

【情報】基本と応用

データベース編

■一般

- ▶ ※ データベースに使われる拡張子は、圧倒的に `.db` が多い。

■データモデル

- ▶ ※ データモデルとは、現実世界にある複雑なデータの相互関係をわかりやすく表した図。
データベースを作る際の設計図になる。
- 関係データモデル：データの集まりを「表」で表す。関係モデルともいう。
- 階層データモデル
- ネットワークデータモデル

■関係データベースと関係データモデルでの用語の違い

- テーブル（表） ⇔ 関係
- レコード ⇔ 組
- 列 ⇔ 属性

■正規化

- ▶ 正規化
- ▶ 正規化の目的
- ▶ 関数従属
- ▶ 完全関数従属
- ▶ 部分関数従属
- ▶ 推移的関数従属
- ▶ 第1正規化
- ▶ 第2正規化
- ▶ 第3正規化

■データベース管理システム（DBMS）

- ▶ ※ DBMSは、アプリケーションソフトウェアの要求に応じてデータベースを操作するシステム。
- ▶ DBMSの3機能
- ▶ ストアドプロシージャ

【情報】基本と応用

データベース編

■一般

- ▶ ※ データベースに使われる拡張子は、圧倒的に `.db` が多い。

■データモデル

- ▶ ※ データモデルとは、現実世界にある複雑なデータの相互関係をわかりやすく表した図。
データベースを作る際の設計図になる。
- 関係データモデル：データの集まりを「表」で表す。関係モデルともいう。
- 階層データモデル
- ネットワークデータモデル

■関係データベースと関係データモデルでの用語の違い

- テーブル（表） ⇔ 関係
- レコード ⇔ 組
- 列 ⇔ 属性

■正規化

- ▶ 正規化 複数の表を用意することでデータ管理を合理化すること
- ▶ 正規化の目的 表中のすべての関数従属を、完全関数従属だけにする
- ▶ 関数従属 ある属性の値が決まると他の属性の値も一意に決まること
- ▶ 完全関数従属 属性が主キー（複合主キーふくむ）に関数従属
- ▶ 部分関数従属 属性が複合主キーの一部に関数従属
- ▶ 推移的関数従属 属性が主キー（複合主キーふくむ）以外の属性に関数従属
- ▶ 第1正規化 属性の繰り返しがない状態にする。レコードを追加して実現。
- ▶ 第2正規化 部分関数従属がない状態にすること。テーブルを分割して実現。
- ▶ 第3正規化 推移的関数従属がない状態にすること。テーブルを分割して実現。

■データベース管理システム（DBMS）

- ▶ ※ DBMSは、アプリケーションソフトウェアの要求に応じてデータベースを操作するシステム。
- ▶ DBMSの3機能 データ操作、トランザクション管理、排他制御
- ▶ ストアドプロシージャ 複数の命令を1つにまとめてDBMSに保存したもの

▶ RDBMS	
▶ SQL	
▶ NoSQL	

データ操作

▶ 選択	
▶ 射影	
▶ 結合	
▶ 挿入	
▶ 更新	
▶ 削除	

結合

▶ 内部結合	
▶ 左外部結合	
▶ 右外部結合	
▶ 完全外部結合	
▶ 交差結合	

トランザクション管理

▶ トランザクション	
▶ ACID特性	
▶ Atomicity	
▶ Consistency	
▶ Isolation	
▶ Durability	
▶ 障害回復（リカバリ）	
▶ バックアップファイル	
▶ バックアップ	
▶ 更新前・後ログファイル	
▶ ロールバック	
▶ ロールフォワード	

▶ RDBMS	関係データベース管理システム
▶ SQL	関係データベースを操作するための言語
▶ NoSQL	RDBMS以外のDBMSのこと

データ操作

▶ 選択	テーブルからある特定のレコードのみを取り出す操作
▶ 射影	テーブルからある特定の列のみを取り出す操作
▶ 結合	複数のテーブルを1つにする操作
▶ 挿入	テーブルにレコードを追加する操作
▶ 更新	レコード内のデータを変更する操作
▶ 削除	テーブルからレコードを削除する操作

