

# セキュアドPC月額レンタルモデル 管理者操作マニュアル Ver1.4

2024年1月26日  
NTTコミュニケーションズ株式会社

## I.ユーザーを追加/削除する時の対処

- 1.アカウントの追加方法
- 2.アカウントの削除方法
- 3.ライセンスの割り当て方法
- 4.ライセンスの割り当てを外す方法

## II.ユーザーがパスワードを忘れてしまった場合の対処

- 1.ユーザーのパスワードのリセット方法

## III.端末のユーザーが変更となった時の対処

- 1.端末のリセット、及び新規ユーザーのログイン

## IV.ユーザーにデバイス管理者権限を付与したい場合の対処

- 1.ローカル管理者ロールの割り当て
- 2.ローカル管理者ロールの割り当て削除

## V.端末の盗難や紛失時の対処

- 1.端末の位置情報検索
- 2.遠隔での端末の初期化

## VI.端末返却時のデータ削除

- 1.端末のリセット（管理者操作）
- 2.端末のリセット（端末操作）

## VII.その他

- 1.ユーザーの端末が故障した場合

## VIII.留意事項

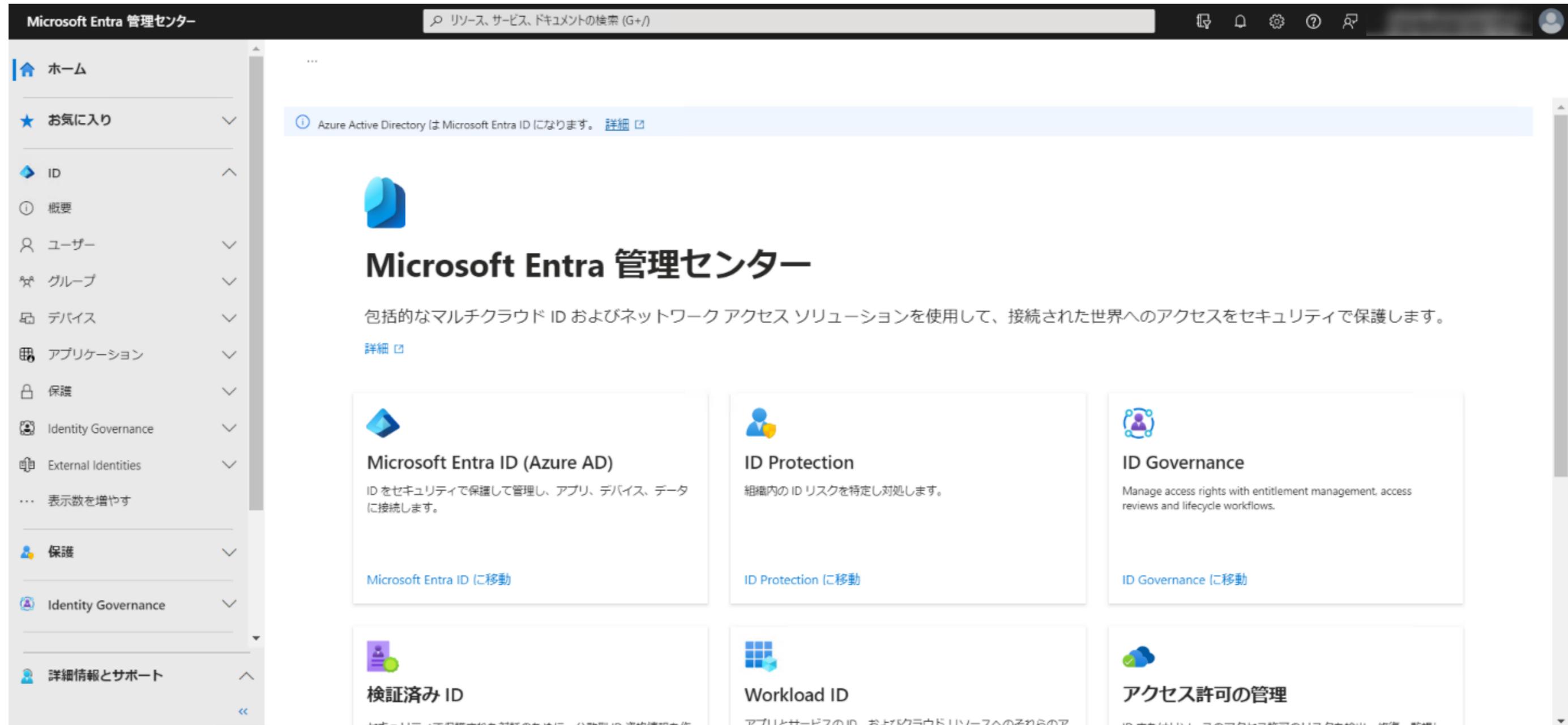
- 1.総務省セキュリティガイドラインに対する機能対応表
- 2.総務省セキュリティガイドラインに準拠したMicrosoft365設定内容

# I .ユーザーを追加/削除する時の対処

- 1.アカウントの追加方法
- 2.アカウントの削除方法
- 3.ライセンスの割り当て方法
- 4.ライセンスの割り当てを外す方法

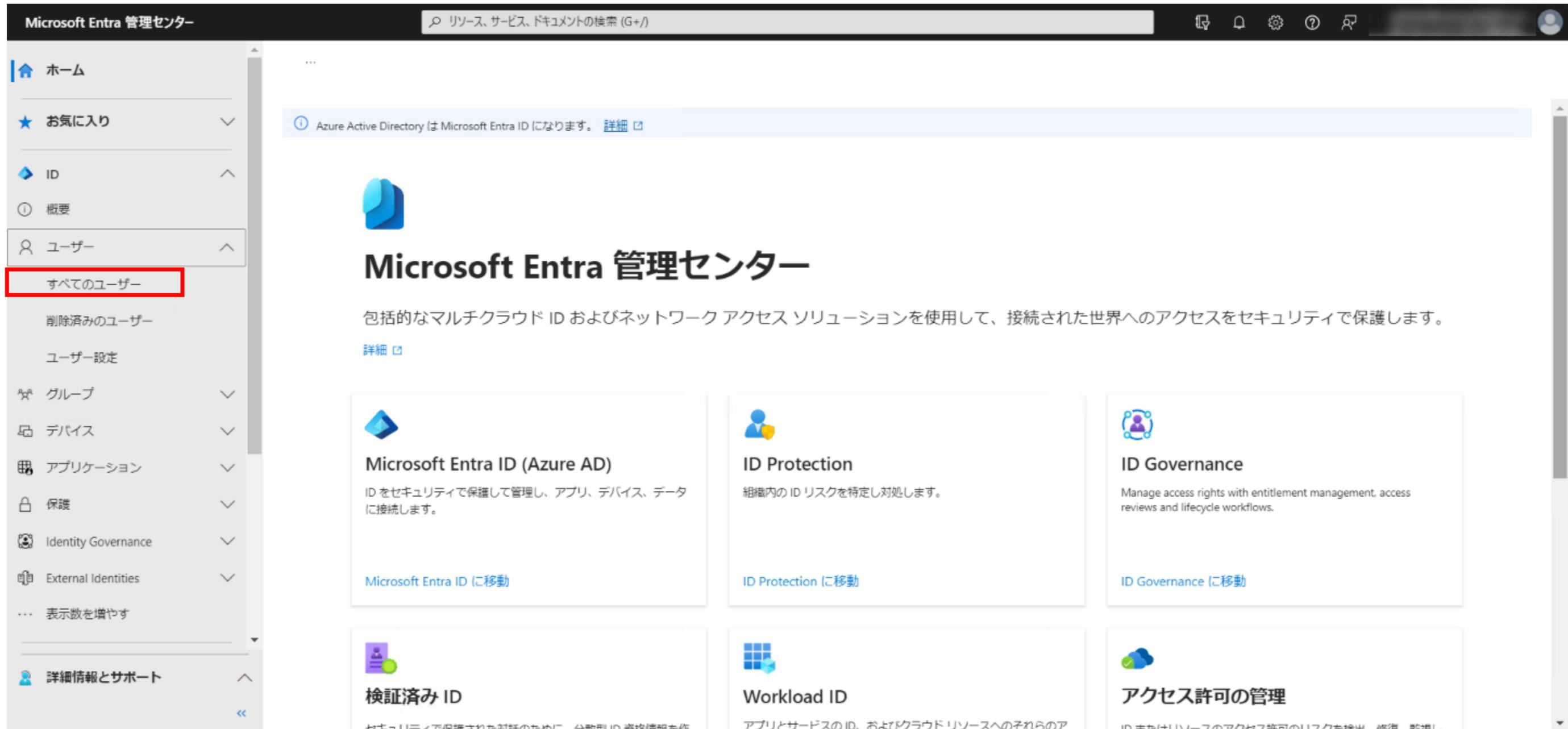
# I-1 アカウントの追加方法

1. Microsoft Entra 管理センター (<https://entra.microsoft.com>) にアクセスします



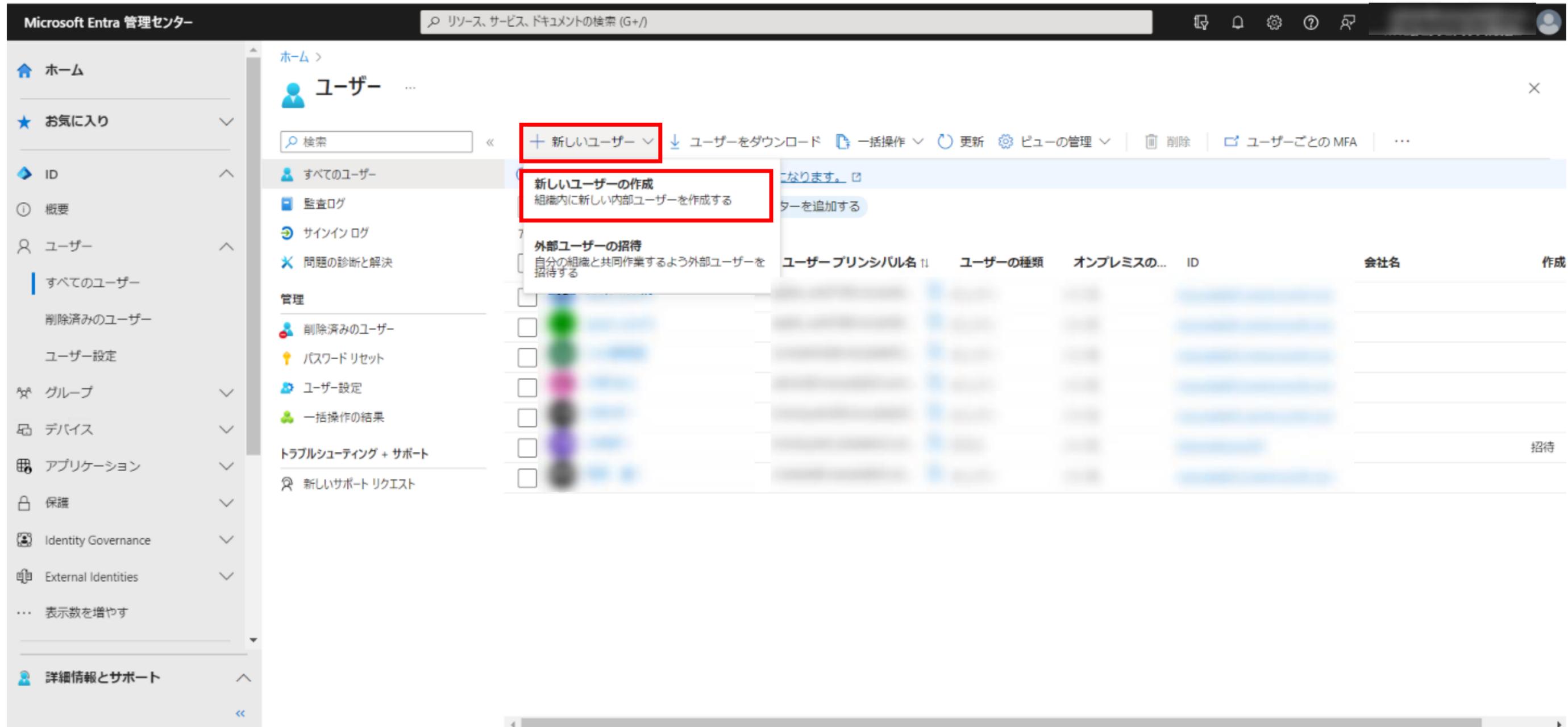
# I-1 アカウントの追加方法

2.左の[ID]-[ユーザー]をクリックして展開し、[すべてのユーザー]をクリックします



# I-1 アカウントの追加方法

3.[新しいユーザー]をクリックし、[新しいユーザーの作成]をクリックします



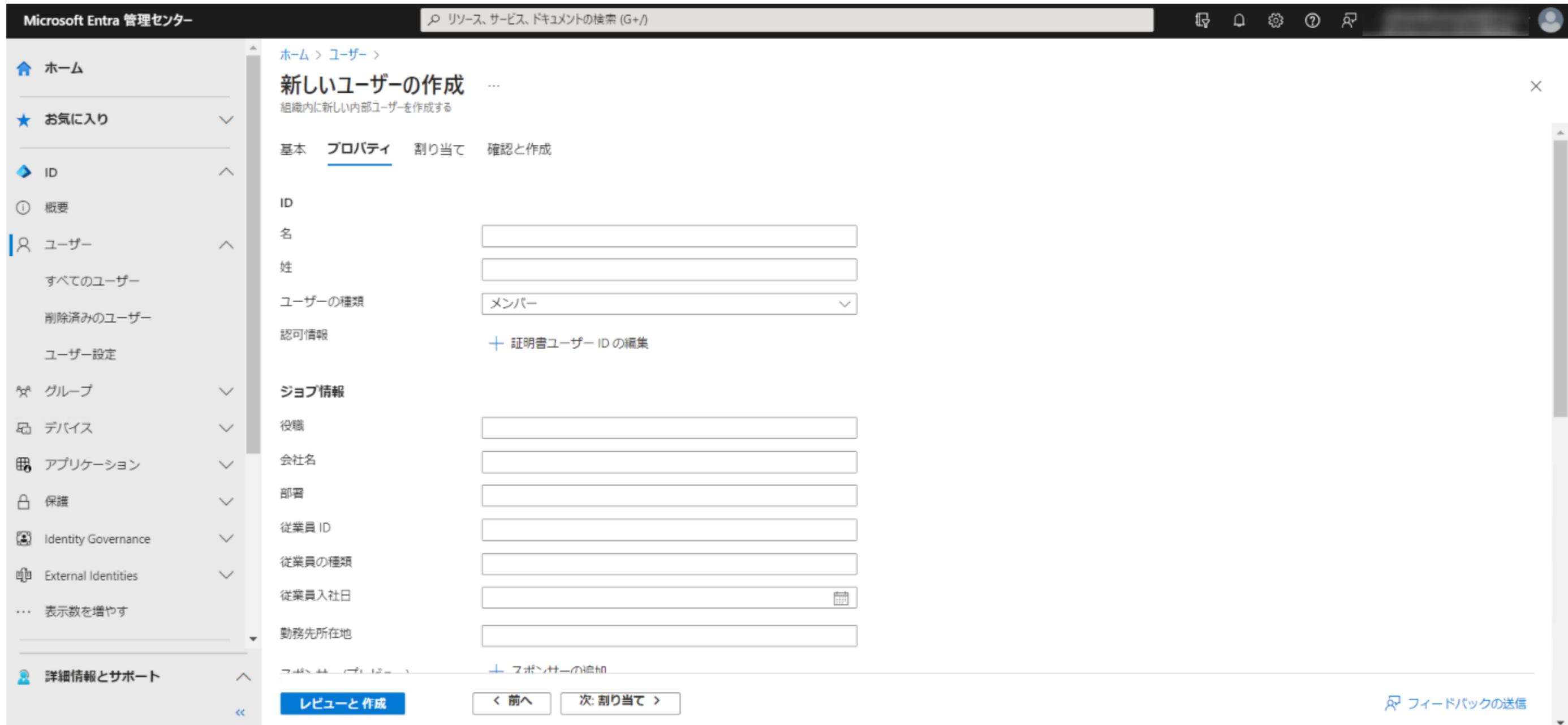
# I-1 アカウントの追加方法

4. ユーザープリンシパル名や表示名、パスワードなどを入力します  
 入力後、[次:プロパティ]をクリックします



# I-1 アカウントの追加方法

5.プロパティの画面で必要に応じ、各情報を入力します



The screenshot shows the Microsoft Entra Management Center interface. The left sidebar contains navigation options like Home, Favorites, ID, Summary, Users, Groups, Devices, Applications, Security, Identity Governance, and External Identities. The main content area is titled '新しいユーザーの作成' (New User Creation) and is currently on the 'プロパティ' (Properties) tab. The form includes the following fields:

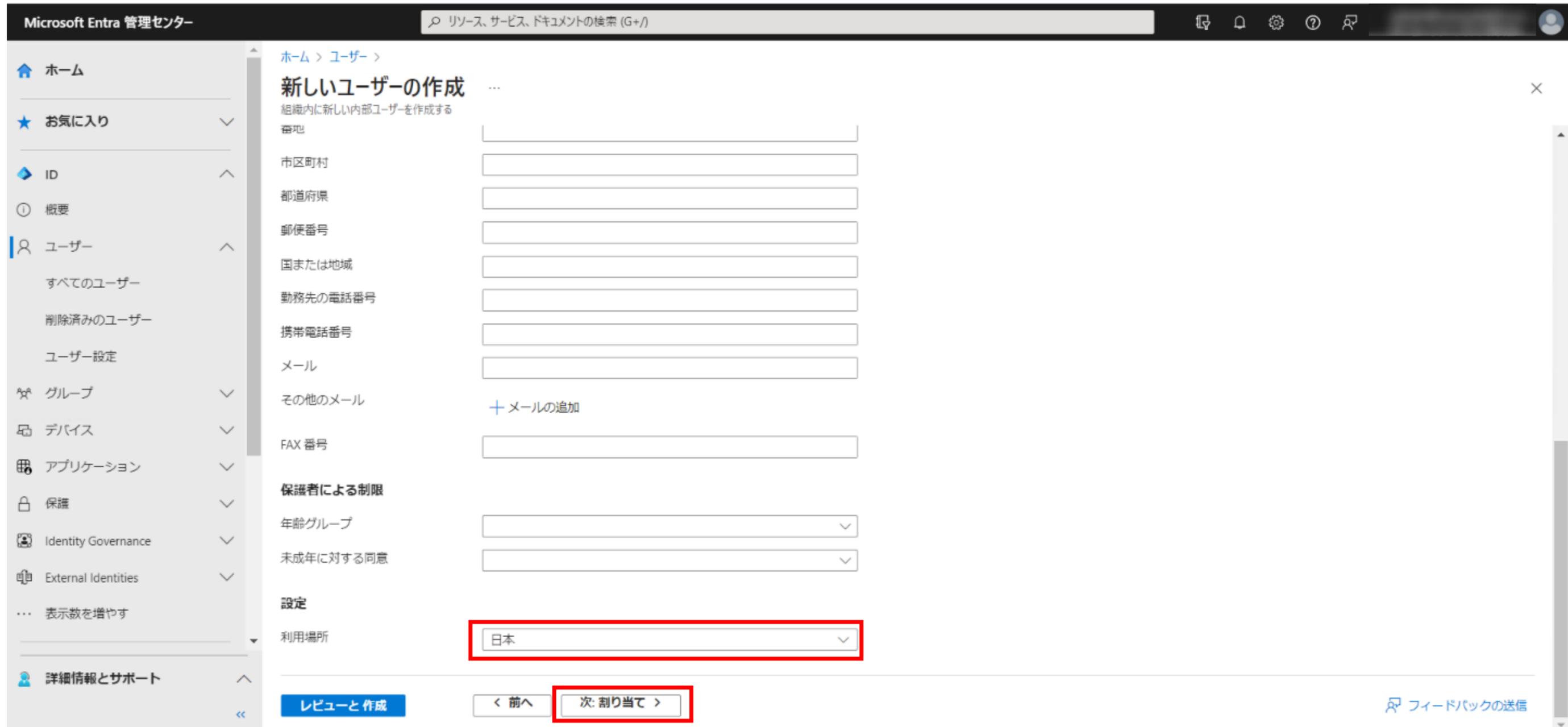
- ID
- 名 (First Name)
- 姓 (Last Name)
- ユーザーの種類 (User Type): Member
- 認可情報 (Authentication Information): + 証明書ユーザー ID の編集 (Edit Certificate User ID)
- ジョブ情報 (Job Information):
  - 役職 (Job Title)
  - 会社名 (Company Name)
  - 部署 (Department)
  - 従業員 ID (Employee ID)
  - 従業員の種類 (Employee Type)
  - 従業員入社日 (Employee Start Date)
  - 勤務先所在地 (Work Location)
- スポンサー (Sponsor): + スポンサーの追加 (Add Sponsor)

At the bottom of the form, there are navigation buttons: 'レビューと作成' (Review and Create), '< 前へ' (Previous), and '次: 割り当て >' (Next: Assign). A 'フィードバックの送信' (Send Feedback) link is also present in the bottom right corner.

# I-1 アカウントの追加方法

6. プロパティ内の利用場所は、[日本]を選択し、[次：割り当て]をクリックします

※利用場所が未設定の状態ですと、後述のユーザーにライセンスを割り当てるできません



The screenshot shows the Microsoft Entra Management Center interface for creating a new user. The left sidebar contains navigation options like Home, Favorites, ID, Summary, Users, Groups, Devices, Applications, Security, Identity Governance, and External Identities. The main content area is titled 'New user creation' (新しいユーザーの作成) and includes various input fields for user details such as Name, Address, Phone numbers, and Email. The 'Location' (利用場所) dropdown menu is currently set to 'Japan' (日本) and is highlighted with a red rectangular box. Below the form, the 'Next: Assign' (次: 割り当て) button is also highlighted with a red rectangular box. Other buttons include 'Review and create' (レビューと作成), 'Previous' (前へ), and 'Feedback' (フィードバックの送信).

# I-1 アカウントの追加方法

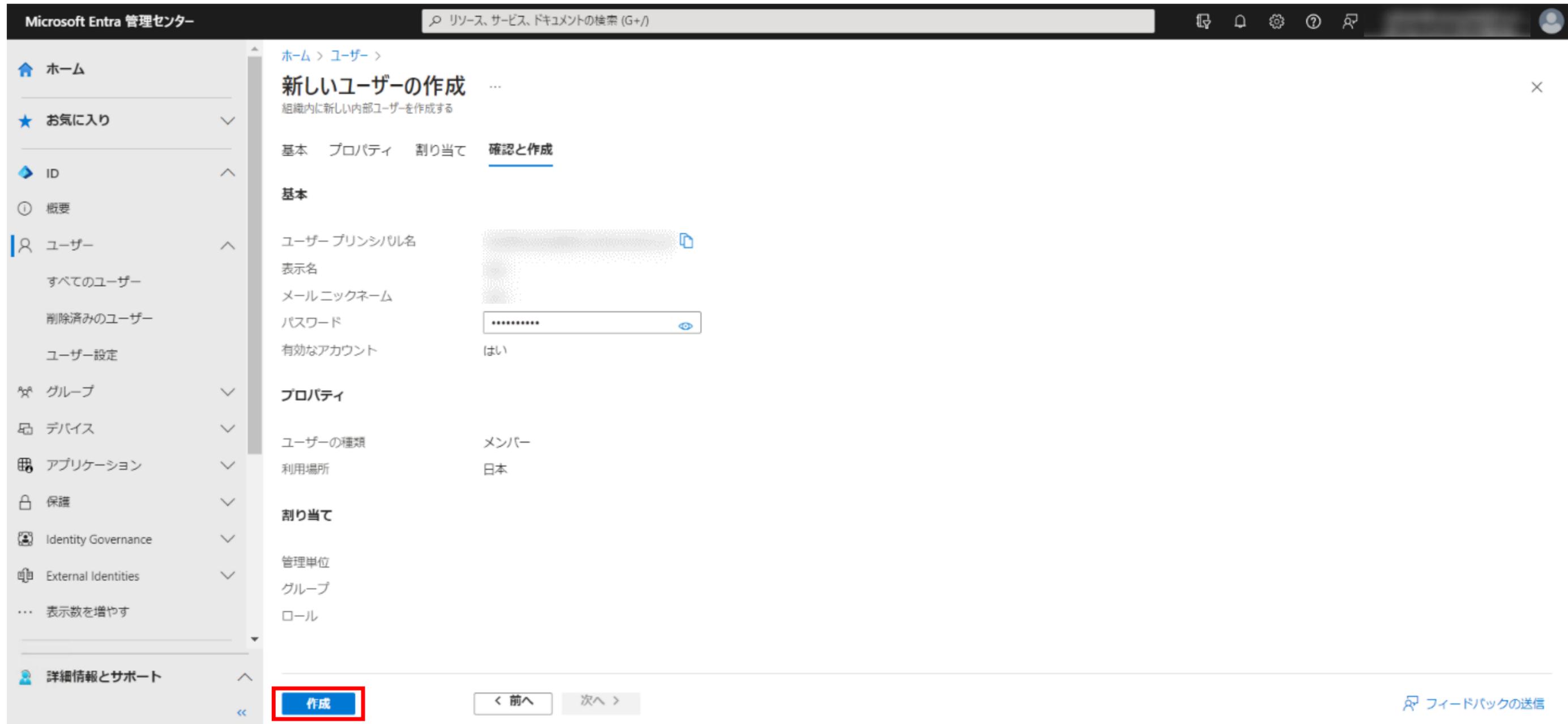
7. グループに割り当てる場合は[グループの追加]、ロールを割り当てる場合は[ロールの追加]をクリックし割り当てます  
[次：確認と作成]をクリックします



The screenshot shows the Microsoft Entra Management Center interface. The left sidebar contains navigation options such as Home, Favorites, ID, Summary, Users, Groups, Devices, Applications, Security, Identity Governance, and External Identities. The main content area is titled 'New User Creation' and includes tabs for 'Basic', 'Properties', 'Assign', and 'Confirm and Create'. The 'Assign' tab is active, showing instructions to assign up to 20 groups or roles. Below the instructions are three buttons: '+ Add Management Unit', '+ Add Group', and '+ Add Role'. At the bottom of the page, there are navigation buttons: 'Review and Create', '< Back', 'Next: Confirm and Create >' (highlighted with a red box), and 'Send Feedback'.

