23. RDB システム管理に関する知識 I

1. 科目の概要

関係データベースの運用管理機能とその管理方法について、具体的な内容と管理のための知識を解説する。バックアップとリカバリ、セキュリティに対する配慮、データベース運用時の動作監視といった基本的な項目について説明する。

2. 習得ポイント

本科目の学習により習得することが期待されるポイントは以下の通り。

習得ポイント	説　明	シラバスの対応コマ
I-23-1. データベース運用管理の目的、方針、主要な問題点と対策	データベースの運用管理が必要になる状況を示し、運用管理の必要性と目的、運用の方針、データベース運用時に遭遇する主要な問題点やリスクとその対策について説明する。	1
I-23-2. データベース運用管理の基本的な項目と作業内容	データベース運用管理の基本的な項目と作業内容を解説する。定期的に行わなければならない作業、継続した利用の際に発生する可能性がある問題に対する作業など、データベース運用に不可欠な作業項目を順序だてて説明する。	1
I-23-3. 運用設計の概要	データベース運用設計作業の内容について述べる。最適なデータベース運用設計のアプローチ方法、アプリケーション設計への反映方法やデータベース運用計画への反映方法、監視計画の策定方法について説明する。またデータベース運用設計作業で検討すべき項目について、その作業内容と手順を説明する。	3
I-23-4. 障害の種類と障害からの復旧方法	データベース運用時に発生する障害の種類とその内容を示す。これらの障害に対して事前にとっておくべき対策と、障害が発生した際に復旧作業としてやらねばならないことの概要を説明する。	2
I-23-5. データベースのバックアップ	一般的なデータベース運用作業における基本項目のひとつとして、障害回復に備えるためのバックアップ作業について説明する。バックアップ作業の必要性、バックアップの種類、バックアップ作業手順などについて述べる。	2
I-23-6. データベースのリカバリ	一般的なデータベース運用作業における基本項目のひとつとして、障害発生時のリカバリ方法について述べる。データベースのリカバリ作業の必要性、具体的な手順を示し、リカバリ作業時の留意点などについて説明する。	5
I-23-7. ログの取得と復旧	データベース運用管理作業において復旧時に取るべき対策のひとつとして、ログの取得について説明する。取得したログの見方と障害の原因追及方法、ログを利用したリカバリ方法などについて解説する。	2,4
I-23-8. データベースのユーザ管理とアクセス制御	データベースにアクセスできるユーザを管理する方法と、アクセス制御の概念について、ユーザ管理およびアクセス制御を実現するための、基本的な作業手順を示す。またこれらに関する作業上の留意点を説明する。	4
I-23-9. データベースセキュリティの内容と留意点	データベース運用時に配慮すべきセキュリティの概要を紹介し、実際の運用作業において実施しなければならないこと、注意すべきポイントについて解説する。また実際にセキュリティ侵害が発生した際の対処方法について説明する。	4
I-23-10. データベース動作環境の管理計画と管理作業	データベースを正常に動作させるために実施しなければならない作業について、バックアッププランの策定、リカバリ方法の決定、データベース動作環境の監視といった一連の作業手順についてまとめる。	5

【学習ガイダンスの使い方】

1. 「習得ポイント」により、当該科目で習得することが期待される概念・知識の全体像を把握する。
2. 「シラバス」、「IT 知識体系との対応関係」、「OSS モデルカリキュラム固有知識」をもとに、必要に応じて、従来の IT 教育プログラム等との相違を把握した上で、具体的な講義計画を考案する。
3. 習得ポイント毎の「学習の要点」と「解説」を参考にして、講義で使用する教材等を準備する。

3. IT 知識体系との対応関係

「23. RDB システム管理に関する知識Ⅰ」と IT 知識体系との対応関係は以下の通り。

科目名	基本レベル（Ⅰ）					応用レベル（Ⅱ）									
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
23. RDBシステム管理に関するスキル	<データベース運用管理の目的と項目>	<データベースの運用作業と障害回復>	<データベース運用設計>	<データベースセキュリティ>	<データベースリカバリ設計>	<データベースの最適化>	<データベースのトラブル>	<データベースチューニング>	<データベース構築>	<データベースインデックスを用いた性能改善>	<MySQLの導入と運用>	<データベーストラブルシューティング>	<データベース運用環境構築>	<データベース運用>	<データベースチューニング>

[シラバス：http://www.ipa.go.jp/software/open/ossc/download/Model_Curriculum_05_23.pdf]

<IT 知識体系上の関連部分>

分野		科目名	1	2	3	4	5	6	7	8	9	10	11	12	13
組織関連事項と情報システム	1	IT-IAS 情報保証と情報セキュリティ	IT-IAS1. 基礎的な問題	IT-IAS2. 情報セキュリティの仕組み（対策）	IT-IAS3. 運用上の問題	IT-IAS4. ポリシー	IT-IAS5. 攻撃	IT-IAS6. 情報セキュリティ分野	IT-IAS7. フォレンジック（情報証拠）	IT-IAS8. 情報の状態	IT-IAS9. 情報セキュリティサービス	IT-IAS10. 脅威分析モデル	IT-IAS11. 脆弱性		
	2	IT-SP 社会的な観点とプロフェッショナルとしての課題	IT-SP1. プロフェッショナルとしてのコミュニケーション	IT-SP2. コンピュータの歴史	IT-SP3. コンピュータを取り巻く社会環境	IT-SP4. チームワーク	IT-SP5. 知的財産権	IT-SP6. コンピュータの法的問題	IT-SP7. 組織の中のIT	IT-SP8. プロフェッショナルとしての倫理的な問題と責任	IT-SP9. プライバシーと個人の自由				
応用技術	3	IT-IM 情報管理	IT-IM1. 情報管理の概念と基礎 [23-Ⅰ-5]	IT-IM2. データベース問合わせ言語	IT-IM3. データアーキテクチャ	IT-IM4. データモデリングとデータベース設計 [23-Ⅰ-3]	IT-IM5. データと情報の管理 [23-Ⅰ-1, 2, 4, 5]	IT-IM6. データベースの応用分野							
	4	IT-WS Webシステムとその技術	IT-WS1. Web技術	IT-WS2. 情報アーキテクチャ	IT-WS3. デジタルメディア	IT-WS4. Web開発	IT-WS5. 脆弱性	IT-WS6. ソーシャルソフトウェア							
ソフトウェアの方法と技術	5	IT-PF プログラミング基礎	IT-PF1. 基本データ構造	IT-PF2. プログラミングの基本的構成要素	IT-PF3. オブジェクト指向プログラミング	IT-PF4. アルゴリズムと問題解決	IT-PF5. イベント駆動プログラミング	IT-PF6. 再帰							
	6	IT-IPT 技術を統合するためのプログラミング	IT-IPT1. システム間通信	IT-IPT2. データ割り当てと交換	IT-IPT3. 統合的コーディング	IT-IPT4. スクリプティング手法	IT-IPT5. ソフトウェアセキュリティの実現	IT-IPT6. 種々の問題	IT-IPT7. プログラミング言語の概要						
	7	CE-SWE ソフトウェア工学	CE-SWE0. 歴史と概要	CE-SWE1. ソフトウェアプロセス	CE-SWE2. ソフトウェアの要求と仕様	CE-SWE3. ソフトウェアの設計	CE-SWE4. ソフトウェアのテストと検証	CE-SWE5. ソフトウェアの保守	CE-SWE6. ソフトウェア開発・保守ツールと環境	CE-SWE7. ソフトウェアプロジェクト管理	CE-SWE8. 言語翻訳	CE-SWE9. ソフトウェアのフォールトトレランス	CE-SWE10. ソフトウェアの構成管理	CE-SWE11. ソフトェアの標準化	
	8	IT-SIA システムインテグレーションとアーキテクチャ	IT-SIA1. 要求仕様	IT-SIA2. 調達/手配	IT-SIA3. インテグレーション	IT-SIA4. プロジェクト管理	IT-SIA5. テストと品質保証	IT-SIA6. 組織の特性	IT-SIA7. アーキテクチャ						
システム基盤	9	IT-NET ネットワーク	IT-NET1. ネットワークの基礎	IT-NET2. ルーティングとスイッチング	IT-NET3. 物理層	IT-NET4. セキュリティ	IT-NET5. アプリケーション分野	IT-NET6. ネットワーク管理							
	10	CE-NWK テレコミュニケーション	CE-NWK0. 歴史と概要	CE-NWK1. 通信ネットワークのアーキテクチャ	CE-NWK2. 通信ネットワークのプロトコル	CE-NWK3. LANとWAN	CE-NWK4. クライアントサーバコンピューティング	CE-NWK5. データのセキュリティと整合性	CE-NWK6. ワイヤレスコンピューティングとモバイルコンピューティング	CE-NWK7. データ通信	CE-NWK8. 組込み機器向けネットワーク	CE-NWK9. 通信技術とネットワーク概要	CE-NWK10. 性能評価	CE-NWK11. ネットワーク管理	CE-NWK12. 圧縮と伸張
			CE-NWK13. クラスタシステム	CE-NWK14. インターネットアプリケーション	CE-NWK15. 次世代インターネット	CE-NWK16. 放送									
	11	IT-PT プラットフォーム技術	IT-PT1. オペレーティングシステム	IT-PT2. アーキテクチャと機構	IT-PT3. コンピュータインフラストラクチャ	IT-PT4. デプロイメントソフトウェア	IT-PT5. ファームウェア	IT-PT6. ハードウェア							
	12	CE-OPS オペレーティングシステム	CE-OPS0. 歴史と概要	CE-OPS1. 並行性	CE-OPS2. スケジューリングとディスパッチ	CE-OPS3. メモリ管理	CE-OPS4. セキュリティと保護	CE-OPS5. ファイル管理	CE-OPS6. リアルタイムOS	CE-OPS7. OSの概要	CE-OPS8. 設計の原則	CE-OPS9. デバイス管理	CE-OPS10. システム性能評価		
コンピュータアーキテクチャ	13	CE-CAO コンピュータのアーキテクチャと構成	CE-CA00. 歴史と概要	CE-CA01. コンピュータアーキテクチャの基礎	CE-CA02. メモリシステムの構成とアーキテクチャ	CE-CA03. インタフェースと通信	CE-CA04. デバイスサブシステム	CE-CA05. CPUアーキテクチャ	CE-CA06. 性能・コスト評価	CE-CA07. 分散・並列処理	CE-CA08. コンピュータによる計算	CE-CA09. 性能向上			
複数領域にまたがるもの	14	IT-ITF IT基礎	IT-ITF1. ITの一般的なテーマ	IT-ITF2. 組織の問題	IT-ITF3. ITの歴史	IT-ITF4. IT分野（学科）とそれに関連のある分野（学科）	IT-ITF5. 応用領域	IT-ITF6. IT分野における数学と統計学の活用							
	15	CE-ESY 組込みシステム	CE-ESY0. 歴史と概要	CE-ESY1. 低電力コンピューティング	CE-ESY2. 高信頼性システムの設計	CE-ESY3. 組込み用アーキテクチャ	CE-ESY4. 開発環境	CE-ESY5. ライフサイクル	CE-ESY6. 要件分析	CE-ESY7. 仕様定義	CE-ESY8. 構造設計	CE-ESY9. テスト	CE-ESY10. プロジェクト管理	CE-ESY11. 並行設計（ハードウェア、ソフトウェア	CE-ESY12. 実装
			CE-ESY13. リアルタイムシステム設計	CE-ESY14. 組込みマイクロコントローラ	CE-ESY15. 組込みプログラム	CE-ESY16. 設計手法	CE-ESY17. ツールによるサポート	CE-ESY18. ネットワーク型組込みシステム	CE-ESY19. インタフェースシステムと混合信号システム	CE-ESY20. センサ技術	CE-ESY21. デバイスドライバ	CE-ESY22. メンテナンス	CE-ESY23. 専門システム	CE-ESY24. 信頼性とフォールトトレランス	

