認　証　報　告　書

独立行政法人 情報処理推進機構
理事長　藤原　武平太　原紙押印済

評価対象

申請受付年月日(受付番号)	**平成18年10月25日(IT認証6109)**
認証番号	C0089
認証申請者	**株式会社エヌ・ティ・ティ・データ**
TOEの名称	PostgreSQL **認証版**
TOEのバージョン	Linux**版** V8.1.5
PP適合	**なし**
適合する保証要件	EAL1
TOE開発者	**株式会社エヌ・ティ・ティ・データ**
評価機関の名称	**社団法人 電子情報技術産業協会　ITセキュリティセンター**

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。
平成19年3月22日

独立行政法人 情報処理推進機構
セキュリティセンター 情報セキュリティ認証室
技術管理者　田渕　治樹

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① Common Criteria for Information Technology Security Evaluation Version 2.3
② Common Methodology for Information Technology Security Evaluation Version 2.3

評価結果：合格

「PostgreSQL 認証版 Linux版 V8.1.5」は、独立行政法人 情報処理推進機構が定める ITセキュリティ認証手続規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

1.1 はじめに

この認証報告書は、「PostgreSQL 認証版 Linux版 V8.1.5」（以下「本TOE」という。）について社団法人 電子情報技術産業協会 ITセキュリティセンター（以下「評価機関」という。）が行ったITセキュリティ評価に対し、その内容の認証結果を申請者である株式会社エヌ・ティ・ティ・データに報告するものである。

本認証報告書の読者は、本書と共に、対応するSTや本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

本認証報告書は、本TOEに対して、適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

1.2 評価製品

1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称:	PostgreSQL 認証版
バージョン:	Linux版 V8.1.5
開発者:	株式会社エヌ・ティ・ティ・データ

1.2.2 製品概要

本製品は、Red Hat Enterprise Linux AS v.4 for x86上で動作するリレーショナルデータベース管理システムである。本製品はオープンソースのPostgreSQLを株式会社エヌ・ティ・ティ・データのソフトウェア製品として提供するもので、次の５つの機能で実現されている。

- バックエンドプロセス管理機能
- ソケット制御機能
- 利用者識別機能
- データベースアクセス機能
- 監査ログ機能

1.2.3 TOEの範囲と動作概要

1.2.3.1 TOEの動作環境

本TOEの動作環境を図1-1に示す。本TOEは、Intel Architectureに準拠したマイクロプロセッサを搭載した単一のサーバマシン上のRed Hat Enterprise Linux AS v.4 for x86オペレーティングシステム（以下「OS」という。）の上で動作する。サーバマシン及びコンソールは物理的に保護されたセキュリティ専用区域に設置される。セキュリティ専用区域への入室権限はシステム及びサーバの運用管理者が持つ。

