

Microsoft Entra ID サービス ユーザガイド

[システム管理者さま向け]

2024年9月2日 Version 4.0

ソニービズネットワークス株式会社

著作権情報

本ドキュメントは、著作権法で保護された著作物で、その全部または一部を許可なく複製したり複製物を配布したり、あるいは他のコンピュータ用に変換したり、他の言語に翻訳すると、著作権の侵害となります。

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。

商標表示

記載されている会社名および製品名は、各社の商標または登録商標です。

目次

1. はじめに	4
2. 設定の流れ.....	5
3. 注意事項	6
4. Microsoft Entra ID へのサインイン	7
4-1 Microsoft Entra 管理センターにアクセス	7
5. ユーザー登録.....	9
5-1 ユーザー追加.....	9
5-2 ユーザー一括登録	12
5-3 ユーザー削除.....	15
5-4 パスワードリセット	16
6. アプリケーション登録.....	18
6-1 アプリケーション登録	18
6-2 アプリケーションパスワード取得	21
6-3 権限追加.....	23
7. MFA(多要素認証)設定	26
7-1 セキュリティの規定値群の無効化	27
7-2 条件付きアクセスの除外ルール設定	29
8. セキュアリモートアクセス認証設定.....	35
8-1 セキュアリモートアクセスの設定	35

1 はじめに

1-1 本マニュアルについて

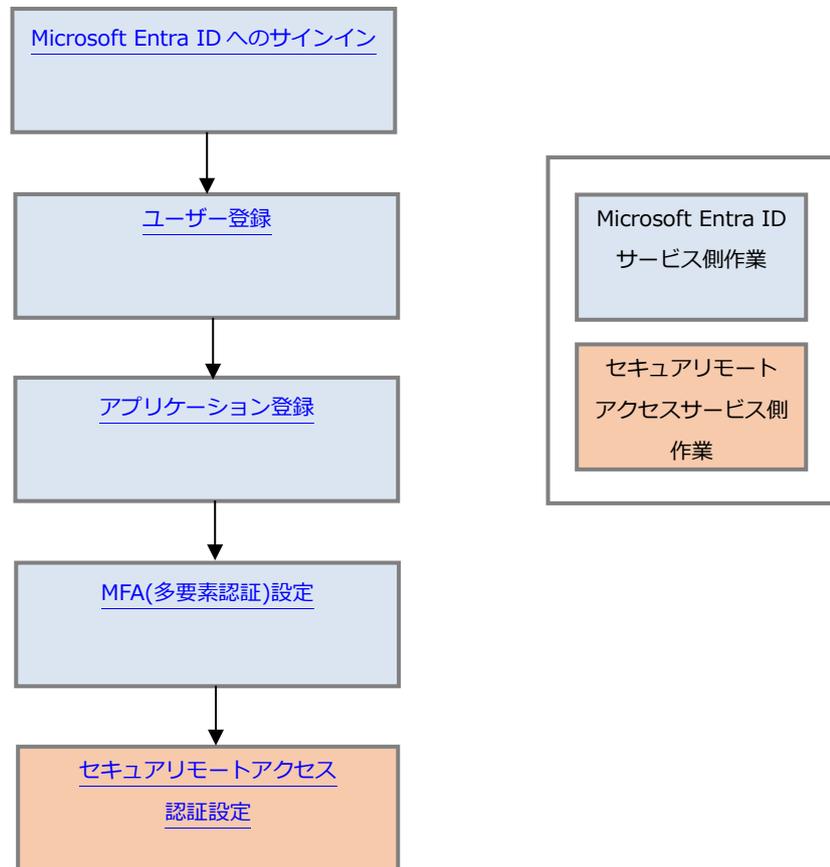
このたびは、Microsoft Entra ID サービスをご契約いただき、ありがとうございます。

本マニュアルは、管理者様向けに Microsoft Entra ID 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

Microsoft Entra ID 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。

- Microsoft Entra ID 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 Microsoft Entra ID へのサインイン

Microsoft Entra ID 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-Microsoft Entra ID-AD*****-**.pdf)をご準備ください。

※旧称：登録内容通知(User-Parameters- AzureAD -AD*****-**.pdf)

4-1 Microsoft Entra 管理センターにアクセス

1. Microsoft Entra 管理センターにアクセスします。

URL : <https://entra.microsoft.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 Microsoft Entra 管理センター (ホーム)画面に遷移します。



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。

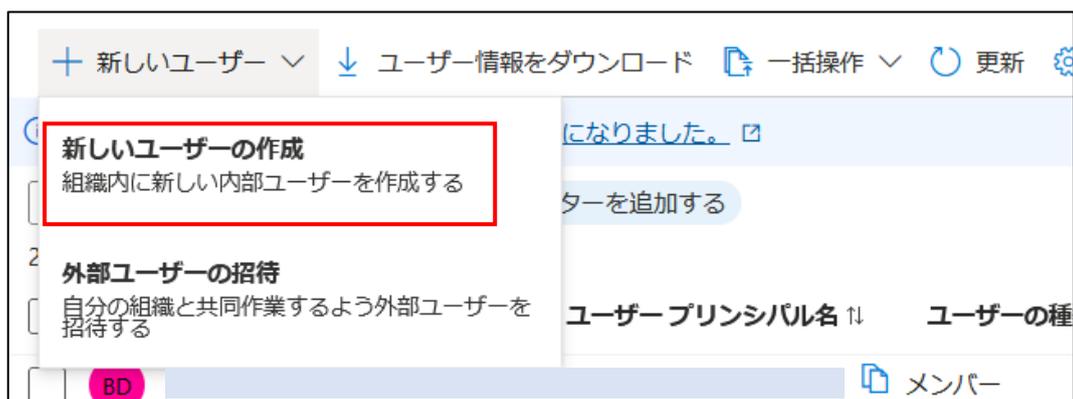
CSVファイルを使ったユーザー一括登録を行なう場合は、[\[5-2ユーザー一括登録\]](#)をご参照ください。