# I-1 アカウントの追加方法

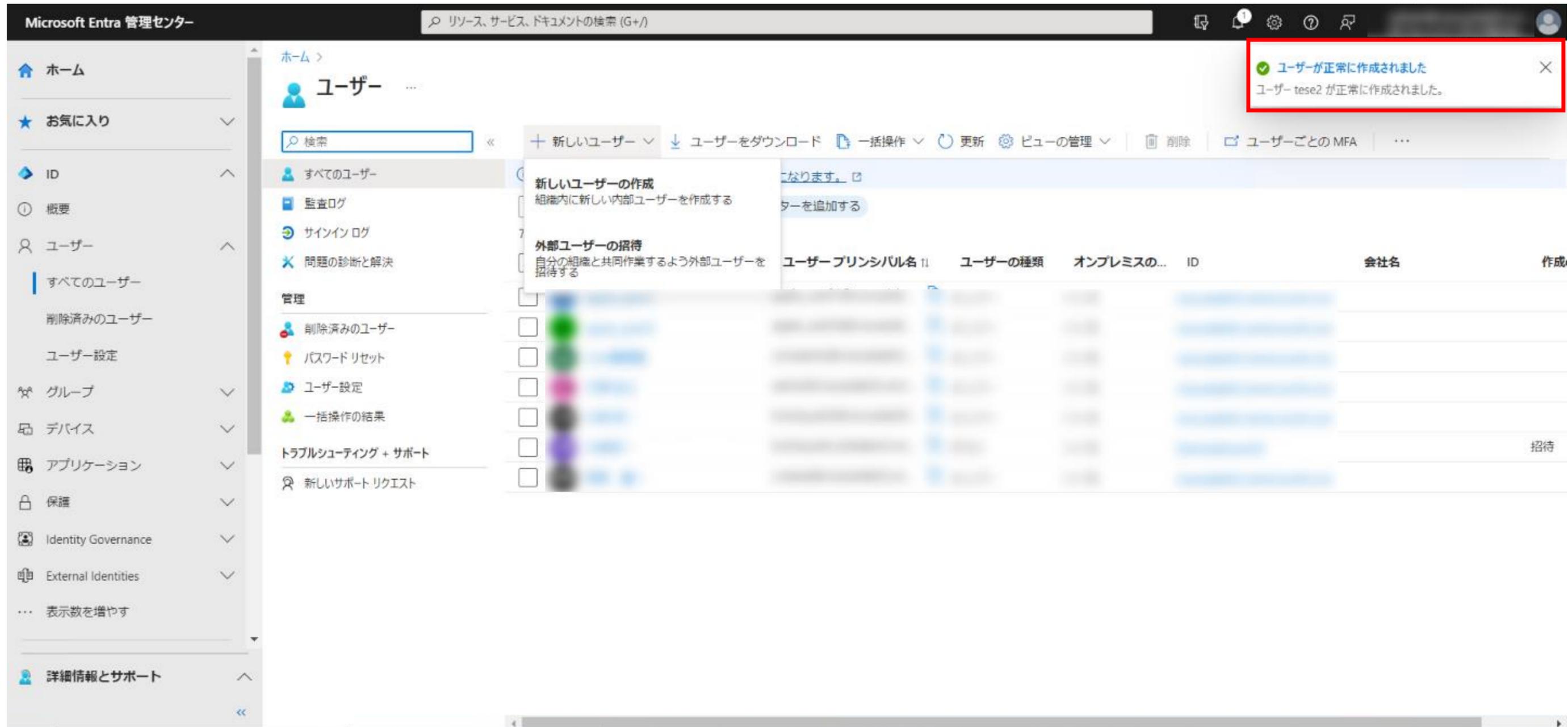
## 8. 作成内容を確認し、[作成] をクリックします



The screenshot shows the Microsoft Entra Management Center interface. The left sidebar contains navigation options such as 'ホーム' (Home), 'お気に入り' (Favorites), 'ID', '概要' (Overview), 'ユーザー' (Users), 'グループ' (Groups), 'デバイス' (Devices), 'アプリケーション' (Applications), '保護' (Protection), 'Identity Governance', 'External Identities', and '詳細情報とサポート' (Details and Support). The main content area is titled '新しいユーザーの作成' (Create New User) and is divided into four tabs: '基本' (Basic), 'プロパティ' (Properties), '割り当て' (Assignments), and '確認と作成' (Review and Create). The '確認と作成' tab is active, showing a summary of the user creation details. At the bottom of the page, the '作成' (Create) button is highlighted with a red box, indicating the final step in the process. Other buttons include '< 前へ' (Previous) and '次へ >' (Next), and a 'フィードバックの送信' (Send Feedback) link is visible in the bottom right corner.

