



日本ビジネスシステムズ株式会社

リファレンスアーキテクチャ

2023 / 10 / 12

Japan Business Systems, Inc.



シナリオ概要

企業向けにセキュアチャットと社内情報の検索

私たちは、Azure OpenAI Serviceを使用して、セキュアな企業向けチャットサービスを提供しています。このサービスでは、ChatGPTの生成AIを活用し、Microsoft Entraを利用し安全なIDをつかってアクセスできます。また閉域網での提供も可能です。

さらに拡張機能として次の4つの機能を提供予定です。1つ目は管理者向けの利用者管理機能や分析機能です。これにより、チャットの利用状況やトレンドを把握し、効果的なコミュニケーション戦略を立てることができます。

2つ目はUIのカスタマイズ機能です。企業のニーズやブランディングに合わせて、チャットの外観をカスタマイズすることができます。

3つ目はTeamsとも同一のアーキテクチャで利用することができます。既存のTeamsの機能を活用することもできます。

4つ目はAzure Cognitive Searchと組み合わせ、特定の社内文書を検索して生成AIで返答する機能です。これにより、会話ベースでの企業内の情報検索が容易になります。

上記の拡張機能により、企業内のコミュニケーションと情報管理を強化するための統合ソリューションとなります。安全性、カスタマイズ性、分析性を備えたチャットサービスで、効率的かつ効果的なコミュニケーションを実現します。



アプリUI

ユーザー利用画面例



管理者向けUI設定画面例

Alplicity-Chat-v2-manageme

Hello, [Log out](#) [About](#)

☰ UI設定

UI設定

テキスト設定

アプリケーション名

チャットAI名

色設定

項目名	ライトモード色	ダークモード色	説明
Icon Background Color			画面左上のアイコン画像やアプリ名称が表示される領域の背景色です。
Big Background Color			画面左側メニューの背景色です。
Small Background Color			画面左側メニューの下部にある帯の色です。

管理者向け利用権限割り当て画面例

The screenshot displays the 'Alplicity-Chat-v2-manage' interface. On the left is a dark sidebar with navigation options: 'UI設定' and 'アクセス設定'. The top right shows a user greeting 'Hello, [redacted]' and links for 'Log out' and 'About'. The main content area is titled 'チャット権限の割り当て状況' (Chat Permission Assignment Status).

GPT-4ユーザー
GPT-4モデルのAIとチャット可能なユーザーです。

名前	オブジェクトの種類
このロールはどのユーザーやグループにも割り当てられていません	

割り当ての編集

GPT-3.5-Turboユーザー
GPT-3.5-TurboモデルのAIとチャット可能なユーザーです。

名前	オブジェクトの種類
[redacted]	User

割り当ての編集

管理権限の割り当て状況

全体管理者
全体管理者は、ロール管理を含めてアプリ内のすべての管理権限を有します。

名前	オブジェクトの種類
[redacted]	User
Alplicity-v2-test-Security-GP	Group

管理者向けチャットログ確認画面例

Alplicity-Chat-v2-manage

Hello, [redacted] [Log out](#) [About](#)

UI設定

全社チャット内容

2023/07/09 ~ 2023/09/08 絞り込み [CSVダウンロード](#)

