【Microsoft Entra Connect】Entra Connect 構成時に作成されるセキュリティグループについて

2025年2月20日

改訂履歴

版数	発行日	改訂内容
第1版	2025年1月31日	初版発行
第2版	2025年1月31日	一部想定外の挙動により、Microsoft社へ確認次第更新予定 (スライド40：3.4. テストケース③パスワードリセットの確認)
第3版	2025年2月20日	Microsoft社へ問い合わせした結果をもとに一部スライド更新 （更新箇所：スライド19 ADsyncPasswordSet の説明更新 スライド28 ADsyncPasswordSet の説明更新 スライド46 テストケース③の検証結果に追記 スライド49 テストケース③の検証結果の内容更新

資料の内容は2025/2/20 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. 前提条件
    2. 用語集
2. 機能の基本情報
    1. サービス概要
    2. Active directory の基本構成
    3. グループの種類について
    4. グループのスコープについて
3. Entra Connect 構成時に作成される
   4つのセキュリティグループについて
    1. Active Directory 構成時に作成される
       セキュリティグループ
    2. Entra Connect 構成時に作成される
       4つのセキュリティグループ
4. グループの確認・ユーザー追加手順
5. テストケース検証
    1. テストケース検証とその結果
    2. テストケース①同期マネージャでの
       同期ログ閲覧、同期実行確認
    3. テストケース②同期ルール作成・変更の確認
    4. テストケース③パスワードリセットの確認

1. 前提情報

1.1. 前提条件

・本書は、クラウドサポートのService Request情報の回答を基に作成しております。
・本書に記載するサービス仕様、サービス名称などの各情報については、2025年1月時点でのサービス仕様に基づくものとしております。
・本書は、Windows Server 2022のキャプチャを利用しております。
・Microsoft Entra Connect は、ドメインに参加している Windows Server 2016 以降にインストールする必要があります。

ドメイン参加済みの Windows Server 2022 を使用することをお勧めします。 Microsoft Entra Connect は Windows Server 2016 にデプロイできますが、Windows Server 2016 は延長サポートであるため、この構成に支援が必要な場合は有償サポート プログラムが必要になることがあります。

・本書は過去に発生した顧客質問を元に仕様の確認および検証を行っています。質問のカテゴリ、内容詳細を以下に記載します。

Azure Service	機能	内容詳細
Microsoft EntraID	Microsoft Entra Connect	①Microsoft EntraConnect インストール後に作成される４つのグループの、それぞれのグループ名は何になるのか。 ②上記4つのグループの初期プロパティ値について、それぞれ下記項目の値が知りたい ・説明 ・電子メール ・グループ名のスコープ ・グループ種類 ・メモ

1.2. 用語集

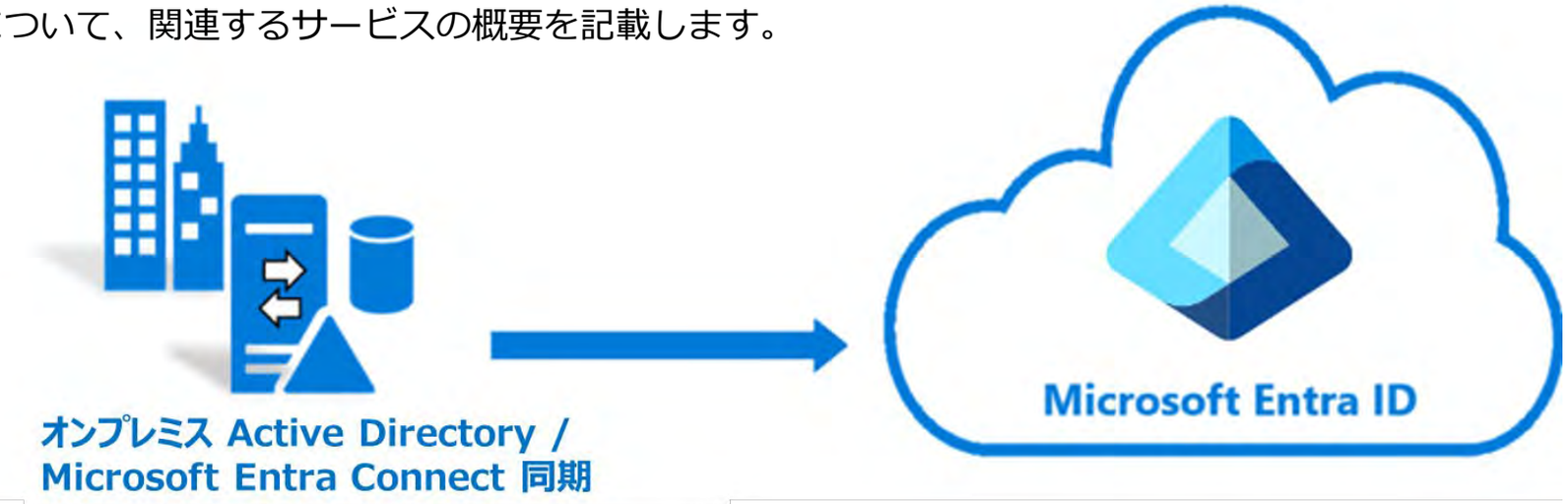
本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
1	Microsoft EntraConnect 同期サービスマネージャ	Synchronization Service Manager。Microsoft Entra Connect の一部。オンプレAD環境と Microsoft Entra ID を統合するために使用し、プロセスにおけるディレクトリ同期の設定や管理、監視を行います。
2	Synchronization Rules Editor	同期ルールエディター。Microsoft EntraConnectにおいて オンプレミスの Active Directory（AD）と EntraID の間でデータの同期を制御するルールを管理するためのツール です。 Microsoft EntraConnect をインストールすると一緒に提供され、「どの属性を、どのような条件で Azure AD に同期するか」 を設定・変更できます。 ドメイン/OU（組織単位）ベースや、グループベースのフィルタリングを行う際はEntra Connectのセットアップウィザードでフィルター処理を行いますが、 より詳細な属性の値の条件作成し同期させたい場合に、Synchronization Rules Editorを使用します。
3	WMI	Windows Management Instrumentation (WMI) は、Windowsにおいて、システムについての情報を様々なソフトウェアから統一的な方法で取得・設定できるようにする仕様です。 WMIを用いてアプリケーションやスクリプトなどからWindowsの設定情報やコンピュータの状態などに容易にアクセスすることができ、管理者がシステムの状態を把握したり、管理を自動化するスクリプトを記述するのに役立ちます。

2. 機能の基本情報

2.1. サービス概要

本書で紹介する機能について、関連するサービスの概要を記載します。

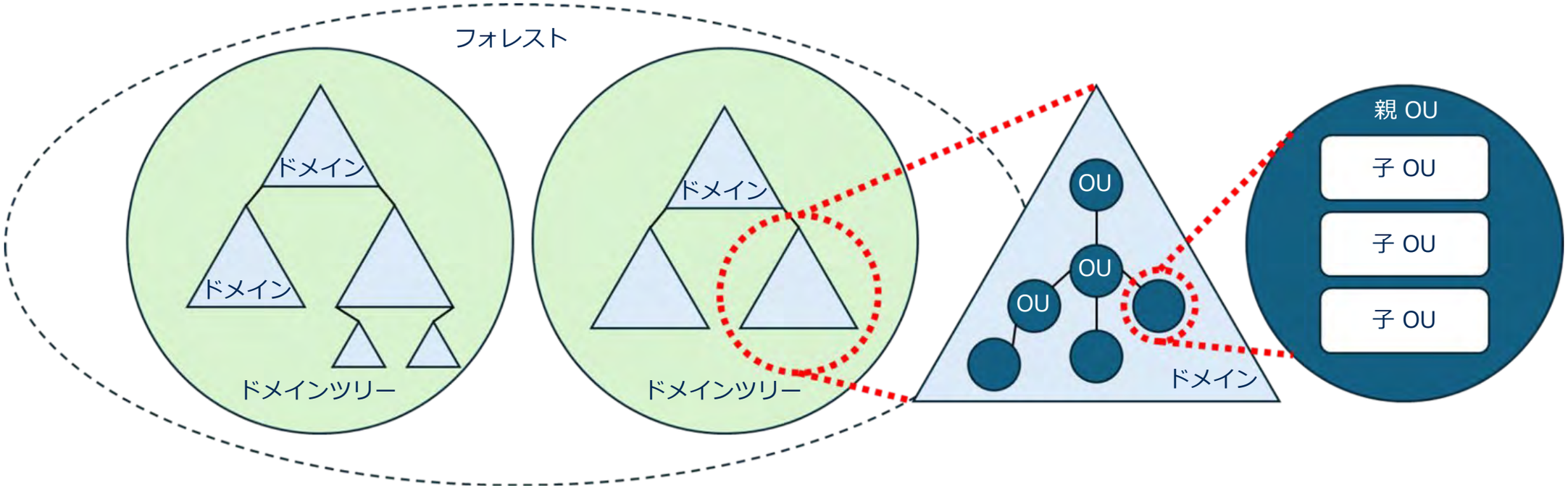


・Active Directory
Windows サーバーに設けられたディレクトリサービスシステム。認証を通し、ユーザやデバイスなどの組織内リソースを一元管理します。

・Microsoft Entra ID
クラウドベースの ID およびアクセス管理サービス。Microsoft 365、Azure を含む SaaS 製品の認証基盤として利用します。

・Microsoft Entra Connect
オンプレミス Active Directory と Microsoft Entra ID の間で ID データの同期に関連するすべての操作を処理します。
ユーザー、グループ、その他のオブジェクトを同期することで一貫したユーザー認証と ID 管理を行います。
同期の仕組みに Connect 同期、クラウド同期の 2種類があります。

2.2. Active directory の基本構成



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。	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。

2.3. グループの種類について

Active Directory には、セキュリティグループと配布グループの 2種類のグループがあります。

・**セキュリティグループ**

ファイルやリソースのアクセス権設定などで利用されるアカウントです。

セキュリティグループは最もよく使われるグループアカウントで、Administrators や Domain Admins などはすべてセキュリティグループに属しています。通常作成されるグループアカウントは、ほとんどセキュリティグループのアカウントです。

・**配布グループ**

主にメールの配布リストとして利用され、複数のユーザーに同時にメールを送信するために使われます。

メーリングリストなどの電子メール一斉配信のために特化したグループであり、セキュリティ設定やアクセス制御などの権限管理には適用できません。

どちらのグループも次ページの3種類のスコープの形式で作成することができます。

2.4. グループのスコープについて

・グループアカウントのスコープ

スコープとは、作成したグループを参照できる範囲のことです。スコープを設定することにより、どの範囲のリソースにアクセスできるか、どのユーザーやグループを追加するのかといったことを定めることが可能です。

Active Directory では、以下の3種類のスコープがあります。

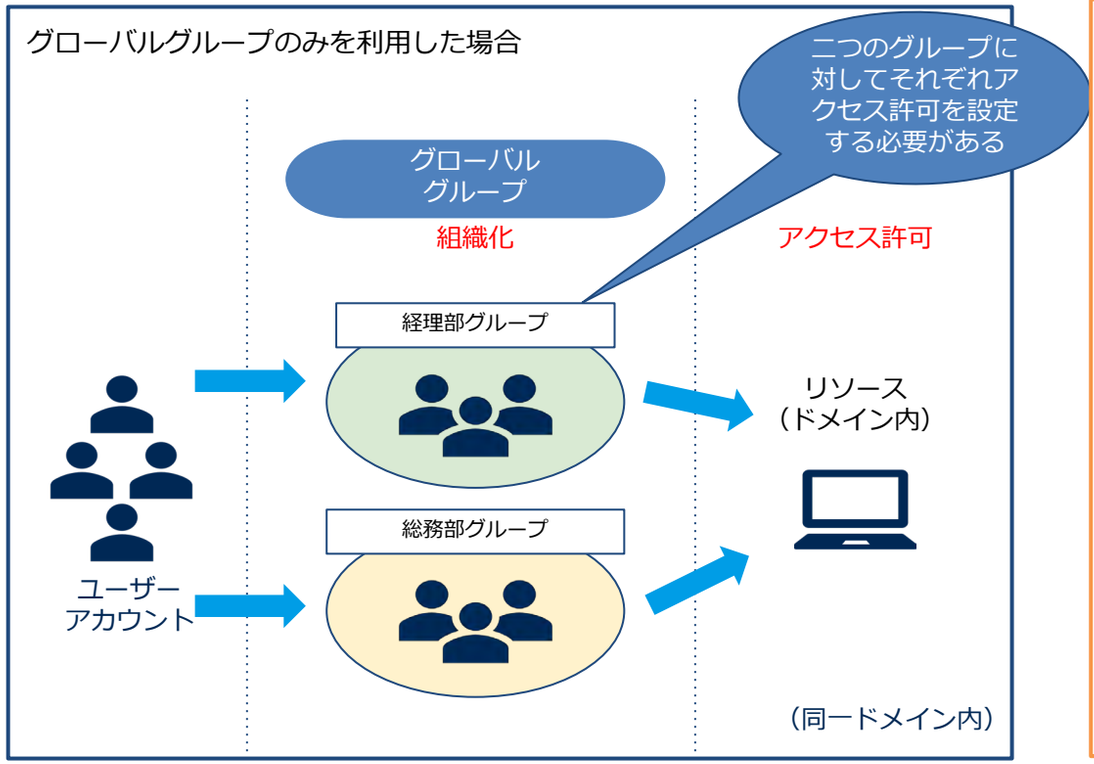
スコープ	アクセス範囲	グループに含めることができるメンバー
ドメイン ローカル グループ	ドメイン内	・フォレスト内のドメイン ユーザー アカウント ・フォレスト内のグローバル グループ ・フォレスト内のユニバーサル グループ ・同一ドメイン内のドメイン ローカル グループ
グローバルグループ	フォレスト全体	・同一ドメイン内のドメイン ユーザー アカウント ・同一ドメイン内のグローバル グループ
ユニバーサルグループ		・フォレスト内のドメイン ユーザー アカウント ・フォレスト内のグローバル グループ ・フォレスト内のユニバーサル グループ

