Securiy セキュリー

01 小売・店舗サービス・全13ページ

業種別 検証シーン集

小売・店舗向け検証シーン集

会員情報の分離・ポイント・クーポンの不正操作・
店舗権限の奪取・AI接客からの流出を検証する

USE CASES ／ FOR RETAIL & STORE SERVICES

FOR RETAIL & STORE SERVICES

攻撃者が AI で自動化する「権限の抜け探し」を、先に試して直す。

攻撃者は AI を使い、公開 API・画面の通信・JavaScript から操作を洗い出し、ID やロールを組み合わせて自動で試します。狙われるのは、スキャナーが拾いにくい「権限の抜け」です。 この冊子は、小売・店舗サービスの3シーン（会員情報の分離・ポイント・クーポンの不正操作・店舗権限の奪取・AI接客からの流出）について、原因・自社での確かめ方・修正の方向まで掘り下げたものです。

「AIを使った攻撃」で想定する2つ

1

攻撃者が AI で自動化する、権限の抜け探し

他社・他人のデータに届く経路、承認を迂回する経路、上限を超える経路を、AI が組み合わせで試す。

2

貴社の AI 機能への誘導と乗っ取り

チャット・エージェント・RAG に仕込んだ指示で、本人の権限を超えた回答や操作をさせる。

こんな兆候があれば、対象です

「対策はしている」と言えるが、会員IDの推測やAPIの直接呼び出しを試した記録がない

他の会員の氏名・連絡先・利用履歴に届かないかを、実際に試して確かめていない。

ポイント・クーポンの不正取得を、画面の制限だけで防いでいる

APIを直接叩いた場合に、付与・利用・交換の条件がサーバー側で確認されているかを確かめていない。

店舗スタッフ・委託先の権限が、店舗を跨いで広がっている

1店舗の端末やアカウントから、全店舗の会員情報や売上に届かないかを確認していない。

対象: 会員アプリ・ポイント・予約システムを自社運用する小売・店舗チェーンの経営者・情報システム・開発責任者の方へ（開発を受託するベンダーの方も）

MAP

3シーンの RULE を、貴社の条件に置き換えて読む

どのシーンも、RULE（守るべき条件）／CHECK（試す操作）／EVIDENCE（記録するもの）の同じ枠です。CHECK の操作を貴社の画面・APIに当てはめてください。

シーン	RULE ／ 守るべき条件	CHECK ／ 試す操作	EVIDENCE ／ 記録するもの	ページ
01 **会員情報の分離**	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	会員IDの列挙、会員証コードの推測、アプリAPIの直接呼び出し、出力機能の悪用	到達の可否、再現手順、修正後に拒否されること	P.05
02 **ポイント・クーポンの不正操作**	付与・利用・交換は、購入実績と上限に一致する要求だけが通る	金額・回数の改ざん、二重送信、キャンセルとの競合、クーポンコードの使い回し	不正取得の可否と、通常の付与・利用が止まらないこと	P.07
03 **店舗権限の奪取・AI接客からの流出**	全店舗の会員情報・売上への到達は、本部の承認を経た操作だけが通る	店舗コードの差し替え、管理APIの直接呼び出し、AI接客への誘導文の注入	越権・漏えいの可否、モデル別の結果、未実施の経路	P.09

初回スコープ　1アプリ・1検証環境・2操作、準備完了後10営業日。1操作は、1つの業務操作（例: 返金、ロール変更）と、それにつながる API・画面の一式です。 どの2操作から始めるかは P.11 へ。

WITH YOUR CURRENT STACK

WAF と診断が通す「正しい形式の不正な要求」を、業務ロジックの層で止める

WAF・診断で既に見ている範囲は対象から外します。下の表の右列だけが、共同検証で追加する範囲です。



既存の対策	担う範囲	共同検証で足すもの
WAF・ボット対策（会員登録・ログイン）	既知の攻撃パターンと自動登録・総当たりの遮断	ログイン済みの会員・スタッフからの越権（他会員の情報、他店舗の操作）が成立しないことの検証
カード決済の不正検知	決済の異常パターンの検知	ポイント・クーポンなど、決済の外側で起きる不正操作の検証
定期的な脆弱性診断	決めた期間に広い範囲を調べ、指摘を出す	指摘の修正案づくりと再検証、会員・店舗権限の業務ルールの検証、再実行できるテストの作成

