B-4.

情報管理者に求められる法的知識とその対応

―改正個人情報保護法・不正アクセス禁止法、著作権法の改訂、GDPRの重点事項―

市川昌
（江戸川大学名誉教授）

情報管理者として求められる法的知識とその対応とは何か？

- 知って欲しい法的対応のシステム？
- セキュリテイ・ポリシーの徹底と見直し。
- 緊急体制におけるCISO（最高情報セキュリティ責任者）と法規専門家などへの連絡体制。
- 情報センターと教職員、事務局への注意喚起と協力体制(最低限必要な法的知識とは）
- インシデント対応と法的知識による判断。

ITC技術に対応する法的規制

- 法的規制への対応は組織的、人的な現状の見直しとハードおよびソフト管理の改善、相互研修。
- 法的環境の順守として昨年５月３０日施行の改正個人情報規制法による保有個人データに注目。
- 不正アクセス禁止法の罰則強化。
- 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。
- 技術革新によるBig　Data, 情報の加工・変形・複製による多様な著作権法の改訂にも注目。

改正個人情報保護法に関する法律および行政手続における個人識別番号と利用の改正

- 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）
- 個人情報と個人データ、保有個人データの分類と管理・・個人情報よりも保有個人データ管理に注意
- 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）

個人情報と保有個人データ

- 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を含む。
- マイナンバー、パスポート番号など。
- 公的個人識別IDと、保有個人データ（家族、成績、学歴、病歴等）の分離管理、暗号化。
- 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・図書閲覧歴等）

個人情報管理違反の場合のリスクと罰則

- 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。
- 情報紛失の民事訴訟の場合：被害者1人あたり数千円から数万円の集団補償の判例。
- 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。
- 外部委託協定などに賠償責任の明確化。

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。除外行為には注意。
  - 第16条の除外事項は2例のみ
  - （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責任者の社会的責任

- 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21条
  「個人データの漏えい、滅失、毀損の防止は、当該従業員に対する指導者監督責任」
- 第35条
  個人情報の「取り扱いへの苦情には適切な処置を講じなければならない」と義務を明記

外部委託業務の指導監督責任は委託業務発注者（第22条）

- 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
- 個人情報保護法、著作権などの遵守規定

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追跡困難。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）

不正取得と不正アクセスの懲罰

- 他人の識別符号を不正取得すると1年懲役または50万円以下の罰金。（12条1号）
- 業務以外で他者の識別符号（パスワード）のアクセス管理者以外への提供・保管禁止。（5条）
- 不審メールへの警戒と開封への注意。
- 不正情報流入、流失などへの（痕跡）追跡調査。
- 不正アクセス禁止法の罰則強化：アクセス許諾違反に3年以下懲役、100万円以下罰金。（第11条）

人的安全管理処置について

- 雇用契約時における従業員との非開示契約の締結。（改正個人情報保護法・不正アクセス禁止法）
- 委託契約等における委託元と委託先との非開示契約における個人情報取り扱いなどの契約の見直しの必要性。
- 部内情報のアクセス許可権限の管理と、適切な運用、定期的な見直しと管理。

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（2005）改正による送信者情報の偽装による刑事罰。「不正メール」「スパム」情報の拡散は罰せられる。
- 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。

技術革新による著作権法の一部を改正する法的対応

- 著作権法は、昭和45年法律第48号以来大きな改訂はなく、現行の技術革新による情報環境の変化、特にインターネット社会に対応できないので大規模改訂が求められている。
- 著作権者の利害を不当に害しない限り、技術革新における情報機器に応じた公開された著作物の複製、翻案は可能とされる改正。（第2条5章）
- 私的録音・録画などの複製権の権利除外の拡大。
- 写真の撮影・録音・録画により複製または翻案する電子計算機処理に伴う著作物の権利と制限。（30条）

著作権法の学校・教育機関の技術革新による権利除外の拡大

- 第35条による学校その他教育機関による教育上で必要な限度の電子的複製ができる。複製の限度は原著作者の利益を損じてはならない。
- 公表された著作物については、教育機関の授業履修者に複製物を提供できる。また利用者に複製物を含む情報を公衆送受信できる。

『ただし許諾権、名誉棄損など原著作者の利益を損じる場合は許されない。』　（第35条の2）

『公表された著作物は、録音、録画など技術開発、実用化のため必要限度において利用できる。』（第30条）

GDPR(EU・欧州連合一般データ保護条例）General Data Protection Regulation

- GDPRはなぜ注目されるのか？
- 欧州連合による世界的な情報セキュリティの保護基準の設定への動き。
- 個人データ保護を先進国だけでなく開発途上国を含めた全ての自然人共通の利害問題として把握している。
- 国際的なビジネス開発のための規制環境を簡潔にして不当な法的障害を克服する試み。

EUにおける個人情報の定義と組織化

- 個人データとは、個人の私生活、職業、公務などに関わる全ての情報である。
- 事例として氏名、住所、写真、電子メール、銀行口座、ソーシャルネットワークなどの書き込み、医療情報、IPアドレス、私的・組織情報など。
- 国家安全保障、法執行、警察司法は個別の保護条例を含む。組織の規模は250名以上の組織に適用される。

データ管理者の責務と対応

- EU加盟国はデータ保護の単一主要監督（one stop)を設置する。
- EU加盟国は欧州データ保護委員会（EDPB)で統合。
- データ管理者は、業務の全ての執行に、データ保護影響評価を組み入れる責務がある。
- データの収集には有効な同意（Opt In)の明示が必要。児童には親または保護者。
- 個人情報としてのデータ保護の仮名・暗号化

データ管理者のデータ侵害の罰則

- データ管理者は、遅滞なく監督機関（SA)に通知義務を負う。
- データ侵害から72時間以内に報告義務。
- 事故が最初で意図的でない場合は警告のみ。
- 侵害者が企業の場合１０００万ー２０００万ユーロ（約13億ー26億円）または利益の２－４　%の罰金。データの仮名化（暗号）を条件に国際可搬性が認められる方向。

仮名化（暗号）された情報の電子処理と国際化

- 仮名化されて個人識別が不能になった情報は、可搬性があり、公共の利益にBig　Dataとして活用することができる。
- データ所有者が復号権を持つ限りは、遠隔のクラウドの記憶装置にアウトソースできる。
- 日本はEUの情報管理機構GDPBには、アメリカ、カナダ、メキシコ、ヴァチカンと共にオブザーバーに留まる。
- 将来はアジア地域にコミットの可能性。

大学とサイバーテロ・インシデントへの法的対応

- 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
- 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。（法律専門機関Net Work）
- 対応職員不足：System、OS基盤、Application、法規などの総合的知識と判断力。外部依存の危険性。
- 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法的責任の自覚。
- 外部依頼の評価は緊急性と費用対効果の問題

大学等学校経営における情報セキュリティ責任者の法的対応（まとめ）

- 組織的対応と安全管理―規程の整備と従うべき運用体制の見直し（改正個人情報保護法の精神）
- 個人識別情報と保有個人データの分離または暗号化による判読困難性の確保（改正第27条）
- 保有個人データの取り扱い状況の確認（第28条の開示、第29条の訂正、第30条の利用停止など）
- 大学内管理業務と外部法律専門家との連絡体制
- インシデント発生時における法的対応のシステム化