データベースセキュリティガイドライン

第 1.0 版
2006 年 11 月 7 日

データベース･セキュリティ･コンソーシアム
セキュリティガイドラインWG

第1章 はじめに....2
1.1 目的....2
1.2 本ガイドラインの前提....2
1.3 本ガイドラインに関する注意事項....2
第2章 全体のセキュリティ対策における ＤＢセキュリティの位置付け....4
2.1 想定システムモデル....4
2.2 全体のセキュリティ対策の概要....5
2.3 ＤＢセキュリティの位置付け、対象範囲....6
2.4 ＤＢに関係する脅威の定義....7
2.4.1 脅威の定義....7
2.4.2 登場人物の定義....7
2.4.3 ＤＢに関係する情報資産の定義....8
2.4.4 手口の定義....8
2.4.5 不正アクションの定義....9
2.4.6 脅威の一覧....10
第3章 基本方針の策定....11
3.1 ＤＢセキュリティポリシーの策定....11
3.1.1 重要情報の定義....11
3.1.2 リスク分析....11
3.1.3 アカウント管理ポリシー....12
3.1.4 ログの取得ポリシー....12
3.2 人的対策....14
3.2.1 啓発/規約....14
第4章 ＤＢセキュリティ対策....16
4.1 防御系のセキュリティ対策....16
4.1.1 初期設定....16
4.1.2 認証....18
4.1.3 アクセスコントロール....20
4.1.4 暗号化....22
4.1.5 外部媒体の利用制御....23
4.1.6 その他....24
4.2 検知、追跡系のＤＢセキュリティ対策....26
4.2.1 ログの管理....26
4.2.2 不正アクセス検知....28
4.2.3 ログの分析....30

第1章　はじめに

1.1 目的

情報漏洩に起因した事件が社会において頻発する中、多くの重要な情報の主たる格納場所であるデータベース（以下ＤＢ）に対するセキュリティ対策が益々重要となりつつある。システムの根幹を構成するＤＢに関して、高度なセキュリティに関わるスタンダードな技術/手法の確立を図っていくことは、高度情報通信ネットワーク社会の中で、安心/安全な利用環境を維持したシステムを構築/運用していく上で急務であると考えられる。

「ＤＢ」、「セキュリティ」それぞれの分野を包括した「ＤＢセキュリティ対策」が求められる中、日本国内において「ＤＢセキュリティについての指針、考え方」をまとめたガイドラインはこれまで存在しなかった。

本ガイドラインは、「ＤＢセキュリティ対策の必要性その有効性（対策、範囲、効果など）」を記したものであり、各企業/団体の「ＤＢセキュリティ対策」の導入の為の参考となることを目的とするものである。

1.2 本ガイドラインの前提

本ガイドラインでは、ＤＢセキュリティを検討するにあたり、次のような想定の元に検討を進める。

本ガイドラインで検討するセキュリティ対策はＤＢでの対策に留め、他のセキュリティ対策（ネットワークなど）については言及しない。他のセキュリティ対策については、既存のガイドラインを参照することとする。

本ガイドラインでは、リスクアセスメントについては言及せず、ＤＢセキュリティの必要性の定義に留める。リスクアセスメントについては、別途検討が必要である。

本ガイドラインにおけるＤＢの定義は、現在もっとも多くのシステムで稼動しているＲＤＢとする。

ＤＢセキュリティ対策を行う上で、あらかじめ実施されていないとＤＢセキュリティ対策が有効でなくなる対策（ＡＰ認証など）は、ＤＢセキュリティ対策の前提対策と位置付け、今後検討を進める。

本ガイドラインの利用者は、ＤＢの管理者、設計者を想定する。

1.3 本ガイドラインに関する注意事項

本ガイドラインに関する注意事項を以下に記述する。

○著作権の所在

本ガイドラインの版権は、データベース・セキュリティ・コンソーシアム（ＤＢＳＣ）に属する。

○利用制限

本ガイドラインの販売は禁止する。それ以外の本ガイドを利用したサービス提供に関しては一切制限しない。

○引用元の明記

本ガイドラインの全文もしくは一部を引用する場合には、必ず引用元として「データベースセキュリティガイドライン」を明記する。営利目的、非営利目的の区別はない。

①ガイドラインの全部あるいは一部をそのまま、使用する場合：

【出典】「データベースセキュリティガイドライン(1.0 版)」
データベース・セキュリティ・コンソーシアム（ＤＢＳＣ）
http://www.db-security.org/

---

②ガイドラインを一部加工して、使用する場合：

【参考文献】「データベースセキュリティガイドライン(1.0 版)」
データベース・セキュリティ・コンソーシアム（ＤＢＳＣ）
http://www.db-security.org/

○免責事項

本ガイドラインを利用したことによって生じるいかなる損害に関しても、ＤＢＳＣは一切責任を負わないものとする。

○利用時窓口

本ガイドラインを報道、記事などメディアで用いる場合には、ＤＢＳＣ事務局（info@db-security.org）まで連絡する。

第2章　全体のセキュリティ対策における　ＤＢセキュリティの位置付け

2.1　想定システムモデル

本ガイドラインは、インターネットとイントラネットからアクセスされるWeb3階層モデルを想定システムモデルとする。

想定システムモデルでは、ネットワークがセグメント分割されており、ＤＢサーバはインターネット、イントラネットからは直接アクセスできないこととする。また、ＤＢサーバへは、運用/管理ゾーン（管理者用 LAN）からのみ直接アクセス可能とするファイアウォールが設置されていることとする。

