Azure ADの機能とライセンス

機能	概要	ライセンス
ハイブリッドID	オンプレミスのAD DSから、Azure ADへと、IDを同期する（Azure AD Connectを使用）	無料
Azure AD DS (AAD DS)	Azure上で、AD DSの機能（ドメインコントローラ）を提供する。AD DSの機能を必要とするオンプレミスのアプリケーションを、Azureにリフト&シフト（移行）するために使用される。	不要（リソースに対する月単位の課金は発生）
セキュリティの既定値群	すべてのユーザーに対しAzure AD MFAへの登録を必須にする。管理者にMFAの実行を要求する。必要に応じてユーザーにMFAの実行を要求する。新しいテナントではデフォルトで有効。「**条件付きアクセス**」を使用する場合は無効に設定しなければならない。	無料
条件付きアクセス	ユーザー、IPアドレス、地域、デバイス、アプリケーションなどに応じて、アクセスをブロックしたり、MFAの実行を要求したりする。 「**Identity Protection**」の**ユーザーリスク**/**サインインリスク**も「条件」の一部として利用できる。	Azure AD Premium P1
Identity Protection	**ユーザーリスク**（ダークウェブ等に流出した「侵害された」IDを使ったサインイン試行の可能性）、**サインインリスク**（匿名IPからのサインイン試行など、本人以外から、サインイン要求が送信されている可能性）を検出し、MFAの実行の要求、パスワードのリセットの要求などを実行する。管理者は、検出されたリスクのレポートを調査できる。	Azure AD Premium P2
Privileged Identity Management (PIM)	ロールの利用（アクティブ化）に対し、期限を設けたり、承認を必要としたりすることができる。	Azure AD Premium P2

Azure ADのパスワードの変更/リセット関係の機能とライセンス

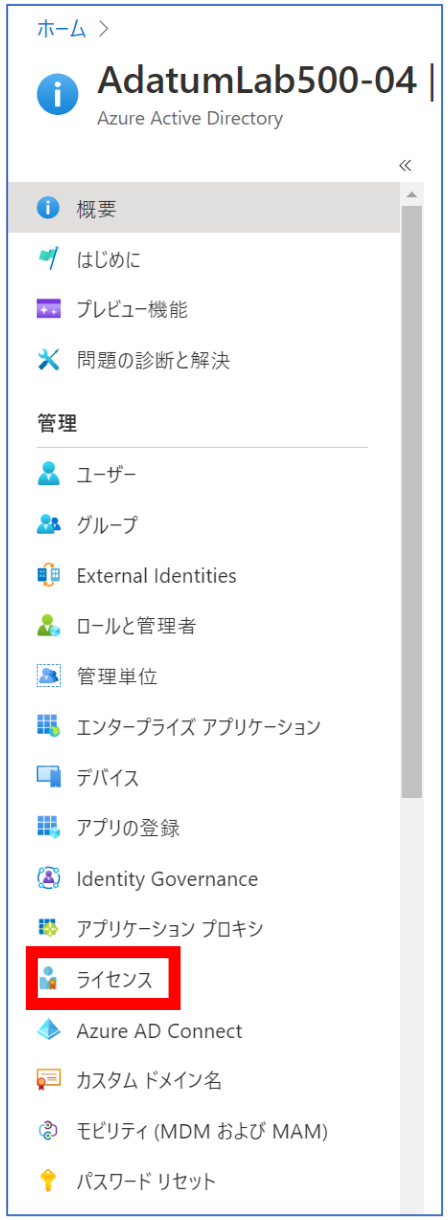
機能	概要	ライセンス
クラウドのみのユーザーパスワードの**変更**	Azure AD のユーザーが自分のパスワードを知っていて、新しいパスワードへの変更を希望する場合。	無料
クラウドのみのユーザーパスワードの**リセット**	Azure AD のユーザーがパスワードを忘れて、リセットする必要がある場合。	Microsoft 365 Business Standard Microsoft 365 Business Premium Azure AD Premium P1 または P2
オンプレミスの書き戻しを含む、ハイブリッドユーザーのパスワードの**変更**または**リセット**	Azure AD Connect を使用してオンプレミスのディレクトリから同期されている Azure AD のユーザーが、パスワードを変更またはリセットし、オンプレミスに新しいパスワードを書き戻す場合。	Microsoft 365 Business Premium Azure AD Premium P1 または P2

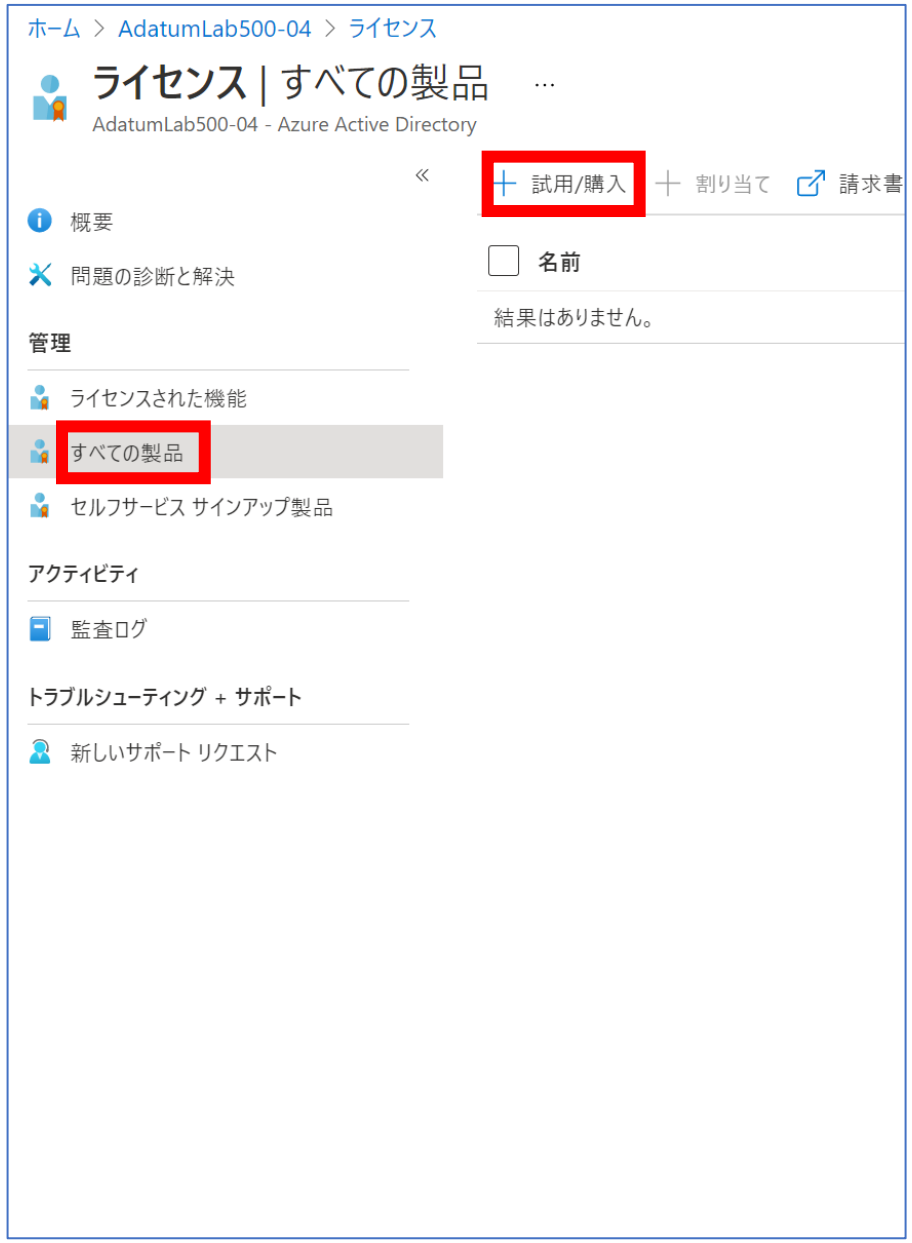
※ユーザーが自分自身のパスワードをリセットできる機能を**Self Service Password Reset (SSPR)**という
※管理者はすべてのユーザーのリセットを実施可能（ライセンス不要）

Premium P2試用版のアクティブ化

テナントで「試用版」をアクティブ化すると、30日間無料で、100ユーザー分のP2ライセンスを試用できます。

Azure AD Premium P2試用版のアクティブ化



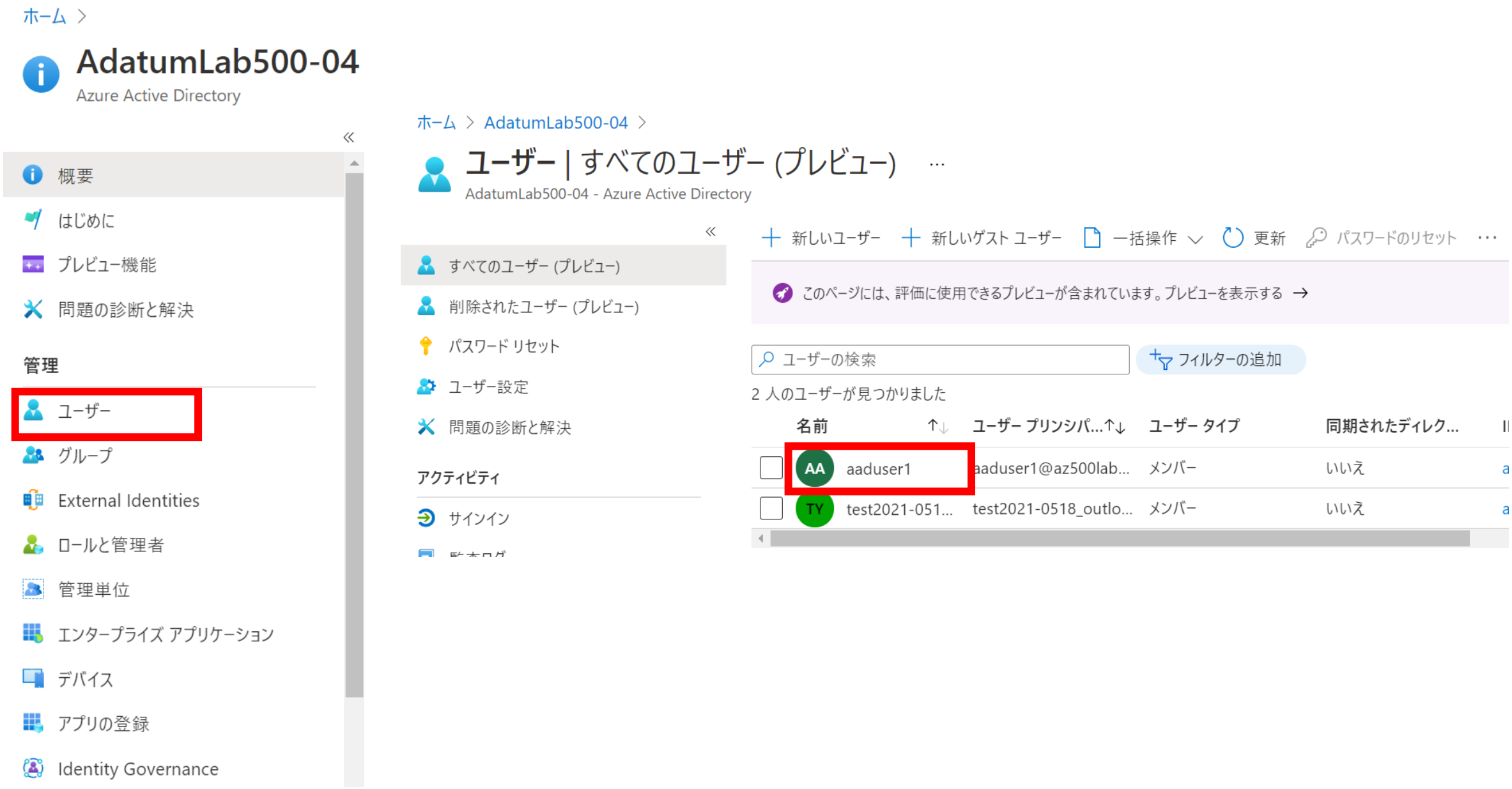


ブラウザをリロードして「すべての製品」を再表示します。
下記のように「Azure Active Directory Premium P2」の行が表示されていればOKです。

ユーザーへの Premium P2ライセンスの 割り当て

P2のライセンスをユーザーへ割り当てすることで、そのユーザーがP2の機能を利用できるようになります。

ユーザーへのPremium P2ライセンスの割り当て



aaduser1 | ライセンス

ユーザー

«

問題の診断と解決

管理

プロファイル

割り当てられたロール

管理単位

グループ

アプリケーション

ライセンス

デバイス

Azure ロールの割り当て

認証方法

アクティビティ

サインイン

監査ログ

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

ライセンスの割り当てが見つかりませんでした。

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
することができません。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

