

# Azure SQL Database Managed Instance ホワイトペーパー

## 著作権情報

このドキュメントに記載されている情報は、このドキュメントの発行時点におけるマイクロソフトの見解を反映したものです。変化する市場状況に対応する必要があるため、このドキュメントは、記載された内容の実現に関するマイクロソフトの確約とはみなされないものとします。また、発行以降に発表される情報の正確性に関して、マイクロソフトはいかなる保証もいたしません。

このドキュメントは情報提供のみを目的としており、明示、黙示、または法律上の保証に関わらず、これらの情報についてマイクロソフトはいかなる責任も負わないものとします。

お客様ご自身の責任において、適用されるすべての著作権関連法規に従ったご使用を願います。このドキュメントのいかなる部分も、米国 Microsoft Corporation の書面による許諾を受けることなく、その目的を問わず、どのような形態であっても、複製または譲渡することは禁じられています。ここでいう形態とは、複写や記録など、電子的な、または物理的なすべての手段を含みます。

ただしこれは、著作権法上のお客様の権利を制限するものではありません。マイクロソフトは、このドキュメントに記載されている内容に関し、特許、特許申請、商標、著作権、またはその他の無体財産権を有する場合があります。別途マイクロソフトのライセンス契約上に明示の規定のない限り、このドキュメントはこれらの特許、商標、著作権、またはその他の知的財産に関する権利をお客様に許諾するものではありません。

© 2018 Microsoft Corporation. All rights reserved.

Microsoft、Active Directory、AZURE、EXPRESSROUTE、HDInsight、Hyper-V、Internet Explorer、Microsoft Dynamics、MSDN、MSN、Office 365、Outlook、SQL Server、STORESIMPLE、Visual Studio、Windows、Windows PowerShell、および Windows Server は、米国 Microsoft Corporation の米国またはその他の国における登録商標または商標です。

このドキュメントに記載されている会社名、製品名には、各社の商標のものもあります。

# 目次

目次.....	2
1 はじめに.....	4
2 Azure SQL Database Managed Instance の概要.....	5
2.1 Azure SQL Database Managed Instance とは.....	5
2.2 Azure SQL Database Managed Instance サポートされる機能.....	8
2.3 SQL Server Managed Instance の基本構成.....	10
2.3.1 Managed Instance の作成方法.....	13
2.3.2 Managed Instance の管理と注意点.....	16
3 Azure SQL Database Managed Instance の機能検証.....	19
3.1 リンクサーバ.....	19
3.1.1 リンクサーバ設定方法 (SQL Database へ接続).....	20
3.2 COPY_ONLY による手動バックアップ.....	22
3.2.1 BLOB ストレージの資格証明の登録.....	22
3.2.2 COPY_ONLY バックアップの取得.....	23
3.3 Azure SQL Database Managed Instance の監査.....	24
3.3.1 Azure SQL Database Managed Instance のサーバレベル監査設定方法.....	25
3.3.2 監査イベントの SQL による確認.....	26
3.4 データベース跨ぎのトランザクション.....	27
3.5 BULK INSERT によるファイルインポート.....	28
3.5.1 データベースマスターキーおよび、データベーススコープベースの資格情報の作成.....	28
3.5.2 外部データソースを登録.....	28
3.5.3 BULK INSERT の実行.....	29
4 Azure SQL Database Managed Instance への移行手順.....	31
4.1 SQL Server ネイティブバックアップを使用した移行.....	31
4.1.1 SQL Server からのバックアップ取得.....	32
4.1.2 Managed Instance での SHARED ACCESS SIGNATURE (SAS) の設定.....	33
4.1.3 Azure SQL Database Managed Instance にてデータベースをリストア.....	33
4.2 BACPAC を使用した移行.....	34
4.2.1 SQL Server からユーザデータベース「AdventureWorks2017」の BACPAC を取得.....	35
4.2.2 SSMS を利用して取得した BACPAC から Managed Instance へインポート.....	38
4.3 Azure Data Migration Service を使用した移行.....	41
4.3.1 Azure Data Migration Service の作成.....	42
4.3.2 新しい移行プロジェクトの作成.....	42
4.3.3 新しい移行アクティビティを作成.....	47
4.3.4 移行状況の確認.....	53
4.4 Data Migration Assistant を利用した互換性調査.....	55

4.4.1	Managed Instance で利用可能な互換性レベル .....	55
4.4.2	Data Migration Assistant の起動 .....	56
4.4.3	Data Migration Assistant を使った互換性調査.....	56
4.4.4	アセスメント結果の確認.....	61
5	最後に.....	62
6	参考 .....	63

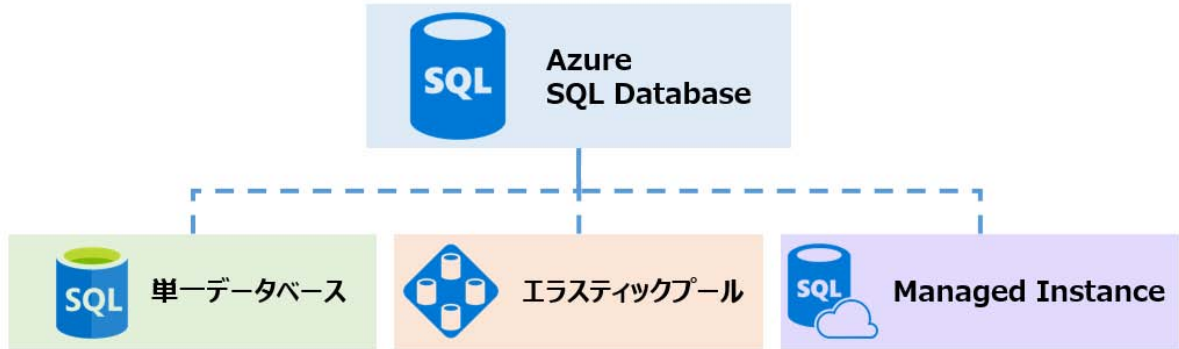
# 1 はじめに

2018年5月、Azure SQL Database に新しい機能、「Azure SQL Database Managed Instance (以下、Managed Instance)」がリリースされた。この機能により Azure SQL Database (以下、SQL Database) は仮想ネットワーク (以下、VNet) に対応できるようになり、また、ほぼすべての SQL Server の機能が SQL Database でも提供されることになる。PaaS の特性 (修正プログラムの管理、自動バックアップ、高可用性構成) も損なわれないため、オンプレミスにある既存の SQL Server をクラウドへ移行する際の選択肢として最善の移行先となるであろう。本ホワイトペーパーは、この Managed Instance の概要や移行方法、移行時の注意点などを記載し、オンプレミスの SQL Server のユーザの Managed Instance への移行や、Managed Instance の活用の一助となることを目的としている。

## 2 Azure SQL Database Managed Instance の概要

### 2.1 Azure SQL Database Managed Instance とは

#### SQL Databaseの種類



Azure SQL Database Managed Instance（以下、Managed Instance）は、Azure SQL Database（以下、SQL Database）の新しい機能として位置付けられる。これまでの SQL Database に比べ、オンプレミスの SQL Server との互換性がより高くなっており、Azure 環境への容易なリフト&シフトを可能とする。また、フルマネージドである PaaS としての特徴も備えており、多くの PaaS のメリットを享受することができる。セキュリティ面では、VNet に対応しており、プライベート IP アドレスで接続を行う。これによりネットワーク的に完全に分離されたセキュリティを確保することができる。

現在 Azure 上で SQL Server を稼働させる方法は、Azure VM 上で SQL Server を稼働させる「SQL Server on Azure VM」、これまで提供されていた SQL Server の PaaS サービス「SQL Database」、今回新しく SQL Database の機能としてリリースされた「Managed Instance」が存在する。各環境の管理範囲と特徴を以下に示す。

	SQL Server on Azure VM	Managed Instance	SQL Database
	データベース	データベース	データベース
	SQL Server	SQL Server	SQL Server
	可用性	可用性	可用性
	ゲストOS	ゲストOS	ゲストOS
	仮想化	仮想化	仮想化
	ホストOS	ホストOS	ホストOS

利用者の管理範囲 (オレンジ色)

Azureの管理範囲 (青色)

Managed Instance では 2 種類のサービス階層および 2 種類のコンピューティング世代が選択可能となる。2 種類のサービス階層では、さまざまなワークロードに汎用的に利用可能なサービス階層である「汎用目的」、I/O および障害時の復旧の要件が厳しいアプリケーションに最適なサービス階層である「ビジネスクリティカル」が存在する。これらのサービス階層ではそれぞれの利用目的に合わせてストレージや可用性にて異なる特徴を持っている。汎用目的のサービス階層ではリモートストレージベースなのに対して、ビジネスクリティカルのサービス階層では高速なローカル SSD ベースで実装されている。可用性の面では、汎用目的ではリモートストレージベースでの 3 レプリカ構成（同一リージョン内に 1 つのマスター DB と 2 つのレプリカを持つ）であるのに対して、ビジネスクリティカルでは Always On AG ベースでの 3 レプリカ構成となる。このため、汎用目的では障害発生時リカバリまで数秒かかるのに対して、ビジネスクリティカルでは数ミリ秒でのリカバリが可能である。導入するシステムの特性に合わせてそれぞれのサービス階層を選定することが望ましい。（2018 年 6 月プレビュー時点では、サービス階層は「汎用目的」のみ利用可能）

機能/サービス階層	汎用目的	ビジネスクリティカル
主な用途	可用性やI/O待ち時間の許容範囲が広いアプリケーション	高可用性・低I/Oが求められるアプリケーション
VCPU	8,16,24 (32,40は2018年Q2にリリース予定)	8,16,24 (32,40は2018年Q2にリリース予定)
HA/RTO	リモートストレージベース/数秒	Always On Agベース/数ミリ秒
ストレージタイプ/サイズ	リモートストレージ(Azure Premium)/最大8TB	高速ローカルSSD/最大4TB
スケールアウト(読み取り専用)	不可	可
インメモリでのオンライントランザクション処理	不可	可
Azureハイブリッドコアライセンス: Vcore (EE/SE)	1:4/1:1	1:1/N/A

コンピューティング世代は Gen4、Gen5 が用意されている。いずれも SQL Server 2017 ベースのエンジンを利用できるようになっており機能に対する差はない。導入するハードウェア要件に合わせ、選定することが望ましい。（2018 年 6 月時点では、Gen5 は東日本リージョンでは利用できない）

	Gen4	Gen5
ハードウェア	Intel E5-2673 v3(Haswell) 2.4 GHz processors attached SSD vCore=1 PP (physical core)	Intel E5-2673 v4(Broadwell) 2.3 GHz processors fast eNVM SSD vCore=1 LP(hyper-thread)
CPUコア	8,16,24 vCores	8,16,24,32,40 vCores
メモリ	7GB/1Core	5.5GB/1Core

また、ソフトウェアアシュアランス (SA) 付きのライセンスを保有しているユーザは、SQL Server のライセンスの利用により Managed Instance のコストを節約ができる「Azure ハイブリッド特典」を利用可能である。

- Standard ライセンス

1 コアにつき、汎用目的の 1 仮想コアを利用可能。

- Enterprise ライセンス

1 コアにつき、汎用目的の 4 仮想コア/ビジネスクリティカルの 1 仮想コアを利用可能。

「Azure ハイブリッド特典」の詳細に関しては以下の URL を参照のこと。

<https://azure.microsoft.com/ja-jp/pricing/hybrid-benefit/>



## 2.2 Azure SQL Database Managed Instance サポートされる機能

Managed Instance でサポートされている機能は以下の URL を参照のこと。

- 機能の比較: Azure SQL Database と SQL Server  
<https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-features>
- Azure SQL Database マネージ インスタンスと SQL Server の T-SQL の相違点  
<https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-managed-instance-transact-sql-information>

本章では上記 URL より一部を主要なポイントとして抜粋し、SQL Server、SQL Database および Managed Instance の機能に関して比較を記す。

機能	SQL Server	SQL Database	Managed Instance
可用性	可用性環境の構築必要	自動的に構築される	自動的に構築される
バージョンアップ	手動でバージョンアップ	自動的にバージョンアップ	自動的にバージョンアップ
DB あたりの最大サイズ	OSの最大容量	4 TB	8 TB
定期的な自動バックアップ	手動で設定	自動的にバックアップが取得される	自動的にバックアップが取得される
ネイティブバックアップ	可能	不可能	可能 (COPY_ONLY による完全バックアップ)
ネイティブバックアップによるリストア	可能	不可能	可能
BACPAC のインポート / エクスポート	可能	可能	可能
自動チューニング	プランの自動強制 (2017 から)	プランの自動強制 インデックスの自動チューニング	プランの自動強制
リストアインデックス	可能	Premium レベル、Standard レベル、S3 以上、General Purpose レベル、および Business Critical レベル	可能
複数のデータベース間のクエリ	可能	なし (エラスティッククエリで一部可能)	可能
データベースをまたがるトランザクション	可能	なし (エラスティックトランザクションで一部可能)	可能
ファイルグループの利用	可能	なし	可能
Geo リストア	なし	可能	なし
Geo レプリケーション	なし	可能	なし
リンク サーバー	さまざまなデータ ソース	不可能	SQL Server and SQL Databaseのみ
監査	サーバー レベル	データベース レベル	サーバー レベル
SQL Server Agent	可能	なし	可能
Azure VNET 利用	可能	なし (サービスエンドポイントで経由接続)	可能
データベースの互換性レベル	SQL Server のバージョンに依存	100 / 110 / 120 / 130 / 140	100 / 110 / 120 / 130 / 140
サーバーレベルの照合順序	インストール時に指定可能	DB 作成時のみ指定可能	SQL_Latin1_General_CP1_CI_AS 固定
日付関数のタイムゾーン	OS の設定に依存	UTC タイムゾーン 固定	UTC タイムゾーン 固定

以下、Managed Instance で利用できない機能に関して、代わりとなる方式を考察する。

- SQL Server Integration Services (SSIS)  
 Managed Instance では SSIS をインストールして利用できない。このため、SQL Server のアプリケーションとして SSIS を利用している場合は、Azure Data Factory でその機能を置き換えるような方式を検討する。特に、より簡単に SSIS のパッケージをマネージドの環境にリフトするには Azure Data Factory version2 (以下、ADF v2) を利用することが望ましいと考えられる。SSIS を ADF v2 へ移行することにより SSIS のプログラムと実行環境に対して、低い TCO と可用性、拡張性を得ることが可能である。

- **SQL Server Analysis Services**

移行対象となる SQL Server 上に OLAP モデルなどを構築するため、SQL Server Analysis Services を利用している場合、Managed Instance へ移行するタイミングで、OLAP モデルを Azure Analysis Services への移行を検討する。ただし、Azure Analysis Services は 2018 年 6 月現在で、OLAP モデルとして表形式のみしかサポートされておらず、多次元モデルやマイニングの移行先としては対応する Azure サービスが存在しない為、注意が必要である。

- **SQL Server Reporting Services (SSRS)**

SQL Server Reporting Services を利用している SQL Server を Managed Instance で移行する場合には、SSRS の代わりに Power BI によって機能を置き換えられないかを検討する。

上記のように SSIS、SSAS、SSRS ともに変わりとなるようなサービスが Azure 上には展開されているため、第一にこれらの利用ができないか確認することが望ましいと考える。しかしながら利用の検討の結果、代替案が受け入れられない場合には、Azure 上に上記のサービスを利用するための SQL Server on VM を起動し利用することは可能である。