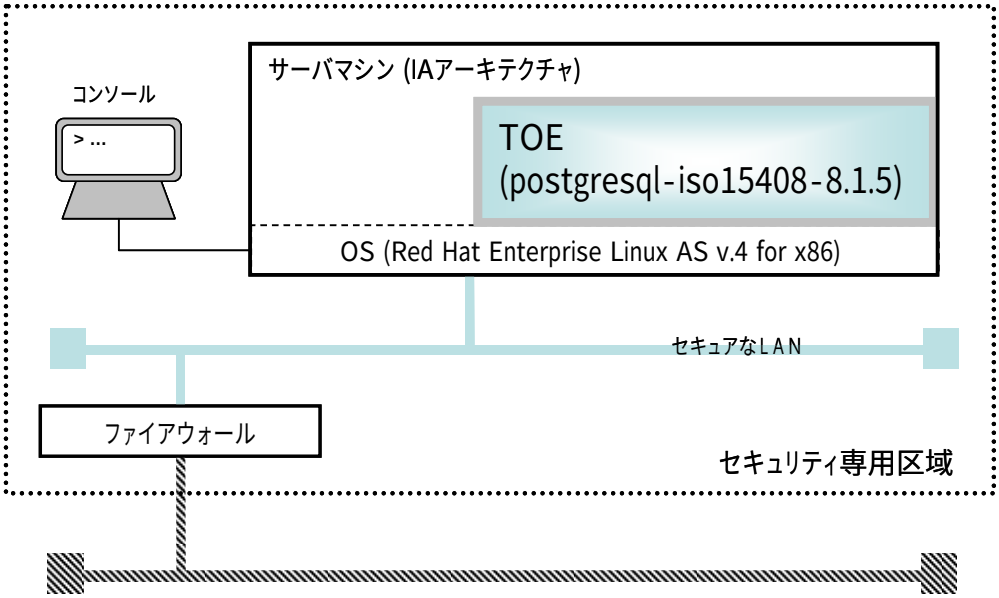

図1-1　TOEの動作環境

サーバが接続されるネットワークはファイアウォールによって保護されたセキュアなLANである。ファイアウォールは特定のポートに対する特定の端末からのパケットだけが通過できるように設定され、当該のLANを保護する。

本TOEの運用環境では、OSの機能により他システムからTCP/IPソケットを経由してTOEを利用することが制限される。また、利用者及び管理者の認証識別はパスワード認証方式で行う。

1.2.3.2 TOEの範囲と動作概要

本TOEの論理的構成を図1-2に示す。図中の灰色太線で囲まれた部分がTOEの範囲である。

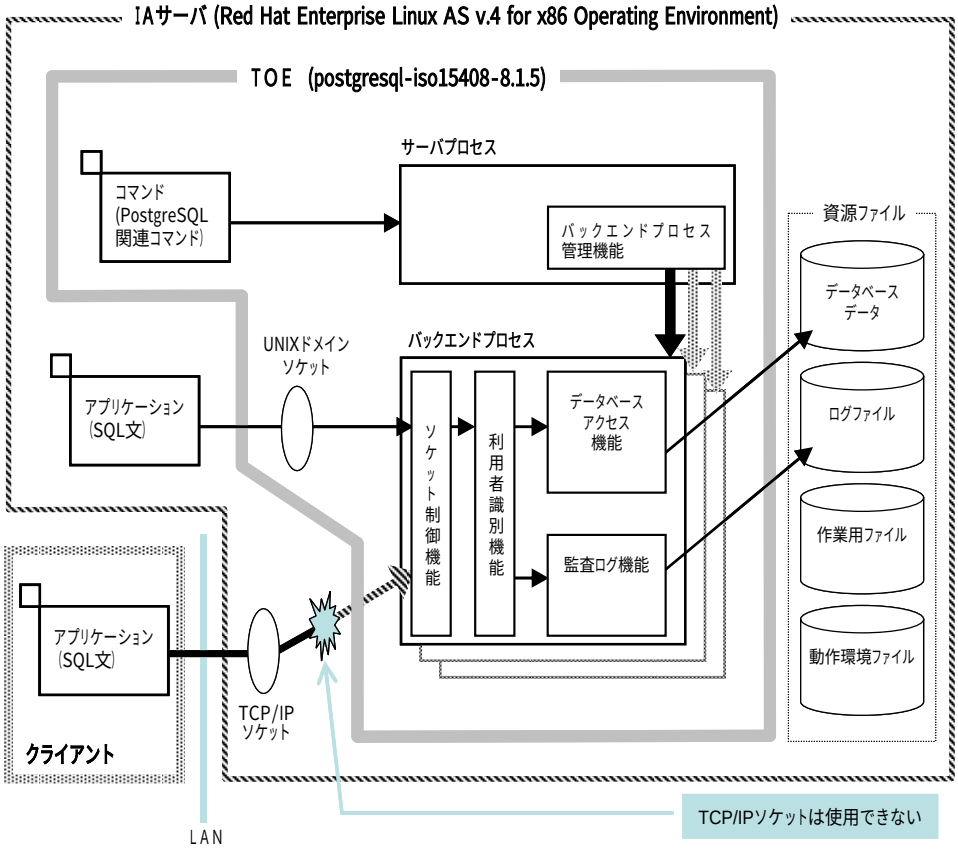

図1-2 TOEの論理的範囲と機能

TOEの機能を利用するには、OSにログインし、自システムでPostgreSQL関連コマンド（以下「コマンド」という。）を通じて管理する方法と自システム上のアプリケーションがUNIXドメインソケットを経由して利用する方法が可能である。

