

個人情報保護委員会 御中

安全なデータ活用のための プライバシー強化技術(PETs)の活用

2024年12月3日

3年ごと見直しの検討の充実に向けたヒアリング



PETs: Privacy Enhancing Technologies

※プラライバシーテック協会では、PETsはプラライバシーテックの別の呼び方であり、同様な技術として捉えています

- 個人情報保護委員会が示した「個人情報保護法のいわゆる3年ごと見直しの検討の充実に向けた視点」において、「個別の個人の権利利益への直接的な影響が想定されない個人データの利用に対する規律の考え方」、「個人データの第三者提供を原則として禁止する仕組みの妥当性」についても検討の視点が示されています
- プライバシーテック（PETs）は、データを適切に保護できる技術であり、これらの検討を進める上で、効果的かつ有用なものであると考えています
- 適切にPETsを用いて本人の権利利益を保護することを前提に、柔軟な利活用及び第三者提供を可能とすることで、権利利益を保護しながらデータ活用の推進が可能と考えます

PETs: Privacy Enhancing Technologies

※プライバシーテック協会では、PETsはプライバシーテックの別の呼び方であり、同様な技術として捉えています

目次

1. プライバシーテック協会の紹介
2. プライバシー強化技術(PETs)とは
3. 秘密計算とは
4. いわゆる 3 年ごと見直しに対する意見



1. プライバシーテック協会の紹介

プライバシーテック協会のご紹介

プライバシーテック協会の概要

基本情報

組織名 : プライバシーテック協会
 ホームページ : <https://privacytech-assoc.org/>

設立日

2022年8月24日

正会員

会長：高橋亮祐（株式会社Acompany 代表取締役CEO）
 理事：今林広樹（EAGLYS株式会社 代表取締役社長）
 中村龍矢（株式会社LayerX 事業部執行役員 AI・LLM事業部長）

賛助会員 特別会員

賛助会員：7社
 特別会員：2団体

アドバイザー

板倉陽一郎（ひかり総合法律事務所 パートナー弁護士）
 落合孝文（渥美坂井法律事務所 外国法共同事業 プロトタイプ政策研究所所長・シニアパートナー弁護士）
 安田孝美（名古屋大学 大学院情報学研究科 情報学部教授）
 坂下哲也（一般財団法人日本情報経済社会推進協会（JIPDEC） 常務理事）
 若目田光生（株式会社日本総合研究所、一般社団法人データ社会推進協議会 理事）
 須崎有康（情報セキュリティ大学院大学 教授）



当協会の活動に賛同する7企業に参画頂いています



第1期賛助会員として 7社が加盟しました



Hakuhodo DY holdings



dentsu
tokyo / osaka / nagoya

TOPPAN

Deloitte.
デロイトトーマツ

Orchestrating a brighter world
NEC

プライバシーテック協会のご紹介

当協会と密に連携している2団体に参画頂いています



特別会員として
2団体が加盟しました



2. プライバシー強化技術(PETs)とは

PETsへの期待

- 秘密計算やPETsは、「デジタル・ニッポン 2024」にて、我が国の国民生活や経済社会の発展に大きく貢献する可能性のある技術として期待されている

「デジタル・ニッポン 2024」(自由民主党)からの引用

6.4 制度見直しの在り方

(1)「三年ごと見直し」

令和2年改正個人情報保護法の附則には「三年ごとの見直し」が規定されており、(略)

この間、生成AIも含め、データを取り扱う技術が急速に発展した一方で、**個人データを安全に扱うためのプライバシー強化技術(PETs¹⁵)も登場してきた**。例えば、**秘密計算は**、個人情報を秘匿したまま統計処理を行うことができる。このような新技術は、**ビジネスと制度の対立関係を解消し、我が国の国民生活や経済社会の発展に大きく貢献する可能性のある、まさにディスラプティブな技術**であって、個人情報保護制度は、その開発と実装の妨げになってはならない。ビジネスの現場と技術動向への理解なしには、豊かな社会は実現しない。

—————
¹⁵ Privacy Enhancing Technologies:データを取り扱う際に、個人データの利用を最小化したり、データセキュリティを強化したりすることにより、当該データの効用を失わせることなく、プライバシー保護を実現させる技術。

統計化と暗号化の違い

- 現行制度では、統計化と暗号化では扱いが大きく異なる
- PETsは暗号化と見なされる可能性があり、プライバシー保護に資するにもかかわらず積極的に導入するインセンティブがない

統計化

- 特定の個人を識別できないようにすれば個人情報ではなくなるという整理
- 個人情報ではないので、同意なく第三者提供も可能
- 個人情報から統計情報を作り出すことも個人情報の処理とはみなされていない

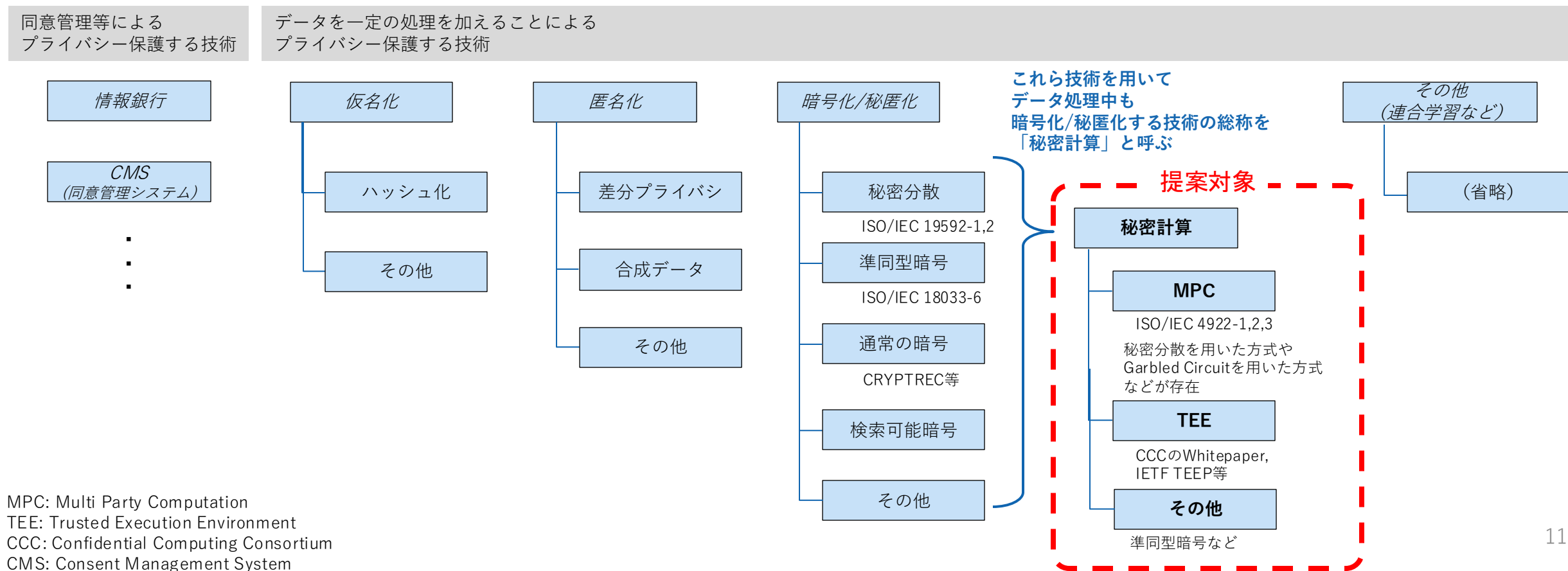
暗号化

- 実質的には特定の個人を識別できないが、個人情報のままと見なされる
- 第三者提供の同意も必要

代表的なPETsの例と今回の提案の範囲

- PETsは、プライバシーを保護したデータ活用に資する技術であり、様々な技術が存在
- 「秘密計算」は、秘匿化しながら処理できる技術であり、利活用と保護の両立が可能な技術
- 適切に「秘密計算」を用いて本人の権利利益の侵害が防げる場合には、同意なく利用・提供ができるように検討いただきたい

図：主なPETsの類型



参考：海外ガイドライン記載のPETs

- 秘密計算は、主な海外公的機関のPETsガイドラインに記載され、注目されている技術である

表：海外公的機関のガイドライン等が対象としているPETs※2

技術※1		(1) OECD PETs ガイドライン	(2) 英国ICO PETsガイドライン	(3) 米国 PPDSA 戦略	(4) UN(国際連合) PETsガイドライン	(5) CIPL(国際法・公法研究所) PETsガイドライン
データ 難読化 技術	匿名化、仮名化	○		○		○
	合成データ	○	○	○	○	○
	差分プライバシー	○	○	○	○	○
	ゼロ知識証明	○	○	○	○	○
暗号化し たままの 処理技術 (秘密計 算)	MPC (秘密分散などを用いた秘密計算)	○	○	○	○	○
	準同型暗号 (準同型暗号を用いた秘密計算)	○	○	○	○	○
	TEE (TEEを用いた秘密計算)	○	○	○	○	○
連合・分 散分析 技術	連合学習	○	○	○	○	○
	Distributed Analytics	○				
アカウン タビリテ ィ技術	Accountable System	○				
	Threshold Secret Sharing	○				
	Personal Data Store (情報銀行)	○				

PPDSA : Privacy Preserving Data Sharing and Analytics
MPC: Multi Party Computation
TEE: Trusted Execution Environment

※1 「OECD PETsガイドライン」の記載内容を簡易的に日本語訳して記載
※2 主な海外公的機関のPETsガイドラインについては後半のスライドで説明

参考：PETsの概要と参考文献

- 主要なPETsは、公的機関等が発行しているガイドラインや標準文書等で定義されている
- ただし、技術が急激に進化しているため、必ずしも国際標準になっていない技術も議論対象とするべき
(例：TEEはグローバルで普及が進み、大企業(Apple、Google等)も導入し、現在は国際的な民間団体での標準が出来ている)

