



クラウド接続 接続先サービス初期設定手順書 (Azure)

〈まえがき〉

1. 本書の位置づけ

本書は、beat クラウド接続サービスをご契約になっているお客様を対象に、Microsoft Azure（以下、Azure といいます。）側にて必要となる、アプリケーション（サービス プリンシパル）の作成手順、また、ロールの設定手順をご案内するものです。アプリケーションを作成されますと、beat-box での設定時に使用する情報を取得することが可能です。

2. 前提条件

本書でご案内している手順は、Azure に Azure Portal を操作できるお客様ご自身のアカウントをお持ちであることを前提としております。

また、本書は、beat クラウド接続サービスをご利用になるために必要なアプリケーション ID（サービス プリンシパル ID）、クライアント シークレットの値（サービス プリンシパルのパスワード）、パブリッシャー ドメインの取得方法とロールの設定方法についてはご案内しておりますが、クラウド接続先の仮想ネットワーク（VNet）の作成やゲートウェイ サブネットの追加、その他の Azure 初期設定については、あらかじめお客様ご自身で実施していただく必要があります。

3. 注意制限事項

本手順書内の Azure Portal 画面は、2021 年 6 月 1 日時点のものを使用しております。以降に Azure の仕様が変更された場合、項目名やレイアウトが異なる可能性がありますのでご注意ください。また、Azure の公式ウェブサイトでも各設定手順がご覧になれます。

4. 商標について

Microsoft、Azure、その他のマイクロソフト製品の名称および製品名は、米国 Microsoft Corporation の米国およびその他の国における商標または登録商標です。

< 目次 >

1. クラウド接続の利用開始までの設定	1
1.1. はじめに.....	1
1.2. クラウド接続利用開始までの設定フロー	1
2. アプリケーションの作成手順	2
3. ロールの設定手順	7
4. beat-box の設定に必要な情報取得手順	9
4.1. 仮想ネットワーク名、仮想ネットワークのアドレス空間、リソース グループ名の確認方法.....	9
4.2. アプリケーション（クライアント）ID の確認方法	10
4.3. クライアント シークレットの再作成方法.....	11

1. クラウド接続の利用開始までの設定

1.1. はじめに

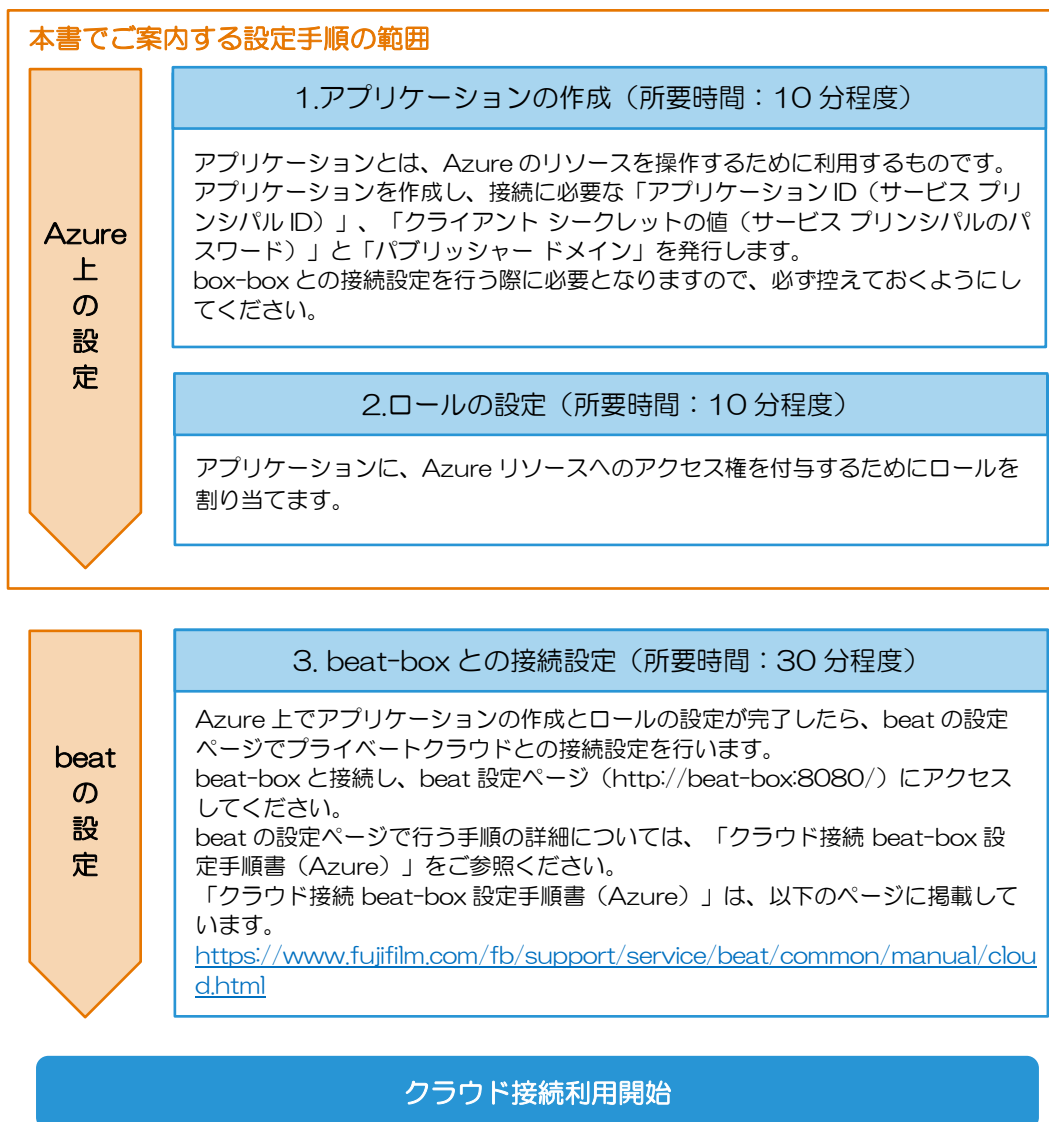
「beat クラウド接続サービス」は、beat-box とパブリッククラウドサービス内の仮想プライベートネットワークとの間を VPN で接続するサービスです。

