Azureの
認証と承認

2023/3/1

認証

認証＝Entra ID認証

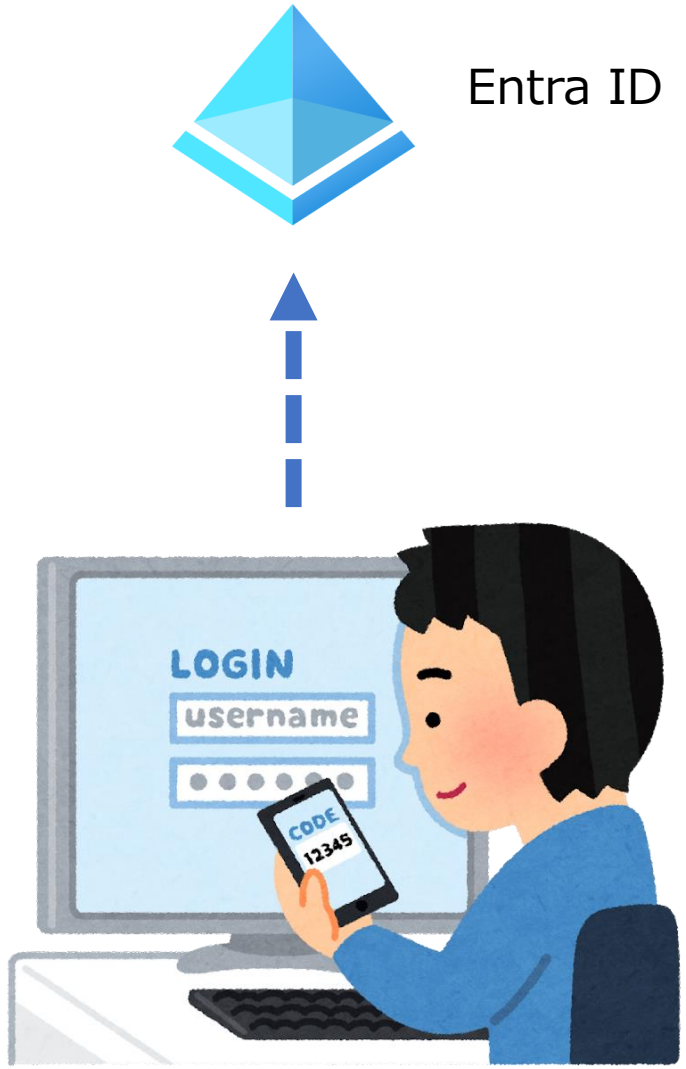
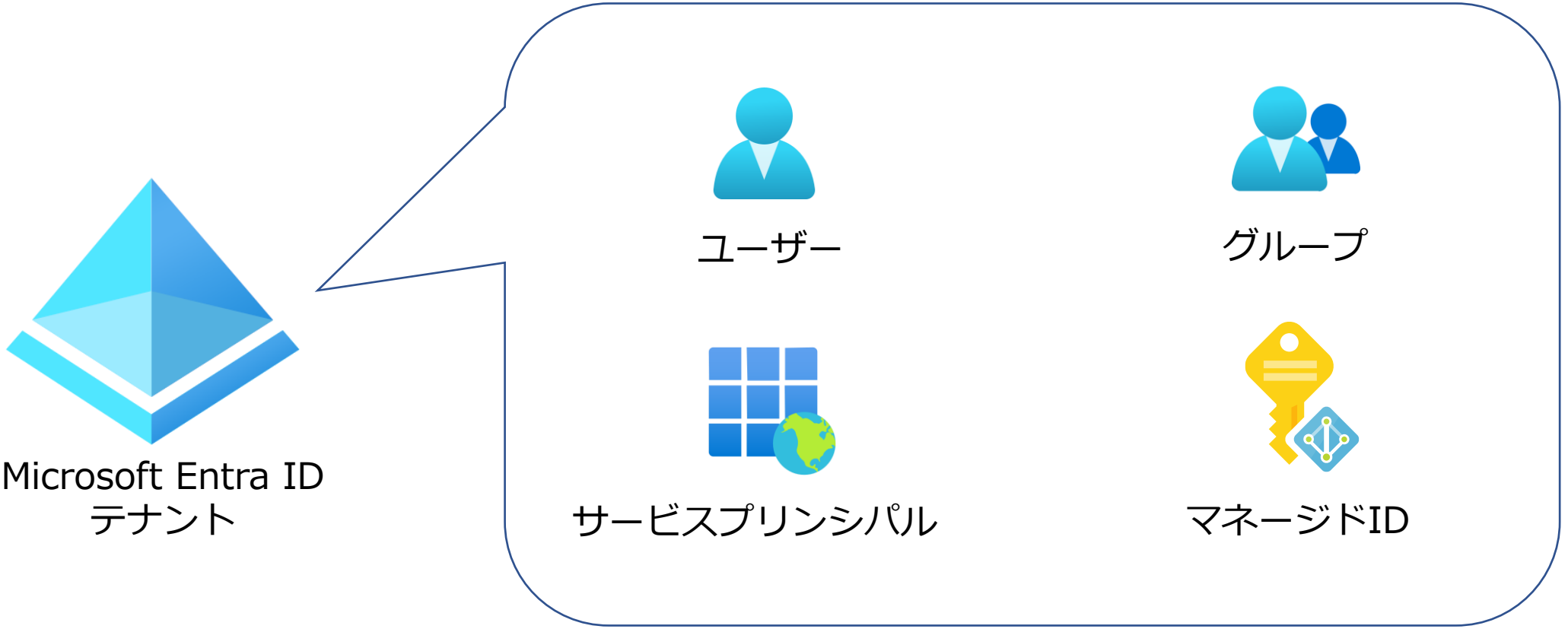


イラスト https://www.irasutoya.com/

■Entra IDで管理されるID（正しいアイコン）



※Azure portal の **[エンタープライズ アプリケーション]** ページを使用して、テナントのサービス プリンシパルを一覧表示および管理することができる。

