Document ID: MIREGISTRY-DS-01 Version: 1.0	Effective Date: 2024/03/14
Document Title: 精神疾患レジストリ設計仕様書	

精神疾患レジストリ
設計仕様書

作成日	2024 年 3 月 14 日
作成者	株式会社アクセライト 石田　精一郎
承認日	2024 年 3 月 14 日
承認者	国立精神・神経医療研究センター 病院　臨床研究・教育研修部門　情報管理・解析部 小居　秀紀

目次

1. はじめに

1.1. 本書の目的

本書は精神疾患レジストリシステムの設計仕様、ソリューションアーキテクチャを記載する

2. IT プラットフォーム共通ソリューション選定

2.1. インフラ環境

1. 満たすべき要件

- 要件定義書に記載された非機能要件を満たすこと

2. 選定結果

- 開発したアプリケーションを実行するサーバープラットフォームとしては、構築内容の正確な記録と構築時・運用時を通した完全な監査ログを取得することができ、また、国内外の主要なガイドライン・各種規制要件にも適合可能であることから原則として Amazon Web Services（AWS）を採用する。
- 利用するデータセンター（リージョン）は、国内のものに限定し、メインのシステムは東京、遠隔地バックアップとして大阪を利用する。
- セキュリティと権限管理の観点からプロジェクト専用の AWS を調達する。また、個人情報を管理するシステムと個人情報を含まない医療情報を管理するシステムは、別の AWS アカウントに構築する。AWS アカウントレベルで権限を分離することで、個人情報と医療情報が結び付けられてしまうリスクを最小化する。

2.2. OS・ミドルウェア等

1. 満たすべき要件

- 要件定義書に記載された機能要件および非機能要件を満たすこと
- 機能仕様書に記載された機能を実装可能であること

2. 選定結果

- 以下の表の通り

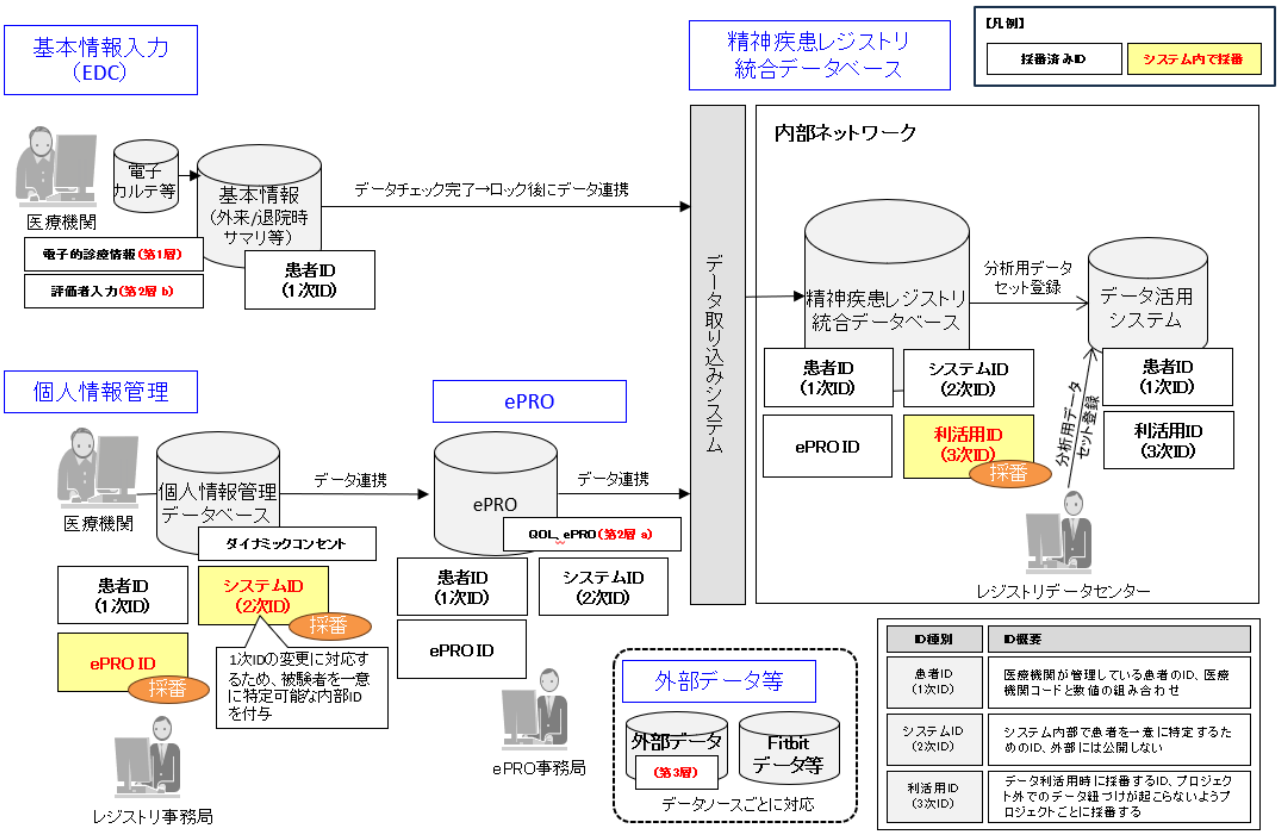
カテゴリ	種別	分類	ソフトウェア ※バージョンは構築時の最新安定版を採用
開発言語	-	-	PHP/JavaScript
開発支援ツール	ソースコード管理	ソース管理ツール	Github
	タスク管理	タスク管理ツール	Backlog
システムソフトウェア製品	ロードバランサー	-	AWS Application Load Balancer
	ファイアーウォール	サーバー	セキュリティグループ
	-	ネットワーク	AWS WAF、Access Control List

