個人情報を守り抜く！

Fujitsu Enterprise Postgres で情報漏洩と改ざんをシャットアウト

近年、企業がインターネットを通じて収集した個人情報をビジネスに活用する取り組みが増えてきています。一方で、本人の承諾なしでの個人情報活用や情報漏洩問題が依然として大きな課題となっており、EU 一般データ保護規則（GDPR）やカリフォルニア州消費者プライバシー法（CCPA）などの個人情報保護規制が世界中で導入され始めています。そのため、企業はこれらの規制に従って個人情報を適切に扱う必要があります。個人情報保護規制の元でデジタルイノベーションを促進し、企業活動を将来に渡り維持するためには、個人情報を含むデータを管理するデータベースシステムのセキュリティを強化することが重要です。

本記事では、個人情報保護規制で重要視されている「機密性」と「完全性」を保つための手段として、Fujitsu Enterprise Postgres によるデータベースシステムのセキュリティ対策を紹介します。この対策により、個人情報を暗号化して「安全に」保管し、改ざんを防止／検知してデータを「正確に」維持することができるようになります。また、Scalar 社のデータベースミドルウェア製品である ScalarDL と連携することで、データが改ざんされていないことの証明もできます。

暗号化による安全なデジタルデータの保管

情報漏洩は、企業の信用を揺るがす重大なセキュリティ事故です。その対策の 1 つが暗号化であり、万が一個人情報が流出した際に第三者によって閲覧されることを防止することができます。しかし暗号化を行う場合、アプリケーションに暗号化処理を追加する開発や、暗号鍵管理などの運用が負担となります。

Fujitsu Enterprise Postgres では、個人情報を含むデータを安全に保管するために富士通独自の透過的データ暗号化機能を提供しています。本機能は、「開発効率化」、「運用性向上」、「性能影響の極小化」の大きく 3 つの特徴を持ちます。暗号化・復号によって生じる開発／運用の複雑性、性能影響を限りなく抑えつつ、データベース全体を暗号化することが可能です。

- 開発効率化
    - データの暗号化・復号はデータベース側で透過的に行われるため、アプリケーション側での暗号化・復号処理の開発は不要
- 運用性向上
    - データベース管理者が 1 コマンドで暗号化キーの更新作業ができるなど、暗号化機能のメンテナンス作業を簡略化
    - 外部の鍵管理システムとの連携により、組織や業務システム内に存在する暗号化キーの管理を一元化することが可能となり、鍵管理作業の負荷を軽減
- 性能影響の極小化
    - AES 暗号化・復号処理をハードウェアと連携して高速化することで、暗号化によるオーバーヘッドを削減

透過的データ暗号化機能については下記の記事でも説明しています。

- 情報漏えいに備えよ！PostgreSQL で透過的暗号化を実現
- 透過的データ暗号化のクラウド鍵管理システム連携

改ざん防止／検知による正確なデジタルデータの維持

個人情報を含むデータを電子的記録媒体に格納する場合、不正アクセスによりデータが改ざんされるリスクが存在します。改ざんが発生すると誤ったデータに基づいて業務が処理されるため、システムが誤作動したり停止する問題が発生して企業活動が継続できなくなり、社会的信頼が低下してしまいます。このリスクに対処するためには、改ざんが発生しないようにデータを管理し、万が一改ざんが発生した際には検知・復旧して対象のデータを正確に保つことが必要です。個人情報保護規制においても、データを正確に維持し、改ざんが発生した場合は迅速に本人へ通知することが求められています。

Fujitsu Enterprise Postgres では、改ざんの防止と検知のための機能を提供しています。防止の観点では、認証やアクセスコントロールの機能により不正なユーザーによる改ざんを防ぐことができます。PostgreSQL 標準の機能に加えて、認証やアクセスコントロールの運用をサポートするための「ポリシーに基づいたパスワードの運用」や「機密管理支援」などの富士通独自の機能も提供しています。さらに、前述の透過的データ暗号化機能を利用することで、ディスク上のデータの改ざんを抑止することも可能です。次に検知の観点では、監査ログ機能を独自に提供しています。本機能を利用することで監査ログを専用のログファイルに出力でき、さらに PostgreSQL の拡張モジュールである file_fdw を介してログ管理ツールと連携することで不正アクセスなどによる改ざんを検知することができます。

