DSA フォーラム開催レポート

秘密計算が実現する安全・安心な企業間データ共有

一般社団法人データ社会推進協議会(法人番号 4011005007414)

2022 年 10 月 20 日

企業や組織をまたいだデータの共有と活用が期待されています。サプライチェーンを通じたカーボンマネジメントや物流危機への対応、人権デューデリジェンス、金融不正防止、スマートシティやスーパーシティ等々、組織を超えてデータとデータをつながなければ、いずれも実現しない世界です。

企業間のデータ共有、活用を安心かつ安全に実現する技術として注目されているのが、本フォーラムで取り上げる「秘密計算」です。秘密計算は、データの値を誰も見ず処理結果だけを共有することによってデータ保護の課題を解決し、データ共有による新たな社会価値創造を手に届く未来にしようとしています。

一般社団法人データ社会推進協議会(DSA)は、ビジョンである「データ利活用によりイノベーションが持続的に起こる世界」を実現する技術と捉えて2021年初より秘密計算活用ワーキンググループを設置し、秘密計算の理解促進や活用ケースの検討を進めています。本DSAフォーラムは日本初の秘密計算総合イベントで、内外のキーパーソンが一同に介して秘密計算の社会実装や利用促進に向けて熱いセッションを展開。最新動向や導入事例だけでなく、法制度や社会受容性といった課題も含めた共有の場となりました。

これまで難しかった企業間データ共有と活用は、秘密計算によってどう進展しうるのか。そのためにDSAや関係者に求められる役割は何か。DSAは今後もフォーラムや情報発信を通じ「イノベーションが持続的に起こる世界」へ向けた議論の場をお示ししてまいります。本レポートが、多くのみなさまに議論へご参加いただくきっかけになれば幸甚です。

一般社団法人データ社会推進協議会

目次

DSA フォーラム「秘密計算が実現する安心・安全な企業間データ共有」について

この資料は、一般社団法人データ社会推進協議会(DSA)が開催した国内初の秘密計算総合イベント「秘密計算が実現する安心・安全な企業間データ共有」の講演内容を再編したものです。

開催概要

- 開催日　2022 年 3 月 11 日(金)13:30～17:00
- 開催方法　Zoom ウェビナー
- 参加費　無料
- 主催　一般社団法人データ社会推進協議会(DSA)
- 後援

▸ 一般社団法人日本経済団体連合会

▸ 一般社団法人日本データマネジメント・コンソーシアム(JDMC)

▸ 一般社団法人 Fintech 協会

▸ 一般財団法人情報法制研究所(JILIS)

プログラム(所属・役職は開催日当日)

- オープニング

▸ 主催者挨拶
一般社団法人 データ社会推進協議会 会長
東京大学大学院 情報学環・教授　越塚 登

▸ オープニングメッセージ(秘密計算への期待)1
一般社団法人日本経済団体連合会 デジタルエコノミー推進委員会委員長
日本電信電話株式会社 取締役会長　篠原 弘道 氏

▸ オープニングメッセージ(秘密計算への期待)2
一般財団法人 情報法制研究所 理事長
新潟大学大学院 現代社会文化研究科・法学部 教授
理化学研究所 革新知能統合研究センター 客員主管研究員　鈴木 正朝 氏

▸ 開催主旨:秘密計算とは
一般社団法人データ社会推進協議会
利活用促進委員会秘密計算活用主査　竹之内 隆夫

- 招待講演

▸ 招待講演 1:秘密計算の国際動向
MPC Alliance President and Co-Founder　Frank Wiener 氏

▸ 招待講演 2:秘密計算に関する法的論点

一般財団法人情報法制研究所 理事
ひかり総合法律事務所 パートナー弁護士　板倉 陽一郎 氏

- 招待講演 3:プライバシー保護連合学習技術の実証実験
  国立研究開発法人情報通信研究機構サイバーセキュリティ研究所研究所長　盛合 志帆 氏
- 招待講演 4:秘密計算の普及に向けた課題と取り組み
  国立研究開発法人産業技術総合研究所
  サイバーフィジカルセキュリティ研究センター 首席研究員　花岡 悟一郎 氏
- 招待講演 5:秘密計算に関する国際標準の動向について
  ISO/IEC JTC 1/SC 27/WG 2 エキスパート NTT 社会情報研究所 研究主任　菊池 亮 氏

● DSA 会員企業による秘密計算実用化に向けた事例紹介

- 『プライバシー強化技術に関する取り組みのご紹介』
  株式会社日本総合研究所先端技術ラボ エキスパート　近藤 浩史 氏
- 『NEC の秘密計算に関する取組みについて』
  日本電気株式会社技術価値創出本部　衛藤 嘉之 氏
- 『秘匿情報管理サービス「匿名バンク」の導入事例』
  株式会社日立製作所研究開発グループ 東京社会イノベーション協創センタ
  価値創出プロジェクト プロジェクトマネージャ　佐藤 嘉則 氏
- 『秘密計算コンソーシアム主催 2 社と SBT の目指す秘密計算の未来』
  株式会社 Acompany 代表取締役 CEO　高橋 亮祐 氏
  株式会社 EAGLYS 代表取締役社長/CEO　今林 広樹 氏
  SB テクノロジー株式会社経営企画本部 事業戦略室 シニアストラテジスト　福嶋 健二 氏
- 『秘密計算に関する NTT コミュニケーションズの取組み』
  NTT コミュニケーションズ株式会社
  スマートワールドビジネス部 スマートヘルスケア推進室担当課長　櫻井 陽一 氏
- 『デジタルガレージの秘密計算の取り組み』
  株式会社デジタルガレージ DGLab CTO (Security)　竹之内 隆夫 氏

● パネルディスカッション『秘密計算の期待と課題、普及に向け今後求められるアクション』

- パネリスト
  - 一般財団法人情報法制研究所理事ひかり総合法律事務所 パートナー弁護士 板倉 陽一郎 氏
  - 日本電気株式会社 NEC フェロー　江村 克己 氏
  - 一般社団法人日本データマネジメント・コンソーシアム 理事　田口 潤 氏
  - 国立研究開発法人情報通信研究機構サイバーセキュリティ研究所 研究所長　盛合 志帆 氏
- ファシリテーター　一般社団法人データ社会推進協議会 理事　若目田 光生

● 閉会挨拶　一般社団法人データ社会推進協議会 理事　若目田 光生

参加者属性

参加人数　　316 名

アンケート回答者数　　83 名

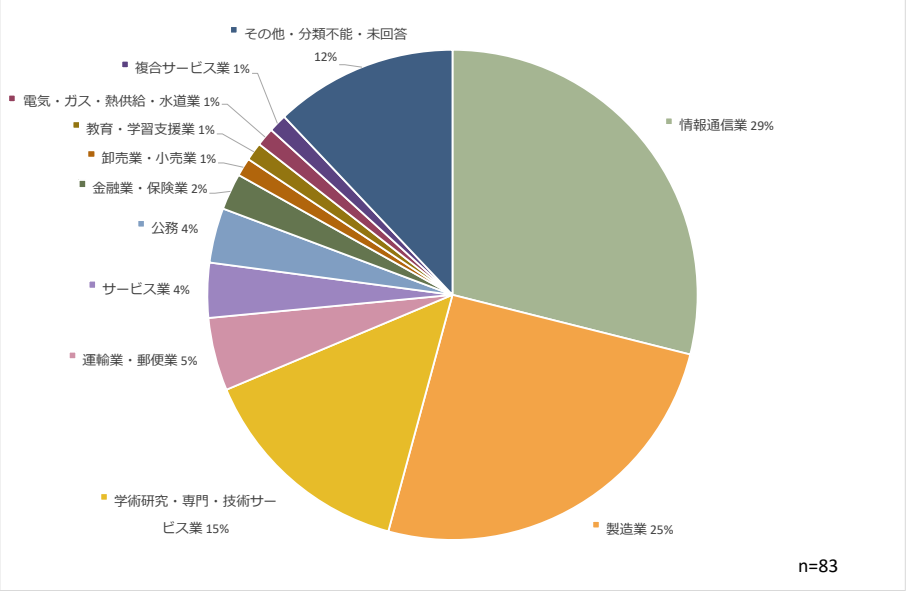


図 1 参加者属性(業種)

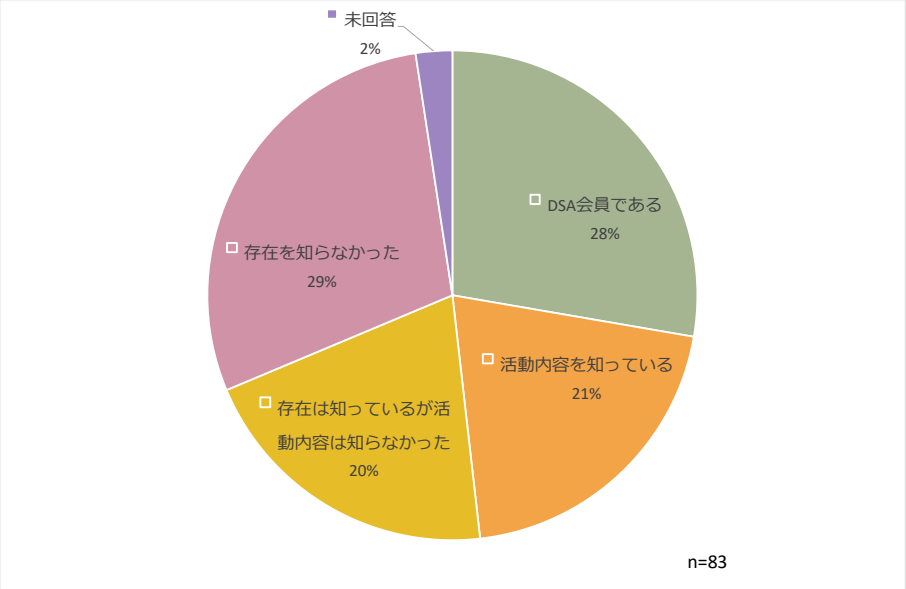


図 2 参加者属性(DSA との関係)

主催者挨拶

一般社団法人 データ社会推進協議会 会長
東京大学大学院 情報学環・教授
越塚 登

「秘密計算が実現する安心・安全な企業間データ共有」フォーラムへのご参加誠にありがとうございます。一般社団法人データ社会推進協議会(DSA)は、前身である旧一般社団法人データ流通推進協議会と一般社団法人官民データ活用共通プラットフォーム協議会が 2021 年 4 月に合併して発足し、ちょうど約 1 年を迎えます。この間 DSA は世界にも存在感を示すデータ基盤、日本のデータ空間として DATA-EX に取り組み、様々な課題に直面してきました。なかでも企業間の秘密やプライバシー等の保護、守りと社会便益やビジネス価値創造の両立はもっとも重要かつ大きな課題で、世界的にも重要と認識されています。データを扱う企業間の秘密をどう保持し、どうプライバシーを守っていくのか――。

こうした課題を解決するいくつかの手法のひとつが、今日のテーマである秘密計算です。暗号化された状態で処理、計算が可能ならば、企業秘密やプライバシーの保護とデータ活用により創出される知見の共有を両立できます。秘密計算のほかに Google 等が採用する連合学習など、分散したデータコンポーネント間での機械学習時の秘密を保持する方法もあります。技術によってメカニズムは異なりますが実現したい世界観は共通していて、いままさにホットなトピックといえるでしょう。データ社会共通の課題解決手段をいち早く取り上げ、こうした議論の場を設けることは、DSA の重要な価値であり責任だと感じます。本日のセッションに大いに期待します。