	サーバ・ミドルウェア	サーバー	Amazon EC2
	-	OS	Amazon Linux
	-	Web サーバー	Apache
	-	分散メモリキャッシュシステム	Memcached
	フレームワーク	アプリケーションパッケージ	Bricks EDC（Accelight 開発パッケージ）
	データベースソフトウェア	RDBMS	MySQL
	メール送信	メール送信サービス	Amazon Simple Email Service
	モニタリング	監視ソフトウェア	Zabbix

3. システムアーキテクチャ

3.1. レジストリシステム全体のデータフロー概念図

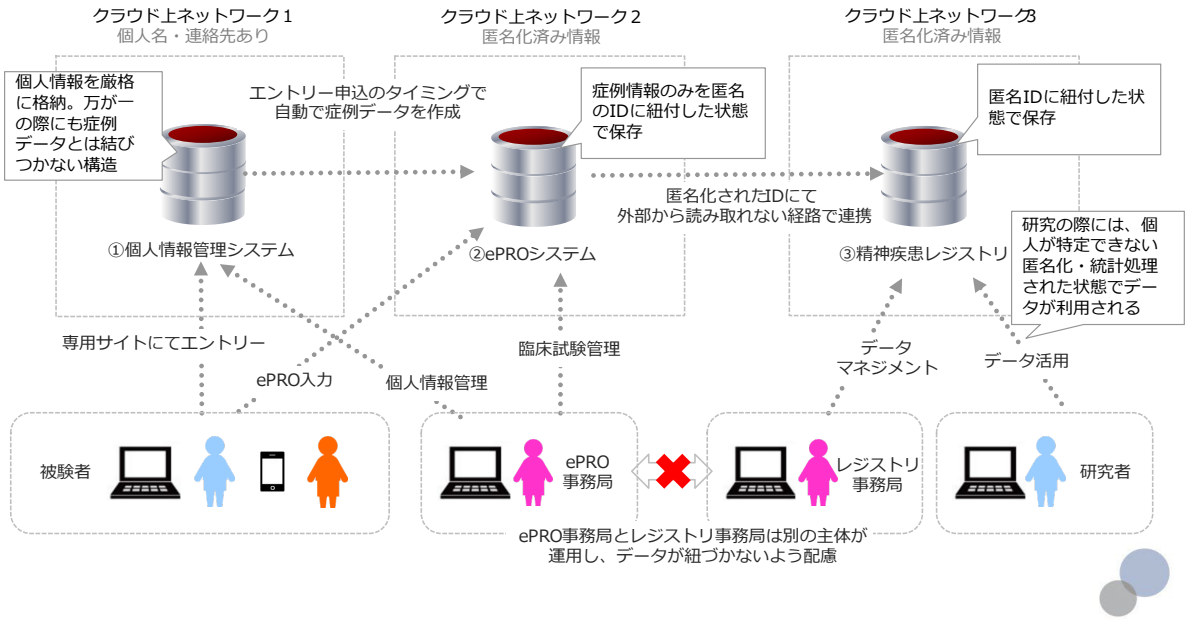
本システムの全体のデータフローは以下の図の通りと定められていている。本書では、これをシステムとして実現するためのアーキテクチャを記述する。



