Azure AD サービス
ユーザガイド

[システム管理者さま向け]

2023 年 4 月 17 日　Version 3.2

ソニービズネットワークス株式会社

ご注意

予告なく本書の一部または全体を修正、変更することがあります。また、本製品の内容またはその仕様により発生した損害については、いかなる責任も負いかねます。
本書で使用されるスクリーンショットは、2022 年 8 月時点のマイクロソフト社から提供される各種 UI を参考情報としております。

目次

1 はじめに

1-1 本マニュアルについて

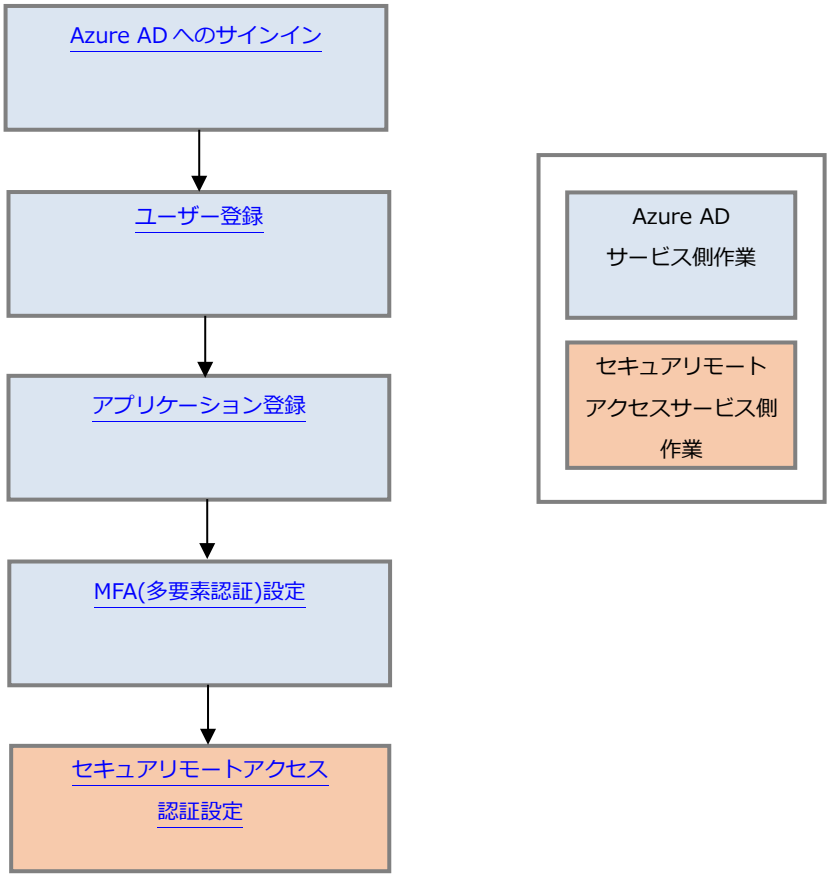
このたびは、Azure AD サービスをご契約いただき、ありがとうございます。

本マニュアルは、管理者様向けに Azure AD サービスを使って、弊社が提供する「セキュアリモートアクセスサービス(以下セキュアリモートアクセス)」のユーザー管理および認証等を設定する方法について記載しています。

サービスを利用開始するにあたり、本マニュアルにある設定を行ってください。

2 設定の流れ

初期設定フローは以下の通りです。



3 注意事項

Azure AD サービスを利用するにあたり以下の注意事項があります。

■ Azure AD サービスでは様々な設定が可能ですが、弊社サポートデスクがお問い合わせなどを受け付けている項目は以下の通りとなります。

- ユーザー追加／削除の手順案内
- 弊社が提供している「セキュアリモートアクセス」との連携手順
- 弊社が提供している「セキュアリモートアクセス」を利用するための MFA(多要素認証)の設定
- 弊社が提供している「セキュアリモートアクセス」とのユーザー認証に関わるトラブルシューティング

その他設定項目につきましては、お客さま自身の自己責任でご利用ください。

4 Azure AD へのサインイン

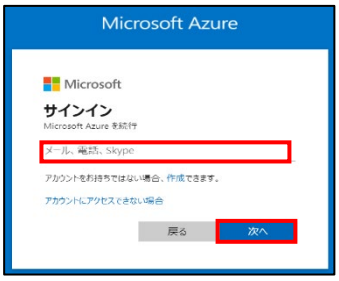
Azure AD へのサインイン手順です。
初回アクセス時は、ご契約時にお送りしている登録内容通知(User-Parameters-AzureAD-AD*****-**.pdf)をご準備ください。