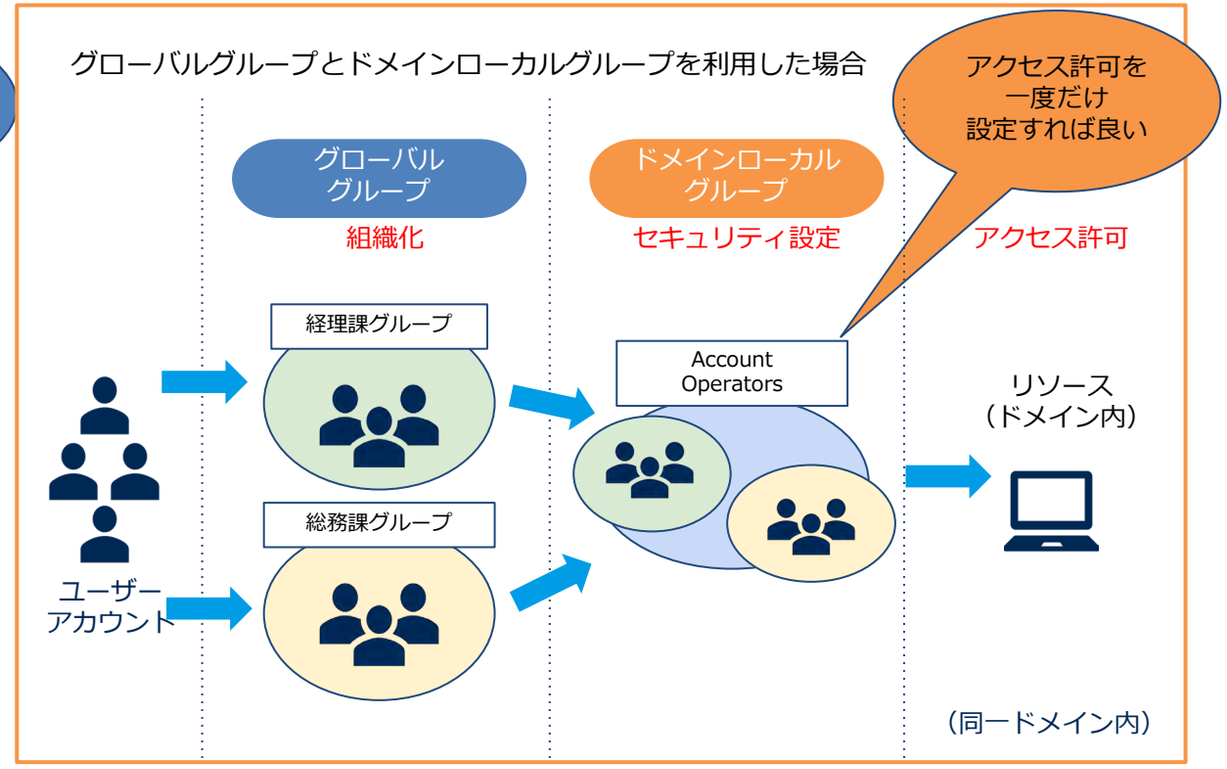
グループアカウントを作成すると、スコープは既定でグローバルグループとなります。

次ページで目的やメリットについて説明します。

2.4. グループのスコープについて

グループを利用する目的は二つあります。一つは、部署や役職などに基づいてユーザーをまとめる目的、
もう一つは、アクセス許可をまとめて割り当てるためです。
この二つの目的が一つのグループで実現できない場合が多いので、グローバルグループとドメインローカルグループのように二種類のグループを作成して使い分けるようにすれば、効率よくアクセス許可を割り当てることが可能となります。
次ページから各スコープの詳細について説明します。





2.4. グループのスコープについて

・ドメインローカルグループ

主に**アクセス権の管理**に使用します。他のドメインのユーザーやグループも追加可能です。

共有フォルダー、プリンター、リモートデスクトップなどのアクセス管理に最適です。

・グローバルグループ

ユーザーを整理・管理するためのグループに適していいます。

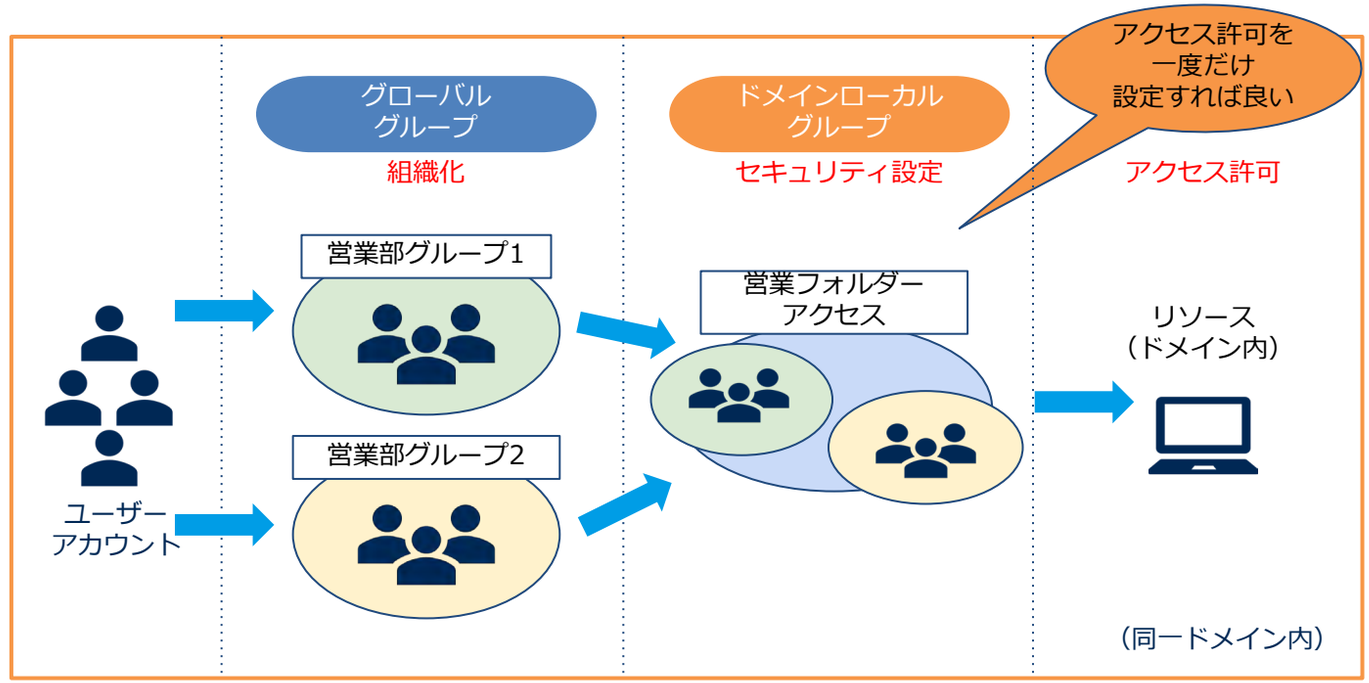
同じドメインのユーザー・グローバルグループのみメンバーにできます。異なるドメインのユーザーを直接追加できません。

【使用例】

＊共有フォルダーやプリンターのアクセス管理

営業部のメンバーをまとめたグローバルグループを、「営業フォルダーアクセス (ドメイン ローカルグループ)」に追加します。

「営業フォルダ アクセス（ドメインローカルグループ）」に、共有フォルダへのアクセス許可を設定します。



2.4. グループのスコープについて

・ユニバーサルグループ

異なるドメイン間でのアクセス管理に最適です。

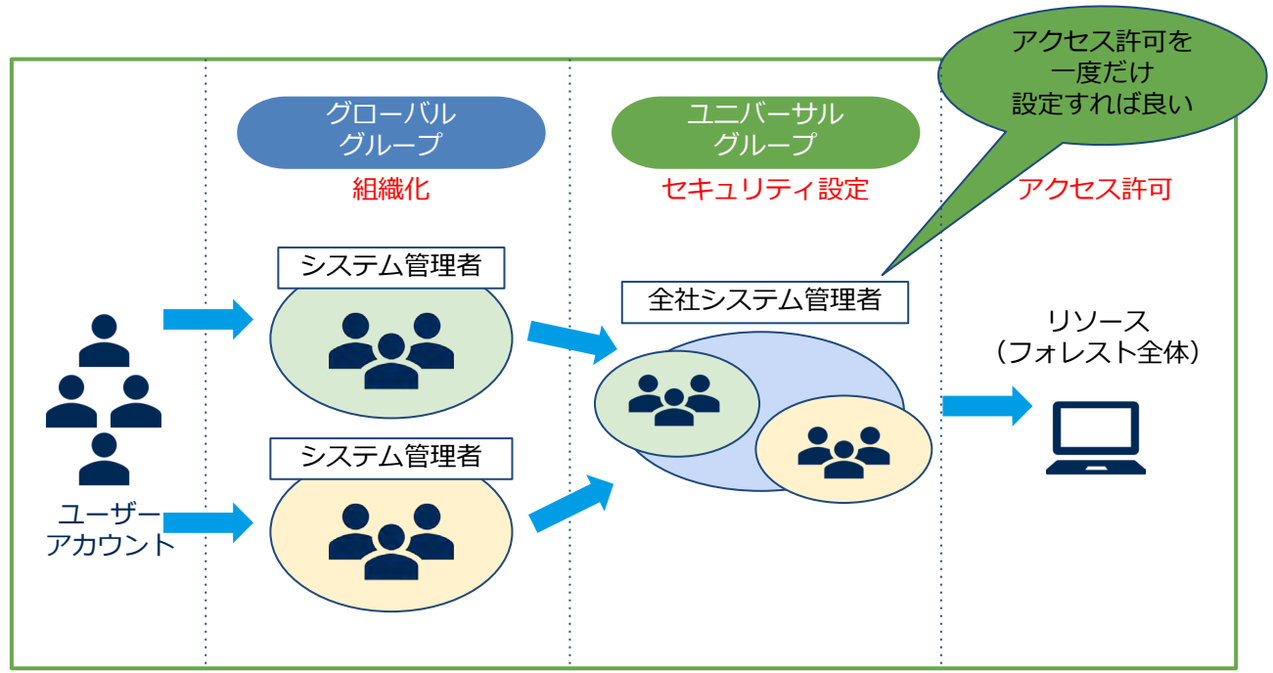
複数のドメイン間で利用可能 (フォレスト全体)であり、他ドメインのグローバルグループ・ユニバーサルグループ・ユーザーを追加可能です。

【使用例】

＊異なるドメイン間でのアクセス管理

各ドメインの管理者をまとめた「システム管理者(グローバルグループ)」を、「全社システム管理者(ユニバーサルグループ)」に追加します。

「全社システム管理者（ユニバーサルグループ）」に、フォレスト全体のリソースのアクセス許可を設定します。



3. Entra Connect 構成時に作成される4つのセキュリティグループについて

3.1. Active Directory 構成時に作成されるセキュリティグループ

Active Directory にデフォルトで作成されるセキュリティグループ（ドメインローカルグループ）と、その主な役割・権限は以下となります。

グループ名	役割・権限
Domain Admins	ドメイン全体を管理するためのグループ。 このグループのメンバーは、ドメイン内のすべてのコンピューターに対するフルコントロール権限を持ちます。
Enterprise Admins	フォレスト全体を管理するためのグループ。メンバーは、すべてのドメインに対して管理権限を持ちます
Schema Admins	スキーマの変更を行うためのグループ。スキーマはActive Directoryのデータ構造を定義します。
Administrators	ドメインの重要な管理タスクを実行するためのグループ。 このグループのメンバーは、ドメイン内のすべてのコンピューターに対する管理権限を持ちます。
Account Operators	ユーザーアカウントの作成と管理を行うグループ。メンバーは、一般的なユーザーアカウントの管理タスクを実行できますが、 管理者アカウントの管理はできません。
Backup Operators	システムのバックアップと復元を行うグループ。メンバーは、バックアップと復元の操作を実行できます
Server Operators	サーバーの管理を行うグループ。メンバーは、サーバーの管理タスクを実行できますが、ドメイン全体の管理は行えません。
Users	ドメインに参加するすべてのユーザーが含まれるグループ。このグループには、基本的なユーザー権限が付与されています。

