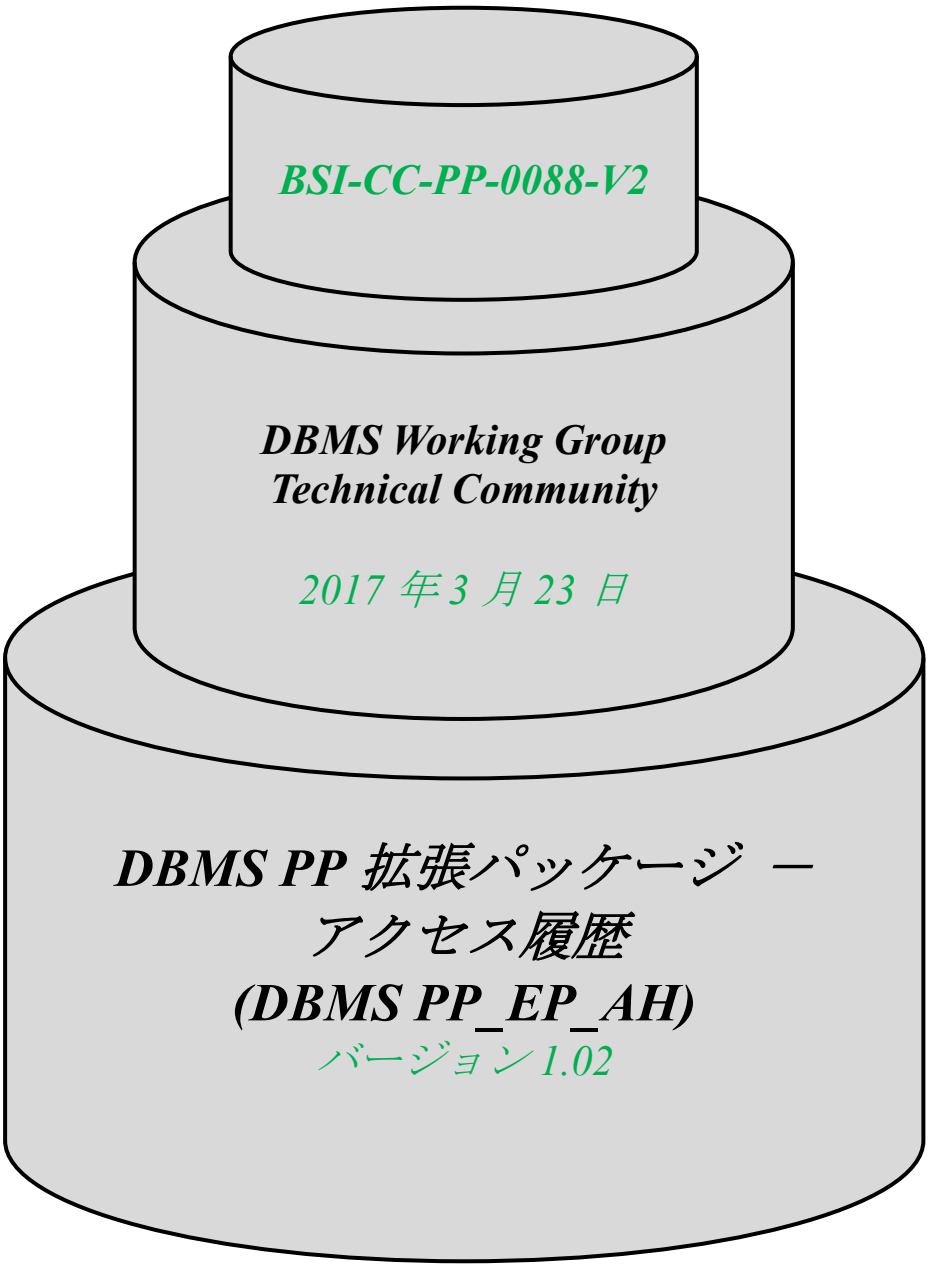

平成 29 年 10 月 25 日　翻訳第 1.0 版
独立行政法人情報処理推進機構
技術本部 セキュリティセンター
情報セキュリティ認証室

改版履歴

バージョン	日付	説明
1.0	2016 年 11 月 xx 日	拡張パッケージの具体化
1.01	2017 年 1 月 30 日	「DRAFT」の透かしを削除し、公開日付を追加
1.02	2017 年 3 月 23 日	認証者からのマイナーなコメントに対処

