【Active Directory】サービス概要とユースケース

2025年2月28日

改訂履歴

版数	発行日	改訂内容
第1版	2025年2月28日	初版発行

資料の内容は2025/2/28 時点のものです。製品のアップデートにより変更となる場合がございます旨ご了承ください。

Agenda

1. 前提情報
    1. 用語集
2. 基本情報
    1. Active Directory とは
    2. Active Directory の仕組み
    3. Active Directory の構成要素
3. ユースケース別 構成バターン
    1. ユースケース別 構成バターン
    2. 小規模組織
    3. 中規模組織
    4. 大規模組織
    5. 企業統合などがあった組織
    6. クラウド環境での活用
4. セキュリティ
    1. Active Directory 認証の仕組み
5. 管理ツール
    1. Active Directory の管理ツール
    2. Active Directory の管理コンソール一覧
    3. Active Directory の管理コンソール①
    4. Active Directory の管理コンソール②
    5. Active Directory の管理コンソール③
    6. Active Directory の管理コンソール④

1. 前提情報

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
1	ディレクトリサービス	あらゆるリソース情報を一つに集約し管理するシステム
2	オブジェクト	AD で管理されるデータの総称。ユーザー、コンピュータ（ドメインに参加する PC やサーバー）、グループなどがある
3	リソース	ファイルサーバー、データベース、プリンタなどユーザーが利用できる資源。オブジェクトの一種
4	サイト	物理ネットワークに合わせた、Active Directory の論理的な区別を可能にする概念 デフォルトでは、全てのドメインコントローラーが「Default-First-Site-Name」という名前のサイトに属す 各サイトには、1つ以上のドメインコントローラーが含まれる
5	サブネット	IP ネットワークの論理的な区分 各サブネットは、1つのサイトに関連付けられる クライアントは、所属するサブネットに基づいて、最適なドメインコントローラーを選択する
6	ドメイン間の信頼関係	2つのドメイン間で認証情報を共有し、リソースへのアクセスを許可する設定 ・一方向の信頼：一方のドメインのユーザーが、もう一方のドメインのリソースにアクセスできる ・双方向の信頼：両方のドメインのユーザーが、互いのドメインのリソースにアクセスできる
7	フォレストの信頼関係	ひとつのフォレストに複数のドメインを用意してドメインツリーを構成した場合、そのドメインツリーを構成する個々のドメインの間では、自動的に双方向の信頼関係を設定する。そのため、同じフォレストに属するドメイン同士であれば、特に信頼関係の設定を行わなくても、相互にアクセス権の設定を行える。 異なる組織同士が合併した場合など、フォレストを超えてお互いにアクセスができるようにする必要がある場合には、フォレスト間の信頼関係を明示的に結ぶ必要がある。

2. 基本情報

2.1. Active Directory とは

Active Directory（AD）は、Windows 2000 から導入されているディレクトリサービスです。ネットワーク上の端末やサーバー、プリンター、アプリケーションなどの情報を収集し、一元的に管理します。
Windows Server に標準搭載されているのでインストールが不要で、サービス利用料などのコストは発生しません。

本資料では Active Directory の構成要素や主な機能、ユースケースに合わせた構成の例を紹介します。

2.2. Active Directory の仕組み

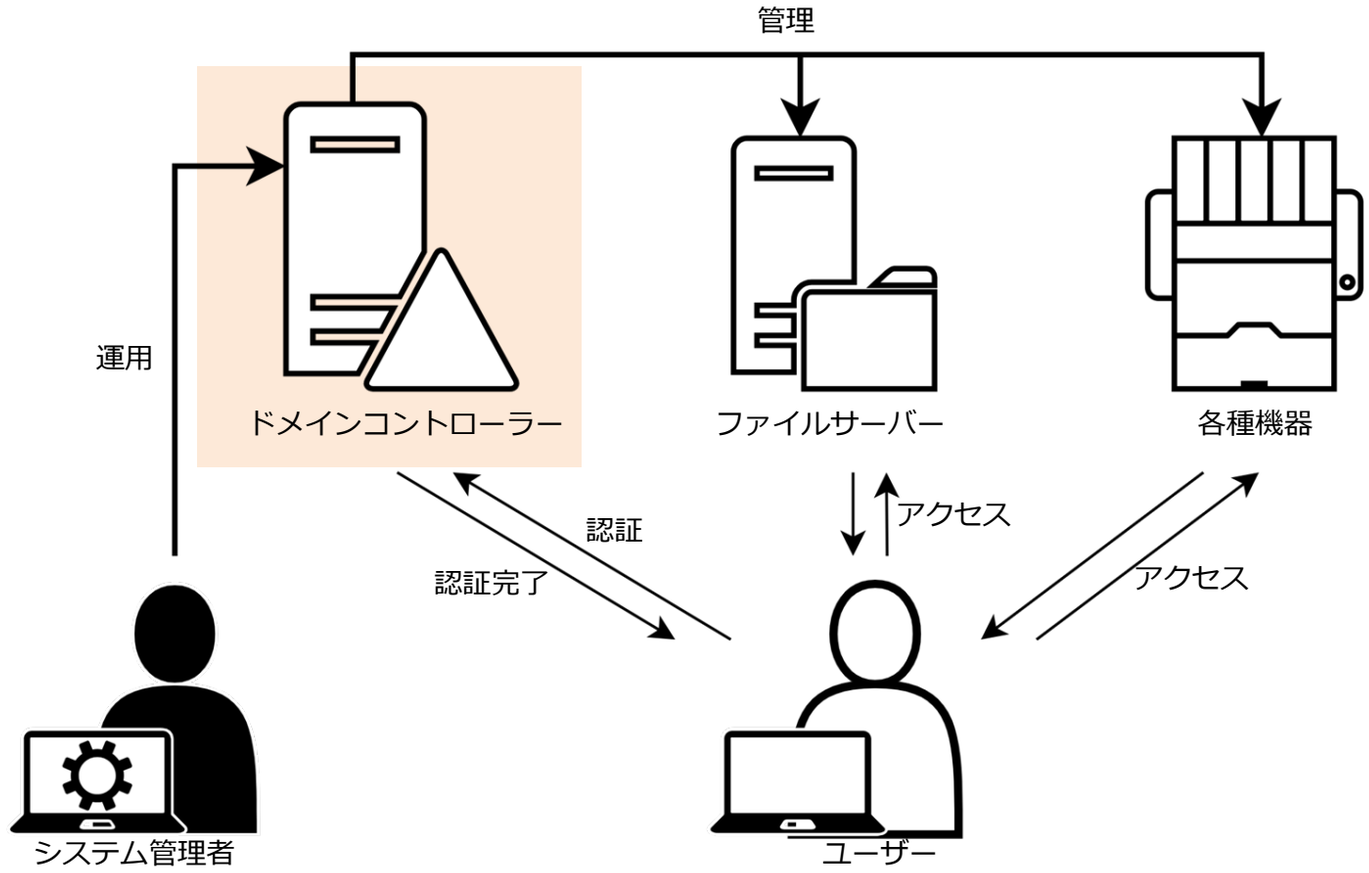
Active Directory がネットワーク上の端末やサーバー、プリンター、アプリケーションなどの情報を一元的に管理するために必要なサーバーが「ドメインコントローラー」です。