表：主なPETsと標準等の文献

技術	概要	主な標準等の文献
秘密計算	データを暗号化・秘匿したまま処理する技術の総称	「秘密計算」は、日本語では「秘匿計算」、英語ではSecure Computationなどとも呼ばれるが、標準文章としての定義は存在しない。「秘密計算」は総称であり、具体的にはMPCやTEEなどが該当する。
MPC(Multi-Party Computation)	複数の組織がそれぞれ保有する秘匿データを、秘匿しながら結合・計算技術	- ISO/IEC 4922-1:2023 Information security — Secure multiparty computation Part 1: General https://www.iso.org/standard/80508.html MPCの概念定義、用語定義、安全性の軸の定義 - ISO/IEC 4922-2:2024 Information security — Secure multiparty computation Part 2: Mechanisms based on secret sharing https://www.iso.org/standard/80514.html MPCのひとつの実現方式である秘密分散を用いた方式を定義。(MPCの実現方式としては、Garbled circuitを用いた方式も存在する https://www.iso.org/standard/87557.html)
TEE (Trusted Execution Environment)	ハードウェアのチップにて秘匿しながら処理	- CCC(Confidential Computing Consortium)という民間企業 (Intel、NVIDIA等参加) が参加するコンソーシアムによって標準策定済み https://confidentialcomputing.io/resources/white-papers-reports/. 「Common Terminology for Confidential Computing」 - その他、GlobalPlatformやIETF TEEPなど
秘密分散	データを複数の分割することによる秘匿化方法	- ISO/IEC 19592-1:2016 Information technology — Security techniques — Secret sharing Part 1: General https://www.iso.org/standard/65422.html - ISO/IEC 19592-2:2017 Information technology — Security techniques — Secret sharing Part 2: Fundamental mechanisms https://www.iso.org/standard/65425.html - NISC「政府機関等のサイバーセキュリティ対策のための統一基準群」にも記載
準同型暗号	データを暗号化したまま処理が可能な特殊な暗号方式	ISO/IEC 18033-6:2019 IT Security techniques — Encryption algorithms Part 6: Homomorphic encryption https://www.iso.org/standard/67740.html など
従来の暗号技術	いわゆる通常の暗号技術	CRYPTREC暗号リスト(電子政府推奨暗号リスト) https://www.cryptrec.go.jp/list.html
匿名化(k-匿名化)	属性による識別がkレコード以上に加工	PPC事務局レポート https://www.ppc.go.jp/files/pdf/report_office_seido2205.pdf 4.2.3.1.1 k-匿名性について
差分プライバシー	複数の集計結果(統計情報)の組み合わせからの個人特定の恐れを防ぐため、集計結果にノイズを付加する	NIST SP 800-226 https://csrc.nist.gov/pubs/sp/800/226/ip

3. 秘密計算とは

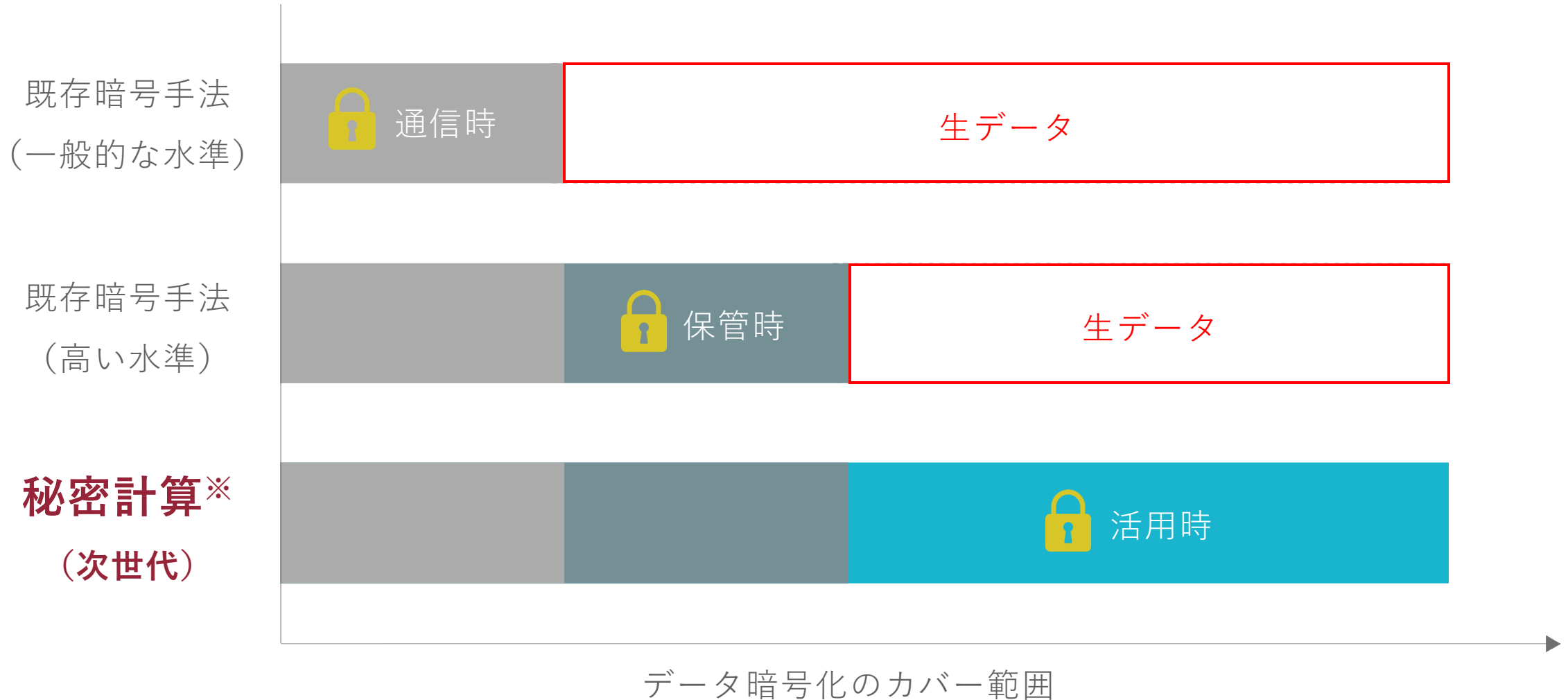
秘密計算とは

- 秘密計算とは、計算過程を暗号化・秘匿化したまま処理する技術の総称



秘密計算と従来暗号の比較

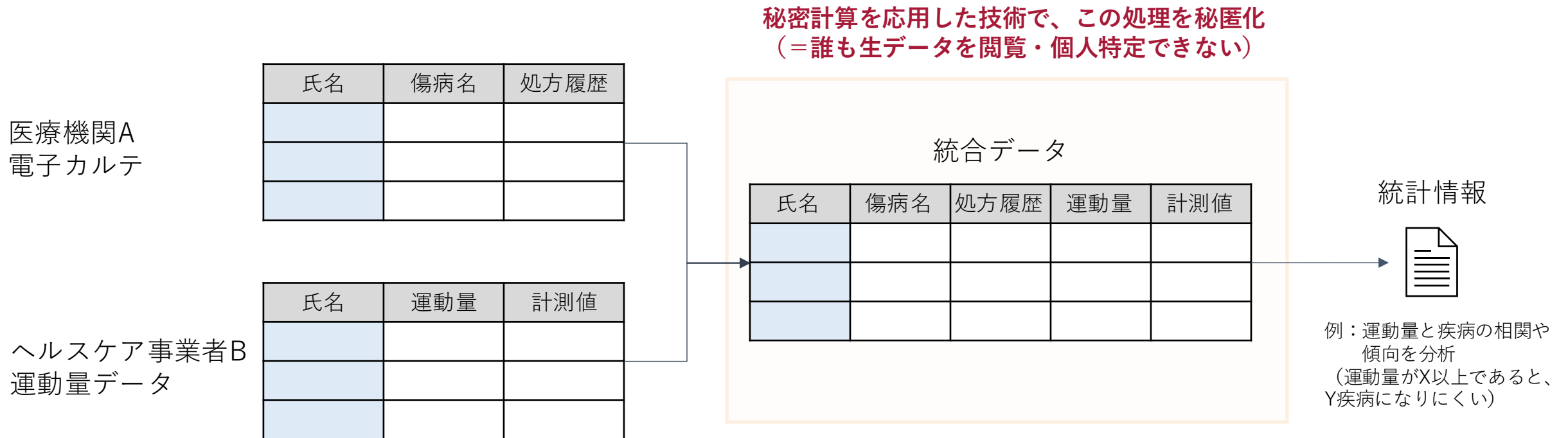
- 秘密計算を用いることで暗号化・秘匿化したままのデータ活用が可能



※ 秘密計算と従来の暗号技術を組み合わせる事によって、通信時・保管時だけでなく、活用時も暗号化・秘匿化を実現

秘密計算の利用例

- 計算過程が暗号化/秘匿化されることで、相互の組織のデータがわからない状態で分析可能



※ **次世代医療基盤法は医療情報に限定される**ため、有効な分析が限定される

(例：ヘルスケア事業者がもつ運動量情報や自治体が持つ要介護度の情報などは対象外)

※ 希少疾患の患者数は少ないため、データを**突合前に属性をk-匿名化などして曖昧化すると、分析精度が大きく低下**するため、統合前の属性の曖昧化は好ましくない

秘密計算への期待

● 日本の成長に不可欠なデータ連携に有用であり、また、国内企業に優位性あり

- AIの時代では学習データが重要であるため、海外BigTech企業はデータを囲い込み
- 日本は事業者間データ連携が成長に不可欠

- 秘密計算（MPC）は日本企業が強みを持ち、関係するISO規格の策定をNTTが主導
- ソリューション構築も世界を主導できる可能性

I. はじめに — なぜデータ利活用・連携か —

データ利活用・連携の目的は何か。経団連はかねて、Society 5.0 for SDGs を実現するうえでDXの推進が不可欠であり、単なる電子化や効率化にとどまらずビジネスモデルを含めた変革が必要であること、そのためにデータ利活用が死活的に重要であることを訴えてきた¹。

