業務上知っておきたい
個人情報保護法・不正アクセス
禁止法の改正のポイント

市川昌
（江戸川大学名誉教授）

サイバーテロ対策として大学など教育機関が今できることは何か？

- 討論して欲しい法的対応の段取り？
- セキュリテイ・ポリシーの徹底と見直し
- 情報センターの役割と責任のシステム化
- 緊急体制における事務局長、学長、学部長、学生部長、広報部長への連絡体制
- 教員、事務職員、研究生、学生への注意喚起と相互協力体制
- 外部の警察、保護者会、地域自治体と協力

個人情報漏えいリスクの対応

（1）情報アクセス権と責任者の特定
（2）個人所有のPC,USBメモリーなどの
　ネットワーク、DB接続の制限と管理の点検
（3）外部持ち出し禁止・パスワード、認証設定
　外部委託事業の監督責任
（4）教職員、学生、外部委託事業者などの
　アクセス制限、情報開示の条件を公的に確定
（5）社会的危機状況などにおけるマスコミ対応と匿名情報の公開

ICT技術に対応する法的規制

- 情報セキュリティ対応は組織的、人的な現状の見直しと機材管理、ソフトおよび管理の改善、相互研修
- 法的環境の認識と順守として5月30日施行の個人情報規制法改正に注目。
- 不正アクセス禁止法の改正点。
- 迷惑メール（特定電子メール送信適正化）規制法などへの理解と順守が必要。

個人情報の保護に関する法律および行政手続における個人識別番号利用の改正

- 個人情報の保護と有用性確保の監視監督権限を有する第三者機関の設置（個人情報保護指針の作成と本人同意のない特例禁止）
- 特定個人情報（マイナンバー）の利用促進と管理について

  ・・・・誰の情報か解読が難しい工夫「匿名加工情報」の活用促進と内部および外部不正提供漏えいの罰則強化
- 個人情報取り扱い事業者の拡大

  （小規模事業者（小規模大学5000人以下）にも適用）

個人情報の範囲の拡大

- 改正法では全ての個人識別情報を対象
- デジタル化映像の送受信・防犯カメラの映像指紋情報など身体的特徴
- マイナンバー、パスポート番号など
- 公的個人識別IDと個人付帯情報（家族、成績、学歴、病歴等）の分離管理
- 他の情報と組み合わせ個人特定可能な情報のすべて（授業料・学務成績・病歴学習歴等）

個人情報管理違反と責任の場合のリスクの罰則

- 刑事罰としてのリスク：６か月以下の懲役または30万円以下の罰金
- 民事訴訟の場合：被害者１人あたり数千円から数万円の集団補償
- 漏えいによる大学など教育機関の信用低下
- システム改善・データなどの復旧・機器設置のコスト拡大
- 外部委託協定などの賠償責任の明確化

個人情報の取り扱いの目的外利用に注意しなければならない

- 最高裁判決「早大講演会参加者名簿提供」
  - 第１６条「あらかじめ許可をとった利用目的の範囲を超えて目的外利用は不可である」
  - 参加者名簿の学外機関に提供・閲覧は原則禁止、例外には注意。
  - 第１６条の除外事項はふたつのみ
  - （１）法令に基づく場合
  - （２）人の生命、身体、財産の保護、公衆衛生

個人データ内容の正確性の確保と安全管理の社会的責任

- 第19条
  - 「個人データを正確かつ最新を保つように務めること」は事業者の社会的義務

  第20条

  「個人データの漏えい、減失、毀損の防止」
- 法律による安全管理、適切な処置を講じなければならないと事業者義務を明記

外部委託業務の指導監督責任は委託業務発注者

- 最高裁判例としての京都府宇治市の住民健康保険データ外注事故における事業当事者責任
- 外部委託事業者の孫発注による情報漏えいは、管理責任者の公的機関監督責任
- 住民基本台帳情報の剽窃とコピーのリスク
  - 法的コンプライアンスとしての指導監督
  - 外部契約条項に情報管理、事故補償
- 著作権、個人情報保護法などの遵守規定

アクション アイテム

不正アクセス禁止法の改正

- サイバー犯罪増大の為2014年年５月施行
- 不正アクセス行為はID，パスワードが第三者に窃取されると困難。不正流通の防止。
- 不正アクセスの規制強化と罰則強化
- 懲役３年を５年以下、５０万円から１００万円
- フィッシング行為の禁止、不正保管禁止。
- 不正取得罪（第４条）、不正保管罪（第６条）

標的型メールと不正アクセス

- 組織および個人標的への偽装メールの開封による不正プログラムおよびウイルスの自己増殖のおそろしさ。
- 不正プログラムによるサーバー侵入による機密・個人情報流失、教務・財務情報流失。
- 不審メールへの警戒と開封への注意。
- 標的型メールへの危機意識の徹底。
- 不正アクセス禁止法の罰則：アクセス許諾違反に3年以下懲役、１００万円以下罰金。

迷惑メール（特定電子メールの送信の適正化）規制法とは？

- 平成17年（2006）改正による送信者情報の偽装による刑事罰「スパム」情報拡散防止策。
- 受信者が送信の停止を求めても送信を続け迷惑行為の罰則：1年以下の懲役100万円以下の罰金。法人の場合は3000万円以下。
- 迷惑メール送信自体にシンプルメール・トランスファープロトコルが用いられた送信行為。
- 電子メール送信者は送信者名明示、受信拒否者への再送信禁止、法令違反の禁止。
- 架空送信者名は禁止。

サイバーテロ・インシデント対応

- サイバーテロの拡大による危機意識の徹底と、国際的、国内的な情報共有の必要性
- ただ1組織では対応が難しく共同防衛のための公的組織の拡充強化が望まれる。
- 対応職員不足：Network,OS基盤、Application、経営などの総合的知識と判断力。
- 組織対応と個人責任：標的型攻撃などの教職員賠償責任保障と学校組織の経営責任。
- 外部依頼の評価は緊急性と費用対効果の問題