秘密の扉の合言葉を知っていることの証明

ある洞窟の入り口にPさんとVさんがいる。Pさんは、洞窟内の秘密の扉を開くための合言葉を知っているが、Vさんは知らない。洞窟は入口で、右と左の二手に分かれており、奥でつながっている。しかし、一番奥で秘密の扉で仕切られており、扉を開けない限り、左から入ると右の口から出られないし、右から入ると左の口からは出られない。

Vさんは、お金を払って合言葉を手に入れたいが、Pさんが本当に知っているか事前に確認したい。一方、Pさんはお金を受取るまでは、合言葉を教えたくない。Pさんが合言葉自身を教えることなく、“合言葉を知っている事実”を証明できるだろうか？

自分が知識を持っていることを、それ以外の何の知識も相手に伝えることなく証明する手法を「ゼロ知識対話証明」といい、単純化したこの問題は“洞窟の問題”と呼ばれる。

回答は、まずPさんに右か左の好きな方から洞窟に入ってもらう。Vさんは洞窟の外で待ち、右左のどちらに入ったか見ない。しばらく後に、Vさんはランダムに、右、あるいは左の口から出ろ！　と大声でPさんに伝える。ここで、もしPさんが本当に合言葉を知っているならば、どちらが指定されたとしても、秘密の扉を開けることで、指定された口から100%出ることが可能だ。

しかし、もしPさんが合言葉を知らない場合は、入った口からしか出られないため、Vさんがランダムに指定した口から出られる確率は50%となる。以上の試行を何回も繰り返すと、全部の回に指定した口から出られる確率は極端に小さく、仮に10回も繰り返すと確率は0.01%以下となる。よって、Vさんは合言葉を知っているか否かの判断が可能だ。

このゼロ知識対話証明は、暗号分野で実用化されている。インターネット上で本人認証を行う際に、パスワード自身は盗まれることがあるので流さない。その代わり認証者は、パスワードを知っている場合にのみ“解ける問題”をユーザに与えて解答させる。特に、一回きりの試行では偶然解けてしまう可能性があるので、何回か問題を繰り返すことで、パスワード保有の確証を高めるのだ。

ちなみにSF映画の中では、ある秘密の理由で登場人物の姿が変わってしまうことがある。この時、恋人に“本人”であることを証明するため“二人だけの秘密の話”をするベタな名場面がある。その秘密を他人が知らないと証明するのは難しいはずだが、対話によって失敗するのを見たことがない。“観客”に与えられた秘密の伏線が開放されない限り、物語は終わらないというセオリー通りだ。

（外園 康智）