認 証 報 告 書

東京都文京区本駒込2丁目28番8号
独立行政法人情報処理推進機構
理事長　富田　達夫

原紙押印済

IT製品（TOE）

申請受付日（受付番号）	令和元年11月6日（IT認証9726）
認証識別	JISEC-C0673
製品名称	Microsoft SQL Server 2017 on Linux Database Engine Enterprise Edition x64 (English)
バージョン及びリリース番号	14.0.3223.3
製品製造者	Microsoft Corporation
機能要件適合	プロテクションプロファイル適合、CCパート2拡張
プロテクションプロファイル	DBMS Working Group Technical Community, Protection Profile for Database Management Systems (DBMS PP) Base Package, Version 2.12, March 23rd, 2017 and DBMS Working Group Technical Community, DBMS PP Extended Package - Access History (DBMS PP_EP_AH), Version 1.02, March 23rd, 2017 (認証識別：BSI-CC-PP-0088-V2-2017)
保証パッケージ	EAL2 及び追加の保証コンポーネントALC_FLR.2
ITセキュリティ評価機関の名称	TÜV Informationstechnik GmbH, Evaluation Body for IT-Security

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。
令和2年6月15日

セキュリティセンター セキュリティ技術評価部
技術管理者　矢野 達朗

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 3.1 Release 5
② Common Methodology for Information Technology Security Evaluation Version 3.1 Release 5

評価結果：合格

「Microsoft SQL Server 2017 on Linux Database Engine Enterprise Edition x64 (English)」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証等に関する要求事項に従い、

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

この認証報告書は、Microsoft Corporation が開発した「Microsoft SQL Server 2017 on Linux Database Engine Enterprise Edition x64 (English)、バージョン 14.0.3223.3」(以下「本 TOE」という。) について TÜV Informationstechnik GmbH, Evaluation Body for IT-Security（以下「評価機関」という。）が令和 2 年 5 月 29 日に完了した 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 Microsoft Corporation に報告するとともに、本 TOE に関心を持つ調達者や消費者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、10 章のセキュリティターゲット（以下「ST」という。）を併読されたい。特に本 TOE のセキュリティ機能要件、保証要件及びその十分性の根拠は、ST において詳述されている。

本認証報告書は、市販される本 TOE を購入する調達者、及び一般消費者を読者と想定している。本認証報告書は、本 TOE が適合する保証要件に基づいた認証結果を示すものであり、個別の IT 製品そのものを保証するものではないことに留意されたい。

1.1 評価対象製品概要

本 TOE の機能、運用条件の概要を以下に示す。詳細は 2 章以降を参照のこと。

1.1.1 プロテクションプロファイルまたは保証パッケージ

本 TOE は、次のプロテクションプロファイル[14] （以下「適合 PP」という。）に適合する。

DBMS Working Group Technical Community, Protection Profile for Database Management Systems (DBMS PP) Base Package, Version 2.12, March 23rd, 2017, and

DBMS Working Group Technical Community, DBMS PP Extended Package - Access History (DBMS PP_EP_AH), Version 1.02, March 23rd, 2017 (認証識別: BSI-CC-PP-0088-V2-2017)

本 TOE の保証パッケージは、EAL2 及び追加の保証コンポーネント ALC_FLR.2 である。

1.1.2 TOEとセキュリティ機能性

本 TOE は、Microsoft 社製のデータベース管理システム（SQL Server 2017 on Linux）を構成するソフトウェアコンポーネントのコア部分である。SQL Server 2017 on Linux は本 TOE であるデータベースエンジンに、各種サポートツール（レプリケーション機能、機械学習サービス、全文検索機能、外部データソースへの接続機能、各種データ解析ツール、ユーザデータベース管理 UI ツール、クライアント開発支援ツール等）が付加される形で構成される。

本 TOE は、データベース管理システム用の Protection Profile である適合 PP[14]で要求されるセキュリティ機能を提供する。

これらのセキュリティ機能性について、その設計方針の妥当性と実装の正確性について保証パッケージの範囲で評価が行われた。本 TOE が想定する脅威及び前提については次項のとおりである。

1.1.2.1 脅威とセキュリティ対策方針

本 TOE は、以下のとおりのセキュリティ機能によりそれぞれの脅威に対抗する。

TOE が扱うデータベースや、セキュリティ機能に関する設定情報等の保護資産に対して、不正なアクセスが行われることによる、暴露、改ざんの脅威が存在する。

本 TOE ではこの脅威に対抗するため、利用者を識別認証し、その利用者に許可された操作のみが行えるようにアクセス制御を行う。また、セキュリティ事象に関する監査データを生成し管理することにより、不正な操作を検知できるようにする。

1.1.2.2 構成要件と前提条件

評価対象製品は、次のような構成及び前提で運用することを想定する。

本 TOE は、TOE が動作するために必要なソフトウェア（OS 等）と共に専用のサーバにインストールされ、ネットワーク経由で接続されたクライアントと通信を行う環境で使用されることを想定している。

本 TOE がインストールされるサーバは、物理的な不正アクセスから保護されるような環境に設置され、サーバ・クライアント間の通信内容の改変や盗聴は防止されるようなネットワーク環境で運用されることを想定する。

