資　料　3
令和８年２月２日
第２回個人情報保護政策に関する懇談会

プライバシーガバナンスとPETs

2026年2月2日
NTT(株) 社会情報研究所
高橋克巳

あらまし

- **（話題１）プライバシーガバナンス**を運用寄り観点からまとめた
  - プライバシーガバナンスは**企業の信頼の確保（経営の基盤づくり）**として進められており、まずは**リスク回避**の文脈から理解が始まっているところである

- **（話題２）**一方、**プライバシー強化技術（PETs）**が注目を集めている
  - PETs: Privacy Enhancing Technologies
  - できるだけ**わかりやすく体系的なPETsの説明**を試みる

- **（話題３）PETsの貢献**
  - PETsがプライバシーガバナンスへどのように貢献するのかの考察
  - データの**機密性・個人識別性**の向上
  - **データライフサイクル・トラスト**との関係

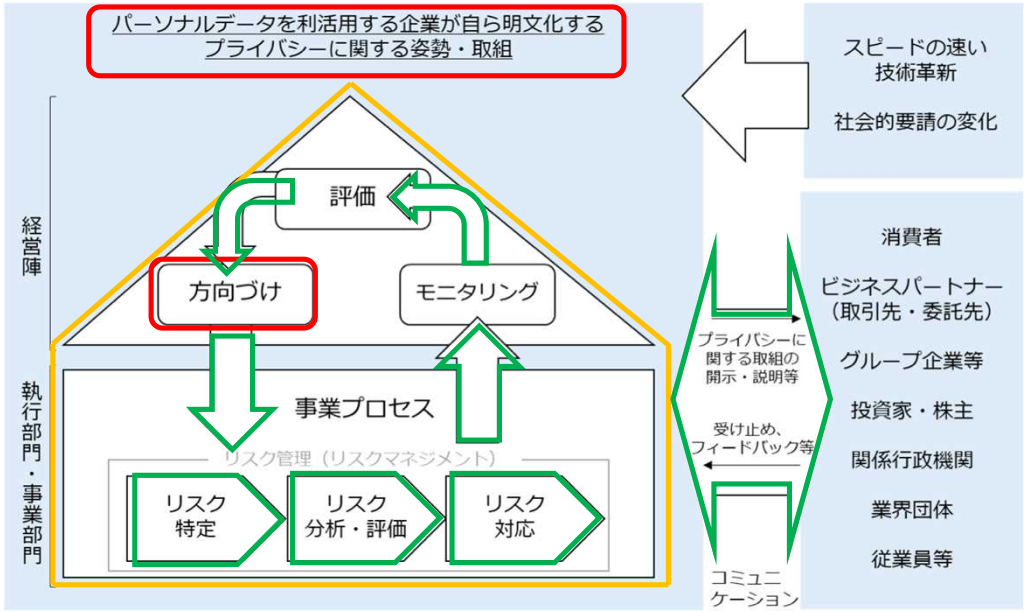
プライバシーガバナンス

話題 1

プライバシーガバナンスとは

- 「プライバシー問題のリスク管理と信頼の確保に向け、経営者がコミットし、組織の体制を構築・機能させること」*1
- その中核要素は下記
  - ルール（方針・規程）
  - 体制（責任）
  - 運用（リスク管理）の整備
    - 運用の要素は以下