SCENE 01 ／ 会員情報の分離 ／ OWASP API1 BOLA

他の会員の情報や利用履歴に、到達できないか。

RULE 「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」

VERIFICATION LOG ／ MEMBER DATA / ACCESS CONTROL　SAMPLE

時刻	操作者	対象	経路	修正前	修正後
10:02	**会員本人**	自分の情報	通常の取得	許可	許可
10:05	**会員本人**	他会員の情報	会員IDの列挙	到達	拒否
10:11	**会員本人（別端末）**	他会員の情報	会員証コードの推測	拒否	拒否
10:18	**外部連携（APIキー）**	他会員の情報	アプリAPIの直接呼び出し	到達	拒否
10:24	**会員本人**	他会員の情報	出力機能の悪用	到達	拒否

他の会員の情報へ、アクセスできないことを確認。

想定リスク

会員本人・店舗スタッフそれぞれの権限で、会員IDの列挙、会員証のバーコード・QRの推測、アプリAPIの直接呼び出し、CSV出力の悪用を試し、分離がサーバー側で確認されているかを検証します。

CHECK ／ 試す操作

- 会員IDの列挙
- 会員証コードの推測
- アプリAPIの直接呼び出し
- 出力機能の悪用

EVIDENCE ／ 記録するもの

- 到達の可否
- 再現手順
- 修正後に拒否されること

SCENE 01 ／ 会員情報の分離

会員IDがURLやQRに載り、差し替えが効く

相談の前にここまで確かめておくと、初回の2操作がすぐ決まります。手順は検証環境・テストアカウントで行ってください。

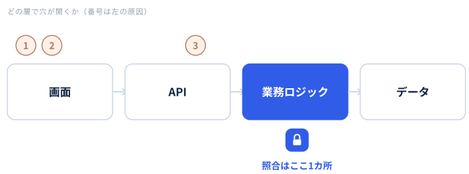
No.	自社で確かめる手順（検証環境で）	期待する結果	自社の結果
1	自分の会員IDを他人のIDに書き換えて、会員情報APIを呼ぶ	拒否される	☐ 到達　☐ 拒否
2	アプリの通信を記録し、本人確認の無いエンドポイントを一覧にする	本人確認の無い経路が0件	☐ 到達　☐ 拒否
3	レシート・予約の共有URLを少しずつ変えて、他人のものが開けないか見る	開けない	☐ 到達　☐ 拒否

