cpl.thalesgroup.com

# Postgresデータベースのセキュリティとコンプライアンス

## タレスのデータベース暗号化をEnterpriseDB Postgres Advanced Serverに導入

## 主な利点:

- 強力なファイルシステムレベルのデータ暗号化
- 簡単な管理
- きめ細かな特権ユーザーアクセスポリシーの適用
- 包括的なコンプライアンス管理と監査証跡

## 問題: 機密データには保護が必要である

EnterpriseDB © (EDB™) Postgres Advanced Serverは、オープンソースのPostgreSQLにエンタープライズ機能を組み合わせており、パフォーマンス診断、Oracle © データベースとの互換性、開発者とDBAの生産性向上などの機能により、リスクと複雑さを軽減します。組織は、レガシーアプリケーションの最新化、新しいアプリケーションの開発、またはレガシーデータベースからの移行の時期に、EDB Postgres Advanced Serverを採用しています。機密性の高い規制されたデータは、増え続けるアプリケーションへのデータ元として、EDB Postgres Advanced Serverデータベースに格納されています。このデータを、悪意のある内部関係者や外部攻撃者から保護する必要があります。

## 課題: セキュリティとコンプライアンスを効率的に満たす必要がある

セキュリティ対策が不十分であると、組織は不正行為やデータ侵害にさらされてしまいます。たとえば、データベース内でセキュリティを扱う場合、DBAはデータベースと平文データの両方を管理できます。データベースは意図的にデータを一元的に集約するため、結果として窃盗犯の関心を集める対象となっています。このデータは多種多様であり、顧客の支払いデータ、患者記録、知的財産など、機密性の高い規制されたリソースが含まれます。データベースが正しく管理または構成されていない場合、内部関係者による悪用や、攻撃者が特権ユーザーを装うAPT（Advanced Persistent Threat; 高度で継続的な脅威）攻撃が発生する可能性があります。EDB Postgres Advanced Serverを導入している組織は、データを保護する方法についても考える必要があります。

幸いなことに、EnterpriseDBとタレスは連携して、このセキュリティとコンプライアンスの問題に対処しています。

# CipherTrust Transparent Encryption (CTE透過暗号化) EnterpriseDBに導入

**ソリューション**

CipherTrust Transparent Encryption (CTE透過暗号化)は、一元化された鍵管理、特権ユーザーアクセス制御、詳細なデータアクセス監査ログに裏打ちされたファイルシステムレベルの暗号化により、EnterpriseDB Postgres Advanced Serverの保存データを保護します。CTE透過暗号化は、Postgres Advanced Serverが存在する、オンプレミス、クラウド全体、コンテナ環境内のどこでもデータを保護します。

CTE透過暗号化の導入はシンプルで拡張性に優れ、迅速に行えます。エージェントはEDB Postgres Advanced Serverがインストールされているオペレーティングファイルシステムまたはデバイスレイヤに常駐し、それより上のレイヤで稼働するデータベースとすべてのアプリケーションに対して透過的に暗号化と復号化を実施します。CTE透過暗号化は、中断、労力、コストを最小限に抑えながら、データセキュリティのコンプライアンスとベストプラクティスの要件に対処します。CTE透過暗号化の実装はシームレスであり、導入時や展開時でもビジネスプロセスと運用プロセスのどちらも変更することなく継続させます。CTE透過暗号化は、FIPS 140-2 Level 3まで認証済みのCipherTrust Manager (CM)連携して動作します。CipherTrust Manager (CM)は、CipherTrust Data Security Platform (CDSPデータセキュリティプラットフォーム) の暗号鍵とポリシー管理を一元化します。

