【Microsoft Entra Connect】同期・認証方式について

2025年2月28日

改定履歴

版数	発行日	改訂内容
第1版	2025年2月28日	初版発行
第2版	2025年2月28日	設定した認証方式に基づいて、ユーザーが正常にサインインできているかを確認する方法について、Microsoft社へ確認出来次第更新予定。 （スライド:40、69、98）

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でご了承ください。

Agenda

1. 前提情報
    1. 前提
    2. 用語集

1. 機能の基本情報
    1. サービス概要
    2. Microsoft Entra Connect 同期について
    3. ハイブリッド環境でない場合の認証方法について

3. Microsoft Entra Connect 認証方式について
    1. パスワードハッシュ同期
    2. パススルー認証
    3. フェデレーション
    4. 認証方式の比較

3. 設定手順
    1. ユーザー作成
    2. 同期ステータス確認
    3. パスワードハッシュ同期 設定
    4. パススルー認証 設定
    5. フェデレーション 設定

1. 前提情報

1.1. 前提条件

・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2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	・Entra Connectにて同期を行う際、パスワードハッシュ同期の構成を取っており、 Kerberos認証を使用していないため、復号化キーのロールオーバーは行う必要性はあるか

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	Kerberos (ケルベロス) 認証	サーバーとクライアント間の身元確認に使うプロトコルのことで、ネットワーク認証方式の一つです。 Kerberos認証では、クライアントとサーバーを相互に認証して互いの通信を暗号化することで、通信を保護します。 一度ログインすると次回以降はIDとパスワードの入力なしでログインできるため、シングルサインオンを実現するための方式として活用されています。代表的な使用例としてはWindowsのActive Directoryが挙げられ、ユーザー認証に使用されている方式がKerberos認証です。 Kerberos認証は、IDとパスワード情報からチケットを発行し、そのチケットを用いることでその後の認証を不要にする仕組みです。
2	多要素認証	多要素認証は、サインイン プロセスでユーザーに別の形式の ID (携帯電話に示されるコードや指紋スキャンなど) を求めるプロセスです。 ユーザーの認証にパスワードのみを使用する場合、不安な攻撃ベクトルが残ります。 パスワードが脆弱である場合、または他の場所で公開されている場合、攻撃者がパスワードを使用してアクセス権を取得している可能性があります。 2 つ目の認証形式を義務付ければ、その二次的な要素は攻撃者が容易に取得したり複製したりできるようなものではないため、セキュリティが向上します。
3	AD FS（Active Directory Federation Services）	ADFS（Active Directory Federation Services）は、Active Directoryの機能の一つで、オンプレミスのActive Directoryにサインインした利用者がクラウドサービスにアクセスできるようにする認証システムです。事前に外部のクラウドサービスなどに利用者登録し、デジタル証明書などの設定を行なうことで実現します。ADFSを利用すれば、所属組織のActive Directoryに利用者がログインを一度行なうだけで利用者が識別され、複数のサービスが利用可能になります

1.2. 用語集

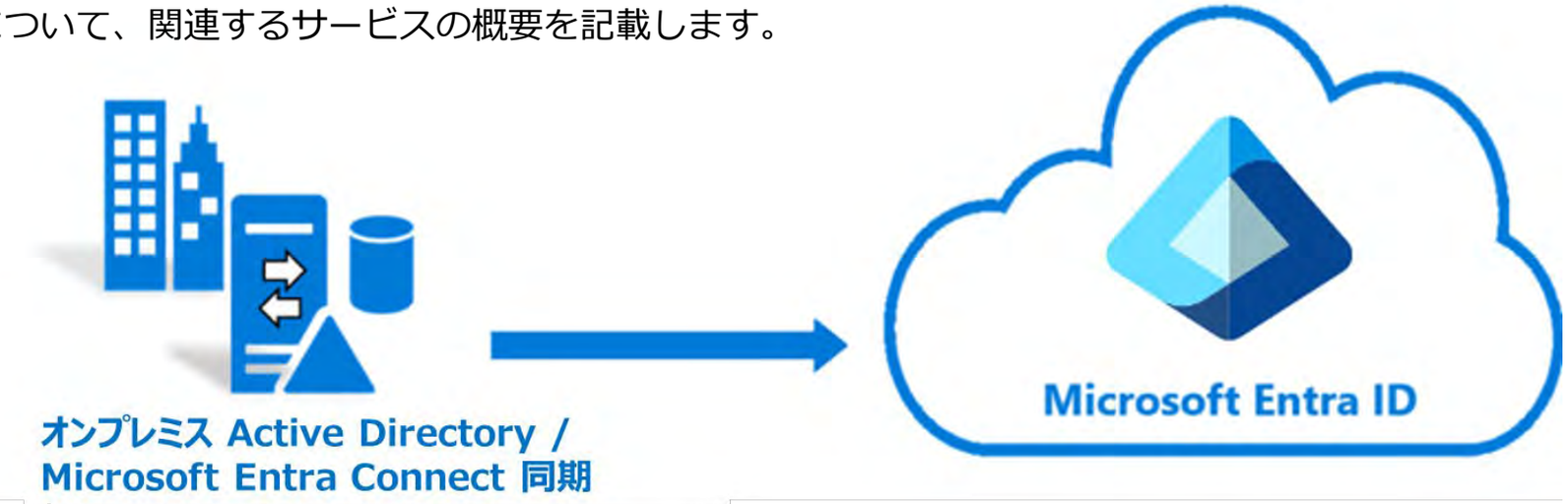
本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
4	パスワードライトバック	Microsoft Entra IDでユーザーのパスワードを変更した際、その変更をオンプレミスのActive Directory（AD）に書き戻す（反映させる）ための機能です。これは、クラウドとオンプレミスの間でパスワードの一貫性を保つために重要な役割を果たします。 パスワードライトバックを有効化するためには、Entra ConnectがオンプレミスADにアクセスできる権限を持っていることや、Entra ID P1 または P2 ライセンスが必要となります。

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（AD）
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 AD 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. Microsoft Entra Connect 同期について

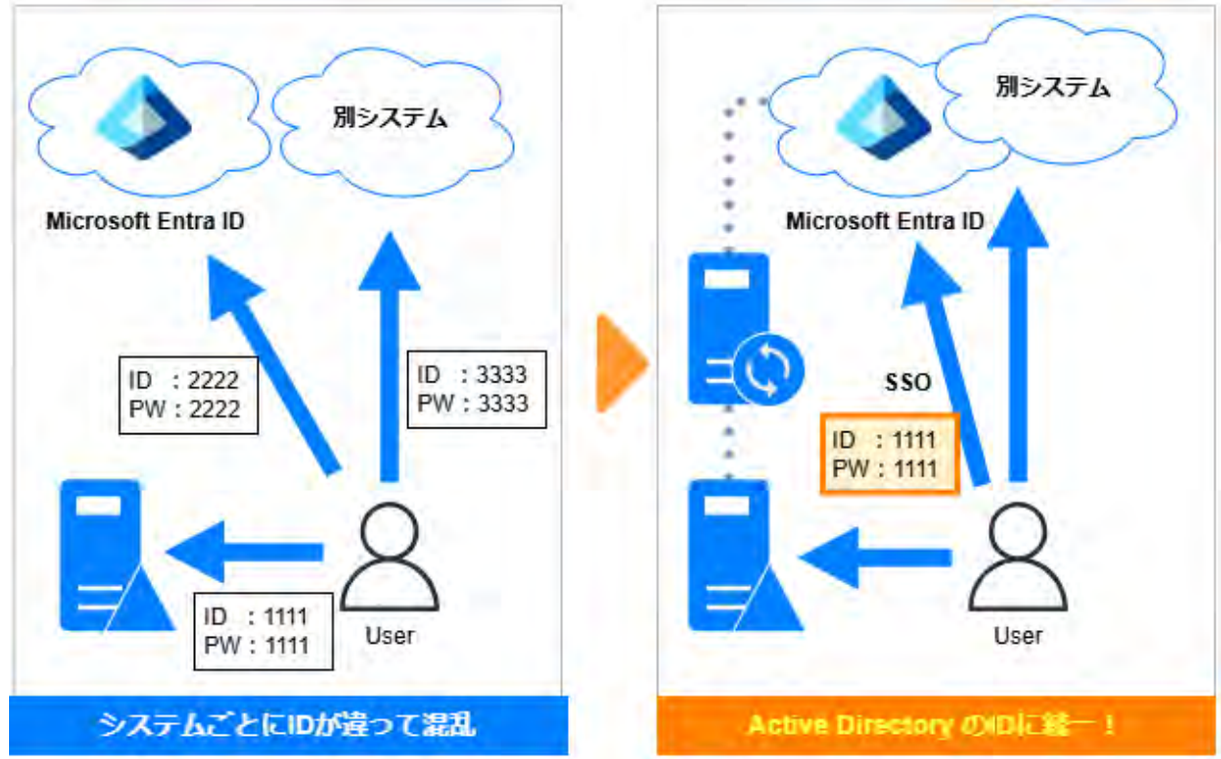
■Microsoft Entra Connect 同期について

ハイブリッド環境とは、オンプレミスとクラウドを連携させて動作する環境 のことを指します。
ハイブリッド環境を構築すると、オンプレのActive DirectoryとクラウドのEntra IDを統合し、
ユーザー管理や認証をスムーズに行えるようになります。

Microsoft Entra ConnectはAD等のオンプレミス環境と
クラウド環境のハイブリッド環境を実現するためのツールとなります。
オンプレAD上のユーザー、デバイスなどの情報を
Microsoft Entra ID に同期する際に使用します。

Active Directoryに保存されたユーザー情報などの
オブジェクトをMicrosoft Entra IDに同期することで
一元的なユーザー管理を実現し、
既存のADのIDとパスワードを継続して利用することができます。

また、シングルサインオン（SSO）機能により、
ユーザーは一度のログインで複数のクラウドサービスに
アクセス可能です。



2.3. ハイブリッド環境でない場合の認証方法について

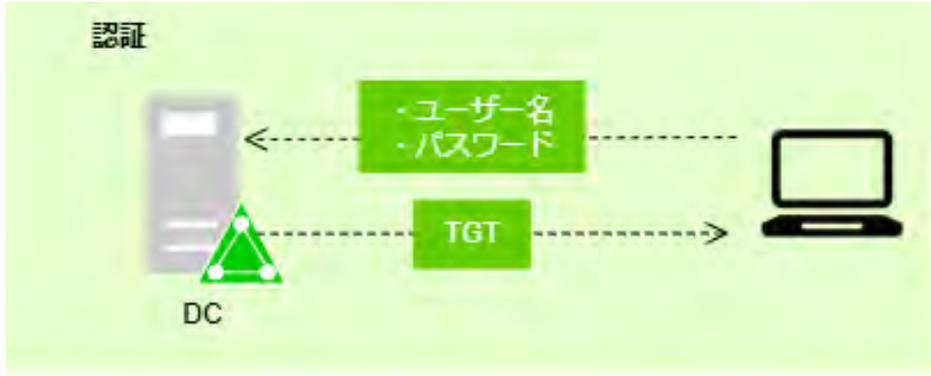
＜補足＞

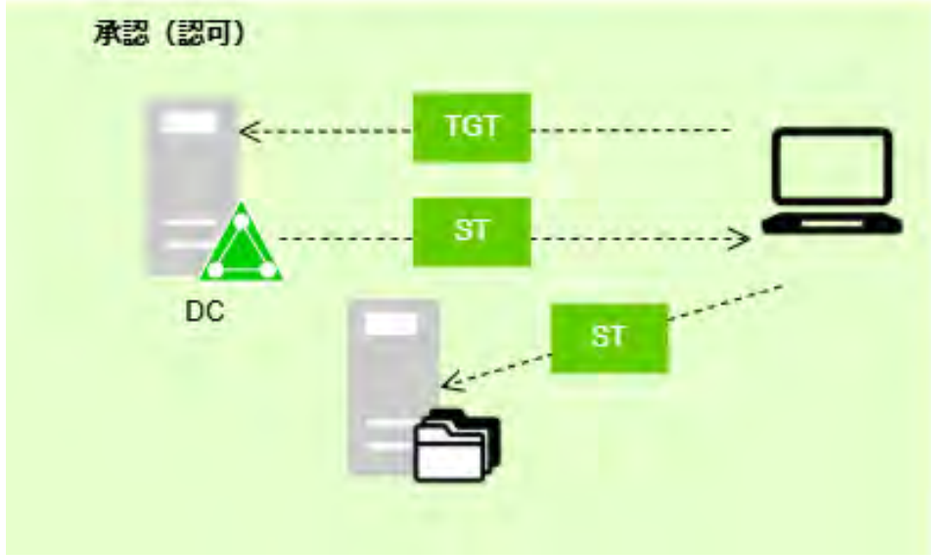
ハイブリッド環境でない場合の
現状のオンプレADと EntraIDのそれぞれの認証・認可方法の方法に
ついて説明します

■オンプレミスAD の 認証・認可方法

オンプレADでは、一般的にID・パスワードで認証を行います。
ユーザーが入力したID・パスワードはドメインコントローラー（DC）に
送られ、内容が正しければ**Kerberos認証**により
Kerberos Ticket Granting Ticket（TGT）が発行されます。

次に、取得したTGTをドメインコントローラーに提示することで、
業務システムなどの対象リソースにアクセス可能か問合せを行います。
アクセスが可能であれば、Service Ticket（ST）が発行され、
これによりリソースへのアクセスが認可されます。





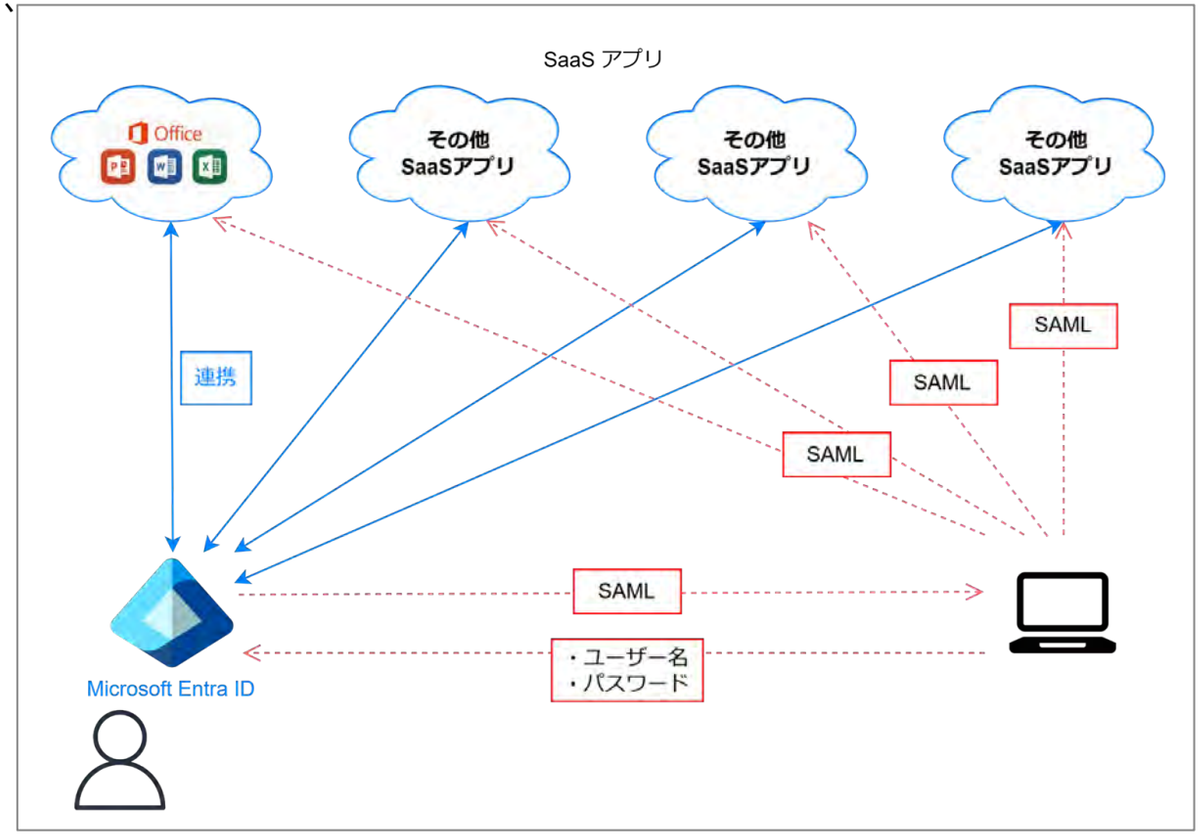
2.3. ハイブリッド環境でない場合の認証方法について

■Microsoft Entra IDの認証・認可方法

Microsoft Entra IDも同様に組織アカウントの認証・認可を実現しますが、
その実現方式や対応範囲はオンプレADと異なります。

Microsoft Entra IDはクラウド上で提供されるため、
場所を問わず認証が可能です。Microsoft Entra IDでは
ID・パスワードに加え、SMSや端末所持などの多要素認証や、
場所・デバイス状態などにより認証可否を判断する
条件付きアクセスなどの機能を利用できます。
これにより、セキュリティ強度を向上できます。

Microsoft Entra IDはSAML等の認証方式にも対応しており、
Microsoft製品以外のクラウドサービスの認可も可能です。
Microsoft Entra IDでは、SalesforceやAWS、Google Workspace
など、数千のクラウドサービスに対応しています。



3. Microsoft Entra Connect 認証方式について

3. Microsoft Entra Connect 認証方式について

■Microsoft Entra Connect　認証方式について

前のページにて説明した通り、Microsoft Entra Connectは、オンプレミスのAD と Entra IDを同期するためのツールです。
このツールを使って、ADのユーザーアカウントやパスワード情報をEntra IDと連携します。
オンプレミスのADに登録されているユーザーが、Entra IDを利用する際の認証を行うための機能として、ユーザーの認証方法が以下の3つあります。

パスワードハッシュ同期

パススルー認証

フェデレーション

本資料では、これらの3つの認証方式の特徴や違いを説明し、最適な認証方式の選定の参考となる情報を提供いたします。
また、実際の設定から同期完了確認方法までの手順についてもご案内いたします。

3.1. パスワードハッシュ同期について

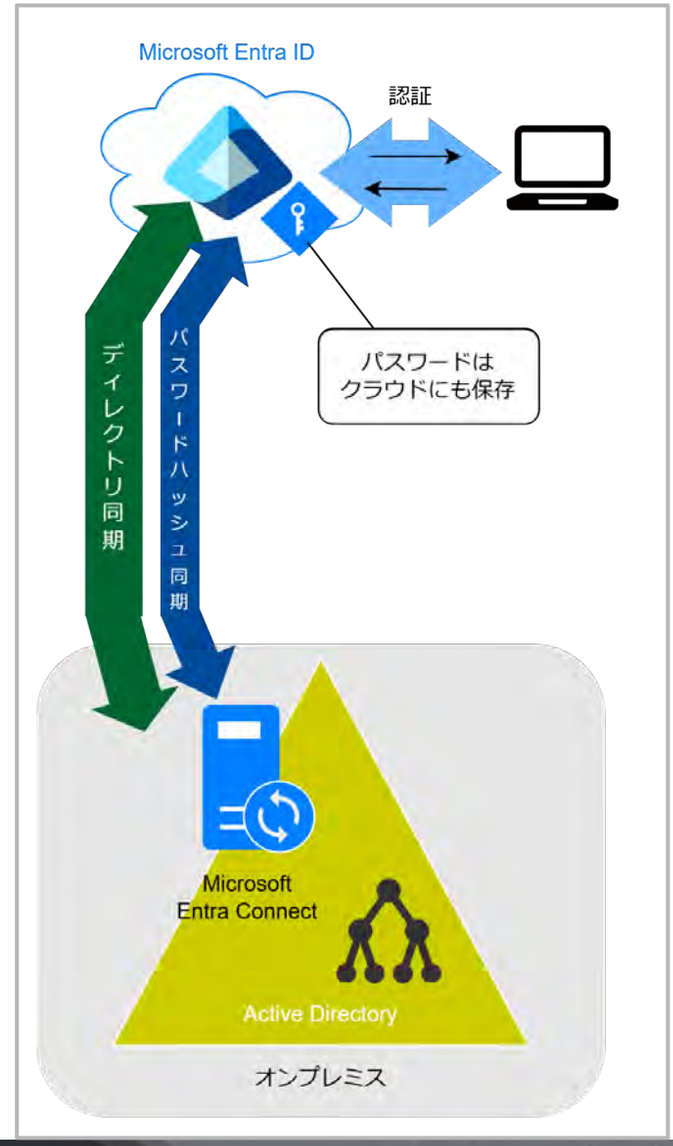
パスワードハッシュ同期

Microsoft Entra Connectを使用したデフォルトの認証方式で、
オンプレミスのAD からEntraDにユーザーのパスワードのハッシュを同期する方式です。

特徴

パスワードのハッシュ化による同期
ユーザーがパスワードを作成すると、そのパスワードはハッシュという暗号化された形式に変換されます。ハッシュは一方向性関数を使用して作成されるため、元のパスワードを簡単に復元できません。

クラウド上での認証
ユーザーがEntra IDにサインインすると、クラウド上で認証が完結します。
（オンプレミスADに問い合わせを行いません）



3.1. パスワードハッシュ同期について

メリット

- **セキュリティ強化**
  漏洩資格情報検出機能が有効になり、セキュリティが強化されます。
  パスワードをクラウド上で直接認証するため、高可用性を実現できます。
- **ユーザーの生産性向上**
  ユーザーはオンプレミスとクラウドで同じパスワードを使用できます。
- **オンプレミス環境がなくても動作**
  認証時にオンプレミスADに接続しないため、ADサーバーがダウンしていてもクラウドで認証可能です。

デメリット

- **同期のタイムラグ**
  パスワードの変更が最低30分程度のタイムラグを伴うことがあります。
- **ADのパスワードポリシーは適用不可**
  ADのアカウントロックアウトポリシーやパスワードポリシーは適用されません

ユースケース

オンプレミスのADとクラウドの認証を統一したい企業や、シンプルなセットアップと管理を求める中小企業に向いています。

3.2. パススルー認証について

パススルー認証

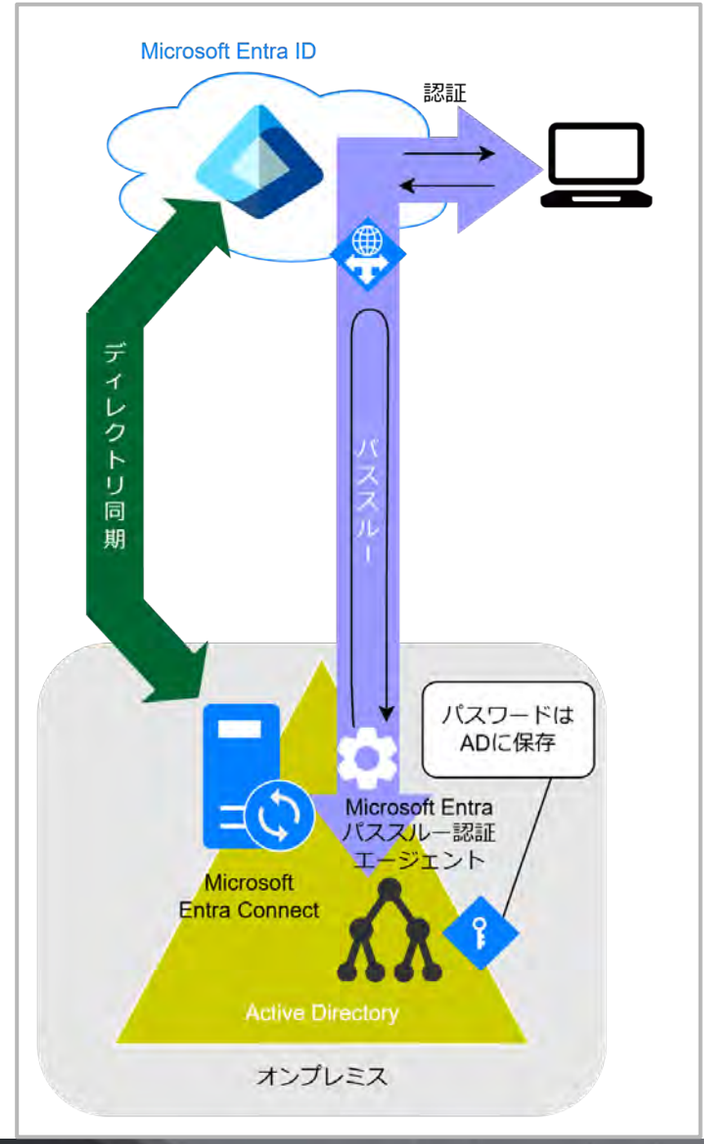
クラウドにサインインの際にEntra ID 経由でAD（オンプレミス）に認証を行う方式です。
ユーザが入力したIDやパスワードなどの認証情報を、そのまま内部の認証システムへ転送（＝パススルー）し、そこで直接認証を実施します。

特徴

オンプレミスADで認証
ユーザーがEntra ID にサインインする際、パスワードをEntraIDに送信せずに、オンプレミスのADで認証を行います。これにより、ユーザーがクラウドとオンプレミス両方で同じパスワードを使い続けることができ、セキュアにログインできるようになります。

パスワードはクラウドに保存されない
パススルー認証はパスワードハッシュ同期と異なり、パスワード情報はMicrosoft Entra IDに同期されず、サインインする際にその都度ActiveDirectoryに対してユーザのパスワードを確認する認証方法になります。パスワードがEntra ID に保存されないため、セキュリティのリスクが少なくなります。

オンプレミス環境が必須
認証エージェントをADサーバー上にインストールし、常に稼働させる必要があります



3.2. パススルー認証について

メリット

・**安全性**
パスワードがクラウドに保存されないので、セキュリティが向上します。

・**ADのポリシーが適用される**
ADのパスワードポリシー、多要素認証（MFA）などを適用できるため、オンプレミスの設定と統一することができます

デメリット

・**オンプレミスＡＤがダウン時にサインイン不可**
オンプレミスのADがダウンしていると認証を行うことができないためサインインすることができなくなります。

・**認証要求のためのNSG/ファイアウォールの設定**
Entra IDからオンプレミスの ADへの認証要求が必要であるため、NSG や ファイアウォール の設定が適切でないと、認証要求が通らない可能性があります。
（例えば、EntraIDと認証エージェント間の通信にはポート443を許可する、等の設定が必要です）

・**高可用性のために冗長化が必要**
認証エージェントがダウンすると認証できなくなるため、複数のサーバーにエージェントをインストールして冗長化することが推奨されます。

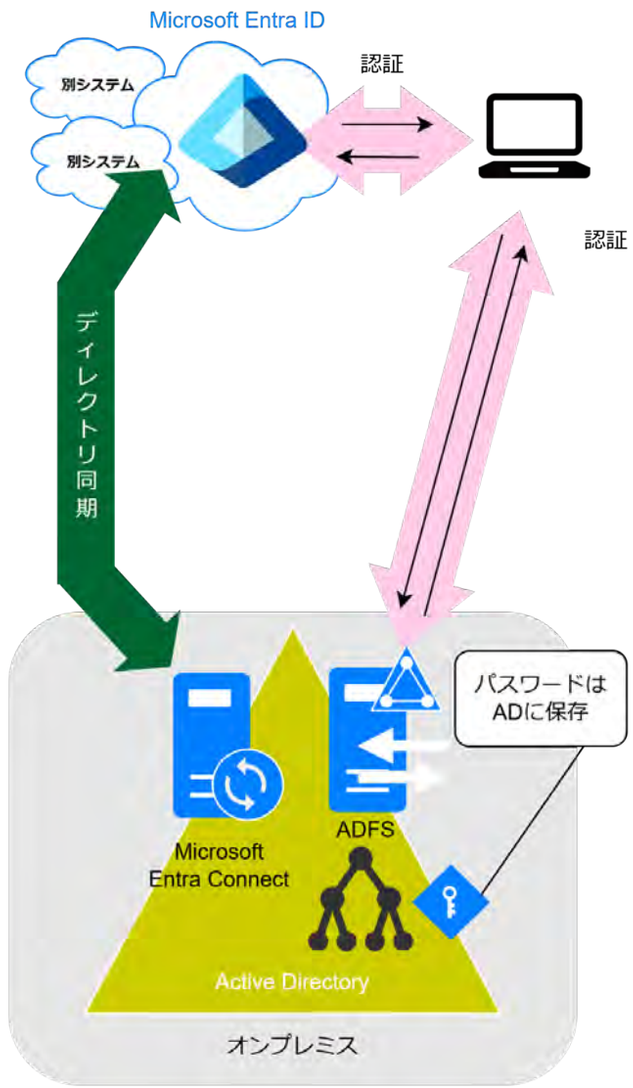
ユースケース

・Entra ID を経由してオンプレミスの AD にて認証が行う方式であり、パスワード情報はオンプレミスのみに保存されるため、クラウドにパスワードを配置したくない場合に向いています。
・オンプレミスのパスワード要件が適用されますので、オンプレミスのADに組織独自のセキュリティポリシーがある場合にも向いているため、高いセキュリティとオンプレミスのパスワードポリシーを維持したい企業に向いています。

3.3. フェデレーションについて

フェデレーション

ユーザーのサインイン要求を、オンプレミスのADFS（Active Directory Federation Services）などのアイデンティティプロバイダー（IdP） に転送し、そこで認証する方式です。
ADFSがユーザーの認証に成功すると、セキュリティトークン（SAMLトークンなど）が発行され、
クラウドサービスはセキュリティトークンを受け取り、ユーザーに対するアクセスを承認します。



特徴

オンプレミスADのユーザー名/パスワードをクラウドサービスでも利用可
この仕組みを使うと、会社のネットワークで使っているユーザー名やパスワードを、クラウドサービスにそのまま使えるようになります。これにより、都度様々なサイトにログインする必要がなくなり、1つのIDだけで様々なサービスを使うことができます。（SSO）

オンプレミスADにパスワードが保存される
具体的には、Microsoft Entra IDにログインするときに、会社のADにある認証情報を使ってログインできるようになります。つまり、Microsoft Entra IDが直接ユーザーを認証するのではなく、会社のサーバーであるADFSなどで認証が行われます。

トークンの発行
例えば、Microsoftにログインする場合、Microsoft Entra IDからADFSに確認を行い、認証されればADFSがトークンを発行します。ユーザーからMicrosoftへトークンを渡し、許可されるとログインが可能となります。

3.3. フェデレーションについて

メリット

- **1つのアカウントで複数のサービスにログインできる**
  Active Directoryのアカウントで
  Microsoftのサービスや他のサービスにもログインできます。
- **シングルサインオン（SSO）で便利**
  1回ログインすれば、他の関連サービスにも自動的にログインできます。
- **セキュリティが高い**
  オンプレミスのサーバー（自社のサーバー）にだけ保存されて
  クラウドには保存されないため、盗まれるリスクが少ないです。
- **パスワードの管理が楽になる**
  パスワードは会社のサーバーで一元管理できるため、
  各サービスのパスワードを覚える必要はありません。

