

HCCJP 第64回勉強会

ハイブリッドクラウド研究 会

2025年8月8日（金）14:00開始



本日のテーマ

BicepでMicrosoft Entra IDリソース & オンプレミスVM管理

- Bicep による Entra ID リソース管理
- Azure Arc によるオンプレミス VM 管理
- Microsoft Adaptive Cloud 最新動向

オープニング

司会：胡田 昌彦

日本ビジネスシステムズ株式会社
Microsoft MVP for Azure Hybrid,
Windows Server



自己紹介

胡田 昌彦（えびすだ まさひこ）

現在の活動

- YouTubeに注力中！ → <https://youtube.com/@ebibibi>

資格・認定

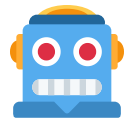
- Microsoft MVP for Azure Hybrid & Windows Server（ダブル受賞）
- Microsoft Certified Trainer

著書

- 「Windowsインフラ管理者入門」 著者

趣味

- ベース、ドラム、セッション、将棋



このスライドについて

生成AIで作成しました！

使用技術

- **Claude** - スライド内容の生成
- **Marp** - Markdownベースのプレゼンテーション
- **VS Code** - 統合開発環境

先月分の内容をもとに「今月分作っておいて！」って頼むだけでバッチリ作ってくれてビビってます。

タイムテーブル

時刻	時間	セッション	スピーカー
14:00	5分	オープニング	胡田 昌彦
14:05	40分	BicepでMicrosoft Entra IDリソース&オンプレミスVM管理	胡田 昌彦
14:45	10分	Q&A	全員
14:55	20分	Microsoft "Adaptive Cloud" Updates	高添 修 氏
15:15	10分	Q&A	全員
15:25	5分	クロージング	胡田 昌彦

HCCJPとは

ハイブリッドクラウド研究会

- 毎月第2金曜日 14時から開催
- Azure + ハイブリッドクラウド関連の最新情報をお届け
- オンライン配信（YouTube HCCJPチャンネル）

📺チャンネル登録お願いします！

<https://www.youtube.com/channel/UCrf4bEI7yJnkGYo3F67gA7w>



本日の注意事項

- 📺 配信は録画されています→アーカイブでもいつでも見られます！
- 💬 YouTubeチャットでの質問・コメント大歓迎！
- 📝 Q&Aセッションでお答えします！

質問・コメント方法

 YouTubeチャットで質問・コメント大歓迎！

新しい質問受付方法

- YouTubeライブチャットを使用
- リアルタイムでコメント・質問可能
- セッション中いつでもお気軽に投稿

チャットの使い方

- YouTube画面右側のチャット欄を使用
- セッション中でも遠慮なく投稿してください

Q&Aタイムについて

- 各セッション後にQ&Aタイムを設けています
- チャットの質問を順次お答えします

今日から新方式！YouTubeチャットでお気軽に参加ください！

セッション①

BicepでMicrosoft Entra IDリソース & オンプレミスVM管理

スピーカー：胡田 昌彦

日本ビジネスシステムズ株式会社

Microsoft MVP for Azure Hybrid, Windows Server

 14:05 - 14:45 (40分)

セッション①について

本セッションのポイント

- Bicep によるEntra IDリソース管理の実演
- Azure Arc によるオンプレミスVM管理の実演
- 実際のコード例とデモンストレーション

実際にお見せして理解いただきます！

Bicepとは？ Infrastructure as Codeの実現

Bicepの基本概念

- **Azure Resource Manager (ARM)** テンプレートの代替言語
- **宣言的な構文**でインフラを定義（何を作るか記述、どう作るかはAzureが判断）
- **JSONより簡潔**で読みやすく、書きやすい

これまでのBicep活用範囲

```
// 従来：Azureリソース（VM、ストレージ、ネットワーク等）の管理
resource storageAccount 'Microsoft.Storage/storageAccounts@2023-05-01' = {
  name: 'mystorageaccount'
  location: 'japaneast'
}
```

2025年7月～ 新たな展開

- **Microsoft Graph Bicep拡張**が一般提供開始
- **Entra IDリソース**もBicepで管理可能に！
- **統一されたIaC**でAzureとEntra IDを一元管理

