攻撃からの安全性を確認

電子割符方式の評価を共同研究

グローバルフレンドシップ／産業技術総合研究所

マイナンバーへのセキュリティなどでも期待される電子割符技術（秘密分散技術）。グローバルフレンドシップ（東京都渋谷区、保倉豊社長、以下GFI）と産業総合技術研究所（東京都千代田区、以下産総研）は、共同で「GFI電子割符」の安全性評価を実施。その結果、「GFI電子割符」のアルゴリズムが攻撃に対する安全性を十分備えていることが報告された。

デジタルデータの管理にあたり、公開鍵暗号をはじめとする暗号技術が普及している。電子割符技術はデータ自体をビット単位に分解して、無作為で毎回異なる振り分けによって、複数の集合（割符ファイル）に分割。基本的な考え方として、割符ファイルが全て揃えればデータを復元できるが、揃えられなければ復元不能とする形で設計されている。分割された情報単体では意味を為さない。

例えば公開鍵暗号等の一般的な暗号の考え方は、データを金庫に収納（暗号化）し錠前をかけることで複合鍵を持つ対象のみがデータを取り出せる仕組み。だが、近年の技術革新等により安全性が懸念視され、強度を高めた次世代暗号が求められている。他方、代表的秘密分散技術である同社電子割符は、安全性に対する経年劣化への耐性が期待できることが判った。

同社の電子割符技術は、高い安全性を備える秘密分散法（理論）と設計思想は同様だが、実社会で利用できる技術・ソフトウエアとして開発されている為、秘密分散法（理論）と異なる点もある。今回共同で行った安全性評価は、電子割符技術が秘密分散法の持つ安全性にどれだけ近付いているのかについて検証した。

検証にあたって「GFI電子割符」の割符生成アルゴリズムが、割符ファイルの1つを持つ攻撃者が完全に元データの復元を試みる攻撃に対する安全性を評価。その結果、「GFI電子割符」のアルゴリズムが、攻撃に対して十分な安全性を備えている点を確認。報告文では「（現時点での安全性評価で得られている内容に限るならば、充分な情報理論的安全性を持っていると考えられるレベルにある）」と記載されており、報告書想定の攻撃に対する安全性のレベルに限定すれば、同社の電子割符技術は暗号技術の標準レベルを大きく上回る結果となった。

現在、類似技術や亜種等による消費者被害発生や市場混乱等を未然防止すべく、電子割符技術の標準化に向けた取り組みが進んでおり、同報告でも「秘密分散技術の標準化を進めている秘密分散法コンソーシアムにおいて、同社技術が標準化のベースとして想定されているが、上述した現時点での安全性評価の途中経過を見る限りにおいて、当該技術の安全性はこうした技術標準化の検討に値する水準にあるものと期待できると考える」と報告されており、今回の実証実験で確認された高い安全性が、電子割符技術標準化と市場普及への追い風となることが期待される。