秘密計算の活用例
～ 秘密計算を利用した安全な組織間でのデータ活用への期待 ～

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
2023年6月2日

DATA-EX
Data Society Alliance

はじめに

- 本資料の作成背景と目的
  - データ社会推進協議会（DSA:Data Society Alliance）は、データを秘匿しながら処理できる技術である「秘密計算」を、単なる安全管理のための技術ではなく、組織間での安全なデータ活用ができる技術と捉え、これにより社会的・経済的利益の向上ができると考えている
  - そこで、 DSA 利活用促進委員会 秘密計算活用WGでは、ヒアリングや講演イベントなどを通じ、どの様な活用例の案（活用案）が期待されているかを整理した
  - 本資料は秘密計算による組織間でのデータ活用の可能性を多くの方に感じて頂くことを目的とする
  - 本資料を参考に新たな活用例の案の議論が進めば幸いである
- 想定読者
  - データ活用を目指す企業関係者、秘密計算を理解したい利用者、政府関係者の方 など
- 本資料の活用場面
  - 組織間でのデータ活用に関する新たな活用案を議論
  - 秘密計算の社会実装に向けた検討の場の設立に向けた議論

本資料は活用案を整理したものであり、秘密計算の技術的な詳細・制限・限界や、秘密計算が出力する計算結果から秘匿したい情報が暴露されるリスクの評価・対策や、秘密計算と法律との関係などは、本資料のスコープ外である

目次

1. 組織間でのデータ活用への期待

組織間でのデータ活用の価値

個人情報や企業秘密のような機密性が高いデータを、組織間で安全にデータ結合して
活用できれば、様々な社会課題の解決が期待できる

EVインフラ最適化

各EV車の充電残量や移動先の
情報を集約し需要予測し
EV設備や電力を最適化

ものづくり・物流最適化

サプライヤやメーカ間で
機密情報を統合し、
最適な生産・物流を最適化

個別化医療

ゲノムと投薬情報の統合・
相関分析による、
個別化医療の実現

金融不正検知

銀行・決済データを
秘匿しながら結合分析し
不正送金を検知

電力消費の見える化

テナント毎の電力消費量の
開示が嫌がられるため
ビルやエリアで秘匿して集計

組織間のデータ活用の課題

- 組織間のデータ活用（データの流通）に阻害要因があり、進んでいない
- 阻害要因として「提供先での目的外利用」「知見等の競合への横展開」などが挙げられている

データ流通の阻害要因の例

1. 提供先での目的外利用（流用）
2. 知見等の競合への横展開
3. パーソナルデータの適切な取扱いへの不安
4. 提供データについての関係者の利害・関心が不明
5. 対価還元機会への関与の難しさ
6. 取引の相手方のデータ・ガバナンスへの不安
7. 公正な取引市場の不足
8. 自身のデータが囲い込まれることによる悪影響

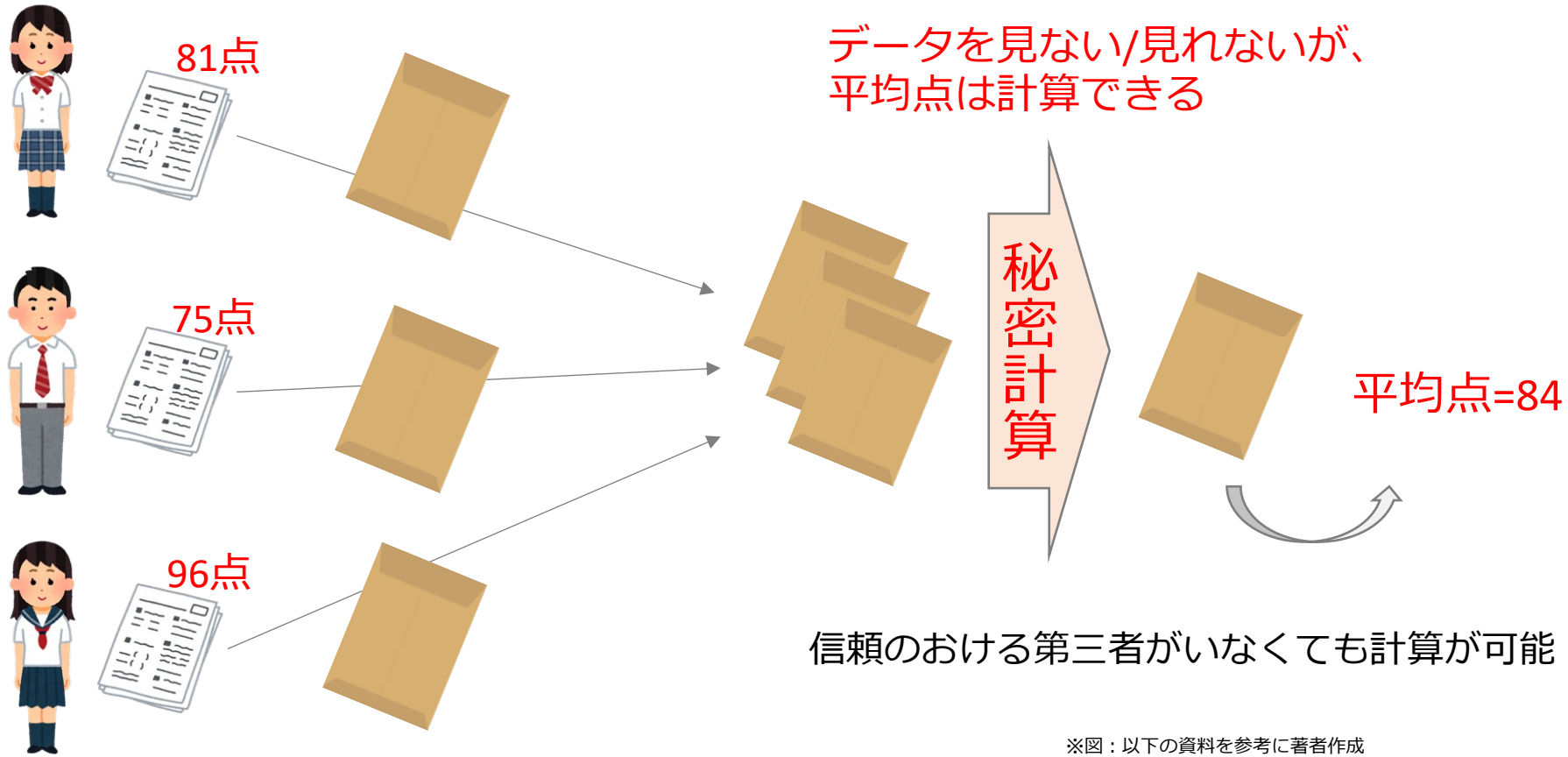
出典：
パブリックコメント「プラットフォームにおけるデータ取扱いルールの実装ガイダンス（案）」に係る意見募集,2021年12月3日
https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000227587

2. 秘密計算とは

秘密計算のイメージ

「秘密計算」とは、データを他人に見せないで処理できる技術である

図：友達同士で点数を隠しながら平均点を計算する例



※図：以下の資料を参考に著者作成
濱田浩気 日本電信電話株式会社 NTTセキュアプラットフォーム研究所
“知られたくない情報を、使える情報に変えるプライバシー保護術～秘密計算のしくみとは？”,
https://www.milive-plus.net/gakumon170202/

従来の暗号技術との比較

従来の暗号技術は、データを処理する際には復号してから処理する必要があったが、
秘密計算は暗号化※3したまま処理が可能

表：従来の暗号技術との比較の例

	従来の暗号技術を利用したシステム	さらに**秘密計算技術**を追加したシステム
処理における暗号化	（対象外）	✓
通信における暗号化	✓	✓ ※1
保存における暗号化	✓	✓ ※1

※1 秘密計算技術を用いて、通信・保存時の暗号化を行うことが望ましいという意味ではない。
例えば準同型暗号は、適応的選択暗号文攻撃に対する識別不可能性（CCA安全）を満たすことが難しい※2など、
従来の暗号技術における通信・保存における安全性とは異なる考え方などが必要となる可能性あり。
※2 参考：江村恵太, 林卓也, 國廣昇, 佐久間淳,"まぜるな危険準同型暗号", CSS2016.
https://ipsj.ixsq.nii.ac.jp/ej/?action=repository_uri&item_id=175711&file_id=1&file_no=1
※3 秘密分散は鍵を用いた暗号化とは異なるが、本資料では秘密分散も含めて秘匿化することを暗号化と記載

秘密計算の名称・方式

本資料では利用案を整理した資料であるため、「秘密計算」をデータを秘匿しながら処理できる技術の総称と捉え、方式や要素技術は言及しない※1

表：秘密計算の方式・要素技術の例※2

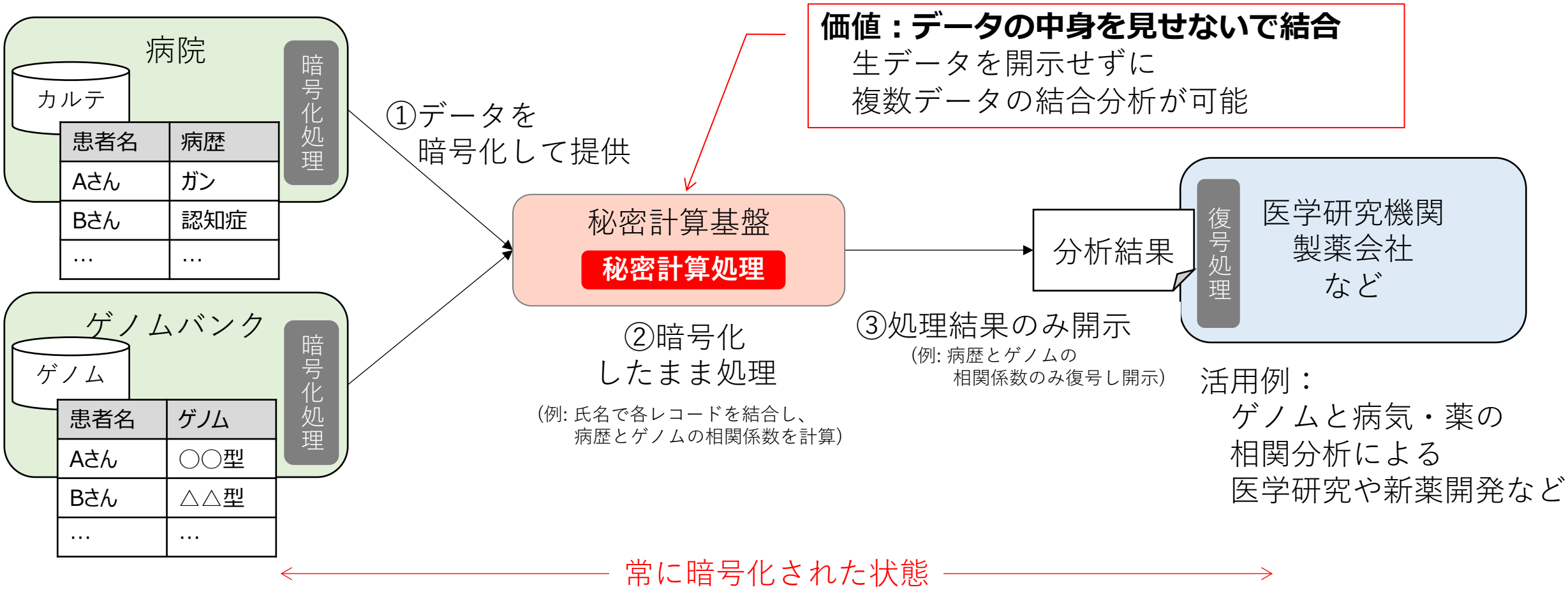
秘密計算の方式・要素技術	秘匿したまま処理可能な内容	技術カテゴリ
TEE （Trusted Execution Environment）	様々な処理が対象	ハードウエア
Garbled Circuit (ガーブルド・サーキット)		ソフトウエア
秘密分散を用いた秘密計算		ソフトウエア
(完全)準同型暗号		ソフトウエア
検索可能暗号	検索処理が対象	ソフトウエア