管理者はOSにログインした後に、自システム上でコマンドの実行を通してTOEを起動、停止する。

TOEのリレーショナルデータベース機能を利用する場合、利用者及び管理者は、アプリケーションを介してTOEに接続する。アプリケーションからTOEに接続する場合には、アプリケーションはTOEに対して利用者ないし管理者の識別情報を指定しパスワード認証を経た後に、SQL文の処理を依頼する。アプリケーションの指定する識別情報に関連付けられた権限に従って、TOEはアプリケーションに埋め込まれたSQL文を処理する。

アプリケーションからTOEへの接続にはUNIXドメインソケットを経由する。TCP/IPソケットを経由して接続する機能は本ST標準のセキュリティ運用では利用が制限される。つまり他システム上のアプリケーションがTCP/IPソケットを経由して利用することはできない。

1.2.4 TOEの機能

本TOEは以下の5つの機能を提供し、リレーショナルデータベース機能を実現している。

(1) バックエンドプロセス管理機能
(2) ソケット制御機能
(3) 利用者識別機能
(4) データベースアクセス機能
(5) 監査ログ機能

以下にそれぞれの機能を説明する。

1.2.4.1 バックエンドプロセス管理機能

サーバプロセスがバックエンドプロセスの起動、停止及びバックエンドプロセスとアプリケーションの接続を管理する機能である。本TOEでは、サーバプロセスはコマンドによって起動されTOE全体で一つである。一方バックエンドプロセスは、アプリケーションの処理に対応してサーバプロセスの子プロセスとして起動（図1-2の上から下への太矢印)、管理される。バックエンドプロセスがマルチプロセスで動作することで、利用者はアプリケーションを複数同時に実行する、あるいはひとつのアプリケーションの中で複数同時にSQL文の処理を依頼することができる。

1.2.4.2 ソケット制御機能

サーバプロセスがアプリケーションから接続の要求を受けると、バックエンドプロセスに対してUNIXドメインソケットをOSの管理機能を用いて割り付ける。バックエンドプロセスはUNIXドメインソケット経由でアプリケーションと接続される。

管理者は、ソケット制御機能を用いてサーバプロセスが割り付けるソケットの種類や利用の可否、またソケットの接続数を制御することができる。

1.2.4.3 利用者識別機能

アプリケーションとバックエンドプロセスの接続において、各利用者の権限を制御し、指定された権限の範囲での処理を保証し、またその範囲を超えた処理を制限する機能である。バックエンドプロセスに接続されたアプリケーションが指定する識別情報を認証し、個々のバックエンドプロセスに論理的なアクセス権限を付与する。利用者の識別情報を指定して実行したバックエンドプロセスを利用者のプロセスと呼ぶ。また、管理者の識別情報を指定して実行したバックエンドプロセスを管理者のプロセスと呼ぶ。管理者が実行したコマンドのプロセスも管理者のプロセスである。

1.2.4.4 データベースアクセス機能

利用者識別機能が関連付けた論理アクセス権限に従って、バックエンドプロセスが各利用者（ないし管理者）のデータ及びデータの構造定義情報の参照、更新等行なう機能である。データベースアクセス機能は、利用者識別機能が関連付けた論理的アクセス権限に従い、各利用者のデータ及びデータの構造定義情報を、当該の利用者のみが利用できることを保証する。

TOEは、リレーショナルデータベース機能で扱うデータを、OSがTOEに割り当てる資源ファイルに格納する。資源ファイルに格納されているデータに対して物理的なアクセスを行うのは、TOEのコマンドのプロセスとバックエンドプロセスである。バックエンドプロセスの資源ファイルへの物理的なアクセスは、TOEの管理者権限で行われるが、利用者データへの論理的なアクセスは、アプリケーションがTOEへの接続の際に指定した識別情報に利用者識別機能が関連付けた論理的アクセス権限に従って適切に制御される。従って、利用者のプロセスは当該の利用者のデータだけを利用できる。

また、バックエンドプロセスと資源ファイルはOSの機能を用いてアプリケーションから分離されているため、例えアプリケーションに論理ミス等があったとしても、アプリケーションが各利用者のデータや資源ファイルに、バックエンドプロセスを介さずに、直接アクセスすることはできない。

