データベース管理システムの
ベースプロテクションプロファイル
(DBMS PP)

バージョン 2.0 7

平成 28 年 3 月 30 日　翻訳 暫定第 0.1 版
独立行政法人情報処理推進機構
技術本部 セキュリティセンター
情報セキュリティ認証室

改版履歴

バージョン	日付	説明
1.0	2004 年 9 月 30 日	U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments BR-DBMSPP
1.1	2006 年 6 月 7 日	U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments BR-DBMSPP
1.2	2007 年 7 月 25 日	U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments BR-DBMSPP
1.3	2010 年 12 月 24 日	U.S. Government Protection Profile for Database Management Systems DBMSPP
2.0	2014 年 12 月 15 日	Base Protection Profile for Database Management Systems DBMS PP
2.07	2015 年 9 月 9 日	データベース管理システムのベースプロテクションプロファイル DBMS PP の認証済みバージョン

本プロテクションプロファイルの状況及び更新を含め、詳細な情報については、CCUF ウェブサイト上の DBMS WG/TC プロジェクトエリアに掲載されている：
https://ccusersforum.onlyoffice.com/products/projects/tasks.aspx?prjID=410822

本書に対するコメントは、DBMS WG/TC ワークスペースへ送付されるべきである。コメントには、文書のタイトル及びバージョン、ページ、セクション番号、行番号、及び詳細なコメント及び勧告が含まれるべきである。

プロテクションプロファイルのタイトル：

データベース管理システムのベースプロテクションプロファイル

コモンクライテリアバージョン：

本プロテクションプロファイル「データベース管理システムのベースプロテクションプロファイル (DBMS PP)」は、コモンクライテリア (CC) のバージョン 3.1 [REF 1] を用いて更新された。

目次

1　プロテクションプロファイル序説 6
1.1　PP 識別情報 6
1.2　TOE 概要 6
1.3　PP の構成 6
1.4　文書の表記法 7
1.5　用語集 8
1.6　文書の構成 8
2　TOE 記述 9
2.1　製品種別 9
2.2　TOE 定義 10
2.3　TOE によって提供されるセキュリティ機能 10
2.4　オプションのセキュリティ機能 11
2.5　TOE 運用環境 12
2.5.1　エンクレーブ 12
2.5.2　TOE アーキテクチャ 12
2.5.3　TOE 管理 13
3　適合主張 14
3.1　CC パート 2 及び 3 への適合 14
3.2　パッケージ適合 14
3.3　その他のプロテクションプロファイルへの適合 14
3.4　適合ステートメント 14
4　セキュリティ課題定義 15
4.1　非形式的な議論 15
4.2　資産及び脅威エージェント 15
4.3　脅威 16
4.4　組織のセキュリティ方針 17
4.5　前提条件 18
5　セキュリティ対策方針 20
5.1　TOE セキュリティ対策方針 20
5.2　運用環境のセキュリティ対策方針 22
6　拡張セキュリティ機能要件 24
FTA_TAH_(EXT).1 TOE アクセス情報 24
FIA_USB_(EXT).2 高度な利用者-サブジェクト結合 25
7　セキュリティ要件 26
7.1　セキュリティ機能要件 26
7.1.1　セキュリティ監査 (FAU) 27
7.1.2　利用者データ保護 (FDP) 31
7.1.3　識別と認証 (FIA) 32
7.1.4　セキュリティ管理 (FMT) 34
7.1.5　TOE セキュリティ機能の保護 (FPT) 36
7.1.6　TOE アクセス (FTA) 37
7.2　セキュリティ保証要件 38
8　根拠 39

8.1　TOE セキュリティ対策方針の根拠 39
8.1.1　TOE セキュリティ対策方針のカバレージ 40
8.1.2　TOE セキュリティ対策方針の根拠 41
8.2　環境のセキュリティ対策方針の根拠 51
8.3　セキュリティ機能要件根拠 64
8.3.1　拡張セキュリティ機能要件根拠 64
8.3.2　TOE セキュリティ機能要件根拠 65
8.3.3　すべてのセキュリティ機能要件の依存性が満たされていることの根拠 70
8.4　すべてのセキュリティ保証要件が満たされていることの根拠 72
8.5　結論 73
9　附属書 74
附属書 A.　参考資料 75
附属書 B.　用語集 76
附属書 C.　略語と頭字語 79

表の目次

表 1：TOE に適用される脅威 16
表 2：TOE に適用される方針 17
表 3：TOE 環境に適用される前提条件 18
表 4：TOE セキュリティ対策方針 20
表 5：運用環境のセキュリティ対策方針 22
表 6：運用環境の IT セキュリティ対策方針 23
表 7：セキュリティ機能要件 26
表 8：監査対象事象 28
表 9：保証要件 38
表 10：TOE セキュリティ対策方針のカバレージ 40
表 11：TOE セキュリティ対策方針の根拠 41
表 12：TOE 環境のセキュリティ対策方針の SPF 項目のカバレージ 51
表 13：環境のセキュリティ対策方針の根拠 52
表 14：拡張セキュリティ機能要件根拠 64
表 15：TOE セキュリティ機能要件根拠 65
表 16：セキュリティ機能要件の依存性 70

1　プロテクションプロファイル序説

1.1　PP 識別情報

タイトル：データベース管理システムのベースプロテクションプロファイル (DBMS PP)

スポンサー：DBMS ワーキンググループ／テクニカルコミュニティ

CC バージョン：コモンクライテリア (CC) バージョン 3.1 [REF 1]

PP バージョン：2.07

発行日：2015 年 9 月 9 日

キーワード：データベース管理システム、DBMS PP、DBMS、COTS、商用セキュリティ、アクセス制御、CC EAL2 要件追加。

1.2　TOE 概要

「データベース管理システムのベースプロテクションプロファイル」は、市販 (COTS) のデータベース管理システム (DBMS) のセキュリティ要件を規定する。TOE 種別は、データベース管理システムである。

本プロテクションプロファイルに適合する TOE には、DBMS サーバが含まれるがそれに限定されるものではなく、基盤となるシステム上、即ち、オペレーティングシステム、ハードウェア、ネットワークサービス、またはカスタムソフトウェア、でのレイヤー化されたアプリケーションのみのソフトウェアとして評価可能であり、また通常はより大規模なシステムのコンポーネントとして運用環境に埋め込まれている。本プロテクションプロファイルは、評価対象 (TOE) 及びその環境のセキュリティ対策方針を達成するために必要な要件を確立する。

適合 TOE は、利用者識別情報、及びオプションとしてグループ所属に基づくアクセス制御、例、任意アクセス制御 (DAC)、並びにセキュリティ関連事象の監査記録の生成を提供する。TOE の許可された管理者は、彼らに割り当てられた特権を誤使用しないと信頼される。

本 PP への適合を主張するセキュリティターゲット (ST) は、CC パート 1 のセクション D3 に定義される論証 PP 適合の最小限の規格を満たさなければならない。[REF 1a]

1.3　PP の構成

データベース管理システムのプロテクションプロファイル (DBMS PP) は、ベースプロテクションプロファイルとして構造化され、一連の (オプションの) プロテクションプロファイル拡張パッケージ[1]を収容する用意ができている。この構造は、さまざまな運用環境及びさまざまな運用要件への適合性を最大化するために選択された。データベース管理システムは、さまざまな形で機能を提供する可能性があるためである。

以下の PP 構成が許容される：

1. ベース PP のみ (DBMS PP)

[1] これらはまた、「プロテクションプロファイルモジュール」とも呼ばれる。より詳細な情報については、 [REF 2] を参照されたい。

1.4　文書の表記法

英国式つづりを米国式つづりに置き換えた以外には、本 PP で用いられる記法、様式、及び表記法は CC のバージョン 3.1 と一貫している。PP の読者を助けるため、選択された表記法についての説明をここで行う。

CC では、機能要件に対していくつかの操作を行うことを許容している。*詳細化*、*選択*、*割付*、及び*繰返し*が CC のパート 1 の第 8 章に定義されている [REF 1a]。これらの操作のすべてが、本 PP で用いられている。

詳細化の操作は、要件に詳細を付け加え、これによってさらに要件を制限するために用いられる。セキュリティ要件の詳細化は、**太字テキスト**、または削除の場合には、~~**取り消し線付きの太字テキスト**~~によって示される。

選択は、要件のステートメントに CC の提供する 1 つ以上の選択肢を選択するために用いられる。PP 作成者による選択は*イタリック体*のテキストによって表示され、セキュリティターゲット (ST) によって記入されるべき選択は、大括弧内に選択が行わるべきことを示す指示 [選択：] と共に、イタリック体ではなく表記される。

割付操作は、パスワード長のような、まだ規定されていないパラメタへ具体的な値を割り付けるために用いられる。PP 作成者による割付は大括弧内に値を示すことによって [割付の値] 表示され、ST 作成者によって記入されるべき割付は大括弧内に割付が行わるべきことを示す指示 [割付：] と共に表記される。

繰返し操作は、さまざまな操作と共にコンポーネントが繰り返されるときに用いられる。

繰返しは、コンポーネントの識別子に続く括弧の中に繰り返し回数を示すことによって表記される (繰り返し回数)。

CC のパラダイムでは、プロテクションプロファイルやセキュリティターゲットの作成者が、彼ら独自の要件を作成することも許容している。そのような要件は「拡張要件」と呼ばれ、作成者の必要性に合致する適切な要件を CC が提供しないときに許容される。**拡張要件**は、識別されなければならず、またその要件を関連付けるにあたって CC のクラス／ファミリ／コンポーネントモデルを利用することが要求される。本 PP では、拡張要件はコンポーネント名の後に伴う「(EXT)」によって示される。

適用上の注釈は、要件の意図を明確化するか、実装上の選択を識別するか、あるいは要件の「合格・不合格」基準を定義して、開発者を助けるために提供される。適用上の注釈が適切であるようなコンポーネントについては、要件コンポーネントの後に適用上の注釈が続く。

1.5　用語集

用語集については、附属書 B を参照されたい。

1.6　文書の構成

セクション 1 では、プロテクションプロファイルの概説資料が提供される。

セクション 2 では、その予想される用途及び接続性の観点から評価対象について記述される。

セクション 3 では、本プロテクションプロファイルによってなされる適合主張が与えられる。

セクション 4 では、脅威及びセキュリティ課題の観点からセキュリティ課題を定義する。

セクション 5 では、これらの脅威及び方針から導き出されるセキュリティ対策方針が識別される。

セクション 6 では、拡張セキュリティ要件が識別され、定義される。

セクション 7 では、機能ベースの対策方針が満たされるために TOE によって満たされなければならない CC からのセキュリティ機能要件が識別され、定義される。このセクションでは、評価セキュリティレベル (EAL) 2 に追加されたセキュリティ保証要件もまた識別される。

セクション 8 では、情報技術セキュリティ対策方針が方針及び脅威を満たすことを論証する根拠が提供される。方針及び脅威それぞれのカバレージについての論拠が提供される。次にこのセクションでは、一連の要件が対策方針に対応して完成されていること、そして各セキュリティ対策方針が 1 つ以上のコンポーネントの要件によって対処されていることが説明される。それぞれの対策方針のカバレージについての論拠が提供される。

セクション 9、附属書は、PP に伴うものであり、読者に明確化及び／または説明を提供するような附属書が含まれる。

> 附属書 A、参考資料では、PP の利用者によるさらなる調査のための背景となる資料が提供される。
>
> 附属書 B、用語集では、用語の定義のリストが提供される。
>
> 附属書 C、略語と頭字語では、文書を通して使用される略語のリストが提供される。

2　TOE 記述

2.1　製品種別

本プロテクションプロファイル (PP) に記述される評価対象 (TOE) は、データベース管理システム (DBMS) である。

DBMS は、情報を保存し、許可された利用者にその情報の検索と更新を可能とする、コンピュータ化されたリポジトリである。DBMS は、任意の時点でただ 1 人の利用者が DBMS にアクセスするかもしれないシングルユーザシステムかもしれないし、同時に多数の利用者が DBMS にアクセスするかもしれないマルチユーザシステムかもしれない。

DBMS には、DBMS アクセスを許可された利用者に制限したり、利用者及びオプションとしてグループの許可に基づいてデータベース管理システムの制御下にあるオブジェクトに任意アクセス制御を実施したり、利用者のアクションの監査により利用者責任追跡性を提供する機能を有する。

DBMS は、以下の機能の一部またはすべてを行う DBMS サーバアプリケーションから構成される。

a) 利用者データ及び DBMS データへの利用者のアクセスを制御すること；

b) 基盤となるオペレーティングシステムと対話し、またもしかするとその一部を補完して、DBMS の管理下にあるデータを検索し提示すること；

c) 値または値の範囲に基づく高速な検索を行うため、データ値をその物理ロケーションにインデックスすること；

d) あらかじめ作成されたプログラム (即ち、ユーティリティ) を実行し、データベースのバックアップ、回復、ロード、及び複製等の共通タスクを行うこと；

e) 同時データベースアクセスを可能とするメカニズム (例、ロック) をサポートすること；

f) 利用者データ及び DBMS データの回復を補助すること (例、トランザクションログ)；及び

g) 利用者が行う操作を追跡すること。

大部分の商用 DBMS サーバアプリケーションは、以下の機能についても提供する。

- DBMS データ構造及び構成が概念化可能なデータモデル (例、階層化、オブジェクト指向、リレーショナルデータモデル) 及び定義済み DBMS オブジェクト。
- 許可された利用者がデータベース構築を定義し；利用者または DBMS データへのアクセス及び改変を行い；利用者または DBMS データを提示し；そしてそれらのデータに関する操作を行うことを許容するような、高レベル言語またはインタフェース。

DBMS は、2 つの主要な利用者の種別をサポートする：

- データオブジェクトを確認及び／または変更するために DBMS と対話するような、アクセスする権限を有する利用者。
- 彼らがインストールし、設定し、管理し、あるいは所有するデータベースに関する組織のさまざまな情報関連の方針 (例、アクセス、完全性、一貫性、可用性) を実施し管理するような、権限付与された管理者。

DBMS は、2 つの種別のデータを保存しアクセスを制御する。

- 第 1 の種別は、DBMS が維持管理し保護する利用者データである。利用者データは、以下から構成可能である：
  a) データベースオブジェクト中に、あるいはデータベースオブジェクトとして保存される利用者データ；
  b) 利用者データベース及びデータベースオブジェクトの定義であって、通常は DBMS メタデータと呼ばれるもの；及び
  c) 利用者によって開発されたクエリ、関数、または手続きであって、DBMS が利用者のために維持管理するもの。
- 第 2 の種別は DBMS データ (例、設定パラメタ、利用者セキュリティ属性、トランザクションログ、監査指示、及び記録) であって、DBMS が維持管理し DBMS の運用のために利用可能である。

DBMS 仕様が、上記のリストに示された DBMS サーバ機能の詳細な要件を識別する。

2.2 TOE 定義

TOE は、DBMS サーバアプリケーションのセキュリティ機能のインスタンス (すなわちデータベースエンジン) の少なくとも 1 つとそれに関連付けられたガイダンス文書及び DBMS が対話する外部 IT エンティティへのインタフェースから構成される。