4. OSS モデルカリキュラム固有の知識

OSS モデルカリキュラム固有の知識は特になく、各回の内容は IT 知識体系と共通した RDB に関する内容を扱う。

科目名	第1回	第2回	第3回	第4回	第5回
23. RDB システム管理に関する知識Ⅰ	(1) データベース運用管理の目的 (2) データベースの運用と管理	(1) 障害回復	(1) 最適なデータベース運用設計のアプローチ (2) 運用設計の検討項目 (3) 監視計画	(1) データベースセキュリティの概要 (2) 基本的な対策 (3) システム構成の問題	(1) リカバリのためのバックアッププラン (2) リカバリ方法の決定 (3) データベース動作環境の監視

（網掛け部分は IT 知識体系で学習できる知識を示し、それ以外は OSS モデルカリキュラム固有の知識を示している）

スキル区分	OSS モデルカリキュラムの科目	レベル
RDB 分野	23　RDB システム管理に関する知識 I	基本
習得ポイント	I-23-1. データベース運用管理の目的、方針、主要な問題点と対策	
対応する コースウェア	第 1 回（データベース運用管理の目的と項目）	

I-23-1. データベース運用管理の目的、方針、主要な問題点と対策

データベースの運用管理が必要になる状況を示し、運用管理の必要性と目的、運用の方針、データベース運用時に遭遇する主要な問題点やリスクとその対策について説明する。

【学習の要点】

＊ データベースを適切に運用管理することで、データベースにまつわる問題を未然に防ぐことができ、万一の問題発生時にも円滑に対処することができる。

＊ データベース運用時に遭遇する問題点やリスクを把握しておくことで、運用管理の面で具体的な対策をたてることができる。

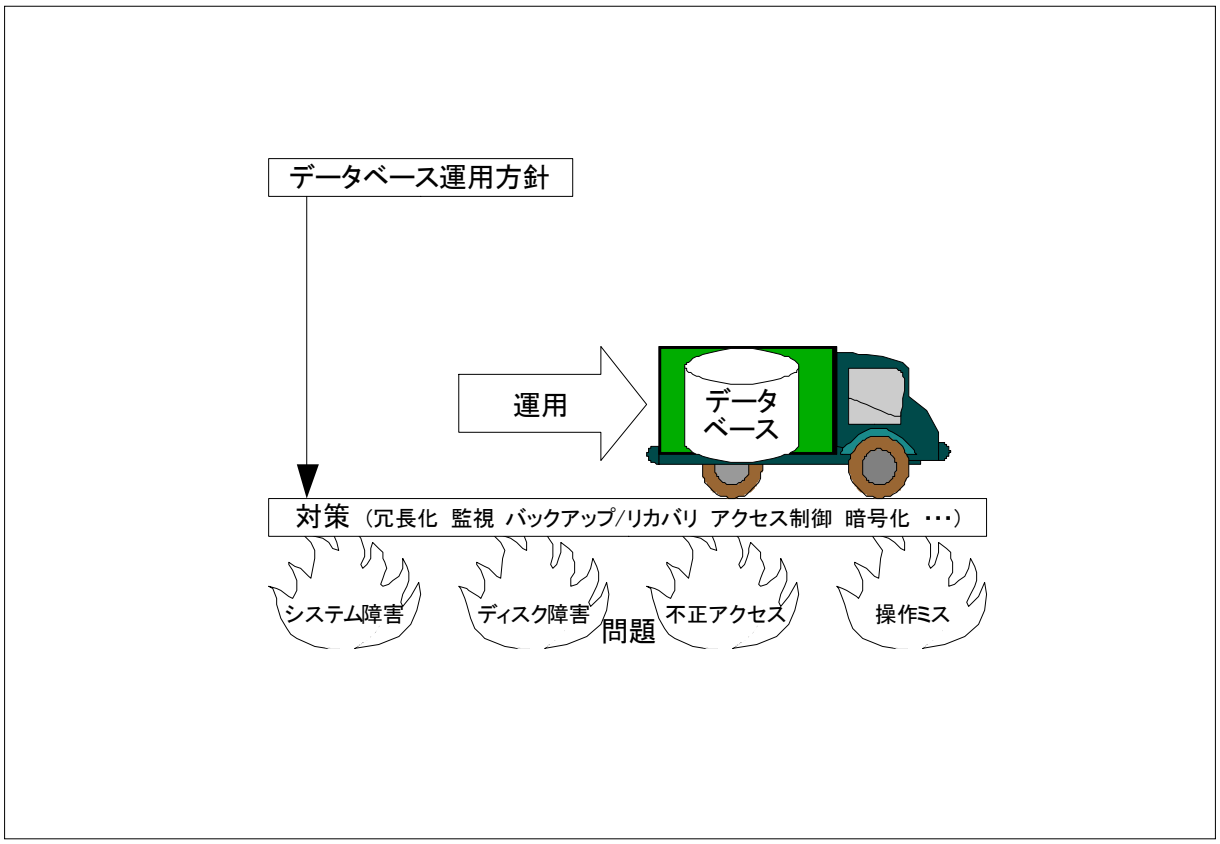

図 I-23-1.　データベース運用の基本概念

【解説】

1) データベース運用管理の必要性と目的

業務でのデータベース利用では、データの損失や DBMS による処理の失敗などの障害が発生すると、業務に重大な被害を与える場合がある。システム開発でのデータベース利用でも、障害によりデータベースの再構築が必要になると開発作業に大きな遅れを生じる。データベース運用時に遭遇する諸問題を未然に防いだり、万一の問題発生時に円滑に対処したりできることはたいへん重要であり、データベース運用管理の目的のひとつとなる。

2) データベース運用時に遭遇する主要な問題点やリスクとその対策

データベース運用時に遭遇する主要な問題点と、主な対策を列挙する。

* システム障害等によるデータベースへのアクセス不可
  → システムの冗長化、システム稼動の監視
* ディスク障害等によるデータベースの破損
  → ディスクの冗長化、ディスクアクセス監視、バックアップ、リカバリ
* データベース利用によるディスクフル
  → ディスク容量監視、データベースサイズの拡張、スキーマ見直し、不要データの削除/退避
* DBMS 処理時間の増加
  → CPU/メモリ監視、SQL のチューニング、スキーマ見直し、不要データの削除/退避
* 不正アクセスや操作ミスによるデータ盗用/損失/改ざん
  → アクセス制御、暗号化、アクセスログ取得、バックアップ、リカバリ

3) データベース運用の方針

データベース運用の際は、次のような方針を策定することが重要である。

* データベースを利用する時間帯
* メンテナンスによるデータベースを利用停止にする時間帯
* 万一の問題発生時に対処できる時間猶予
* 運用体制（メンバー、役割、問題発生時の連絡手順等）
* データの保存期間、バックアップ期間
* バックアップの範囲、間隔、手順
* リカバリ手順
* システム監視の設定、確認方法や警告通知
* セキュリティレベル(個人情報その他セキュリティ上重要なデータへのアクセス許可等)
* データベースユーザの分類とアクセス権
* 定期的に必要となる作業の選定
* 予測される問題とその具体的な対処方法

