

Web データベースの構築技術

博士（工学） 速水 治夫 編著
博士（情報科学） 古井陽之助 共著
博士（学術） 服部 哲

コロナ社

PHP 書式 簡便一覧

■フォームの処理

- (1) リクエストパラメータの取得用配列

```
$var1 = $_GET[パラメータ名];  
//GET メソッドの場合  
$var2 = $_POST[パラメータ名];  
//POST メソッドの場合  
$var3 = $_REQUEST[パラメータ名];  
//GET, POST のどちらの場合でも利用可能
```

注意: パラメータ名を文字列で与える場合は, `$_REQUEST ['fukuoka']` のようにシングルクォートで囲む. パラメータ名に変数を使うときは, `$_REQUEST [$paramname]` のようにシングルクォートで囲まない.

- (2) ファイル受信後のパラメータの取得用 2 次元配列

```
$var1 = $_FILES[パラメータ名]['tmp_name'];  
//受信後に一時ディレクトリに保存されたときのパス名  
$var2 = $_FILES[パラメータ名]['name'];  
//クライアント側における転送前のファイル名  
$var3 = $_FILES[パラメータ名]['type'];  
//MIME タイプ  
$var4 = $_FILES[パラメータ名]['size'];  
//ファイルの大きさ. 単位はバイト  
$var5 = $_FILES[パラメータ名]['error'];  
//エラーコード. 受信成功ならゼロ, エラーなら正の整数
```

■データベースの操作

- (1) MySQL への接続とデータベースの選択

```
$db = mysql_connect(  
サーバ名('localhost'),  
ユーザ名, パスワード);  
$src = mysql_select_db(データベース名);
```

- (2) クエリの実行と結果の処理 (Web 製品データベースを例として)

- (2-1) データの検索

```
$query = "select product, factory,  
cost from product_t";  
//SQL 文の記述  
$result = mysql_query($query);  
//SQL 文の実行  
while($row = mysql_fetch_array($result))  
{  
//実行結果 1 行の取得  
$var1 = echo $row['product'];  
//列の値の取得  
$var2 = echo $row['factory'];  
$var3 = echo $row['cost'];  
}
```

(2-2) データの挿入 (\$productなどはフォーム処理により得られたとする)
\$query = "insert into product_t (product, factory, cost) values
('\$product', '\$factory', \$cost)";
\$result = mysql_query(\$query);

(2-3) データの変更 (\$productなどはフォーム処理により得られたとする)
\$query = "update product_t set factory='\$factory', cost=\$cost where
product='\$product'";
\$result = mysql_query(\$query);

(2-4) データの削除 (\$productはフォーム処理により得られたとする)
\$query = "delete from product_t where product='\$product'";
\$result = mysql_query(\$query);

(3) MySQL接続を閉じる
mysql_close();

(4) MySQLアクセスのエラー処理 (クエリ実行を例として)
\$query = "select product, factory, cost from product_t";
\$result = mysql_query(\$query);
if (!\$result)
exit('クエリが失敗しました。');

■セキュリティ関連

(1) リクエストパラメータ値の検査と変換 (\$varにパラメータ値を代入したとする)

(1-1) 数値への変換

```
$var = 0 + $var; // $var=(int)$var;としてもよい
```

(1-2) シングルクォート、ダブルクォートなどのエスケープ

```
$var = addslashes($var);
```

(2) 文字列のWebブラウザ出力用への変換 (文字列を\$strとする)

```
$var = htmlspecialchars($str, ENT_QUOTES);
```

(3) セッションの管理

(3-1) セッションの開始と配列 \$_SESSIONへの値の格納

```
session_start(); //セッションの開始  
$_SESSION['loginname'] = $name; //loginnameは要素名なので自由につけてよい
```

(3-2) 新しいセッションへの切り替え

```
session_regenerate_id();
```

(3-3) セッションIDの取得

```
$var = session_id();
```

■その他

(1) 文字コードの変換

```
// 文字列「$str」の文字コードをWindows-31JからEUCJP-WINに変換  
$var = mb_convert_encoding($str, 'EUCJP-WIN', 'Windows-31J');
```

(2) ページの遷移

```
header('Location: ページ遷移先の絶対URL');
```


まえがき

本書は、Web データベースの構築技術をはじめて学ぶ人の入門書として書かれている。大学の学部レベルの情報系学生向けの教科書として、また Web データベースを構築しようとしている企業の技術者向けの参考書として読まれることを想定している。

大学では各章を 2 コマ (3 時間) で学ぶことを想定している。全 8 章を 8 週間で学ぶことができる。これに加えてガイダンスと学生による独自の Web データベースを企画・設計・構築することを含めて半期の実験 (演習) 科目用の教科書として使用できる。

まず、Web データベースとは何かを理解した後、Windows 環境でオープンソースの Apache、MySQL、PHP を使用して画像などのマルチメディアデータを Web ブラウザから登録したり検索したりする Web データベースを実際に構築しながら、そのために必要な技術を学んでいくことができる。Apache は Web サーバソフトウェア、MySQL はリレーショナルデータベース管理システム、PHP は Web サーバ上で実行されるスクリプト言語である。これらおよび Windows の頭文字をつなげて WAMP と称し、実用の Web データベース構築によく使用されている。

類書にない特徴として、最初 (第 1 部 (1~3 章) と第 2 部 (4~6 章) で) はセキュリティなどの高度な機能を入れないで (つまり悪意のユーザやいたずらがいないことを前提とした) 正常系の基本的な機能のみでシステムを構築することを学ぶ。類書ではセキュリティなどの機能が最初からプログラム例中に散在しているので、初心者はどこが実現したい機能の本質的な部分かを理解しにくい。本書では、本質的なプログラムを理解した後、第 3 部 (7~8 章) の技法編で高度な機能を学ぶ。しかも、そこではこのような機能を入れないとどのような不都合があるかを示し、その対策としての機能を学ぶので理解しやすくなっている。

