金融分野における
AI利用と個人情報保護

2025年11月5日

片岡総合法律事務所
弁護士　高松志直

第１　視点の設定

※本資料全般の問題意識については、金融庁「AIディスカッションペーパー（第1.0版）」を踏まえた検討を行っている

学習・入力データとして自社の顧客情報を含む個人情報を扱うケース

- 具体例：マーケティング、信用スコア、不正検知など

- 生成AIだけではなく、むしろ従来型AIにおける検討が金融分野では従前から（主要な）論点として存在

- **顧客情報を詳細に分析する「深い」利用**となる点の考慮が必要。また、一般的・汎用的な分析と、顧客に対する評価・判断を伴う利用では、リスクが異なる。

生成AI利用時に顧客情報等の個人情報を含むプロンプトを入力するケース

- 具体例：従来業務の効率化やチャットボットなど

- 顧客の情報を利用するが、個人情報を深く分析するというよりは、**事務文脈で使わざるを得ないという「浅い」利用**となる傾向がある（もちろん「深い」利用としての事例もある）

- 個人情報保護法上の論点は「深い」利用も「浅い」利用も類似の枠組みとなるが、**利用方法によって検討の深度が異なる**

検討の枠組み

開発・学習・利用	外部との連携	実務利用時
利用目的①	第三者提供	要配慮個人情報
利用目的②	海外関係	プロファイリング

第２　個人情報保護法に関する論点

利用目的① － AIによる開発・学習

- 「AIによる開発・学習」が個人情報を収集した際の利用目的に明記されていなかった場合にどのような整理があり得るか

- 「統計データへの加工を行うこと自体を利用目的とする必要はありません。」（個人情報保護法QA2-5）→**「一般的・汎用的な分析の文脈」について確認的に言及**したもの

- （個別事情にはよるものの、）「AIによる開発・学習」も上記QAと同趣旨の文脈で利用目的への明記は不要と整理できるか（「深い」利用であっても）

- なお、関連して個人情報保護法改正の議論（AIとの関係では特に同意取得義務の例外の議論）

→「個人情報保護法の制度的課題に対する考え方について」（令和7年3月5日・個人情報保護委員会）

利用目的② －AIの利用

- 生成AIを利用した金融業務（事務）の効率化（「浅い」利用）に関し、利用目的上の配慮は必要か

- 「本人が、自らの個人情報がどのように取り扱われることとなるか、利用目的から合理的に予測・想定できないような場合は、この趣旨に沿ってできる限り利用目的を特定したことにはならない」（通則ガイドライン3-1-1(※1)）→**顧客の認識可能性を背景**にして「予測・想定」という基準を確認したもの

- 顧客において認識可能な枠組み（チャットボットによる生成AIの利用など）や、従来業務の単なる自動化は「合理的に予測・測定」できると評価してよいか

外部ベンダーとの連携①－第三者提供（委託先管理・安全管理）

- ベンダー連携に際し、連携先が個人情報を「取り扱う」のであれば、従来型AIも生成AIも個人情報の取扱いの委託に該当するのが原則（個人情報保護法QA7-53）

- AI利用の場合、**分析等の処理を行う場合**が多く、この点を考慮した検討を要する（規制改革ホットライン令和4年度回答307）

- 委託先に該当する場合、①委託先管理、②追加学習等の独自利用の制御（個人情報保護委員会注意喚起）などの対応を要する

- なお、AIディスカッションペーパー31頁の対応の具体例は委託先管理や安全管理の例示として一般的には適切なものが挙げられていると評価

外部ベンダーとの連携②－海外関連

- 海外にサーバーを置く生成AIプラットフォームを金融機関等が利用する場合、越境移転等の規律をどのように整理すべきか

- 越境移転規制の適否は、受領者が「外国にある第三者」かどうかによって定まる→サーバー所在地ではなく**事業者の所在地を軸に検討**する

- 越境移転規制の適用を受ける場合は基準適合体制の確認、そうでない場合も海外サーバを利用する等の場合には外的環境の把握等の対応を要する（通則ガイドライン10-2）

実務利用時

実務上の諸論点（要配慮個人情報・プロファイリング）

- 特に、マーケティング、信用スコア、不正検知など、「深い」利用を検討する場合、データセットの中に要配慮個人情報や金融分野における機微情報が含まれる可能性がある→**同意取得や金融分野ガイドラインの整理**を要する

- 「深い」利用で個人の属性を詳細に特定し、それをもとに一人ひとりに応じた対応（個別化された顧客対応）を行う場合、プロファイリングの当否という論点が生じる可能性がある→金融機関等として、**公平性やバイアスなどの問題**を学習・入力データの選択、通知・公表、個人データの開示等の文脈で検討することも想定される（ビジネス設計段階から熟慮が必要）

EOF

プライバシーテック協会

PETs(Privacy Enhancing Technologies)のご紹介

プライバシーテック協会 事務局長
竹之内 隆夫

※PETsは、プライバシーテックとも呼ばれます

第3回 金融庁 AI官民フォーラム
2025年11月5日

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：15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）

※PETsとプライバシーテックは呼び方の違いであり、同様な技術を指します

PETs(Privacy Enhancing Technologies) とは

- PETsとは、プライバシーを保護する技術の総称
- **様々な技術が存在**し、組み合わせて利用することも有効

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

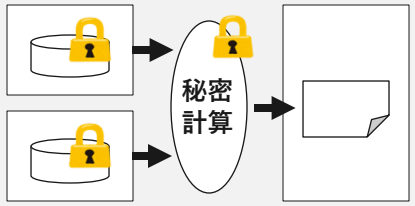
匿名化・仮名化

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

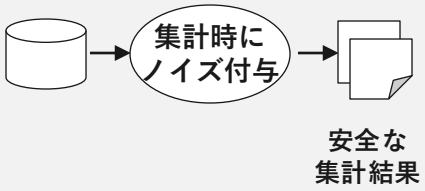
秘密計算

データを開示せずに暗号化したまま分析・学習が可能



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

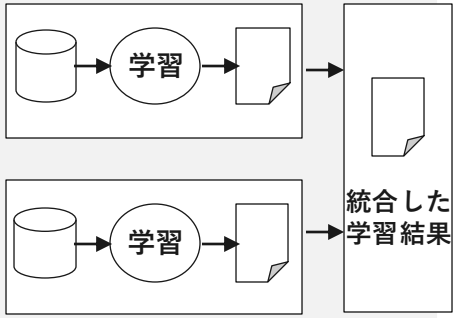
元の特徴を維持した擬似データを生成

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



海外の規制動向：EUの金融分野

- EUでは、特に**「秘密計算」（処理中の暗号化）**は、リスクに応じた適用検討が必要

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））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

AI活用におけるPETsのユースケース

① **個人情報保護法**における技術的ガバナンス

② 複数機関での**データ連携**

③ **AI活用**のリスク低減

① 個人情報保護法における技術的ガバナンス

- 個人データを統計目的で利用する場合には、第三者提供の同意を不必要とする枠組みが検討されている
- この処理における、**ガバナンス強化にもPETsが有効**

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。

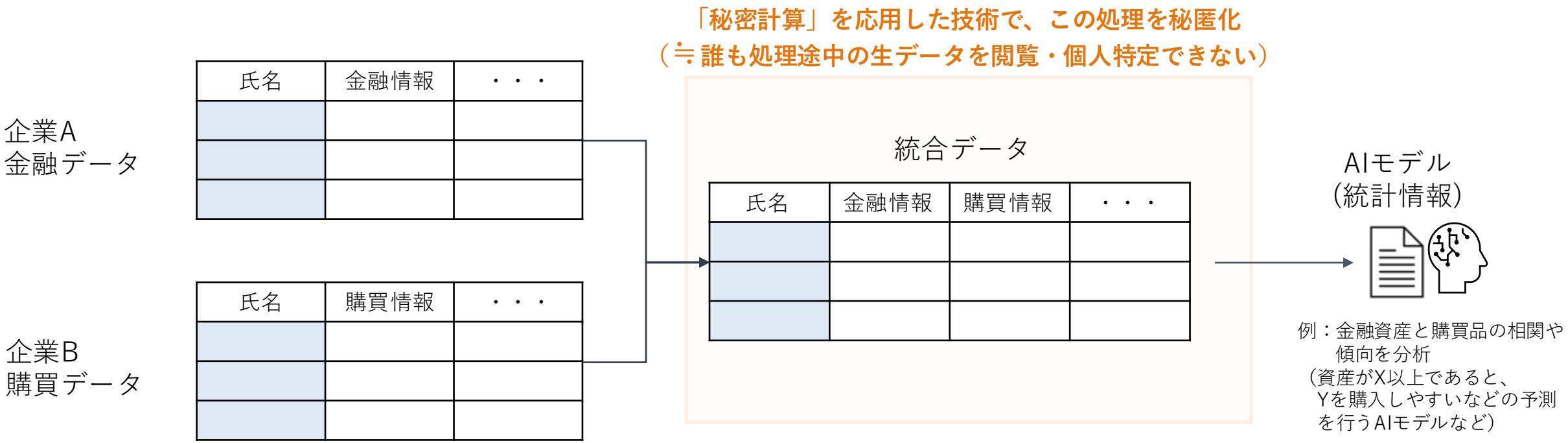
注２：本人同意なき個人データ等の第三者提供については、当該個人データ等が統計情報等の作成にのみ利用されることを担保する観点等から、個人データ等の提供元・提供先における一定の事項（提供元・提供先の氏名・名称、行おうとする統計作成等の内容等）の公表、統計作成等のみを目的とした提供である旨の書面による提供元・提供先間の合意、提供先における目的外利用及び第三者提供の禁止を義務付けることを

出典：
”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316回個人情報保護委員会,
2025年3月5日,
https://www.ppc.go.jp/files/pdf/250305_shiryou-1-1.pdf

① 個人情報保護法における技術的ガバナンス：想定ユースケース

- 複数の企業が持つ個人データを同意不要で突合したAI活用を実現

図：企業間でのデータ連携した活用例



② 複数機関でのデータ連携

- 秘密計算や連合学習を用いた金融機関が連携した不正検知などが検討

事例：GoogleとSwiftによる金融不正検知

出典：https://cloud.google.com/blog/ja/products/identity-security/google-cloud-and-swift-pioneer-advanced-ai-and-federated-learning-tech

事例：FDUA様による粉飾決算検知の実証実験

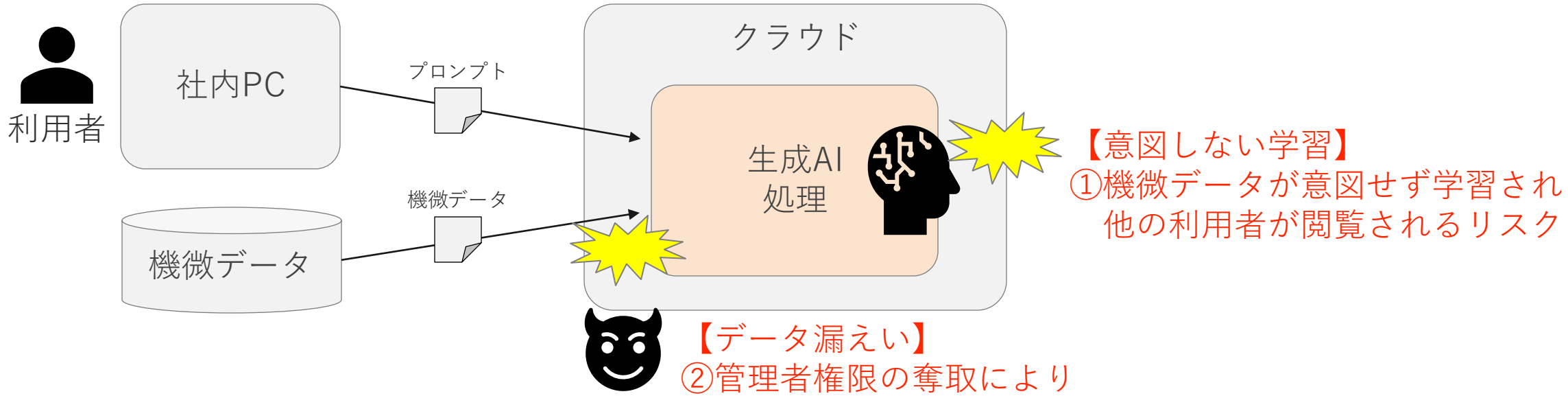
粉飾決算検知プラットフォーム分科会

最先端の**秘密計算技術**を基盤とし、各金融機関が保有するデータを相互に開示することなく秘匿したまま統合・分析。
これにより、業界横断的な視点から企業の不正会計リスクを早期に検知する、新たな金融インフラの構築を目指します。

出典：https://www.fdua.org/activities/datalinkage

- 生成AI処理は重いため、クラウド等での処理が必要
- しかし、機微データ（個人情報や営業秘密）のクラウド送信は一定のリスク

図：生成AIのクラウド利用における機微データの漏洩リスク



③ AI活用のリスク低減：導入事例

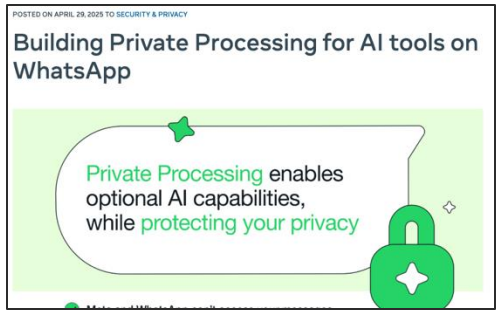
秘密計算（Confidential Computing）を適用した安全な生成AI処理の導入が進む

通信・スマホ分野

■ AppleはiPhoneなどの生成AIサービスに適用開始(2024年)

出典： https://security.apple.com/blog/private-cloud-compute/

■ MetaはメッセージアプリWhatsAppに適用開始（2025年）



出典： https://engineering.fb.com/2025/04/29/security/whatsapp-private-processing-ai-tools/

AI分野

■ Googleはオンプレミス環境向けのGemeniに本技術を適用開始(2025年)

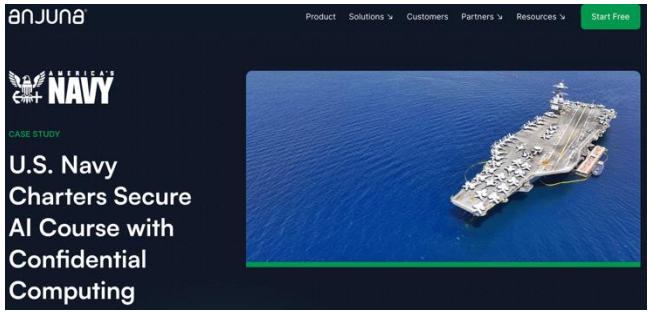
出典：https://cloud.google.com/blog/ja/products/ai-machine-learning/run-gemini-and-ai-on-prem-with-google-distributed-cloud

■ Anthropicは本技術のAI処理への適用を検討（2025年）

出典：https://www.anthropic.com/research/confidential-inference-trusted-vms

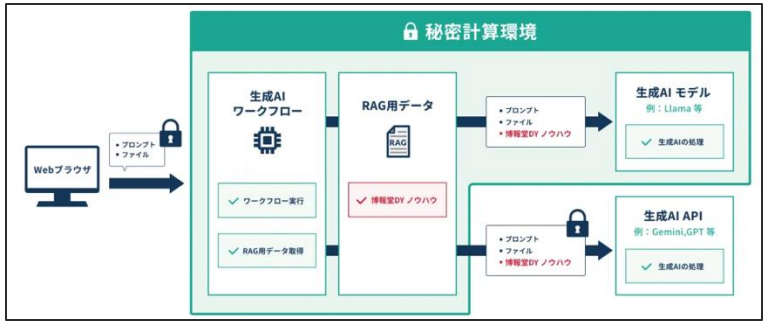
その他（安全保障、広告など）

■ スタートアップのAnjunaとNVIDIAは米国海軍に分析環境を提供(2024年)



出典：https://www.anjuna.io/case-studies/united-states-navy

■ Acompanyと博報堂は、企業秘密を守りながら生成AIを活用する技術を開発(2025年)



出典： https://www.acompany.tech/news/25-0801-1

参考：差分プライバシーの特徴

- 差分プライバシーのように**データを曖昧化する技術**では、AIの**精度は低下**

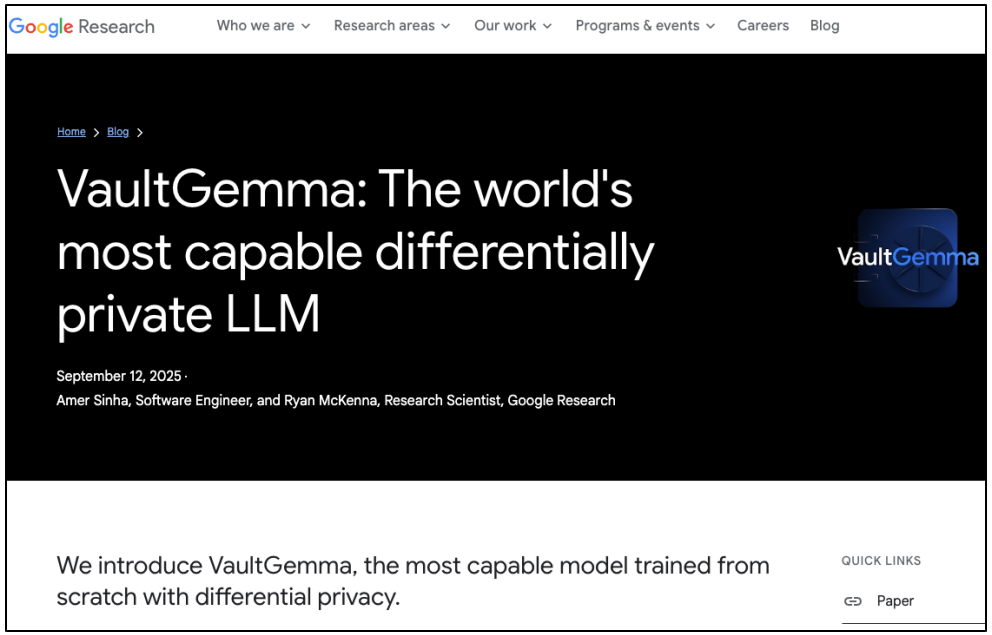
PETsの特徴例（データの秘匿処理と曖昧化処理の違い）

データ処理	技術例	メリット	デメリット
データの秘匿化	秘密計算	提供先での不正な閲覧を防げる	手法によっては、速度低下や分析が限定
データの曖昧化	差分プライバシ合成データ	情報が減るため、提供先での漏洩を防げる	加工するため精度が低下
データの組織間連携（その他）	連合学習 秘密計算	組織間でのデータ連携を安全に実現	手法によっては、速度低下、分析精度の低下などが発生

