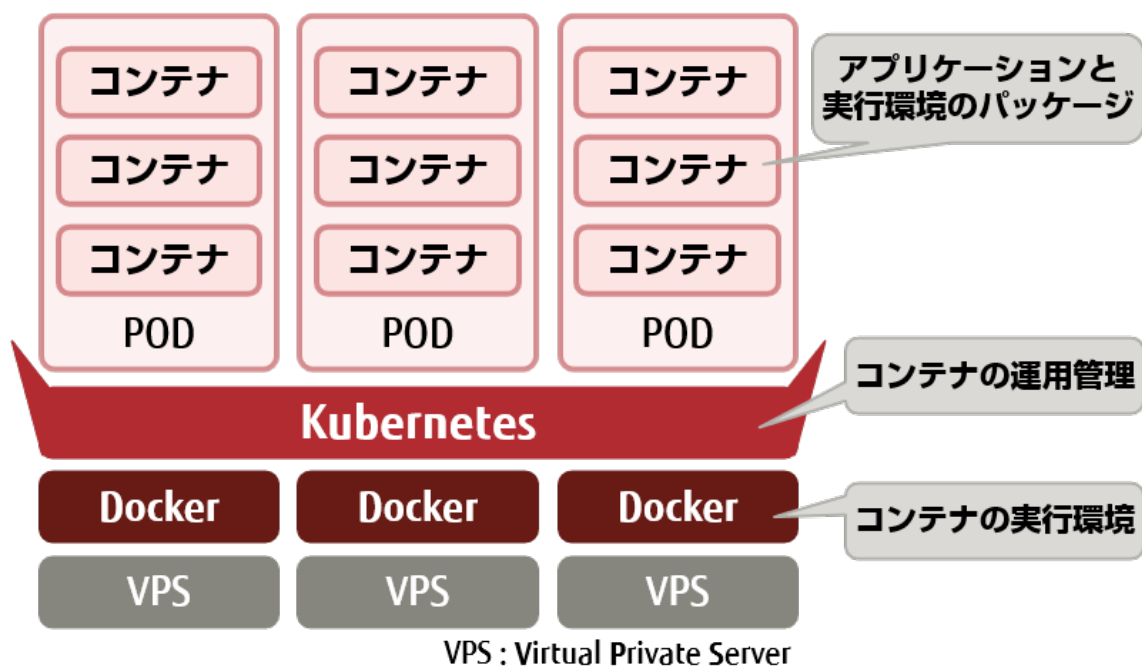


DX の浸透により企業のクラウド利用が本格化しています。データベースにおいても、Amazon や Google などのクラウドベンダーも PostgreSQL を活用したサービスを展開するなど、クラウドでの利用が活性化しています。しかし、仮想環境やプライベートクラウド、パブリッククラウドを併用するハイブリッドクラウドのようなクラウド環境では、それぞれ異なる環境でデータベースを利用するため、運用が複雑になる可能性があります。これを解決するのがコンテナです。それぞれの環境にコンテナ化されたデータベースを配備し利用することで、導入や運用負荷を軽減させることができます。富士通のデータベース「Fujitsu Enterprise Postgres（以降、Enterprise Postgres）」もさまざまなクラウド環境での活用を目的として、コンテナに対応しています。本記事では、コンテナ対応した Enterprise Postgres について、機能と特長を解説します。

コンテナを取り巻く技術について

Enterprise Postgres を説明する前に、まずコンテナを取り巻く技術を簡単に解説します。以下は、その技術を図で示したものです。



コンテナ、POD、Docker、Kubernetes

「コンテナ」は、アプリケーションとアプリケーションの動作に必要な実行環境（ミドルウェア、ランタイム、エンジン、ライブラリーなど）をパッケージ化したものです。コンテナを実行する場合は、個々のコンテナがあたかも別マシンで動いているような隔離環境が作成され、その中でアプリケーションを動作させることができます。コンテナはよく仮想マシンと比較されますが、コンテナには仮想マシンに必要な OS が不要なため、非常に軽量で高速な起動/停止が可能です。「POD」は、アプリケーションの実行単位で 1 つ以上のコンテナから構成されます。そして、コンテナの実行環境が「Docker」です。また、コンテナのシステムでは、上記の図で示すとおり、1 つのシステム内の複数サーバーにコンテナが配備され運用されます。このとき、どのサーバ