**タレスのCipherTrust Transparent Encryption (CTE透過暗号化) をEnterpriseDB Postgres Advanced Serverに導入する理由**

CTE透過暗号化をEnterpriseDB Postgres Advanced Serverに導入すると、機密性の高い規制されたデータが安全であり、保存データの保護を義務づけるコンプライアンスに対処していることを確信できるため、自信を持って新しいアプリケーションを構築したり、レガシーシステムをPostgresに移行したりすることができます。タレスの一元化された鍵管理を使用すると、EnterpriseDB Postgres Advanced Serverを組織の大規模なセキュリティ戦略に効率的に組み込むことができます。特権ユーザーアクセス制御と詳細なデータアクセス監査ログにより、チーム間でセキュリティと管理データベースの職務を分離し、データのセキュリティの可視性を向上させることができます。これにより、データの安全性が向上すると同時に、主要なコンプライアンス要件を満たすことができます。

## 簡単な管理

CipherTrust Transparent Encryption (CTE透過暗号化)は、データ暗号化の実装と維持に必要な時間と労力を、最小限に抑えます。CTE透過暗号化ファイル暗号は、データベースや関連するアプリケーションのコード変更を必要とせずにデータを保護します。さらに、基盤となるCipherTrust Manager (CM)は、エンタープライズのストレージ、データベース、アプリケーション全体にわたって保存データの暗号鍵とポリシーを管理する、統合された一元的なプラットフォームを提供します。

## きめ細かな特権ユーザーアクセスポリシーの適用

セキュリティチームは、CTE透過暗号化を使用して、EDB Postgres Advanced Serverへのきめ細かな、最小特権のユーザーアクセスポリシー(ユーザー、プロセス、ファイルタイプ、時刻など)を設定し適用できます。セキュリティ管理者はこれらのポリシーを使用して、特定のユーザーに平文データへのアクセス権を付与したり、実行できるファイルシステムコマンドを制限したりすることができます。これらのアクセス制御は、システムとデータの間に分離層を確立し、データへのアクセスのセキュリティと可視性を向上させます。これによりセキュリティチームは、データベース管理者に、EDBのPostgres Advanced Serverデータベースの構成と継続的な保守を、そのデータベース内の機密データに平文アクセスせずに管理する許可を与えることができます。

## 包括的なコンプライアンス管理と監査証跡

CTE透過暗号化は、詳細なデータアクセス監査ログを提供して、暗号化、データ主権、最小特権のポリシー、データアクセス監査に関連する多くの一般的なコンプライアンスと規制管理に対処します。監査人は、インテリジェンスログを使用して、暗号化、鍵管理、アクセスポリシーの有効性を評価します。ログには、ユーザーとプロセスによってデータにアクセスされた日時、適用されているポリシー、リクエストが許可されたかどうか、さらには特権ユーザーが「switch user」などのコマンドを送信して別のユーザーになろうとした日時も記録されます。また、VTEには主要なSIEM(Security Information and Event Management; セキュリティ情報およびイベント管理)システムとの統合機能があらかじめ組み込まれているため、ログデータをすぐに活用できます。

## EnterpriseDB

エンタープライズPostgres企業であるEnterpriseDB (EDB)は、優れたスケーラビリティ、セキュリティ、および信頼性を実現できるように最適化された、オープンソースをベースとしたデータ管理プラットフォームを提供しています。EDB Postgresは、組織をよりスマートにするとともに、エンタープライズで実績のある管理ツール、セキュリティ強化、Oracleとの互換性により、リスクと複雑さを軽減します。世界の4000以上の顧客が、トランザクション処理、データウェアハウス、顧客分析、Webベースアプリケーションを含むさまざまなワークロードを、オンプレミスおよびクラウドの両方に展開しています。

詳細な技術仕様については、cpl.thalesgroup.comまたはwww.enterprisedb.comをご覧ください。

## タレスについて

皆様がプライバシー保護を信頼して任せている相手は、そのデータを保護するためにタレスに頼っています。データセキュリティに関しては、組織が直面する決定的な局面は次々と増え続けています。その局面が暗号化戦略の策定、クラウドへの移行、コンプライアンス要件の順守のいずれであっても、デジタルトランスフォーメーションを保護するためにタレスに頼ることができます。

決断の瞬間のための、確実なテクノロジー。





**お問い合わせ先 –** cpl.ipsales@thalesgroup.com すべてのオフィスの所在地と連絡先情報につきましては 、cpl.thalesgroup.com/ja/contact-usをご覧ください。