6U-05

個人情報保護と災害時情報共有に生じるトレードオフ解決機構の設計

萱場啓太　　高橋晶子
（独）国立高等専門学校機構　仙台高等専門学校

1　はじめに

東日本大震災時，インターネットを介して大量の安否情報や災害情報（以下災害時情報と呼ぶ）が利用者同士で共有された．災害時情報共有では，利用者自身の個人情報を開示するほど，自身に適した有用な情報を得ることができるが，それに伴い個人情報が悪用されるリスクも高まる．すなわち，個人情報保護と災害時情報共有にはトレードオフの関係が生じる [1]．プライバシバイデザインの重要性の高まりとともに，利用者の意思を考慮しつつ，このトレードオフを解決することが非常に重要な課題となっているが [2]，一般利用者が自身の意思に基づきこの問題を解決することは困難である．

そこで本稿では，客観的に評価されたリスクだけでなく，利用者の個人情報を保護したいという個人情報保護意思と有用な災害時情報を得たいという災害時情報要求意思を考慮してこのトレードオフを合理的に解決する手法を提案する．

2　関連研究

プライバシとサービス品質に生じるトレードオフを解決する手法としては，GrIP（Granularity Control Mechanism based on Person Identification Probability）が提案されている [3]．GrIP は個人が特定されるリスクを表すパラメータである特定確率を基にこのトレードオフを解決する．また，プロバイダが既に持っている氏名や年齢などの利用者背景情報や利用者が現在おかれているコミュニティの情報，および利用者の希望する匿名度を考慮して個人情報の開示を制御することでこのトレードオフを解決する手法が提案されている [4]．

しかし，これらの手法では，サービスが扱う個人情報項目に対して利用者が持つ個人情報保護意思，およびそのサービスの各種機能に対する利用者の利用意思を考慮してこのトレードオフを解決することは困難である．

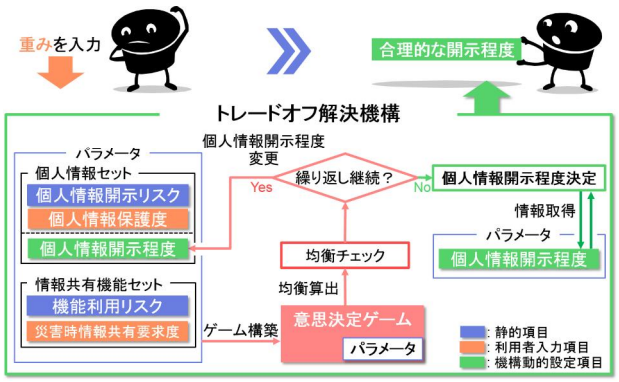

図 1: 個人情報開示程度決定手法の概要

そこで本稿では，自身の個人情報保護意思と災害時情報要求意思に基づき利用者が入力するそれぞれの意思の重み，および客観的に評価されたリスクから利用者意思決定ゲームを構築し，このゲームを用いてトレードオフを合理的に解決する機構の設計について述べる．

3　トレードオフ解決機構の設計

本研究で提案する個人情報開示程度決定手法の概要を図 1 に示す．個人情報セットと情報共有機能セットは，それぞれサービスが扱う個人情報項目と災害時情報共有機能項目に対応するパラメータ集合である．個人情報開示リスクは，個人情報セットが対応する個人情報項目が持つ客観的に評価されたリスクである．機能利用リスクは，情報共有機能セットが対応する災害時情報共有機能項目を利用した際に，利用者の個人情報項目に与えるリスクの程度を表す．個人情報保護度／災害時情報共有要求度（以下情報共有要求度と呼ぶ）は，それぞれ自身の個人情報保護意思／災害時情報要求意思に基づき利用者が入力する意思の重みである．個人情報開示程度は，個人情報セットが対応する個人情報項目の開示程度であり，個人情報開示程度が 0.0 のときは非公開，0.5 のときは半公開，1.0 のときは全公

Design of Mechanism Solving Tradeoff between Privacy and Quality of Information
Keita Kayaba, Akiko Takahashi
National Institute of Technology, Sendai College

