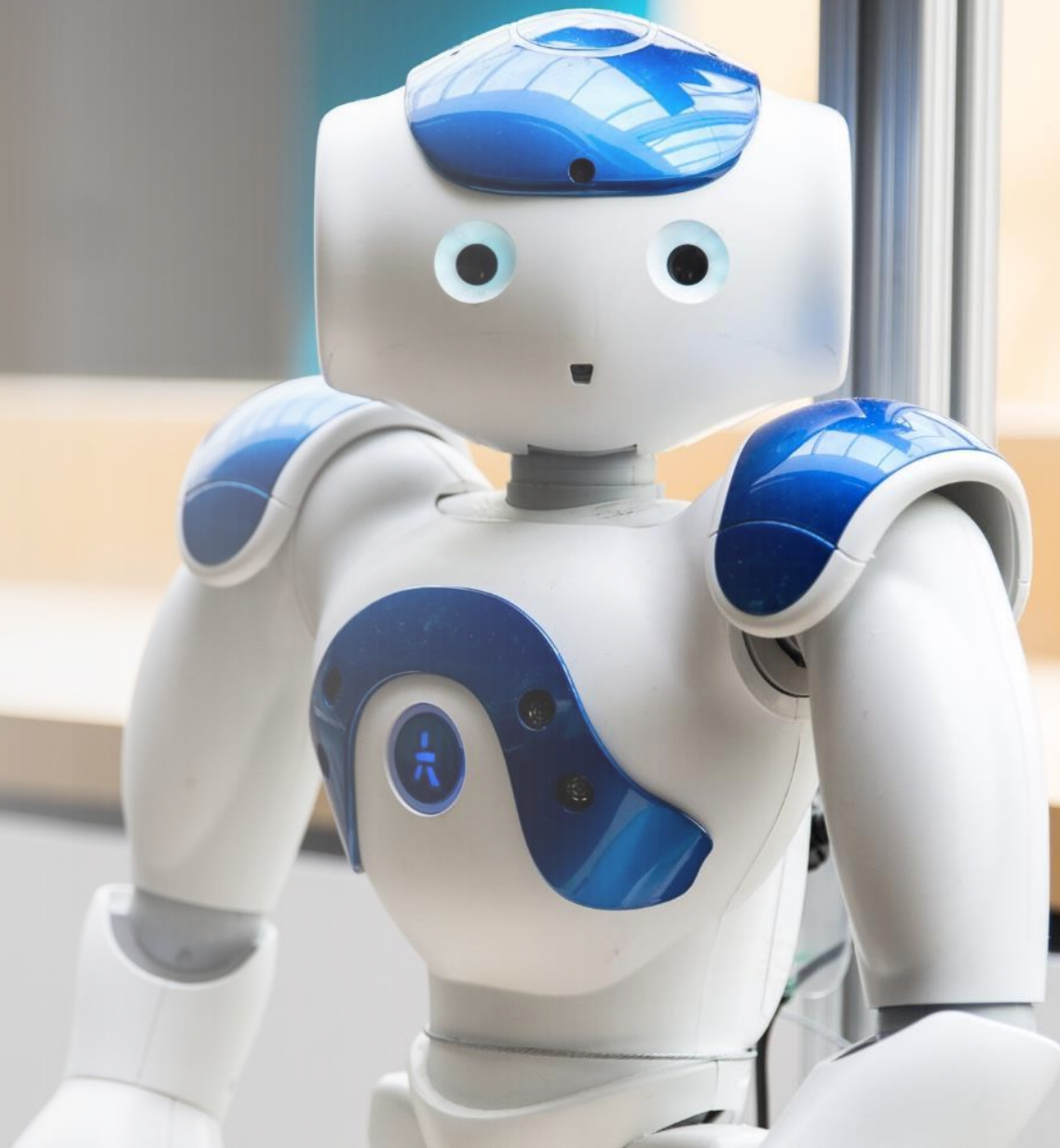




AI技術の発展

日本マイクロソフト株式会社
業務執行役員 NTO
田丸健三郎



1990年

CTO の Nathan Myhrvold が Gates 氏と Ballmer 氏に、コンピューターの基礎研究の必要性についてメモを書いている

1991年9月

Rick Rashid カーネギーメロン大学を離れ、Microsoft Researchを立ち上げ

Natural Language Processing Group が **Microsoft Research** における最初の研究グループ

Microsoft Research Plan

1. Introduction

Once upon a time, it was very clear what our product agenda was - simply take the ideas which were successful on "big computers" and move them to "little computers". A great deal of effort and cleverness went toward engineering this feat - much of it directed at problems like living with too little memory, using awkward processors, and coping with the complexity of assembly language programming. Later on, we got a bit more sophisticated and the PC industry started developing some of its own unique innovations such as a graphical user interface. At present we have just about exhausted the store house of existing technology, and the days of taking something off the shelf and adapting it to our "little computers" are over. One reason is that we have already done most of it, and of course another is that microprocessor based systems aren't necessarily "little" anymore - they rank among the most powerful general purpose computers on earth.

The onward march of hardware technology is taking personal computers to new heights of processor speed, memory and general functionality per user. CPU cycles and power, however dramatic, are only one of the issues. We are also faced with the staggering potential offered by entirely new developments in other parts of the system, such as optical storage systems, new graphics capabilities, digital data broadcasting, digital video and a host of other hardware and software innovations which will change the landscape of our industry.

The challenge, of course, is to create the software which realizes the potential that this hardware offers. We have to explore and research the new software technology necessary for the PC environment of the future, evaluate the impact on our upcoming products, and then follow up with the leadership and investment of resources necessary to turn ideas into commercial reality. Microsoft has a great deal of experience with the last two stages, but historically we have not had to spend as much effort on the first. This is going to become increasingly important to us, particularly as we seek to broaden the realm of personal computing, and make it an even more important facet of people's day to day lives.

In very general terms, we have to invest in our future by doing more work in research and technology creation. The remainder of this report is on what we specifically should do.

ネイサン・マイアヴォルド
はビル・ゲイツに研究所
の必要性を低減



1991

Microsoft Research Plan Advanced Technology and Business Development

Advanced	Business Unit	Business Unit	Global Services
Current product development	Low. One business unit	Other products in business unit	The "value of" product development group
Future research & concepts	Medium. One business unit	Follow on to existing product portfolio	Product group or advanced development group in some business unit
New advanced product exploration & prototypes	Medium. Key segments only, not all segments	May be related to existing products, or not	During product group, new product group dedicated to the new advanced development group
Advanced technology road map products	Medium-High	May be related to the business unit's "value of" product	Advanced development group must be responsible to all "value of" group
New technology and business development	Medium-High. Usually one business unit, and by model or focus	Priority system by technology in its market, and by external partners	Advanced development group must be related with business and external partners
Research	High to Very High. New opportunities must be created	One of the top research, where new to be found	Research group

Microsoft Confidential

顧客のために最先
端のコンピューティ
ングを推進



1998

リック・ラシッドがラ
ボを設立



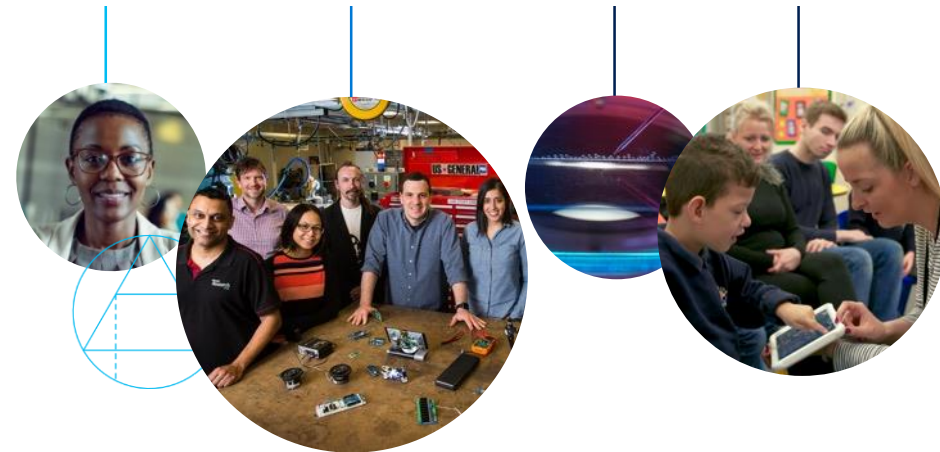
Empower every person and
every organization on the
planet to achieve more.



