

グローバル拠点のオンプレADとAzure Active Directoryの同期、ユーザー情報とデバイス情報の連携、デバイスのIntuneでの管理

業種	運輸業
目的	既に Azure Active Directory を利用して MS365 からメールを利用している。しかし、オンプレミス環境にもメールアドレスがあるため、Azure Active Directory のメールアドレスを利用するように統一したい。
作業規模	拠点数 国内外 3 拠点
作業ボリューム	作業期間 3 カ月間(工数 約 3 人月)
作業内容	グローバル拠点のオンプレ AD と Azure Active Directory の同期、ユーザー情報とデバイス情報の連携、デバイスのIntuneでの管理

今回ご紹介する事例のお客様は、運輸業でグローバルに拠点を持つお客様企業です。オンプレ ADとAzure Active Directory を同期させ、ユーザー情報とデバイス情報を連携し、デバイスをIntuneで管理できる環境づくりを、弊社IIMヒューマン・ソリューション株式会社(通称 IHS)が日本語・英語の 2 か国語でご支援した事例となります。

背景

昨今、IT環境のクラウド化において、まずはオンプレとクラウドを同期してデバイスを管理し、完全クラウド移行は将来の課題とするケースが増加しております。

今回ご紹介する事例のお客様は、運輸業でグローバルに拠点を持つお客様企業です。

お客様は東京やアジア、ヨーロッパに拠点があります。そして過去に複数の会社が合併した経緯があり、現在の新しい企業ドメインではなく、複数の古いドメインをオンプレ環境で使用していました。それを Azure Active Directory のメールアドレスに統一し、Intune でデバイスを管理したいというご要望がありました。

弊社はこのようなお客様のIT環境において、オンプレADと Azure Active Directory を同期させる Hybrid Azure AD join を構築しました。そしてユーザー情報とデバイス情報を連携し、デバイスを Intune で管理できる環境づくりを、日本語・英語のバイリンガルでご支援いたしました。

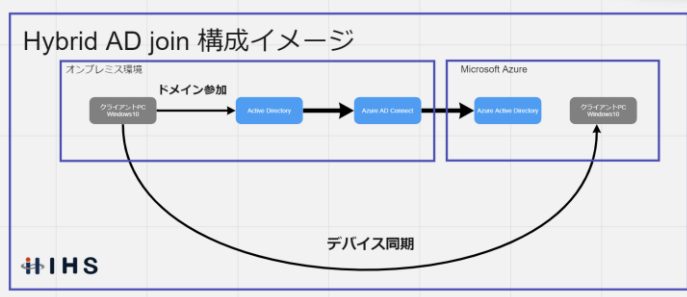


図 : Hybrid Azure Active Directory join

お客様が本件で弊社を選んだ理由

1. 実績

直近に総合電機メーカー様にて Azure AD Connect の環境を作っており、認証基盤まわりの知見が豊富にありました。そのため、お客様のご相談に対し、構成を見て即時に受け答えができ、お客様の環境を理解した上で具体的なすり合わせを行うことができました。

2. より安価なコスト

競合 Sier の見積もりに対し弊社の提案は安価でした。弊社はお客様の最終ゴールに合わせて構成検討と提案を行いました。大手 Sier はパッケージでのサービス提供となり、それ以外はすべてオプションとして価格が高くなっていくケースが多いのですが、弊社はお客様に合わせて必要な作業に絞って提案をしたため安価にできたのではと考えています。

3. 適切かつ具体的な提案

構築前、ご提案の時点で、弊社は本件に関わる複数の会社ごとの利用状況や登録状況を整理し、ある程度の仕様を固めておりました。初めてご支援させていただくにあたり、お客様が実現したいことに対して、弊社は実績を踏まえ、お役様の環境を詳細に把握した上で、お客様に納得していただける提案ができました。

