数理の窓

ビザンチン将軍の裏切り

帝国軍VS同盟軍9か国で戦争状態にある。同盟軍は岐路にあり「攻撃」か「撤退」かで揺れている。ただ各国ではどちらの方針か決めている。残念なことに同盟軍には裏切り者の国があり、どの国か、いくつあるかも分からない。全同盟国が一堂に会さず、2国間の情報交換のみで、裏切り国以外の同盟国全体で正しく方針を伝達しあうことはできるか？

これは、ビザンチン将軍問題と呼ばれるネットワークの分散合意の有名な問題である。よく知られた解は「各国が知った情報」の情報を交換する方法で、次の4つのステップを踏む。

①まず2国間で情報交換し、1階情報として

「A国攻撃、B国攻撃、C国撤退、・・・」

を各国それぞれが得る。勿論、裏切り国からの情報は虚偽の可能性がある。

②次に「1階情報」自体を交換する。これにより2階情報として次のマトリクスを各国が得る。

A国から「A国攻撃、B国攻撃、C国撤退、・・・」

B国から「A国攻撃、B国攻撃、C国攻撃、・・・」

C国から「A国撤退、B国撤退、C国撤退、・・・」

・・・

この際にも裏切り国からは、でたらめな1階情報が送られている可能性がある。

③各国は、さらに2階情報のマトリクスを縦に見て、過半数が同じ方針を示していれば、その国の方針は正しいと判断する。

A国の判断「A国攻撃、B国攻撃、C国撤退、・・・」

・・・

I国の判断「A国攻撃、B国攻撃、C国攻撃、・・・」

④最後にこのマトリクスを縦に見ると、裏切り国以外の同盟国分の方針は完全に一致する。つまり、正しく方針が伝達されたことになり、これに基づいて攻撃か撤退か決定すればよい。ただし、残念ながら裏切り国数が3分の1以上あると、正しい伝達にならないことが証明されている。

仮想通貨ネットワーク上で用いられるプルーフオブワークの報酬システムは、“裏切り者”より“正直”な参加者を多くする仕組みである。参加者の中で、“ブロックチェーンに関する問題”[1)]を一番早く正しく解いたものに報酬が与えられる。一方で、不正を試みるものは、このような問題を何倍も解いて、正直な参加者たちに勝たねばならない。これが極めて困難で、単純に問題を解く方が“お得”なことが、ビットコインのセキュリティを支えている。

ところで、複数の人で意見交換するより、その間に一人で勝つ方法を編み出す方が勝率がよい気がしてしまう。こんなことを言うと、“裏切り者”とみなされるのがつらいところだが。。　（外園 康智）

1）新しい取引ブロックを元のブロックチェーン台帳に正しくつなぐために必要なハッシュ値を見つけるマイニングのこと。