以下に本ガイドラインの想定システムモデル図を示す。

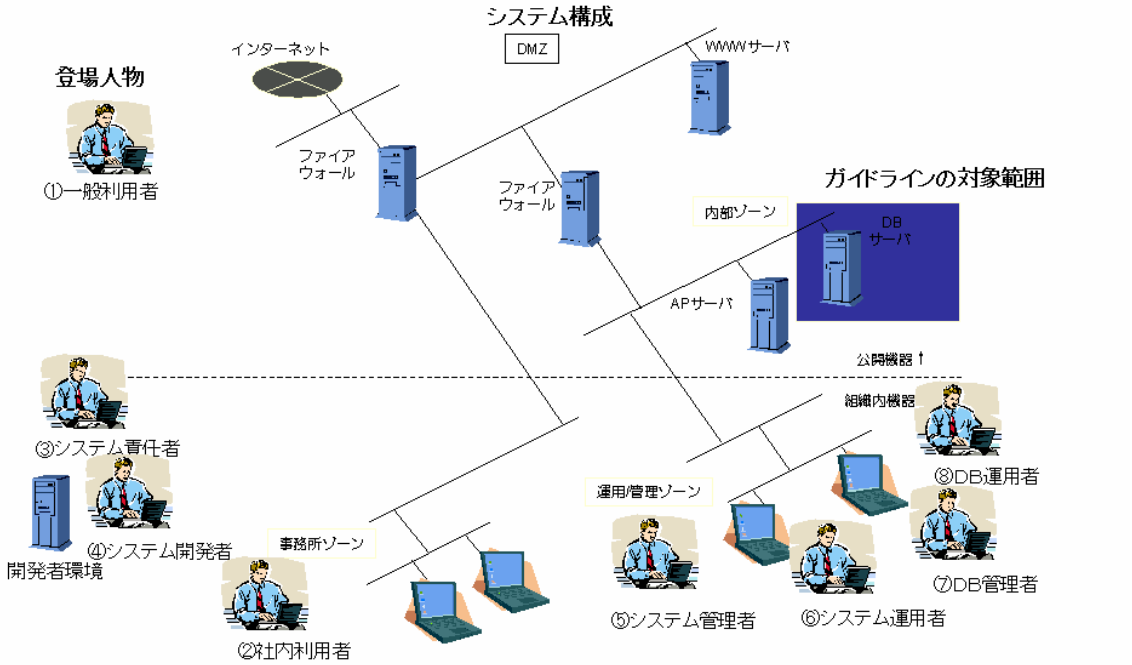

図1．想定システムモデル

※アプリケーションは以下ＡＰとする。

2.2 全体のセキュリティ対策の概要

想定システムモデルに対する全体のセキュリティ対策の概要を以下に示す。

全体のセキュリティ対策は大きく以下の種類を想定する。

1. ネットワーク対策
2. Web対策
3. ＡＰ対策
4. ＤＢ対策
5. 端末対策

本ガイドラインでは、「4．ＤＢ対策」に着目し、「第4章　ＤＢセキュリティ対策」で対策を記述する。

以下にセキュリティ対策全般の概要図を示す。

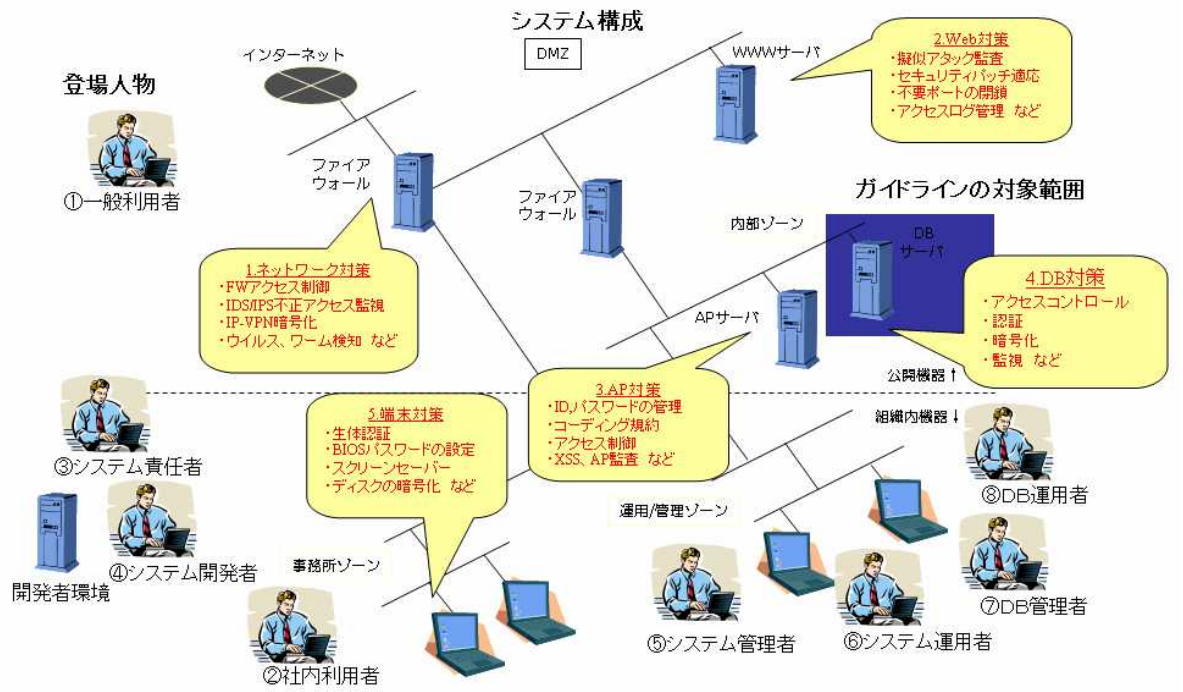

図2．セキュリティ対策全般の概要

2.3　ＤＢセキュリティの位置付け、対象範囲

本ガイドラインでのＤＢセキュリティの位置付けはＤＢに格納されている情報を守ることとし、対象範囲はＤＢサーバ、およびＤＢ周辺ネットワークとする。

以下にＤＢセキュリティの位置付け、対象範囲の概要図を示す。

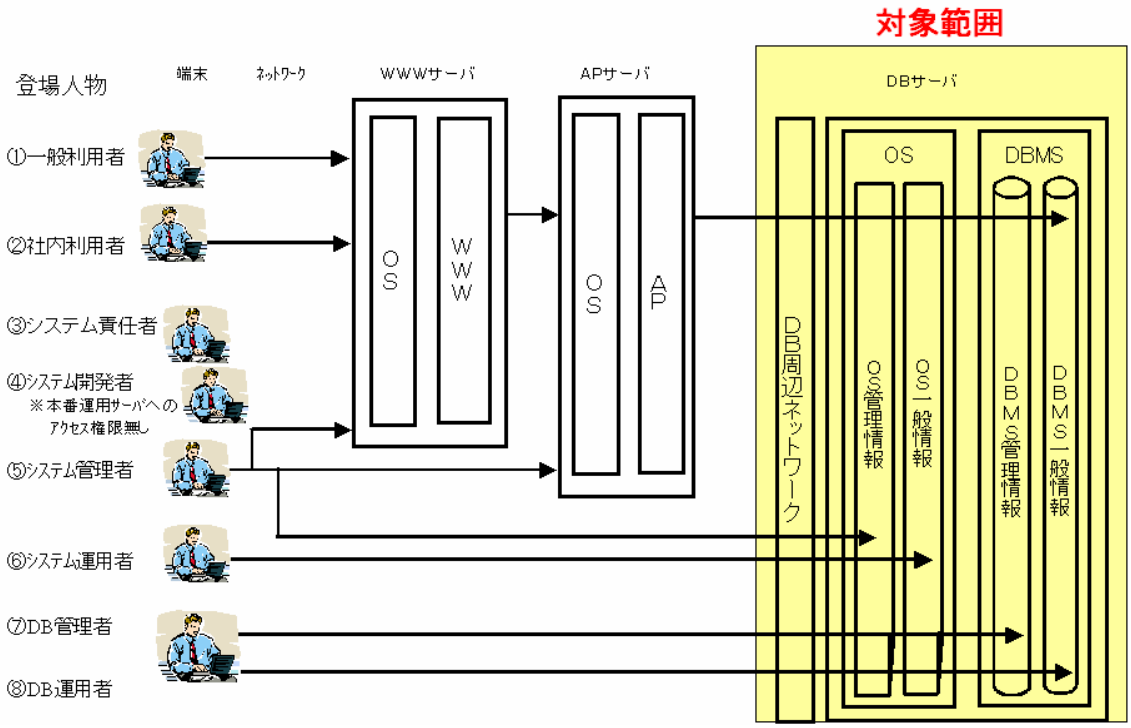

図3．ＤＢセキュリティの位置付け、対象範囲の概要

※矢印は正規のアクセスを示す。

2.4 ＤＢに関係する脅威の定義

2.4.1 脅威の定義

本ガイドラインでは、ＤＢセキュリティを考えるにあたり、まず脅威を洗い出し、その脅威を防ぐ為の対策を記述する。脅威とは守るべき情報資産に対する「機密性」、「完全性」、「可用性」を脅かすものと定義し、脅威の発生元である登場人物、守るべき情報資産、手口、不正アクションの組合せで考える。

（例：一般利用者がＤＢ管理情報を脆弱性の利用により不正入手する。）

以下に脅威の定義を示す。

- 情報資産に対する「機密性」、「完全性」、「可用性」を脅かすものを脅威とする。
- 物理的な破壊は対象外とする。ＤＢへのアクセスなど技術的な脅威を対象とする。

2.4.2 登場人物の定義

ＤＢに関わる人物と、その役割を決め、脅威の発生元である登場人物を定義する。

これらの登場人物を脅威の発生元と考え、想定される不正行為の洗い出しを行う。

以下に登場人物の定義を示す。

表1．登場人物の定義

登場人物	定義、役割
①一般利用者	社外のエンドユーザ
②社内利用者	社内のエンドユーザ
③システム責任者	④～⑧の管理、判断