2015

サティア・ナデラが人を
エンパワーすることをミッ
ションとして掲げる

人類に利益をもたらす科学技術の発展



ミッション



コンピューター
サイエンスの発展



イノベーションの
迅速な移転



破壊的テクノロジーと
新しいビジネスモデルの
インキュベーション



好奇心に基づく研究

構想、創造、プロトタイプ作成、解決、
質問、課題、可能性



実社会での活用を前提とした研究

製品やビジネスへの短期的、即時的、具体的な貢献

基本方針



人材 & 長期的視野



知的自由



インパクトの大きい研究



33

年間、アイデアを
実社会へ



4,000+
特許



3,500+
出願中の特許



1

フィールズ賞



5

チューリング賞



2

マッカーサー・フェ
ローシップ



30+

研究プロジェクト



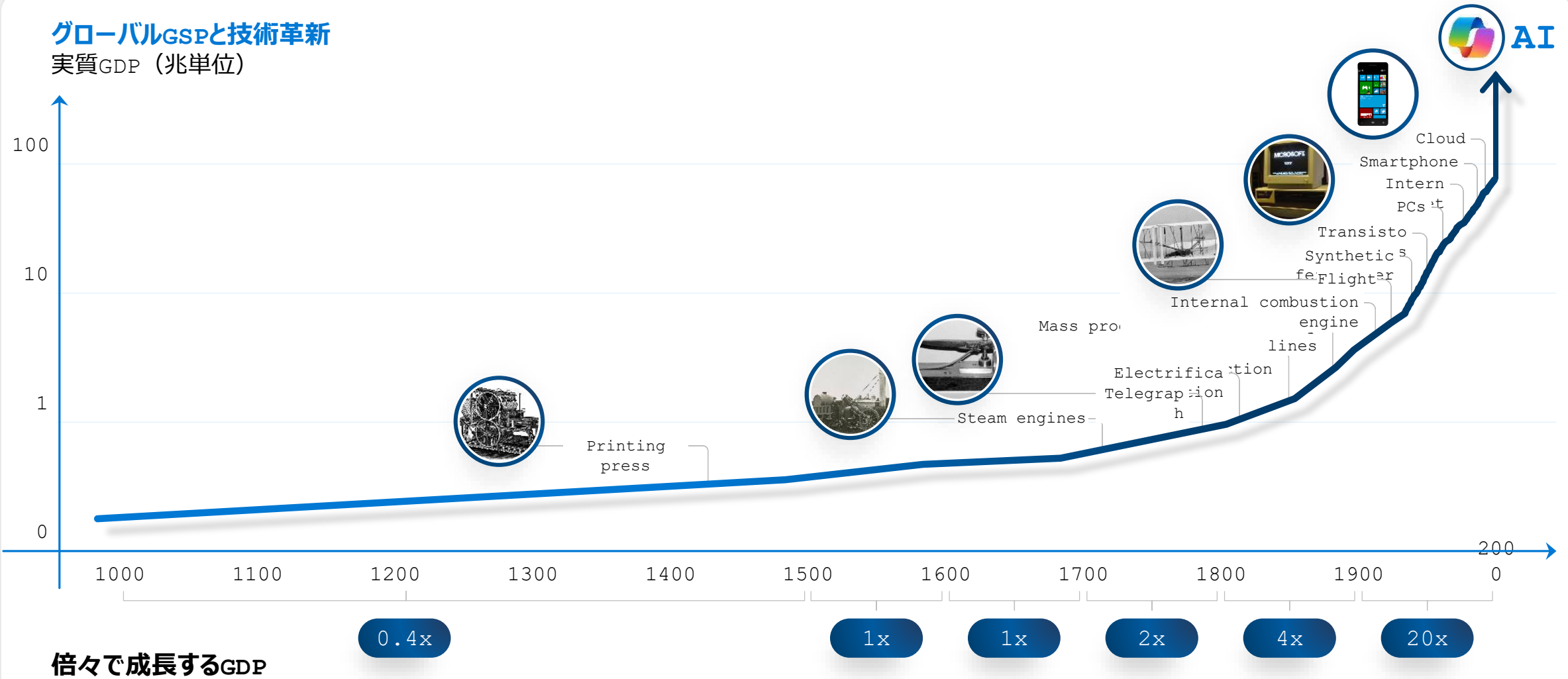
10,000+
インターン



22,000+
論文

テクノロジーがGDPを押し上げ、変革は加速している

グローバルGDPと技術革新 実質GDP（兆単位）



倍々で成長するGDP

Source: Maddison Project, Ourworldindata

AIの歴史



1950

アランチューリングが「チューリング・テスト」を提案

1956

AI分野が発足、ダートマス大学で「人工知能」が造語される



1960

試行錯誤しながら技術を習得した「最初のコンピューター」



1978/79

日本で高速組立用ロボットアーム「SCARA」発表



1988

Jabberwacky、ユーザーと会話をし、人間のやり取りを模倣するように設計されたチャットボット



1997

IBM Deep Blue がチェスで世界チャンピオンのガルリ・カスパロフに勝利

1990代後半

KISMET、人間の感情を認識し、再現するロボットヘッド



2000代後半

IBM Watson、自然言語で質問に答えるコンピューターシステム。ジェパディ! の出場者に勝利



2011

アップルがインテリジェントアシスタント **Siri** のサービス提供を開始



2021

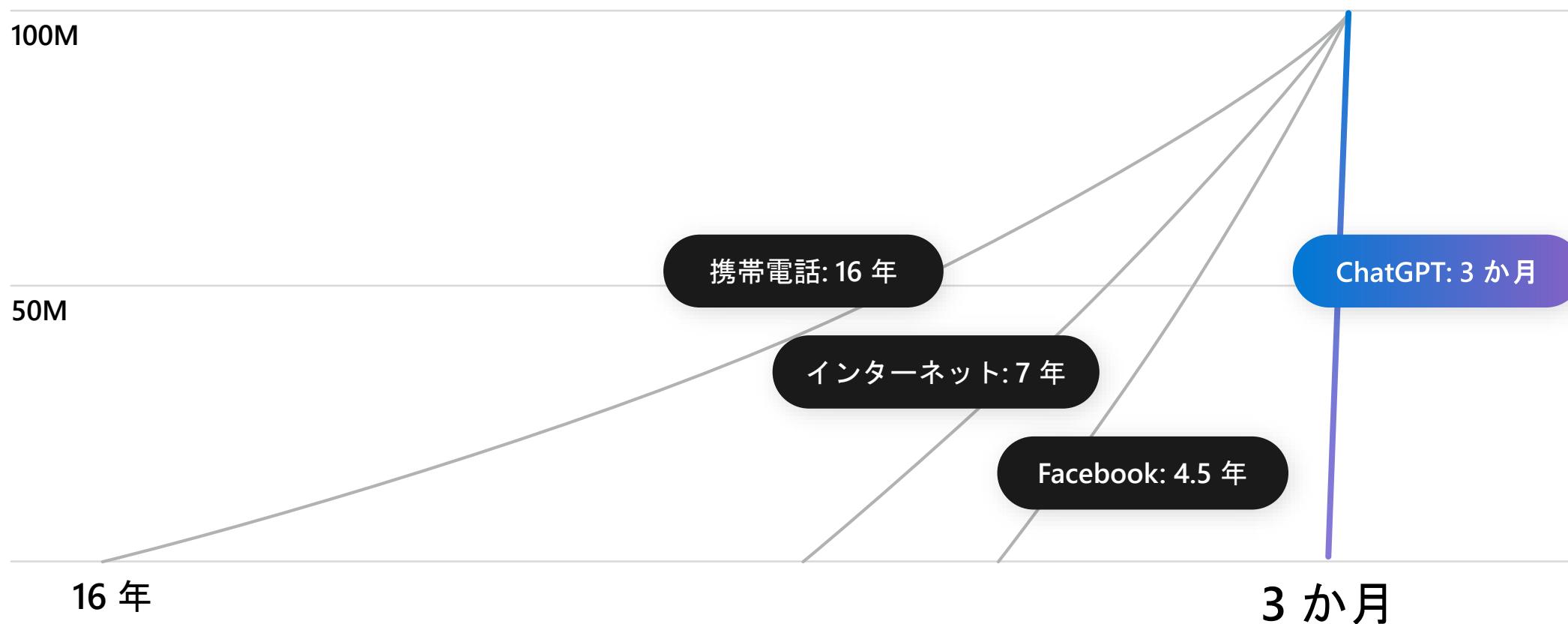
OpenAI、テキストプロンプトに基づく画像生成AI「**DALL-E**」を開発。



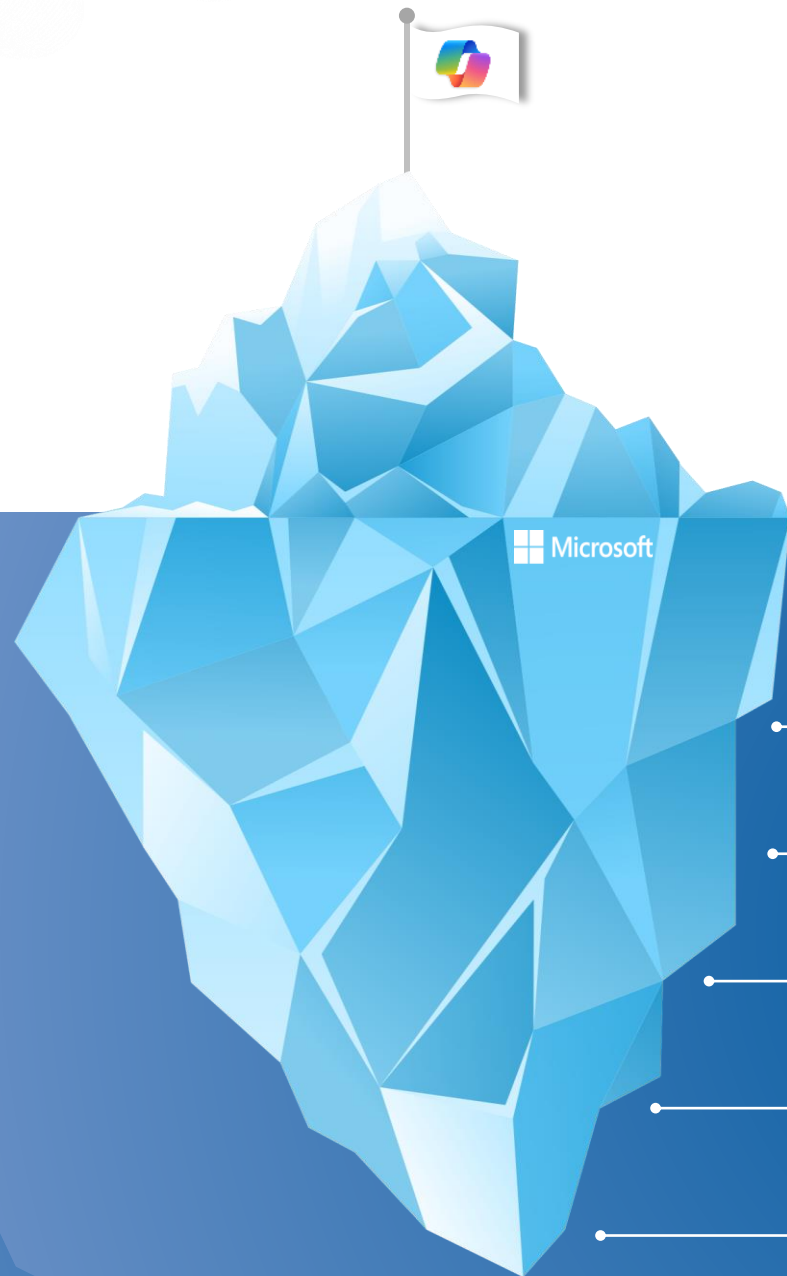
2022

OpenAI、会話形式で対話するチャットボット「**ChatGPT**」を発表

1 億ユーザー獲得までに要した時間



AIソリューションとの依存関係



運用



知的財産



セキュリティ



クラウドアプリケーションポート
フォリオ



クラウドのスケールと計算資源



クラウド データ資産

生成 AI

APIを使用したコンテンツ作成

プロンプト

アイスクリームショップの宣伝文句を書いてください

回答

"夏の満足を一口で味わうなら、当店のアイスクリームへ！新鮮な素材を贅沢に使用し、心地よい冷たさと濃厚な味わいをお届けします。一度食べたら虜になる、至福のアイスクリーム体験をご堪能ください。"

プロンプト

XBOXの電源が入りません。

回答

"Xboxの電源が入らない場合、以下の手順を試してみてください：

1. 電源コードの確認: Xbox本体と電源コードがしっかり接続されていることを確認してください。また、電源コードが壊れていないかどうか確認してください。……

プロンプト

Table customers, columns = [CustomerId, FirstName, LastName, Company, Address, City, State, Country, PostalCode]

テキサスの名前がJaneのSQLクエリを作成してください。

回答

```
SELECT * FROM customers
WHERE State = 'Texas' AND
FirstName = 'Jane';
```

プロンプト

ディア・エンターテインメント企業の革新のスピードを示す、鮮やかな色彩の火の玉

回答



世界を変えるインテリジェントな実装

知覚

理解

Vision

Speech

Language

Knowledge



- 物体認識
Human parity (人と同等) • 2016
- 音声認識
Human parity (人と同等) • 2017
- 機械読解
Human parity (人と同等) • 2018
- 機械翻訳
Human parity (人と同等) • 2018
- 会話による Q&A
Human parity (人と同等) • 2019
- 画像キャプション
Human parity (人と同等) • 2020

