大学における情報セキュリティマネジメントの諸問題

京都大学大学院工学研究科
附属情報センター

上原哲太郎

大学における情報セキュリティの位置づけ

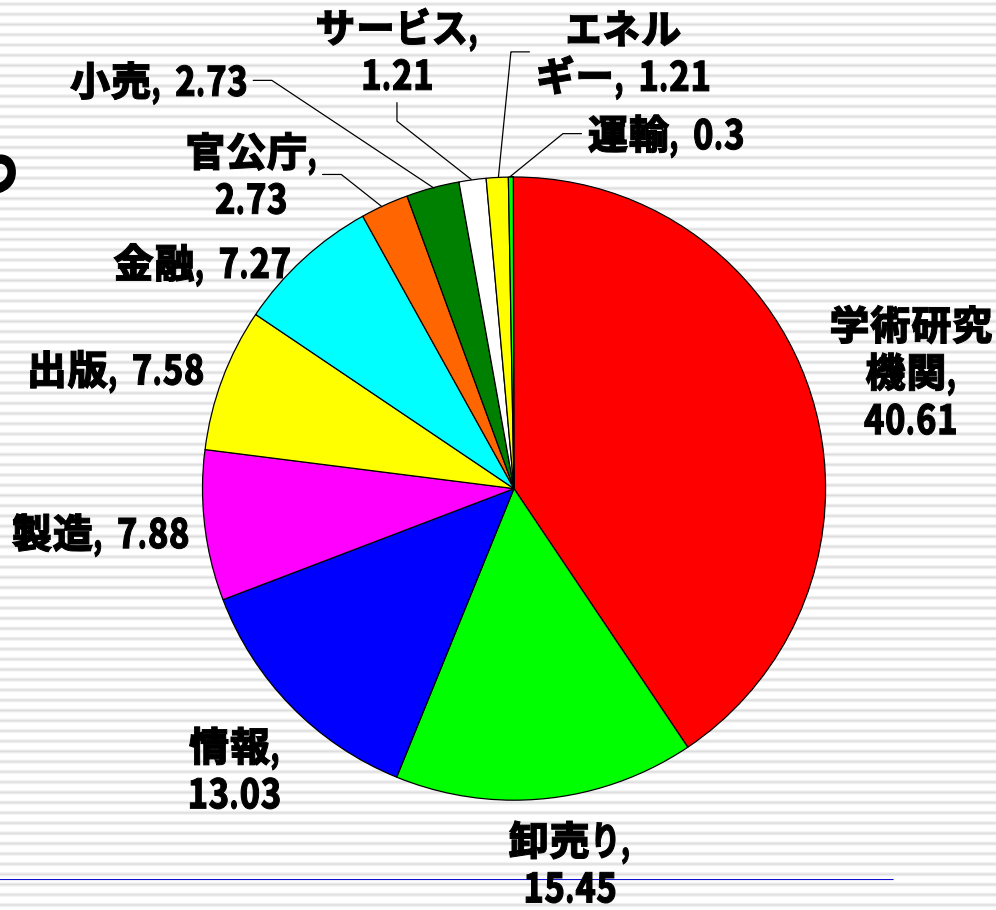
- ネット社会の一員としての責務
  - ウィルスや踏み台で「よそに迷惑をかけない」
  - インターネットを育てたのは大学だが、インターネットを無法地帯にしたのも大学かも？
- 大学の「ブランド」を守るため
- 社会からの要請に応えるため
  - 高まる情報セキュリティ/プライバシーに関する意識
  - 「研究してくれ」「教育してから社会に出してくれ」
- 政府からの要請に応えるため
  - OECD情報セキュリティガイドライン/プライバシーガイドラインに従う施策
  - 「知的財産立国」
- 個人情報保護法の完全施行への対応
- (国立大学のみ) 法人化に伴う訴訟リスクへの対応

大学の情報セキュリティ上の脅威

- 外部からの脅威
  - ネット越しのハッキングによるもの／ウィルス→「猛烈」
  - 部外者によるネットの不正利用（公開端末・無線LAN）
  - 物理的盗難→情報漏えいの危険
- 内部の脅威
  - 構成員によるネットの不正利用
    （アタック・掲示板荒らし・P2P・・・）
  - 情報持ち出し・漏えい（今のところあまり顕在化してない）
- 番外
  - 構成員による不祥事
  - 著作権法違反