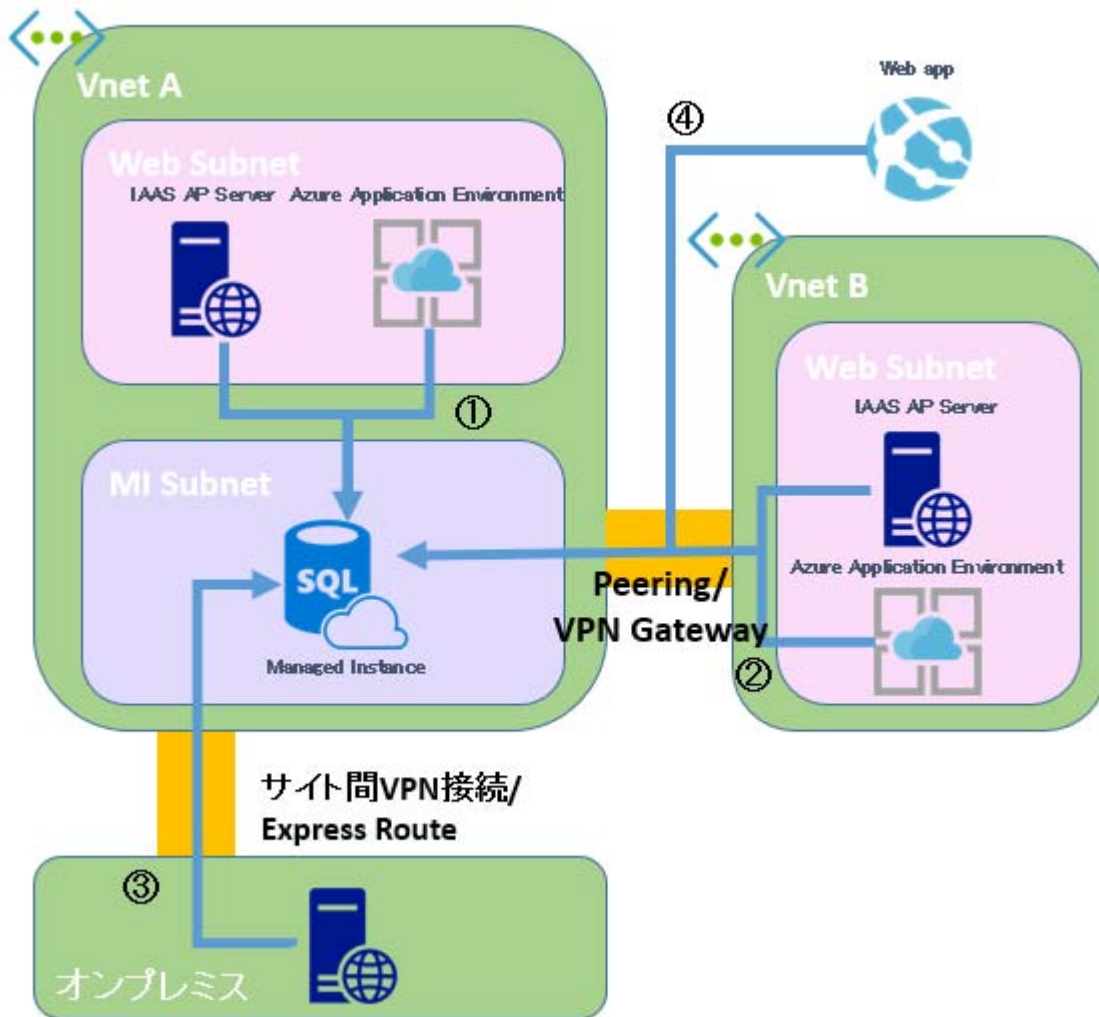
## 2.3 SQL Server Managed Instance の基本構成

Managed Instance は VNet 上に起動させる必要がある。VNet 上に起動させることによりネットワーク的に完全に分離された環境を実現する。これまであった SQL Database とは異なりパブリック IP を付与することはできず、アプリケーションは基本的に Managed Instance が有するプライベート IP に接続を行うことになり、インターネットから直接 Managed Instance へ接続を行う事が出来ない。このため、Managed Instance へ接続を行うアプリケーションについては、Managed Instance が起動している VNet へアクセスする必要がある。Managed Instance を起動する場合には VNet 上に Managed Instance 専用のサブネットを作成する必要がある。Managed Instance を配置する VNet 上のサブネットの要件と、アプリケーションと Managed Instance が起動している VNet の接続方法を以下に記す。

### Managed Instance を起動するサブネットの要件

- サブネットは /24～ /28 を使用
- 最大で 256 個の IP が使用される可能性がある
- サブネットは MI 専用にする（複数の MI を同一のサブネットに配置は可能）
- MI のサブネットには「0.0.0.0/0」の次ホップを「Internet」にするルートテーブルを設定
- MI のサブネットは、サービスエンドポイントを無効の状態にする
- MI のサブネットは、ネットワークセキュリティグループ (NSG) を設定しない

## アプリケーションと Managed Instance が起動している VNet の接続方法



- 同じ VNet 内のアプリケーション接続 (①)  
同じ VNet 内の仮想マシンは、異なるサブネット内にあっても、直接相互接続が可能である。このため、Managed Instance に必要な接続文字列を設定することで、接続を完了することが可能である。一方で接続が確立できない場合には、サブネット上のネットワークセキュリティグループの設定を確認することが望ましい。設定されているネットワークセキュリティグループでは、SQL のポート 1433 と、リダイレクト用のポート範囲 11000-12000 で、アウトバウンド接続を開く必要がある。
- 異なる VNet 内のアプリケーション接続 (②)  
Managed Instance が起動している VNet と異なる VNet 上のアプリケーション間で接続を行う場合、Managed Instance が起動している VNet に対して、アプリケーションがアクセスできるようにする必要がある。VNet 間で通信を行う場合には以下の 2 つの方法が存在する。
  - VNet Peering
  - VPN GatewayVNet Peering では Azure 内のバックボーン ネットワークが使用されるため、同一 VNet 内の仮想マシンとの接続同様、VNet Peering 経由の仮想マシンであっても接続や通信に遅延が発生

することはない。異なるリージョン間のネットワーク接続（Global VNet Peering）の制約により MI に接続することができない、同じリージョン内のネットワークに制限される。

- オンプレミス アプリケーションを接続（③）

Managed Instance は、プライベート IP アドレスを介してのみアクセスが可能である。このため、オンプレミスのマシンからアクセスを行う場合には、アプリケーションと Managed Instance の VNet にサイト間接続を確立する必要がある。オンプレミスと Azure VNet 間のサイト間接続では以下の 2 つの方法が存在する。

- サイト間 VPN 接続(Point to Site・Site to Site での接続可)
- ExpressRoute 接続

- VNet 対応していないサービスを接続（④）

Managed Instance は、プライベート IP アドレスを介してのみアクセスが可能である。PaaS サービスなどからアクセスするには、VNet 統合・統合ランタイムなどを利用し Managed Instance との接続を確立する必要がある。

## 2.3.1 Managed Instance の作成方法

本章では Azure Portal より Managed Instance を作成する方法を記載する。

### 2.3.1.1 VNet の作成

Azure Portal より「仮想ネットワーク」を選択し「追加」を押下、仮想ネットワーク作成画面にて、P9.「Managed Instance を起動するサブネットの要件」で記載した要件に沿った Vnet を作成する。

The screenshot shows the 'Create Virtual Network' form in the Azure Portal. The form is titled '仮想ネットワークの作成' (Create Virtual Network). It contains several fields and options, with red boxes highlighting specific areas and callout boxes providing instructions:

- Name:** 'Azure-Vnet' is entered in the '名前' (Name) field. Callout: 'Managed Instance用のサブネットの名称を入力' (Enter the name of the subnet for Managed Instance).
- Address Space:** '10.3.0.0/16' is entered in the 'アドレス空間' (Address Space) field.
- Subscription:** 'Microsoft Azure Sponsorship' is selected in the 'サブスクリプション' (Subscription) dropdown.
- Resource Group:** 'Azure-EastAsia-rg' is selected in the 'リソースグループ' (Resource Group) dropdown.
- Location:** '東アジア' (East Asia) is selected in the '場所' (Location) dropdown. Callout: 'リージョンを選択。2018年6月現在、日本で選択可能なリージョンは東日本リージョンのみ。' (Select a region. As of June 2018, the only region available for selection in Japan is the East Japan region).
- Subnet Name:** 'MI-Subnet' is entered in the '名前' (Name) field under the 'サブネット' (Subnet) section. Callout: 'Managed Instanceのサブネット名称。' (Managed Instance subnet name).
- Subnet Address Range:** '10.3.0.0/24' is entered in the 'アドレス範囲' (Address Range) field. Callout: 'サブネットは/24~/28を使用。' (Subnets use /24~/28).
- DDoS Protection:** 'Basic' is selected in the 'DDoS Protection' section.
- Service Endpoints:** '無効' (Disabled) is selected in the 'サービスエンドポイント' (Service Endpoints) section.
- Buttons:** '作成' (Create) and 'Automation オプション' (Automation Options) are at the bottom.

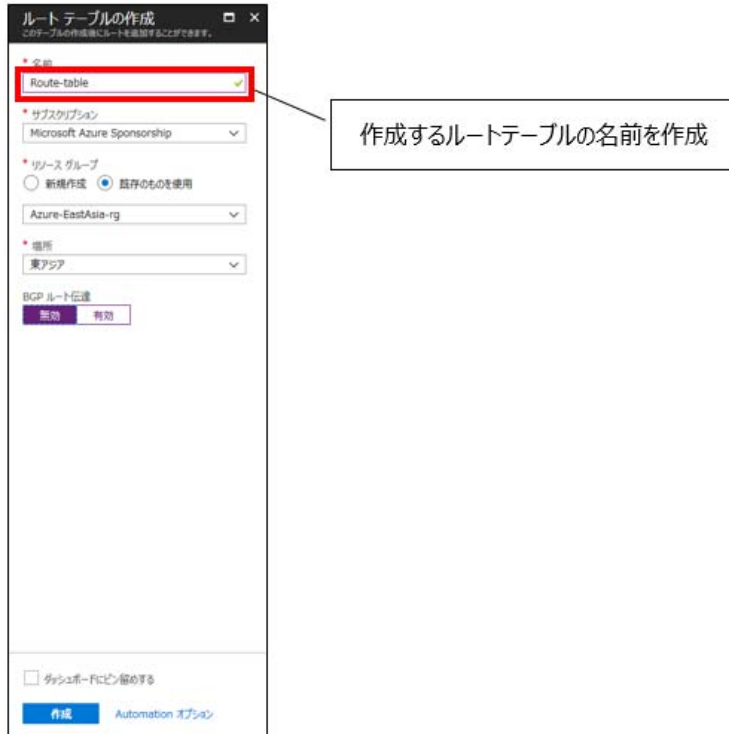
作成されたサブネットを確認する。

+ サブネット		+ ゲートウェイサブネット	
サブネットの検索			
名前	アドレス範囲	使用可能なアドレス	セキュリティグループ
MI-Subnet	10.3.0.0/24	251	-

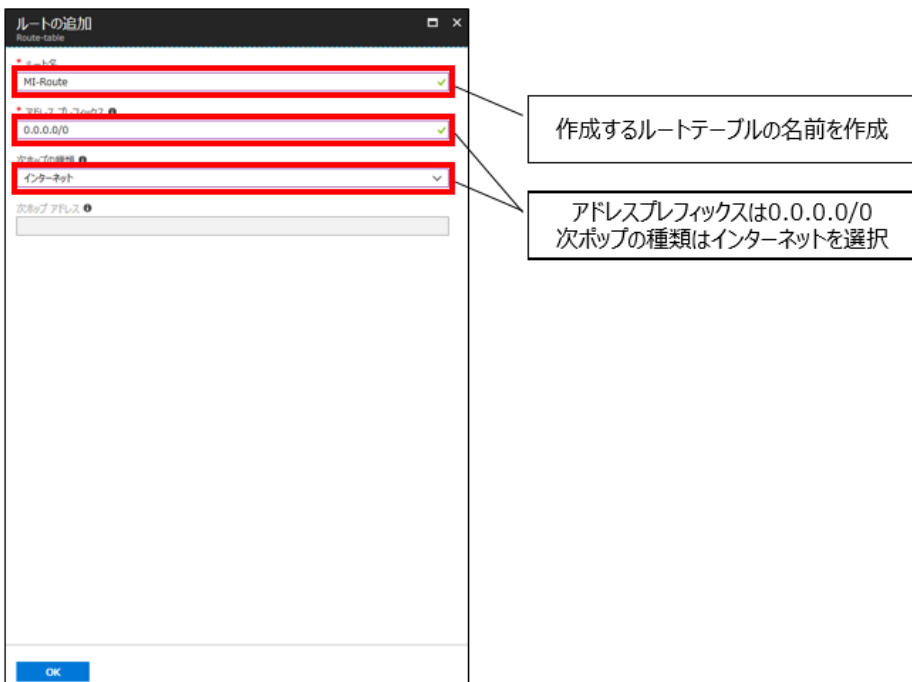
このサブネットは Managed Instance 専用のサブネットとなるため、その他のサービスを起動する等を行わない。ただし、複数の Managed Instance をこのサブネットへ配置することは可能である。

### 2.3.1.2 ルートテーブルを設定とサブネットの割り当て

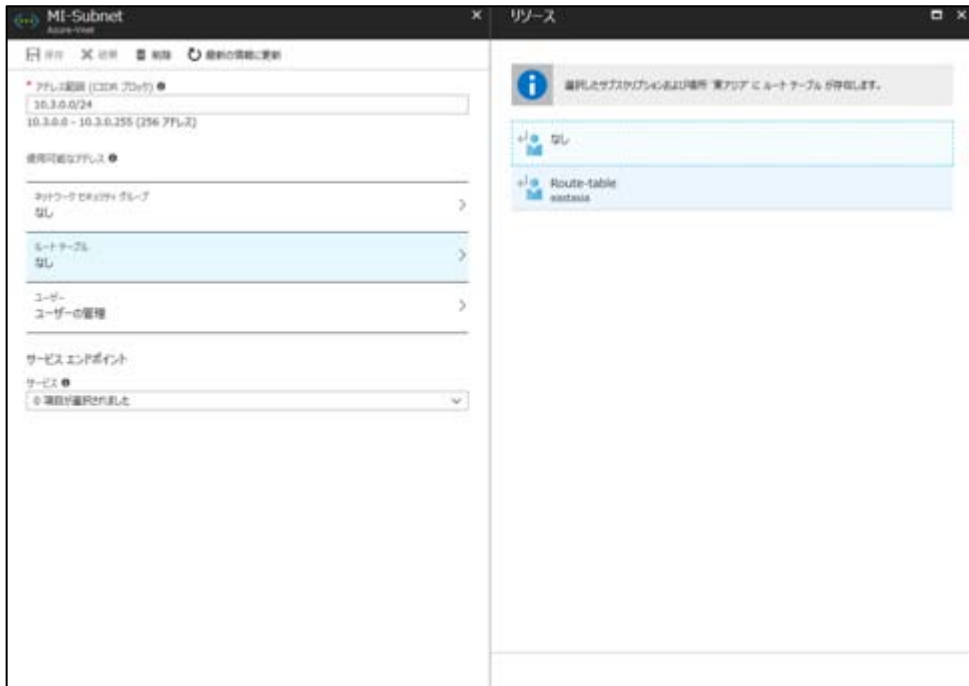
Managed Instance 専用のサブネットにルートテーブルを作成し、作成したルートテーブルを Managed Instance 専用のサブネットへ割り当てる。まずはルートテーブルを作成するため、Azure Portal より「ルートテーブル」選択し、追加を押下。ルートテーブルの作成画面にて、作成を行う。



P9. 「Managed Instance を起動するサブネットの要件」の作成要件に合わせた、ルートの追加を行う。



ルートの追加を行ったルートテーブルを Managed Instance 用のサブネットへ割り当てを行う。

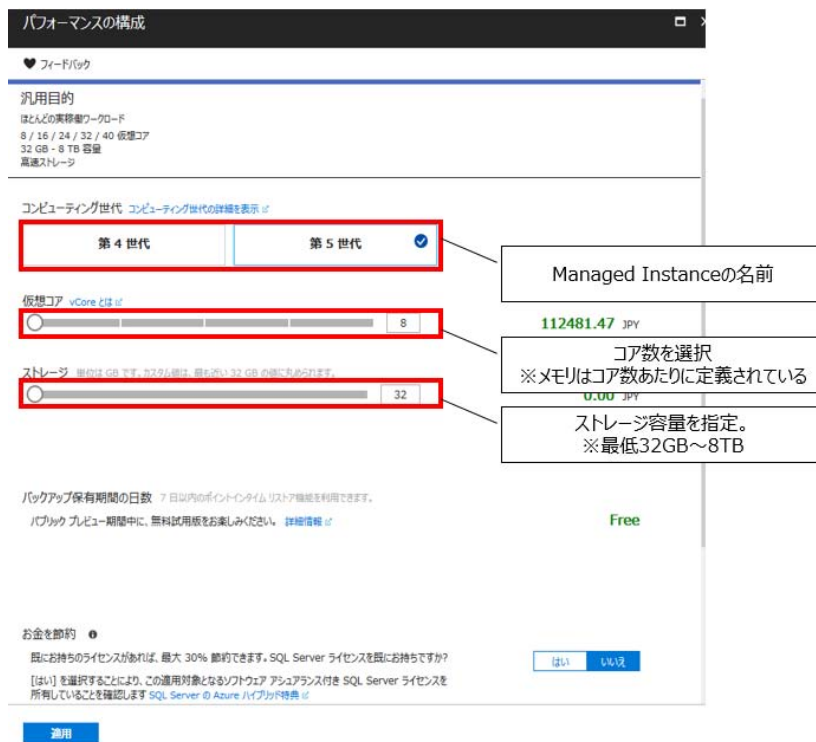


### 2.3.1.3 Managed Instance の作成

Managed Instance の作成では Azure Portal より「SQL マネージドインスタンス」を選択し、「追加」を押下、Managed Instance の作成を行う。







## 2.3.2 Managed Instance の管理と注意点

### 2.3.2.1 データベースの作成

Managed Instance では 1 つのインスタンスにつき、最大 100 個までデータベースの作成が可能である。通常の SQL Server 同様以下のコマンドで、Database の作成を実施する。

```
CREATE DATABASE [<データベース名>] COLLATE <照合順序>
```

ファイル/ファイルグループの追加や DB のプロパティの設定変更が必要な場合には、データベースの作成後に作業を行う。また、複数のログファイル (ldf) を追加することはできない。インスタンスごとの使用可能なファイル数、すなわち Managed Instance 内の全データベースの合計ファイル数は 280 となる。