本 PP は、特定のアーキテクチャを規定しない。ST 作成者は、評価されるべき TOE アーキテクチャを識別し記述する必要がある。

DBMS が対話する可能性のある外部 IT エンティティ (それが TOE の外側に存在する場合) には、以下が含まれる：

- 利用者に DBMS サーバとのインタフェースを可能とするクライアントアプリケーション。
- TOE がインストールされているホストオペレーティングシステム (ホスト OS)；
- ホスト OS が DBMS または DBMS 利用者に代わって対話する可能性のあるネットワーキング、プリンティング、データ記憶等のデバイス；並びに、アプリケーションサーバ、ウェブサーバ、認証サーバ、ディレクトリサービス、監査サーバ、及びトランザクションプロセッサ等の IT 製品であって、DBMS 機能またはセキュリティ機能を行うために DBMS が対話する可能性のあるもの。

ホスト OS が TOE の外側に存在する場合、DBMS は望ましい度合いのセキュリティ機能の統合を提供するために常駐しなければならないホスト OS と共に、DBMS 機能をサポートするために必要とされるそれらの 1 つまたは複数の OS の設定を規定しなければならない。しかし、TOE の機密性、完全性、及び可用性の目標は、DBMS 及びそれが対話する外部 IT エンティティという、トータルなパッケージによって満たされなければならない。すべての場合において、TOE は TOE の設置及び管理指示に従って設置され管理されなければならない。

2.3 TOE によって提供されるセキュリティ機能

本 PP に対して評価される DBMS は、以下のセキュリティサービスを提供する。

TOE によって提供されなければならないセキュリティサービス：

- サブジェクトの識別情報またはサブジェクト及びオブジェクトが属するグループ

に基づいてオブジェクトへのアクセスを制限する任意アクセス制御 (DAC) であって、許可された利用者が彼らの制御するオブジェクトがどのように保護されるか規定することを可能とするもの。

- すべての監査対象事象に関する情報を作成するための監査取得。
- 許可された管理者が任意アクセス制御、識別と認証、及び監査の方針を設定することを可能とする、許可された管理者の役割。TOE は、許可された管理者の役割を強制しなければならない。

  注記 : 一部の管理タスクは、特定の利用者へ移管される可能性がある (その利用者はその移管によって管理者となるが、一部の制限された管理アクションのみを行うことができる)。これらの利用者が、自分に割り当てられた管理者の権利を拡張できないことを保証することは、TOE が提供しなければならないセキュリティ機能の 1 つである。

2.4 オプションのセキュリティ機能

TOE 及び／または IT 環境によって提供されなければならないセキュリティサービス。

このセキュリティ機能は、DBMS ベース PP の以下の章ではモデル化されない。ST 作成者は、追加の (オプションの) セキュリティ機能及び対応するセキュリティ機能要件の記述を統合しなければならない。

- 利用者が DBMS 上に保存された情報へアクセスする許可を得る前に一意に識別され認証される、識別と認証 (I&A)。
- 利用者及び DBMS データに利用者が行うすべてのセキュリティ関連操作の記録を保存する、監査格納サービス。
- 潜在的及び実際のセキュリティ侵害を検出するために保存された監査記録を許可された管理者がレビューすることを可能とする、監査レビュー。

しかし、本 PP への適合は、以下を保証するものではない：

- 物理的保護メカニズム及びそれらを利用するための管理手続きが用意されていること。
- DBMS に常駐するデータの完全な可用性を保証するメカニズムが用意されていること。DBMS は、特定の時点で複数の人物へデータの利用を可能とするデータへの同時アクセスを提供でき、また利用者が DBMS サービス／資源を独占することを防止する DBMS 資源割当て制限を強制できる。しかし、物理的または環境的災害、記憶デバイスの故障、または基盤となるオペレーティングシステムへのハッカー攻撃によって発生する可能性のある利用不能を検出または予防することはできない。そのような可用性への脅威については、必要とされる対策を環境が提供しなければならない。
- 利用者が DBMS から取り出すデータを適切に保全することを保証するメカニズムが用意されていること。DBMS を利用し管理する 1 つまたは複数の組織のセキュリティ手続きによって、利用者のデータ検索、記憶、エクスポート、及び廃棄の責任が定義されなければならない。
- 許可された管理者が賢明に DAC を利用することを保証するメカニズム。DBMS は、利用者及びオプションとして定義済みグループに属する利用者が彼らの仕事を行うために必要なデータのみへのアクセスを許可されるアクセス制御方針をサポー

トできるが、アクセス制御を設定できる許可された管理者がそれを思慮深く行うことは完全には保証できない。

2.5 TOE 運用環境

2.5.1 エンクレーブ

「エンクレーブ」という用語が、TOE の運用が意図される環境をさらに特徴づける。エンクレーブは 1 つの権威の制御下にあり、それを他の環境から保護するための、人的及び物理的セキュリティを含めた均質なセキュリティ方針を有する。エンクレーブは、組織またはミッション特有のものであってもよいし、複数のネットワークを含むかもしれない。エンクレーブは、運用エリアネットワーク等、論理的なものであったり、物理ロケーション及び近接性に基づいていたりするかもしれない。エンクレーブ内部の資源へアクセスする任意のローカル及び外部エレメントは、エンクレーブの方針を満たさなければならない。

DBMS は、ホスト OS 中、ホストコンピュータ及びホスト OS が常駐する IT 環境中、並びに環境の外側だがエンクレーブの内側に常駐する、他の IT 製品と対話することが期待される。DBMS とそのような製品との間の情報のセキュアなやり取りに用いられる IT 及び非 IT メカニズムは、管理的に決定され調整されることが期待される。同様に、そのようなやり取りに伴う DAC 方針をネゴシエーションまたは翻訳する IT 及び非 IT メカニズムは、関連する組織によって解決されることが期待される。

また DBMS はエンクレーブの外側の IT 製品、認証局 (CA) のような、エンクレーブ内部の IT 製品によって信頼済み CA と定義されているものと対話するかもしれない。

2.5.2 TOE アーキテクチャ

本 PP は、特定のアーキテクチャを規定しない。本 PP に適合する TOE は、複数のアーキテクチャにおいて評価されてもよいし運用されてもよい、以下の 1 つ以上を含むがそれに限定されない：

- DBMS サーバアプリケーションが動作するスタンドアロンシステム；DBMS サーバと DBMS クライアントが動作するスタンドアロンシステムであって、所与の時点で 1 人、または複数のオンライン利用者にサービスを提供するもの；
- 複数の分散 DBMS サーバと同時に通信を行うシステムのネットワーク；
- DBMS クライアントが動作し同時に DBMS サーバと通信を行うワークステーションまたは端末のネットワーク；これらのデバイスはホストコンピュータとハードワイヤード接続されているかもしれないし、ローカルまたはワイドエリアネットワークによって接続されているかもしれない。
- 1 つまたは複数のアプリケーションサーバと通信を行うワークステーションのネットワークであって、そのアプリケーションサーバがワークステーションの利用者またはその他のサブジェクトに代わって DBMS と対話するもの (例、利用者要求を管理するトランザクションプロセッサと対話する DBMS サーバ)；及び
- 複数の分散 DBMS サーバと同時に通信を行うワークステーションのネットワーク；DBMS サーバはすべて単一のローカルエリアネットワーク内部に存在するかもしれないし、地理的に分散しているかもしれない。

本 PP は、他のものも含め、これらのアーキテクチャのそれぞれがサポートされることを可能とする。考えられるアーキテクチャとして、DBMS 利用者が TOE へローカルエリアネットワーク (LAN) を介してアクセスするエンクレーブがある。他のエンクレーブの中の利用

者は、1 つまたは複数の境界保護メカニズム (例、ファイアウォール) を経由し、次に LAN への通信サーバまたはルータを介して、LAN 及びそれに接続されたホストコンピュータ及びサーバへアクセスする。具体的なエンクレーブ構成及びそのサポートする DBMS アクセス方針に応じて、すべての利用者 (エンクレーブの内側と外側の両方) は次にアプリケーションサーバへアクセスし、それが TOE 利用者を TOE が動作するエンクレーブコンピュータへ接続したり、完全な利用者／DBMS セションを管理したりするかもしれない。

2.5.3　TOE 管理

本 PP は、DBMS の開発者によって確立される 1 つの必要な管理者役割 (許可された管理者) を定義する。本 PP は、DBMS 開発者またはセキュリティターゲット作成者が、より多くの役割を定義することを可能とする。

セキュリティターゲットがそれを可能とした場合、システムの管理者が利用者に特権を割り当てるかもしれない。DBMS が設置されたときには、特権及びそれに関連する責任を割り当てる能力もまた存在していなければならない。

TOE の許可された管理者は、彼らに割り当てられた管理特権に対応した能力を持つことになる。もちろん、特権を確立し割り当てる能力そのものも、特権機能の 1 つである。

3　適合主張

以下のセクションでは、データベース管理システムプロテクションプロファイル (DBMS PP) の適合主張を記述する。

3.1　CC パート 2 及び 3 への適合

DBMS PP は、CC バージョン 3.1 改訂第 4 版パート 2 拡張及びパート 3 適合である。

3.2　パッケージ適合

DBMS PP は、評価保証レベル EAL2 及び追加の保証コンポーネント ALC_FLR.2 を主張する。

3.3　その他のプロテクションプロファイルへの適合

DBMS PP は、その他のいかなるプロテクションプロファイルへの適合も主張しない。

3.4　適合ステートメント

DBMS PP は、ST による論証適合を要求する。

4　セキュリティ課題定義

このセクションでは、DBMS のセキュリティ課題定義 (SPD) を記述する。まず、SPD の非形式的な議論が、続いて本 PP によって対応される具体的なセキュリティ要件の識別に利用される識別された脅威、方針、及び前提条件についてのより形式的な記述が提示される。

4.1　非形式的な議論

高価値データのリポジトリとしてよく利用されていることから、攻撃者は DBMS 設置を危殆化のターゲットとすることが通例である。以下に挙げる脆弱性を、攻撃者が利用するかもしれない：

- DBMS 及び関連するプログラム及びシステム中の設計の欠陥及びプログラミングのバグであって、さまざまなセキュリティ脆弱性 (例、弱い、または効果的でないアクセス制御) を作り出し、データの損失／破損、性能の劣化等を引き起こす可能性のあるもの。
- 許可されたデータベース利用者、またはネットワーク／システム管理者、または許可されない利用者またはハッカーによる、許可されないまたは意図されないアクティビティまたは乱用 (例、データベース内の機微なデータ、メタデータまたは機能への不適切なアクセス、あるいはデータベースのプログラム、構造またはセキュリティ設定への不適切な変更)
- 許可されないアクセス、個人または独占的データの漏えいまたは暴露、データまたはプログラムの削除またはそれらへの損害、データベースへの許可されたアクセスの中断または拒否、他のシステムへの攻撃及び予期されないデータベースサービスの故障等のインシデントを引き起こすマルウェア感染。
- 無効なデータまたはコマンドの入力、データベースまたはシステム管理プロセスの間違い、サボタージュ／犯罪による損害等が原因のデータ破損及び／または損失。

4.2　資産及び脅威エージェント

セクション 4.3 に示す脅威は、さまざまな脅威エージェント及び資産に対応している。「脅威エージェント」という用語は、CC パート 1 に定義されている。本 PP で用いられる「利用者または利用者に代わって作用するプロセス」という用語は、資産に悪影響を与える可能性のあるエンティティの特定のクラスを規定する。

以下の表 1 に言及される資産は、CC パート 1 [REF 1a] 、または本文書の附属書 B に示される用語集で定義されている。

「TSF データ」、「TSF」及び「利用者データ」という用語は、CC パート 1 に定義されている。「TSF 内の実行可能コード」、「公開オブジェクト」、「TOE 資源」及び「設定データ」という用語は、本文書の附属書 B に示される用語集で規定されている、

4.3　脅威

以下の脅威は、TOE によって識別され対応されるものであり、セクション 8.1 の脅威の根拠と組み合わせて読まれるべきである。

適合 TOE は、TOE への脅威に対抗するセキュリティ機能を提供し、また法令によって課される方針を実装する。

表 1：TOE に適用される脅威

脅威	定義
T.ACCESS_TSFDATA	脅威エージェントが、適切な許可なしに TOE の機能を利用して TSF データを読み出したり改変したりするかもしれない。
T.ACCESS_TSFFUNC	脅威エージェントが、TSF の保護メカニズムをバイパスして TSF を利用したり管理したりするかもしれない。
T.IA_MASQUERADE	利用者または利用者に代わって作用するプロセスが、利用者データ、TSF データ、または TOE 資源への許可されないアクセスを得るために許可されたエンティティに成りすますかもしれない。
T.IA_USER	公開オブジェクトを例外として、脅威エージェントが、識別され認証されることなく、利用者データ、TSF データ、または TOE 資源へアクセスするかもしれない。
T.RESIDUAL_DATA	利用者または利用者に代わって作用するプロセスが、1 利用者またはプロセスから別の利用者またはプロセスへの TOE 資源の再割当てによって、利用者または TSF データへの許可されないアクセスを得るかもしれない。
T.TSF_COMPROMISE	利用者または利用者に代わって作用するプロセスが、設定データの不適切なアクセス (閲覧、改変または削除) を引き起こしたり、TSF 内の実行可能コードを危殆化させたりするかもしれない。
T.UNAUTHORIZED_ACCESS	脅威エージェントが、TOE のセキュリティ方針に従えば権限のない利用者データへの許可されないアクセスを得るかもしれない。

4.4　組織のセキュリティ方針

以下の組織のセキュリティ方針は、PP に適合する TOE によって対応される。

表 2：TOE に適用される方針

方針	定義
P.ACCOUNTABILITY	TOE の許可された利用者は、TOE 内での自分のアクションに責任を持たなければならない。
P.ROLES	TSF 機能への管理権限は、信頼される要員へ与えられ、その人物が有する管理職務のみをサポートするよう、なるべく制限されなければならない。この役割は、他の許可された利用者とは分離された別個のものでなければならない。
P.USER	権限は、そのアクションを正しく行うと信頼される利用者のみへ与えられなければならない。

4.5　前提条件

本セクションには、TOE が常駐する IT 環境に関する前提条件が含まれる。

表 3：TOE 環境に適用される前提条件

前提条件	定義
物理的側面	
A.PHYSICAL	TOE によって保護される IT 資産の価値に対応する適切な物理的セキュリティを IT 環境が TOE に提供することが前提となる。
人的側面	
A.AUTHUSER	許可された利用者は、TOE によって管理される情報の少なくとも一部へアクセスするために必要な許可を有する。
A.MANAGE	TOE のセキュリティ機能は、1 人以上の適格な管理者によって管理される。システム管理要員は不注意であったり、意図的に怠慢であったり、敵対的であったりせず、ガイダンス文書によって提供される指示を遵守する。
A.TRAINEDUSER	利用者は、自分の利用者データへの完全な制御を行使することにより、セキュアな IT 環境内で何らかのタスクまたは一群のタスクを完了できるよう十分に教育され信頼されている。
手続き的側面	
A.NO_GENERAL_PURPOSE	DBMS の動作、管理、及びサポートに必要なサービス以外に、DBMS 上で利用可能な汎用コンピューティング機能 (例、コンパイラやユーザアプリケーション) が存在しない。
A.PEER_FUNC_&_MGT	TOE へ TSF データまたはサービスを提供する、またはセキュリティ方針の決定の実施において TSF をサポートすると TSF によって信頼されたすべてのリモート高信頼 IT システムは、TSF によって用いられる機能をこの機能に定義された前提条件と一貫して正しく実装し、TOE のセキュリティ方針の制限と適合性のあるセキュリティ方針の制限のもとで適切に管理され運用されることが前提となる。
A.SUPPORT	IT 環境における信頼されたエンティティによって提供され、TOE によって使用される、時刻と日付の設定、監査取得で使用される情報、利用者認証、及び許可をサポートするために使用される任意の情報は、正確であり、最新のものである。
接続性の側面	
A.CONNECT	リモート高信頼 IT システムへの、及びそれからのすべての接続、並びに TSF の分割された部分間のすべての接続は、送信されるデータの完全性及び機密性を保証し、通信エンドポイントの真正性を保証するために、TOE 環境内で物理的または論理的に保護される。 *適用上の注釈：　TOE が分割された部分から構成され TOE がこれらの部分間で通過中の TSF データの保護を保証するメカニズムを実装する場合、ST 作成者は*