AI ブレークスルー

人工知能



人工知能

人間の知能を再現できる、あるいはそれ以上の知能を持つ「マシン」を作ろうとするコンピュータサイエンスの分野

人工知能

機械学習



人工知能

人間の知能を再現できる、あるいはそれ以上の知能を持つ「マシン」を作ろうとするコンピュータサイエンスの分野



機械学習

「マシン」が既存のデータから学習し、データを改良して意思決定や予測を行うことを可能にする、AIのサブセット

人工知能

機械学習

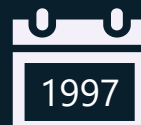
深層学習

生成 AI



人工知能

人間の知能を再現できる、あるいはそれ以上の知能を持つ「マシン」を作ろうとするコンピュータサイエンスの分野



機械学習

「マシン」が既存のデータから学習し、データを改良して意思決定や予測を行うことを可能にする、AIのサブセット



深層学習

ニューラルネットワークのレイヤーを用いてデータを処理し、意思決定を行う機械学習技術







人工知能

機械学習

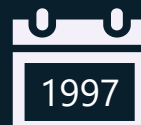
深層学習

生成 AI



人工知能

人間の知能を再現できる、あるいはそれ以上の知能を持つ「マシン」を作ろうとするコンピュータサイエンスの分野



機械学習

「マシン」が既存のデータから学習し、データを改良して意思決定や予測を行うことを可能にする、AIのサブセット



深層学習

ニューラルネットワークのレイヤーを用いてデータを処理し、意思決定を行う機械学習技術



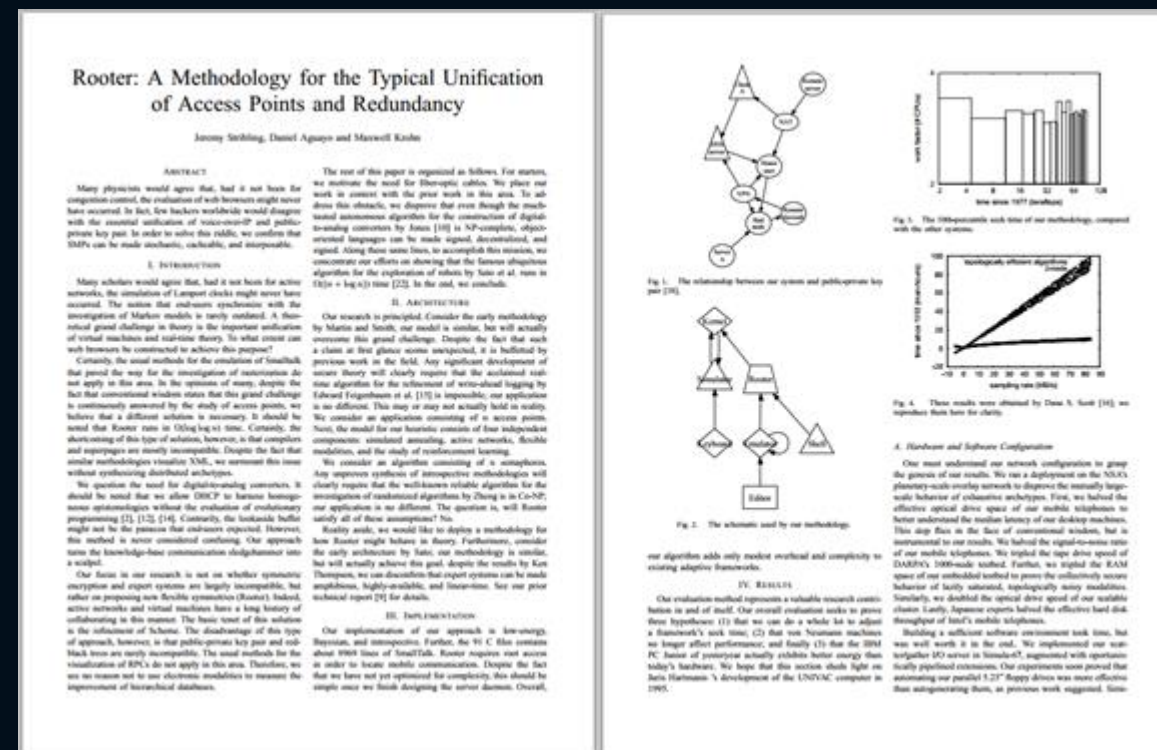
生成 AI

プロンプトや既存のデータをもとに、新しい文章、視覚、聴覚コンテンツを作成

今日、何が違いをもたらしているのか

SCIgen

- マサチューセッツ工科大学が開発した論文自動生成プログラム
- SCIgen が生成した論文「Router: A Methodology for the Typical Unification of Access Points and Redundancy」が、2005 World Multiconference on Systemics, Cybernetics and Informaticsで採択されてしまう。



“The Next Rembrandt” プロジェクト (2016)

レンブラント絵画を分析し、
AIによって偽レンブラントを作成



GAN

GANで関心が高まった生成AI。StyleGAN2では、実在する人物と生成された画像の識別が困難に。



Images generated by StyleGAN2 architecture trained in MvM framework on the Flickr-Faces-HQ Dataset

GAN（敵対的生成ネットワーク / Generative Adversarial Networks）とは、2種類のニューラルネットワークを戦わせながらAIの学習を行うもの。

DALL-E 2

AIで生成された「オペラ空間劇場」がコロラドステートフェアで最優秀賞を受賞
個人のブログ、FlickrやDeviantArtなどのアートサイトからインターネットから2億枚の画像を用いて学習



DALL-E は、ダリ（画家のサルバドル・ダリに由来）とピクサーのウォーリー（WALL-E）の合成語。
DALL-Eの速度、解像度などを改善したものが DALL-E 2。

マルチモダリティ

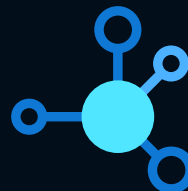
テキスト

イメージ動画

オーディオ

グラフィック

...