第 1 部では、本書で使用するオープンソースの Apache、MySQL、PHP を自分の PC にインストールしそれぞれの使用方法を学ぶ。

第 2 部では、Web データベースの基本的な構築技術を学ぶ。また、画像を取り扱う技術も学ぶ。

第 3 部では、セキュリティやセッションといった高度な技術を学ぶ。

前見返しによく使用する PHP 書式の簡便一覧を、後ろ見返しには SQL 書式の簡便一覧を示している。一通り学習した後に書式を思い出すときに参照すると便利であ

る。

リレーショナルデータベースの基本を学ぶには、姉妹編の「リレーショナルデータベースの実践的基礎」が用意されている。

なお、本書の特徴として、教科書としてご採用の先生方に対して、コロナ社を通じてプログラムリストのファイル、演習問題解答や使用ソフトウェアのインストール手順書などの教材をご提供する仕組みを備えている。

2009年8月

速水 治夫

本書姉妹編の内容梗概と特徴

【リレーショナルデータベースの実践的基礎】

データベースがなぜ必要なのかを理解し、リレーショナルデータベースを実践的に使用できる実力が備わる内容になっている。特に、リレーショナルモデルの論理設計およびSQLを具体例で学ぶことができる。SQLの実行例はオープンソースのデータベース管理システムであるMySQLを使用して示している。

【データベースの実装とシステム運用管理】(2010年9月発行予定)

データベースシステム開発において、論理設計以降で重要となる「データベースの実装・テスト」および「データベースシステムの運用管理」を重点的に学ぶことができる。高度な内容であるが、具体例を交えてわかりやすく記述しているので、初心者でも十分理解することができる。

【特徴】

両著書をあわせて学ぶことによって、「情報処理技術者試験」の「データベーススペシャリスト試験(DB)」の出題範囲を理解することができる。

また、両著書の特徴として、教科書としてご採用の先生方に対して、コロナ社を通じて講義を進めるためのPowerPointの資料などの教材をご提供する仕組みを備えている。

目 次

0 章 準 備

0.1	この本で学習する内容	1
0.2	この本の学習で使用する機器とソフトウェア	1
0.3	この本の学習の構成	2
0.4	各章の確認事項と演習問題	2
0.4.1	確 認 事 項	2
0.4.2	演 習 問 題	3
0.5	本書の学習のための基礎知識	3
0.5.1	Web サーバによる情報提供方法の分類	3
0.5.2	Web アプリケーション	4
0.5.3	Web データベース	5
0.5.4	ま と め	6

第 1 部

1 章 MySQL 入門・その 1

1.1	本章について	7
1.2	MySQL のインストール	8
1.3	簡単なデータベース	8
1.3.1	作成する製品データベースの仕様	8
1.3.2	自分のユーザアカウントの準備	8
1.3.3	製品データベースの作成	9
1.3.4	自分のユーザアカウントによるログイン	10
1.3.5	製品テーブルへのデータ入力と検索	11
1.3.6	製品データベースの消去	12
1.4	バッチ処理によるデータベースの作成	13
1.4.1	本節の作業を行う前に	13
1.4.2	バッチ処理によるデータベースの作成	13
1.4.3	バッチ処理によるデータベースの消去	15
1.5	CSV ファイルからデータベースへの入力	15
1.5.1	CSV ファイルの作成	15

1.5.2	CSV ファイルからテーブルへの取込み	16
1.5.3	テーブルから CSV ファイルへの抽出	17
1.6	MySQL 5.0 の管理	17
1.6.1	コマンドおよびステートメント	17
1.6.2	PHP 4 との互換性について	18
1.7	演習問題	20

2章 MySQL 入門・その2

2.1	本章について	21
2.2	リレーショナルデータベースの設計	22
2.2.1	テーブルの正規化	22
2.2.2	主キーと外部キー	25
2.2.3	主キーとしての ID 番号	26
2.3	データベースの作成	27
2.3.1	CREATE DATABASE 文によるデータベースの作成	27
2.3.2	CREATE TABLE 文によるテーブルの作成	28
2.3.3	CREATE TABLE 文の詳細	30
2.4	データの入力	33
2.4.1	INSERT 文によるデータの挿入	33
2.4.2	LOAD DATA INFILE 文による CSV ファイルからのインポート	33
2.5	データの検索	35
2.5.1	SELECT 文による検索の基本	35
2.5.2	WHERE 句による検索条件の指定	36
2.5.3	ORDER BY 句による並び順の指定	38
2.5.4	テーブルの結合	38
2.6	データの変更・削除	42
2.6.1	UPDATE 文によるデータの変更	42
2.6.2	DELETE 文によるデータの削除	42
2.7	演習問題	43

3章 Apache HTTP Server と PHP

3.1	本章について	44
3.2	Apache HTTP Server と PHP のインストール	45
3.3	PHP による Web アプリケーション入門	45
3.3.1	Web アプリケーション	45
3.3.2	例題 Web アプリケーション「福岡名物をどうにかしよう」	45

3.3.3 実 装	47
3.4 PHPによるWebアプリケーションの実行の仕組み	49
3.4.1 システム構成	49
3.4.2 動 作	49
3.4.3 特 徴	50
3.5 HTML フォーム	51
3.5.1 フォームとWebアプリケーション	51
3.5.2 FORM タ グ	51
3.5.3 ラジオボタン	52
3.5.4 テキストフィールド	53
3.5.5 送信ボタンとリセットボタン	54
3.6 PHPスクリプトによるフォーム処理	55
3.6.1 PHP コ ー ド	55
3.6.2 変 数	56
3.6.3 リクエストパラメータの取得	56
3.6.4 条件分岐 (if文)	57
3.7 演 習 問 題	58

第 2 部

4章 データベース接続

4.1 本章について	60
4.2 Apache・PHP・MySQLによるWebデータベース入門	61
4.2.1 Webデータベース	61
4.2.2 例題Webデータベース「Web製品データベース」	61
4.2.3 製品データ表示機能の実装	61
4.3 Apache・PHP・MySQLによるWebデータベースの実行の仕組み	63
4.3.1 システム構成	63
4.3.2 動 作	63
4.4 PHPスクリプトからのMySQLアクセス	64
4.4.1 MySQLアクセスのためのPHP関数	64
4.4.2 繰り返し (while文)	64
4.4.3 MySQLアクセスのエラー処理	65
4.5 検 索	66
4.5.1 製品データ検索機能	66
4.5.2 製品データ検索機能の実装	67
4.5.3 製品データ検索機能の動作	68

