KPMG あずさ監査法人

Start Judgment_Project Explanation Materials

POC Cat KIT

株式会社 KPMG Ignition Tokyo

August 2023

This report contains 21 pages

POC Cat KIT Start Decision Plan Template .docx

スタート判定計画書
August 2023

Document review and approval

Revision history

Version	Author	Date	Revision
1.0	Ken Izumi	2023/08/03	first edition

This document has been reviewed by

	Reviewer	Date reviewed
1	Naoko Iwamoto	2023/08/03
2		
3		
4		
5		

This document has been approved by

	Subject matter experts		
	Name	Signature	Date reviewed
1	Tsuyoshi Moriya		2023/08/04
2			
3			
4			
5			

スタート判定計画書
August 2023

Contents

1 Outline of the project 4
1.1 Background & Purpose [ST1] 4
1.2 Service User [ST1] 4
1.3 Structure [ST1] 5
1.4 schedule 5
1.4.1 Hope for a period [ST1] 5
1.4.2 Deployment Schedule [ST2] 5

2 Technology Overview 6
2.1 Technology & Functional Overview [ST2] 6
2.2 System Overview Diagram [ST2] 7
2.3 Hosting Environment [ST2] 8

3 Type of information 9
3.1 Information - System Confidentiality, Integrity, and Availability [ST1] 9
3.1.1 Confidentiality of information 9
3.1.2 Completeness of information 10
3.1.3 System Availability 11

4 security 12
4.1 Permissions [ST2] 12
4.2 Encryption [ST2] 12
4.3 Network Isolation [ST2] 12
4.4 Logging Monitoring [ST2] 13
4.5 Redundancy and backup [ST2] 13

5 Software Development Approach 14
5.1 Documenting Frameworks and Processes [ST2] 14
5.2 Development Language [ST2] 14

6 Operation and Maintenance System 15
6.1 Corresponding department [ST1] 15
6.2 Security Incident System [ST2] 15
6.3 System Failure System [ST2] 15
6.4 System Operation and Maintenance System [ST2] 16
6.5 User Support System [ST2] 16

7 Test Preparation 17
7.1 UAT (User Acceptance Test) [ST2] 17
7.2 BCP テスト（Business Continuity Planning） [ST2] 17

8 Release plan 18
8.1 Preparing for Release [ST2] 18

9 Establishment of OSS (Open Software) Management System 19
9.1 OSS Management Responsibilities and Response Policy [ST2] 19

10 approval 20
10.1 Service Owner Approval [ST1] 20
10.2 Budget Approval [ST1] 20

11 Security Assessment 21
11.1 Vendor Security Assessment Results [ST2] 21
11.2 Independence check [ST2] 21
11.3 Outsourcing of personal data processing [ST2] 21
11.4 Cloud Service Risk Assessment [ST2] 21

1 Outline of the project

1.1 Background and Purpose [ST1]

(Describe the background and purpose)

Led by KIT's data scientists, we conducted research on generative AI. I would like to verify whether it can be used for KIT's internal operations. There is an issue that it takes time for KIT employees to grasp internal rules, and we will take it up as a use case to be verified.

Implementation period: September-October 2023

Purpose: To verify the feasibility and practicality of in-house use of generative AI technology. In addition, we will decide whether or not to proceed with commercial development for KIT use.

Scope:

- ***Usage data: KIT-INTERNAL Some content in SharePoint, mainly attendance-related rules and instructions, such as work rules and how to take leave*** *(personal information is not included in the data used in this PoC)*
- **利用技術：*Azure Open AI Service、Azure Cognitive Search、One Platform Japan Country Hosting***

1.2 Service User [ST1]

(Describe the scope of service users (clients, KPMGJapan users, KPMG member firms, public users, etc.), the number of users, and the frequency of use.))

