PETs(Privacy Enhancing Technologies)とガバナンス

※PETsはプライバシーテックの別名です

プライバシーテック協会　事務局長
竹之内隆夫

プライバシーテック協会

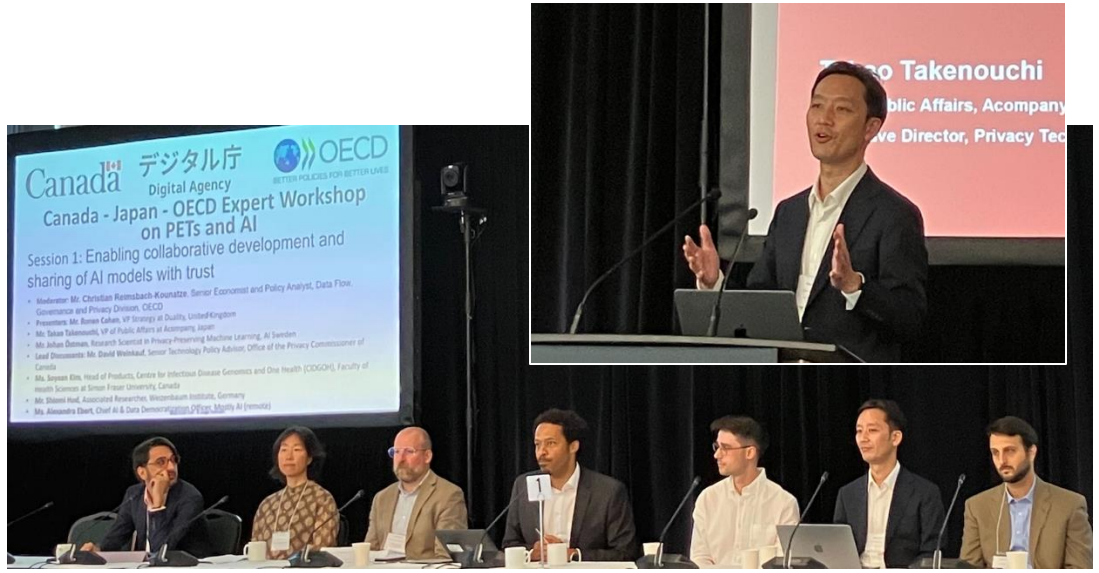
My Data Japan
2025年7月17日

自己紹介

■ 竹之内 隆夫 (たけのうち たかお)
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 IAP Expert Community



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

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　執行役員 AI・LLM事業部長）

賛助会員
特別会員

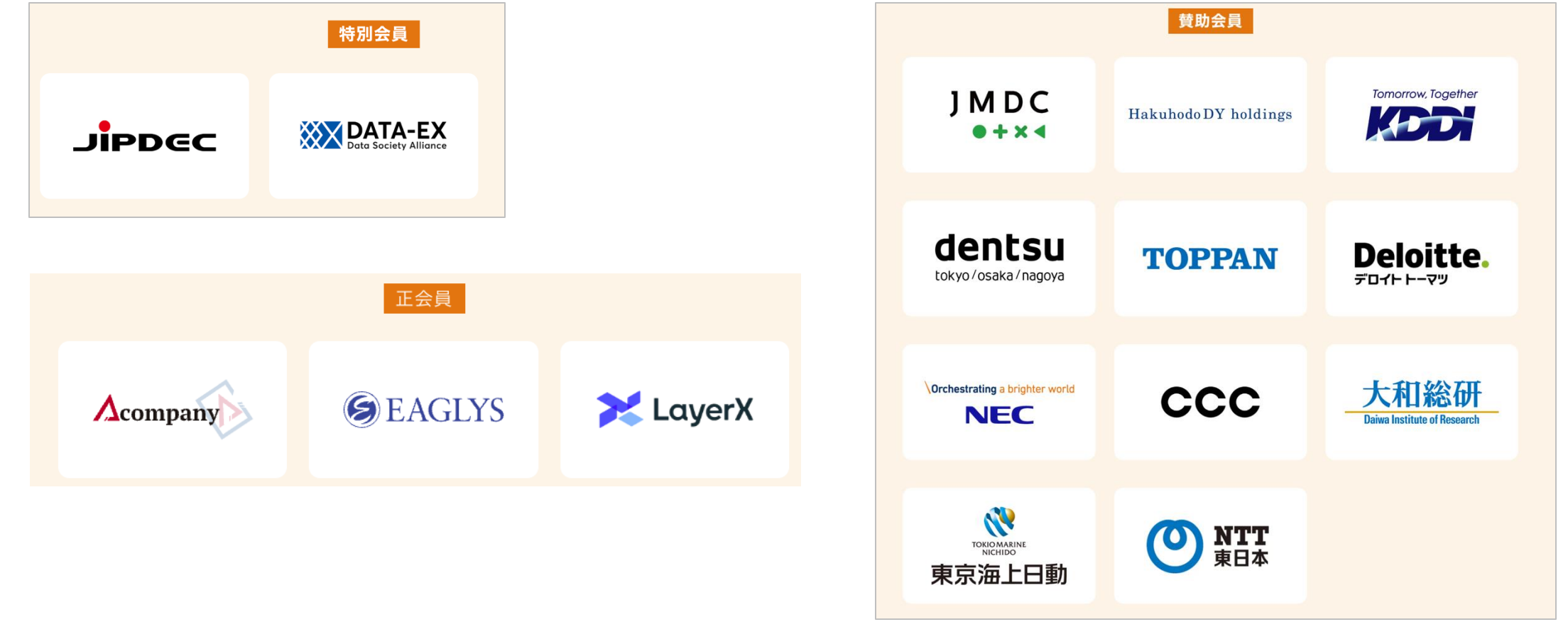
賛助会員：11社
特別会員：２団体

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）
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）
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）
須崎有康　（情報セキュリティ大学院大学 教授）