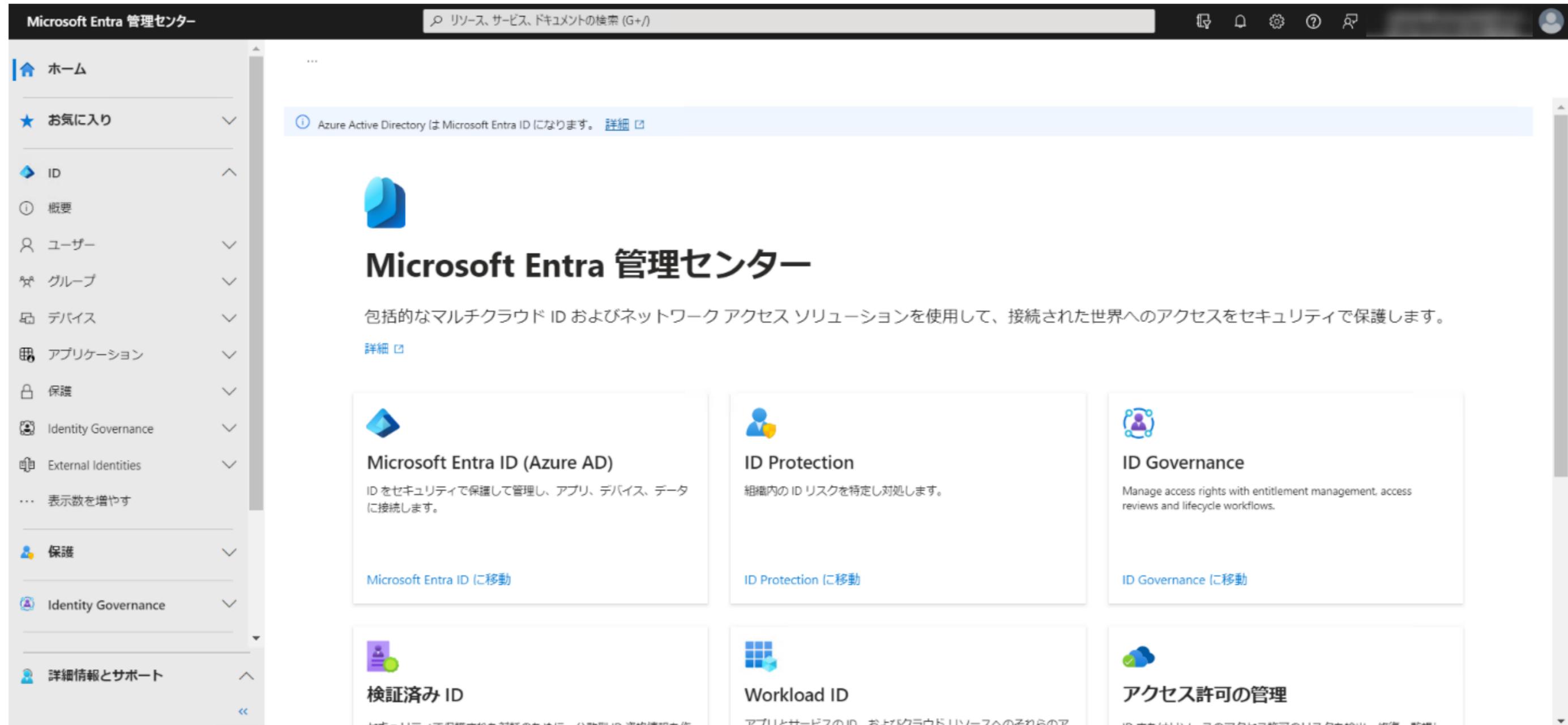
# I-1 アカウムの追加方法

9. 「ユーザーが正常に作成されました」が表示されたら完了です



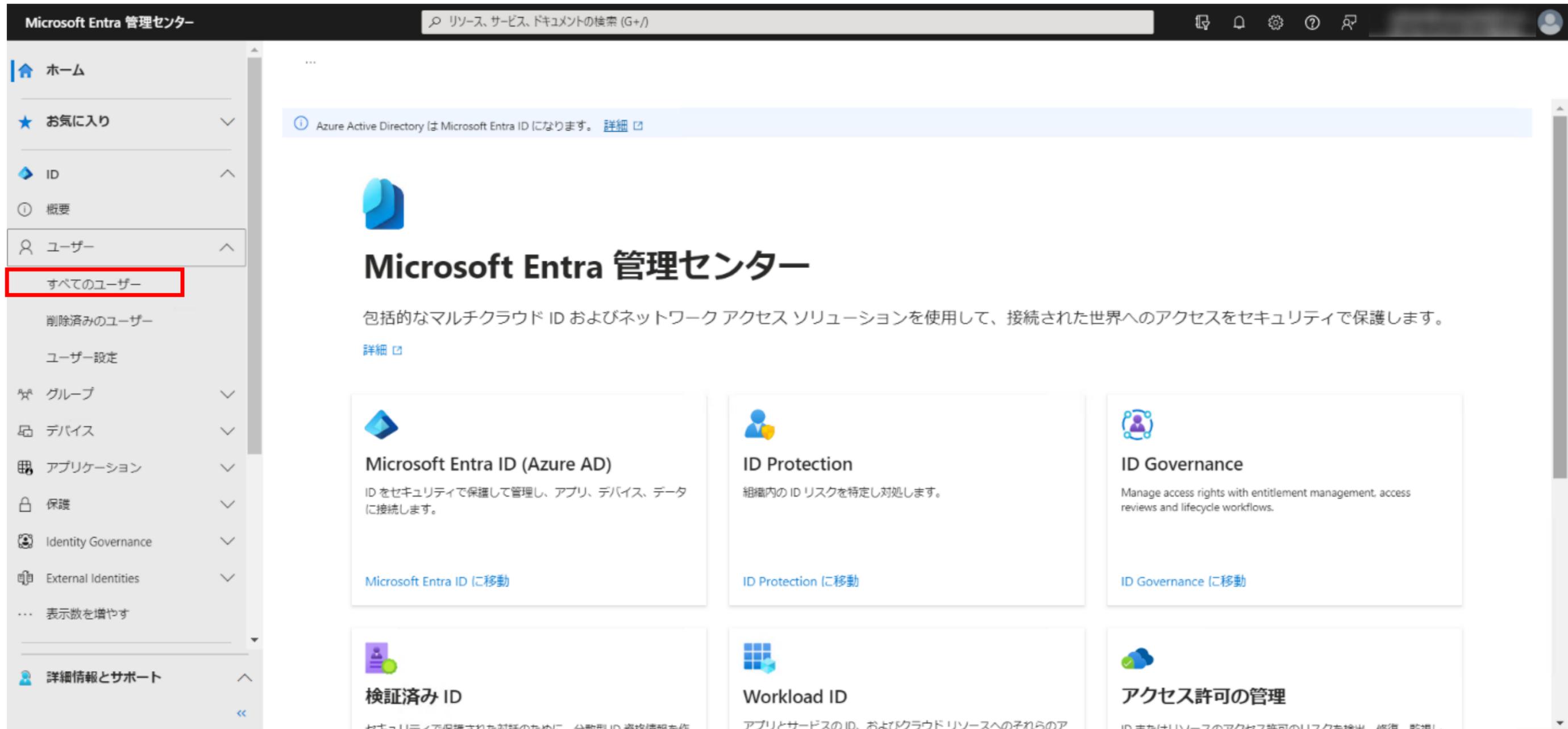
# I-2 アカウントの削除方法

1. Microsoft Entra 管理センター (<https://entra.microsoft.com>) にアクセスします



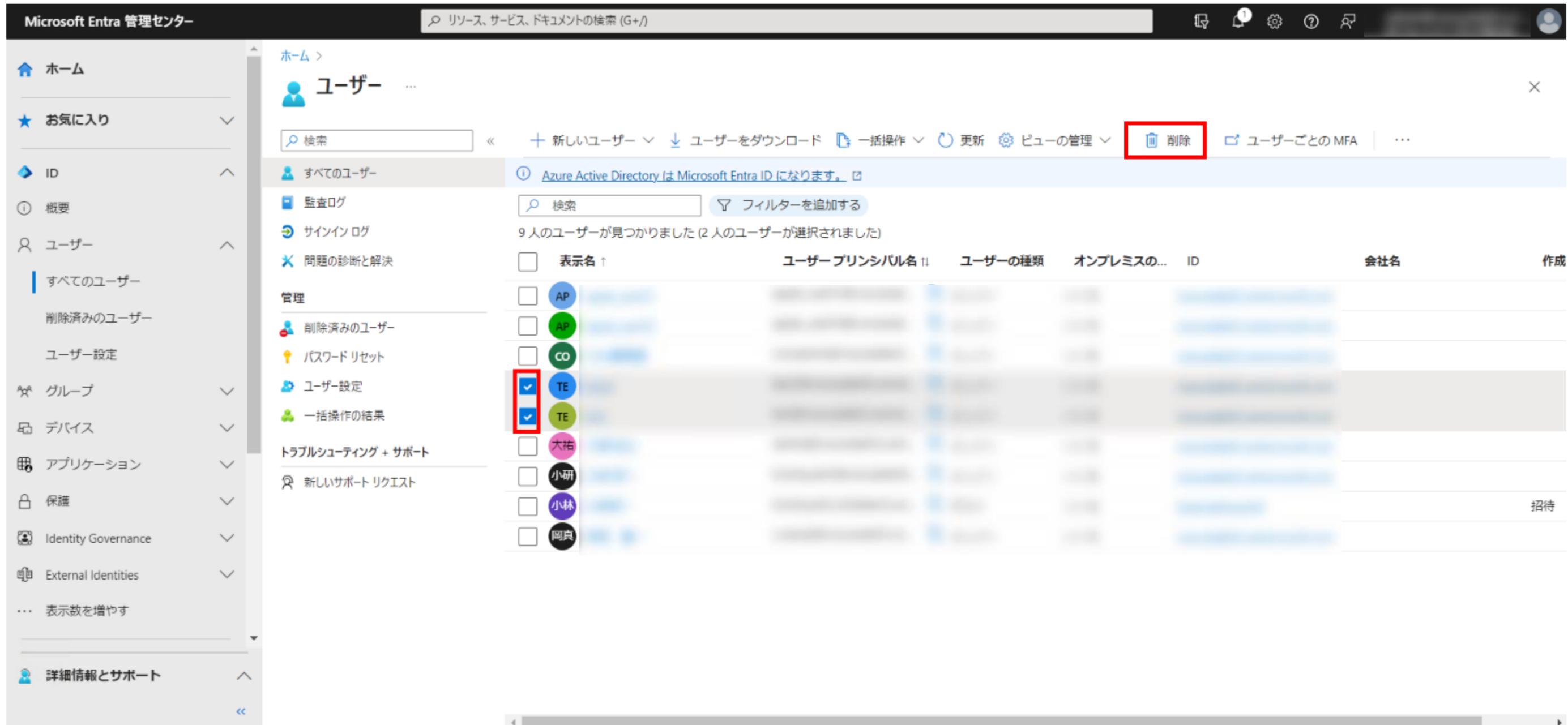
# I-2 アカウントの削除方法

2.左の[ID]-[ユーザー]をクリックして展開し、[すべてのユーザー]をクリックします



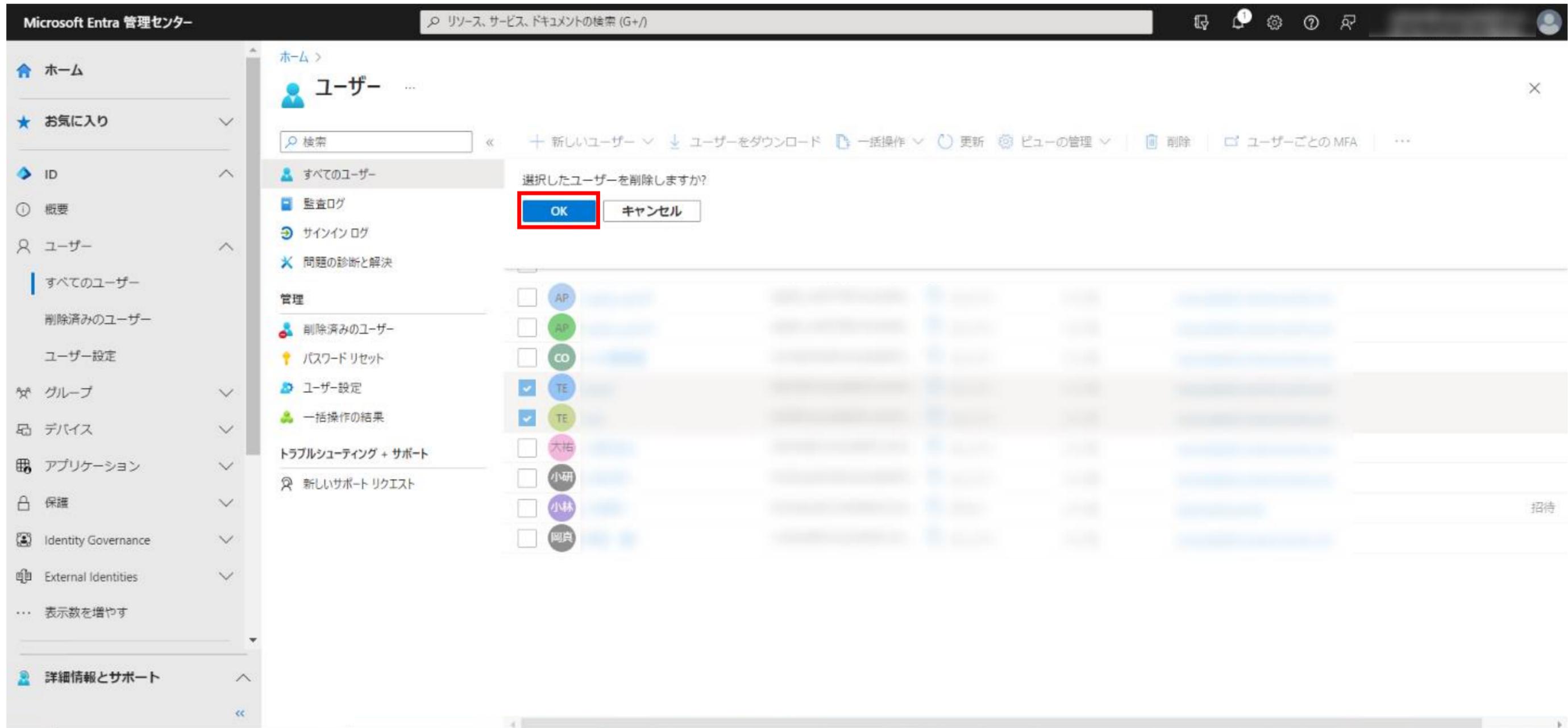
# I-2 アカウムの削除方法

3.削除対象のアカウントの[□]にチェックを入れ、[削除]をクリックします



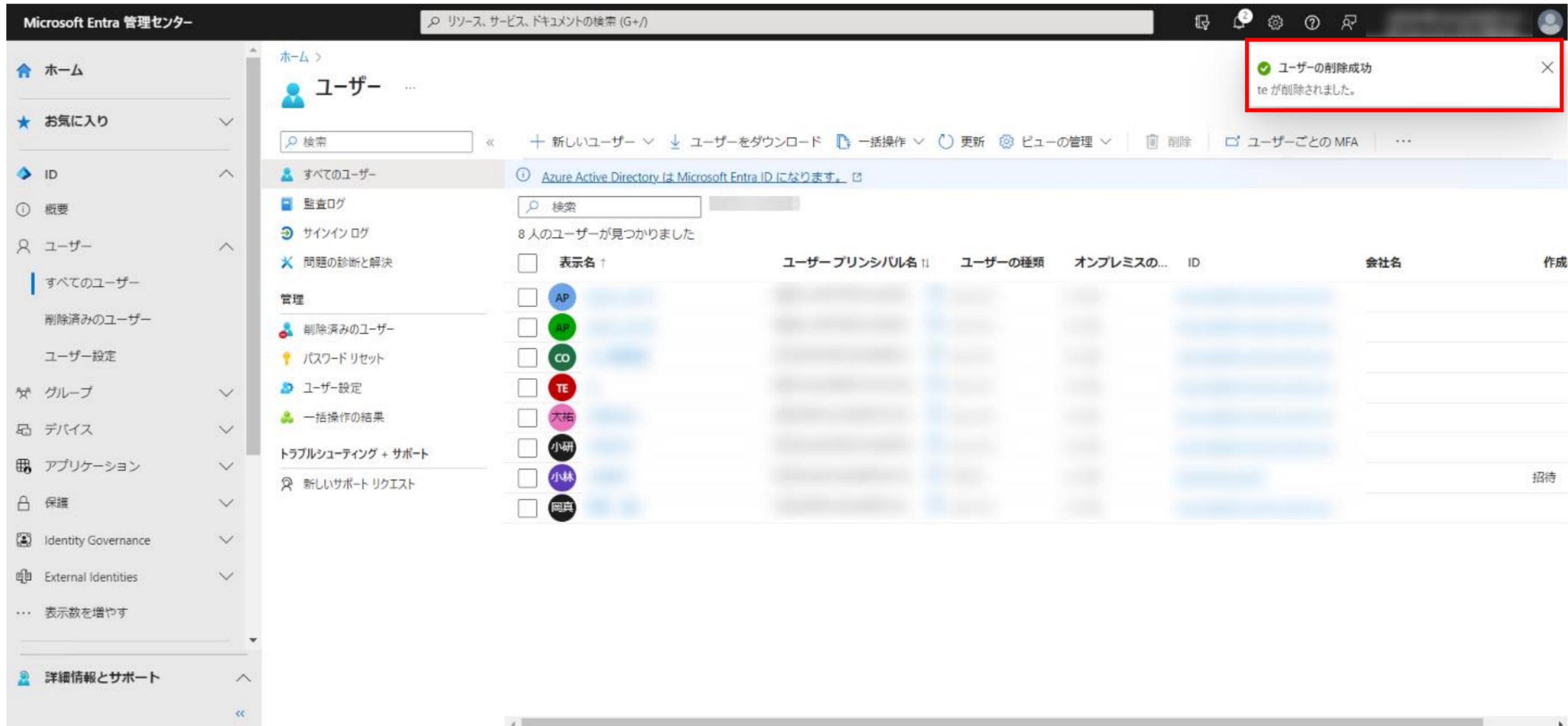
# I-2 アカウムの削除方法

4. 「選択したユーザーを削除しますか？」の[OK]をクリックします



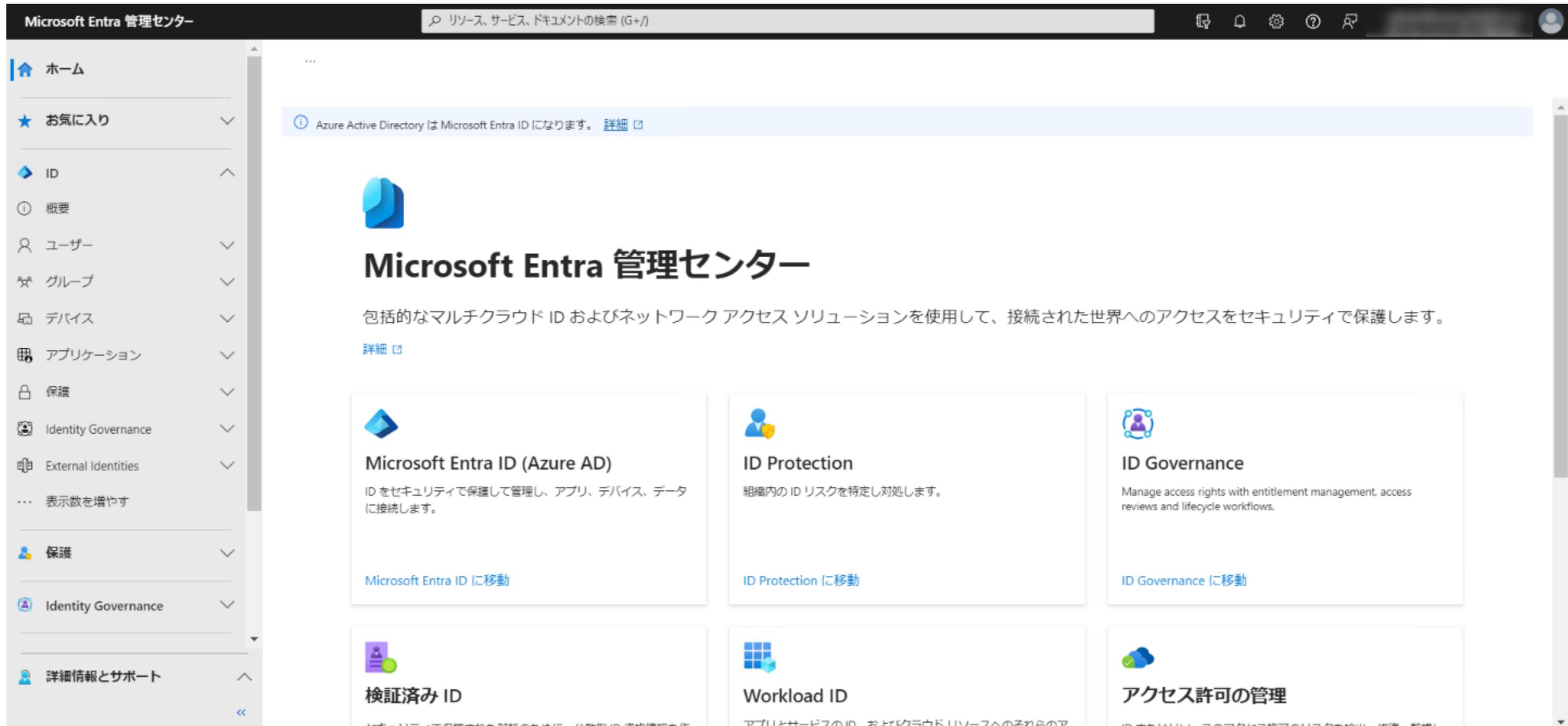
# I-2 アカウムの削除方法

5. 「ユーザーの削除成功」が表示されたら完了です



# I-3 ライセンスの割り当て方法

1. Microsoft Entra 管理センター (<https://entra.microsoft.com>) にアクセスします



# I-3 ライセンスの割り当て方法

2.左の[ID]-[ユーザー]をクリックして展開し、[すべてのユーザー]をクリックします

The screenshot shows the Microsoft Entra Management Center interface. On the left, a navigation sidebar is visible with the following items: ホーム (Home), お気に入り (Favorites), ID, 概要 (Overview), ユーザー (Users), **すべてのユーザー** (All Users - highlighted with a red box), 削除済みのユーザー (Deleted Users), ユーザー設定 (User Settings), グループ (Groups), デバイス (Devices), アプリケーション (Applications), 保護 (Protection), Identity Governance, External Identities, and 表示数を増やす (Increase the number of items displayed). The main content area features a search bar at the top, a notification banner for Azure Active Directory, and a central heading for Microsoft Entra Management Center. Below the heading, there are six service tiles: Microsoft Entra ID (Azure AD), ID Protection, ID Governance, 検証済み ID (Verified ID), Workload ID, and アクセス許可の管理 (Access Permissions Management). Each tile includes a brief description and a link to move to that service.

# I-3 ライセンスの割り当て方法

3.ライセンスを割り当てる対象のユーザーをクリックします

The screenshot shows the Microsoft Entra Management Center interface. The left sidebar contains navigation options like 'ホーム', 'お気に入り', 'ID', '概要', 'ユーザー', 'すべてのユーザー', '削除済みのユーザー', 'ユーザー設定', 'グループ', 'デバイス', 'アプリケーション', '保護', 'Identity Governance', 'External Identities', and '詳細情報とサポート'. The main content area shows a list of users under the 'ユーザー' section. A table lists users with columns for '表示名', 'ユーザープリンシパル名', 'ユーザーの種類', 'オンプレミスの...', 'ID', '会社名', and '作成'. The user 'デモ デモユーザー-001' is highlighted with a red box. Other users listed include AP, CO, 大祐, 小研, 小林, and 岡真.

表示名	ユーザープリンシパル名	ユーザーの種類	オンプレミスの...	ID	会社名	作成
AP						
AP						
CO						
デモ デモユーザー-001	demouser001	メンバー	いいえ			
大祐						
小研						
小林						招待
岡真						

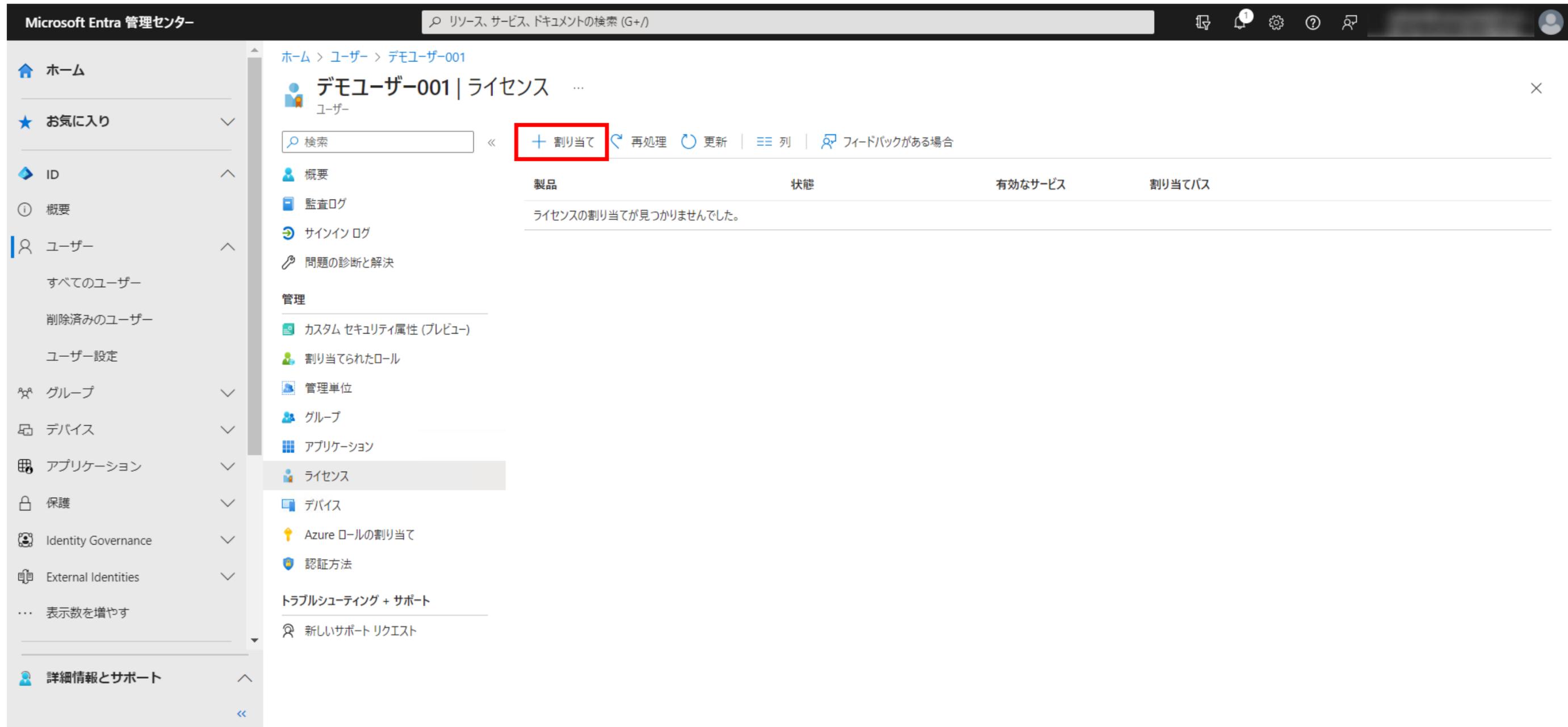
# I-3 ライセンスの割り当て方法

## 4.[ライセンス]をクリックします

The screenshot shows the Microsoft Entra Admin Center interface. On the left, the navigation pane is open, and the 'ユーザー' (Users) section is expanded. The 'ライセンス' (Licenses) option is highlighted with a red rectangular box. The main content area displays the user profile for 'デモユーザー-001'. At the top of the main area, there are action buttons: 'プロパティの編集' (Edit properties), '削除' (Delete), '更新' (Refresh), 'パスワードのリセット' (Reset password), 'セッションの取り消し' (Cancel session), 'ビューの管理' (Manage views), and 'フィードバックがある場合' (If you have feedback). Below these are tabs for '概要' (Overview), '監視中' (Monitoring), and 'プロパティ' (Properties). The '概要' tab is active, showing a '基本情報' (Basic information) section with a user profile card and a table of assigned licenses. The table lists various licenses with their counts, such as 'グループメン...' (2), 'アプリケーシ...' (0), '割り当てられ...' (0), and '割り当て済み...' (0). At the bottom of the page, the URL is visible: `https://entra.microsoft.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade/~/overview/userId/06190c47-7861-40c9-913d-6cc573866391/hidePreviewBanner~/true`.

# I-3 ライセンスの割り当て方法

5.[割り当て]をクリックします



# I-3 ライセンスの割り当て方法

6.割り当てたいライセンス[□]にチェックを入れます



# I-3 ライセンスの割り当て方法

7.[保存]をクリックし、[ライセンスの割り当て成功]と表示されたら完了です

Microsoft Entra 管理センター

ホーム > ユーザー > デモユーザー-001 | ライセンス >

ライセンス割り当ての更新

ユーザーが直接と継承の両方のライセンスを持っている場合、[ライセンス] チェック ボックスをオフにしたときに直接ライセンス割り当てのみが削除されます。継承されたライセンスは、直接割り当てたり、削除したり、ライセンス間でユーザーを移行することもできます。

ライセンスの選択

- Enterprise Mobility + Security E3
- Microsoft 365 Business Premium
- Microsoft Power Automate Free

ライセンス オプションの確認

選択

- Microsoft 365 Business Premium
- Viva Engage Core
- Microsoft Defender for Business
- Viva Learning Seeded
- Windows Update for Business Deployment Service
- Universal Print
- Power Virtual Agents for Office 365
- Common Data Service for Teams
- Project for Office (Plan E5)
- Common Data Service
- Microsoft Azure Multi-Factor Authentication
- Microsoft Defender for Cloud Apps Discovery
- Azure Active Directory Premium P1
- Microsoft Kaizala Pro
- Office Shared Computer Activation
- Whiteboard (Plan 1)

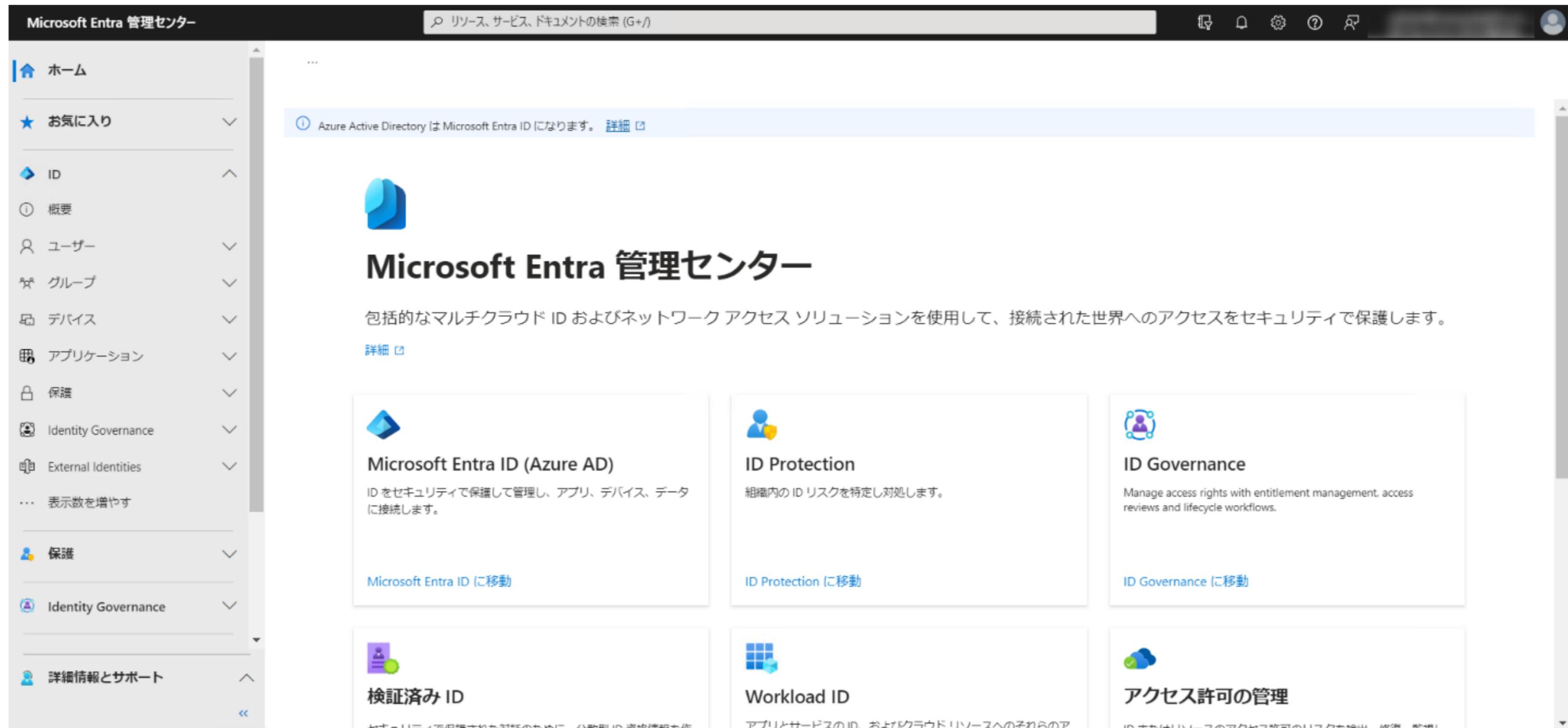
**■ 注意事項**  
**ライセンスの割り当てに成功しなかった場合、9ページに戻って再度設定を実施してください**  
**※利用場所に[日本]が設定されている必要があります**

保存

ライセンスの割り当て成功  
 メンバーへのライセンス割り当てが成功しました。

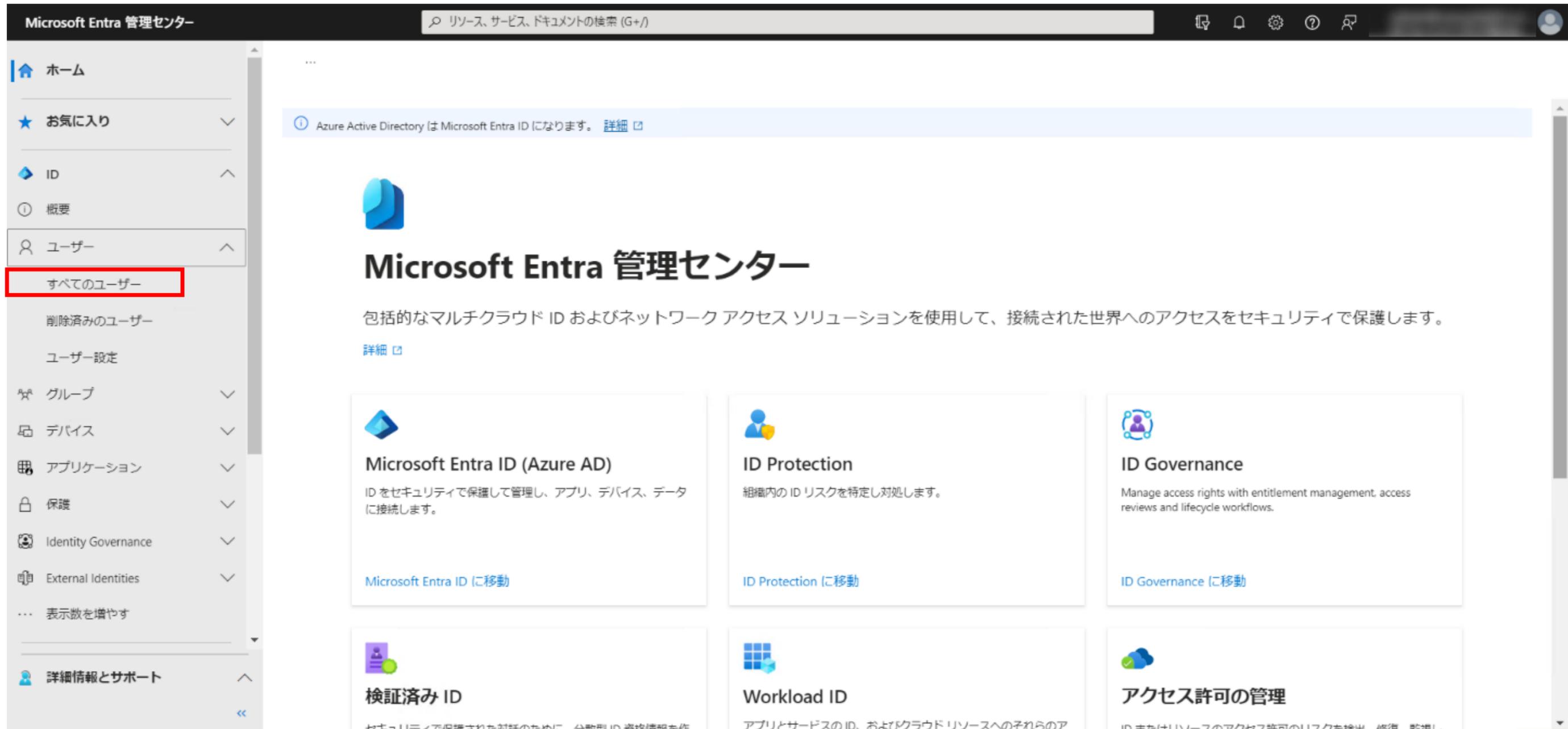
# I-4 ライセンスの割り当てを外す方法

1. Microsoft Entra 管理センター (<https://entra.microsoft.com>) にアクセスします



# I-4 ライセンスの割り当てを外す方法

2.左の[ID]-[ユーザー]をクリックして展開し、[すべてのユーザー]をクリックします



# I-4 ライセンスの割り当てを外す方法

## 3. ライセンスの割り当てを外す対象のユーザーをクリックします

The screenshot shows the Microsoft Entra Management Center interface. The left sidebar contains navigation options like 'ホーム', 'お気に入り', 'ID', '概要', 'ユーザー', 'すべてのユーザー', '削除済みのユーザー', 'ユーザー設定', 'グループ', 'デバイス', 'アプリケーション', '保護', 'Identity Governance', 'External Identities', and '詳細情報とサポート'. The main area displays a list of users under the 'ユーザー' section. A search bar and various action buttons are visible at the top of the user list. The user 'デモ デモユーザー-001' is highlighted with a red box, indicating the target for license removal.

表示名 ↑	ユーザープリンシパル名 ↑	ユーザーの種類	オンプレミスの...	ID	会社名	作成
AP						
AP						
CO						
デモ デモユーザー-001	demouser001	メンバー	いいえ			
大祐						
小研						
小林						招待
岡真						

# I-4 ライセンスの割り当てを外す方法

4.[ライセンス]をクリックします

The screenshot shows the Microsoft Entra Admin Center interface. The left-hand navigation pane is expanded to the 'ユーザー' (Users) section, where the 'ライセンス' (Licenses) option is highlighted with a red box. The main content area displays the user profile for 'デモユーザー-001'. The 'ライセンス' tab is selected, showing a table of assigned licenses. The table has columns for 'ユーザー プリンシパ...' (User Principal Name), 'グループ メン...' (Group Membership), 'オブジェクト ID' (Object ID), '作成日時' (Created Date), 'ユーザーの種類' (User Type), and 'ID'. The table shows 2 group memberships, 0 applications, 0 licenses assigned, and 0 licenses removed.

ユーザー プリンシパ...	グループ メン...	オブジェクト ID	作成日時	ユーザーの種類	ID
	2			割り当てられ...	0
				割り当てられ...	0
				割り当てられ...	0
				割り当てられ...	0

# I-4 ライセンスの割り当てを外す方法

5. 割り当てを外したいライセンスをクリックします

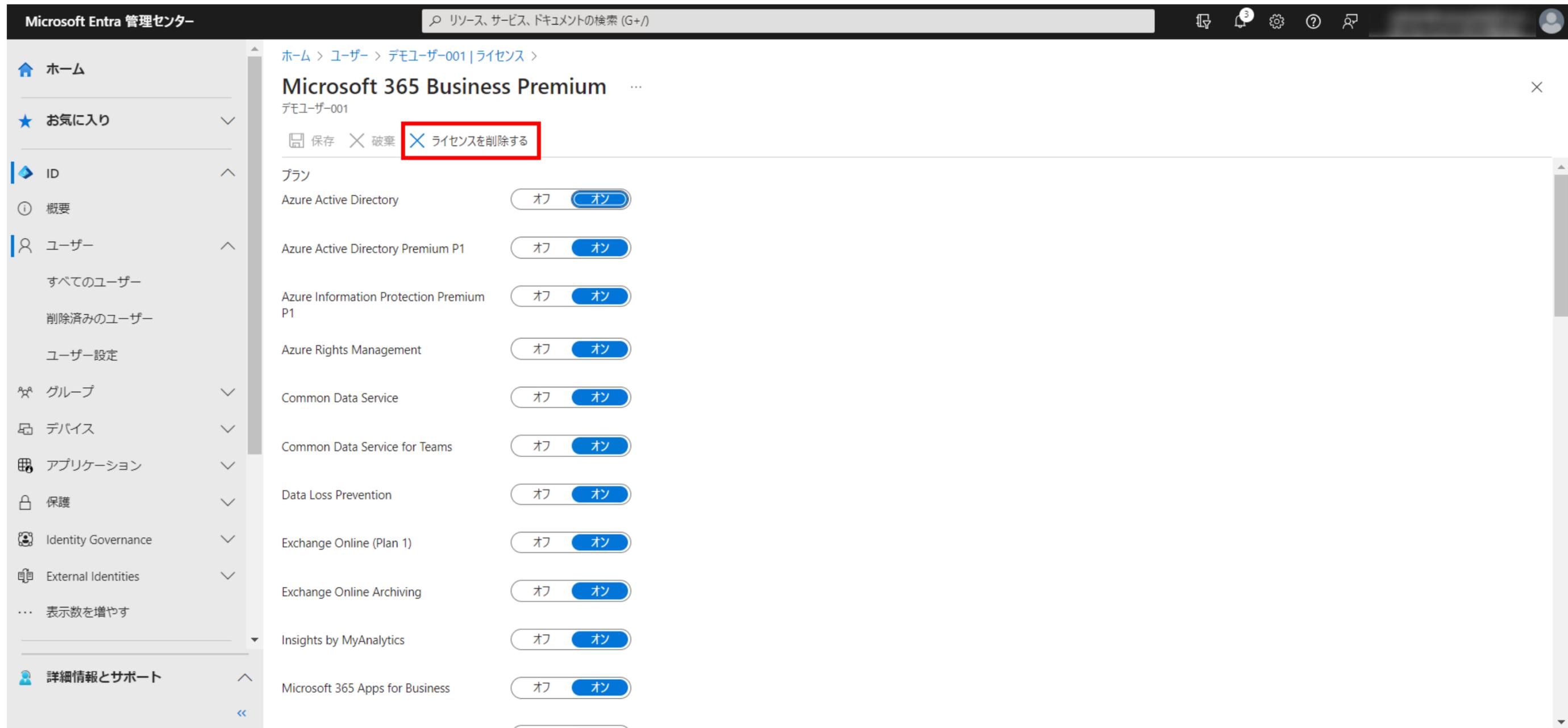
The screenshot shows the Microsoft Entra Management Center interface. The left sidebar contains navigation options like Home, Favorites, ID, Summary, Users, Groups, Devices, Applications, Protection, Identity Governance, External Identities, and Detailed Information and Support. The main content area shows the 'Licenses' page for the user 'デモユーザー-001'. A table lists the assigned licenses:

製品	状態	有効なサービス	割り当てパス
Microsoft 365 Business Premium	アクティブ	42/42	直接

The 'Microsoft 365 Business Premium' license is highlighted with a red box, indicating it is the target for removal.

