PWS企画セッション２

個人情報保護法の改正議論における統計目的第三者提供とPETs

PWS企画セッション２

「個人情報保護法の改正議論における統計目的第三者提供とPETs」

■セッション説明

個人情報保護法の「いわゆる３年ごと見直し」に関して、統計目的であれば本人同意なき個人データ等の第三者提供が認められる方針が示され、議論がされている。

この方針について、個人情報の安全な活用を実現するには、第三者提供先での技術的なガバナンスも重要となると考える。

そこで、本セッションではPWS(Privacy Work Shop)の企画セッションにて過去から議論してきた経緯も踏まえ、このような技術的なガバナンスのために望ましいプライバシー保護技術（PETs: Privacy Enhancing Technologies)や制度などについて議論する。

■登壇者・パネリスト

・板倉 陽一郎（ひかり総合法律事務所）

・高橋 克巳（NTT社会情報研究所）

・寺田 雅之（NTTドコモ）

・美馬 正司（日立コンサルティング/慶應義塾大学）

■座長：竹之内 隆夫（Acompany）

セッションの流れ

1. セッション概要、背景、PETsの概要など
   竹之内 隆夫（Acompany）
2. 過去のPWS企画セッションの議論など
   寺田 雅之（NTTドコモ）
3. 個人情報保護法の改正議論の動向やPETsの法的な扱いや期待など
   板倉 陽一郎（ひかり総合法律事務所）
4. 事業者・コンサルティング業務としての意見・懸念
   美馬 正司（日立コンサルティング）
5. 個人情報保護法と技術について
   高橋 克巳（NTT社会情報研究所）
6. ディスカッション

セッションの背景と概要

自己紹介

■ 竹之内 隆夫 (たけのうち たかお)

株式会社Acompany(アカンパニー)
執行役員 VP of Public Affairs

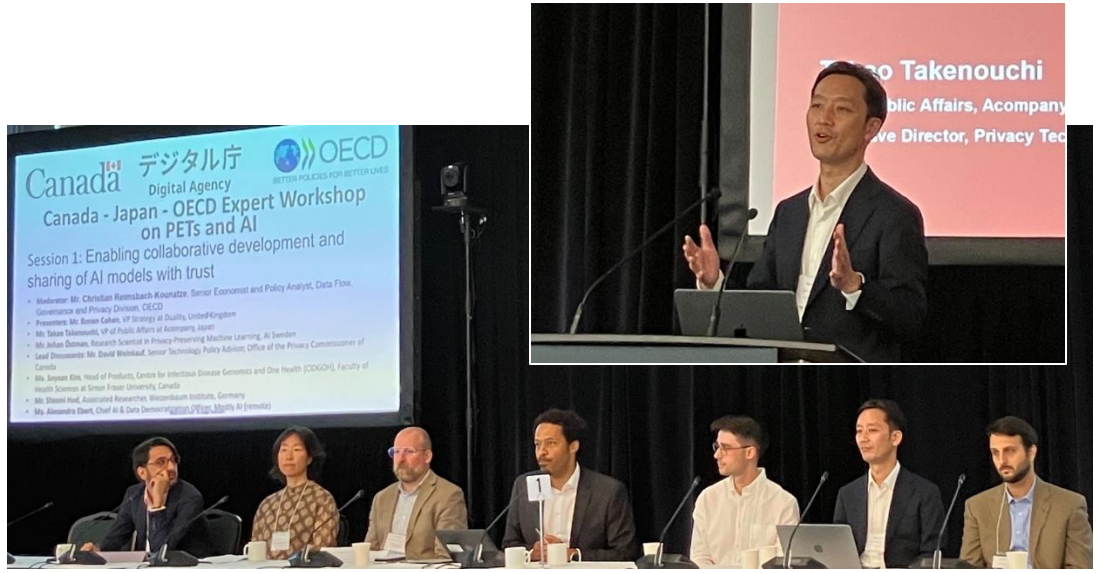
プライバシーテック協会 事務局長

■ 経歴：

- セキュリティ・プライバシーで約15年の研究開発
  - NEC→デジタルガレージ→ LINE(LINEヤフー) → Acompany
- 技術だけでなく法制度議論も
  - 「秘密計算研究会」、 DSA「秘密計算活用WG」 設立
- 博士(工学)、MBA

■ 政府関係の委員

- デジタル庁 データセキュリティWG 委員
- DFFT Expert Community メンバー



2025年6月カナダのOECD会合に日本からの代表としてプレゼン

個人情報保護法の改正議論： 本資料における「統計目的第三者提供」について

- 2025年3月5日に提示された以下の方針について、本資料では「統計目的第三者提供」と表記

第１　個人データ等の取扱いにおける本人関与に係る規律の在り方

１　個人の権利利益への影響という観点も考慮した同意規制の在り方

(1) 統計作成等、特定の個人との対応関係が排斥された一般的・汎用的な分析結果の獲得と利用のみを目的とした取扱いを実施する場合の本人の同意の在り方

【規律の考え方】

- 統計情報等の作成(注1)のために複数の事業者が持つデータを共有し横断的に解析するニーズが高まっていること、特定の個人との対応関係が排斥された統計情報等の作成や利用はこれによって個人の権利利益を侵害するおそれが少ないものであることから、このような統計情報等の作成にのみ利用されることが担保されていること等(注2)(注3)を条件に、本人同意なき個人データ等の第三者提供(注4)(注5)及び公開されている要配慮個人情報の取得を可能としてはどうか(注6)。

注１：統計作成等であると整理できるAI開発等を含む。

注２：本人同意なき個人データ等の第三者提供については、当該個人データ等が統計情報等の作成にのみ利用されることを担保する観点等から、個人データ等の提供元・提供先における一定の事項（提供元・提供先の氏名・名称、行おうとする統計作成等の内容等）の公表、統計作成等のみを目的とした提供である旨の書面による提供元・提供先間の合意、提供先における目的外利用及び第三者提供の禁止を義務付けることを

出展：”個人情報保護法の制度的課題に対する考え方について”, 2025年3月5日, 個人情報保護委員会, https://www.ppc.go.jp/files/pdf/seidotekikadainitaisurukangaekatanitsuite_250305.pdf

参考：「データ利活用制度の在り方に関する基本方針」

- データ活用・連携のために、PETsや秘密計算（例：ハードウエア型の秘密計算のTEE）が有用と言及

データ利活用制度の在り方に関する基本方針

2025 年６月 13 日
デジタル行財政改革会議決定

○また、データ連携が拡大し、さらに、多数の AI が協働することも考えられる中、社会全体においても、データの価値を最大化しつつ、リスクを低減していくためには、各データ関係主体におけるデータガバナンスの取組に加え、データのライフサイクルにおいてデータがクラウド事業者による場合などデータ関係主体の制御を離れてアクセスされる可能性があることも想定し、データの性質等に応じて必要な場合には、秘密計算[14]その他のプライバシー強化技術（PETs）などの技術的手法によって、適切なデータ関係主体によって防護されることが有用であり、制度面を含めて対応を検討する。その際、PETs 技術の発展に応じて、アジャイルな対応が必要となることに留意する。加えて、AI に関わるガバナンスについては総合科学技術・イノベーション会議、統合イノベーション戦略推進会議、AI 戦略会議などと連携をしながら推進する。