デメリット

- **設定が難しい**
  オンプレミスのADとMicrosoft Entra IDをつなげる設定は、
  少し複雑で専門的な知識が必要です。
- **トラブルシューティングが難しい**
  オンプレミスのADとMicrosoft Entra IDをつなげているため、
  問題が発生した場合に調べるのが複雑になることがあります。
- **ADサーバーに依存する**
  会社のADサーバーがダウンすると
  Microsoft Entra IDやクラウドサービスにも影響が出る可能性があります。

ユースケース

フェデレーション認証は、主に大規模な企業や、複雑なITシステムを持つ企業が使うことが多いです。オンプレミスのADとMicrosoft Entra IDをつなげることで、一貫したユーザー管理ができ、セキュリティが強化され、シングルサインオン（SSO）を実現できます。これにより、企業の規模が大きかったり、セキュリティを重視していたりする場合に特に役立つ認証方式です。

3.4. 認証方式の比較

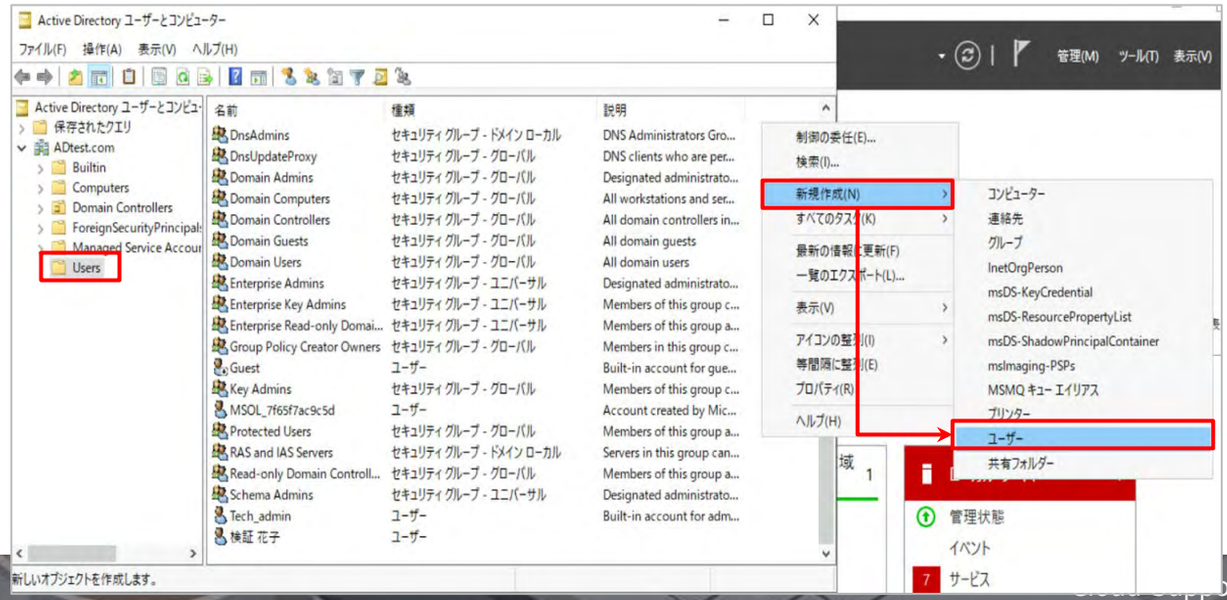
各認証方式の特徴の比較は以下となります

項目	パスワードハッシュ同期	パススルー認証	フェデレーション
認証の流れ	Entra IDが直接認証	Entra ID ⇒ 認証エージェント ⇒ AD	Entra ID ⇒ AD FS ⇒AD
パスワードの保存場所	Entra IDにハッシュを保存	ADに保存	ADに保存
クラウド上でパスワード変更した際のAD側への反映	✕ 反映されない （ライトバック機能で実現可）	✕ 反映されない （ライトバック機能で実現可）	✕ 反映されない （ライトバック機能で実現可）
ADと同じパスワードでのサインイン	○ 可能	○ 可能	○ 可能
ADのパスワードポリシー適用	✕ 適用されない	○ 可能	○ 可能
ADがダウンした際のサインイン可否	○ サインイン可能	✕ サインイン不可	✕ サインイン不可
運用のシンプルさ	○ シンプル	▲認証エージェントの管理が必要	✕ 複雑（サーバー・証明書管理が必要）
認証速度	○ クラウドで完結し高速	ADへの問い合わせが発生	▲AD FSの負荷による
追加認証要素（MFA等）	✕ Entra IDのMFAのみ	○ ADの認証ポリシーを適用可能	○ AD FSでカスタム認証可能
シングルサインオン（SSO）	▲可能（社内NW内のみ）	▲ 可能（社内NW内のみ）	○ 可能

4. 設定手順

4.1. ユーザー作成

共通作業



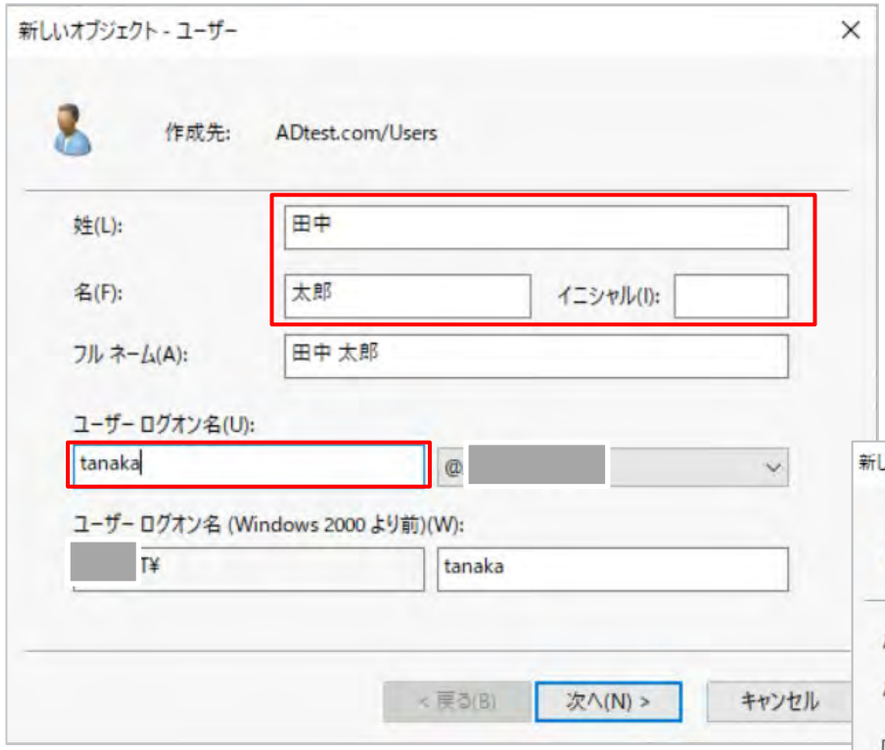
※前提として、AD上にユーザーを作成します
（3つの認証方式共通手順となります）

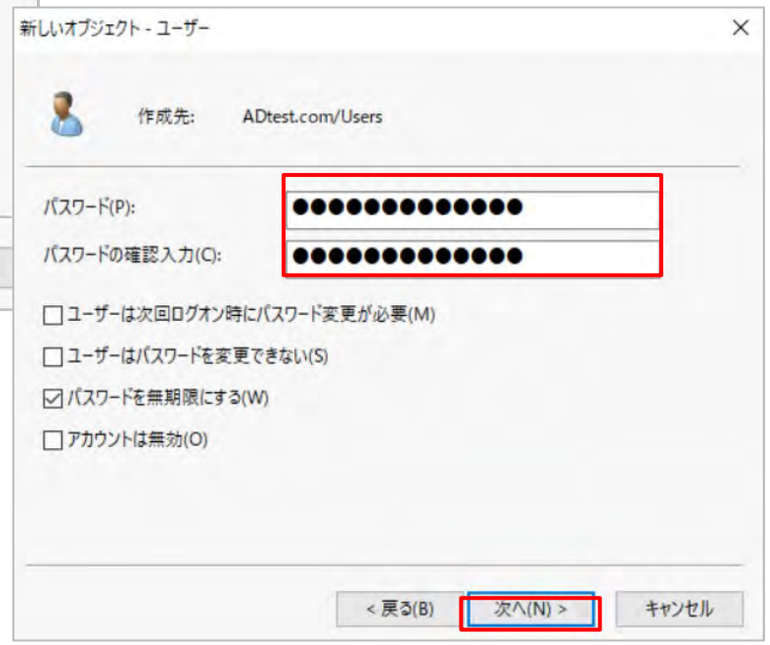
【Active Directory の設定】

1. サーバーマネージャーから、 「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

2. 左ペインから [Users] をクリックし、画面を右クリック＞「新規作成」 ＞ 「ユーザー」　をクリックします

4.1. ユーザー作成



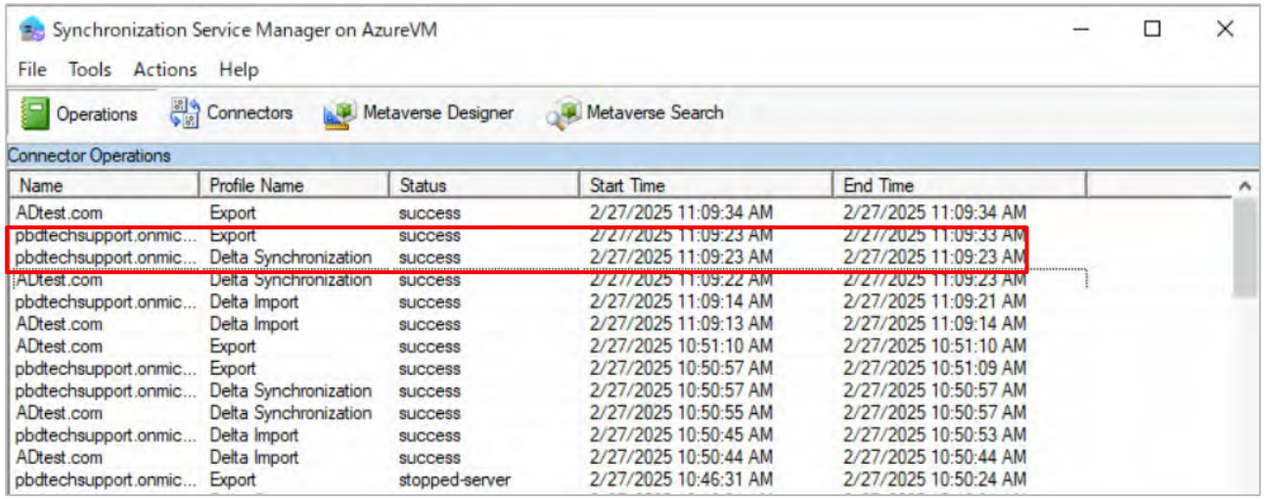


3. 「姓」、「名」、「ユーザーログオン名」を入力し「次へ」をクリックします

4. [パスワード] を入力し、「次へ」をクリックし登録を完了させます。

4.2. 同期ステータスの確認

■Synchronization Service Manager



Name	Profile Name	Status	Start Time	End Time
ADtest.com	Export	success	2/27/2025 11:09:34 AM	2/27/2025 11:09:34 AM
pbdtechsupport.onmic...	Export	success	2/27/2025 11:09:23 AM	2/27/2025 11:09:33 AM
pbdtechsupport.onmic...	Delta Synchronization	success	2/27/2025 11:09:23 AM	2/27/2025 11:09:23 AM
ADtest.com	Delta Synchronization	success	2/27/2025 11:09:22 AM	2/27/2025 11:09:23 AM
pbdtechsupport.onmic...	Delta Import	success	2/27/2025 11:09:14 AM	2/27/2025 11:09:21 AM
ADtest.com	Delta Import	success	2/27/2025 11:09:13 AM	2/27/2025 11:09:14 AM
ADtest.com	Export	success	2/27/2025 10:51:10 AM	2/27/2025 10:51:10 AM
pbdtechsupport.onmic...	Export	success	2/27/2025 10:50:57 AM	2/27/2025 10:51:09 AM
pbdtechsupport.onmic...	Delta Synchronization	success	2/27/2025 10:50:57 AM	2/27/2025 10:50:57 AM
ADtest.com	Delta Synchronization	success	2/27/2025 10:50:55 AM	2/27/2025 10:50:57 AM
pbdtechsupport.onmic...	Delta Import	success	2/27/2025 10:50:45 AM	2/27/2025 10:50:53 AM
ADtest.com	Delta Import	success	2/27/2025 10:50:44 AM	2/27/2025 10:50:44 AM
pbdtechsupport.onmic...	Export	stopped-server	2/27/2025 10:46:31 AM	2/27/2025 10:50:24 AM

■Microsoft Entra 管理センター

【同期ステータスの確認】
作成したユーザー情報がEntraIDに同期されたかを確認します

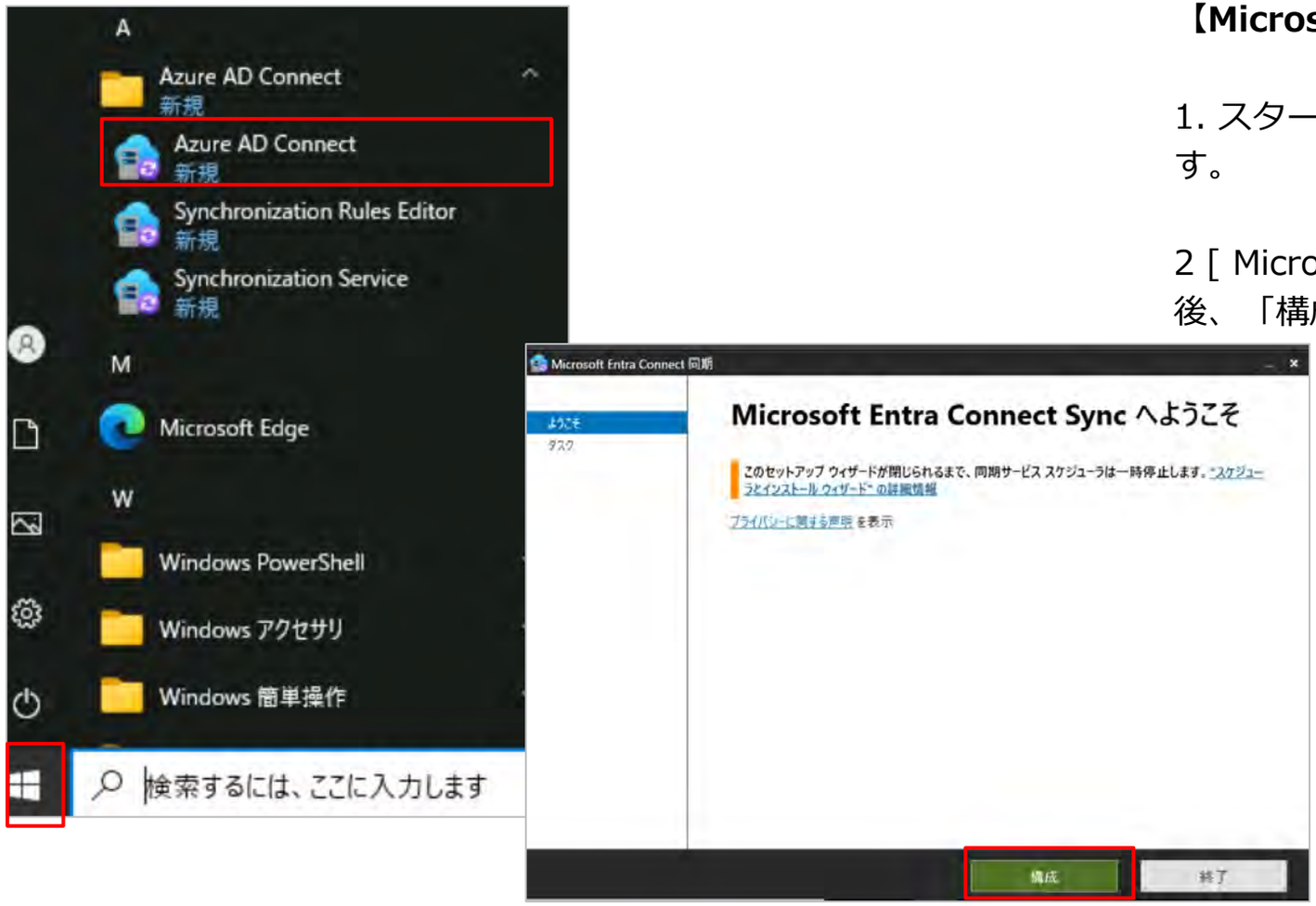
1. 自動的に実行されるまで待つか、同期を手動で実行します。
※通常の同期間隔は30分です。
　PowerShellでコマンドを実行することで、即時同期も可能です。

2．Synchronization Service Managerから同期ステータスを確認します。同期が成功した場合、「Success」と表示されます。

3. Microsoft Entra 管理センター にアクセスし、作成したユーザーが作成されていることを確認します。

4.3. パスワードハッシュ同期 設定

4.3. パスワードハッシュ同期 設定

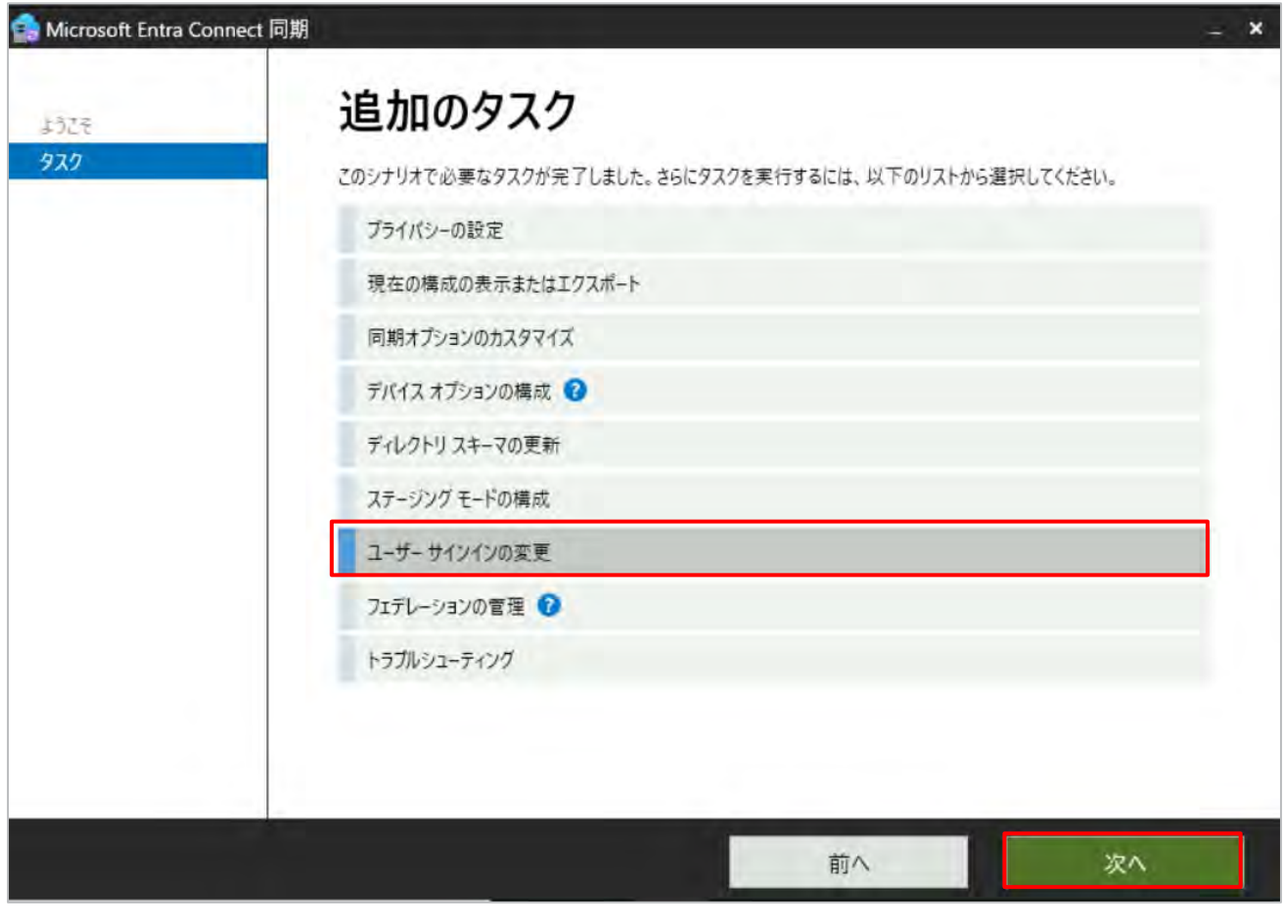


【Microsoft Entra Connect での設定】

1. スタートボタンから [Azure AD Connect] をクリックします。

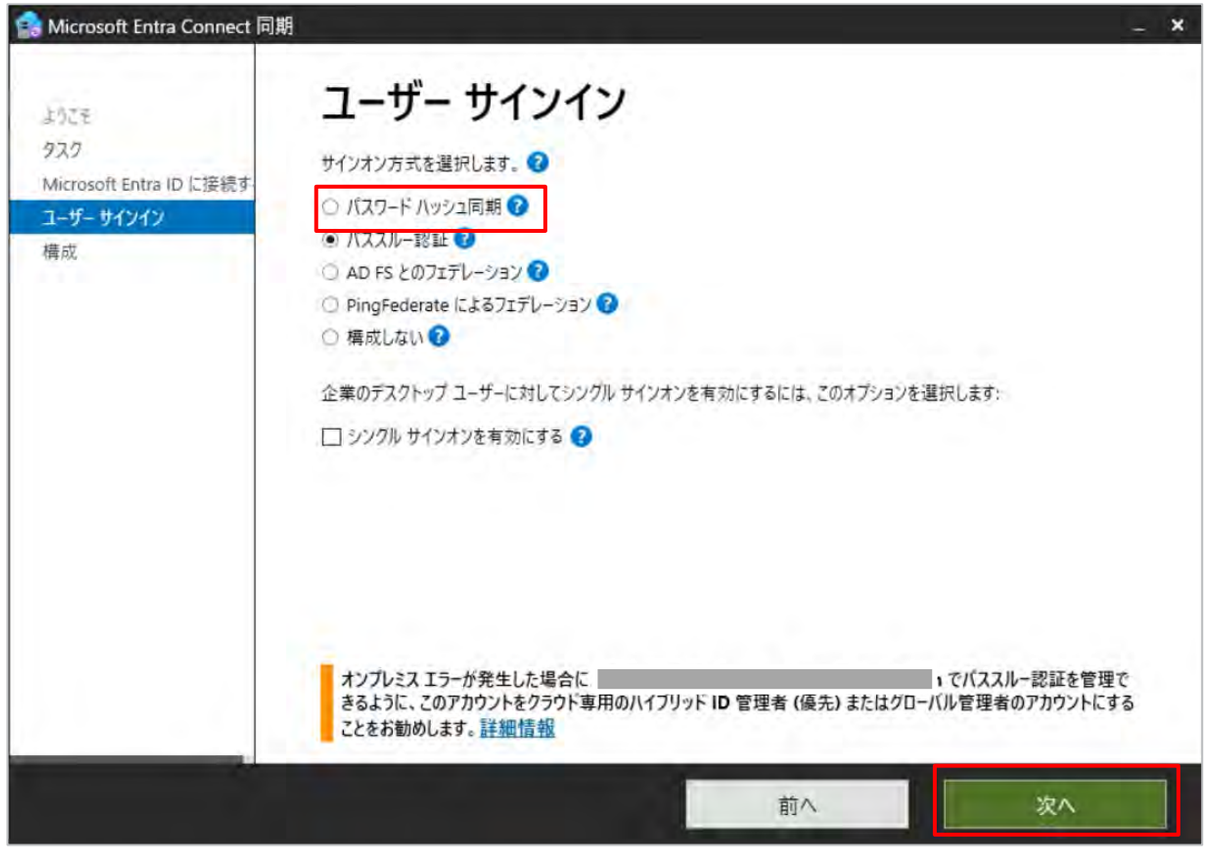
2 [Microsoft　Entra Connectへようこそ]という表示された後、「構成」をクリックします。

4.3. パスワードハッシュ同期 設定



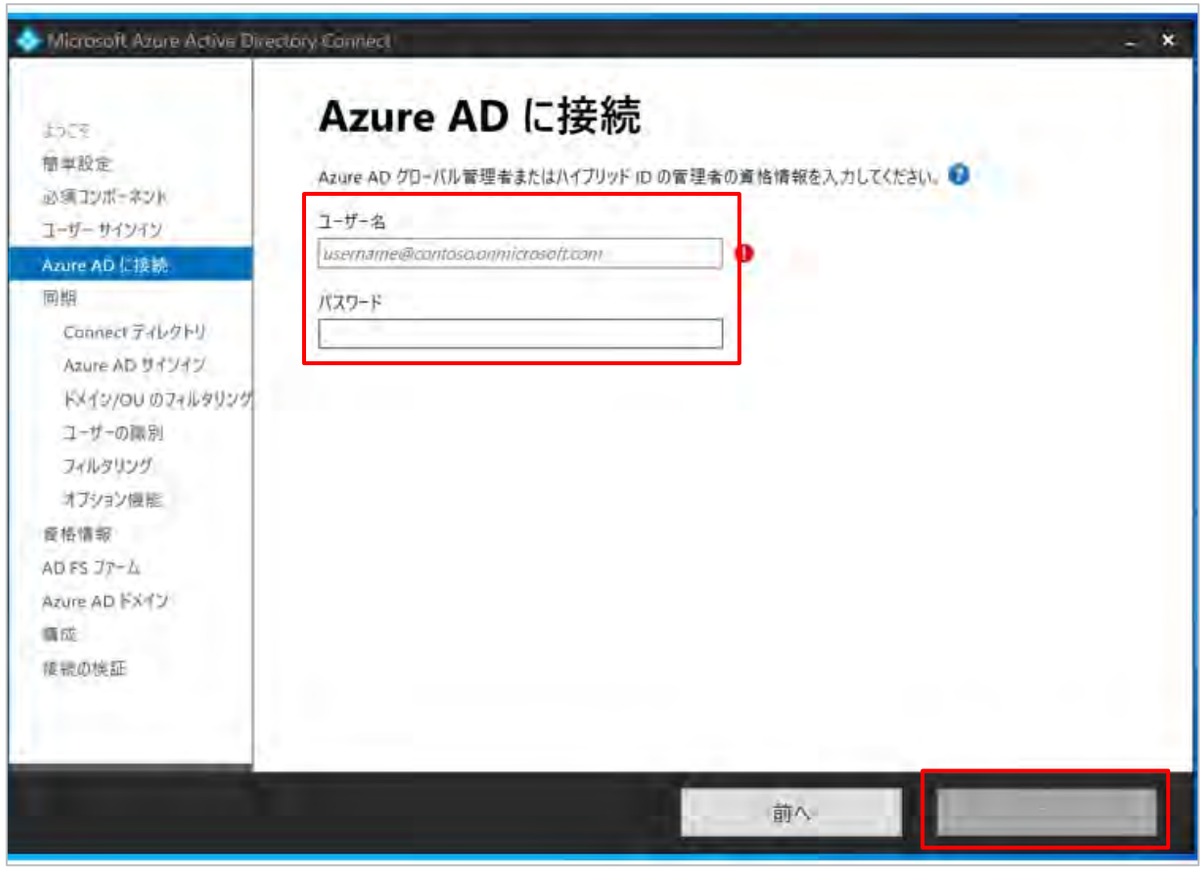
3. 「タスク」 > 「ユーザーサインインの変更」をクリックし「次へ」をクリックします。