- [x] Azure Active Directory Premium P2

ライセンス オプションの確認

選択

Azure Active Directory Premium P2

- [x] Cloud App Security Discovery
- [x] Microsoft Azure Multi-Factor Authentication
- [x] Azure Active Directory Premium P1
- [x] Azure Active Directory Premium P2

保存

ユーザーへのPremium P2ライセンスの割り当てができました

aaduser1 | ライセンス

ユーザー

«
問題の診断と解決

管理

プロファイル
割り当てられたロール
管理単位
グループ
アプリケーション
ライセンス
デバイス
Azure ロールの割り当て

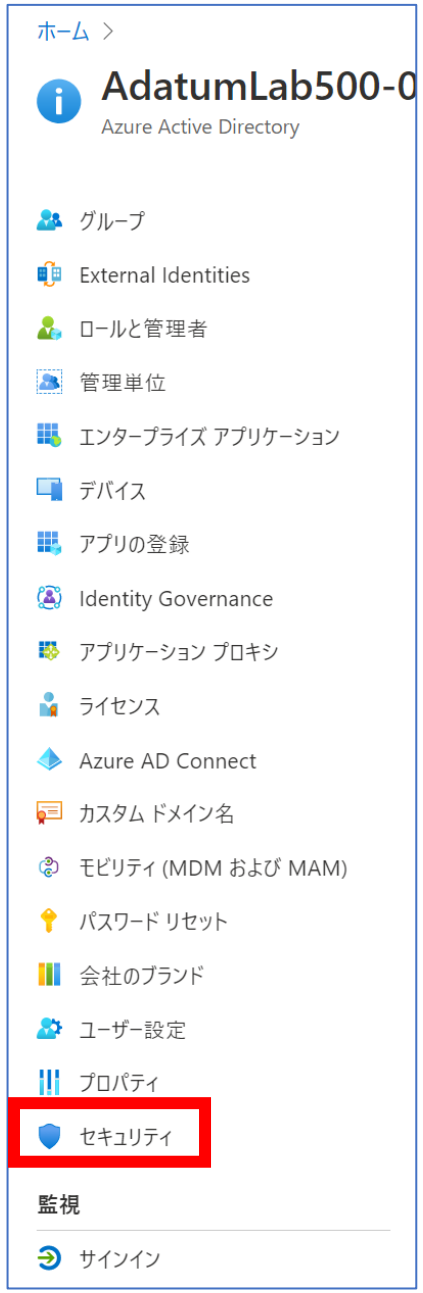
製品	状態	有効なサービス	割り当てパス
Azure Active Directory Prem...	アクティブ	4/4	直接

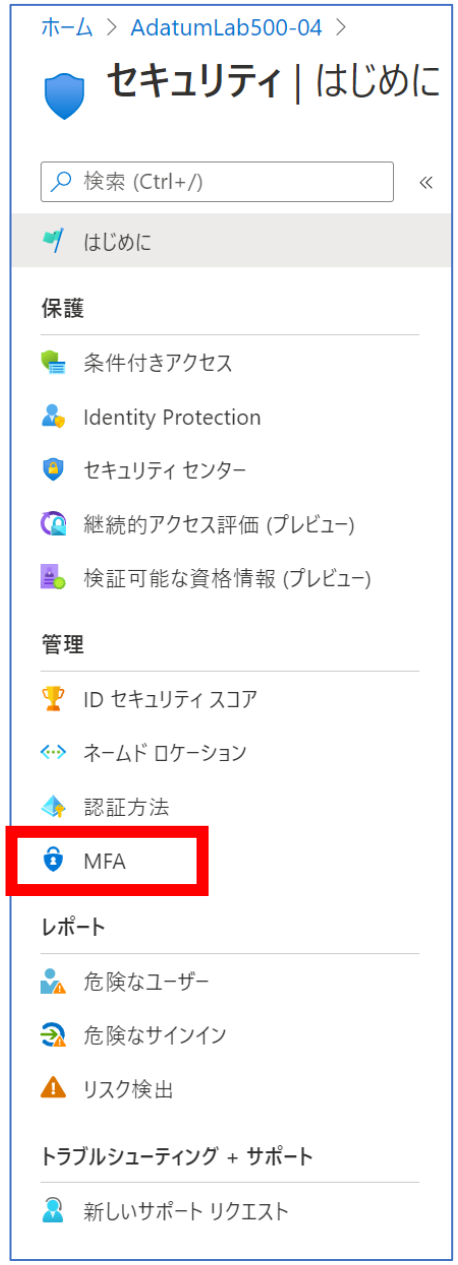
※Azure AD＞ライセンス＞すべての製品＞Azure AD Premium P2 で、
「＋割り当て」をクリックし、複数のユーザーを選択して、割り当てすることもできます。
多数のユーザーに割り当てを行う場合はこちらが便利です。

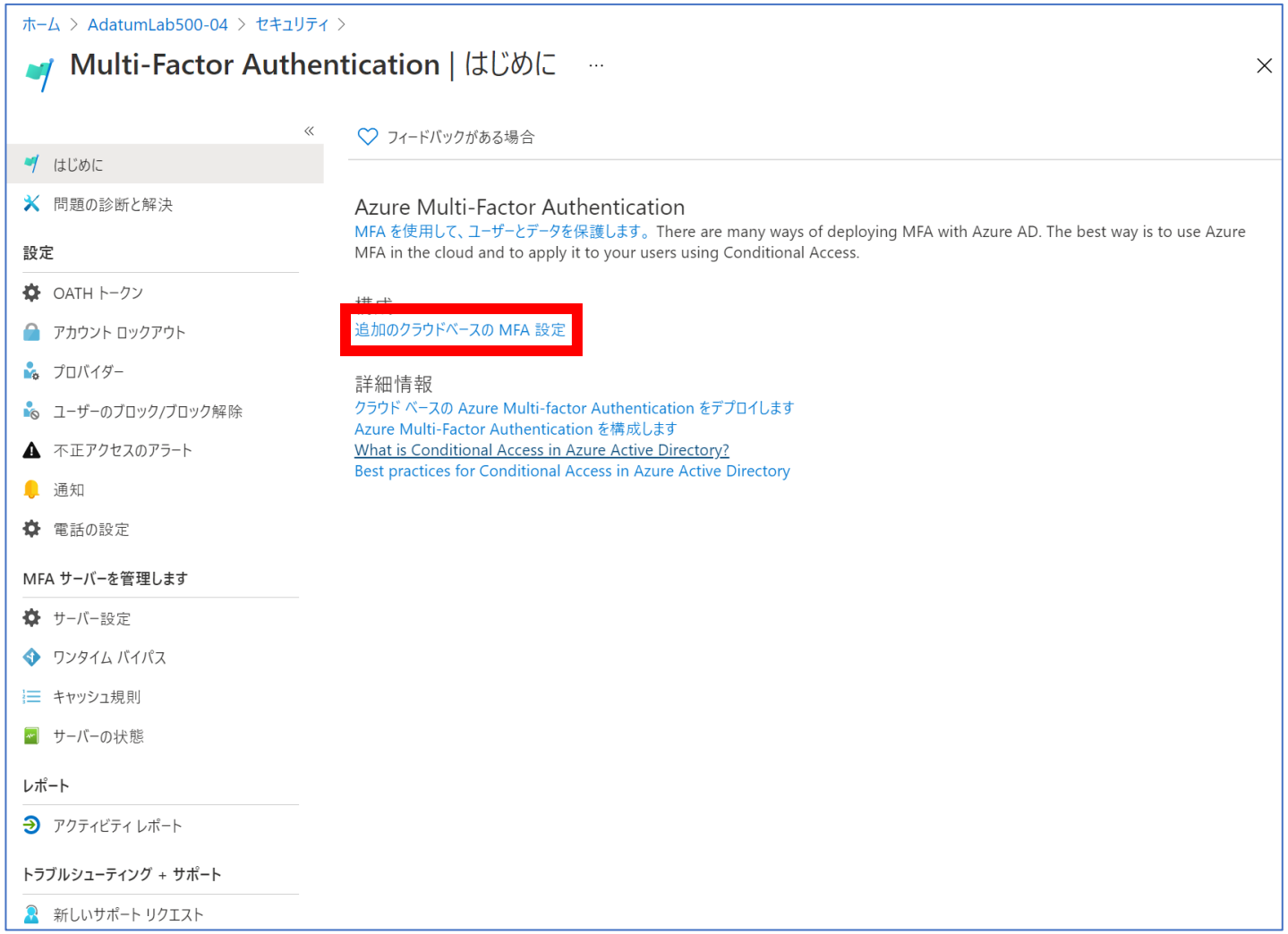
ユーザーのMFAの有効化

MFA（多要素認証）を使用することで、ユーザーはサインイン時、ID・パスワードの入力（第1の認証）に加え、Microsoft Authenticator等による認証（追加の認証）が求められます。

MFAの設定







※「ユーザー一覧」の上部の「MFA」リンクからも
同じ画面に移動できます。

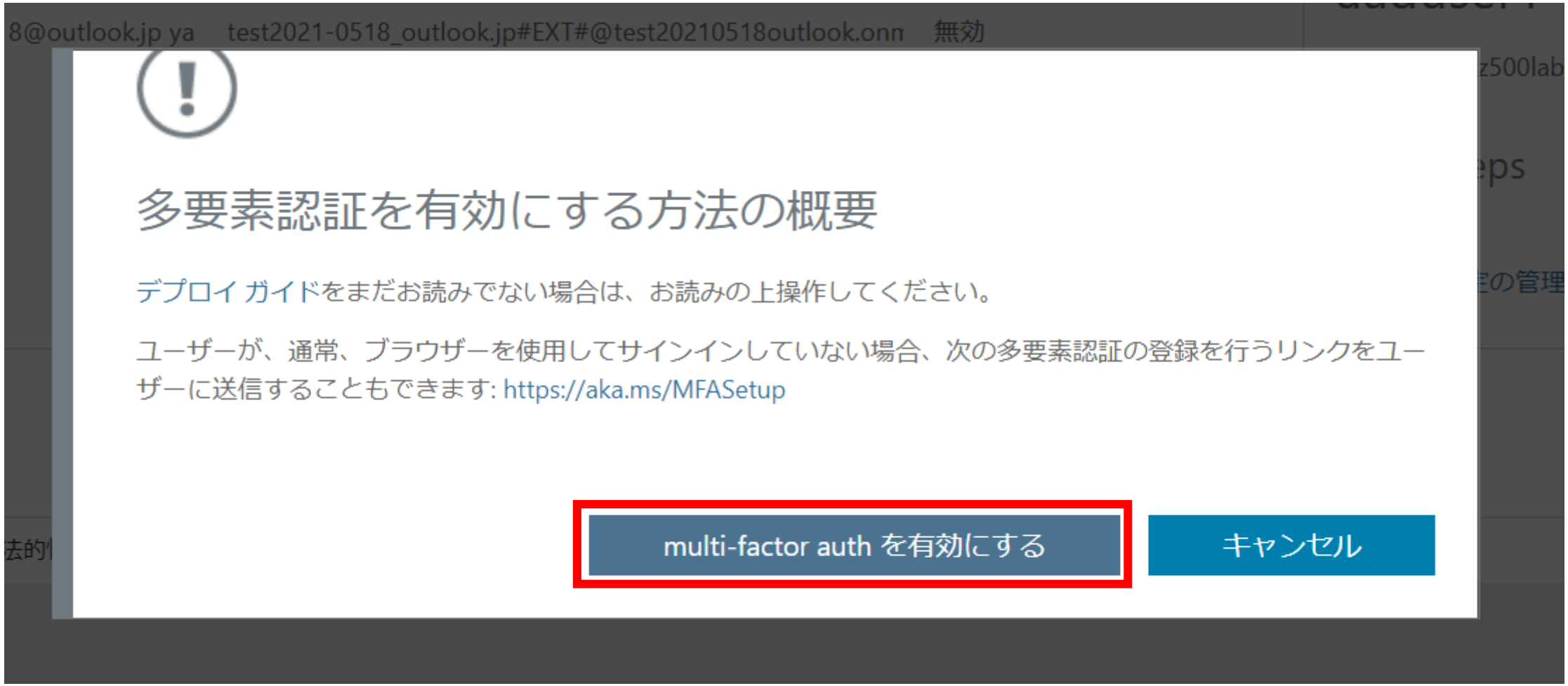
多要素認証＞サービス設定

多要素認証＞ユーザー


Microsoft
test2021-0518_outlook.jp#EXT#_test20210518outlook.onmiHMNAQ#EXT#@az500lab20210518.onmicrosoft.com
?
多要素認証
ユーザー
サービス設定
始める前に、多要素認証のデプロイ ガイドを参照してください。
表示: サインインが許可されているユー
Multi-Factor Authentication の状態: 任意
一括更新
表示名
ユーザー名
MULTI-FACTOR AUTHENTICATION の状態
aaduser1
aaduser1@az500lab20210518.onmicrosoft.com
無効
test2021-0518@outlook.jp ya
test2021-0518_outlook.jp#EXT#@test20210518outlook.onn
無効
ユーザーを選択
©2021 Microsoft
法的情報
プライバシー