4.5.4 文字列の結合	69
4.6 テーブルの結合	70
4.7 演習問題	72

5章 データベース更新

5.1 本章について	74
5.2 データ追加	75
5.2.1 製品データ追加機能	75
5.2.2 製品データ追加機能の実装	75
5.2.3 製品データ追加機能の動作	77
5.2.4 フォーム送信のための POST メソッド	78
5.2.5 自動的なページ遷移	79
5.2.6 フォーム記入のエラー処理	80
5.3 データ編集	82
5.3.1 製品データ編集機能	82
5.3.2 製品データ編集機能の実装	83
5.3.3 製品データ編集機能の動作	85
5.3.4 記入欄のデフォルト値の表示	86
5.4 外部キー値の追加・編集	87
5.4.1 外部キーの整合性の確認	87
5.4.2 配列の生成と検索 (配列関数と foreach 文)	90
5.5 設定情報の共通ファイル化	91
5.6 データ削除	92
5.7 タブ表示	93
5.8 追加・編集機能の実装における留意点のまとめ	94
5.9 演習問題	95

6章 画像処理

6.1 本章について	97
6.2 ファイルアップロードの処理	97
6.2.1 例題 Web アプリケーション「Web ファイラ」	97
6.2.2 Web ファイラの実装	99
6.2.3 Web ファイラの動作	100
6.2.4 フォームによるファイル送信	101
6.2.5 PHP スクリプトによるファイル受信	102
6.2.6 設定ファイル php.ini による制限	104

6.2.7 MIME タイプ	105
6.3 サムネイル画像の生成	106
6.3.1 PHPによるサムネイルの生成	106
6.3.2 受信した画像ファイルをサムネイルへ変換し保存する機能	107
6.3.3 保存済み画像ファイルのサムネイル表示機能	108
6.4 PHPとMySQLによるファイルデータベース	111
6.4.1 Webファイルデータベース	111
6.4.2 設計	112
6.4.3 MySQLデータベースの実装	113
6.4.4 PHPスクリプトの実装	115
6.5 演習問題	122

第 3 部

7章 セキュリティ

7.1 本章について	124
7.2 セキュリティ上危険な Web データベース	124
7.2.1 ダメな Web データベース「DAME」	124
7.2.2 フォームの改変	133
7.3 Web データベースに対する攻撃と対策方法	134
7.3.1 大切な前置き	134
7.3.2 強制ブラウジング	134
7.3.3 フォームの改ざんと偽装	137
7.3.4 SQL インジェクション	138
7.3.5 クロスサイトスクリプティング	141
7.3.6 クロスサイトリクエストフォージェリ	143
7.3.7 ディレクトリさかのぼり攻撃	144
7.3.8 NULL バイト攻撃	144
7.4 パラメータ値の変換処理	145
7.4.1 PHPによる自動変換	145
7.4.2 シフト JIS (Shift JIS) コードと変換処理の問題	146
7.4.3 エスケープ用関数の作成	148
7.5 その他の留意点：手がかりを隠すこと	151
7.6 演習問題	153

8章 セッション

8.1 本章について	154
------------	-----

8.2 セッションを利用する Web アプリケーション	155
8.2.1 セッションのテスト	155
8.2.2 ログインのテスト	156
8.2.3 ワンタイムチケットのテスト	158
8.3 セッション	162
8.3.1 HTTP とセッション管理	162
8.3.2 PHP のセッション処理関数	164
8.4 セッションとセキュリティ	165
8.4.1 ワンタイムチケット	165
8.4.2 セッション固定化攻撃	166
8.4.3 ログイン	168
8.5 演習問題	174
参 考 文 献	175
あ と が き	176
付 録	177
PHP 関数・MySQL 関数の説明	177
インストール時の注意事項	182
索 引	184

0

準備

0.1 この本で学習する内容

本書では、マルチメディアデータを Web ブラウザから登録したり検索したりするシステムを実際に構築しながら、そのために必要な技術を学ぶ。構築したシステムは Web アプリケーション（0.5.2 項を参照）、より詳しくは Web データベース（0.5.3 項を参照）といわれるものとなる。

具体的に学ぶ内容としては、0.2 節に示すソフトウェアを各自の PC にインストールし、その PC を用いて Web データベースプログラミングを学ぶ。

0.2 この本の学習で使用する機器とソフトウェア

本書の学習で使用する機器を表 0.1 に、また PC にインストールして使用するソフトウェアを表 0.2 に示す。表中の名称や版番号などは本書執筆時点のもので、実際に使用するものとは異なる場合がある。

表 0.1 使用機器

機器	条件
各読者の所有する PC	Windows XP SP2 以降がインストールされており、200 MB 以上の空き容量があること。

表 0.2 インストールするソフトウェア

ソフトウェア	説明
Apache HTTP Server 2.0 (アパッチ)	Web サーバソフトウェア。単に Apache と呼ぶ。Web サーバのなかでは最大の稼働台数を誇る。
PHP 4.4 (ピー・エイチ・ピー)	スクリプト言語実行環境。Web アプリケーション向けとして人気が高い。4 系列は後の系列より稼働実績があり情報も豊富である。
MySQL 5.0 (マイ・エス・キュー・エル)	リレーショナルデータベース管理システム。基本的な機能とトランザクションなどの高度な機能を兼ね備える。

0.3 この本の学習の構成

本書の学習は大きく3部に分かれる(表0.3)。第1部において、Web データベースを学ぶための基礎を固める。第2部においては、簡単な Web データベースを実際に作りながら、Web データベースプログラミングの基本的な技術を学ぶ。第3部においては、実用的な Web データベースを作るために必要なセキュリティやセッションについての知識や技法を学ぶ。第2部まで学べば、自分の PC だけで楽しむ Web データベースは十分構築することができる。

各部はさらに章に分かれる。各章の概要については表0.3中に示す。

表0.3 本演習の構成

部	題	テキスト		説明
		章	章 題	
1	SQL と Web の基礎	1	MySQL 入門・その1	MySQL を各自の PC にインストールする。バッチ処理、CSV ファイルからの入出力を学ぶ。
		2	MySQL 入門・その2	複数のテーブルを使ってデータを格納する方法や、SELECT 文による検索の方法を学ぶ。
		3	Apache HTTP Server と PHP	Apache と PHP を各自の PC にインストールする。PHP の基本的な文法を学ぶ。
2	Web データベース入門	4	データベース接続	PHP と MySQL を接続し、MySQL データベースのデータ一覧を Web ページに表示する方法を学ぶ。
		5	データベース更新	Web フォームから受信したデータで MySQL データベースを更新する方法を学ぶ。
		6	画像処理	画像の登録やサムネイル(縮小画像)表示ができる Web データベースを作る方法を学ぶ。
3	Web データベース技法	7	セキュリティ	不正なアクセスを防ぐための基礎知識を学ぶ。
		8	セッション	セッション(ログイン・ログアウト)を実現するための基礎知識を学ぶ。