本資料では、Entra Connect構成時に「Users」内に作成される4つのグループの権限について詳しくご紹介していきます。

。

3.2. Entra Connect構成時に作成される4つのセキュリティグループ

Microsoft Entra connect（旧Azure AD Connect） のインストールを実行するときに既定で以下の4つのセキュリティ グループがインストールされます。
(Active Directoryのデフォルトインストール時には自動的に作成されません)

ADSyncAdmins
ADSyncOperators
ADSyncPasswordset
ADSyncBrowse

これらのグループは、EntraConnectの適切な管理と同期を行うために重要です。それぞれのグループには特定の役割と権限があり、EntraConnectの設定や運用を円滑に行うために設けられています。

尚、これらのデフォルトのセキュリティグループを使用しなくても、同じような権限を持つカスタムグループを作成することができます。カスタムグループを作成する際には、必要な権限を手動で設定する必要がありますが、これにより特定のニーズに合わせた権限管理が可能になります。

次のページから各グループの権限についてご説明いたします。

3.2. Entra Connect構成時に作成される4つのセキュリティグループ

1. ADSyncAdmins

Microsoft EntraIDの管理タスク（構成の変更や同期プロセスの管理）等を行います。
同期マネージャ（Synchronization Service Manager ）を操作し同期したり、Synchronization Rules Editor にて同期ルールの設定変更などが行えます

2. ADSyncOperators

Microsoft EntraConnectの状態を監視したり、同期確認エラーの確認などを行えます。
一部の読み取りタスクを実行できるが同期ルールの設定変更等を行う権限はありません。

3.2. Entra Connect構成時に作成される4つのセキュリティグループ

3. ADSyncPasswordSet

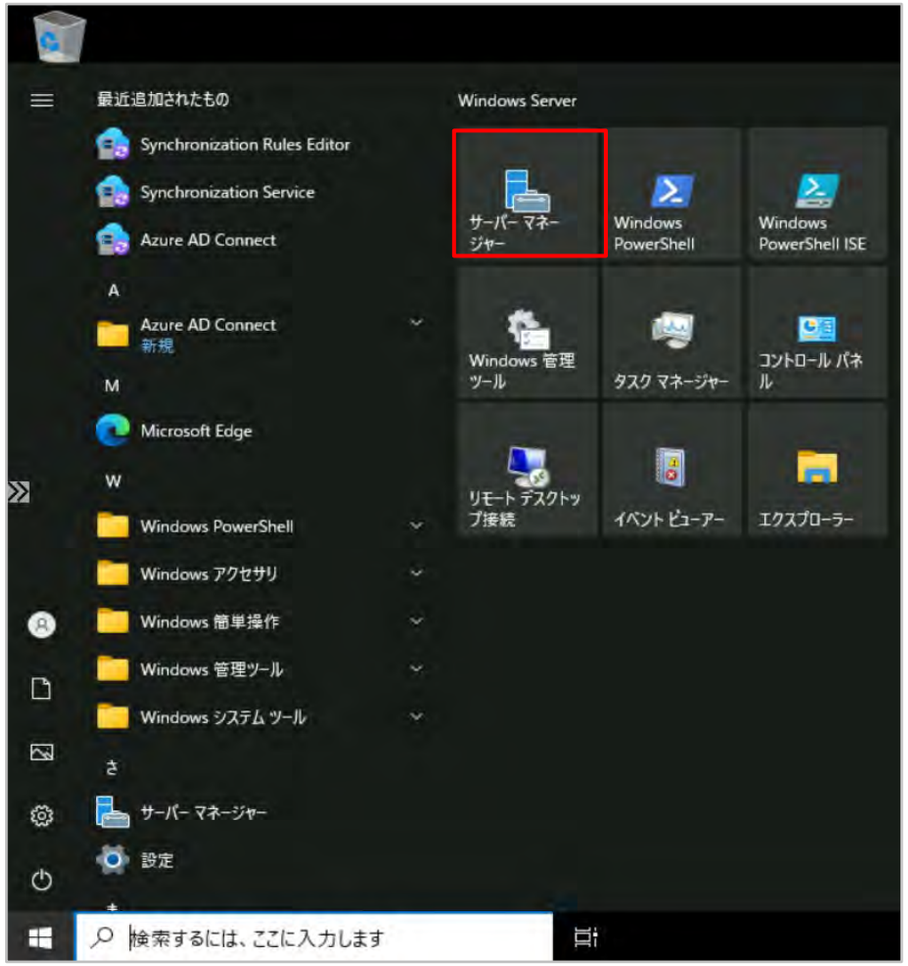
WMIのパスワード管理インターフェイスを使用して、すべての操作を実行する権限を持ちます。
尚、グループにユーザーを追加してパスワードリセットの権限を直接追加する用途では使用されません。
（PowerShell 経由でパスワードを変更するのに必要な権限もないことが考えられます）
※Admin権限を持つユーザーであれば、サーバーマネージャーからパスワード変更は可能です。
基本的にパスワードの変更はAdmin権限をもつユーザーが行うことを想定されています。

4. ADSyncBrowse

WMI を使ったパスワードのリセット時にユーザーの情報を集める権限を持ちます。
PowerShell で直接ユーザーが情報を収集するのではなく、Microsoft EntraConnect の機能が WMI を通じてシステム内部で自動的に処理し、ユーザー情報を取得する 形になります。

