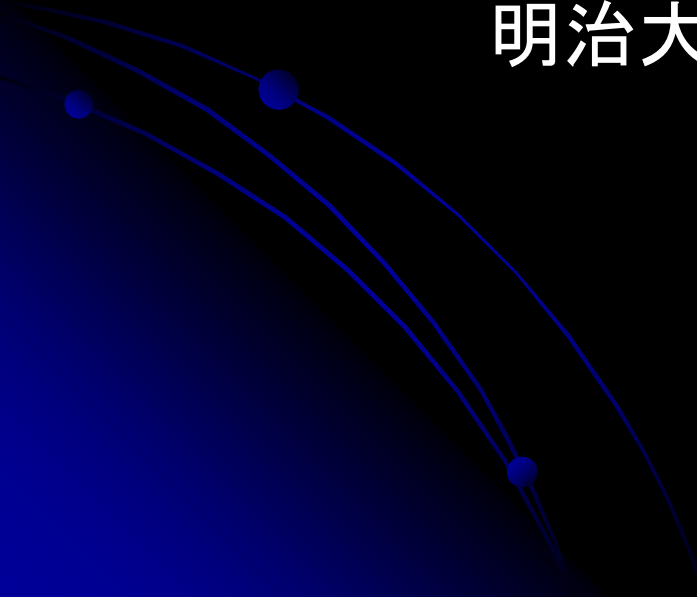


JIPDEC 地方自治体個人情報保護セミナー2008年10月

プライバシーと個人情報の保護

明治大学法学部教授・弁護士
夏井高人



プライバシーの概念

- 宴のあと事件第一審判決(昭和39年9月28日)
 - 近代法の根本理念の一つであり、また日本国憲法によって立つところでもある個人の尊厳という思想は、相互の人格が尊重され、不当な干渉から自我が保護されることによってはじめて確実なものとなるのであって、そのためには、正当な理由がなく他人の私事を公開することが許されてはならないことは言うまでもないところである。
- プロッサーの4類型
 - (1)原告が一人で他人から隔絶されて送っている私的な生活状態への侵入。
 - (2)原告が知られたくない私的な事実の公開。
 - (3)原告について一般の人に誤った印象を与えるような事実の公表。
 - (4)原告の氏名又は肖像を、被告の利益のために盗用すること。

個人データの電子的処理の影響

- データベースへの格納・集積
- 大量処理
- 移転の容易性(時間・距離)
- データの濫用または不適切な管理
 - 予め定められた目的の範囲を逸脱する利用
 - 権限のない者による利用
 - 権限を超過してなされる利用
 - 故意・過失による公開
 - 故意・過失によるデータの消失・改変等

電子化されたデータとプライバシー

- OECD理事会勧告8原則(昭和55年(1980年)9月)
 1. **収集制限の原則** 個人データの収集には、制限を設けるべきであり、いかなる個人データも、適法かつ公正な手段によって、かつ適当な場合には、データ主体に知らせめ又は同意を得た上で、収集されるべきである。
 2. **データ内容の原則** 個人データは、その利用目的に沿ったものであるべきであり、かつ利用目的に必要な範囲内で正確、完全であり最新なものに保たなければならない。

3. **目的明確化の原則** 個人データの収集目的は、収集時よりも遅くない時点において明確化されなければならない、その後のデータの利用は、当該収集目的の達成又は当該収集目的に矛盾しないであつ、目的の変更毎に明確化された他の目的の達成に限定されるべきである。
4. **利用制限の原則** 個人データは、第9条(目的明確化の原則)により明確化された目的以外の目的のために開示利用その他の使用に供されるべきではないが、次の場合はこの限りではない。
 - (a) データ主体の同意がある場合、又は、
 - (b) 法律の規定による場合
5. **安全保護の原則** 個人データは、その紛失もしくは不当なアクセス・破壊・使用・修正・開示等の危険に対し、合理的な安全保護措置により保護されなければならない。