日時	セッションID	ユーザー	Sender	モデル名	チャットメッセージ	セッションごとの累積Promptトークン数	Completionトークン数
2023/08/09 2:32:14	14a1493c-9fd7-44dc-a698-fd43e65884c8	[redacted]	assistant	gpt-35-turbo	Azure のマネージドIDは、Azure環境内において、リソースへの認証用に使用される安全なアイデンティティです。簡単に言うと、Azure上の仮想マシンやAzure Functionsなどのリソースが使用する認証キーのようなものです。従来の認証方式では、アプリケーションやサービスには、通常、ユーザーアカウントやクレデンシャルが必要でした。しかし、この方法だと、認証情報を管理することが手間やセキュリティ上の問題もありました。そこで、AzureではマネージドIDという仕組みを導入することで、リソースに必要な認証情報を簡単かつ安全に管理できるようにしました。マネージドIDを使用すると、認証情報を設定する必要がなく、Azure ADとは別途で生成された一意のIDを使用するため、セキュリティも高くなります。また、マネージドIDは、Azureリソース上の認証情報の中で特定の範囲内で使用されることで、アプリケーションやサービスによって直接的なアクセス制限をかけることができます。簡単に言うと、マネージドIDはAzure環境内においてセキュアかつ簡単に認証に必要なキーを管理するための仕組みであり、従来の認証方式と比べて簡単かつ高セキュリティな認証ができます。	0	497
2023/08/09 2:31:58	14a1493c-9fd7-44dc-a698-fd43e65884c8	[redacted]	user		Azure のマネージドIDについてわかりやすく説明してください。	768	0
2023/08/09 2:29:15	14a1493c-9fd7-44dc-a698-fd43e65884c8	[redacted]	assistant	gpt-35-turbo	Azure のアプリロールを簡単に説明すると、アプリケーション内での各種操作や機能に対して、それぞれ異なる管理者権限やアクセス権限を定義するというものです。例えば、企業内の複数の部署が同じアプリケーションを使用する場合、営業部門のユーザーは顧客情報の閲覧や取引の確定など特定の機能にアクセスできるように定義された役割を持ち、経理部門のユーザーは請求書の発行や決算処理の権限を持つ役割を持つことができます。このように、アプリロールを使用することで、各々のユーザーに必要な操作権限のみ与えることができるため、セキュリティを確保し、情報漏洩や不正操作を防ぐことができます。	0	314
2023/08/09 2:29:05	14a1493c-9fd7-44dc-a698-fd43e65884c8	[redacted]	user		もっとわかりやすく説明してください。	420	0
2023/08/09 2:27:59	14a1493c-9fd7-44dc-a698-fd43e65884c8	[redacted]	assistant	gpt-35-turbo	Azure のアプリロールは、Azure AD (Azure Active Directory) の役割ベースのアクセス制御を実現するために使用される機能の一つです。アプリロールは、アプリケーションで実施するタスクに応じた特定の資格情報を持つユーザーのグループを定義します。アプリロールを使用すると、アプリケーション上で必要な操作に対応する役割を定義できます。例えば、営業部門にアプリケーション上で見積もりや受注を行うためのロールを設けたり、管理者用にすべての機能を含む特別なロールを作成することができます。Azure AD のアプリロールを使用することで、役割に割り当てられたユーザーは、決まった範囲内でのみアプリケーション上のアクションを実行できます。これは、セキュリティの強化にも繋がります。	0	327
2023/08/09 2:27:48	14a1493c-9fd7-44dc-a698-fd43e65884c8	[redacted]	user		Azure のアプリロールについて教えてください。	68	0
2023/07/26 2:13:36	6cb22b65-0f93-4fed-b7cf-eaddb147f69d	[redacted]	assistant	gpt-35-turbo	Microsoft AzureのOpenAI Serviceは、AI開発者が機械学習と人工知能のアプリケーションを開発、学習、展開するためのプラットフォームです。OpenAI Serviceは、自然言語処理、画像および音声認識、自動要約などのAI機能を提供し、多くの用途で使用されます。OpenAI Serviceを使用することで、開発者は、Azure Machine Learning、Jupyter ノートブック、TensorFlow、Keras、PyTorchなどの一般的なフレームワークやツールを使用して、AIモデルを開発、トレーニング、デプロイすることができます。OpenAI Serviceの機能には、自動機械学習、パイプライン処理、マネージドモデルサービス、リアルタイムサービス、バッチ推論などが含まれます。また、OpenAI Serviceには、Language Understanding (LUIS) や Text Analyticsなどのコグニティブサービスもあります。これらのサービスは、自然言語処理、感情分析、言語翻訳などの処理を容易にするために設計	0	623