4. グループの確認・ユーザー追加手順

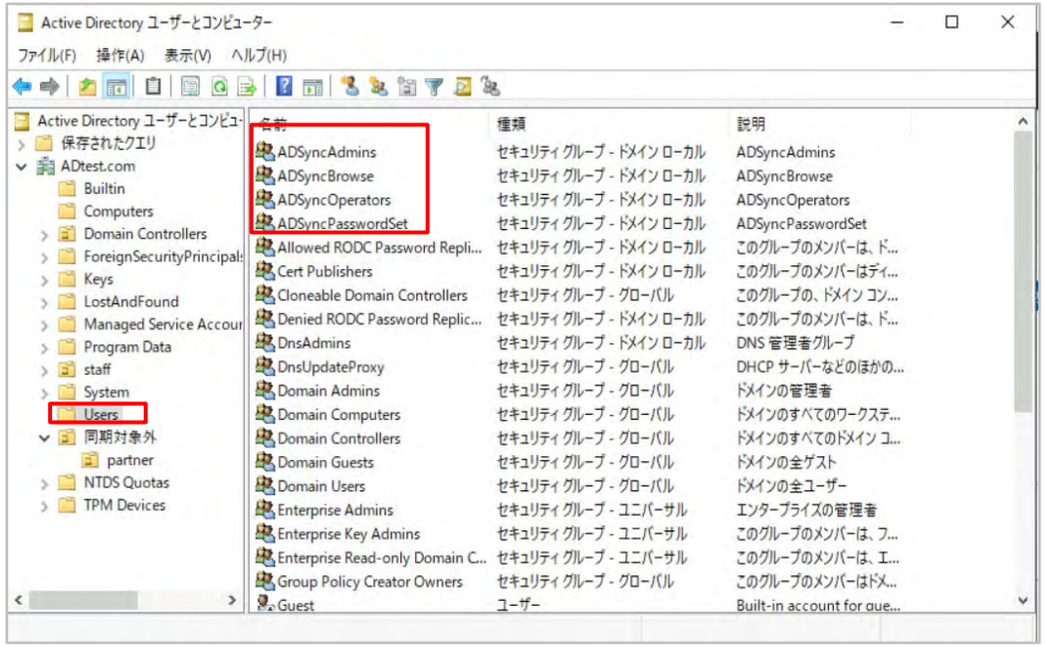
4. グループの確認・ユーザー追加手順



【グループの確認手順】

1. スタートボタンからサーバーマネージャーを起動します。

4. グループの確認・ユーザー追加手順



2. 画面右上のメーニューバーより

［ツール］ > ［ Active Directory ユーザーとコンピューター ］をクリックします。

3. [Users] 内に、以下4つのグループがあることを確認します。

ADSyncAdmins

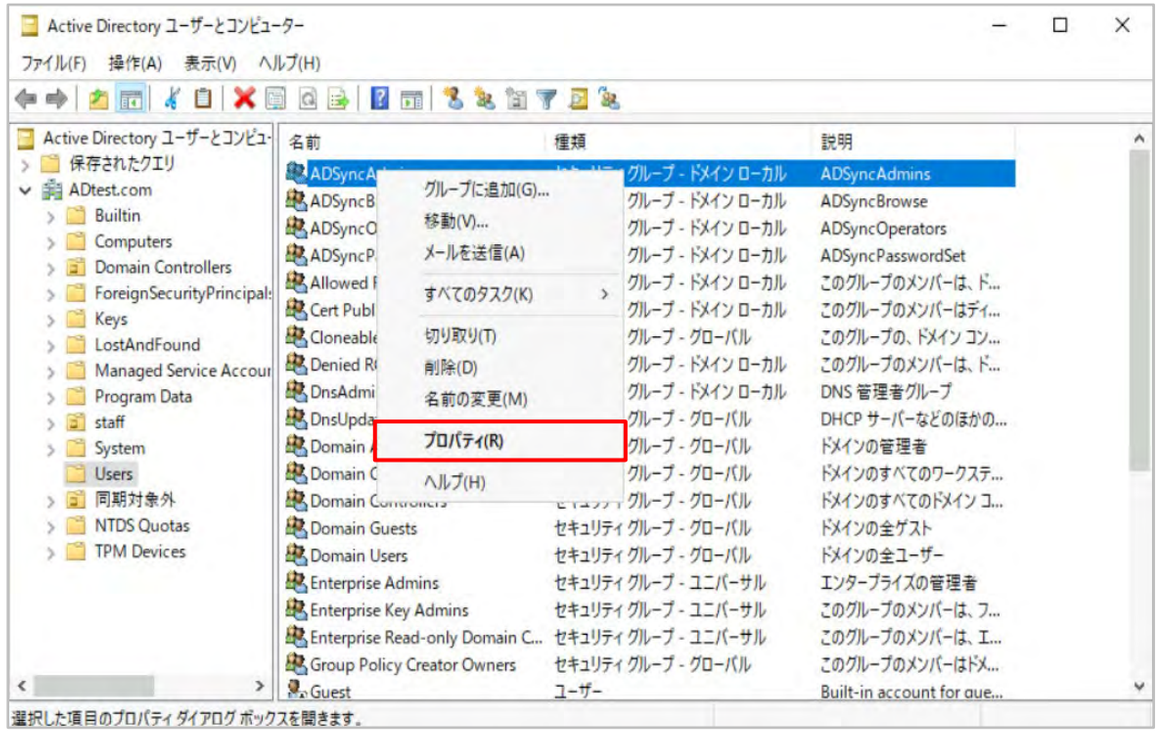
ADSyncBrowse

ADSyncOperators

ADSyncPasswordSet

。

4. グループの確認・ユーザー追加手順



【プロパティの確認手順】

1. 確認したいグループを右クリックし「プロパティ」をクリックします。

4. グループの確認・ユーザー追加手順

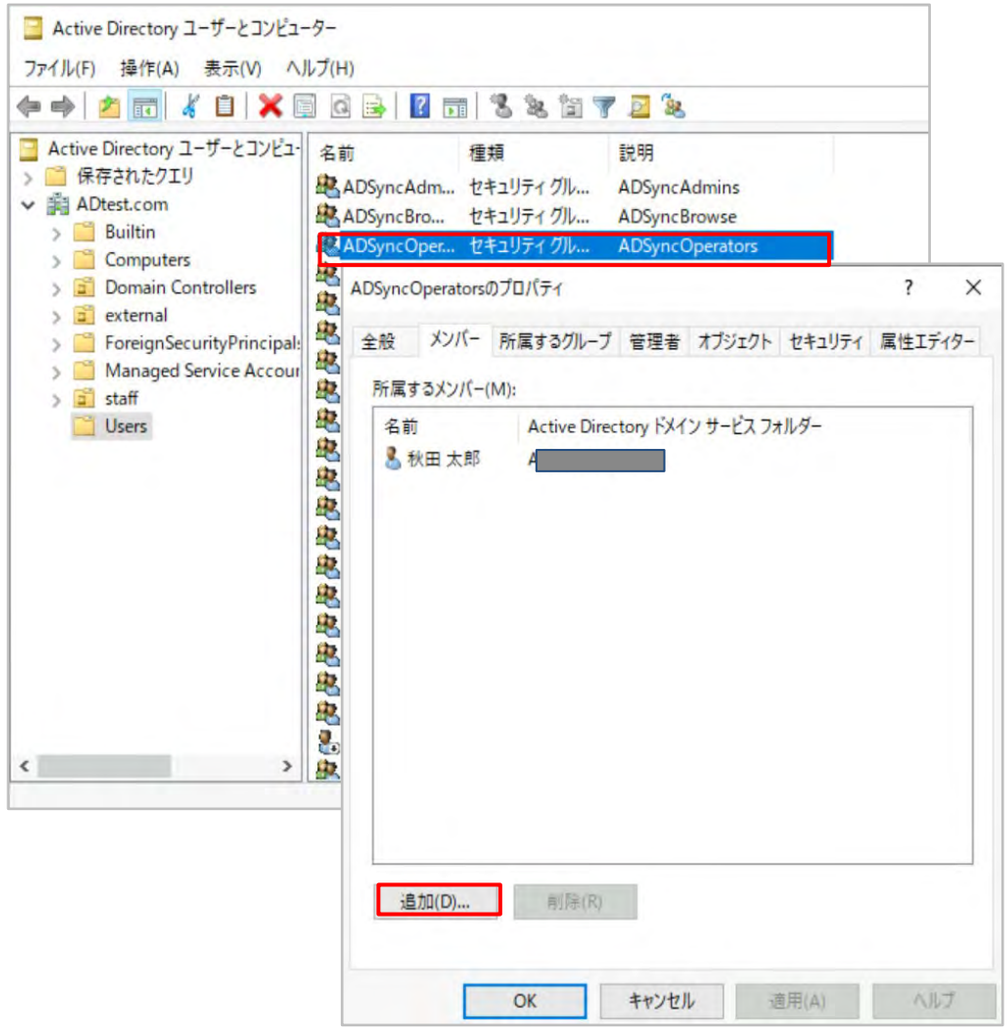
【例】 ADSync Admins のプロパティ初期値

2. [全般]タブが表示され、以下の値が初期値として入力されています。

・説明：ADSyncAdmins（グループ名）
・電子メール：空欄
・グループのスコープ：ドメインローカル
・グループの種類：セキュリティ
・メモ：空欄

※他3グループ（ADSyncBrowse、ADSyncOperators、ADSyncPasswordSet）も同様の値が既定で入力・選択されています。

4. グループの確認・ユーザー追加手順



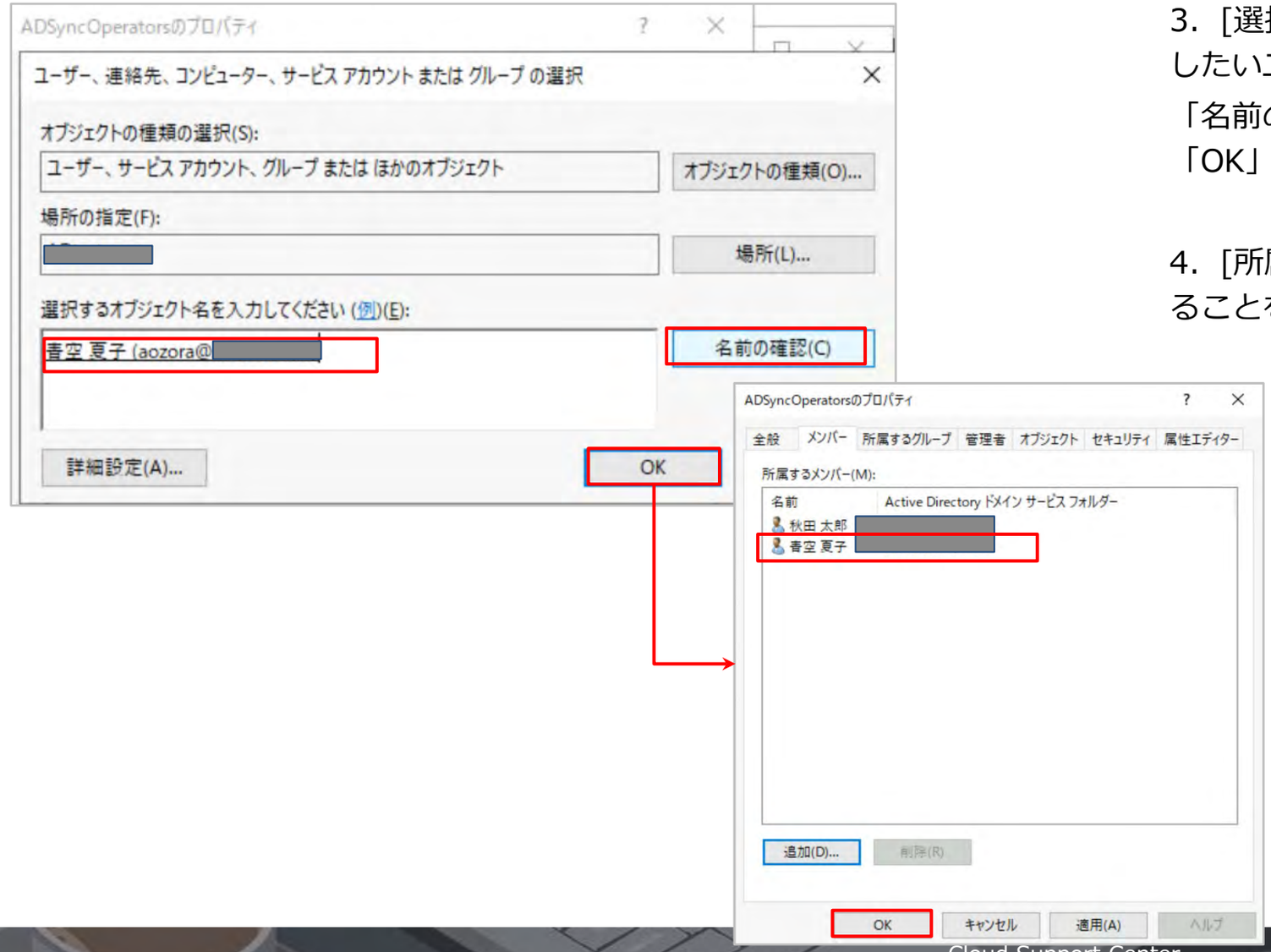
【グループへユーザーの追加手順】

1．グループ名をダブルクリック、もしくは右クリック> [プロパティ]をクリックします

2．[メンバー]タブにて「追加」をクリックします

※[所属するメンバー]には現在追加されているアカウントが表示されます。

4. グループの確認・ユーザー追加手順



3. [選択するオブジェクト名を入力してください]欄に、追加したいユーザー名を入力し（一部でも可）、
「名前の確認」をクリックしユーザーに間違いなければ
「OK」をクリックします

4. [所属するメンバー]欄に追加したユーザーが表示されていることを確認し「OK」をクリックします

5. テストケース検証

5.1. テストケース検証とその結果

本書は以下のテストケースに沿って検証を行っています。検証の詳細は [5.2. テストケース①] ～ [5.4. テストケース③] をご確認ください。

No.	グループ	テストケース	内容	検証結果
1	・ADsyncAdmins ・ADsyncOperators	同期マネージャでの同期ログ閲覧、同期実行確認	同期マネージャで同期のログが確認できること、手動で同期実行ができることを確認	ログの閲覧・同期実行ができることを確認できました
2	ADsyncAdmins	同期ルール作成・変更	Synchronization Rules Editorにて同期ルールの作成・変更ができることを確認	Synchronization Rules Editorにて同期ルールの作成・変更ができることを確認できました
3	ADsyncPasswordSet	パスワードリセット確認	Powershellにて、他アカウントのパスワードを変更できないことを確認	パスワードリセットを実行できませんでした

5.2. テストケース①
同期マネージャでの同期ログ閲覧、
同期実行確認

5.2.テストケース① 同期マネージャでの同期ログ閲覧、同期実行確認

■検証内容
・同期マネージャで同期ログの閲覧、同期の実行ができることを確認します。
「AdsyncAdmins」グループ、「ADsyncOperators」グループに所属するそれぞれのユーザーにて確認します。

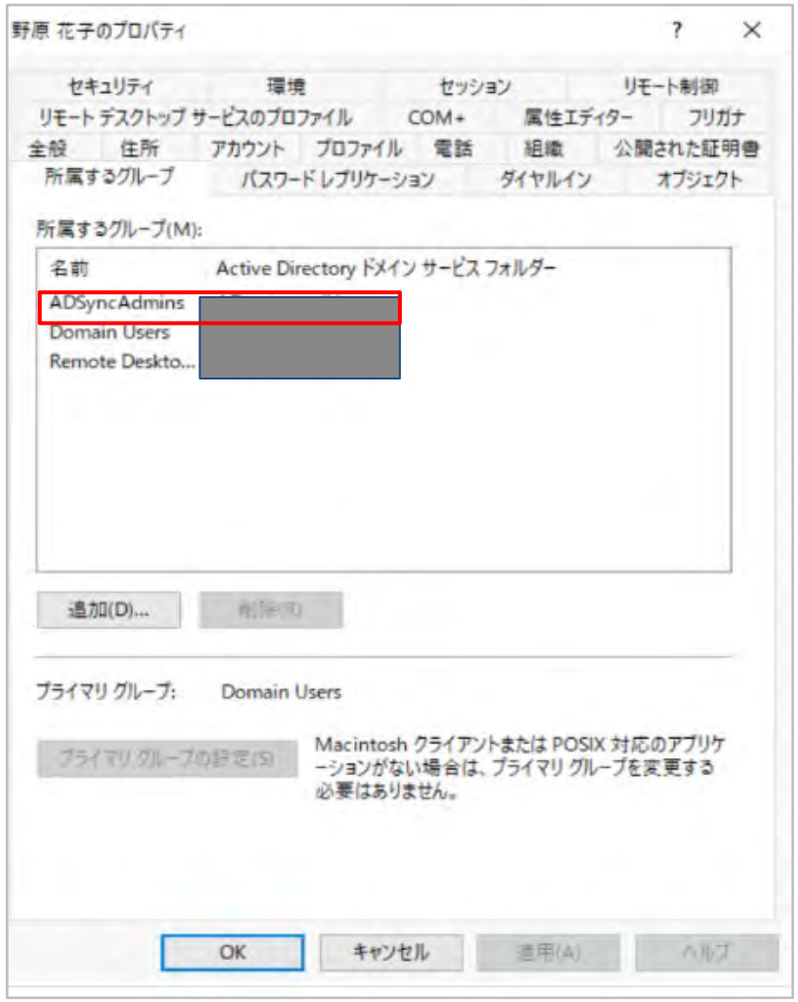
■検証条件
1・対象ユーザーを「AdsyncAdmins」グループに追加
2・対象ユーザーを「ADsyncOperators」・「ADsyncBrowse」グループに追加

■検証結果
・「AdsyncAdmins」、「ADsyncOperators」グループに所属するそれぞれのユーザーは
同期マネージャにて、同期ログの閲覧、同期の実行をすることができました。

【備考】
・「AdsyncAdmins」グループ：同期マネージャで全てのタブ（「Operartions」,「Connectors」,「Metaverse Designer」「Metaverse Search」）が表示され、[Actions]から同期以外の項目（「create」「propaties」）等も全て表示され同期以外の設定等も行えるようでした。

・「ADsyncOperators」グループ：同期マネージャで同期の履歴が確認できる「Operartions」タブしか表示されませんでした。
[Actions]から実行できるタスクも同期に関する一部の項目のみ表示され機能が制限されていました。

