知っておきたい情報漏えい対応と個人情報保護法・不正アクセス禁止法の改正

市川昌
（江戸川大学名誉教授）

サイバー攻撃の動向

- サイバー攻撃の種類、被害件数の増加
- 名誉棄損、人格攻撃から、高度化して、情報資産狙いの標的型攻撃、インターネットバンキング不正送入金、相手の見えない卑劣な犯罪。
- 不正メール添付、サイト閲覧による組織内ネットワークへの不正侵入。
- マルウエア（不正プログラム）によるメール・サイト閲覧で侵入。アカウント乗っ取り。
- フィッシングによるなりすまし犯罪の危機。

ITC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、ハードウエアおよびソフトウエアの管理の改善、相互研修
- 法的環境の認識と順守として、個人情報規制法、著作権法、不正アクセス禁止法などの改正の動向と共に、電子商取引関連法、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。

第1段階　初期対応と報告義務確認

- 情報流失･漏えいを初期段階で把握、運行一時停止、調査体制。
- 何が、どこで、影響はどこまで
- 日常的な緊急連絡体制の確認
- 情報対応の一元化
- 関係者の守秘義務の確認と広報管理
- リスク対応の意思決定システム点検

第２段階　流失･紛失･違法コピーなどの調査と回復の方法

- 初動調査のための必要点検項目
  - デジタル系、アナログ系、人間系かの違い
  - 初期段階の追跡と検証
  - 法の順守（コンプライアンス）、相互責任体制
- 状況の把握
  - 事故原因となる問題点（人間系、機械系）
  - 機器管理、システム管理、ウイルス対応
  - 単純ミス、過失、失念などへの意識向上
  - ２重チェック体制、相互補正、声かけ運動

第３段階　今後の事故防止のための防御マニュアル

- 個人情報保護委員会設置･連携
- 機器管理とともにソフト契約管理を
- 関係者相互のコミュニケーションを円滑に
- 情報資産、金融資産の脅威と危機意識
- 職員規則、雇用契約、外部契約の見直し
- 個人情報の管理と法的責任の明確化
- 教職員、管理者、従業員の教育研修

スケジュール

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）２０１５年４月改正。
- 特定個人情報（マイナンバー）の利用促進と管理について

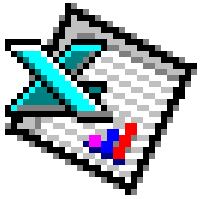
  ・・・・誰の情報か内容解読が難しい工夫「匿名加工情報」

  の適正管理と活用および不正提供漏えいの罰則強化。

  従来対象外の小規模事業者（５０００人以下）にも適用。

個人情報、個人データ、保有個人データの違いに注意

- 個人情報とは生存する個人に関する情報（第２条１・２項）
  - 氏名、生年月日、記述等による個人識別と要配慮の分離
- 個人データは取扱い事業者が管理する要配慮（第２条３項）
  個人データベースなどを構成する情報の分離、暗号化
- 保有個人データとは開示、内容の訂正、追加または削除の
  個人情報取り扱い事業者（学校教育法関連）責任
- 利用の停止、消去および
  第三者への提供などの経営判断（トレーサビリテイ確保）
  的確な個人データ処理の確認義務（第２５・２６条）



見積もり

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

第83条で「データベース盗用、不正利用の罪」明確化

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防御困難。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１年を３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：メール・侵入・不正閲覧を含む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。

サイバー攻撃・インシデント対応

- サイバー攻撃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