【Microsoft Entra Connect】 同期・認証方式について

2025年2月28日



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. 設定手順
 - 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
- - 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



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



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

Cloud Support Center

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。



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。

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。

・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。

・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 \Rightarrow AD FS \Rightarrow 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



🖤 🙋 💽 🖬 🛄 🙆 📑 🚺 🗉		8		107	
Active Directory ユーサーとコンヒュー名前 ② 保存されたクエリ 鋼 ADtest.com > 🎬 Builtin	dmins pdateProxy	権類 セキュリティグループ - ドメイン ローカル セキュリティグループ - グローバル	説明 DNS Administrators Gro DNS clients who are per	へ 制御の委任(E) 検索(I)	
Computers	in Computers	セキュリティ グループ - グローバル	All workstations and ser	新規作成(N)	> コンピューター
Domain Controllers	in Controllers	セキュリティ グループ - グローバル	All domain controllers in	すべてのタス? (K)	> 連絡先
Users Users & Doma	iin Guests iin Users prise Admins prise Key Admins	セキュリティ グループ - グローバル セキュリティ グループ - グローバル セキュリティ グループ - ユニバーサル セキュリティ グループ - ユニバーサル	All domain guests All domain users Designated administrato Members of this group c	最新の債報 (更新(F) 一覧のエクスポート(L) 表示(V)	グループ InetOrgPerson msDS-KeyCredential
오 Enter 오 Group 오 Guest 운 Key A 호 MSOI	orise Read-only Domai o Policy Creator Owners dmins 7f65f7ac9c5d	セキュリティグループ - ユニバーサル セキュリティグループ - グローバル ユーザー セキュリティグループ - グローバル ユーザー	Members of this group a Members in this group c Built-in account for gue Members of this group c Account created by Mic	アイコンの整う(II) 等間隔に整う(E) ブロパティ(R) ヘルプ(H)	msDs-hesdurceruperyust msDs-ShadowPrincipalContainer msImaging-PSPs MSMQキューエイリアス ブリンター
4월 Prote 오 RAS a 오 Read 오 Scher 킹 Tech_ 3 Hett	cted Users nd IAS Servers only Domain Controll na Admins admin 77.72	ゼキュリティ クルーフ - クローバル ゼキュリティ クルーブ - ドメイン ローカル ゼキュリティ クルーブ - グローバル ゼキュリティ クループ - ユニバーサル ユーザー	Members of this group a Servers in this group can Members of this group a Designated administrato Built-in account for adm	域 ₁	2-ザ- 共有フォルダ- ① 管理状態

※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

23

4.1. ユーザー作成

6 作成先:	ADtest.com/Users				3. 「約 へ」を
姓(L):	田中	/=>			4. [ノ
る(r): フルネーム(A):	田中太郎	1-219/2010:]		了させ
ユーザー ログオン名(U): tanaka	æ	*	新しいオブ	ジェクト - ユーザー	
ユーザー ログオン名 (Wir 「¥	ndows 2000 より前)(W): tanak	xa	8	作成先: 4	ADtest.com/Users
	× 戻る(B	次へ(N) > キャン	パスワ- セル パスワ-	-ド(P): -ドの確認入力(C):	•••••
			-ב -ב- שולת תקת	ザーは次回ログオン時に ザーはパスワードを変更 (ワードを無期限にする(ロウントは無劾(O)	にパスワ−ド変更が必要(M) できない(S) W)
	× 戻る(B	次へ(N) > キャン	セル パスワー コユー ロユー ロノバス ロアカ	-ドの確認入力(C): ザーは次回ログオン時(ガーはパスワードを変更 ワードを無期限にする(ウントは無効(O)	 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・

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。

X

キャンセル

4.2. 同期ステータスの確認

Synchronization Service Manager

synchronization Service Manager on AzureVM File Tools Actions Help					-	×
Operations Operations Co	nnectors 🙀 Me	taverse Designer	A Metaverse Search			
Connector Operations						
Name Pro	ofile Name	Status	Start Time	End Time	1	 ^
ADtest.com Ex	port	success	2/27/2025 11:09:34 AM	2/27/2025 11:09:34 AM		 10
pbdtechsupport.onmic Ex	port	success	2/2//2025 11:09:23 AM	2/2//2025 11:09:33 AM		
pbdtechsupport.onmic De	elta Synchronization	success	2/27/2025 11:09:23 AM	2/27/2025 11:09:23 AM		
ADtest.com De	elta Synchronization	SUCCESS	2/2//2025 11:09:22 AM	2/2//2025 11:09:23 AM	1	
pbdtechsupport.onmic De	elta Import	success	2/27/2025 11:09:14 AM	2/27/2025 11:09:21 AM		
ADtest.com De	elta Import	success	2/27/2025 11:09:13 AM	2/27/2025 11:09:14 AM		
ADtest.com Ex	port	success	2/27/2025 10:51:10 AM	2/27/2025 10:51:10 AM		
pbdtechsupport.onmic Ex	port	success	2/27/2025 10:50:57 AM	2/27/2025 10:51:09 AM		
pbdtechsupport.onmic De	etta Synchronization	success	2/27/2025 10:50:57 AM	2/27/2025 10:50:57 AM		
ADtest.com De	elta Synchronization	success	2/27/2025 10:50:55 AM	2/27/2025 10:50:57 AM		
pbdtechsupport.onmic De	elta Import	success	2/27/2025 10:50:45 AM	2/27/2025 10:50:53 AM		
ADtest.com De	elta Import	success	2/27/2025 10:50:44 AM	2/27/2025 10:50:44 AM		
pbdtechsupport.onmic Ex	port	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。





【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。

Microsoft Entra Connec	t 同期	÷. ×
1925	追加のタスク	
920	このシナリオで必要なタスクが完了しました。さらにタスクを実行するには、以下のリストから選	見沢してください。
	プライパシーの設定	
	現在の構成の表示またはエクスポート	
	同期オプションのカスタマイズ	
	デバイスオブションの構成 2	
	ディレクトリスキーマの更新	
	ステージング モードの構成	
	ユーザー サインインの変更	
	フェデレーションの管理 🕜	
	トラブルシューティング	
	前へ	次へ