Teams連携画面例

▼1対1チャット

Aiplicity-v2.0-test チャット 情報

18:09

世界で一番高い山は何ですか？

Aiplicity-v2.0-test 18:09

世界で一番高い山は、エベレスト (Mount Everest) です。エベレストはヒマラヤ山脈に位置し、ネパールと中国 (チベット自治区) の国境にまたがっています。エベレストの標高は8,848.86メートル (29,031.7フィート) あり、世界で最も標高の高い山として知られています。

18:09

2番目は何ですか？

Aiplicity-v2.0-test 18:09

2番目に高い山は、エベレストと同じヒマラヤ山脈に位置するK2 (カラコラム) です。K2の標高は8,611メートル (28,251フィート) で、世界で2番目に高い山です。K2はパキスタンと中国 (新疆ウイグル自治区) の国境付近に位置しており、登山家たちにとって非常に難易度の高い山として知られています。

▼チャンネル

AzureBot用チャンネル 投稿 ファイル Notes +

A0 18:27
Aiplicity-v2.0-test
世界で一番高い山は何ですか？

すべて折りたたむ

B 18:27
Aiplicity-v2.0-test
世界で一番高い山はエベレスト (マウントエベレスト) です。エベレストはヒマラヤ山脈に位置し、標高8,848メートル (29,029フィート) です。

A0 18:27
Aiplicity-v2.0-test
2番目は何ですか？

B 18:27
Aiplicity-v2.0-test
世界で2番目に高い山はK2 (カラコラム) です。K2はカラコラム山脈に位置し、標高8,611メートル (28,251フィート) です。

