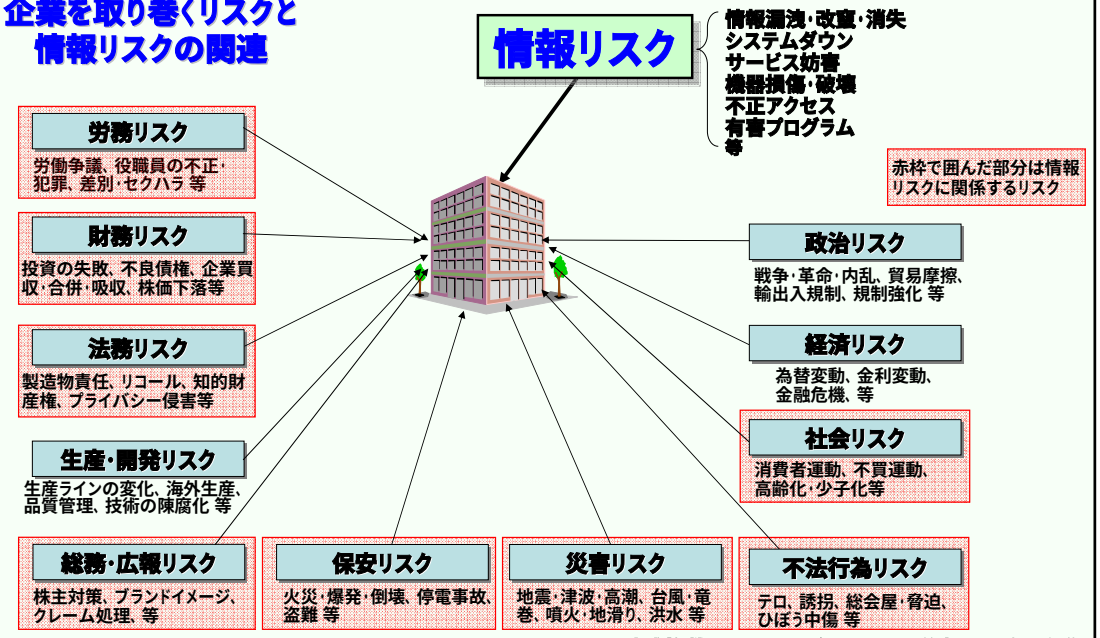
Network Security A Beginner's Guide, by Eric Maiwald
中央大学修士課程（情報セキュリティ副専攻）で「Network Security」講座の開講時に参考資料としたもの

1	導入: 最近の事例，工学と情報セキュリティとの関わり，安全性と利便性のトレードオフ等
2	エンドユーザのセキュリティ: パスワード管理，コンピュータウイルス，ソーシャルエンジニアリング等
3	暗号系の準備: 諸概念，古典暗号，単一換字暗号の解読方法等
4	秘密鍵暗号系: DES，AES，ブロック暗号等
5	セキュリティのための数学: 整数論，計算モデル(決定性/非決定性/確率)，計算の複雑さ等
6	公開鍵暗号系: 公開鍵の概念，RSA等
7	鍵管理: 鍵生成と乱数，Diffie-Helman 鍵交換等
8	認証: 一方向ハッシュ関数，メッセージ認証コード，ディジタル署名等
9	公開鍵基盤: 証明書，認証局，X.509等
10	暗号プロトコル: 暗号系とプロトコルとの関係，暗号プロトコルの具体例等
11	セキュリティソフトウェア: SSH，PGP，VPN，SSL 等
12	Web セキュリティ: Web サーバからの情報漏洩，クロスサイトスクリプティング，フィッシング等
13	OS のセキュリティ: バッファーオーバーラン，特権ユーザ等
14	組織のセキュリティ: リスク分析，セキュリティポリシー，法律(不正アクセス防止法，個人情報保護法)等

国内の学部での「情報セキュリティ」シラバス
良くできており、比較的暗号関係が少ないが、それでも半分程度。
情報セキュリティのタイトルで暗号だけ教えているものもある