ドメインコントローラーは以下のような役割をします。
・ドメイン内のリソース管理
・ユーザー認証
・アクセス制御
・グループポリシー設定
・セキュリティ設定

ユーザーはドメインコントローラーを通して認証を行うことで、自分がアクセスできるリソースを自由に利用できるようになります。

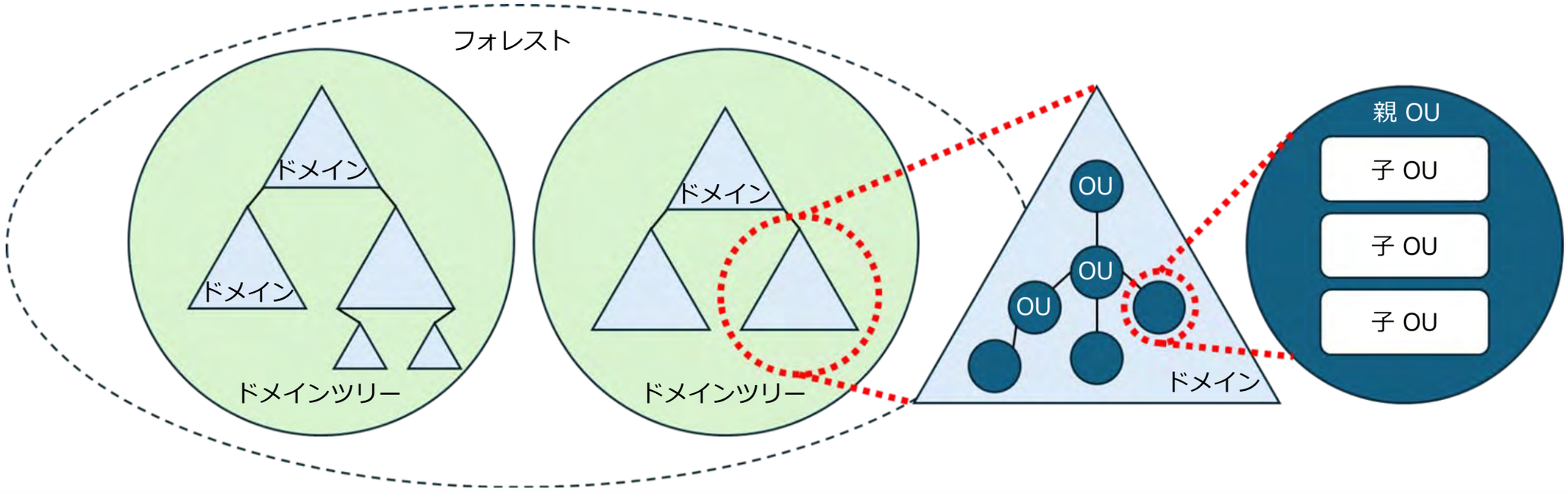
また、システム管理者はドメインコントローラーを利用してドメイン(*)そのものやドメイン内のリソースを管理できます。

*ドメイン：次のページ参照



2.3. Active Directory の構成要素

Active Directory を構成する基本要素には以下の4つがあります。



構成要素	内容	構成要素	内容
フォレスト	Active directory が管理するドメイングループの最も大きな管理単位。1つ以上のドメインツリーで構成される。	ドメイン	Active Directory 理論構造の基本単位。 認証されたユーザが、リソースを管理・共有する範囲。
ドメインツリー	ドメインの階層構造をツリー状で表現したもの。各ドメイン間で信頼関係を構築し、アクセスポリシー設定などに活用する。	OU（組織単位）	ドメイン管理の最小単位で、親/子の階層構造を作れる。ユーザアカウントやコンピュータ、リソースの集合。

