# APIキー発行および制限管理方針策定ドキュメント

## 1. 概要

本ドキュメントでは、クライアント側でAPIキーを発行し、アクセス制限・利用監視・セキュリティ対策を包括的に管理するための技術的な方針を示します。

## 2. APIキー発行構成

クライアントがAPIプロバイダ（例：OpenAI、Anthropic、Google Cloud等）のダッシュボード上で個別にAPIキーを発行します。

発行されたAPIキーは以下のポリシーに基づき管理されます：

・キーの発行は管理者権限のみ実行可能とする。

・キーごとに用途（開発・検証・本番）を明確化し、タグ付けを行う。

・不要なキーは即時無効化し、失効キーは定期的に削除する。

・APIキーの形式はUUIDv4またはBase64で生成し、16文字以上を推奨。

## 3. アクセス制御およびレート制限

APIアクセスはIPアドレス単位またはJWTトークン単位で制限します。

各APIキーに対して、API Gateway（AWS API Gateway / Cloudflare Workers）上で以下の制限を設定します：

・1分間あたりのリクエスト上限（例：60 req/min）

・日次利用上限（例：10,000 req/day）

・特定エンドポイントごとの利用制限ルール（例：/admin系は管理者のみ）

・レート超過時はHTTP 429 Too Many Requestsを返却し、再試行間隔（Retry-Afterヘッダ）を通知。

## 4. セキュリティ方針

・APIキーは暗号化（AES-256）して保存し、平文ではログに出力しない。

・環境変数（.env）経由でのみアプリケーションに渡す。

・アクセスログをCloudWatchまたはDatadogで集中管理し、異常検知時に通知。

・キーの利用状況を月次で監査し、漏洩検知時は即時ローテーションを実施。

## 5. 運用・管理体制

・APIキーの管理はシステム管理者が担当し、発行・破棄履歴を監査ログに記録。

・アクセス制限ポリシー変更時は必ずPull Requestベースでレビューを実施。

・年1回以上のセキュリティレビューを実施し、方針のアップデートを行う。

## 6. 今後の拡張方針

今後、OAuth 2.0 / JWTベースの動的トークン管理への移行を検討。APIキー管理の自動化（Vault連携）も視野に入れる。