生成AI時代のセキュリティガバナンス

AI活用を把握し、最大活用を推進するためのIT基盤

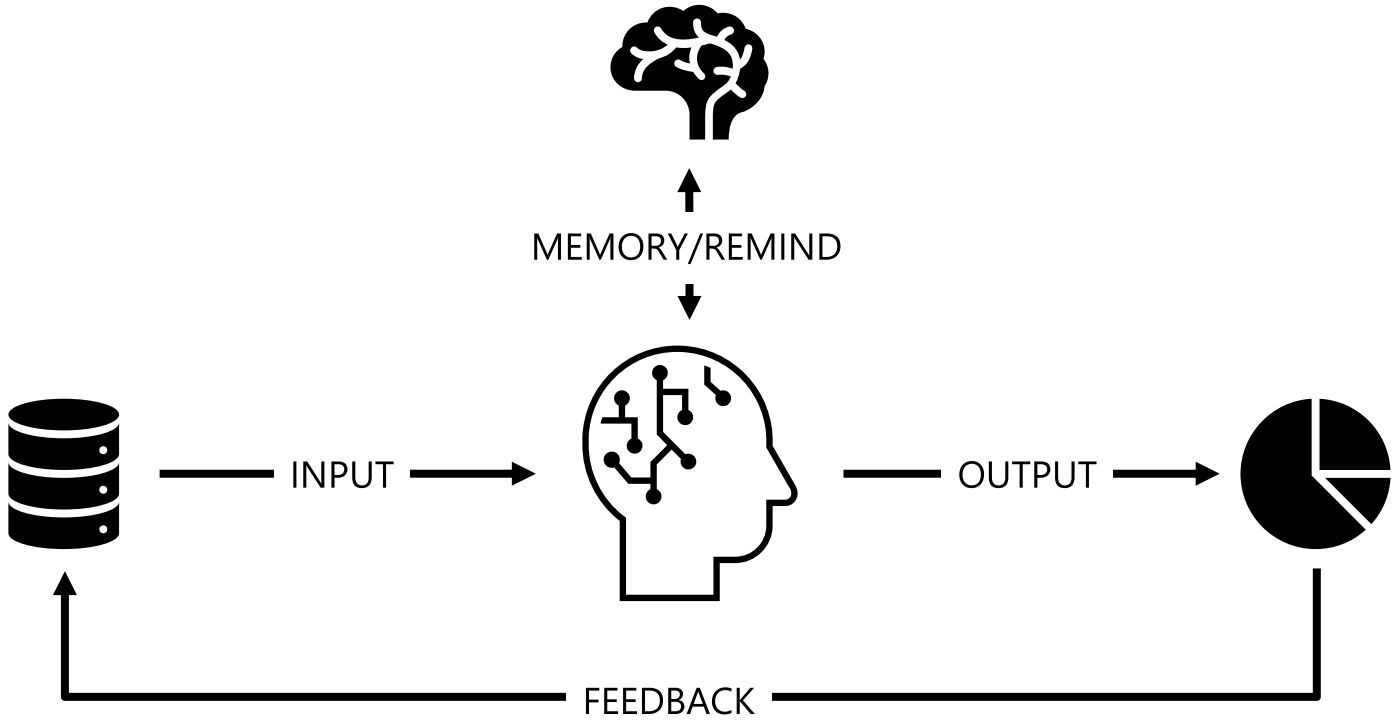
日本マイクロソフト株式会社
Chief Security Officer
河野省二, CISSP