At the time of verification, the following is assumed

user	Number of users	Frequency of use
KIT Project Members	About 5 people	About 20 hours per week
KIT User Test Participants	About 3-5 people	About 10 hours per week during 1-2 weeks during the project period

1.3 Structure [ST1]

team	person in charge
KIT Project Members	Deleva, Giacomo (KIT) Ahi, Sercan (KIT) Izumi, Ken (KIT) Bangari, Samuel (KIT) Iwamoto, Naoko (KIT)
KIT User Test Participants	About 3-5 people will be assigned. 確定：Hashimoto, Mika (KIT)

1.4 schedule

1.4.1 Desired delivery date [ST1]

(Describe the desired delivery date and scheduled release date)

Desired delivery date: Subscription for CH verification should be provided by August 25thRelease date:
Not eligibleSubmit to a separate judgment meeting at the time of release after verification.

1.4.2 Deployment Schedule [ST2]

(Outline schedule of introduction is described)

This time, it is for verification purposes, and there is no production release. If you want to apply it in production, apply for a start gate separately.

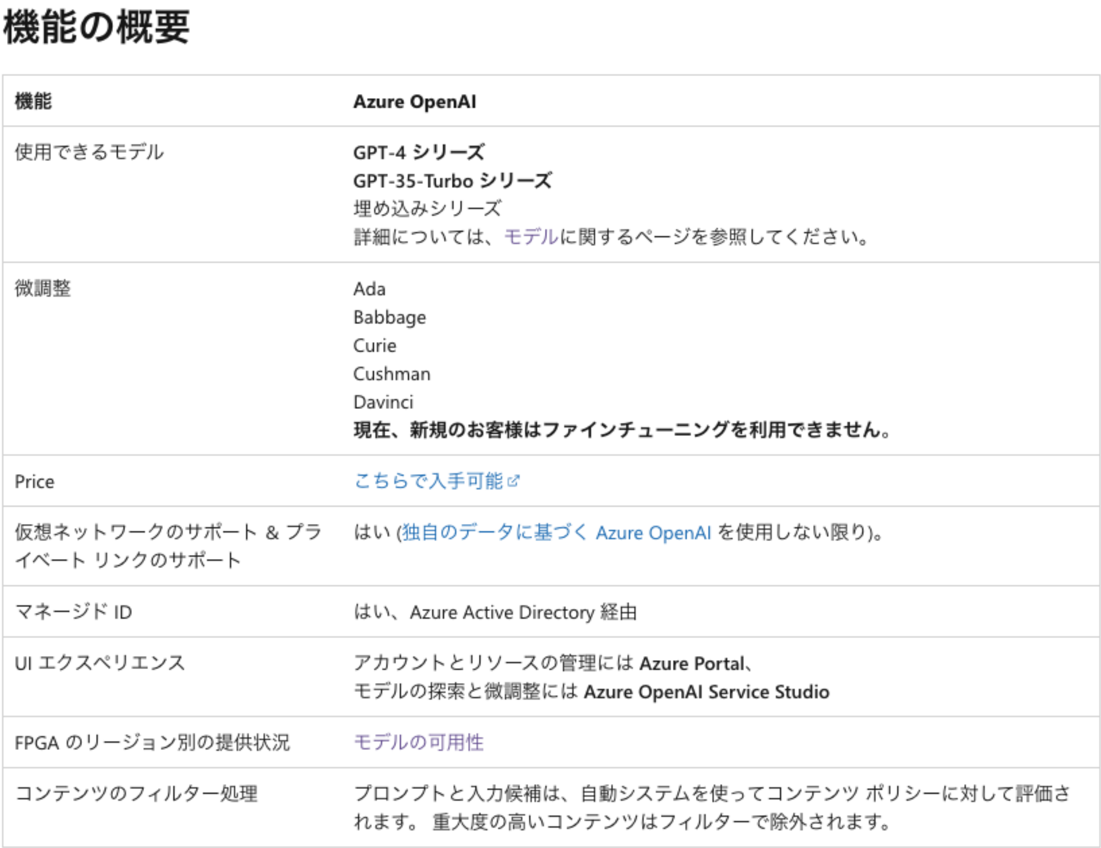
Verification period: September to October 2023

2 Technology Overview

2.1 Technology & Feature Overview [ST2]

(Provide an overview of the main technologies and functions used in system services)