※1 「秘密計算」は別名として、秘匿計算、 Multi-Party Computation、Secure Computing、Confidential Computing とも呼ばれる
※2 本資料は技術の詳細を記載するは主な目的ではないため、この表では方式や要素技術を網羅的に示さず、いくつかの例を記載している

3. 秘密計算の価値

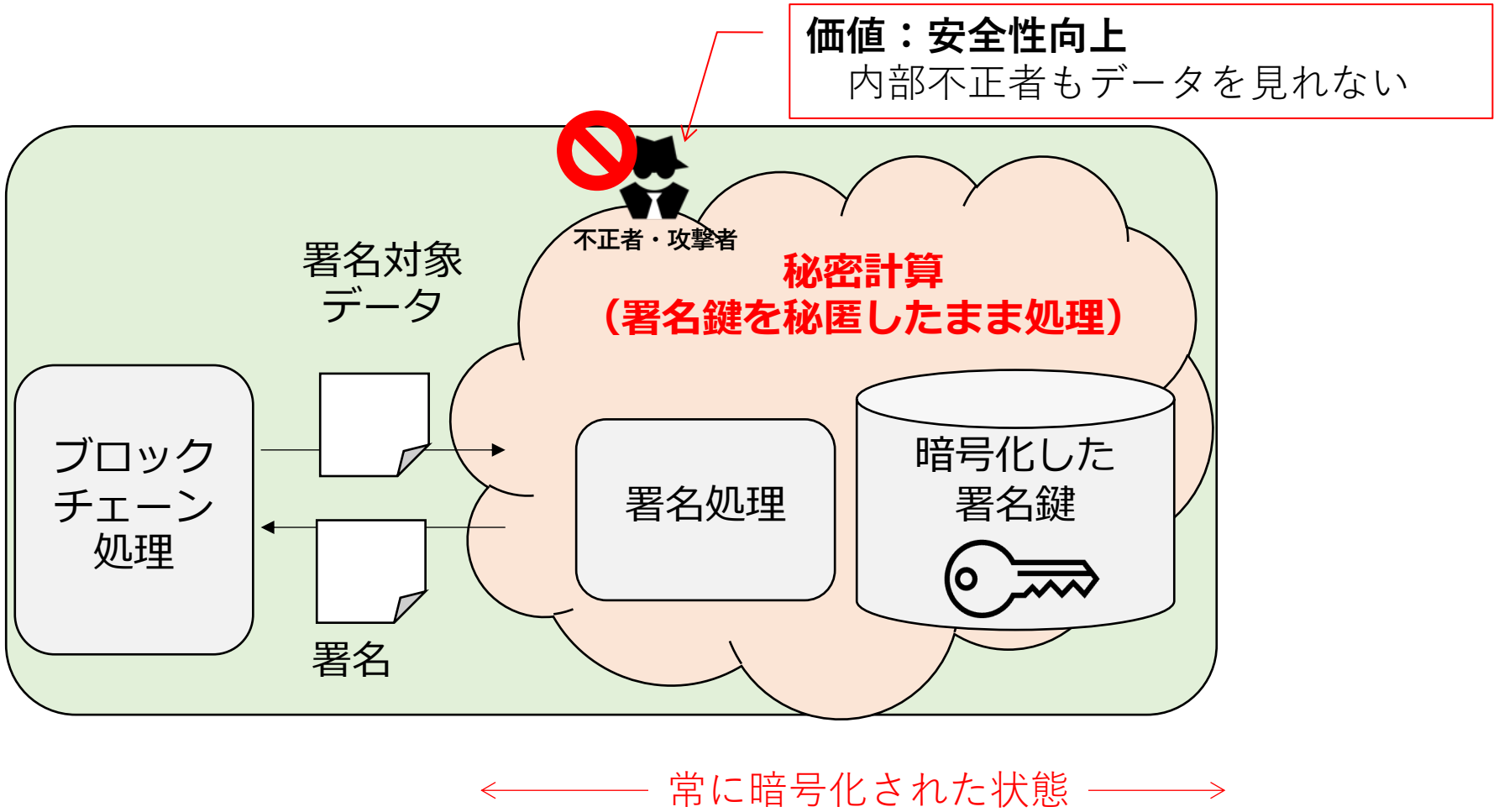
秘密計算の価値：①組織間でのデータ活用の促進

- 複数の組織のデータを、秘匿したまま結合・分析し、分析結果だけを開示可能
  - 例：病院のカルテデータと、ゲノムバンクのゲノム情報を、秘匿したまま結合分析し、病気・投薬とゲノムとの関係だけ開示



秘密計算の価値：②安全性の向上

- データを秘匿しながら処理するため、安全性が格段に向上
  - 例：ブロックチェーン処理の署名鍵を秘匿したまま署名処理などを実施



データ社会推進協議会が注目する秘密計算の価値

- DSAが注目するのは、価値①「**組織間でのデータ活用の促進**」である
- ヒアリングや講演イベントを通じたニーズ調査の結果、期待は大きいと考える

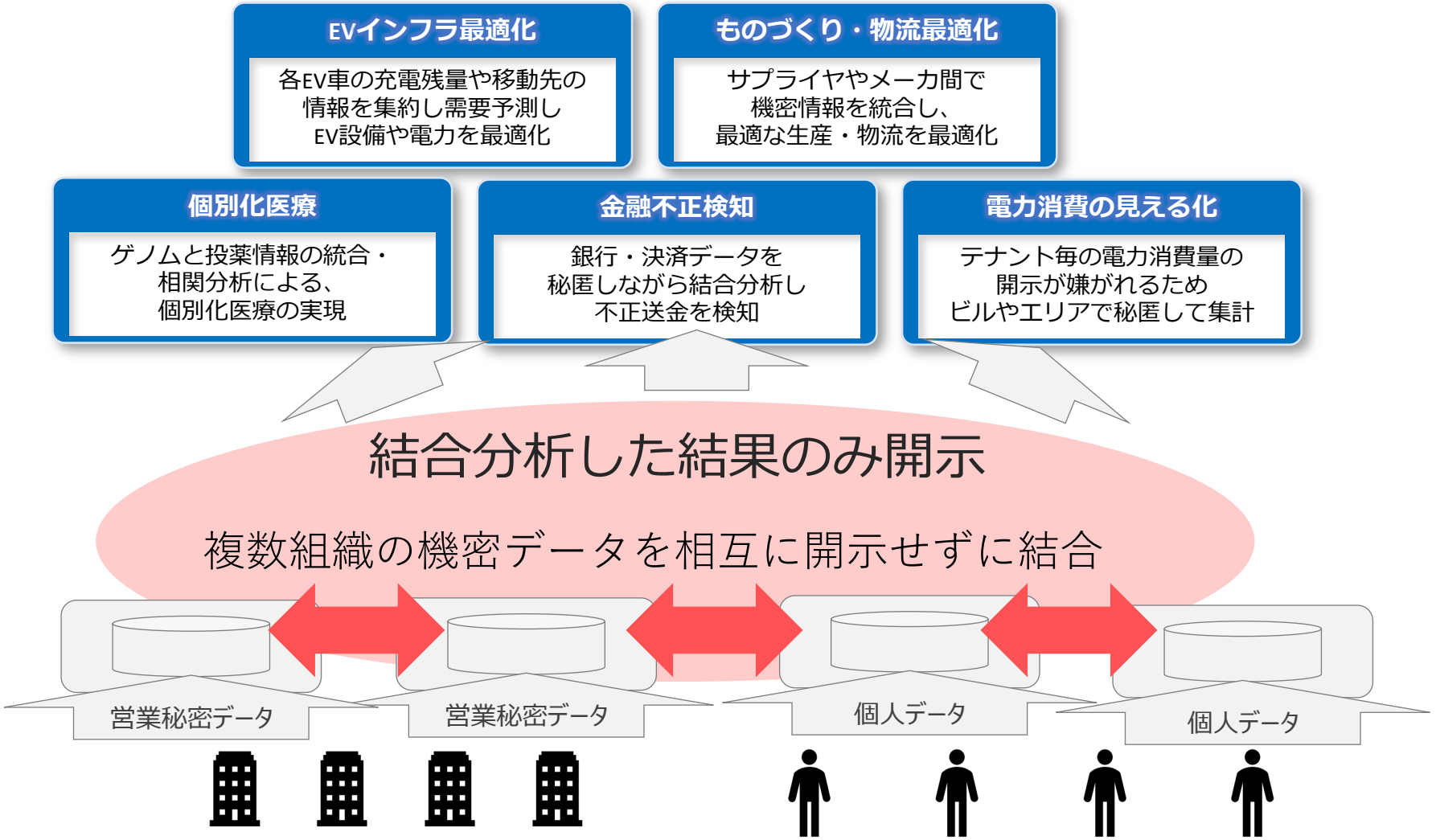
表：秘密計算の対象データと提供する価値

処理対象のデータ	価値① 組織間でのデータ活用の促進	価値② 安全性の向上
複数の データ	◯	◯
単一の データ	(対象外)	◯

なお、価値②「安全性の向上」については、ブロックチェーンの鍵管理のシステムが、
全世界で100社程度技術採用され、特に海外にて大企業がスタートアップを買収されており、すでに実用化されている。

