主役登場

データを安全に流通させられる仕組みをめざして

菊池　亮
NTT社会情報研究所
主任研究員

一般に暗号を含むセキュリティの研究は，他の分野に比べて利用者がその効果を感じづらいと思っています．例えば，既存のサービスなどに対して攻撃方法を発見し，それに対策をする営みはセキュリティ分野では一般的ですが，この営みにより利用者から目に見える効果があるのは稀です．通常は，対策によりセキュリティインシデントは未然に防げるが，何かできることが増えたわけではないからです．

実際にはこれらの営みも非常に重要なのですが，大学で暗号分野に足を踏み入れて研究を進めるにつれ，個人の志向として「せっかく研究するのだったら，できることが増えることをやりたい」と思うようになりました．そのときの考えが，自分の専門とする暗号と「今まで外に出せなかったデータを流通できるようにする」という“できること”がリンクした現在の研究テーマにつながっていると思います．

今まで外に出せなかったデータ，例えば企業の機密情報などを出してもらうために，技術では何ができるでしょうか．外に出せないデータはそもそも他者に知られたくないものだと思われるので，他人に見られてしまうことは避けたいと考えられます．これは一見，暗号化して流通させれば他人が見られなくなりそうですが，流通したデータは利用（分析）するためにどこかで一度復号する必要があり，結局そこで他人に見られてしまいます．言い換えると，データを「分析する」ために「見る」ことは必要条件になっており，切り離すことができません．しかし，このままでは他人に見られたくないデータを流通させることは困難に思えます．

この仕組みの限界を突破するために，技術を使って「見る」ことと「分析する」ことを切り離すことはできないでしょうか．私が，今主に取り組んでいる秘密計算技術は，暗号化したまま分析を行う技術です．この技術では，分析結果を計算する際にもデータは暗号化されたままのため，誰も元のデータを見ることなく分析結果を得ることができます．言い換えると，「分析する」ことはできるが「見る」ことはできないという状況を，暗号技術を用いて実現しているととらえることができます．

当然，良いことばかりではなく分析速度の低下などのデメリットもあるのですが，諸先輩方の先見の明と継続的な研究開発のおかげで一定のレベルで動くシステムができており，NTTコミュニケーションズからも商用サービスが開始されています．

現在，この技術は学術・産業界で注目を集め，Googleをはじめ多数の会社や大学が参入してきているため，今はしっかり優位性を確保できるための機能拡充や性能向上の研究開発を行っています．加えて，よりこの技術が広まって使われるようISO/IECで国際標準の策定をエディタとして主導することや，複数社での業界団体をつくり業界標準を提案していく活動も行っています．

今後は本技術やその他の技術も組み合わせ，AI（人工知能）時代のデータガバナンスを実現するためのトラステッド・データスペースの構築に貢献していきたいと考えています．