2022 年 3 月 10 日

株式会社デジタルガレージ
株式会社イエラエセキュリティ
日本電気株式会社
日本電信電話株式会社

# 秘密計算の提供者向けの安全性基準を提案

～利用者が安心して秘密計算を利用できる世界の実現に向けて～

株式会社デジタルガレージ（本社：東京都渋谷区、代表取締役 兼 社長執行役員グループ CEO：林 郁、以下「DG」）、株式会社イエラエセキュリティ（※1）（本社：東京都渋谷区、代表取締役社長：牧田　誠、以下「イエラエセキュリティ」）、日本電気株式会社（本社：東京都港区、代表取締役 執行役員社長 兼 CEO：森田 隆之、以下「NEC」）、日本電信電話株式会社（本社：東京都千代田区、代表取締役社長：澤田　純、以下「NTT」）は、様々なデータの安全な流通・利活用に貢献できる秘密計算の安全性が秘密計算の提供者と利用者で相互に理解され、誰もが安心し秘密計算が利用できることを目的として、秘密計算の提供者向けの安全性基準を作成しました。

秘密計算はデータを暗号化したまま計算できる技術で複数の方式が存在します。これらの方式と安全性について、専門知識のない秘密計算の利用者が違いを理解することは難しいため、適切な方式を選択できないという問題がありました。今回、複数の方式で異なっていた安全性を、一般の利用者でも統一的な評価を可能とした安全性基準を作成し、公開しました。この安全性基準に則って秘密計算の提供者が利用者に安全性を説明することで、秘密計算の提供者と利用者の相互理解が促進され、結果として利用者が適切な方式を選択することができると考えています。

なお、作成した安全性基準は秘密計算研究会のホームページにて公開するとともに、秘密計算に取り組む企業や学術機関等と連携し、広く秘密計算の理解に役立つ安全性基準となるよう、継続的に議論・改善していきます。

秘密計算とは：
秘密計算は、高度な暗号理論を用いて、データを暗号化した状態のままで、データベース処理、統計分析、AI による分析等ができる技術です（※2）。データ保護性が非常に高いクラウドサービスや、複数組織のデータを安全に共有・統合して 1 つのビッグデータとして利活用できるシステムを実現する技術として、期待されています。

秘密計算の安全性の相互理解に向けた課題：

秘密計算には「秘密分散（※3）」をベースとする方式、「準同型暗号（※4）」をベースとする方式等の構成方法によって、方式の安全性、すなわち「暗号化したまま処理する」ことの定義が異なり、それぞれの方式によって異なる安全性が主張されていました。また、一部の秘密計算方式では、安全性の前提として「入力の一部が暗号化しなくても良いデータである」等の条件を持つものも存在しています。
これら秘密計算の方式によって主張する安全性が異なっていることや、方式によって必要となる前提は、秘密計算の利用者にとって理解することが困難でした。そのため、秘密計算の提供者と利用者の間で、提供される秘密計算の安全性を相互に理解することは難しく、その結果、利用者は秘密計算を利用する価値があっても理解できない故に導入を躊躇ってしまったり、暗号化されている範囲に理解の齟齬があり潜在的なリスクを利用者が抱えてしまう等の問題がありました。

秘密計算の提供者向けの安全性基準の概要と効果：
このような課題を解決するため、DG、イエラエセキュリティ、NEC、NTT は、秘密計算の提供者と利用者の間で秘密計算の安全性を相互に理解するため、今回は主に秘密計算の提供者に向け、「データを暗号化したまま処理」するために満たすべき条件を整理し、方式に依存しない統一的な基準として纏めました。また、安全性の前提があり暗号化しない部分がある場合、その部分が秘密計算のデータ保護の考えに反さないことを示すために、秘密計算の提供者が明示的に宣言するための基準も併せて提案しました。
秘密計算の提供者はこの安全性基準に則り、自身の秘密計算が安全であることを確認したり、前提により暗号化したまま処理されていない部分があれば明確にしたりすることができます。また、それらを宣言することで、専門的な知識を有しない利用者は、どこが暗号化したまま処理されているのか理解しやすくなり、提供者と利用者の相互理解が促進されると考えています。

・安全性基準文書
秘密計算技術の基本方式の安全性に関する基準およびその応用方式・応用システムの安全性の宣言に関する基準

今後の活動：
4 社は、今後も秘密計算に取り組む企業や学術機関等と連携し、本安全性基準を継続的に議論・改善していくとともに、秘密計算の提供者や利用者の相互理解を通じ、安全なデータ流通社会の実現に資する活動を行っていきます。

※1：「株式会社イエラエセキュリティ」は 2022 年 4 月 1 日に「GMO サイバーセキュリティ by イエラエ株式会社」へ社名を変更いたします。
※2：ここでは暗号鍵を用いた暗号化の他に、「秘密分散技術」を用いてデータを保護することも暗号化と呼びます。

※3：データを複数の断片に分割するものであり、それぞれの断片からは元データの情報がわからないように断片を生成する暗号技術。
※4：暗号文に対して特殊な処理を行うと、暗号化を解くことなく加算などの処理ができるような暗号技術。

■秘密計算研究会のお問い合わせ先
秘密計算研究会 事務局 （株式会社デジタルガレージ DG Lab 内）
ホームページ： https://secure-computation.jp/

■報道関係者からのお問い合わせ先
株式会社デジタルガレージ 広報担当 dg4819.pr@garage.co.jp
株式会社イエラエセキュリティ 広報担当 info@ierae.co.jp
日本電気株式会社 コーポレートコミュニケーション本部　広報室 press@news.jp.nec.com
日本電信電話株式会社 サービスイノベーション総合研究所 企画部広報担当 randd-ml@hco.ntt.co.jp