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

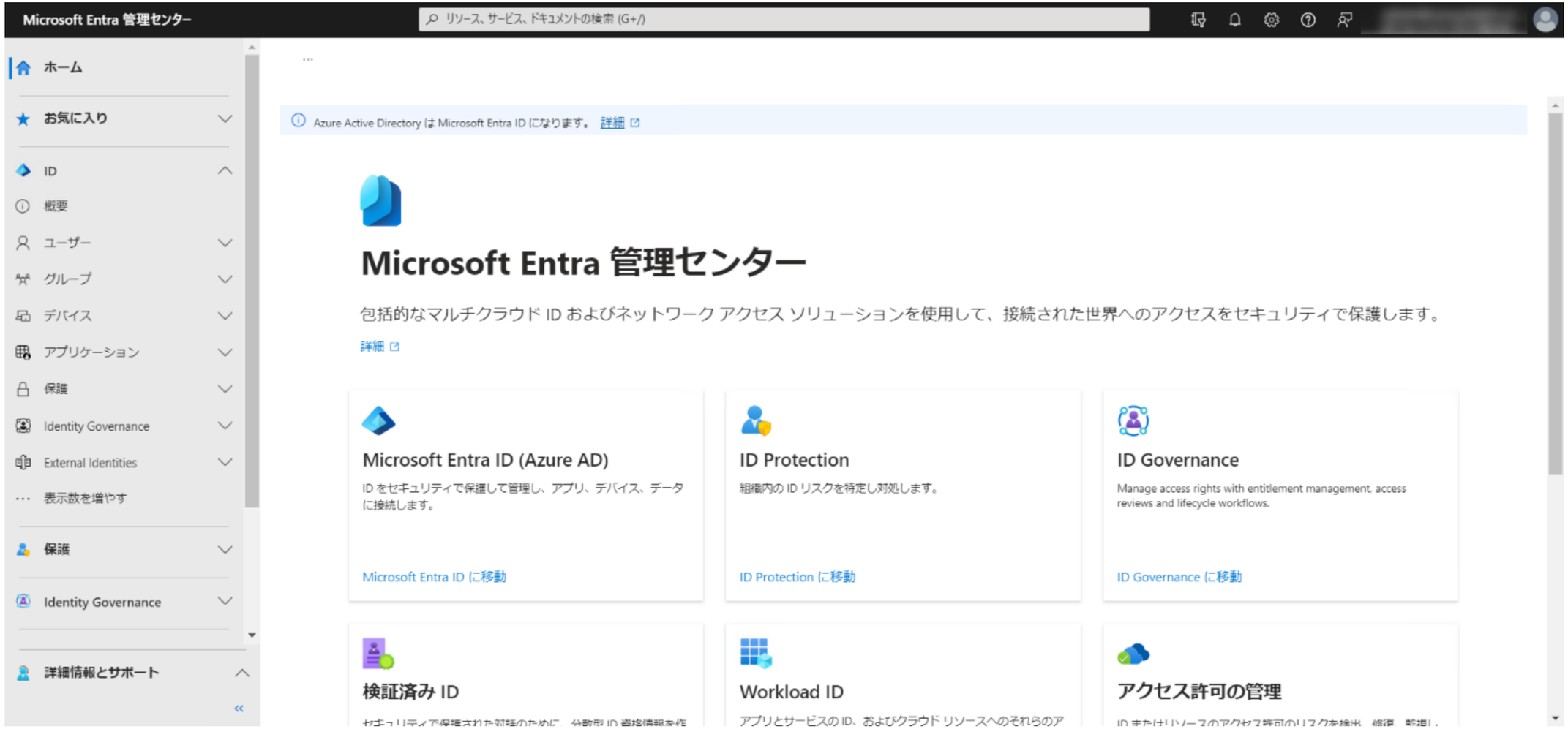
目次

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

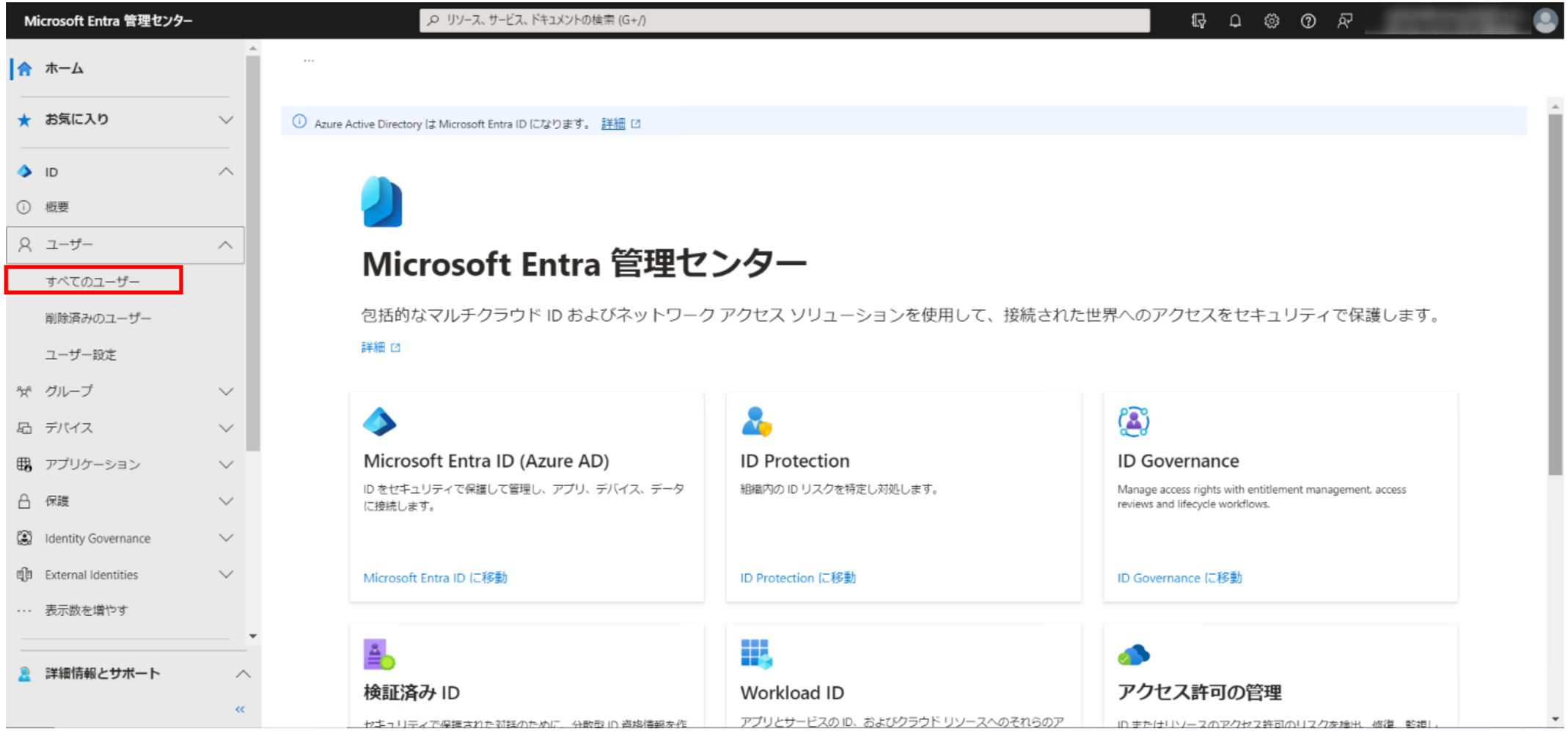
Ⅰ-1　アカウントの追加方法

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



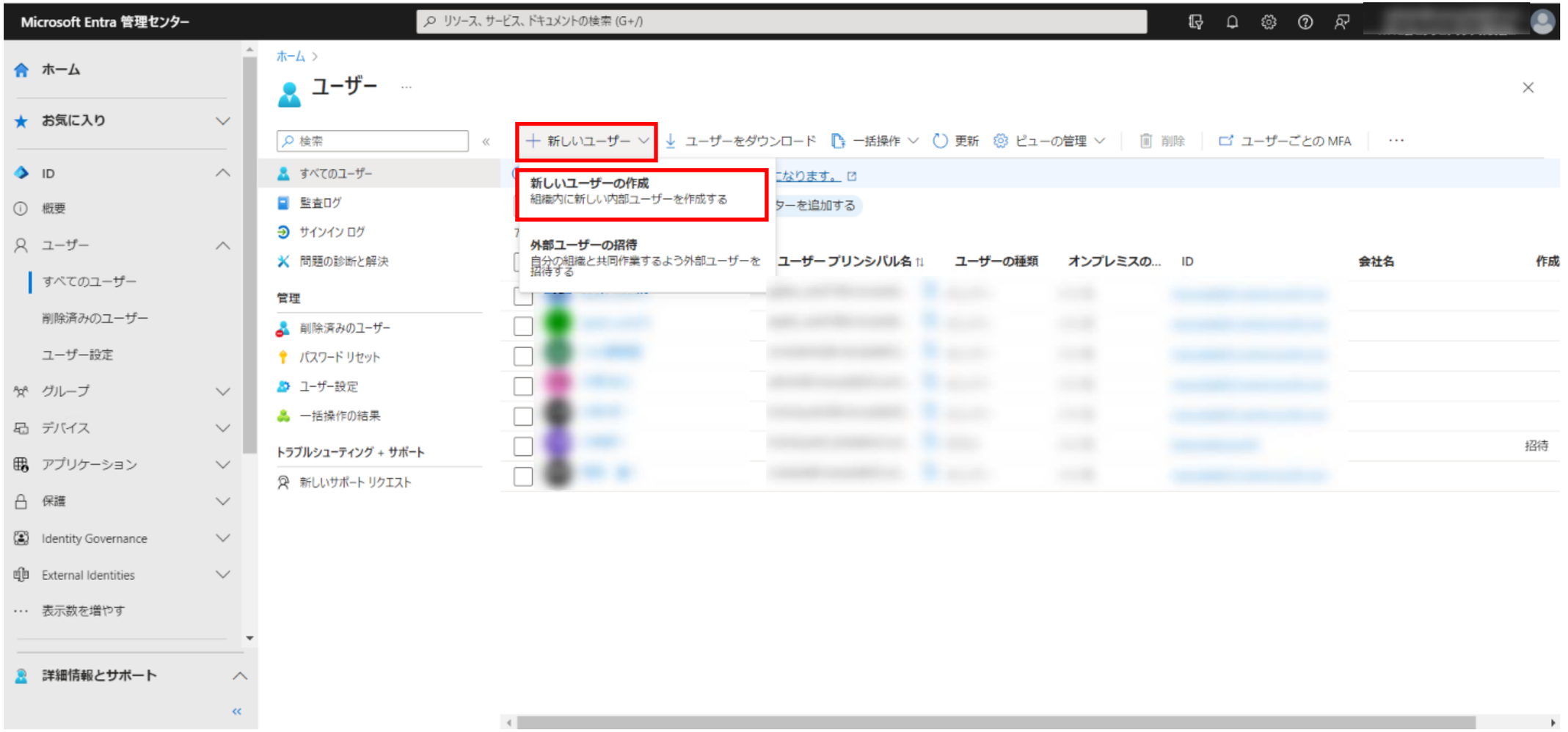
Ⅰ-1　アカウントの追加方法

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

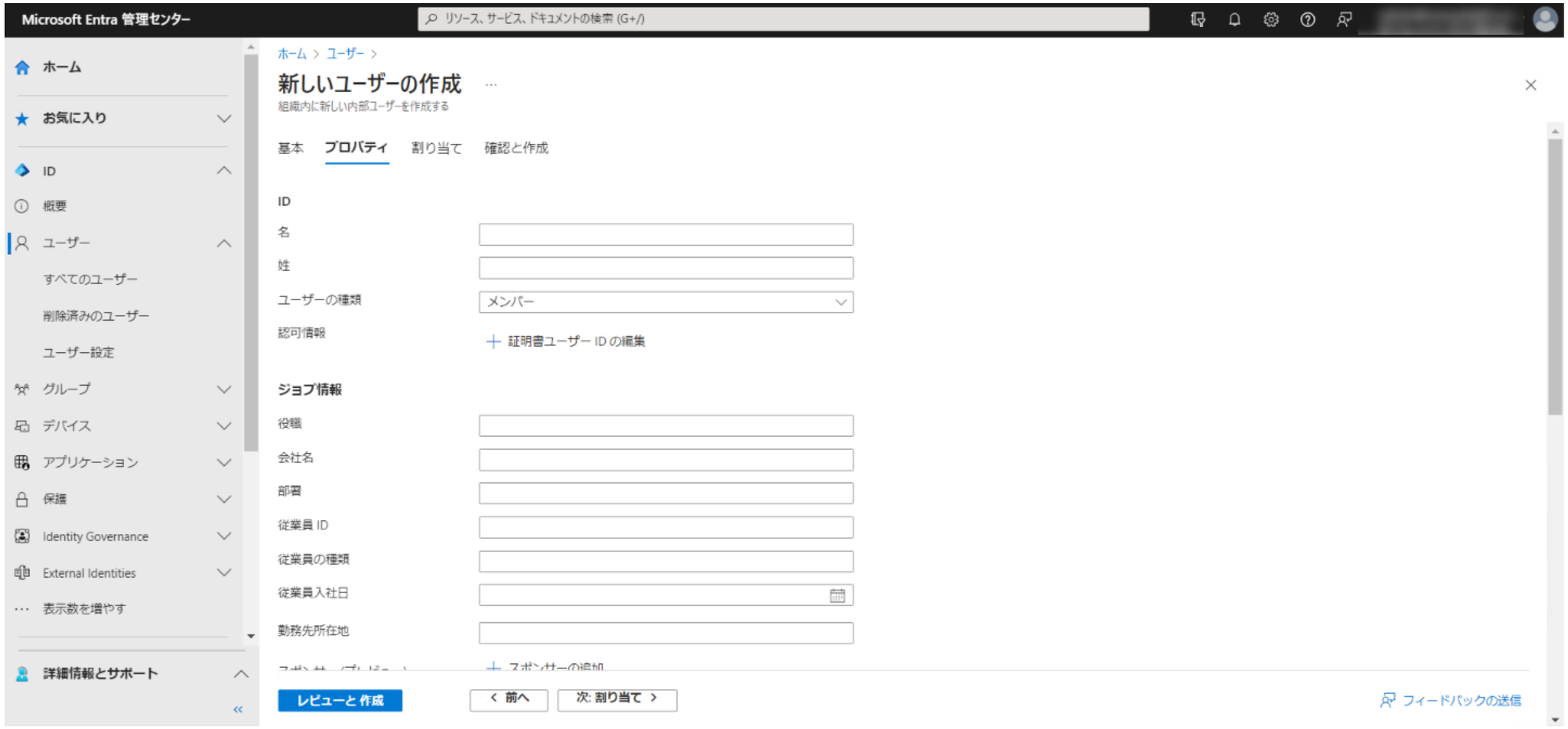


Ⅰ-1　アカウントの追加方法

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

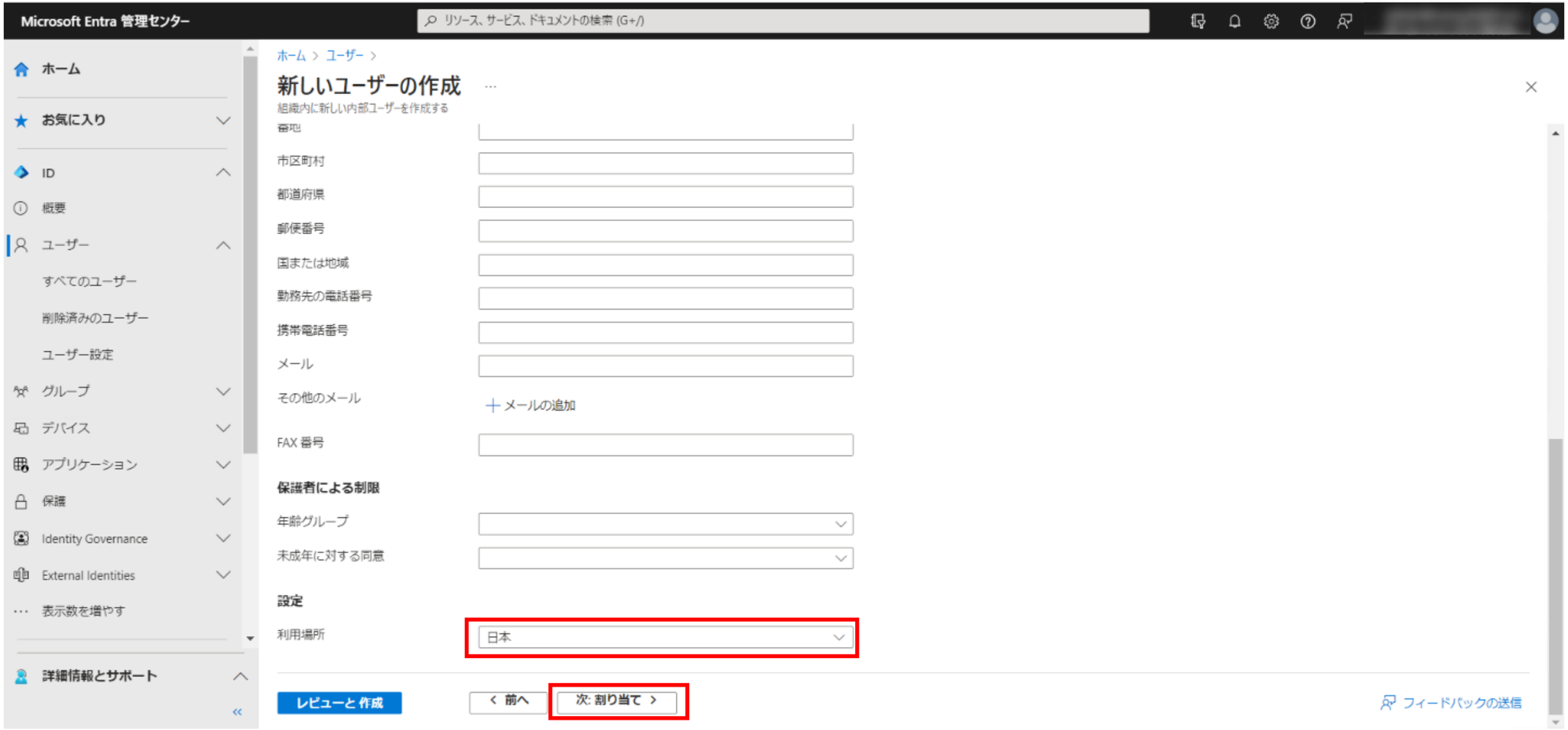
Ⅰ-1　アカウントの追加方法

5.プロパティの画面で必要に応じ、各情報を入力します



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ことができません

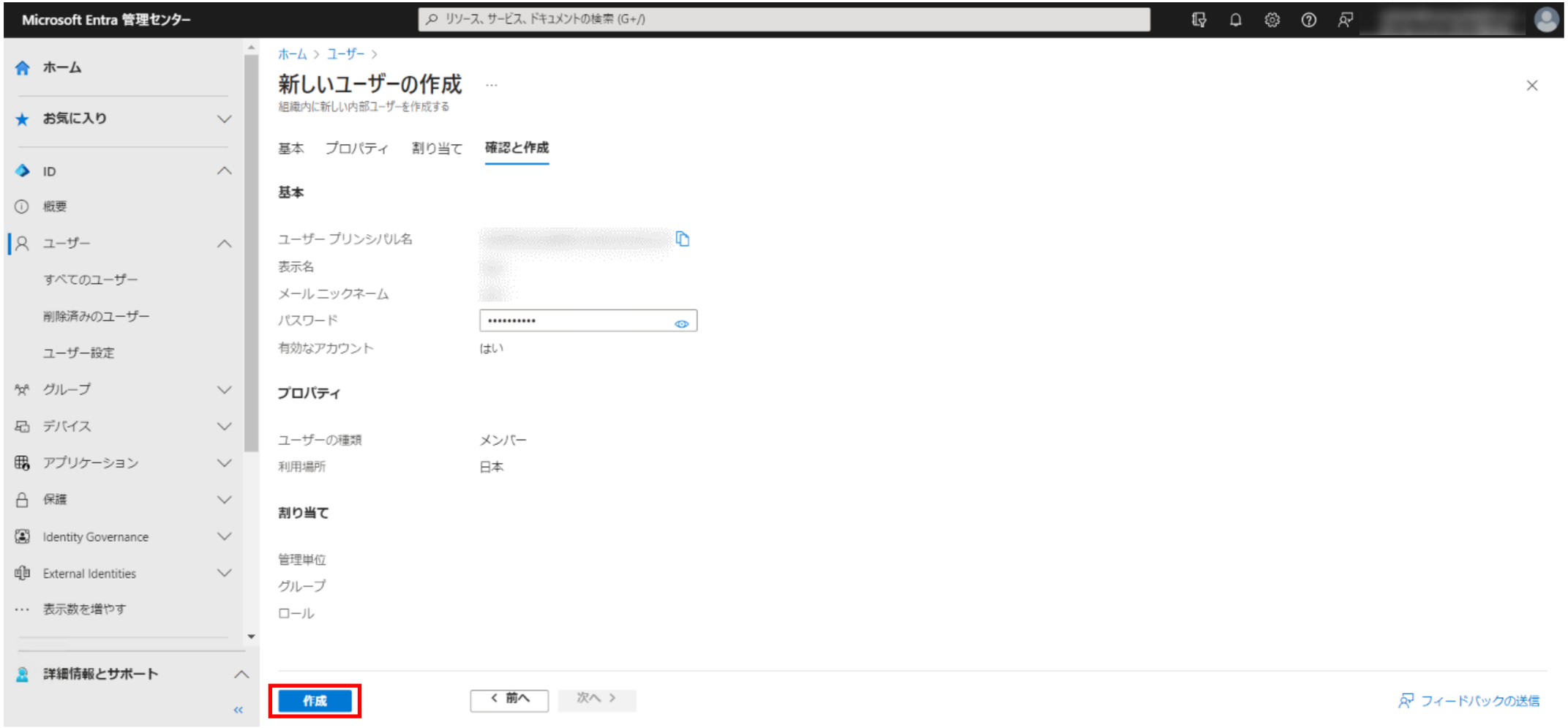


Ⅰ-1　アカウントの追加方法

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