ユーザーのMFAの有効化

ユーザーのMFAの有効化

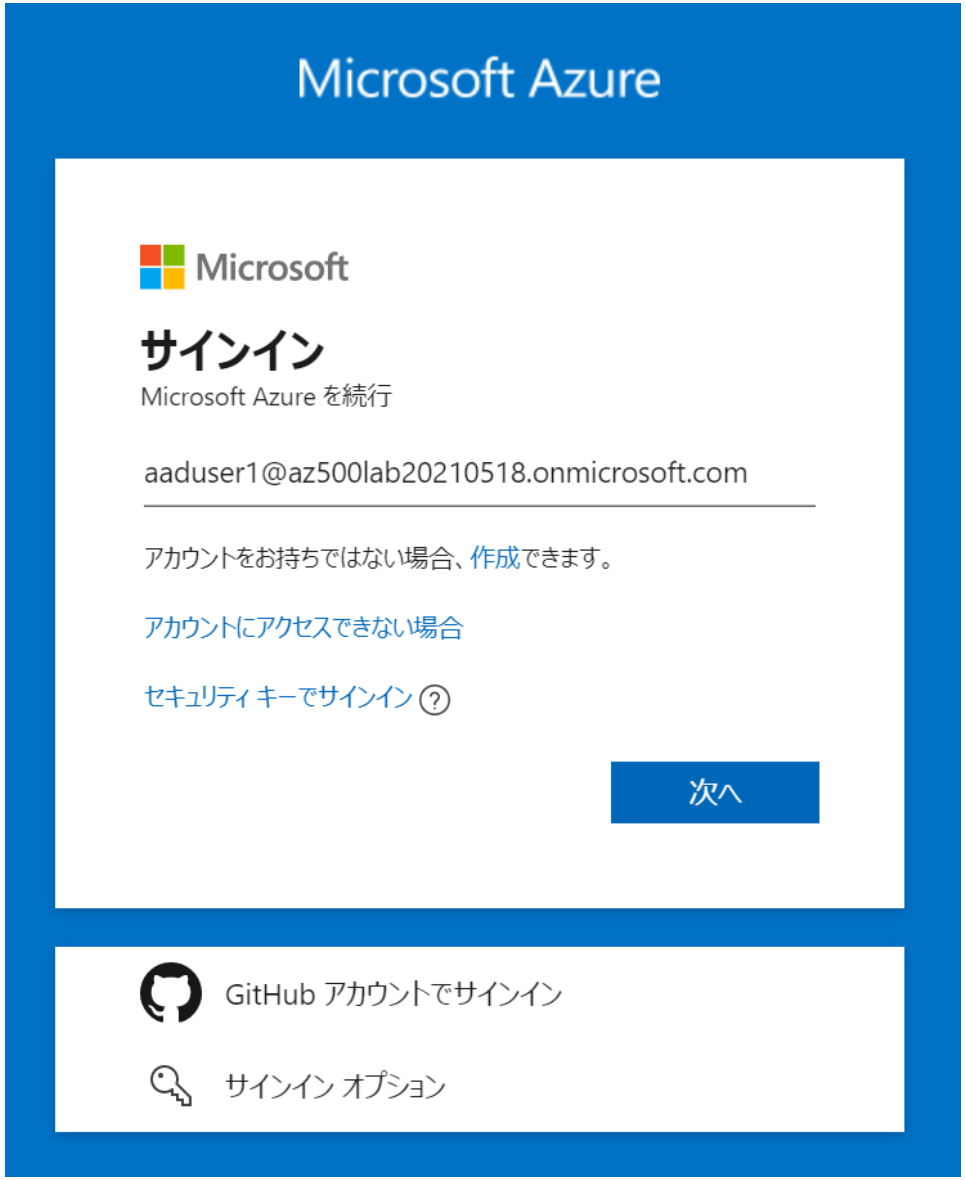


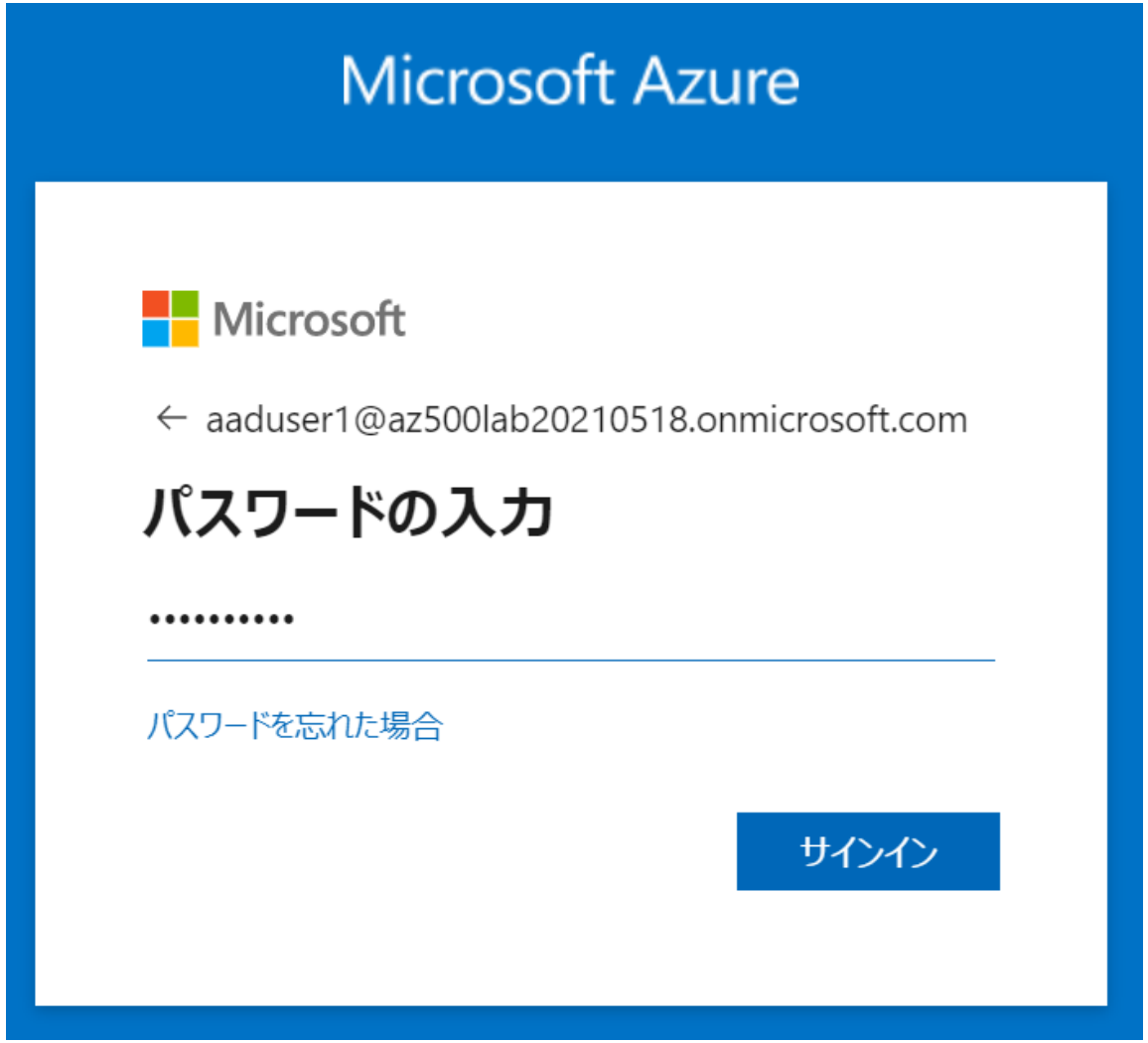
ユーザーのMFAが「有効」になりました

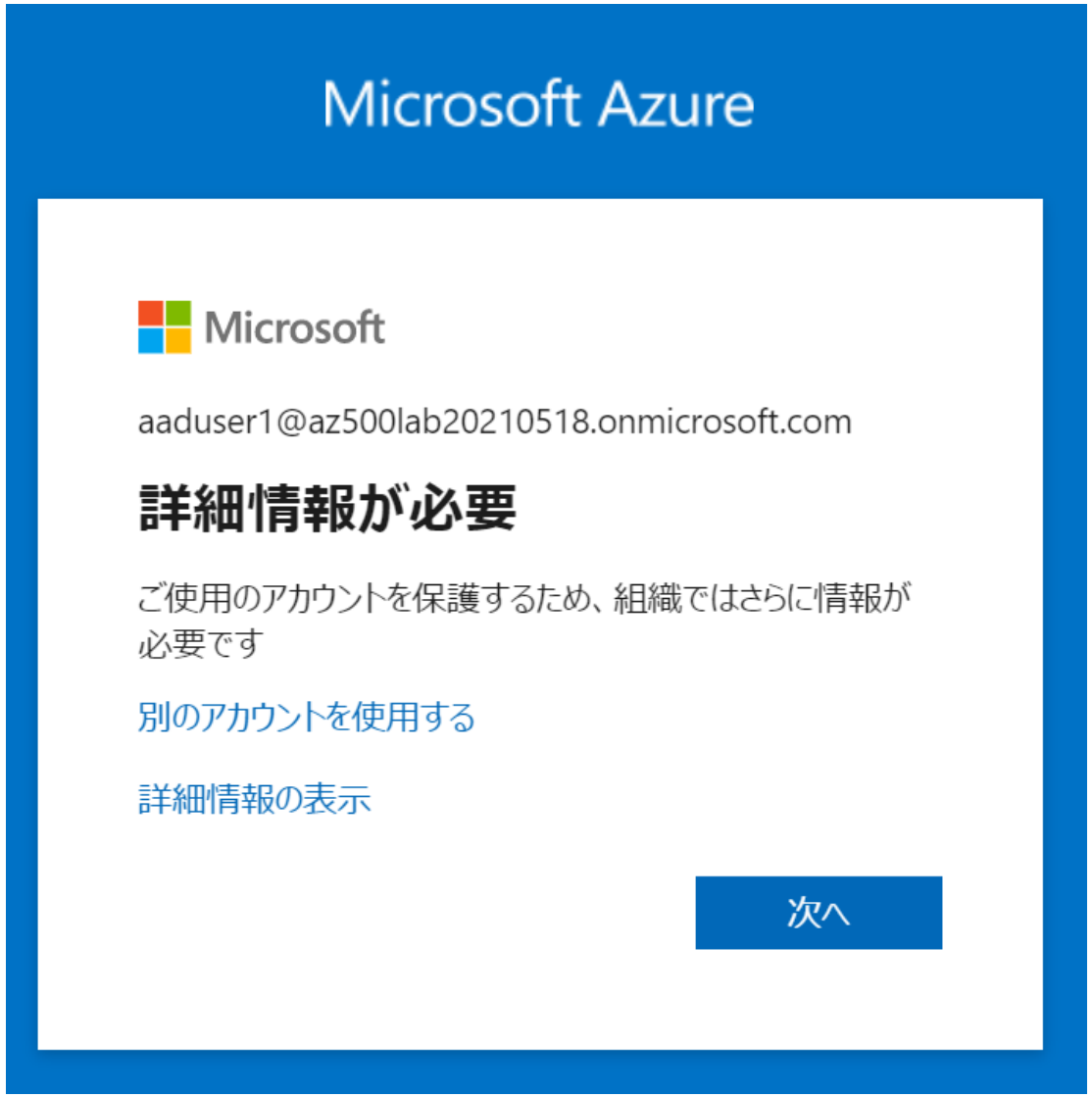
ユーザー側での
MFAの初期セットアップ

MFAを「有効」に設定したユーザーがサインインする際に、MFAのセットアップ（画面に表示されるQRコードをMicrosoft Authenticatorモバイルアプリでスキャンするなど）が求められます。

MFAを有効化したユーザーで、Azure portalにサインインする






Microsoft Azure
Microsoft
aaduser1@az500lab20210518.onmicrosoft.com
詳細情報が必要
ご使用のアカウントを保護するため、組織ではさらに情報が必要です
別のアカウントを使用する
詳細情報の表示
次へ

アカウントのセキュリティ保護

組織により、身元を証明するための次の方法を設定することが求められています。

Microsoft Authenticator

最初にアプリを取得します

お客様の電話に Microsoft Authenticator アプリをインストールします。 今すぐダウンロード

デバイスに Microsoft Authenticator アプリをインストールした後、[次へ] を選択します。

別の認証アプリを使用します

次へ

別の方法を設定します

アカウントのセキュリティ保護

組織により、身元を証明するための次の方法を設定することが求められています。

Microsoft Authenticator

アカウントのセットアップ

プロンプトが表示されたら、通知を許可します。アカウントを追加し、[職場または学校]を選択します。

戻る　次へ

別の方法を設定します

アカウントのセキュリティ保護

組織により、身元を証明するための次の方法を設定することが求められています。

Microsoft Authenticator

QR コードをスキャンします

Microsoft Authenticator アプリを使用して QR コードをスキャンします。これにより、Microsoft Authenticator アプリとご自分のアカウントがつながります。

QR コードをスキャンした後、[次へ] を選択します。

画像をスキャンできませんか?