🎯 なぜ今、BicepでEntra IDなのか？

⚠️ ID管理の現状と課題

- 手動でのグループ作成・権限設定 → ヒューマンエラーの温床
- 設定の属人化 → 担当者不在時に困る
- 環境間の設定差異 → 開発・本番で設定が異なる
- 監査証跡の不足 → 誰がいつ何を変更したか不明

✅ Bicepによる解決

- コードによる管理 → レビュー可能、ミス削減
- Git管理 → 変更履歴、ロールバック可能
- CI/CDパイプライン → 自動デプロイ、環境間の一貫性
- 宣言的な記述 → あるべき状態を定義

🎯 本日のゴール

「Entra IDもAzureリソースもコードで管理」する時代へ！

Microsoft Graph Bicepで管理可能なリソース

 現在サポートされているEntra IDリソース (v1.0)

作成・更新・削除が可能

-  **Applications** - アプリケーション登録の管理
-  **Groups** - セキュリティグループ・Microsoft 365グループの作成
-  **Service Principals** - サービスプリンシパルの管理
-  **Federated Identity Credentials** - フェデレーション認証の設定
-  **App Role Assignments** - アプリロールの割り当て
-  **OAuth2 Permission Grants** - OAuth2権限の付与

読み取り専用

-  **Users** - 既存ユーザーの参照 (`existing` キーワード使用)

主な活用シナリオ

- 自動化されたアプリ登録 - CI/CDパイプラインでの自動デプロイ
- グループ管理の標準化 - 一貫性のあるグループ構成
- 権限管理の自動化 - アプリケーションへの権限付与

BicepでEntra ID管理 :

今回のデモで扱う内容

- グループの作成・管理
- グループオーナーの設定
- グループメンバーの管理
- サービスプリンシパルの作成
- アプリケーション登録
- Web Appsとの認証統合
- 既存ユーザーの参照（読み取り専用）

現在の制限事項（2025年8月時点）

✗ まだできないこと

- What-If
- ユーザーアカウントの作成（読み取り専用のみサポート）
- 条件付きアクセスポリシー（機能リクエスト中）
- アプリケーションパスワードの作成（証明書のみサポート）
- ロール割り当て可能グループ（デプロイ時にエラーが発生）

回避策

- DeploymentScript リソースでMicrosoft Graph APIを直接呼び出し
- Azure PowerShell/CLI による補完的な処理

情報源

- Microsoft Learn: [Microsoft Graph Bicep Limitations](#)
- GitHub: [Azure/bicep Issues #13734](#)

今日のデモ構成

Demo 1-5: Entra ID リソース管理

- **demo1**: グループ作成の基本
- **demo2**: マネージドIDをグループオーナーに設定
- **demo3**: ユーザーをグループメンバーに追加
- **demo4**: サービスプリンシパルによる自動化
- **demo5**: Web Apps + Entra ID認証統合

Demo 6: Azure Arc VM管理

- **demo6**: オンプレミスVMの構成管理

実際のコードを見ながら解説していきます！

ソースコード:

https://github.com/ebibibi/presentations/tree/main/HCCJP_64_Bicep_Entra



Demo 1: グループ作成の基本



Demo 2: マネージドIDをオーナーに設定



Demo 3: ユーザーをメンバー に追加



Demo 4: サービスプリンシパ ルで自動化



Demo 5: Web Apps + Entra ID 認証



Demo 6: Azure Arc VM管理

プロジェクト構成

ファイル構成の説明

```
HCCJP_64_Bicep_EntraID_Arc/  
├── slides.md          # 本日のプレゼンスライド  
├── Demos/  
│   ├── demo1_グループ作成/  
│   │   ├── main.bicep      # グループ作成のメインコード  
│   │   ├── deploy.ps1     # デプロイスクリプト  
│   │   └── bicepconfig.json # Bicep設定ファイル  
│   ├── demo2_グループ所有者にマネージドIDを設定/  
│   ├── demo3_グループメンバーにユーザーを設定/  
│   ├── demo4_サービスプリンシパルを使って自動化/  
│   ├── demo5_WebAppsとEntraID認証/  
│   └── demo6_ArcVM構成/
```