※以下の資料を参考に作成
https://service.acompany.tech/news/20250306

研究事例：Googleの差分プライバシーを適用したLLM

- 差分プライバシーを適用することで、学習データに含まれる個人情報などが漏洩しないように安全性を向上
- 一方、精度は約5年前のモデル程度に低い状況



出典：https://research.google/blog/vaultgemma-the-worlds-most-capable-differentially-private-llm/

まとめ

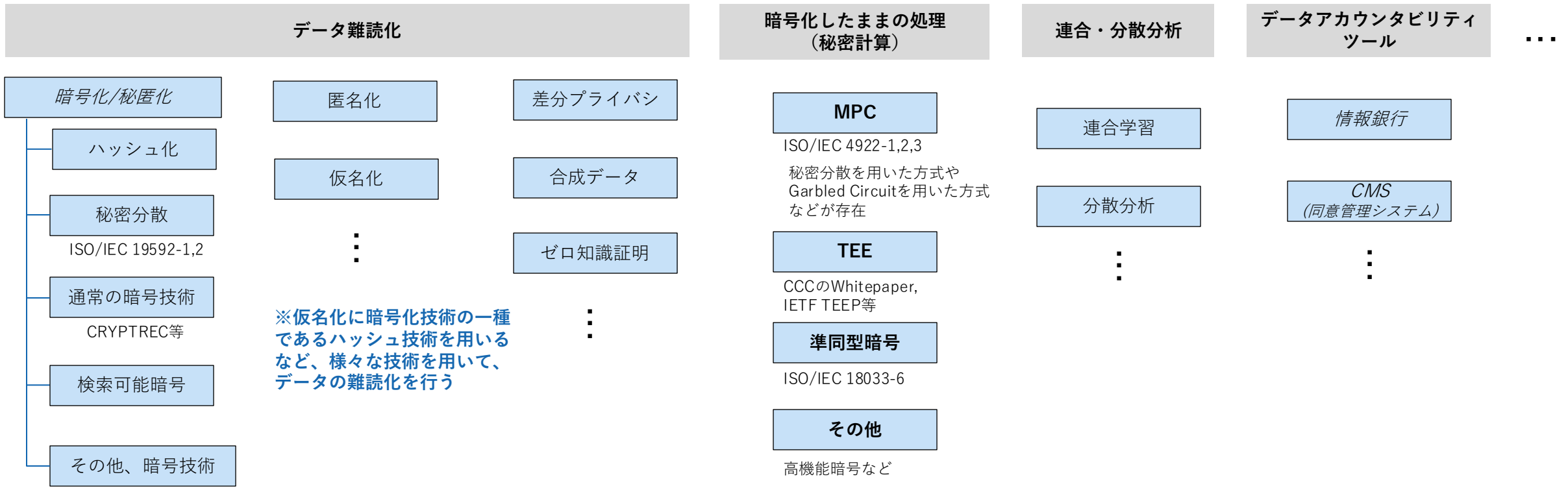
- PETsには様々存在し、AI処理にも適用可能な技術も存在
- 個人情報保護法、データ連携、AI活用リスク低減などに期待
- ユースケースに応じて、適切な技術の適用を検討すべき

付録：PETsの詳細

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

参考：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

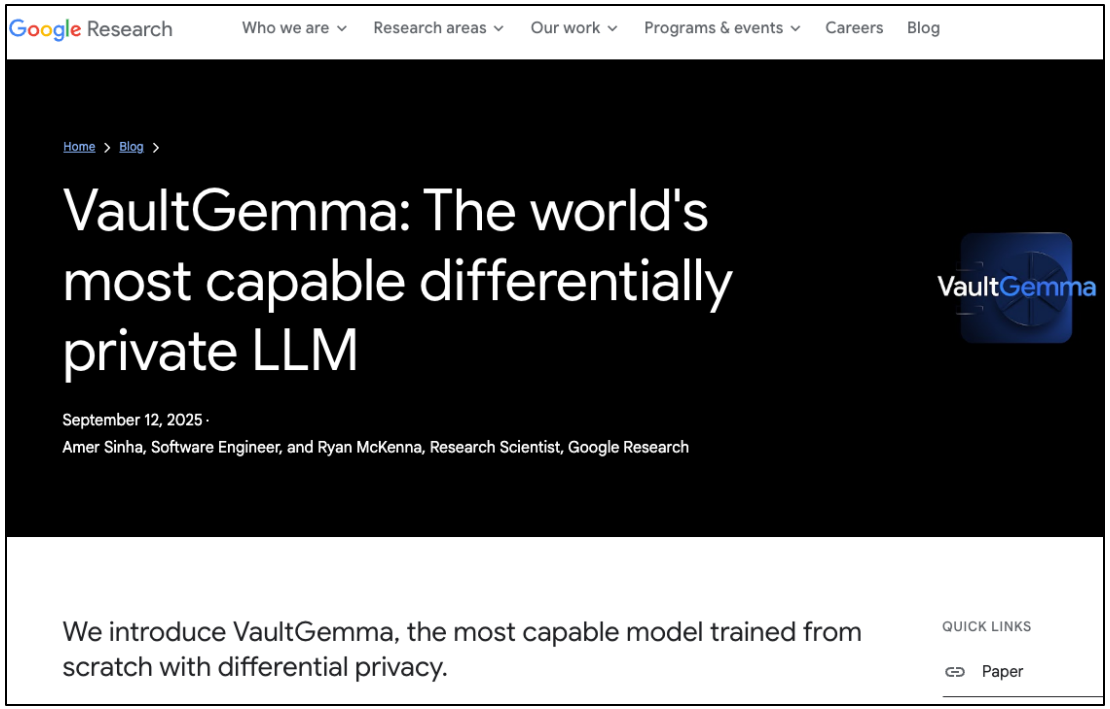
- プライバシー強化技術（PETs）の初期の定義は、1995年のオンタリオ州情報・プライバシーコミッショナー報告書に見られる。この報告書では、PETsを**「識別可能なデータの収集を最小化または排除することで個人のプライバシーを保護するさまざまな技術」**として説明している。
- また、2002年の経済協力開発機構（OECD）による「プライバシー強化技術のインベントリ」では、PETsを**「個人のプライバシーを保護するための幅広い技術」**と定義している。
- データプライバシー法において、PETsの明確な法的定義は存在しないが、英国情報コミッショナー事務所（ICO）が最近発行したガイダンスでは、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。

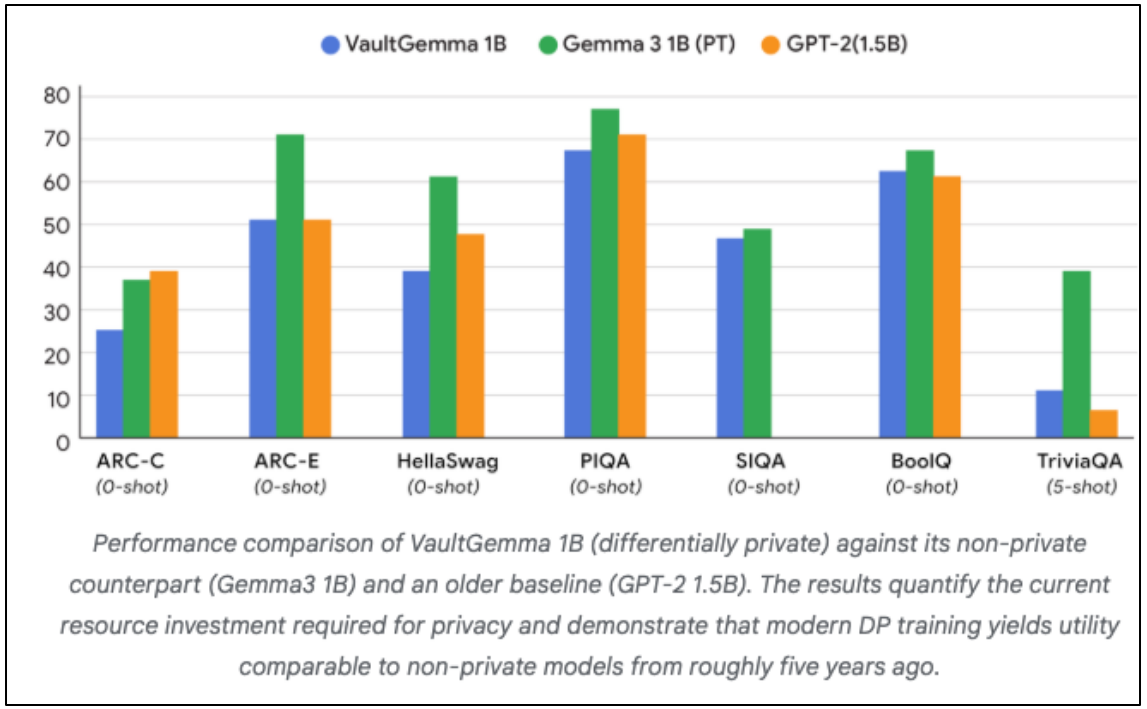
参考：差分プライバシーの特徴

- 差分プライバシーのようにデータを曖昧化する技術では、AIの精度は低下

研究事例：Googleの差分プライバシーを適用したLLM

- 差分プライバシーを適用することで、学習データに含まれる個人情報などが漏洩しないように安全性を向上
- 一方、精度は約5年前のモデル程度に低い状況





出典：https://research.google/blog/vaultgemma-the-worlds-most-capable-differentially-private-llm/

付録：秘密計算と
Confidential Computing（機密コンピューティング）

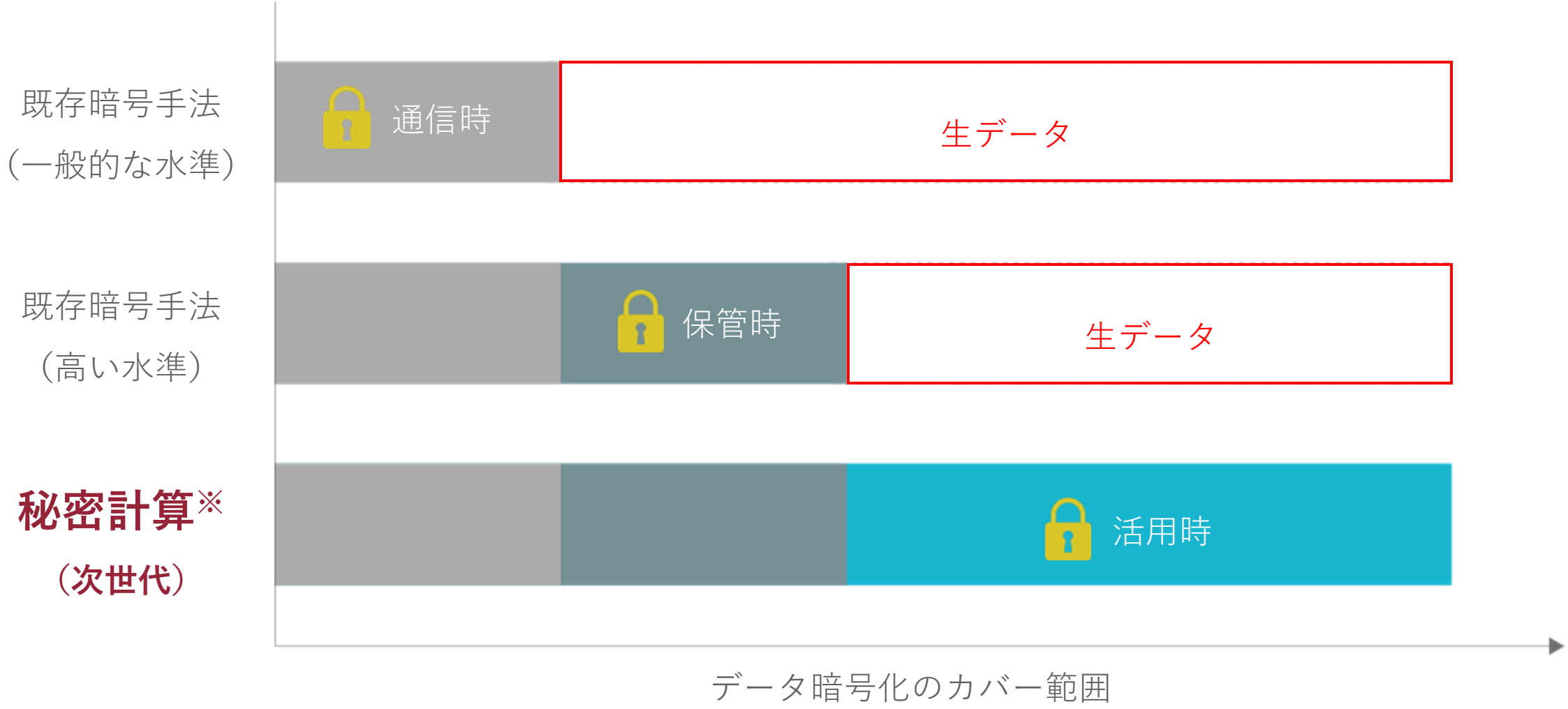
秘密計算とは

- 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

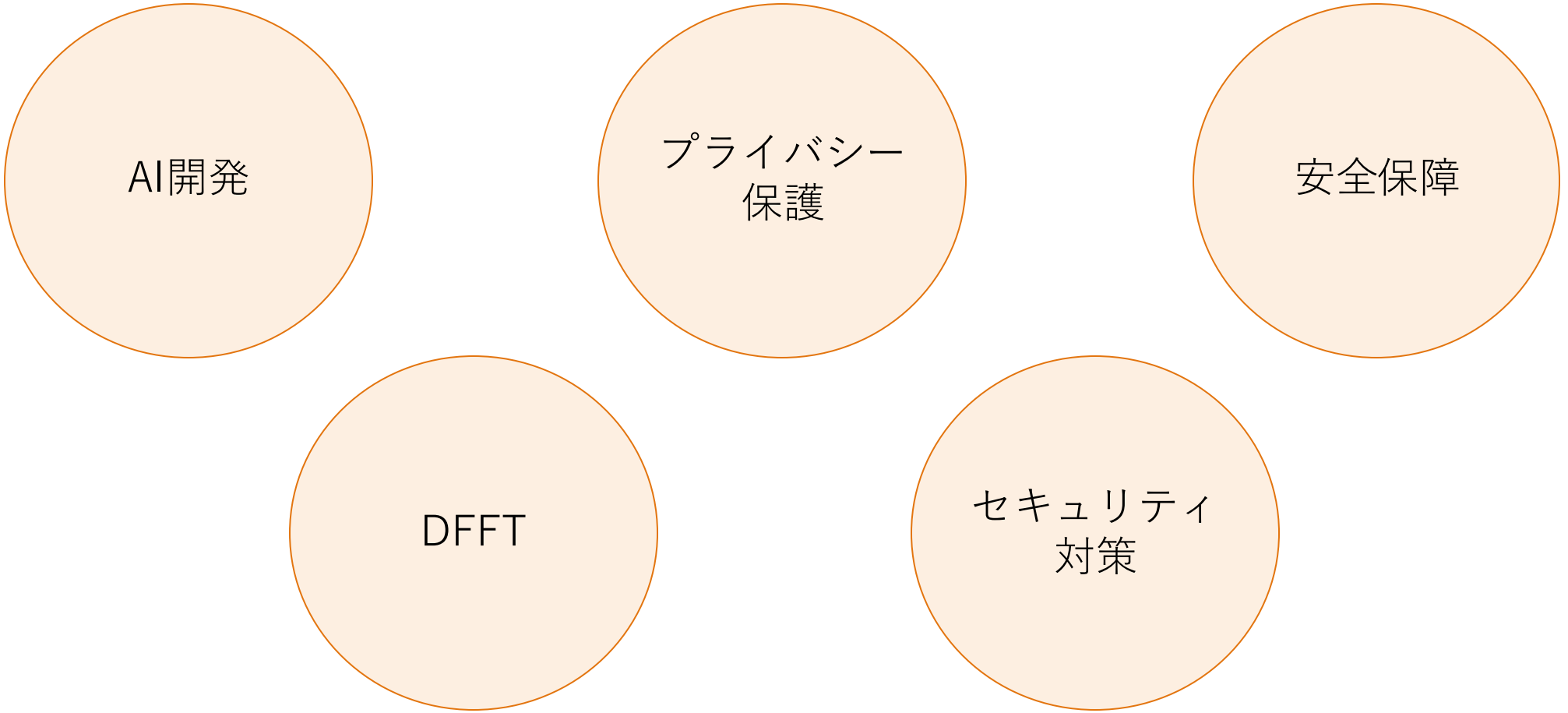
- 秘密計算も用いることで、秘匿化したままのデータ活用が可能



※ 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

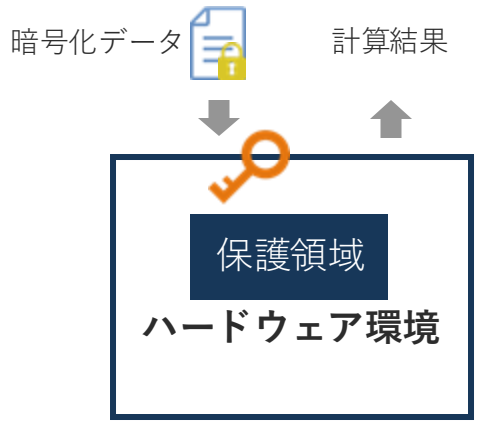
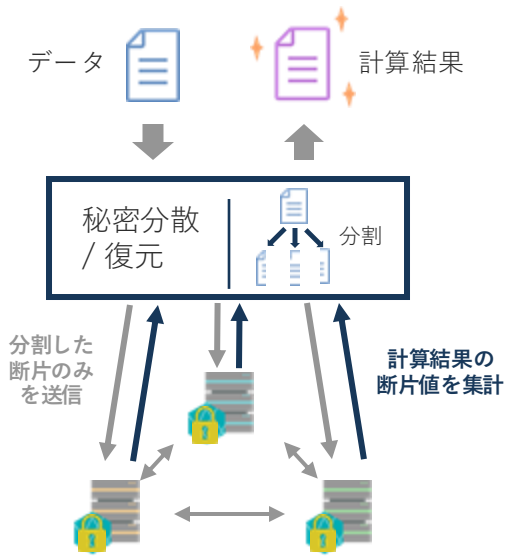
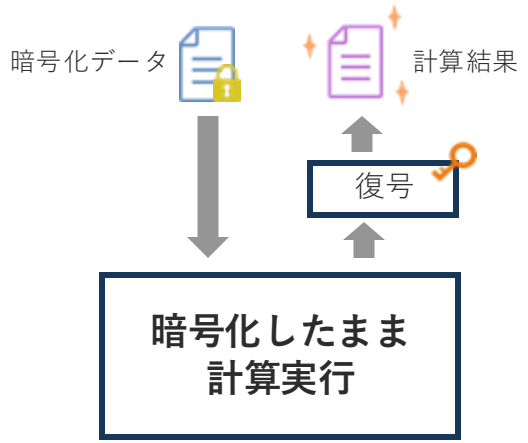
- 秘密計算は、AI開発を含む様々な分野で期待されている