スキル区分	OSS モデルカリキュラムの科目	レベル
RDB 分野	23　RDB システム管理に関する知識 I	基本
習得ポイント	I-23-2. データベース運用管理の基本的な項目と作業内容	
対応する コースウェア	第 1 回（データベース運用管理の目的と項目）	

I-23-2. データベース運用管理の基本的な項目と作業内容

データベース運用管理の基本的な項目と作業内容を解説する。定期的に行わなければならない作業、継続した利用の際に発生する可能性がある問題に対する作業など、データベース運用に不可欠な作業項目を順序だてて説明する。

【学習の要点】

＊ 運用管理の定期的な作業によって、問題発生の予防や、万一の問題発生時の被害を最小限にとどめることができる。

＊ 発生の想定される問題とその対策手順を確立しておくことで、万一の問題発生時の被害を最小限にとどめることができる。

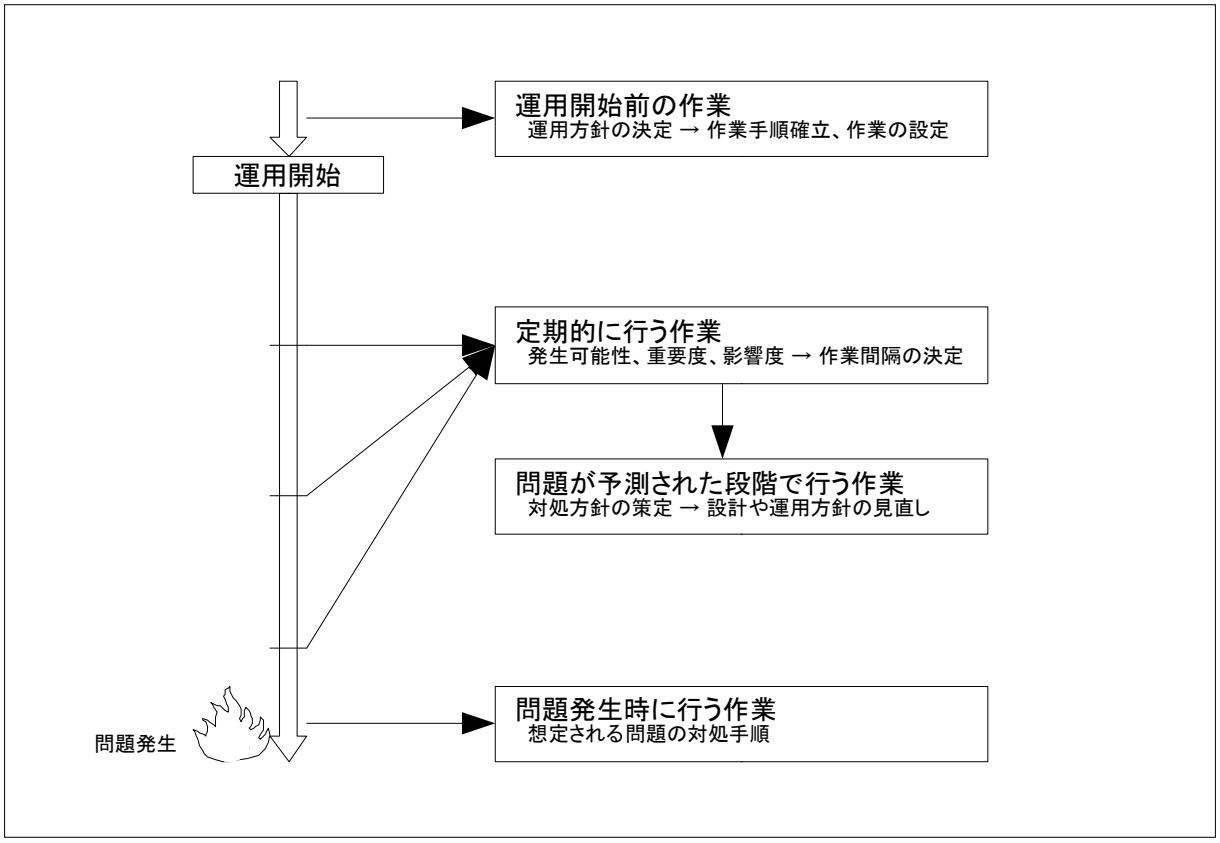

図 I-23-2.　データベース運用管理の各種作業

【解説】

1) 運用開始前の作業

データベース運用開始前に行う作業とは、運用方針を決定し、その方針に基づいて、作業手順の確立や、自動化できる定期的な作業の設定を行うことである。

＊ 運用方針の策定

＊ アクセス権の設定、暗号化の設定

＊ DBMS 起動/終了手順の確立、自動起動/自動終了の設定

＊ バックアップ手順、リカバリ手順の確立、自動バックアップの設定

＊ システム監視(CPU、メモリ、ディスク、ネットワーク等)の設定(監視間隔、しきい値、警告通知等)

＊ ログ出力の設定

＊ 運用テスト

2) 定期的に行う作業

データベース運用時の定期的な作業の多くは、短い間隔で行うほど問題発生の予防や万一の問題発生時の対処に有効であるので、問題発生の可能性、問題回避の重要度、利用者への影響を考慮し、定期作業の間隔を決定するのが望ましい。

＊ 保存期間を過ぎたデータ、その他不要なデータの削除または退避

＊ 索引の再構築

＊ バックアップ

＊ システム監視と傾向の把握

＊ ログの確認

3) 問題が予測された段階で行う作業

システム監視等により、問題発生の可能性が高いと予測された場合は、対処方針を策定し以下の作業を行う。

＊ データベース設計(スキーマ等)の見直し

＊ 運用方針の見直し

＊ 定期作業の見直し

4) 問題発生時に行う作業

万一問題が発生した場合には、迅速かつ確実に対処するため、想定される問題の対処手順を確立しておく。

＊ リカバリ

5) その他非定期的な作業

OS や DBMS その他のソフトウェアのアップデート時、データベーススキーマ変更時などに行う作業をあげる。

＊ DBMS の停止/起動

＊ 既存データの新システムへの移行

スキル区分	OSS モデルカリキュラムの科目	レベル
RDB 分野	23　RDB システム管理に関する知識 I	基本
習得ポイント	I-23-3. 運用設計の概要	
対応する コースウェア	第 3 回（データベース運用設計）	

I-23-3. 運用設計の概要

データベース運用設計作業の内容について述べる。最適なデータベース運用設計のアプローチ方法、アプリケーション設計への反映方法やデータベース運用計画への反映方法、監視計画の策定方法について説明する。またデータベース運用設計作業で検討すべき項目について、その作業内容と手順を説明する。

【学習の要点】

＊ 従来は、システム開発に偏ったデータベース設計のアプローチが多くみられたが、システムのライフサイクル全体を見据えたデータベースの運用設計が重要視されてきている。

＊ アプリケーション設計と運用設計とは、双方を考慮して設計するよう、注意を要する。

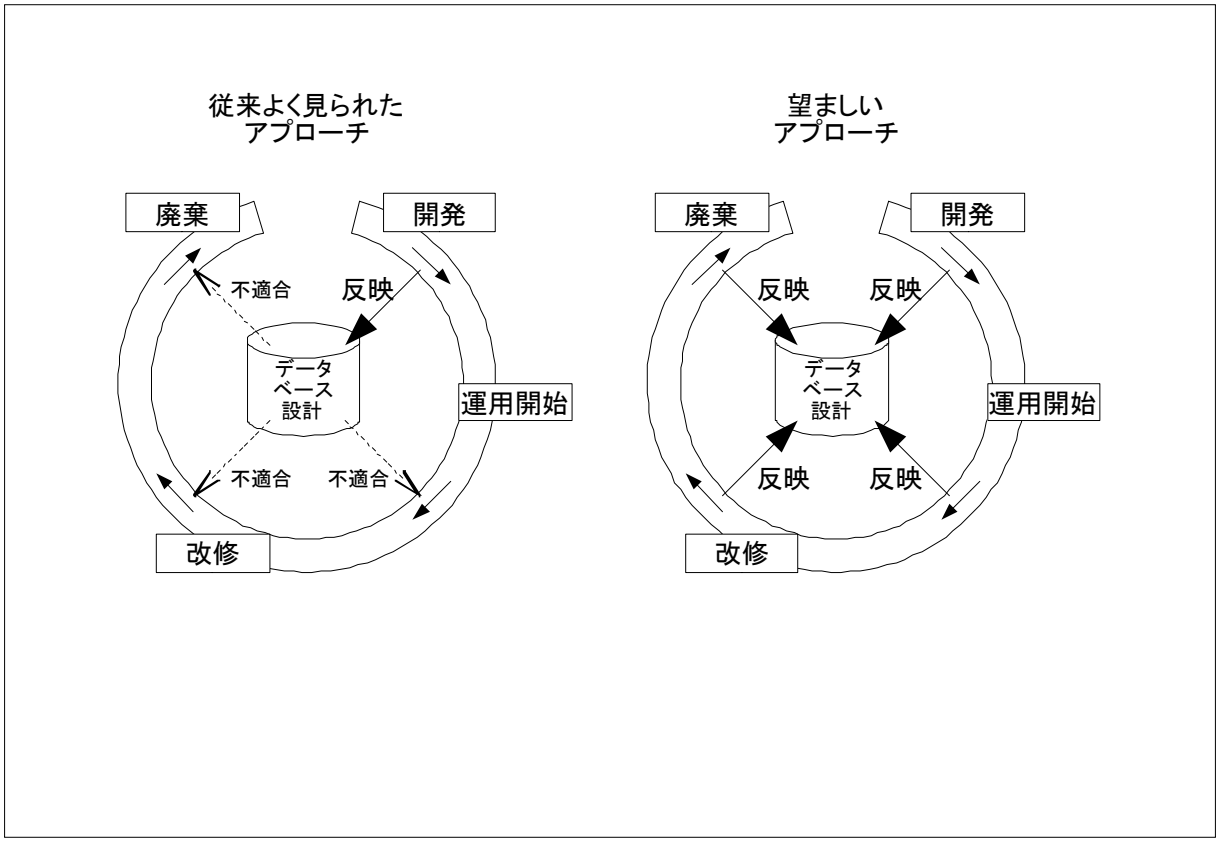

図 I-23-3.　システムライフサイクルとデータベース設計のアプローチ

【解説】

1) 運用設計のアプローチ

システム開発を優先し、データベースの設計やアプリケーション開発が一通り終わってからデータベース運用の設計をするというアプローチでは、次のような問題が起こりうる。

* アプリケーションからのデータベースアクセスが、運用上のセキュリティ要件を満たせない。
* DB 運用が DBMS に依存した設計であるがゆえに、システムのリプレースに際し、DB 運用についても膨大な変更が必要になる。