4-1 Azure AD ポータルにアクセス

1. Microsoft Azure ポータルにアクセスします。

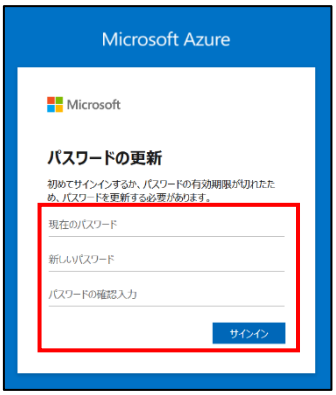
URL：https://portal.azure.com

2. 登録内容通知に記載されている「管理者 ID」を入力し、「次へ」をクリックします。

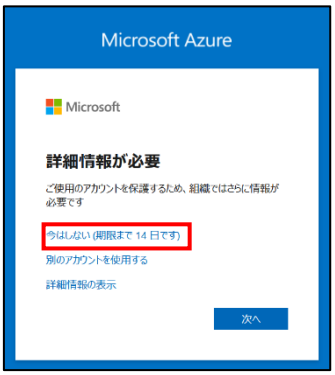


3. 登録内容通知に記載されている「パスワード」を入力し、「次へ」をクリックします。

4. 初回アクセス時は、パスワードの更新が必要です。
新しいパスワードを設定後、「サインイン」をクリックします。



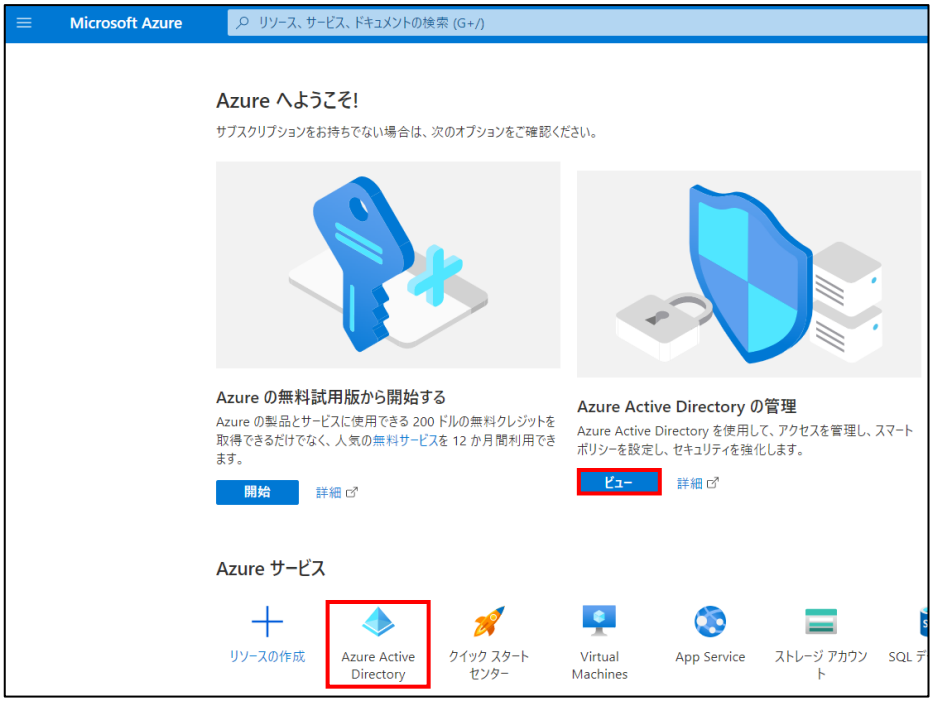
5. MFA 設定が有効になっている場合(初期状態)、MFA を設定するための詳細情報の入力が求められます。
下記図より「今はしない（期限まで〇〇日です）」をクリックします。



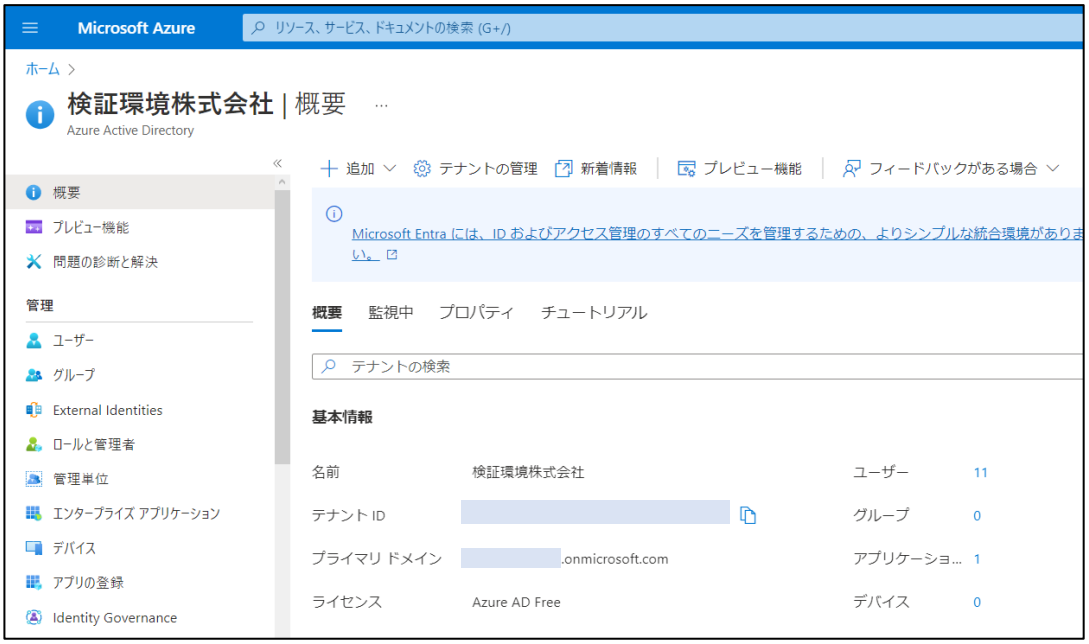
重要

- 初期状態で「セキュリティの既定値」は有効になっているため、すべてのユーザーの MFA が有効になっています。
- MFA を無効へ変更しない、もしくは各ユーザーが最初のサインインから 14 日以内に MFA の設定をしない場合、サインイン時に MFA の設定が強制され、パスワードのみでのサインインができなくなります。

6. サインインすると Azure AD ポータル(ホーム)画面に遷移します。
「Azure Active Directory の管理」の「ビュー」をクリックするか、「Azure Active Directory」をクリックして、概要ページを表示します。



概要ページ



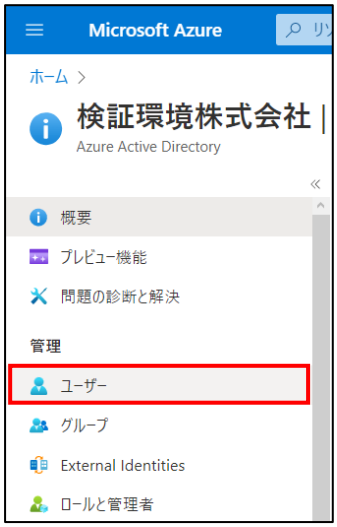
5 ユーザー登録

認証するユーザーの追加や削除などの管理を行うための手順です。

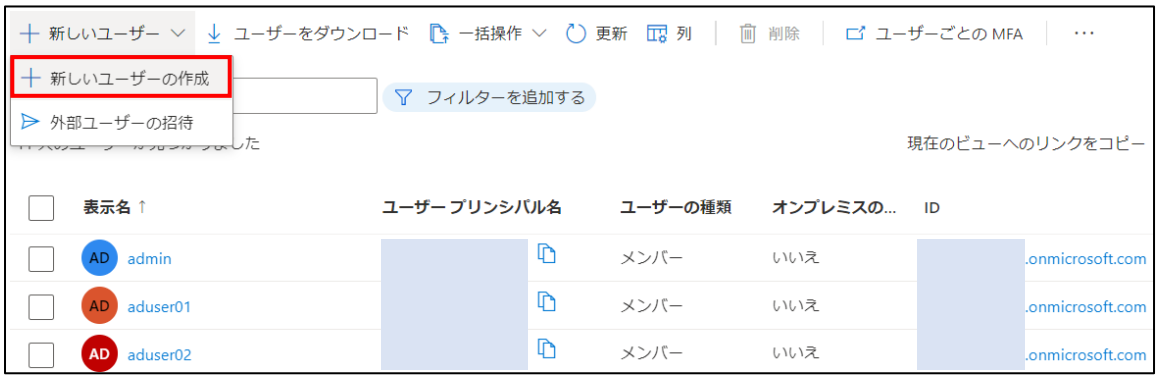
CSV ファイルを使ったユーザー一括登録を行なう場合は、[5-2 ユーザー一括登録]をご参照ください。

