大学における個人情報保護とセキュリティマネジメント

京都大学大学院工学研究科
附属情報センター

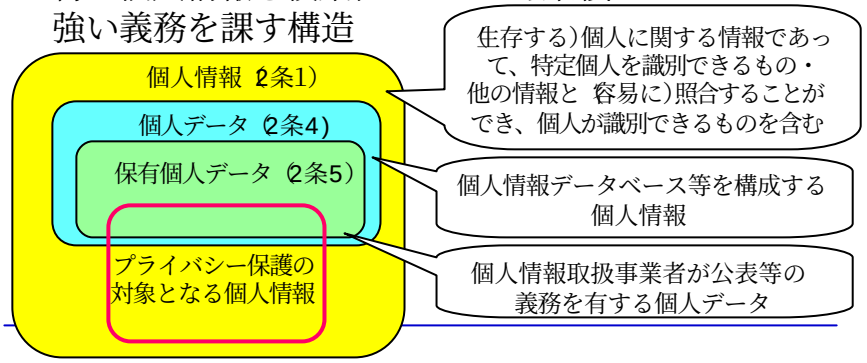
上原哲太郎
tetsu@info.kogaku.kyoto-u.ac.jp

個人情報保護法制の成立過程

- OECDプライバシーガイドライン(1980)・EU個人データ保護指令(1995)への対応と住基ネットを契機にした法整備の必要性
- 多発する漏洩事件への対応としての必要性
  - 漏洩自体は昔からあったが、世論が変化
- 旧行政機関個人情報保護法(1988)を全面改正する形で成立
  - 旧法は電算処理のみ、新法は包括的
  - 分野ごとに分かれる
  - 地方公共団体は未カバー 条例は先行している)
- いよいよ2005年4月完全施行へ

個人情報の保護とは？

- 「個人情報」＝「個人識別情報」の保護である
  - 直接または他の情報との照合により個人が識別できる情報
- 特に個人情報を検索性があるよう集積したものに強い義務を課す構造



個人情報一般にはOECD8原則が守られるべき

- 収集制限の原則
  - 適法・公正な手段で、通知・同意を得て収集するべき
- データ内容の原則
  - 利用目的に沿っており、完全・正確・最新であるべき
- 目的明確化の原則
  - 収集時に目的を明確化し、利用はその制限を受けるべき
- 利用制限の原則
  - 同意または法による場合を除き、目的以外に開示利用されてはならない
- 安全保護の原則
  - 紛失・無権限アクセス・破壊・仕様・修正・開示等から保護されるべき
- 公開の原則
  - 収集方針等は公開され、存在・種類・利用目的・管理者は公開されるべき
- 個人参加の原則
  - 本人に関するデータの存在確認・開示・削除・訂正請求できるべき
- 責任の原則
  - データ管理者は上記諸原則を実施するための措置に従う責任を有する

義務を負うのは誰か(2条3)

- 「個人情報取扱事業者」
  ＝個人情報データベース等を事業の用に供しその個人情報の総数が5000件以上の者
  - 除外規定あり（50条）
    - 報道・著述・学術研究・宗教活動・政治活動の用に供する際は除外
- 公的部門（これらは例外なく義務を負う）
  - 国の行政機関
  - 独立行政法人
  - 地方公共団体
    - および地方独立行政法人

個人情報データベース等とは(2条2)

- 個人情報を検索できるようにしたもの
  - コンピュータ上のいわゆるデータベース
  - 名簿等、インデックスがついた紙情報
- これ以外の規定はない、ので・・・
  - 個人情報の性質によらない
    - 機微な情報だからといって特別扱いされない
    - 個人情報になるかどうか微妙な場合も
      - IPアドレスは？メールアドレスは？
        結局は照合できるかどうかの問題になる
  - 件数規定は個人情報データベース等の定義には無関係
    - 単一の個人情報データベースが5000件以下でも義務は負う

個人情報全体に必ずかかる義務

- 「目的明確化の原則」
  - 利用目的をできる限り特定しなくてはならない(15条)
- 「利用制限の原則」
  - 目的達成に必要な範囲を超えて取り扱ってはならない(16条)
- 「収集制限の原則」
  - 偽りその他不正の手段によって取得してはならない(17条)
- 「公開の原則」「個人参加の原則」
  - 取得したときは利用目的を通知または公表しなければならない(18条)
- 「責任の原則」
  - 苦情の適切かつ迅速な処理に努めなくてはならない(31条)

個人データに関する義務

- 個人データ
  ＝個人情報データベース等を構成する個人情報
- 「データ内容の原則」
  - 正確かつ最新の内容に保つよう努めなくてはならない(19条)
- 「安全保護の原則」
  - 安全管理のために措置を講じなくてはならない(20条)
  - 従業者・委託先を監督しなければならない(21,22条)
- 「利用制限の原則」
  - 本人の同意を得ずに第三者に提供してはならない(23条)