本サービスをご利用になるために、Azure の設定と beat-box の設定をお客様に実施していただく必要があります。本書では、お客様に実施していただく設定のうち、Azure Portal 上で行う設定の手順についてご案内しております。

1.2. クラウド接続利用開始までの設定フロー

お客様に実施していただく作業のフローは以下のとおりです。

なお、下の図にて示している所要時間は目安であり、お客様の環境により異なります。

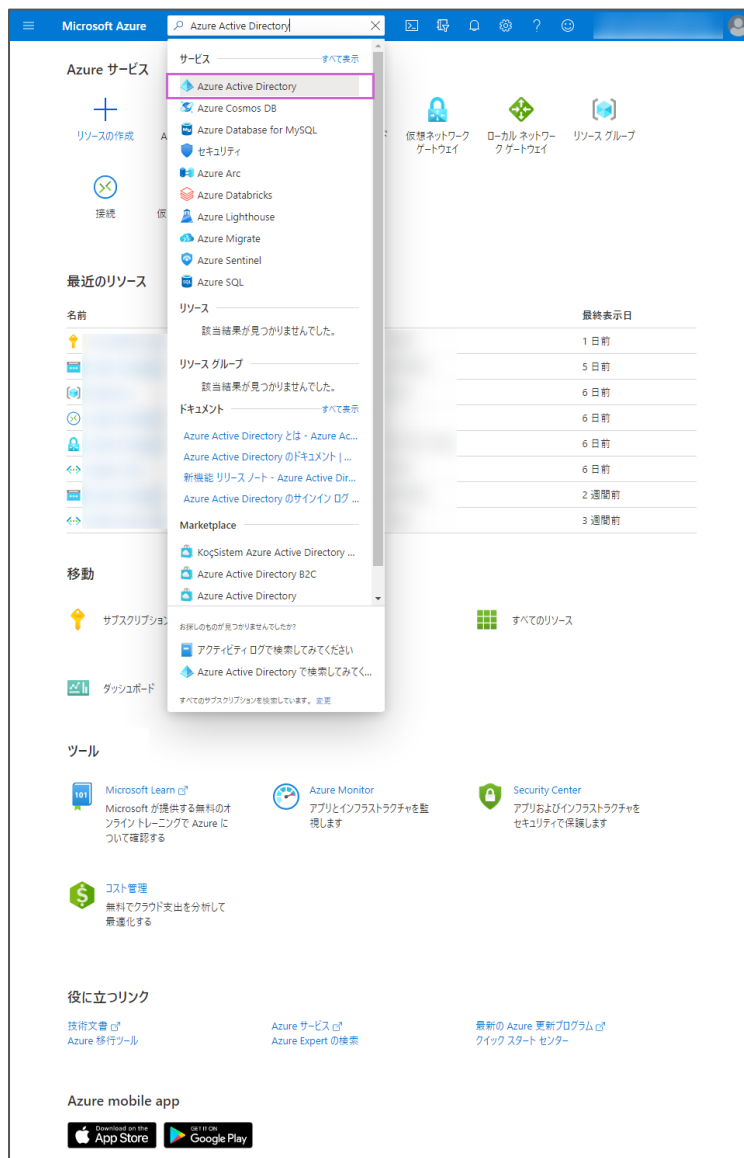


2. アプリケーションの作成手順

beat-box との接続設定では、Azure の設定情報が必要になります。
本章では、以下 3 項目を取得することがきます。既に情報をお持ちの場合は、次の設定に進んでください。