データをデジタル技術と組み合わせることによって、新たな価値の創造が可能となる。そのため、各国・地域やプラットフォームは、データを一元的に掌握することで競争力の源泉としている。他方、わが国が目指すべきはデータの一極集中ではなく、日本型の協創DX²、すなわち多様な主体による生活者価値の創造である。そのためには、企業を含めあらゆるステークホルダーによるデータ連携が各分野において欠かせない。

出典：
経団連，“データ利活用・連携による新たな価値創造に向けて - 日本型協創DXのリススタート -”，
2023年5月16日 https://www.keidanren.or.jp/policy/2023/034_honbun.pdf#page=4



[NTTグループについて](#)
[ニュース](#)
[事業案内](#)
[株主・投資家情報](#)
[研究開発](#)
[災害対策](#)
[サステナビリティ](#)
[会社案内](#)
[採用情報](#)

[トップページ](#) / [ニュースリリース](#) / NTTが規格作成を主導した初の「秘密計算技術」ISO国際標準が発行～データ利活用とプライバシー保護を両立する先進テクノロジーの普及を推進～

2023年9月15日

日本電信電話株式会社

NTTが規格作成を主導した初の「秘密計算技術」ISO国際標準が発行～データ利活用とプライバシー保護を両立する先進テクノロジーの普及を推進～

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：島田 明、以下「NTT」）が長年研究開発を行い標準化活動を推進し主導してきた、データを暗号化したままで処理ができる秘密計算技術について、初の標準規格『ISO/IEC 4922-1:2023』が国際標準化機構（International Organization for Standardization、以下ISO）から発行されました^[1]。

今回の規格化により、世界中の秘密計算技術の開発者や利用者の秘密計算技術についての認識を一致させ相互理解を深めて、技術開発や技術活用を正確かつ容易に行うことができるようになります。ユーザーにとっては、本規格に準拠し開発されたものであれば、安心して使うことが出来るようになります。

本標準をベースに、秘密分散技術を利用した秘密計算を規定する、ISO/IEC 4922-2も規格化の最終段階に入っており、NTTは引き続き秘密計算技術の標準化に貢献していきます。

1. 背景

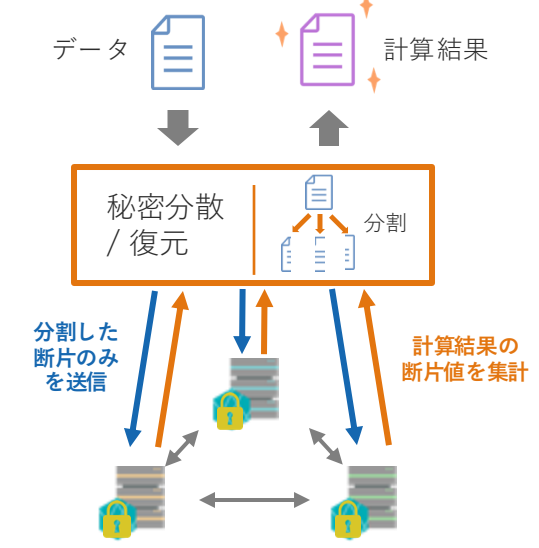
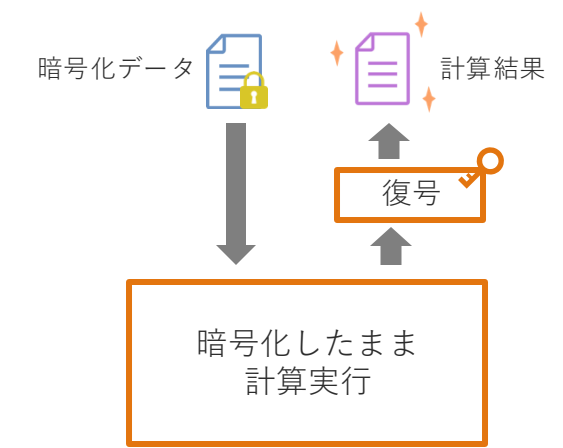
昨今、データに基づく意思決定の広がりや分野横断的なサプライチェーンの最適化などのため、様々なデータを共有し多分野での利活用を図る機運が高まっています。しかし、個人のプライバシーに関わるデータや企業運営、営業秘密に関わるデータなどは、情報漏洩や不正利用の懸念もあるためデータの共有がはばかられ利活用が進んでいない現状があります。その解決策として注目されているのが、データを暗号化したまま一度も元に戻さず処理ができる秘密計算技術です。Gartner社が発行する先進テクノロジーの普及度やトレンド推移を示す

出典：
NTT, プレスリリース, 2023年9月15日,
<https://group.ntt.jp/newsrelease/2023/09/15/230915a.html>

MPC：Multi-Party Computation
（秘密計算の一種）

● データを秘匿しながら処理できる総称である「秘密計算」には様々な方式が存在

「秘密計算」の各種方式の概要※1

TEE (Trusted Execution Environment)	MPC (Multi Party Computation)		その他 (例：準同型暗号など)
	秘密分散を用いた方式	その他の方式	
ハードウェアのチップにて 秘匿しながら処理 	データを分割して秘密分散値として 秘匿化し、秘匿化したまま処理 	Garbled Circuit を用いた 方式など	データを暗号化したまま処理 

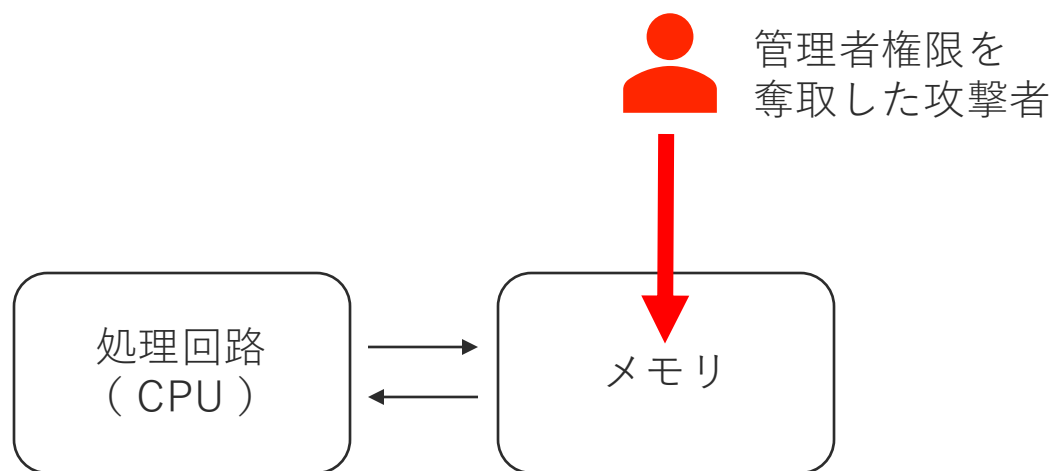
※1: 「秘密計算」というデータを秘匿しながら処理できる技術として、現在ある程度広く利用されている技術としては、TEEやMPCや準同型暗号等が該当