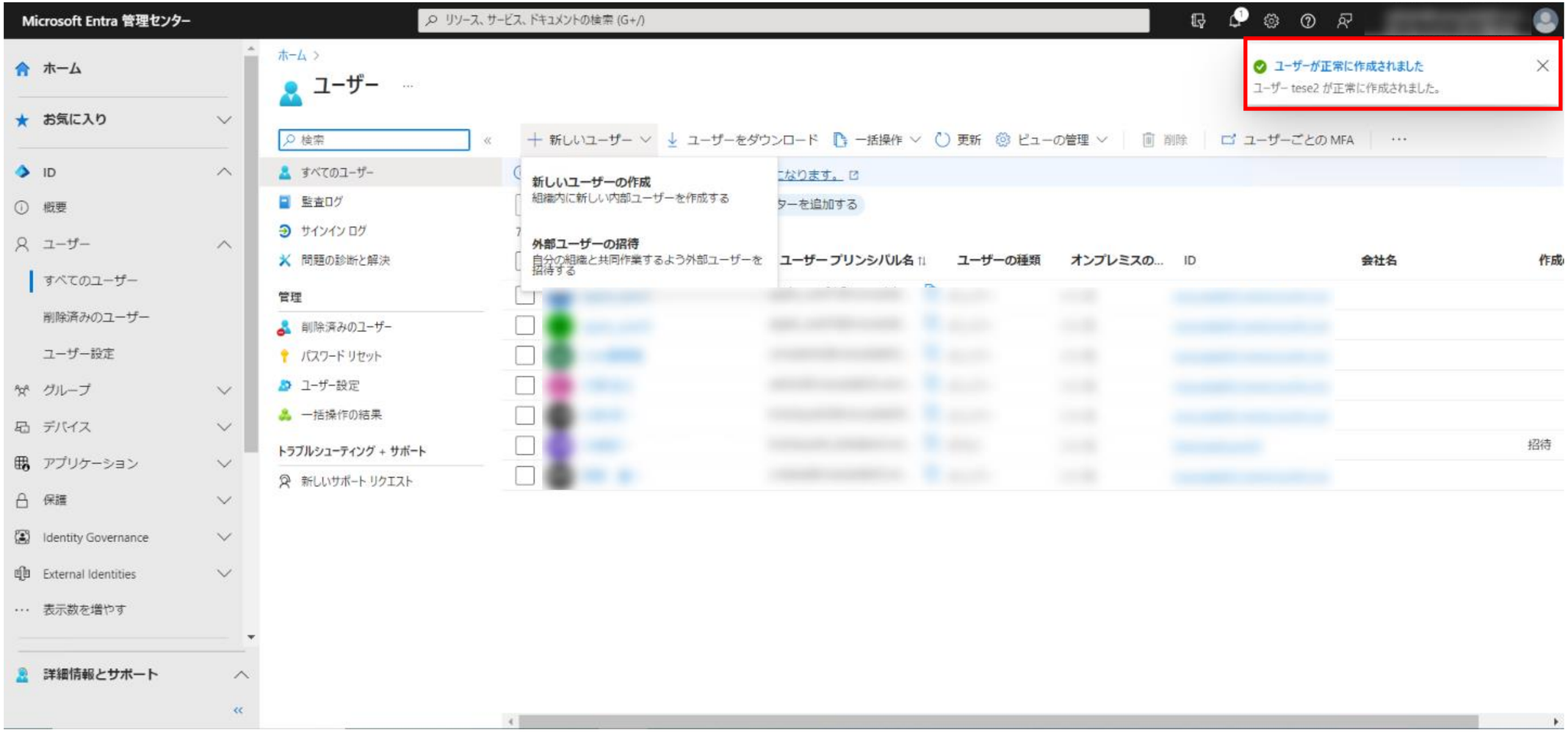
Ⅰ-1　アカウントの追加方法

8. 作成内容を確認し、[作成]をクリックします



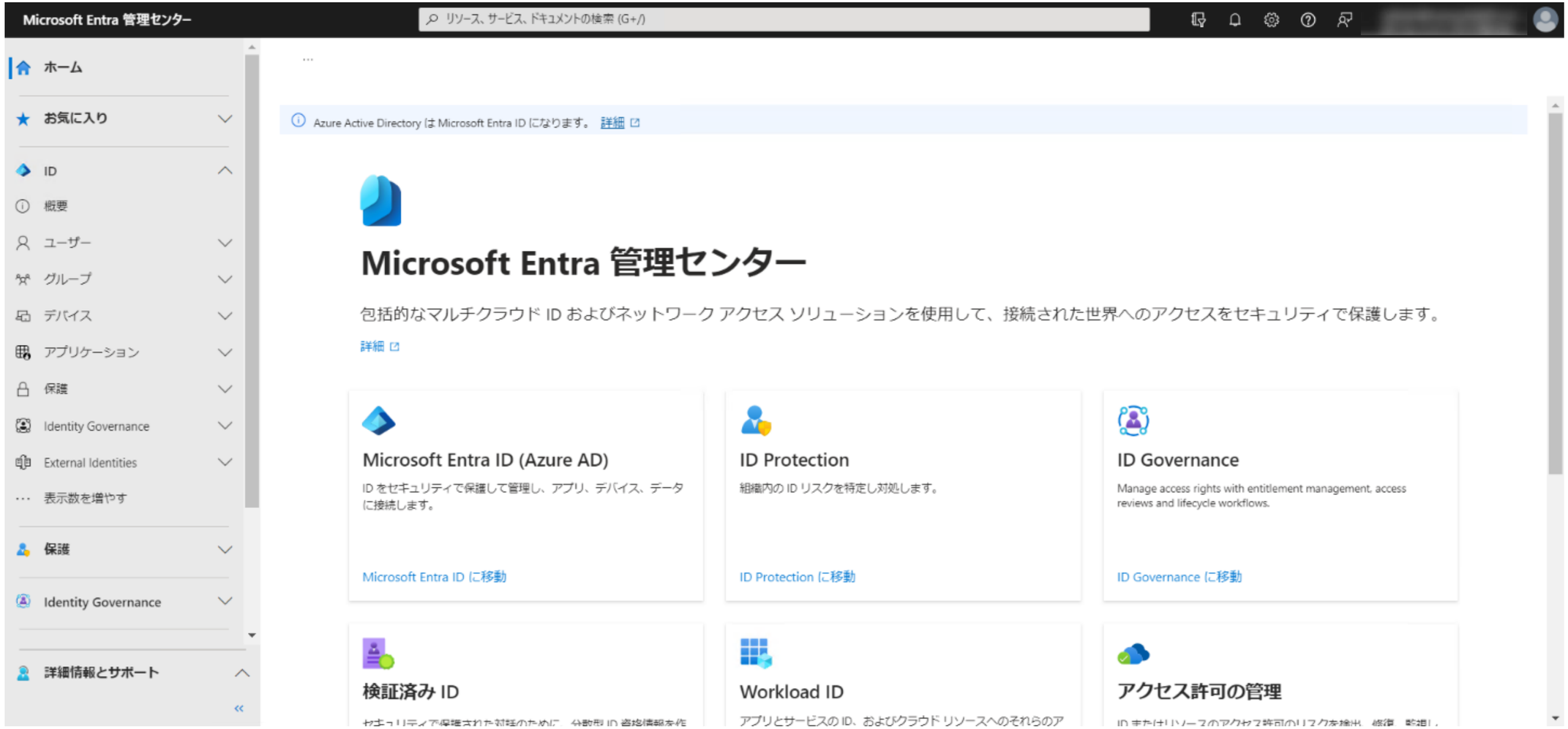
Ⅰ-1　アカウントの追加方法

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



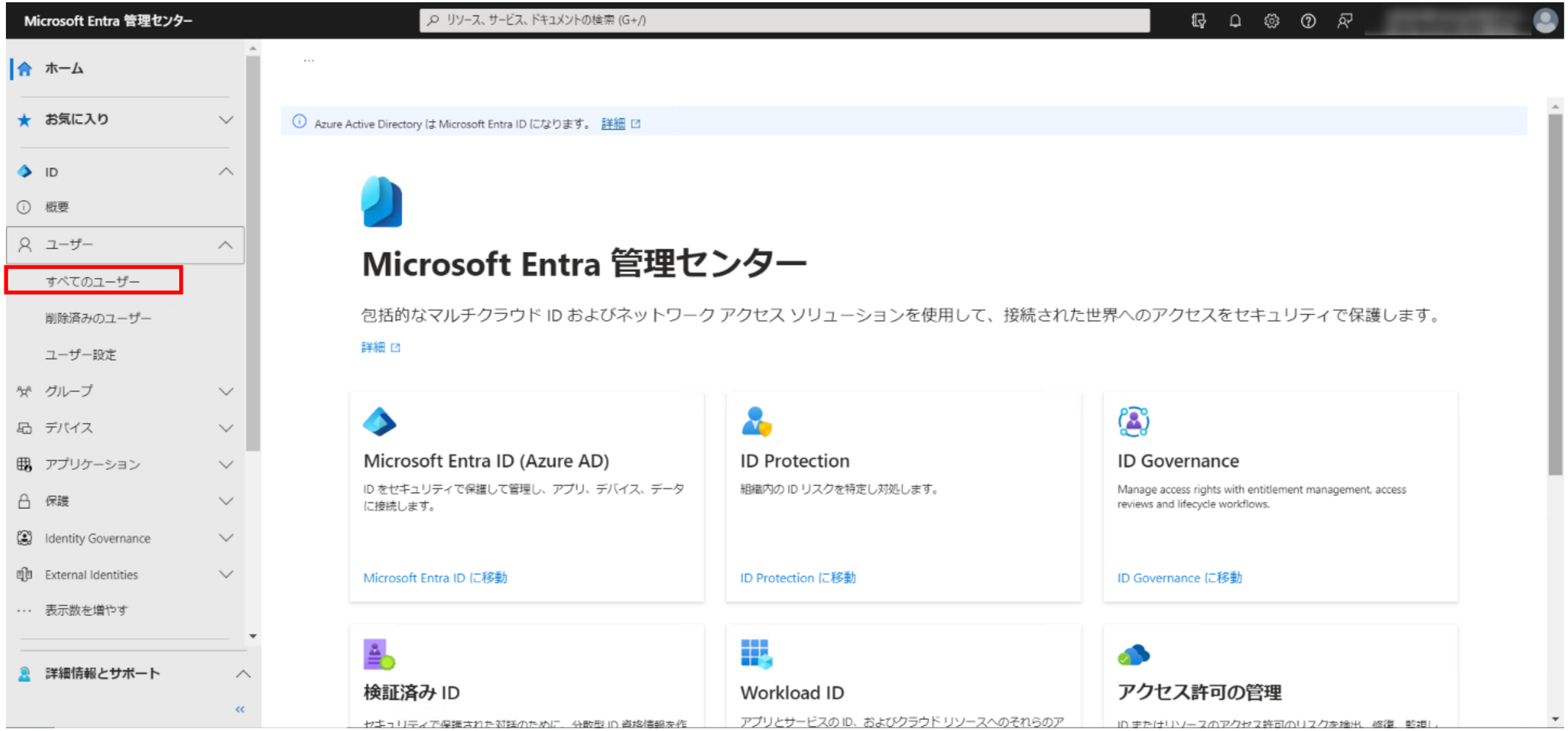
Ⅰ-2　アカウントの削除方法

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



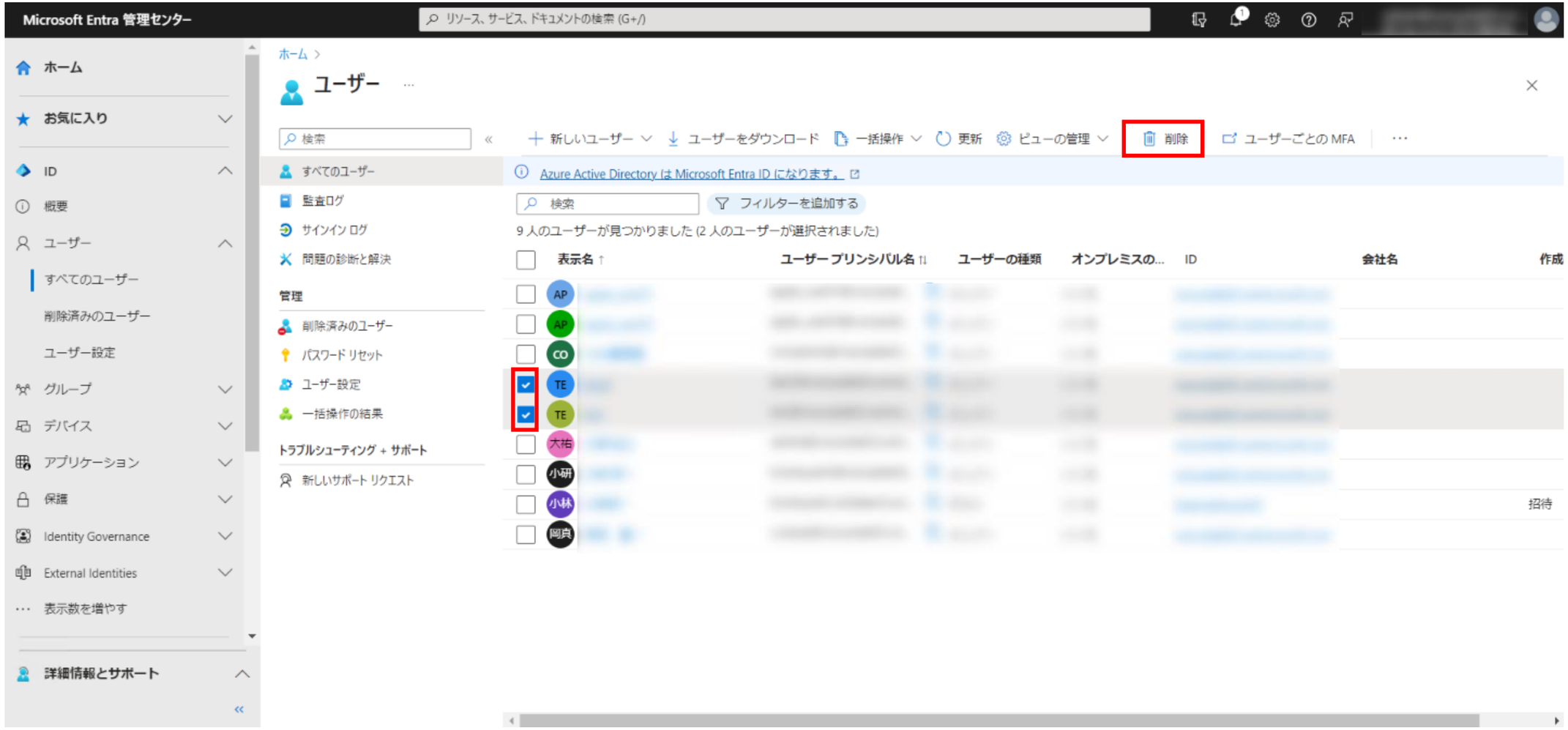
Ⅰ-2　アカウントの削除方法

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



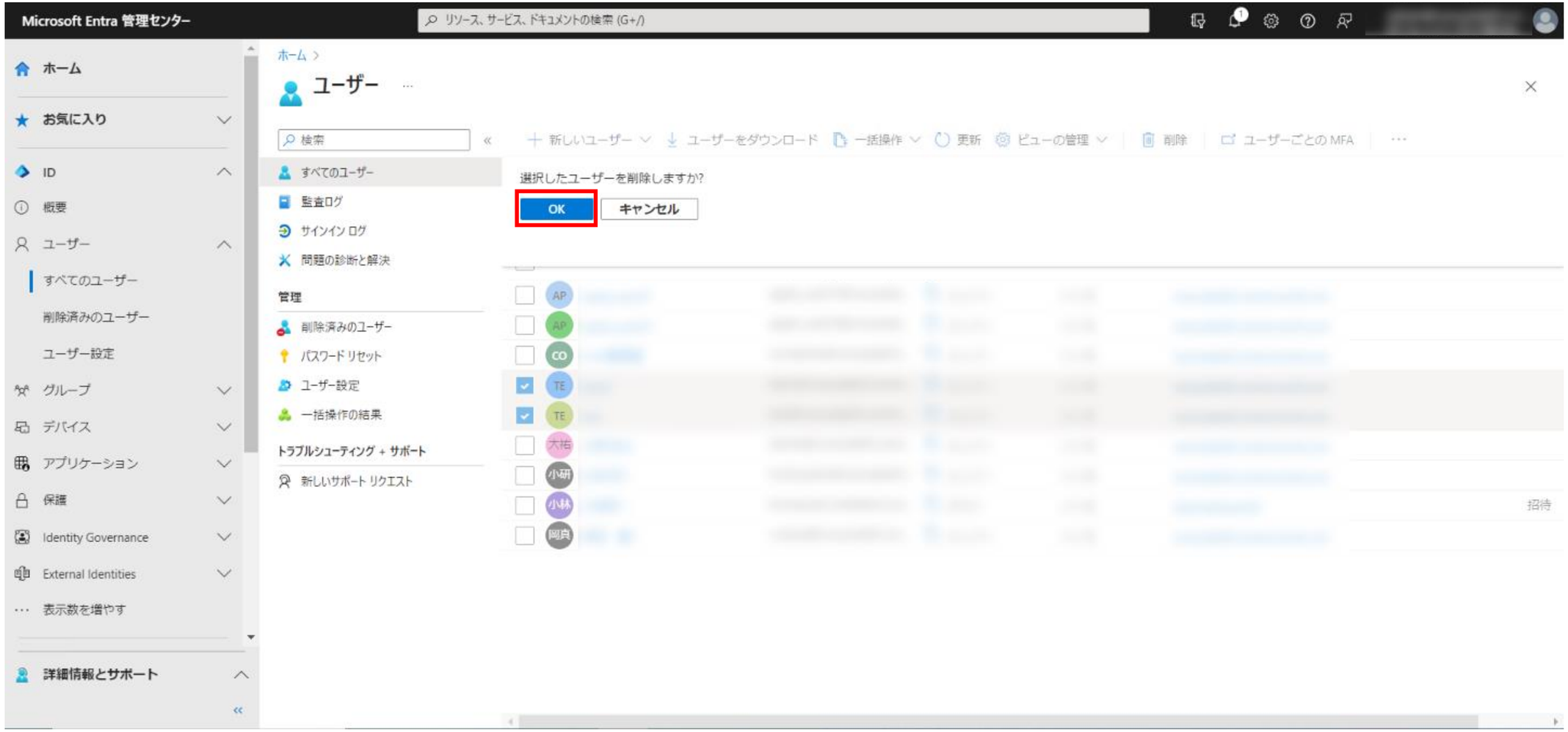
Ⅰ-2　アカウントの削除方法

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



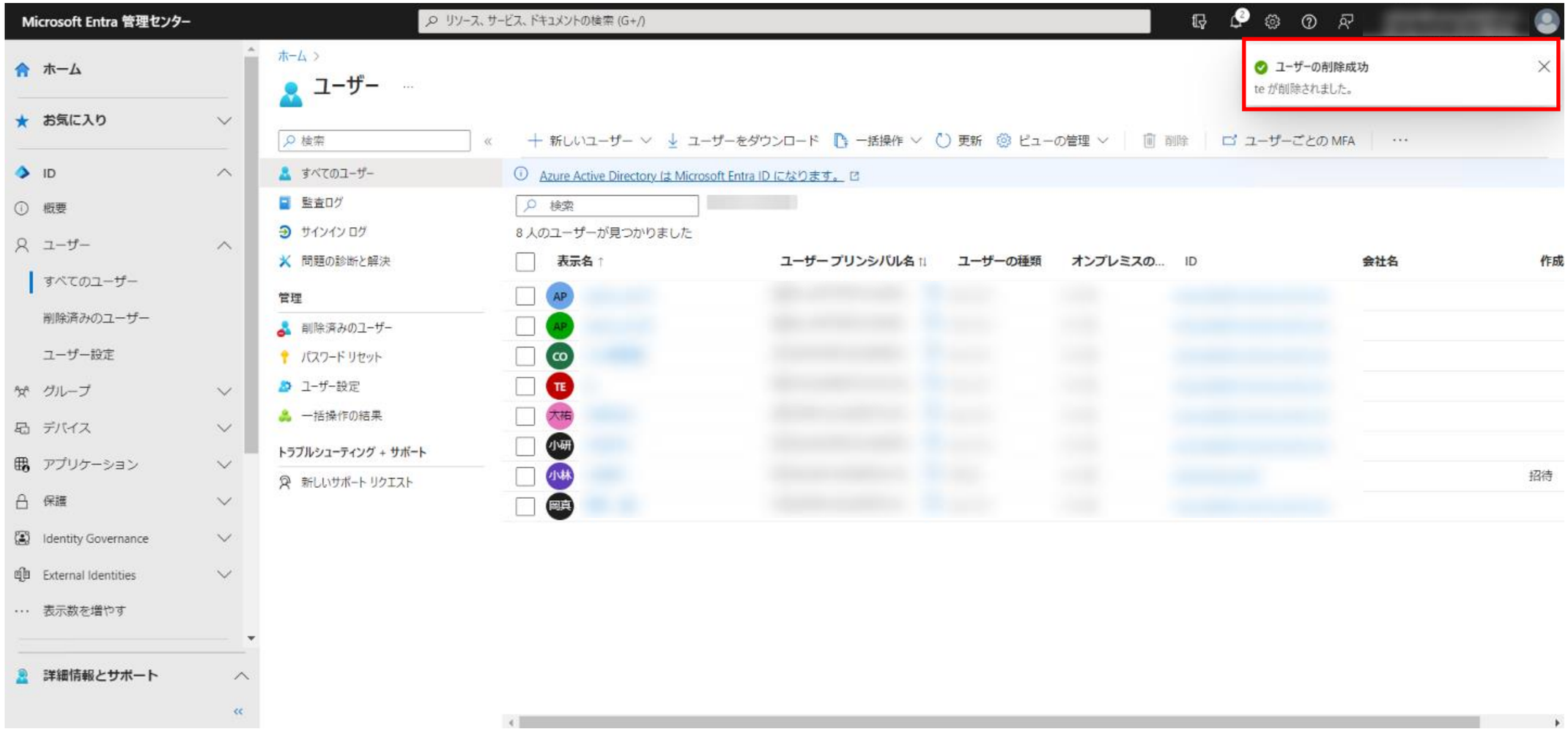
Ⅰ-2　アカウントの削除方法

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



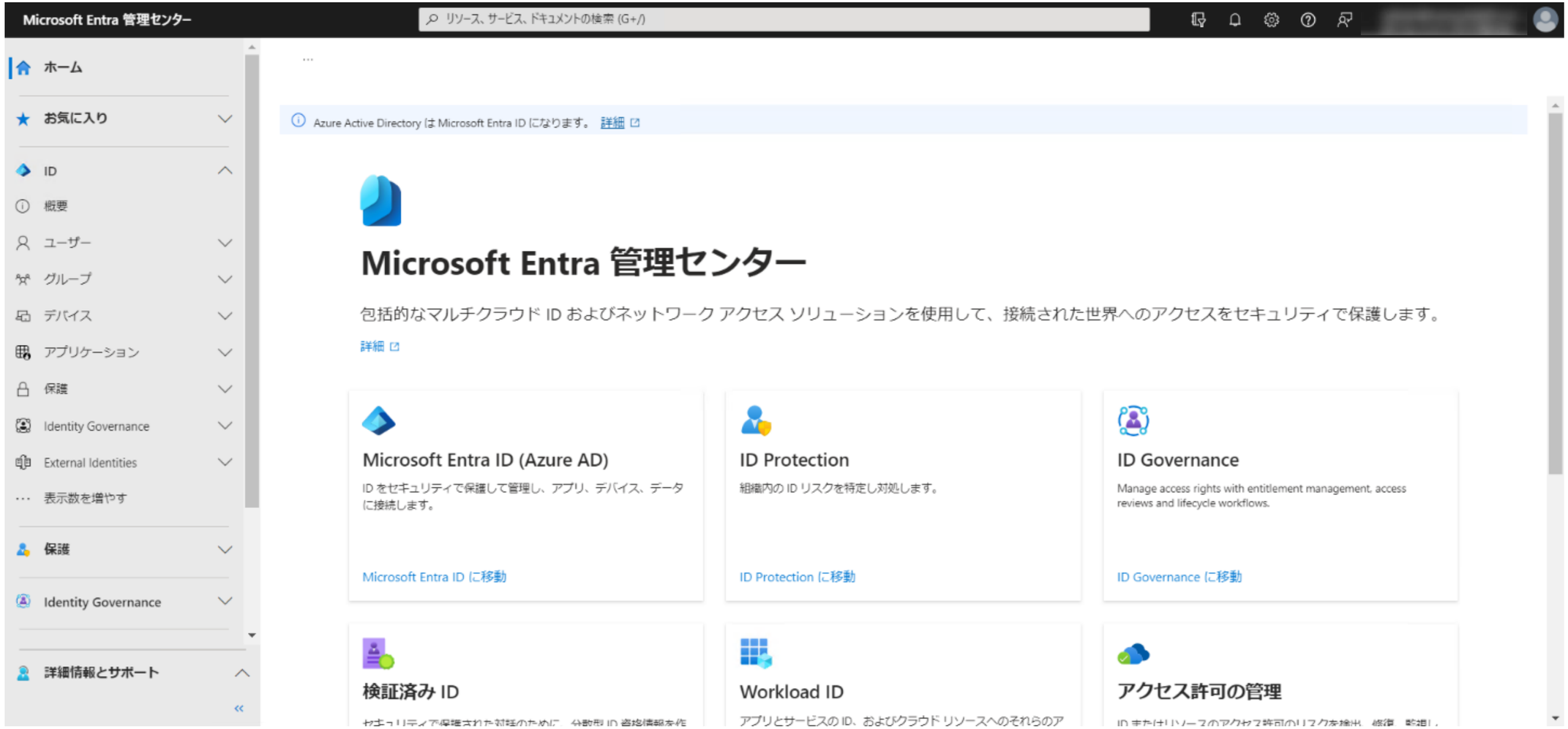
Ⅰ-2　アカウントの削除方法

5.「ユーザーの削除成功」が表示されたら完了です