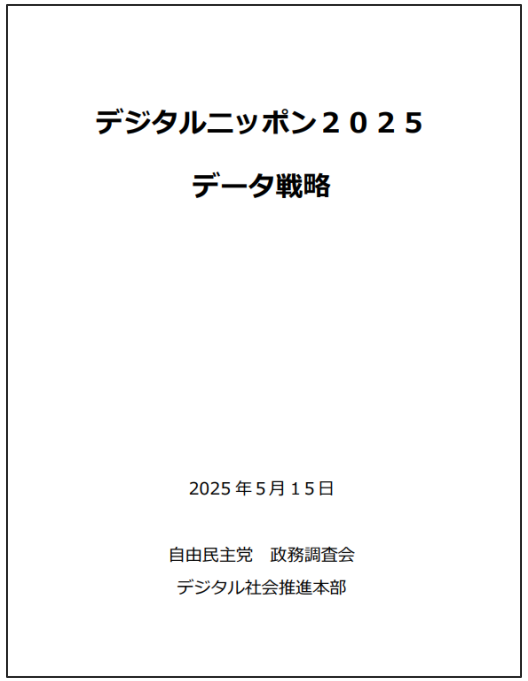
[13] 文脈によっても多義的であり、例えば、経営者によるガバナンスや、それをコーポレートガバナンスとして推進する施策を指すこともある。企業等の個々の主体データに係る各種取組を統合的にバランスよく進めるためには、データを使いこなす能力を高める取組、データに係るリスクに対応するための取組（法令遵守のための業務プロセス構築、データセキュリティのためのデータ防護策等）を適切に組み合わせることで効率よく目的を達成する必要があり、経営者が経営問題として取り組むことが不可欠となるため、データガバナンスとして一連の取組を促すもの。

[14] データの処理中においても暗号化・秘匿化を行うことが可能な TEE（Trusted Execution Environment）など復号鍵がチップ内にのみ存在するハードウェア型の秘密計算が世界的に AI 処理にも活用され始めている。

参考：「デジタル・ニッポン2025 データ戦略」

- 自民党の「デジタル・ニッポン 2025」にて「PETsの活用を推進」と記載

自民党の「デジタル・ニッポン 2025」にて「PETs」について記載



デジタルニッポン２０２５

データ戦略

2025年5月15日

自由民主党　政務調査会

デジタル社会推進本部

2.4　データ利活用に向けた個人情報保護制度のアップデートと特別の規律の設定等

特に、AIの進展をはじめとして、情報技術の急速な進展や国際動向等を踏まえた個人情報の利活用ニーズが高まる中、個人情報保護法において求められている本人同意の範囲について見直す必要がある。例えば、個人に直接の影響がないと考えられる統計やAIの「パラメータ」などの作成については同意不要とすべきである。また、利活用を推進するに当たっては、適切なガバナンスの確保や最新のプライバシー保護技術（PETs）の活用を推進し、信頼ある個人情報の取扱いにつなげる必要がある。こうした内容を盛り込んだ、全体としてバランスのとれた個人情報保護法改正法案を早期に提出する必要がある。

出典：https://www.jimin.jp/news/policy/210615.html

参考：PETsへの期待の例（国会答弁）

- 個人情報保護法におけるPETsの位置づけについて、共に検討できればと思います

2025年4月18日のAI法の審議においてPETs(プライバシー保護技術)と個人情報保護法について議論

自由民主党 平井卓也 委員

個人情報の利用を最小化する技術、これは今物すごく、**プライバシー・エンハンシング・テクノロジー(PETs)**なんかが非常に進んでいますので、そういうものの利活用も考えながら、不安を解消してＡＩ開発を後押しするような見直しをすべきだというふうに考えておりますが、個人情報保護委員会、政府参考人の皆さんに御意見を承りたいと思います。

個人情報保護委員会事務局 佐脇事務局長

PETsといったものの技術をしっかり位置づけるとか、あるいはルールにしっかり見合った、バランスの取れた違反行為抑止策を検討するといったことが重要であろうかと思ってございます。

　こうしたことを踏まえまして、今回の規律が、利用者や消費者を含め、様々な幅広い関係者に受け入れられる内容となりますよう、引き続き対話も重ねながら検討してまいりたいと思います。

出典：2025年4月18日衆議院 内閣委員会「人工知能関連技術の研究開発及び活用の推進に関する法律案」の審議の動画から抜粋 。
https://www.shugiintv.go.jp/jp/index.php?ex=VL&deli_id=55719&media_type=
「第217回国会 衆議院 内閣委員会 第15号 令和7年4月18日」会議録から抜粋し、わかりやすさのため「(PETs)」を付記。
https://kokkai.ndl.go.jp/#/detail?minId=121704889X01520250418&current=7

参考：日本医師会様のご意見

- 「統計目的第三者提供」について心配の声も

⇒ PETsによる技術的なガバナンスが可能であることを示すことが重要と理解

出典： "医療等情報の利活用に関する日本医師会の見解", 医療等情報の利活用の推進に関する検討会（第2回）,
https://www8.cao.go.jp/iryou/studygloup/20250910/agenda.html

1. 要配慮個人情報が本人同意なく第三者提供されることについての懸念

「個人データ等」には、当然ながら医療情報等の要配慮個人情報も含まれていますが、従来要配慮個人情報については、間違っても国民一人一人の不利益につながることがないよう、非常に慎重に取り扱われてきたところです。

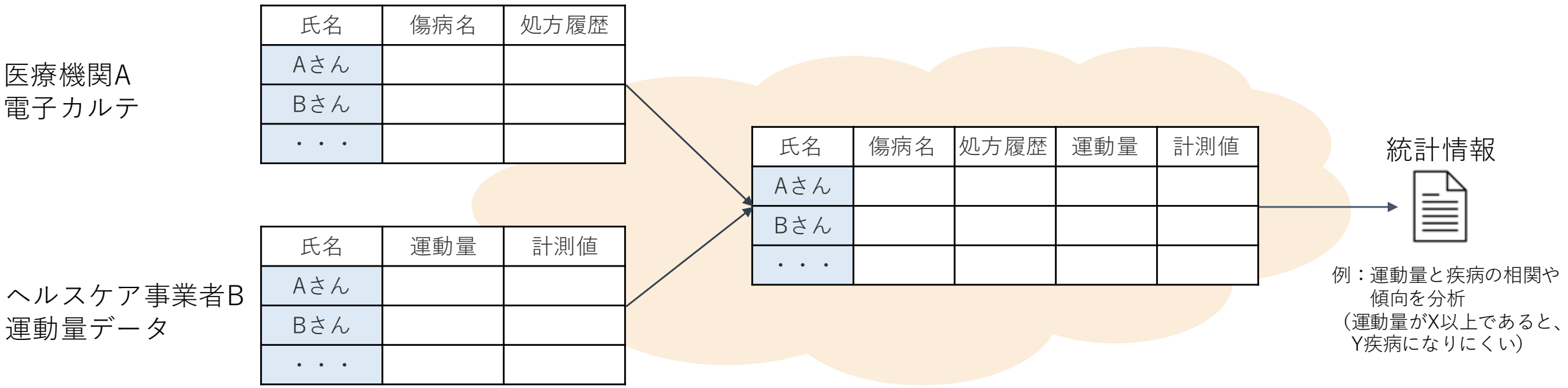
例えば、現在国が進めている医療 DX においては、目の前の患者により良い医療を提供する目的であっても、オンライン資格確認等システムによる確実な本人確認と本人同意の取得なしには、医師は当該患者の過去の医療情報を閲覧することはできない仕組みとなっており、患者の権利が担保されています。

