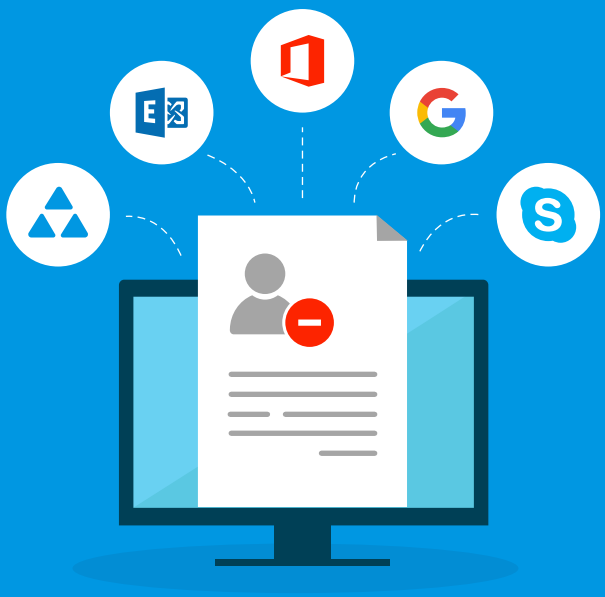
ManageEngine
ADManager Plus

Active Directory＆Azure AD ハイブリッド環境における ユーザープロビジョニング効率化ガイド



https://www.manageengine.jp/products/ADManager_Plus/

はじめに

多くの企業にとって、オンプレミスのActive Directory（AD）は、重要なデータへのアクセスを制御するネットワーク・インフラの中核的存在を担っています。ADが一般的に広く普及している一方で、クラウドを活用して新しい機能を利用しようとする組織も珍しくありません。オンプレミスのADとクラウドベースのAzure ADを併用した「ハイブリッドAD環境」が目指すのは、両者のメリットを享受しながら管理の行き届いた環境を構築することです。

ハイブリッドAD環境でも、日常的にユーザーのプロビジョニング／デプロビジョニングの業務はもちろん発生します。しかし、新規ユーザーのために、ADのユーザーアカウントやMicrosoft 365のアカウント、メールボックスなどを作成するには、Microsoftが提供する標準の管理ツールでは機能制限が多く、効率性とセキュリティの面で大きな課題が生じます。

本ホワイトペーパーでは、ハイブリッドAD環境におけるユーザーのプロビジョニング／デプロビジョニング向けにMicrosoftの標準管理ツールが提供する機能について考察し、そのデメリットを解説します。また、そのデメリットに対して一貫性、セキュリティ、効率性を確保しながら、より優れた方法でアプローチするために役立つソリューション「ADManager Plus」について併せて紹介します。

標準管理ツールを使用したプロビジョニング

ハイブリッドAD環境におけるユーザープロビジョニングでは、オンプレミスとクラウド環境の両方でユーザーアカウントを作成し、ユーザー属性、メールボックス、ホームフォルダーなどを設定する必要があります。（図１参照）
ADのユーザーアカウント管理の標準管理ツールである「Active Directory ユーザーとコンピューター（ADUC）」では、一度に一つのユーザーアカウントしか作成できず、プロパティの設定オプションも十分ではありません。