各デモは独立して実行可能です！

デプロイの基本手順

PowerShellスクリプトによる自動デプロイ

各デモ共通の手順

```
# リソースグループの作成とデプロイ  
./deploy.ps1
```

スクリプトの内容例

```
# リソースグループ名とロケーションの設定  
$resourceGroupName = "hccjp-demo1"  
$location = "japaneast"  
  
# リソースグループの作成  
az group create --name $resourceGroupName --location $location  
  
# Bicep テンプレートのデプロイ  
az deployment group create `   
    --resource-group $resourceGroupName `   
    --template-file ".\main.bicep"
```

ワンクリックでInfrastructure as Codeが実現！



**デモ作成中に気が付いた注意
点！**

⚠ 実装時のハマりポイント

🔧 bicepconfig.jsonの配置場所

- VS Codeで開いているフォルダのルートに配置する必要あり
- サブディレクトリに置いても認識されない
- 各デモディレクトリに個別配置が必要(だと思う)
- VS CodeのBicep拡張は挙動が不安定で結果が一意でないように思う。

🔄 グループのowner設定は2回実行が必要

- ManagedIDをグループオーナーに設定する場合
- 1回目のデプロイでは失敗することが多い
- 2回目で成功するパターン
- `dependsOn` を設定しても同様
- Microsoft公式ドキュメントにも記載されている既知の問題

⚠ 削除とトラブルシューティング

🗑 リソース削除の注意点

- リソースグループ削除だけでは不十分
- Entra IDリソース（グループ、アプリ等）は別途削除が必要

🐛 Azure CLI のバグ対応

よく遭遇するエラー

```
The content for this response was already consumed
```

解決方法

- Azure CLI のバグが原因
- Azure PowerShell を使用することで回避可能
- Bicepの展開時エラー時にこのメッセージが表示される模様



今日学んだこと

セッションのまとめ

Bicep × Entra ID

- Infrastructure as CodeでIDリソース管理
- グループ・アプリケーションの自動化
- Web Apps認証との統合

Bicep × Azure Arc

- オンプレミスVMのクラウド管理
- 拡張機能の自動デプロイ
- リモート実行による構成管理

次のステップ

より深く学習するために

Microsoft 公式学習リソース

Bicep 関連

- Bicep 基礎学習パス: <https://learn.microsoft.com/ja-jp/training/paths/fundamentals-bicep/>
- Bicep 上級学習パス: <https://learn.microsoft.com/ja-jp/training/paths/advanced-bicep/>
- Bicep 公式ドキュメント: <https://learn.microsoft.com/ja-jp/azure/azure-resource-manager/bicep/>
- Microsoft Graph Bicep: <https://learn.microsoft.com/ja-jp/graph/templates/bicep/>

Azure Arc 関連


- Azure Arc 概要: <https://learn.microsoft.com/ja-jp/azure/azure-arc/overview>
- Azure Arc 入門モジュール: <https://learn.microsoft.com/ja-jp/training/modules/intro-to-azure-arc/>
- Azure Arc サーバー管理: <https://learn.microsoft.com/ja-jp/training/paths/deploy-manage-azure-arc-enabled-servers/>
- Azure Arc サーバー公式ドキュメント: <https://learn.microsoft.com/ja-jp/azure/azure-arc/servers/overview>

ありがとうございました！

質問をお待ちしています！

Q&Aセッション

 YouTubeチャットからの質問にお答え
します！

- YouTubeライブチャットでの質問にお答え
-  質問、 コメント 区別して投稿歓迎
- どんな質問でもOK！

 14:45 - 14:55 (10分)

セッション②



Microsoft "Adaptive Cloud" Updates

スピーカー：高添 修 氏
日本マイクロソフト株式会社

 14:55 - 15:15 (20分)

Q&Aセッション

YouTubeチャットからの質問にお答え します！

- YouTubeライブチャットでの質問にお答え
-  質問、 コメント 区別して投稿歓迎
- どんな質問でもOK！

 15:15 - 15:25 (10分)

次回予告



次回は9月12日（金） 14:00～

毎月第2金曜日に開催！

YouTubeチャンネル登録をお忘れなく！

<https://www.youtube.com/channel/UCrf4bEI7yJnkGYo3F67gA7w>



ご参加ありがとうございました！

また来月お会いしましょう！

 本日の資料は後日公開予定

 お問い合わせは ebibibi@gmail.com まで

#HCCJP でツイートお願いします！