これらの問題を防ぐため、システムのライフサイクル全体を見据えて運用設計を行い、システム開発の段階から反映していくというアプローチが望まれる。

2) 作業内容と手順

* 運用方針の策定
  利用時間帯、メンテナンス時間帯、体制、バックアップの範囲や間隔、セキュリティレベル、リプレース時期、廃棄方法などの要件を踏まえ、データベース運用の全体方針を策定する。
* 具体的な要件の洗い出しと作業手順の確立
  運用方針をもとに、アクセス権の設定、暗号化の設定、監視項目、ログ出力設定、バックアップ世代管理などの具体的な要件を洗い出し、また、起動/終了手順、バックアップ/リカバリ手順、等の具体的な作業手順を確立する。
* アプリケーション設計への反映
  アプリケーションの基本設計によって作成された概念スキーマをもとに、運用設計の要件を満たすように内部スキーマおよび外部スキーマの設計を行う。運用設計を反映した外部スキーマをもとに、アプリケーションの詳細設計を行う。
* 運用計画、監視計画の策定
  運用設計をもとに、具体的な運用作業計画(DBMS の起動/終了時刻、バックアップ時刻など)および監視計画(監視間隔、しきい値など)を策定する。
* 運用テスト
  運用開始前に運用設計に即してテストを行い、運用設計に問題がないかをチェックする。
* 運用設計の見直し
  運用テスト時や運用開始後に問題が発見された場合、その他定期的に運用設計の修正必要性を確認し、必要に応じて運用設計を修正する。

スキル区分	OSS モデルカリキュラムの科目	レベル
RDB 分野	23　RDB システム管理に関する知識 I	基本
習得ポイント	I-23-4. 障害の種類と障害からの復旧方法	
対応する コースウェア	第 2 回（データベースの運用作業と障害回復）	

I-23-4. 障害の種類と障害からの復旧方法

データベース運用時に発生する障害の種類とその内容を示す。これらの障害に対して事前にとっておくべき対策と、障害が発生した際に復旧作業としてやらねばならないことの概要を説明する。

【学習の要点】

＊ 想定される障害の種類を把握し、事前対策を講じることで、障害発生のリスクを減らすことができる。

＊ 個々の障害に対する復旧作業を把握しておくことで、万一の障害発生にも速やかに対処することができる。

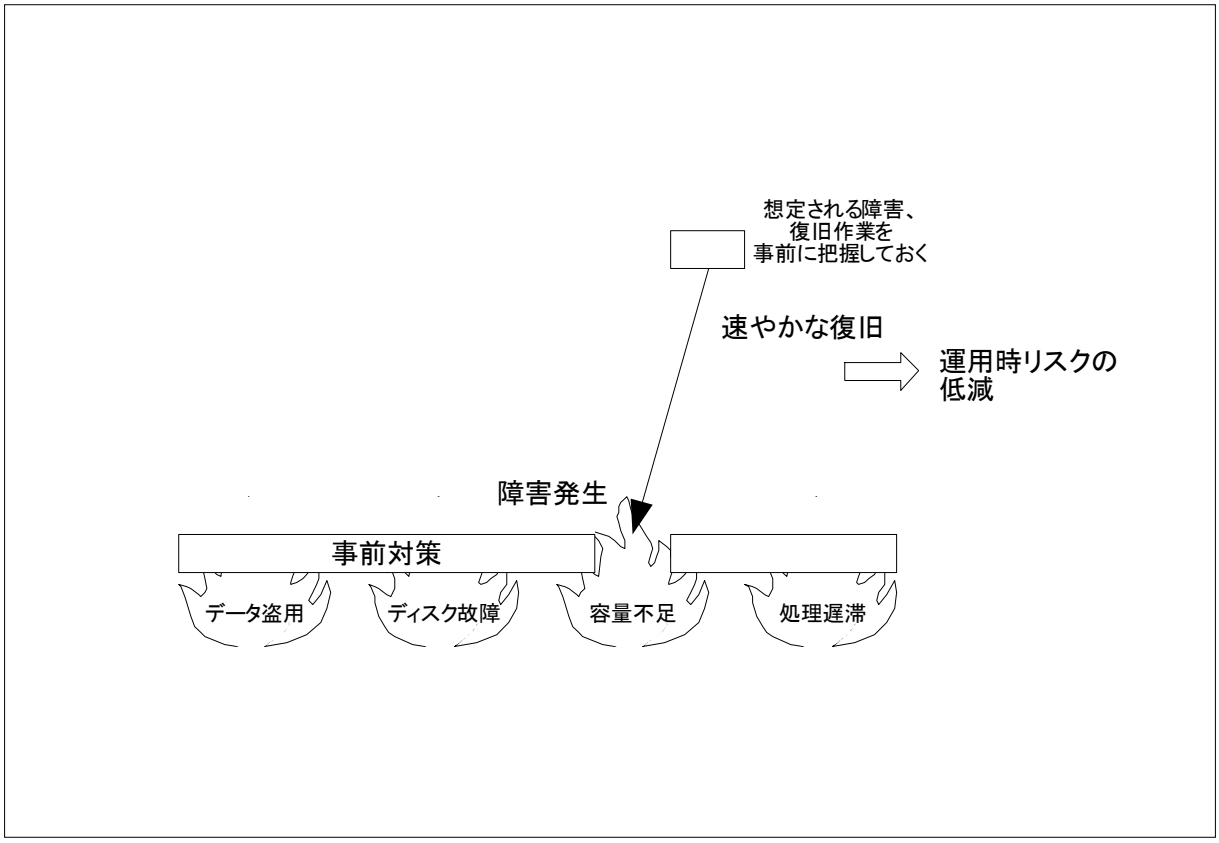

図 I-23-4.　障害復旧のポイント

【解説】

1) データの盗用/損失/改ざん

不正アクセスや操作ミスにより、データが盗用/損失/改ざんされる。

＊ 事前対策
適切なユーザ管理(最小限の権限付与、パスワード管理)、バックアップの取得、アクセスログの出力と監視

＊ 障害発生時の復旧作業
バックアップデータのリストア、不正アクセス経路の遮断、不正アクセスユーザの無効化、通信経路の暗号化、データの暗号化、アプリケーションの脆弱性排除

2) 記憶装置(ディスク)の故障

ディスクの故障により、ディスク上のデータベースにアクセスできなくなる。

＊ 事前対策
ディスクの冗長化、ディスクアクセス監視、バックアップの取得

＊ 障害発生時の復旧作業
バックアップデータのリストア

3) 記憶装置(ディスク)やファイルの容量不足

データベースのデータが肥大化し、データベースファイルの空きやディスクの空きがなくなる。

＊ 事前対策
ディスク使用率監視、データベースファイル使用率監視、不要データの削除/退避

＊ 障害発生時の復旧作業
ディスク増設、データベースファイルサイズ拡張、スキーマ見直し、不要データの削除/退避

4) DBMS の処理遅滞

CPU、メモリ、ディスクアクセス、ネットワークの使用が増え、処理に時間がかかるようになる。

＊ 事前対策
CPU/メモリ/ディスクアクセス/ネットワーク監視、不要データの削除/退避

＊ 障害発生時の復旧作業
CPU 増強、メモリ増設、ディスク分散、ネットワーク増強、SQL チューニング、スキーマ見直し、不要データの削除/退避

5) コンピュータウィルス感染

ウィルスに感染し、データの損失、DBMS のダウンなどが起こる。

＊ 事前対策
ウィルス検査、アクセスログの出力と監視、バックアップの取得

＊ 障害発生時の復旧作業
ネットワーク分断、ウィルス駆除、バックアップデータのリストア

スキル区分	OSS モデルカリキュラムの科目	レベル
RDB 分野	23　RDB システム管理に関する知識 I	基本
習得ポイント	I-23-5. データベースのバックアップ	
対応する コースウェア	第 2 回（データベースの運用作業と障害回復）	

I-23-5. データベースのバックアップ

一般的なデータベース運用作業における基本項目のひとつとして、障害回復に備えるためのバックアップ作業について説明する。バックアップ作業の必要性、バックアップの種類、バックアップ作業手順などについて述べる。

