

ネットワークにおけるセキュリティと個人情報保護

土屋俊
(千葉大学)

観点

- 「技術」ではなく、
 - 技術開発は結局いたちごっこ
- 「法律」論ではなく、
 - 立法は遅く、日本の立法過程は不透明
 - 理論、解釈は将来の課題を解決しない
- 倫理的観点
 - 俯瞰的考察 (科技庁チームでなく)
 - 価値を中心として同時代同時進行的に

素朴な疑問

ネットワークにとってよいことは、社会にとってよいことか？

- 「ネットワークにとってよいこと」
= 「ネットワークのセキュリティ」
- 「社会にとってよいこと」
= 「ネットワークにおける個人情報保護」

プライバシーの放棄は必要悪か

- 公害は産業発展の必要悪であったか

参考までに (Richardsonレポート、1973) Code of Fair Information Practicesの5原則

- 存在を秘匿された個人情報記録追跡システムは認めない
- 自分の個人情報の内容と利用を個人が知る手段の保証する
- 収集目的外の目的で同意なく個人情報を利用することの阻止する手段を保証する
- 自分に関する情報を訂正する手段を保証する
- 個人情報を収集・蓄積・利用・配布する機関は、情報の信頼性を保証し、濫用誤用を予防する警告をする

個人情報(個人に関する、その個人を同定できる情報)

- 身体 (biometricな情報: 指紋、虹彩紋、DNAなど)
- 行動 (“data shadow”, VIN, PSN, RFID, etc)
 - Ross Stapleton の例: 1993年のInternetで148件
 - わが同僚M氏の場合
- 位置 (Corona, Landsat, SPOT, EOSATetc)
 - SPOT: 50 cents/acre, KFC, 携帯
 - EOSAT: IRS-1C(インド), 5.8mの解像度, 固定資産税
- 自分の将来 (健康情報、保険会社の情報)
- 属性 (選好、収入、などなど)
 - 通信販売(Direct marketing)、OPT OUTの機能は十分?
 - 名前、肖像
 - 病歴 (Hungchinton氏病、185delAGと東欧系ユダヤ人)
 - 健康統計 (アイスランドとdeCode Genetics社: 同意、秘匿性、利益、学術的公開性)
 - 著作物

個人情報情報を収集する意義

- 利益
- 公共サービス
- (国家と社会の) 安全保障 (セキュリティ)
 - テロ対策、ドラッグ対策
- ネットワークセキュリティ
 - 認証 (ログインからeCommerceまで)
 - システムの保護 (サイバーテロ対策、なりすまし対策、ネットワーク利用犯罪対策)

個人情報保護を保護する意義

- 個人の尊厳、基本的人権を守る
- 個人の不利益を守る
 - ジャンクDM
 - ストーカー
 - 差別(不平等) - 人権でもあるが
- 社会の安定を守る
 - 「陰謀」を防ぐ

しかし、

1. ネットワークの進歩は、(すでに事例でみたように)個人情報技術的保護そのものの不可能にしているのではないか？
2. 社会的インフラとしてのネットワークの進歩は、セキュリティを保証して一層発展するためには、個人情報の保護に制限を加えることを要求しているのではないか(表現・報道の自由の問題は別として)？

1 に対しては、YES

2 に対しては、NO

結論にかえて

- ネットワーク上の個人情報保護の努力がないと、むしろ社会が不安定になるかもしれない(インフラだから当たり前)
- ネットワーク上の個人情報の保護は倫理的手法によって行われなければならない(ガイドラインなど、教育など、)
 - 逸脱的犯罪者は、犯罪者として扱う
 - 事例は、犯罪ではないが個人情報が保護されていない状況を示している(しかも、他の権利との調停を考えると法律で禁止するのは困難)
 - 政府の役割、国際間、個人セクターの役割

ネットワークに