【DevSecOps を導入する】
データベース観点でのセキュリティ対策

DevSecOps（デブセックオプス）は、開発チームと運用チームが協力しあってシステムを開発・運用することで、ビジネスの価値を高めるための様々な取り組みを示す DevOps に、セキュリティも融合させて、柔軟かつスピーディーにシステム開発を行う手法です。 DevSecOps は大きく開発工程（Dev）と運用工程（Ops）の 2 つに分かれ、さらに細分化されて全体で 8 つの工程があり、各工程でセキュリティ対策（Sec）を実施します。 DevSecOps の概要については、「【DevSecOps とは？】入門者向けにメリットなどの概要を分かりやすく解説」を参照ください。

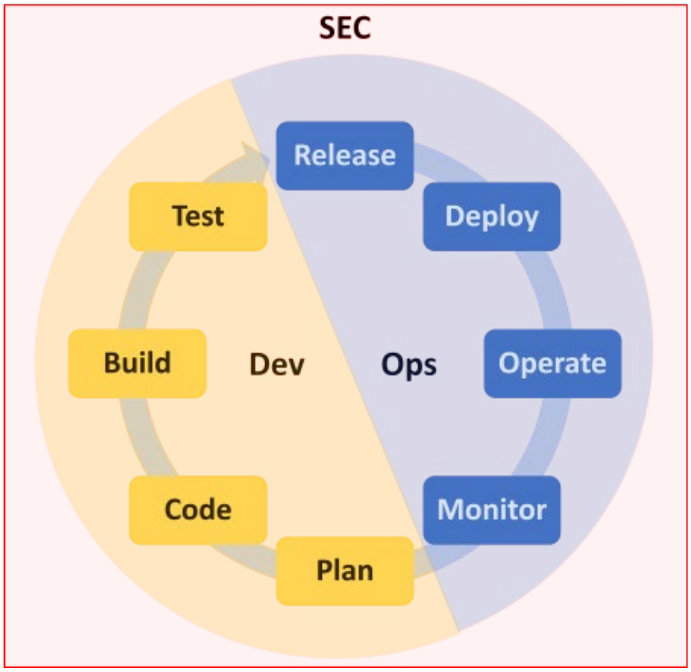

図 1：DevSecOps の全体像

富士通では、製品およびサービスを通してお客様の情報セキュリティの確保・向上に努めています。そのため、セキュリティは製品品質を担保するうえで必須と考えています。 本記事では、DevSecOps での「データベース観点でのセキュリティ対策」で実施すべきことを、富士通のデータベース「Fujitsu Enterprise Postgres（以降、Enterprise Postgres）」を例として詳しく解説します。なお、Enterprise Postgres の情報セキュリティポリシーの考え方については、以下を参照ください。

- データベース製品の情報セキュリティポリシー

1. 開発工程におけるセキュリティ対策

DevSecOps の開発工程である Plan 工程から Test 工程に対し、データベース観点でのセキュリティ対策を解説します。 開発工程の詳細、データベース観点でのセキュリティ対策と作業の詳細、および利用可能な Enterprise Postgres の機能について、表 1 に示します。

表 1 DevSecOps の開発工程（Dev）におけるデータベース観点でのセキュリティ対策

工程	データベース観点でのセキュリティ対策	作業の概要	利用可能な Enterprise Postgres の機能
Plan	セキュリティポリシーの策定	機密性、完全性、可用性の観点で情報セキュリティポシリーを検討	機密管理支援、透過的データ暗号化、クラウド鍵管理サービス連携、データ秘匿化、監査ログ、バックアップ・リカバリー、データベース多重化、フェイルオーバー
	基盤選択	運用するシステムやサービスの規模に合ったリソースの見積り、HA 構成（注 1）、DR 構成（注 2）、およびクラウドの鍵管理システムなど可用性観点での構成の検討	
	コンプライアンスチェック	OSS のライセンス、他社特許混入を確認	
	DBMS 設計	データ構造・正規化、ペルソナ・ロール、アクセス権限などを検討	
Code	データベースの定義資材の作成	スキーマ、ロール、権限などのデータベースの Data Definition Language（以降、DDL）定義を作成	pgAdmin、デザインシート（注 3）、機密管理支援
	プログラミング	SQL 文によるプログラム作成、コード静的品質の確保	—
Build	資源の一元管理	データベースを構成するための定義資材を一元管理	—
	資源の分散管理	HA 構成、DR 構成、および暗号化した鍵の分散管理を考慮した資源配置	—
Test	業務テスト	システムテスト（業務結果、資源量の調整、性能・セキュリティの確認）を実施	機密管理支援、透過的データ暗号化、クラウド鍵管理サービス連携、データ秘匿化、監査ログ、バックアップ・リカバリー、データベース多重化、フェイルオーバー
	ペネトレーションテスト	侵入防止策に応じたテストを実施	—