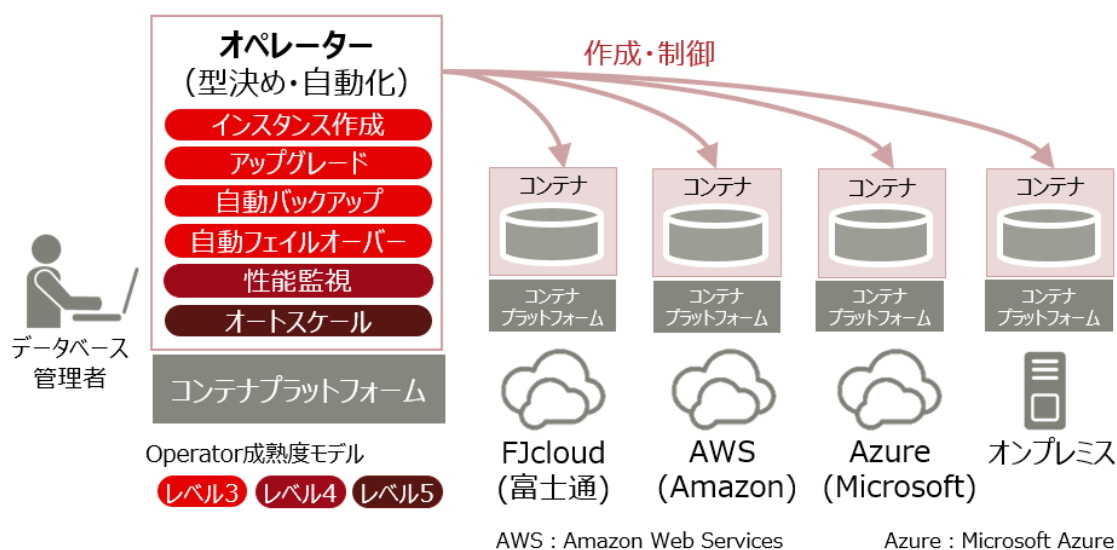
ーにコンテナを配備するのといった振り分けや、サーバーがダウンした場合の冗長化など、コンテナの運用管理を担うプラットフォームが「Kubernetes」です。

ただし、Kubernetes は、オープンソースであることから「サポート期間が短い」、「バージョンアップが頻繁にある」といった点でエンタープライズ向けには課題があります。これらの課題を解決し、エンタープライズに向けて機能を拡張したさまざまな Kubernetes ディストリビューションが提供されています。Kubernetes ディストリビューションは、共通の Kubernetes のコアを持っていることからどこでも使用でき（ベンダー無依存）、また、導入しやすい（サポート期間が長いなど）というメリットがあります。そして、数ある Kubernetes ディストリビューションの中でも Red Hat 社が提供する「OpenShift」は、グローバルで広く利用されている商用のプラットフォームです。

Enterprise Postgres のオペレーターを紹介

Enterprise Postgres は、Red Hat OpenShift Container Platform（RHOCP）をはじめ、Kubernetes をコアとするさまざまなコンテナプラットフォーム上で利用可能であり、マルチクラウドやハイブリッドクラウドに適用することができます。また、クラウド上でのデータベースの運用においては、運用管理のコスト削減が期待されます。Enterprise Postgres では、データベースをコンテナ化するだけでなく、データベースの運用管理を支援/自動化するツール「オペレーター」を提供しています。オペレーターでは、データベースの構築や運用作業が型決めされており、クラウド上でのデータベースの導入やセットアップ、運用管理を自動化することができます。

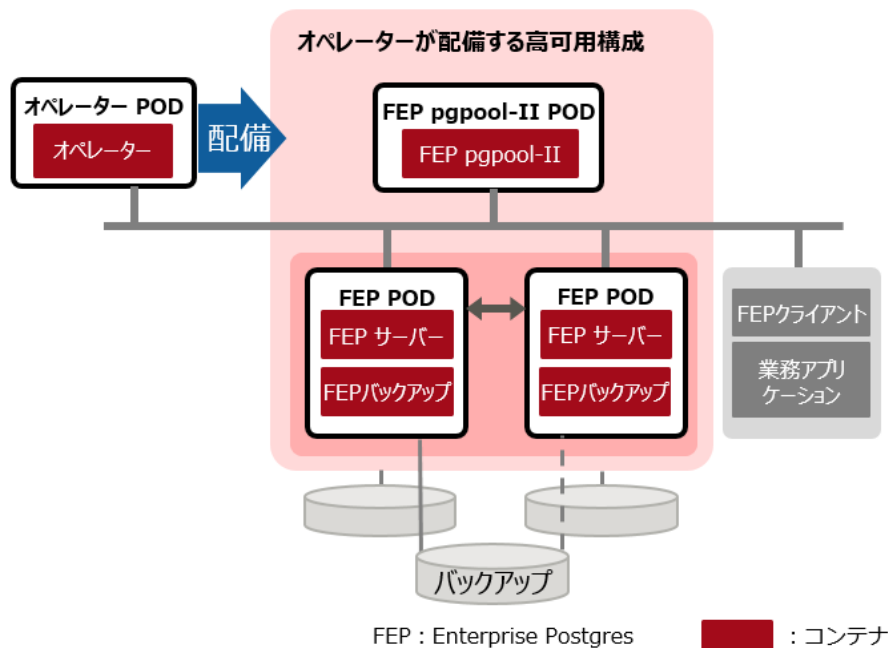
オペレーターは、Operator 成熟度モデルの「レベル5」に対応した Operator です。OpenShift の利用者であれば、Red Hat Ecosystem Catalog から Enterprise Postgres のコンテナとオペレーターが利用可能です。