1.1.3 免責事項

TOE の運用環境におけるサーバ･クライアント間の通信データの保護については保証の対象外であり、運用者の責任において対策されなければならない。

1.2 評価の実施

認証機関が運営する IT セキュリティ評価及び認証制度に基づき、公表文書「IT セキュリティ評価及び認証制度の基本規程」[1]、「IT セキュリティ認証等に関する要求事項」[2]、「IT セキュリティ評価機関承認等に関する要求事項」[3]に規定された内容に従い、評価機関によって本 TOE に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、令和 2 年 5 月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[13]、及び関連する評価証拠資料を検証し、本 TOE の評価が所定の手続きに沿って行われたことを確認した。認証機関が指摘した問題点は、すべて解決され、かつ、TOE の評価が CC（[4][5][6]または[7][8][9]）及び CEM（[10][11]のいずれか）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。

2 TOE識別

本 TOE は、以下のとおり識別される。

TOE名称：	Microsoft SQL Server 2017 on Linux Database Engine Enterprise Edition x64 (English)
バージョン：	14.0.3223.3
開発者：	Microsoft Corporation

製品が評価･認証を受けた本 TOE であることを、利用者は以下の方法によって確認することができる。

マニュアルに記載された手順に従い、TOE バージョン取得のための SQL コマンドを運用中の TOE に送信することにより TOE のバージョンが得られ、TOE 構成品一覧の当該記載を比較することにより、設置された製品が評価を受けた本 TOE であることを確認できる。

3 セキュリティ方針

本章では、本 TOE が脅威に対抗するために採用したセキュリティ機能方針や組織のセキュリティ方針を説明する。

TOE は内部で管理するデータベースに対する不正なアクセスに対抗するための、セキュリティ機能を提供する。

TOE は組織のセキュリティ方針を満たすため、セキュリティに関連する事象について監査データを生成し、生成された監査データを適切に管理する機能を提供する。

また、上記セキュリティ機能に関する各種設定をシステム管理者のみが行えるよう制限することで、セキュリティ機能の無効化や不正使用を防止する。

本 TOE のセキュリティ機能において保護の対象とする資産を以下に示す。

(1) 保護資産（利用者データ）

- データベース内に格納、管理するユーザ情報
- 一般に DBMS メタデータの呼び名で知られている、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情報
- 利用者が作成し、TOE 内で管理されるストアドプロシージャ等のクエリー情報

(2) 保護資産（主な TSF データ）

- セキュリティ機能に関する各種設定情報
- ユーザアカウント情報やロール定義に関する情報
- セキュリティ監査データ

3.1 セキュリティ機能方針

TOE は、3.1.1 に示す脅威に対抗し、3.1.2 に示す組織のセキュリティ方針を満たすセキュリティ機能を具備する。

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

本 TOE は、表 3-1 に示す脅威を想定し、これに対抗する機能を備える。

表3-1 想定する脅威

識別子	脅威
T.ACCESS_TSFDATA	A threat agent may read or modify TSF data using functions of the TOE without the proper authorization.
T.ACCESS_TSFFUNC	A threat agent may use or manage TSF, bypassing the protection mechanisms of the TSF.
T.IA_MASQUERADE	A user or a process acting on behalf of a user may masquerade as an authorized entity in order to gain unauthorized access to user data, TSF data, or TOE resources.
T.IA_USER	A threat agent may gain access to user data, TSF data, or TOE resources with the exception of public objects without being identified and authenticated.
T.RESIDUAL_DATA	A user or a process acting on behalf of a user may gain unauthorized access to user or TSF data through reallocation of TOE resources from one user or process to another.
T.TSF_COMPROMISE	A user or a process acting on behalf of a user may cause configuration data to be inappropriately accessed (viewed, modified or deleted), or may compromise executable code within the TSF.
T.UNAUTHORIZED_ ACCESS	A threat agent may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.

3.1.1.2 脅威に対するセキュリティ機能方針

表 3-1 に示す全ての脅威は、TOE の正当な利用者以外の者、もしくは正当な権限を有さない者による利用者情報、TSF 情報への侵害（閲覧、改ざん）に関するものである。これら脅威に対しては、以下のセキュリティ機能方針で対抗する。

(1) 識別認証機能

TOE を利用しようとする者が正当な利用者であることを検証し、正当な利用者のみに TOE へのアクセスを許可する機能である。本機能を実現するメカニズムとして、Active Directory 認証方式と SQL Server 認証方式があり、システム管理者が利用者アカウントを生成する際に、そのアカウント毎にいずれかの方式を選択する。以下に両認証方式について説明する。

（Active Directory 認証方式）

運用環境に存在する Active Directory を利用して、利用者を識別認証する方

式。Active Directory との連携に際して、Active Directory アカウントの利用者情報を取り扱う TOE の設定として、次の二つの方法のいずれかを選択する。

— TOE が、Linux プラットフォームのシステムサービスを利用する方法
— TOE が、TOE 内部の LDAP の実装を使用する方法

その上で、Active Directory と連携するために、利用者認証に、Linux プラットフォームの Kerberos プロトコル対応ソフトウェアを使用する。

（SQL Server 認証方式）

入力されたログイン名、パスワードを、TOE が管理する利用者のアカウント情報と照合し利用者の正当性を TOE 自身が検証する方式。

認証に成功した利用者に対して、そのアカウントに割り当てられた利用者役割での TOE の利用を許可する。

(2) セキュリティ管理機能

ユーザアカウントに関する操作（生成、削除、権限変更等）、データベースアクセス権限に関する操作、その他セキュリティに関する設定変更等については、利用者権限に従いアクセス制御を実施する。本 TOE はこれらの操作を、システム管理者権限を有する利用者のみに許可することにより、不正なアクセスを防ぐ。

(3) アクセス制御機能

各データベースに対する操作毎の許可、拒否を定義したアクセス制御リストを管理し、このアクセス制御リストと、上記識別認証機能により識別された利用者アカウントの情報を使用し、利用者からの操作が要求されたタイミングでアクセス制御を行うことで、データベースに対する不正なアクセスに対抗する。以下にアクセス制御機能の詳細について説明する。