5-1 ユーザー追加

1. IDメニューで「ユーザー」タブから「すべてのユーザー」を選択します。



2. 「新しいユーザーの作成」を選択します。



3. 「ユーザープリンシパル名」、「メールニックネーム名」、「パスワード」を入力して、「レビューと作成」をクリックします。

新しいユーザーの作成

組織内に新しい内部ユーザーを作成する

基本 プロパティ 割り当て 確認と作成

組織内に新しいユーザーを作成します。このユーザーは alice@contoso.com などのユーザー名になります。 [詳細情報](#)

ID

ユーザープリンシパル名* @ [ドメインが一覧にありません](#)

メールニックネーム* ユーザープリンシパル名から受け継ぐ

表示名

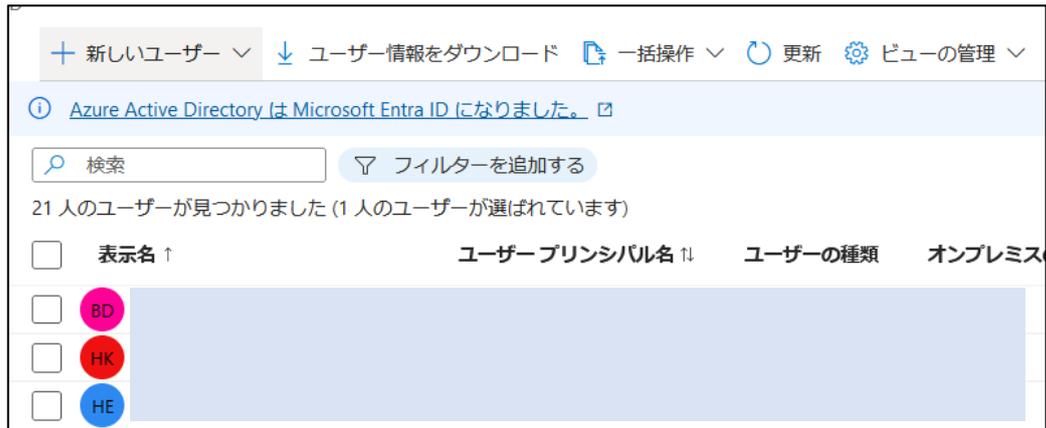
パスワード* パスワードの自動生成

有効なアカウント①

レビューと作成
< 前へ
次: プロパティ >

項目	値
ユーザープリンシパル名	Microsoft Entra ID にサインインする際に必要な識別子
メールニックネーム名	任意のメールニックネームを入力 ※[ユーザープリンシパル名から受け継ぐ]が「オン」の場合は入力不要。(デフォルトは「オン」)
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)
表示名	任意に設定
有効なアカウント	任意に設定 (デフォルトは「オン」) ※オフにした場合、このユーザーのサインインはブロックされます。これはユーザーの作成後に更新できます。

4. ユーザーが登録されたことを確認します。



+ 新しいユーザー ▾ ↓ ユーザー情報をダウンロード 📄 一括操作 ▾ 🔄 更新 ⚙️ ビューの管理 ▾

ⓘ Azure Active Directory は Microsoft Entra ID になりました。 ☒

21 人のユーザーが見つかりました (1 人のユーザーが選ばれています)

<input type="checkbox"/>	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
<input type="checkbox"/>	BD			
<input type="checkbox"/>	HK			
<input type="checkbox"/>	HE			

重要

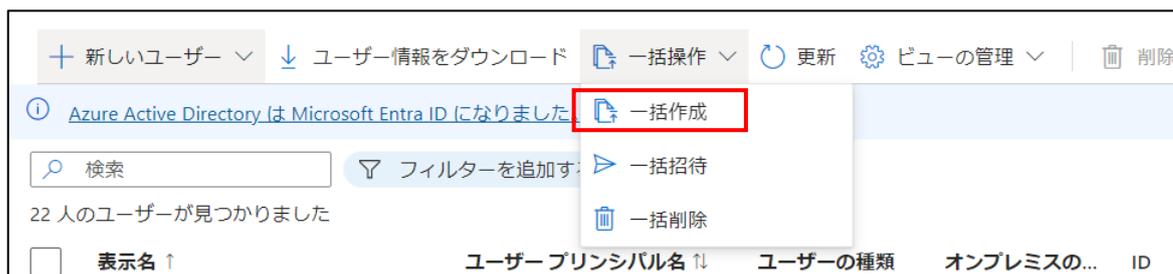
- ここで設定されるパスワードは一時パスワードとなります。初期パスワードは必ず各ユーザーが Microsoft Entra 管理センター (<https://entra.microsoft.com>) にサインインして変更する必要があります。

5-2 ユーザー一括登録

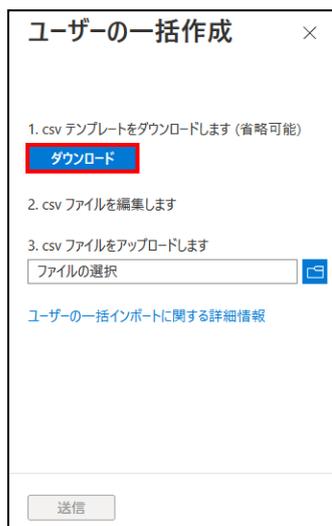
1. IDメニューで「ユーザー」タブから「すべてのユーザー」を選択します。



2. 「一括操作」タブから「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	Microsoft Entra ID 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。