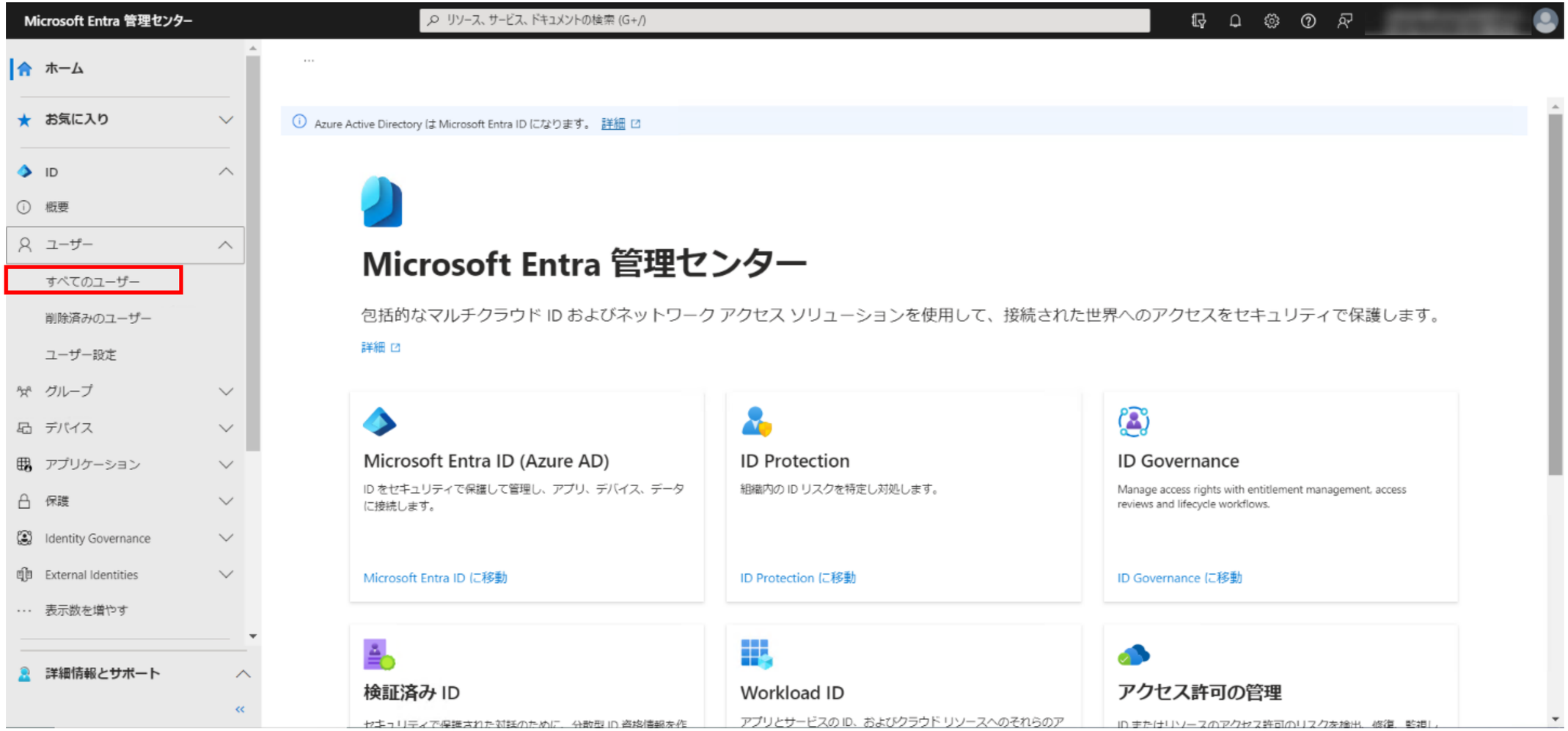
Ⅰ-3　ライセンスの割り当て方法

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



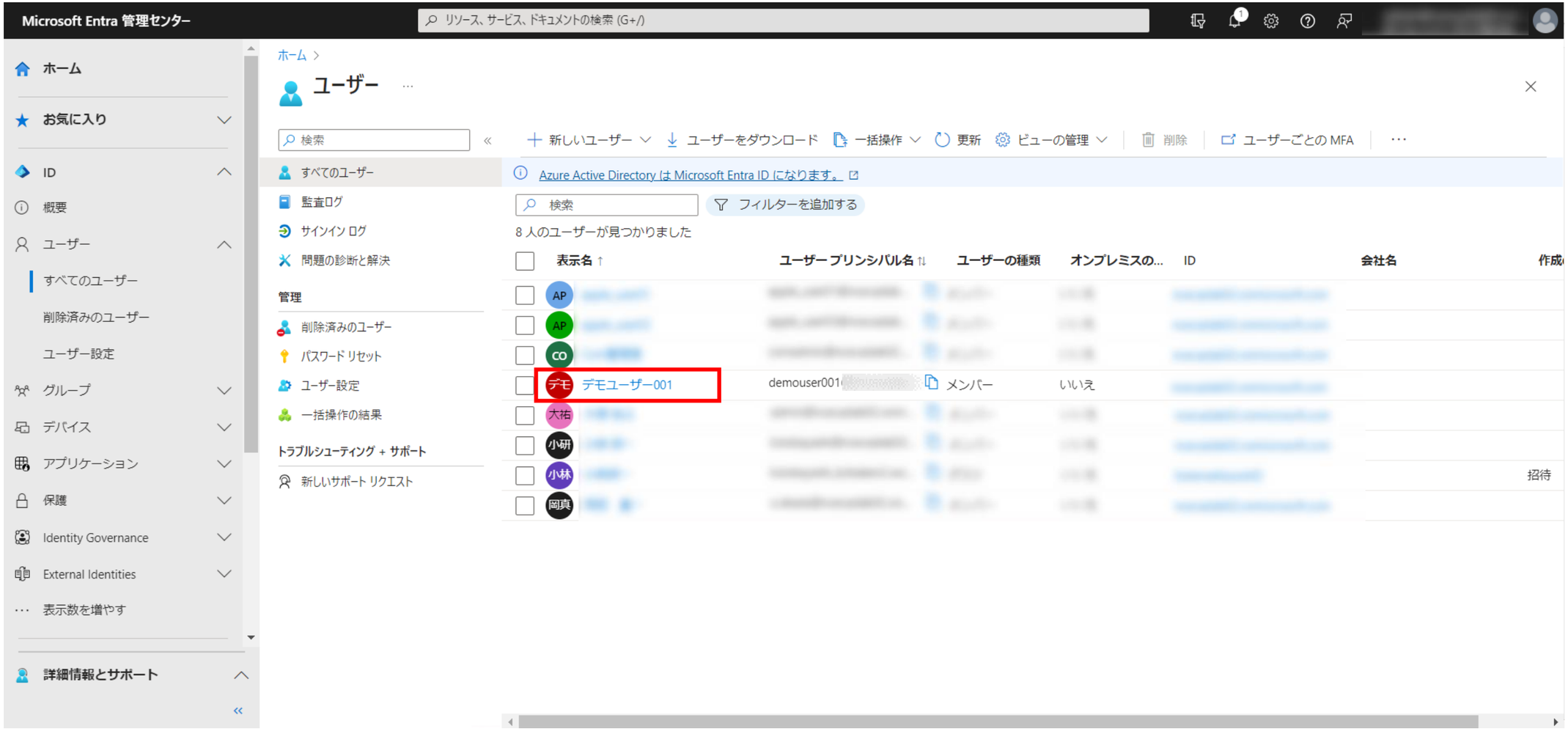
Ⅰ-3　ライセンスの割り当て方法

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



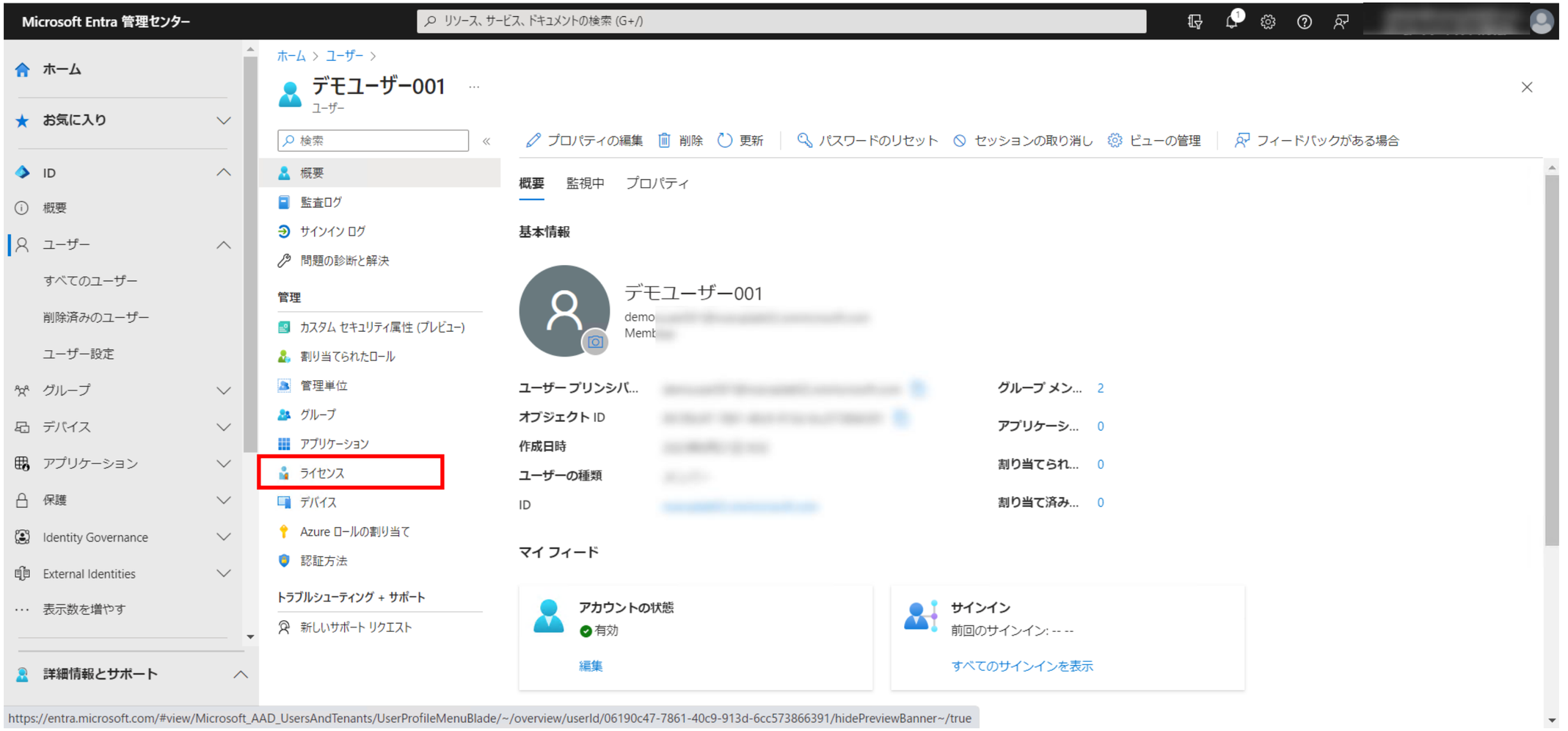
Ⅰ-3　ライセンスの割り当て方法

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



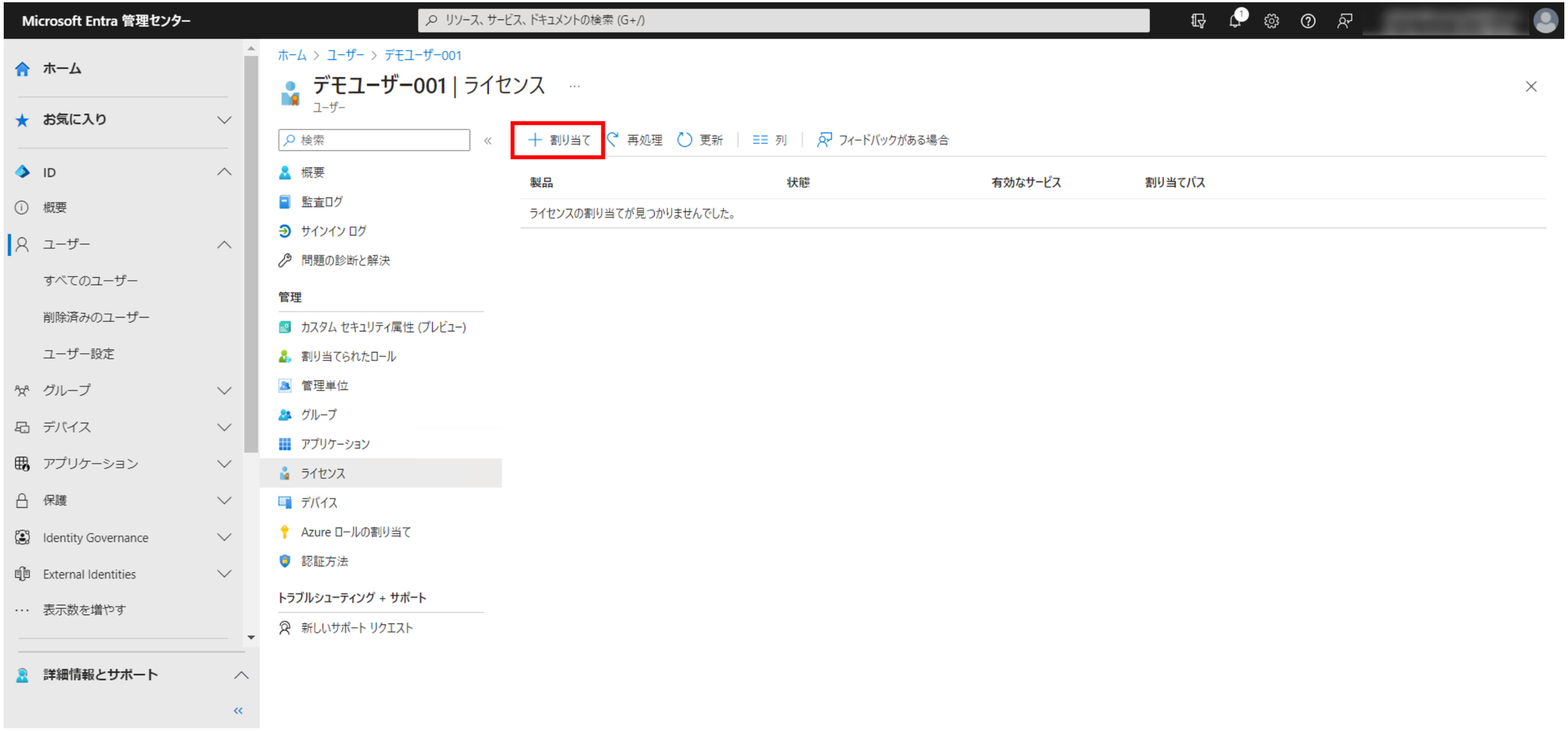
Ⅰ-3　ライセンスの割り当て方法

4.[ライセンス]をクリックします



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

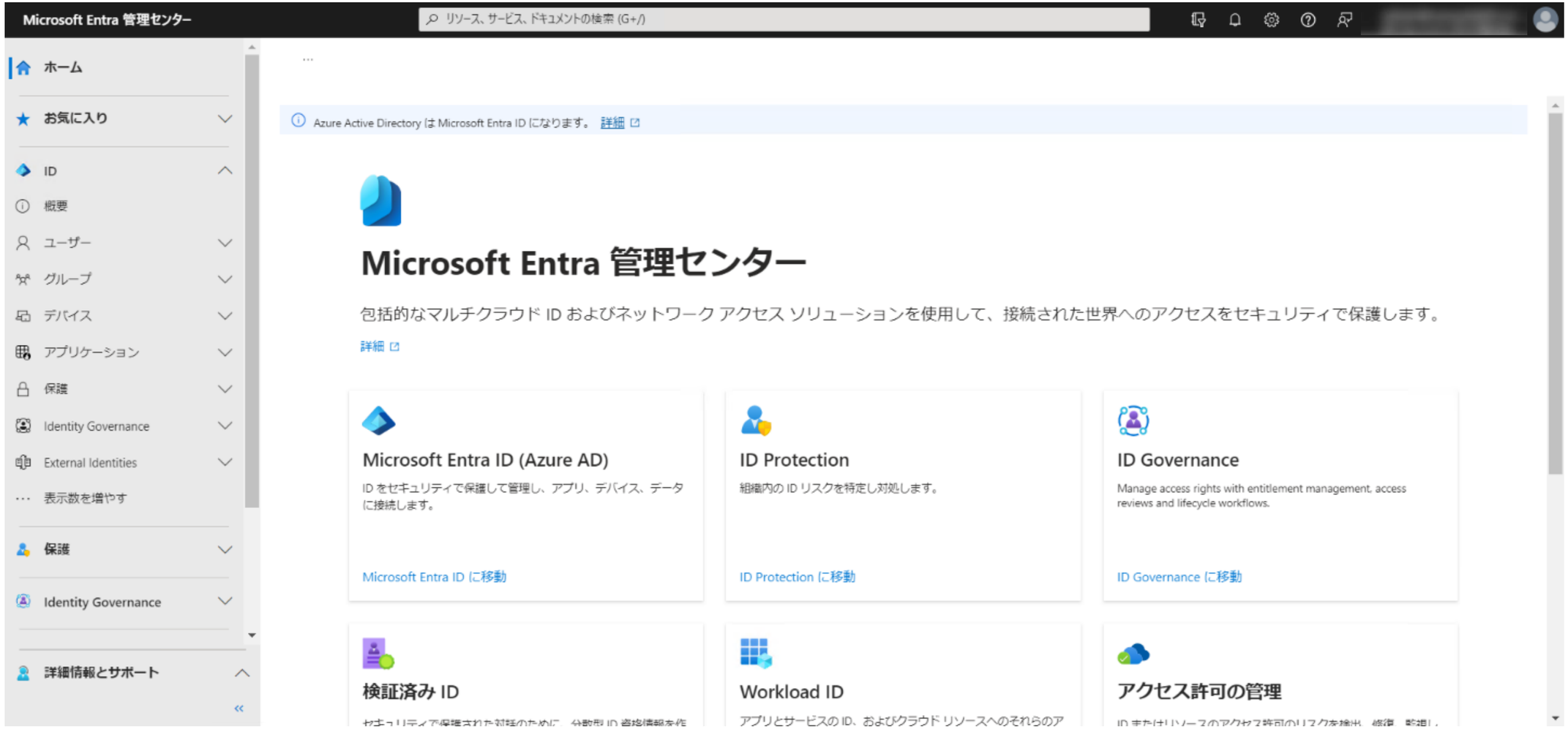
6.割り当てたいライセンス[□]にチェックを入れます

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

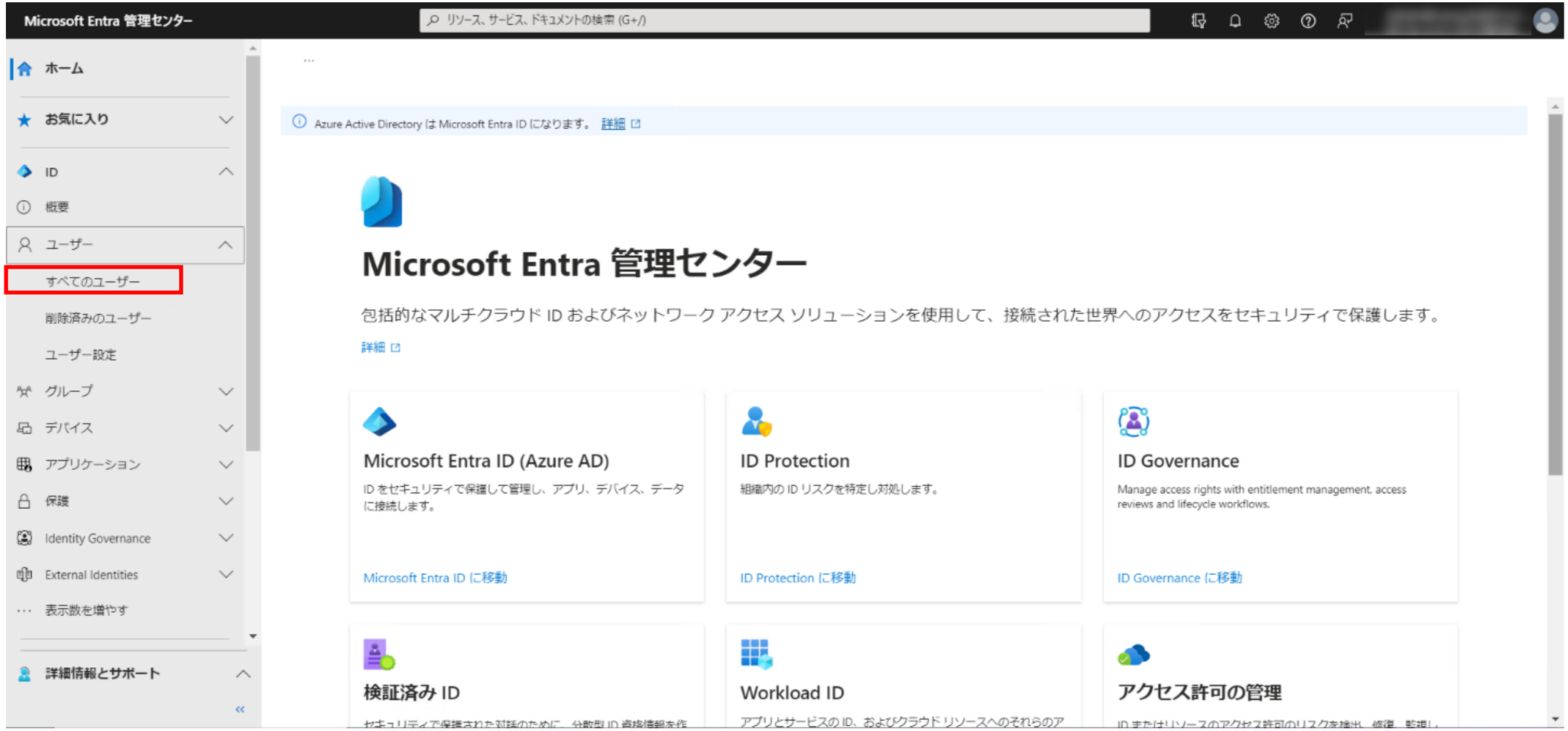
Ⅰ-4　ライセンスの割り当てを外す方法

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