秘密計算の技術的安全性 TEEの例

- TEEとは、ハードウェアレベルで安全な、秘匿化したまま処理できる環境のこと
- 仮に管理者権限を取られたとしても、メモリ内のデータの閲覧は不可

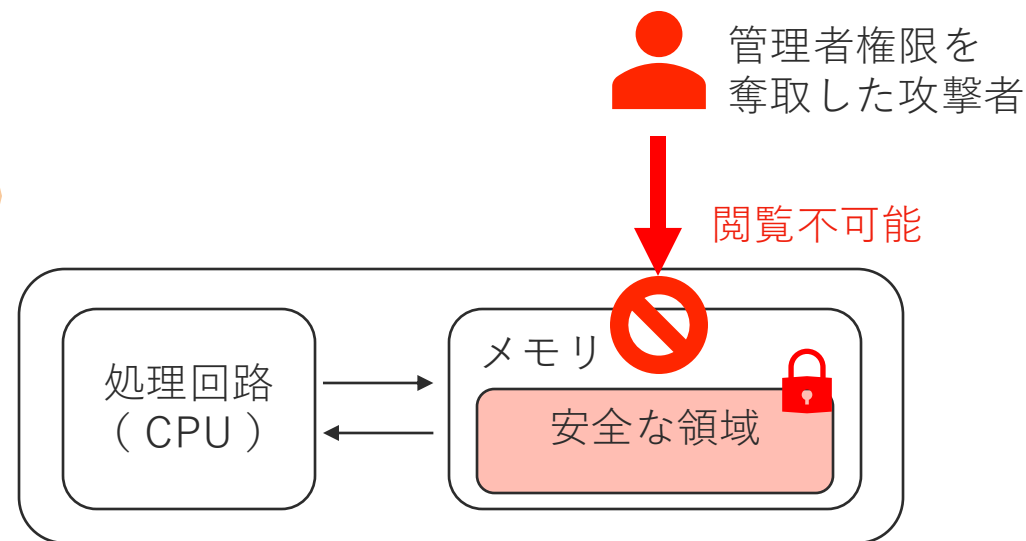
TEEなしのシステム

管理者権限があると
処理途中の**メモリ内のデータ**を閲覧可能



TEEありのシステム

管理者権限をとられても
処理途中の**メモリ内のデータ**は閲覧不可



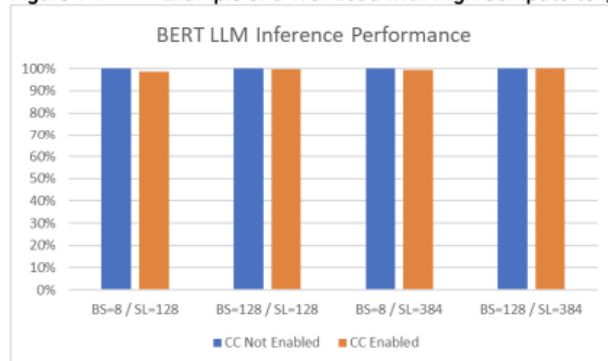
※TEEを用いた処理を「コンフィデンシャル・コンピューティング」と呼びます

参考：TEEのAI処理への適用

- GPUでもTEEがサポートされ、AI処理向けの「秘密計算」としてTEEが注目
- 海外テック企業を中心に導入が急速に進んでいる

NVIDIAのH100でのAI推論と学習の処理時間の比較の例

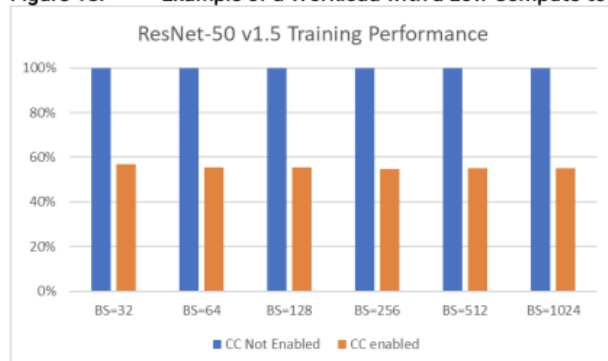
Figure 14. Example of a Workload with High Compute to I/O Ratio



推論処理は、
ほぼ同じ処理時間

BS is the batch size, and SL is the sequence length.

Figure 15. Example of a Workload with a Low Compute to I/O Ratio

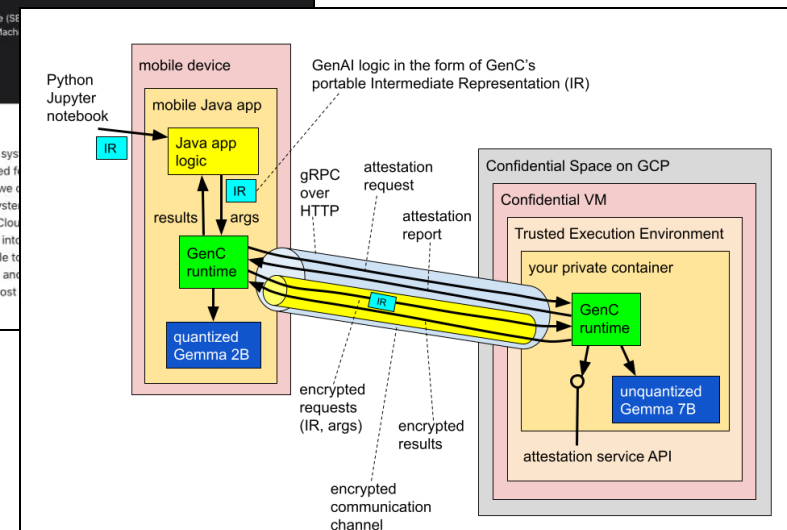
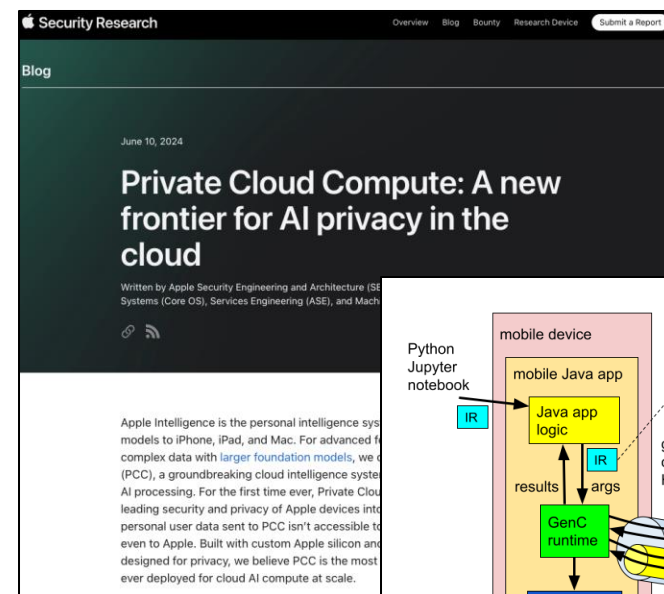


学習処理は、
50%程度の速度劣化

BS is the batch size.

出典：
“Confidential Compute on NVIDIA Hopper H100”, NVIDIA,
<https://images.nvidia.com/aem-dam/en-zz/Solutions/data-center/HCC-Whitepaper-v1.0.pdf>

AppleやGoogleはTEEを生成AI処理に適用



出典：

<https://security.apple.com/blog/private-cloud-compute/>
<https://developers.googleblog.com/ja/enabling-more-private-gen-ai/>

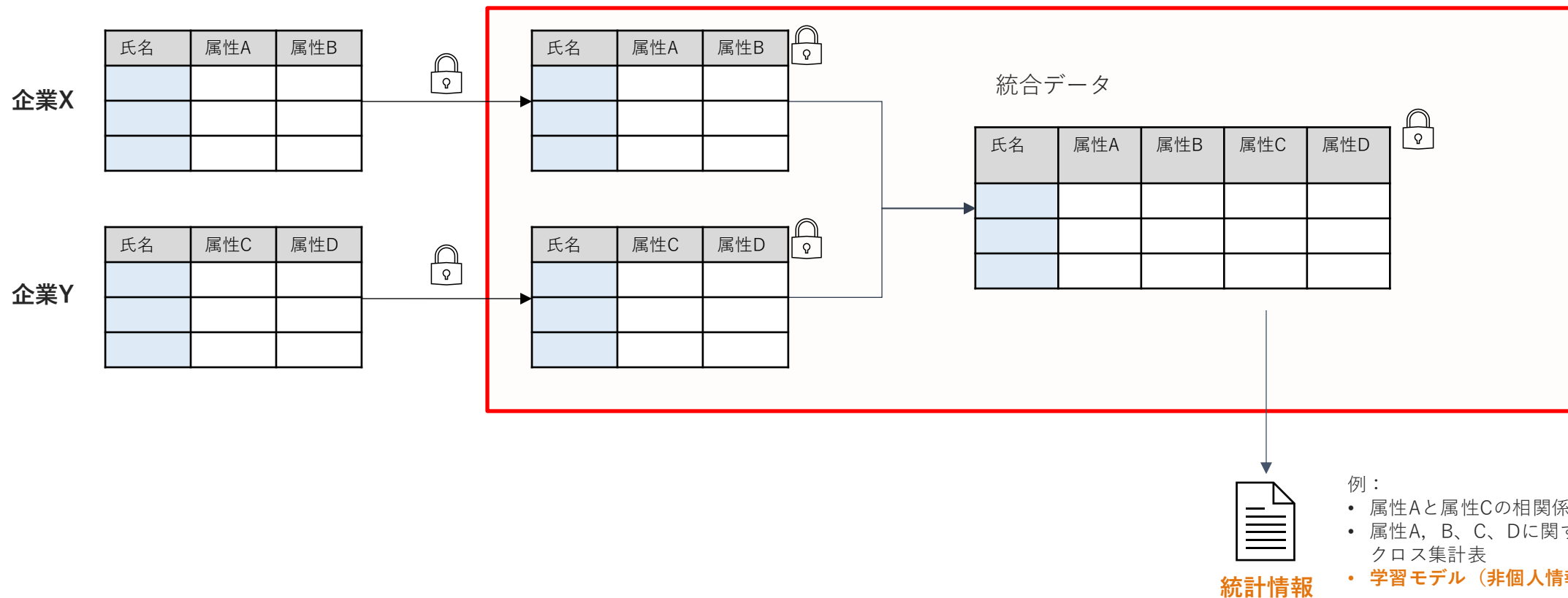
※ AppleはSecure EnclaveというTEEの一種を生成AIの処理に適用。Googleは技術BlogにてTEE利用を言及

4. いわゆる 3 年ごと見直しに対する意見

秘密計算を用いてデータを統合し、統計情報を生成する場合は同意の対象外としていただきたい

- ①適切に秘密計算を用いて統合データやデータ処理の過程を秘匿化する
- ②アウトプットは統計情報とする
- これら2つの条件を満たす場合は、複数の組織が保有する個人データを突合する行為に対して同意不要としていただきたい

秘密計算を用いて処理し、出力は「統計情報」



「個人情報保護法のいわゆる 3 年ごと見直しの検討の充実に向けた視点」に対する意見

- 統計的利用や一般的・汎用的な分析を行うことに限定される場合は、権利利益の保護が図られていると考える
- ただし、統計的利用や一般的・汎用的な分析を行うことが担保されることが大前提である
- この前提を担保する方法として、秘密計算などのPETsは、合理的かつ効果的な方法
- また、技術的な担保により、人の関与を極力低減することで、人為的ミスや悪意ある者からの保護も実現でき、積極的に推奨すべきものとする

2 個別の個人の権利利益への直接的な影響が想定されない個人データの利用に対する規律の考え方

本人の関与を通じた利用の適正性担保の仕組みは、その利用の結果本人の権利利益への影響が具体的に見込まれる場合に必要とされるのではないか。例えば、**統計的利用など**、一般的・汎用的な分析結果の獲得と利用のみを目的とする場合には、**本人の関与を通じて適正な利用を確保するという仕組みは求められるか**（なお、1⑧の見地から、本人の関与を権利として認める立場はあり得るが、適正な取扱いを担保する上での本人関与の機能とは趣旨を異にすることに留意。）。

