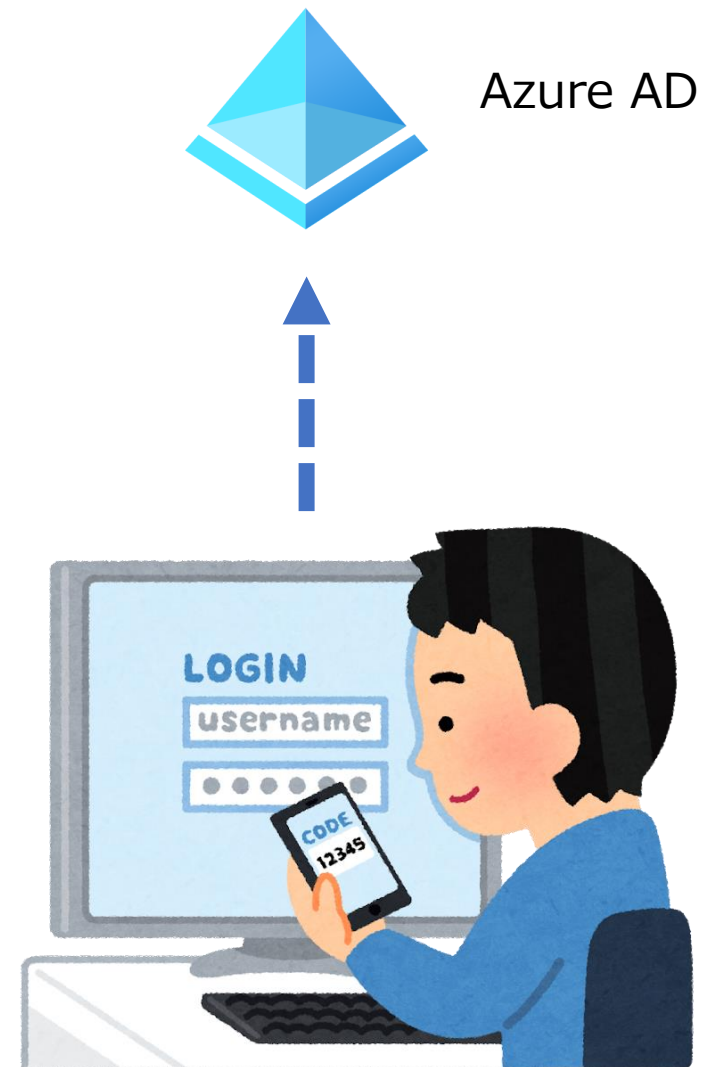


Azureの 認証と承認

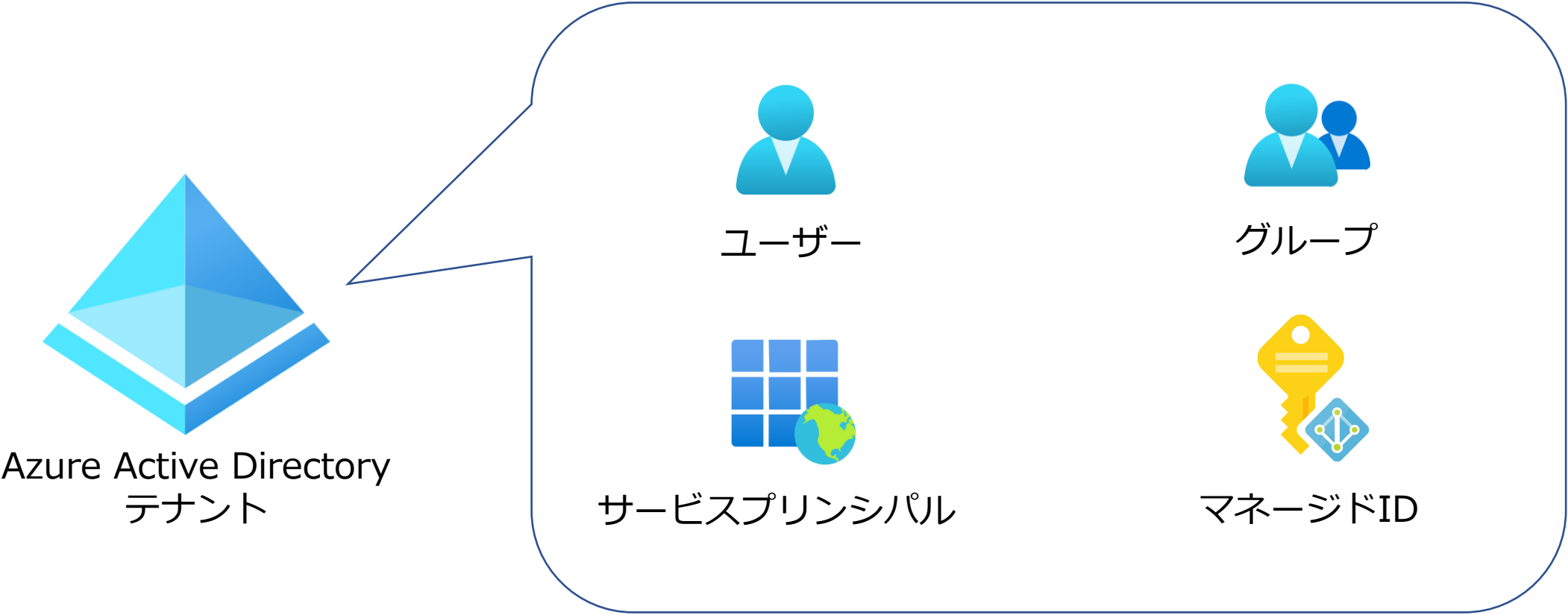
2023/3/1

認証

認証 = Azure AD認証



■ Azure AD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

■ Azure ADで管理されるID

az ad user create

az ad group create



