# 第7章 ユーザーおよびセキュリティの管理

# 7-1 ユーザーの作成・変更・削除

## 7-1-1 ユーザーの作成

- 管理ユーザー
  - 管理用ユーザーをアプリケーションのデータ管理/処理で使用してはいけない

| アカウント | 説明 |
|---|---|
| SYS | データベースの起動/停止を含むすべての操作を実行できる管理用ユーザー<br>データディクショナリの実表とビューの所有者 |
| SYSTEM | データベースの起動/停止などの一部をのぞき、ほぼすべての操作を実行できる管理用ユーザー |

CREATE USERコマンド

| 属性 | 説明 |
|---|---|
| ユーザー名 | 新規に作成するユーザー名 |
| パスワード | Oracleに接続するときに指定するパスワード |
| デフォルト表領域 | 格納先表領域を指定せずにオブジェクトを作成した場合に格納先となる表領域 |
| デフォルト一時表領域 | 大量のデータ処理（ソートなど）を実行するときに使用される一時表領域 |
| 表領域のクオータ | 表領域を使用できるサイズの上限（割り当て制限）。なお、サイズとしてUNLIMITEDを指定した場合、その表領域を無制限に使用できる |
| プロファイル | パスワードポリシーまたはリソース制限。 |
| パスワード期限切れ | 初回ログイン時にパスワードの設定を必要とするかどうか |
| アカウントロック | 一時的にログイン不可状態とするかどうか |

```
CREATE USER ユーザー名
 --パスワードを指定する
 IDENTIFIED BY パスワード
 --デフォルト表領域を指定する
 DEFAULT TABLESPACE 表領域名
 --一時表領域名を指定する
```

```
TEMPORARY TABLESPACE 表領域名
--ユーザーが使用できる表領域のサイズを指定する
QUOTA [サイズ | UNLIMITED] ON 表領域名
--プロファイルを指定する
PROFILE [プロファイル名 | DEFAULT]
--アカウントが使用可か不可かを指定する
ACCOUNT [LOCK | UNLOCK]
--次回ログイン時にパスワードの変更が必要になるように指定する
PASSWORD EXPIRE
```

## ユーザ名とパスワードの規則

### ユーザー名の制限

- 長さは30バイト以内（12c R1以前）、または、128バイト以内（12c R2以降）
- 以下の場合は、ユーザー名をダブルクォートで囲む
    - 英数字および「$」「_」「#」以外の文字を使用した場合
    - 先頭にアルファベット以外の文字を使用した場合
    - Oracleの予約語を使用した場合
    - アルファベットの大文字/小文字を区別する場合
- データベース内で名前は一意に保つ

### パスワードの制限

- 長さは30バイト以内
- 以下の場合はパスワードをダブルクォートで囲む
    - 英数字および「$」「_」「#」以外の文字を使用した場合
    - 先頭にアルファベット以外の文字を使用した場合
    - Oracleの予約語を使用した場合

### 表領域のクオータ

- **自分にクオータが割り当てられていない表領域に表や索引を作成することはできない**
    - **つまり、デフォルト表領域を指定しても、そこへのクオータが割り当てられていなければ利用できない**

### 表領域の割り当て

- 表領域の割当て制限を「0MB」に変更すると、その表領域に新しい領域を確保できなくなります。しかし、割当て制限の変更は、既にオブジェクト用に確保された領域には影響しません。新しい領域を確保する必要がないオブジェクトへの操作(確保済みのエクステントで行われる更新や挿入など)は引き続き実行できます。データの増加で新しい領域の確保が必要となった時、領域を確保できずエラーとなります。

### ユーザーのデフォルト表領域

- ユーザー作成時にデフォルト表領域の指定を省略した場合、そのユーザーのデフォルト表領域は、データベースのデフォルト表領域になる

## 7-1-2 プロファイル

- パスワードポリシーをまとめたセット
- すべてのユーザーには、いづれかのプロファイルを割り当てる必要がある
- 省略した場合は、DEFAULTという名前のプロファイルが割り当てられる

| **設定可能なパラメータ** | **説明** | **デフォルト値** |
|---|---|---|
| PASSWORD_LIFE_TIME | パスワードの有効期限(日数) | 180日 |
| PASSWORD_GRACE_TIME | パスワードの有効期限が終了した場合、警告は出されるが、<br>ログインしてパスワードを変更することが許可される猶予期間 | 7日 |
| PASSWORD_REUSE_MAX | パスワードを再利用できるようになるまでの変更回数。<br>PASSWORD_REUSE_TIMEと組み合わせて設定する | UNLIMITED |
| PASSWORD_REUSE_TIME | パスワードを再利用できない日数。<br>PASSWORD_REUSE_MAXと組み合わせて設定する | UNLIMITED |
| PASSWORD_VERIFY_FUNCTION | パスワードルールを実装したPL/SQL関数名を指定。<br>パスワードの文字数や使用可能な文字の指定などが可能 | NULL |
| FAILED_LOGIN_ATTEMPS | 指定した回数連続してログインに失敗するとアカウントがロックされる | 10回 |
| PASSWORD_LOCK_TIME | FAILED_LOGIN_ATTEMPTSに指定された回数連続してログインに失敗したときにアカウントがロックされる日数 | 1日 |