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. 「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。



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。

Microsoft Azure Active Direc	tory Connect _ X
55.2そ 部単設定 公面コンボーネント ローザー サインイン Azure AD に接続: 期間 Connect ディレクトリ Azure AD サインイン ドメイン/OU のフィルタリング コーザーの簡別 フィルタリング オブション/感聴 総括情報: DFS ファーム Szure AD ドメイン 職成: 義続の検証:	Standard Standard Sta
	ок <i>+</i> руель

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。



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。





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。





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。

Aure AD BY 742 Aure AD BY 7	Microsoft Azure Active Direction	tory Connect	- ×
<mark>自格情報</mark> AD FS ファーム Azure AD Fメイン 構成 接続の検証) 5.5-5 簡単設定 必須コンホーネント ユーザー サイソイン Azure AD 同世 晩 同期 Connect ディレクトリ Azure AD サインイン ドメイン/OU のフィルタリング ユーザーの場別 フィルタリング オ ディーン論師 	ドメイン管理者の資格情報 Azure AD Connect Cla, AD FS が雇用されているか構成されているドメインのドメイン管理者の資格情報が必要です。	
	蘇格情報 AD FS ファーム Azure AD Fメイン 構成 接続の検証		

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。


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。



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。

アカ	ウントを選択する	
Ř	田中 太郎	
M	サインイン済み	
+	別のアカウントを使用する	

【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ポータルヘサインインします

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

Microsoft Entra 管理センター		
佘 ホーム		TH 設定 EST_技術支援チーム検証用 サインアウト
✓ 新着情報	🕂 追加 🗸 🐯 テナントの管理 🚺 新着情報 🛛 🗟 プレビュー機能 🛛 🔗 フィードバックがある場	tanaka@
▶ 問題の診断と解決	 お使いのホームページで、エクスペリエンスを向上させるための取り組みが行われています。[フィードハンさい]。 	アカウントを表示
★ お気に入り	☆ 概要 監視中 プロパティ 推奨事項 セットアップガイド	
o ID	ヘ アナントの検索	(冬) 別のアカウントでサインインする
① 概要	基本情報	
A 7-4-		

Microsoft社へ確認中

【サインインログ/ 〇〇 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。



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。

≥ 管理者: Windows PowerShell (x86)

Windows PowerShell Copyright (C) Microsoft Corporation. All rights reserved. 新機能と改善のために最新の PowerShell をインストールしてください!https://aka.ms/PSWindows PS C:¥Users¥Tech_admin> Test-NetConnection -ComputerName login.microsoftonline.com -Port 443

ComputerName : login.microsoftonline.com RemoteAddress : 20.190.141.33 RemotePort : 443 InterfaceAlias : Ethernet SourceAddress : 10.0.0.4 TcpTestSucceeded : True

PS C:¥Users¥Tech_admin> Test-NetConnection -ComputerName login.microsoftonline.com -Port 80

ComputerName : login.microsoftonline.com RemoteAddress : 20.190.141.33 RemotePort : 80 InterfaceAlias : Ethernet SourceAddress : 10.0.0.4 TopTestSucceeded : True

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。



windows belender 771777 -10				- 0
	キュリティ > Windows Defender ファイアウォール	~	õ	
コントロール パネル ホーム	Windows Defender ファイアウォールに	13 PC	の保護	
Windows Defender ファイアウォー ルを介したアプリまたは機能を許可	Windows Defender ファイアウォールによって、ハッカ クを経由したアクセスを防止できるようになります。	ーまたは悪	意のあるソフ	トウェアによるインターネットまたはネット
通知設定の変更	V ドメイン ネットワーク(M)			接続されていません(
Windows Defender ファイアウォー しの有効化素たは無効化	♥ プライベート ネットワーク(R)			接続されていません(
設定値に戻す		-///0		接続这次(
詳細設定	9 7 XF3/CIA/()999 49F9	-9(P)		北京の小町の大
ネットワークのトラブルシューティング	空港、喫茶店など、公共の場のネットワーク			
	Windows Defender ファイアウォールの状態:	有效	5	
	著信接続:	許可	iされたアプリの ックする	の一覧にないアプリへのすべての接続
	アクティブなパブリック ネットワーク:	11	Network	
	通知の状態・	Min	dows Defen	der ファイアウォールボモー いアプリをつ

【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。

をクリックします。

🔗 セキュリティが強化された Window	ws Defender 7	ァイアウォール							- 🗆 X		
ファイル(F) 操作(A) 表示(V)	ヘルプ(H)										
🗢 🔿 🖄 🔂 📆 🔂 🔂 🖬	1 TEOHR								10.15	3.	「受信の規則」>「新しい規則」をクリックします
 <u>□ − ¬ル □ 2/2 − </u>∂[−] 0 ℓ² + 1)[−] <u>□ 受信の規則</u> <u>□ 支信の規則</u> <u>□ 支信の利用</u> <u>□ 支信の規則</u> <u>□ 支信の利用</u> <u>□ 支信の</u> <u>□ 支信の</u> <u>□ 支信の</u> <u>□ 支</u>	f) 受信の規則 fレクサー(T (-(RTCP (-(RTCP (-(RTCP (-(RTCP (-(RTCP (-(RTCP))))) 求 - ICMR 受信)) 受信) MPv4 受信 (MPv6 受信) (TCP 受信)	 グルーブ スタート ソフトウエア ロード パランサー デスクトップ アブリ Web ビューアー デスクトップ アブリ Web ビューアー デパイス キャスト機能 デパイス キャスト機能 デパイス キャスト機能 パフォーマンス ログと警告 パフォーマンス ログと警告 パフォーマンス ログと警告 パフォーマンス ログと警告 アイルとプリンターの共有 リモート デスクトップ ルーディングとリモート アクセス 仮想マシンの監視 分散トランザクション コーディネー・ 	プロファイル ドメイン、ブラ すべて すべて ドメイン ブライベート パブリック ドメイン ブライベート, すべて すべて すべて すべて すべて	有はいははははいいたえいいいはいいいはいいいはいいいはいいいはいいいはいいいいはないいいいたえ お 作	操許許許許許許許許許許許許許許許許許許許許許許許許許許許許許許許許。 、 、 、 、 、 、 、 、 、 、 、 、 、	使いいいいいいいいいいいいいいいいいいいいいいいいいいいいいいいいいいいい	プログラム 任意 %System 任意 任意 %System %System %system %system System 規則ウィザー	ローカルア 任任 任任 任任 任任 任任 任任 任任 任任 任任 任	操作 学(信の規則) 新しい規則 マ ブロファイルでフィルタ- マ 状態でフィルタ- マ が、総でフィルタ- 表示 会 最新の情報に更新 テ つ覧のエクスポート マ ヘルブ れしてください。	4.	「犬ート」を選択し、「次へ」をクリックします。
	• <	職場または学校アカウント	ドメイン, ブラ	ر ال ال ال	テップ: 規則の利	種類	40_L	٤	ごの種類の規則を作成しますか?		
					プロトコノ 操作 プロファイ	()L	W-F	C) プログラム(P) プログラムの接続を制御する規則です。		
				•	名前			۲	 ボート(O) TCP または UDP ボートの接続を制御する規則 	です。	
								C) 事前定義(E):		
									Active Directory Domain Services		
									Windows エクスペリエンスのために接続を制御す	る規則です。	0
								C) カスタム(C) カスタムの規則です。		

