

# **Transparent Data Encryption for PostgreSQL**

## **行単位暗号化 メッセージ解説書**

---

## 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 の各機能で出力されるメッセージについて説明したものです。

本書の構成は、次のとおりです。

章	タイトル	内容
1	概要	本書の概要
2	セットアップ機能で出力されるエラーメッセージ	セットアップ機能で出力されるエラーメッセージ
3	透過的暗号化機能で出力されるメッセージ	透過的暗号化機能コマンド (pgtde) および透過的暗号化機能利用時に PostgreSQL により出力されるメッセージ

関連マニュアルとしては次のものがあります。

- 『行単位暗号化 セットアップカード (Linux 版)』
- 『行単位暗号化 透過的暗号化機能 利用の手引』

2021年 4月 初版

## 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. 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 概要.....	1
第2章 セットアップ機能で出力されるエラーメッセージ.....	2
2.1 コマンドエラーメッセージ.....	2
第3章 透過的暗号化機能で出力されるメッセージ.....	4
3.1 コマンドエラーメッセージ.....	4
3.2 透過的暗号化機能により PostgreSQL が出力するメッセージ一覧.....	5

---

---

# 第1章 概要

Transparent Data Encryption for PostgreSQL には以下の機能があり、コマンド実行時や警告や異常を検知したとき、さまざまなメッセージを出力します。

機能	説明
セットアップ機能	セットアップ機能が提供するスクリプト実行時に異常を検知した時に出力されるエラーメッセージ
透過的暗号化機能	透過的暗号化機能実行時に異常を検知したときに出力されるエラーメッセージ

## 第2章

# セットアップ機能で出力されるエラーメッセージ

セットアップ機能で表示されるエラーメッセージについて説明します。

## 2.1 コマンドエラーメッセージ

セットアップ機能 `cipher_setup.sh` で表示されるエラーメッセージの一覧を下記に記載します。

表 2-1 Linux 版エラーメッセージ一覧

エラーメッセージ	対処方法
ERROR: You must be root to execute this command.	root ユーザで再度実行してください。
ERROR: The length of port number must not be zero	ポート番号空文字以外を入力してください。
ERROR: The length of user name must not be zero	ユーザ名は空文字以外を入力してください。
ERROR: Can not use template1 database	「template1」以外のデータベースを指定してください。
ERROR: The length of database name must not be zero	空文字以外のデータベース名を指定してください。
ERROR: must be superuser to execute this command	接続ユーザは PostgreSQL のスーパーユーザを指定してください。
ERROR: There is not exist a definition-script : <ファイル名>	インストールしたファイル構成が破損している可能性があります。Transparent Data Encryption for PostgreSQL の再インストールを実行してください。
ERROR: Invalid input.	入力内容を確認して、正しい値を入力してください。
ERROR: input length must not be zero.	空文字は指定できません。
ERROR: Could not connect to the database	接続情報の内容を確認してください。
WARN: Transparent data encryption function has already been activated	既に対象データベースは透過的暗号化機能が有効になっているため、有効化は不要です。
ERROR: input user must not be super user	スーパーユーザでないユーザを指定してください。
ERROR: Retype password does not match.	パスワードが一致しません。正しいパスワードを入力してください。
ERROR: Could not access to DB.	データベースに接続できませんでした。接続情報の内容を確認してください。
ERROR: Invalid arguments.	コマンドパラメータが間違っています。表示された Usage に従い、再実行してください。
ERROR: Could not read config file: <ファイル名>	非対話型実行で、コンフィグファイルが読み込めません。コンフィグファイルが指定した場所に存在するか、または権限の設定が正しいか確認してください。
ERROR: Setting of <設定項目> is not found.	非対話型実行で、コンフィグファイルの設定項目が見つかりません。コンフィグファイルの設定項目を正しく記載しているか確認してください。
ERROR: Security user must not be super user	非対話型実行で、セキュリティ管理ユーザは非スーパーユーザを指定してください。
ERROR: Security user could not access to DB.	非対話型実行で、セキュリティ管理ユーザでユーザデータベースに接続できませんでした。接続情報の内容を確認してください。
ERROR:'PKGLIBDIR' was not found in pg_config.	PostgreSQL の動的ローディング可能なモジュールの場所を取得できませんでした。データベース管理者に連絡を行ってください。

