

摩擦を生まない不正対策： 監査チェックリスト

貴社のセキュリティコントロールは、収益を守っていますか？
それとも顧客の購入をブロックしていますか？

顧客をストアフロントへ誘導するだけでも、決して容易なことではありません。それにもかかわらず、購入手続き時に煩わしいCAPTCHAや誤検知拒否、予期せぬログイン時の障壁によって正当な購入者をブロックしてしまうことは、ユーザーにストレスを与えるだけでなく多大な機会損失をもたらします。

多くの経営陣はチャージバックのコストを綿密に追跡していますが、誤検知による拒否や、コンバージョンを阻害するセキュリティ上の摩擦によって生じる「目に見えない収益の漏れ」まで測定できている企業はほとんどありません。

このチェックリストを活用して、現在の不正対策およびアイデンティティ管理環境を点検してください。硬直化したセキュリティ障壁が売上の妨げになっている箇所や、シンプルでモダンな脅威インテリジェンスにより、ユーザーに負担をかけることなくバックグラウンドで不正をブロックできる箇所を特定できます。

手順：現在の構成・環境に該当する各項目にチェックを入れてください。不明な場合や、一律で固定的なルールに頼っていることがわかっている場合は、チェックを入れずに未対応の課題として扱ってください。

1. ボット防御と境界セキュリティ

- ☐ ログインボックスやAPIに到達する前に、自動化されたボットトラフィックやクレデンシャルスタッフィングのスクリプトを境界でフィルタリングしていますか？
- ☐ 正当な顧客は、煩わしい画像認証やパズル認証（CAPTCHA）に邪魔されることなく、決済を完了できますか？
- ☐ エッジでのレート制限やIPレピュテーションによるフィルタリングを使用して、総当たり攻撃を自動的に阻止していますか？
- ☐ アクセスが急増するセール期間中に、正当なユーザーの処理速度を低下させることなく、悪意のあるスクリプトを賢くブロックできるボット対策を導入できていますか？

2. 認証情報セキュリティとATOの防止

- ☐ 送信されたパスワードをリアルタイムの流出認証情報データベースと自動的に照合し、悪用・流出したログインをブロックしていますか？
- ☐ パスワードの脆弱性を完全に排除するために、生体認証パスキー（Touch ID、Face ID、Windows Hello）を提供していますか？
- ☐ ユーザーは、チェックアウト時に時間のかかる摩擦の大きいメールリセットのループに陥ることなく、リスクのあるアカウントを安全にリセットできますか？
- ☐ 流出チェックの際、機密性の高いユーザー認証情報が平文で露出・送信されないよう、暗号ハッシュ照合（k-Anonymityなど）を使用していますか？

3. バックグラウンドリスクテレメトリー

- ☐ 貴社のシステムは、バックグラウンドシグナル（デバイスフィンガープリント、ブラウザの状態、IPレピュテーションなど）を50ミリ秒未満で評価できますか？
- ☐ シカゴでのログインから数分後にフランクフルトからAPIリクエストが送信されるなど、地理的に不可能な移動による異常を検知できますか？
- ☐ 正当でリスクの低いユーザーの90%以上が、セキュリティプロンプトやチャレンジなしでログインやチェックアウトを完了できていますか？
- ☐ コンテキストに基づくリスクが低いと判断された場合、透過的にバックグラウンドでセッショントークンが発行されますか？

4. アダプティブな検証とステップアップセキュリティ

- ☐ 多要素認証などの追加のセキュリティチェックは、セッションのリスクスコアが実際に急増した場合にのみ、確実に発動するようになっていますか？
- ☐ 認識済みのデバイスにおけるリスクの低いリピート購入について、追加の検証手順を強制することなくスムーズに購入手続きを進められますか？
- ☐ ステップアップ認証の実行を、配送先住所の更新や高額ポイントの交換などリスクの高いアクションだけに限定して適用していますか？
- ☐ 遅延の発生しやすいSMSのワンタイムパスコードのみに頼るのではなく、シームレスなプッシュ通知や生体認証による検証の選択肢はありますか？

