Securiy セキュリー

01 金融サービス・Fintech・全13ページ

業種別 検証シーン集

Fintech向け検証シーン集

送金先の不正変更・承認の迂回・
利用上限・回数の超過を検証する

USE CASES ／ FOR FINANCIAL SERVICES

FOR FINANCIAL 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、金融サービス・Fintechの3シーン（送金先の不正変更・承認の迂回・利用上限・回数の超過）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

承認フローを自動化したが、迂回経路を試した記録がない

承認APIと実行APIが別で、順序や状態の確認が抜けると、承認なしで実行に届く可能性がある。

他社の不正送金の報道を見て、自社は大丈夫かと聞かれた

経営・提携先の金融機関から聞かれて、即答できる材料がない。

取引APIを更新するたびに、確認項目が増え続ける

変更のたびに人手で再確認しており、前回と同じ条件で試せていない。

対象: 金融サービス・Fintechの経営者・CTO・開発責任者の方へ

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 **送金先の不正変更**	送金先の変更は、本人確認と承認を経た要求だけが通る	セッションの流用、パラメータ改ざん、変更APIの直接呼び出し	変更の可否、再現手順、修正後に拒否されること	P.05
02 **承認の迂回**	実行される内容は、承認された内容と一致する	状態遷移の飛ばし、承認IDの使い回し、承認後の内容変更	不一致で実行されたか否か、正常な承認フローへの影響	P.07
03 **利用上限・回数の超過**	上限はサーバー側で、要求ごとに確認される	並行リクエスト、分割、再送、AI経由の操作	超過の可否と、通常の取引が止まらないこと	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・不正検知（アカウント・決済）	既知の攻撃パターンの遮断と、取引の異常パターンの検知	正常に見える不正操作（承認の迂回、送金先の書き換え）が成立しないことの検証
外部の脆弱性診断、ペネトレーションテスト	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、承認・上限の業務ルールの検証、再実行できるテストの作成
監査ログ・承認ワークフロー	承認の手順と記録	承認した内容と実行された内容が一致することの検証

SCENE 01 ／ 送金先の不正変更 ／ OWASP API6（業務フロー）

登録済みの送金先を、権限外の操作で書き換えられないか。

RULE 「送金先の変更は、本人確認と承認を経た要求だけが通る」

REQUEST LEDGER ／ PAYEE CHANGE / VERIFICATION　SAMPLE

要求	本人確認	承認	権限	結果
10:02 **本人が再認証して送金先を追加**	✓	✓	✓	許可
10:05 他人の送金先IDを指定して変更	✓	✗	✓	拒否
10:11 再認証なしで送金先を変更	✗	✓	✓	拒否
10:18 通知先を変えた直後の送金先変更	✓	✓	✗	拒否
10:24 **修正後の通常の変更の要求**	✓	✓	✓	許可

本人の承認済み変更は継続。権限外の書き換えは拒否。

想定リスク

盗まれたアカウントやAPIキーの悪用を想定し、送金先・取引先の変更が本人確認・承認を経ずに通らないかを確認します。

CHECK ／ 試す操作

- セッションの流用
- パラメータ改ざん
- 変更APIの直接呼び出し

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 01 ／ 送金先の不正変更

送金先の変更に、再認証と所有者の照合が無い

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。

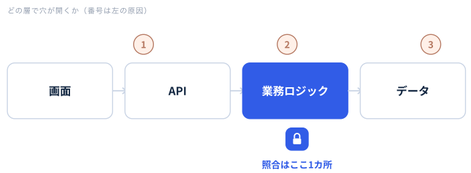
No.	自社で確かめる手順（検証環境で）	期待する結果	自社の結果
1	ログイン直後に、再認証なしで送金先を追加・変更できるか試す	再認証を求められる	☐ 到達　☐ 拒否
2	他人の送金先IDを指定して変更APIを呼ぶ	拒否される	☐ 到達　☐ 拒否
3	通知先を変更した直後に送金先を変更し、元の通知先に通知が届くか見る	元の通知先にも通知が届く	☐ 到達　☐ 拒否

