

富士通のデータベース「Fujitsu Enterprise Postgres 15（以降、Enterprise Postgres 15）」は、初版が 2023 年 4 月にリリースされました。さらに、セキュリティ機能を強化した SP1 が 2023 年 10 月、PostgreSQL 15 の最新版にリベースした SP2 が 2024 年 1 月にリリースされました。ここでは、Enterprise Postgres 15 の製品概要をご紹介します。（注）

- 注） 本記事では、初版と SP1、SP2 を合わせて Enterprise Postgres 15 と定義します。

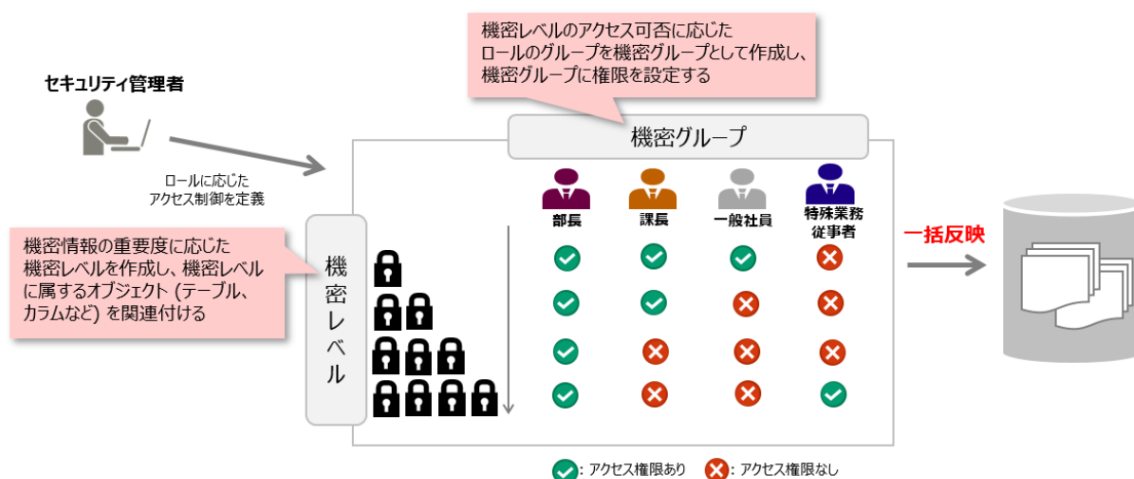
Enterprise Postgres 15 ご紹介

Enterprise Postgres は、PostgreSQL を拡張し、セキュリティ、性能、信頼性を強化したデータベースです。開発当初より、堅牢な運用性が求められるミッションクリティカルシステムに対応するため、さまざまな機能を提供してきました。また、DX(デジタルトランスフォーメーション)に向けてデジタル化が加速する社会に対応するため、オンプレミス、クラウド、エッジなどさまざまなプラットフォームを併用するハイブリッドな環境やマルチクラウドでの運用を実現するハイブリッドデータベースとしての側面も持ち合わせています。しかし、このような環境下では、データの活用方法やデータの管理方法が多様となり、限定されていたデータの活用領域が飛躍的に広がることで、情報漏洩やサーバー攻撃といったセキュリティ脅威につながりかねません。

Enterprise Postgres は、このようなセキュリティの脅威に対応するため、従来から「透過的データ暗号化」や「監査ログ」といったセキュリティの機能を提供してきました。Enterprise Postgres 15 ではデータへのアクセス制御の設定を支援する「機密管理支援機能」の提供や「透過的データ暗号化」の機能エンハンスを行うことで、セキュリティ機能をさらに強化しています。

機密管理支援機能

誰がどのデータをどのようにアクセス可能とするのかといったデータベースへのアクセス制御の設定を支援する機能です。通常、このアクセス制御を 1 件 1 件設定していく必要があり、設定する際もデータベースのセキュリティに関する高度なスキルが必要となります。機密管理支援機能を利用することで、あらかじめ、ロールがどの機密レベルにアクセス可能かを示す機密グループと機密レベルの組み合わせを定義し、その定義に基づいて、一括してアクセス制御を設定できます。煩雑な設定操作を繰り返す必要がありません。また、運用開始後のセキュリティ監査においても、セキュリティ設定時の定義内容と実際に設定されている内容との比較を支援する機能が提供されているためセキュリティ監査作業の負荷が軽減でき、効率的なセキュリティ運用が可能となります。