0.4 各章の確認事項と演習問題

0.4.1 確認事項

各章の途中に「確認事項」がある。本書での学習の進行は読者がこれらの確認事項を実施することを前提としているので、読者はしっかりと取り組んでもらいたい。

0.4.2 演習問題

各章の末尾には「演習問題」がある。これについてもぜひ取り組んでもらいたい。

0.5 本書の学習のための基礎知識

0.5.1 Webサーバによる情報提供方法の分類

Webサーバによる情報提供の方法は、大きく2種類、細かくは3種類に分類できる(表0.4)。

表0.4 情報提供方法の分類

分類	小分類	例	インタラクション
(1) 固定情報の提供	(1-1) 静的な情報の提供	HTML 文書, 画像	なし
	(1-2) プログラムの提供	Flash, JavaScript	ユーザごと
(2) 動的に生成される情報の提供		CGI, PHP, JSP, ASP	ユーザどうし

(1) **固定情報の提供** ファイルに記録された情報を提供する。つぎの(1-1)と(1-2)に分類される。

(1-1) **静的な情報の提供** HTML文書や画像など固定的・静的な情報の提供であり、ユーザとのインタラクションがない(図0.1)。すべてのユーザは同じ情報を見ることになる。

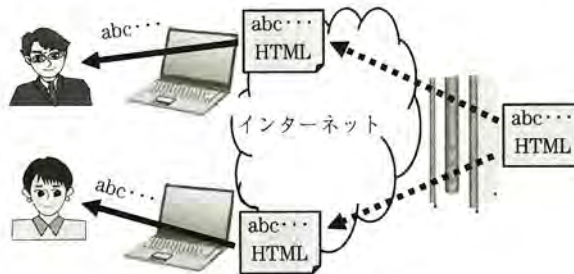


図0.1 静的な情報の提供

(1-2) **プログラムの提供** クライアント上で動作するプログラム(Flash, JavaScript, Java アプレットなど)を提供する。ユーザはそのプログラムとインタラクションを行う(図0.2)。ユーザ間のインタラクションはない。

(2) **動的に生成される情報の提供** Webサーバ上のプログラム(CGI, PHPなど)が動的に生成する情報を提供する。ユーザの入力をサーバに記録し、それを他のユーザが参照するといったユーザどうしのインタラクションも可能となる(図0.3)。

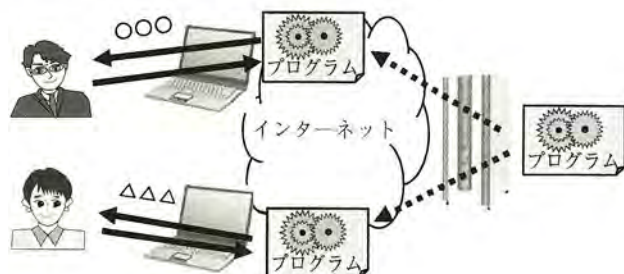


図 0.2 プログラムの提供

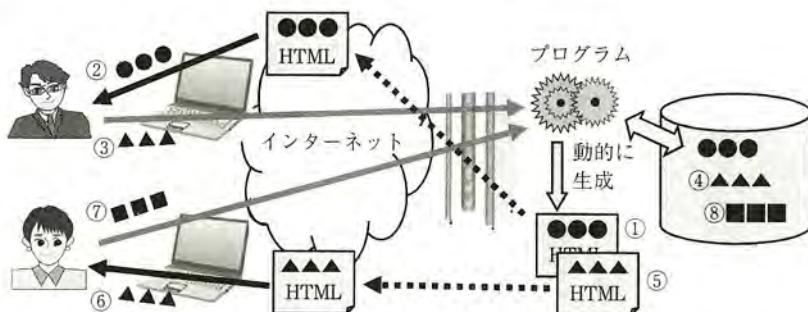


図 0.3 動的に生成される情報の提供

ユーザのリクエストに応じた情報が提供されるため、すべてのユーザが同じ画面を見るときは限らない。

0.5.2 Web アプリケーション

動的な情報の生成は Web サーバに搭載されたプログラムによって実現される。このようなプログラムを **Web アプリケーション** と呼ぶ。Web アプリケーションはユーザからのアクセスに応じてデータを生成することも、それをユーザに渡すこともできるし、また Web サーバに蓄積することもできる。このようにして蓄積されたデータはユーザどうしで共有することができる。これを利用して、ユーザどうしが **Web サーバ** を介して **インタラクション** を行うことも可能になる。

Web アプリケーションの例としては、電子掲示板やブログをはじめ、Google^{†1}、Yahoo!^{†2}、MSN^{†3} のような Web 検索エンジン、図書館の蔵書検索システム、Amazon^{†4} のような物販サイト、価格.com^{†5} のような商品情報サイト、CinemaScape^{†6} や IMDb^{†7}

†1 Google. <http://www.google.co.jp/> (以下、本書の URL はすべて 2009 年 8 月現在)

†2 Yahoo! 検索. <http://search.yahoo.co.jp/>

†3 MSN サーチ. <http://search.msn.co.jp/>

†4 Amazon.co.jp. <http://www.amazon.co.jp/>

†5 価格.com. <http://kakaku.com/>

†6 CinemaScape. <http://cinema.intercritique.com/>

†7 The Internet Movie Database. <http://www.imdb.com/>

のような映画情報サイト、Wikipedia^{†1}のような百科事典…など多数ある。

Web アプリケーションでは、ユーザが直接操作するのは Web ブラウザであるが、処理の大部分はサーバ側で行われるので、Web ブラウザに特別な仕掛けを必要とせず、Internet Explorer などよりさらに**低機能な Web ブラウザでも Web アプリケーションへのアクセスが可能**である。携帯電話のような小型の情報機器からでも Web アプリケーションにアクセスできることはこの好例である。

また開発者・運営者の立場から見ると、システムの変更作業をすべてサーバ側だけで行うことができるので**保守効率が高い**。開発環境としても、かつては Perl のような汎用言語が主流であったが、最近では Web アプリケーション構築用に開発された PHP や JSP などの **Web アプリケーション構築言語**が主役の座を占めている。なかでも、本書で使用する PHP は高い人気を誇るスクリプト言語である。

