

Transparent Data Encryption for PostgreSQL

行単位暗号化 リリースメモ

ご注意

1. 本書の内容の一部または全部を無断転載することは、禁止されています。
2. 本書の内容に関しては将来予告なしに変更することがあります。
3. 本書の内容について万全を期して作成いたしましたが、万一ご不審な点や誤り、記載漏れなど、お気づきのことがありましたらご連絡ください。

輸出する際の注意事項

本製品（ソフトウェア）は、外国為替管理令に定める提供を規制される技術に該当致しますので、日本国外へ持ち出す際には日本国政府の役務取引許可申請等必要な手続きをお取りください。

許可手続き等にあたり特別な資料等が必要な場合には、お買い上げの販売店またはお近くの当社営業拠点にご相談ください。

はしがき

本書は、Transparent Data Encryption for PostgreSQL の新機能の概要やリビジョンアップによる更新履歴などについて説明しています。

Transparent Data Encryption for PostgreSQL は、PostgreSQL で透過的暗号化環境を実現するソフトウェアです。また、Enterprise Edition では透過的暗号化機能だけでなく、データベースの診断機能や復旧機能を提供することによりデータベースのセキュリティや信頼性を向上させるサブスクリプション製品です。

本書の構成は、次のとおりです。

章	タイトル	内容
1	Transparent Data Encryption for PostgreSQL マニュアル一覧	Transparent Data Encryption for PostgreSQL の全機能のマニュアル一覧
2	各バージョンの概要	Transparent Data Encryption for PostgreSQL の新機能やリビジョンの更新履歴についての説明
3	各バージョンでの注意制限事項	Transparent Data Encryption for PostgreSQL の使用上の注意制限

備考

1. 本書に説明しているすべての機能はプログラムプロダクトであり、次のプロダクト型番に対応しています。

プロダクト型番	プロダクト名	対応モデル
UL4027-H204-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Linux 版 1CPU(1年間)	64 ビット
UL4027-H205-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Linux 版 1CPU 追加(1年間)	64 ビット
UL4027-H206-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Linux 版 待機用 1CPU(1年間)	64 ビット
UL4027-H214-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Linux 版 1CPU(3年間)	64 ビット
UL4027-H215-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Linux 版 1CPU 追加(3年間)	64 ビット
UL4027-H216-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Linux 版 待機用 1CPU(3年間)	64 ビット
UL4027-J204-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Linux 版 1CPU(1年間)(時間延長保守)	64 ビット
UL4027-J205-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Linux 版 1CPU 追加(1年間)(時間延長保守)	64 ビット
UL4027-J206-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Linux 版 待機用 1CPU(1年間)(時間延長保守)	64 ビット
UL4027-J214-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Linux 版 1CPU(3年間)(時間延長保守)	64 ビット
UL4027-J215-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Linux 版 1CPU 追加(3年間)(時間延長保守)	64 ビット
UL4027-J216-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Linux 版 待機用 1CPU(3年間)(時間延長保守)	64 ビット

プロダクト型番	プロダクト名	対応モデル
UL1298-H301-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Windows 版 1CPU(1 年間)	64 ビット
UL1298-H302-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Windows 版 1CPU 追加(1 年間)	64 ビット
UL1298-H303-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Windows 版 待機用 1CPU(1 年間)	64 ビット
UL1298-H311-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Windows 版 1CPU(3 年間)	64 ビット
UL1298-H312-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Windows 版 1CPU 追加(3 年間)	64 ビット
UL1298-H313-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Windows 版 待機用 1CPU(3 年間)	64 ビット
UL1298-J301-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Windows 版 1CPU(1 年間)(時間延長保守)	64 ビット
UL1298-J302-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Windows 版 1CPU 追加(1 年間)(時間延長保守)	64 ビット
UL1298-J303-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Windows 版 待機用 1CPU(1 年間)(時間延長保守)	64 ビット
UL1298-J311-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Windows 版 1CPU(3 年間)(時間延長保守)	64 ビット
UL1298-J312-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Windows 版 1CPU 追加(3 年間)(時間延長保守)	64 ビット
UL1298-J313-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.4 Windows 版 待機用 1CPU(3 年間)(時間延長保守)	64 ビット