よくある原因

① 会員ID・予約IDがURLやQRに載っていて、差し替えると他人の情報が返る

② 会員アプリ用APIがアプリの実装を信用し、サーバー側で本人確認していない

③ 利用履歴・レシートの共有URLが推測可能で、失効しない



修正の方向

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。

共同検証では、会員向けAPI・店舗端末・共有URLの全経路を AI で洗い出し、IDの差し替えを網羅的に試します。

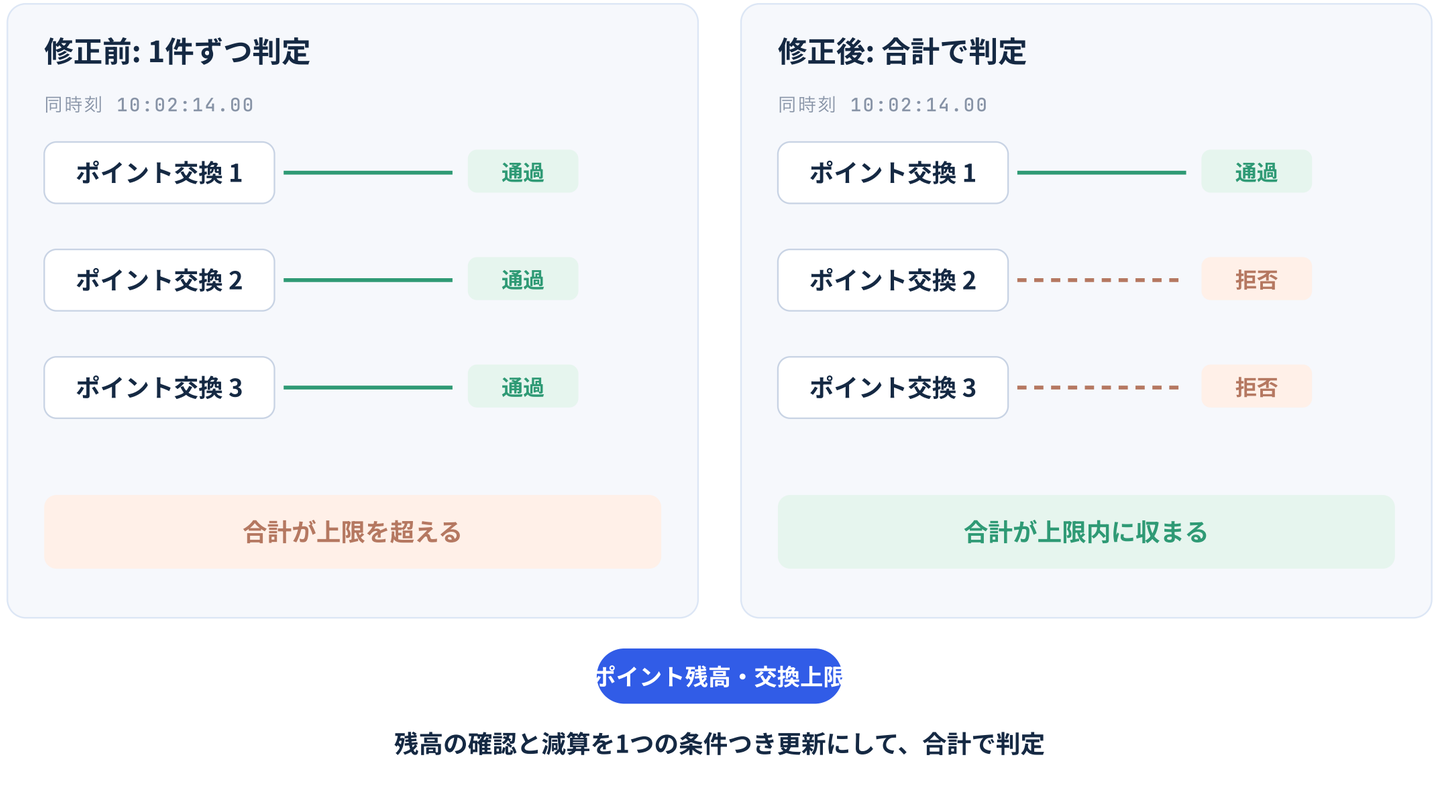
SCENE 02 ／ ポイント・クーポンの不正操作 ／ OWASP API6（業務フロー）／ API4

購入実績や上限を超えた付与・交換が、通らないか。

RULE 「付与・利用・交換は、購入実績と上限に一致する要求だけが通る」

CONCURRENT REQUESTS ／ POINTS / COUPON VERIFICATION

SAMPLE



想定リスク

ポイント付与・利用・交換、クーポン適用のAPIについて、金額・回数の改ざん、二重送信、キャンセルとの競合、コードの使い回しを試し、条件の照合がサーバー側で行われているかを確認します。

CHECK ／ 試す操作

- 金額・回数の改ざん
- 二重送信
- キャンセルとの競合
- クーポンコードの使い回し

EVIDENCE ／ 記録するもの

- 不正取得の可否と
- 通常の付与・利用が止まらないこと

SCENE 02 ／ ポイント・クーポンの不正操作

付与・交換を、画面側の計算のまま受け取っている

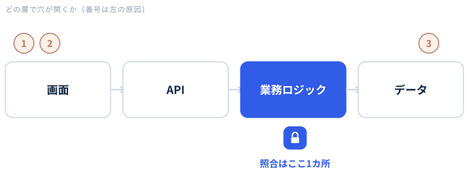
No.	自社で確かめる手順（検証環境で）	期待する結果	自社の結果
1	交換APIに残高を超えるポイント数を送る	拒否される	☐ 到達　☐ 拒否
2	同じクーポンを2端末から同時に使う	1回だけ通る	☐ 到達　☐ 拒否
3	ポイント付与後に返品し、付与分が取り消されるか見る	付与分が取り消される	☐ 到達　☐ 拒否

よくある原因

① ポイント付与・交換が、画面側の計算結果をそのまま受け取っている

② 交換の上限・回数がクライアント判定で、連打や並行で超えられる

③ 返品・キャンセル後も付与ポイントが残る。クーポンコードが使い回せる



修正の方向

付与・交換はサーバー側で購入実績と残高を照合し、残高の確認と減算を1つの条件つき更新にする。返品・キャンセルと付与を連動させる。

共同検証では、付与・交換・返品・クーポンの組み合わせを AI で生成し、どの順序で超えたかを記録します。

SCENE 03 ／ 店舗権限の奪取・AI接客からの流出 ／ OWASP API5 BFLA ／ API6

1店舗のアカウントやAI接客から、全店舗の情報に届かないか。

RULE 「全店舗の会員情報・売上への到達は、本部の承認を経た操作だけが通る」

APPROVAL MATCH ／ STORE PRIVILEGE BOUNDARY

SAMPLE

承認画面

申請者	起票者
要求	店舗端末の要求
対象	承認時の内容
承認者	権限のある担当者

承認

照合

EXECUTE REQUEST ／ diff

承認ID: #A-1042

要求: 店舗端末の要求

- 対象: 承認時の内容

+ 対象: 承認後に書き換え

× 不一致 → 実行しない

一致した要求だけが実行される: 担当店舗の操作

他店舗・本部の操作は、実行しない

想定リスク

店舗コードの差し替えや管理APIの直接呼び出しで本部・他店舗の会員情報や売上に到達しないか、AI接客・問い合わせ応答がある場合は誘導によって他の会員の情報を回答しないかを複数モデル・手順で確認します。