### 2.3.2.2 サービス階層「汎用目的」のインスタンスのストレージ性能

Managed Instance では 1 インスタンスあたり最大で 8TB をデータファイル、すなわちデータベースの利用可能な領域として利用することが可能である。一方で、Managed Instance で作成したデータベース上の各データファイルは作成したデータファイルの容量に合わせて、128GB/256GB/512GB/1TB/4TB のいずれかのディスク (Premium Storage) に配置されることになる。このため、1 インスタンスあたりではデータベースとして最大で 8TB の容量までしかデータファイルを配置し利用することができないが、Managed Instance として、このデータファイルが配置されるディスクの総容量は最大で 35TB まで確保される可能性がある。これは最小ディスクのサイズ 128GB と「2.3.2.1 データベースの作成」の項で記した、Managed Instance 最大合計ファイル数である 280 か

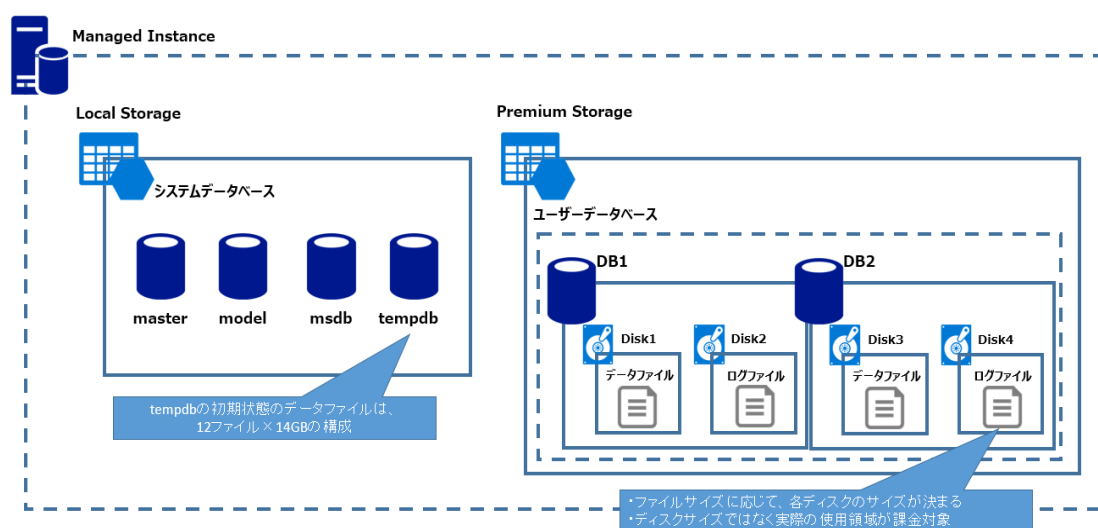
らも計算で求める事が可能である。[最小ディスク 128GB×最大ファイル数 280 ファイル=35,840GB（最大 Premium Storage 容量）]。

データファイルが配置される各ディスクに関しては、性能がそれぞれ異なる。このため、初期構築の段階で、データファイルの容量とディスク性能を把握し、初期サイズを設定することが望ましい。例えば 10GB のデータを格納する場合、初期サイズ 100GB のデータファイルだとスループットは 100MB/sec になるのに対して、初期サイズ 200GB のデータファイルだとスループットは 125MB/sec となる。このような事象が発生するのは、データファイルのサイズが 100GB の場合は 128GB のストレージに配置されるが、200GB の場合は 256GB のディスクへ配置されるためである。

**Premium Storageのディスク性能**

ディスクサイズ	128GB	256GB	512GB	1TB	4TB
ディスク当たりのIOPS	500	1100	2300	5000	7500
ディスク当たりのスループット	100 MB/秒	125 MB/秒	150 MB/秒	200 MB/秒	250 MB/秒

Managed Instance ではデータファイルを作成するタイミングで割り当てが行われる Premium Storage のディスクの容量（1 インスタンスあたり Premium Storage の総量が最大 35TB）と、データファイルそのものの容量（1 インスタンスあたりデータファイルの総量が最大 8TB）の 2 つの容量が存在することになるが、料金の課金対象となるのは後者の作成を行ったデータファイルの総容量となる。



### 2.3.2.3 照合順序

Managed Instance のインスタンスの照合順序は「SQL\_Latin1\_General\_CP1\_CI\_AS」で固定されており、システムデータベースと tempdb の照合順序はインスタンスの照合順序となる。一方でユーザーデータベースの照合順序については任意の設定に変更可能となる。このため、一時テーブル等の利用の際に非 Unicode 文字列型 (char/varchar) を利用する場合は、包含データベースの利用などを検討する必要がある。

#### 2.3.2.4 タイムゾーン

2018年6月現在 **Managed Instance** では日本のタイムゾーンに対応していない。日付関数 (`GET_DATE`) などで日付を取得する場合、**UTC** の日付時刻の取得となる。このため、ローカルタイムゾーンでの日付取得を行う際は、タイムゾーンに対しての考慮が必要となる。[日本時間 (**JST**) の場合、9時間をプラスする。]

#### 2.3.2.5 自動で取得されるバックアップと手動バックアップ

**SQL Database** と同様にデータベースを作成すると自動的にバックアップの取得が行われる。自動バックアップは7日～35日の間で保持期間を設定可能となっており、同一のサーバ内にデータベース名を指定して、ポイントインタイムリストアが可能である。

また、**Managed Instance** では「**COPY\_ONLY**」オプションを指定して、利用者の任意のタイミングで「**BACKUP DATABASE**」の実行が可能である（差分/ログバックアップを取得することはできない）。取得したバックアップに関しては **Managed Instance** にリストアすることが可能である。「**COPY\_ONLY**」による手動バックアップについての手順は後述する。

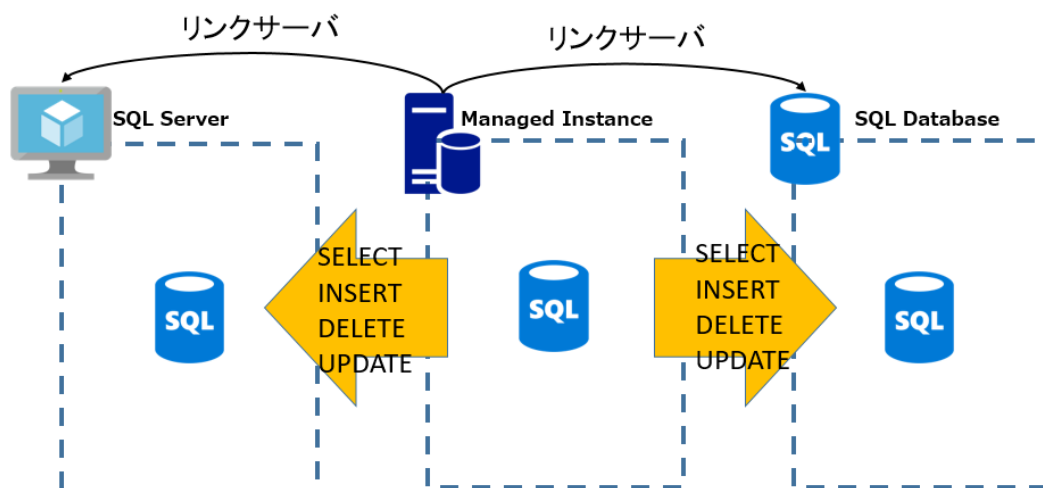
### 3 Azure SQL Database Managed Instance の機能検証

本章では Managed Instance のいくつかの機能に対して、使用方法などを説明する。特にこれまでの SQL Database では利用できなかった機能を中心に以下の機能について説明を行う。

- リンクサーバ
- COPY\_ONLY による手動バックアップ
- Azure SQL Database Managed Instance の監査※SQL Database でもデータベースレベルの監査は可能
- データベース跨ぎのトランザクション実行
- BULK INSERT ※本機能は SQL Database でも利用可能

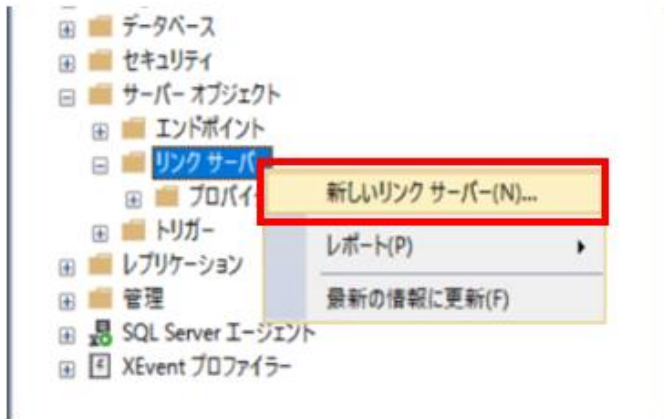
#### 3.1 リンクサーバ

Managed Instance では SQL Server と SQL Database に対してリンクサーバを設定することが可能である。リンクサーバを利用することで、接続しているデータベースとは異なるデータベースのデータを参照、更新、データのインサートなどを行うことが出来る。これまでの SQL Database ではこの機能は利用することが出来なかったが、Managed Instance ではこの機能を利用することができるようになっている。本章では SQL Server Management Studio (以下、SSMS) を利用して Managed Instance から SQL Server や SQL Database へのリンクサーバ経由で DML の実行を行う手順を記載する。

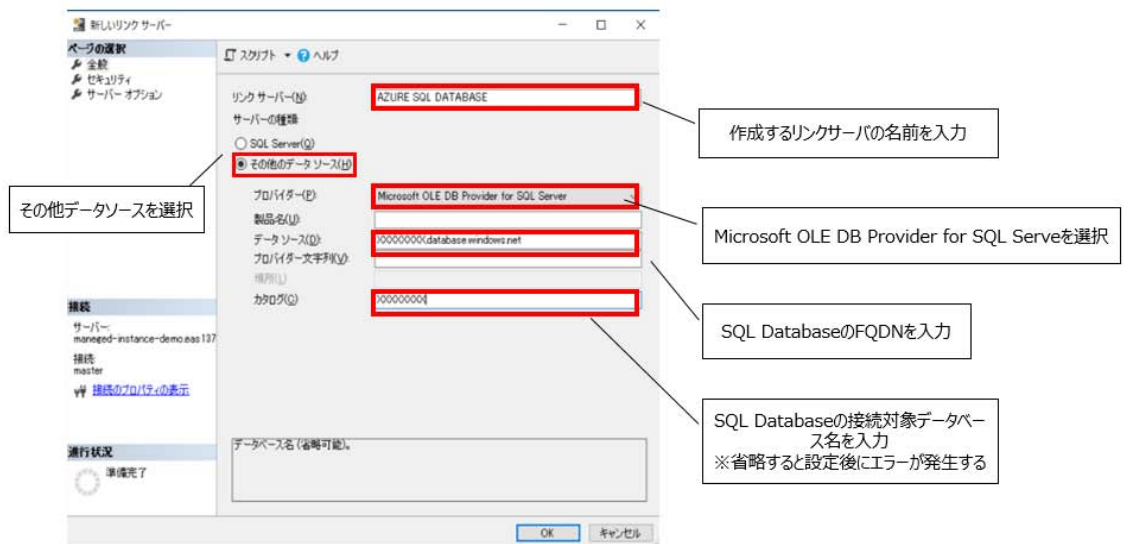


### 3.1.1 リンクサーバ設定方法 (SQL Database へ接続)

- ① SSMS より、リンクサーバを選択、右クリック。「新しいリンクサーバ」を押下。



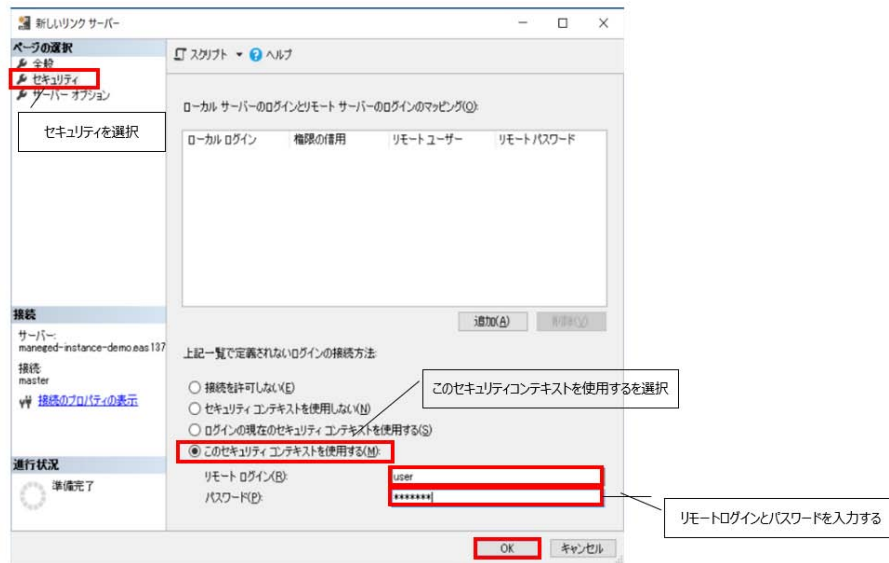
- ② 「リンクサーバ」にてリンクサーバの名前を入力し、「サーバの種類」で「その他データソース」選択。「プロバイダー」で「Microsoft OLE DB Provider for SQL Server」を選択し、「データソース」にて Managed Instance から接続を行う SQL Database の FQDN、「カタログ」にて接続を行うデータベース名を入力する。



カタログを省略した場合、リンクサーバのデータベースのテーブルを表示する際に下記のエラーが発生する。このエラーは、SQL Database がマスターデータベースを変更できないために発生する。

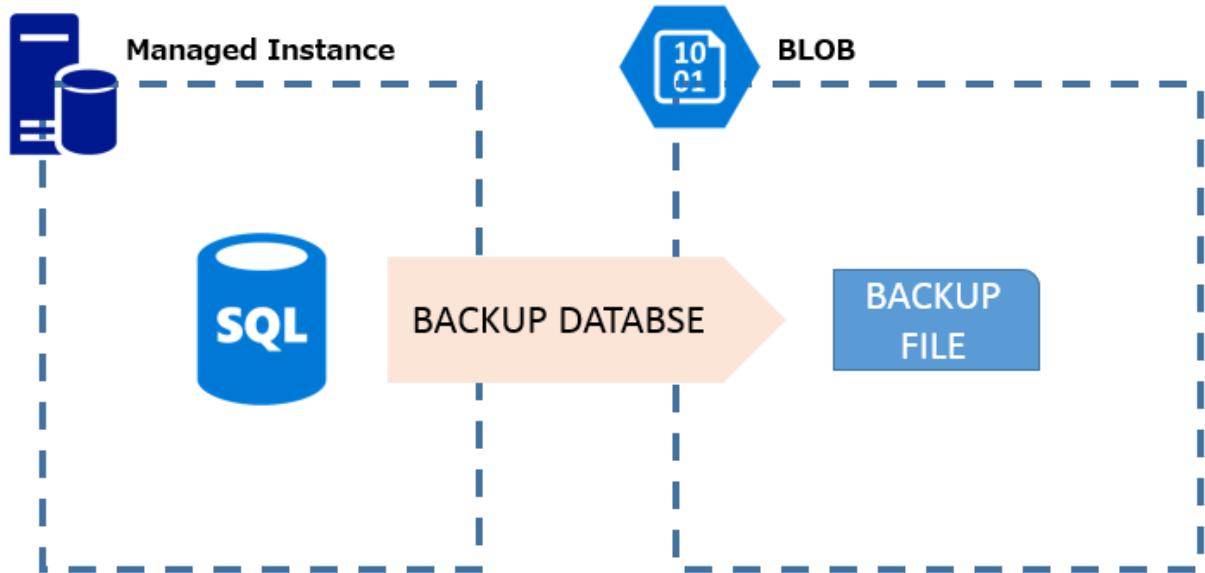


- ③ 「セキュリティ」を選択し、「このセキュリティコンテキストを使用する」選択。リモートサーバで接続する SQL Database のユーザのユーザ名とパスワードを「リモートログイン」と「パスワード」へ入力し、「OK」を押下。



## 3.2 COPY\_ONLY による手動バックアップ

Managed Instance では自動バックアップ以外にも「COPY\_ONLY」にてユーザ任意のバックアップが可能である。COPY\_ONLY によりバックアップを取得する場合、バックアップファイルは BLOB ストレージへ格納されることになる。本章では Managed Instance における「COPY\_ONLY」による手動バックアップの手順を記載する。



取得可能なバックアップは「COPY\_ONLY を指定した完全バックアップ」のみとなり、差分/ログバックアップを取得することは出来ない。また、バックアップファイルの取得先である BLOB ストレージは 1 ファイルあたり 200GB の制限があるため、大きなバックアップファイルの場合はファイルを分割して取得するようにし、1 ファイルあたり 48GB を超えないようにすることが推奨値となる。