日本は、新分野の技術に先鞭をつけること、個々の技術を一点集中で深化していくことに長けています。他方、技術をプラットフォーム化したり、法制度やルールへ取り込んだりすることは、得意ではありません。一点突破ではなく産業社会全体の面にしていくことが苦手です。しかしデータは、プラットフォーム上で連携してこそ価値があります。日本が得意でなかったプラットフォームや法制度をどうしていくかがもっとも大切であり、DSA が取り組むべき領域です。秘密計算に限らず技術は沢山存在しますが、それをどう社会に役立つようプラットフォーム化していくのか。制度にしていくのか。個人情報保護法への影響も考慮すべきかもしれません。最先端の技術や DATA-EX 構築へ向けた取組みにおいて、そうした議論を重ねる場の提供は DSA の価値です。

あらためて、今日の視聴者、登壇者にお礼申しあげます。ともに実りあるフォーラムを創っていきましょう。

オープニングメッセージ 1「秘密計算への期待」

一般社団法人日本経済団体連合会 デジタルエコノミー推進委員会 委員長
日本電信電話株式会社 取締役会長
篠原 弘道 氏

日本初の秘密計算総合イベント開催を、心からお祝い申しあげる。データ活用の重要性が叫ばれるなか、時機を得たフォーラムである。持続成長へ向けたデジタル・トランスフォーメーション(DX)にデータ活用が重要なことは自明だ。これまでもビッグデータ、量が注目されてきたが、いまやより重要度を増しているのは、データの種類だ。1 種類のデータではなく、様々組み合わせることで生まれる価値が期待されている。

日本には沢山価値あるデータが存在するが、致命的な弱点がある。多様な組織にデータが分散していて単独企業では多種作用組み合わせることが難しい、いわゆるサイロ化現象だ。それが日本における DX のアキレス腱になると懸念する。経団連では業界や会社を超えたデータ活用、共有が極めて重要と考え、価値創造型 DX、すなわち企業、スタートアップ、アカデミア、自治体や政府、医療機関等がデータ共有を通じ価値を共創するモデルを提案してきた。しかしデータ共有にはプライバシー問題や自社データ開示の不安が大きなハードルになっている。

本日テーマの秘密計算は秘匿を前提としており、複数の組織が互いにデータを生で開示することなく統合して活用できる。前述の DX のハードルを乗り越える解決策として非常に大きな期待を抱いている。10 年前知ったときは実装可能な計算処理が限定的だったが、深層学習にも適用できるようになり、応用範囲も格段に広がった。

越塚会長の指摘以外に、解決すべき課題は大きく 2 点ある。安全の根拠について一般データ活用ユーザーの理解を得るかという課題が 1 点目。秘密計算は高度な数学的手法で実現されているため、安全のロジックを一般の方が理解するのは難しい。RSA[1]等も原理を知らずに使われていると思うと杞憂かもしれないが、機微なデータほど活用ユーザーは慎重にならざるを得ない。安全性をどう活用ユーザーに理解してもらうのか、認証制度等を考えるのかといった課題がある。

2 つ目は将来へ向けた課題だ。秘密計算の実現法は複数存在するため、普及してきた段階で複数の秘密計算システムをどう連携させていくか。何れにせよこれらの課題は、今日のようなフォーラム活動を通じた課題解決に期待する。

技術の作り手、法制度専門家、秘密計算の潜在的ユーザーであるデータ活用専門家が一堂に会するこうした場は極めて重要だ。日本でのデータ活用すなわち DX 推進には、秘密計算が国内で広く認知され活用されていく必要がある。こうしたイベントが、今回だけでなく継続的に開催されることを期待する。

[1] Revest-Shamir-Adleman cryptosystem。公開鍵暗号の一種で、電子署名アルゴリズムとして普及している。

オープニングメッセージ 2「秘密計算への期待」

一般財団法人 情報法制研究所(JILIS) 理事長
新潟大学大学院 現代社会文化研究科・法学部 教授
理化学研究所 革新知能統合研究センター 客員主管研究員
鈴木 正朝 氏

JILIS では、本日企画者の若目田、竹之内両氏らの提案で 2018 年 8 月から秘密計算技術応用研究タスクフォースを設置し、高木浩光理事中心に内外専門家を招き議論を重ねてきた。報告書は 9 割以上まとめたが最終稿調整で 1 年止まっている間に両氏が経団連や DSA で着々と秘密計算の研究意義や社会実装へ向けたデータビジネスの協調領域としての基盤整備を進めてこられた。意義を再認識し敬意を表するとともに、法的視点から一緒に取組み貢献していきたい気持ちで今日を迎えている。

折しも 3.11 だ。11 年前の震災では、世界が衝撃をもって映像を目撃し、内外の方々が現地で救助、復旧、復興に尽力した。しかし医療や自治体のデータ利活用は各地で目詰まりが生じ、助かる命を失った。我々は立法論におけるデータ利活用の切実な課題として 2000 個問題の解消を提言してきたがコロナでも同じ問題が起き、改正個人情報保護法の公民一元化によってようやく解消の見込みが立ったところだ。経団連からも提言を得て 10 年かかりやっと個人データの保護と利活用の土台が整理され、このあとの標準化に道筋がついた。

DFFT では、ルールと権限の一元化により個人データの議論が可能になる。標準化やハーモナイゼーションの統一された窓口があって初めて GAFA 交渉や個人情報保護統制の申し入れができる、その準備が整った。この整備なくドメスティックな法的対応にとどまれば、秘密計算関連法はグローバルなビジネス展開にも欧米型人権保障にも全く対応できず、ビジネス展開に禍根を残す。グローバルな問題提起、ルールメイキングへの参加が不可欠である。

JR 東日本の Suica 事件や米国で先行した Netflix 事件は、匿名加工と仮名加工の違いを認識させる契機だった。統計化、匿名化、仮名化に加えて秘密計算という第 4 のパーソナルデータ利活用手法を技術、ビジネス基盤、そして法の観点で模索しているのが現在地だ。法的にはいずれも個人情報・個人データとは何か、データ保護の目的とは何かを問う作業といえる。前述の JILIS 報告書中断は、まさに個人情報保護法の根本問題解決なく秘密計算の法的説明は困難という課題に突き当たったためで、必要な回り道に時間がかかった。

個人情報の定義は令和 3 年改正で公民同一に統合され条文上解決したものの、択一ではない 2 つの解釈が併存する点は要注意だ。一般の取扱いと開示請求では法目的と制度趣旨が異り、使い分ける必要がある。匿名・仮名加工実務の拠り所は自社データベース、他の情報は提供元の基準だが、データ提供先で識別や暴露のリスクが伴う情報開示や情報公開請求は提供先の他の情報との照合性が論点だ。自社データベースを他の情報と捉え、無自覚に揺れているのが現在の日本だ。非個人情報の解釈でデータ利活用しようとする際、2 つの解釈に気付かないと大問題になる。地方自治法専門家、立法担当者、企業法務部、法曹界も無自覚だ。

JILIS は法制度の面から秘密計算に貢献していく。今日は技術的、ビジネス的、法的に第 4 の利活用の道をみんなで探っていく契機にしたい。

開催趣旨「秘密計算とは」

一般社団法人データ社会推進協議会　利活用促進委員会秘密計算活用WG　主査
竹之内隆夫

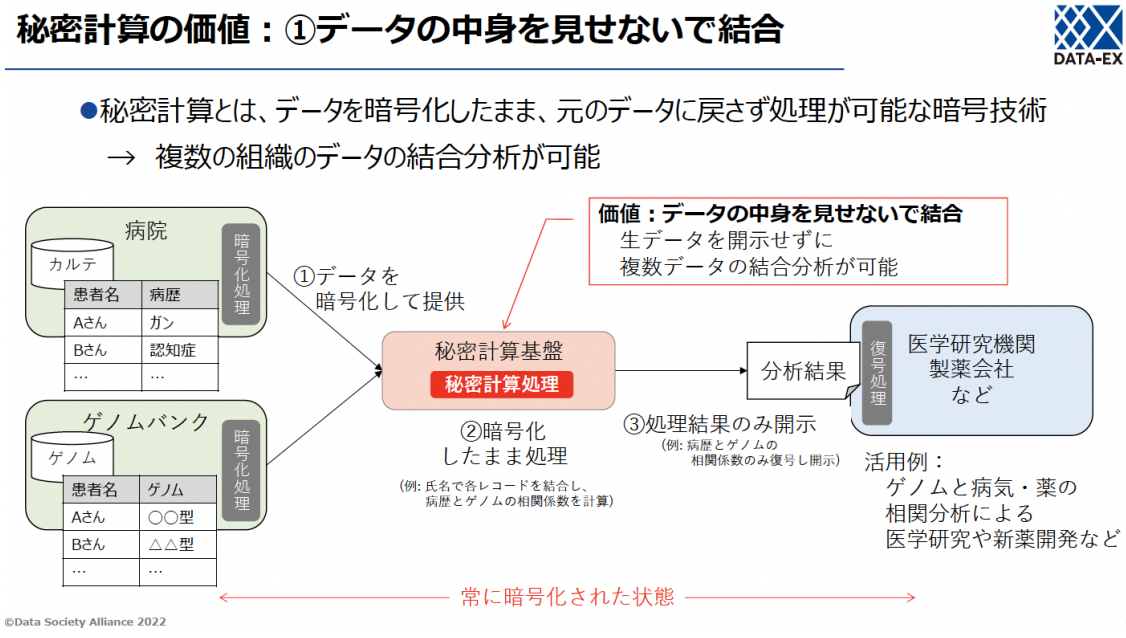
開催趣旨として、秘密計算の概要の説明と、本イベントが想定する組織間での安全なデータ結合のユースケースについて説明を行い、本イベントの開催背景を説明した。

まず秘密計算とは、データを暗号化したまま、元のデータに戻さず処理が可能な暗号技術のことである。秘密計算には、別名として秘匿計算とも呼ばれる。また、英語では Multi-Party Computation(マルチパーティ計算)や Secure Computation や、Confidential Computing とも呼ばれるが、本イベントでは、これらの総称として秘密計算と呼んでいる。

この秘密計算技術では、大きく 2 種類の価値が生まれる。一つ目は、複数のデータを安全に組織間で結合分析することで新たな知見を得ることができるという価値であり、二つ目はデータを秘匿したまま処理するため安全性が高まるという価値である。

本イベントでは、特に組織間でのデータ結合に注目しており、従来はデータを囲い込む発想であったものが、安全に組織間で活用することが促進され、さまざまな社会課題の解決に活用できるのではないかと期待している。

本イベントにて秘密計算による社会価値の創造の可能性を感じて頂き、社会実装・利活用の道筋・課題の議論促進を期待している。



招待講演 1「秘密計算の国際動向」

MPC Alliance President and Co-Founder
Frank Wiener 氏

MPC Alliance は、2019 年に Frank が所属している Sepior 社、Unbound Security 社と ZenGo 社の 3 社にて 2020 年 7 月に非営利組織として設立した。MPC Alliance の目的は、MPC（Multiparty Computation:秘密計算）技術の開発者・実務者・支持者を集め、MPC の製品・サービスの市場認知度・受容度・採用度を高めることである。