# I-4 ライセンスの割り当てを外す方法

6.[ライセンスを削除する]をクリックします



# I-4 ライセンスの割り当てを外す方法

7.[はい]をクリックします

The screenshot shows the Microsoft Entra management center interface. The left sidebar contains navigation options: Home, Favorites, ID, Summary, Users, Groups, Devices, Applications, Protection, Identity Governance, External Identities, and Detailed Information and Support. The main content area shows the 'Licenses' page for a user named 'デモユーザ-001'. A modal dialog titled 'ライセンスを削除する' (Remove license) is displayed, with the text '直接ライセンス割り当てが削除されます。' (Direct license assignment will be deleted). The 'はい' (Yes) button is highlighted with a red box, indicating the next step in the process. Below the dialog, a list of services with their status (On/Off) is visible:

Service Name	Status
Azure Information Protection Premium P1	オン (On)
Azure Rights Management	オン (On)
Common Data Service	オン (On)
Common Data Service for Teams	オン (On)
Data Loss Prevention	オン (On)
Exchange Online (Plan 1)	オン (On)
Exchange Online Archiving	オン (On)
Insights by MyAnalytics	オン (On)
Microsoft 365 Apps for Business	オン (On)

# I-4 ライセンスの割り当てを外す方法

6.[ライセンスの割り当て成功]と表示されたら完了です

※作業直後はライセンスが割り当てた状態が表示されていますが、[更新]をクリックすると割り当て解除されています

Microsoft Entra 管理センター

ホーム > ユーザー > デモユーザー-001

デモユーザー-001 | ライセンス

検索

+ 割り当て 再処理 **更新** 列 フィードバックがある場合

製品	状態	有効なサービス	割り当てパス
Microsoft 365 Business Premium	アクティブ	42/42	直接

通知: 割り当てが削除されました  
1件のライセンス割り当てが削除されました。

# Ⅱ.ユーザーがパスワードを忘れてしまった場合の対処

## 1.ユーザーのパスワードのリセット方法

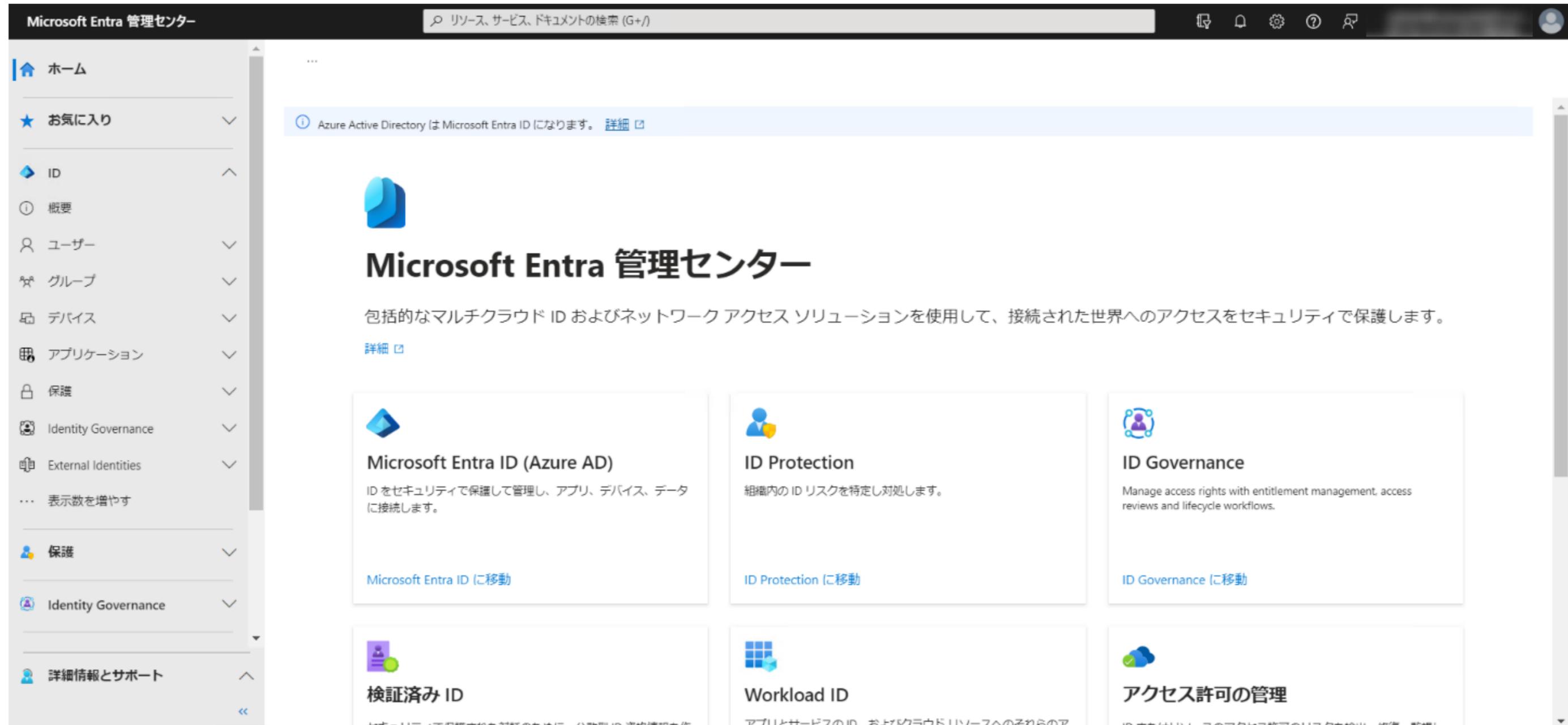
## II-1 ユーザーのパスワードのリセット方法

本項目では、管理者によるユーザーのパスワードリセットを実施する手順を記載しておりますが、本サービスでは、セルフパスワードリセット機能を有効化しているため、管理者の介在なく、ユーザーご自身にてパスワードリセットを実施することも可能です。

ユーザーご自身によるセルフパスワードリセットの方法については、ユーザーマニュアルに記載がございますので、必要に応じて、こちらをご案内ください。

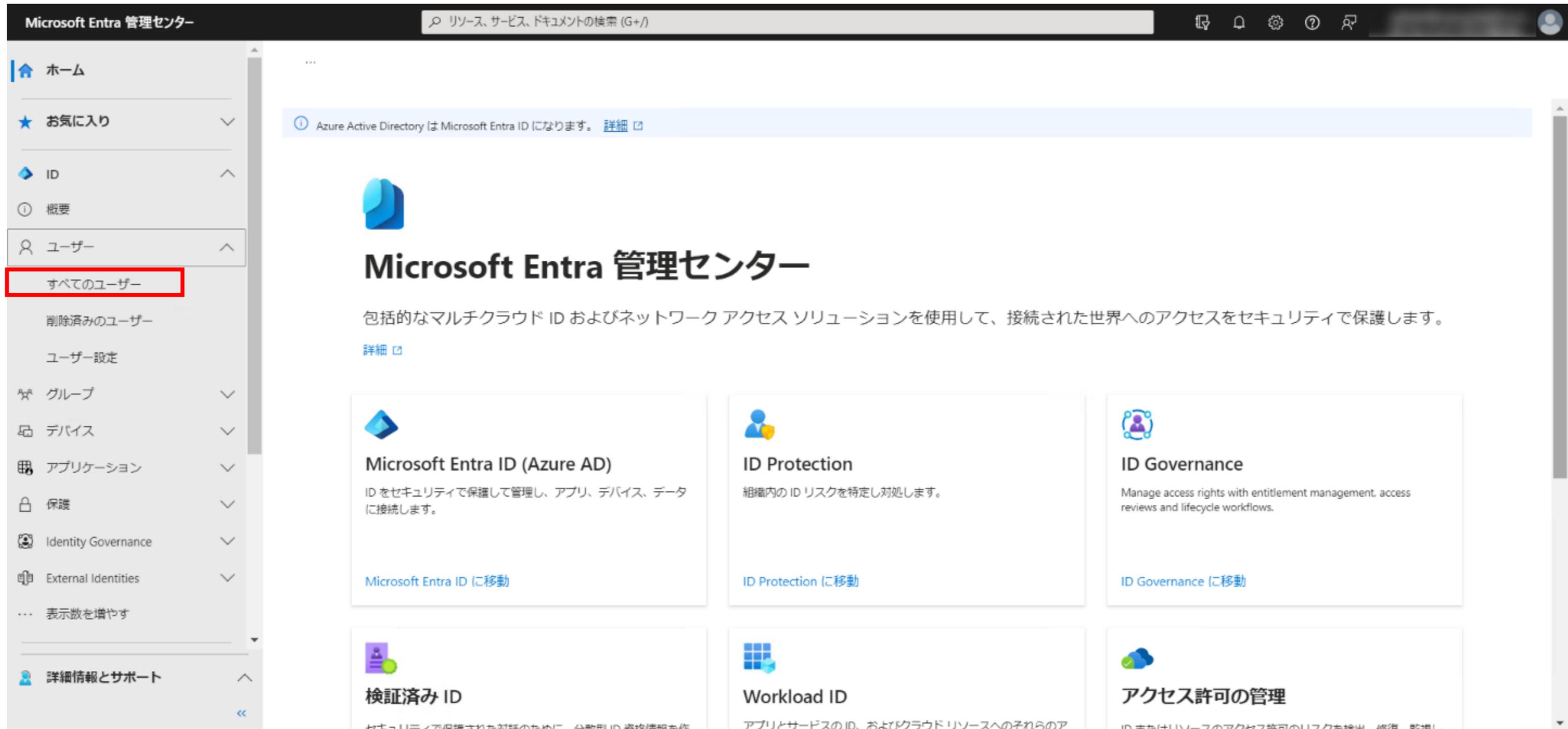
# II-1 ユーザーのパスワードのリセット方法

1. Microsoft Entra 管理センター (<https://entra.microsoft.com>) にアクセスします



# II-1 ユーザーのパスワードのリセット方法

2.左の[ID]-[ユーザー]をクリックして展開し、[すべてのユーザー]をクリックします



# II-1 ユーザーのパスワードのリセット方法

## 3. パスワードをリセットするユーザーをクリックします

The screenshot shows the Microsoft Entra management center interface. The left sidebar contains navigation options like 'ホーム', 'お気に入り', 'ID', '概要', 'ユーザー', 'すべてのユーザー', '削除済みのユーザー', 'ユーザー設定', 'グループ', 'デバイス', 'アプリケーション', '保護', 'Identity Governance', 'External Identities', and '詳細情報とサポート'. The main area displays a list of users under the heading 'ユーザー'. A search bar and various action buttons are visible at the top of the list. The user 'デモ デモユーザー-001' is highlighted with a red box, indicating the step of selecting the user for password reset.

表示名 ↑	ユーザープリンシパル名 ↑	ユーザーの種類	オンプレミスの...	ID	会社名	作成
AP						
AP						
CO						
デモ デモユーザー-001	demouser001	メンバー	いいえ			
大祐						
小研						
小林						招待
岡真						

# II-1 ユーザーのパスワードのリセット方法

4.[パスワードのリセット]をクリック、ポップアップに表示される[パスワードのリセット]をクリックします

The screenshot shows the Microsoft Entra Management Center interface. The left sidebar contains navigation options like 'ホーム', 'お気に入り', 'ID', '概要', 'ユーザー', 'グループ', 'デバイス', 'アプリケーション', '保護', 'Identity Governance', 'External Identities', and '詳細情報とサポート'. The main content area displays the user profile for 'デモユーザー-001'. At the top of the user profile, there are action buttons: 'プロパティの編集', '削除', '更新', 'パスワードのリセット', 'セッションの取り消し', and 'ビューの管理'. The 'パスワードのリセット' button is highlighted with a red box. A modal window titled 'パスワードのリセット' is open on the right, showing instructions and a 'パスワードのリセット' button, which is also highlighted with a red box.

# II-1 ユーザーのパスワードのリセット方法

5.パスワードがリセットされ、一時パスワードが表示されるので、メモします

6.パスワードリセットされたユーザーに、一時パスワードをお伝えください

※ユーザーは一時パスワード入力後、新規パスワードを設定するよう促されます

The screenshot shows the Microsoft Entra Admin Center interface. On the right, a 'パスワードのリセット' (Reset Password) pane is open for the user 'demo-user-001'. A green notification states 'パスワードがリセットされました' (Password has been reset). Below this, a text box displays the temporary password 'Danu5310', which is highlighted with a red box. A pink callout box points to this temporary password with the text: '一時パスワードをユーザーに通知していただく必要があります' (You need to notify the user of the temporary password).

# (参考) パスワードポリシー

ユーザーが設定するパスワードは、以下の必要条件を満たす必要があります

プロパティ	必要条件
使用できる文字	大文字 (A から Z) 小文字 (a から z) 数字 (0 から 9) 記号: - @ # \$ % ^ & * - _ ! + = [ ] { }   ¥ : ' , . ? / ` ~ " ( ) ; < > - 空白
使用できない文字	Unicode 文字
パスワードの長さ	パスワードに必要な条件 - 最小 8 文字 - 最大 256 文字
パスワードの複雑さ	パスワードには、次の 4 つのカテゴリのうち 3 つが必要です。 - 大文字 - 小文字 - 数字 - 記号
最近使用されていないパスワード	ユーザーが自分のパスワードを変更またはリセットする場合、新しいパスワードを、現在のパスワードや最近使用したパスワードと同じにすることはできません。
単純なパスワード	既知の脆弱なパスワードやそのバリエーションを検出してブロックします 例) Password1234 など

《引用元》

パスワード ポリシーの組み合わせと、Azure Active Directory での脆弱なパスワードのチェック | Microsoft Docs  
<https://docs.microsoft.com/ja-jp/azure/active-directory/authentication/concept-password-ban-bad-combined-policy>

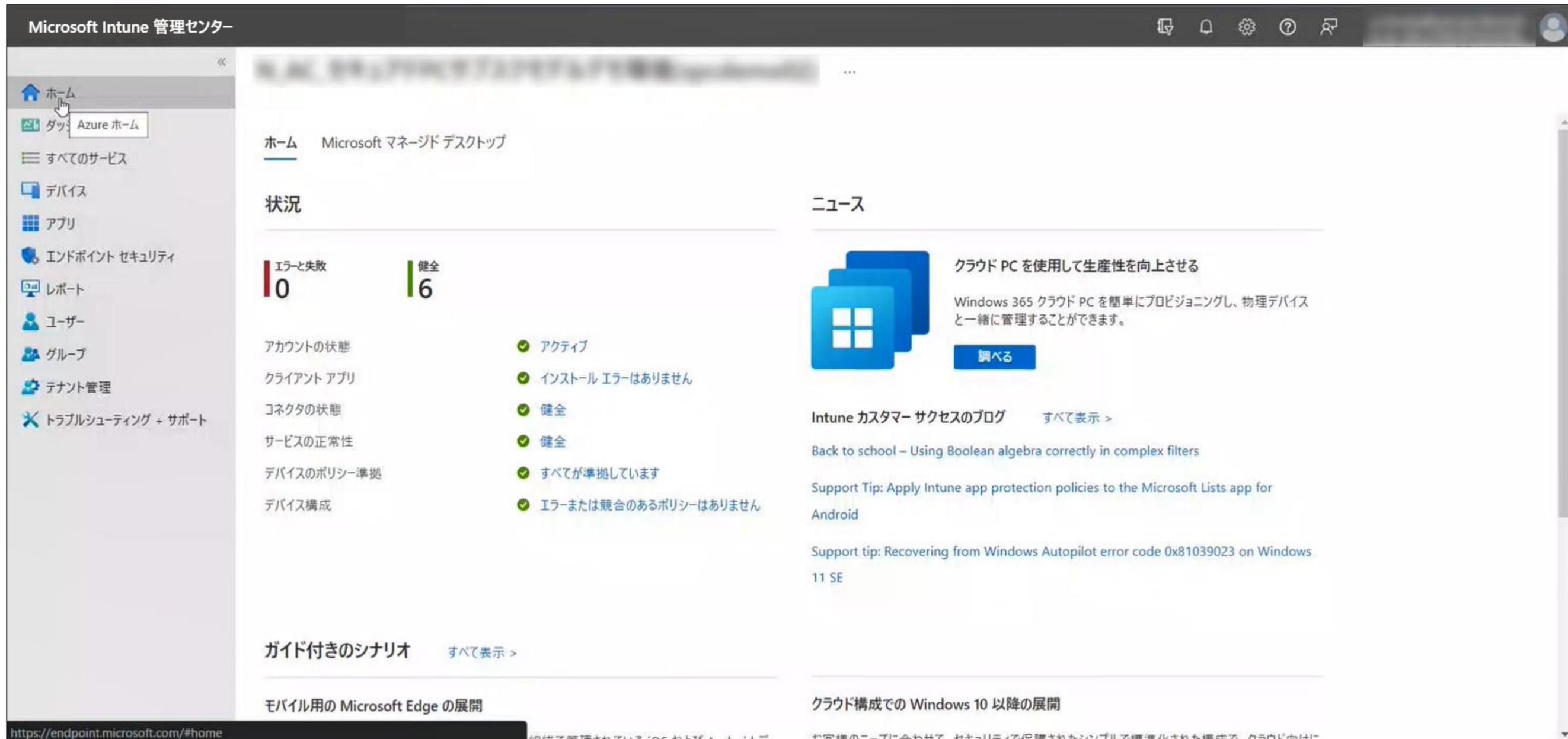
## Ⅲ. 端末のユーザーが変更となった時の対処

端末のユーザーが変わる際には、端末から既存ユーザーのファイルや設定等を削除し、リセットする必要があります。ここでは、管理者から端末を遠隔でリセットする手順を説明します。

管理者の操作が完了後、リセットする端末側で再起動する必要があります。

# Ⅲ-1 端末のリセット、及び新規ユーザーのログイン

1. Microsoft Intune 管理センター (<https://intune.microsoft.com/>) にアクセスします



# Ⅲ-1 端末のリセット、及び新規ユーザーのログイン

2.[デバイス]をクリックし、[すべてのデバイス]をクリックします

The screenshot shows the Microsoft Intune management center interface. The left sidebar contains a navigation menu with the following items: ホーム, ダッシュボード, すべてのサービス, デバイス (highlighted with a red box), アプリ, エンドポイントセキュリティ, レポート, ユーザー, グループ, テナント管理, and トラブルシューティング + サポート. The main content area is titled 'デバイス | 概要' and includes a search bar and a sub-menu where 'すべてのデバイス' is highlighted with a red box. The main content area displays a table of registered devices, a bar chart of OS registration failures, and a table of top registration errors.

プラットフォーム	デバイス
Windows	1
Android	0
iOS/iPadOS	0
macOS	0
Windows Mobile	0
合計	1

OS	登録失敗数
iOS	0
macOS	0
Android	0
Windows	0
Windows Mobile	0

エラー	カウント
表示するデータはありません	

# Ⅲ-1 端末のリセット、及び新規ユーザーのログイン

3.登録されているデバイスの一覧が表示されるので、リセットする端末の[デバイス名]をクリックします

Microsoft Intune 管理センター

ホーム > デバイス

デバイス | すべてのデバイス ...

検索 (Ctrl+/)

最新の情報 | フィルター | 列 | エクスポート | デバイスの一括操作

検索

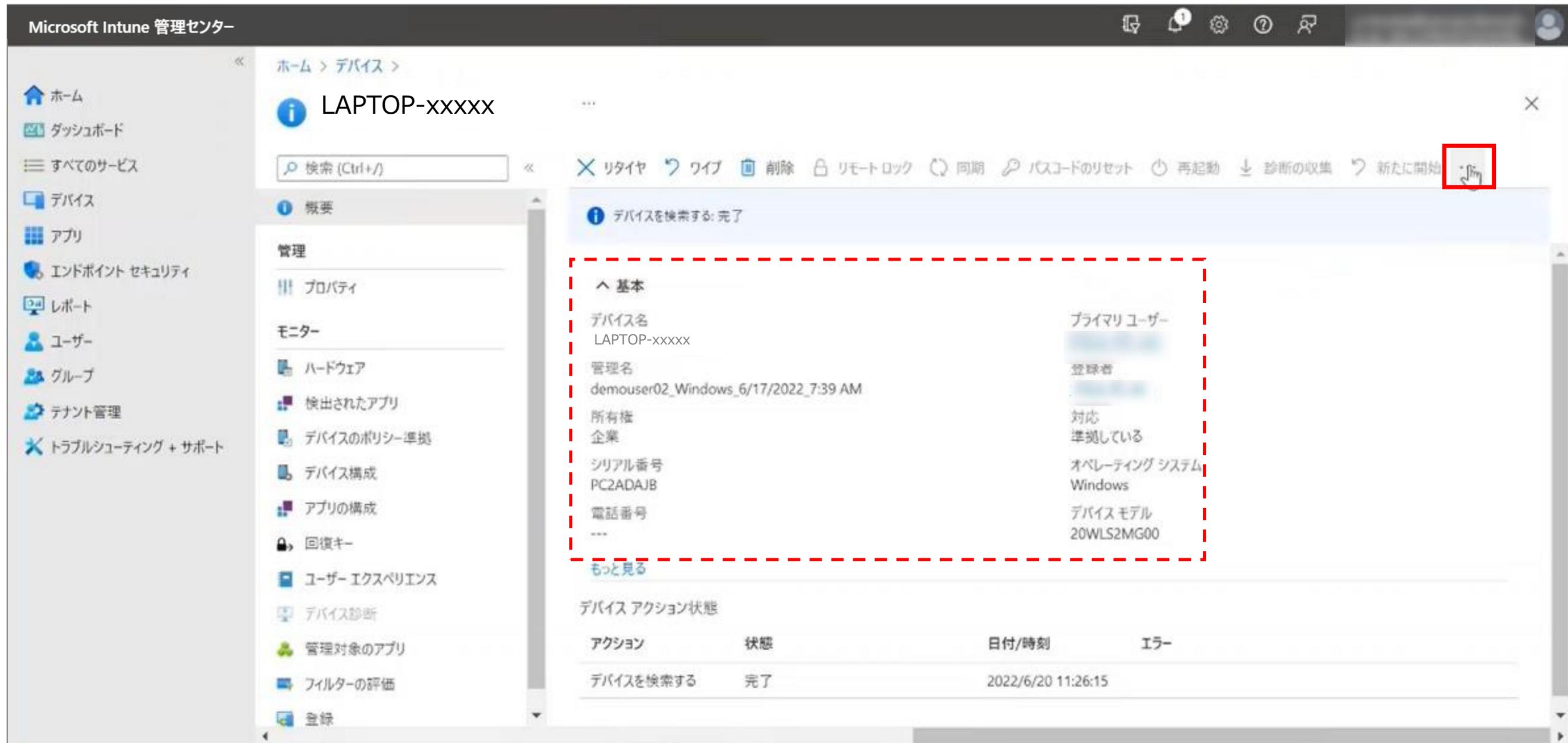
2件中 1 ~ 2 件のレコードを表示しています

デバイス名 ↑↓	管理者 ↑↓	所有権 ↑↓	対応 ↑↓	OS	OS のバージョン ↑↓	最後のチェックイン ↑↓	プライマリユーザーの...
LAPTOP-xxxxx	Intune	企業	✔ 準拠している	Windows	10.0.19043.1706	2022/6/21 14:14:02	
	Intune	企業	✔ 準拠している	Windows	10.0.19043.1586	2022/6/8 14:01:10	