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：

DBMS PP 拡張パッケージ － アクセス履歴

コモンクライテリアバージョン：

本拡張パッケージは、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

表の目次

1 DBMS PP 拡張パッケージへの序説

1.1 DBMS PP 拡張パッケージの識別情報

タイトル：DBMS PP 拡張パッケージ － アクセス履歴

DBMS PP 拡張パッケージ略号：AH

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 R4

EP バージョン：1.02

発行日：2017 年 3 月 23 日

キーワード：データベース管理システム、DBMS PP、DBMS、COTS、アクセス履歴

1.2 DBMS PP 拡張パッケージ概要

ベース DBMS PP セキュリティ課題定義には、アクセス履歴に関するセキュリティ対策方針が含まれない。

多くの組織は、セキュリティ課題の一部としてこの対策方針を規定しないが、この追加のセキュリティ対策方針は、T.ACCESS_TSFDATA、T.IA_MASQUERADE と T.TSF_COMPROMISE の脅威のさらなる軽減を支援するために、いくつかの組織によってセキュリティ課題定義に含まれる必要があるかもしれない。これは、アクセス試行失敗を識別する支援のために、訓練された利用者に対して、それらのアクセス履歴のレビューを許可することによって達成される。

この拡張パッケージは、TOE セキュリティ対策方針 O.ACCESS-HISTORY とその対策方針を支援するセキュリティ機能要件の追加によって DBMS PP を補足する。

1.3 DBMS PP 拡張パッケージのフレームワーク

DBMS PP 拡張パッケージ － アクセス履歴は、[DBMS PP] 第 1.3 章で定義された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のフレームワークの一部である。ST 作成者は、オプションで、[DBMS PP] 第 3 章とともに定義された DBMS ベースプロテクションプロファイルに追加して拡張パッケージを規定する本文書を利用することができる。

1.4 拡張パッケージの構成

本文書は、以下のような構成である：

- 第 1 章は、DBMS PP 拡張パッケージへの序説を提供する。
- 第 2 章は、DBMS PP 拡張パッケージの適合主張を規定する。
- 第 3 章は、本 DBMS PP 拡張パッケージに適用可能なセキュリティ課題定義を含む。
- 第 4 章は、本 DBMS PP 拡張パッケージに適合する TOE によってカバーされる対策方針を定義する。
- 第 5 章は、本 DBMS PP 拡張パッケージで利用される拡張コンポーネントの定義を含む。
- 第 6 章は、本 DBMS PP 拡張パッケージ.データベース管理システムのセキュリテ

ィ要件定義を保持する。

1.5 参考文献

[DBMS PP]で与えられた参考文献は、本文書にも適用可能である。次の参考文献は、本文書にも適用される：

DBMS PP　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(ベースパッケージ) V2.12

1.6 文書の表記法

[DBMS PP]の 1.4 章で説明される文書の表記法は、本文書にも適用される。

2 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。

2.1 CC への適合

本拡張パッケージは、[DBMS PP] 第 3 章で規定された DBMS PP ベースの適合主張への追加はない。

2.2 拡張パッケージ適合規則

本拡張パッケージは、他の DBMS PP 拡張パッケージに依存しない。

本パッケージは、[DBMS PP]で定義されたバージョンにおいて、DBMS PP ベースパッケージと伴った場合にのみ主張が可能である。

本拡張パッケージは、公開時点では、他のいずれの DBMSPP 拡張パッケージとも競合しない。

3 セキュリティ課題定義

DBMS PP 拡張パッケージ － アクセス履歴のセキュリティ課題定義は、DBMS PP ベースのセキュリティ課題定義を変更しない。

3.1 脅威

本拡張パッケージは、[DBMS PP]で与えられた脅威を追加も変更もしない。

3.2 組織のセキュリティ方針

本拡張パッケージは、[DBMS PP]で与えられた組織のセキュリティ方針を追加も変更もしない。

3.3 前提条件

本拡張パッケージは、[DBMS PP]で与えられた前提条件を追加も変更もしない。

4 セキュリティ対策方針

本セクションでは、本拡張パッケージによって満たされる TOE 及びその支援環境の追加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。

