情報量を利得とするゲームとプライバシー定量化への応用

川本 裕輔

（国研）産業技術総合研究所

本研究報告では、ゲーム理論と情報理論を用いて、情報量を利得とするゲームとして「プライバシーゲーム」を定義し、通常のゲームと異なる性質やナッシュ均衡点の存在を示し、このゲームを用いるとプライバシーへの攻撃と防御を定式化できることを示す。

情報量を利得とするゲームは、（通常のゲーム理論で見られるような）金額や時間などの数量を利得とするゲームとは違った性質を持つ。非常に単純な例として、A さんがコインを投げた結果（表/裏）を B さんに教える状況を考えてみよう。A さんがコインの表裏を必ず正直に伝える純粋戦略に従っていると分かっている場合、B さんに伝わる情報量は 1 ビットである。また、必ず嘘を伝える純粋戦略に従っていると分かっている場合も、伝わる情報量は 1 ビットである。一方、A さんが 50% の確率で正直に答え、50% の確率で嘘を答える混合戦略に従っていると分かっている場合、B さんはいかなる情報も得られず、伝わる情報量は 0 ビットである。ここで、A さんから B さんに伝わった情報量を B さんの利得（A さんの損失）と定義すると、混合戦略の利得（0 ビット）が純粋戦略の利得の期待値（1 ビット）よりも小さい。このことから、情報量を利得とするゲームが、数量を利得とする通常のゲームと異なる性質を持つことが分かる。

本研究では、情報量を利得とする攻撃者と防御者の間のゼロ和ゲームとして、プライバシーゲームを定義する。具体的には、このゲームでは、何らかの秘密情報を取り扱い、攻撃者と防御者の行動に応じて異なる振る舞いをする確率的システムを考える。このシステムに対して、攻撃者がより多くの秘密情報を得ようと行動する一方で、防御者は攻撃者に漏洩する秘密情報の量を少なくしようと行動する。いったん攻撃者と防御者の行動が定まると、システムの確率的な振る舞いを表す行列（秘密情報と観測情報の同時確率分布行列）が定まる。攻撃者は、システムの振る舞いを観測し、観測情報から秘密情報を推測する。この際に攻撃者が得る秘密情報の量の期待値を攻撃者の利得（および防御者の損失）と定義する。ここで、情報量としては、プライバシーの定量化の研究で盛んに用いられる情報量の定義を含む一般的なクラスを扱う。具体的には、秘密情報と観測情報の同時確率分布行列を受け取って情報量（実数値）を返す関数として、任意の連続な凸関数を考える。

プライバシーゲームでは、数量を利得とする通常のゲームとは異なり、混合戦略の利得が純粋戦略の利得の期待値と等しいとは限らず、混合戦略が行動戦略と異なる場合があることを明らかにする。また、ナッシュ均衡点の存在を示し、これを計算するアルゴリズムを与える。最後に、プライバシーゲームの応用例として、通信プロトコルの匿名性やサイドチャネル情報漏洩などの定量的なモデル化について述べる。

なお、本研究報告は、Mário S. Alvim、Konstantinos Chatzikokolakis、Catuscia Palamidessi との共同研究をもとにしたもので、JSPS 科研費 JP17K12667 および日本学術振興会と Inria との二国間交流事業（共同研究）の助成を受けている．研究成果の詳細は、査読付きの国際会議論文 [1] および国際雑誌論文 [2]（著者順はアルファベット順）を参照してほしい。

参考文献

[1] Mário S. Alvim, Konstantinos Chatzikokolakis, Yusuke Kawamoto, and Catuscia Palamidessi. Information leakage games. In *Decision and Game Theory for Security - 8th International Conference, GameSec 2017, Vienna, Austria, October 23-25, 2017, Proceedings*, pages 437–457, 2017.

[2] Mário S. Alvim, Konstantinos Chatzikokolakis, Yusuke Kawamoto, and Catuscia Palamidessi. A game-theoretic approach to information-flow control via protocol composition. *Entropy*, 20(5):382, 2018.