5-1 ユーザー追加

1. 概要ページで「ユーザー」を選択します。



2. 「新しいユーザーの作成」を選択します。



3. 「ユーザーの作成」をチェックし、「ユーザー名」と「名前」を入力して、「作成」をクリックします。

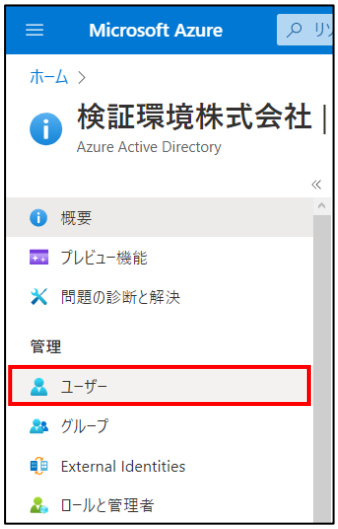
項目	値
ユーザー名	Azure AD にサインインする際に必要な識別子
名前	任意の名前を入力
パスワード	自動で生成されます （パスワードは控えておいてください）
グループとロール	不要
サインのブロック	任意に設定（デフォルトは「いいえ」）
利用場所	任意に設定
ジョブ情報	不要

4. ユーザーが登録されたことを確認します。

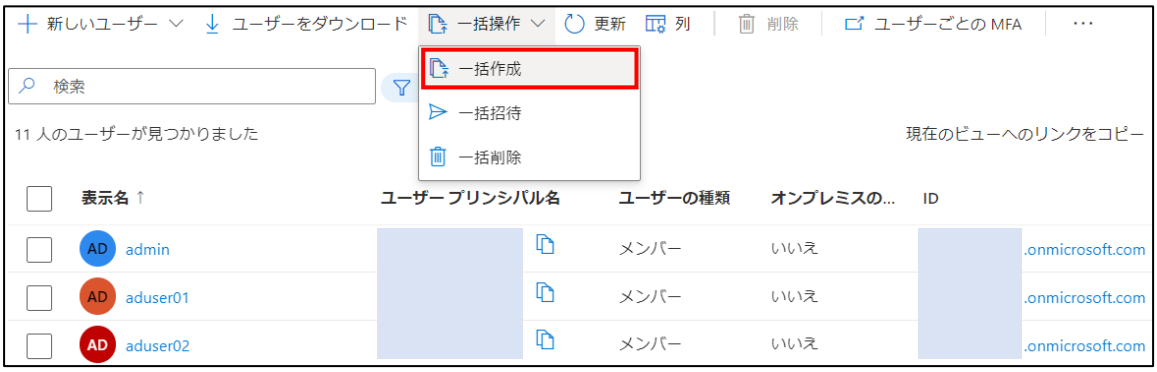
重要
- 初期パスワードは必ず各ユーザーが管理ポータル(https://portal.azure.com)にサインインして変更する必要があります。

5-2 ユーザー一括登録

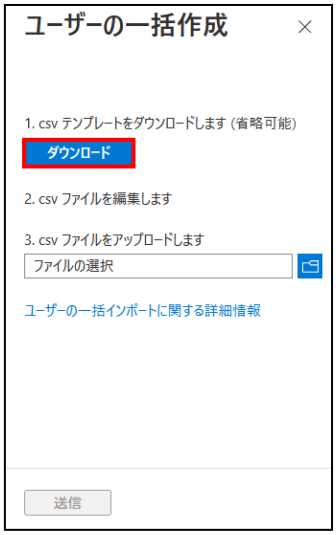
1. 概要ページで「ユーザー」を選択します。



2. 「一括作成」を選択します



3. 「ダウンロード」をクリックし、CSV テンプレートファイルをダウンロードします。

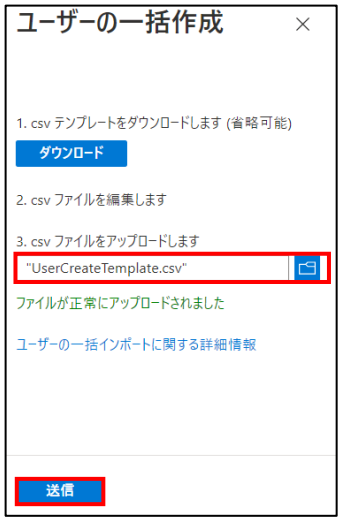


※既に取得済みの場合は省略可能。

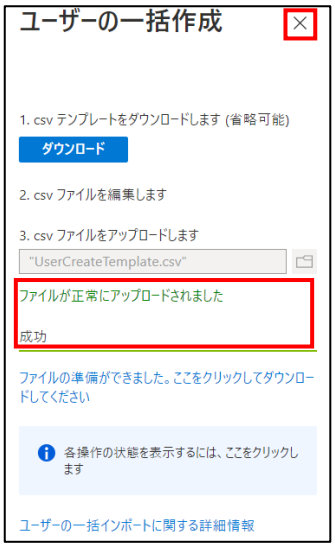
4. ダウンロードした、CSV テンプレートファイルへ必要事項を入力します。
※アップロードファイルには、バージョン番号が必要となりますので、テンプレートファイルの[1 行目、2 行目]は削除せず、3 行目以降を編集しご利用ください。

項目	値
名前 *[displayName]* 必須	任意の名前を入力
ユーザー名 *[userPrincipalName]* 必須	*Azure AD* にサインインする際に必要な識別子
初期パスワード *[passwordProfile]* 必須	パスワードを入力 （パスワードポリシーに従って設定ください）
サインインのブロック *(はい/いいえ)* *[accountEnabled]* 必須	任意に設定（デフォルトは「いいえ」）
名 *[givenName]*	任意に入力
姓 *[surname]*	任意に入力
役職 *[jobTitle]*	任意に入力
部署 *[department]*	任意に入力
利用場所 *[usageLocation]*	任意に入力
番地 *[streetAddress]*	任意に入力
都道府県 [state]	任意に入力
国/リージョン [country]	任意に入力
Office [physicalDeliveryOfficeName]	任意に入力
市区町村 [city]	任意に入力
郵便番号 [postalCode]	任意に入力
会社電話 [telephoneNumber]	任意に入力
携帯電話 [mobile]	任意に入力