- **Azure Open AI Service**



機能の概要

機能	Azure OpenAI
使用できるモデル	**GPT-4 シリーズ** **GPT-35-Turbo シリーズ** 埋め込みシリーズ 詳細については、モデルに関するページを参照してください。
微調整	Ada Babbage Curie Cushman Davinci **現在、新規のお客様はファインチューニングを利用できません。**
Price	こちらで入手可能
仮想ネットワークのサポート & プライベート リンクのサポート	はい (独自のデータに基づく Azure OpenAI を使用しない限り)。
マネージド ID	はい、Azure Active Directory 経由
UI エクスペリエンス	アカウントとリソースの管理には **Azure Portal**、 モデルの探索と微調整には **Azure OpenAI Service Studio**
FPGA のリージョン別の提供状況	モデルの可用性
コンテンツのフィルター処理	プロンプトと入力候補は、自動システムを使ってコンテンツ ポリシーに対して評価されます。 重大度の高いコンテンツはフィルターで除外されます。

Source: Azure OpenAI Service とは - Azure AI services | Microsoft Learn

- **Azure Cognitive Search**

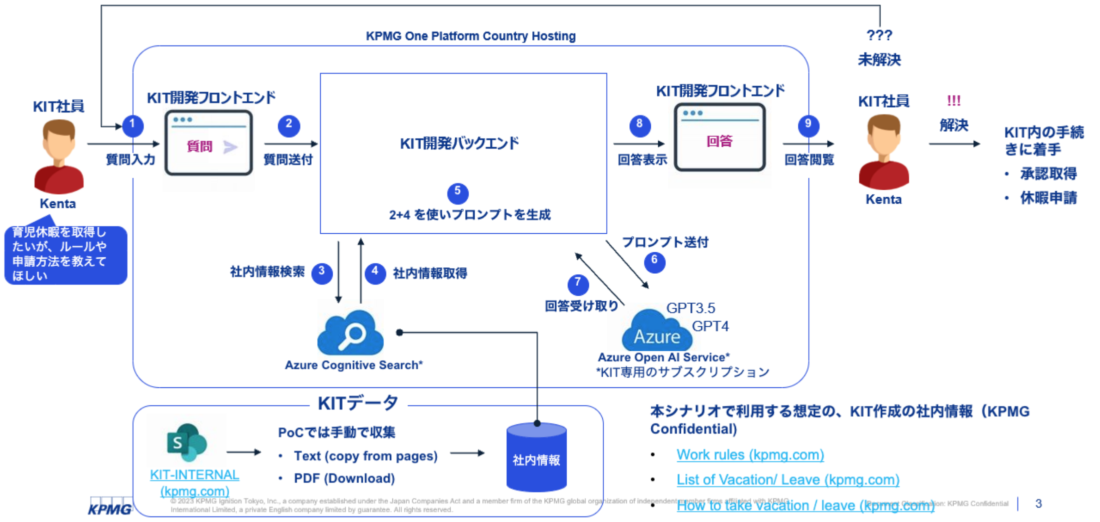
Azure Cognitive Search is a cloud search service that provides developers with the infrastructure, APIs, and tools to build rich search experiences for private, heterogeneous content into web, mobile, and enterprise applications.

Source: Azure Cognitive Search の概要 - Azure Cognitive Search | Microsoft Learn

2.2 System Overview Diagram [ST2]

(Describe the outline configuration diagram of the system)

Users & Data Flows



KPMG One Platform Country Hosting

???
未解決

KIT社員

Kenta

育児休暇を取得したいが、ルールや申請方法を教えてほしい

1 質問入力

KIT開発フロントエンド

質問

2 質問送付

KIT開発バックエンド

5 2+4 を使いプロンプトを生成

社内情報検索 3

4 社内情報取得

Azure Cognitive Search*

プロンプト送付 6

7 回答受け取り

GPT3.5
GPT4

Azure

Azure Open AI Service*
*KIT専用のサブスクリプション

8 回答表示

KIT開発フロントエンド

回答

9 回答閲覧

KIT社員

Kenta

!!!
解決

KIT内の手続きに着手
- 承認取得
- 休暇申請

KITデータ

KIT-INTERNAL (kpmg.com)

PoCでは手動で収集
- Text (copy from pages)
- PDF (Download)