	FPT_ITT.1 を主張して A.CONNECT を補完または置換することを考慮してもよい。

5　セキュリティ対策方針

本セクションでは、TOE 及びその支援環境のセキュリティ対策方針を識別する。

これらのセキュリティ対策方針は、セキュリティ課題定義 (SPD) を満たす上での TOE 及びその環境の責任を識別する。

5.1　TOE セキュリティ対策方針

表 4：TOE セキュリティ対策方針

対策方針の名称	対策方針の定義
O.ACCESS_HISTORY	TOE は、過去のセション確立試行に関連する情報を保存し、その情報を利用者が利用できるようにする。
O.ADMIN_ROLE	TOE は、管理特権を利用したアクションが制限され得るようなメカニズム (例、「役割」) を提供する。
O.AUDIT_GENERATION	TSF は、定義済みセキュリティ関連事象 (これには通常、TOE の利用者のセキュリティに関して重要なアクションが含まれる) を記録できなければならない。セキュリティ関連事象に関して記録される情報には、発生した事象の時刻及び日付、及び可能であればその事象を引き起こした利用者の識別情報が含まれなければならず、またセキュリティ侵害の試行または IT 資産が危殆化の危険にさらされるような TOE セキュリティ機能の誤設定の可能性を許可された利用者が検出するために役立つほど十分に詳細なものでなければならない。
O.DISCRETIONARY_ACCESS	TSF は、オブジェクト、サブジェクト、または利用者の識別情報に基づいて、サブジェクト及び／または利用者の、名前付きリソースへのアクセスを制御しなければならない。TSF は、そのアクセスモードでどの利用者／サブジェクトに特定の名前付きオブジェクトへのアクセスが許可されるかを許可された利用者が各アクセスモードにおいて指定できるようにしなければならない。
O.I&A	TOE は、認証を必要とする任意のアクションを TOE が処理する前に、利用者が認証されることを保証する。
O.MANAGE	TSF は、TOE セキュリティメカニズムの管理に責任を持つ許可された利用者をサポートするために必要なすべての機能及びファシリティを提供しなければならず、そのような管理アクションが専門の利用者に限定されることを可能としなければならず、またそのような許可された利用者のみが管理機能にアクセスできることを保証しなければならない。
O.MEDIATE	TOE は、そのセキュリティ方針に従って利用者データを保護しなければならず、またそのようなデータへアクセスするすべての要求を仲介しなければならない。

対策方針の名称	対策方針の定義
O.RESIDUAL_INFORMATION	TOE は、その制御範囲内の保護された資源に含まれる任意の情報が、その資源の再割当て時に不適切に暴露されないことを保証すること。
O.TOE_ACCESS	TOE は、利用者データへの、及び TSF への利用者の論理的なアクセス [2]を制御する機能を提供すること。

[2] ここで、「論理的なアクセス」が特定されているのは、「物理的なアクセス」の制御が本 PP の適用範囲外であるためである。

5.2　運用環境のセキュリティ対策方針

表 5：運用環境のセキュリティ対策方針

対策方針の名称	定義
OE.ADMIN	TOE の責任者は適格かつ信用のおける個人であり、TOE 及びそれに含まれる情報のセキュリティの管理が可能であること。
OE.INFO_PROTECT	TOE の責任者は、情報が適切な方法で保護されることを保証する手続きを確立し、実施しなければならない。特に： ・ すべてのネットワーク及び周辺機器のケーブリングは、そのリンクを介して送信される最も機微なデータの送信が許可されたものでなければならない。そのような物理リンクは、適切な物理的及び論理的保護手法を用いて送信されるデータの機密性及び完全性への脅威に対して十分に保護されることが前提となる。 ・ セキュリティ関連ファイル (監査証跡や権限データベース等) に関する DAC 保護は、常に正しく設定されなければならない。 ・ 利用者は、TOE によって管理されるデータの一部へアクセスする権限を持ち、また彼ら自身のデータに関する制御を行使するよう教育される。
OE.NO_GENERAL_PURPOSE	DBMS の動作、管理、及びサポートに必要なサービス以外に、DBMS 上で利用可能な汎用コンピューティング機能 (例、コンパイラやユーザアプリケーション) が存在しないこと。
OE.PHYSICAL	TOE の責任者は、セキュリティ方針の実施に重要な TOE の部分が、IT セキュリティ対策方針を危殆化させる可能性のある物理的攻撃から保護されることを保証しなければならない。その保護は、TOE によって保護される IT 資産の価値に見合ったものでなければならない。

表 6：運用環境の IT セキュリティ対策方針

対策方針の名称	定義
OE.IT_I&A	環境において信頼されたエンティティによって提供され TOE によって利用者認証及び許可をサポートするために用いられる任意の情報は、正確で最新のものである。
OE.IT_REMOTE	TOE がリモート高信頼 IT システムに依存してその方針の実施を支援している場合、その機能及び TOE が方針決定を行うにあたって利用する任意のデータを TOE の要求によって提供するシステムは、それらの機能に間違った結果の提供を引き起こす可能性のある任意の攻撃から十分に保護される。
OE.IT_TRUSTED_SYSTEM	リモート高信頼 IT システムは、TSF によって要求されるプロトコル及びメカニズムを実装してセキュリティ方針の実施をサポートする。 これらのリモート高信頼 IT システムは、TOE へ適用されるものと同一の規則及び方針に基づいた、既知の、受容された、及び信頼された方針に従って管理され、また TOE と同等に物理的及び論理的に保護される。

6　拡張セキュリティ機能要件

FTA_TAH_(EXT).1 TOE アクセス情報

FTA_TAH_(EXT).1 TOE アクセス情報は、TOE がセション確立試行に関連する利用可能な情報を作成するための要件を提供する。

コンポーネントのレベル付け

FTA_TAH_(EXT).1 は、その他のいかなるコンポーネントとも階層関係にない。

管理：FTA_TAH_(EXT).1

予見される管理アクティビティは存在しない。

監査：FTA_TAH_(EXT).1

予見される監査対象事象は存在しない。

FTA_TAH_(EXT).1 TOE アクセス情報

下位階層：　他のコンポーネントなし。

依存性：　依存性なし。

FTA_TAH_(EXT).1.1

セション確立の試行時、TSF は、以下の情報を保存しなければならない

a.　利用者のセション確立の試行 [日付及び時刻]。

b.　連続した不成功なセション確立の試みの累積数。

FTA_TAH_(EXT).1.2

セション確立の成功時、TSF は、以下の [日付及び時刻]

a.　最後に成功したセション確立、及び

b.　最後の不成功なセション確立の試み、及び最後に成功したセション確立以後の不成功な試みの数

が利用者によって取り出されることを可能にしなければならない。

FIA_USB_(EXT).2 高度な利用者-サブジェクト結合

FIA_USB_(EXT).2 は FIA_USB.1 と似ているが、利用者セキュリティ属性以外にサブジェクトのセキュリティ属性もまた TSF データから導出されるという規則が規定される可能性が追加されている点が異なる。

コンポーネントのレベル付け

FIA_USB_(EXT).2 は、FIA_USB.1 と階層関係にある。

管理

[CC] (訳注：[REF 1b]) の FIA_USB.1 に関して規定された管理記述を参照されたい。

監査

[CC] (訳注：[REF 1b]) の FIA_USB.1 に関して規定された監査記述を参照されたい。

FIA_USB_(EXT).2 高度な利用者-サブジェクト束縛

下位階層：　FIA_USB.1 利用者-サブジェクト結合

依存性：　FIA_ATD.1 利用者属性定義

FIA_USB_(EXT).2.1

TSF は、以下の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトと関連付けなければならない：[割付：利用者セキュリティ属性のリスト]。

FIA_USB_(EXT).2.2

TSF は、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない：[割付：属性の最初の関連付けの規則]。

FIA_USB_(EXT).2.3

TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない：[割付：属性の変更の規則]。

FIA_USB_(EXT).2.4

TSF は、以下の利用者セキュリティ属性から導出されないサブジェクトセキュリティ属性の割付の規則を、サブジェクトが作成される際に実施しなければならない：[割付：利用者セキュリティ属性から導出されないサブジェクトセキュリティ属性の最初の関連付けの規則]。

7　セキュリティ要件

7.1　セキュリティ機能要件

本セクションでは、TOE の機能要件を定義する。本 PP の機能要件は CC [REF 1b] のパート 2 から直接引用されたものであるか、または CC パート 2 に基づいたものであり、拡張コンポーネントの利用を含む。これらの要件は、TOE のセキュアな運用をサポートすることに関連している。

表 7：セキュリティ機能要件

機能コンポーネント	
FAU_GEN.1	監査データ生成
FAU_GEN.2	利用者識別情報の関連付け
FAU_SEL.1	選択的監査
FDP_ACC.1	サブセットアクセス制御
FDP_ACF.1	セキュリティ属性によるアクセス制御
FDP_RIP.1	サブセット残存情報保護
FIA_ATD.1	利用者属性定義
FIA_UAU.1	認証のタイミング
FIA_UID.1	識別のタイミング
FIA_USB_(EXT).2	高度な利用者・サブジェクト結合
FMT_MOF.1	セキュリティ機能のふるまいの管理
FMT_MSA.1	セキュリティ属性の管理
FMT_MSA.3	静的属性初期化
FMT_MTD.1	TSF データの管理
FMT_REV.1(1)	取消し (利用者属性)
FMT_REV.1(2)	取消し (サブジェクト、オブジェクト属性)
FMT_SMF.1	管理機能の特定
FMT_SMR.1	セキュリティの役割
FPT_TRC.1	TSF 内一貫性
FTA_MCS.1	複数同時セションの基本制限
FTA_TAH_(EXT).1	TOE アクセス履歴
FTA_TSE.1	TOE セション確立

7.1.1　セキュリティ監査 (FAU)

7.1.1.1　FAU_GEN.1 監査データ生成

FAU_GEN.1.1

TSF は、以下の監査対象事象の監査記録を生成できなければならない：

a) 監査機能の開始と終了；

b) 表 8：監査対象事象に列挙される監査の*最小*レベルのすべての監査対象事象；及び

c) [DBMS の開始と終了；

d) 特別な許可の使用 (例、アクセス制御方針を迂回するために許可された管理者によってしばしば用いられるもの)；及び

e) [選択：[割付：ST 作成者によって決定される追加の SFR を含めることによって導入される最小レベルの監査の事象]、[割付：ST 作成者によって決定される拡張要件を含めることによって導入される最小レベルの監査に対応した事象]、「追加の事象なし」]]。

適用上の注釈：　選択について、ST 作成者は、割付の 1 つまたは両方を選ぶか (以下のパラグラフに詳述されるように)、「追加の事象なし」を選択すべきである。

適用上の注釈：　最初の割付について、ST 作成者は、本 PP に含まれないものを ST 作成者が含めるような、任意の SFR についての最小レベルの監査に関連する監査事象を表に追加する (または明示的に列挙する)。

適用上の注釈：　同様に、ST 作成者が本 PP に含まれない拡張要件を含める場合、対応する監査事象が 2 番目の割付に追加されなければならない。「最小の」監査は、このような要件について定義されていないため、ST 作成者は同様な要件の最小レベルで取り込まれた情報のタイプに対応する一連の事象を決定する必要があるだろう。

適用上の注釈：　追加の (CC または拡張) SFR が一切含まれない場合、またはそれらに関連する「最小の」監査を持たないような追加の SFR が含まれる場合、本項目に「追加の事象なし」を割り付けることは受容可能である。

FAU_GEN.1.2

TSF は、各監査記録において少なくとも以下の情報を記録しなければならない：

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報 (該当する場合)、事象の結果 (成功または失敗)；及び

b) 各監査事象種別に対して、PP/ST の機能コンポーネントの監査対象事象の定義に基づいた、[以下の表 8：監査対象事象の 3 列目で規定される情報]。

適用上の注釈：　下表の 3 列目、「追加の監査記録の内容」は、その記録を生成した事象の文脈においてそれが「意味を成す」場合に監査記録に含まれるべきデータを明示するために用いられる。特定の監査対象事象種別に関してその他の情報が (上記 a) に列挙されたもの以外に) 要求されない場合には、「なし」の割付が受容可能である。

表 8：監査対象事象

1 列目： セキュリティ機能要件	2 列目 監査対象事象	3 列目 追加の監査記録の内容
FAU_GEN.1	なし	なし
FAU_GEN.2	なし	なし
FAU_SEL.1	監査収集機能が動作中に生じた監査設定に対するすべての改変	その監査設定への変更を行った許可された管理者の識別情報
FDP_ACC.1	なし	なし
FDP_ACF.1	SFP によって網羅されるオブジェクトについて操作を実行するための要求の成功	操作を行うサブジェクトの識別情報
FDP_RIP.1	なし	なし
FIA_ATD.1	なし	なし
FIA_UAU.1	不成功に終わった認証メカニズムの使用	なし
FIA_UID.1	不成功に終わった利用者識別メカニズムの利用、提供された利用者識別情報を含む	なし
FIA_USB_(EXT).2	不成功に終わった利用者セキュリティ属性のサブジェクトへの結合 (例、サブジェクトの作成)	なし
FMT_MOF.1	なし	なし
FMT_MSA.1	なし	なし
FMT_MSA.3	なし	なし
FMT_MTD.1	なし	なし
FMT_REV.1(1)	不成功に終わったセキュリティ属性の失効	セキュリティ属性の失効を試行した個人の識別情報

1 列目： **セキュリティ機能要件**	**2 列目** **監査対象事象**	**3 列目** **追加の監査記録の内容**
FMT_REV.1(2)	不成功に終わったセキュリティ属性の失効	セキュリティ属性の失効を試行した個人の識別情報
FMT_SMF.1	管理機能の使用	これらの機能を実行する管理者の識別情報
FMT_SMR.1	役割の一部である利用者のグループへの改変	役割定義を改変する許可された管理者の識別情報
FPT_TRC.1	一貫性の復元	なし
FTA_MCS.1	複数同時セションの制限による新規セションの拒否	なし
FTA_TAH_(EXT).1	なし	なし
FTA_TSE.1	セション確立メカニズムによるセション確立の拒否	セション確立を試行する個人の識別情報

7.1.1.2　FAU_GEN.2 利用者識別情報の関連付け

FAU_GEN.2.1

識別された利用者**及び任意の識別されたグループ**のアクションがもたらした監査事象に対し、TSF は、各監査対象事象を、その原因となった**[選択：**「利用者」、「利用者**及びグループ**」] の識別情報に関連付けられなければならない。

7.1.1.3　FAU_SEL.1 選択的監査

FAU_SEL.1.1

TSF は、以下のような属性に基づいて、すべての監査対象事象のセットから監査されるべき事象のセットを選択することができなければならない：

a) *オブジェクト識別情報；*

b) *利用者識別情報；*

c) [選択：「サブジェクト識別情報」、「ホスト識別情報」、**「グループ識別情報」**、**「その他の識別情報なし」**、] ;

d) *事象種別；*

e) [監査対象セキュリティ事象の成功；

f) 監査対象セキュリティ事象の失敗；及び

g)　[選択：[割付：監査の選択性の基礎となる追加属性リスト]]。]