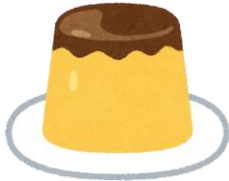
Azure Active Directory
テナント



ユーザー



グループ



サービスプリンシパル

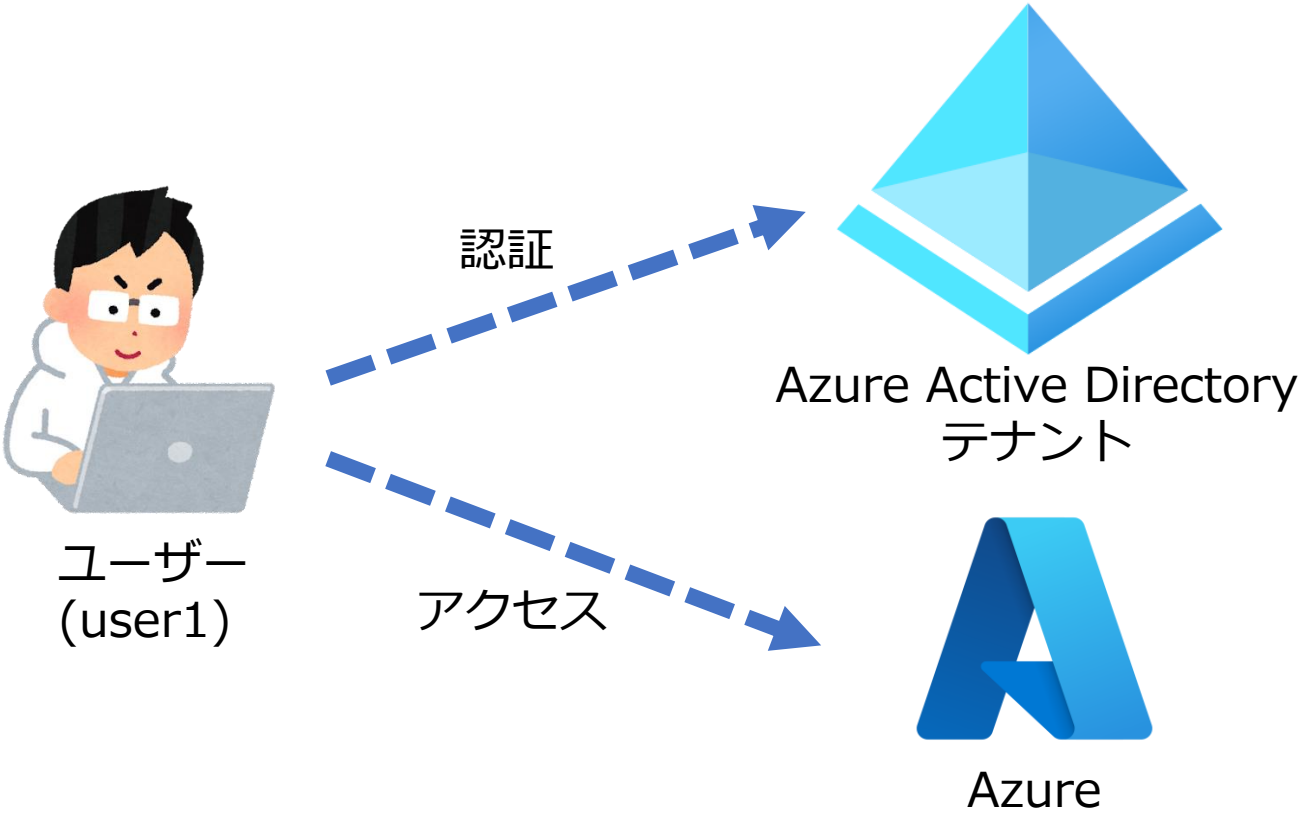


マネージドID

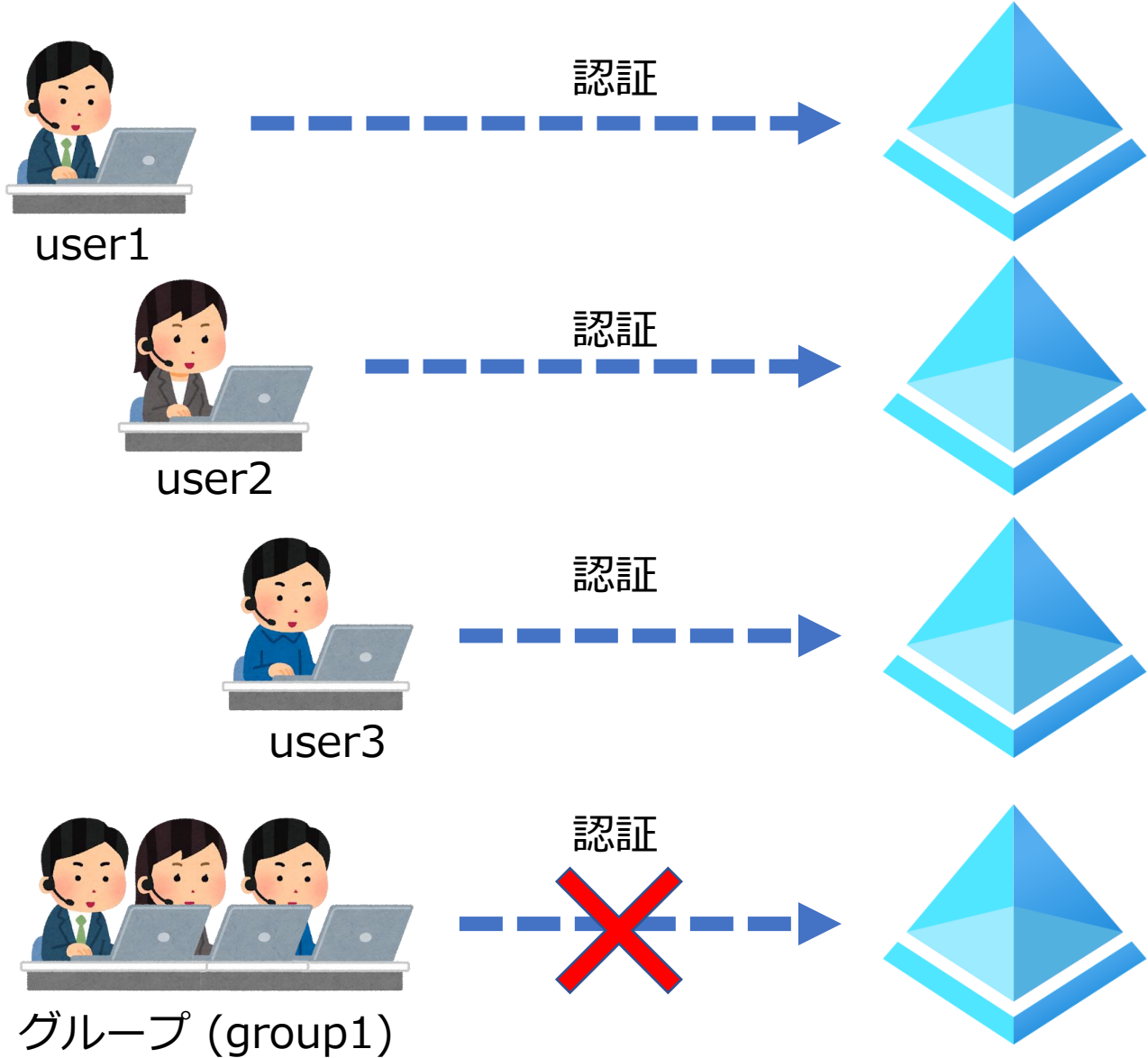
az ad sp create-for-rbac

az identity create

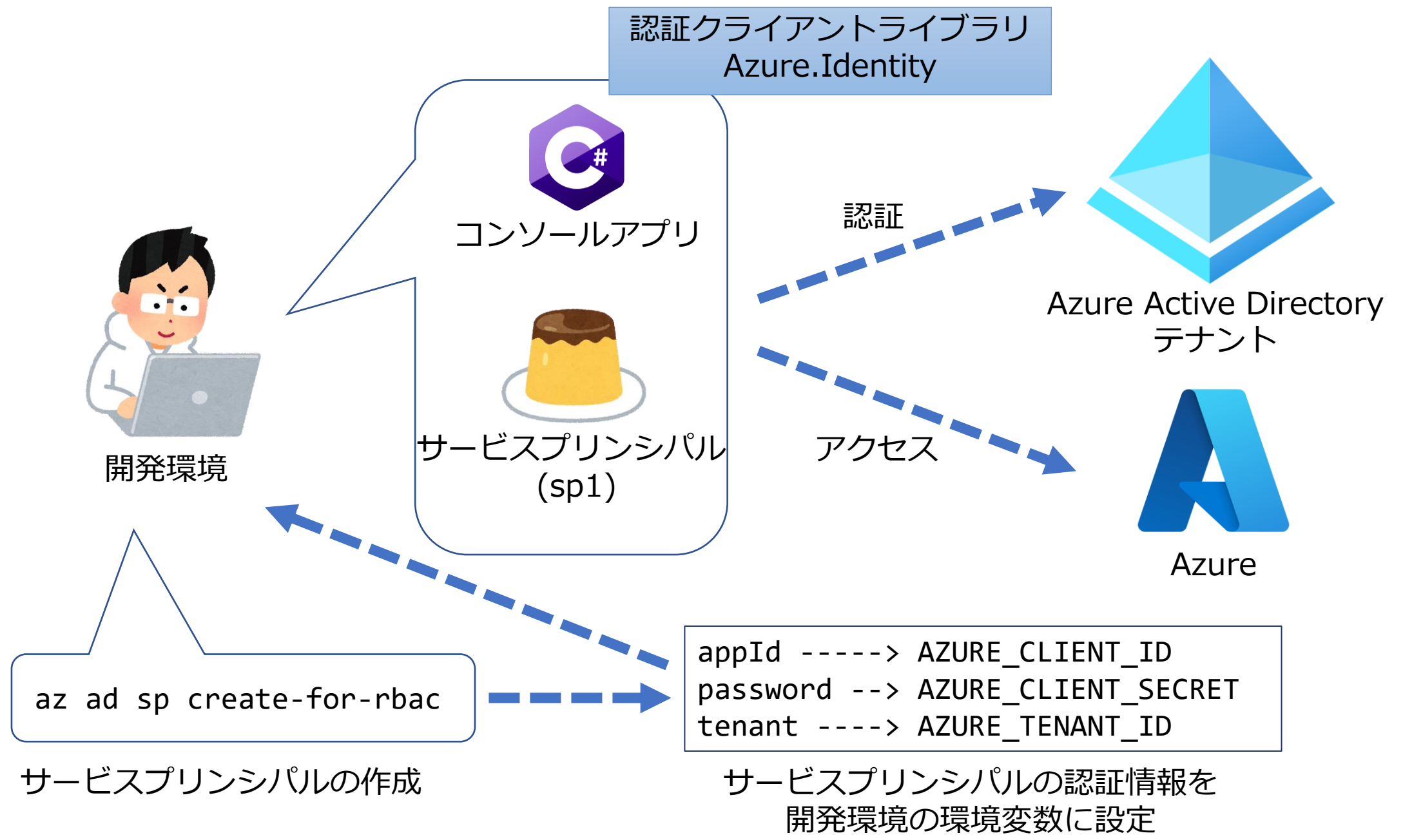