【学習の要点】

* データベースの運用作業において、バックアップ/リカバリは、最も重要な作業項目である。
* 近年は DBMS を停止できないシステムが増えており、単なるファイルのコピーではない、オンラインバックアップが求められている。

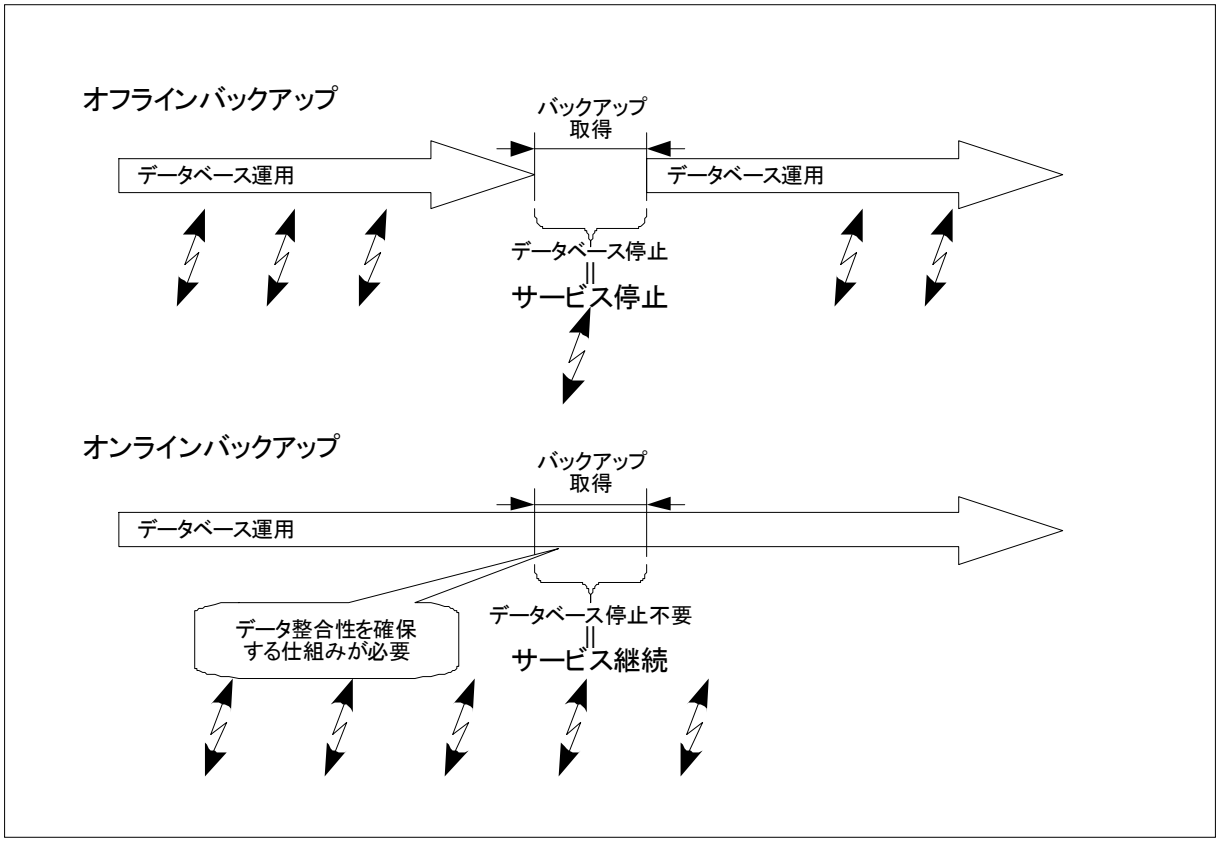

図 I-23-5.　オフラインバックアップとオンラインバックアップ

【解説】

1) バックアップの必要性

記憶装置の故障、ユーザの操作ミス、コンピュータウィルスへの感染等によってデータベースが破損した場合、復旧に莫大な人手と時間を費やさねばならなくなったり、復旧が困難になったりする。データのバックアップを行っておくことで、バックアップを取得した時点の状態までは復旧(リカバリ)が容易になる。

2) バックアップの世代管理

バックアップデータは最新のものだけを優先して保管を行うのではない。ユーザの操作ミスによるデータ削除やコンピュータウィルス感染などがバックアップ取得後に判明した場合に備えて、過去に取得したバックアップデータを複数管理し、リカバリ可能な時点を複数用意しておく。これをバックアップの世代管理という。

3) バックアップの種類（バックアップ取得時の状態による分類）

＊ オフラインバックアップ
DBMS を停止して行うバックアップ。データベースファイルのクローズにより、ファイルのコピーとして安易なバックアップが可能である。（近年はバックアップのためにDBMSを停止することが許されないシステムが増えている。）

＊ オンラインバックアップ
DBMS を起動した状態で行うバックアップ。DBMS の機能やサードパーティ製のツールを利用して行う。バックアップ処理中にデータを更新するトランザクションが処理されてしまうと、バックアップデータに不整合が起きてしまうため、更新処理をロックするなどの工夫が必要となる。

4) バックアップの種類（バックアップ取得の対象による分類）

＊ フルバックアップ
データベース全体のバックアップ。初回時はフルバックアップが必要になる。リカバリは容易だが、バックアップに時間と記憶装置の領域を要する。毎回フルバックアップを行うのは非効率である場合が多い。

＊ インクリメンタルバックアップ
前回のバックアップ時点からの増分/変更分のみを対象とするバックアップ。バックアップ時間と記憶装置の領域の節約になるが、リカバリ作業に多くの手順が必要となる。追加や変更の少ないデータベースに向いている。

＊ 部分バックアップ
重要なデータや変更のあった表などに対象を限定して行うバックアップ。場合によってはバックアップ時間が節約できリカバリ作業が容易になるが、データの整合性取得が困難となるリスクが高いので、バックアップの際は十分な注意が必要となる。

5) 作業手順

DBMS によるが、バックアップ手順は大まかに次のようになる。

＊ データの更新処理が比較的少ない時間帯を選び、バックアップ処理を実行する。

＊ 取得したバックアップデータは、データベースとは異なる記憶装置に退避しておく。

＊ 記憶装置のラベルやファイル名等で、バックアップ日時と対象が判別できるようにしておく。

スキル区分	OSS モデルカリキュラムの科目	レベル
RDB 分野	23　RDB システム管理に関する知識 I	基本
習得ポイント	I-23-6. データベースのリカバリ	
対応する コースウェア	第 5 回（データベースリカバリ設計）	

I-23-6. データベースのリカバリ

一般的なデータベース運用作業における基本項目のひとつとして、障害発生時のリカバリ方法について述べる。データベースのリカバリ作業の必要性、具体的な手順を示し、リカバリ作業時の留意点などについて説明する。

【学習の要点】

＊ データベースの運用作業において、バックアップ/リカバリは、最も重要な作業項目である。

＊ リカバリ計画を行うことで、万一の障害時に速やかにリカバリ作業を遂行できる。

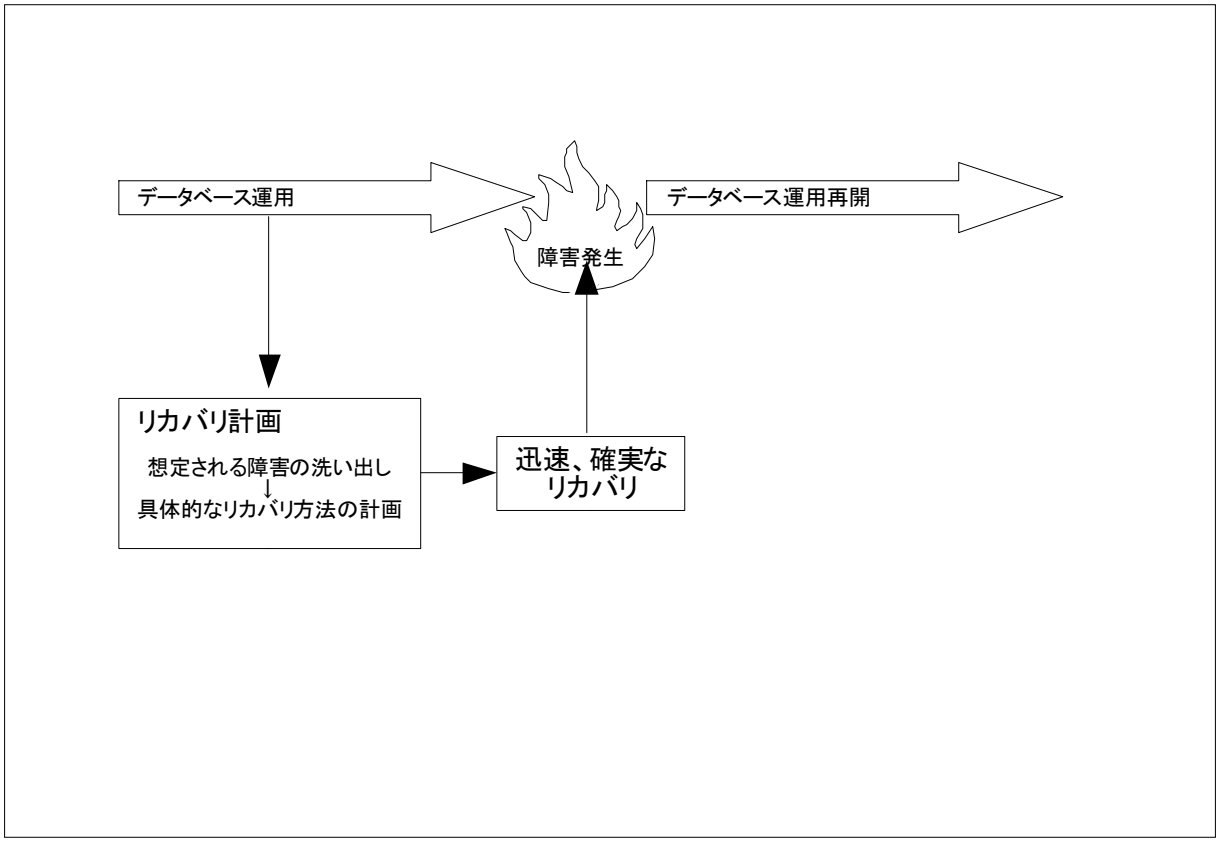

図 I-23-6.　データベースリカバリの概念

【解説】

1) リカバリ作業の重要性と留意点

データベースのバックアップを正しく行っていても、万一の障害の際、リカバリに時間を費やして長時間データベースを停止状態にしてしまったり、正しくリカバリできずにデータベースに不整合が生じたりというケースは避けなければならない。障害を想定し、速やかにリカバリできるよう計画しておくことが重要である。