CHECK ／ 試す操作

- 店舗コードの差し替え
- 管理APIの直接呼び出し
- AI接客への誘導文の注入

EVIDENCE ／ 記録するもの

- 越権・漏えいの可否
- モデル別の結果
- 未実施の経路

SCENE 03 ／ 店舗権限の奪取・AI接客からの流出

店舗端末の権限が、店舗単位で切られていない

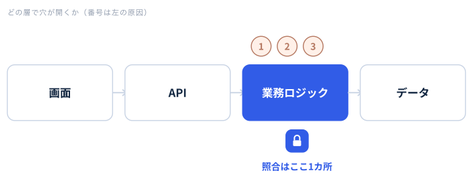
No.	自社で確かめる手順（検証環境で）	期待する結果	自社の結果
1	1店舗のアカウントで他店舗の会員・売上を検索する	担当店舗の結果だけ	☐ 到達　☐ 拒否
2	店舗端末から本部メニューのURLを直接開く	開けない	☐ 到達　☐ 拒否
3	AI接客に、他の会員の来店履歴を聞く	答えない	☐ 到達　☐ 拒否

よくある原因

① 店舗端末のアカウントが、全店舗の会員・売上を見られる権限になっている

② 本部機能に、店舗アカウントのロール変更で到達できる

③ AI接客が会員DB全体を参照でき、本人以外の情報を答える



修正の方向

店舗権限は店舗単位に限定し、本部機能は別ロールにする（複数店舗を担当する責任者は、担当店舗の一覧と照合）。AI は本人のセッション権限だけで回答する。

共同検証では、店舗・本部・AI接客の権限表を先に作り、表の「—」のマスが実際に拒否されるかを網羅的に試します。

FIRST 2 OPERATIONS

初回の2操作は、影響の広さと、10営業日で一巡できるかで選ぶ

当社が推奨する順です。順番は相談で入れ替えられます。1操作は、1つの業務操作（例: 返金、ロール変更）と、それにつながる API・画面の一式です。



1

会員情報の分離

会員情報の流出は店舗の信用に直結する。会員ID・予約IDの差し替えは経路が少なく、10営業日で一巡できる

2

ポイント・クーポンの不正操作

不正な付与・交換は金銭損失になり、気づきにくい

次回以降

店舗権限の奪取・AI接客からの流出 — 店舗権限の越境は、多店舗展開でスタッフ端末を共用している場合に優先度が上がります。

CHECK SHEET

6つの欄を埋めれば、初回の2操作はほぼ決まる

印をつけた状態でご相談いただくと、30分で初回スコープと費用の出し方まで決められます。

Q1

守りたいデータ

☐ 会員情報
☐ ポイント・クーポン
☐ 店舗スタッフ権限
☐ その他（　　）

Q2

気になる操作

☐ 会員IDの列挙
☐ 会員証コードの推測
☐ 金額・回数の改ざん
☐ 二重送信
☐ その他（　　）

Q3

権限の種類

☐ 会員
☐ 店舗スタッフ
☐ 店舗責任者
☐ 本部管理者
☐ その他（　　）

Q4

既存の対策

☐ WAF・ボット対策（会員登録・ログイン）
☐ カード決済の不正検知
☐ 定期的な脆弱性診断
☐ その他（　　）

Q5

検証環境の有無

☐ 検証環境がある
☐ これから用意する
☐ その他（　　）

Q6

提出先・期限

提出先: _____　期限: ____／____

チェックシートに印をつけて、30分の無料相談へ。

守りたいデータと気になる操作が分かれば、初回に検証する2操作と環境を一緒に決められます。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。

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。

FREE CONSULTATION

30分無料相談を予約する

チェックシート（P.12）の内容をもとに、初回スコープと費用の出し方をご説明します。

予約ページへ →

SET

02 プログラムのご案内 ／ 03 設計の考え方

対象・期間・費用・体制は 02、権限表と照合の場所は 03 へ。