2. Linux は、Linus Torvalds 氏の米国およびその他の国における登録商標または商標です。
3. Red Hat、Red Hat Enterprise Linux は、米国 Red Hat, Inc.の登録商標です。
4. Oracle、Oracle Linux は、Oracle Corporation およびその子会社、関連会社の米国およびその他の国における登録商標または商標です。
5. AlmaLinux は、The AlmaLinux OS Foundation の商標です。
6. Rocky Linux は、Rocky Enterprise Software Foundation の商標または登録商標です。
7. Amazon Linux 2 および Amazon Linux 2023 は、米国その他の諸国における、Amazon.com, Inc.またはその関連会社の商標です。
8. Microsoft、Windows、Windows Server、Windows PowerShell は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。
9. その他、記載されている会社名および製品名は、一般的にそれぞれ各社の商標または登録商標です。

目次

第 1 章 Transparent Data Encryption for PostgreSQL マニュアル一覧	1
第 2 章 各バージョンの概要	2
2.1 V2.1	2
2.1.1 V2.1 の強化ポイント	2
2.1.2 V2.1 リビジョン更新履歴	2
2.1.2.1 V2.1.0 から V2.1.1 の変更点	2
2.2 V2.2	3
2.2.1 V2.2 の強化ポイント	3
2.2.2 V2.2 リビジョン更新履歴	3
2.2.2.1 V2.1.1 から V2.2.0 の変更点	3
2.3 V2.3	3
2.3.1 V2.3 の強化ポイント	3
2.3.2 V2.3 リビジョン更新履歴	3
2.3.2.1 V2.2.0 から V2.3.0 の変更点	4
2.3.2.2 V2.3.0 から V2.3.1 の変更点	4
2.3.2.3 V2.3.1 から V2.3.2 の変更点	5
2.4 V2.4	5
2.4.1 V2.4 の強化ポイント	5
2.4.2 V2.4 リビジョン更新履歴	5
2.4.2.1 V2.3.2 から V2.4.0 の変更点	5
第 3 章 各バージョンでの注意制限事項	7
3.1 注意事項	7



第 1 章

Transparent Data Encryption for PostgreSQL マニュアル一覧

Transparent Data Encryption for PostgreSQL に関するマニュアルです。

表 1-1 Transparent Data Encryption for PostgreSQL マニュアル一覧

コード	マニュアル名	概要
OSSDBTDE07	Transparent Data Encryption for PostgreSQL 行単位暗号化 セットアップカード (Linux 版)	Linux 版 Transparent Data Encryption for PostgreSQL のセットアップ方法について記載しています
OSSDBTDE08	Transparent Data Encryption for PostgreSQL 行単位暗号化 透過的暗号化機能 利用の手引	Transparent Data Encryption for PostgreSQL の透過的暗号化機能の概要や環境設定、利用方法について記載しています
OSSDBTDE09	Transparent Data Encryption for PostgreSQL 行単位暗号化 メッセージ解説書	Transparent Data Encryption for PostgreSQL で出力するエラーメッセージの一覧と対処方法について記載しています
OSSDBTDE10	Transparent Data Encryption for PostgreSQL 行単位暗号化 リリースメモ	新機能や変更点について記載を行っています (本書)
OSSDBTDE11	Transparent Data Encryption for PostgreSQL 行単位暗号化 セットアップカード (Windows 版)	Windows 版 Transparent Data Encryption for PostgreSQL のセットアップ方法について記載しています

第2章 各バージョンの概要

Transparent Data Encryption for PostgreSQL のメジャーバージョンでの機能概要や、リビジョンアップによる更新履歴について記載します。