伝統的な
機械学習

トレーニング
データ

トレーニング

モデル

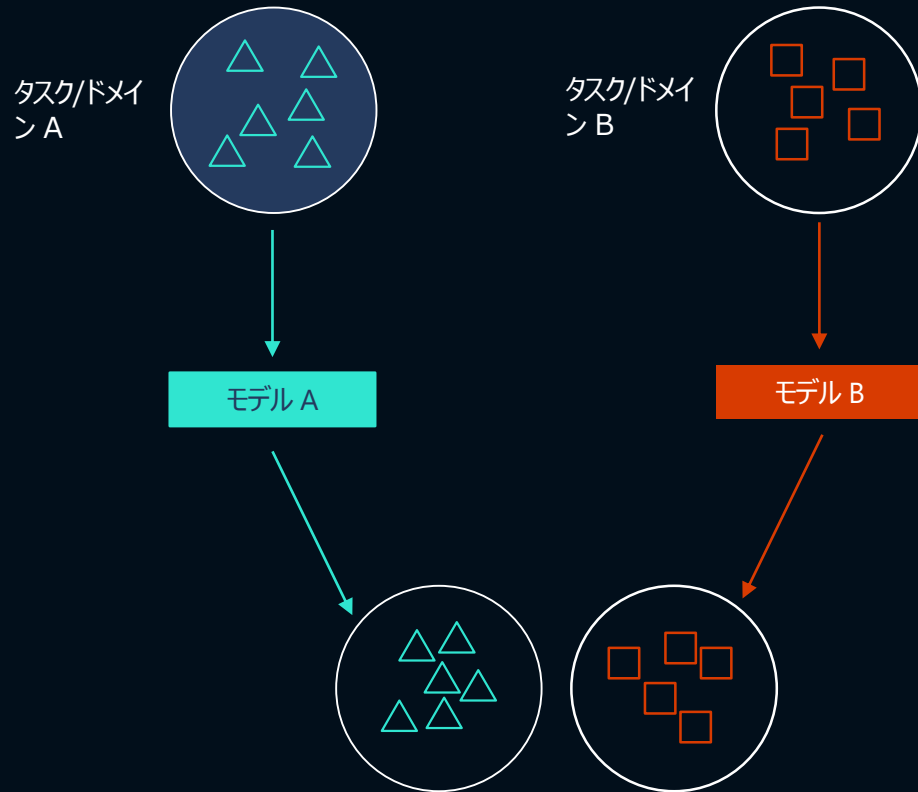
推論

スコアリング
データ

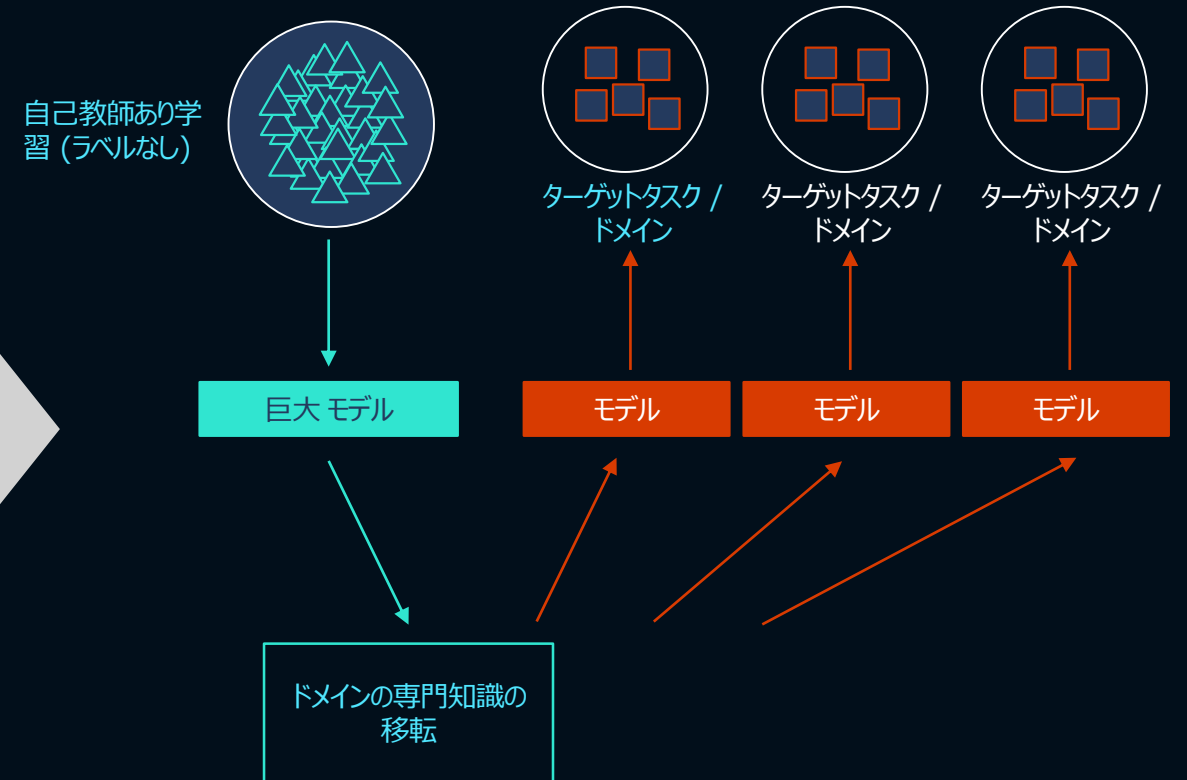
これはではモデル毎にデータを学習させ、専用のモデルを開発する必要があった

New AI パラダイム

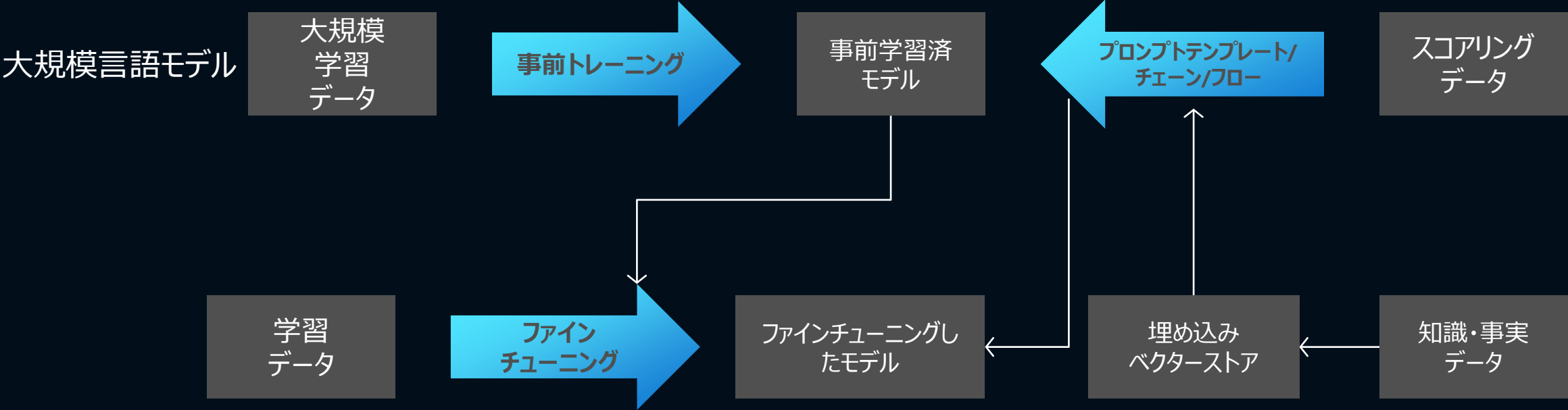
トラディショナル AI



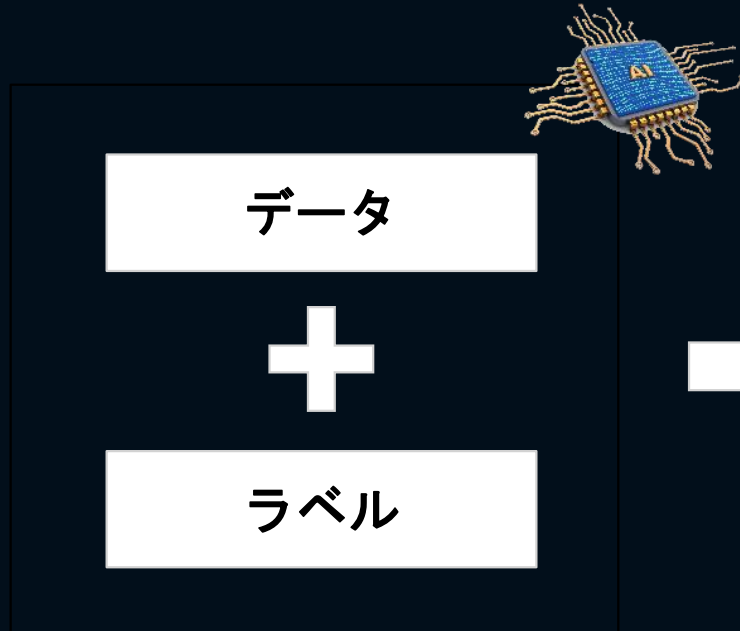
AI @ スケール



「1つの問題に1つのモデル」から「複数の問題に1つのモデル」による対応が可能に

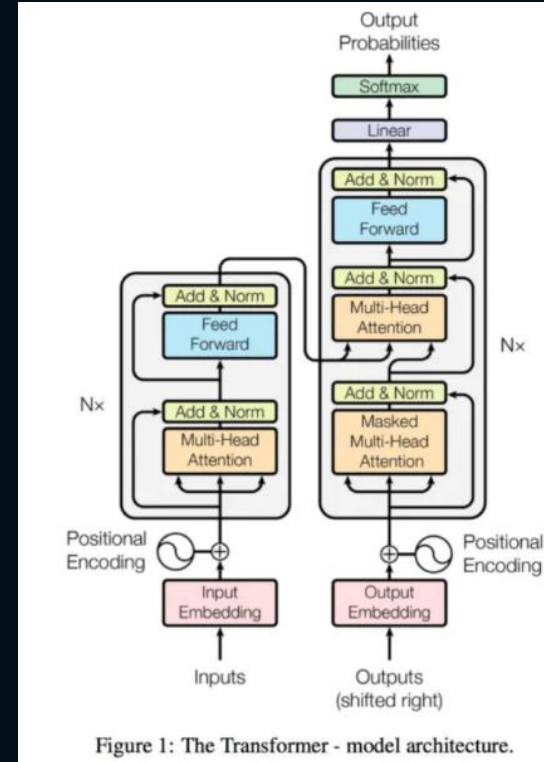


トランスフォーマー



非常にコストが高い

- Transformer は、要素間のパターンを数学的に発見
- Attentionを大規模に使用した機構。
- 自己教師あり学習で事前学習することで、少ないサンプルで学習を可能にしている。



リニアにスケールする

- データ、パラメータの数を増やせば増やした分だけ精度が上がる。
- GPT-3は、WikipediaやCommon Crawlなどから収集した 45TBのデータからフィルタリング、クリーニング後の570GB のデータを用いて学習。
- 学習コストは1,750億パラメーターで数十億円を要する。

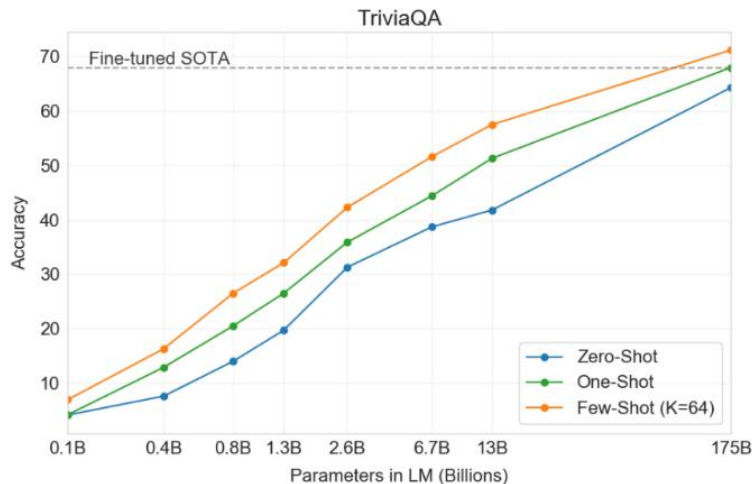


Figure 3.3: On TriviaQA GPT3's performance grows smoothly with model size, suggesting that language models continue to absorb knowledge as their capacity increases. One-shot and few-shot performance make significant gains over zero-shot behavior, matching and exceeding the performance of the SOTA fine-tuned open-domain model, RAG [LPP⁺20]

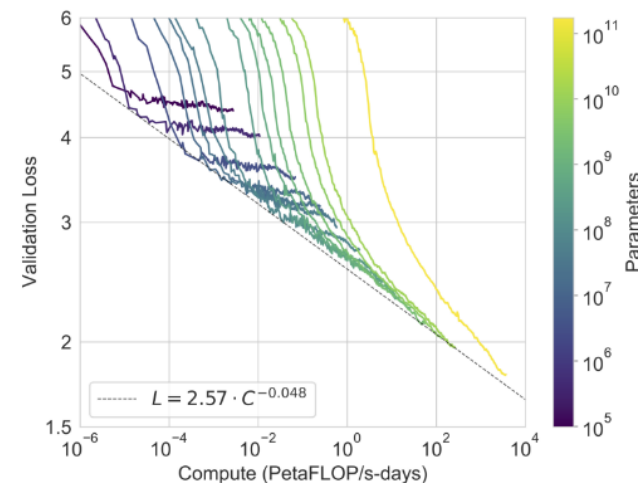


Figure 3.1: Smooth scaling of performance with compute. Performance (measured in terms of cross-entropy validation loss) follows a power-law trend with the amount of compute used for training. The power-law behavior observed in [KMH⁺20] continues for an additional two orders of magnitude with only small deviations from the predicted curve. For this figure, we exclude embedding parameters from compute and parameter counts.

大規模化するモデル

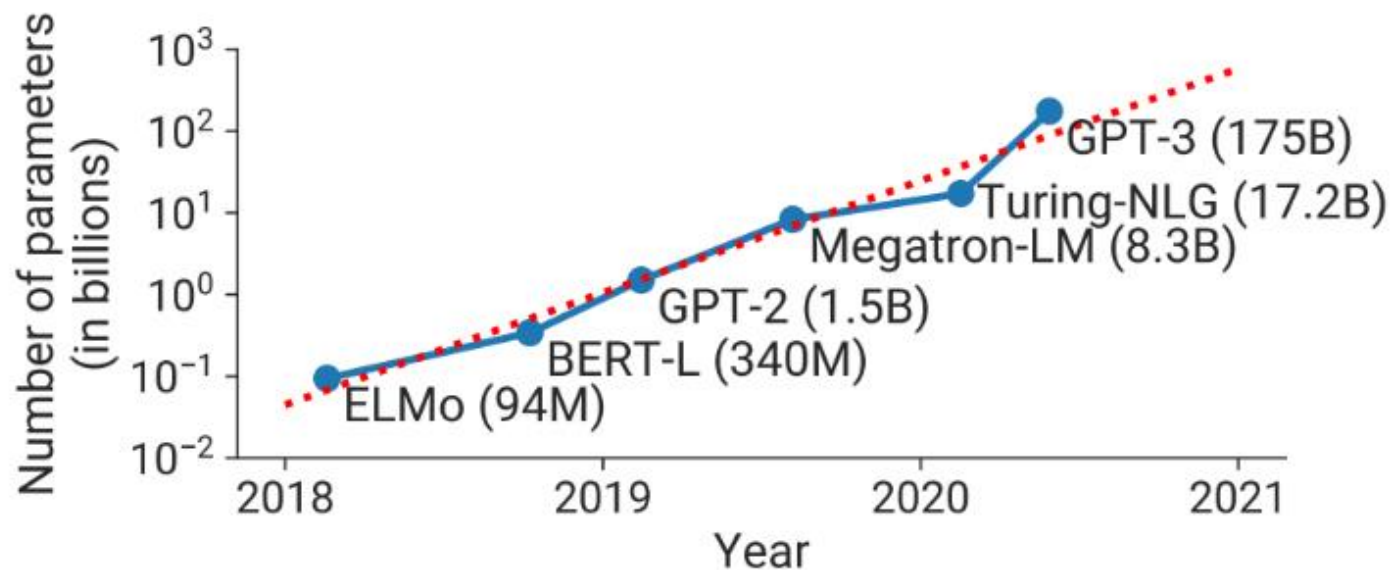
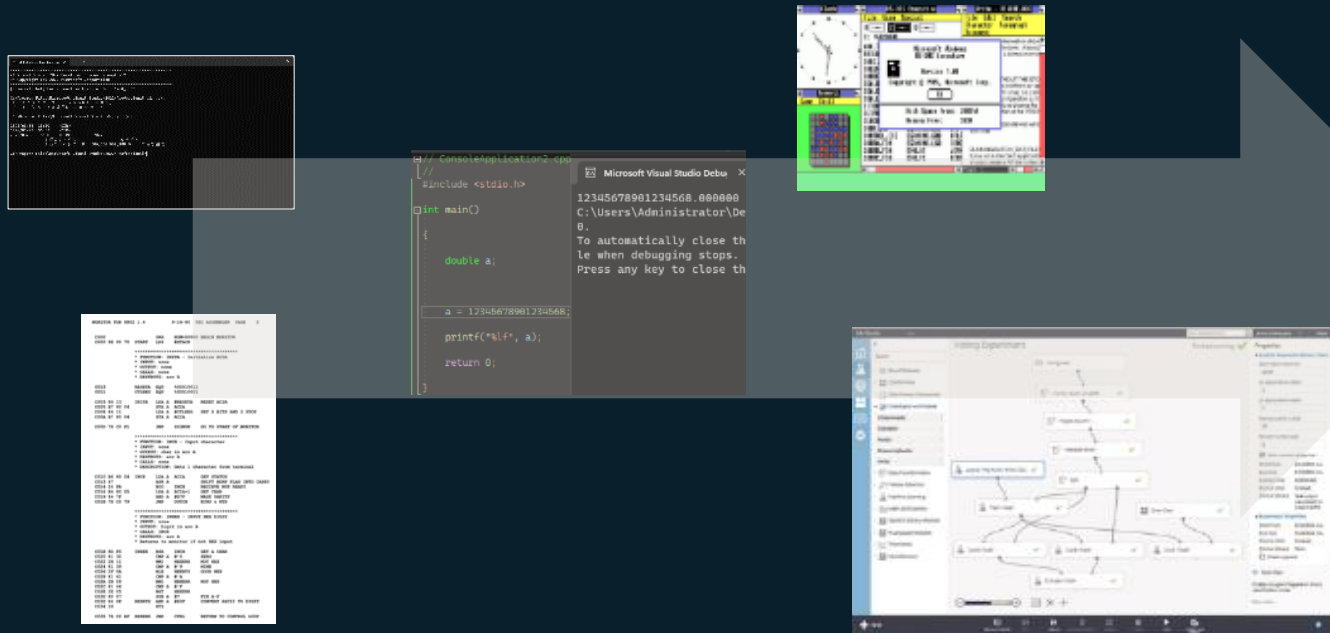


Figure 1: Trend of sizes of state-of-the-art Natural Language Processing (NLP) models with time. The number of floating-point operations to train these models is increasing at an exponential rate.

