

Transparent Data Encryption for PostgreSQL

列単位暗号化 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-H201-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.1 Linux 版 (1CPU)(1年間)	64 ビット
UL4027-H231-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.1 Linux 版 1CPU 追加(1年間)	64 ビット
UL4027-H203-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.1 Linux 版 Cluster Option(1年間)	64 ビット
UL4027-H211-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.1 Linux 版 (1CPU)(3年間)	64 ビット
UL4027-H212-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.1 Linux 版 1CPU 追加(3年間)	64 ビット
UL4027-H213-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.1 Linux 版 Cluster Option(3年間)	64 ビット
UL4027-J201-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.1 Linux 版 (1CPU)(1年間)(時間延長保守)	64 ビット
UL4027-J231-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.1 Linux 版 1CPU 追加(1年間)(時間延長保守)	64 ビット
UL4027-J203-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.1 Linux 版 Cluster Option(1年間)(時間延長保守)	64 ビット
UL4027-J211-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.1 Linux 版 (1CPU)(3年間)(時間延長保守)	64 ビット
UL4027-J212-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.1 Linux 版 1CPU 追加(3年間)(時間延長保守)	64 ビット
UL4027-J213-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.1 Linux 版 Cluster Option(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. 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。
 6. Amazon Web Services およびすべての AWS 関連の商標、ならびにその他の AWS のグラフィック、ロゴ、ページヘッダーボタンアイコン、スクリプト、サービス名は、米国および/またはその他の国における、AWS の商標、登録商標またはトレードドレスです。
 7. 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 V1.1	2
2.1.1 V1.1 の強化ポイント	2
2.1.2 V1.1 リビジョン更新履歴	2
2.1.2.1 V1.1.0 から V1.1.1 の変更点.....	2
2.1.2.2 V1.1.1 から V1.1.2 の変更点.....	3
2.1.2.3 V1.1.2 から V1.1.3 の変更点.....	4
2.1.2.4 V1.1.3 から V1.1.4 の変更点.....	4
2.2 V1.2.....	4
2.2.1 V1.2 の強化ポイント	4
2.2.2 V1.2 リビジョン更新履歴	4
2.2.2.1 V1.1.4 から V1.2.0 の変更点.....	5
2.2.2.2 V1.2.0 から V1.2.1 の変更点.....	5
2.3 V1.3.....	5
2.3.1 V1.3 の強化ポイント	5
2.3.2 V1.3 リビジョン更新履歴	6
2.3.2.1 V1.2.1 から V1.3.0 の変更点.....	6
2.4 V2.1	6
2.4.1 V2.1 の強化ポイント	6
2.4.2 V2.1 リビジョン更新履歴	6
2.4.2.1 V1.3.0 から V2.1.0 の変更点.....	7
2.4.2.2 V2.1.0 から V2.1.1 の変更点.....	7
第 3 章 各バージョンでの注意制限事項	8
3.1 注意事項	8



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
OSSDBTDE01	Transparent Data Encryption for PostgreSQL 列単位暗号化 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
OSSDBTDE02	Transparent Data Encryption for PostgreSQL 列単位暗号化 透過的暗号化機能 利用の手引き	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
OSSDBTDE04	Transparent Data Encryption for PostgreSQL 列単位暗号化 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
OSSDBTDE05	Transparent Data Encryption for PostgreSQL 列単位暗号化 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)

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 V1.1

Transparent Data Encryption for PostgreSQL V1.1 の概要について記載します。

2.1.1 V1.1 の強化ポイント

- 透過的暗号化機能として4つの暗号属性をリリースしました。
- 鍵のバージョン管理機能やそれらの運用コマンド機能をリリースしました。
- AWS KMS と連携する鍵管理機能をリリースしました。
- データベースの診断・救出/復旧機能を保有するメンテナンス機能をリリースしました。

2.1.2 V1.1 リビジョン更新履歴

Transparent Data Encryption for PostgreSQL V1.1 の更新履歴は以下のとおりです。

表 2-1 Transparent Data Encryption for PostgreSQL V1.1 の更新履歴

リリース時期	Transparent Data Encryption for PostgreSQL のバージョン
2015年7月	V1.1.0
2015年11月	V1.1.1
2017年2月	V1.1.2
2017年9月	V1.1.3
2017年12月	V1.1.4