● 新規の受信の規則ウィザート			×
プロトコルおよびポート			
この規則を適用するプロトコルとポ	ートを指定してください。		
えテップ:			
規則の種類	TCP と UDP のどちらにこの規則を適	用しますか?	
プロトコルおよびポート	TCP(T)		
● 操作	O UDP(U)		
 プロファイル 			
• 名前	すべてのローカル ボートと特定のロー てください。 〇 すべてのローカル ボート(A)	カル ポートのどちらを対象にこの規則を適用するかを選択し	
	◉ 特定のローカル ポート(S):	443,80	
		例: 80、443、5000-5010	
			_

- 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。

X

新規の受信の規則ウィザード 名前 この規則の名前と説明を指定してくださ(10		×	9. 「名 (例:	前」 PTA	を) 用7	入力 ポー	し、完了です ト開放)
ステ ゥフ: 規則の種類 プロトコルおよびポート 操作 プロファイル 名前	名前(N): パススルー認証用443,80ポート開放		1	10. —	覧で	「許	F可」	になってい
	説明 (オプション)(D): 	 	wws Defender ファイアウォール ヘルブ(H) そイ 受信の規則 全前 ④ Active Directory ドメイン コントローラー - SAM ● Active Directory ドメイン コントローラー - SAM	グルーブ Active Directory Domain Ser Active Directory Domain Directory Domain QUIC でのフィイルとフリンターの Secure Socket トンネリングブ AD ES	プロファイル すべて すべて すべて すべて すべて すべて	有効はい	操作 許可 許可 許可 許可 許可	- □ 操作 実像の規則 総 新しい規則 マ プロファイルでフィルター マ 状態でフィルター マ グループでフィルター
			A Drs n n b s) = CA ((CP 受信) ④ Active Directory ドメイン コントローラー - LDA ネットワーク探索 (WSD 受信) ホットワーク探索 (Pub WSD 受信) BranchCache ビア捜出 (WSD-受信) リモート デスクトップ - ユーザー モード (UDP 受信) リモート デスクトップ - ユーザー モード (TCP 受信) ○ Active Directory ドメイン コントローラー - グロ. ホットワーク探索 (UPnP 受信) ○ デバイス キャスト UPnP イベント (TCP 受信) > <	A Stive Directory Domain Ser A Active Directory Domain Ser ネットワーク探索 BranchCache - ビア検出 (WS リモート デスクトップ (WebSocket) リモート デスクトップ リモート デスクトップ リモート デスクトップ リモート デスクトップ レート デスクトップ Active Directory Domain Ser ネットワーク探索 デバイス キャスト機能	ッハン すべてて すべてて すべてて すべてて すべてて すべてて すべてて すべて	いいん いいん いいん いいい いいい いいい いいい いいい いいいい い	计操作计算计算符 计算机	 表示 ● 景新の情報に更新 ● 一覧のエクスポート ○ ヘルブ パススル-認証用443,80ポート構故 ● 規則の無効化 ↓ 切り取り ○ コピー ※ 削除 ③ ブロパティ ② ヘルブ

完了です。 開放)

こなっていることを確認します。

- 🗆 X

.



【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。



se Microsoft Entra Connect 同期		~
ようごそ 簡単設定 必須コンポーネント ユーザー サインイン	必須コンポーネントのインストール このコンビューターでは既存の同期サービスが検出されませんでした。Microsoft Entra Connect Sync サービスがインストー ルされます。 ?	
»	 ✓ カスタム インストール先を指定する インストール場所 C:¥Program Files¥Microsoft Azure AD Sync ● 既存の SQL Server を使用する □ 既存のサービス アカウントを使用する □ カスタム同期グループを指定する □ 同期設定をインボート 	
	前へ	インストール

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. 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。

R Microsoft Entra Connect 同期		- ×
	Microsoft Entra ID に接続する Microsoft Entra ID ハイブリッド ID の管理者 (優先) またはグローバル管理者の真格情報を入力してください。 ユーチー&* Istmin@pbdtechsupport.onmicrosoft.com	
	前へ 次へ	

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。



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。

Microsoft Entra Connect 同期		
ようごそ 簡単設定 必須コンポーネント ユーザー サインイン Microsoft Entra ID に接続す 同期 <u>Connect ディレクトリ</u> Microsoft Entra サインイン ドメイン/OU のフィルタリンク >> ユーザーの時間	ディレクトリの接続 オンプレミスのディレクトリまたはフォレストの接続情報を入力してください。 ディレクトリ タイプ Active Directory ADtest.com ディレクトリは現在構成されていません。	8. [新しいA エンタープラ
- パルラリング オプション機能 構成	AD フォレスト アカウント AD フォレスト アカウント AD フォレスト アカウン 定期的な同期には、十分なアクセス許可を持つ AD はアカウントを作成できます。また、必要なアクセス許 トのアクセス許可の管理に関する 詳細情報。 最初のオプションをお勧めします。そこでは、エンタープ アカウント オプションを選択します。	ノト のアカウントが必要です。Microsoft Entra Connect Sync で 可を持つ既存のアカウントを指定することもできます。アカウン ライズ管理者の資格情報を入力する必要があります。
	 新しい AD アカウントを作成 既存の AD アカウントを使用 エンターブライズ管理者ユーザー名 パスワード 	
		OK キャンセル