- アプリケーション ID (サービス プリンシパル ID)
- クライアント シークレットのパスワード (サービス プリンシパルのパスワード)
- パブリッシャー ドメイン

1. Azure Portal にサインインします。
以下の URL にアクセスし、お持ちのアカウントで Azure Portal にサインインしてください。
<https://portal.azure.com/>
2. Azure Portal のトップ画面が表示されます。
画面上部の検索バーにて[Azure Active Directory]と入力し、検索バーの下に表示される検索候補から[Azure Active Directory]を選択してください。



- Azure Active Directory の概要画面が表示されます。
画面左部のメニューから、[アプリの登録]をクリックしてください。
- Azure Active Directory のアプリの登録画面が表示されます。
画面上部の[新規登録]をクリックしてください。
- アプリケーションの登録画面が表示されます。
任意で名前を入力し、サポートされているアカウントの種類にチェックを入れ、リダイレクト URI を入力してください。
[登録]をクリックしてください。

Microsoft Azure リソース、サービス、ドキュメントの検索 (G+)

ホーム > **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 (後で変更できます)。
example_app

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 (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...](#)

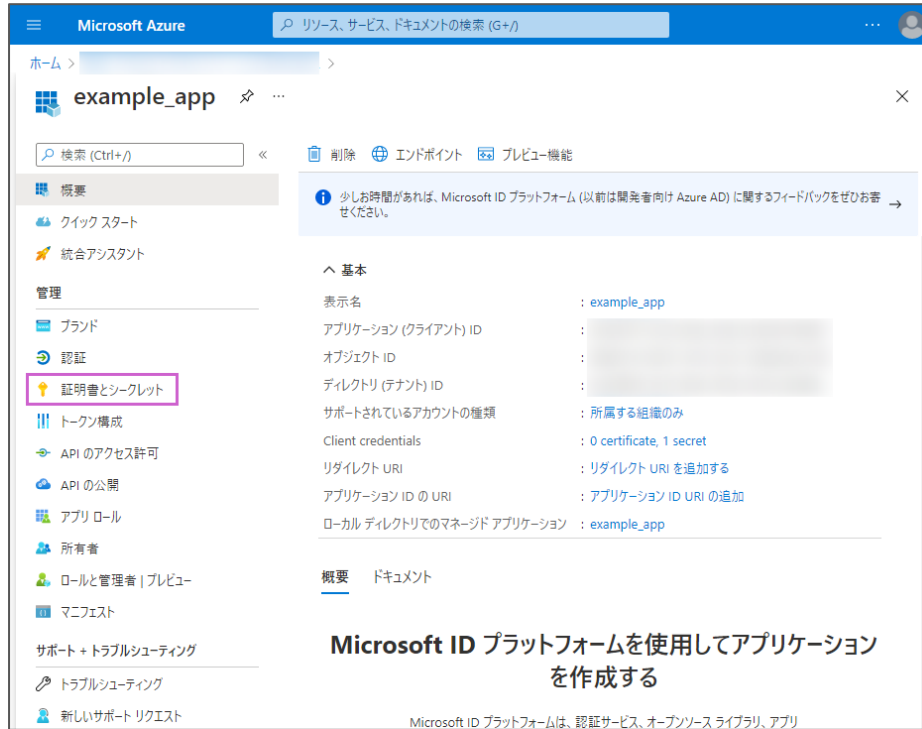
リダイレクト URI (省略可能)
ユーザー認証が成功すると、この URI に認証応答を返します。この時点での指定は省略可能で、後ほど変更できますが、ほとんどの認証シナリオで値が必要となります。
Web 例: https://example.com/auth