プライバシーテック協会の会員一覧

JIPDEC様、KDDI様など様々な団体・企業様と連携して活動



出典：プライバシーテック協会ホームページ, https://privacytech-assoc.org/#member

※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

プライバシーテック・PETs(Privacy Enhancing Technologies)とは

- プライバシーテック（PETs）とは、プライバシーを保護する技術の総称
- 特に「秘密計算」という技術が注目されている

PETsの一例と、PETsの適用場面

データ収集 → データ保管 → データ分析 → データ活用

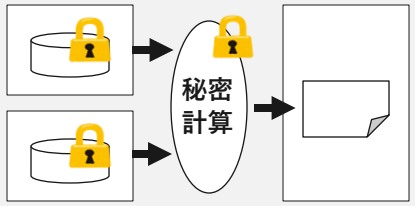
匿名化・仮名化

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

秘密計算

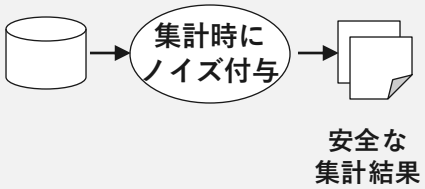
データを開示せずに暗号化したまま分析・学習が可能



本日の対象

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



合成データ

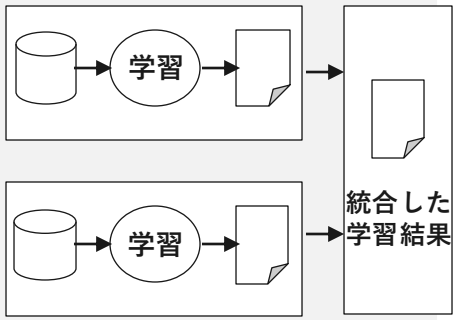
元の特徴を維持した擬似データを生成

28	男	174
31	女	164
55	男	172

27	男	176
32	女	162
54	男	171

連合学習

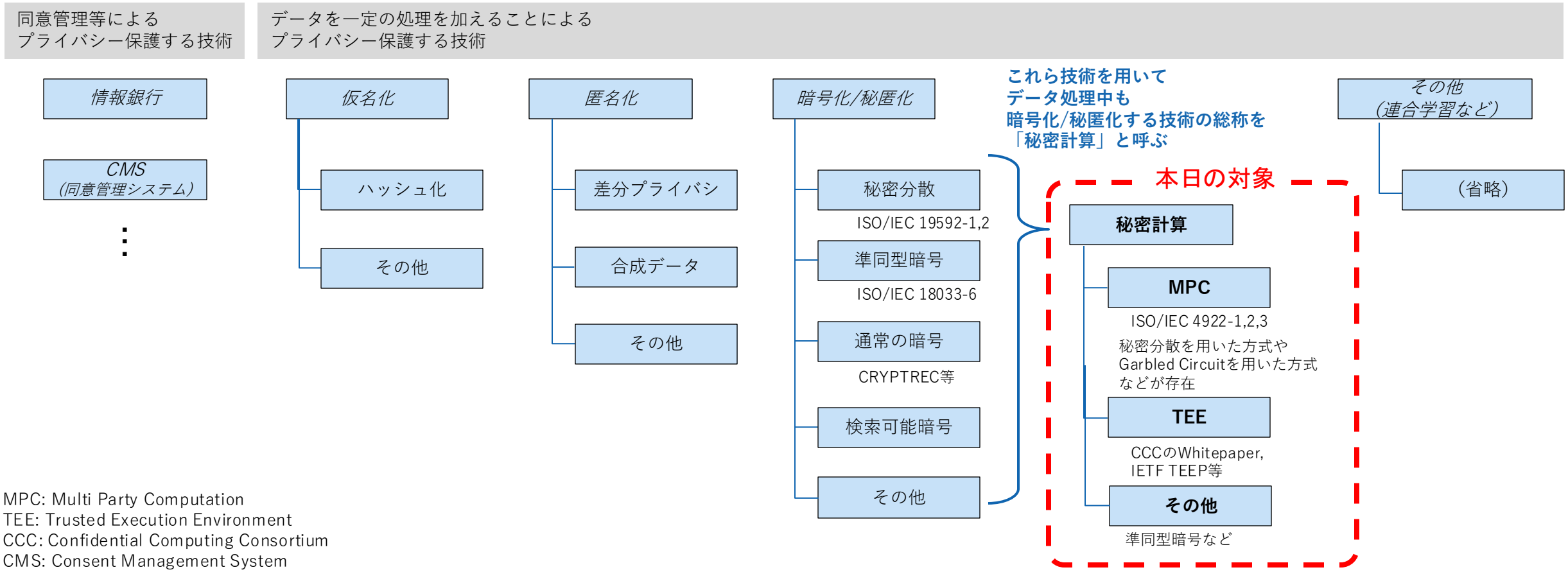
データを収集せずに学習結果のみを中央で統合



参考：代表的なPETsと「秘密計算」の位置付け

- データ処理中も暗号化/秘匿化する技術の総称を、いわゆる「秘密計算」と呼ぶ

図：主なPETsの類型



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

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	o		o		o
	合成データ	o	o	o	o	o
	差分プライバシー	o	o	o	o	o
	ゼロ知識証明	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
	準同型暗号（準同型暗号を用いた秘密計算）	o	o	o	o	o
	TEE（TEEを用いた秘密計算）	o	o	o	o	o
連合・分散分析技術	連合学習	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