注 1） HA は High Availability の略で、可用性が高められたシステム構成のことです。

注 2） DR は Disaster Recovery の略で、災害対策が施されたシステム構成のことです。

注 3） Enterprise Postgres の動作に必要な設定値を一覧にまとめた資料です。

1.1 Plan 工程

Plan 工程では、業務システム全体のタスク管理や開発要件に基づき、設計します。具体的には、次の 4 つを実施します。Plan 工程の内容が後工程の礎となるため、詳細かつ綿密にセキュリティ対策を検討することが重要です。

セキュリティポリシーの作成

構築する業務システムのセキュリティ対策を、機密性、完全性、可用性の 3 つの観点で設計します。各観点に対応した Enterprise Postgres の機能とその解説記事をご紹介します。

- 機密性：情報に対するアクセス権限を徹底して保護管理するために、ロール設計とアクセス制御、暗号化によるデータ盗難時のリスクヘッジ、暗号化した鍵の管理、データ秘匿化など、機密性確保の方針を決めます。
    - **機密管理支援**：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**：情報に漏えいに備えよ！PostgreSQL で透過的暗号化を実現
    - **クラウド鍵管理サービス連携**：Enterprise Postgres 運用ガイドの「鍵管理システムをキーストアとして使用する場合の透過的データ暗号化の運用」
    - **データ秘匿化**：Enterprise Postgres 運用ガイドの「データ秘匿化」
- 完全性：改ざんや過不足のない正確な情報を保持するために、監査ログの取得やデータの保管や転送などの運用に準じたバックアップとリカバリーなど、完全性確保の方針を決めます。また、ランサムウェア攻撃を考慮したバックアップ運用も重要です。
    - **監査ログ**：PostgreSQL の監査ログ ～セキュリティ対策は万全！監査ログで情報漏えいを検知～
    - **バックアップ・リカバリー**：PostgreSQL のバックアップとリカバリ –
- 可用性：情報をいつでも安全に利用できるようにするために、データベースの多重化構成との切り替え運用、被災後に業務継続するためのクラスタソフトウェアと連携したフェイルオーバー手番、事業継続対策など、可用性確保の方針を決めます。
    - **データベース多重化**：Enterprise Postgres クラスタ運用ガイド（データベース多重化編）
    - **フェイルオーバー**：Enterprise Postgres クラスタ運用ガイド（PRIMECLUSTER 編）

基盤選択

「セキュリティポリシーの作成」で決めた方針を実現するために、次の 3 つの観点で業務システムの基盤を選択します。

- サイジング：扱うデータ量とデータ増加量、および業務の性能要件などを考慮して、運用するシステムやサービスの規模に合ったリソース（サーバーやネットワーク）を見積ります。クラウドサービスの場合は臨機応変にリソースの増減が可能ですが、オンプレミスの場合は現状想定される最大量と将来の増分量を事前に見積ることをお薦めします。リソースの見積もりは以下を参照ください。
    - Enterprise Postgres 導入ガイド（サーバ編）の「資源の見積り」
- サーバーの分散構成：セキュリティの観点から、HA 構成、DR 構成、および「**クラウド鍵管理サービス連携**」の分散方法について、サーバー構成や配置場所を決めます。
- ランサムウェア対策：ランサムウェア攻撃に備えて、オンラインバックアップの方法、バックアップ用のディスクの分散数、更新不可ディスクの利用を決めます。

コンプライアンスのチェック

業務システムを構築するソフトウェアについて、同梱する周辺 OSS のライセンスに遵守しているか、他社特許を侵害していないか、問題発生時のパッチ提供対応が規定されているかなどのコンプライアンス上の問題が無いかを確認します。

DBMS 設計

「セキュリティポリシーの作成」で決めた方針を実現するために、データ構造・正規化、ペルソナ・ロール、アクセス制御などデータベースシステムを設計します。
特にセキュリティ対策で重要なのは、ロールとアクセス制御の設計です。 誰がどのデータにどのようにアクセス可能とするかといったデータベースへのアクセス制御の設定や運用を設計します。制限するオブジェクトの種別や分類方法（ポリシー）を決めておくことで、セキュリティポリシーに則ったシステム開発ができます。 アクセス制御の詳細設計には、「**機密管理支援**」を利用します。詳細は以下を参照ください。