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

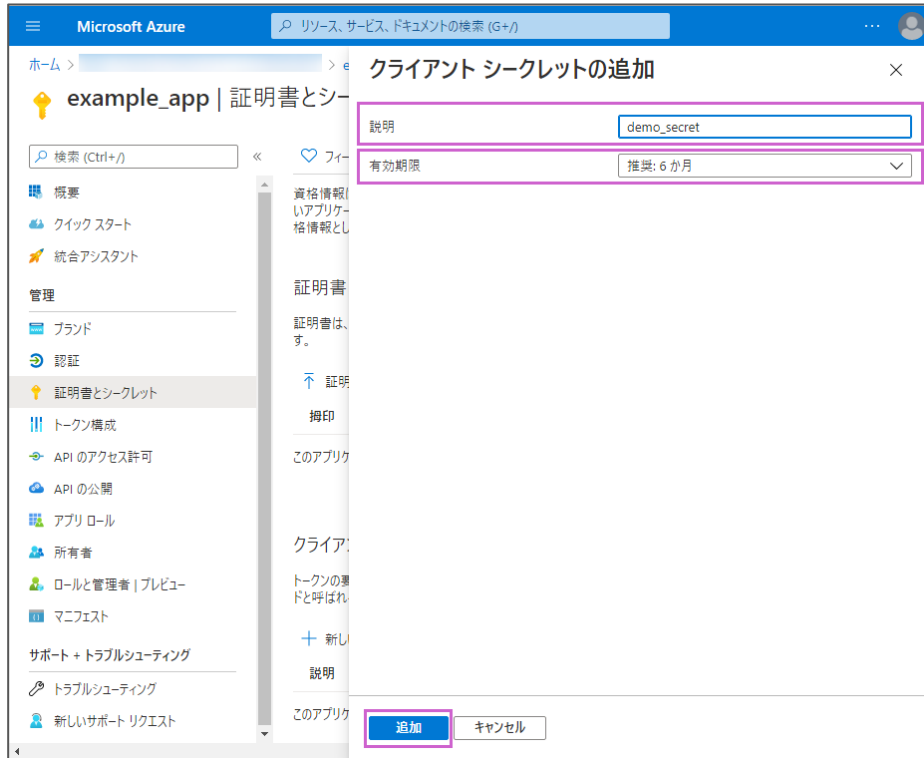
登録

6. アプリケーションの作成が完了し、アプリケーションの概要が表示されます。画面左部のメニューから、[証明書とシークレット]をクリックしてください。



7. 証明書とシークレット画面が表示されます。[新しいクライアント シークレット]をクリックしてください。

8. クライアント シークレットの追加ウィンドウが表示されます。任意で説明を入力し、有効期限を選択し、[追加]をクリックしてください。



注意

クライアント シークレットの有効期限が切れてしまった場合、再度作成し直す必要があります。

9. クライアント シークレットが作成され、クライアント シークレットの値（サービス プリンシパルのパスワード）が表示されます。「クライアント シークレットの値（サービス プリンシパルのパスワード）」はクライアント シークレットの作成時にのみ表示されますので、必ずメモに控えておいてください。



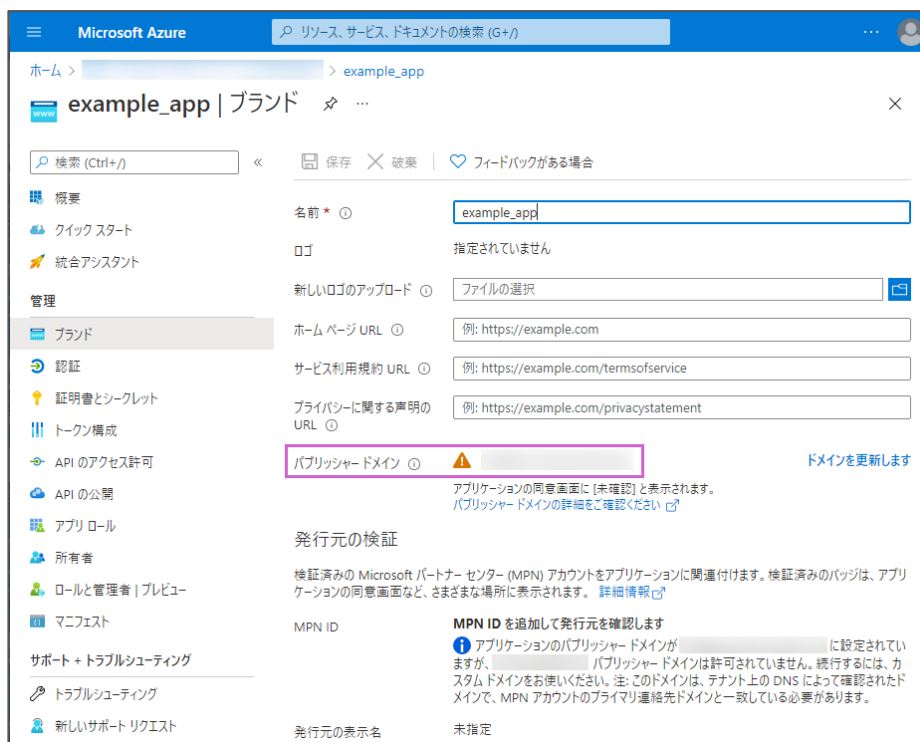
注意

「クライアント シークレットの値 (サービス プリンシパルのパスワード)」は、beat-box との設定で必要となります。もし忘れてしまった場合は、クライアント シークレットを作成し直す必要があります。