### 3.2.1 BLOB ストレージの資格証明の登録

BLOB ストレージへバックアップファイルを出力するため、対象となる Managed Instance へ BLOB ストレージの資格情報を登録する。以下の SQL にて登録を行う。(出力を行う BLOB へも Shared Access Signature の設定を行っている必要がある。)

```
CREATE CREDENTIAL [https://<ストレージアカウント名>.blob.core.windows.net/<コンテナ名>]
WITH IDENTITY = 'SHARED ACCESS SIGNATURE'
, SECRET = '<Shared Access Signature>'
GO
```

### 3.2.2 COPY\_ONLY バックアップの取得

バックアップの取得は以下のコマンドで行う。COMPRESSION で圧縮して帯域を節約し、CHECKSUM or STATS オプションを指定して取得したバックアップが正しく取得できたかを確認することが望ましい。

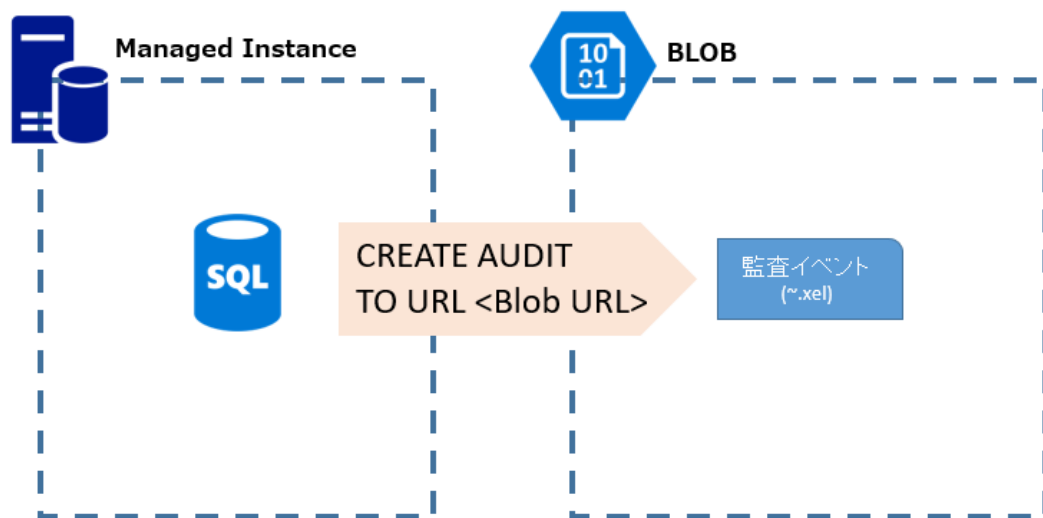
```
BACKUP DATABASE [<DB 名>]
TO
URL = 'https://<ストレージアカウント>.blob.core.windows.net/<コンテナ名>/<バックアップファイル>'
WITH COMPRESSION , STATS = 5, COPY_ONLY, INIT,FORMAT
GO
```

大きなデータベースで取得する場合は「MAXTRANSFERSIZE=4194304」のようにオプションを指定し分割で取得する。



### 3.3 Azure SQL Database Managed Instance の監査

Managed Instance でも監査の設定が可能である。SQL Database と同様、データベースレベルで機能することが可能であり、また、SQL Database とは異なりサーバレベルで監査を機能させることも可能である。オンプレミス/仮想 VM 上の SQL Server は、監査をサーバレベルで機能させることが可能な点は Managed Instance と同様だが、監査イベントはファイルシステムまたは Windows ログに保存される。一方で Managed Instance では監査イベントは Azure Blob Storage 上に .xel ファイルとして保存される。このため、Managed Instance では CREATE AUDIT 構文にて、「TO URL 構文」が用意されているが、「TO FILE 構文」はサポートされない仕様となっている。またその他の相違点として、「Shutdown オプション」、「queue\_delay の値として 0 を指定」をサポートしていない。本章では、Managed Instance におけるサーバレベル監査方法に関して記載する。



### 3.3.1 Azure SQL Database Managed Instance のサーバレベル監査設定方法

- ① 監査イベントの「~.xel」ファイルを出力させるコンテナを Azure Blob Storage へ作成する。
- ② Managed Instance が①で設定を行った Blob ストレージへアクセスするために、Shared Access Signature (SAS) の設定を行う。ストレージアカウントに対して SAS の設定を行った後に、Managed Instance で CREATE CREDENTIAL を実行する。  
以下、SAS の設定値の一例を示す。

Shared Access Signature (SAS) は、Azure Storage リソースに対する期限付きのアクセス権を付与する URI です。ストレージ アカウント キーを渡すことはできませんが、特定のストレージ アカウントのリソースへのアクセスを委任したいクライアントには Shared Access Signature を提供できます。このようなクライアントに Shared Access Signature URI を配布することで、指定した期間にリソースへのアクセスを許可します。

アカウントレベルの SAS では、複数の Storage サービス (BLOB, File, Queue, Table) へのアクセスを委任できます。ただし、現在、保存されているアクセス ポリシーは、アカウントレベルの SAS でサポートされていません。

詳細情報

使用できるサービス

BLOB  ファイル  キュー  テーブル

使用できるリソースの種類

サービス  コンテナ  オブジェクト

与えられているアクセス許可

読み取り  書き込み  削除  リスト  追加  作成  更新  プロセス

開始日時と有効期限の日時

開始

2018-06-08 18:46:51

終了

2018-06-10 02:46:51  
(UTC+09:00) --- 現在のタイムゾーン ---

使用できる IP アドレス

例: 168.1.5.65 または 168.1.5.65-168.1.5.70

許可されるプロトコル

HTTPS のみ  HTTPS と HTTP

署名キー

key1

SAS と接続文字列を生成する

SAS の設定完了後以下のコマンドを Managed Instance で実行する。

```
CREATE CREDENTIAL [https://<ストレージアカウント名>.blob.core.windows.net/<コンテナ名>]
WITH IDENTITY = 'SHARED ACCESS SIGNATURE'
, SECRET = '<Shared Access Signature>'
GO
```

- ③ CREATE SERVER AUDIT を実行し、サーバレベル監査を作成する。

```
CREATE SERVER AUDIT <audit 名>
TO URL ( PATH = 'https://<ストレージアカウント名>.blob.core.windows.net/<コンテナ名>',
RETENTION_DAYS = integer )
GO
```

④ AUDIT SERVER AUDIT にて、サーバレベル監査を有効化する。

```
ALTER SERVER AUDIT <audit 名>  
WITH (STATE = ON)  
GO
```

監査が有効になれば、出力先に指定した Blob ストレージ上へ .xel ファイルが出力される。

場所: miaudit / managed-instance-demo / master / audit\_name / 2018-06-09

プレフィックスによる BLOB の検索 (大文字と小文字を区別)  削除された Blob を表示

名前	変更日時	アクセス権	BLOB の種類	サイズ	リース状態	
[-]						...
09_58_53_674_0.xel	2018/6/9 午後6:58:54	ホット (推定)	BLOB の追加	7.5 KiB	リース中	...

### 3.3.2 監査イベントの SQL による確認

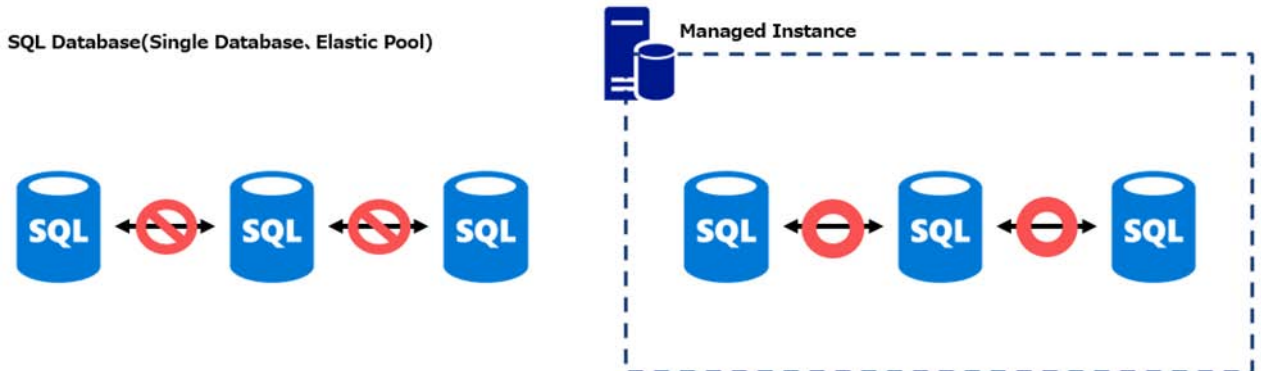
監査イベントは以下のような SQL を実行することで確認が可能である。

```
SELECT * FROM  
FROM sys.fn_get_audit_file ('<ストレージアカウント名>.blob.core.windows.net/<コンテナ名>/<.xel ファイル名>',  
null, null);
```

### 3.4 データベース跨ぎのトランザクション

SQL Database ではデータベースを跨いだトランザクションを実行する事が出来なかった。この為、オンプレミスの SQL Server から Azure への移行を検討する際、SQL Database の移行を行えず、仮想 VM 上に SQL Server を起動する「SQL Server on Azure VM」の構成で移行を実施するケースが多かった。

Managed Instance では一つのインスタンスの中に 100 までのユーザデータベースの作成が可能であり、インスタンス内のデータベース間であれば、データベース跨ぎのトランザクションを実行する事が可能である。



また、包含データベースを使用した場合、データベース内にパスワードを持つユーザを作成する事も可能となる。このユーザの場合はログインを持たないため、データベース内に作成されたユーザでそのデータベースへ接続する事になるが、このユーザでは別のデータベースに対してクエリを実行する事が出来ない。この為、このユーザでデータベースを跨いだクエリを実行する場合、以下の URL 内に記載されている対応が必要となる。

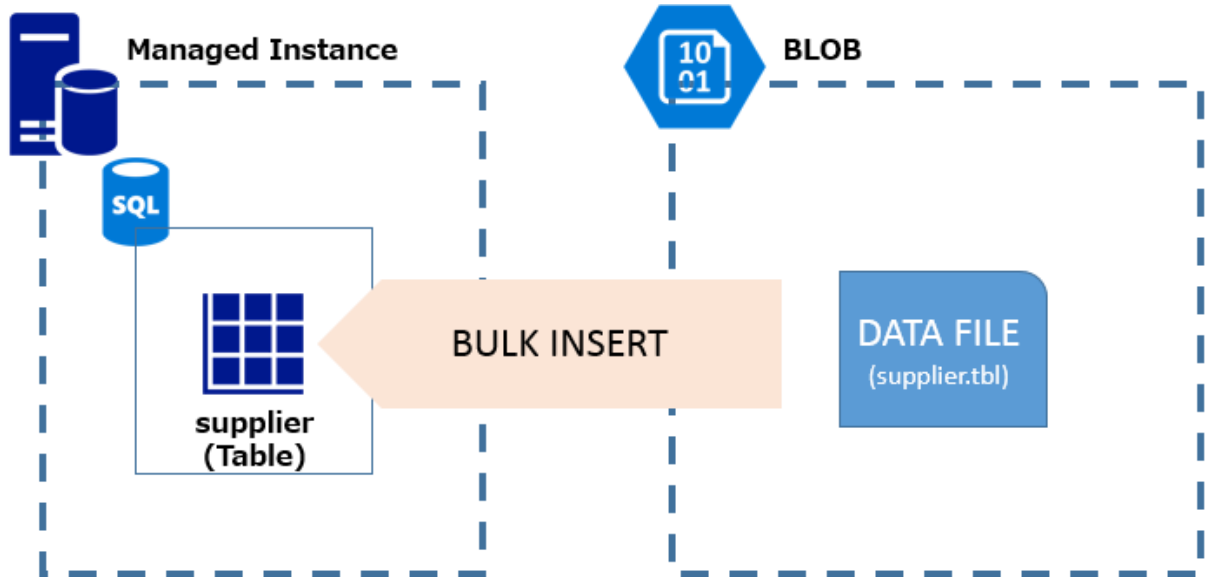
包含データベースでのセキュリティのベスト プラクティス

<https://docs.microsoft.com/ja-jp/sql/relational-databases/databases/security-best-practices-with-contained-databases?view=sql-server-2017>

データベース跨ぎのトランザクションの実行の対象となる両データベースに対して、同一の SID のユーザを作成して、最初に接続するデータベースに対して「TRUSTWORTHY」を有効にする。この設定により包含データベースを利用してもデータベースを跨いだトランザクションの実行が可能となる。

### 3.5 BULK INSERT によるファイルインポート

SQL Database では、BCP によるファイルデータのインポートに加え、新しく Azure BLOB 上のファイルから BULK INSERT によりデータのインポートが行えるようになった。Managed Instance でもこの機能は踏襲されており、BULK INSERT は実行可能である。Managed Instance を含む SQL Database で BULK INSERT を行う場合、インポート対象のファイルについては BLOB に格納する必要がある。本章では Managed Instance における BULK INSERT の手順に関して記載する。



#### 3.5.1 データベースマスターキーおよび、データベーススコープベースの資格情報の作成

```
CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<任意のパスワード>';  
CREATE DATABASE SCOPED CREDENTIAL <任意の CREDENTIAL の名前>  
WITH IDENTITY = 'SHARED ACCESS SIGNATURE'  
SECRET = 'KEY';
```

#### 3.5.2 外部データソースを登録

BULK INSERT を行う対象となるファイルを外部データソースとして Managed Instance へ登録する。

```
CREATE EXTERNAL DATA SOURCE <外部データソース名>  
WITH(  
    TYPE = BLOB_STORAGE,  
    LOCATION = 'https://{ストレージ名}.blob.core.windows.net'  
    CREDENTIAL = <3.3.1 で作成した任意の CREDENTIAL 名>  
);
```

### 3.5.4 BULK INSERT の実行

```
BULK INSERT [dbo].[SUPPLIER]
FROM 'supplier.tbl'
WITH (
    DATA_SOURCE = '<3.3.2 で作成した外部データソース名>',
    TABLOCK,                --テーブルのロック取得
    DATAFILETYPE='char',   --データファイルの型（今回は文字形式）
    CODEPAGE='raw',         --コードページの指定
    FILEDTERMINATOR='|',    --区切り文字
    ROWTERMINATOR='¥n'      --行ターミネータ
)
```

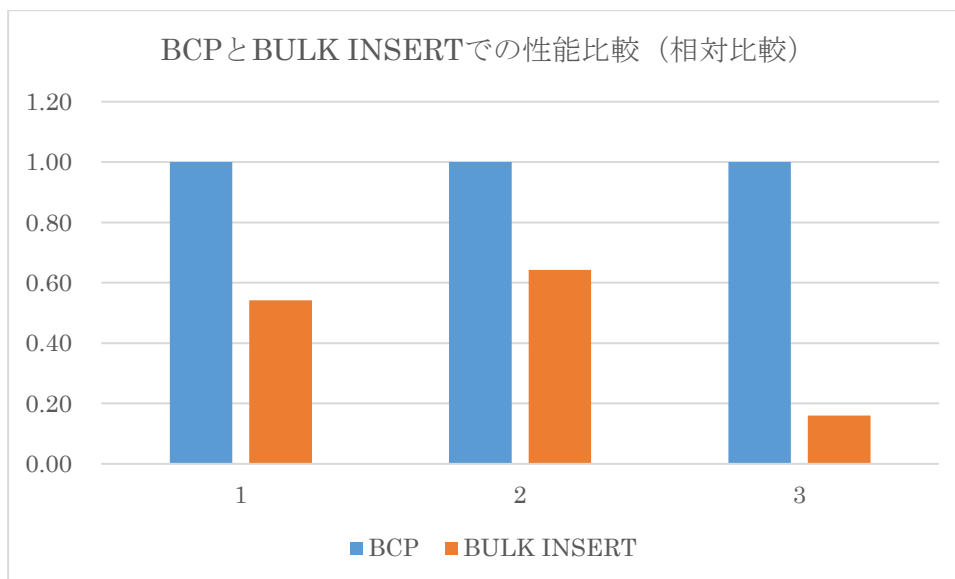
### 3.5.5 BULK INSERT と BCP でのデータインポートの性能比較

Managed Instance（Gen4 16 コア、汎用目的ベース、128GB のデータファイル）を利用し BULK INSERT と、BCP の性能比較を実施した。性能については以下 3 つのファイルを使用し、BULK INSERT と BCP 間の性能比較を実施している。

ファイル名	件数	データサイズ
orders.tbl	90,000,000 行	9.9GB
part.tbl	12,000,000 行	1.4GB
supplier.tbl	600,000 行	81MB

BULK INSERT の場合、まずは上記 3 ファイルを BLOB ストレージへ転送し、BLOB ストレージへ展開した 3 ファイルを対象に、BULK INSERT を実施しデータを Managed Instance へ取り込む。計測値としてこの BULK INSERT に掛かった時間を採用している。一方 BCP では上記 3 ファイルを仮想マシンのローカルに配置し、BCP を使って Managed Instance へデータの取り込みを行う。計測値として、この BCP の実行時間を採用している。