~ >

クトリの追加」をクリックします。

ADアカウントを作成]を選択し、 ライズ管理者ユーザー名、パスワードを入力します。

202そ	ディレクトリの接続		
ー 必須コンボーネント ユーザー サインイン	オンプレミスのディレクトリまたはフォレストの接続情報を入力してくたさい。 🍞 ディレクトリ タイプ Active Directory		
Microsoft Entra ID に使成9 同期 Connect ディレクトリ	フォレスト 🕢		
Microsoft Entra サインイン ドメイン/OU のフィルタリング ユーザーの識別 フィルタリング	構成済みディレクトリ ADtest.com (Active Directory) 🥑	削除	
オプション機能 構成			
		***	100

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 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。

딇 Microsoft Entra Connect 同期			
\$727	Microsoft Entra サイン	インの構成	
簡単設定 必須コンポーネント	オンプレミスのディレクトリと同じ資格情報で Azure にサインイン です。 次の表に、オンプレミスの環境の UPN サフィックスおよび型 一覧表示されます。 😯	するには、一致する Microsoft Entra ID ドメインが必要 見運付けられている Microsoft Entra ドメインの状態が	
ユージー リインイン Microsoft Entra ID に接続す	Active Directory UPN サフィックス	Microsoft Entra ID ドメイ ン	
同期	adtest.com	追加されていません 🕢	
Microsoft Entra サインイン ドメイン/OU のフィルタリンク ≫ ユーザーの識別 フィルタリング オプション機能 構成	Microsoft Entra ID ユーザー名として使用するオンプレミスの属 ユーザー プリンシバル名 ② userPrincipalName	Q 性を選択	
	✓ 一部の UPN サフィックスが確認済みドメインに一致してい UPN サフィックスが検証済みのドメインと一致してい場合、 Microsoft Entra ID にサインインできなくなります。詳細情	なくても統行する ユーザーはオンプレミスの資格情報を使用して <u>青報</u>	
		前へ	次^

■ 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。

ようごそ 簡単投記 が高コンポーキンド コーガー サインイン Microsoft Entra iD に接続す 同期 Commet ディレクトリ	ドメインと OU のフィルタリング Frit PH: ADtest.com - ドメインの更新 ② ・ To ZONK4/16 OU の原料 ③ 選択したドメインと OU の原料 ・ S ^A ADtest.com	
Microsoft Entra サインイン ドイインパロ シオトシリング ユーザーの運動 フィルクリング オプション場話 構成		
		前へ 次へ

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。



B Microsoft Entra Connect 同期		and the second strength of the		*
 Microsoft Entra Connect 同期 ようごモ 簡単段定 必須コンボーネント ユーザー サインイン Microsoft Entra ID に接続す 同期 Connect ディレクトリ Microsoft Entra サインイン ドメイン/OU のフィルタリング ユーザーの識別 フィルクリング オブション機能 構成 	ユーザーおよ バイロット デブロイには、同 れていないので、無視されま ④ すべてのユーザーとデバイ 〇 選択した項目の同期 フォレスト ADtest.com	はびデバイスのフィルタリング 約するユーザーおよびデバイスを含むグループを指定してください。入れう ます。 (スの同期 クループ グループ グループの名前または DN を入力してください)	-のクルーフはサポートさ 解決	
			前へ	次へ

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。

必須コンポーネント ユーザー サインイン Microsoft Entra ID に接続す 同期 Connect ディレクトリ Microsoft Entra ID に接続す Connect ディレクトリ Microsoft Entra サインイン ドメイン/OU のフィルタリンク レインクー 「ハッシュ同期 ② コーザーの観別 フィルクリンク オブション機能に関する 評細情報。	ようこそ 簡単設定	オプション機能	
(回)府 □ // Connect ディレクトり Connect ディレクトリ □ // スワード ハッシュ回期 ② Microsoft Entra サインイン □ // スワード ハッシュ回期 ③ ドメイン/OU のフィルタリング □ // スワード の書き戻し ④ ユーザーの取別 □ デバイス ライトバック ② フィルクリング □ ディレクトリ拡張機能の属性の同期 ③ オブション機能に関する 詳細情報。	◎ 〒 = ×××E 必須コンポーネント ユーザー サインイン Microsoft Entra ID に接続す	組織の必要に応じて拡張機能を選択してくたさい。 Exchange ハイブリッド展開 Exchange メールのパブリック フォルダー コ	
(編) オブション機能に関する <u>詳細情報</u> 。	 同期 Connect ディレクトリ Microsoft Entra サインイン ドメイン/OU のフィルタリンク ユーザーの頭別 フィルタリング オブション機能 	 Microsoft Entra ID アプリと属性フィルター ② ✓ パスワード ハッシュ同期 ③ □ パスワードの書き戻し ③ □ グルーブの書き戻し ▲ □ デバイス ライトバック ② □ ディレクトリ拡張機能の属性の同期 ② 	
	96702	オプション機能に関する <u>詳細情報</u> 。	

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。



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。



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。

M	icrosoft Entra 管理センター	21	Jソース、サービス、ドキュメントの検索 (G+/)			
^ "	ホーム 新着情報	*	^{π−Δ >} Microsoft Entra Connect	-		
	問題の診断と解決		🗙 トラブルシューティング 🕐 更新 🛛 🗔 プレビ	ユー機能	フィードバックがある場合	
*	お気に入り	~	ここをクリックして、改良された新しい Microsoft Ent ベッロックのフィー・マーマー・マーマー・マー・マー・マー・マー・マー・マー・マー・マー・マー・マ	ra Connect エクス	ペリエンスをお試しください。 →	
•	ID	~	Microsoft Entra クラウド同期の管理 Microsoft Entra Connect 同期			
0	概要		同期状態	有効		
8	ユーザー	\sim	最後の同期	1 時間前		
°x°	グループ	\sim	バスワード ハッシュの同期	有効		
8	デバイス	\sim	ユーザー サインイン			
æ	マプリケーション	×	コ フェデレーション	無効	0 ドメイン	
щ 0	アノリソーション	~	シームレスなシングル サインオン	無効	0 ドメイン	
8	保護	\sim	パススルー認証	有効	2 件のエージェント	
	Identity Governance	\sim	証明書ベースの認証	無効		
-0-			代替ログイン ID として電子メールを送信する	無効		

