Transparent Data Encryption for PostgreSQL Enterprise Edition
行単位暗号化 セットアップカード

（Windows 版）

ＯＳＳＤＢＴＤＥ１１－０２

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、お気付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

このたびは、Transparent Data Encryption for PostgreSQL Enterprise Edition をお買い上げいただき、誠にありがとうございます。

本書は、Transparent Data Encryption for PostgreSQL を使用した透過的暗号化機能の導入を行うエンジニアを対象読者とし、Transparent Data Encryption for PostgreSQL のインストール、アップグレード、アンインストールの手順について説明します。なお、透過的暗号化機能をご使用の際は、さらに『行単位暗号化 透過的暗号化機能利用の手引』をご確認ください。

重要

本手順書に記載された方法以外でインストールおよびアンインストールを行った場合は、動作の保証はいたしません。

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
UL1298-H201-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.2 Windows 版 1CPU(1 年間)	64 ビット
UL1298-H202-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.2 Windows 版 1CPU 追加(1 年間)	64 ビット
UL1298-H203-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.2 Windows 版 待機用 1CPU(1 年間)	64 ビット
UL1298-H211-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.2 Windows 版 1CPU(3 年間)	64 ビット
UL1298-H212-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.2 Windows 版 1CPU 追加(3 年間)	64 ビット
UL1298-H213-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.2 Windows 版 待機用 1CPU(3 年間)	64 ビット
UL1298-J201-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.2 Windows 版 1CPU(1 年間)(時間延長保守)	64 ビット
UL1298-J202-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.2 Windows 版 1CPU 追加(1 年間)(時間延長保守)	64 ビット
UL1298-J203-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.2 Windows 版 待機用 1CPU(1 年間)(時間延長保守)	64 ビット
UL1298-J211-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.2 Windows 版 1CPU(3 年間)(時間延長保守)	64 ビット
UL1298-J212-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.2 Windows 版 1CPU 追加(3 年間)(時間延長保守)	64 ビット
UL1298-J213-I	Transparent Data Encryption for PostgreSQL Enterprise Edition V2.2 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. 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。
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。

本書の表記規則

本書では、注意すべき事項、重要な事項および関連情報を以下のように表記します。

注

この表記は、重要であるがデータ損失やシステムおよび機器の損傷には関連しない情報を表します。

重要

この表記は、データ損失やシステムおよび機器の損傷を回避するために必要な情報を表します。

ヒント

この表記は、お客様に役立つ可能性のある情報を表します。

実行例およびファイルの設定例は以下のように表記します

```
コマンドラインの実行例を示します
```

```
ファイルの設定例を示します
```

また、本書では以下の表記法を使用します。

表記	使用方法	例
コマンドライン中の [ ] 角かっこ	かっこ内の値の指定が省略可能であることを示します	cipher_setup.sh [-s {1|2} [path] | -h］
コマンドライン中の { } 波かっこ	かっこ内の値のいずれかを指定する必要があることを示します	cipher_setup.sh [-s {1|2} [path] | -h] 上記例の場合角かっこ内に波かっこがあるため、"-s" オプションを指定した場合、 "1" または "2" を指定する必要があります
#	OS の管理者ユーザーで発行するコマンドを示すプロンプトです	# `./cipher_setup.sh`
$	OS の一般ユーザー（postgres など）で発行するコマンドを示すプロンプトです	$ `psql`
=#	PostgreSQL のスーパーユーザーで SQL を発行する場合は、「=#」のように表記しますが、明示的に接続しているデータベース名を示す場合は、「postgres=#」や「testdb=#」のように先頭にデータベース名を含みます	=# SELECT count(*) FROM public.cipher_key_table;
=>	PostgreSQL の一般ユーザーで SQL を発行する場合は、「=>」のように表記しますが、明示的に接続しているデータベース名を示す場合は、「postgres=>」や「testdb=>」のように先頭にデータベース名を含みます	=> SELECT c1 FROM t1;
CMD>	Windows のコマンドプロンプトで発行するコマンドを示します	CMD>`ipconfig`
モノスペースフォント斜体	ユーザーが有効な値に置き換えて入力する項目	tdeforpg2_pg<*PostgreSQL メジャーバージョン*>-<*Transparent Data Encryption for PostgreSQL バージョン*>-.<*Red Hat Enterprise Linux バージョン*>.x86_64.rpm

最新情報の入手先

最新の製品情報については、以下の Web サイトを参照してください。

https://jpn.nec.com/tdeforpg/

目次

第 1 章
はじめに

本章では、Transparent Data Encryption for PostgreSQL の紹介と Edition ごとの提供機能やサービスについて説明します。

1.1　Transparent Data Encryption for PostgreSQL とは

Transparent Data Encryption for PostgreSQL を使用することで、表に格納する機密データを暗号化できます。また、暗号化されたデータを処理するアプリケーションは、ほとんどあるいはまったく変更せずに透過的にデータを暗号化、復号することができます。さらに、暗号鍵の管理を簡単に行う機能も提供するサブスクリプション製品です。

1.2　利用可能な機能と提供されるサービス

Transparent Data Encryption for PostgreSQL には、商用版の Enterprise Edition があります。利用可能な機能と提供されるサービスを示します。

表 1-1　機能/サービス

機能/サービス	Enterprise Edition for Linux	Enterprise Edition for Windows
Transparent Data Encryption 機能		
行単位の暗号化機能	○	○
鍵の更新、バージョン管理機能	○	○
簡易 TDE モード	○	○
サポートサービス		
Transparent Data Encryption for PostgreSQL の PP サポートサービス	○	○
PostgreSQL 本体の保守サポートサービス	○	○

第 2 章
インストールの概要

本章では、Transparent Data Encryption for PostgreSQL のインストール、アップグレード、アンインストールの概要について説明します。

2.1 インストールの種類

本書で説明する Transparent Data Encryption for PostgreSQL のインストールの種類は以下の 3 つがあります。

- 新規インストール

  Transparent Data Encryption for PostgreSQL を初めてインストールする場合に行います。

- ストリーミングレプリケーション構成への新規セットアップ

  PostgreSQL の標準機能である、ストリーミングレプリケーションを利用した環境に Transparent Data Encryption for PostgreSQL を初めてインストールする場合に行います。

- 高可用性構成（HA 構成）への新規セットアップ

  CLUSTERPRO X の高可用性構成（HA 構成）を利用した環境に Transparent Data Encryption for PostgreSQL を初めてインストールする場合に行います。

2.2 アップグレードの種類

本書で説明するアップグレードは以下の 2 つがあります。

- Transparent Data Encryption for PostgreSQL のアップグレード

  Transparent Data Encryption for PostgreSQL のマイナーバージョンまたはメジャーバージョンをアップグレードする場合に行います。

- 透過的暗号化機能が有効な PostgreSQL のメジャーバージョンアップグレード

  Transparent Data Encryption for PostgreSQL がインストールされ透過的暗号化機能が有効な PostgreSQL をメジャーバージョンアップ(PostgreSQL 13 から PostgreSQL 15 にアップグレードなど)する場合に行います。

注

Transparent Data Encryption for PostgreSQL はメジャーバージョン、マイナーバージョンともにダウングレードはできません。

2.3　アンインストールの種類

本書で説明する Transparent Data Encryption for PostgreSQL のアンインストールには以下の 3 つがあります。

- アンインストール

  Transparent Data Encryption for PostgreSQL をアンインストールする場合に行います。

- ストリーミングレプリケーション構成からのアンインストール

  PostgreSQL の標準機能である、ストリーミングレプリケーションを利用した環境から Transparent Data Encryption for PostgreSQL をアンインストールする場合に行います。

- 高可用性構成（HA 構成）からのアンインストール

  CLUSTERPRO X の高可用性構成（HA 構成）を利用した環境から Transparent Data Encryption for PostgreSQL をアンインストールする場合に行います。

第 3 章
動作環境の確認とインストール前の準備

本章は、Transparent Data Encryption for PostgreSQL を使用するために必要な動作環境とインストール前に確認しておくべきことについて説明します。

3.1　PostgreSQL のインストール

Transparent Data Encryption for PostgreSQL を利用するためには、事前に PostgreSQL をインストールしておく必要があります。「3.4.1.2　ソフトウェア要件（7 ページ）」の条件を満たす PostgreSQL バージョンをインストールしてください。

また、インストール後システム変数 PATH に PostgreSQL の bin を設定します。次の例ではコマンドプロンプトより、システム変数を確認しています。また、PostgreSQL は `C:\Program Files\PostgreSQL\15` にインストールされていることとします。

```
CMD>echo %PATH%
C:\Program Files\PostgreSQL\15\bin;...
```

3.2　JDK のインストール

Transparent Data Encryption for PostgreSQL を利用するためには、事前に JDK Version 8 以降の長期サポート（LTS）リリースされているものをインストールしておく必要があります。

また、インストール後システム変数 PATH に JDK の Java の場所を設定する必要があります。次の例ではコマンドプロンプトより、システム変数を確認しています。Eclipse Temurin™のインストーラーを使用し、インストール先はデフォルトの状態でインストールされていることとします。

```
CMD>echo %PATH%
C:\Program Files\Eclipse Adoptium\jdk-17.0.7.7-hotspot\bin;...
```

注

インストーラーを使用して JDK をインストールした場合、自動的にシステム変数 PATH に JDK の PATH が登録されることがあります。

システム変数 PATH に JDK のパスが設定されていない場合は、システム変数 JAVA_HOME を追加します。 次の例では、OpenJDK が `C:\openlogic-openjdk-8u362-b09-windows-x64\openlogic-openjdk-8u362-b09-windows-64` に展開されている場合になります。