④システム開発者	・WWW開発、AP開発 ・WWWサーバ、APサーバ構築（OS/ﾐﾄﾞﾙｳｪｱ含む） ・DB周辺ネットワーク構築 ・DBサーバ構築（OS/ﾐﾄﾞﾙｳｪｱ含む）
⑤システム管理者	・WWWサーバ、APサーバ運用（OS/ﾐﾄﾞﾙｳｪｱ含む） ・DBサーバ運用（OS/ﾐﾄﾞﾙｳｪｱ含む） ・DB周辺ネットワーク機器運用
⑥システム運用者	・WWW運用、AP運用 ・DB周辺ネットワーク運用
⑦DB管理者	・DBMS構築 ・DBMS運用
⑧DB運用者	・業務運用（テーブル、データ含む）

2.4.3 ＤＢに関係する情報資産の定義

本ガイドラインでは、守るべき資産をＤＢサーバ格納情報と定義する。ＤＢサーバ格納情報の詳細については、以下のように定義する。

1．ＤＢＭＳ管理情報

－ＤＢ構成情報（ディクショナリ、ユーザID/パスワードなど）

－ＤＢログ（アクセスログなど）

2．ＤＢＭＳ一般情報

－業務データ

－業務アプリ（ストアードプロシージャなど）

3．ＯＳ管理情報

－ＯＳ構成情報

－ＯＳログ（トレースログ、アラートログなど）

4．ＯＳ一般情報

－ＤＢ関連ファイル

（定義ファイル、物理ファイル、ログ、バックアップなど）

2.4.4 手口の定義

手口とは、登場人物が情報資産に対して行う不正行為の手段のことである。手口がわかると、それに有効な対策を明確にすることができる。

以下に、想定される手口を示す。

- パケットの盗聴
- パスワードへの辞書攻撃
- ソーシャルエンジニアリングによるID/パスワードの不正入手
- 設定ミスを悪用したＤＢＭＳ情報の不正入手
- ＤＢＭＳの脆弱性を悪用したＤＢＭＳ情報の不正入手
- ＤＢ関連ファイルの改ざんによるＤＢＭＳ情報の不正入手
- 管理情報からID/パスワードの不正利用
- バックドアの作成
- 不正なＤＢＭＳ管理者/ＤＢＭＳ運用者アカウントの作成によるＤＢＭＳ情報の不正入手
- 不正ルートで入手後、情報の悪用（持ち出し）
- 管理情報の改ざんによるＤＢＭＳ情報の不正入手
- 業務妨害を狙ったＳＱＬ発行
- 通常ルートで入手後、情報の悪用（持ち出し）

2.4.5 不正アクションの定義

不正アクションとは、登場人物が情報資産に対して行う不正行為のことである。
「2.4.4 手口の定義」で示した手口は、この不正行為を行う為の手段である。
以下に想定される不正アクションを示す。

- 入手できる情報の悪用（持ち出し）
- 入手できる情報の改ざん、破壊
- 業務妨害（リソース枯渇）
- ＤＢＭＳ情報の不正改ざん、破壊（更新）
- ＤＢＭＳ情報の不正入手（参照）