検索バーで、利用ユーザー名を入力し、端末を検索できます

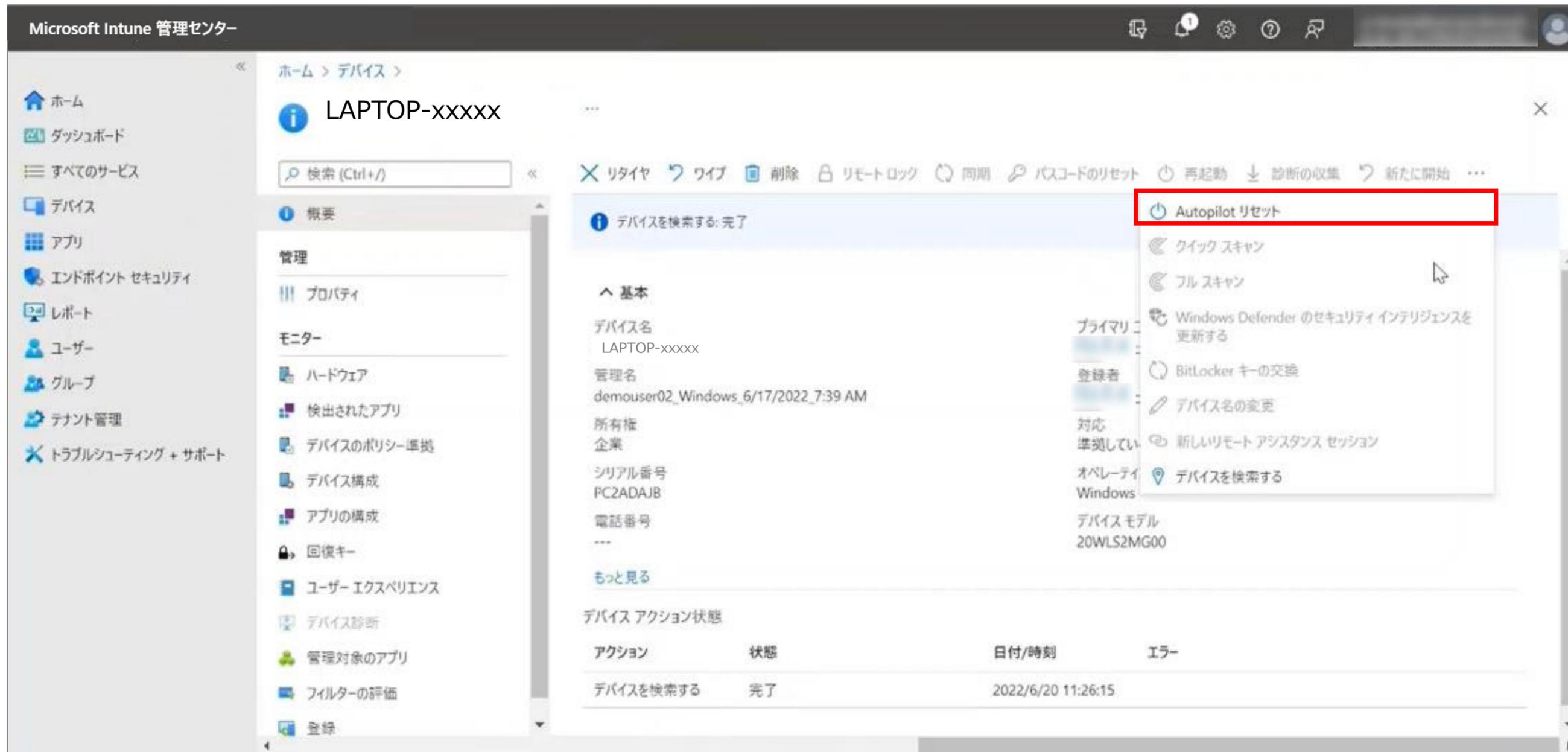
# Ⅲ-1 端末のリセット、及び新規ユーザーのログイン

4.基本情報から、リセットするデバイスで間違いないことを確認し、右上の[...]をクリックします



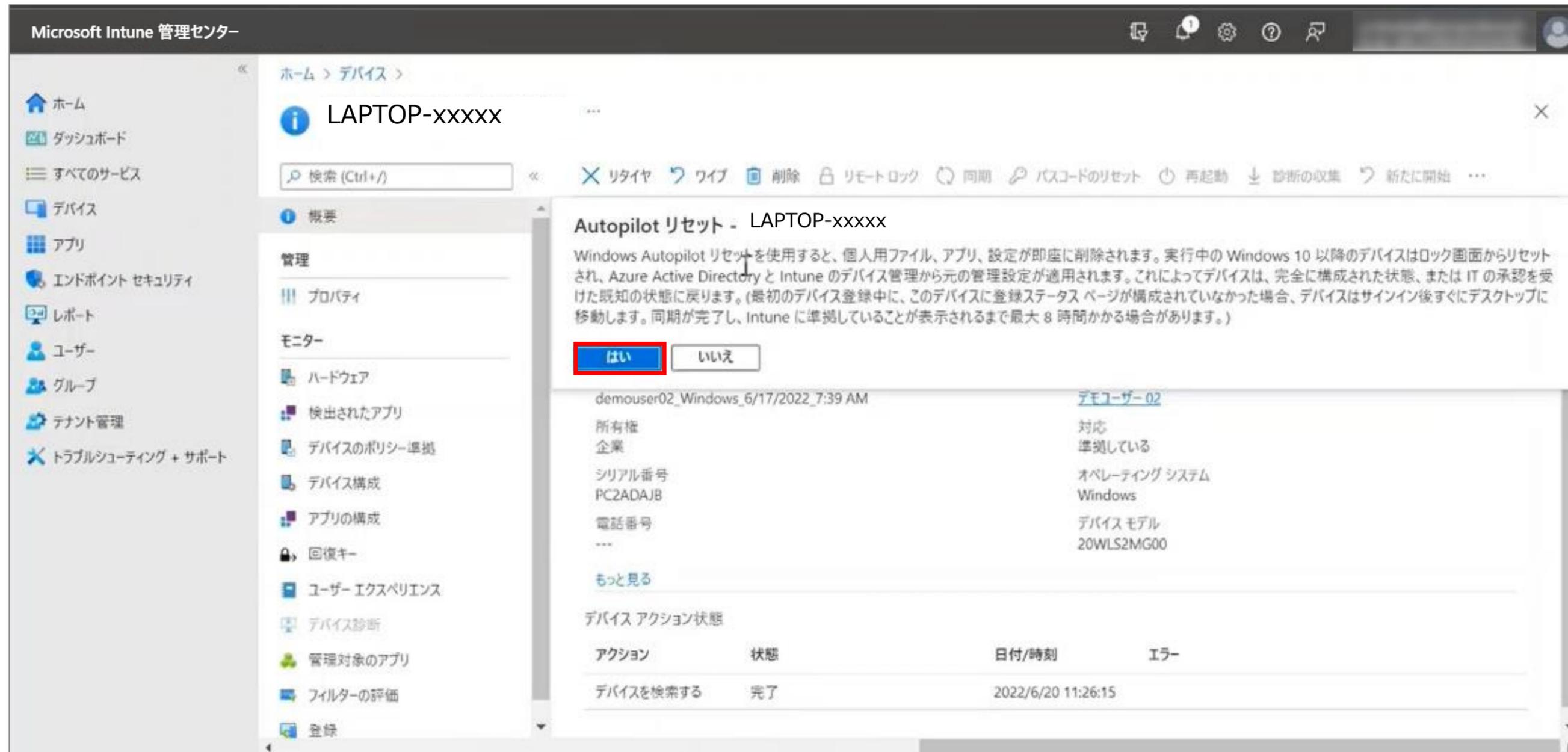
# Ⅲ-1 端末のリセット、及び新規ユーザーのログイン

5. [Autopilot リセット]をクリックします



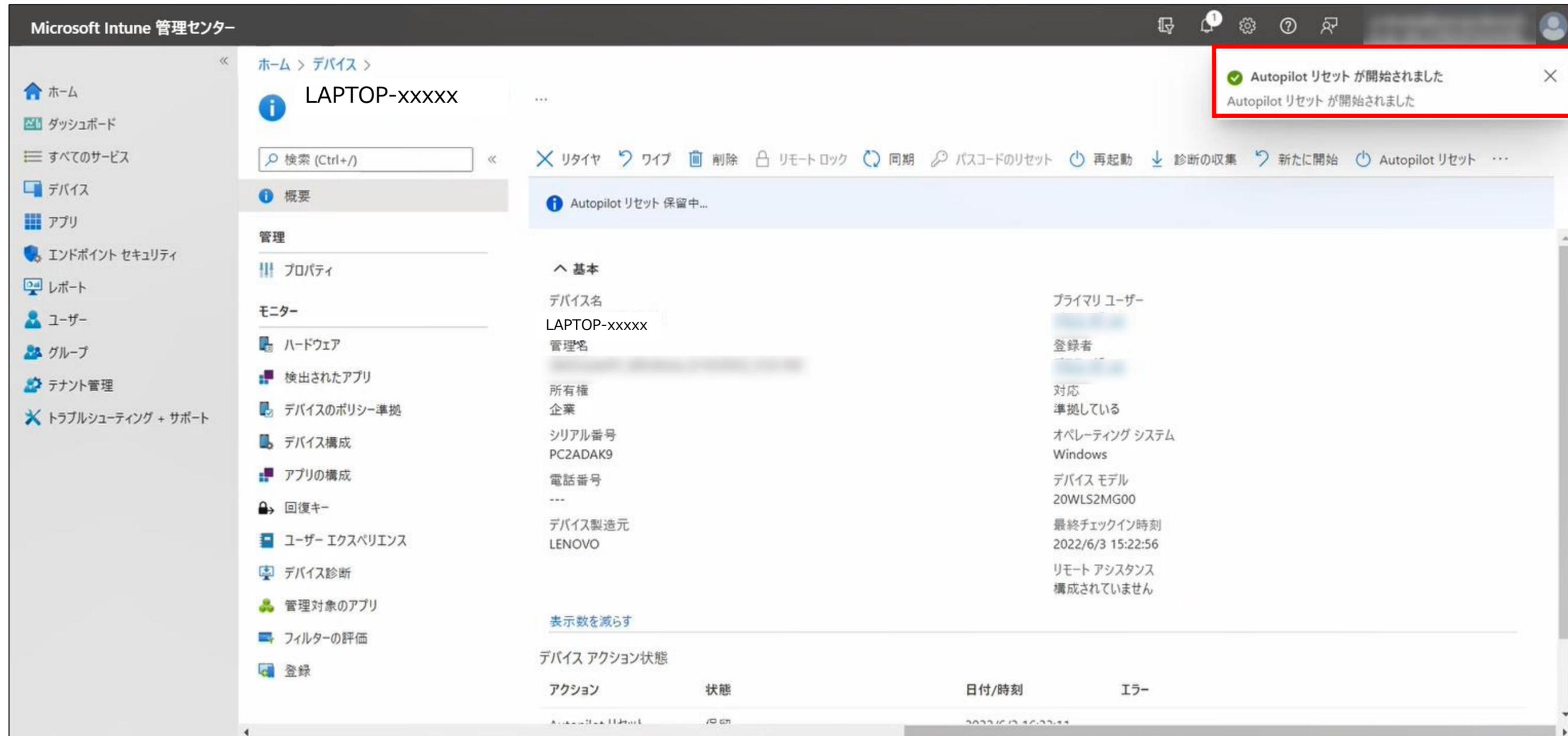
# Ⅲ-1 端末のリセット、及び新規ユーザーのログイン

6. リセットの確認画面が表示されるので、[はい]をクリックします



# Ⅲ-1 端末のリセット、及び新規ユーザーのログイン

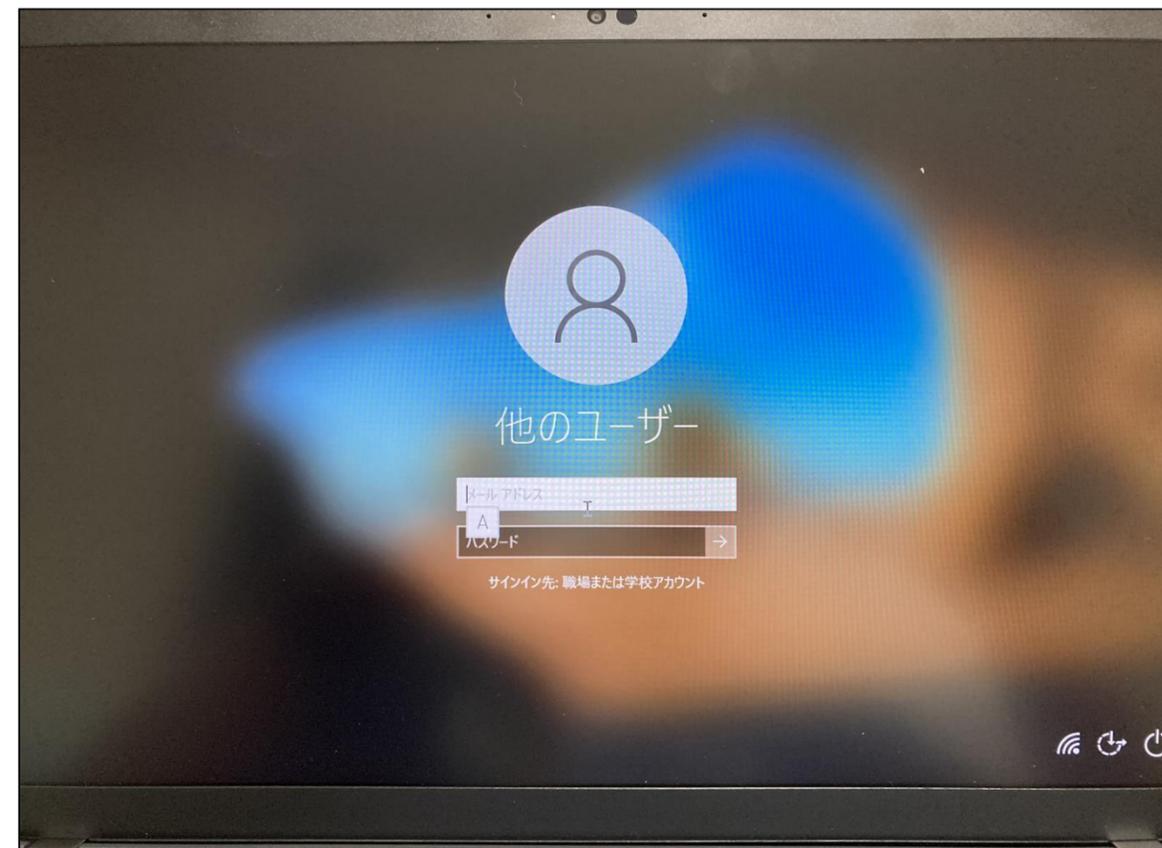
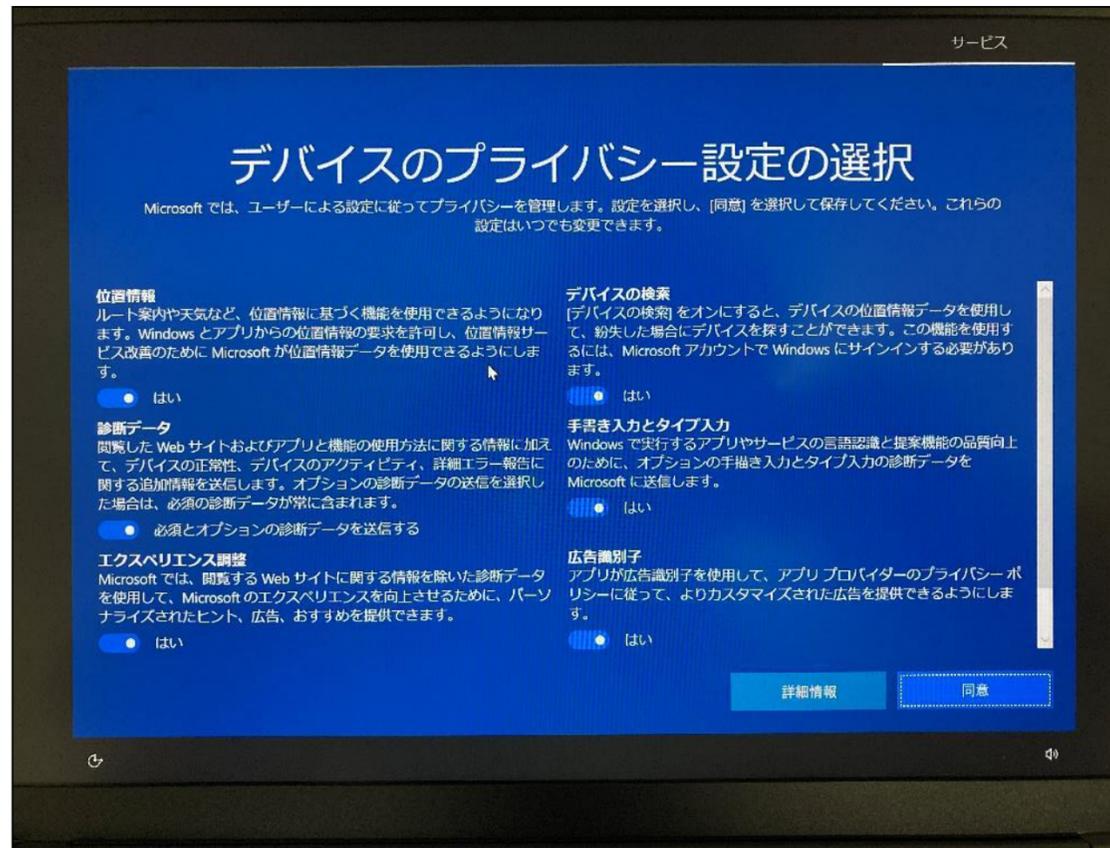
## 7. Autopilotリセットが開始されたことを確認します



# Ⅲ-1 端末のリセット、及び新規ユーザーのログイン

※以降はリセットする端末側での操作になります

- 8.リセットする端末を起動し、端末がインターネットにつながっている状態で10分程度待機します
- 9.Windowsキーから、[電源]>[再起動]を実行すると端末のリセットが始まります  
リセットが始まらない場合は、手順7から再度実施してください
- 10.リセットが完了し、以下の画面が表示されたら、新しいユーザーで利用ができます  
以降は初期設定マニュアルに従って設定が可能です



新しい端末ユーザーのメールアドレス、パスワードを入力してください

# IV.ユーザーにデバイス管理者権限を付与したい場合の対処

1. ローカル管理者ロールの割り当て
2. ローカル管理者ロールの割り当て削除

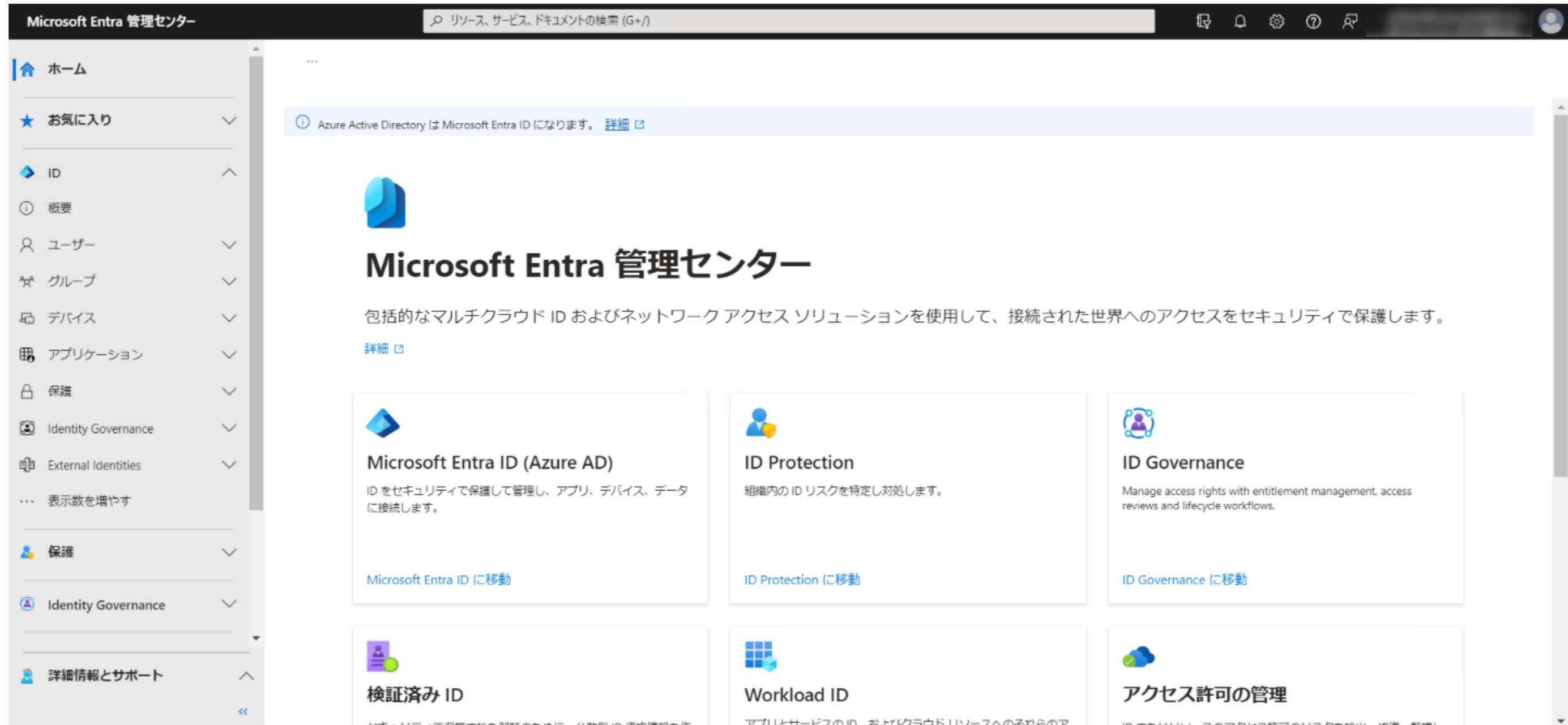
# IV.ユーザーにデバイス管理者権限を付与したい場合の対処

本サービスでは、デバイスのアカウントは標準ユーザーとして提供しております。  
原則、AzureADの管理者ロールが割り当てられていないアカウントは、デバイスの設定変更など  
管理者権限が必要な動作を実行することができません。

本項目を設定することで、ユーザー自身のユーザー名・パスワードで管理者権限が必要な動作を  
実行できるようになります。  
セキュリティの観点から、管理者権限が不要になった際は、権限の割り当て削除を実施することを推奨します。

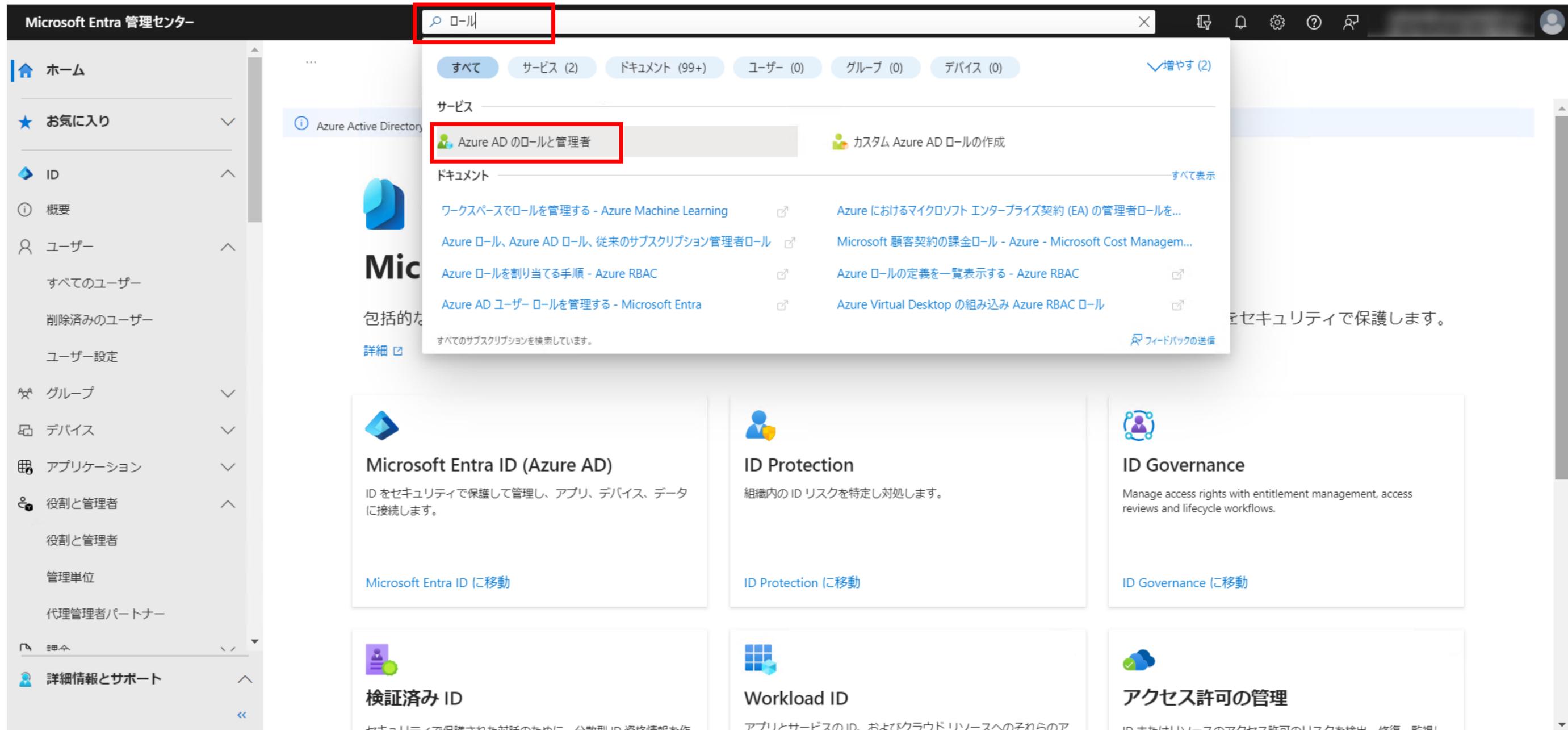
# IV-1 ローカル管理者ロールの割り当て

1. Microsoft Entra 管理センター (<https://entra.microsoft.com>) にアクセスします



# IV-1 ローカル管理者ロールの割り当て

2. 上部の検索欄で「ロール」と検索し、[Azure ADのロールと管理者]をクリックします



# IV-1 ローカル管理者ロールの割り当て

## 3.[Azure AD参加済みデバイスのローカル管理者]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+)

ホーム > **すべてのロール** ...