MPC Alliance には現在 50 社以上のメンバー企業が参加している。これらの企業には、スタートアップ企業から非営利団体、Digital Garage、NTT、Salesforce 等の大企業などが含まれる。

MPC Alliance では、MPC のアプリケーションを大まかに 2 つに分類している。一つ目は「データ・プライバシー」のユースケースである。プライバシーを強化する技術として MPC を使用し、安全でプライベートなデータコラボレーションを可能にできる。そして、二つ目は「データ・セキュリティ」のユースケースである。データの盗難や悪用を防ぐためにデータを保護できる。

MPC Alliance は、昨年から 3 部構成のバーチャル・カンファレンス・シリーズを開催し、業界の認知度を高める活動を行っている。初回のイベントには高い興味が示された。イベントでは、様々な MPC のアプリケーションやユースケースとして広告、金融詐欺犯罪の検出、ヘルスケアや電力網の最適化など紹介された。2 回目のイベントでは、「セキュリティ」のユースケースに特化し、デジタル資産のブロックチェーンの秘密鍵の安全管理のための MPC を対象にした。現在 MPC はデジタル資産市場にて何百もの企業で利用されている。

MPC は「セキュリティ」のユースケースに限らず、「プライバシー」のユースケースでも市場が立ち上がっている。例えば、MPC Alliance の会員企業である Nth Party 社は、最近世界最大の広告プラットフォーム企業の Magnite 社に買収されている。

このように、MPC は「データ・プライバシー」と「データ・セキュリティ」の両方に素晴らしい価値を付加する。

各社の取組みは、市場が初期のニッチなアプリケーションから、よりメインストリームなアプリケーションに移行していることを示している。この技術は十分成熟し、有用性が示され、既に適用されている。現在は限られた領域での適用であるが、この領域での成功体験により、MPC の採用がより広範囲に広がると確信する。今が、MPC に関与すべきタイミングとして完璧である。

招待講演 2「秘密計算に関する法的論点」

一般財団法人情報法制研究所(JILIS) 理事
ひかり総合法律事務所 パートナー弁護士
板倉 陽一郎 氏

秘密計算と個人情報保護法制

秘密計算の法的論点について、最も関連が深い個人情報保護法制との関係を中心に解説する。まず個人情報保護法制全体としては、令和 3 年改正による極端な縦割り構造の相当程度な一元化がポイントだ。国立大学や国立病院など医療分野・学術分野は原則民間企業と同等の規律が適用され、例えば国立病院のデータを対象に秘密計算を使う場合は民間ルールに基づくことになる点に注意が必要だ。

秘密計算との関係における論点を 4 つ挙げる。**個人情報該当性**は「個人に関する情報」であることが要件のひとつなので、「個人に関する情報」ではないといえるレベルまで加工されれば、個人情報には該当しない。しかし、秘密計算など暗号化等によって秘匿化されていたとしても、個人情報該当性は失われないという点は個人情報保護委員会のガイドライン(以下、GL)等で明記され、準同型暗号を用いた秘密計算も同様であることが確認されている。

安全管理措置(セキュリティ)としての秘密計算の有効性は疑う余地がない。GL 通則編には、講ずべき安全管理措置の具体的な手法として「個人データを含む通信の経路又は内容を暗号化」と例示されている。自民党の「経済構造改革戦略」や「デジタル・ニッポン」等でも安全担保技術として導入推進が提言され、内閣情報セキュリティセンター(NISC)「政府機関等の対策基準策定のためのガイドライン」にも情報漏洩対策として有効性が明記された。

個人情報保護法に定められた漏洩等の**監督官庁への通知義務要否**への影響は、現時点で明示されていない。GL は個人データの漏洩等が発生しても当該データに対し高度な暗号化やその他の個人の権利利益保護に必要な措置が講じられている場合は報告を要しないとしている。措置は Q&A で「第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置」とされ、技術の具体的な判断基準例として電子政府推奨暗号リストや ISO/IEC 18033 等への掲載が示された。しかし秘密分散を含む秘密計算技術が「必要な措置」に該当するか否かは、GL、Q&A、推奨暗号リストに記述がない。私見だが、秘密分散は ISO/IEC 19592 が技術基準となっており、これに従う限りは「必要な措置」に該当すると考えられ、電子政府推奨暗号リストへの記載も検討すべきだ。

最も関心の高い論点は**利用目的規制・第三者提供規制との関係**だ。複数の組織が各組織のデータを他組織に開示せず、互いの価値につながる計算結果だけを得られる点に大きな期待が寄せられる。利用目的や第三者提供に関する本人の同意なしに個人情報・個人データの計算結果を導出できないか、という期待だ。

利用目的規制の観点では、単独の事業者において複数組織が保有する個人データを秘密計算で結合し計算結果を得る場合、「計算結果」の導出の利用目的への記載が必須ではないと考えられるだろう。「統計データへの加工を行うこと自体を利用目的とする必要は無い」旨が従前から個人情報保護委員会 Q&A で示されていることからそうした解釈が可能だ。

第三者提供すなわち複数の組織が秘密計

算を活用するケースでの扱いは現時点で明確にされていない。JILIS から個人情報保護委員会へパブリックコメントとして確認した際は「暗号化は安全管理措置の一つとして考慮されるべき要素で、個人情報該当性に影響するものではない」と回答された。個人情報に該当しないことを理由にした内容ではなく「個人情報(個人データ)の提供に当たらない」との解釈を提案した意図に正面から回答する内容ではないと感じるが、第三者提供規制の解釈になり得るのではないかとの見解はピン止めされている。

令和 2 年度改正個人情報保護法では共同利用可能な新たな利活用手段として仮名加工情報制度が導入された(第三者提供は不可)。同じアルゴリズムで作成した仮名加工情報を複数事業者が秘密計算で共同利用し計算結果を導出してもよいという解釈も可能であろう。ただし「加工の方法に関する情報」の共有が「削除情報等の安全管理のための措置」違反になるかという論点、同じアルゴリズムで作った仮名加工情報を名寄せすることが識別のための当該仮名加工情報を他の情報と照合したことになるかという論点は明確にする必要がある。

※「個人情報保護委員会事務局レポート　仮名加工情報・匿名加工情報　信頼ある個人情報の利活用に向けて」で同様の解釈が採用。

海外事例

2014 年にエストニアデータ保護機関が秘密計算による処理は個人データ処理に該当しない見解を示した例がある(同国個人データ保護法はセンシティブデータの処理に関しデータ保護機関の事前許諾が必要と規定)。GDPR 以前の国内データ保護法に基づくデータ保護機関の判断とはいえ、現在も有効な解釈として維持されている。日本と欧州は相互にデータ保護制度を認証していることもあり、日本法の解釈にあたって参考にすべきと考える。

欧米間の越境データ移転では追加的措置の有効なケースとして秘密計算利用が挙げられた。SchremsII 決定では米国諜報法分野でのデータ主体保護の薄弱さを理由に欧米プライバシーシールドの十分性決定が無効とされ、標準データ保護約款による移転がすべて無効になる懸念が生じた。結果的には「追加的措置」を前提に移転の余地を残す決定がなされ、後に欧州データ保護ボードによる追加的措置に関する検討では適切な仮名化、エンドツーエンドの暗号化、秘密計算利用などが例示された。有効な手段として秘密計算が掲げられた事実は参考にしてもよい。米国議会に提出された、プライバシー保護技術の振興をはかる「デジタルプライバシーテクノロジー法案」では「secure multi-party computation」が対象技術として明記された。法案レベルだが、秘密計算と法との接点が出てきたことに注目したい。

今後の展望

個人情報法制以外の法的論点としては不正競争防止法との関係も注目だ。産業データ活用の観点からは、不正競争防止法における営業秘密の秘密計算技術を用いた相互提供と計算結果の取得では営業秘密の秘密管理性が失われないかという論点、限定提供データの技術的管理性の論点などが存在するが、秘密保持契約等の契約上の措置を前提とすれば、むしろ産業データの共有の促進に適した技術として積極的に活用されるべきであろう。

社会課題の解決に有効な仕組みとして、産官学とも総論では秘密計算や秘密分散の社会実装推進に前向きだ。現時点では個人情報利用時の目的外利用や第三者提供の例外とすることの壁は厚いが、本フォーラムを機に、仮名加工情報の共同利用など新たなスキームや、いわゆる 3 年ごと見直しに向けた議論を継続すべきだろう。さらに産業データへの適用による企業秘密の壁の突破、欧米の動きとの平仄や働きかけなどについても期待する。

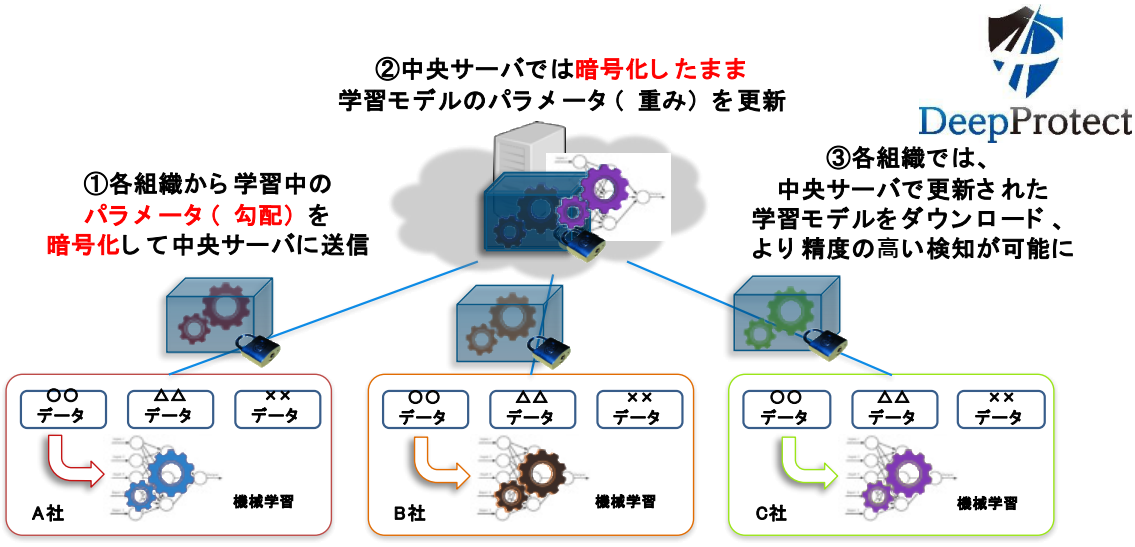
招待講演 3「プライバシー保護連合学習の実証実験」

国立研究開発法人情報通信研究機構(NICT)サイバーセキュリティ研究所　研究所長
盛合　志帆　氏

NICT では、データそのものを外部に開示することなく、複数の組織で連合学習を行うことができるプライバシー保護連合学習技術「DeepProtect」を開発し、社会実装を進めている。本技術は、各組織で構築した学習モデルの勾配情報を加法準同型暗号で暗号化して中央サーバに送り、暗号化したまま連合学習モデルを更新することができる(下図参照)。この技術を活用し、現在、社会課題となっている金融不正取引の検知精度向上をめざし、神戸大学及び(株)エルテスとともに、千葉銀行、三菱 UFJ 銀行、中国銀行、三井住友信託銀行及び伊予銀行の 5 つの銀行と実証実験を行った。