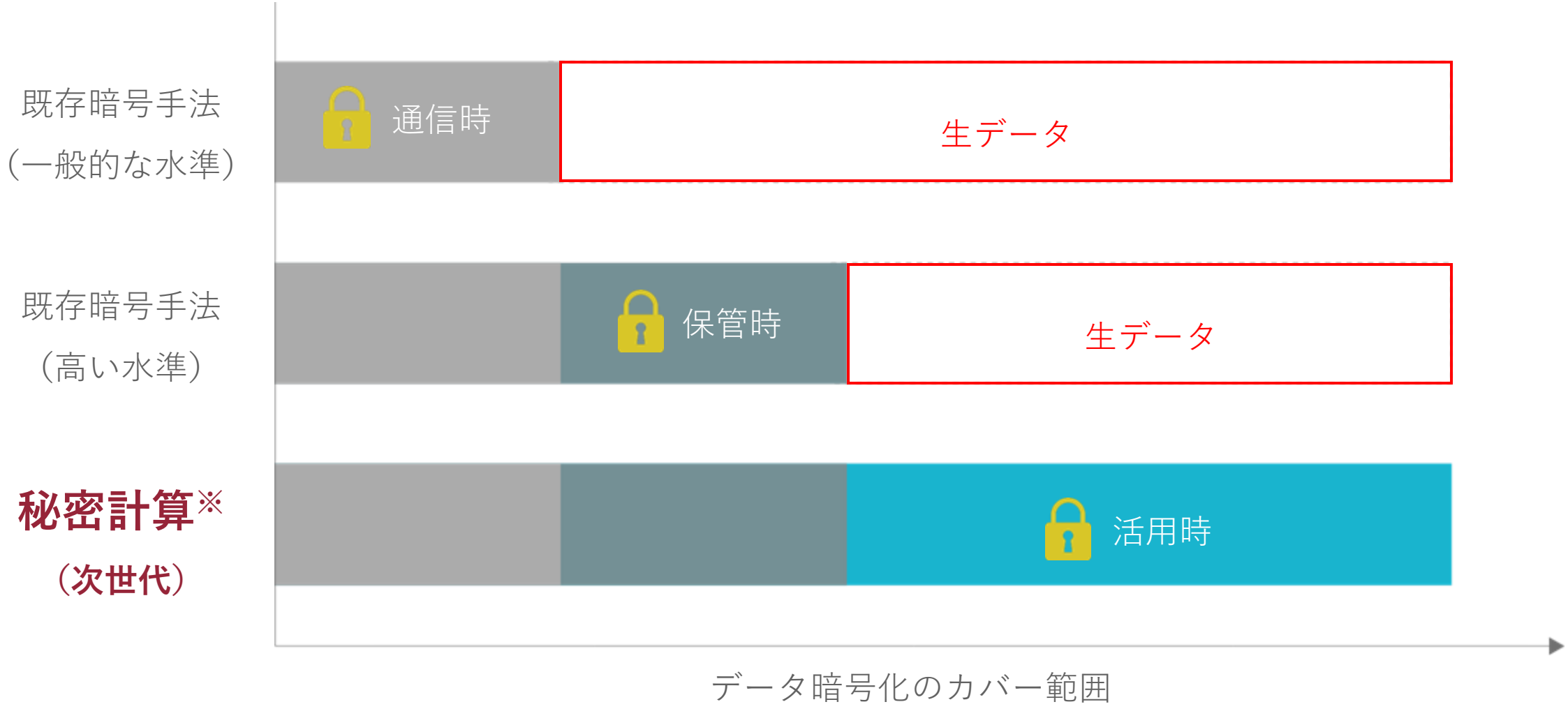
秘密計算とは

- 秘密計算とはデータを暗号化(秘匿化)したまま処理できる技術※1

PETs：Privacy Enhancing Technologies(プライバシー強化技術)、プライバシーテックとも言う
※1 本資料の「秘密計算」は、秘匿しながら処理できる技術の総称としている。「秘匿計算」などとも呼ぶ