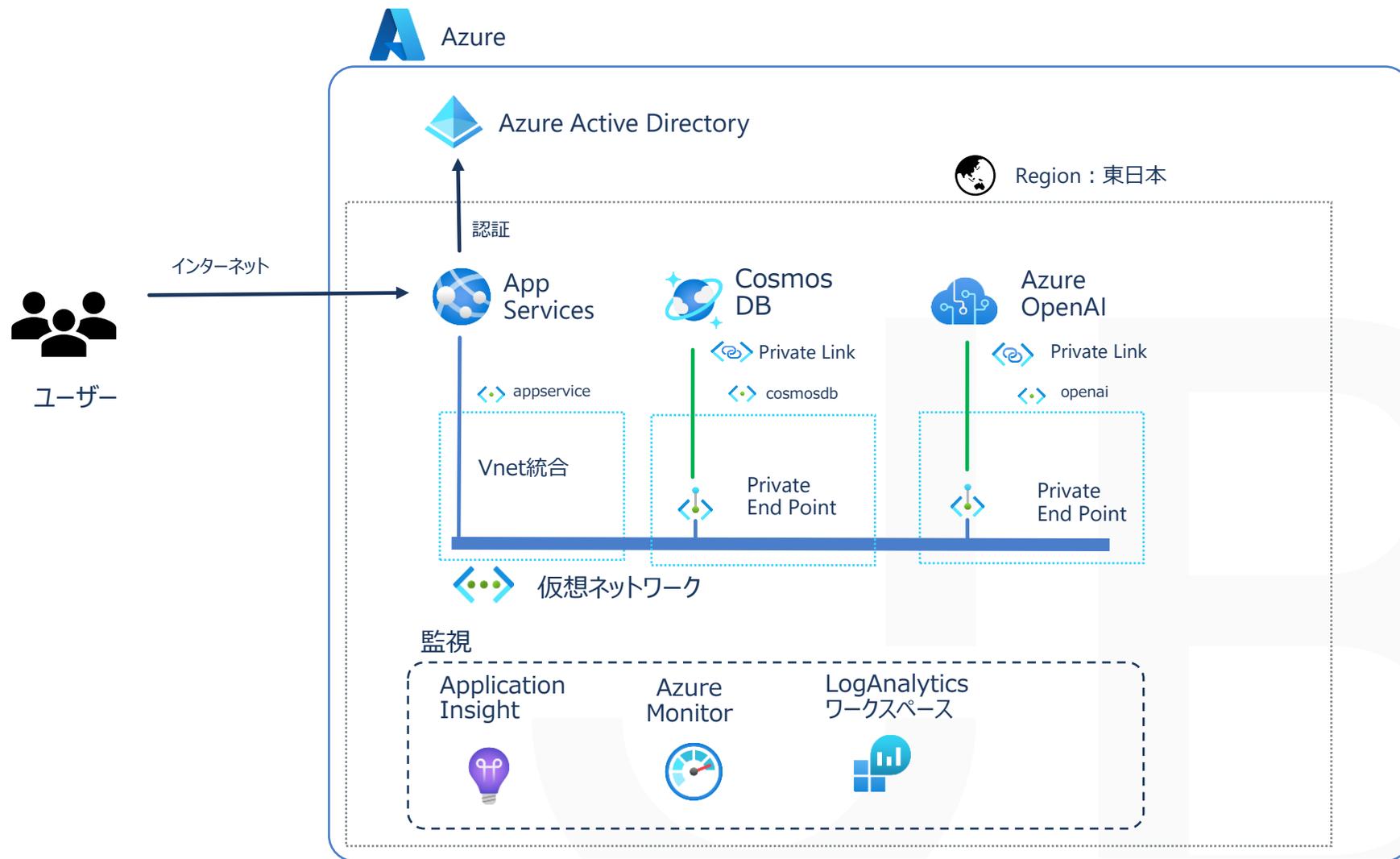
返信

A0 18:27
Aiplicity-v2.0-test
3番目は何ですか？

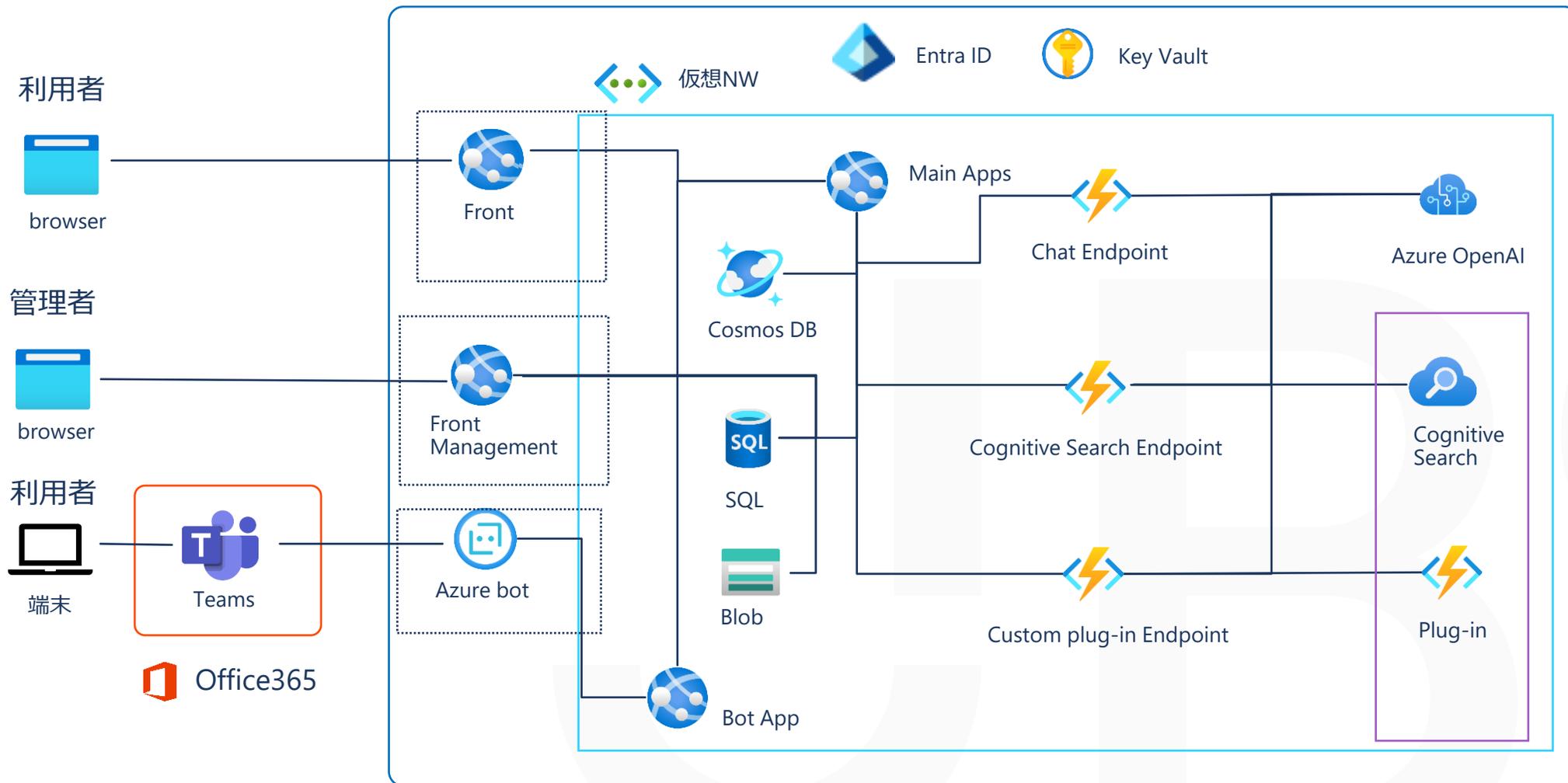
B 18:27
Aiplicity-v2.0-test
3番目は何か具体的な情報がないため、何を指しているのかわかりません。もし、3番目の何かを指しているのであれば、具体的な内容を教えていただければ、お答えすることができます。