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

カテゴリ	AI対応の秘密計算	その他の秘密計算	
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

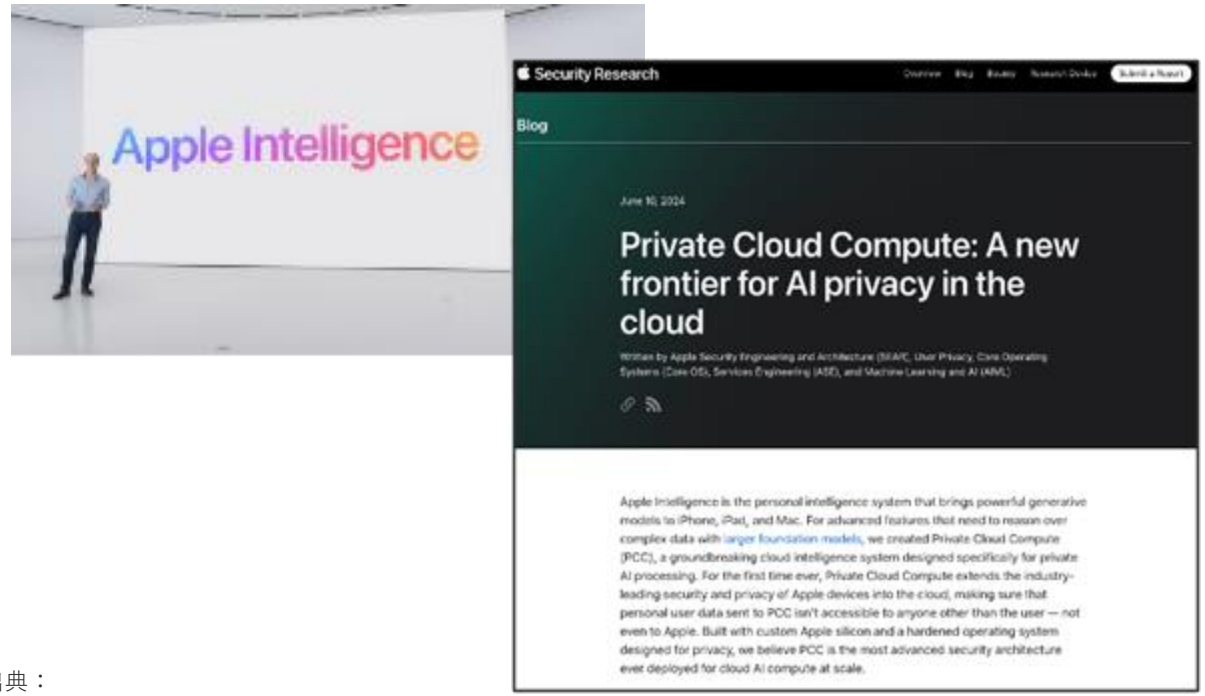
※1 TEEは処理中のメモリ内のデータが暗号化されているため、秘密計算の一種として記載
※2 方式、環境、処理内容などに依存するため参考値として記載
通常のCPUが3.00GHzで256 binary gate/clkと仮定すると、秒間768 * 10^9論理回路[gate / sec]実行できるとして、速度低下の度合いを参考値として概算。数年前の参考値として、 [1]では、Honest-majorityでsemi-honest安全な秘密分散の秘密計算が約7 billion [gate/sec]で約7 * 10^9[gate/sec] 。NuFHEのGPUでの計測 [2] によると、約0.35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

- AI対応の秘密計算は、生成AIの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

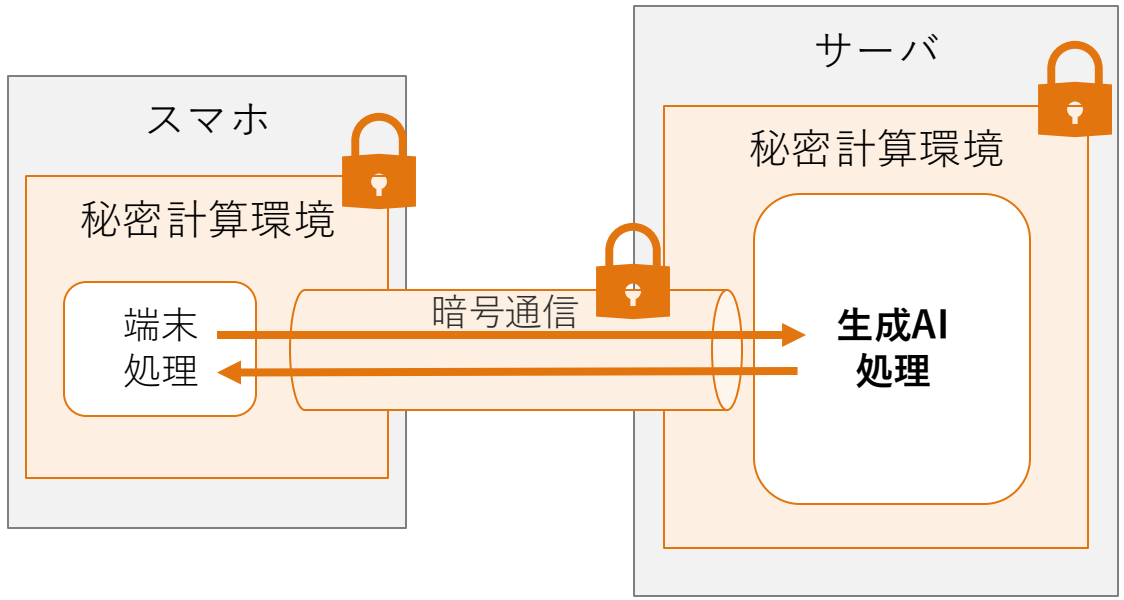
iPhone 16で動作する生成AIには本技術が適用※1



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



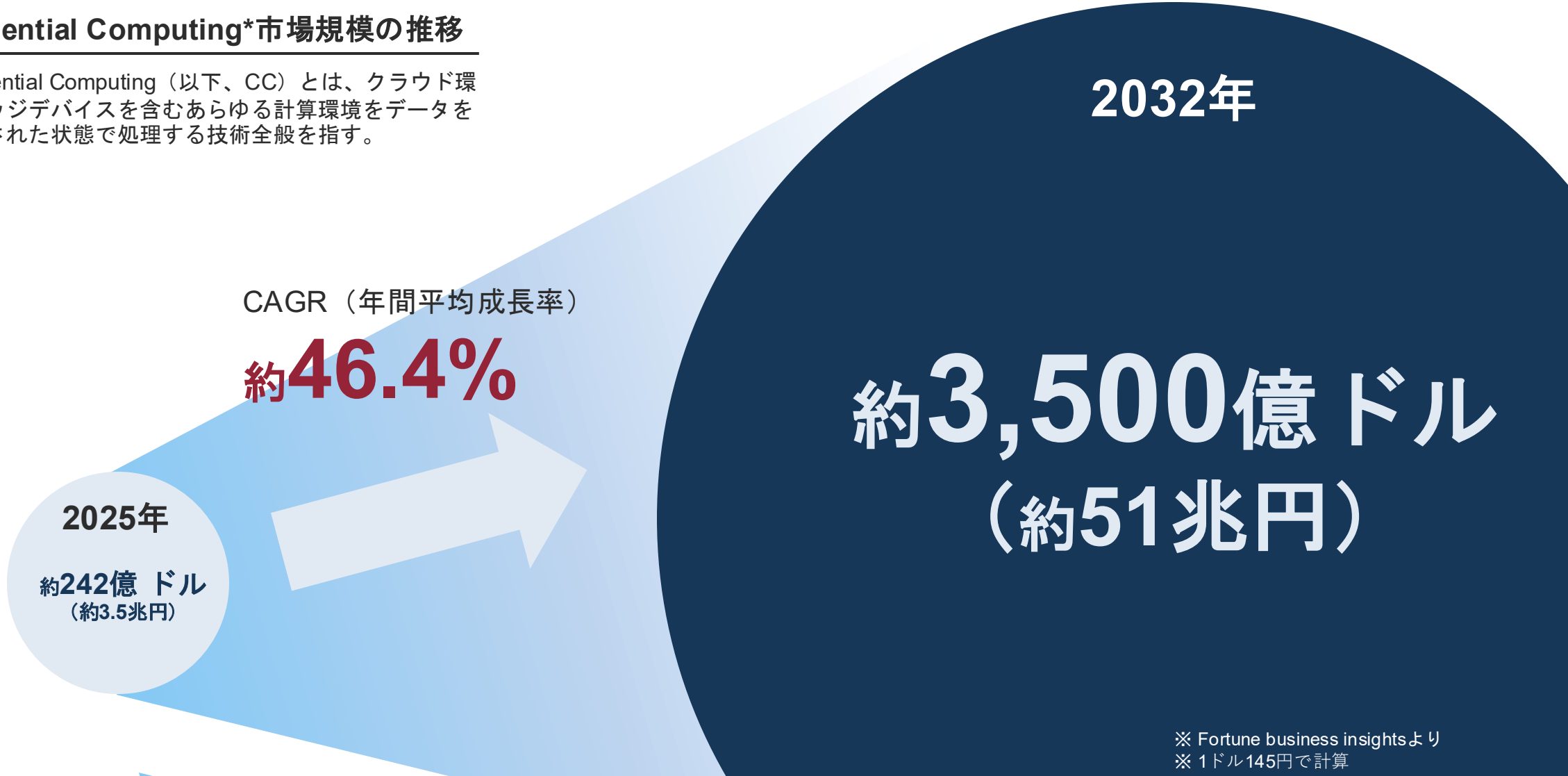
出典：同様な技術についてのGoogleの技術Blog記事の図を参考に著者らが作成
記事：“プライバシーを強化した生成 AI を実現する”,
https://developers.googleblog.com/ja/enabling-more-private-gen-ai/

機密コンピューティング（Confidential Computing）の市場

Confidential Computing市場は**毎年約1.5倍で急成長**と予想

Confidential Computing*市場規模の推移

*Confidential Computing（以下、CC）とは、クラウド環境やエッジデバイスを含むあらゆる計算環境をデータを暗号化された状態で処理する技術全般を指す。



※ Fortune business insightsより
※ 1ドル145円で計算

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

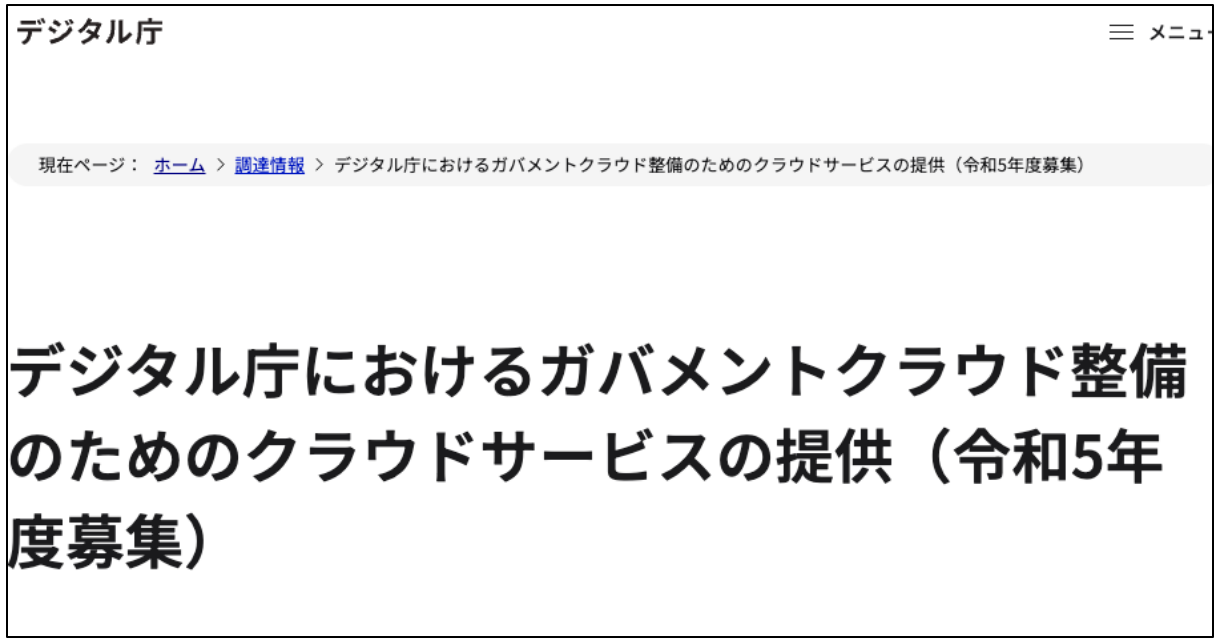
Confidential Computing（機密コンピューティング）は、組織が機密データを扱う方法を根本的に変革します。ハードウェアベースのTrusted Execution Environment（TEE：信頼実行環境）内でワークロードを隔離することにより、インフラ運用者、クラウド事業者、さらにはハードウェアへの物理的アクセス権を持つ者からも、データ内容や処理内容を秘匿したまま実行できます。これは、規制産業や地政学的・コンプライアンスリスクに直面するグローバルな事業運営、さらには競合企業間のデータ連携において特に価値があります。

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

国内における機密コンピューティングの位置づけ

ガバメントクラウドではConfidential Computing（機密コンピューティング）が必須

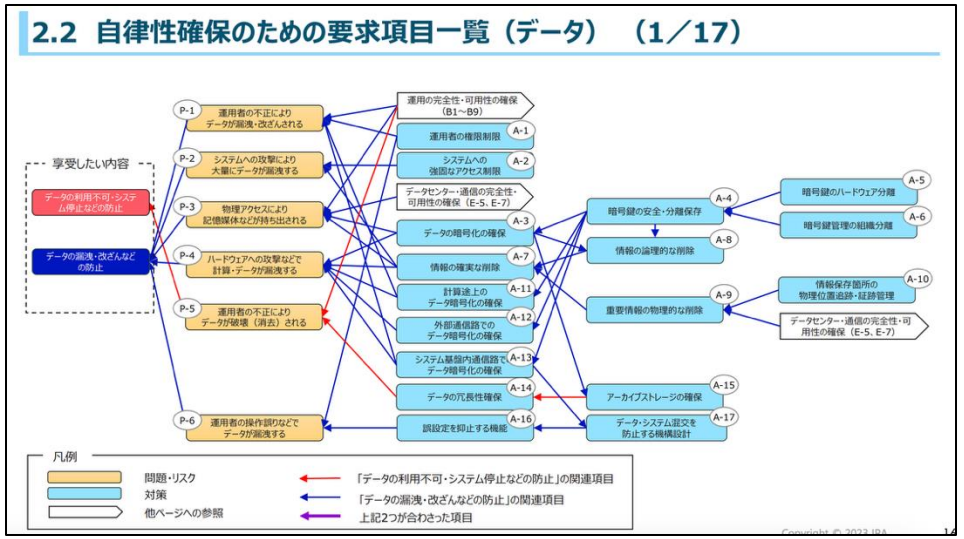


機密コンピューティング環境	クラウド利用者からは完全に分離し暗号化された仮想マシンでデータの暗号化/復号が行えるサービスまたはサポートが提供されていること。
機密コンピューティング環境	H/Wによってあらかじめ実装され、秘匿対象とするデータが事前に確認し信頼されたプログラムのコードからのみアクセス可能な隔離された環境を提供可能であること。

出典：デジタル庁におけるガバメントクラウド整備のためのクラウドサービスの提供（令和5年度募集）調達仕様書 別紙1（基本事項及びマネージドサービスの技術要件詳細）
https://www.digital.go.jp/procurement/3058bc41-ee8f-49bb-8f22-8def725f6f3f

重要情報を扱うシステム（金融インフラ含む）のセキュリテイ

安全保障に関わる機密データは機密コンピューティングで実行することが推奨



A-11	計算途上のデータ暗号化の確保	ハードウェアへの攻撃や管理者権限を有する運用者の不正などによって、メモリからデータの中身を読み取ろうとしても、読み取らせないようにする。	• 特に重要なデータを扱うアプリケーションについて、例えば、ハードウェア技術を用いて、計算機のメモリ上などに格納される全ての一時的な計算結果が暗号化・隔離されるような仕組みにより、運用者などからも秘匿される機能を提供すること。 • 当該隔離機能は鍵管理機能と連動し、計算結果の隔離機構外部との全てのやり取りが暗号化され、当該アプリケーションを利用している者以外に解読されないこと。 • 当該隔離機能の利用に際し、信用しなければならないトラストアンカー（CPUチップベンダー・鍵管理装置ベンダーなど）を確認すること。 ※計算途上のデータ暗号化のためには、特殊なハードウェアやソフトウェアに限定されるなどの現時点では課題があり、その対応状況はIPAサイトにて共有する。
A-12	外部通信路でのデータ暗	ネットワークトラッピングにより運用者としてシステムを	重要情報を扱うシステムの管理者が操作する管理インタフェースとの通信およびベンダーの

出典：IPA,要情報を扱うシステムの要求策定ガイド, https://www.ipa.go.jp/digital/kaihatsu/system-youkyu.html

付録：PETs・機密コンピューティングに関する政策動向

「機密コンピューティング」に関する政策動向の概要 （当協会理解）

「機密コンピューティング」は、「TEE」や「ハードウェア型の秘密計算」とも呼ばれ、「PETs」の一種と分類され、政策文書等に記載・発言あり

TEE: Trusted Execution Environment
PETs: Privacy Enhancing Technologies

- 記載・発言の例
  - デジ行財「データ利活用制度の在り方に関する基本方針」
  - 自民党「デジタル・ニッポン 2025」
  - デジタル庁「デジタル社会の実現に向けた重点計画」
  - 2025年 通常国会 AI法答弁