Microsoft

そもそもAIってなんだろう

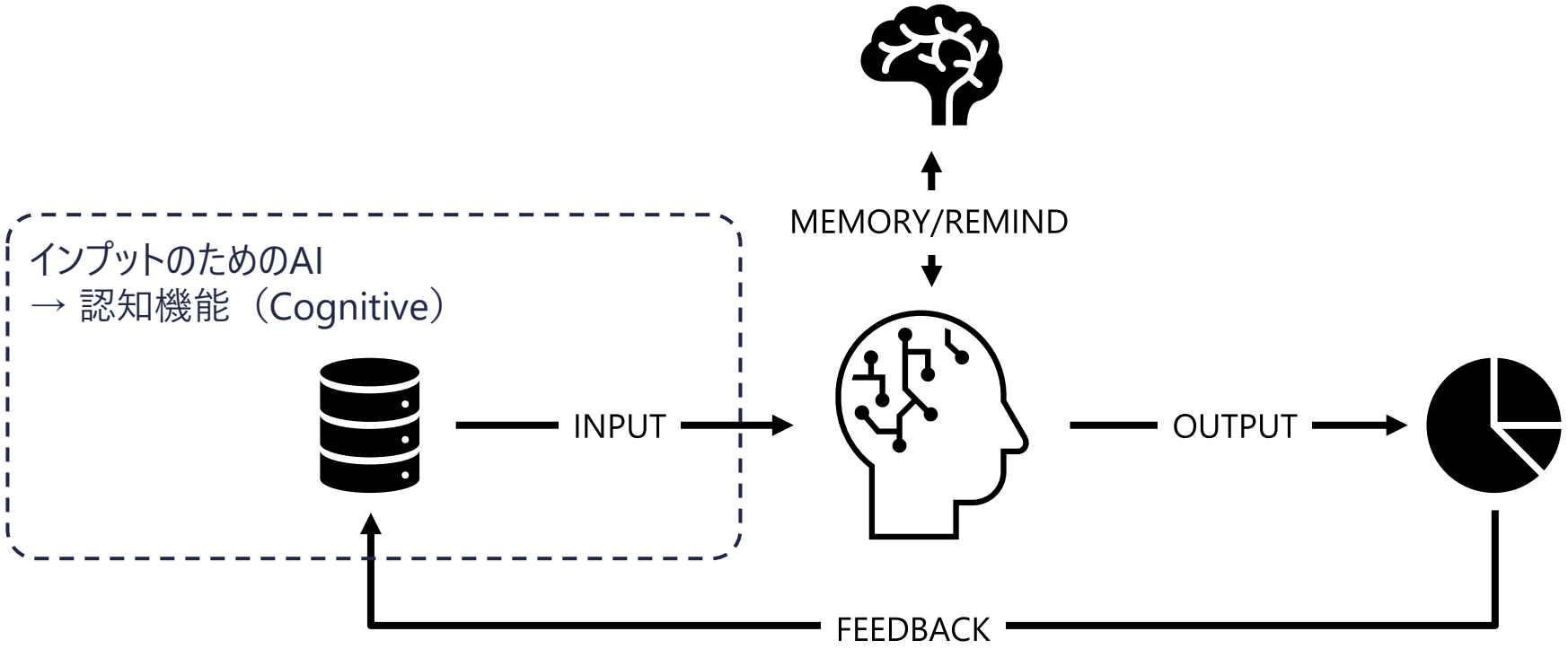
人工知能っていうんだから、人間の知能に似せたものでしょ

そもそもAIってなんだ？



AIとは人間の思考を機械的に実現する技術

そもそもAIってなんだ？



AIとは人間の思考を機械的に実現する技術

Human Parity

人間と同程度の課題解決能力

Human Parity – データの判断

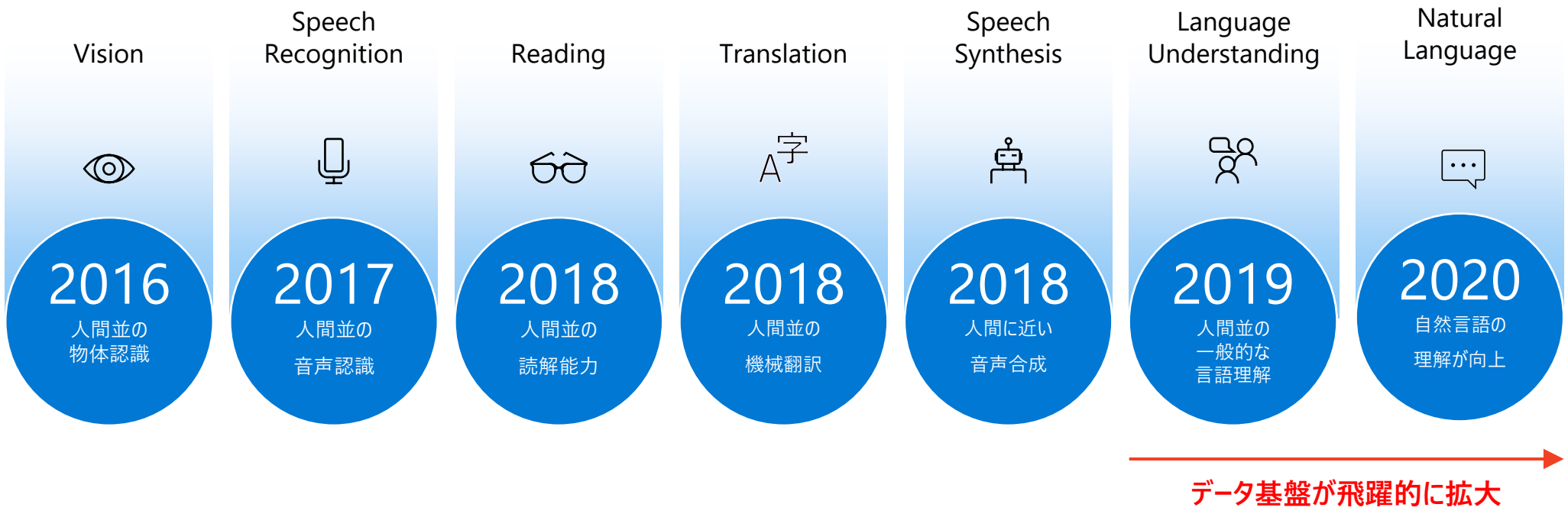
様々なものを判断できるようになり、データ収集に役立つようになりました

Human Parity – データの合成

音声合成ができるようになったことで、音声データを集めなくてもデータを自ら作り出すことができるように

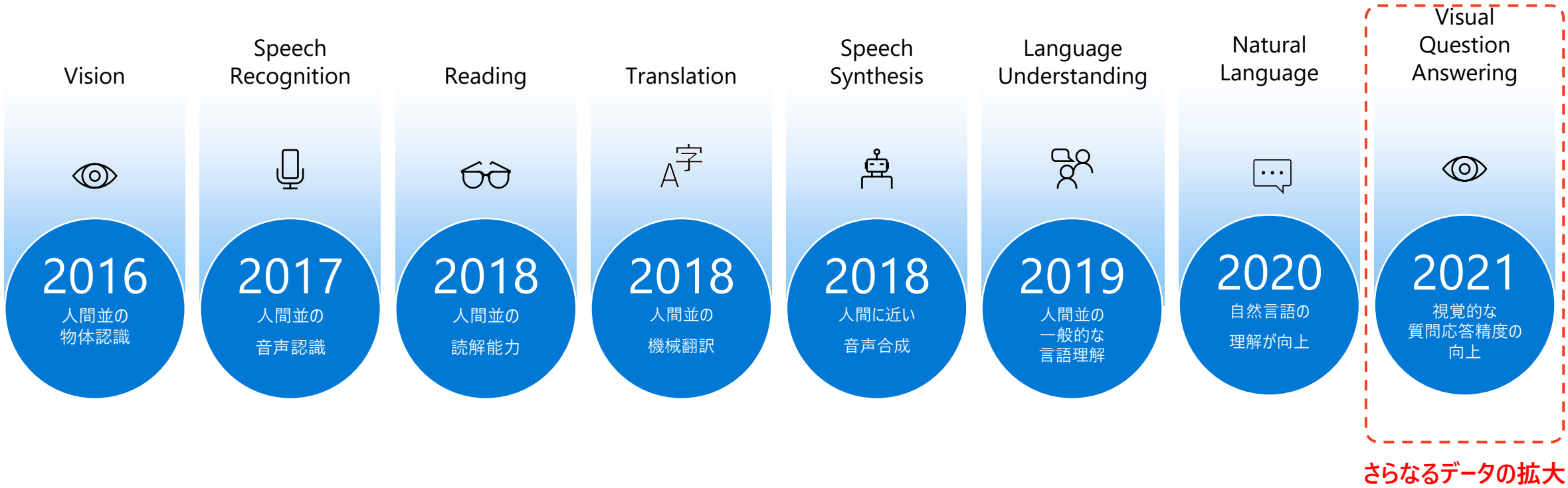
Human Parity – データ基盤の拡大

自ら作成したデータで自律的にデータ基盤を拡大することができるように



Human Parity – 人間の目と同じ機能を獲得

Visual Question Answering によって、目の前にあるもの全てを自然言語で表せるようになった

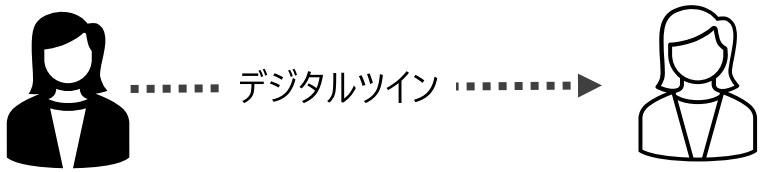


Industrial Metaverse

データを作り出すための基盤としてのメタバース


Kawasaki

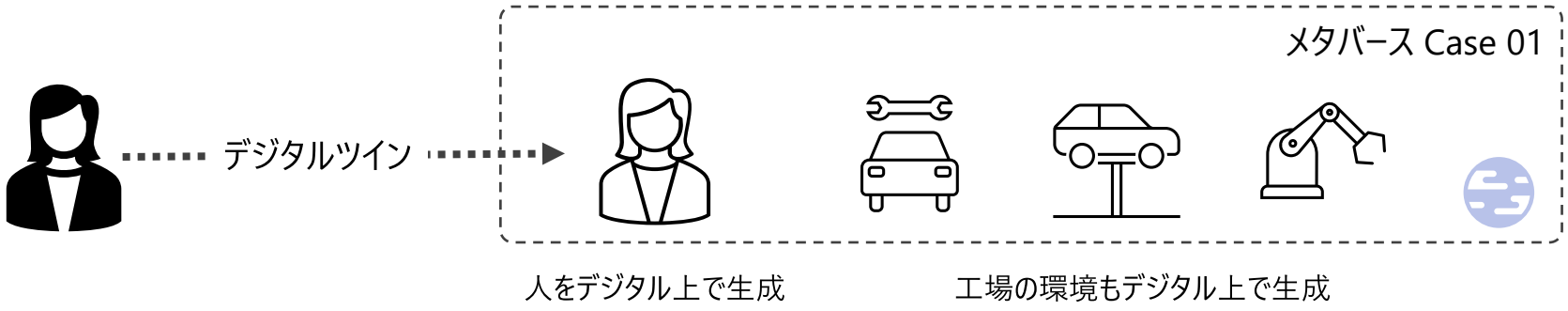
AIが新たなデータを作り出す環境 – メタバース



人をデジタル上で生成

AIによって現実社会と同じものを複製することができるようになります

AIが新たなデータを作り出す環境 – メタバース

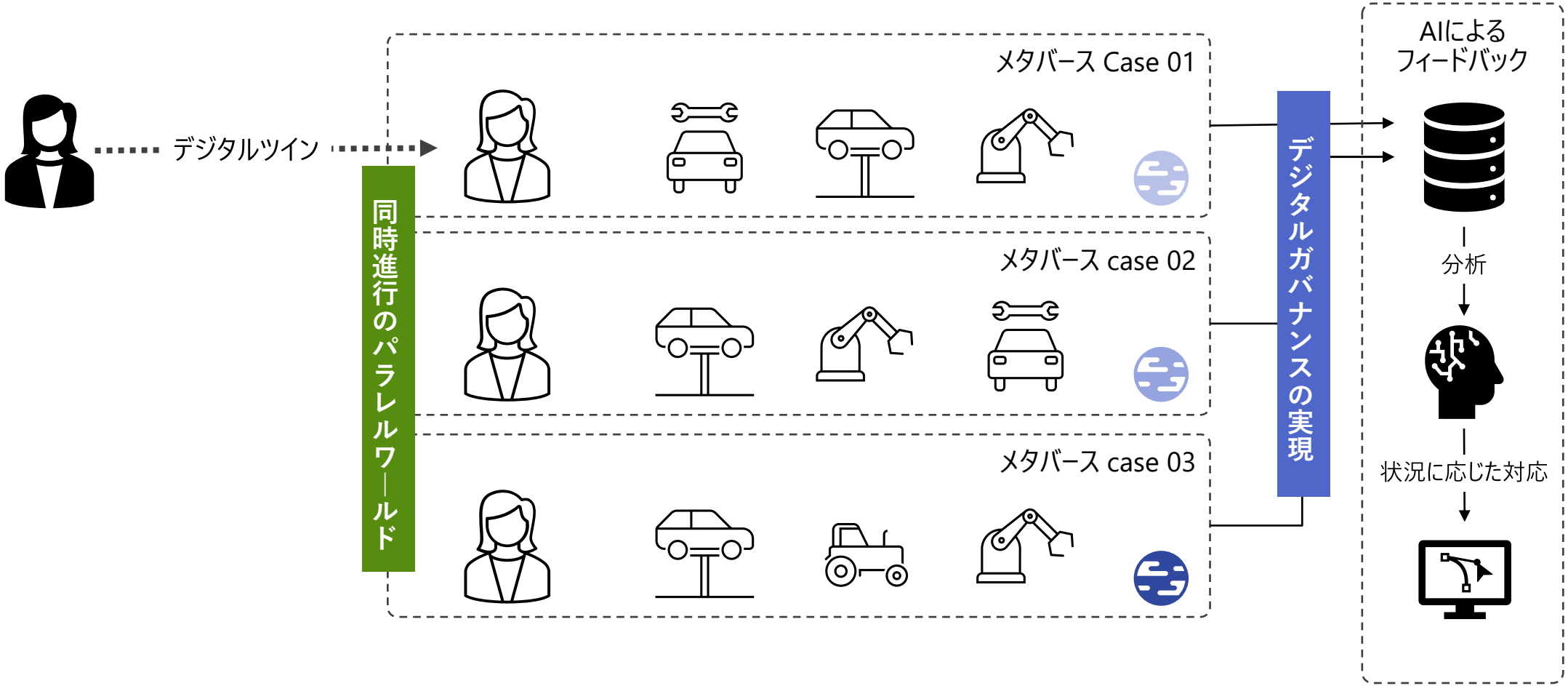


それは人間だけではなく、機械や工場の機器、そこで利用される素材も同様です

AIが新たなデータを作り出す環境 – メタバース

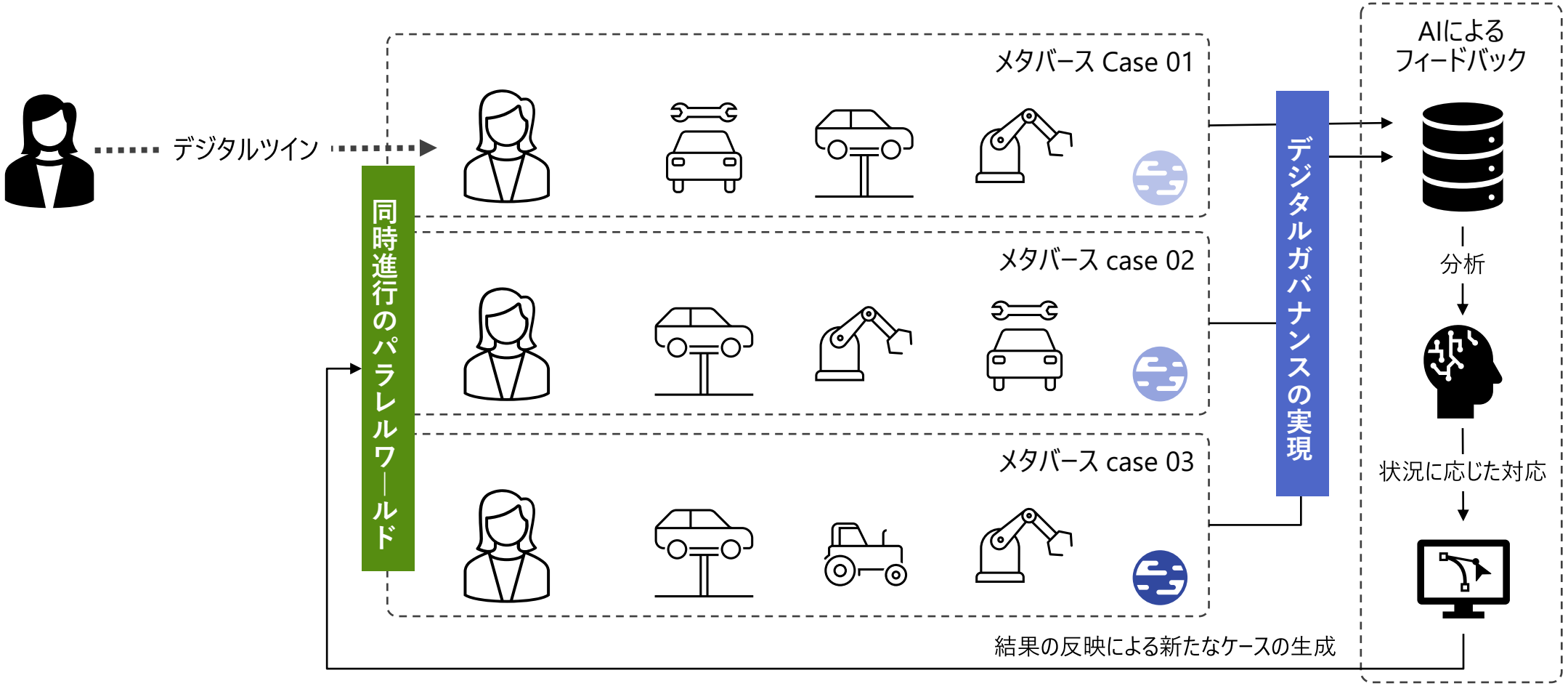