ユーザーの一括作成

1. csv テンプレートをダウンロードします (省略可能)
ダウンロード

2. csv ファイルを編集します

3. csv ファイルをアップロードします
"UserCreateTemplate.csv" [選択]

ファイルが正常にアップロードされました

ユーザーの一括インポートに関する詳細情報

送信

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。

ユーザーの一括作成

1. csv テンプレートをダウンロードします (省略可能)
ダウンロード

2. csv ファイルを編集します

3. csv ファイルをアップロードします
"UserCreateTemplate.csv" [選択]

ファイルが正常にアップロードされました

成功

ファイルの準備ができました。ここをクリックしてダウンロードしてください

各操作の状態を表示するには、ここをクリックします

ユーザーの一括インポートに関する詳細情報

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。

+ 新しいユーザー ▾ | ↓ ユーザー情報をダウンロード | 一括操作 ▾ | 更新 | ビューの管理 ▾

Azure Active Directory は Microsoft Entra ID になりました。

検索 | フィルターを追加する

21 人のユーザーが見つかりました (1 人のユーザーが選ばれています)

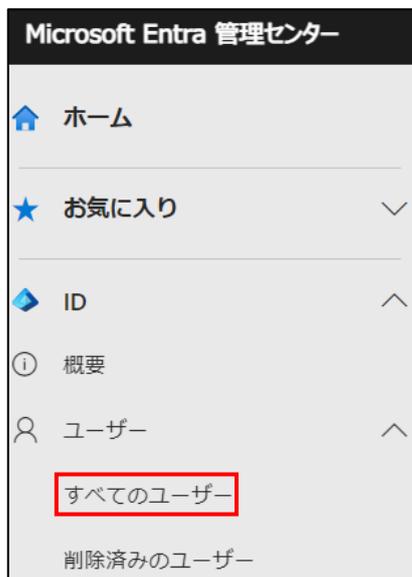
<input type="checkbox"/>	表示名 ↑	ユーザープリンシパル名 ↓	ユーザーの種類	オンプレミス
<input type="checkbox"/>	BD			
<input type="checkbox"/>	HK			
<input type="checkbox"/>	HE			

重要

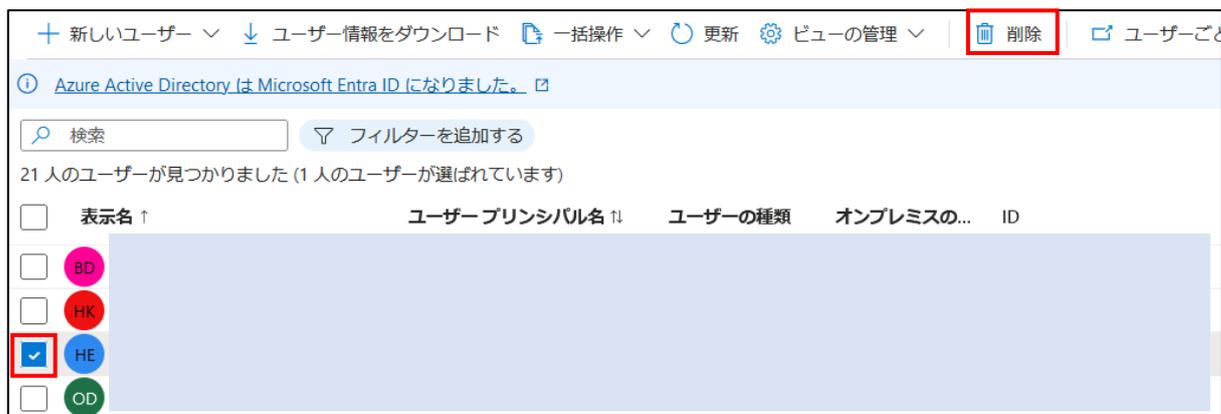
- ここで設定されるパスワードは一時パスワードとなります。初期パスワードは必ず各ユーザーが Microsoft Entra 管理センター (<https://entra.microsoft.com>) にサインインして変更する必要があります。

