DP-300
Microsoft Azure
SQL ソリューションの管理

Day 2 – (3)セキュリティ

※補足説明,対応ラボなし

ラーニングパス3　追加解説
※対応ラボなし

- TLS（Transport Layer Security）
- TDE （Transparent Data Encryption）
- Always Encrypted
- 動的データマスク

ラーニングパス3　追加解説
※対応ラボなし

- TLS（Transport Layer Security）
- TDE （Transparent Data Encryption）
- Always Encrypted
- 動的データマスク

TLS (Transport Layer Security)

- データを暗号化して送受信するプロトコル
- クライアントとサーバーの間の通信が暗号化され、第三者による通信内容の盗聴が不可能となる
- SQL Database、 SQL Managed Instance、 Azure Synapse Analytics では、 すべての接続に対して **常に** 暗号化 (SSL/TLS) が適用される。
  - 接続文字列の設定（`Encrypt` または `TrustServerCertificate`）に**関係なく**、すべてのデータがクライアントとサーバー間の "移動中" に暗号化されることが保証される。
- Azure SQL Database, Azure SQL Database Managed Instance, SQL Server (on Azure VM)で利用可能
- 無料

ラーニングパス3　追加解説
※対応ラボなし

- TLS（Transport Layer Security）
- TDE （Transparent Data Encryption）
- Always Encrypted
- 動的データマスク

TDE（Transparent Data Encryption）

- 保存データを**透過的に**暗号化（アプリケーションの変更は不要）
- ページ レベルでデータの暗号化と暗号化解除が実行される
  - 各ページは、メモリに読み込まれるときに暗号化解除され、ディスクに書き込まれる前に暗号化される
- 無料
- Azure SQL Database / Azure SQL Managed Instance では、（新規に作成されるデータベースでは）デフォルトで有効化される
  - 暗号化に使用する証明書はデフォルトではサービスによって管理される
- SQL Server (on Azure VM)では、SQLを実行してTDEを有効化する
  - 暗号化に使用する証明書はSQLで指定する

■ Azure SQL DatabaseでのTDEの有効化

■ SQL Server (on Azure VM)でのTDEの有効化

```
USE master;
GO

CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<UseStrongPasswordHere>';
GO

CREATE CERTIFICATE MyServerCert
    WITH SUBJECT = 'My DEK Certificate';
GO

USE AdventureWorks2022;
GO

CREATE DATABASE ENCRYPTION KEY
    WITH ALGORITHM = AES_256
    ENCRYPTION BY SERVER CERTIFICATE MyServerCert;
GO

ALTER DATABASE AdventureWorks2022
    SET ENCRYPTION ON;
GO
```

ラーニングパス3　追加解説
※対応ラボなし

- TLS（Transport Layer Security）
- TDE （Transparent Data Encryption）
- Always Encrypted
- 動的データマスク

Always Encrypted

- 機密データをデータベース エンジンに送信する前に**クライアント側で**暗号化する機能
- 悪意のある内部関係者によるデータ盗難のリスクが軽減される。
  - 悪意のある内部関係者がDBのデータを読み取る権限を持っている場合、その権限を悪用してデータを盗難する可能性がある。
  - Always Encryptedで保護されたデータはクライアント側で暗号化済みのため、そのデータを盗難しても内容を読み取ることができない
- Azure SQL Database, Azure SQL Database Managed Instance, SQL Server (on Azure VM)で利用可能
- 無料

動的なデータ マスキング(DDM)

- データが表示される際にマスクをかける。090-1234-5678 → 090-XXXX-XXXX 等
- DDM によって、データベース内のデータが変更されることはない。
- 悪意のある内部関係者によるデータ盗難のリスクが軽減される
- Azure SQL Database, Azure SQL Database Managed Instance, SQL Server (on Azure VM)で利用可能
- 無料

ラーニングパス3　追加解説
※対応ラボなし

- TLS（Transport Layer Security）
- TDE （Transparent Data Encryption）
- Always Encrypted
- 動的データマスク

■DDM有効化時のSELECT文の実行結果例