情報セキュリティの将来ニーズに応える暗号研究の継続的なチャレンジ

千田 浩司　　五十嵐 大　　濱田 浩気　　高橋 克巳

NTTセキュアプラットフォーム研究所

〔受賞論文〕
エラー検出可能な軽量 3 パーティ秘匿関数計算の提案と実装評価
千田浩司，五十嵐大，濱田浩気，高橋克巳（NTTセキュアプラットフォーム研究所）
情報処理学会論文誌，Vol.52, No.9, pp.2674-2685（2011）

新しいセキュリティ技術を世の中に出すまで 10 年かかるという話を聞いたことがあります．本研究もまさにこの言葉通りと思うようになりました．秘密計算（筆者らは秘匿関数計算をこう呼んでいます）は，計算を行うコンピュータにも本来のデータを一切明かさずデータ処理できるセキュリティ技術です．1980 年代には実現方式が知られていましたが，通常と比べ膨大な処理を必要とし，筆者らが知る限りまだ実用に至っておりません．

筆者らがはじめて秘密計算について学会発表したのが 2004 年，以来，安全性や高速化を追求して試行錯誤を繰り返し，このたび受賞した論文の成果を得ることができました．本提案方式は，データを 3 カ所に分散させたまま元に戻さず加算，乗算や論理回路演算を可能とし，データを保護しつつ統計分析やデータ検索等を行うことができます（**図 -1**）．当該論文の掲載後には，臨床研究医と共同で機微な情報を扱う医療統計処理に秘密計算を適用した実証実験を行い，実用に向けた取り組みに力を入れてきました（「医療統計処理における秘密計算技術を世界で初めて実証」，http://www.ntt.co.jp/news2012/1202/120214a.html）．

筆者らの研究も当初は「処理が重すぎて使えない秘密計算を速くしよう」が目的化していましたが，計算を行うコンピュータにも本来のデータが存在しない秘密計算の特長は，（当時の流行り言葉だった）ユビキタス社会に求められるセキュリティや，個人情報保護法施行に伴う国民のプライバシ意識の高まりから，将来的なニーズがあると信じて研究を進めてきました．最近ではクラウドに預けるデータの機密性確保や，「ビッグデータ」の利活用においてプライバシ問題が懸念される等，秘密計算の潜在ニーズの高まりを感じます．研究をスタートさせてから間もなく 10 年，手塩にかけた技術が実際に世の中で使われ，役に立つ日が来ることを楽しみにしながら現在も研究開発を進めています．

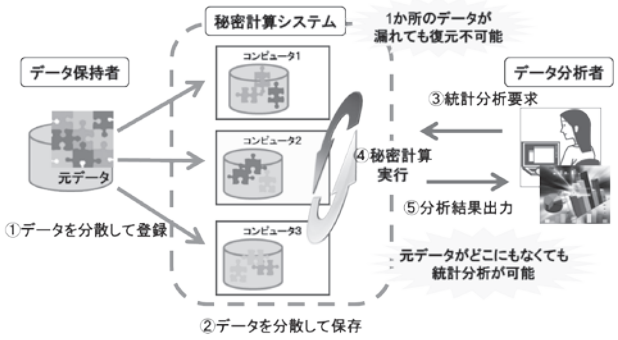

図 -1　提案方式による秘密計算システム全体像

（2012 年 4 月 16 日受付）

千田 浩司（正会員）　chida.koji@lab.ntt.co.jp
2000 年早稲田大学大学院理工学研究科数理科学専攻修士課程修了．同年日本電信電話（株）入社．博士（工学）．暗号応用技術の研究開発に従事．2001 年電子情報通信学会 SCIS 論文賞．電子情報通信学会会員．

五十嵐 大（正会員）　ikarashi.dai@lab.ntt.co.jp
2008 年東京大学大学院情報理工学修士課程修了．同年日本電信電話（株）入社．プライバシ保護データ活用技術の研究開発に従事．2008 年ソフトウェア科学会 PPL 論文奨励賞．2009 年本会 CSS 論文賞．2012 年電子情報通信学会 SCIS 論文賞．ソフトウェア科学会会員．

濱田 浩気（正会員）　hamada.koki@lab.ntt.co.jp
2009 年京都大学大学院情報学研究科通信情報システム専攻博士前期課程修了．同年日本電信電話（株）入社．プライバシ保護技術，暗号応用技術の研究に従事．2012 年電子情報通信学会 SCIS 論文賞．電子情報通信学会会員．

高橋 克巳（正会員）　takahashi.katsumi@lab.ntt.co.jp
1988 年東京工業大学理学部数学科卒業．2006 年東京大学情報理工学博士課程修了．博士（情報理工学）．1988 年日本電信電話（株）入社．情報検索，データマイニング，情報セキュリティの研究開発に従事．2000 年度本会論文賞．電子情報通信学会会員．