TOEがOSから獲得する資源ファイル及びプロセス、UNIXドメインソケットの保護はOSが行う。

データベースアクセス機能を利用するために、管理者及び利用者はSQL文を埋め込んだアプリケーションを通じてTOEに接続し、バックエンドプロセスにSQL文の実行を依頼する。管理者はデータベースアクセス機能の利用に際して、以下の機能を持つSQL文を利用することができる。

- データベースの構造定義及びユーザ定義関数の作成
- データのロード
- データのアンロード
- データのバックアップ
- データのリカバリ

管理者及び利用者はデータベースアクセス機能の利用に際して、以下の機能を持つSQL文を利用することができる。

- データの挿入
- データの更新
- データの削除
- データの参照

- 登録関数の実行

1.2.4.5 監査ログ機能

管理者や利用者がTOEに行なった操作を記録する。また、管理者は監査ログ機能を用いて監査記録を取得・参照することができる。管理者は以下の機能を利用することができる。

- 監査ログの取得
- 監査ログの参照

1.3 評価の実施

認証機関が運営するITセキュリティ評価・認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証手続規程」[3]、「評価機関承認手続規程」[4]に規定された内容に従い、評価機関によって本TOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

(1) 本TOEのセキュリティ設計が適切であること。

(2) 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。

(3) 本TOEがセキュリティ設計に基づいて開発されていること。

(4) 上記(1)、(2)、(3)を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「PostgreSQL 認証版　セキュリティターゲット 第1.0版」（以下「ST」という。）[1] 及び本TOE開発に関連する評価用提供物件を調査し、本TOEがCCパート1 ([5][8][11]のいずれか) 附属書C、CCパート2（[6][9][12]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発がCCパート3（[7][10][13]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「PostgreSQL 認証版 Linux版 V8.1.5 評価報告書」（以下「評価報告書」という。）[18]に示されている。なお、評価方法は、CEM（[14][15][16]のいずれか）に準拠する。また、CC及びCEMの各パートは補足[17]の内容を含む。

1.4 評価の認証

認証機関は、評価機関が作成した、評価報告書、所見報告書、及び関連する評価証拠資料を検証し、本TOE評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。評価は、平成19年3月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

1.5 報告概要

1.5.1 PP適合

適合するPPはない。

1.5.2 EAL

STが規定する本TOEの評価保証レベルは、EAL1適合である。

1.5.3 セキュリティ機能強度

本STは、AVA_SOF.1を含まないため、最小機能強度を主張しない。

1.5.4 セキュリティ機能

本TOEのセキュリティ機能は、以下のとおりである。

(1) 運用選択機能 (F.SEL)

管理者がセキュリティパラメタを使用して、セキュリティ機能のふるまいを変更する機能である。この機能を使用して、セキュリティの強度を変更することができる。

a. パラメタを変更する機能(F.SEL.PARA)

利用者のアプリケーションからのSQL文のアクセス機能を、利用者制限機能に関連するパラメタで使用可能な範囲の指定と実行可能な関数の登録により、運用として不要な機能を抑止する。セキュリティパラメタの設定及びチェックはDDL文の投入により実行され、これらの行為はDDL文とともに記録される。

(2) 利用者制御機能 (F.USER)

利用者を識別し、権限を制御し、指定された権限の範囲での処理を保証し、さらに範囲を超えた処理を制限する。

a. 利用者の登録機能 (F.USER.DEF)

管理者がDDL文によりTOEに利用者の認証及び識別情報を登録する機能。登録の行為はDDL文とともに記録される。

b. 認証識別機能 (F.USER.AUTHEN)

TOEは利用者の識別と認証を行い、失敗時には結合依頼を拒否する機能。TOEは認証情報の登録時に、セキュリティパラメタで指定されたパスワードの最低長、文字種及び前回パスワードとの差分を考慮した品質を要求する。また、セキュリティパラメタにより設定された有効期限を過ぎた場合、利用者に対しパスワードの変更を促す。認証の成功、失敗及び認証情報の変更の発生は記録される。

c. 権限の制御機能 (F.USER.PRIV)

