資料2-5

RITSUMEIKAN

情報信託機能を持つ機関が備えるセキュリティ基準について

立命館大学情報理工学部
上原哲太郎
t-uehara@fc.ritsumei.ac.jp

セキュリティ基準を検討する上で考慮するべき点

- 原則1：他のセキュリティ基準と矛盾しない
  - 多くの情報銀行はISO等の他の制度に基づいて
    セキュリティ基準を設けて遵守し
    個人情報保護法上の要請に応えていると思われるので
    それと矛盾する基準を設けることは適当ではない
- 原則2：個人情報の特性に配慮する
  - 情報銀行は個人情報を主に扱うことから
    その特性に応じた取扱いや技術が必要となる
- 原則3：事故発生時の対応を予め考慮する
  - 事故の無限責任を問われるなら事業化が困難

原則1：
他のセキュリティ基準と矛盾しない

- **ISO 27001またはJIS Q 15001の認証を必須にした上で上乗せする基準を設けることでどうか**
  - **後者がISO27001と親和性が高まっているため受け入れられやすい**
  - **マネジメントだけでは不足する技術基準、運用基準を上乗せする**

運用基準：データ加工、運用の人員、CSIRT

技術基準：クレジットカードにおけるPCIDSSと同様

標準的マネジメント基準：ISO27001、JIS Q 15001等

原則2：個人情報の特性に配慮する

- 取扱の透明性の確保や本人の関与の仕組みが必要
  これを基準で義務づける
- 機微性が異なる場合があるので例外的取扱を規定
  - 有名人の住所、トランスジェンダーの性別など

- 仮名識別子への置換・匿名加工や
  PPDM対応の撹乱、
  トレーサビリティ確保のためのダミーデータ挿入
  などが併用された場合に
  管理要件の緩和がどの程度可能か決める必要

原則3：
事故発生時の対応を予め考慮する

- 事故は絶対に許されないという風潮下では
  実際に流出が発生すると公表が遅れ被害は拡大
- 素早い対応や公表に対するインセンティブが必要

- 平時の事故監視体制や事故発生時の対応体制を
  基準に入れることで事故対応への迅速さへの
  動機付けをする
- 免責を受けられる基準なども必要？

技術基準のイメージ

- 開発・保守に関わる人員のスキルに関する基準（資格等）
- 暗号技術に関する基準
  （CRYPTREC準拠、JCMVP対応、TLSの扱い…）
- 既知脆弱性への対応基準
- 機微情報を扱うネットワークの構成に関する基準
  - L3分離、L4制限、監視技術導入など
- 運用前セキュリティ検査の基準
- 匿名加工等のデータ加工の程度と技術対策の関係
- その他…

- 技術基準にどの程度準拠しているかを
  外部に公表する仕組み

運用基準のイメージ

- 運用に携わる人員の資格や体制の基準
- 平時のログ管理や攻撃監視、CSIRTとの連携に関する基準
- 定期的脆弱性検査に関する基準
- 脆弱性発見時の対応体制に関する基準
  - SLAとの関係
- 事故発生時の対応報告公表体制に関する基準

- これらの基準の成熟度を外部に公表する仕組み

基準そのものの改訂

- 基準は情報銀行事業の実態に応じ頻繁に改訂が必要
  - そのためにも基準策定は自主的な取り組みに
- その改訂時対応も基準に含める

- 目標は「準拠することで万一の事故の一部が免責できる」基準