3. ユースケース別 構成バターン

3.1.ユースケース別 構成バターン

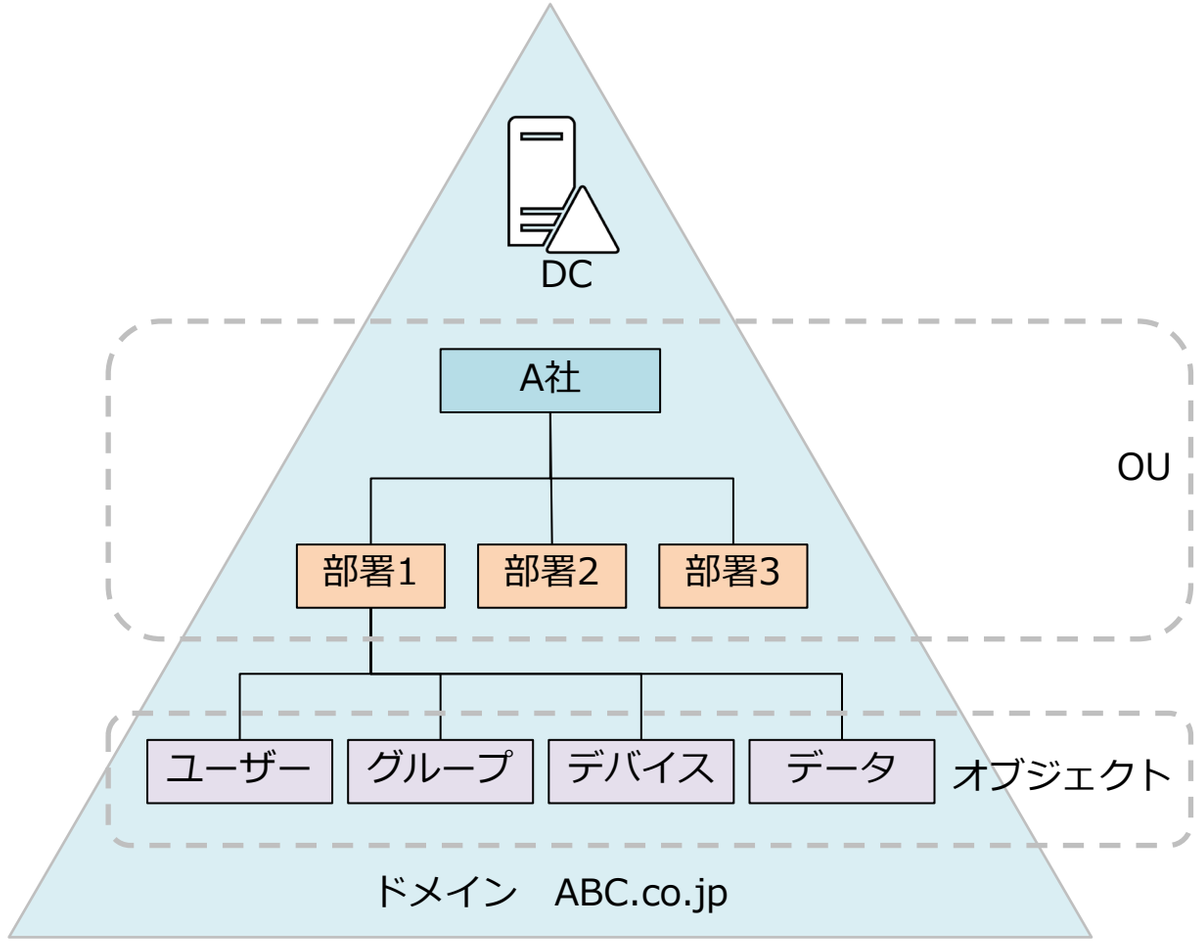
Active Directory の構成例について、以下のようなユースケースでの構成パターンを紹介します。

No.	ユースケース	重視するポイント
1	小規模組織	シンプルな利用
2	中規模組織	シンプルかつ効率的な構成、冗長化構成
3	大規模組織	複数ドメインの独立した管理、各ドメイン間でリソース管理およびアクセス管理
4	企業統合などがあった組織	複数ドメイン/フォレストの独立した管理、各ドメイン間でリソース管理およびアクセス管理
5	クラウド環境での活用	社内/社外のネットワークから社内リソースを利用