4.3. パスワードハッシュ同期 設定



4. 「パスワードハッシュ同期」を選択し、「次へ」をクリックします。

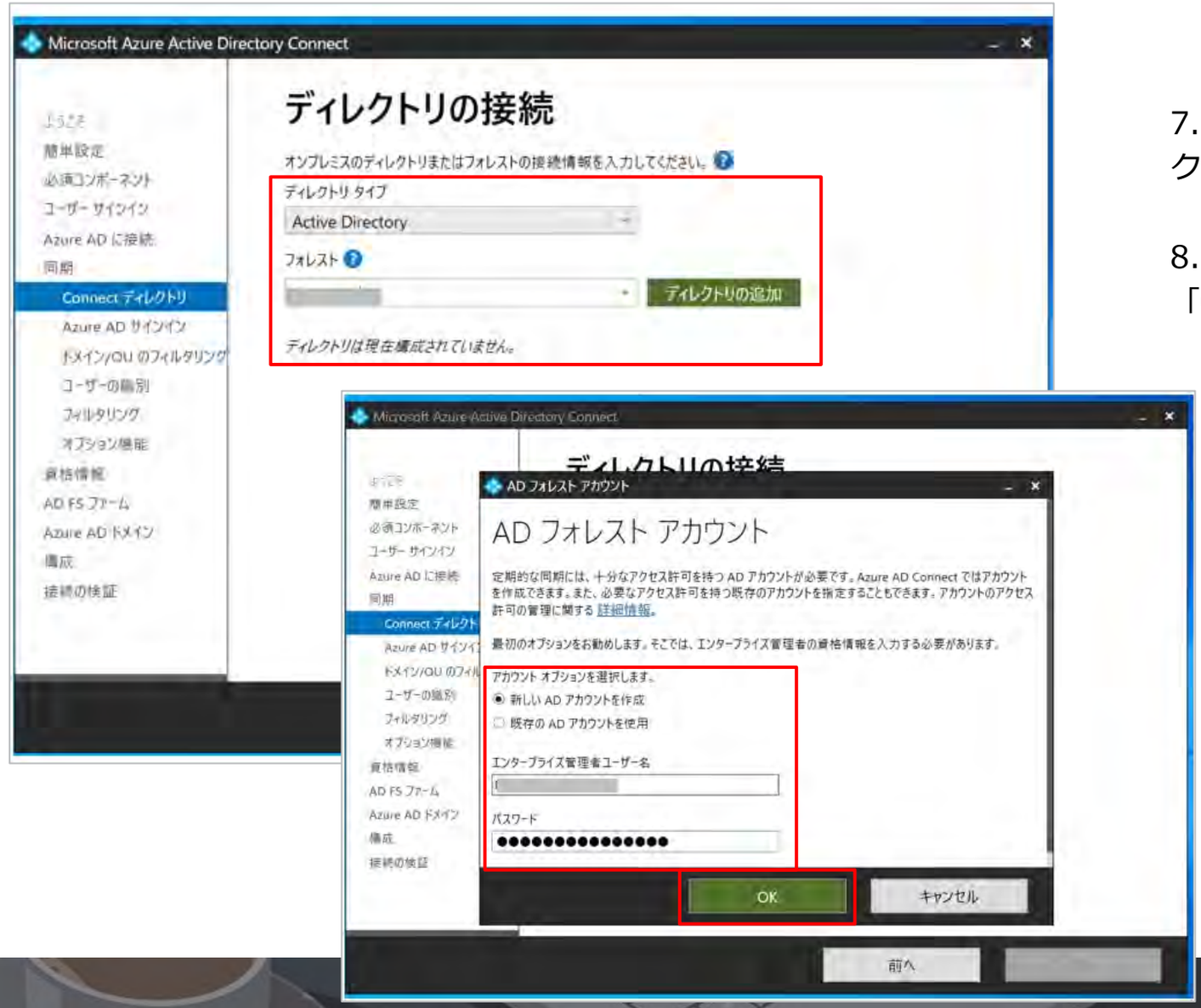
4.3. パスワードハッシュ同期 設定



5. Entra IDのユーザ情報を入力し、「次へ」をクリックします。必要なロールは、グローバル管理者またはハイブリッドIDの管理者です。

6. ポップアップで、「アカウントにサインイン」が出てきますので、必要情報を入力します。

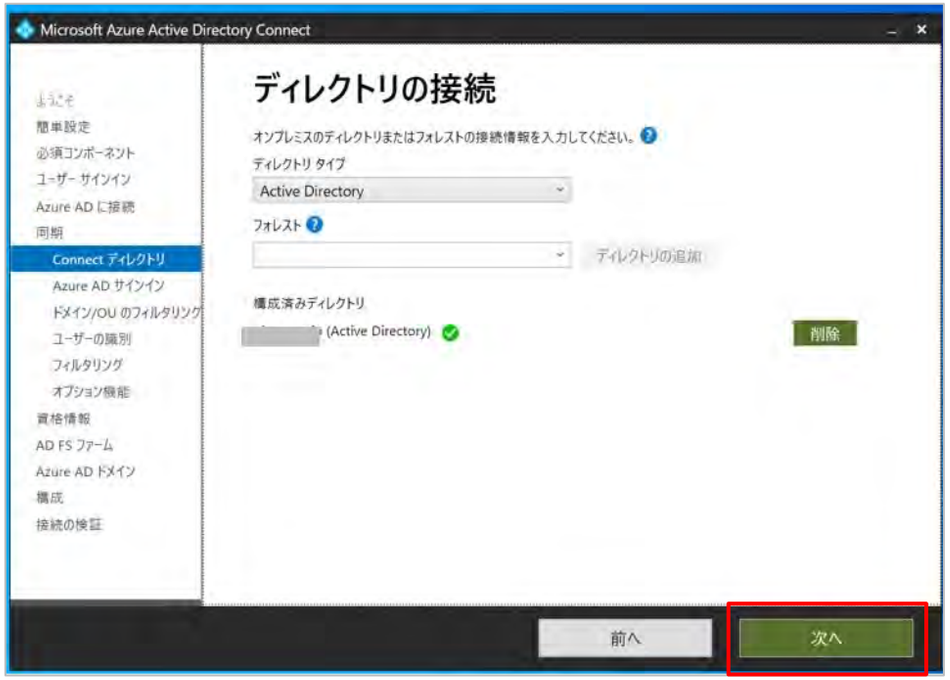
4.3. パスワードハッシュ同期 設定



7. 対象となるドメイン名をフォレストの欄に入力し、「ディレクトリの追加」をクリックします。

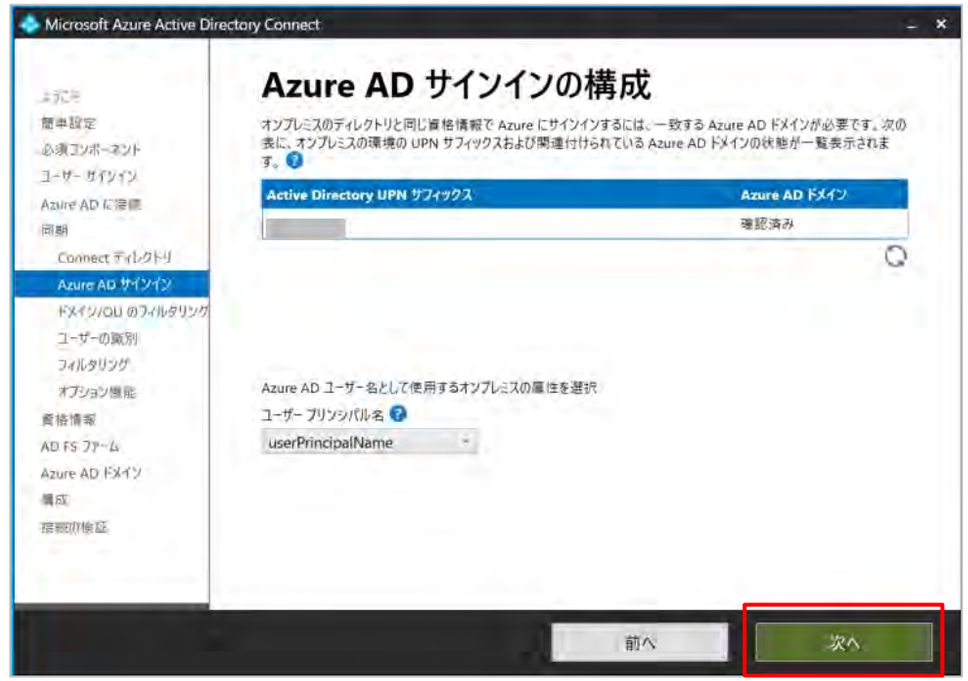
8. Enterprise Adminの権限を有したアカウント情報を入力し、「OK」をクリックします。

4.3. パスワードハッシュ同期 設定

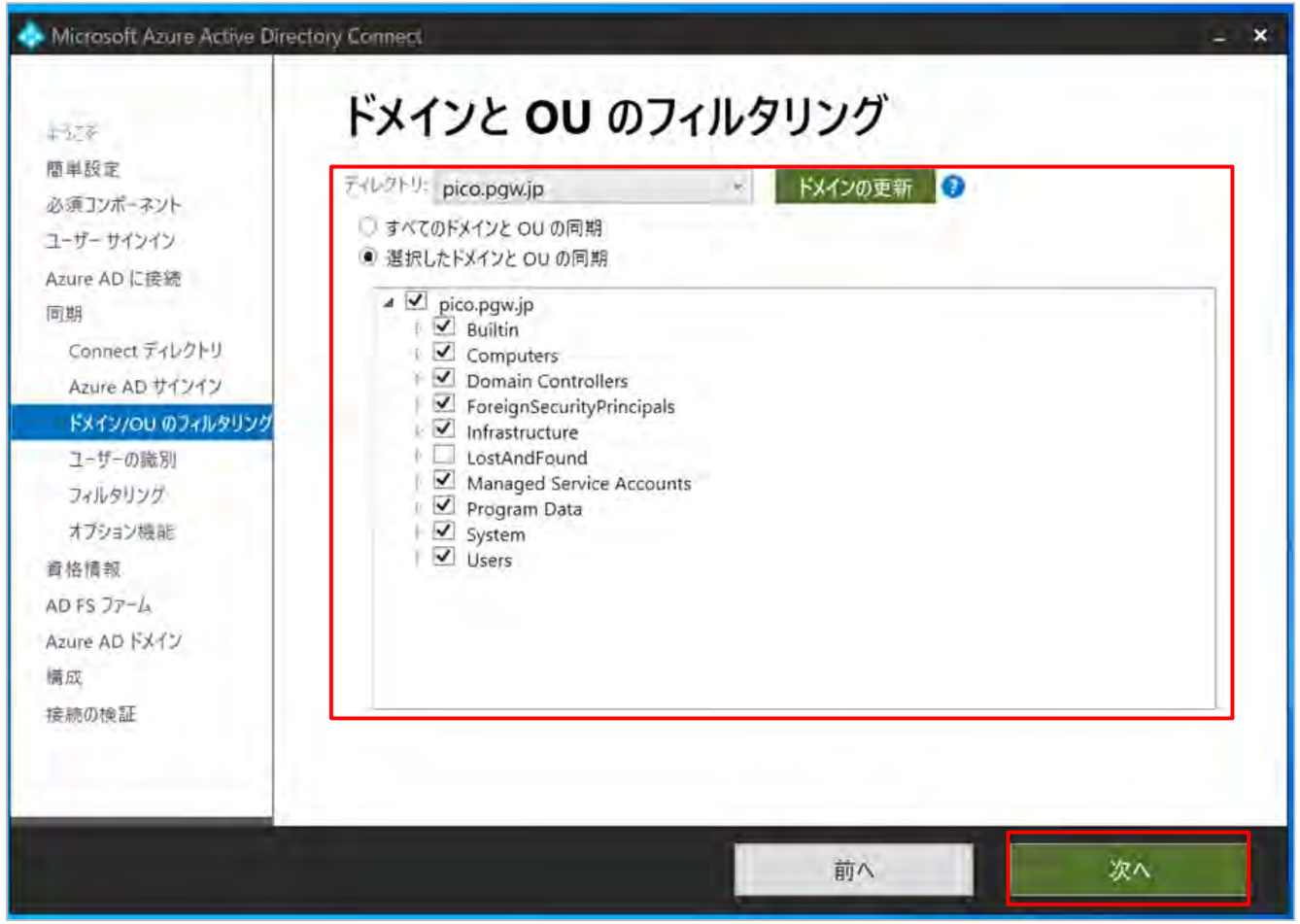


9. 構成済みディレクトリが追加されたことを確認して、「次へ」をクリックします。

10. そのまま「次へ」をクリックします。

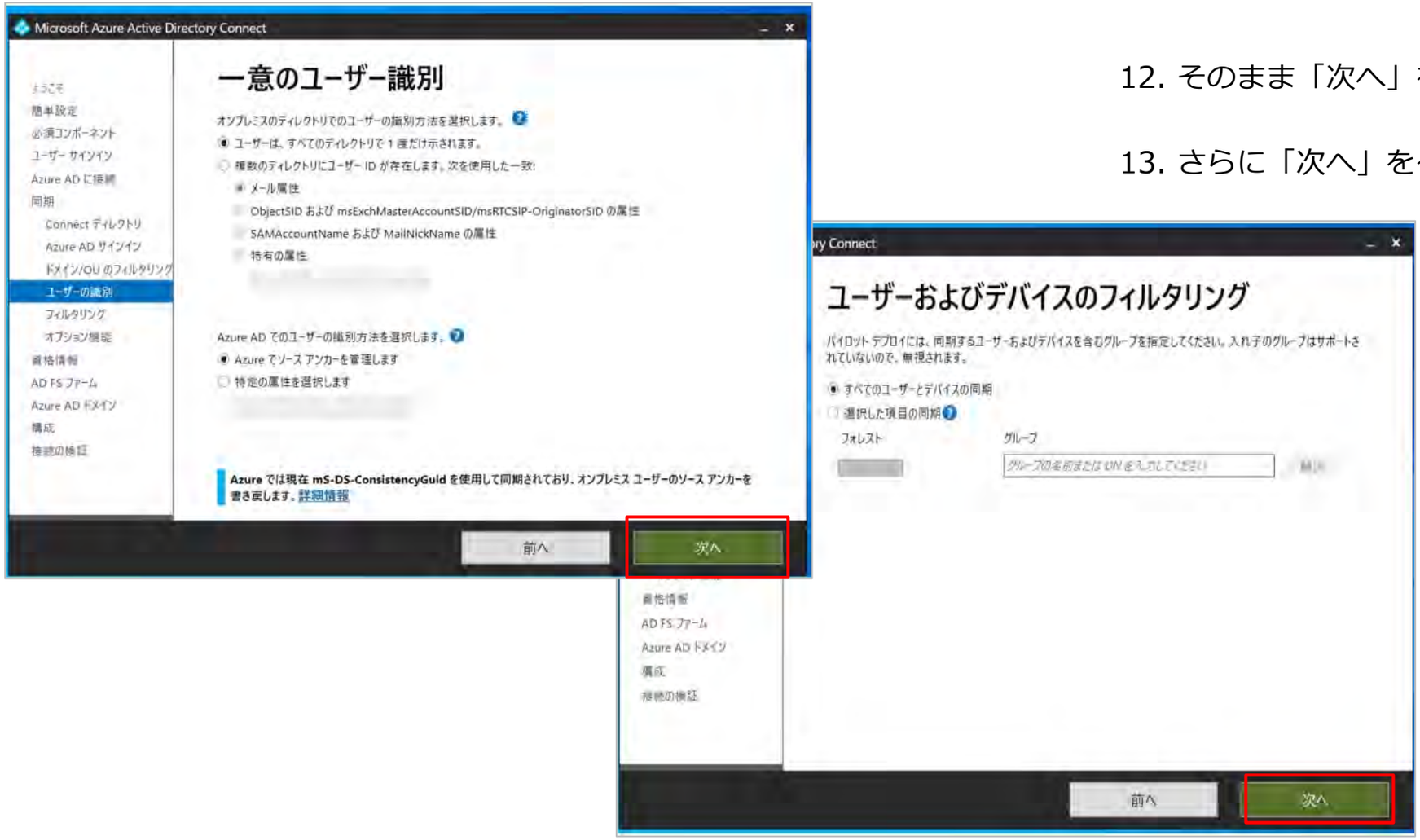


4.3. パスワードハッシュ同期 設定



11. ADから Microsoft Entra IDに同期させる対象となるドメインとOUを指定し、「次へ」をクリックします。

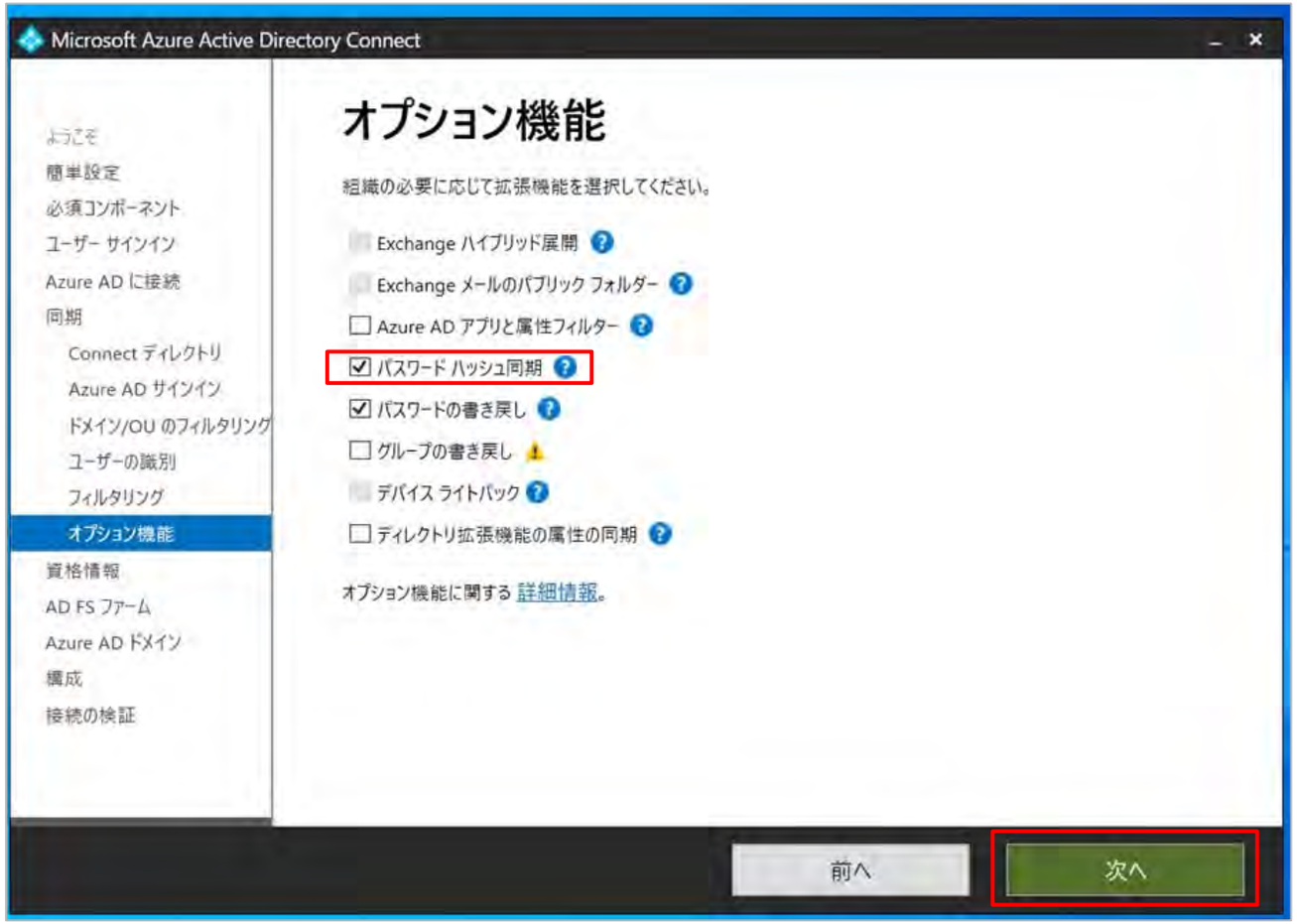
4.3. パスワードハッシュ同期 設定



12. そのまま「次へ」をクリックします。

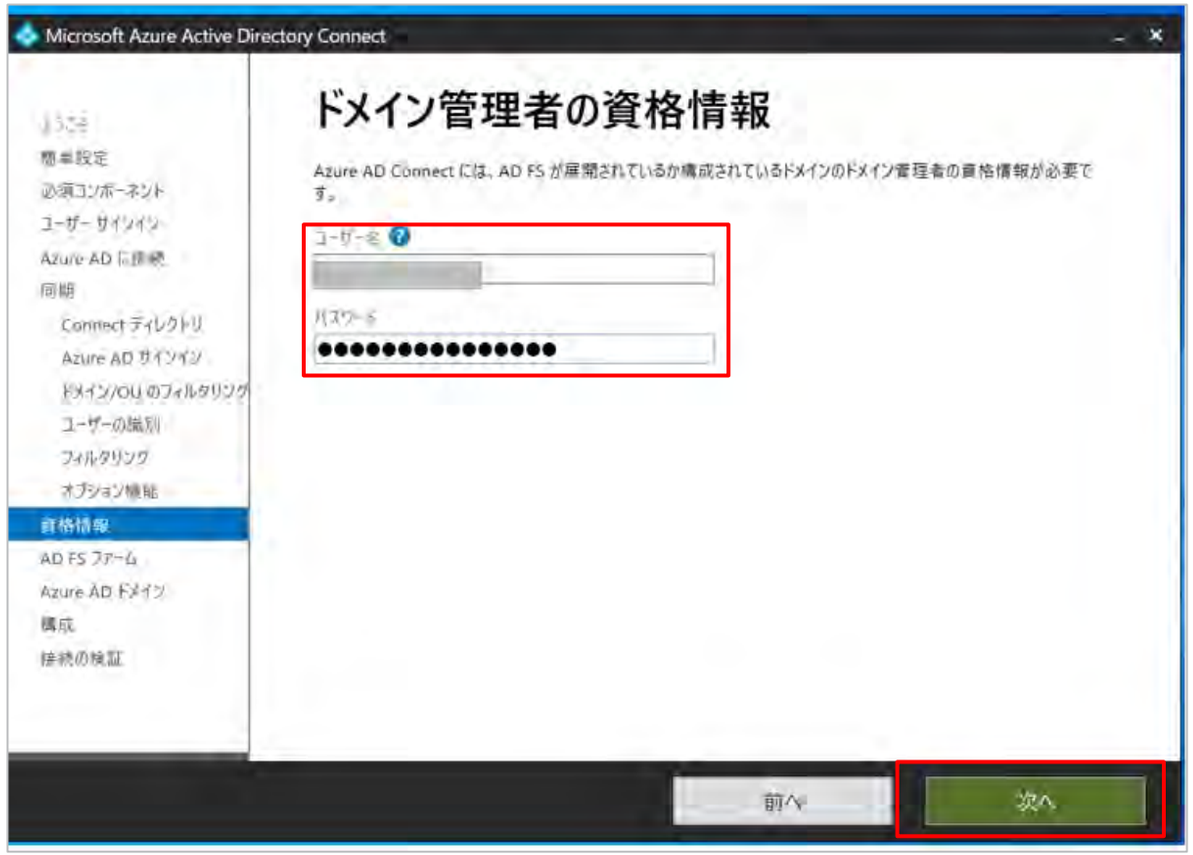
13. さらに「次へ」をクリックします。

4.3. パスワードハッシュ同期 設定



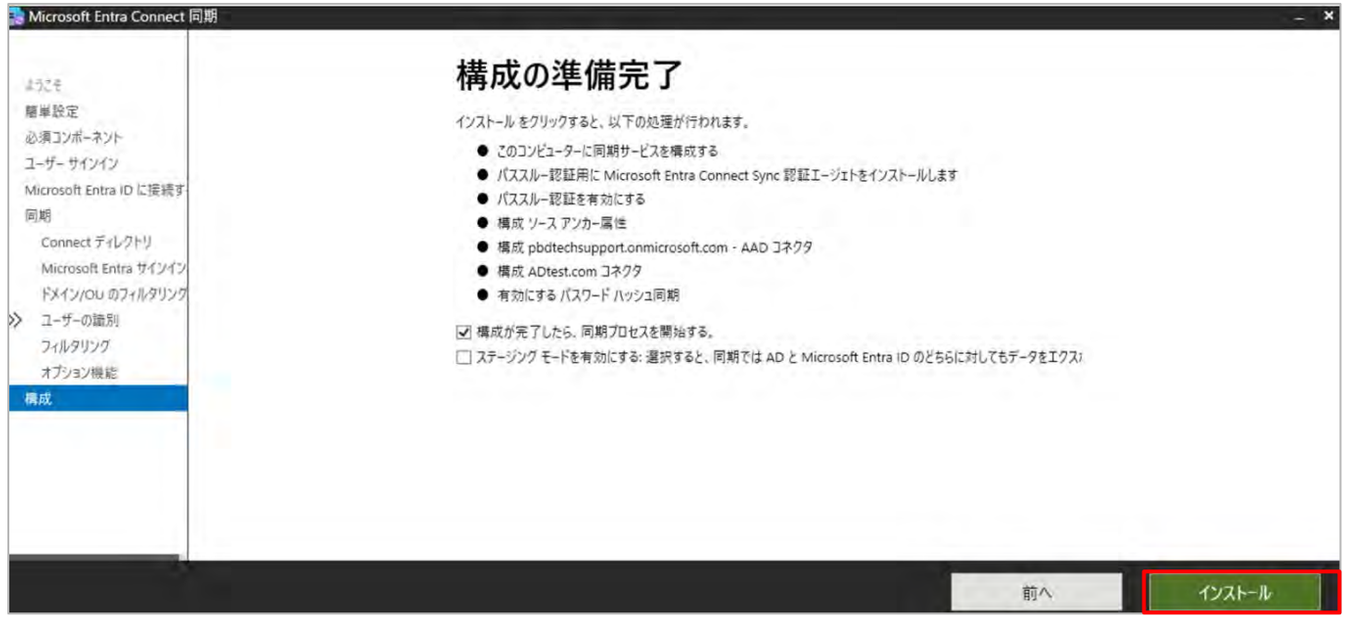
14. 「パスワードハッシュ同期」にチェックが入っていることを確認し、「次へ」をクリックします。

4.3. パスワードハッシュ同期 設定



15. ドメイン管理者の資格情報を入力し、「次へ」をクリックします。

4.3. パスワードハッシュ同期 設定

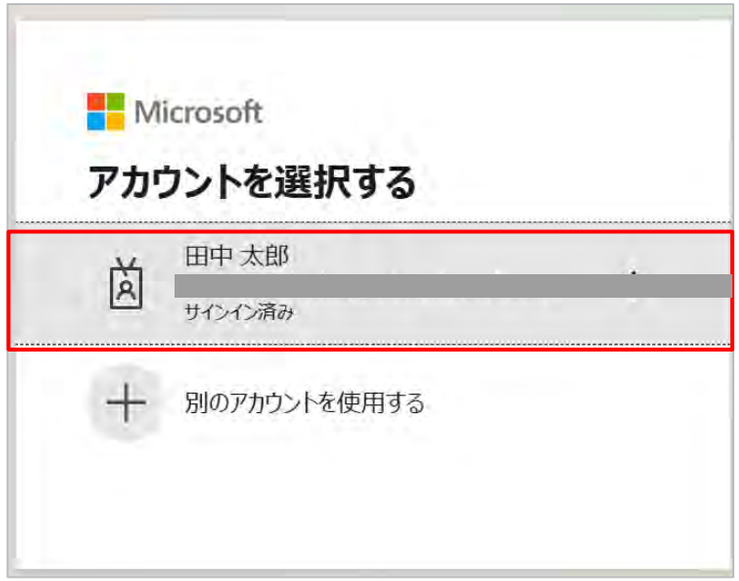


16. 構成の準備完了画面が表示されるので、画面に表示されている内容で問題がなければ「インストール」をクリックします。

4.3. パスワードハッシュ同期 設定

17. しばらくすると「構成が完了しました」と表示されるので「終了」をクリックし完了させます。
　これでEntraConnectでの作業は完了となります。

4.3. パスワードハッシュ同期 設定



【作成したユーザーでサインイン】
同期したユーザーのパスワードで別サービスにサインインできるか確認します

1. Microsoft Entra IDポータルへサインインします

2. 前ページで作成したユーザーのアカウント/ パスワードを入力し、サインインできることを確認できます

4.3. パスワードハッシュ同期 設定

Microsoft社へ確認中

【サインインログ/ ○○ の確認方法】

設定した認証方式に基づいて、ユーザーが正常にサインインできているかを確認します。

4.4. パススルー認証 設定

4.4. パススルー認証 設定

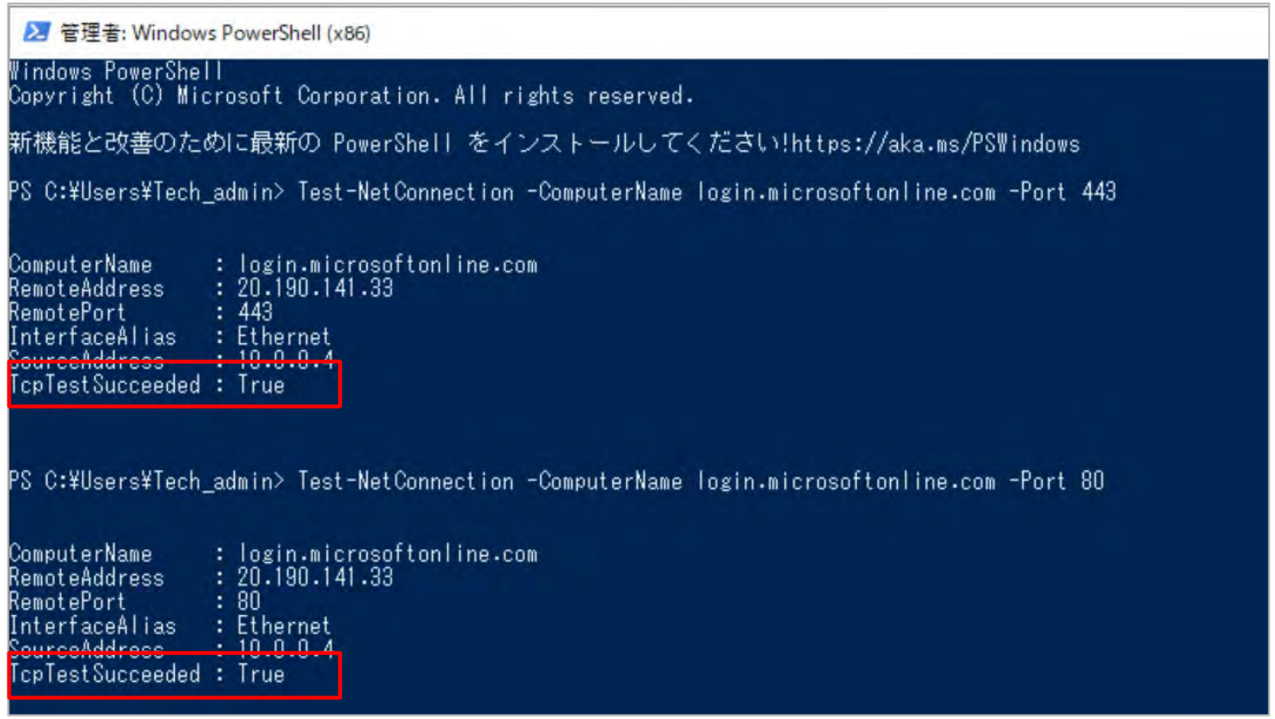
ポート番号	用途
80	TLS/SSL 証明書を検証する際に証明書失効リスト (CRL) をダウンロードします
443	サービスを使用したすべての送信方向の通信を処理する
8080 (省略可能)	ポート 443 が使用できない場合、認証エージェントは、ポート 8080 経由で 10 分ごとにその状態を報告します。 この状態は、Microsoft Entra 管理センターに表示されます。 ポート 8080 は、ユーザー サインインには 使用されません。

【前提】

1. サーバーと Microsoft Entra ID の間にファイアウォールがある場合は、次の項目を構成します。

認証エージェントが次のポートを介して Microsoft Entra ID に "送信" 要求を行うことができるようにします。

4.4. パススルー認証 設定

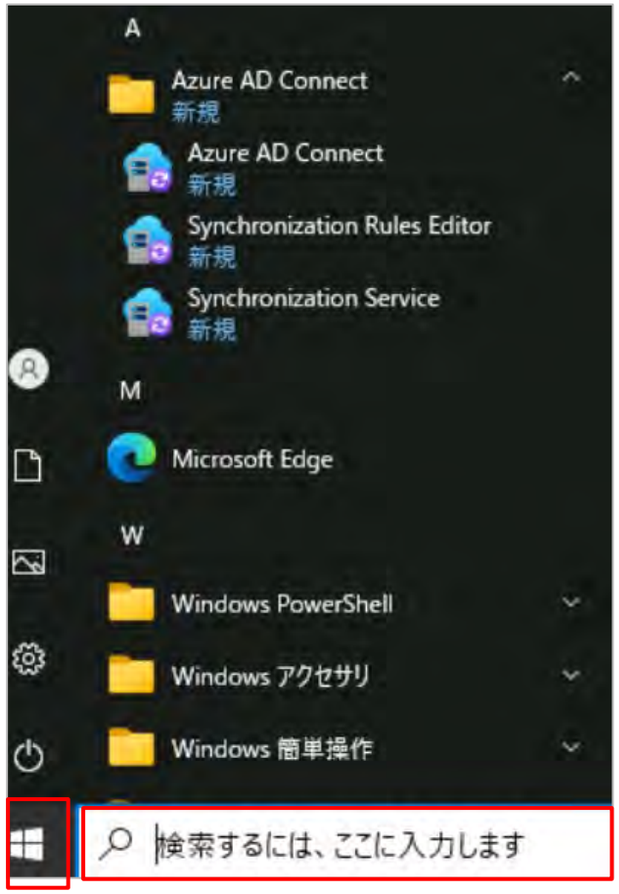


2. ポート80,443 が開いているかどうかはPowerShellのコマンドにて確認を行うことができます。

コマンド
==========
Test-NetConnection -ComputerName login.microsoftonline.com -Port 443
Test-NetConnection -ComputerName login.microsoftonline.com -Port 80
==========