5. 誤検知による拒否と収益ガバナンス

- ☐ 経営陣やリスク管理チームは、従来のチャージバック指標に加え、誤検知拒否（False Decline）率も積極的に測定していますか？
- ☐ 誤検知による取引拒否率を追跡し、業界の平均ベンチマークである1.5%未満に維持していますか？
- ☐ 過去に本人確認が完了している再訪問ユーザーに対し、アイデンティティ履歴に基づいて、決済時の過剰な不正利用チェックを自動的に免除・緩和していますか？
- ☐ 貴社のアイデンティティシステムは、リアルタイムのユーザーコンテキストやリスクテレメトリーを、下流の決済エンジンや不正検知エンジンに直接共有していますか？

6. 業種別のフリクション管理

- ☐ **小売・Eコマース**：購入意欲の高い顧客が、必須のアカウント作成フォームや重複する本人確認を強制されることなく、スムーズに決済を完了できますか？
- ☐ **ストリーミング・メディア**：ユーザーは、スマートTVとモバイルデバイス間で、頻繁な再認証プロンプトが表示されることなくログイン状態を維持できますか？
- ☐ **フィンテック・iGaming**：ユーザーは、初期段階での過度な本人確認手続きで待たされることなく、会員登録や少額の送金を即時に完了できますか？
- ☐ **旅行・ロイヤルティ**：顧客のロイヤルティポイント、ギフトカード、VIPマイルは、日常的なゲスト体験を損なうことなく、クレデンシャルスタッフィングから保護されていますか？

7. AIエージェントと自動トランザクションへの対応

- ☐ 貴社のセキュリティアーキテクチャは、悪意のあるスクレイピングボットと、顧客が利用する正当なAIショッピングエージェントを区別できますか？
- ☐ ユーザーの認証情報を直接露出させることなく、OAuth 2.0 Token Exchangeを使用して、有効期限が短く権限スコープを限定したトークンをAIアシスタントに発行できますか？
- ☐ 自動化されたAIトランザクションに対して、きめ細かな支出制限と実行可能な操作範囲を設定・適用していますか？
- ☐ 顧客は、個人のAIショッピングアシスタントに付与した権限を簡単に確認、管理、または取り消しできますか？

スコアを計算する

チェックを入れた項目の数を合計して、自社の顧客認証環境およびセキュリティ構成がどの段階にあるかを確認しましょう。

チェックが付いた項目24～28個 最適化済み

貴社の現在の環境・構成により、ユーザーに負担をかけずにバックグラウンドで不正をブロックし、正当な購入者にはスムーズな決済プロセスを提供できています。

チェックが付いた項目16～23個 堅牢だが収益漏れが発生

主要な防御機能は動作していますが、固定的なセキュリティ障壁や誤検知拒否により、売上機会を失っている可能性があります。

チェックが付いた項目16個未満 コンバージョン低下リスク大

時代遅れのセキュリティ対策と一律に課される操作障壁により、顧客が競合他社へ流出し、正当なユーザーに負担を強いています。

セキュリティリスクを高めることなく、決済時の摩擦を解消しませんか？

不正対策の評価は、あくまで出発点にすぎません。誤検知による拒否やログイン離脱を解消するために、技術スタックを全面的に入れ替えたり、セキュリティ基準を下げたりする必要はありません。ユーザーの負担にならないようバックグラウンドでコンテキストに基づくリスクを評価することで、正当な顧客のスムーズな購入手続きを維持しつつ、自動化された不正アクセスをリアルタイムで阻止できます。

30分間の技術スコープセッションをご予約ください。 Auth0のソリューションアーキテクトが、チェックリストの診断結果と一緒に確認し、現在のセキュリティ環境を評価したうえで、誤検知拒否をなくし売上を守るための個別プランを提案します。