教育機関における
情報セキュリティ教育の取組み

京都大学
学術情報メディアセンター

上原哲太郎

教育機関における情報セキュリティ教育への要求

- 情報セキュリティポリシーそのものの周知のため
  - ポリシーの「精神」を伝え「文化」を築く
- ポリシーで各構成員に課せられた「手順」の順守のため (時にはOJT)
- ポリシーに明文化されていなくとも一般に組織と構成員を守るためのモラル・倫理的事項
  - セキュリティ・メディアリテラシなどを含む
- 教育機関として人材育成のために
  - セキュリティリテラシそのものが講義となる

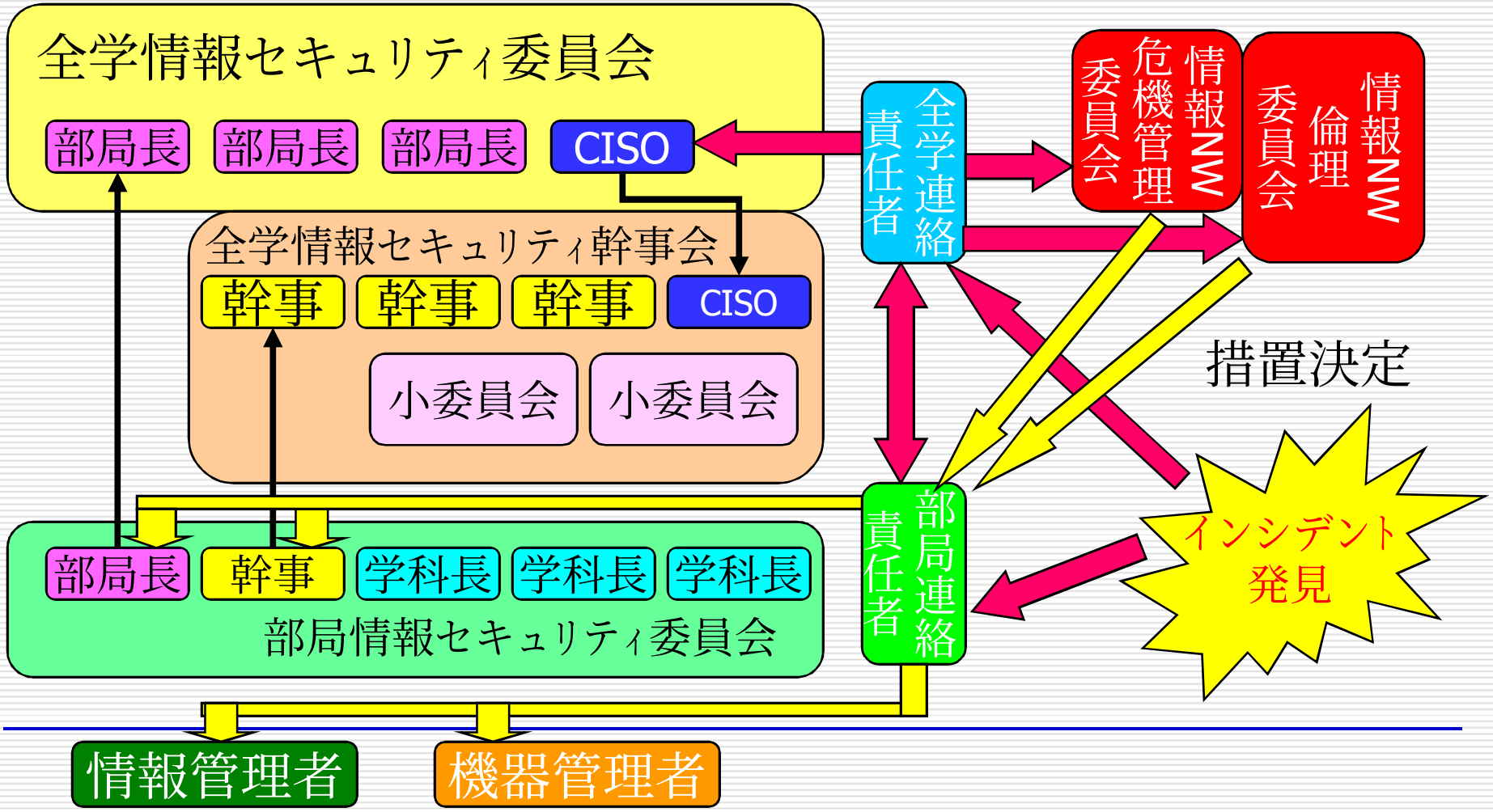
教育機関における「ポリシー」での「教育」の特殊性

- そもそも「情報セキュリティポリシー」の枠組みは教職員には簡単に適用できるが学生には向かない
  - 何かを「命令する」のがなかなか難しいから
- 一方でインシデントのリスクは学生に少なからずある
- 幸い、教育機関には「教育」というミッションがある
  よって情報セキュリティそのものを
  教育ミッションに明確に組み入れることにより
  結果的にポリシーの要求を満たしてゆく、という枠組み

情報セキュリティポリシーの周知としての教育および手順の教育

- まずはポリシーの要求に合致すること
  - 対象、デッドライン
- 教材例がサンプル規程集ではA330Xで提供されている
- 全構成員が対策基準の全ての条項を知っている必要はない(不可能)
- 使える手段
  - 短時間の講習会(座学)
  - e-Learning
  - パンフレット類(実効性に難あり)

情報セキュリティ組織


全学情報セキュリティ委員会
部局長
部局長
部局長
CISO
全学情報セキュリティ幹事会
幹事
幹事
幹事
CISO
小委員会
小委員会
部局長
幹事
学科長
学科長
学科長
部局情報セキュリティ委員会
全学連絡責任者
部局連絡責任者
情報NW危機管理委員会
情報NW倫理委員会
措置決定
インシデント発見
情報管理者
機器管理者