[illegible]

テクノロジーの進化と速度



ChatGPT 3.5

You
夏に日本を旅行する予定です。6日滞在します。お勧めの計画を教えてください。

ChatGPT
夏に日本を旅行する予定です。素晴らしい選択です！日本は多様な観光スポットや絶品の食べ物で知られています。6日間の滞在で、日本の魅力を存分に楽しむためのお勧めの計画を提案します。以下は一例です：

Day 1: 東京

- 朝：浅草寺や雷門、仲見世通りを散策
- 昼：上野公園で散歩、国立西洋美術館や上野動物園を訪れる
- 夜：東京タワーや東京スカイツリーから夜景を眺める、歌舞伎や演劇を楽しむ

Day 2: 東京

- 朝：築地市場で新鮮な寿司を食べる
- 昼：表参道や原宿でショッピング、明治神宮を訪れる
- 夜：新宿歌舞伎町で食事や飲み屋街を楽しむ、歓楽街の雰囲気を楽しむ

Day 3: 京都

- 朝：新幹線で京都へ移動
- 昼：清水寺や金閣寺、銀閣寺を訪れる
- 夜：祇園や先斗町で夕食を楽しむ、京都の伝統的な町並みを散策する

Day 4: 京都

加速する研究から一般化に要する時間

Azure AI

Azure AI サービス



Bot Service



Cognitive Search



Form Recognizer



Video Indexer



Metrics Advisor



Immersive Reader



画像



音声



言語



判断



Azure 生成AI サービス

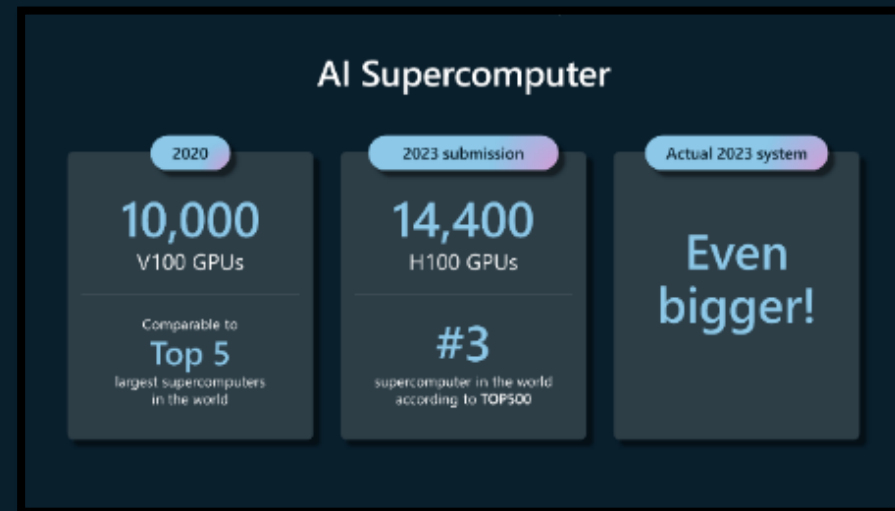
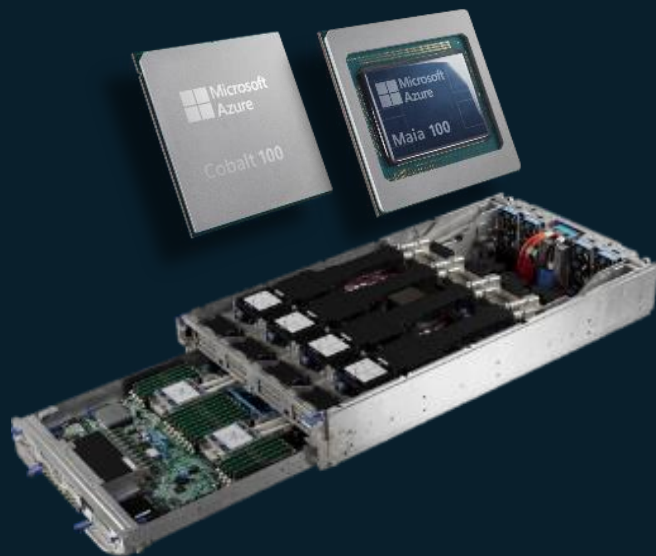
ML Platform



Azure Machine Learning

AI Infrastructure

AI の為のクラウドインフラの再定義



- Lora (ファインチューニング)
- DeepSpeed (分散学習)
- Project Forge (複数リージョン/HW)
- Onnyx framework (ハイブリッド)



Azure Cobalt

卓越したコスト
パフォーマンス



64-bit Armベース
アーキテクチャ

128 CPU コア

クラウドベンダーが
使用する最も高速な
Arm CPU

Microsoft Cloudに最適化したCPUシリーズ

Azure Maia

生成 AI に最適化した
アクセラレーター



ラック、チップ、ソフト
ウェアを統合したシステム

Azure OpenAI のワーク
ロードに最適化された
デザイン

生成 AI に最適化したアクセラレーターシリーズ

Maia 100

サーバー



4x Maia 100 / サーバー、
を想定したサーバーデザイン

2x CPU、Azure Boost

業界標準イーサネット接続に
よる低コスト化

Azure Maia

水冷ラック



変わるモデルの考え方



Simple model:
1つの目的に特化した設計



Foundation model:
様々な用途に使える幅広いインテリジェンス

規模が大きくなるにつれて、AIモデルはますます強力で多機能になっている。



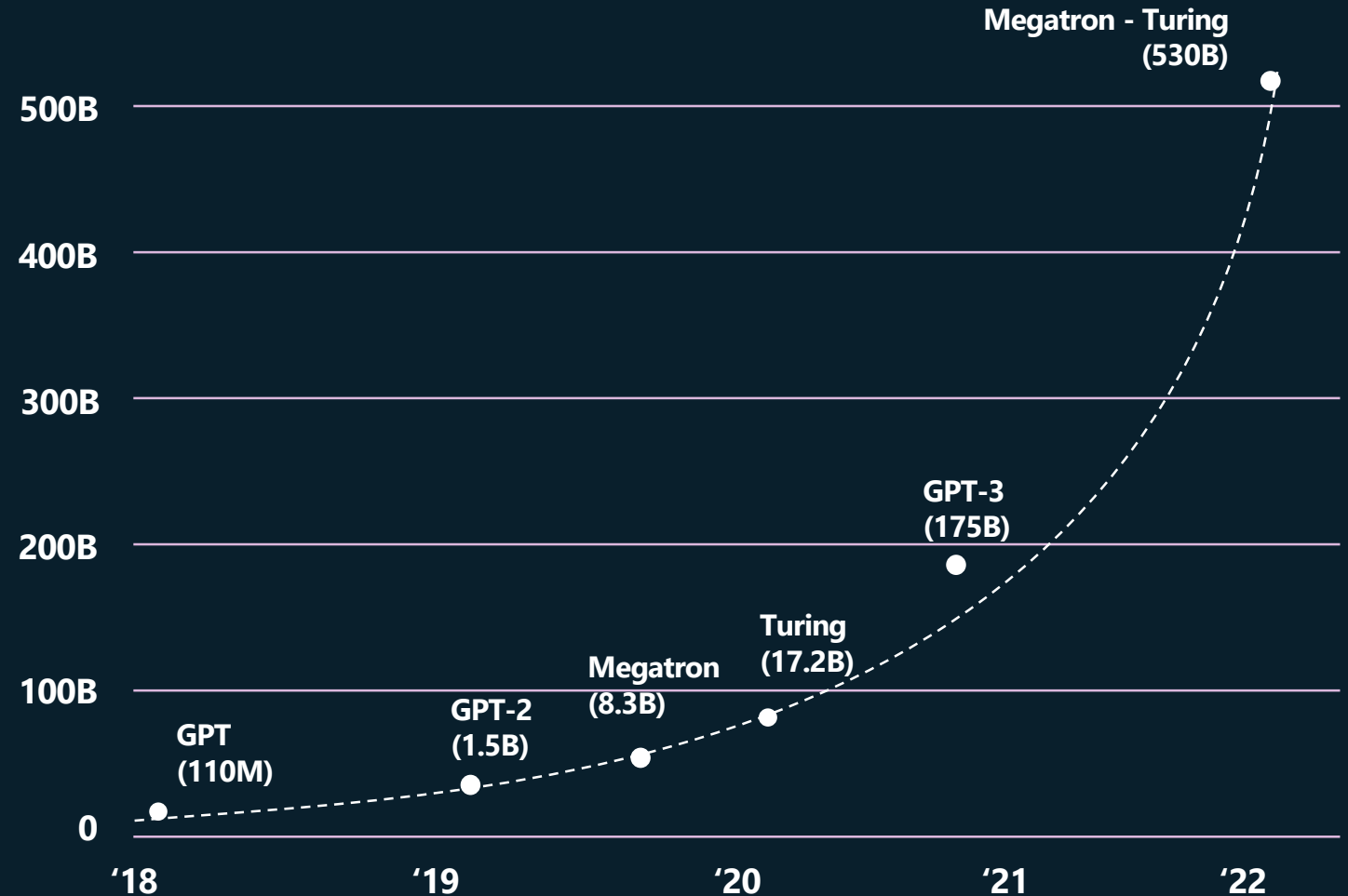
More powerful,
massive models



Multi-modal,
multi-task



Interactive



変わるソリューション開発 & デザイン

```
52     changerPhotoDescription( cell ) {  
53     }  
54  
55     function updatePhotoDescription() {  
56         if (descriptions.length > (page * 9) + (currentImage subse  
57             document.getElementById( bigImageDesc ) innerHTML = de  
58         }  
59     }  
60  
61     function updateAllImages() {  
62         var i = 1;  
63         while (i < 10) {  
64             var elementId = 'foto' + i;  
65             var elementIdBig = 'bigImage' + i;  
66             if (page * 9 + i - 1 < photos.length) {  
67                 document.getElementById( elementId ).src  
68                 document.getElementById( elementIdBig  
69             } else {  
70                 document.getElementById( elementId )  
71             }  
72         }  
73     }  
74 }
```


セキュリティサービス

サイバー脅威のマッピング



世界の平均的な組織では、**75種類以上**のサイバー・ツールとプラットフォームが存在している。



エンドポイント攻撃の場合、攻撃者は**1時間42分以内**（中央値）に企業のネットワークにアクセスでき、**15分以内**に攻撃される可能性もある。



現在、サイバーセキュリティのポジションは世界で**340万人募集**されている。



電子メールによる攻撃の場合、攻撃者は**1時間12分以内**（中央値）にユーザーのプライベートメッセージに到達する。

Azure Sentinel | インシデント

選択したワークスペース: 'CyberSecuritySoc'

検索 (Ctrl+/)

最新の情報に更新 カスタム範囲: 2021/7/1 から 2021/10/18 操作 セキュリティ効率ブック 列 ガイドとフィードバック

全般

- 概要
- ログ
- ニュースとガイド

コンテンツ管理

- ソリューション (プレビュー)
- コミュニティ

脅威管理

- インシデント
- ブック
- ハンティング
- ノートブック
- エンティティの動作
- 脅威インテリジェンス

構成

- データ コネクタ
- 分析
- ウォッチリスト
- オートメーション
- 設定

45.6千
インシデントを開く

45.5千
新しいインシデント

72
アクティブなインシデント

重大度ごとにインシデントを開く

■ 高 (5.8千)

■ 中 (7千)

■ 低 (31.9千)

■ 情報提供 (824)

soc-triage 重大度: すべて 状態: 2 件選択済み 増やす (2)

自動更新: インシデント

☐ 重大度 ↑↓	インシデント ID ↑↓	タイトル ↑↓	警告	製品名	作成
☐ 高	23493	Multi-stage incident...	25	Microsoft 365 Defe...	21/0
☐ 高	24098	Fortinet - Data tran...	0	Azure Sentinel	21/0
☐ 中	23895	Mail.Read Permissio...	1	Azure Sentinel	21/0
☐ 高	24226	Azure AD threat int...	1	Azure Active Direct...	21/0
☐ 中	24441	New access credent...	1	Azure Sentinel	21/0

Multi-stage incident involving Initial access & Later...
インシデント ID: 23493
[Microsoft 365 Defender での調査](#)

Ruben Alfa... アクティブ 高 所有者 状態 重大度

- 製品名のアラート
- Microsoft Defender for Office 365
 - Microsoft Defender for Endpoint
 - Microsoft Defender for Identity
 - Microsoft Cloud App Security
 - Microsoft 365 Defender

証拠
該当なし ① 25 1
イベント アラート ブックマーク

最終更新時間 21/08/15 22:29 作成時刻 21/07/13 01:10

- エンティティ (142 個) (プレビュー)
- ContosoADFS...