TOEは認証識別機能(F.USER.AUTHEN)により識別された情報に関連付けられるアクセス権限に従って、アプリケーションのバックエンドプロセスを介するデータベースデータへのアクセスを制御する。初期状態では、管理者はデータベースデータやログファイルなどの資源に対しすべての操作が可能(すべてのSQL文及びコマンドの実行権限を持つ)である。利用者権限の初期値はいずれも不許可に設定されており、管理者は利用者に対し以下のSQL文の実行の権限付与及び剥奪をDDL文により行う。

・表の参照
・表の更新
・表の削除
・表の挿入
・シーケンスの参照
・登録関数の実行

権限のチェックはデータベースへのアクセス時に毎回実施される。このチェックでの成功及び失敗について利用者の権限やアクセス対象とともに記録される。

d. 資源量の制御機能 (F.USER.RES)

管理者が、各利用者の使用可能な資源量を制限する機能。制限の対象となる資源は、動作環境ファイルを除く資源ファイルのセッションあたりのファイル数、作業メモリ量と一人当たりが同時に実行可能なバックエンドプロセス数である。前者は動作環境ファイル中にて、後者はDDL文にてパラメタを設定する。使用可能な資源量を超える獲得の試みは記録される。

e. 権限情報の参照機能 (F.USER.REF)

各利用者の識別情報、権限情報、使用可能な資源量は、システムカタログ内に格納されており、SQL文により参照可能である。管理者は、全利用者に関する情報を参照することができる。利用者は、自分に関する情報のみ参照することができる。参照時の参照権限チェックの失敗及び成功は記録される。

(3) 資源制御機能 (F.RES)

TOEが使用する資源を制御する。

a. 属性の制御機能 (F.RES.ATTR)

TSFデータ(システムカタログ及びログファイル)の参照を管理者のみに制限する。

(4) 監査ログ機能 (F.AUDIT)

利用者や管理者の処理の情報を取得、保持、参照する機能。

a. 監査ログの取得機能 (F.AUDIT.COL)

以下の事象を監査ログとして取得する。

① 利用者によるTOEに対する結合と結合解除
利用者や管理者によるTOE結合の発生日時、認証の成功/失敗、失敗理由、アプリケーション識別、利用者識別、結合から結合解除までの処理の要約。

② 利用者からの要求によるデータベースへのアクセス
利用者や管理者によるデータベースへのアクセス要求の発生日時、権限チェックの成功/失敗、アプリケーション識別、利用者識別、アクセス対象資源。

③ 管理者によるTOEの操作
管理用SQL文またはコマンドの実行、DDL文の実行、監査ログ参照が発生した際のコマンドやSQL文を含む要約。システム起動/停止の発生日時。

④ システムで発生した異常
監査ログ溢れ、監査ログ閾値超、同時使用セッション数超、利用者最大使用可能資源量超が発生した際のアプリケーション識別、利用者識別、日時を含むエラーメッセージ。

b. 監査ログの参照機能 (F.AUDIT.VIEW)
取得した監査ログの記録を、管理者が検索、読み出しできる機能。

c. 監査ログ領域管理機能 (F.AUDIT.SPACE)
監査ログは複数個のエレメントに分割格納され、管理者はエレメント単位で管理（作成、追加、参照、削除、バックアップ、復元）する。TOEは、特定のエレメントに監査ログを取得し、そのエレメントが満杯になると、管理者に通知した後、次のエレメントに情報を取得する。すべてのエレメントが満杯になった場合（通常管理者がバックアップ、削除をするため発生しない)、TOEは最も古く格納されたエレメントに監査ログを上書きし取得を継続する。

1.5.5 脅威

本TOEは、表1-1に示す脅威を想定し、これに対抗する機能を備える。

表1-1 想定する脅威

識別子	脅 威
T.ACCESS (アプリケーションを使用したデータベースへの結合)	TOEへの結合を許可されていない者が、TOEの機能を使用して、保護資産への許可されていない操作を行う。あるいは利用者がTOEの機能を使用して、保護資産への許可されていない操作を行う。