大学は脆い・・・恥ずかしいくらい

- ウィルスには「かなりしょっちゅう」罹る・・・
- アタックは「猛烈に」やってきている・・・
  - そして恥ずかしいことに成功率が高い？
  - 国内のインシデントの約4割が大学関係？
- 問題を起こす構成員
  - 時々内部から不祥事
  - P2Pの火消しが必要



出典：(株)ラック　侵入傾向分析レポート 2003年度サマリレポート

何故こんなことになっているのか

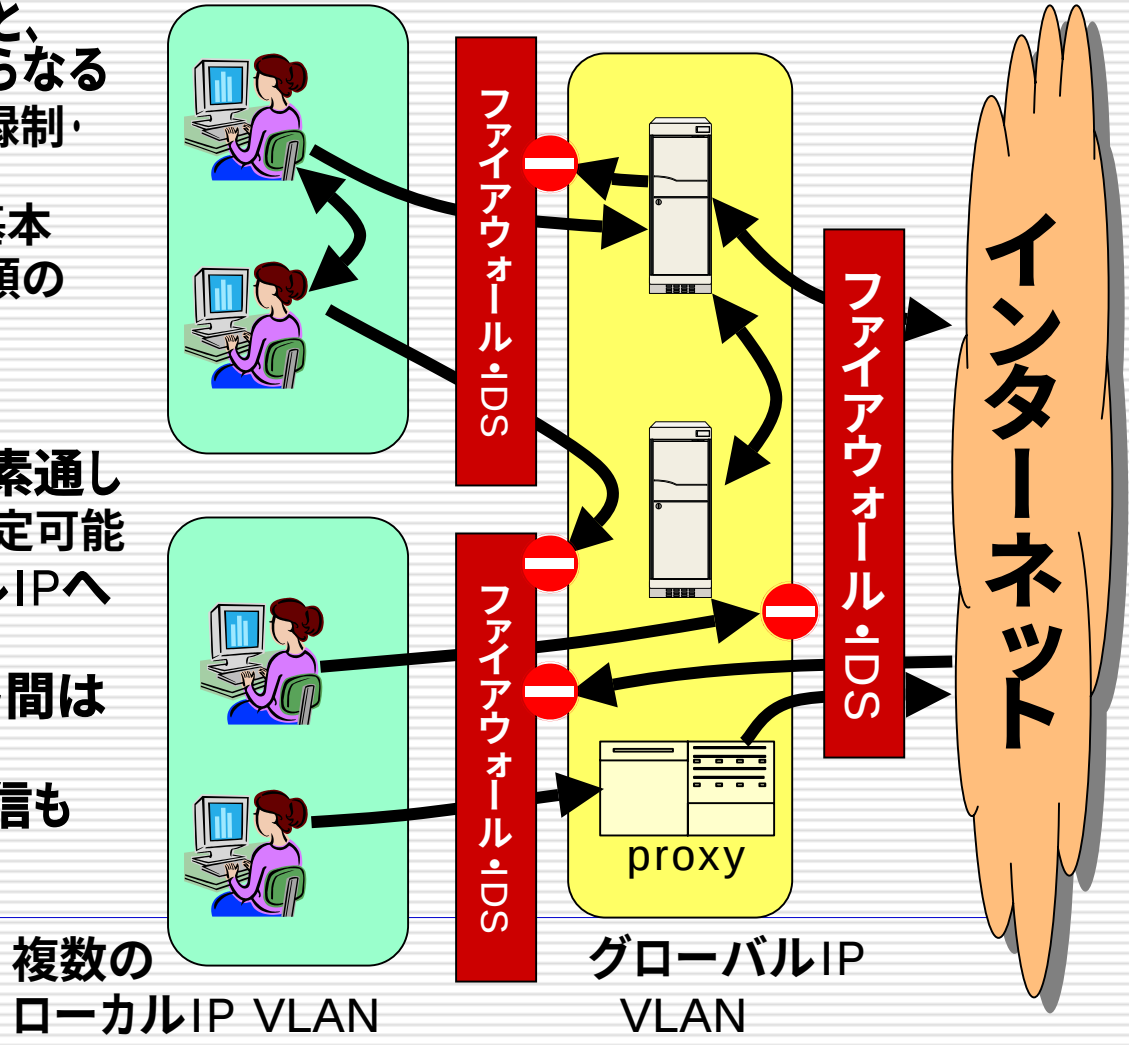
- 歴史的問題が圧倒的に大きい
  - 「実験」の名残り・・・タダで使い放題　サーバ立て放題
  - 学生・ボランティアによる管理体制のツケ
    - まじめな管理体制が未だに不在
- サーバ管理は誰にでも出来るという幻想
  - 「動く」と「管理する」の差は大きいのに・・・
  - 一度動かしてしまうと既得権益が発生→自縄自縛
- 「ネットには自由がある」という文化
  - 「コピーできるものをコピーして何が悪い？」
- 常に使われる「金がない」という言い訳