京都大学における状況（1）教職員

- e-Learningによる周知
  - 教材は京大で内製したもの＋購入教材
    （ややポリシーよりも一般的）
  - 履修率を上げるためいくつかの工夫
    - 学内ポータル(Domino)からの直接リンク
      履修率のフィードバックなど
- キーパーソンへのポリシーそのものの徹底は
  「情報セキュリティ幹事会」
  および年1回（以上）の「講習会」にて
  - 「幹事会」は部局情報セキュリティ担当者の連絡会的役割

https://el.iimc.kyoto-u.ac.jp - Internet Navigware 学習 - Mozilla Firefox

京都大学情報セキュリティ | a0061225 | 0 % | INTERNET NAVIGWARE

次へ | 進む→ | ←戻る | 採点 | 再解答 | ヒント | 正解 | 解説 | Q&A | 復帰 | 印刷 | 終了 | リファレンス | ヘルプ | よくある質問 | 設定 | しおり追加 | 目次 | しおり一覧

第三章　情報セキュリティポリシー

3-1　情報セキュリティポリシーとは

情報セキュリティポリシーとは

京都大学という組織としてセキュリティ対策を考えたとき、各構成員任せにしたのでは、セキュリティ意識の低い人が原因となって、周りにまで被害が拡大したり組織全体に迷惑が及びかねません。また、実際にトラブルが発生した場合に、あらかじめ対応方法を決めておかないと的確な対応を行うことができません。そこで、組織に所属する人々が従うべき決まりを作っておくことが大事です。

組織が情報資産に対してどのようにして取り組み，組織に所属する人々がどのように行動すべきかの方針を明文化した規範のことを、情報セキュリティポリシーといいます。情報セキュリティポリシーはほとんどの学生や教員には直接関係してくることは少ないかもしれません。しかし組織の構成員として、情報セキュリティポリシーというものが定められていることと、どのような場合に情報セキュリティポリシーを参照する必要があるかは知っておくべきでしょう。