3.2. 小規模組織

10人以下程度の小規模組織では、このような活用が考えられます。

・1つのドメイン（シングルドメイン）
・1つのドメインコントローラー（DC）
・必要に応じて管理対象を OU で分けたシンプルな構成

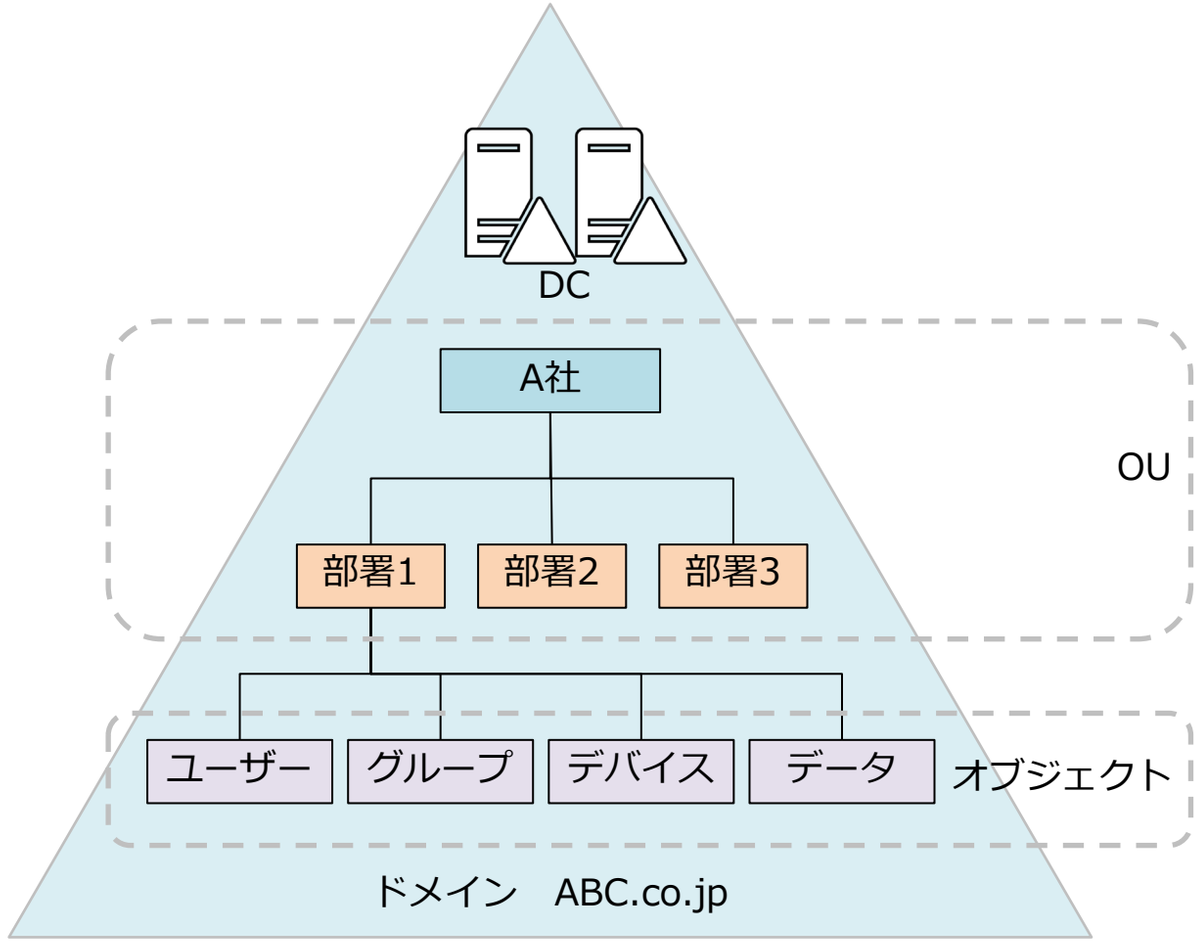


3.3. 中規模組織

100人以下程度の中規模組織では、このような活用が考えられます。

・1つのドメイン（シングルドメイン）
・2つ以上のドメインコントローラー（DC）
・部署ごとに OU を作成
・OU ごとにグループポリシー管理

ドメインコントローラーはネットワーク上のリソース管理の利便性を高める分、障害などで停止した場合のリスクが大きいです。
可用性向上のため、組織の規模が大きい場合は複数のドメインコントローラーを構成（冗長化構成）することがおすすめです。



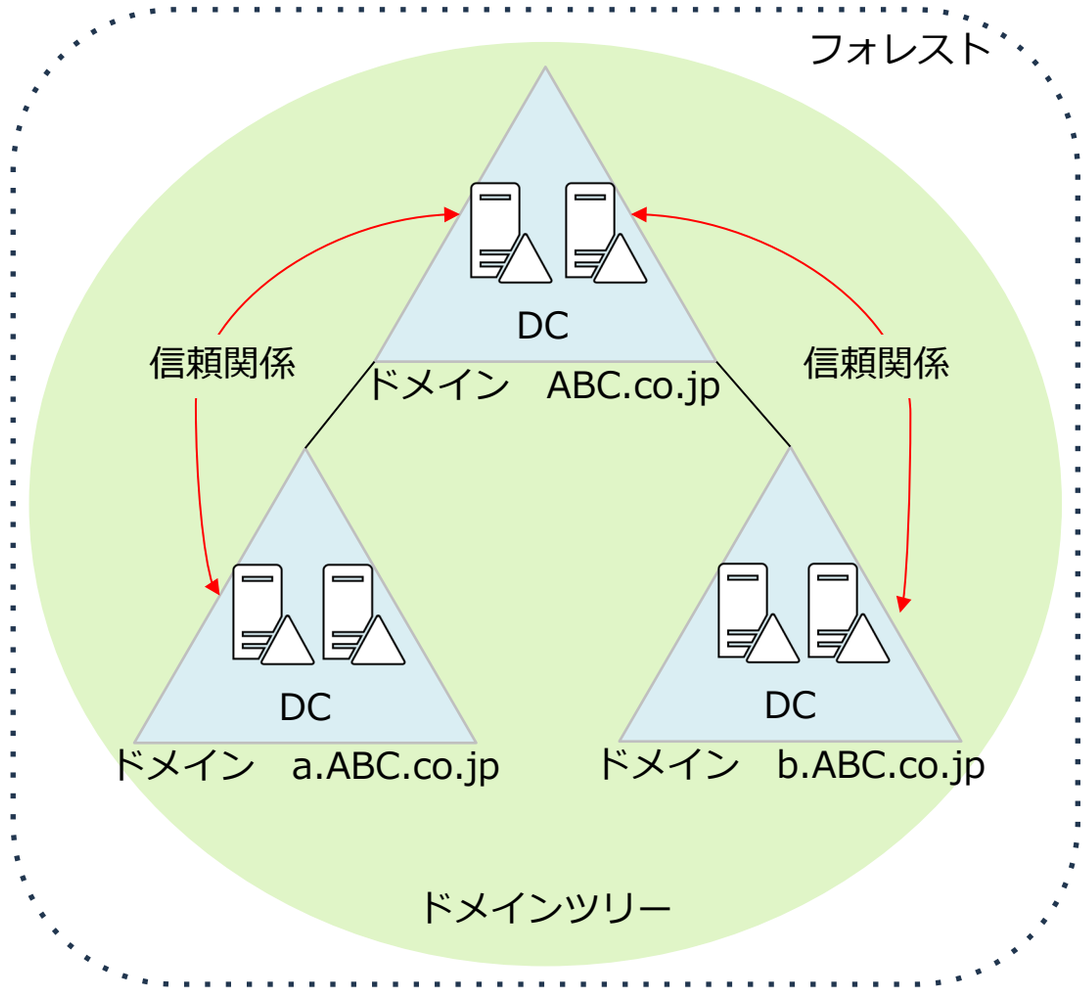
3.4. 大規模組織

本社と支社にそれぞれシステム管理機能があり機能としては独立しているが、本社と支社間でリソースの共有が頻繁に行われるような大規模のネットワークを持つ組織では、このような活用が考えられます。

