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

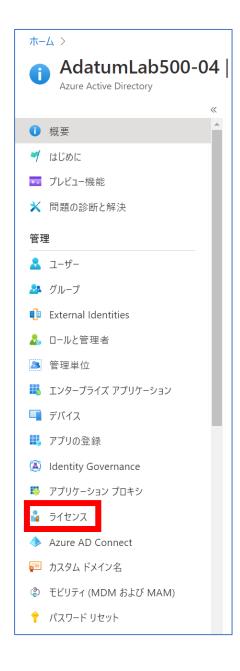
機能	概要	ライセンス
クラウドのみのユーザー パスワードの 変更	Azure AD のユーザーが自分のパスワードを知っていて、新しいパスワードへの変更を希望する場合。	無料
クラウドのみのユーザー パスワードの リセット	Azure AD のユーザーがパスワードを忘れて、リセットする必要がある場合。	Microsoft 365 Business Standard Microsoft 365 Business Premium Azure AD Premium P1 または P2
オンプレミスの書き戻し を含む、ハイブリッド ユーザーのパスワードの 変更 または リセット	Azure AD Connect 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





アクティブ化

利用可能なプランと機能の参照

Microsoft からサブスクリプションを直接購入する場合は、サービスの購入

ENTERPRISE MOBILITY + SECURITY E5

Enterprise Mobility + Security E5 は、IT のコンシューマライゼーション、BY 括的なクラウド ソリューションです。 このスイートには、Azure Active Director Microsoft Intune および Azure Rights Management が含まれています

∨ 無料試用版

AZURE AD PREMIUM P2

Azure Active Directory Premium P2 を使用すると、高度なセキュリティ様ケーションに対するルール ベースの割り当てにアクセスできます。 エンド ユーザーイズされたブランドを利用できるようになります。

へ 無料試用版

Azure Active Directory Premium P2 を使用すると、多要素認証 ユーザーのセルフサービスなど、追加の機能によってディレクトリを強化

試用版には 100 個のライセンスが含まれており、有効期限はライセンす。有料版へのアップグレードを希望される場合は、Azure Active D 入いただく必要があります。価格の詳細情報

Azure Active Directory Premium P2 は、Azure サービスとは別に ライセンス認証を確認すると、マイクロソフト オンライン サブスクリプシ: 声明に同意したことになります。

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。

ホーム > ライセンス

トラブルシューティング + サポート

ゑ 新しいサポート リクエスト



🔪 ライセンス | すべての製品

	«	十 試用/購入 十 割り当て 🗹 請	求書 │ 〓 列 │	♡ フィードバックがある場合	
・ 概要		名 前	合計	割り当て済み	使用可能
管理		Azure Active Directory Premium P	2 100	0	100
🗼 すべての製品					
🙀 セルフサービス サインアップ製品					
アクティビティ					
■ 監査□グ					

まもなく有効期限切れ

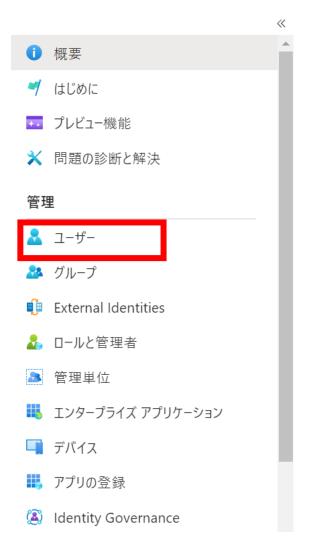
ユーザーへの Premium P2ライセンスの 割り当て

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

ホーム >



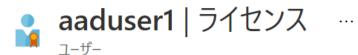




ホーム > AdatumLab500-04 > ユーザー > aaduser1

 \ll

製品



•••

X

✗ 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□グ



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ま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

/

Azure Active Directory Premium P2

ライセンス オプションの確認

選択

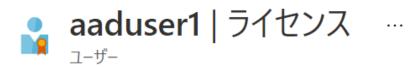
 \vee

Azure Active Directory Premium P2

- ✓ Cloud App Security Discovery
- ✓ Microsoft Azure Multi-Factor Authentication
- Azure Active Directory Premium P1
- ✓ Azure Active Directory Premium P2