技術でがんばってみる

- ネットワーク構成の見直し
  - クライアント系のローカルIPへの閉じ込め
- アンチウィルスソフトウェアの導入
  - クライアントに全部入れるのが徹底できない・・・
  - メールサーバが無数にあって・・・
- ファイアウォールの導入
  - 設定のコンセンサスは？
- IDSの導入
  - とにかく監視し続けるのが大変
    - 何かわかったときにアクションを起こすのはもっと大変
  - 盗聴とか監視とかはとても嫌われる

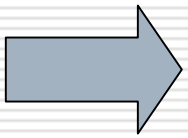
京大キャンパスLANの論理的構成

- 単一のグローバルIP空間と、多数のローカルIP空間からなる
  - グローバルIPは完全登録制・固定IPのみ・課金あり
  - ローカルIPはDHCPが基本
  - ローカルIPはさらに2種類の設定（オープンスペース／クローズドスペース）
- グローバルIP空間とインターネットの間はほぼ素通し
  - 希望によりポート毎の設定可能
- ローカルIPからグローバルIPへは出られるが逆はダメ
- ローカルIPとインターネット間は通信不能
- ローカルIP VLAN間の通信も原則不許可
- IDSによる常時監視



ここまでやっても事件は起きる・・・

- 人的要素があまりにも大きい
  - P2Pによる不正利用
  - 掲示板への書き込み・・・
  - 不適切なコンテンツの公開
    - 匿名Remailer, Uploaderなども・・・
- もはや技術だけではどうしようもない