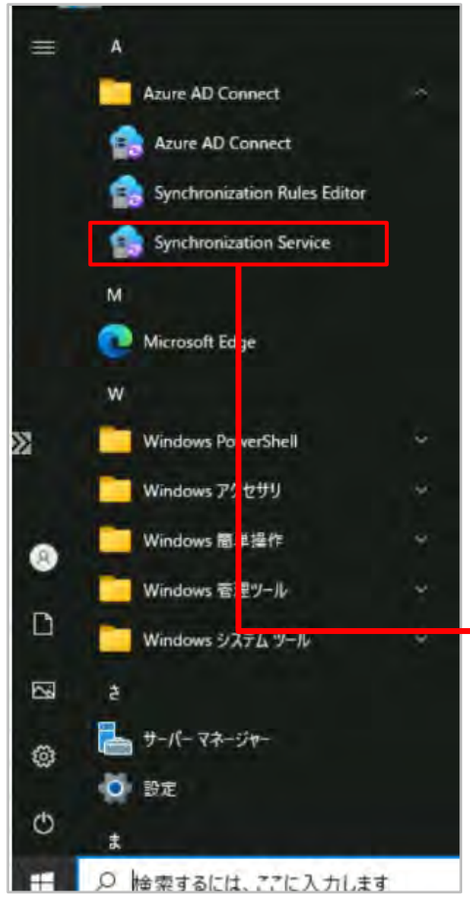
5.2.テストケース① 同期マネージャでの同期ログ閲覧、同期実行確認

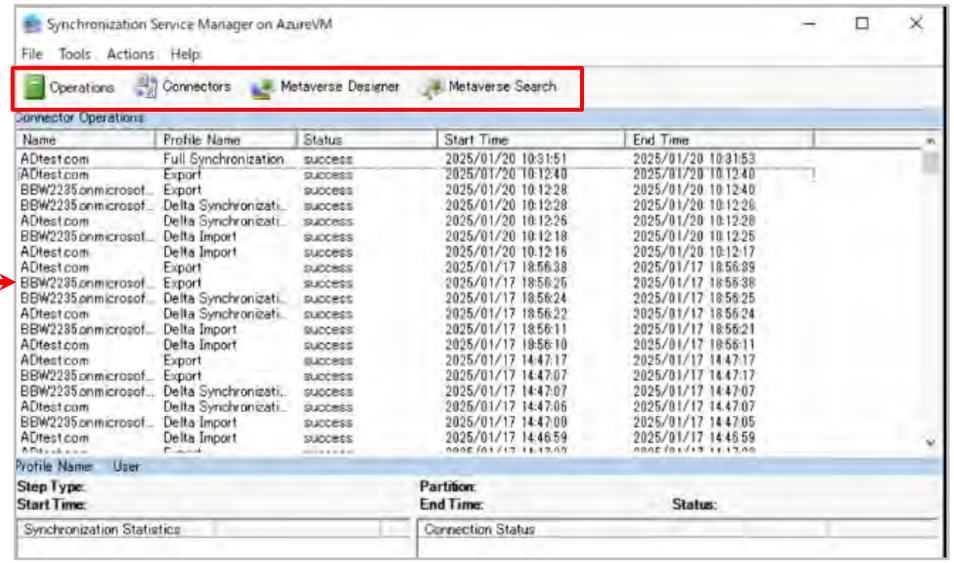


条件１【AdsyncAdmins】

1.対象のユーザーのプロパティ > 所属するグループタブに「AdsyncAdmins 」グループが追加されていることを確認します。

5.2.テストケース① 同期マネージャでの同期ログ閲覧、同期実行確認

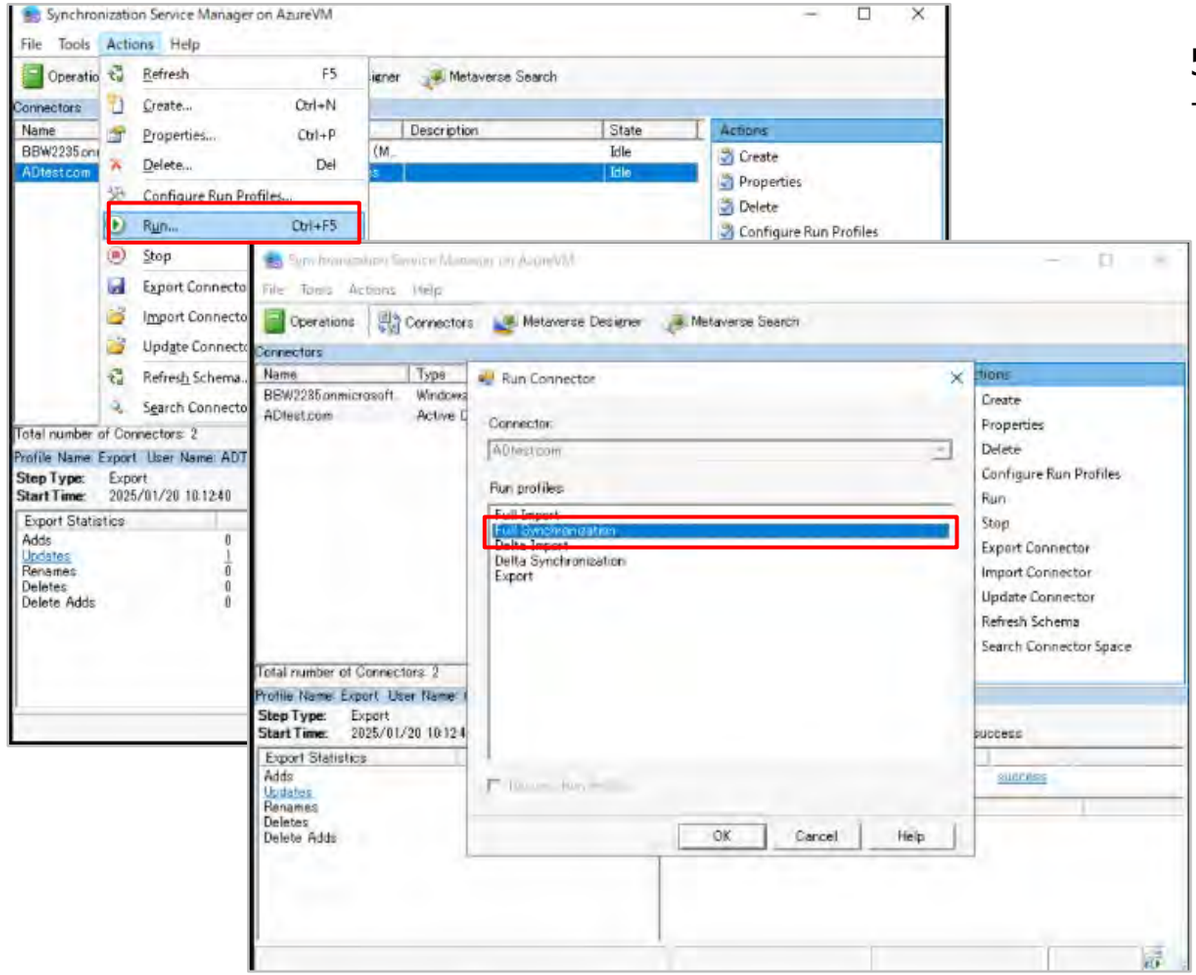




2. ホームボタンから「Synchronization Service」をクリックし開きます

3. Synchronization Serviceにて全てのタブ（「Operartions」,「Connectors」,「Metaverse Designer」 「Metaverse Search」）が表示されていることを確認します

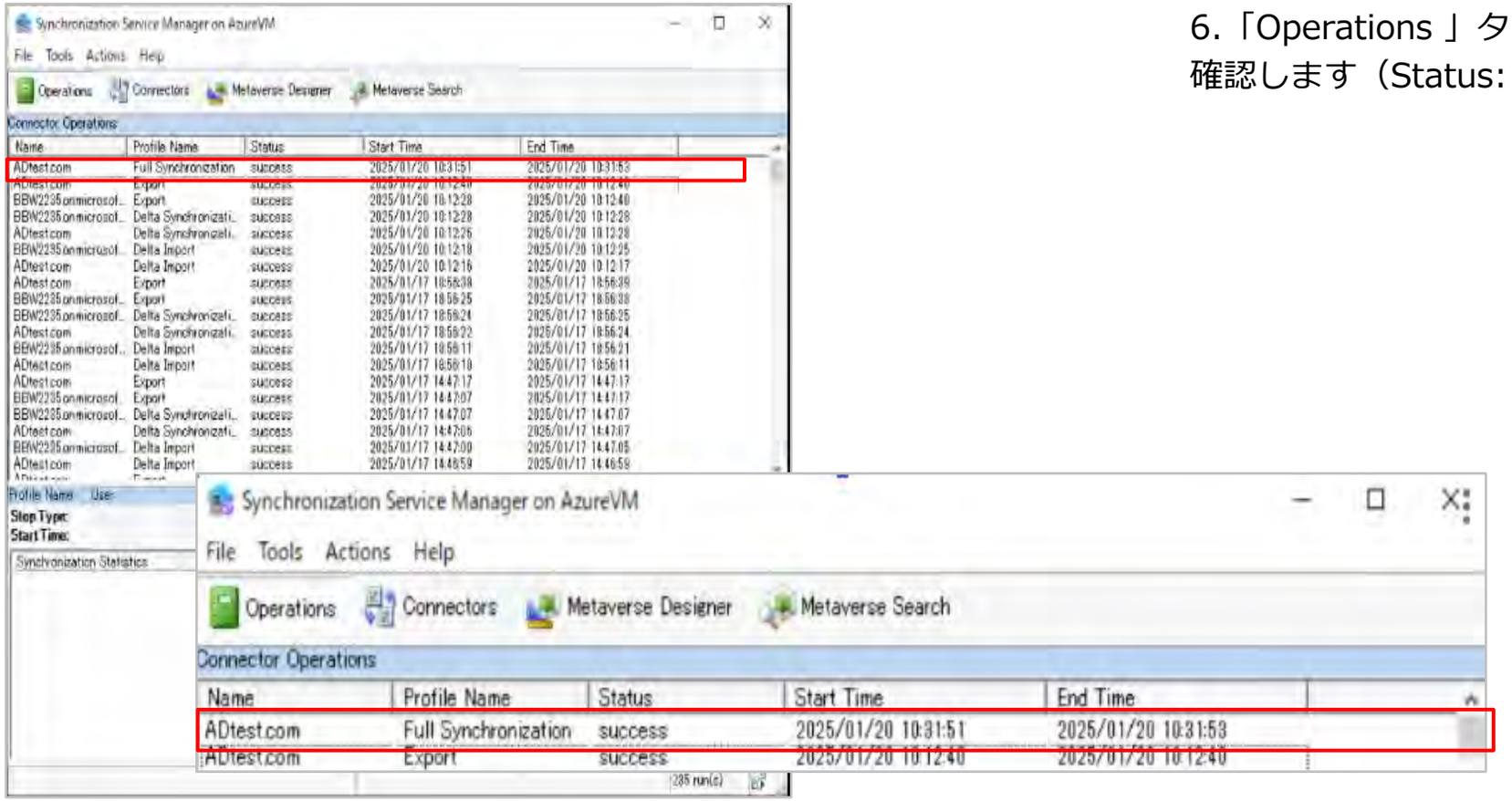
5.2.テストケース① 同期マネージャでの同期ログ閲覧、同期実行確認



4.「Actins」＞「Run」をクリックします

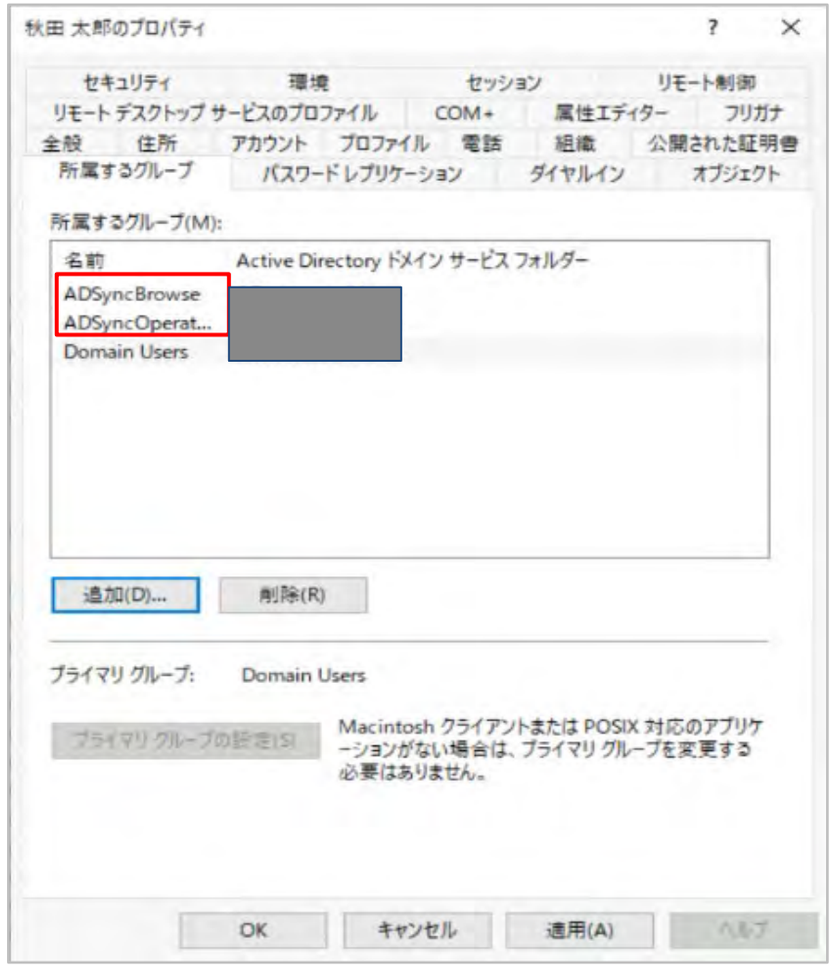
5. 「Full Synchronization」を選択し「OK」をクリックします