京都大学における情報セキュリティポリシー

京都大学には以下の規定があり、これらを総称して情報セキュリティポリシーと呼びます。

- 京都大学における情報セキュリティの基本方針
- 京都大学の情報セキュリティ対策に関する規程
- 京都大学情報セキュリティ対策基準

概略だけを解説すると、以下のような内容になっています。

1. 取り扱うさまざまな情報を、重要な情報を重点的に管理しつつ公開にも努めるために、情報の分類を行う
2. 情報資産を保護するため、設置場所についての物理的セキュリティの対策を定める
3. 全構成員に基本方針の内容を周知徹底するなど、十分な教育及び啓発活動を図るための人的なセキュリティ対策を定める
4. 不正なアクセス等から情報資産を守るため、技術的なセキュリティ対策を定める
5. 不正アクセスを防止するための運用面の規定を行い、不正アクセスなどの緊急事態が発生した場合の連絡体制を定める

完了 | el.iimc.kyoto-u.ac.jp

京都大学における状況(2)学生

- (ほぼ)全学生が入学時にアカウント取得に際し30分のアカウント講習を受けるのでこの場を活用
  - 講習は「教育用コンピュータシステム」の利用心得の周知が主目的だがセキュリティポリシーの一部をカバー
- (かなりの)学生が情報リテラシ教育を受けるので講師に情報倫理教育資料を提供
- E-Learningの利用
  - 教材は教職員向けと同じ
  - 履修率を上げるための工夫として情報リテラシ教育のシラバス内に受講を条件として明記

補足：e-Learningは万能ではない

- システム構築と運用は楽ではない
  - 認証をどうするか
    - 京大は教職員の統合認証開始とともに展開可能に
      (学生はもともとほぼ教育用システムで実現済み)
  - 数が多いと運用コストやライセンスコストが問題に
- 難しい対象がどうしても残る
  - 外国人・障がい者・・・・
  - 1人1台PCが実現不可能な組織(例えば付属病院)
- 座学などとの併用で取りこぼしをなくしてゆく
  - 逆に座学などでは遠隔地対応などが困難

一般的な情報モラルや倫理の教育

- ポリシーを補う効果（特に一般モラルや法令遵守）
- 今はよい教材も比較的手に入りやすい
  - 日本ネットワークセキュリティ協会（JNSA）
    情報セキュリティ教育の指導者向け手引書（2007年版）
  - 学生向けにはメディア教育開発センター（NIME）
    情報倫理デジタルビデオ小品集シリーズ
    - Vol.3がこの春リリース
  - 学生なら、意外と高校向け「情報モラル教育」教材も使える
    - 教科「情報」の副読本など
    - 文部科学省「情報モラル等指導サポート事業」成果物
      http://kayoo.org/moral-guidebook/
    - ほか各教育委員会等で情報モラル教本の作成が盛ん

教育としての情報セキュリティ

- 情報セキュリティ技術者育成という面では
  IPA「情報セキュリティのためのスキルマップ」や
  JITEC「情報セキュリティアドミニストレータスキル標準」などの指標があるので参考になる
- 情報セキュリティ技術を教えることはできるが・・・
  「情報セキュリティ教育」？
  「情報セキュリティリテラシ教育」？
  「情報倫理教育」？「メディアリテラシ教育」？
  - 範囲が広くなり過ぎて、どこを教えるべきか悩ましい

先導的ITスペシャリスト育成推進プログラム「IT-Keys」

- 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
- 奈良先端大を代表に、阪大、北陸先端大、京大およびJP/CERT, RIIS(NPO), NTTデータの連携
- 大学院修士課程の学生を対象に年20人程度、
  実践的実習による経験と勘の習得
  最近技術知識の獲得
  法律・経営・政策・倫理的知識の習得を狙う

Microsoft Office
werPoint 97-2003

アウトリーチ

- 構成員の情報セキュリティ教育を必要としている組織は大学だけではない
  - 特に公的団体は人材不足で困り果てている
- 社会活動的にこれらの組織に出かける
  - Eネットキャラバン（文科省・総務省）との連携
  - インターネット安全教室(警察庁・経産省）との連携
  - 地域の小中高等学校・校長会・教育委員会・PTA
  - 地方公共団体や関連組織
  - 地元商工会議所・NPO等との連携