秘密計算による組織間でのデータ活用のイメージ

機密性の高いデータ（営業秘密、個人データ）を秘匿したまま組織間で結合分析し、
分析結果のみを開示することで、様々な社会課題を解決



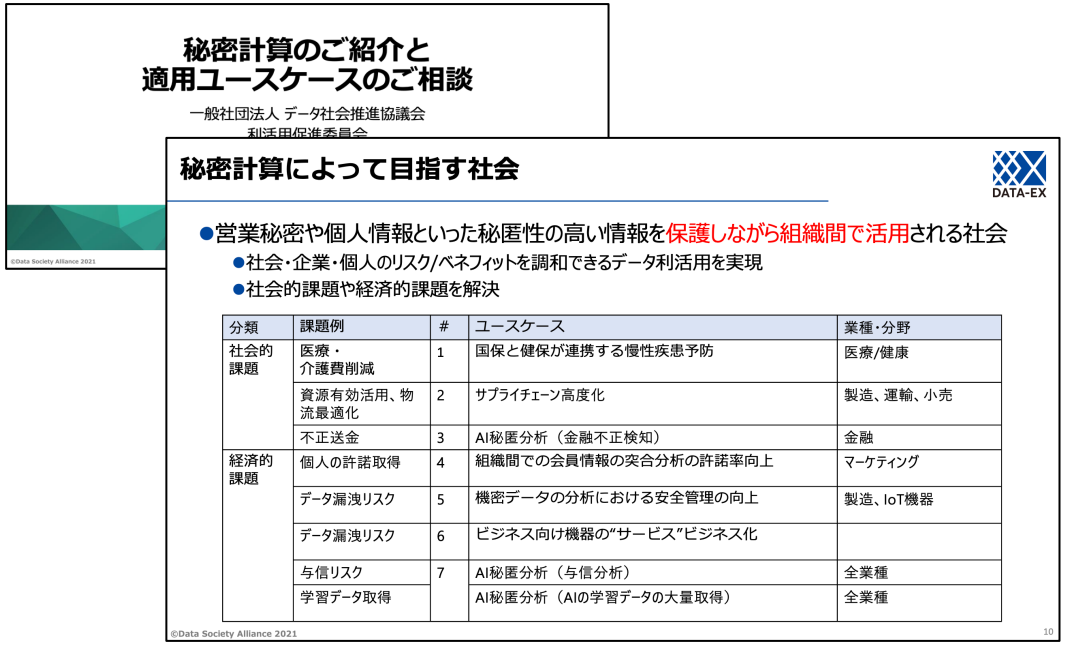
4. 秘密計算を用いた組織間でのデータ活用案

4-1. 活用案の検討の背景・目的・分類

秘密計算を用いた組織間データ活用案の検討の背景・目的

- DSA 利活用促進委員会 秘密計算活用WGにて、関連企業ヒアリングやイベントを実施して、組織間でのデータ活用の案を検討し、ニーズがあるか調査を実施
- 結果、いくつかの分野で組織間データ活用のニーズがある可能性があることが分かり、本資料に活用案を整理
- 本資料で示す活用案を参考に、データ活用を目指す企業・組織にて新たな活用案が検討されることを期待

関連企業へのヒアリング資料（抜粋）



秘密計算のご紹介と適用ユースケースのご相談

一般社団法人 データ社会推進協議会
利活用促進委員会

©Data Society Alliance 2021

秘密計算によって目指す社会

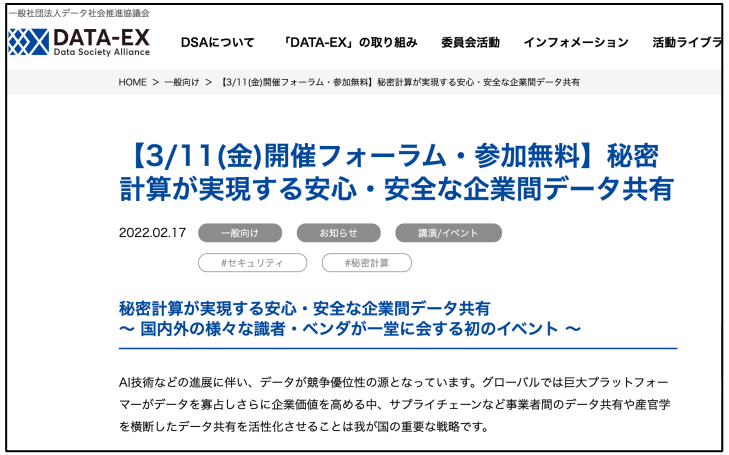
DATA-EX

●営業秘密や個人情報といった秘匿性の高い情報を保護しながら組織間で活用される社会
- ●社会・企業・個人のリスク/ベネフィットを調和できるデータ利活用を実現
- ●社会的課題や経済的課題を解決

分類	課題例	#	ユースケース	業種・分野
社会的課題	医療・介護費削減	1	国保と健保が連携する慢性疾患予防	医療/健康
	資源有効活用、物流最適化	2	サプライチェーン高度化	製造、運輸、小売
	不正送金	3	AI秘匿分析（金融不正検知）	金融
経済的課題	個人の許諾取得	4	組織間での会員情報の突合分析の許諾率向上	マーケティング
	データ漏洩リスク	5	機密データの分析における安全管理の向上	製造、IoT機器
	データ漏洩リスク	6	ビジネス向け機器の"サービス"ビジネス化	
	与信リスク	7	AI秘匿分析（与信分析）	全業種
	学習データ取得		AI秘匿分析（AIの学習データの大量取得）	全業種

©Data Society Alliance 2021 10

秘密計算に関するイベント概要



一般社団法人データ社会推進協議会

DATA-EX Data Society Alliance　DSAについて　「DATA-EX」の取り組み　委員会活動　インフォメーション　活動ライブラ

HOME ＞ 一般向け ＞ 【3/11(金)開催フォーラム・参加無料】秘密計算が実現する安心・安全な企業間データ共有

【3/11(金)開催フォーラム・参加無料】秘密計算が実現する安心・安全な企業間データ共有

2022.02.17　一般向け　お知らせ　講演/イベント

#セキュリティ　#秘密計算

秘密計算が実現する安心・安全な企業間データ共有
～ 国内外の様々な識者・ベンダが一堂に会する初のイベント ～

AI技術などの進展に伴い、データが競争優位性の源となっています。グローバルでは巨大プラットフォーマーがデータを寡占しさらに企業価値を高める中、サプライチェーンなど事業者間のデータ共有や産官学を横断したデータ共有を活性化させることは我が国の重要な戦略です。

登録者：402名
参加者：316名

4.20★
評価平均

概要：
- 秘密計算に関するキーパーソン、ベンダーが集まる国内初のイベント

内容：
- 技術や標準化の概要、最新の実証ケースの紹介
- 法制度の専門家含む様々な識者によるパネルディスカッション
- 社会実装や活用促進の道筋と課題について議論

活用案整理による秘密計算の組織間データ活用への知見

- 【知見１】様々な事業領域にて、秘密計算の組織間データ活用の期待あり
  - 医療・ヘルスケア領域、マーケティング領域、スマートシティ領域（自動車、不動産、MaaS）など
- 【知見２】個人情報に限らず、秘密計算の組織間データ活用の期待あり
  - 必ずしも、個人情報（プライバシー保護）の観点でのみ期待されているのではなく、個人に関係ない営業秘密等の安全な活用にも期待
- 【知見３】経済的利益と社会的利益といった主な連携目的※1によって、組織間での連携の傾向が異なる※2

表：経済的利益と社会的利益における連携の傾向

主な連携目的	連携組織数の傾向	連携の主導の傾向	連携先の傾向	連携先の傾向
経済的利益 （例：主に自社の課題の解決）	少数企業連携	一社が主導	提携企業間連携 （社内、グループ企業間）	異業種との連携
社会的利益 （例：社会的共通課題の解決）	多数企業連携	コンソーシアム等で協力	競合含め連携 (競合、国家間連携)	同業種との連携

※1 連携の目的は自社の経済的な利益でもあると同時に社会的な利益でもあることが多いが、ここでは主にどちらの目的が比較的大きいかを、可能な限り消費者の視点で判断している
※2 あくまで、そのような傾向があるだけで、連携の主な目的に応じて形式が決定するわけではない

活用案の分類

- 分類軸１：業種・分野

- 分類軸２：データ種類※1
  - 個人情報
    - 個人情報保護法の「個人情報」※2に該当する情報 （例：カルテ情報、個人の購買情報）
  - 人に関する情報
    - 「個人情報」ではないが、人間に関する情報（例：個人情報を集計した統計情報※3、端末識別子等の個人関連情報※4）
  - その他機密情報
    - 上記ではない（個人情報や人に関する情報ではない）機密情報（例：製品製造数(営業秘密)、人工衛星の軌道 (国家機密)）

- 分類軸３：主な連携目的※5
  - 経済的利益（例：主に自社の課題の解決）
  - 社会的利益（例：社会的共通課題の解決）

※1 処理やデータの内容によって、明確な分類が困難な場合もあるが、可能な限り消費者の視点で判断している。
　なお、秘密計算が対象とするのは少なくとも秘匿したい情報（例：プライバシーに関わる情報、営業秘密、国家機密に関わる情報など）である。
※2 https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/#a2-1
※3 参考：個人情報保護委員会 FAQ Q15-1 https://www.ppc.go.jp/all_faq_index/faq1-q15-1/
※4 端末識別子は、個人関連情報に該当し提供先で「個人データ」となる場合もある。 参考：https://www.ppc.go.jp/all_faq_index/faq1-q8-1/ https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/#a3-7
※5 連携の目的は自社の経済的な利益でもあると同時に社会的な利益でもあることが多いが、ここでは主にどちらの目的が比較的大きいかを、可能な限り消費者の視点で判断している

