

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。

無料チェックのレポート

bookings.example.com

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

作成日 2026年10月6日

バージョン 2

ステータス Aaronによる確認済み

概要

今週中に直していただきたいことが二つあります。すべての訪問者がダウンロードするJavaScriptに含まれた本番用のStripeシークレットキーと、アプリの元のソースコードを公開してしまっているソースマップです。残りは通常のスプリントで対応できます。自動検出の項目のうち一つは、確認の結果、削除しました。バンドル内のGoogle Maps用のキーは、このドメインからの利用に正しく制限されています。

重要度別の指摘事項

重大	高	中	低	情報	合計
1	1	3	2	0	7

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。

#	指摘事項	重要度	対応の目安
1	配信されるJavaScriptに、本番用のStripeシークレットキーが含まれている セキュリティリスク	重大	数時間
2	JavaScriptのソースマップが公開されている セキュリティリスク	高	数時間
3	予約確認ページのURLに、お客様のメールアドレスが含まれている セキュリティリスク	中	数時間
4	エラーページにスタックトレースが表示される セキュリティリスク	中	数時間
5	Strict-Transport-Securityヘッダーがない 資金調達・法人営業	中	数時間
6	最初の画面の前に1.9 MBのJavaScriptを読み込んでいる 売上	低	数日
7	X-Powered-Byヘッダーでフレームワークがわかる 資金調達・法人営業	低	数時間

指摘事項の詳細

重大

配信されるJavaScriptに、本番用のStripeシークレットキーが含まれている

ビジネスへの影響・セキュリティリスク

予約ページを開いた人なら誰でも、このキーを使って返金や請求を行ったり、お客様の支払いの記録を閲覧したりできます。

推奨する対応

本日中にStripeのダッシュボードでキーを再発行し、予約金と返金の処理をサーバー側のコードに移して、キーがブラウザに届かないようにしてください。

対応の目安

数時間

根拠

- `/assets/index-3e7a19c0.js: sk_live_...FAKE` (107文字)

高

JavaScriptのソースマップが公開されている

ビジネスへの影響・セキュリティリスク

スタッフ用の画面や予約金の計算を含む、アプリの元のソースコードを誰でもダウンロードして読めるため、模倣も攻撃もしやすくなります。

推奨する対応

本番のビルドでソースマップを無効にするか (Viteなら `build.sourcemap: false`)、エラー監視ツールにだけアップロードし、再デプロイしてください。

対応の目安

数時間

根拠

- `/assets/index-3e7a19c0.js.map`: 配信あり: 200、application/json、3,412,880バイト。ソースマップの形式

中

予約確認ページのURLに、お客様のメールアドレスが含まれている

ビジネスへの影響・セキュリティリスク

予約の確認ページでは、ページのアドレスにお客様のメールアドレスが入るため、アクセス解析ツールや、ページのリンク先のサイトに記録されることがあります。

推奨する対応

確認ページのURLには予約IDだけを使い、メールアドレスはサーバー側で参照してください。あわせて Referrer-Policy: strict-origin-when-cross-origin を送ってください。

対応の目安

数時間

根拠

- /assets/index-3e7a19c0.js: 確認ページへの遷移で /booking/confirmed?email=... を組み立てている

中

エラーページにスタックトレースが表示される

ビジネスへの影響・セキュリティリスク

存在しないアドレスを開くと、ファイルのパス、ライブラリのバージョン、内部の構成が見えるため、アプリを探ろうとする人の手間を省いてしまいます。

推奨する対応

本番環境ではデバッグ用のエラーページを無効にし、詳細はサーバー側のログに残してください。

対応の目安

数時間

根拠

- /.git/HEAD: 配信なし。ただし、500のエラーページにファイルのパスを含むスタックトレースがある

中

Strict-Transport-Securityヘッダーがない

ビジネスへの影響・資金調達・法人営業

法人のお客様のセキュリティチェックシートではHSTSの有無を聞かれることが多く、ベンダー審査で失点しやすい項目です。また、httpでの最初のアクセスは盗聴や改ざんを受けるおそれがあります。

推奨する対応

ホスティングのヘッダー設定に Strict-Transport-Security: max-age=31536000; includeSubDomains を追加してください。

対応の目安

数時間

根拠

- <https://bookings.example.com/>: トップページのレスポンスにヘッダーがない

低

最初の画面の前に1.9 MBのJavaScriptを読み込んでいる

ビジネスへの影響・売上

一般的なスマートフォンでは予約ページの表示に数秒かかり、広告から来た方の予約を逃す原因になります。

推奨する対応

スタッフ用の画面とカレンダーのライブラリを遅延読み込みのルートに分け、予約ページでは描画に必要なものだけを配信してください。

対応の目安

数日

根拠

- [/](#): スクリプト5件、デコード後1,992,431バイト

低

X-Powered-Byヘッダーでフレームワークがわかる

ビジネスへの影響・資金調達・法人営業

このヘッダーから、アプリを動かしているフレームワークがわかるため、既知の弱点を探す手間が減ります。

推奨する対応

X-Powered-Byヘッダーを削除してください（Expressなら `app.disable('x-powered-by')`）。

対応の目安

数時間

根拠

- <https://bookings.example.com/>: X-Powered-By: Express

評価していない項目

- **データアクセス:** データベースのアクセスルールの確認は、まだ無料チェックの対象外です

次のステップ

この無料チェックで確認したのは、公開中のアプリがインターネットに公開している部分だけです。有料の監査では、コードそのものと、その背景にあるプロダクトやビジネスの目標をあわせてレビューし、重要な点を直すための固定価格のプランをご提案します。

監査について相談する: <https://anyfront.co/ja/book>

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はありません。