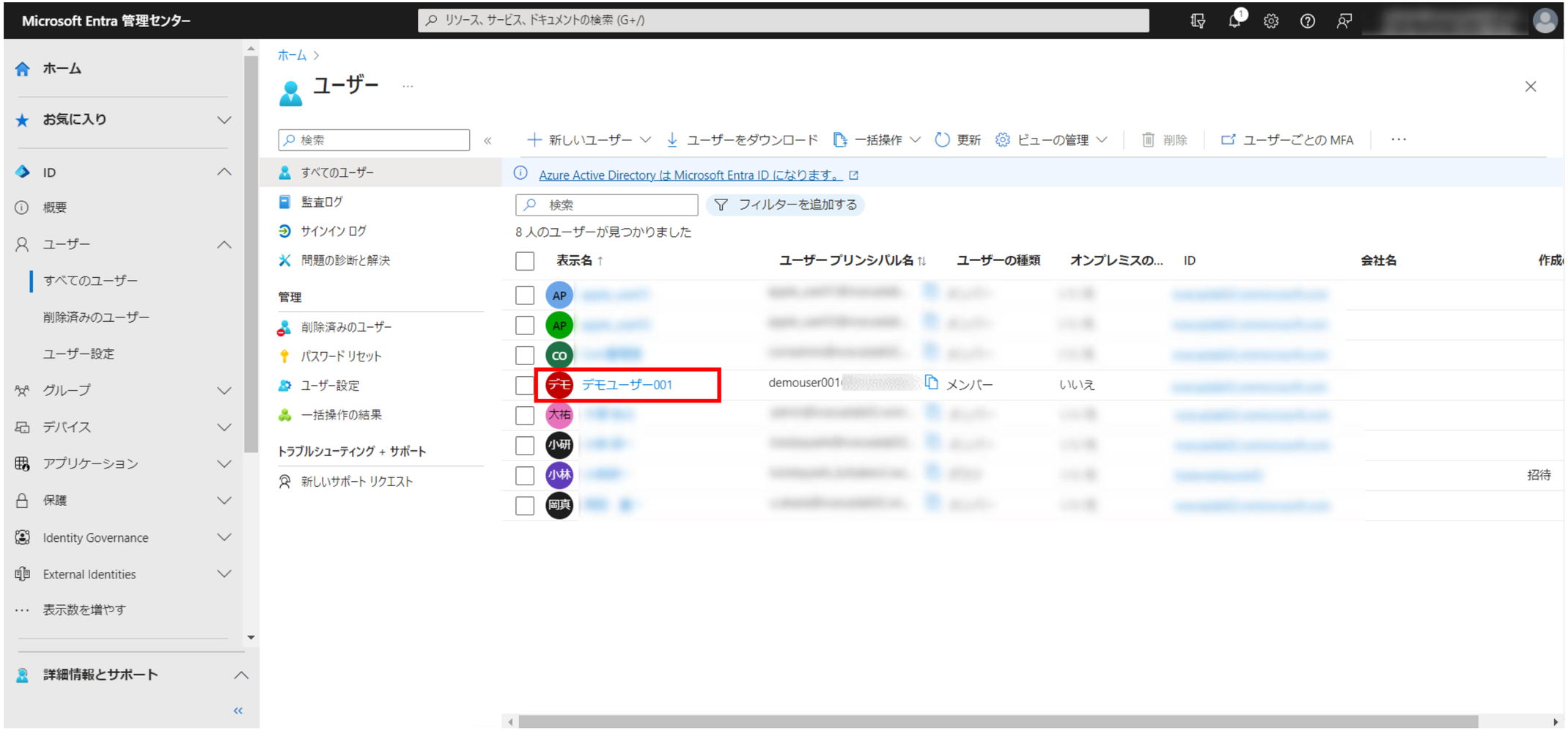
Ⅰ-4　ライセンスの割り当てを外す方法

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



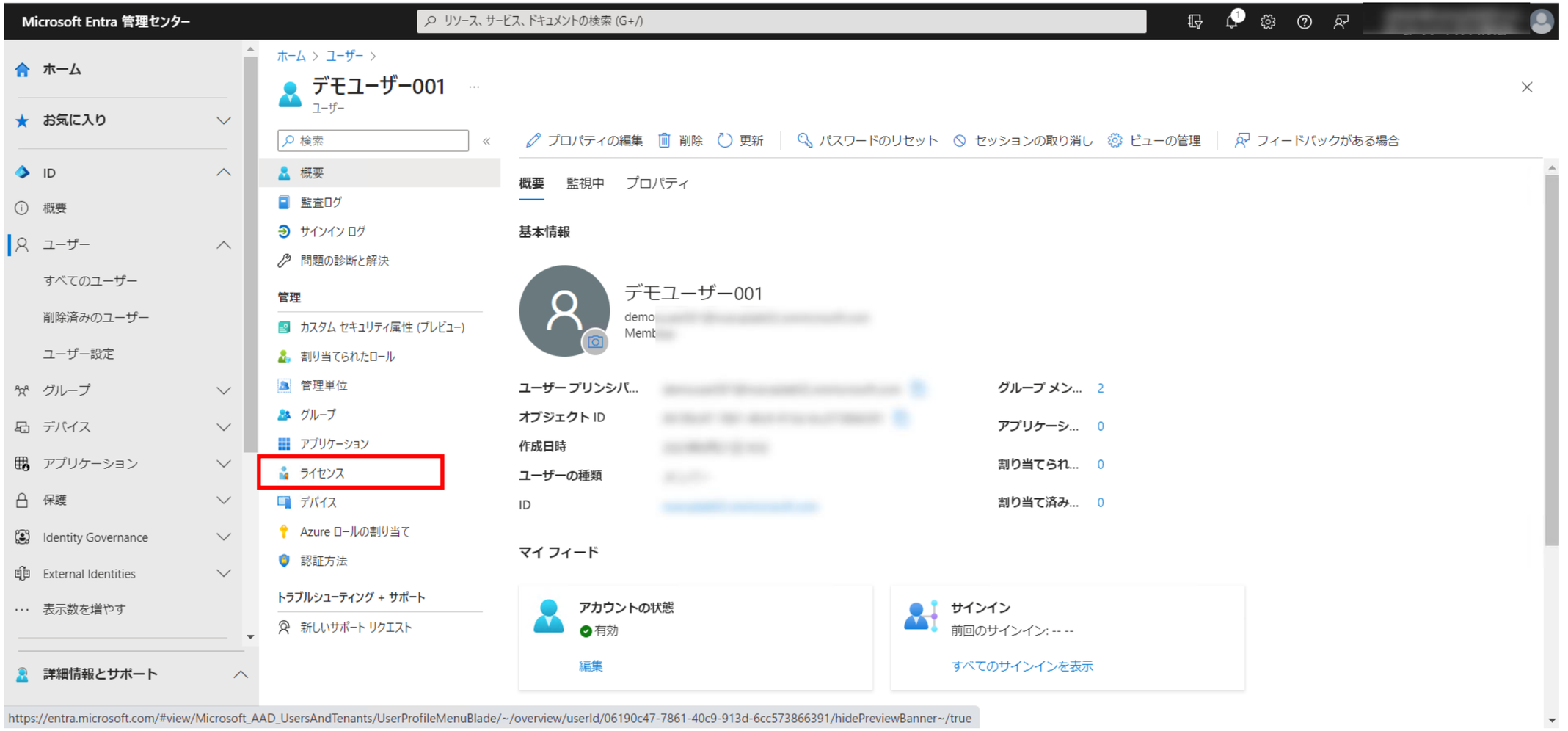
Ⅰ-4　ライセンスの割り当てを外す方法

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



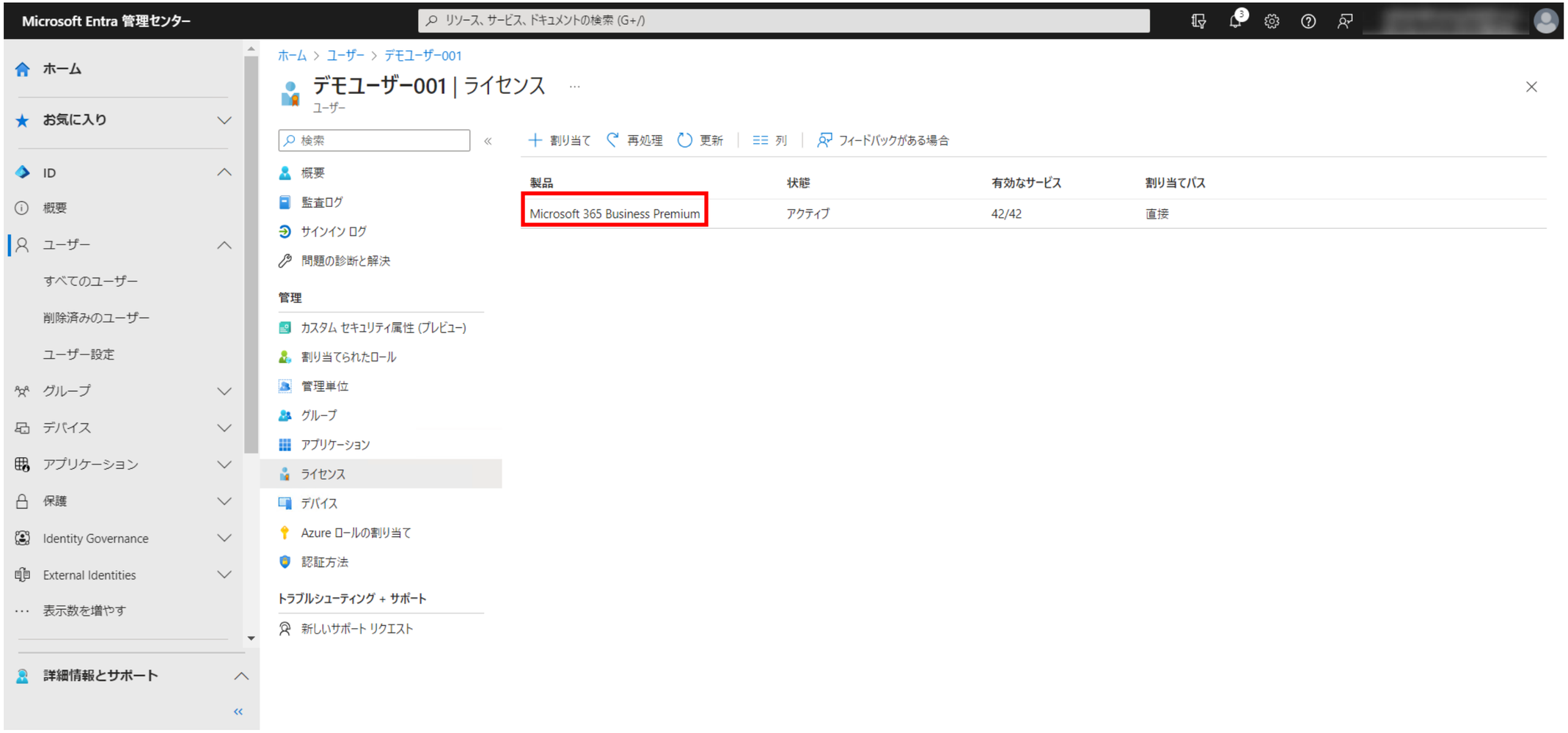
Ⅰ-4　ライセンスの割り当てを外す方法

4.[ライセンス]をクリックします



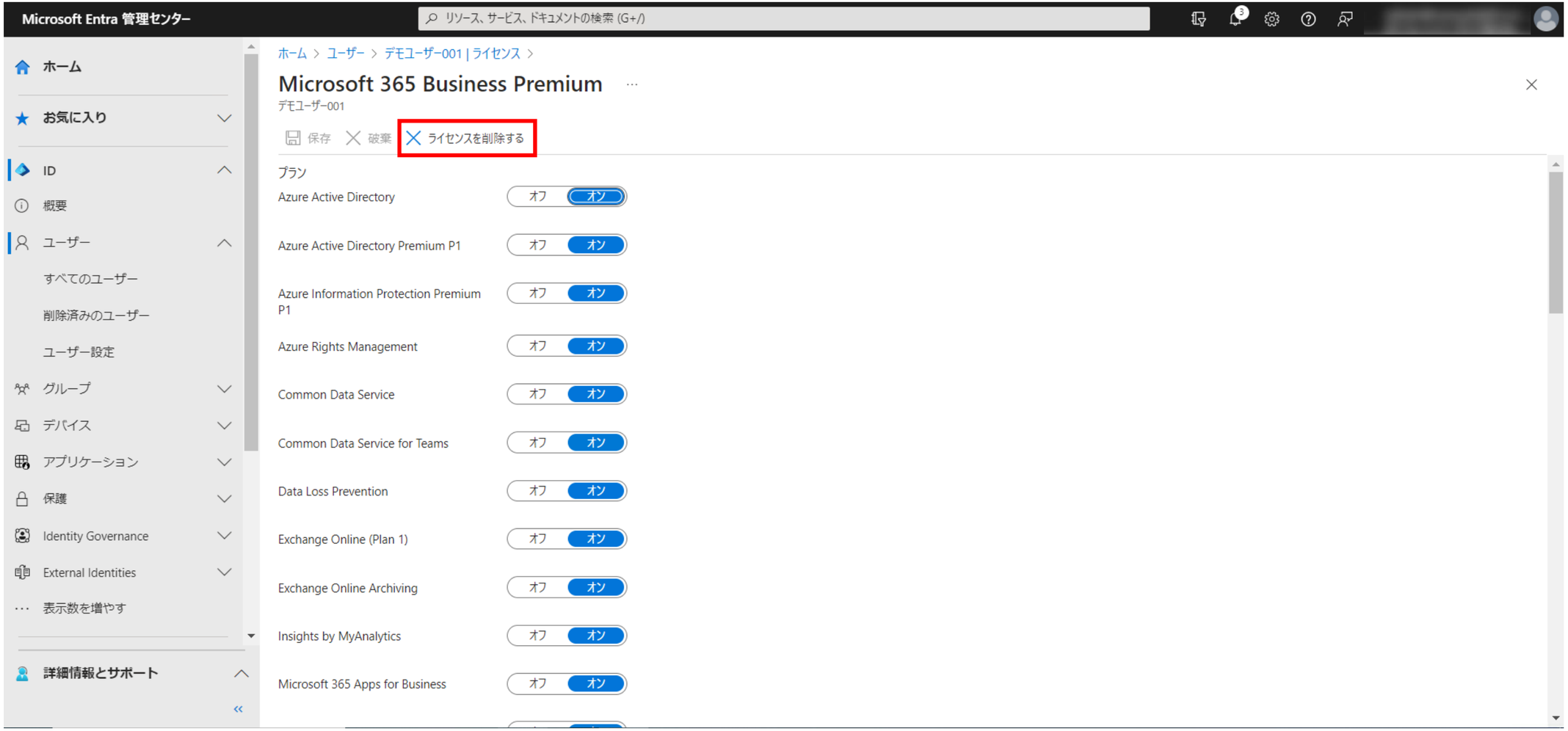
Ⅰ-4　ライセンスの割り当てを外す方法

5.割り当てを外したいライセンスをクリックします



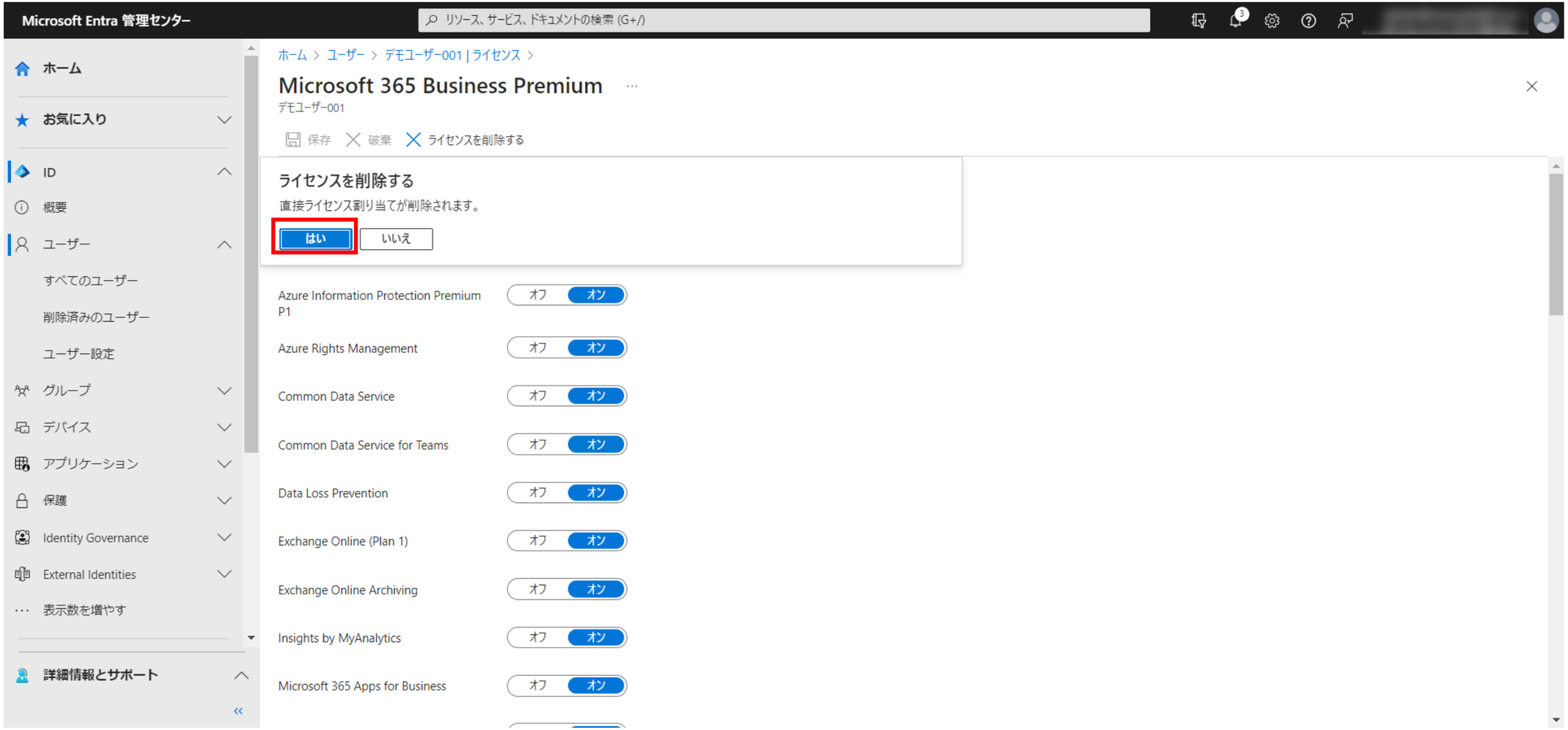
Ⅰ-4　ライセンスの割り当てを外す方法

6.[ライセンスを削除する]をクリックします



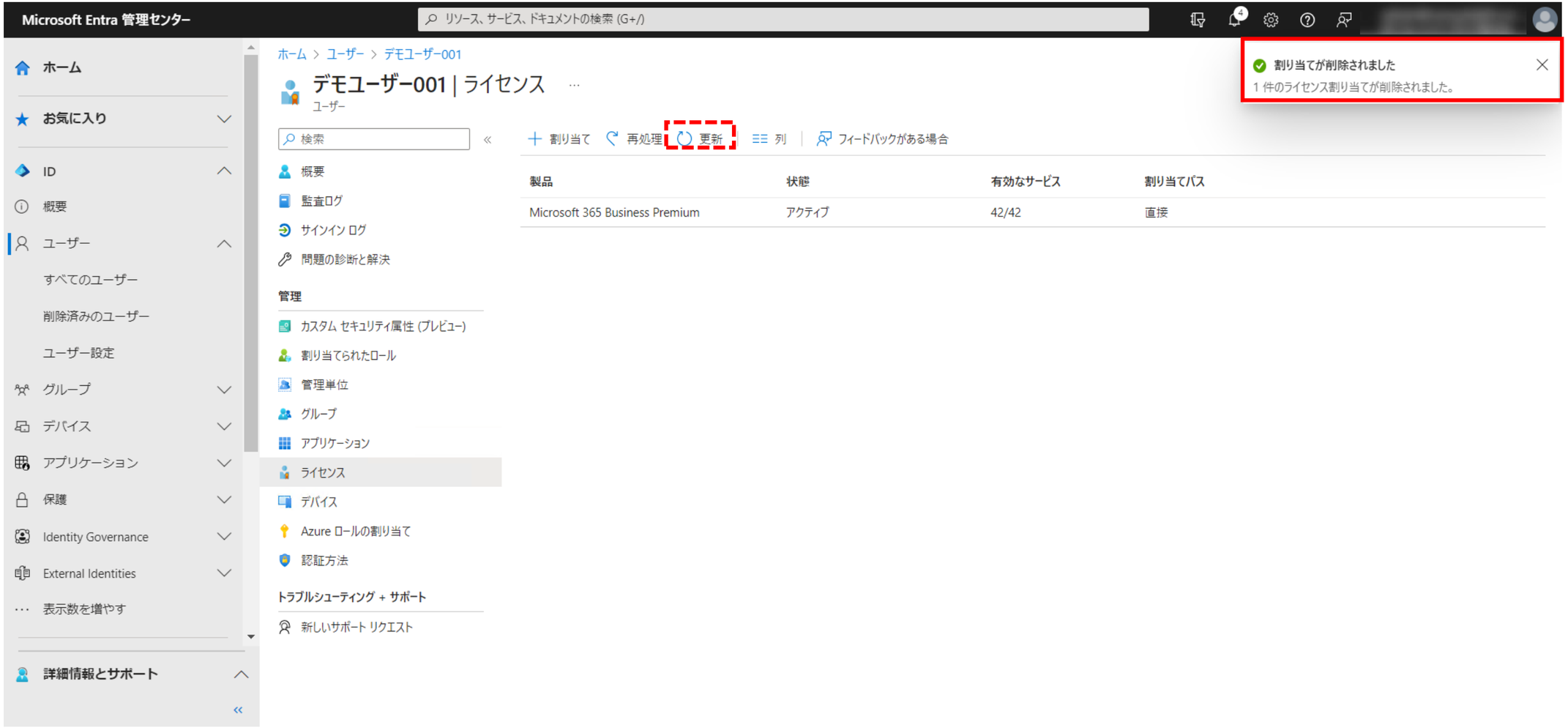
Ⅰ-4　ライセンスの割り当てを外す方法

7.[はい]をクリックします



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



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

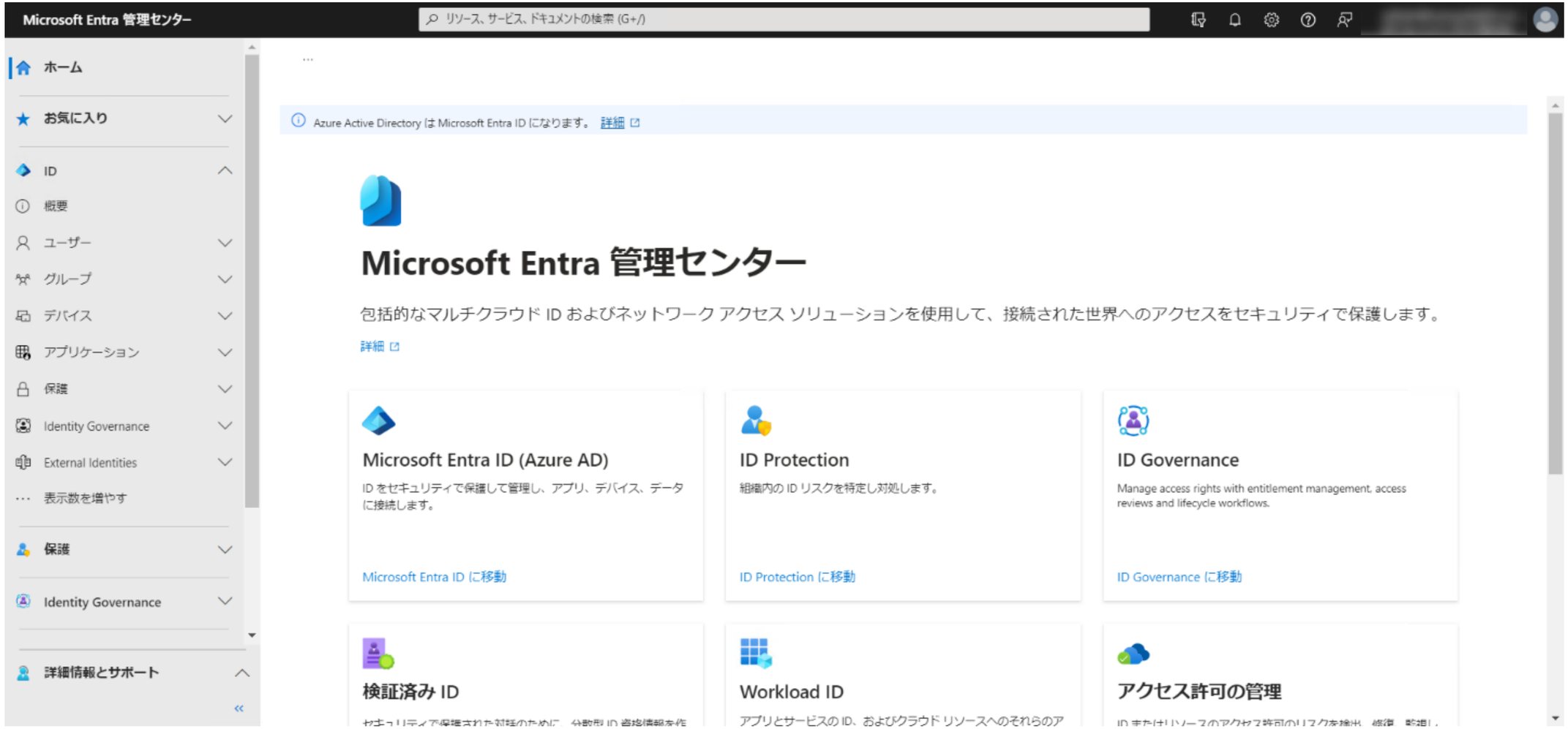
Ⅱ-1　ユーザーのパスワードのリセット方法

