SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

カードベース暗号を題材にした小中学生向け授業の報告
A Report on a Lecture for Elementary and Junior High School Using Card-based Cryptography

品川 和雅 *
Kazumasa Shinagawa

キーワード カードベース暗号，情報セキュリティ教育，授業実践

あらまし

情報技術の発展及び普及によって日常生活の様々な場面で利便性が向上している一方で，情報漏洩のリスクやサイバー犯罪の被害に合うリスクも年々高まっている．こうした背景から，小学校学習指導要領にも「情報の表現，記録，計算，通信の特性等の原理・法則と，情報のデジタル化や処理の自動化，システム化，**情報セキュリティ等に関わる基礎的な技術の仕組み及び情報モラルの必要性**について理解すること。」と明記されており，情報セキュリティ教育は全ての人々にとって重要であることが分かる．

一方で，非専門家向けの情報セキュリティ教育はしばしば，サイバー犯罪の危険性を訴え,「パスワードの使い回しを**してはいけない**」「ウイルス対策ソフトを導入**しなければならない**」等の対策方法を伝えるという展開になりがちで，一般の人々，特に情報技術に明るくない人々は，まるで脅迫されているかのような気持ちにならないとも限らない．

人々の情報モラルを高めるために重要なのが，情報セキュリティ自体に興味関心を持ってもらうことである．そのための一つのアプローチとして,「サイバー犯罪に巻き込まれないためには···」というところから出発するのではなく,「暗号理論でこんな不思議なことが実現できます」というところから出発することを考えてみるのはどうだろうか．しかし，暗号理論を理解するためには，基礎知識（数学など）が必要であり，全ての人々を対象とする授業の題材としては難しいと考えられている．

カードベース暗号ならこのような状況を打開することができるかもしれない．カードベース暗号とは，物理的なカード組を用いて秘密計算を実現する分野であり，実際にカードを並べて自分の手でプロトコルを実行することができるため，正当性や安全性を体験的に学ぶことができるという特徴がある．そのため，情報セキュリティ教育への応用が検討されており，実際にいくつかの大学ではカードベース暗号を題材とした講義が行われている [1].

本稿では，カードベース暗号を題材にした小中学生向け授業プラン「秘密計算を体験しよう」の授業実践の報告を行う．筆者はこの授業プランを 2021 年 10 月 17 日に小中学生 32 名に実践した．授業終了後に受講生に感想文を書いてもらい，その結果 32 名中 26 名が五段階評価の最高評価「５とても楽しかった」を，残りの 6 名が次点評価の「４楽しかった」を選び，非常に好意的な反応をもらうことができた．結果として「カードベース暗号なら小学生から秘密計算を楽しく学べる」ということに関して確信を強めることができた．

参考文献

[1] 水木敬明, “カードベース暗号の教育への応用,” 電子情報通信学会 ISEC 研究会報告集, 2016.

* 茨城大学, shinagawakazumasa@gmail.com