本機能では、TOE 内で保持されるデータベース毎に、以下の権限リストを管理する。

— 特定のアカウントに対する、データベース操作毎（作成、改変、参照、削除等）の明示的な許可、もしくは拒否のリスト
— 特定の役割に対する、データベース操作毎の明示的な許可、もしくは拒否のリスト（各役割、及び各役割に属するアカウント情報はデータベース、及び関連するオブジェクト毎に管理される）。

TOE に対するデータベース操作要求（SQL）がクライアントを介して利用者から送信される度に、利用者情報とこの権限リストを参照し、以下の規則に従ったアクセス制御を実施する。

1. 利用者から要求された操作について、その利用者アカウントに対する明示的な拒否が規定されている場合はその操作を拒否する
2. 利用者から要求された操作について、その利用者アカウントが属する役割に対する明示的な拒否が規定されている場合はその操作を拒否する
3. 利用者から要求された操作について、その利用者アカウントに対する明示的な許可が規定されている場合はその操作を許可する
4. 利用者から要求された操作について、その利用者アカウントが属する役割に対する明示的な許可が規定されている場合はその操作を許可する
5. 上記規則のいずれにも該当しない場合は、その操作を拒否する

但し、システム管理者、及びデータベースを作成した利用者（データベース所有者）は、そのデータベースに対する全ての操作が許可される。本機能で使用される役割は、TOE により予め提供される既定の役割（db_datareader：データベースの全てのテーブル情報の参照権限を有する役割、db_datawriter：データベースの全てのテーブル情報の追加、削除、変更権限を有する役割 等）もしくは、システム管理者及びデータベース所有者が新たに定義した役割が用いられる。

(4) ユーザセッション管理機能

上記識別認証機能により識別された利用者アカウントの情報を使用し、予めシステム管理者により設定されたセキュリティポリシーに反する TOE へのアクセスを制限する。セキュリティポリシーには、TOE へのアクセスを制限する特定の利用者アカウント、日時や曜日、最大同時接続数等が設定される。TOE は利用者からのアクセスが行われた際に、このセキュリティポリシーを基にそれ以降の利用者操作を許容するかどうか判断する。

その他、脅威の軽減を支援する目的で、TOE は次の情報を利用者に提供する機能を有する。

- 最後にログインに成功した時刻
- 最後にログインに失敗した時刻、及び最後のログイン成功から現在のログイン成功までの間のログイン試行の回数

(5) 残存情報削除機能

利用者による TOE へのアクセスに伴い再利用されるメモリ領域については、予め特定パターンでの上書き処理が実行され、以前の残存情報が利用できないようにする。

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

3.1.2.1 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を表 3-2 に示す。

表 3-2 組織のセキュリティ方針

識別子	組織のセキュリティ方針
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.ROLES	Administrative authority to TSF functionality shall be given to trusted personnel and be as restricted as possible supporting only the administrative duties the person has. This role shall be separate and distinct from other authorized users.
P.USER	Authority shall only be given to users who are trusted to perform the actions correctly.

3.1.2.2 組織のセキュリティ方針に対するセキュリティ機能方針

TOE は、表 3-2 に示す組織のセキュリティ方針を満たす機能を具備する。

⑴ 組織のセキュリティ方針「P.ACCOUNTABILITY」への対応

このセキュリティ方針は、TOE 利用者の操作に対して責任追跡性を求めている。TOE ではこの方針を実現するため、以下に示すセキュリティ監査機能を提供し、セキュリティ機能に関する全ての事象についての監査ログを生成し、監査ログファイルとして管理することで、利用者アクションについての責任追跡性を実現する。

・セキュリティ監査機能

TOE は、監査対象となるセキュリティ事象が発生した際に、事象種別、利用者識別、発生日時、結果等の項目から成る監査ログを生成し、監査ログファイルとして保存する。また生成した監査ログファイルを読み出すためのインタフェースをシステム管理者に対して提供する。生成された監査ログファイルは OS の提供するアクセス制御機能により保護される。

また、監査ログの事象発生日時を記録するため、日付、時間情報を OS のシステム時計から取得する。

⑵ 組織のセキュリティ方針「P.ROLES」、「P.USER」への対応

これらのセキュリティ方針は、TOE を安全に管理するための制限的な役割を一般利用者とは独立した形で定義すると共に、利用者の権限管理を適切に実施することを求めている。

本 TOE ではセキュリティ機能に関する管理権限を有するシステム管理者役割を定義し、一般利用者と区別して管理するメカニズムと、3.1.1.2 に記載のセキュリティ管理機能及びユーザセッション管理機能により、このセキュリティ方針を実現する。

4 前提条件と評価範囲の明確化

本章では、想定する読者が本 TOE の利用の判断に有用な情報として、本 TOE を運用するための前提条件及び運用環境について記述する。

4.1 使用及び環境に関する前提条件

本 TOE を運用する際の前提条件を**表 4-1** 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 4-1 前提条件

識別子	前提条件
Physical aspects (物理的側面)	
A.PHYSICAL	It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.
Personnel aspects (人的側面)	
A.AUTHUSER	Authorized users possess the necessary authorization to access at least some of the information managed by the TOE.
A.MANAGE	The TOE security functionality is managed by one or more competent administrators. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.
A.TRAINEDUSER	Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.
Procedural aspects (手続き的側面)	
A.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration, and support of the DBMS.