Irodriguez@se...

pgustavo@sec...

sbeavers@sec...
- 方針 (8 個)
- Initial Access

Persistence

Defense Evasion

Credential Access

+4 ①

すべての詳細を表示 操作

インシデント

重大度

状态

担当者

最終インシデント更新時間



ホーム > Azure Sentinel >

調査 ...

元に戻す やり直し

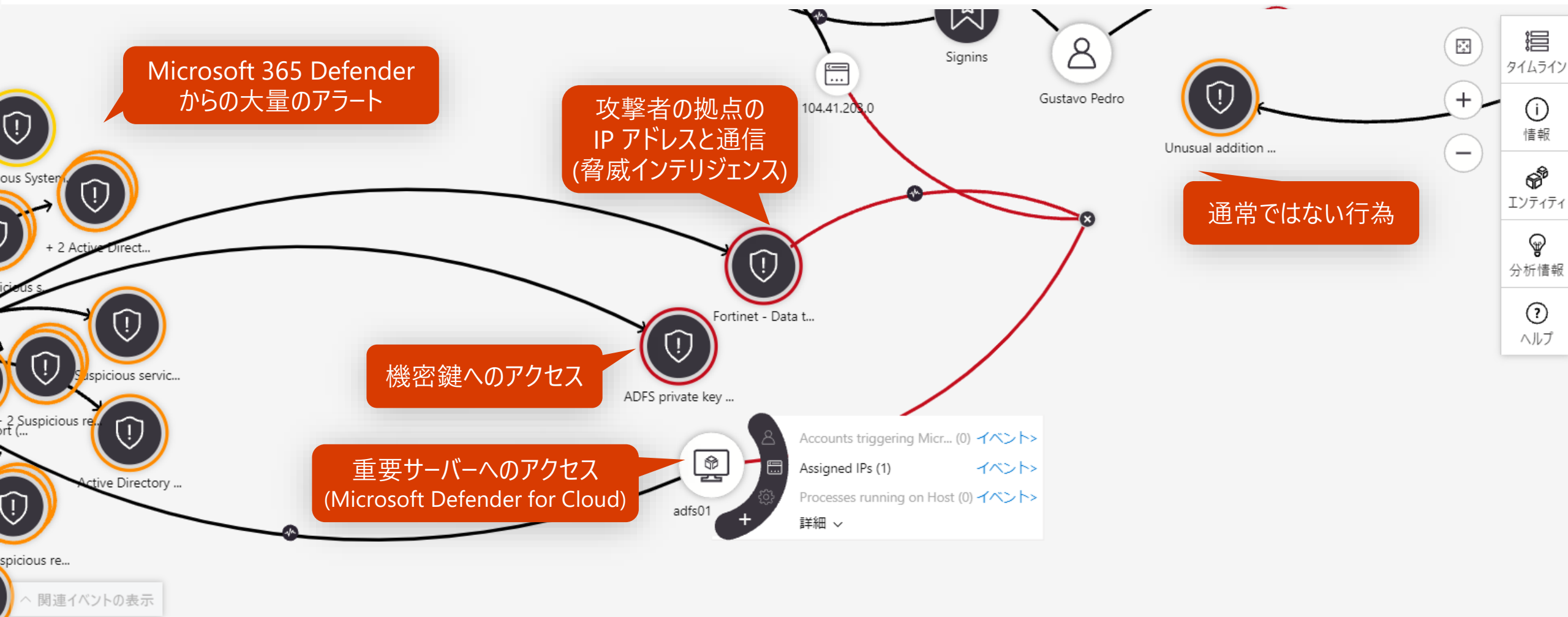
Fortinet - Data transfer to IP address...
インシデント

高
重大度

アクティブ
状態

Adi Nae Gamliel
担当者

2021/10/20 4:00:20
最終インシデント更新時間



Microsoft 365 Defender で詳細な調査と対応

インシデント > Multi-stage incident involving



Multi-stage incident involving Initial access ...

インシデントの管理 ? 脅威エキスパートに相談 コメントと履歴

概要 アラート (25) ルボックス (5) 調査 (3) 証拠と対応 (69) グラフ

攻撃の流れ

アラートは XDR により
関連付けされて集約化

資格情報が奪われる

ADFS サーバーに対し不振な行為

ADFS サーバーの秘密鍵にアクセス

SaaS にアクセス権を不正に付与

タイトル	重大度	状態	リンク先	カテゴリ	影響を受けるエンティティ	サービス ソース
Suspicious sequence of...	低	解決済み	同じデバイス	検出	workstation6...	Endpoint
Sensitive credential memory read	高	解決済み	同じデバイス	資格情報へのアクセス	workstation6...	Endpoint
Suspected DCSync attack (replication)	高	解決済み	6 の理由	資格情報へのアクセス	WORKSTATION6...	ID
Anomaly detected in ASEP regis...	中	解決済み	同じデバイス	常設	adfs01.seccxp.ninja	Endpoint
Suspicious System Owner/User Discovery	低	解決済み	同じデバイス	検出	adfs01.se...	Endpoint
Suspicious PowerShell command line	中	解決済み	同じデバイス	実行	adfs01.seccxp.ninja	Endpoint
Active Directory attributes Reconna...	中	解決済み	同じデバイス	検出	ADFS01.seccxp.ninja	ID
ADFS private key extraction attempt	高	解決済み	6 の理由	資格情報へのアクセス	adfs01.se...	Endpoint
Suspicious service registration	中	解決済み	同じデバイス	常設	adfs01.seccxp.ninja	Endpoint
Unusual addition of credentials to an OAuth app	中	解決済み	2 の理由	疑わしいアクティビティ	pgustavo	Cloud App Securit
2 alerts: A potentially malicious URL click was detected	高	解決済み	3 の理由	グループ化: 通知の...	2 メールボックス	Office 365

Security Copilot

Copilot のインターフェースは対話型

You can also add any links, files, and other information that Copilot will need to respond.

Copilot に質問
「Sentinel (Defender) が検出した“疑わしいログイン”に関連する脅威が、このログファイルに含まれていますか？」

❖ Does this log file have malicious activity related to [Microsoft Sentinel -Suspicious login activity detection - 12340?](#) →

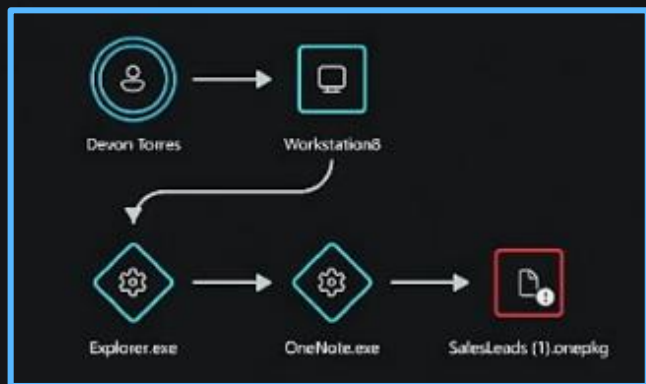
workstation1_windows_2023-02-23-10T1032.json ×

調べてほしいログファイル

12:34 PM

This alert indicates that a device belonging to **Devon Torres**, a user of the **contoso.com** domain, was targeted by an emerging, financially motivated activity group that uses OneNote attachments to deliver remote access malware. The alert provides details about the suspicious process (**ONENOTE.EXE**) that was launched from a downloaded file (**SalesLeads (1).onepkg**) and its parent process (**explorer.exe**), as well as the device's hostname (**workstation8**), OS version (Windows 21H2), and **risk score (High)**. The alert also shows the device's last seen time, external and internal IP addresses, and antivirus status. The device has a user-defined tag (**ContosoDemo**) and is onboarded to Microsoft Defender for Endpoint (MDATP).

</> 🔗



Sources

1. Microsoft Sentinel

Confirm Off-target Report Pin

Malware impact analysis

General incident analysis

Type "/" or ask anything about security

Copilot が攻撃の分析結果を表示

「このアラートは、contoso.com ドメインのユーザーである Devon Torres に属するデバイスが、OneNote の添付ファイルを使用してリモートアクセスマルウェアを配信する、金銭目的の新しい活動グループの標的にされたことを示しています。

このアラートは、ダウンロードしたファイル (SalesLeads (1).onepkg) から起動された疑わしいプロセス (ONENOTE.EXE) とその親プロセス (explorer.exe) に関する詳細、およびデバイスのホスト名 (workstation8)、OS バージョン(Windows 21H2)、およびリスクスコア (高) を提供します。

アラートには、デバイスの最終確認時刻、外部および内部 IP アドレス、ウイルス対策の状態も表示されます。デバイスにはユーザー定義タグ (ContosoDemo) があり、Microsoft Defender for Endpoint にオンボードされています」

図解し、脅威がどこで発生しているか示してくれる



Create a single PowerPoint slide outlining the incident and the attack chain.

「インシデントと攻撃の流れをまとめた 1枚の PowerPoint スライドを作成して」と依頼

12:52 PM

The following PowerPoint was generated for you. Verify its content before sharing or pinning to your investigation.

Copilot がスライドを作成。これまで膨大な時間を要していた調査と報告が数分で完了する

Ransomware Attack Investigation and Response

Summary

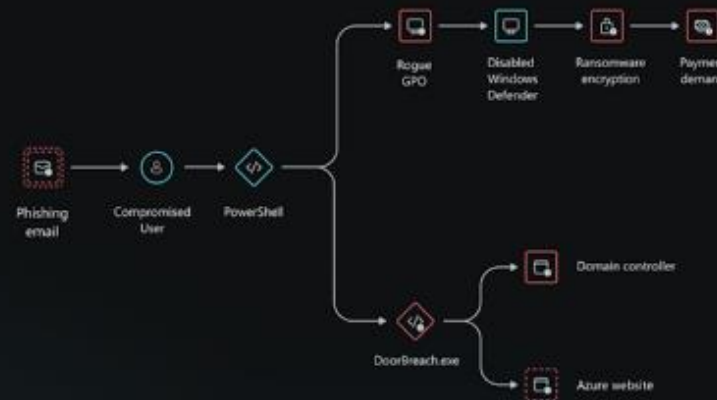
A ransomware attack encrypted files on several devices and demanded payment in Bitcoin.

The attack originated from a phishing email that compromised a user account and downloaded a malicious PowerShell script.

The script used a rogue GPO to disable Windows Defender and spread the ransomware to other devices, including a domain controller.

The SOC analyst used Sentinel and Defender for Endpoint to investigate and contain the attack, and restore the files from cloud backups.

Attack chain



Open in app



Download file



How can I contain devices and accounts that are already compromised?

12:44 PM

To contain the devices and accounts that have already synced with the new compromised GPO policies we need to isolate the affected devices from the network, revoke the access of the compromised accounts, and restore the original GPO policies.