本実証実験では、「振り込め詐欺等の被害に遭った取引（被害取引）の検知」と、「不正取引に悪用された口座（不正口座）の検知」という二つの目的に対し、複数銀行が連携して「DeepProtect」を活用した学習モデルを構築し、不正取引の検知を行った。その結果、目標としていた検知精度 80%以上を達成するとともに、前者では、一銀行では検知できなかった不正取引が検知されるケースが確認され、後者では、不正口座として実際に凍結されるより 20～50 週早く検知することに成功した。

本実証実験で得られた成果と課題を踏まえ、不正取引の検知精度をさらに向上させるとともに、銀行での取引モニタリングの実業務に適用できるよう検証を進めたいと考えている。



招待講演 4「秘密計算の普及に向けた課題と取り組み」

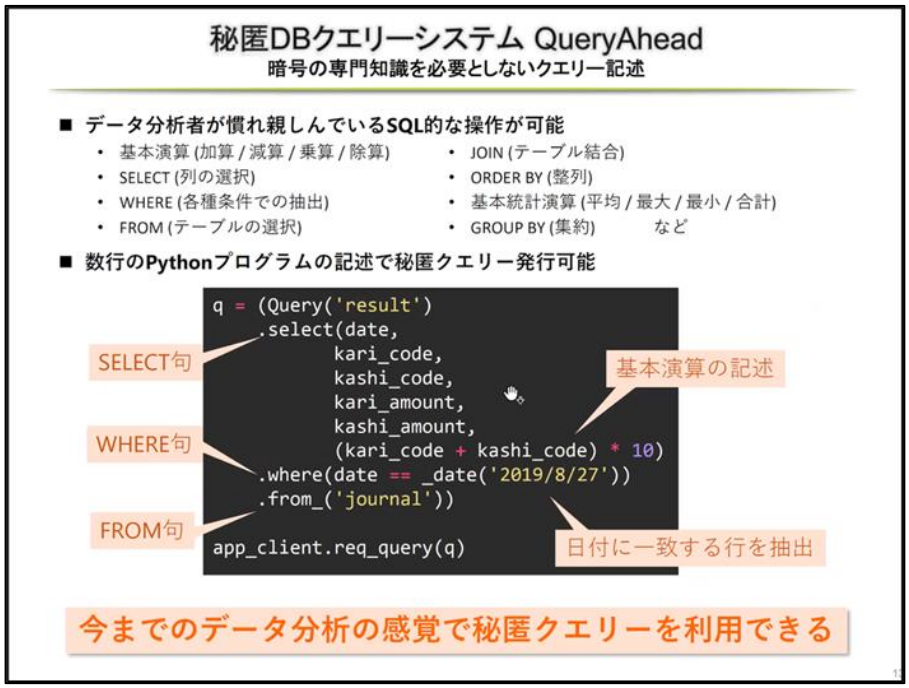
国立研究開発法人産業技術総合研究所
サイバーフィジカルセキュリティ研究センター首席研究員
花岡 悟一郎

秘密計算の普及に向け、秘密計算の原理と、それを踏まえた現状の研究開発動向を説明し、普及に向けた課題と取り組みについて紹介する。

現段階で、すでに秘密計算技術の処理性能については、十分実用的と言えるレベルに達している。しかしその具体的なアプリケーションの実装には、先端的な秘密計算要素技術を適切に組み合わせた設計を行い、実用的な処理速度と安全性を両立させる必要がある。このような設計については、トップ国際会議に採択されるレベルの技量を持った専門的な研究者・開発者が職人的に対処する必要があるため、本格的な普及のためには人材が足らないという課題がある。

したがって、今後、秘密計算技術の社会展開を進めるにあたり、処理性能面のみを向上させていくのではなく、上記のような専門的な研究者や開発者を必要とせずにアプリケーション開発を行うことができる「使い勝手の良さ」を高めていくことが重要である。(株)ZenmuTech では、そうした要望に応える秘密計算アプリケーション開発ツールとして、産総研の協力のもと秘匿 DB クエリーシステム QueryAhead を開発し、その有効性を示している。

また、秘密計算技術の仕組みや活用方法について、社会全体における理解の深化を推進していくことも、上記課題の解決において重要である。そのため、秘密計算の機能と安全性を理解が容易となるように、視覚的な手法等で表現する技術開発なども別途必要と考えられる。



招待講演 5「秘密計算の国際標準化動向」

ISO/IEC JTC 1/SC 27/WG 2 エキスパート
NTT 社会情報研究所 研究主任　菊池 亮 氏

一般に標準化とは、ある技術やモノを規格に沿って統一し、互換性の確保、技術の普及、品質の担保、利便性の向上などを狙うものである。標準化には大きく分けデジュールとデファクトの 2 種類がある。前者は公的な標準化機関によって合意され制定される標準であり、具体的には ISO や IEC、ITU が挙げられる。後者は特定企業の製品・サービスが普及することで生まれる事実上の標準であり、具体的には IETF や IEEE などがある。

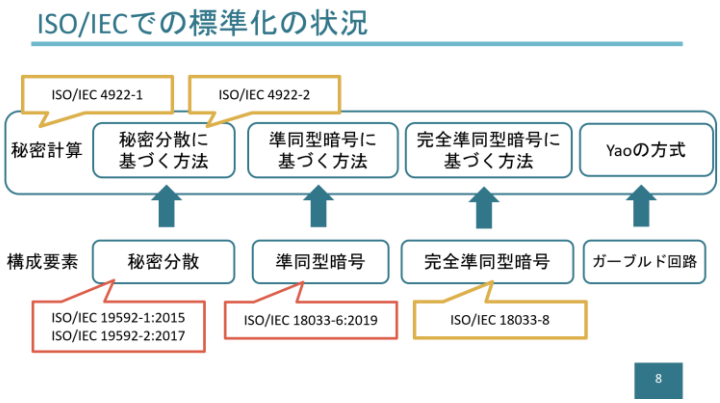
暗号要素技術は、暗号技術が厳しい輸出規制の対象であった歴史的経緯も影響し、各国の国内での標準規格、特に米国の標準規格に一定の権威がある。その一方で、近年では国際標準化の流れも強く、特に ISO/IEC や IETF は暗号要素技術の規格化に積極的に取り組んでいる。暗号要素技術を利用するアプリケーションの規格では、主にこれらの国や団体が策定した暗号要素技術の標準規格を参照することが多い。

さて、データを暗号化したまま分析する秘密計算技術は、近年 ISO/IEC JTC 1/SC 27/WG 2 において規格策定の動きがある。

秘密計算技術はその構成方法に応じて、秘密分散、(完全)準同型暗号、ガーブルドサーキットなどの構成要素が必要となる。これらの構成要素のうち、秘密分散は ISO/IEC 19592-1 および 19592-2 においてそれぞれ 2016 年、2017 年に規格化されている。また、準同型暗号も ISO/IEC 18033-6 として 2018 年に規格化されている。

現在、これら既存の規格を参照した秘密計算の規格化が進行しており、ISO/IEC 4922-1 では秘密計算(総論)、ISO/IEC 4922-2 では秘密分散を用いた秘密計算が、他の構成方法に先んじて規格化のステップに入っている(ともに筆者がエディタを務める)。また、秘密計算の構成要素である完全準同型暗号も、ISO/IEC 18033-8 として現在規格化が進行中である。

また、それ以外にも、独自に完全準同型暗号の規格案を策定するコンソーシアムが立ち上がったことや、IEEE においても秘密計算の利用に関する議論が為されており、多くの団体やその参加企業が秘密計算に着目し、国際標準の規格化に取り組み始めていることが見て取れる。



DSA 会員事例紹介「プライバシー強化技術に関する取り組みのご紹介」

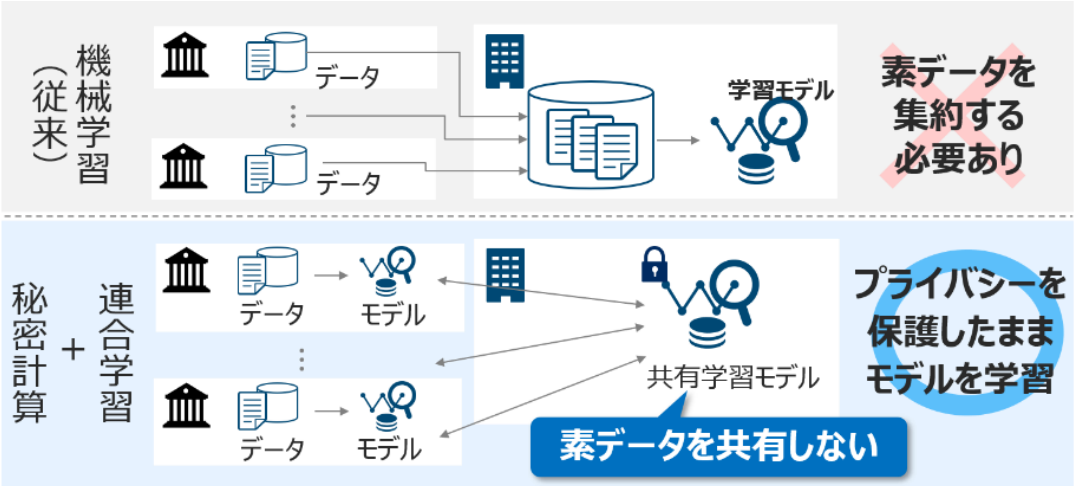
株式会社日本総合研究所　先端技術ラボ　エキスパート
近藤　浩史　氏

我々はプライバシー保護の原則を実現・強化する技術としてプライバシー強化技術（Privacy Enhancing Technologies : PETs）に着目しており、秘密計算は PETs の一技術と捉えている。

PETs に関する我々の活動は大きく 2 つある。1 つめの活動は、PETs に関する技術レポートの発行（URL : https://www.jri.co.jp/page.jsp?id=101511)である。本レポートでは秘密計算・差分プライバシー・連合学習の 3 つの技術を中心に、特定製品・ベンダーに依らない観点から技術概要と今後の動向をオピニオンとして発信している。例えば、技術普及に向けた今後の課題として、①法律、②システム開発、③人材・体制の 3 つの側面から整理している。

2 つめの活動は、連合学習の技術検証である。複数の金融機関が連携したローンのデフォルト予測をユースケースに設定して検証した。連合学習によるモデル構築のプロセスをよりセキュアにするため、秘密計算と組み合わせた連合学習の検証も行った（下図）。秘密計算の検証では、社内の検証環境構築に苦労した側面があるため、秘密計算を手元で手軽に試行できるツールなどが整備されることに期待している。