利用の妥当性
利用目的
適切な処理
利用条件
本人権利への対応
インシデント対応

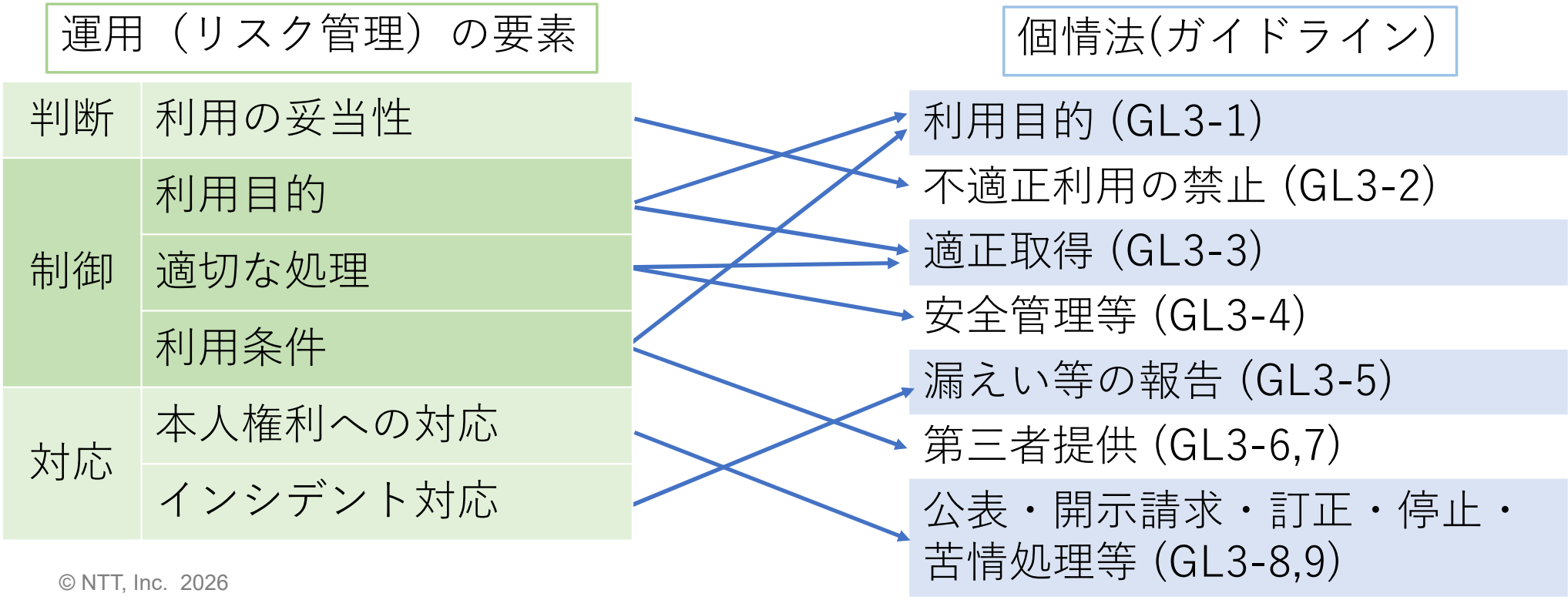


図表 4 プライバシーガバナンスのフレームワーク（イメージ）
※色枠は筆者が加筆

*1) DX時代における企業のプライバシーガバナンスモデルガイドブックver1.3（令和5年4月25日改訂）
https://www.meti.go.jp/policy/it_policy/privacy/guidebook_ver1.3.pdf

プライバシーガバナンスの運用（リスク管理）と個情法との対応

- 運用の要素は、大きく判断、制御、対応に分けられる
- 利用の妥当性とは利用のあり方の点検で、その前提として利用の是非判断がある
- 運用要素と我が国の個人情報保護法との対応は以下のとおり



プライバシー原則

OECD プライバシーガイドライン８原則[*1]と ISO プライバシーフレームワーク[*2]

- プライバシーガバナンスの要素および各国のデータ保護法の基礎となっている

1. Collection Limitation/収集制限の原則→ ISOではData Minimization を外出し
2. Data Quality/データ内容の原則→ ISOでは Accuracy and Quality と明確化
3. Purpose Specification/目的特定の原則→ ISOでは Purpose legitimacy and specification と明確化
4. Use Limitation/利用制限の原則→ ISOでは Use, retention and disclosure limitation に拡大
5. Security Safeguards/安全保護の原則
6. Openness/公開の原則→ ISOでは Openness, transparency and noticeと明確化
7. Individual Participation/個人参加の原則→ ISOでは Individual participation and accessと明確化
8. Accountability/責任の原則→ ISOでは Accountability + Privacy complianceに分解

- なおISOでは収集や利用に分散していた Consent and choice を独立整理

*1 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
*2 ISO/IEC 29100:2024 Information technology — Security techniques — Privacy framework

プライバシーガバナンス（小括）

- プライバシーガバナンスとは「プライバシー問題のリスク管理と信頼の確保に向け、経営者がコミットし、組織の体制を構築・機能させること」
  - プライバシーガバナンスの中核要素はルール(方針・規程)、体制(責任)、運用(リスク管理)の整備
  - 運用の要素は、利用の評価、利用目的、適切な処理、利用条件、本人権利への対応、インシデント対応
- 我が国の実務では
  - リスク回避、特に適切な利用(安全管理)や利用目的(による制限)を軸に運用に力が入れられている
  - データ活用における判断軸、とりわけ利用の是非判断をどう扱うかはこれからと考えられる