5.2.テストケース① 同期マネージャでの同期ログ閲覧、同期実行確認



6.「Operations 」タブにて、データの同期が完了したことを確認します（Status: Success）

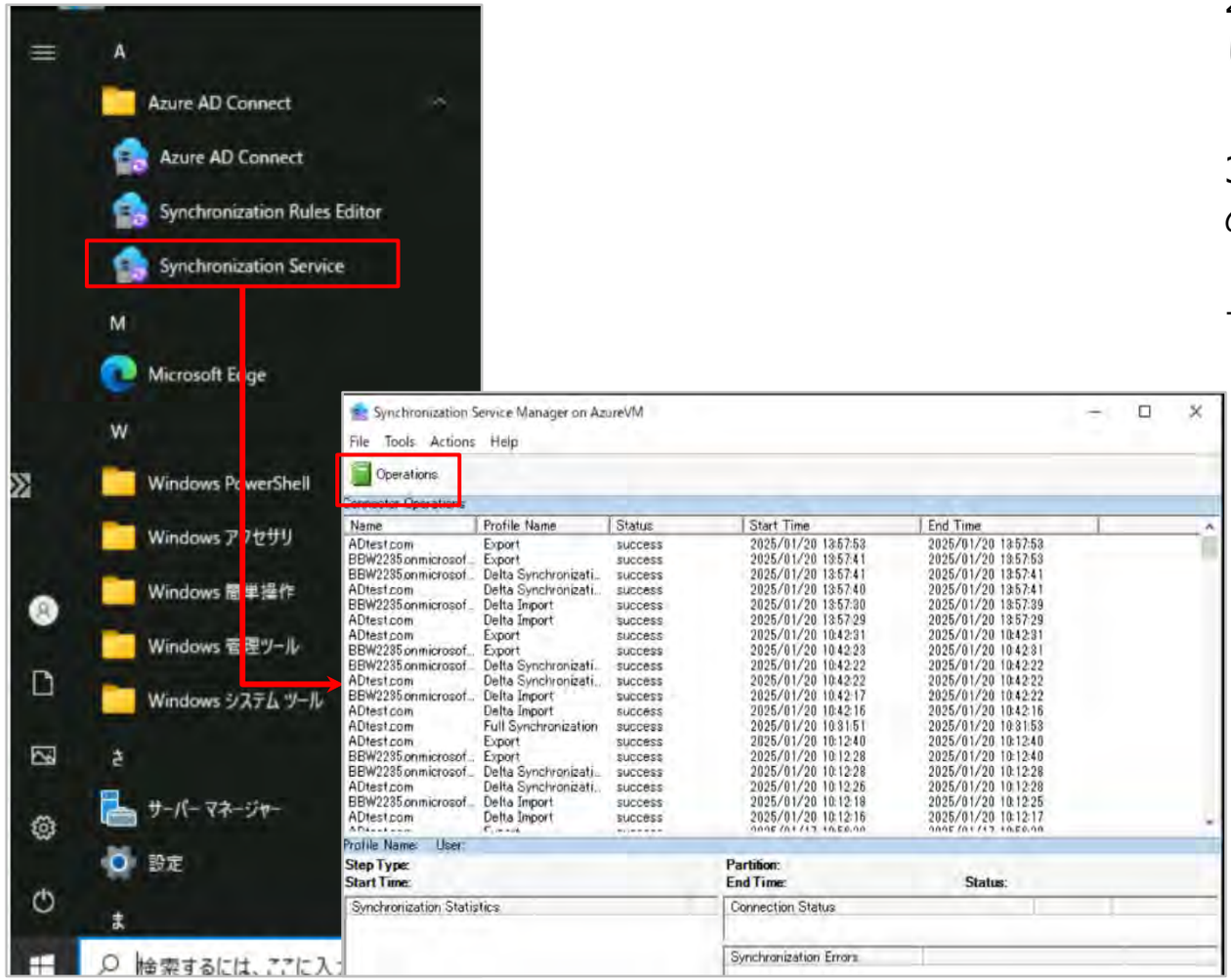
5.2.テストケース① 同期マネージャでの同期ログ閲覧、同期実行確認



条件２【AdsyncOperators】

1. 対象のユーザーのプロパティ > [所属するグループ]タブに「AdsyncBrowse 」、「ADsyncOperators」グループが追加されていることを確認します。

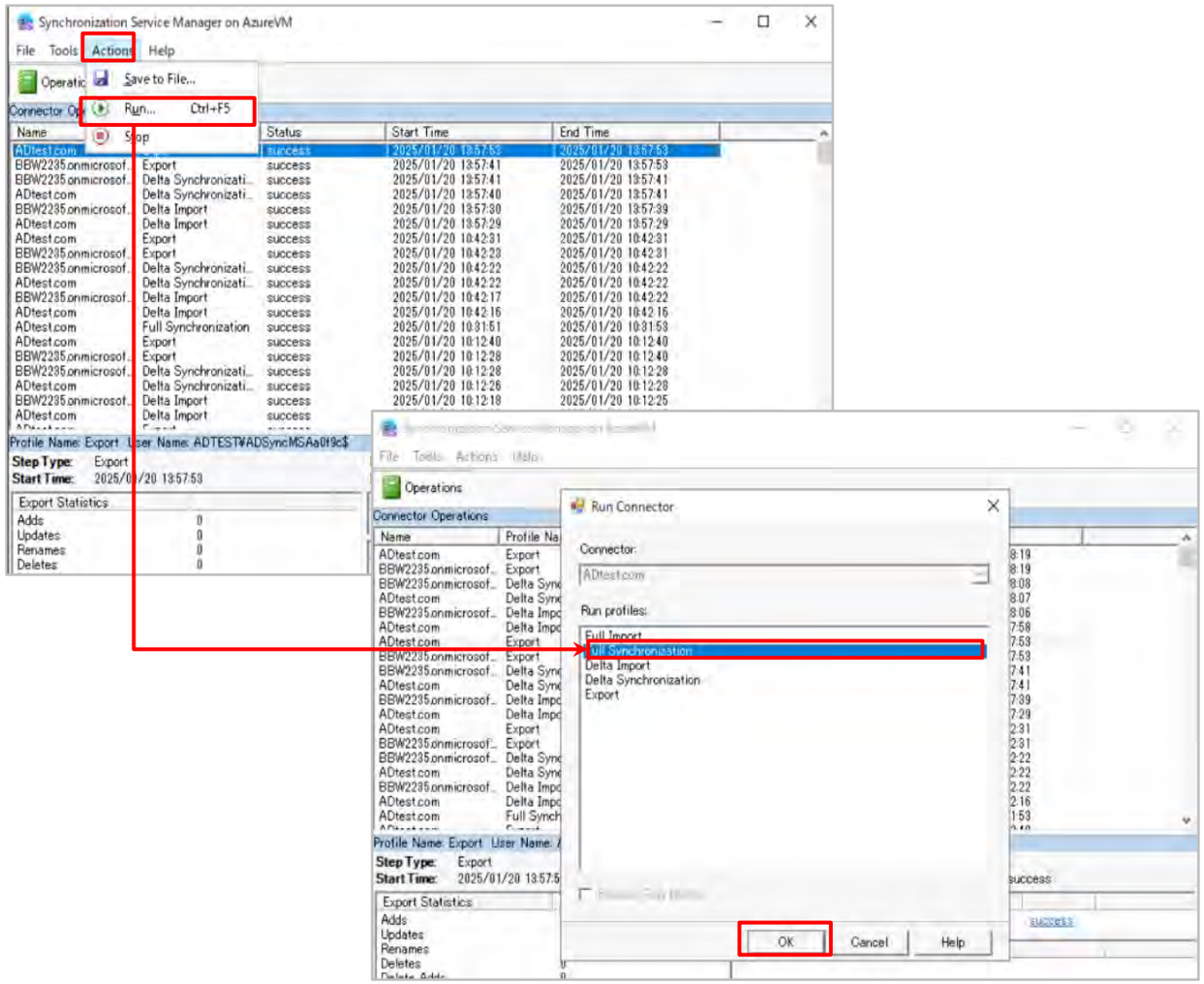
5.2.テストケース① 同期マネージャでの同期ログ閲覧、同期実行確認



2. ホームボタンから「Synchronization Service」をクリックし開きます

3. 同期マネージャにて「Operations」タブのみ表示され、他の3つのタブ（「Connectors」,「Metaverse Designer」「Metaverse Search」）は表示されていないことを確認します

5.2.テストケース① 同期マネージャでの同期ログ閲覧、同期実行確認

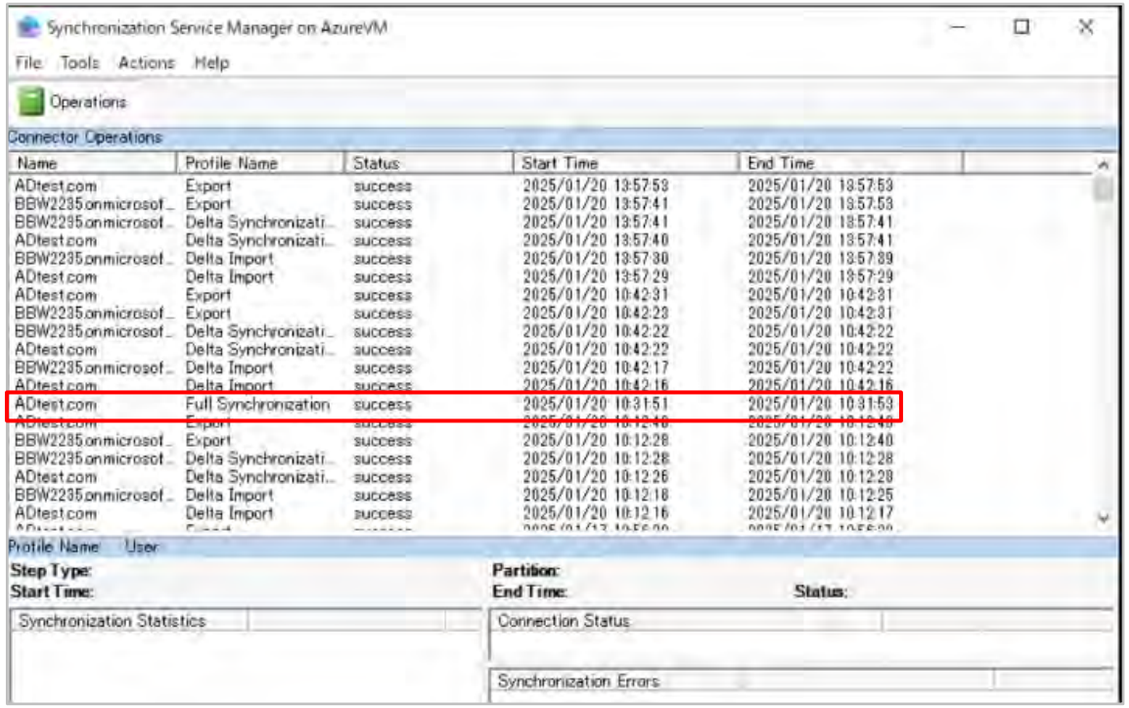


4.「Actins」をクリックします。
　「Save to File」、「Run」「Stop」のみ、選択肢として表示されることを確認します。

5.「Run」をクリックします

6.「Full Synchronization」を選択し「OK」をクリックします

5.2.テストケース① 同期マネージャでの同期ログ閲覧、同期実行確認



7.「Operations 」タブにて、データの同期が完了したことを確認します（Status: Success）

5.3. テストケース②

同期ルール作成・変更の確認

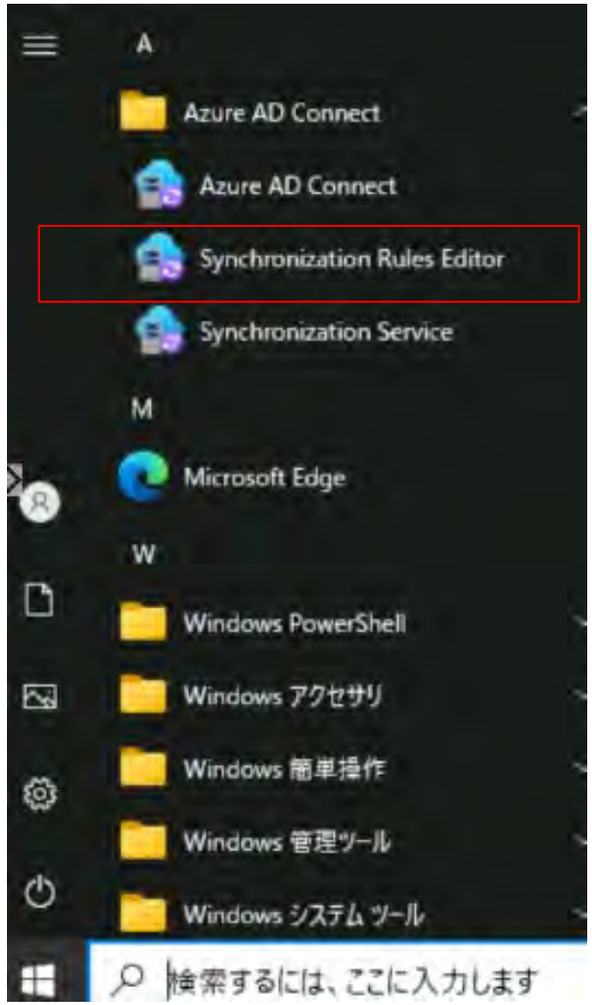
5.3. テストケース③ 同期ルール作成・変更の確認

■検証内容
Synchronization Rules Editor にて同期ルールの作成や設定変更ができることを確認します
「AdsyncAdmins」グループに所属するユーザーにて確認します。