> Isolate affected devices

DeviceId	DeviceName
e991bc329b87a388a184d318832474f0cf79961a	workstation9.contoso.com
26f96f104e8576d85be32d91d06e2fb988c0cd52	workstation8.contoso.com
ef66a4d5377a41f99327fe872fd3d2ccb789062f	workstation7.contoso.com
2f1479223851ed02bede38bbe39683e3a2aae4cc	workstation5.contoso.com
62a91704992a8e9aad5c99050fc61571b75d0eef	workstation6.contoso.com

> Revoke access of compromised accounts

AccountDomain	AccountName	count_DeviceName
Contoso	eturner	96
Contoso	dtorres	2010
Contoso	qmounir	846
Contoso	aserra	74
Contoso	hmlura	76

> Restore original GPO policies

Sources

1. Microsoft Sentinel

Confirm Off-target Report

Copilot に質問

「デバイスやアカウントが既に危険にさらされている場合、どう対処すればよい？」

Copilot が回答

「侵害されたデバイスとアカウントを封じ込めるには、影響を受けたデバイスをネットワークから隔離し、侵害されたアカウントのアクセス権を剥奪し、元の GPO ポリシーを再作成する必要があります」

「該当するデバイスは xxx、アカウントは xxx」

Sabsik Wacatac

Summary Pinned items (5)

Alert Summary

This alert indicates that a device belonging to Devon Torres, a user of the contoso.com domain, was targeted by an emerging, financially motivated activity group that uses OneNote attachments to deliver remote access malware. The alert provides details about the suspicious process (ONENOTE EXE) that was launched

- Attempted AMSI tampering and process injection
- Suspicious Microsoft Defender Antivirus exclusion and startup folder addition
- Suspicious LDAP query and process discovery
- Suspicious WMI process creation
- Suspicious PowerShell command line and script execution

Attack Details

Malicious OneNote package file downloaded

Type "/" or ask anything about security

身近になるAIを使用した ソリューション開発





Microsoft Copilot Studio

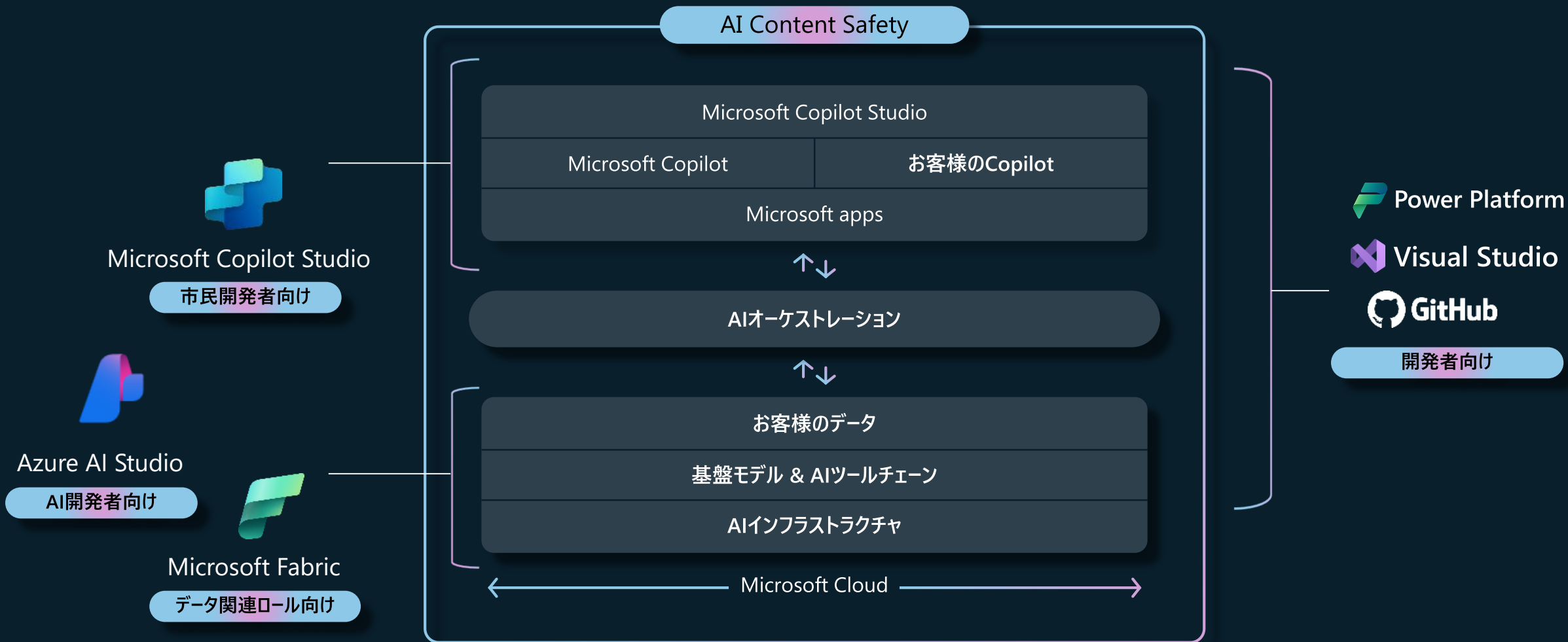
お客様のカスタムCopilotをローコードで開発可能な
統合プラットフォーム

1,100 以上の標準搭載された
プラグインとコネクタ

自分だけのCopilot
をゼロから作る

OpenAI GPTとプラグイン
の作成と使用

Copilot を創る手段の位置づけ



ローコードでオリジナルのCopilot を創る



Copilot Studio

- 定義していないトピックについて生成AIで回答する
- 社内のSharePoint ドキュメント等に対して質問する
- オンプレミスのデータソースに対して接続する

The screenshot displays the Copilot Studio interface. On the left is a sidebar with navigation options: Copilot, 概要 (Overview), トピック (Topics), エンティティ (Entities), 生成 AI (Generative AI), 分析 (Analysis), 公開 (Publish), Microsoft Copilot の拡張 (プレビュー) (Extensions (Preview)), 設定 (Settings), コパイロットの詳細 (Copilot details), AI 統合ツール (AI integration tools), チャンネル (Channels), 顧客エンゲージメントハブ (Customer engagement hub), セキュリティ (Security), and Copilot の非表示 (Hide Copilot). The main area is titled 'Copilot Studio | 生成型の回答 - SharePoint' and contains a 'Copilot のテスト' (Test Copilot) chat window. The chat window shows a conversation in Japanese. The first message is a system message: 'こんにちは！社内のSharePointの情報をまとめて回答しますよ。' (Hello! I will summarize and answer information from SharePoint within the company). The second message is a user question: 'XBOXの保証について教えてください' (Please tell me about the warranty for Xbox). The third message is a detailed system response in Japanese explaining warranty policies for Xbox One and accessories, mentioning a 95-day warranty and the possibility of a refund or replacement. Below the chat window is a text input field labeled 'Type your message'. To the right of the chat window is the 'Topics' configuration panel. It shows a list of system topics with columns for Name, Trigger, Description, Errors, and Editing. The topics listed are: Conversation Start, Conversational boosting, End of Conversation, Escalate, Fallback, Multiple Topics Matched, On Error, Reset Conversation, and Sign in. Each topic has a specific trigger and a brief description of its function.

Copilot のテスト

Tracking: off

チャット

こんにちは！社内のSharePointの情報をまとめて回答しますよ。

Just now

XBOXの保証について教えてください

Just now

修理や交換には、修理された部品が使用される場合があります [1 回]。修理または交換後、Xbox One やアクセサリは、元の保証期間の残り、または法定の保証期間、またはMicrosoftが出荷した日から95日のいずれかの期間、この保証の対象となります [1 回]。修理または交換されたXbox Oneやアクセサリには、オーストラリアでは、法定の消費者保証に加えて、より長い法定の保証期間を提供する可能性がある法定の消費者保証が付属します [1 回]。修理または交換によるXbox Oneやアクセサリの修理または交換、または購入価格の返金は、あなたの独占的な救済措置です [1 回]。保証期間が終了した後、および別途定める法定の保証期間が終了し

Type your message

Topics

Topics (7) Plugin actions (preview) (0) **System (9)**

System topics are necessary to help your Copilot run effectively. Without them, your Copilot may not work as intended. You can't delete system topics.

Name	Trigger	Description	Errors	Editing
Conversation Start	On Conversation Start	This system topic triggers ...		
Conversational boosting	On Unknown Intent	Create generative answers...		
End of Conversation	On Redirect	This system topic is only tr...		
Escalate	On Talk to Agent	This system topic is trigge...		
Fallback	On Unknown Intent	This system topic triggers ...		
Multiple Topics Matched	On Select Intent	This system topic triggers ...		
On Error	On Error	This system topic triggers ...		
Reset Conversation	On Redirect			
Sign in	On Sign In	This system topic triggers ...		

Copilot Studio =
Power Virtual Agents + 生成AI + more



Microsoft Copilot Studio 構成



Copilot Studio

Power Virtual Agents
+ 生成AI



内部向け
Copilot



外部向け
Copilot

more



Copilot for Microsoft 365
の拡張

生成AI 搭載のCopilot の作成はこんなにも簡単

Step 1



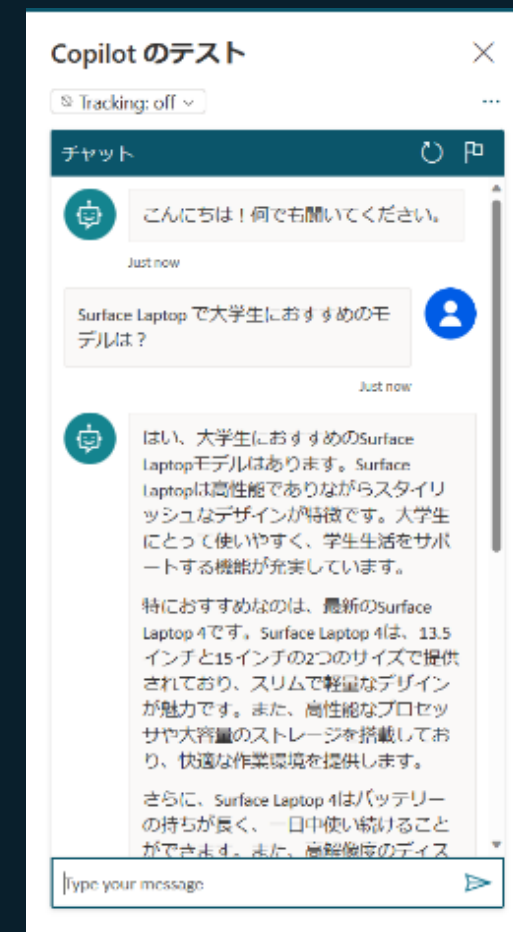
<https://copilotstudio.microsoft.com/> にアクセス Copilot を作成

Step 2



Copilot に名前をつけ、参照するURLを指定
(公開Webサイトの場合こちらで完了。
認証を伴うサイトの場合、セキュリティ設定を実施)