秘密計算と従来の暗号技術との比較

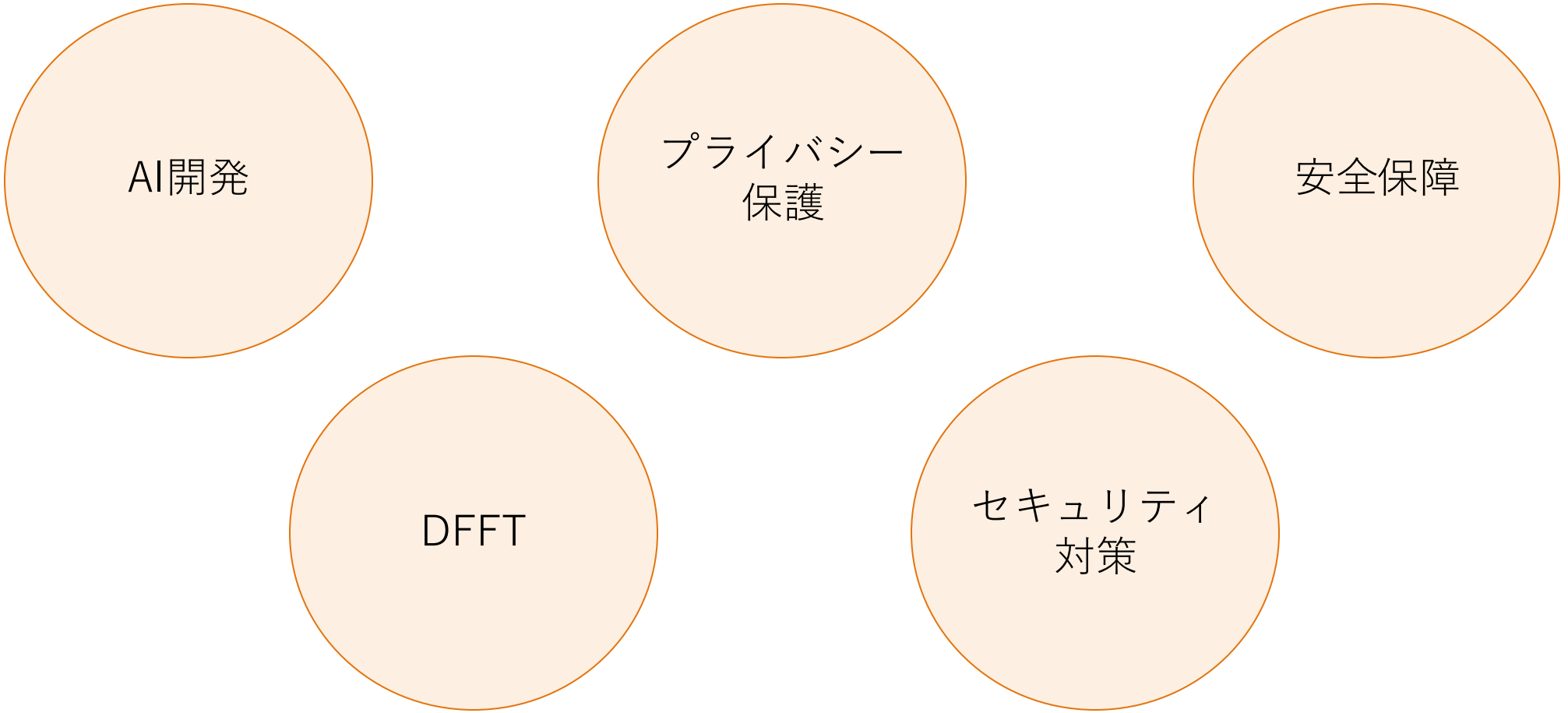
- 秘密計算も用いることで、秘匿化したままのデータ活用が可能



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

秘密計算への期待

- 秘密計算は、AI開発を含む様々な分野で期待されている

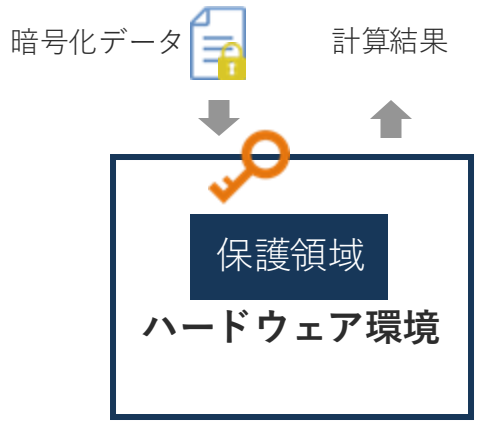
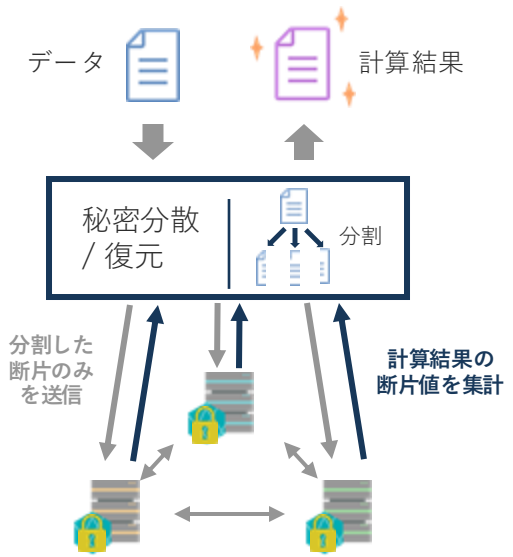
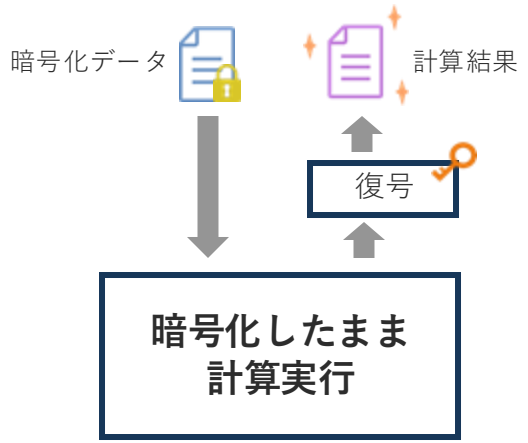


DFFT: Data Free Flow with Trust

TEE: Trusted Execution Environment
MPC: Multi-Party Computation
HE: Homomorphic Encryition

秘密計算の方式例

- 幾つかの方式が存在するが、ハードウエアを用いた方式は比較的高速

方式	TEE/機密コンピューティング※1 （ハードウェアを利用）	MPC （秘密分散を利用）	HE （準同型暗号を利用）
概要			
セキュリティ	**チップベンダーに依存** サイドチャネル攻撃	**管理者の結託**による 漏洩リスク	**暗号鍵の管理不備**による 漏洩によるリスク
速度※2	◎ 平文とほぼ同等	△ 数倍～数十倍程度低下	△ 数百倍以上低下