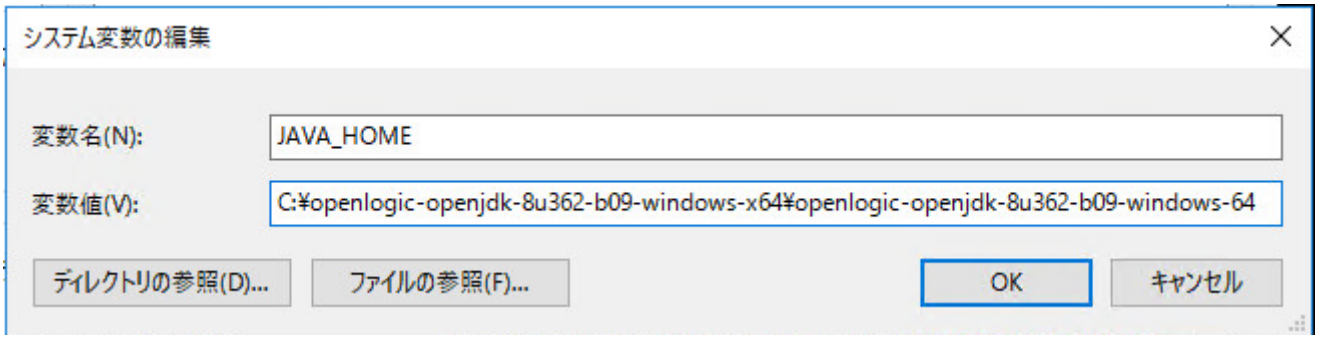

図 3-1　システム変数 JAVA_HOME の追加

システム変数 PATH を編集し、`%JAVA_HOME%\bin` を追加します。

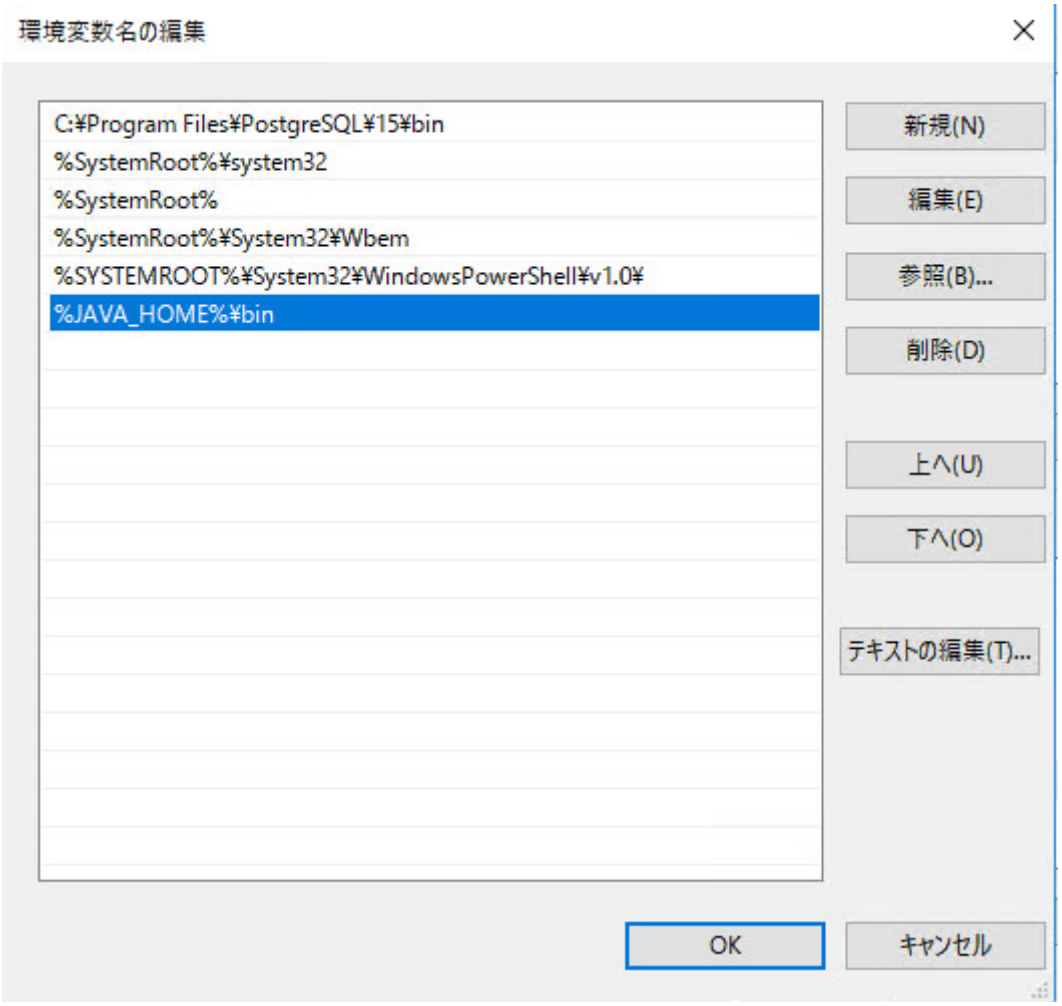

図 3-2　システム変数 PATH の編集

3.3　透過的暗号化機能をセットアップするために必要な情報

透過的暗号化機能をセットアップするために必要な PostgreSQL の接続情報を確認します。

表 3-1　透過的暗号化機能をセットアップするために必要な PostgreSQL の接続情報

ポート番号	透過的暗号化機能をセットアップするデータベースが定義された PostgreSQL のサービス待ち受けポート番号です。
データベース名	透過的暗号化機能をセットアップするデータベースの名前です。
スーパーユーザー名	透過的暗号化機能をセットアップするデータベースに接続するためのスーパーユーザーです。
スーパーユーザーのパスワード	透過的暗号化機能をセットアップするデータベースに接続するためのスーパーユーザーのパスワードです。
セキュリティ管理ユーザー名	透過的暗号化機能の暗号鍵を管理するための専用のユーザーです。
セキュリティ管理ユーザーのパスワード	透過的暗号化機能の暗号鍵を管理するための専用のユーザーのパスワードです。

重要

禁則文字

本ツールで構築する透過的暗号化環境の中で使用する次のオブジェクトでは、「機種依存文字」「Unicode の重複文字」「改行文字」「空文字」の使用を禁止しています。また、個々のオブジェクトで使用を禁止している文字・文字列は次の通りです。

- ホスト名

  {「!」,「'」}を同時使用,「マルチバイト文字」の使用を禁止しています

- データベース名

  {「!」,「'」}を同時使用,「'」,「"」,「/」,「¥」,「=」,「:」,「?」「マルチバイト文字」の使用を禁止しています。

  複数のデータベースインスタンス（データベースクラスタ）を同時に使用する場合、データベース名が重複しないようご注意ください。

- ユーザー名

  {「!」,「'」}を同時使用,「'」,「"」,「マルチバイト文字」の使用を禁止しています。

- パスワード

  {「!」,「'」}を同時使用,「マルチバイト文字」の使用を禁止しています。

表 3-2　接続情報禁則文字一覧

	マルチバイト文字	「!」,「'」を同時使用	「template1」	「'」	「"」	「/」	「¥」	「=」	「:」	「?」
ホスト名	×	×								
データベース名	×	×	×	×	×	×	×	×	×	×
ユーザー名	×	×		×	×					
パスワード名	×	×								

×…禁則文字として扱われる文字・文字列

3.4　インストール要件の確認

3.4.1　データベースサーバー

Transparent Data Encryption for PostgreSQL をインストールする PostgreSQL がインストールされているサーバーのハードウェアとソフトウェア要件について説明します。

3.4.1.1　ハードウェア要件

Transparent Data Encryption for PostgreSQL のインストールには下記のハードウェア要件を満たす必要があります。

表 3-3　データベースサーバー側のハードウェア要件

プロセッサ	x86_64 プロセッサ
メモリ容量	約 200M バイト以上を推奨
ディスク容量	任意のディスクに約 100M バイト以上の空き領域

ヒント

AES-NI の利用

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 を利用するためには、以下の条件を満たす必要があります。

- PostgreSQL 12 以上に対して透過的暗号化機能が有効となっていること
- Windows では Transparent Data Encryption for PostgreSQL V2.2.0 以降が利用されていること
- OpenSSL がインストールされていること
  - コミュニティ推奨 Windows インストーラーによりインストールされた PostgreSQL を利用します。（同梱されている OpenSSL を利用するため）

3.4.1.2　ソフトウェア要件

Transparent Data Encryption for PostgreSQL のインストールには下記のソフトウェア要件を満たす必要があります。

表 3-4　データベースサーバー側のソフトウェア要件（Windows 版）

PostgreSQL バージョン	オペレーティングシステム（Windows）		
	Windows Server 2016	Windows Server 2019	Windows Server 2022
12	○	○	○
13	○	○	○
14	○	○	○
15	○	○	○
必要パッケージ（Windows）	Microsoft Visual C++ 2015-2022 Redistributable(x64) JDK Version 8 以降の長期サポート（LTS）リリースされているもの「表 3-5　動作確認済 JDK のバージョン一覧（2023 年 8 月時点）（8 ページ）」		

重要

Windows プラットフォームではコミュニティが推奨している Windows インストーラーからインストールされた PostgreSQL のみをサポートします。https://www.postgresql.org/download/windows/

