2014 年 1 月 21 日
株式会社日立製作所

暗号化したままデータ分析を行う秘匿分析技術を開発

ビッグデータ分析業務委託時の情報漏えいリスクを低減

株式会社日立製作所(執行役社長：中西　宏明／以下、日立)は、このたび、暗号化されたデータを復号化することなく、頻度集計、相関ルール分析(*1)が可能な秘匿分析技術を開発しました。具体的には、高速検索可能暗号方式(*2)を応用することで、10 万件規模の暗号化されたデータに対して約 10 分で相関ルールの分析を可能にするとともに、暗号化されたまま分析処理を実行するため、分析受託者による盗み見や持ち出しなどの情報漏えいリスクの低減を実現しました。

近年、医療や購買履歴、位置情報センサーなどの大量のデータから隠れた価値を抽出するビッグデータ分析が大きな注目を集めています。それに伴い、分析のノウハウを持たない事業者が外部組織に分析業務を委託する分析委託サービスが活用されるようになってきました。しかし、機密性の高い自社データの分析業務を外部組織に委託する場合、情報漏えいリスクが懸念され、ビッグデータ利活用の妨げとなっていました。そこで今回、日立は暗号化されたデータを復号化することなく、頻度集計、相関ルール分析が可能な秘匿分析技術を開発しました。開発技術の特徴は以下の通りです。

（1）　秘匿分析技術の開発

日立が 2012 年 3 月に開発した検索キーワードとデータベースを暗号化したまま検索できる高速検索可能暗号方式を応用し、複数の分析キーワードが暗号化データベース中に出現する頻度を求め、それらを比較して相関ルールを調べる秘匿分析技術を開発しました。

（2）　実用的な高速性を実証

本技術で用いた高速検索可能暗号方式は、共通鍵暗号(*3)をベースに設計されており、公開鍵暗号(*4)をベースとする検索可能暗号方式に比べ約 1000 倍の速度で分析処理を行います。汎用 PC（CPU：Intel® Core™ i7-3820、メモリ：32GB 搭載）を用いた実験では、1 台の PC 上で 10 万件規模の暗号化データに対して、約 10 分で相関ルール分析を完了し、実用的な時間で秘匿分析が実現出来ることを実証しました。

本技術において、分析受託者は暗号化された分析対象データと分析用クエリ(命令)のみを用いて、元のデータを見ることなく相関ルール分析を実行します(図 1)。暗号化されたまま分析

処理を実行することにより、分析受託者による盗み見や持ち出しなどの情報漏えいリスクを低減することが可能となります。日立は今後、より安全なビッグデータ分析の実現に向けて、2014 年度中に医療分野での実証試験を行い、2015 年度中の実用化をめざします。

なお、本成果は 2014 年 1 月 21 日から 24 日まで鹿児島県鹿児島市で開催される暗号と情報セキュリティシンポジウム 2014(SCIS2014)にて発表予定です。

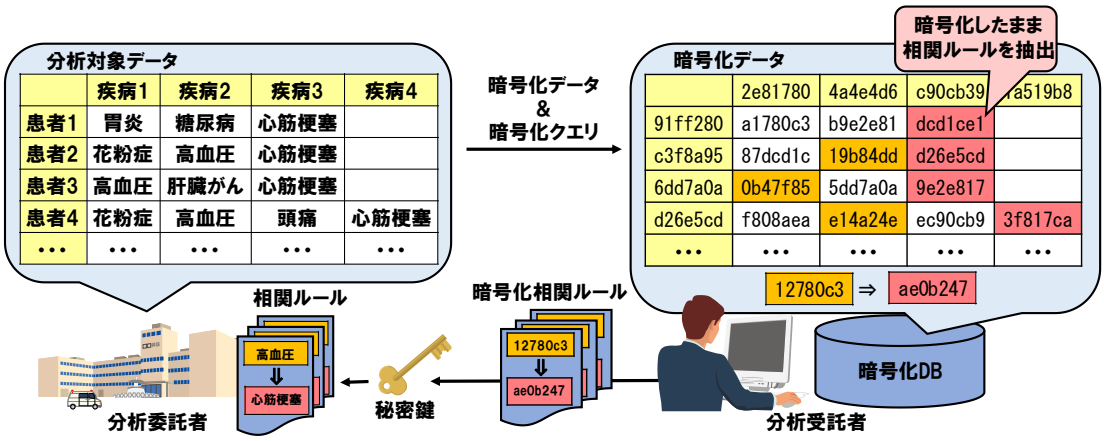

図1暗号化データベース上での相関ルール分析

*1 相関ルール分析:分析対象データ中に存在する事象間の相関を抽出するデータ分析手法、例えば大量の購買履歴データの中から「商品 A を購入」する人は「商品 B も購入」するといった事象間の相関ルールを抽出することが可能です。

*2 検索可能暗号方式:標準的な暗号機能である「暗号化」と「復号化」に加え、暗号化したまま、2 つの暗号文が暗号化前に同じデータであったかどうかを確認できる「検索」機能を有します。この検索機能は、秘密鍵を持たない分析受託者でも実行可能です。また、本技術で用いた検索可能暗号方式では、暗号化の際、毎回異なる乱数を用いることにより、同一の平文であっても全く異なる暗号文になるようにランダム性を高めています。通常、暗号化データに対して相関ルール分析を行う際には、同一の平文は同一の暗号文に変換することで、各暗号文の暗号化データ中の出現頻度を算出します。しかし、同一の平文に対する暗号文が全て同一となってしまうため安全性に不安があります。本技術で用いた検索可能暗号方式は平成 22 年度総務省委託研究「大規模仮想化サーバ環境における情報セキュリティ対策技術の研究開発」における研究成果です。

*3 共通鍵暗号:暗号化と復号化の鍵が同じ暗号方式は共通鍵暗号と呼ばれています。代表的な方式の多くは処理効率を重視して設計されており、大容量データの暗号化に適しています。

*4 公開鍵暗号:暗号化の鍵を公開しても安全性が確保できる暗号方式を公開鍵暗号と呼びます。鍵の管理が容易な反面、共通鍵暗号よりも処理が複雑になる傾向があり、暗号化、復号化により多くの計算資源を必要とします。

■照会先

株式会社日立製作所 研究開発本部 技術統括センタ [担当:吉田]
〒244-0817 神奈川県横浜市戸塚区吉田町 292 番地
電話 050-3135-3409 (直通)