#4 Azure Active DirectoryとAzure AD Connect

株式会社grasys

INDEX

1.はじめに

本書の主な想定読者

- Active Directoryドメインサービスをすでに社内に導入しており、クラウド活用の検討に関わる方
- ハイブリッドクラウドのID運用方法を考えている、IT部門の方

本書の目的・ゴール

社内でAzure ADを利活用するイメージをつかみ、検討を行えること

2.比較検討が難しい3大クラウド：Azureが向いている企業は？

Amazon Web Services (AWS) や Google Cloud をはじめとして様々なクラウドサービスが存在しており、どのクラウドサービスが良いか比較し、頭を悩ませている企業は多いです。
特に3大クラウドは、提供しているサービス内容もよく似ており、下記のサービスを使う上では大きな差がないのが現状です。

サービスの一例
- 仮想マシン
- ストレージ
- データベース
- コンテナー
- ネットワーク
- 機械学習
- ブロックチェーン
- IoT

など

他のクラウドサービスと比較した時に、Azureの特長がいくつかあります。

・オンプレミスとの結合に強い（ハイブリッドクラウド）
・金融、航空、電力など、堅牢性が高いシステムに向いている
・標準で日本法に準拠

特に、下記に当てはまる企業は、Azureが選択肢となり得ます。

・オンプレミス環境ですでにWindows Serverベースのサーバーを利用している
・クラウド上の仮想マシンのOSとしてWindows 10を使用したい
・Microsoft 365などのMicrosoft製品との連携を考えている

特に、Windows ServerでActive Directoryによる管理を行っている場合は、Azureと組み合わせるメリットが大きいです。
まずは、Azure Active Directoryがどのようなものなのか見ていきましょう。

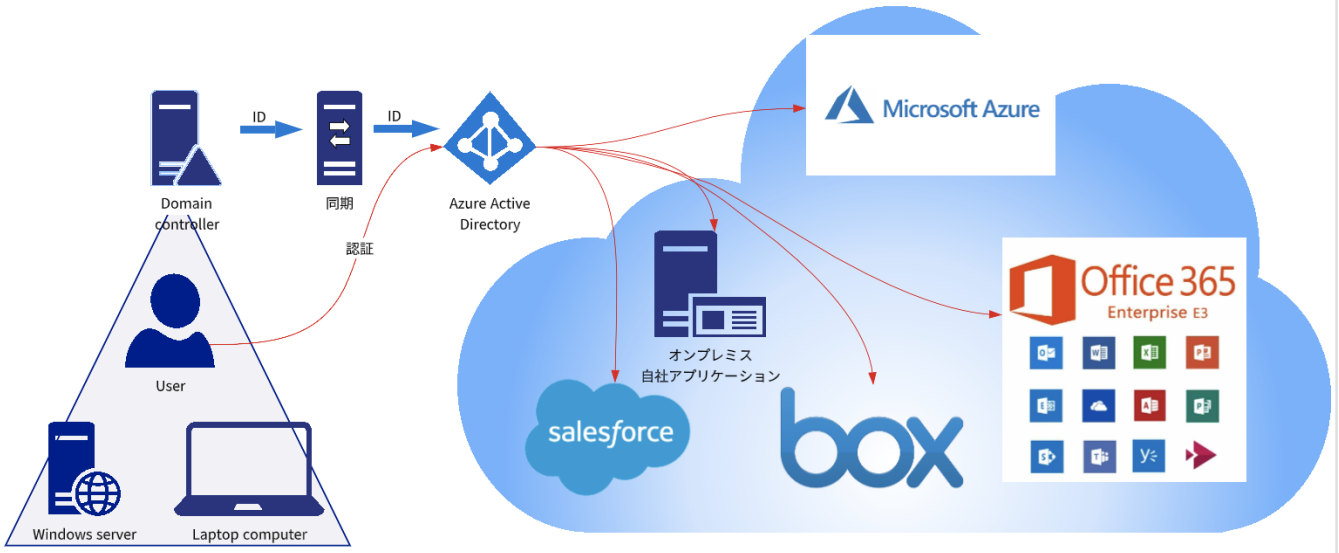
3.Active Directory(AD)と Azure Active Directory (Azure AD)の違いとは？ ～Azure Active Directoryで実現できること～

どちらもActive Directoryと名前がついていて、機能も似ていますが、その管理方法や管理する範囲は異なります。
AD DSが社内ネットワーク内のユーザーとコンピュータを管理する認証基盤なのに対し、Azure ADはクラウドベースのIDおよびアクセスを管理するサービスです。