結合

▶ 内部結合	2つの表の合体可能な録のみ取り出す
▶ 左外部結合	表1の全録を取り出して、それに表2の録をくっつける
▶ 右外部結合	表2の全録を取り出して、それに表1の録をくっつける
▶ 完全外部結合	両表の全録を取り出して、くっつけられる範囲でくっつける
▶ 交差結合	両表の全録を取り出して、すべての組み合わせでくっつける

トランザクション管理

▶ トランザクション	途中で終わってはならない、関連する複数の処理のまとめ
▶ ACID特性	原子性 Atomicity, 一貫性 Consistency, 独立性 Isolation, 耐久性 Durability
▶ Atomicity	「全く処理していない」か「完了」かのどちらかの結果になること
▶ Consistency	トランザクション前後でDBに矛盾がないこと
▶ Isolation	単独処理でも並行処理でも同じ結果になること
▶ Durability	正常終了したら、そのあと障害があっても結果が変わらないこと
▶ 障害回復（リカバリ）	壊れたデータやハードウェアを直すこと
▶ バックアップファイル	データベース全体を保存しているファ
▶ バックアップ	バックアップファイルを取得する処理
▶ 更新前・後ログファイル	トランザクション開始直前・完了直後の状態を保存したファ
▶ ロールバック	トランザクション開始直前の状態に戻す障害回復手法
▶ ロールフォワード	トランザクション完了直後の状態に戻す障害回復手法

排他制御

▶ 排他制御	
▶ ロック	
▶ 専有ロック	
▶ 共有ロック	
▶ ロックの両立性	
▶ ロックの粒度	

■DDLにおける制約の種類

▶ 非NULL制約	
▶ 一意性制約	
▶ 主キー制約	
▶ 外部キー制約 （参照制約）	
▶ 検査制約	

■その他の用語

▶ トリガー	
▶ インデックス	

ネットワーク編

■回線

▶ 回線	
▶ 回線速度	
▶ 伝送速度	
▶ 伝送効率	
▶ 伝送時間	

■伝送方式

▶ 回線交換方式	
▶ パケット交換方式	

排他制御

▶ 排他制御	複数の人が同じデータを同時に更新しようとした場合にデータに矛盾が生じないようにする機能
▶ ロック	データベースに対するデータの読み書きを一時的に制限する機能
▶ 専有ロック	ロックをかけたトランザクションのみがデータを読み書きできる
▶ 共有ロック	ロックをかけたトランザクションと他のそのの両方がデータを読める
▶ ロックの両立性	複数のトランザクションが共有ロックを同時にかけられる特性
▶ ロックの粒度	ロックの対象となるデータの単位（DB単位、表単位、録単位、...）

■DDLにおける制約の種類

▶ 非NULL制約	列の値がNULLであることを許可しない
▶ 一意性制約	列の値が重複する行を作成できない
▶ 主キー制約	表のなかで行を一位に特定できる主キーの列を指定する
▶ 外部キー制約 （参照制約）	外部キー（別の表の主キーを取り込んだ列）として指定した列の値と同じ値を持つ主キーの列が参照先の表に存在しなければならない
▶ 検査制約	検査条件を満たさない値を格納することはできない

■その他の用語

▶ トリガー	表の更新（録の追加、変更、削除）の前後に、自動で他の表も更新
▶ インデックス	ある列を予めグルーブ化させておくことで検索を高速化を図る仕組み

ネットワーク編

■回線

▶ 回線	データが通る線。伝送路、通信回線とも。
▶ 回線速度	その回線でデータをやり取りできる最大の速さ [bps]
▶ 伝送速度	その回線でデータをやり取りする実際の速さ [bps]
▶ 伝送効率	伝送速度 ÷ 回線速度
▶ 伝送時間	あるデータ量 ÷ 伝送速度 ※転送時間とも。