ユーザーへのPremium P2ライセンスの割り当てができました

ホーム > AdatumLab500-04 > ユーザー > aaduser1



★ 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 □ールの割り当て

+	割り当て	(")	再処理	7	更新	== 列	(()	フィードバックがある場合
			开处生		火 和	/.j		ノー エハフフカの2000日

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。

ホーム \rightarrow AdatumLab500-04 \rightarrow ライセンス \rightarrow

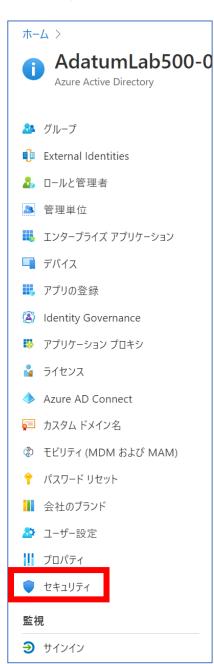




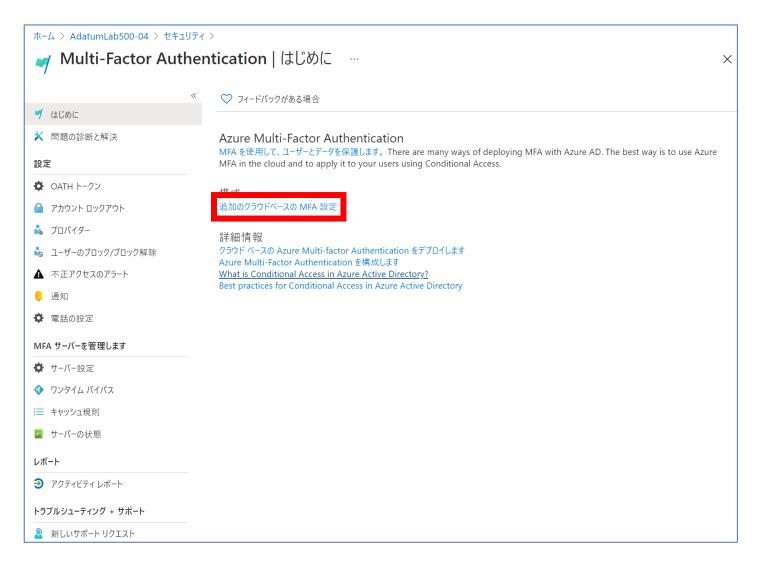
ユーザーのMFAの有効化

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。

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

アプリケーション パスワード (詳細情報を見る)

- ブラウザーではないアプリケーションへのサインイン用にアプリケーション パスワードの作成を許可する
- ブラウザーではないアプリケーションへのサインイン用にアプリケーション パスワードの作成を許可しない

信頼済み ip (詳細情報を見る)

□ イントラネット内のフェデレーション ユーザーからのリクエストの場合、多要素認証をスキップする次の範囲の IP アドレス サブネットから送信されたリクエストの場合、多要素認証をスキップする

192.168.1.0/27 192.168.1.0/27 192.168.1.0/27

検証オプション (詳細情報を見る)

ユーザーが利用可能な方法:

- 電話への連絡
- ☑ 電話へのテキスト メッセージ
- ☑ モバイル アプリによる通知
- ☑ モバイル アプリまたはハードウェア トークンからの確認コード

信頼済みデバイスで多要素認証を記憶する(詳細情報を見る)

□ 信頼済みデバイスでユーザーが多要素認証を記憶できるようにする (1 - 365 日)

ユーザーがデバイスを信頼できる日数 90

注: 最適なユーザー エクスペリエンスのためには、MFA のプロンプトを最小限にします。条件付きアクセスのサインイン頻度を使用して、信頼済みのデバイスや場所、危険度の低いセッションでのセッションの有効期間を延長することをお勧めします。別の方法として、[信頼済みデバイスで MFA を記憶する] を使用する場合は、期間を 90 日以上に延長してください。 再認証のプロンプトに関する詳細情報をご確認ください。

保存

Microsoft

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**~[2**] Multi-Factor Authentication の状態: 任意 🗸 一括更新 **MULTI-FACTOR** 表示名 ▲ ユーザー名 AUTHENTICATION の状態 aaduser1@az500lab20210518.onmicrosoft.com 無効 aaduser1 ユーザーを選択 test2021-0518@outlook.jp ya test2021-0518_outlook.jp#EXT#@test20210518outlook.onn