0.5.3 Web データベース

Web アプリケーションのうちデータを大量に格納し活用するものを、特に **Web データベース**と呼ぶ。0.5.2 項で挙げた Web アプリケーションの例はほとんどそのまま Web データベースの例でもある。

多くの場合、Web データベースは Web アプリケーションに **リレーショナルデータベース管理システム (RDBMS)** を組み合わせて実現される (図 0.4)。これをクライアント側も含めた全体で見れば、Web ブラウザ・Web サーバ・RDBMS が三段重ねのようになって連携している^{†2}。

このような三段重ねのシステム構成を **3 層クライアントサーバシステム**と呼ぶ。Web ブラウザ (**プレゼンテーション層**) は、Web ページを表示し、またユーザからの入力を受け取るためのユーザインタフェースとして機能する。Web サーバ (**アプリケーション層**、または **ファンクション層**、**ビジネスロジック層**などともいう) ではアプリケーションプログラムが動作し、その目的に応じてデータの加工などの処理を行う。いふならば、この層がデータをどのように処理するかを定める。RDBMS (**データベース層**) はアプリケーションプログラムの指示に従ってデータの更新や検索を行う。つまり、この層は大量のデータを管理・操作するための手段を提供する。

RDBMS を使い、各層の役割分担を明確にして Web データベースを構築することには、**開発者にとって開発効率の向上という利点**がある。例えば、大規模なデータの蓄積や高速な検索・並べ替えといった操作は RDBMS に任せられるのでアプリケーションプ

†1 Wikipedia. <http://ja.wikipedia.org/>

†2 本書では扱わないが、サーバ側では他にも何らかのシステムと連携していることがある。例えば、物販サイトはクレジットカード番号を審査するためにクレジット会社のシステムと接続し、また商品の配送状況を知るために配送業者のシステムと接続しているであろう。

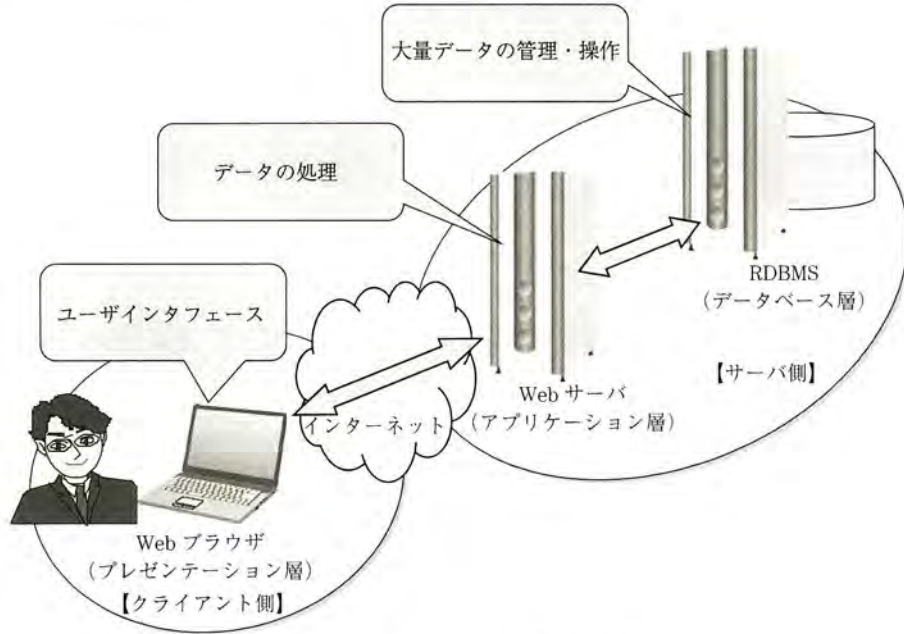


図0.4 Web データベースの3層構造

プログラムには記述する必要がない。実績のある RDBMS 製品を採用することで Web データベース全体の安定性を高めることもできる。標準的なデータ操作言語である SQL を実装した RDBMS 製品を利用すれば、個々の RDBMS 製品について学習する必要がほとんどなく、またソフトウェア資産の蓄積や活用も容易である。本書で使用する MySQL も SQL を実装しており、またその優れた処理性能によって人気が高い。

0.5.4 ま と め

本書で学ぶ Web データベースの技術は、多くのユーザが集まるインタラクティブな Web サイトを効率よく作り上げるための技術である。

1

MySQL 入門・その 1

1.1 本章について

本章では、簡単なデータベースおよびテーブルを作成しながら MySQL の使用方法を学ぶ。

本章における学習のポイントはつぎの 3 点である。

- MySQL を PC にインストールし、動作を確認する。
- データベースやテーブルを作る操作・除く操作の手順を覚える。
- ユーザアカウントによるアクセス制御の概念を理解し、その操作手順を覚える。

本章における学習の進め方を図 1.1 に示す。1.2 節では付録の「インストール時の注意事項」を併用しよう。SQL 文や MySQL については巻末の文献 1), 2) および MySQL リファレンスマニュアル 3), 4) を参照しよう。



図 1.1 1 章における学習の進め方

1.2 MySQL のインストール

MySQL のインストーラを入手し、付録の「インストール時の注意事項」の（1）の説明を確認したうえで、（2）の説明に従って自分の PC に MySQL をインストールしよう。

1.3 簡単なデータベース

1.3.1 作成する製品データベースの仕様

本節では、簡単な「製品データベース」product_db を例に、MySQL を使ってデータベースの作成、データの入力・検索、データベースの消去までを行う手順を説明する。この製品データベースは製品テーブル product_t のみを持つ。このテーブルの仕様を表 1.1 に、内容を表 1.2 に示す。

表 1.1 製品テーブル product_t の仕様

カラム名	和名	型	制約			説明
			NOT NULL	ユニーク	主キー	
product	製品名	varchar (20)	—	—	—	「テレビ」など
factory	工場名	varchar (20)	—	—	—	「厚木工場」など
cost	工場原価	int	—	—	—	単位は円

表 1.2 製品テーブル product_t の内容

product	factory	cost
ラジオ	厚木工場	1000
テレビ	厚木工場	30000
洗濯機	本厚木工場	15000
冷蔵庫	厚木北工場	40000
ラジカセ	ニカラグア工場	5000