■伝送方式

▶ 回線交換方式	回線を占有して情報をやり取り
▶ パケット交換方式	データをパケット単位に分割し、複数の回線で情報をやり取り

▶ パケット	
▶ ヘッダ	

情報セキュリティ編

■人的脅威

▶ ソーシャル エンジニアリング	
▶ 不正の トライアングル	

■技術的脅威

攻撃の準備

▶ ポートスキャン	
▶ セキュリティホール	

パスワードを割り出す攻撃

▶ ブルートフォース攻撃	
▶ 辞書攻撃	
▶ パスワードリスト攻撃	

マルウェアによる攻撃

▶ ※ マルウェア（Malware）とは、悪意のあるソフトウェアの総称である。

▶ ボット	
▶ スパイウェア	
▶ ランサムウェア	
▶ キーロガー	
▶ バックドア	

Webサイトに仕掛けられる攻撃

▶ フィッシング	
▶ ドライブバイダウンロード	
▶ SEOポイズニング	

▶ パケット	データを小分けにし、それぞれにヘッダをつけた単位
▶ ヘッダ	パケットの宛先などの説明書き。制御情報とも。

情報セキュリティ編

■人的脅威

▶ ソーシャル エンジニアリング	特別なツールや技術を使わず、人間の心理的な隙を利用して機密情報を手に入れること
▶ 不正の トライアングル	人が不正を働くのは、機会・動機・正当化の3条件が揃った時に限られるという理論

■技術的脅威

攻撃の準備

▶ ポートスキャン	攻撃できそうなサービスがあるかどうかの事前調査
▶ セキュリティホール	システムに存在する欠陥。脆弱性。

パスワードを割り出す攻撃

▶ ブルートフォース攻撃	可能な文字列を総当たりで試して割り出す
▶ 辞書攻撃	辞書や人名録などに載っている全単語を使って割り出す
▶ パスワードリスト攻撃	ほかのサービスから不正に入手したID・PWの一覧を使う

マルウェアによる攻撃

▶ ※ マルウェア（Malware）とは、悪意のあるソフトウェアの総称である。

▶ ボット	攻撃者から遠隔で指令を受けて動作するプログラム
▶ スパイウェア	利用者に気づかれないように個人情報などを収集するプログラム
▶ ランサムウェア	身代金を要求するプログラム
▶ キーロガー	キーボード入力を記録するプログラム
▶ バックドア	システムに不正アクセスするための裏口。

Webサイトに仕掛けられる攻撃

▶ フィッシング	利用者を偽サイトに誘導し、個人情報を入力させる
▶ ドライブバイダウンロード	サイトの閲覧だけでマルウェアをダウンロードさせる
▶ SEOポイズニング	SEOを行って悪質サイトを検索結果上位に表示させる

▶ DNSキャッシュポイズニング	
▶ SQLインジェクション	
▶ クロスサイト スクリプティング	

その他の攻撃

▶ スпам	
▶ DoS攻撃	
▶ DDoS攻撃	
▶ ディレクトリトラバーサル攻撃	

■物理的攻撃

▶ ※ 物理的攻撃は、ネットワークなどを使わない直接的な手段によって引き起こされる脅威。	
▶ 具体例は	

▶ DNSキャッシュポイズニング	DNSサーバにキャッシュされているドメイン名とIPアドレスの対応を置き換えることで悪質サイトに誘導
▶ SQLインジェクション	SQLの実行によるデータベース改竄、不正なデータ取得
▶ クロスサイト スクリプティング	ユーザの入力データが後で表示されるようなフォームに第三者が悪意あるスクリプトを書くことでデータを盗む

その他の攻撃

▶ スпам	受信者の承諾なしに無差別に送付されるメール
▶ DoS攻撃	メールやリクエストを大量に送り、サービスを提供不能に
▶ DDoS攻撃	多数のコンピュータによるDoS攻撃
▶ ディレクトリトラバーサル攻撃	管理者の意図しないファイルを不正に閲覧

■物理的攻撃

▶ ※ 物理的攻撃は、ネットワークなどを使わない直接的な手段によって引き起こされる脅威。	
▶ 具体例は	台水害、落雷、地震、大気汚染、爆発、火災、侵入、盗難など