エラーメッセージ	対処方法
ERROR:'SHAREDIR' was not found in pg_config.	PostgreSQL のアーキテクチャ非依存のサポートファイルの場所を取得できませんでした。データベース管理者に連絡を行ってください。
ERROR: Failed to copy tdeforpg2--2.1.sql	tdeforpg2--2.1.sql のコピーに失敗しました。PP サポートサービスにご連絡ください。
ERROR: Failed to copy tdeforpg2.control	tdeforpg2.control のコピーに失敗しました。PP サポートサービスにご連絡ください。
ERROR: Failed to Link tdeforpg2.so	tdeforpg2.so のハードリンクに失敗しました。PP サポートサービスにご連絡ください。

# 第3章

## 透過的暗号化機能で出力されるメッセージ

透過的暗号化機能実行時に出力されるメッセージには、コマンドを実行時に異常を検知すると出力されるメッセージと PostgreSQL が出力するメッセージがあります。

### 3.1 コマンドエラーメッセージ

コマンド実行時に出力されるメッセージには「FATAL」、「ERROR」、「WARN」の3つのレベルがあります。エラーメッセージ一覧の対処方法を参照し、原因を取り除いてください。

表 3-1 コマンドエラーメッセージ一覧

レベル	エラーコード	エラーメッセージ	対処方法
FATAL	F000	その他のエラー	メッセージを確認して、不明点があれば PP サポートサービスにご連絡ください。
FATAL	F001	UNDEFINED ERROR	システム内部に原因があるため、PP サポートサービスにご連絡ください。
FATAL	F002	ILLEGAL ERROR CODE : "エラーコード"	システム内部に原因があるため、PP サポートサービスにご連絡ください。
FATAL	F009	No console	システム内部に原因があるため、PP サポートサービスにご連絡ください。
FATAL	F016	cipher_key_table or key_management_table table does not exist.	システム内部に原因があるため、PP サポートサービスにご連絡ください。
FATAL	F999	INTERNAL ERROR. Please confirm pgtdc.log and PostgreSQL server log for details.	内部処理でエラーが発生しています。pgtdc.log および PostgreSQL サーバログに出力されているメッセージを含め、PP サポートサービスにご連絡ください。
ERROR	E002	Failed to connect to PostgreSQL	共通パラメータを確認してください。また、PostgreSQL 側が接続を受け付ける設定になっているか確認してください。
ERROR	E003	Given command's argument is incorrect. Try "--help" for more information	正しい引数を入力してください。--help パラメータで機能のヘルプ情報を参照することができます。
ERROR	E122	Invalid number format for "数値"	正しい数値を指定してください。
ERROR	E123	User name is not set	ユーザー名を入力してください。
ERROR	E125	Database name is not set	データベース名を入力してください。
ERROR	E126	Port number is not set	ポート番号を入力してください。
ERROR	E127	Host name is not set	ホスト名を入力してください。
ERROR	E136	Input mode is invalid	実行コマンドに対応したモードを入力してください。
ERROR	E137	Data key is not yet registered	暗号鍵の登録をしてください。
ERROR	E138	Mode is not input	モードを指定してください。
ERROR	E144	New data key does not match	もう一度新しい暗号鍵を入力してください。
ERROR	E145	Selected algorithm is invalid	メニューに表示されている項目を選択してください。
ERROR	E147	Data key's length must not be zero	暗号鍵は空文字以外を入力してください。