社内情報

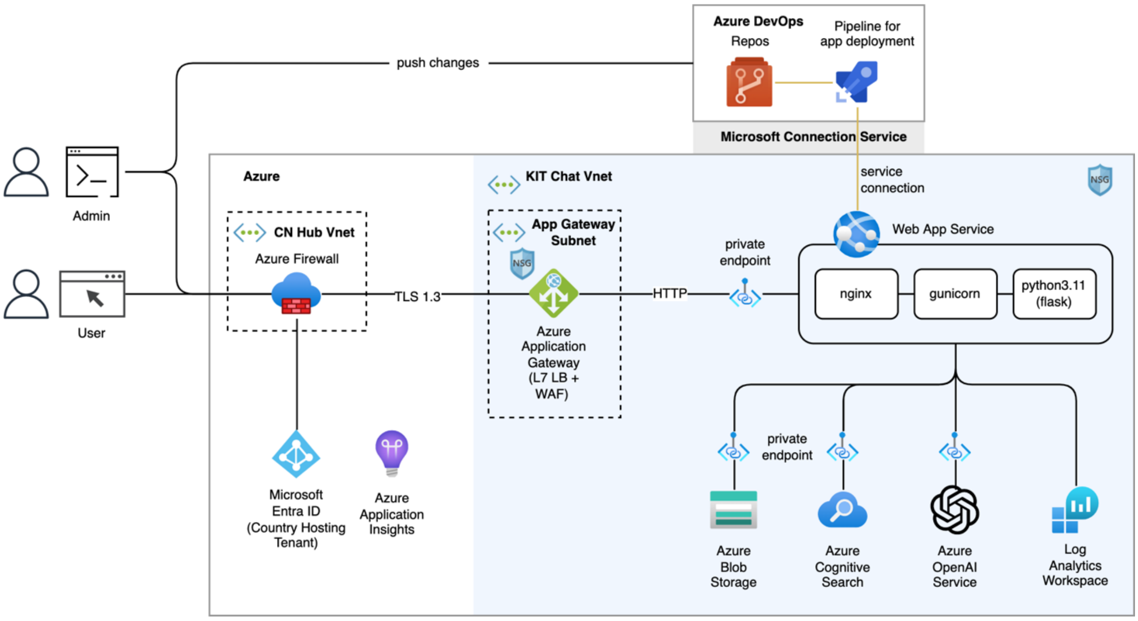
本シナリオで利用する想定の、KIT作成の社内情報（KPMG Confidential)
- Work rules (kpmg.com)
- List of Vacation/ Leave (kpmg.com)
- How to take vacation / leave (kpmg.com)

© 2023 KPMG Ignition Tokyo, Inc., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Document Classification: KPMG Confidential | 3

architecture

The following is the construction design on Cloud Next. Planned to be customized for CH



2.3 Hosting Environment [ST2]

(Describe the hosting environment of the system.) Public Cloud, One Platform, CloudNext, on-premise, etc. ）

*One Platform (Country Hosting)*上に構築する

3 Type of information

3.1 information - System confidentiality, integrity, and availability [ST1]

(Select the confidentiality, integrity, and availability of information and systems from the following definitions.))

3.1.1 Confidentiality of information

Confidentiality of information

Level of management required	division	explanation	
4	supreme	If information is leaked to unauthorized persons, it will have a serious impact on business, so it must not be disclosed or circulated to anyone other than the specific person involved in the information	□
3	high	If information is leaked to unauthorized persons, it will have a significant impact on business, so it must not be disclosed or circulated to anyone other than the specific person involved in the information	□
2	middle	If information is leaked to unauthorized persons, it will affect the business, so it can be disclosed and provided only to those involved in the business of the organization.	☑
1	low	Even if information is leaked to unauthorized persons, it can be disclosed and provided outside the company without affecting business operations.	□

■ Presence or absence of personal information

	Yes/No	detail

Presence or absence of personal information and My Number	possession	The personal data used includes user names, employee numbers, organizational affiliations, IIDs, and email accounts registered in Active Directory
Whether or not GDPR applies	nothing	
Whether or not the client handles confidential data	nothing	