識別子	前提条件
A.PEER_FUNC_&_MGT	All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality and to be properly managed and operate under security policy constraints compatible with those of the TOE.
A.SUPPORT	Any information provided by a trusted entity in the IT environment and used to support the provision of time and date, information used in audit capture, user authentication, and authorization that is used by the TOE is correct and up to date.
Connectivity aspects (接続性の側面)	
A.CONNECT	All connections to and from remote trusted IT systems and between separate parts of the TSF are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.

4.2 運用環境と構成

本 TOE は物理的に保護された環境に置かれたサーバマシン上に、OS と共にインストールされ、ネットワークを介して接続されるクライアントから利用される。

クライアントとの通信は、TOE 開発者から提供されるコマンド通信用のツールや、TOE と共に製品に含まれる開発支援ツール等を利用して、独自に開発されたクライアントアプリケーションを利用して行われることを想定している。

サーバマシンを構成するハードウェア、及び OS 等の関連ソフトウェアについては、その信頼性も含め本評価の範囲ではない（十分に信頼できるものとする）。

TOE がインストールされるサーバマシンに必要となる、ハードウェアスペック、TOE 以外のソフトウェアを**表 4-2**、**表 4-3** に示す。

表 4-2　ハードウェア要件

CPU	x64互換、最低2コア以上かつ2GHz以上のCPU
RAM	最小3.25GB

Hard Disk	最小6GB

表 4-3　ソフトウェア要件

OS	Red Hat Enterprise Linux Server 7.3
Other software	OpenSSL Library Active Directory 認証方式を選択した場合: realmd , Kerberos Client package, System Security Services Daemon (SSSD), Name Service Switch (NSS)
	Active Directory 認証方式を選択した場合、別途 Active Directory (AD) 認証サーバが必要。

4.3　運用環境におけるTOE範囲

4.2 に示した通り、本 TOE はサーバマシン上にインストールされたソフトウェア製品である。

本 TOE の提供する機能、及び、本評価で保証される本 TOE の機能には、以下の制約がある。

(1) 通信データの保護

TOE の運用環境におけるサーバ・クライアント間の通信データを保護することは、管理者の責任である。

(2) Active Directory 認証サーバ

Active Directory 認証方式を選択した場合、TOE は、TOE 外の Linux プラットフォームにインストールされる**表 4-3** に記載されたソフトウェア及び Active Directory 認証サーバに依存する。

Linux プラットフォームの**表 4-3** に記載されたソフトウェア及び環境設定を適切に管理し、並びに Active Directory 認証サーバで管理される利用者情報及び認証メカニズムをセキュアに保つことは管理者の責任である。

5 アーキテクチャに関する情報

本章では、本 TOE の範囲と主要な構成を説明する。

5.1 TOE境界とコンポーネント構成

本TOEはOS (Operating System)上の１アプリケーションとして動作する。TOEの内部構成を図 5-1 に示す。TOE は図 5-1 の斜線部分であり、Local SQL Client、Remote SQL Client、Other parts of SQL Server Platform、及び Resources of the OS は TOE に含まない。

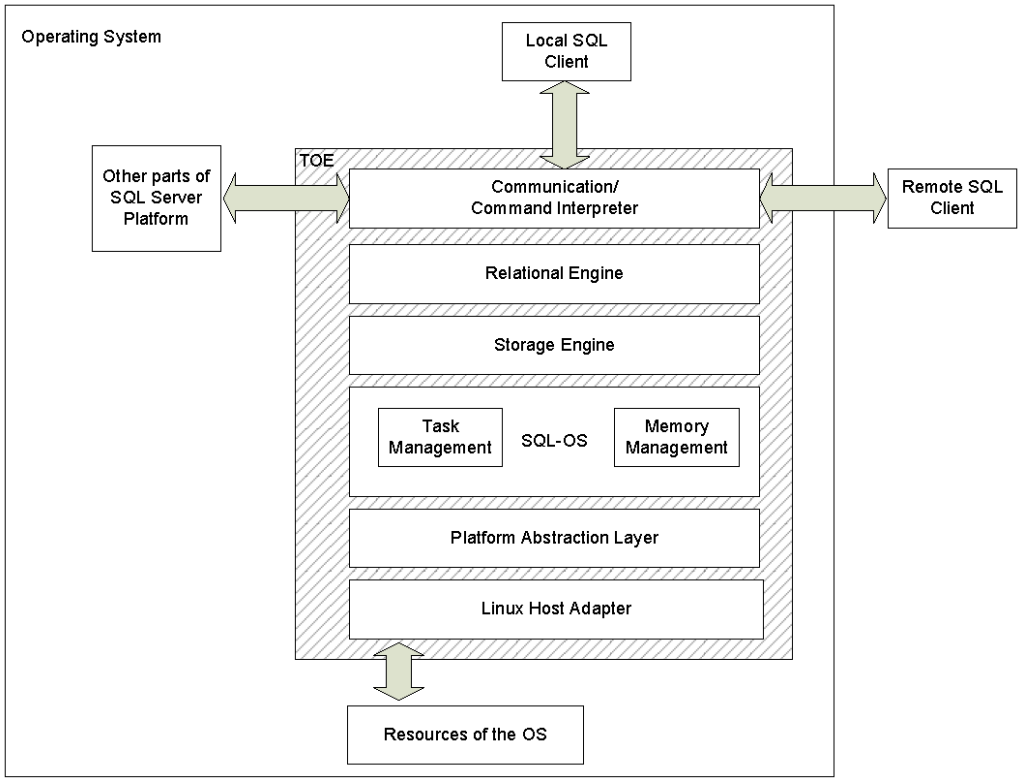

図 5-1　TOE境界

以下に各コンポーネントの概要を示す。

Communication/Command Interpreter

TOE外部との通信処理を担うコンポーネント。クライアント等の外部から送信されるSQL受信処理、及び外部へのレスポンス処理は全てこのコンポーネントを通じて行われる。