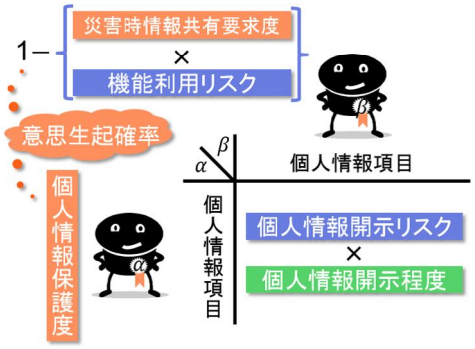

図 2: 利用者意思決定ゲームの表現

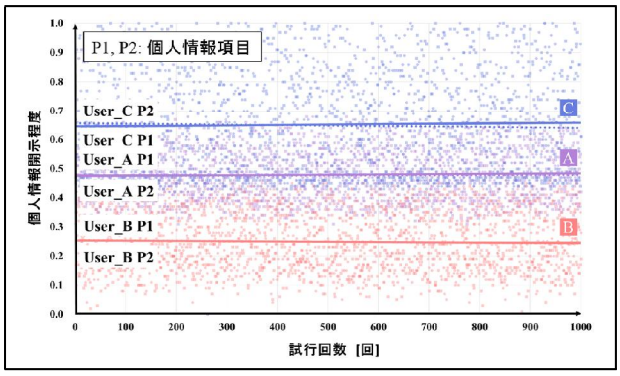

図 3: 3 種類の利用者を想定した機構動作実験結果

開を意味する．トレードオフ解決機構は，個人情報セットおよび情報共有機能セットに基づき利用者意思決定ゲームを構築し，これのナッシュ均衡を用いて個人情報開示程度を決定することで，個人情報保護と災害時情報共有に生じるトレードオフを合理的に解決する．

利用者意思決定ゲームの表現を図 2 に示す．本ゲームは，利用者の個人情報保護意思と災害時情報要求意思をそれぞれ合理的なプレイヤ α, β として，ゲーム理論の枠組みに基づき構築される．これにより，客観的に評価されたリスクと自身の意思の重みを考慮する完全合理的な利用者の個人情報開示に関する意思決定を可能にする．

4 実験

本提案の実現可能性を確認するために，利用者意思の重み入力に関する実験を行った．本実験では，3 種類の利用者を想定して意思の重みを決定し，それぞれの利用者に対してトレードオフ解決機構が示す合理的な個人情報開示程度を確認する．

本実験では，トレードオフ解決機構が扱う個人情報項目と情報共有機能項目をそれぞれ 2 つとした．3 種類の利用者は「個人情報保護意思と災害時情報要求意思が拮抗している利用者 (User_A)」,「個人情報保護意思が大きい利用者 (User_B)」,「災害時情報要求意思が大きい利用者 (User_C)」を想定した．また，利用者意思の重みの範囲を以下とし，この範囲内で無作為に値を決定した．

$$User\_A\text{: } [0.4, 0.7]\ for\ P\ and\ D$$
$$User\_B\text{: } [0.7, 1.0]\ for\ P,\ [0.0, 0.3]\ for\ D$$
$$User\_C\text{: } [0.0, 0.3]\ for\ P,\ [0.7, 1.0]\ for\ D$$

ここで，P, D はそれぞれ個人情報保護度，情報共有要求度を表し，$[X, Y]\ for\ P\ and\ D$ とは，個人情報保護度および情報共有要求度を X から Y の範囲で決定することを意味する．

また，個人情報開示リスクと機能利用リスクはすべて 0.5 とした．この条件下でトレードオフ解決機構を 1000 回動作させた．

実験結果を図 3 に示す．図 3 では，実験によって得られた個人情報開示程度と，それを利用者と個人情報項目それぞれについて線形近似したグラフを示す．図 3 より，線形近似グラフが対応する利用者は，上から順に個人情報保護意思が小さい（災害時情報要求意思が大きい）ことが分かる．これは，個人情報保護に重きをおく利用者に対しては低い個人情報開示程度を，災害時情報共有に重きをおく利用者に対しては高い個人情報開示程度をトレードオフ機構機構が示すことを意味する．これにより，本提案の実現可能性が示された．

5 おわりに

本稿では，個人情報保護と災害時情報共有に生じるトレードオフを合理的に解決する機構を設計し，複数の利用者を想定した実験を行うことでトレードオフ解決機構の実現可能性を確認した．今後は利用者意思の入力手法やリスクの決定手法について検討し，実験を行うことで本提案の有効性を確認する．

謝辞 本研究は日本学術振興会の科学研究補助金（若手研究（B）26730054）の助成を受けて実施された．

参考文献

[1] 下羅弘樹，野田五十樹：災害時情報共有のための動的アクセス権限機構を備えたデータベース管理システム，人工知能学会「社会における AI」研究会 第 12 回研究会予稿集 (オンラインプロシーディングス) (2011).

[2] 佐古和恵：パーソナルデータエコシステム構築に向けて，情報処理学会誌，Vol. 55，No.12, pp.1361–1367 (2014).

[3] 宮本崇弘，竹内亨，奥田剛，春本要，有吉勇介，下條真司：プライバシとサービス品質のトレードオフを考慮した個人情報制御機構の提案，電子情報通信学会第 16 回データ工学ワークショップ (DEWS2005) 論文集 (2005).

[4] 一知浜本，康之田原，昭彦大須賀：ユーザ背景情報及びコミュニティ状況を考慮した匿名度制御によるプライバシ保護エージェントの提案 (エージェント応用，＜特集＞ソフトウェアエージェントとその応用論文)，電子情報通信学会論文誌.D，情報・システム，Vol.94，No.11，pp.1812 1824 (2011).