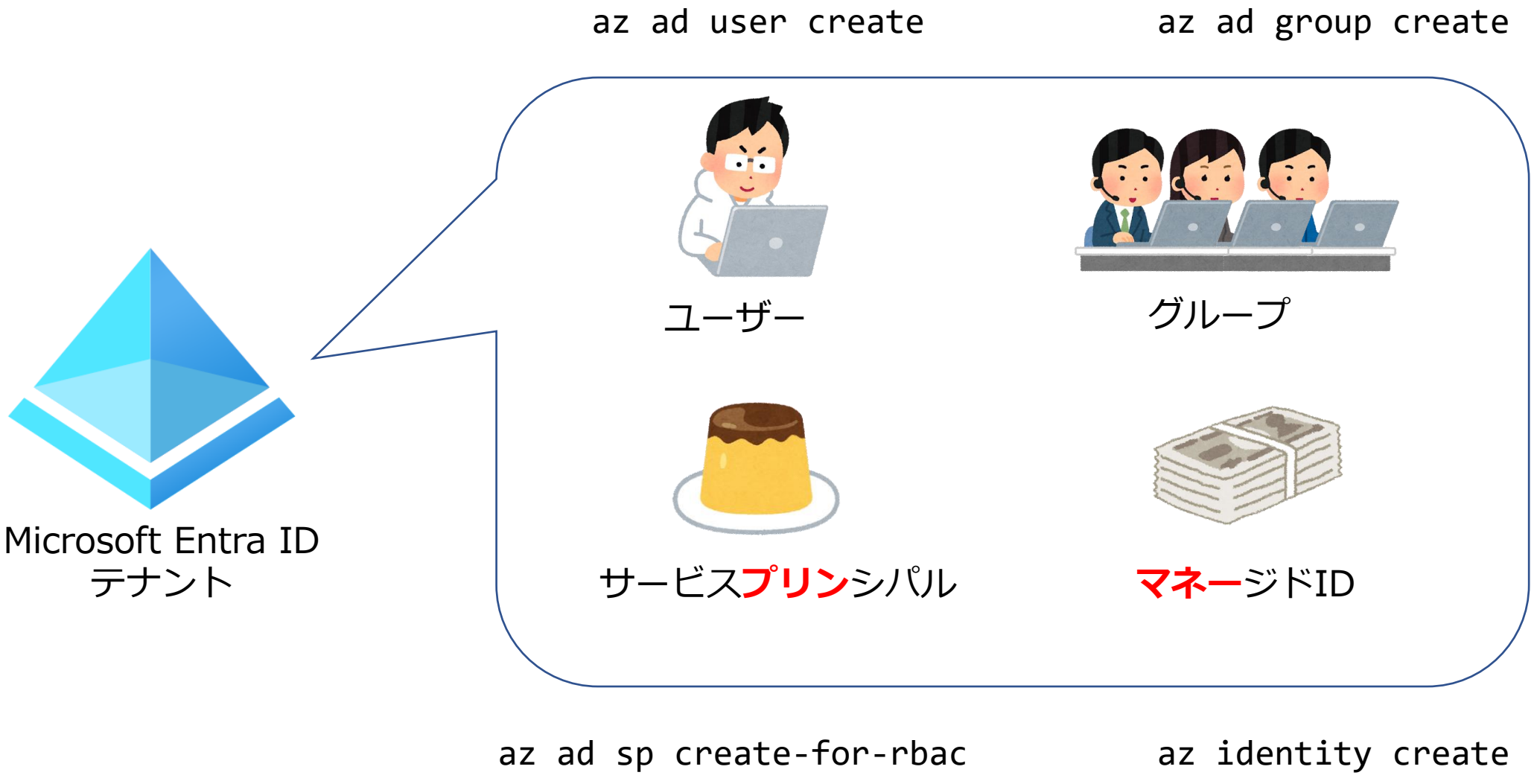
https://learn.microsoft.com/ja-jp/azure/active-directory/develop/app-objects-and-service-principals

