

Azure, Teams, PowerPlatformに 関わる開発



株式会社QES

Copyright © QES Corp. All Rights Reserved.

会社概要

商号	株式会社QES
設立	1983年3月1日
資本金	2億5000万円
代表者	代表取締役社長 和智徳男
拠点	東京（本社）、大阪
売上高	108億円（2021年度）
従業員数	230人（2022年4月現在）
株主	株式会社 QUICK
関係企業	株式会社 日本経済新聞社
許認可	プライバシーマーク：10820787(08) ISO/IEC27001:2013 (ISMS) 一級建築士事務所：東京都知事登録第49085号 労働者派遣事業：派13-309151 他

QESの強み

豊富な経験と技術力	大規模な構築・移行 実績多数
システムソリューションでは、Microsoftソリューションは2003年から、仮想化への取り組みは2004年から、積み重ねた経験と技術があります。	システムソリューションでは、数千アカウントの構築や移行を行った実績が数多くあります。大規模構築、移行に対応できる能力に富んでいます。
提案・解決力	ワンストップで提供
システム、オフィスのソリューションで、幅広い製品を取り扱う中からお客様の目的に合わせたご提案をします。	システム、オフィスのソリューションで、お客様のご予算に合わせてハード、ソフトの選定から作業まで、ワンストップで対応することができます。


QESのサービス内容

仮想化・クラウドを利用したシステム構築、システム運用・保守サービスまで、業種業態を問わずお客様のビジネスをICTソリューションで支援致します。



株式会社QES 事業体制について

- QESは日経グループを代表するITベンダーとして、最新のインフラ基盤からクライアント、
- プログラム開発、納品後の保守運用まで、フルラインナップのサービス提供を行っております。

 株式会社QES	オフィスソリューション営業本部	ファシリティ・オフィスソリューション事業 ・本社・拠点移転PM, レイアウト変更工事, 設備工事... ※QESのバーチャルオフィスツアー実施中! ご興味あれば、 こちら 参照ください。
	システム基盤本部	AWS インフラ構築 ・サービス基盤 設計・構築 ・AWS基盤運用
	システムソリューション営業本部 ※弊本部	インフラ構築 (オンプレミス・クラウド) ・Microsoft 製品 (Active Directory, Exchange, SharePoint, ID統合管理 ...) ・Microsoft 365 導入支援 (Teams, Exchange Online, SharePoint ...) ・Microsoft Azure サービス 設計・構築 (基盤設計, 仮想マシン構築・移行, PowerPlatform, WVD ...) ・仮想基盤構築 (VMware, HCI ...) ・SKYSEA Client View 導入支援・サポート ・その他サードパーティ製品 導入支援 (i-FILTER, m-FILTER, FinalCode ...)
	システム開発本部	クライアント・モバイルデバイス ・PC調達・設計・展開 ・モバイルデバイス管理・展開
	サービスサポート本部	プログラム開発 ・Microsoft 製品を使ったID統合管理、ID同期・SSOソリューション ・SharePoint/Exchange の機能拡張開発 ・Microsoft 365 上でのパッケージ製品開発 ・Power Platform での教育、開発 ・マイクロサービスを使った開発 ・C, C++, C#, .NET ... ・Java, PHP, Perl, Ruby ...
		保守・運用サービス ・サポートサービス, コールセンター, システム・クライアント保守

Microsoft社関連の注力分野と事例紹介

Microsoft
Partner


Gold Collaboration and Content
Gold Data Analytics
Gold Datacenter

Microsoft
Partner


Silver Cloud Productivity
Silver Small and Midmarket Cloud Solutions
Silver Application Development

Power Platform

Power Platform とは

Power Platform は、Power Apps、Power Automate、Power BI、Power Virtual Agents なるクラウド製品群であり、データの収集から解析・可視化までローコーディングで実現できるクラウドプラットフォームです。



Power Apps

ローコード アプリ開発

Power Point の要領で画面を作成し、Excel関数レベルでアプリケーションを作ることができます。



Power Automate (旧Microsoft Flow)

業務ワークフローの自動化

Office365 内はもちろん外部のクラウドを含めたワークフローやデータの自動連携等を作成することができます。



Power BI

データの可視化

データを視覚的に見せることができるクラウド上のBIツールです。

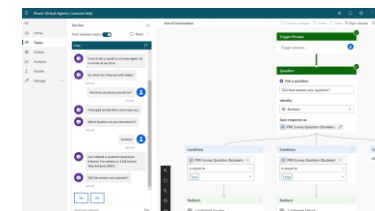
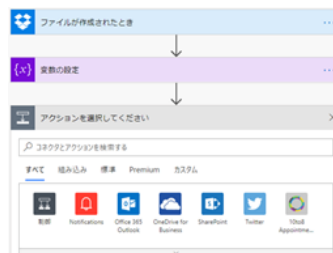
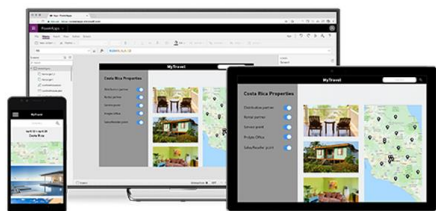


Power Virtual Agents

チャットボットの開発

コーディング不要でチャットボットを開発することができます。

Power Platform



QES の とりくみ

QES 提供 サービス

Microsoft との協業

QES は、技術/営業の両面で Microsoft と協業しております。
その経験を元に最適なソリューションの提案やサービスの提供が可能です。

Power Apps の公式セミナー

QES は、Microsoft に認定された公式のトレーナーです。
1日ハンズオンセミナー「App in a Day」の講師として様々な業種のお客様に向けて Power Apps のトレーニングを行っております。

AppSource へのアプリ公開

QES オリジナルアプリを AppSource に公開し、新規顧客の獲得・アプリの販売を行っております。
(AppSource … Office 365 上で利用可能な業務アプリケーションを公開する、所謂アプリネットショップ)

サポート&アプリカタログサービス **NEW!**

「技術サポート」と「アプリカタログ」を組み合わせ、Power Platform 環境の導入・活用と DX を支援します。

コンサルティング (SES)

お客様が導入を検討しているシステムについて、Power Platform で実現可能なソリューションをご提案します。
また、Power Platform の運用や管理方法等もご提案します。

アプリ / PoC 開発 (請負 / SES)

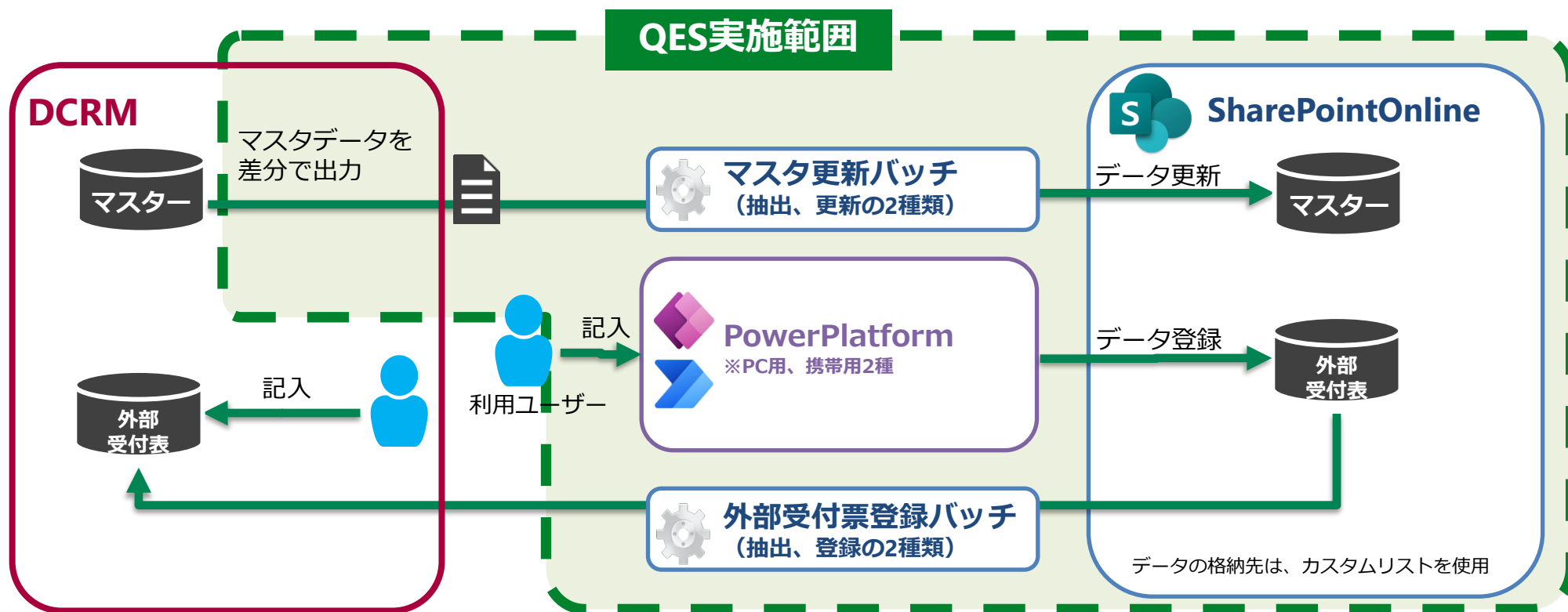
Power Platform を用いて、業務アプリケーションを開発します。
また、PoC での開発を行い、導入予定のシステムについて実用性や安定性・コスト面等で検証支援を行います。