5-3 ユーザー削除

1. IDメニューで「ユーザー」タブから「すべてのユーザー」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。



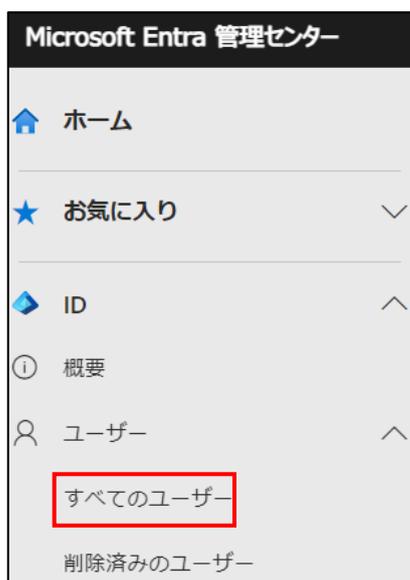
3. 確認のポップアップが表示されるので、「OK」をクリックします。



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

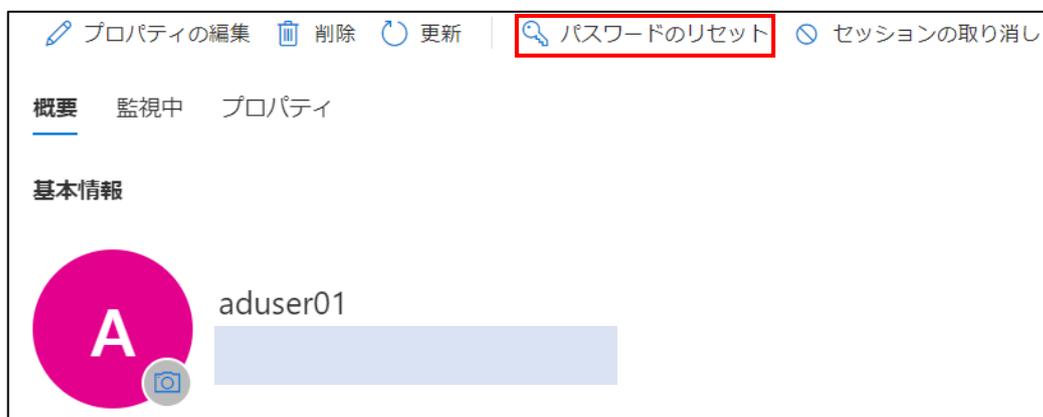
1. IDメニューで「ユーザー」タブから「すべてのユーザー」を選択します。



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

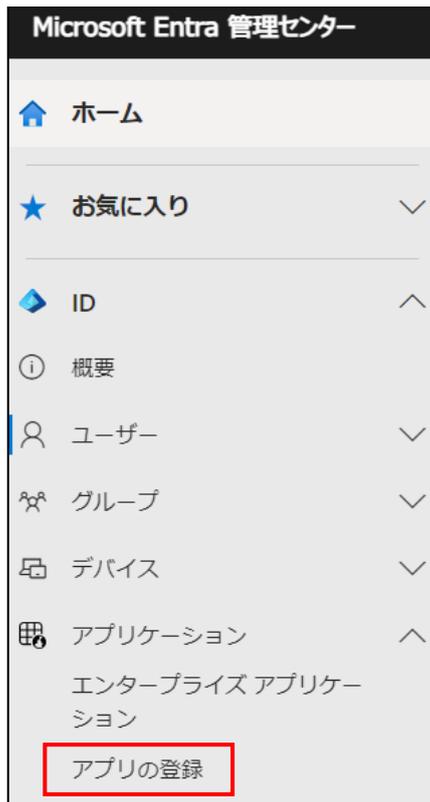
- ここで設定されるパスワードは一時パスワードとなります。パスワードリセット後は、必ず Microsoft Entra 管理センター (<https://entra.microsoft.com>) にアクセスして新しいパスワードへ変更する必要があります。

6 アプリケーション登録

本手順は Microsoft Entra ID 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. ID メニューで「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。

アプリケーションの登録 ...

*** 名前**
このアプリケーションのユーザー向け表示名 (後で変更できません)。

セキュアリモートアクセス ✓

サポートされているアカウントの種類
このアプリケーションを使用したりこの API にアクセスしたりできるのはだれですか?

この組織ディレクトリのみに含まれるアカウント (検証環境株式会社のみ - シングル テナント)

任意の組織ディレクトリ内のアカウント (任意の Azure AD ディレクトリ - マルチテナント)
 任意の組織ディレクトリ内のアカウント (任意の Azure AD ディレクトリ - マルチテナント) と個人の Microsoft アカウント (Skype、Xbox など)
 個人用 Microsoft アカウントのみ

[選択に関する詳細...](#)

リダイレクト URI (省略可能)
ユーザー認証が成功すると、この URI に認証応答を返します。この時点での指定は省略可能で、後ほど変更できますが、ほとんどの認証シナリオで値が必要となります。

プラットフォームの選択 ▼

例: https://example.com/auth

作業に使用しているアプリをこちらで登録します。ギャラリー アプリと組織外の他のアプリを [\[エンタープライズ アプリケーション\]](#) から追加して統合します。

[続行すると、Microsoft プラットフォーム ポリシーに同意したことになります](#)

登録

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。)

セキュアリモートアクセス
✱ ...

削除
エンドポイント
プレビュー機能

概要

クイック スタート

統合アシスタント

管理

ブランド化とプロパティ

認証

証明書とシークレット

トークン構成

API のアクセス許可

少しお時間があれば、Microsoft ID プラットフォーム (以前の)

基本

表示名
セキュアリモートアクセス

アプリケーション (クライアント) ID

オブジェクト ID

ディレクトリ (テナント) ID

サポートされているアカウントの種類

5. 画面左上の「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

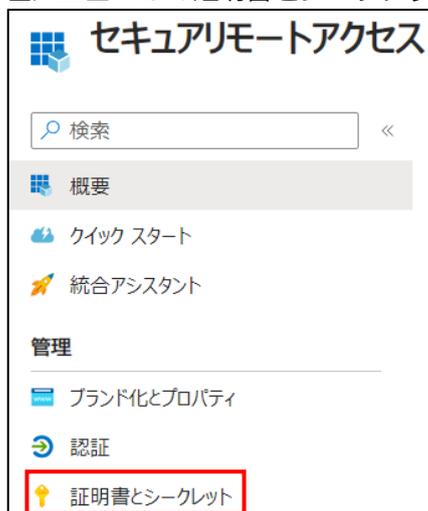
1. ID メニューで「アプリの登録」を選択します。



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。

セキュアリモートアクセス | 証明書とシークレット

検索 (Ctrl+F) << フィードバックがある場合

お時間があれば、フィードバックをお寄せください。 →

資格情報は、Web アドレスの指定が可能な場所で (HTTPS スキーマを使用して) トークンを受信する際に、機密性の高いアプリケーションが認証サービスに対して自身を識別できるようにするためのものです。より高いレベルで保証するには、資格情報として (クライアントシークレットではなく) 証明書を使うことをお勧めします。

アプリケーション登録証明書、シークレット、フェデレーション資格情報は、下のタブにあります。

証明書 (0) **クライアントシークレット (0)** フェデレーション資格情報 (0)

