

サンプル：架空のアプリです。実在のお客様ではありません。

コード・プロダクト監査のレポート

bookings.example.com

<https://bookings.example.com/>

宛先	Example Bookings（架空の会社です。このレポートはすべてサンプルです）
範囲	リポジトリexample-bookings/app（コミット4b7e21c）と https://bookings.example.com 。2026年10月12日～21日に、読み取り権限でレビュー
作成日	2026年10月22日
バージョン	1
ステータス	Aaronによる確認済み

エグゼクティブサマリー

Example Bookingsは、契約を目指している30店舗のチェーンを迎えられる状態にはまだなく、その理由は外からのスキャンでは見えない部分にあります。セキュリティ上の問題は2週間のスプリント1回で解消でき（F-01～F-03）、2回目のスプリントでデータモデルを法人向けプランに合わせます（F-04）。

ログインした顧客なら誰でも、アドレスの数字を変えるだけで、他の顧客の予約を電話番号や来店メモごと開けます（F-01）。10月13日、見つけたその日に創業者にお知らせし、翌日には応急の確認が本番に入りました。また、ある店舗のスタッフが別の店舗の顧客一覧を取得でき（F-02）、予約金の額をサーバーではなくブラウザが決めています（F-03）。セキュリティ以外では、データモデルに複数の店舗を持つ会社という考え方がなく（F-04）、チェーンが求める形では法人向けプランを販売できません。

良い状態にあるもの：無料チェックの緊急の指摘二つは3日以内に解消済みで、カード情報はアプリを一切通らず（F-13）、データベースのスキーマも整っていて、制約とマイグレーションがバージョン管理されています（F-14）。そのため、F-04は作り直しではなく数週間の変更で済み、作り直す理由はありません。

下記のお見積りにある2週間の本番化スプリントで、F-01～F-03とF-05～F-10に対応することをおすすめします。チェーンのセキュリティ審査で指摘されそうな点は、これですべて解消できます。F-04は、法人向けプランを販売できるかどうかを左右するため、より小さなセキュリティ上の指摘より上の4番目に置きました。同じ価格の2回目のスプリントで対応します。

重要度別の指摘事項

重大	高	中	低	情報	合計
1	3	5	3	2	14

事業の目標

2026年10月12日の創業者へのヒアリングから：

- 2027年3月までに、最初の複数店舗のお客様として、30店舗のフィットネスチェーンと法人向けプランで契約する。

- 契約の前に、そのチェーンのセキュリティチェックシートとデータ保護の審査を通過する。
- 予約金を確実に受け取れるようにし、無断キャンセルを減らす。
- 2027年前半にシードラウンドの資金調達を行う。すでに2社の投資家から、アプリをどのようにレビューしたかを聞かれている。

これらの目標にとって最も重要なのは、予約金付きの予約、店舗スタッフのカレンダー、返金の三つの流れです。

レビューの前提となった制約：店舗の中には理学療法のクリニックもあるため、アプリが保存する来店メモに健康に関する情報が含まれることがあります。

範囲と方法

リポジトリ（コミット4b7e21c）と公開中のアプリを、2026年10月12日から21日まで、Anyfrontの専用アカウントへの読み取り権限でレビューしました。

- 2026年10月12日の創業者へのヒアリングと、1店舗のマネージャーとのスタッフ画面の確認。
- 公開部分のスキャン（エンジン1.2.0）を10月12日に再実行し、各指摘を手作業で確認。
- 監査の手順に沿った、ログインとセッション、データへのアクセス、予約金と返金、データモデル、エラー処理、ログ、バックアップ、デプロイのレビュー。
- だれが何を見られるかを確かめるため、ステージング環境にテスト用の顧客2名と店舗2つを作成。
- 依存関係の監査と、リポジトリの履歴に対するシークレットのスキャン。
- こちらで用意したスクリプトを使い、創業者に実行していただいたデータベースのクエリ（設定と件数のみで、行の中身は見えていません）。