我々の今後の活動として、個人情報以外の企業内データ（機密情報など）に対して PETs を活用し、 組織間の共通課題や社会課題の解決を模索・検討したいと考える。



DSA 会員事例紹介「NEC の秘密計算に関する取り組み」

日本電気株式会社　技術価値創出本部
衛藤　嘉之　氏

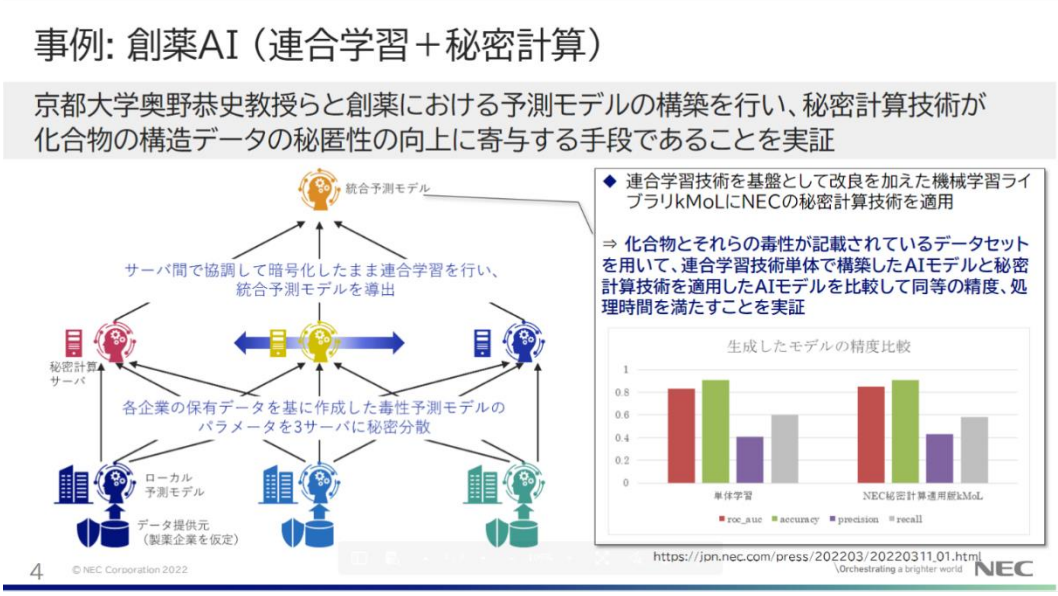
コンピュータの計算能力の向上はデータ活用の可能性を提示し、多くの領域において社会実装が進んでいる。そうした中、データの漏洩リスクや利用に伴う内容の露見が活用を妨げるケースが存在する。

創薬領域においても、複数企業やアカデミアと連携した新薬開発が期待されているが、医薬品などの原料となる化合物の構造データ等は機密性の高い情報であることから、データの共有が課題となっていた。

国立大学法人京都大学大学院医学研究科奥野恭史教授の研究室では上記課題に対し、機密データである化合物情報及び活性情報等を直接拠出せずに AI モデルの構築・統合を実現する連合学習技術を基盤として改良を加えた機械学習ライブラリ kMoL を開発し、情報の機密性を担保しつつ、企業・組織間の連携を可能とした。

今回の実証実験では、kMoL に NEC の秘密計算技術を適用し、様々な化合物とそれらの毒性が記載されているデータセットを用いた毒性予測モデル等の評価を行い、連合学習技術単独の場合に加えて、統合時の AI モデルの秘匿性をさらに高めることを試みた。結果、連合学習技術単独で構築した AI モデルと同等の精度を満たすことを確認し、秘密計算技術が毒性予測モデルの構築において化合物データの秘匿性の向上に寄与する実用的な手段であることを示した。

NEC は今後も秘密計算技術の社会実装を通じ、データ保護と活用の両立を実現し、社会課題の解決に貢献する所存である。



DSA 会員事例紹介「秘匿情報管理サービス「匿名バンク」の導入事例」

株式会社日立製作所 研究開発グループ 東京社会イノベーション協創センタ
価値創出プロジェクトプロジェクトマネージャ
佐藤 嘉則 氏

日立製作所の秘匿情報管理サービス「匿名バンク」[1]は、お客様がセキュアな個人情報利活用サービスを運用するためのクラウドサービスである。匿名バンクは、同一人の個人情報を個人特定情報と匿名化情報に分離してクラウド上で管理する。個人特定情報は、秘密計算技術の一種[2]である PIR(Private Information Retrieval)で保護されており、匿名バンクでは、独自の検索可能暗号技術で実装している。これにより、クラウド上で個人特定情報を確率暗号化したまま、検索結果に基づいてビジネスロジックを実行することが可能となっている。

検索可能暗号を匿名バンクに導入した 2014 年以降、個人情報保護法や各種ガイドラインに準拠する形で、より厳格な安全管理措置を所望されるヘルスケア、金融分野、公共分野等の多数のお客様が匿名バンクを導入している。

ヘルスケア分野の導入事例の一つが、希少疾患研究のための患者データ管理サービス（患者レジストリサービス）である[3]。本サービスでは、協力医療機関、CRC(Clinical Research Coordinator)、製薬企業、研究機関等が、患者同意に基づいてクラウド上で患者データを取り扱う。協力医療機関や CRC は、担当範囲の個人情報のみ検索可能暗号の復号鍵を有するクライアント PC から閲覧できるが、クラウド側では一切閲覧することはできない仕様となっている。全国の希少疾患の患者データをセキュアに集約することにより、効率的な臨床研究・治験推進を可能としている。

金融分野では銀行の NISA 口座開設サービスのマイナンバー管理に導入されており[4]、また 2021/6 には同意に基づく個人情報利活用サービスを構築するための「個人情報管理基盤サービス」を提供している。その他の導入事例については、匿名バンク紹介サイト[1]を参照されたい。

[1]https://www.hitachi.co.jp/Prod/comp/app/tokumei/index.html

[2]https://www.enisa.europa.eu/publications/data-protection-engineering

[3]https://www.hitachi.co.jp/products/it/magazine/hitac/document/2017/10/1710c.pdf

[4]https://www.hitachi.co.jp/products/it/finance/topics/20181029-topics.html

DSA 会員事例紹介「コンソーシアム設立による秘密計算の啓蒙とプライバシーテックへの拡張」

株式会社 Acompany
代表取締役 CEO 高橋亮祐 氏

データを暗号化して分析する「秘密計算技術」はどのようにして社会へ貢献するのだろうか。

2021 年 6 月、Acompany は EAGLYS と共同で、秘密計算のコミュニティ「秘密計算コンソーシアム」を立ち上げた。 メインコンテンツは 7 回開催した定期イベント「秘密計算.jp」。秘密計算に関する実証実験や事業化などの取り組みをテーマに、インテルやデジタル・アドバタイジング・コンソーシアム(DAC)、SB テクノロジーなどが登壇。総計 300 人以上が参加した。

このコンソーシアムを運営する Acompany は、名古屋大学・名古屋工業大学発スタートアップだ。メイン活動拠点を名古屋に構え、データ分析を得意とする秘密分散法を用いた MPC による秘密計算の社会実装に取り組んでいる。注力分野として掲げるのは「マーケティング」や「ヘルスケア」、「モビリティ」、「金融」の 4 領域だ。中でもマーケティングは、DAC との実証実験を実施。ビッグデータの集計・分析結果を提供するプラットフォームへの応用を目的に、パーソナルデータを秘匿したまま統合分析を実施し、成功した。今話題の Cookie 規制による広告ターゲティングの代替手段へ貢献する可能性を秘める。

GDPR（一般データ保護規則）や改正個人情報保護法などにより、世界各国でプライバシー規制への需要は高まる一方だ。その中で Acompany は秘密計算以外の技術展開も視野に入れ、合成データや差分プライバシーなどプライバシー保護技術提供も進める。

DSA 会員事例紹介「秘密計算＝プライバシー＋セキュリティ＋データバリュー」

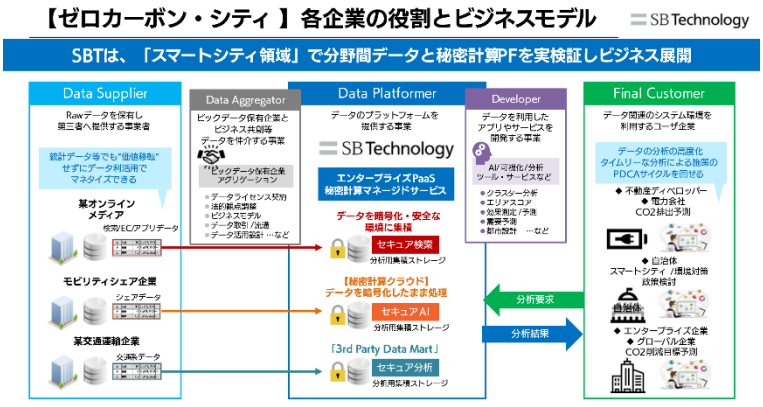
SB テクノロジー株式会社　サービス統括　ビジネスイノベーション本部
プリンシパルストラテジスト　福嶋　健二　氏

ビッグデータの課題の 1 つ目は、匿名化等による分析データの欠落(プライバシー)。2 つ目は、機微データをクラウド上に置けない(セキュリティ)。3 つ目は、他組織とのデータ共有(データバリュー)。SB テクノロジーはデータ資産活用でこの 3 つの課題を解決するパラダイムシフトの実現を目指している。秘密計算技術を活用で有効と考えるマルチパーティ(データホルダーが 2 つ以上)でデータを掛け合わせる相関/クロス分析・クラスター分析、希薄データ項目の補完/補填、スコア化、需要予測、効果測定などに活用できると考えている。

マネタイズ・パターンは 3 つと考えている。1つ目は、「ID におりマルチパーティで掛け合わせたデータから算出したバリュー」で、理由は分析データで導かれる相関関係は、母集団の相関関係としてマーケティング施策に生かすことができ、適用領域は《マーケティング領域》など。2 つ目は、「企業/組織間データ活用でのマルチパーティのデータ掛け合わせで創出したバリュー」で、理由は企業グループ間で分断されたデータから業務改善などデータドリブンでの経営方針や戦略検討等へ活かすことができ、適用領域は《新ビジネス/業務改善/効率向上領域》など。3 つ目は、「A 統計×B 統計＝クロス分析結果」で、理由は個人情報に関するデータが必要な統計分析が可能で、分析粒度を目的に合わせて対応でき、適用領域は《調査領域》などである。

SBT が取り組んでいるゼロ・カーボンシティに向けた事例では「グリーン×デジタル」スマートシティで都市 OS でのトータルマネージメントにおいても【プライバシー保護】で必須の技術になると考えている。SBT はゼロ・カーボンシティでの各企業などの役割とビジネスモデル（下図）で「スマートシティ領域」で分野間データと秘密計算 PF の実検証を行いながらビジネス展開を目指している。SBT が現在進める実証実験ではオンラインメディアサービスとシェアモビリティサービスのマルチパーティデータを活用して、カスタマーを不動産ディベロッパー、自治体に向けてのサービスとして社会実装を目指している。

SBT は秘密計算コンソーシアム主催 2 社の保有するコア技術特性を活かしマルチパーティデータでの活用時に最大化する為に「秘密分散＋MPC(マルチパーティ計算)方式」と「準同型暗号方式」の 2 つの技術を“ハイブリッド秘密計算クラウドサービス”として研究開発で整え、2 つの秘密計算の有効性などを検証や実用へ向け活用進める企業などへ向け PoC 用途から利用できる“トライアルサービス”を提供し、更なる秘密計算技術の実活用に向けたユースケースを様々な企業と共創で進めている。