教育 (SES)

Power Platform エンジニアの育成を目的に、お客様のレベルに合わせた教育を行います。
既存の教育メニューの他にオリジナルの教育メニューをご用意可能です。(1日~複数日可、費用面は別途相談)

特定のユーザが使用するCRM機能の一部をアプリ化

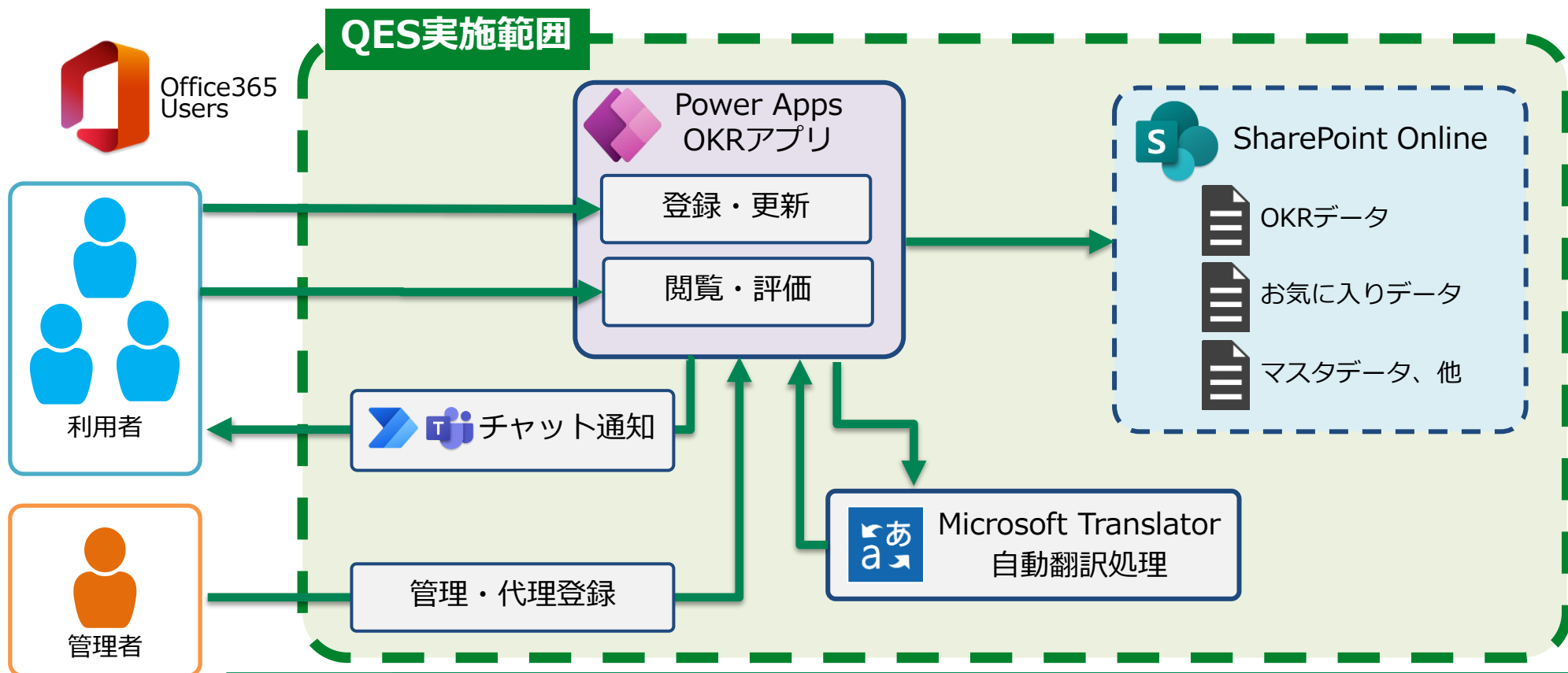
Dynamics CRMで行っていた商品のクレームや問合せ等の内容を登録する画面をPower Appsで構築。SharePoint Onlineに登録されたデータをDynamics CRMに連携することで、利用頻度が低いユーザーのDynamics CRMのライセンスが不要となり、ランニングコストの削減に成功した。



OKR (目標管理) 評価システム

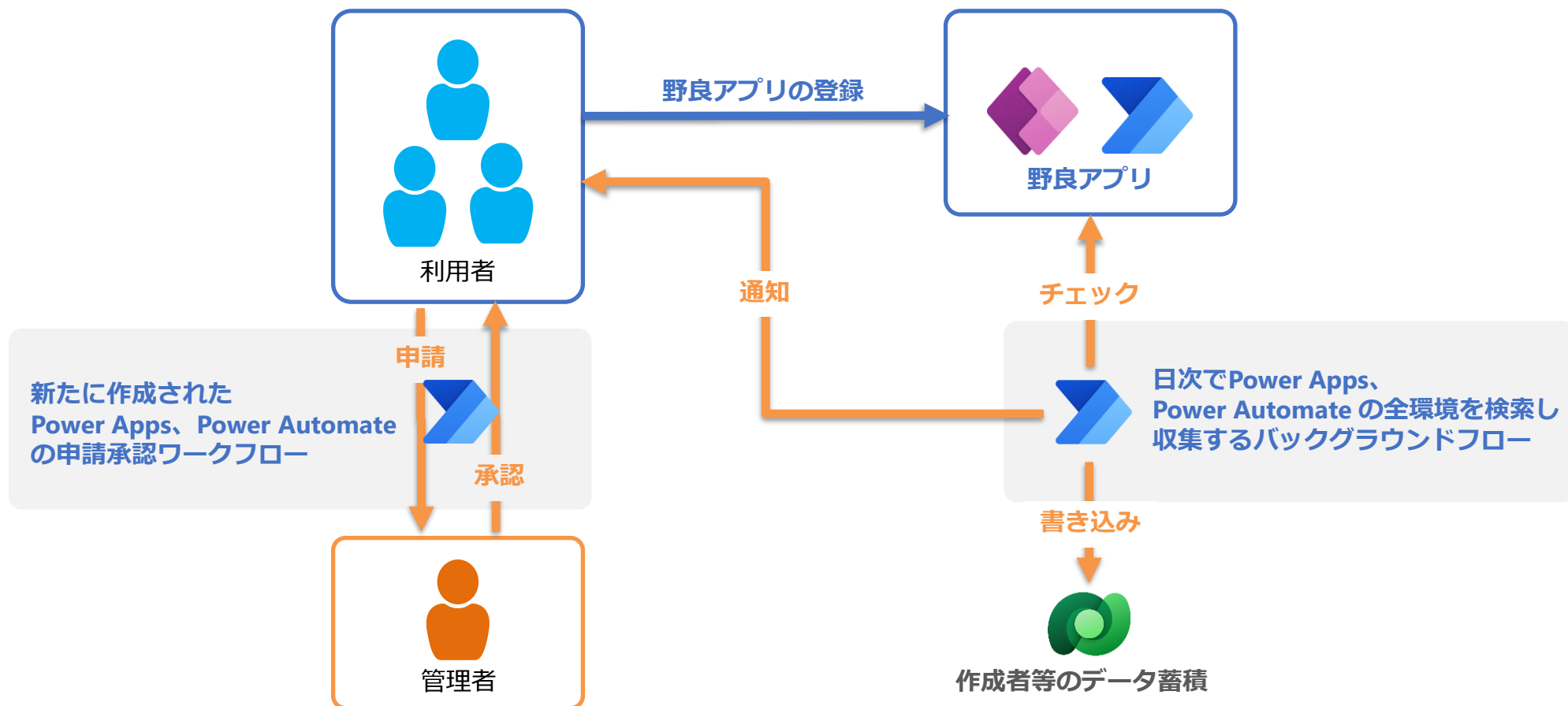
目標管理のデータを登録、公開、管理するシステムをPowerApps/PowerAutomate/SharePoint Onlineで構築。

最大3万人が利用するアプリをパフォーマンスを維持しつつ、追加ライセンス費用なしで実装を行った。グローバル対応のため自動翻訳、多言語機能を搭載した。



ガバナンス管理

ユーザー自身に申請を促すことでアプリの目的や用途を明確化させ、野良アプリを無くす仕組みを構築。運用や制度決めなどコンサルから開発までを担当。



Power Platform サポート&アプリカタログサービス

技術サポートに加え、カタログ化されたアプリケーションを無償利用できるサービス

「技術サポート」と「アプリカタログ」を組み合わせ、お客様 Power Platform 環境の導入・活用とDXを支援します。

技術サポートサービス

Power Platformに関する技術的な支援を実施いたします。契約しているコースに基づいてサポート時間が付与されており、その時間を消費することで様々なサポート提供します。