動作確認済 JDK のバージョンは下記になります。

表 3-5　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

第 4 章
新規セットアップ

本章では、Transparent Data Encryption for PostgreSQL Enterprise Edition を初めてセットアップする手順について説明します。また、「4.6　ストリーミングレプリケーション構成への新規セットアップ　（17 ページ）」、「4.7　高可用性構成（HA 構成）への新規セットアップ（19 ページ）」の手順についても説明します。

重要

Windows 版 Transparent Data Encryption for PostgreSQL は異なるバージョンを同一の端末に構成することをサポートしません。複数のバージョンを構成したい場合は Linux 版 Transparent Data Encryption for PostgreSQL のご利用をご検討ください。ただし、Linux 版 Transparent Data Encryption for PostgreSQL でも同一データベースインスタンス(データベースクラスタ)内で異なるバージョンの Transparent Data Encryption for PostgreSQL を構成することはサポートしていません。以下に Windows 版 Transparent Data Encryption for PostgreSQL のサポートしない構成例を示します。

- PostgreSQL 14 に対応する Transparent Data Encryption for PostgreSQL V2.3.0 と PostgreSQL 15 に対応する Transparent Data Encryption for PostgreSQL V2.3.0 を同一端末に構成
- Transparent Data Encryption for PostgreSQL V2.3.0（列単位暗号化）と Transparent Data Encryption for PostgreSQL V2.3.0（行単位暗号化）を同一端末に構成

ヒント

鍵管理機能は PostgreSQL データベースサーバーがインストールされた端末リモートコンピューターからも実行が可能です。リモートコンピューターから鍵管理機能を利用する場合、リモートコンピューターにも Transparent Data Encryption for PostgreSQL をインストールしてください。

4.1　新規セットアップの流れ

1. 「4.2　Transparent Data Encryption for PostgreSQL のインストール（10 ページ）」
2. 「4.3　透過的暗号化機能を対話型で有効化する方法（12 ページ）」
3. 「4.4　postgresql.conf の編集（13 ページ）」
4. 「4.5　よりセキュアな運用のための設定（14 ページ）」

   ヒント

   PostgreSQL のユーザーデータを暗号化するためには、上記手順完了後に以下の作業が必要です。詳細は『行単位暗号化 透過的暗号化機能 利用の手引』をご確認ください。

5. 利用するモードの検討
   - 簡易 TDE モード

- 標準 TDE モード

6. 利用する暗号化アルゴリズムの検討
   - aes(Rijndael-128)
   - bf (Blowfish、非サポート)
7. 暗号鍵のパスフレーズの検討
8. 暗号鍵の登録
9. 暗号化対象のユーザーテーブルを作成
10. 暗号化対象のユーザーテーブルに対するデータ操作

4.2　Transparent Data Encryption for PostgreSQL のインストール

以下の手順に従って Transparent Data Encryption for PostgreSQL をインストールしてください。

1. Administrator 権限を持つアカウントでログインします。
2. Transparent Data Encryption for PostgreSQL Enterprise Edition インストール媒体をマウントします。
3. インストール媒体の `windows\installer\PostgreSQL` **フォルダー**の配下に格納されている対応する PostgreSQL バージョンの exe ファイルをクリックします。

   exe ファイルの命名規則は以下の通りです。

   TDEforPG2_PG<*PostgreSQL バージョン*>_<*Transparent Data Encryption for PostgreSQL バージョン*>.exe

   - PostgreSQL バージョン

     Transparent Data Encryption for PostgreSQL が対応する PostgreSQL バージョンを示します。15 は 15 と表示されます。

   - Transparent Data Encryption for PostgreSQL バージョン

     表記形式は X_Y_Z です。X_Y はメジャーバージョン、Z はマイナーバージョンを示します
4. [**Transparent Data Encryption for PostgreSQL Enterprise Edition (PostgreSQL XX)用の InstallShield ウィザードへようこそ**]画面が表示されますので、[**次へ**]をクリックします。
5. [**インストール先のフォルダー**]画面が表示されます。変更する場合は[**変更**]をクリックしてフォルダーを指定し、[**次へ**]をクリックします。

図 4-1　インストール先のフォルダー画面

6. [**プログラムをインストールする準備ができました**]画面が表示されますので、[**インストール**]をクリックしてインストールを開始します。

7. [**InstallShield ウィザードを完了しました**]画面が表示されます。[**完了**]をクリックします。

8. インストール完了後、システム変数 PATH に Transparent Data Encryption for PostgreSQL Enterprise Edition のインストールディレクトリ配下の `lib` が設定されていることを確認します。

   次の例ではコマンドプロンプトより、システム変数を確認しています。また、Transparent Data Encryption for PostgreSQL Enterprise Edition は `C:\Program Files\NEC\TDEforPG2_PG15` にインストールされていることとします。

```
CMD>echo %PATH%
C:\Program Files\NEC\TDEforPG2_PG15\lib;...
```

注

システム変数 PATH に設定した PostgreSQL 本体の `bin` は、Transparent Data Encryption for PostgreSQL の後に設定されている必要があります。Transparent Data Encryption for PostgreSQL の前に PostgreSQL 本体の `bin` が設定されている場合、パフォーマンスに影響する恐れがあります。

[システム変数 PATH の推奨設定例]

```
C:\Program Files\NEC\TDEforPG2_PG15\lib;C:\Program Files\PostgreSQL
\15\bin;...\
```

[システム変数 PATH の非推奨な設定例]

```
C:\Program Files\PostgreSQL\15\bin;C:\Program Files\NEC
\TDEforPG2_PG15\lib;...\
```

4.3　透過的暗号化機能を対話型で有効化する方法

以下の手順に従って対話型で透過的暗号化機能を有効化してください。

重要

透過的暗号化機能を有効化する際に cipher_setup.bat を介して、PowerShell のスクリプトを起動しています。そのため、Windows PowerShell スクリプトの実行ポリシーを RemoteSigned もしくは Unrestricted に設定する必要があります。設定方法は Microsoft 公式ページをご確認ください。

1. Administrator 権限を持つアカウントでログインします。
2. [**スタートメニュー**]>[**cipher_setup の実行**]をクリックします。
3. [**NEC TDE for PG VX.Y.Z Cipher Setup**]画面が表示されます。

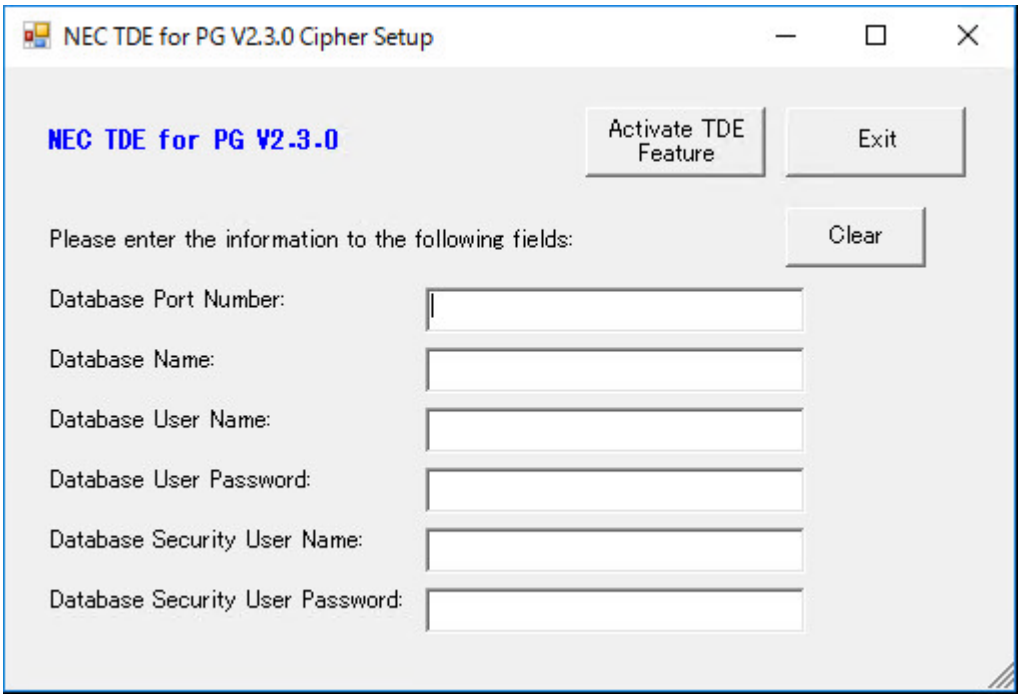

図 4-2　NEC TDE for PG VX.Y.Z Cipher Setup 画面

注

GUI の右上の[×]ボタンをクリックすると、警告なしに閉じられます。

表 4-1　各項目の説明

項目	説明	有効化の際の入力有無
Database Port Number	ポート番号	入力必要
Database Name	データベース名	入力必要
Database User Name	スーパーユーザー名	入力必要
Database User Password	スーパーユーザーのパスワード	入力必要
Database Security User Name	セキュリティ管理ユーザー名	入力必要
Database Security User Password	セキュリティ管理ユーザーのパスワード	入力必要

4. 「3.3　透過的暗号化機能をセットアップするために必要な情報（5 ページ）」を参考に PostgreSQL への接続情報、およびセキュリティ管理ユーザーを入力し、[**Activate TDE Feature**]をクリックします。

   透過的暗号化機能を有効化するデータベース は事前に作成されている必要があります。入力したセキュリティ管理ユーザー名が PostgreSQL に存在しない場合、新規に PostgreSQL ユーザーを作成します。この際にセキュリティ管理ユーザーは、 MD5 パスワードで定義されます。