従業員用の Azure AD

+ 新しいカスタムロール | 削除 カスタムロールの削除 | 割り当てのダウンロード | 更新 | プレビュー機能 | フィードバックがある場合

PIM の使用時に必要となる場合に役割への Just-In-Time アクセスを取得します。PIM に関する詳細をご確認ください →

① **ロール: グローバル管理者**

**管理者ロール**  
 管理者ロールは、Azure AD 内で特権の必要な操作を行うためのアクセス権を付与するために使用されます。アプリケーション構成に関係のない Azure AD の他の部分への管理アクセスを許可せずに、広範なアプリケーション構成アクセス許可への管理アクセスを委任するときに、これらの組み込みロールを使用することをお勧めします。[詳細については、こちらをご覧ください。](#)

[Azure AD ロールベースのアクセス制御に関する詳細情報](#)

名前または説明で検索します フィルター追加

ロール	説明	種類
<input checked="" type="checkbox"/> Azure AD 参加済みデバイスのローカル管理者	このロールに割り当てられているユーザーは、Azure AD 参加済みデバイスのローカル管理者グループに追加されます。	ビルトイン
<input type="checkbox"/> Azure DevOps 管理者	Azure DevOps 組織のポリシーと設定を管理できます。	ビルトイン
<input type="checkbox"/> Azure Information Protection 管理者	Azure Information Protection 製品のすべての側面を管理できます。	ビルトイン
<input type="checkbox"/> B2C IEF キーセット管理者	Identity Experience Framework (IEF) でフェデレーションおよび暗号化のシークレットを管理できます。	ビルトイン
<input type="checkbox"/> B2C IEF ポリシー管理者	Identity Experience Framework (IEF) で信頼フレームワーク ポリシーを作成および管理できます。	ビルトイン
<input type="checkbox"/> Cloud App Security 管理者	Cloud App Security 製品のすべての側面を管理できます。	ビルトイン
<input type="checkbox"/> Desktop Analytics 管理者	デスクトップの管理ツールとサービスにアクセスして管理することができます。	ビルトイン
<input type="checkbox"/> Dynamics 365 管理者	Dynamics 365 製品のすべての側面を管理できます。	ビルトイン
<input type="checkbox"/> Edge 管理者	Microsoft Edge のすべての側面を管理します。	ビルトイン
<input type="checkbox"/> Exchange 受信者管理者	Exchange Online 組織内で Exchange Online 受信者を作成または更新できます。	ビルトイン
<input type="checkbox"/> Exchangeの管理者	Exchange 製品のすべての側面を管理できます。	ビルトイン

# IV-1 ローカル管理者ロールの割り当て

4.[割り当ての追加]をクリックします

Microsoft Entra 管理センター

ホーム > すべてのロール > Azure AD 参加済みデバイスのローカル管理者

Azure AD 参加済みデバイスのローカル管理者 | 割り当て

問題の診断と解決

管理

割り当て

説明

アクティビティ

一括操作の結果

トラブルシューティング + サポート

新しいサポート リクエスト

検索する

名前検索

種類

すべて

名前	ユーザー名	種類	スコープ
ロールの割り当てが見つかりませんでした			

# IV-1 ローカル管理者ロールの割り当て

5.割り当て可能なユーザーやグループが表示されるため、割り当てを行うユーザーの[]を選択し、[追加]をクリックします

The screenshot shows the Microsoft Entra Management Center interface. The main pane displays the 'Assign' dialog for the 'Azure AD 参加済みデバ' role. The dialog includes a search bar and a table of available users and groups. The user 'デモユーザー-001' is selected, and the '追加' (Add) button is highlighted with a red box.

名前	種類	詳細
<input type="checkbox"/> [User Icon]	グループ	[Blurred]
<input type="checkbox"/> [User Icon]	グループ	[Blurred]
<input type="checkbox"/> [User Icon]	グループ	[Blurred]
<input checked="" type="checkbox"/> [User Icon]	ユーザー	デモユーザー-001
<input type="checkbox"/> [User Icon]	グループ	[Blurred]
<input type="checkbox"/> [User Icon]	グループ	[Blurred]
<input type="checkbox"/> [User Icon]	グループ	[Blurred]
<input type="checkbox"/> [User Icon]	グループ	[Blurred]

# IV-1 ローカル管理者ロールの割り当て

6. 割り当てが正常に完了した通知を確認し、作業完了です

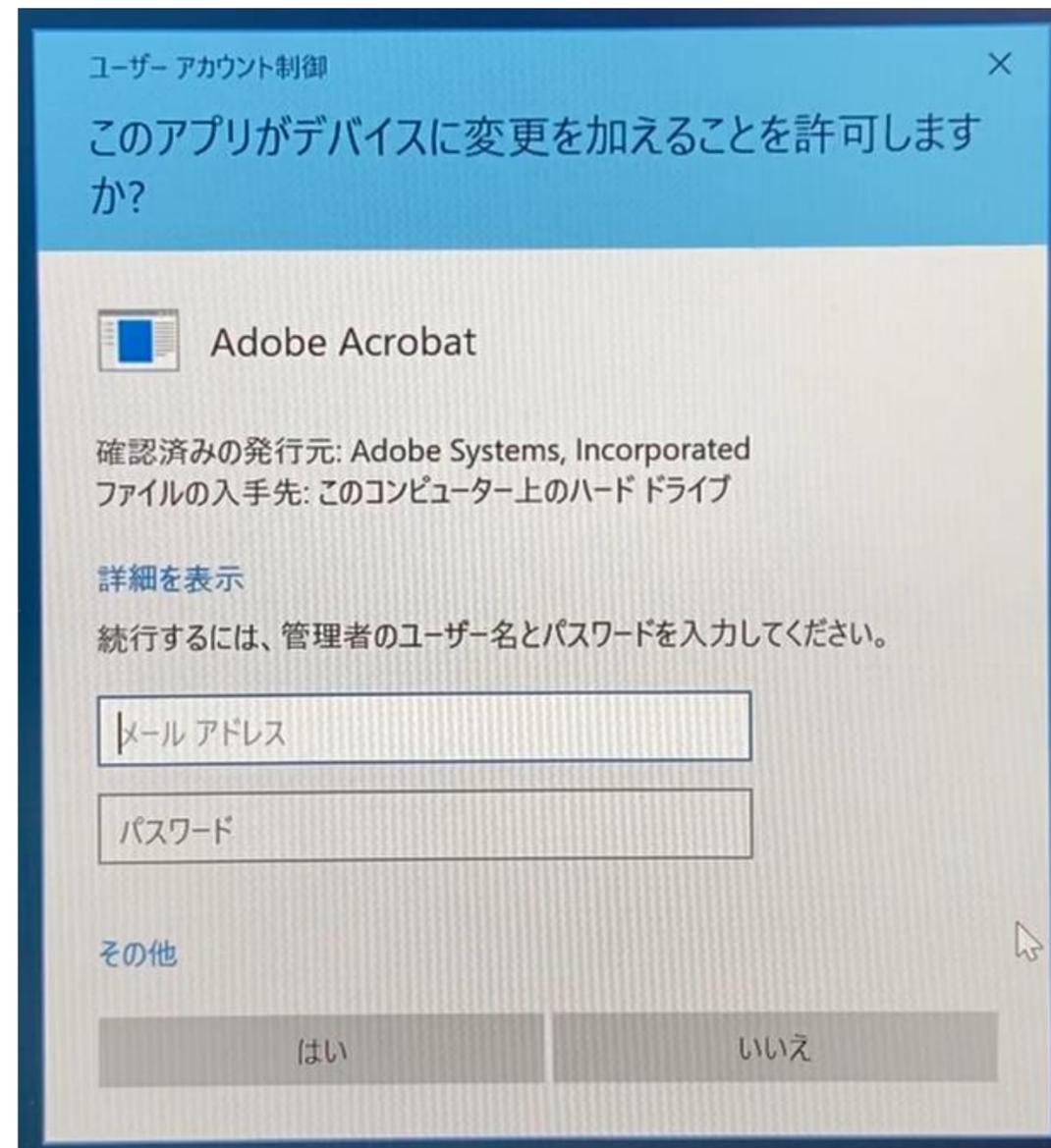
※ 割り当てられたユーザーが実際にローカル管理者として操作できるようになるまで、多少のラグがあります

The screenshot shows the Microsoft Entra Management Center interface. The main content area displays the 'Azure AD 参加済みデバイスのローカル管理者' role assignment page. A notification banner at the top right indicates that the assignment was successful: '割り当てが正常に追加されました' (Assignment added successfully) and '割り当て デモユーザー-001 が正常に追加されました' (Assignment for demo user-001 added successfully). Below this, a table lists the assigned users:

名前	ユーザー名	種類	スコープ
<input type="checkbox"/>	デモユーザー-001	User	ディレクトリ

# 補足 ユーザーへの周知

ローカル管理者ロールを割り当てられたユーザーは、自身のユーザー名とパスワードで各種設定を行うことが可能です。設定をするうえで以下のような画面が表示される場合がございますが、ロールを割り当てられたユーザーの情報で設定を進めることが可能なので、その旨をユーザーにお伝えください。



# IV-2 ローカル管理者ロールの割り当て削除

1.対象のユーザーの[□]を選択し、[割り当ての削除]をクリックすることで管理者ロールを剥奪することができます

The screenshot shows the Microsoft Entra management center interface. The breadcrumb path is: ホーム > すべてのロール > Azure AD 参加済みデバイスのローカル管理者. The main heading is "Azure AD 参加済みデバイスのローカル管理者 | 割り当て". Below the heading, there are action buttons: "+ 割り当ての追加", "X 割り当ての削除" (highlighted with a red box), "↓ 割り当てのダウンロード", "更新", "PIMで管理", and "フィードバックがある場合". A notification banner states: "組み込みのロールをグループに割り当てることもできるようになりました。詳細情報". Below this, there is a search bar with "名前を検索" and a "種類" dropdown menu set to "すべて". A table lists the role assignments:

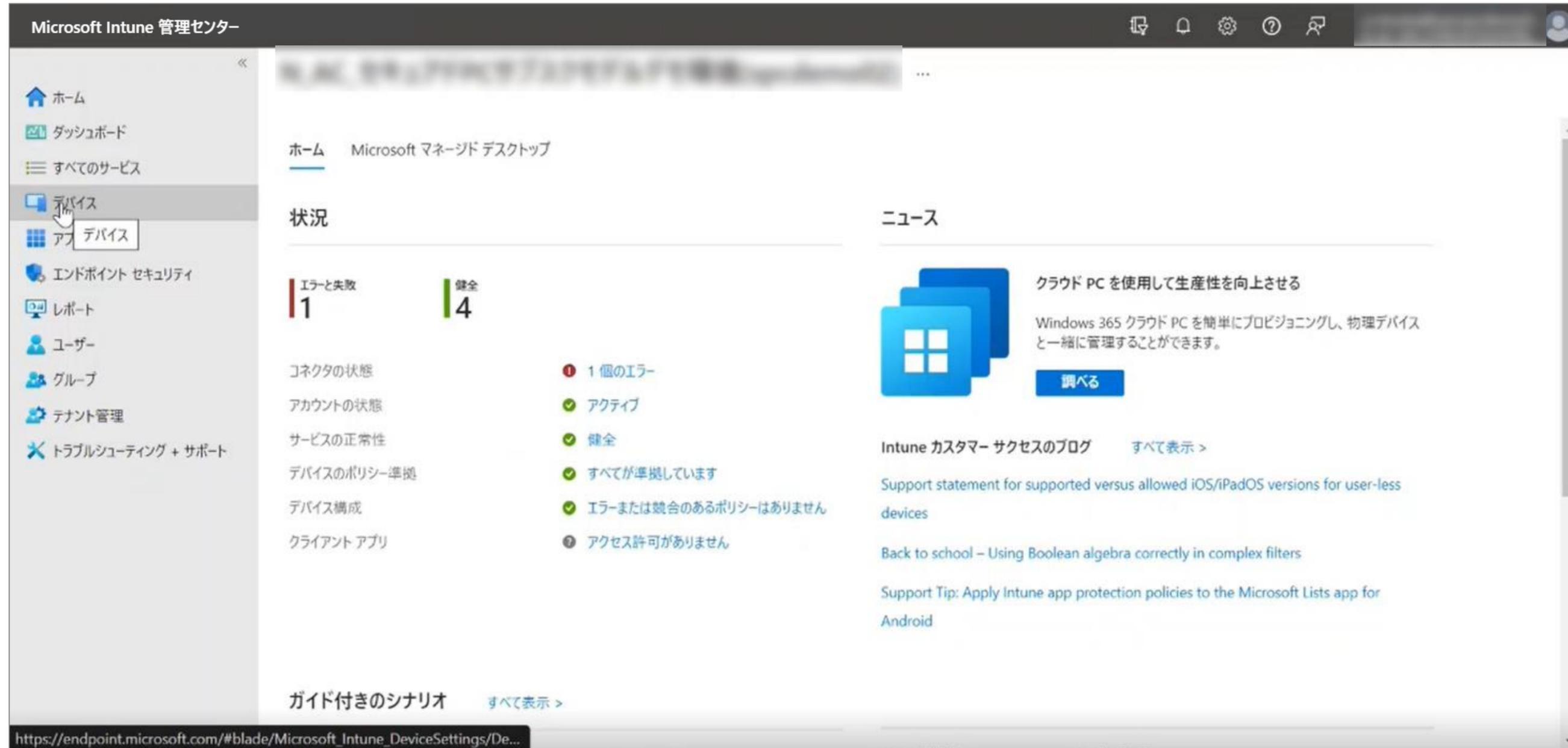
名前	ユーザー名	種類	スコープ
<input checked="" type="checkbox"/> デモユーザー-001		User	ディレクトリ

# V. 端末の盗難や紛失時の対処

1. 端末の位置情報検索
2. 遠隔での端末の初期化

# V-1 端末の位置情報検索

1. Microsoft Intune 管理センター (<https://intune.microsoft.com/>) にアクセスします



# V-1 端末の位置情報検索

2.[デバイス]をクリックし、[すべてのデバイス]をクリックします

The screenshot shows the Microsoft Intune management center interface. On the left sidebar, the 'デバイス' (Devices) menu item is highlighted with a red box. In the main content area, the 'すべてのデバイス' (All Devices) option is also highlighted with a red box. The main content area displays a summary of devices registered in Intune, including a table of device counts by platform and a chart showing OS registration failures over time.

プラットフォーム	デバイス
Windows	1
Android	0
iOS/iPadOS	0
macOS	0
Windows Mobile	0
合計	1

OSによる登録失敗 (OS Registration Failures):

OS	Count
iOS	0
macOS	0
Android	0
Windows	0
Windows Mobile	0

# V-1 端末の位置情報検索

3.登録されているデバイスの一覧が表示されるので、位置検索する端末の[デバイス名]をクリックします

Microsoft Intune 管理センター

ホーム > デバイス

デバイス | すべてのデバイス ...

検索 (Ctrl+/)

最新の情報 | フィルター | 列 | エクスポート | デバイスの一括操作

検索

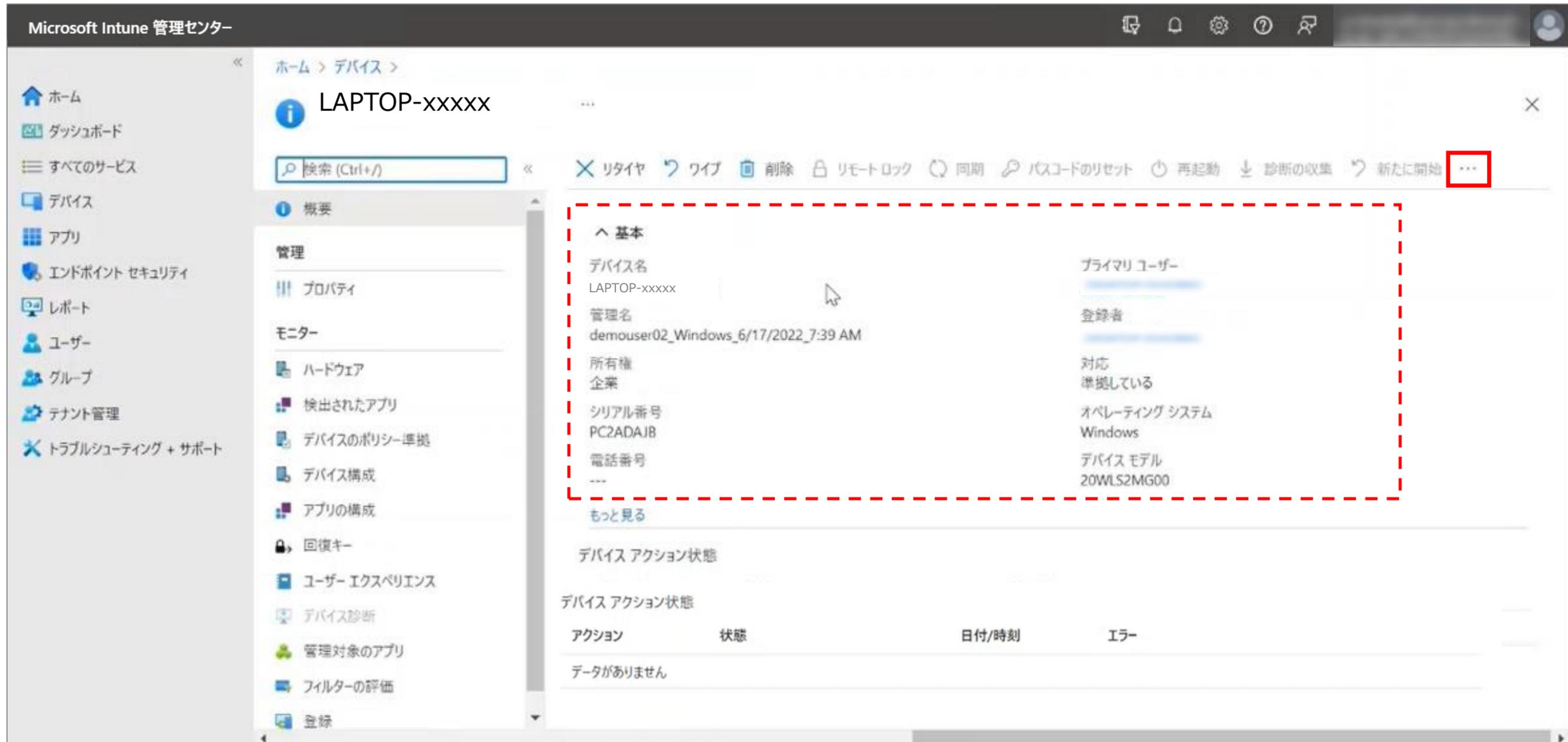
2件中 1 ~ 2 件のレコードを表示しています

デバイス名 ↑↓	管理者 ↑↓	所有権 ↑↓	対応 ↑↓	OS	OS のバージョン ↑↓	最後のチェックイン ↑↓	プライマリユーザーの...
LAPTOP-xxxxx	Intune	企業	✔ 準拠している	Windows	10.0.19043.1706	2022/6/21 14:14:02	
	Intune	企業	✔ 準拠している	Windows	10.0.19043.1586	2022/6/8 14:01:10	

検索バーで、利用ユーザー名を入力し、端末を検索できます

# V-1 端末の位置情報検索

4.基本情報から、位置検索するデバイスで間違いがないことを確認し、右上の[... ]をクリックします



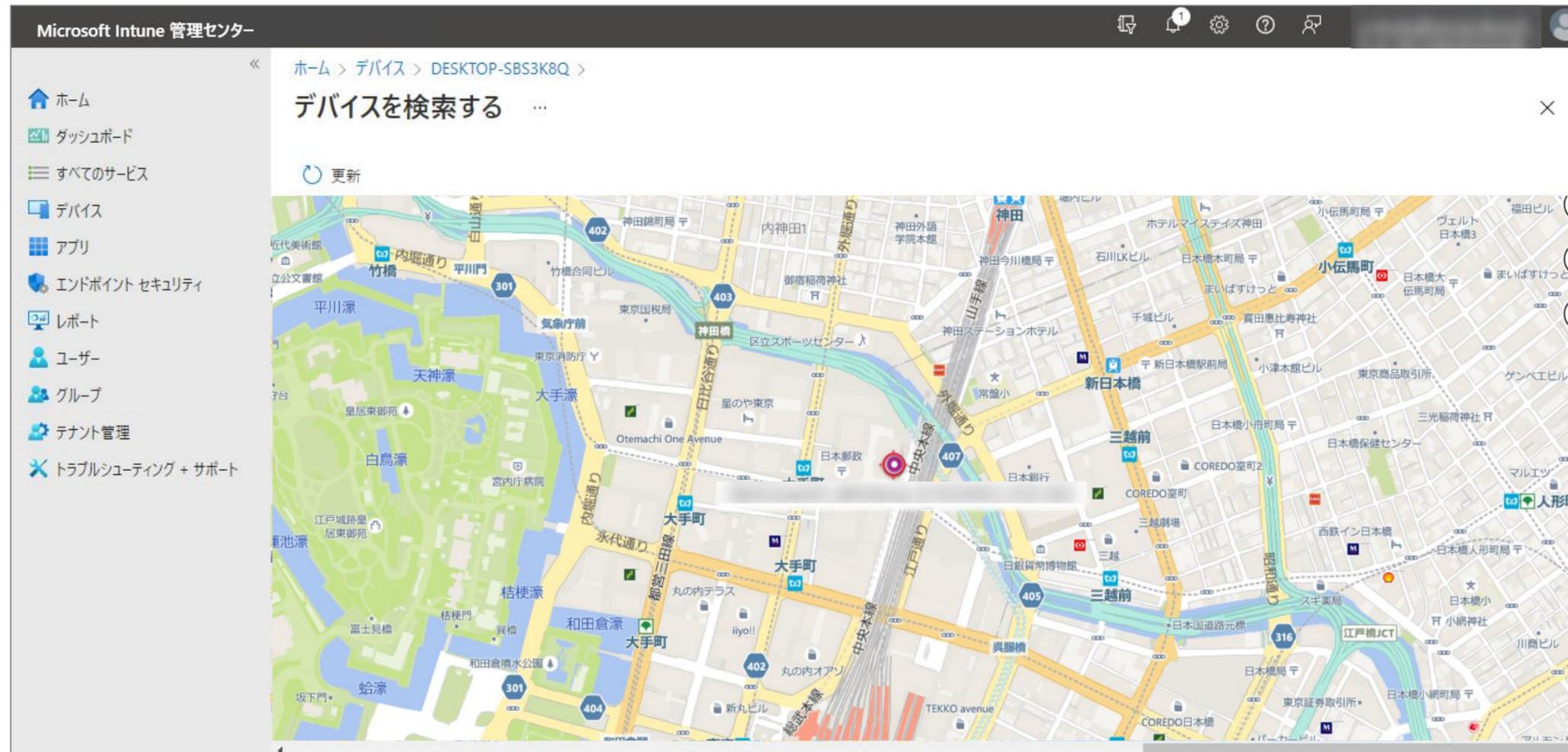
# V-1 端末の位置情報検索

5.[デバイスを検索する]をクリックします

The screenshot shows the Microsoft Intune Management Center interface. The left sidebar contains navigation options like 'ホーム', 'ダッシュボード', 'すべてのサービス', 'デバイス', 'アプリ', 'エンドポイント セキュリティ', 'レポート', 'ユーザー', 'グループ', 'テナント管理', and 'トラブルシューティング + サポート'. The main content area is titled 'LAPTOP-xxxxx' and includes a search bar with the text '検索 (Ctrl+F)'. Below the search bar, there are sections for '概要', '管理', 'プロパティ', and 'モニター'. The 'モニター' section lists various monitoring tasks. A context menu is open over the search bar, listing actions such as 'リタイア', 'ワイプ', '削除', 'リモートロック', '同期', 'パスワードのリセット', '再起動', '診断の収集', '新たに開始', 'Autopilot リセット', 'クイック スキャン', 'フル スキャン', 'Windows Defender のセキュリティ インテリジェンスを 更新する', 'BitLocker キーの交換', 'デバイス名の変更', and '新しいリモート アシスタンス セッション'. The 'デバイスを検索する' option is highlighted with a red box, and a tooltip with the same text is visible below it.