Relational Engine

データベース操作処理、及びセキュリティ機能関連処理のメインとなるコンポーネント。Communication/Command Interpreterを介して受信したSQLス

テートメントの解釈、権限チェックを行い、データベースに対する内部処理として実行し、必要なレスポンスを送信する。

Storage Engine

データベースや関連オブジェクトを格納するメモリ、HDD等の物理的なストレージ情報を管理するコンポーネント。Relational Engineからの要求に従い、必要な格納アドレス等の情報を受け渡す。

SQL-OS

TOEが動作するために必要となる各種内部リソースの管理等を行うコンポーネント。本コンポーネントは、主にスレッドのスケジューリング等を行うTask Management部と、内部で使用するメモリリソースの管理を行うMemory Management部とで構成される。

Platform Abstraction Layer

TOEの上位層にWindows互換のインタフェースを提供するコンポーネント。Windows DLLやWindows OSへの呼出をLinux Host Adapter インタフェースへの呼出に変換する。

Linux Host Adapter

Platform Abstraction Layerを初期化するLinuxの実行可能形式。Platform Abstraction Layerからの要求に応じて、Linux OSのリソースへのアクセスを提供する。

5.2 IT環境

本 TOE はハードウェアとオペレーティングシステム上で動作し、ネットワーク経由でクライアントから送信される SQL ステートメントを処理する。

TOE が提供するセキュリティ機能の一部は、TOE 自身と Linux プラットフォームが提供する機能との組み合わせにより実現される。以下については IT 環境である Linux プラットフォームの提供する機能により実現される。

・Active Directory 認証方式を使用する場合であって、SSSD 及び NSS を使用する場合の、Windows SID と Linux のユーザ識別子及びグループ識別子とのマッピング

・パスワードのハッシュ処理

・生成されたログデータの保護

・監査ログに使用される日時情報の提供

6 製品添付ドキュメント

本 TOE に添付されるドキュメントの識別を以下に示す。TOE の利用者は、前提条件を満たすため下記ドキュメントの十分な理解と遵守が要求される。

SQL Server 2017 on Linux Database Engine – Common Criteria Evaluation (EAL2+) - Guidance Addendum, Version 2.3, 2020-05-22

Microsoft SQL Server 2017 Technical Documentation (2019-09-09)
(File name: Offline-Book.SQL-Server-2017-CU16.zip)

これらのドキュメントは下記 Web サイトからのダウンロードにより提供される。TOE 利用者は TOE の購入時に下記 Web サイトを参照する必要がある。

https://www.microsoft.com/en-us/sql-server/data-security

7 評価機関による評価実施及び結果

7.1 評価機関

評価を実施した TÜV Informationstechnik GmbH, Evaluation Body for IT-Security は、IT セキュリティ評価及び認証制度により承認されるとともに、ILAC（国際試験所認定協力機構）の相互承認に加盟している認定機関（独立行政法人製品評価技術基盤機構認定センター）により認定を受けており、評価品質維持のためのマネジメント及び要員等の適切性についての要求事項を満たしていることが定期的に確認されている。

7.2 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た。評価報告書では、本 TOE の概要と、CEM のワークユニットごとの評価内容及び判断結果を説明する。

7.3 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、令和元年 11 月に始まり、令和 2 年 5 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、IT セキュリティ評価及び認証制度の監督の下、平成 30 年 1 月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付の各ワークユニットに関するプロセスの施行状況の調査を行った。また、評価機関においてテスト環境を構築し、開発者テストのチェック及び評価者テストを実施した。

評価作業中に発見された問題点は、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、認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。

これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

7.4 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テスト及び脆弱性評定に基づく侵入テストを実行した。

7.4.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価者が評価した開発者テストの内容を以下に説明する。

(1) 開発者テスト環境

表 4-3 の中で、OS に関するシステム要件として、Red Hat Enterprise Linux Server 7.3 が指定されている。これら OS に対応して、開発者が実施したテスト構成を表 7-1 に示す。

表 7-1 開発者テスト構成

構成品		概要
TOE		Microsoft SQL Server 2017 on Linux Enterprise Edition - x64 (English), version 14.0.3223.3 (including CU16)
動作環境		TOEがインストールされた動作環境。以下の構成を用いる。
	Hardware	Intel(R) Xeon(R) CPU E5-2650 v4 @ 2.2GHz (2 processors), 4 GB RAM
	Hypervisor	VMware ESXi Version 6.5.0
	OS	Red Hat Enterprise Linux Server 7.3 **表 4-3**のOther softwareを含む。
	追加のソフトウェア	SQL-OSの内部インタフェースをテストするためのファイル

Active Directory 認証方式を実現するために、Windows マシン上に構成された Active Directory 認証サーバを用意し、表 7-1 に示したマシンを Active Directory 認証サーバが管理するドメインに参加させた状態でテストを実施した。

これらの開発者テスト構成は、開発者が選択したものであり、いずれの開発者テスト構成においても、物理マシン上に hypervisor をインストールし、その上にゲスト OS をインストールした動作環境に、TOE をインストールして評価を行っている。

ST[12]では、ST に記載された要件を満たす OS を物理マシン上に直接インストールすることを求めていないため、これらの開発者テスト構成は、ST[12]に記載されたシステム要件と整合すると評価者は判断した。