2.4.6 脅威の一覧

登場人物、情報資産、手口、不正アクションの1セットで脅威とする。

以下に脅威の一覧を示す。

表2．脅威一覧

A:誰が？ （登場人物）	B:何を？ （情報資産）	C:どうやって？ （手口）	D:どうする？ （不正アクション）	不正アクス or 正規アクセス
①ー般利用者 ②社内利用者 ③システム責任者 ④システム開発者 ⑤システム管理者 ⑥システム運用者	DBMS 管理情報	パケットの盗聴	・DBMS情報の不正入手（参照） ・DBMS情報の不正改ざん、破壊（更新）	不正
		パスワードの辞書攻撃		
		ソーシャルエンジニアリングによるID/パスワードの不正入手		
		設定を悪用したDBMS情報の不正入手		
		DBMSの脆弱性を悪用したDBMS情報の不正入手		
		不正ルートで入手後、情報の悪用（持ち出し）		
①ー般利用者	DBMS ー般情報	通常ルートで入手後、情報の悪用（持ち出し）	・入手できる情報の 悪用（持ち出し）	正規
		業務妨害を狙ったSQL発行	・業務妨害（リソース枯渇）	
②社内利用者	DBMS ー般情報	通常ルートで入手後、情報の悪用（持ち出し）	・入手できる情報の 悪用（持ち出し）	正規
		業務妨害を狙ったSQL発行	・業務妨害（リソース枯渇）	
①ー般利用者 ②社内利用者	DBMS ー般情報	パケットの盗聴	・DBMS情報の不正改ざん、破壊（更新）	不正
		パスワードの辞書攻撃		
		ソーシャルエンジニアリングによるID/パスワードの不正入手		
		設定ミスを悪用したDBMS情報の不正入手		
		DBMSの脆弱性を悪用したDBMS情報の不正入手		
		不正ルートで入手後、情報の悪用（持ち出し）		
③システム責任者 ④システム開発者 ⑤システム管理者 ⑥システム運用者	DBMS ー般情報	パケットの盗聴	・DBMS情報の不正入手（参照） ・DBMS情報の不正改ざん、破壊（更新）	不正
		パスワードの辞書攻撃		
		ソーシャルエンジニアリングによるID/パスワードの不正入手		
		設定ミスを悪用したDBMS情報の不正入手		
		DBMSの脆弱性を悪用したDBMS情報の不正入手		
		不正ルートで入手後、情報の悪用（持ち出し）		
④システム開発者	DBMS 管理情報	バックドアの作成	・DBMS情報の不正入手（参照） ・DBMS情報の不正改ざん、破壊（更新）	不正
	DBMS ー般情報	バックドアの作成	・DBMS情報の 不正入手（参照） ・DBMS情報の不正改ざん、破壊（更新）	
③システム責任者 ⑤システム管理者	DBMS 管理情報	不正なDBMS管理者アカウントの作成によるDBMS情報の不正入手	・DBMS情報の不正入手（参照） ・DBMS情報の不正改ざん、破壊（更新）	不正
	DBMS ー般情報	不正なDBMS運用者アカウントの作成によるDBMS情報の不正入手	・DBMS情報の不正入手（参照） ・DBMS情報の不正改ざん、破壊（更新）	
③システム責任者 ⑥システム運用者	DBMS 管理情報	DB関連ファイルの改ざんによるDBMS情報の不正入手	・DBMS情報の不正入手（参照） ・DBMS情報の不正改ざん、破壊（更新）	不正
	DBMS ー般情報	DB関連ファイルの改ざんによるDBMS情報の不正入手	・DBMS情報の不正入手（参照） ・DBMS情報の不正改ざん、破壊（更新）	
⑦DB管理者	DBMS 管理情報	通常ルートで入手後、情報の悪用（持ち出し）	・入手できる情報の悪用（持ち出し）	正規
		管理情報からID/パスワードの不正利用	・入手できる情報の改ざん、破壊	
		管理情報の改ざんによるDBMS情報の不正入手		
		業務妨害を狙ったSQL発行	・業務妨害（リソース枯渇）	
	DBMS ー般情報	パケットの盗聴	・DBMS情報の不正入手（参照） ・DBMS情報の不正改ざん、破壊（更新）	不正
		不正ルートで入手後、情報の悪用（持ち出し）		
⑧DB運用者	DBMS 管理情報	パケットの盗聴	・DBMS情報の不正入手（参照） ・DBMS情報の不正改ざん、破壊（更新）	不正
		パスワードの辞書攻撃		
		ソーシャルエンジニアリングによるID/パスワードの不正入手		
		設定ミスを悪用したDBMS情報の不正入手		
		DBMSの脆弱性を悪用したDBMS情報の不正入手		
		不正ルートで入手後、情報の悪用（持ち出し）		
	DBMS ー般情報	通常ルートで入手後、情報の悪用（持ち出し）	・入手できる情報の悪用（持ち出し）	正規
		業務妨害を狙ったSQL発行	・業務妨害（リソース枯渇）	

※図3「ＤＢセキュリティの位置付け、対象範囲の概要」の矢印を正規アクセスとし、それ以外を不正アクセスとする。

第3章　基本方針の策定

情報セキュリティでは、「誰が」「何を」「どのように」利用するかということが基本となる。これらが整理されていない状況では、正常なアクセス、不正なアクセスの区別がつかず、有効な対策を行うことができない。

ここでは、ＤＢセキュリティ対策を有効に機能させる為の前提条件となる考え方を整理し、基本方針とする。基本方針は、「第4章　ＤＢセキュリティ対策」を検討する上での方針となる。

3.1　ＤＢセキュリティポリシーの策定

ＤＢセキュリティ対策を実施するにあたり、利用される情報資産とＤＢを利用する利用者を役割ごとに整理する必要がある。利用者や情報資産を整理することでどのような対策が必要になるかが明確になる。また、対策を有効に機能させる為にあらかじめ検討しなければならないことも存在する。

ここでは、アクセスコントロールや監査などのセキュリティ対策を有効にする為の前提条件となるポリシーについて記述する。

3.1.1　重要情報の定義

セキュリティ対策を有効に実施する為、以下の対策を実施すること。

- 守るべき情報を洗い出す。（必須）

  例：

  - ＤＢＭＳ管理情報、ＤＢＭＳ一般情報

- 保持している情報を重要度などにより分類する。（必須）

  例：

  - 個人情報、機密情報

3.1.2　リスク分析

セキュリティ対策を有効に実施する為、以下の対策を実施すること。

- 脅威を洗い出して、リスク分析を行う。（必須）
- 情報資産の重要度、リスク分析の結果に基づいて、必要なＤＢセキュリティ対策を講じる。（必須）

3.1.3 アカウント管理ポリシー

(1)利用者の整理

セキュリティ対策を有効に実施する為、以下の対策を実施すること。

- 利用者を役割ごとに分類する。(必須)
- 分類した役割ごとの要員を整理する。(必須)

(2)アカウントの整理

セキュリティ対策を有効に実施する為、以下の対策を実施すること。

- 役割ごと、利用者ごとに、適切な権限を持ったアカウントを整理する。(必須)

(3)アカウント管理ポリシーの見直し

セキュリティ対策を有効に実施する為、以下の対策を実施すること。

- 整理したアカウント、権限を定期的にチェックし、状況に適しているかを判断する。(必須)
- システム変更、運用変更時には、アカウント、権限の見直しを行う。(必須)
- 不適切なアカウント、権限を発見した場合は、再度整理を行う。(必須)

3.1.4 ログの取得ポリシー

(1)ログ取得の目的の整理

ログ取得を有効にする為、以下の対策を実施すること。

- 取得するログの目的を整理する。(必須)

  例:

  - 不正アクセス時の調査、捜査機関への証拠提出

(2)取得ログの整理

適切なログを取得する為、以下の対策を実施すること。

- 対象システムにおいて取得できるログの種類を整理する。(必須)

  例:

  - ＯＳログ、ソフトウェアログ
  - ＡＰログ
  - ＤＢ監査ログ

(3)ログ取得対象アクセスの整理

適切なログを取得する為、以下の対策を実施すること。

- 重要情報に関するアクセスの種類を整理する。(必須)