【Entra管理ポータルにて同期設定確認】

1 <u>Microsoft Entra IDポータル</u>ヘサインインします。

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。

Microsoft Entra 管理センター	♀ リソース、サービス、ドキュメントの検索 (G+/)			🧔 Cc
 ☆ ホーム ✓ 新着情報 図 問題の診断と解決 	ホーム > Microsoft Entra Connect > パススルー認証 … Microsoft Entra ID ↓ ダウンロード ② トラブルシューティング ◯ 最新の情報に更新			
★ お気に入り	 ・ テナントで少なくとも3つの認証エージェントが実行されていることをお勧めします。 ・ 詳細情報 口 			
 ▶ ID ① 概要 	へ 認証エージェント IP	状態		
R ユーザー	V AzureVM.ADtest.com		0	

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。

Microsoft Entra 管理センター	21	リソース、サービス、ドキュ	メントの相	续 (G+/)					🧔 Copilot	0 @ 0 A	admin@nbdtechsunn
パ ユーサー エクスペリエンス	× .	ホ−ム >									
○ ハイブリッド管理	\sim	監査ログ									×
⊗ 監視と正常性	~										
サインインログ		⊻ ダウンロード	🕐 更新	i ≡≣列 🖗 :	フィードバックがある場合						
監査ログ		許可された時刻	: 過去]	日間 日付を次の	シ基準で表示:ローカル	サービス:すべて	カラ	コリ:すべて	アクティビティ: すべて	+マ フィルターの追加	
プロビジューングログ	_	日付	4	サービス	ภราวับ ↑.	アクティビティ	↑↓	状態	状態の理由	ターゲット	開始者 (アクター)
, uc , u , u ,		2025/3/3 10:59	9:35	Application Proxy	DirectoryManagem	Enable passthro	bugh	Success		14c5b368-772d-46	·· admin@pbdtechsup····
正常性		2025/3/3 10:59	9:26	Application Proxy	ResourceManagem-	Register conner	tor	Success		14c5b368-772d-46-	·· admin@pbdtechsup···
Log Analytics		2025/3/3 10:58	3:39	Core Directory	UserManagement	Update StsRefr	eshT…	Success		Sync_AzureVM_7f6-	·· admin@pbdtechsup···
診断設定		2025/3/3 10:58	3:39	Core Directory	UserManagement	Reset user pass	word	Success		Sync_AzureVM_7f6-	··· admin@pbdtechsup···

監査ログの詳細 アクティビティ ダーゲット 変更されたプロパティ アクティビティ 日付 2025/3/3 10:59 アクティビティの種類 Enable passthrough authentication 4ad6fd42-5272-429f a4b2-797b377de9ce 関連付け ID カテゴリ DirectoryManagement 状態 SUCCESS 状態の理由 ユーザーエージェント 開始者 (アクター) その他の詳細情報

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。

M	icrosoft Entra 管理センター	Q	リソース、サービス、ドキュメントの検索 (G+/)			
↑ 1	ホーム 新着情報 問題の診断と解決	Í	 ホーム > Microsoft Entra Connect メ トラブルシューティング ○ 更新 ○ 団 ブレビ 		マ フィードバックがある場合	
*	お気に入り	~	ここをクリックして、改良された新しい Microsoft Ent ハッコマフロロアバロション ここのフロッファ ?	ra Connect エクフ	スペリエンスをお試しください。 →	
•	ID	~	Microsoft Entra クラウド同期の管理			
0	概要		同期状態	有効		
8	ユーザー	\sim	最後の同期	1 時間前		
⁹ 2 ⁸	グループ	\sim	パスワード ハッシュの同期	有効		
8	デバイス	\sim	ユーザー サインイン			
Æ	マゴリケーション	~	「 フェデレーション	無効	0 ドメイン	
α0	アノリソーション	~	シームレスなシングル サインオン	無効	0 ドメイン	
B	保護	\sim	パススルー認証	有効	2 件のエージェント	
3	Identity Governance	\sim	証明書ベースの認証	無効		
-			代替ログイン ID として電子メールを送信する	無効		

【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。



- 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。

Microsoft Azure AD Connect Authentication Agent Packa... – × Microsoft Azure AD Connect Authentication Agent Package

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。

Microsoft Entra 管理センター	P リソース、サービス、ドキ	キュメントの検索 (G+/)	💋 Copilot 🗘 🐯		
 ☆ ホーム ✓ 新着情報 図 問題の診断と解決 	ホーム > Micr パススル・ Microsoft Entr 业 ダウンロ	crosoft Entra Connect > 一認証 … ra ID コード 🤌 トラブルシューティング 🕐 最新の情報に更新			×
★ お気に入り	→	トで少なくとも 3 つの認証エージェントが実行されていることをお勧めしま 「報 ^[2]	ます。		
▲ ID① 概要	へ 認証エージ:	コント IP	状態		
R ユーザー	~			2	
& グループ	~			>	