モノの状態や活動はデータとして記録され、それを元に分析、改善が行われます

AIが新たなデータを作り出す環境 – メタバース



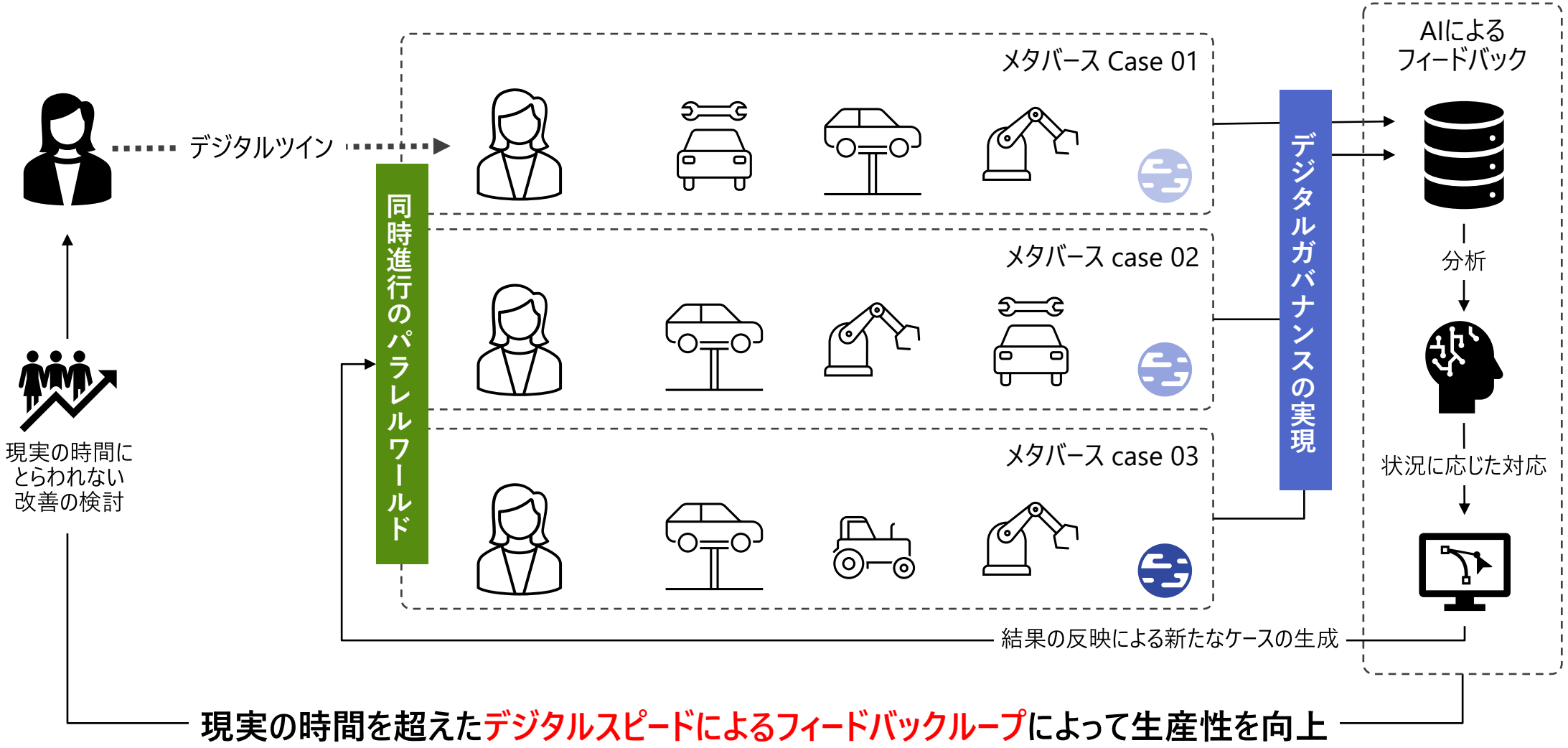
デジタルツインをさらに複製することで、同時に様々な環境を実現することができます

AIが新たなデータを作り出す環境 – メタバース

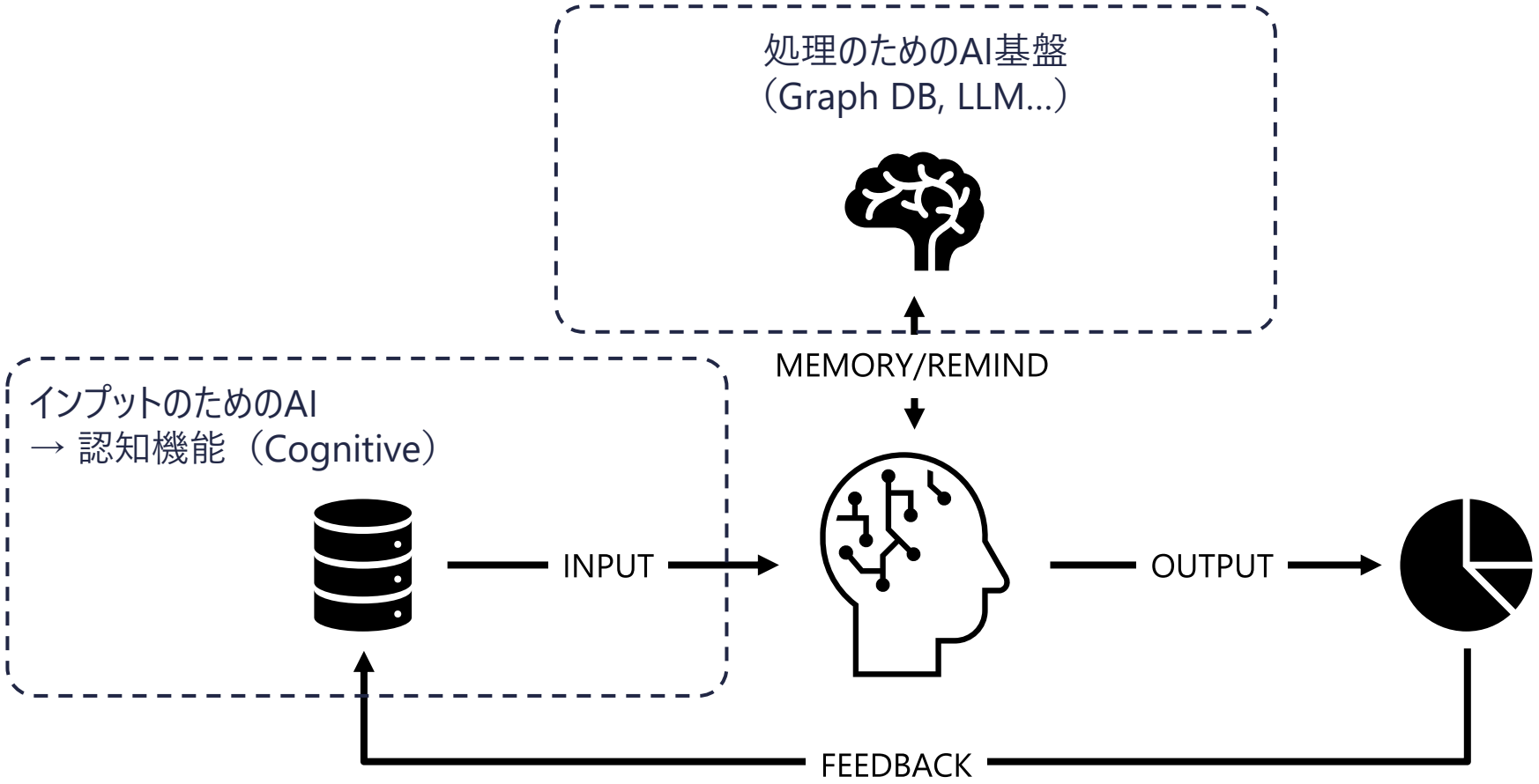


複数の環境で得られた結果を元に詳細な分析をし、その結果を反映してさらに改善をします

AIが新たなデータを作り出す環境 – メタバース



そもそもAIってなんだ？

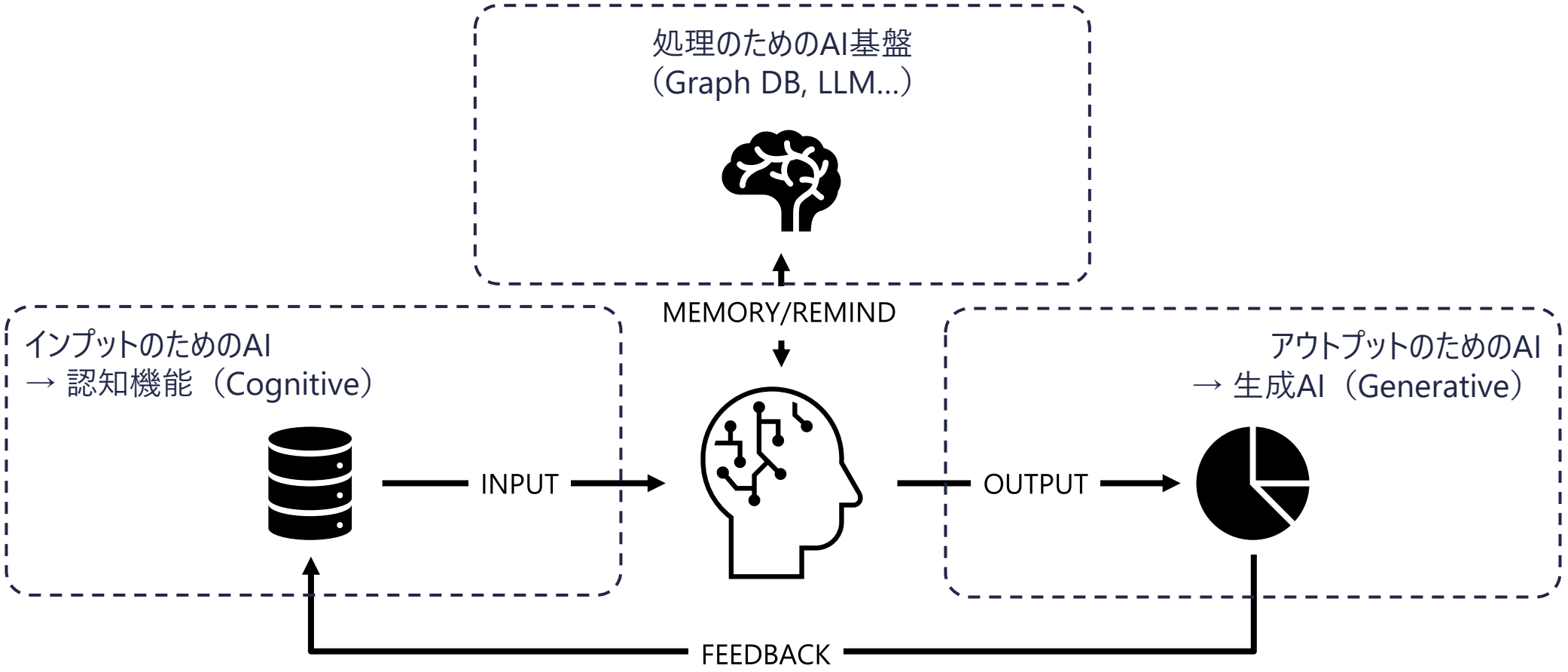


AIとは人間の思考を機械的に実現する技術

Generative AI

アウトプットのためのAIの進化による業務の変化

そもそもAIってなんだ？



AIとは人間の思考を機械的に実現する技術

生成系AIの能力を理解する

情報抽出系

要約

小学生にも分かるように
300文字程度で要約して

感情分析

喜び/怒り/悲しみの感情を
0~5で表現して

エンティティ分析

場所/人物名/組織名を
抽出して

文脈理解系

キーフレーズ抽出

次の文章の重要なフレーズ
を抽出して

インサイト抽出

次のレビューから商品の
改善点を考えて

チェック系

校正

誤字/脱字/タイプミスを
見つけて

添削/評価

〇〇の基準で10点満点で
評価して

翻訳系

翻訳

次の文章をフォーマルな
日本語に翻訳して

分類系

テキスト分類

次のニュース記事の
カテゴリを教えて

文章生成系

思考の壁打ち

〇〇という考えで抜けている
点を指摘して

記述アシスタント

このメールの日程調整をする
メールを書いて

問題作成

次の文章から4択問題を
作成して

アイデア創出

人気の出るブログの
内容案を提案して

コード作成

OpenAIのAPIを実行する
コードを書いて

情報検索

WEBアプリの要件定義に
ついて教えて

従来からできるタスク

新しくできるタスク

従来からのタスクは精度が向上し、