検証結果は以下の通り。



BCP に比べて BULK INSERT の方が高速にデータロードを行えるという結果となった。BULK INSERT を Managed Instance で利用する場合、BLOB ストレージにデータをアップロードする必要があるため、実際に利用する際にはその時間も鑑み、機能の選定を行う方が望ましい。

## 4 Azure SQL Database Managed Instance への移行手順

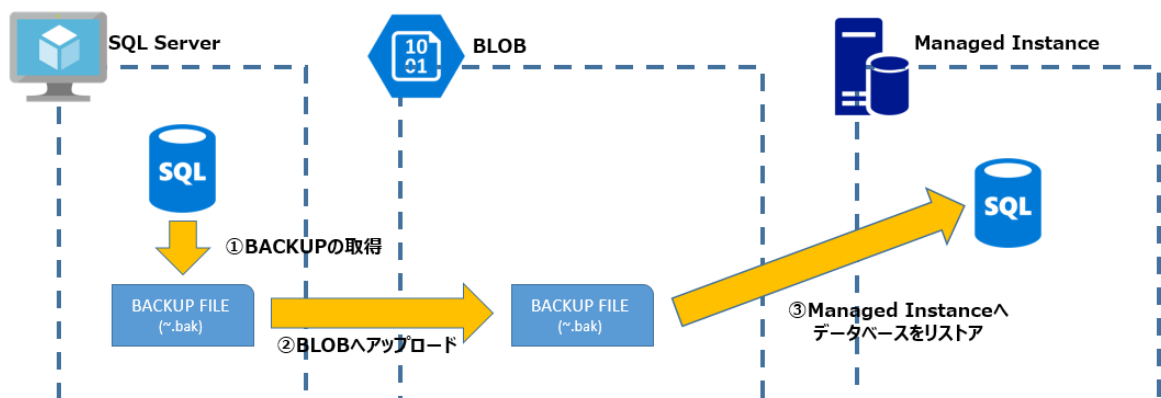
本章では、SQL Server から Managed Instance への移行方式について注意点なども含めていくつかの方法を記載する。本章で利用している SQL Server は、Azure VM 上で構築したものを利用しているが、オンプレミスの物理サーバからの移行であったとしても方法、手順は基本的に変わらない。

### 4.1 SQL Server ネイティブバックアップを使用した移行

Managed Instance では SQL Server から取得したネイティブバックアップを利用し、Managed Instance へリストアを行うことで移行できる。リストア可能なバックアップの制限についていくつか記載するが、詳細は以下の URL を参照のこと。

- 一つのバックアップファイルに複数のバックアップが含まれているファイルをリストアすることはできない
- 複数のログファイルで構成されたデータベースをリストアすることはできない
- FILESTREAM が含まれたデータベースをリストアすることはできない
- In-Memory OLTP が含まれたデータベースをリストアすることはできない
- WITH 句が使用できない。このため、差分バックアップや、トランザクションログバックアップを組み合わせ Managed Instance にリストアすることはできない。
- サポートされている構文
  - RESTORE DATABASE
  - RESTORE FILELISTONLY ONLY
  - RESTORE HEADER ONLY
  - RESTORE LABELONLY ONLY
  - RESTORE VERIFYONLY ONLY
- サポートされていない構文
  - RESTORE LOG ONLY
  - RESTORE REWINDONLY ONLY

<https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-managed-instance-transact-sql-information#restore-statement>





Managed Instance へネイティブバックアップをリストアする場合、BLOB からしかリストアをすることが出来ない。このため、取得したバックアップを BLOB へアップロードすることが必要となる。以下に実際の手順を記載する。

#### 4.1.1 SQL Server からのバックアップ取得

SQL Server からバックアップを取得する。今回の例では VM 上へ構築された SQL Server 上のデータベース「AdventureWorks2017」のバックアップを「C:¥backup¥」へ出力させる。

```
USE master
Go

BACKUP DATABASE [AdventureWorks2017]
    TO DISK = N'C:¥backup¥AdventureWorks2017.bak'
GO
```

取得したバックアップファイルを Azure CLI や Microsoft Azure Storage Explorer にて BLOB へアップロードする。

また、ネイティブバックアップの取得を行う SQL Server が、SQL Server 2012 SP2 CU2 以降であれば、BACKUP の取得の際に「TO URL」の指定が可能である。このため、SQL Server のバックアップを直接 BLOB ストレージへ出力させることも可能である。

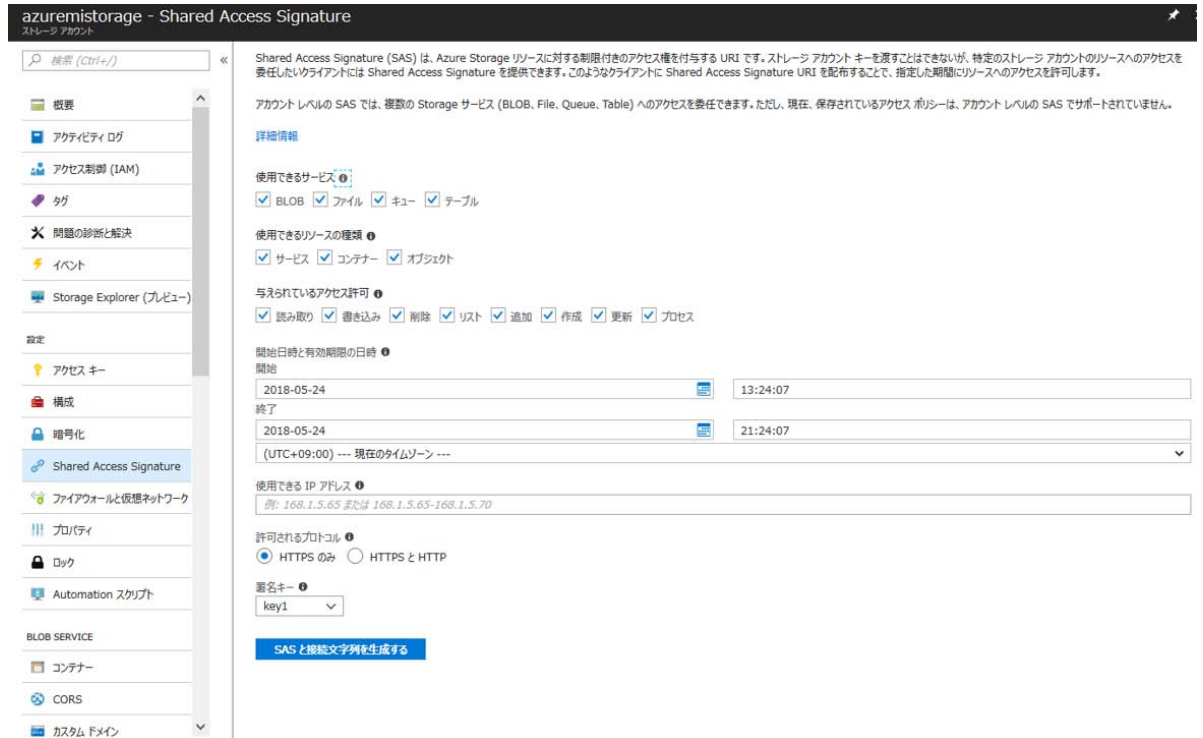
```
CREATE CREDENTIAL [https://<ストレージアカウント名>.blob.core.windows.net/<コンテナ名>]
    WITH IDENTITY = 'SHARED ACCESS SIGNATURE'
    , SECRET = '<Shared Access Signature>'
GO

BACKUP DATABASE [AdventureWorks2017]
    TO URL = N'https://<ストレージアカウント名>.blob.core.windows.net/<コンテナ名>
    >/adventureworks2017_backup_4.bak'
GO
```

#### 4.1.2 Managed Instance での SHARED ACCESS SIGNATURE (SAS) の設定

Managed Instance が BLOB ストレージへアクセスするために、SAS の設定を行う。ストレージアカウントに対して SAS の設定を行った後に、Managed Instance で CREATE CREDENTIAL を実行する。

以下、SAS の設定値の一例を示す。



SAS の設定完了後以下のコマンドを Managed Instance で実行する。

```
CREATE CREDENTIAL [https://<ストレージアカウント名>.blob.core.windows.net/<コンテナ名>]
WITH IDENTITY = 'SHARED ACCESS SIGNATURE'
, SECRET = '<Shared Access Signature>'
GO
```

#### 4.1.3 Azure SQL Database Managed Instance にてデータベースをリストア

BLOB に格納されたバックアップファイルから Managed Instance へリストアを行う。

```
RESTORE DATABASE AdventureWorks2017
FROM URL= https://<ストレージアカウント名>.blob.core.windows.net/<コンテナ名>
>/adventureworks2017_backup_4.bak'
```

SQL Server の場合はリストアを実行したセッションから同期的にリストアの実行状況が返されるが、Managed Instance の場合、リストアの要求を投げた後は非同期でリストアされる。

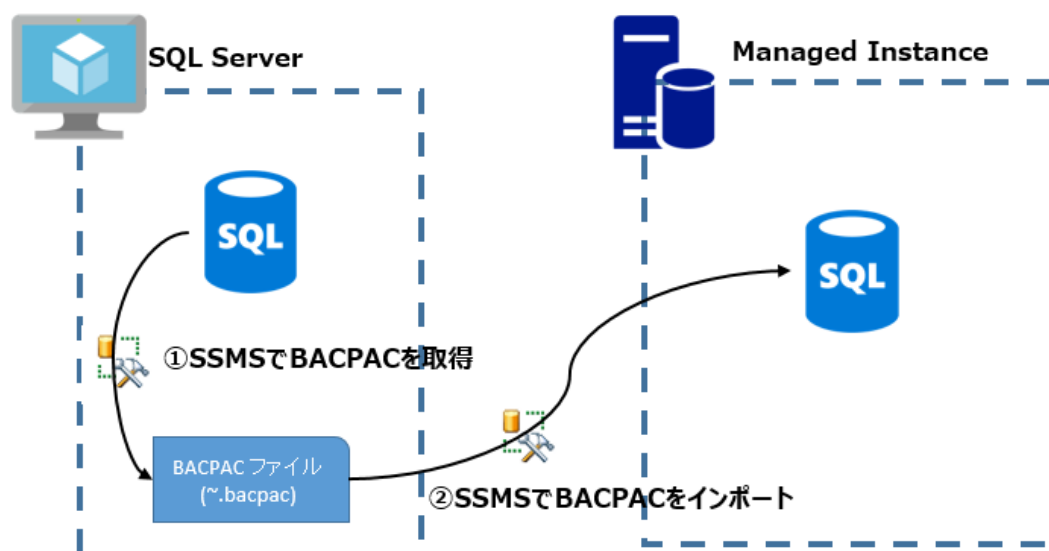
RESTORE ステートメントを実行したセッションを切断了しても、リストア自体は非同期でバツ

クランド実行が継続される。リストアの状況については以下のクエリで確認を行うことが可能である。

```
SELECT * FROM sys.dm_operations_status  
WHERE operation = 'CreateManagedRestoreRequest'
```

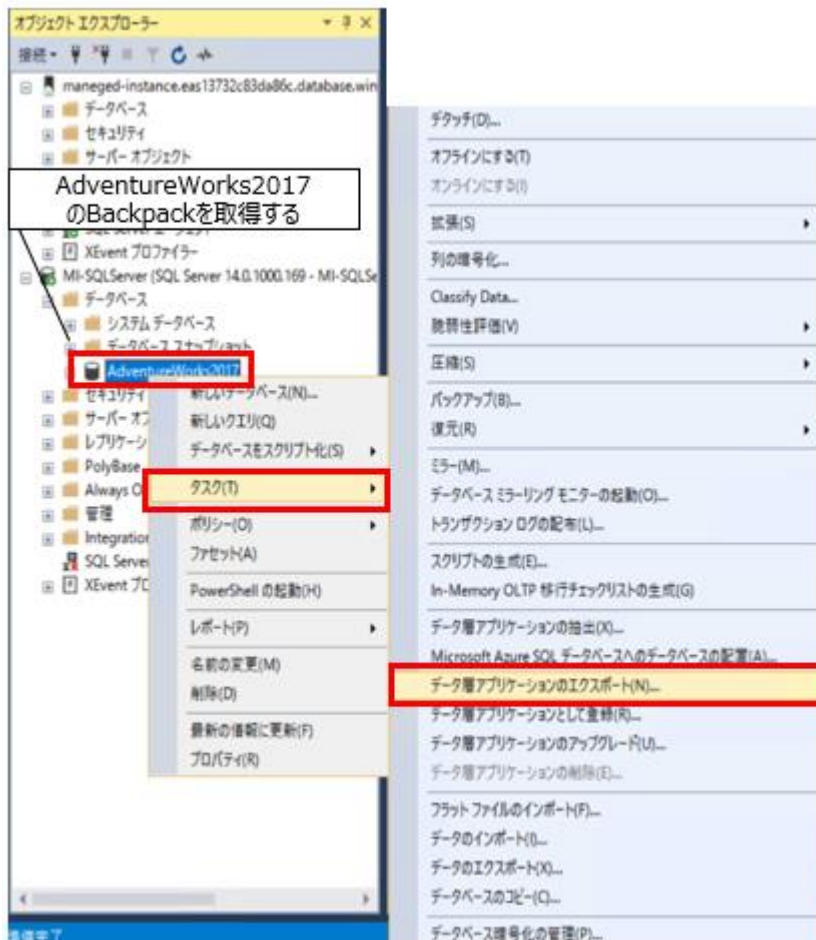
## 4.2 BACPAC を使用した移行

BACPAC を使用して、SQL Server から Managed Instance に対してデータの移行を行うことが可能である。今回は SQL Server Management Studio (以下、SSMS) を利用して SQL Server から BACPAC を取得し、Managed Instance にてインポートを行う。また、SSMS では 17.6 以降で Managed Instance への接続をサポートしているが、Managed Instance へ BACPAC をインポートする場合は SSMS 18 以降でなくてはならない点に注意が必要となる。



#### 4.2.1 SQL Server からユーザデータベース「AdventureWorks2017」の BACPAC を取得

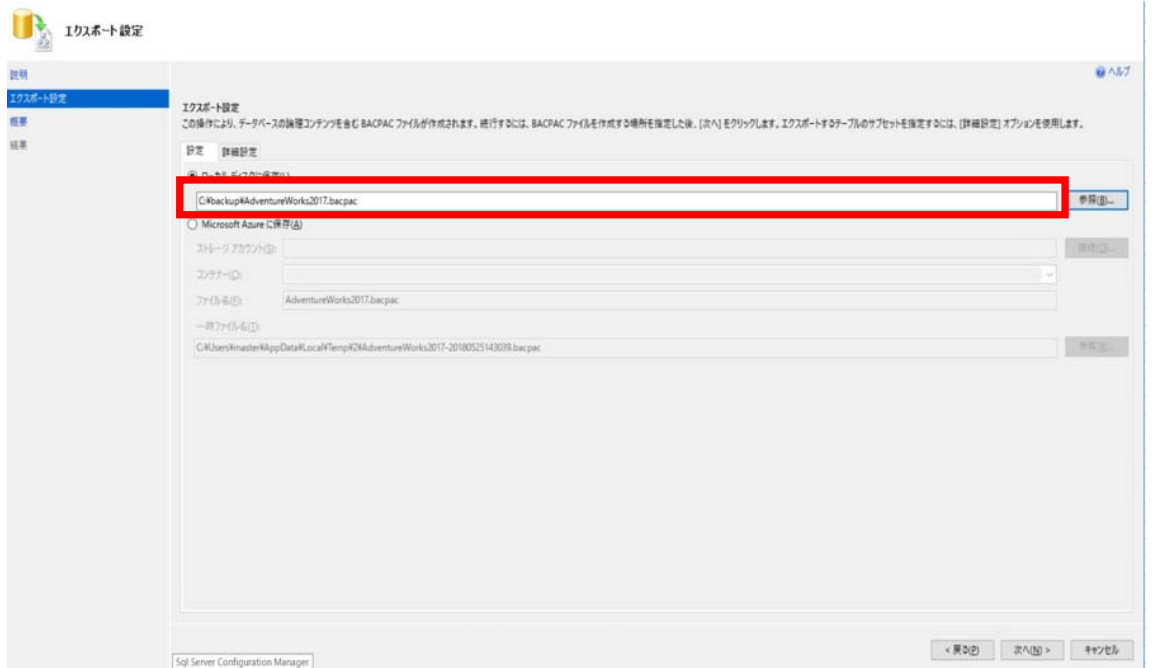
- ① BACPAC 取得対象である AdventureWorks2017 を選択、右クリックし、「タスク」⇒「データ層アプリケーションのエクスポート」を押下。