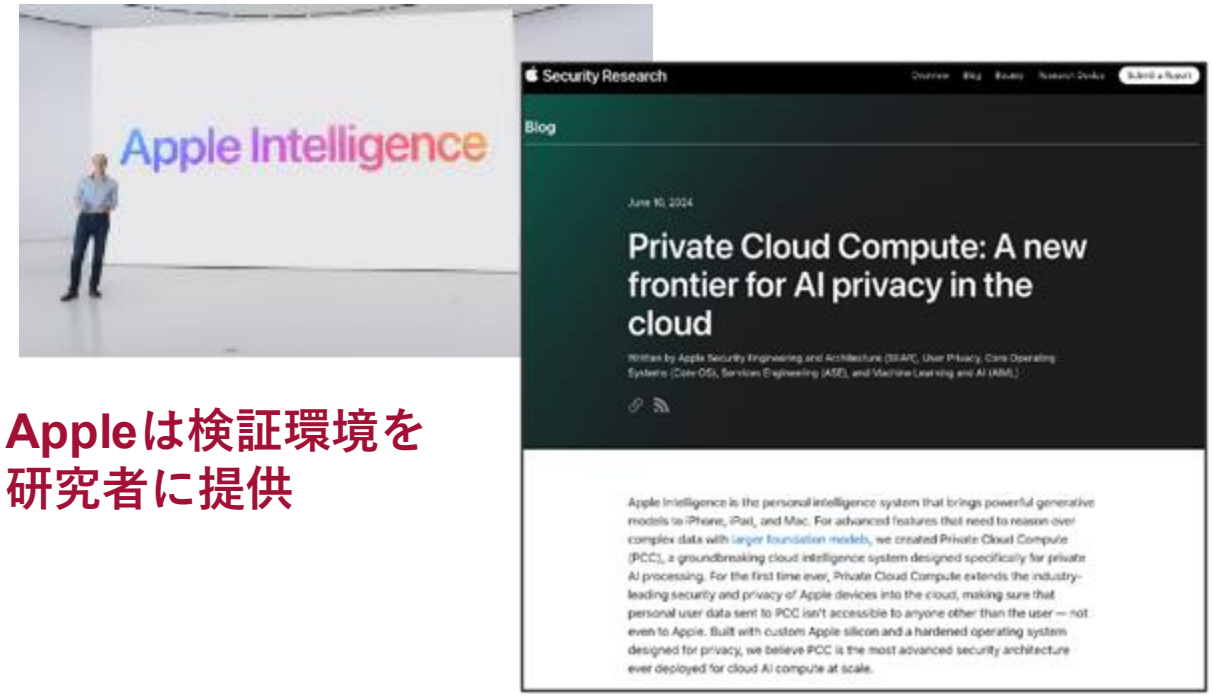
※1 TEEは処理中のメモリ内のデータが暗号化されているため、秘密計算の一種として記載
※2 方式、環境、処理内容などに依存するため参考値として記載
通常のCPUが3.00GHzで256 binary gate/clkと仮定すると、秒間768 * 10^9論理回路[gate / sec]実行できるとして、速度低下の度合いを参考値として概算。数年前の参考値として、 [1]では、Honest-majorityでsemi-honest安全な秘密分散の秘密計算が約7 billion [gate/sec]で約7 * 10^9[gate/sec] 。NuFHEのGPUでの計測 [2] によると、約0.35 [msec / gate] ≒ 2857[gate / sec]で約2 * 10^3[gate/sec] 。

[1] Toshinori Araki, Jun Furukawa, Yehuda Lindell, Ariel Nof, Kazuma Ohara, "High-Throughput Semi-Honest Secure Three-Party Computation with an Honest Majority", ACM CCS 2016, https://eprint.iacr.org/2016/768.pdf
[2] NuCypser, “NuCypher fully homomorphic encryption (NuFHE) library implemented in Python https://nufhe.readthedocs.io/en/latest/”, https://github.com/nucypher/nufhe