医療提供という一次利用においてさえ、このように厳格に医療情報を扱っている現状に対して、顕名の要配慮個人情報が本人同意なく第三者提供し、二次利用が可能となり得る今回の案は、最終的に統計情報等の作成にのみ利用されることが担保されればという条件付きであっても、著しく乖離しており、俄かに容認できるものではありません。

同文書では、統計情報等の作成にのみ使用されることを担保する観点から、個人データ等の提供先・提供元における一定事項の公表や目的の合意、目的外利用及び提供先からの更なる第三者提供の禁止を義務付けることを想定するとされています。しかし、利用目的となる統計情報等について、特定の個人との対応関係が排斥されているか否かを、誰が確認し、責任を負うのかを明確にする必要がありますし、プライバシーやセキュリティについて十分に理解していない民間事業者も含まれる個人情報取扱事業者に対して、要配慮個人情報の第三者提供を公表のみで認めることは極めて危険であると考えます。

本資料が想定するデータ連携のユースケースの例

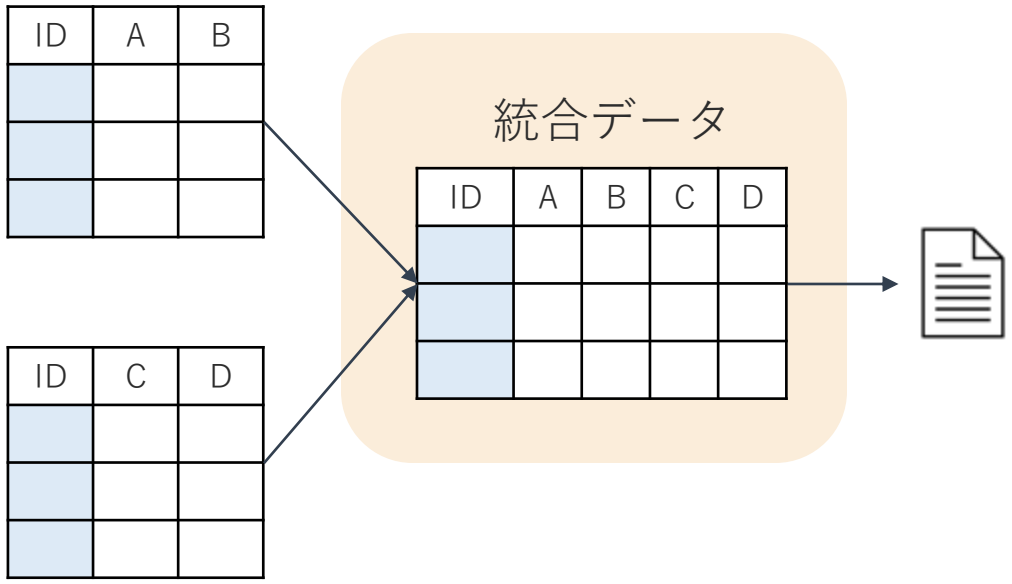
- 複数の企業が保有する個人データを、PETsを用いて安全に突合分析
- 出力は「統計情報」とする



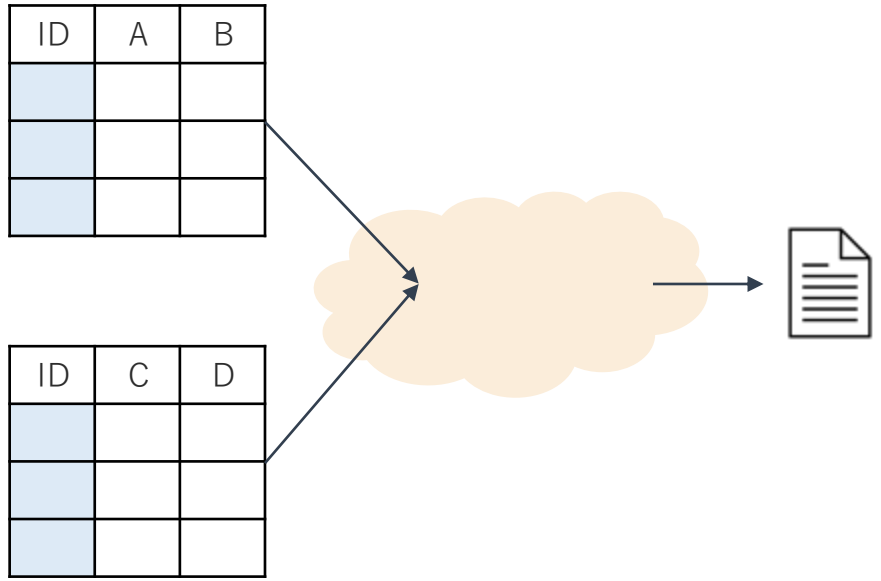
参考：個人データと突合して統計情報を得る処理のパターン

明確に「突合データ」を作る方法もあれば、作らなくても良い方法も

パターン１：統合データを作り統計処理



パターン２：統合データを作らずに統計処理



過去のPWS企画セッションの議論

2年前のPWSの企画セッションでも、組織横断した分析について議論

2C2: Privacy Techを用いた安全なデータ活用事例と課題

座長：竹之内隆夫(LINE株式会社)

本企画セッションでは、秘密計算(MPCやTEE）や差分プライバシーや連合学習などの様々なPrivacy Techを活用した、個人データの安全な活用事例の紹介し、今後の望ましいデータ活用・プライバシー保護について議論する。 Privacy Techを活用することが、今後の個人データの活用推進に資することを、技術や信頼感・ブランドや法律の観点で議論する。

Privacy Techの概要と連合学習と差分プライバシーの事例

竹之内隆夫(LINE株式会社)

秘匿クロス統計：組織横断の安全なデータ活用に基づく社会課題解決の試み

寺田雅之(株式会社NTTドコモ)

秘密計算を用いた大学間でのデータ分析 ～トライアルサービスの概要とシステム構成の紹介～

藤原 一毅 (国立情報学研究所)

秘密計算を用いた大学間でのデータ分析 ～トライアルで秘密計算に取り組むモチベーションを紹介～

高木 理 (群馬大学)

https://www.iwsec.org/css/2023/program.html#2C2

「統計情報」とは

「統計情報」の定義については直前セッションにて議論

2E3: PWS企画セッション１「安全かつ有用な合成データの生成に関する現状と課題」

座長：千田浩司 (群馬大学)

【セッション説明】
近年、わが国では民間が保有する個人情報の活用が広範になされているが、センシティブな情報を含む個人情報の場合、その利活用については法制度面から制約が課せられている。そうした中で、合成データ(synthetic data)の作成と利活用について、実務家やプライバシー保護の専門家の間で関心が高まっている。こうした状況を踏まえ、現在データ合成技術評価委員会では、合成データ作成に関する技術的検討を進めるだけでなく、社会実装の可能性が模索されている。

そこで本セッションでは、安全かつ有用な合成データの作成の可能性をさらに追究するために、合成データの生成技法や有用性の評価方法に関する最新の動向について報告を行う。さらに、データ合成技術評価委員会による研究の方向性についても論じることによって、安全かつ有用な合成データの生成の現状と課題に関して議論を行いたい。