PETs
Privacy Enhancing Technologies

話題 2

PETsとは何か？

- 下記の総称として捉えられている
  - 仮名化、匿名化、統計化、差分プライバシー、合成データ(以上統計的開示抑制)、MPC、準同型暗号(以上秘密計算)、TEE、連合学習ら
  - まじめに定義を考えだすと、プライバシーを強化するのか疑問なものもある（使い方次第でもある）
- PETs (Privacy Enhancing Technologies) の定義
  - アカデミックな定義はない
  - OECDなどの定義がある
  - 国際規格での定義はない
    - PETsの具体的技術のいくつかが標準化されていることはある
- 分類の観点がいろいろある
  - 複数の異なる観点で語られている
  - その結果、共通理解が醸成されていないことも
- 本資料の内容
  - 代表的な政策文書のサーベイを行い、分類観点と定義をまとめる
  - 代表的なPETsを列挙する

PETs関連の主要報告書

- OECD (2023)
  - Emerging privacy-enhancing technologies: Current regulatory and policy approaches
  - PETsの類型と政策動向のまとめ
- ENISA, EU (2022)
  - Data Protection Engineering
  - データ保護原則を技術で実装する方法
- ICO, UK (2023)
  - Privacy-enhancing technologies (PETs)
  - PETsは制度上、何の役に立つのか
- NSTC, US (2023)
  - National Strategy to Advance Privacy-Preserving Data Sharing and Analytics
  - プライバシーを前提にデータを社会の力に変えるための国家戦略
- 参考 内閣府 文部科学省 (2023)
  - 「セキュアなデータ流通を支える暗号関連技術（高機能暗号）」に関する研究開発構想
  - PETsの研究開発構想 (※報告書ではありません)

OECD (2023)

- Emerging privacy-enhancing technologies: Current regulatory and policy approaches
  - https://doi.org/10.1787/bf121be4-en
- PETsの類型と政策動向のまとめ
- 取り上げられているPETs
  - Data obfuscation tools (ぼかす)
    - Anonymisation / Pseudonymisation, Synthetic data, Differential privacy, Zero-knowledge proofs
  - Encrypted data processing tools (暗号)
    - Homomorphic encryption, Multi-party computation, TEE
  - Federated and distributed analytics (連合/分散)
    - Federated learning, Distributed analytics
  - Data accountability tools (説明責任対応)
    - Accountable systems, Threshold secret sharing, Personal data stores / Personal Information Management Systems

ENISA (European Union Agency for Cybersecurity) (2022)

- Data Protection Engineering
  - https://www.enisa.europa.eu/publications/data-protection-engineering
- データ保護の原則を「データ保護バイデザインおよびバイデフォルト」へ実装するための実務者向け技術情報
- 取り上げられているPETs
  - Anonymisation and pseudonymisation (匿名化・仮名化)
    - Anonymisation, k-anonymity, Differential privacy, Selecting the anonymisation scheme
  - Data masking and privacy-preserving computations (暗号等)
    - Homomorphic encryption, Secure multiparty computation, TEE, Private information retrieval, Synthetic data
  - Access, communication and storage (アクセス制限等)
    - Communication Channels (End to end encryption), PE access control, authorization and authentication (PE attribute-based credentials, ZKP)
  - Transparency, intervenability and user control tools (透明性等)

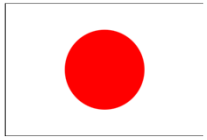
ICO (2023)

- Privacy-enhancing technologies (PETs)
  - https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/
- 企業のデータ保護責任者向けに、PETsがデータ保護法遵守にどう役立つのか、およびPETsの技術情報の提供
- 取り上げられているPETs (分類学は提示されていない)
  - Differential privacy, Synthetic data, Homomorphic encryption (HE), Zero-knowledge proofs, TEE, Secure multiparty computation (SMPC), Private set intersection (PSI), Federated learning
- プライバシータイプとして以下を提示
  - input privacy / output privacy

NSTC (2023)

- National Strategy to Advance **P**rivacy-**P**reserving **D**ata **S**haring and **A**nalytics
  - https://www.nitrd.gov/pubs/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf
- プライバシーを前提にデータを社会の力に変えるための国家戦略
- 取り上げられているPETs (PPDSA)
  - Data anonymization and statistical disclosure limitation techniques (匿名化・統計的開示抑制)
    - k-anonymity, Differential privacy, Synthetic data
  - Cryptographic techniques (暗号)
    - Secure multiparty computation, Homomorphic encryption, Zero-knowledge proof, Functional encryption
  - TEE
  - Policy-based approaches (ポリシーベース)
  - Other approaches
    - Privacy-preserving record linkage, Private information retrieval, Federated learning