Q&A

技術的な質問に回答
手順やサンプルコードの提供
を行う

トラブル対応

トラブルの調査や解決策の提
示などを行います。

アプリ導入支援

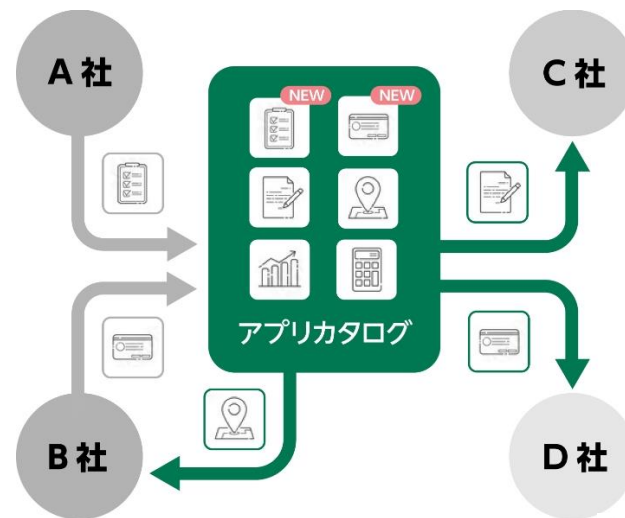
契約時間を消費することでア
プリカタログ内のアプリ導入
を支援します。

アプリ開発支援

契約時間を消費することでお
客様の要望に合わせたアプリ
ケーションを開発します。

アプリカタログサービス

本サービスを利用するユーザが作成したアプリを全顧客で共有し、相互活用します。全てのアプリを1から開発する無駄なコストを省き、継続的に利用できるアプリケーションを拡大することで、その課題を解決していきます。

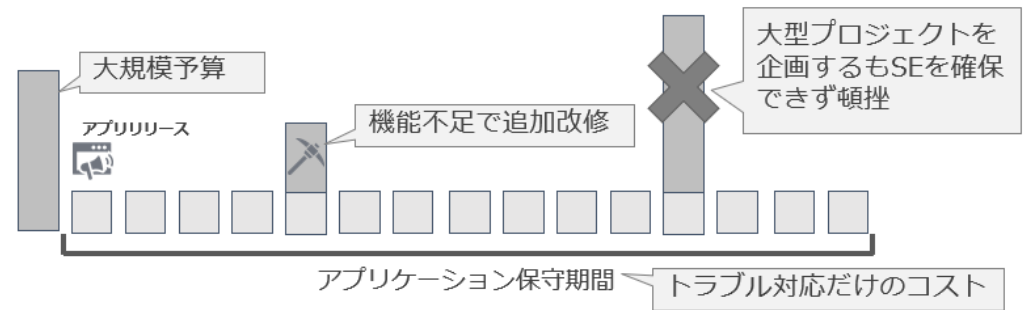


作ったものは共有
 必要なものは無料で利用

開発手法とコスト、得られるメリット

エンジニア確保が難しい、これからのアプリ開発は、発注元・開発元が協力し、コストを抑えながら利用者が本当に必要な機能を提供し、業務を改善し続けることが必要です。

従来型のアプリ開発



Power Platform と本サービスによるこれからのアプリ開発

アプリカタログを元にカスタマイズ



使いながら改善・改修・追加機能開発を継続(CI/CD)

ID統合管理

弊社はMIIS2003からID統合管理を行ってきた数少ないSIerです。

- ・ 対応可能Ver : MIIS、ILM、FIM、MIM
- ・ 規模 : ~50万ユーザ

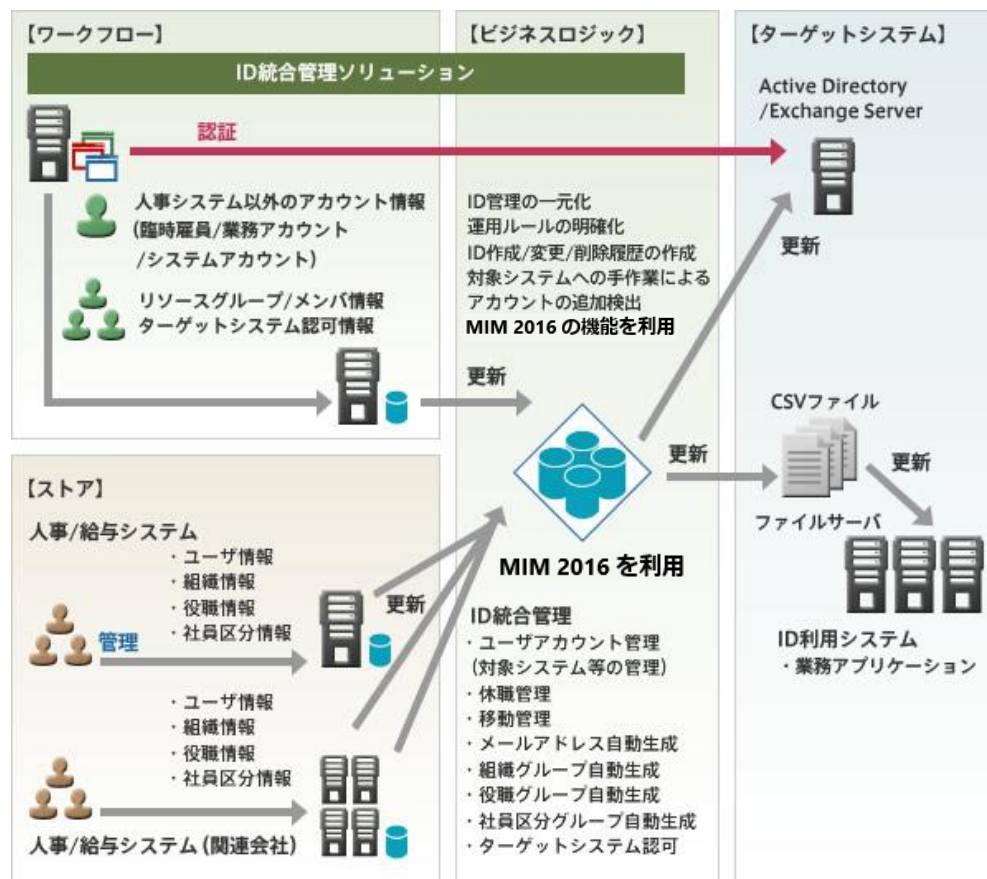
I D統合管理ソリューション全般

ID統合管理ソリューションは、ソースデータ（人事データや承認ワークフロー）をマスタデータとし、ターゲットシステム（ActiveDirectoryや業務システム）に適切なユーザ情報、権限情報、パスワードなどを自動連携するシステムです。

こんなお客様に最適！！

- アカウント情報や権限設定を手動でメンテナンスしているため、人事異動時にシステム管理者の負荷が高くなる。
- 退職したユーザのアカウントが残り続けたり、異動したユーザに異動前の権限が残り続ける。
- アカウントを作成した理由や証跡が残っていない。
- 複数システムアカウント/パスワードが異なっており、利用者が不便を感じている。