NPO「情報セキュリティ研究所」RIIS

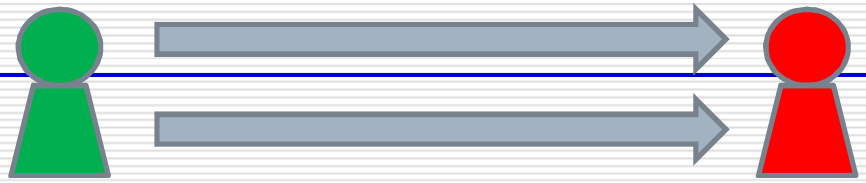
- 平成14年1月設立
  - 代表：臼井義美（企業社長）
  - 副代表：上原哲太郎
  - 理事：近畿大学・企業（ISACA元支部代表）・事務局長（専任）
  - 社員（会員）17　企業会員5
  - 専任スタッフ3名（＋現在臨時1）
- 和歌山県田辺市
- 主な事業
  - 自治体情報セキュリティ
  - 電子自治体推進
  - 地域情報化推進
  - 地域での情報セキュリティ啓蒙
  - 教育分野でのセキュリティ
  - 人材育成事業
- http://www.riis.or.jp

協議会を通じた情報セキュリティポリシー策定

- 県下をいくつかのブロックに分ける
- ブロックごとに市町村の担当者を集めて勉強会
  - 意識あわせ・レベルあわせ・底上げ
  - 業務分析を「自分たちで」「他と較べながら」
    →これが予想以上にスキルアップ効果を産んだ！
- その結果を元にポリシーを策定
  - 作業の一部は業者に委託：ただし「まとめて」
- 非常に安価に・レベルの高いポリシー策定
  - 詳しくは日経ガバメントテクノロジーの記事を
    http://premium.nikkeibp.co.jp/e-gov/case/2004/case40a.shtml
- 最初は対策基準まで：順次実施手順策定支援
- 平行して全職員研修を実施
- さらにセキュリティ監査支援→内部監査人養成

自治体の内部監査人養成

- 自治体担当者同士の「横のつながり」は
  思った以上に互いに刺激に
  - 同じスキームで監査をやろう
- ブロックごとに情報セキュリティ監査の勉強会
  その後ブロック内で「互いに他の自治体の
  システムを監査する」
- そのノウハウを自治体に持ち帰り自治体では
  「互いに他部署のシステムを監査する」