3. TcpTestSucceededが ”True” なら、ポートは開いていることになります。

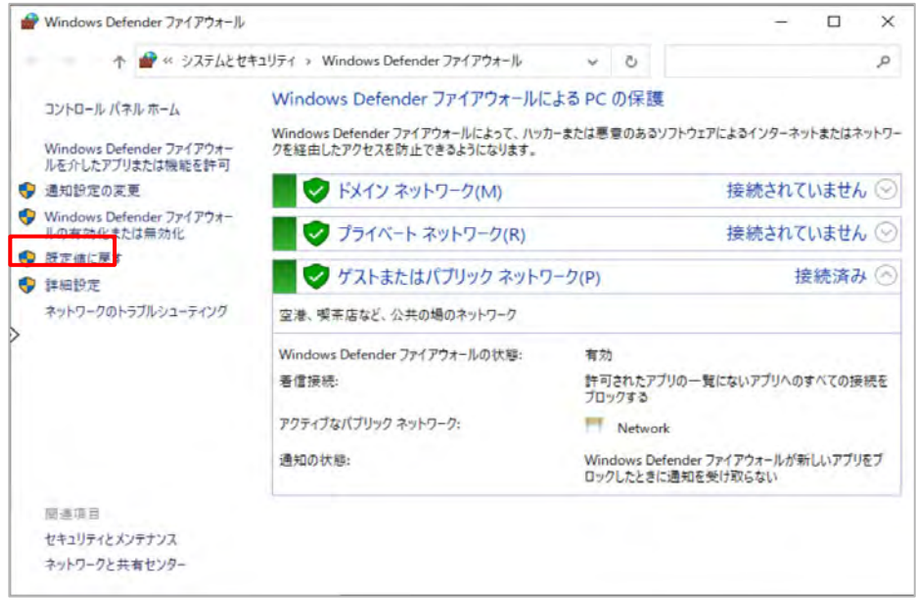
4.4. パススルー認証 設定



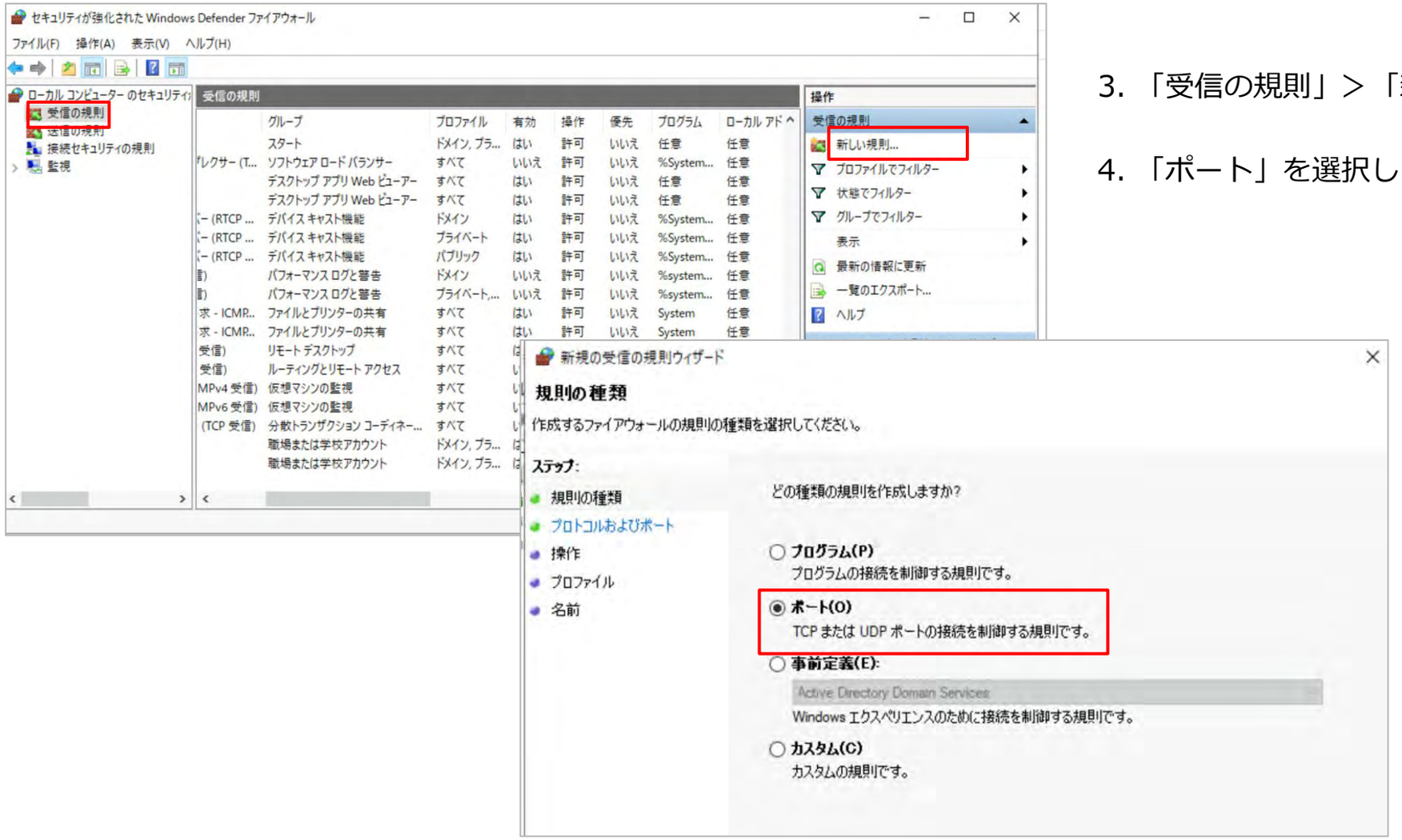
【ポート80,443 が開いていない場合のファイアウォール設定】

1. スタートボタンから [Windows Defender ファイアウォール] をクリックします。

2. 「詳細設定」をクリックします。



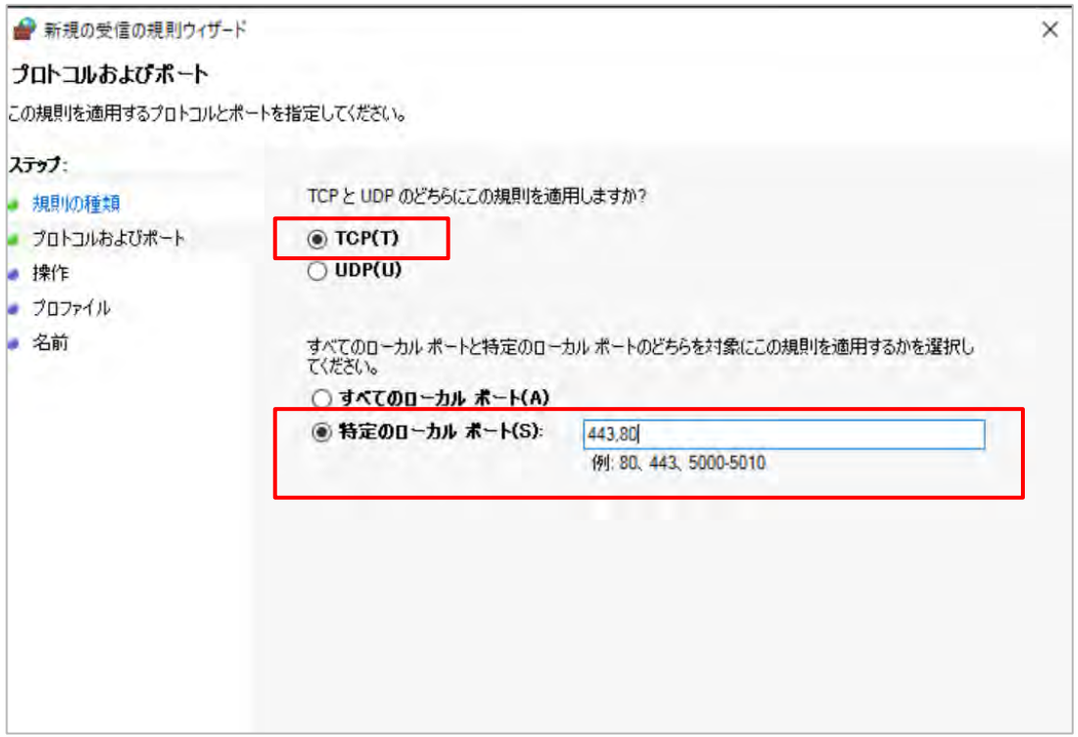
4.4. パススルー認証 設定



3. 「受信の規則」＞「新しい規則」をクリックします。

4. 「ポート」を選択し、「次へ」をクリックします。

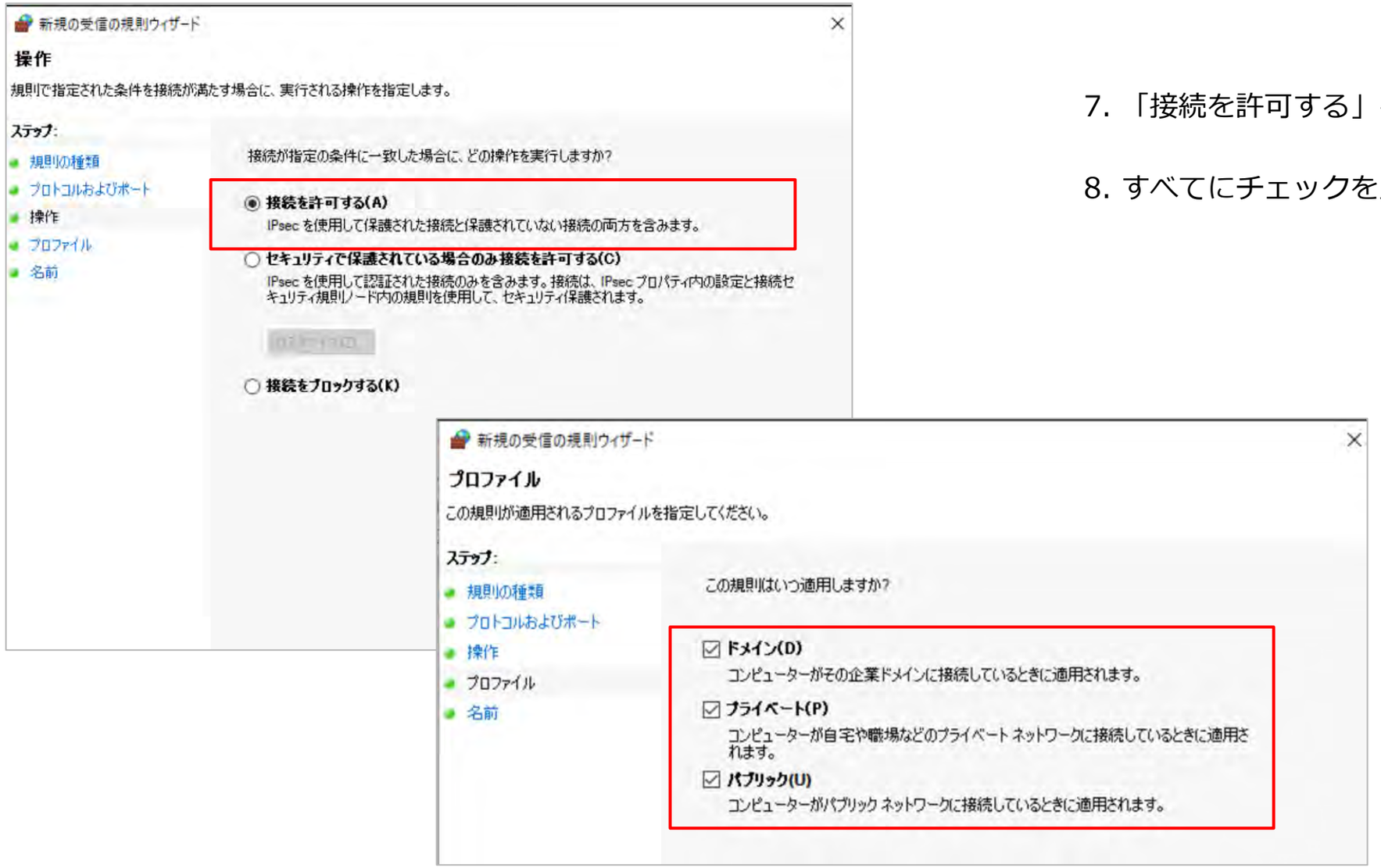
4.4. パススルー認証 設定



5. 「TCP」を選択します。

6. 「特定のローカルポート」を選択し、「443,80」を入力し、「次へ」をクリックします。

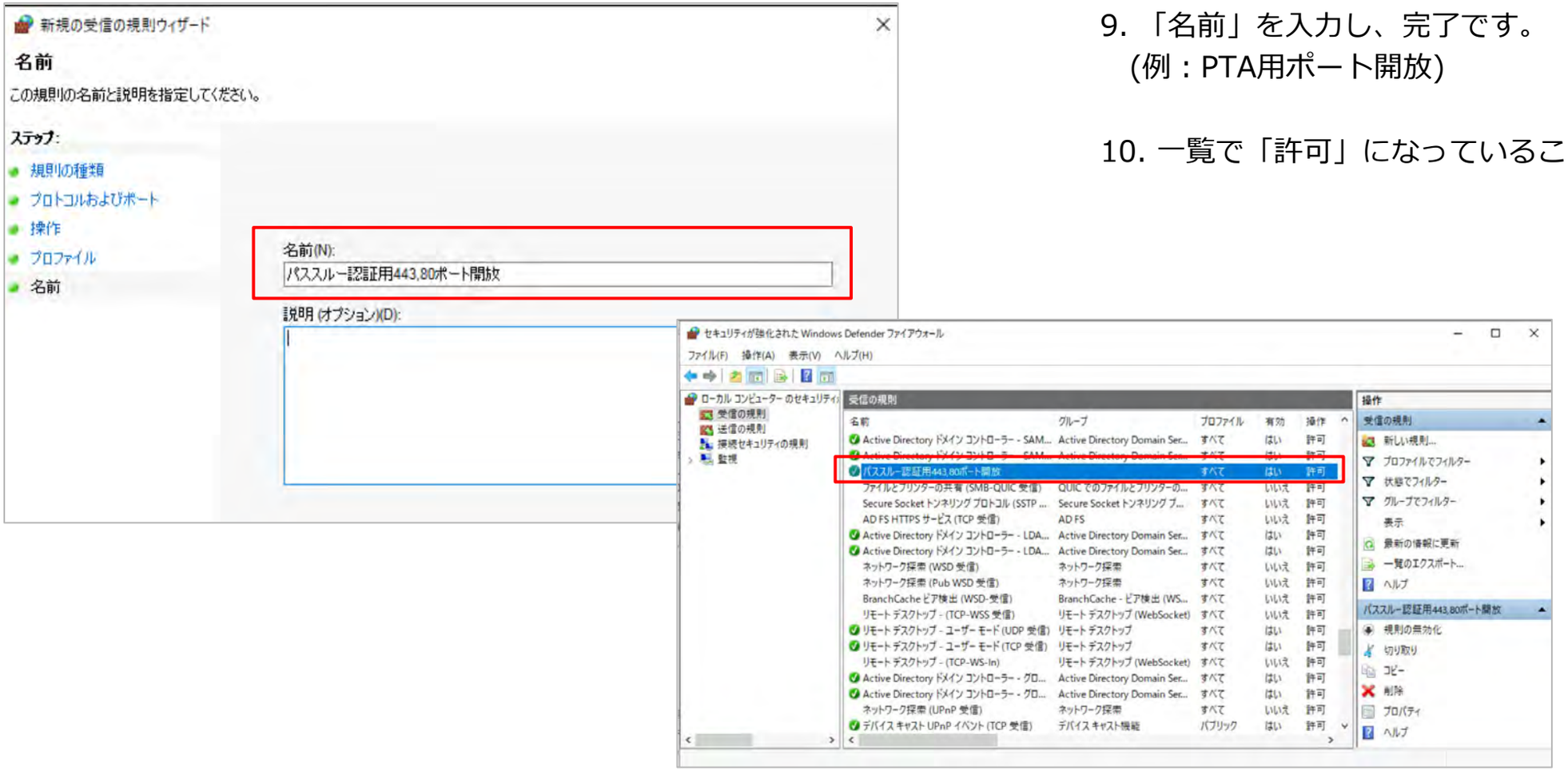
4.4. パススルー認証 設定



7. 「接続を許可する」を選択し、次へ」をクリックします。

8. すべてにチェックを入れ、「次へ」をクリックします。

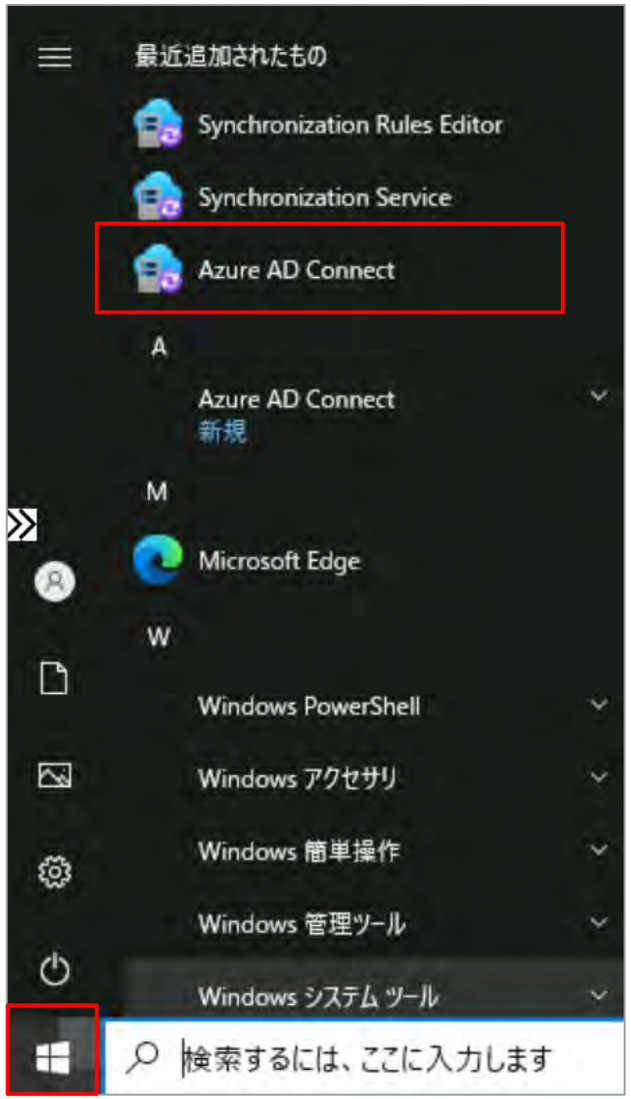
4.4. パススルー認証 設定



9. 「名前」を入力し、完了です。
   (例：PTA用ポート開放)

10. 一覧で「許可」になっていることを確認します。

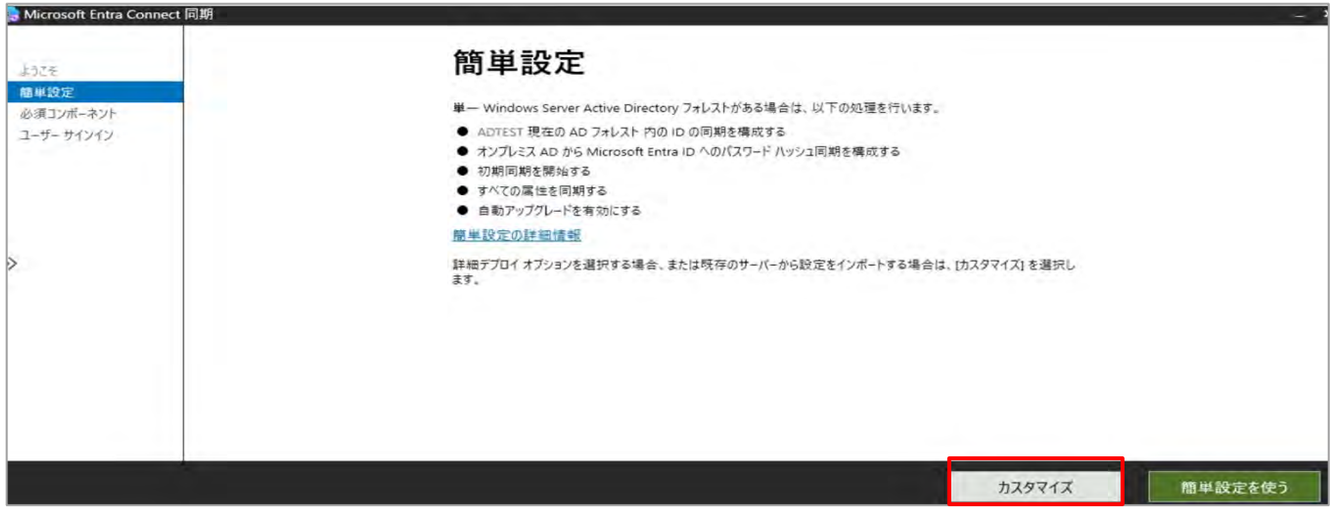
4.4. パススルー認証 設定



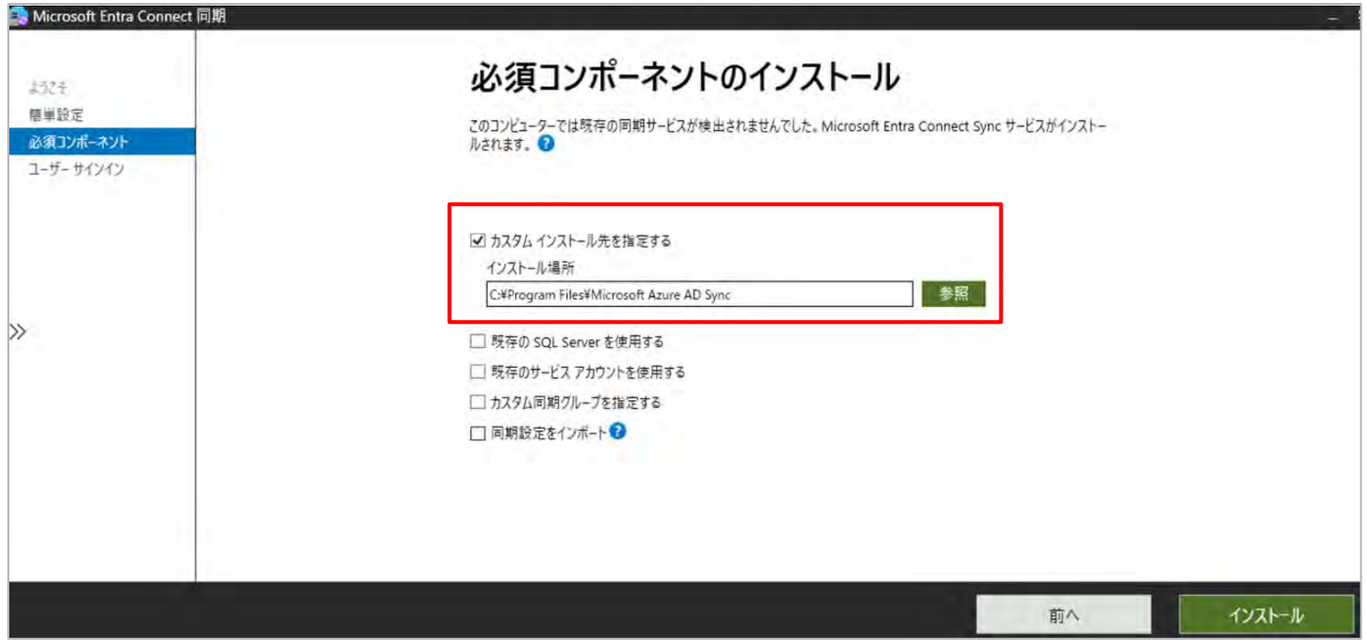
【Microsoft Entra Connect での設定】

1.Entra Connectをダウンロード後、 スタートボタンから
[Azure AD Connect] をクリックします。

2 [Microsoft　Entra Connectへようこそ]という表示された後、「簡単設定」＞「カスタマイズ」をクリックします。

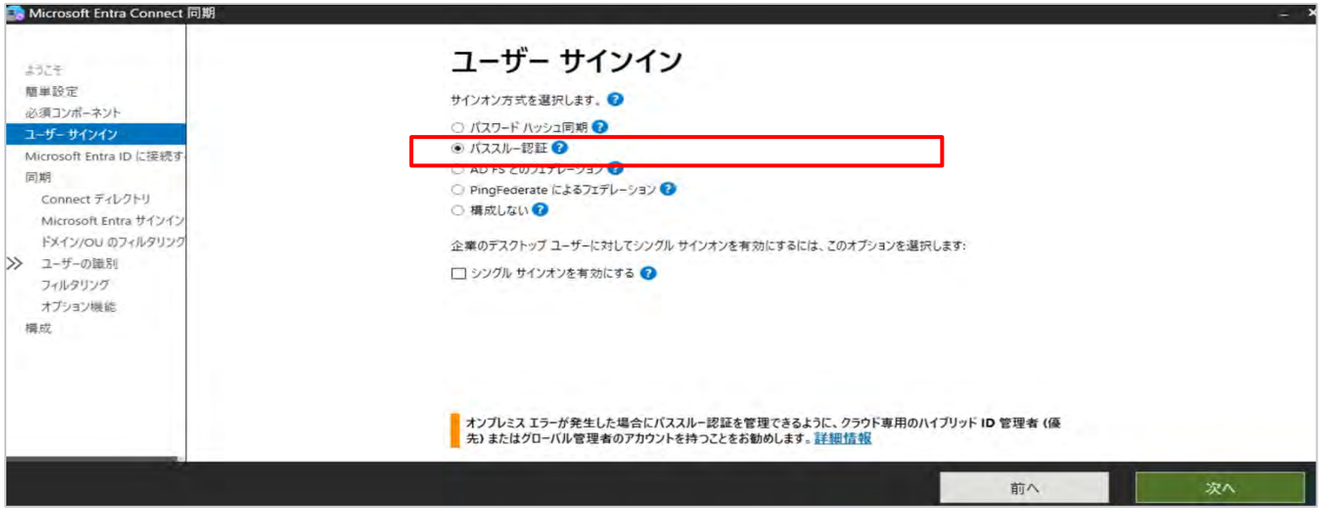


4.4. パススルー認証 設定



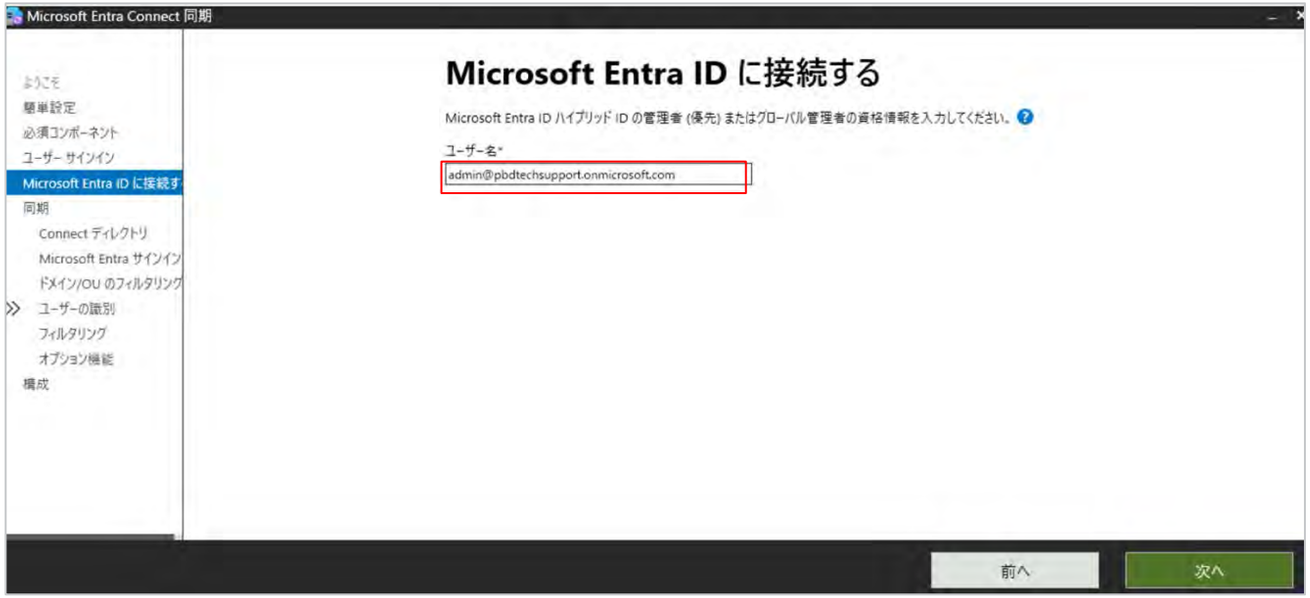
3. 必須コンポーネントのインストールから
［ カスタムインストール左記を指定する ］をクリックし「次へ」をクリックします。

4.4. パススルー認証 設定



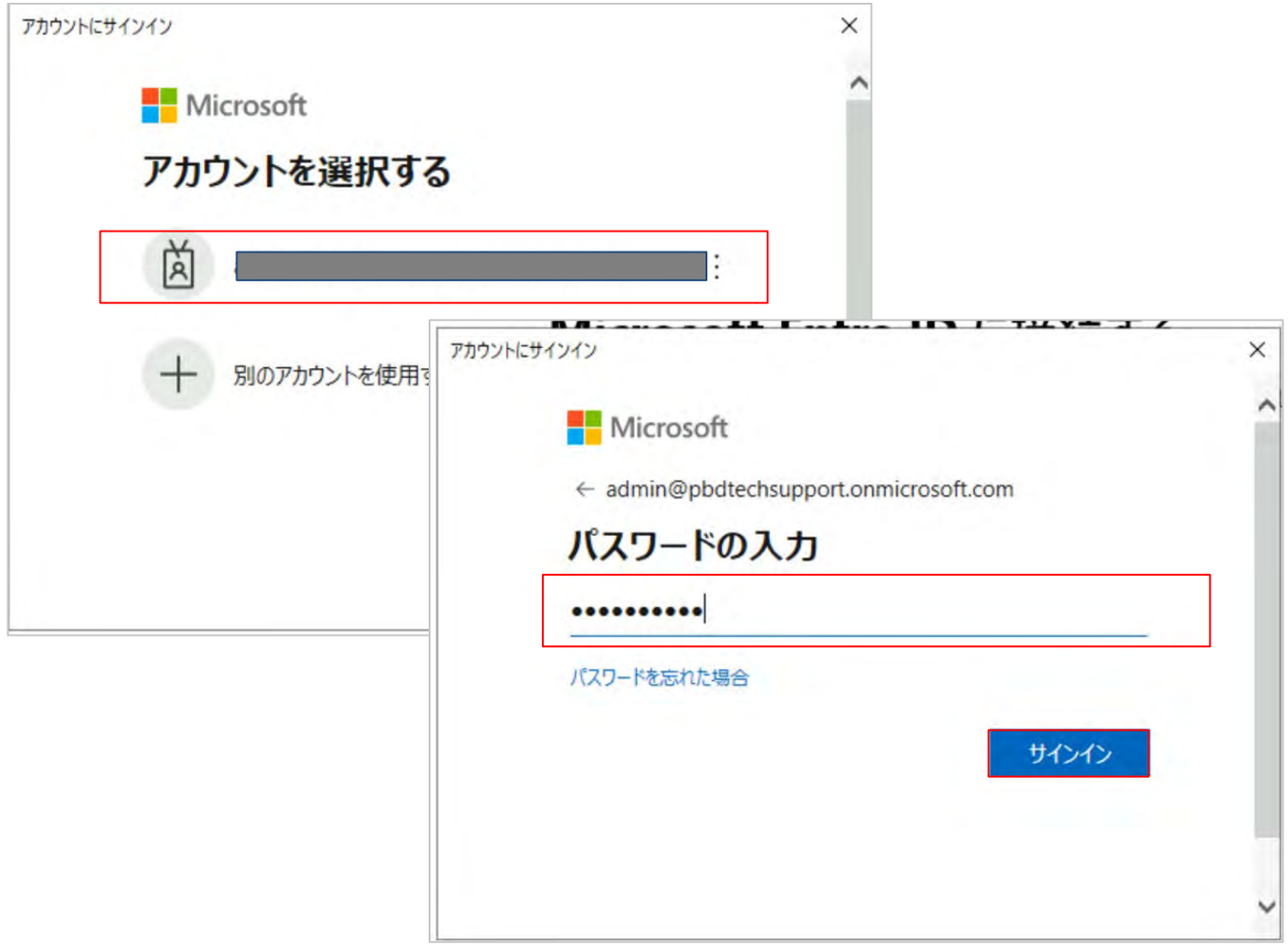
4. サインイン方式について「パススルー認証」を選択し「次へ」をクリックします。