行っていないこと：ペネトレーションテスト、負荷テスト、本番データや本番環境のシークレットへのアクセス。

無料チェックと監査の違い

10月6日の無料チェックでは、bookings.example.comがインターネット上の誰にでも見せている部分を確認しました。緊急の指摘だった、JavaScriptに含まれた本番用のStripeシークレットキーと公開されたソースマップは10月9日までに解消され、この監査でも確認しまし

た。比較的小さな指摘のうち五つはまだ残っており、F-07、F-10、F-11に引き継いでいます。

監査では表面の奥、つまりコード、データベース、ホスティング、そして創業者の計画を見て、スキャンでは見つけられないことを確認しました。

- ログインしたユーザーが、他のユーザーのデータに届いてしまわないか（F-01、F-02）。スキャンに見えるのはログイン画面までで、2人の顧客としてログインし、見えるものを比べることはできません。
- サーバーが、ブラウザから送られてくる値をそのまま信用していないか（F-03）。
- データモデルが、事業の向かう先に合っているか。コードだけでなく、創業者の計画を聞いて初めてわかります（F-04）。
- 問題が起きた日に立て直せるか。バックアップ、アラート、テストです（F-05、F-06、F-08）。

指摘事項（ビジネスへの影響が大きい順）

ビジネスにとって重要な順に並べています。各項目の詳細は次の章に記載しています。

#	ID	指摘事項	重要度	対応の目安
1	F-01	ログインした顧客なら誰でも、どの予約でも開ける セキュリティリスク	重大	数日
2	F-02	店舗のスタッフが、別の店舗の顧客一覧を取得できる セキュリティリスク	高	数日
3	F-03	予約金の額を、ブラウザが決めている 売上	高	数時間
4	F-04	データモデルに、複数の店舗を持つ会社を表す場所がない 資金調達・法人営業	高	数週間
5	F-05	バックアップを復元したことがなく、戻せるのは前日の夜まで 売上	中	数時間
6	F-06	予約金の支払いの失敗やサーバーのエラーが、誰にも届かない 売上	中	数時間
7	F-07	顧客の連絡先と来店メモが、ログに書き込まれている セキュリティリスク	中	数時間
8	F-08	予約と予約金に自動テストがなく、デプロイがCIを通らない 改修コスト	中	数日
9	F-09	セッションが1年間続き、パスワードを変えても終わらない セキュリティリスク	中	数時間
10	F-10	無料チェックのヘッダーとエラーページの指摘が、三つ残っている 資金調達・法人営業	低	数時間
11	F-11	予約ページが、表示しないスタッフ画面まで読み込んでいる 売上	低	数日
12	F-12	依存パッケージの二つに、公開済みのセキュリティ勧告がある 資金調達・法人営業	低	数時間
13	F-13	カード情報がアプリを一切通らない 資金調達・法人営業	情報	数時間
14	F-14	データベースのスキーマは、良い土台になっている 改修コスト	情報	数時間

指摘事項の詳細

重大

F-01 ログインした顧客なら誰でも、どの予約でも開ける

ビジネスへの影響・セキュリティリスク

顧客アカウントを持つ人なら誰でも、アドレスの数字を変えるだけで、他の顧客の氏名、電話番号、来店メモを読めてしまい、チェーンのセキュリティ審査はこの時点で終わってしまいます。

推奨する対応

予約は必ずログイン中のアカウントを通して読み込み、それ以外には404を返します。予約に関する23のルートそれぞれに、別の顧客には何も返らないことを確かめるテストを加えます。予約を1件表示するルートには、10月14日に応急の確認が入っています。

対応の目安

数日

根拠

- `server/routes/bookings.js:41: Booking.findById(req.params.id)` で、予約の所有者を確認していない
- ステージング環境: テスト用の顧客2名で確認。顧客Bが顧客Aの予約を開けた。200で、記録がすべて返った
- `public.bookings`: IDは連番で、発行済みは約18,400件。どの予約も推測1回で届く

高

F-02 店舗のスタッフが、別の店舗の顧客一覧を取得できる

ビジネスへの影響・セキュリティリスク

ある店舗のスタッフアカウントから、他のすべての店舗の顧客一覧をダウンロードできてしまい、予約システムとしてどの店舗にも、どのチェーンにも受け入れられません。

推奨する対応

店舗はリクエストからではなく、ログイン中のスタッフのメンバーシップから必ず取り、スタッフ向けのすべてのクエリを1か所でその店舗に絞り込みます。別の店舗のスタッフには何も返らないことを確かめるテストを加えます。