・複数ドメインでドメインツリー構成
・フォレストルートドメイン（図の「ABC.co.jp」）の下位にサブドメインを作成し、ドメイン間で信頼関係を設定
・各ドメインに2つ以上のドメインコントローラー（DC）

各ドメインはそれぞれドメインコントローラーを持ち、独立した管理が可能です。また、ドメイン間で信頼関係を設定することで必要に応じてリソースの共有やアクセス管理を簡単に行えます。

ドメインツリーで構成した場合、下位のドメイン名はフォレストルートドメインのドメイン名の前に文字列を追加します。



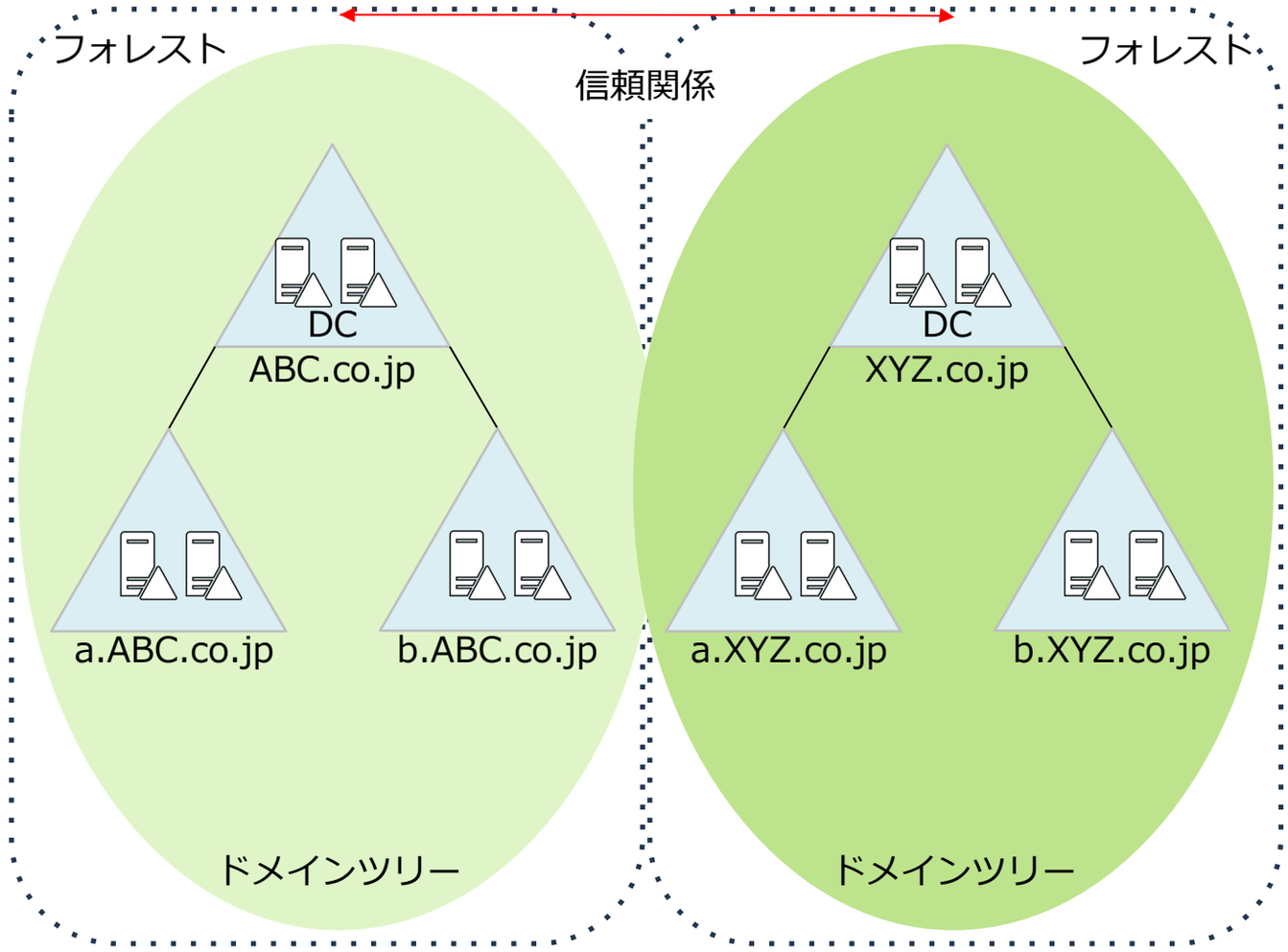
3.5. 企業統合などがあった組織

既存 Active Directory を導入している企業同士が統合するなどにより、異なるドメインツリーとの間でユーザーがリソースへアクセスする必要がある組織では、このような活用が考えられます。