■ ユーザーの認証



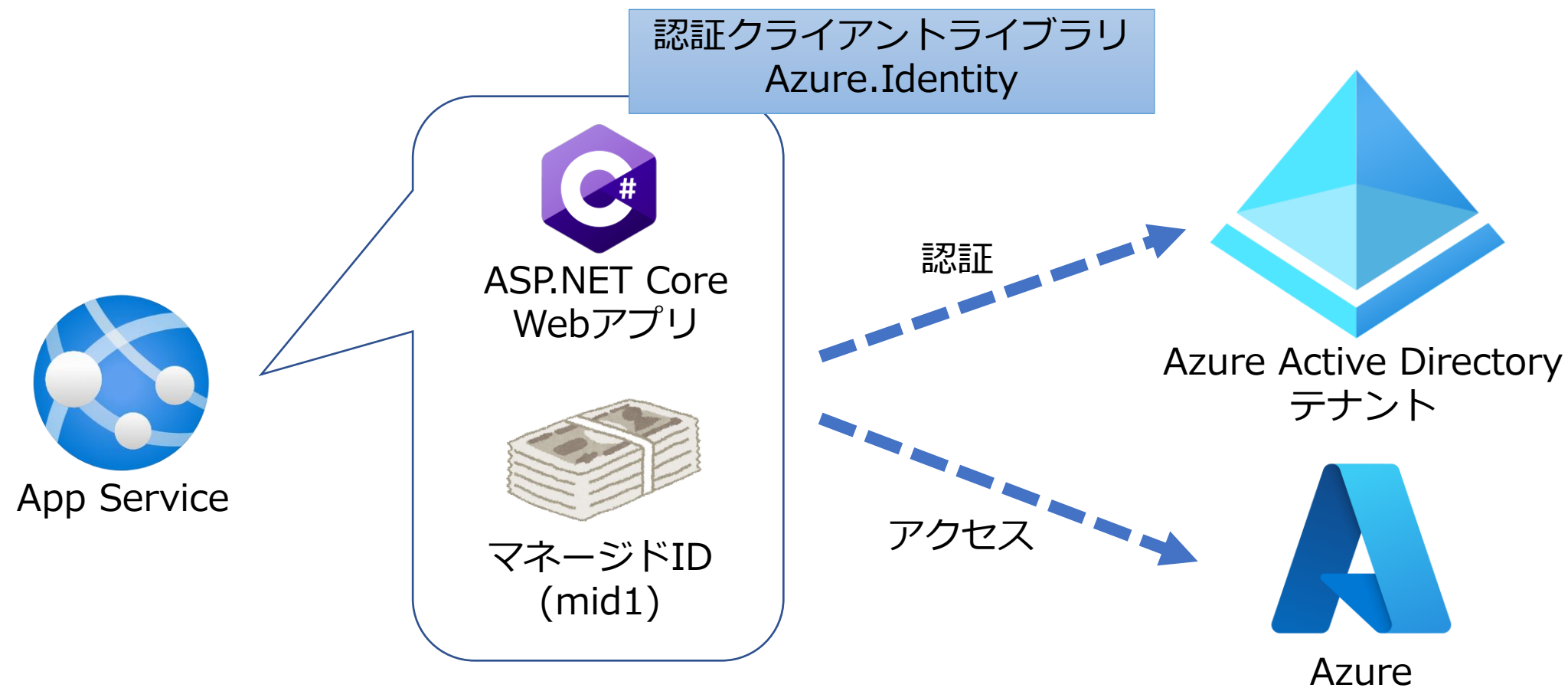
■グループ内の個々のユーザーは、それぞれ、ユーザーとしてサインインが可能だが、グループによる認証（グループとしてのサインイン）はできない。



■ 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]'
```


Examples

参考: az loginコマンドによるサインイン

Log in interactively.