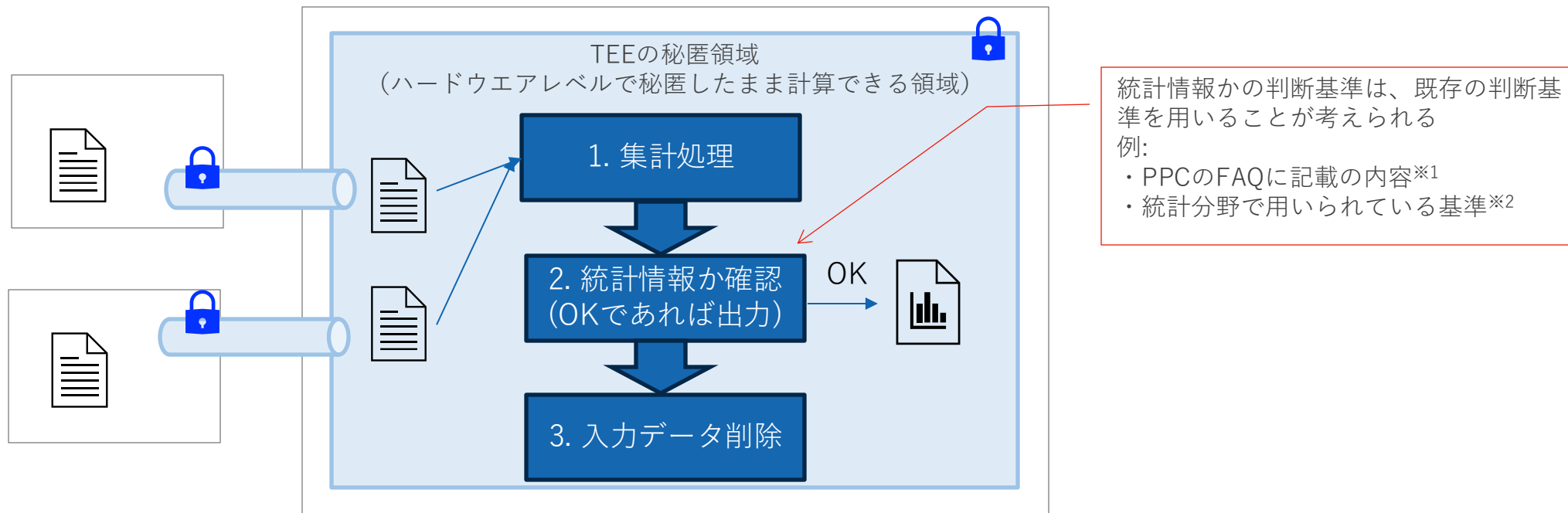
3 個人データの第三者提供を原則として禁止する仕組みの妥当性

個人情報取扱事業者に対して本人が関与・監視することを通じた利用の適正性担保の仕組みを前提とすることから、本人の関与が著しく困難になる第三者提供を原則として禁止している。一方、その**提供先における利用目的が特定の個人への影響を伴わない一般的・汎用的な分析に限定**されるなど本人の関与を通じた規律によらない規律を導入することに合理性がある場合や、本人にとって、提供時の認識に照らし、当該第三者に対する提供を当然のものと思うなど躊躇するとは想定されない場合、さらには、利用目的の継承などを通じ、当該第三者への提供後も、**提供前と同等に本人の権利利益の保護が図られる状態が保証される場合**など、第三者提供を禁止する必要のない類型はあるか。

参考：出力が統計情報となることの技術的な担保方法

- 例えば、秘密計算の一例であるTEEには、事前登録されている処理プログラムが確実に実行されていることを確認する機能※3が存在
- この機能を用いて、統計情報であるかをチェックするプログラムが実行されていることを確認することで、統計情報のみが出力されることを担保可能（統計情報に該当する情報の出力を抑制可能）
- さらに、分析に用いたデータを復号することなく処理後に確実に削除することで、過度にデータが蓄積・統合されることを防ぎ、プライバシーリスクの低減につながる

図：秘密計算（TEE）を用いた統計情報か確認するプログラムの確実な実行



※1 https://www.ppc.go.jp/all_faq_index/faq1-q15-2/ 「統計情報は、複数人の情報から共通要素に係る項目を抽出して同じ分類ごとに集計等して得られる情報であり、一般に、特定の個人との対応関係が排斥されているため、「個人情報」に該当しないもの」

※2 https://www.e-stat.go.jp/microdata/sites/default/files/share/data-use/video/03_video.pdf

※3 Remote Attestation機能と呼ばれる機能。付録に機能概要を記載。

PETs普及を急ぐ必要がある理由①：委託先での個人情報の漏洩事故の多発

- 委託先等での人為的・技術的な理由による個人情報の漏えい事故は後を絶たず、従来よりも安全性が高い秘密計算などのPETsの導入が望まれる

表：委託先での個人情報の漏洩事故の例

事例の概要	件数	時期
複数の企業・自治体のコールセンター業務の委託/再委託を受けていた企業の元派遣社員が、顧客情報を不正に持ち出し	約900万件	2023年12月
通信事業者の委託先の元派遣社員が、顧客情報を不正に持ち出し	約600万件	2023年7月
保険事業者の委託先のサーバが不正アクセスを受け、顧客情報が流出	約100万件	2023年1月
保健事業者の委託先のサーバの不適切なセキュリティ対策により、顧客情報が流出	約70万件	2023年1月

※事例はニュース等を参考に調査した内容を記載（企業名等は意図的に伏せている）

PETs普及を急ぐ必要がある理由②：海外では既にPETsの導入が活発化

- PETsは安全なデータ活用に有用なため、海外公的機関は昨年相次いでガイドライン等を発行し、導入を加速
- PETsの導入はグローバル動向を踏まえても、導入推奨をしていくべきである

本文書における略称	タイトル	概要	発行時期
OECD PETs ガイドライン	Emerging privacy-enhancing technologies Current regulatory and policy approaches	OECDが発行しているPETsの利用促進に向けたガイドライン	2023年3月
英国ICO PETs ガイドライン	Privacy-enhancing technologies (PETs)	英国ICOが発行しているPETsの利用促進に向けたガイドライン	2023年6月
米国 PPDSA 戦略	NATIONAL STRATEGY TO ADVANCE PRIVACY-PRESERVING DATA SHARING AND ANALYTICS	PETsを用いた安全なデータ分析（PPDSA: Privacy Preserving Data Sharing and Analytics）に関する米国の国家戦略文章	2023年3月
UN(国際連合) PETs ガイドライン	THE PET GUIDE THE UNITED NATIONS GUIDE ON PRIVACY-ENHANCING TECHNOLOGIES FOR OFFICIAL STATISTICS	UN(国連)が発行している公的統計におけるPETsの利用促進に向けたガイドライン	2023年
CIPL(国際法・公法 研究所) PETsガイドライン	Privacy-Enhancing and Privacy-Preserving Technologies: Understanding the Role of PETs and PPTs in the Digital Age	CIPLが発行しているPETsの利用促進に向けたガイドライン	2023年12月

- 1.OECD PETs https://www.oecd.org/en/publications/emerging-privacy-enhancing-technologies_bf121be4-en.html
- 2.ICO PETs <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/>
- 3.US PPDSA <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf>
- 4.UN PETs https://unstats.un.org/bigdata/task-teams/privacy/guide/2023_UN%20PET%20Guide.pdf
- 5.CIPL PETs <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf>

なお、個人情報保護委員会のページにて公開されている「欧米主要国におけるプライバシー強化技術（PETs）の利用に関する法制度に関する調査」は、調査時期が令和4年度（2022年度）（調査結果は2023年3月発行）である。https://www.ppc.go.jp/files/pdf/R503_pets_houseido_report.pdf

PETs普及を急ぐ必要がある理由③：グローバル競争力と経済安全保障

- 国内企業は秘密計算（TEE）の技術開発を進めているが、国内市場への適用は遅く、海外展開も弱い
 - 一方海外では、クラウドでの秘密計算（TEE）適用や国防領域への適用が急速に進んでいる
- ⇒ 秘密計算・PETs導入促進は、グローバル競争力確保や技術の国内保有（経済安全保障）の観点で急務

海外の防衛領域への秘密計算（TEE）の導入動向

- 米国スタートアップのEnveil社は、米国陸軍に秘密計算（TEE）のAI処理基盤を提供（2024年7月）※1
- 米国スタートアップのAnjuna社とNVIDIAは、米国海軍にGPUの秘密計算（TEE）を提供（2024年5月）※2
- Anjuna社（CEOはイスラエル出身）は、イスラエル国防省に秘密計算（TEE）の処理基板を提供（2022年2月）※3

※1 <https://www.enveil.com/enveil-wins-army-linchpin-contract-for-secure-ai/>

※2 <https://blogs.nvidia.com/blog/rsa-2024-ai-cybersecurity/>

※3 <https://www.anjuna.io/press/israels-ministry-of-defense-selects-anjuna-security-software-to-lockdown-sensitive-data-in-public-clouds>

クラウドにおける秘密計算サービスに日本企業は無い

■ Microsoftのクラウド（Azure）における秘密計算（TEE）のサービスのリスト※4

- Anjuna（米国）
- BeeKeeperAI（米国）
- Decentriq（スイス）
- Edgeless Systems（ドイツ）
- Enclave System（ドイツ）
- Fortanix（米国）
- Habu（米国）
- Mithril Security（フランス）
- Opaque Systems（米国）
- SCONE（ドイツ）

※4 <https://learn.microsoft.com/en-us/azure/confidential-computing/partner-pages/partner-pages-index>