Azure ADは、ユーザーIDの一元管理・シングルサインオンの実現・組織IDの管理・IDの防御・仮想マシン用ドメインサービス・デバイスの管理、などの組織向けの各種管理機能を持ちます。
このサービスは、従業員がMicrosoft 365や、Azure portal やその他のさまざまな SaaS アプリケーションなどの外部リソースにアクセスするのに役立ちます。

Azure ADを使用して共通認証基盤にすることで、IT部門の運用業務を軽減することができます。各種SaaSサービスのログインをシングルサインオン機能で一元管理することで、従業員は複数のIDを持つ必要がなくなり、パスワードリセットの対応回数を減らせます。さらに、新しいクラウドサービスを利用し始める際も、グループ単位で権限を付与するなど、導入が容易になるメリットもあります。

また、不審なアクセスへの検知とロックアウト、多要素認証機能の追加など、Azure ADの機能を使ったセキュリティ面の強化を行うことも可能になります。



1つのID で様々なクラウドサービスへアクセス可能にするイメージ

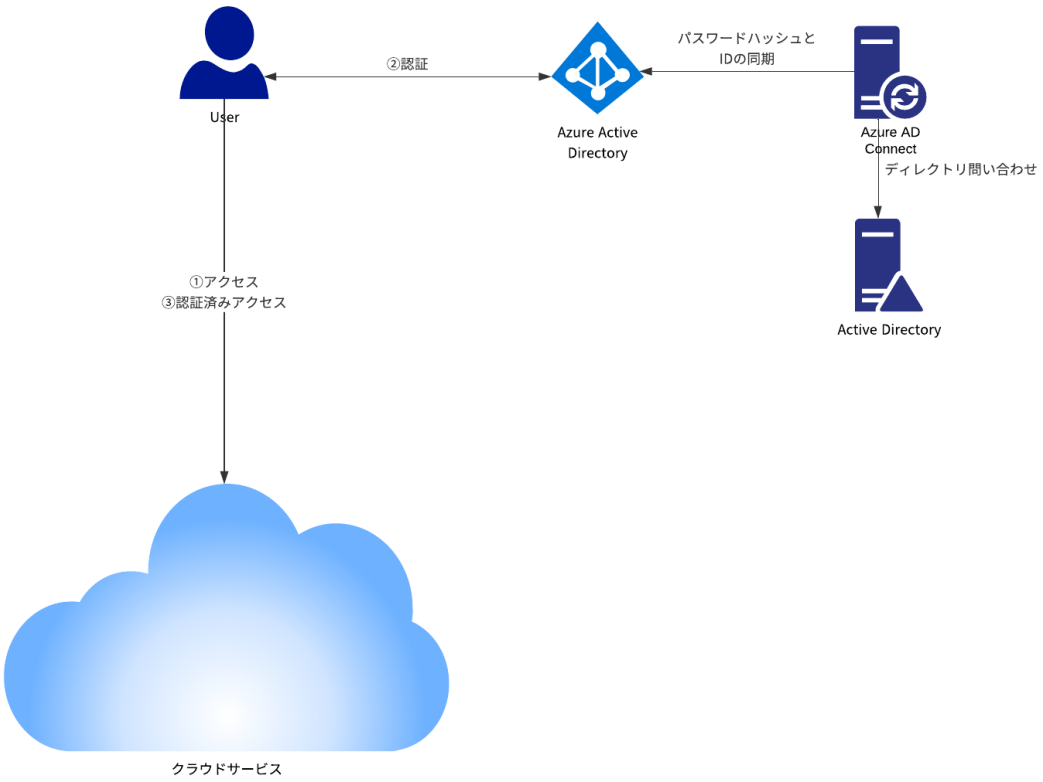
4.Azure AD Connectを使うメリット

AWSやGoogleCloudのID管理でも同様のことが行えますが、Azureの場合はAzure AD Connectを使用することで、ADに登録されているアカウント情報をそのまま利用し、クラウドとオンプレミス全体のすべてのアプリに対してID管理を行えるようになります。