5. 作成した CSV ファイルを選択し、「送信」をクリックします。



6. 「ファイルが正常にアップロードされました」と表示されたことを確認し、画面右上の「×」をクリックします。



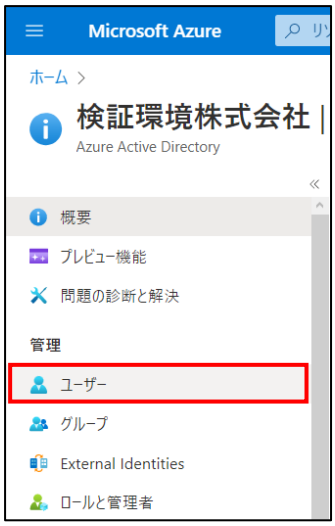
7. 「更新」をクリックし、ユーザーが登録されたことを確認します。

重要

- 初期パスワードは必ず各ユーザーが管理ポータル(https://portal.azure.com)にサインインして変更する必要があります。

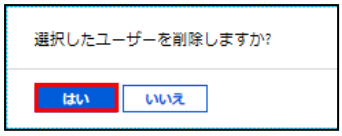
5-3 ユーザー削除

1. 概要ページで「ユーザー」を選択します。



2. 削除したいユーザーをチェックし、「削除」をクリックします。

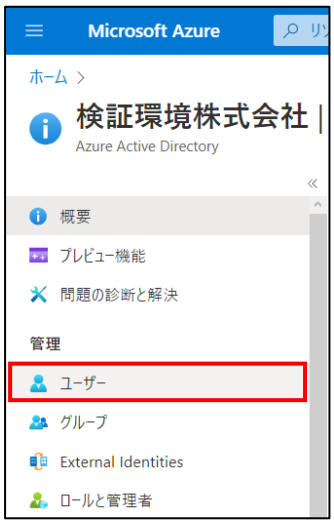
3. 確認のポップアップが表示されるので、「はい」をクリックします。



4. ユーザー一覧画面にて該当ユーザーが削除されたことを確認します。

5-4 パスワードリセット

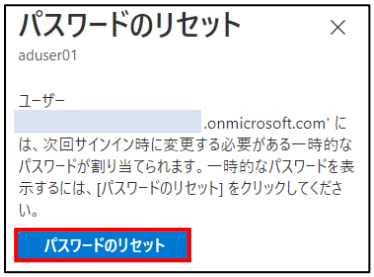
1. 概要ページで「ユーザー」を選択します。



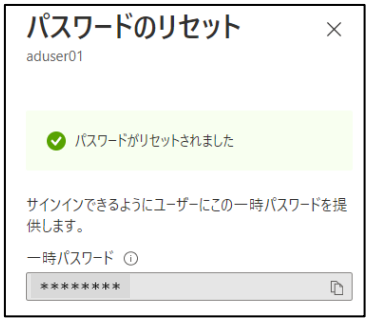
2. パスワードリセットしたいユーザーをクリックします。

3. 「パスワードのリセット」をクリックします。

4. 画面右の「パスワードリセット」をクリックします。



5. パスワードがリセットされ、一時パスワードが発行されます。



重要

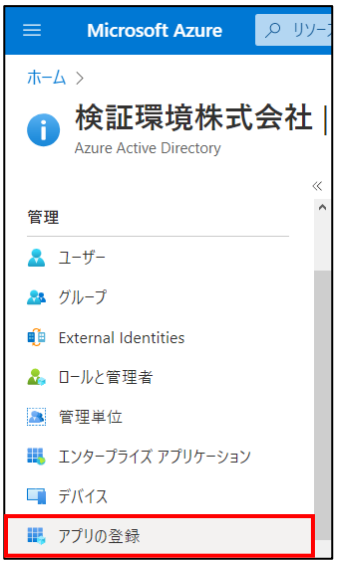
- パスワードリセット後は、必ず管理ポータル(https://portal.azure.com)にアクセスして新しいパスワードへ変更する必要があります。