```
az login
```

Log in with user name and password. This doesn't work with Microsoft accounts or accounts that have two-factor authentication enabled. Use -p=secret if the first character of the password is '- '.

```
az login -u johndoe@contoso.com -p VerySecret
```

Log in with a service principal using client secret. Use -p=secret if the first character of the password is '- '.

```
az login --service-principal -u http://azure-cli-2016-08-05-14-31-15 -p VerySecret --tenant contoso.onmicrosoft.com
```

Log in with a service principal using client certificate.

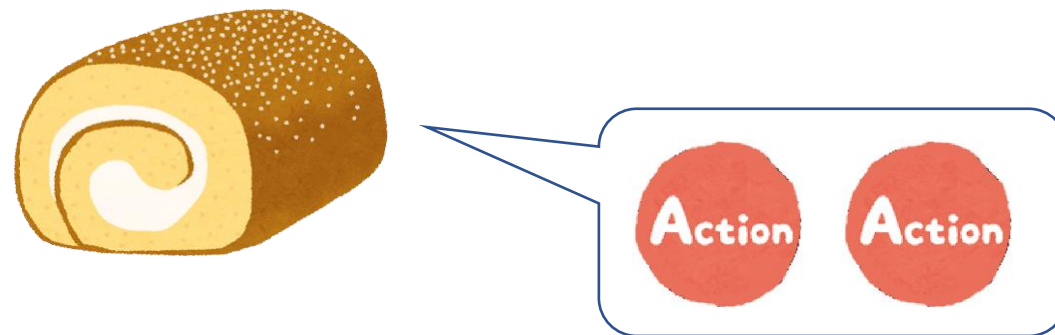
```
az login --service-principal -u http://azure-cli-2016-08-05-14-31-15 -p ~/mycertfile.pem --tenant contoso.onmicrosoft.com
```

Log in using a VM's system-assigned managed identity.

```
az login --identity
```

Log in using a VM's user-assigned managed identity. Client or object ids of the service identity also work.

```
az login --identity -u /subscriptions/<subscriptionId>/resourcegroups/myRG/providers/Microsoft.ManagedIdentity/userAssignedIdentities/myID
```



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

■ Azure RBAC以外のロール






Azure サブスクリプション

-  アカウント管理者
-  サービス管理者
-  共同管理者

従来のサブスクリプション管理者ロール





Azure AD

-  グローバル管理者
-  ユーザー管理者
-  ディレクトリ閲覧者

Azure ADの管理者ロール






Cosmos DB

-  Cosmos DB組み込みデータ共同作成者
-  Cosmos DB組み込みデータリーダー

Azure Cosmos DB
組み込みロール
(Cosmos DBに固有のロール)



SQL Database

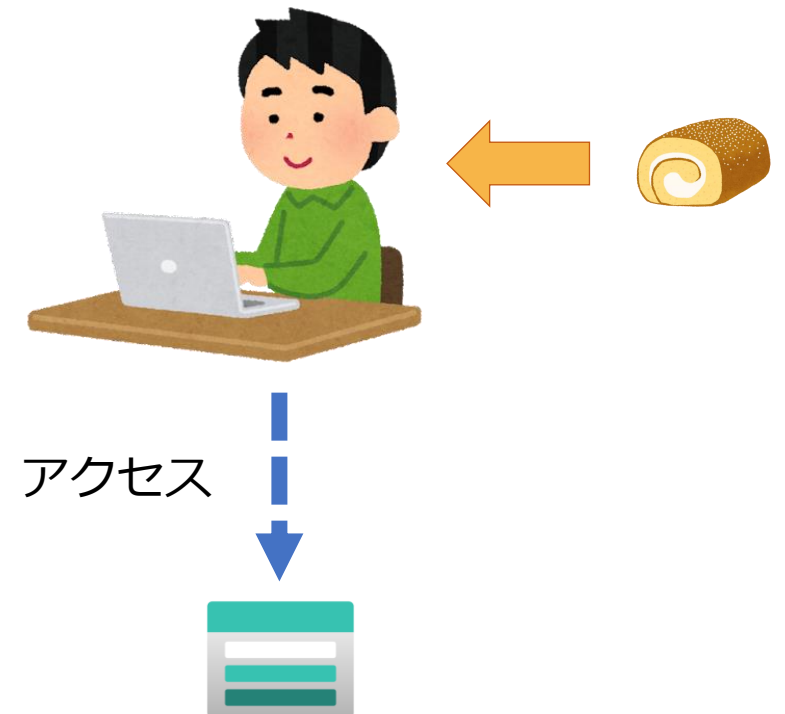
-  db_datareader
-  db_datawriter
-  db_owner

データベース レベルのロール
(固定データベース ロール / ユーザー定義データベース ロール)



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

ロール割り当てを行う「スコープ」

ロール割り当てを実行するために必要なロール

-  所有者
(Azure RBAC)
- or
-  ユーザーアクセス管理者
(Azure RBAC)
- or
-  サービス管理者
(従来のサブスクリプション管理者ロール)

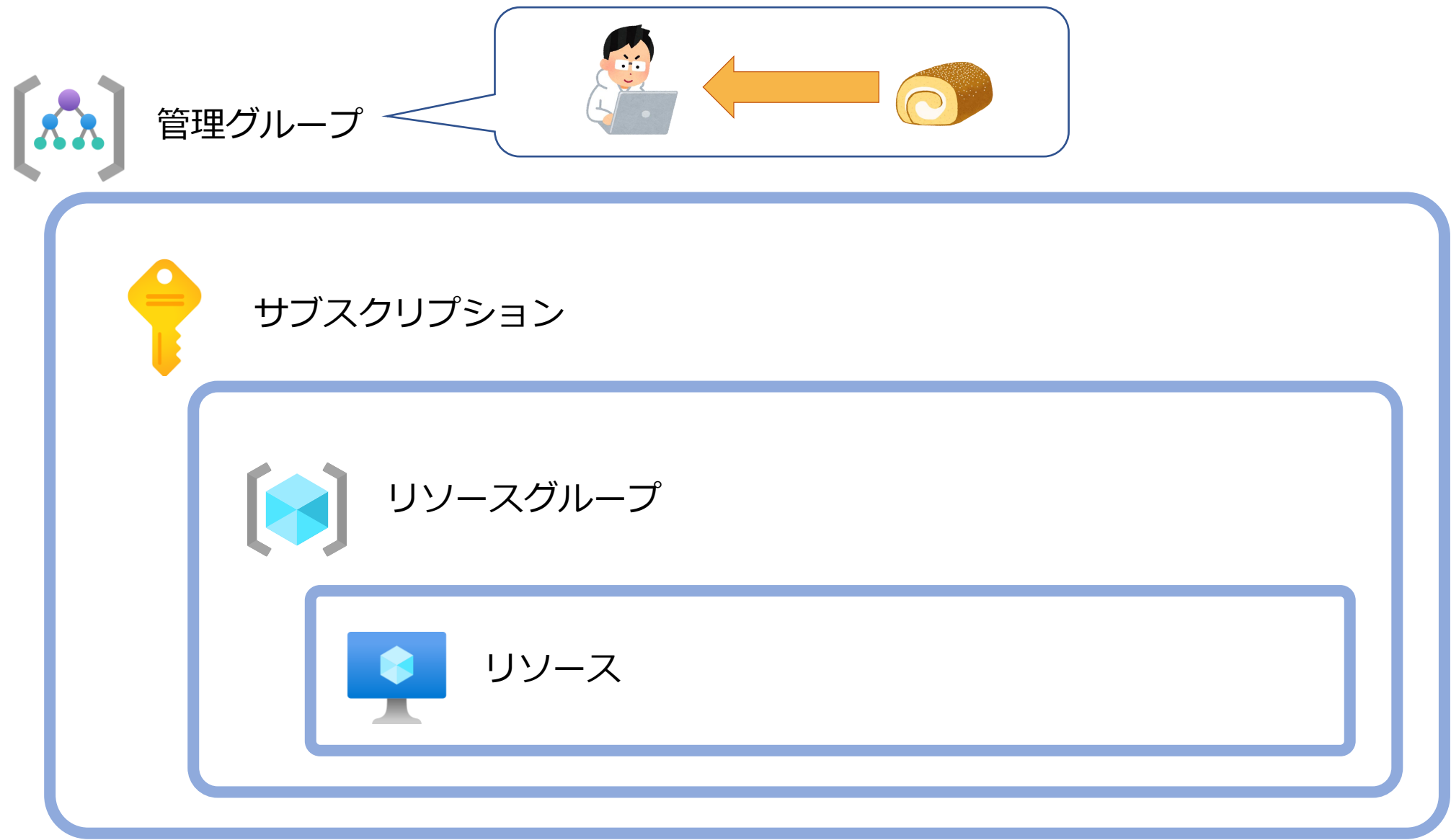
-  管理グループ
-  サブスクリプション
-  リソースグループ
-  リソース



