データベース操作監査（不正アクセス検知のための設定）

データベース操作に対する監視内容は、以下の４つがあります

【必須監査】

データベースの起動や停止、管理者権限ユーザーのリスナー経由での接続に対して、その記録が、アラートログに出力されます

【SYS 管理ユーザーの監査】

管理者権限ユーザーが行った操作記録をログに出力します

初期化パラメータ AUDIT_SYS_OPERATIONS の値設定により指定した操作が対象になります（例、アクセスした時間　実行した SQL 文）

ログの出力先

初期化パラメータ AUDIT_TRAIL＝db の場合

SYS ユーザーの sys.AUD$表

初期化パラメータ AUDIT_TRAIL＝以外の場合

初期化パラメータ AUDIT_FILE_DEST で指定した場所に、ログファイルが出力される

ログ出力例

Sat　Mar　10　09:45:46　2016
ACTION：‘insert into scott.table1 values(1, ”こずえ”)’
DATABASE USER：/
PRIVILEGE：SYSDBA
CLIENT USER：yamada
CLIENT TERMINAL：PC-1
STATUS：0

【標準監査（一般ユーザーの操作監査)】

一般ユーザーが行った操作記録をログに出力します
初期化パラメータ AUDIT_TRAIL の値設定により指定した操作が対象になります
（例、アクセスした時間　実行した SQL 文）

ログの出力先
初期化パラメータ AUDIT_TRAIL＝db の場合
SYS ユーザーの sys.AUD$表
初期化パラメータ AUDIT_TRAIL＝以外の場合
初期化パラメータ AUDIT_FILE_DEST で指定した場所に、ログファイルが出力される

【ファイングレイン監査】

監査対象のオブジェクトや、オブジェクトの中の列名を決め、監査する操作方法（SELECT or UPDATE など）を設定することにより、監査対象の操作記録がログ出力されます

ログの出力先
SYS ユーザーの FGA_LOGS$表
この情報を見るためには、DBA_FGA_AUDIT_TRAIL ビューを SELECT します

注意事項

操作記録がログとして保存されるテーブルには、大量のレコードが保存されることになります
ディスク残量不足が発生しないように、不要となった情報を削除すること