ユーザーのMFAの有効化

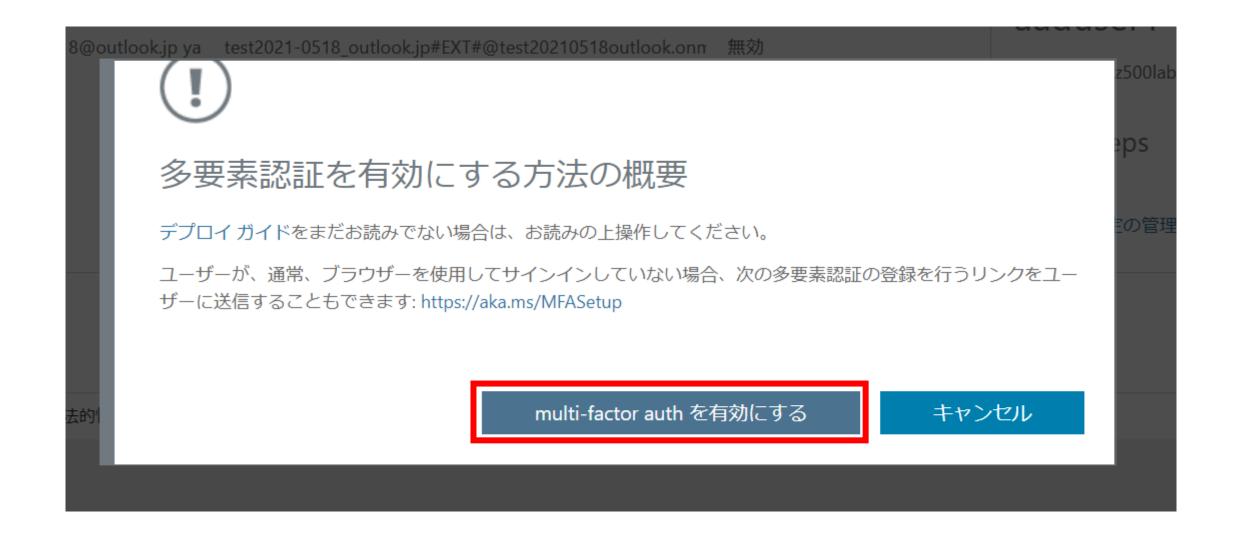
test2021-0518_outlook.jp#EXT#_test20210518outlook.onmiHMNAQ#EXT#@az500lab20210518.onmicrosoft.com

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	3ユ−マ Р 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	
7	aaduser1	aaduser 1@az 500 lab 20210 518. on microsoft.com	無効	aaduser1
	test2021-0518@outlook.jp ya	test2021-0518_outlook.jp#EXT#@test20210518outlook.onm	無効	aaduser1@az500lab20210518.onr
				quick steps 有効にする ユーザー設定の管理

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



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

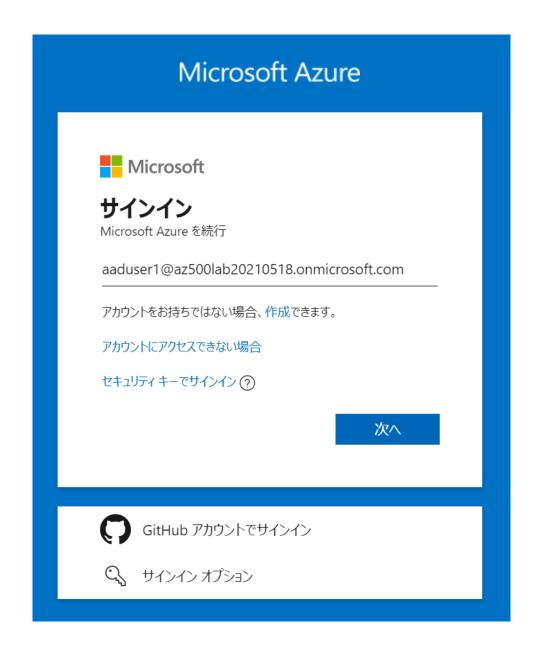
始める前に、多要素認証のデプロイガイドを参照してください。

表	示: サインインが許可されている	るユ−∨	一指	舌更新	
	表示名 📤	ユーザー名	MULTI-FACT	TOR CATION の状態	
	aaduser1	aaduser 1@az 500 lab 20210 518. on microsoft.com	有効		ユーザーを選択
	test2021-0518@outlook.jp ya	test2021-0518_outlook.jp#EXT#@test20210518outlook.onn	無効		ユーリーで選択
				状態が「有	効」となります。

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



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

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

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

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?