鍵マークのアイコンはいろいろ

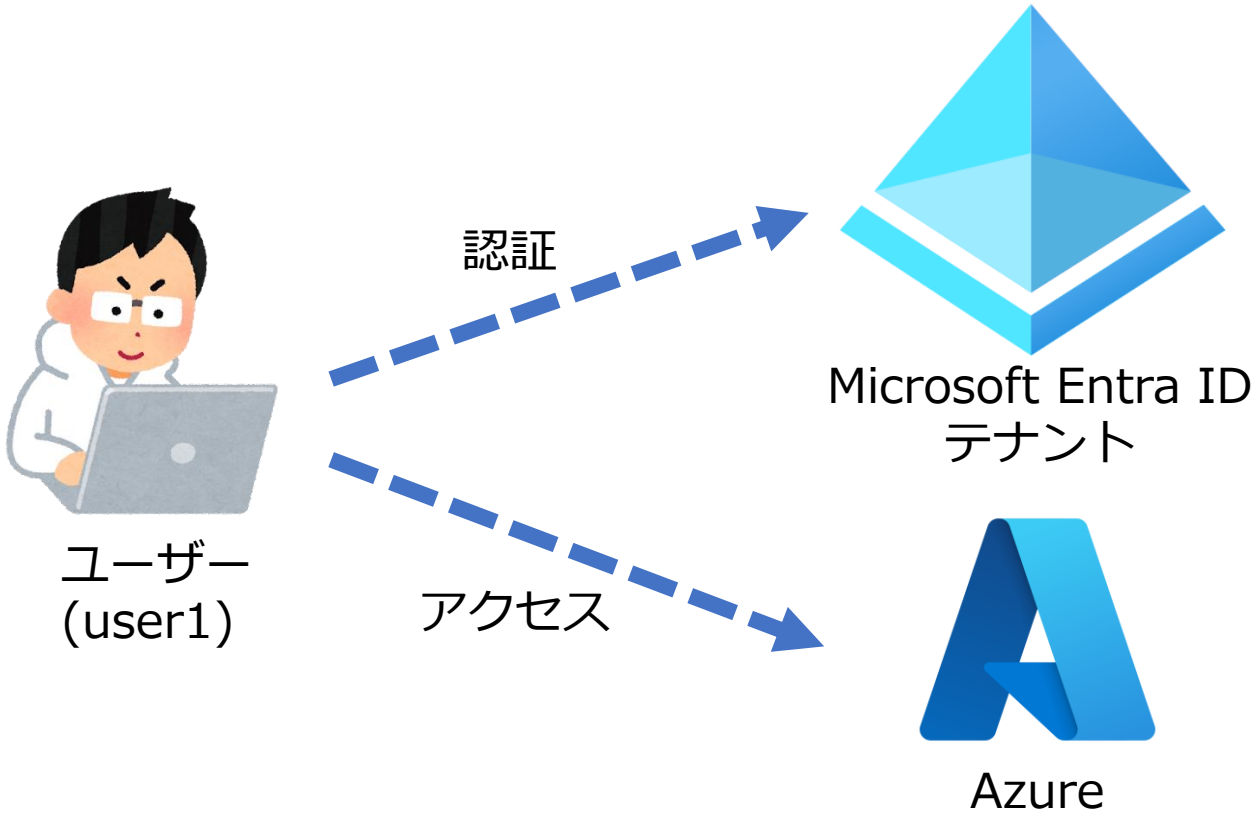
サブスクリプション

Key Vault

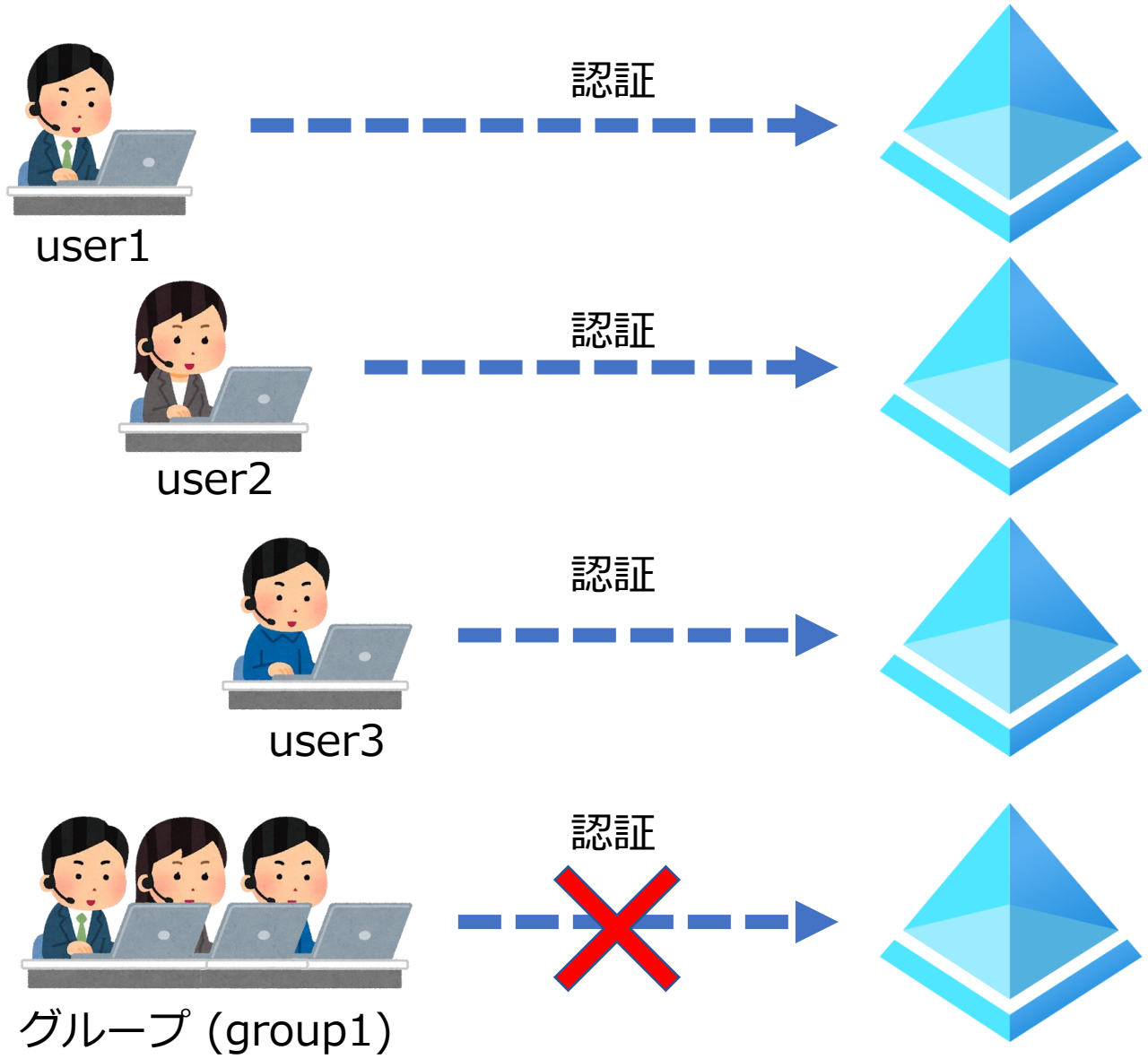
■Entra IDで管理されるID



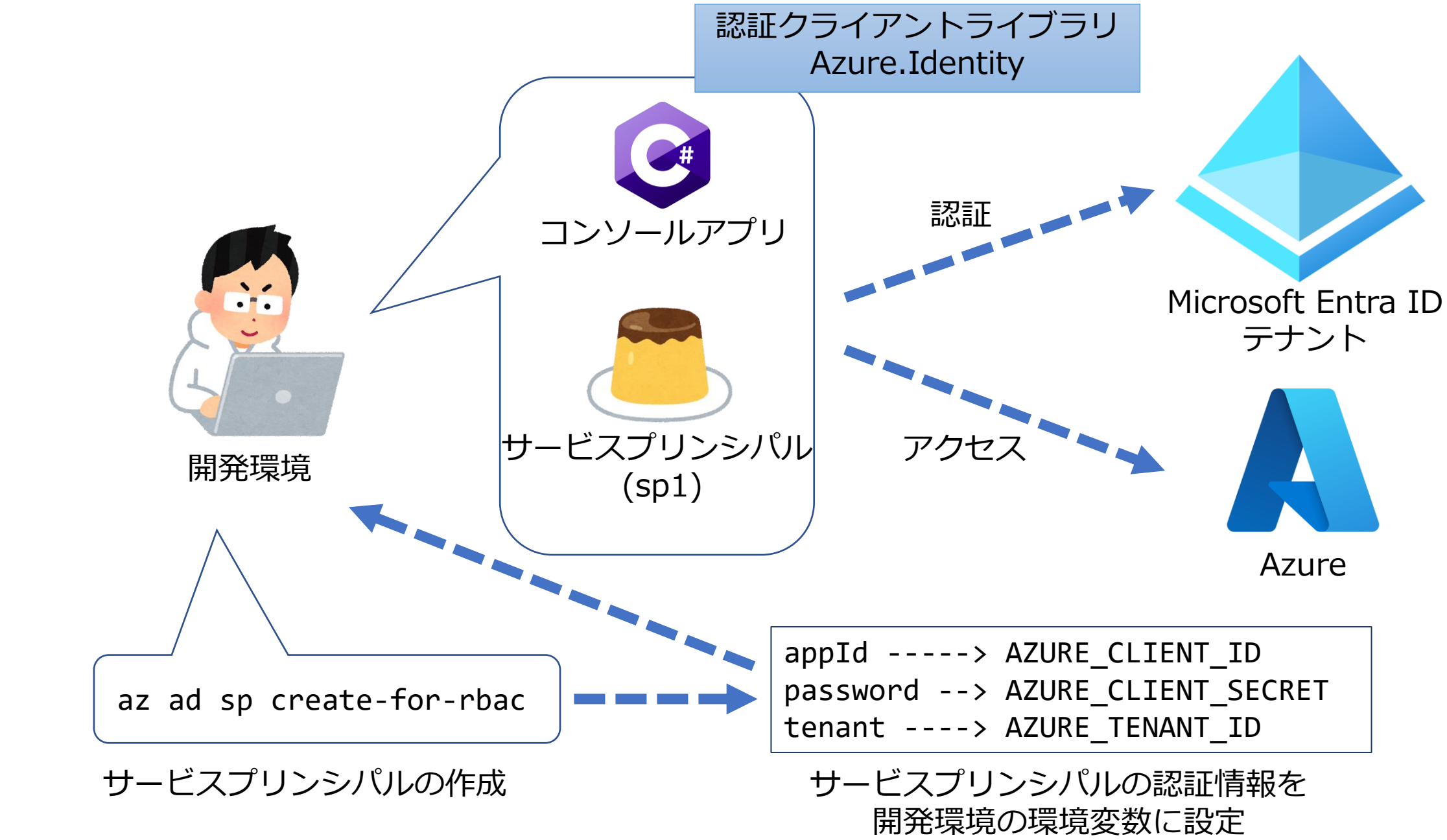
■ユーザーの認証



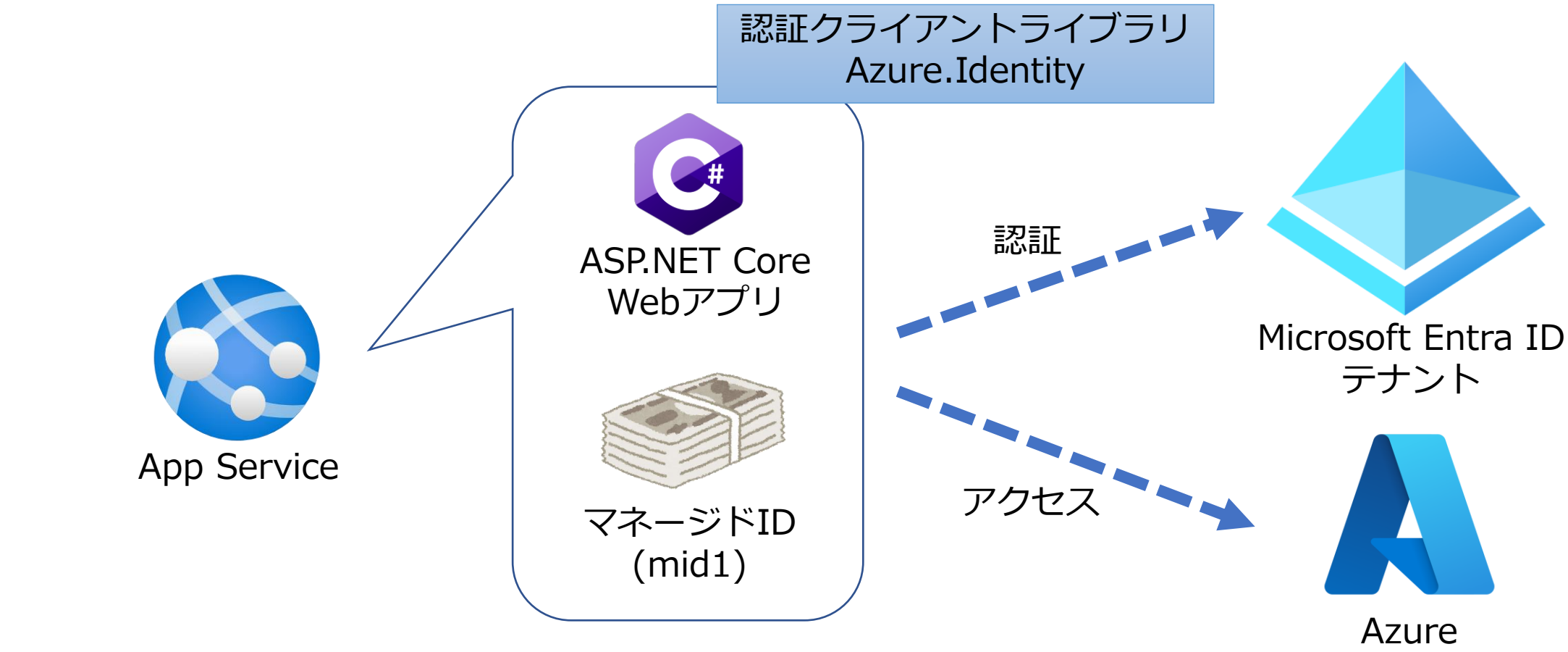
■グループ内の個々のユーザーは、それぞれ、ユーザーとしてサインインが可能だが、
グループによる認証（グループとしてのサインイン）はできない。



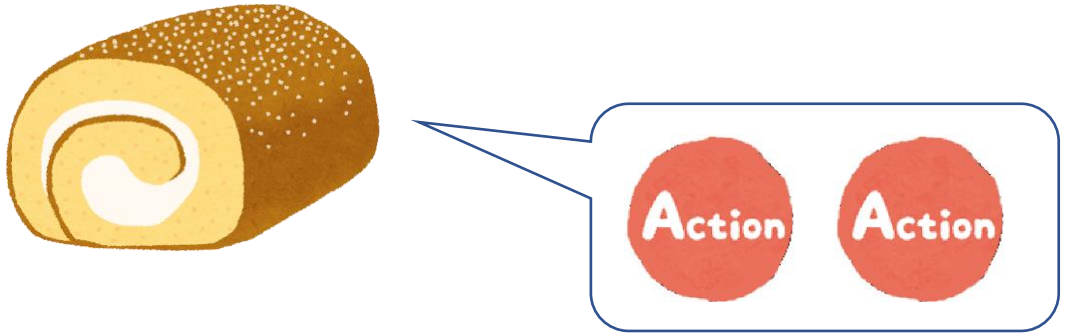
■サービスプリンシパルによる認証



■マネージドIDによる認証



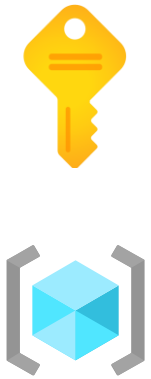
```
