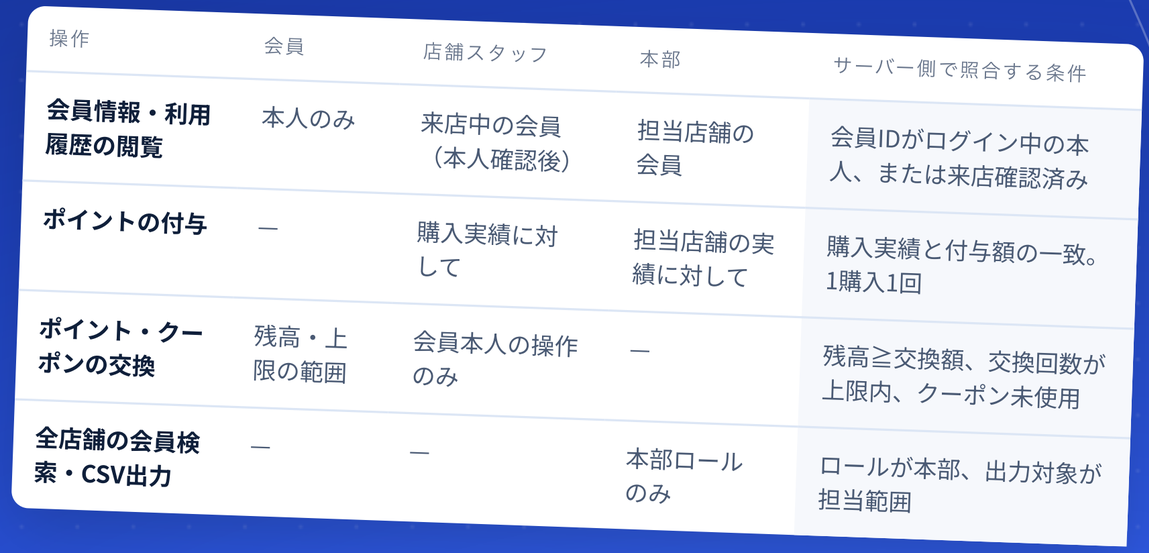
03 全8ページ

小売・店舗サービス向け

会員情報・ポイントの不正操作を防ぐ

設計の考え方

照合の場所・権限の書き方・直した後の確認を
1冊にまとめる



操作	会員	店舗スタッフ	本部	サーバー側で照合する条件
会員情報・利用履歴の閲覧	本人のみ	来店中の会員（本人確認後）	担当店舗の会員	会員IDがログイン中の本人、または来店確認済み
ポイントの付与	—	購入実績に対して	担当店舗の実績に対して	購入実績と付与額の一致。1購入1回
ポイント・クーポンの交換	残高・上限の範囲	会員本人の操作のみ	—	残高≧交換額、交換回数が上限内、クーポン未使用
全店舗の会員検索・CSV出力	—	—	本部ロールのみ	ロールが本部、出力対象が担当範囲

Securiy セキュリー

WHEN YOU NEED IT

機能追加のたびに、権限確認のない経路が増える

見つけて直すだけでは、次の機能追加で同じ穴が開きます。この冊子は、不正操作が成立しない設計の考え方と、確認の仕方をまとめたものです。

PULL REQUEST ／ 機能追加のレビュー（想定）　app/members.py

```
1    @app.get('/members/{member_id}/history')
2  + def handler(req):
3  +     m = Member.get(member_id)
4  +     return m.history            # ← ログイン中の会員と照合していない
5  +     return ok()
```

レビュー　権限の確認がありません。会員は自分の情報・履歴、店舗スタッフは担当店舗の範囲だけを扱える、という条件をサーバー側のどこで照合しますか？

設計を見直す場面

会員アプリ・ポイント機能の改修

会員IDの照合が API に1つ抜けると、他会員の情報に届く

店舗端末・本部機能の追加

1店舗のアカウントから全店舗の情報に届く経路ができやすい

AI接客・チャットの導入

画面と同じ権限確認が、AIの回答にも適用されているかを確かめる必要がある

PERMISSION TABLE

権限は「誰が・何を・どの条件で」の表にする

会員／店舗スタッフ／本部について、操作ごとの許可条件と、サーバー側で照合する条件を1枚にします。「—」のマスが実際に拒否されるかが、検証の対象です。

操作	会員	店舗スタッフ	本部	サーバー側で照合する条件
会員情報・利用履歴の閲覧	本人のみ	来店中の会員（本人確認後）	担当店舗の会員	会員IDがログイン中の本人、または来店確認済み
ポイントの付与	—	購入実績に対して	担当店舗の実績に対して	購入実績と付与額の一致。1購入1回
ポイント・クーポンの交換	残高・上限の範囲	会員本人の操作のみ	—	残高≧交換額、交換回数が上限内、クーポン未使用
全店舗の会員検索・CSV出力	—	—	本部ロールのみ	ロールが本部、出力対象が担当範囲

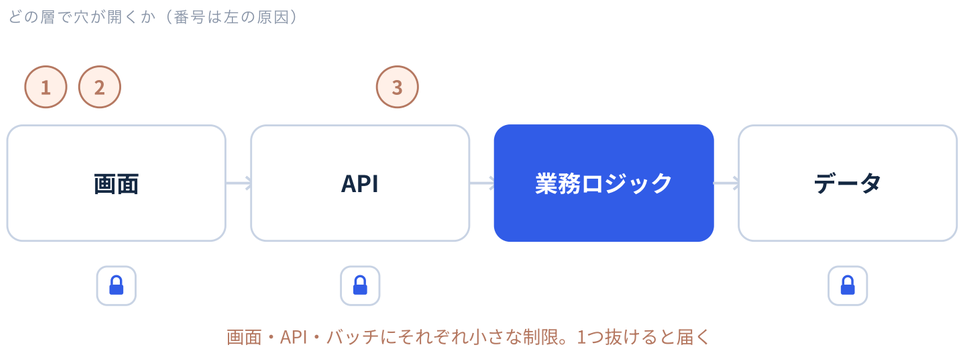
使い方　新しい機能を足すときは、先にこの表に行を足す。右列が書けない操作は、照合の場所が決まっていない。