# V-1 端末の位置情報検索

6.しばらくすると、端末の位置情報が地図に表示されます



## 《位置検索が可能な条件》

- 端末の電源が入っていること
- インターネットに接続されている状態であること
- 端末の位置情報がONになっていること

上記が満たされていない場合、端末を検索しても、ステータスは保留中となります。

# V-1 端末の位置情報検索

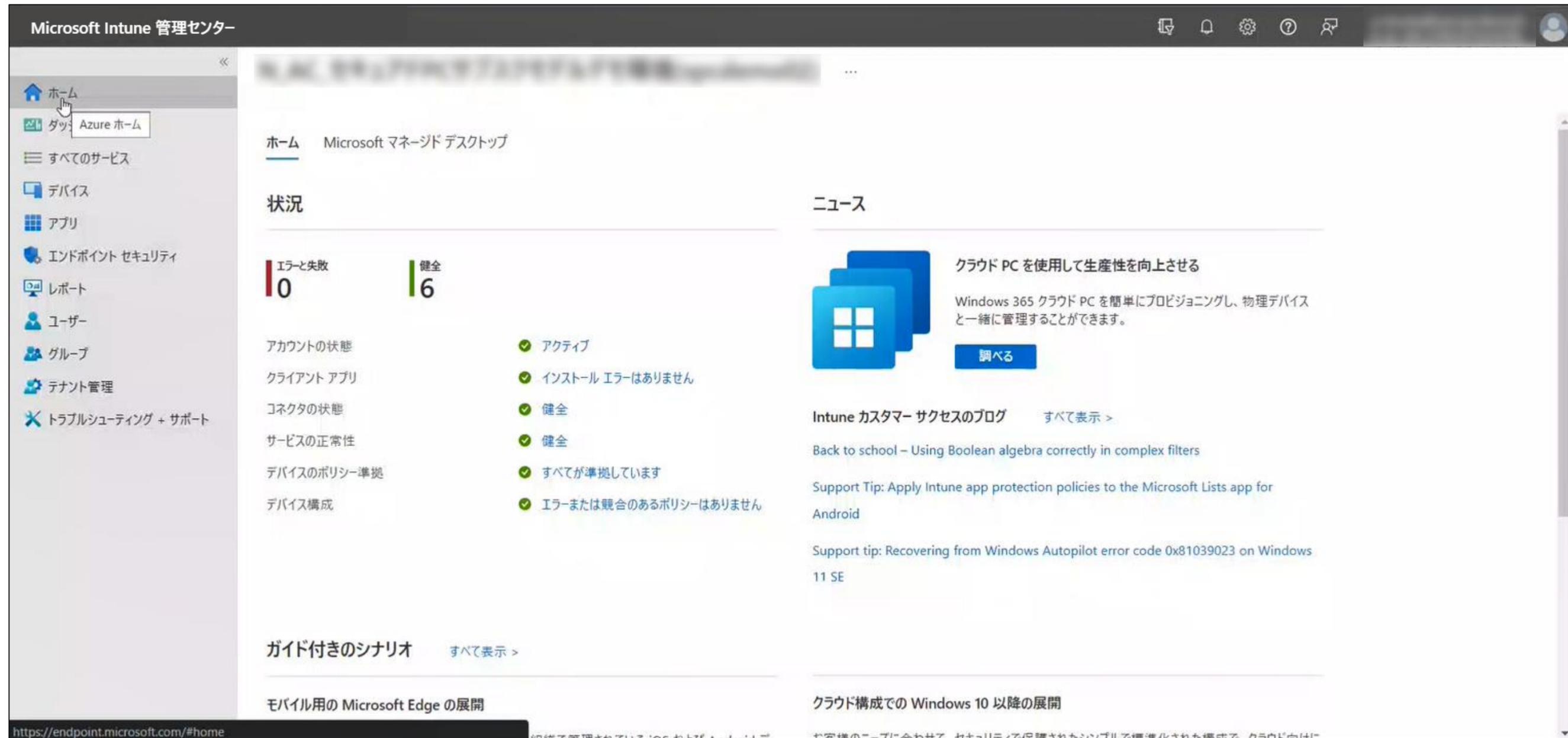
7.検索結果は、[デバイスのアクション状態]から確認することが可能です

The screenshot shows the Microsoft Intune Management Console interface. The left sidebar contains navigation options like 'ホーム', 'ダッシュボード', 'すべてのサービス', 'デバイス', 'アプリ', 'エンドポイントセキュリティ', 'レポート', 'ユーザー', 'グループ', 'テナント管理', and 'トラブルシューティング + サポート'. The main content area is titled 'LAPTOP-xxxxx' and shows a search bar with '検索 (Ctrl+)' and a list of actions: 'リタイア', 'ワイプ', '削除', 'リモートロック', '同期', 'パスワードのリセット', '再起動', '診断の収集', and '新たに開始'. Below this, a notification states 'デバイスを検索する: 完了'. The '基本' (Basic) section lists device details: 'デバイス名: LAPTOP-xxxxx', '管理名: [redacted]', '所有権: 企業', 'シリアル番号: PC2ADAJB', '電話番号: ---', 'プライマリユーザー', '登録者', '対応: 準拠している', 'オペレーティングシステム: Windows', and 'デバイスモデル: 20WLS2MG00'. At the bottom, the 'デバイス アクション状態' (Device Action Status) table is shown with a red box highlighting the search action.

アクション	状態	日付/時刻	エラー
デバイスを検索する	完了	2022/6/20 11:26:15	

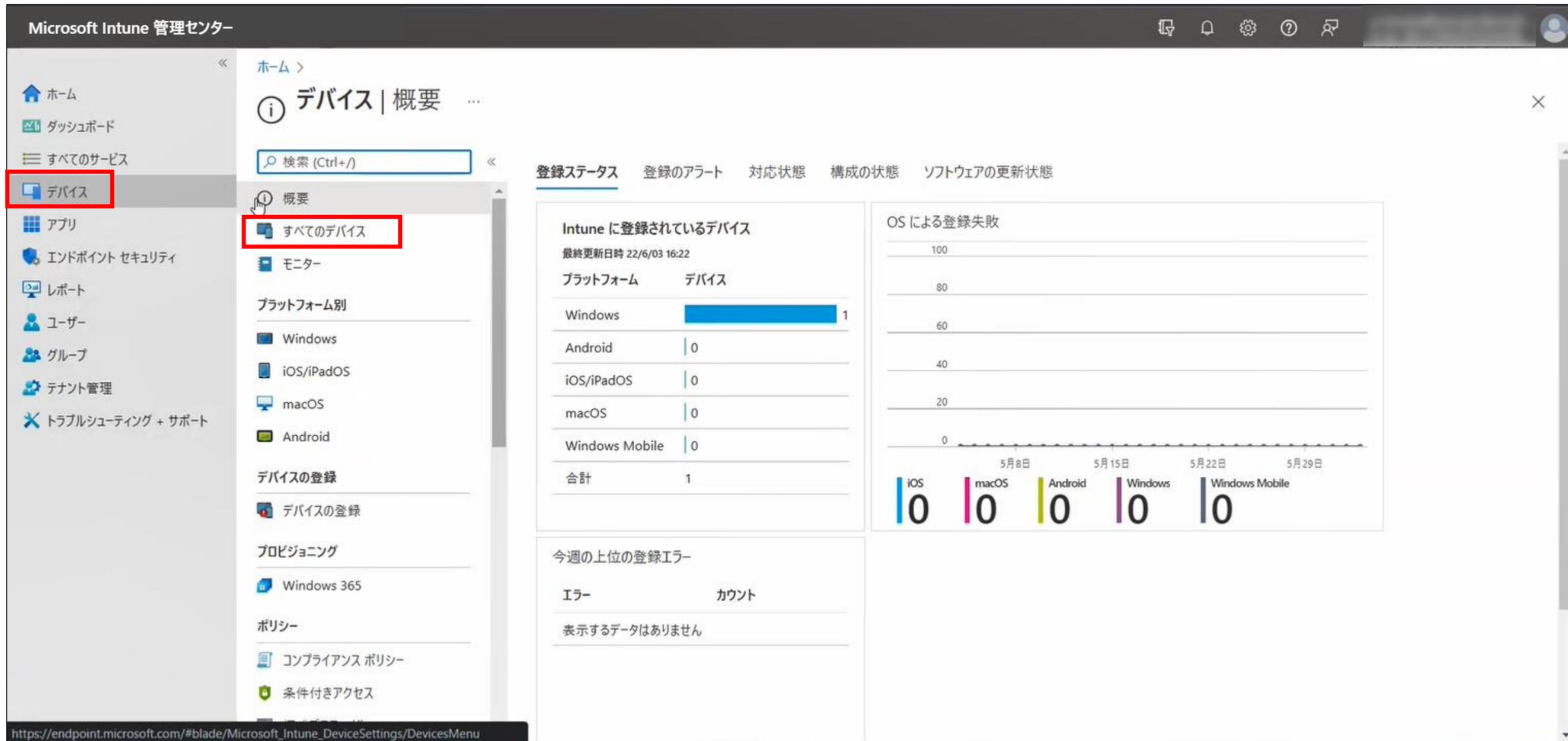
# V-2 遠隔での端末の初期化

1. Microsoft Intune 管理センター (<https://intune.microsoft.com/>) にアクセスします



# V-2 遠隔での端末の初期化

2.[デバイス]をクリックし、[すべてのデバイス]をクリックします



# V-2 遠隔での端末の初期化

3.登録されているデバイスの一覧が表示されるので、リセットする端末の[デバイス名]をクリックします

Microsoft Intune 管理センター

ホーム > デバイス

デバイス | すべてのデバイス ...

検索 (Ctrl+/)

最新の情報 | フィルター | 列 | エクスポート | デバイスの一括操作

検索

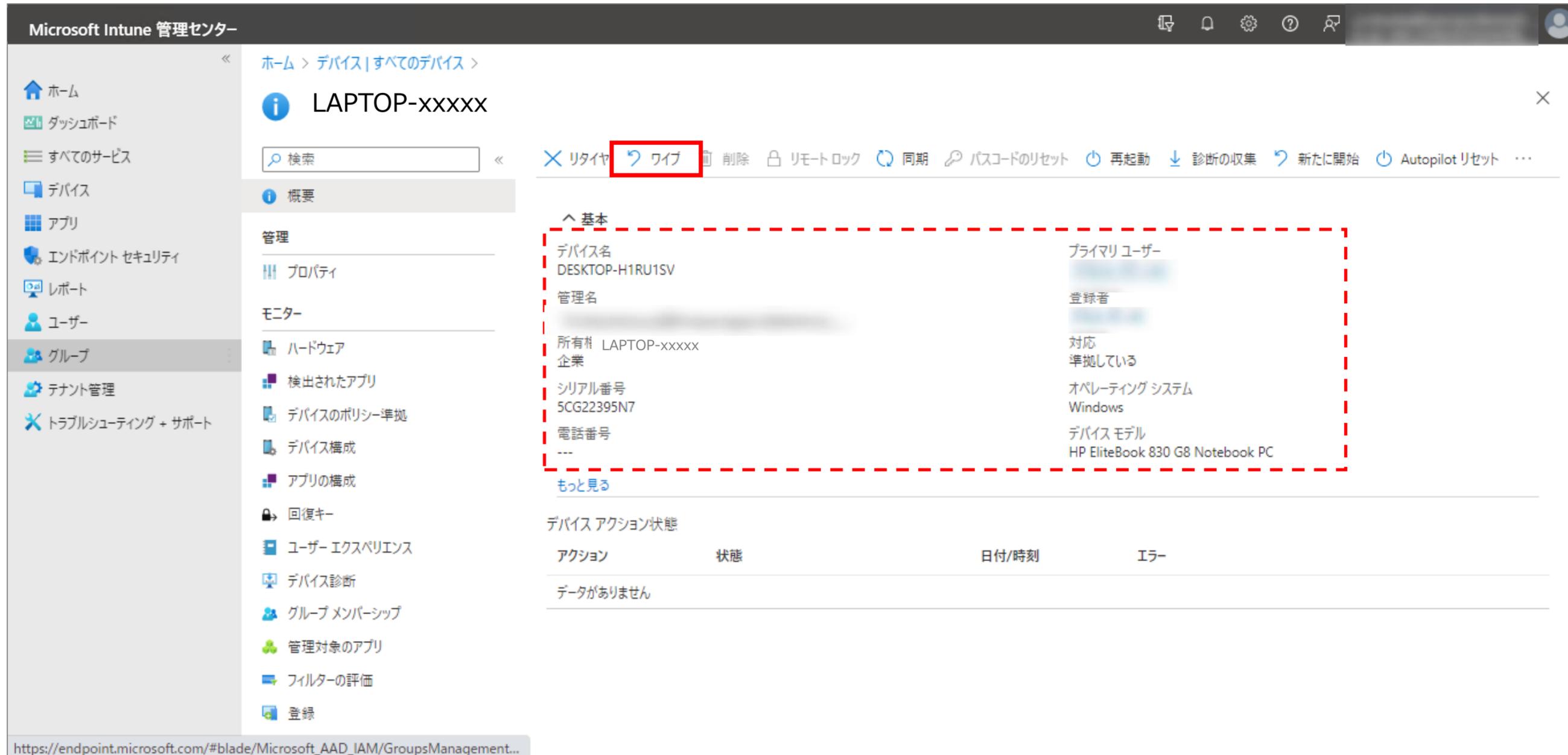
2件中 1 ~ 2 件のレコードを表示しています

デバイス名 ↑↓	管理者 ↑↓	所有権 ↑↓	対応 ↑↓	OS	OS のバージョン ↑↓	最後のチェックイン ↑↓	プライマリユーザーの...
LAPTOP-xxxxx	Intune	企業	✔ 準拠している	Windows	10.0.19043.1706	2022/6/21 14:14:02	
	Intune	企業	✔ 準拠している	Windows	10.0.19043.1586	2022/6/8 14:01:10	

検索バーで、利用ユーザー名を入力し、端末を検索できます

# V-2 遠隔での端末の初期化

4.基本情報から、リセットするデバイスで間違いないことを確認し、[ワイプ]をクリックします



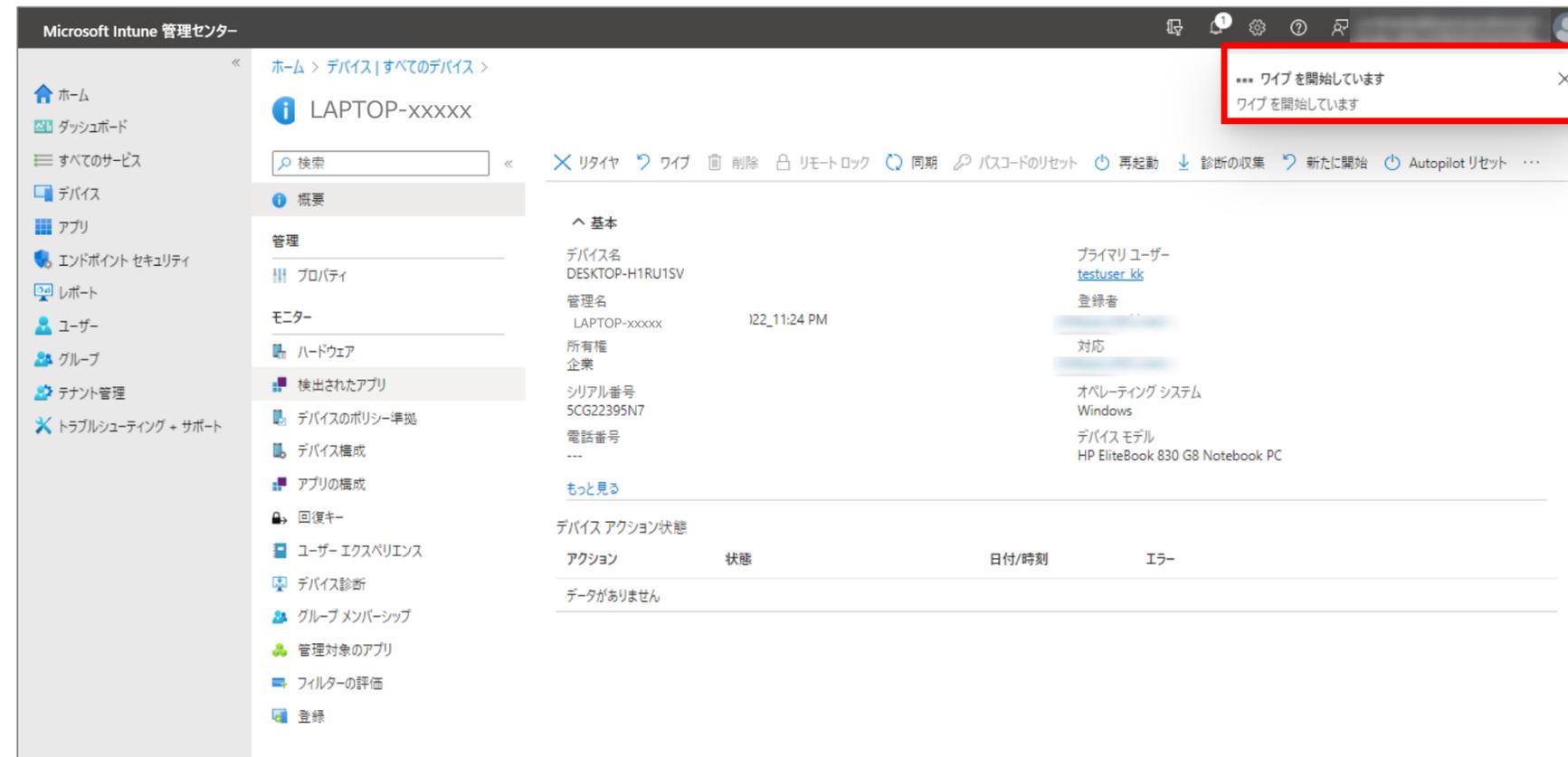
# V-2 遠隔での端末の初期化

5.リセットの確認画面が表示されますので、[デバイスをワイプして、デバイスの電源が切れてもワイプを続行します。 . . . . ]に☑を入れて、[ワイプ]をクリックします



# V-2 遠隔での端末の初期化

## 6. ワイプが開始されたことを確認します



### 《 端末でワイプが実行される条件》

- ・ 端末の電源が入っていること
- ・ インターネットに接続されている状態であること

※端末の電源が入っていなかったとしても、端末のリセットが成功するまで繰り返し試行されます。

# V-2 遠隔での端末の初期化

7.実行結果は、[デバイスのアクション状態]から確認することが可能です

The screenshot shows the Microsoft Intune management center interface. The left sidebar contains navigation options like 'ホーム', 'ダッシュボード', 'すべてのサービス', 'デバイス', 'アプリ', 'エンドポイントセキュリティ', 'レポート', 'ユーザー', 'グループ', 'テナント管理', and 'トラブルシューティング + サポート'. The main content area displays details for a device named 'LAPTOP-xxxxx'. The 'デバイス アクション状態' section contains a table with the following data:

アクション	状態	日付/時刻	エラー
protectedWipe	保留	2022/12/19 9:10:13	

## V-2 遠隔での端末の初期化

8.ワイプを実施後、セキュアドPCヘルプデスクへご連絡ください



セキュアドPCヘルプデスク  
連絡先 : 0570-016-112  
受付時間 : 9:00-17:00 (平日)

### 《留意事項》

- ・ 端末の情報流出を防ぐため、前頁まで手順に沿って、初期化を実施後、セキュアドPCヘルプデスクへご連絡ください
- ・ 盗難、紛失が発生した場合、端末の解約処理を実施頂くこととなります  
解約処理が完了するまでの間、端末の月額料金がかかります
- ・ 端末の盗難、紛失したユーザーに新たな端末を割り当てる際、万一来るべく、ユーザーパスワードの変更をお願いいたします

# VI. 端末返却時のデータ削除

1. 端末のリセット（管理者操作）
2. 端末のリセット（端末操作）

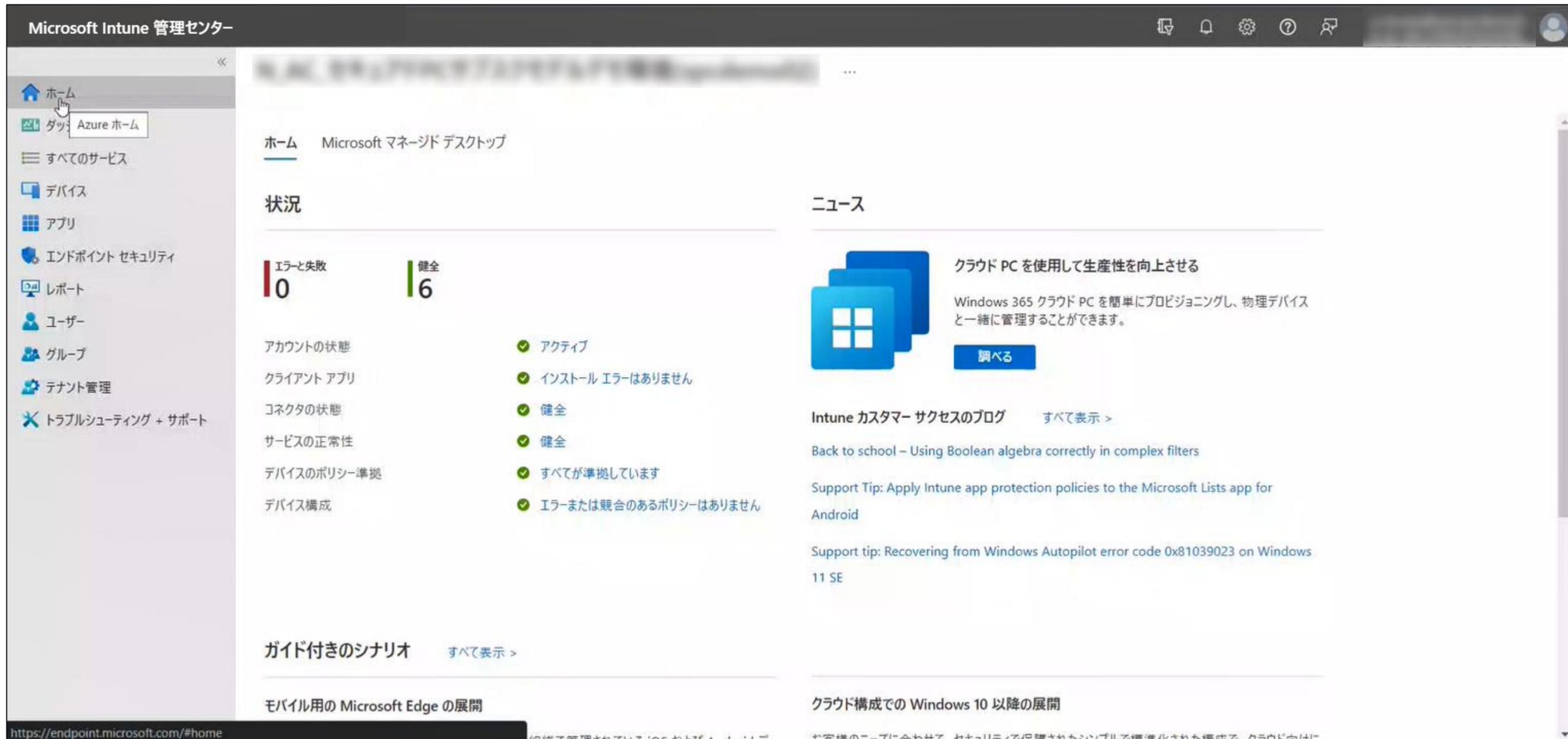
端末を返却いただく際には、お客様責任の下、端末のデータや設定等をリセットする必要があります。