   注

   セキュリティ管理ユーザーとして PostgreSQL のスーパーユーザーを指定することはできません。

5. [**Activate confirm**]が表示されます。[**はい**]をクリックします。

入力した情報に問題が無ければ[**Activate success!**]ダイアログが表示されます。表示されたメッセージを確認し、[**OK**]をクリックします。これで指定したデータベースに対して透過的暗号化機能が有効化されます。また、セキュリティ管理ユーザーの接続情報が記載された設定ファイルが作成されます（本手順では `C:\Program Files\NEC\TDEforPG2_PG15\conf\pgtde_secuser.properties`）。暗号鍵を管理するオペレーティングシステムユーザーは、このファイルを透過的暗号化機能コマンド（`pgtde`）実行時の接続情報ファイルとして使用することが可能です。

4.4　postgresql.conf の編集

Transparent Data Encryption for PostgreSQL のインストール完了後、透過的暗号化機能を利用するために PostgreSQL の設定ファイル（`postgresql.conf`）を変更し、設定の変更を有効にします。

1. PostgreSQL の設定ファイル（`postgresql.conf`）の shared_preload_libraries パラメータに Transparent Data Encryption for PostgreSQL のダイナミックリンクライブラリ `tdeforpg2.dll` を設定します。

   [postgresql.conf 設定例]

次の設定例では、C:\Program Files\NEC\TDEforPG2_PG15 に Transparent Data Encryption for PostgreSQL がインストールされていることとします。

```
shared_preload_libraries = 'tdeforpg2.dll'
```

2. 変更した設定を有効にするため、PostgreSQL を再起動します。

   次の例では、サービスを再起動することで PostgreSQL を再起動します。

```
CMD>sc stop postgresql-x64-15
CMD>sc start postgresql-x64-15
```

ヒント

サービスとして登録していない場合は、pg_ctl[*1] コマンドを利用して PostgreSQL を再起動しています。

```
CMD> pg_ctl restart
```

4.5　よりセキュアな運用のための設定

透過的暗号化機能は、OS ユーザーおよびファイルの権限を適切に設定することでよりセキュアな運用が実現できます。よりセキュアな運用を行いたい場合は以下の設定を実施してください。

1. 透過的暗号化機能をよりセキュアな状態で運用するためには、各機能毎に OS ユーザーおよび OS グループを作成します。

   それぞれの OS ユーザーが適切な PostgreSQL ユーザーを使用するような運用方針を策定する必要があります。作成するユーザーと対応する PostgreSQL ユーザーの一覧については下記をご参考の上作成してください。

表 4-2　作成する OS ユーザー一覧

OS ユーザー	OS グループ	役割	使用可能な PostgreSQL ユーザー
データベース管理者	透過的暗号化機能管理グループ	PostgreSQL 起動ユーザーであり、PostgreSQL に対する全権限を持つユーザー。	スーパーユーザー
セキュリティ管理者	透過的暗号化機能管理グループ	透過的暗号化機能で利用する鍵の管理権限を持つユーザー	透過的暗号化機能のセットアップで作成または指定したセキュリティ管理ユーザー
アプリケーション管理者（アプリケーション開発者）	透過的暗号化機能利用グループ	透過的暗号化機能を利用しているユーザーデータに対する暗号化・復号権限を持つユーザー	透過的暗号化機能を利用するユーザーデータにアクセスできる一般ユーザー

*1　pg_ctl コマンドの詳細な利用方法は PostgreSQL マニュアルをご確認ください。

次の例では透過的暗号化機能管理グループ「tde_manager」と透過的暗号化機能利用グループ「tde_user」を作成し、セキュリティ管理者「secuser」、アプリケーション管理者（アプリケーション開発者）「apuser」をそれぞれのグループに所属させるよう作成しています。

```
CMD>NET USER secuser /ADD ******
CMD>NET USER apuser /ADD ******
CMD>NET LOCALGROUP tde_manager /ADD
CMD>NET LOCALGROUP tde_user /ADD
CMD>NET LOCALGROUP tde_manager secuser /ADD
CMD>NET LOCALGROUP tde_user apuser /ADD
CMD>NET LOCALGROUP Users secuser /ADD
CMD>NET LOCALGROUP Users apuser /ADD
```

2. 透過的暗号化機能をよりセキュアな状態で運用するためには、各種ファイルをそれぞれ適切な所有者に設定します。

   次の表を参考に、作成したユーザー毎にファイルの権限を設定してください。

表 4-3　アクセス権限設定を推奨する透過的暗号化機能関連ファイル一覧

対象ファイル	所有者
conf/pgtde_secuser.properties	セキュリティ管理者
lib/jar/pgtde.jar	アプリケーション管理者（アプリケーション開発者）
lib/jar/pgtde_regist.jar	セキュリティ管理者

次の例では、セキュリティ管理者に「secuser」、アプリケーション管理者（アプリケーション開発者）に「apuser」として各種ファイルの所有者を設定しています。また、PostgreSQL 15 用の Transparent Data Encryption for PostgreSQL が C:\Program Files\NEC\TDEforPG2_PG15 にインストールされていることとします。

```
CMD>CD "C:\Program Files\NEC\TDEforPG2_PG15"
CMD>ICACLS "conf\pgtde_secuser.properties" /grant secuser:F
CMD>ICACLS "conf\pgtde_secuser.properties" /inheritance:r
CMD>ICACLS "lib\jar\pgtde.jar" /grant apuser:F
CMD>ICACLS "lib\jar\pgtde.jar" /grant Administrators:F
CMD>ICACLS "lib\jar\pgtde.jar" /inheritance:r
CMD>ICACLS "lib\jar\pgtde_regist.jar" /grant secuser:F
CMD>ICACLS "lib\jar\pgtde_regist.jar" /grant Administrators:F
CMD>ICACLS "lib\jar\pgtde_regist.jar" /inheritance:r
```

上記ファイルの権限設定により、透過的暗号化機能コマンド（pgtde）の各-m オプションの実行がユーザー毎に以下のように制限されます。(各-m オプションの詳細は『行単位暗号化 透過的暗号化機能 利用の手引』をご確認ください)

表 4-4　モード毎実行可能ユーザー一覧

各-m オプション	実行可能ユーザー
暗号鍵の登録・更新(-m regist)	セキュリティ管理者
モードの変更(-m switch)	

各-m オプション	実行可能ユーザー
利用状況を表示(-m show)	
最新の暗号鍵による再暗号化(-m cipher)	アプリケーション管理者（アプリケーション開発者）

3. 透過的暗号化機能を利用したいデータベースの一般ユーザーは、暗号鍵情報テーブルに対して適切なアクセス権限を設定します。対象のデータベースに存在する暗号鍵情報テーブル(cipher_key_table)に対して GRANT 文を利用して一般ユーザーに UPDATE と DELETE 権限を設定します。

   次の例では、データベースの一般ユーザー「apuser」に対して暗号鍵情報テーブル(cipher_key_table)の UPDATE と DELETE 権限を設定しています。

```
=# CREATE ROLE apuser WITH LOGIN ENCRYPTED PASSWORD '******';
=# GRANT UPDATE ON cipher_key_table TO apuser;
=# GRANT DELETE ON cipher_key_table TO apuser;
```

ヒント

PostgreSQL のセキュリティ管理ユーザーに透過的暗号化機能のセットアップで作成したユーザー以外の一般ユーザーを割り当てる場合、対象のデータベースに対して次の権限を設定します。次の例では 一般ユーザー「secuser」を透過的暗号化機能のセキュリティ管理者用として設定しています。

```
=# CREATE ROLE secuser WITH LOGIN ENCRYPTED PASSWORD '******';
=# GRANT INSERT ON cipher_key_table TO secuser;
=# GRANT UPDATE ON cipher_key_table TO secuser;
=# GRANT DELETE ON cipher_key_table TO secuser;
=# GRANT EXECUTE ON FUNCTION cipher_key_backup() TO secuser;
```

4. 暗号化対象テーブルの所有者は、アプリケーション管理者（アプリケーション開発者）「apuser」へ変更します。暗号化対象テーブルの所有者がアプリケーション管理者（アプリケーション開発者）「apuser」でない場合、最新の暗号鍵による再暗号化(-m cipher)はエラーになります。

   次の例では、暗号化対象テーブル「Employee」の所有者をアプリケーション管理者（アプリケーション開発者）「apuser」へ変更します。

```
=# ALTER TABLE Employee OWNER TO apuser;
```

注

暗号化対象テーブルは、アプリケーション管理者（アプリケーション開発者）「apuser」で作成して使用することも可能です。

4.6　ストリーミングレプリケーション構成への新規セットアップ

PostgreSQL の標準機能である、ストリーミングレプリケーションを利用した環境に Transparent Data Encryption for PostgreSQL を初めてインストールする手順について説明します。以下の手順でセットアップを行います。なお、手順 1～4 は参考として記載していますが、詳細な手順については、各手順の参照先をご確認ください。