新たに文脈理解・文章生成系タスクができるようになった

生成系AIの活用事例

コンテンツ生成

コード生成

要約

セマンティック検索

複数のモデルでの業界のユースケースの例

電気通信

メディアワークフロー、クロスコンテンツリンク、メディアのコンテンツ作成、音声分析、B2Cコンタクトセンターの分析、コグニティブコンタクトセンター、スキル自動化、リアルタイム音声文字起こしと要約

製造業と工業

ChatGPT対応テクニカルサポート、顧客センチメント分析、カスタマーサービスナレッジマイニング、デジタル提案アシスタント、カスタマージャーニー分析、コンシューマーインサイト高度な分析、レコードの概要作成、異常検出、Copilotを使用した仮想エージェント

自動車、モビリティ、輸送

マーケティングコンテンツ生成、コンテキストコンタクトセンター、顧客フィードバックループ、スマートインシデントマネージャー、顧客コミュニケーション、テキスト要約&分析

実現しているお客様

STRABAG　Coca-Cola　KPMG　Icertis　ODP　CARMAX　zammo.ai

新たなカーナビの世界 – メルセデスベンツ様

Mercedes-Benz

状況

メルセデスベンツは、MBUXインフォテインメントシステムを搭載した車両に「HeyMercedes」MBUX音声アシスタントを提供しています。同社は、この機能を改善し、AIを組み込んで、強化された差別化された顧客体験を提供する方法を模索していました。

ソリューション

メルセデス・ベンツは、Azure OpenAI サービスを介して会話型 AI を統合し、"Hey Mercedes" 機能をさらに直感的で会話的なものにしました。90万台超の車両を対象に3カ月間のベータプログラムを開始し、ベータプログラムの成果を踏まえてさらなる導入を検討する。

インパクト

Azure OpenAI サービスでは、音声アシスタントが高度な機能を提供します。これにより、ユーザーとアシスタントの間でより動的な会話が可能になり、フォローアップの質問中にコンテキストの理解が維持されます。また、タスク機能が拡張されているため、ドライバーはハンドルを握ることができます。

