

第1回 秘密計算研究会 開催メモ

秘密計算研究会の第1回を2020年12月～2021年2月に計3回でオンライン開催し、本研究会の以下の活動内容を合意した。

■秘密計算の課題：

秘密計算には「秘密分散」をベースとするもの、「準同型暗号」をベースとするものなど、アプローチの異なる多数の方式が存在し、それぞれ独立に研究開発が進められてきている。そのため、方式によらない俯瞰した議論がされておらず、安全性や性能などを一定の基準で比較することはこれまで専門家の間でもなされていない。

結果、ユーザが様々な選択肢の中から適切な方式を選定することが容易ではなく、社会実装の妨げとなっている。

■活動目的：

秘密計算研究会は、上記の課題を解決し、秘密計算技術が広く社会実装され、クラウドサービスのデータ保護に対する不安の払拭や、組織や企業の枠を超えたデータ利活用により新たな価値が創出されることを目的とする。

■活動内容：

- 様々な秘密計算方式を俯瞰した実用的かつ客観的な安全性基準や、ユーザが秘密計算を活用する際の参考となる指針の検討
- ホームページやイベントを通じた、上記基準や指針の検討状況、方式の性能などに関する技術資料や先端事例の情報発信

■第1回 秘密計算研究会の講演者・参加企業

- ・【招待講演】日本電信電話株式会社 菊池 亮、五十嵐 大、高橋 克巳
- ・株式会社デジタルガレージ
- ・日本電気株式会社
- ・株式会社レピダム

以上