適用上の注釈：　*「事象種別」は、ST 作成者によって定義されるべきである；その意図は、監査事象のクラスを含めたり除外したりできるようにすることである。*

適用上の注釈：　*本要件の意図は、必ずしも必要とされる監査データのみを取り込むことでなく、管理者が彼らの任務を遂行できるように十分な監査データを取り込むことである。別の言い方をすれば、任意の所与の時点で DBMS は必ずしもすべての属性に基づいて監査対象事象を含めたり除外したりする必要はない。*

7.1.2　利用者データ保護 (FDP)

7.1.2.1　FDP_ACC.1 サブセットアクセス制御

FDP_ACC.1.1

TSF は、[すべてのサブジェクト、すべての DBMS 制御下オブジェクト、及びそれらの間のすべての操作] 上のオブジェクトに対して [任意アクセス制御方針] を実施しなければならない。

7.1.2.2　FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACF.1.1

TSF は、以下の[割付：示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ]に基づいて、オブジェクトに対して [任意アクセス制御方針] を実施しなければならない。

適用上の注釈： *DBMS 制御下オブジェクトは、DBMS への利用者インタフェースにおいて許可された利用者へ提示される実装特有オブジェクトであるかもしれない。それらは、テーブル、レコード、ファイル、インデックス、ビュー、制限、保存されたクエリ、及びメタデータが含まれるかもしれないが、これらに限定されない。DBMS 利用者インタフェースにおいて許可された利用者に提示されないが内部的に利用されるデータ構造は、内部的 TSF データ構造である。内部的 TSF データ構造は、FDP_ACF.1 で規定される規則に従って制御されない。*

FDP_ACF.1.2

TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうかを決定するために、次の規則を実施しなければならない：**[**割付：制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則**]**。

FDP_ACF.1.3

TSF は、次の追加規則、**[**割付：セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則**]**に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。

FDP_ACF.1.4

TSF は、次の追加規則、**[**割付：セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則**]**に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

7.1.2.3　FDP_RIP.1 サブセット残存情報保護

FDP_RIP.1.1

TSF は、[割付：オブジェクトのリスト]のオブジェクトへの*資源の割当*において、資源の以前のどの情報の内容も利用できなくすることを保証しなければならない。

7.1.3　識別と認証 (FIA)

適用上の注釈：　識別と認証ファミリは、I&A サービスが TOE それ自体によって行われる場合と、TOE 環境内で行われる場合の両方に SFR が利用され得るように書かれていることに、ST 作成者は注意されたい。

7.1.3.1　FIA_ATD.1 利用者属性定義

FIA_ATD.1.1

TSF は、個々の利用者に属する以下のセキュリティ属性のリストを維持しなければならない：

a)　[データベース利用者の識別子及び任意の関連するグループ資格；

b)　セキュリティ関連のデータベース役割；及び

c)　[割付：セキュリティ属性のリスト]]。

適用上の注釈：　本要件の意図は、アクセスを決定するために TOE が利用する TOE セキュリティ属性を規定することである。これらの属性は、環境によって、または TOE そのものによって、管理されてもよい。

7.1.3.2　FIA_UAU.1 認証のタイミング

FIA_UAU.1.1

TSF は、利用者が認証される前に利用者を代行して行われる**[**割付：***TSF*** 仲介アクションのリスト**]**を許可しなければならない。

FIA_UAU.1.2

TSF は、その利用者を代行する他の **TSF** 仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

7.1.3.3　FIA_UID.1 識別のタイミング

FIA_UID.1.1

TSF は、利用者が識別される前に利用者を代行して実行される**[**割付：***TSF*** 仲介アクションのリスト**]**を許可しなければならない。

FIA_UID.1.2

TSF は、その利用者を代行する他の **TSF** 仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

7.1.3.4　FIA_USB_(EXT).2 強化された利用者-サブジェクト結合

FIA_USB_(EXT).2.1

TSF は、以下の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない：[割付：利用者セキュリティ属性のリスト]。

FIA_USB_(EXT).2.2

TSF は、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない：[割付：属性の最初の関連付けの規則]。

FIA_USB_(EXT).2.3

TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない： [割付：属性の変更の規則]。

FIA_USB_(EXT).2.4

TSF は、以下の利用者セキュリティ属性から導出されないサブジェクトセキュリティ属性の割付の規則を、サブジェクトが作成される際に実施しなければならない： [割付 : 利用者セキュリティ属性から導出されないサブジェクトセキュリティ属性の最初の関連付けの規則]。

7.1.4　セキュリティ管理 (FMT)

7.1.4.1　FMT_MOF.1 セキュリティ機能のふるまいの管理

FMT_MOF.1.1

TSF は、 [監査されるべき事象の特定に関連する]機能を*無効化及び有効化*する能力を[許可された管理者] に制限しなければならない。

7.1.4.2　FMT_MSA.1 セキュリティ属性の管理

FMT_MSA.1.1

TSF は、 [すべての] セキュリティ属性に対し*管理*する能力を[許可された管理者] に制限する [任意アクセス制御方針] を実施しなければならない。

適用上の注釈： *ST 作成者は、FIA_ATD.1 で規定されるすべての属性が十分に管理され保護されることを保証すべきである。*

7.1.4.3　FMT_MSA.3 静的属性初期化

FMT_MSA.3.1

TSF は、その SFP を実施するために使われるセキュリティ属性に対して*制限的な*デフォルト値を与える [任意アクセス制御方針] を実施しなければならない。

適用上の注釈： *本要件は、トップレベルの新規コンテナオブジェクト (例、テーブル) に適用される。より低レベルのオブジェクトが作成されるとき (例、列、セル)、これらはデフォルトでトップレベルオブジェクトのアクセス権限を継承するかもしれない。別の言い方をすれば、「子」オブジェクトのアクセス権限は、デフォルトで「親」オブジェクトのアクセス権限を取ってもよい。*

FMT_MSA.3.2

TSF は、オブジェクトや情報が生成されるとき、[一切の利用者が]デフォルト値を上書きする代替の初期値を規定 [しない] ことを許可しなければならない。

7.1.4.4　FMT_MTD.1 TSF データの管理

FMT_MTD.1.1

TSF は、 [監査対象事象] を*含めたり除外したり*する能力を [許可された管理者] に制限しなければならない。

7.1.4.5　FMT_REV.1(1) 取消し

FMT_REV.1.1(1)

TSF は、TSF の制御下で、*利用者*に関連した[割付：セキュリティ属性のリスト] を取り消す能力を、 [許可された管理者] に制限しなければならない。

FMT_REV.1.2(1)

TSF は、 規則**[**割付：取消し規則の詳述**]**を実施しなければならない。

7.1.4.6　FMT_REV.1(2) 取消し

FMT_REV.1.1(2)

TSF は、TSF の制御下で、*オブジェクト*に関連した [割付：セキュリティ属性のリスト] を取り消す能力を、 [許可された管理者] **及び任意アクセス制御方針によって許可される十分な特権を有するデータベース利用者**に制限しなければならない。

FMT_REV.1.2(2)

TSF は、規則**[**割付**:**取消し規則の詳述**]**を実施しなければならない。

7.1.4.7　FMT_SMF.1 管理機能の特定

FMT_SMF.1.1

TSF は、以下の管理機能を実行することができなければならない**:[**割付**:*TSF* **に**よって提供される管理機能のリスト**]**。

7.1.4.8　FMT_SMR.1 セキュリティの役割

FMT_SMR.1.1

TSF は、役割 [許可された管理者及び[割付：追加の許可された識別された役割]] を維持しなければならない。]

FMT_SMR.1.2

TSF は、利用者を役割に関連付けなければならない。

適用上の注釈：　*本要件は、管理者役割の最小セットを識別する。ST または運用環境には、ここで識別された役割に対応する、よりきめ細かく分類された役割が含まれるかもしれない (例、データベースの非管理者利用者またはデータベースオペレータ)。ST 作成者は、上記の識別された役割の名称を変更してもよいが、その「新しい」役割は依然として本 PP の FMT 要件で定義された機能を実行しなければならない。*

7.1.5　TOE セキュリティ機能の保護 (FPT)

適用上の注釈：　最初のエレメントのセキュリティドメイン境界は TSF ドメインであり、その意図はTSFI に存在する信頼できないサブジェクトから TSF を保護することである。2 番目のエレメントのセキュリティドメイン境界は完全な TOE 制御範囲をカバーし、その意図は TOE 制御範囲の任意のサブジェクト間の分離を維持することである。

7.1.5.1　FPT_TRC.1 TSF 内一貫性

FPT_TRC.1.1

TSF は、**TOE** のパート間で複製される場合、**TSF** データが一貫していることを保証しなければならない。

FPT_TRC.1.2

複製された **TSF** データを含む **TOE** のパートが切り離される場合、**TSF** は、再接続で**[**割付**:** ***TSF*** データ複製の一貫性に依存する機能のリスト**]**に対するいかなる要求についてもそれを処理する前に、複製された **TSF** データの一貫性を保証しなければならない。

適用上の注釈：　本要件は、TOE に物理的に分離したコンポーネントが含まれない場合、自明に満たされる。適用上の注釈：一般的に言って、TOE のリモート部分に分散された TSF データの完全な一貫性を達成することは不可能である。TSF の分散された部分が異なる時間に活性化したり、互いに切断されたりするかもしれないからである。本要件は、TSF データの不一致が存在しても過度の遅延なく修正されることを認めることによって、現実的な方法でこの状況に対応しようとするものである。例えば、複製された TSF データを維持管理するすべての TSF ノードに対して TSF データの周期的なブロードキャストを行うことによって、TSF はタイムリーな一貫性を提供できるかもしれない。別のアプローチの例として、TSF がリモート TSF ノードの不一致を明示的に探るメカニズムを提供し、識別された不一致を修正するためのアクションで応答することが考えられる。

7.1.6　TOE アクセス (FTA)

7.1.6.1　FTA_MCS.1 複数同時セションの基本制限

FTA_MCS.1.1

TSF は、同一利用者に属する同時セションの最大数を制限しなければならない。

FTA_MCS.1.2

TSF は、デフォルトで、利用者あたり[割付 : デフォルト数] セションの制限を実施しなければならない。

適用上の注釈：　ST 作成者は、CC [REF 1b] パラグラフ 473 で FMT 中の管理機能としてデフォルト数の定義が許可されていることに留意されたい。

7.1.6.2　FTA_TAH_(EXT).1 TOE アクセス情報

FTA_TAH_(EXT).1.1

セション確立の試行時、TSF は、以下の情報を保存しなければならない。

a. 利用者のセション確立の試行の [日付及び時刻]。

b. 連続した不成功なセション確立の試みの累積数。

FTA_TAH_(EXT).1.2

セション確立の成功時、TSF は、以下の [日付及び時刻]

a. 最後に成功したセション確立、及び

b. 最後の不成功なセション確立の試み、及び最後に成功したセション確立以後の不成功な試みの数

が利用者によって取り出せることを可能にしなければならない。

7.1.6.3　FTA_TSE.1 TOE セション確立

FTA_TSE.1.1

TSF は、 [利用者識別情報、時刻、曜日を含め、許可された管理者によって明示的に設定可能な属性]、及び[選択：グループ識別情報、[割付：追加の属性リスト]] に基づきセションの確立を拒否できなければならない。

7.2 セキュリティ保証要件

評価保証レベル (EAL) 2 に含まれるすべての保証要件及び以下の追加の保証コンポーネント：

- ALC_FLR.2：欠陥修正

以下は、本プロテクションプロファイルに必要とされる保証要件のリストである：

表 9：保証要件

保証クラス	保証コンポーネント	保証コンポーネントの記述
開発	ADV_ARC.1	セキュリティアーキテクチャ記述
	ADV_FSP.2	セキュリティ実施機能仕様
	ADV_TDS.1	基本設計
ガイダンス文書	AGD_OPE.1	利用者操作ガイダンス
	AGD_PRE.1	準備手続き
ライフサイクルサポート	ALC_CMC.2	CM システムの使用
	ALC_CMS.2	TOE の一部の CM 範囲
	ALC_DEL.1	配付手続き
	ALC_FLR.2	欠陥報告手続き
テスト	ATE_COV.1	カバレージの証拠
	ATE_FUN.1	機能テスト
	ATE_IND.2	独立テスト-サンプル
脆弱性評定	AVA_VAN.2	脆弱性分析
セキュリティターゲット評価	ASE_CCL.1	適合主張
	ASE_ECD.1	拡張コンポーネント定義
	ASE_INT.1	ST 概説
	ASE_OBJ.2	セキュリティ対策方針
	ASE_REQ.2	派生したセキュリティ要件
	ASE_SPD.1	セキュリティ課題定義
	ASE_TSS.1	TOE 要約仕様

8　根拠

本セクションでは、IT セキュリティ要件、対策方針、前提条件、及び脅威の選択の根拠を提供する。特に、IT セキュリティ要件がセキュリティ対策方針を満たすために適切であることを示し、またセキュリティ対策方針が TOE セキュリティ環境のすべての側面をカバーするために適切であることが示される。

8.1　TOE セキュリティ対策方針の根拠

以下の表は、脅威、方針、及び前提条件によって定義される環境に対するセキュリティ対策方針の対応付けを提供し、それぞれのセキュリティ対策方針が少なくとも 1 つの脅威、前提条件または方針をカバーすること、及びそれぞれの脅威、前提条件、または方針が少なくとも 1 つのセキュリティ対策方針によってカバーされることを説明するものである。

8.1.1　TOE セキュリティ対策方針のカバレージ

以下の表は、TOE セキュリティ対策方針に関連した方針、及び脅威の要約を示すものである。

表 10：TOE セキュリティ対策方針のカバレージ

対策方針の名称	SPD カバレージ
O.ACCESS_HISTORY	T.TSF_COMPROMISE T.ACCESS_TSFDATA T.IA_MASQUERADE
O.ADMIN_ROLE	P.ACCOUNTABILITY P.ROLES T.ACCESS_TSFFUNC
O.AUDIT_GENERATION	P.ACCOUNTABILITY T.TSF_COMPROMISE
O.DISCRETIONARY_ACCESS	T.IA_USER T.UNAUTHORIZED_ACCESS
O.I&A	P.ACCOUNTABILITY T.ACCESS_TSFFUNC T.ACCESS_TSFDATA T.IA_MASQUERADE T.IA_USER
O.MANAGE	P.USER T.ACCESS_TSFDATA T.ACCESS_TSFFUNC T.UNAUTHORIZED_ACCESS
O.MEDIATE	T.IA_MASQUERADE T.UNAUTHORIZED_ACCESS T.IA_USER
O.RESIDUAL_INFORMATION	T.ACCESS_TSFDATA T.ACCESS_TSFFUNC T.RESIDUAL_DATA
O.TOE_ACCESS	P.ACCOUNTABILITY P.ROLES P.USER T.ACCESS_TSFDATA T.ACCESS_TSFFUNC T.IA_USER T.IA_MASQUERADE T.TSF_COMPROMISE