az identity create --name id1
az webapp identity assign --identies id1
az webapp identity assign --identies '[system]'
```



ロール

ロールはアクション（操作の許可）の集まり

■Azure RBAC（ロールベースのアクセス制御）のロール



コントロールプレーンのロール

- 所有者
- 共同作成者
- 閲覧者
- ユーザーアクセス管理者

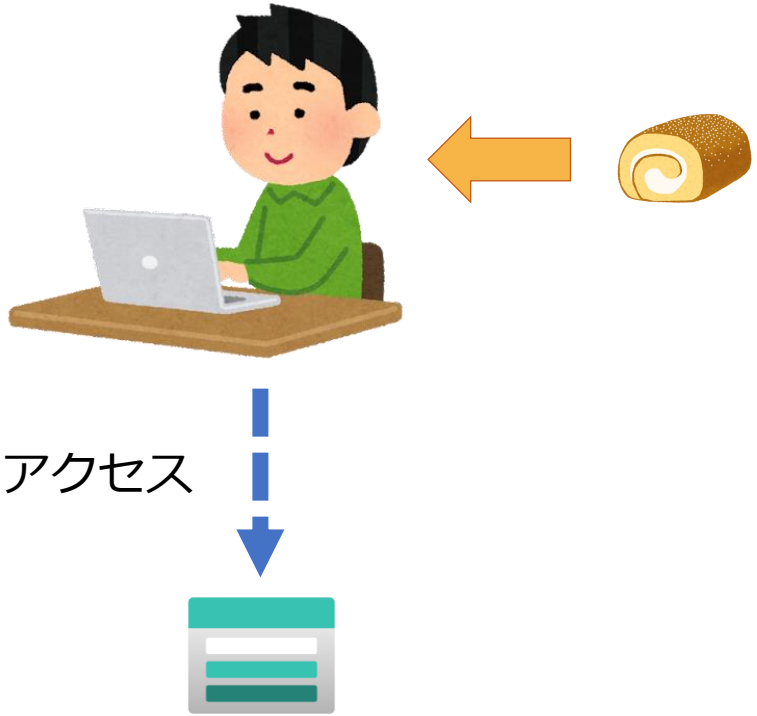
データプレーンのロール

- ストレージBlobデータ共同作成者
- ストレージBlobデータ閲覧者
- Key Vaultシークレット管理者
- Key Vaultシークレット閲覧者
- App Configurationデータ所有者
- App Configurationデータ閲覧者
- Cognitive Service Speechユーザー