保有個人データに関する義務

- 保有個人データ=事業者が管理する個人データのうち以下のものを除くもの
  - 6ヶ月以内に消去するもの
  - その存否が明らかになると公益を害するもの
    - 生命財産の危害・犯罪の誘発・他国との関係etc
- 「公開の原則」「個人参加の原則」
  - 利用目的を本人の知りうる状態に置かねばならない(24条)
  - 本人の求めに応じて内容を開示・訂正・利用停止しなければならない(25,26,27条)

事業者の責務をまとめると・・・

- 個人情報の入り口において・・・
  - 本人から得る
  - 利用目的を提示し同意を得る
  - 第三者提供をするときはあらかじめ同意を得る（オプトイン・オプトアウトとも）
- 個人情報を取り扱う際には・・・
  - 安全に管理する
  - 適正に利用する
  - 不要になったら捨てる
  - 存在を公表する
  - 本人からの開示・訂正・停止等の受付の窓口を提示する

オプトイン・オプトアウト

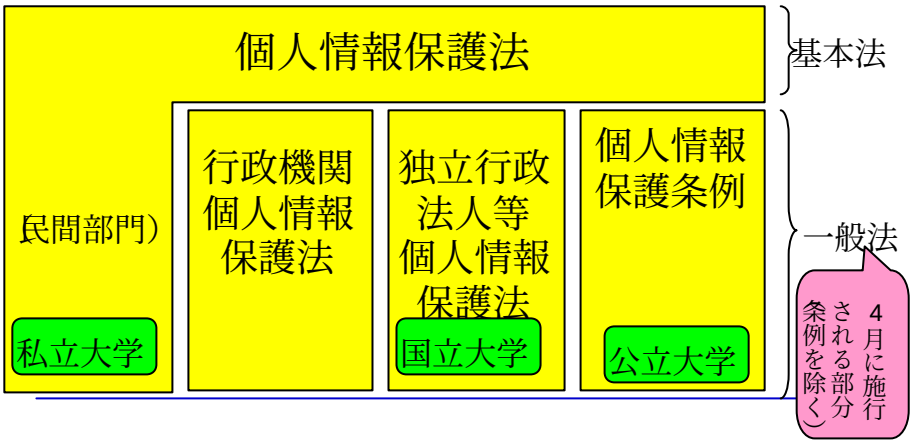
- 第3者提供の2方式
- オプトイン(23条1)
  - 第3者提供に際しあらかじめ本人の同意を得る
- オプトアウト(23条2)
  - 以下の場合に本人の同意なく第3者提供可能
    - あらかじめ「第3者に提供することが利用目的」「提供データの項目」「手段」「停止可能であること」が通知され、本人が知りうる状態に置かれている
    - 本人からの求めがあれば提供を停止する

ところで・・・誤解なきよう

- 個人情報保護法でいう「個人情報」はあくまで「個人識別情報」である
  → 「プライバシー」を保護する法律ではない
  - 例えばメールの本文は個人情報を含むが個人情報そのものではない
- 個人情報の概念は極めて広い
  - センシティブかどうかは無関係・構成員の情報（インハウス情報）も含む
- あらゆる個人情報の取り扱いが制限されるわけではない
  →強い義務は「保有個人データ」に対してのみ
  それも学術研究は除外規定あり
- 5000件規定ではなく、総数5000人規定である
  →構成員や現取引先が5000人以下でも該当する可能性あり
  名簿を分割したからといって逃れられるわけではない
- 漏らした者に直ちに厳しい刑事罰があるとは限らない
  - あくまで「コンプライアンス」が主眼　あとは監督官庁次第
  - ただし違法性は明らかなら民事は厳しく問えるだろう

個人情報保護法制の構造

- 分野によって適用される法が異なる



法制の差が産む細かな違い

- 一部の条例は個人情報の定義が異なる
  - 生存してなくても個人情報の場合がある
  - センシティブ情報を特別扱い（収集の原則禁止など）の場合
  - 計算機管理のみを対象の場合（ただし、改正の方向）
    - 一部地方公共団体にはまだ条例がない場合も・・・
- 公共は一般に民間より厳しくなっている
  - 民間は「容易に」他と照合できることを要するが
    国や独立行政法人は単に照合できれば個人情報
  - 保有個人情報に関し全ての義務を課す
  - 個人情報データベース等ではなく「個人情報ファイル」
  - 1000件を超える個人情報ファイルのリストを
    「個人情報ファイル簿」として公表する義務

大学における個人情報保護

- 実はきっちりと整理がされていない・・・・
  - 個別分野に関しては監督官庁がガイドラインを示すべきだが、文部科学省は「生徒等の個人情報」の扱いについて比較的常識的ラインを示したのみ
- 大学の扱う個人情報の種類の多さ
  - 教務・同窓会・健康診断・病院・教職員・研究関係
- 管理者も実質的には多い
  - 「組織」と「個人」、「同窓会」「学会」「生協」「組合」

