データベース製品の情報セキュリティポリシー

富士通では情報セキュリティポリシーを定め、製品およびサービスを通じ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。

- 富士通の情報セキュリティ
  https://www.fujitsu.com/jp/about/csr/security/
    - 補足：情報セキュリティとは
        - 押さえておきたい基礎知識！情報セキュリティの 3 要素とは
          https://www.fujitsu.com/jp/solutions/business-technology/security/secure/column/201703-1/

データベース製品の開発部隊では、お客様の財産であるデータを守るための製品提供にむけ、当社の情報セキュリティポリシーに沿った確かな製品とサービスを提供いたしております。
遂行にあたっては「人、プロセス、体制の強化と継続的な改善が必須」と考え、このポリシーに則りながら活動の改善を続けています。

1. 人材教育

情報社会において組織を脅威から守り、事業を継続するためには、従業員の情報セキュリティ知識と意識の醸成が起点になると考えています。

セキュリティ教育の徹底

情報セキュリティを取り巻く環境は様々な側面で変化しており、それを取り巻く脅威や課題も変わります。例え強固な情報セキュリティの対策を施してルールを策定しても、環境の変化をキャッチアップしたものでない限り、そのルールは陳腐化し守られなくなっていきます。そのため、社員の意識を維持・向上させるには定期的に最新の情報提供を伴う情報管理研修を行い、社員教育を徹底する必要があります。
富士通では、全社員に毎年セキュリティ教育を実施し、社員の知識と意識の向上に努めています。また、協業関係のパートナー会社への教育も実施し、富士通グループとして同水準の商品およびサービスの提供を実現しています。

セキュリティアーキテクト制度

教育により得たルール順守と、専門知識による情報セキュリティの強靭化を推進するために「セキュリティアーキテクト」制度を導入しています。それぞれの製品やサービスの知識と情報セキュリティに関する最新知識を統合し、富士通が提供する製品の情報セキュリティの強度を向上させる施策開発を目的に、情報セキュリティの品質確保を主導・監督する担当者を各製品開発プロジェクトに配置しています。これにより、最新の情報セキュリティの脅威への対応と監査、および問題への迅速な対応が可能となり、お客様への安心・安全な製品提供へとつながります。

2. セキュアな開発プロセス

次に、最新の情報セキュリティの脅威に対応できるセキュアな物作りです。長年にわたり製品開発プロセスに対して情報セキュリティの脅威への対応方針を取り込み続け、品質向上に努めています。
セキュアな製品とサービスを実現・維持するため、製品開発プロセスに情報セキュリティの脅威に対応する活動を組み込むことが重要です。富士通では、ソフトウェア開発におけるビジネスプロセスを体系化した独自規約に基づく開発プロセスがあります。ミドルウェアの開発は約 40 年前から継続して行われており、このプロセスは製品開発で得られた知識、トラブル対応からのフィードバック、お客さまの要望の取り込みなど、最新技術と様々な知見の融合によって常に洗練され続けています。
さらにこのプロセスでは、蓄積してきた知見を何時でも活用できるようにすることで安定した製品提供を実現しています。具体的にはユースケース分析・最新 IT ツール活用・セキュリティアーキテクトによる監査の体系化により、開発プロセスでの情報セキュリティの確保に必要な観点を平準化していることが特徴です。特にデータベース製品の開発の歴史は古く、ユースケース分析に利用できる運用実績を潤沢に備えていることが強みになっています。