※返却後、当社側でも端末クリーン作業を実施します

ここでは、管理者から端末を遠隔でリセットする手順を説明します。  
管理者の操作が完了後、リセットする端末側で再起動する必要があります。

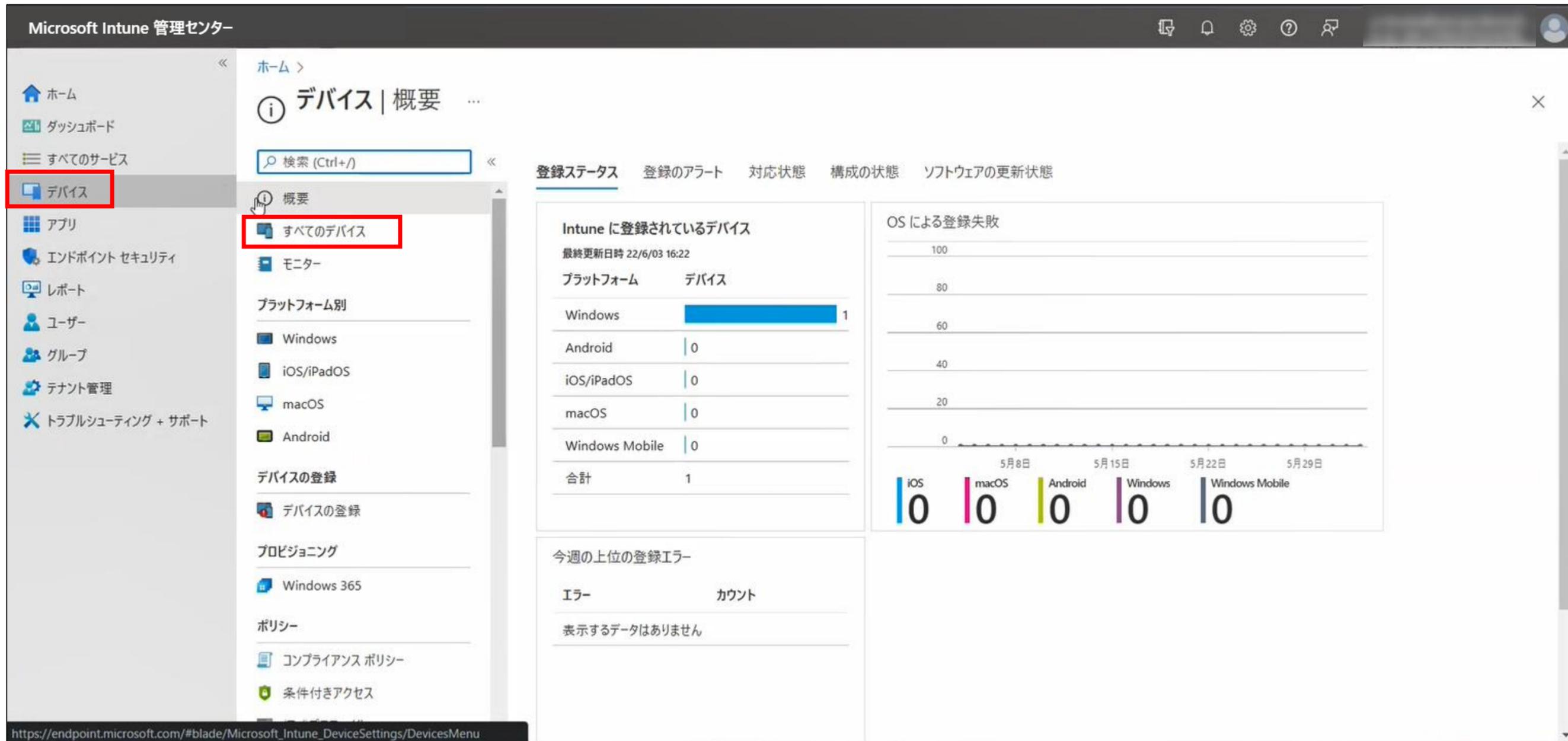
# VI-1 端末のリセット（管理者操作）

1. Microsoft Intune 管理センター (<https://intune.microsoft.com/>) にアクセスします



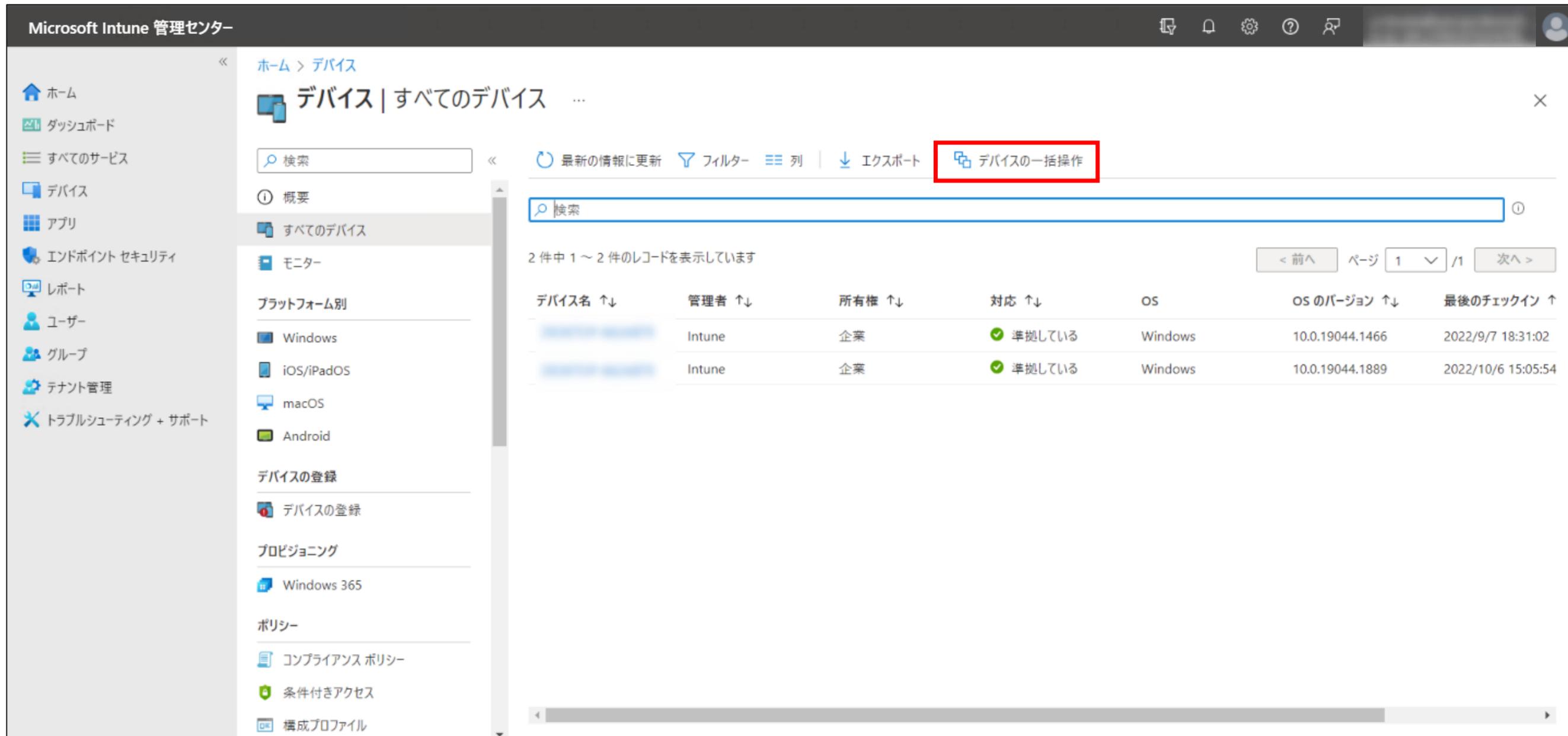
# VI-1 端末のリセット（管理者操作）

2.[デバイス]をクリックし、[すべてのデバイス]をクリックします



# VI-1 端末のリセット（管理者操作）

3.[デバイスの一括操作]をクリックします



# VI-1 端末のリセット（管理者操作）

4.OSは[Windows]、デバイスアクションは[Autopilotリセット]を選択し、[次へ]をクリックします





# VI-1 端末のリセット（管理者操作）

6.[選択]をクリックし、[次へ]をクリックします

Microsoft Intune 管理センター

ホーム > デバイス | すべてのデバイス >

デバイスの一括操作 ...

✖ 少なくとも 1 つのデバイスを選択する必要があります

✔ 基本 ✖ デバイス ③ 確認および作成

0 台のデバイスが選択されています (最大 100 台)

デバイスは追加されていません

+ 含めるデバイスを選択

前へ 次へ 選択

デバイスの選択

OS == Windows フィルターを追加

デバイス名	プライマリ ユーザーの UPN	OS
[Redacted]	[Redacted]	Windows
[Redacted]	[Redacted]	Windows

デバイス が選択済み

[Redacted]	[Redacted]	Windows	削除
[Redacted]	[Redacted]	Windows	削除

# VI-1 端末のリセット（管理者操作）

7. 選択されたデバイスが返却する端末であることを確認し、[作成]をクリックします

Microsoft Intune 管理センター

ホーム > デバイス | すべてのデバイス >

## デバイスの一括操作

基本
  デバイス
  3 確認および作成

概要

基本

デバイス アクション      Autopilot リセット

OS                                  Windows

デバイス

2 台のデバイスが選択されています (最大 100 台)

デバイス名	プライマリ ユーザーの UPN	OS
[Redacted]	[Redacted]	Windows
[Redacted]	[Redacted]	Windows

前へ    **作成**

# VI-1 端末のリセット（管理者操作）

8. 右上の通知から、Autopilotリセットが実行されたことを確認します

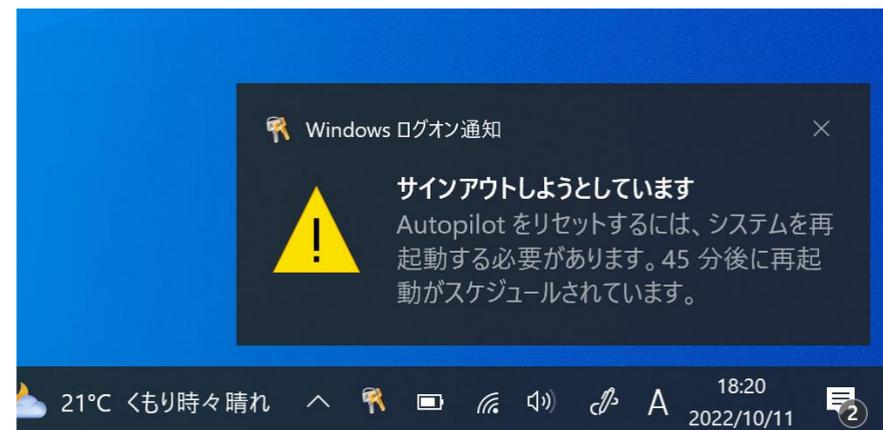
The screenshot shows the Microsoft Intune management center interface. A notification in the top right corner, highlighted with a red box, states: "すべてのデバイスでAutopilot リセットの開始成功" (Successful start of Autopilot reset for all devices) and "Intune から 2 台のデバイスでAutopilot リセットを開始しました" (Started Autopilot reset for 2 devices from Intune). Below the notification, a table displays the status of two devices:

デバイス名 ↑↓	管理者 ↑↓	所有権 ↑↓	対応 ↑↓	OS	OS のバージョン ↑↓	最後のチェックイン ↑
[Redacted]	Intune	企業	✔ 準拠している	Windows	10.0.19044.1466	2022/10/11 13:18:3
[Redacted]	Intune	企業	✔ 準拠している	Windows	10.0.19044.1889	2022/10/6 15:05:54

## VI-2 端末のリセット（端末操作）

Autopilotリセットが実行された端末は、数分から数十分程度で以下のように、サインアウトする通知がされます。  
端末利用ユーザーに再起動するようご案内をお願いいたします。

またサインアウトの通知がされない、またはリセットが始まらない端末については、再起動をすることでリセットが実行される場合がございますので、リセットがうまく実行されない場合はお試しください。



# VII. その他

## 1. ユーザーの端末が故障した場合の対応

## VII-1 ユーザーの端末が故障した場合

端末に故障、不具合等が発生した場合は、ユーザーご自身から直接セキュアドPCヘルプデスクまでご連絡ください。故障内容のヒアリングをさせていただきます。

端末の交換や回収が必要と判断した場合は、ユーザーから管理者様へご連絡するよう案内いたします。ユーザーからご連絡受け取りましたら、お手数ですがセキュアドPCヘルプデスクまでご連絡ください。予備機の利用や、代替機発送に伴うご調整等の案内をいたします。



セキュアドPCヘルプデスク  
連絡先 : 0570-016-112  
受付時間 : 9:00-17:00 (平日)

### 《留意事項》

- ・ 端末の故障理由により、修理交換費を請求させていただく場合がございます

# Ⅷ. 留意事項

1. 総務省セキュリティガイドラインに対する機能対応表
2. 総務省セキュリティガイドラインに準拠してMicrosoft365設定内容

# Ⅷ-1 総務省セキュリティガイドラインに対する機能対応表

優先度◎ 総務省発行のセキュリティガイドラインに対してセキュアドPC月額レンタルモデルが提供する機能のマトリックス表

No.	分類	対策内容	サービスにて 対応済	想定脅威	弊社対応内容	お客様対応内容
1-1	資産 構成管理	テレワークには許可した端末のみを利用するよう周知しテレワーク端末とその利用者を把握する。	○	マルウェア感染 不正アクセス盗難 紛失	・ Intuneにて、利用者の把握が可能 ・ 周知資料提示	周知
1-2	資産 構成管理	テレワークで利用しているシステムや取り扱う重要情報を把握する。	○	不正アクセス情報の盗聴	・ データにはアクセス権・暗号化設定が可能 ・ 周知資料提示（システム管理者様向け）	周知（システム管理者様向け）
2-1	マルウェア対策	テレワーク端末にウイルス対策ソフトをインストールしリアルタイムスキャンを有効にする。ウイルス対策ソフトの定義ファイルを自動更新する設定にするか手動で更新するルールを作成する。	○	マルウェア感染	・ Defenderを有効化しポリシーとして端末に自動配布	
2-2	マルウェア対策	不審なメールを開封しメールに記載されている URL をクリックしたり添付ファイルを開いたりしないよう周知する。	○	マルウェア感染	・ 周知資料提示	周知
3-1	アクセス制御 認可	許可された人のみが重要情報を利用できるようにシステムによるアクセス制御やファイルに対するパスワード設定等を行う。	○	不正アクセス	・ データにはアクセス権・暗号化設定が可能 ・ 周知資料提示	
4-1	物理セキュリティ	テレワーク端末にのぞき見防止フィルタを貼り付けるよう周知する。	○	情報の盗聴	・ 周知資料提示	周知
4-2	物理セキュリティ	テレワーク端末から離れる際にはスクリーンロックをかけるよう周知する。	○	情報の盗聴	・ 強制適用検討中 ・ 周知資料提示	周知
5-1	脆弱性管理	テレワーク端末にはメーカーサポートが終了したOS やアプリケーションを利用しないよう周知する。	○	不正アクセス	・ 端末更新サイクルは最長4年のためサポート終了したOSが提供されることは無し ・ 周知資料提示	周知
5-2	脆弱性管理	テレワーク端末のOS やアプリケーションに対して最新のセキュリティアップデートを適用するよう周知する。	○	不正アクセス	・ ポリシーとして端末に自動配布 ・ 周知資料提示	周知
7-1	インシデント対応 ログ管理	セキュリティインシデントの発生時や、そのおそれがある状況に備えて対応手順及び関係者への各種連絡体制を定め従業員に緊急連絡先を周知する。	○	マルウェア感染不正アクセス盗難・紛失	・ 周知資料提示（システム管理者様向け）	周知（システム管理者様向け）
8-1	データ保護	スマートフォン等のテレワーク端末の紛失時に端末の位置情報を検出できるようにする。	○	盗難・紛失	・ 端末検索の機能を有効化	
9-1	アカウント 認証管理	テレワーク端末のログインアカウントやテレワークで利用する各システムのパスワードには、「長く」「複雑な」パスワードを設定するようルール化する。また可能な限りパスワード強度の設定を強制する。	○	不正アクセス	・ Microsoftのパスワードポリシー及び多要素認証を適用	
9-2	アカウント 認証管理	テレワーク端末のログインパスワードやテレワークで利用する各システムの初期パスワードは必ず変更するよう設定する。	○	不正アクセス	・ Microsoftのパスワードポリシー及び多要素認証を適用	

# VII-1 総務省セキュリティガイドラインに対する機能対応表

優先度○ 総務省発行のセキュリティガイドラインに対してセキュアドPC月額レンタルモデルが提供する機能のマトリックス表

No.	分類	対策内容	サービスにて 対応済	想定脅威	弊社対応内容	お客様対応内容
2-3	マルウェア対策	メール製品に不審なメールを除外する機能がある場合は有効化しておく。	○	マルウェア感染	・ Microsoftの規定のポリシーにて運用	
2-4	マルウェア対策	スマートフォン等のテレワーク端末にアプリケーションをインストールする場合は公式アプリケーションストアを利用するよう周知する。	○	マルウェア感染	・ 必須アプリ（弊社選定）は、強制配布 ・ 周知資料提示	周知
3-3	アクセス制御 認可	オンライン会議の主催者は会議に招集した参加者なのかどうか名前や顔を確認してから会議への参加を許可するよう周知する。	○	情報の盗聴	・ 周知資料提示	周知
3-4	アクセス制御 認可	オンライン会議に参加するためのパスワードの設定は原則必須としURL と合わせて必要なメンバーだけに伝えるよう周知する。	○	情報の盗聴	・ Teamsは、デフォルトパスワード設定有 ・ 周知資料提示	周知
3-5	アクセス制御 認可	オンライン会議の主催者は会議に招集した覚えのない参加者の参加を許可しないよう周知する。	○	情報の盗聴	・ 周知資料提示	周知
5-3	脆弱性管理	テレワークで利用するネットワーク機器にはメーカーサポートが終了した製品を利用せず、最新のファームウェアを適用するよう周知する。	○	不正アクセス	・ 周知資料提示	周知
6-1	通信暗号化	Web メール、チャット、オンライン会議、クラウドストレージ等のクラウドサービスを利用する場合（特にID・パスワード等の入力を求められる場合）は暗号化されたHTTPS 通信であること接続先のURLが正しいことを確認するよう周知する。	○	情報の盗聴	・ M365はHTTP通信で暗号化 ・ 周知資料提示	周知
6-2	通信暗号化	無線LANルーターを利用する場合はセキュリティ方式として「WPA2」又は「WPA3」を利用し無線の暗号化パスワードは第三者に推測されにくいものにする。	○	情報の盗聴	・ 周知資料提示	周知
7-2	インシデント対 ログ管理	テレワーク端末と接続先の各システムの時刻を同期させる。	○	マルウェア感染 不正アクセス盗難 紛失	・ 端末はWindowsのタイムサーバーと時刻の同期 を有効化	

# VIII-1 総務省セキュリティガイドラインに対する機能対応表

優先度○ 総務省発行のセキュリティガイドラインに対してセキュアドPC月額レンタルモデルが提供する機能のマトリックス表

No.	分類	対策内容	サービスにて対応済	想定脅威	弊社対応内容	お客様対応内容
8-2	データ保護	テレワーク端末の紛失時に備えてMDM等を導入しリモートからのデータ消去、ログイン時の認証ポリシーやハードディスクの暗号化などのセキュリティ設定を強制的に適用する。	○	盗難 紛失	・ リモートワイプの機能の提要 ・ Bitlockerをポリシーにて強制配布	
8-3	データ保護	テレワーク端末の盗難・紛失時に情報が漏えいしないよう端末に内蔵されたハードディスクやフラッシュメモリ等の記録媒体の暗号化を実施する。ただし端末に会社のデータを保管しない場合を除く。	○	盗難 紛失	・ HDD/SSD暗号化(Bitlocker)の強制 ・ 周知資料提示(外付けHDDの扱い)	周知
8-4	データ保護	テレワーク端末には原則として重要情報を保管しないよう周知する。万一その必要性が生じた場合にはパスワードの設定やファイルの暗号化を実施し一時的な保管のみを許可する。ただし端末に会社のデータを保管しない場合を除く。	○	不正アクセス盗難 紛失	・ データにはアクセス権・暗号化設定が可能 ・ 周知資料提示	周知
8-5	データ保護	オンライン会議のタイトルや議題には重要情報を記載せず会議の録画ファイルに対してはパスワードの設定や期間指定の自動削除等を実施するよう周知する。また上記ルールは可能な限り設定を強制する	○	情報の盗聴	・ 録画は、デフォルトで参加者のみ閲覧可能 ・ 保存期間は規定で120日(保存期間) ・ 周知資料提示	周知
9-3	アカウント・認証管理	テレワーク端末やテレワークで利用する各システムに対して一定回数以上パスワードを誤入力した場合それ以上のパスワード入力を受け付けられないよう設定する。	○	不正アクセス	・ Microsoftのパスワードポリシーにて運用	
9-4	アカウント・認証管理	テレワークで利用する各システムへのアクセスには多要素認証を求めよう設定する。	○	不正アクセス	・ 全端末に対して多要素認証を強制適用	
10-1	特権管理	テレワーク端末やテレワークで利用する各システムの管理者権限は業務上必要な最小限の人に付与する。	○	不正アクセス	・ 管理者アカウントを管理者グループへユーザを追加削除する事により実現 ・ 周知資料提示(システム管理者様向け)	周知(システム管理者様向け)
10-2	特権管理	テレワーク端末やテレワークで利用する各システムの管理者権限のパスワードには強力なパスワードポリシーを適用する。	○	不正アクセス	・ Microsoftのパスワードポリシーを強制適用	
10-3	特権管理	テレワーク端末やテレワークで利用する各システムの管理者権限は必要な作業時のみ利用する。	○	不正アクセス	・ M365のグローバル管理者権限はCOMにて管理 ・ 周知資料提示(システム管理者様向け)	周知(システム管理者様向け)

## 引用

中小企業等担当者向けテレワークセキュリティの手引き(チェックリスト) 会社支給端末:クラウドサービス方式 30ページ ~ 33ページ  
 URL [https://www.soumu.go.jp/main\\_content/000816096.pdf](https://www.soumu.go.jp/main_content/000816096.pdf)

## Ⅷ-2 総務省セキュリティガイドラインに準拠したMicrosoft365設定内容

原則的に総務省セキュリティガイドラインに準拠したMicrosoft365設定を行った状態で提供しています。  
 お客様にて各種設定変更が可能です。セキュリティガイドラインから外れてしまう場合があります。  
 設定変更の際は、お客様責任にてお願いします。

Microsoft365 設定サイト	設定項目
Azure Portal <a href="https://portal.azure.com/">https://portal.azure.com/</a>	<b>MDMの設定</b> [Azure Active Directory] → [モビリティ(MDM および MAM)] → Microsoft Intune  <b>MFAの強制設定</b> [Azure Active Directory] → [プロパティ] → セキュリティの既定値群の管理 [Azure Active Directory] → [セキュリティ] → [多要素認証] → クラウドベースの多要素認証の追加設定
Microsoft365コンプライアンス <a href="https://compliance.microsoft.com/">https://compliance.microsoft.com/</a>	<b>Azure Information Protectionの設定</b> [情報保護] → [ラベル] → 暗号化有り(社外閲覧不可)・暗号化無し(社外閲覧可能)  <b>Windows Autopilot Deployment (OOBE) 設定</b> [デバイス] → [デバイスの登録] → [Windows登録] → [デプロイ プロファイル] → OOBProfile
Microsoft Endpoint Manager admin center <a href="https://endpoint.microsoft.com/">https://endpoint.microsoft.com/</a>	<b>既知のフォルダーをOneDriveにサイレントバックアップする設定</b> [デバイス] → [構成プロファイル] → OneDrive_backup  <b>Defender (リアルタイム検知、ウイルス定義ファイル等) の有効化</b> [デバイス] → [構成プロファイル] → Windows Defender ウィルス対策  <b>Defender Web保護の有効化</b> [エンドポイントセキュリティ] → [攻撃面の減少] → Windows Defender Web保護  <b>Windows更新プログラムのポリシー設定</b> [デバイス] → [Windows 10 以降向け更新リング] → windows10以降向け更新リング  <b>Bitlockerの有効化</b> [デバイス] → [構成プロファイル] → Bitlocker  <b>スクリーンロックの設定</b> [デバイス] → [構成プロファイル] → スクリーンロック