ADとAzure ADの間で同期を取るサービスが、Azure AD Connectです。

5. 認証方式比較

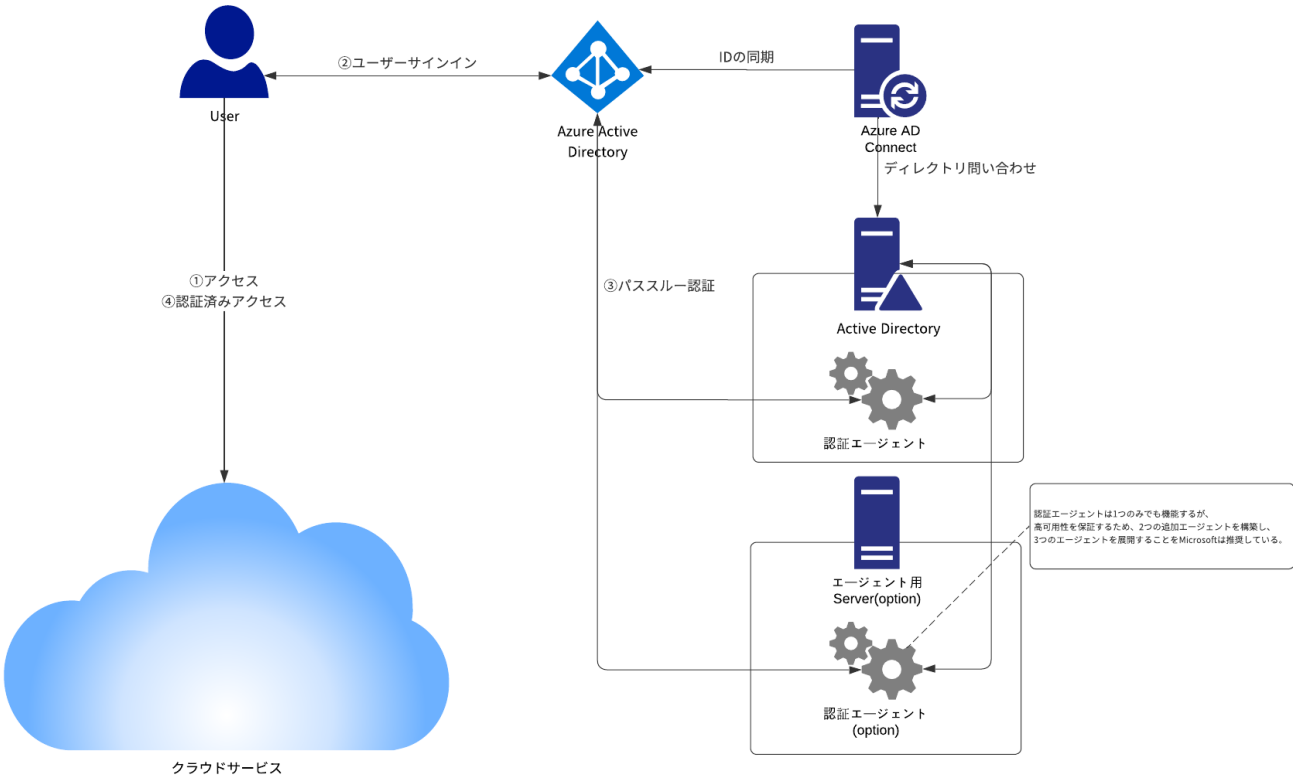
5-1.パスワードハッシュ同期方式



1. クラウドサービスにアクセスする
2. 未認証の場合、Azure ADへ資格情報の入力し、Azure ADでユーザー認証を行う
3. 認証された状態でクラウドサービスにアクセスする

3つの方式の中でもっともシンプルなのがこのパスワードハッシュ同期方式です。
IDとパスワードハッシュを用いてAzure ADで認証を行うため、オンプレミス環境と通信が取れない状態でもAzure ADのみで認証・認可を行うことができます。
そのため、他の方式でも認証システムの不具合時のバックアッププランとして、併用されるケースもあります。
一方、パスワードハッシュをクラウド上に保存することが適さないケースでは、パススルー認証方式やフェデレーション方式が取られます。