Microsoft アカウントを選択する		【作成したユーザーでサイン ・ 同期したユーザーのパスワー るか確認します。
田中太郎		1. Microsoft Entra IDポータ
十 別のアカウントを使用す	3	2. 前ページで作成したユーザ カし、サインインできること ³
Microsoft Entra 管理センター の	いース サービス ドキュメントの検索 (G+/)	Conjust 0 th @ P
 ☆ ホーム ✓ 新着情報 △ 問題の診断と解決 	TEST_TEST_技術支援チーム検証 + 追加 > ③ テナントの管理 ③ 新着情報 □ 図 ① お使いのホームページで、エクスペリエンスを向上させ	アカウントを表示
 ☆ ホーム ✓ 新着情報 ○ 問題の診断と解決 ★ お気に入り ✓ 	 TEST_TEST_技術支援チーム検証 + 追加 ∨ ◎ テナントの管理 ③ 新着情報 □ ① お使いのホームページで、エクスペリエンスを向上させ さい。 概要 監視中 プロパティ 推奨事項 セットアック 	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
 ☆ ホーム ✓ 新着情報 ◇ 問題の診断と解決 ★ お気に入り 〜 ◇ ID へ ① 概要 	 TEST_TEST_技術支援チーム検証 + 追加 ∨ ◎ テナントの管理 ③ 新着情報 □ ① お使いのホームページで、エクスペリエンスを向上させ さい。 概要 監視中 プロパティ 推奨事項 セットアッ ② テナントの検索 基本情報 	・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・

げーでサインイン】 -のパスワードで別サービスにサインインでき

ra IDポータルヘサインインします。

成したユーザーのアカウント/ パスワードを入 レできることを確認できます。

Microsoft社へ確認中

【サインインログ/ 〇〇 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

🔁 役割と機能の追加ウィザード					×
インストールの種類	の選択			対象サーバー AzureVM.ADtest.com	
開始する前に	インストールの種類を選択します。 の仮想ハードディスク (VHD) にイン	受割および機能は、実行中の物 ノストールできます。	カ理コンピューター、 仮	想コンピューター、またはオフライン	r
インストールの種類 サーバーの選択	 役割ベースまたは機能ベースの 役割、役割サービス、および機能)インストール 能を追加して、1 台のサーバーを)	構成します。		
1-1-01-01 後期 福夏	 リモートデスクトップサービスの 仮想デスクトップインフラストラ? ンベースのデスクトップ展開を作)インストール クチャ (VDI) に必要な役割サーと ■成します。	ごスをインストールして	仮想マシン ベースまたはセッシ	з
	■ 役割と機能の追加ウィザード 対象サーバーの違	建択			ー ロ × 対象サーバー AzureVMADtest.com
	開始する前に インストールの種類 サーバーの選択	役割と機能をインストールす ● サーバー ブールからサーバ ○ 仮想ハード ディスクから	るサーバーまたは仮想ハ- ーを選択 蠶択	ドディスクを選択します。]
	サーバーの役割 機能 	サーバー プール			
	同果	名前	IPアドレス	オペレーティング システム	
		AzureVM.ADtest.com	10.0.0.4	Microsoft Windows Server 2	022 Datacenter Azure Editi
		4			- x
		1 台のコンピューターが見つか このページには、サーバー マネ それ以降のリリースの Wind てデータ収集が完了していな	りました ニジャーの [サーバーの追 ows Server を実行して いサーバーは表示されま	加] コマンドを使用して追加された、V いるサーバーが表示されます。オフライ せん。	Vindows Server 2012 または ンサーバーや、新たに追加され
			< 前	へ(P) 次へ(N) > イ	シストールのキャンセル

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



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。

_	- 3 I 🍢
4	展開後構成 タスク - X
-	AzureVM で Active Directory Federation Services の構成が必要です
	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。

【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。



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。

📥 Active Directory フェデレーション	サービス構成ウィザード	– 🗆 X
Active Directory	ドメイン サービスへの接続	ターゲット サーバー AzureVM.ADtest.com
ようごそ AD DS への接続 サービスのプロパティの指定	フェデレーション サービス構成を実行するための Active Directory ドメ ントを指定してください。	イン管理者のアクセス許可を持っているアカウ
サービス アカウントの指定 データペースの指定 マラリミンの理訳 ま を⇒(小の確認) 「「トー」」	(現在のユーザー)	<u>发史(L)</u> ,,,
	<前へ(P) 次へ(N)	> 構成(C) キャンセル

📥 Active Directory フェデレーション 🕯	サービス構成ウィザード		- 🗆 X
サービスのプロパテ	ィの指定	A	ターゲット サーバー JFS1.Labdomain.local
ようこそ AD DS への接続 サービスのプロパティの指定	SSL 証明書:	sts.t * 表示	インボート(!)
サービス アカウントの指定 データベースの指定 オブションの確認	フェデレーション サービス名:	sts.t	
前提条件の確認 インストー1 行業	フェデレーション サービスの表示名:	O ユーザーはサインイン時に表示名を確認しま 例: Contoso Corporation	₫。
	[<前へ(<u>P</u>) 次へ(<u>N</u>) > 構成	(<u>C</u>) キャンセル

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。

Active Directory フェデレーション サ	ービス構成ウィザード		-		>
ナービス アカウントの	の指定		ADFS1.La	ターゲット サ abdomain	-/(- loca
ようこそ	ドメイン ユーザー アカウントまた	こはグループの管理されたサービス アカウントを指定し	してください。		
AD DS への接続 サービスのプロパティの指定 サービス アカウントの指定	・ グループ管理サービス アカ アカウント名:	ウントを作成します LABDOMAIN¥ adfsSystemU	ser		
データベースの指定	〇 既存のドメイン ユーザー フ	アカウントまたはグループの管理されたサービス アカウ	ントを使用してくた	ざい	
オフンヨンの確認 前根条件の確認	アカウント名:	<未指定>		選択(<u>S</u>)	
12.21-1					
結果					
		<前へ(P) 次へ(N) >	構成(<u>C</u>)	キャンセ	211

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"

م ۲۹۶۲ ADFS1.Labdomain.l	ーバー ocal
るためのデータベースを指定してください。 ニスを作成します。	
スを使用するには、このフィールドを空白のまま	
	_
(80)、 様式(の) キャンカ	
	るためのデータベースを指定してください。 ニースを作成します。 <i>スを使用するには、このフィールドを空白のまま</i> .(Ŋ) > 構成(<u>C</u>) キャンセ