対応の目安

数日

根拠

- `server/routes/staff/customers.js:18: studio_id`をクエリ文字列から読んでいる
- ステージング環境: テスト用の店舗2つで確認。2つ目の店舗のスタッフが、`studio_id`を書き換えるだけで1つ目の店舗の顧客一覧を取得できた

高

F-03 予約金の額を、ブラウザが決めている

ビジネスへの影響・売上

顧客はどの予約でも1円の予約金で済ませられるため、無断キャンセルを防ぐための予約金を、いつでも回避できてしまいます。

推奨する対応

予約金は店舗の設定からサーバーで計算し、その金額でのみ支払いを作成します。金額を書き換えた支払いが拒否されることを確かめるテストを加えます。

対応の目安

数時間

根拠

- `server/routes/payments.js:27`: 支払いを `amount: req.body.amount` で作成している
- `src/pages/Book.tsx:212`: 予約金をブラウザで計算し、予約とあわせて送信している

高

F-04 データモデルに、複数の店舗を持つ会社を表す場所がない

ビジネスへの影響・資金調達・法人営業

30店舗のチェーンは、スタッフも集計も請求も共有できない30個の別々のアカウントが必要になり、事業が次に売り出そうとしている法人向けプランの妨げになります。

推奨する対応

店舗の上に組織を置き、各人に組織内の一つ以上の店舗でのロールを与えるメンバーシップを加えます。既存の店舗はそれぞれ専用の組織に移し、クエリを組織で絞り込みます。作業は2週間ほどで、スプリントでアクセスのテストがそろってから行うのが最善です。

対応の目安

数週間

根拠

- `db/migrations/0003_users.sql`: `users.studio_id`: 各人はちょうど一つの店舗にだけ所属する
- `db/migrations/0007_billing.sql`: 契約が店舗ごとのため、チェーンには30通の請求書が届く
- `server/lib/auth.js:12`: セッションが持つ店舗は一つで、切り替える方法がない

中

F-05 バックアップを復元したことがなく、戻せるのは前日の夜まで

ビジネスへの影響・売上

マイグレーションの失敗や誤った削除があれば、最大で1日分の予約と予約金が失われ、残りを取り戻すのにどれだけかかるかも、まだ誰にもわかりません。

推奨する対応

データベースのポイントインタイムリカバリーを有効にし、月に1回、前夜のバックアップを作業用のデータベースに復元して、手順とかった時間を記録します。

対応の目安

数時間

根拠

- データベースのホスティング設定: 創業者のスクリーンショットより：毎日のスナップショットを7日間保存。ポイントインタイムリカバリーは無効
- docs/: 復元の手順書がなく、復元した記録もない

中

F-06 予約金の支払いの失敗やサーバーのエラーが、誰にも届かない

ビジネスへの影響・売上

予約金の支払いが失敗したり予約ページが動かなくなったりしても、店舗はアラートではなく顧客から、それも一番忙しい時間帯に知ることになります。

推奨する対応

サーバーとアプリにエラーラッキングを入れ、支払いの失敗、サーバーのエラー、止まったジョブキューを創業者のスマートフォンに通知します。

対応の目安

数時間

根拠

- server/index.js: エラーはコンソールに出力するだけで、ホスティングのログの保存期間は3日間
- Stripeのダッシュボード: 創業者によるエクスポートより：9月の予約金の支払いの失敗は41件で、どれもフォローされていない

中

F-07 顧客の連絡先と来店メモが、ログに書き込まれている

ビジネスへの影響・セキュリティリスク

健康に関する内容を含むこともある氏名、電話番号、来店メモが、データベースより多くの人やサービスが読めるログにコピーされており、チェーンのデータ保護の審査で必ず聞かれます。