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。

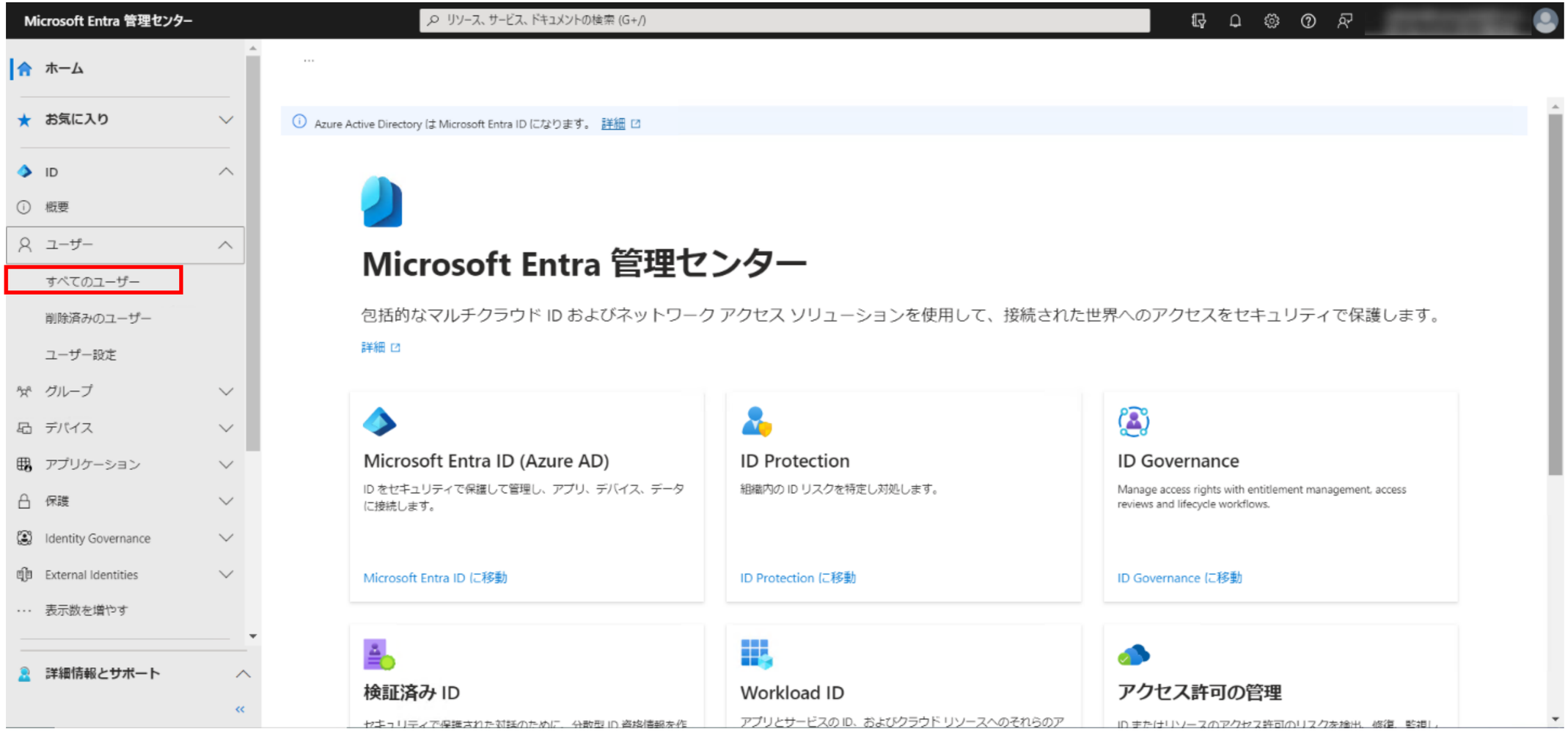
Ⅱ-1　ユーザーのパスワードのリセット方法

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



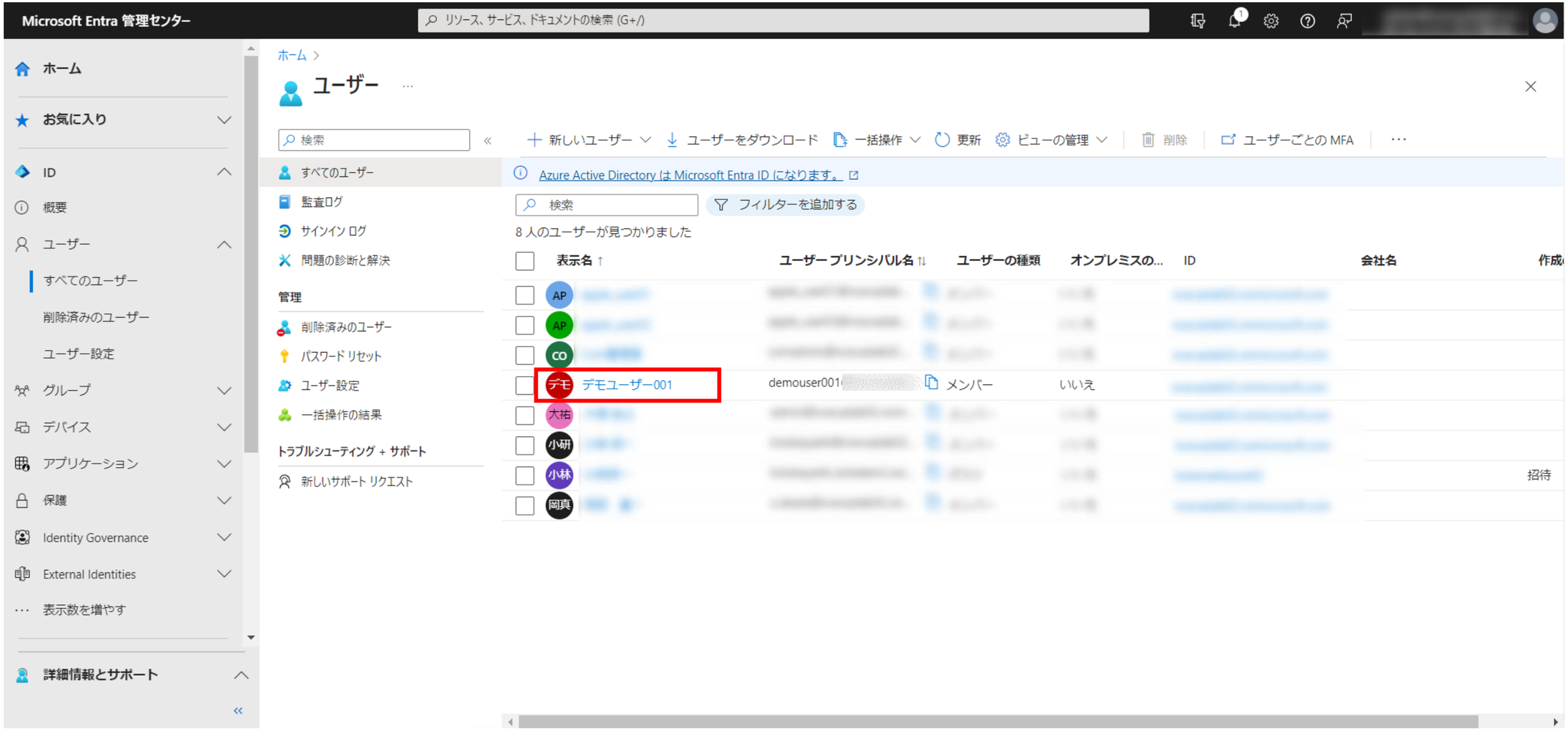
Ⅱ-1　ユーザーのパスワードのリセット方法

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



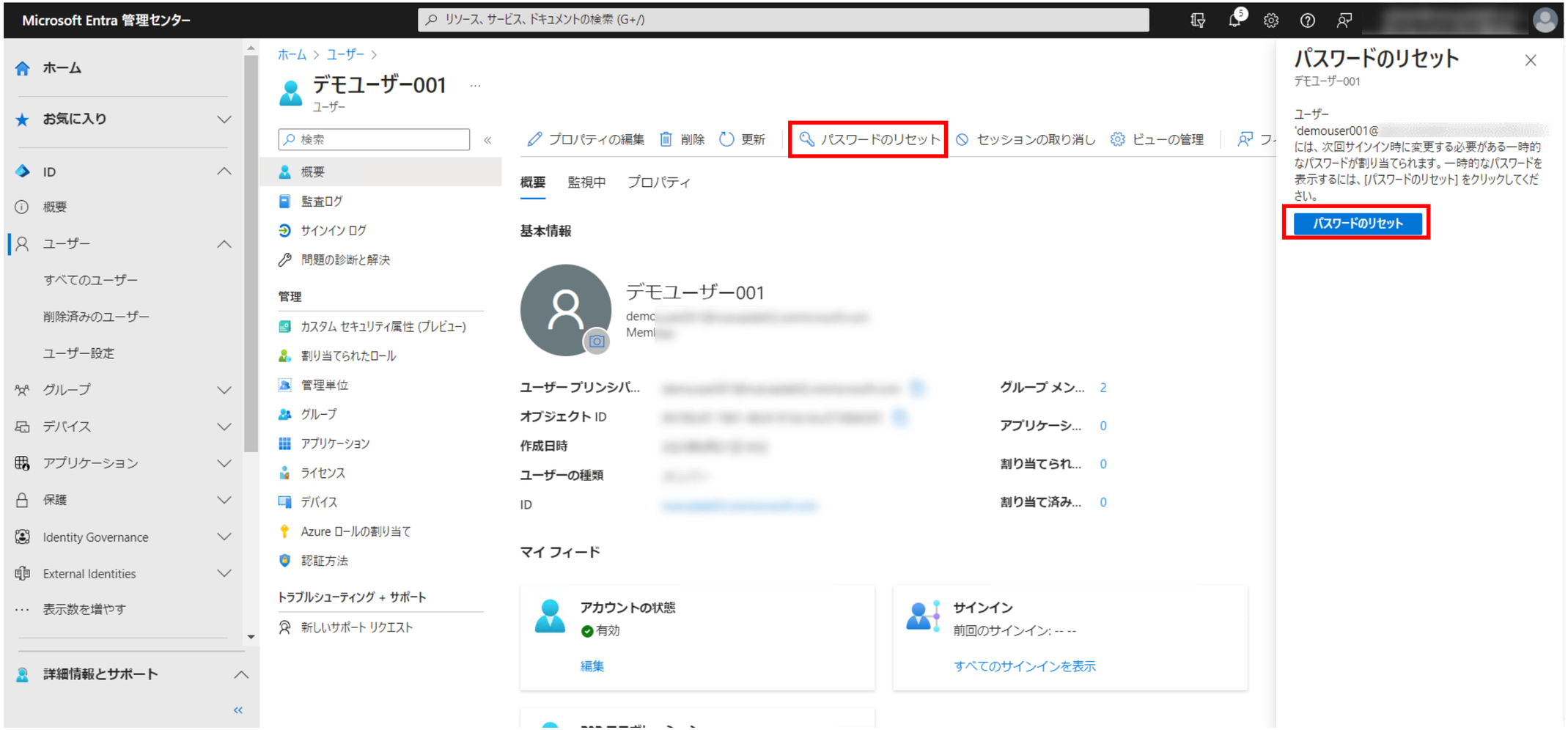
Ⅱ-1　ユーザーのパスワードのリセット方法

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



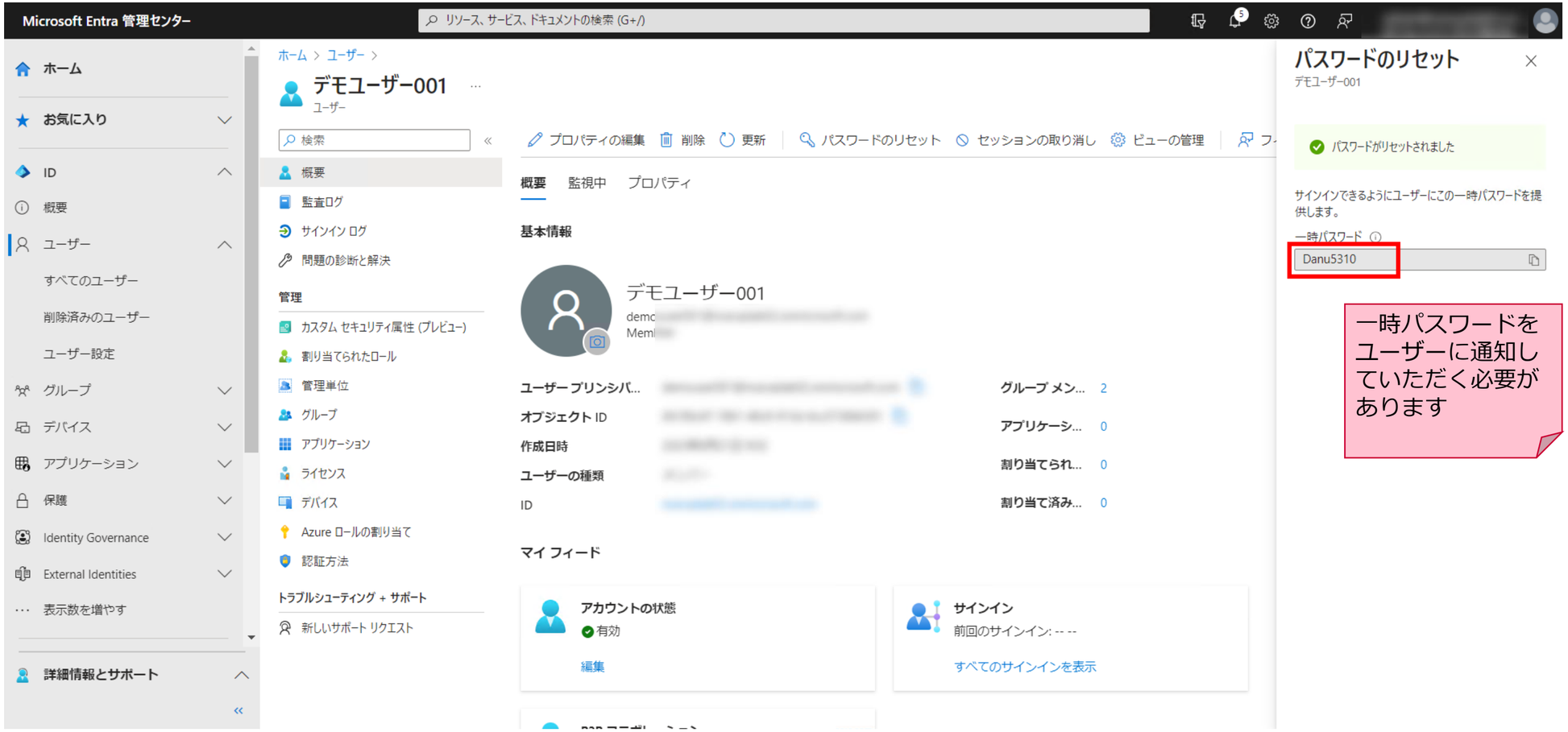
Ⅱ-1　ユーザーのパスワードのリセット方法

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



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



（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

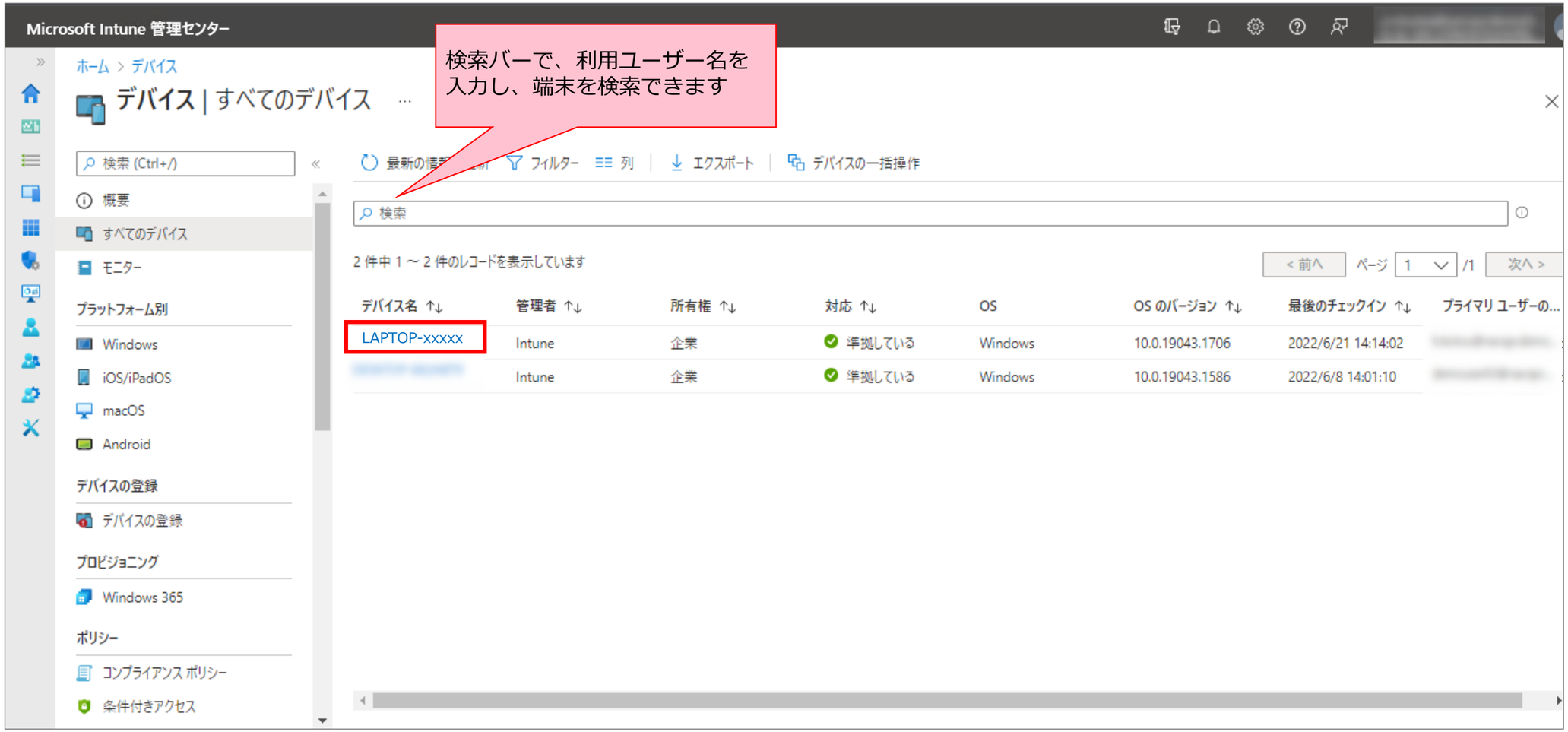
1.Microsoft Intune 管理センター（https://intune.microsoft.com/）にアクセスします