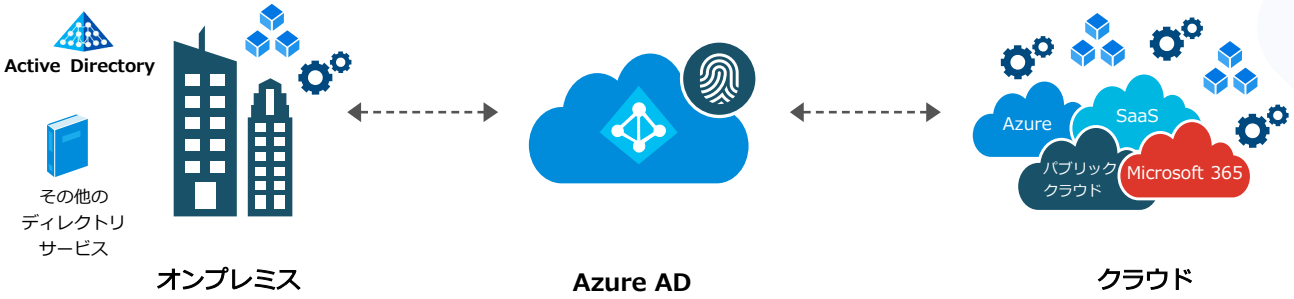


図１：ハイブリッドAD環境

また、Azure ADでは、複数のユーザーに対して一括でプロビジョニングする機能は提供されていません。Azure AD Connectを使用して、オンプレミスADとAzure ADの間でユーザーアカウントを同期させることはできるものの、設定できる属性は限られています。また、 ADUCではカスタム属性を作成できますが、Azure ADでは作成できません。

Microsoftはユーザーを一括で作成するためのソリューションとして、PowerShellを提供しています。PowerShellでは、ユーザー属性の設定から、ランダムパスワードの生成、最小権限の定義、ユーザーメールの設定、さらにはハイブリッドAD環境でのワークフローや自動化の実装なども可能です。

このように、様々なアクションの実行が可能なPowerShellですが、その操作にはスクリプトの専門知識が必要であり、処理が複雑になることが多々あります。また、ユーザーアカウントの作成を完全に自動化することはできません。さらに、GUIではないため操作が成功したかどうかを確認できず、失敗を特定したり原因を説明したりする仕組みがないことなどが、PowerShellを使用する際に直面する一般的な課題になっています。

標準管理ツールを使用したデプロビジョニング

従業員が組織を去る際、ユーザーアカウントの無効化／削除や、すべてのクラウドアプリの ライセンスやアクセス権の削除は必須のタスクです。この時ユーザーアカウントのセキュリティを確保しながらも、個人が管理してきたデータやメールへのアクセスをユーザーに短期 間許可する必要がある場合があります。理想的には、ユーザーアカウントを安全なOUに移し、アクセスが必要とされる時以外はアカウントを無効化することが望ましいです。

その後、ユーザーアカウントを完全に削除する際、標準管理ツールでは関連付けられた設定やデータまで完全に削除することはできません。また、実行するプロセス自体は単純なものの、管理者が削除すること自体を忘れてしまう可能性もあります。

このような問題を解決し、ユーザーアカウントのデプロビジョニングを簡略化するための方法として、一連のプロセスを自動化するという手段があります。しかし、オンプレミスADとAzure ADの標準管理ツールではそのような機能は提供されていないため、ハイブリッドADで自動化を実装する際は、複雑なPowerShellスクリプトを書かなければなりません。

ADManager Plusを活用しよう

ハイブリッドAD環境におけるユーザープロビジョニング／デプロビジョニングに関する課題を解決するには、「オンプレミス－クラウド」間でシームレスに動作するツールを選ぶことが重要です。セキュリティ上の脆弱性を減らすだけでなく、ハイブリッドAD環境の一貫性や効率性を高めることにも繋がります。

複数ユーザーの一括プロビジョニング

ADManager Plusは、AD／Microsoft 365／Exchange／G Suiteのユーザーを一つのコンソールから複数同時に作成・管理することができるWebベースのソフトウェアです。（図2参照）