参考：情報リスクと企業リスク

企業を取り巻くリスクと情報リスクの関連



実践「危機マネジメント」ぎょうせいより、筆者による追加・編集

参考：事件・事故から学ぶ

情報セキュリティのプロフェッショナルがいたら、以下の事件・事故等は防ぐことができたのではないだろうか？

注） 以下の内容は、該当企業のニュースリリース、マスコミ報道、インターネット等からの情報をもとに作成したものであり、直接、該当企業・組織から得た情報で作成したものではありません。

参考：事件・事故から学ぶ

アウトソース、管理・監督に関する問題

例 耐震偽装事件で、某自治体の関係者は、今まで、「"性善説"でやってきた」と述べていた

↓

この自治体では、今まで、「どのような"マネジメント"をやってきた」のだろうか？
単に、マネジメント不在だったのでは？

例 自治体の市営プールで、女児が排水溝に引き込まれ、死亡

↓

- 受託者（含 監視員）の問題 ⇒ 監視員教育、日々のチェック、緊急対応
- 市側の問題 ⇒ 「丸投げ」（アウトソース：専門家不在）
- 担当官庁の問題 ⇒ 毎年の習慣化を指示すべきでは？

他社事例から学ぶ

例 2005年6月：価格比較サービス大手のサイトの不正アクセスをした留学生の自宅から押収したパソコンに、利用者のメールアドレスなどの個人情報計約9万件が保管されていることが判明。サイトの欠陥をつき、外部から不正な命令を入力しデータベースを直接操作する「SQLインジェクション」を使用。攻撃用ソフトは、中国語のインターネットサイトから入手

↓

企業・組織の情報セキュリティ担当者であれば、以下の2つ程度は考えられるはずだが・・・

① 同じ問題が自社・自組織で起こる可能性はないのか？ ② 同じ問題は他にないか？

参考：事件・事故から学ぶ

企業のパソコンの持ち出し禁止

- 個人情報保護の高まり等から、企業や政府・自治体ではパソコンの持出を禁止令がでているが、それで企業活動などが円滑でできるのだろうか？
- 全ての従業員がそれで問題ないので、あればいいのだが・・・
  - 電車内にパソコンを忘れてしまう人の特質を考えた管理方法を考えることも必要では？
  - また、車内に置いたパソコンや重要書類が車上荒らしにあうことも多いようであるが、そのためには何を考える必要があるだろうか？

➢ 電車内にパソコンを忘れる人の多くは、以下のような方が多い
① 普段、何も持たない
② 電車内で荷物を網棚に上げ、座っても荷物を膝上に置かない
もちろん、それでも忘れる人はいるので、ファイルの暗号化等は必要であるが

➢ 車上荒らしの場合、パソコン、アタッシュケース、重要そうな書類封筒を助手席、後部座席に残している。
① トランクにいれる等の工夫があれば、かなりの確率で車上荒らしを防止できるのでは？
② 大きな駐車場であれば、駐車場所も重要になる

参考：事件・事故から学ぶ

コンピュータウイルスによるネットワーク障害

某自治体 平成15年8月22日（金）発表資料より

作業経過

- 8月19日（火）午前9時10分ごろ、コンピュータウイルス「Welchia（ウエルチア）」によるネットワーク障害が発生
  初日の対応：状況把握、作業方針の確認、ウイルス対策ソフト（CD－ROM）の作成（約500枚）及び作業手順書を作成
- 8月20日：本庁及び出先機関の職員へ作業手順を説明。安全確認されたPCを順次接続する予定であったが、ウイルス対策が不完全なPCが接続され、ウイルスがネットワークに広がる恐れがあり、PCのクリーニング作業のみ実施
- 8月21日：感染したPCが接続されないよう、所属単位での対応を徹底。準備の整った所属からネットワークに接続を開始。本庁・出先あわせて92所属、PC全体の約半分を接続
- 8月22日：前日と同様の手順で接続作業を継続し、ネットワークの再接続はほぼ完了する見込み
- 当面の対応：感染した端末機が残っている恐れもあるため、ネットワークの常時監視を継続する