8.1.2　TOE セキュリティ対策方針の根拠

以下の表は、TOE セキュリティ対策方針の根拠を示すものである。

表 11：TOE セキュリティ対策方針の根拠

脅威／方針	脅威／方針に対処する TOE セキュリティ対策方針	根拠
P.ACCOUNTABILITY TOE の許可された利用者は、TOE 内での自分のアクションに説明責任を負わなければならない。	O.ADMIN_ROLE TOE は、管理者特権を用いるアクションが制限できるメカニズム (例、「役割」) を提供する。	O.ADMIN_ROLE セキュアな管理に必要とされる特権を許可された管理者に提供する対策方針を TOE が有することを保証することによって、この方針をサポートする。
	O.AUDIT_GENERATION TOE は、利用者と関連付けられたセキュリティ関連事象を検出し記録を作成する能力を提供すること。	O.AUDIT_GENERATION 監査記録が生成されることを保証することによって、この方針をサポートする。これらの記録を利用可能とすることによって、責任追跡性が可能となる。
	O.I&A TOE は、認証を必要とする任意のアクションを TOE が処理する前に、利用者が認証されることを保証する。	O.I&A 認証された利用者のみに提供するために TOE が定義された任意のアクションを許可する前に、TOE と対話する各エンティティが適切に識別され認証されることを要求することによって、この方針をサポートする。
	O.TOE_ACCESS TOE は、利用者データ及び TSF への利用者の論理的アクセスを制御するメカニズムを提供する。	O.TOE_ACCESS アクセスを制御するメカニズムを許可された利用者へ提供することによって、この方針をサポートする。

脅威／方針	脅威／方針に対応する TOE セキュリティ対策方針	根拠
P.USER 権限は、そのアクションを正しく実行すると信頼される利用者のみへ与えられなければならない。	O.MANAGE TSF は、TOE セキュリティメカニズムの管理に責任を持つ許可された利用者をサポートするために必要なすべての機能及びファシリティを提供しなければならず、そのような管理者アクションが専門の利用者に限定されることを可能としなければならず、またそのような許可された利用者のみが管理機能にアクセスできることを保証しなければならない。	O.MANAGE 許可された管理者役割をサポートする機能及びファシリティが用意されていることを保証することによって、この方針をサポートする。
	O.TOE_ACCESS TOE は、利用者データ及び TSF への利用者の論理的アクセスを制御するメカニズムを提供すること。	O.TOE_ACCESS 許可された利用者に対してアクセス制御のメカニズムを提供することによって、この方針をサポートする。
	OE.ADMIN TOE の責任者は、力量がありかつ信用のおける個人であり、TOE 及びそれに含まれる情報のセキュリティの管理が可能であること。	OE.ADMIN 許可された管理者役割が力量のある管理者によって理解され使用されることを保証することによって、この方針をサポートする。

脅威／方針	脅威／方針に対応する TOE セキュリティ対策方針	根拠
P.ROLES TSF 機能への管理者権限は、信頼される要員へ与えられ、その人物が有する管理職務のみをサポートするよう、なるべく制限されなければならない。この役割は、他の許可された利用者とは分離された別個のものでなければならない。	O.ADMIN_ROLE TOE は、管理特権を利用したアクションが制限され得るようなメカニズム (例、「役割」) を提供する。	O.ADMIN_ROLE TOE は、セキュアな管理のために許可された管理者を提供するという対策方針を有する。TOE は他の役割もまた提供してよいが、許可された管理者の役割のみが要求される。
	O.TOE_ACCESS TOE は、利用者データ及び TSF への利用者の論理的アクセスを制御するメカニズムを提供すること。	O.TOE_ACCESS 許可された管理者役割が他の許可された利用者から区別できることを保証することによって、この方針をサポートする。

脅威／方針	脅威／方針に対応する **TOE セキュリティ対策方針**	根拠
T.ACCESS_TSFDATA 脅威エージェントが、適切な許可なしに TOE の機能を利用して TSF データを読み出したり改変したりするかもしれない。	O.ACCESS_HISTORY TOE は、過去のセション確立試行に関連する情報を保存し、その情報を利用者が利用できるようにする。	O.ACCESS_HISTORY 利用者に過去の認証試行を通知するために必要な情報を TOE が保存することを保証し、またこの情報の検索を可能とするため、この脅威を低減する。
	O.I&A TOE は、認証を必要とする任意のアクションを TOE が処理する前に、利用者が認証されることを保証する。	O.I&A 認証された利用者のみに提供するため TOE に定義された任意のアクションを許可する前に TOE と対話する各エンティティが適切に識別され認証されることを要求することによって、この方針をサポートする。
	O.MANAGE TSF は、TOE セキュリティメカニズムの管理に責任を持つ許可された利用者をサポートするために必要なすべての機能及びファシリティを提供しなければならず、そのような管理アクションが専門の利用者に限定されることを可能としなければならず、またそのような許可された利用者のみが管理機能にアクセスできることを保証しなければならない。	O.MANAGE TSF データを改変するために用いられる機能及びファシリティが許可されない利用者に利用できないことを保証するため、この脅威を低減する。
	O.RESIDUAL_INFORMATION TOE は、その制御範囲内の保護された資源に含まれる任意の情報が、その資源の再割当て時に不適切に暴露されないことを保証すること。	O.RESIDUAL_INFORMATION 保護された資源に含まれる情報が再割当て攻撃によって簡単には脅威エージェントに利用できるようにならないため、この脅威を低減する。
	O.TOE_ACCESS TOE は、利用者データ及び TSF への利用者の論理的アクセスを制御するメカニズムを提供すること。	O.TOE_ACCESS 脅威エージェントが TOE へアクセスする可能性をより低くするため、この脅威を低減する。

脅威／方針	脅威／方針に対処する TOE セキュリティ対策方針	根拠
T.ACCESS_TSFFUNC 脅威エージェントが、TSF の保護メカニズムをバイパスして TSF を利用したり管理したりするかもしれない。	O.ADMIN_ROLE TOE は、管理特権を利用したアクションが制限され得るようなメカニズム (例、「役割」) を提供する。	O.ADMIN_ROLE 特権アクションの分離を提供することによって、この脅威を低減する。
	O.I&A TOE は、認証を必要とする任意のアクションを TOE が処理する前に、利用者が認証されることを保証する。	O.I&A 任意のアクセス制御された内容へのアクセスを得る前に TOE への認証が成功することを TOE が要求するため、この脅威を低減する。これらのサービスへのアクセスを得るための強力な認証を実装することにより、攻撃者がデータまたは TOE 資源への許可されないアクセスを得るために別のエンティティになりすます機会は低減される。
	O.MANAGE TSF は、TOE セキュリティメカニズムの管理に責任を持つ許可された利用者をサポートするために必要なすべての機能及びファシリティを提供しなければならず、そのような管理アクションが専門の利用者に限定されることを可能としなければならず、またそのような許可された利用者のみが管理機能にアクセスできることを保証しなければならない。	O.MANAGE TSF データへのアクセスを制御するためにアクセス制御方針が規定されるため、この脅威を低減する。この対策方針は、誰が TSF データを閲覧し改変できるのかと共に、TSF 機能のふるまいをも規定するために用いられる。
	O.RESIDUAL_INFORMATION TOE は、その制御範囲内の保護された資源に含まれる任意の情報が、その資源の再割当て時に不適切に暴露されないことを保証すること。	O.RESIDUAL_INFORMATION 資源がある利用者／プロセスによって解放され別の利用者／プロセスに割り当てられたとき、TSF データ及び利用者データが残存しないことを保証することによって、この脅威を低減する。
	O.TOE_ACCESS TOE は、利用者データ及び TSF への利用者の論理的アクセスを制御するメカニズムを提供すること。	O.TOE_ACCESS 脅威エージェントが TOE へアクセスする可能性をより低くするため、この脅威を低減する。

脅威／方針	脅威／方針に対応する TOE セキュリティ対策方針	根拠
T.IA_MASQUERADE 利用者または利用者を代行して動作するプロセスが、利用者データ、TSF データ、または TOE 資源への許可されないアクセスを得るために許可されたエンティティに成りすますかもしれない	O.ACCESS_HISTORY TOE は、過去のセション確立試行に関連する情報を保存し、その情報を利用者が利用できるようにする。	O.ACCESS_HISTORY 利用者に最後の成功したログイン試行及び彼らが知ることなく行われたアクションについて通知する情報を TOE が保存し検索できることを保証するため、この脅威を低減する。
	O.I&A TOE は、認証を必要とする任意のアクションを TOE が処理する前に、利用者が認証されることを保証する。	O.I&A 認証された利用者のみに提供するために TOE に定義された任意のアクションを許可する前に TOE と対話する各エンティティが適切に識別され認証されることを要求することによって、この脅威を低減する。
	O.MEDIATE TOE は、そのセキュリティ方針に従って利用者データを保護しなければならず、またそのようなデータへアクセスするすべての要求を仲介しなければならない。	O.MEDIATE 利用者データへのすべてのアクセスが仲介の対象となる (当該データが公開データと明確に識別されない限り) ことを保証することによって、この脅威を低減する。TOE は、任意のアクセス制御された内容へのアクセスを得る前に TOE への認証が成功することを要求する。これらのサービスへのアクセスを得るための強力な認証を実装することにより、攻撃者がデータまたは TOE 資源への許可されないアクセスを得るために別のエンティティになりすます機会は低減される。
	O.TOE_ACCESS TOE は、利用者データ及び TSF への利用者の論理的アクセスを制御するメカニズムを提供すること。	O.TOE_ACCESS TOE 及びその資源への論理的なアクセスを制御することによって、この脅威を低減する。許可された利用者が TOE へアクセス可能な方法及び時間を制限することによって、また認証メカニズムの種別及び強度を義務付けることによって、この対策方針は利用者がログインを試行し許可された利用者になりすます可能性を低減するために役立つ。さらに、この対策方針はアカウントがロックアウトされる前に利用者が行えるログイン試行失敗の回数を制御する手段を管理者に提供し、利用者が TOE への許可されないアクセスを得る可能性をさらに低減する。

脅威／方針	脅威／方針に対応する TOE セキュリティ対策方針	根拠
T.IA_USER 脅威エージェントは、識別及び認証されることなく、公開のオブジェクトを除き、利用者データ、TSF データまたは TOE 資源へのアクセスを得るかもしれない。	O.DISCRETIONARY_ACCESS TSF は、オブジェクト、サブジェクト、または利用者の識別情報に基づいて、サブジェクト及び／または利用者の、名前付きリソースへのアクセスを制御しなければならない。TSF は、そのアクセスモードでどの利用者／サブジェクトに特定の名前付きオブジェクトへのアクセスが許可されるかを許可された利用者が各アクセスモードにおいて指定できるようにしなければならない。	O.DISCRETIONARY_ACCESS TOE と共に保存される利用者データを含め、データに任意アクセス制御による保護が提供されることを要求することによって、この脅威を低減する。
	O.I&A TOE は、認証を必要とする任意のアクションを TOE が処理する前に、利用者が認証されることを保証する。	O.I&A 認証された利用者にのみ提供するため TOE に定義された任意のアクションを許可する前に TOE と対話する各エンティティが適切に識別され認証されることを要求することによって、この脅威を低減する。
	O.MEDIATE TOE は、そのセキュリティ方針に従って利用者データを保護しなければならず、またそのようなデータへアクセスするすべての要求を仲介しなければならない。	O.MEDIATE 利用者データへのすべてのアクセスが仲介の対象となる (当該データが公開データと明確に識別されない限り) ことを保証することによって、この脅威を低減する。TOE は、任意のアクセス制御された内容へのアクセスを得る前に TOE への認証が成功することを要求する。これらのサービスへのアクセスを得るための強力な認証を実装することにより、攻撃者がデータまたは TOE 資源への許可されないアクセスを得るために別のエンティティになりすます機会は低減される。
	O.TOE_ACCESS TOE は、利用者データ及び TSF への利用者の論理的アクセスを制御するメカニズムを提供すること。	O.TOE_ACCESS 利用者データ、TSF データまたは TOE 資源への論理的なアクセスを制御することによって、この脅威を低減する。

脅威／方針	脅威／方針に対応する **TOE セキュリティ対策方針**	根拠
T.RESIDUAL_DATA 利用者または利用者を代行して動作するプロセスが、ある利用者またはプロセスから別のものへの TOE 資源の再割当てを通して、利用者または TSF データへの許可されないアクセスを得るかもしれない。	O.RESIDUAL_INFORMATION TOE は、その制御範囲内の保護された資源に含まれる任意の情報が、その資源の再割当て時に不適切に暴露されないことを保証すること。	O.RESIDUAL_INFORMATION この脅威を低減する。セキュリティメカニズムによって利用者が TSF の閲覧が許可されない場合であっても、もし TSF データが利用者に利用可能な資源に不適切にも存在するようなことがあれば、認証なしにその利用者が TSF を閲覧できてしまうためである。

脅威／方針	脅威／方針に対応する TOE セキュリティ対策方針	根拠
T.TSF_COMPROMISE 利用者または利用者に代わって作用するプロセスが、設定データの不適切なアクセス (閲覧、改変または削除) を引き起こしたり、TSF 内の実行可能コードを危殆化させたりするかもしれない。	O.ACCESS_HISTORY TOE は、過去のセション確立試行に関連する情報を保存し、その情報を利用者が利用できるようにする。	O.ACCESS_HISTORY 利用者に最後の成功したログイン試行及び彼らが知ることなく行われたアクションについて通知する情報を TOE が保存し検索できることを保証するため、この脅威を低減する。
	O.AUDIT_GENERATION TOE は、利用者と関連付けられたセキュリティ関連事象を検出し記録を作成する能力を提供すること。	O.AUDIT_GENERATION TSF の危殆化の検出をサポートする適切な監査記録を管理者に提供することによって、この脅威を低減する。
	O.TOE_ACCESS TOE は、利用者データ及び TSF への利用者の論理的アクセスを制御するメカニズムを提供すること。	O.TOE_ACCESS この脅威を低減する。TOE への利用者の論理的アクセスが制御されることによって、設定データへ攻撃者がアクセスできる機会が減少するためである。

脅威／方針	脅威／方針に対応する TOE セキュリティ対策方針	根拠
T.UNAUTHORIZED_ACCESS 利用者が、TOE のセキュリティ方針に従えば権限のない利用者データへの許可されないアクセスを得るかもしれない。	O.DISCRETIONARY_ACCESS TSF は、オブジェクト、サブジェクトまたは利用者の識別情報に基づいて、サブジェクト及び／または利用者の名前付きリソースへのアクセスを制御しなければならない。TSF は、そのアクセスモードでどの利用者／サブジェクトに特定の名前付きオブジェクトへのアクセスが許可されるかを許可された利用者が各アクセスモードについて規定することを許可しなければならない。	O.DISCRETIONARY_ACCESS TOE と共に保存される TSF データを含め、データに任意アクセス制御による保護が提供されることを要求することによって、この脅威を低減する。
	O.MANAGE TSF は、TOE セキュリティメカニズムの管理に責任を持つ許可された利用者をサポートするために必要なすべての機能及びファシリティを提供しなければならず、そのような管理アクションが専門の利用者に限定されることを可能としなければならず、またそのような許可された利用者のみが管理機能にアクセスできることを保証しなければならない。	O.MANAGE 許可された管理者が許可された利用者に彼らのアクションに関して責任を課すことをサポートする機能及びファシリティが用意されていることを保証することによって、この脅威を低減する。
	O.MEDIATE TOE は、そのセキュリティ方針に従って利用者データを保護しなければならず、またそのようなデータへアクセスするすべての要求を仲介しなければならない。	O.MEDIATE 利用者データへのすべてのアクセスが仲介の対象となる (当該データが公開データと明確に識別されない限り) ことを保証するため、この脅威を低減する。TOE は、任意のアクセス制御された内容へのアクセスを得る前に TOE への認証が成功することを要求する。これらのサービスへのアクセスを得るための強力な認証を実装することにより、攻撃者が中間者攻撃及び／またはパスワード推測攻撃を成功させる機会は大幅に低減される。最後に、TSF は利用者が TOE または TOE 仲介サービスへのアクセスを許可される前に、すべての設定された強制機能 (認証、アクセス制御規則等) が起動されなければならない　ことを保証する。TOE は、アクセス制御規則に関連付けられたセキュリティ属性を改変する能力、認証されたサービスと認証されていないサービス等へのアクセスを管理者に制限する。この機能は、一切のその他の利用者が情報フロー方針を改変して意図された TOE セキュリティ方針を迂回できないことを保証する。