6 アプリケーション登録

本手順は Azure AD サービスのユーザー認証機能を利用し、他のアプリケーションのユーザー認証と連携するための手順です。

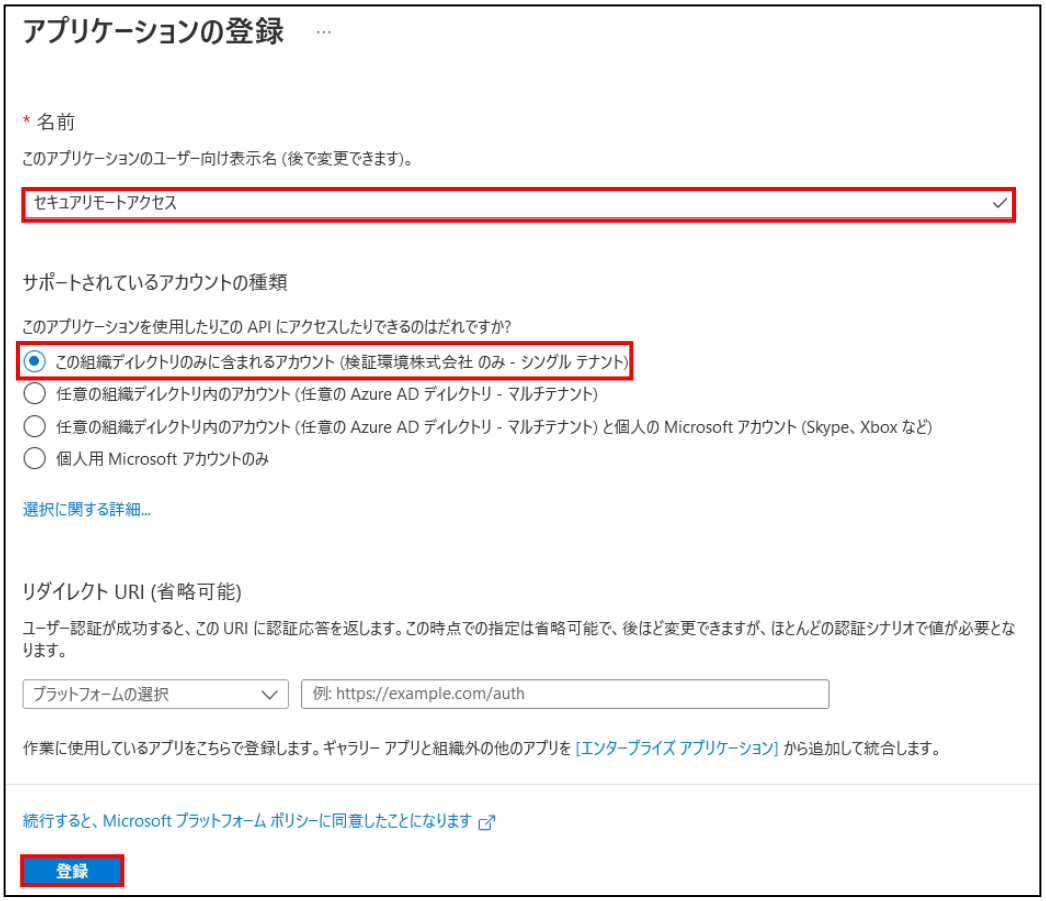
6-1 アプリケーション登録

1. 概要ページで「アプリの登録」を選択します。



2. 「新規登録」をクリックします。

3. 「名前」を入力後、「サポートされているアカウントの種類」を選択し、「登録」をクリックします。



項目	値
名前	“セキュアリモートアクセス”など任意の名前を入力
サポートされている アカウントの種類	この組織ディレクトリのみに含まれるアカウント （〇〇会社のみ-シングルテナント）

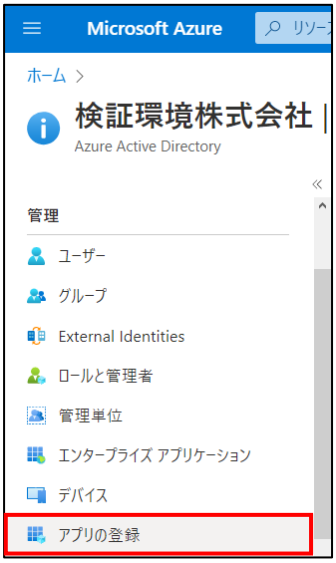
4. アプリケーション登録内容が表示されます。
「8-1 セキュアリモートアクセスの設定」で使用するため、「アプリケーション(クライアント)ID」をコピーしておいてください。(後から確認することも可能です。)

5. 画面左上の「テナント名｜アプリの登録」をクリックし、アプリケーション登録一覧ページへ移動します。

6. 「最新の情報に更新」をクリックし、作成したアプリケーションが登録されたことを確認します。

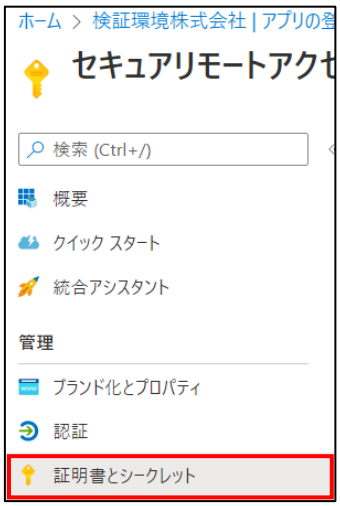
6-2　アプリケーションパスワード取得

1. 概要ページで「アプリの登録」を選択します。

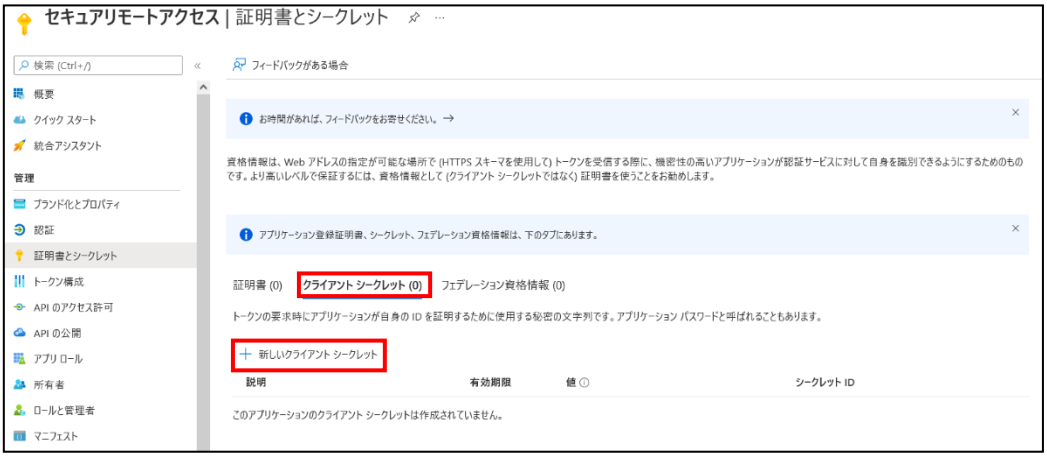


2. 対象のアプリケーションをクリックします。

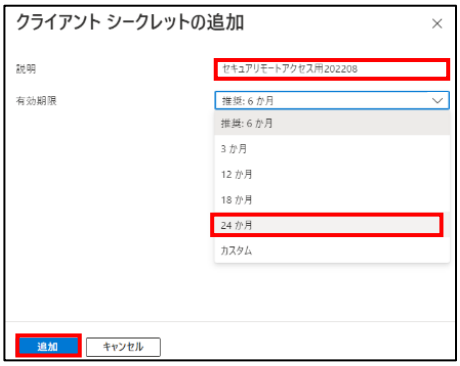
3. 左メニューの「証明書とシークレット」をクリックします。



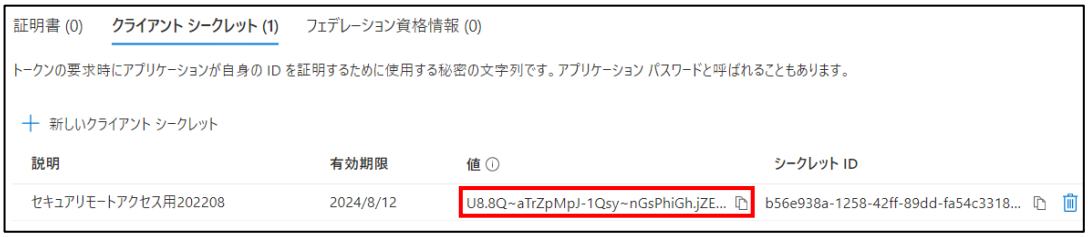
4. 「クライアントシークレット」タブから「新しいクライアントシークレット」をクリックします。