情報セキュリティマネジメントシステムの導入
セキュリティポリシーの策定と実装

情報セキュリティマネジメントとは

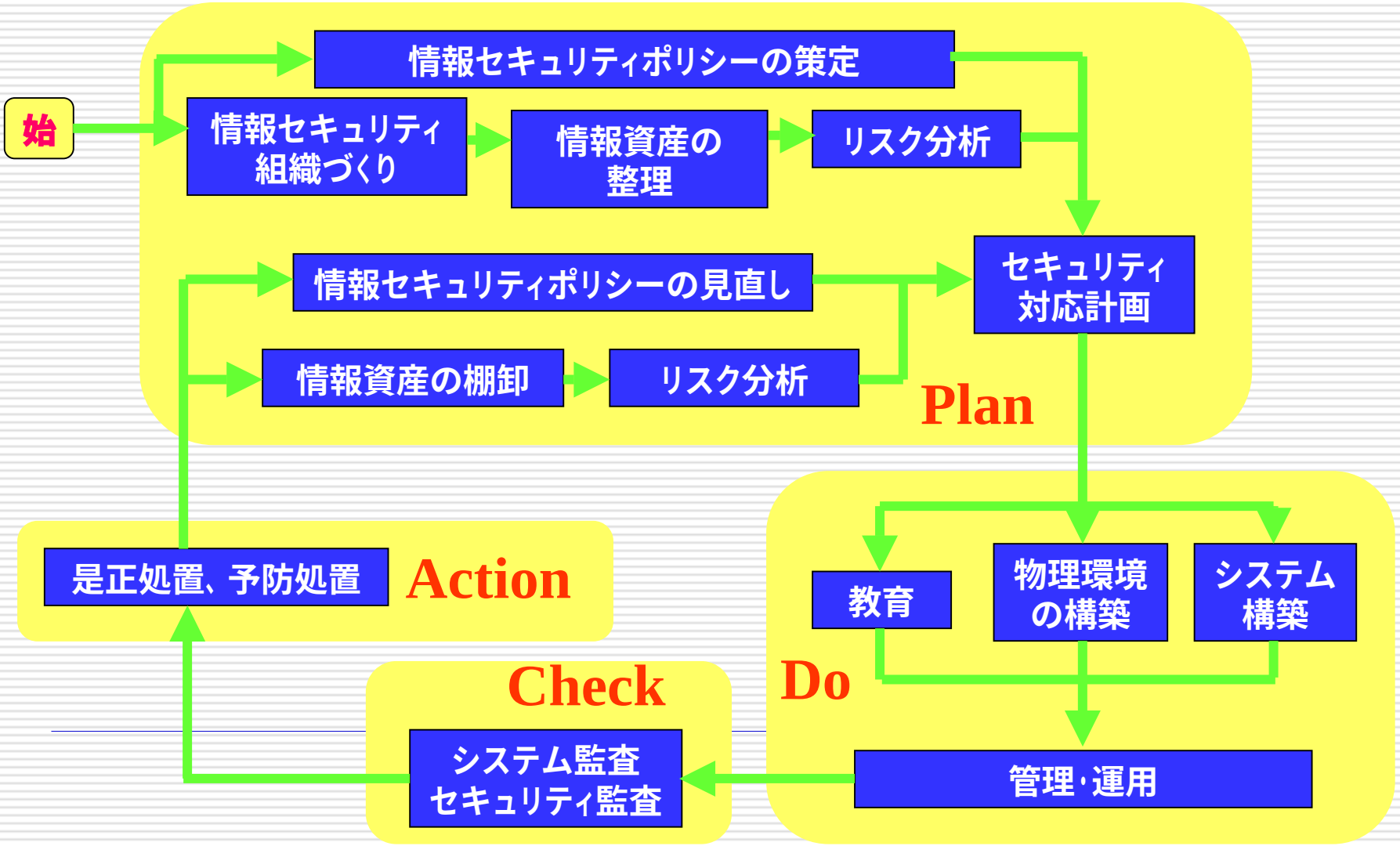
- 情報資産について次の事柄を「維持」すること
  - Confidentiality（機密性）
    - 情報をアクセス権に従い管理する
  - Integrity(完全性)
    - 情報の内容を正確に保つ
  - Availability(利用の可能性)
    - 必要なときに常に利用できるように運用する
- これを実現するのが情報セキュリティマネジメントシステム（ISMS）
- BS7799、ISO17799、JIS X 5080等で規格化
  - 実はISO9001/ISO14001などと似た流れ
  - 認定制度としてJIPDECのISMS認証制度など

いわゆる「情報のCIA」

情報セキュリティポリシーとは

- 情報セキュリティマネジメントシステムを維持するための方針や具体的基準・手順をまとめたもの
- 3段階の文書からなる
  - 基本方針（ポリシー：組織で1つ）
    - 組織の情報資産をどのような脅威からどのようにして守るかについての基本的な考え方
  - 対策基準（スタンダード：組織または部門単位）
    - 基本方針を実現するために何をやらなければならないかという遵守すべき行為及び判断などの基準
  - 実施手順（プロシジャ：各担当向け）
    - 対策基準に基づいた、業務、情報システムまたは職務ごとの具体的なセキュリティ対策の手順書、マニュアル等
- これらの文書を段階的に策定し構成員に守らせる