表 4-5　インストール時の手順要否

手順	作業項目		参照先
	プライマリサーバー	スタンバイサーバー	
1	PostgreSQL のインストール		関連リンク参照
2	インスタンスの作成・設定		関連リンク参照
3		インスタンスの作成・設定	関連リンク参照
4	ストリーミングレプリケーションの状態確認		関連リンク参照
5	Transparent Data Encryption for PostgreSQL のインストール		「4.6.1　Transparent Data Encryption for PostgreSQL のインストール（手順 5）（18 ページ）」
6		透過的暗号化機能のファイル配置	「4.6.2　透過的暗号化機能のファイル配置（手順 6）（18 ページ）」
7	透過的暗号化機能の有効化		「4.6.3　透過的暗号化機能の有効化（手順 7）（19 ページ）」
8	postgresql.conf の編集		「4.6.4　postgresql.conf の編集（手順 8）（19 ページ）」
9	よりセキュアな運用のための設定		「4.6.5　よりセキュアな運用のための設定（手順 9）（19 ページ）」

関連リンク

PostgreSQL のインストール（PostgreSQL の Windows インストーラー、Linux ディストリビューション・パッケージなどのリンク集、およびインストールガイド URL https://www.postgresql.jp/download）

インスタンスの作成・設定（最新バージョンの PostgreSQL マニュアル URL https://www.postgresql.jp/document/current/html/admin.html）

ストリーミングレプリケーションの状態確認（最新バージョンの PostgreSQL マニュアル URL https://www.postgresql.jp/document/current/html/high-availability.html）

4.6.1　Transparent Data Encryption for PostgreSQL のインストール（手順 5）

ストリーミングレプリケーションを利用する場合は、「4.2　Transparent Data Encryption for PostgreSQL のインストール（10 ページ）」を参考にプライマリサーバーとスタンバイサーバーの両方にインストールを行ってください。

重要

インストールパスの指定は、プライマリサーバーとスタンバイサーバーを同じフォルダーパスに統一する必要があります。

4.6.2　透過的暗号化機能のファイル配置（手順 6）

ストリーミングレプリケーションを利用する場合は、透過的暗号化機能で使用するファイルをスタンバイサーバー内に配置してください。次の例では、PostgreSQL 15 用の Transparent Data Encryption for PostgreSQL が `C:\Program Files\NEC\TDEforPG2_PG15`（デフォルト）にインストールされていることとします。

1. PostgreSQL の<SHAREDIR>のパスを確認します。

   [<SHAREDIR>のパス確認例]

```
CMD> pg_config --sharedir
C:/PROGRA~1/POSTGR~1/15/share
```

2. <SHAREDIR>に tdeforpg2--*.sql をコピーします。

   [tdeforpg2--*.sql のコピー例]

```
CMD> COPY "C:\Program Files\NEC\TDEforPG2_PG15\lib\tdeforpg2--*.sql" "C:/PROG
RA~1/POSTGR~1/15/share/extension"
C:\Program Files\NEC\TDEforPG2_PG15\lib\tdeforpg2--2.1--2.1.1.sql
C:\Program Files\NEC\TDEforPG2_PG15\lib\tdeforpg2--2.1.1--2.2.sql
C:\Program Files\NEC\TDEforPG2_PG15\lib\tdeforpg2--2.1.sql
C:\Program Files\NEC\TDEforPG2_PG15\lib\tdeforpg2--2.2--2.3.sql
        4 個のファイルをコピーしました。
```

3. <SHAREDIR>に tdeforpg2.control をコピーします。

   [tdeforpg2.control のコピー例]

```
CMD> COPY "C:\Program Files\NEC\TDEforPG2_PG15\lib\tdeforpg2.control" "C:/PRO
GRA~1/POSTGR~1/15/share/extension"
        1 個のファイルをコピーしました。
```

4. PostgreSQL の<PKGLIBDIR>のパスを確認します。

   [<PKGLIBDIR>のパス確認例]

```
CMD> pg_config --pkglibdir
C:/PROGRA~1/POSTGR~1/15/lib
```

5. <PKGLIBDIR>に tdeforpg2.dll をコピーします。

   [tdeforpg2.dll のコピー例]

```
CMD> COPY "C:\Program Files\NEC\TDEforPG2_PG15\lib\tdeforpg2.dll" "C:/PROGRA~
1/POSTGR~1/15/lib/"
        1 個のファイルをコピーしました。
```

4.6.3　透過的暗号化機能の有効化（手順 7）

「4.3　透過的暗号化機能を対話型で有効化する方法（12 ページ）」を参考にプライマリサーバーのみ透過的暗号化機能を有効化してください。

4.6.4　postgresql.conf の編集（手順 8）

ストリーミングレプリケーションを利用する場合は、「4.4　postgresql.conf の編集（13 ページ）」を参考にプライマリサーバーとスタンバイサーバーの両方の postgresql.conf の shared_preload_libraries パラメータに Transparent Data Encryption for PostgreSQL のダイナミックリンクライブラリ tdeforpg2.dll を設定してください。

4.6.5　よりセキュアな運用のための設定（手順 9）

ストリーミングレプリケーションを利用した環境でよりセキュアな運用を行いたい場合は、「4.5　よりセキュアな運用のための設定（14 ページ）」を参考にプライマリサーバーとスタンバイサーバーの両方を同一の構成となるよう設定してください。

4.7　高可用性構成（HA 構成）への新規セットアップ

CLUSTERPRO X の高可用性構成（HA 構成）を利用した環境に Transparent Data Encryption for PostgreSQL を初めてインストールする手順について説明します。以下の手順でセットアップを行います。なお、手順 1～6 は参考として記載していますが、詳細な手順については、各手順の参照先をご確認ください。

表 4-6　インストール時の手順要否

手順	作業項目		参照先
	現用系サーバー	待機系サーバー	
1	CLUSTERPRO のインストール、設定		関連リンク参照
2	PostgreSQL のインストール		関連リンク参照
3	PostgreSQL の設定		関連リンク参照
4		PostgreSQL の設定	関連リンク参照

手順	作業項目		参照先
	現用系サーバー	待機系サーバー	
5	CLUSTERPRO の EXEC リソースの設定		関連リンク参照
6	CLUSTERPRO の監視リソースの設定		関連リンク参照
7	Transparent Data Encryption for PostgreSQL のインストール		「4.7.1　Transparent Data Encryption for PostgreSQL のインストール（手順 7）（20 ページ）」
8		透過的暗号化機能のファイル配置	「4.7.2　透過的暗号化機能のファイル配置（手順 8）（20 ページ）」
9	透過的暗号化機能の有効化		「4.7.3　透過的暗号化機能の有効化（手順 9）（21 ページ）」
10	postgresql.conf の編集		「4.7.4　postgresql.conf の編集（手順 10）（21 ページ）」
11	よりセキュアな運用のための設定		「4.7.5　よりセキュアな運用のための設定（手順 11）（21 ページ）」

関連リンク

CLUSTERPRO のインストール、設定（CLUSTERPRO X システム構築ガイド URL https://jpn.nec.com/clusterpro/clpx/manual.html）

PostgreSQL のインストール（PostgreSQL の Windows インストーラー、Linux ディストリビューション・パッケージなどのリンク集、およびインストールガイド URL https://www.postgresql.jp/download）

PostgreSQL の設定、CLUSTERPRO の EXEC リソースの設定、監視リソースの設定（CLUSTERPRO® X for Windows PP ガイド(PostgreSQL) URL https://jpn.nec.com/clusterpro/clpx/doc/guide/HOWTO_PostgreSQL_Windows_JP_03.pdf）

4.7.1　Transparent Data Encryption for PostgreSQL のインストール（手順 7）

CLUSTERPRO X の高可用性構成（HA 構成）を利用する場合は、「4.2　Transparent Data Encryption for PostgreSQL のインストール（10 ページ）」を参考に現用系サーバーと待機系サーバーの両方にインストールを行ってください。

重要

インストールパスの指定は、現用系サーバーと待機系サーバーを同じフォルダーパスに統一する必要があります。

4.7.2　透過的暗号化機能のファイル配置（手順 8）

CLUSTERPRO X の高可用性構成（HA 構成）を利用する場合は、「4.6.2　透過的暗号化機能のファイル配置（手順 6）（18 ページ）」を参考に待機系サーバー内に透過的暗号化機能で使用するファイルを配置してください。

4.7.3　透過的暗号化機能の有効化（手順 9）

「4.3　透過的暗号化機能を対話型で有効化する方法（12 ページ）」を参考に現用系サーバーのみ透過的暗号化機能を有効化してください。

4.7.4　postgresql.conf の編集（手順 10）

CLUSTERPRO X の高可用性構成（HA 構成）を利用する場合は、「4.4　postgresql.conf の編集（13 ページ）」を参考に現用系サーバーと待機系サーバーの両方の postgresql.conf の shared_preload_libraries パラメータに Transparent Data Encryption for PostgreSQL のダイナミックリンクライブラリ tdeforpg2.dll を設定してください。

4.7.5　よりセキュアな運用のための設定（手順 11）

CLUSTERPRO X の高可用性構成（HA 構成）を利用した環境でよりセキュアな運用を行いたい場合は、「4.5　よりセキュアな運用のための設定（14 ページ）」を参考に現用系サーバーと待機系サーバーの両方を同一の構成となるよう設定してください。

第 5 章
アンインストール

本章では、Transparent Data Encryption for PostgreSQL Enterprise Edition をアンインストールする手順について説明します。また、「5.7　ストリーミングレプリケーション構成からのアンインストール（26 ページ）」、「5.8　高可用性構成（HA 構成）からのアンインストール（26 ページ）」についても説明します。

重要

本製品をアンインストールするには、暗号化対象テーブルを全て削除する必要があります。

5.1　アンインストールの流れ

1. 「5.2　透過的暗号化機能の無効化（22 ページ）」
2. 「5.3　Transparent Data Encryption for PostgreSQL のアンインストール（23 ページ）」
3. 「5.4　postgresql.conf の編集（24 ページ）」
4. 「5.5　ファイルの削除（25 ページ）」
5. 「5.6　インストールディレクトリの削除（25 ページ）」