レベル	エラーコード	エラーメッセージ	対処方法
ERROR	E321	This feature is not implemented due to technical reason.	「-m cipher」は制限事項です。
ERROR	E709	The specified cipher key is not valid.	正しい暗号鍵を入力してください。
ERROR	E713	Invalid option. Can not use -conf and "オプション" options simultaneously.	-conf オプションと {-h -p -d -pw -U} は同時に指定しないでください。
ERROR	E714	Could not open "ファイル名" file specified in -conf option.	-conf で指定したファイルが存在し適切な権限が設定されているかどうか確認してください。
ERROR	E718	Selected key management mode is invalid.	選択可能な鍵管理方式を選択してください。
ERROR	E719	Could not open "ファイル名" file.	アクセス可能なファイルを指定してください。
ERROR	E720	Failed to register new data key.	発生条件と、出力されたメッセージを PP サポートサービスにご連絡ください。
ERROR	E722	Failed to reencrypt data.	発生条件と、出力されたメッセージを PP サポートサービスにご連絡ください。
ERROR	E723	Length of input must not be zero.	空文字以外を入力してください。
ERROR	E724	Could not write to file: "ファイル名"	フォルダの権限を確認してください。
ERROR	E727	Failed to switch key management mode.	発生条件と、出力されたメッセージを PP サポートサービスにご連絡ください。
ERROR	E728	Failed to show status of TDE.	発生条件と、出力されたメッセージを PP サポートサービスにご連絡ください。
ERROR	E729	Key management mode is already in "鍵管理方式名"	現在既に指定された鍵管理方式で運用されています。現在の設定を確認してください。

## 3.2 透過的暗号化機能により PostgreSQL が出力するメッセージ一覧

透過的暗号化機能利用時に PostgreSQL により出力されるメッセージは「ERROR」「WARNING」「INFO」「LOG」ログがあります。エラーメッセージ一覧の対処方法を参照し、原因を取り除いてください。

表 3-2 PostgreSQL が出力するエラーメッセージ一覧

レベル	エラーコード	エラーメッセージ	対処方法
ERROR	E0001	log_statement must not be 'all'	「log_statement」の設定を「all」以外に変更してください。
ERROR	E0002	new cipher key is invalid	暗号鍵に空文字は指定できません。登録可能な暗号鍵文字列を入力してください。
ERROR	E0003	invalid cipher algorithm "アルゴリズム名"	暗号化アルゴリズムは"aes"か"bf"のみサポートしています。いずれかの暗号化アルゴリズムを入力してください。
ERROR	E0007	encrypt key version over 2147483647 for database "データベース名"	暗号鍵を登録しようとしたデータベースの暗号鍵のバージョンが最大値に達しているため、PP サポートサービスへお問い合わせください。
ERROR	E0008	current cipher key is not correct	指定した暗号鍵が現在使用されている暗号鍵であることを確認してください。
ERROR	E0012	cipher key is not correct	引数に指定した暗号鍵が正しいことを確認してください。
ERROR	E0014	could not get data directory path	cipher_key_table テーブルのバックアップに失敗しました。適切な権限で関数を実行しているか確認してください。encrypt.backup パラメータにバックアップ先ファイルパスを指定して実行してください。