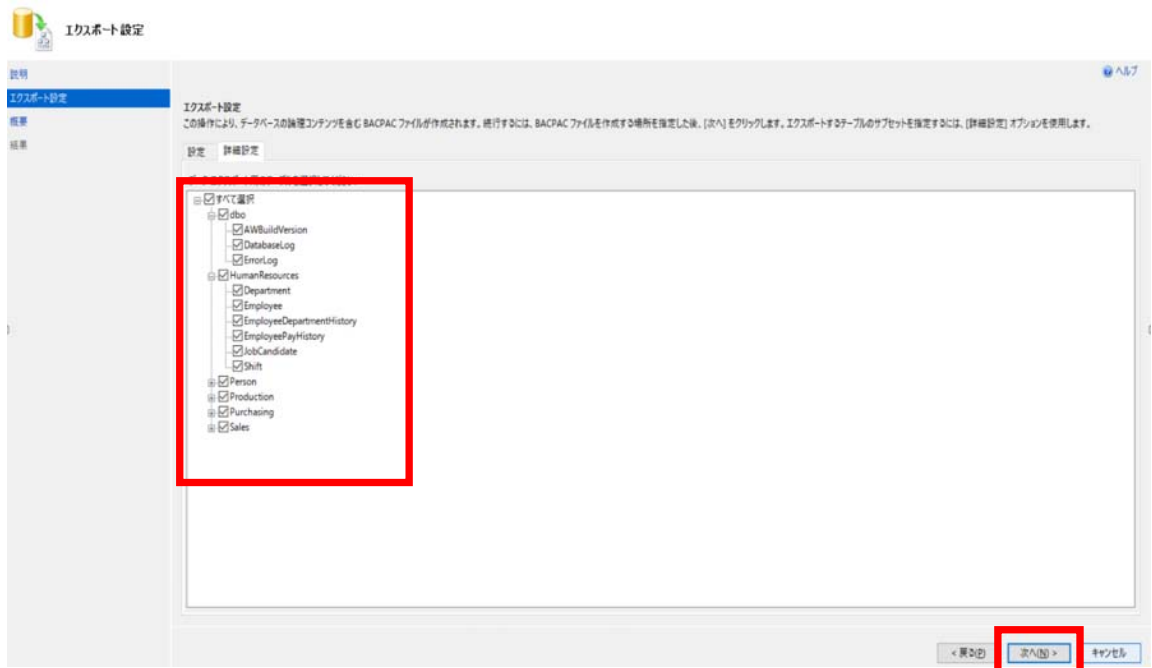
- ② 説明を確認し、「次へ」を押下。



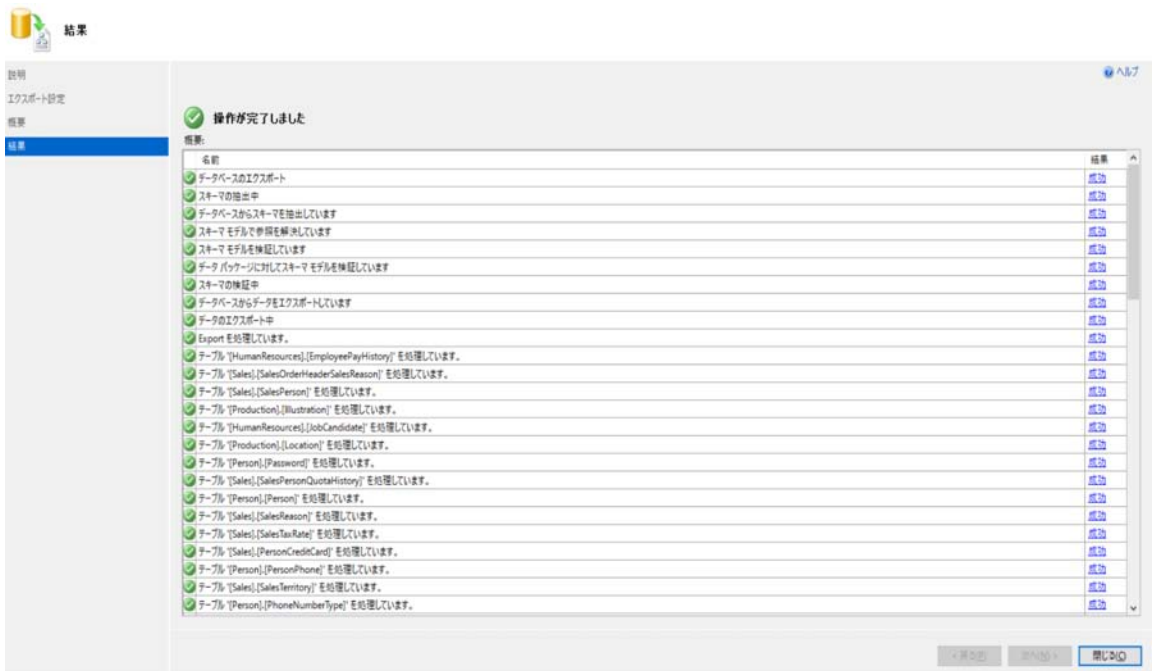
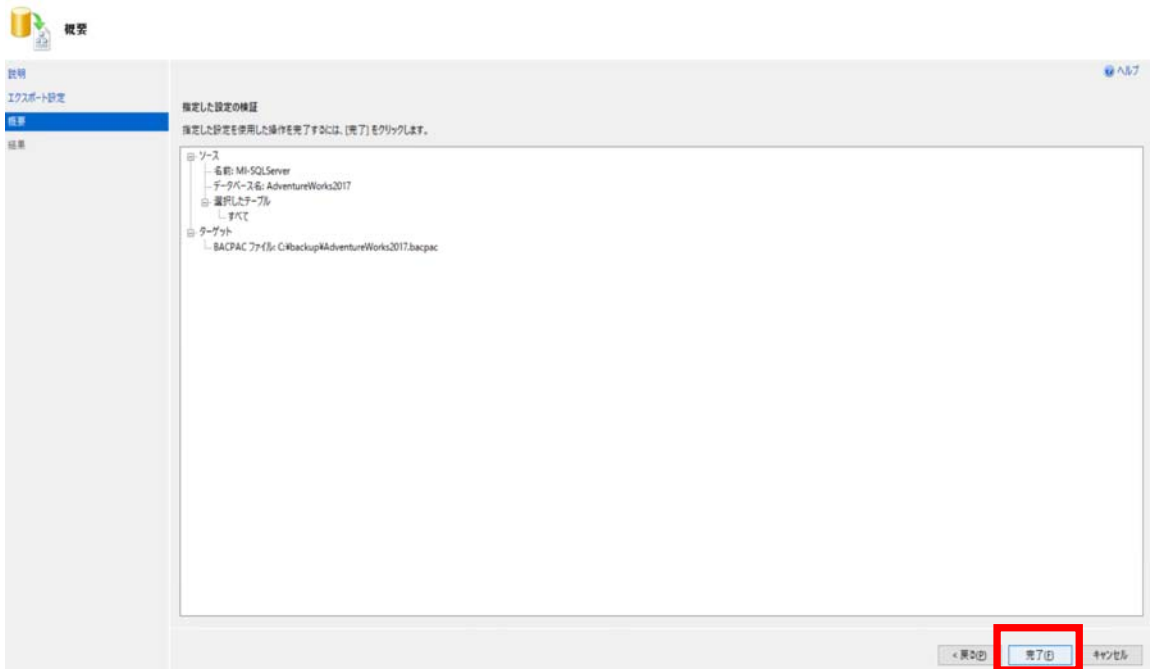
- ③ BACPAC のエクスポートの設定を実施する。今回は BACPAC の出力先とファイル名を「C:\¥backup¥AdventureWorks2017.bacpac」と指定している。



また、「詳細設定」では、エクスポートする対象を選択することが可能である。設定が完了すれば、「次へ」を押下。

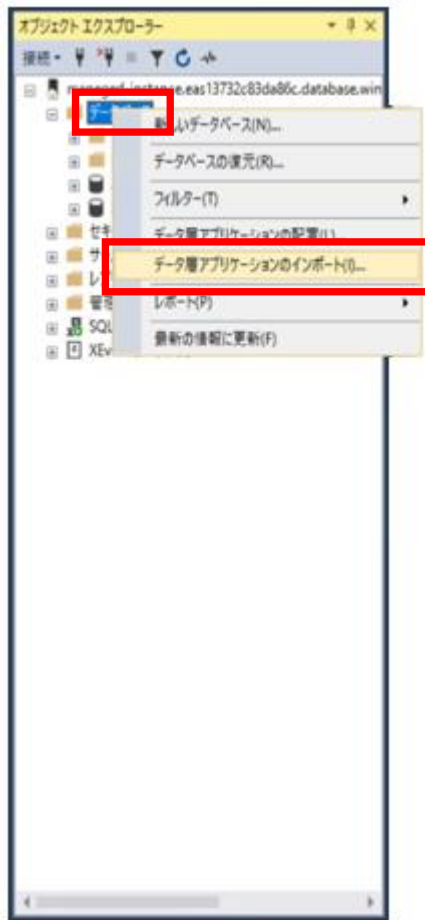


- ④ 概要が表示される。「完了」を押下後、エクスポートが開始され、BACPAC の取得が行われる。



#### 4.2.2 SSMS を利用して取得した BACPAC から Manage Instance へインポート

- ① SSMS で Managed Instance へ接続し、データベースを右クリック。「データ層アプリケーションのインポート」を押下する。



- ② 説明を確認し、「次へ」を押下。



- ③ インポートする BACPAC ファイルを選択する。ここでは、4.2.1 で取得した AdventureWorks2017 の BACPAC を指定している。指定が完了したら、「次へ」を押下。

インポートの設定

説明

インポートの指定

データベースの指定

概要

結果

インポートする BACPAC を指定します。  
この操作では、BACPAC ファイルからデータベースが作成されます。続行するには、BACPAC の場所を指定します。必要に応じて、新しいデータベースの設定を指定します。続行するには、[次へ] をクリックしてください。

ローカルディスクからインポート

C:\Backup\AdventureWorks2017.bacpac

Windows Azure からインポート

ストリーミングアカウント

コンテナー

ファイル

一時ファイル

C:\Users\master\AppData\Local\Temp\Temp\_bacpac-20180525143620.bacpac

< 戻る

次へ >

キャンセル

- ④ Managed Instance でのデータベース名を指定し、「次へ」を押下。

データベースの設定

説明

インポートの指定

データベースの指定

概要

結果

新しいデータベースの設定を指定します。  
この操作では、BACPAC ファイルからデータベースが作成されます。続行するには、新しいデータベースの設定を指定して [次へ] をクリックします。

managed-instance.eas13732c63da85c.database.windows.net (MIADMIN)

新しいデータベース名

AdventureWorks2017

SQL Server の設定

データファイルのパス

C:\WF\Root\08\_1\Fabric\work\Applications\Work\CL\_App15\work\data

ログファイルのパス

C:\WF\Root\08\_1\Fabric\work\Applications\Work\CL\_App15\work\data

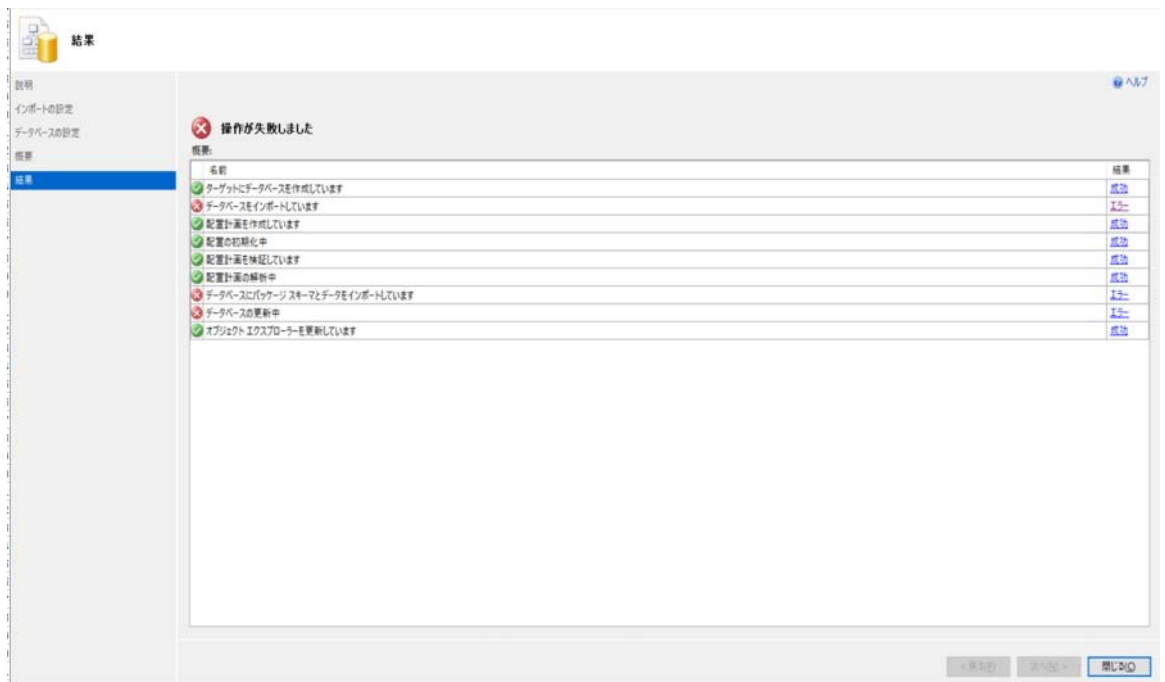
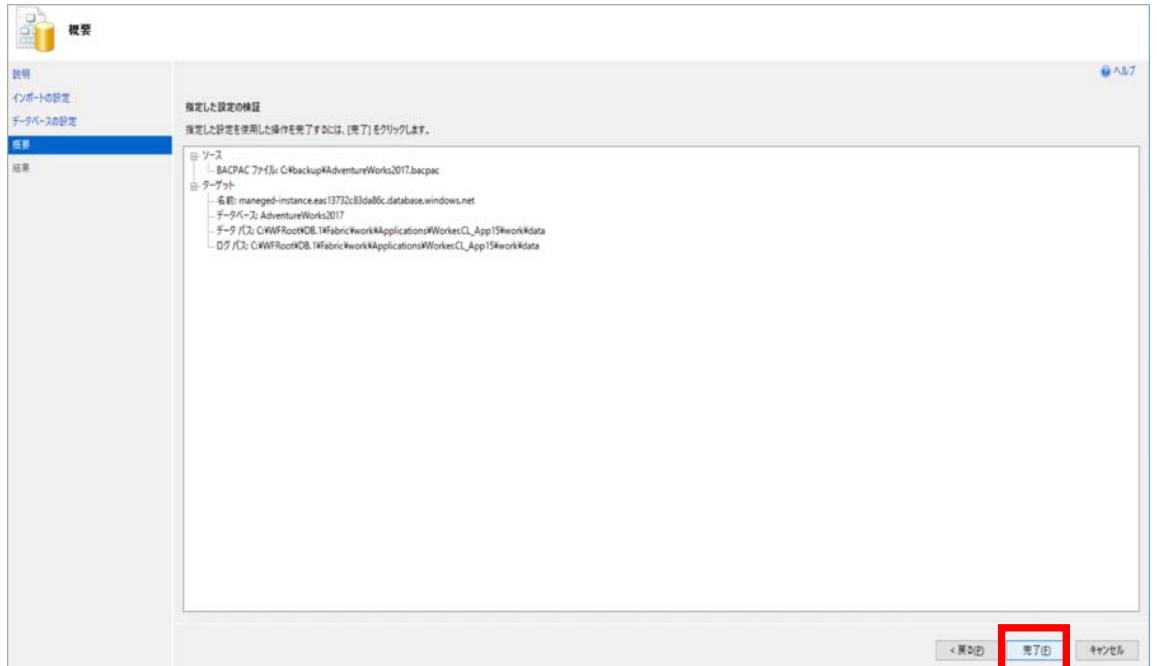
< 戻る

次へ >

キャンセル

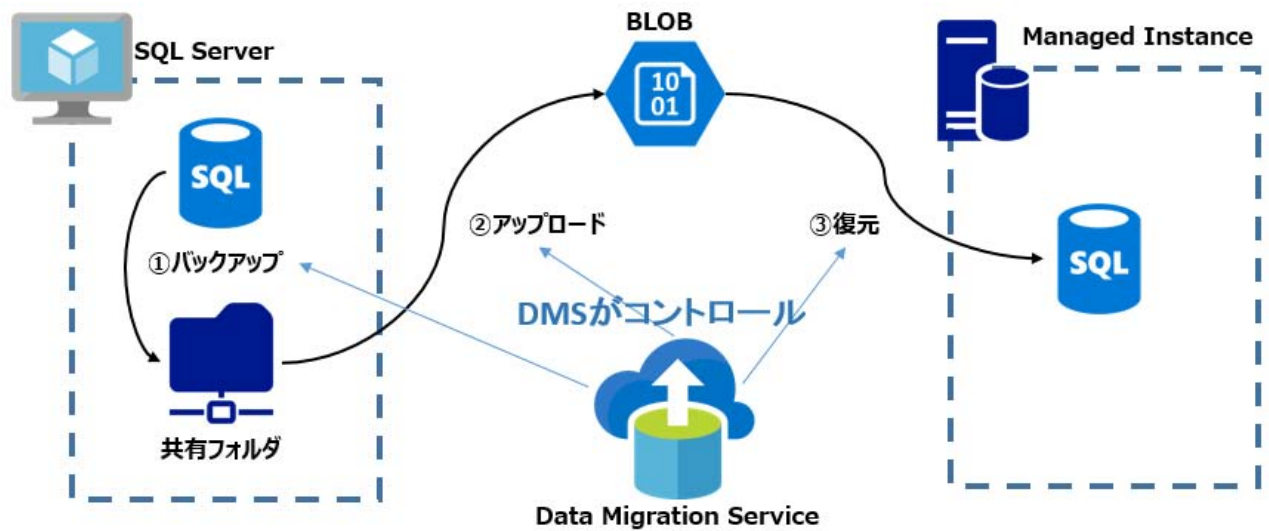


- ⑤ 概要が表示される。「完了」を押下後、インポートが開始され、Managed Instance へ BACPAC からデータベースが作成される。SSMS 18 より前のバージョンを利用していると、このタイミングでエラーが発生する。