小中高等学校に対する情報セキュリティ啓蒙

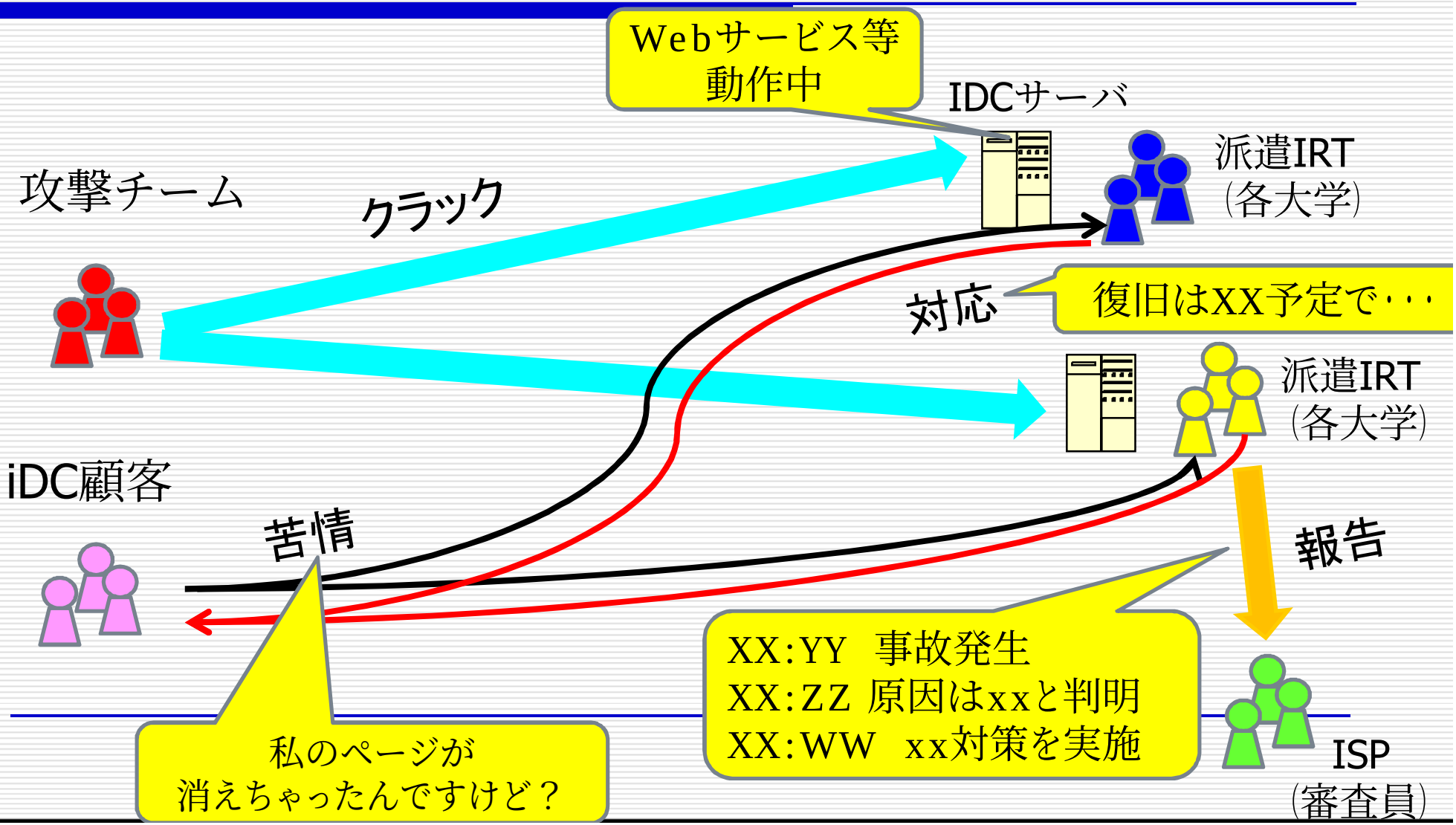
- 3つの危機感
  - 「パソコン担当」教員の過剰な負荷
  - 学校関係から減らない「個人情報漏洩」
  - 初等中等教育における情報倫理教育の不備
- NPOを通じて「学校まわり」を開始
- JNSA「インターネット安全教室」の県内展開
- 昨年度より和歌山県の「NPO協業事業」の枠組みを使い県警と一緒に講演会を開催
  - 昨年は6箇所　今年は（目標）50箇所！
- 「学校共同サーバ」研究会も主催
  - 報告書を取りまとめ中
- 課題は「教師」と「保護者」への教育

大学にツケが！

IT危機管理コンテストの内容

- 各大学でチームを結成:「IRTチーム」を模擬してもらう
- コンテスト会場にはチーム数分のサーバ等を配置
  (iDCを想定) IRTチームは各iDCに派遣された
  専門家集団というシナリオ
- コンテスト開始とともに各サーバに(あらかじめ仕組まれたシナリオに沿った)「事故」が発生する
  - 事故を発生させる攻撃チームを運営が担当
    同時に「iDC顧客」の役目としてトラブル発生のたびに
    その苦情をメールや電話で各チームに投げつける
  - IRTは苦情処理と事故原因解析・対策を同時にやって、
    そのレポートをまとめてiDCに提出
  - このレポートの内容を主に審査対象として競う
- これを数ターン行う

