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ます。

応用と展開

このやりかたは、秘密の投票にも使えます。賛成の場合は 1 を足し、反対の場合は何も足さないことにすればよいのです。もし誰かが 1 より大きい（あるいはマイナスの）値を足してしまうと投票は不正なものとなりますが、全員が賛成したときに賛成数が人数より大きくなり不正がばれるリスクを冒すことになります。

実際のコンピュータでは

世の中のコンピュータには、我々に関する多数の個人情報が収められています。例えば、銀行の収支や納税金額、運転免許を取得してからの年数、クレジットカード使用履歴、試験の点数、医療履歴などです。したがって、プライバシー保護はたいへん重要なのです。ところが、これら個人情報のいずれかを他の人と共有せざるを得ない場合があります。例えば、店での買い物をデビットカードで支払う際、私たちは店が自分の銀行にその支払ができるだけの残高があることを確認する必要があることを知っていて、それを許しています。

私たちはしばしば、実際に必要となる以上の個人情報が相手に提供されていることを経験します。例えば、ある店で電子決済をするとき、店には誰がその口座に預金していて、口座番号が何番で、氏名は何であるかがわかってしまうでしょう。さらに、口座を設置している金融機関は、その人がどこで買い物をしたかがわかってしまいます。原理上、金融機関は顧客がどこでガソリンや日用品を購入したか、毎日こうした消費にどれだけの支出をしているか、いつそこへ行ったかを記録監視することによって、その履歴を作成することができます。現金ですべての支払いをすれば、こうした情報が開示されることは一切ありません。ほどんどの人はこうした情報共有の事実にはそれほど危惧をいだいていませんが、情報が濫用される可能性はあり、これがターゲット型マーケティング（例えば、航空券をよく購入する人に旅行の広告が送り付けられるなど）、差別（富裕顧客のみに特化した金融機関利用者に対する優良サービスの提供など）、あるいは脅迫（やや後ろめたい取引についての詳細をばらすぞという脅しなど）に使われることさえありえます。特にこうした経験がなくとも、自分の行動が誰かに監視されていると考える人は、購買行動を変える必要があるかもしれません。

このようにプライバシーが明らかになることはかなり広く許容されていますが、それでもなお、現金での取引と同程度のプライバシーを確保しながら電子商取引を可能にする暗号プロトコルは存在しています。自分の銀行口座から店の口座へのお金の移動が、どこにあるお金がどこへ送られているか知られずにできるということを信じるのは難しいことです。しかし、この学習を通した、限られた範囲の情報共有と巧みなプロトコルがこれを可能にするという体験によって、そうした取引について、少しは納得できるようになるでしょう。

参考文献

デビッド・ショームは、次のような挑発的なタイトルの論文を書いています：「Security without identification: transaction systems to make Big Brother obsolete」（識別情報なしのセキュリティ：ビッグブラザー（訳注：ジョージ・オーウェルの小説「1984 年」に描かれた巨大国家における一党独裁体制を率いる謎に包まれた全知全能の絶対君主）を時代遅れにする取引システム）。この論文は非常に読みやすく、情報秘匿プロトコルについてシンプルな例を挙げ、完全に非公開の取引が「電子通貨」を使うことで可能となることを示しています。この論文は、Communication of the ACM 誌（訳注： http://cacm.acm.org/）の 1985 年 10 月号に掲載されています。[*1]

[*1]（訳注：この論文は、著者によってオンラインで公開されています。http://www.chaum.com/articles/Security_Wthout_Identification.htm）
※デビッド・ショームはデジキャッシュ社の創立者で数学者。1985 年 7 月に『暗号識別，金融取引および認証に関する装置』で特許取得。2002 年 7 月に期限切れ