### 4.3 Azure Data Migration Service を使用した移行

Azure Data Migration Service（以下、DMS）は複数のデータベースソースから Azure への移行を最小限のダウンタイムで実現する PaaS のサービスである。2018 年 6 月現在では移行先のデータベースとして SQL Database と Managed Instance をサポートしている。本章ではこの DMS を利用した SQL Server から Managed Instance への移行方法を記載する。



### 4.3.1 Azure Data Migration Service の作成

Azure Portal より「Azure Data Migration Service」を選択し、「移行サービスの作成」を実施する。



### 4.3.2 新しい移行プロジェクトの作成

① 作成した DMS から「新しい移行プロジェクト」を押下。



- ② 「プロジェクト名称」を入力し、「ソースサーバの種類」で「SQL Server」選択。「ターゲットサーバの種類」で「Azure SQL Database マネージインスタンス」を選択し「作成」を押下する。

新しい移行プロジェクト

プロジェクト名  
SQLServerToMI

\* ソースサーバの種類  
SQL Server

\* ターゲットサーバの種類  
Azure SQL Database マネージ インスタンス

SQL Server から Azure SQL Database マネージド インスタンスへのプロジェクトの移行はプレビュー中です。  
Microsoft Azure プレビューの追加使用 [条件をご確認ください。](#)

作成

- ③ 移行ウィザードの画面にて、様々な情報の詳細を設定する。まず、「1. ソースの選択」にて、移行元となる SQL Server の情報を入力する。「ユーザー名」には SQL Server の管理者ユーザを入力し、「パスワード」では管理者ユーザのパスワードを入力する。

移行ウィザード  
SQL Server 移行

1 ソースの選択 >

2 データソースの選択 >

3 データの選択 >

4 完了 >

ソース SQL Server インスタンス名  
XXXXXXX ✓

認証の種類  
SQL 認証 ▼

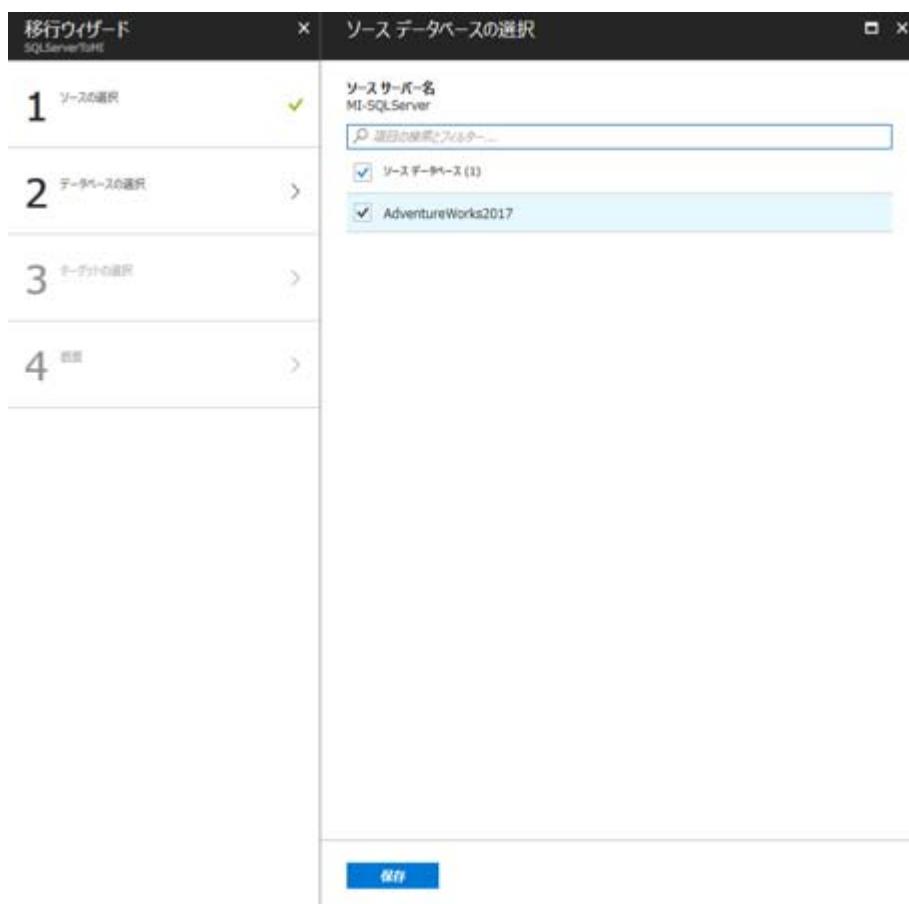
ユーザー名  
XXXXXXX ✓

パスワード  
●●●●●●●●●●●●●●●● ✓

接続のプロパティ  
 接続を暗号化する  
 サーバー証明書を信頼する

保存

- ④ 「2. データベースの選択」では移行対象とするデータベースを選択する。今回は「AdventureWorks2017」を選択している。



- ⑤ 「3. ターゲットの選択」では移行先となる **Managed Instance** の情報を入力する。「ユーザー名」には **Managed Instance** の管理者ユーザを入力し、「パスワード」では管理者ユーザのパスワードを入力する。

ステップ	内容	完了
1	ソースの選択	完了
2	データベースの選択	完了
3	ターゲットの選択	現在
4	確認	完了

**ターゲットの詳細**

\* Azure SQL Database マネージ インスタンスをプロビジョニングしましたか?  
 はい  いいえ

\* 対象サーバー名

認証の種類  
SQL 認証

\* ユーザー名

パスワード

保存

- ⑥ 概要が表示され「保存」を押下後プロジェクトの作成が完了する。

移行ウィザード × プロジェクトの概要

1 ソースの選択 ✓

2 データベースの選択 ✓

3 ターゲットの選択 ✓

4 詳細 >

移行プロジェクト名  
SQLServerToMI

ソースサーバー名  
MI-SQLServer

ソースサーバーのバージョン  
SQL Server 2017  
14.0.1000.169

対象サーバー名  
XXXXXXXXXX

ターゲットサーバーのバージョン  
Azure SQL Database  
12.0.2000.8

移行するデータベース  
1/1

保存

#### 4.3.3 新しい移行アクティビティを作成

- ① プロジェクトの作成が完了後、作成したプロジェクトに対して、新しい移行アクティビティを作成する。「新しい移行アクティビティ」を押下する。

+ 新しい活動 / プロジェクトを編集する / プロジェクトの削除 / 更新

✓ 成功しました。Database Migration プロジェクトが正常に作成されました。今すぐ最初の移行アクティビティを作成できます。

ソースサーバー  
MI-SQLServer  
ソースのバージョン  
SQL Server 2017  
14.0.1000.169

ターゲットサーバー  
---  
ターゲットのバージョン  
---

移行アクティビティ (0)

名前	活動の種類	状態	開始時刻
アクティビティが見つかりません。			

成功しました。Database Migration プロジェクトが正常に作成されました。今すぐ最初の移行アクティビティを作成できます。

新しい移行アクティビティ



- ② 移行ウィザードの画面にて、様々な情報の詳細を設定する。まず、「1. ソースの選択」にて、移行元となる **SQL Server** の情報を入力する。(プロジェクト作成時にも入力したが再度入力を行う。)「ユーザ名」には **SQL Server** の管理者ユーザを入力し、「パスワード」では管理者ユーザのパスワードを入力する。

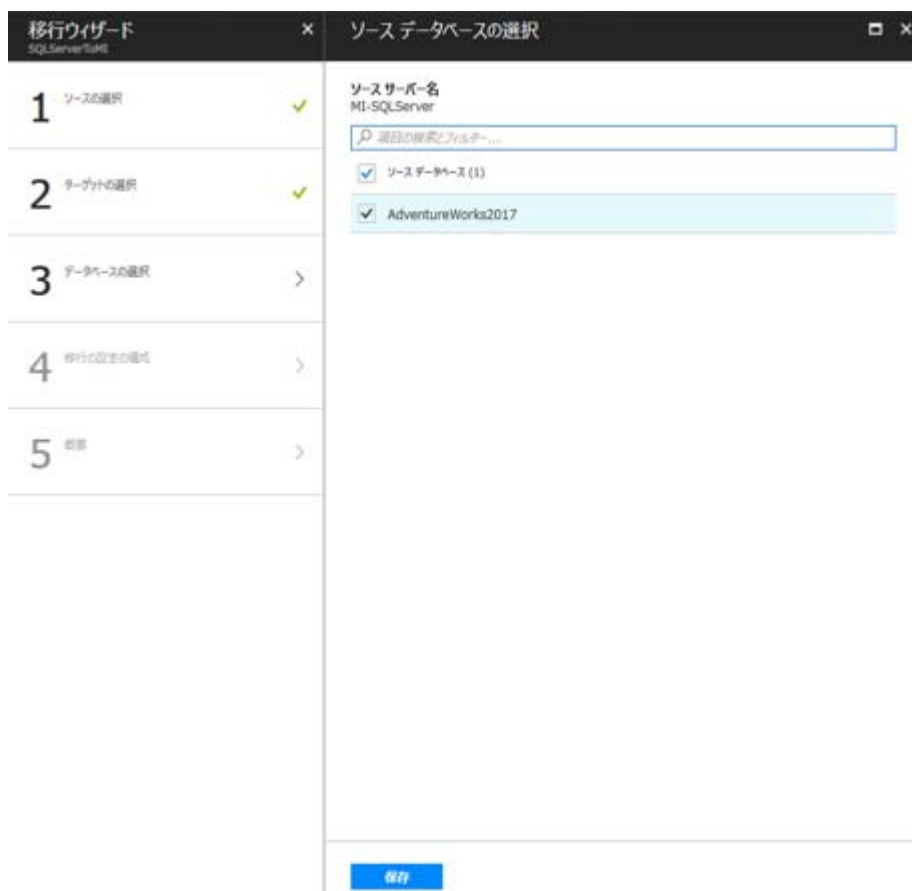
ステップ	詳細
1 ソースの選択	* ソース SQL Server インスタンス名 XXXXXXXX ✓ 認証の種類 SQL 認証 * ユーザー名 XXXXXXXX ✓ パスワード ●●●●●●●●●●●●●●●● ✓
2 ターゲットの選択	
3 データソースの選択	
4 移行の設定の種類	接続のプロパティ <input checked="" type="checkbox"/> 接続を暗号化する <input type="checkbox"/> サーバー証明書を信頼する
5 完了	

保存

- ③ 「2. ターゲットの選択」では移行先となる **Managed Instance** の情報を入力する。「ユーザー名」には **Managed Instance** の管理者ユーザを入力し、「パスワード」では管理者ユーザのパスワードを入力する。

The screenshot shows the '移行ウィザード' (Migration Wizard) for SQL Server TSM. The left pane shows the progress of five steps: 1. ソースの選択 (Source Selection) - completed with a green checkmark; 2. ターゲットの選択 (Target Selection) - current step with a right arrow; 3. データベースの選択 (Database Selection) - right arrow; 4. 移行の設定の指定 (Specify Migration Settings) - right arrow; 5. 完了 (Complete) - right arrow. The right pane, titled '移行のターゲットの詳細' (Target Details), contains the following fields: '対象サーバー名' (Target Server Name) with value 'XXXXXXXXXX'; '認証の種類' (Authentication Type) set to 'SQL 認証' (SQL Authentication); 'ユーザー名' (Username) with value 'XXXXXXXX'; and 'パスワード' (Password) masked with dots. A '保存' (Save) button is located at the bottom of the right pane.

- ④ 「3. データベースの選択」では移行対象とするデータベースを選択する。今回は「AdventureWorks2017」を選択している。



⑤ 「4. 移行の設定の構成」を設定する。

The screenshot shows the '移行の設定の構成' (Configure Migration Settings) page in the Azure Database Migration Service wizard. The left sidebar lists five steps: 1. ソースの選択 (Source Selection), 2. ターゲットの選択 (Target Selection), 3. データベースの選択 (Database Selection), 4. 移行の設定の構成 (Configure Migration Settings), and 5. 結果 (Results). Step 4 is currently active.

The main content area contains several sections:

- バックアップ設定 (Backup Settings):**
  - Information: Azure Database Migration Service uses SMB network shares to store backups. The SAS URI must be specified.
  - Warning: The source SQL Server instance must be running on a service account with write permissions on the network share.
  - Requirement: The service must be able to write to the network share.
  - Field (1): Network share path (e.g., \\XXXXXXXXXXXXXXXXXX).
  - Requirement: The Windows user must have full control permissions on the share.
  - Field (2): Windows user (e.g., XXXXXXXXXXXXXXX).
  - Field: Password (masked with dots).
- ストレージアカウントの設定 (Storage Account Settings):**
  - Information: The service needs a SAS URI to access the storage account for file uploads.
  - Warning: The SAS URI must be created with appropriate permissions.
  - Field (3): SAS URI (e.g., XXXXXXXXXXXXXXX).

At the bottom, there is a '保存' (Save) button.

### (1) Server Backup Location

移行元の SQL Server のバックアップの取得先の共有フォルダ。

移行元の SQL Server のサービスアカウントが指定した共有フォルダに対して、バックアップを出力できる権限を有している必要がある。

### (2) User Name / Password

DMS が、SQL Server のバックアップが取得された、共有フォルダにアクセスを行うために使用する資格情報を入力する。

共有フォルダがドメイン環境でない場合「IP アドレス¥ユーザ名」で指定する。

(ユーザ名だけでは、アクティビティ作成時のバリデーションでエラーとなる)

### (3) Storage SAS URL

DMS が Managed Instance にリストアを行うために、バックアップをアップロードする Azure BLOB ストレージの「コンテナ」にアクセスをするための SAS の URL を入力する。Managed Instance が BLOB にアクセスする際の資格情報としても使用される。SAS については、バックアップをアップロードするコンテナの SAS を指定する必要があるため、Azure Storage Explorer を利用する。

- ⑥ 「移行の概要」が表示される。検証オプションを指定することで、移行の前に検証を実行することが可能である。「移行を実行する」を押下して実際の移行が始まる。

The screenshot displays a three-pane window for a migration wizard. The left pane, titled '移行ウィザード' (Migration Wizard), shows a progress list with five steps: 1. ソースの選択 (Source Selection), 2. ターゲットの選択 (Target Selection), 3. データベースの選択 (Database Selection), 4. 移行の設定の構成 (Configure Migration Settings), and 5. 概要 (Summary). Steps 1-4 are marked with green checkmarks, and step 5 is the current active step. The middle pane, titled '移行の概要' (Summary of Migration), displays the following configuration details: Activity Name: SQLServerToMI; Target Server Name: managed-instance.eas13732c83da86c.database.windows.net; Target Server Version: Azure SQL Database 12.0.2000.8; Source Server Name: MI-SQLServer; Source Server Version: SQL Server 2017 14.0.1000.169; Databases to Migrate: 1/1. A '検証オプション' (Validation Options) section at the bottom of the middle pane shows a red warning icon and the text '必要な設定の構成' (Configure required settings). The right pane, titled '検証オプションの選択' (Select Validation Options), has two radio buttons: 'データベースを検証しない' (Do not validate database) and 'データベースの検証' (Validate database), with the latter selected. Below these are checkboxes for '検証オプション' (Validation Options) and 'クエリの正確さ' (Query Accuracy), both of which are checked. At the bottom of the window, there are two buttons: '移行を実行する' (Execute Migration) and '保存' (Save).

#### 4.3.4 移行状況の確認

移行状況は Azure Portal より確認することが可能である。以下の図では1つのデータベースに対して処理が実行中であることを示している。



完了すると DMS のステータスに変更され、移行が完了したことを確認できる。

The screenshot displays the Azure Database Migration Service (DMS) console for a migration job named 'SQLServerToMI'. The interface is split into two main panels. The left panel provides details about the source and target servers, including their versions and configurations. The right panel shows a table of migration progress for the databases.