5.2　透過的暗号化機能の無効化

透過的暗号化機能を無効化する方法として以下の 2 つを実施します。

- 暗号化対象テーブルを手動で削除します。DROP EXTENSION 実行時に CASCADE オプションを指定することで、暗号化対象テーブルを一括削除することも可能です。
- データベースにスーパーユーザーで接続し、tdeforpg2 を DROP EXTENSION クエリでアンインストールします。

```
=# DROP EXTENSION tdeforpg2;
DROP EXTENSION
```

注

DROP EXTENSION クエリ実施後は、暗号鍵情報を格納する cipher_key_table テーブルと key_management_table テーブルが削除されます。

5.3　Transparent Data Encryption for PostgreSQL のアンインストール

以下の手順に従って Transparent Data Encryption for PostgreSQL をアンインストールしてください。

1. Administrator 権限を持つアカウントでログインします。
2. [**コントロールパネル**]>[**プログラムと機能**]を選択し、[**プログラムと機能**]画面を起動します。
3. [**Transparent Data Encryption for PostgreSQL Enterprise Edition (PostgreSQL *XX*)**]を右クリックし、[**アンインストール**]をクリックします。

   XX は PostgreSQL のメジャーバージョンです。
4. [**プログラムと機能**]ダイアログが起動し、アンインストールを実行するか確認されるので[**はい**]を選択します。[**いいえ**]を選択した場合、アンインストールは中止されます。

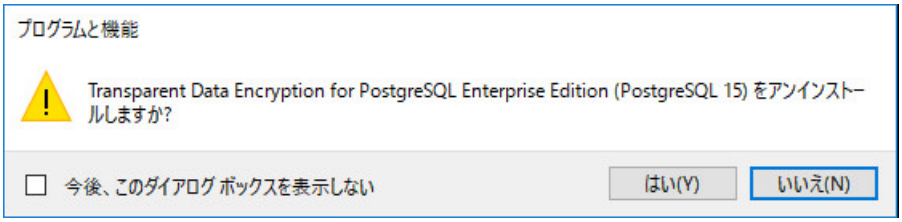

図 5-1　プログラムと機能ダイアログ

5. アンインストールの前に透過的暗号化機能を無効化したか確認するダイアログが表示されるので[**はい**]を選択します。[**いいえ**]を選択した場合、アンインストールは中止されます。

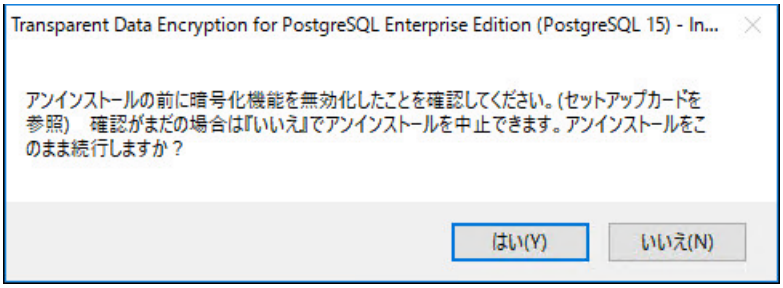

図 5-2　透過的暗号化機能の無効化する際の確認ダイアログ

6. 「アンインストールを続行します」と確認するダイアログが表示されるので[**OK**]をクリックします。
7. 再起動が必要なことを通知するダイアログが表示された場合は[**OK**]をクリックします。

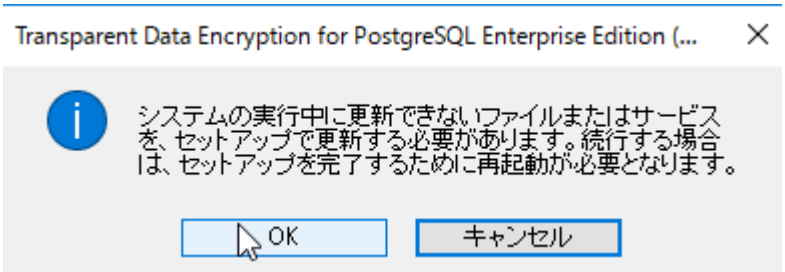

図 5-3　再起動を促すダイアログ

注

再起動を促すダイアログが表示されない場合もセットアップは完了します。

8. 必要に応じて、再起動します。

5.4　postgresql.conf の編集

Transparent Data Encryption for PostgreSQL のインストール完了後、透過的暗号化機能を利用停止するために PostgreSQL の設定ファイル（`postgresql.conf`）を変更し、設定の変更を有効にします。

1. PostgreSQL の設定ファイル（`postgresql.conf`）の shared_preload_libraries パラメータに Transparent Data Encryption for PostgreSQL のダイナミックリンクライブラリ `tdeorpg2.dll` を削除、またはパラメータ自体をコメントアウトします。

   [postgresql.conf 設定例]

```
shared_preload_libraries = ''
```

2. 変更した設定を有効にするため、PostgreSQL を再起動します。

   次の例では、サービスを再起動することで PostgreSQL を再起動しています。

```
CMD>sc stop postgresql-x64-15
CMD>sc start postgresql-x64-15
```

ヒント

サービスとして登録していない場合は、`pg_ctl`[*1] コマンドを利用して PostgreSQL を再起動しています。

```
CMD> pg_ctl restart
```

*1　`pg_ctl` コマンドの詳細な利用方法は PostgreSQL マニュアルをご確認ください。

5.5 ファイルの削除

Transparent Data Encryption for PostgreSQL を今後利用しない場合、透過的暗号化機能を有効化した際に配置されたファイルを削除します。

1. tdeforpg2.control を削除します。

   次の例では、PostgreSQL 15 用の Transparent Data Encryption for PostgreSQL が/opt/nec（デフォルト）、PostgreSQL 15.2 をコミュニティ推奨 Windows インストーラー（デフォルト）でインストールされていることとします。

```
CMD> DIR /b "C:/PROGRA~1/POSTGR~1/15/share/extension\tdeforpg2.control"
tdeforpg2.control
CMD> DEL /p "C:/PROGRA~1/POSTGR~1/15/share/extension\tdeforpg2.control"
C:\PROGRA~1\POSTGR~1\15\share\extension\tdeforpg2.control を削除しますか (Y/N)?
y
```

2. tdeforpg2--*.sql を削除します。

```
CMD> DIR /b "C:/PROGRA~1/POSTGR~1/15/share/extension\tdeforpg2--*.sql"
tdeforpg2--2.1--2.1.1.sql
tdeforpg2--2.1.1--2.2.sql
tdeforpg2--2.1.sql
tdeforpg2--2.2--2.3.sql
CMD> DEL /p "C:/PROGRA~1/POSTGR~1/15/share/extension\tdeforpg2--*.sql"
C:\PROGRA~1\POSTGR~1\15\share\extension\tdeforpg2--2.1--2.1.1.sql を削除しますか
 (Y/N)? y
C:\PROGRA~1\POSTGR~1\15\share\extension\tdeforpg2--2.1.1--2.2.sql を削除しますか
 (Y/N)? y
C:\PROGRA~1\POSTGR~1\15\share\extension\tdeforpg2--2.1.sql を削除しますか (Y/N)?
 y
C:\PROGRA~1\POSTGR~1\15\share\extension\tdeforpg2--2.2--2.3.sql を削除しますか (
Y/N)? y
```

3. tdeforpg2.dll を削除します。

```
CMD> DIR /b "C:/PROGRA~1/POSTGR~1/15/lib\tdeforpg2.dll"
tdeforpg2.dll
CMD> DEL /p "C:/PROGRA~1/POSTGR~1/15/lib\tdeforpg2.dll"
C:\PROGRA~1\POSTGR~1\15\lib\tdeforpg2.dll を削除しますか (Y/N)? y
```

5.6 インストールディレクトリの削除

Transparent Data Encryption for PostgreSQL を今後利用しない場合、インストールディレクトリを削除します。

1. インストールディレクトリを削除します。

   次の例では、PostgreSQL 15 用の Transparent Data Encryption for PostgreSQL が C:\Program Files\NEC\TDEforPG2_PG15 にインストールされていることとします。

```
CMD>CD "C:\Program Files\NEC"
CMD>dir
2023/08/15  11:24    <DIR>          TDEforPG2_PG15
CMD>RMDIR /S TDEforPG2_PG15
TDEforPG2_PG15、よろしいですか (Y/N)?Y
```

5.7　ストリーミングレプリケーション構成からのアンインストール

ストリーミングレプリケーションを利用した環境から Transparent Data Encryption for PostgreSQL をアンインストールする手順について説明します。以下の手順でアンインストールします。

また、アンインストール時のプライマリサーバーとスタンバイサーバーのセットアップ手順の要否については、以下の通りです。

表 5-1　アンインストール時の手順要否

手順	作業項目		参照先
	プライマリサーバー	スタンバイサーバー	
1	透過的暗号化機能の無効化		「5.2　透過的暗号化機能の無効化（22 ページ）」
2	Transparent Data Encryption for PostgreSQL のアンインストール		「5.3　Transparent Data Encryption for PostgreSQL のアンインストール（23 ページ）」
3	postgresql.conf の編集		「5.4　postgresql.conf の編集（24 ページ）」
4	ファイルの削除		「5.5　ファイルの削除（25 ページ）」
5	インストールディレクトリの削除		「5.6　インストールディレクトリの削除（25 ページ）」