オペレーターで簡単に高可用運用を実現

Enterprise Postgres は、もともとミッションクリティカルを目的としたデータベースですが、コンテナでもその方向性は変わりません。この Enterprise Postgres が持つ高可用性、高信頼性をコンテナで可能にしているのが Kubernetes のオペレーターである「オペレーター」です。Kubernetes のオペレーターは、コンテナのインストールや運用の自律化を支援する機能であり、オペレーターもこの考え方を継承しています。オペレーターは、データベース運用に必要な運用管理（冗長化やフェイルオーバー/復旧、コネクションプーリング、ロードバランス、バックアップ/リカバリ など）を自動化することで、高可用、高信頼を保持したままクラウド上でのシステム構築や運用の容易性を実現します。

例えば、以下のシステムをオペレーターで構築する場合には3分で Enterprise Postgres サーバーの配備が完了します。また、フェイルオーバー発生時の切り替えと冗長化構成への復元も3分で実現できます。オペレーターは、起動、停止、配備が迅速に行えるコンテナの特長を活かした機能だと言えます。



オペレーターでセキュリティも万全

オンプレミスと比べると、クラウド環境における情報漏洩、不正アクセスなどのセキュリティリスクを不安視する声が少なくありません。Enterprise Postgres では、「機密管理支援機能」、「監査ログ」、「透過的データ暗号化」などセキュリティリスクに対抗する機能が提供されていますが、これらの機能は、コンテナ上でも利用することができ、セキュアなデータベース運用が実現できます。

さらに、オペレーターを利用することで、これらのセキュリティ機能の設定や運用を自動化したり、セキュリティをさらに強化することができ、低コストで高度なセキュリティ運用が可能です。

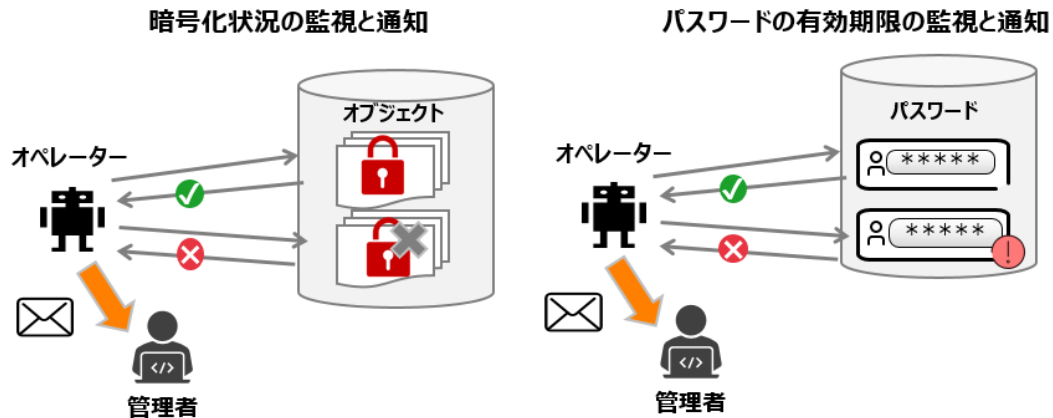
機密管理支援機能の自動化

Enterprise Postgres の機密管理支援機能は、データベースに対するアクセス制御の設定を支援する機能です。オペレーターではインストール時に機密管理支援機能がセットアップ済みで、セキュリティポリシーに準拠した適切なアクセス制御を簡単に設定できます。これによりヒューマンエラーが減少し、不正アクセスなどのセキュリティリスクを軽減できます。