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

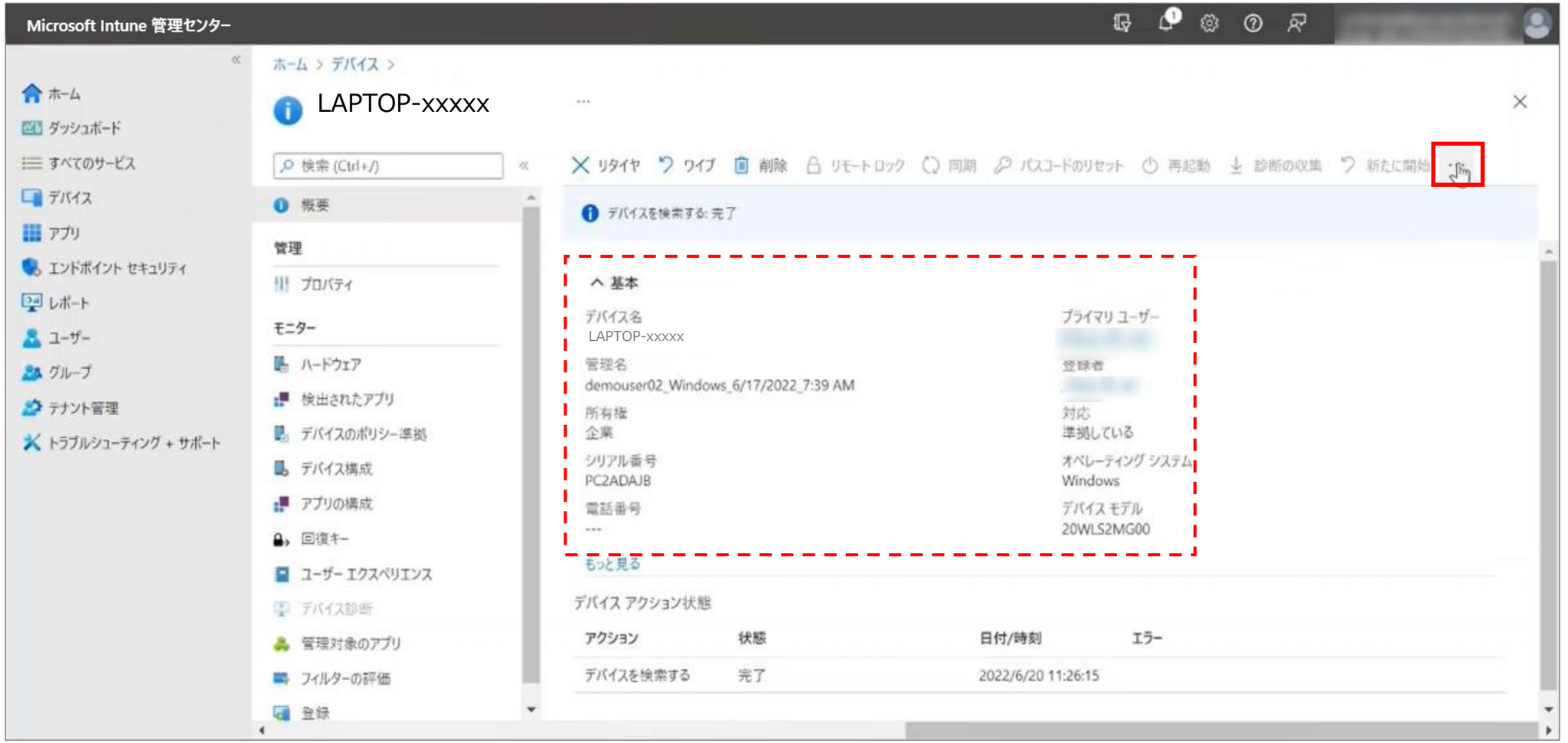
Ⅲ-1　端末のリセット、及び新規ユーザーのログイン

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



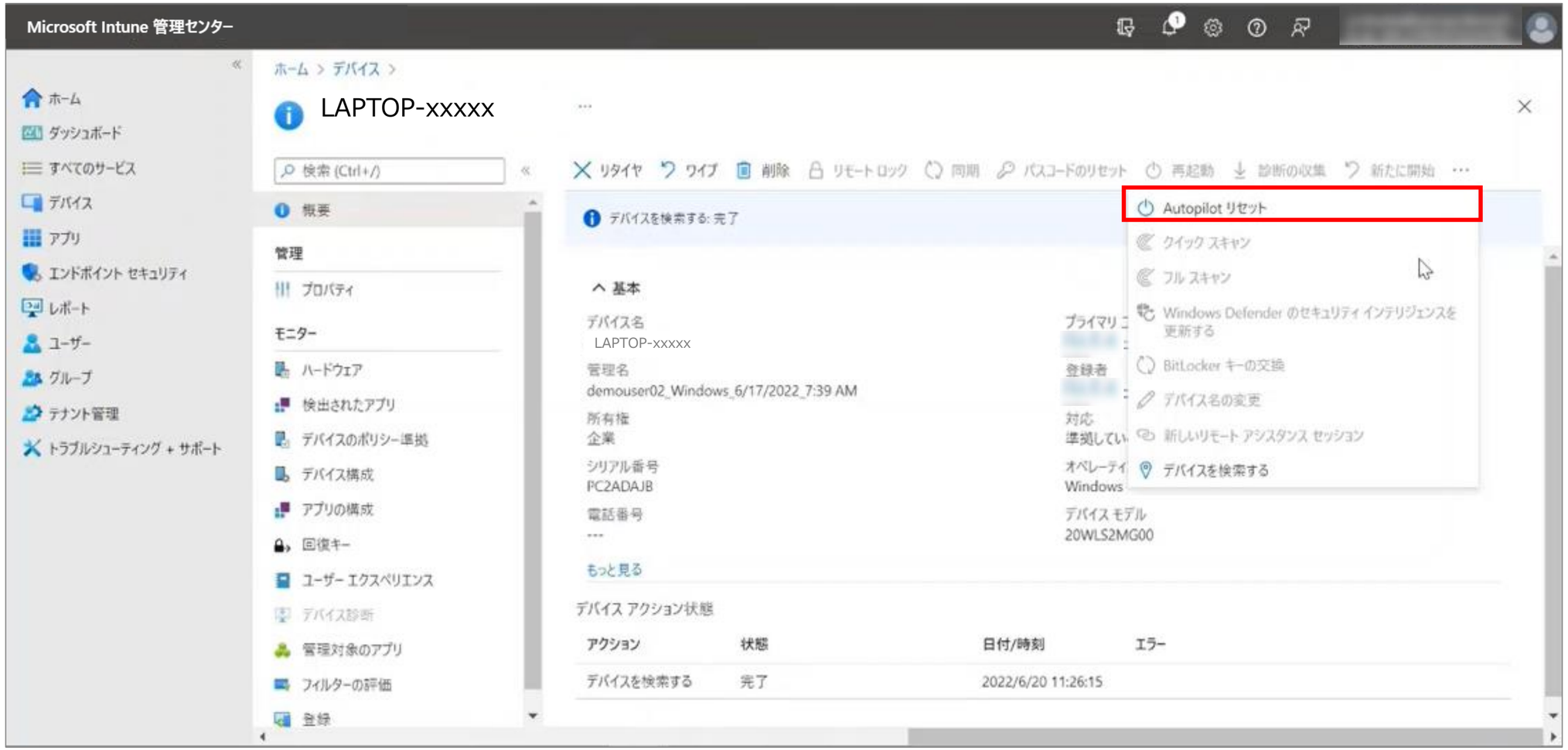
Ⅲ-1　端末のリセット、及び新規ユーザーのログイン

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



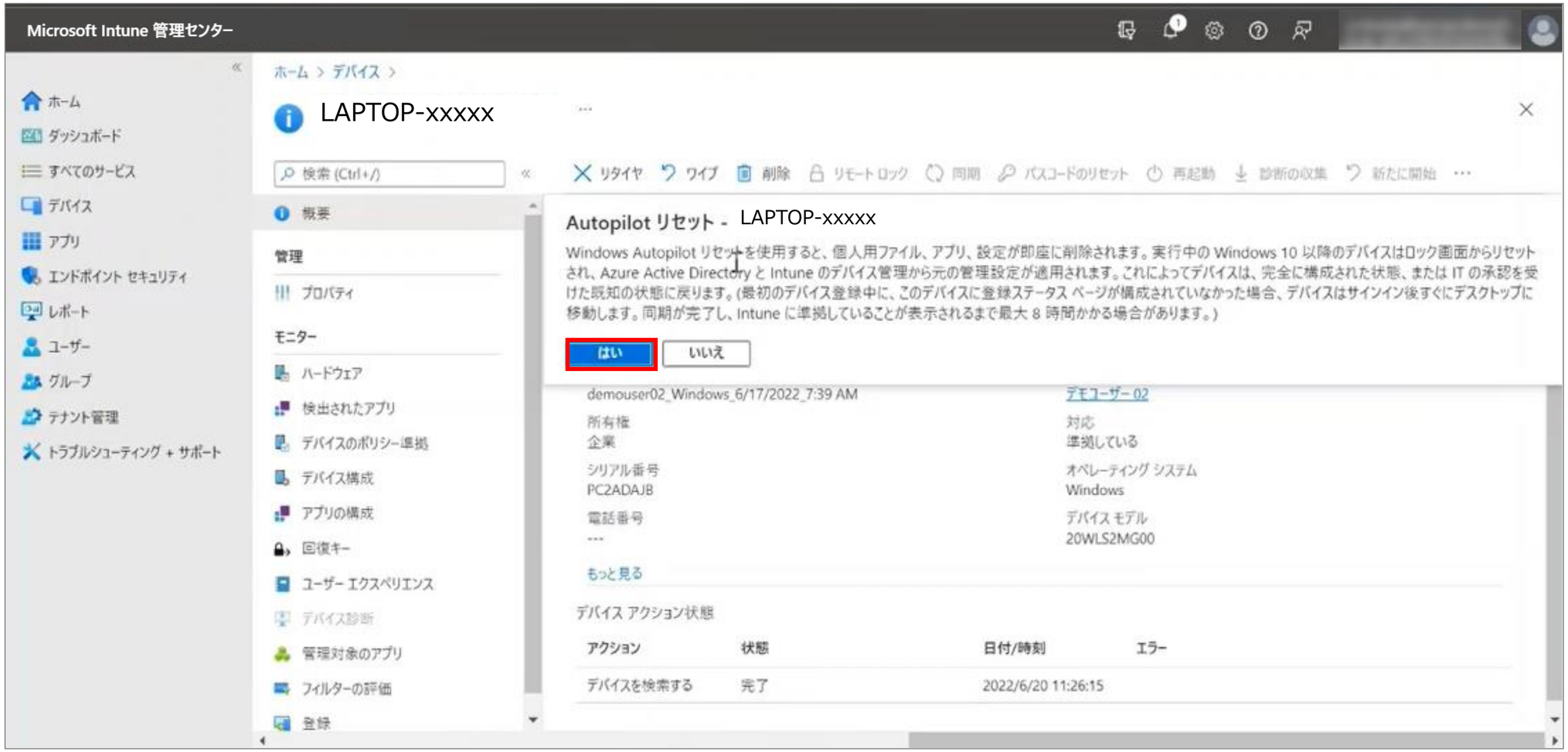
Ⅲ-1　端末のリセット、及び新規ユーザーのログイン

5. [Autopilot リセット]をクリックします



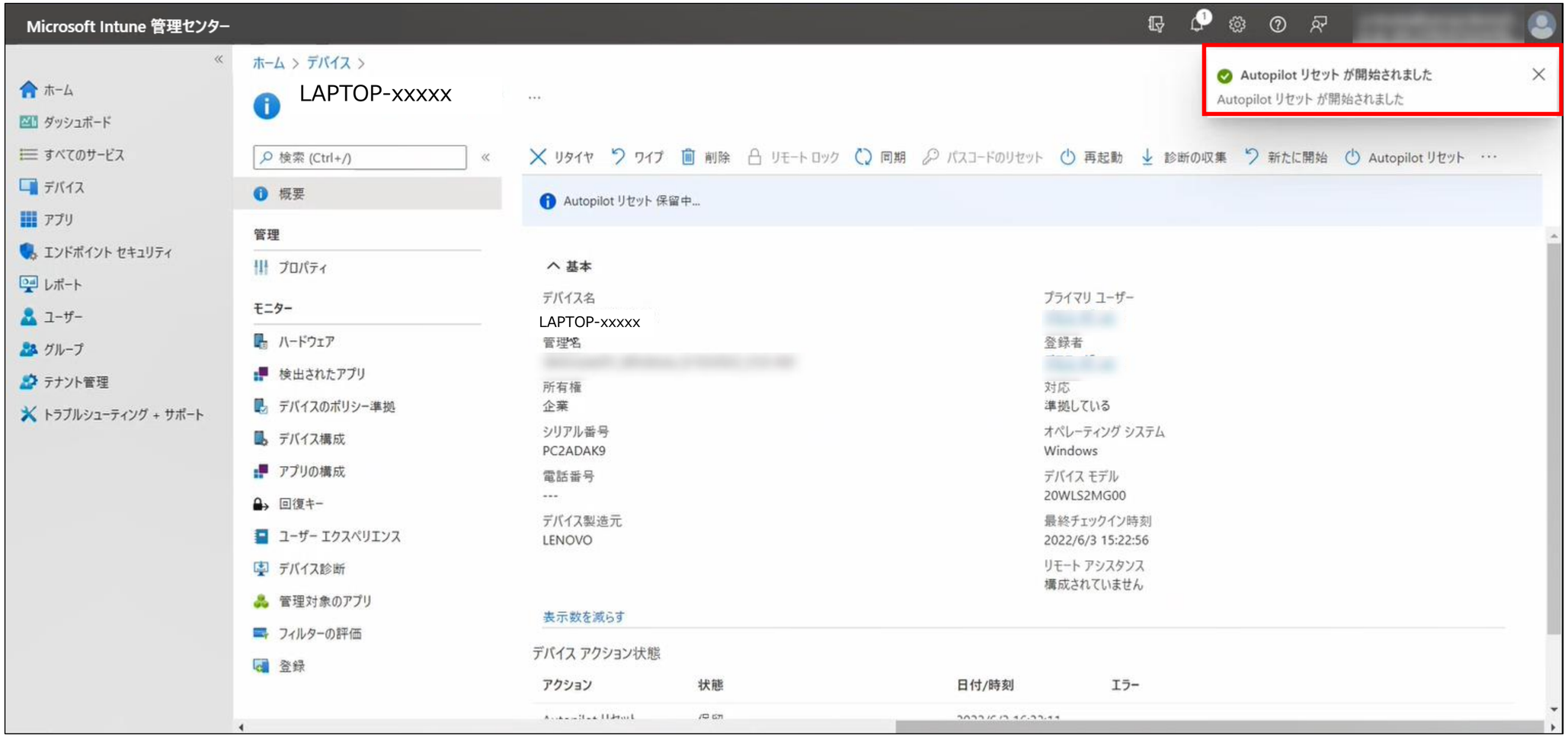
Ⅲ-1　端末のリセット、及び新規ユーザーのログイン

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



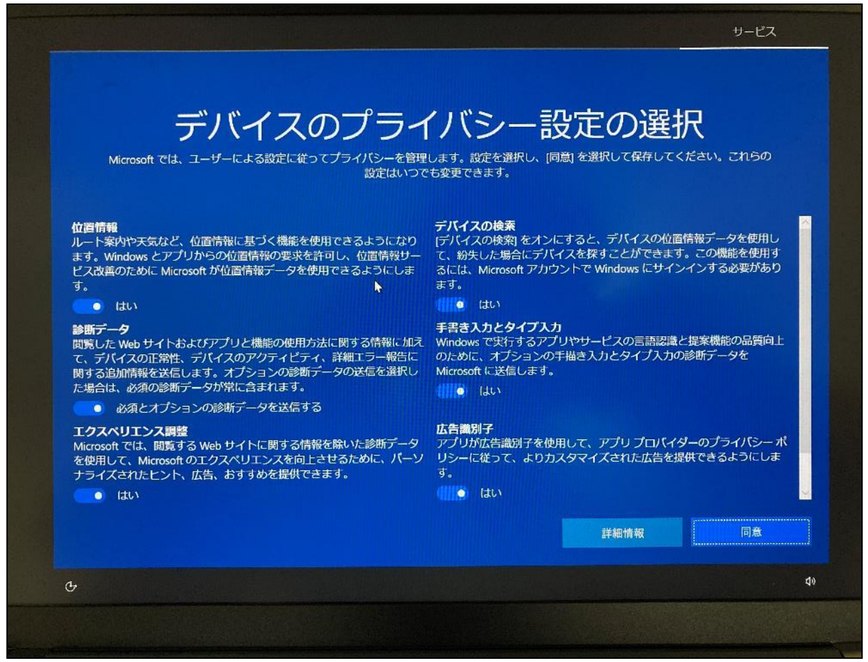
Ⅲ-1　端末のリセット、及び新規ユーザーのログイン

※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

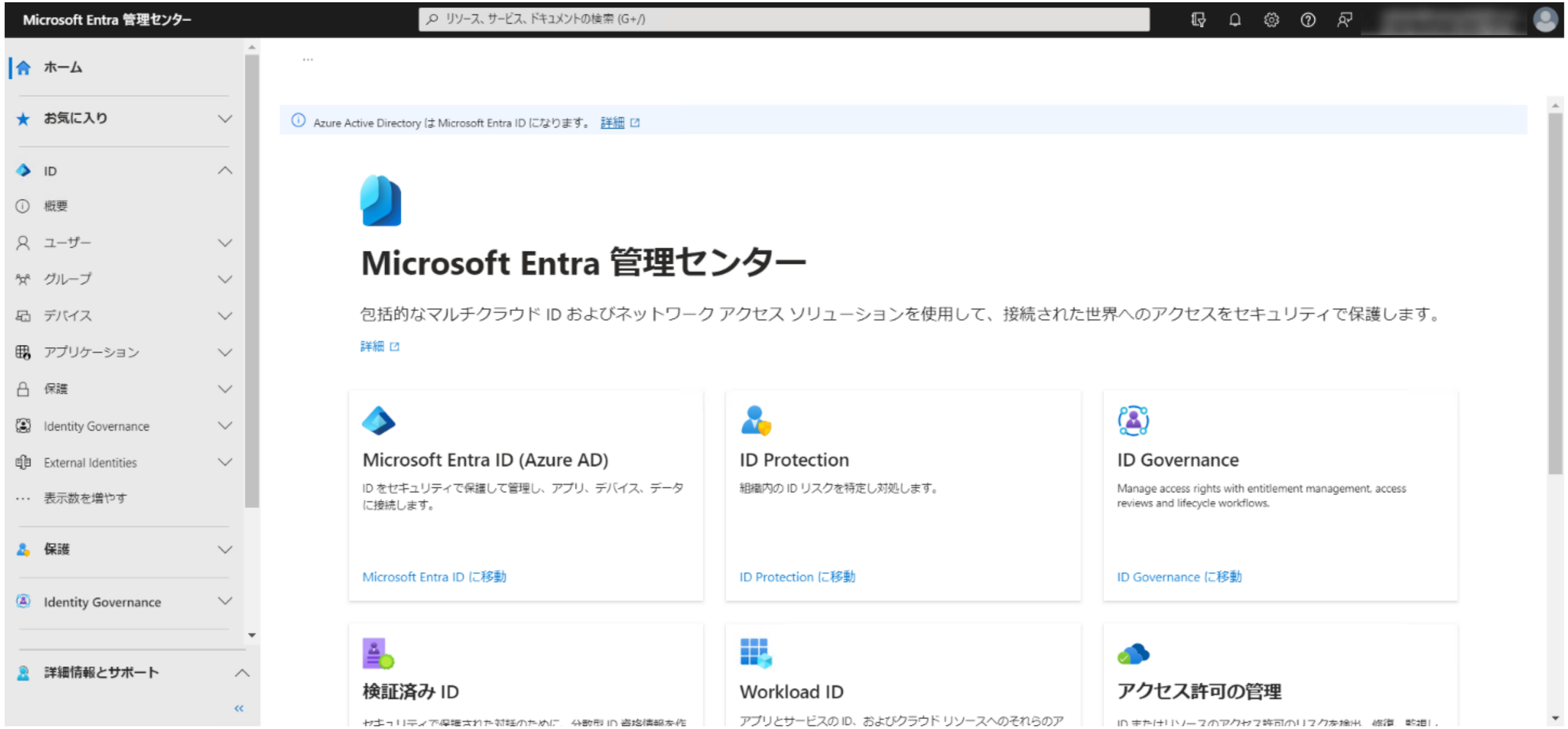
Ⅳ.ユーザーにデバイス管理者権限を付与したい場合の対処

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。

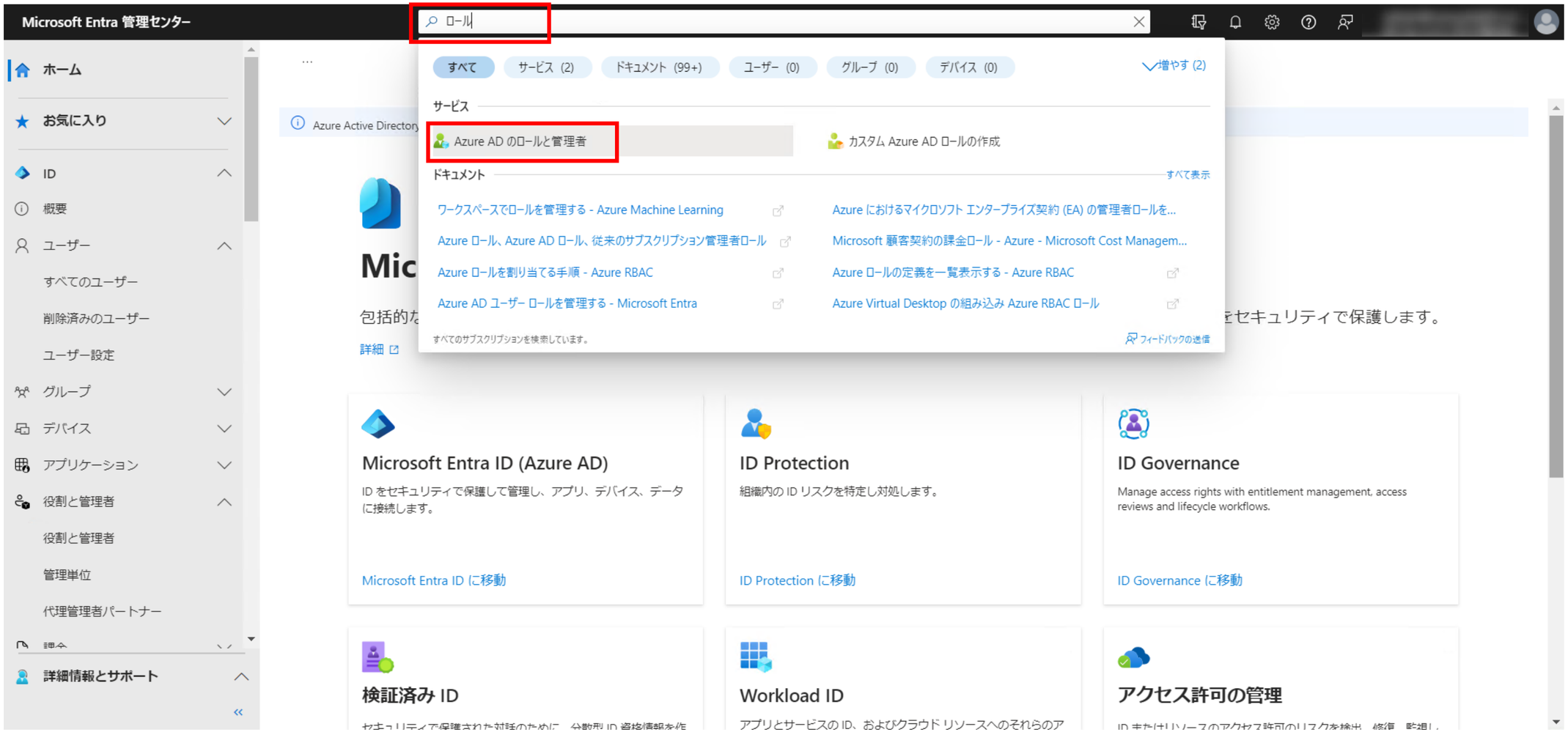
Ⅳ-1　ローカル管理者ロールの割り当て

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



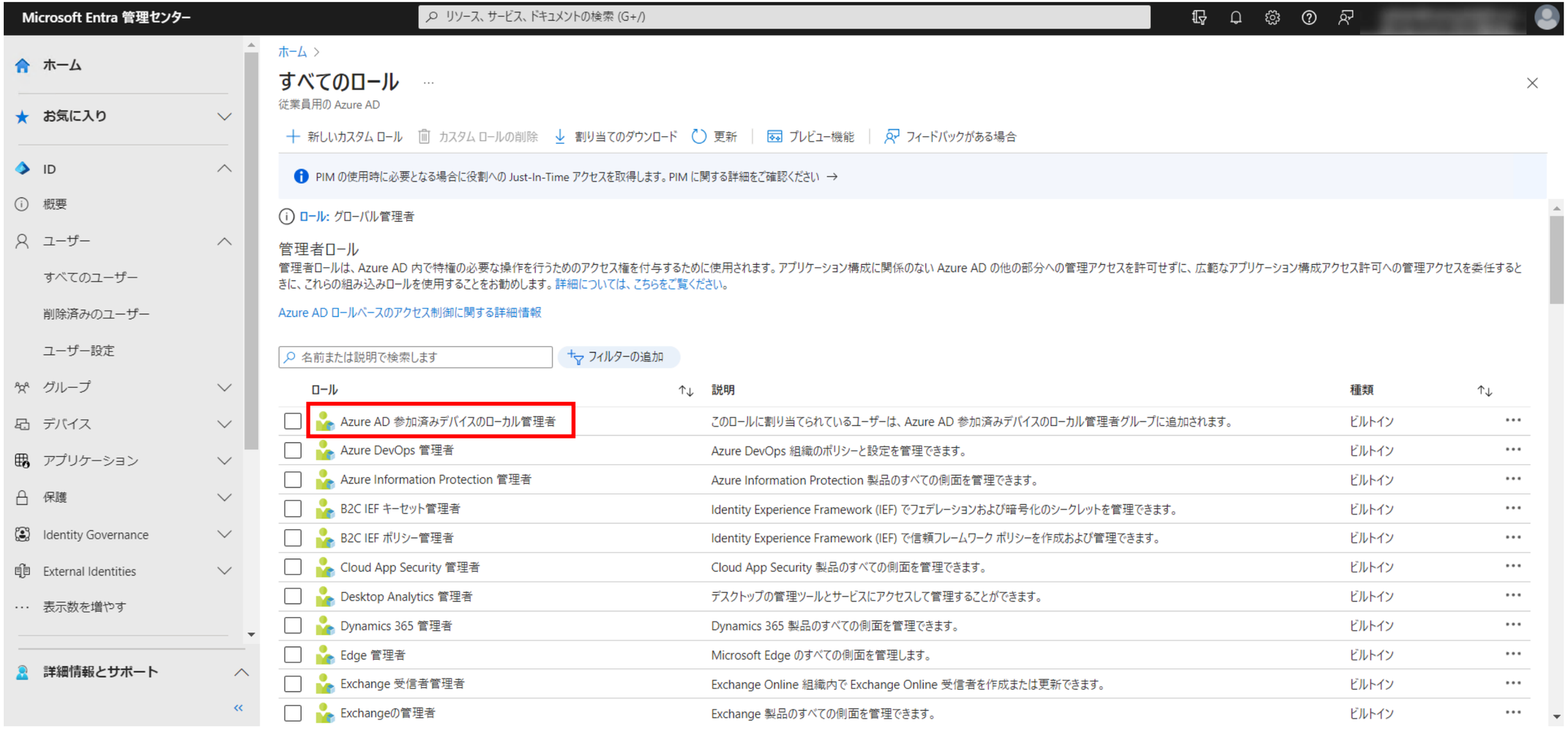
Ⅳ-1　ローカル管理者ロールの割り当て

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

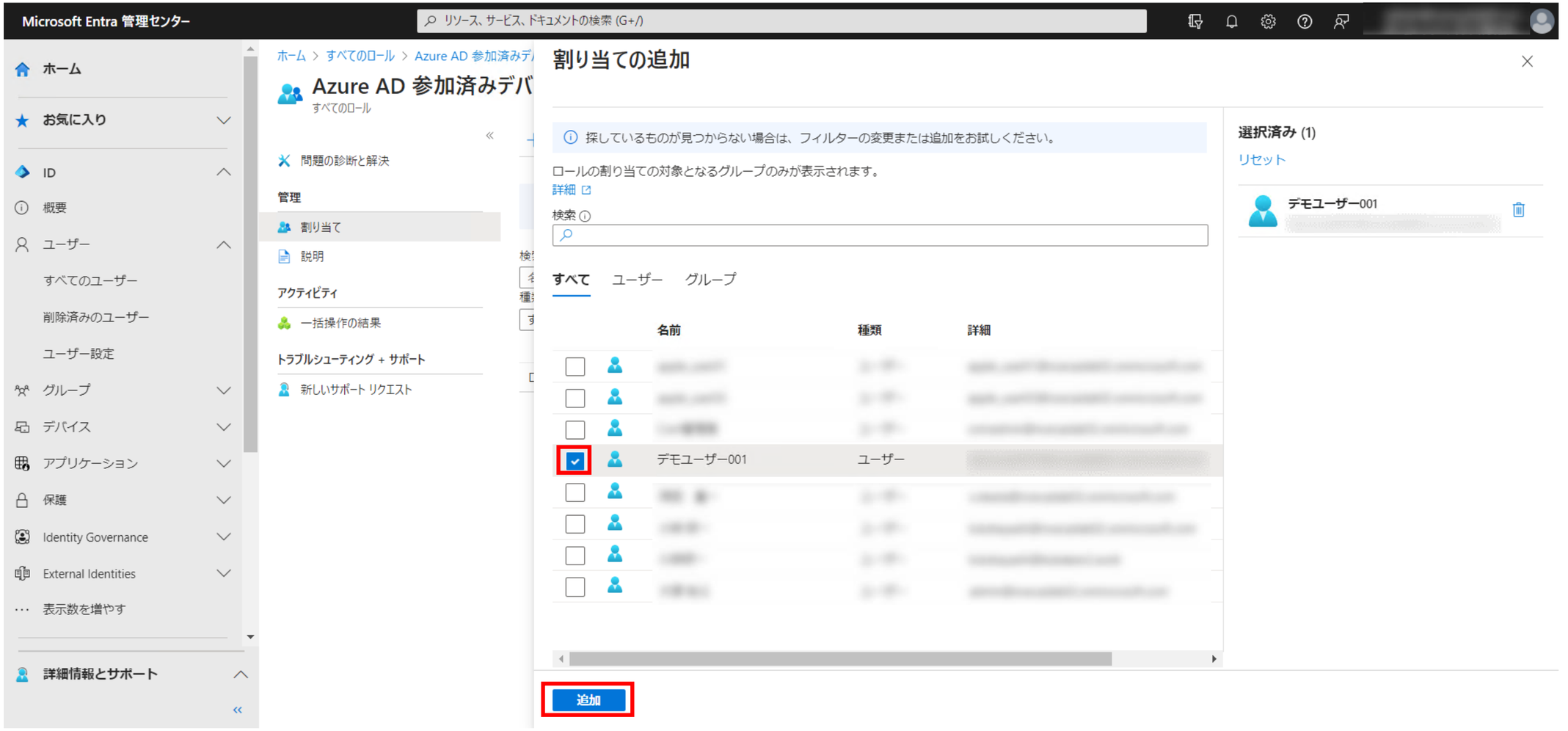


Ⅳ-1　ローカル管理者ロールの割り当て

4.[割り当ての追加]をクリックします