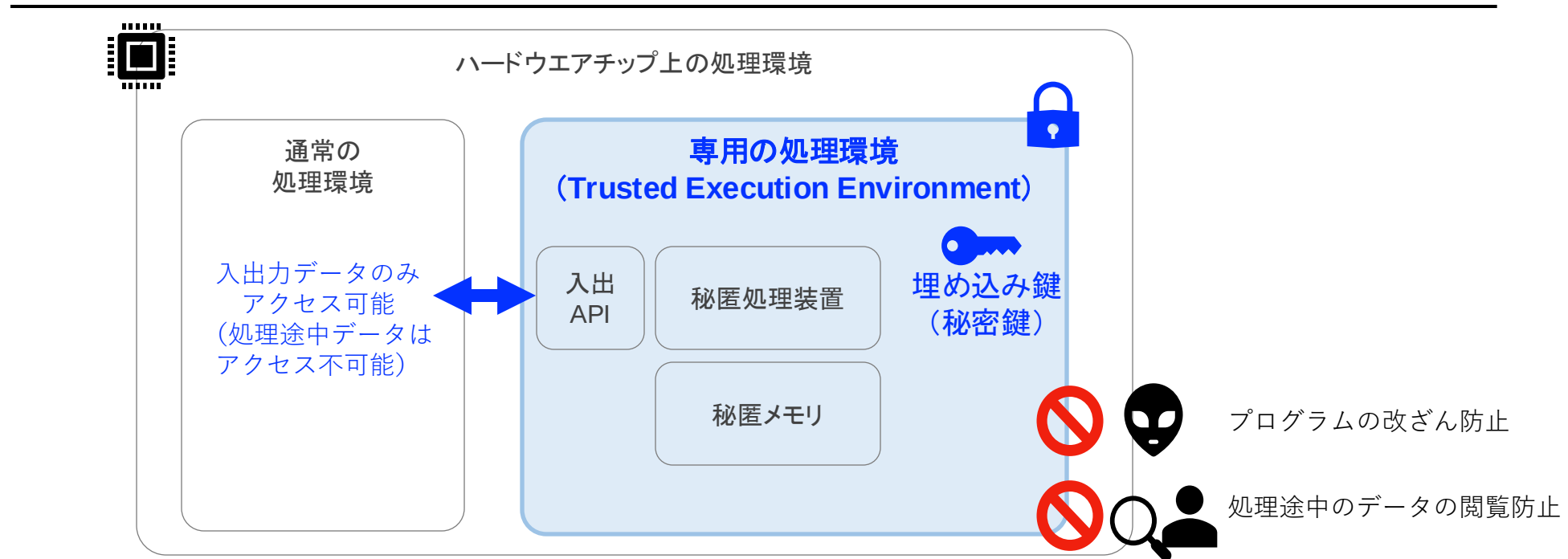


付録：秘密計算(TEE)を用いたデータ連携分析の詳細

TEE(Trusted Execution Environment)とは

- TEEとは、ハードウェアレベルで安全な秘匿化したまま処理できる環境のこと
- ハードウェアの製造段階で秘密鍵が埋め込まれ※1、設計上は鍵が漏洩しないため、TEE内のデータはそもそもアクセスが困難である上に、仮にアクセスできても秘匿化されているため、グローバルで安全性が評価され、普及しつつある※2

図: TEEの安全な実行環境の概要



※1 TEEの一種であるIntel SGXでは、「Root Seal Key」「Root Provisioning Key」と呼ばれる。「Root Seal Key」はチップ製造者のIntelが埋め込むが、データはIntelも知り得ないとしている。チップ製造者を一定レベル信頼している前提となる。
<https://qiita.com/Clifford/items/19145f6fa0340013f94f>

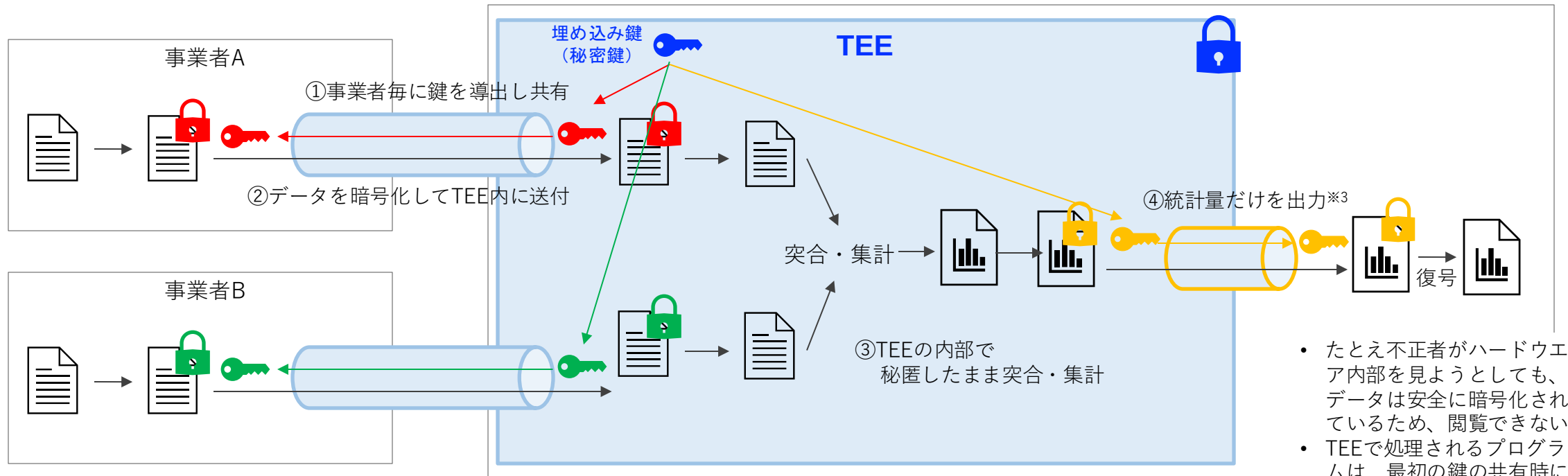
※2 TEE(≒Secure Enclave)はAppleも採用し、端末の個人データをクラウドで安全に処理する際に適用
<https://security.apple.com/blog/private-cloud-compute/>

TEEを用いた個人特定されずに突合・集計する方法の例

- TEE内の秘密鍵をもとに事業者毎に通信用に一時的な鍵を作成・共有し、その鍵で各事業者が持つ個人データを暗号化してTEEの秘匿処理領域に送信※1

→ TEE内に安全にデータ集めることができ、その後はTEEで秘匿した状態で突合・集計し、統計量のみ開示

図: TEEを用いた個人特定を防いだデータ突合・集計の例（概念図）



※1 Intel SGXでの事業者間での鍵交換の例：<https://qiita.com/Clifford/items/095b1df450583b4803f2>

鍵の生成や共有は設計思想に依存し、この図では一例として記載している。

また、わかりやすさを優先し概念的な記載をしているため、技術的には一部不正確な記載となっている。

※2 鍵共有時にTEEのRemote Attestation機能（付録に詳細記載）を利用し、TEEで実行するアプリケーションのプログラムが事前に登録しているプログラムと一致しているか（改ざんされていないか）をハードウェアの機能を用いて検証可能

※3 統計量だけが出力されるような制限が入った集計処理のプログラムを実行することで、統計量のみが出力されるように制御可能

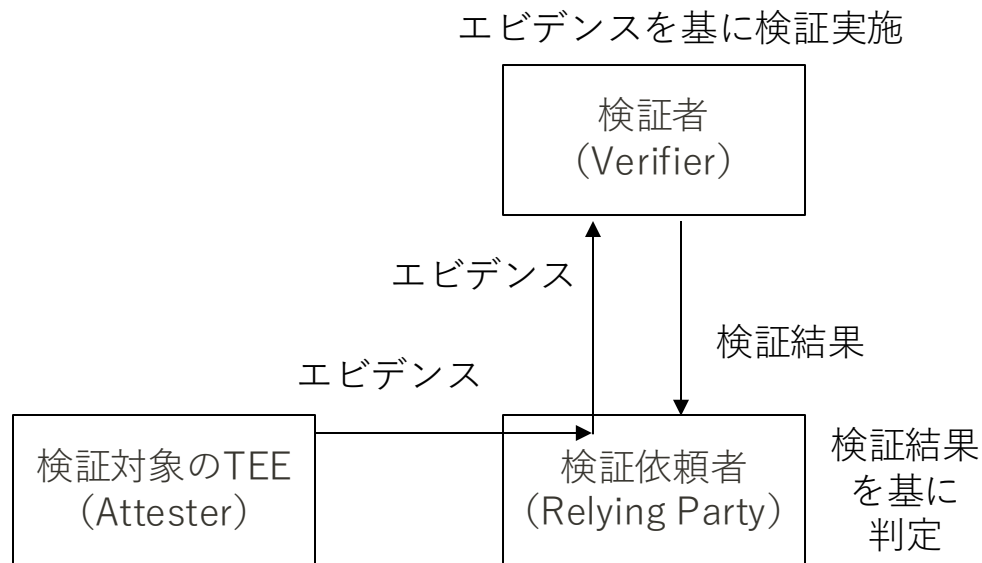
- たとえ不正者がハードウェア内部を見ようとしても、データは安全に暗号化されているため、閲覧できない
- TEEで処理されるプログラムは、最初の鍵の共有時にチェックが行われ、不正な改ざんを防止※2

TEEのRemote Attestationとは

- TEE(Trusted Execution Environment)のRemote Attestationという技術を用いることで、事前に登録したプログラムが確実に実行されていることを外部から検証が可能