WHERE TO CHECK

照合はサーバー側の1カ所に置く

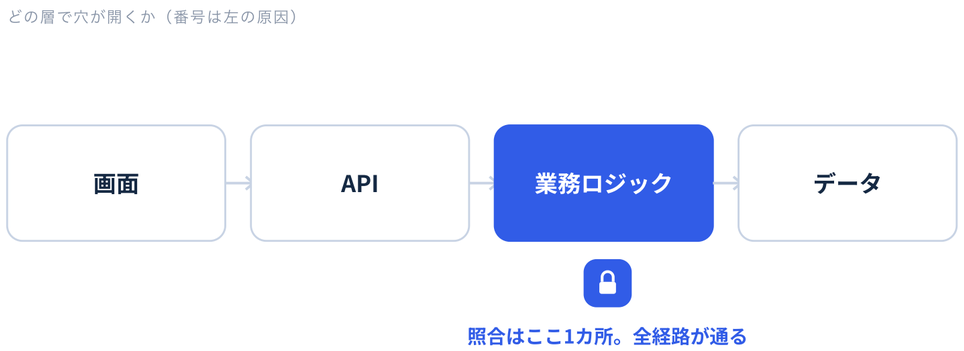
画面・API・バッチ・AI と経路が増えても、照合の場所を増やさない。データ取得・更新の共通層に1カ所置き、どの経路もそこを通す。

Before ／ 経路ごとに散らばる



会員IDがURLやQRに載り、差し替えが効く

After ／ 共通層に1カ所



会員IDはログイン中の本人とサーバー側で照合してから使い、URLの値は使わない。共有URLは推測不能・有効期限付きにする。

DESIGN PRINCIPLES

不正操作が成立しない設計の3原則

直す場所を増やすより、照合の場所を1カ所にまとめる方が、機能追加に強くなります。

1

会員IDは本人のセッションと照合する

URL やリクエストの会員IDを信用せず、ログイン中の本人とサーバー側で突き合わせます。

2

ポイントは実績と上限で二重に確認する

交換・付与の要求は、購入実績・残高・上限をサーバー側で再確認してから通します（P.03）。

3

店舗の権限は店舗単位で切る

店舗端末・スタッフの操作は担当店舗に限定し、本部機能は別の権限にします（P.07）。

DESIGN REVIEW

設計レビューの10問（機能追加のたびに）

「いいえ」「不明」が1つでもあれば、その操作が検証の候補です。共同検証の初回2操作もここから選べます。

01	テナント・店舗・会員のIDは、リクエストの値ではなく、ログイン中の所属と照合してから使っているか	☐ はい ☐ いいえ ☐ 不明	
02	照合はデータ取得・更新の共通層に1カ所あるか。画面側の制限だけに頼っていないか	☐ はい ☐ いいえ ☐ 不明	
03	一覧・検索・CSV出力・帳票など、後から足した経路も同じ共通層を通るか	☐ はい ☐ いいえ ☐ 不明	
04	金額・数量・ポイントは、画面から来た値ではなく、サーバー側の実績（注文額・残高）と照合しているか	☐ はい ☐ いいえ ☐ 不明	
05	累計（返金累計・付与累計）で上限を判定しているか。1回ごとの判定だけになっていないか	☐ はい ☐ いいえ ☐ 不明	
06	並行リクエストで残高・回数の確認が競合しないか（条件つき更新・ロック）	☐ はい ☐ いいえ ☐ 不明	
07	確定後（出荷後・確定後）の変更は、状態を検査し、承認付きの経路に限定しているか	☐ はい ☐ いいえ ☐ 不明	
08	運営者・本部の機能は別ロール・別経路か。URLを知っているだけで到達しないか	☐ はい ☐ いいえ ☐ 不明	
09	共有URL・招待リンク・クーポンコードは推測不能で、失効・1回限りの制約があるか	☐ はい ☐ いいえ ☐ 不明	
10	AI チャット・外部 API からの要求にも、画面と同じ照合が適用されているか	☐ はい ☐ いいえ ☐ 不明	

RETEST

直した後に、通常操作が通ることを同じ表で確かめる

修正で不正操作が拒否されるようになったことと、通常の操作がそのまま通ることを、経路×シーンの同じ表で確認してからリリースします。



拒否されること

他会員の情報は拒否。別の手順・モデルでも同じ結果

通常操作が通ること

通常のポイント利用は継続。正規の担当者の操作が止まらない

未確認

初回に入れなかったシーンと経路は、理由と次回の予定を記録

記載の検証シーンは共同検証のテーマ例で、業界別の導入実績・認証取得を示すものではありません。対象は、検証と修正を行える自社アプリ・独自APIです。

権限表と照合の場所を、共同検証で一緒に決める。

初回スコープ（1アプリ・2操作・10営業日）で、権限表の「—」のマスが実際に拒否されるかを試し、修正案・再検証チェック・再実行用テストをお渡しします。本番の認証情報や実データは不要です。

Securiy は Tempura technologies株式会社のセキュリティ事業です。

FREE CONSULTATION

30分無料相談を予約する

権限表の下書きをお持ちいただければ、どの操作から検証するかを一緒に決めます。

予約ページへ →

SET

01 検証シーン集 ／ 02 プログラムのご案内

小売・店舗サービスの3シーンは 01、対象・期間・費用・体制は 02 へ。