2012 年 3 月 12 日
株式会社日立製作所
株式会社日立ソリューションズ

クラウド上での情報漏えい防止に貢献する検索可能暗号技術を開発

暗号化したゲノムデータベースの検索に応用

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、クラウド上にある暗号化したデータベースを、復号化することなく暗号化したまま、データの検索・照合ができる検索可能暗号技術*1 を開発しました。従来、クラウド上の暗号化したデータベースを検索・照合する場合には、いったんデータベースを復号化しなければならず、その際に情報漏えいのリスクがありました。本技術は、クラウド上で検索・照合する際にデータベースの復号化の必要がなくなるため、情報漏えいのリスクが低減し、パブリッククラウド上での機密性の高いデータベースの利活用の拡大に大きな貢献が期待されます。

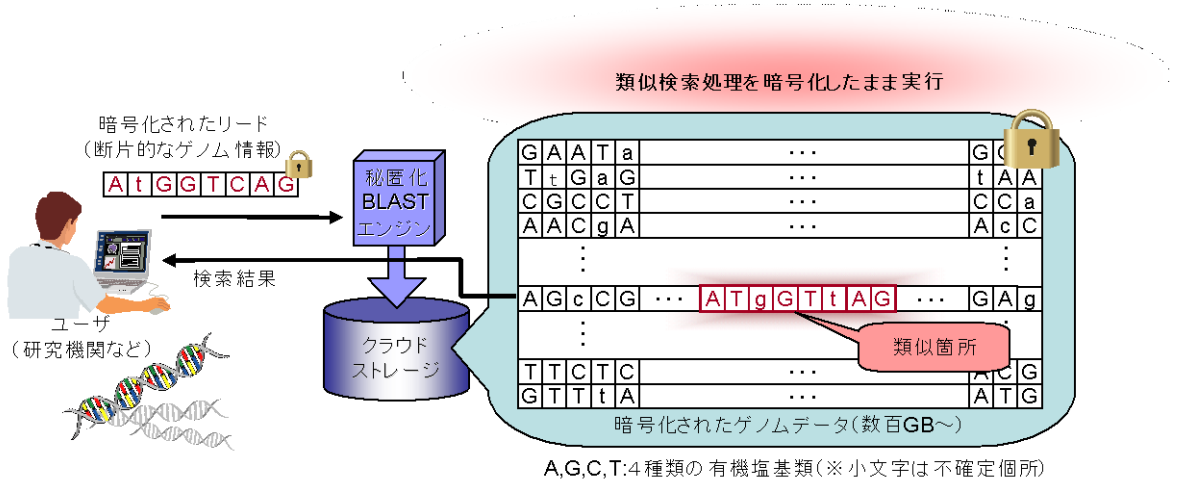
今後は、本技術を応用し、株式会社日立ソリューションズ（取締役社長：林　雅博／以下、日立ソリューションズ）と共同で、既存のパブリッククラウドでも適用可能な、ゲノムデータ解析向けセキュリティソリューションサービスとして 2013 年度中に提供開始する予定です。

なお、本技術は、総務省委託研究の平成 22 年度「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。

近年、業務のアウトソーシング先としてクラウドを活用したサービスが大きな注目を集めていますが、クラウド上に保管するデータ漏えいに対するユーザの不安が大きいため、機密性の高いデータを保管する場合には、暗号化などのセキュリティ対策が必須となっています。また、クラウド上でデータの検索・照合を行う場合には、暗号化したデータをいったんクラウド上で復号化しなければならず、その際、クラウド管理者も含めた第三者への情報漏えいに対するリスクの懸念が強く、クラウド上の機密性の高いデータベースの利活用の妨げとなっていました。

そこで、日立は、クラウド上でデータベースを復号化することなく、暗号化したままデータの検索・照合ができる検索可能暗号技術を開発しました。開発した技術は、高い安全性を保ちながら、大容量データでも検索・照合などの処理が可能です。従来は、同一データを複数回暗号化した場合、暗号文は全て同一となってしまうため安全性に不安がありましたが、本技術では、毎回異なる乱数を用いることにより、同一のデータ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。また、高速処理が可能な共通鍵暗号技術*2 を用いることで、暗号化による処理のオーバーヘッドを最小限に抑え、大容量データも効率よく検索・照合します。本技術は、データが万が一盗難されたとしても暗号文の解析が困難なため、情報漏えいの防止に貢献するとともに、クラウド上のデータベースの利活用の拡大に大きな貢献が期待されます。

開発した検索可能暗号技術は、急速に進展が進むバイオインフォマティクス（生物情報科学）におけるゲノムデータ解析での応用が期待されています。ゲノムデータの解析では、大容量のデータベースの保管や解析処理のために膨大な計算リソースが必要なため、クラウドを用いたデータ検索・照合サービスの活用が検討されています。一方で、情報の機密性の高いデータを安全に利用するためには、ゲノム解析に特有の類似検索*3 に対応した暗号化技術が必要でした。日立は、日立ソリューションズと共同で、開発した検索可能暗号技術を、ゲノムデータの類似判定に用いられる標準的なアルゴリズムである BLAST*4 と組み合わせ、ゲノムデータ解析向け秘匿検索処理技術へ応用し、既存のパブリッククラウドでも適用可能なセキュリティソリューションサービスとして、2013 年度中の提供開始を目指します。



図：検索可能暗号技術のゲノムデータ解析への応用

*1 検索可能暗号技術：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は同じデータ値であったかを確認可能な「検索」機能を有します。この検索機能は、本人以外の第三者でも実行可能です。

*2 共通鍵暗号技術：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。

*3 類似検索：誤りや不確定な部分を含むゲノムデータ同士を比較し、高い類似性を持つ個所をリストアップします。

*4 BLAST：1990 年に提案された BLAST(Basic Local Alignment Search Tool)は、大規模なデータの類似検索向けに、高速性を重視して設計されました。DNA の塩基配列やタンパク質のアミノ酸列の分析など、バイオインフォマティクス分野においては、最も広く使われるアルゴリズムの一つです。

■照会先

株式会社日立製作所 横浜研究所 企画室 [担当:塚越]
〒244-0817 神奈川県横浜市戸塚区吉田町 292 番地
電話 045-860-3092(直通)

株式会社日立ソリューションズ
〒140-0002　東京都品川区東品川四丁目 12 番 7 号
ホームページ：https://www.hitachi-solutions.co.jp/inquiry/
電話：0120-571-488

以 上