AI処理も可能な秘密計算（TEE/機密コンピューティング）

- 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

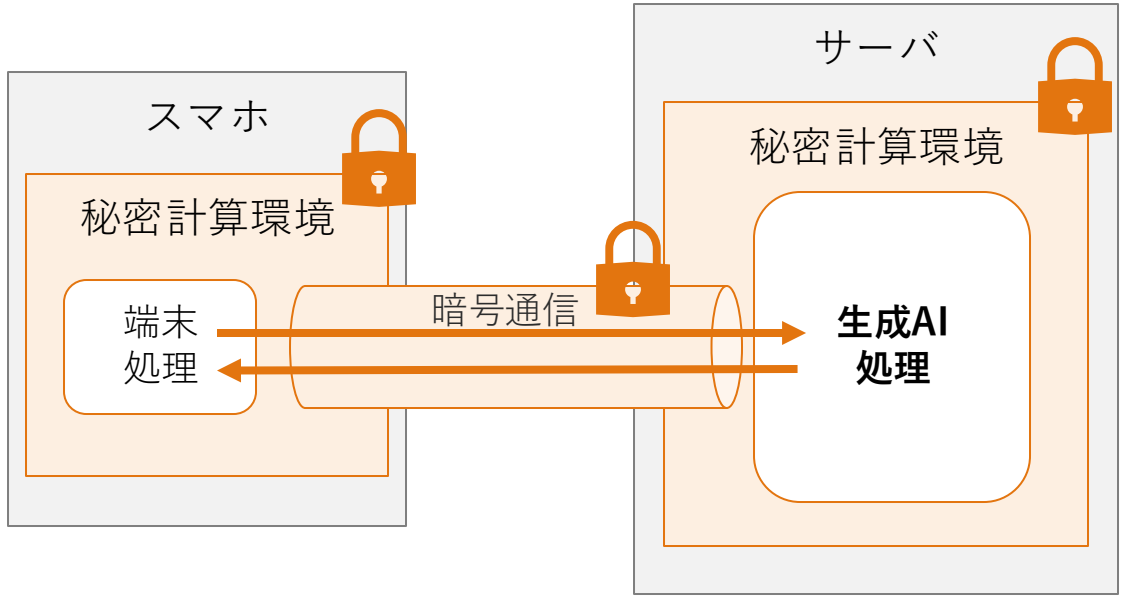


Appleは検証環境を研究者に提供

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

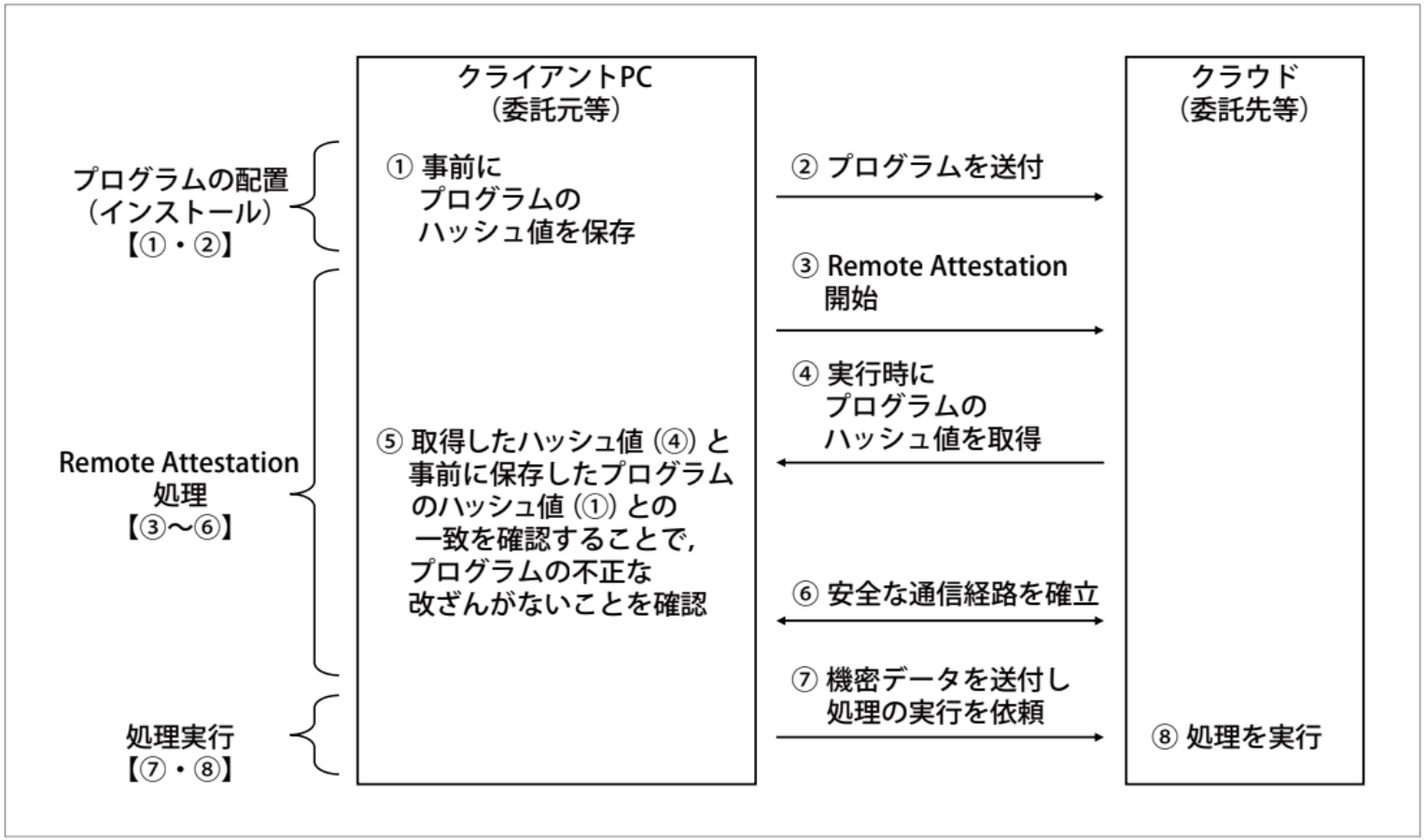
重たい処理をサーバで秘密計算で安全に処理



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/

リモートアテステーション機能（コードの完全性）

- 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

個人情報保護法の改正議論と PETsによるガバナンス

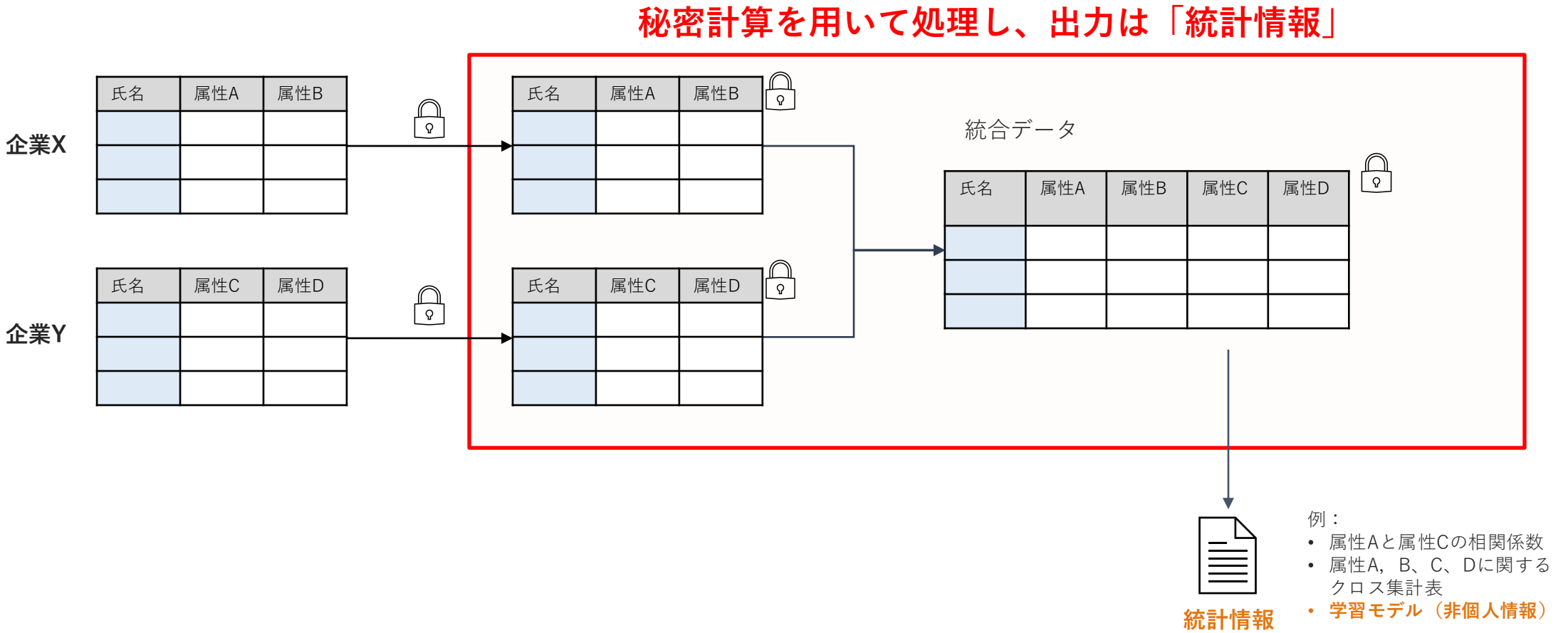
出典：プライバシーテック協会スライド

プライバシーテック協会からの提言内容

以下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することを提言

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



個人情報保護委員会の公式文書

2025年3月5日発表　個人情報保護法の制度的課題に対する考え方（案）について

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

統計情報等の作成のために、複数の事業者が持つデータを共有し横断的に解析することが、本人同意なき個人データの第三者提供が可能と明記

「統計情報等」には、AIモデルも含まれる

「統計情報等の作成にのみ利用されることを担保」するため、現行の個人情報保護法における安全対策とは別で、ガバナンスのための規律が設けられる想定

国会における議論

4月の国会の答弁においても、技術を活用する方針で言及

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**今ものすごくPrivacy Enhancing Technologies(PETs)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の政府参考人の皆様にご意見を承りたいと思います。

個人情報保護委員会 佐脇事務局長

PETsといったもののですね、 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 違反行為を施策を検討するといったことが重要だ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、今回の技術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、 引き続き対話をもかせながら検討してまいりたいと思います。