■検証条件
・対象ユーザーを「AdsyncAdmins」グループに追加

■検証結果
Synchronization Rules Editor にて同期ルールを作成したり、設定変更ができることを確認

5.3. テストケース③ 同期ルール作成・変更の確認

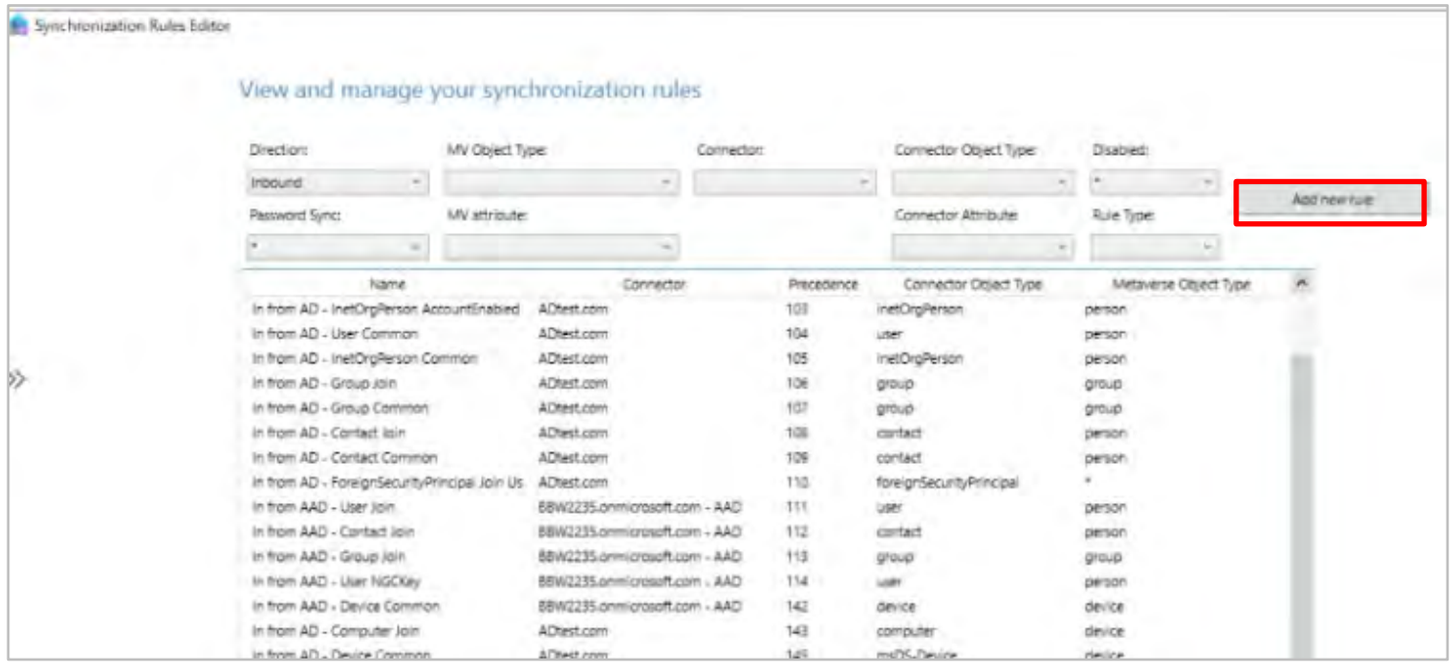


【ADsyncAdmins】同期ルール作成

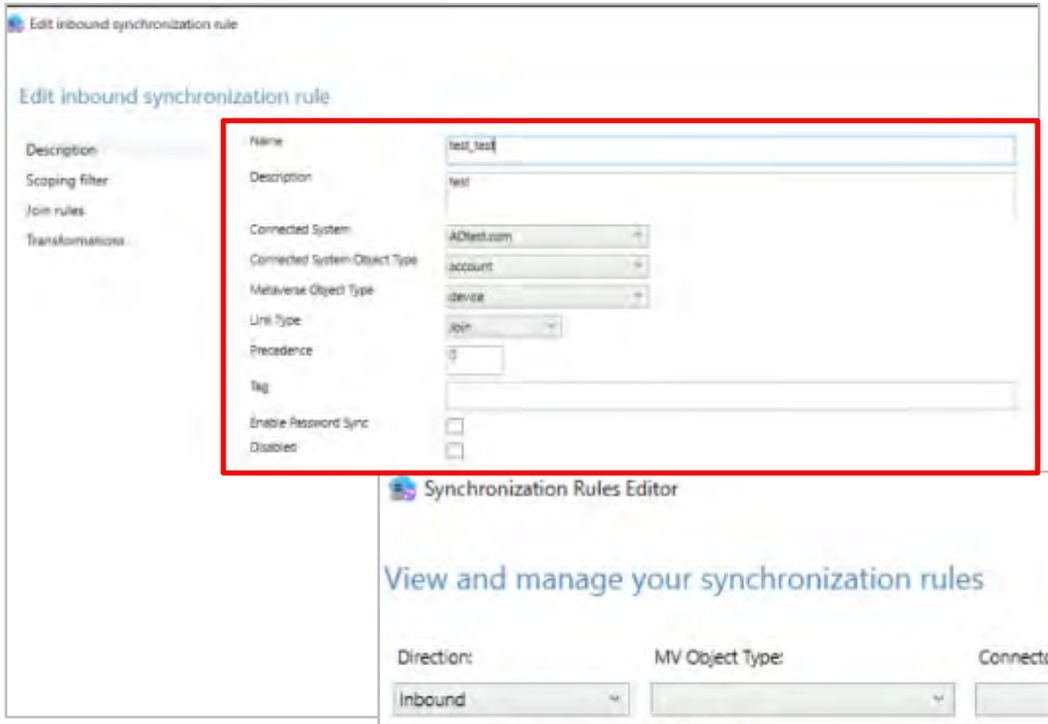
1．ホームボタンから「Synchronization Rules Editor」 をクリックし開きます。

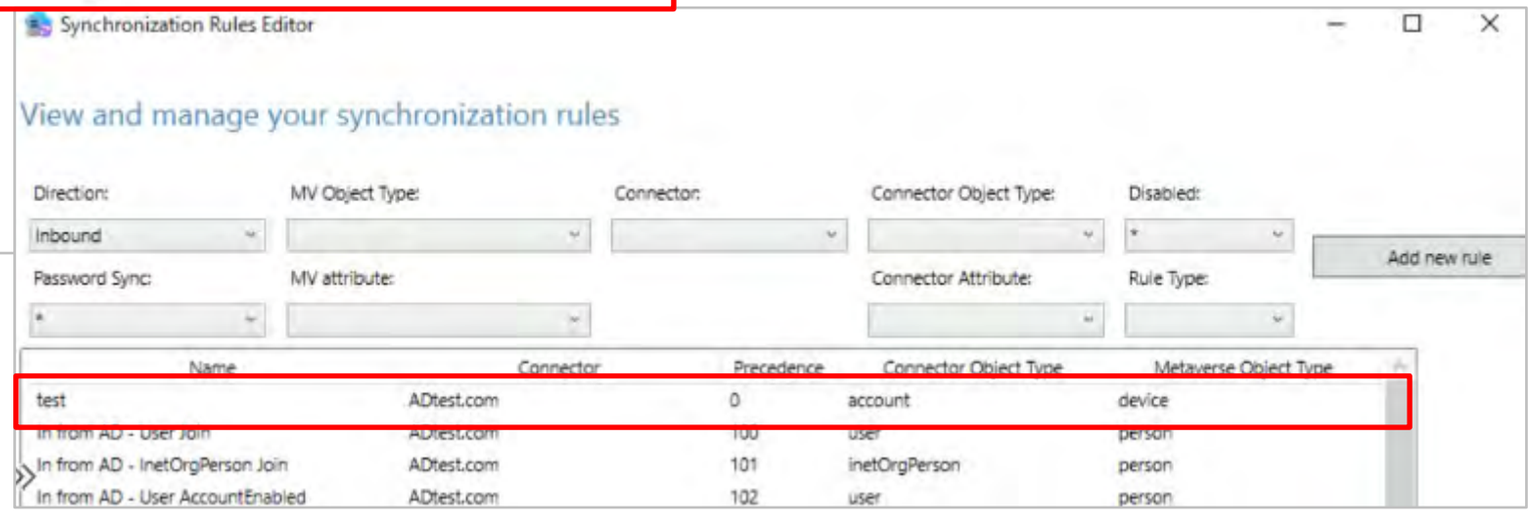
5.3. テストケース③ 同期ルール作成・変更の確認

2.「Add new Rule 」をクリックします



5.3. テストケース③ 同期ルール作成・変更の確認

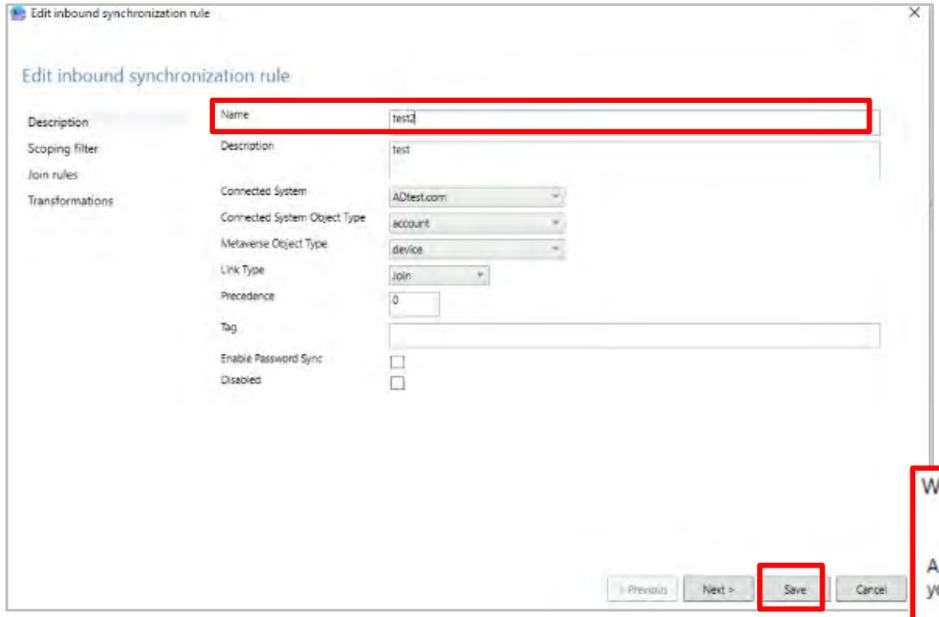


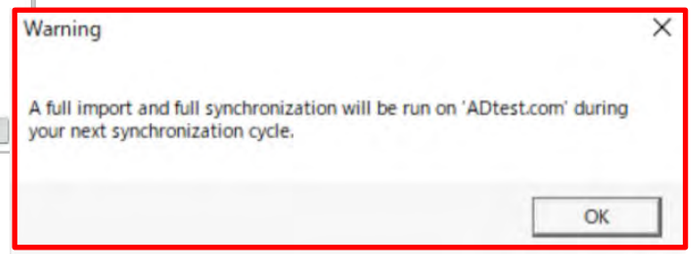


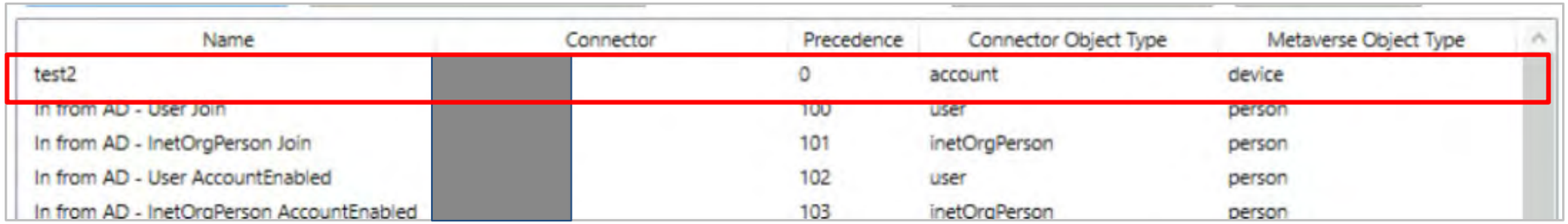
3. ルールの名前や条件を入力し、「Next」をクリックし入力を進め最後に[add]をクリックします

4. 作成したルールが表示されていることを確認します

5.3. テストケース③ 同期ルール作成・変更の確認







Name	Connector	Precedence	Connector Object Type	Metaverse Object Type
test2		0	account	device
In from AD - User Join		100	user	person
In from AD - InetOrgPerson Join		101	inetOrgPerson	person
In from AD - User AccountEnabled		102	user	person
In from AD - InetOrgPerson AccountEnabled		103	inetOrgPerson	person

【ADsyncAdmins】同期ルール変更

1. Editから作成したルールの名前([name])を変更し、Saveします。変更できた旨のメッセージが表示されます

2. ルールが作成されたことを確認します
(検証ではルール名の変更を行っています)

5.4. テストケース③
パスワードリセットの確認

5.4. テストケース③ パスワードリセットの確認

■検証内容
PowerShellにて他のアカウントのパスワードを変更できるかを確認します
「AdsyncPasswordSet」グループに所属するユーザーにて確認します。