推奨する対応

リクエストの本文ではなく予約のIDを記録し、予約確認ページのアドレスからメールアドレスを外し（無料チェックの指摘）、変更が本番に入ったら既存のログを削除します。

対応の目安

数時間

根拠

- `server/middleware/log.js:9`: すべてのリクエストの本文を、そのままログに記録している
- `/booking/confirmed`: 10月6日の無料チェックの指摘どおり、顧客のメールアドレスがまだアドレスに含まれている

中

F-08 予約と予約金に自動テストがなく、デプロイがCIを通らない

ビジネスへの影響・改修コスト

予約や支払いに関わる変更はすべて手作業で確認しているため変更に時間がかかり、このレポートの修正が元に戻ってしまっても、それを止めるものではありません。

推奨する対応

すべてのプルリクエストで実行され、失敗したらデプロイを止めるCIを用意し、予約、予約金、返金、そしてF-01とF-02のアクセスのルールをテストします。

対応の目安

数日

根拠

- `tests/`: ユニットテストは4件で、すべて日付の書式に関するもの
- ホスティングの設定: `main`へのプッシュのたびにデプロイされ、必須のチェックがない

中

F-09 セッションが1年間続き、パスワードを変えても終わらない

ビジネスへの影響・セキュリティリスク

なくしたスマートフォンや、辞めたスタッフのノートパソコンから、店舗のカレンダーと顧客情報に最長1年間、すべてアクセスできてしまいます。

推奨する対応

セッションは使っている間だけ延長する30日間とし、パスワードの変更時とスタッフの削除時にすべてのセッションを終了します。店舗のオーナーが、スタッフをすべての端末からログアウトさせられるようにします。

対応の目安

数時間

根拠

- `server/lib/auth.js:31`: CookieのmaxAgeが365日で、セッションを途中で終わらせる方法がない

低

F-10 無料チェックのヘッダーとエラーページの指摘が、三つ残っている

ビジネスへの影響・資金調達・法人営業

一つひとつは小さなものですが、チェーンのチェックシートや投資家側のレビュー担当者が最初に確認する項目に入っています。

推奨する対応

10月6日の無料チェックのレポートのとおり、Strict-Transport-Securityを追加し、本番環境ではデバッグ用のエラーページを無効にし、X-Powered-Byヘッダーを削除します。

対応の目安

数時間

根拠

- `https://bookings.example.com/`: Strict-Transport-Securityヘッダーがなく、X-Powered-By: Express。10月12日に再確認
- `server/index.js:58`: 環境にかかわらず、エラーハンドラーがスタックトレースを返している

低

F-11 予約ページが、表示しないスタッフ画面まで読み込んでいる

ビジネスへの影響・売上

スマートフォンの顧客は予約ページが出るまで数秒待つことになり、店舗が広告で集めたお客様の予約を逃します。

推奨する対応

スタッフ画面とカレンダーのライブラリは、それを使うルートでだけ読み込み、予約ページには表示するものだけを送ります。

対応の目安

数日

根拠

- `/`: スクリプト5本、展開後1,992,431バイト。無料チェックのとおり
- `src/main.tsx:7`: スタッフ画面のルートを最初からまとめて読み込んでおり、バンドルの大半を占めている

