歯科医院向け初診予約システム 要件定義書

作成日: 2025年04月10日

# 1. システムの目的

本システムは、歯科医院における初診予約の効率化、患者の利便性向上、受付業務の負担軽減を目的とする。

# 2. 利用者と権限

- 患者（予約者）  
- 受付スタッフ  
- 管理者

# 3.現状の課題（As-Is）

# 3.1 現在の予約フロー

- 予約は電話で受け付ける。

- 受付スタッフが初診患者の対応を行い、来院日時の調整をする。

- 受付業務の負担が大きい。

# 4.業務要件（To-Be）

### 4.1 予約フロー

- 予約は即時確定とし、医院側の承認は不要とする。

- 予約方法はWebアプリとする。

- 患者の予約確定時に確認メールを送信する。

- 予約前日にリマインド通知を送信する。

### 4.2 受付フロー

- 受付スタッフは管理画面で予約一覧を見ながら口頭確認を行う。

- 患者の来院をシステムで管理する（来院チェック機能を実装）。

### 4.3 予約の変更・キャンセルについて

### 患者側

- 予約変更・キャンセルは前日まで可能。

- 変更・キャンセル時の医院側への通知は不要。

# 医院側

- 受付スタッフが予約を変更・キャンセルするケースがある。

- 受付スタッフが予約を変更・キャンセルした場合、患者へメール通知を送信する。

# 4. 機能要件

## 4.1 初診予約機能

患者がWeb上で初診予約を行い、即時確定する機能。医院側での承認は不要。

## 4.2 予約変更・キャンセル

患者またはスタッフが予約の変更・キャンセルを行える。

## 4.3 予約一覧・カレンダー表示

受付スタッフが管理画面で予約一覧を確認できる。

## 4.4 来院管理

患者の来院状況を受付スタッフが管理画面で記録できる。

## 4.5 通知機能

患者に対して予約に関する各種通知をメールで送信する。

通知は主に以下の3種類であり、トリガーに応じて自動送信される。

| **通知種別** | **トリガー** | **宛先** | **備考** |
| --- | --- | --- | --- |
| 予約確定通知 | 患者が予約を完了したとき | 患者メールアドレス | 即時送信 |
| 予約リマインド通知 | 予約日前日等の定期バッチ処理 | 患者メールアドレス | 日次バッチで前日分を送信 |
| 予約キャンセル通知 | キャンセル操作が行われたとき | 患者メールアドレス | 手動キャンセルにも対応 |
| 再送通知（手動／自動） | 初回送信に失敗した場合の再送 | 患者メールアドレス | 送信失敗ログをもとに再送 |

- 患者への予約確定時の確認メールを送信。  
- 医院側へのメール通知は不要。

## 4.7 システム設定（診療時間・休診日）

管理者が診療時間や休診日を設定できる。

## 4.8 予約データのエクスポート

管理者または受付スタッフがCSVで予約データを出力できる。

## 4.5 アカウント登録（招待制）

本システムでは、管理者・スタッフアカウントの登録に「事前招待制」を採用する。

管理者が招待リンクを発行し、対象のメールアドレスへ通知することで、該当スタッフはアカウント登録が可能となる。

# 5. 非機能要件

- セキュリティ：2段階認証、操作ログ記録、アクセス制限

## 5.1ログイン管理（二段階認証）

管理者・スタッフのログインにはGoogle Authenticatorによる二段階認証を導入する。

2段階認証はログイン時に毎回要求されるものとする。

ログイン失敗が5回連続した場合、アカウントを30分間ロックする。

(アカウントロック)

・ロックされたユーザーには、登録メールアドレス宛にロック通知メールを送信する。

・ロック解除は以下のいずれかで行う：

- 30分経過後に自動解除

- ロック通知メールに記載された手順に従って、ユーザー自身が解除操作を行う

※ ロック通知メールには解除リンクまたは解除手順を含めることを想定する。

#### 5.2セッション管理

・無操作状態が30分間続いた場合、セッションをタイムアウトとし、自動的にログアウトする。

・ログインから最大12時間が経過した場合も、自動的にログアウトする。

・セッションタイムアウト時はログイン画面に遷移させる。

・セッション延長確認（「延長しますか？」等のダイアログ）は表示しない。

## 5.3操作ログ記録

・管理者および受付スタッフによる操作ログを記録する。

・操作ログはシステム内部用とし、ユーザーインターフェース（UI）での参照機能は提供しない。

・ログはデータベースに記録され、保管期間は1年間とする。

・保管期間を過ぎたログは自動的に削除する。

| **項目** | **要件内容** |
| --- | --- |
| ログ記録対象 | 管理者・受付スタッフによる管理画面上の主要操作（例：アカウント登録、編集、削除、パスワードリセット） |
| ログ記録項目 | ログID/スタッフID／ユーザー権限/操作種別（登録・変更・削除・リセット等）/IPアドレス/操作日時／有効期限 |
| ログ保存方法 | 内部用ログとしてデータベースに記録し、UI上では表示しない（初期運用） |
| ログ保管期間 | 操作ログは1年間保管し、保管期限を過ぎたデータは自動削除する。 |
| ログのセキュリティ | 不正なアクセスを防ぐため、ログテーブルへのアクセス権はシステム管理者に限定する。 |

### 5.4 通知送信ログ機能

通知送信の成否を記録するため、以下の内容を専用テーブルに保存する。  
本ログは障害時の原因調査、再送処理、運用監視の基盤として利用する。

| **項目名** | **説明** |
| --- | --- |
| 通知種別 | 予約確定／リマインド／キャンセル等 |
| 宛先メールアドレス | 通知の送信先 |
| 送信ステータス | success / failure |
| エラー内容 | 失敗時のエラーメッセージ（任意） |
| 送信日時 | 実際に送信を試みた日時 |

### 5.5 パスワードポリシー

・パスワードは以下の条件を満たすものとする：

- 最低8文字以上

- 英大文字・英小文字・数字・記号のうち3種以上を含むこと

・初期パスワードはシステムから自動発行し、初回ログイン時に変更を必須とする。

・一定期間（例：90日）ごとにパスワード変更を促す機能は当初導入しないが、将来的な実装を検討する。

## 5.6 パスワードリセット

本システムでは、ユーザー自身によるリセット（メールリンク式）は実装しない。管理者が手動でパスワードを初期化する方式とする。

## 5.7 アクセス制御

ユーザーごとに権限を制御。受付・管理者のみ管理画面にアクセス可能。

パスワードリセットは管理者のみ可能とし、受付スタッフは操作できない。受付スタッフのリセット対応は管理者が代行する。

- 保守性：内部ログDBでの保管、自動削除処理  
- 拡張性：初期段階ではUIを作らず、将来的に管理画面への表示を検討可能