【講演者および講演タイトル】

1. 上田 聖 (統計センター)：　公的統計の二次利用の現状と課題
2. 伊藤 伸介 (中央大学)：　公的統計における合成データの作成に関する動向
3. 石原 琢磨 (岐阜大学)、山本 景一 (大阪歯科大)：　医療健康情報に関する合成データの作成に関する現状と課題
4. 千田 浩司 (群馬大学)：　データ合成技術評価委員会による研究の動向

https://www.iwsec.org/css/2025/program.html#2E3

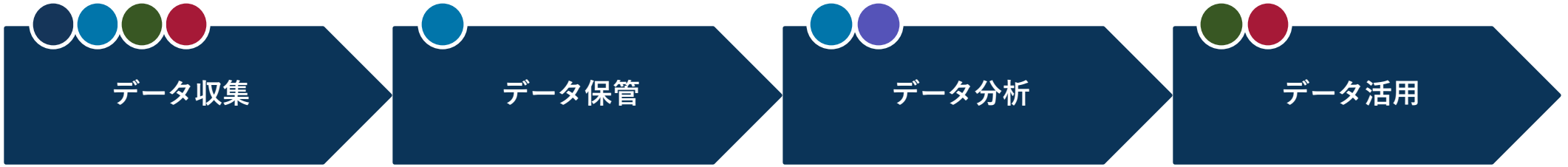
PETsとは

※PETsとプライバシーテックは呼び方の違いであり、ほぼ同じ技術を指します

主要なPETs(Privacy Enhancing Technologies) の概要

- PETsとは、**プライバシーを保護する技術の総称**
- データ活用において適用場所が異なるため、**組み合わせることも可能**

PETsの一例と、PETsの適用場面



匿名化・仮名化

個人特定が困難なように加工

~~山田一郎~~	~~28~~ → 20代	男
加藤花子	~~31~~ → 30代	女
鈴木太郎	~~55~~ → 50代	男

合成データ

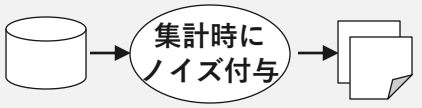
元の特徴を維持した擬似データを生成

28	男	174
31	女	164
55	男	172

27	男	176
32	女	162
54	男	171

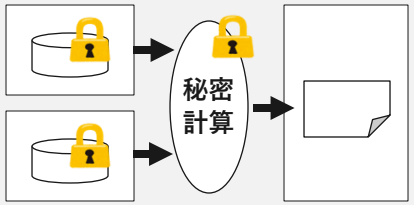
差分プライバシー

複数の集計結果からの個人特定をノイズ付与で防ぐ



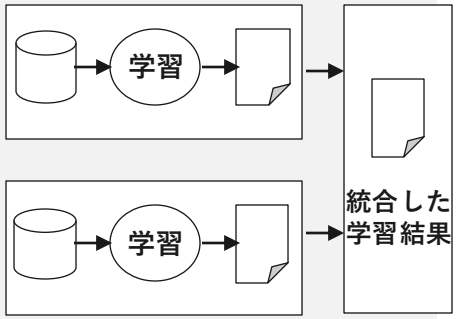
秘密計算

データを開示せずに暗号化したまま分析・学習が可能



連合学習

データを収集せずに学習結果のみを中央で統合



PETsの定義

PETsは様々な定義が存在するが、総じて“**プライバシーを保護する技術の総称**”と捉えられる

参考：PETsの定義について記載しているISACAのホワイトペーパー　※機械翻訳

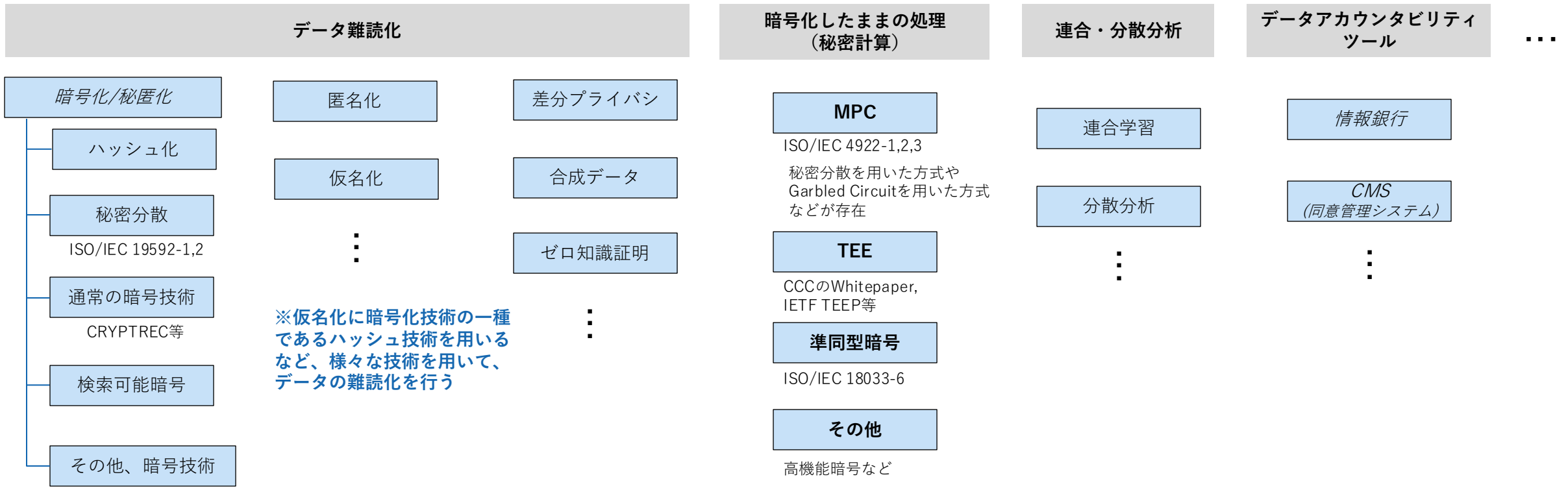
ISACA,
”Exploring Practical Considerations and Applications for Privacy Enhancing Technologies”
https://www.isaca.org/resources/white-papers/2024/exploring-practical-considerations-and-applications-for-privacy-enhancing-technologies

- プライバシー強化技術（PETs）の初期の定義は、1995年のオンタリオ州情報・プライバシーコミッショナー報告書に見られる。この報告書では、PETsを**「識別可能なデータの収集を最小化または排除することで個人のプライバシーを保護するさまざまな技術」**として説明している。
- また、2002年の経済協力開発機構（OECD）による「プライバシー強化技術のインベントリ」では、PETsを**「個人のプライバシーを保護するための幅広い技術」**と定義している。
- データプライバシー法において、PETsの明確な法的定義は存在しないが、英国情報コミッショナー事務所（ICO）が最近発行したガイダンスでは、PETsを次のように説明している。「**個人情報の利用を最小化し（これは英国GDPRにおける個人データの法的定義を含む）、情報セキュリティを最大化し、人々に力を与えることで、データ保護の基本原則を具体化する技術。**」
- 国際標準化機構（ISO）は、PETsを次のように定義している「**プライバシーコントロールであり、情報通信技術（ICT）の手段、製品、またはサービスから構成される。これらは、個人識別可能情報（PII）を削除または削減すること、または不要もしくは望まれないPIIの処理を防止することによってプライバシーを保護しつつ、ICTシステムの機能性を損なうことなく実現するものである。**」
- 本ホワイトペーパーでは、欧州連合サイバーセキュリティ庁（ENISA）の定義を採用する。ENISAはPETsを**「特定のプライバシーまたはデータ保護機能を実現する、または個人もしくは自然人のグループのプライバシーに対するリスクを防ぐための技術的プロセス、方法、または知識を包含するソフトウェアおよびハードウェアソリューション」**と定義している。
- PETsは、企業内部でのプライバシーとデータの有用性を高めるとともに、データ共有に伴うリスクを低減することにより、潜在的に競合する外部組織との協業を促進する。そのため、PETsは非公式には「partnership enhancing technologies」や「trust technologies」とも呼ばれている。