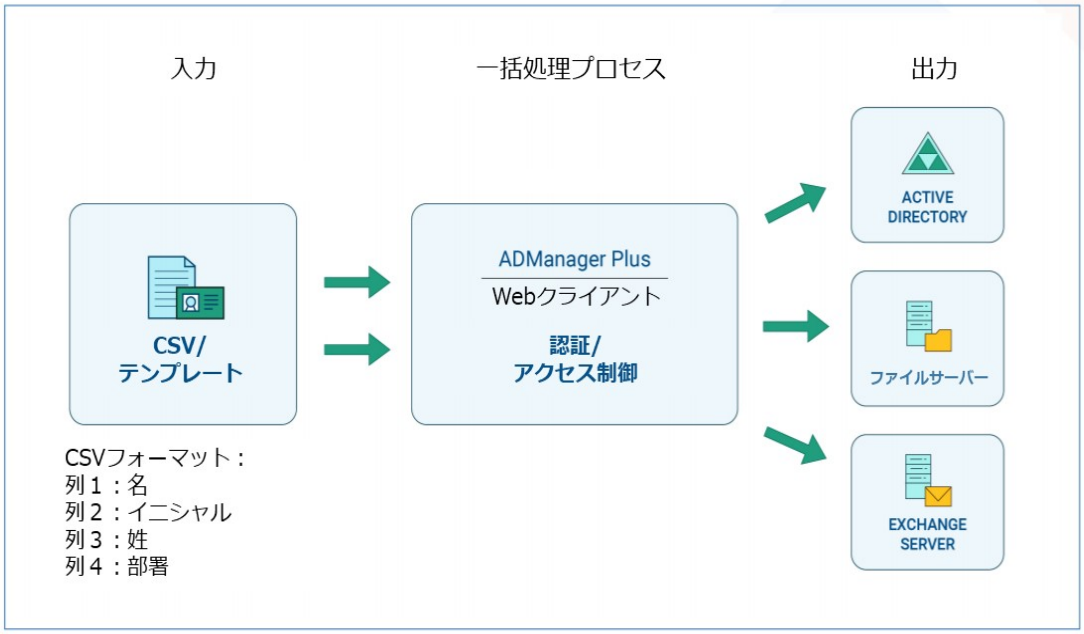


図2：ADManager Plusを用いた複数ユーザーアカウントの作成フロー

ユーザーアカウントのプロビジョニングを自動化する際に重要な役割を果たす「ユーザー作成テンプレート」を使用することで、CSVファイルからの簡単な入力で、セキュアで一貫性のある設定が可能になります。（図３参照）

図３：CSVファイルのインポートによる複数ユーザーの一括プロビジョニング

ADManager Plus を通してADのユーザーアカウントを新規作成すると、同時にExchangeメールボックスや、Microsoft 365、G Suiteのユーザーアカウントも作成することができます。ユーザーの作成を効率化するだけでなく、ユーザーのプロビジョニングを自動化することで、一連のプロセスを漏れなく実行することが可能です。（図３・図４参照）複雑なPowerShellスクリプトや、標準管理ツー ルを使用した作業は必要なくなります。

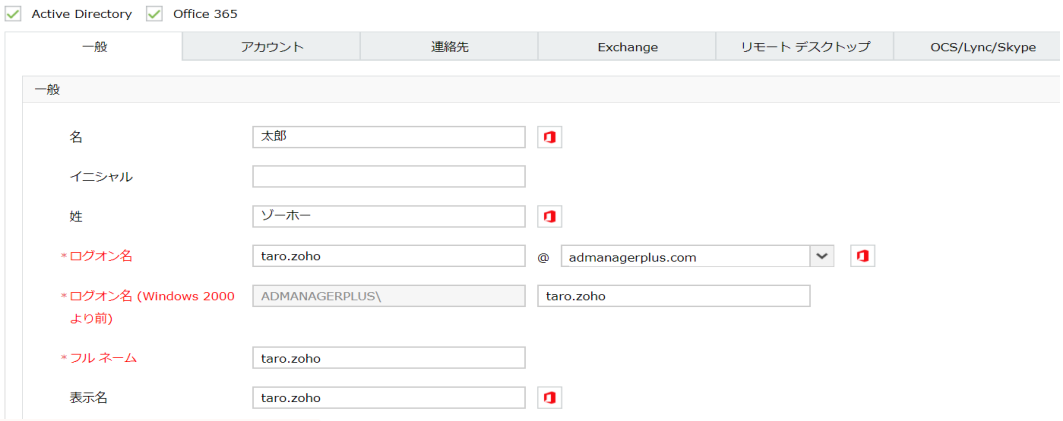


図４：AD・Microsoft 365での同時プロビジョニング

ランダムパスワードの生成

新規ユーザー用にランダムなパスワードを生成するのは、組織にとって非常に重要なタスクです。ユーザーアカウントごとに同じパスワードが再利用されるのを防ぐことで、アカウントが不正利用されるリスクを下げることができます。ADManager Plusでは、ドメインのパスワードポリシーに準拠したランダムなパスワードを生成できます。（図５参照）