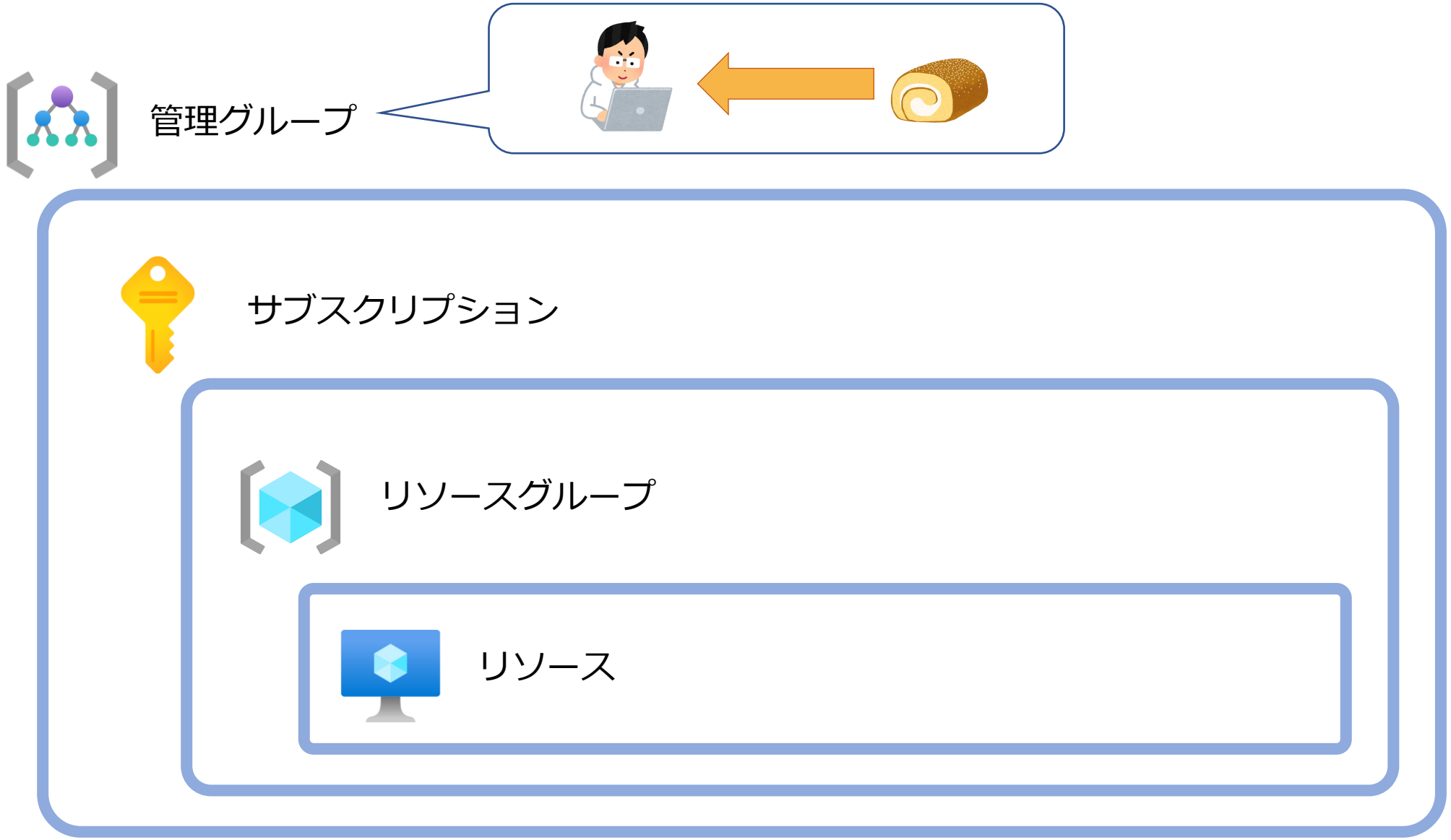
上記の「組み込みのロール」のほか、ユーザーが独自の「カスタムロール」を定義することもできる

