数理の窓

プログラムの暗号パズルピース

「最後にたどり着いた部屋に、1つのパズルが置かれていた。そこには『正しい手順なら、宝が取り出せる。しかし一手でも間違うとパズル自体が破壊される』と忠告がある。外からは中身の解析は全くできない」

宝を守る物理パズルはファンタジーの世界だけかもしれないが、セキュリティソフトウェア上では実現しつつある。

大事なソフトウェアを違法コピー・改ざんから守る手段に“プログラム難読化”がある。難読化は、ハッカーの解読を難しくするために、コードを複雑に変換するものの、変換前後で全く同じ機能が保たれる必要がある。初歩的な手段として、①変数名の文字列を意味のないものにする、②1つの命令を同じ機能の複数の命令に分割する、③無駄なコード・計算式を入れる、等がある。しかし、これらは、注意深く読めば解読できるので完全ではない。

よって、より先進的な“プログラム自身を暗号化する難読化*”が模索された。プログラムは復号時の盗難を防ぐため、復号なしで動作する必要がある。そして2013年に「多重線形ジグソーパズル」と呼ばれる、かなり高度な数学を駆使した手法が考案された。プログラムは複数のピースに分けられ、各ピースはランダムな要素を混ぜることで難読化される。これを正しい手順で動かすと、個々のピースのランダム性が打ち消され、パズルが解かれ、意図通りの計算が行われる。逆に、間違ったインプット・手順だと、ピースは無作為に働き、全体では意味のない結果となる。まさに冒頭のパズルだ。

難読化の応用として、違法コピー発見のための電子署名（電子透かし）が挙げられる。配布時に1つ1つのプログラムにユニークな署名IDを組み込んでおくと、プログラム改変ができない（＝署名が消せない）ため、違法コピーが見つかった場合に、どの配布IDから流出したかの識別が可能となる。デジタル著作権問題が劇的に解決できる可能性がある。さらに、自動運転、IoTの分野への応用は重要だ。搭載された自動運転プログラムがハッキング・改ざんされ、誤作動を引き起こすようなテロへの防止手段になる。

ところで、DNAは生命のソフトウェアである。解読が難しいため、ある種の難読化が施されているように思える。DNAを完全に解読できる生命がいたら、“意図的な操作”により、進化プロセスを支配できたかも知れない。よって、ある程度の難読化が生命のランダム性・多様性を生んだともいえる。DNAの奥底には、生命の創造主の署名が隠されているかも知れない。。(外園 康智)

＊暗号化による難読化は、2001年にすべてのプログラムに対する一律に可能な方法は理論上否定された。その後、2013年に安全性の定義を緩めると可能なことが示され、希望が開けた。