3.2. レジストリシステムのセキュリティ対策

本レジストリシステムでは、高度なセキュリティ対策が求められる。そのため、個人情報管理システムが属する個人情報を管理するネットワークと、個人情報を持たない EDC/ePRO 用ネットワーク、レジストリ本体のネットワークに分け、症例データが特定の個人と紐付かない形で保存し、それぞれ厳格なセキュリティ基準を定めて運用することで情報漏洩のリスクを最小する

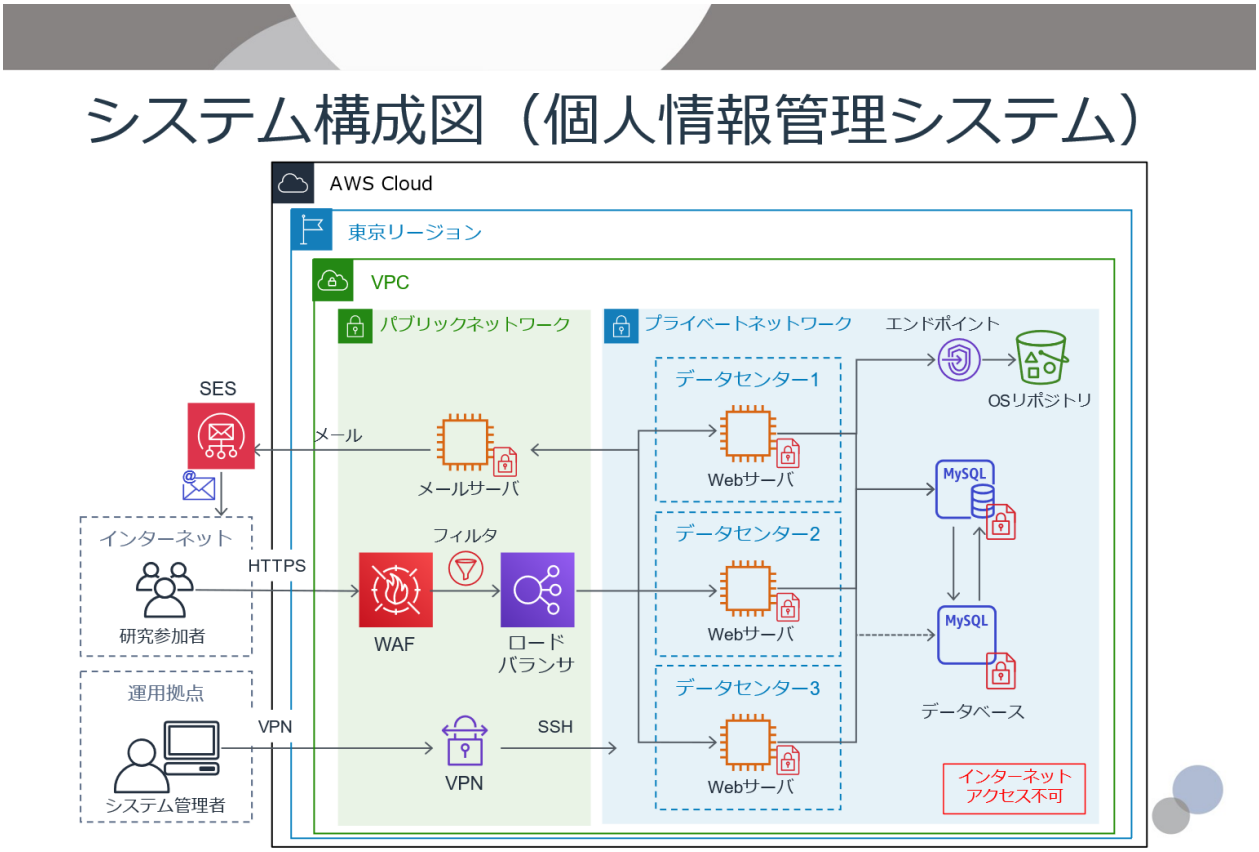
レジストリシステムのセキュリティ対策



3.3.　本システムのシステムアーキテクチャ

上記の基本アーキテクチャの実現のため、システムごとに独立した AWS を利用し、それぞれ最小の権限での連携を行う。各システム構成は以下に示す通り。

1. 個人情報管理システム



【凡例】