1.3.2 自分のユーザアカウントの準備

次項の手順では、データベースにアクセスするためのユーザアカウントを設定する。そのユーザアカウント名（以下、ユーザ名）とパスワードをつぎのルールに従ってあらかじめ決めておき、忘れないようにメモしておくとい。

- ユーザ名：英字から始まり、英数文字 16 文字以内（例：ichiro）。
- パスワード：英数字 8 文字以内（例：num51）。実用で使用しているものではないほうが望ましい。

1.3.3 製品データベースの作成

スタートメニューから [すべてのプログラム]-[MySQL]-[MySQL Server 5.0]-[MySQL Command Line Client] を選択して MySQL モニタを起動し、つぎの操作（網掛け部分）を行ってデータベース product_db を作成しよう。なお、このスタートメニューのなかに登録されている MySQL モニタは管理者（root）として MySQL に接続するので、1 行目で入力するパスワードとしては、自分のパスワードではなく、インストール時に設定した管理者（root）のパスワードを入力するようにする。

```
Enter password: 管理者のパスワード
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10 to server version: 5.0.22-community-nt

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> create database product_db;
Query OK, 1 row affected (0.01 sec)

mysql> use product_db
Database changed
mysql> create table product_t (product varchar(20), factory varchar(20),
cost int);
Query OK, 0 rows affected (0.09 sec)

mysql> show columns from product_t;
+-----+-----+-----+-----+-----+-----+
| Field | Type          | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| product | varchar(20) | YES  |     | NULL    |      |
| factory | varchar(20) | YES  |     | NULL    |      |
| cost    | int(11)     | YES  |     | NULL    |      |
+-----+-----+-----+-----+-----+-----+
3 rows in set (0.01 sec)
```

続けてつぎの操作（網掛け部分）を行い、自分のユーザアカウントからデータベース product_db にアクセスできるように設定しよう[†]。「ユーザ名」および「パスワード」の部分には、1.3.2 項で準備した自分のものを入れよう。以上を完了したら QUIT コマンドで MySQL モニタを終了しよう。

```
mysql> grant all on product_db.* to ユーザ名@localhost identified by 'パスワード';
Query OK, 0 rows affected (0.03 sec)

mysql> set password for ユーザ名@localhost = old_password('パスワード');
```

[†] いったん GRANT 文で設定したパスワードを、つぎに SET PASSWORD 文で関数 OLD_PASSWORD を使って再設定するのは、3 章から扱う PHP との互換性のためである。MySQL のみを使う限りはこのような二度手間は不要である。詳しくは 1.6.2 項を参照しよう。

```
Query OK, 0 rows affected (0.00 sec)

mysql> quit
```

1.3.4 自分のユーザアカウントによるログイン

適当なテキストエディタでリスト 1-1 のように記述したバッチファイル mymon.bat をデスクトップに作ろう。「ユーザ名」の部分には、1.3.2 項で準備した自分のユーザ名を入れよう。

リスト 1-1 バッチファイル mymon.bat

```
@echo off
"C:\Program Files\MySQL\MySQL Server 5.0\bin\mysql.exe" -u ユーザ名 -p
```

作成したバッチファイルをマウスの左ボタンでダブルクリックすることにより実行できる。このバッチファイル mymon.bat を実行すると、自分のユーザアカウントを使って MySQL モニタを起動することができる。つぎの操作（網掛け部分）を実行し、データベース product_db およびテーブル product_t にアクセスできることを確認しよう。なお、1 行目では**自分のパスワードを入力**すること。

```
Enter password: 自分のパスワード
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 14 to server version: 5.0.22-community-nt

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> show databases;
+-----+
| Database          |
+-----+
| information_schema |
| product_db        |
+-----+
2 rows in set (0.01 sec)

mysql> use product_db
Database changed
mysql> show tables;
+-----+
| Tables_in_product_db |
+-----+
| product_t             |
+-----+
1 row in set (0.00 sec)

mysql> show columns from product_t;
```

```

+-----+-----+-----+-----+-----+-----+
| Field | Type          | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| product | varchar(20) | YES  |     | NULL    |      |
| factory | varchar(20) | YES  |     | NULL    |      |
| cost    | int(11)     | YES  |     | NULL    |      |
+-----+-----+-----+-----+-----+-----+
3 rows in set (0.01 sec)

```

1.3.5 製品テーブルへのデータ入力と検索

つぎのように INSERT 文を使うと、表 1.2 に示した内容を製品テーブル product_t に挿入（追加）することができる。（もちろん、データを 1 行ずつ INSERT 文で挿入するのは効率的ではないが、ここでは動作確認を兼ねて実行してみよう。これをさらに効率的に行う方法は 1.5 節で紹介する。）

```

mysql> insert into product_t values ('ラジオ', '厚木工場', 1000);
Query OK, 1 row affected (0.09 sec)

mysql> insert into product_t values ('テレビ', '厚木工場', 30000);
Query OK, 1 row affected (0.04 sec)

mysql> (以下同様)

```

続けて、つぎのように SELECT 文を使うと、すべてのデータを表示したり、WHERE 句で指定した条件に合致するデータを取り出したりすることができる。以上を確認したら QUIT コマンドで終了しよう。

```

mysql> select * from product_t;
+-----+-----+-----+
| product | factory          | cost |
+-----+-----+-----+
| ラジオ  | 厚木工場         | 1000 |
| テレビ  | 厚木工場         | 30000|
| 洗濯機  | 本厚木工場       | 15000|
| 冷蔵庫  | 厚木北工場       | 40000|
| ラジカセ| ニカラグア工場  | 5000 |
+-----+-----+-----+
5 rows in set (0.00 sec)

mysql> select * from product_t where cost < 10000;
+-----+-----+-----+
| product | factory          | cost |
+-----+-----+-----+
| ラジオ  | 厚木工場         | 1000 |
| ラジカセ| ニカラグア工場  | 5000 |
+-----+-----+-----+
2 rows in set (0.00 sec)