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。





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

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

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 アプリが正常に登 × 録されました

Tue, 18 May 2021 09:02:00 GMT

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

一括更新

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マ 🎤 Multi-Factor Authentication の状態: 任意 🗸

	表示名 ▲	ユーザー名	MULTI-FACTOR AUTHENTICATION の状態	
	aaduser1	aaduser 1@az 500 lab 20210 518. on microsoft. com	強制	ユーザーを選択
	test2021-0518@outlook.jp ya	test2021-0518_outlook.jp#EXT#@test20210518outlook.onn	無効	

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 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 (?)





GitHub アカウントでサインイン



Q、サインイン オプション

Microsoft Azure



← aaduser1@az500lab20210518.onmicrosoft.com

• • • • • • • • •

パスワードを忘れた場合

サインイン

Microsoft Azure



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。

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。

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

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

ホーム > AdatumLab500-04 AdatumLab500-04 | プロパティ … Azure Active Directory □ 保存 🗙 破棄 🎎 グループ テナントのプロパティ 詳細情報 External Identities 名前 * ▲ □-ルと管理者 AdatumLab500-04 いいえ はい 🚵 管理単位 国/リージョン **United States** エンタープライズ アプリケーション 場所 デバイス United States datacenters アプリの登録 通知言語 Identity Governance English ₩ アプリケーション プロキシ その他 テナント ID 64b38159-da70-4ccc-83cf-2cebe66a7f86 Azure AD Connect 技術部連絡先 test2021-0518_outlook.jp#EXT#@test20210518outlook.onr 同 カスタム ドメイン名 ② モビリティ (MDM および MAM) グローバル プライバシー連絡先 ↑ パスワード リセット プライバシーに関する声明 URL 会社のブランド ♪ ユーザー設定 プロパティ Azure リソースのアクセス管理 セキュリティ yamada test2021-0518@outlook.jp (test2021-0518@outlook び管理グループへのアクセスを管理できます。詳細情報 監視 いいえ ⇒ サインイン セキュリティの既定値群の管理 ■ 監杏□ガ

セキュリティの既定値群の有効化

セキュリティの既定値群は、Microsoft によって推奨されている基本的な ID セ キュリティ機構のセットです。有効にすると、これらの推奨事項が組織内で自動 的に適用されます。管理者とユーザーは、一般的な ID 関連の攻撃からより良 く保護されるようになります。

 \times

セキュリティの既定値群の有効化

品質向上のため、セキュリティの既定値群を無効にしている理由をお聞かせくだ

✓ 自分の組織では条件付きアクセスを使用している

| 目分の組織で必要小可欠なビシネスアプリケーションを使用できない

自分の組織では MFA チャレンジが多くなり過ぎる

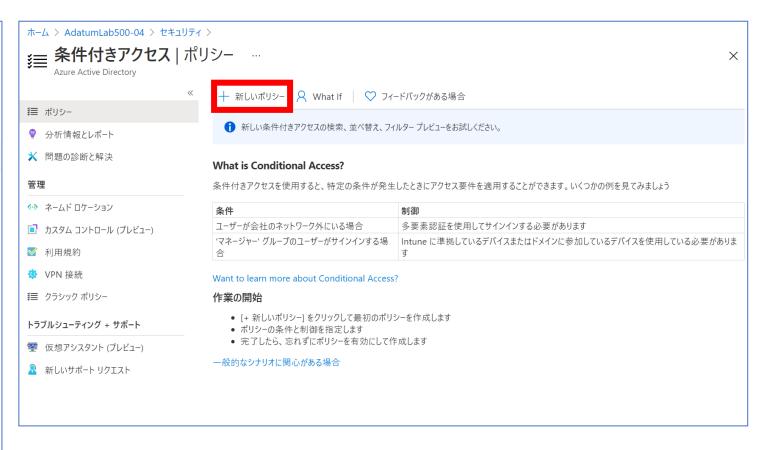
「条件付きアクセス」の利用 (ポリシーの作成)