パブリックネットワーク
インターネットゲートウェイを通じて外部との通信

プライベートネットワーク
外部との通信経路を持たない

サービスエンドポイント
プライベートネットワークにあるシステムが別のAWSサービスに接続するための接続口

Web Application Firewall
インターネットからのリクエストをモニタリングし、不審なアクセスをブロックする

Application Load Balancer
インターネットからのリクエストを受け付けてアプリケーションに転送する

Amazon Simple Email Service(SES)
信頼性の高いメール送信を実現するAWSのメールサーバー

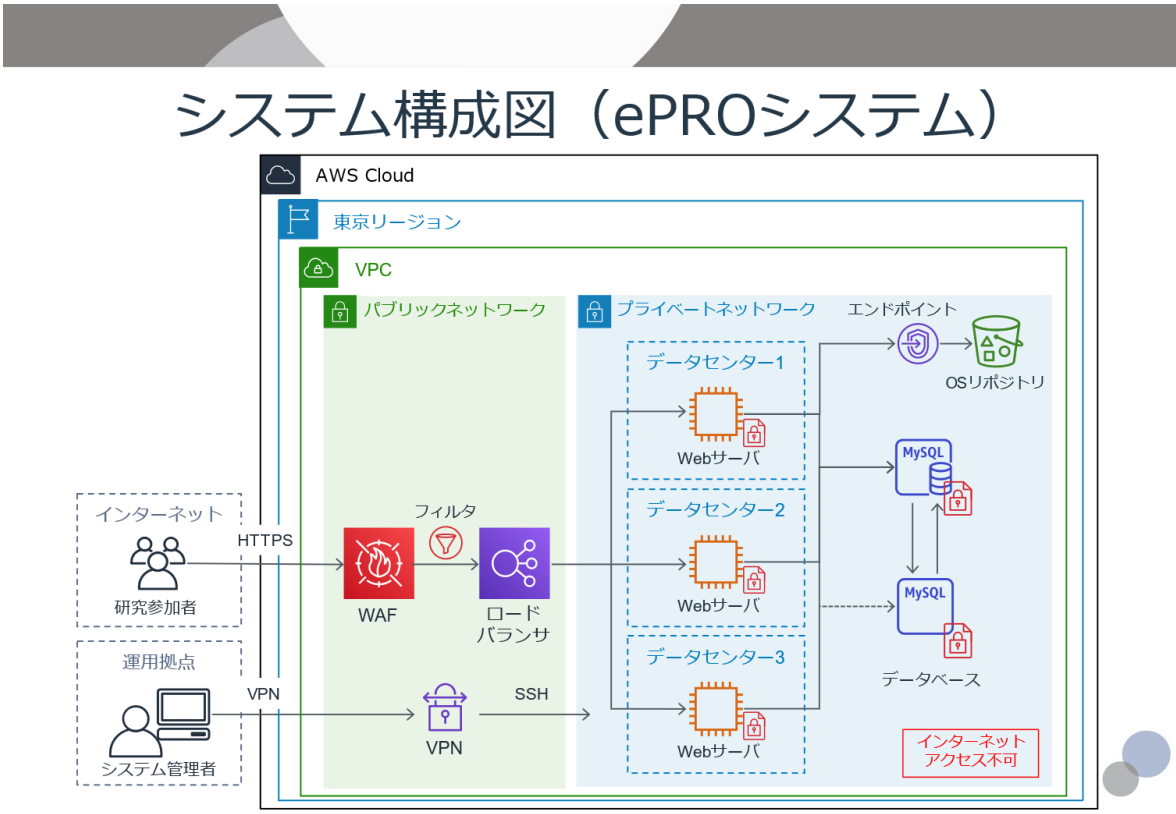
Amazon EC2 Instance
AWSが提供している最も基本的な仮想サーバー