原因について

- 詳細は、究明中だが、何らかの原因によりウイルスに感染したPCが庁内ネットワークに接続されたと考える。
- また、ウイルス定義のパターンファイルが最新のものに更新されていないPCが一定数あったため感染が一気に拡大し、感染PCからの異常な通信がネットワーク回線を埋め、他のPCの通信ができなくなった。

今後の対応

- セキュリティホールに対するセキュリティパッチの適用
- 個人所有のパソコンの庁内使用の禁止など、ネットワーク利用のモラルの徹底
- ネットワーク管理体制及び監視機能の強化

ウイルス感染状況（8月21日16時現在）	調査台数：4,174台	感染台数：1,314台（約31.5%）	
端末機との再接続	本　庁	80／91	約88%
（8月22日15時現在）	出先機関	73／106	約69%
	全　体	153／197	約77%

- 発表から、2日間、パソコンを利用した作業ができなかった。
- 3日目に半数が復旧し、完全復旧は4日目になった。

これだけの費用損害が発生しているのだが・・・

筆者による費用損害計算

直接費用	CD-ROM作成費用：500枚×10分／枚×7,200円／時間	61万円
	作業手順書作成：1日 × 50,000円	5万円
	端末クリーニング：1時間×8,000台×7,200円／時間	5,760万円
間接費用	8,000台×50,000円／日／人×20%×2日	1億6,000万円
	8,000台×50,000円／日／人×20%×0.5日	4,000万円
合　計		2億5,826万円

参考：事件・事故から学ぶ

株主総会事項に

- 株主総会で、インターネット接続サービスの加入者約450万人の個人情報が流出したことについて、社長が「多大なご迷惑をかけておわびします」と陳謝、原因究明と再発防止に全力を挙げると述べた（2003年12月に事件発生したと思われる）。
- 株主からは、情報管理の甘さを指摘する厳しい質問が相次いだ。社長は、個人情報を扱う部署への指紋認証制度導入などセキュリティー対策を説明。「社員、委託会社に対するコンプライアンス（法令順守）研修をより一層強化する」と述べた。

ミスマッチ？

ログの管理不十分？

- 流出元と見られる保守用のパソコンはICカードで入退室が管理されたシステムルームにあり、社員48人、業務を委託していたシステム会社の社員177人が利用できる状態にあったという。外部から不正侵入することは不可能だったという。
- アクセスログの保存期間が1年間だったため、当時のログがなく、誰がデータベースにアクセスしたかは分かっていないという。

