Securiy セキュリー

01 EC・マーケットプレイス・全13ページ

業種別 検証シーン集

EC向け検証シーン集

返金額・対象の改ざん・注文・配送先の変更・
権限の越境を検証する

USE CASES ／ FOR COMMERCE & MARKETPLACES

FOR COMMERCE & MARKETPLACES

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、EC・マーケットプレイスの3シーン（返金額・対象の改ざん・注文・配送先の変更・権限の越境）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

返金を自動化したが、金額と対象の確認はフロント頼み

画面では制限していても、APIを直接叩くと注文額を超える返金や他人の注文への返金が通るかを確かめていない。

他社の情報流出の報道を見て、自社は大丈夫かと聞かれた

経営・出店者・決済代行会社から聞かれて、実際に試した記録がない。

出店者・購入者・運営者の権限が、機能追加で入り組んでいる

出店者が他店の注文や売上に届かないか、購入者が配送先を他人の注文で変えられないかを全部は追えていない。

対象: EC・マーケットプレイスの経営者・プロダクト責任者・開発リードの方へ

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 **返金額・対象の改ざん**	返金は、注文の金額・対象・状態と一致する要求だけが通る	金額の改ざん、注文IDの差し替え、二重送信、状態の競合	改ざんの可否と、通常の返金が止まらないこと	P.05
02 **注文・配送先の変更**	確定後の変更は、本人または権限を持つ運営者だけが行える	注文IDの列挙、状態の飛ばし、価格・数量の書き換え	変更の可否、再現手順、修正後に拒否されること	P.07
03 **権限の越境**	出店者は自店の範囲、運営者は承認された操作の範囲に限る	店舗IDの差し替え、管理画面APIの直接呼び出し、AI応答への誘導	越権の可否、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	既知の攻撃パターンと自動アクセスの遮断	正常な通信として通る不正操作（他人の注文への返金、他店のデータ取得）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	返金・注文変更など、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、返金・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 ／ 返金額・対象の改ざん ／ OWASP API6（業務フロー）

注文額を超える返金や、他人の注文への返金が通らないか。

RULE 「返金は、注文の金額・対象・状態と一致する要求だけが通る」

REQUEST LEDGER ／ ORDER / REFUND VERIFICATION　SAMPLE

要求		権限	対象	金額	結果
10:02	**注文額の範囲内の返金**	✓	✓	✓	許可
10:05	注文額を超える返金	✓	✓	✗	拒否
10:11	他店の注文への返金	✓	✗	✓	拒否
10:18	返金済み注文への再返金	✓	✓	✗	拒否
10:24	**修正後の通常の返金要求**	✓	✓	✓	許可

通常の返金は継続。不正な対象・金額の変更は拒否。

想定リスク

返金APIのパラメータ差し替え、重複送信、キャンセルと返金の競合を試し、権限・対象・金額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

- 金額の改ざん
- 注文IDの差し替え
- 二重送信
- 状態の競合

EVIDENCE ／ 記録するもの

- 改ざんの可否と
- 通常の返金が止まらないこと

SCENE 01 ／ 返金額・対象の改ざん

返金額と対象を、画面の値のまま信じている

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。

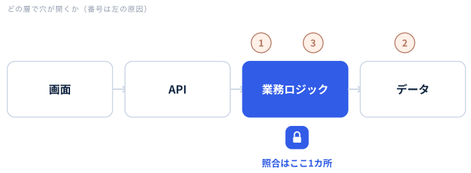
No.	自社で確かめる手順（検証環境で）	期待する結果	自社の結果
1	注文額を超える返金額をAPIで送る	拒否される	☐ 到達　☐ 拒否
2	同じ注文に部分返金を繰り返し、累計が支払額を超えるか見る	累計が支払額に達した時点で拒否	☐ 到達　☐ 拒否
3	他人・他店の注文IDで返金を要求する	拒否される	☐ 到達　☐ 拒否