4-2. 活用案の一覧

活用案の一覧と分類

※ 分類軸の説明は別スライドを参照

DATA-EX

#	活用案の名称	分類１：業種・分野	分類２：データ種類 （個人情報 / 人に関する情報 / その他機密情報）	分類３：主な連携目的 （経済的利益 / 社会的利益）	検討レベル※1 (ヒアリング / 実証実験)
1-1	個人情報の結合分析の同意率向上	マーケティング	個人情報	経済的利益	ヒアリング
1-2	データ開示を防いだデータクリーンルーム	マーケティング	個人情報、 人に関する情報	経済的利益	ヒアリング、実証実験
1-3	商品購買の全体傾向分析	マーケティング	個人情報、 人に関する情報	経済的利益	ヒアリング
2-1	移動の需要予測（個人情報を統合）	SDGsスマートシティ （スマートシティ関係）	個人情報	社会的利益 （脱炭素・エネルギー効率化）	ヒアリング
2-2	充電設備の需要予測（営業秘密の統合）	SDGsスマートシティ （EV関係）	人に関する情報	社会的利益 （脱炭素・エネルギー効率化）	ヒアリング
3-1	物流最適化・共同配送可能性の判断	物流・サプライチェーン （同業種との連携）	その他機密情報	社会的利益 （脱炭素・エネルギー効率化）	ヒアリング
3-2	系列や国を跨いだサプライチェーンの高度化	物流・サプライチェーン （異業種との連携）	その他機密情報	社会的利益 （効率化、フードロス）	ヒアリング
4	医療データ（個人情報）の結合分析	医療	個人情報	社会的利益・経済的利益	実証実験
5	金融不正検知（連合学習への適用）	金融	人に関する情報、 その他機密情報	社会的利益・経済的利益	実証実験
6	政策関係の分析（エストニアの事例）	政府・自治体	個人情報	社会的利益	実証実験
7	人工衛星軌道の衝突検知	国家間	その他機密情報	社会的利益	実証実験

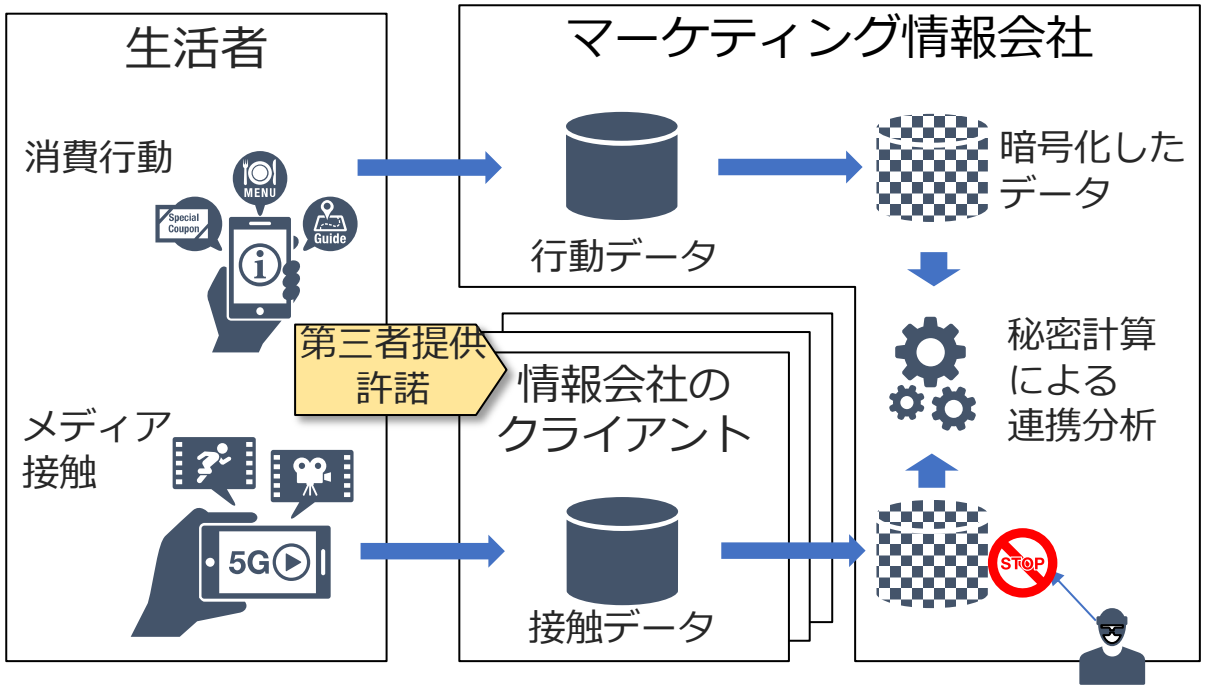
※1 活用案がヒアリングにて検討されたものか、実証実験まで行われているものかの観点で整理

参考：活用案の記載内容

- 背景・課題
  - 活用案の背景と、従来の課題
- ソリューション内容
  - 秘密計算による課題解決の内容
- 提供価値
  - 誰に、どのような価値を提供するか
- 説明図
  - 活用案を説明する簡単な図

1-1. 個人情報の結合分析の同意率向上

背景・課題	ソリューション内容
生活者の行動データを自社と他社で連携分析したいが、第三者提供の許諾率が低く、マッチング可能なデータ量が少ない	秘密計算を用いて行動データを安全に取り扱うことで、連携分析に対する生活者の不安を解消し、許諾率を高め、分析に使える多量のデータを確保



■提供価値

生活者に

■自分のデータのセキュリティを維持しつつ、データの用途を広げて価値を増やせる

マーケティング情報会社とクライアントに

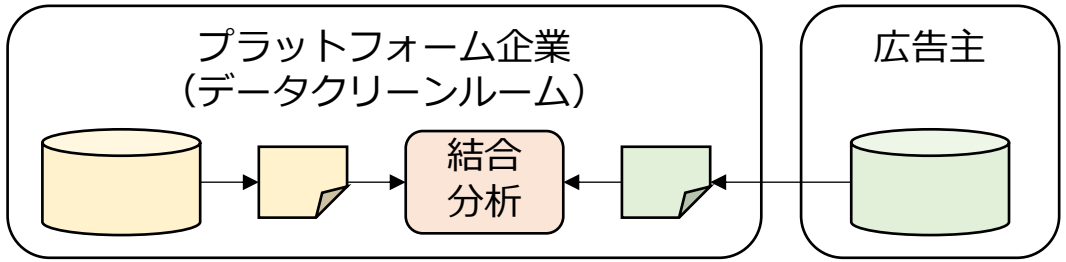
■連携分析に使えるデータが増えて、実用的意義のある分析が可能に

1-2. データ開示を防いだデータクリーンルーム

- 背景：プラットフォーム企業※1は、データクリーンルームという発想で、自社が保有するデータを外部に出さず
  他社（広告主など）からのデータを受けて自社データと結合して分析を実施
- 課題：広告主の保有データ※1は営業秘密でもあるため、他社（プラットフォーム企業）への送信は可能な限り避けたい
- ソリューション内容：秘密計算を用いて、相互にデータを秘匿しながら、データの結合して分析
- 提供価値：広告主は安心してデータ結合分析を実現し、プラットフォーム企業はデータ結合分析を促進

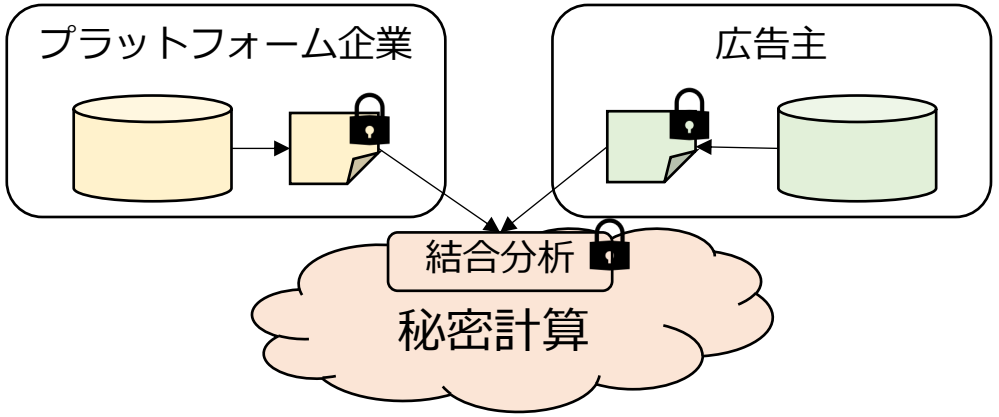
図：従来（秘密計算を用いない場合）

広告主のデータをプラットフォーム企業に
送信する必要がある



図：提案（秘密計算を用いた場合）

秘密計算を用いて秘匿しながら結合分析するため
データを送信先に見られる心配がない

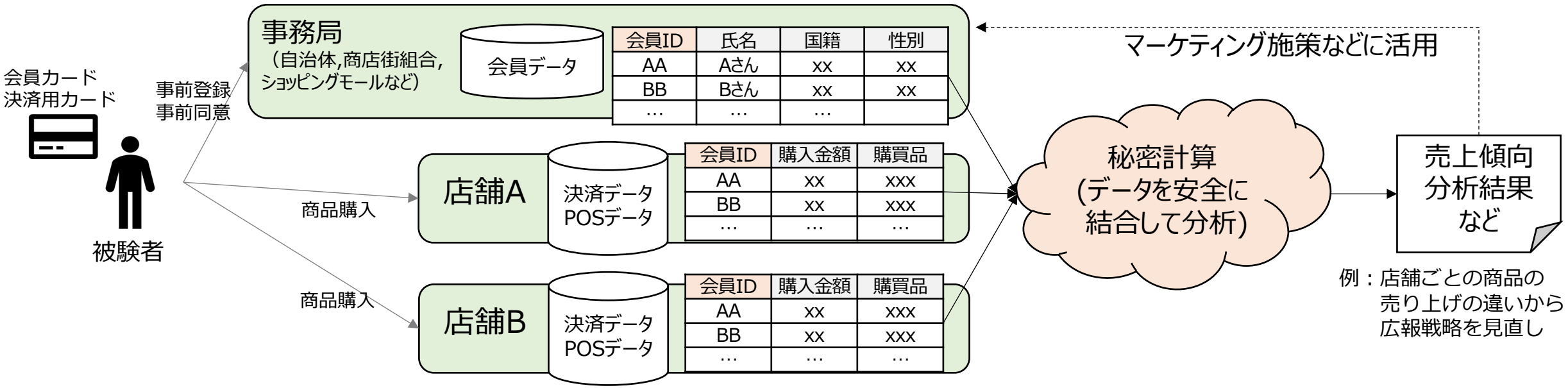


※1 デジタルプラットフォームを運営する事業者など。参考： 経済産業省,デジタルプラットフォーム, https://www.meti.go.jp/policy/mono_info_service/digitalplatform/index.html
※2 広告主が保有するデータはcookieや広告関係のIDに紐づく情報である場合は、個人情報に該当しなくとも、個人関連情報に該当する場合がある。少なくとも、このデータは公開したくない情報であることが多い。

1-3. 商品購買の全体傾向分析

- 背景：ショッピングモール運営事業者は、モール全体での購買傾向を分析し、マーケティング施策を検討したい
- 課題：各店舗の購買データは個人情報や営業秘密であるため他社（他店舗等）へ開示したいくない
- ソリューション内容：購買データを、秘密計算を用いて統合分析（個人情報の結合分析について同意を得る前提）
- 提供価値：顧客の購買傾向に基づいた、広報戦略や商品の品揃えの見直しによる売り上げ向上と利便性向上 (※1の事例を参考)

