先端技術キーワード解説

知っておきたい最新の動き

[秘密計算（secure computation）]

AI の進展などに伴い、データの秘匿性と相互活用のニーズが増えてきています。両者を成り立たせるのは難しそうに思えます。そこで、注目されるようになったのが「秘密計算（secure computation）」です。

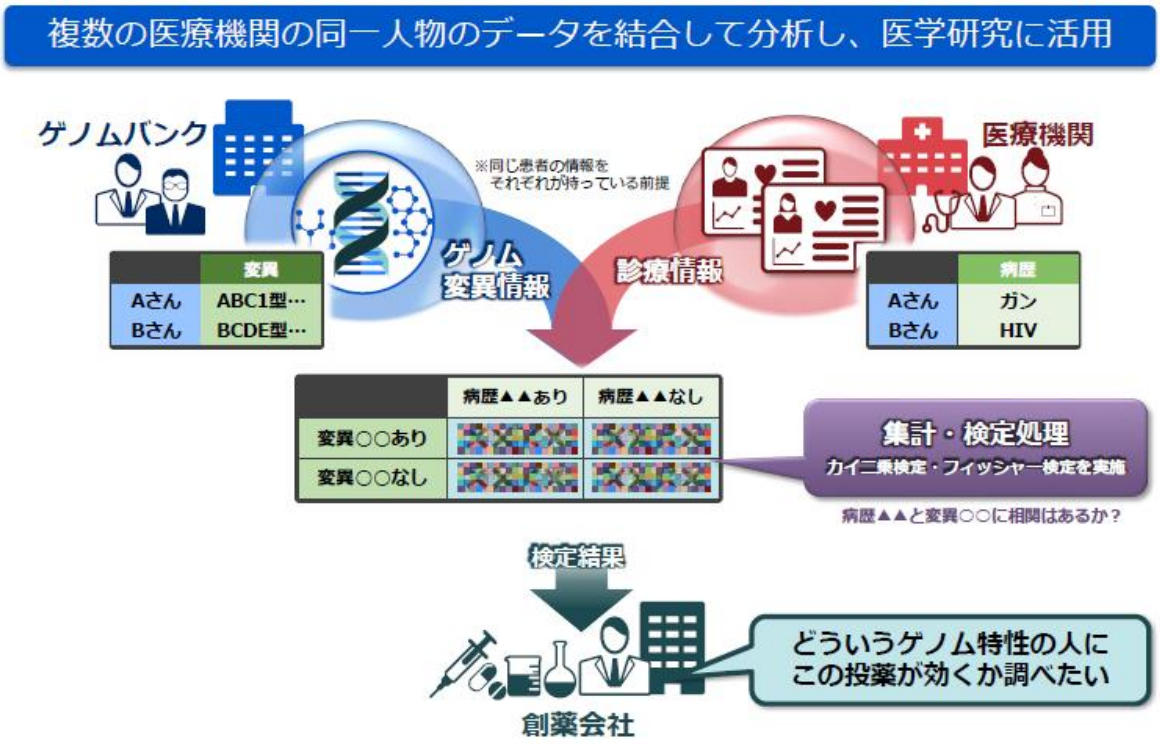
１．秘密計算とは

秘密計算とは、データを暗号化したまま計算できる技術です。これまで、計算に時間がかかることが実用化を阻んでいました。それが、近年、計算機やネットワークの性能向上に加え、高速な秘密計算用のアルゴリズムの研究開発が進み、今では、研究レベルから実用レベルに移行しつつあります。

２．秘密計算の適用分野

本技術により、個人のデータや企業の営業秘密を用いる分析業務で、データの中身を見せない運用が可能になります。これにより、より安全なデータ処理はもちろんのこと、今まで他組織に開示することが難しかったデータを持ち寄った、企業や業界の枠を越えた新しい統合分析が可能になります。

具体的な例としては、疾病と運動の相関分析による予防医療／健康指導、ゲノムと投薬の相関分析による個別化医療、金融情報の結合分析による不正送金検知、消費者データをマーケティングに利活用などがあります。



３．秘密計算を実現する技術

（１）秘密分散：NTT、NEC が取り組んでいる手法です。データを複数に分割し、さらにそれぞれを複数のサーバーへ分散して計算します。データは常に秘密分散のシェアと呼ばれる断片として暗号化された状態で扱われ、複数のサーバーへ分けられています。このため復元が極めて難しく、非常に高いレベルのセキュリティを保つことができます。

（２）Garbled circuit：Garbled circuit とは、通常の回路と異なり、入力は 0,1 ではなく、0,1 に対応したラベル K_0,K_1 を用いて計算を行うような回路です。これを利用して、サーバーにはデータを見せることなく、計算させることができます。

（３）準同形暗号：準同型暗号とは、暗号文のままで平文の加算、あるいは乗算ができる暗号です。線形演算では暗号化したままでも計算ができますが、乗算は暗号化したままではできないため、特別な工夫が必要となります。

（４）完全準同形暗号：暗号文のままで平文の線形演算と乗算の両方が計算可能な暗号です。2009 年、Gentrty によって提案されて以来、研究が進められています。

４．秘密計算の課題

現状の課題としては、秘密計算の技術にはいくつかあり、それぞれ、相互に接続することが難しいことです。今後の展開を見守りたいと思います。

［参考文献］

[1] 菊地　亮、五十嵐大：秘密計算の発展　ーデータを隠しつつ計算する仕組みとその発展、IEICE Review, Vol.12 No.1、2018

[2] NEC：情報を秘匿したままデータ解析ができる　秘密計算技術
https://jpn.nec.com/rd/technologies/201805/index.html

[3]竹之内隆夫：秘密計算の PWS2018 での議論と最近の動向、2019　（図を引用）
http://www.iwsec.org/pws/2018/slides/PWSMeetUp2019_takenouchi.pdf

（注）

本解説は、執筆当時の状況に基づいて解説をしております。ご覧になる時には、状況が変わっている可能性がありますので、ご注意をお願いします。

技術・経営の戦略研究・トータルサポータ
ティー・エム研究所
工学博士
中小企業診断士
社会保険労務士（登録予定）
代表　芳賀　知
E-Mail：info_tm-lab@mbn.nifty.com　URL：http://tm-lab@a.la9.jp/