Amazon RDS Mysql Instance
AWSが提供しているリレーショナルデータベースサービスのMySQLサーバー

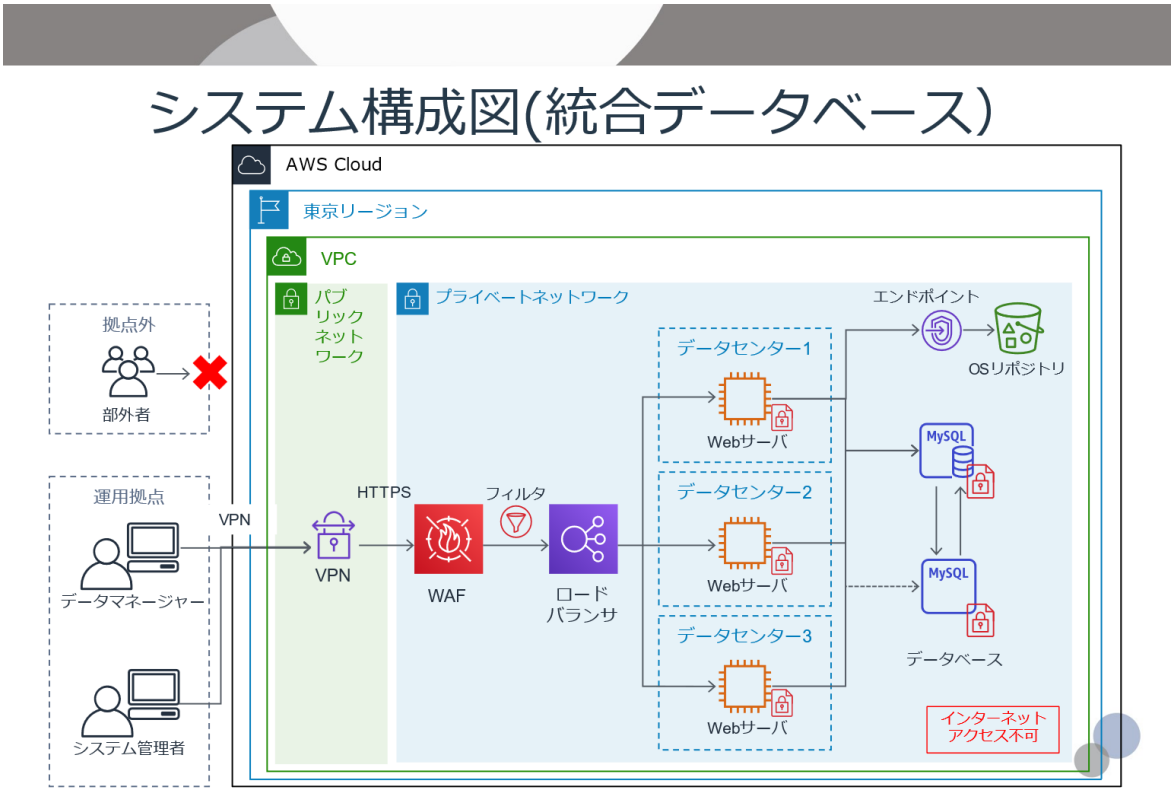
暗号化済みストレージ
ストレージを暗号化し、物理レイヤーでの情報漏洩を防ぐ

Amazon S3
AWSが提供している信頼性の高いデータストレージ

2. ePRO システム

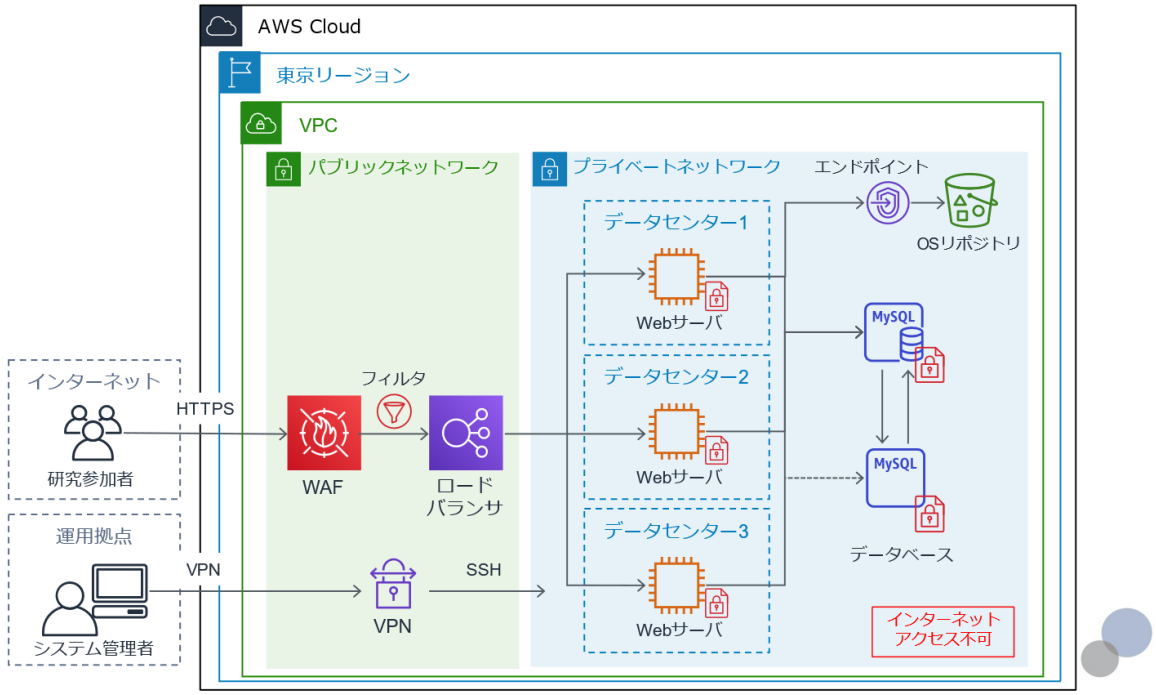