様々な業種の様々な業務で活用が進んでいます

業界	社内チャットボット（GPTモデルをそのまま利用）	社内チャットボット（社内情報の活用）	Smart Virtual Agents（製品への搭載）	自動ドキュメント処理	自動コンテンツ生成	コンタクトセンター	インシデント報告と予測	異常検出	コパイロットを使用した仮想エージェント	リアルタイムの音声文字起こしと要約	予知保全	不正検出	電子メールの自動化
自動車 モビリティ&輸送	●		General Motors FIAT	●	CARMAX	●	●	●					
製造業と工業	村田製作所 アサヒグループジャパン ライオン	Panasonic	ABB SIEMENS 東芝デジタルソリューションズ	●		●	●	STRABAG	●				
電気通信	AT&T KDDI ソフトバンク 楽天		NTT西日本 NTTデータ		●	vodafone	●			●			
金融サービス	三菱UFJ みずほ 三井住友 明治安田生命 損害保険ジャパン		Morgan Stanley	●		●		●				●	
流通/サービス	Coca-Cola Heineken ベネッセ	EY	弁護士ドットコム 食べログ			CallMiner				KPMG			
ヘルスケア	小野薬品		Epic							Epic	●	●	
政府/自治体	東京都 大阪府 その他地方自治体	日本政府	Smart Nation SINGAPORE	農林水産省									●

Responsible AI

心配な時にいつでも確認できる環境を構築する

情報セキュリティリスク

情報セキュリティにおける**リスク**とは

「資産をコントロールできない状態」

情報セキュリティ**対策**とは

「資産を常にコントロールできる状態にすること」

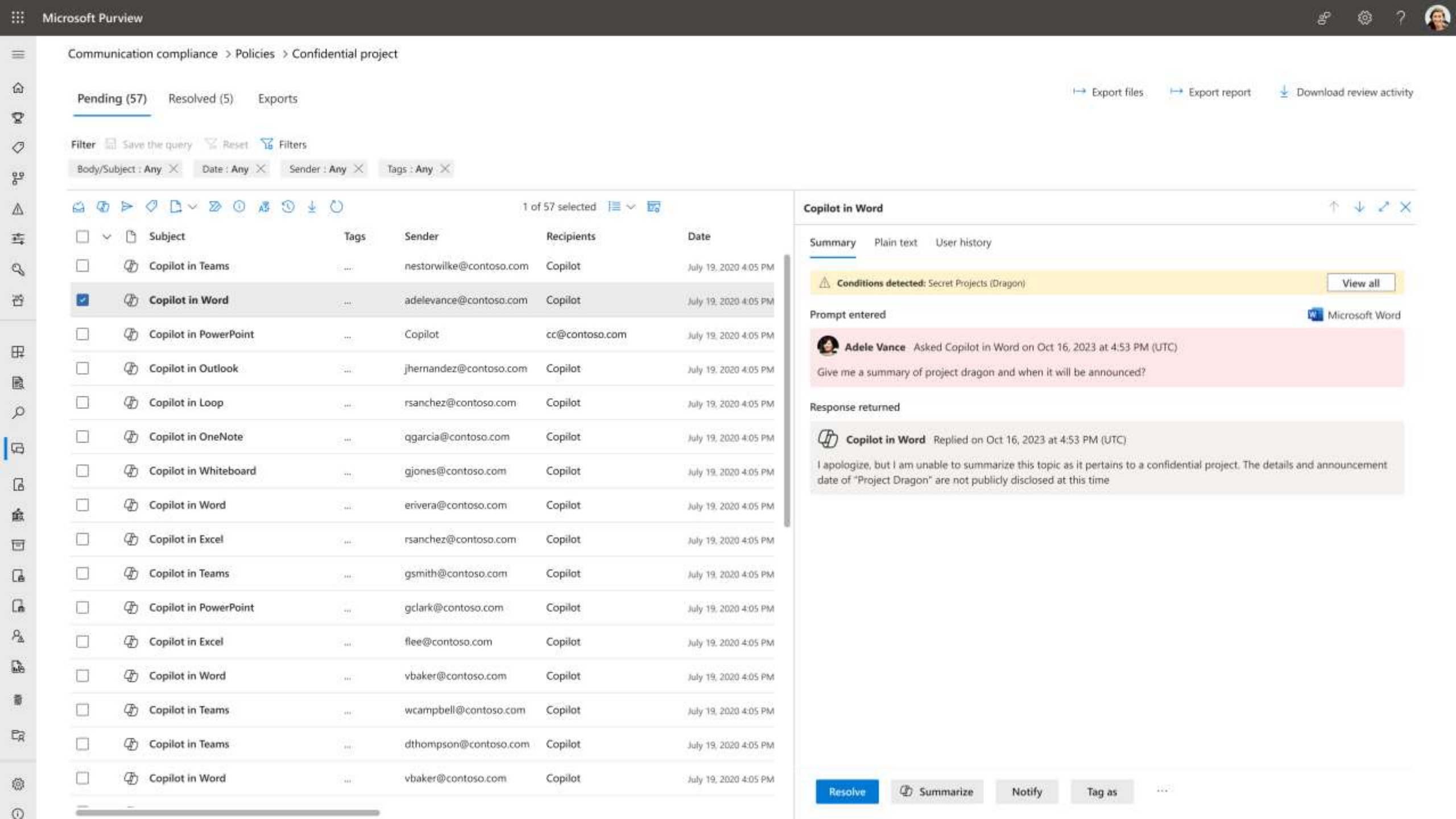
- 機密性：アクセス制御
- 完全性：整合性の確保
- 可用性：利用、判断

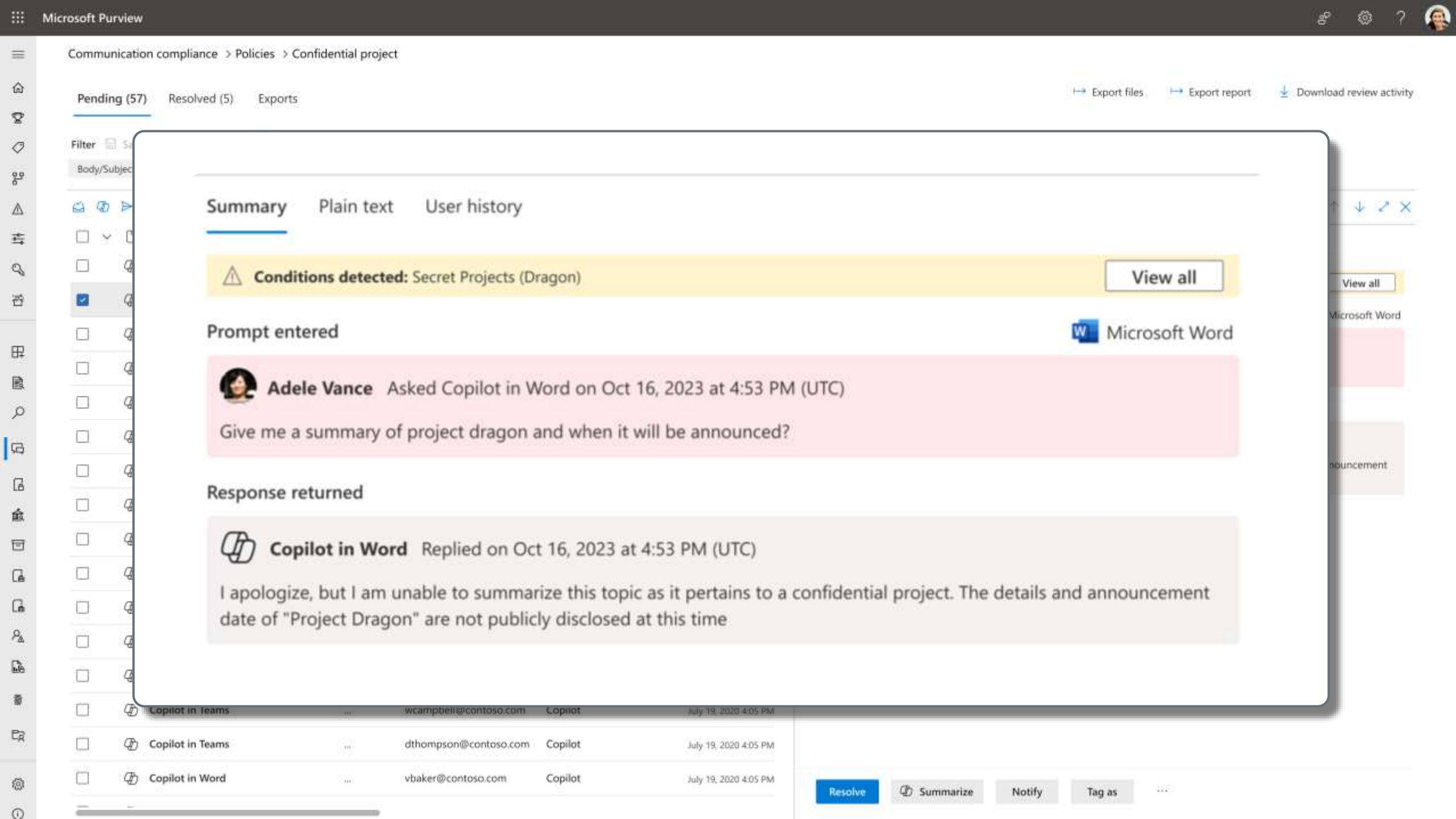
Survey on Corporate Engagement on Diversity

A brief questionnaire to assess the level of diversity and inclusion in your organization

Survey Questions

- How would you rate the overall level of diversity in your organization?
- Very low
- Low
- Moderate
- High
- Very high
- How would you rate the overall level of inclusion in your organization?
- Very low
- Low
- Moderate
- High
- Very high
- How often do you interact with people from different backgrounds, identities, perspectives, and