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。

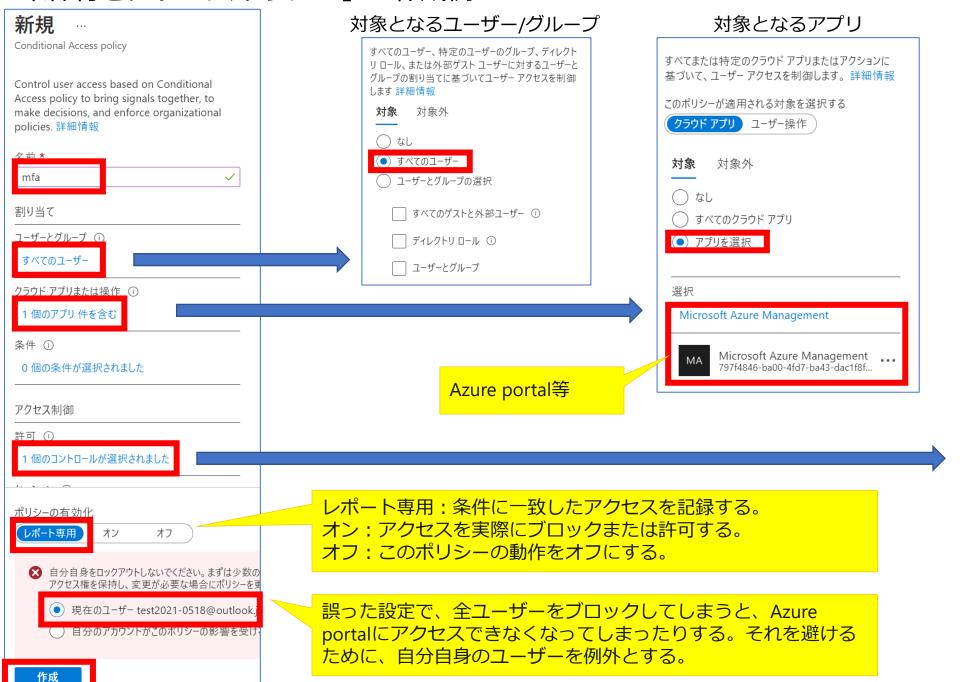
「条件付きアクセス」のポリシー







「条件付きアクセスポリシー」の作成例



アクセスのブロック/許可

, , <u> </u>
許可 ×
アクセスをブロックまたは許可するため、ユーザー アクセ スの適用を制御します。 詳細情報
アクセスのブロックアクセス権の付与
✓ 多要素認証を要求する ①
デバイスは準拠しているとしてマーク済みである必要があります ①
Hybrid Azure AD Join を使用したデバイス が必要 ①
承認されたクライアント アプリが必要です ① 承認されたクライアント アプリの一覧を表示 します
アプリの保護ポリシーが必要 ① ポリシーで保護されたクライアント アプリの一覧を表示します
パスワードの変更を必須とする ①
複数のコントロールの場合
● 選択したコントロールすべてが必要
○ 選択したコントロールのいずれかが必要

選択

「条件付きアクセスポリシー」の「条件」



リスク、デバイス プラットフォーム、場所、クライアント ア プリ、またはデバイスの状態などの条件からのシグナル に基づいて、ユーザーアクセスを制御します。詳細情 報 ユーザーのリスク (i) 未構成 サインインのリスク ① 未構成 デバイス プラットフォーム (1) 未構成 場所 ① 未構成 クライアント アプリ ① 未構成 デバイスの状態 (プレビュー) ① 未構成