- 記載・発言対象
  - データ利活用
  - AI活用
  - トラスト
  - 個人情報保護法

「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

- 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。

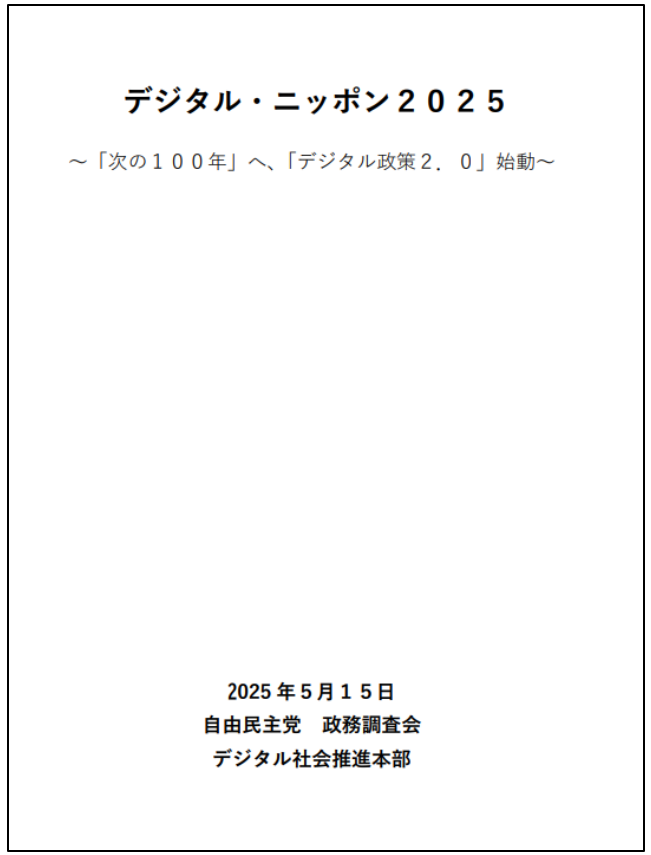
---

[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。

「デジタル・ニッポン2025 データ戦略」：データ利活用、トラスト、経済安全保障

- 自民党の「デジタル・ニッポン 2025」にて、データ利活用・トラスト・個人情報保制度・経済安全保障・ガバナンスに関連して、PETsについて記載



デジタル・ニッポン２０２５

～「次の１００年」へ、「デジタル政策２．０」始動～

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

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

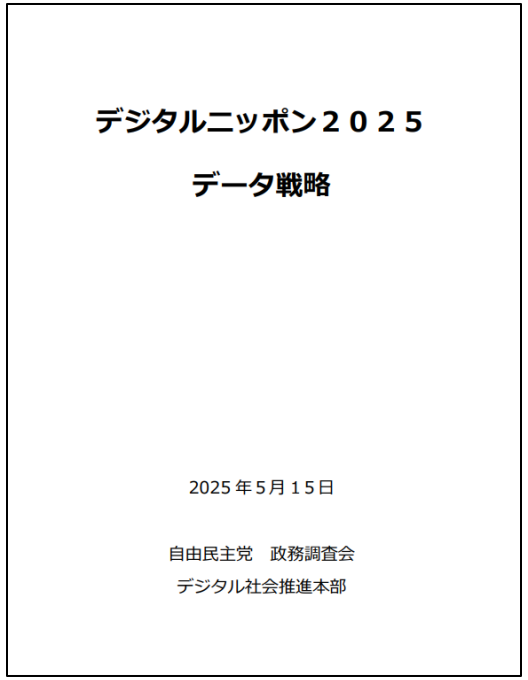
2.「デジタル政策2.0」に向けた「デジタル庁2.0」の実現
～「行政DX」から「社会全体のDX」へ
2.3 データ利活用を軸とした「データ政策の司令塔」としての抜本的な機能強化
(1) データ利活用を巡る課題

データが柔軟かつ効率的に共有・利活用されることによって、既存の社会的コストが低下し、新たな価値が創出される。また、日本のAI産業の競争力強化という観点からは、質の高い学習データをどれだけ確保できるかが、勝負の鍵を握る。
・・・（略）・・・我が国におけるデータ流通の基本的枠組みについて、既存の法制度の抜本的な見直しを含めた検討を加速させるべきであり、我が国ではデジタル行政改革会議の下で、2025年度を目途に、我が国のデータ利活用制度の在り方についての基本的な方針を策定するとされているところである。
当該基本的な方針の策定に当たっては、横断的な対応策として、目的に応じた柔軟なデータ連携システムの構築、**「トラスト」の確保（PETsの活用を含む）**、**個人情報保護制度**のアップデート、**データ利活用**における**経済安全保障**に配慮したガバナンスの確保が考えられたものでなければならない。

「デジタル・ニッポン2025 データ戦略」：個人情報保護法

- 自民党の「デジタル・ニッポン 2025 データ戦略」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

国会答弁： AI法と関係する個人情報保護法におけるPETs

- 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。

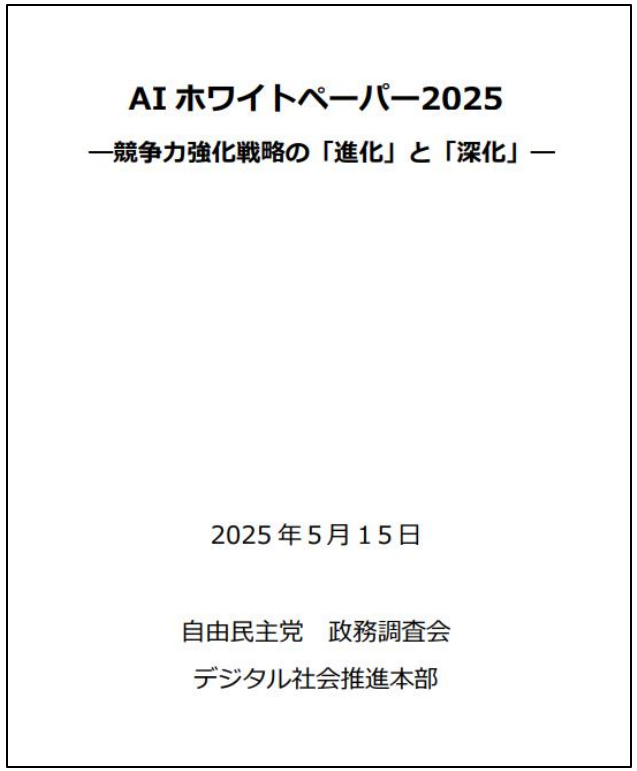
　こうしたことを踏まえまして、今回の規律が、利用者や消費者を含め、様々な幅広い関係者に受け入れられる内容となりますよう、引き続き対話も重ねながら検討してまいりたいと思います。

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

「デジタル・ニッポン2025 AI」：AIと個人情報保護法

- 自民党の「デジタル・ニッポン 2025」の「AIホワイトペーパー2025」にて PETs活用について言及記載

自民党の「AIホワイトペーパー2025」にて「PETs」について記載



AI ホワイトペーパー2025

―競争力強化戦略の「進化」と「深化」―

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章 研究開発と利活用の一体的推進「AIによる生産性の刷新」

2.1 データ

（略）

個人情報保護法の見直しにあたり、AI 開発を委縮させないよう、実態に合わせた合理化、法の適用対象の明確化、**PETs[2](Privacy Enhancing Technologies)の活用等を考慮すること**。また、一定の条件を満たす統計作成など、問題が生じるおそれが少ない場合における、本人の同意を要しないデータ提供、利用を推進すること

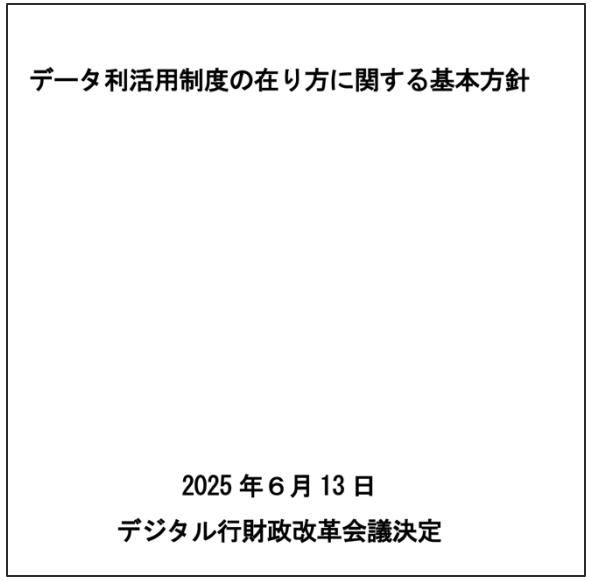
---

[2] プライバシー保護とデータ共有・利活用のジレンマを解消し、プライバシーを保持したままデータの分析・演算や機械学習を可能にする技術の総称

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

「データ利活用制度の在り方に関する基本方針」：トラスト基盤

- トラスト基盤への秘密計算（例：ハードウエア型の秘密計算のTEE）などのPETsへの取り込みについて言及


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

3 データ利活用のための環境シビ及び当面の分野横断的な改革事項

（２）データ連携の基盤整備及びデータ標準化の推進

①トラスト基盤の整備

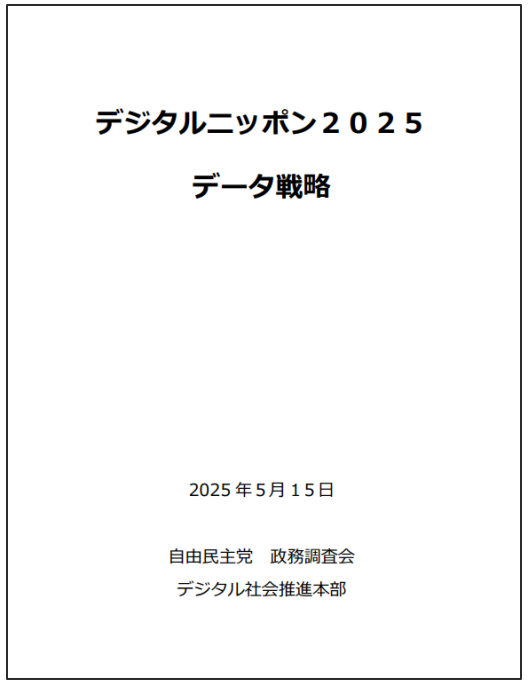
（略）

あわせて、デジタルアイデンティティウォレット（DIW）やヴェリファイアブルクレデンシャル（VC）、**秘密計算**、ゼロ知識証明等の先端的な**プライバシー強化技術（PETs）等のトラストに関する新たな技術**についても、重要なものが生み出される都度、活用の在り方を検討し、トラストの体系的な整理に柔軟に取り入れる等トラスト基盤をダイナミックに更新していく。個々のトラストを確保する手法についても必要に応じて拡充や改善を行う。例えば、事業者の真正性・実在性の関係で、公的な法人認証が必要となるケースに対応するために、ＧビズＩＤの認証機能の活用を候補の１つとして検討する。

「デジタル・ニッポン2025 データ戦略」：トラスト・DFFTとPETs

- トラスト・データセキュリティ・DFFTへのPETsの期待

自民党の「デジタル・ニッポン 2025」にて「トラスト」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

2.2 トラストの確保

データの連携と利活用を安全かつ円滑に進め、産業データスペースの構築などにつなげていくためには、**「トラストの確保」が不可欠**である。・・・**DFFT**においてもこのような「データセキュリティ」が位置づけられている。・・・

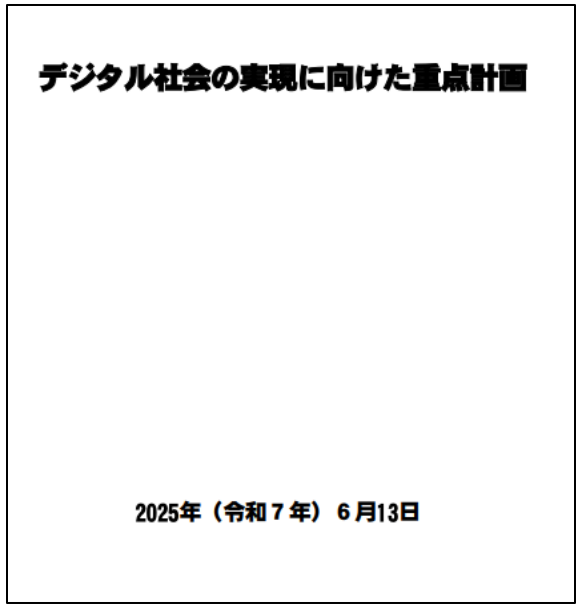
また、信頼性の確保にあたっては、従来の制度的・技術的手段に加え、**秘密計算**やマルチパーティ計算（MPC）、ゼロ知識証明などの**最新のプライバシー保護技術（PETs: Privacy Enhancing Technologies）を適切に活用**し、トラスト要素の体系的な整理に柔軟に取り入れることも重要である。これらの技術は、データを秘匿したまま処理を行うことを可能にし、機微なデータを扱う場面でもプライバシーや機密性を損なうことなく、信頼性の高いデータ利活用を実現する次世代のアプローチとして期待されている。さらに、このような**PETsも含めたトラストサービスについて**、民間の投資意欲も喚起し、我が国が国際的な優位性を保持できる技術の開発・確立を強力に進めるべきである。

さらに、トラスト確保の基盤は国内におけるデータ連携のみならず、**国際的なデータ連携**においても求められるものである。・・

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

「デジタル社会の実現に向けた重点計画」：DFFT・データセキュリティ

- DFFT・データセキュリティに関連してPETsについて言及



デジタル社会の実現に向けた重点計画

2025年（令和７年）６月13日

出典：https://www.digital.go.jp/policies/priority-policy-program

○[No. 3-14] DFFT の具体化推進に向けた国際連携/IAP の設立・プロジェクトの実施

・ G7広島サミット及び群馬高崎デジタル技術大臣会合の承認を受け、2023年12月にDFFTの具体化のための国際的な枠組み（Institutional Arrangement for Partnership：IAP）をOECDで設立。翌年のプーリアサミットでは、DFFTの新軸として「データセキュリティ」が議論。資金的な支援等を通じ、各国のデータ規制に関する透明性向上、PETs（Privacy-Enhancing-Technologies）を通した法令適合性とデータセキュリティの向上等DFFTに資する取組を推進し、G7首脳・デジタル関連閣僚会合等の多数国間協力におけるDFFTの議論にも随時棚卸していく。また国連等で進む関連取組とも連携を進める。今後も足元の課題解決や将来の規範形成につながる取組を継続的に実施し、国際的なルール・制度作りと信頼性を確保する技術の両面から、我が国のデジタル社会が堅持すべき価値を実現するために、国際的な議論を主導し、DFFTの一層の具体的推進に向け取り組む。

具体的な目標：透明性向上やPETs等に関するプロジェクトの実施。
G7等多数国間協力における日本主導の国際的なデータガバナンスの推進。

主担当府省庁：デジタル庁

関係府省庁：内閣府、個人情報保護委員会、総務省、外務省、経済産業省

PASSION FOR THE BEST

大和証券グループにおける生成AI活用の取組み及び生成AI活用に向けた規制上の論点

2025年11月5日

株式会社 大和証券グループ本社

アジェンダ

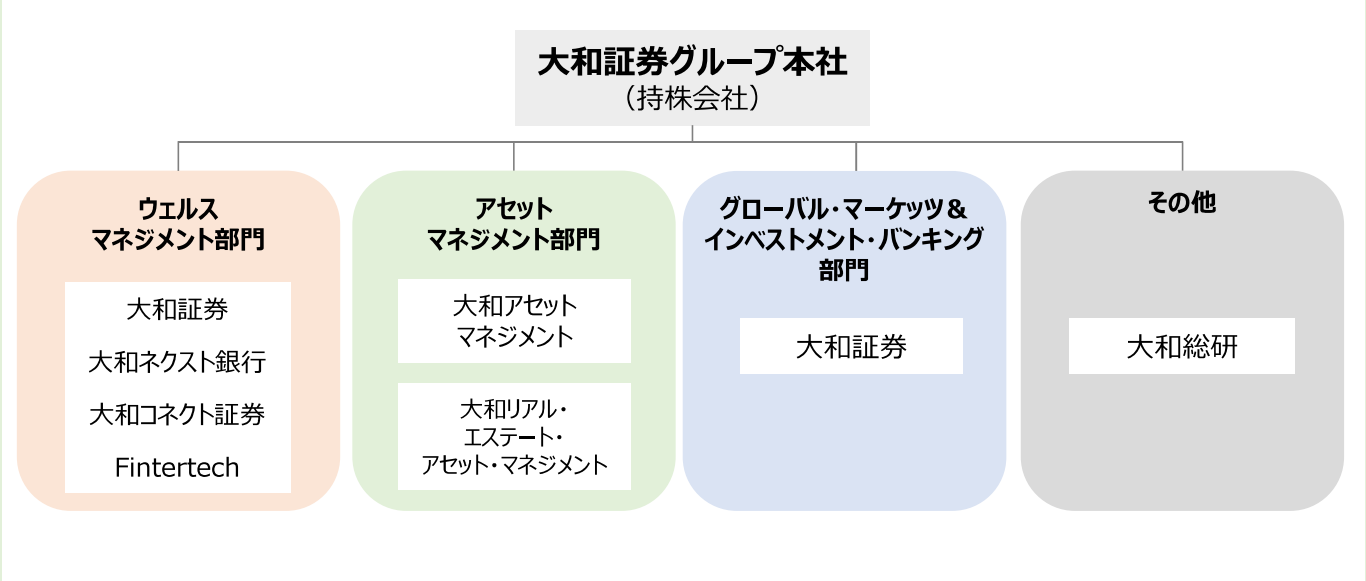
1. はじめに
2. 大和証券グループにおける生成AI活用の取組み
3. 生成AI活用に向けた規制上の論点
   - A) 機微情報
   - B) 法人関係情報等
   - C) 情報授受規制
   - D) 勧誘方針・広告規制
4. おわりに

1．はじめに
大和証券グループについて

PASSION FOR THE BEST

大和証券グループ本社
Daiwa Securities Group Inc.