承認

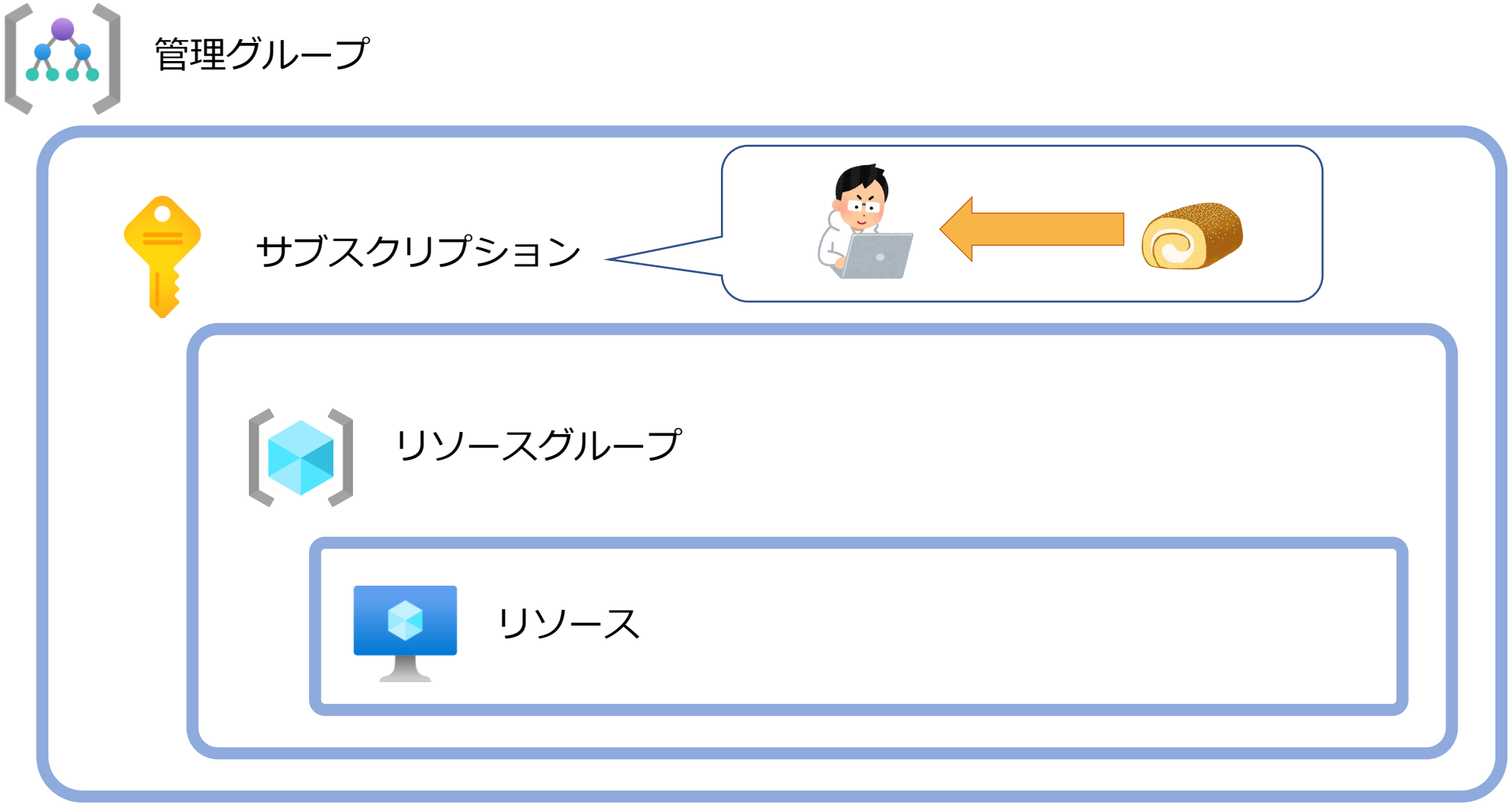
承認＝操作の許可を与えること
ロールの割り当てによって承認を行う



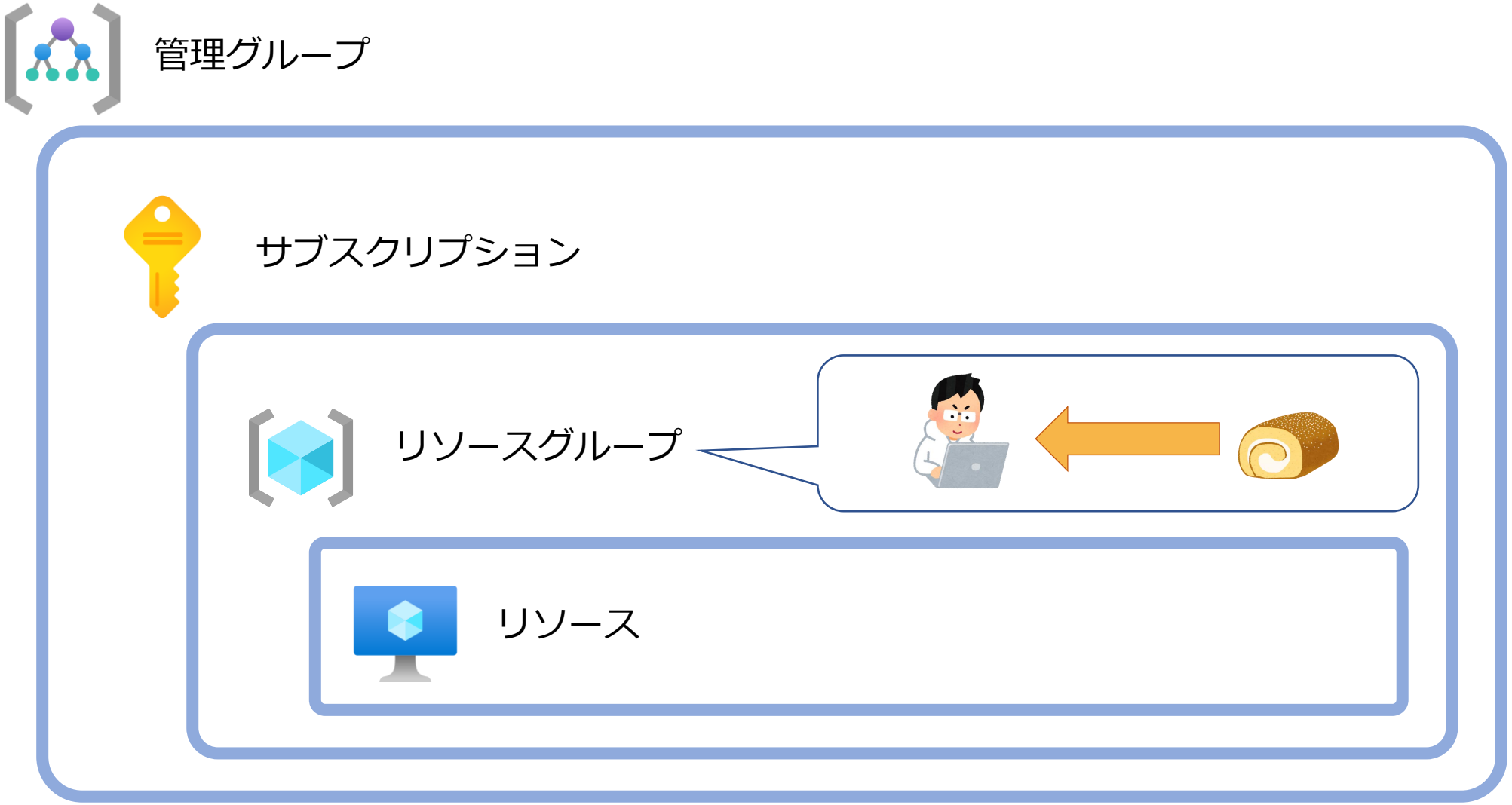
■ロールの割り当てを行うスコープ



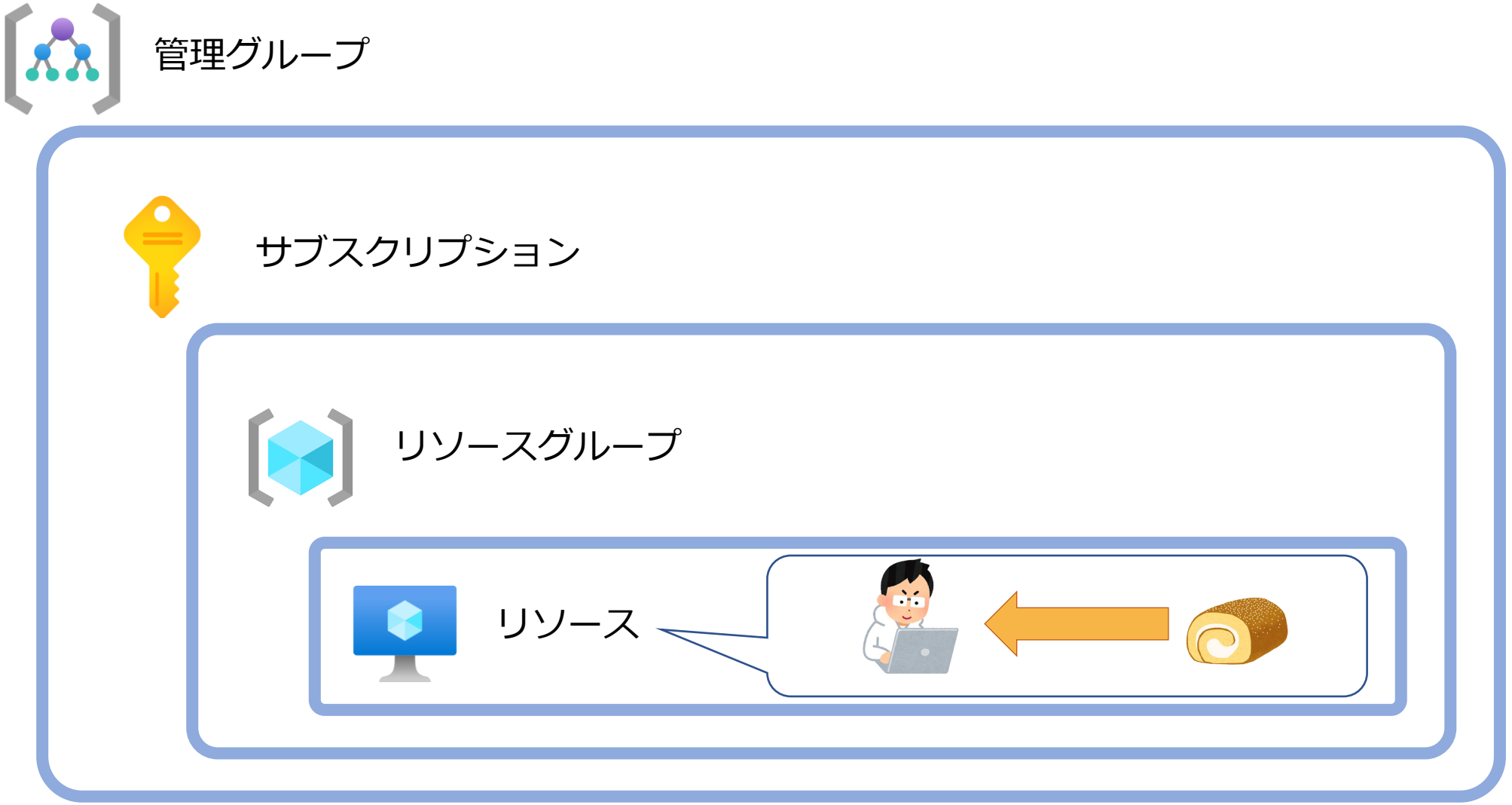
■ロールの割り当てを行うスコープ



■ロールの割り当てを行うスコープ