・それぞれのフォレストが存在
・フォレスト間で信頼関係を明示的に設定
・複数ドメインでドメインツリー構成

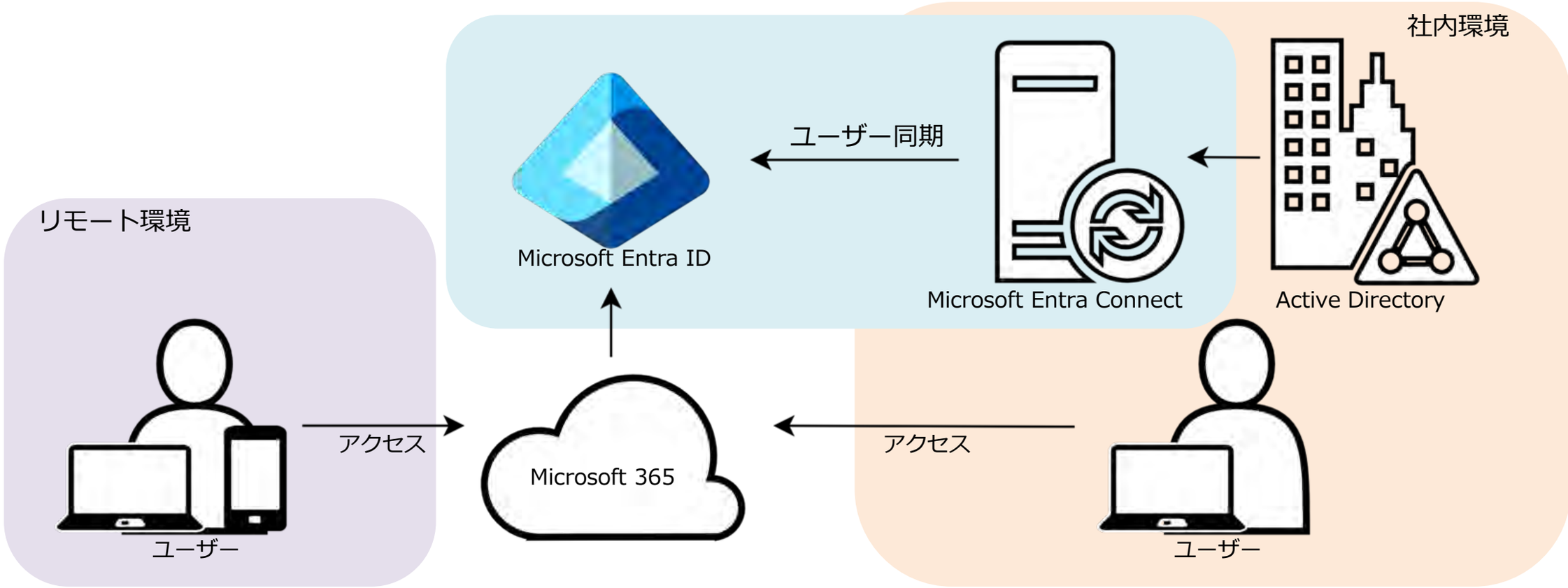
各ドメインはそれぞれドメインコントローラーを持ち、独立した管理が可能です。また、フォレスト間で信頼関係を設定することで必要に応じてリソースの共有やアクセス管理を簡単に行えます。

このような構成例は以下のようなときにも考えられます。
・すでに確保したドメインを必ず使用する必要がある
・認知度のために既存のブランド(組織)を維持する必要がある



3.6. クラウド環境での活用

外出先・在宅からのリモートワークなど社外ネットワークからの接続が発生する場合、社内外からのアクセスを統一した認証基盤で管理する必要があります。クラウドサービスである Microsoft Entra ID を既存オンプレミスの Active Directory と連携することで、シームレスな利用が可能です。



4. セキュリティ

4.1. Active Directory 認証の仕組み

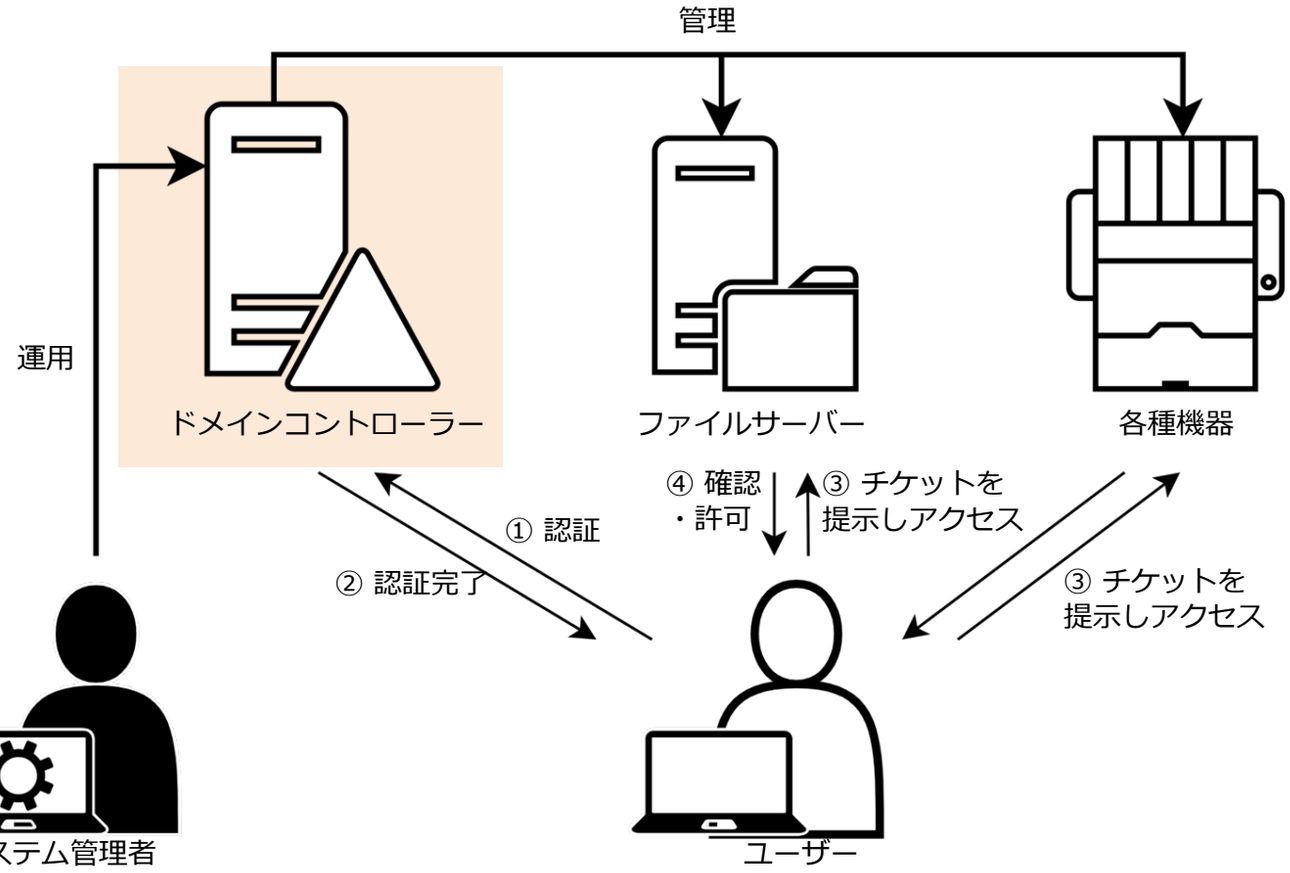
Active Directory 環境では、アカウントの認証がドメインコントローラで行われます。認証をドメインコントローラでまとめて行うことによって、ユーザー・デバイス追加や変更/無効化などのリソースを一元管理できるようになります。