4.4. パススルー認証 設定



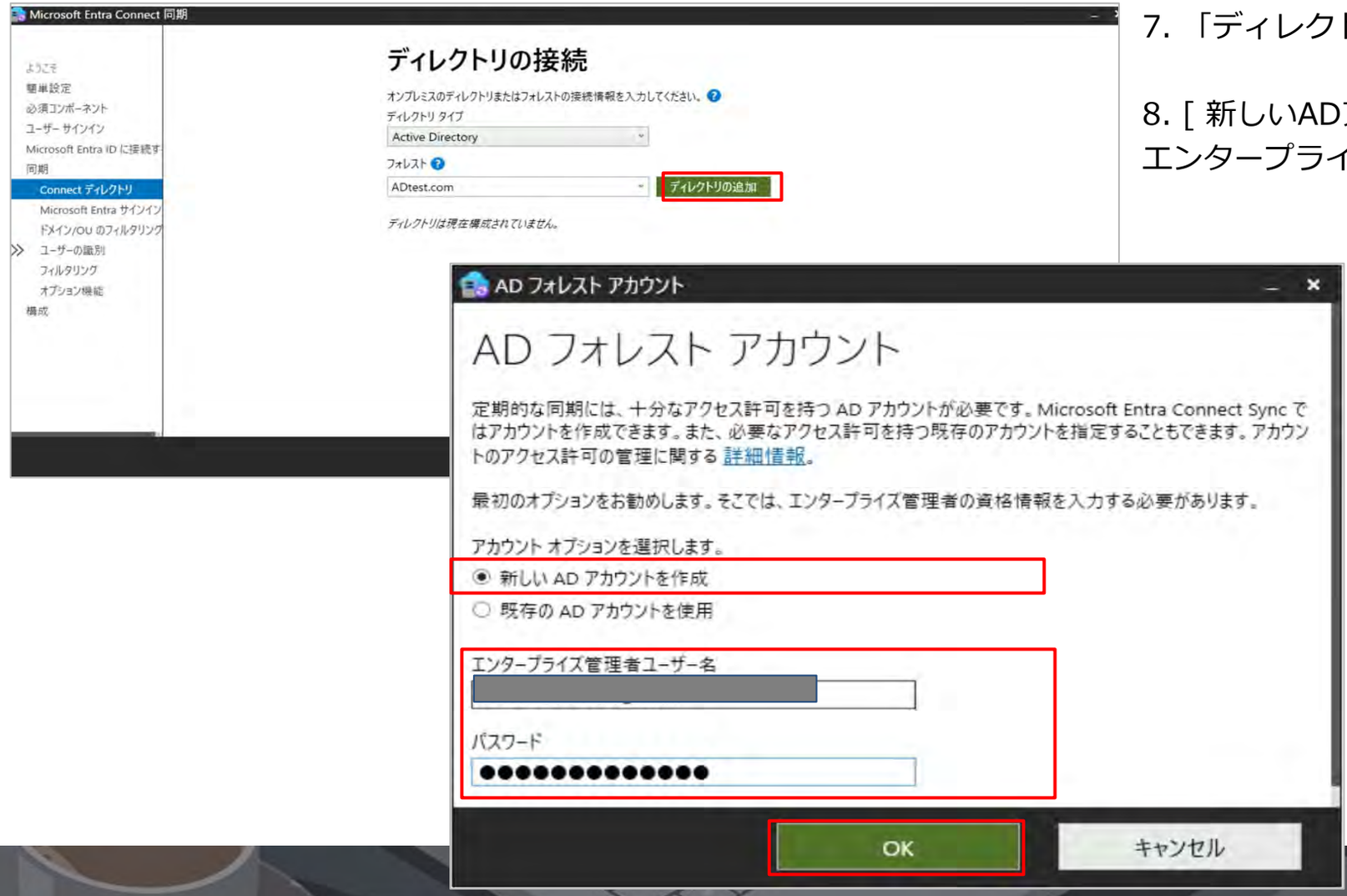
5. [ユーザ名] へMicrosoft Entra IDのハイブリッド管理者またはグローバル管理者のアカウントを入力します。

4.4. パススルー認証 設定



6. アカウントの認証画面に遷移するので、
アカウントとパスワードを入力し「サインイン」をクリックします。

4.4. パススルー認証 設定



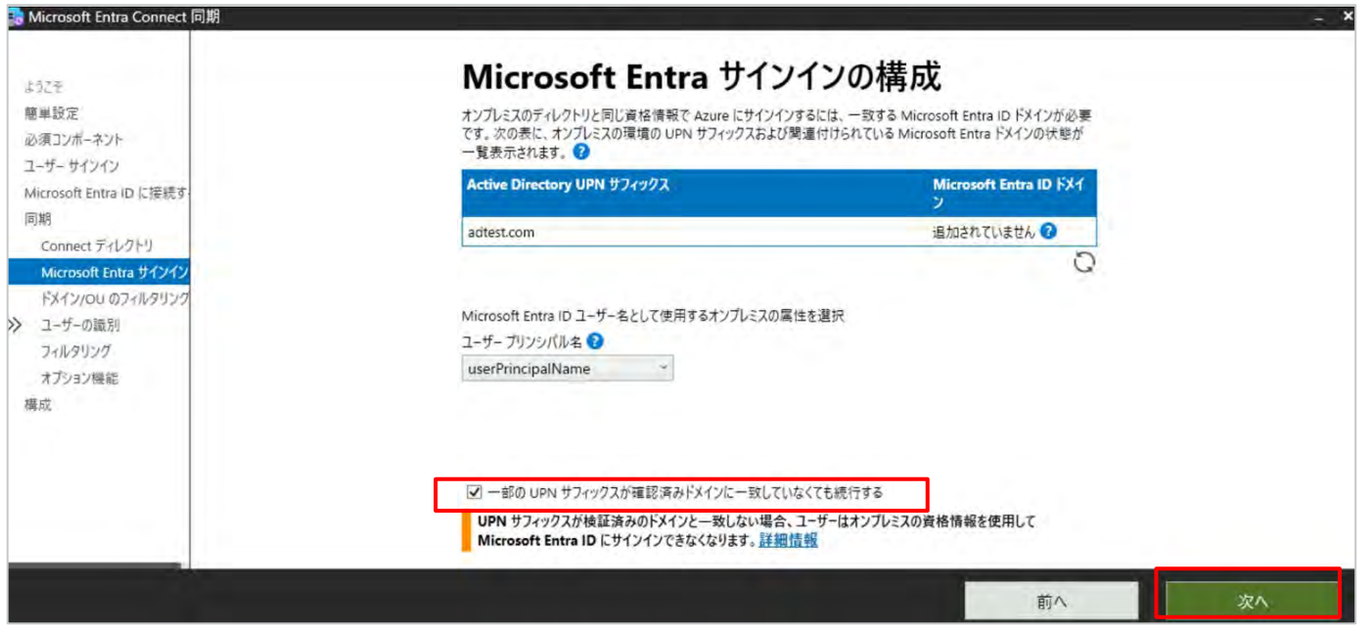
7. 「ディレクトリの追加」をクリックします。

8. [新しいADアカウントを作成]を選択し、
エンタープライズ管理者ユーザー名、パスワードを入力します。

4.4. パススルー認証 設定

9. [構成済みディレクトリ] に前のページで作成したディレクトリが反映されていることを確認し「次へ」をクリックします。

4.4. パススルー認証 設定



10. [一部のUPNサフィックス…] にチェックが入っていることを確認し「次へ」をクリックします。

4.4. パススルー認証 設定

11. ドメインとOUのフィルタリング画面で[すべてのドメインとOUの同期]が選択されていることを確認し「次へ」をクリックします。

12. 一部のユーザー識別画面においては、設定変更せずに「次へ」をクリックします。

4.4. パススルー認証 設定

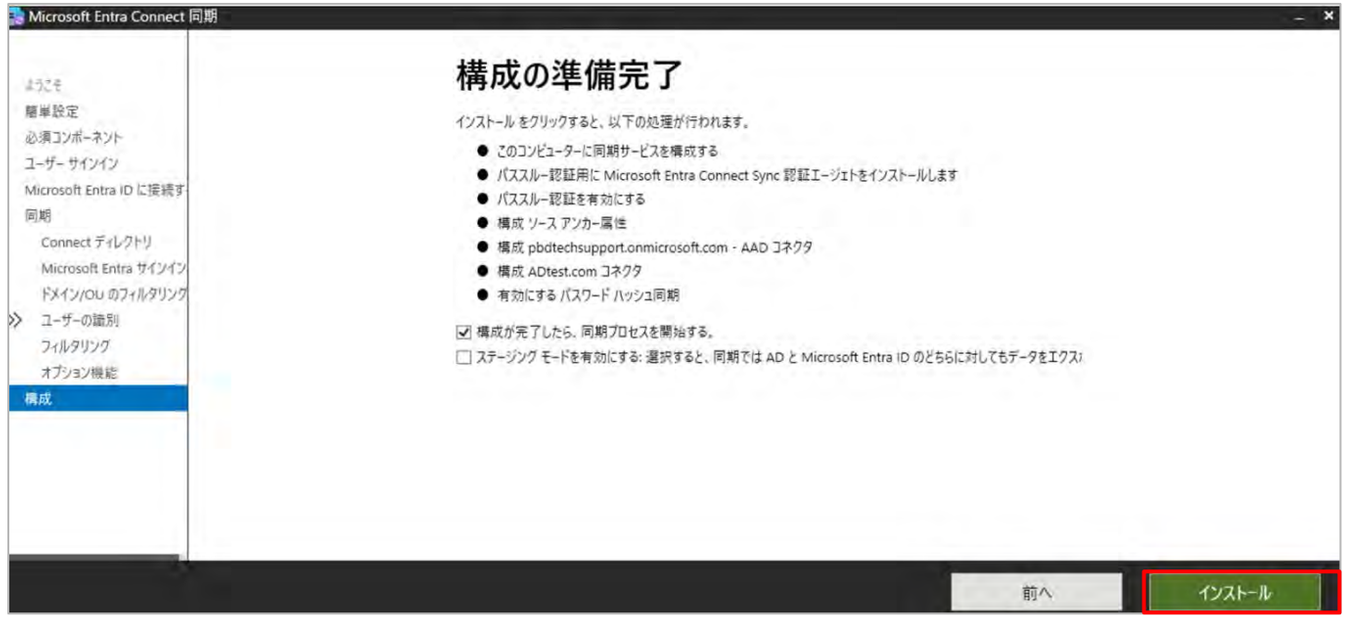
13. ユーザーおよびデバイスのフィルタリング画面では
何も変更せずに「次へ」をクリックします。

4.4. パススルー認証 設定

14. オプション機能で「パスワードハッシュ同期」を選択し必要に応じて他のオプションも選択し「次へ」をクリックします。

※「パスワードハッシュ同期」にチェックを入れておくと、Pパススルー認証が動かない時に自動でパスワードハッシュ同期が使われます。

4.4. パススルー認証 設定

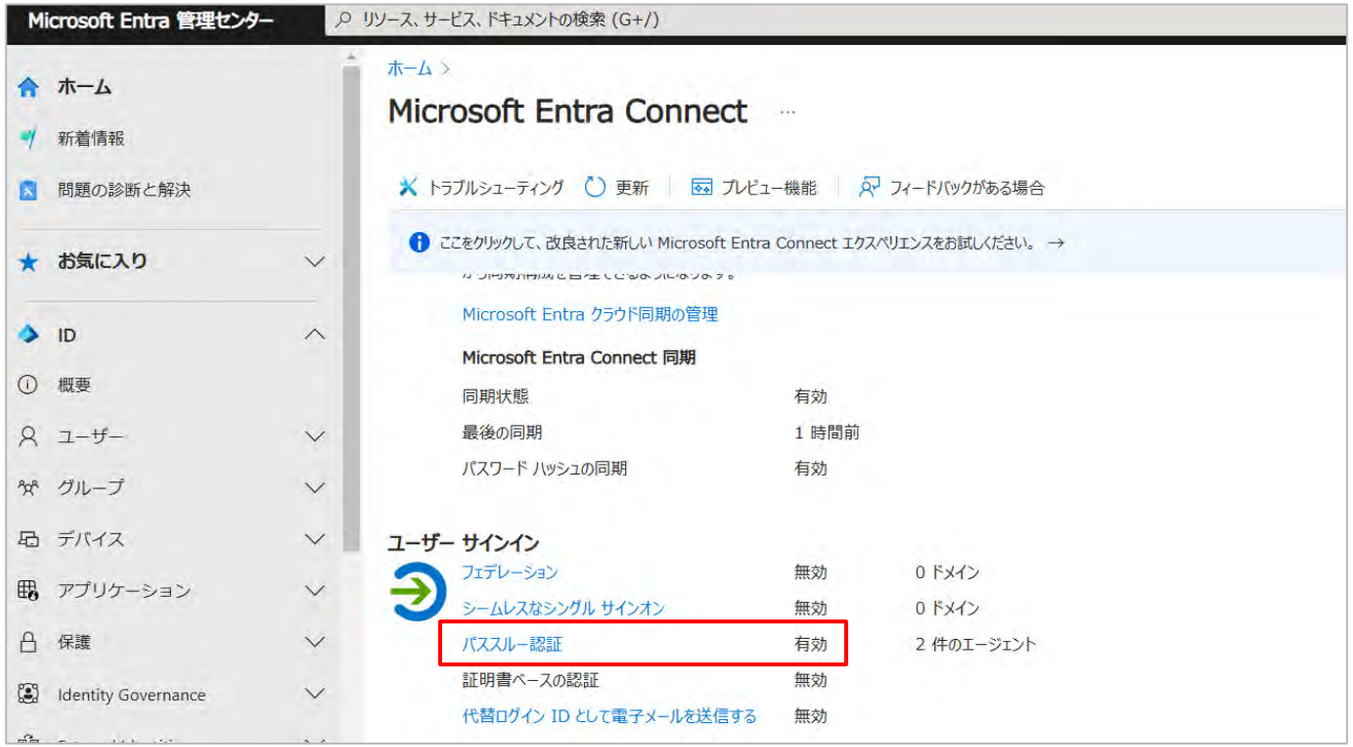


15. 構成の準備完了画面が表示されるので、画面に表示されている内容で問題がなければ「インストール」をクリックします 。

4.4. パススルー認証 設定

16. しばらくすると「構成が完了しました」と表示されるので「終了」をクリックし完了させます。
　これでEntraConnectでの作業は完了となります。

4.4. パススルー認証 設定



【Entra管理ポータルにて同期設定確認】

1 Microsoft Entra IDポータルへサインインします。

2. Microsoft Entra Connect にて、[パススルー認証] が“有効”になっていることを確認します。

3. [パススルー認証]をクリックします。

4.4. パススルー認証 設定

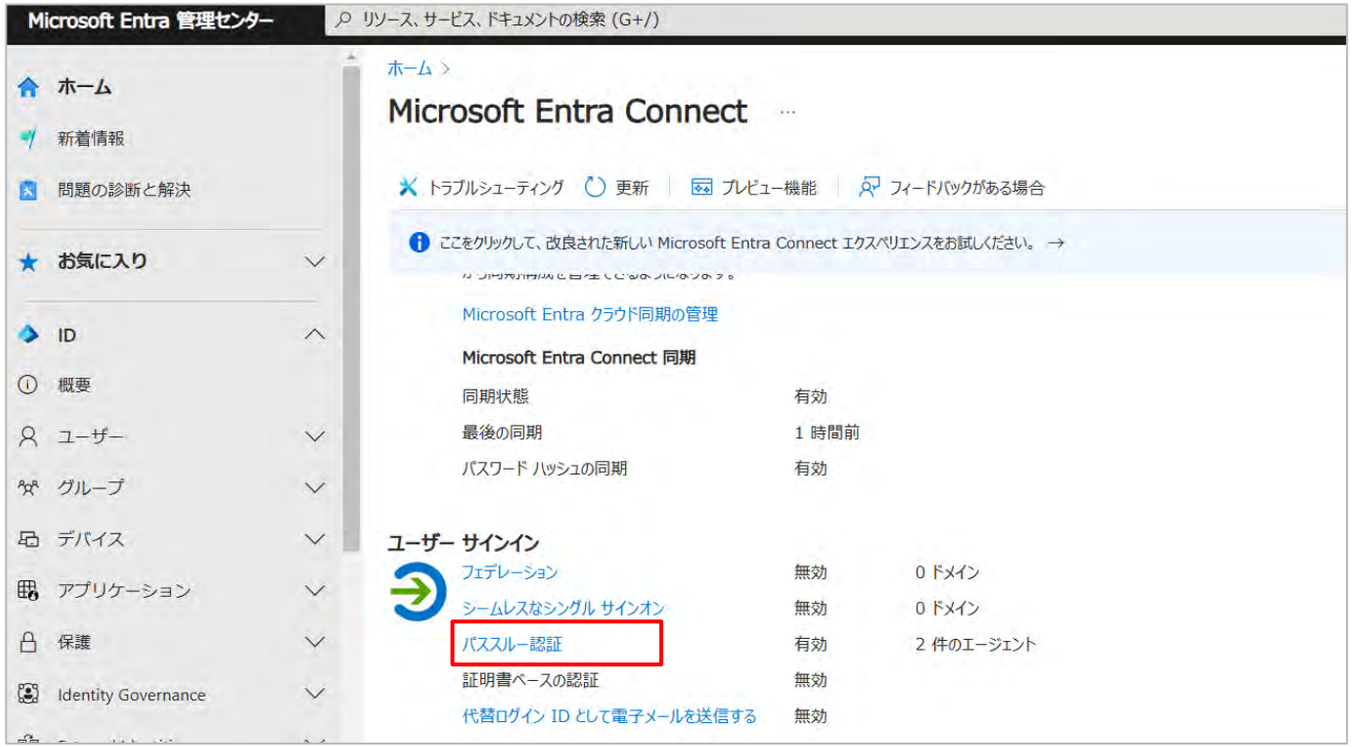
4. 認証エージェントに追加されていることを確認し、
状態が”アクティブ（緑のチェックマーク）”になっていることを
確認します。

4.4. パススルー認証 設定

5. 左ペインの「監視と正常性」＞「監査ログ」をクリックします。

6. アクティビティ[Enable passthrough authentication]のログにて状態が[success] となっていることを確認します。

4.4. パススルー認証 設定



【2台目以降の認証エージェントのインストール方法】

認証エージェントが1台だけだと、サーバーがダウンしたときにパススルー認証が機能しなくなるため、Microsoft社で3台以上の構成が推奨されています。

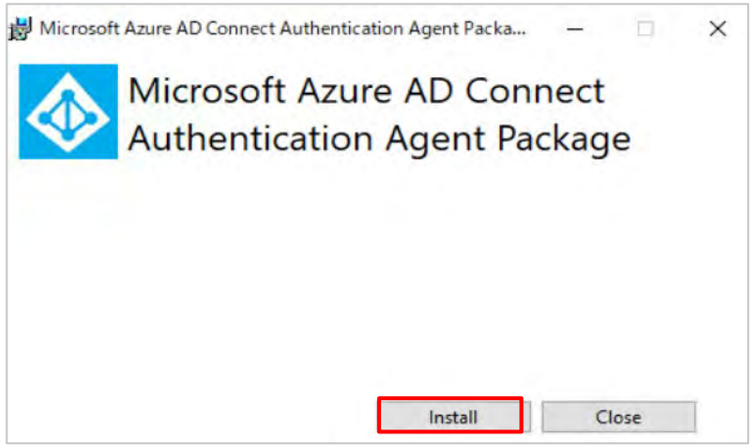
1. Microsoft Entra Connect にて、[パススルー認証] をクリックします。