  例:

  - 重要情報 (個人情報/機密情報など) へのアクセス
  - 重要情報 (ＤＢ管理情報) へのアクセス
  - 業務時間外のアクセス
  - ログイン
  - その他特定のＳＱＬ など

- 不正が疑われるアクセスを整理する。(必須)

  例:

  - 大量検索アクセス
  - 異なる場所からのアクセス
  - 業務時間外のアクセス

- ＤＢに関する全てのアクセスをログ取得する。(推奨)

(4)ログ取得内容の整理

取得したログを有効に利用する為、以下の対策を実施すること。

- ログに出力する内容を整理する。(必須)

  例:

  - 時間 (いつ)
  - ＤＢアカウント、アプリユーザ (誰が)
  - オブジェクトID、テーブル名 (何を)
  - マシン名、IPアドレス (どこから)
  - ＳＱＬ種別、ＳＱＬ全文 (どうやって)
  - 成功、失敗 (結果)

(5)ログの保全

ログの正当性を確保し利用する為、以下の対策を実施すること。

- ログの保全指針を整理する。(必須)

  例:

  - 保管場所
  - 保管媒体
  - 保管期間
  - アクセス制御

3.2 人的対策

情報セキュリティ対策において、システムに対する技術的対策だけを実施しても、脅威に対して有効な対策を実施したとは言えない。技術的対策を利用、管理、運営するのは人である。よって、システムの機能を十分に活かした効果的な対策を行うには、人的対策を実施することが必要不可欠となってくる。特に、ＤＢは内部利用者が多くかつ強力な権限も与えられている為、人的対策が重要である。

ここでは、規約の策定や教育などの人的対策を記述する。

3.2.1 啓発/規約

(1)規約の策定

対象とするシステムのセキュリティレベルを設定し、セキュリティ対策の基準とする為、以下の対策を実施すること。

- 規約を策定する。(必須)

  例:

  - 個人による誓約書の提出義務の規定
  - 無許可でのＤＢからの情報入手の禁止
  - 入手した情報の許可された記憶媒体以外への保存禁止
  - ID/パスワードの付箋禁止
  - ＤＢ管理者とシステム運用者の兼任禁止
- 不正利用による罰則を規定する。(必須)

  例:

  - 就業規則での罰則の規定
  - 罰則金の設定

(2)教育の実施

漏れやミスによる不正アクセスを防ぎ、情報セキュリティの重要性/必要性を認識させる為、以下の対策を実施すること。

- 全従業員/パートナーへの教育を完全実施する。(必須)

  例:

  - セキュリティポリシー策定の広報
  - 教育スケジュールの策定
  - 教育資料の策定
- 教育成果のフォローアップを実施する。(推奨)

  例:

  - 教育成果の定期的な確認

(3)ＤＢ管理業務のチェック

システム管理者/ＤＢ管理者によるミスや不正行為を防止する為、以下の対策を実施すること。

- ＤＢに関するセキュリティの事故や脆弱性の最新情報を常に収集する。（必須）
- 管理者権限で作業を行う場合、必ず複数名で作業を実施する。（推奨）
- 複数のシステム管理者間でパスワードを分割して保持する。（推奨）

  例：

  - パスワードの割符化
- 管理者のローテーションを実施する。（推奨）
- 管理業務は事前申請を行った上で実施する。（推奨）
- 管理業務の記録を残す。（推奨）

第4章　ＤＢセキュリティ対策

「第3章　基本方針の策定」に基づいたＤＢセキュリティ対策の詳細を以降に記述する。

ＤＢセキュリティ対策は、「不正行為を防御する為の対策」、「不正行為を検知する為の対策」、「不正行為を追跡する為の対策」に分類される。

また、ＤＢセキュリティ対策を実装する際には、システムの性能面やコストなどの様々な要素を考慮し対策を選択する必要がある。実装を検討する際の参考になるよう、それぞれの対策には必須対策、推奨対策を明記する。

4.1　防御系のセキュリティ対策

昨今、システムの高度/複雑化により、ＤＢへのセキュリティリスクは増加の一途を辿っており、事前の対策を講じることは必要不可欠である。

ここでは、不正行為を未然に、かつ効率的に防ぎつつ、正当行為への影響を最小限に抑える為のセキュリティ対策方法を記述する。

4.1.1　初期設定

古いバージョンのＤＢＭＳをインストールした状態や、不要な機能を実装した状態では、製品の脆弱性が多数存在する可能性がある。 また、通信機能においてデフォルトポートの利用やパスワード保護無しの利用のままでは、不正アクセスの危険性が増大する。

ここでは、ＤＢの脆弱性、および不正アクセスの可能性が最小限となるように、ＤＢＭＳの初期構築の段階で必要な対策を記述する。

4.1.1.1　インストール

(1)最新バージョンの導入

最新のセキュリティ対策を反映する為、以下の対策を実施すること。

- ＤＢＭＳのバージョンを調査し、最新のものを導入する。（推奨）
- 常に最新のパッチを入手し、適用する。（推奨）

(2)必要最低限の機能の導入

不正利用や資源の無駄を防ぐ為、以下の対策を実施すること。

- インストール時に必要な機能を選択し、対象機能のみを導入する。（必須）
- インストール時にデフォルトで導入される機能の中で、使用しない機能は削除または無効化する。（必須）

(3)ポートの変更

不正利用を防ぐ為、以下の対策を実施すること。

- インストール時に作成されるポートや、一般的なポート番号を変更する。(必須)

(4)通信機能のパスワード保護

通信機能を使用した不正利用を防ぐ為、以下の対策を実施すること。

- ＤＢＭＳの通信機能には、パスワードを設定する。(必須)

  例:

  - Oracleリスナーには、パスワードを設定

4.1.2 認証

現在のＤＢ認証システムの多くは、ログイン時のパスワード認証が用いられている。従って、悪意を持った利用者のなりすましによる情報漏洩や改ざん事故を防ぐ為、利用者を特定するアカウントとパスワードを厳重に管理する必要がある。さらにＤＢ管理者アカウントはＤＢＭＳ全ての操作が可能である為、一般アカウント以上の厳重な管理が必要である。

ここではアカウント管理においてセキュリティレベルを高く保つ対策を記述する。

4.1.2.1 アカウントの管理

(1)必要なアカウントの作成

なりすましなどのアカウントの不正利用を防ぐ為、以下の対策を実施すること。

- 必要なアカウントを洗い出し、作成する。（必須）
- 利用者の権限を規定する。（必須）
- 管理者アカウントと一般アカウントは、それぞれの権限に応じて別々に作成する。（必須）

(2)不要なアカウントの削除

なりすましなどのアカウントの不正利用を防ぐ為、以下の対策を実施すること。

- 未使用となったアカウントは削除する。(必須)