レベル	エラーコード	エラーメッセージ	対処方法
ERROR	E0015	could not rename old backup file of cipher key	暗号鍵テーブルのバックアップ時に、前回のバックアップファイルのリネームに失敗しました。暗号鍵バックアップファイルの出力先の権限設定を確認してください。
ERROR	E0016	could not encrypt data, because key was not set	暗号化テーブルに透過的にアクセスするため、事前にセッション開始関数を実行してください。
ERROR	E0017	could not decrypt data, because key was not set	暗号化テーブルに透過的にアクセスするため、事前にセッション開始関数を実行してください。
ERROR	E0037	Error while executing query in SPI mode.	SPI モードでクエリの実行に失敗しました。再度実行しても失敗する場合は、発生条件とエラーメッセージを PP サポートサービスにご連絡ください。
ERROR	E0038	Data key is not yet registered.	データ鍵を登録してください。
ERROR	E0040	Could not create hash table for cipher key table.	SPI モードで鍵情報用ハッシュテーブルの作成に失敗しました。再度実行しても失敗する場合は、発生条件とエラーメッセージを PP サポートサービスにご連絡ください。
ERROR	E0042	Error while setting key in simple TDE mode. Error code: %d	SPI モードで鍵情報用ハッシュテーブルの作成に失敗しました。再度実行しても失敗する場合は、発生条件とエラーメッセージを PP サポートサービスにご連絡ください。
ERROR	E0043	Error while creating management key. Error code: %d	SPI モードで鍵情報用ハッシュテーブルの作成に失敗しました。再度実行しても失敗する場合は、発生条件とエラーメッセージを PP サポートサービスにご連絡ください。
ERROR	E0044	Error while registering new key. Error code: %d	SPI モードで鍵情報用ハッシュテーブルの作成に失敗しました。再度実行しても失敗する場合は、発生条件とエラーメッセージを PP サポートサービスにご連絡ください。
ERROR	E0045	Error while reencrypting cipher_key_table. Error code: %d	SPI モードで鍵情報用ハッシュテーブルの作成に失敗しました。再度実行しても失敗する場合は、発生条件とエラーメッセージを PP サポートサービスにご連絡ください。
ERROR	E0046	could not find management key	簡易 TDE モードにおいて、鍵管理テーブル (key_management table) にデータが無い状態で、暗号化対象テーブルにデータの挿入が行われました。発生条件とエラーメッセージを PP サポートサービスにご連絡ください。
ERROR	E0047	could not reset key info	暗号鍵のリセット処理の前に正常に既存の鍵情報が取得できません。再度実行しても失敗する場合は、発生条件とエラーメッセージを PP サポートサービスにご連絡ください。
ERROR	E0048	could not encrypt data len, because key was not set	内部エラーが発生しました。再度実行しても失敗する場合は、発生条件とエラーメッセージを PP サポートサービスにご連絡ください。
ERROR	E0049	could not get cipher provider.	内部エラーが発生しました。再度実行しても失敗する場合は、発生条件とエラーメッセージを PP サポートサービスにご連絡ください。
ERROR	E0050	length of decrypted data is less than 0.	内部エラーが発生しました。再度実行しても失敗する場合は、発生条件とエラーメッセージを PP サポートサービスにご連絡ください。
ERROR	E0051	invalid encrypt key version.	内部エラーが発生しました。再度実行しても失敗する場合は、発生条件とエラーメッセージを PP サポートサービスにご連絡ください。
ERROR	E0052	invalid data.	内部エラーが発生しました。再度実行しても失敗する場合は、発生条件とエラーメッセージを PP サポートサービスにご連絡ください。
ERROR	E0053	could not encrypt data.	内部エラーが発生しました。再度実行しても失敗する場合は、発生条件とエラーメッセージを PP サポートサービスにご連絡ください。

レベル	エラーコード	エラーメッセージ	対処方法
ERROR	E0054	could not decrypt data.	内部エラーが発生しました。再度実行しても失敗する場合は、発生条件とエラーメッセージを PP サポートサービスにご連絡ください。
ERROR	E0055	Error while setting key in internal TDE mode. Error code: %d	内部エラーが発生しました。再度実行しても失敗する場合は、発生条件とエラーメッセージを PP サポートサービスにご連絡ください。
ERROR	E0056	encrypt error: %s	内部エラーが発生しました。再度実行しても失敗する場合は、発生条件とエラーメッセージを PP サポートサービスにご連絡ください。
ERROR	E0057	The input value of encrypt.cipherkey is incorrect.	encrypt.cipherkey パラメータの入力値が間違っています。設定した暗号鍵が正しいか確認してください。
ERROR	E0058	Failed to execute pgtdc_begin_session with parameter encrypt.cipherkey. Error code: %s	encrypt.cipherkey パラメータを使用して pgtdc_begin_session を実行できませんでした。再度実行しても失敗する場合は、発生条件とエラーメッセージを PP サポートサービスにご連絡ください。
WARNING	W0001	encrypt key version over 30000 for database "データベース名"	暗号鍵を登録しようとしたデータベースの暗号鍵のバージョンの最大値が 2100000000 を超えています。
WARNING	W0002	number of encrypt key version over 10 for database "データベース名"	pgtdc_begin_session で取得した暗号鍵の数が 10 を超過しています。
WARNING	W0003	The current mode is simple TDE mode. encrypt_cipherkey can be used in standard TDE mode	encrypt.cipherkey パラメータは簡易 TDE モードの場合は設定不要です。



---

**Transparent Data Encryption for PostgreSQL**  
**行単位暗号化 メッセージ解説書**

**O S S D B T D E 0 9 - 0 1**

**2021 年 04 月 第一版 発行**

**日本電気株式会社**

---

**©NEC Corporation 2021-2021**