認証は以下のステップで行われます。

① ユーザーがドメインに参加したコンピューターにログインしたら、認証データがドメインコントローラーに送られる
② ドメインコントローラー側で認証データを確認し、正しい場合はチケットが発行される
③ ユーザーはチケットを提示することでアクセス先コンピューターに対し認証を実施
④ アクセス先コンピューターはチケットがドメインコントローラーから発行されたものであるかを確認し、正しい場合はユーザーのアクセスを許可

この認証方式により、ユーザーは一度認証を受けると、どのコンピューターに対してもパスワードの入力を要求されることなくアクセスすることが可能になります。

この認証方式が**ケルベロス（Kerberos）認証**です。
Active Directory の基盤技術として採用されています。



5. 管理ツール

5.1. Active Directory の管理ツール

Active Directory 内の管理対象に合わせて、主に以下のツールを使い分け管理を行います。

ツール名	管理内容	使用例
Active Directory ユーザーとコンピュータ	Active Directory 環境におけるユーザー、グループ、コンピューター、OU などのオブジェクトとその属性の作成と管理	・ユーザー管理の一元化：組織内のユーザーアカウントを一元的に管理 ・アクセス制御：ユーザーをグループに所属させることで、リソースへのアクセス権限を容易に管理 ・コンピューター管理：ドメインに参加しているコンピューターを管理し、セキュリティポリシーの適用やソフトウェアの展開を効率化
Active Directory サイトとサービス	サイト、サブネット、ドメインコントローラーの管理	・クライアントコンピューターとドメインコントローラー間の認証トラフィックの最適化 例）大阪のユーザーは大阪のドメインコントローラーに、東京のユーザーは東京のドメインコントローラーに優先的に認証を行わせる ・ドメインコントローラー間のレプリケーション（複製）トラフィックの最適化 例）東京でユーザーアカウントを作成すると、その情報は設定されたスケジュールに従って大阪のドメインコントローラーにも複製される
Active Directory ドメインと信頼関係	複数の Active Directory ドメインが存在する環境において、異なるドメインのユーザー/グループに対してアクセス権を設定	・複数のドメインに所属するユーザーが、1つのアカウントで全てのリソースにアクセスできるようにする 例）A社とB社が合併し、それぞれのドメインを統合する場合、ユーザーは以前のアカウントで両方のドメインのリソースにアクセス可能 ・異なるドメインに存在するリソースへのアクセスを、ユーザーに意識させずに行えるようにする 例）開発部門のドメインと営業部門のドメインを分離している場合でも、営業部門のユーザーが開発部門のファイルサーバーにアクセスできるように設定

各ツールをそれぞれ実行し管理を行えますが、一カ所でまとめて管理できるコンソールも用意されています。次のページから紹介します。

5.2. Active Directory の管理コンソール一覧

Active Directory を一カ所で管理できるコンソールのうち、主な4つを紹介します。各コンソールの比較は以下です。

項目	サーバーマネージャー	Active Directory 管理センター	PowerShell	リモートサーバー管理ツール
特徴	Windows サーバーの役割や機能を管理するための総合的なツール。	AD のユーザーやグループ、コンピューターなどを管理するための専用ツール。	コマンドラインベースの管理ツール。	リモートでサーバーの管理ができる。ADの管理を含む多くの機能を提供。
メリット	・統合的なサーバー管理が可能 ・直感的に操作できる	・簡単にユーザーやグループの管理ができる ・直感的に操作できる	・スクリプトや自動化に強い ・詳細な管理が可能 ・高度な操作が可能	・リモートでサーバー管理が可能
デメリット	・多機能のため、特定の役割に焦点を絞りづらい	・機能が限定的で、詳細な設定には不向き	・コマンドを覚える必要があり、初心者には難易度が高い ・エラーやトラブルシューティング対応の難易度が高い	・インストールが必要 ・リモート接続が必要
使用の条件	Windows Server 2008 以降のバージョンで標準利用可能	Windows Server 2008 R2 以降のバージョンで標準利用可能	Windows Server 2008 R2 以降のバージョンで標準利用可能	クライアント PC へのインストールが必要
主な使用者	サーバー管理者、ITインフラ担当者	AD 管理者	高度な管理を行うシステム管理者、スクリプトを使用するエンジニア	複数のサーバーを管理する IT 管理者、リモート管理が必要な人

5.3. Active Directory の管理コンソール①

■サーバーマネージャー
サーバーマネージャーは Windows Server の管理コンソールです。サーバーの役割や機能、サービスの管理を行うために使用します。

サーバーマネージャーには、Windows サーバーの管理メニューに加え、関連する管理ツールも表示することができます。そのため、前述した Active Directory 管理ツールや後述する Active Directory 管理センター、Windows PowerShell などをサーバーマネージャー画面で実行・管理できます。