  例：

  — 異動、退職に伴うアカウント削除

- ＤＢＭＳインストール時にデフォルトで作成される業務に必要がないアカウントは削除する。(必須)

(3)長期間未使用アカウントのロック

なりすましなどのアカウントの不正利用を防ぐ為、以下の対策を実施すること。

- 長期間使用しないアカウントがある場合は、アカウントをロックする。（必須）

  例：

  — 一年に一回だけ使用するアカウントをロック

- 定期的にアカウントの使用頻度をチェックする。(推奨)

(4)ログイン失敗回数によるアカウントロック

なりすましなどのアカウントの不正利用を防ぐ為、以下の対策を実施すること。

- アカウントにログイン失敗回数の許容限度を設定する。（推奨）

(5)ＤＢ管理者アカウントの管理

ＤＢ管理者によるオペレーションミスや不正利用の発生を少なくする為、以下の対策を実施すること。

- ＤＢ管理者アカウントは特定の者しか、利用できないようにする。（必須）
- ＤＢ管理者権限を必要としない作業は、別アカウント（ＤＢ管理者権限無し）で実施する。（必須）
- ＤＢ管理者アカウントは、担当者別に割当てる。（必須）
- ＤＢ管理者アカウントを使用する端末は特定する。(推奨)

(6)開発機と本番機のID/パスワード

開発環境で利用したアカウントの不正利用を防ぐ為、以下の対策を実施すること。

- 開発機と本番機でIDを同一とせざるを得ない場合には、少なくともパスワードは変更する。（必須）
- 開発機と本番機のアカウントは全く別なものとする。(推奨)

(7)一時利用アカウントの設定

一時的な利用者の不正利用を防ぐ為、以下の対策を実施すること。

- 一時的な利用者にはその都度、共有アカウントに対し一時的なパスワードを与える。または一時的なアカウントを作成する。(必須)

4.1.2.2 パスワードの管理

(1)パスワードの複雑化

アカウントのパスワードは、容易に推察されないようにする為、以下の対策を実施すること。

- 他者に容易に推察されるパスワードの使用を禁止する。（必須）

  例：
  - IDと同じパスワード
  - [1234]など判り易いパスワード
  - インストール時のデフォルトパスワード

(2)パスワードの定期的な変更

万が一パスワードを不正入手されても、不正利用を困難にする為、以下の対策を実施すること。

- ＤＢ管理者アカウントのパスワードを定期的に変更する。（必須）
- 利用開始時に設定されているパスワードは変更する。（必須）
- 一般アカウントのパスワードを定期的に変更する。（推奨）

(3)パスワードの有効期限の設定

定期的なパスワードの変更実施を促進する為、以下の対策を実施すること。

- ＤＢ管理者アカウントにパスワード有効期限を設定する。（必須）
- 一般アカウントにパスワード有効期限を設定する。(推奨)

4.1.3 アクセスコントロール

適切なアクセス権限の設定がなされていない場合、いくらＤＢサーバが社外からセキュアな状態に保たれていたとしても、万が一社内の悪意のある者にそのアカウントとパスワードを知られてしまった場合は、情報漏洩などの事故被害が広範囲に渡ってしまう恐れがある。対策が強制力を発揮するには、しっかりとしたルールに基づいたアクセスコントロールが必須である。

ここでは、適切なアクセス権限を利用者に設定する為のセキュリティ対策を記述する。

4.1.3.1 アクセス権限の設定

(1)ＤＢへのアクセス要件の洗い出し

適切なアクセス制限を実現する為、以下の対策を実施すること。

- アカウントの利用目的を分類する。(必須)

  例:

  - ＤＢ管理用、オブジェクト管理用、データアクセス用　など
- アカウントの利用目的ごとに必要な権限を分類する。(必須)

  例:

  - 機能別、経路別、オブジェクト別　など
- それぞれの権限に基づいてアカウントを分割する。(必須)
- 分割されたアカウントそれぞれについて、アクセスする必要がある必要最小範囲のデータと必要最低限のアクセス内容(参照、更新、作成、削除)を洗い出し、ＤＢへのアクセス要件を決定する。(必須)

(2)アクセス権限の設定

不必要なデータアクセスを制限する為、洗い出されたＤＢへのアクセス要件に基づいて、以下の対策を実施すること。

- 分割された各アカウントについて、ＤＢへのアクセス要件に基づき、必要最低限のアクセス権限を付与する。(必須)
- 管理者権限は、アカウントを限定して設定する。(必須)

(3)ＤＢへのアクセス要件検討、アクセス権限の設定における留意点

特に以下の点に留意し、アクセス要件を決定すること。

- データアクセスにおいて、全ユーザに権限を付与できる特殊なアカウントの作成は禁止する。(必須)
- 一般情報へのアクセス権限を付与できる一般アカウントの作成は禁止する。(必須)
- オブジェクトの作成、削除、メンテナンスなどを除いて、オブジェクトの所有者であるアカウントでの接続は禁止し、通常はロックする。(推奨)

(4)アクセス権限の見直し

システムに対する要求の変化とともに変化するアクセス権限を、適切な設定に維持する為、以下の対策を実施すること。

- 定期的にアクセス権限を調査し、不要なアクセス権限がないかどうか確認する。(必須)
- システム変更、運用変更時にアクセス権限を調査し、不要なアクセス権限がないかどうか確認する。(必須)
- 不要なアクセス権限が設定してある場合、速やかにアクセス権限を修正する。(必須)

4.1.4 暗号化

情報漏洩事件は組織外部からの盗難や盗聴よりも、内部関係者による意図的な機密情報の窃盗や盗聴、重要情報を記録した PC の外部持ち出しなど、組織内部が起因となる傾向にあり、データが漏洩した場合でも重要情報を守る必要がある。

ここでは、上記のような組織の外部、内部からのデータの盗難や通信の盗聴に対して、DB に格納されたデータを防御する、暗号化によるセキュリティ対策を記述する。

4.1.4.1 通信の暗号化

ＤＢサーバとクライアント間のパケット盗聴対策の為、以下の対策を実施すること。

- 通信暗号化機能/ツールを利用する。（推奨）

4.1.4.2 データの暗号化

(1)ＤＢＭＳ格納データの暗号化対策

ＤＢＭＳ格納データの盗難行為を無害化/防御/抑止する為、以下の対策を実施すること。

- データ暗号化機能/ツールを利用し、格納データを暗号化する。（推奨）

(2)物理ファイルの暗号化対策

物理ファイルの暗号化によって、盗難行為を無害化/防御/抑止する為、以下の対策を実施すること。

- データ暗号化機能/ツールを利用し、物理ファイルを暗号化する。（推奨）

(3)バックアップデータの暗号化対策

バックアップデータの盗難行為を無害化/防御/抑止する為、以下の対策を実施すること。

- 暗号化機能/ツールを利用し、バックアップデータを暗号化する。（推奨）

4.1.4.3 プロシージャの暗号化

プロシージャの暗号化によって盗難行為を無害化/防御/抑止する為、以下の対策を実施すること。

- プロシージャ暗号化機能/ツールを利用し、プロシージャを暗号化する。（推奨）

4.1.5 外部媒体の利用制御

ＤＢサーバに対するＦＤやＣＤ-Ｒ/ＲＷ、ＤＶＤ-Ｒ/ＲＷ/ＲＯＭ、ＵＳＢメモリなどの外部記憶媒体を接続制限することは情報漏洩事故を未然に防ぐ最後の砦である。また、外部記憶媒体のみならずプリンタの利用制限も考慮する必要がある。