1.5.6 組織のセキュリティ方針

本TOEの利用に当たって要求される組織のセキュリティ方針はない。

1.5.7 構成条件

本TOEは、Intel Architectureに準拠したマイクロプロセッサを搭載した単一サーバマシン上で動作する。図1-1で示したようにサーバマシン及びコンソールは物理的に保護されたセキュリティ専用区域に設置される。サーバはファイアウォールによって保護されたセキュアなLANに接続される。

本TOEで求められるハードウェア及びソフトウェアは以下のとおりである。

(1) ハードウェア

本TOEはIntel Architectureに準拠したマイクロプロセッサを搭載したサーバマシン上で動作する。本TOEはソフトウェア製品であり、ハードウェア構成は次項のソフトウェアで識別されたOSが動作するもので必要十分であり、付加的な装置・機器を要するものではない。

- プロセッサ　400MHz以上
- メモリ　1GB以上
- ハードディスク　2GB以上

(2) ソフトウェア

本TOEは「Red Hat Enterprise Linux AS v.4 for x86」上で動作する。

1.5.8 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表1-2に示す。

これらの前提条件が満たされない場合、本TOEのセキュリティ機能が有効に動作することは保証されない。

表1-2　TOE使用の前提条件

識別子	前提条件
A.MANAGER (管理者の正当性)	管理者は、不正を行わない。
A.USER (利用者による管理)	利用者は、TOEの利用者識別に際して、利用者自身がアプリケーションを介して使用する識別情報や、利用者がアプリケーションに埋め込んで使用する識別情報を漏洩させない。
A.PHYSICAL (物理的な保護)	管理者以外はTOEの動作するサーバマシンに対し物理的なアクセスはできない。
A.OS (OSによる保護)	管理者以外はTOEの動作するサーバのOSへログインすることはできない。TOEがOSから獲得する資源ファイルの保護はOSが行う。管理者は、TOEの保護資産にOS機能

識別子	前提条件
	を用いてアクセスする関数の登録をしない。
A.TCP (TCP/IP ソケットを経由した利用の停止)	TOEの機能をTCP/IPソケットを経由して利用する機能を停止する。

1.5.9 製品添付ドキュメント

本TOEに添付されるドキュメントを以下に示す。

・PostgreSQL 認証版 Linux版 V8.1.5 セキュリティガイド Ver.1.0

2 評価機関による評価実施及び結果

2.1 評価方法

評価は、CCパート3の保証要件について、CEMに規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告されている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

2.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成18年10月に始まり、平成19年3月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成19年1月に開発者サイトで開発者のテスト環境を使用し、評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

2.3 製品テスト

評価者が評価した開発者テスト及び評価者の実施した評価者テストの概要を以下に示す。

2.3.1 開発者テスト

本TOEでは、開発者テストは評価対象外である。

2.3.2 評価者テスト

1) 評価者テスト環境

評価者が実施したテストの環境を図2-1に、テスト環境の機器構成を表2-1に示す。

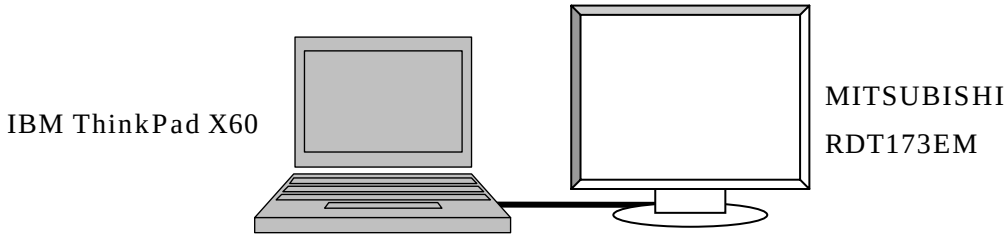

図2-1　評価者テストの環境

表2-1　評価者テストの環境の機器構成

TOEインストール用PC	
ノートPC	型名：IBM ThinkPad X60
	ＣＰＵ：Intel Core Duo T2300(1.66GHz)
	メモリ：1034604KB
	ハードディスク：7905MB
OS	Red Hat Enterprise Linux AS v.4 for x86
仮想マシン環境	VMware Workstation 5.0
ディスプレイ	MITSUBISHI RDT173EM