戻る　次へ

アカウントのセキュリティ保護

組織により、身元を証明するための次の方法を設定することが求められています。

Microsoft Authenticator

試してみましょう

アプリに送信される通知を承認します。

戻る　次へ

別の方法を設定します

アカウントのセキュリティ保護

組織により、身元を証明するための次の方法を設定することが求められています。

Microsoft Authenticator

通知が承認されました

戻る　次へ

別の方法を設定します

Microsoft Authenticator アプリが正常に登録されました

Tue, 18 May 2021 09:02:00 GMT

アカウントのセキュリティ保護

組織により、身元を証明するための次の方法を設定することが求められています。

成功

セキュリティ情報が正常にセットアップされました。[完了] を選択し、サインインを続行します。

既定のサインイン方法:

Microsoft Authenticator

完了

Microsoft

test2021-0518_outlook.jp#EXT#_test20210518outlook.onmiHMNAQ#EXT#@az500lab20210518.onmicrosoft.com | ?

多要素認証

ユーザー　サービス設定

始める前に、多要素認証のデプロイ ガイドを参照してください。

表示: サインインが許可されているユー　Multi-Factor Authentication の状態: 任意　一括更新

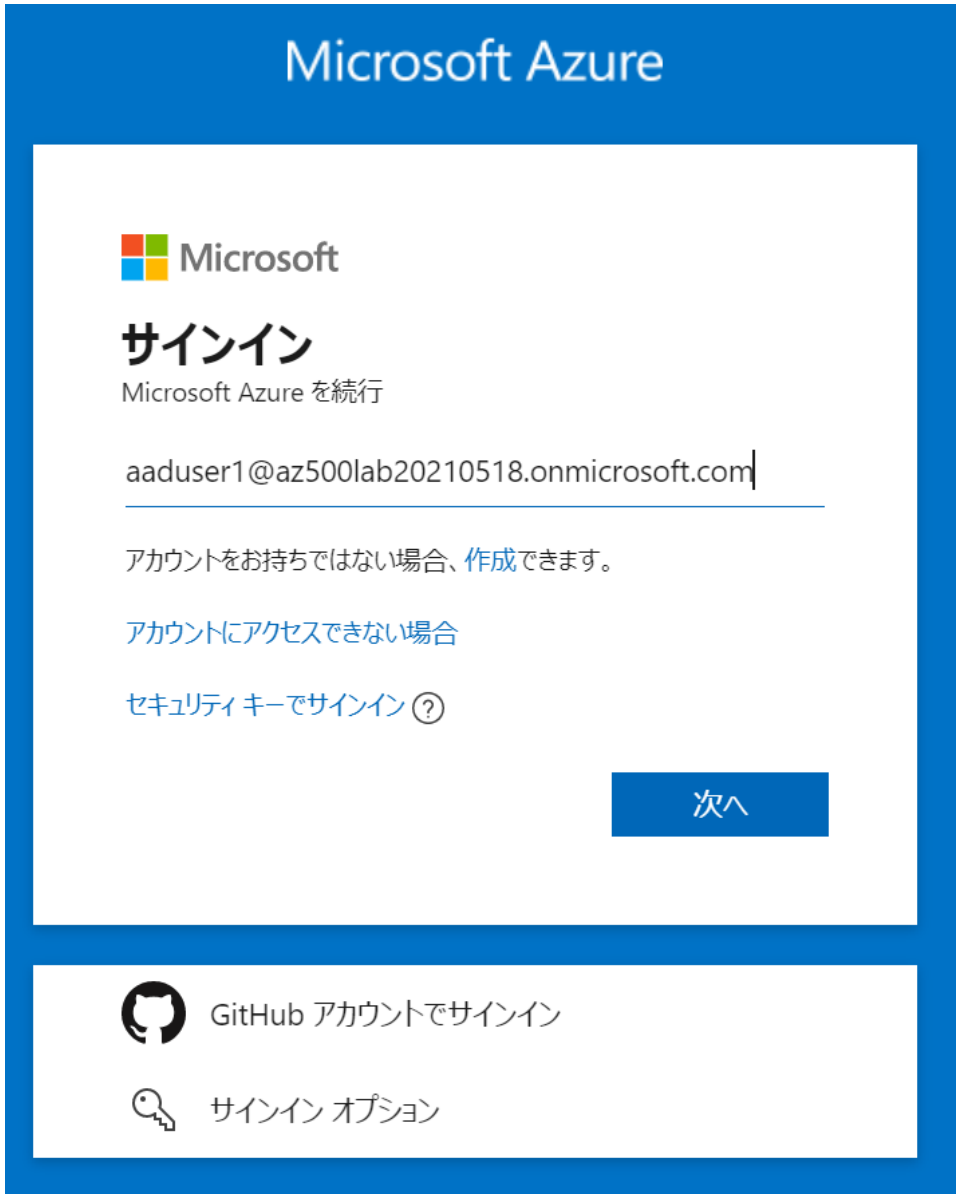
表示名	ユーザー名	MULTI-FACTOR AUTHENTICATION の状態
aaduser1	aaduser1@az500lab20210518.onmicrosoft.com	強制
test2021-0518@outlook.jp ya	test2021-0518_outlook.jp#EXT#@test20210518outlook.onn	無効

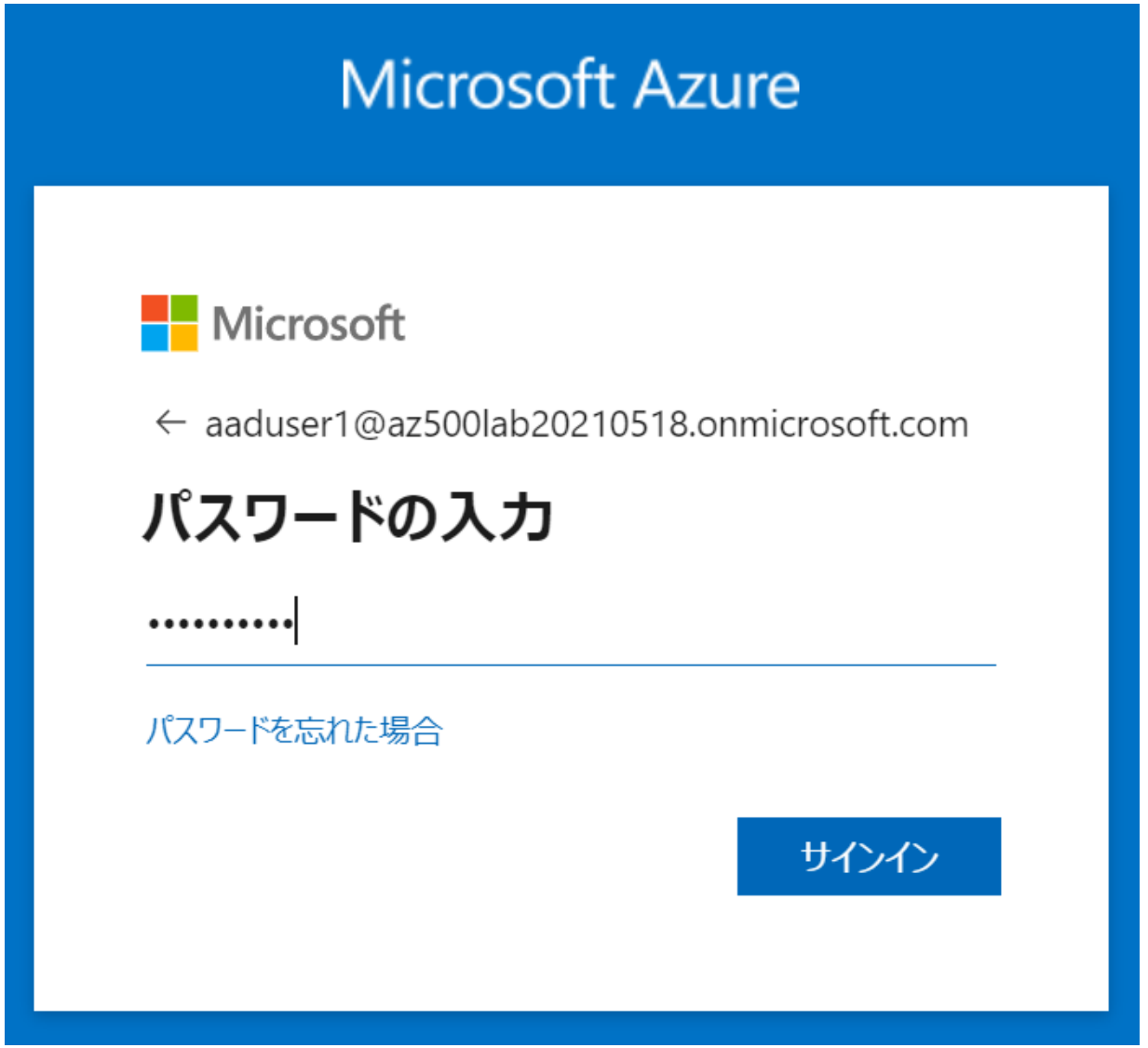
ユーザーを選択

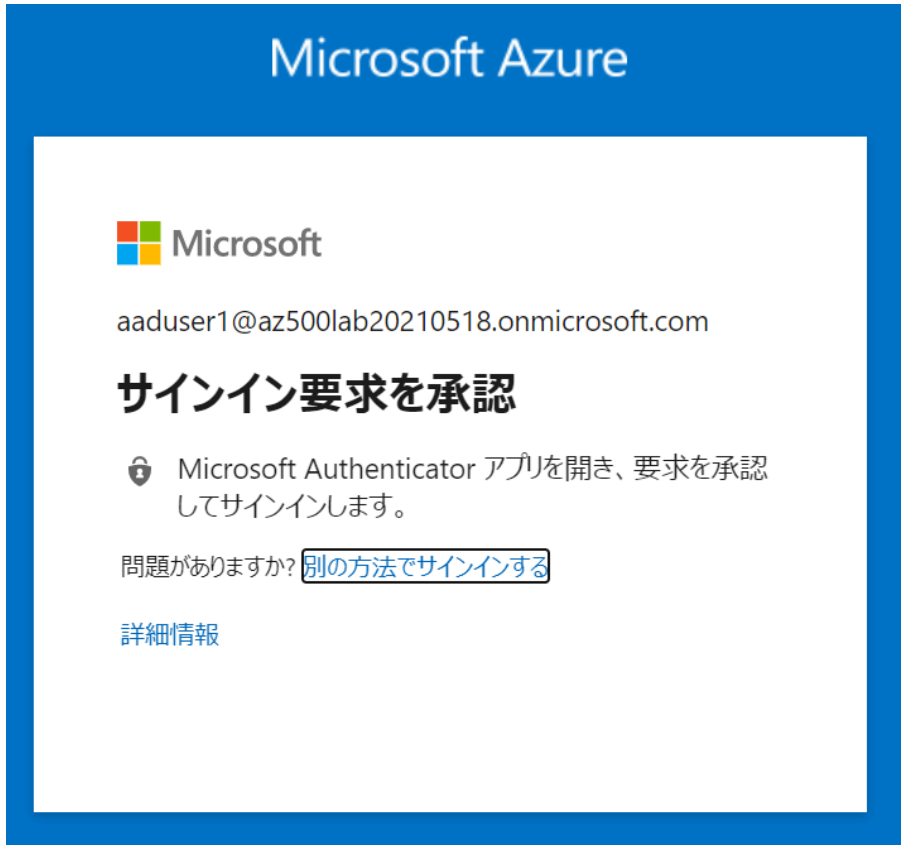
ユーザーのMFAのセットアップが完了すると、そのユーザーのMFA状態が「強制」となります。