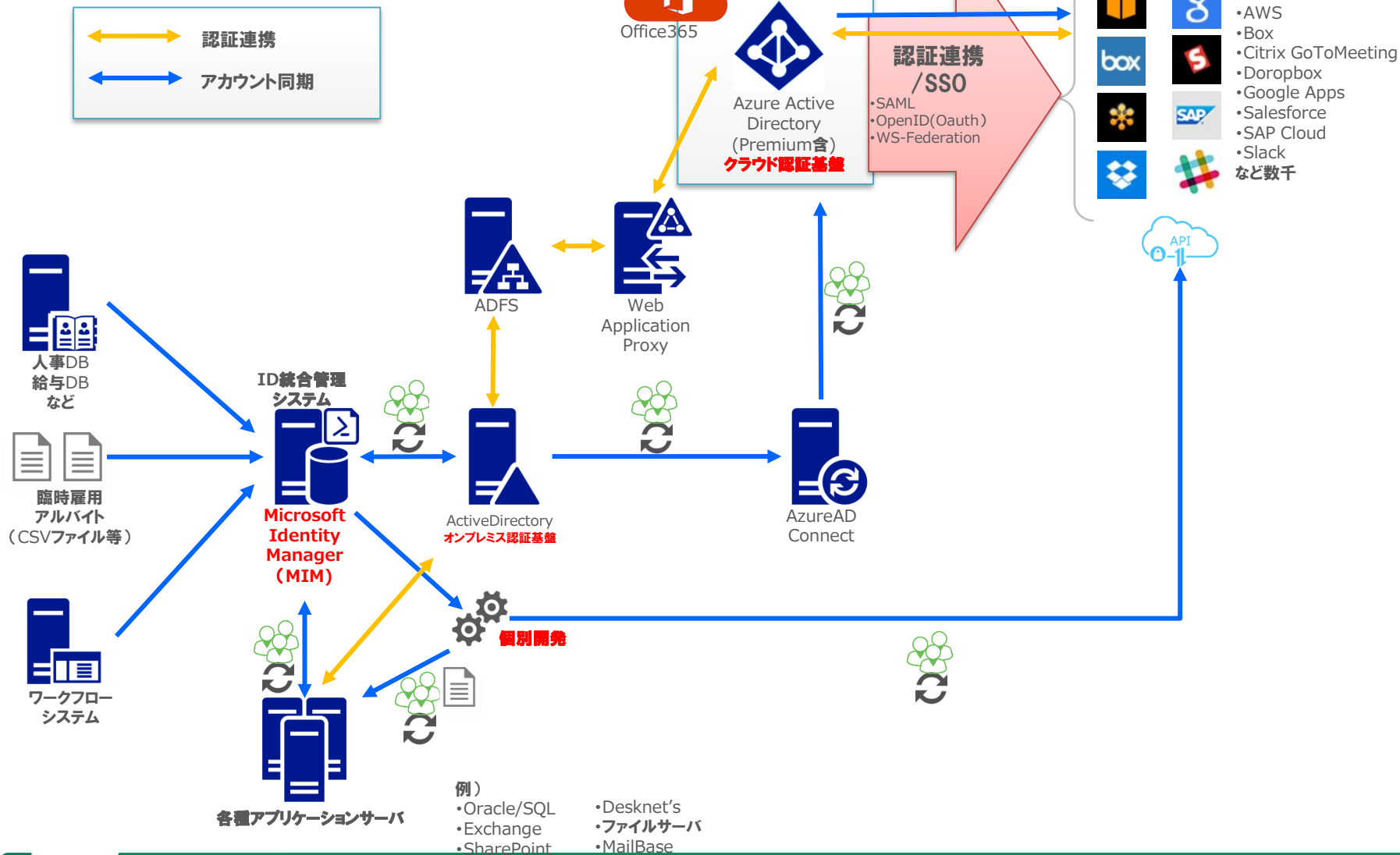
MIM 2016 を利用した場合の構成例



クラウド統合認証 クラウドアカウント連携

ID統合管理 + クラウド統合認証基盤

オンプレミスおよびクラウドのアカウント管理を統合し
プロビジョニングや変更処理、認証の連携/統合が可能となります。



クラウド統合認証基盤について

様々なクラウドサービスは、サーバ管理の手間が省け、インターネットさえあればどこからでも接続できるため非常に便利な反面、**ID管理が多重**になったり、**セキュリティリスク**が増すなど、**問題も多くなりがち**です。

- クラウドサービス利用における**統合認証基盤**を持つことで、**セキュリティリスクを排除し、ID管理をシンプル**にすることが可能です。
- Azure ActiveDirectoryを使うことで、他のクラウドサービスに対し、セキュリティレベルの高いシングルサインオン環境を実現することができます。
- クラウドとのアカウント連携は、Microsoft社のID統合管理システム（Microsoft Identity Manager（以下MIM））を中核に導入し、人事DB等から**オンプレミス/クラウドへのアカウント自動プロビジョニング**を可能にします。
- 年度末の**人事異動処理**や退職者の**棚卸作業**はもちろん、ファイルサーバのアクセス権管理やクラウドサービスのアカウント管理まで自動化することで、**大幅に作業コストや人的ミスを削減**することが可能です。

Microsoft社のID統合管理ソリューションに関する主な実績は以下の通りです。

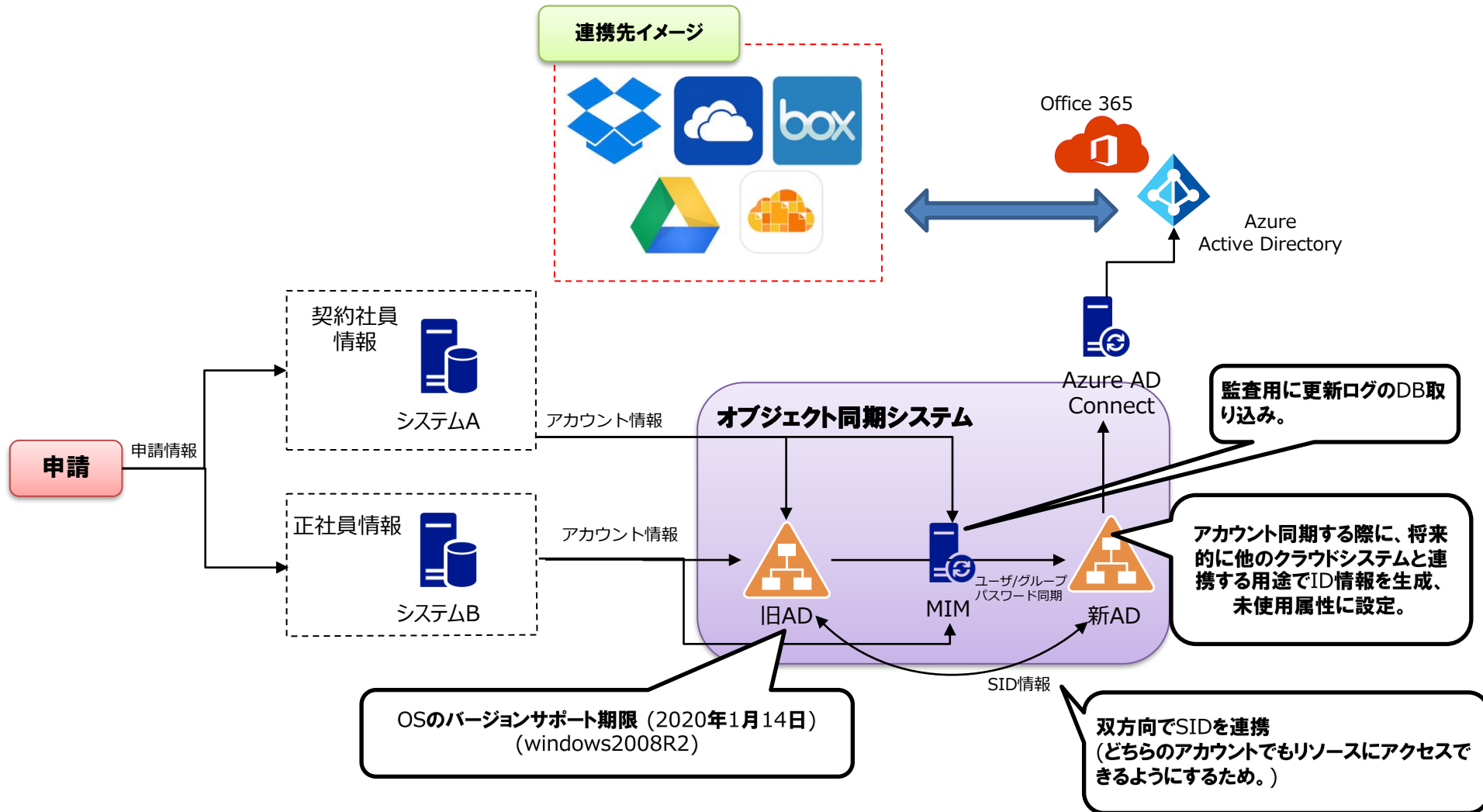
QESはMIIS 2003から着手し、現行のMicrosoft Identity Manager 2016 (MIM 2016) に至るまで、既に10年以上の実績がある数少ないベンダーです。

No.	ケース	業種	バージョン	オブジェクト数	同期元システム	同期先システム	その他備考等
1	人事連携	不動産	MIIS FIM	22,000	ワークフロー、人事CSV	AD、業務アプリケーション(9システム)	
2		公共	ILM MIM	5,000	CSV	AD、DB(2システム)、Exchange、CRM、MailBase、Desknet's	
3		公共	FIM	6,000	人事DB	AD、FS、SharePoint、Exchange、CSV(8ファイル)	個人組織フォルダ作成、権限設定
4		公共	フルスクラッチ	1600	DB、CSV	AD、Exchange	
5		銀行	フルスクラッチ	800	ワークフロー、部署マスタ	AD、Exchange、SharePoint、SQL Server、CSV	差分ソース
6	オブジェクト同期	運輸	MIM	66,000	AD、CSV	AD、SQL Server	
7		製造	MIM	20,000	リソースAD	AD、Office365	
8		製造	MIM	50,000	中間DB	AD、Office365、SQL Server	アドレス帳同期
9		精密機器	MIM	6,000	CSV	AD、Office365(5ドメイン)、Skype for Business	アドレス帳同期
10		金融	ILM FIM	1,500	人事DB	AD、業務システム	アドレス帳同期/アカウント同期/パスワード同期
11		金融	MIM	1,500	AD	業務システム	アカウント同期/パスワード同期
12		繊維	MIM	13,200	DB、CSV	AD、LDAP	
13		金融	MIM	500,000	Oracle(2システム)、ユーザCSV	AD、IBM Directory Server	パスワード同期

ID統合管理 代表的事例 1 運輸業 オブジェクト同期システム

旧ADから新ADに移行する際の、並行運用期間（数年間）におけるオブジェクト同期システム。
オブジェクト同期（ユーザ/グループ）と**パスワード同期**を行う。旧ADにオブジェクトが作成されてから、新ADに同期されるまでの時間が短くなることを求められていたため、短期サイクルの差分同期実行。