3. 統合データベース



4. 基本情報入力システム

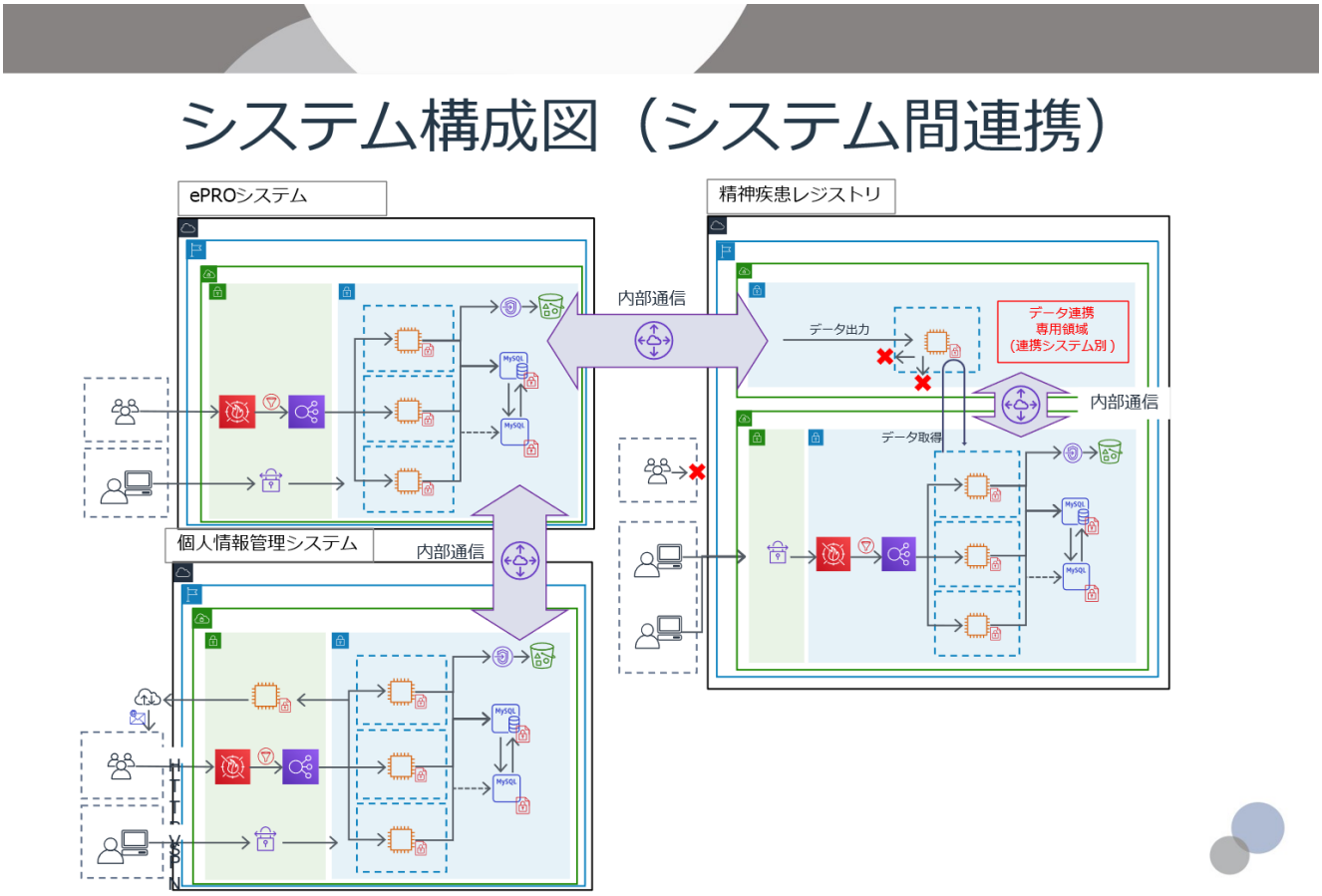
システム構成図（基本情報入力システム）



3.4. システム間連携

1. 個人情報管理システム、ePRO システム、統合データベースの連携

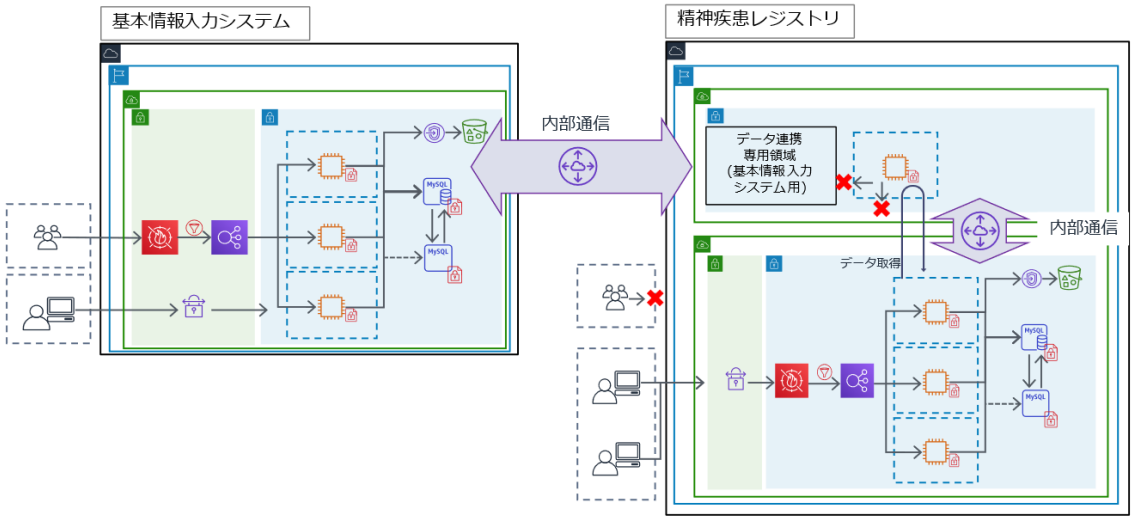
個人情報管理システム、ePRO システム、統合データベースの連携方式は、以下の通り。
各システムは、Peering 接続を用いてインターネットを経由しない内部通信で接続される。
また、ePRO システムから統合データベースへのデータ取り込みの際には、対象のシステム専用のデータ連携専用領域（VPC）を置き、ePRO システムからはデータ連携専用領域のみにアクセス可（レジストリ本体にはアクセス不可）とするとともに、精神疾患レジストリ本体は、各データ連携専用領域のデータ読み込みのみ可能とすることで、外部へのアクセスを遮断する。