ユーザー側での
MFAを使用したサインイン

MFAのセットアップ後、ユーザーがサインインする際に、追加の認証が求められるようになります。


Microsoft Azure
Microsoft
サインイン
Microsoft Azure を続行
aaduser1@az500lab20210518.onmicrosoft.com
アカウントをお持ちではない場合、作成できます。
アカウントにアクセスできない場合
セキュリティ キーでサインイン
次へ
GitHub アカウントでサインイン
サインイン オプション


Microsoft Azure
Microsoft
aaduser1@az500lab20210518.onmicrosoft.com
パスワードの入力
パスワードを忘れた場合
サインイン

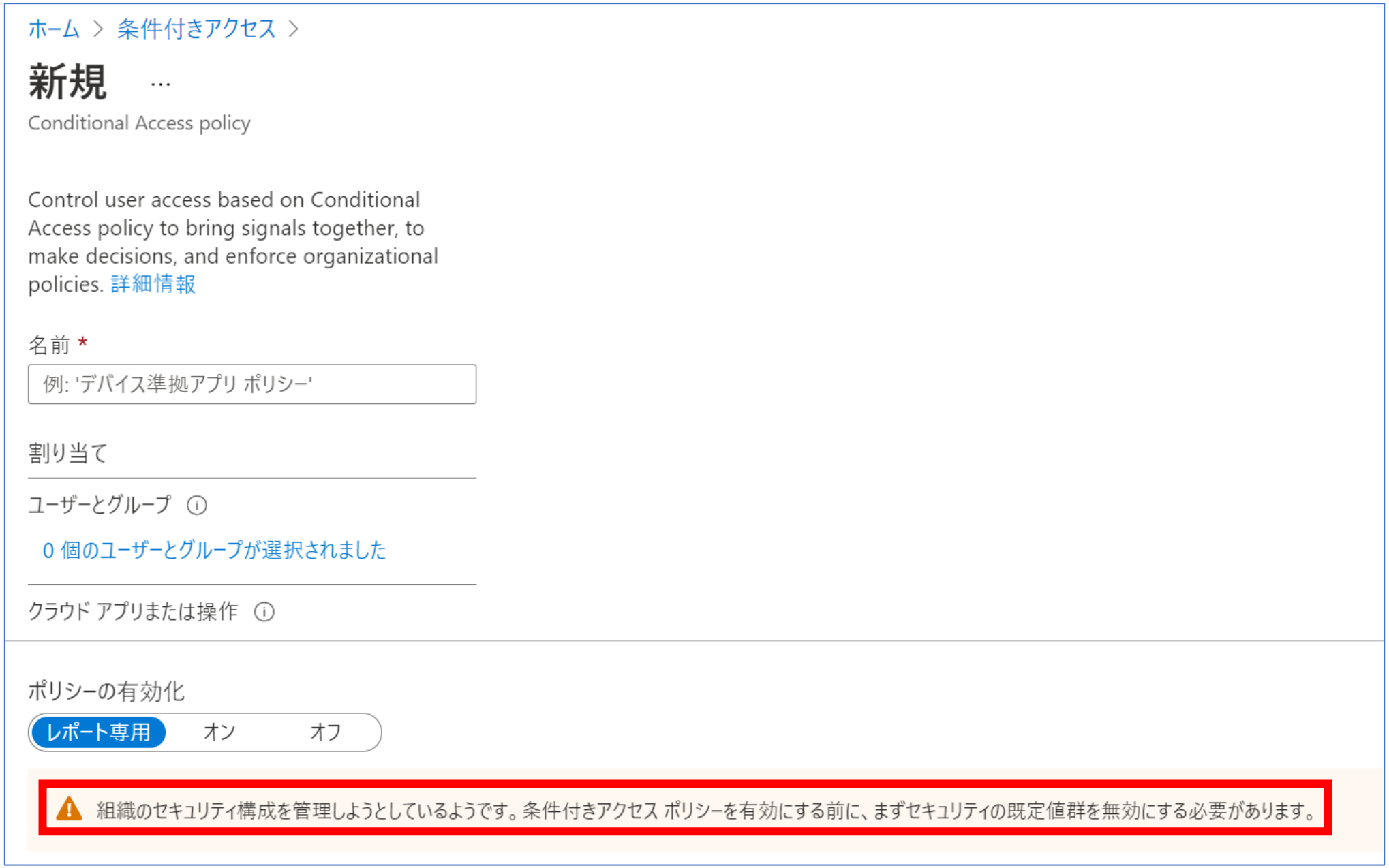

Microsoft Azure
Microsoft
aaduser1@az500lab20210518.onmicrosoft.com
サインイン要求を承認
Microsoft Authenticator アプリを開き、要求を承認してサインインします。
問題がありますか? 別の方法でサインインする
詳細情報


Microsoft Azure
リソース、サービス、ドキュメントの検索 (G+/)
aaduser1@az500lab202...
ADATUMLAB500-04 (AZ500L...
Azure へようこそ!
サブスクリプションをお持ちでない場合は、次のオプションをご確認ください。
Azure の無料試用版から開始する
Azure の製品とサービスに使用できる 200 ドルの無料クレジットを取得できるだけでなく、人気の無料サービスを 12 か月間利用できます。
開始
詳細情報
Azure Active Directory の管理
Azure Active Directory を使用して、アクセスを管理し、スマート ポリシーを設定し、セキュリティを強化します。
表示
詳細情報
学生特典へのアクセス
教育機関ステータスの確認後、無料のソフトウェアまたは Azure クレジットを取得するか、Azure Dev Tools for Teaching にアクセスしてください。
探索
詳細情報