対応Ver：MIM
 規模：60,000ユーザ、6,000グループ

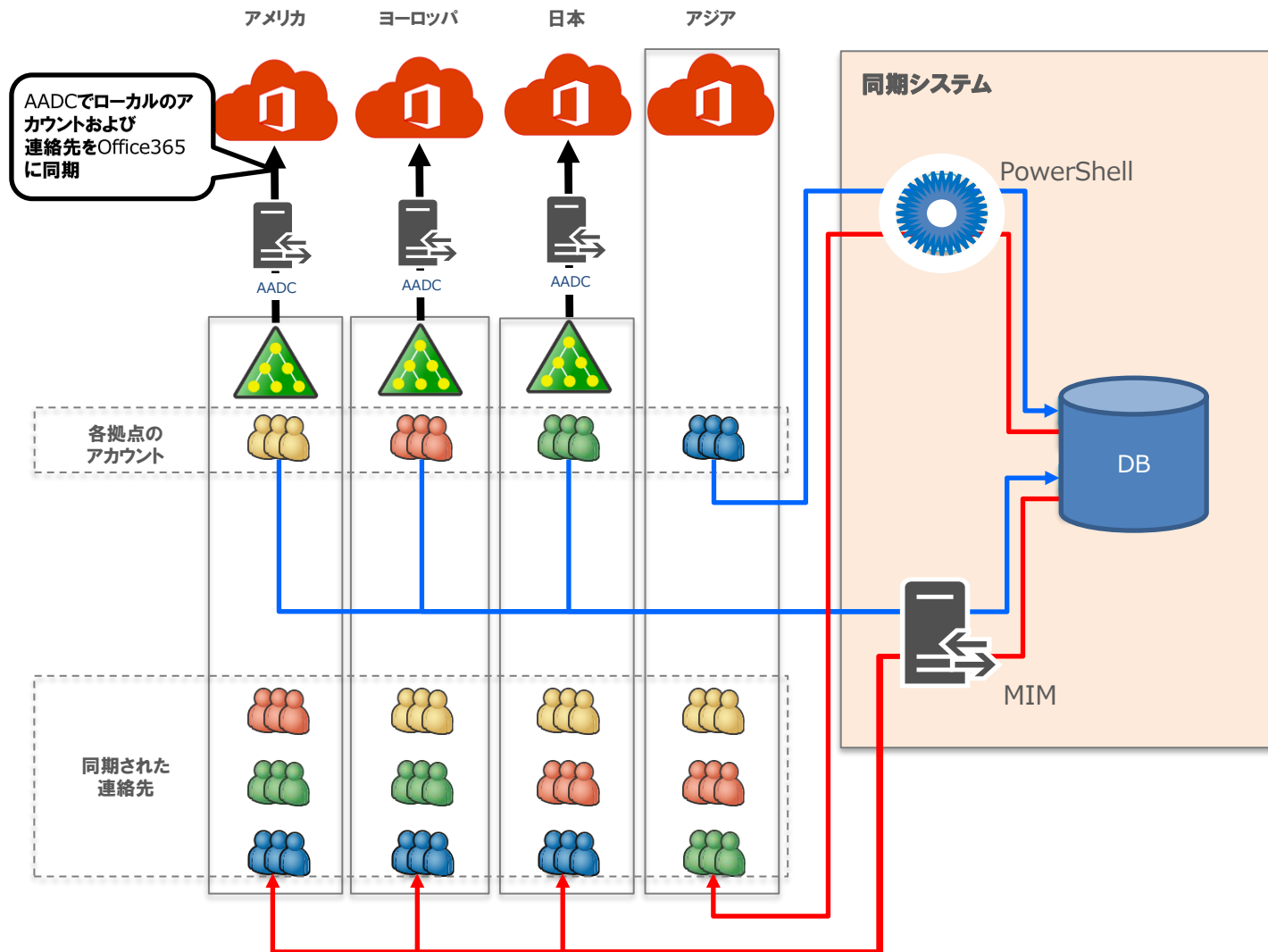


ID統合管理 代表的事例2 製造業 アドレス帳同期 (GAL同期) システム

各拠点が個別のOffice365テナントで管理するメールアドレス情報を連絡先として連携するシステム。

対応Ver : MIM

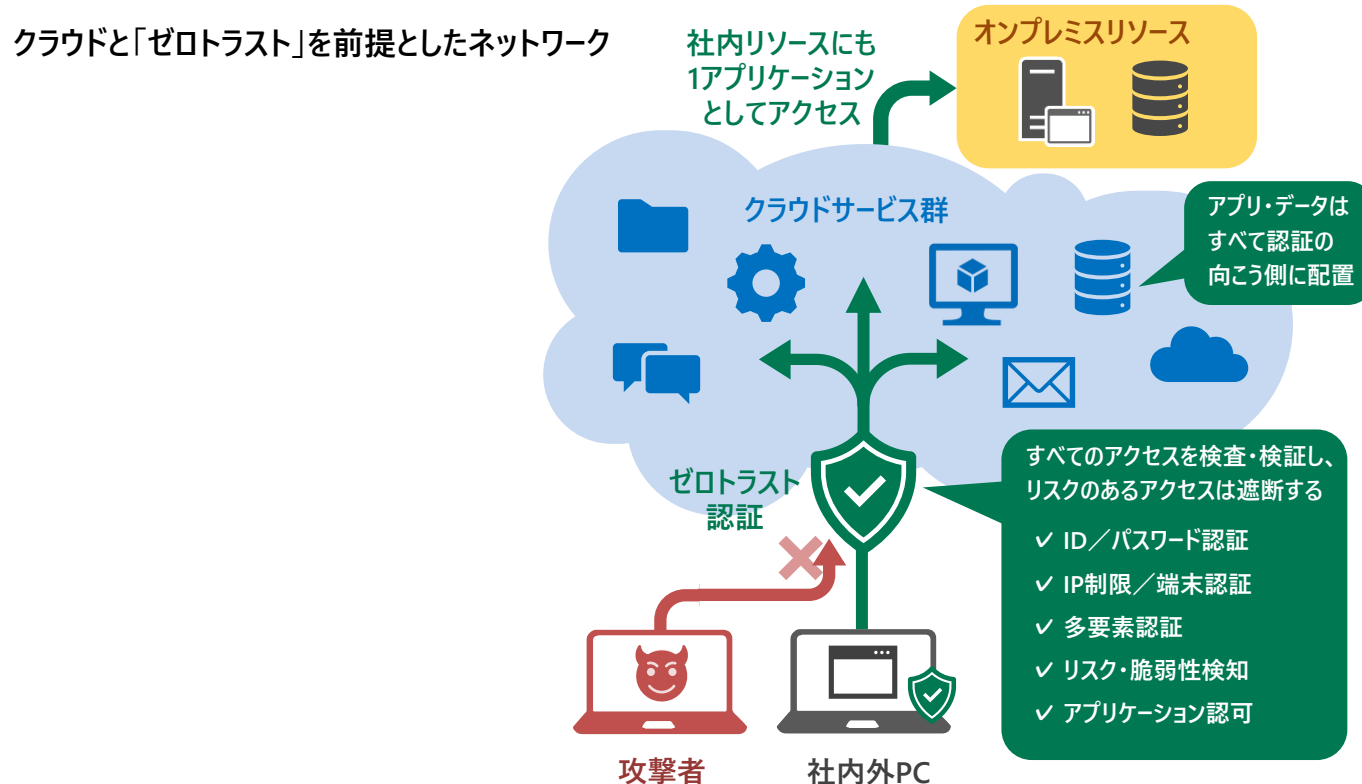
規模 : 50,000ユーザ (連携オブジェクトは、連絡先)