3.1.2 Completeness of information

Completeness of information

Level of management required	division	explanation	
3	high	Even if the information is changed (tampered with, destroyed, etc.) without permission, if the content of the information is incorrect, or if all or part of the information is not available, the impact on business operations is serious and significant.	□
2	middle	Even if the information is changed (falsified, destroyed, etc.) without permission, if there is an error in the content of the information, or if all or part of the information is not available, the impact on business will be significant.	□
1	low	Even if the information is changed (falsified, destroyed, etc.) without permission, if the content of the information is incorrect, or if all or part of the information is not available, there will be little impact on business	☑

3.1.3 System Availability

■Business Criticalityレート

Business Criticality	
BC4 – Mission Critical System A system that is critical to business execution, if it is not available even for a short period of time, it will have a significant impact on the business. Recovery time is less than 4 hours;Always on.	□
BC3 – Essential If the system is down for more than one day, it will have an impact on the business and the bottom line. Recovery time is less than 24 hours;High availability.	□
BC2 – Critical If the system goes down for a few days, you can lose a lot of revenue and reputation. Recovery time is less than 7 days, standby facility (with or without expedited shipping contract).	□
BC1 – Important If the system goes down for a few weeks, you can lose revenue. The recovery period is no more than 2 months;Standby facility.	□
BC0 – Low Impact If the system goes down for a few weeks, you can lose revenue. Recovery time is less than 1 year	☑

* Those set to BC3 or higher are subject to the BCP test. In that case, at the time of release judgment, it is necessary to switch to the DR site and prepare a cutback procedure manual, and to conduct a switch-back test even once, and to have a trail of it.

4 security

4.1 Permissions [ST2]

(Describe the operation plan for access rights.) Administrators and users should have minimal access and comply with the Global Standard, and the start decision confirms that the operation of access rights is planned in the design phase.)

Submit the required JP-SG application

- *Groups containing JP-DL KIT-Employee*
- *Groups containing JP-DLKIT-Intern*

Limited number of users at the time of verification

4.2 Encryption [ST2]

(Describe the operation plan for encryption.) It is necessary to encrypt data at rest, data in transit, and communication data in accordance with the Global standard, and the start decision confirms that encryption is planned in the design phase.)

Communication is encrypted by TLS 1.2.

Access keys to Azure resources, including Azure Open AI, are protected by storing them in Key Vault.

Data at rest on Azure (Azure Storage, PostgreSQL) is encrypted with FIPS 140-2 certified cryptographic modules.

4.3 Network Isolation [ST2]

(Describe the plan for network isolation.) It is necessary to physically and logically separate the network according to the application (production, development, staging, etc.), and the start decision confirms that network isolation is planned in the design phase.)

The resource to be created uses Private Endpoint and blocks access from outside the company (= Internet). Users of the internal network access the application through ExpressRoute.

Specific VNet and NSG configurations are set in consultation with the ITS team at the time of subscription configuration.

4.4 Logging Monitoring [ST2]

(Audit log acquisition and monitoring are described.) The start decision confirms that logging and monitoring will be planned in the design phase.)

Application logs, Activity Logs (Azure Platform logs), various metrics, and OpenAI's output data required for quality improvement analysis are also maintained.

4.5 Redundancy and backup [ST2]

*(System redundancy and backup are described.) It is necessary to ensure availability according to the BC rate (Business Criticality rate), and confirm that redundancy and backup operations are planned in the design phase. * For backup operation, please refer to the backup implementation procedure manual (LINK).*

Since the Business Criticality rate is BC0, redundancy is not performed.
Backups use regular Azure services

5 Software Development Approach

5.1 Documenting Frameworks and Processes [ST2]

(If software development occurs, describe the framework and process (waterfall, prototyping, iteration, agile).))

prototyping
KIT: Advance the project with iteration (sprint) planning on regular Azure DevOps

5.2 Development Language [ST2]

(The development language is described.))

Backend: Python (flask)
Frontend: JavaScript (react)

6 Operation and Maintenance System

6.1 Corresponding department [ST1]

(Describe the names of the system operation and maintenance and user support departments.) An agreement must be reached with the relevant department.)

	Department Name
System Operation & Maintenance Department	Solution&Products, Technology Foundation, Incubation
User Support Department	Solution&Products, Technology Foundation, Incubation

6.2 Security Incident System [ST2]

(Describe the system in the event of a security incident.) In the start judgment, confirm that the construction of a system and the creation of a procedure manual in the event of a security incident are planned in the design phase.)