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a.テスト構成

評価者が実施したテストの構成は図2-1、各構成要素は表2-1に示すとおり。インストールされたTOEのバージョンは、ガイダンスでしめされたversion()関数により確認し、「PostgreSQL 8.1.5-iso15408 Linux」と表示された。これはSTで識別されたTOEと一致する。ハードウェア環境もSTに記載された環境を満足している。ソフトウェア環境もSTで記載されたOSと一致している。

TOEの使用環境条件について、人的側面である「A.MANAGER」、「A.USER」及び物理的側面である「A.PHYSICAL」はテスト環境においては考慮する必要はない。IT環境条件の「A.OS」及び「A.TCP」はインストール手順の中で実現されている。IT環境条件により対応されるOSの設定により期待されるIT環境の機能については本テストの範囲外とする。

以上により評価者テストはTOE構成を満たすテスト環境で実施されている。

b.テスト手法

テストには、以下の手法が使用された。

①セキュリティパラメタに関する設定ファイルを編集し、それぞれの設定項目に対応する機能をOSコマンド、PostgreSQLコマンド及びSQL文をターミナル画面より直接入力し、セキュリティ機能の刺激及びふるまいを確認する。
②結果確認のための入力のバリエーションを要するテストは、SQL文をTOE上で動作させるテストプログラムを実施することにより、あるいはターミナル画面からの直接操作によりセキュリティ機能の刺激を実施し、ターミナル画面あるいは結果ファイルへの出力によりセキュリティ機能のふるまいを確認する。

c.実施テストの範囲

評価者が独自に考案した計112項目のテストを実施した。テスト項目の選択基準はすべてのセキュリティ機能を網羅することと、以下の観点でのサブセットを考案した。

a. ST／機能仕様書では、セキュリティ機能を大きく分けて4つに分類されていることから、確認機能をその4つとした。

b. さらに、4つの各機能はST／機能仕様書において18種類の機能に分類されていることから、その18種類の機能を大項目として設定した。

c. 大項目とした18種類の機能それぞれに存在するインタフェース、操作対象となる利用者属性、及び機能動作のきっかけとなる事象を中項目／小項目に設定し、その組み合わせにて動作する機能の正常時／異常時を考慮したふるまいを、個々のテスト項目とした。

d.結果

実施したすべての評価者テストは正しく完了し、TOEのふるまいを確認することができた。テスト項目の選択基準も妥当であり、評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

2.4 評価結果

評価報告書をもって、評価者は本TOEがCEMのワークユニットすべてを満たしていると判断した。

3 認証実施

評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 当該所見報告書でなされた指摘内容が妥当であること。

② 当該所見報告書でなされた指摘内容が正しく反映されていること。

③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。

④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。

⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。

認証機関は、ST及び評価報告書において、所見報告書及び認証レビューで指摘された問題点が解決されていることを確認した。

4 結論

4.1 認証結果

提出された評価報告書、当該所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL1保証要件を満たしていることを確認した。

評価機関の実施した各評価者エレメントについての検証結果を表4-1にまとめる。

表4-1　評価者アクションエレメント検証結果

評価者アクションエレメント	検証結果
セキュリティターゲット	**適切な評価が実施された。**
ASE_DES.1.1E	評価はワークユニットに沿って行われ、TOE種別、境界の記述が明瞭であることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然とし一貫していることを確認している。
ASE_DES.1.3E	評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。
ASE_ENV.1.1E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_ENV.1.2E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.1E	評価はワークユニットに沿って行われ、ST概説がST及びTOEの識別、概要及びCC適合が明確に述べられていることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_INT.1.2E	評価はワークユニットに沿って行われ、ST概説の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.3E	評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。

ASE_OBJ.1.1E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が、脅威、組織のセキュリティ方針、前提条件へ遡れ、その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_OBJ.1.2E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が完全で、理路整然としていて、かつ一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_PPC.1.1E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_PPC.1.2E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_REQ.1.1E	評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_REQ.1.2E	評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が完全で、理路整然としていて、かつ一貫していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ASE_SRE.1.1E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_TSS.1.1E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていること、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。また、当評価に至るまでになされ