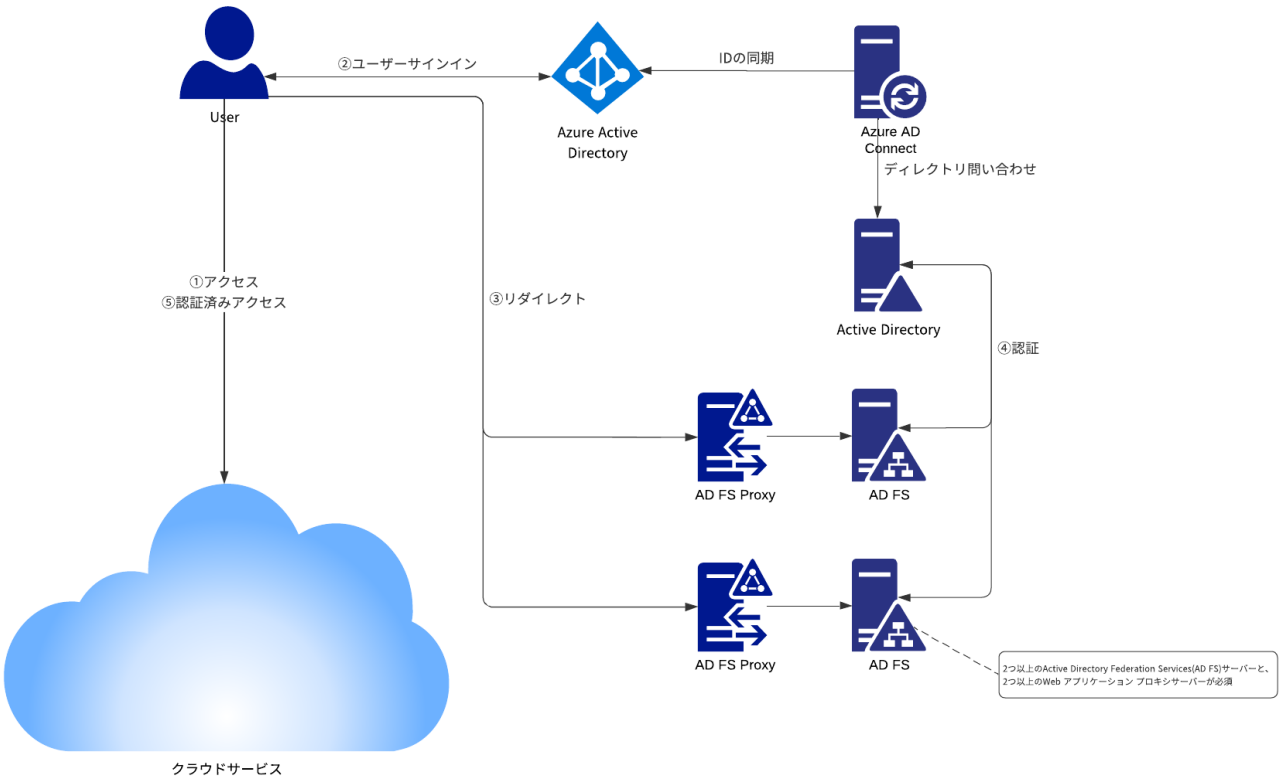
5-2.パススルー認証方式



1. クラウドサービスにアクセスする
2. 未認証の場合、Azure ADへ資格情報の入力する
3. Azure ADから認証情報をActive Directoryに送り、Active Directoryでユーザー認証を行う
4. 認証された状態でクラウドサービスにアクセスする

認証をオンプレミス上のADで行う方式です。
パスワードハッシュはAzure AD上に保持しません。
セキュリティポリシーの適用条件によっては選択される場合があります。