トークンの要求時にアプリケーションが自身の ID を証明するために使用する秘密の文字列です。アプリケーション パスワードと呼ばれることもあります。

+ 新しいクライアントシークレット

説明	有効期限	値	シークレット ID
このアプリケーションのクライアント シークレットは作成されていません。			

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。

クライアント シークレットの追加

説明

有効期限

推奨: 180 日 (6 か月)

90 日 (3 か月)

365 日 (12 か月)

545 日 (18 か月)

730 日 (24 か月)

カスタム

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。

証明書 (0) クライアント シークレット (1) フェデレーション資格情報 (0)

トークンの要求時にアプリケーションが自身の ID を証明するために使用する秘密の文字列です。アプリケーション パスワードと呼ばれることもあります。

+ 新しいクライアント シークレット

説明	有効期限	値	シークレット ID
セキュアリモートアクセス用202208	2024/8/12	U8.8Q~aTrZpMpJ-1Qsy~nGsPhiGhJZE...	b56e938a-1258-42ff-89dd-fa54c3318...

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。

説明	有効期限	値
セキュアリモートアクセス用202208	2024/8/12	U8.8Q~aTrZpMpJ-1Qsy~nGsPhiGhJZE...

- アプリケーションパスワードの有効期限は最長 730 日 (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

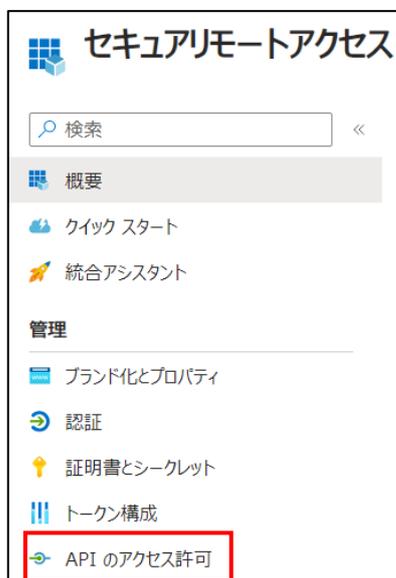
1. ID メニューで「アプリの登録」を選択します。



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。

最新の情報に更新 | フィードバックがある場合

⚠ アプリケーションに対するアクセス許可を編集しています。ユーザーは、既に同意したことがある場合でも同意が必要になります。

📘 "管理者の同意が必要" 列には、組織の既定値が表示されます。ただし、ユーザーの同意は、アクセス許可、ユーザー、アプリごとにカスタマイズできます。この列には、ご自分の組織や、このアプリが使用される組織の値が反映されていない場合があります。 [詳細情報](#)

構成されたアクセス許可

アプリケーションは、同意のプロセスの一環としてユーザーが管理者からアクセス許可が付与されている場合、API を呼び出すことが承認されます。構成されたアクセス許可の一覧には、アプリケーションに必要なすべてのアクセス許可を含める必要があります。 [アクセス許可と同意に関する詳細情報](#)

+ **アクセス許可の追加** ✓ 検証環境株式会社 に管理者の同意を与えます

API / アクセス許可の名前	種類	説明	管理者の同意が必要	状態

5. 「Microsoft Graph」を選択します。

API アクセス許可の要求

API を選択します

Microsoft API 所属する組織で使用している API 自分の API

よく使用される Microsoft API

 **Microsoft Graph**

Office 365、Enterprise Mobility + Security、Windows 10 の大量のデータを活用しましょう。Microsoft Entra ID、Excel、Intune、Outlook/Exchange、OneDrive、OneNote、SharePoint、Planner などに単一エンドポイント経由でアクセスできます。

 **Azure Communication Services**

Microsoft Teams で使用されるのと同じセキュリティで保護された CPaaS プラットフォームを使用した豊富なコミュニケーション エクスペリエンス

 **Azure Data Catalog**

データ資産を登録、注釈、検索するための Data Catalog リソースへのプログラムによるアクセス

 **Azure Rights Management Services**

検証済みのユーザーに、保護されたコンテンツの読み取りと書き込みを許可します

6. 「アプリケーションの許可」をクリックします。

API アクセス許可の要求

すべての API

 Microsoft Graph
<https://graph.microsoft.com/> [ドキュメント](#)

アプリケーションに必要なアクセス許可の種類

委任されたアクセス許可

アプリケーションは、サインインしたユーザーとして API にアクセスする必要があります。

アプリケーションの許可

アプリケーションは、サインインしたユーザーなしで、バックグラウンドサービスまたはデーモンとして実行されます。

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。

▼ User (1)

<input type="checkbox"/>	User.Export.All ⓘ Export user's data	はい
<input type="checkbox"/>	User.Invite.All ⓘ Invite guest users to the organization	はい
<input type="checkbox"/>	User.ManageIdentities.All ⓘ Manage all users' identities	はい
<input checked="" type="checkbox"/>	User.Read.All ⓘ Read all users' full profiles	はい
<input type="checkbox"/>	User.ReadWrite.All ⓘ Read and write all users' full profiles	はい

アクセス許可の追加
破壊

8. 「〇〇に管理者の同意を与えます」をクリックします。

構成されたアクセス許可

アプリケーションは、同意のプロセスの一環としてユーザーが管理者からアクセス許可が付与されている場合、API を呼び出すことが承認されます。アプリケーションに必要なすべてのアクセス許可を含める必要があります。[アクセス許可と同意に関する詳細情報](#)

+ アクセス許可の追加

✓ 検証環境株式会社 に管理者の同意を与えます

API / アクセス許可の名前	種類	説明	管理者の同意が必要
▼ Microsoft Graph (2)			
User.Read	委任済み	Sign in and read user profile	いいえ
User.Read.All	アプリケー...	Read all users' full profiles	はい