関連コンテンツ

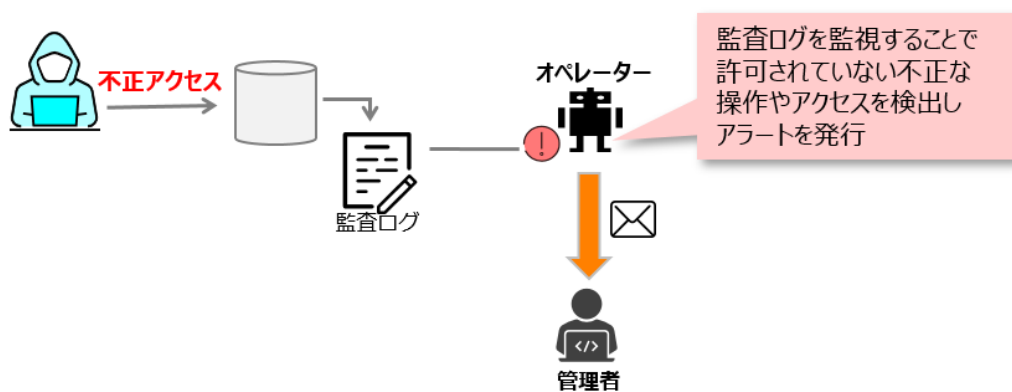
- データベースのアクセス制御を簡単に実現 ～Enterprise Postgres の機密管理支援機能～

また、セキュリティポリシーに違反する操作（暗号化されていないオブジェクトの検出やパスワードの有効期限切れ）が発生した場合、迅速に違反操作を検出し、アラートが通知されます。



監査ログ運用の自動化

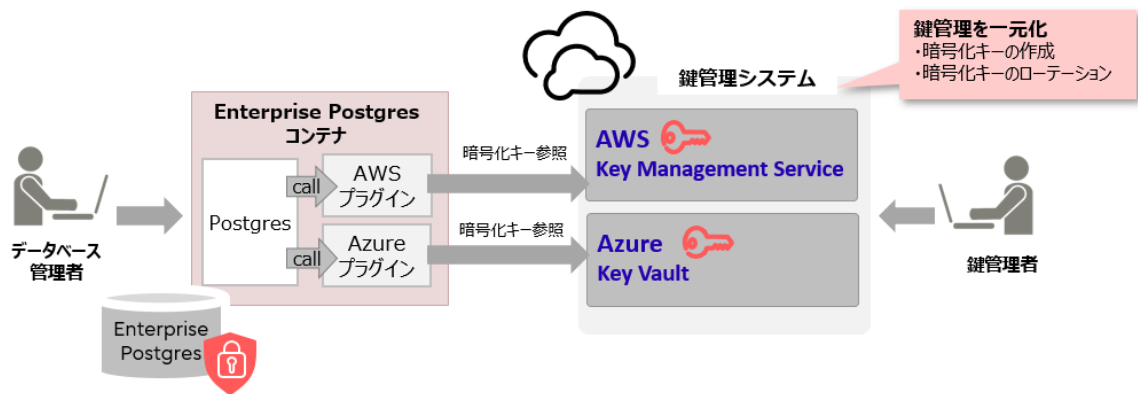
監査ログ機能は、データベースアクセスに関する詳細な情報を監査ログとして取得します。オペレーターでは設定パラメーターを簡素化し、取得した監査ログは外部ストレージに一定期間保存できます。また不正アクセスを自動で検出し、アラートが通知されます。



これらのアラート機能を使用することで、早い段階でセキュリティ違反の検知が可能となり、その影響を最小限に抑えることができます。

透過的データ暗号化のクラウド鍵管理システム連携

透過的データ暗号化は、Enterprise Postgres が従来から提供している、データを暗号化する際にアプリケーションの修正が不要な暗号化の機能です。暗号化キーの保存場所として、外部のクラウドの鍵管理システム（AWS の「Key Management Service」や Azure の「Key Vault」）を利用できます。オペレーターでは、配備するコンテナイメージにあらかじめパッケージ化された AWS および Azure プラグインを備えているため、このプラグインを利用することで簡単に鍵管理システムと連携することができます。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。



今後の取り組み

Enterprise Postgres が提供するオペレーターは、高信頼、高可用、セキュリティといったデータベースシステムにおける必須要件を維持しつつ、どのような環境においても、データベースを堅牢に、かつ容易に運用できることを目指しています。そして、DX によるクラウド利用が加速するなか、セキュリティ運用の自動化や災害対策運用の強化など、Enterprise Postgres は、今後もセキュアなデータベース運用を、簡単に、かつ安全に実現するための取り組みを続けていきます。

2023 年 5 月 15 日