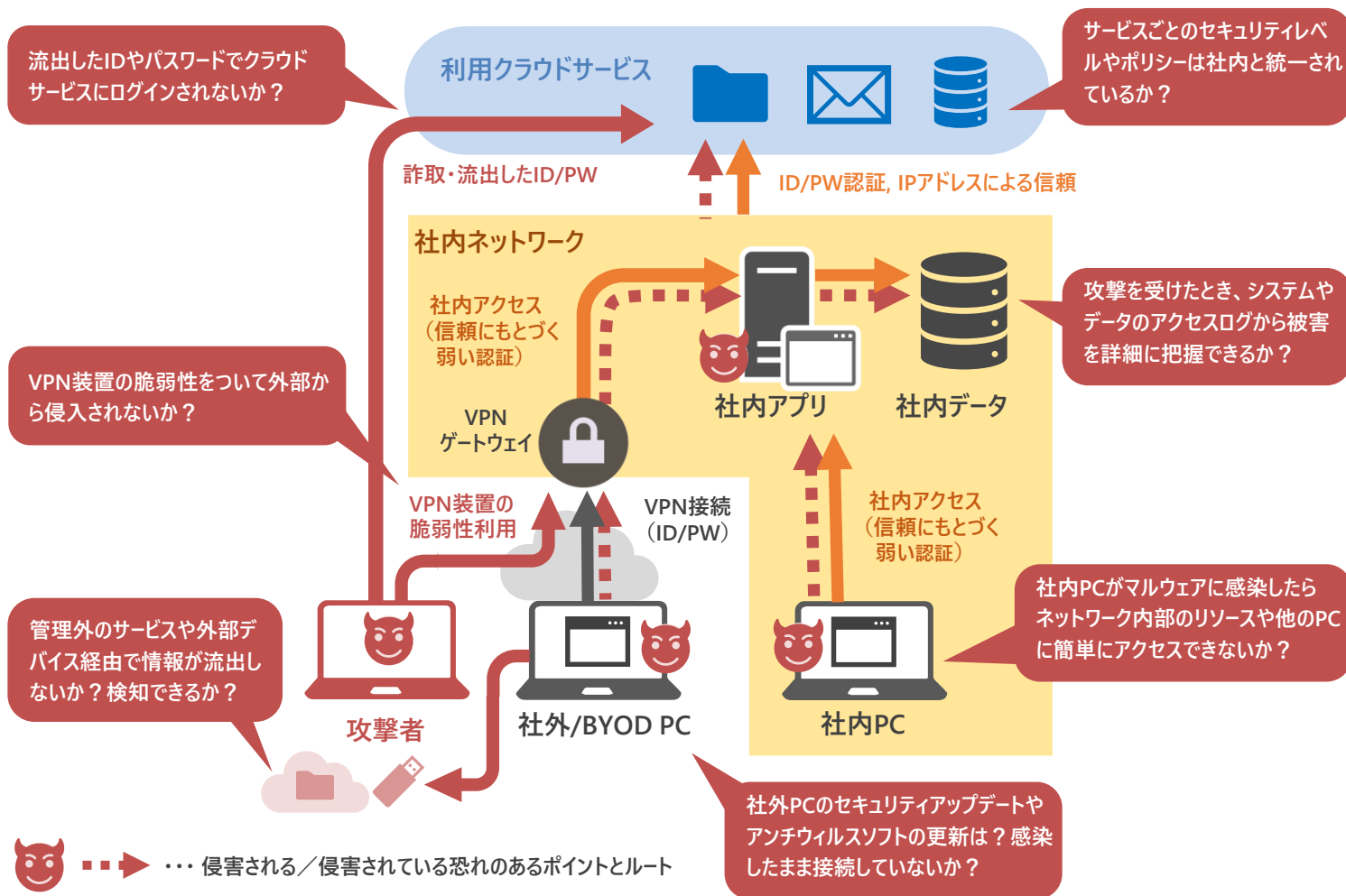
ゼロトラストネットワーク (MS)

ゼロトラストとは

「ゼロトラスト・セキュリティ」は米調査会社「Forrester Research」社が提唱した、複雑化し続ける企業のセキュリティ対策を整理・一本化する新たなフレームワークです。その名前（Zero-Trust）の通り、すべてのアクセスを信頼せず、統一した認証とポリシーでデータを守るのが考え方の基本となります。



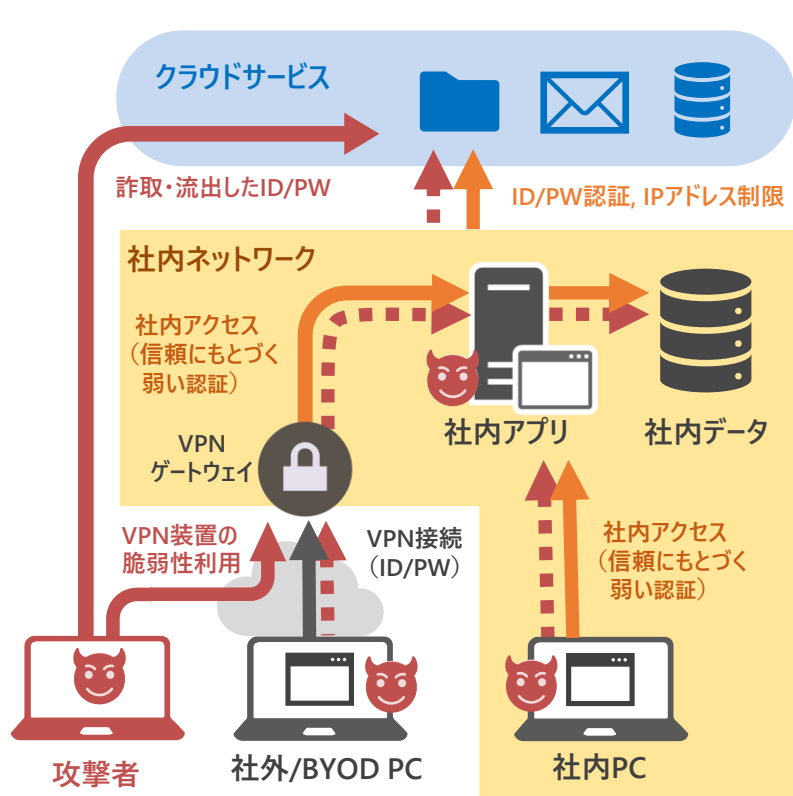
一般的な「境界型ネットワーク+クラウド」の企業が晒されているリスク・脅威のマップ



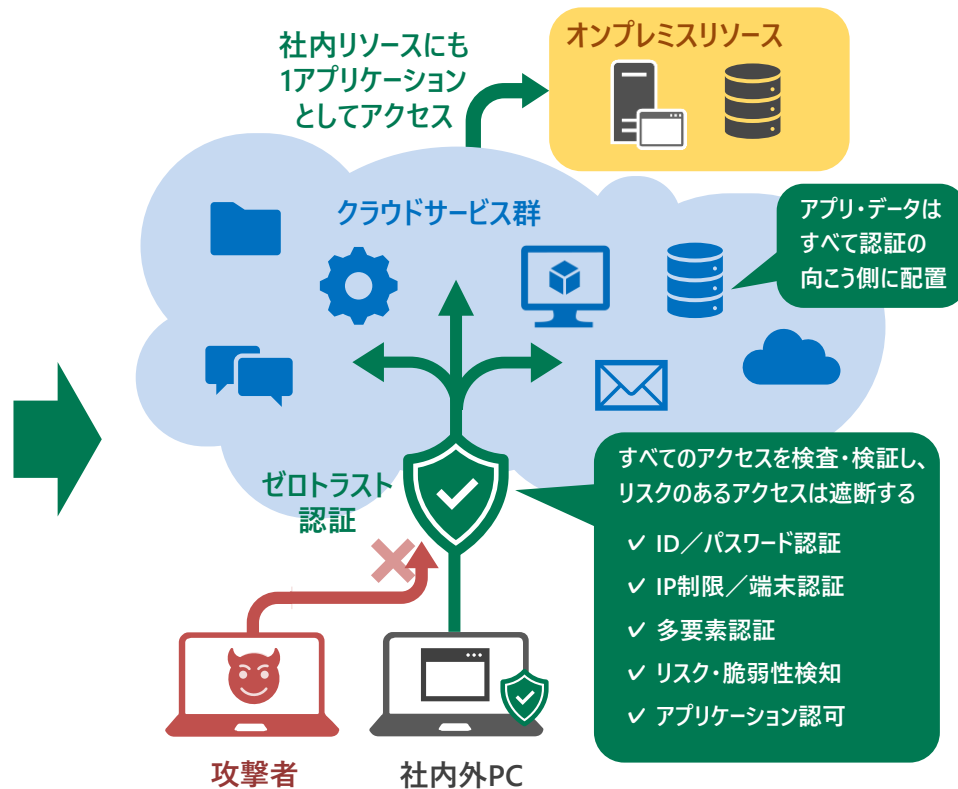
ゼロトラストによる解決

ゼロトラスト実現によるセキュリティ課題解決のイメージ

従来の「境界型ネットワーク」とクラウドの混在



クラウドと「ゼロトラスト」を前提としたネットワーク



... 侵害される／侵害されている恐れのあるポイントとルート

Microsoft 365・Azureシリーズにおけるゼロトラストのサービス構成

No	構成要素	機能	製品・機能概要	M365/Azure 機能	必要ライセンス
1	アイデンティティ・セキュリティ ID管理・認証・認可	IAM	ID管理、シングルサインオン（SSO）、デバイス環境とポリシーに基づく高度なアクセス条件制御	Azure AD, 条件付きアクセスポリシー	Microsoft 365 E3
2	ネットワーク・セキュリティ ネットワーク経路のセキュリティを確保する	SWG	クラウドプロキシ等によるWebアクセスセキュリティ	Microsoft Defender for Endpoint (プレビュー)	Microsoft 365 E5
		SDP, ZTNA	社内アプリケーションの安全なインターネット接続	Azure AD Application Proxy	Microsoft 365 E3
3	デバイス・セキュリティ デバイスのセキュリティ・管理・監視	EDR	侵害監視・対応	Microsoft Defender for Endpoint	Microsoft 365 E5
		EPP	アンチマルウェア・アンチウィルス	Microsoft Defender for Endpoint	Microsoft 365 E5
		MDM	デバイス管理	Intune	Microsoft 365 E3
		アップデート管理	OSによるアップデート管理	MECM, WSUS	MS 個別ライセンス
4	ワークロード・セキュリティ サービス・IT資産のセキュリティ確保・監視	CWPP	サービス・IaaSの管理・監視	Azure Defender	Azure 個別機能
		CSPM	サービスの設定・ポリシー不備監視	Azure Security Center (Azureのみ)	Azure 標準機能
5	データ・セキュリティ データ保護・情報漏洩対策	DLP	情報のタグ付け・監視による情報流出対策	Azure Information Protection	Microsoft 365 E3 ※一部機能には E5 が必要
6	可視化と分析 アクセス状況・ログの分析による制御・可視化	CASB	クラウドサービスアクセス制御	Cloud App Security	Microsoft 365 E5
		SIEM	各製品ログの収集・統合的なログ分析	Azure Sentinel	Azure 個別機能
		UEBA	ユーザー・機器等のふるまい分析による異常検知	Azure AD Identity Protection	Microsoft 365 E5
7	自動化 インシデント対応の自動化・効率化	SOAR	様々なログ分析とサービス連携によるインシデント対応の自動化・効率化	Azure Sentinel	Azure 個別機能