```

索引

【あ】		【く】		【せ】	
アカウントの削除	18	区切り記号	34	正規化	22
アカウントの作成	18	クッキー	163	正規ユーザ	169
アクセス権限の削除	18	繰り返し	64	静的な情報の提供	3
アクセス権限の設定	18	クロスサイトスクリプティング		制約	31
アクセス制限	169		141	成立	37
アクセス元	169	クロスサイトリクエストフォー		セッション	155, 163
アスタリスク	35	ジェリ	143	セッション ID	155, 163, 164
アプリケーション層	5			——を再生成	168
【い】		【け】		【そ】	
インターネット一時ファイル	163	結合	38	送信先 URL	51
インタプリタ型言語	50	結合演算子	69	送信ボタン	45, 54
インタラクション	3	結合代入演算子	69	添え字	56
インポート	16, 33	検索	35, 66	【た】	
【え】		【こ】		第1正規形	
永続クッキー	163	降順	38	第2正規形	
永続的なクッキー	163	更新時不整合	23	第3正規形	
エクスポート	17	固定情報の提供	3	大なり記号	
エスケープ	70, 146	コマンド	18	代入演算子	
エスケープ処理	140	【さ】		タブ表示	
エラー処理	65	サムネイル	106	ダブルクォート	
エラー制御演算子	107	【し】		ダラー	
エラーメッセージ	152	識別子	26, 56	短縮形	
エンティティ	51	自然結合	38, 39	【ち】	
【か】		自動的なページ遷移	79	チェックボックス	
改行記号	34	自動連番	32	直接アクセス	
外部キー	26	シフト JIS	146	【て】	
外部キー制約	26, 32	主キー	23, 25	ディレクトリさかのぼり攻撃	
——の整合性	87	主キー制約	26, 32	ディレクトリトラバーサル攻撃	
隠れフィールド	102	条件分岐	57		
型	56	昇順	38	144	
カラム型	31	状態	162	テキストフィールド	
関数	64	小なり記号	36	45, 53	
関数従属する	23	情報無損失分解	25	データ型	
関数従属性	23	真	37	31	
完全関数従属性	23	シングルクォート	57, 146	データ削除	
【き】		【す】		92	
偽	37	推移的関数従属性	24	データ追加	
キー	56	数値パラメータ	140	75	
旧形式	38	ステートメント	18	データの検索	
強制ブラウジング	134	ステートレス	162	35	
共通ファイル化	91			データの削除	
				42	
				データの変更	
				42	
				データベース層	
				5	
				データ編集	
				82	
				デバッグ情報	
				151	

デフォルト値制約	32
テーブル	22
【と】	
問合せ	35, 66
等結合	38, 71
等号	36, 58
等号否定	36, 58
動的に生成される情報の提供	3
通し番号	32
ドキュメントルート	134
特殊文字	142
トラバーサル攻撃	144
ドロップダウンメニュー	59
【な】	
ナル	31
【に】	
入力ミス	169
【は】	
配列	90
——のキー	56
——の添え字	56
バージョン番号	151
パスワードの設定	18
バックスラッシュ	146
バッチ処理	13
バッチファイル	10
パラメータ	51, 56
パラメータ名	56
半角スペース	139
判定不能	37
【ひ】	
比較演算子	36, 58
比較述語	36

非キー	23
非第1正規形	22
【ふ】	
ファイル一覧表示機能	111
ファイル検索機能	112
ファイル指定フィールド	102
ファイル転送機能	111
ファイル表示機能	112
フォーム	45
複合検索	37
複数の列からなる主キー	29
複数列からなるユニークキー	31
不正ユーザ	169
不成立	37
不定	37
部分関数従属性	23
不明	31
ブラックリスト	138
プレゼンテーション層	5
プログラムの提供	3
文	18
【へ】	
ページ遷移	80
変数	56, 163
——の置き換え	69
変数宣言	56
【ほ】	
ホワイトリスト	138
【み】	
未定	31
【む】	
無意味	31

【め】	
メソッド	51
【も】	
文字列パラメータ	140
【ゆ】	
ユーザアカウント	8
ユーザどうしの インタラクション	3
ユニーク制約	28, 31
【ら】	
ラジオボタン	45, 52
【り】	
リクエストパラメータ	51, 56
リセットボタン	45, 54
リモートホスト	169
リレーショナルデータベース 管理システム	5
リロード	78
【れ】	
例題アプリ	45
連想配列	56
【ろ】	
ログイン	156, 168
論理演算子	37, 58
論理積	58
論理和	58
【わ】	
ワイルドカード	37
ワнтаイムチケット	158, 165

【A】	
action 属性	51, 85
addslashes	146
AMP	61
AND	37
ANSI 方式	38
Apache	1
Apache HTTP Server	45
array	90
array_search	90
ASC	38
ASCII コード	146
AUTO_INCREMENT	32

【B】	
basename	104, 109
【C】	
CGI	3
CHAR	31
checkbox	92
checked 属性	53
Content-Type	109
Cookie	163
CREATE DATABASE 文	27
CREATE TABLE 文	28
CREATE USER 文	19

CSV ファイル	15, 33
CURRENT_TIMESTAMP	116
【D】	
DAME	125
DATE	31
DATETIME	31
DEFAULT	32
DELETE 文	42
desc;	38
DF	166
DROP DATABASE 文	12
DROP TABLE 文	12, 42
DROP USER 文	12