4.4. パススルー認証 設定

2. 「ダウンロード」をクリックします。

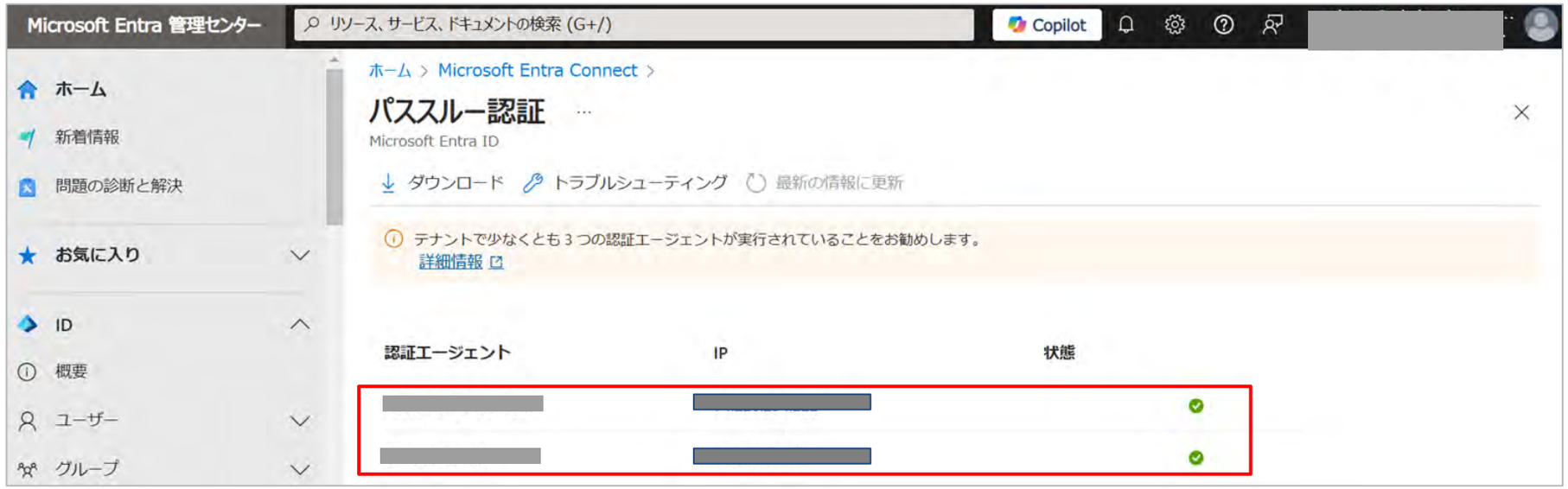
3.「使用条件に同意してダウンロード」をクリックします。

4.4. パススルー認証 設定

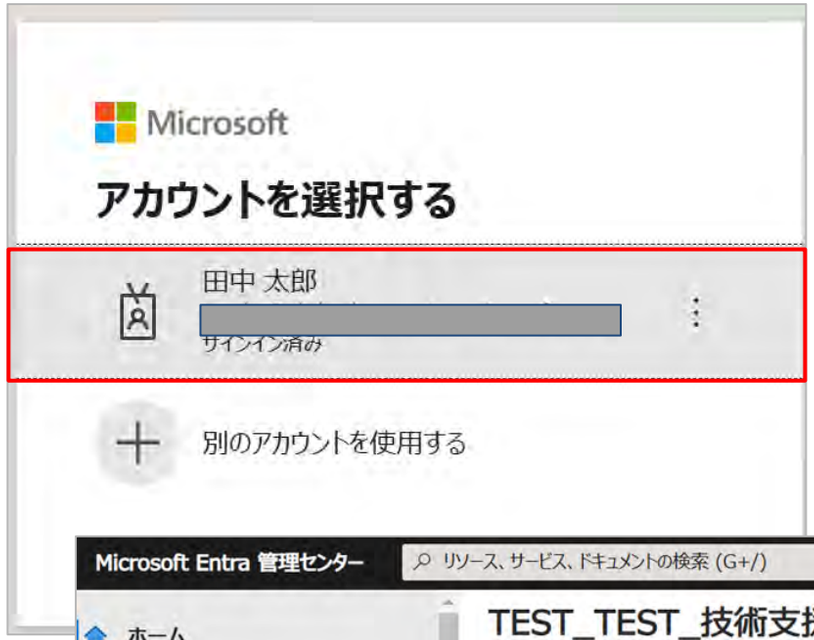


4. 画面ウィザードに沿ってインストールを実行します。

5. インストール完了後、 認証エージェントが二つに増えていることが確認できます。



4.4. パススルー認証 設定



【作成したユーザーでサインイン】
同期したユーザーのパスワードで別サービスにサインインできるか確認します。

1. Microsoft Entra IDポータルへサインインします。

2. 前ページで作成したユーザーのアカウント/ パスワードを入力し、サインインできることを確認できます。

4.4. パススルー認証 設定

Microsoft社へ確認中

【サインインログ/ ○○ の確認方法】

設定した認証方式に基づいて、ユーザーが正常にサインインできているかを確認します。

4.5. フェデレーション 設定

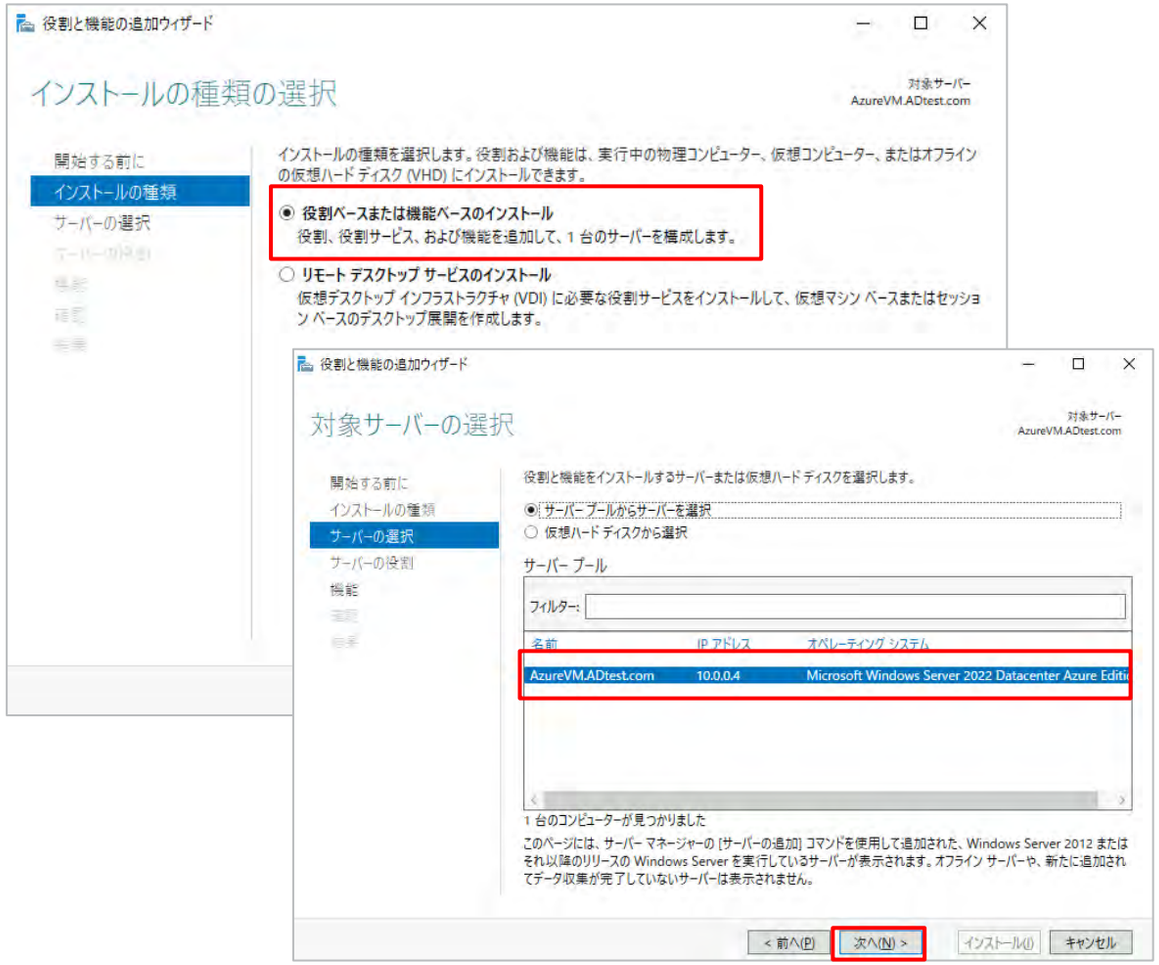
4.5. フェデレーション 設定

※事前にADFS用のSSL証明書を取得・インストールしていることが前提となります。

【WindowsサーバーへADFSをインストールする】

1. サーバーマネージャーで「役割と機能の追加」をクリックし、「次へ」をクリックします。

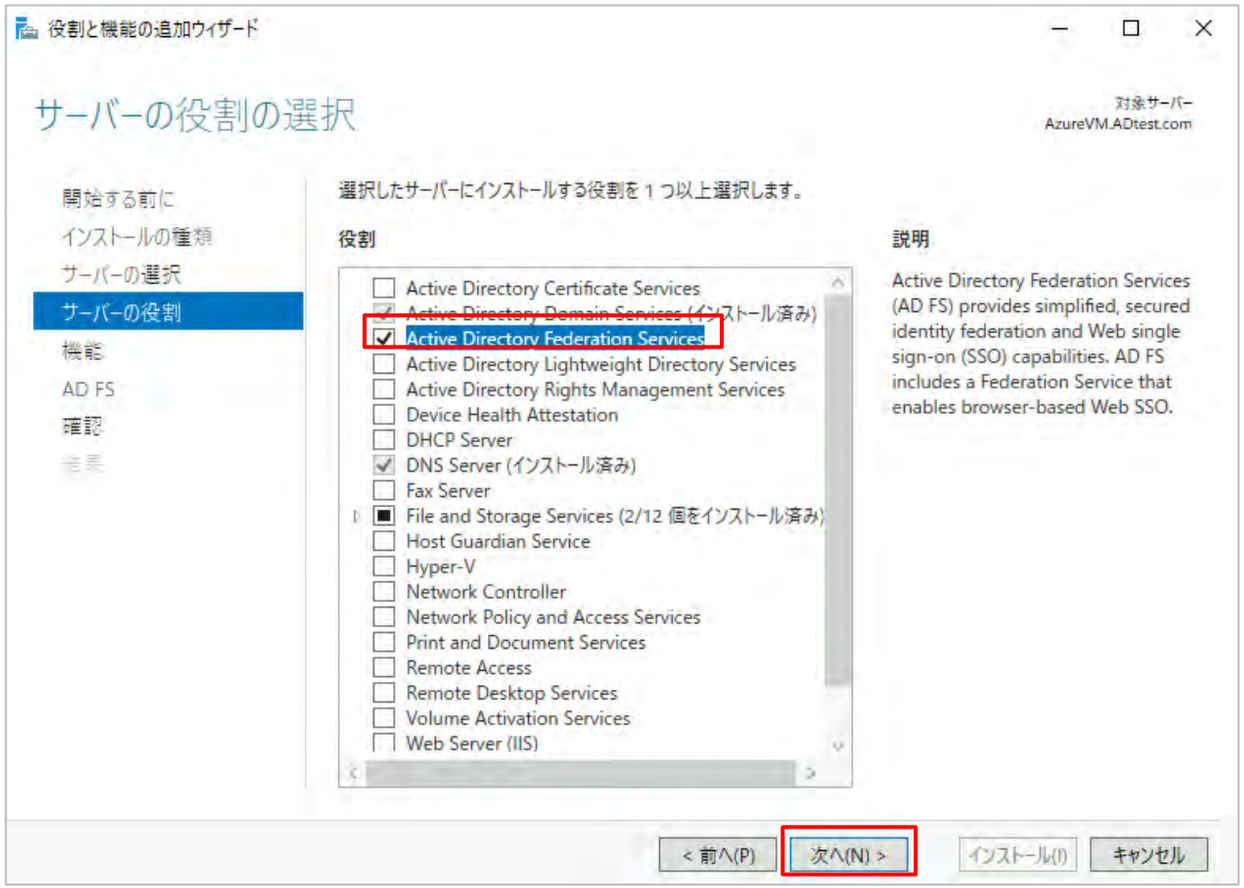
4.5. フェデレーション 設定



2. 「役割ベースまたは機能ベースのインストール」を選択し、「次へ」をクリックします。

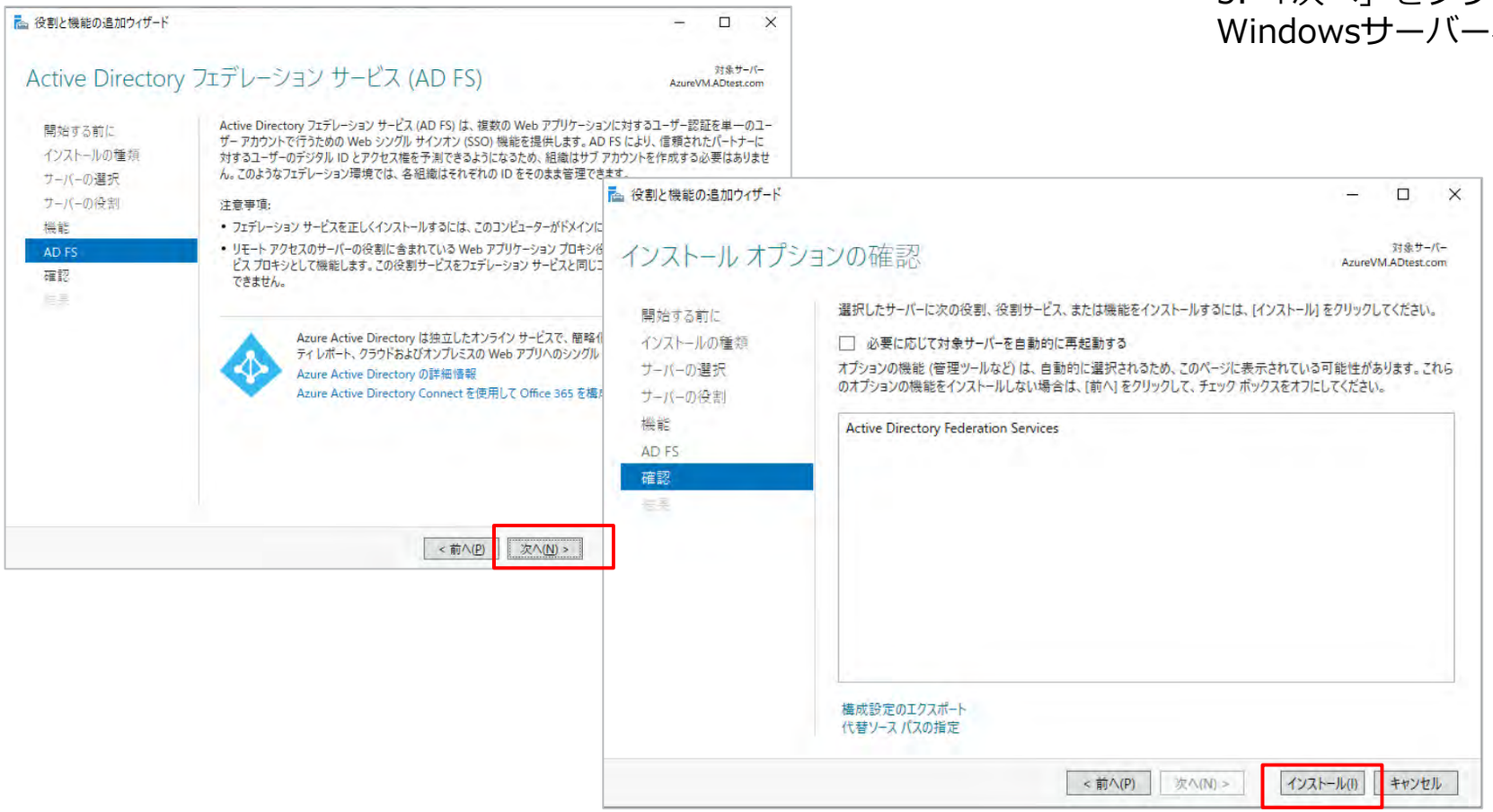
3. インストール先のサーバーを選択し、「次へ」をクリックします。

4.5. フェデレーション 設定



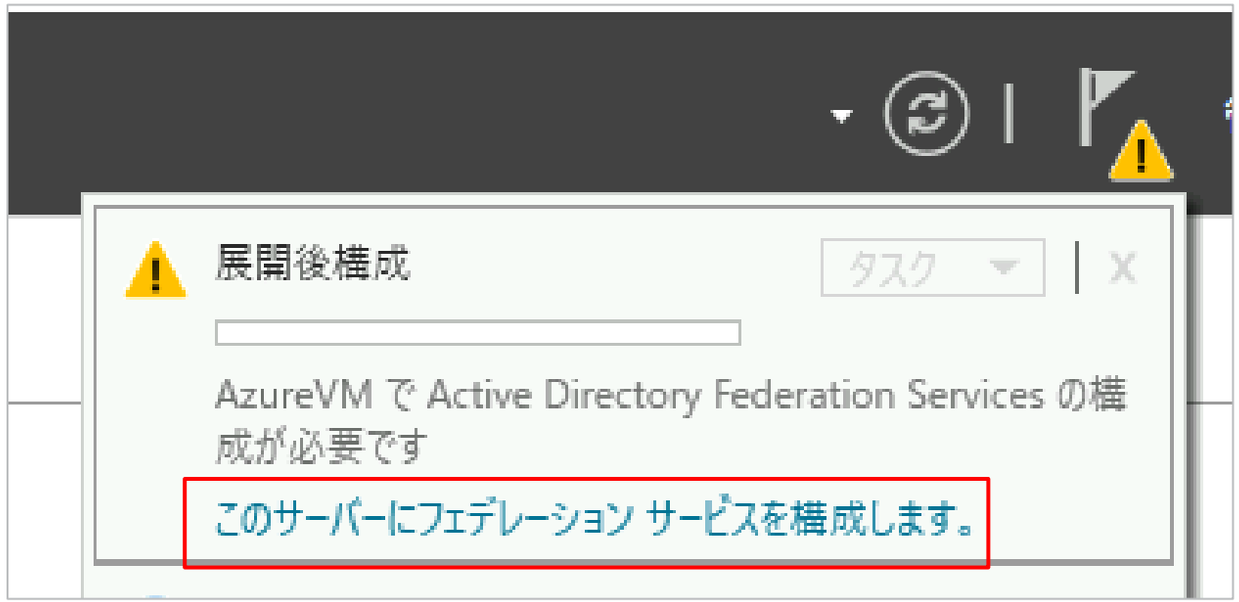
4. 「Active Directory Federation Service」にチェックを入れ、「次へ」をクリックします。

4.5. フェデレーション 設定



5. 「次へ」をクリックし、「インストール」を実行したら、WindowsサーバーへのADFSインストールが完了となります。

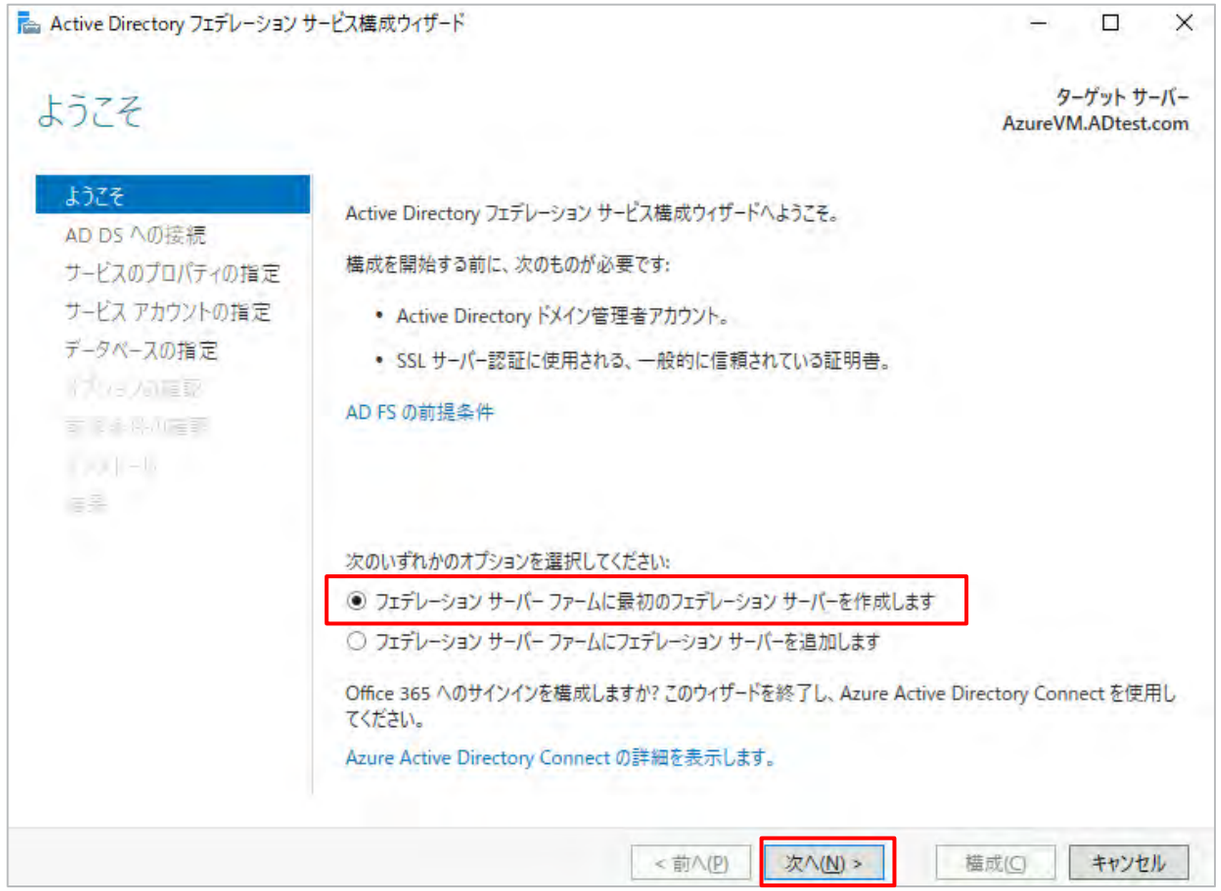
4.5. フェデレーション 設定



【AD FSの設定】

1．サーバーマネージャーの画面右上にある「展開後構成」から、「このサーバーにフェデレーション サービスを構成します。」をクリックします。

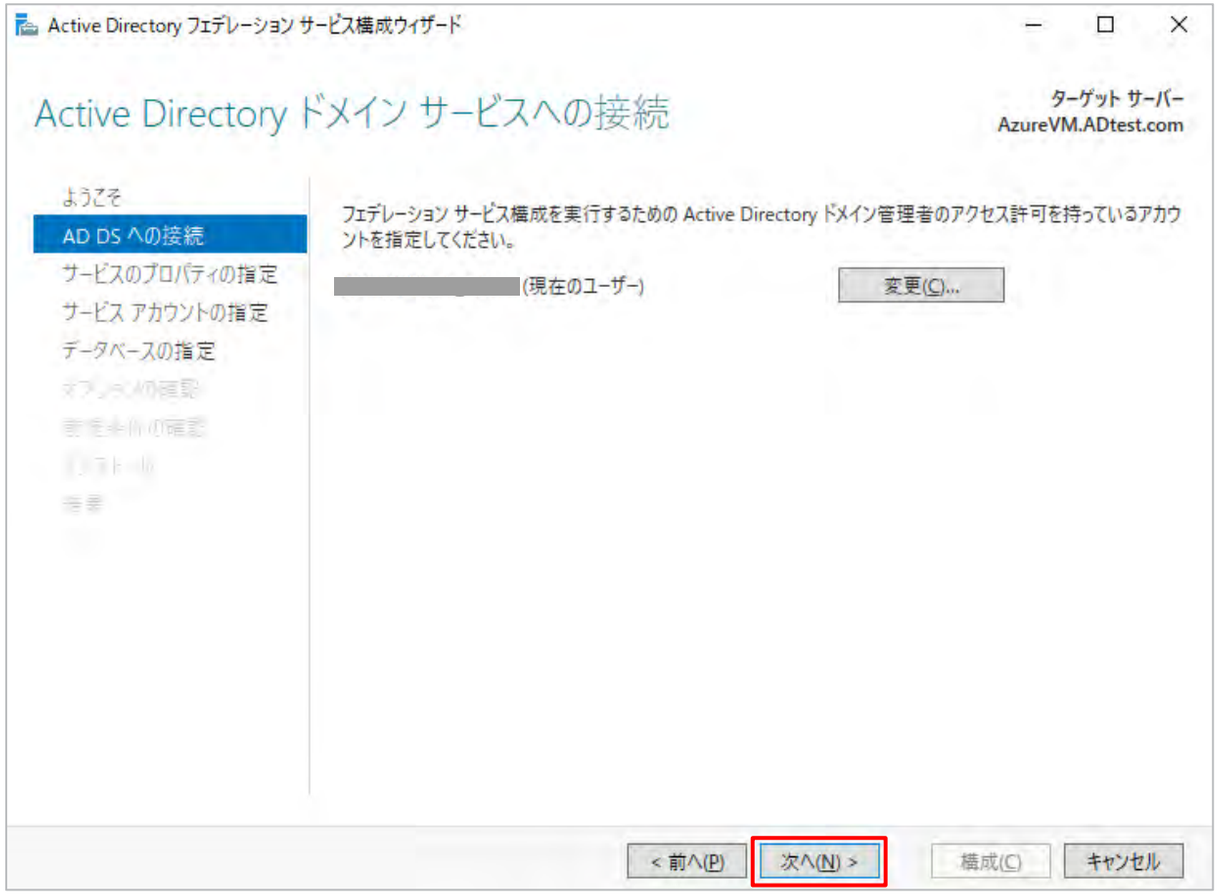
4.5. フェデレーション 設定



2. 今回は初回作成を例とするため「フェデレーション サーバー ファームに最初のフェデレーション サーバーを作成します。」を選択します。

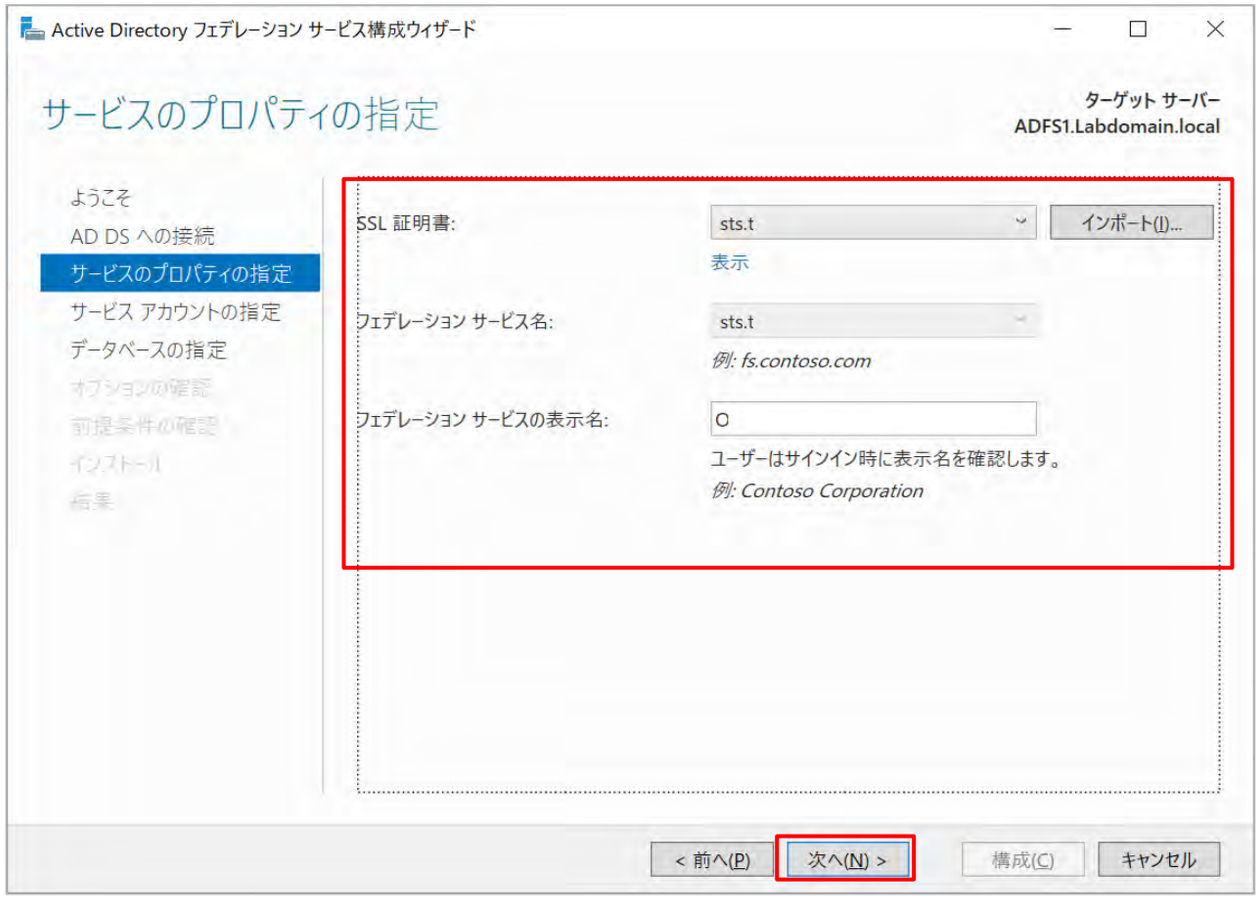
3. 「次へ」をクリックします。

4.5. フェデレーション 設定



4. 「次へ」をクリックします。

4.5. フェデレーション 設定



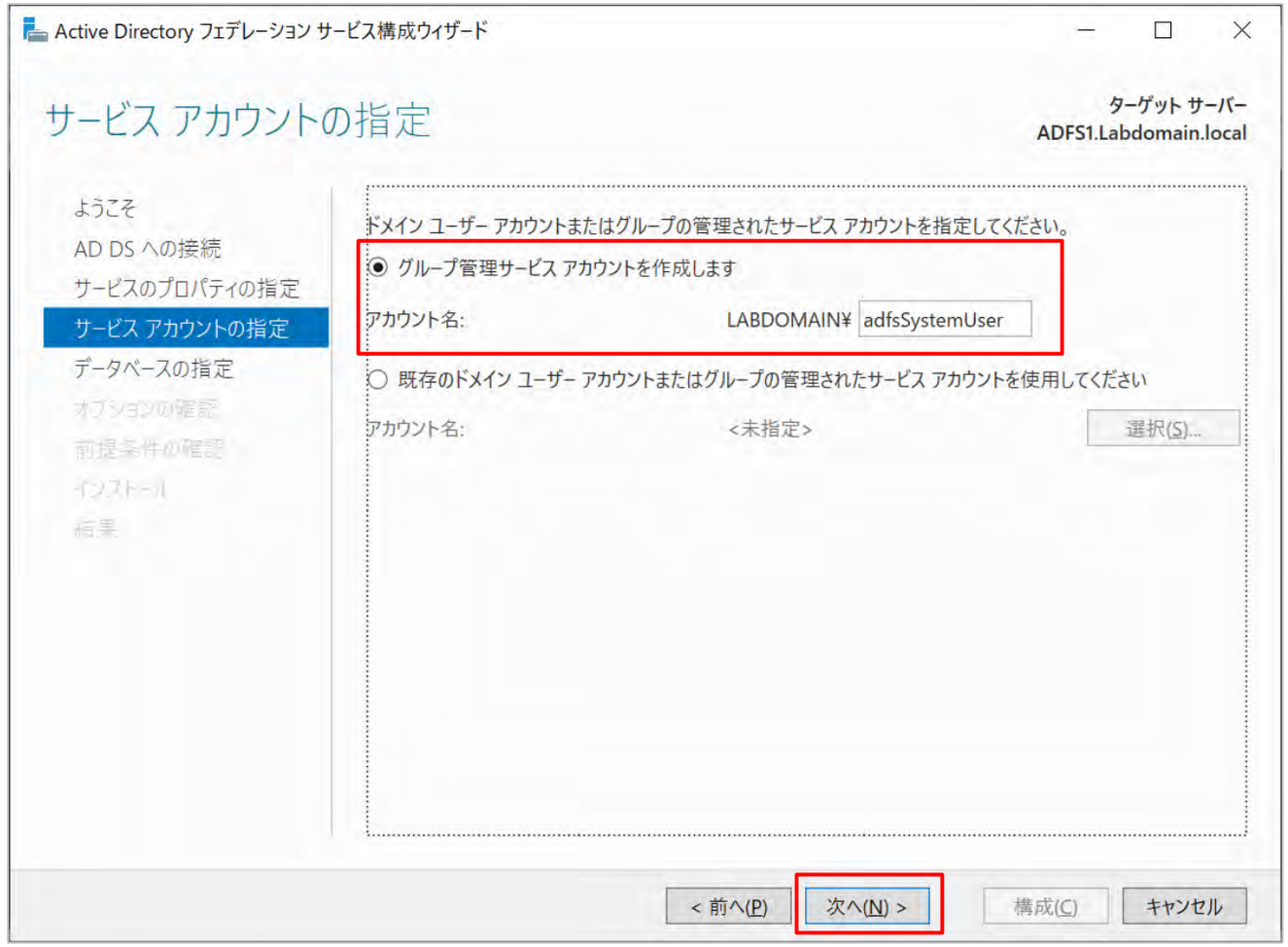
5. [SSL証明書]について、ドロップダウンリストから該当の証明書を選択またはインポートを行います。

6. [フェデレーション サービス名] をドロップダウンリストから選択します。

7. [フェデレーション サービス表示名] を入力します。
この名前は Microsoft 365 などのログイン画面で表示されます。

8. 「次へ」をクリックします。

4.5. フェデレーション 設定



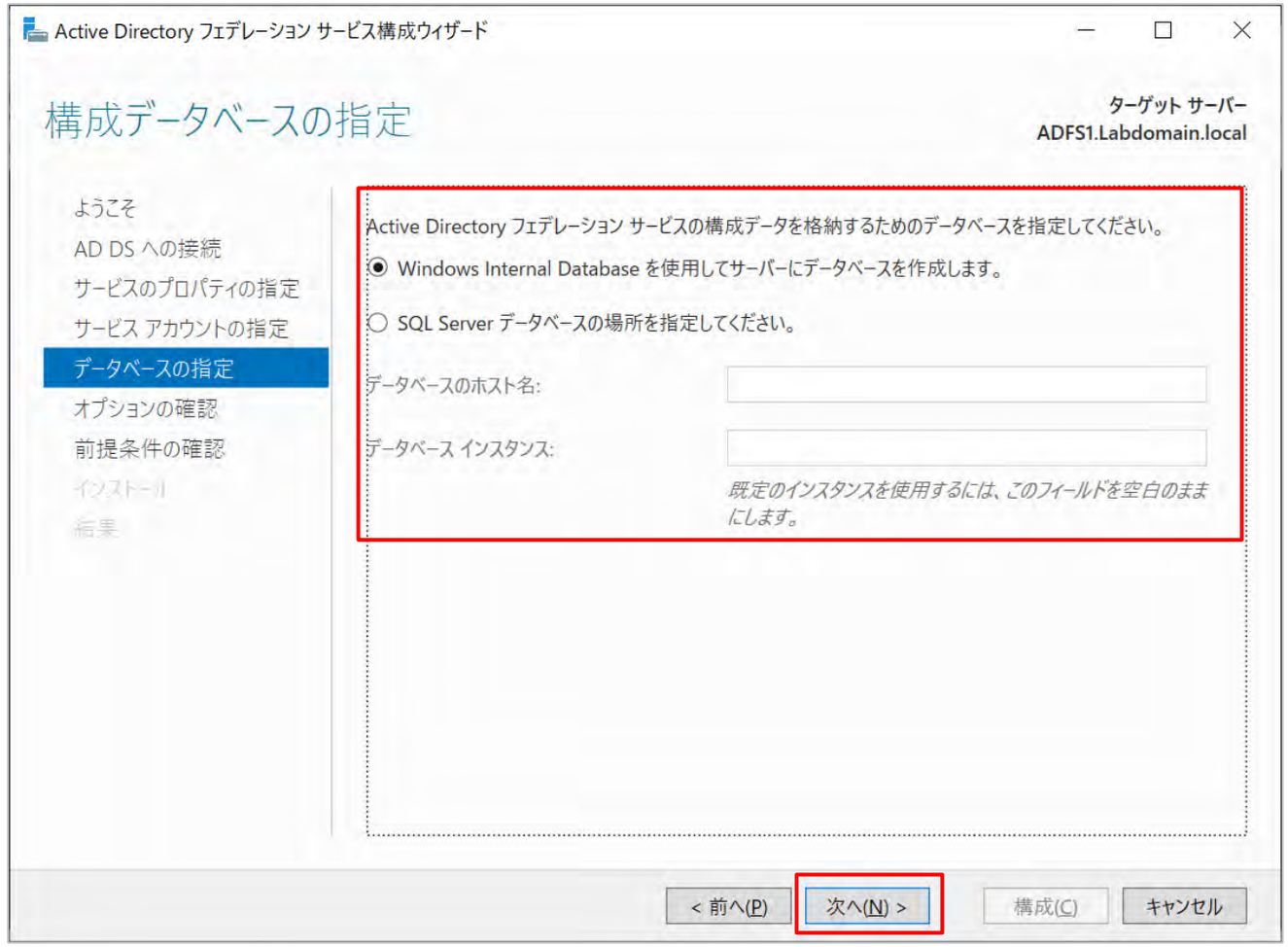
9. ADFSとActive Directoryを連携するため、サービスアカウントが必要であるため、グループ管理サービスアカウント（gMSA）を指定します。
gMSA を作成していない場合は、PowerShellで作成します。

powershellで以下のコマンドを入力します。

```
----------------------------------
New-ADServiceAccount -Name gmsa-adfs -
DNSHostName fs.XXXX -
PrincipalsAllowedToRetrieveManagedPassword
"XXXXXXXX"
----------------------------------
```

10. 「次へ」をクリックします。

4.5. フェデレーション 設定

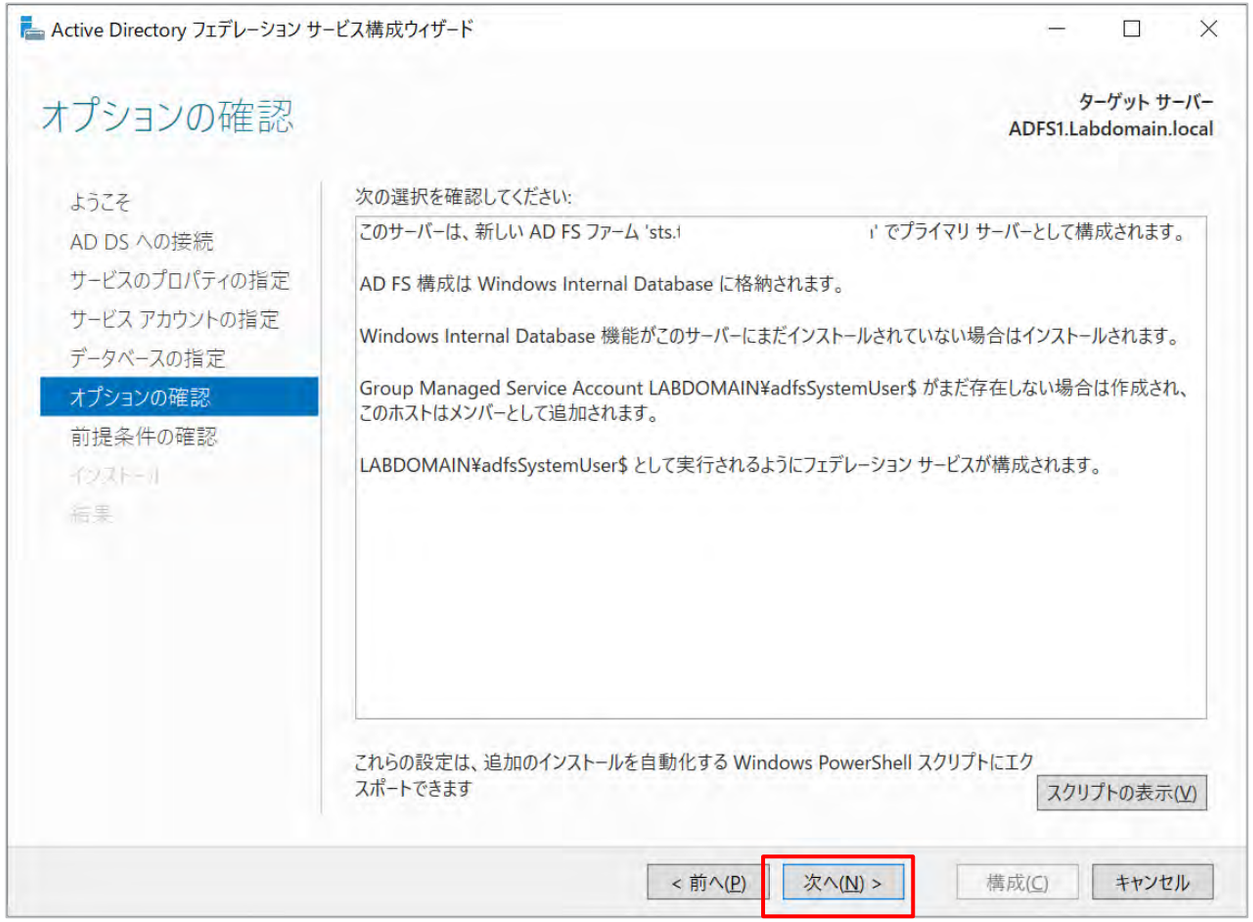


11. ADFSのデータ格納データベースを指定します。

・”Windows Internal Database（WID）”の場合は同期が5分間隔になるため、そういったケースを意識しておく必要があります。
・複数台のファーム構成で組む場合、”SQL Server”を選択します。