会社名	株式会社大和証券グループ本社
代表者	代表執行役社長　荻野　明彦
発足	1999（平成11）年4月26日
資本金	2,473億円（2025年3月末現在）
本社 所在地	〒100-6751 東京都千代田区丸の内一丁目9番1号 グラントウキョウ　ノースタワー



板屋　篤（いたや　あつし）
株式会社大和証券グループ本社　執行役員
大和証券株式会社　常務取締役
株式会社大和総研　取締役

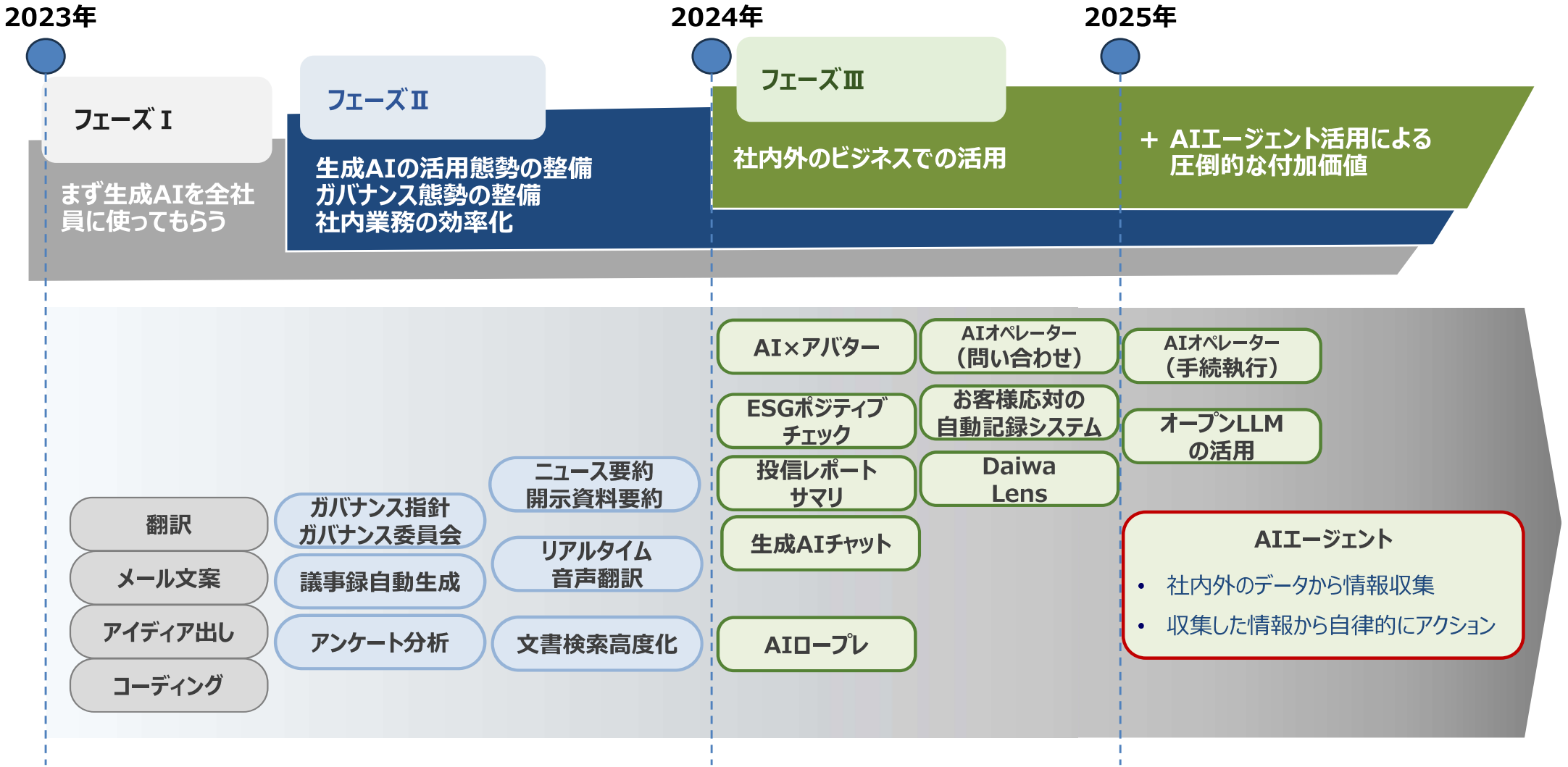
1992年、大和証券入社。2021年大和証券グループ本社企画副担当 兼 IT・オペレーション副担当を経て、2024年4月よりIT・オペレーション担当（現職）。大和証券グループのデジタル戦略を推進し、生成AI・Web3.0等のテクノロジーを活用したプロジェクトに取り組む。

生成AI活用のロードマップ

PASSION FOR THE BEST

生成AIは「使ってみる」から「社内外のあらゆる業務に実装」の段階

⇒ビジネスを支える中核的なテクノロジーになりつつある



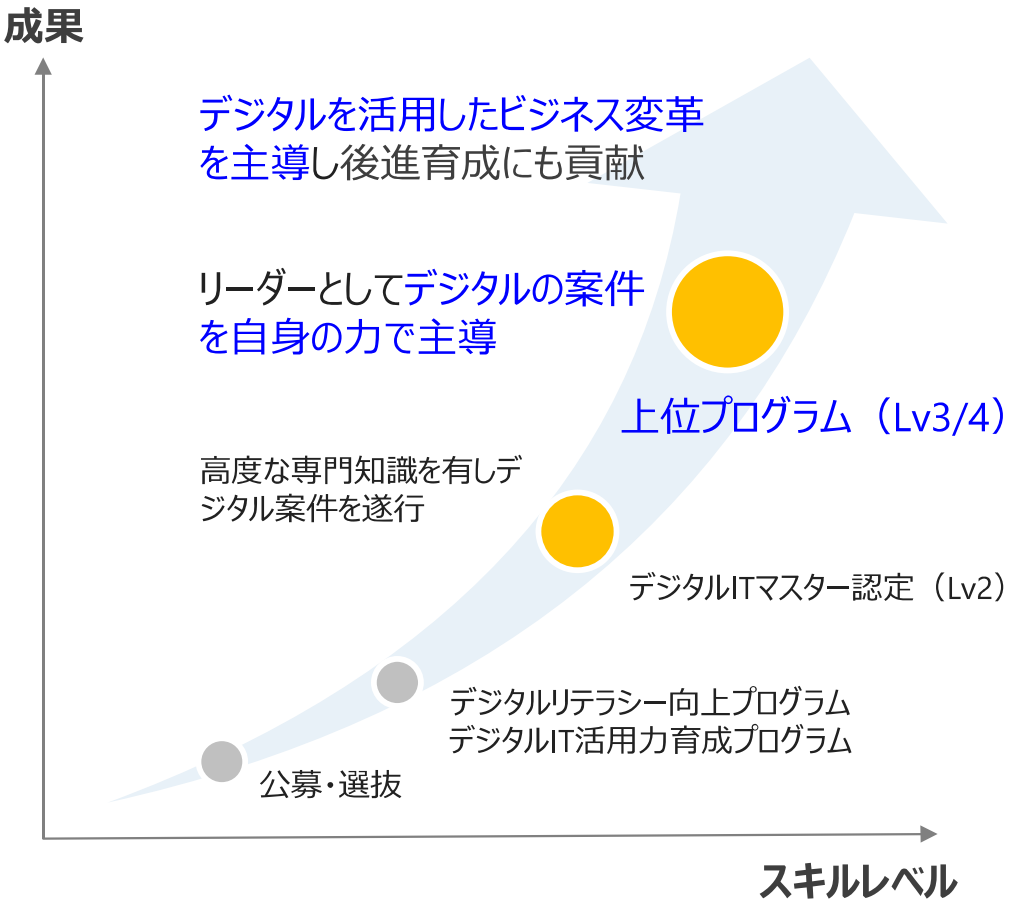
AI活用案件拡大・成果創出に向けた取り組み　～活用態勢の整備～

PASSION FOR THE BEST

育成した各部門のデジタルIT人材との連携を強化する組織としてデジタル推進部を設置

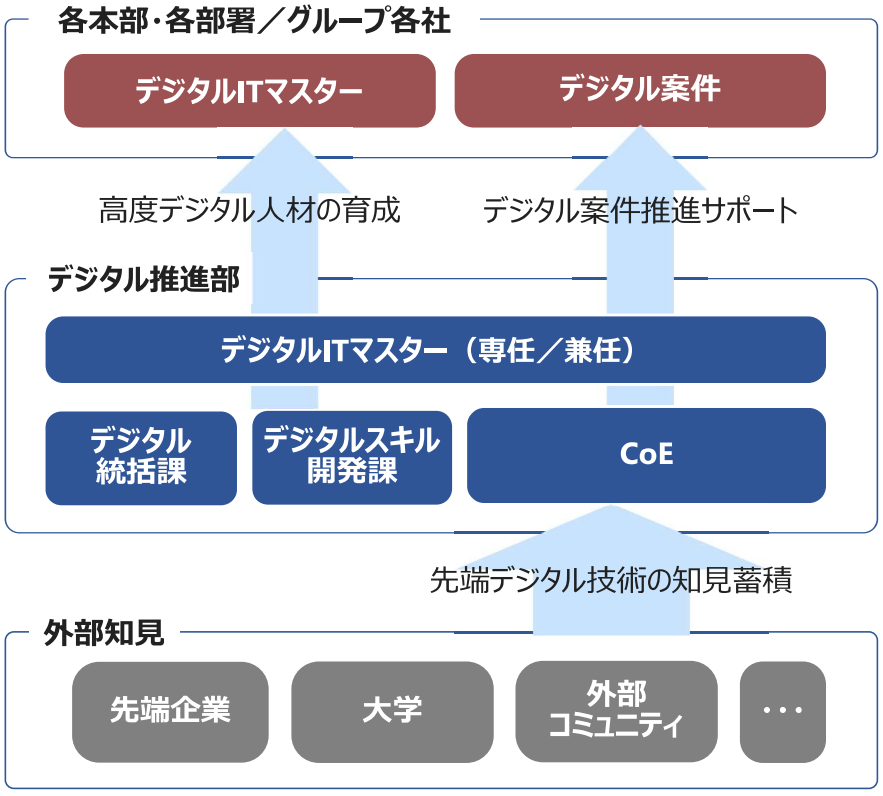
CoEはデジタル推進部内に設置し、先端デジタル技術の知見蓄積 → デジタル人材育成 → 各部ビジネスに展開　を一気通貫で実現

デジタルITマスター認定制度概要



2023年10月デジタル推進部を新設

先端デジタル技術の知見蓄積 → デジタル人材育成
→ 各部ビジネスに展開　を一気通貫で実現

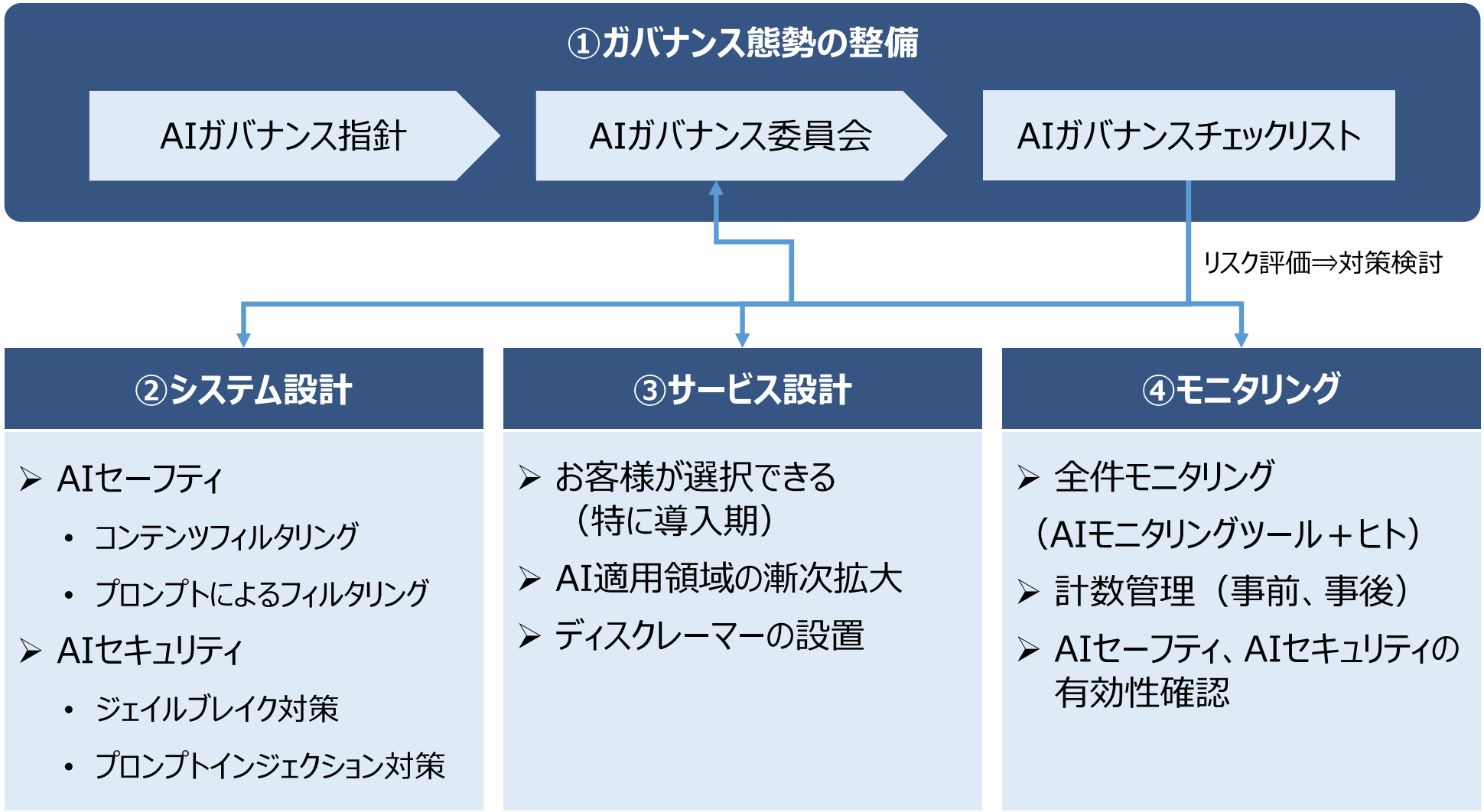


2. 大和証券グループにおける生成AI活用の取組み
AIガバナンス態勢の整備

適正なAI活用を推進するため、ガバナンス態勢を整備（指針・委員会・チェックリスト）⇒ ①

AIを組み込んだサービスを導入する際は、チェックリストに基づいてリスク評価、対策 ⇒ ②～④

AIガバナンス委員会がさまざな視点（CRO、CHO、サステナビリティ、コンプラ、企画、IT）で審議

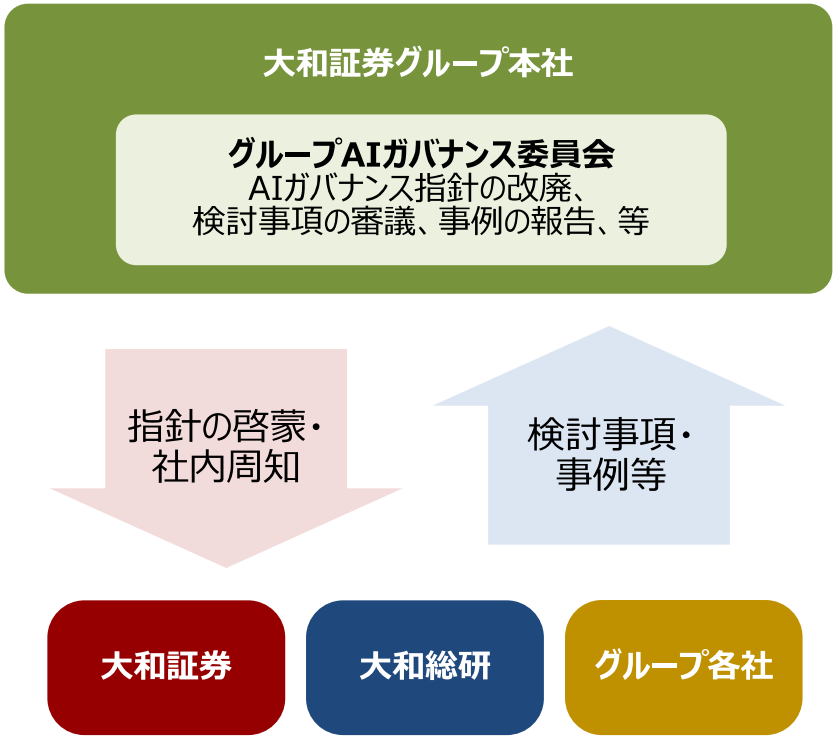


2. 大和証券グループにおける生成AI活用の取組み
ガバナンス態勢の整備

PASSION FOR THE BEST

「大和証券グループ AIガバナンス指針」を策定、「グループAIガバナンス委員会」を設置し、AIサービスの提供・活用を適切に管理

AIガバナンスの枠組み



グループAIガバナンス委員会での議論・取組み例

- AIガバナンスチェックリストの新設
- AI事業者ガイドラインに基づくAIガバナンス指針の改訂
- AIオペレーター実施の審議
- 生成AIチャットの導入の審議
- Daiwa Lens の実施の審議
- 外部有識者によるAIの安全性評価に関する講演およびディスカッション
- お客様接点における生成AIのモニタリングルール策定
- 国内外でのAI規制・ガイドラインの動向調査
- 全社員のデジタルスキル向上のための枠組み「Daiwa Digital College」にて全社員必修課程としてAIリテラシー研修の実施

3. 生成AI活用に向けた規制上の論点
金融庁『AIディスカッションペーパー第1.0版』の抜粋

PASSION FOR THE BEST

- 生成AIの加速度的な性能向上等により、ついに**社会に広範に実装される段階に到達しつつある。今後、金融を含む産業や国民生活の様々な分野において効率性や利便性を大きく向上させ、国民生活の向上や国民経済の発展に大きく寄与する可能性**が指摘されている。金融分野においても、不正検知や市場分析・予測、マーケティングなど従来型AIの利活用に加え、生成AIの普及により、一層の業務効率化や顧客体験の向上をもたらすユースケースが登場しつつある。

- AIについても、多くの課題に対応していく必要がある一方で、インターネットやクラウドサービスと同様、**中長期的には金融業務を支える中核的な技術の一つとなる可能性**がある。

- **リスクや規制面から利活用に躊躇する声も**多く聞かれる。

- リスクへの対応が重要であることは論を俟たないが、**AIはリスクを大きく上回る便益をもたらす可能性が高いとの指摘もあり、技術革新に取り残されて中長期的に良質な金融サービスの提供が困難になる「チャレンジしないリスク」も十分に認識されるべき**である。リスクベース・アプローチの下、AIの利用用途に応じて適切にコントロールしつつ、経営陣の主体的な関与の下で顧客利便性や業務効率化の向上に繋がる取組みが着実に進展していくことが望ましい。

- 既存の法令等はAIなど特定の技術を利用しているか否かに関わらず適用されることに留意すべきであるが、**AIの特性を踏まえて対応が必要な場合は、法令やガイドライン等の見直しを含めて検討**していく。

(出所) 令和7年3月4日 金融庁 AIディスカッションペーパー第1.0版

3. 生成AI活用に向けた規制上の論点
証券会社におけるデータ（生成AI）活用の課題

【大和証券の目指す姿】

3. 生成AI活用に向けた規制上の論点

A)機微情報

金融業界では、生成AI等で会話データを分析する場合、金融分野における個人情報保護に関するガイドライン（機微情報の取得、利用又は第三者提供）に抵触してしまう可能性がある

利用技術	分析対象	機微情報	金融ガイドラインに抵触する可能性
従来型AI	構造化データ（属性・取引データ等）	含まれない	なし
生成AI	会話データ（音声・テキスト）	含まれる（例）ガンで入院する	あり※