5. 「説明」を入力後、「有効期限」を選択して「追加」をクリックします。



6. 「値」の列に表示された「アプリケーションパスワード」をコピーし、メモ帳などに保存してください。



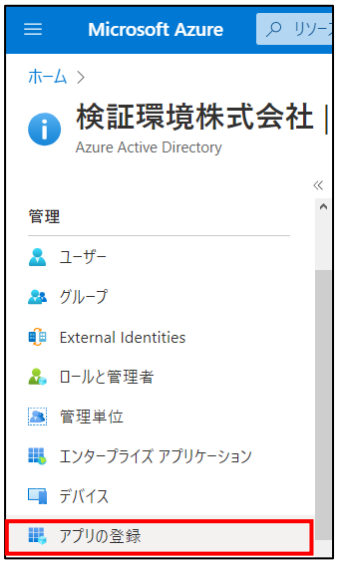
重要

- 「アプリケーションパスワード」は画面を遷移すると閲覧できなくなります。
  必ずコピーを取ってください。
  右側にあるコピーアイコンをクリックすると、クリップボードにコピーできます。

- アプリケーションパスワードの有効期限は最長 24 か月です。
  有効期限を過ぎると、セキュアリモートアクセスのログインができなくなります。
  有効期限が切れる前に、再度本手順で、新しいクライアントシークレットを追加し、「8-1 セキュアリモートアクセスの設定」の手順で「アプリケーションパスワード」を更新してください。

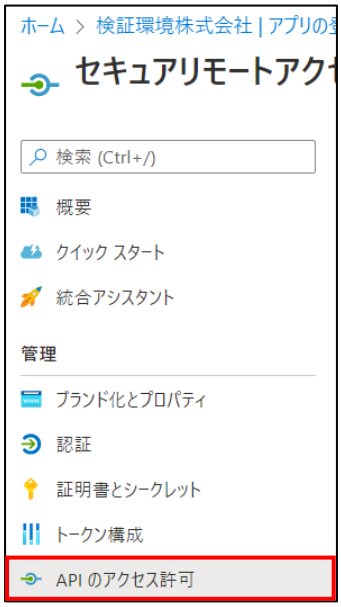
6-3　権限追加

1. 概要ページで「アプリの登録」を選択します。



2. 対象のアプリケーション(セキュアリモートアクセス)をクリックします。

3. 「API のアクセス許可」をクリックします。



4. 「アクセス許可の追加」をクリックします。

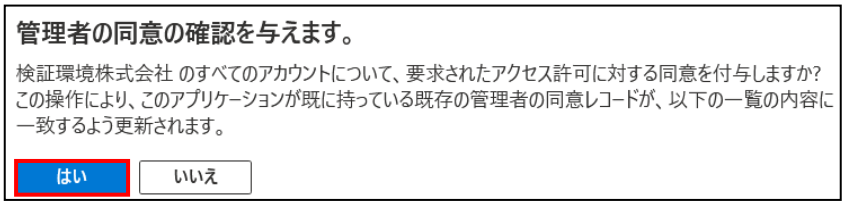
5. 「Microsoft Graph」を選択します。

6. 「アプリケーションの許可」をクリックします。

7. アクセス許可一覧の中から「User > User Read All (Read all user's full profiles)」をチェックし、「アクセス許可の追加」をクリックします。

8. 「〇〇に管理者の同意を与えます」をクリックします。

9. 「はい」をクリックします。



10. 正常に反映されたことを確認します。

7 MFA(多要素認証)設定

セキュアリモートアクセスの接続時の認証として、Azure AD の MFA（スマートフォン等を使った多要素認証）は使用できません。

セキュアリモートアクセスでは、クライアントソフトウェアの"Cisco AnyConnect"がインストールされた機器の固有な ID と Azure AD のパスワードを組み合わせて多要素認証を実現しています。

Azure AD の MFA は、セキュアリモートアクセスでは利用できないものの、設定方法によって接続時の認証に影響を与える場合があります。

以下は Azure AD の MFA の設定方法とセキュアリモートアクセスへの影響をまとめたものです。

Azure AD の MFA 設定方法

① セキュリティの既定値群
すべての Azure AD ユーザー共通で、有効か無効を選択する場合はこの設定を使用できます。
デフォルトは有効になっていますが、セキュアリモートアクセスをご利用の場合は、設定を無効へ変更してご利用ください。

② ユーザーごとの MFA
Azure AD ユーザー個別に有効、無効を設定できます。
デフォルトはすべてのユーザーで無効です。
有効にしたユーザーはセキュアリモートアクセスでの接続ができなくなりますので、「ユーザーごとの MFA」を使った MFA の有効化は行わないでください。

③ 条件付きアクセス(ユーザー数分の Azure AD Premium P1 または P2 のライセンスが必要)
Azure AD ユーザー個別に有効、無効を設定できます。
デフォルトはすべてのユーザーで無効です。
セキュアリモートアクセスを対象外のアプリケーションとして設定することで、セキュアリモートアクセスのログインと Azure AD での MFA サインインをともに利用することができます。

重要

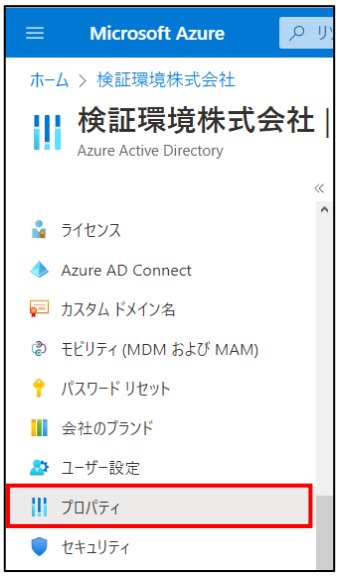
- 「②ユーザーごとの MFA」で MFA を有効化したユーザーはセキュアリモートアクセスではログインできなくなります。
  ユーザーごとに有効、無効を使い分ける場合は「③条件付きアクセス」で設定してください。
- 「③条件付きアクセス」を利用するためには、ユーザー数分の Azure AD Premium P1 または P2 のライセンスが必要になります。
  弊社で提供している「Azure AD サービス スタンダードプラン」では Azure AD Premium P1 のライセンスが 1 ユーザー分しか含まれておりませんので、「③条件付きアクセス」は設定できません。
  「③条件付きアクセス」を利用する場合は「Azure AD サービス プレミアムプラン」で人数分のライセンスをご購入ください。
  「③条件付きアクセス」を利用する場合は、「①セキュリティの既定値群」を無効化してください。