内閣府 文部科学省 (2023)



- 「セキュアなデータ流通を支える暗号関連技術（高機能暗号）」に関する研究開発構想
  - https://www8.cao.go.jp/cstp/anzen_anshin/4_20231225_mext.pdf
- セキュアなデータ流通を実現するために、データ流通のライフサイクル全体でデータを保護する技術獲得のための研究開発構想
- 分類
  - 暗号技術
  - 暗号処理を安全に実行する環境技術（TEE 等）
  - 統計的開示抑制技術（SDC）

PETsの定義

- OECD (2023)
  - PETs are digital solutions that allow information to be collected, processed, analysed, and shared while protecting data confidentiality and privacy.
    - 機密性とプライバシーを守りながらデータ処理を可能にする
- ENISA (2022)
  - 定義なし
  - 参考：Data Protection Engineering can be perceived as part of data protection by Design and by Default.
    - データ保護バイデザイン・バイデフォルト
- ICO (2023)
  - Data protection law does not define PETs.
  - PETs are technologies that embody fundamental data protection principles by: minimising personal information use, maximising information security; or empowering people. - 個人情報の利用を最小化・セキュリティを最大化
- NSTC (2023)
  - PPDSA methods and technologies can unlock the beneficial power of data analysis while protecting privacy.
    - プライバシーを保護することでデータの価値をアンロック

PETsの定義

- PETsとは、個人データの取扱いを、目的やリスクに応じて精緻化し、その妥当性を法や社会に照らして説明可能にする技術群である
  （報告者による定義）
  - Enhance は Protect ほど強くはない語であるが、やはり「もっと強化を」に聞こえる
  - バランスの取れたプライバシー保護を標榜・表現したい

PETs分類学（一覧、詳しくは後続ページで説明）

① 工学的
- 暗号系、統計系、分散計算系、セキュアハードウェア系

② 保護性質
- 機密性、個人識別耐性

③ データライフサイクル：どの段階で効くか
- 収集、保存、処理・分析、共有・二次利用、公開

④ トラスト（脅威）：どの主体を信頼しないか
- 事業者を疑う、第三者を疑う、協調参加者を疑う

⑤ 説明責任・透明性
- 利用条件、適切な処理方法、利用目的が守られているかの説明

PETsと呼ばれている技術の例 1/3

- 仮名化（Pseudonymisation）
  - 個人識別子を分離し、直接的に個人を特定できないようにする。
- 匿名化（Anonymisation）
  - 個人を識別できないようデータを不可逆的に加工する。GDPRなどで個人データに該当しないと扱われる場合がある。
- 統計化（Aggregation）
  - 個票データを集計し統計的表現に変換する。
- 差分プライバシー（Differential Privacy, DP）
  - 特定の個人が含まれているかどうかを推測できないようにするために、統計出力にノイズを加える。
- ローカル差分プライバシー（Local Differential Privacy, LDP）
  - 特定の個人がどのような値を入力したかが推測できないようにするために、送信前のデータに各個人がノイズを加える。
- 合成データ（Synthetic Data）
  - 元データの統計的特性を保ちながら人工的に生成したデータ。
- 統計的開示抑制（SDC : Statistical Disclosure Control）
  - データを加工することにより、データが個人に与える影響を減じる。本ページの技術の総称。

PETsと呼ばれている技術の例 2/3

- 準同型暗号（Homomorphic Encryption, HE）
  - 暗号化したまま加算や乗算などの演算を行える暗号技術。
- マルチパーティ計算（Multi-Party Computation, MPC）
  - 複数の当事者がデータを秘匿したまま共同で計算し、最終結果のみを共有できる技術。
- 秘密計算（Secure Computation）
  - 暗号技術により、データを復号せずに計算を行う方式の総称。MPCやHEなどを含む。
- PSI（Private Set Intersection）
  - 複数主体が保有するデータ集合の共通部分のみを計算し、それ以外の情報を開示しない。
- 関数型暗号／属性ベース暗号（Functional / Attribute-Based Cryptography）
  - 復号可能条件や取得可能な計算結果を暗号文に埋め込む暗号方式。
- 属性ベース証明 Attribute-based Credentials（ABCs）
  - 属性情報に基づく選択的開示を可能にする認証・証明技術。
- ゼロ知識証明（Zero-Knowledge Proofs, ZKP）
  - ある命題が真であることだけを暗号学的に示す技術で、データを渡さずに条件確認できることが期待されている。
- 高機能暗号
  守秘・署名らにおさまらない機能を持つ暗号。本ページの技術の総称。

