NTT持株会社ニュースリリース

（報道発表資料）

2012年2月14日

日本成人白血病治療共同研究グループ
日本電信電話株式会社

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

日本成人白血病治療共同研究グループ（静岡県浜松市、代表：直江知樹、以下JALSG）と日本電信電話株式会社（東京都千代田区、代表取締役社長：三浦惺、以下NTT）は、臨床研究データ※1をはじめとする秘匿が必要なデータの更なる安心・安全な活用を目的とした、秘密計算技術※2を世界で初めて実証しました。本成果により、臨床研究データを暗号化したまま統計分析を行う事が可能となり、その性能は実用化に即した速度を達成しました。

1. 研究背景および経緯

医療分野においては、学会を中心に国内の至るところで均質な医療が受けられるよう、臨床研究で証明されたエビデンスに基づき、各種診療のガイドラインや標準治療法を定める等の「エビデンスに基づく医療（EBM）」が進められています。

JALSGは1987年に多施設共同臨床研究グループの先駆けとして発足し、日本全国の白血病治療のレベル向上を目指して数々の臨床研究を実施してきました。現在では213の医療施設が参画し、成人白血病の標準的治療の確立に貢献し続けています。

ただし、臨床研究データを集約して預かる医療施設においては、患者のプライバシーを守るため、セキュリティ対策が課題となってきています。臨床研究データは個人情報のため、管理には最大限の注意を払う必要があることから、研究者・医療施設双方が臨床研究データを安全に取り扱うことができ、医療統計分析を実施可能な技術のニーズが高まっています。

NTTはユビキタス社会の実現に向けた取り組みの一環として、医療や健康管理を支えるサービスの実現に取り組んできました。その一環としてNTT情報流通プラットフォーム研究所は、データを保護する暗号研究を重ね、データを暗号化したまま統計処理の結果を得ることが可能な秘密計算技術について研究を進めて参りました。これまで秘密計算技術は理論上安全であると知られていましたが処理速度に課題があり、システムの実用化が待たれていました。

JALSGとNTTは、JALSGの臨床研究データを対象に、NTTの秘密計算技術を活用し医療統計分析を実証する研究事業を共同で開始しました。

2. 研究の成果

NTTはJALSGの臨床研究データを暗号化したまま統計処理を行い、安全かつ効率よく計算結果を導くことが可能な秘密計算技術を世界で初めて実証しました。（図1、図2）今回開発されたプロトタイプでは、平均、分散、中央値といった基本的な統計値演算や、t検定※3やKaplan-Meier法※4などの医療統計で用いられる機能が実装されています。（図3）

JALSGの約1,000症例×800項目の臨床データを用いて、汎用的なPCによる秘密計算技術の速度性能の評価を実施しました。その結果、一般統計分析では平均・分散の計算が1秒以内、中央値の計算も5秒以内で完了し、実用的な処理速度を実証しました。医療統計分析で代表的なt検定も3秒以内での処理を実現しました。

3. 技術のポイント

NTTでは、データを暗号化したまま統計処理を行い、その計算結果を安全かつ効率よく導くことが可能な秘密計算技術の実現方式を考案し、試作ソフトウェアを開発しました。本試作ソフトウェアを用いて、NTT独自の設計とアルゴリズム開発により従来にない安全性と処理効率を兼ね備えた汎用型秘密計算システムを構築しました。

（1）秘密分散※5にもとづく安全なデータ管理

データを秘密分散で保管することによりデータの機密性を担保しています。秘密分散の方法で暗号化された各々の分散データは意味のない情報で、そこから何の情報も得ることができない一方、災害時には分散したデータが全てそろわなくてもデータを復旧できる可用性を持ちます。

（2）マルチパーティ計算※6による汎用型秘密計算システムの実現

秘密計算は複数のコンピュータが安全な手順に従い協調して処理を行うマルチパーティ計算により、データを秘密にしたままの処理を可能にします。まず秘密分散の方法でデータを分散したまま算術演算（加減算と乗算）を実現し、それを用いて論理回路を構成（論理和、論理積、排他的論理和、否定演算）することで、汎用計算が可能なアーキテクチャを実現しました。また、マルチパーティ計算が正しく行われていることを確認する不正検知を行うことが可能であり、処理負荷を従来方式の1/100以下に減じることを可能にします。

（3）多様な演算処理の実現

秘密計算の基本性能を決める乗算処理は世界最高レベルである1秒間100万回を実現しました。さらに独自のアルゴリズムのデータ操作演算を開発したため、10万件ソートを20秒で行うなど、様々なデータ処理実現が実用的な時間で処理可能になりました。

4. 今後の予定

秘密計算技術を活用することで、安心・安全な臨床研究データの環境を実現し、医療の質のさらなる向上を目指します。秘密計算サーバを複数拠点へ分散配置した運用形態での検証を手始めに、インターネット等のネットワークを介した速度性能の検証等、実用化に向けた評価等を継続します。また本技術は医療業界だけでなく、秘匿が必要なデータを扱って統計処理を行う必要がある様々な業界に適用可能であり、法人向けの機密情報保護対策として有効な技術であると期待されます。今後は国が行う統計分析や、位置情報・購買情報・M2M情報※7等の秘匿が必要なビッグデータを分析する、幅広い分野での活用も推進していきます。

用語解説

※1 臨床研究データ

臨床研究データ：臨床現場で行われた医学研究によって得られた情報を指し、具体的には、患者情報や検査、診断、治療などによって得られたデータ。

※2 秘密計算技術

データを暗号化したまま処理し、処理を実行する側にはデータを一切秘密にしたまま、処理結果のみを得ることができる技術。

※3 t検定

2組の集団の平均の間に、統計学的に有意な差があるかどうかを判断する方法。

※4 Kaplan-Meier法

累積生存率を計算する方法の一種。

※5 秘密分散

データを秘匿できる形式で複数に分散する方法。

※6 マルチパーティ計算

複数のコンピュータが安全な手順に従い協調して処理を行う計算方法。

※7 M2M情報

装置やセンサーなどのモノ対モノ間でやりとりされる情報。

別紙・参考資料

- 図1 秘密計算の処理イメージ
- 図2 秘密計算における臨床研究データの扱い例
- 図3 Kaplan-Meier法の結果画面

ニュースリリースに記載している情報は、発表日時点のものです。現時点では、発表日時点での情報と異なる場合がありますので、あらかじめご了承いただくとともに、ご注意をお願いいたします。

NTT持株会社ニュースリリース インデックスへ

**NTT持株会社
ニュースリリース**

- 最新ニュースリリース
- バックナンバー
- English is Here

**NTT持株会社
ニュースリリース内検索**

1997 年 04 月 ～
2021 年 11 月
検索

NTTグループの情報は
こちらからもご覧いただけます。

NTT広報室 on twitter
NTTグループの旬な情報をチェック！

Facebook
NTTグループ 公式フェイスブックページ

▲このページの先頭へ