8.2　環境のセキュリティ対策方針の根拠

下表は、環境のセキュリティ対策方針に関連した前提条件、方針、及び脅威の要約を示すものである。

表 12：TOE 環境のセキュリティ対策方針の SPF 項目のカバレージ

対策方針の名称	SPD カバレージ
OE.ADMIN	A.MANAGE P.ACCOUNTABILITY P.ROLES P.USER
OE.INFO_PROTECT	A.AUTHUSER A.CONNECT A.MANAGE A.PHYSICAL A.TRAINEDUSER P.ACCOUNTABILITY P.USER T.TSF_COMPROMISE T.UNAUTHORIZED_ACCESS
OE.IT_I&A	A.SUPPORT
OE.IT_REMOTE	A.AUTHUSER A.CONNECT A.PEER_FUNC_&_MGT T.TSF_COMPROMISE
OE.IT_TRUSTED_SYSTEM	A.AUTHUSER A.CONNECT A.PEER_FUNC_&_MGT T.TSF_COMPROMISE
OE.NO_GENERAL_ PURPOSE	A.NO_GENERAL_PURPOSE T.IA_MASQUERADE T.TSF_COMPROMISE
OE.PHYSICAL	A.CONNECT A.PHYSICAL T.TSF_COMPROMISE

下表は、環境のセキュリティ対策方針の根拠を示すものである。

表 13：環境のセキュリティ対策方針の根拠

前提条件	前提条件に対処する環境対策方針	環境のセキュリティ対策方針を規定した根拠
A.AUTHUSER 許可された利用者は、TOE によって管理される情報の少なくとも一部へアクセスするために必要な許可を有する。	OE.INFO_PROTECT TOE の責任者は、情報が適切な方法で保護されることを保証する手続きを確立し、実施しなければならない。特に： ・ すべてのネットワーク及び周辺機器のケーブリングは、そのリンクを介して送信される最も機微なデータの送信が許可されたものでなければならない。そのような物理リンクは、適切な物理的及び論理的保護手法を用いて送信されるデータの機密性及び完全性への脅威に対して十分に保護されることが前提となる。 ・ セキュリティ関連ファイル (監査証跡や権限データベース等) に関する DAC 保護は、常に正しく設定されなければならない。 ・ 利用者は、TOE によって管理されるデータの一部へアクセスする権限を持ち、また彼ら自身のデータに関する制御を行使するよう教育される。	OE.INFO_PROTECT TOE によって管理されるデータの部分へアクセスする権限を利用者が持ち、また彼ら自身のデータへの制御を行使するよう教育されることを保証することによって、この前提条件をサポートする。 教育された、許可された利用者に、情報保護に関連する手続きが提供されていることが、共同作業の前提条件をサポートする。
	OE.IT_REMOTE TOE がリモート高信頼 IT システムに依存してその方針の実施を支援している場合、その機能及び TOE が方針決定を行うにあたって利用する任意のデータを TOE の要求によって提供するシステムは、それらの機能に間違った結果の提供を引き起こす可能性のある任意の攻撃から十分に保護される。	OE.IT_REMOTE IT 環境の一部を形成するリモートシステムが保護されることを保証することによって、この前提条件をサポートする。これによって、環境が善良なものであるという確信が得られる。
	OE.IT_TRUSTED_SYSTEM リモート高信頼 IT システムは、TSF によって要求されるプロトコル及びメカニズムを実装してセキュリティ方針の実施をサポートする。 これらのリモート高信頼 IT システムは、TOE へ適用されるものと同一の規則及び方針に基づいた、既知の、受容された、及び信頼された方針に従って管理され、また TOE と同等に物理的及び論理的に保護される。	OE.IT_TRUSTED_SYSTEM TOE の IT 環境のシステムが善良な環境に寄与するという確信を提供することによって、この前提条件をサポートする。

前提条件	前提条件に対処する環境対策方針	環境のセキュリティ対策方針を規定した根拠
A.CONNECT リモート高信頼 IT システムへの、及びそれからのすべての接続、並びに TSF の分割された部分間のすべての接続は、送信されるデータの完全性及び機密性を保証し、通信エンドポイントの真正性を保証するために、TOE 環境内で物理的または論理的に保護される。	OE.IT_REMOTE TOE がリモート高信頼 IT システムに依存してその方針の実施を支援している場合、その機能及び TOE が方針決定を行うにあたって利用する任意のデータを TOE の要求によって提供するシステムは、それらの機能に間違った結果の提供を引き起こす可能性のある任意の攻撃から十分に保護される。	OE.IT_REMOTE 高信頼システム間または TOE の物理的に分離した部分間の接続が、それらの機能に間違った結果の提供を引き起こす可能性のある任意の攻撃から十分に保護されるという要件を環境に課すことによって、前提条件をサポートする。
	OE.INFO_PROTECT TOE の責任者は、情報が適切な方法で保護されることを保証する手続きを確立し、実施しなければならない。特に： ・ すべてのネットワーク及び周辺機器のケーブリングは、そのリンクを介して送信される最も機微なデータの送信が許可されたものでなければならない。そのような物理リンクは、適切な物理的及び論理的保護手法を用いて送信されるデータの機密性及び完全性への脅威に対して十分に保護されることが前提となる。 ・ セキュリティ関連ファイル (監査証跡や認証データベース等) に関する DAC 保護は、常に正しく設定されなければならない。 ・ 利用者は、TOE によって管理されるデータの一部へアクセスする権限を持ち、また彼ら自身のデータに関する制御を行使するよう教育される。	OE.INFO_PROTECT すべてのネットワーク及び周辺機器のケーブリングがそのリンクを介して送信される最も機微なデータの送信が許可されたものでなければならないことを要求することによって、前提条件をサポートする。そのような物理リンクは、適切な物理的及び論理的保護手法を用いて送信されるデータの機密性及び完全性への脅威に対して十分に保護されることが前提となる
	OE.IT_TRUSTED_SYSTEM リモート高信頼 IT システムは、TSF によって要求されるプロトコル及びメカニズムを実装してセキュリティ方針の実施を支援する。 これらのリモート高信頼 IT システムは、TOE へ適用されるものと同一の規則及び方針に基づいた、既知の、受容された及び信頼された方針に従って管理され、また TOE と同等に物理的及び論理的に保護される。	OE.IT_TRUSTED_SYSTEM リモート高信頼 IT システムが TSF によって要求されるプロトコル及びメカニズムを実装してセキュリティ方針の実施を支援することを保証することによって、前提条件をサポートする。
	OE.PHYSICAL TOE の責任者は、セキュリティ方針の実施に重要な TOE の部分が、IT セキュリティ対策方針を危殆化させる可能性のある物理的攻撃から保護されることを保証しなければならない。その保護は、TOE によって保護される IT 資産の価値に見合ったものでなければならない。	OE.PHYSICAL ドメイン内部に適切な物理的セキュリティが提供されることを保証することによって、前提条件をサポートする。

前提条件	前提条件に対処する環境対策方針	環境のセキュリティ対策方針を規定した根拠
A.SUPPORT IT 環境における信頼されたエンティティによって提供され、TOE によって使用される、時刻と日付の設定、監査取得で使用される情報、利用者認証、及び許可をサポートするために使用される任意の情報は、正確であり、最新のものである。	OE.IT_I&A 環境における信頼されたエンティティによって提供され、TOE によって利用者認証と許可をサポートするために用いられる任意の情報は、正確であり、最新のものである。	OE.IT_I&A 前提条件を暗黙的にサポートする。

前提条件	前提条件に対処する環境対策方針	環境のセキュリティ対策方針を規定した根拠
A.MANAGE TOE のセキュリティ機能は、1 人以上の適格な管理者によって管理される。システム管理要員は不注意であったり、意図的に怠慢であったり、敵対的であったりせず、ガイダンス文書によって提供される指示を遵守する。	OE.ADMIN TOE の責任者は適格かつ信用のおける個人であり、TOE 及びそれに含まれる情報のセキュリティの管理が可能であること。	OE.ADMIN 前提条件をサポートする。許可された管理者は、すべてのタスク及び責務が効果的に行われることの保証に役立つ適任者であることが前提となっているためである。
	OE.INFO_PROTECT TOE の責任者は、情報が適切な方法で保護されることを保証する手続きを確立し、実施しなければならない。特に： ・ すべてのネットワーク及び周辺機器のケーブリングは、そのリンクを介して送信される最も機微なデータの送信が許可されたものでなければならない。そのような物理リンクは、適切な物理的及び論理的保護手法を用いて送信されるデータの機密性及び完全性への脅威に対して十分に保護されることが前提となる。 ・ セキュリティ関連ファイル (監査証跡や認証データベース等) に関する DAC 保護は、常に正しく設定されなければならない。 ・ 利用者は、TOE によって管理されるデータの一部へアクセスする権限を持ち、また彼ら自身のデータに関する制御を行使するよう教育される。	OE.INFO_PROTECT TOE の情報保護の側面並びに TOE のプラットフォームを形成する 1 つまたは複数のシステム及び関連する接続性が、本 PP に記述されたセキュリティ問題への対処に不可欠であることを保証することによって、前提条件をサポートする。 定義された手続きを用いてこれらを効果的に管理することは、適格な管理者を有することに依存する。

前提条件	前提条件に対処する環境対策方針	環境のセキュリティ対策方針を規定した根拠
A.NO_GENERAL_PURPOSE DBMS の動作、管理、及びサポートに必要なサービス以外に、DBMS 上で利用可能な汎用コンピューティングまたは記憶リポジトリ機能 (例、コンパイラやユーザアプリケーション) が存在しない。	OE.NO_GENERAL_PURPOSE DMBS の動作、管理、及びサポートに必要なサービス以外に、DBMS 上で利用可能な汎用コンピューティング機能 (例、コンパイラやユーザアプリケーション) が存在しないこと。	OE.NO_GENERAL_PURPOSE DBMS サーバには、一切の汎用コンピューティングまたは記憶機能が含まれてはならない。これによって、TSF データは悪意のあるプロセスから保護される。この環境の対策方針は前提条件と緊密に関連しており、満たされたとき、これは前提条件に対処する。

前提条件	前提条件に対処する環境対策方針	環境のセキュリティ対策方針を規定した根拠
A.PEER_FUNC_&_MGT TOE へ TSF データまたはサービスを提供する、またはセキュリティ方針の決定の実施において TSF をサポートすると TSF によって信頼されたすべてのリモート高信頼 IT システムは、TSF によって用いられる機能をこの機能に定義された前提条件と一貫して正しく実装し、TOE のセキュリティ方針の制限と適合性のあるセキュリティ方針の制限のもとで適切に管理され運用されることが前提となる。	OE.IT_REMOTE TOE がリモート高信頼 IT システムに依存してその方針の実施を支援している場合、その機能及び TOE が方針決定を行うにあたって利用する任意のデータを TOE の要求によって提供するシステムは、それらの機能に間違った結果の提供を引き起こす可能性のある任意の攻撃から十分に保護される。	OE.IT_REMOTE 高信頼システム間または TOE の物理的に分離した部分間の接続の前提条件は、そのようなシステムがそれらの機能に間違った結果の提供を引き起こす可能性のある任意の攻撃から十分に保護されることを規定する対策方針によって対処される。
	OE.IT_TRUSTED_SYSTEM リモート高信頼 IT システムは、TSF によって要求されるプロトコル及びメカニズムを実装してセキュリティ方針の実施をサポートする。 これらのリモート高信頼 IT システムは、TOE へ適用されるものと同一の規則及び方針に基づいた、既知の、受容された、及び信頼された方針に従って管理され、また TOE と同等に物理的及び論理的に保護される。	OE.IT_TRUSTED_SYSTEM すべてのリモート高信頼 IT システムがこの機能について定義された前提条件と一貫して TSF によって用いられる機能を正しく実装するという前提条件は、TOE に適用されるものと対応した物理的及び論理的保護並びに信頼された方針の適用によってサポートされる。

前提条件	前提条件に対処する環境対策方針	環境のセキュリティ対策方針を規定した根拠
A.PHYSICAL TOE によって保護される IT 資産の価値に対応する適切な物理的セキュリティを IT 環境が TOE に提供することが前提となる。	OE.PHYSICAL TOE の責任者は、セキュリティ方針の実施に重要である TOE の部分が、IT セキュリティ対策方針を危殆化するかもしれないような物理的攻撃から保護されることを保証しなければならない。その保護は、TOE によって保護される IT 資産の価値に見合ったものでなければならない。	OE.PHYSICAL TOE、TSF データ、及び保護された利用者データは、物理的攻撃 (例、窃盗、改変、破壊、または盗聴) から保護されることが前提となる。物理的攻撃には TOE 環境への許可されない侵入者が含まれるかもしれないが、TOE 環境へのアクセスを許可された個人によって取られるかもしれない物理的破壊アクションは含まれない。
	OE.INFO_PROTECT TOE の責任者は、情報が適切な方法で保護されることを保証する手続きを確立し、実施しなければならない。特に： ・すべてのネットワーク及び周辺機器のケーブリングは、そのリンクを介して送信される最も機微なデータの送信が許可されたものでなければならない。そのような物理リンクは、適切な物理的及び論理的保護手法を用いて送信されるデータの機密性及び完全性への脅威に対して十分に保護されることが前提となる。 ・セキュリティ関連ファイル (監査証跡や認証データベース等) に関する DAC 保護は、常に正しく設定されなければならない。 ・利用者は、TOE によって管理されるデータの一部へアクセスする権限を持ち、また彼ら自身のデータに関して管理を行うよう教育される。	OE.INFO_PROTECT すべてのネットワーク及び周辺機器のケーブリングがそのリンクを介して送信される最も機微なデータの送信が許可されたものでなければならないことを要求することによって、前提条件をサポートする。そのような物理リンクは、適切な物理的及び論理的保護手法を用いて送信されるデータの機密性及び完全性への脅威に対して十分に保護されることが前提となる。

前提条件	前提条件に対処する環境対策方針	環境のセキュリティ対策方針を規定した根拠
A.TRAINEDUSER 利用者は、自分の利用者データへの完全な制御を行使することにより、セキュアな IT 環境内で何らかのタスクまたは一群のタスクを完了できるよう十分に教育され信頼されている。	OE.INFO_PROTECT TOE の責任者は、情報が適切な方法で保護されることを保証する手続きを確立し、実施しなければならない。特に： · すべてのネットワーク及び周辺機器のケーブリングは、そのリンクを介して送信される最も機微なデータの送信が許可されたものでなければならない。そのような物理リンクは、適切な物理的及び論理的保護手法を用いて送信されるデータの機密性及び完全性への脅威に対して十分に保護されることが前提となる。 · セキュリティ関連ファイル (監査証跡や認証データベース等) に関する DAC 保護は、常に正しく設定されなければならない。 · 利用者は、TOE によって管理されるデータの一部へアクセスする権限を持ち、また彼ら自身のデータに関して管理を行うよう教育される。	OE.INFO_PROTECT TOE によって管理されるデータの部分へアクセスする権限を利用者が持ち、また彼ら自身のデータへの制御を行使するよう教育されることを保証することによって、この前提条件をサポートする。