4.1 TOE セキュリティ対策方針

本拡張パッケージは、[DBMS PP]で与えられたものに追加して、1 つの追加のセキュリティ対策方針を規定する。

表 1：追加の 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。

4.2 運用環境のセキュリティ対策方針

本拡張パッケージは、[DBMS PP]で与えられる運用環境のセキュリティ対策方針を追加も変更もしない。

4.3 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に関連する方針の要約、及び脅威を与える。

セキュリティ対策方針カバレージ

表 2：TOE の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 (from DBMS PP base) T.ACCESS_TSFDATA (from DBMS PP base) T.IA_MASQUERADE (from DBMS PP base)

セキュリティ対策方針の十分性の根拠

以下の表は、TOE のセキュリティ対策方針の根拠を与える。本拡張パッケージにおいてセキュリティ対策方針 O.ACCESS_HISTORY は、ベース DBMS PP で与えられた脅威 T.ACCESS_TSFDATA、T.IA_MASQUERADE 及び T.TSF_COMPROMISE の軽減を支援する。

表 3：TOE セキュリティ対策方針の十分性についての追加の根拠

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。
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 なりすまし試行の表示に違いない、TOE を用いた認証の試行失敗のログ出力の要求は、脅威の更なる低減を支援するだろう
T.TSF_COMPROMISE 利用者または利用者を代行して動作するプロセスが、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。

5 拡張セキュリティ機能要件

本拡張パッケージは、1 つの拡張 SFR を定義する。

5.1 本拡張パッケージにより規定される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. セション確立試行の連続した失敗の累積回数。

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. 最後のセション確立成功、及び

b. 最後のセション確立試行の失敗、及び最後のセション確立成功以後の試行失敗回数

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。

5.2 拡張セキュリティ機能要件の根拠

以下の表は、本拡張パッケージで見つかった拡張セキュリティ機能要件の包含についての根拠を示す。

表 4：拡張セキュリティ機能要件の根拠

拡張要件	識別子	根拠
FTA_TAH_(EXT).1	TOE アクセス履歴	本 PP は、TOE にクライアントを含むことを要求しない。ゆえに、PP は、クライアントがメッセージを表示することを要求できない。本要件は、TOE がアクセス履歴を表示する代わりに、それを格納し、取り出すことを要求するように改変された。

6 セキュリティ要件

6.1 ベース DBMS PP に追加されるセキュリティ機能要件

本セクションでは、本拡張パッケージにより追加される、または規定される TOE の機能要件を定義する。

本拡張パッケージの機能要件は、拡張コンポーネントの利用を含めて、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った。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 5 : セキュリティ機能要件

機能コンポーネント	
FTA_TAH_(EXT).1	TOE アクセス履歴

TOE アクセス (FTA)

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. セション確立試行の連続した失敗の累積回数。

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. 最後のセション確立成功、及び

b. 最後のセション確立試行の失敗、及び最後のセション確立成功以後の試行失敗回数

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。

6.2 ベース DBMS PP から詳細化されたセキュリティ機能要件

表 6 : 本 EP によって改変された DBMS PP 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

セキュリティ監査（FAU）

FAU_GEN.1 監査データ生成

[DBMS PP]で与えられた、表 8、監査対象事象は、以下のエントリーを追加するよう詳細化された。

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
FTA_TAH_(EXT).1	なし	なし

6.3 追加の TOE セキュリティ機能要件の根拠

以下の表は、セキュリティ機能要件野選択のための根拠を提供する。それぞれの 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たどる。

表 7：TOE セキュリティ機能要件の根拠

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)

6.4 すべてのセキュリティ機能要件の依存性の根拠

本拡張パッケージは、依存性を持った追加の SFR を含まない。

6.5 セキュリティ保証要件

本拡張パッケージは、[DBMS PP]で与えられたセキュリティ保証要件を追加も変更もしない。