セキュリティポリシーのPDCAサイクル



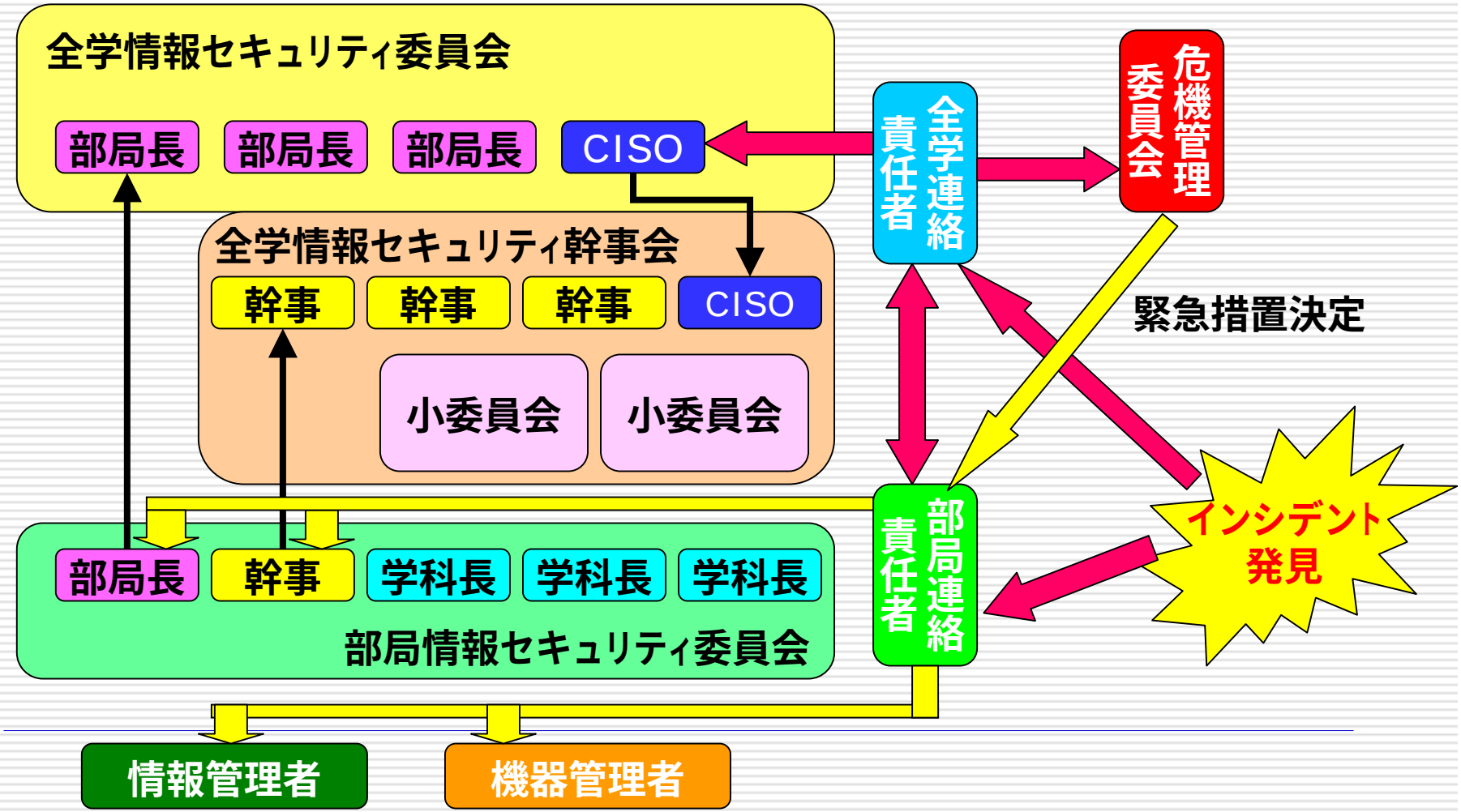
大学に情報セキュリティポリシーの策定が求められるまでの流れ

- 平成12年7月「情報セキュリティポリシーに関するガイドライン」情報セキュリティ対策推進会議決定
  - 政府機関は平成15年度までに情報セキュリティポリシーを
- 平成14年3月「大学における情報セキュリティポリシーの考え方」情報セキュリティ対策推進会議決定
  - この文書を元に各大学でポリシー策定に着手
- 平成15年1月「高等教育機関におけるネットワーク運用ガイドライン」電子通信情報学会他
  - かなり具体的な運用実態に沿ったガイドラインが示される