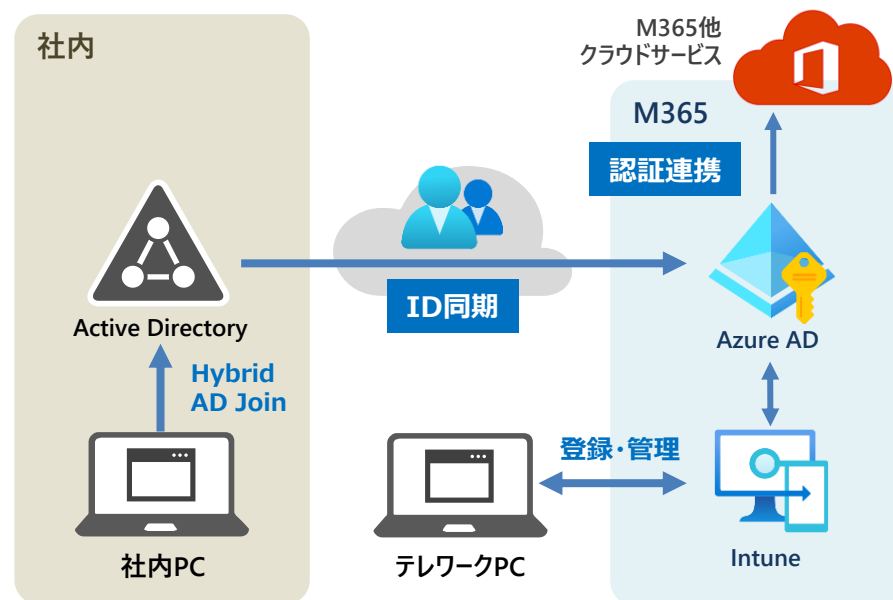
A社：社内ADとAzure ADを同期し社内外のデバイス管理と認証を統合

顧客 製造業 500～1000名企業様

課題 クラウド認証の強度を強め、テレワークPCの管理・認証も統合したい

解決 オンプレミスADとAzure ADを同期・連携するよう構成し（Hybrid AD Join）、テレワークPCをIntuneで管理することで、クラウドサービスの認証条件としてPCがADまたはIntuneで管理されていること、管理ポリシーに適合していることを追加しました。

構成 Azure AD（AADC, 条件付きアクセス）, Intune



B社： 社外PCに対してAzure AD Application Proxyで安全に社内アプリを公開

顧客 金融系 300～500名企業様

課題 持ち出しで使う社外PCを管理し、安全に社内アプリ（事務、ファイル閲覧）に接続させたい

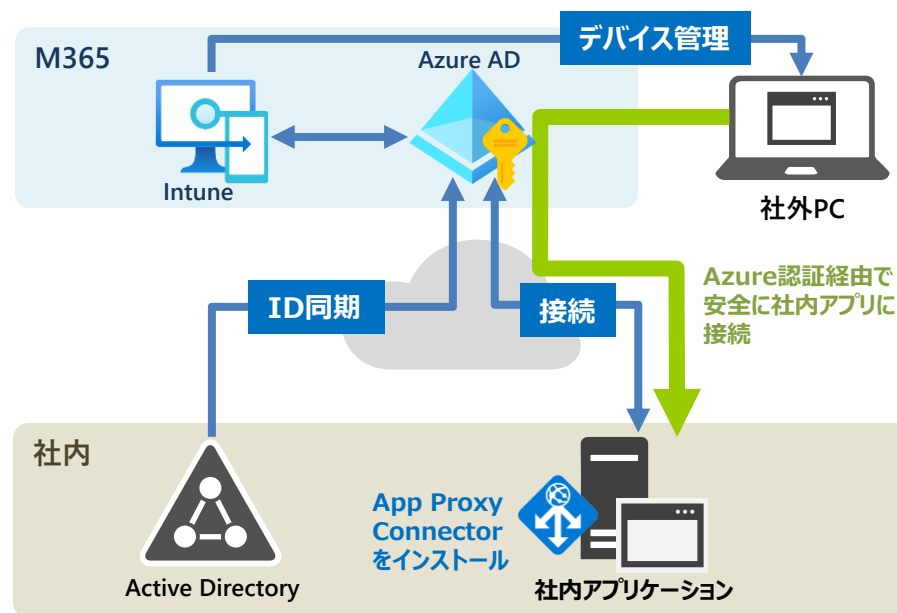
解決 社外デバイスをIntuneで管理し、App Proxyを構成して社内アプリをAzureに接続、

多要素認証を経由した安全なアクセスだけ社内アプリに接続できるよう設計しました。

App Proxyは内部からAzureにセッションを張るため、社内ネットワークを公開する

必要がなく、ネットワーク設計の変更が発生しない点も大きなメリットです。

構成 Azure AD（AADC, 条件付きアクセス）, Intune, Azure App Proxy



Microsoft Endpoint Configuration Manager環境事例の ご紹介

構成事例① 国内複数拠点 クライアント数40,000台規模

構成事例② 社外クライアント管理用環境 クライアント数5,000台規模

構成事例① 国内複数拠点 クライアント数40,000台規模

【導入の目的】

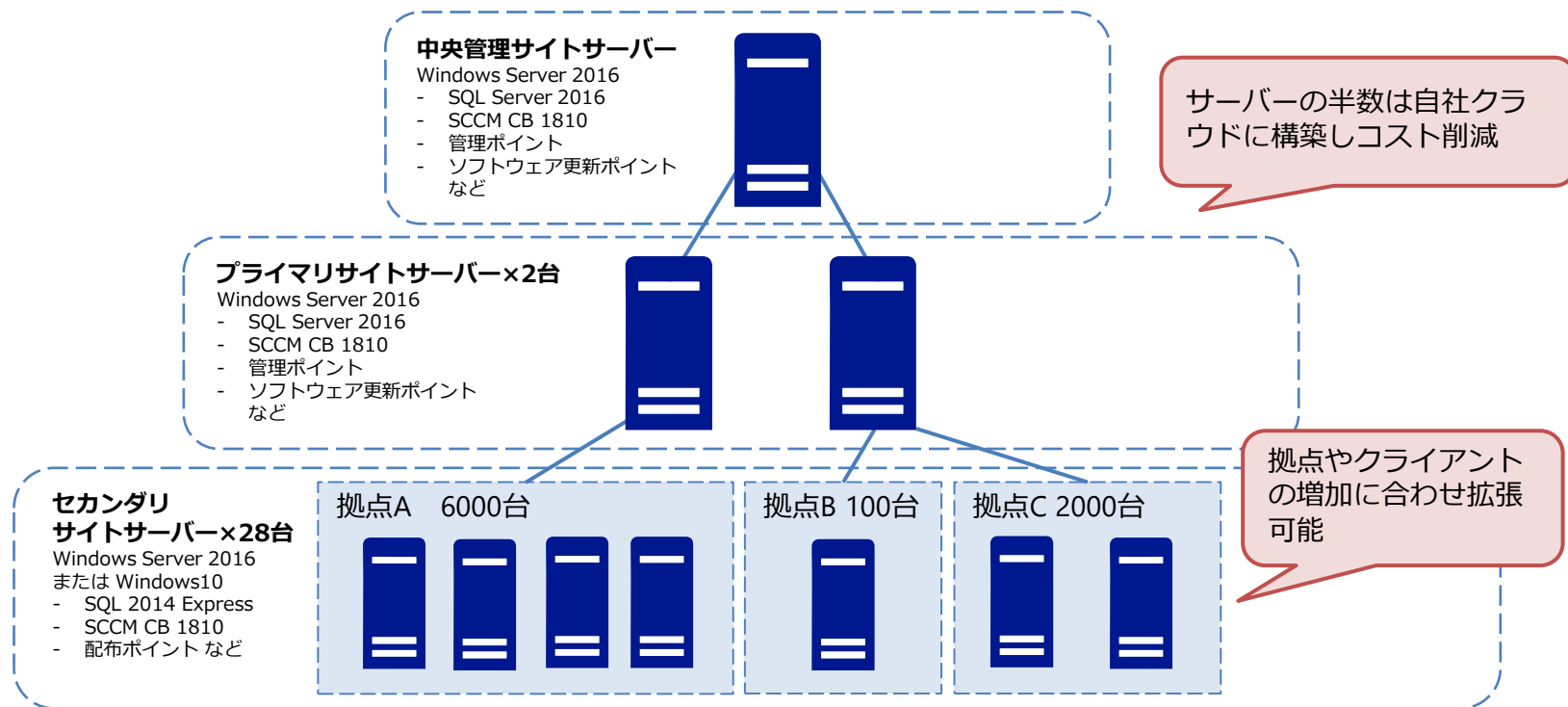
クライアントのWindows Update管理、リモート操作、ソフトウェア配信管理