よくある原因

① 返金額を注文額・支払済額と照合せず、画面から来た値を信用している

② 部分返金を繰り返すと累計が支払額を超える。ポイント・クーポンで払った分を現金で返している

③ 返金対象の注文IDが、操作者の権限（担当店舗・自分の注文）と照合されていない



修正の方向

返金はサーバー側で注文額・支払額・返金累計・対象の所有を照合し、累計が支払額を超える要求は拒否する。一定額以上は承認必須にする。

共同検証では、返金・キャンセル・交換の経路を AI で洗い出し、CS向けツールや一括処理も含めて試します。

SCENE 02 ／ 注文・配送先の変更 ／ OWASP API5 BFLA ／ API6

確定後の注文内容や配送先を、権限外の操作で変えられないか。

RULE 「確定後の変更は、本人または権限を持つ運営者だけが行える」

APPROVAL MATCH ／ ORDER CHANGE / AUTHORIZATION

SAMPLE



一致した要求だけが実行される: 権限内の変更

他人の注文への変更は、実行しない

想定リスク

購入者・出店者それぞれの権限で、他人の注文の配送先・数量・価格を変更できないか、変更の通知や承認が迂回されないかを試します。

CHECK ／ 試す操作

- 注文IDの列挙
- 状態の飛ばし
- 価格・数量の書き換え

EVIDENCE ／ 記録するもの

- 変更の可否
- 再現手順
- 修正後に拒否されること

SCENE 02 ／ 注文・配送先の変更

確定後の注文変更が、状態と所有者を見ていない

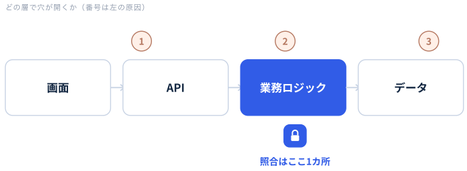
No.	自社で確かめる手順（検証環境で）	期待する結果	自社の結果
1	出荷済み注文の配送先をAPIで変更する	拒否される	☐ 到達　☐ 拒否
2	他人の住所IDを指定して注文を更新する	拒否される	☐ 到達　☐ 拒否
3	ゲスト注文の確認URLで、他の注文番号を推測して開く	開けない	☐ 到達　☐ 拒否

よくある原因

① 確定後の注文変更APIが、注文のステータスを確認せずに通る

② 配送先IDを本人の住所帳と照合していない

③ ゲスト注文の変更が、注文番号だけで可能になっている



修正の方向

注文の変更は状態と所有者をサーバー側で検査し、確定後は承認付きの経路に限定する。ゲスト注文の確認URLは推測不能・期限つきにする。

共同検証では、注文の状態遷移ごとに変更できる項目を表にし、経路（画面・API・外部連携）を横断して試します。

SCENE 03 ／ 権限の越境 ／ OWASP API1 BOLA

出店者が、他店のデータや運営者の機能に到達しないか。

RULE 「出店者は自店の範囲、運営者は承認された操作の範囲に限る」

VERIFICATION LOG ／ SELLER / OPERATOR BOUNDARY　SAMPLE

時刻	操作者	対象	経路	修正前	修正後
10:02	**出店者**	自店の売上	通常の取得	許可	許可
10:05	**出店者**	他店の売上	店舗IDの差し替え	到達	拒否
10:11	**出店者（別端末）**	他店の売上	管理画面APIの直接呼び出し	到達	拒否
10:18	**外部連携（APIキー）**	他店の売上	AI応答への誘導	到達	拒否
10:24	**出店者**	他店の売上	IDの差し替え	拒否	拒否

他店の情報と運営者の機能へ、到達できないことを確認。

想定リスク

出店者アカウントで他店の売上・顧客情報に届かないか、運営者向けの機能（一括操作・手数料の変更）に到達しないか、AIによるレコメンドや問い合わせ応答がある場合はその経路も確認します。

CHECK ／ 試す操作

- 店舗IDの差し替え
- 管理画面APIの直接呼び出し
- AI応答への誘導

EVIDENCE ／ 記録するもの

- 越権の可否
- モデル別の結果
- 未実施の経路

SCENE 03 ／ 権限の越境

店舗IDをリクエストから受け取っている

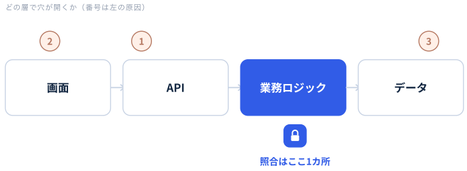
No.	自社で確かめる手順（検証環境で）	期待する結果	自社の結果
1	出店者Aのトークンで店舗BのIDを指定し、売上を取得する	拒否される	☐ 到達　☐ 拒否
2	運営者画面のURLを出店者アカウントで開く	開けない	☐ 到達　☐ 拒否
3	出店者の売上CSVに他店の行が混ざらないか確認する	自店の行だけ	☐ 到達　☐ 拒否

よくある原因

① 出店者向けAPIが店舗IDをリクエストから受け取り、ログイン店舗と照合していない

② 運営者機能のURLが推測可能で、ロール確認が画面側だけ

③ 店舗の集計・CSV出力が店舗横断で取得できる



修正の方向

リクエストの店舗IDは、ログイン中の出店者がその店舗を運営しているかをサーバー側で照合してから使う（複数店舗の出店者も同じ）。運営者機能は別ロール・別経路にする。

共同検証では、出店者・運営者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 AI で網羅的に試します。

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

返金額・対象の改ざん

金銭損失に直結し、カスタマーサポート経由で日常的に発生する操作。照合の場所が1カ所なので直しやすい

2

権限の越境

出店者が他店のデータに届くと、マーケットプレイス全体の信頼に関わる

次回以降

注文・配送先の変更 — 注文・配送先の変更は2操作目と入れ替えられます。既製ECの標準機能のみの構成は、提供事業者へのご確認をお勧めします。

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

☐ 返金
☐ 注文・配送先
☐ 出店者権限
☐ その他（　　）

Q2

気になる操作

☐ 金額の改ざん
☐ 注文IDの差し替え
☐ 注文IDの列挙
☐ 状態の飛ばし
☐ その他（　　）

Q3

権限の種類

☐ 購入者
☐ 出店者
☐ 運営者（CS）
☐ 運営者（管理者）
☐ その他（　　）

Q4

既存の対策

☐ WAF・ボット対策
☐ 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。