

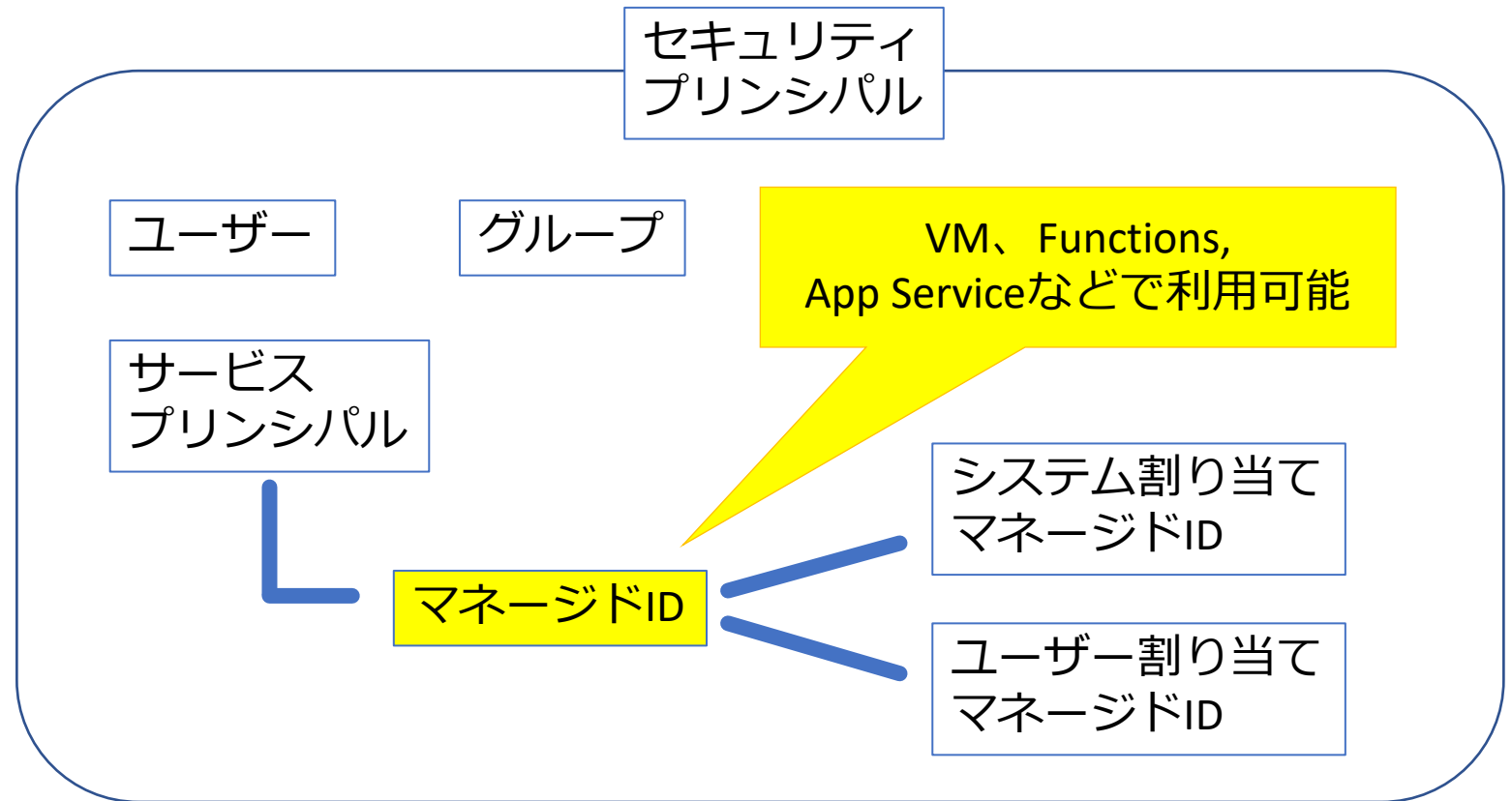
マネージドID

セキュリティ プリンシパルは、Azure リソースへのアクセスを要求するユーザー、グループ、サービス プリンシパル、またはマネージド ID を表すオブジェクトです。