9. 「はい」をクリックします。

管理者の同意の確認を与えます。

検証環境株式会社 のすべてのアカウントについて、要求されたアクセス許可に対する同意を付与しますか？この操作により、このアプリケーションが既に持っている既存の管理者の同意レコードが、以下の一覧の内容に一致するよう更新されます。

はい
いいえ

10. 正常に反映されたことを確認します。

✓

同意する

同意の付与に成功しました

×

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、Microsoft Entra ID 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 Microsoft Entra ID のパスワードを組み合わせることで多要素認証を実現しています。

Microsoft Entra ID 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 Microsoft Entra ID 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。

Microsoft Entra ID の MFA 設定方法

① セキュリティの既定値群

すべての Microsoft Entra ID 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

Microsoft Entra ID 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 Microsoft Entra ID P1 または P2 のライセンスが必要)

Microsoft Entra ID 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 Microsoft Entra ID 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

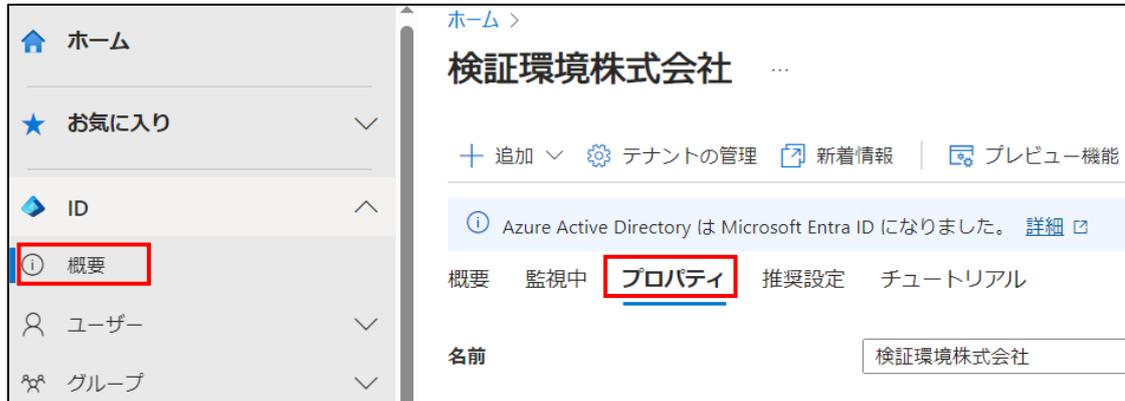
- 「②ユーザーごとの MFA」で MFA を有効化したユーザーはセキュアリモートアクセスではログインできなくなります。
ユーザーごとに有効、無効を使い分ける場合は「③条件付きアクセス」で設定してください。
- 「③条件付きアクセス」を利用するためには、ユーザー数分の Microsoft Entra ID P1 または P2 のライセンスが必要になります。
弊社で提供している「Microsoft Entra ID サービス スタンダードプラン」では Microsoft Entra ID P1 のライセンスが 1 ユーザー分しか含まれておりませんので、「③条件付きアクセス」は設定できません。
「③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

Microsoft Entra ID 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. ID メニューから「概要」を選択し、「プロパティ」を参照します。



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]から「無効(推奨しません)」を選択し、「保存」をクリックします。
 ※[無効にする理由]から、お客さま任意の理由を選択ください。

セキュリティの規定値群 ×

セキュリティの規定値群

無効 (推奨しません) ▼

⚠ セキュリティの規定値群が無効になっている場合、組織は ID 関連の一般的な攻撃に対して脆弱です。

多要素認証を使用すると、アカウント侵害の 99.9% を停止させることができます。これは、セキュリティの規定値群によって提供される機能です。

Microsoft のセキュリティ チームによると、セキュリティの規定値群を有効にすることで侵害率に 80% の低下が見られます。

無効にする理由 *

このフィードバックは Microsoft の製品とサービスの改善に使用されま
 ず。 [プライバシーに関する声明の表示](#)

自分の組織でアプリまたはデバイスを使用できない

自分の組織では条件付きアクセスを使用している

⚠ セキュリティの規定値群を無効にすると、ID を保護するために条件付きアクセス ポリシーを作成するまで、組織は保護されません。 [詳細情報](#)