5.8　高可用性構成（HA 構成）からのアンインストール

CLUSTERPRO X の高可用性構成（HA 構成）を利用した環境から Transparent Data Encryption for PostgreSQL をアンインストールする手順について説明します。以下の手順でアンインストールします。

また、アンインストール時の現用系サーバーと待機系サーバーのセットアップ手順の要否については、以下の通りです。

表 5-2　アンインストール時の手順要否

手順	作業項目		参照先
	現用系サーバー	待機系サーバー	
1	透過的暗号化機能の無効化		「5.2　透過的暗号化機能の無効化（22 ページ）」
2	Transparent Data Encryption for PostgreSQL のアンインストール		「5.3　Transparent Data Encryption for PostgreSQL のアンインストール（23 ページ）」
3	postgresql.conf の編集		「5.4　postgresql.conf の編集（24 ページ）」
4	ファイルの削除		「5.5　ファイルの削除（25 ページ）」
5	インストールディレクトリの削除		「5.6　インストールディレクトリの削除（25 ページ）」

第 6 章
アップグレード

本章では下記 2 パターンのアップグレードについて説明します。

- 「6.1　Transparent Data Encryption for PostgreSQL のアップグレード（28 ページ）」
- 「6.2　透過的暗号化機能が有効な PostgreSQL のメジャーバージョンアップグレード（31 ページ）」

注

以下のような場合は PP サポートサービスにご連絡ください。

- クラスタ構成のアップグレードをご検討の場合

  クラスタ構成の仕様（利用製品）によっては、待機系のアップグレード手順が異なります。
- クラスタ構成で透過的暗号化機能を有効化した端末以外で透過的暗号化機能を制御したい場合
- PostgreSQL の標準機能ストリーミングレプリケーション構成でのアップグレードをご検討の場合
- 高可用性構成（HA 構成）でのアップグレードをご検討の場合

6.1　Transparent Data Encryption for PostgreSQL のアップグレード

アップグレードを行う前に `pg_dumpall` を使用してデータベース全体のバックアップを取得していただくことを推奨いたします。

Transparent Data Encryption for PostgreSQL のメジャーバージョン、マイナーバージョンともに以下の手順に従ってアップグレードを行ってください。

1. Administrator 権限を持つアカウントでログインします。
2. アップグレード対象のデータベースに対して `pg_dump`[*1] コマンドを実行します。透過的暗号化機能を利用するデータベースが複数存在する場合はデータベース毎に実施してください。なお、`pg_dump` 実行前に `PGOPTIONS` 環境変数で encrypt.cipherkey パラメータにデータ鍵の情報を設定することで復号したデータをバックアップすることが可能です（簡易 TDE モードの場合データ鍵の情報の設定は不要です）。バックアップしたデータは復号した状態のため、漏えいのリスクがありますのでご注意ください。

   次の例では、ダンプファイル名として「pg_dump_tdedb.dump」、バックアップ対象のデータベースとして「tdedb」を指定しています。

   - 標準 TDE モードの場合

```
CMD> set PGOPTIONS=-c encrypt.cipherkey=key1234567890
CMD> pg_dump -f pg_dump_tdedb.dump -Fc tdedb
```

- 簡易 TDE モードの場合

```
CMD> pg_dump -f pg_dump_tdedb.dump -Fc tdedb
```

3. 「5.2　透過的暗号化機能の無効化（22 ページ）」を参考に透過的暗号化機能を無効化します。
4. 透過的暗号化機能を利用しているデータベースを停止します。

   次の例では、サービスを停止することで PostgreSQL を停止します。

```
CMD>sc stop postgresql-x64-13
```

ヒント

サービスとして登録していない場合は、pg_ctl[*2] コマンドを利用して PostgreSQL を停止します。

```
CMD> pg_ctl stop
```

5. 「5.3　Transparent Data Encryption for PostgreSQL のアンインストール（23 ページ）」を参考に Transparent Data Encryption for PostgreSQL をアンインストールします。
6. 「5.4　postgresql.conf の編集（24 ページ）」を参考に PostgreSQL の設定ファイル（postgresql.conf）の shared_preload_libraries パラメータに Transparent Data Encryption for PostgreSQL のダイナミックリンクライブラリ tdeforpg2.dll を削除、またはパラメータ自体をコメントアウトします。
7. 透過的暗号化機能を利用しているデータベースを起動します。

```
CMD> sc start postgresql-x64-13
```

ヒント

サービスとして登録していない場合は、pg_ctl コマンドを利用して PostgreSQL を起動します。

```
CMD> pg_ctl start
```

*1　pg_dump コマンドの詳細な利用方法は PostgreSQL マニュアルをご確認ください。

*2　pg_ctl コマンドの詳細な利用方法は PostgreSQL マニュアルをご確認ください。

8. インストール媒体の windows\installer フォルダー配下に格納されている対応する PostgreSQL バージョンの exe ファイルをクリックします。

   exe ファイルの命名規則は以下の通りです。

表 6-1　exe ファイルの命名規則

Edition	命名規則
Enterprise Edition	TDEforPG2_PG<*PostgreSQL バージョン*>_<*Transparent Data Encryption for PostgreSQL バージョン*>.exe

   - PostgreSQL バージョン

     Transparent Data Encryption for PostgreSQL が対応する PostgreSQL バージョンを示します。13 は 13 と表示されます。

   - Transparent Data Encryption for PostgreSQL バージョン

     表記形式は X_Y_Z です。X_Y はメジャーバージョン、Z はマイナーバージョンを示します

9. 「4.2　Transparent Data Encryption for PostgreSQL のインストール（10 ページ）」を参考に新バージョンの Transparent Data Encryption for PostgreSQL をインストールします。

注

インストール先ディレクトリを指定してインストールした場合

Transparent Data Encryption for PostgreSQL の旧バージョンを任意のフォルダーにインストールしている場合は、同一のフォルダーをインストール先フォルダーとして指定します。指定せずに再インストールした場合、デフォルトで指定されたフォルダーにインストールされます。

10. 「4.3　透過的暗号化機能を対話型で有効化する方法（12 ページ）」を参考に透過的暗号機能を有効化します。

11. 「4.4　postgresql.conf の編集（13 ページ）」を参考に postgresql.conf を編集します。

12. 旧バージョンでよりセキュアな運用のための設定を行っていた場合、再度「4.5　よりセキュアな運用のための設定（14 ページ）」を参考に設定を行います。

13. 透過的暗号化機能を利用するデータベースに対して暗号鍵の再登録を行います。旧バージョンで利用していた最新の暗号鍵と同じ暗号鍵をリストアするデータベースに登録する必要があります。また登録する暗号鍵は暗号化アルゴリズムも一致している必要がある点にご注意ください。

```
CMD> "C:\Program Files\NEC\TDEforPG2_PG13\bin\pgtde.bat" -m regist -conf ^
More?  "C:\Program Files\NEC\TDEforPG2_PG13\conf\pgtde_secuser.properties"
Key management mode is not yet set.
Please select key management mode:
1. Simple TDE mode.
```

```
2. Standard TDE mode.
1
Enter new data key:
Retype new data key:
Select algorithm:
1. aes
2. bf
1
Are you sure you want to Regist new key to "tdedb"(DATABASE) with "aes" algori
thm? (Press Y(y) key to execute): Y
New key version 1 is registered to tdedb
```

14. 透過的暗号化機能を利用するデータベースに対してバックアップファイルを使用し、pg_restore[*3] コマンドでリストアします。

    次の例では、バックアップファイルに「pg_dump_tdedb.dump」を、リストア対象のデータベースとして「tdedb」を指定します（簡易 TDE モードの場合 encrypt.cipherkey パラメータは不要です）。

    - 標準 TDE モードの場合

    ```
    CMD> set PGOPTIONS=-c encrypt.cipherkey=key1234567890
    CMD> pg_restore -d tdedb -e pg_dump_tdedb.dump
    ```

    - 簡易 TDE モードの場合

    ```
    CMD> pg_restore -d tdedb -e pg_dump_tdedb.dump
    ```

注

透過的暗号化機能を利用するデータベースが複数ある場合は、バックアップファイルの対応付けにご注意ください。

6.2　透過的暗号化機能が有効な PostgreSQL のメジャーバージョンアップグレード

アップグレードを行う前に pg_dumpall を使用してデータベース全体のバックアップを取得していただくことを推奨いたします。

透過的暗号化機能が有効となっている PostgreSQL のメジャーバージョンアップグレードを行う場合、以下の手順に従って PostgreSQL のメジャーバージョンアップグレードを行ってください。透過的暗号化機能を利用しているデータベースは PostgreSQL の標準機能である pg_dump/pg_restore コマンドを利用します。透過的暗号化機能を利用するデータベースを含んだ状態で pg_dumpall コマンドや pg_upgrade コマンドを使ってデータベースクラスタ全体を移行する方法はサポートしていません。本節の手順を利用することで、Transparent Data Encryption for PostgreSQL と PostgreSQL のメジャーバージョンアップグ

*3　pg_restore コマンドの詳細な利用方法は PostgreSQL マニュアルをご確認ください。

レードを同時に行うことできます。本節の例では、Transparent Data Encryption for PostgreSQL V2.3.0 がセットアップされた PostgreSQL 13 を PostgreSQL 15 にアップグレードします。また、手順では Transparent Data Encryption for PostgreSQL が C:\Program Files\NEC（デフォルト）にインストールされていることとし、透過的暗号化機能コマンド（pgtde）のデータベース接続ファイルとして C:\Program Files\NEC\TDEforPG2_PG13\conf\pgtde_secuser.properties を使用します。