2) リカバリ計画

＊ 想定される障害を洗い出す。
記憶装置の故障、マシントラブル、OS や DBMS の不具合、ユーザ操作ミス、ウィルス感染等

＊ 個々の想定される障害に対し、リカバリ方法を具体的に計画する。
作業時間帯、所要時間、データベースリカバリ前後の作業、どの時点の状態に復旧するか等

3) リカバリの手順例 ～ ディスクの故障の場合

＊ 障害確認とリカバリ作業開始を通知する。
＊ DBMS を停止する。(必要に応じて他のサービスを停止する)
＊ ディスクを交換する。
＊ 故障したディスクのファイルレベルでのバックアップデータを復元する。
＊ データベースを最新のバックアップの時点に復旧する。(必要に応じて DBMS を起動する。)
インクリメンタルバックアップを行っていた場合は、最新のフルバックアップデータを適用後、それ以降のすべてのインクリメンタルバックアップデータを順に適用する。
＊ 停止していたサービスを起動する。
＊ 動作確認を行う。
＊ リカバリ作業完了を通知する。

4) リカバリの手順例 ～ ウィルス感染の場合

＊ 障害確認とリカバリ作業開始を通知する。
＊ データベースサーバをネットワークから切り離す。
＊ 必要に応じて他のサービスや OS を停止する。
＊ データベースやログから感染箇所と感染時期を特定する。(必要に応じて DBMS を停止する)
＊ 特定した情報等から、復元方針を速やかに決定する。
復元方針は、以下のようなものを条件に応じて複数、具体的に計画しておく。
- ウィルス感染の直前のバックアップ時点に復旧する
- ウィルス駆除ソフトにより駆除する

＊ 決定した方針に従って作業する。
＊ 停止していたサービスシステムと DBMS を起動する。
＊ ウィルス検査を行う。
＊ 動作確認を行う。
＊ リカバリ作業完了を通知する。

スキル区分	OSS モデルカリキュラムの科目	レベル
RDB 分野	23　RDB システム管理に関する知識 I	基本
習得ポイント	I-23-7. ログの取得と復旧	
対応する コースウェア	第 2 回（データベースの運用作業と障害回復） 第 4 回（データベースセキュリティ）	

I-23-7. ログの取得と復旧

データベース運用管理作業において復旧時に取るべき対策のひとつとして、ログの取得について説明する。取得したログの見方と障害の原因追及方法、ログを利用したリカバリ方法なとについて解説する。

【学習の要点】

＊ ログを適切に出力することによって、DBMS に関する情報を効率よく収集することができる。

＊ ログの見方を把握しておくことで、速やかに障害の原因追求を行うことができる。

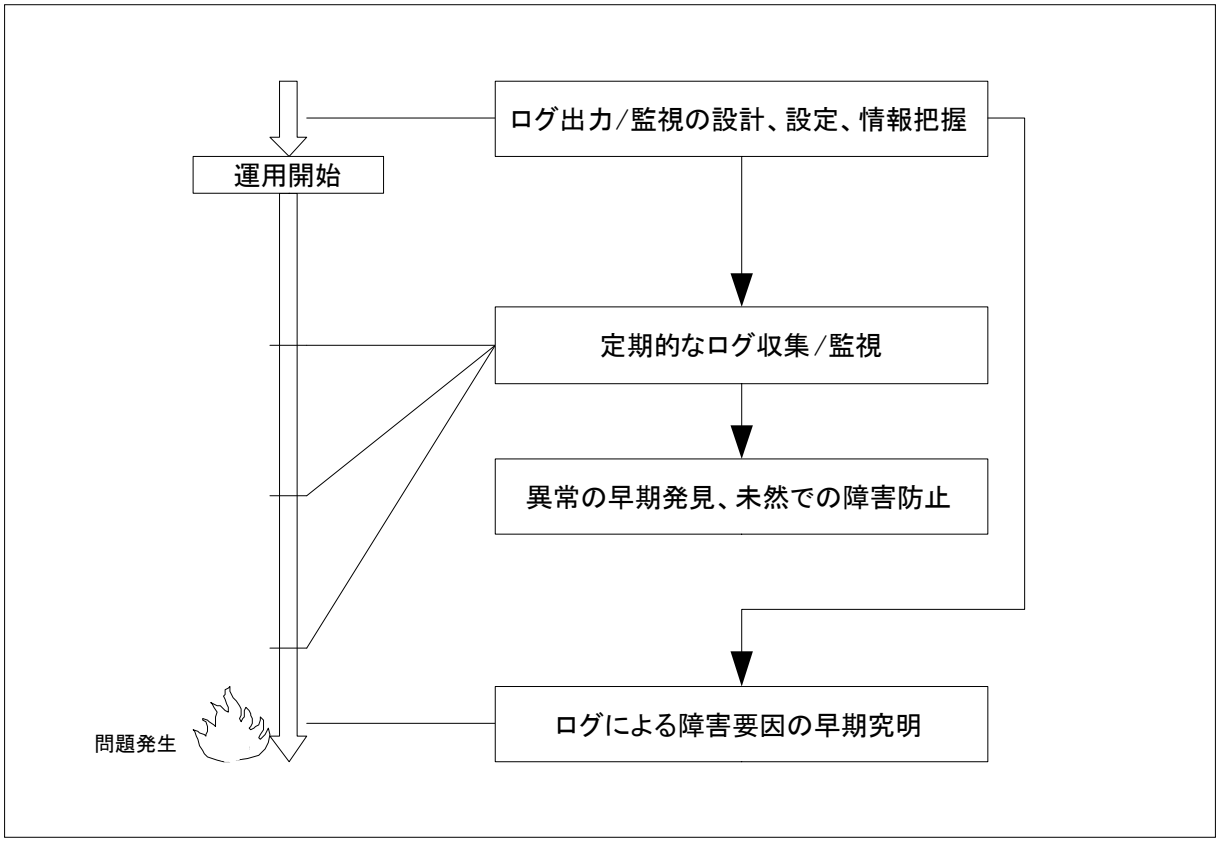

図 I-23-7.　ログの利用

【解説】

1) 取得したログの見方

ログファイルの種類は DBMS により様々であるが、いくつかの例をあげる。

＊ DBMS の起動/停止に関するログ(成功/失敗)

＊ 利用者によるデータベース接続や命令のログ(成功/失敗)

＊ コミットされた全トランザクションのログ
→ログに見られる傾向から、例えば以下のように、不正アクセスの確認や障害の予測ができる。

＊ 同一のユーザでデータベース接続の失敗が多数見られる。
→ 辞書攻撃などによる不正ログインが試みられている可能性が高い。

＊ アプリケーションでは使われないような SQL の発行が見られる。
→ アプリケーション以外からのアクセスや、SQL インジェクションの可能性がある。

＊ DBMS 起動時にメモリ不足の警告が出ている。
→ データ肥大化によりメモリを圧迫している可能性がある。

DBMS には、ログの出力レベルを変更したり、出力内容を限定したりできるものがある。重要なものを漏らさずログ出力し、不要なログ出力を抑制することで、効率的なログ確認ができる。

2) 障害の原因追及方法

万一の障害の際、ログを確認することで、原因が追求できる場合がある。

＊ DBMS が起動しない場合
DBMS の起動/停止に関するログを確認することで、メモリ不足などの原因が特定できる。

＊ データが改ざんされた場合
不正な SQL の発行やデータベース接続を特定することで、SQL インジェクション、部内者による不正アクセスなどの原因が特定できる。

3) ログを利用したリカバリ方法

DBMS には、コミットされた全トランザクションのログを保存し、それを用いてデータを復旧できるものがある。この場合、最後のバックアップ作業以降に更新されたデータについても復旧が可能となる。リカバリ方法は次のとおり。

＊ 最新のフルバックアップデータを適用する。

＊ (インクリメンタルバックアップを行っている場合) フルバックアップ以降のすべてのインクリメンタルバックアップのデータを順に適用する。

＊ コミットされた全トランザクションのログを用いて、最後のバックアップ以降のデータ更新を適用する。

ログファイルは、データベース用の記憶装置が故障した場合の復旧に備えて、データベースとは異なる記憶装置に出力しておくことが重要である。

スキル区分	OSS モデルカリキュラムの科目	レベル
RDB 分野	23　RDB システム管理に関する知識 I	基本
習得ポイント	I-23-8. データベースのユーザ管理とアクセス制御	
対応する コースウェア	第 4 回（データベースセキュリティ）	