多要素認証のサインアップ要求が多くなり過ぎる

サインイン情報の多要素認証チャレンジが多くなり過ぎる

その他

保存

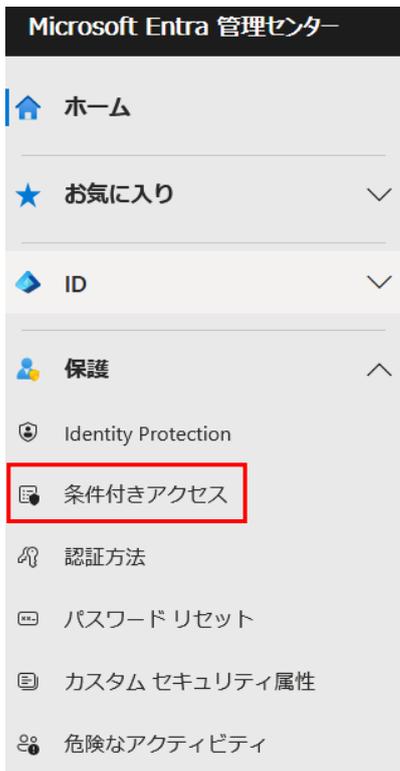
キャンセル

7-2 条件付きアクセスの除外ルール設定

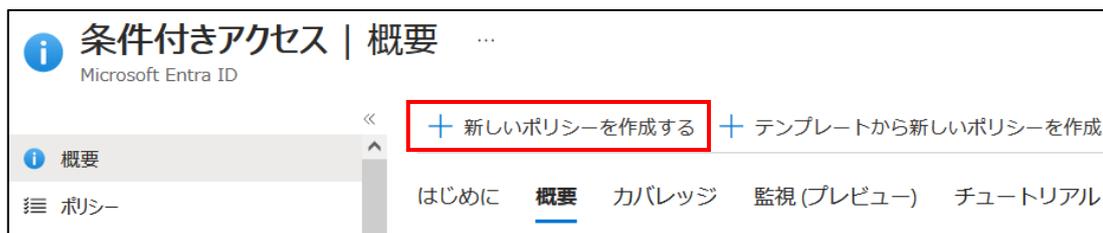
条件付きアクセスを使って MFA の設定を行う場合、事前に「[7-1 セキュリティの規定値群の無効化](#)」を実施してください。

「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. 保護メニューから「条件付きアクセス」を選択します。



2. 新規にポリシーを作る場合には、「+新しいポリシー」をクリックします。



3. 各設定項目を入力し、「作成」ボタンをクリックします。

- 名前
- 割り当てユーザー
 - ・対象
 - ・対象外
- ポリシーの有効化を「オン」を選択

新規 ...

条件付きアクセス ポリシー

シグナルを統合し、意思決定を行い、組織のポリシーを適用するために、条件付きアクセス ポリシーに基づいてアクセスを制御します。 [詳細情報](#)

ユーザーとグループ、ワークロード ID、ディレクトリ ロール、外部ゲストなど、ポリシーを適用するユーザーに基づいてアクセスを制御します。 [詳細情報](#)

名前 *

特定ユーザーのMFA(セキュアリモートアクセス除く) ✓

割り当て

ユーザー ①

すべてのユーザー

対象 対象外

なし

すべてのユーザー

ユーザーとグループの選択

⚠ 自分自身をロックアウトしないでください。このポリシーは、すべてのユーザーに影響します。まずは少数のユーザーにポリシーを適用して、想定どおりに動作するかどうかを確認することをお勧めします。 [詳細情報](#)

ターゲット リソース ①

ターゲット リソースが選択されていません

条件 ①

0 個の条件が選択されました

アクセス制御

許可 ①

ポリシーの有効化

レポート専用 オン オフ

作成

4. 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。

条件付きアクセス | ポリシー

Microsoft Entra ID

概要
ポリシー
 分析情報レポート
 問題の診断と解決

管理
 ネームド ロケーション
 カスタム コントロール (プレビュー)
 利用規約
 認証コンテキスト
 認証強度
 クラシック ポリシー

監視
 サインイン ログ

新しいポリシー + 新しいポリシーをテンプレートから + ポリシー ファイルのアップロード What If 最新の情報に更新

前のビューに戻るには、ここをクリックするか [プレビュー機能] を使用して、拡張されたポリシー リスト機能を無効にし、タブを更新してください。

ポリシーのフィルター処理の新しいエクスペリエンスをお試しください。割り当て、条件、アクセスの制御でポリシーをフィルター処理できるようになりました。

すべてのポリシー Microsoft マネージド ポリシー

0 (全 2 項目中)

合計 2
 検索 フィルター追加

2 個のポリシーのうち 2 個が見つかりました

ポリシー名	状態	作成日	更新日
特定ユーザーのMFA(セキュアリモートアクセス除く)	オン		
	オン		

5. 「ユーザー」を選択し、対象となるユーザーやグループを選択します。

特定ユーザーのMFA(セキュアリモートアクセス除く)

条件付きアクセス ポリシー

削除 ポリシー情報の表示

シグナルを統合し、意思決定を行い、組織のポリシーを適用するために、条件付きアクセス ポリシーに基づいてアクセスを制御します。 [詳細情報](#)

ユーザーとグループ、ワークロード ID、ディレクトリ ロール、外部ゲストなど、ポリシーを適用するユーザーに基づいてアクセスを制御します。 [詳細情報](#)

名前 *

特定ユーザーのMFA(セキュアリモートアクセス除く)

割り当て

ユーザー ①

組み込まれた特定のユーザー および 除外された特定のユーザー

ターゲット リソース ①

すべてのクラウド アプリ 件を含む および 1 個のアプリが除外されました

条件 ①

0 個の条件が選択されました

対象 対象外

なし

すべてのユーザー

ユーザーとグループの選択

ゲストまたは外部ユーザー ①

ディレクトリ ロール ①

ユーザーとグループ

選択

1 ユーザー

6. 対象外のロールまたはユーザー、グループを選択します。

特定ユーザのMFA(セキュアリモートアクセス除く) ...

条件付きアクセス ポリシー

🗑️ 削除
🔍 ポリシー情報の表示

シグナルを統合し、意思決定を行い、組織のポリシーを適用するために、条件付きアクセス ポリシーに基づいてアクセスを制御します。 [詳細情報](#)

ユーザーとグループ、ワークロード ID、ディレクトリロール、外部ゲストなど、ポリシーを適用するユーザーに基づいてアクセスを制御します。 [詳細情報](#)

名前 *

特定ユーザのMFA(セキュアリモートアクセス除く)

割り当て

ユーザー ⓘ

組み込まれた特定のユーザー および 除外された特定のユーザー

ターゲットリソース ⓘ

すべてのクラウド アプリ 件を含む および 1 個のアプリが除外されました

対象 対象外

ポリシーから除外するユーザーとグループを選択します

ゲストまたは外部ユーザー ⓘ

ディレクトリロール ⓘ

グローバル管理者 ▼

ユーザーとグループ

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://learn.microsoft.com/ja-jp/entra/identity/conditional-access/howto-conditional-access-policy-all-users-mfa>

Microsoft Entra ID で緊急アクセス用管理者アカウントを管理する
<https://learn.microsoft.com/ja-jp/entra/identity/role-based-access-control/security-emergency-access>

7. 「ターゲットリソース」を選択し、対象となるクラウドアプリを選択します。

特定ユーザのMFA(セキュアリモートアクセス除く) ...