2.1.2.1 V1.1.0 から V1.1.1 の変更点

V1.1 から V1.1.1 の変更点について記載します。

全体

- PostgreSQL9.4 に対応しました。

透過的暗号化機能

- ORM(オブジェクト関係マッピング)ソフトから透過的暗号化機能を利用するための専用 JDBC ドライバをリリースしました。詳しくは透過的暗号化機能 利用の手引の動作環境項目を参照してください。
- スーパーユーザが `pg_stat_activity` 関数を利用したとき、暗号鍵が見える可能性があった問題を修正しました。
 - 本修正により、`cipher_key_disable_log` 関数、`cipher_key_enable_log` 関数の仕様が変更されました。詳しくは透過的暗号化機能 利用の手引のログ出力無効化、ログ出力有効化項目を確認してください。
- 透過的暗号化機能の利用の手引に「バックアップとリストア」について記載を行いました。
- ストリーミングレプリケーションのセットアップ手法について各マニュアルに記載を行いました。
- PostgreSQL の文字セットを `EUC_JP` に設定したとき、透過的暗号化機能のセットアップに失敗する問題を修正しました。
- 内部的な暗号鍵管理方法を改善し、暗・復号性能を向上させました。

メンテナンス機能

- サルベージ、サルベージ用ロードについて PostgreSQL のバージョンチェックを行うように動作を変更しました。
- メンテナンス機能の内部で利用する SQL の文字列処理でメモリの取扱の問題を修正しました。
- ベリファイについて HOT 機構のあるテーブルに対する検査で、正常なテーブルでも異常と検出するケースについての問題を修正しました。
- ベリファイについてインデックスのリンク検査で、正常なインデックスで異常を検査してしまうケースについての問題を修正しました。

2.1.2.2 V1.1.1 から V1.1.2 の変更点

V1.1.1 から V1.1.2 の変更点について記載します。

透過的暗号化機能

- PostgreSQL9.5 に対応しました。
- Red Hat Enterprise Linux 7(7.1 以上)に対応しました。
- 透過的暗号化機能のセットアップを非対話型で実行する機能を追加しました。

2.1.2.3 V1.1.2 から V1.1.3 の変更点

V1.1.2 から V1.1.3 の変更点について記載します。

透過的暗号化機能

- psqlODBC に対応しました。

2.1.2.4 V1.1.3 から V1.1.4 の変更点

V1.1.3 から V1.1.4 の変更点について記載します。

透過的暗号化機能

- PostgreSQL 9.6 に対応しました。
- AES による暗号化および復号の高速化を目的とした CPU の命令セット AES-NI に対応しました。

2.2 V1.2

Transparent Data Encryption for PostgreSQL V1.2 の概要について記載します。

2.2.1 V1.2 の強化ポイント

- 透過的暗号化機能として4つの暗号属性に加えて整数型に対応する暗号化整数型をリリースしました。
- セッションごとのファンクション実行について不要となる簡易 TDE モードをリリースしました。
- 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 V1.2 リビジョン更新履歴

Transparent Data Encryption for PostgreSQL V1.2 の更新履歴は以下のとおりです。

表 2-2 Transparent Data Encryption for PostgreSQL V1.2 の更新履歴

リリース時期	Transparent Data Encryption for PostgreSQL のバージョン
2018 年 4 月	V1.2.0
2018 年 7 月	V1.2.1

2.2.2.1 V1.1.4 から V1.2.0 の変更点

V1.1.4 から V1.2.0 の変更点について記載します。

透過的暗号化機能

- PostgreSQL 10 に対応しました。
- 透過的暗号化機能として4つの暗号属性に加えて整数型に対応する暗号化整数型をリリースしました。
- セッションごとのファンクション実行について不要となる簡易 TDE モードをリリースしました。また、簡易 TDE モードのリリースに伴い、用語を以下のように変更しています。
 - (V1.1.4 まで) 鍵管理方式 → (V1.2.0 以降) モード
 - (V1.1.4 まで) ローカル鍵管理方式 → (V1.2.0 以降) 標準 TDE モード
 - (V1.1.4 まで) AWS KMS 管理方式 → (V1.2.0 以降) AWS KMS モード
 - `pgtde -m` の文章内の記載：(V1.1.4 まで) モード → (V1.2.0 以降) `-m` オプション
- Windows 版 PostgreSQL に対応した Transparent Data Encryption for PostgreSQL をリリースしました。