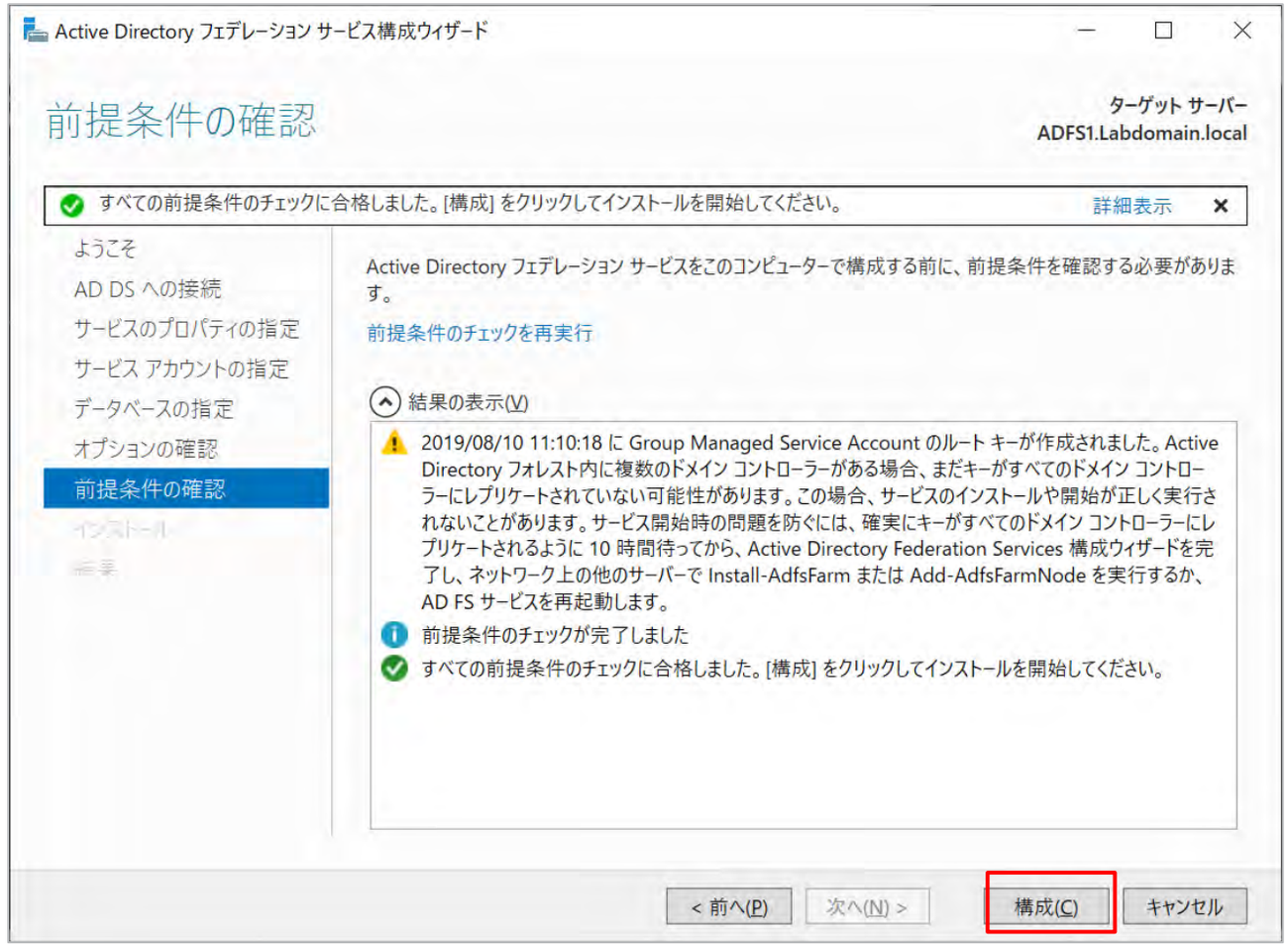
12. 「次へ」をクリックします。

4.5. フェデレーション 設定



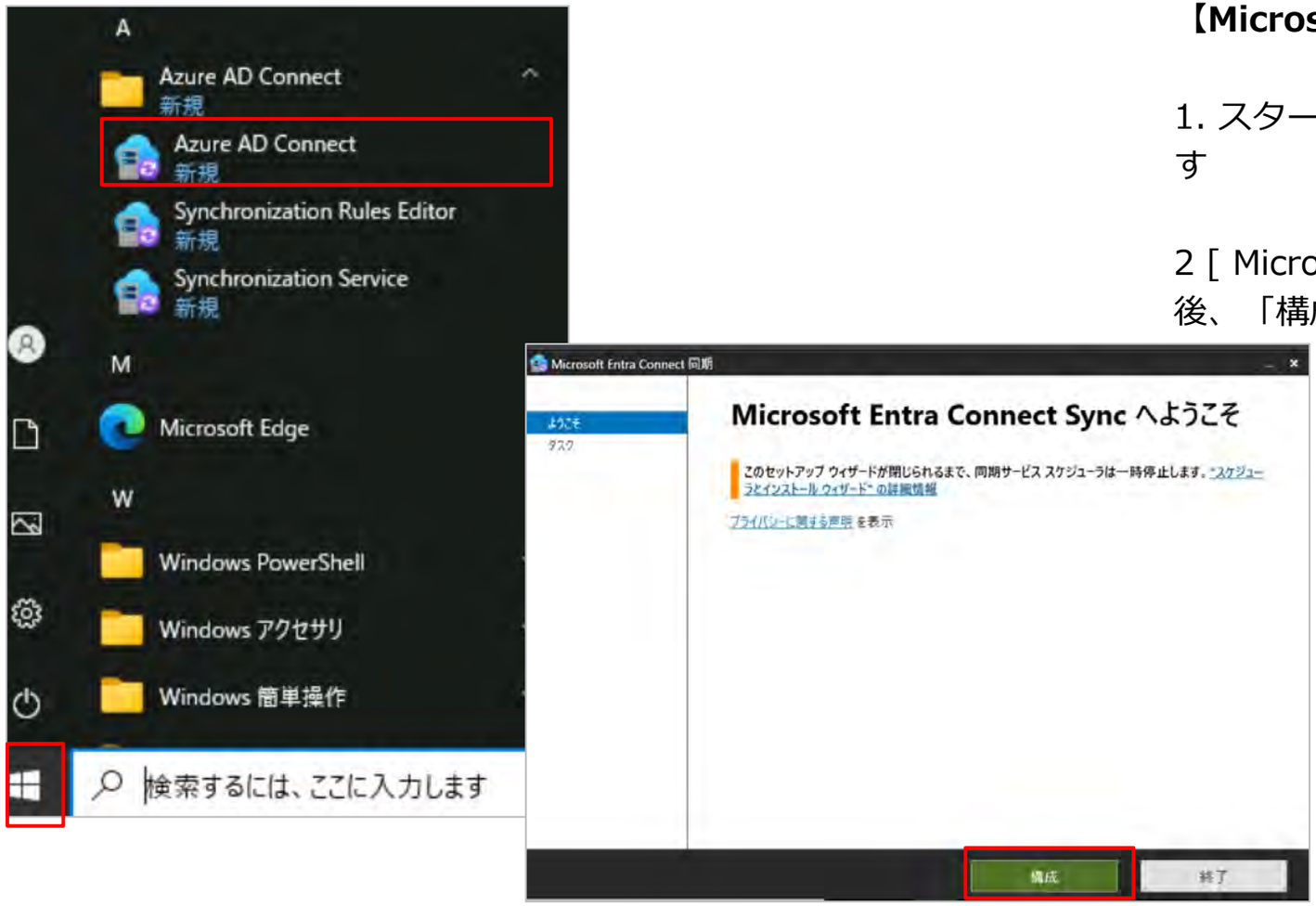
13. 「次へ」をクリックします。

4.5. フェデレーション 設定



14. 「構成」をクリックし、完了です。

4.5. フェデレーション 設定

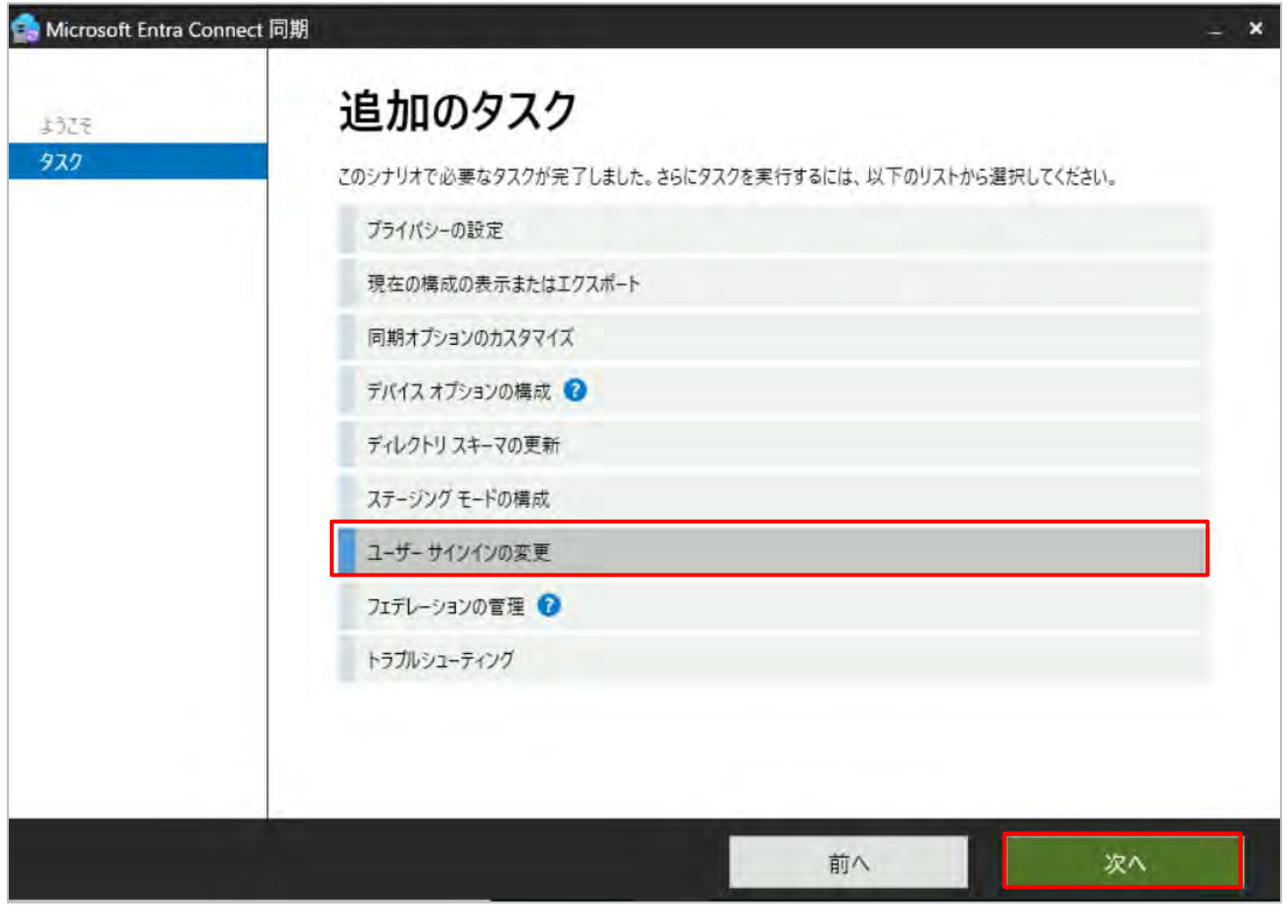


【Microsoft Entra Connect での設定】

1. スタートボタンから [Azure AD Connect] をクリックします

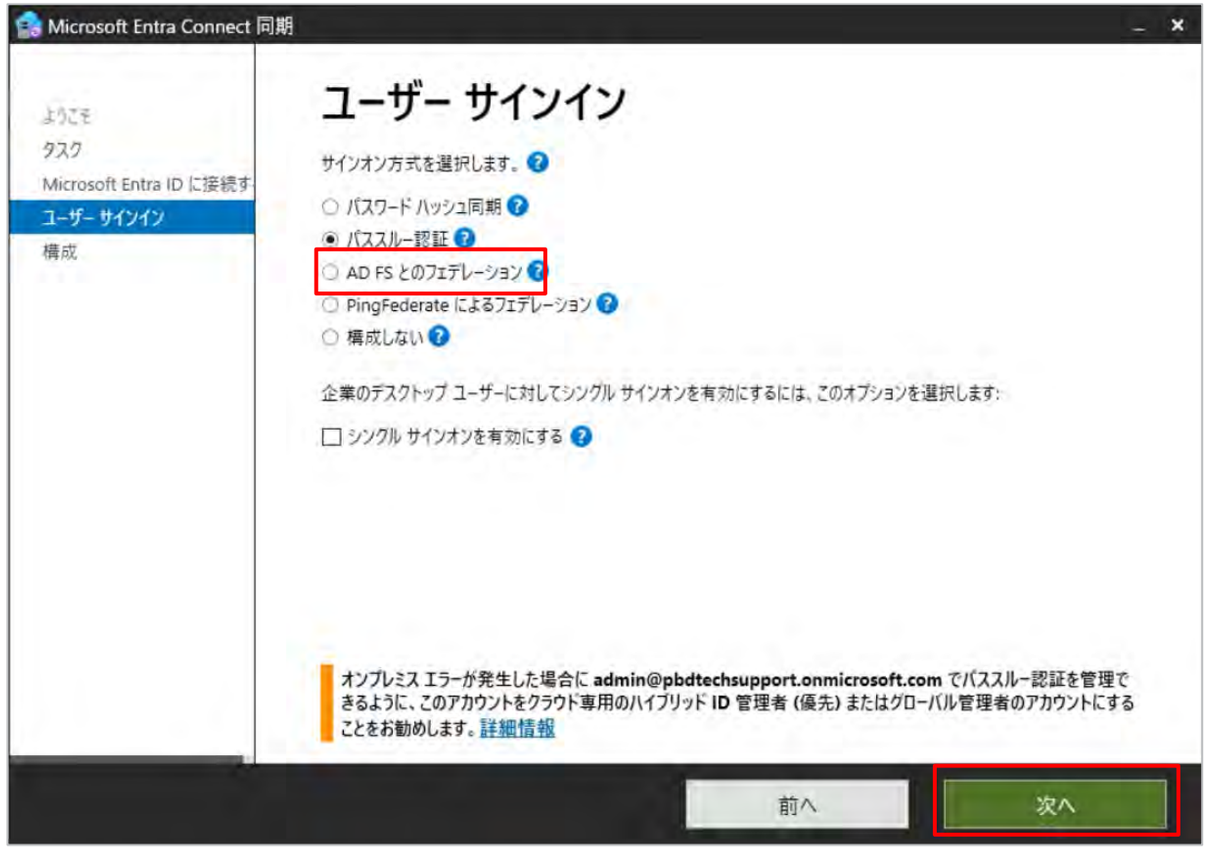
2 [Microsoft　Entra Connectへようこそ]という表示された後、「構成」をクリックします

4.5. フェデレーション 設定



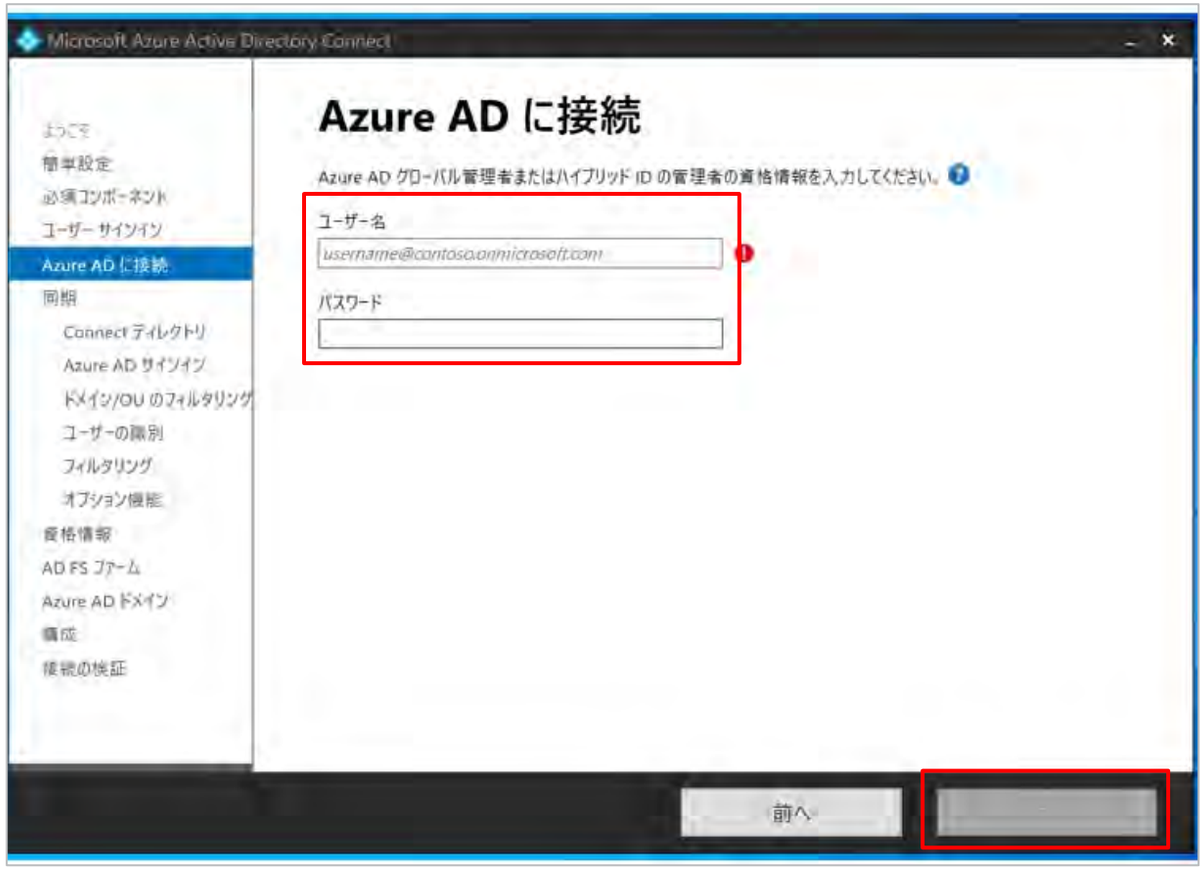
3. 「タスク」 > 「ユーザーサインインの変更」を選択し、「次へ」をクリックします。

4.5. フェデレーション 設定



4. 「AD FSとのフェデレーション」を選択し、「次へ」をクリックします。

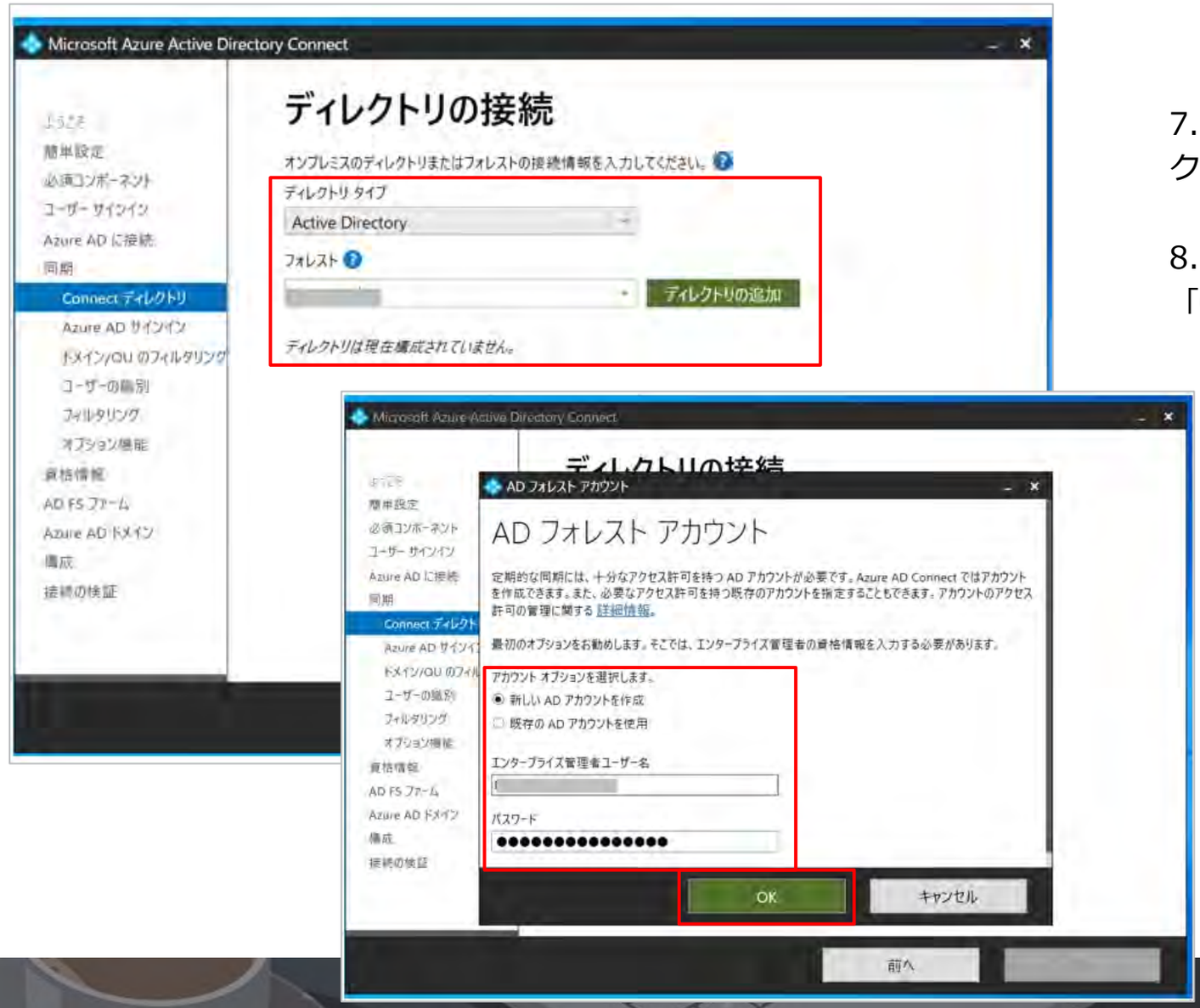
4.5. フェデレーション 設定



5. Entra IDのユーザ情報を入力し、「次へ」をクリックします。必要なロールは、グローバル管理者またはハイブリッドIDの管理者です。

6. ポップアップで、「アカウントにサインイン」が出てきますので、必要情報を入力します。

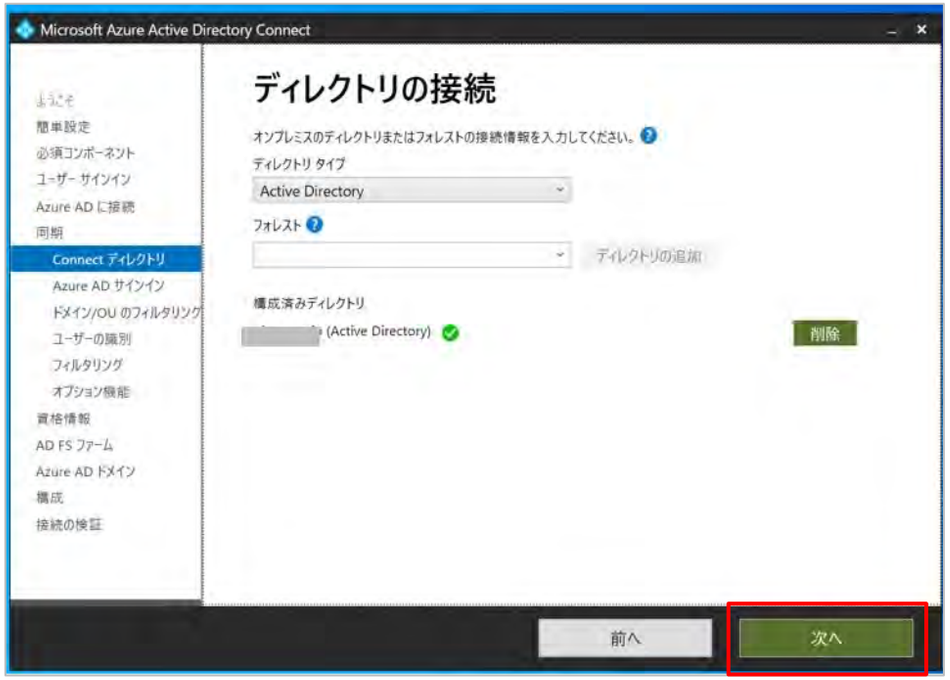
4.5. フェデレーション 設定



7. 対象となるドメイン名をフォレストの欄に入力し、「ディレクトリの追加」をクリックします。

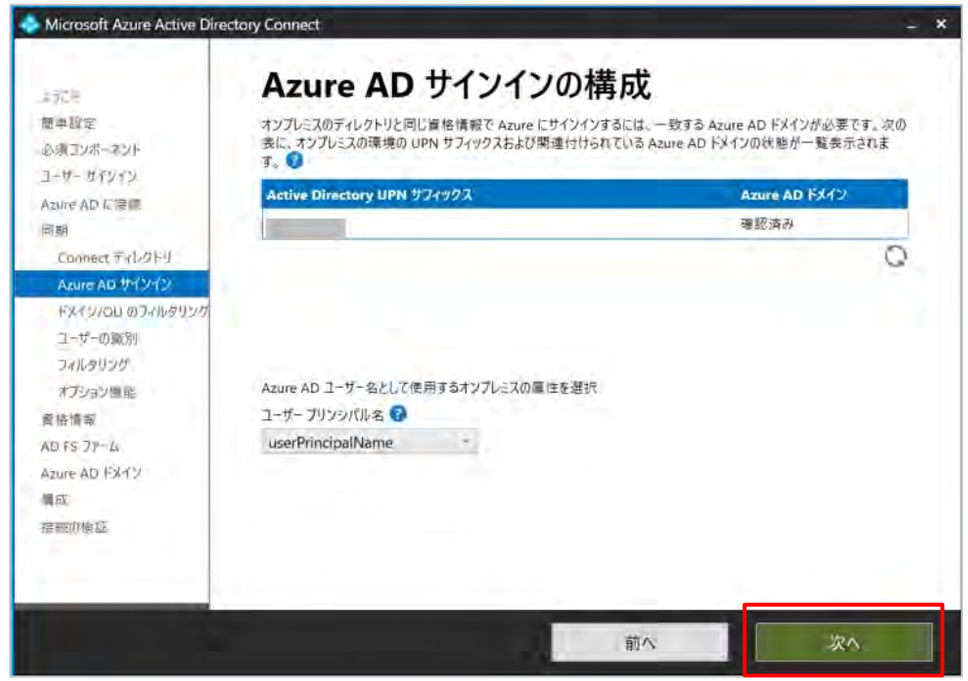
8. Enterprise Adminの権限を有したアカウント情報を入力し、「OK」をクリックします。