条件付きアクセス ポリシー

削除
ポリシー情報の表示

シグナルを統合し、意思決定を行い、組織のポリシーを適用するために、条件付きアクセス ポリシーに基づいてアクセスを制御します。 [詳細情報](#)

名前 *

このポリシーが適用される対象を選択する

クラウド アプリ

対象 対象外

なし

すべてのクラウド アプリ

アプリを選択

割り当て

ユーザー ①

組み込まれた特定のユーザー および 除外された特定のユーザー

ターゲット リソース ①

すべてのクラウド アプリ 件を含む および 1 個のアプリが除外されました

条件 ①

0 個の条件が選択されました

⚠️ 自分自身をロックアウトしないでください。このポリシーは Azure portal に影響します。続行する前に、自分または他のユーザーがポータルに戻れることをご確認ください。
"すべてのクラウド アプリ" が選択されている場合にのみ正常に機能する永続的ブラウザ

8. 「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。

ホーム > 条件付きアクセス | ポリシー >
除外されたクラウド アプリの選択 ×

新規 ...

条件付きアクセス ポリシー

シグナルを統合し、意思決定を行い、組織のポリシーを適用するために、条件付きアクセス ポリシーに基づいてアクセスを制御します。 [詳細情報](#)

名前 *

このポリシーが適用される対象

クラウド アプリ

対象 **対象外**

ポリシーから除外するクラウド

フィルターの編集

なし

除外されたクラウド アプリの選

なし

クラウド アプリ

<input type="checkbox"/>	WA	Windows Azure Service Manage... 797f4846-ba00-4fd7-ba43-dac1f8f63013
<input type="checkbox"/>	WS	Windows Store for Business 45a330b1-b1ec-4cc1-9161-9f03992aa49f
<input checked="" type="checkbox"/>	セキ	セキュアリモートアクセス 16414a9e-5fb2-4193-b82c-915322a087d3

選択したアイテム

セキ
セキュアリモートアクセス
16414a9e-5fb2-4193-b82c-9...

削除

選択

ポリシーの有効化

レポート専用
オン
オフ

作成

9. 「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。

ホーム > 条件付きアクセス | ポリシー >

新規 ...

条件付きアクセス ポリシー

ユーザー

すべてのユーザー

ターゲット リソース

すべてのクラウド アプリ 件を含む および 1 個のアプリが除外されました

条件

0 個の条件が選択されました

アクセス制御

許可

0 個のコントロールが選択されました

ポリシーの有効化

レポート専用 **オン** オフ

作成

許可

アクセスをブロックまたは許可するため、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

新しい "認証強度が必要" のテストを検討してください。 [詳細情報](#)

認証強度が必要

"認証強度が必要" と "多要素認証を要求する" は同時に使用できません。 [詳細情報](#)

選択

8 セキュアリモートアクセス認証設定

本手順は Microsoft Entra ID 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「Microsoft Entra ID」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。

Microsoft Entra ID (旧称 AzureAD) 設定

Microsoft Entra ID (旧称 AzureAD) と連携してVPN接続のユーザ認証をおこないます。
 下記の項目を入力して設定ボタンを押してください。
 ※管理者ユーザ名/パスワードは初回の認証確認のみに利用されます。

アプリケーションID 必須	<input type="text" value="123456789-abcdefghi-123456"/>	✓
アプリケーションパスワード 必須	<input type="password" value="....."/>	✓
ドメイン名 必須	<input type="text" value="bit-drive"/>	✓
管理者ユーザ名 必須	<input type="text" value="administrator"/>	✓
管理者パスワード 必須	<input type="password" value="....."/>	✓
シークレット有効期限 必須	<input type="text" value="2028/12/31"/> <small>📅</small>	✓

設定
キャンセル

項目	説明	参考ページ
アプリケーション ID 【必須】	Microsoft Entra ID の「アプリケーション登録」より確認したアプリケーション 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 【必須】	Microsoft Entra ID の「アプリケーション登録」より作成したアプリのクライアントシークレットキー	6-2 アプリケーションパスワード取得
ドメイン名【必須】	Microsoft Entra ID で使用中のドメイン名	—
管理者ユーザ名【必須】	Microsoft Entra ID に登録しているアカウント ※@以降は不要です。 ※一般ユーザでも指定可能です。 ※多要素認証を有効にしている管理者ユーザ名は利用できません。	5 ユーザ登録
管理者パスワード【必須】	上記アカウントに紐づくパスワード	5 ユーザ登録
シークレット有効期限 【必須】	Microsoft Entra ID の「アプリケーション登録」より作成したアプリのシークレット有効期限 ※有効期限を設定することで、6ヶ月前より毎月メールで期限を通知することができます。 なお、通知先は全体設定「通知メール宛先」に設定しているメールアドレス宛に通知されます。	6-2 アプリケーションパスワード取得

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、セキュアリモート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。

重要

- 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。
- Microsoft Entra ID の仕様により、管理者ユーザの認証には多要素認証が必要となります。
しかし、セキュアリモートアクセスでは Microsoft Entra ID の多要素認証の機能に対応していません。
そのため、管理者ユーザ名には多要素認証を設定されていないユーザ名にてご登録ください。