Microsoft Purview
Communication compliance > Policies > Confidential project
Pending (57)
Resolved (5)
Exports
Export files
Export report
Download review activity
Filter
Save the query
Reset
Filters
Body/Subject : Any
Date : Any
Sender : Any
Tags : Any
1 of 57 selected
Subject
Tags
Sender
Recipients
Date
Copilot in Teams ... nestorwilke@contoso.com Copilot July 19, 2020 4:05 PM
Copilot in Word ... adelevance@contoso.com Copilot July 19, 2020 4:05 PM
Copilot in PowerPoint ... Copilot cc@contoso.com July 19, 2020 4:05 PM
Copilot in Outlook ... jhernandez@contoso.com Copilot July 19, 2020 4:05 PM
Copilot in Loop ... rsanchez@contoso.com Copilot July 19, 2020 4:05 PM
Copilot in OneNote ... qgarcia@contoso.com Copilot July 19, 2020 4:05 PM
Copilot in Whiteboard ... gjones@contoso.com Copilot July 19, 2020 4:05 PM
Copilot in Word ... erivera@contoso.com Copilot July 19, 2020 4:05 PM
Copilot in Excel ... rsanchez@contoso.com Copilot July 19, 2020 4:05 PM
Copilot in Teams ... gsmith@contoso.com Copilot July 19, 2020 4:05 PM
Copilot in PowerPoint ... gclark@contoso.com Copilot July 19, 2020 4:05 PM
Copilot in Excel ... flee@contoso.com Copilot July 19, 2020 4:05 PM
Copilot in Word ... vbaker@contoso.com Copilot July 19, 2020 4:05 PM
Copilot in Teams ... wcampbell@contoso.com Copilot July 19, 2020 4:05 PM
Copilot in Teams ... dthompson@contoso.com Copilot July 19, 2020 4:05 PM
Copilot in Word ... vbaker@contoso.com Copilot July 19, 2020 4:05 PM
Copilot in Word
Summary
Plain text
User history
Conditions detected: Secret Projects (Dragon)
View all
Prompt entered
Microsoft Word
Adele Vance Asked Copilot in Word on Oct 16, 2023 at 4:53 PM (UTC)
Give me a summary of project dragon and when it will be announced?
Response returned
Copilot in Word Replied on Oct 16, 2023 at 4:53 PM (UTC)
I apologize, but I am unable to summarize this topic as it pertains to a confidential project. The details and announcement date of "Project Dragon" are not publicly disclosed at this time
Resolve
Summarize
Notify
Tag as


Microsoft Purview
Communication compliance > Policies > Confidential project
Pending (57)
Resolved (5)
Exports
Export files
Export report
Download review activity
Filter
Summary
Plain text
User history
Conditions detected: Secret Projects (Dragon)
View all
Prompt entered
Microsoft Word
Adele Vance Asked Copilot in Word on Oct 16, 2023 at 4:53 PM (UTC)
Give me a summary of project dragon and when it will be announced?
Response returned
Copilot in Word Replied on Oct 16, 2023 at 4:53 PM (UTC)
I apologize, but I am unable to summarize this topic as it pertains to a confidential project. The details and announcement date of "Project Dragon" are not publicly disclosed at this time
Copilot in Teams
Copilot in Teams
Copilot in Word
Resolve
Summarize
Notify
Tag as

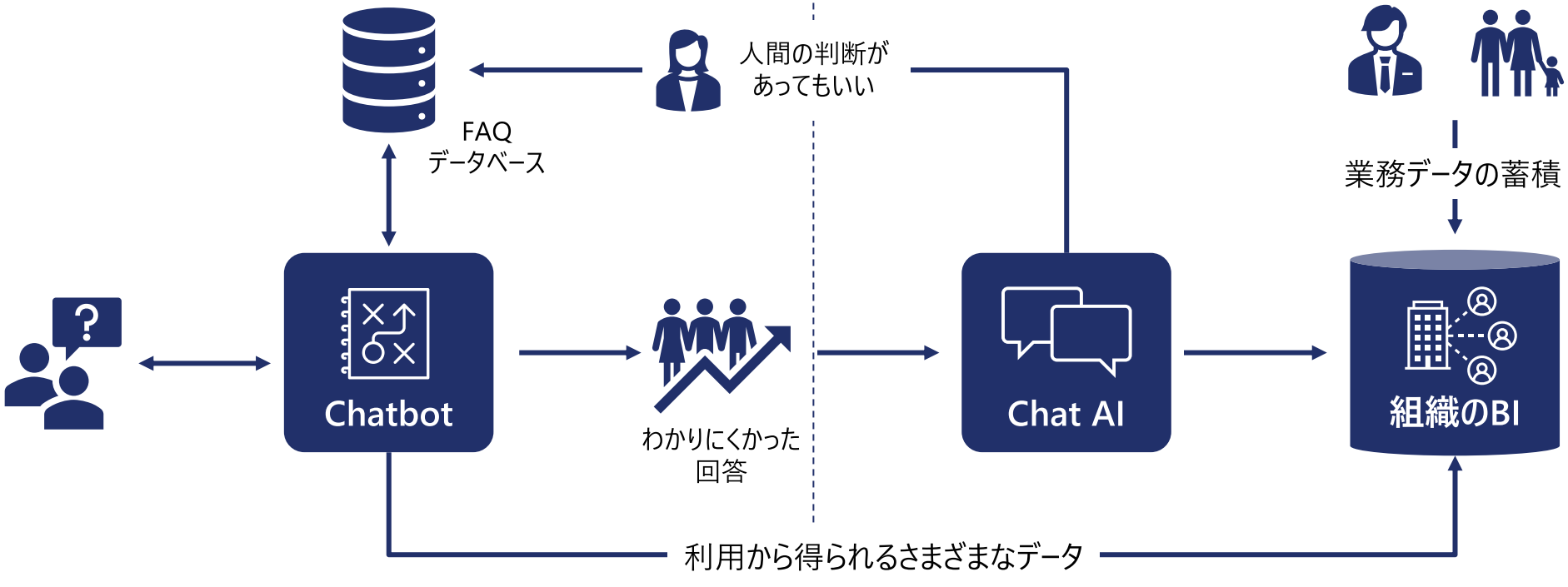
Get AI-Ready

AIを最大限に活用するためのIT基盤を構築する

Chat AIの活用 – コールセンターでは・・・

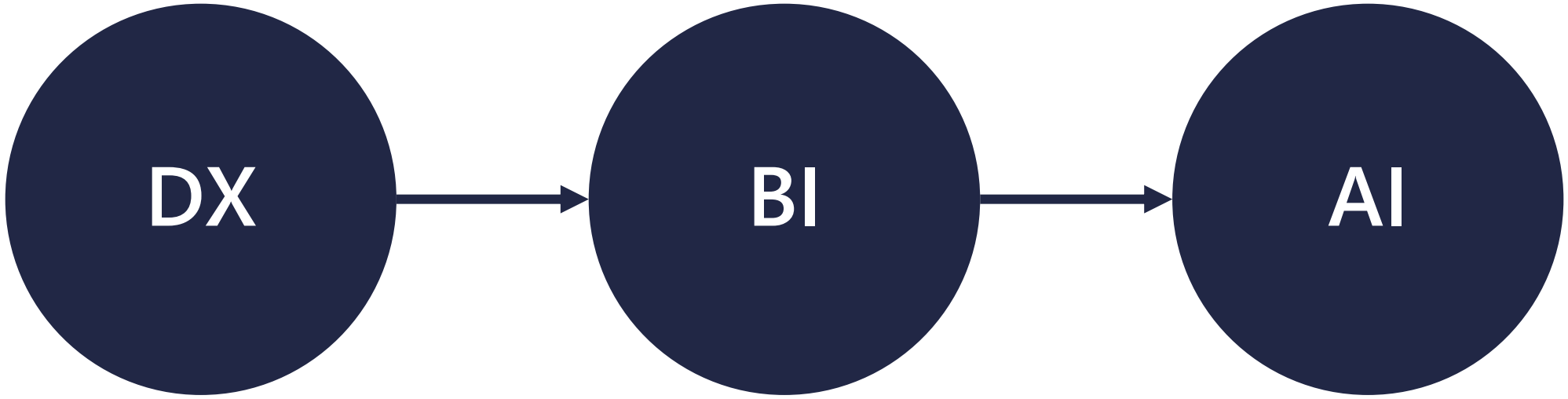
正確な回答を提供するためのChatbotの活用

蓄積された業務データから回答を作るChat AIの活用



正確な回答に導くためにはChatbotの利用が向いており、膨大なナレッジ（BI）からFAQデータベースを構築するためにはChat AIを活用することが望ましい。データソースとなるBIを充実させるためには、業務のDXが必須であり、やり取りの全てを蓄積できるようなシステムの構築が求められる