図：Remote Attestationの方式の一例

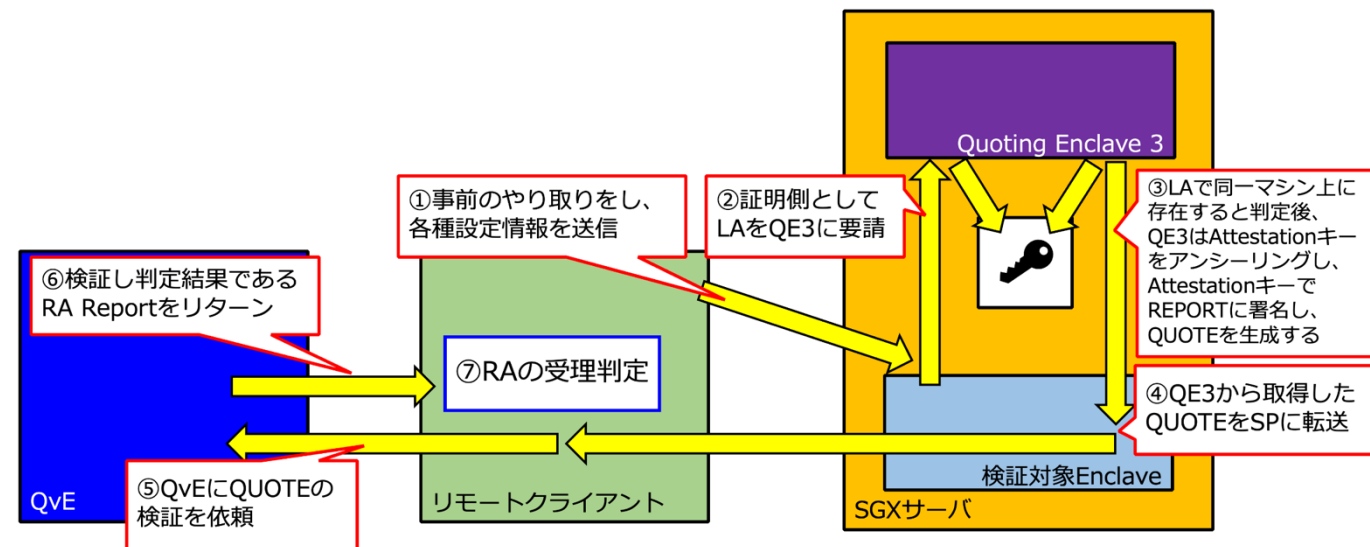
- 検証対象（TEE）からエビデンス（実行されるプログラムの情報等）を得て、不正が無いかを検証
- 実行プログラムが改ざんされていないかの確認が可能



出典：”Remote ATtestation procedureS (RATS) Architecture” RFC 9334の Background-Check Modelの図を参考に作成

図：TEEの一例であるIntel SGXの例

TEEの一種であるIntel SGXでは、Intel社が提供する検証用のサービスを利用して、Remote Attestationを実施



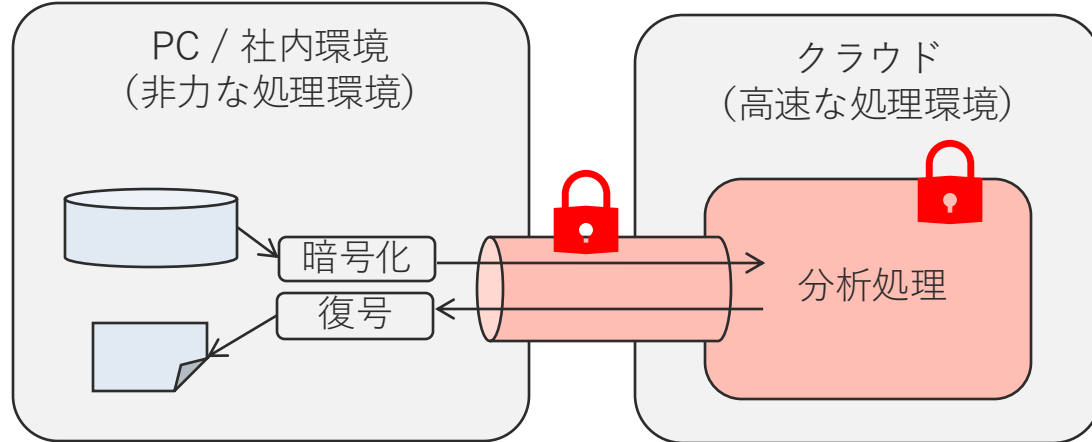
出典：<https://acompany.tech/privacytechlab/intel-sgx-dcap-ra>

秘密計算を用いた活用例

- 秘密計算を用いることで、データを秘匿化したままの処理が可能であり、組織間で相互にデータをしたままの結合分析を実現

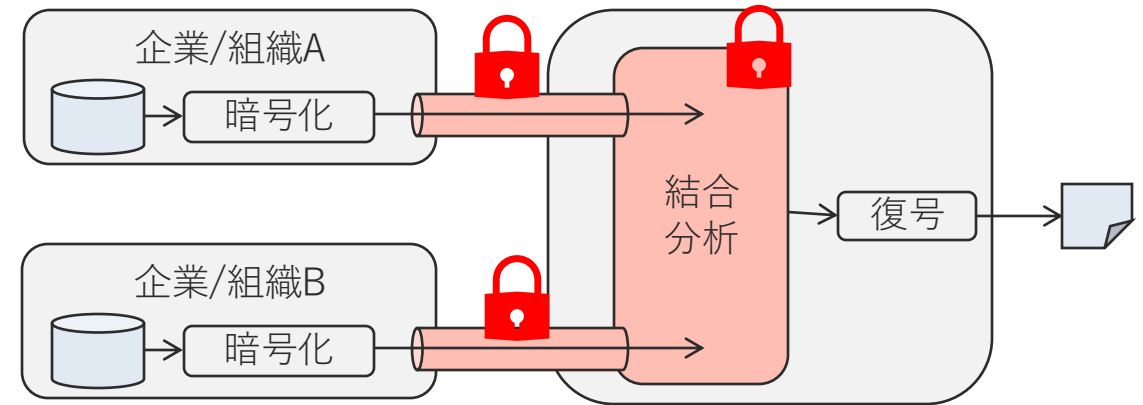
1. クラウドでの安全確保

クラウドでデータを秘匿しながら処理



2. 組織間データ連携での安全確保

組織間でデータを秘匿しながら結合分析





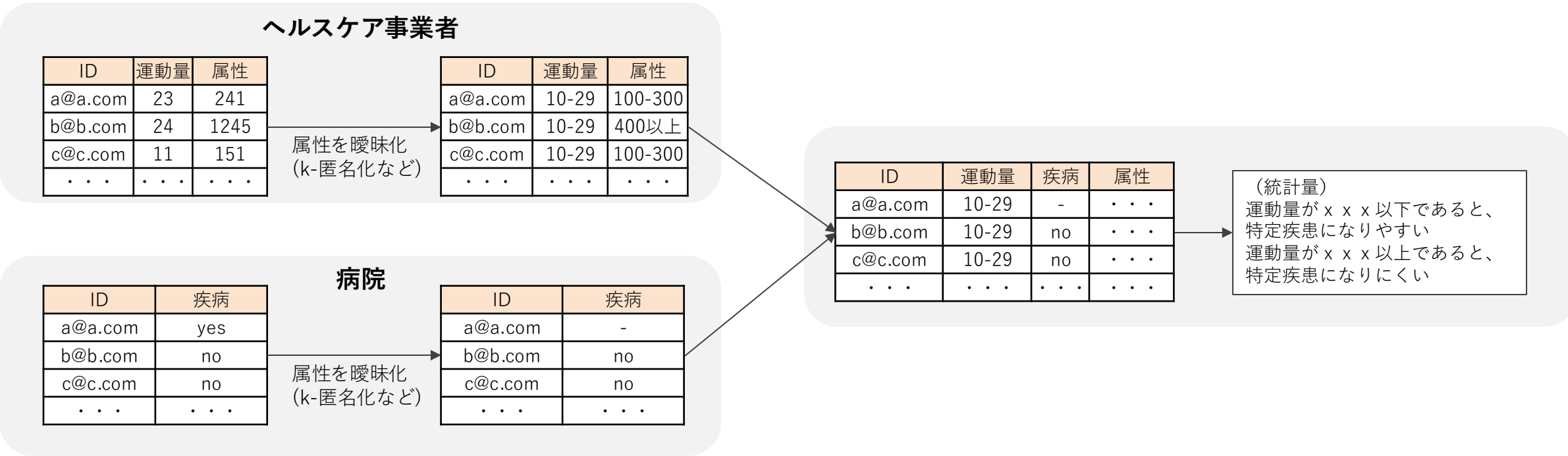
付録：個人データを突合・分析するユースケース例

（突合前に個人データを曖昧化することが望ましく無いユースケース例）

希少疾患の分析

- 医療情報とヘルスケア情報とを突合分析できると、医療・ヘルスケア分野に資する分析が可能
- しかし、希少疾患の患者数は少ないため、k-匿名化などで属性を曖昧化されると、分析精度が低下