**Source Server Details:**

- ソースサーバー: MI-SQLServer
- ソースのバージョン: SQL Server 2017, 14.0.1000.169
- サーバーオブジェクト: 1

**Target Server Details:**

- ターゲットサーバー: managed-instance:eas13732c83da86c.database.windows.net
- ターゲットのバージョン: Azure SQL Database, 12.0.2000.8

**Migration Progress Table:**

SERVER	オブジェクト	処理中	停止	成功	警告	失敗
データベース		0	0	1	0	0

**Database Migration Details Table:**

名前	状態	サイズ	移行の詳細	期間
AdventureWorks2017	完了	352.00 MB		00:01:39

DMS では、移行の途中に共有フォルダや BLOB に対してバックアップファイルを作成するが、これらは移行完了したタイミングで DMS により自動で削除される。

## 4.4 Data Migration Assistant を利用した互換性調査

Managed Instance は SQL Server 2017 ベース相当のエンジンが採用されている。Microsoft Data Migration Assistant v3.5 を利用することで、SQL Server 2008 や 2008 R2/2012/2014 を SQL Server 2017 へ移行/アップグレードした際に発生する問題を事前にチェックすることができる (SQL Server 2014 まではアップグレード アドバイザーとして提供されていた)。Data Migration Assistant v3.5 を使用して SQL Server 2017 との互換性調査を行うことで、Managed Instance へ過去バージョンから移行する際の事前の調査が可能である。

Data Migration Assistant は、次の URL からダウンロードすることができる。

<https://www.microsoft.com/en-us/download/details.aspx?id=53595>

プログラムのダウンロードを行い、ローカルへインストールし利用する。

### 4.4.1 Managed Instance で利用可能な互換性レベル

2018 年 6 月時点で Managed Instance が利用可能な互換性レベルは以下の通りとなっている。

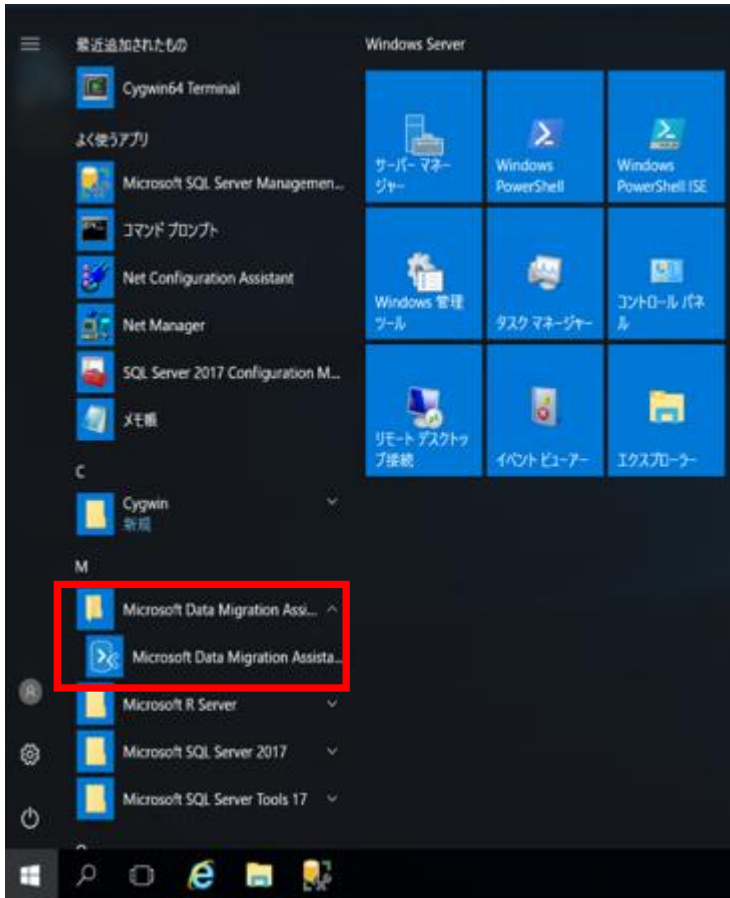
- 100  
SQL Server 2008
- 110  
SQL Server 2012
- 120  
SQL Server 2014
- 130  
SQL Server 2016
- 140  
SQL Server 2017

Managed Instance でサポートされる最小の互換性レベルは「100」となっている。SQL Server 2005 のバックアップをリストアすると、自動的に互換性レベルが「100」に変更される動きとなる。



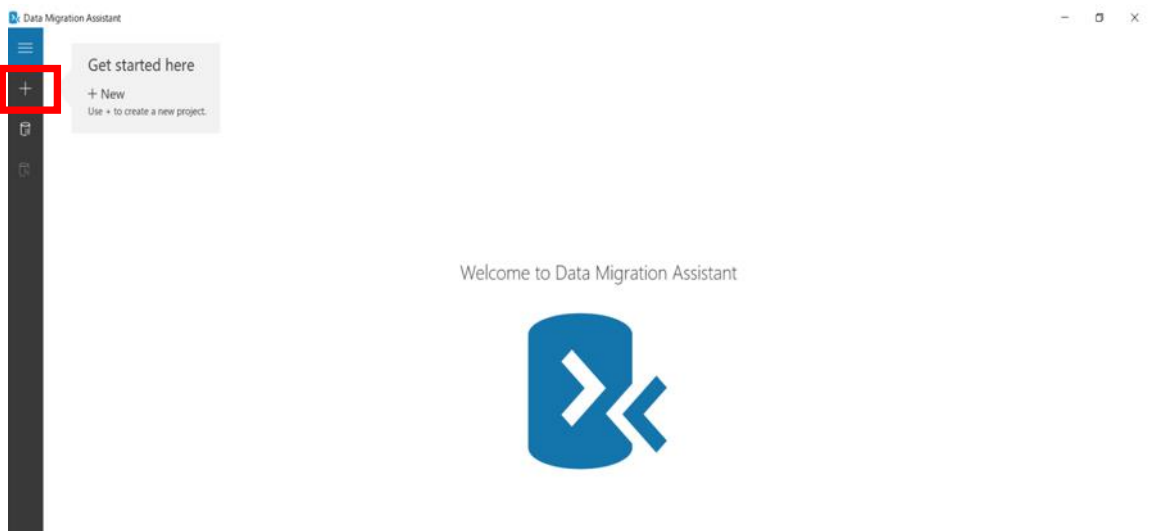
#### 4.4.2 Data Migration Assistant の起動

Data Migration Assistant を起動するには、スタートメニューで「Microsoft Data Migration Assistant」グループから「Microsoft Data Migration Assistant」をクリックする。

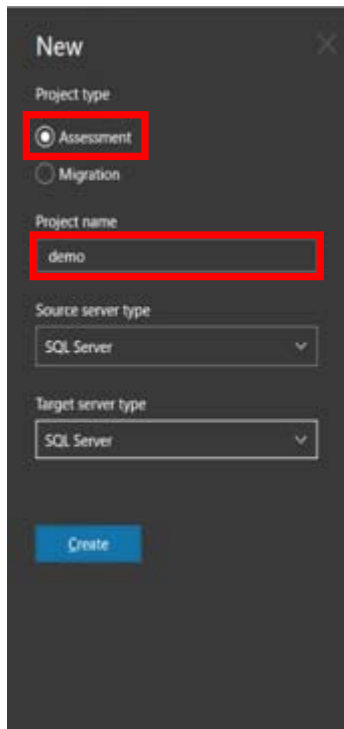


#### 4.4.3 Data Migration Assistant を使った互換性調査

① Data Migration Assistant の起動後、画面左上の「+」(New) ボタンを押下。



- ② 「New」 ブレードが表示されたら、「Project type」で「Assessment」（アセスメント）、「Project name」に任意のプロジェクト名を入力する。画面では「demo」を入力する。



New

Project type

Assessment

Migration

Project name

demo

Source server type

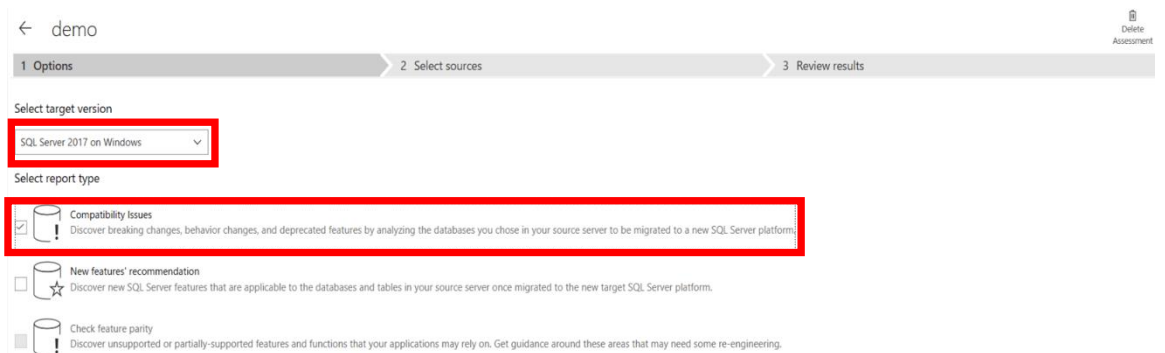
SQL Server

Target server type

SQL Server

Create

- ③ 以下のページが表示されたら、「Select target version」で「SQL Server 2017 on Windows」を選択し、「Compatibility Issues」を選択する。




← demo Delete Assessment


1 Options 2 Select sources 3 Review results


Select target version

SQL Server 2017 on Windows

Select report type

 **Compatibility Issues**  
Discover breaking changes, behavior changes, and deprecated features by analyzing the databases you chose in your source server to be migrated to a new SQL Server platform.

 **New features' recommendation**  
Discover new SQL Server features that are applicable to the databases and tables in your source server once migrated to the new target SQL Server platform.

 **Check feature parity**  
Discover unsupported or partially-supported features and functions that your applications may rely on. Get guidance around these areas that may need some re-engineering.

- ④ 「Connect to Server」が表示されたら、「Server Name」で接続先となる SQL Server（アップグレード前の SQL Server）の名前を入力し、「Connect」ボタンをクリックする。

Connect to a server

Connect to a server and select sources

Server name The field must have a value.

Authentication type

Windows Authentication

Connection properties

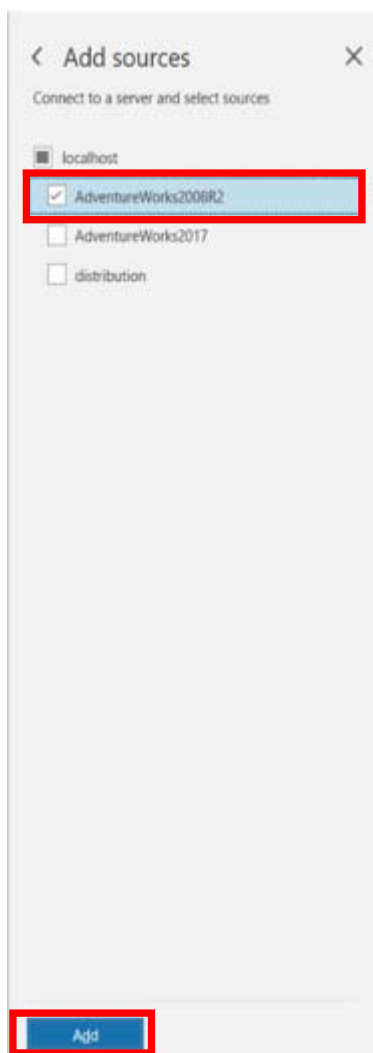
Encrypt connection

Trust server certificate

**SQL Server permissions**

To run the selected advisor(s), credentials used to connect to source SQL Server instance must have CONNECT SQL, VIEW SERVER STATE, and VIEW ANY DEFINITION permissions.

- ⑤ 「Add sources」のページ表示後、接続した SQL Server 上のデータベースが一覧される。互換性のチェックを行う、対象のデータベースをチェックし、「Add」ボタンを押下する。今回は「AdventureWorks2008R2」というデータベースを選択している。



- ⑥ 選択したデータベースの一覧が表示される。「Start Assessment」のボタンをクリックし、アセスメントを開始する。

← demo Delete Assessment

1 Options ✓ 2 Select sources 3 Review results

Add sources Remove sources

Name	Compatibility Level	Database Size
localhost (SQL Server 2017) (1)		
AdventureWorks2008R2	100	200.06 MB

Back Start Assessment

#### 4.4.4 アセスメント結果の確認

アセスメントが完了すると以下のような画面が表示される。互換性に問題がないか確認を行う。

- **Breaking changes**

下位互換性のない変更点。未サポートの機能になるので、修正しないと動作しないもの。

- **Behavior changes**

変更された動作。そのまま利用することも可能だが、気を付けたほうが良い／変更したほうが良いリストとなる。

- **Deprecated features**

将来廃止される機能。利用は可能だが、次のバージョン以降ではサポートされなくなる予定のものが表示される。

The screenshot displays the 'Review results' step of a compatibility assessment. The target platform is 'SQL Server 2017 on Windows' and the source is 'AdventureWorks2008R2'. The overall compatibility is 140 (2). The 'Behavior changes' category is expanded and highlighted with a red box, showing two items: 'Full-Text Search has changed since SQL Server 2008' with 3 impacted objects, and 'SERVERPROPERTY('LCID') result...' with 1 impacted object. The 'Issue details' for the first item indicate that many full-text search options and settings have changed, and a recommendation is provided to test applications. The 'Impacted objects' table lists three FullTextIndex objects: HumanResources.JobCandidate, Production.Document, and Production.ProductReview. An 'Object details' section shows the specific details for the first object.

Type	Name
FullTextIndex	HumanResources.JobCandidate
FullTextIndex	Production.Document
FullTextIndex	Production.ProductReview

Type	Name
FullTextIndex	HumanResources.JobCandidate

Full-Text indexes Full-text index on [HumanResources].[JobCandidate] found.

## 5 最後に

Managed Instance については、これまでの SQL Database や SQL Database Elastic Pool に比べて、オンプレミスの SQL Server との高い互換性を持っている事は明らかである。また、移行に関してもこれまでの SQL Database と比べても柔軟に対応する事が可能であり、より PaaS 環境へ安心かつ安全な移行を可能とする。

一方で高い互換性を備えているとはいえ、完全にオンプレミスと同じかと言うとそういう訳ではない。違いを理解し、Managed Instance では実装出来ない機能をどのように Azure の他のサービスなどで置き替え可能かを検討する事も重要である。また、本文書内ではこれまで記載していないが、SQL Database は Managed Instance も含めて PaaS のサービスとなる。この為、障害が発生した場合は自動で速やかに復旧が行われ、また、データベースのそのものの最新化も基本的には自動的に実行される。こういった事項が発生すると、SQL Database ではセッションの一時的な切断などが発生するがこれは不具合ではなく、SQL Database の仕様通りの動きとなる。これらの動きも理解し、「一時的な切断」について、アプリケーション側で事前に考慮することも PaaS へ移行する際の重要な要素である。

- ・ [SQL Database] アプリケーション作成における推奨事項について (Microsoft Azure SQL Database)

<https://blogs.msdn.microsoft.com/jpsql/2014/10/22/sql-database-microso/>

- ・ SQL Database の SQL 接続エラーと一時エラーのトラブルシューティング、診断、防止

<https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-connectivity-issues>

- ・ Azure SQL Database との接続に関する一般的な問題のトラブルシューティング

<https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-troubleshoot-common-connection-issues>

- ・ SQL Database クライアント アプリケーションの SQL エラー コード: データベース接続エラーとその他の問題

<https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-develop-error-messages>

Azure SQL Database Managed Instance の特性、オンプレミスの SQL Server との違い、PaaS での利点と注意事項。ユーザがこれらを理解する上で本文書が助けになると幸いである。

## 6 参考

- 価格

<https://azure.microsoft.com/ja-jp/pricing/details/sql-database/managed/>

- マネージ インスタンス (プレビュー) とは?

<https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-managed-instance>

- 機能の比較: Azure SQL Database と SQL Server

<https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-features>

- Azure SQL Database マネージ インスタンスと SQL Server の T-SQL の相違点

<https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-managed-instance-transact-sql-information>

- Azure SQL Database マネージ インスタンスへの SQL Server インスタンスの移行

<https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-managed-instance-migrate>

- SQL Server を Azure SQL Database マネージ インスタンスに移行する

<https://docs.microsoft.com/ja-jp/azure/dms/tutorial-sql-server-to-managed-instance>

- Restore a database backup to an Azure SQL Database Managed Instance

<https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-managed-instance-restore-from-backup-tutorial>

- Azure Database Migration Service を使用して Azure SQL DB マネージ インスタンスを移行するためのネットワーク トポロジ

<https://docs.microsoft.com/ja-jp/azure/dms/resource-network-topologies>

- Azure SQL Database マネージ インスタンスの VNet を構成する

<https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-managed-instance-vnet-configuration>

- Azure SQL Database マネージ インスタンスのカスタム DNS の構成

<https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-managed-instance-custom-dns>

- Azure SQL Database マネージ インスタンスにアプリケーションを接続する

<https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-managed-instance-connect-app>

- Azure SQL Database マネージ インスタンスの監査の概要

<https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-managed-instance-auditing>

- Azure SQL Database マネージ インスタンスの脅威検出

<https://docs.microsoft.com/ja-jp/azure/sql-database/sql-database-managed-instance-threat-detection>

- 包含データベースでのセキュリティのベスト プラクティス

<https://docs.microsoft.com/ja-jp/sql/relational-databases/databases/security-best-practices-with-contained-databases?view=sql-server-2017>