10. 画面左部のメニューから、[ブランド]を選択してください。

11. ブランド画面が表示されます。

表示された「パブリッシャー ドメイン」をメモに控えておいてください。



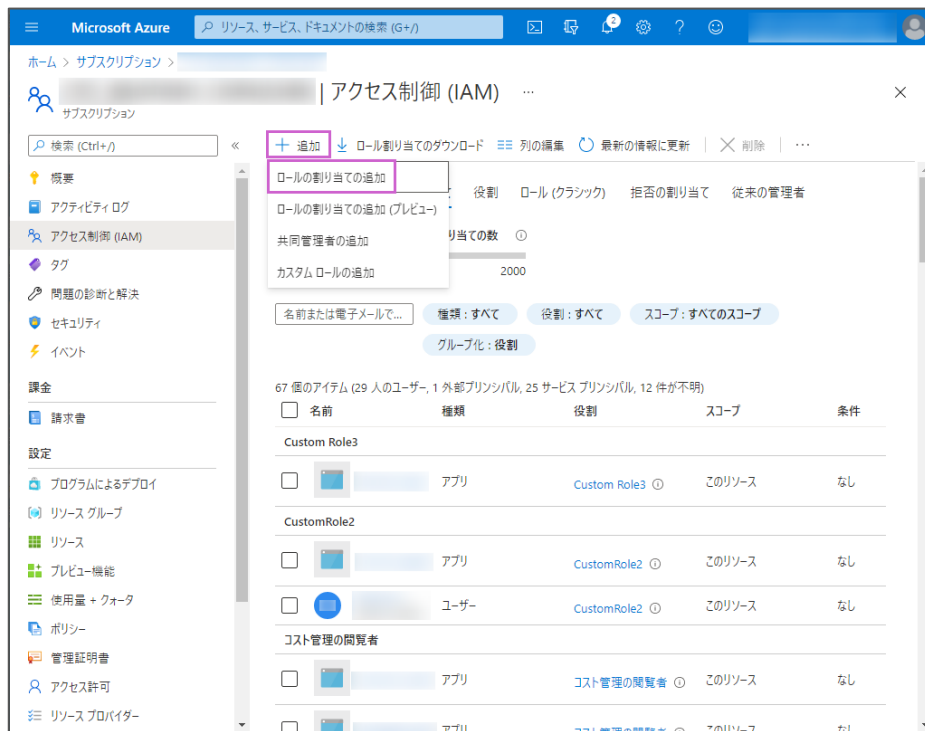
以上で、アプリケーションの作成は完了です。

続いて、ロールの設定を行ってください。

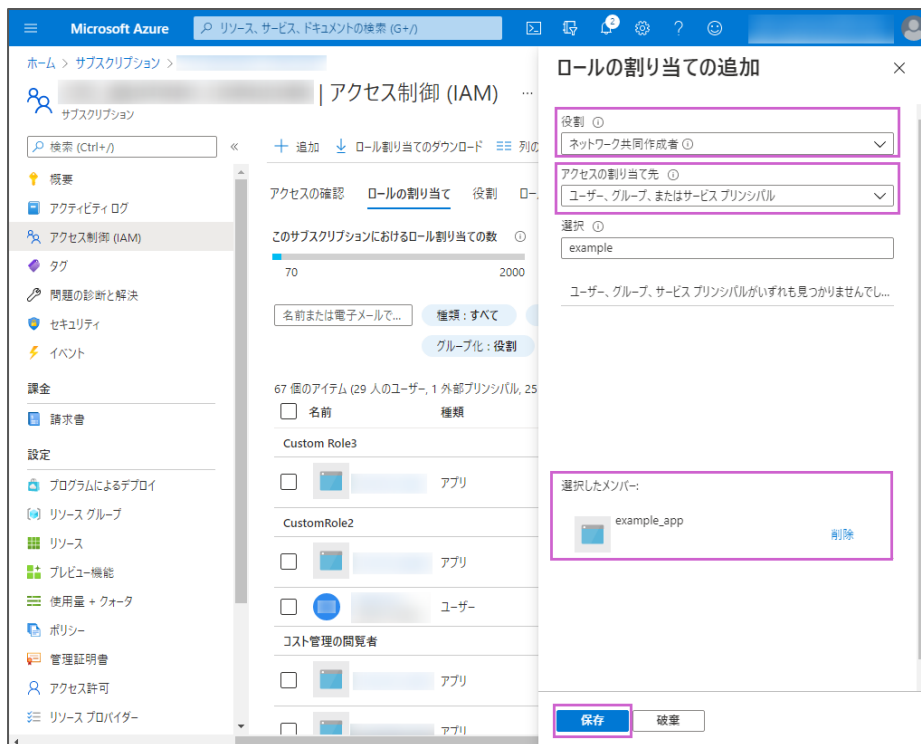
3. ロールの設定手順

「2.アプリケーションの作成手順」で作成したアプリケーションにロールを割り当てます。
ロールを割り当てることで、Azure リソースへのアクセス権を付与することが可能になります。