ランダムパスワードの生成は、脆弱なパスワードを使用している既存のユーザーアカウントや、初期設定のパスワードのままになっているユーザーアカウントを保護するための重要な鍵となります。生成されたランダムパスワードは、手動でユーザーにメール通知するか、*SMS*経由で自動的に送信できます。

図５：パスワードポリシーの設定

最小権限の原則の適用

ADManager Plusでは、各ユーザーが必要とする最小限の権限のみを付与することができ、「最小権限の原則」を簡単に実現可能です。（図６参照）

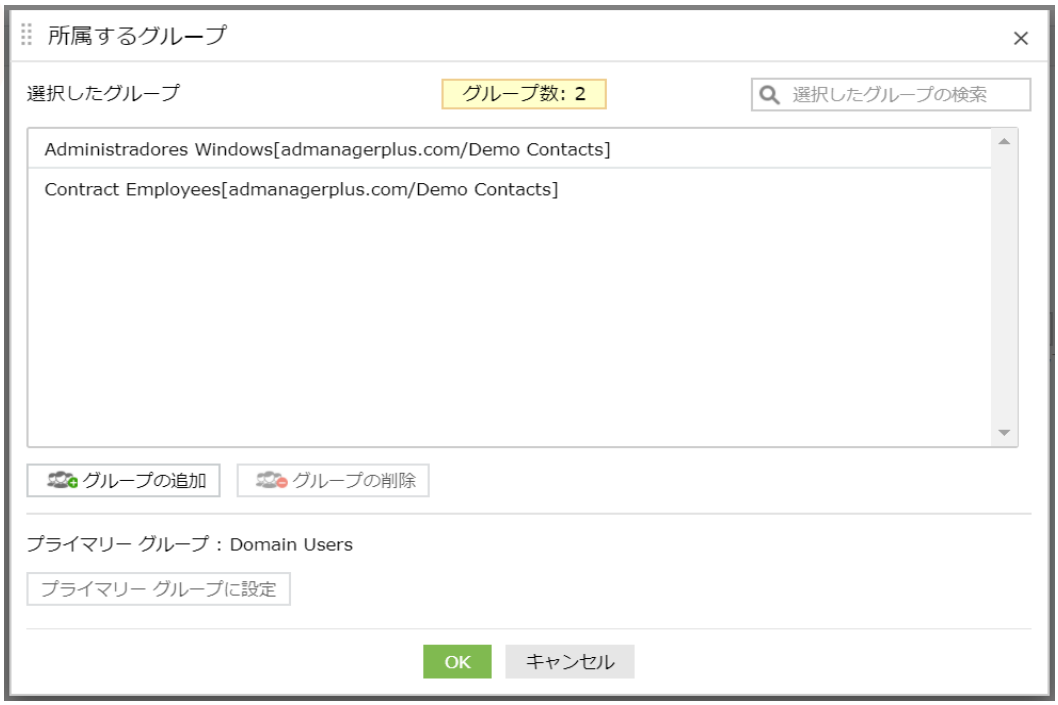


図６：グループメンバーの追加

ユーザーデプロビジョニングの自動化

ADManager Plusは、従業員が組織を離れる際に、ユーザーアカウントのデプロビジョニング、つまりメールボックスの削除、ライセンスの削除、クラウドアプリへのアクセス権の削除を自動的に実行するよう設定することができます。「無効化／削除ポリシー」を設定することで、非アクティブ／無効化された／期限切れのユーザーアカウントやメンバーのいないグループを特定し、一括削除を自動化できます。

ADManager Plusでは、カスタマイズ可能なテンプレートを使用し、CSVファイルからデータをインポートし、組織のポリシーに基づいてアカウントを一括で無効化／削除することができます。（図７参照）これにより、ユーザーのデプロビジョニングの効率化だけでなく、解雇された従業員や攻撃者からの企業ネットワークへの不正アクセスを防止し、セキュリティ体制を強化します。