2. 基本情報入力システムと統合データベースの連携

基本情報入力システムと統合データベースの連携は、ePRO システムと統合データベースの連携と同様に、対象のシステム専用のデータ連携専用領域（VPC）を置き、ePRO システムからはデータ連携専用領域のみにアクセス可（レジストリ本体にはアクセス不可）とするとともに、精神疾患レジストリ本体は、各データ連携専用領域のデータ読み込みのみ可能とすることで、外部へのアクセスを遮断する。

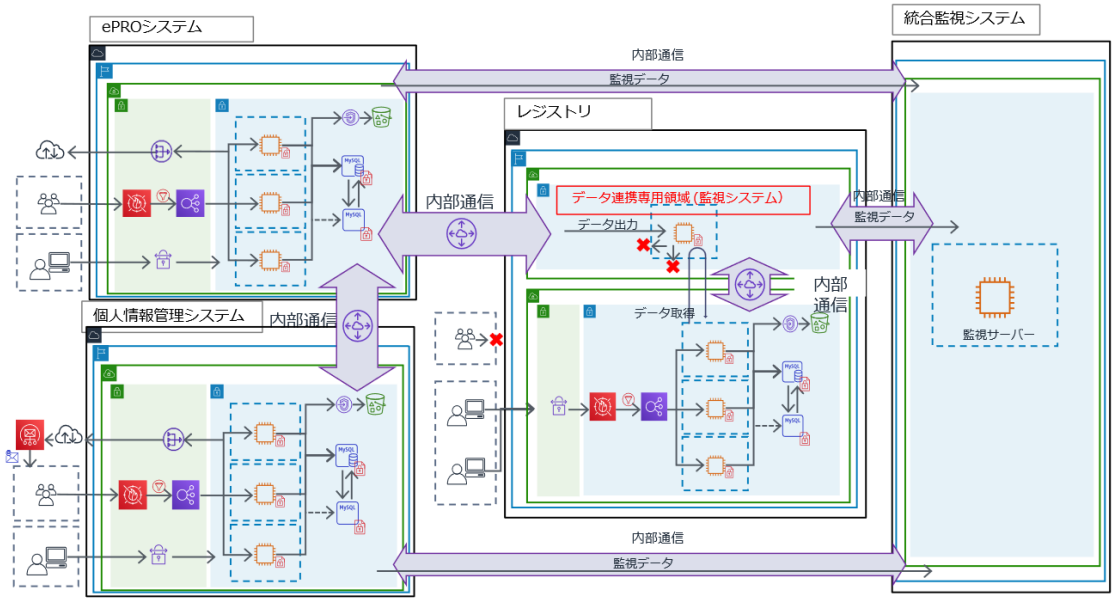
システム構成図（基本情報入力システム連携）



3. 監視システムとの連携

　システムの安定運用のため、各システムはアクセライトが保有している Zabbix を利用した統合監視システムでシステム監視を実施する。
　システム監視の際には、統合監視システムと各システムを内部通信で接続し、監視データの連携のみ可能なネットワーク設定を実施する。監視システムは各システムからのメトリクスデータを収集するのみで、システムへの干渉はできないものとする。
　また、統合データベースの監視の際には、ePRO システムや基本情報入力システムと統合データベースとの連携等同様に監視データ連携用の VPC を経由して監視データを収集するものとし、直接のネットワーク接続を禁止する。

システム構成図（システム間連携全体像）



以上