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。

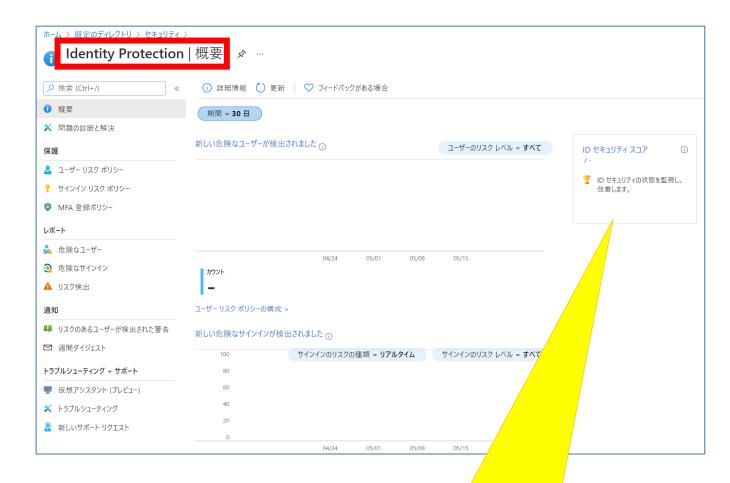
Identity Protection

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





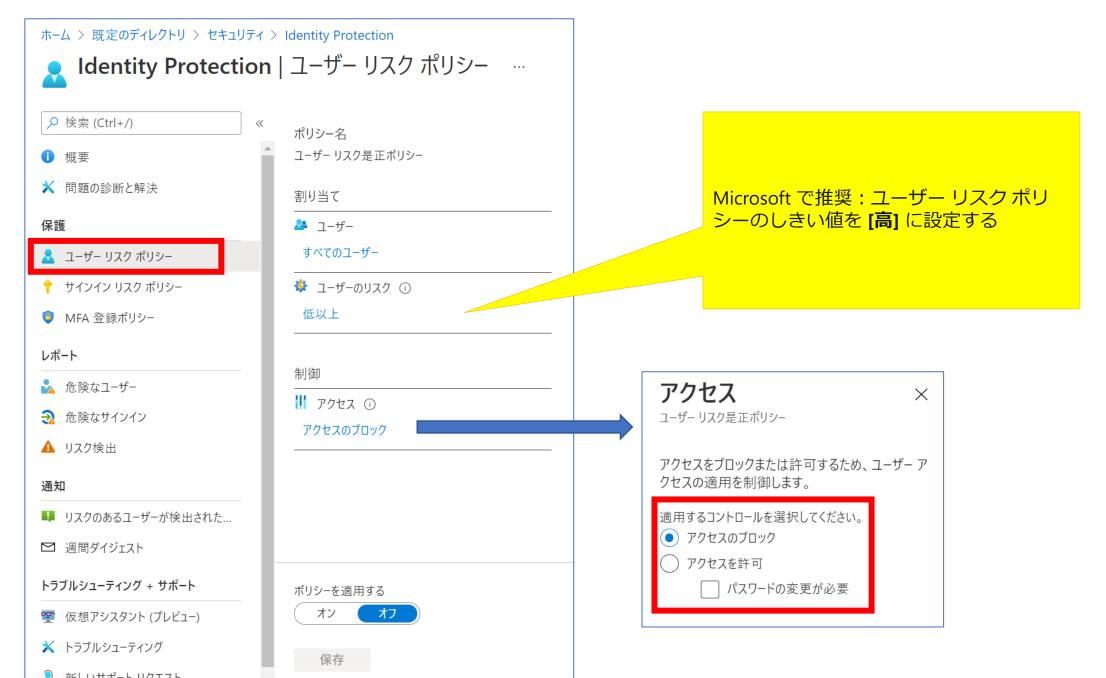


ID セキュリティ スコアは、セキュリティに関する Microsoft のベスト プラクティスの推奨 事項にどれだけ適合しているかを示す指標(0 ~100%)。

IDセキュリティスコアの画面



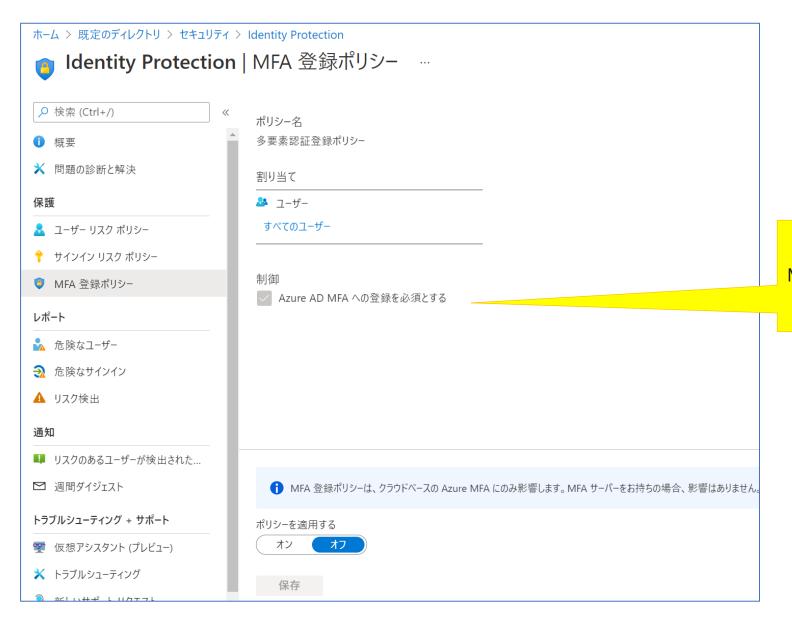
ユーザーリスク(ダークウェブ等に流出した「侵害された」IDを使ったサインイン試行の可能性)のポリ



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

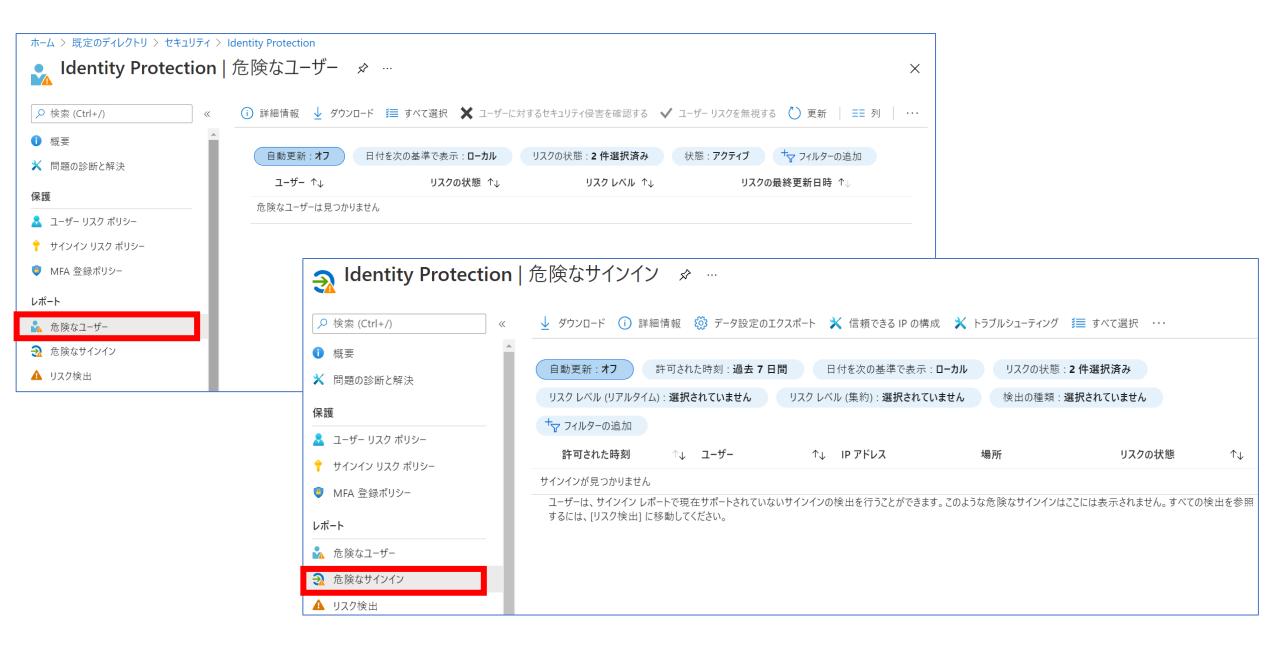


MFA登録ポリシー



MFAへの登録を必須とするよう設定できる

レポート機能



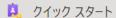
ホーム >



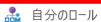
Privileged Identity I

Privileged Identity Management

<<



タスク





🖫 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

- メ 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 □-J
- № 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

- メ トラブルシューティング
- 新しいサポート リクエスト

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

↑↓ スコープ ロール

() 最新の情報に更新 ○ Got feedback?

↑↓ メンバーシップ

↑↓ 終了時刻

操作

結果がありません