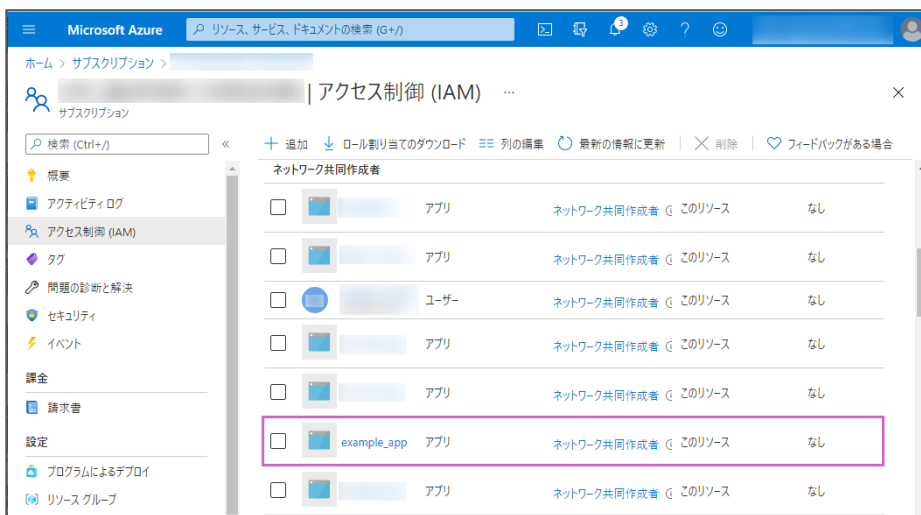
1. 画面上部の検索バーにて[サブスクリプション]と入力し、検索バーの下に表示される検索候補から[サブスクリプション]を選択してください。
2. サブスクリプション画面が表示されます。
対象のサブスクリプションを選択してください。
3. 選択したサブスクリプションの管理画面が表示されます。
画面左部のメニューから、[アクセス制御(IAM)]をクリックしてください。
4. サブスクリプションのアクセス制御(IAM)画面が表示されます。
[ロールの割り当て]タブをクリックしてください。
5. ロールの割り当てタブが表示されます。
画面上部のメニューから、[追加]、さらに[ロールの割り当ての追加]をクリックしてください。



6. ロールの割り当ての追加ウィンドウが表示されます。役割にて[ネットワーク共同作成者]、アクセスの割り当て先にて[ユーザー、グループ、またはサービス プリンシパル]を選択してください。また、選択にて「2.アプリケーションの作成手順」で作成したアプリケーションを検索し、検索バーの下に表示されるアプリケーションを選択後、[保存]をクリックしてください。