4.5. フェデレーション 設定

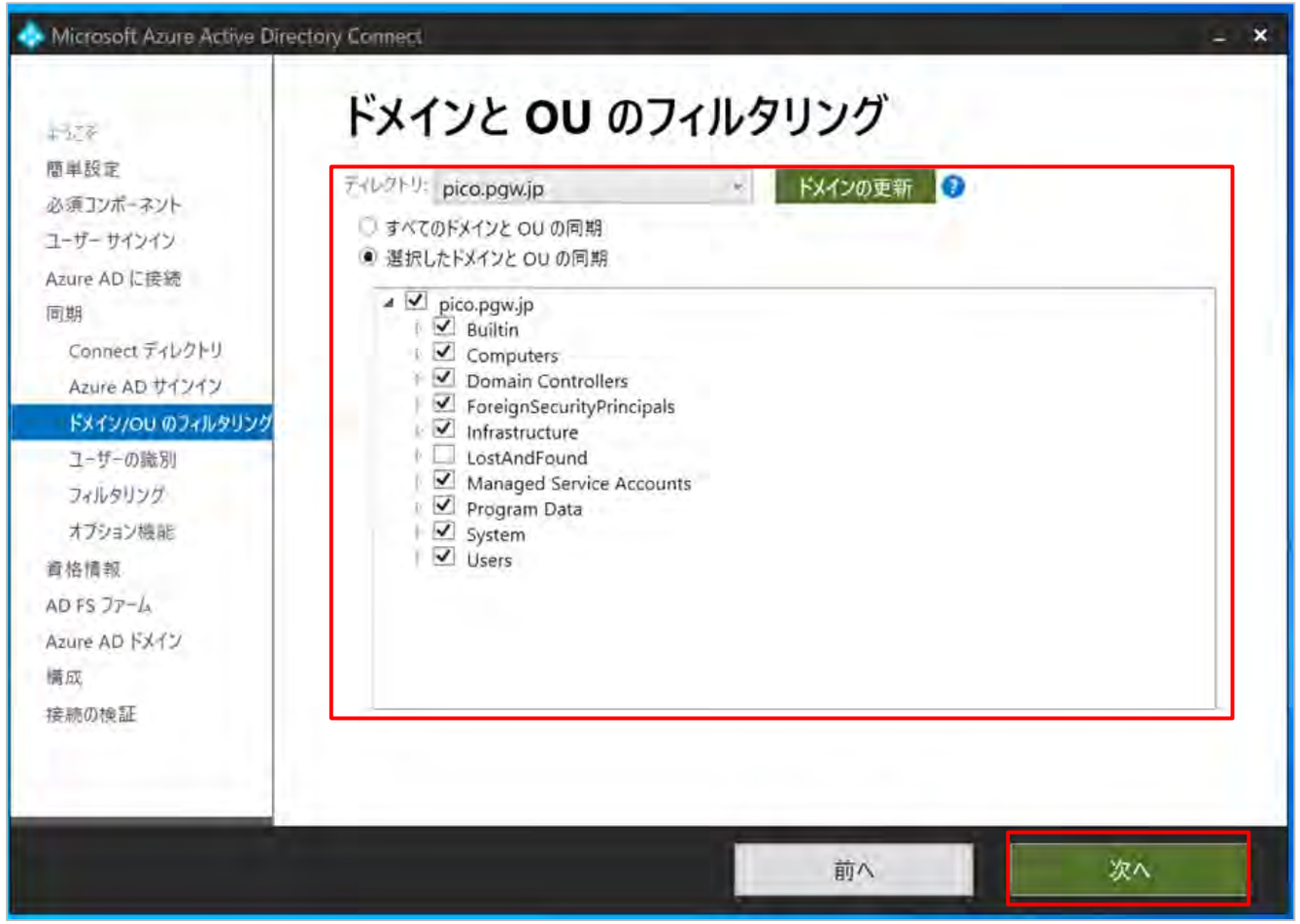


9. 構成済みディレクトリが追加されたことを確認して、「次へ」をクリックします。

10. そのまま「次へ」をクリックします。

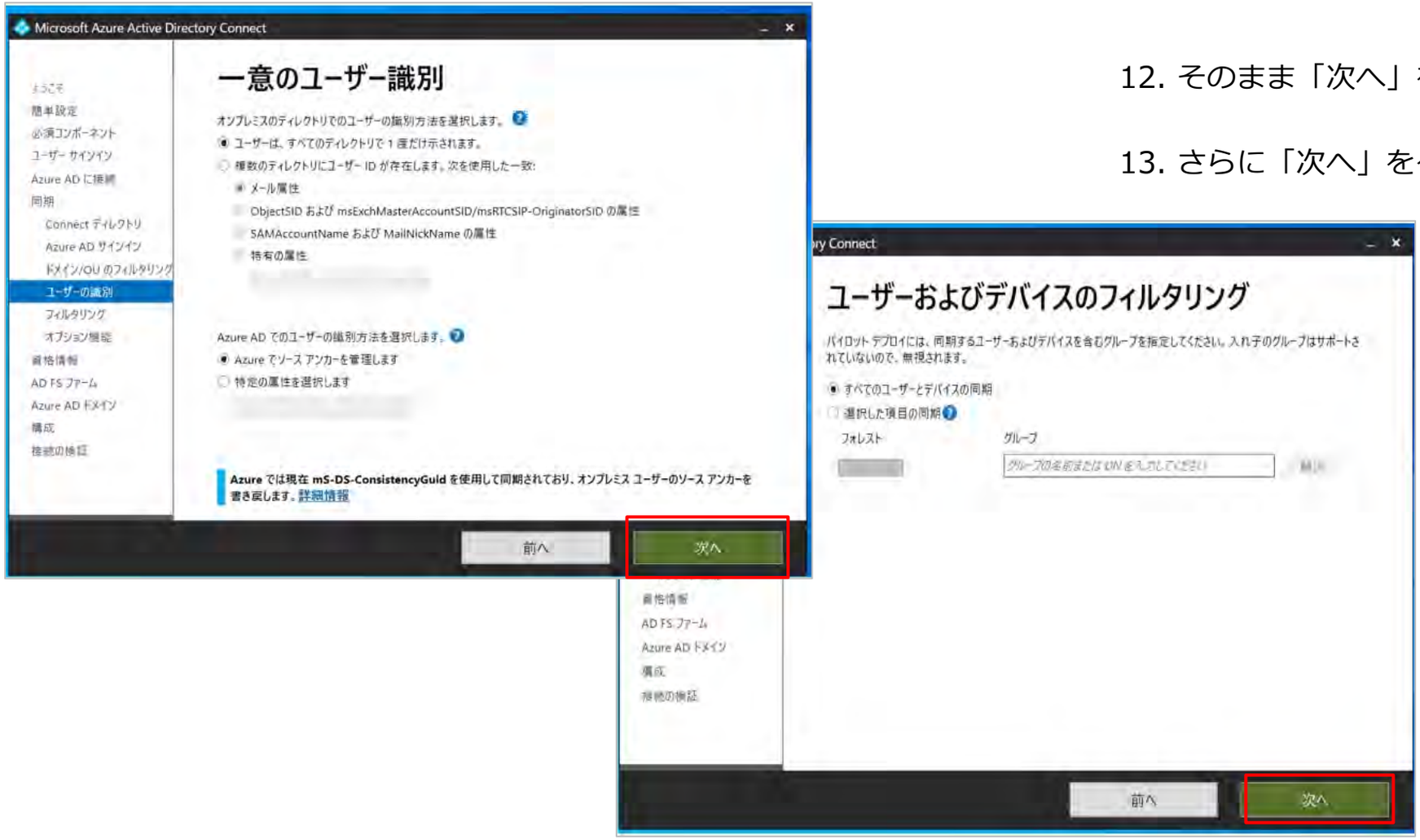


4.5. フェデレーション 設定



11. ADから Microsoft Entra IDに同期させる対象となるドメインとOUを指定し、「次へ」をクリックします。

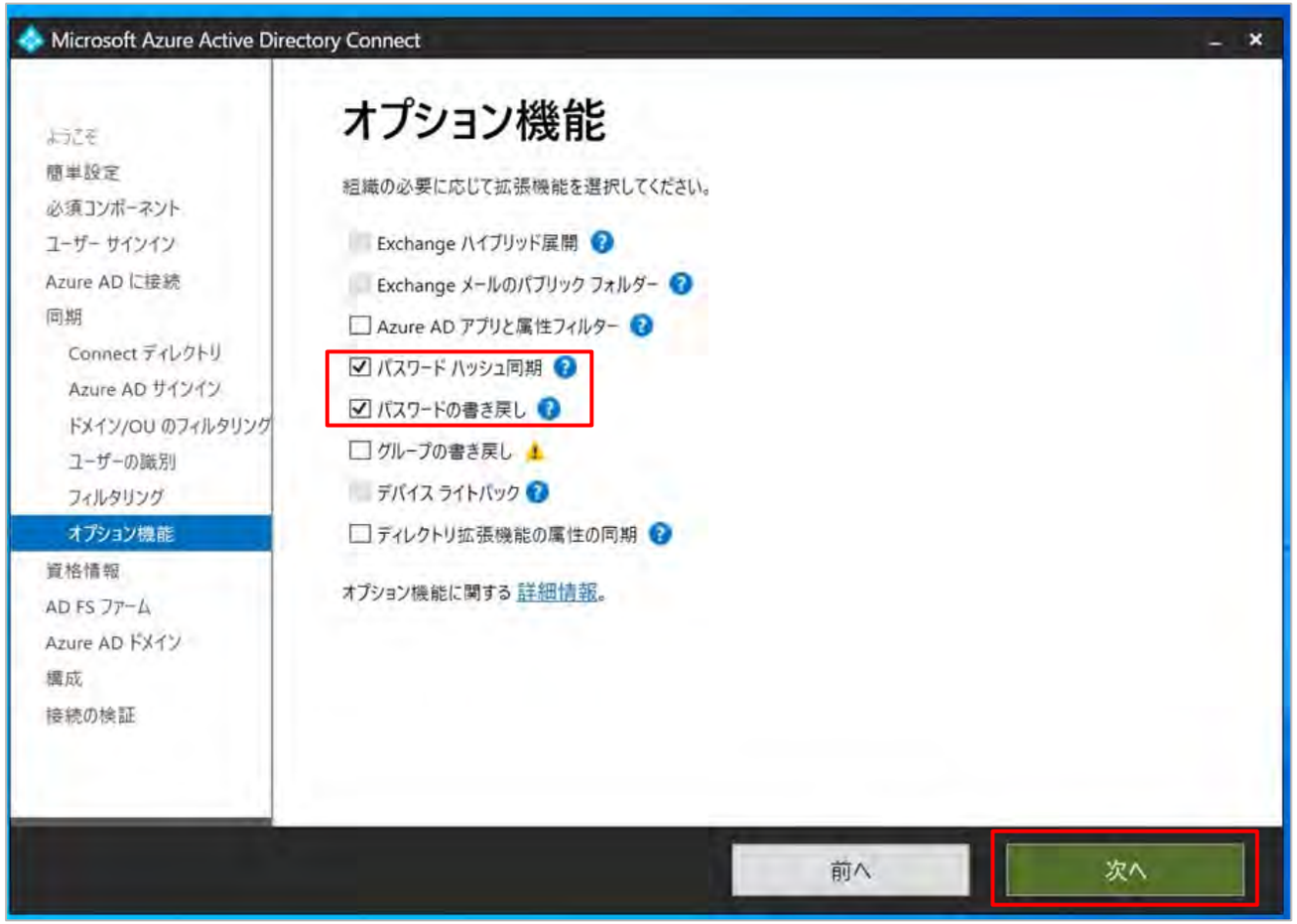
4.5. フェデレーション 設定



12. そのまま「次へ」をクリックします。

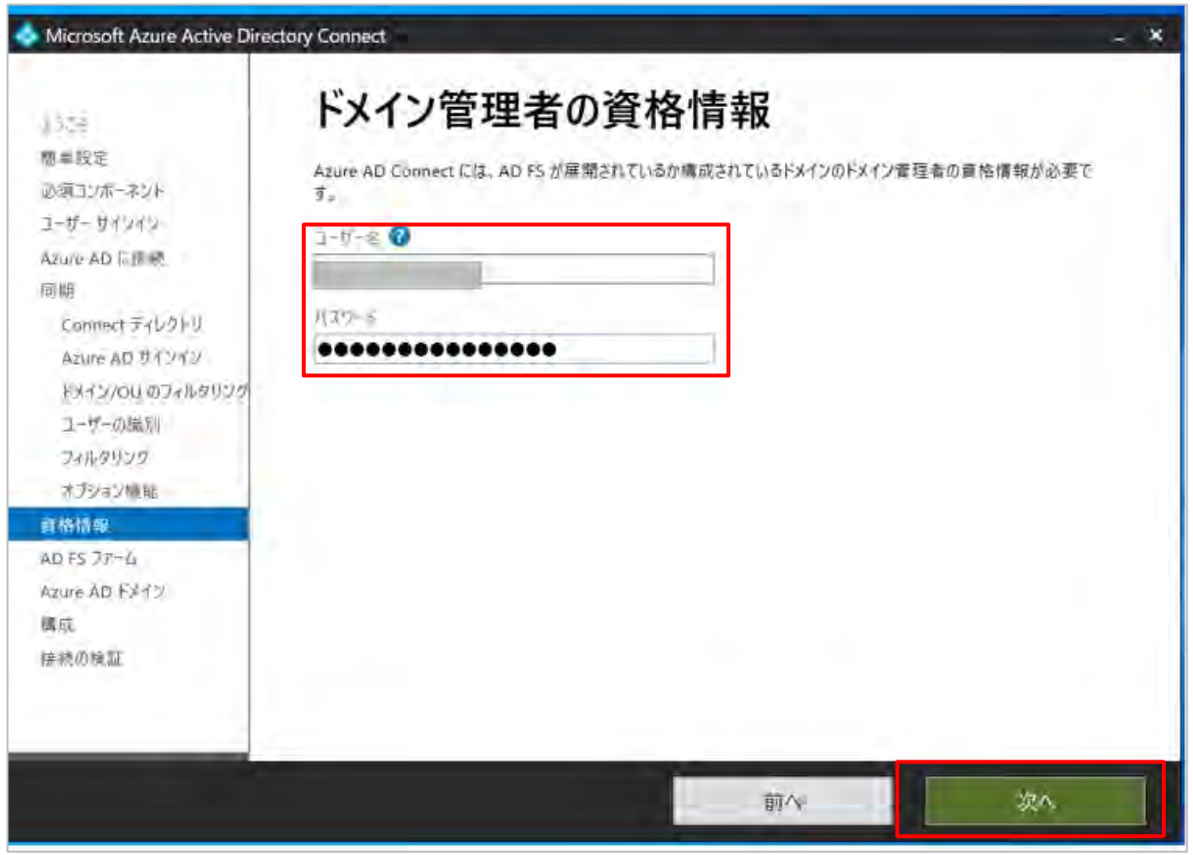
13. さらに「次へ」をクリックします。

4.5. フェデレーション 設定



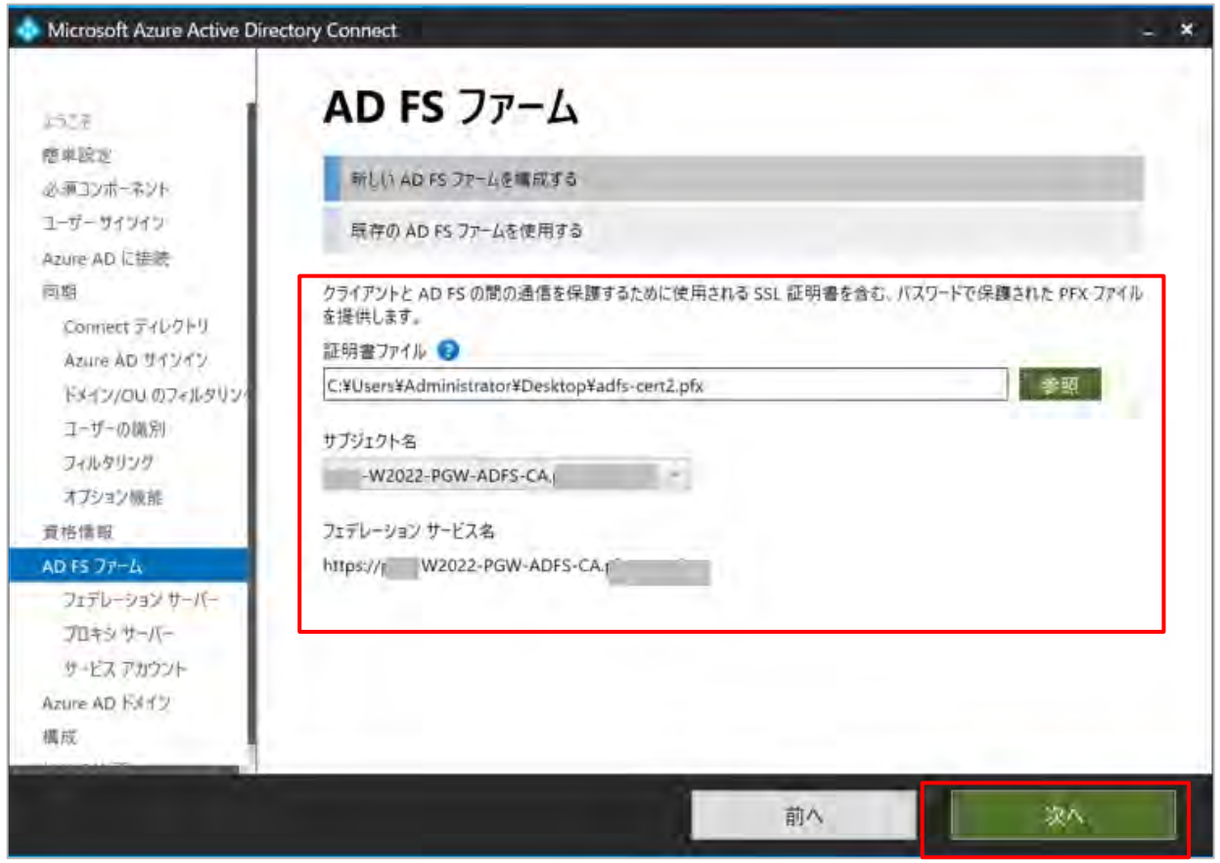
14. 「パスワードハッシュ同期」と「パスワードの書き戻し」にチェックを入れ、「次へ」をクリックします。

4.5. フェデレーション 設定



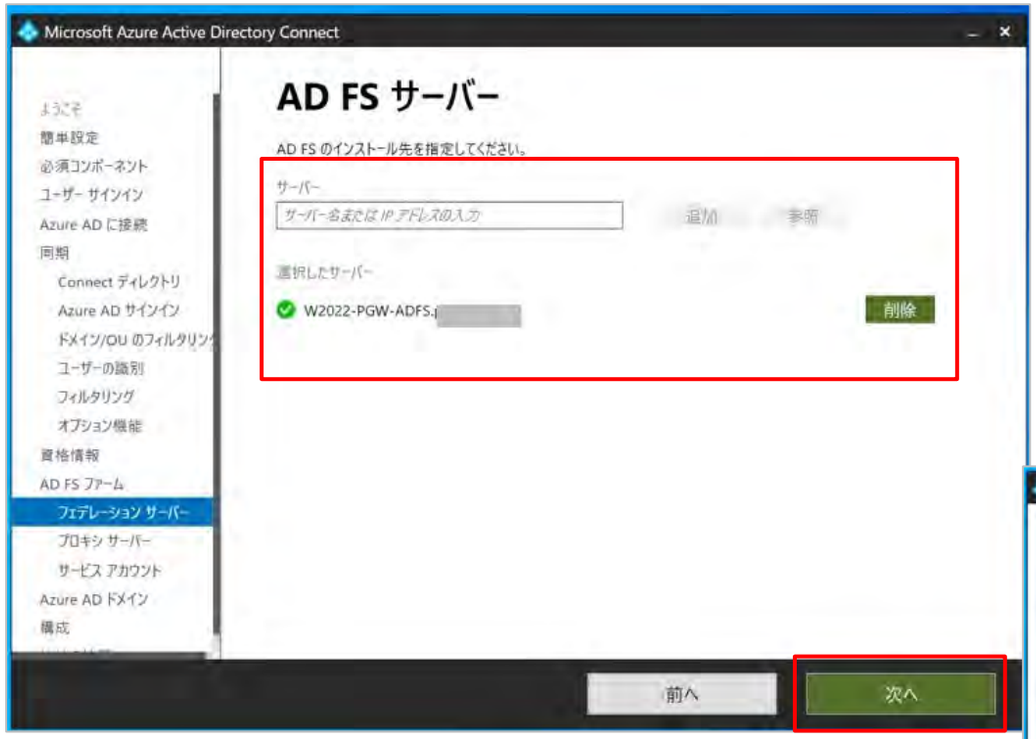
15. ドメイン管理者の資格情報を入力し、「次へ」をクリックします。

4.5. フェデレーション 設定



16. SSL証明書をアップロードし、「次へ」をクリックします。

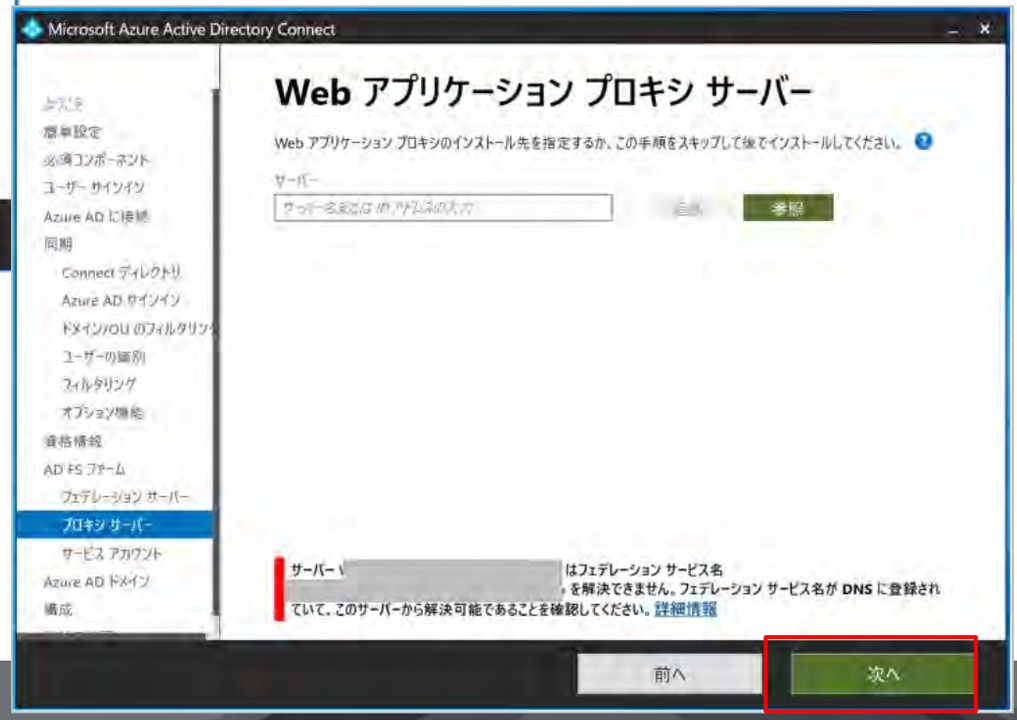
4.5. フェデレーション 設定



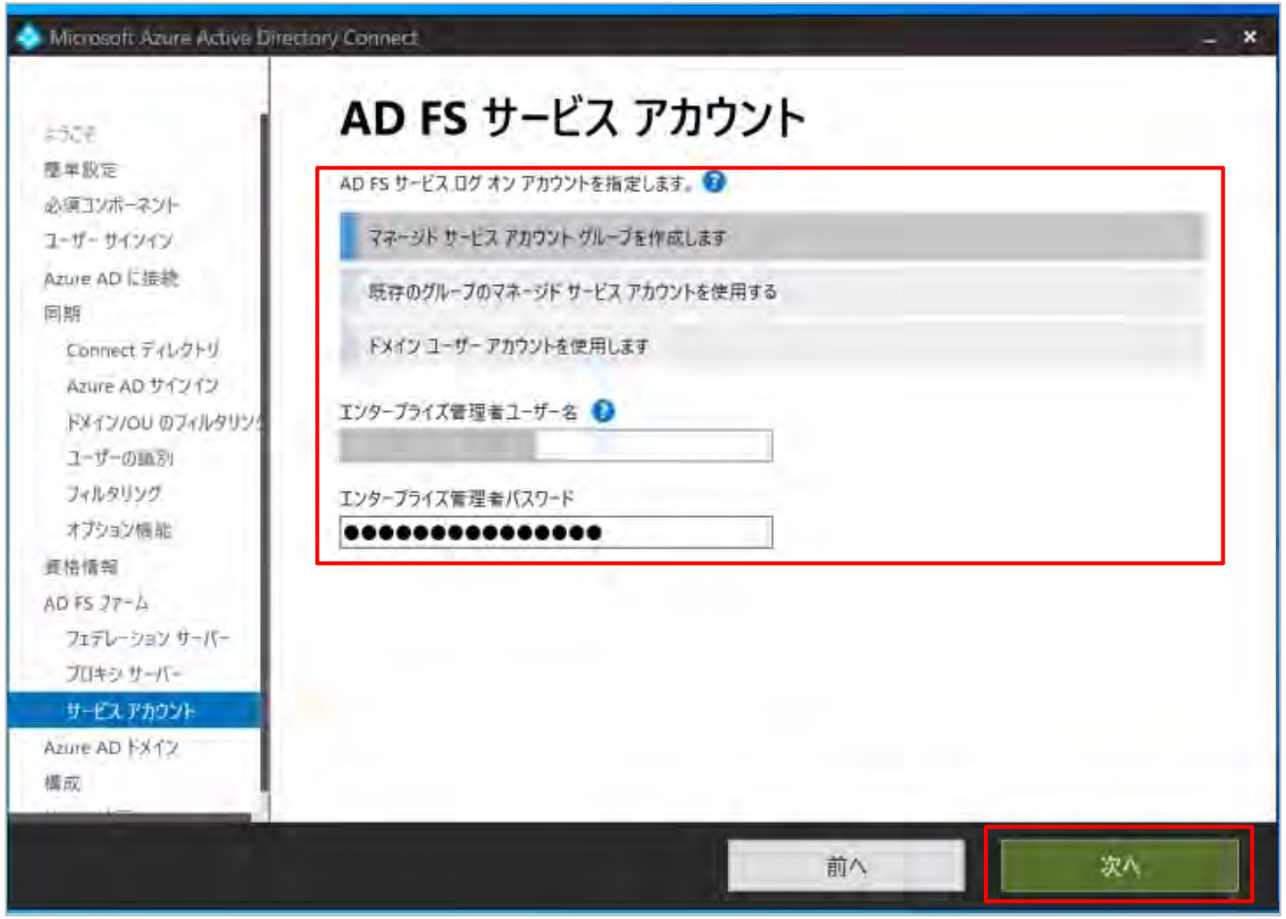
17. ADFSのFQDN情報、または、IPアドレスを入力します。
問題なければ、選択したサーバーに表示されます。

18. 「次へ」をクリックします。

19. そのまま「次へ」をクリックします。



4.5. フェデレーション 設定

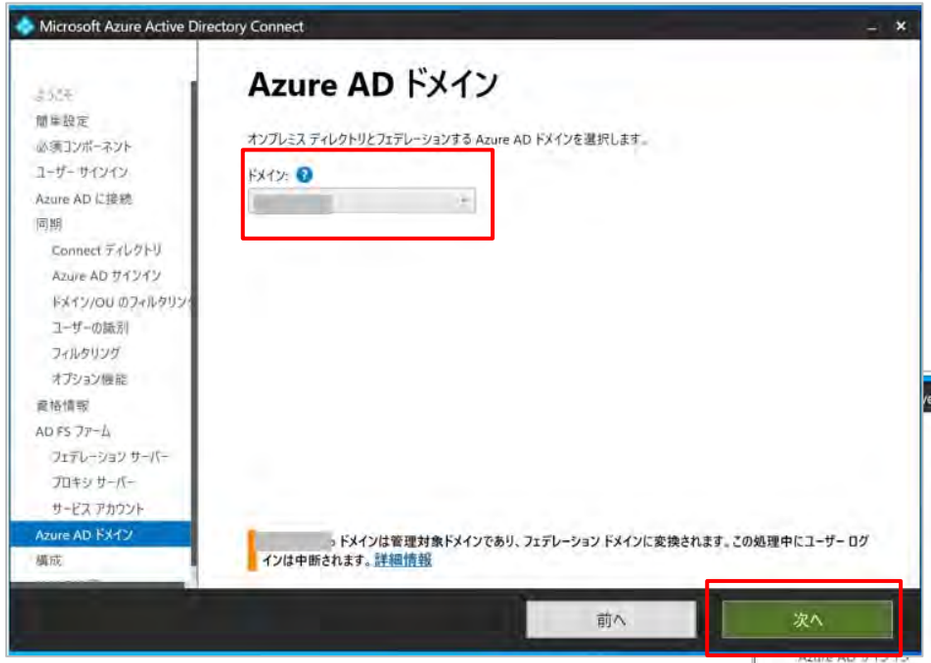


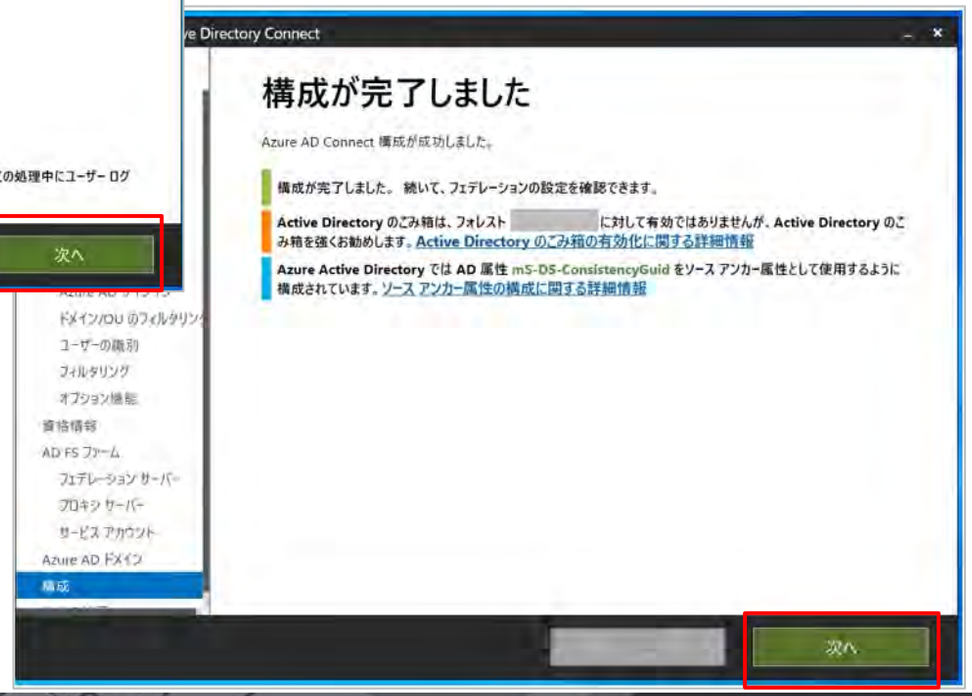
20. マネージドサービスアカウントを作成または既存のサービスアカウントを指定します。

複数のサーバーで動かすサービスに共通のサービスアカウントを使いたいときに使用します。
そのため、ここでgMSAを作るために、Enterprise Admins の資格をもつユーザの情報を入力します。

21. 「次へ」をクリックします。

4.5. フェデレーション 設定

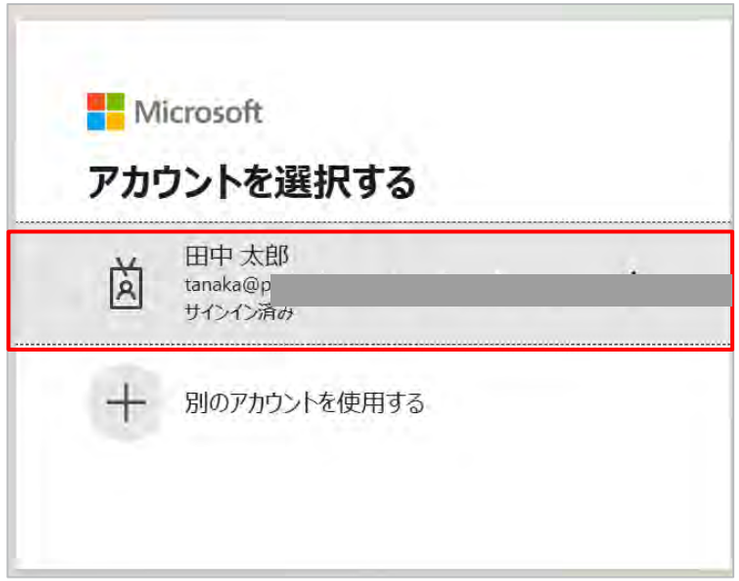




22. フェデレーションさせるドメインを選択し、「次へ」をクリックします。

23. 構成完了後、「次へ」をクリックすると完了です。

4.5. フェデレーション 設定



【作成したユーザーでサインイン】
同期したユーザーのパスワードで別サービスにサインインできるか確認します。

1. Microsoft Entra IDポータルへサインインします。

2. 前ページで作成したユーザーのアカウント/ パスワードを入力し、サインインできることを確認できます。

4.5. フェデレーション 設定

Microsoft社へ確認中

【サインインログ/ ○○ の確認方法】

設定した認証方式に基づいて、ユーザーが正常にサインインできているかを確認します。