アーキテクチャ

標準構成



拡張アーキテクチャ



デプロイ方法

デプロイ方法

ARMテンプレートを利用してデプロイします。



考慮事項

Azure Well-Architected Framework観点での考慮事項 - 1

- **信頼性(可用性)**

本アーキテクチャはミッションクリティカルな位置づけのシステムとしては想定していないため標準構成では冗長構成を採用していません。Azure App ServiceやAzure Cognitive Searchは、可用性ゾーンなどの機能を利用することで、さらにAzure Cosmos DBはGeoレプリケーションを使うことで可用性を高めることができます。

- **信頼性(回復性)**

アプリケーションの正常性はApplication Insightsを用いて監視しています。Azure Monitorでメトリックを監視し、必要な場合はアラートで管理者へ通知し対応します。また、Log Analytics ワークスペースでログを一元管理し、回復に必要なログを収集します。Azure Cosmos DBは標準でバックアップが取られているのでそのバックアップからデータを復元

Azure Well-Architected Framework観点での考慮事項 - 2

- **セキュリティ**

Azure Cosmos DBやAzure Storageの機能を使用して、データは暗号化されてAzure内に保存されます。

アプリケーションとお客様との通信はHTTPSで暗号化され、保護されています。閉域網からの接続やエクスプレスルートを利用しているお客様に対しては、Appendixのスライドで示す閉域網での接続を提供しています。また、閉域網を利用していないお客様に対しては、WAFの利用も可能です。

さらに、Microsoft EntraのIDを利用してアプリケーションの認証を行っています。

- **コスト最適化**

Azureのコスト管理機能により、サブスクリプションやリソースごとにコストの分析が可能です。Azure App ServiceやAzure Cosmos DBのメトリックを監視することで、適切なインスタンス数やRUを割り当て、コスト最適化を行います。

Azure Well-Architected Framework観点での考慮事項 - 3

- **オペレーショナルエクセレンス**

お客様のアプリケーションは、弊社の監視サービスにより監視とログの収集を行い、必要に応じてお客様にご連絡いたします。ソースコードは弊社のInternal GitHubで管理し、開発や改修はAzure DevOpsを使用してタスク管理を行っています。脆弱性が発見された場合は、弊社の保守サービスによりお客様のソフトウェアを更新いたします。