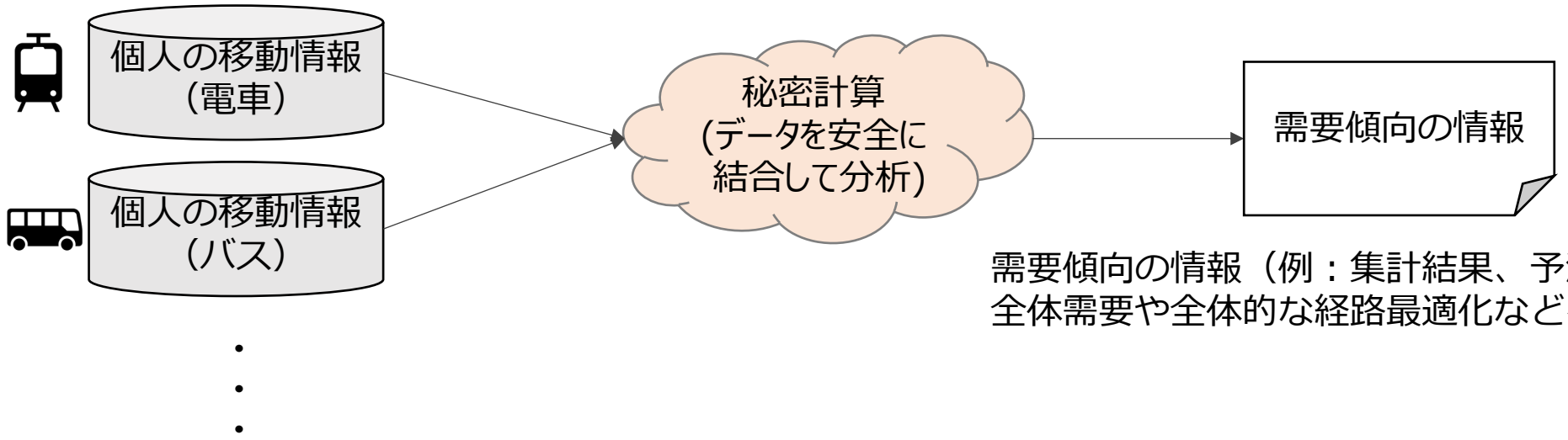
(図：※1の実証を参考に作成)



※1 参考資料： “2. 算師®を用いたデータ利活用事例～複数組織のデータの安全な統合分析～”, NTT 西田, BUSINESS COMMUNICATION, https://www.bcm.co.jp/solution-now/cat-solution-now/2019-06_1975/

2-1. 移動の需要予測（個人情報を統合）

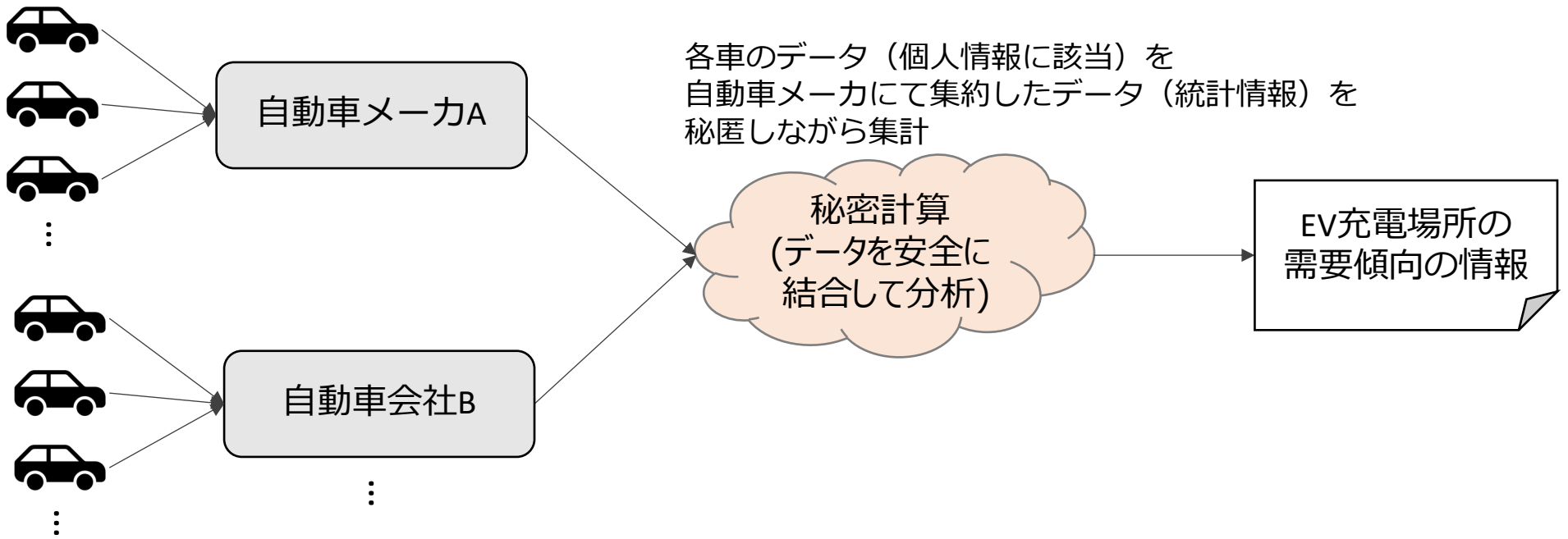
- 背景・課題：
  - MaaSなどでは、移動の需要を予測するために、過去の移動に関する情報から予測モデルの学習が必要
  - そのためには、個人の様々な移動手段（電車、バス、タクシー、徒歩など）の移動履歴の情報を統合したいが、統合したデータベースを構築するのはプライバシー観点で懸念がある
  - 個人個人の移動そのものを知りたいのではなく、全体としての傾向を学習したいだけである
- ソリューション内容：様々な個人の移動手段の情報を秘匿しながら結合し、統計的な分析として移動需要の学習を行う
- 提供価値：プライバシーや営業秘密を秘匿した高精度な移動需要予測の実現による、快適なMaaSサービス



需要傾向の情報（例：集計結果、予測モデル）を用いて、
全体需要や全体的な経路最適化などを行う

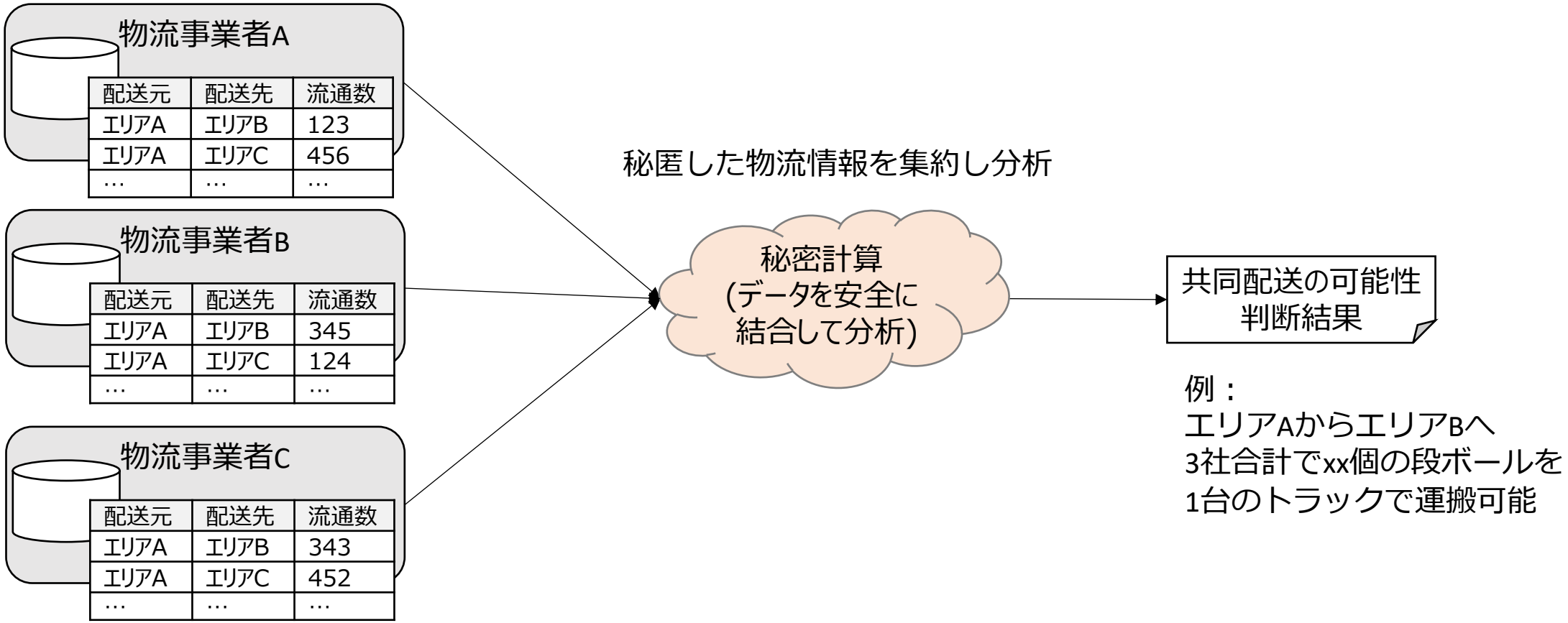
2-2. 充電設備の需要予測（営業秘密の統合）

- 背景：EVの充電場所には限りがあり、充電の需要を予測して混雑回避などの最適化が望ましい
- 課題：需要予測に必要な各EV車の充電残量や移動先の情報は営業秘密やプライバシーに関わる
  （各EV車の充電残量等の個人に関わる情報を自動車メーカにて集約し統計情報にできるが、営業秘密に該当）
- ソリューション内容：秘密計算を用いて、各EV車の充電残量や移動先の情報を集約し需要予測
- 提供価値：混雑回避による利便性向上や、需要に基づくエネルギーの効率化