(2) 開発者テスト概説

開発者テストの概説は以下のとおりである。

a) テスト概要

開発者テストの概要は、以下のとおりである。

＜開発者テスト手法＞

開発者テストは、TOE の外部インタエースであるクライアントとの通信インタフェースに対して SQL を送信し、SQL の操作が反映されたデータベースの内容、TOE からの応答メッセージ（エラーメッセージ等）を観察する手法が取られた。

実際のテストでは、スクリプト化された一連の SQL を TOE に送信し、同様にスクリプトとして記述された処理結果の確認方法に従い自動的に結果を判断し､テスト結果として出力するテストツールが開発者によって開発され、このツールとスクリプト（テストシナリオ）によってテストが実施されている。

尚、本テストツール及びテストシナリオの妥当性については、設計仕様、及びドキュメントとの整合性も含め評価者により確認されている。

＜開発者テストの実施内容＞

開発者テストでは、前記テストツールを用いて、各種スクリプト（テストシナリオ）を実行し、スクリプトに記述された確認方法に従いツールが判断したテスト結果をテストログとして出力し、その内容を確認した。

また、アクセス制御機能に関する幾つかのテストについては、複数のクライアントを想定し、マルチセッション環境での確認が行われている。

b) 開発者テストの実施範囲

開発者テストは開発者によって177項目実施された。カバレージ分析によって、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースがテストされたことが検証された。

c) **結果**

評価者は、開発者テストの実施方法、実施項目の正当性を確認し、テスト計画書に示された実施方法と実際の実施方法が一致することを確認した。評価者は、開発者が期待したテスト結果と開発者によって実施されたテスト結果が一致していることを確認した。

7.4.2 評価者独立テスト

評価者は、開発者テストから抽出したテスト項目を使用して製品のセキュリティ機能が実現されていることを再確認するサンプルテストを実施するとともに、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実現されていることをより確信するための評価者独立テスト（以下「独立テスト」という。）を実施した。評価者が実施した独立テストを以下に説明する。

(1) 独立テスト環境

評価者が実施した独立テストの構成を、表 7-2 に示す。

表 7-2 独立テスト構成

構成品		概要
TOE		Microsoft SQL Server 2017 on Linux Enterprise Edition - x64 (English), version 14.0.3223.3 (including CU16)
動作環境		TOEがインストールされた動作環境。以下の構成を用いる。
	Hardware	Intel(R) Xeon(R) CPU E5-2650 v4 @ 2.20GHz (2 processors), 3.9 GB RAM
	Hypervisor	VMware ESXi Version 6.7.0
	OS	Red Hat Enterprise Linux Server 7.3

Active Directory 認証方式を実現するために、Windows マシン上に構成された Active Directory 認証サーバを用意し、表 7-2 に示したマシンを Active Directory 認証サーバが管理するドメインに参加させた状態でテストを実施した。

評価者テストは開発者テスト同様、本 ST において識別されている TOE 構成に整合すると評価者が判断した TOE テスト環境で実施されている。尚、クライアントマシンには SQL ステートメントを送信するためのテストツール等がインストールされる。

(2) 独立テスト概説

評価者の実施した独立テストは以下のとおりである。

a) 独立テストの観点

評価者が､開発者テスト及び提供された評価証拠資料から考案した独立テストの観点を以下に示す。

＜独立テストの観点＞

① セキュリティに関する複数の操作（アカウント生成、権限操作、データベース操作）を組み合わせのバラエティを増やし、一連の処理として実行する

② TOE に対する SQL 送信処理、及びレスポンスの取得処理について、開発者テストと異なるツールを用いてテストを実施する

③開発者テストの妥当性について確信を得るため､全ての開発者テスト項目を評価者が実施し同じ結果が得られることを確認する

b) 独立テスト概要

評価者が実施した独立テストの概要は以下のとおりである。

＜独立テスト手法＞

独立テストは､開発者テストと同様にクライアントとの通信インタフェースに対して SQL を送信し、SQL の操作が反映されたデータベースの内容、TOE からの応答メッセージ（エラーメッセージ等）を観察する手法が取られたが､テスト環境のバラエティを増やしより高い信頼性を得るために､開発者テストで使用されたツールとは異なる確認手段を用いている。

＜独立テストツール＞

独立テストでは、SQL 送信等を行うためのコマンドラインツールである Microsoft Command Line Utilities for SQL Server を使用し、一連の SQL 処理を実行するためのスクリプトを評価者が開発した。

＜独立テストの実施内容＞

独立テストは、評価者によって 11 項目実施された。サンプリングテストでは、全ての開発者テスト項目(177 項目)が実施されている。また、TOE

の配付､インストール処理等がガイダンスに記載された通りに実施できることを確認するための関連テスト(6 項目)も評価者により実施されている。

独立テストの観点とそれに対応したテスト内容を表 7-3 に示す。

表 7-3 実施した独立テスト

観点	テスト概要
①、②	・ユーザアカウント生成、各種デフォルトの役割の設定、新規役割の定義・設定、データベース作成、データベース操作の一連のSQLを実行し定義された権限に従ったアクセス制御が実行されることを確認する。また、一連の監査ログが正しく生成されていることを確認する。 ・識別認証機能の正常系、異常系に関するテストを、TOEが提供する2種類の認証方式について開発者テストと異なる通信ツール、及び異なるアカウント設定を用いて実施し開発者テストと一貫した結果が得られることを確認する。

c) 結果

評価者が実施したすべての独立テストは正しく完了し、評価者は TOE のふるまいを確認した。評価者は、すべてのテスト結果と期待されるふるまいが一致していることを確認した。

7.4.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性となる可能性があるものについて、必要と思われる評価者侵入テスト（以下「侵入テスト」という。）を考案し実施した。評価者が実施した侵入テストを以下に説明する。