出典：2025年4月18日内閣委員委員会「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=

参考：現行法でのデータ突合分析の事例

- 現行法でも突合分析が可能な方式は存在（準同型暗号やTEEやk-匿名化等を利用）
- 本方式はデータの曖昧化の処理が必須であるため分析精度は低下する

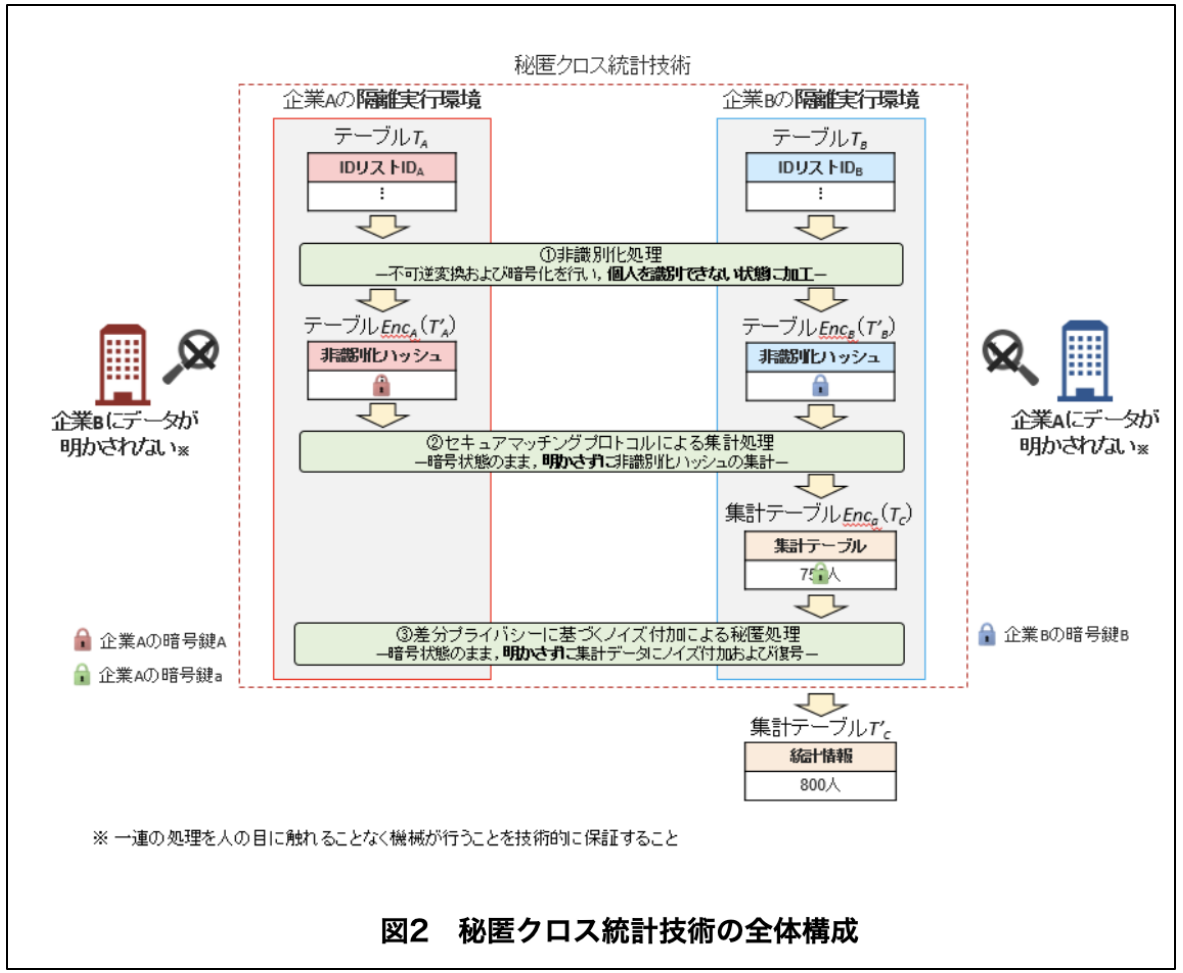


図2　秘匿クロス統計技術の全体構成

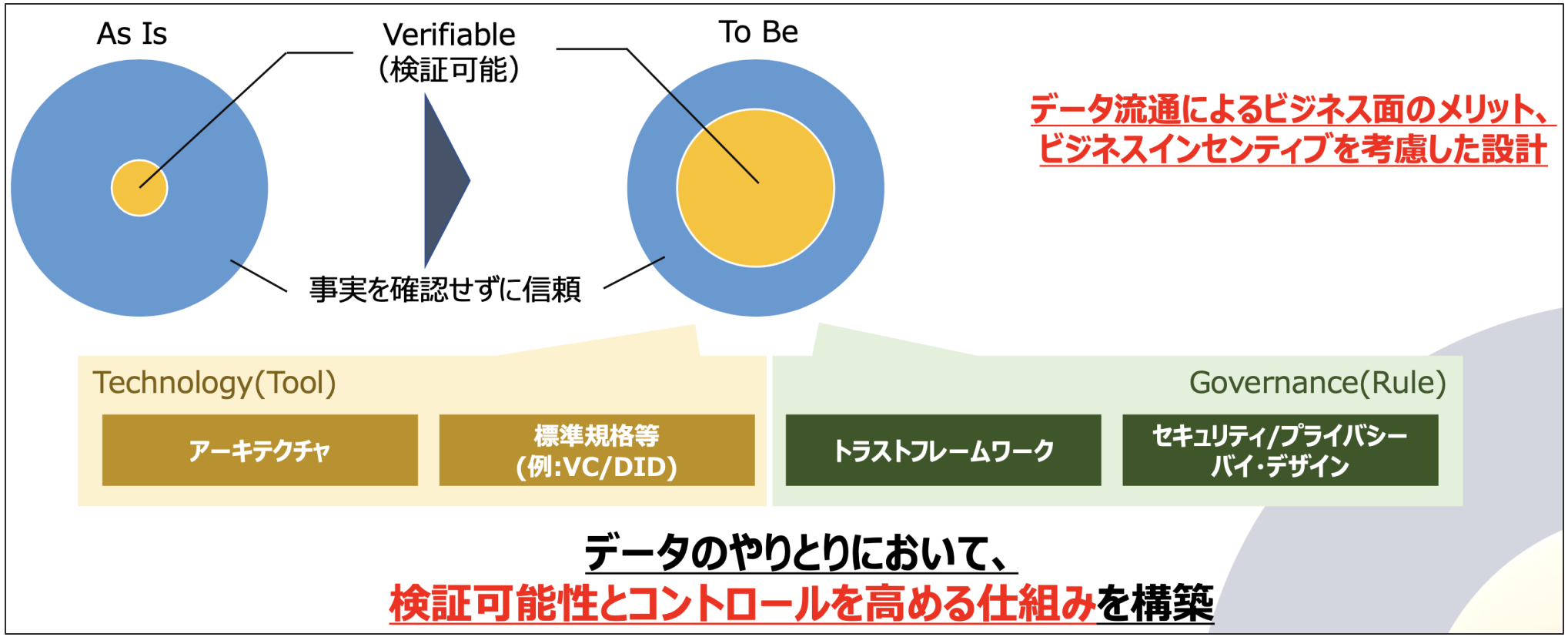
出典：秘匿クロス統計技術特集 ―企業横断の統計的なデータ活用による社会課題解決―, NTTドコモ・テクニカル・ジャーナル Vol.31 No.1（Apr.2023）
https://www.docomo.ne.jp/corporate/technology/rd/technical_journal/bn/vol31_1/index.html

参考：PETsによるトラスト（≒ガバナンス）

トラストはVerifiable（検証可能）が必要

- トラスト(Trustworthiness)は、**Verifiable（検証可能）**であるべき
- 技術だけでなく、ガバナンス・ルールも必要

日本政府の「Trusted Web」における検討でも、「Verifiable」はキーワード



出典：“Trusted Web ホワイトペーパーver.3.0概要”, https://trustedweb.go.jp/documents/

AI時代のトラスト

- 特にAI処理においては、IDや属性だけでなく、**処理基板のトラスト**が重要

表：トラストの対象とそのための技術

トラストの対象	トラストを支える技術/PETs等
処理基盤	Confidential Computing (TEE/機密コンピューティング)
Data Integrity / Authenticity	Verifiable Credentials, Digital Signatures,…
Data Confidentiality	MPC (Multi-Party Computation), Homomorphic Encryption,…
Counterparty	PKI, Trust Frameworks,…
…	…

AI処理で
特に重要