ロボットがもつプライバシー情報と保護技術

電気通信大学／北京理工大学　新井健生

１．ロボットが取得しうるデータ

製造業で用いられる産業用ロボット（以下 IR と略記）と，人や社会に様々なサービスを提供するサービスロボット（SR）などがあり，現状実用化されているものと今後実用に供されるロボットが考察の対象となる．プライバシーを念頭に置くと，IR，特定個人に特化する家庭用 SR（HSR），オフィスや病院など特定多数を対象とするオフィス SR（OSR），公共で不特定多数を対象とする公共 SR（PSR）を分けて考察する必要がある．これらを，ユーザ，技術的に可能と思われる保持可能情報，保持形態，利用形態の視点で整理，分類したものが発表資料 P2~P5 である．

２．ロボットがもつ情報保護の必要性

日本では 2005 年に個人情報保護法が施行，その後ビッグデータの利活用の進展に伴い 15 年に改正個人情報保護法の成立，16 年に個人情報保護委員会が発足するなど，情報社会における個人情報の取り扱いについて社会全体が敏感になってきた [1)]．このような視点で，ロボットの持つ個人情報も，同法律に照らし合わせて適切に取り扱う必要性が生じた．ロボットの持つ情報が適切に保護されず漏洩すると，例えば IR や OSR では，企業や法人が持つ生産・運用管理や開発計画，企業戦略などの重要データが漏洩する危険性がある．PSR では，公共情報が不正利用されることにより，公共の利益や安全が侵される可能性が生じる．HSR では，まさに個人情報が漏洩することになり，その情報が悪用され，しつこいターゲティングや，保険審査における不利益，不当な濡れ衣や搾取，盗難や DV 再被害など犯罪の危険性が高まる．

３．プライバシー保護技術の概要

データベース（DB）を対象とするプライバシーは 2 種類あり，DB に対して質問をする質問者のプライバシーと，DB 中に個人データがある個人自身のプライバシーに分けられる [2)]．前者では質問者の位置やアドレスを秘匿する技術や，質問内容の改ざん，準同型性暗号処理を用いた質問内容の秘匿などがある．後者では個人名は乱数やハッシュ関数を使い仮名化する技術，同じ属性値を多数人がもつように変形する k -匿名化 l -多様化技術，更新ＤＢに雑音を付加して元ＤＢとの差が検知できなくする差分プライバシー法などが開発されている．これらの技術はロボットがもつプライバシー情報を適切に保護する上で十分に応用可能な技術である．

４．ロボットの安心モデル

ロボットの物理安全と安心の関係は，独立 2 事象のモデルとして記述できることを提案している [3)]．プライバシーに関する保護安全と安心についても，図 1（発表資料 P13 を改訂）に示すとおり同様に議論することが可能と考えられる．情報の漏洩や不正利用はなかなか感知しがたい現象であるから，プライバシーの危険が重大であるにもかかわらず，当事者

は全く気付かず安心している状況が多々ありうる．適切な保護制度や保護技術の開発と運用により，プライバシーの安全性を高めると同時に，危険な状況下のプライバシーに対してその漏洩を感知し，当事者へそのことを通知し注意を喚起することも重要なアクションと考えられる．

５．まとめ

ロボットにおけるプライバシー保護技術に関しては，情報分野で開発された多くの技術が適用可能と考えられる．ただし，ロボットはユーザが必要とするサービスを提供する上でリアルタイムにＤＢを更新しており，秘匿データへの移行は時間と状況に大いに依存するため，その仕分けに工夫を要すると考えられる．１．で議論したＤＢの外部との接続状況や利用形態については，坂田先生が提案されたレベル分類に従うのが合理的と考えられる．このレベル分類は，保持情報の内容や動作形態，利用形態も考慮して細分化を図るのが良いと考える．なおこの作業は，データを個人 ID，疑似 ID，機微情報，その他情報に分類し[4]，それぞれのデータの秘匿や活用のあり方について法律の視点から十分に議論する必要がある．これらの作業は今後の専門委員会や，適宜設置する作業部会などで実施し，できればある程度まとめて 2020 年 9 月の RSJ オーガナイズドセッションで発表できると良い．また，議論の中で新たな研究開発項目の洗い出しなども行い，早期に大型プロジェクト化されることが望まれる．

参考文献

1）保護と利用 個人情報巡る攻防，朝日新聞朝刊，令和 2 年 2 月 9 日第 4 面.
2）中川裕志，プライバシー保護の技術，情報管理，60，pp.710-718，2018.
3）新井健生，安心なロボットを考える，日本ロボット学会誌，38，pp.266-269，2018.
4）中川裕志，プライバシー保護入門，勁草書房，2016.

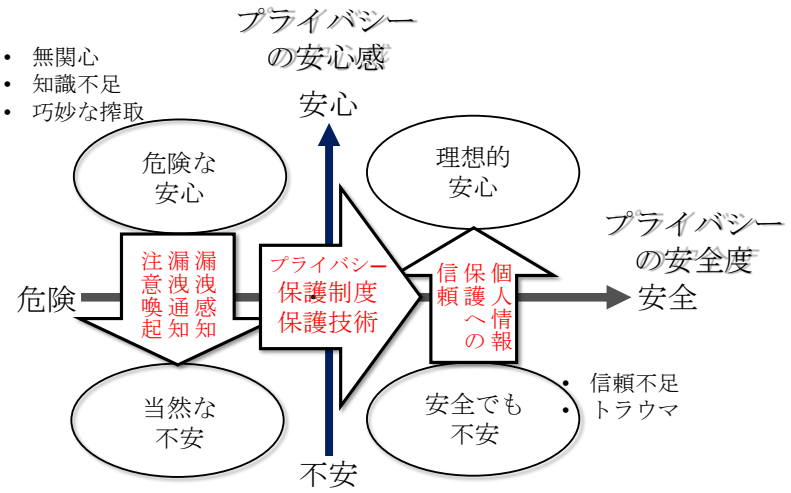

図１　ロボットにおけるプライバシーの安全と安心