秘密分散技術の初の国際標準にNTTの秘密分散技術が採択

NTTが研究開発を行った秘密分散技術が，国際標準化機構（ISO: International Organization for Standardization）が発行した秘密分散技術初の国際標準において，標準技術として採択されました．

秘密分散技術の国際標準が確立したことにより，利用者の皆様に，国際機関から認められた安心・安全な秘密分散方式を選択していただけるようになりました．

また，NTTの高効率な秘密分散技術を含む国際標準が発行されたことで，安全なデータの分散保存を可能とするtrust-ss，オープンソースの分散オブジェクトストレージ製品「OpenStack Swift」の堅牢性補償機能に対応した高速秘密分散エンジンSHSS（Super Highspeed Secret Sharing）を，ISO標準準拠としてお使いいただけるようになりました．また，データを暗号化したまま分析を可能とする秘密計算システム（算師®）のデータ保存方式も，ISO標準準拠となりました．

■背景・経緯

IT業界におけるデータ活用の広まりに伴い，利用されるデータの容量や種類が爆発的に増加しており，災害時のデータ消失対策などデータの可用性が求められることと同時に，機微な情報の漏洩対策などの安全性も求められてきています．

このような背景のもと，データに特殊な符号化を施して複数の断片に分割することで，個々の断片からは情報が漏れず，いくつかの断片が消失しても復元が可能な秘密分散技術を用いて，可用性と安全性を両立させるオンラインストレージの実用化や，データを秘匿しながら分析も可能な秘密計算技術の研究開発が進んできています（**図**）．

秘密分散技術では主に，元データの秘匿強度を示す「安全性」や，複数に分かれた断片ファイルの合計データ量が元ファイルのデータ量に比べてどの程度大きいかを示す「容量効率」，さらに保存・復元以外に分析も行う場合に必要となる「拡張性」といった評価項目があります．

しかしながら，秘密分散技術には多くの実現手段（方式）が存在し，必ずしも学術的に安全と認められないような方式や，保存する総容量が元データに比べ非常に大

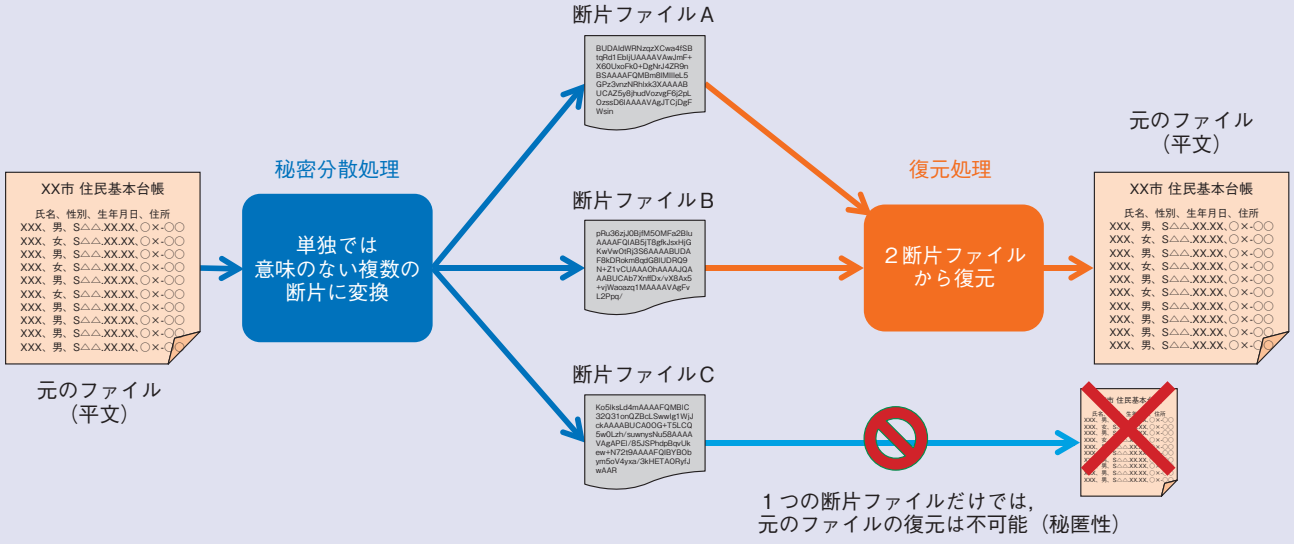

図　2つの断片から復元できるような秘密分散の例

きくなってしまう方式があり，利用者は適切な秘密分散方式を選択することが難しい状態でした．

■安全な秘密分散方式を皆様に選択いただくために

適切な秘密分散を選択できるよう，NTTはISOでの秘密分散技術の標準化において，エディタとして規格作成を主導してきました．その成果として，このたびISOから秘密分散技術の国際標準が発行されることとなり，利用者の皆様に，国際機関から認められた安心・安全な秘密分散方式を選択していただけるようになりました．

■規格内容とNTT技術について

NTTでは秘密分散技術の重要性を認識し，長年にわたり研究活動を行ってきました．NTTの研究開発では，独自の秘密分散方式1つを含む3方式を使用しており，すべてが標準として採択されました．これにより，NTTが提供する秘密分散技術を基にしたソフトウェアはすべてISO規格準拠としてお使いいただけるようになりました．

今回発行されたISO標準では5つの秘密分散方式が採択されており，それぞれ安全性，容量効率，拡張性が異なります．5つの方式のうち1方式はNTTの独自方式であり，これは標準に採録された秘密分散方式の中でもっとも容量効率に優れるものです．これを用いることにより，trust-ssやSHSSは高い容量効率を実現しています．残りの4方式は古くから知られている方式であり，NTTの秘密計算技術（算師®）はこれらの方式を複数組み合わせて使用しています．

◆問い合わせ先
NTTサービスイノベーション総合研究所
企画部　広報担当
TEL　046-859-2032
E-mail　randd@lab.ntt.co.jp
URL　http://www.ntt.co.jp/news2017/1710/171023a.html

使える技術をつくれる研究者に

研究者紹介

菊池　亮
NTTセキュアプラットフォーム研究所
データセキュリティプロジェクト
セキュリティエンジニアリンググループ

学生のときに暗号理論の研究を始め，NTTに入社後も（運良く？）暗号にかかわりながら，現在は，プライバシの問題などで外に出しづらいデータをうまく活用するための技術として「秘密計算」や「匿名化」といったキーワードの周りで研究をしています．

入社当時驚いたのは（少し失礼かもしれないですが），皆さん本当に使えるものをつくりたいんだな，ということです．現在取り組んでいる秘密計算は，入社する前は「理論的には面白くて論文は書けるが，実際には遅すぎて使えない技術」という漠然としたイメージを持っていました．おそらく私だけではなく，暗号業界全体としてそういった意識があったと思います．現在の部署に配属後，本当に使える秘密計算をつくろうとしている（そして実際につくっている）先輩方を見てとても驚いたのを覚えています．先輩方は意識も技術も当時の私の遥か先を行っており，自分が当時の先輩方の年次になっても尚，追いつけたかどうかは分かりませんが，少なくとも他の研究者から「本当につくれるんですね」と驚かれる側には回ることができました．

現在はコア技術の研究に加えて，普及のための非常勤研究員や外部委員なども掛け持ちしており忙しい日々が続いていますが，自分のかかわった技術が実際に世の中で使われて役に立つために，自分がもっとも役に立てることは何かを考えながら日々研究開発に取り組んでいます．