PETsの概観と分類

- PETsとは、**プライバシーを保護する技術の総称**
- データを加工する技術や同意管理技術など**様々存在**

図：主なPETsの類型　（※OECDの2023年のPETsガイドラインを参考に分類）



MPC: Multi Party Computation
TEE: Trusted Execution Environment
CCC: Confidential Computing Consortium
CMS: Consent Management System

参考：OCDEの2023年のPETsガイドラインにおける分類

Table 1. Overview of major types of PETs, their opportunities and challenges

Types of PETs	Key technologies	Current and potential applications*	Challenges and limitations
Data obfuscation tools	Anonymisation / Pseudonymisation	Secure storage	- Ensuring that information does not leak (risk of re-identification) - Amplified bias in particular for synthetic data - Insufficient skills and competences
	Synthetic data	Privacy-preserving machine learning	
	Differential privacy	Expanding research opportunities	
	Zero-knowledge proofs	Verifying information without requiring disclosure (e.g. age verification)	- Applications are still in their early stages
Encrypted data processing tools	Homomorphic encryption	Computing on encrypted data within the same organisation Computing on private data that is too sensitive to disclose Contact tracing / discovery	- Data cleaning challenges - Ensuring that information does not leak - Higher computation costs
	Multi-party computation (including orivate set intersection)		
	Trusted execution environments	Computing using models that need to remain private	- Higher computation costs - Digital security challenges
Federated and distributed analytics	Federated learning	Privacy-preserving machine learning	- Reliable connectivity needed - Information on data models need to be made available to data processor
	Distributed analytics		
Data accountability tools	Accountable systems	Setting and enforcing rules regarding when data can be accessed Immutable tracking of data access by data controllers	- Narrow use cases and lack stand-alone applications - Configuration complexity - Privacy and data protection compliance risks where distributed ledger technologies are used - Digital security challenges - Not considered as PETs in the strict sense
	Threshold secret sharing		
	Personal data stores / Personal Information Management Systems	Providing data subjects control over their own data	

Note: (*) Only one application has been included for the sake of readability.

■原文

The PETs are divided into the following four broad categories: (i) data obfuscation, (ii) encrypted data processing, (iii) federated and distributed analytics, and (iv) data accountability tools.Some of the 14 PETs can fit in more than one category; in which case they are assigned to a main category.

■参考日本語訳

これらのPETsを、次の4つの大きなカテゴリーに分類される：

- データ難読化（data obfuscation）
- 暗号化データ処理（encrypted data processing）
- 連合・分散分析（federated and distributed analytics）
- データアカウンタビリティツール（data accountability tools）

一部の**PETは複数のカテゴリーに該当する場合もあり、その場合は主たるカテゴリーに分類**される。

Source:
OECD, “EMERGING PRIVACY ENHANCING TECHNOLOGIES CURRENT REGULATORY ANDPOLICY APPROACHES”, 2023,
https://www.oecd.org/en/publications/emerging-privacy-enhancing-technologies_bf121be4-en.html

参考：海外ガイドライン記載のPETs

- この1～3年にて海外公的機関・業界団体からPETsに関するガイドラインが出されてており、いくつかのPETsが注目
- 特に**秘密計算、差分プライバシー、連合学習、合成データ**は近年特に注目

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	(2) OECD AI PETs	(3) 英国ICO PETs	(4) 米国 PPDSA	(5) UN PETs	(6) CIPL PETs	(7) ISACA PETs
データ難読化技術	匿名化、仮名化	o			o		o	
	合成データ	**o**	**o**	**o**	**o**	**o**	**o**	**o**
	差分プライバシー	**o**	**o**	**o**	**o**	**o**	**o**	**o**
	ゼロ知識証明	o		o	o	o	o	o
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）**	**o**	**o**	**o**	**o**	**o**	**o**	**o**
	準同型暗号（準同型暗号を用いた秘密計算）	**o**	**o**	**o**	**o**	**o**	**o**	**o**
	TEE（TEEを用いた秘密計算）	**o**	**o**	**o**	**o**	**o**	**o**	**o**
連合・分散分析技術	**連合学習**	**o**	**o**	**o**	**o**	**o**	**o**	**o**
	Distributed Analytics	o						
アカウンタビリティ技術	Accountable System	o						
	Threshold Secret Sharing	o						
	Personal Data Store（情報銀行）	o						

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：公的機関が発表しているPETsに関するガイドラインの一例

本文書における略称	タイトル	概要	発行時期
OECD PETs	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
OECD AI PETs	Sharing trustworthy AI models with privacy-enhancing technologies	OECDが発行しているAI開発・利用におけるPETs活用を整理した資料	2025年6月
ICO PETs	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
US PPDSA	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 PETs	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 PETs	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
ISACA PETs	Exploring Practical Considerations and Applications for Privacy Enhancing Technologies	PETs活用に向けた、評価方法やケーススタディや法規制との関係の検討項目を示したホワイトペーパー	2024年3月

OECD PETs https://www.oecd.org/en/publications/emerging-privacy-enhancing-technologies_bf121be4-en.html
OECD AI PETs https://www.oecd.org/en/publications/sharing-trustworthy-ai-models-with-privacy-enhancing-technologies_a266160b-en.html
ICO PETs https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/
US PPDSA https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf
UN PETs https://unstats.un.org/bigdata/task-teams/privacy/guide/2023_UN%20PET%20Guide.pdf
CIPL PETs https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-understanding-pets-and-ppts-dec2023.pdf
ISACA PETs https://www.isaca.org/resources/white-papers/2024/exploring-practical-considerations-and-applications-for-privacy-enhancing-technologies

なお、個人情報保護委員会のページにて公開されいる「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関係の最近動向）