5-3.フェデレーション方式

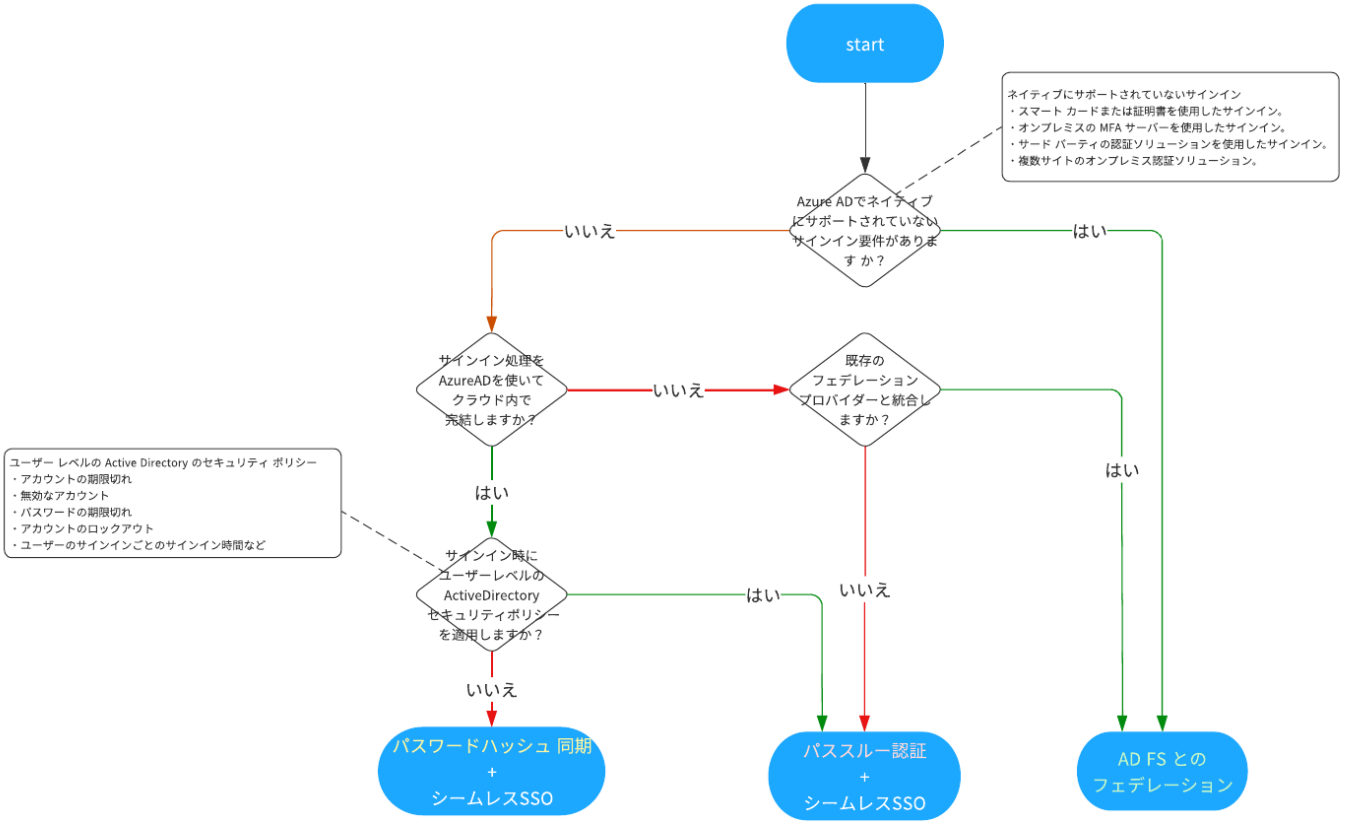


1. クラウドサービスにアクセスする
2. 未認証の場合、Azure ADへ資格情報の入力する
3. Azure ADが認証先として指定する、AD FSのWAPへリダイレクトする
4. Active Directoryでユーザー認証を行う
5. 認証された状態でクラウドサービスにアクセスする

認証をフェデレーションシステムで行う方式です。
パスワードハッシュはAzure AD上に保持しません。
また、フェデレーションシステム独自のサインイン機能を使用することが出来ます。

5-4.どのように選択するか？

既存の状態・セキュリティ要件に応じて、どの方式を取るべきかは異なります。



6.Azure AD活用事例

Microsoftの公開情報より、Azure ADを活用した事例をピックアップしました。

公立大学法人 北九州市立大学 様:
　学内で使用している Microsoft Office 365 とのシングル サインオンを実現
https://customers.microsoft.com/ja-jp/story/819450-university-kitakyushu-jp-japan

国立大学法人名古屋工業大学 様:
　Azure ADを活用し、全学的な認証基盤そのものをクラウドに移行
https://customers.microsoft.com/ja-jp/story/1368257927380855682-nagoya-institute-of-technology-higher-education-microsoft365-jp-japan

花王株式会社 様:
　セキュアな状態のまま、モバイル デバイスや在宅環境から社内システムへのアクセスを実用化
https://customers.microsoft.com/ja-jp/story/1470730537447118501-kao-consumer-goods-microsoft-365-ja-japan

株式会社ゲームスタジオ 様:
　開発環境のシングル サインオンの実現
https://customers.microsoft.com/ja-jp/story/1364935832890127585-game-studio-gaming-azure-jp-japan

株式会社東京スター銀行 様:
　ユーザー ID を保護し、ID ベースのリスクの検出や修復なども自動的に行える認証システム
https://customers.microsoft.com/ja-jp/story/819758-the-tokyo-star-bank-limited

免責事項

本書は、2022年4月時点の情報を元に作成しています。
内容については万全を期しておりますが、疑問点やご指摘などがございましたら下記へ御連絡頂けますようお願い申し上げます

本件に対するお問合せは、
お問合せフォーム まで