監査ログ機能の詳細については下記の記事で説明しています。

- 技術を知る：PostgreSQL の監査ログ ～ データベースのセキュリティ脅威を検知する ～

非改ざん性保証への取り組み

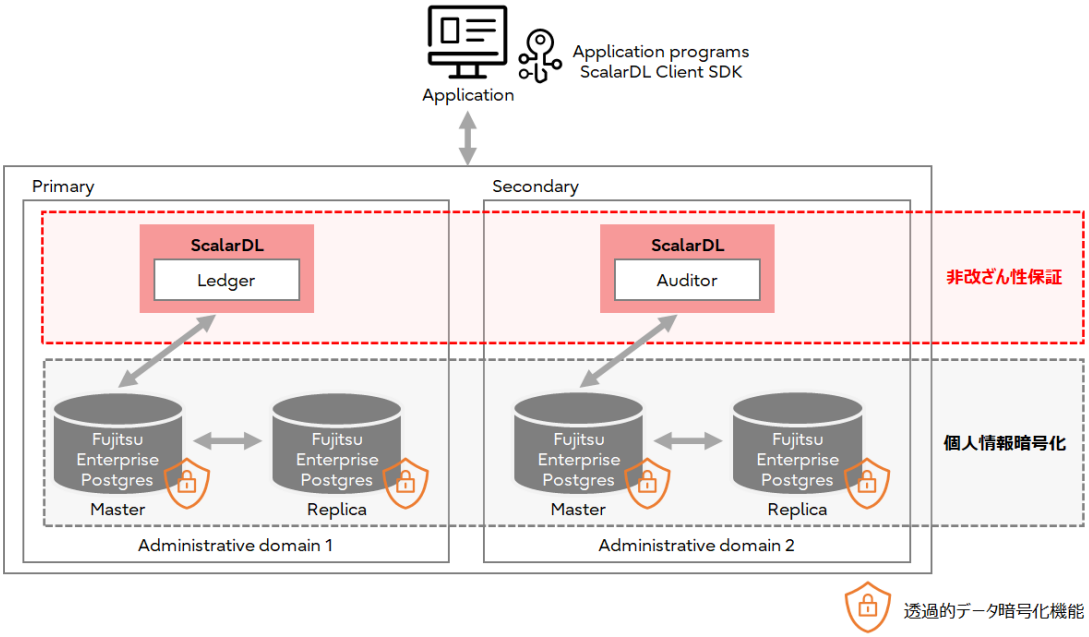
改ざんの防止や検知だけでなく、データが改ざんされていないことの証明（非改ざん性保証）が必要になることもあります。例えば、GDPR では個人情報提供時の同意履歴が改ざんされていないことの証明が必要になります。また、特許訴訟においては知的財産の先使用権の証明にもなります。この非改ざん性保証のためには、分散型台帳技術で守られたデータの更新履歴を管理する仕組みを追加しなければなりません。

Fujitsu Enterprise Postgres は、Scalar 社が提供するミドルウェア製品である ScalarDL と連携することで、このようなデータの非改ざん性保証をデータベースに導入できます。

ScalarDL は、データベースに対して耐改ざん性を付与する製品であり、改ざん検知および非改ざん性保証を実現できます。
ScalarDL は以下の特徴を持っています。

- Ledger と Auditor という 2 つの管理ドメインで管理することで、データベース全体が改ざんされるケースに対しても非改ざん性の保証が可能
- アプリケーションは電子署名されたコントラクトによって管理されるため、トレーサビリティが向上

Fujitsu Enterprise Postgres と ScalarDL を連携する場合、ユーザーは ScalarDL 経由で非改ざん性の担保が必要となるデータの登録を行います。登録されたデータは、改ざんされてしまうと参照時に必ずエラーが発生します。そのため、参照できたデータは改ざんされていないことの証明にもなります。



まとめ

デジタルイノベーションによるビジネスプロセスや顧客体験の改革を推し進めるためには、個人情報を含むあらゆるデータを適切に管理し、活用することが重要となります。Fujitsu Enterprise Postgres は、個人情報を管理する上で必要となる透過的データ暗号化や監査ログなどの機能を独自に備える、安心して利用可能なデータベースです。また、ScalarDL との連携によってデータの非改ざん性の保証を支援します。

- ScalarDL（Scalar 社の製品ページへ）
  https://www.scalar-labs.com/ja/scalardl
- Fujitsu Enterprise Postgres（当社の製品ページへ）
  https://www.fujitsu.com/jp/products/software/middleware/database/enterprisepostgres/

2024 年 5 月 13 日