ここでは、「①セキュリティの既定値群」と「③条件付きアクセス」の設定方法を記載しています。

7-1　セキュリティの規定値群の無効化

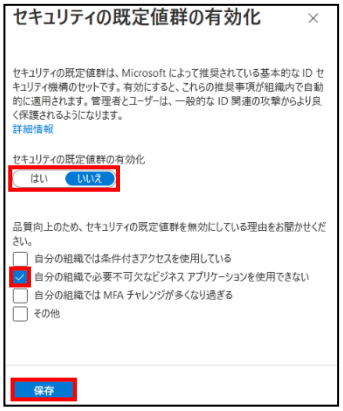
Azure AD にサインインする際に、すべてのユーザーで MFA を無効にします。
一部のユーザーのみ MFA を有効にする場合は、本手順でセキュリティの規定値群を無効化したうえで、「7-2 条件付きアクセスの除外ルール設定」の手順へお進みください。

1. 概要ページで「プロパティ」を選択します。



2. 画面下部「セキュリティの規定値群の管理」をクリックします。

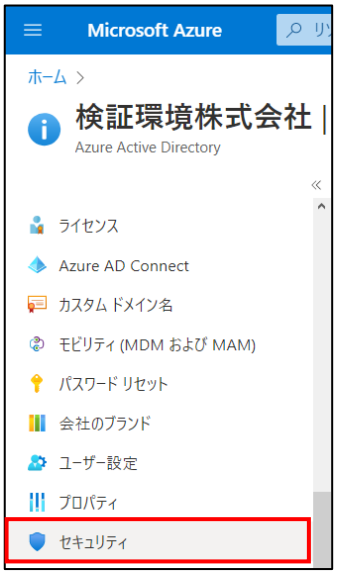
3. [セキュリティの規定値群の有効化]から「いいえ」を選択し、「保存」をクリックします。
※[品質向上のため、セキュリティの規定値群を無効にしている理由]から、お客さま任意の理由を選択ください。



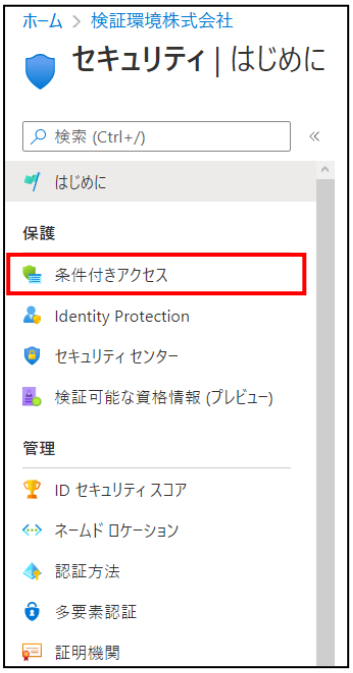
7-2　条件付きアクセスの除外ルール設定

条件付きアクセスを使って MFA の設定を行う場合、事前に「7-1 セキュリティの規定値群の無効化」を実施してください。
「セキュリティの規定値群」と「条件付きアクセス」の両方で MFA の有効化を行うことは、マイクロソフトで推奨されていません。