2.2.2.2 V1.2.0 から V1.2.1 の変更点

V1.2.0 から V1.2.1 の変更点について記載します。

透過的暗号化機能

- Transparent Data Encryption for PostgreSQL Free Edition V1.2.1 のリリースに伴い、Enterprise Edition V1.2.1 へのアップグレード機能に対応しました。

2.3 V1.3

Transparent Data Encryption for PostgreSQL V1.3 の概要について記載します。

2.3.1 V1.3 の強化ポイント

- PostgreSQL の対応 Ver を拡充しました。
- Linux、Windows の対応製品を拡充しました。

2.3.2 V1.3 リビジョン更新履歴

Transparent Data Encryption for PostgreSQL V1.3 の更新履歴は以下のとおりです。

表 2-3 Transparent Data Encryption for PostgreSQL V1.3 の更新履歴

リリース時期	Transparent Data Encryption for PostgreSQL のバージョン
2020 年 9 月	V1.3.0

2.3.2.1 V1.2.1 から V1.3.0 の変更点

V1.2.1 から V1.3.0 の変更点について記載します。

透過的暗号化機能

- PostgreSQL 11 に対応しました。
- Red Hat Enterprise Linux 8(8.1 以上)に対応しました。
- Windows Server 2019 に対応しました。
- 報告されている不具合について対応しました。
 - 簡易 TDE モードで `pg_dump` がエラーになる問題を修正しました。
 - 簡易 TDE モードで再暗号化時にリセットを行うとエラーになる問題を修正しました。
 - JDBC ドライバで複数 DB に接続した場合、暗号化列に正しくアクセスできなくなる問題を修正しました。
 - ODBC ドライバで複数 DB に接続した場合、暗号化列に正しくアクセスできなくなる問題を修正しました。

2.4 V2.1

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

2.4.1 V2.1 の強化ポイント

- PostgreSQL の対応 Ver を拡充しました。

2.4.2 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 2-4 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

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

2.4.2.1 V1.3.0 から V2.1.0 の変更点

V1.3.0 から V2.1.0 の変更点について記載します。

透過的暗号化機能

- PostgreSQL 12 に対応しました。

2.4.2.2 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。

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
V1.1.0	-	-
V1.1.1	透過的暗号化機能	V1.1.1 から、セッション開始ファンクション実行前には、ログ出力無効化ファンクションの実行が必須となりました。
V1.1.2	透過的暗号化機能	Transparent Data Encryption for PostgreSQL 対応 JDBC ドライバは、PostgreSQL9.5 以降に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。
V1.1.3	V1.1.3 のバイナリについて	本リリースでは、V1.1.2 の ISO に加えて Transparent Data Encryption for PostgreSQL 対応 ODBC ドライバ psqlODBC バイナリの同梱のみです。既存の V1.1.2 の物件に修正は入っていません。
V1.1.3	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。
V1.1.4	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が動作しないよう制御しています。暗号化データ型を処理の対象に含めない場合は通常通り動作します。
V1.2.0	外部統計情報の作成について	PostgreSQL 10 でリリースされた CREATE STATISTICS はサポートしていません。
V1.2.0	宣言的 Partitioning について	PostgreSQL 10 でリリースされた宣言的 Partitioning はサポートしていません。
V1.2.0	ロジカルレプリケーション	PostgreSQL 10 でリリースされたロジカルレプリケーションは Linux 版のみサポートし、Windows 版はサポートしません。
V1.2.0	Windows 版 PostgreSQL 対応について	Windows 版は Linux 版と比較して多くの制限があります。
V1.3.0	JIT コンパイルについて	PostgreSQL 11 でリリースされた JIT コンパイルはサポートしていません。
V1.3.0	Windows 版インストーラについて	インストールしている PostgreSQL のバージョンが OpenSSL 1.1.0 をサポートしたのかによって対象となる Transparent Data Encryption for PostgreSQL のインストーラが異なります。

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	OSSDBTDE05-08	貴社名 所属
マニュアル名	Transparent Data Encryption for PostgreSQL 列単位暗号化 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-A0703)

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) AIプラットフォーム事業部 SDP 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
列単位暗号化 リリースメモ

OSSDBTDE05-08

2022年04月 第八版 発行

日本電気株式会社

©NEC Corporation 2015-2022