2.1 V2.1

Transparent Data Encryption for PostgreSQL V2.1 の概要について記載します。

2.1.1 V2.1 の強化ポイント

- Table Access Method を利用した暗号化方式を採用することで、行単位暗号化に対応した Transparent Data Encryption for PostgreSQL をリリースしました。
- PostgreSQL 12、13 に対応しました。

2.1.2 V2.1 リビジョン更新履歴

Transparent Data Encryption for PostgreSQL V2.1 の更新履歴は以下のとおりです。

表 2-1 Transparent Data Encryption for PostgreSQL V2.1 の更新履歴

リリース時期	Transparent Data Encryption for PostgreSQL のバージョン
2021 年 4 月	V2.1.0
2022 年 4 月	V2.1.1

2.1.2.1 V2.1.0 から V2.1.1 の変更点

V2.1.0 から V2.1.1 の変更点について記載します。

透過的暗号化機能

- PostgreSQL 13 に対応しました。
- アップデート機能に対応しました。
- 以下の制限事項について対応しました。
 - パラレルクエリ
 - TOAST
 - * PostgreSQL 12 はサポートしていません。
 - 最新の暗号鍵によるデータ再暗号化 (-m cipher)

2.2 V2.2

Transparent Data Encryption for PostgreSQL V2.2 の概要について記載します。

2.2.1 V2.2 の強化ポイント

- Windows 版 PostgreSQL に対応した Transparent Data Encryption for PostgreSQL をリリースしました。

2.2.2 V2.2 リビジョン更新履歴

Transparent Data Encryption for PostgreSQL V2.2 の更新履歴は以下のとおりです。

表 2-2 Transparent Data Encryption for PostgreSQL V2.2 の更新履歴

リリース時期	Transparent Data Encryption for PostgreSQL のバージョン
2023 年 1 月	V2.2.0

2.2.2.1 V2.1.1 から V2.2.0 の変更点

V2.1.1 から V2.2.0 の変更点について記載します。

透過的暗号化機能

- Windows 版 PostgreSQL に対応した Transparent Data Encryption for PostgreSQL をリリースしました。

2.3 V2.3

Transparent Data Encryption for PostgreSQL V2.3 の概要について記載します。

2.3.1 V2.3 の強化ポイント

- PostgreSQL 14、PostgreSQL 15 に対応した Transparent Data Encryption for PostgreSQL をリリースしました。
- Windows Server 2022 に対応しました。

2.3.2 V2.3 リビジョン更新履歴

Transparent Data Encryption for PostgreSQL V2.3 の更新履歴は以下のとおりです。

表 2-3 Transparent Data Encryption for PostgreSQL V2.3 の更新履歴

リリース時期	Transparent Data Encryption for PostgreSQL のバージョン
2023 年 8 月	V2.3.0

リリース時期	Transparent Data Encryption for PostgreSQL のバージョン
2023 年 11 月	V2.3.1
2023 年 12 月	V2.3.2

2.3.2.1 V2.2.0 から V2.3.0 の変更点

V2.2.0 から V2.3.0 の変更点について記載します。

透過的暗号化機能

- PostgreSQL 14、PostgreSQL 15 に対応しました。
- Windows Server 2022 に対応しました。
- Transparent Data Encryption for PostgreSQL をインストールする際には、JDK の Version 8 以降で長期サポート (LTS) リリースされているものを事前にインストールしてください。

表 2-4 動作確認済 JDK のバージョン一覧 (2023 年 8 月時点)

JDK の種類	動作確認済バージョン
Oracle Java SE	8, 11, 17, 20
OpenJDK	8, 11, 17

- 透過的暗号化機能で利用できる暗号化アルゴリズムの bf (Blowfish) は、非サポートとします。OpenSSL 3.0.0 以降がインストールされている場合、本製品で暗号化アルゴリズムの bf (Blowfish) を使用するとエラーが発生します。