しかし対処法はありそう・・・

- 研究者個人の学術研究用途は除外規定がある
- 同窓会や組合などの密接な団体はオプトアウトで第3者提供できる体制を作る
  - 学会活動は明確に分離する必要がありそう
- 多くの個人情報は利用目的が明確・提示できるはず
  - 逆に、提示できない情報は収集するべきではない
- 個人情報データベース/ファイル簿のリストが必要
- 本人からの申し出の受付窓口も必要
- 後の問題は安全管理・・・・

→ 残る問題は情報セキュリティマネジメントに

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

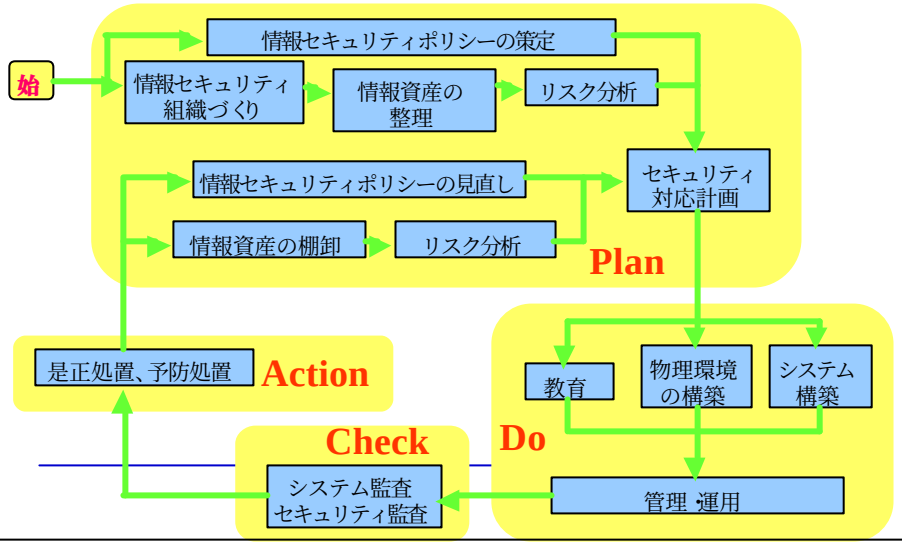
いわゆる「情報のCIA」

- 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

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

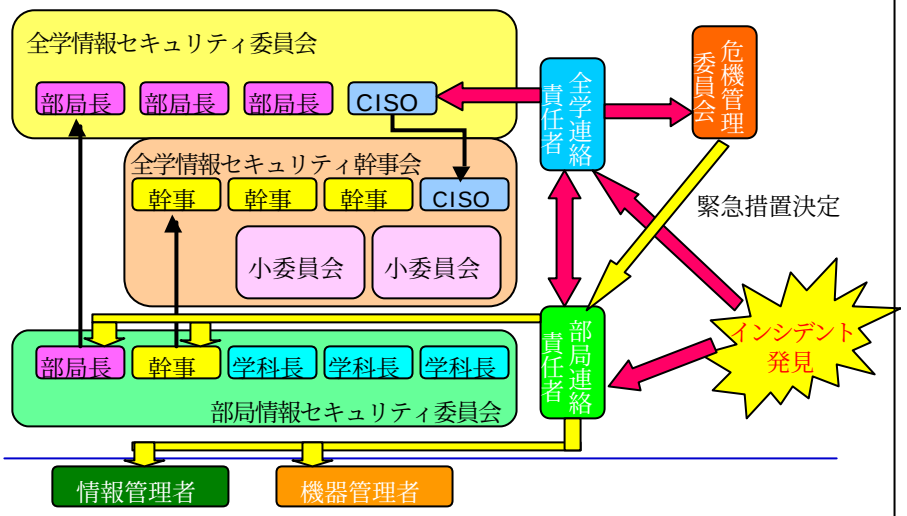
セキュリティポリシーのPDCAサイクル



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
    →マスコミ対応はとても重要

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）
  - 個人情報はデフォルトで特定情報
- 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　特に個人情報
- 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
    - 個人情報保護としては除外規定適用可能　個人の責任に帰する
  - 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
- 学生の個人情報にはセンシティブなものが多い
  - 成績・健康診断・授業料払い込み状況etc.
  - これらを最高機密のものとして守るべき→事務方に注力

おそらく必要なこと

- 事務組織内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
  - 徹底した人的セキュリティ強化へ
    - 今後は人員削減で外注が増えそう→監督強化
- 教員組織内でのコンセンサス
  - 技術セキュリティ向上のためにネットワークの構成が重要
  - 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

- 大学の個人情報保護も
  セキュリティマネジメントもまだ模索状態
- 個人情報保護では・・・
  - 漏洩リスクを減らすために個人情報は減らしたい
    しかし十分な個人情報なしに教育が成り立つか？
    - できれば条例で先行した地方公共団体での議論が知りたい
- セキュリティマネジメントでは・・・
  - そもそもガバナンスをどう確保するか
- しばらくは試行錯誤が続く