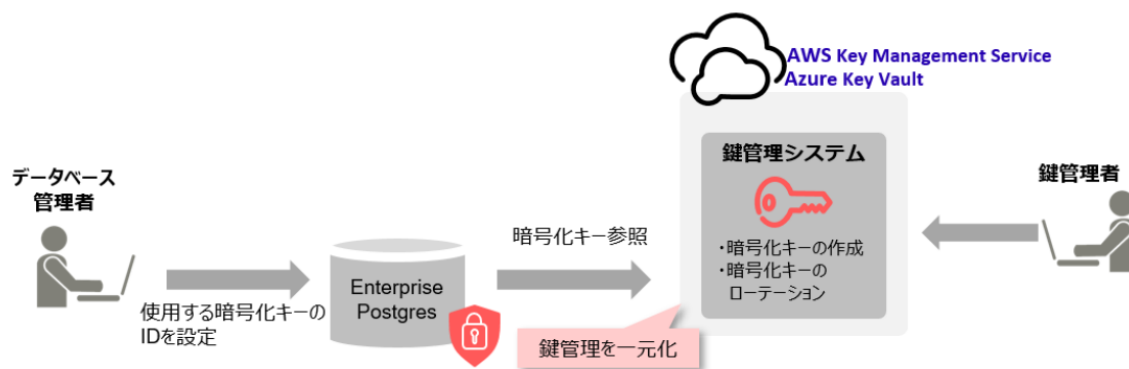


関連コンテンツ

- データベースのアクセス制御を簡単に実現 ～Enterprise Postgres の機密管理支援機能～

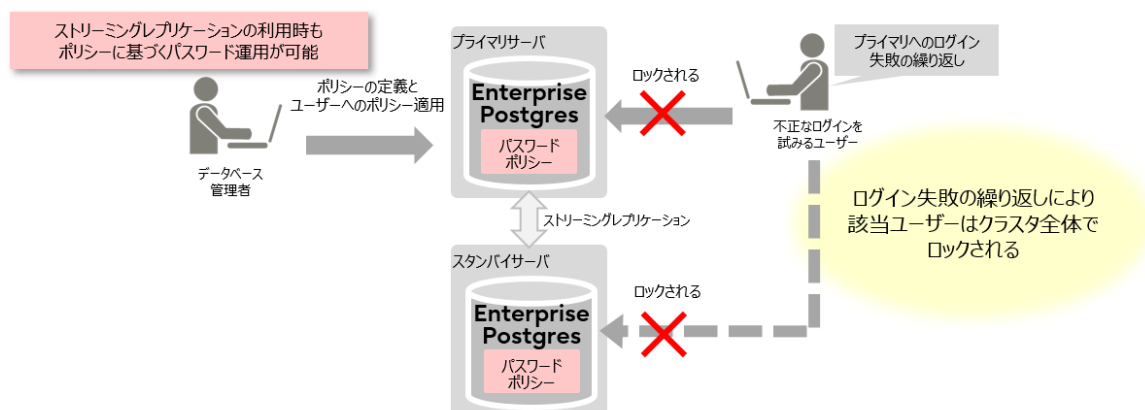
透過的データ暗号化のクラウド鍵管理システム連携

Enterprise Postgres では、従来よりデータベースの格納データを暗号化する「透過的データ暗号化」機能を提供しています。Enterprise Postgres 15 では、透過的データ暗号化で使用するキーストアとして、クラウドの鍵管理システム（Amazon Web Services（以降、AWS）の「Key Management Service」や Microsoft Azure（以降、Azure）の「Key Vault」など）を利用した暗号化キーの管理が可能となりました。鍵管理システムは、暗号化キーの保存やアクセス制御などセキュリティを強化する機能とともに、暗号化キーのライフサイクル管理など運用コストを削減するための機能を実装しています。透過的データ暗号化のクラウド鍵管理システム連携により、データベースの暗号化データと暗号化キーを分離して保存することで、データ漏洩のリスクを軽減することができます。また、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で鍵管理作業の負荷を減らしつつ、セキュアな鍵管理が実現できます。

