devise-two-factorを4.xから5.xに上げた話

Kazuhiro NISHIYAMA

株式会社*Ruby*開発

大阪*Ruby*会議*04*

2024-08-24

self.introduction

- 西山 和広
- Ruby のコミッター
- github など: @znz
- 株式会社Ruby開発
  www.ruby-dev.jp

devise-two-factor とは?

- devise を TOTP の2要素認証に対応するのに使う gem
- ユーザごとに以下のデータを保存
  - 暗号化された OTP シークレット (認証アプリに登録するもの)
  - 使用済み OTP を区別できる情報
  - OTP が有効かどうか

4.x から 5.x への変更

- 下2個はそのままでいいが OTP シークレットの保存方法が変更
- (再掲載) ユーザーごとに以下のデータを保存
  - 暗号化された OTP シークレット
  - 使用済み OTP を区別できる情報
  - OTP が有効かどうか

4.x から 5.x への変更

- 4 は attr_encrypted gem
  - `encrypted_otp_secret`, `encrypted_otp_secret_iv`, `encrypted_otp_secret_salt` に Base64 でそれぞれ保存
- 5 は Rails 7+ 標準の encrypted attribute
  - 暗号化したものを Base64 して JSON で `otp_secret` 1カラムに保存

更新手順

- 4 から 5 は Rails 6 から Rails 7 と同時に上げる必要あり
  - https://github.com/devise-two-factor/devise-two-factor/blob/main/UPGRADING.md に手順あり
- ほとんど gem は複数の Rails に対応していて独立して更新可能
  - 今回はそうなっていない

なぜか? (推測)

- `attr_encrypted` gem と Rails 7 で `#encrypted_attributes` メソッドが衝突する
- Rails 7 対応の `attr_encrypted` に更新すると二度手間だから一気に移行する手順になっている?

問題点

- 実運用環境なら Rails 7 に上げた後に Rails 6 に戻す可能性もあるのでは?
  - Rails 7 でユーザーの認証アプリと `otp_secret` だけが更新
    → このまま Rails 6 に戻すと `encrypted_*` が古くて認証失敗
  - UPGRADING.md には戻す手順はない
    → 独自対応が必要

具体的には

- UPGRADING.md に `legacy_otp_secret` の実装例
- 公式の手順途中の動作
  - 読み込み
    - 新カラムが設定されていれば → `otp_secret`
    - なければ旧カラムを読む → `legacy_otp_secret`
  - 書き込み は新しい `otp_secret` のみ

独自に書き込み対応

- 新しい `otp_secret` 書き込み時に `legacy_otp_secret` の逆手順で `encrypted_*` に同期
  - → `legacy_otp_secret` でデコードした結果が `otp_secret` と一致するのを確認して自動テストも追加

手動ダウングレードテスト

- 実際に戻してみてテスト → うまく動かないので、さらに調査
  - → `attr_encrypted` が `salt` に prefix として `_` をつける `encode_salt` オプションがデフォルトで `true`
- `Base64.decode64` は `_` を無視するので `legacy_otp_secret` は動く
  - → 同期時に `_` を prepend して解決

まとめ

- 非互換のダウングレード対応は新バージョンでの互換メソッドの自動テストだけでは不十分
- 手動でダウングレード確認も必須
- その他の対応も場合分けして用意
  - 例: ダウングレード中に encrypted_* だけが更新されて otp_secret が古くなる → otp_secret を nil に戻すタスク

宣伝

- 福岡Rubyist会議04 https://regional.rubykaigi.org/fukuoka04/
  - 2024.09.07 Sat. 9:30–18:00
  - 主催: Fukuoka.rb / 株式会社Ruby開発