図：希少疾患の分析（突合前にk-匿名化を行うと分析精度が低下）

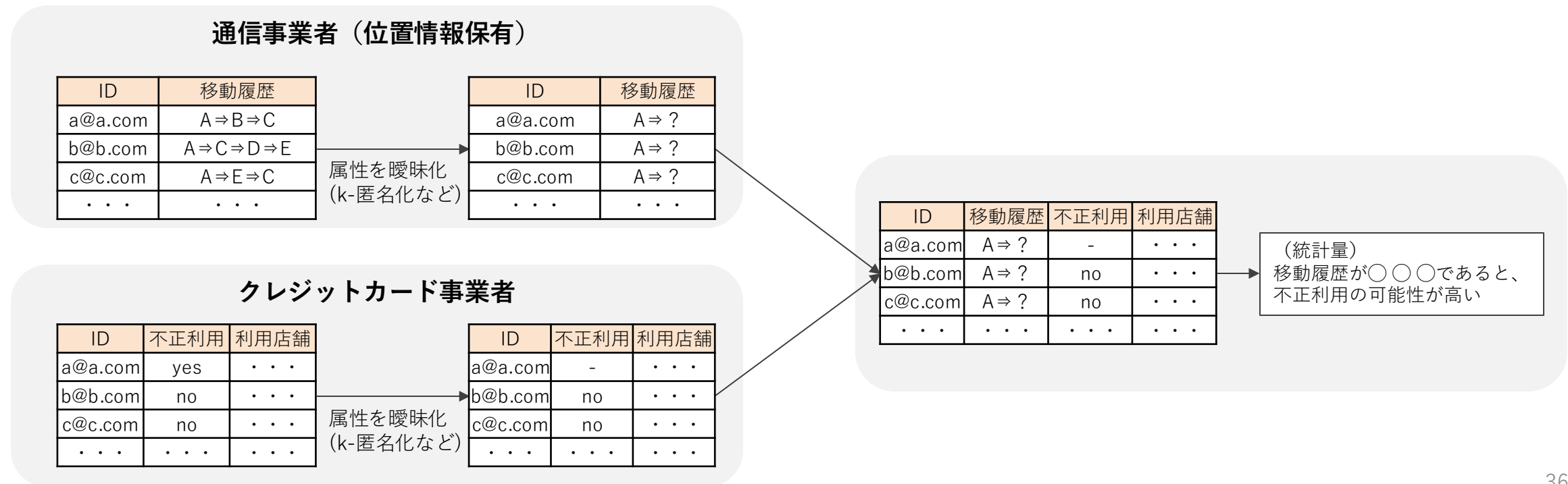


※ 次世代医療基盤法は医療情報に限定される（例：ヘルスケア事業者がもつ運動量情報や自治体を持つ要介護度の情報などは対象外）

クレジットカードの不正利用分析

- クレジットカードの不正利用検知は、位置情報などの他の情報と組み合わせることで、検知精度が向上
 - ・ 従来は、短時間での利用における店舗距離が遠いと不正利用の可能性高いと判断するため、旅行等の移動中の利用を不正利用と誤判断
 - ・ 利用者の位置情報を含めた不正利用の検知ができれば、本人の位置情報と利用店舗の矛盾からの判断が可能
- しかし、位置情報の移動履歴情報を匿名化（k-匿名化）すると履歴情報が消えてしまい、検知モデルの精度が低下

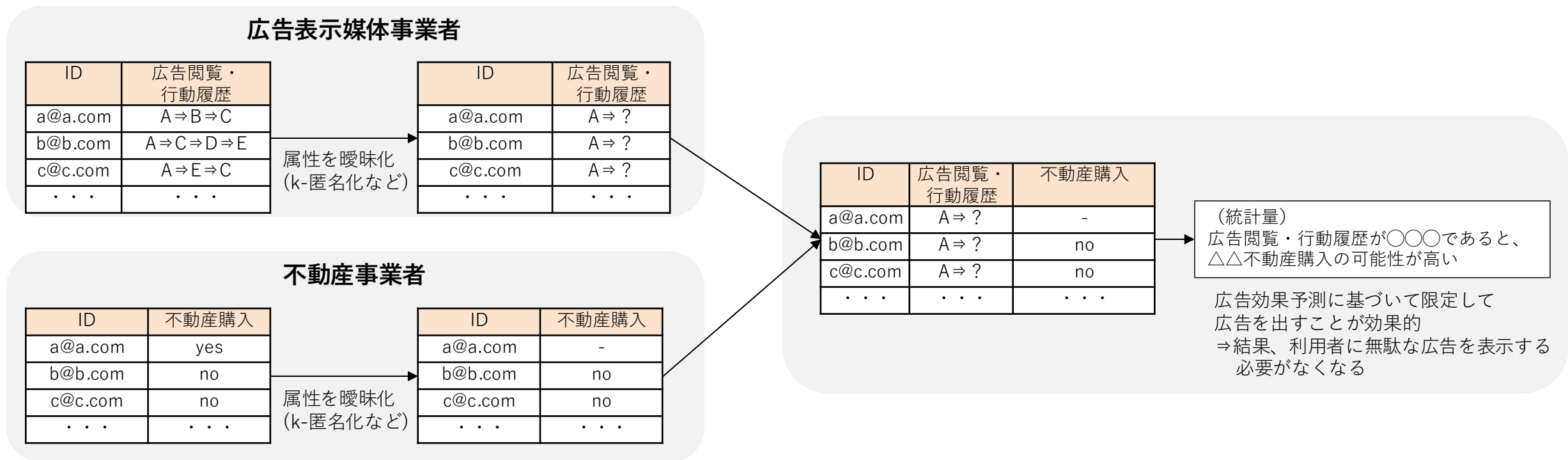
図：クレジットカードの不正利用分析（突合前にk-匿名化を行うと分析精度が低下）



マーケティングの分析

- 今後の広告分析では最終的な購買行動まで紐づけた分析が困難となり、購買行動に関連しない無駄な広告が増える恐れ
- もし、購買行動まで紐づけた広告効果が可能となれば、広告効果予測の精度が良くなり、無駄な広告を減らせる可能性
- しかし、広告閲覧履歴や行動履歴が曖昧に加工されると、分析精度が悪くなり適切な分析が困難となる

図：マーケティングの分析（突合前にk-匿名化を行うと分析精度が低下）

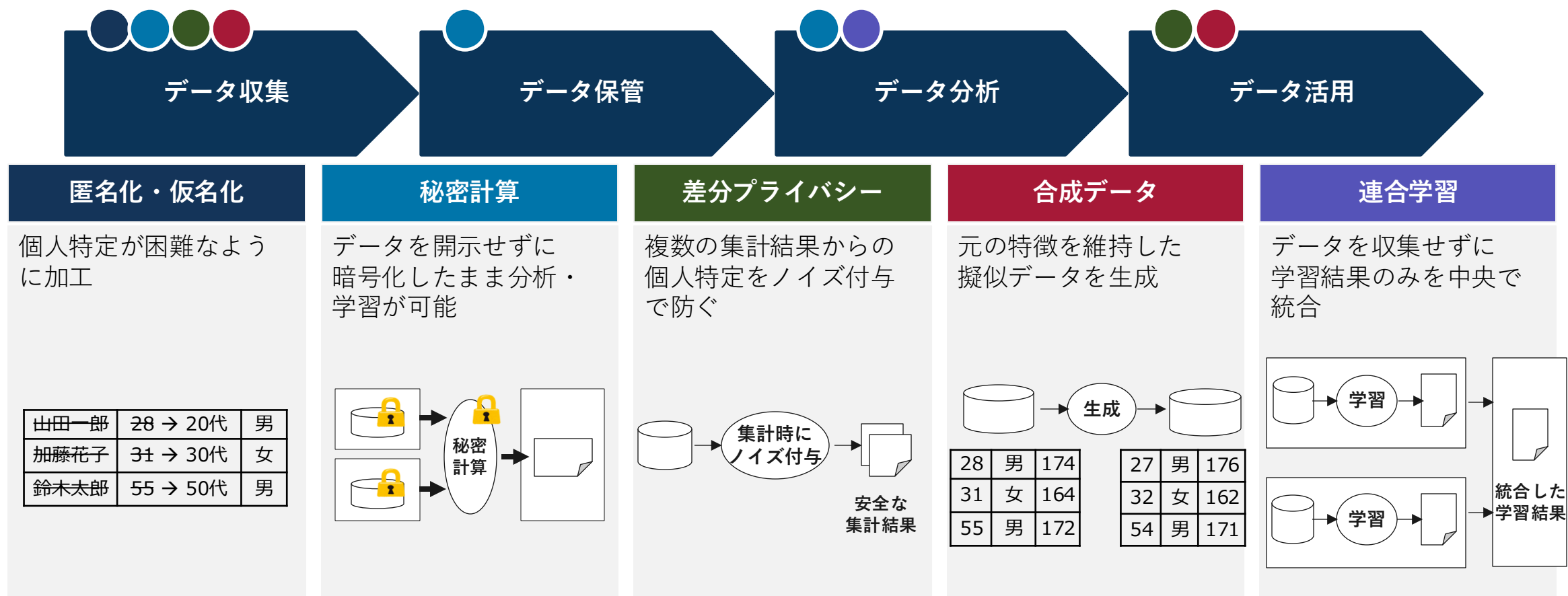


付録：他のPETsの概要

PETsについて

- PETsは様々存在し、技術によって保護する箇所も異なり、組み合わせた利用も効果的

データ活用のステップ概略





付録：GDPRやGDPRとの十分性認定の補完的ルール

■ GDPR

GDPR Chapter 2 Principles Article 5. (中略)

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; **further processing for archiving purposes** in the public interest, scientific or historical research purposes or **statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible** with the initial purposes ('purpose limitation');

公共の利益における保管の目的、科学的研究若しくは歴史的研 究の目的又は**統計の目的のために行われる追加的取扱い**は、第 89 条第 1 項に従い、当初の目的と適合しないものとはみなされない。

Article 89 Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

第89 条 公共の利益における保管の目的、科学調査若しくは歴史調査の目的又は統計の目的のための取扱いと関連する保護措置及び特例

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

1. 公共の利益における保管の目的、科学調査若しくは歴史調査の目的又は**統計の目的のための取扱い**は、本規則に従い、データ主体の権利及び自由のための**適切な保護措置に服する**。それらの保護措置は、とりわけ、データの最小化の原則に対する尊重を確保するため、**技術的及び組織的な措置を設けることを確保する**。それらの措置は、それらの目的がそのような態様で充足されうる限り、仮名化を含むことができる。データ主体の識別を許容しない又は許容することのない別の目的による取扱いによってそれらの目的が充足されうる場合、それらの目的は、その態様によって充足される。

出典：GDPRのPPCによる仮日本語訳, <https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf>

■ 補完的ルール

個人情報の保護に関する法律に係るEU及び英国域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール

(4) 仮名加工情報

(中略) この場合、**統計目的**とは、統計調査のため又はその他の統計結果を作成するためのあらゆる処理を意味し、それにより作成された統計結果は集計データであり、**特定の個人に関する措置又は決定を裏付けるために利用してはならない**。

出典：https://www.ppc.go.jp/files/pdf/Supplementary Rules_jp.pdf