	た所見報告書による指摘も適切と判断される。
ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
構成管理	**適切な評価が実施された**
ACM_CAP.1.1E	評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理･追跡が可能な手続きが妥当であり正しく運用されていることを確認している。
配付と運用	**適切な評価が実施された**
ADO_IGS.1.1E	評価はワークユニットに沿って行われ、TOEがセキュアにセットアップされるための手順が提供されていることを確認している。
ADO_IGS.1.2E	評価はワークユニットに沿って行われ、ADO_IGS.1.1Eにて提供されたセットアップの手順がセキュアであることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
開発	**適切な評価が実施された**
ADV_FSP.1.1E	評価はワークユニットに沿って行われ、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完全に表現している論拠を含んでいることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ADV_FSP.1.2E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
ADV_RCR.1.1E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能の正しく完全な表現であることを、それらの対応分析により確認している。
ガイダンス文書	**適切な評価が実施された**

AGD_ADM.1.1E	評価はワークユニットに沿って行われ、管理者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
AGD_USR.1.1E	評価はワークユニットに沿って行われ、利用者ガイダンスがTOEの管理者でない利用者が利用可能なセキュリティ機能やユーザインタフェース、セキュリティ機能の使用法、対応すべき機能や特権に関する警告、TOEのセキュアな操作に必要なすべての利用者責任が記述してあり、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
テスト	**適切な評価が実施された**
ATE_IND.1.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、TOEと同等の資源が提供されていることを確認している。
ATE_IND.1.2E	評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。

4.2 注意事項

特になし。

5 用語

本報告書で使用された略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
DB	DataBase
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

本報告書で使用された用語を以下に示す。

エレメント	監査ログは監査記録を複数の単位に分割して格納する。この分割の単位を監査ログエレメント（またはエレメント）と呼ぶ。
関数	予め複雑な演算処理の定義を登録しておき、SQL文から利用できる機能。
コマンド	PostgreSQL認証版を運用・管理するためのコマンド。
バックエンドプロセス	アプリケーションやコマンドの処理を行うTOEのプロセス。
作業用ファイル	資源ファイルのひとつ。処理途中のソート結果や中間データが格納される領域。
シーケンス	一意性のある番号を自動的に割り付ける機能。シーケンスは予め定義しておく（例：レコードが追加されるごとに、特定の列の値を1から順番に値を採番する）。
システムカタログ	利用者が利用するデータベースに対して、データベースの論理構造、格納構造、物理構造に関する情報が格納されている。
セキュリティパラメ	TOEにおいてアクセスや資源量の制御などセキュリティ

タ	に係るパラメタ。
動作環境ファイル	資源ファイルのひとつ。アプリケーションがデータベースをアクセスするふるまいを決定する定義が格納されている。
DDL文	データ定義文(Data Definition Language)。データベースの構造を定義し、データベースの作成、削除に使用するSQL文。
SQL	国際標準のリレーショナルデータベース操作言語。データベース構造を定義するDDLと、データベースへのデータ入力、登録、更新、変更、削除、検索などを行うDML(Data Manipulation Language)から構成される。

6 参照

[1] PostgreSQL 認証版　セキュリティターゲット 第1.0版 2007/3/9 株式会社エヌ・ティ・ティ・データ

[2] ITセキュリティ評価及び認証制度の基本規程　平成18年9月　独立行政法人 情報処理推進機構　EC-01

[3] ITセキュリティ認証手続規程　平成18年9月　独立行政法人 情報処理推進機構　EC-03

[4] 評価機関承認手続規程　平成18年9月　独立行政法人 情報処理推進機構　EC-05

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8] 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 バージョン2.3 2005年8月 CCMB-2005-08-001　(平成17年12月翻訳第1.0版)

[9] 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 バージョン2.3 2005年8月 CCMB-2005-08-002　(平成17年12月翻訳第1.0版)

[10] 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 バージョン2.3 2005年8月 CCMB-2005-08-003　(平成17年12月翻訳第1.0版)

[11] ISO/IEC 15408-1:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン2.3 2005年8月 (平成17年12月翻訳第1.0版)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] 補足-0512　平成17年12月

[18] PostgreSQL 認証版 Linux版 V8.1.5 評価報告書 第1.4版 2007/3/9 社団法人 電子情報技術産業協会 ITセキュリティセンター