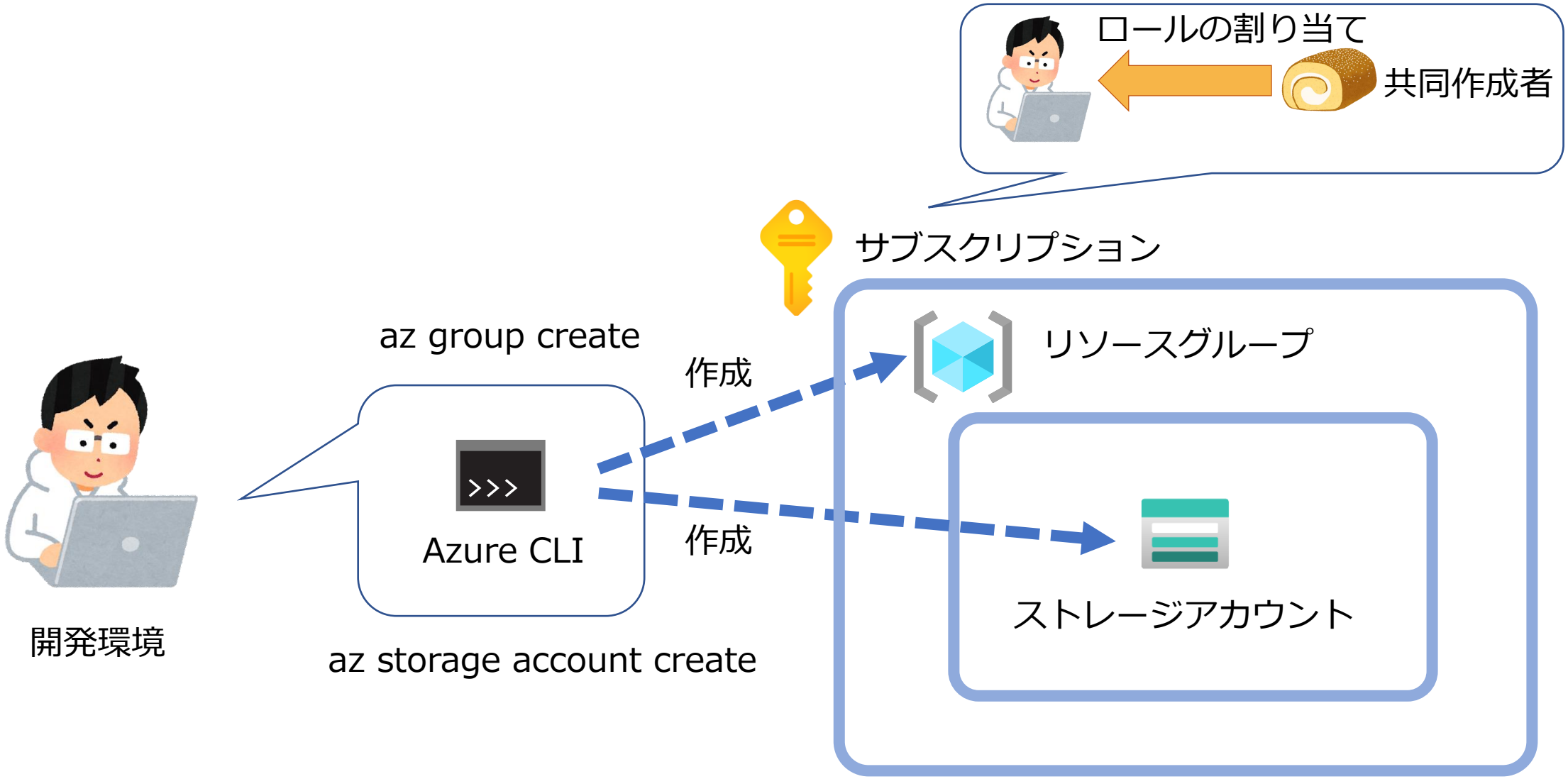
■ロールの割り当てを行うスコープ



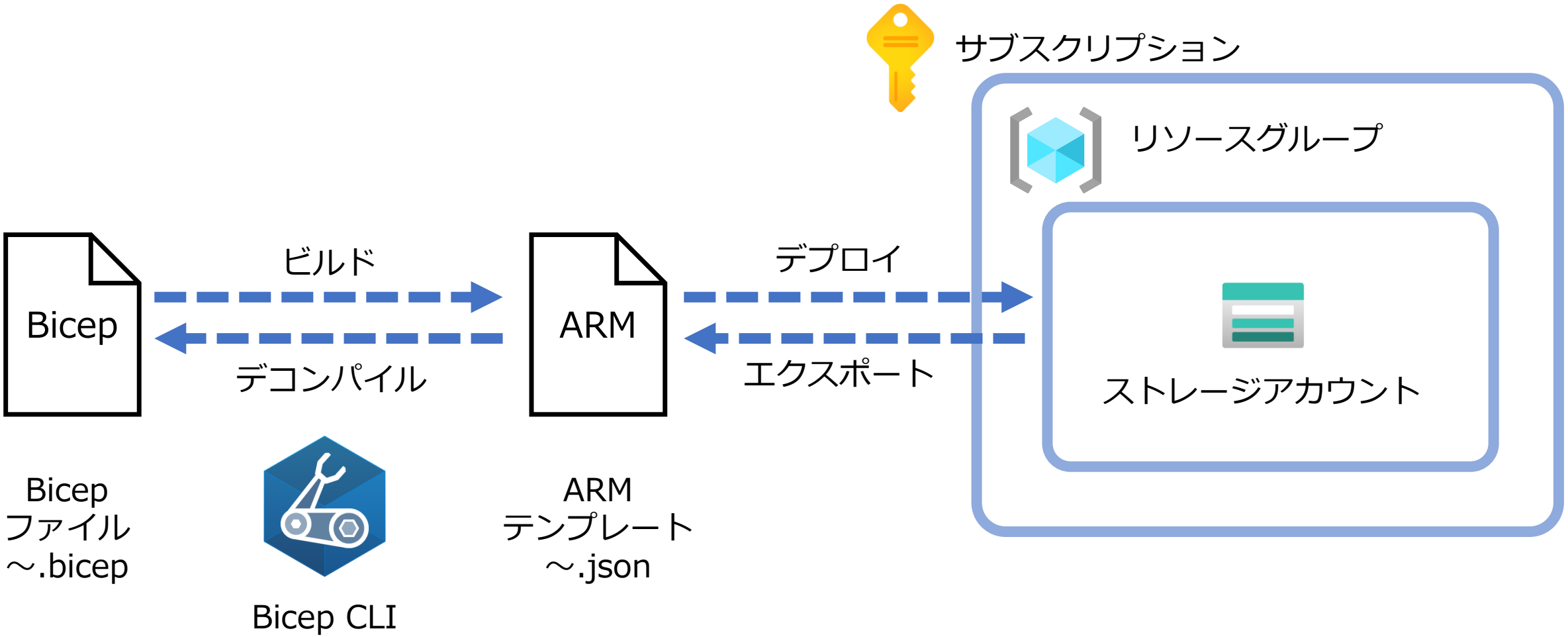
ロールの利用例(1)
リソースの作成

リソースを作成するためのロール割り当てが必要

■Azure CLIによるリソースの作成



■参考: Bicepのしくみ



ロールの利用例(2)
ストレージアカウント（Blob）へのアクセス

Blobの読み書きを行うための