(1) 侵入テスト概説

評価者が実施した侵入テストの概説は以下のとおりである。

a) 懸念される脆弱性

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

① パスワードの総当たり攻撃により識別認証機能がバイパスされる可能性がある。
② 不正なフォーマット、パラメタを用いたクライアントからの要求によりTOEのセキュリティ機能がバイパスされる可能性がある
③ 識別認証情報として不正なフォーマットのデータや特殊文字コード等が使用されることによりセキュリティ機能がバイパスされる可能性がある。
④ 意図しないネットワークポートインタフェースが存在し、そこからTOEに不正にアクセスされる可能性がある。
⑤ メモリ上の残存情報やファイルシステムに直接アクセスすることにより、保護資産に対して不正にアクセスされる可能性がある。
⑥ 過去のバージョンの製品等に存在する脆弱性が本TOEに残存し、それを悪用することによってセキュリティ機能がバイパスされる可能性がある。

b) **侵入テストの概要**

評価者は、潜在的な脆弱性が悪用される可能性を検出するために、以下の侵入テストを実施した。

＜侵入テスト構成＞

表 4-3 の中で、OS に関するシステム要件として、Red Hat Enterprise Linux Server 7.3が指定されている。このOSに対応した侵入テスト構成を、表 7-4 に示す。

表 7-4　侵入テスト構成

構成品		概要・利用目的
TOE		Microsoft SQL Server 2017 on Linux Enterprise Edition - x64 (English), version 14.0.3223.3 (including CU16)
動作環境		TOEがインストールされた動作環境。以下の構成を用いる。
	Hardware	Intel(R) Xeon(R) CPU E5-2650 v4 @ 2.20GHz (2 processors), 4 GB RAM
	Hypervisor	VMware ESXi Version 6.7.0
	OS	Red Hat Enterprise Linux Server 7.3 **表 4-3**のOther softwareを含む。
	Software	①Netstat ②top
Client PC		Windows 10 Proマシンであり、侵入テストのため以

構成品	概要・利用目的
	下のツールを動作させる。 ① Microsoft Command Line Utilities for SQL Server ② Microsoft ODBC Driver for SQL Server ③ Metasploit Pro ④ Nmap ⑤ Python

表 7-4 に記載された、侵入テストで使用した主なツールを表 7-5 に示す。

表 7-5　侵入テストで使用したツール

名称 (バージョン)	概要
Metasploit Pro (4.14.3)	脆弱性スキャナ、及び攻撃コードを用いた攻撃ツール
Microsoft Command Line Utilities for SQL Server (15.0.1300.359)	Microsoft社が提供する（SQL Serverと共に提供される）コマンドラインツール
Microsoft ODBC Driver for SQL Server (17.4.1.1)	TOEに接続するためのODBCドライバ
Nmap (7.70.0.0)	ポートスキャンツール
Python (3.7.0)	侵入テストのスクリプトを実行させるためのインタープリタ

また、Active Directory 認証方式を選択した際に使用された、Active Directory 認証サーバの構成を表 7-6 に示す。

表 7-6　Active Directory 認証サーバ

構成品	概要
Hardware	Intel(R) Xeon(R) CPU E3-1220 @ 3.10GHz (2 processors), 6 GB RAM
Hypervisor	VMware ESXi Version 6.7.0
OS	Windows Server 2016 Standard

＜侵入テストの実施項目＞

懸念される脆弱性と対応する侵入テスト概要を表 7-7 に示す。評価者は潜在的な脆弱性が悪用される可能性の有無を決定するため、侵入テストを実施した。

表 7-7　侵入テスト概要

脆弱性	テスト概要
①	SQL Server認証方式を選択した上で、ポリシーに従ってパスワードが設定されたアカウントに対して総当たり攻撃を実施し、測定された所要時間、通信帯域等から論理的に十分な強度を有していること、及び生成したアカウントに対して確実にポリシーが適用されていることを確認する。
②	SQL Server認証方式を選択した上で、TOEが管理するストアドプロシージャの実行フォーマット、使用パラメタを対象にしてファジングテストを実施し、TOEが非セキュアな状態にならないことを確認する。
③	SQL Server認証方式を選択した上で、識別認証情報に対してファジングテストを実施し、不正なフォーマットデータや特殊文字コード等が使用された場合でもTOEが非セキュアな状態にならないことを確認する。
④	ポートスキャンツール、脆弱性スキャンツールを使用し、必要としないネットワークポートが開いていないことを確認する。また、TOEの起動タイミング等によって想定外のネットワークポート制御が行われないことを複数のツールの結果を比較して確認する。
⑤	TOE実行プロセスの終了後に、メモリ上に不正アクセスに繋がる情報が残存していないことをメモリダンプにより確認する。また、保護資産が格納されるファイルシステムが適切にアクセス制御されていることを確認する。
⑥	過去のバージョンの製品等に存在した、リモートコード実行の脆弱性が悪用できなくなっていることを確認する。

c) 結果

評価者が実施した侵入テストでは、想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

7.5　評価構成について

本 TOE には、いくつかの動作モードが存在する。評価構成としてみなされるための条件については、Guidance Addendum[15]の 5.1 節を参照されたい。

本評価では、脆弱性分析に基づき、認証方式として、Active Directory 認証方式又は SQL Server 認証方式を適宜選択して、侵入テストを実施している。