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

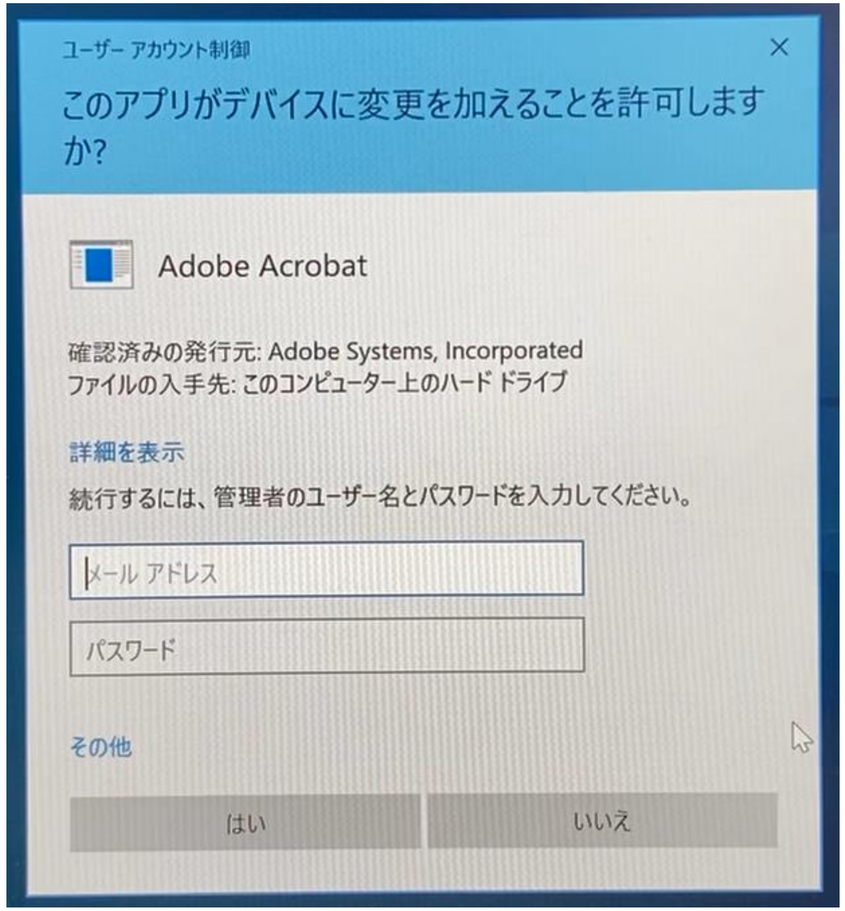


Ⅳ-1　ローカル管理者ロールの割り当て

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

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

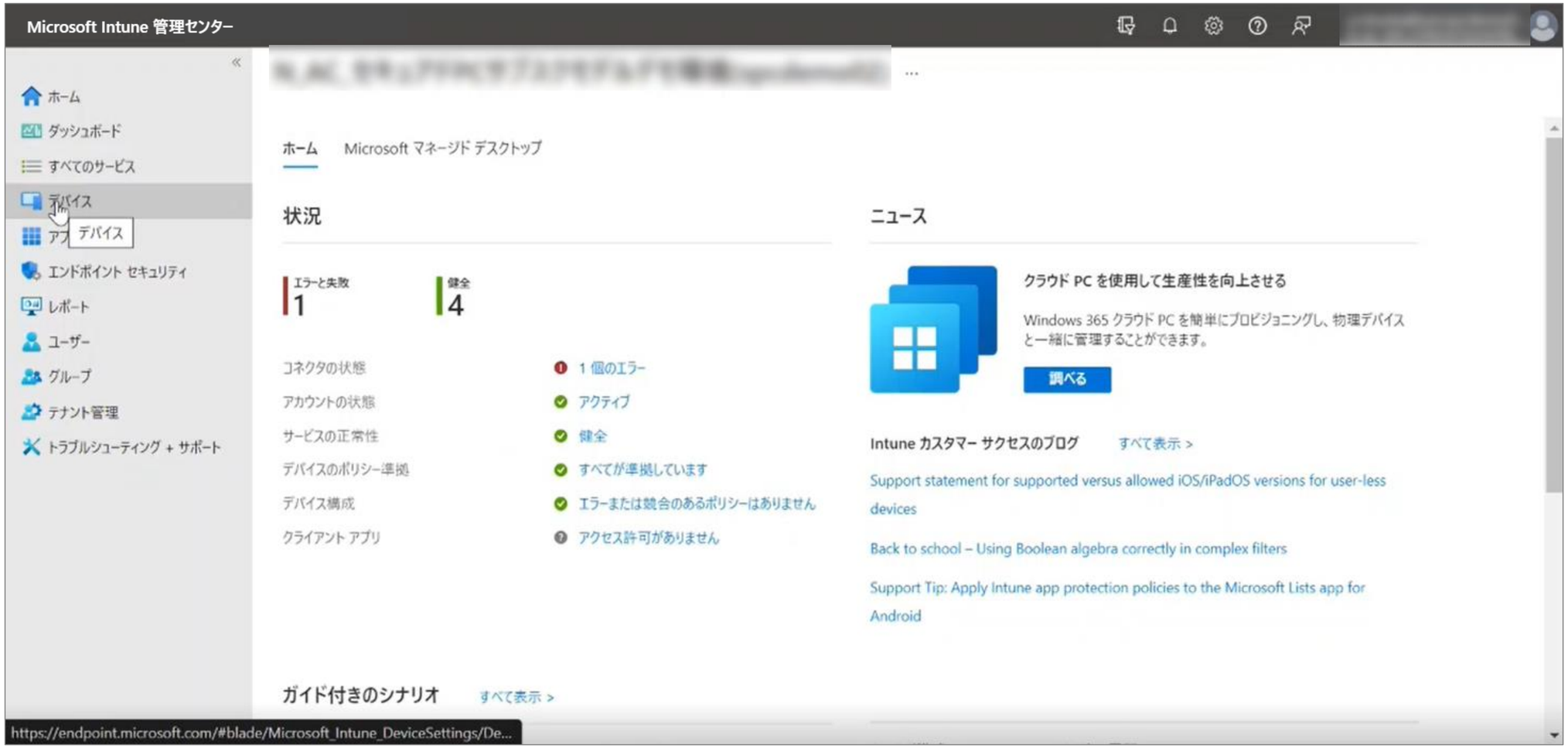
1.対象のユーザーの[□]を選択し、[割り当ての削除]をクリックすることで管理者ロールを剥奪することができます

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

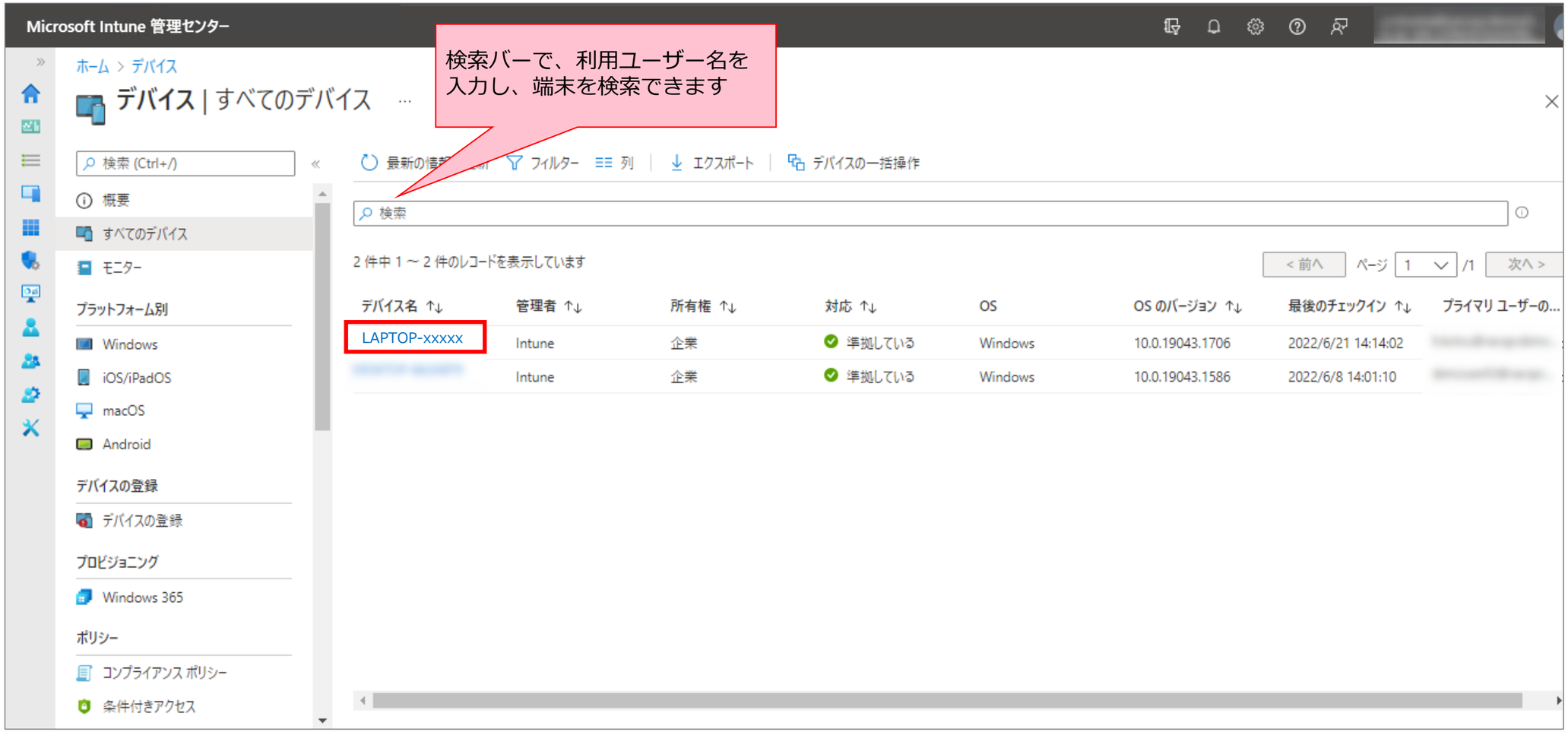


V-1　端末の位置情報検索

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

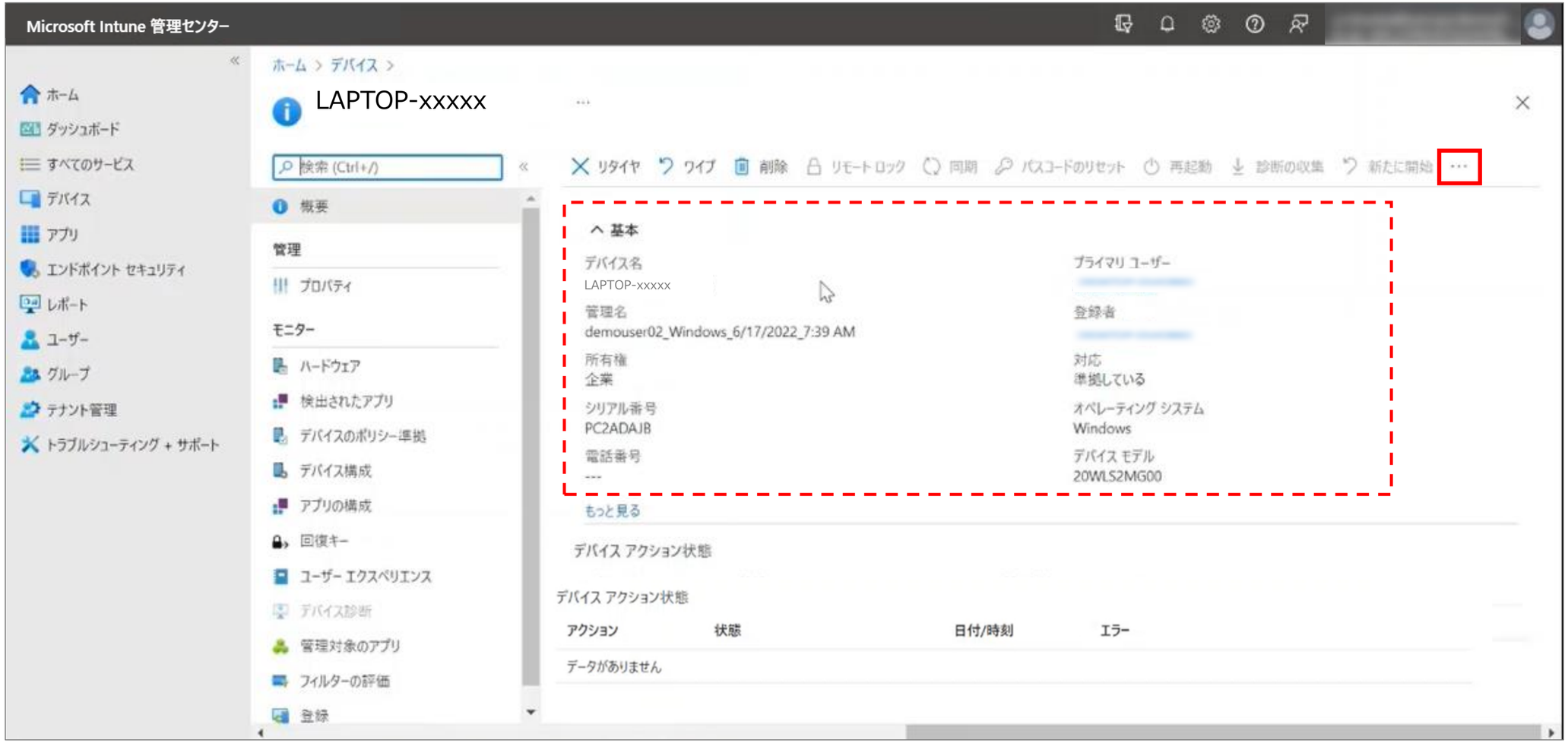
V-1　端末の位置情報検索

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



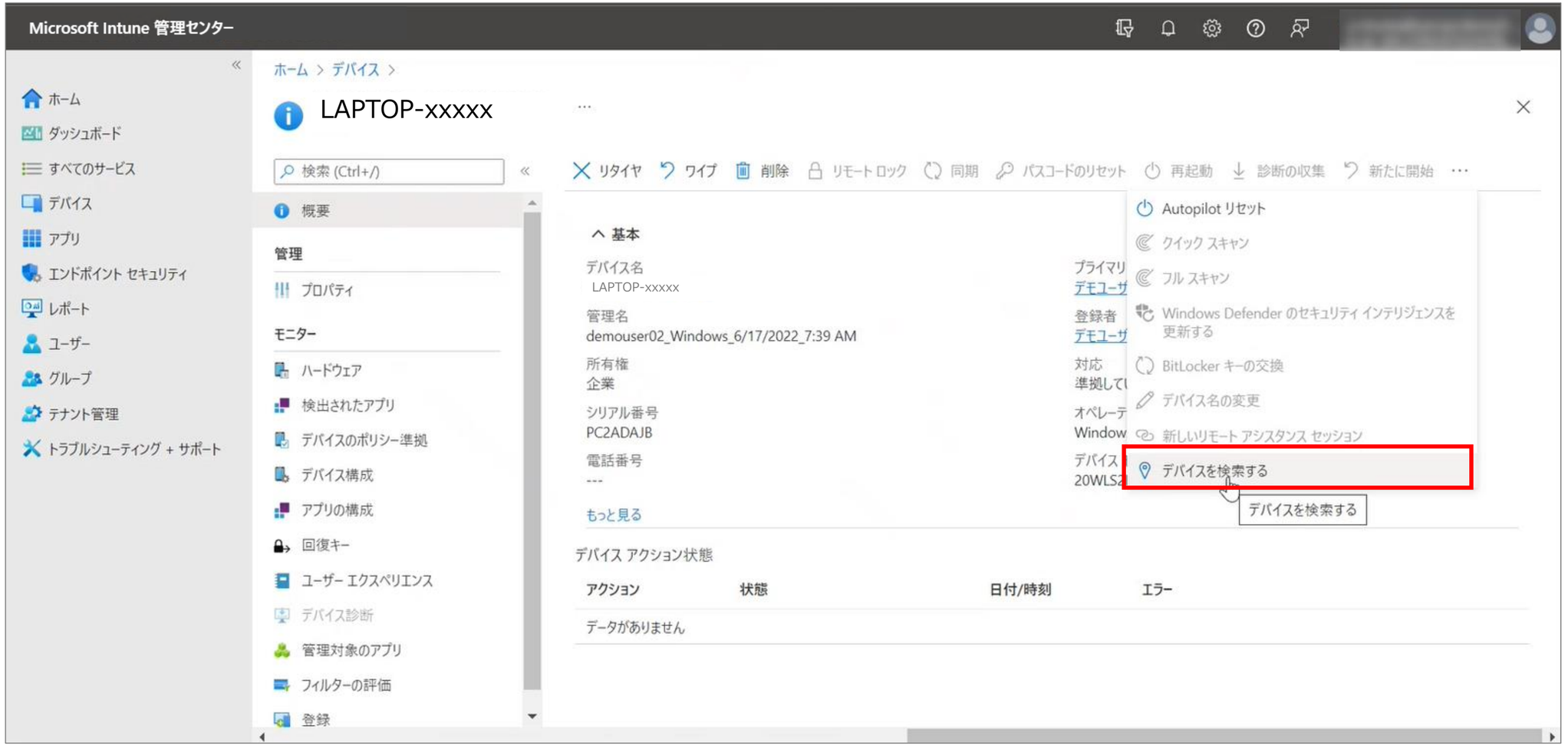
V-1　端末の位置情報検索

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



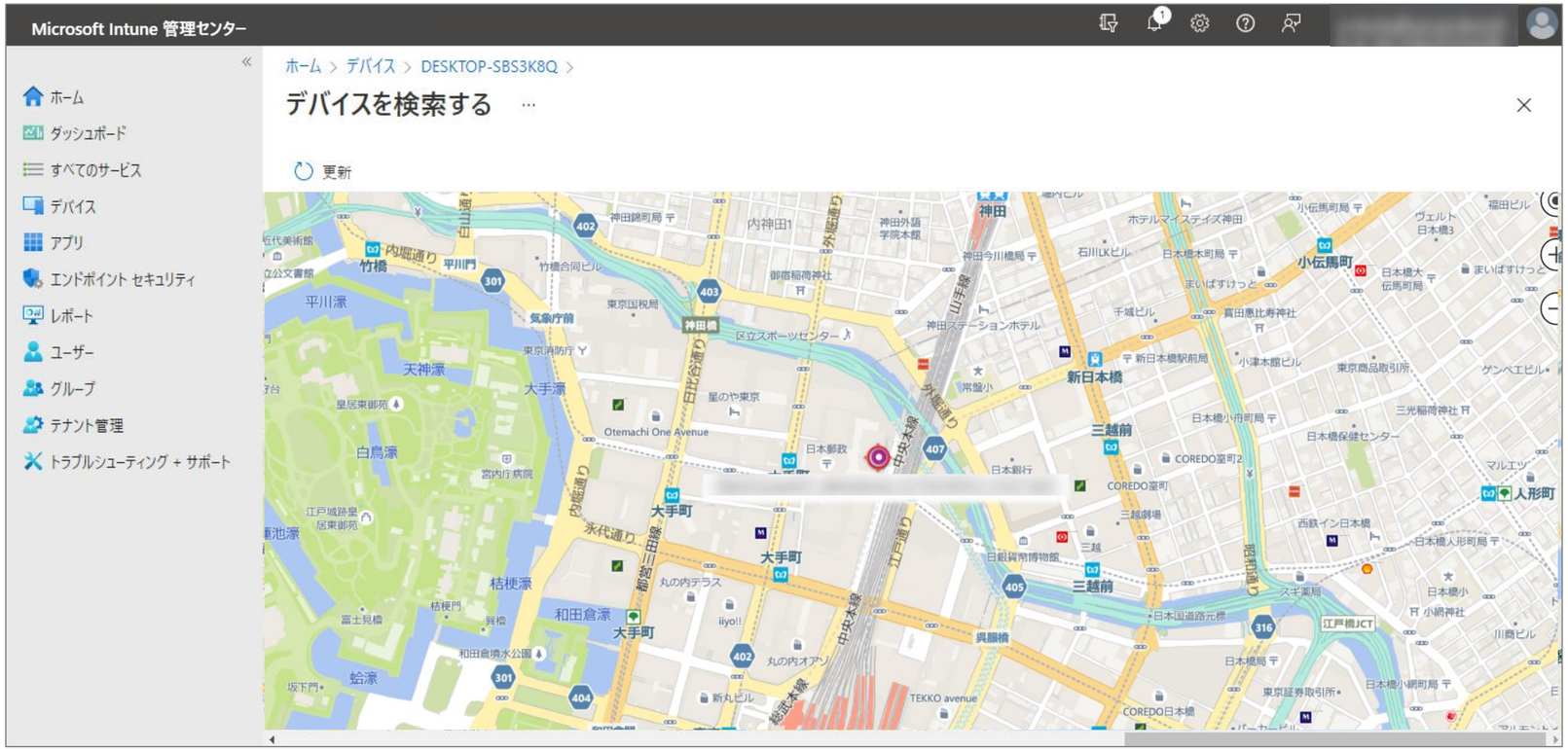
V-1　端末の位置情報検索

5.[デバイスを検索する]をクリックします



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



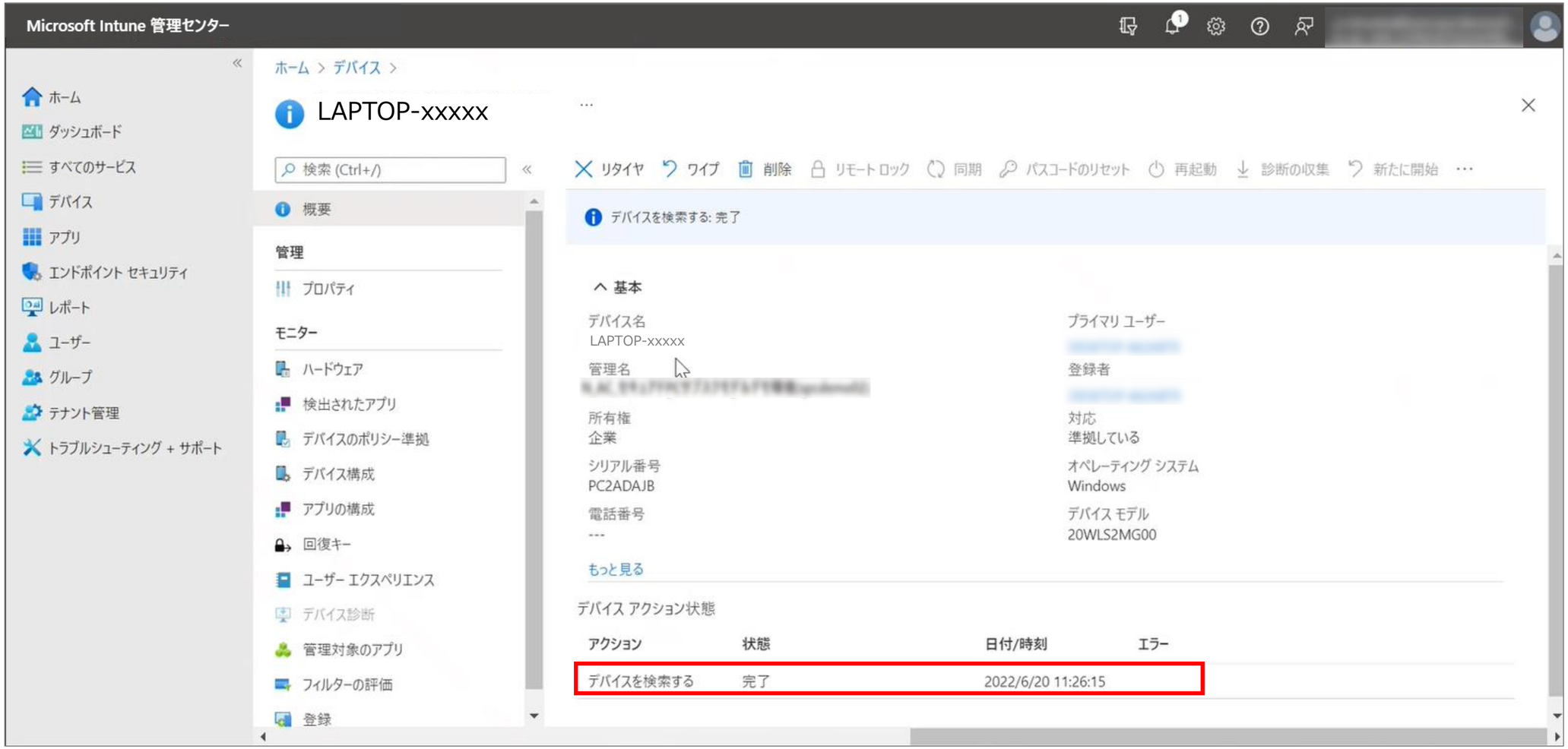
《位置検索が可能な条件》

・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



V-2　遠隔での端末の初期化

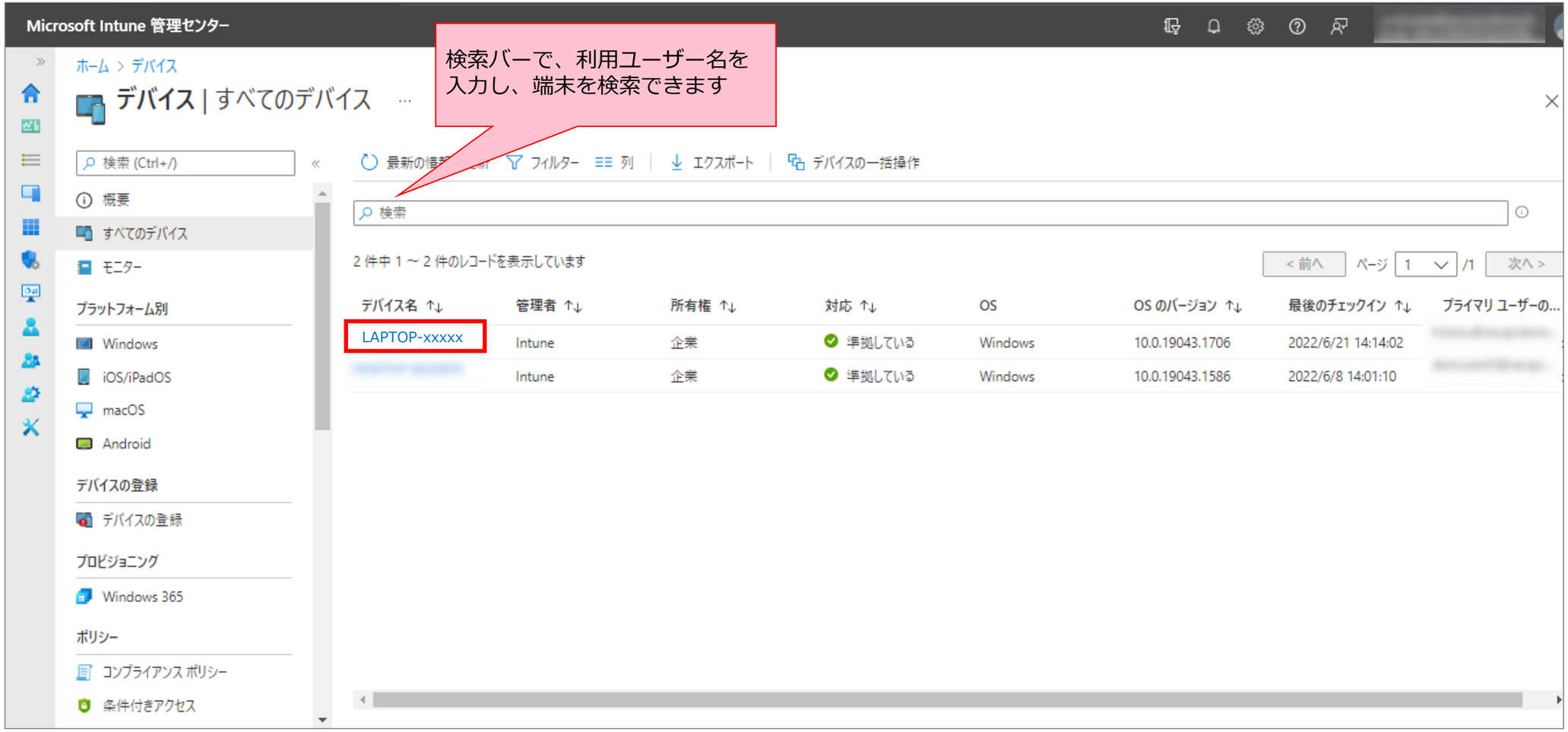
1.Microsoft Intune 管理センター（https://intune.microsoft.com/）にアクセスします