他社の事故は他人事？

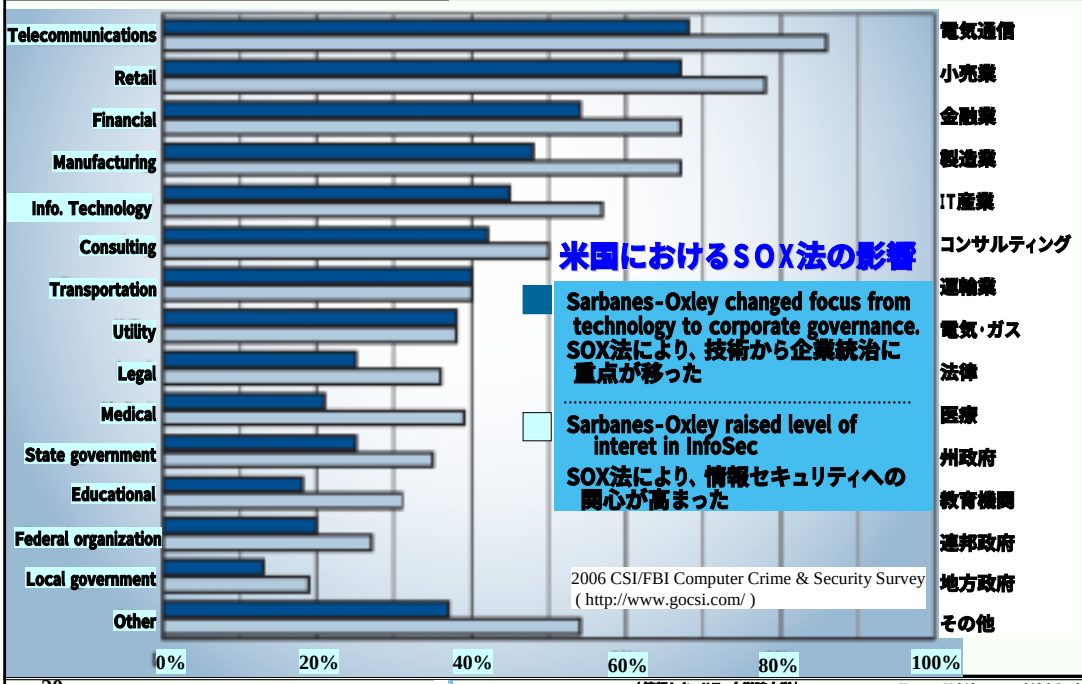
参考：ログ記録が役立たない（ログ記録がない？）

- ある個人情報漏洩企業が、原因を追及した結果報告（2003年8月）
  - 弁護士を含めた社内外の専門家で調査を行ったが、最後の1人に絞れなかった。
  - 当社及び子会社に設置してある数台のコンピュータを利用した約20名であることが判明したが、それ以上は強制力をもたない調査委員会の限界である。

もし、皆さんがこの20名の中の1人だったとしたら・・・
- 20名全てが犯人であるとは考え難い。
- リスクコミュニケーション（事後対応）の失敗？

情報セキュリティ人材育成・資格制度について

参考：彼我の差？

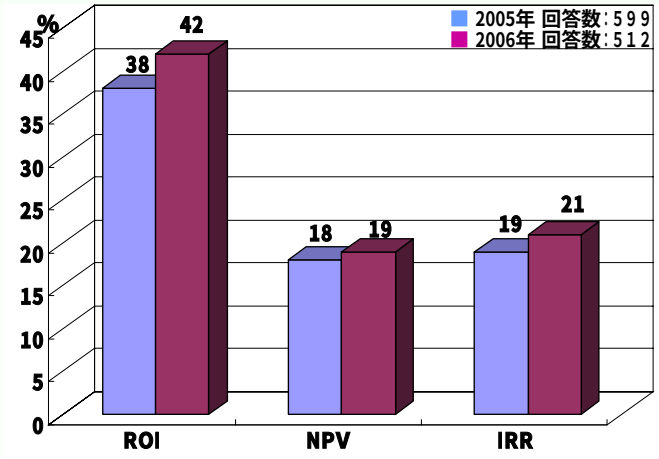


情報セキュリティ人材育成・資格制度について

参考：彼我の差？

日米における投資対効果算定手法

CSI/FBI Computer Crime & Security Survey



ROI: Return on Investment 投資収益率
NPV: Net Present Value 正味現在価値
IRR: Internal Rate of Return 内部収益率

情報セキュリティ投資はやらなければならないものであり、「費用対効果」を計算するものではないとの考えもあるが・・・

この差はどこにあるのだろうか？

- 2006 CSI/FBI Computer Crime & Security Survey http://www.gocsi.com/
- 第3回情報セキュリティ調査 http://www2.gol.com/users/uchidak/

国内調査（「第3回情報セキュリティ調査」2006年1月 筆者により実施）中央大学21世紀COE 調査研究

ROI	NPV	IRR	不明・その他	未実施
1 %	0.3 %	0.4 %	9.6 %	88.7 %

合計 17 企業・組織　94 企業・組織　回答数 980

ありがとうございました

内田　勝也

情報セキュリティ大学院大学

uchida@iisec.ac.jp

http://www2.gol.com/users/uchidak/

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

http://www.iisec.ac.jp/