IT危機管理コンテスト



「IT危機管理塾」の実施

- ターゲットは3つ
  - 団塊の世代をCISO人材に！：危機管理者コース
  - 若手の技術者のリカレントの場を！：技術者コース
  - 経営者にMoT＋情報セキュリティを：経営者コース
- 危機管理者コースをまず実施
  - 1週間白浜に泊り込みで講習
  - 講師陣と親交が深まる

概要		企業の危機管理責任者を養成する。マネジメントに関する基本的な知識を前提にして、危機管理に必要な知識を習得する。				
日程		第1日	第2日	第3日	第4日	第5日
第1回		2006/12/4(月)	2006/12/5(火)	2006/12/6(水)	2006/12/7(木)	2006/12/8(金)
第2回(予定)		2007/2/19(月)	2007/2/20(火)	2007/2/21(水)	2007/2/22(木)	2007/2/23(金)
9:00－10:30	テーマ	なし	知的財産論	情報管理と個人情報保護	セキュリティ監査概論	セキュリティ対策と企業責任
	内容		企業の保有する特許権や著作権などの無体財産の保護と活用	情報の管理方法と、個人情報を含む機密保護について(情報セキュリティをめぐる事件および判決の動き'06)	組織の中の情報セキュリティの状況を調査し、報告する	情報セキュリティ事故、社会的責任と広報対応
	講師		須川賢洋(新潟大学)	高橋郁夫(弁護士)	高瀬宣士(帝塚山大学)	丸山満彦(監査法人トーマツ)
10:40－12:10	テーマ	オリエンテーション	コンプライアンスプログラム	ウィルスと不正アクセス	システムの現状復帰対策	クロージングとセキュリティ関連資格について
	内容	カリキュラムの説明	企業活動における法律などの遵守のしくみと計画	コンピュータウィルスや外部からの不正アクセスの防御など	事故発生に備えて、現状復帰を迅速に行うバックアップ対策など	修了証の授与とRIISの支援ネット 各種セキュリティ関連資格と対策
	講師	事務局	山地真開(RIIS)	高瀬宣士(帝塚山大学)	野川裕記(東京医科歯科大学)	臼井義美(RIIS)
13:00－14:30	テーマ	企業とIT危機管理	リスク分析とリスクマネジメント	フォレンジック概論	内部統制とJ-SOX法対策	なし
	内容	企業で考えられるIT危機の概要と、サイバー犯罪事件の概要	保有する情報資産の流出などによる経済的損失評価や管理	情報関連の事故発生に伴う捜査や法的証拠を得る手段のビジネスへの応用	日本版SOX法の実施に備えて、企業経営に望まれる内部統制の方法	
	講師	上原哲太郎(RIIS)	山崎文明(ネットワンシステムズ㈱)	高橋郁夫(弁護士)	丸山満彦(監査法人トーマツ)	
15:00－16:30	テーマ	サイバー法概論	情報セキュリティ管理規定と体制	インターネットセキュリティ	事業継続対策	
	内容	サイバー犯罪を構成する各種法律の状況と適用事例	情報資産を保護するための、アクセス制御などの管理方法と体制	インターネットを利用する上で必要とされるセキュリティ技術	事故発生時に、迅速に事業を再開するための計画と実施	
	講師	須川賢洋(新潟大学)	山崎文明(ネットワンシステムズ㈱)	野川裕記(東京医科歯科大学)	山地真開(RIIS)	
18:00－20:00	BOF	須川賢洋先生を囲んで	高橋郁夫弁護士を囲んで	高瀬宣士先生、野川裕記先生を囲んで	丸山満彦氏を囲んで	

終わりに

- 情報セキュリティポリシーの展開については
  粛々と行えばよい　ツールもノウハウもある
  - 効率よく、全構成員に適切な内容を短時間で網羅する
- 問題はポリシーに現れない部分
  - 構成員のモラル･倫理教育はどうするか
  - そもそも情報セキュリティリテラシ教育･モラル教育･倫理教育はどのようにあるべきか見えにくい
- 講師や教育展開を主導できる人材の不足
- アウトリーチはどうあるべき？