The Core Subscription part of Country Hosting will be handled by the ITS Operations Department.
As for the subscription part for verification, the project team will be in charge of security incident response at the time of verification, and in the event of an incident, the person in charge will escalate to KJ-CSIRT via KIT's security office.

* In the event of a P-1 and P-2 security incident in the Japan Country Hosting environment, Global will contact the Japan member firm as follows.

- Primary contact of the Information Security Department: Toshiyuki Ishige <toshiyuki.ishige@jp.kpmg.com>
- Secondary Contact for Information Security Department: Cornelius Smith <cornelius.smith@jp.kpmg.com>

6.3 System Failure System [ST2]

(The system in the event of a system failure is described.) In the start judgment, it is confirmed that the construction of a system in the event of a system failure and the creation of a procedure manual are planned in the design phase.)
At the time of verification (Failure response will be carried out by the members described in "1.3 System").

6.4 System Operation and Maintenance System [ST2]

(The system operation and maintenance system is described.) In the start judgment, it is confirmed that the construction of a system operation and maintenance system and the creation of a procedure manual are planned in the design phase.)

At the time of verification, the members listed in "1.3 System" will respond to failures.

6.5 User Support System [ST2]

(Describe the support system.) In the start judgment, it is confirmed that the construction of a support system and the creation of a procedure manual are planned in the design phase.)

At the time of verification, the members listed in "1.3 System" will respond to failures.

7 Test Preparation

7.1 UAT (User Acceptance Test) [ST2]

(An overview of UAT is described.) In the start decision, in the design phase, it is confirmed that the plan includes the construction of a system acceptance process before release. ）

Since it is a simple application and there is no content that the user is confused about, UAT is not implemented.

7.2 BCP テスト（Business Continuity Planning） [ST2]

（3.2 For those that are set to BC3 or higher in the Business Criticality rate, they are subject to BCP testing, so it is necessary to prepare a switchover procedure and a cutback procedure manual to the DR site at the time of release judgment, and to perform a switch-back test at least once, and to have a trail of it. When requesting work from a contractor, etc., it is necessary to include the contents in the RFP, so state that the preparation procedures for these tasks have been completed. ）

Not applicable

8 Release plan

8.1 Preparing for Release [ST2]

(Describe the release plan.) In the start judgment, it is confirmed that the plan includes preparations for the release, such as the creation of a cutback plan, the implementation of rehearsals, the creation of release procedures, and the creation of a user deployment plan in the design phase.)

Not applicable in the validation phase

9 Establishment of OSS (Open Software) Management System

9.1 OSS Management Responsibilities and Response Policy [ST2]

(When using OSS, describe the OSS name, the person in charge of management, and the response policy.) In the start judgment, it is confirmed that the construction of an OSS management system, such as the person in charge of management and the response policy, is included in the plan in the design phase.)

The Technical Lead will be responsible for the management of the OSS in accordance with the current KIT Development Process (SDLC).
We have confirmed that there are no problems with the license of all OSS used at this time, but if the license is changed and some action is required, we will promptly respond with the KIT legal department.

10 approval

10.1 Service Owner Approval [ST1]

(Describe the name of the service owner and whether or not it has been approved for introduction)

It has been approved by the service owner, Tsuyoshi Moriya (Partner).

10.2 Budget Approval [ST1]

(Indicate whether or not the budget has been approved.) Approval is required, including the possibility of incurring security testing costs, especially depending on the BC, confidentiality, and integrity rates.)

The budget at the time of verification (about 5 million) has been approved in the KIT.

11 Security Assessment

11.1 Vendor Security Assessment Results [ST2]

(Describe whether or not the "Confirmation of Information Security for Contractors" has been implemented.))

Not applicable

11.2 Independence check [ST2]

(Describe whether or not the vendor has been confirmed for independence)

Not applicable

11.3 Outsourcing of personal data processing [ST2]

(In the case of outsourcing, check whether the outsourced work includes the processing of personal information.))

Not applicable

11.4 Cloud Service Risk Assessment [ST2]

(In the case of a cloud service, describe whether or not the Cloud Service Risk Assessment has been conducted.))