方針	方針に対処する環境対策方針	環境のセキュリティ対策方針を規定した根拠
P.ACCOUNTABILITY TOE の許可された利用者は、TOE 内での自分のアクションに責任を持たなければならない。	OE.ADMIN TOE の責任者は適格かつ信用のおける個人であり、TOE 及びそれに含まれる情報のセキュリティの管理が可能であること。	OE.ADMIN 許可された管理者がすべてのタスク及び責務が効果的に行われることの保証に役立つ適任者であることが前提となる方針をサポートする。
	OE.INFO_PROTECT TOE の責任者は、情報が適切な方法で保護されることを保証する手続きを確立し、実施しなければならない。特に： ・ すべてのネットワーク及び周辺機器のケーブリングは、そのリンクを介して送信される最も機微なデータの送信が許可されたものでなければならない。そのような物理リンクは、適切な物理的及び論理的保護手法を用いて送信されるデータの機密性及び完全性への脅威に対して十分に保護されることが前提となる。 ・ セキュリティ関連ファイル (監査証跡や権限データベース等) に関する DAC 保護は、常に正しく設定されなければならない。 ・ 利用者は、TOE によって管理されるデータの一部へアクセスする権限を持ち、また彼ら自身のデータに関して管理を行うよう教育される。	OE.INFO_PROTECT 許可された利用者が教育され自分たちをサポートするために利用可能な手続きを持ち、また DAC 保護が機能し責任追跡性を追求する彼らに通知する十分な情報を提供できることを保証することによって、方針をサポートする。

方針	方針に対処する環境対策方針	環境のセキュリティ対策方針を規定した根拠
P.ROLES TOE は、TOE のセキュアな管理を行う許可された管理者を提供しなければならない。この役割は、他の許可された利用者とは分離された別個のものでなければならない。	OE.ADMIN TOE の責任者は適格かつ信用のおける個人であり、TOE 及びそれに含まれる情報のセキュリティの管理が可能であること。	OE.ADMIN TOE のセキュアな管理を行う許可された管理者役割が確立されていることを保証することによって、方針をサポートする。

方針	方針に対処する環境対策方針	環境のセキュリティ対策方針を規定した根拠
P.USER 権限は、そのアクションを正しく行うと信頼される利用者のみへ与えられなければならない。	OE.ADMIN TOE の責任者は適格かつ信用のおける個人であり、TOE 及びそれに含まれる情報のセキュリティの管理が可能であること。	OE.ADMIN 利用者へ適切な権限を与える責任を持つ許可された管理者が信頼できることを保証することによって、方針をサポートする。
	OE.INFO_PROTECT TOE の責任者は、情報が適切な方法で保護されることを保証する手続きを確立し、実施しなければならない。特に： ・ すべてのネットワーク及び周辺機器のケーブリングは、そのリンクを介して送信される最も機微なデータの送信が許可されたものでなければならない。そのような物理リンクは、適切な物理的及び論理的保護手法を用いて送信されるデータの機密性及び完全性への脅威に対して十分に保護されることが前提となる。 ・ セキュリティ関連ファイル (監査証跡や権限データベース等) に関する DAC 保護は、常に正しく設定されなければならない。 ・ 利用者は、TOE によって管理されるデータの一部へアクセスする権限を持ち、また彼ら自身のデータに関する制御を行使するよう教育される。	OE.INFO_PROTECT TOE によって管理されるデータの部分へアクセスする権限を利用者が持ち、また彼ら自身のデータへの制御を行使するよう教育され、さらにセキュリティ関連ファイル (監査証跡や権限データベース等) に関する DAC 保護が常に正しく設定されなければならない　ことを保証することによって、方針をサポートする。

脅威	脅威に対処する環境対策方針	環境のセキュリティ対策方針を規定した根拠
T.IA_MASQUERADE 利用者または利用者に代わって作用するプロセスが、利用者データ、TSF データ、または TOE 資源へ許可されないアクセスを得るために許可されたエンティティに成りすますかもしれない。	OE.NO_GENERAL_PURPOSE DMBS の動作、管理、及びサポートに必要なサービス以外に、DBMS 上で利用可能な汎用コンピューティング機能 (例、コンパイラやユーザアプリケーション) が存在しないこと。	OE.NO_GENERAL_PURPOSE DBMS サーバには、一切の汎用コンピューティングまたは記憶機能が含まれてはならない。 これによって、なりすましの脅威は低減される。DBMS または関連する機能の利用者のみが TOE 環境中で定義されることになるためである。

脅威	脅威に対処する環境対策方針	環境のセキュリティ対策方針を規定した根拠
T.TSF_COMPROMISE 利用者または利用者に代わって作用するプロセスが、設定データの不適切なアクセス (閲覧、改変または削除) を引き起こしたり、TSF 内の実行可能コードを危殆化させたりするかもしれない。	OE.INFO_PROTECT TOE の責任者は、情報が適切な方法で保護されることを保証する手続きを確立し、実施しなければならない。特に： ・すべてのネットワーク及び周辺機器のケーブリングは、そのリンクを介して送信される最も機微なデータの送信が許可されたものでなければならない。そのような物理リンクは、適切な物理的及び論理的保護手法を用いて送信されるデータの機密性及び完全性への脅威に対して十分に保護されることが前提となる。 ・セキュリティ関連ファイル (監査証跡や権限データベース等) に関する DAC 保護は、常に正しく設定されなければならない。 ・利用者は、TOE によって管理されるデータの一部へアクセスする権限を持ち、また彼ら自身のデータに関する制御を行使するよう教育される。	OE.INFO_PROTECT すべてのネットワーク及び周辺機器のケーブリングがそのリンクを介して送信される最も機微なデータの送信が許可されたものでなければならないことを保証することによって、脅威を低減する。そのような物理リンクは、適切な物理的及び論理的保護手法を用いて送信されるデータの機密性及び完全性への脅威に対して十分に保護されることが前提となる。
	OE.IT_REMOTE TOE がリモート高信頼 IT システムに依存してその方針の実施を支援している場合、その機能及び TOE が方針決定を行うにあたって利用する任意のデータを TOE の要求によって提供するシステムは、それらの機能に間違った結果の提供を引き起こす可能性のある任意の攻撃から十分に保護される。	OE.IT_REMOTE リモート高信頼 IT システムが十分に保護されることを保証することによって、脅威を低減する。
	OE.IT_TRUSTED_SYSTEM リモート高信頼 IT システムは、TSF によって要求されるプロトコル及びメカニズムを実装してセキュリティ方針の実施をサポートする。 これらのリモート高信頼 IT システムは、TOE へ適用されるものと同一の規則及び方針に基づいた、既知の、受容された及び信頼された方針に従って管理され、また TOE と同等に物理的及び論理的に保護される。	OE.IT_TRUSTED_SYSTEM リモート高信頼 IT システムが、TOE へ適用されるものと同じ規則及び方針に基づいた、既知の、受容された及び信頼された方針に従って管理され、また TOE と同等に物理的及び論理的に保護されることを保証することによって、脅威を低減する。
	OE.NO_GENERAL_PURPOSE DMBS の動作、管理、及びサポートに必要なサービス以外に、DBMS 上で利用可能な汎用コンピューティング機能 (例、コンパイラやユーザアプリケーション) が存在しないこと	OE.NO_GENERAL_PURPOSE TOE 環境において TOE に関連しない機能を阻害する機会を減らすことによって、この脅威を低減する。

脅威	脅威に対処する環境対策方針	環境のセキュリティ対策方針を規定した根拠
	OE.PHYSICAL TOE の責任者は、セキュリティ方針の実施に重要な TOE の部分が、IT セキュリティ対策方針を危殆化させる可能性のある物理的攻撃から保護されることを保証しなければならない。その保護は、TOE によって保護される IT 資産の価値に見合ったものでなければならない。	OE.PHYSICAL 攻撃ベクタとして物理的な弱点または脆弱性が悪用されることによる TSF の危殆化の脅威を低減する。

脅威	脅威に対処する環境対策方針	環境のセキュリティ対策方針を規定した根拠
T.UNAUTHORIZED_ACCESS ある利用者は、TOE のセキュリティ方針に従って許可されていない利用者データへの許可されないアクセスを得るかもしれない。	OE.INFO_PROTECT TOE の責任者は、情報が適切な方法で保護されることを保証する手続きを確立し、実施しなければならない。特に： ・すべてのネットワーク及び周辺機器のケーブリングは、そのリンクを介して送信される最も機微なデータの送信が許可されたものでなければならない。そのような物理リンクは、適切な物理的及び論理的保護手法を用いて送信されるデータの機密性及び完全性への脅威に対して十分に保護されることが前提となる。 ・セキュリティ関連ファイル (監査証跡や権限データベース等) に関する DAC 保護は、常に正しく設定されなければならない。 ・利用者は、TOE によって管理されるデータの一部へアクセスする権限を持ち、また彼ら自身のデータに関する制御を行使するよう教育される。	OE.INFO_PROTECT ネットワーク及び周辺機器配線への論理的及び物理的脅威が適切に保護されることを保証することによって、脅威を低減する。 正しく実装された場合、DAC 保護が許可されないアクセスの識別をサポートするかもしれない。

8.3　セキュリティ機能要件根拠

8.3.1　拡張セキュリティ機能要件根拠

下表は、本 PP に見られる拡張機能セキュリティ要件を含めることの根拠を提示するものである。拡張セキュリティ保証要件 (SAR) は存在しないことに注意されたい。

表 14：拡張セキュリティ機能要件根拠

拡張要件	識別子	根拠
FTA_TAH_(EXT).1	TOE アクセス履歴	本 PP は、TOE がクライアントを含むことを要求していない。したがって、PP はクライアントにメッセージの表示を要求できない。本要件は、TOE がアクセス履歴を表示する代わりに、それを保存し検索することを要求するよう改変されている。
FIA_USB_(EXT).2	高度な利用者-サブジェクト結合	DBMS は、直接的には利用者セキュリティ属性ではない他の TSF データからサブジェクトセキュリティ属性を導出するかもしれない。例としては、利用者が接続を確立するために利用したエントリーポイントが挙げられる。アクセス制御方針もまた、そのアクセス制御方針のこのサブジェクトセキュリティ属性を利用して、利用者が特定の入力ポートを通して接続したときのみ重要なオブジェクトへのアクセスを可能とするかもしれない。

8.3.2　TOE セキュリティ機能要件根拠

下表は、セキュリティ機能要件の選択の根拠を提供するものである。この表では、各 TOE セキュリティ対策方針から識別されたセキュリティ機能要件への追跡が行われる

表 15：TOE セキュリティ機能要件根拠

対策方針	対策方針へ対処する要件	根拠
O.ACCESS_HISTORY TOE は、過去のセション確立試行に関連する情報を保存し、その情報を利用者が利用できるようにする。	FTA_TAH_(EXT).1	TOE は､利用者が自分のアカウントへログインするたびに､以前の許可されないログイン試行に関する情報及びログインが試行された回数を保存及び検索できなければならない。また TOE は、最後の成功した許可されたログインを保存しなければならない。この情報には、試行の日付、時刻、手法、及び場所が含まれる。適切に表示された場合、これによって自分のアカウントへ別の利用者がアクセスを試行しているかどうかを利用者が検出することが可能となる。 これらの記録は､利用者に自分のアクセス履歴が通知された後でなければ削除されるべきではない。 (FTA_TAH_(EXT).1)
O.ADMIN_ROLE TOE は、管理特権を利用したアクションが制限され得るようなメカニズム (例、「役割」) を提供する。	FMT_SMR.1	TOE は､少なくとも､許可された管理者役割を確立する。ST 作成者は、より多くの役割を規定することを選んでもよい。許可された管理者には､他の利用者が行うことのできない特定のタスクを行う特権が与えられる。これらの特権には､監査情報やセキュリティ機能へのアクセスが含まれるが､これには限定されない。 (FMT_SMR.1)

対策方針	対策方針へ対処する要件	根拠
O.AUDIT_GENERATION TOE は、利用者と関連付けられたセキュリティ関連事象を検出し記録を作成する能力を提供すること。	FAU_GEN.1 FAU_GEN.2 FAU_SEL.1	FAU_GEN.1 は、TOE が記録することができなければならない事象のセットを定義する。本要件によって、TOE 中で発生する任意のセキュリティ関連事象を監査する能力を管理者が有することが保証される。また本要件は、各監査対象事象の監査記録中に含まれなければならない情報も定義する。また本要件は、ST 作成者が本 PP に追加する任意の追加的セキュリティ機能要件に関して記録される詳細さのレベルに関する要件も課す。 FAU_GEN.2 は、利用者及び任意の関連したグループ識別情報が監査記録によって監査事象と関連付けられることを保証する。許可された利用者の場合、この関連付けは利用者 ID を用いて行われる。許可されたグループの場合、この関連付けはグループ ID を用いて行われる。 FAU_SEL.1 は､監査証跡中にどの監査対象事象が記録されるかを管理者が設定することを可能とする。これによって管理者には､サイトの方針によって必要とみなされる事象のみを記録する柔軟性が提供され､したがって監査メカニズムによって使用される資源の量が減少する。
O.DISCRETIONARY_ACCESS TSF は、オブジェクト、サブジェクトまたは利用者の識別情報に基づいて、サブジェクト及び／または利用者の、名前付きリソースへのアクセスを制御しければならない。TSF は、そのアクセスモードでどの利用者／サブジェクトに特定の名前付きオブジェクトへのアクセスが許可されるかを許可された利用者が各アクセスモードにおいて指定できるようにしなければならない。	FDP_ACC.1 FDP_ACF.1	TSF は､自分のデータを保存するためにアクセスしたい資源の指定を許可された利用者の識別情報に基づいて､資源へのアクセスを制御しなければならない。 アクセス制御方針は､定義された制御範囲を持たなければならない [FDP_ACC.1]。 アクセス制御方針の規則が定義される [FDP_ACF.1]。

対策方針	対策方針へ対処する要件	根拠
O.I&A TOE は、認証を必要とする任意のアクションを TOE が処理する前に、利用者が認証されることを保証する。	FIA_ATD.1 FIA_UAU.1 FIA_UID.1 FIA_USB_(EXT).2	TSF は、許可された利用者のみが TOE 及びその資源へアクセスできることを保証しなければならない。TOE へアクセスする権限を持つ利用者は、識別と認証プロセスを用いなければならない[FIA_UID.1, FIA_UAU.1]。 アクセスを決定するために用いられるセキュリティ属性が定義され認証決定をサポートするために利用可能であることを保証する。[FIA_ATD.1]. 利用者に代わって作用するサブジェクトの適切な認証もまた、保証される[FIA_USB_(EXT).2]。 認証メカニズムの適切な強度が保証される。
O.MANAGE TSF は、TOE セキュリティメカニズムの管理に責任を持つ許可された利用者をサポートするために必要なすべての機能及びファシリティを提供しなければならず 、そのような管理アクションが専門の利用者に限定されることを可能としなければならず、またそのような許可された利用者のみが管理機能にアクセスできることを保証しなければならない。	FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_REV.1(1) FMT_REV.1(2) FMT_SMF.1 FMT_SMR.1	FMT_MOF.1 は、特定の TOE 機能を利用する能力が管理者に制限されることを要求する。 FMT_MSA.1 は、セキュリティ属性に関する操作を行う能力が特定の役割に制限されることを要求する。 FMT_MSA.3 はセキュリティ属性に用いられるデフォルト値が制限的であることを要求する。 FMT_MTD.1 は、TOE の内容を操作する能力が管理者に制限されることを要求する。 FMT_REV.1 は、属性を失効させる能力を管理者に制限する。 FMT_SMF.1 は、許可された管理者に利用可能な管理機能を識別する。 FMT_SMR.1 は、サポートされるべき具体的なセキュリティ役割を定義する。