```
az role assignment create
--role [ロール名]
--scope [スコープ]
--assignee [割り当て先のID]
```

ロールの割り当て
(「ロールの割り当て」の作成)

■ ロールの割り当てを行うスコープ



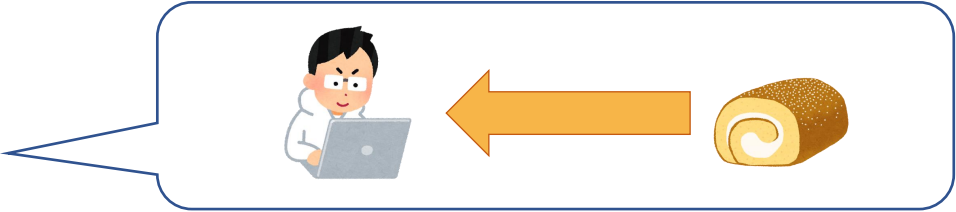
■ ロールの割り当てを行うスコープ



管理グループ



サブスクリプション



リソースグループ



リソース

■ ロールの割り当てを行うスコープ



管理グループ



サブスクリプション



リソースグループ



リソース

■ ロールの割り当てを行うスコープ



管理グループ



サブスクリプション



リソースグループ

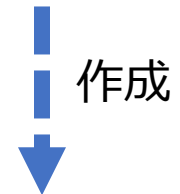


リソース

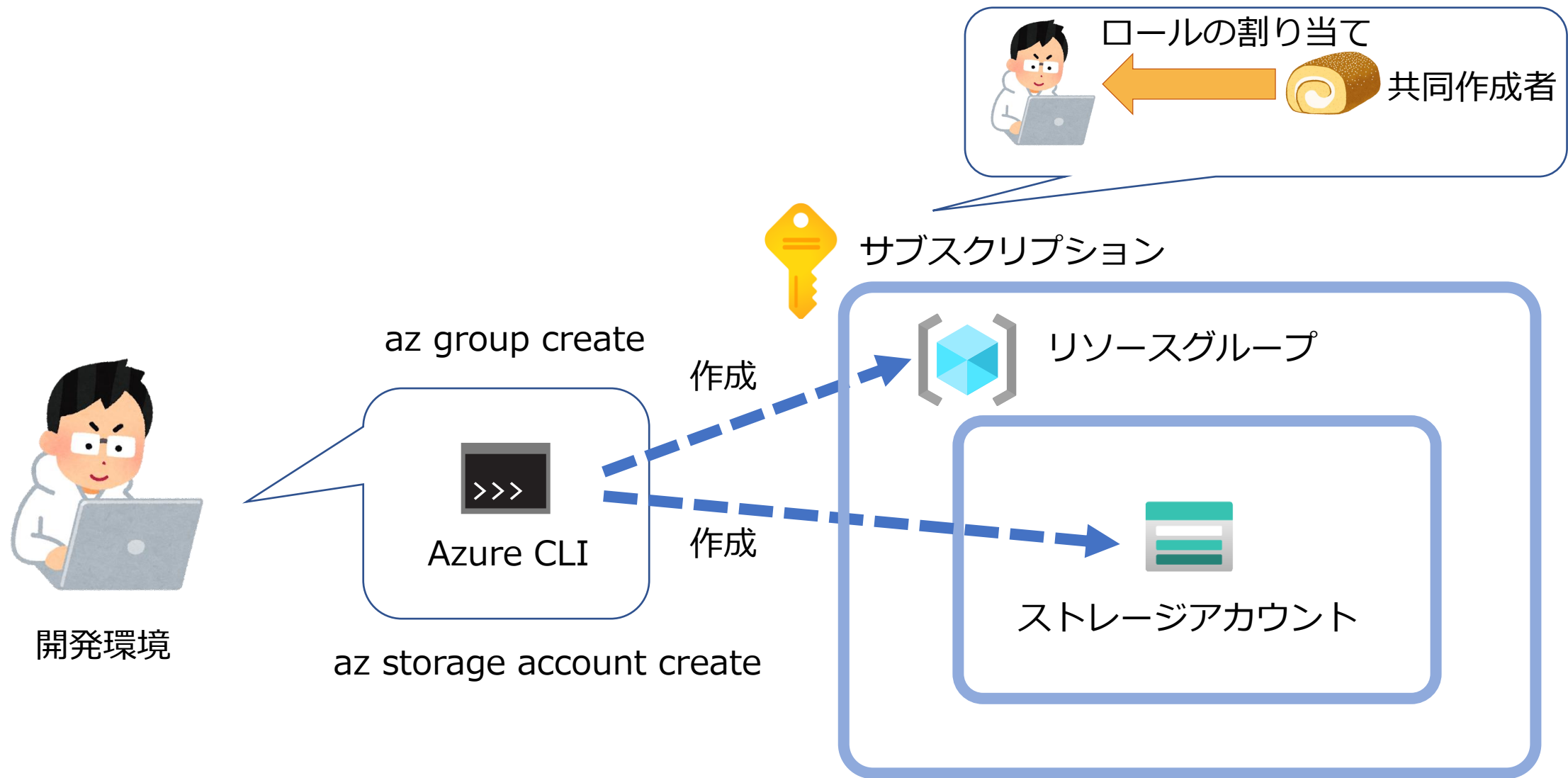


ロールの利用例(1) リソースの作成