I-23-8. データベースのユーザ管理とアクセス制御

データベースにアクセスできるユーザを管理する方法と、アクセス制御の概念について、ユーザ管理およびアクセス制御を実現するための、基本的な作業手順を示す。またこれらに関する作業上の留意点を説明する。

【学習の要点】

* RDBMS のユーザに対し、データベースの操作やデータベースの構成要素ごとに、アクセス権を設定することが出来る。
* RDBMS のユーザに与えるアクセス権を必要最小限とすることで、ユーザのミスや不正アクセスによるデータの損失/改ざんのリスクを減らすことが出来る。

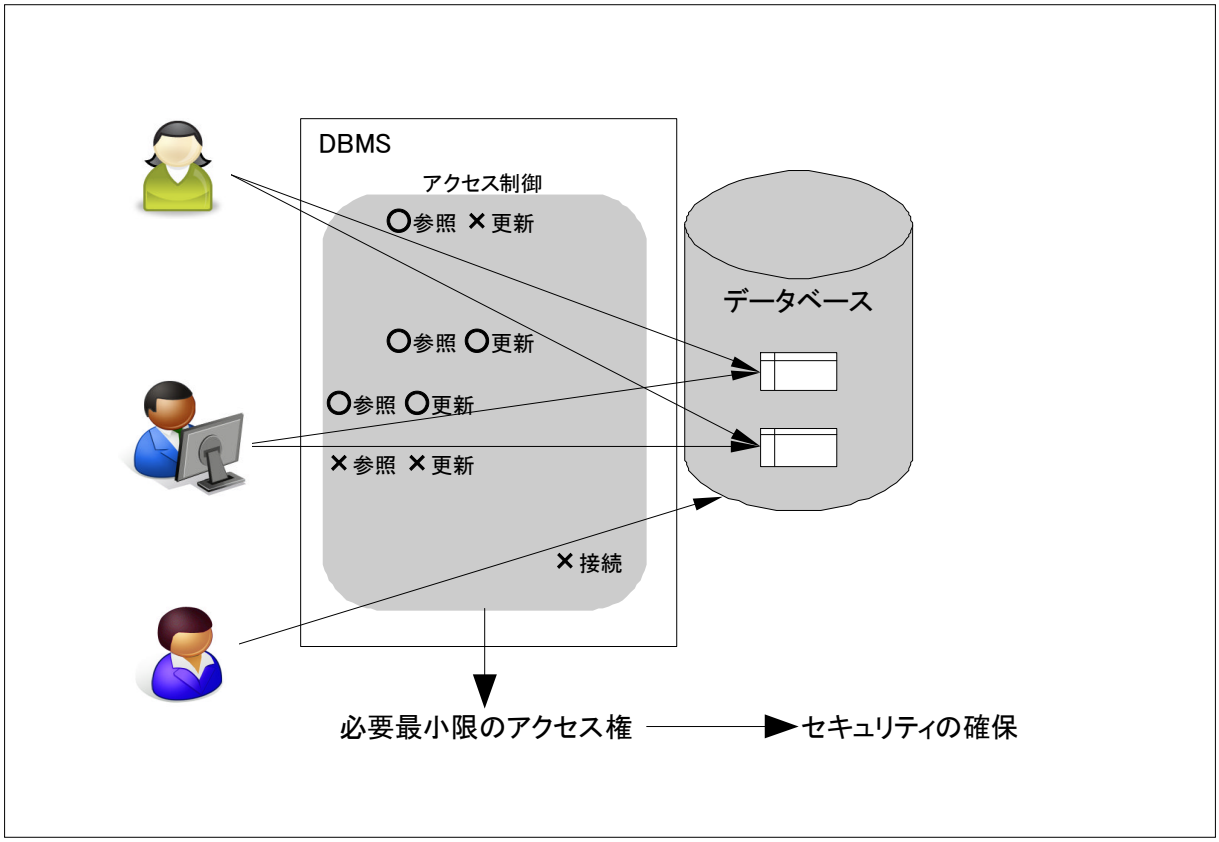

図 I-23-8.　データベースのユーザ管理とアクセス制御

【解説】

1) ユーザ管理とアクセス制御の目的

データベースを運用していると、利用者によって参照/更新可能なデータを限定したい場合がある。このような目的のため、多くの DBMS ではユーザ管理とアクセス制御の機能を有する。OS によるデータベースファイルへのアクセス制御では困難な細かなアクセス制御を実装することができる。

2) ユーザ管理と認証

データベース接続時の認証方式は DBMS に依存するが、もっとも一般的なものは、DBMS 独自のユーザとパスワードによって DBMS にログインさせる認証方式である。SQL には、

＊ 「CREATE USER」文（ユーザの作成）

＊ 「DROP USER」文（作成済みのユーザの削除）

といったユーザ管理用の命令がある。

3) アクセス制御

アクセス権には、「データベースへ接続する」「データを検索する」「データを新規登録する」「データを削除する」「データを更新する」「ユーザを作成する」など、さまざまなものがある。作成したユーザに対しアクセス権を設定しておくことで、ユーザがデータベースにアクセスする際の権限を制御できる。SQL には、

＊ 「GRANT」文（権限の付与）

＊ 「REVOKE」文（付与済みの権限の剥奪）

といったアクセス権設定用の命令がある。

権限付与の際は適用範囲を設定できる。適用範囲のレベルには、「DBMS」「データベース」「表」などがあり、例えば「データベース」のレベルで「表に行を挿入する」権限を付与すると、指定したデータベースのすべての表において、行を挿入することが可能となる。

4) 基本的な作業手順

ユーザ管理とアクセス制御を実現する基本的な手順は以下の通りである。

＊ DBMS の管理権限を持つ既存のユーザで DBMS にログインする。

＊ データベースを作成し、作成したデータベース上に表や索引などのスキーマを定義する。

＊ ユーザを作成し、パスワードを設定する。

＊ 作成したユーザに必要最小限の権限を付与する。

5) 作業上の留意点

＊ ユーザに権限を付与する場合は、セキュリティを考慮し、必要最小限の権限とする。必要以上に権限を付与すると、ユーザの操作ミスや不正アクセスによるデータの損失/改ざんのリスクが増大する。

＊ ユーザに権限を付与する時は、極力、対象ユーザをデータベースから切断しておく。対象ユーザがデータベースに接続した状態のまま権限を変更した場合、その変更がどの程度即時に反映されるかは DBMS に依存してしまう。

スキル区分	OSS モデルカリキュラムの科目	レベル
RDB 分野	23　RDB システム管理に関する知識 I	基本
習得ポイント	I-23-9. データベースセキュリティの内容と留意点	
対応する コースウェア	第 4 回（データベースセキュリティ）	

I-23-9. データベースセキュリティの内容と留意点

データベース運用時に配慮すべきセキュリティの概要を紹介し、実際の運用作業において実施しなければならないこと、注意すべきポイントについて解説する。また実際にセキュリティ侵害が発生した際の対処方法について説明する。