注

PostgreSQL 13.10 まで動作確認を行っておりますが、それ以降の PostgreSQL バージョンにて手順が失敗する場合は別途お問合せください。

1. アップグレード対象のデータベースに対して pg_dump[*4] コマンドを実行します。透過的暗号化機能を利用するデータベースが複数存在する場合はデータベース毎に実施してください。なお、pg_dump 実行前に PGOPTIONS 環境変数で encrypt.cipherkey パラメータにデータ鍵の情報を設定すること復号したデータをバックアップすることが可能です（簡易 TDE モードの場合データ鍵の情報の設定は不要です）。バックアップしたデータは復号した状態のため、漏えいのリスクがありますのでご注意ください。

   次の例では、ダンプファイル名として「pg_dump_tdedb.dump」、バックアップ対象のデータベースとして「tdedb」を指定しています。

   - 標準 TDE モードの場合

   ```
   CMD> set PGOPTIONS=-c encrypt.enable=key1234567890
   CMD> pg_dump -f pg_dump_tdedb.dump -Fc tdedb
   ```

   - 簡易 TDE モードの場合

   ```
   CMD> pg_dump -f pg_dump_tdedb.dump -Fc tdedb
   ```

2. Transparent Data Encryption for PostgreSQL のアップグレードも同時に行っており、旧バージョンの Transparent Data Encryption for PostgreSQL が不要な場合、「第 5 章　アンインストール（22 ページ）」を参考にアンインストールします。アンインストールを行わない場合は、「5.2　透過的暗号化機能の無効化（22 ページ）」のみ実施します。

3. ここまでの手順が完了後、透過的暗号化機能を利用するデータベースを削除します。

   ```
   CMD> dropdb tdedb
   ```

4. PostgreSQL のメジャーバージョンアップグレードを行います。バージョンアップ手順については本節下部の関連リンクをご確認ください。

*4　pg_dump コマンドの詳細な利用方法は PostgreSQL マニュアルをご確認ください。

5. メジャーアップグレード後の PostgreSQL で透過的暗号化機能を利用するデータベースを作成します。

```
CMD> createdb tdedb
```

6. 「第 4 章　新規セットアップ（9 ページ）」を参考にメジャーアップグレード後の PostgreSQL に透過的暗号機能をインストールします。

7. 透過的暗号化機能を利用するデータベースに対して暗号鍵の再登録を行います。旧バージョンで利用していた最新の暗号鍵と同じ暗号鍵をリストアするデータベースに登録する必要があります。また登録する暗号鍵は暗号化アルゴリズムも一致している必要がある点にご注意ください。

```
CMD> "C:\Program Files\NEC\TDEforPG2_PG15\bin\pgtde.bat" -m regist ^
More? -conf "C:\Program Files\TDEforPG2_PG15\conf\pgtde_secuser.properties"
Key management mode is not yet set.
Please select key management mode:
1. Simple TDE mode.
2. Standard TDE mode.
1
Enter new data key:
Retype new data key:
Select algorithm:
1. aes
2. bf
1
Are you sure you want to Regist new key to "tdedb"(DATABASE) with "aes" algori
thm? (Press Y(y) key to execute): Y
New key version 1 is registered to tdedb
```

8. 透過的暗号化機能を利用するデータベースに対してバックアップファイルと作成したユーザーデータリストファイルを使用し、pg_restore コマンドでリストアします。

   次の例では、バックアップファイルに「pg_dump_tdedb.dump」を、リストア対象のデータベースとして「tdedb」を指定します（簡易 TDE モードの場合 encrypt.cipherkey パラメータは不要です）。

   - 標準 TDE モードの場合

```
CMD> set PGOPTIONS=-c encrypt.enable=key1234567890
CMD> pg_restore -d tdedb -e pg_dump_tdedb.dump
```

   - 簡易 TDE モードの場合

```
CMD> pg_restore -d tdedb -e pg_dump_tdedb.dump
```

注

透過的暗号化機能を利用するデータベースが複数ある場合は、バックアップファイルの対応付けにご注意ください。

関連リンク

PostgreSQL アップグレード手順

付録 A. 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。

A.1 コマンドエラーメッセージ

セットアップ機能 cipher_setup.bat（cipher_setup.ps1）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 A-1 Windows 版エラーメッセージ一覧

エラーメッセージ	対処方法
Internal error occurred	内部エラーが発生しています。システム管理者に連絡を行ってください。
You must be Administrators to execute this action.	Administrators 権限を持つアカウントで再度実行してください。
File does not exist: <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。
Must be superuser to execute this action.	接続ユーザーは PostgreSQL のスーパーユーザーを指定してください。
Could not connect to the database.	接続情報の内容を確認してください。
Could not use template1 database.	「template1」以外のデータベースを指定してください。
Security user must not be super user.	セキュリティ管理ユーザーにはスーパーユーザーではないユーザーを指定してください。
Security user could not access to database.	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。
The length of Port must not be zero.	ポート番号には空文字以外を入力してください。
Port must be integer.	ポート番号には整数を入力してください。
The length of Database must not be zero.	データベース名には空文字以外を入力してください。
The length of Superuser must not be zero.	スーパーユーザー名には空文字以外を入力してください。
The length of Database Password must not be zero.	スーパーユーザーのパスワードには空文字以外を入力してください。
The length of Security User must not be zero.	セキュリティ管理者ユーザー名には空文字以外を入力してください。
The length of Security User Password must not be zero.	セキュリティ管理者ユーザーのパスワードには空文字以外を入力してください。
Lock file already exists. File name: $env:INSTALLFILE	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。
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。
Could not activate transparent data encryption feature.	透過的暗号化機能の有効化に失敗しました。出力されたエラーメッセージファイルを確認してください。
'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。
'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。

エラーメッセージ	対処方法
Failed to copy file for tdeforpg2--2.1.sql	tdeforpg2--2.1.sql ファイル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。
Failed to copy file for tdeforpg2--2.1--2.1.1.sql	tdeforpg2--2.1--2.1.1.sql ファイル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。
Failed to copy file for tdeforpg2--2.1.1--2.2.sql	tdeforpg2--2.1.1--2.2.sql ファイル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。
Failed to copy file for tdeforpg2--2.2--2.3.sql	tdeforpg2--2.2--2.3.sql ファイル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。
Failed to copy file for 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。
Failed to copy file for tdeforpg2.dll	tdeforpg2.dll 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。

付録 B. ディレクトリ・ファイル構成

表 B-1 Windows ディレクトリ・ファイル構成

ディレクトリ・ファイル構成			説明
TDEforPG2_PG<XX>\ XX は PostgreSQL メジャーバージョン	bin\	cipher_setup.bat	透過的暗号化機能セットアップ起動バッチ
		cipher_setup.ps1	透過的暗号化機能セットアップスクリプト
		pgtde.bat	暗号化機能実行コマンド
	conf\		
	lib\	tdeforpg2.control	透過的暗号化機能用拡張ファイル
		tdeforpg2--2.1.sql	透過的暗号化機能内部実行スクリプト群
		tdeforpg2--2.1--2.1.1.sql	透過的暗号化機能内部実行スクリプト群（バージョン更新用）
		tdeforpg2--2.1.1--2.2.sql	透過的暗号化機能内部実行スクリプト群（バージョン更新用）
		tdeforpg2--2.2--2.3.sql	透過的暗号化機能内部実行スクリプト群（バージョン更新用）
		tdeforpg2.dll	透過的暗号化機能用ライブラリ
	lib\conf		透過的暗号化機能内部設定ファイル群
	lib\prop		透過的暗号化機能定義ファイル群
	lib\jar		透過的暗号化機能実行基盤ファイル群
	lib\psql	libpq.dll	PostgreSQL 接続用ライブラリ
		psql.exe	内部コマンド発行用 PostgreSQL クライアントプログラム
	template\	pgtde.properties.template	透過的暗号化機能コマンド pgtde 用設定ファイルのテンプレート
	log\		Transparent Data Encryption for PostgreSQL 用のデフォルトログ出力先
	LICENSE		利用しているオープンソースライセンスについて

付録 C. 改訂履歴

本マニュアルの改訂履歴は以下のとおりです。

表 C-1 改訂履歴一覧

版数	発行日	改訂履歴
初版	2023 年 1 月	初版作成
第二版	2023 年 8 月	• 実行コマンドや実行例を修正（全体） • Windows Server 2022 に対応したことを追記(第 3 章 動作環境の確認とインストール前の準備) • PostgreSQL 14、PostgreSQL 15 に対応したことを追記(第 3 章 動作環境の確認とインストール前の準備) • 「OpenJDK Version 8(JRE 8)のインストール」を「JDK のインストール」へ修正(第 3 章 動作環境の確認とインストール前の準備) • 利用する暗号化アルゴリズム bf(Blowfish)は、非サポートであることを追記（第 4 章 新規セットアップ） • アップグレードを追記

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	ＯＳＳＤＢＴＤＥ１１－０２	貴社名 所 属	
マニュアル名	Transparent Data Encryption for PostgreSQL 行単位暗号化 セットアップカード（Windows 版）	お名前	

項番	ﾍﾟｰｼﾞ	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 データ利活用基盤統括部 データモダナイズ事業開発グループ宛

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 Enterprise Edition
行単位暗号化 セットアップカード
（Windows 版）

ＯＳＳＤＢＴＤＥ１１－０２

2023 年 8 月 第二版 発行

日本電気株式会社