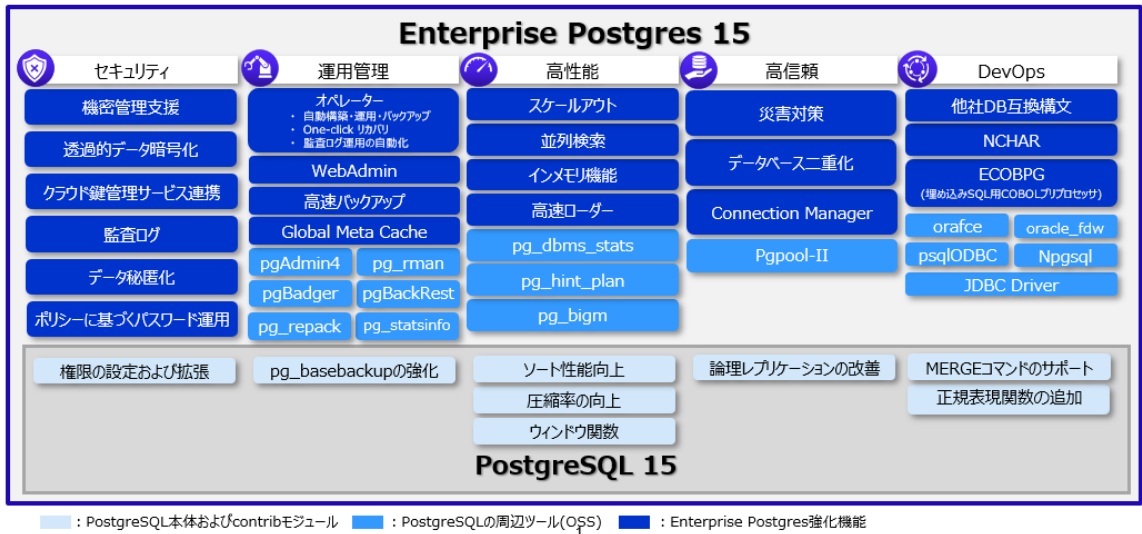


ポリシーに基づくパスワード運用

データベースに接続する際のクライアント認証としてパスワード認証を利用する場合、データベース管理者は事前に定義されたセキュリティポリシーに基づいたパスワードの運用をデータベースの利用者に強制できます。データベースユーザーのパスワードの利用状況が事前に定められたポリシーから外れている場合、データベースへの接続を拒否したり、パスワードの変更を強制したりできます。パスワード認証に対する制限は、パスワードポリシーを定める情報をデータベースユーザーに適用することで有効になります。組織のポリシーに沿ったパスワード運用を強制することにより、コンプライアンスを強化します。ログインに失敗し続けたユーザーに対してはアカウントをロックし、不正ログインを防止します。



以下の図は、Enterprise Postgres 15 が提供する機能の一部です。Enterprise Postgres 15 においては、PostgreSQL 本体と製品に同梱されている OSS が最新化されています。



PostgreSQL 15 では、「ソート性能向上」や「pg_basebackup の強化」など、性能や運用に関する機能が強化されています。PostgreSQL 15 の機能の詳細については、当社社員で PostgreSQL メジャーコントリビューターの Amit Kapila が技術者 Blog で解説していますので、併せてご覧ください。

関連コンテンツ

- PostgreSQL15 とその後（技術者 Blog）

また、PostgreSQL 15 の「論理レプリケーションの改善」については、富士通が PostgreSQL コミュニティに提案し、コミットされた機能が取り込まれています。以下では、これらの機能を提案/開発した富士通の技術者が機能を詳しく解説しています。

関連コンテンツ

- 最新動向を知る（技術者 Blog）

DX を推進していくうえで、セキュリティの確保はとても重要な課題です。従来の、守るべきデータはネットワークの内側にある、という考え方ではなく、ネットワークの内外に関わらず、すべてのアクセスやデバイス、ユーザーを監視・制御し、万全の対策を実施しなければなりません。Enterprise Postgres は、あらゆるセキュリティ脅威からデータを守るために、今後もセキュリティに対する機能強化を続けていきます。DX の実現に向け、Enterprise Postgres の利用をご検討ください。

2024 年 1 月 5 日