ロールの割り当てが必要

■グループ（に含まれるユーザー）の認証と承認

グループ (group1)

ユーザー (user1)

認証

Microsoft Entra ID

アクセス

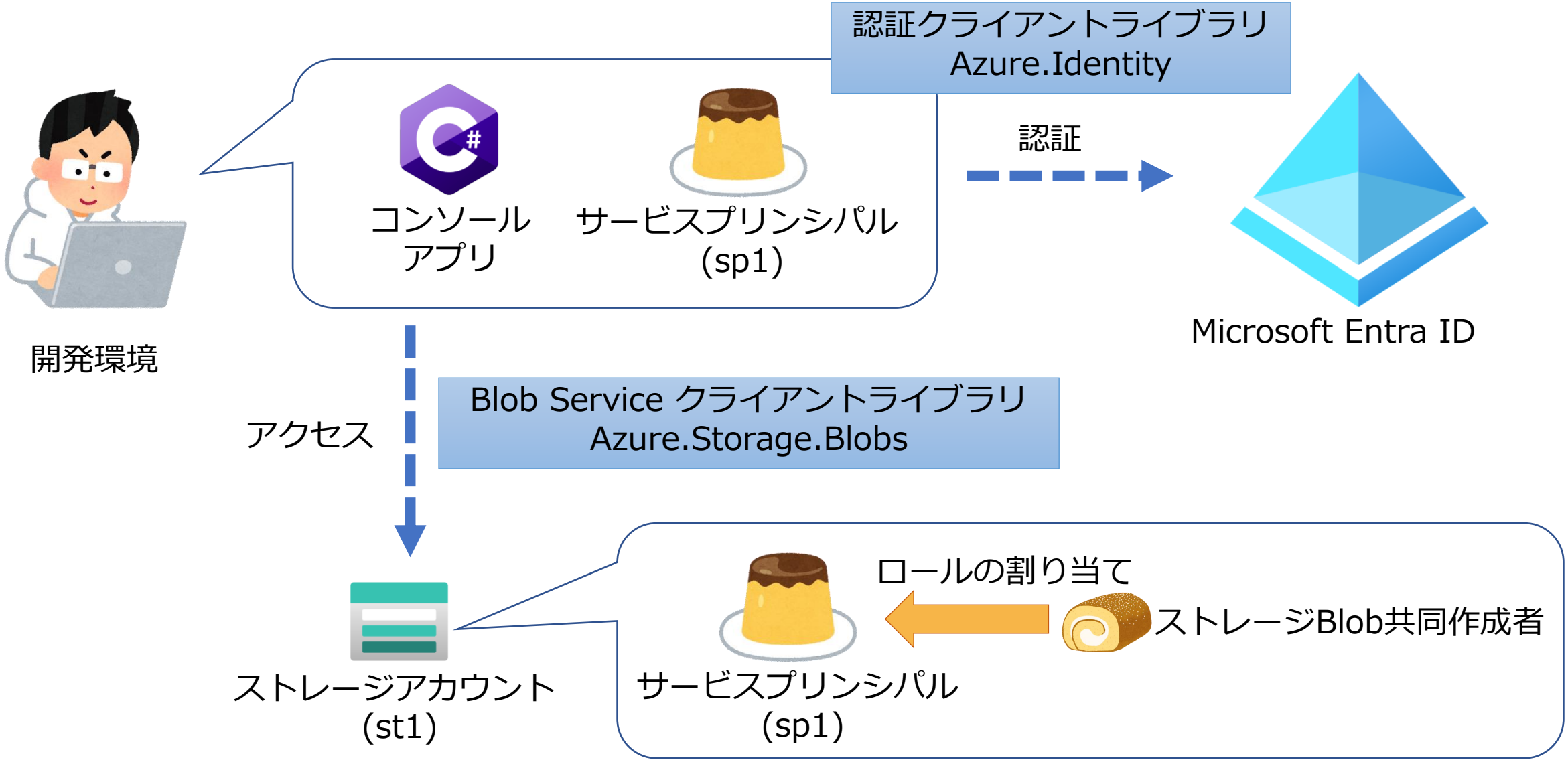
ストレージアカウント (st1)

グループ (group1)

ロールの割り当て

ストレージBlob共同作成者

■サービスプリンシパルの認証と承認



■マネージドIDの認証と承認