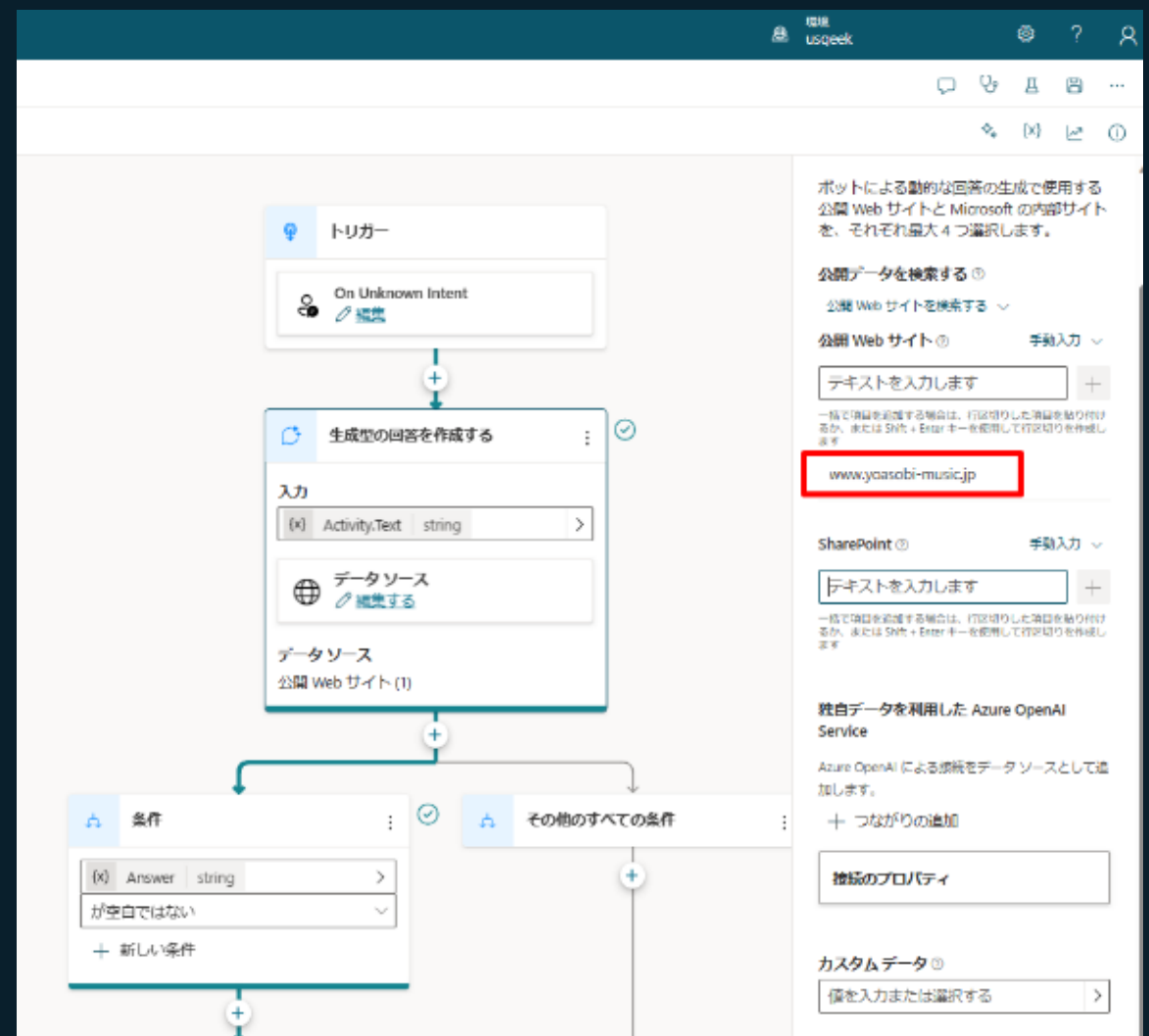
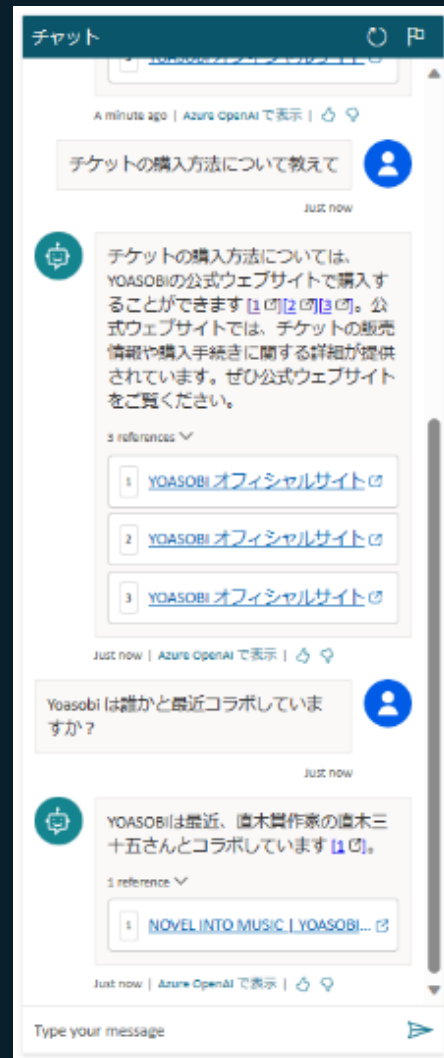
Step 3



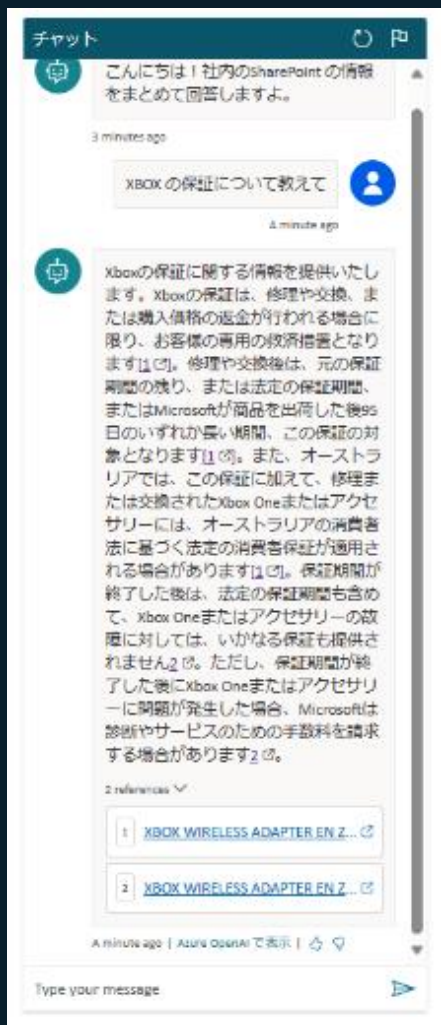
Copilot が利用可能に

公開サイトをソースとして生成型の回答を行う

- 公開サイトのURLを指定するのみで作成
- 最大4個のURLを指定
- 自社の公開FAQサイトなどに接続して外部向けのCopilot 等にご利用



認証サイトをソースとした回答を行う



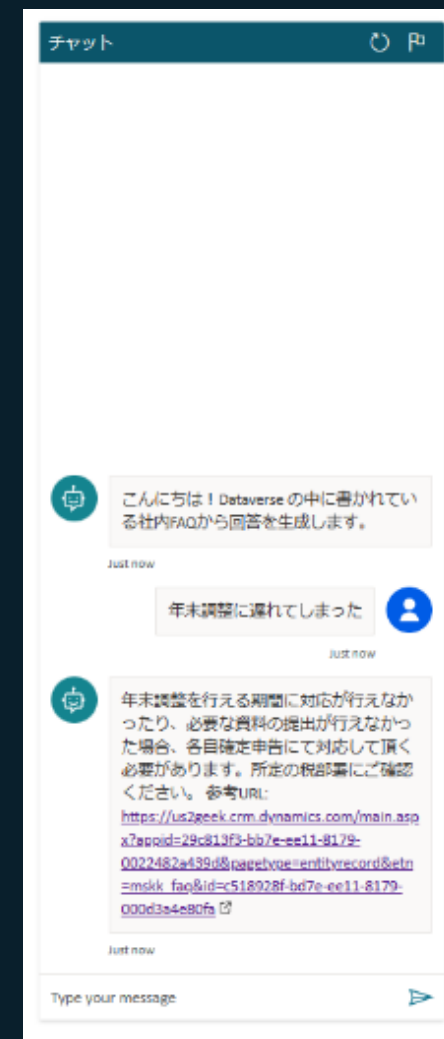
Microsoft Graph



ユーザーのアクセス許可がある
範囲での検索

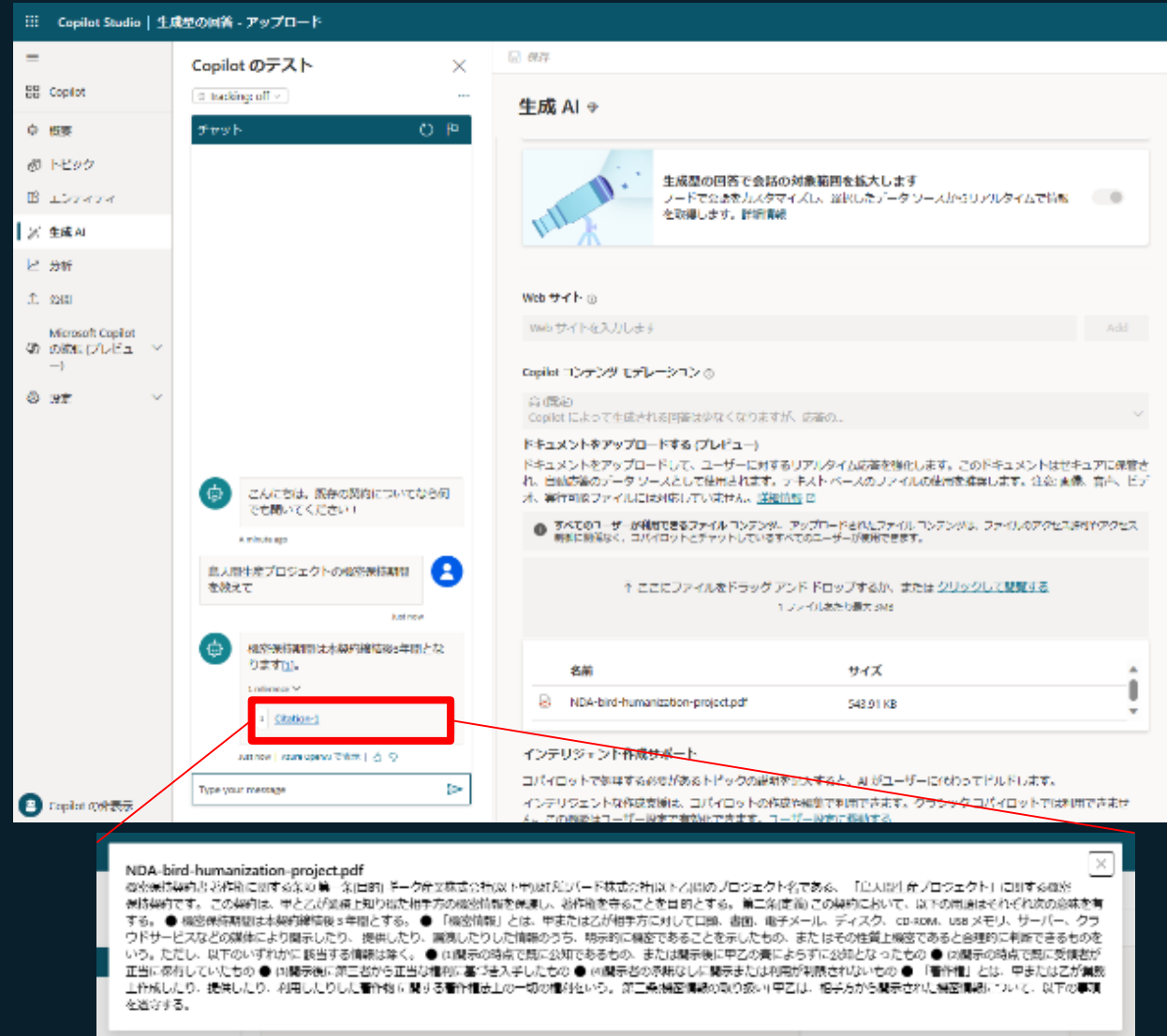
対応データソース

1. 公開サイト
2. SharePoint
3. アップロードしたファイル
4. カスタムデータソース
5. その他コネクタ 1,000以上



アップロードしたファイルをソースとして生成型の回答を行う

オフィスファイル（DOCX、PPTXなど）、PDFファイルなど一般的に使用されているファイルを活用した回答



AI 活用環境は常に進化
今日の**研究**も明日には**汎用化**される



Microsoft