ここではデータ持ち出しを制御する為に、ＤＢサーバに接続される外部媒体や端末の利用に関する対策を記述する。

4.1.5.1 ＤＢサーバ接続外部媒体の利用制御

(1)外部媒体の接続制限

情報を入手して書き出し先である外部媒体が接続されないようにする為、以下の対策を実施すること。

- 業務上必要のない外部記憶媒体は取り外す。(必須)
- 業務上必要のないプリンタは取り外す。(必須)

(2)外部媒体の利用制限

情報を入手しても、外部媒体へ書き出して情報を持ち出されないようにする為、以下の対策を実施すること。

- 外部記憶媒体へアクセス制御を実施する。(必須)
- 外部記憶媒体の接続制御を実施する。(推奨)
- プリンタへの接続制御を実施する。(推奨)

(3)外部媒体の接続ログ取得

外部媒体の利用ログを収集することで、情報漏洩事故に対する抑止効果と事故発生時の証拠とする為、以下の対策を実施すること。

- 外部媒体が接続された際のログを取得する。(推奨)
- 外部媒体へのアクセス状況のログを取得する。(推奨)
- ユーザからのアクセスを監視するログを取得する。(推奨)

4.1.5.2 ＤＢサーバ接続端末の利用制御

端末から情報が持ち出されるのを防御する為、以下の対策を実施すること。

- 外部記憶媒体の接続制限を実施する。(必須)
- 端末に対しては、堅牢化の為のセキュリティ対策を実施する。(必須)
- 端末アクセスの個人認証を実施する。(必須)
- インストールソフトウェアの管理、およびソフトウェア利用状況の監視をする。(必須)
- プリンタへの接続制限を実施する。(必須)

4.1.6 その他

ここまで防御系のセキュリティ対策として、ＤＢＭＳの設定などによる対策を示してきたが、サーバそのものへのアクセス、またサーバリソースの使用制限を設定することなどにより、さらに情報の保護を高めることができる。

ここでは、ＤＢサーバへの不正アクセスの可能性の低減、および大量データの抽出に規制をかける為に必要な対策を記述する。

4.1.6.1 アクセス可能な端末/IPアドレスの固定

ＤＢへのアクセスを制限する為、以下の対策を実施すること。

- ＤＢサーバはファイアウォールより内側に設置し、不特定多数の端末から直接ＤＢサーバにアクセスできないようにする。(必須)
- ローカルネットワークにおいては、直接ＤＢサーバにアクセスできる端末あるいはセグメントを限定する。(推奨)

例:

- ルータによるIPアドレスの制限
- ＤＢＭＳのネットワーク機能による制限

4.1.6.2 ユーザごとのリソース制限

サービス妨害、および大量データの抽出を制限する為、以下の対策を実施すること。

- 通常業務において、一般ユーザの想定を超えるCPUリソースの使用を制限する。(推奨)

4.1.6.3 セキュリティ対策状況の診断

(1)稼動前の診断

ＤＢセキュリティポリシーに従って対策が実装されているかを確認する為、以下の対策を実施すること。

- システム稼動前のセキュリティ診断を実施する。(必須)

(2)定期的な診断

セキュリティ対策の有効性を維持する為、以下の対策を実施すること。

- 最新の脅威をふまえてセキュリティ診断を定期的に実施する。(必須)

4.1.6.4 バックドアへの対処

(1)サーバの堅牢化

ＤＢを動作させるサーバへの侵入や破壊などを防ぐ為、以下の対策を実施すること。

- セキュアなサーバにてＤＢＭＳが稼動されるよう、OSやネットワークの設定をする。(必須)

例:

- アクセスポートの制限

(2)不正プログラムへの対処

いわゆるプログラムソースコードの改ざんなどバックドアによるシステムへの侵入を防ぐ為、以下の対策を実施すること。

- 稼動するプログラムは作成者を明文化し、改ざんがなされないようチェック、およびテストを実施する。(必須)

4.1.6.5　必要のないファイルアクセス経路への制限

(1)ＤＢ構成ファイルへのアクセス経路禁止設定

ＤＢの破壊防止の為、以下の対策を実施すること。

- 管理者以外のＤＢ構成ファイルへのアクセスは、制限する。(必須)

  例:

  - utl_fileパッケージの実行権限
  - utl_file_dirの設定

- 表などの定義スクリプトへのアクセスは、管理者のみに制限する。(必須)
- 定期的にＤＢ構成ファイルへのアクセス許可者の権限見直しを実施する。(必須)

(2)ＤＢへのアクセス経路の制限

ＤＢの不正利用、操作ミス防止の為、以下の対策を実施すること。

- ＤＢへアクセスする為のＡＰ(運用ツールなども含む)の配布範囲は、アクセスを許可した者が使用する機器のみに限定する。(必須)
- ＤＢ/サーバへのアクセス経路(ネットワーク経路など)は、必要最小限の範囲に限定する。(推奨)

4.2 検知、追跡系のＤＢセキュリティ対策

問題が発生した場合に備え、適切な内容のログを取得することが必要である。さらにログを監視、分析することで問題の早期検知や原因の究明が可能になる。

ここでは、有効な検知、および追跡の対策を記述する。

4.2.1 ログの管理

ＤＢＭＳにおいてログを取得していない状況では、実際に情報漏洩や不正アクセスの被害に遭っても調査/追跡が困難もしくは不可能となってしまう。また、取得したログを適切に管理しておかなければ、証拠としての信頼性が低下する。

ここでは、情報漏洩や不正アクセスなど有事の際に調査/追跡を可能する為に、ログを証拠として残しかつ安全に管理する為の対策を記述する。

4.2.1.1 ログの取得

(1)ログイン情報取得

ログインを知る為、以下の対策を実施すること。

- ログイン時のログを取得する。(必須)