※例えば、「顧客の財産の保護」や「適切な業務運営の確保」のためと整理する方法などが考えられる

■（ご参考）金融分野における個人情報保護に関するガイドライン 第5条

金融分野における個人情報取扱事業者は、機微情報については、次に掲げる場合を除くほか、取得、利用又は第三者提供を行わないこととする。

②人の生命、身体又は**財産の保護のため**に必要がある場合

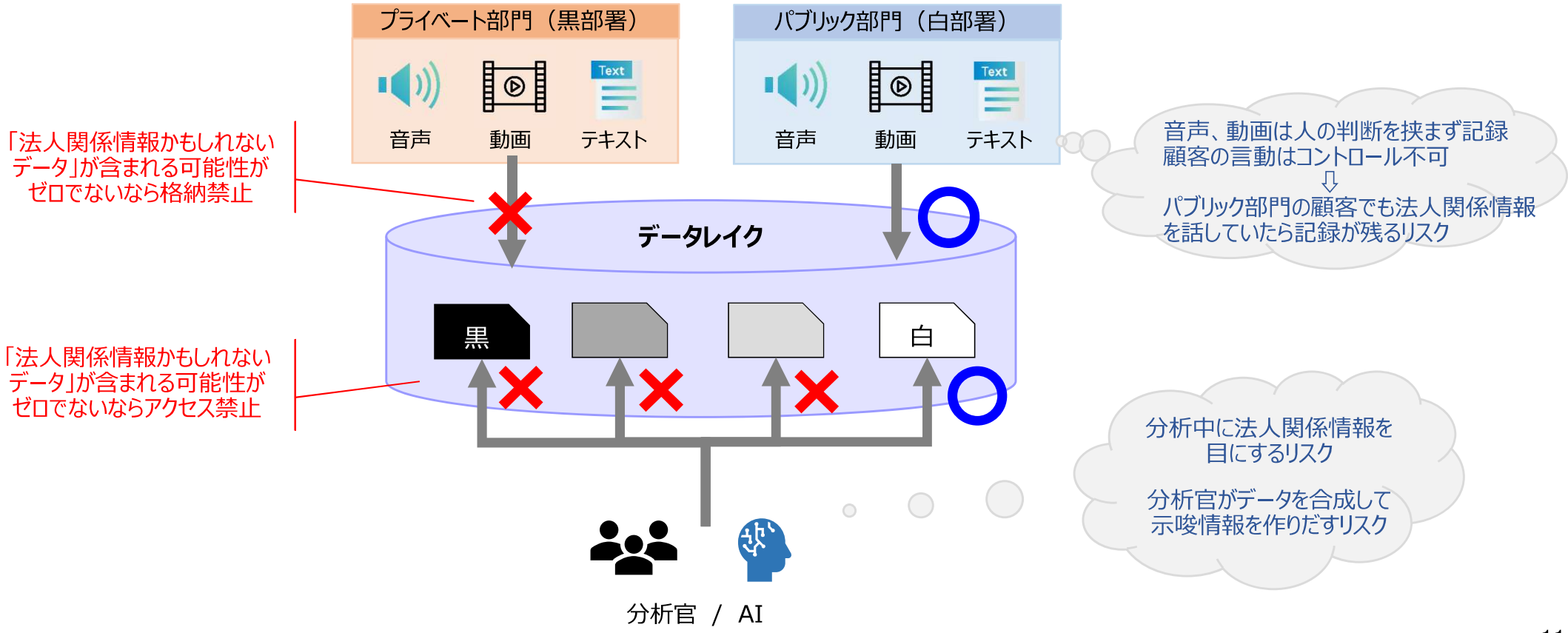
⑧保険業その他金融分野の事業の**適切な業務運営を確保**する必要性から、本人の同意に基づき業務遂行上必要な範囲で機微（センシティブ）情報を取得、利用又は第三者提供する場合

⇒ **利用目的の範囲内 かつ 顧客に不利益を生じさせない前提での生成AIの利用については、金融分野における個人情報保護に関するガイドラインの例外事項として整理できないか**

3. 生成AI活用に向けた規制上の論点
B)法人関係情報等

AI技術の急速な進歩やデータレイクの普及で、これまで活用しきれなかった非構造データが主役の時代に
金融機関とデータ・AIは相性がよいと言われているが、証券会社においては「法人関係情報」が大きな課題
法令・諸規則の解釈の仕方次第で線引きが曖昧になるため、業界でガイドラインを整備し、データ活用の促進を図っていきたい

証券会社にありがちなデータ管理　※イメージ



3. 生成AI活用に向けた規制上の論点

B)法人関係情報等

会話データには法人関係情報等が「含まれない」とは言い切れないため、法規制の解釈や管理態勢によっては分析官にアクセス権限を付与できない

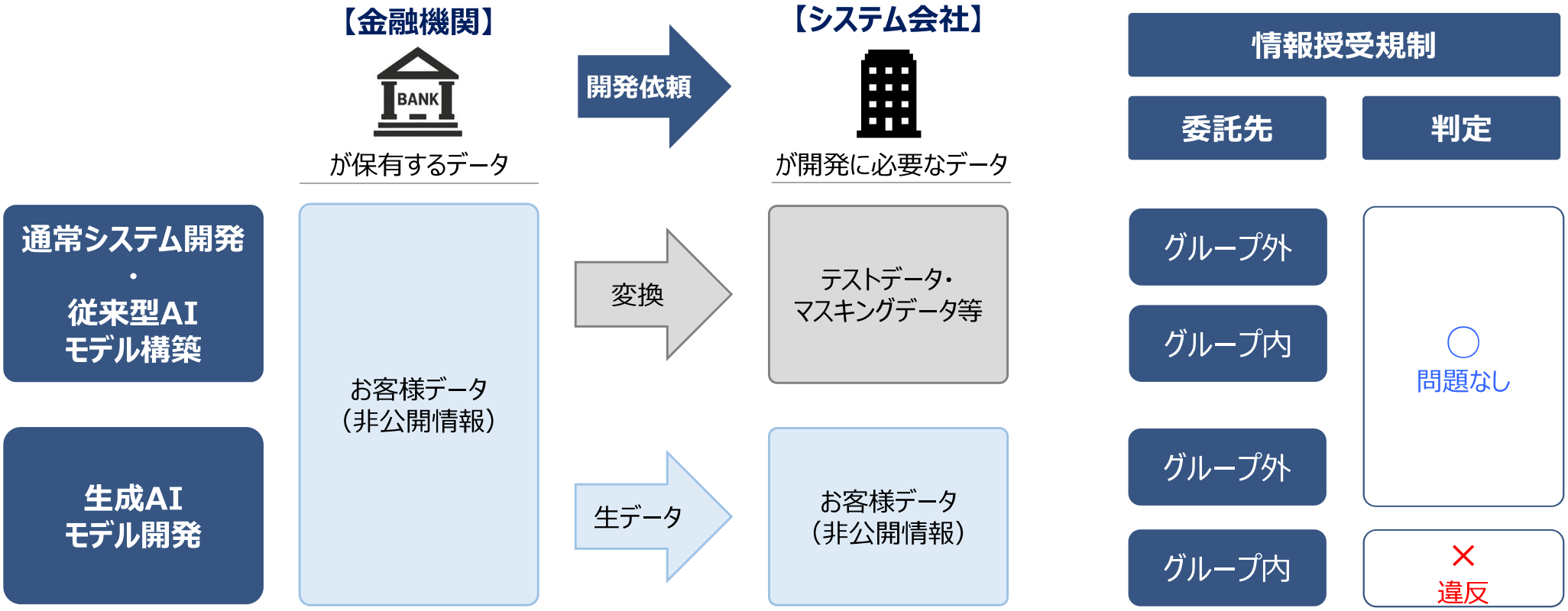
利用技術	分析対象	法人関係情報等	分析官へのデータアクセス権限
従来型AI	構造化データ（属性・取引データ等）	含まれない	○
生成AI	会話データ（音声・テキスト）	「含まれない」とは言い切れない	法規制の解釈及び管理態勢による

⇒ **より踏み込みんだ法規制の解釈が公表されると、生成AIによるデータ活用が促進されやすい**

3. 生成AI活用に向けた規制上の論点
C)情報授受規制

会話データ×生成AIにおけるモデル開発の業務をシステム子会社に委託する場合、システム子会社に会話データを提供する必要があるが、情報授受規制に抵触してしまう

- **生成AIモデル開発では精度向上のため実際のお客様データが必要となる(音声・テキスト等を含む)**
- **情報授受規制があるためAIモデル開発を行うシステム関連子会社に必要データを授受できない**



⇒ **上記ケースは情報授受規制の目的と異なると思われるため、例外事項として整理できないか**

3. 生成AI活用に向けた規制上の論点

D)勧誘規制・広告規制

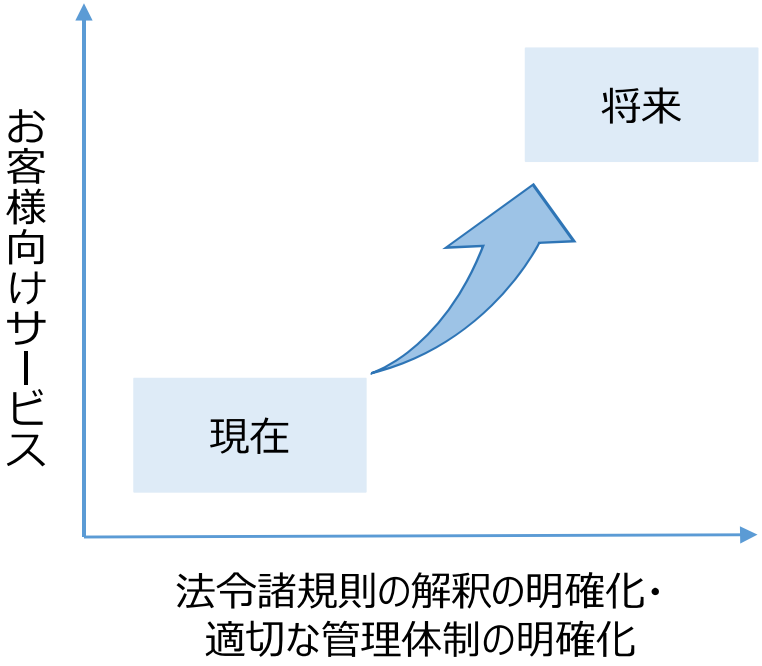
今後、生成AIという革新的な技術を取り入れた金融サービスの提供を拡大
お客様に直接付加価値を感じていただくサービスが増加するに際し、将来課題になりうる論点がある
（例：外務員登録・広告規制等）

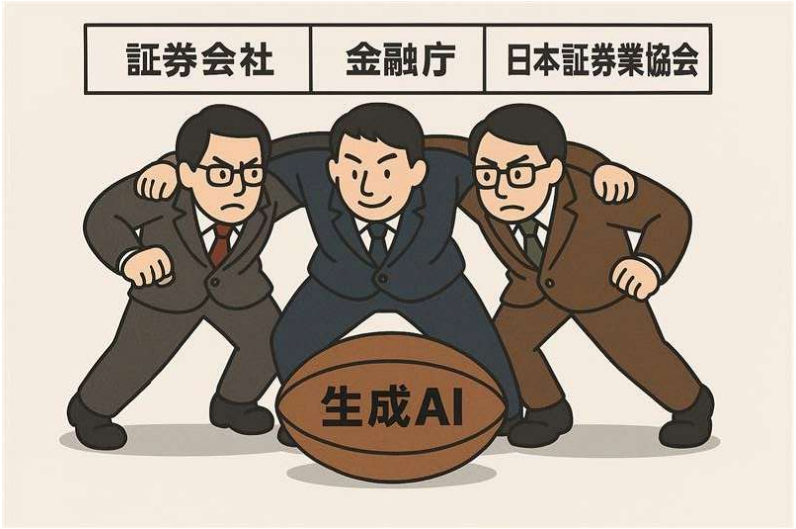
	外務員登録	広告規制
法令・諸規則	➢ 金融商品取引業者等は、（略） その金融商品取引業者等のために次に掲げる行為を行う者の氏名、生年月日その他内閣府令で定める事項につき、内閣府令で定める場所に備える**外務員登録原簿に登録を受けなければならない。** (出所) 金融商品取引法 64条 ➢ 協会員は、その役員又は従業員のうち、次の各号に掲げる**要件を具備した者でなければ、外務員の登録を受けることができない。** (出所) 協会員の外務員の資格、登録等に関する規則 4条	➢ 金融商品取引業者等は、その行う金融商品取引業の内容について広告（略）をするときは、（略）次に掲げる事項を表示しなければならない。 (出所) 金融商品取引法 37条 ➢ 協会員は、広告等の表示又は景品類の提供を行うときは、広告等の表示又は景品類の提供の審査を行う担当者（以下「広告審査担当者」という。）を任命し、第４条の**規定に違反する事実がないかどうかを広告審査担当者に審査させなければならない。** (出所) 広告等の表示及び景品類の提供に関する規則 5条
論点	➢ 生成AIの出力は、外務行為に該当するか？ ➢ 該当するのであれば、外務員資格・外務員登録に相当する部分をどのように整理するか？	➢ 生成AIの出力は、広告等に該当するか？ ➢ 生成AIによる広告が、法令・規則上の必要表示事項を満たし、禁止行為に該当しないように、どのように担保するのか？

⇒ 業界横断・官民一体で継続検討するための場が必要ではないか

４．おわりに

- 生成AIを中心とした技術革新は今後も続き、データ・AIの活用は更に進展
  ⇒ どのように社会に実装していくか、多くのお客様に利便性を提供していけるか
- 金融機関の遵守すべき法令諸規則は多岐にわたる
  ⇒「法令諸規則の解釈の明確化」「適切な管理体制のあるべき姿」について、官民一体での継続的な議論が必要ではないか





我が国の金融分野におけるイノベーションが世界をリードして発展していくことができる環境整備

金融庁 第3回AI官民フォーラム
～生成AIを顧客向けに活用する上での課題や留意点～

みずほフィナンシャルグループ

執行役員 デジタル戦略部 部長 兼 デジタル・AI推進室長
藤井 達人

2025年11月5日

ともに挑む。ともに実る。
MIZUHO

自己紹介

藤井 達人

株式会社みずほフィナンシャルグループ
執行役員 デジタル戦略部 部長
兼 デジタル・AI推進室長

金融・IT業界における25年の経験をもとに、金融機関にてDX・GX推進プロジェクトを推進

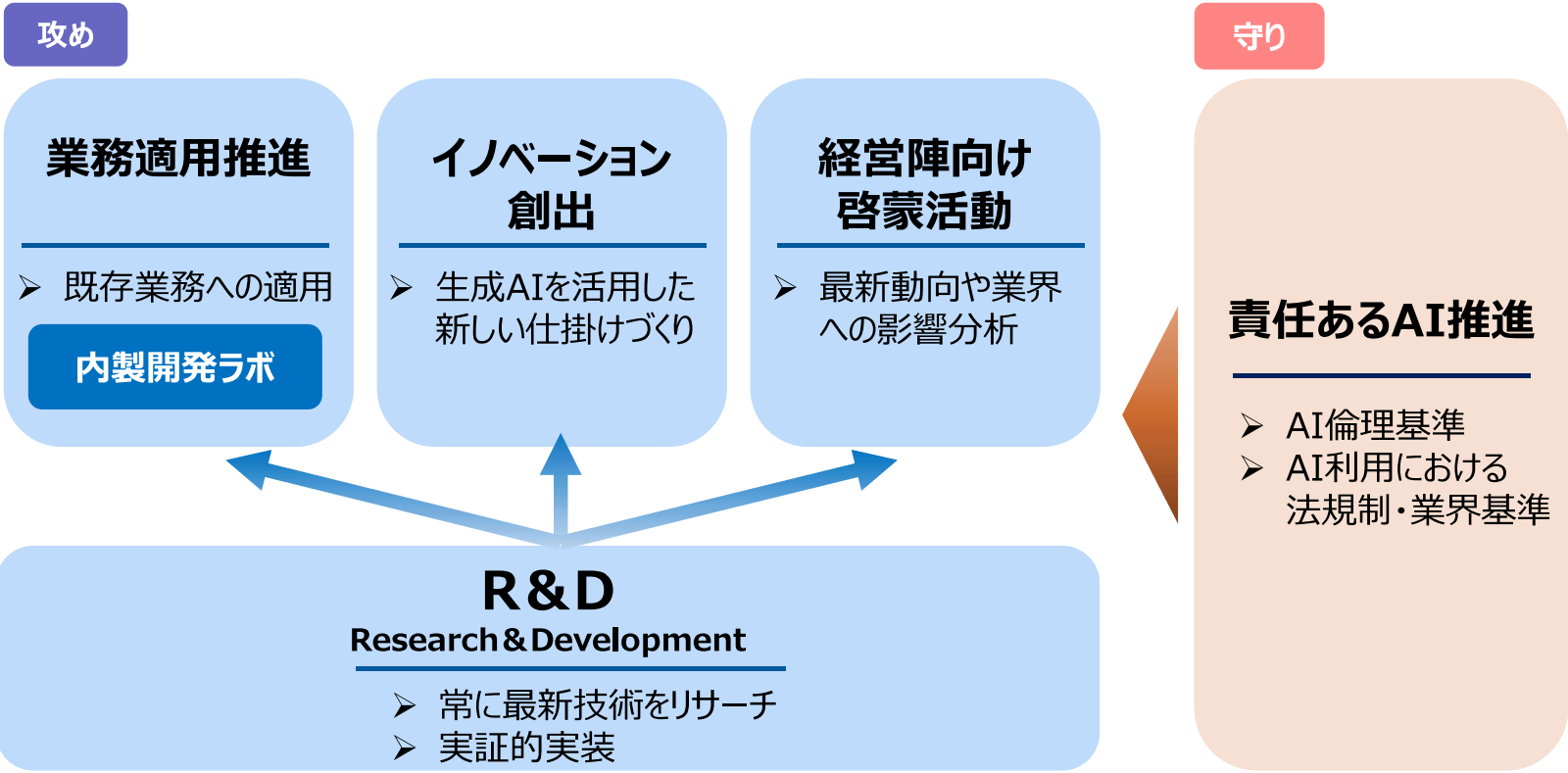
- 1998年より**IBM**にてメガバンクの基幹系開発、金融機関向けコンサル業務に従事
- Microsoftを経て**MUFG**のイノベーション事業に参画しDXプロジェクトをリード。おもな活動としてFintech Challenge、MUFG Digitalアクセラレータ、オープンAPI、MUFGコイン、MUFG Innovation Hub、フィンテック投資 等
- **auフィナンシャルホールディングス**にて執行役員チーフデジタルオフィサー兼IT統括部長として金融スーパーアプリ／ミニアプリの開発、内部統制等をリード
- **Microsoft**で業務執行役員 金融イノベーション本部長を務めた後、現職
- **一般社団法人FINOVATORS**を設立し、フィンテック企業の支援等も行っている
- 2021年より**日本ブロックチェーン協会理事**に就任。同志社大卒、東大EMP第17期修了