DSA 会員事例紹介「グローバルに先駆けた秘密計算ユースケース創出に向けて」

EAGLYS 株式会社
代表取締役社長　今林広樹　氏

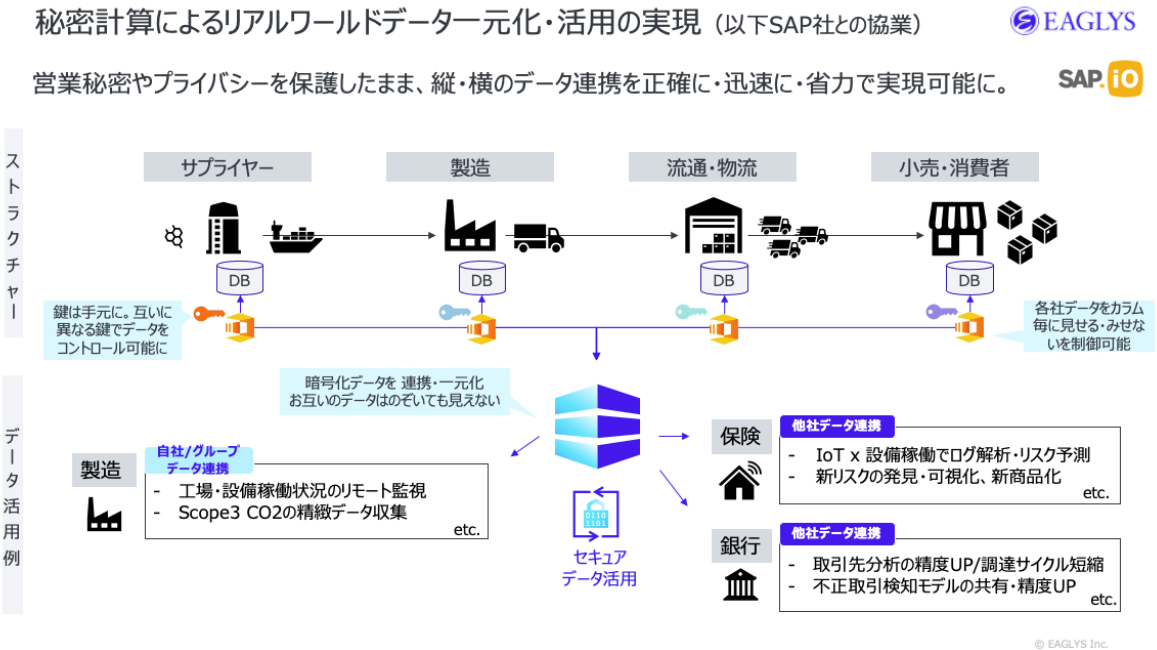
企業内外のデータ活用が進む一方、急速なクラウド移行が招くセキュリティホールの拡大や、機密データ漏洩やプライバシー侵害といったデータに纏わるリスク接面拡大とその対応が喫緊の課題となっている。

これらのデータアクセス・利活用の課題を取り除きつつ、AI・データ活用を量・質ともに最大化するために、秘密計算をはじめとする AI・データセキュリティ技術は有用であり、Gartner を始め戦略的技術としてグローバルトレンド化している。

EAGLYS は秘密計算の中でも、データ連携・一元化や AI アルゴリズムにおける秘匿化機能・データ保護機能(独自機能開発)とその高速化技術(独自技術研究)に強みをもち、その技術優位性や応用実績を武器にグローバルに先駆けて事例を創出している。3/11 開催のフォーラムでは、ERP パッケージ世界トップシェアの SAP 社とのプロダクト連携・協業の取り組みを紹介した。サプライチェーンのタテデータ連携により、製造設備の稼働状況や CO2 排出量などの機密データ収集や金融機関による一元化データの分析活用など、企業をまたいだデータ活用が秘密計算領域では検討されやすい。

また今後の秘密計算のビジネス展開を加速するため、SB テクノロジー社とは秘密計算クラウドサービス提供に向けて協業を進めており、共同で発表を行った(SB テクノロジー社紹介を参照)。

今後も引き続き、データ連携・AI 活用における正確性・ロバスト性の向上とスムーズな価値転換に向けて、プライバシー強化/AI セキュリティ技術(秘密計算、連合学習、疑似データ生成等)の応用研究と社会実装を進めていく。



DSA 会員事例紹介「秘密計算に関する NTT コミュニケーションズの取り組み」

NTT コミュニケーションズ株式会社
スマートワールドビジネス部 スマートヘルスケア推進室　担当課長 櫻井 陽一　氏

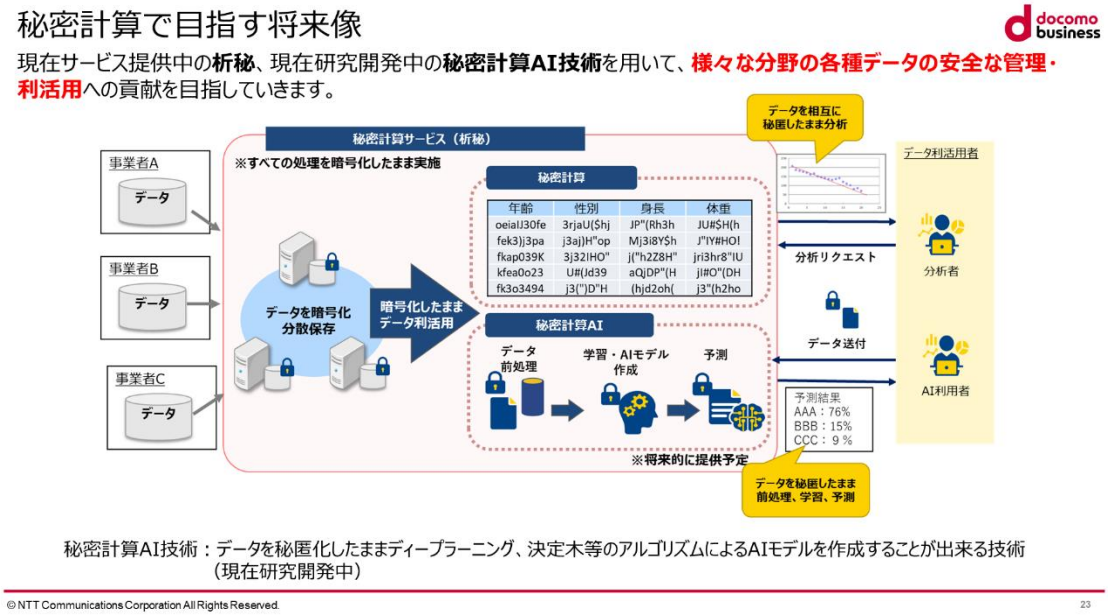
NTT コミュニケーションズでは、スマートワールド推進のキーテクノロジーの一つとして秘密計算を位置付け、秘密計算サービス「析秘」の開発、提供、「内閣府 SIP AI ホスピタルによる高度診断・治療システムにおける参画医療機関との秘密計算技術を活用した共同研究」や「千葉大学附属病院複数診療科との秘密計算 AI を活用した共同研究」に取組んでおり、社会実装、サービス提供を目指している。

医療・ヘルスケア分野を最初のターゲットに設定したのは、機微性の高い個人情報である医療情報が対象となるため、安全にデータ利活用が可能となる秘密計算技術が提供できる効能の適応性が高いと考えたからである。

NTT コミュニケーションズでは、医療・ヘルスケア分野だけではなく、他の分野においても秘密計算を導入することで課題解決に繋げられるように、PoC 等に取り組んでいる。

「析秘」については、まずは秘密計算に手軽に触れてもらえる機能を絞ったファーストリリースをしているが、今後も様々な解析手法や API の提供を予定している。

さらに、現在 NTT 研究所にて研究開発中のディープラーニング等が実現可能な「秘密計算 AI」技術についても、析秘に組み込み、様々な方々に利用してもらえるようにNTT研究所と連携し、開発を進めており、Smart Data Platform for Healthcare の機能群と併せて、様々な分野でのデータの安全な利活用への貢献を目指していく。



秘密計算AI技術：データを秘匿化したままディープラーニング、決定木等のアルゴリズムによるAIモデルを作成することが出来る技術
（現在研究開発中）

DSA 会員事例紹介「デジタルガレージの秘密計算の取り組み」

株式会社デジタルガレージ DG Lab　Chief Technology Officer (Security)
竹之内 隆夫 氏

デジタルガレージは、秘密計算の社会実装に向けた業界団体の主導や、スタートアップ投資、そして、技術パートナーと事業化検討を進めている。

まず、業界団体の主導については、具体的には、データ社会推進協議会(DSA)において秘密計算活用 WG の主査や、秘密計算研究会の事務局を行っている。DSA が利活用の観点での議論を進めているのに対し、秘密計算研究会では技術の観点で活動を行なっており、2022 年 3 月に秘密計算の安全性基準を公表した。秘密計算は様々な方式が存在し、安全性の理解が困難という課題の解決のため、統一的な評価が可能な基準を作成した。これにより、技術の提供者と利用者との相互理解を促進されることを期待している。

続いて、デジタルガレージはスタートアップ投資を積極的に行っている。デジタルガレージは様々な技術分野の中、秘密計算にも注目しており、既に国内では Curv に投資している。Curv は無事 PayPay に買収されている。

最後に、デジタルガレージは技術パートナーとの事業化も検討している。秘密計算にはさまざまな方式が存在するが、デジタルガレージは一つの方式に限定せずに、各方式を技術パートナーと実現する方針をとっている。一例としては、2020 年に行った、Fortanix 社と連携し、MS Azure で動作するハードウエアチップを用いた秘密計算技術を実証している。

パネルディスカッション「秘密計算の期待と課題、普及に向け今後求められるアクション」

多様な角度からの講演/事例紹介を通じ、プラットフォーム化やルール整備、ユーザビリティや人材といった秘密計算普及の課題認識が共有された。講演者である板倉陽一郎氏・盛合志帆氏に加え、江村克己氏と田口潤氏にご参加いただき、それらの課題をどう乗り越えていくべきかをテーマに、パネルディスカッションを行った。ファシリテーターはDSA 理事・若目田光生が務めた。

パネリスト

- 一般財団法人情報法制研究所理事・ひかり総合法律事務所パートナー弁護士　板倉 陽一郎 氏
- 日本電気株式会社 NEC フェロー　江村 克己 氏
- 一般社団法人日本データマネジメント・コンソーシアム理事　田口 潤 氏
- 国立研究開発法人情報通信研究機構サイバーセキュリティ研究所長　盛合 志帆 氏

ファシリテーター

- 一般社団法人データ社会推進協議会 理事　若目田 光生

問題意識

――各セッションをふまえて、まずは秘密計算普及に向けた課題認識、ご意見をお聞かせください。

田口潤氏

田口潤(以下、田口)　30 年以上にわたる IT 専門記者歴において暗号化や秘密分散を含む先端技術を取り上げてきたが、秘密計算がこれだけ濃く熱いとは認知していなかった。プライバシーや法、政策、技術など色々な論点がある。近年稀なエネルギーを感じ、プラットフォーム化にも期待する。

一方で、IT プロにすら、そのエネルギーが適切に伝達できていないという課題も感じるところだ。個々のピースとそれらの重要性は理解するものの、全体像がわからない。DSA なのかより特化した業界団体なのかといった枠組みはさておき、秘密計算にまつわるアーキテクチャを整理してとっつきにくさを払拭する必要があるだろう。日本は技術開発が先行して「いいものはいつかわかってもらえる」姿勢に陥りがちだが、海外で一般的なカオスマップを整理するなど、伝える、わかってもらう取組みこそ重要だ。最初は誤解も生じるだろうが続けていくこと、そこにコミュニティの意義と責任がある。今後の取組みへ向けてメッセージを発し続けるべきだ。

