障害回復

授業計画

第1回　ガイダンス・データベースの基本概念
第2回　データモデル
第3回　関係代数
第4回　データベース設計
第5回　リレーションの正規化
第6回　中間まとめ
第7回　関係データベース言語（SQL1）
第8回　関係データベース言語（SQL2）
第9回　計算機実習
第10回　データの検索機構　MySQL実習
第11回　トランザクション管理　MySQL実習
第12回　障害回復　MySQL実習
第13回　分散データベース　MySQL実習
第14回　期末まとめ
第15回　応用技術と将来動向　MySQL実習

講義内容

- 障害回復の概要
- ロールフォワードとロールバック
- ログファイル
- チェックポイント
- 障害への対応

１．障害回復の概要

- DBMSはコンピュータ上で動作するために，停電やハードウェア障害の危険性を絶えず抱えている。
- 障害回復機能は，トランザクションのACID特性の中で原子性，一貫性，耐久性を維持するために重要な機能である。

- トランザクション障害（transaction failure）：
  - 論理的な誤動作によるプログラム障害である。
  - データベース操作の失敗，データの不備，資源不足，デッドロック，論理エラーなとによって発生する障害である。
  - 障害回復は，トランザクション開始後に行ったすべての更新作業を取り消し，ロールバックし再スタートする。

１．障害回復の概要

■ システム障害（system failure）：

- ソフトウェアやハードウェアのトラブルによりシステムが停止する障害である。
- 障害回復は，データベースの一貫性が保証されるチェックポイントまでロールバックし，コミットしたトランザクションはロールフォワードにより処理が完了した状態に復旧させる。
- コミットしていないトランザクションはロールバックし再スタートする。

１．障害回復の概要

■ メディア障害（media failure）：

- データを格納している記憶媒体の故障により，データの読み書きができなくなり，データベースの一部または全部を失ってしまう障害である。
- 事前に複写されているバックアップコピーを記憶媒体上に戻し，ログファイルを利用して障害直前の状態にロールフォワードし復旧させる。

１０．障害回復

２．ロールフォワードとロールバック

- トランザクションの**原子性**を保障するためには，トランザクション中で実行した全ての更新をデータベースに反映するか，全て取り消す必要がある。
- 障害が発生した時点でトランザクションが実行中で**未コミット**であれば，そのトランザクション中で実行した全ての更新を**取り消す**必要がある。
- トランザクション中で実行した全ての更新を取り消して，障害回復を行うことを**ロールバック**（**後退復帰**または**UNDO**）という。

１０．障害回復

２．ロールフォワードとロールバック

- トランザクションがコミットされたが，まだ2次記憶装置に書き込まれていない更新がある場合には，そのトランザクションを再実行して，そのトランザクション中で実行した全ての更新をデータベースに反映させる必要がある。
- トランザクション中で実行した全ての更新を再実行して，障害回復を行うことを**ロールフォワード**（前進復帰または**REDO**）という。

２．ロールフォワードとロールバック

障害種類とロールバック･ロールフォワードとの関係

障害の種類	障害回復方式	
	ロールバック（後退復帰）	ロールフォワード（前進復帰）
トランザクション障害	そのトランザクションに対して，障害発生時に適用する。	―
システム障害	障害が発生したときに実行中であった全てのトランザクションに対して，DBMSの再起動時に適用する。	障害が発生したときにコミット済みであるが，2次記憶装置への書き込みが未完了の全てのトランザクションに対して，DBMSの再起動時に適用する。
メディア障害	―	バックアップを用いてデータベースを回復した後，バックアップ以降で障害発生までの間にコミット済である全てのトランザクションに対して適用する。

３．ログファイル

- トランザクションが行った更新などの操作は，障害に備えて**ログファイル**または**ジャーナルファイル**に記録される。
- ログファイルへの書き出し方式には，**ログ先書き出し方式**（**WAL : write ahead log**）が使用される。
- ログ先書き出し方式は，データベースを更新する前に，まず更新内容をログファイルへ書き込む方式である。
- ログを先に書き出すことによって，トランザクション障害が発生した場合にもデータベースを回復できる。

３．ログファイル

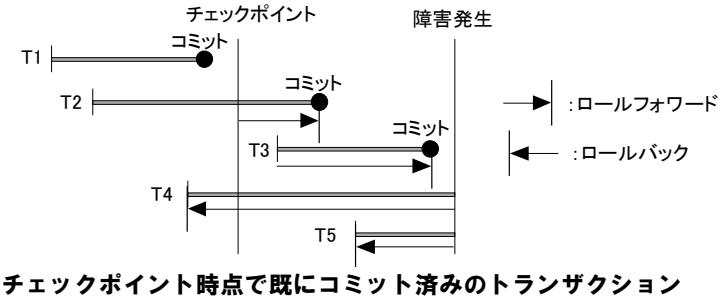
- WALプロトコルは以下の規則に従う。
  - ① ログ先書き出し方式：データベースの更新データの書き出しより先に，その更新のログを書き出す。
  - ② コミット時ログ強制書き出し方式：コミットより先に，当該トランザクションがデータベースに対して行ったすべての更新ログを書き出す。
- ログファイルの種類には，データベースの更新前ログとデータベースの更新後ログがある。
- 更新前ログは，データベースを更新前に戻すUNDO処理（ロールバック）のために使用される。
- 更新後ログは，トランザクション障害から復旧するREDO処理（ロールフォワード）のために使用される。

４．チェックポイント

- データベースへの更新は主メモリ上で行われた後に，2次記憶装置へ書き出されるので，主メモリ上の内容と2次記憶装置上のデータが常に一致するとは限らない。
- DBMSはチェックポイントという技法を用いて，主メモリ上のデータを強制的に2次記憶装置上に反映させている。
- チェックポイントの時点では，ログファイルの内容と2次記憶装置上の内容が一致している。
- システム障害などが発生した場合には，このチェックポイント時点からロールフォワードにより回復することができるので，障害回復時間を短縮することができる。
- チェックポイントの設定方法は，①一定時間間隔ごと，②一定のトランザクション実行数ごと，③一定のログ量ごと，などがある。

４．チェックポイント

チェックポイントを用いた回復方法



T1: チェックポイント時点で既にコミット済みのトランザクション
T2: チェックポイント時点に実行中で，障害発生前にコミット済みのトランザクション
T3: チェックポイント後に開始され，障害発生前にコミット済みのトランザクション
T4: チェックポイント時点に実行中で，障害発生時点に実行中のトランザクション
T5: チェックポイント後に開始され，障害発生時点に実行中のトランザクション

５．障害への対応

障害への対応

障害の種類	障害回復方法
トランザクション障害 （プログラム障害）	当該トランザクションをロールバックする。
システム障害 （ソフトウェアやハードウェアの障害）	チェックポント時点からログファイルを使用して，システム発生時点の状態に回復する。
メディア障害 （記憶媒体の障害）	バックアップファイルから回復する。

まとめ

- 障害回復の概要
- ロールフォワードとロールバック
- ログファイル
- チェックポイント
- 障害への対応