- **パフォーマンス効率**

Azure App ServiceやAzure Cognitive Searchは、負荷に応じてインスタンス数をスケールさせることが可能です。

また、Azure Cosmos DBでは、お客様の利用状況に合わせてRUを設定します。

さらに、GPT-4の利用可能な人数を管理者が制御できるようにし、TPMがオーバーしないように管理できます。

Appendix セキュリティ



インターネット

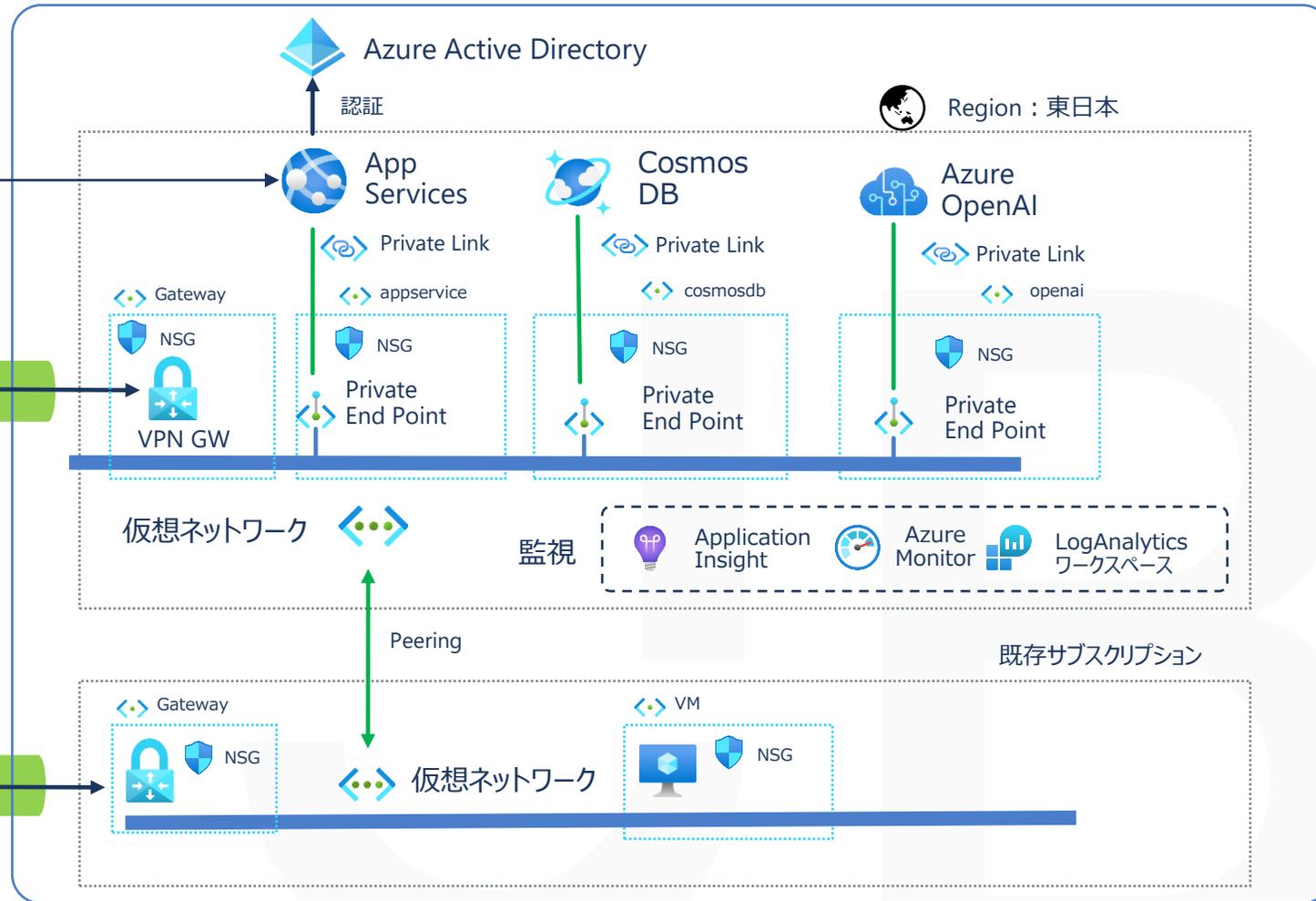


On-premises



VPN

VPN



Azure Active Directory

認証

Region : 東日本

App Services

Cosmos DB

Azure OpenAI

Private Link

Private Link