(2)ＤＢＭＳ一般情報へのアクセス情報の取得

重要情報(個人情報、機密情報 など)に対するアクセスを知る為、以下の対策を実施すること。

- 重要な一般情報へのアクセス(参照/更新)をログとして取得する。(必須)

(3)ＤＢＭＳ管理情報へのアクセス情報の取得

重要なＤＢＭＳ管理情報に対するアクセスを知る為、以下の対策を実施すること。

- 重要な管理情報へのアクセス(参照/更新)をログとして取得する。(必須)

(4)ＤＢオブジェクトの変更情報の取得

ＤＢオブジェクトの変更を知る為、以下の対策を実施すること。

- ＤＢオブジェクト(ＤＢアカウント、テーブル、ビュー など)の作成、変更ログを取得する。(必須)

4.2.1.2 ログの保全

取得したログが必要な場合に利用できるようにする為、以下の対策を実施すること。

- ログを外部記憶媒体に保管すること。（必須）

  例：

  - テープ、ＬＴＯ装置、ディスク、外部サーバ、外部ＤＢなどに保管
  - 書き換え不能なストレージを使用

- ログを保存した外部記憶媒体は安全な場所に保管する。（必須）

  例：

  - 外部記憶媒体は施錠出来るところに保管
  - 台帳により持ち出し管理の実施

- ログの改ざん対策を講じる。（必須）

  例：

  - ログへのアクセス制御
  - ログの暗号化/多重化
  - 電子証明書（タイムスタンプなど）の付加

4.2.2 不正アクセス検知

ＤＢへの不正アクセスを防御していても、アクセスを試みられる可能性はある。このような動きを検知する仕組みを設け、体制を整備する必要がある。

ここでは、ＤＢへの不正アクセスを検知する為に必要な、運用上の監視項目について記述する。

4.2.2.1 監視の仕組み作り

不正アクセスを検知する為、以下の対策を実施すること。

- 検知した不正アクセスを通知する仕組みを設ける。（必須）

  例：

  - ログイン失敗の回数オーバによるアカウントロックはシステム責任者/管理者/運用者にメールで通知

4.2.2.2 アクセス時間のチェック

(1)ＤＢＭＳ管理情報へのアクセス検知

ＤＢＭＳ管理情報への時間帯での疑わしいアクセスを検知する為、以下の対策を実施すること。

- ログを監視し、申請されていない時間帯のアクセスを検知する。（必須）
- 申請された内容と、作業結果に相違のないことをログと申請内容を確認する。（推奨）

(2)一般情報へのアクセス検知

一般情報への時間帯での疑わしいアクセスを検知する為、以下の対策を実施すること。

- 一般(ＡＰ)ユーザアカウントごとに、ＤＢＭＳにアクセスし得る正規の時間帯、曜日がいつであるのかの定義を行う。（必須）
- セッション情報のログを監視し、正規のアクセス時間帯でないアクセスを検知する。（必須）

4.2.2.3 アクセス不可の端末/IPアドレスのチェック

(1)アクセス不可の端末/IPアドレスの検知

許可されていない端末からのアクセスを検知する為、以下の対策を実施すること。

- ＤＢＭＳへアクセス可能な端末を定義する。（必須）
- 許可されていない端末からのアクセスを検知する。（必須）

(2)管理者アカウントによるアクセス

ＤＢＭＳ管理者アカウントのアクセス経路からのアクセスを検知する為、以下の対策を実施すること。

- ＤＢＭＳ管理者が使用する端末/ＯＳユーザ/アカウントの組合せを定義する。（必須）
- 上記の組合せ以外のアクセスを検知する。（必須）

(3)一般アカウントのアクセス

一般アカウントのアクセス経路からのアクセスを検知する為、以下の対策を実施すること。

- 一般アカウントによるアクセスのパターン（ＡＰサーバ、アカウントなど）を定義する。（必須）
- 上記パターン以外のアクセスを検知する。（必須）

4.2.2.4 その他

上記以外の不正アクセスを検知する為、以下の対策を実施すること。

- ログイン失敗の回数が、ある期間想定以上に多くないかログを監視し、パスワードの辞書攻撃を検知する。（推奨）
- 取得したログを監視し、ＳＱＬ文の発行を検知する。（推奨）
- 取得したログを監視し、ＤＢオブジェクトの作成、変更を検知する。（推奨）

4.2.3 ログの分析

ある行為を不正と判断するには、様々な角度からの調査を必要とする場合がある。また不正行為を発見した場合、過去に遡ってログを分析する必要がある。

ここでは、取得したログから不正行為を効率的に検出する為の対策を記述する。

4.2.3.1 ログ分析の仕組み作り

不正アクセスの原因究明や、不正行為を検出する為、以下の対策を実施すること。

- ログを分析する仕組みを設ける。(必須)

  例:

  - ログ分析システムの導入

4.2.3.2 定期的なログの分析

(1)定期的なセッション情報の分析

ログインを検出する為、以下の対策を実施すること。

- セッション情報を分析する。(必須)

  例:

  - ログイン失敗回数が多いセッションの傾向分析
  - 長時間に渡りログインしているセッションの傾向分析
  - 大量のリソースを消費するセッションの傾向分析

(2)定期的なＤＢアクセス情報の分析

ＤＢアクセスを検出する為、以下の対策を実施すること。

- ＳＱＬ文を分析する。(必須)

  例:

  - 長時間に渡り実行されているＳＱＬの傾向分析
  - 大量のリソースを消費するＳＱＬの傾向分析

データベースセキュリティガイドライン執筆者（敬称略）

ＤＢＳＣセキュリティガイドラインワーキンググループ（社名５０音順）

主査 ：	株式会社富士通大分ソフトウェアラボラトリ	三河尻　浩泰
	アイピーロックスジャパン株式会社	成田　泰彦
	株式会社アシスト	小河　昭一
	株式会社アシスト	徳原　茂之
	株式会社インサイトテクノロジー	岸本　拓也
	エー・アンド・アイシステム株式会社	佐伯　雪
	エー・アンド・アイシステム株式会社	水谷　政芳
	新日鉄ソリューションズ株式会社	金本　直子
	新日鉄ソリューションズ株式会社	白杉　武志
	日本オラクル株式会社	北野　晴人
	株式会社日立システムアンドサービス	小川　清司
	富士通株式会社	大可　正龍
	富士通株式会社	都築　和則
	富士通株式会社	能宗　賢治
	株式会社富士通大分ソフトウェアラボラトリ	大石　卓哉
	株式会社富士通大分ソフトウェアラボラトリ	佐藤　恵
	株式会社富士通大分ソフトウェアラボラトリ	前嶋　浩司
	株式会社富士通ソーシアルサイエンスラボラトリ	大國　将彦
	株式会社ラック	大野　祐一
	株式会社ラック	菅原　良也
	株式会社ラック	須田　堅一