「セキュリティの既定値群」の無効化

「条件付きアクセス」を使用する場合は、テナントの「セキュリティの既定値群」（セキュリティ推奨値のセット。デフォルトで有効）を無効化します。

「条件付きアクセスポリシー」を有効にする前に、「セキュリティの既定値群」を無効にする必要がある

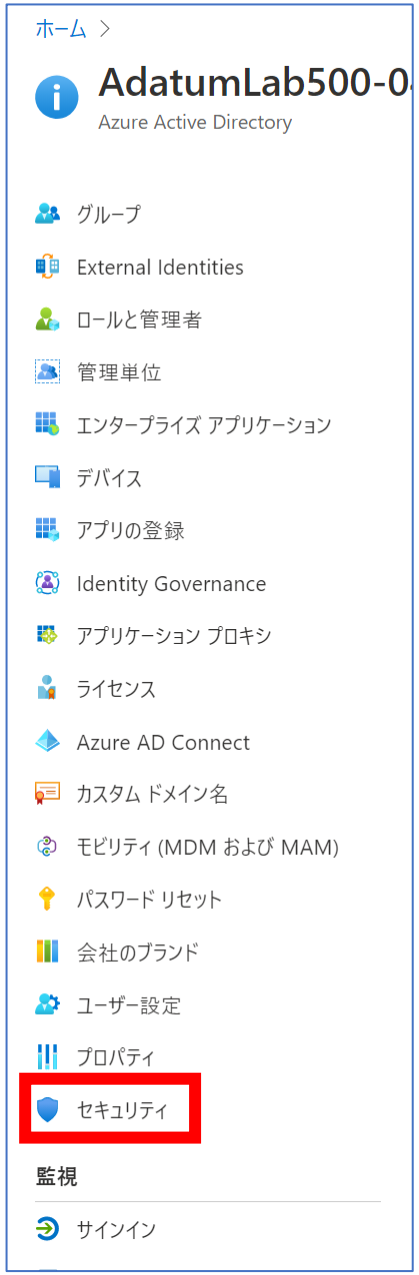


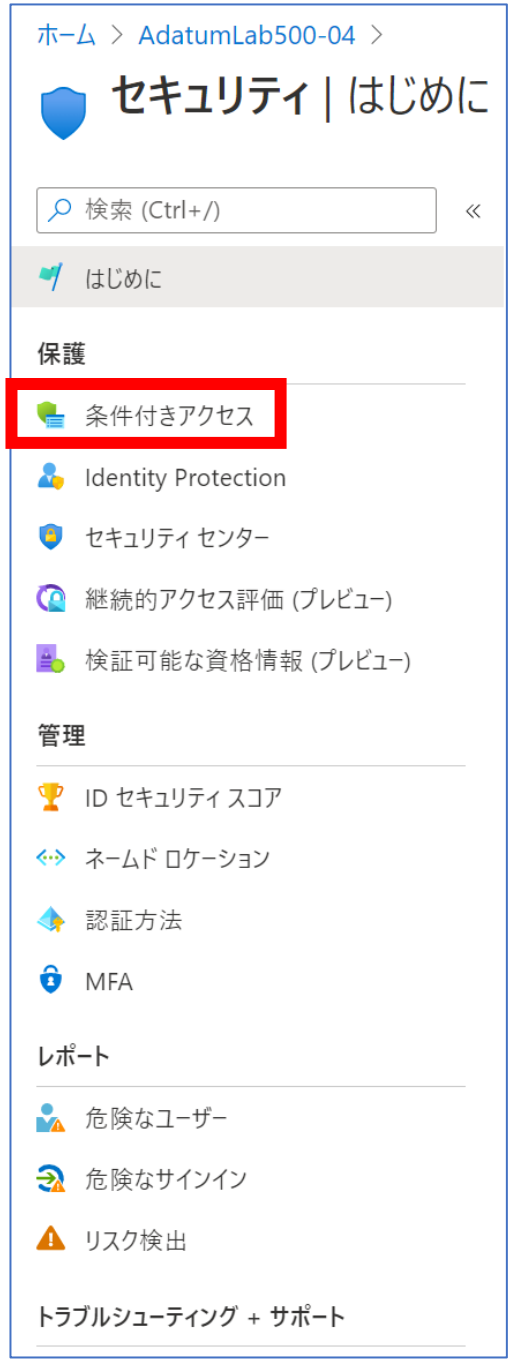
「セキュリティの既定値群」を無効にする

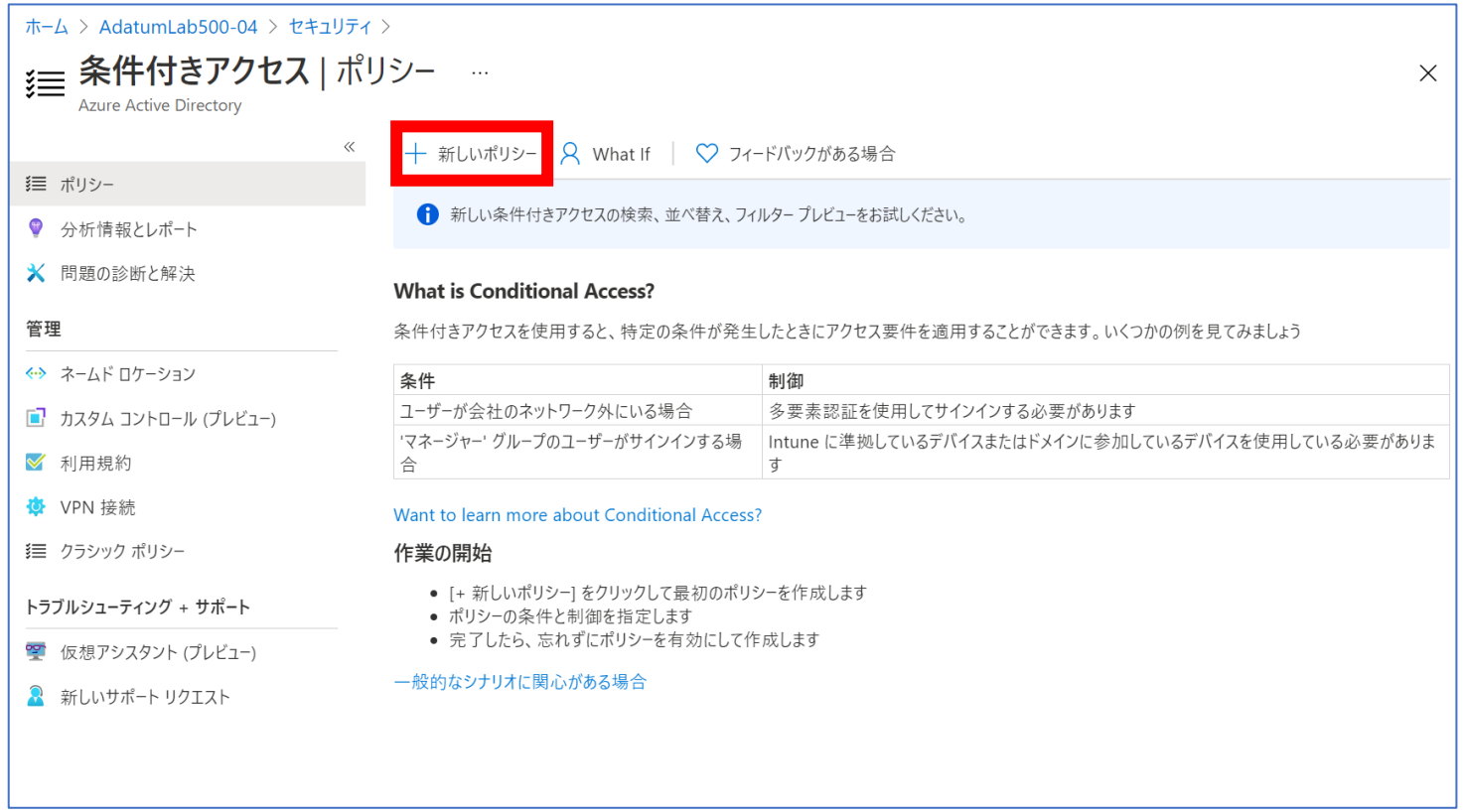
「条件付きアクセス」の利用（ポリシーの作成）

ユーザー、アプリ、その他の条件（リスク等）に応じて、アクセスをブロックまたは許可する仕組み。

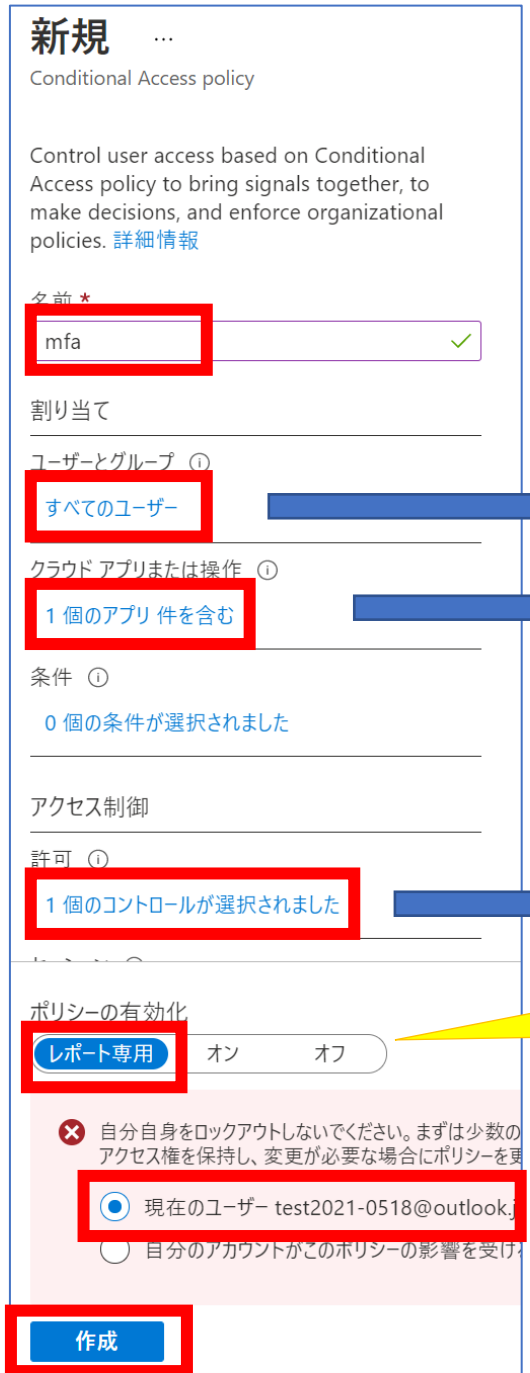
「条件付きアクセス」のポリシー



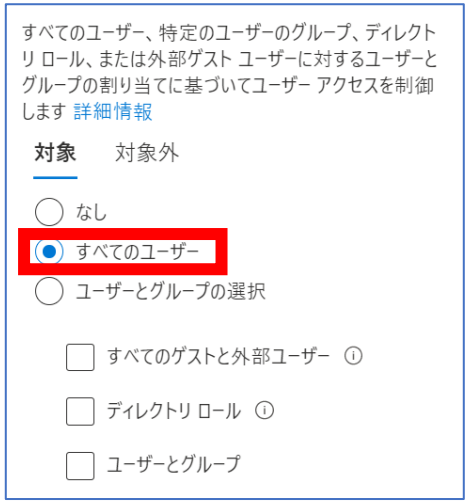




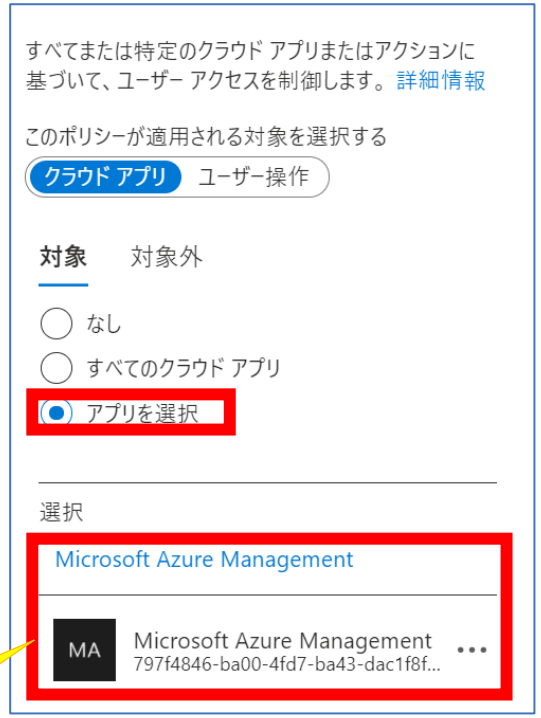
「条件付きアクセスポリシー」の作成例



対象となるユーザー/グループ

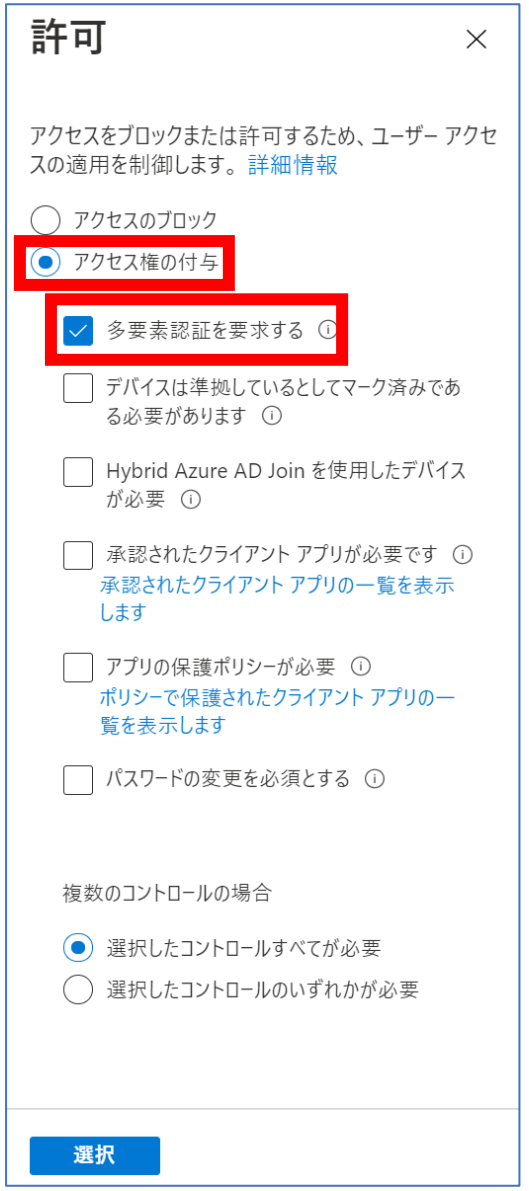


対象となるアプリ



Azure portal等

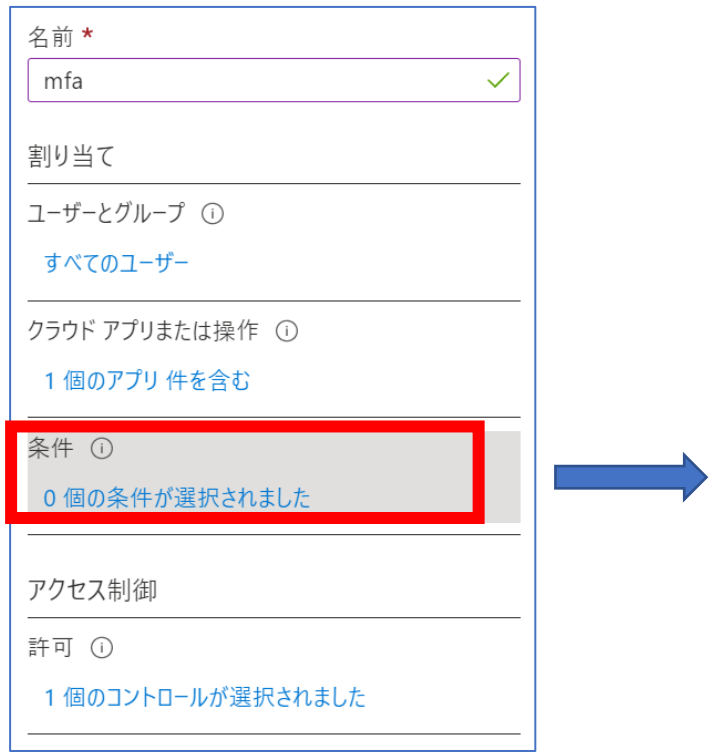
アクセスのブロック/許可



レポート専用：条件に一致したアクセスを記録する。
オン：アクセスを実際にブロックまたは許可する。
オフ：このポリシーの動作をオフにする。

誤った設定で、全ユーザーをブロックしてしまうと、Azure portalにアクセスできなくなってしまったりする。それを避けるために、自分自身のユーザーを例外とする。

「条件付きアクセスポリシー」の「条件」



Azure AD Identity Protection と組み合わせて利用可能となる機能。

たとえば、ダークウェブに流出しているユーザーIDが使用された場合、「ユーザーリスクが高い」（IDが侵害されている可能性が高い）と判定される。

Azure AD Identity Protection と組み合わせて利用可能となる機能。

たとえば、匿名のIPアドレス（Torネットワーク）からのサインインの場合、「サインインリスクが高い」（正規ユーザー以外によってサインインが試行されている可能性が高い）と判定される。

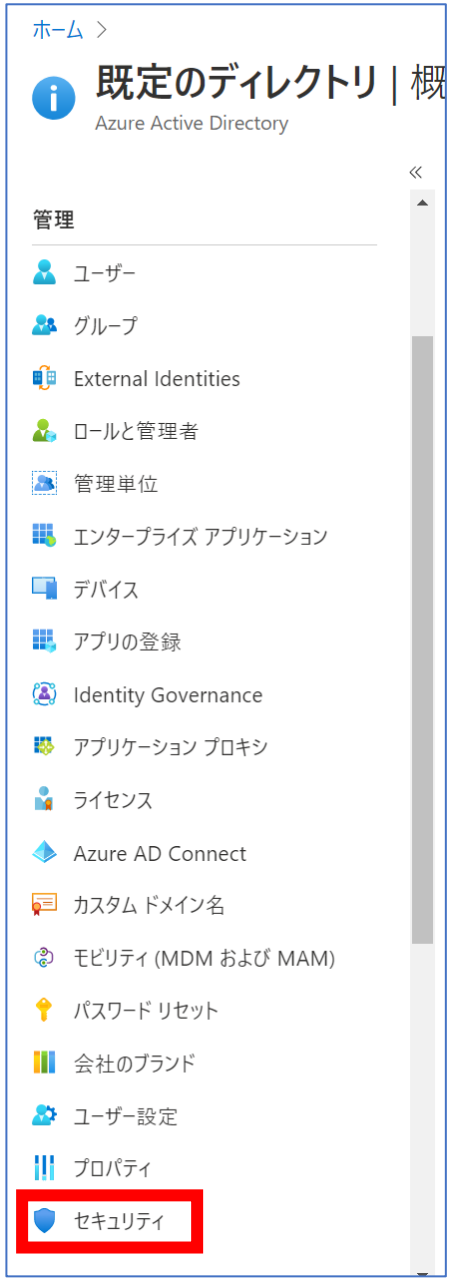
Android, iOS, Windows, macOSなどを選択して、その種類のデバイスからのアクセスかどうかを判定する。