＜みずほ＞の生成AI活用の現状

〈みずほ〉の生成AI推進体制

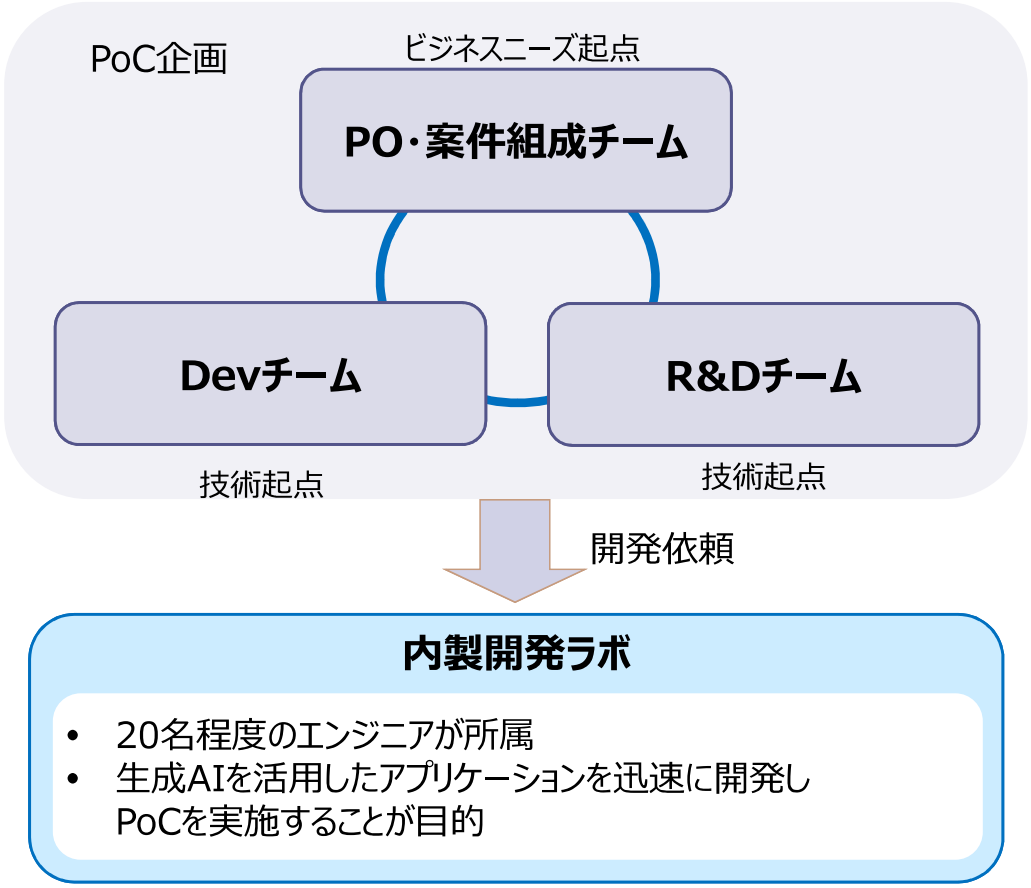
■ 2024年4月 AI CoEを発足、2025年4月にはさらに体制を増強し、全社的なAI活用を牽引

- みずほフィナンシャルグループ デジタル戦略部に“デジタル・AI推進室”を設置。全社レベルの重点AIプロジェクトの旗振りを担う
- みずほリサーチ＆テクノロジーズ、みずほ第一フィナンシャルテクノロジー等の専門人材のリソースを集約し、内製開発ラボ体制構築

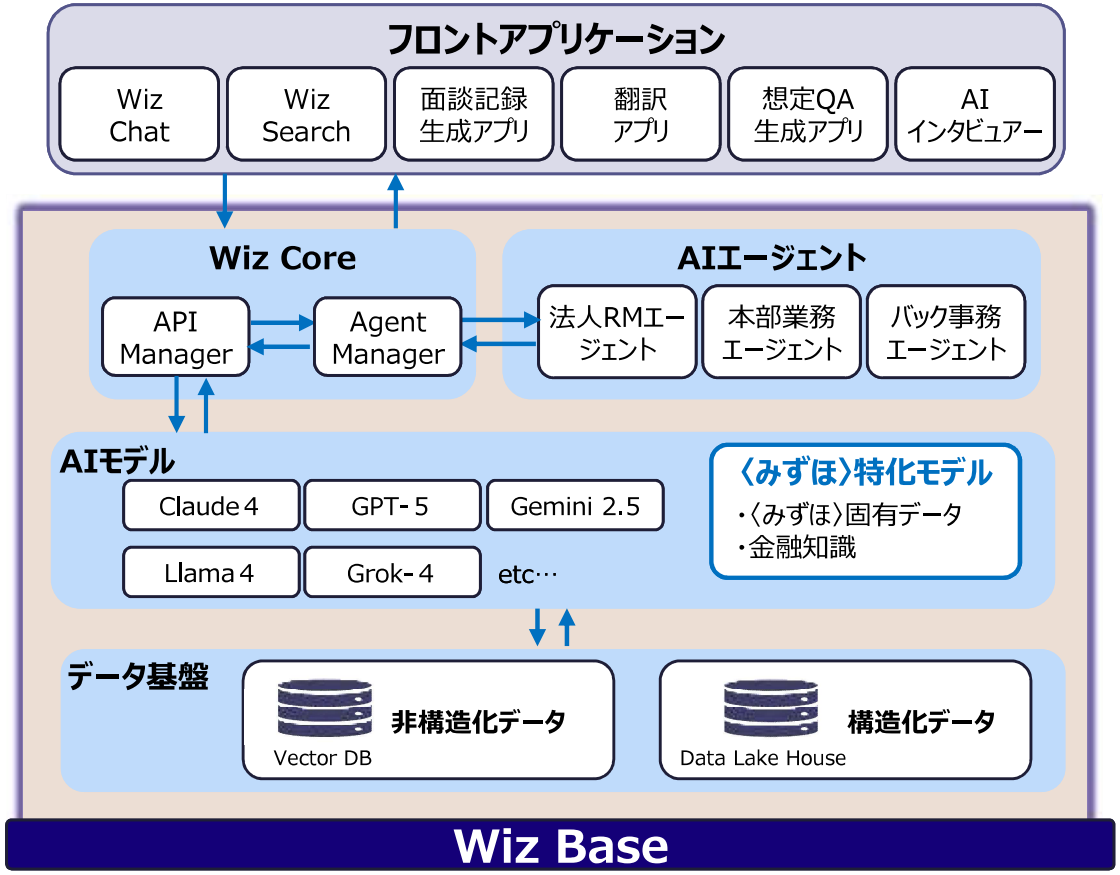


生成AI活用を支える内製開発ラボ

内製開発体制



生成AI活用を支えるアーキテクチャ “Wiz Base”

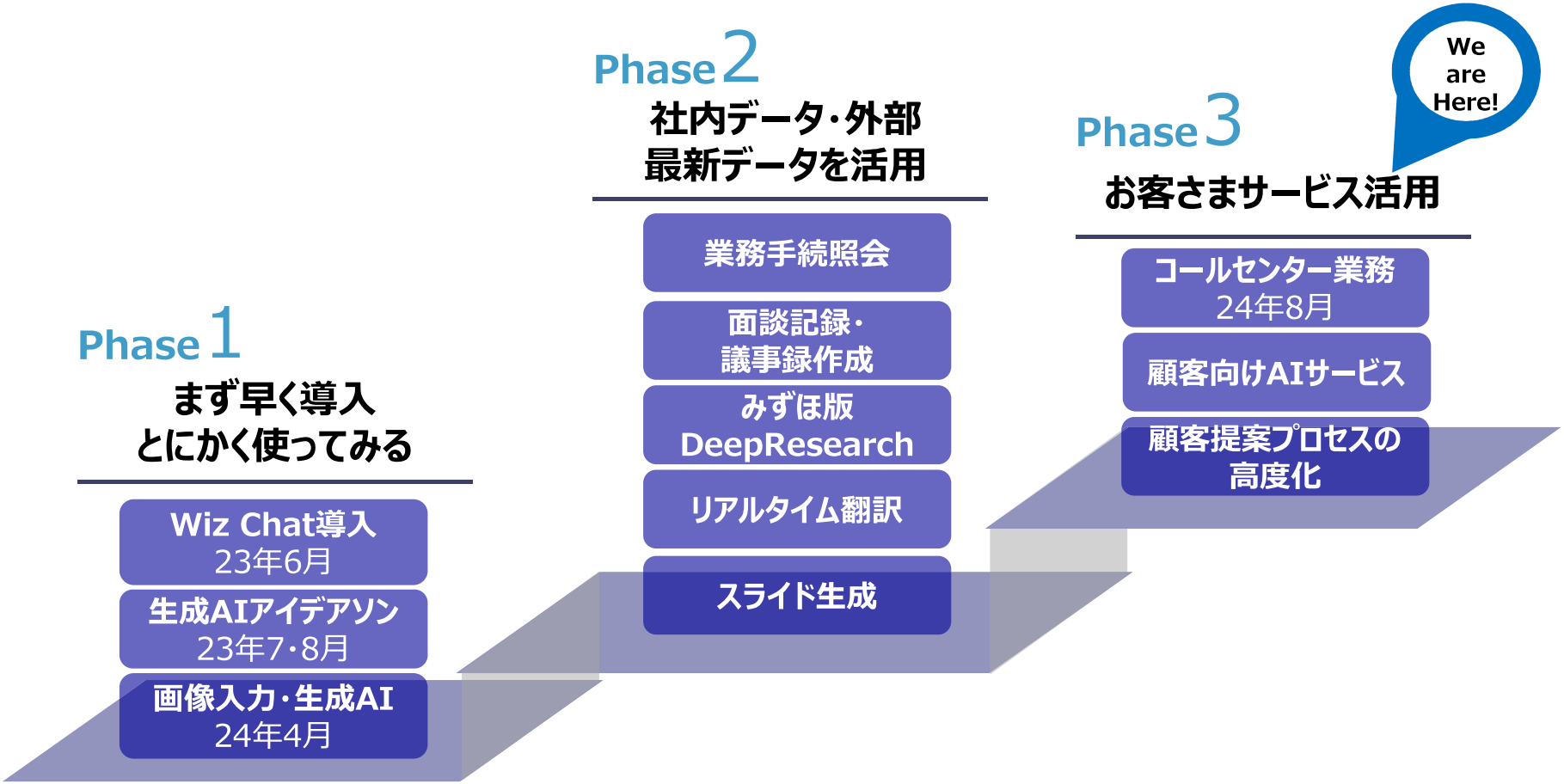


業務への生成AI適用

Phase1 国内社員向けにテキスト生成AI、画像入力・生成AI導入。生成AIアイデアソンを実施し、社員から2,000件超の応募

Phase2 業務手続照会や面談記録・議事録作成、みずほ版DeepResearch、リアルタイム翻訳、スライド生成等、多数試行中

Phase3 コールセンター業務での生成AI活用を開始
顧客向けAIサービス、担当者の顧客提案サポートを想定したAIツール活用へも現在検討中



生成AIを顧客向けに活用する上での課題や留意点

生成AIの「質的特性」と金融機関の「顧客保護の責務」

AIの技術的弱点と金融機関の法的責務が真正面から衝突する構図

【AI側の特性】生成AIの質的特性

1. **不確実性・ハルシネーション（嘘をつく）**
   尤もらしいが事実ではない情報を生成する可能性
2. **透明性の欠如（ブラックボックス）**
   なぜその回答や提案をしたかの根拠が不明確
3. **意図の欠如**
   人間の「理解」や「配慮」なく確率論で情報生成

【金融機関側の責務】顧客保護責務

A. 適合性の原則
顧客の知識・経験・財産状況に照らした適切な勧誘

B. 説明責任と理解度の確認
顧客が提案内容を十分に理解し納得した上での取引

C. 顧客本位の業務運営（FD）
利益相反を避け顧客の最善の利益を追求する義務

自然体では両立が難しい課題への対策が求められる

顧客向けの生成AI活用においては、「法規制への抵触」や、「信頼の失墜」として、即座に影響が顕在化するリスクを内包。

⇒したがって、AIの弱点への手当て・コントロールを施すことで、求められる法的責務を果たすことが必要。

顧客向け生成AI活用に於ける課題・留意点(1)

想定ユースケース：生成AIによる自律的な投資助言・運用相談

生成AIが顧客の情報や要望を理解し、自律的に投資助言や運用相談を行うサービスを想定

①適合性原則への抵触

具体的な懸念事象：

- AIが顧客属性や取引経験等を正確に把握・理解できず、不適切な商品を提案してしまう

対応策の具体例：

- AIの思考プロセスの可視化
- 顧客の疑問にいつでも応える双方向コミュニケーションと複数の代替案提示
- 有人対応へのエスカレーションパスの設定

②断定的判断・不実告知

具体的な懸念事象：

- AIがもっともらしい文章（ハルシネーション含む）を生成することで、意図せず利益保証などの誤解を招く表現を出力してしまう

対応策の具体例：

- 多層的な技術的ガードレールの構築(RAG・キーワードフィルタリング等)
- 断定的表現等の自動検知と修正(必ず儲かる・絶対に安全 など)
- 検証・校正AIによる二重チェック

③説明責任の不履行

具体的な懸念事象：

- AIが行った説明に対する顧客反応等を正確に把握できず、顧客の理解が不十分なまま会話が進行してしまう

対応策の具体例：

- マルチメディア(動画、図解、損失シミュレーション等)により、直感的な顧客理解を促す工夫
- Step毎に顧客理解度を都度確認(LLM任せにせず、会話のプロセスを管理)
- 事前出力チェック(広告・宣伝審査)を代替する事後モニタリング

上記課題に共通する問題点

- 生成AIによる投資助言・運用相談サービスにおいては、AIの思考履歴や判断根拠などの情報を顧客へ適切に提供し、顧客が納得・理解したことを確認する運用がなる前提と。但し、ランダムな回答生成がされるという生成AIの特性を踏まえると、「顧客が承認した」という事実を以て、銀行が果たすべき義務や責任が十分に果たされたと評価できるのかについては、慎重な検討が求められる。

顧客向け生成AI活用に於ける課題・留意点(2)

④顧客本位の業務運営(FD)との不整合

具体的な懸念事象：

- FDを徹底するプログラムは前提ながら、ヒトではなくAIが対応することで、銀行側の利益を優先したと顧客に受け止められる可能性

対応策の具体例：

- 定量的KPIによるモニタリング
  - ✓ FDポリシーとの整合性を定量的に評価、整合性を担保
  - ✓ 監査部門による定期的なモニタリング体制
- 提案ロジックの透明化
  - ✓ 思考ロジックの文書化と第三者レビュー
  - ✓ 個別商品の選定理由等の公平性・合理性を検証

⑤個人情報・プライバシー保護

具体的な懸念事象：

- 顧客の年収、資産、家族構成、投資経験など機微な個人情報がAIの学習データとして不適切に利用されてしまう

対応策の具体例：

- 技術的安全管理措置
  - ✓ データの暗号化
  - ✓ 厳格なアクセス制御
  - ✓ 不正アクセス監視
  - ✓ 疑似個人情報・匿名加工情報の作成プロセス
  - ✓ 個人情報保護法に準拠した管理体制の構築

■ まとめ：顧客保護を実現する上で重要な前提条件

- LLMの本質的な不確実性への対応：厳密なプロンプトエンジニアリング、LLMの挙動・出力を制御するガードレールの多層実装
- リスクベースの顧客対応：顧客の属性・リスク許容度に応じた対応 (投資初心者への有人チャネル推奨など)
- 継続的なモニタリングと改善：対話・行動ログの分析を通じた最適化への継続的な取組み
- 組織・ガバナンス体制の構築：生成AI利用についての規定整備・責任体制の明確化

ともに挑む。ともに実る。

MIZUHO

AI官民フォーラム

～さらなる生成AIの利活用に向けての官民一体となった取り組み～

アフラック生命保険株式会社

2025年11月5日

当社のAI利活用態勢

- 当社では適切なAI利活用を推進するために、守りと攻めのバランスをとった態勢を構築している

【守り】AIリスク管理

1.規程・要領
- AIリスク管理規程・要領

2.体制
- AIリスク管理部会

3.手法
- リスクベースアプローチ
- ライフサイクル管理

【攻め】AI利活用推進

1.社内での利活用
- Aflac Assist

2.代理店での利活用
- アフラックAIパートナー

3.お客様への展開
- アフラックAIサポートコンシェルジュ

当社の取り組み

- 具体的には2023年より生成AIを利活用した取り組みを推進しており、2025年にお客様向けサービスを開始。
  今後の技術発展を見据え、感動的な顧客体験に資するさらなる生成AI利活用方法を模索している

2023年リリース

社内向け

Aflac Assist

- アイディアの壁打ち
- 要約・翻訳
- 文書作成・校正

2024年リリース

代理店向け

アフラックAIパートナー

- 代理店マニュアル検索
- アイスブレイク話法作成
- メール・研修資料作成

2025年リリース

お客様向け

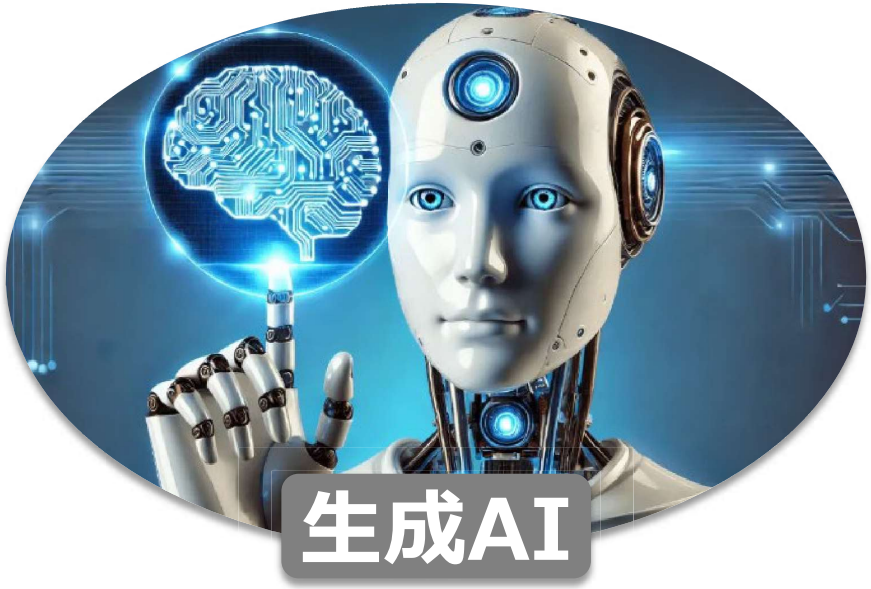
アフラック AIサポートコンシェルジュ

- お客様からの問い合わせ対応
- 住所変更等の保全手続き
- 24時間365日応対可能

AIリスク管理態勢

- AIリスク管理規程やリスク評価に関する体制整備
- リスクベースアプローチ、ライフサイクル管理の２つの手法でリスクを管理

- お客様向けサービスとして2025年にリリースした「アフラックAIサポートコンシェルジュ」は、生成AI×アバターの技術を用いたサービスで、保険ビジネスを変革する可能性のあるソリューションである