【学習の要点】

＊ データベースは個人情報や企業の極秘情報等が格納される場所であり、システム中で最もセキュリティを考慮しなければならない部分である。

＊ セキュリティ向上のための個々の対策について、メリット、デメリット(コストを含む)、注意点を理解することで、システム全体としての効率的な対策が可能になる。

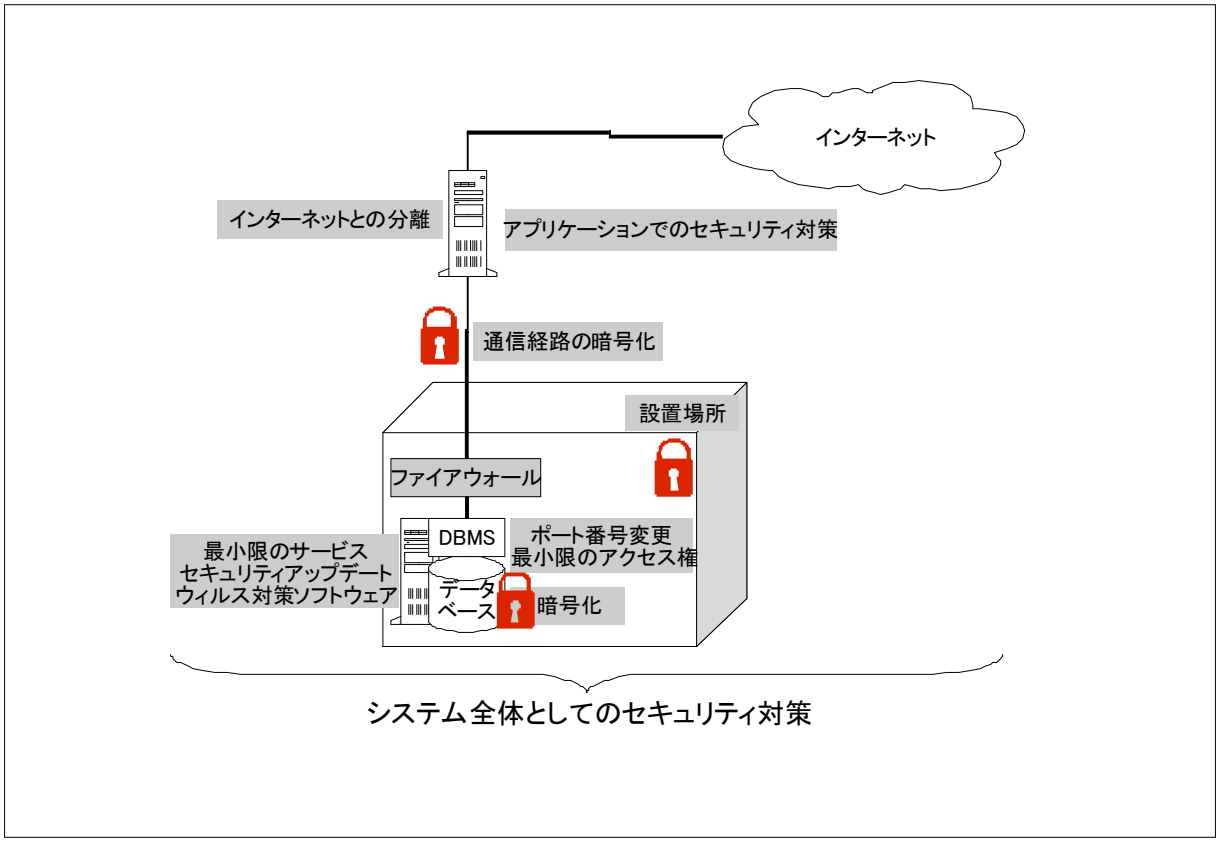

図 I-23-9.　さまざまなデータベースセキュリティ対策

【解説】

1) データベースセキュリティのために検討すべき項目と実施例

＊ データベースの物理的な設置場所（データセンターなど部外者の入室を防げる場所におく）

＊ データベースのネットワーク上の配置（LAN 内に設置しプライベートアドレスを設定）
(LAN であっても部外者がアクセスできる場合は別途対策が必要)

＊ DBMS サーバ起動時の設定（ポート番号をデフォルトの番号から変更）

＊ 不要なサービスや不要なユーザアカウントの排除

＊ DBMS のデフォルトユーザ（アカウントを無効化またはパスワードを変更）

＊ DBMS のユーザアカウント（必要最小限の権限を持つユーザで接続、IP アドレスによる制限）
(DBMS の認証に OS の認証を用いるか独自の認証を用いるかも検討)

＊ パスワードの制限の設定（簡易なパスワードの排除、誤入力時のロック）

＊ ビューの設計（ユーザ権限に応じてビューを作成し、必要最小限のアクセス権を付与）

＊ DBMS の制約の利用（適切なデータ型の設計、整合性制約の適用）

＊ ストレージの暗号化

＊ OS 等によるデータベースファイルの暗号化

＊ DBMS によるデータの暗号化

＊ アプリケーションによるデータの暗号化（DBMS でのソートや条件指定には使えなくなる）

＊ 通信経路の暗号化 － VPN の利用

＊ OS や DBMS へのセキュリティアップデートの適用

＊ セキュリティ対策ソフトウェアの利用

＊ アクセス経路へのファイアウォールの設置

＊ アクセスログの採取（目的を明確にして不要なログを大量に採取することを避ける）

＊ エラー情報/デバッグ情報の出力（利用者の画面に SQL や DBMS ユーザ情報を表示しない）

＊ データベースを利用するアプリケーションの脆弱性の排除（SQL インジェクション対策）

＊ データベースを利用するアプリケーションの設計（利用者に表名等が推測されないようにする）

＊ Web サーバやアプリケーションサーバの配置−データベースとは異なるホストに設置
(同一ホストでは OS の管理権限が奪われた場合にリスクが高いが、別ホストの場合は経路盗聴の対策が必要)

＊ Web サーバやアプリケーションサーバ自体のセキュリティ対策

2) セキュリティ侵害が発生した際の対処方法

万一データベースのセキュリティが侵害された場合は、以下の順で対処を行う。

＊ データベースをネットワークから切り離す。

＊ アクセスログを確認し、盗み出されたデータ、改ざんされたデータ、不正アクセスの方法/経路を特定する。

＊ 特定できたアクセスに対し、さらなるセキュリティ対策を講じる。

＊ 利用者に侵害があったこととその範囲を正しく伝える。(隠蔽しない)

スキル区分	OSS モデルカリキュラムの科目	レベル
RDB 分野	23　RDB システム管理に関する知識 I	基本
習得ポイント	I-23-10. データベース動作環境の管理計画と管理作業	
対応する コースウェア	第 5 回（データベースリカバリ設計）	

I-23-10. データベース動作環境の管理計画と管理作業

データベースを正常に動作させるために実施しなければならない作業について、バックアッププランの策定、リカバリ方法の決定、データベース動作環境の監視といった一連の作業手順についてまとめる。

【学習の要点】

＊ データベースのバックアップ、リカバリ、監視といった作業の手順を把握しておくことで、万一のデータベース障害時に、速やかに復旧することができる。

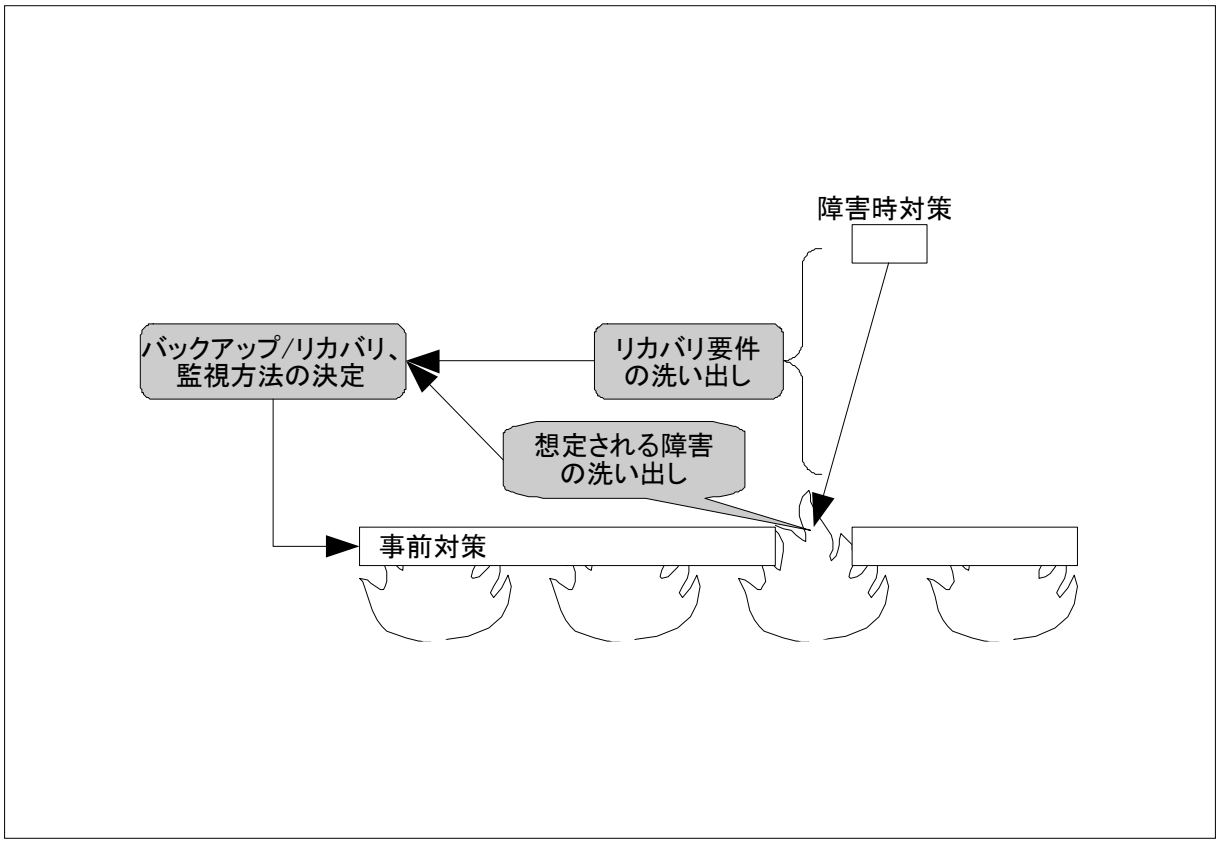

図 I-23-10.　障害復旧と対策の流れ

【解説】

1) 想定される障害の洗い出し

記憶装置の故障、マシントラブル(CPU やメモリの障害)、OS や DBMS の不具合、ユーザ操作ミス、ウィルス感染などの想定される障害を洗い出す。

2) リカバリ要件の洗い出し

個々の想定される障害に対し、データベースリカバリ前後の作業、作業時間帯、所要時間、どの時点の状態に復旧するかなどの要件を洗い出す。

3) バックアップ/リカバリ方法、監視方法の決定

要件を満たすよう、具体的なバックアップ/リカバリ方法、監視方法を決定する。以下の項目を決定する必要がある。

* バックアップ時間帯、バックアップ間隔
* バックアップ世代数
* バックアップ対象（フル、インクリメンタル、部分）
* バックアップ時の状況（オンライン、オフライン）
* バックアップ作業者（自動、手動）
* リカバリ時間帯
* リカバリ時の状況（オンライン、オフライン）
* リカバリ対象データ（どの世代か）
* トランザクションのログを利用したリカバリを行うか
* トランザクションのログを利用したリカバリを行う場合のリカバリ対象日時
* 監視項目
* 監視項目のしきい値
* 監視時間帯、監視間隔
* 監視警告通知設定

監視項目には以下のようなものがある。

* CPU 使用率、メモリ使用率、ネットワーク帯域使用率
* ディスク使用率、ディスク I/O 効率、データファイル使用率
* ログ出力内容
* 表データの断片化
* 表データの参照頻度、更新頻度
* 索引の更新頻度