企業講演にあった AI 活用はとても大きな次の成長領域だが、プライバシーを考えすぎず猛スピードで処理結果に到達してしまう中国の存在が脅威だ。ハンディキャップを負った日米欧は、個別企業の利害を超えて協調し民益の全体最適を優先すべきだろう。

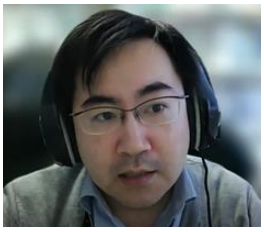
江村克己氏

江村克己(以下、江村)　大変濃密な時間にお礼申しあげる。NEC で永く CTO として研究開発に関わり、秘密計算とは 10 年前に出会っている。当時は処理が遅すぎて「できたらすごいね」のレベルだったが、かなり実用に近づいたことに感慨を覚えている。

SB テクノロジーのスマートシティ事例には共感する。データ駆動形社会の創造においてどうデータを活用していくか。秘密計算の普及には、個別事例からの発想の転換が必要だ。いま見えている課題のリスク低減にとどまらず、データ活用社会全体の視座で、あらゆるプレイヤーが集う場での議論が欠かせない。

プラットフォーム化は重要だが、秘密計算のためのプラットフォーム構築という話ではないだろう。SIP はじめあちこちでデータ連携プラットフォーム、基盤と謳っているが、社会実装に至っていない。それらの大きなプラットフォームへ秘密計算を入れ込んでいく前提でバラバラの課題を紐解き、次のステップやチャンスを考えるべきだ。小さな事例を個別に積み上げても、解決しうる課題が繋がっていかない。

法制度や社会受容性といった課題解決に向けて、発信すべき情報も転換点を迎えている。技術紹介にとどまらず、秘密計算という手段で実現した実利、価値を多くの人に伝えていくフェイズにきている。



板倉陽一郎氏

板倉陽一郎(以下、板倉)　今日紹介された取組みは同意が前提であり、基本的に問題は起きない。ただし、本質ではない。本当にニーズがあるのは既存未同意データの安全な活用と効果の導出であり、私への相談のほぼ 100%を占める。優秀な安全措置技術としての秘密計算はどんどん活用すべきだが、現時点では秘密計算だから未同意データも利用可能という解釈はなく、本当のニーズは満たせない。4 月以降個人情報保護委員会の見解には期待するし、対話しつつ実効性のある解を見出していくべきなのだろう。

理解促進は難しいところで、一般の方に何となくでも伝わるためには運も重要だ。インターネット SSL の鍵マークや行動ターゲティングが経てきたような「そういうもの」という認知レベルへの到達へ向けて、読まないかもしれなくても、色々と丁寧に説明していくしかない。個人データについても過去には適切に理解するメディアがほとんどなく誤報と絶望を繰り返してきたが、誤った記事がそれでも現在は消滅しつつある。間違っていたら地道に訂正を求め、諦めずに続けていくことでブレークスルーを迎えられると期待する。

盛合志帆氏

盛合志帆(以下、盛合)　法律、学術、標準化など多様な論点をひとまとまりのプログラムにしてもらい、理解が進んだ。実用化へ向けた DSA 会員企業の事例紹介は、とくに興味深かった。

今後の課題としては、銀行実証実験でデータから触ってみた経験をふまえ、データ標準化が肝だとあらためて痛感する。スピード感をもっていますぐ始めたいという相談が増え、今日参加のユーザー企業との橋渡し企業や、プラットフォームの出番がきている。

優先的に取り組む領域

――ユースケースや事例をふまえて課題や目的に合った解決手段としての秘密計算を捉えるとき、適用が急がれる領域などはありますか。

田口　いざ使いたいとき、企業は法務から止められたり他社に呼びかけてもデータが出てこなかったりといった課題に直面する。Acompany の SAP サプライチェーン連携のような未同意データの活用は有望だ。炎上後の続報が少ないが、JR の Suica データは各社の交通カード連携が可能になっている。一企業では大変な取組みだが、わかりやすく関心を引く領域といえる。

江村　田口氏から具体例が上がったように、次代は組織間のデータ連携だ。人口減少国日本にあっては、トラック積載率向上など物流も大きな課題解決が期待できる。別業界がデータを出し合うならどういう課題が解決できるポテンシャルがあるのか、メリットがあるか。ヘルスケア領域は SIP 含めてプロジェクトごとに多数の適用先がある。

盛合　名前は開かせないが、移動データで秘密計算の発展形を推進するプロジェクトが進んでいる。

板倉　国内は待望の仮名加工情報の共同利用で秘密計算活用を使うとよさそうだ。グローバルでプライバシーや Cookie の課題が浮上し各国とも困ってはいるが、秘密計算だからそれらの課題をクリアしているという解釈には踏み込んでいない。欧州の最新追加措置では技術の意義を認めるものの、同意に代わるところまでは踏み込めない。

EU は GDPR で作ったトラストマークに関し、4 年経ってベースのガイドラインはできてきたところだ。EU 全体は難しくても各国なら輸出できる可能性があり、戦略的に推進すべき。議会を通ったというと、国際的にはとても拘束力強い。日本は得意でないが、EU のどこかと共同していくと有効な戦略になり、OECD にも打ち込める。日本から働きかけていくべきだろう。他方米国は GDPR のような詳細ルールではないため、ただちに市場としては期待できない。

田口　ユーザー企業を多数取材してきた観点で重要な話だ。企業は Suica 問題の社会的批判や SNS 炎上が身にしみすぎ、危うきには近寄らない姿勢で何とかしてしまっている。物流、小売も秘密計算必要のちょっと前の段階で、企業を超えた取組みまで進んでない。攻めないとブレークスルーできない医療が例外か。DSA、個社、コンソーシアムの何れにせよ、企業間データ利活用の成果を出していくと雰囲気が変わるはずだ。

組織間データ共有の注目領域

――安全、トラストを担う組織や基準についても、国や業界団体などの選択肢が提示されました。フードロスや需要予測、環境負荷対応など、組織間データ共有が欠かせないないかで、企業秘密に関する注目領域はありますか。第 4 の手法が重要というコメントもありました。

ファシリテーター若目田光生

盛合　SAP サプライチェーンのようなブローバルプラットフォームづくりは注目に値する領域だ。秘密計算を含む Privacy Enhancing Computing(PEC)、Privacy Enhancing Technology(PET)は、ガートナートップトレンドに取り上げられている世界の潮流だ。米国も国を挙げて売り込みにきている。データ越境問題が気になって手を上げづらかったが、国際的

データ連携のデモに使えないかという相談もあった。日本が良い技術をもっていても、機動力などの差でこうした黒船に負けてしまう面もある。

――DFFT も共通ルール、バイラテラルに話が偏りがちですが、技術による解決も重要な側面と感じます。国際間のデータ共有についてはいかがでしょう。

板倉　国際間データ共有の取組みはなんともいえない。国内でも国際でもまだソリューションを提供できていない。エストニアの企業が頑張っていたが、対民より対電子政府にシフトした。各国でも大丈夫とはとてもいえない。日本から打って出るとすれば、国内で確認できた安全の枠組みを広げていき、そこを軸に売っていくのだろう。

――個人情報依存ではない領域から進めるべきという指摘が日本総研からありました。国際間データ共有では一層重要かもしれません。

優先すべきアクション

――企業に対する啓発、国や団体への啓発ともに、様々な課題が提示されました。いま優先すべきアクションについて提言をお願いします。

田口　長年 IT 動向を見てきた経験から、これまでとは異なる提供者側の取組みが重要と感じる。MPC アライアンスと協調するのか競合するのか。スマートフォンや PDA など、たいてい日本の技術は先行するのに、iPhone に席巻されてしまってきた。日本一企業より海外有力ベンダーの方が「なんとなく安心」と思われてしまう。

パネルディスカッションまとめ

- ☑ **グローバルも展望した本格的な社会実装(プラットフォーム化)を展望した、制度ルール、安全性基準、運営、ガバナンス、データ整備の検討**
- ☑ **利用者やデータ主体への普及啓発による理解促進(社会受容性の拡大)、ブランディング**
- ☑ **共有価値の訴求と視座を上げた適用領域の設定、及びそれを強力に推進する体制や人材、政策**

一般に理解されるのは難しいが、アピールし続けていくのも重要だ。最初は誤解があっても、継続していく。海外ベンダーは Youtube を使った啓発が増えた。ブロックチェーンもちゃんと理解している人はほぼ皆無だが、動画なら「なんかすごそう」とわかった気にはなる。

板倉　海外事業者の方が信頼できるという話は、制度面から見ると「なんとなく」ではない。消費者からすると Google や Facebook は、厳しい規制を潜り抜けたサービスだ。GAFA は各国で目をつけられ叱られているが、各国で監視の目が行き届いている企業ということの裏返しでもある。国内の規制をいやがる日本の消費者は、EU の厳しい規制にタダ乗りしている。経済産業省は業法も規制も嫌いでガイドラインに逃げるし、経済団体は単純に規制緩和と謳う。消費者や官庁、経済界に甘やかされるから、日本企業は世界に出ていけない。海外で戦える枠組みが最初から必要で、国内しか見ていないことが敗因だ。

盛合　情報発信がすごく大事で、今日のようなフォーラムも続けていくべき。我々も黎明期にすぐ結果を出しやすい領域テーマを選んできた。また、本日講演で紹介した事例については動画を公開している。ブランディングを含めてみんなで推進していく。

江村　プラットフォームに関する議論は、必要なエコシステムができているかという視点が大事だ。いまやれる人の範囲で小さな活動になることを避け、発展のためにはどういうプレイヤーが必要なのか誰がいるのかという順番で考える。竹之内氏からガイドラインの説明があったが、国レベルでやっていく必要がある。そのうえで「技術で勝つ日本」ではなくルールづくり、標準化、海外連携と進めていくべきだ。しかしこの領域は人材含めて日本が弱い。「いまいる人が集まればなんとかなる」という世界ではなくなりつつあり、日本経済新聞にも取り上げられるほど標準化が再度見直されている昨今だ。そこをどうしていくかの意識が不可欠である。

アウトリーチや諦めない姿勢も大切だ。初等中等教育に秘密計算の情報を入れ込むなど、若いデジタルネイティブへの早めのインプットが必要だろう。

――*ありがとうございました。*

付録　参加者アンケート概要

満足度

本フォーラム全体に対する 5 段階評価を伺ったところ、全体平均スコアは 4.2 と、多くの参加者が内容を高く評価していただきました。とくに運輸業・郵便業、学術研究・専門・技術サービス業の参加者は満足度が高かったようです。