Active Directory 認証方式を選択した場合の評価構成として、次の 2 つの選択肢が含まれる。

1) Linux プラットフォームのシステムサービス(SSSD 及び NSS)によって Linux のユーザ識別子及びグループ識別子に対応付ける選択肢

2) SSSD 及び NSS を使用せず、TOE 内に実装された LDAP の実装を経由して、Active Directory 認証サーバによって対応付けを行う選択肢

また、本評価では、開発者テスト及び侵入テストにおいて、物理マシン上に hypervisor をインストールし、その上にゲスト OS をインストールした動作環境に、TOE をインストールして評価を行っている。ST[12]では、ST に記載された要件を満たす OS を物理マシン上に直接することを求めていないため、評価者は、上記の評価構成は、適切であると判断した。

7.6 評価結果

評価者は、評価報告書をもって本 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。

評価では以下について確認された。

PP 適合：DBMS Working Group Technical Community, Protection Profile for Database Management Systems (DBMS PP) Base Package, Version 2.12, March 23rd, 2017 and
DBMS Working Group Technical Community, DBMS PP Extended Package - Access History (DBMS PP_EP_AH), Version 1.02, March 23rd, 2017

セキュリティ機能要件： コモンクライテリア パート2 拡張

セキュリティ保証要件： コモンクライテリア パート3 適合

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

EAL2パッケージのすべての保証コンポーネント

追加の保証コンポーネント ALC_FLR.2

評価の結果は、第 2 章に記述された識別に一致する TOE によって構成されたもののみに適用される。

7.7 評価者コメント/勧告

本 TOE の利用者は、評価構成における OS として、Red Hat Enterprise Linux Server 7.3 が指定されていることに留意されたい。

8 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の観点で認証を実施した。

① 所見報告書でなされた指摘内容が妥当であること。

② 所見報告書でなされた指摘内容が解決されていること。

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で示されている方法に適合していること。

8.1 認証結果

評価機関より提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本 TOE の評価が CC パート 3 の EAL2 及び保証コンポーネント ALC_FLR.2 に対する保証要件を満たすものと判断する。

8.2 注意事項

適合 PP[14]では、データベースのレプリケーションが行われる場合について、監査証跡を生成することを求めている。ST[12]における TOE の評価構成では、TOE は物理的に分散してインストールされないため、レプリケーションに関する監査証跡は生成されない。

9 附属書

特になし。

10 セキュリティターゲット

本 TOE のセキュリティターゲット[12]は、本報告書とは別文書として以下のとおり提供される。

Microsoft SQL Server 2017 on Linux Database Engine Common Criteria Evaluation (EAL2+) Security Target　Version 1.9, 2020-04-24, Microsoft Corporation

11 用語

本報告書で使用された CC に関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation（セキュリティ評価基準）
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

本報告書で使用された TOE に関する略語を以下に示す。

AD	Active Directory
LDAP	Lightweight Directory Access Protocol
NSS	Name Service Switch
ODBC	Open Database Connectivity
SQL	Structured Query Language リレーショナルデータベースに対してデータ操作や定義を行うためのデータベース言語。
SID	Security Identifier Windows OSで管理されるユーザアカウント、グループに付与される一意の識別子
SSSD	System Security Services Daemon

本報告書で使用された用語の定義を以下に示す。

システム管理者	TOEの管理者権限を有する利用者に割り当てられる役割。 セキュリティ管理に関する操作、及び全てのデータベースに対する操作が許可される。 TOE設置時に必ず１つのシステム管理者アカウントが生成されるが、別の利用者に対してシステム管理者権限を付与することもできる。
ストアドプロシージャ	データベースに対する一連の処理手順を１つのプログラムにまとめ、データベース管理システムに保存したもの。

12 参照

[1] ITセキュリティ評価及び認証制度の基本規程, 平成30年7月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証等に関する要求事項, 平成30年9月, 独立行政法人情報処理推進機構, CCM-02

[3] ITセキュリティ評価機関承認等に関する要求事項, 平成30年9月, 独立行政法人情報処理推進機構, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 5, April 2017, CCMB-2017-04-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

[7] 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3.1 改訂第5版, 2017年4月, CCMB-2017-04-001 (平成29年7月翻訳第1.0版)

[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2: セキュリティ機能コンポーネント バージョン3.1 改訂第5版, 2017年4月, CCMB-2017-04-002 (平成29年7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3: セキュリティ保証コンポーネント バージョン3.1 改訂第5版, 2017年4月, CCMB-2017-04-003 (平成29年7月翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 5, April 2017, CCMB-2017-04-004

[11] 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3.1 改訂第5版, 2017年4月, CCMB-2017-04-004 (平成29年7月翻訳第1.0版)

[12] Microsoft SQL Server 2017 on Linux Database Engine Common Criteria Evaluation (EAL2+) Security Target Version 1.9, 2020-04-24, Microsoft Corporation

[13] Microsoft SQL Server 2017 on Linux Database Engine Enterprise Edition x64 (English) Evaluation Technical Report, Version 12, 2020-05-29, TÜV Informationstechnik GmbH, Evaluation Body for IT-Security

[14] DBMS Working Group Technical Community, Protection Profile for Database Management Systems (DBMS PP) Base Package, Version 2.12, March 23rd,

2017, and
DBMS Working Group Technical Community, DBMS PP Extended Package - Access History (DBMS PP_EP_AH), Version 1.02, March 23rd, 2017
（認証識別: BSI-CC-PP-0088-V2-2017）

[15] SQL Server 2017 on Linux Database Engine – Common Criteria Evaluation (EAL2+) - Guidance Addendum, Version 2.3, 2020-05-22

[16] Microsoft SQL Server 2017 Technical Documentation (2019-09-09)
(File name: Offline-Book.SQL-Server-2017-CU16.zip)