7. 一覧に、ロールが割り当てられたアプリケーションが表示されます。



以上で、ロールの設定は完了です。

続いて、beat-box の設定を行ってください。

beat-box での設定方法については、以下のページに手順書を掲載しています。

<https://www.fujifilm.com/fb/support/service/beat/common/manual/cloud.html>

4. beat-box の設定に必要な情報取得手順

beat-box との接続設定では、Azure の設定情報が必要になります。

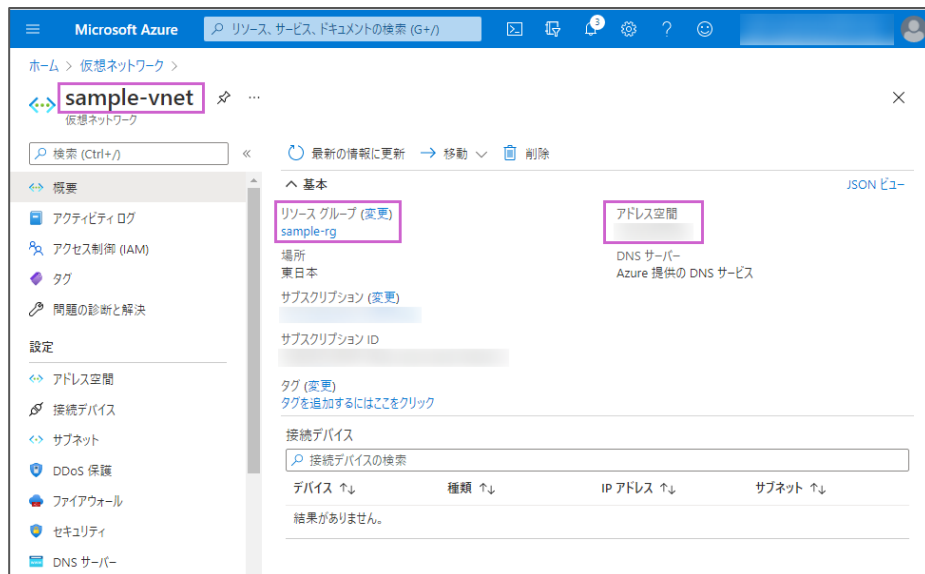
入力が必要な情報は、Azure Portal で確認できます。

本章では、以下5項目の確認手順をご案内します。既に情報をお持ちの場合は、beat-box との接続設定に進んでください。

- 仮想ネットワーク名 (VNet のリソース名)
- 仮想ネットワーク (VNet) のアドレス空間
- リソース グループ名
- アプリケーション (クライアント) ID ※
- クライアント シークレットの値 (サービス プリンシパルのパスワード)
※beat-box の設定画面では、「サービス プリンシパル」として記載しています。

4.1. 仮想ネットワーク名、仮想ネットワークのアドレス空間、リソースグループ名の確認方法

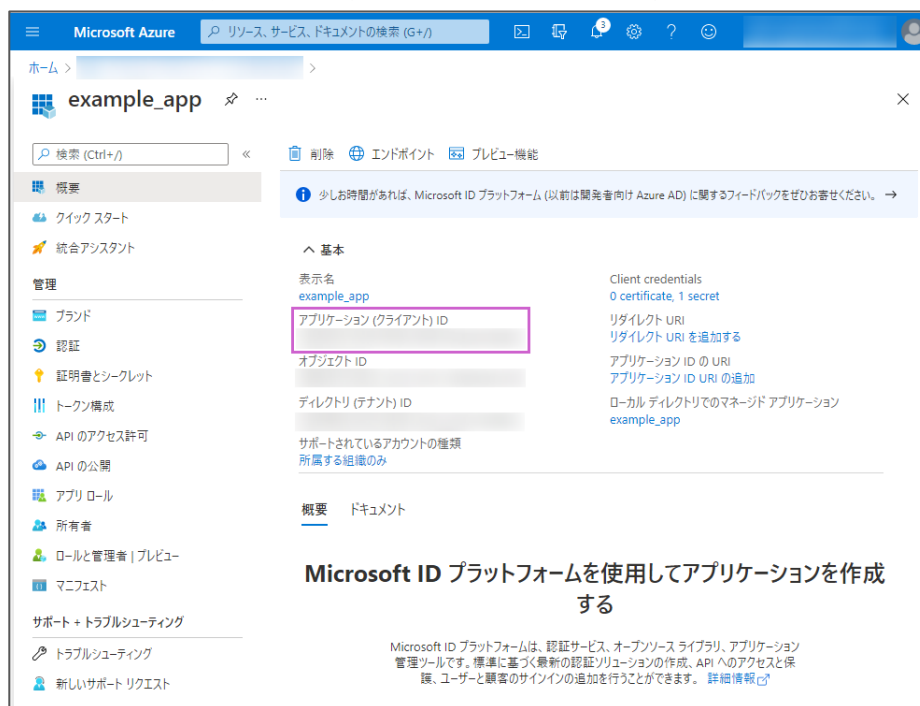
1. 画面上部の検索バーにて[仮想ネットワーク]と入力し、検索バーの下に表示される検索候補から[仮想ネットワーク]を選択してください。
2. 仮想ネットワーク画面が表示されます。
対象の仮想ネットワークを選択してください。
3. 選択した仮想ネットワークの管理画面が表示されます。
仮想ネットワーク名、仮想ネットワークのアドレス空間とリソース グループ名をメモに控えてください。



以上で、仮想ネットワーク名、仮想ネットワークのアドレス空間、リソース グループ名の確認は完了です。

4.2. アプリケーション（クライアント）ID の確認方法

1. 画面上部の検索バーにて[Azure Active Directory]と入力し、検索バーの下に表示される検索候補から[Azure Active Directory]を選択してください。
2. Azure Active Directory の概要画面が表示されます。
画面左部のメニューから、[アプリの登録]をクリックしてください。
3. Azure Active Directory のアプリの登録画面が表示されます。
対象のアプリケーションを選択してください。
4. 選択したアプリケーションの詳細画面が表示されます。
アプリケーション（クライアント）ID をメモに控えてください。