- Enterprise Postgres セキュリティ運用ガイドの「機密管理の設計」

1.2 Code 工程

Code 工程では、Plan 工程で定義した開発要件に沿って、実際にデータベースの構成要素を作成します。

データベースの定義資材の作成

本工程において、セキュリティ対策として実施すべき作業は以下です。

- 業務システムの処理するための定義するものとして、ロール、権限、プロシージャ、スキーマ、テーブル、インデックス、ビュー、設定ファイルなどのデータベース観点の資材を作成します。Enterprise Postgres は、DDL の範囲は基本的に PostgreSQL をベースとしています。DDL 定義には、「pgAdmin」や PostgreSQL の周辺 OSS である DBeaver を利用できます。
- データベース全体の動作環境は設定ファイルに指定します。Enterprise Postgres の設定ファイルについては、「**デザインシート**」を用意していますのでご利用ください。
- 機密管理支援を考慮した定義：「**機密管理支援**」の関数とテーブルを使って、管理アクセス制御の観点を考慮します。「**機密管理支援**」の定義については以下を参照ください。
    - Enterprise Postgres セキュリティ運用ガイドの「機密管理支援機能の使用方法（定義）」

プログラミング

構築する業務システムで動作する業務アプリケーションを作成します。アプリケーション開発については以下を参照ください。

- Enterprise Postgres アプリケーション開発ガイド

本工程において、セキュリティ対策として実施すべき作業は、以下です。

- アプリケーションの静的解析：セキュリティの脆弱性、性能問題、SQL 基準への不適合などを検出します。PL/pgSQL の静的解析や SQL インジェクションの脆弱性検出には、PostgreSQL の周辺 OSS である plpgsql_check を利用できます。
- SQL の性能を考慮したコーディング：アプリケーションの組み方により、処理性能が異なるため、性能要件に見合ったアプリケーションになるようチューニングが必要です。
    - チューニング ～SQL チューニングを実施する～

1.3 Build 工程

Build 工程では、Code 工程で作成した資材を基に開発環境に業務システムを構築します。次の観点で必要な資源を配置します。

- 資源の一元管理：「1.2 Code 工程」で作成したデータベースの構成要素をまとめて配置・管理します。
- 資源の分散管理：「1.1 Plan 工程」の「基盤選択」で決めたとおりに、資源を分散配置します。

1.4 Test 工程

Test 工程では、開発環境や検証環境でビルドしたものに不具合が無いか、Plan 工程の設計通りに動作するかを確認します。本工程を踏むことで、開発工程の生産物の品質を確保できます。テスト結果に問題があった場合は、Code 工程に戻って修正します。脆弱性スキャンやその他のテスト用の自動ツールを利用します。

- 業務テスト：業務単位の動作、性能およびアクセス制御（認証、許可、監査）の観点で、「1.1 Plan 工程」で取り入れた機能を使って検証テストを実施します。「**機密管理支援**」に沿って設定した内容と実際のオブジェクトやロールの状態確認することで、業務テストを効率化できます。
- ペネトレーションテスト：システム全体の観点で、サイバー攻撃耐性がどれくらいあるかを試すための侵入テストを実施します。

開発工程（Dev）の Test 工程で、すべてのテストが完了し、残課題が無いことを確認したら、運用工程（Ops）に進みます。

2. 運用工程におけるセキュリティ対策

DevSecOps の運用工程である Release 工程から Monitor 工程に対し、データベース観点でのセキュリティ対策を解説します。 運用工程の詳細、データベース観点でのセキュリティ対策と作業の詳細、および利用可能な Enterprise Postgres の機能について、表 2 に示します。

表 2 DevSecOps の運用工程（Ops）におけるデータベース観点でのセキュリティ対策

工程	データベース観点でのセキュリティ対策	作業の概要	利用可能な Enterprise Postgres の機能
Release	なし	なし	なし
Deploy	セットアップ	本番環境のセットアップ、データベースの構築	WebAdmin、サーバーコマンド、オペレーター
Operate	起動・停止、バックアップ・リカバリー、計画切り替え、トラブル対処	アクセス制御、データの保護、ランサムウェア攻撃を考慮した定期バックアップ	WebAdmin、サーバーコマンド、オペレーター
Monitor	容量監視、性能監視、アクセス監視	業務量、資源量、性能低下、DB 容量、およびアクセス状況（監査ログ）を監視	WebAdmin、サーバーコマンド、監査ログ、機密管理支援、オペレーター
	セキュリティ障害の通知	セキュリティ障害に関する修正対応の広報	富士通セキュリティ広報（注 4）

