付録P

「秘密を共有する—情報秘匿プロトコル」の学習

学習活動

準備物

メモパッド、ペン

解説

•

授業展開の例を示す。(約 40 分)

実習「個人情報の平均値を計算しよう」

1. クラスをそれぞれ数名程度のグループに分け、共同作業をさせることとする。
2. グループで秘密にしている（またはお互いに知られていない）個人の情報を示す数値にはどのようなものがあるかを考えさせる。(例えば、テストの点数 , 体重 , 小遣いの金額等)
3. その中の一つ（ここでは例として「年齢」を用いる）について、その平均値を求める方法があることを伝える。そして、どうすればそれが出来るかを考えさせる。
4. 最初の子どもにメモパッドを渡し、いちばん上の紙に適当に選んだ 3 桁の数字をこっそり書かせる。(例：613)
5. 同じ子どもに 1 枚目を破り取らせ、次の紙に、1 枚目に書いた数字に自分の年齢を加えた値を書かせる。(例：621)
6. メモパッドを次の子どもに渡す。表に書かれている数字に自分の年齢を足して 2 枚目に書かせ、1 枚目を破り取り、隠し持たせる。この作業を、最後の子どもが終えるまで続ける。
7. メモパッドを、最初の子どもに戻す。その子に、自分が手に持っている最初の数字（613）を、最後に書かれた数字 (657) から引いてもらう (657 − 613 = 44)。平均年齢は、この数値を子どもの人数で割ることで計算することができる (44 ÷ 5 = 8.8)。
8. 子どもたちに、各自が持っている紙を全員が破ってしまえば、隣どうしで相談しない限り、他の子どもの年齢を誰も知ることができないことを話し、あらためて秘密が守られていることを確認させる。

応用と先生によるまとめ

この方法が他のことに応用できないかを生徒に考えさせる。例えば、賛成なら 1 を足し、反対なら何も足さないことにすれば、秘密の投票にも使える。本実習の応用として試してみるのも良い。また、世の中のコンピュータには、我々の個人情報がたくさん収められていることを示すと共に、それらが他の人と共有せざるを得ない場

合があることを意識させる。