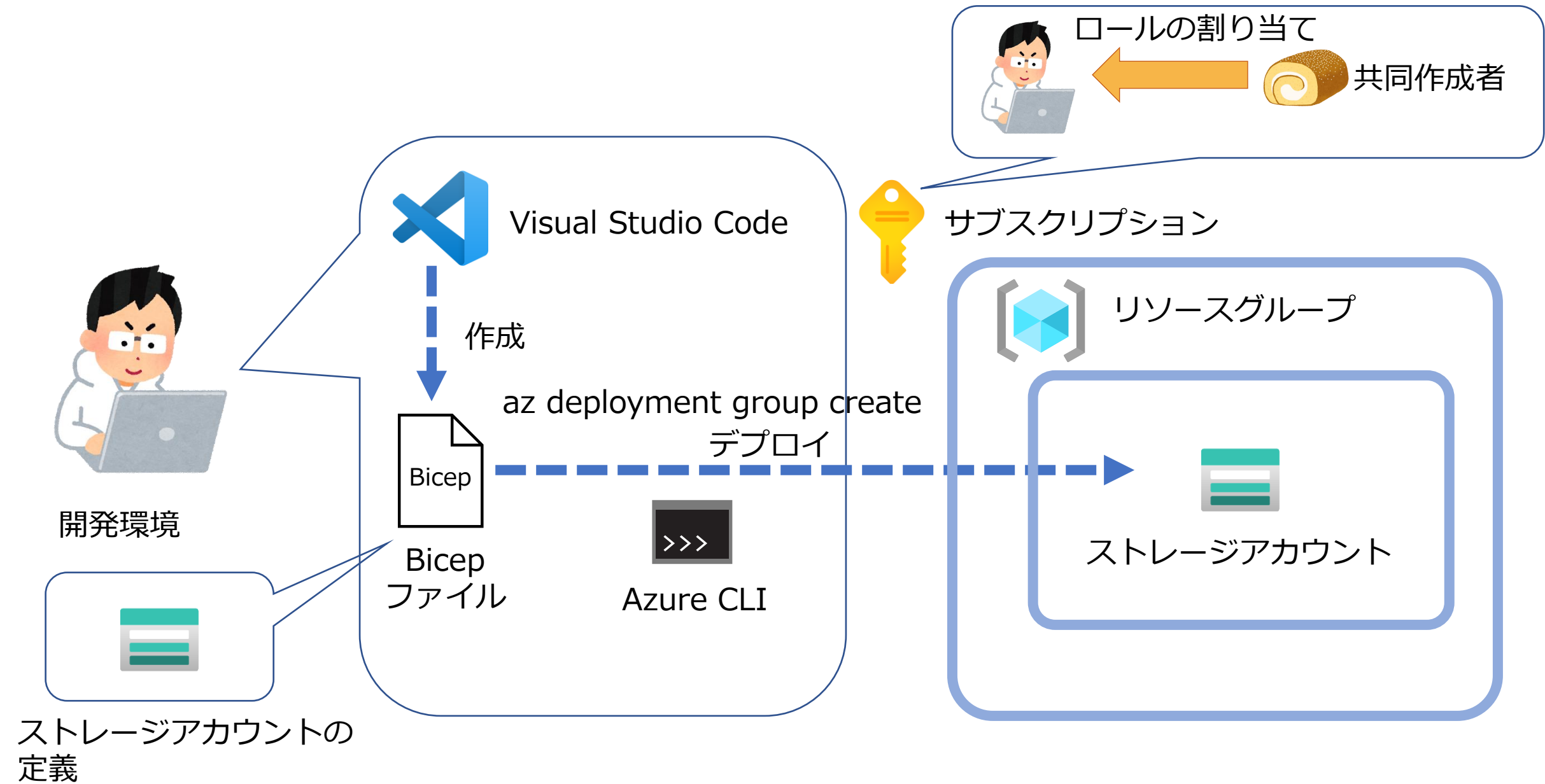
リソースを作成するためのロール割り当てが必要



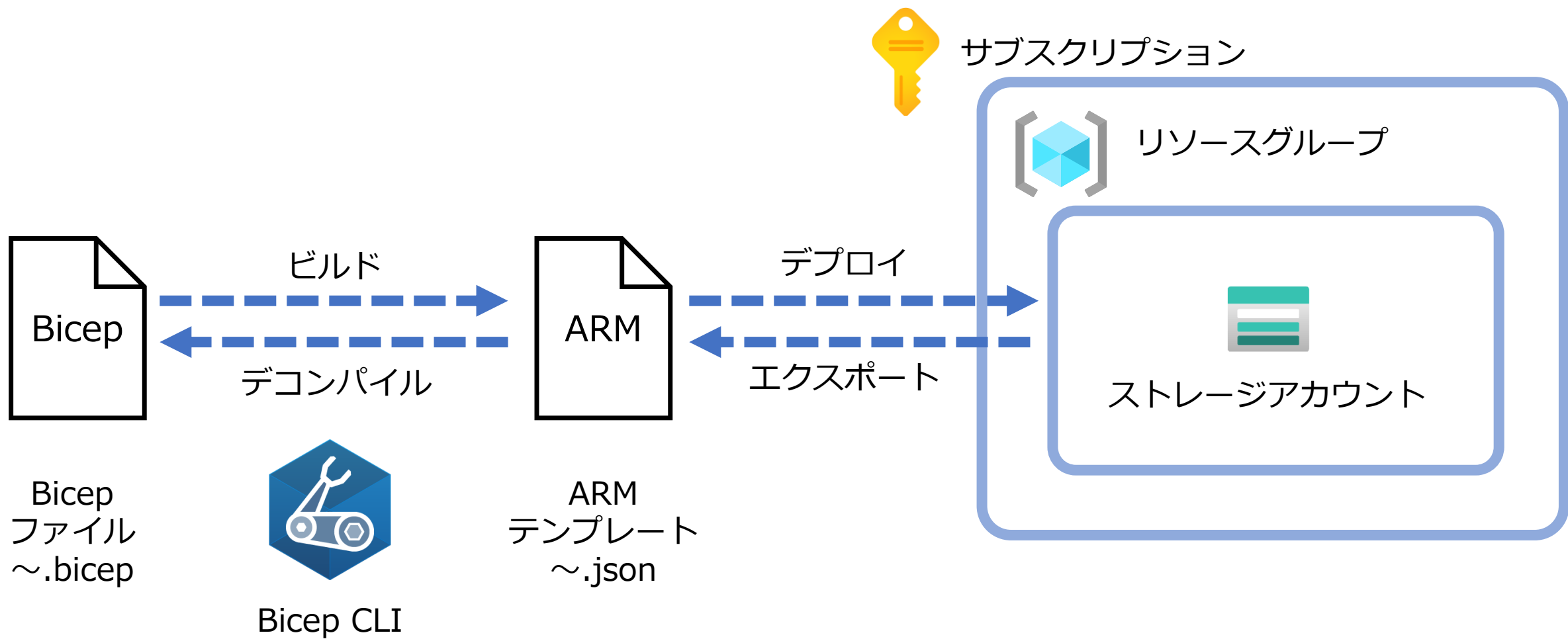
■ Azure CLIによるリソースの作成



■ Bicepによるリソースの作成



■参考: Bicepのしくみ

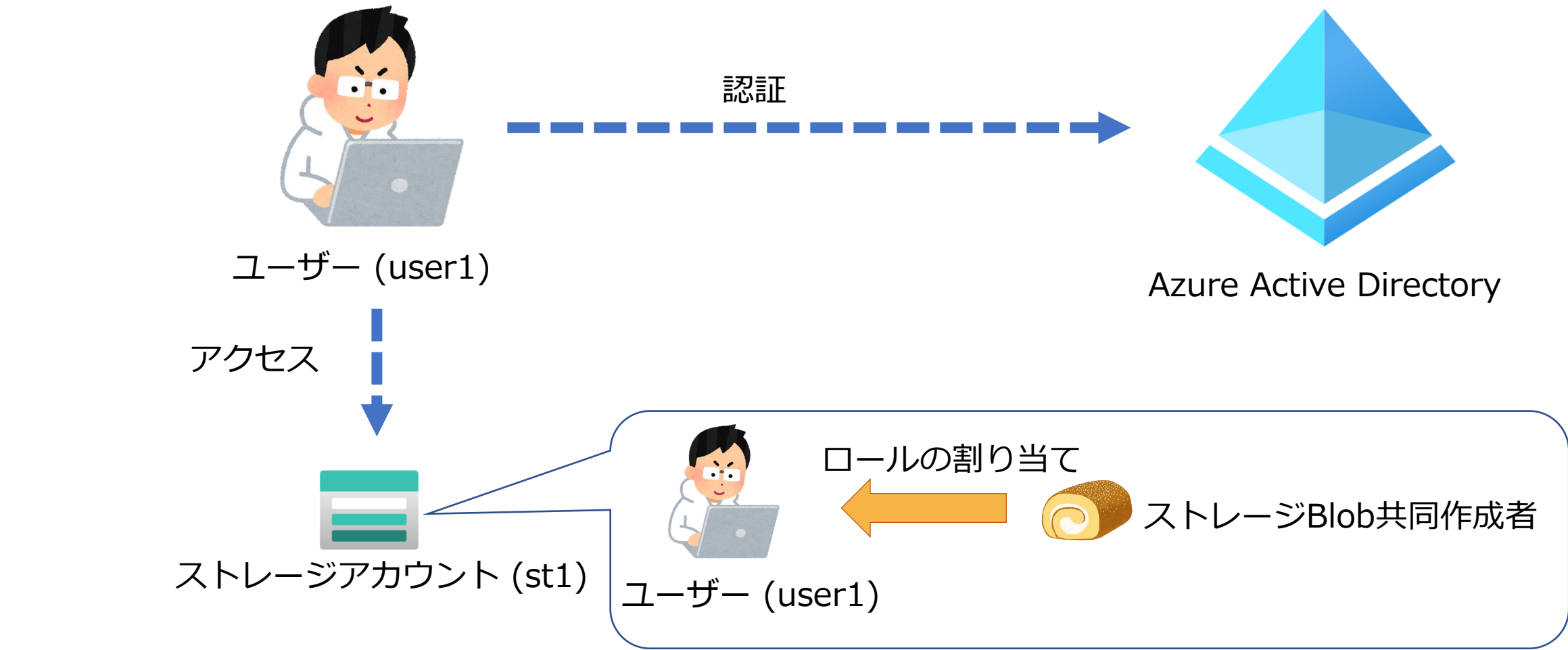