図７：ハイブリッドAD環境におけるデプロビジョニングの自動化

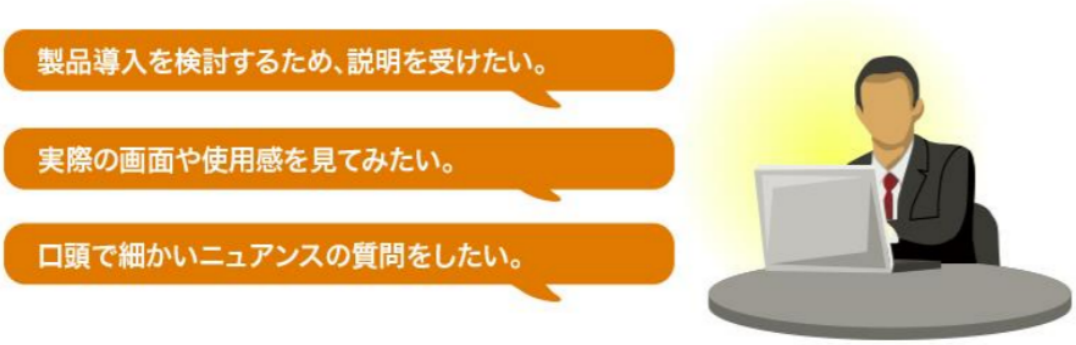
まとめ

ハイブリッドAD環境におけるユーザーアカウントの管理は、管理者・組織のどちらにとっても複雑な作業です。Microsoftの標準管理ツールは、ユーザーアカウントのライフサイクル管理に関しては完全ではありません。そのため、管理者はユーザーのライフサイクルに応じた適切な管理を行うために、平凡なタスクに多くの工数を割いたり、複雑なスクリプトを開発したりしなければなりません。

ADManager Plusは、このような問題を効率的に、かつ低コストで解決します。Active Directoryにおけるユーザーアカウントのライフサイクル管理や、その他オブジェクトの管理におけるあらゆる課題を考慮した上で設計されています。操作しやすいGUIや自動化機能、および包括的なレポート機能を備えたADManager Plusは、ハイブリッドAD環境におけるユーザーアカウント管理を効率化することで、企業に付加価値をもたらします。

製品の詳細を確認されたいという方は、「オンライン相談」を受け付けておりますので、お気軽にお申込みください。

こんな方におすすめです



お申し込みはこちらから

関連製品情報

ManageEngine
AD360

【国内No.1※】Active Directory管理ツール

AD360は、Active Directory(AD)・Azure ADの運用管理に必要な機能を包括的に備えた、AD統合運用管理ツールです。 ADアカウント管理ツール「ADManager Plus」、AD監査レポートツール「ADAudit Plus」、アカウント管理セルフサービスツール「ADSelfService Plus」、Microsoft 365監査・監視・管理ツール「O365 Manager Plus」の4製品をバンドルしています。業務工数の削減とセキュリティ対策を両軸に備え、AD／Azure AD／Microsoft 365の運用に関する課題に幅広く対応します。

※国内出荷本数No.1：ミックITリポート2020年8月号「Active Directory管理ソフトウェア市場動向」掲載

Webサイトはこちら　概要資料はこちら　無料版はこちら

本製品に関するお問い合わせ
ゾーホージャパン株式会社 ManageEngine 事業部
〒222-0012 神奈川県横浜市西区みなとみらい三丁目 6 番 1 号 みなとみらいセンタービル 13 階
ADManager Plus 製品ページ：https://www.manageengine.jp/products/ADManager_Plus/
ホームページ：https://www.manageengine.jp/

■注意事項

本ガイドの内容は、改良のため、予告なく変更することがあります。 ゾーホージャパン株式会 社は本ガイド に関しての一切の責任を負いかねます。 当社は、本ガイドを使用することにより引き起こさ れた偶発的もし くは間接的な損害についても責任を負いかねます。