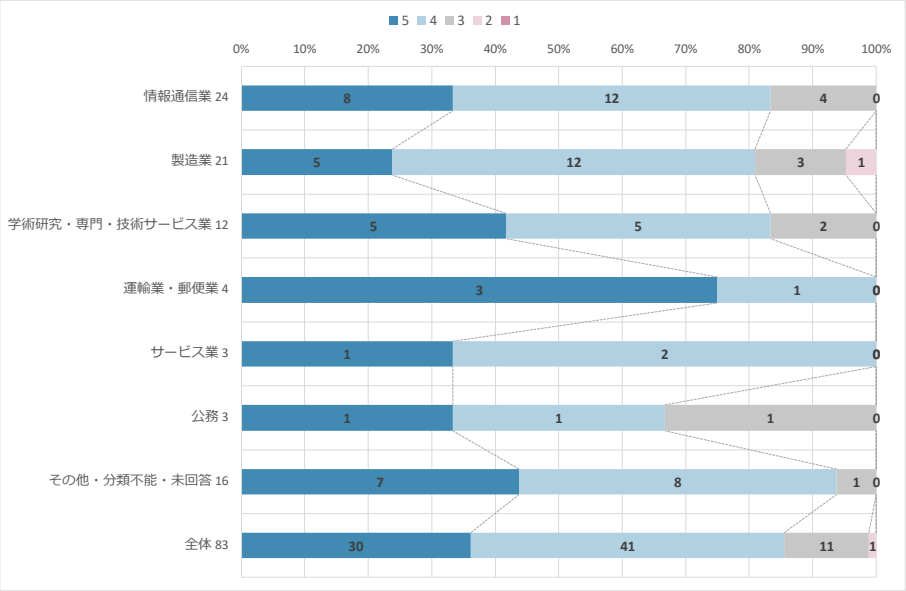


図 3 参加者業種別満足度(期待以上～期待はずれの 5 段階評価)

セッション別評価

セッション別の評価はいずれも 90%以上が「期待通り」～「期待以上」でした。なかでも「DSA 会員による事例紹介」は 97%、「パネルディスカッション」は 96%が「期待通り」～「期待以上」の評価です。

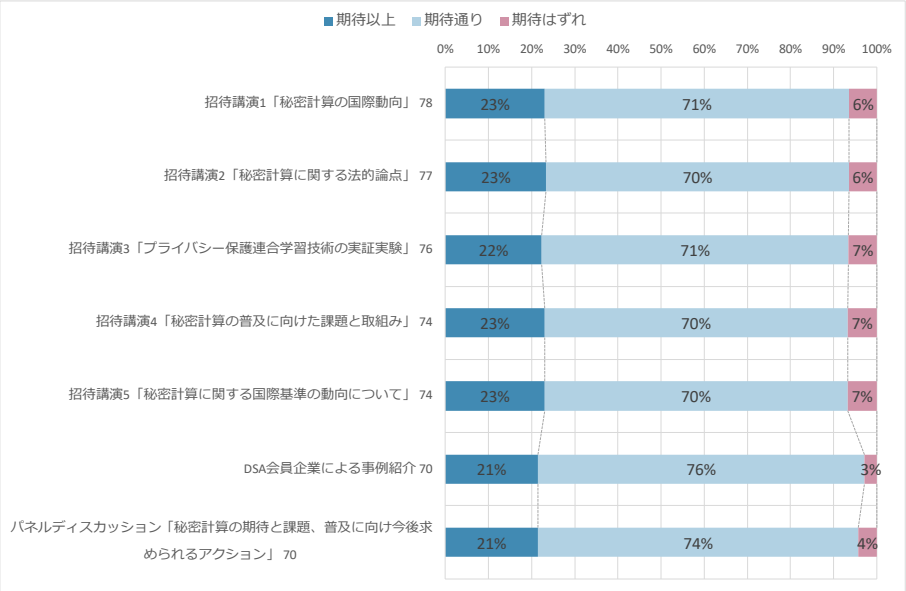


図 4 セッションごとの評価(期待以上～期待はずれの 3 段階評価)

とくに役立った点や興味深かった点など

パーソナルデータを含むデータ活用促進における秘密計算の役割に対する驚きと期待が寄せられました。とくに導入事例から実装の進捗を感じていただけたようです。課題としては法制度や国際標準化、また社会実装へ向けた価値や安全性の伝達などのご意見をいただきました。

表 1 とくに役立った点や興味深かった点(自由記述、原文のまま)

コメント	業種
・大元のデータが個人情報というところで世界的にぶつかる壁が同じということ。 ・例に物流がよく出てきたので、物流はやはり今後の大きな社会課題なのだなと感じた。	運輸業・郵便業
データ活用が社会に受容される要件となりうる技術である点。	製造業
プライバシー保護学習技術	製造業
技術者目線の発表が大多数だったなかで、板倉先生の見解が世の中的には一番重要だと思われる。	学術研究・専門・技術サービス業
法制度の点と国際的な標準化の点	情報通信業
個人情報保護法との関係の整理で、仮名加工情報の共同利用、という整理でいける可能性を始めて認識できた。パネルの最後で、ディジタルネイティブに向けて発信すべしという指摘は興味深かった。	学術研究・専門・技術サービス業
国際的なルールマーキングの重要性を改めて感じました。	その他
実際の利用例が示され、さまざまな応用を頭に浮かべることができました。ただ、パネルディスカッションでもありましたが、示された利用例の図では、一般の人に理解してもらうのは困難に思いました。私も社内で展開したいとは思いますが、うまく伝える自信がありません。わかりやすい資料があるといいと思いました。	製造業

コメント	業種
まったくの門外漢ですが、ここまで実装、実証が進んでいることに驚きです。秘密計算について、素人でも安全性となぜ計算できるのか、わかりやすいポンチ絵があると良い。	製造業
社会実装の進ませ方は中々難しいと感じました。	情報通信業
複数の企業から事例の紹介が役に立つ。秘密計算という技術を評価するのではなく、社会にどう役立てるのかの議論を厚くして盛り上げることが現在の課題だろうと思う。	情報通信業
冷静に法制面からコメントする板倉弁護士さんと、各社の姿勢のコントラストが、リアルでした。	情報通信業

全体についてのご意見、ご感想、ご質問など

フォーラムでお伝えした情報量と領域の広さから、全体像が把握できたというご意見の一方で、法規制などテーマ別に掘り下げる機会についてのご要望もいただきました。個別の具体的なご質問も複数いただき、関心の高さが伺えます。資料提供のご要望に関しては、本レポートにてお応えすることとしました。

表 2 セミナー全体についてのご意見、ご感想、ご質問(自由記述、原文のまま)

コメント	業種
JDMC2022 のラウンジトークで初めて「秘密計算」というワードを知ったので、第一人者の皆様から基本概念や世界的な動向をお聞きすることができて良かった。実用されたらデータ活用の促進や社会課題解決に役立つだろうなと感じた。	運輸業・郵便業
それぞれ、もう少しじっくりと内容を聴きたいという希望はあるのですが、これだけの講演者が一同に会したことで、横断的に状況を把握できました。ありがとうございました。	学術研究・専門・技術サービス業
全体的に熱量の高い、密度の濃いセミナーを受講させて頂き、ありがとうございました。法規制に関する話題は、是非独立したセミナーとして別途開催して頂くとうれしいです。	情報通信業
大変な関心と盛り上がりを実感しました。	製造業
短時間でこれだけ山盛りの情報をご提供いただきました。しばらく反芻が必要かも。	サービス業
秘密計算の概要とデータ利活用する上での課題について、アウトラインが分かった	製造業
秘密計算は以前から追っているが、これほど多数の企業から新しい事例をまとめて聞いたことはなく、新しい段階に進んだと感じた。各社とも利用企業と相談中の案件が増えてきているようで、競争領域が拡大していそうではあるが、まだまだ手を組んで進めるべきことが多く、DSA を始めとする連携組織の活動は重要。	学術研究・専門・技術サービス業
非常に勉強になりました。身近な環境との適合性を考えながら、学びを継続させて頂きたく存じます。	学術研究・専門・技術サービス業
講演資料をできる範囲で結構なので共有していただきたい	電気・ガス・熱供給・水道業
受講できなかった方にも、内容を紹介したい	情報通信業

コメント	業種
1. 本日の資料はいただけますでしょうか。法律のところは早すぎて、良くわかりませんでした。 2. 質問1（板倉さま） 秘密計算は、個人情報保護法に対応するための方法として推奨されていくのでしょうか？ 3. 質問2（近藤さま？他の方でも） 秘密計算用に暗号化されたデータが、本当に暗号化されているかどうかを、データ提供者が確認するにはどうしたらよいのでしょうか。秘密計算を使うと称して、あたかも暗号化したように見せかけてデータを覗き見てしまうという詐欺が考えられます。	製造業
SBTech 殿＞スマートシティに社会実装するためのコストや具体的ハードル、な課題について教えていただければ幸いです。	製造業
これまでの取組の中で、安全を確保するために暗号化をしたのだが、想定外の事が起きて、安全が確保されなかったケースというのはないのでしょうか？ 可能な範囲で教えて下さい。	製造業
セッション講演での御話しではありませんでしたが、秘密計算に関するご説明で、通常の暗号化との比較をした発言で、「暗号化したらそのまま計算できない 秘密計算は暗号化したまま計算できる」と言っていましたが、それって暗号化していると言えるのでしょうか。例えば、秘密計算に適した特定の変換技術（暗号）だけが秘密計算の対象ですか。	情報通信業

DSA へのメッセージなど

AI 規制法における位置づけの検討、データ活用の定義といった、DSA が取り組むべき活動について具体的なご意見をいただきました。また DSA の情報発信をご評価いただくコメントも見られました。

表 3 DSA へのコメント、印象など(自由記述、団体名称のみ修正)

コメント	業種
AI 規制法案は EU では年内に成立しそうだが、日本の事業者はこれに追随するのに汲々とする。今回の秘密計算は AI 規制法の観点からはどう位置付けられるものになるのか、そろそろ DSA も検討したほうがよいのではありませんか？	学術研究・専門・技術サービス業
今回の企画は秘密計算について俯瞰することができる良い機会となりました。一方で、”データを扱う”ということについて一般の人に理解してもらうことも必要だと思います。単に”データ”と言っても、ひとそれぞれ認識していることは千差万別です。データを扱うということがどういうことなのかがわかるような資料やフォーラム（テーマにはそのへんに配慮する必要がありますが）が必要だと思います。	製造業
このようなイベントを定期的に開催いただけると嬉しいです。	情報通信業
日本のデータ利活用を牽引してくれると期待しています。	製造業
当協議会との連携をよろしくお願いします。	その他
いつも積極的に情報発信いただき大変役立っております。	製造業

この文書について

- 名称　DSA フォーラム「秘密計算が実現する安心・安全な企業間データ共有」開催レポート
- ファイル名　220311_SecureComputationForum.pdf
- 掲載 URL　https://data-society-alliance.org/event-report/2203_securecomputation/
- 概要

  この資料は、一般社団法人データ社会推進協議会(DSA)が開催した国内初の秘密計算総合イベント「秘密計算が実現する安心・安全な企業間データ共有」の講演内容を再編したものです。
- 基本情報
  - DSA 基準文書区分　ホワイトペーパー
  - 作成者　一般社団法人データ社会推進協議会 4011005007414
  - 公開者　一般社団法人データ社会推進協議会 4011005007414
  - 著作権者　一般社団法人データ社会推進協議会 4011005007414
  - 発行日　2022 年 10 月 20 日
  - 公開日　2022 年 10 月 20 日
  - 作成アプリケーション　Microsoft Word
  - 公開形式　PDF
  - 公開ファイル容量　2,982KB
  - ページ数　33 ページ
- 利用条件
  - 本書を利用したこと、利用しなかったことにより直接または間接に生じた損害に対して、DSA は一切の責任を負いません。
  - 本書を組織や団体として活用される際は、DSA へご一報いただければ幸いです。

本書に関するお問い合わせ

一般社団法人データ社会推進協議会(DSA) 4011005007414

E-mail　info@data-society-alliance.org
ホームページ https://data-society-alliance.org/contact/