3-1. 物流最適化・共同配送可能性の判断

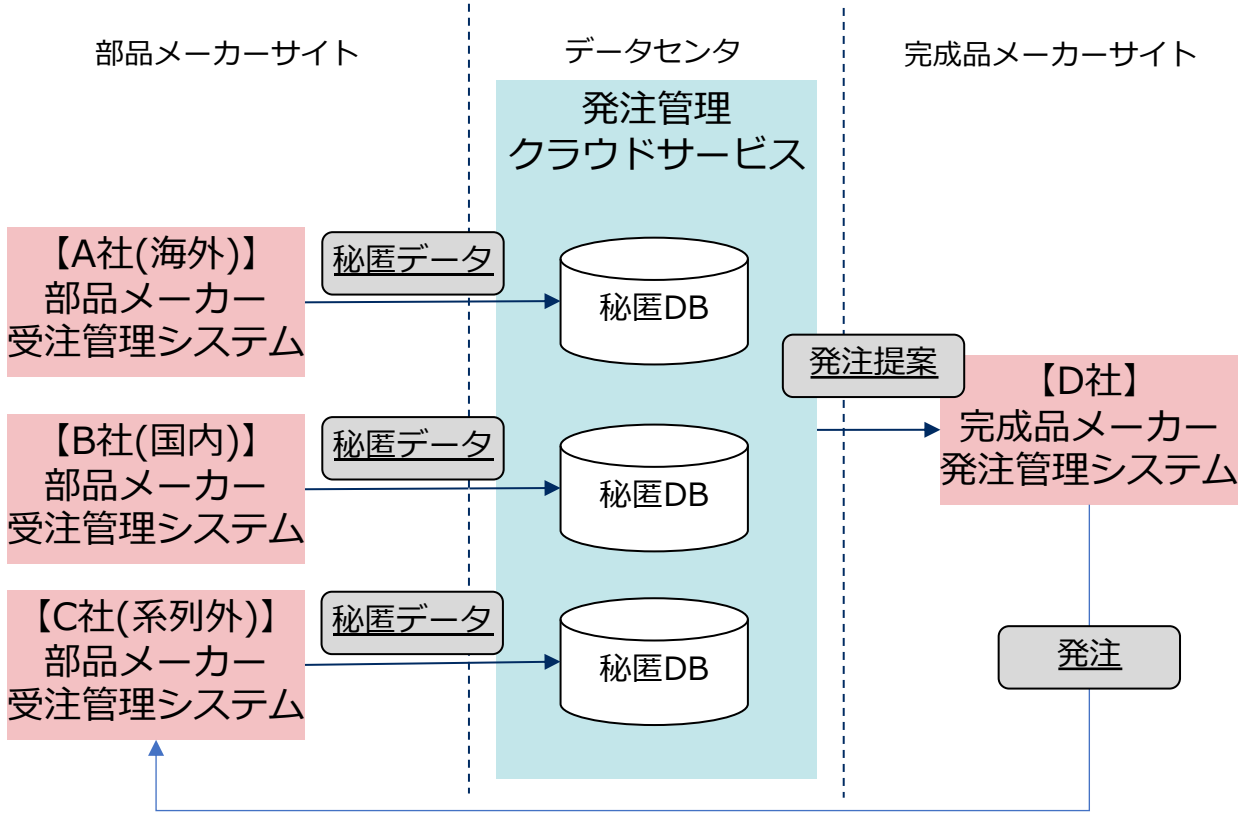
- 背景・課題：物流の人手不足等のため共同配送を行いたいが、物流の需要に関する情報は営業秘密に関わる
- ソリューション内容：秘密計算を用いて、物流量や配送先の情報を集約し共同配送の可能性を判断
- 提供価値：物流が最適化され物流サービスの質向上（例：離島における配送費用や配送時間の削減、人手不足解消）



3-2. 系列や国を跨いだサプライチェーンの高度化

DATA-EX

課題	ソリューション内容
完成品メーカーが、系列外や海外等の部品メーカーの稼働状況を確認し、適切な発注管理をしたいが、営業秘密等の観点で部品メーカーは詳細な情報を提供したくない	部品メーカーが保有する受注管理のデータを秘匿しながら収集することで、最適化された発注管理を実現



■提供価値

完成品メーカーに

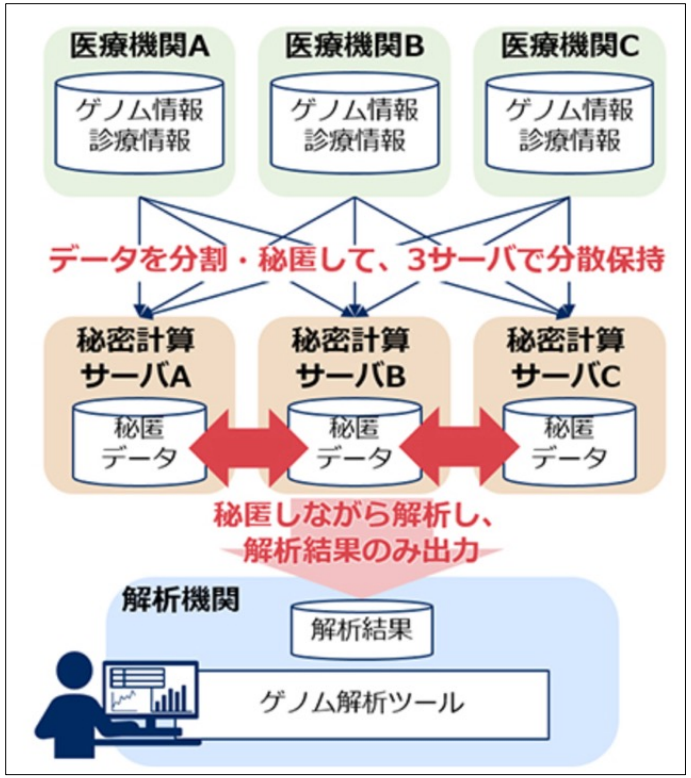
■調整コストなどの時間・費用をかけずに迅速に発注できる

部品メーカーに

■調整コストなどの時間・費用をかけずに受注管理ができる

4. 医療データ（個人情報）の結合分析

- 背景・課題：医療データ（カルテデータやゲノム情報等）は医学研究に役立つが、プライバシーや研究機関の競争力の観点で、他機関へのデータ開示は好まれない
- ソリューション内容：医療データを秘匿しながら結合し分析し、解析結果のみを開示
（例：ゲノムバンクが持つゲノムと、病院が持つカルテとを1:1で結合分析。個人同意済み）
- 提供価値：プライバシー等を保護しつつ新薬開発等の医学研究の促進

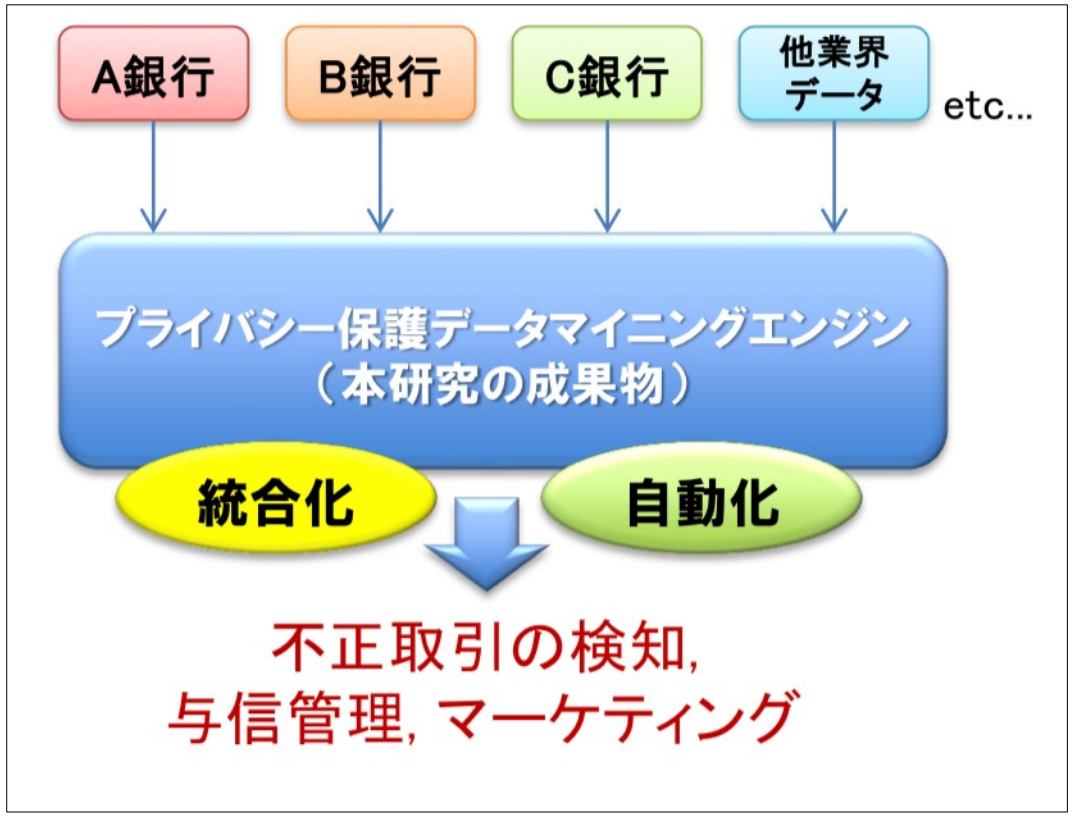


図出典：NECプレスリリース, “NEC・大阪大学、複数機関が保有するゲノム情報をプライバシー侵害リスクを抑えて解析できることを実証 ～データを暗号化したまま解析できる秘密計算で実現～”, https://jpn.nec.com/press/201907/20190723_03.html

5. 金融不正検知（連合学習への適用）

- 背景：銀行等において不正送金を予測検知したいが、そのためには多量な過去の不正送金データが必要
- 課題：予測のためにデータを集めたいが、送金関係の金融データ（集約したデータ）は営業秘密に該当
- ソリューション内容：各銀行にて学習を行い、その学習結果※を秘匿しながら統合して予測モデルを作成し、共有
- 提供価値：不正送金の検知精度の向上