- 注 4） 富士通がセキュリティ障害に関する情報を社内外に向けて広報することを指します。

2.1 Release 工程

Release 工程では、開発環境に構築した業務システムを本番環境に適用するスケジュールや手順を決めます。

2.2 Deploy 工程

Deploy 工程では、開発環境に構築した業務システムを本番環境に配備します。Enterprise Postgres のインストール、セットアップおよびマスターとなるデータベースを構築します。 Enterprise Postgres のセットアップには、Web ベースの GUI ツール「**WebAdmin**」および「**サーバーコマンド**」の 2 つがあります。「**WebAdmin**」を使用すると、基本的な設定や運用操作を GUI で行うことができます。 運用管理ミドルウェアと連携する場合や、より高度な運用を行う場合は、「**サーバーコマンド**」を使ってセットアップします。詳細は以下を参照ください。

- Enterprise Postgres 導入ガイド（サーバ編）

また、コンテナ型データベースを利用して「**オペレーター**」を使うと、クラスタ配備の支援や以降の運用操作の自動化ができます。詳細は以下を参照ください。

- Enterprise Postgres オペレーターユーザーズガイド

2.3 Operate 工程

Operate 工程では、本番環境で業務を開始します。起動・停止、定期バックアップ、保守作業およびトラブル対応を実施します。Enterprise Postgres の運用には、「**WebAdmin**」および「**サーバーコマンド**」で実施できます。 「1.1 Plan 工程」で設計した方針に基づいて運用します。セキュリティ対策としては、トラブル発生抑止のために定期バックアップを確実に実施することと、ランサムウェア攻撃などによるトラブル発生時の迅速なリカバリーが大切です。富士通の統合運用管理ソフトウェア Systemwalker や周辺 OSS である Hinemos と連携することで、業務システムの運用管理を軽減できます。
また、コンテナ型データベースを利用して「**オペレーター**」を使うと、自動バックアップ、自動リカバリー、自動フェイルオーバー、オートスケールなどにより運用操作を自動化できます。詳細は以下を参照ください。

- 環境を選ばずにデータベースの運用を自動化！ ～Enterprise Postgres のオペレーター機能～

2.4 Monitor 工程

Monitor 工程では、運用やお客様から得られた情報（性能値、評価、要望など）を確認します。監視項目には、サーバーの死活、OS のリソース、メッセージ、ディスクの容量、PostgreSQL の死活、性能、監査ログ、機密管理支援の設定内容、セキュリティ障害状況などがあります。
Enterprise Postgres の監視は、「**WebAdmin**」または「**サーバーコマンド**」で確認できます。 セキュリティ対策としては、「**監査ログ**」や「**機密管理支援**」を使い、セキュリティ上の問題が無いかを定期的に監視します。周辺 OSS の pg_statsinfo、pgBadger および Zabbxi などと連携して業務システムを監視することもできます。連携できる監視ツールの詳細や利用方法については、以下を参照ください。

- データベースシステムの監視 ～監視の概要～の「3.3 監視ツール」
- pg_statsinfo で統計情報を収集・蓄積する
- pgBadger でログファイルを解析し、統計レポートを作成する

また、コンテナ型データベースを利用して「**オペレーター**」を使うと、監査ログ運用の自動化や OSS の監視ツールと連携して自動化できます。詳細は以下を参照ください。

- コンテナ型データベースで運用コアストを削減 ～Enterprise Postgres の高可用オペレーター機能～

万が一、富士通製品にセキュリティ障害が検出された場合には、出荷済の富士製品の公式対応に則り、富士通は「**富士通セキュリティ広報**」を迅速に行い、SE またはシステムの保守担当が修正対応することで、お客様のセキュリティ被害を最小限に抑えます。

現業務システムに対する改善点や要望は、次の Plan 工程につなげます。

3. DevSecOps の導入効果

Enterprise Postgres を使った業務システムの開発・運用に DevSecOps の手法を導入することで、脆弱性などのセキュリティリスクの早期検出および全体のリスク低減と、設計から運用開始までの開発速度の向上を実現できます。各工程でサイクルが回ってセキュリティ対策の確認やツールのチェックを重ねることで、担当者はセキュリティを含めてやるべきことを明確にでき、好循環を得られます。特に Plan 工程にセキュリティ観点を入れることが、セキュリティ上の品質向上と工程全体の効率化につながります。

現在のビジネスにおいて IT は欠かせないものとなりました。頻繁な機能追加や継続的なアップデートが必要なシステムやサービスには、迅速かつ効率的な対応が求められます。開発チームと運用チームそれぞれの業務範囲の目的達成だけではなく、お客様のシステム利用価値を意識した DevSecOps の考え方は、現代のビジネスを実行するために、重要なファクターになるでしょう。
業務システムの構築に、Enterprise Postgres を導入する際には DevSecOps を活用し、安心・安全な業務システムの運用管理を実現ください。

2023 年 8 月 4 日