## ユーザーの属性の変更

- ユーザー名以外のユーザー属性はALTER USERコマンドであとから変更が可能

## ユーザーのロック

- 特定のデータベース・ユーザーのデータベースへのアクセスを一時的に拒否したい場合、データベース管理者はユーザー・アカウントをロックできます。ロックされたユーザーは、データベースへ接続しようとするとエラーとなり、接続を許可されません。接続中のユーザーがロックされた場合は、次回のログインよりロックが有効になります。

## ユーザーの削除

- DROP USER コマンドで削除
    - データベースに接続中のユーザーは削除できない
    - ユーザーが表や索引などオブジェクトを所有している場合は、あらかじめオブジェクトを削除しておくか、**CASCADE**コマンドを指定する
    - ユーザーを削除するとユーザー所有しているオブジェクトも削除される

# 7-2 権限の管理

## 7-2-1 権限とは

- 2種類に分類できる

| 権限 | 概要 | 権限付与の対象となる操作（カッコ内は権限名） |
|---|---|---|
| システム権限 | データベースに対してどのような操作を許可するか | ・データベースにログインする（CREATE SESSION）<br>・表を作成する（CREATE TABLE）<br>・表領域を作成する（CREATE TABLESPACE）<br>・ユーザーを作成する（CREATE USER） |
| オブジェクト権限 | オブジェクトに対してどのような操作を許可するか<br>オブジェクトが削除されると、そのオブジェクト権限も自動削除 | ・検索する（SELECT）<br>・新規行を挿入する（INSERT）<br>・既存値を更新する（UPDATE）<br>・既存行を削除する（DELETE） |

### 権限の付与、取り消し

```
# システム権限をユーザーに付与する
GRANT システム権限名 TO ユーザ名;

# システム権限をユーザーから取り消す
REVOKE システム権限名 FROM ユーザ名;
```

```
# オブジェクト権限をユーザーに付与する
GRANT オブジェクト権限名 ON オブジェクト TO ユーザ名;

# オブジェクト権限をユーザーから取り消す
REVOKE オブジェクト権限名 ON オブジェクト FROM ユーザ名;
```

### システム権限

- ほかのユーザーにシステム権限（データベースにログインなど）を付与するには「**ADMIN**」オプションを指定して、システム権限を付与する必要がある
- **GRANT ANY PRIVILEGEシステム権限**が付与されていると、すべてのシステム権限をほかのユーザーに付与できる

### オブジェクト権限

- 「オブジェクト権限を付与されたユーザーが、さらに他ユーザーにそのオブジェクト権限を付与する」ことを許可する**GRANTオプション**を指定する
- **GRANT ANY OBJECT PRIVILEGEシステム権限**が付与されると、すべてのオブジェクト権限をほかのユーザに付与できる

### 権限が不要な操作

- 自分が所有するオブジェクトのすべての操作（SELECT,INSERTなど）
- 自分のパスワードの変更

## 7-2-2 ロール

- 複数の権限を一つにまとめたもの。
- ロールはパスワードで管理できます。パスワードで管理する場合は、ロールを付与され、且つロールのパスワードを知っているユーザーだけがロールを使用可能にできます。

### ロールを付与する/取り消す

```
GRANT ロール名 TO ユーザ名;
REVOKE ロール名 FROM ユーザ名;
```

- ロールと権限の付与は同時に実施できる

### 事前定義済みロール

| **ロール** | **説明** |
|---|---|
| CONNECT | CREATE SESSIONのみ。データベースへの接続を可能にする。<br>OEMを利用してユーザを作成すると自動的に付与 |
| RESOURCE | スキーマオブジェクトの作成、変更、削を可能にする。<br>開発者など向け |
| DBA | SYS/SYSTEMにデフォルトで付与。<br>「インスタンスの起動/停止」「バックアップ/リカバリ」の権限は含まれない |
| SELECT_CATALOG_ROLE | データディクショナリ内のオブジェクトに対するSELECT権限 |
| EM_EXPRESS_BASIC | EM Expressに接続して、読み取り専用モードでページを表示する権限 |
| EM_EXPRESS_ALL | EM Expressに接続して、すべての機能を使用できる権限 |

## 7-2-3 管理権限 - SYSDBA権限/SYSOPER権限

- SYSユーザは、DBAロールに加えて**SYSDBA権限**が付与されている
    - 「インスタンスの起動/停止」「バックアップ/リカバリ」ができる
- SYSTEMユーザには、管理権限が付与されていない
- **SYSOPER権限**も「インスタンスの起動/停止」「バックアップ/リカバリ」はできるが、以下でできない
    - 「データベースの作成と削除」

    - 「不完全リカバリ」
    - ユーザのデータにアクセス不可
    - PUBLICユーザーで接続される（SYSDBAはSYSユーザーで接続）

## 管理権限を持つユーザーの接続と認証

- AS SYSDBA または AS SYSOPERをつけてログイン
- データベースがオープンしていない状態でデータベースへ接続および認証できる必要があるので、以下の認証方法が用意されている
    - OS認証
        - OSDBAグループにOSユーザーが所属している場合、スキップ
    - パスワードファイル認証