2.3.2.2 V2.3.0 から V2.3.1 の変更点

V2.3.0 から V2.3.1 の変更点について記載します。

透過的暗号化機能

- 以下の不具合について対応しました。
 - WAL (トランザクションログ) に UPDATE 文による更新データが含まれる場合、この WAL を使用した処理が実行されると、該当データを正常に復元できず参照時にエラーが発生する問題を修正しました。
 - * 本不具合により影響する処理
 - + クラッシュリカバリ
 - + ポイントインタイムリカバリ (PITR)
 - + ストリーミングレプリケーション

2.3.2.3 V2.3.1 から V2.3.2 の変更点

V2.3.1 から V2.3.2 の変更点について記載します。

透過的暗号化機能

- 以下の不具合について対応しました。
 - PostgreSQL サーバーの設定ファイル (`postgresql.conf`) の `wal_level` に「logical」を設定した場合、クラッシュリカバリで該当データを正常に復元できず参照時にエラーが発生する問題に対応しました。この問題の対応により、`wal_level` に「logical」はご利用できません。`wal_level` は、「logical」以外を設定してご利用ください。

2.4 V2.4

Transparent Data Encryption for PostgreSQL V2.4 の概要について記載します。

2.4.1 V2.4 の強化ポイント

- PostgreSQL 16 に対応した Transparent Data Encryption for PostgreSQL をリリースしました。
- Red Hat Enterprise Linux 9(9.0 以上)、Red Hat Enterprise Linux 互換 OS (Oracle Linux、AlmaLinux、Rocky Linux、Amazon Linux) に対応しました。

2.4.2 V2.4 リビジョン更新履歴

Transparent Data Encryption for PostgreSQL V2.4 の更新履歴は以下のとおりです。

表 2-5 Transparent Data Encryption for PostgreSQL V2.4 の更新履歴

リリース時期	Transparent Data Encryption for PostgreSQL のバージョン
2024 年 11 月	V2.4.0

2.4.2.1 V2.3.2 から V2.4.0 の変更点

V2.3.2 から V2.4.0 の変更点について記載します。

透過的暗号化機能

- PostgreSQL 16 に対応しました。
- Red Hat Enterprise Linux 9(9.0 以上)、Red Hat Enterprise Linux 互換 OS (Oracle Linux、AlmaLinux、Rocky Linux、Amazon Linux) に対応しました。

- 以下の不具合について対応しました。
 - 他のセッションが問い合わせの対象行を同時並行で更新していた際、復号処理が行われない不具合
 - Transparent Data Encryption for PostgreSQL の DML 処理中にメモリ使用量が増加していた不具合
 - 標準 TDE モードで `pg_dump/pg_restore` を実行したときのリストア中にエラーが発生することがある不具合

第3章

各バージョンでの注意制限事項

各バージョンごとの注意制限事項について記載します。

3.1 注意事項

Transparent Data Encryption for PostgreSQL の注意事項の一覧を記載します。

Transparent Data Encryption for PostgreSQL の特に注意いただきたい点を記載します。基本的に記載されている注意事項は「バージョン」列に記載されたバージョン以降すべてのバージョンが対象となります。