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。

📥 Active Directory フェデレーション サ	ービス構成ウィザード	- 🗆 X
オプションの確認		ターゲット サーバー ADFS1.Labdomain.local
ようこそ AD DS への接続 サービスのプロパティの指定 サービス アカウントの指定 データベースの指定 オプションの確認 前提条件の確認 インストール	次の選択を確認してください: このサーバーは、新しい AD FS ファーム 'sts.1 AD FS 構成は Windows Internal Database に格納されます。 Windows Internal Database 機能がこのサーバーにまだインストー Group Managed Service Account LABDOMAIN¥adfsSyster このホストはメンバーとして追加されます。 LABDOMAIN¥adfsSystemUser\$ として実行されるようにフェデレ	・ でプライマリ サーバーとして構成されます。 かされていない場合はインストールされます。 mUser\$ がまだ存在しない場合は作成され、 テーション サービスが構成されます。
	これらの設定は、追加のインストールを自動化する Windows Pow スポートできます < 前へ(P) 次へ(L	erShell スクリプトにエク スクリプトの表示(Y) 構成(<u>C</u>) キャンセル

前提条件の確認		ターゲット サ ADFS1.Labdomain.	ーバー local
♂ すべての前提条件のチェックに	合格しました。[構成] をクリックしてインストールを開始してください。	詳細表示	×
ようこそ AD DS への接続 サービスのプロパティの指定 サービス アカウントの指定 データベースの指定	Active Directory フェデレーション サービスをこのコンピューターで構成する前に す。 前提条件のチェックを再実行 (へ) 結果の表示(<u>V</u>)	、前提条件を確認する必要があ	りま
オプションの確認 前提条件の確認 インストール モモ	 2019/08/10 11:10:18 に Group Managed Service Account のJ Directory フォレスト内に複数のドメイン コントローラーがある場合、ま: ラーにレプリケートされていない可能性があります。この場合、サービスの れないことがあります。サービス開始時の問題を防ぐには、確実にキー プリケートされるように 10 時間待ってから、Active Directory Federa 了し、ネットワーク上の他のサーバーで Install-AdfsFarm または Add- AD FS サービスを再起動します。 前提条件のチェックが完了しました すべての前提条件のチェックに合格しました。[構成] をクリックしてイン 	レート キーが作成されました。Activ だキーがすべてのドメイン コントロー)インストールや開始が正しく実行: がすべてのドメイン コントローラーに1 ntion Services 構成ウイザードを完 -AdfsFarmNode を実行するか、 シストールを開始してください。	
	- #5 A (D)		

14. 「構成」をクリックし、完了です。



【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

🔒 Microsoft Entra Co	onnect 同期	- ×
1925	追加のタスク	
920	このシナリオで必要なタスクが完了しました。さらにタスクを実行するには、以下のリストから選択してください。	
	プライバシーの設定	
	現在の構成の表示またはエクスポート	
	同期オプションのカスタマイズ	
	デバイス オブションの構成 😢	
	ディレクトリスキーマの更新	
	ステージング モードの構成	
	ユーザーサインインの変更	
	フェデレーションの管理 🕜	
	トラブルシューティング	
	前へ	<u>دم</u>

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. 「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。



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。

vilcrosoft Azure Active Direc	tory connect - *
5.5.7 部単設定 A両コンボーネント (- ザー ワインイン zure AD に接続: 両期 Connect ディレクトリ Azure AD サインイン ドメイン/QU のフィルタリング コーザーの簡別 フィルタリング オブション爆能 総信情能 D FS ファーム zure AD ドメイン 職 動の検証	<complex-block></complex-block>
	Azure AD ドメイン 備成 接続の検証 のK キャンセル

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。



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。





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。

ectory Connect		-	×	
 中意のユーザー識別方法を選択します。 コーサーは、すべてのティレクトリで 1 産だけ示されます。 単数のティレクトリにユーザー 1D が存在します。次を使用し メール属性 Object5ID および msExchMasterAccountSID/msR SAMAccountName および MailNickName の属性 特布の属性 Azure AD でのユーザーの戦別方法を選択します。 Azure でゾースアンカーを審理します 特定の属性を選択します 	た一致: ITCSIP-OriginatorSit	つの属性 フレミス ユーザーのソース アンカーを	yy Connect ユーザーおよびデ パイロット テプロイには、同期するユーザー れていないので、無視されます。 ・ すべてのユーザーとデバイスの同期 - 選択した項目の問題・ フォレスト 4	12. そのまま「次々 13. さらに「次へ」 「バイスのフィルタリング ちょりデバイスを含むグループを推定してください。入れ子のグループはサポートさ
書き戻します。詳細情報	前へ	灾へ.		
		■悟情報 AD FS:ファーム Azure AD Fメイン 構成 接続の検証		
	 ctory Connect 一一意のユーザー識別方法を選択します ユ・サーは、すべてのティレクトリでのユーザーの施別方法を選択します ユ・サーは、すべてのティレクトリで1 国だけ示されます。 確飲のティレクトリにユーザー ID が存在します。次を使用し、 メール属性 ObjectSID あよび msExchMasterAccountSID/msR SAMAccountName および MailNickName の属性 特有の属性。 Azure AD でのユーザーの識別方法を選択します。 Azure でし、アンカーを管理します。 特定の属性を選択します Azure では現在 mS-DS-ConsistencyGuid を使用して 書を回します。 	tory Connect 	tory Connect	tory Connect ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★

12. そのまま「次へ」をクリックします。



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。

Microsoft Azure Active Direction	tory Connect	- ×
 うこき 悪事設定 必須コンボーネジト ユーザー サイソイン Azure AD 下掛 続 同期 Connect ディレクトリ Azure AD サインイン ドメイン/OU のフィルタリング ユーザーの識別 フィルタリング ナニーン(単い) 	ドメイン管理者の資格情報 Azure AD Connect ICは、AD FS が雇用されているか痛成されているドメインのドメイン管理者の直格情報が必要で す。	
<u>創格情報</u> AD FS ファーム Azure AD Fメイン 構成 接続の検証	前个一次个	