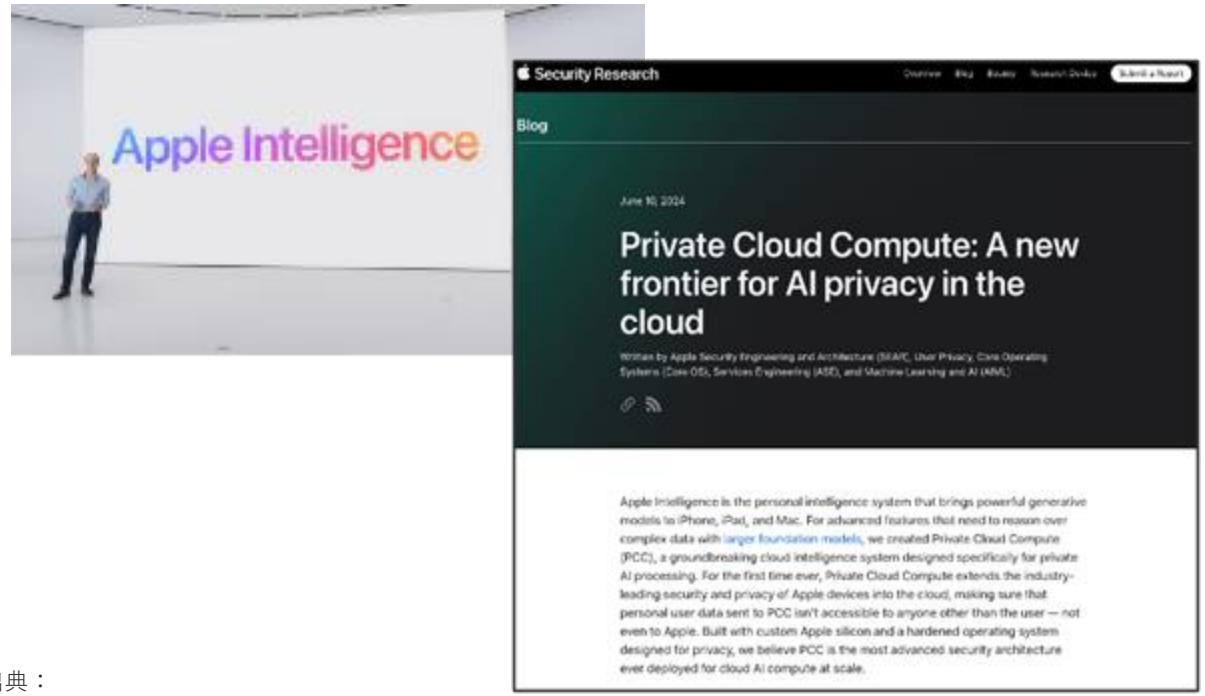
TEE/Confidential Computingの動向

※他のPETsと組み合わせた利用が有用

TEE/機密コンピューティングの動向

- 秘密計算は、今やAI処理も高速に実行可能
- 特に昨年6月のAppleの本技術の適用発表をきっかけに、この1年で一気に注目

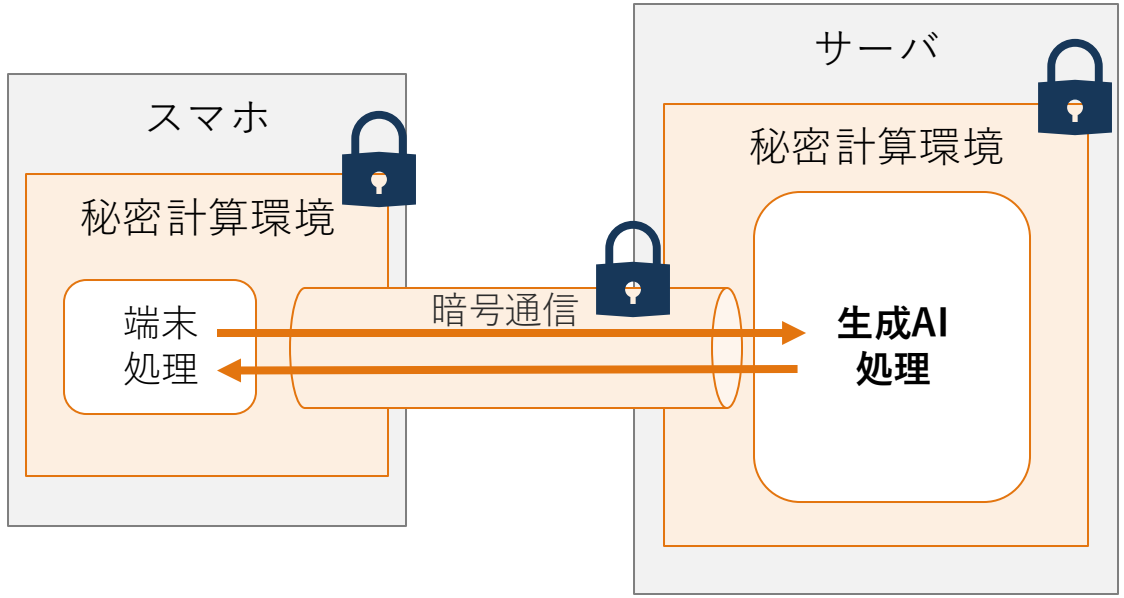
iPhone 16で動作する生成AIには本技術が適用※1



出典：
WWDC2024, https://www.youtube.com/live/RXeOiIDNNek?si=op_XevL-6fco944o&t=4000
“Private Cloud Compute: A new frontier for AI privacy in the cloud”,
“Private Cloud Compute: A new frontier for AI privacy in the cloud”, Apple, Security Research Blog, https://security.apple.com/blog/private-cloud-compute/

※1 AppleはSecure EnclaveというTEEを用いて本技術（機密コンピューティング）を実現

重たい処理をサーバで秘密計算で安全に処理



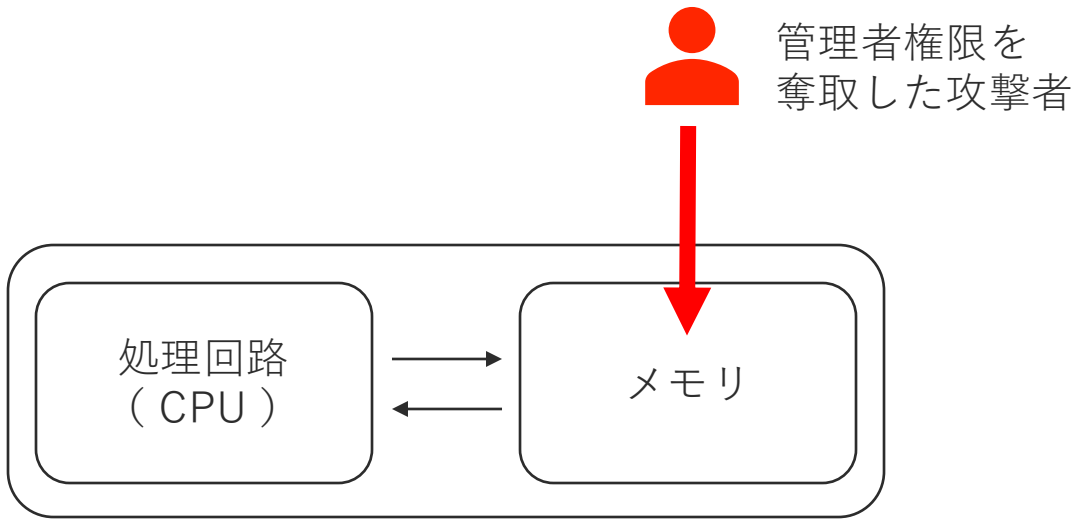
出典：同様な技術についてのGoogleの技術Blog記事の図を参考に著者らが作成
記事：“プライバシーを強化した生成 AI を実現する”,
https://developers.googleblog.com/ja/enabling-more-private-gen-ai/

TEE（Trusted Execution Environment）とは

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

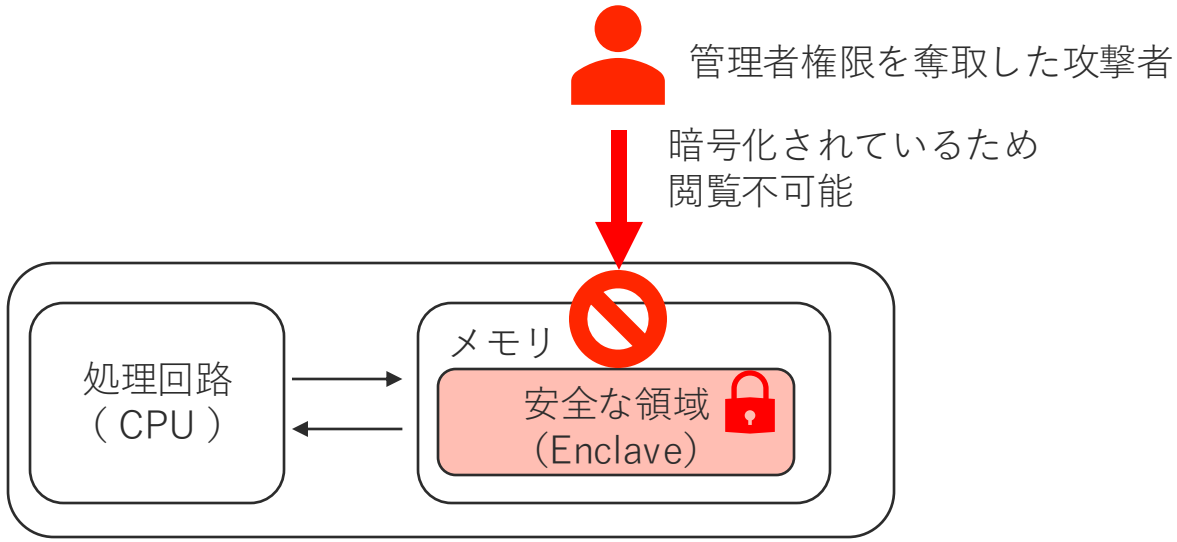
TEEなしのシステム

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での処理をConfidential Computing(機密コンピューティング)という