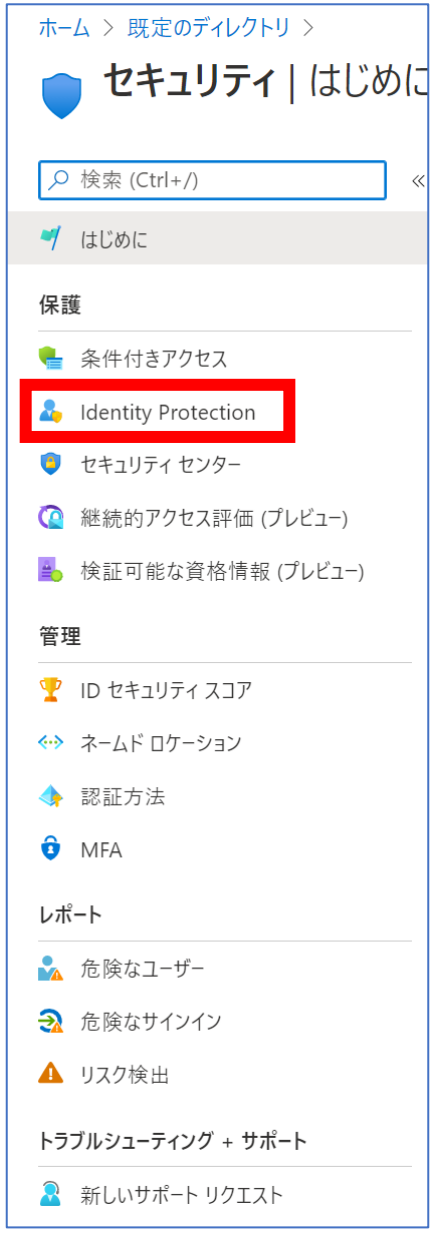
あらかじめ、IPアドレスの範囲などを使用して「場所」を定義しておき、その場所からのアクセスかどうかを判定する。

Identity Protection

ユーザーリスク（ダークウェブ等に流出した「侵害された」IDを使ったサインイン試行の可能性）、**サインインリスク**（匿名IPからのサインイン試行など、本人以外から、サインイン要求が送信されている可能性）を検出し、MFAの実行の要求、パスワードのリセットの要求などを実行する。管理者は、検出されたリスクのレポートを調査できる。

Identity Protection > 概要

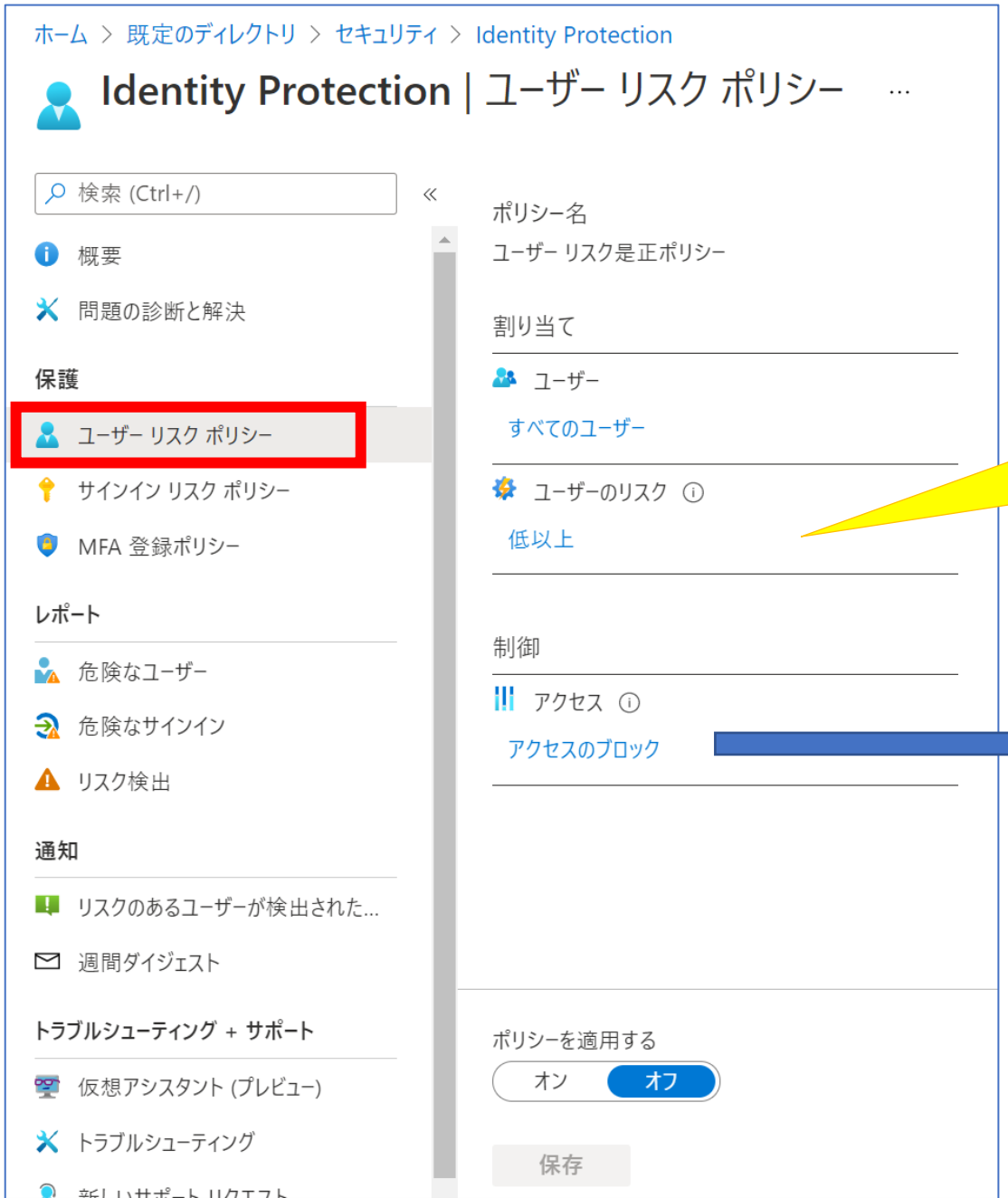




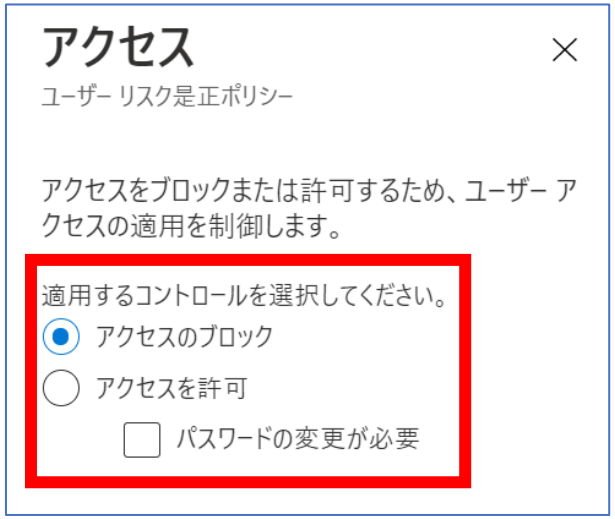
ID セキュリティ スコアは、セキュリティに関する **Microsoft のベスト プラクティスの推奨事項にどれだけ適合しているかを示す指標**（0～100%）。

IDセキュリティスコアの画面

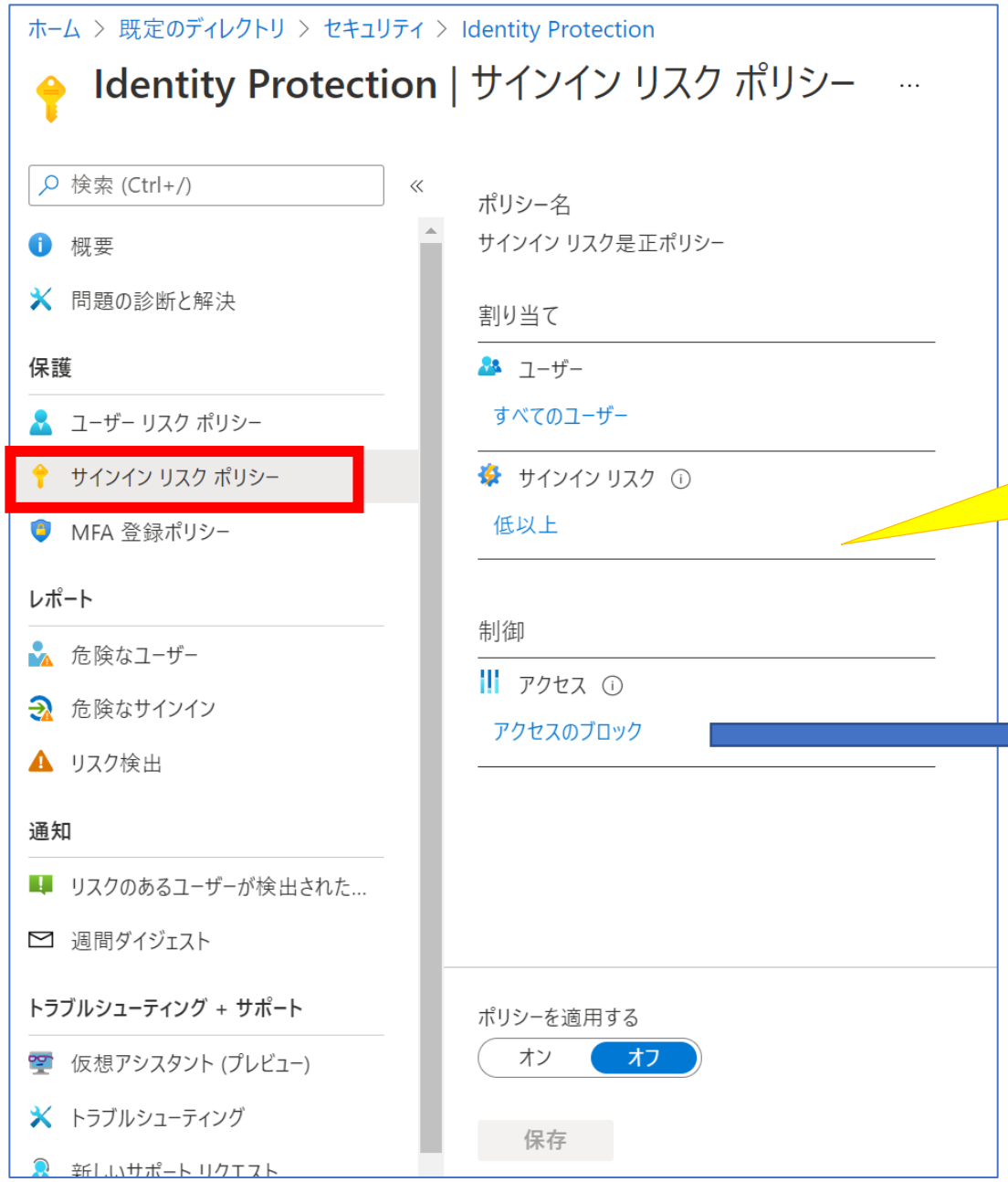
ユーザーリスク（ダークウェブ等に流出した「侵害された」IDを使ったサインイン試行の可能性）のポリシー



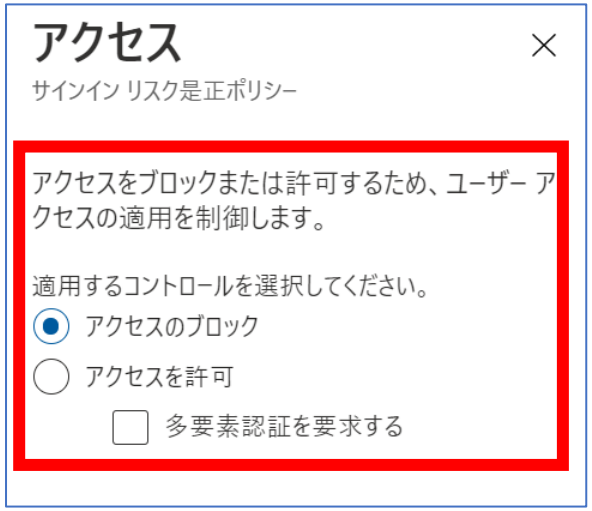
Microsoft で推奨：ユーザー リスク ポリシーのしきい値を **[高]** に設定する