PETsと呼ばれている技術の例 3/3

- Trusted Execution Environment（TEE）
  - CPU内の隔離領域でプログラムとデータを保護し、安全に実行する技術。
- データクリーンルーム（Data Clean Room, DCR）
  - 複数主体のデータを隔離環境で分析し、統計的結果のみを外部に出力する仕組み。技術的担保はTEEや暗号技術に依存する場合がある。
- 連合学習（Federated Learning, FL）
  - 生データを各主体が保持したままモデルを協調的に学習する方式。単体ではPETs機構を内包しない。
- オンデバイス処理（On-device Processing）
  - 端末内で前処理や統計化を行い、サーバーには加工済みデータのみを送信する方式。
- その他、セキュリティ技術一般はPETsとみなされうる（データセキュリティの確保はプライバシー保護の一環であるため）
  - 暗号技術：データの機密性
  - 認証技術：データのアクセス管理
  - いわゆるネットワークセキュリティ：データの機密性（漏えい対策）等

PETs分類学（詳細）

①工学的
- 暗号系
  - 秘密計算（MPC/準同型暗号）
- 統計的系
  - 仮名化、匿名化、統計化、差分プライバシー、合成データ
- 分散計算系
  - 連合学習
- セキュアハードウェア系
  - TEE

②保護性質
- 機密性
  - 秘密計算（MPC/準同型暗号）、TEE
- 個人識別耐性
  - 仮名化、匿名化、統計化、差分プライバシー、合成データ
  - 連合学習？

PETs分類学（詳細）

③データライフサイクル：データのどの段階で効くか

- 収集
  - PETsの効能は限定的
  - ローカル差分プライバシー
  - オンデバイス処理や連合学習に親和性があると考えられている
- 保存
  - 暗号（準同型暗号、秘密分散（MPC））
  - 仮名化
- 処理・分析
  - 秘密計算（MPC/準同型暗号）、TEE
  - 連合学習
- 共有・二次利用：匿名化、合成データ
- 公開：合成データ、統計化、差分プライバシー

PETs分類学（詳細）

④トラスト（脅威）：どの主体を信頼しないか
- 事業者 (processor) を疑う
  - 見せてもいいデータにする→匿名化
  - 見せないでデータ処理する→秘密計算(暗号)、TEE
- 第三者を疑う
  - 見せてもいいデータにする→匿名化、統計化、差分プライバシー
- 協調参加者を疑う
  - 見せないでデータ処理→秘密計算(暗号)、TEE

⑤説明責任・透明性：プライバシー要件が遵守されているか
- 利用条件、適切な処理方法、利用目的が守られているかの説明
  - ログ管理
  - ゼロ知識証明やTEEのリモートアテステーションに期待