6. **公開の原則** 個人データに係る開発、運用及び政策については、一般的な公開の政策が取られなければならない。

個人データの存在、性質及びその主要な利用目的とともにデータ管理者の識別、通常の住所をはっきりさせるための手段が容易に利用できなければならない。

7 **個人参加の原則** 個人は次の権利を有する。

(a) データ管理者が自己に関するデータを有しているか否かについて、データ管理者又はその他の者から確認を得ること。

(b) 自己に関するデータを、i1)合理的な期間に、ii2)もし必要なら、過度にならない費用で、iii3)合理的な方法で、かつ、iv4)自己にわかりやすい形で自己に知らしめられること。

(c) 上記(a)及び(b)の要求が拒否された場合には、その理由が与えられること及びそのような拒否に対して異議を申立てることができること。

(d) 自己に関するデータに対して異議を申立てることができること及びその異議が認められた場合には、そのデータを消去、修正、完全化、補正させること。

8. **責任の原則** データ管理者は、上記の諸原則を実施するための措置に従う責任を有する。

地方自治体における個人情報

- 法令・条例の定めに基づく個人情報の収集
 - 地方税徴収のためのデータ
 - 住民基本台帳データ
 - 地域衛生上のデータ
 - 教育上のデータ
 - 自治体警察が収集するデータ
 - その他のデータ
- 個人情報の保護と情報開示請求

法的ルールに住み分け

- 基本法制

- 民間事業者 個人情報保護法
- 国及び国の機関 行政機関個人情報保護法
- 独立行政法人 独立行政法人等個人情報保護法
- 地方自治体 個人情報保護条例

- 関連する法制

- 日本国憲法に定める公務員の中立性, 公平性の確保
- 国家公務員法, 地方公務員法に定める守秘義務など

- 競合する領域

- 事務委託などの場合

何が問題か？

- 個人情報の管理について、国民や住民は国や自治体を信頼できなくなってしまった(例：年金データの問題)
- 個人情報の管理について、国民や住民はデータ処理事業者を信頼できなくなってしまった(例：宇治市の個人情報漏えい事件)
- 公務員の資質について、国民や住民は何も信頼しなくなってしまった(例：大分県の教員採用試験における不正)
- 管理体制それ自体の欠陥(例：教員の私用PCやメモリの紛失事故、ゴミ処理場からの情報流出など)

何が検討されなければならないか

- マネジメントシステムの重要性を正しく理解する
 - PDCAサイクル
 - 基本方針と管理策, 詳細な実施手順
 - 実行と点検, 再評価(見直し), 第三者監査
 - 予算
- 地方自治体職員に対する教育
 - 管理職に対するマネジメント教育
 - 一般職員に対するOJT
- 非違行為に対する対処
 - 問題点の把握と改善
 - 非違行為者に対する断固たる対処(処罰, 懲戒処分)
 - 情報の適切な公開
 - 損害に対する公平かつ妥当な弁償
- 職員の採用と査定
 - 一定の要求水準に達しない職員は採用しない
 - 職員教育によって改善が見られない場合には解雇する

要約すると

- プライバシー侵害や個人情報の管理の失敗をリスクとして理解すると、セキュリティの問題の一種として認識することができる。
- 対応策として、
 - 物的なセキュリティの確保は当然のことだが、
 - 人的なセキュリティはもっと重要。
- しかし、
 - 悪しき慣行や馴れ合いが横行している。
 - 「ことなかれ主義」が蔓延している。
 - 断固とした措置を講ずることのできるリーダーが存在せず、権限も曖昧になっている。
 - 財政悪化により予算を確保できない。
- したがって、このままでは**日本の未来はない**。
- 子孫のためにどのような日本(世界)を残すかについて、本気で考えるかどうか、そのために必要な教養と想像力をどのようにして培い活用するかが最大のポイント。