表 3-1 注意事項一覧

バージョン	機能	内容
V2.1.0	透過的暗号化機能	Transparent Data Encryption for PostgreSQL 対応 JDBC ドライバは、プロトコルバージョン 2.0 を利用して接続することをサポートしていません。
V2.1.0	psqlODBC について	psqlODBC から出力されるログメッセージに対して暗号鍵情報をマスクするようになっていますが、ODBC トレースの実行により出力されるログは対象外となります。
V2.1.0	パラレルクエリについて	Transparent Data Encryption for PostgreSQL ではパラレルクエリ機能に対応していません。PostgreSQL サーバーの設定ファイル (postgesql.conf) の max_parallel_maintenance_workers に 0、max_parallel_workers_per_gather に 0 を設定してパラレルクエリを無効にしてください。
V2.1.0	JIT コンパイルについて	JIT コンパイルはサポートしていません。
V2.1.0	ロジカルレプリケーション	ロジカルレプリケーションはサポートしていません。PostgreSQL サーバーの設定ファイル (postgres.conf) の wal_level は、「logical」以外を設定してください。 ※V2.3.2 以降は、wal_level に「logical」が設定されている場合は PostgreSQL サービスの起動を抑制しています。
V2.1.0	TOAST について	TOAST はサポートしていません。 格納可能な行データの最大長は 8123 バイトとし、超える場合は Transparent Data Encryption for PostgreSQL 列単位暗号化をご利用ください。
V2.1.0	最新の暗号鍵によるデータ再暗号化 (-m cipher) について	最新の暗号鍵によるデータ再暗号化 (-m cipher) はサポートしません。 再暗号化を実施する場合はデータベースにスーパーユーザーで接続し、データベース全体に対して VACUUM FULL を実施してください。
V2.1.0	Hash インデックス以外のインデックスについて	Hash インデックス以外のインデックスは、暗号化されたデータではなく、復号済データが格納されます。
V2.1.0	INSERT 構文における ON	INSERT 構文において ON CONFLICT 句の利用はサポートしていません。

バージョン	機能	内容
	CONFLICT 句について	
V2.1.1	V2.1.0 の制限事項解除について	本リリースでは、下記の制限事項を解除しました。 <ul style="list-style-type: none"> パラレルクエリ TOAST (PostgreSQL 13 は制限解除、PostgreSQL 12 は未サポートとなります) 最新の暗号鍵によるデータ再暗号化 (-m cipher) について
V2.3.0	利用する暗号化アルゴリズム	bf(Blowfish)は非サポートとします。OpenSSL 3.0.0 以降がインストールされている場合、本製品で暗号化アルゴリズムのbf(Blowfish)を使用するとエラーが発生します。
V2.4.0	メモリ使用量について	暗号化対象テーブルに対して、下記の処理を実行中に、一時的にメモリ使用量が増加します。処理するレコードが多いほどメモリを消費し、1レコードあたりのレコードサイズ(※)の1.5倍~2倍程度のメモリを消費します。 なお、メモリはクエリ完了時に解放されるため、永続的にメモリを消費することはありません。 <ul style="list-style-type: none"> SELECT FOR UPDATE TABLESAMPLE が含まれる SELECT 句 AUTOVACUUM や明示的な ANALYZE 文で実行される統計情報採取処理 (※) 2KB 以上のレコードは圧縮または分割して保存されるため、2KB を超えるレコードを INSERT してもレコードサイズは最大で 2KB になり、レコードサイズが大きくなってもメモリ消費量は単調増加することはありません。

マニュアルコメント用紙

読者各位

説明書に関するご意見、ご要望、内容不明確な部分について具体的にご記入のうえ、販売店または、当社担当営業、担当SEにお渡しください。		お客様ご提出日	年 月 日
		〒 ご住所	〒
マニュアルコード	OSSDBTDE10-07	貴社名 所属	
マニュアル名	Transparent Data Encryption for PostgreSQL 行単位暗号化 リリースメモ	お名前	

項番	ページ	行・図番	指摘区分	指摘内容	添付資料
1					

備考 指摘区分 1 : 誤り 2 : 誤字・脱字 3 : 難解 9 : ご要望
ご協力ありがとうございます。

(注意) 販売店員または、当社営業部員、SEは、すみやかに所定の手続きに従ってマニュアル担当までお送りください。(メール：22-A0704)

なお、NECメールがない場合は、下記まで郵送してください。

〒211-8666 神奈川県川崎市中原区下沼部1753

日本電気(株)プラットフォーム・テクノロジーサービス事業部門 データ基盤サービス統括部 カスタマーサクセスグループ宛

販売店員 営業部員 SE記入	販売店名 または 所属名		担当		メール TEL	
----------------------	--------------------	--	----	--	------------	--

NEC

Transparent Data Encryption for PostgreSQL
行単位暗号化 リリースメモ

OSSDBTDE10-07

2024年11月 第七版 発行

日本電気株式会社

©NEC Corporation 2021-2024