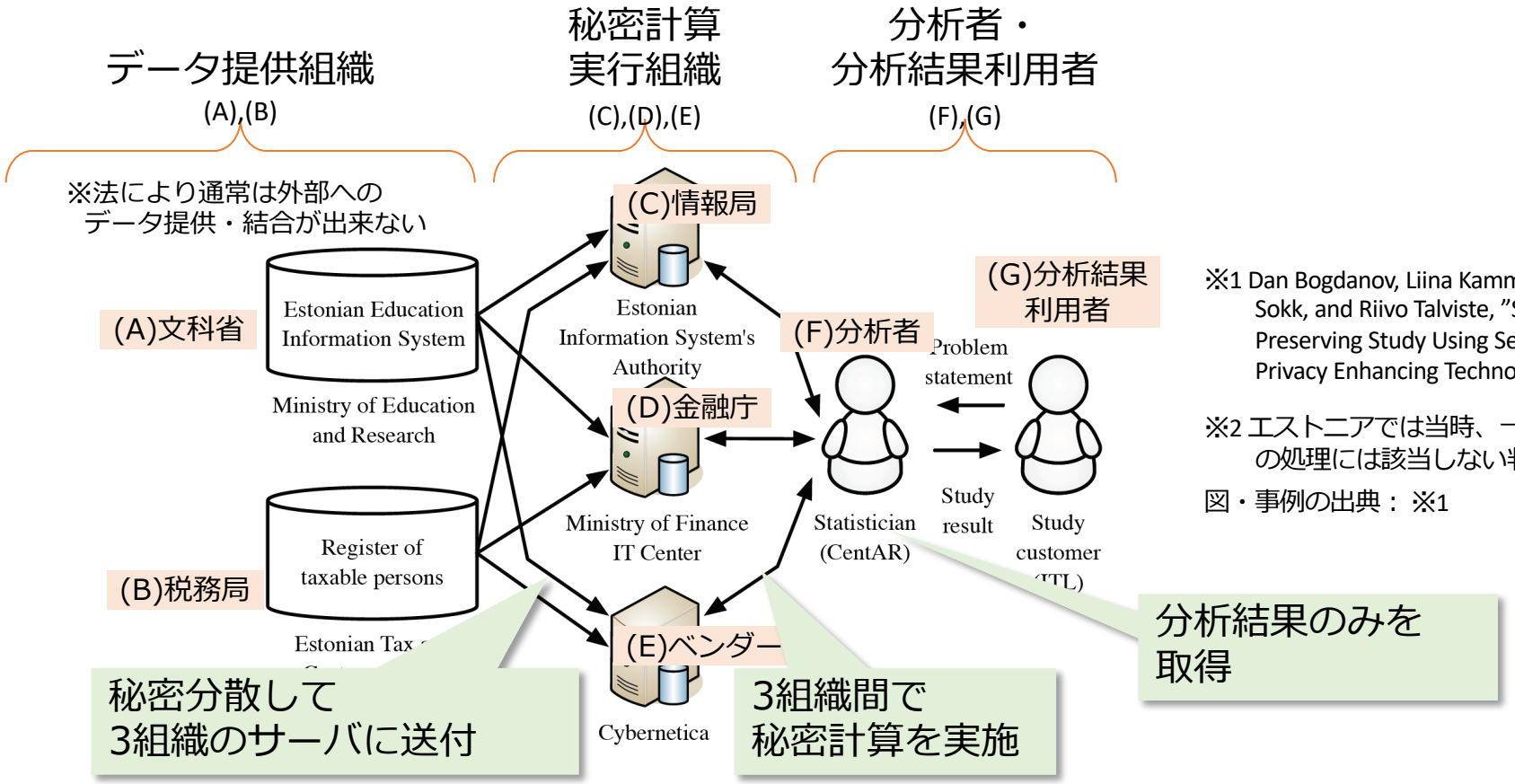
※ この例では、各銀行で学習した結果データは複数の個人情報を集約したデータであるため、統計情報に該当する想定。
また、複数機関で連携して機械学習を行う処理を連合学習（Federated Learning）と呼ぶ場合もある。



出典: 花岡ら, “プライバシー保護データ解析技術の 社会実装”, CREST:イノベーション創発に資する人工知能基盤技術の創出と統合化, 2019年6月
https://www.jst.go.jp/kisoken/crest/research/activity/1111094/ai_sympo2/pdf/03_crest_ai_sympo2.pdf

6. 政策関係の分析（エストニアの事例）

- 背景・課題：政府機関の保有データを用いて社会的な調査したいが、個人情報に該当するため処理が容易では無い
  （例：エストニアでは、学生のアルバイト就業が成績へ影響するかの調査を実施※1）
- ソリューション内容：秘密計算を用いて安全に結合分析※2
- 提供価値：安全に社会的な調査の分析結果が得られ、政策判断等へ利用可能に



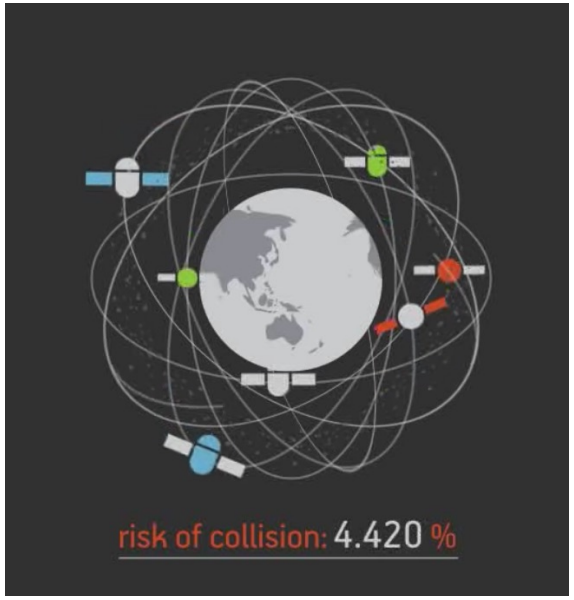
※1 Dan Bogdanov, Liina Kamm, Baldur Kubo, Reimo Rebane, Ville Sokk, and Riivo Talviste, ”Students and Taxes: a Privacy-Preserving Study Using Secure Computation”, Proceedings on Privacy Enhancing Technologies ; 2016 (3):117–135

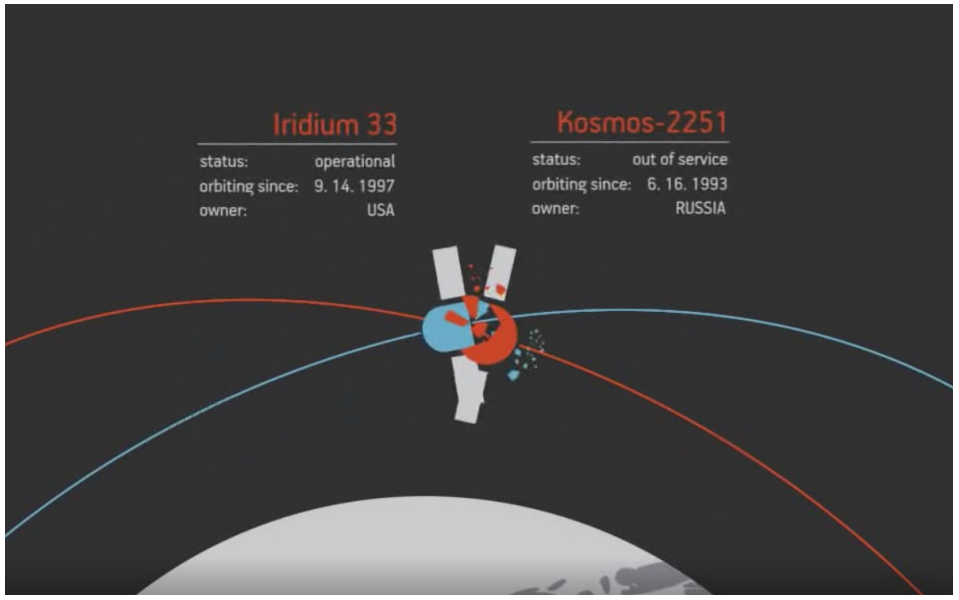
※2 エストニアでは当時、一定の条件を満たせば、個人情報の処理には該当しない判断をした

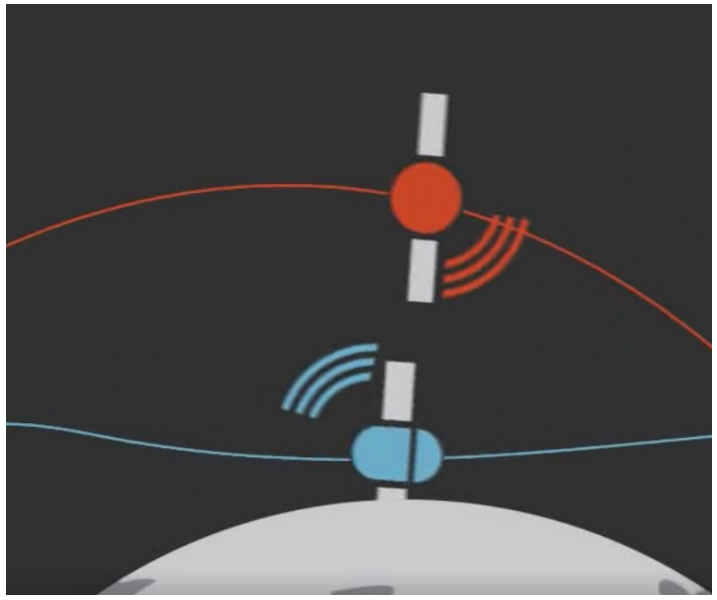
図・事例の出典： ※1

7.人工衛星の軌道

- 背景・課題：人工衛星は一定の衝突のリスクがあるが、軌道情報は国家機密に該当する場合もあり、情報開示は困難
- ソリューション内容：秘密計算を用いて軌道情報を秘匿しながら、衝突するかどうかだけを判定し、判定結果だけ共有
- 提供価値：衝突の可能性が高い場合に衝突回避行動をとり、人工衛星の事故を防ぐ







図・事例の出典：
Cybernetica sharemind, “Using Sharemind to Estimate Satellite Collision Probability”, https://sharemind.cyber.ee/satellite-collision-security/

5. まとめ

まとめ

- ヒアリングや講演イベントを通じ、秘密計算を用いた組織間でのデータ活用が期待を確認
  - 【知見１】様々な事業領域にて、秘密計算の組織間データ活用の期待あり
  - 【知見２】個人情報・非個人情報の両方で、秘密計算の組織間データ活用の期待あり
  - 【知見３】自社利益と社会利益といった目的によって、組織間での連携の傾向が異なる
- 秘密計算の実用化・普及に向けた活動に期待
  - イベント・ホワイトペーパーを元にした議論活発化に期待
  - DSAは引き続きイベント等を実施予定
- 本資料の活用例仮説から見えてきた課題
  - さまざまな活用事例の検討のための技術の周知
  - 社会的な利益のための業界主導・社会課題のため座組みの必要性
    - 異業種の連携（例：サプライチェーン連携）や、同業種の連携（例：業界でのデータ集約）
    - 営業秘密（非個人情報）の安全な処理の利用例の検討
  - 個人情報関係の活動
    - 個人情報保護法との秘密計算技術の関係整理
    - 秘密計算による安心感の成熟による個人同意率の向上のための、消費者を含めた技術周知など

付録A：実証実験の事例

国内での実証実験等の事例の一部（DSA会員企業） (1/2)