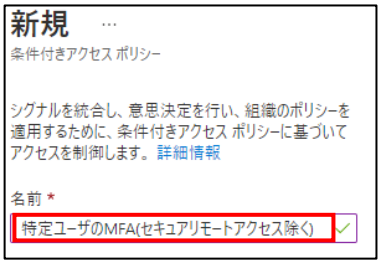
1. 概要ページで「セキュリティ」を選択します。



2. 画面左の「条件付きアクセス」を選択します。

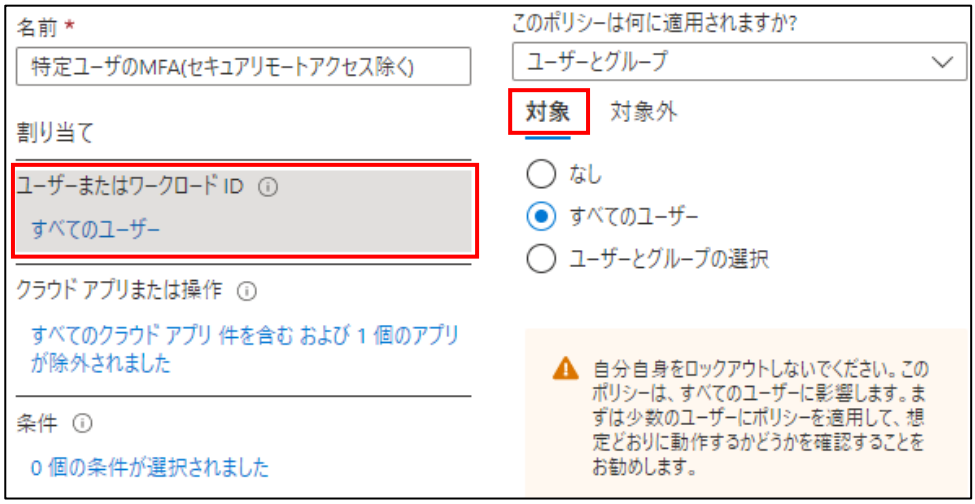


3. 新規にポリシーを作る場合には、「＋新しいポリシー」をクリックして名前を入力します。

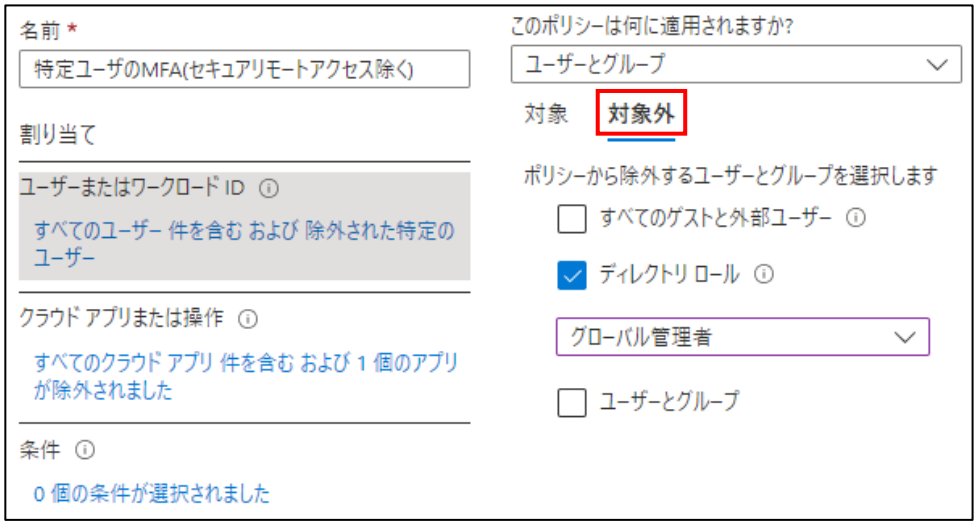


既存のポリシーを編集する場合は、対象の既存ポリシー名を選択します。

4. 「ユーザーまたはワークロード ID」を選択し、対象となるユーザーやグループを選択します。



5. 対象外のロールまたはユーザー、グループを選択します。



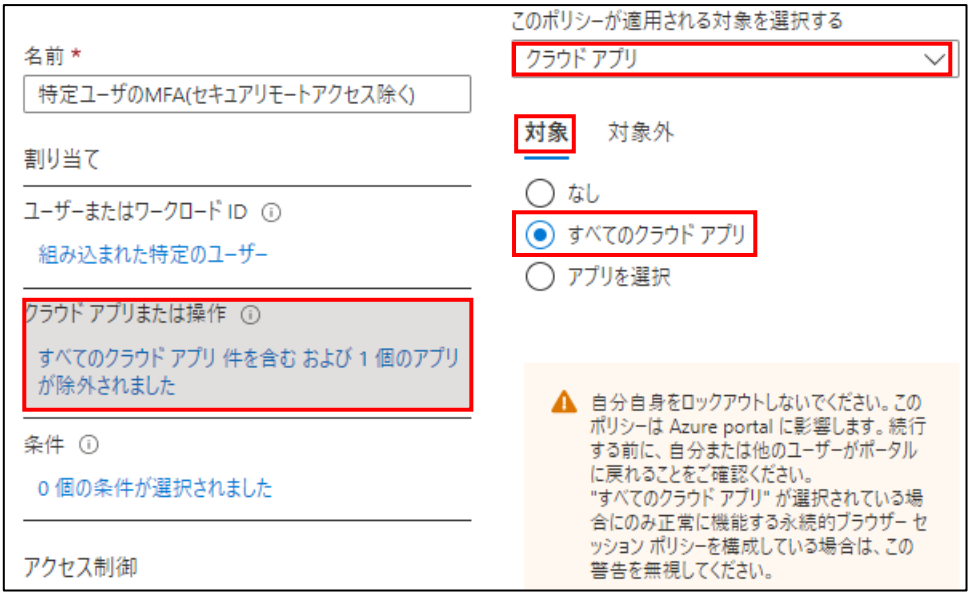
重要

- グローバル管理者が一つしか登録されていない初期状態で、ログインアカウントに対して、MFA を有効にすると、何らかのミスがあった時に復旧が困難になるため、初期状態では対象外とするか、緊急用アカウントなどを作成した後、有効にしてください。
- テナント全体でアカウントがロックアウトされることを防ぐために、マイクロソフトでは、緊急アクセス用アカウントを MFA の対象外とすることを推奨しています。

  参考 URL
  条件付きアクセス:すべてのユーザーに対して MFA を必須にする
  https://docs.microsoft.com/ja-jp/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa

  Azure AD で緊急アクセス用管理者アカウントを管理する
  https://docs.microsoft.com/ja-jp/azure/active-directory/roles/security-emergency-access

6. 「クラウドアプリまたは操作」を選択し、対象となるクラウドアプリを選択します。



7. 「対象外」タブから「6-1 アプリケーション登録」で追加した「セキュアリモートアクセス」を選択し、を対象外として登録します。

8. 「アクセス制御」を選択し、「アクセス権の付与」から「多要素認証を要求する」にチェックを入れ、「選択」をクリックします。
その後、ポリシーの有効化を「オン」にして、「作成」ボタンをクリックするとポリシーが作成されます。

8 セキュアリモートアクセス認証設定

本手順は Azure AD サービスとセキュアリモートアクセスとを連携するための手順であり、セキュアリモートアクセスのマネージメントツールでの手順となります。

8-1 セキュアリモートアクセスの設定

1. マネージメントツールにログインします。

   https://acmt.ravpn.bit-drive.ne.jp

2. 「全体設定」をクリックします。

3. 認証タイプにて「Azure AD」を選択します。

4. 以下の通り設定を入力し、「設定」をクリックします。

項目	説明	参考ページ
アプリケーション ID	Azure AD のアプリ登録した際に払い出される ID	6-1 アプリケーション登録
アプリケーション パスワード	Azure AD のアプリ登録より作成したクライアントシークレットのアプリケーションパスワード	6-2 アプリケーションパスワード取得
ドメイン名	Azure AD で使用中のドメイン名	―
管理者ユーザー名	Azure AD の管理者アカウント ※@以降は不要です。	―
管理者パスワード	Azure AD の管理者パスワード	―

重要

- 「アプリケーションパスワード」の有効期限は最長 24 か月です。
有効期限を過ぎると、セキュアリモートアクセスのログインができなくなります。
有効期限が切れる前に、「6-2 アプリケーションパスワード取得」の手順にて、新しいクライアントシークレットを追加し、セキュアリモーアクセスのマネージメントツールから「アプリケーションパスワード」を更新してください。
- 「管理者ユーザー名」で入力する管理者アカウントは Azure AD 上でグローバル管理者権限を持ったアカウントを使用してください。
- この管理者アカウントで MFA を使用する場合は、「7-2 条件付きアクセスの除外ルール設定」を参考に、セキュアリモートアクセスのアプリケーションを MFA から除外するように設定してください。