PETsは
プライバシガバナンスへ
どのように貢献するか

話題 3

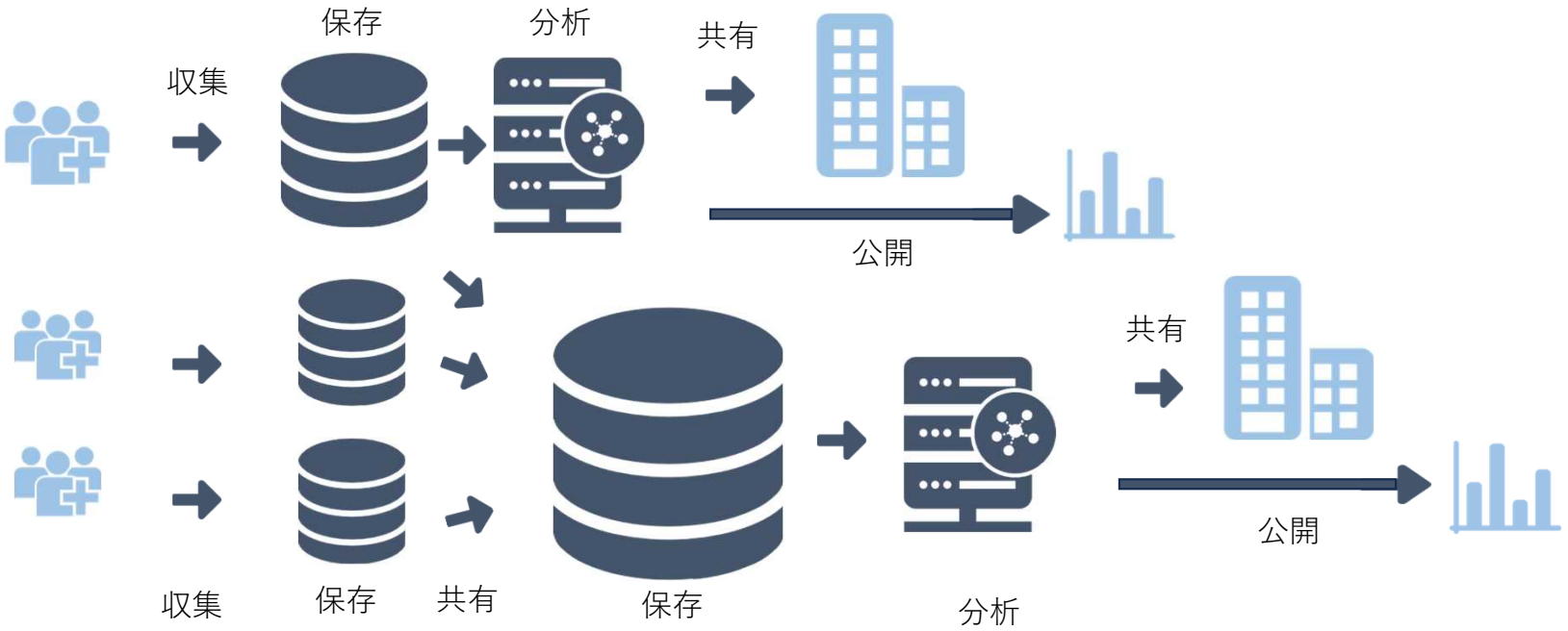
PETsのプライバシーガバナンスへの貢献

- PETsは特にリスクを管理する運用に貢献する
- 運用をPETsとして固めれば、その部分は個別対応や属人的判断に依らず、バイデザインで回し続けられるようになる
- なお日本には匿名加工・仮名加工という、ある意味PETsによる法的特例がある
- しかしPETsの価値はリスク空間の限定、運用の軽減、説明性の向上にある
  - この部分はデータの機密性の確保が機械的にできている
  - この先はデータの個人識別性を気にすることがない
- さらには事業者がPETsを含んだリスク評価とリスク固定を自主的に行い、彼ら自身でデータ利用の是非を主体的に判断し、説明できるようになる姿が望ましい

代表的なPETs	できること	貢献例
仮名化	データから個人識別子を分離し、直接的には個人を特定できないようにする	• 安全管理がやや楽に • 利用目的の変更@仮名加工
匿名化、統計化、差分プライバシー	データを統計的・確率的に粗くし、個人に与える影響を減じる	• 個人から集団としての統計的リスクにシフト • 個人データとしての管理を回避 • 利用目的・第三者提供の制限の解除@匿名加工・非個人情報
秘密計算、TEE	データを暗号等で「読めない」状態まま処理し、計算結果だけを得る	• 生データへの接触機会の制限 • データ共有の新しいガバナンス手段への期待
連合学習	生データを各主体が保持したままモデルを協調的に学習する	• データ移動の個人識別性軽減への期待

PETsの貢献 / データライフサイクル・トラスト

- どの段階のデータが機密になっているか？
- どの段階のデータが個人識別できなくなっているか？
- 誰を信じて、誰を信じないか？



この図はさまざまなデータの流通をイメージしていただくために作成したもの
個々のケースを描き出しPETsを当てはめることでレシピとなる

まとめ

- プライバシーガバナンスの中核要素はルール、体制、運用の整備
- 運用は、利用の妥当性、利用目的、適切な処理、利用条件、本人権利への対応、インシデント対応から構成される
- PETsは下記の総称である
  - 仮名化、匿名化、統計化、差分プライバシー、合成データ(統計的開示抑制)／MPC、準同型暗号(秘密計算)／TEE、連合学習ら
  - 定義（提案）：PETsとは、個人データの取扱いを、目的やリスクに応じて精緻化し、その妥当性を法や社会に照らして説明可能にする技術群である
- PETsは個人データの機密性と個人識別耐性を高め、リスク空間の限定、運用の軽減、説明性の向上に貢献する
- PETsをデータライフサイクルとトラストを考えて配置することが大事