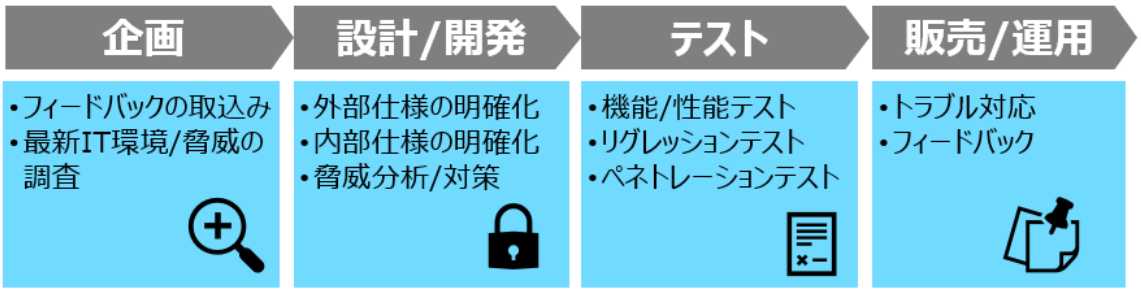

図 1：セキュアな開発プロセス

企画では、製品の利用シーンを様々なユースケースに基づき運用モデルとして作成することで、製品がおかれる環境・状況が可視化され、適切な脅威想定と対策定義・リスクが評価できます。次に構成モデルを作成し、脅威を分析して対策を検討します。設計の「脅威分析」には最新の IT ツールの利用をルール化することで担当者の知識に依存せず正確な分析を行っています。開発が終わったら、セキュリティアーキテクトが製品に問題が無いことを監査します。テストでは、使用ポートやファイル・フォルダのアクセス権限が適切であることなど、頻発する脆弱性の有無をツールによって確認します。販売/運用後は、常にトラブルの発生傾向やフィールド情報を収集し、次の開発に備えて情報を蓄積しています。販売/運用段階(出荷後)に判明した脆弱性に対しては、「富士通の情報セキュリティ」に示した脆弱性対応フレームワークにより、迅速な対応体制を構築しています。

以上のように、最新の IT 活用と最適なヒューマンリソースの両用により、品質の高い製品を安定してお届けできるプロセスが構築されています。

3. 方式と体制

富士通では、安心・安全な製品をお客様に提供するため、品質を作り込むための万全の体制を構築しています。1 つの製品をお届けするまでに複数の議論やチェックを経ることで、お客さまに使っていただく価値ある製品にブラッシュアップを行います。

図 2：プロセスにおけるチェック体制

組織の壁を越えた体制

企画から販売/運用・次期計画まで一貫した製品作りのため、組織の壁を越えた体制を作ります。これは組織横断型の検討・実行チームで、製品所管部門だけでなく、販売管理部門、フィールド運用部門、製品検査部門などから構成され、製品の技術的な側面とビジネスの側面の両面が議論されます。

- 技術的な側面では、市場動向を捉え最新の技術により、お客様課題を解決できているか
- ビジネスの側面では、市場性や他社優位性の判断から、ビジネス継続を維持し、お客様に長く・安定して製品をご利用いただけるか

特に、製品検査部門が企画から運用まで製品所管部門と並走する形で、品質確保に協業する体制が組まれていることが特徴です。最上流工程から入ることにより、問題点を早期検出・解決し、強固な品質確保を実現しています。

これらにより、時代の流れに沿った最新の技術を安定して提供し続けられる活動としていくことで、お客様システムで長期的に安心してご利用頂ける製品にブラッシュアップしていきます。

チェックポイントによる審議

プロセスの区切りにはプログラムマネージャーによるチェックポイントを設けて、現プロセスでの目標や基準値が達成できていることを多角的に審議し、次のプロセス開始の可否を判定します。
企画後の第 1 チェックポイントにおいては、商品企画の背景、商品の顧客価値、拡販・サポート・サービス戦略、リスク管理などを基に審議します。当該製品を開発することにより、お客様に価値ある製品とサービスを安定的に提供できることと共にビジネス性についても確認します。
販売前の第 2 チェックポイントにおいては、製品の品質はもとより、法的な規制の順守、ビジネス状況の再確認などを行います。 このような複数のチェックポイントを設けることにより、お客様の要件を満たし、安心・安全な製品で、永続的にお使いいただける製品をお届けしています。

4. データベース製品の取り組み

ご説明した取り組みのもと、富士通では、お客様の大切な資産であるデータを守るため、情報セキュリティに対応するための機能を備えたデータベース製品として、Fujitsu Enterprise Postgres（以降、Enterprise Postgres と略す）を提供しています。Enterprise Postgres は、OSS（オープン・ソース・ソフトウェア）の PostgreSQL をエンジンとし、富士通のデータベース技術とノウハウで導入・運用のしやすさを向上し、高いセキュリティを持つデータベースです。

データベースに必要な機能

データベースは、お客様情報や社内情報など、企業活動に関わる重要なデータの保管庫です。企業にとって重要な資産が多いため、サイバー攻撃の対象になりやすく、個別の情報セキュリティ対策が必要です。情報セキュリティの 3 要素(機密性、完全性、可用性)に加えて拡張された 4 要素（真正性、責任追跡性、否認防止、信頼性)を意識し、お客様の大切なデータを様々な脅威から守るために、Enterprise Postgres は次に示す機能を提供しています。