大学向け情報セキュリティ組織例

- 最高情報セキュリティ責任者（CISO）が必要
  - 学長または副学長・理事
  - 大学全体としてのリスクマネジメント
- 各部局長（学部長）を部局情報セキュリティ責任者に
  - 各部局がもつ情報資産の最終的責任を負う
- 実働部隊が重要（システム管理責任者等）
  - 専門的判断が出来る集団
- 事務局も重要
  - 「なにもない」時こそいろんなことを動かさねばならない
    →委員会開催等の「トリガ」
  - 「なにかあった」時には窓口を一元化しなくてはならない
    →マスコミ応対はとても重要

情報セキュリティ組織の例



ある大学のポリシーの例

- 電子化された情報資産のみをポリシーで扱う
  - 文書管理規則との不整合を避ける
- 情報資産と、それが格納された機器について管理者を定義（情報管理者・機器管理者）
- リスク分析は2段階
  - 普通の情報と、「特定情報」（部局長が指定）
- 特定情報になった場合は対策基準に従った管理が求められる
  ∴特定情報が入っている機器の管理は制限を受ける

やってみてわかったこと

- ISMSは、大学に必要なものがいくつか欠けている
  - 「学生」という微妙な構成員の扱い　教育との兼ね合い
  - 情報のCIA「以外」のインシデントの扱い
    - 情報資産ではなく機器を用いたインシデント
    - 著作権法違反などの外部からの訴え
- 大学には、ISMSに必要なものがいろいろ欠けている
  - 命令伝達系統と強制の仕組み・・・要はガバナンス
    - 特に教員組織と事務組織の乖離
    - 教員はどこまで組織に帰属している意識があるか？？
  - 情報資産の所属や管理責任の明確化
    - 研究で得られた情報資産はどこに帰属？
- 大学の情報セキュリティは事務組織と教員組織で違う
  - 教員組織は「機器に関するインシデント」がメイン
  - 事務組織は「情報漏えい」がメイン
- 結局はインシデント・レスポンスが一番時間と手間がかかる・・・

大学が本当に守るべきもの？

- 情報資産のうち本当に組織にとって大事なものは？
  - 機密性が求められるのは、入試問題、個人情報、調達関連など
  - 研究成果は組織があまり関わっていない部分
  - 本当に機密性の高い医療関係は法のカバーがある
  - 文書は取り扱い規定がある
- 本当に怖いものは「訴訟」と「ブランドの失墜」？
  - 情報漏れより不祥事のほうが怖い
    - 実情や内容がどうであれ、事件で大学の名前が出ると大騒ぎ
  - 大事なことは「新聞沙汰にならないこと」と「裁判を起こされないようにすること」
    - 直接被害よりもはるかに大きくなる可能性
  - ありそうなシナリオを考え、可能性の芽を摘む

さらに個人情報保護法対応

- そもそも情報セキュリティ対策がちゃんとできれば個人情報保護はほとんどできる
  - 必要なのは適正取得、開示・訂正・利用停止請求等に対応することを加えること
- あとは該当する情報資産を把握さえできていれば、それほど難しくない話なのだが・・・
  - 研究関係で該当するものを全て把握できるか？

おそらく必要なこと

- 事務方の情報セキュリティ組織の強化と啓蒙
  - 個人情報保護法対策に対する関心が高まっているのを利用
  - 「セキュリティ」「プライバシー」に関しての意識改革を促す効果
  - 今後は人員削減で外注が増えそう
    - セキュリティ的なノーチェックは恐ろしい
- 教員組織内でのコンセンサス
  - 研究組織のインフラとしてのネットワークはどうあるべき？
    - 持ち込み私物PC全面禁止に出来る？
    - 『学生にメールサーバ管理させないで』って言える？
    - 合意が取れた時点でそれと整合するように、キャンパスネットワークに関して利用形態制限を行い、ISMSの技術セキュリティに盛り込む（変則だが、情報資産を起点にするとここにたどり着けない）
  - 研究によって得られた情報資産をどう位置づける？

おわりに

- マネジメントそのものが難しい
  - そもそもトップダウン的マネジメント手法は大学には適用しにくい（特に一部の大学は）
  - 学生はまた別のルールで動いている
  - その中で組織内に統一した基準での情報資産の管理が強制できるか？
- 情報資産そのもの以外の扱いを考える必要
  - もはやCIAと関係ない話だが、どうやって？
- まだまだ模索中・・・