対策方針	対策方針へ対処する要件	根拠
O.MEDIATE TOE は、そのセキュリティ方針に従って利用者データを保護しなければならず、またそのようなデータへアクセスするすべての要求を仲介しなければならない。	FDP_ACC.1 FDP_ACF.1 FPT_TRC.1	FDP 要件は、TOE 中で仲介がいつ、そしてどのように発生するかに関する方針、サブジェクト、オブジェクト、そして操作を定義するために選ばれた。 FDP_ACC.1 は、名前付きオブジェクトのリストへのアクセスの取得を試行する利用者に代わって作用するサブジェクトのリストに実施されるアクセス制御方針を定義する。サブジェクトとオブジェクトとの間のすべての操作は、TOE の方針によって定義される。 FDP_ACF.1 は、TOE のアクセス制御方針に基づいてオブジェクトへアクセス制御を提供するために用いられるセキュリティ属性を定義する。 FPT_TRC.1 は、アクセス制御に用いられる属性を規定する複製された TSF データが、TOE の分散コンポーネントにわたって一貫していなければならない　ことを保証する。この要件は、複製された TSF データの一貫性を維持するためである。
O.RESIDUAL_INFORMATION TOE は、その制御範囲内の保護された資源に含まれる任意の情報が、その資源の再割当て時に不適切に暴露されないことを保証すること。	FDP_RIP.1	FDP_RIP.1 は、資源の内容がそのデータへのアクセスを明示的に許可されたサブジェクト以外には利用できないことを保証するために利用される。

対策方針	対策方針へ対処する要件	根拠
O.TOE_ACCESS TOE は、利用者データ及び TSF への利用者の論理的アクセスを制御するメカニズムを提供すること。	FDP_ACC.1 FDP_ACF.1 FIA_ATD.1 FTA_MCS.1 FTA_TSE.1	FDP_ACC.1 は、TOE 中のオブジェクトのサブセットに関して可能な操作のサブセットに関して、識別されたアクセス制御 SFP それぞれが用意されていることを要求する。 FDP_ACF.1 は、セキュリティ属性及び属性の名前付きグループに基づいて TSF がアクセスを強制することを可能とする。さらに、TSF はセキュリティ属性に基づいてオブジェクトへのアクセスを明示的に許可したり拒否したりする能力があるかもしれない。 FIA_ATD.1 は、利用者の識別子及び任意の関連付けられたグループへの所属を含め、個別利用者のセキュリティ属性を定義する。セキュリティ関連の役割及びその他の識別セキュリティ属性。 FTA_MCS.1 は、任意の所与の時点で利用者が最大で規定された数だけのアクティブなセションをオープンさせ得ることを保証する。 FTA_TSE.1 は、TOE が特定の基準に基づいて TOE へのアクセスを制限することを可能とする。

8.3.3　すべてのセキュリティ機能要件の依存性が満たされていることの根拠

表 16：セキュリティ機能要件の依存性

要件	依存性	満たされる
FAU_GEN.1	FPT_STM.1	本要件は、A.SUPPORT に与えられる IT 環境に関する前提条件によって満たされる。
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 によって満たされる。 FIA_UID.1 によって満たされる。
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	FAU_GEN.1 によって満たされる。 FMT_MTD.1 によって満たされる。
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1 によって満たされる。
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 によって満たされる。 FMT_MSA.3 によって満たされる。
FDP_RIP.1	なし	N/A
FIA_ATD.1	なし	N/A
FIA_UAU.1	FIA_UID.1	FIA_UID.1 によって満たされる。
FIA_UID.1	なし	N/A
FIA_USB_(EXT).2	FIA_ATD.1	FIA_ATD.1 によって満たされる。
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 によって満たされる。 FMT_SMR.1 によって満たされる。
FMT_MSA.1	[FDP_ACC.1 または FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	FDP_ACC.1 によって満たされる。 FMT_SMF.1 によって満たされる。 FMT_SMR.1 によって満たされる。
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 によって満たされる。 FMT_SMR.1 によって満たされる。
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 によって満たされる。 FMT_SMR.1 によって満たされる。
FMT_REV.1(1)	FMT_SMR.1	FMT_SMR.1 によって満たされる。
FMT_REV.1(2)	FMT_SMR.1	FMT_SMR.1 によって満たされる。
FMT_SMF.1	なし	N/A
FMT_SMR.1	FIA_UID.1	FIA_UID.1 によって満たされる。
FPT_TRC.1	FPT_ITT.1	FPT_ITT.1 は適用されない。 分散 TOE については、送信されるデータの機密性及び完全性を保証する、環境に関する前提条件 A.CONNECT によって依存性が満たされる。

要件	依存性	満たされる
FTA_MCS.1	FIA_UID.1	FIA_UID.1 によって満たされる。
FTA_TAH_(EXT).1	なし	N/A
FTA_TSE.1	なし	N/A

8.4　すべてのセキュリティ保証要件が満たされていることの根拠

本プロテクションプロファイルは、商用 DBMS セキュリティソフトウェア開発者によって使用されるために開発された。本 PP は、国際的に利用される商用 DBMS 製品に適用されるため、コモンクライテリア承認アレンジメント (CCRA) によって国際的に承認される最大レベルの保証を満たすため、EAL 2 保証パッケージが PP 作成者によって選択された。

欠陥修正は、現在のシステムに対して何ら保証を追加するものではないが、今後のリリースに対する保証を追加するものであるため、どの EAL レベルにも含まれない唯一の要件である。ゆえに、DBMS WG／TC は、ベンダに適切な欠陥修正手法に関して指示するため、EAL2 及び追加の保証要件 ALC_FLR.2 と決めた。

セキュリティ保証要件の依存性は、以下の事実に基づいてすべてが満たされる：

- EAL2 は、EAL2 のパッケージによってすべての依存性が満たされ、完全に自給自足している。
- EAL 2 に追加される ALC_FLR.2 のセキュリティ保証要件は、一切の依存性を持たない。

8.5　結論

セキュリティ対策方針及びセキュリティ対策方針の根拠に基づき、以下の結論が導き出される : すべてのセキュリティ対策方針が達成された場合には、セキュリティ課題定義 (SPD) に定義されるセキュリティ問題が解決される : すべての脅威が対抗され、すべての組織のセキュリティ方針 (OSP) が実施され、そしてすべての前提条件が是認される。

9　附属書

以下のセクションは、本プロテクションプロファイルの附属書である。

附属書A.　参考資料

[REF 1] Common Criteria Management Board、情報技術セキュリティ評価のためのコモンクライテリア、CCMB-2012-09、バージョン 3.1、2012 年 9 月

[REF 1a] Common Criteria Management Board、情報技術セキュリティ評価のためのコモンクライテリア、パート 1:概説と一般モデル、CCMB-2012-09-01、バージョン 3.1、2012 年 9 月

[REF 1b] Common Criteria Management Board、情報技術セキュリティ評価のためのコモンクライテリア、パート 2 : セキュリティ機能要件、CCMB-2012-09-02、バージョン 3.1、2012 年 9 月

[REF 1c] Common Criteria Management Board、情報技術セキュリティ評価のためのコモンクライテリア、パート 3 : セキュリティ保証要件、CCMB-2012-09-03、バージョン 3.1、2012 年 9 月

[REF 2] Common Criteria Development Board、CC and CEM addenda、CCDB-2014-03-01、バージョン 1.0、2014 年 3 月

附属書B.　用語集

CC パート 1 及び以下の用語及び定義が適用される。矛盾がある場合、本文書に与えられる用語または定義が優先する。

アクセス (Access) - データのフローまたは改変がもたらすような、エンティティとオブジェクトとの間の対話。

アクセス制御 (Access Control) - 資源 [3]の利用並びにデータ [4]の暴露及び改変を制御するセキュリティサービス。

責任追跡性 (Accountability) - 追跡されるべき IT システムでのアクティビティを、そのアクティビティに責任を持つエンティティに対して許容するような特性。

管理者 (Administrator) - TOE の一部または全部を管理する権限を具体的に許可された利用者であって、そのアクションは TSP に影響するかもしれない。管理者は、TSP の一部を上書きする能力を提供する特別な特権を保有するかもしれない。

保証 (Assurance) - IT システムのセキュリティ機能がそのセキュリティ方針を実施するために十分であるという確信の度合い。

攻撃 (Attack) - IT システムのセキュリティ方針への侵害を試行する意図的な行為。

認証 (Authentication) - 主張される識別情報を検証するセキュリティ手段。

認証データ (Authentication data) - 主張される識別情報を検証するために用いられる情報。

許可、権限付与 (Authorization) - 機能を実行しデータへアクセスするために、そのような権限を持つエンティティによって与えられる許可。

許可された管理者 (Authorized Administrator) - 評価対象と接触する許可された人物であって、その運用能力の維持管理に責任を負う。

許可された利用者 (Authorized user) - 認証された利用者であって、TSP に従って、操作を行うことができる。

可用性 (Availability) - IT 資源へのタイムリー[5]で確実なアクセス。

危殆化 (Compromise) - セキュリティ方針の侵害。

機密性 (Confidentiality) - データの暴露に関するセキュリティ方針。

設定データ (Configuration data) - TOE の設定に用いられるデータ。

適合製品 (Conformant Product) - セクション 7.1 のすべての機能的セキュリティ要件を満たした、そして本文書のセクション 7.2 のすべての TOE セキュリティ保証要件を満たす、評価対象。

データベース管理システム (DBMS) - 通常、永続的データの大規模に構造化されたセットを管理するプログラムのスイートであって、数多くの利用者にアドホックなクエリ機能を提供する。ビジネス用途に広く利用されている。

任意アクセス制御 (Discretionary Access Control) (DAC) - サブジェクトの識別情報及び／またはそれらが属するグループに基づいて、オブジェクトへのアクセスを制限する手段。こ

[3] ハードウェア及びソフトウェア
[4]保存データまたは通信データ
[5]定義される基準に従う

れらの制御は、特定のアクセス権限を有するサブジェクトがそのアクセス権限を (たぶん間接的に) 任意の他のサブジェクトへ渡すことができるという意味で、任意である。

エンクレーブ (Enclave) - 1 つの権威の制御下にあるエンティティの集まりであって、均質なセキュリティ方針を持つもの。これは論理的なものであったり、物理的な場所と近接性に基づいていたりするかもしれない。

エンティティ (Entity) - TOE オブジェクト、データ、または資源と対話するような、サブジェクト、オブジェクト、利用者または別の IT デバイス。

TSF 内の実行可能コード (Executable code within the TSF) - TSF を構成するソフトウェアであって、コンピュータによって実行可能な形式であるもの

外部 IT エンティティ (External IT entity) - 任意の情報技術 (IT) 製品またはシステムであって、TOE の外部に位置し、TSP に従って操作を行い得るもの。

識別情報 (Identity) - 許可された利用者を一意に識別する表現 (例、文字列) であって、その利用者のフルネームまたは短縮名であってもよいし、ペンネームであってもよい。

完全性 (Integrity) - データ及び TSF メカニズムの破損に関するセキュリティ方針。

名前付きオブジェクト (Named Object) - 以下の特徴すべてを示すオブジェクト：

- そのオブジェクトは、TSF 内の利用者及び／またはグループの識別情報が異なるサブジェクト間で情報を転送するために使用されてもよい。
- TOE におけるサブジェクトは、そのオブジェクトの特定のインスタンスを要求できなければならない。
- 異なる利用者及び／またはグループの識別情報を持つサブジェクトがそのオブジェクトと同じインスタンスを要求することを許容する可能性があるように、そのオブジェクトの特定のインスタンスを参照するために用いられる名前が存在しなければならない。

オブジェクト (Object) - TSC (TSF 制御範囲) 内のエンティティであって、情報を含む、または情報を受信し、またそれに対してサブジェクトが操作を行うもの。

運用環境 (Operating Environment) - TOE が動作する環境全体。これには、物理的なファシリティ並びに物理的、手続き的、管理的及び人的管理策が含まれる。

公開オブジェクト (Public Object) - TSF が無条件にすべてのエンティティに「読み出し」アクセスを許可するオブジェクト。TSF または許可された管理者のみが、公開オブジェクトを作成し、削除し、または改変することができる。

セキュアな状態 (Secure State) - すべての TOE セキュリティ方針が実施されている条件。

セキュリティ属性 (Security attributes) - サブジェクト、オブジェクト、及び利用者と関連付けられた TSF データであって、TSP の実施に用いられるもの。

セキュリティレベル (Security level) - 階層的なクラス分けと非階層的なカテゴリのセットの組み合わせであって、情報の機密性を表現するもの。

機微な情報 (Sensitive information) - その情報の許可されない暴露、改ざん、喪失、または破棄が、少なくとも人または物に対して検知可能な損害の原因となるため、適格な権限者の決定のとおり保護されなければならない情報。

サブジェクト (Subject) - TSC 内部のエンティティであって、操作を行わせるもの。

脅威 (Threat) - 敵対者の能力、意図及び攻撃手法、あるいは任意の状況または事象であって、TOE セキュリティ方針を侵害する可能性のあるもの。

TOE 資源 (TOE resources) - TOE 内で使用または消費可能なもの。

許可されない利用者 (Unauthorized user) - システムによって提供される公開オブジェクトが存在する場合にはそれのみへアクセスするかもしれない利用者。

利用者 (User) - TOE と対話する、TOE 外部のエンティティ (人間の利用者または外部 IT エンティティ)。

脆弱性 (Vulnerability) - TOE セキュリティ方針を侵害するために悪用可能な弱点。

附属書C.　略語と頭字語

CA	認証局 (Certificate Authority)
CC	コモンクライテリア (Common Criteria)
CCIMB	Common Criteria Interpretations Management Board
CM	構成管理 (Configuration Management)
COTS	市販の (Commercial Off The Shelf)
DAC	任意アクセス制御 (Discretionary Access Control)
DBMS	データベース管理システム (Database Management System)
DBMS PP	データベース管理システムプロテクションプロファイル (Database Management System Protection Profile)
EAL	評価保証レベル (Evaluation Assurance Level)
I&A	識別と認証 (Identification and Authentication)
IT	情報技術 (Information Technology)
LAN	ローカルエリアネットワーク (Local Area network)
OS	オペレーティング システム (Operating System)

OSP	組織のセキュリティ方針 (Organizational Security Policy)
PP	プロテクションプロファイル (Protection Profile)
SAR	セキュリティ保証要件 (Security Assurance Requirement)
SFP	セキュリティ機能方針 (Security Functional Policies)
SFR	セキュリティ機能要件 (Security Functional Requirement)
SPD	セキュリティ課題定義 (Security Problem Definition)
ST	セキュリティターゲット (Security Target)
TOE	評価対象(Target of Evaluation)
TSC	TSF 制御範囲 (TSF Scope of Control)
TSE	TOE セキュリティ環境 (TOE Security Environment)
TSF	TOE セキュリティ機能 (TOE Security Functions)
TSFI	TSF インタフェース (TSF Interfaces)
TSP	TOE セキュリティ方針 (TOE Security Policy)