低

F-12 依存パッケージの二つに、公開済みのセキュリティ勧告がある

ビジネスへの影響・資金調達・法人営業

どちらもレビューしたコードからは使われていませんが、チェーンの依存関係のスキャンには表示されるため、説明が必要になります。

推奨する対応

両方を更新し、依存関係の自動更新を有効にして、新しい勧告がプルリクエストとして届くようにします。

対応の目安

数時間

根拠

- `package-lock.json`: 重要度が高い勧告が2件。どちらも間接的な依存で、レビューしたコードの経路にはない

情報

F-13 カード情報がアプリを一切通らない

ビジネスへの影響・資金調達・法人営業

カード情報はすべてStripeの決済画面が受け取るため、カードのセキュリティ基準の多くがアプリの対象外になり、チェーンからの決済に関する質問も少なく済みます。

推奨する対応

この形を保ちます。F-03の修正と同じく、予約金と返金はStripeのサーバー側のAPIだけで扱います。

対応の目安

数時間

根拠

- `src/pages/Book.tsx`: Stripeの決済画面へのリダイレクト。アプリにカードの入力欄はない

情報

F-14 データベースのスキーマは、良い土台になっている

ビジネスへの影響・改修コスト

制約、外部キー、バージョン管理されたマイグレーションがそろっているため、F-04の変更は作り直しではなく数週間で済みます。

推奨する対応

今と同じく、スキーマの変更はすべてレビューを経たマイグレーションで行い、F-04の組織のテーブルも同じ方法で追加します。

対応の目安

数時間

根拠

- `db/migrations/`: マイグレーションは14本で、どの環境でも順に適用されている

改善計画

今すぐ（創業者が今週中に）：

- 応急の確認はそのまま残し、7月以降のアクセスログで、所有者以外が予約を開いた記録がないか調べてください。記録があれば、顧客へのお知らせについて専門家にご相談ください。
- データベースのポイントインタイムリカバリーを有効にしてください（F-05）。

対応の目安 F-05・数時間

スプリント（2週間）：

- F-01、F-02、F-03：データへのアクセスと予約金。それぞれテストとあわせて対応します。

対応の目安 F-01・数日 F-02・数日 F-03・数時間

- F-08：すべてのプルリクエストでCIを実行し、以後の変更をテストで守ります。

対応の目安 F-08・数日

- F-05、F-06、F-07、F-09、F-10：バックアップ、アラート、ログ、セッション、無料チェックの残り。

対応の目安 F-05・数時間 F-06・数時間 F-07・数時間 F-09・数時間 F-10・数時間

次に（2回目のスプリント、その後は月額契約で）：

- F-04：組織、メンバーシップ、ロール。同じ価格の2回目のスプリントで対応します。

対応の目安 F-04・数週間

- F-11とF-12は、チェーンの導入作業とあわせて開発支援契約で対応します。

対応の目安 F-11・数日 F-12・数時間

継続して確認すること：

- ホスティングやヘッダーが変わるリリースの後と、チェーンの審査の前に、無料チェックを再実行します。
- 毎月バックアップを復元し、その記録をチェーンのチェックシートのために残します。

おすすめしないこと：作り直しや、別のプラットフォームへの移行。どの指摘も、今の環境のまま解消できます。

スプリントのお見積り

サンプルです。事業、範囲、日程は架空で、価格と条件は公開しているとおりです。

- 範囲（重要な順）：F-01、F-02、F-03（予約と顧客一覧は所有者にだけ応答し、予約金はサーバーで計算。それぞれテストつき）、F-08（失敗したらデプロイを止めるCI）、F-05、F-06、F-07、F-09、F-10（復元の記録、アラート、ログからの個人データの除去、30日間のセッション、無料チェックの残り三つ）。
- 価格：¥1,200,000（税抜、固定）。消費税は、該当する場合に別途申し受けます。
- 条件：2026年11月4日から2週間、Example Bookingsがマージするプルリクエストでお届けします（標準のアクセス方式）。ご予約時と納品時に50%ずつ、請求書の発行から7日以内にお支払いください。報告会から30日以内の11月22日までのご予約で、監査料金（¥490,000）を充当します。
- 範囲に含まれないもの：F-04は同じ固定価格（¥1,200,000）の2回目のスプリントで、F-11、F-12とチェーンの導入作業は開発支援契約（月額¥550,000（税抜）、月20時間まで）で対応します。

制約事項

本レポートは、上記の範囲について、その時点で行った専門的なレビューです。セキュリティの保証、ペネトレーションテスト、第三者認証ではありません。コミット4b7e21cのコードと、2026年10月21日時点のアプリを対象としており、それ以降の変更は含みません。Example Bookingsからご提供いただいた情報とクエリの結果にもとづいています。自動ツールでも手作業のレビューでも見落としはありうるため、指摘がないことは、問題がないことを意味しません。実際の支払いは行っていないです。

評価していない項目

- パフォーマンス: 負荷テストは、今回の監査の範囲外でした。

記載した範囲と時点について行う、専門的なレビューです。ペネトレーションテストや第三者認証ではなく、アプリに脆弱性がないことを保証するものでもありません。