参考：メモリを閲覧する攻撃の例（米国CISAレポート）

- 米国CISAは2022年に米国重要インフラへの侵入試験(red team assessment)を実施
- メモリからの認証情報の奪取により、様々な重要サーバへの侵入が成功

America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

レッドチームは**メモリから復号鍵を抜き出し**、その鍵でデータベースを解錠
The red team pulled the decryption key from memory using KeeThief and used it to unlock the database

チームはそれを利用して、**他の社内ウェブサイト、カーネルベースの仮想マシン（KVM）サーバー、仮想プライベートネットワーク（VPN）エンドポイント、ファイアウォール、**そして**認証情報を含む別の KeePass データベースのパスワードを取得**することができました
The team was able to use to obtain passwords for other internal websites, a kernel-based virtual machine (KVM) server, virtual private network (VPN) endpoints, firewalls, and another KeePass database with credentials.

出典：“CISA Red Team Shares Key Findings to Improve Monitoring and Hardening of Networks”, Alert Code：AA23-059A, 2023年2月28日, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-059a

参考：海外の規制動向（EU金融分野）

EUの金融機関は、「処理途中の暗号化」はリスクに応じて適用すべきと規定

EU金融機関のICTリスクに関する法律（デジタル・オペレーショナル・レジリエンス法（DORA）2025年適用開始）に関する規定

EUROPEAN COMMISSION

Brussels, 13.3.2024
C(2024) 1532 final

COMMISSION DELEGATED REGULATION (EU) .../...

of 13.3.2024

supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework

(Text with EEA relevance)

出典：
COMMISSION DELEGATED REGULATION (EU) of 13.3.2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk managementframework
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=intcom:C%282024%291532

金融機関は、データ分類と包括的なICTリスク評価という二段階のプロセスの結果に基づき、対象となるデータを保存時や送信時、**そして必要な場合は処理中も暗号化すべきである（should）**。
ただし、使用中データの暗号化は技術的に複雑であるため、**金融機関は、ICTリスク評価の結果に照らして適切と判断される場合にのみ、使用中データを暗号化すべきである**。

プライバシーテック協会による参考日本語訳

Financial entities should encrypt the data concerned at rest, in transit or, where necessary, in use, on the basis of the results of a two-pronged process, namely data classification and a comprehensive ICT risk assessment.
Given the complexity of encrypting data in use, financial entities should encrypt data in use only where that would be appropriate in light of the results of the ICT risk assessment.

英語原文

参考：NVIDIAのGPUの動向

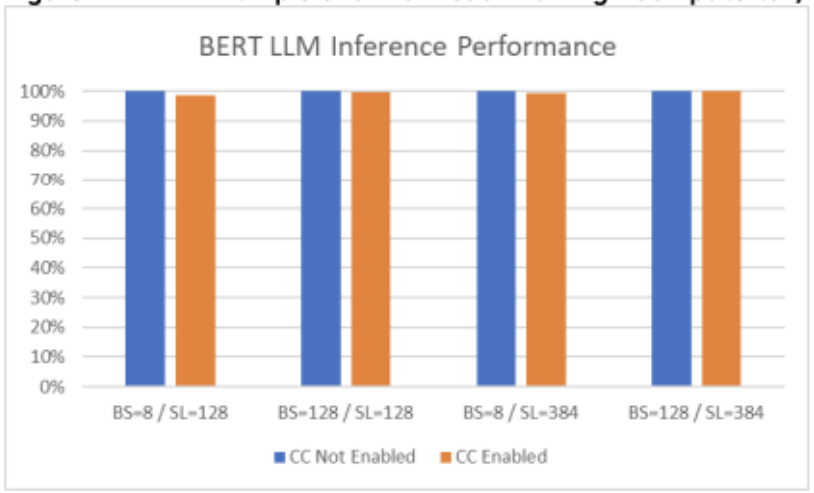
- GPUチップメーカーのNVIDIAのHopperシリーズからTEEに対応
- 処理内容にも依存するが、推論処理についての速度低下はさほど多くない

NVIDIAのH100でのAI推論と学習の処理時間の比較(言語処理モデルの例)

