

法律はあなたのプライバシーを守ってくれるか？

～プライバシーの数理的定式化と法律への適用～

どんな研究？

日本における法的なプライバシー権侵害の問題は、1960年代に示された判例にもとづいて処理されています。しかし高度情報通信社会では、この判例でうまく処理できない問題も起こりつつあります。数理的なアプローチで、これを解決するための研究を紹介します。

どこが凄い？

プライバシー概念を数理的に厳密に定式化し、これとプライバシー権侵害による不法行為の成立要件と比較検討することで、法学者が従来指摘しなかった、同定可能性要件がかかえる問題を見出しました。また、これに代わる要件として、自己情報性を提案しました。

どんな風に役立つ？

高度情報通信社会において私達のプライバシーを守るための、合理的なプライバシー概念を定式化するのに役立ちます。たとえば、生体センサや街頭監視カメラなどがいたるところにある現代社会で、プライバシー概念を明確化し、将来の法令化につながります。

法的プライバシー (従来の社会通念)

最重要判例: 「宴のあと」事件判決

プライバシー権侵害による不法行為の成立要件

- 故意または過失
- 私事性
- 非公知性
- 公開性
- 感情侵害性
- 同定可能性

匿名性の否定(≒同定可能性)が
プライバシー権侵害の前提

数理的プライバシー (新たなとらえ方)

iさんがaという属性を持つ事実($\theta(i, a)$)に関する情報を、観測者jから隠す。

$$\text{プライバシー: 属性 } a \text{ を隠す} \\ \theta(i, a) \rightarrow \bigwedge_{a' \in A} P_j[\theta(i, a')]$$

⇔ 対称的(双対)

匿名性: 個人 i を隠す

$$\theta(i, a) \rightarrow \bigwedge_{i' \in I} P_j[\theta(i', a)]$$

匿名性とプライバシーは互いに独立な概念
(一般には、含意の関係にない)

高度情報通信社会がもたらす、新たなプライバシー権侵害

ある人の属性情報が集積(バイOMETリック情報の収集、街頭カメラやセンサネットワークによる行動監視、インターネット上での仮名の名寄せ、など)

その人を同定することなく、属性情報を介してはたらきかけが可能(襲撃、誹謗中傷、など)

匿名性が保たれていても、**プライバシー権侵害**が起こり得る!

数理的プライバシーにもとづく新たな要件: 自己情報性

同定可能性: 他人から見て、公開された情報から当該個人が分かるかどうか

自己情報性: (他人からどう見えるかにかかわらず)それが自己に関することからかどうか

➡ プライバシー概念の明確化、法令化

関連文献

- [1] 真野健, “プライバシー侵害に係る定義の検討における数理的表現方法の利用 – 同定可能性の問題を中心として –”, 情報ネットワークローレビュー, Vol. 9, No. 2, pp.54-66, 2010
- [2] 真野健, “匿名性とプライバシーのためのフォーマルメソッド”, 情報処理, Vol. 49, No.5, pp. 530-536, 2008

連絡先

真野健 (Ken Mano) 協創情報研究部 情報基礎理論研究グループ
E-mail: mano.ken@lab.ntt.co.jp ({at} の部分を @ に置き換えてください)