よくある原因

① 送金先の変更APIが、再認証（OTP・パスワード）なしで通る

② 変更対象の送金先IDを、呼び出し元の口座の所有者と照合していない

③ 先に通知先（メール・電話番号）を変えてから送金先を変えると、本人が気づけない



修正の方向

送金先の変更は再認証と承認を必須にし、所有者をサーバー側で照合する。変更直後の一定時間は送金上限を下げ、変更履歴と本人への通知を残す。

共同検証では、送金先・通知先・本人確認の組み合わせを AI で洗い出し、連鎖させた場合も含めて試します。

SCENE 02 ／ 承認の迂回 ／ OWASP API5 BFLA ／ API6

未承認の取引を、実行できないか。

RULE 「実行される内容は、承認された内容と一致する」

APPROVAL MATCH ／ TRANSACTION INTEGRITY

SAMPLE



一致した要求だけが実行される: 一致した操作

不一致は、実行しない

想定リスク

承認待ちの取引を書き換える、承認済みIDを別の取引に使い回す、承認と実行の間で内容を変える、といった手順を試します。

CHECK ／ 試す操作

- 状態遷移の飛ばし
- 承認IDの使い回し
- 承認後の内容変更

EVIDENCE ／ 記録するもの

- 不一致で実行されたか否か
- 正常な承認フローへの影響

SCENE 02 ／ 承認の迂回

承認IDと実行内容が結びついていない

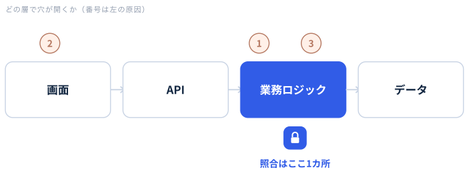
No.	自社で確かめる手順（検証環境で）	期待する結果	自社の結果
1	承認後に取引内容を変更して実行し、承認時の内容と比較する	不一致として実行されない	☐ 到達　☐ 拒否
2	承認前の取引IDで実行APIを呼ぶ	拒否される	☐ 到達　☐ 拒否
3	同じ実行リクエストを2回送り、起票者本人で承認を試す	2回目は拒否。自己承認は拒否	☐ 到達　☐ 拒否

よくある原因

① 承認IDと実行内容の紐づけが無く、承認後に金額・送金先を書き換えられる

② 承認ステータスを画面側で判定していて、サーバーが再確認していない

③ 起票者が自分で承認できる（自己承認）。承認済みの取引を再送すると二重に実行される



修正の方向

承認時の取引内容のハッシュを承認IDに結び、実行時に再計算して一致を確かめる。起票者と承認者は別にし、実行要求には冪等キーをつける。

共同検証では、承認フローの状態遷移（起票・承認・実行・取消）を AI で網羅し、順序の入れ替えや再送を含めて試します。

SCENE 03 ／ 利用上限・回数の超過 ／ OWASP API6（業務フロー）／ API4

1回・1日の上限を、分割や並行で超えられないか。

RULE 「上限はサーバー側で、要求ごとに確認される」



想定リスク

同時リクエストや分割送金で上限を超えられないか、AI機能（チャット経由の操作）がある場合はその経路も含めて確認します。

CHECK ／ 試す操作

- 並行リクエスト
- 分割
- 再送
- AI経由の操作

EVIDENCE ／ 記録するもの

- 超過の可否と
- 通常の取引が止まらないこと

SCENE 03 ／ 利用上限・回数の超過

上限の判定が、1回ごと・画面側だけになっている

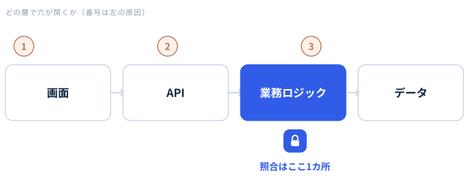
No.	自社で確かめる手順（検証環境で）	期待する結果	自社の結果
1	上限ぎりぎりの送金を分割して連続で送る	合計が上限を超えた時点で拒否	☐ 到達　☐ 拒否
2	同じ送金を同時に複数送り、合計が上限を超えないか見る	1本だけ通る	☐ 到達　☐ 拒否
3	上限に達した直後と日付の境界で、再度送金を試す	リセット前は拒否	☐ 到達　☐ 拒否

よくある原因

① 上限の判定が画面側か、1リクエスト単位でしか行われていない

② 並行リクエストで残高・回数の確認が競合し、両方通る

③ 日次上限のリセット時刻やタイムゾーンの扱いに抜けがある



修正の方向

残額の確認と減算を1つの条件つき更新（残額 ≧ 金額のときだけ減らす）で行い、アプリ・API・AI 経由の合計で判定する。

共同検証では、分割・並行・時刻境界の組み合わせを AI で生成し、どの条件で超えたかを記録します。

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

承認の迂回

承認と実行が別の API になっていると、照合の抜けが1カ所でも直接の金銭損失になる

2

送金先の不正変更

被害が直接の金銭損失になる。本人確認・承認の経路は数が少なく、10営業日で一巡できる

次回以降

利用上限・回数の超過 — 利用上限の超過は分割・並行の試験が中心です。2操作目と入れ替えられます。

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

☐ 送金先
☐ 承認
☐ 利用上限
☐ その他（　　）

Q2

気になる操作

☐ セッションの流用
☐ パラメータ改ざん
☐ 状態遷移の飛ばし
☐ 承認IDの使い回し
☐ その他（　　）

Q3

権限の種類

☐ 一般利用者
☐ 起票者
☐ 承認者
☐ オペレーター
☐ システム管理者
☐ その他（　　）

Q4

既存の対策

☐ WAF・不正検知（アカウント・決済）
☐ 外部の脆弱性診断、ペネトレーションテスト
☐ 監査ログ・承認ワークフロー
☐ 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 検証記録の作り方

対象・期間・費用・体制は 02、記録の残し方と提出先への説明は 03 へ。