- **アクセスコントロール**：データベースのオブジェクトの所有者、またはスーパーユーザーは、データベースユーザーに対するアクセス権限を制御することで、データベースに接続したデータベースユーザーがどのようなテーブルにアクセスできるか、どのような操作を行うことができるかを制御できます。詳細については、以下を参照ください。
    - 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~
    - PostgreSQL: Documentation: 15: Privileges（PostgreSQL オフィシャルのページへ）
      https://www.postgresql.org/docs/15/ddl-priv.html
- **認証**：データベースにアクセスするデータベースユーザーの認証を行うことで、アクセス可能なデータベースを制限できます。また、サーバーを認証して、データベースサーバーのなりすましを防止できます。詳細については、以下を参照ください。

    - Enterprise Postgres 運用ガイドの「ポリシーに基づいたパスワードの運用」
    - PostgreSQL: Documentation: 15: Client Authentication（PostgreSQL オフィシャルのページへ）
      https://www.postgresql.org/docs/15/client-authentication.html
- **監査ログ**：管理者の権限乱用、利用者のデータベースへの不正アクセスなどの脅威に対抗するための機能です。管理者や利用者の処理を追跡するための情報を監査ログとして取得・保持します。詳細については、以下を参照ください。
    - 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～
- **暗号化**：データベース上のデータを閲覧しただけではどのような情報なのかわからない状態にする機能です。機密情報などの盗難や外部漏えいを防ぐことができます。詳細については、以下を参照ください。
    - 情報漏えいに備えよ！PostgreSQL で透過的暗号化を実現
- **データの秘匿化**：アプリケーションによって発行された問合せに対して、一部のデータを改定して参照させることです。例えば、キャッシュカード番号などの個人情報の問合せに対して、最後の数桁を“*”で改訂して返信する場合などに利用できます。詳細については、以下を参照ください。
    - Enterprise Postgres 運用ガイドの「データ秘匿化」
- **バックアップ・リカバリー**：ディスク障害やデータ破壊に備えて、定期的にデータをバックアップします。バックアップを基に最新状態に確実に復旧できます。詳細については、以下を参照ください。
    - PostgreSQL のバックアップとリカバリー
- **データベース多重化**：ハードウェアやソフトウェアの故障などに備えて、あらかじめデータベースを多重化することで、重要なデータを保護し、高信頼なデータベース運用を実現します。詳細については、以下を参照ください。
    - 業務停止はさせない！トラブル時は自動切り替えで PostgreSQL の運用を継続
- **フェイルオーバー**：クラスタソフトウェアと連携したフェイルオーバー機能により、異常発生時のシステムの停止時間を短く抑えます。詳細については、以下を参照ください。
    - Enterprise Postgres クラスタ運用ガイド（PRIMECLUSTER 編）

なお、Enterprise Postgres の製品機能の詳細については、以下の製品サイトを参照ください。

- Enterprise Postgres

今後のセキュリティ戦略

ビジネス環境の急速なデジタル化により、今までになかった情報セキュリティの脅威が増えており、従来の情報セキュリティの対応では不十分な状況に陥るケースも珍しくありません。増加・変貌する脅威を分析し、組織に必要な対策を継続して講じることが大切です。
また、データベースの利用は、ますますクラウドへの移行が進み、クラウドベンダーの提供するサービスと共にビジネスを支えるインフラとして重要な役割を果たすようになりました。私達データベース製品の開発部隊では、今後のデータベース利用における脅威として、「特定のクラウドベンダーへの依存」を想定しています。企業の情報セキュリティポリシーは業務や扱うデータによって異なるのが一般的ですが、特定ベンダーのクラウド環境では、そのベンダーの提供する限られたセキュリティのサービスレベルに自社の環境を合わせなければなりません。
そのような状況下でデータベースをセキュアでかつスムーズに運用するには、お客様の用途に応じたきめ細かいセキュリティ機能とハイブリッドクラウドによる運用が最適です。Enterprise Postgres では、パブリッククラウド、プライベートクラウド、オンプレミスの各サービスを効果的にミックスさせたハイブリッドクラウド環境をご提案できます。例えば、個人情報などの機密性の高い重要なデータは社内のオンプレミス環境に配置して高いセキュリティを保ち、公開情報や新しいデータと連携したデータ活用などはデータ量の増減に柔軟に対応できるクラウド環境に配置します。これにより、お客様は多様なセキュリティ要件を満たし、最適なインフラを活用できます。

ぜひ、お客様の情報セキュリティ運用に Enterprise Postgres をご利用ください。

2023 年 10 月 2 日