メリット

・包括的なサーバー管理
AD だけでなく、サーバーの役割やサービス全体を一元的に管理できる。

・複数サーバーの管理
複数のサーバーを一つのコンソールで管理できる。

デメリット

・AD 管理に特化していない
AD に関する細かな管理操作には不向き。

5.4. Active Directory の管理コンソール②

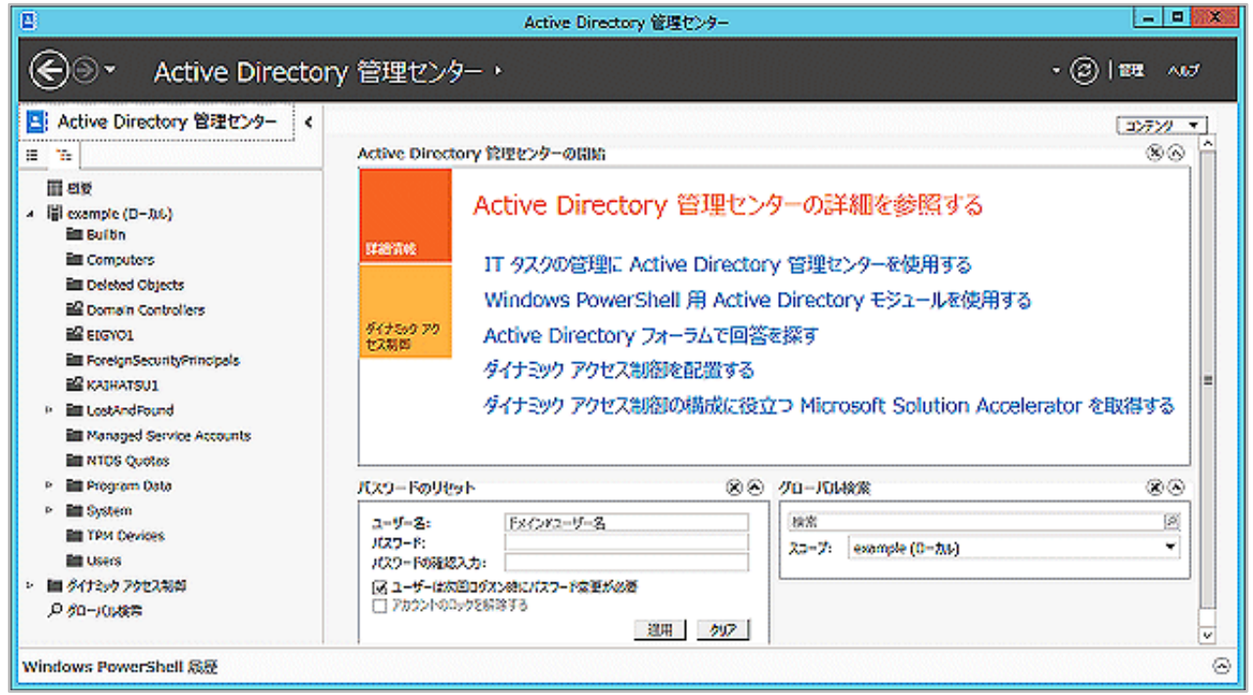
■Active Directory 管理センター（ADAC)
GUI (Graphical User Interface) ベースでより視覚的で使いやすいインターフェースで構成されている Active Directory 管理コンソールです。PowerShell のスクリプトを GUI で生成できるため、操作の自動化を手助けします。

メリット

・直感的な操作方法
操作が簡単に行える。
・スクリプトの生成
PowerShell コマンドを自動的に生成してくれる。スクリプトを活用した操作の自動化が可能。

デメリット

・大規模環境での GUI 操作の非効率性
GUI 操作のため大規模な AD 環境ではパフォーマンスが低下する場合がある。
・複雑な機能の実施には不向き
複雑なスクリプトやバッチ処理など一部の高度な管理操作については対応できない。



5.5. Active Directory の管理コンソール③

■PowerShell
PowerShell でも Active Directory を管理できます。スクリプトやコマンドを使った高度なカスタマイズや自動化が可能で、広範囲にわたるオブジェクトを効率的に操作できます。

メリット

・スクリプトの再利用
一度作成したスクリプトは他の環境やシステムで再利用でき、作業の効率化を助ける。
・高度な自動化
スクリプトを利用して繰り返し作業を自動化できるため、大幅な時間短縮と人的ミスの削減が可能。大規模な環境での管理に効果的。
・フレキシブルな操作
コマンドを使用して、GUI ツールでは難しい複雑な処理や、大量のオブジェクトに対する一括操作を柔軟に行える。

デメリット

・コマンドライン利用に関する壁
コマンドラインでの管理のためにはナレッジが必要。
・エラーのリスク
間違ったコマンドやスクリプトを実行すると、大規模な変更や誤った設定を引き起こす可能性がある。
・トラブルシューティング
PowerShell スクリプトでエラーが発生した場合、原因を特定し、解決策を見つけるのが難しい場合がある。

5.6. Active Directory の管理コンソール④

■リモートサーバー管理ツール (RSAT)
クライアント PC にインストールすることで、Windows サーバーの管理をリモートで行うことができるようにするツールです。
物理的にサーバーにアクセスできない場合でも、クライアントPCからサーバー管理ツールを利用できるので、管理者はネットワーク越しに自分のPCからサーバーを管理できます。
リモート サーバー管理ツールには、サーバーマネージャー、Microsoft 管理コンソール (MMC) のスナップイン、コンソール、Windows PowerShell のコマンドレットとプロバイダー、Windows Server で実行される役割と機能を管理するためのコマンドラインツールが含まれています。

メリット

・リモート管理
リモートで他のサーバーやドメインを管理できるため、物理的にサーバーの前にいなくても管理が可能。
・Windows に統合
Windows サーバーに直接インストールできるため、別途サーバー管理専用のコンソールを使用する必要がない。
・フル機能
サーバーのローカル管理ツールとほぼ同じ機能をリモートで利用できるため、サーバーの管理が一貫して行える。

デメリット

・インストールが必要
特定のバージョンのWindowsにインストールする必要がある。