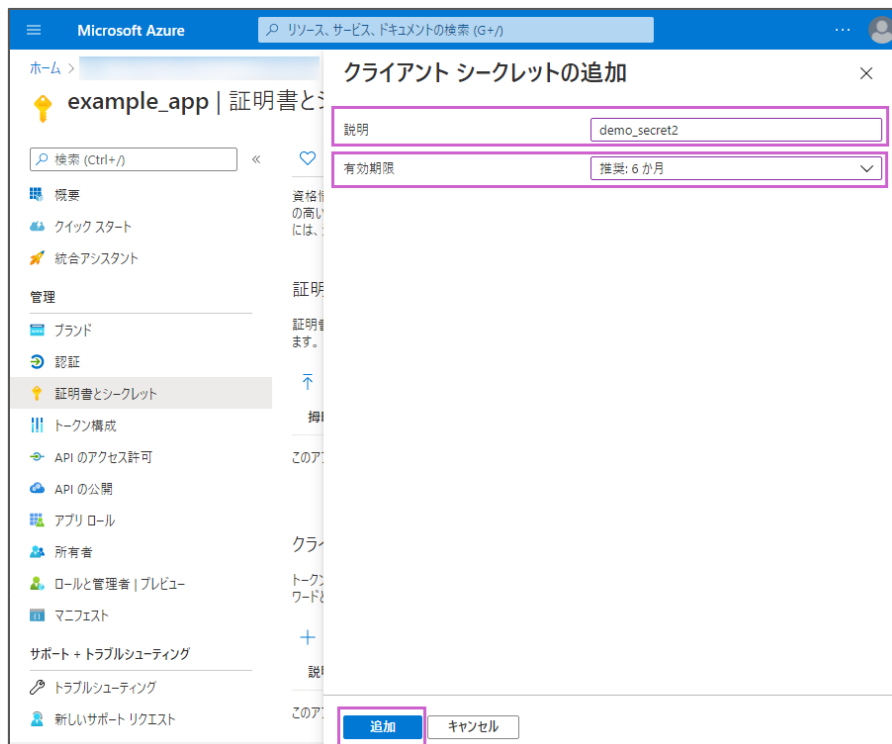
以上で、アプリケーション（クライアント）ID の確認は完了です。

4.3. クライアント シークレットの再作成方法

クライアント シークレットの値（サービス プリンシパルのパスワード）は作成時にのみ表示されます。値がマスク表示になると、参照することはできません。

「2.アプリケーションの作成手順」のクライアント シークレット作成時に、値をメモに控えておらず、再度、値を参照したい場合や、クライアント シークレットの有効期限が切れてしまった場合は、新たにクライアント シークレットを作成していただく必要があります。

1. 画面上部の検索バーにて[Azure Active Directory]と入力し、検索バーの下に表示される検索候補から[Azure Active Directory]を選択してください。
2. Azure Active Directory の概要画面が表示されます。画面左部のメニューから、[アプリの登録]をクリックしてください。
3. Azure Active Directory のアプリの登録画面が表示されます。対象のアプリケーションを選択してください。
4. 選択したアプリケーションの詳細画面が表示されます。画面左部のメニューから、[証明書とシークレット]をクリックしてください。
5. 証明書とシークレット画面が表示されます。[新しいクライアント シークレット]をクリックしてください。
6. クライアント シークレットの追加ウィンドウが表示されます。任意で説明を入力し、有効期限を選択し、[追加]をクリックしてください。



7. 新たにクライアント シークレットが作成され、クライアント シークレットの値が表示されます。「クライアント シークレットの値」を、メモに控えておいてください。

Microsoft Azure | リソース、サービス、ドキュメントの検索 (G+)

example_app | 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

概要

クイック スタート

統合アシスタント

管理

ブランド

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

API の公開

アプリ ロール

所有者

ロールと管理者 | プレビュー

マニフェスト

サポート + トラブルシューティング

トラブルシューティング

新しいサポート リクエスト

証明書

証明書は、トークンの要求時にアプリケーションの ID を証明するシークレットとして使用できます。公開キーとも呼ばれます。

証明書のアップロード

拇印	開始日	有効期限	Certificate ID
このアプリケーションには証明書が追加されていません。			

クライアント シークレット

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	Secret ID
demo_secret	2021/12/1	X~.....	
demo_secret2	2021/12/1		

補足

以前に作成したクライアント シークレットは無効になります。対象のクライアント シークレットの右端にあるゴミ箱マークをクリックすると、削除することができます。

以上で、クライアント シークレットの再作成は完了です。

クラウド接続 接続先サービス初期設定手順書 (Azure)

著作者 — 富士フイルムビジネスイノベーション株式会社
発行者 — 富士フイルムビジネスイノベーション株式会社

発行年月 — 2020年 11月 初版
2021年 7月 第2版