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。

 席申設定 必須コンボーネット コーヴー ヴイブックン Azure AD に接続 D型 Connect ディレクトリ Azure AD サインイン ドメイン/OU のフィルタリンク コーヴーの観別 フィルタリンク オフション機能 DIFUーション サーバー プロキシ サーバー ウビス アカウント Azure AD ドメイン 	1577	AD FS ファーム
A2010 AD 1: East: 回期 Connect デイレクトリ Azure AD サイソイン ドメイン/OU のフォルタリン コーザーの識別 フィルタリング オブション機能 資格情報 AD FS ファーム フェデレーション サーバー ウェデレーション サーバー ウェデレーション サーバー ケーズ ウェジン ア・ビス アカウント Azure AD ドメイン	簡単設定 必須コンポーネント ユーザー サインイン	新し() AD FS ファームを構成する 既存の AD FS ファームを使用する
フィルタリング -W2022-PGW-ADFS-CA, オブション機能 フェデレーション サービス名 責任情報 フェデレーション サービス名 AD FS ファーム https://g アロキシ サーバー ワェデレーション サービス名 サ・ビス アカウント Azure AD ドダイン	Radire AD に出版 回期 Connect ディレクトリ Azure AD サインイン ドメイン/OU のフィルタリン・ コーザーの観別	クライアントと AD FS の間の通信を保護するために使用される SSL 証明書を含む、バスワードで保護された PFX ファイル を提供します。 証明書ファイル ② C:¥Users¥Administrator¥Desktop¥adfs-cent2.pfx
AD F5 ファーム https://g W2022-PGW-ADFS-CA.g フェデレーション サーバー プロキシ サーバー サービス アカウント Azure AD ドメイツ	フィルタリンク オプション版能 責格情報	-W2022-PGW-ADFS-CA, フェデレーション サービス名
偶成	AD FS ファーム フェデレーション サーバー プロキシ サーバー サービス アカウント Azure AD ドメイン 構成	https://fW2022-PGW-ADFS-CA.f

16. SSL証明書をアップロードし、「次へ」をクリックしま

す。

A Microsoft Azure Active Dire	ctory Connect		- *
まえごそ 簡単設定 必須マンポータント	AD FS サーバー AD FS のインストール先を指定してください。		
ロッスコンパ ネット ユーザー サインイン Azure AD に接続 同期 Connect ディレクトリ Azure AD サインイン ドメイン/QU のフィルクリン/ ユーザーの識別	サーバー 「サーバー <i>含または IP アドレスの入力</i> 運択したサーバー ジ W2022-PGW-ADFS.;	遥加 参照 削除	
フィルタリング オプション機能 資格情報 AD FS ファーム フェデレーション サーバー プロキシ サーバー サービス アカウンド Azure AD ドメイン			Microsoft Azure 上記史 宿中設定
		前へ次へ	ユーザー サインイン ユーザー サインイン Azure AD に接続 同期 Connect ディレ! Azure AD やすS ドメイン/OU のフ ユーザーの編例
			メイルタクジング オブション爆発 資格情報 AD FS ファーム フェデレーション 5

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。



「単秋元 、項コンポーネント	AD FS サービス ログ オン アカウントを指定します。 🗊	
ーザー サインイン	マネージド サービス アカウント グループを作成します	
zure AD 信接続 期	既存のグループのマネージド サービス アカウントを使用する	
Connect ディレクトリ	ドメイン ユーザー アカウントを使用します	
Azure AD サインイン ドメイン/OU のフィルタリンク	エンタープライズ管理者ユーザー名 🕖	
フィルタリング	エンタープライズ管理者パスワード	
オプション機能	***********	
格情報		
5 FS 27-4		
フェテレージョン サーバー		
ታ-ሮጊ ፖስዕንት		
ure AD FX12		
et v		

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。

Microsoft Azure Active Dire	ctory Connect	- ×.	
ようごそ 簡単設定 必須コンポーネント ユーザーサインイン Azure AD に接続 同期 Connect ディレクトリ Azure AD サインイン ドメイソ/OU のフィルクリン ユーザーの版別 フィルクリング オプション/原能	Azure AD ドメイン オンプレミス ディレクトリとフェデレーションする Azure AD ドメインを選択します。 ドメイン: ②		22. フェデレー: をクリックしま 23. 構成完了後、
 愛袖信歌 AD FS ファーム フェテレージョン サーバー プロキシ サーバー サービス アカウント Azure AD FXイン 構成 	→ ドメインは管理対象ドメインであり、フェテレーション ドメインに変換されます インは中断されます。詳細情報 前へ	 この処理中にユーザーログ 次へ ドメインハロレ のフィルタリン・ ユーザーの取別 フィルタリング オフション機能 資格情報 	ectory Connect 構成が完了しました Azure AD Connect 構成が成功しました。 構成が完了しました。続いて、フェテレーションの設定を確認できます。 Active Directory のごみ箱は、フォレスト に対して有効ではありませんが、Active Directory のごみ箱の有効化に関する詳細情報 Azure Active Directory では AD 属性 m5-D5-ConsistencyGuid をソース アンカー属性として使用するように 構成されています。ソース アンカー属性の構成に関する詳細情報
		AD FS ファーム フェテレーション サーバー フロキシ サーバー サービス アカウント Azure AD FXイン	20.

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。

アカ	ウントを選択する	
Ă	田中 太郎 tanaka@p サインイン済み	•
+	別のアカウントを使用する	

【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ポータルヘサインインします。

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。

Microsoft Entra 管理センター	21	ハソース、サービス、ドキュメントの検索 (G+/) Copilot Copilot	٤Ğ	® &		9
★ ホーム	1		ТÉ	設定 EST_打	支術支援チーム検証用	サインアウト
➡ 新着情報		🕂 追加 🗸 🕸 テナントの管理 🖄 新着情報 🛛 📴 プレビュー機能 🛛 🔗 フィードバックがある	5場		tanaka@,	•
▶ 問題の診断と解決		 お使いのホームページで、エクスペリエンスを向上させるための取り組みが行われています。[フィード さい。 	л (3	アカウントを表示	
★ お気に入り	\sim	概要 監視中 プロパティ 推奨事項 セットアップガイド				
ID	~	タ テナントの検索	_ (8 ₊) 別のア:	カウントでサインインする	
① 概要		基本情報				
R ユーザー	\sim					

Microsoft社へ確認中

【サインインログ/ 〇〇 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。