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

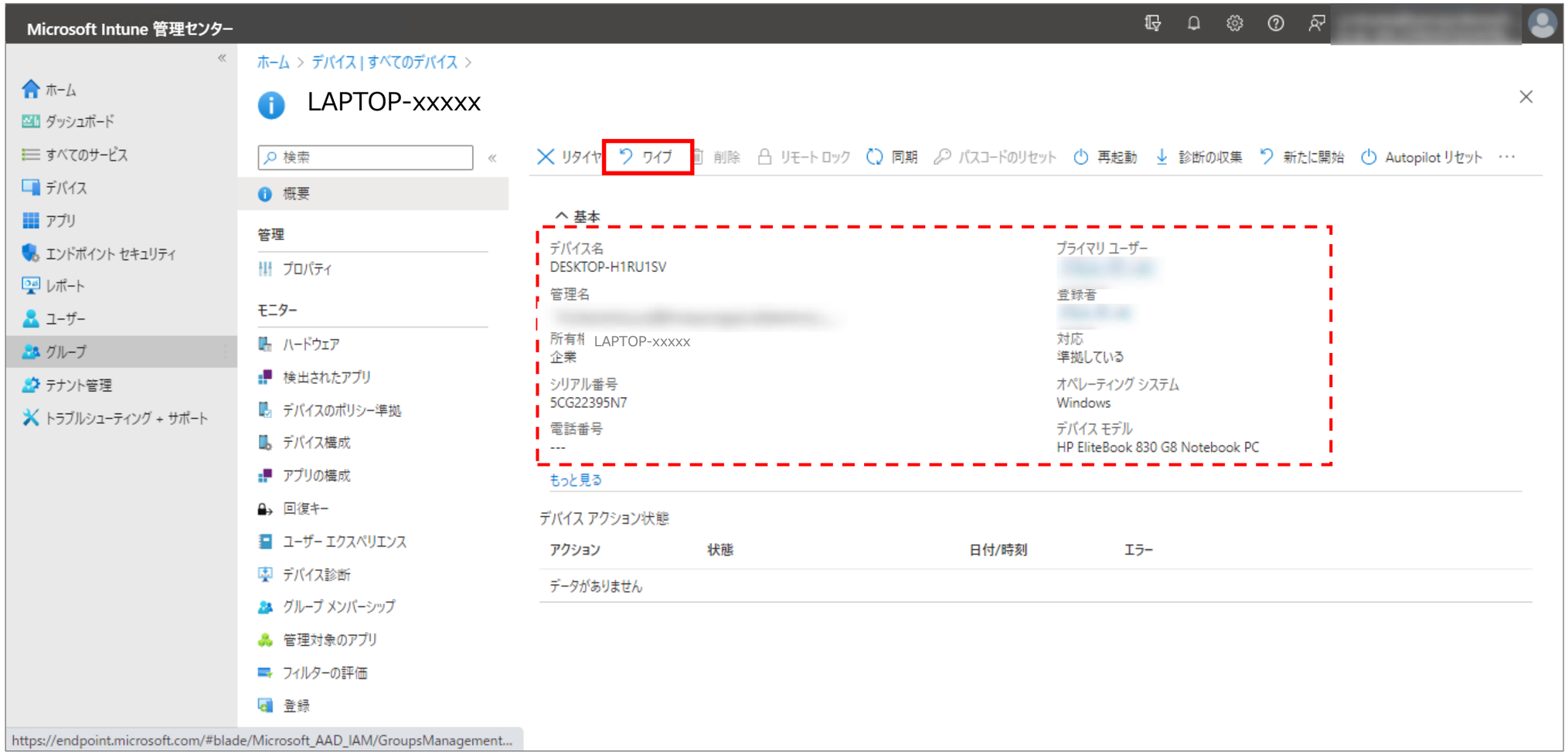
V-2　遠隔での端末の初期化

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



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

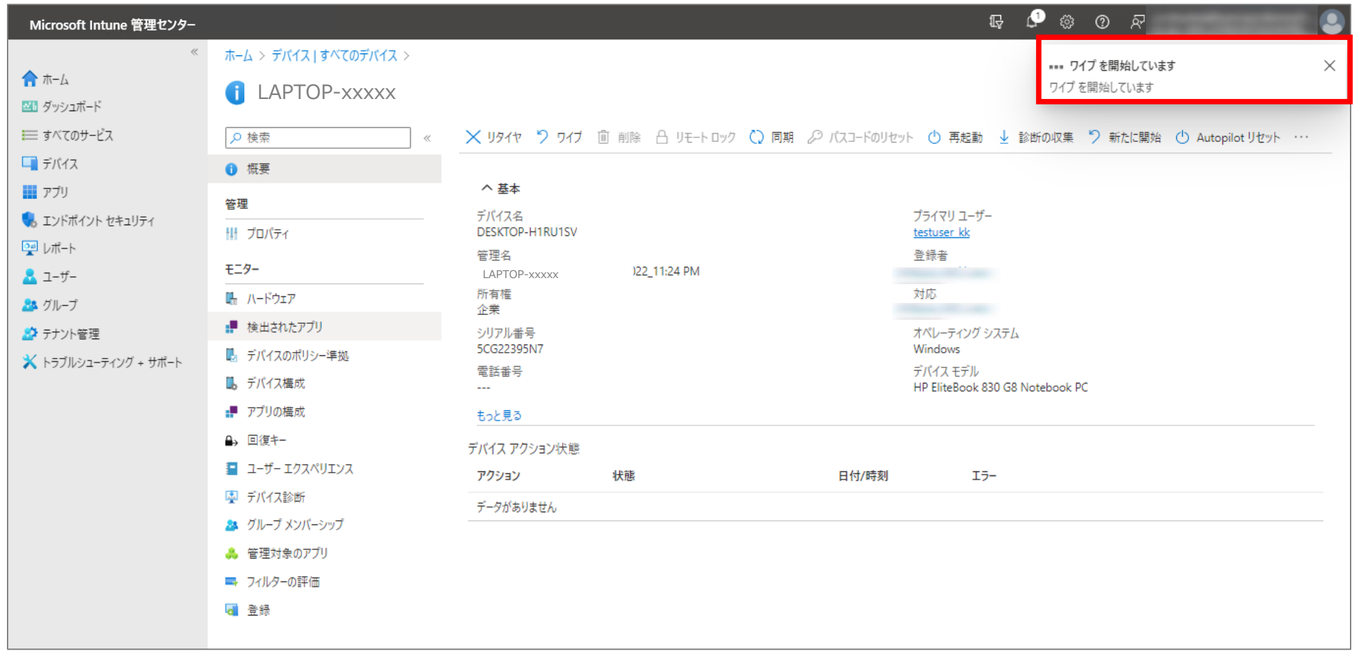


V-2　遠隔での端末の初期化

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

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になります
  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、万一に備え、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）

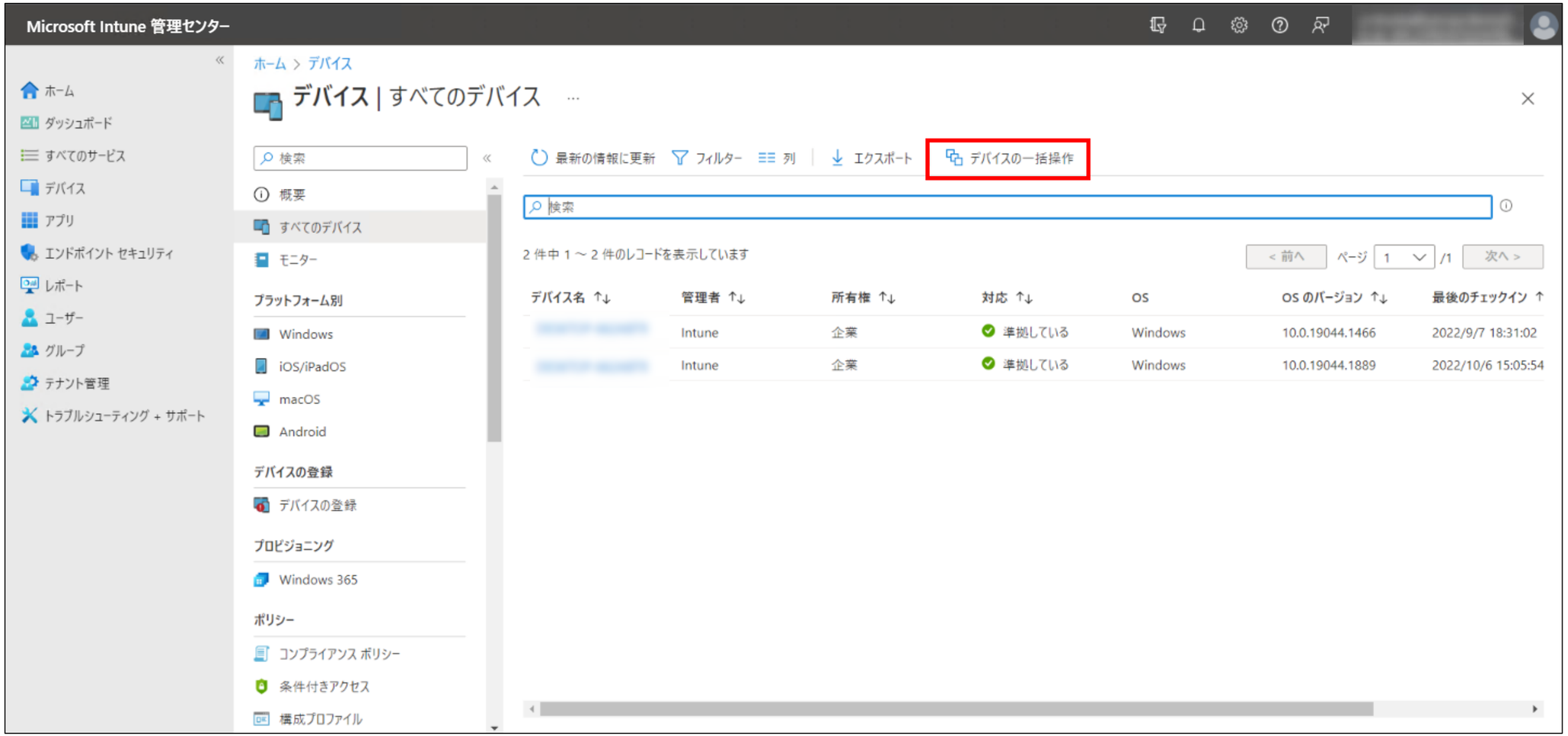
1.Microsoft Intune 管理センター（https://intune.microsoft.com/）にアクセスします

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

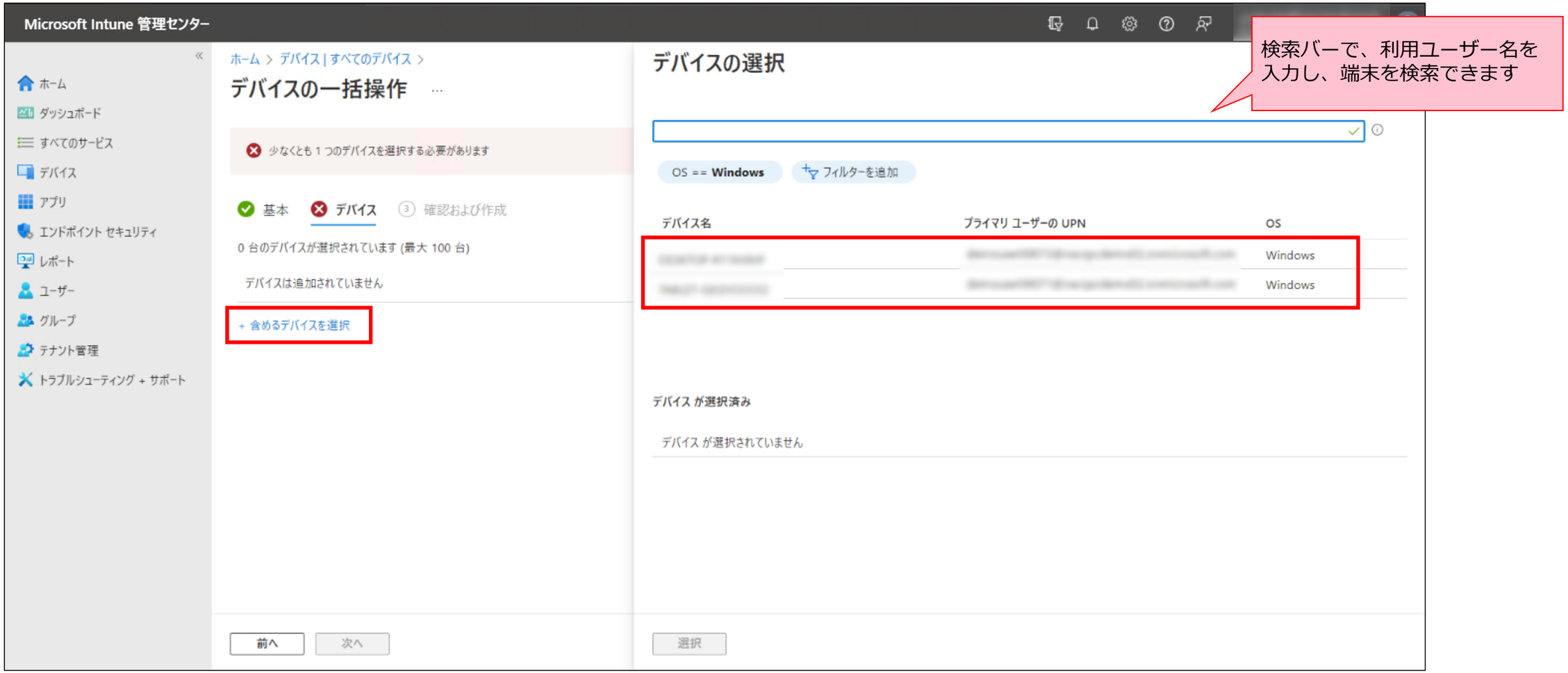


Ⅵ-1　端末のリセット（管理者操作）

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）

5.[含めるデバイスを選択]をクリックし、デバイス一覧から解約する端末をクリックし選択します
※一度に選択できる上限は100台までです。100台以上解約する場合は、繰り返し作業してください。

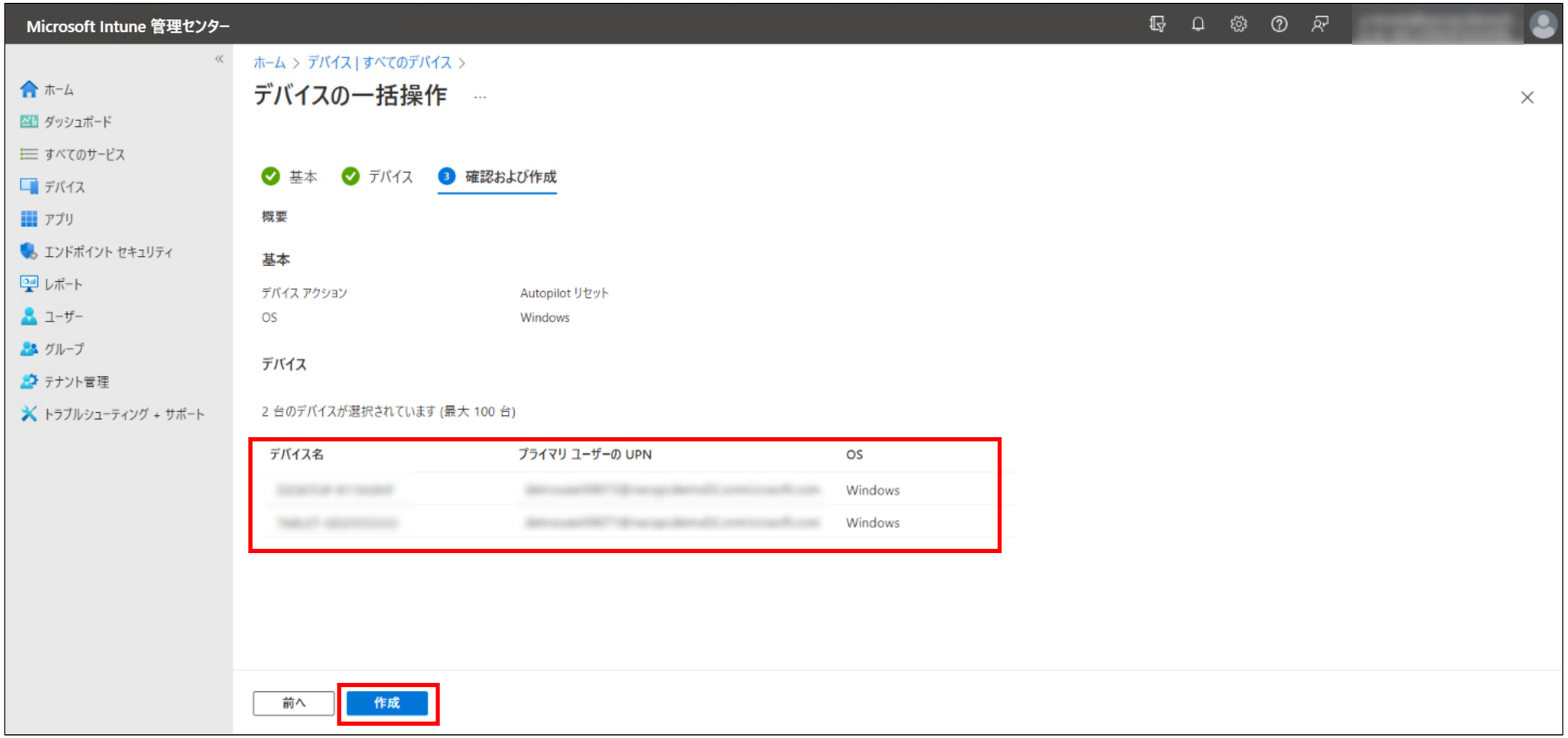


Ⅵ-1　端末のリセット（管理者操作）

6.[選択]をクリックし、[次へ]をクリックします

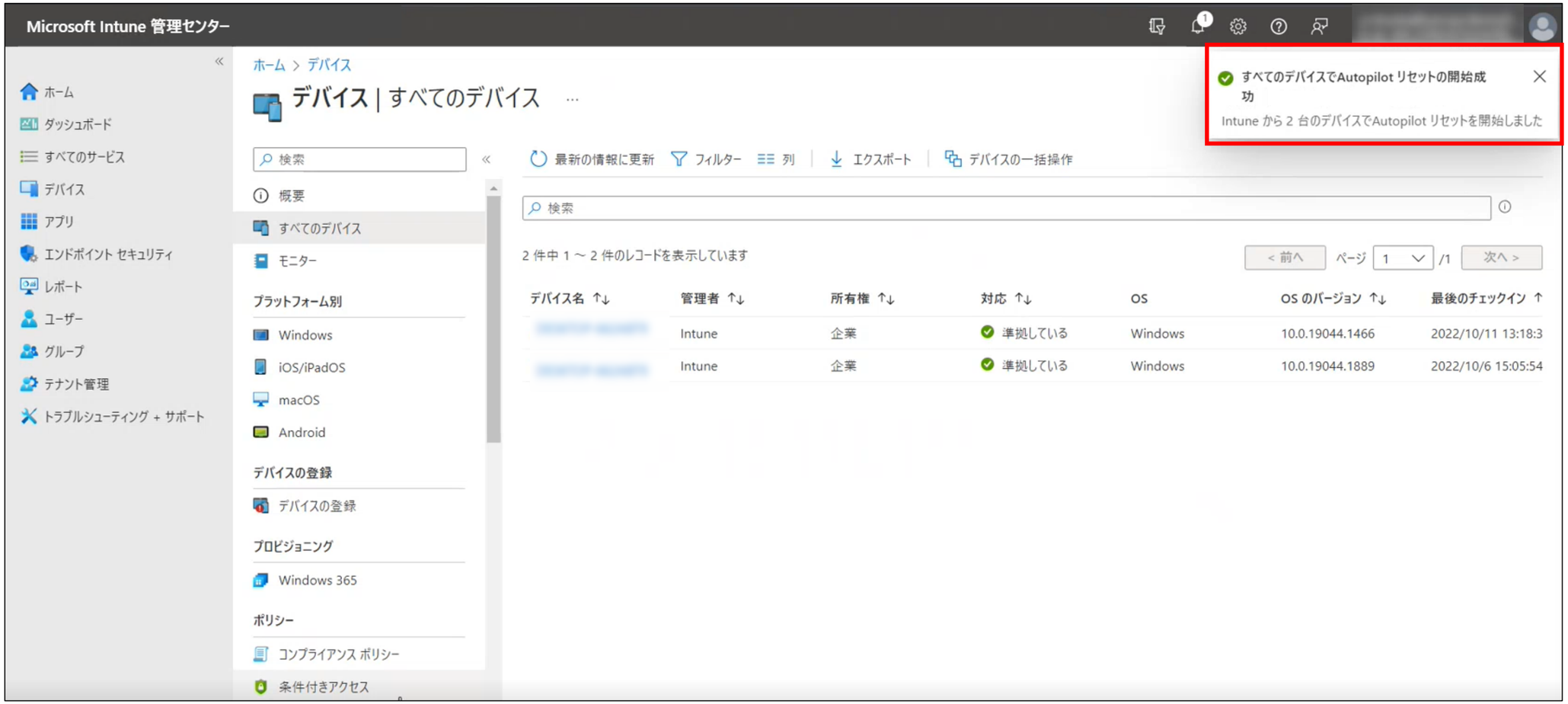
Ⅵ-1　端末のリセット（管理者操作）

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



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



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	

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

優先度〇　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。	〇	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。	〇	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。	〇	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。	〇	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。	〇	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。	〇	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。	〇	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。	〇	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。	〇	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

優先度〇　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。	〇	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。	〇	盗難 紛失	・HDD/SSD暗号化(Bitlokker）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。	〇	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	〇	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ないよう設定する。	〇	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るよう設定する。	〇	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。	〇	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。	〇	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。	〇	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

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が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 https://portal.azure.com/	MDMの設定 [Azure Active Directory] → [モビリティ(MDM および MAM)] → Microsoft Intune
	MFAの強制設定 [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 https://compliance.microsoft.com/	Azure Information Protectionの設定 [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)
	Windows Autopilot Deployment （OOBE）設定 [デバイス] → [デバイスの登録] → [Windows登録] → [デプロイ プロファイル] → OOBE_Profile
Microsoft Endpoint Manager admin center https://endpoint.microsoft.com/	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 [デバイス] → [構成プロファイル] → OneDrive_backup
	Defender（リアルタイム検知、ウィルス定義ファイル等）の有効化 [デバイス] → [構成プロファイル] → Windows Defender ウイルス対策
	Defender Web保護の有効化 [エンドポイントセキュリティ] → [攻撃面の減少] → Windows Defender Web保護
	Windows更新プログラムのポリシー設定 [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
	Bitlockerの有効化 [デバイス] → [構成プロファイル] → Bitlocker
	スクリーンロックの設定 [デバイス] → [構成プロファイル] → スクリーンロック