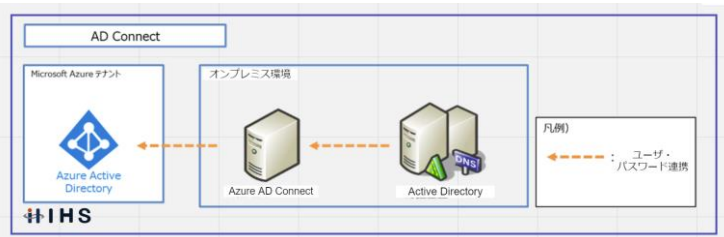


図 : AD Connect

アピールポイント

1. 日本語・英語の2か国語でのプロジェクト進行

グローバル企業様の海外拠点をまたがる案件で日本語、英語の2か国語にてスムーズにプロジェクトを進行できました。必要に応じて、海外拠点の方と直接メールでやりとりを行い、会議の際には日本法人のお客様と同席いただき、同時通訳をしていただきました。

すべてのドキュメント(基本は日本語)に英語の備考を付けて送っていました。

2. 柔軟性

プロジェクトの進行中、お客様の完全な把握を経ていない部分に対する新たな要望が発生しましたが、新たに確認された環境情報に適応し、適切な提案と対応を行いました。これらの追加要件により費用が増加し、スケジュールの変更も必要でしたが、柔軟に対応し、お客様の希望納期内でプロジェクトを完遂しました。

3. 必要最低限のコスト

前述のお客様に合わせた構成検討に加えて、ドキュメントについてもお客様に確認して必要と判断されたもののみ納品していることも、コストが安価となっている理由と思います。過剰なドキュメントをつくって価格を上げるようなことをしておりません。

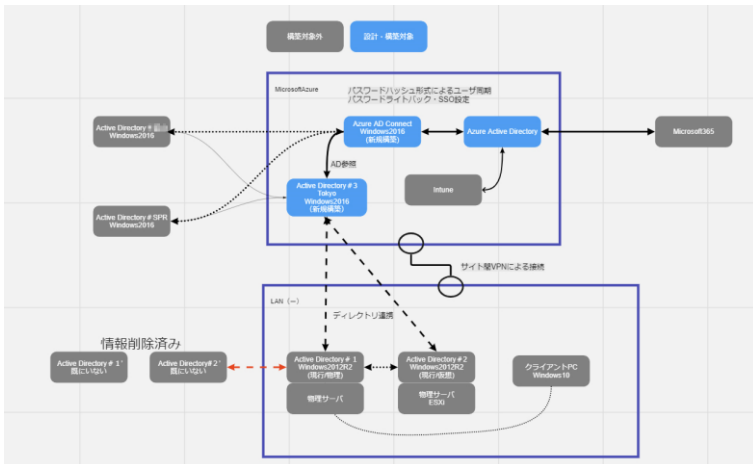


図: 海外拠点も含めたActive Directory、Azure AD Connect、Azure ADの相関図
(ユーザーと認識合わせの際に作成)

作業内容の詳細

1. 設計

・現行環境の状況整理

- 海外拠点のActive Directoryの利用状況や、制約事項を整理します。

・Azure ADとオンプレActive Directoryの連携アカウント属性設計

- Azure Active Directory上に存在するユーザーアカウントの属性情報とオンプレActive Directoryのユーザーアカウントの属性情報を整理します。連携を希望する属性情報を洗い出し、どの属性がAzure Active DirectoryのUPNと連携するのかを決定します。また、連携する属性情報をCLIによる一括設定ツールも提供しました。

・Azure AD Connectの設定

- 運用を考慮した同期周期や同期対象のOUを整理します。さらに、シングルサインオン方式の決定、ハイブリッドAzure AD参加のための同期オプション構成も行います。

2. 環境構築

・Azure VM (Windows Server OS) の初期構築

- ドメイン参加や環境共通の設定を実施します。

・Active Directory サーバの構築

- Azure環境のサーバにActive Directory機能の追加
- DNS設定情報修正
- 同期用にOU構成の修正
- GPO設定

・Azure AD Connect サーバの構築

- Azure AD Connectの実装
 - ディレクトリ同期設定
 - シングルサインオンの設定
 - ハイブリッドAzure AD参加の設定

・テスト実施

- 構築したサーバ、機能の単体および結合テストの実施

3. 納品ドキュメント

・詳細設計書

- Azure VM (Windows Server)
- Azure AD Connect
- Active Directory

・評価仕様書兼報告書

- Active Directory
- Azure AD Connect
- Azure Active Directory

・操作手順書

- Azure AD Connect