推論処理は、ほぼ同じ処理時間

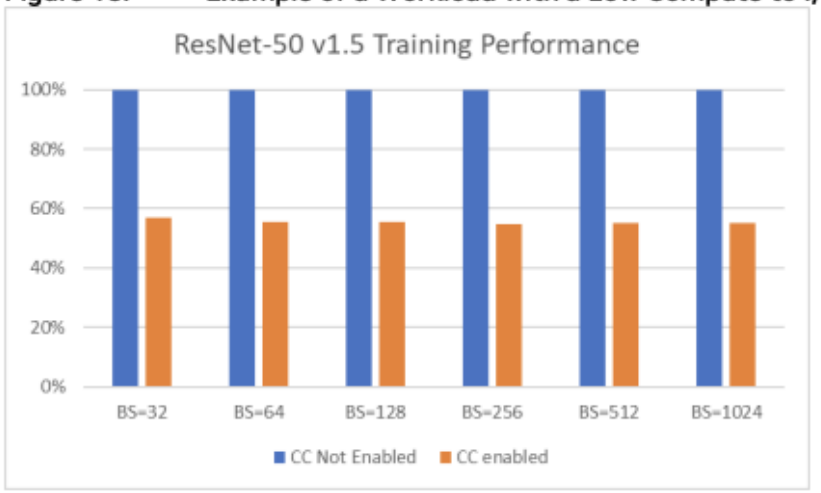
学習処理は、50%程度の速度劣化

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



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



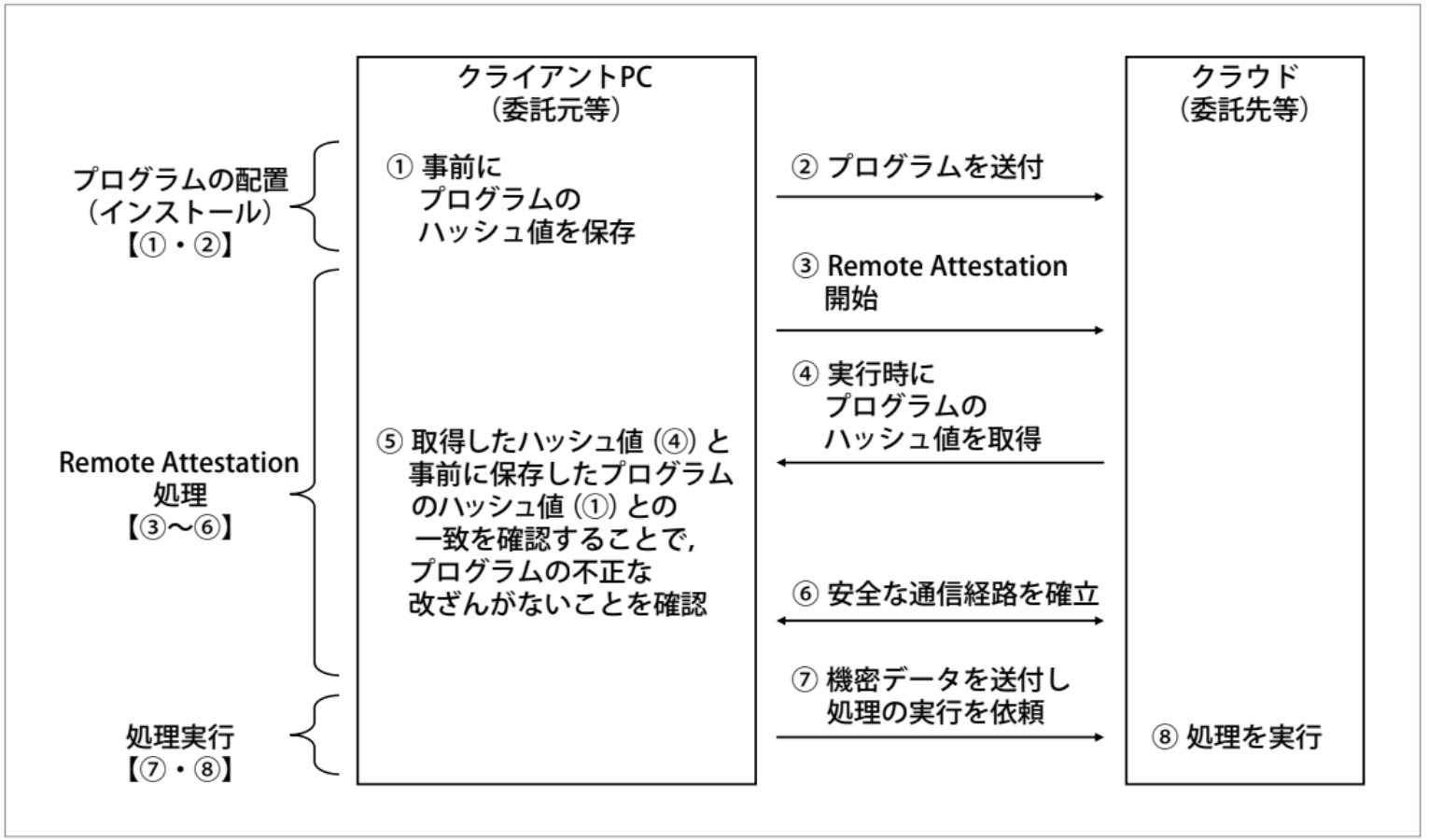
BS is the batch size.

出典：
https://images.nvidia.com/aem-dam/en-zz/Solutions/data-center/HCC-Whitepaper-v1.0.pdf

データの「機密性」：データが不正に閲覧できないこと
コードの「完全性」：コードが改ざんされていないこと

リモートアテステーションとは（コードの完全性を担保する技術）

- リモートアテステーションによって、提供先にて不正な処理が行われていないことを、提供元から検証が可能



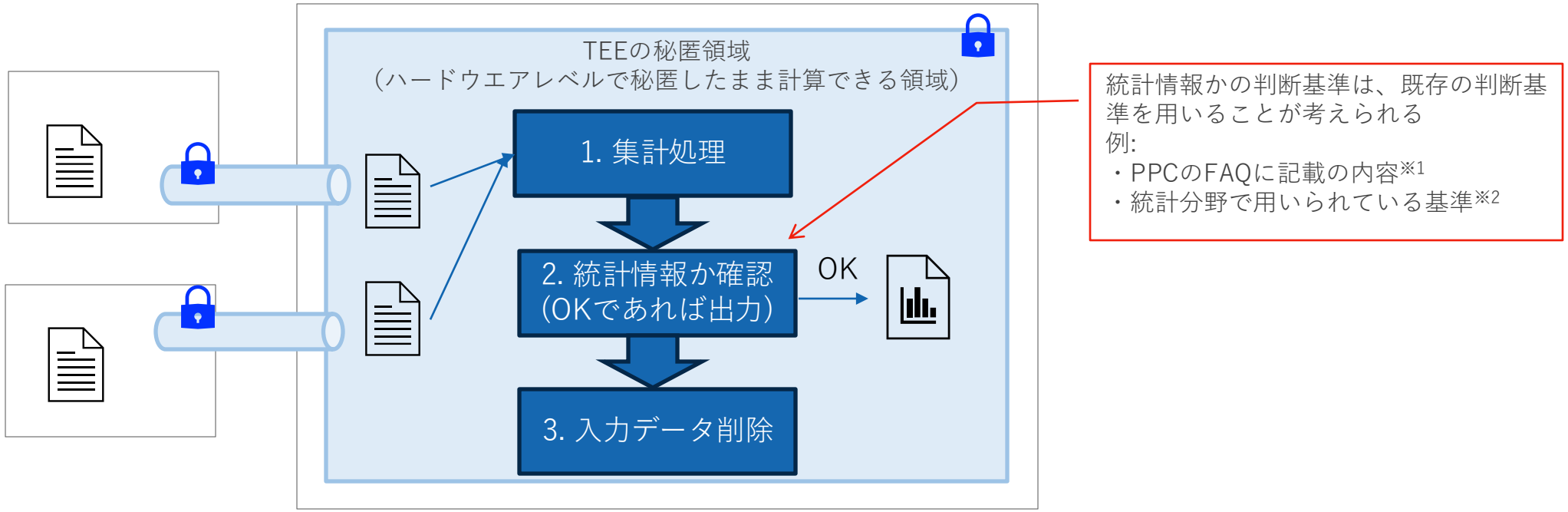
■図 -2
Remote Attestation の
処理概要の例

「Confidential Computing に関する法的論点」情報処理 Vol.66 No.7 (July 2025)より引用

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。

Confidential Computingの市場予測（Gartner）

- ガートナーの「2026年の戦略的テクノロジのトップ・トレンド」の6項目
- 2029年までにクラウド等の信頼できないインフラ上で処理される業務の75%以上にConfidential Computingが適用されると予測

Gartner Identifies the Top Strategic Technology Trends for 2026

出典：
https://www.gartner.com/en/newsroom/press-releases/2025-10-20-gartner-identifies-the-top-strategic-technology-trends-for-2026

Confidential Computing（機密コンピューティング）は、組織が機密データを扱う方法を根本的に変革します。ハードウェアベースのTrusted Execution Environment（TEE：信頼実行環境）内でワークロードを隔離することにより、インフラ運用者、クラウド事業者、さらにはハードウェアへの物理的アクセス権を持つ者からも、データ内容や処理内容を秘匿したまま実行できます。これは、規制産業や地政学的・コンプライアンスリスクに直面するグローバルな事業運営、さらには競合企業間のデータ連携において特に価値があります。

ガートナーは、2029年までに信頼されないインフラ上で処理される業務の75%以上が、Confidential Computingによって「使用中（in-use）」の状態で保護されるようになると予測しています。

プライバシーテック協会による参考日本語訳