ロールの利用例(2) ストレージアカウント (Blob) へのアクセス

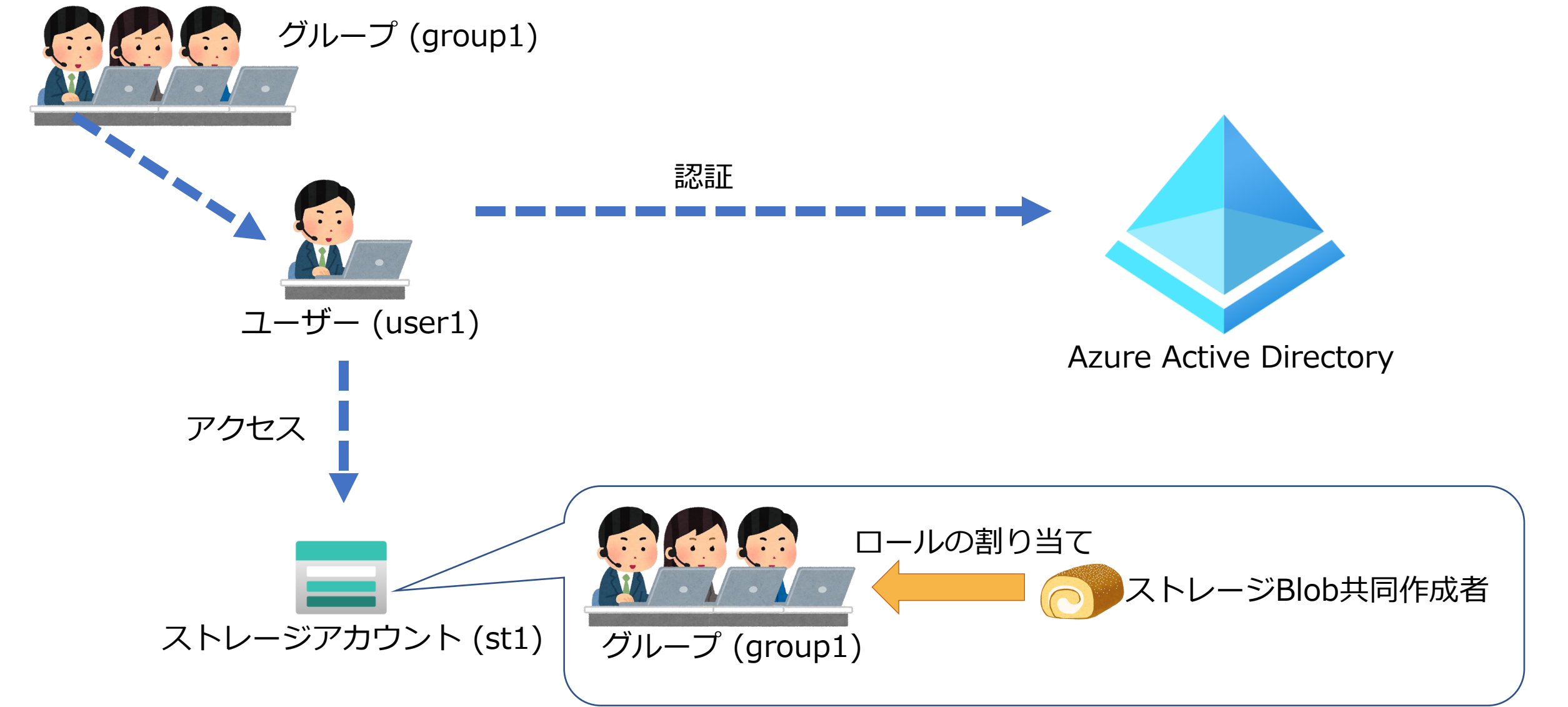
Blobの読み書きを行うための
ロールの割り当てが必要



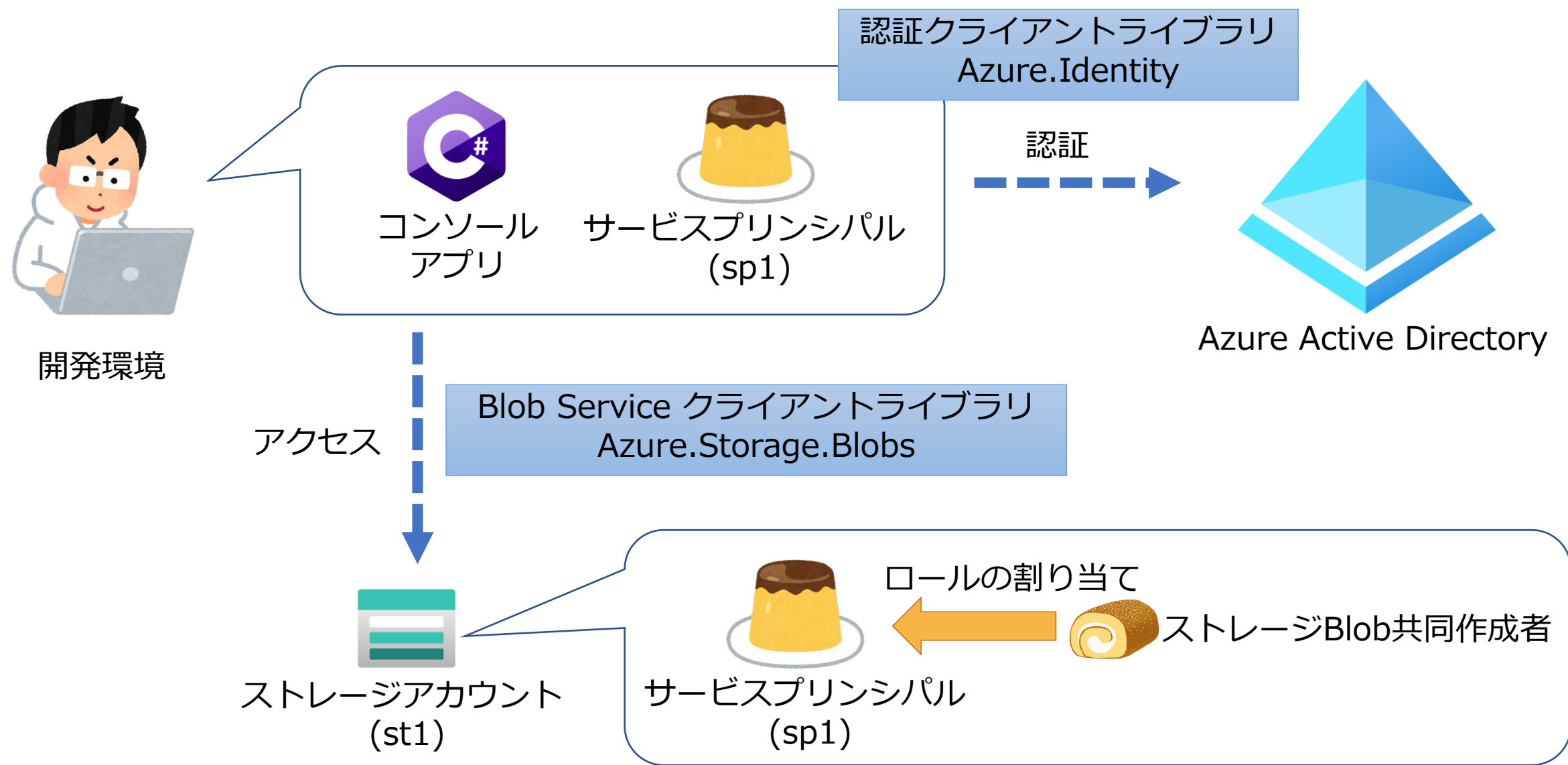
■ ユーザーの認証と承認



■グループ（に含まれるユーザー）の認証と承認



■ 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