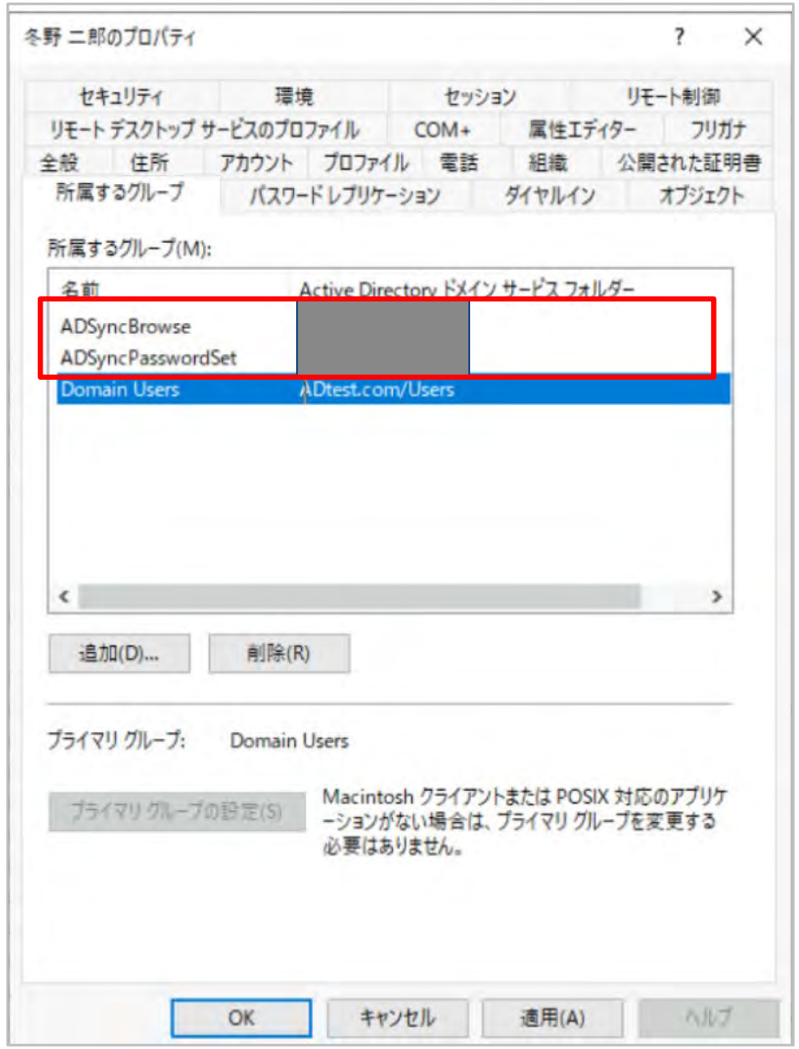
■検証条件
・対象ユーザーを「AdsyncPasswodSet」・「AdsyncBrowse」グループに追加します

■検証結果
・対象ユーザーにてPowershellより、Setコマンドでパスワードの変更を試みましたが
「アクセスが拒否されました」というメッセージが表示され変更することはできませんでした。

当グループの権限/機能に関してMicrosoft社に問い合わせたところ、当グループはパスワードリセットの権限を直接追加する用途では使用されないとのことでした。
また、Microsoft社側にて当グループを含む4グループに関するナレッジが乏しく、過去の事例も少ないことから、
当グループにユーザーを追加してパスワードの管理を行うことは想定されていないことが考えられます。

パスワードの変更/管理においては、Admin権限を持つユーザーであればサーバーマネージャーを使用して簡単に変更することが可能となりますため、通常パスワードの変更/管理はAdmin権限を持つユーザーが行います。

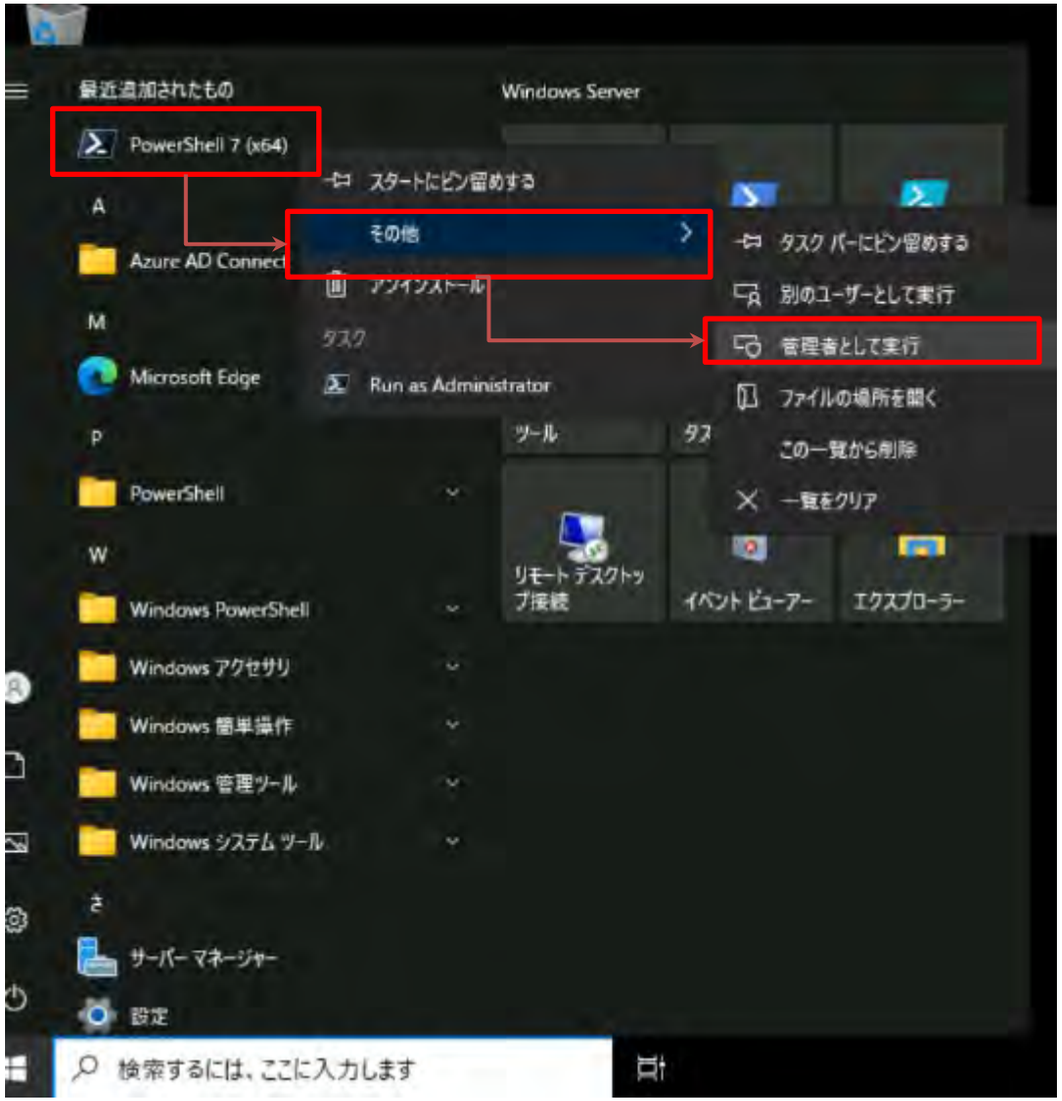
5.4. テストケース③ パスワードリセットの確認



【AdsyncPasswordSet】

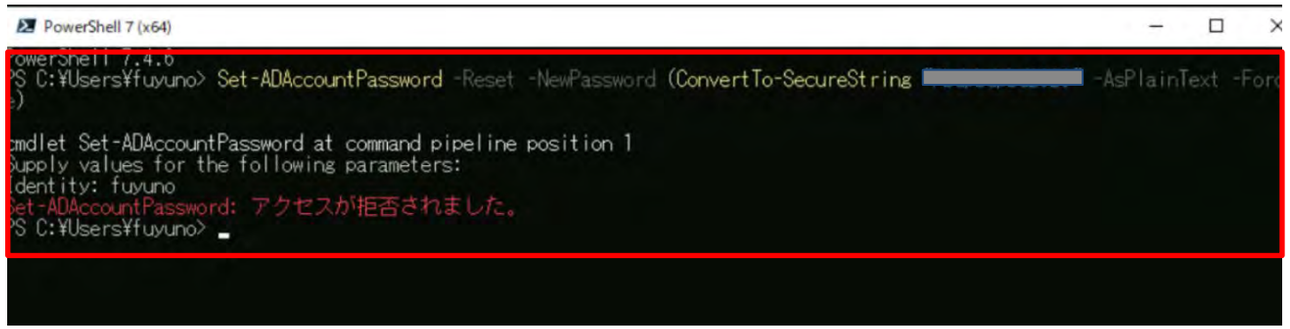
1. 対象のユーザーのプロパティ > 所属するグループタブに「AdsyncAdmins 」・「ADsyncBrowse」グループが追加されていることを確認します。

5.4. テストケース③ パスワードリセットの確認



2. ホームボタンから、Powershellを探し、
右クリック　＞その他＞「管理者として実行」をクリックします

5.4. テストケース③ パスワードリセットの確認



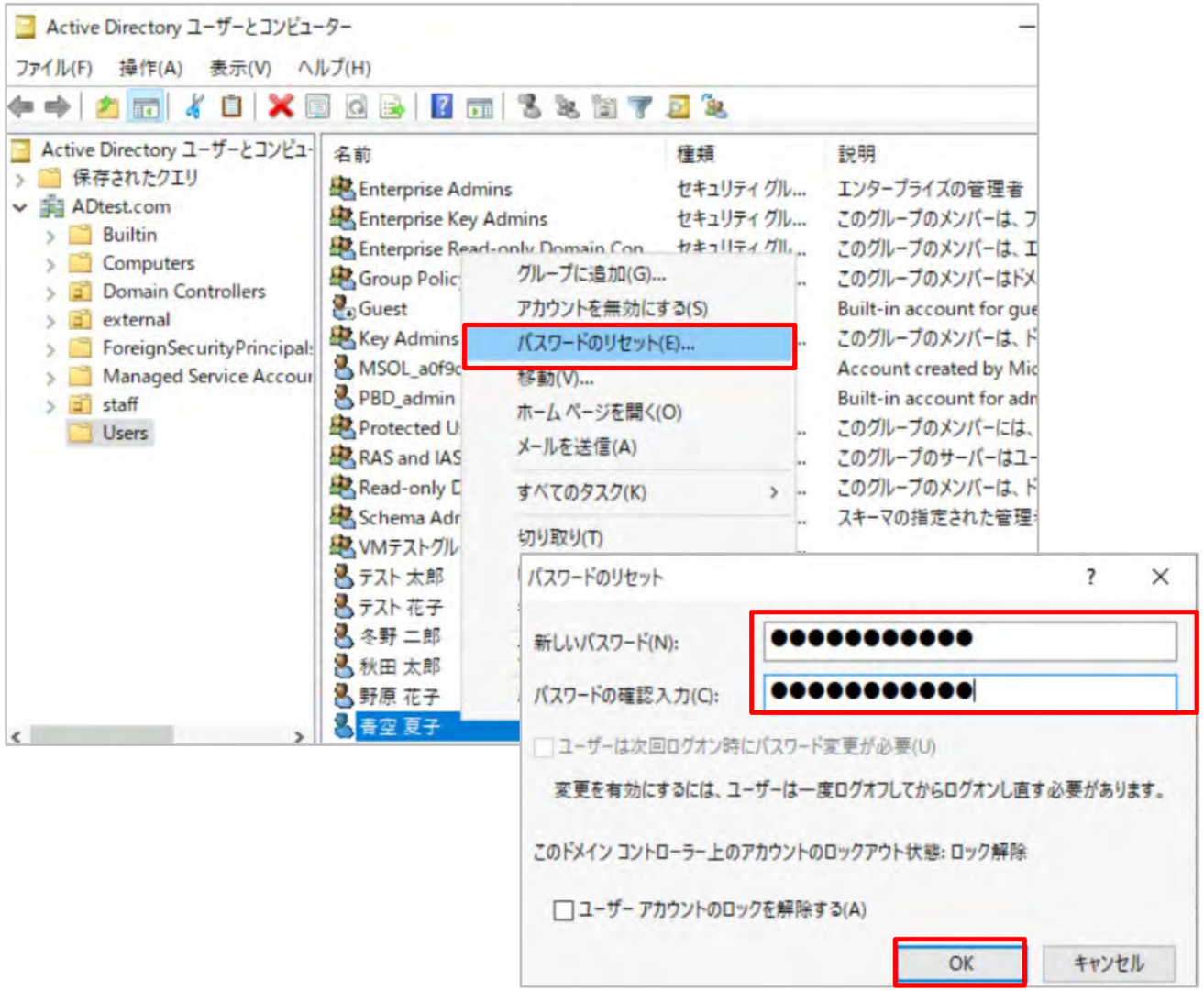
3.Powershellの画面に以下コマンドレットを入力します。

Set-ADAccountPassword -Reset -NewPassword (ConvertTo-SecureString "新しいパスワード" -AsPlainText -Force)

4. [identity：]にパスワードを変更する対象のユーザーアカウントを入力します

5. [アクセスが拒否されました]と表示され、変更を確認することはできませんでした。

5.4. テストケース③ パスワードリセットの確認



【補足】

パスワードの変更は、**Admin権限のユーザー**であれば
本グループに所属しなくとも、サーバーマネージャーから簡単に変更することが可能です

1. サーバーマネージャー[Active Directory ユーザーとコンピューター]から、パスワードを変更したいユーザーを右クリックします

2.「パスワードのリセット」をクリックします

3. 新しいパスワードと確認用にもう一度パスワードを入力し「OK」をクリックします