【構築のポイント】

- ① 拠点ごとクライアント数の多さをカバーする、MECM階層の構築
- ② 今後のクライアント増を見込み、拡張の余地を残した構成

【プロジェクト期間(設計～引渡)】 5ヶ月

【構築予算】 2000万円 ※クライアント展開は除く



【導入の目的】

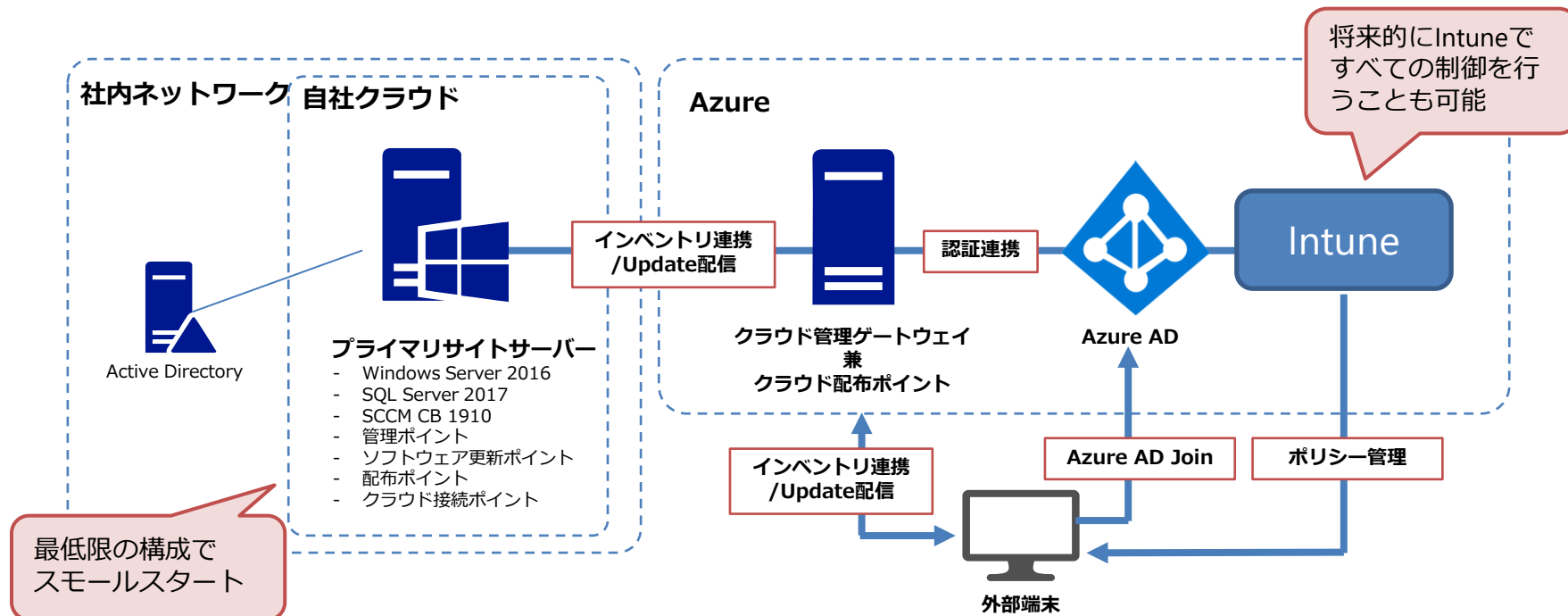
インターネットにのみ接続する端末のWindows Updateを、社内端末と同等に管理

【構築のポイント】

- ① 社外クライアントを社内外から管理できるスモール環境
- ② 将来的なIntune完全移行を見据えた構成

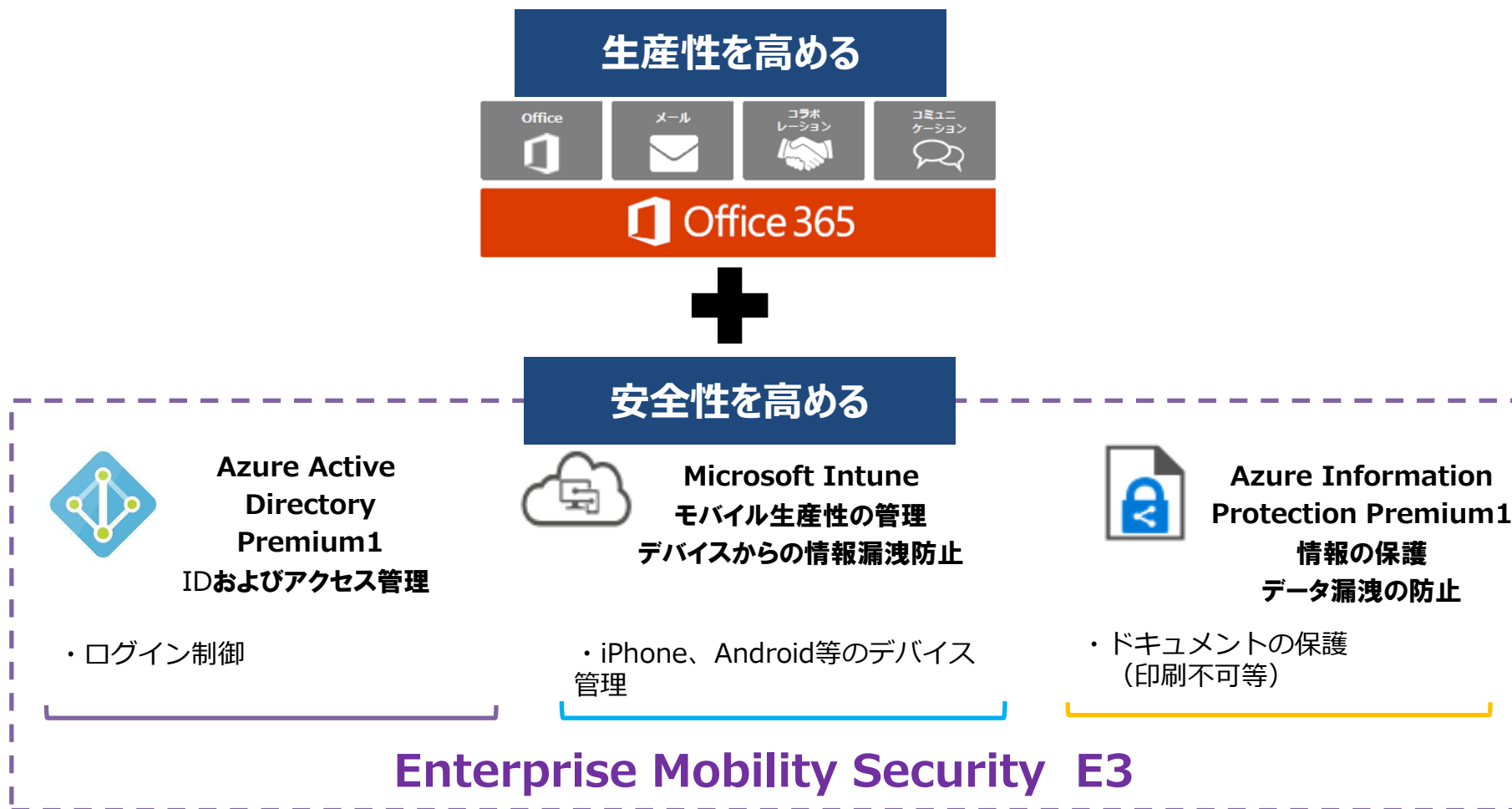
【プロジェクト期間(設計~引渡)】 3.5ヶ月

【構築予算】 500万円 ※MECM部分のみ、クライアント展開除く



セキュリティ/MDM (EMS)

Office365を利用するとアクセスの利便性が飛躍的に上がり、生産性の向上につながります。便利になる分、セキュリティ面の考慮も必要となります。EMS（Enterprise Mobility + Security）を導入することにより、アクセス制御、データ保護、ユーザー/デバイス管理、データ漏洩の防止が実現できます。



EMS E3の利用により、以下のような統制を行う事が可能です。



■ 社外からのアクセスを制限したい

社内からのアクセスや、登録したデバイスのみアクセス可能にすることができます。ネットカフェや自宅PCからのログインを防ぎます。



■ MDM (モバイルデバイス マネジメント)

スマートフォン、持ち出しPCの紛失時にリモートワイプができます。アプリケーションを手軽に配布し、利用状況の確認を行えます。



■ ファイルの保護

Officeドキュメントや電子メールを保護し、配布後にアクセス禁止が出来ます。閲覧・編集権限の付与や閲覧有効期限、印刷不可等細かな制御が可能です。