マネージド ID は、Azure Active Directory で自動的に管理される ID を Azure サービスに提供します。

内部的には、**マネージド ID は特別な種類のサービスプリンシパル**であり、Azure リソースとだけ使用できます。

マネージド ID が削除されると、対応するサービスプリンシパルが自動的に削除されます。

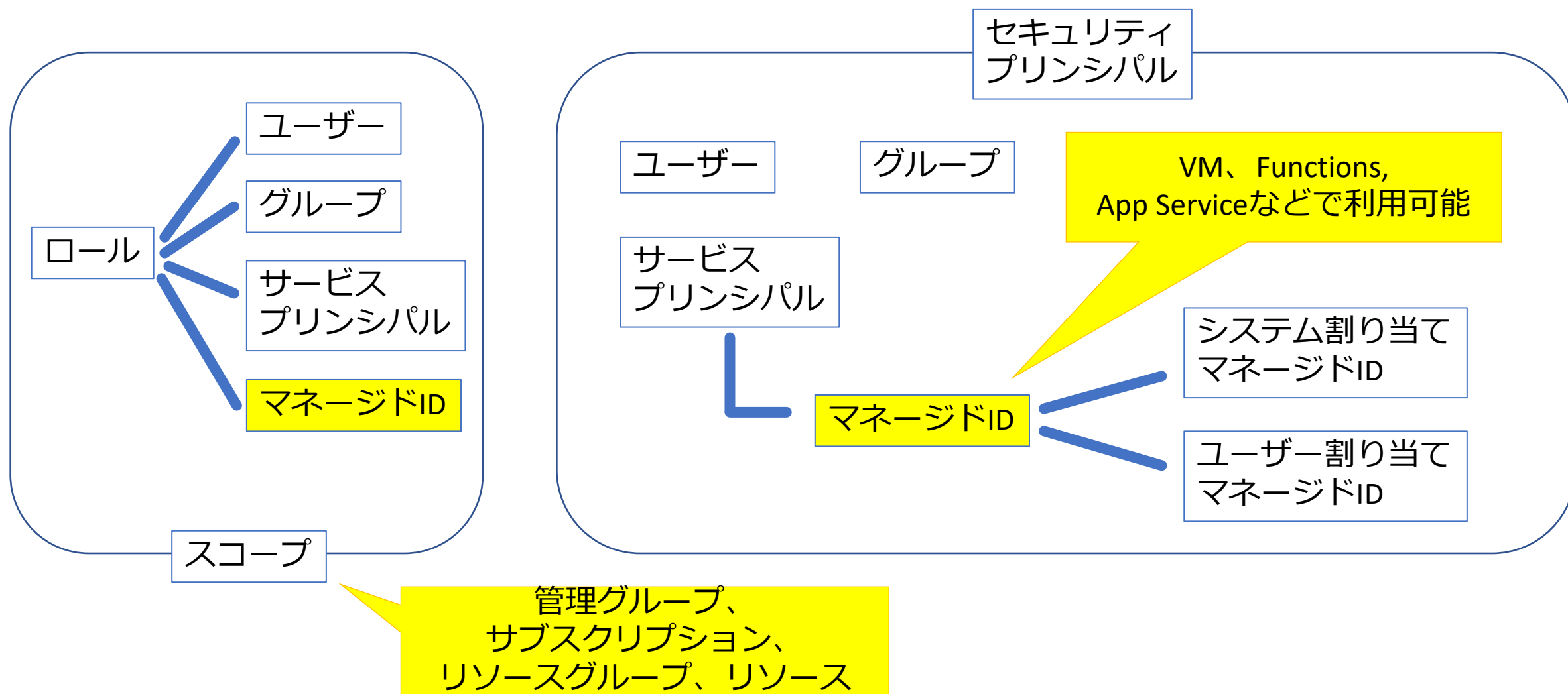


<https://docs.microsoft.com/ja-jp/azure/active-directory/managed-identities-azure-resources/how-managed-identities-work-vm#how-it-works>

<https://docs.microsoft.com/ja-jp/azure/role-based-access-control/overview#security-principal>

ロールの割り当て

セキュリティプリンシパルのいずれかに、ロールを割り当てることができます。



マネージドIDとサービスプリンシパルの使い分け

サービスプリンシパルを使用する場合

- ・アプリケーションまたはサービスが**オンプレミスで実行されている場合**。
- ・アクセスする必要があるリソースまたはアプリケーションで、**マネージド ID がサポートされていない場合**。

Azure 内で認証を処理するための最も安全で便利な方法は、**マネージド ID を使用する**ことです。