※法人分類順、社名振仮名辞書順

- 株式会社Acompany
  - マーケティング（DAC）
    https://www.dac.co.jp/index.php?p=press/2021/20210518_dac_acompany
  - 医療（三谷産業）
    https://prtimes.jp/main/html/rd/p/000000013.000046917.html
  - 医療（名古屋大学病院)
    https://acompany.tech/news/21-0701-2/
  - 分析サービス（CTC）
    https://www.ctc.co.jp/news/2022/20220719/
  - 走行情報分析（オプティマインド）
    https://prtimes.jp/main/html/rd/p/000000012.000046917.html
- EAGLYS株式会社
  - 交通（JR東日本）
    https://www.eaglys.co.jp/news/press-release/20201110-2
  - ERP（SAPジャパン）
    https://www.eaglys.co.jp/news/press-release/20211006
  - 創薬・素材（三井物産）
    https://prtimes.jp/main/html/rd/p/000000041.000041103.html
- エヌ・ティ・ティ・コミュニケーションズ株式会社
  - 医療（千葉大学病院）
    https://www.ntt.com/about-us/press-releases/news/article/2021/0208.html
    https://www.ntt.com/about-us/press-releases/news/article/2022/1129.html

国内での実証実験等の事例の一部（DSA会員企業） (2/2)

※法人分類順、社名振仮名辞書順

- 日本電気株式会社
  - 医療（大阪大学）
    https://jpn.nec.com/press/201907/20190723_03.html
  - 創薬（京都大学）
    https://jpn.nec.com/press/202203/20220311_01.html
  - 工場（三菱重工）
    https://jpn.nec.com/press/202209/20220928_03.html
- 株式会社日立製作所
  - 医療（東京大学）
    https://www.hitachi.co.jp/products/it/magazine/hitac/document/2017/10/1710c.pdf
  - 金融（千葉銀行）
    https://www.hitachi.co.jp/products/it/finance/topics/20181029-topics.html
- 国立研究開発法人産業技術総合研究所
  - 創薬
    https://www.aist.go.jp/aist_j/press_release/pr2011/pr20111101/pr20111101.html

海外での実証実験等の事例（参考として一部記載）

分野カテゴリ	処理カテゴリ	名称	課題	解決策	企業
証券	マッチング	安全な証券取引	・代替取引システム(ATS) による株式の相対取引時に、売手と買手の売価/買価情報、及びマッチング結果は第三者に漏洩されてはいけない。 ・ATSは、機密情報の一極集中になり、セキュリティ攻撃、データ漏洩に対して脆弱である。	・MPCの新規プロトコルMultiparty Agile Computation Engineer (MACE) にて、セキュリティ脆弱性の改善を図る。	PARTISIA
銀行	突合、AI/予測	本人確認、信用評価	・第三者金融機関が、不正な口座開設を抑止するためにKYCプロセスを強化する時に、他機関と同調してワンストップチェックプロセスの実行の担保を図るケースがあるが、その際にでも自社の顧客情報の第三者への非公開が条件となる。	・各機関は、顧客情報を暗号化し、KYCスコアリングシステムに当該暗号化された情報のアクセスを許諾する。KYCスコアリングシステムは、同様に他機関の暗号化された顧客情報と先の顧客情報から、顧客のスコアリングを算出して、各機関に結果を返す。	cosmian
銀行	突合、AI/予測	協調詐欺検知	・金融機関間の協調により、不正行為の検出精度の向上が期待できる。プライバシー保護、及びデータ機密保持の観点から、多くの場合は、第三者とのデータ共有は不可能。	・銀行口座の信用度の評価に、PageRankアルゴリズム活用 ・MPC技術を使って、複数の銀行にて各行の取引データをベースにした詐欺検知モデルを構築した。参加銀行間で、取引データは共有されない。	Inpher
保険	突合	協調型顧客分析、信用評価	・協調顧客分析、統計分析は、競合銀行間で、秘密情報連携を可能にする。データそのものは、秘密が保持されていなくてはならない。	・Cosmianのサービスを使用すると、各組織の秘密情報をアクセスすることなく、複数の組織間で秘密計算が可能になる。 ・同サービスにて、支店間で、スコアリングアルゴリズムの高度化が可能。	cosmian
ヘルスケア	突合、AI/予測、統計解析	安全な患者情報共有による病気の治療法開発支援	・COVID-19の治療方法探索のために、患者の性別、年齢、所在地等の個人情報を収集する必要があるが、プライバシー保護の関係で困難。	・MPC技術を使用することで、患者のデータを秘匿したまま、EMRデータの共有が可能。 ・データ提供者は、匿名化されたデータの匿名性が奪われることがないことを保証される。	Enya
ヘルスケア	突合、統計解析	安全な電子カルテ共有	・電子カルテには、患者の個人情報及び病歴情報が記録されており、必要に応じて患者の医療データの共有を可能にする。 ・電子カルテの情報を使って新しい治療法（ゲノム活用、等々）の開発が可能になる。 ・しかし、患者の情報は非公開情報なので、組織間での共有が困難。プライバシー保護の課題の解決が必要。	・MPC技術を使用することで、患者のデータを秘匿したまま、EMRデータの共有が可能。 ・データ提供者は、匿名化されたデータの匿名性が奪われることがないことを保証される。	BenhaUniversity他
官庁	突合、統計解析	勤労学生の卒業状況分析	・エストニアで、勤労学生と正規期間での卒業の相関関係を調査 ・分析のために、課税情報と就学情報の連携が必要。プライバシー保護の関係で両者の連携は困難。	・SharemindMPCシステム	Cybernetica
官庁	突合、AI/予測	複数の国間でのプラバシー保護データの分析	・政府の規制は、個人が認識できる情報(PII) を国間で共有することを禁じている。 ・企業間、国間でデータの共有が可能になれば、組織運営の効率が向上する。 ・組織間のデータ共有を阻害する要因は多数あります。	・米国のInpherは、XOR 秘密計算エンジンを使って、厳格にデータセキュリティを確保されている各国のデータの共有を可能にしている。	Inpher
官庁	突合、 統計解析、 スコアリング	効率的な脱税リスク分析	・エストニアでは、一部の悪意のある企業が売上高を申告しないために、一部の税収の徴収が困難になっている。	・SMPC技術を利用して解決を図る。 ・VAT申告書を３つに分解し、同社のリスクスコア算出のために分散計算を実行する。 ・計算結果を税務署と共有する	Cybernetica

付録B：ヒアリングコメントの概要

ヒアリングの概要

- ヒアリング方法
  - 各ヒアリング先と技術概要・利用例を説明し、適用可能性をヒアリング
    - ヒアリング時間：各ヒアリング先に対し1時間程度
    - ヒアリング実施時期：2021年8～11月

- 主なヒアリング先 (10数社 非公開)
  - 広告系事業者
  - 自動車関係事業者
  - 不動産関係事業者
  - その他

- ヒアリングのコメントは以下の2種類に集約
  - 広告・マーケティング系
  - スマートシティ（MaaS・自動車・不動産など）系

広告・マーケティング系のコメント概要(1/2)

- 個人情報の結合の活用例に関して
  - 同意率が低い問題は存在
    - 安全管理を契約で担保するのではなく、技術で担保する考え方
    - 導入コストとメリットのトレードオフがあり、特に広告効果は商品単価に依存
      （例：自動車や不動産は高単価）
  - 個人同意の不安感への対応が必要そうである
    - ①自分の個人情報が第三者提供される恐れ　→　秘密計算で担保可能
    - ②自分への広告からの気持ち悪さ　→　秘密計算で担保不可能
  - 秘密計算の技術以外の必要性もありそうである
    - 案：マーク制度　（安全な秘密計算を用いて、統計的に処理していることを監査）
    - 案：透明性の確保（広告の「i」ボタンのように、どのように分析・処理されているかを説明する）
- 個人情報に該当しないデータの結合の活用例に関して
  - IDFA(Identifier for Advertisers: 端末ID、個人関連情報(非個人情報))をキーにしたデータ結合分析があり得そう
    - 売上データ（非個人情報）を相互に開示しあって分析（例：TVのCMとオンライン広告のCMの視聴量を結合）
    - A企業とB企業とが連携すると良いという仮説を事前に検証（例：A商品とB商品の売上の相関）

広告・マーケティング系のコメント概要(2/2)

- 分析における現状と課題
  - まずは、自社内・企業グループ内でのデータ結合の段階である
  - 企業間でデータ流通できると考えていないため、活用例が考えられていないのが現状
    → ホワイトペーパーの発行により議論が進む
- 他の技術の比較も必要
  - 他技術の例：データフュージョン技術（データの統計的な傾向として結合する技術。共通の本人がいなくて良い）
  - 課題から秘密計算の適用箇所の整理が必要
- その他の活用例の案
  - 安全なデータアグリゲーター：家電製品の売れ筋を業界全体でランキング
  - 安全な国勢調査：秘密計算を用いて国勢調査データと結合分析
  - ポストクッキーにおける安全な分析：個人情報とクッキー情報とを紐付けないことを秘密計算で担保

スマートシティ（MaaS・自動車・不動産など）系のコメント概要

- MaaS領域における期待領域
  - 全般：ある地点に何人いるか、いたか、いそうか。移動の需要予測、過去の結果の取得。まずは、人の流れを見れるだけでも良い
  - 活用案①：複数事業者を跨いだフリーパス・サブスクの利用率に応じた料金分配（レベニューシェア）
    - フリーパス・サブスクでは利用実績の合算が必要だが、競合企業でもある他交通事業者に開示したくない
    - 秘密計算技術を利用して、利用実績の割合だけ計算できると良い
  - 活用案②：プローブデータなど個人を特定できてしまうデータへの活用
    - プローブデータから個人の自宅の推定などを防ぐために、匿名化技術や秘密計算が適する可能性
  - 活用案③：自宅や家族構成、年収、病歴等を加味した交通割引をデジタルで行う際の利用や秘匿した集計
    - 例えば、障害やひとり親等補助が出るが他者に見られたくない
- EV関係について
  - 活用案：EV充電設備の需要予測の活用
- 物流最適化について
  - 共同運行は必要である
  - 長距離輸送だけでなく短距離（自宅配送も）共同で行うことも良い
- 不動産関係について
  - 自社の利益と業界共通の利益の大きく2パターンが存在しそうである

この文書について

- 名称　秘密計算の活用例～ 秘密計算を利用した安全な組織間でのデータ活用への期待
- ファイル名　20230602-D-secure-computation-wp-application.pdf
- 掲載URL　https://data-society-alliance.org/survey-research/securecomputing/
- 概要

  この資料は、秘密計算による組織間でのデータ活用の可能性を多くの方に感じて頂くことを目的に、一般社団法人データ社会推進協議会(DSA)がとりまとめ公開するホワイトペーパーです。

- 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　2023年6月2日
  - 公開日　2023年6月2日
  - 作成アプリケーション　Microsoft PowerPoint
  - 公開形式　PDF
  - 公開ファイル容量　4,809KB
  - ページ数　46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/