DXは全てを記録するための最初の一歩



すべての事象を記録する
ための業務設計と実装

記録をベースにした
組織のインテリジェンスの形成

組織のインテリジェンスを
最大限に活用する仕組み

AI活用のためのアプリケーション環境作り

全てのデータや活動を記録

AIアプリの活用の記録も管理

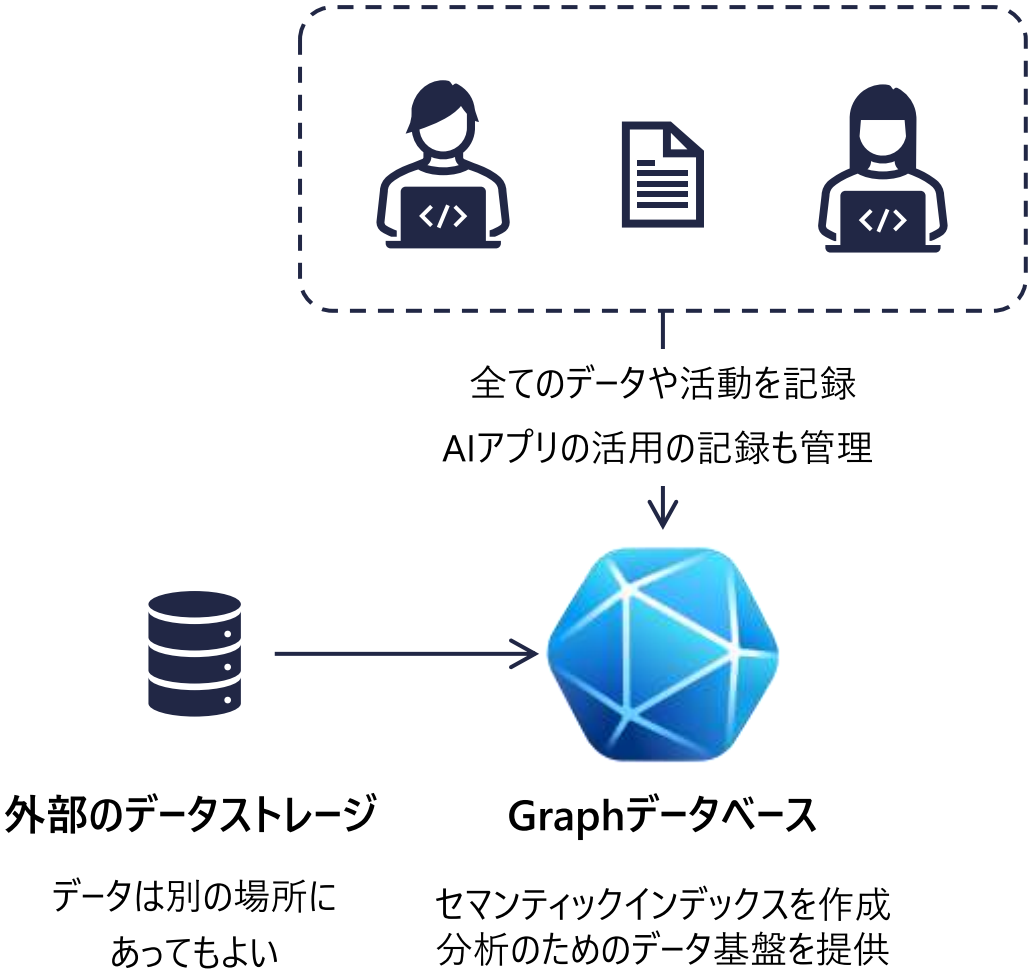
Graphデータベース

セマンティックインデックスを作成
分析のためのデータ基盤を提供

DXによりデジタル化された環境のデータは全てGraphデータベースで管理

- データがストックされるとすぐに関係性を構築
- データの関係性をもとにデータの意味（セマンティック）を生成
- いつでも活用できるようにセマンティックインデックスを構築

AI活用のためのアプリケーション環境作り



DXによりデジタル化された環境のデータは全てGraphデータベースで管理

- データがストックされるとすぐに関係性を構築
- データの関係性をもとにデータの意味（セマンティック）を生成
- いつでも活用できるようにセマンティックインデックスを構築