Private Link

Gateway

NSG

VPN GW

Private End Point

appservice

NSG

Private End Point

cosmosdb

NSG

Private End Point

openai

NSG

Private End Point

仮想ネットワーク

監視

Application Insight

Azure Monitor

LogAnalytics
ワークスペース

Peering

既存サブスクリプション

Gateway

NSG

仮想ネットワーク

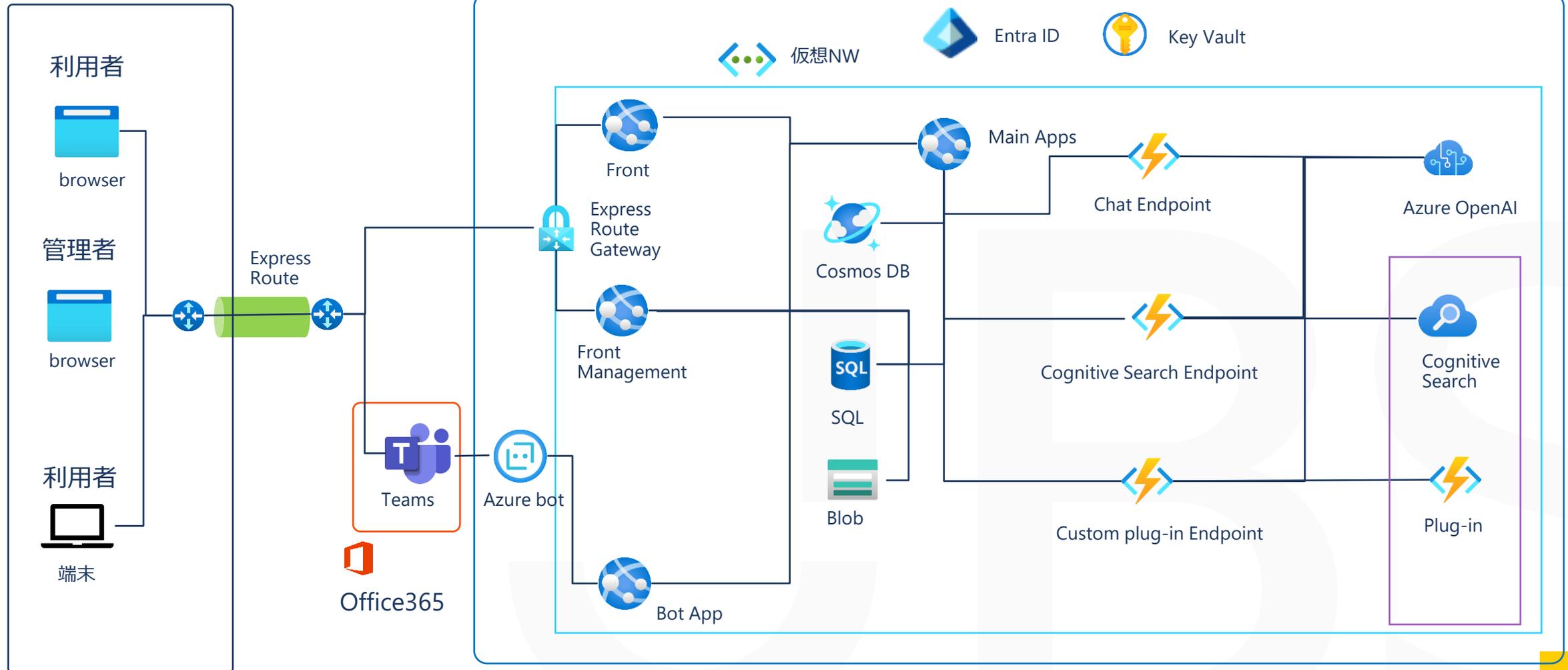
VM

NSG

Appendix セキュリティ (拡張構成)



On-premises





優れたテクノロジーを、親しみやすく