- [E]**
- echo コマンド 55
 - enctype 属性 101
 - ENT_COMPAT 142
 - ENT_NOQUOTES 142
 - ENT_QUOTES 142
 - exit 65
- [F]**
- FIELDS TERMINATED BY 34
 - file 102
 - FILE 権限 34
 - Flash 3
 - foreach 文 9
 - FORM タグ 51
 - FROM 句 35
- [G]**
- GET 51
 - get_magic_quotes_gpc 150
 - gethostbyaddr 169
 - GRANT 文 9, 18
- [H]**
- header 79
 - hidden 102
 - htmlspecialchars 142
 - HTML 埋め込み型言語 50
 - HTML フォーム 45
 - HTML 文書 3
 - HTTP リクエスト 63
 - HTTP レスポンス 64
- [I]**
- ID 26
 - IDENTIFIED BY~ 19
 - identifier 26
 - if 文 57
 - image/jpeg 109
 - imagecreatefromjpeg 106
 - imagejpeg 106
 - include 91
 - INPUT タグ 52
 - INSERT 文 11, 33, 77
 - INT 31
 - INTEGER 31
 - is_numeric 80
 - is_uploaded_file 103
- [J]**
- JavaScript 3
 - Java アプレット 3
- [L]**
- LAMP 61
 - LIKE 演算子 37
 - LIKE 述語 36, 69
 - LINES TERMINATED BY 34
 - LOAD DATA INFILE 文 17, 33
- [M]**
- magic_quote_gpc=Off 149
 - magic_quotes_gpc=On 146
 - MAX_FILE_SIZE 101
 - maxlength 属性 54
 - mb_convert_encoding 149
 - method 属性 51
 - MIME 105
 - MIME タイプ 105
 - MIME メディアタイプ 105
 - move_uploaded_file 103
 - multipart/form-data 101
 - my.ini 18
 - MySQL 1, 8
 - mysql_connect 65
 - mysql_fetch_array 64
 - mysql_query 65
 - mysql_select_db 65
 - MySQL モニタ 9, 10, 12
- [N]**
- name 属性 52, 53, 54
 - NATURAL JOIN 39
 - NOT 37
 - NOT NULL 31
 - NOT NULL 制約 28, 31
 - NULL 31
 - NULL 述語 37
 - NULL バイト攻撃 144
 - NULL 文字 146
- [O]**
- OLD_PASSWORD 9, 19
 - old-passwords 18
 - One fact in One place 25
 - One fact in One relation 25
 - OPTION タグ 59
 - OR 37
 - ORDER BY 句 35, 38
- [P]**
- pathinfo 109
 - PHP 1, 3, 45
 - php.ini 104, 146, 149, 167
 - PHPSESSID 167
 - PHP 関数 64
- PHP スクリプト 45
- PHP の検査機能 140
- POST 51
- POST メソッド 78, 95
- PRIMARY KEY 29, 32
- [Q]**
- QUIT 18
 - QUIT コマンド 9
- [R]**
- radio 52
 - RDBMS 5
 - Referer ヘッダフィールド 143
 - require 91
 - reset 54
 - REVOKE 文 12, 18
- [S]**
- SELECT タグ 59
 - SELECT 文 11, 35
 - ServerSignature Off 151
 - ServerSignature On 151
 - session_id 165
 - session_regenerate_id 168
 - session_start 164
 - SET PASSWORD 9
 - SET PASSWORD 文 19
 - Shift JIS 146
 - SHOW COLUMNS 文 18
 - SHOW DATABASES 文 12
 - SHOW TABLES 文 18
 - size 属性 53, 54
 - SQL インジェクション 138
 - state 162
 - stripslashes 140, 146
 - strtolower 107
 - submit 54
- [T]**
- TABLE タグ 64
 - text 53
 - TIME 31
 - trim 68
 - type 属性 52
- [U]**
- UNIQUE 31
 - UPDATE 文 42, 86
 - urlencode 86
 - USE 18
- [V]**
- value 属性 52, 53, 54

VARCHAR	31	3層クライアントサーバシステム	5	.	69
				.=	69
【w】		3層構造	63	.htaccess	136
WAMP	61	3値論理	37	@	107
Webアプリケーション	4, 45	5C問題	147	_	37
Webアプリケーション構築言語		~~~~~		{ }	69
	5	θ方式	38		58
Webサーバ	3, 4	!=	58	+	139
Web製品データベース	61	"	57	<?= ~ ?>	55
Webデータベース	5, 61	\$	56	<?php ~ ?>	55
Webファイラ	97	\$_FILES	103	<=	36
Webファイルデータベース		\$_GET	57	<>	36
	97, 111	\$_POST	57	=	36, 56
Webブラウザ	5	\$_REQUEST	56	==	58
WHERE句	11, 35	\$_SERVER	57	>	36
while文	64	\$_SESSION	164	>=	36
【数字】		%	37	¥	69
3階層クライアントサーバシステム	63	&&	58	¥N	31
		,	57		
		*	35		

速水 治夫 (はやみ はるお)

1970年 名古屋大学工学部応用物理学卒業
 1972年 名古屋大学大学院工学研究科博士前期課程修了 (応用物理学専攻)
 1972年
 ~98年 日本電信電話公社 (現NTT) 勤務
 1993年 博士 (工学)
 1994年
 ~98年 電気通信大学客員教授 (兼務)
 1997年 工学院大学非常勤講師 (兼務)
 1998年 神奈川工科大学教授
 現在に至る
 2004年 Workflow Management Coalition (WfMC) Fellow
 2007年 情報処理学会フェロー

古井 陽之助 (ふるい ようのすけ)

1993年 九州大学大学院工学研究科修士課程修了
 1993年~
 2001年 日本アイ・ビー・エム株式会社勤務
 2001年
 ~04年 九州大学大学院システム情報科学府
 博士後期課程 (単位取得後退学)
 博士 (情報科学)
 2004年
 ~07年 神奈川工科大学助手
 2007年 九州産業大学講師
 2012年 九州産業大学准教授
 現在に至る

服部 哲 (はっとり あきら)

2004年 名古屋大学大学院人間情報学研究科
 博士後期課程 (単位取得満期退学)
 博士 (学術)
 2004年 神奈川工科大学助手
 2007年 神奈川工科大学助教
 2010年 神奈川工科大学准教授
 2014年 駒澤大学准教授
 現在に至る

Web データベースの構築技術

Web Database Development Technology

© Hayami, Furui, Hattori 2009

2009年10月8日 初版第1刷発行
 2017年9月25日 初版第2刷発行



検印省略

編著者 速水治夫
 著者 古井陽之助
 服部哲
 発行者 株式会社 コロナ社
 代表者 牛来真也
 印刷所 萩原印刷株式会社
 製本所 有限会社 愛千製本所

112-0011 東京都文京区千石4-46-10
発行所 株式会社 コロナ社
 CORONA PUBLISHING CO., LTD.
 Tokyo Japan
 振替 00140-8-14844・電話 (03)3941-3131 (代)
 ホームページ <http://www.coronasha.co.jp>

ISBN 978-4-339-02440-1 C3055 Printed in Japan

(齋藤)



JCOPY <出版者著作権管理機構 委託出版物>

本書の無断複製は著作権法上での例外を除き禁じられています。複製される場合は、そのつど事前に、出版者著作権管理機構 (電話 03-3513-6969, FAX 03-3513-6979, e-mail: info@jcopy.or.jp) の許諾を得てください。

本書のコピー、スキャン、デジタル化等の無断複製・転載は著作権法上での例外を除き禁じられています。購入者以外の第三者による本書の電子データ化及び電子書籍化は、いかなる場合も認められません。落丁・乱丁はお取替えいたします。