- 外部にあるデータのインデックスだけを持つような仕組みでも構わない

AI活用のためのアプリケーション環境作り

全てのデータや活動を記録

AIアプリの活用の記録も管理

AIアプリの活用

外部のデータストレージ

データは別の場所に
あってもよい

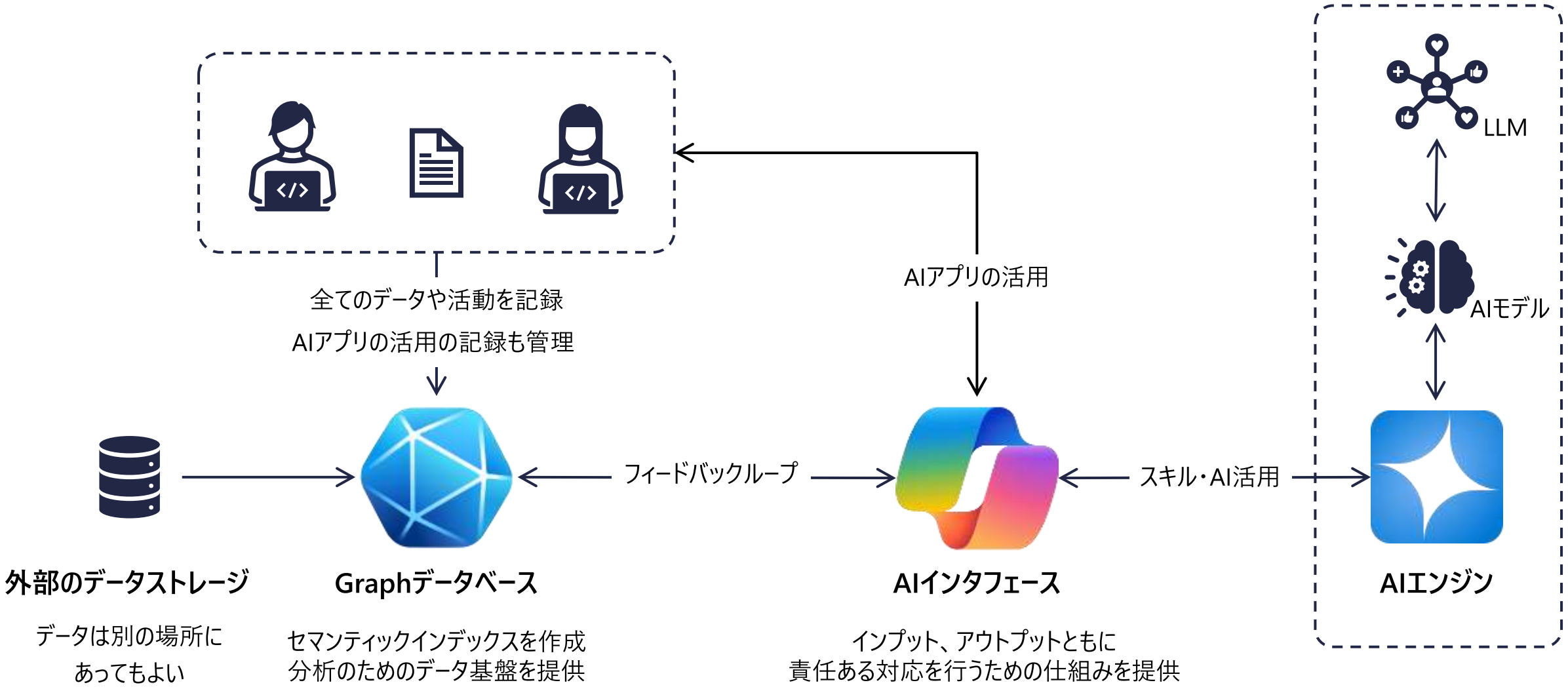
Graphデータベース

セマンティックインデックスを作成
分析のためのデータ基盤を提供

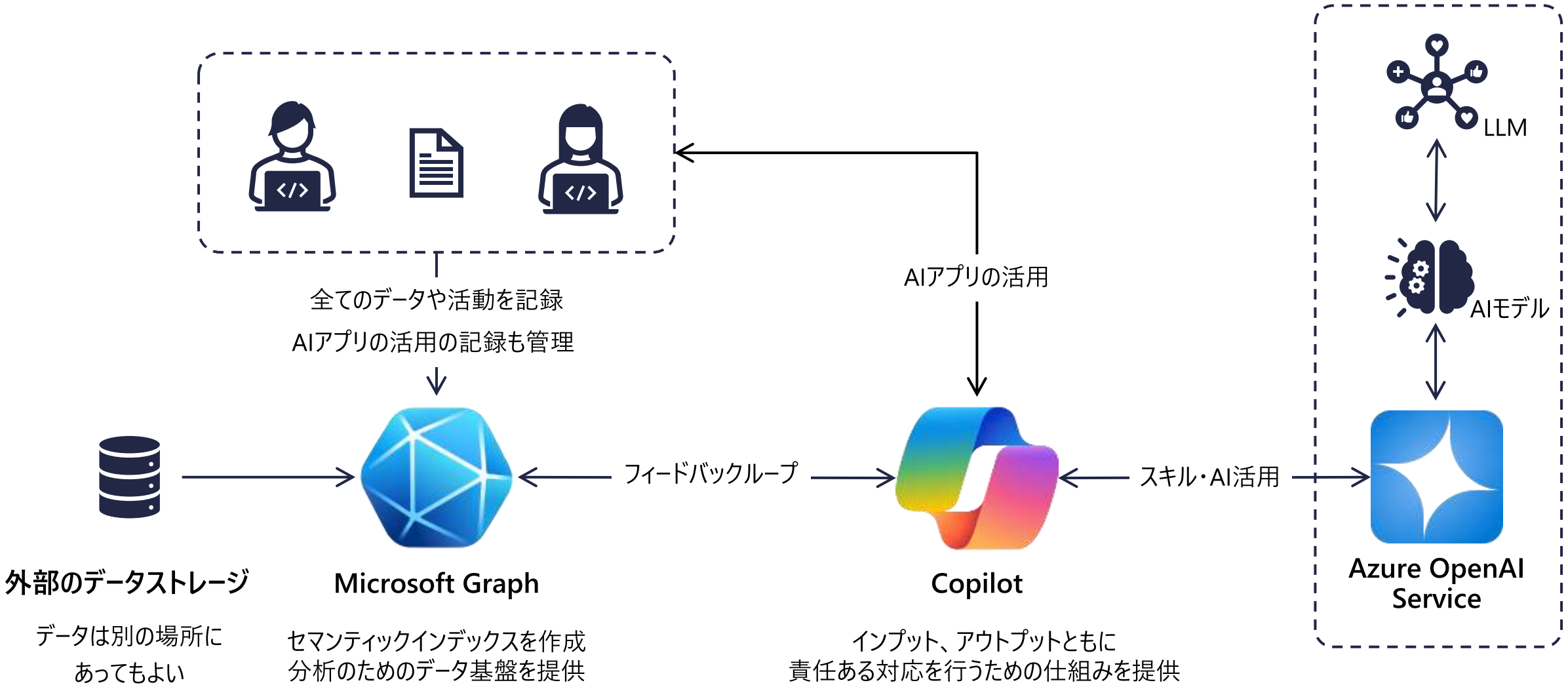
AIインタフェース

インプット、アウトプットともに
責任ある対応を行うための仕組みを提供

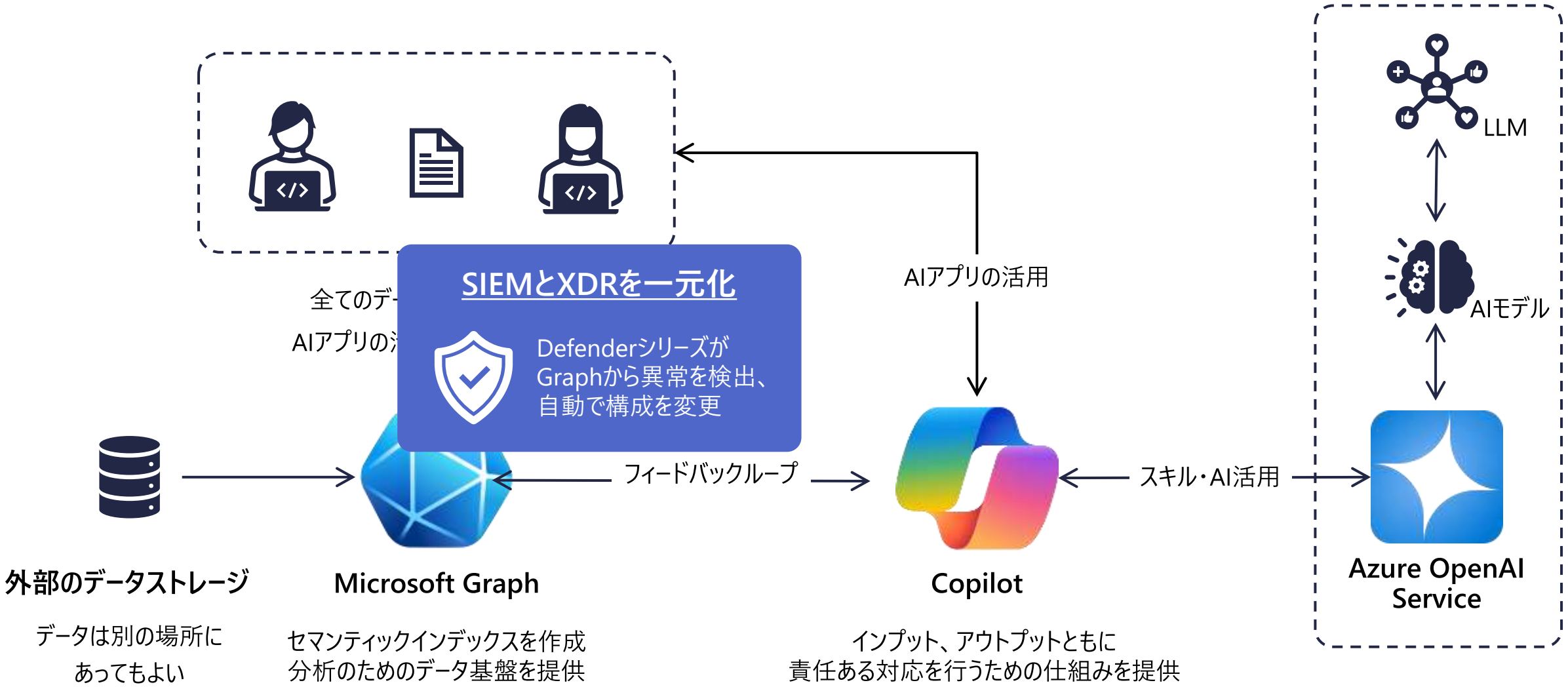
AI活用のためのアプリケーション環境作り



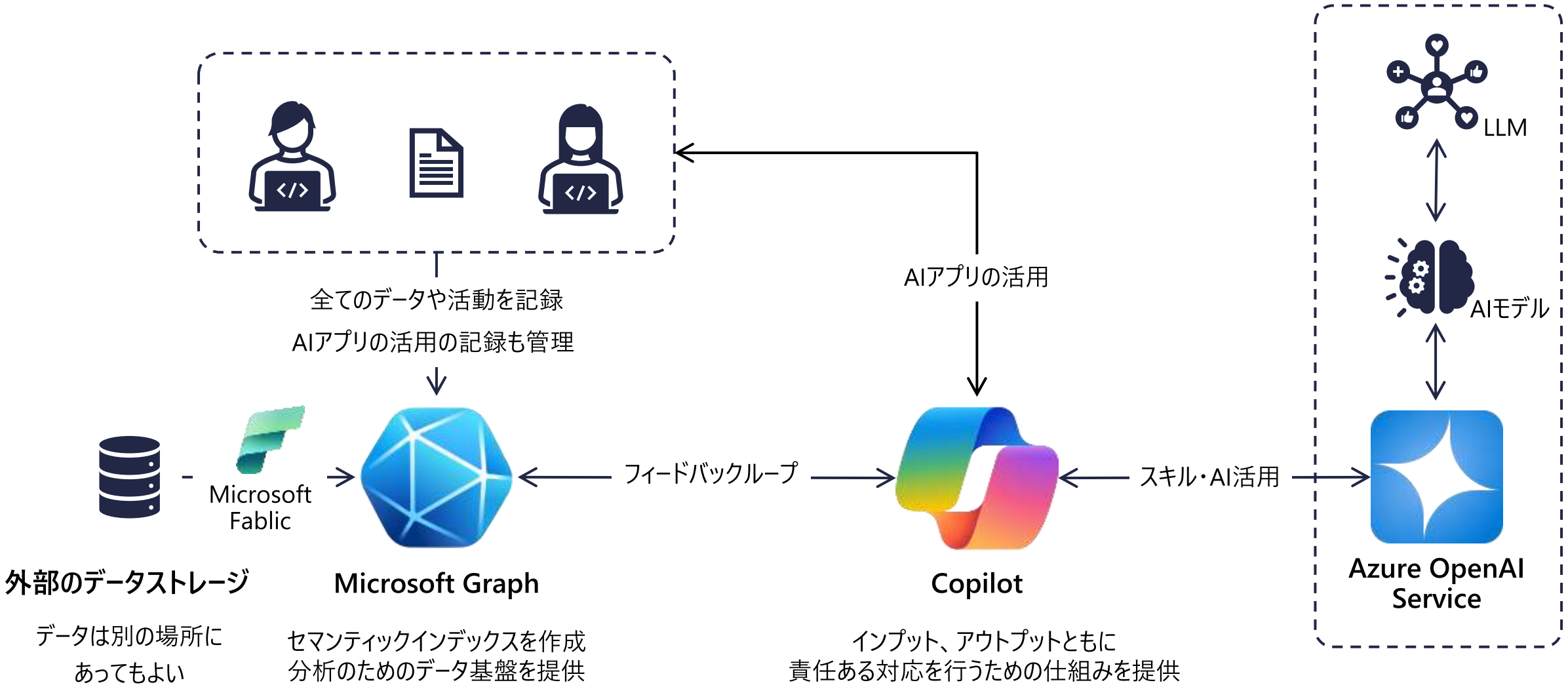
Microsoftのソリューションでは・・・



Microsoftのソリューションでは・・・



Microsoftのソリューションでは・・・



Microsoftのソリューションでは・・・

外部のデータストレージ

データは別の場所に
あってもよい

セマンティックインデックスを作成
分析のためのデータ基盤を提供

インプット、アウトプットともに
責任ある対応を行うための仕組みを提供

Are you AI-Ready?

AIを活用するためのアイデアはたくさん浮かびましたか
自由に使うための安全な環境を構築しましょう

Microsoft Secure

包括的なプラットフォーム、独自のインテリジェンス、幅広いパートナーシップを通じて、デジタルトランスフォーメーションによるセキュリティを確保します

Microsoft