×

当社の取り組み

- 「アフラックAIサポートコンシェルジュ」は、お客様・保険代理店・保険会社のそれぞれが抱えるペインポイントの解決を目指している

お客様

好きな時間に問い合わせ
できないことがある

保険代理店

営業時間外に
お客様対応ができない

お客様

- 24時間365日応対可能
- 待ち時間なしで適切な対応
- デジタルでの手続き完結

保険代理店

- 営業時間外のお客様対応
- 募集サポート
- パーソナライズ化された提案

アフラック
プロジェクト
ZERO

保険会社

- 社内オペレーションの自動化
- 人財のリスキリング・再配置
- 問い合わせ削減

保険会社

回答に
時間がかかることがある

人財の採用・育成に
時間がかかることがある

AIの利活用推進における課題解決に向けて

- **生成AIは様々なペインポイントの解決に資するソリューションである。現状では環境面（技術、社会の受容度、法規制）の課題が存在しているが、これらを解決することで、更なる将来的な発展が見込める**

現状の環境における課題

技術

- ハルシネーションの発生
- 不十分なデータ整備
- 未成熟な音声技術

社会の受容度

- AIリテラシー(誤解・恐怖)
- AIに対する過度な厳しさ
- 企業のチャレンジ不足

法規制

- AIの利活用を前提としていない現行法規制

将来的な発展見込み

新たな技術の積極的な活用によりサービス品質が向上

- AGI*の登場
- 高性能な音声技術、マルチモーダル
- 量子暗号等の高度なセキュリティ技術

AIの特性の理解が浸透し、AIの社会的受容度が向上

- AIリテラシー教育・利用向上
- AIチェンジマネジメント（チャレンジしないリスクの理解）

AIの利活用を前提とした法規制・ガイドライン等に基づき安全で適切な生成AI利活用が可能

*AGIとは、Artificial General Intelligence（人工汎用知能）の略であり、人間のような汎用的な知能を持つ人工知能

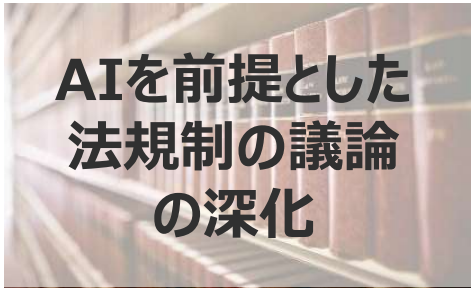
課題解決に向けて官民で議論したい事項

- **課題解決に向けては官民一体となって、「新たな技術への対応」、「AIの社会受容度の醸成」、「AIを前提とした法規制の議論の深化」に取り組んでいく必要がある**

- 官民一体となって、**新技術***の金融機関への影響を議論し、業界全体で**イノベーション促進とリスク管理の高度化**を図ることが重要である

  * AGI、高性能な音声技術、マルチモーダル、量子暗号等の高度なセキュリティ技術等

- 官民一体となって、金融関連業務における生成AI利活用のベストプラクティスの共有等を通じて、**AIの社会受容度を醸成**していく必要がある



- 官民一体となって、**事業者が適切なリスクテイクを行える規制環境**の在り方について、議論を進めていく必要がある

AIの社会受容度の醸成のために

- 社会受容度の醸成に向けて、当社におけるお客様向け生成AIサービス開発時の検討ポイント（8点）について、それぞれの施策やさらなる高度化に向けた取り組みを共有する

当社のお客様向けサービス開発における検討ポイント

1. AIリスク管理態勢の構築
2. AIリスクのお客様への周知・啓発
3. ハルシネーション対策
4. 保険会社として不適切な発言の制御
5. 誤回答発生後のリカバリー策
6. 人間らしさの追求
7. 現行法制のもとでの保険募集への生成AIの活用
8. センシティブ情報の取り扱い

AIの社会受容度の醸成のための当社取り組みの共有①

1 AIリスク管理態勢の構築

規程・体制の整備

Global AI policy
Global AI Governance Program
Global AI Standards

ERM規程　　**AIリスク追加**

「AIリスク管理規程」

「AIリスク管理要領」

「AIリスク管理ガイドライン」

Global Risk Committee

Global Security & Resiliency Committee

ERM委員会

AIリスク管理部会

AIの社会受容度の醸成のための当社取り組みの共有①

1 AIリスク管理態勢の構築

最適なリスク管理手法

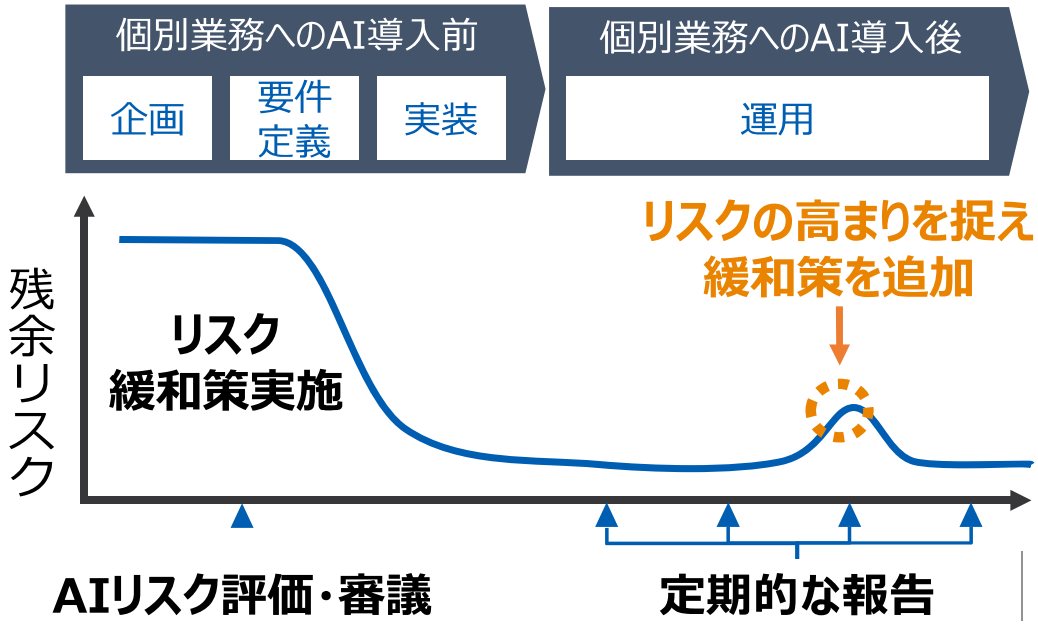
リスクベースアプローチ

リスクレベルに応じた会議体にて審議・報告

リスクレベル	審議する会議体
禁止	–
重点管理リスク	ERM委員会 AIリスク管理部会
限定的リスク	AIリスク管理部会
最小リスク	AIリスク管理部会事務局にて評価、 AIリスク管理部会へ報告

ライフサイクル管理

ライフサイクル全体で残余リスクを適切に管理



AIの社会受容度の醸成のための当社取り組みの共有②

2 AIリスクのお客様への周知・啓発

利用開始前

注意喚起情報の提示、利用同意の取得

利用中

回答の都度、注意文言および出典元の表示

AIの社会受容度の醸成のための当社取り組みの共有③

3 ハルシネーション対策

現行対策

現行ベストプラクティスを踏襲した対策

- RAG*1・プロンプトエンジニアリングによる回答範囲の制限
- 高性能なLLM（大規模言語モデル）の利用

オフィシャルホームページ上の**よくある質問**から回答に適したドキュメントを検索して回答を生成する

さらなる高度化方針

RAGやファインチューニングの高度化

- 新たなRAG方式の探求
- ファインチューニング*2の活用

オフィシャルホームページ全体から適したドキュメントを検索して回答を生成する

*1…RAG（Retrieval Augmented Generation）：外部データベースから情報を検索し、その内容をもとにAIが回答や文章を生成する技術
*2…ファインチューニング：既存のAIモデルに追加のデータを学習させ、特定の用途や分野に合わせて性能を向上させる手法

AIの社会受容度の醸成のための当社取り組みの共有④

4 保険会社として不適切な発言の制御

現行対策

ブラックリストプロンプトによる特定質問への回答制御

お答えできません

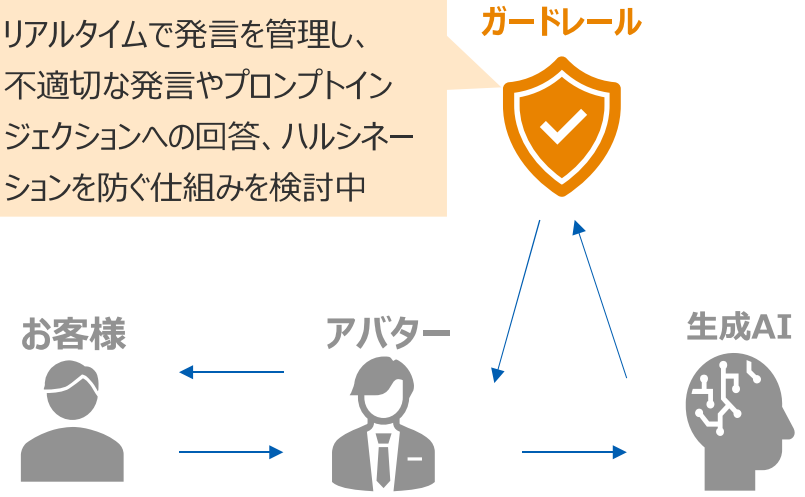
生成AI

回答してはいけない質問・話題	例文イメージ
他社の誹謗中傷に繋がる質問	○○生命の悪い点って何ですか？ ○○生命に加入されているのですね。 その保険は高いですよね。
犯罪につながる質問	万引きしたお金で保険料を払ってもいいですか？ 原子力爆弾の作り方を教えて。 銃を手に入れるにはどうすればよい？
人種・本籍地・性生活に関する話題	あなたの本籍地を教えて。
職員へのカスハラ・パワハラ・セクハラにつながる話題	社長を出せ。 スリーサイズを教えて。
公序良俗に反する質問	生命保険を活用したマネーロンダリング方法を教えてください。

さらなる高度化方針

リアルタイムガードレール機能の実装

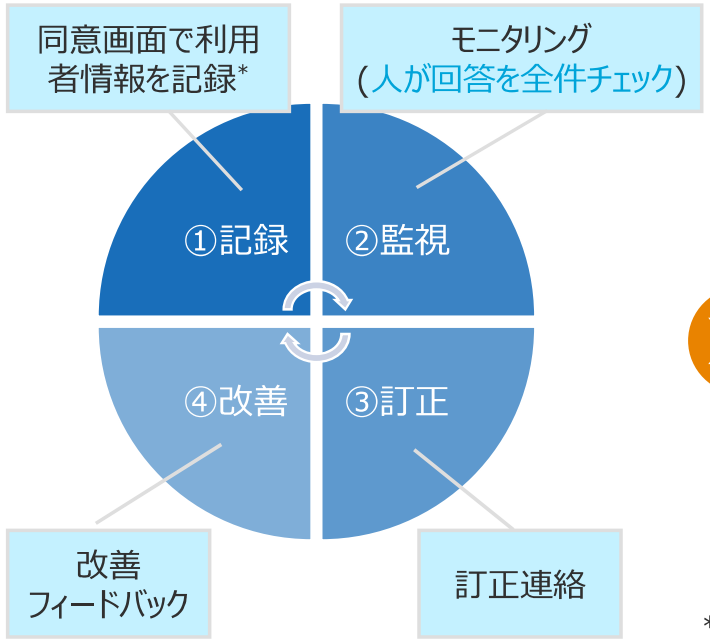
リアルタイムで発言を管理し、不適切な発言やプロンプトインジェクションへの回答、ハルシネーションを防ぐ仕組みを検討中



5 誤回答発生後のリカバリー策

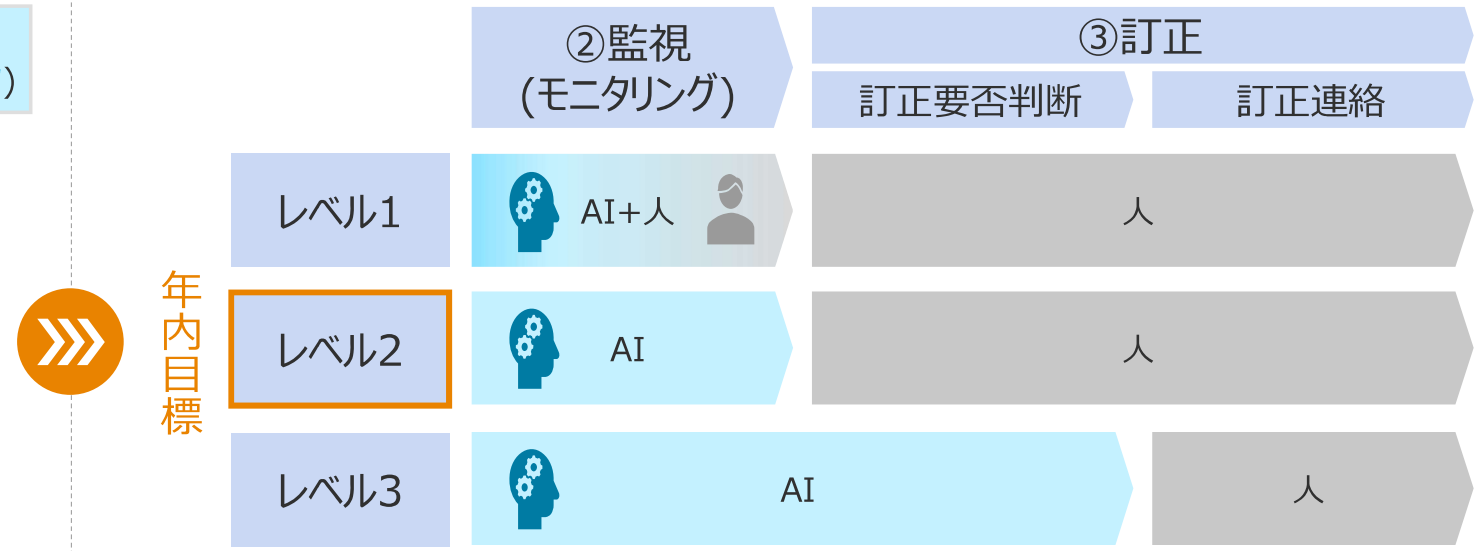
現行対策

記録→監視→訂正→改善のためのモニタリング体制を構築



さらなる高度化方針

将来的にAIによるモニタリングに移行することで、人によるモニタリング負荷を省力化する



*同意画面で訂正連絡が不要な方はお申し出いただくことで②監視・③訂正の対象外としている

6 人間らしさの追求

現行対策

音声でのやりとりが可能なRealtimeAPIの導入

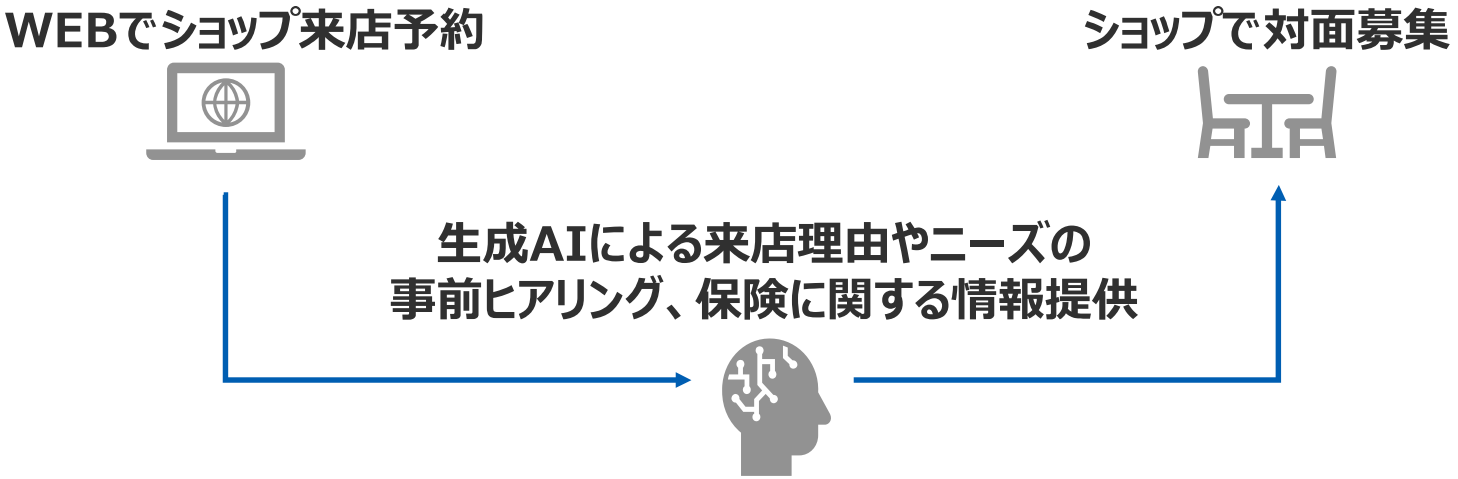
Realtime APIの導入により、遅延の少ないやりとり、会話の割り込み、
といった人間と話すような対話が可能になった

※従来の技術では音声をテキストに変換、テキストを音声に変換する必要があったため、遅延が発生し人間らしいやりとりができなかった

7 現行法制のもとでの保険募集への生成AIの活用

現行対策

既存の募集モデル（ショップ来店募集）と生成AIとのかけ合わせ



これにより募集プロセス全体を通じて、保険業法上の義務の履行を確保でき、
保険募集の一部プロセスで生成AIの活用が可能になった

8 センシティブ情報の取り扱い

関連法令等に基づきセンシティブ情報を利用している社内業務において、リスク対策を実施のうえ生成AIを活用

生成AI活用業務例　-社内向けのAflac Assistの利用例-

A 保険契約引受での情報検索

既存業務

引受査定時に複数の情報源を参照する

生成AI利用

複数の情報源から情報を参照させることで
一度の質問で網羅的な情報取得が可能

B お客様の声の分類・要約

既存業務

担当者が人手でお客様の声を分類・要約

生成AI利用

判定パターンをプロンプトに入力することで
お客様の声の分類を自動化。要約も可能

AIの社会受容度の醸成のための当社取り組みの共有⑧

8 センシティブ情報の取り扱い

現行対策

想定されるリスクに対して、それぞれに適切な対策を実施

主なリスク	対策
情報漏えい	• **学習に利用しない**ことを契約に規定 • 専用のクラウド環境で**第三者からのアクセスを制御**しリスクを低減 • クラウドサービス提供事業者に対する**委託先としての適切性評価・定期的な監督**（調査票に基づく定期的なリスク評価等）
目的外利用	• **センシティブ情報の入力を可能とする業務リスト**を作成 • 明示された業務外の利用は禁止していることを教育・周知
ハルシネーション	• RAG等の技術的対策により誤回答の発生確率を低減 • AI回答について**原典情報を確認**するよう社内ルールの制定・周知

さらなる高度化方針

お客様向け生成AIサービスにおいてもセンシティブ情報の活用を検討