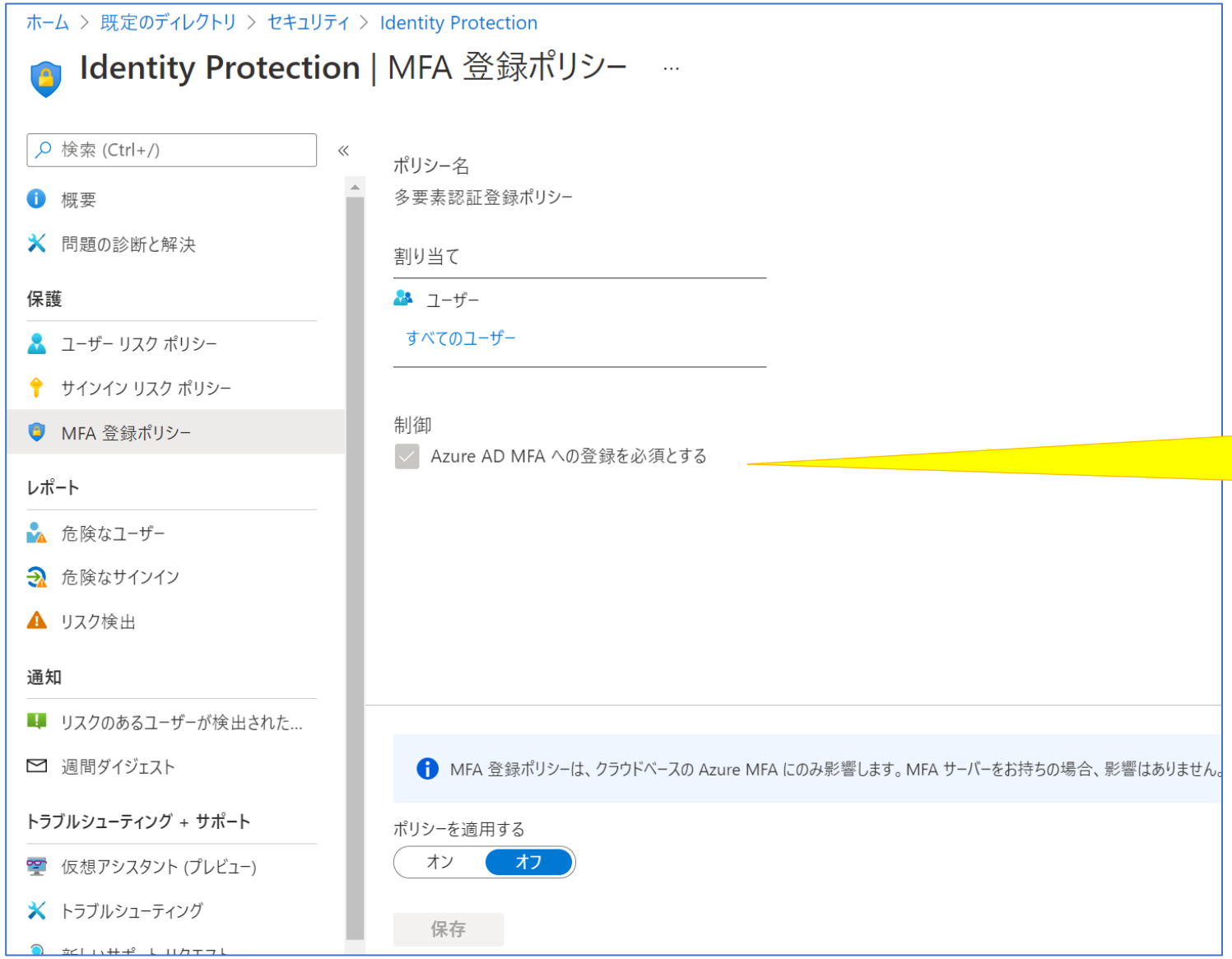
サインインリスク（匿名IPからのサインイン試行など、本人以外から、サインイン要求が送信されている可能性）のポリシー



Microsoft で推奨：サインイン リスク ポリシーを **[中以上]** に設定する

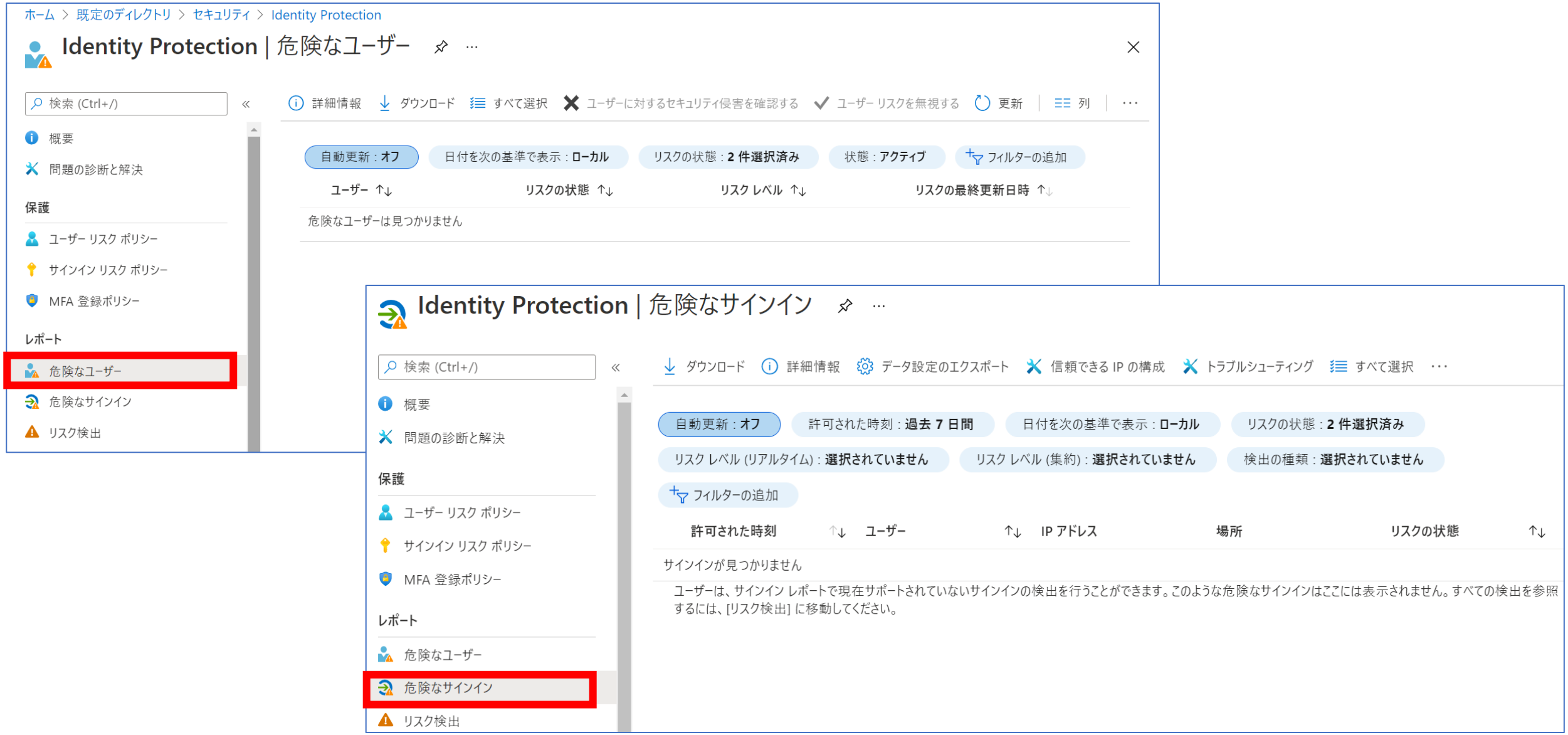


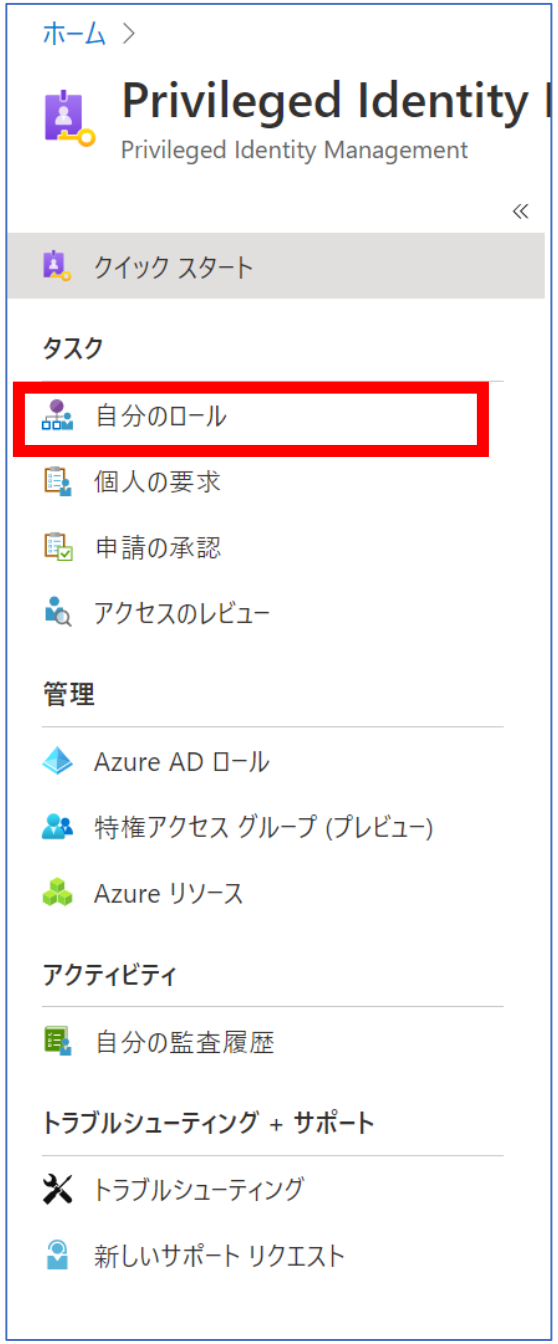
MFA登録ポリシー



MFAへの登録を必須とするよう設定できる

レポート機能


ホーム > 既定のディレクトリ > セキュリティ > Identity Protection
Identity Protection | 危険なユーザー
検索 (Ctrl+/)
詳細情報
ダウンロード
すべて選択
ユーザーに対するセキュリティ侵害を確認する
ユーザー リスクを無視する
更新
列
概要
問題の診断と解決
保護
ユーザー リスク ポリシー
サインイン リスク ポリシー
MFA 登録ポリシー
レポート
危険なユーザー
危険なサインイン
リスク検出
自動更新 : オフ
日付を次の基準で表示 : ローカル
リスクの状態 : 2 件選択済み
状態 : アクティブ
フィルターの追加
ユーザー
リスクの状態
リスク レベル
リスクの最終更新日時
危険なユーザーは見つかりません
Identity Protection | 危険なサインイン
検索 (Ctrl+/)
ダウンロード
詳細情報
データ設定のエクスポート
信頼できる IP の構成
トラブルシューティング
すべて選択
概要
問題の診断と解決
保護
ユーザー リスク ポリシー
サインイン リスク ポリシー
MFA 登録ポリシー
レポート
危険なユーザー
危険なサインイン
リスク検出
自動更新 : オフ
許可された時刻 : 過去 7 日間
日付を次の基準で表示 : ローカル
リスクの状態 : 2 件選択済み
リスク レベル (リアルタイム) : 選択されていません
リスク レベル (集約) : 選択されていません
検出の種類 : 選択されていません
フィルターの追加
許可された時刻
ユーザー
IP アドレス
場所
リスクの状態
サインインが見つかりません
ユーザーは、サインイン レポートで現在サポートされていないサインインの検出を行うことができます。このような危険なサインインはここには表示されません。すべての検出を参照するには、[リスク検出] に移動してください。


ホーム
Privileged Identity
Privileged Identity Management
クイック スタート
タスク
自分のロール
個人の要求
申請の承認
アクセスのレビュー
管理
Azure AD ロール
特権アクセス グループ (プレビュー)
Azure リソース
アクティビティ
自分の監査履歴
トラブルシューティング + サポート
トラブルシューティング
新しいサポート リクエスト


ホーム > Privileged Identity Management >
自分のロール | Azure AD ロール
Privileged Identity Management | 自分のロール
アクティブ化
Azure AD ロール
特権アクセス グループ (プレビュー)
Azure リソース
トラブルシューティング + サポート
トラブルシューティング
新しいサポート リクエスト
最新の情報に更新
Got feedback?
資格のある割り当て
アクティブな割り当て
期限切れの割り当て
ロールで検索します
ロール
スコープ
メンバーシップ
終了時刻
操作
結果がありません