02 全9ページ・全業種共通

AI攻撃対策・共同検証プログラム

プログラムのご案内

対象・進め方・費用・体制・情報の扱いを、
社内で回せる1冊に

Securiy セキュリー



ABOUT THE PROGRAM

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。



01 SIMULATE ／ 検証で実際にやること

1. API 仕様・画面・対象部分のソースコードから、操作と権限の一覧を作る
2. 「利用者の種類 × 操作 × 対象ID」の組み合わせを AI が手順として作り、検証環境で実行する
3. 成立した手順は担当者が手で再現して確かめ、RULE／CHECK／EVIDENCE として記録する。AI の出力をそのまま報告しない

〔要確定: 手順の表現を実施者と合わせる〕

02 PROTECT ／ 対策の設計

要求ごとに権限・承認・実行条件を照合し、範囲外の操作を止める仕組みを設計します。初回のプログラムで SDK の導入はお願いしません。照合の仕組みは、貴社のコードで実装する設計案と修正案としてお渡しします（SDK・制御サービスは設計・検証段階）。

03 ADAPT ／ 修正と再検証

見つかったリスクを直し、拒否されることと通常業務が壊れていないことの両方を確かめて、判断を記録します。

WHO IT IS FOR

対象は、検証と修正を自分で行えるチーム

3つの問いに「はい」なら対象です。業種別の検証シーンは 01 検証シーン集にまとめています。

Q1
自社で開発・運用している Web アプリ・API がある（受託開発のベンダーも可）
はい ↓ ／ いいえ → 対象外

Q2
検証用の環境とテストアカウントを用意できる
はい ↓ ／ いいえ → 対象外

Q3
目的が規制の適合審査・決済基盤全体の監査ではない
はい ↓ ／ いいえ → 対象外

対象です。初回スコープ（1アプリ・2操作）からご相談ください。

SaaS・ソフトウェア	テナント分離 ／ 管理者権限の奪取 ／ AI機能経由の持ち出し
金融サービス・Fintech	送金先の不正変更 ／ 承認の迂回 ／ 利用上限・回数の超過
EC・マーケットプレイス	返金額・対象の改ざん ／ 注文・配送先の変更 ／ 権限の越境
小売・店舗サービス	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
自治体・公共向けシステム	団体・住民間の分離 ／ 職員権限の奪取 ／ AI相談窓口からの流出
医療・介護向けシステム	施設間のデータ分離 ／ AI問診・記録支援からの持ち出し ／ 記録の改ざん・権限外の閲覧

PROCESS ／ 10 BUSINESS DAYS

貴社の作業は、準備と打ち合わせとレビューだけ

準備が整ってから10営業日。検証・修正案・再検証・報告の各段階で、成果物をお渡しします。コード・権限・モデルが変わったら、再実行用テストで必要な範囲を再検証します。



当社作業は合計40時間（うち改修2件・12時間まで）。貴社の作業は、準備と打ち合わせとレビューだけ。

SCOPE ／ FIRST ENGAGEMENT

初回スコープ確認書: この1枚で社内に回せる

小さく始めて、結果を見て広げます。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。 費用は対象と操作を決めた時点で、着手前に提示します。

初回スコープ確認書

共同検証プログラム ／ 着手前に合意

対象アプリ	[　　] 検証環境: [　　]
操作 1 ／ 操作 2	[　　] ／ [　　] ※1操作＝1つの業務操作と、それにつながる API・画面の一式
期間	準備完了後 10営業日（週次共有 2回、報告会 30分）
当社作業	合計 40時間（検証・修正案 2件まで 12時間・再検証・報告）
費用	着手前に提示。参加条件に合う場合は無償 （要確定：参加条件の文言）
お渡しするもの	☑ 検証記録　☑ 修正案（プルリクエスト）　☑ 再検証チェック　☑ 再実行用テスト
含まれないもの	規制の適合審査、本番環境での試験、決済基盤全体の監査

合意日　／　／　　貴社担当　　当社担当

TEAM ／ CONTRACT ／ DATA

体制・契約・情報の扱い

稟議に必要な3点です。経歴・第三者認証の取得状況は、相談時に現状をそのままお答えします。

体制

設計と最終確認は人が行う

検証の設計、成立した手順の再現、報告書の最終確認は、アプリケーションセキュリティの実務経験を持つ担当者が行います。AI は洗い出しと反復に使います。

〔要確定: 担当者の役割と経歴の書き方（社名を出さない範囲）〕

契約

秘密保持契約と業務委託契約を結んでから着手

着手前に秘密保持契約と業務委託契約を締結します。貴社の委託先評価の質問票には個別にご回答します。

〔要確定: 契約書のひな形・締結の流れ〕

AIモデルと情報の扱い

どのモデルに何を送るかを、先に決める

検証に使う AI モデルと処理場所、モデルに渡すデータの範囲を着手前に一覧でお示しします。貴社の指定でモデルを限定できます。本番の認証情報と実データは受け取りません。

〔要確定: 使用モデル・学習不使用の契約条件・処理場所〕

判断材料　初回は2操作・10営業日。結果の記録を見てから、続けるかどうかを判断できます。Securiy は Tempura technologies株式会社のセキュリティ事業です。

WHAT WE ASK ／ DATA HANDLING

本番の認証情報と実データは受け取らない

お預かりするのは、検証環境への接続情報、テストアカウント、対象部分のソースコードの閲覧権限です。

受け取らないもの

- ✕ ~~本番の認証情報（パスワード・APIキー）~~
- ✕ ~~顧客・患者・住民の実データ~~
- ✕ ~~本番環境への無断アクセス~~
- ✕ ~~検証に不要なソースコード~~

ご用意いただくもの

- ✓ 検証環境の URL と接続情報
- ✓ テストアカウント（利用者の種類ごと）
- ✓ 対象部分のソースコードの閲覧権限
- ✓ 構成・権限の説明、質問への回答
- ✓ 修正案（プルリクエスト）のレビューとマージ、報告会（30分）

データの扱い

合意
共有先・保管期間・公開可否・使用する AI モデルを文書で合意

検証
合意した環境・時間帯・停止条件の中で実施

保管
検証記録とログを合意した期間だけ保管

削除
期間後に削除し、削除の記録を残す

SecuriyのSDK・制御サービスは設計・検証段階です。本ページは共同検証プログラムのご案内であり、すべての問題の解消やリリース可否を保証するものではありません。合意した検証を完了し、判断に必要な検証結果をご報告します。

FAQ

よくあるご質問

ご検討の際に確認いただきたい5つの点です。

Q1 本番環境を直接攻撃するのですか？

初回は許可された隔離検証環境を前提にします。対象、データ、実行できる操作、停止条件を事前に合意してから実施します。

Q2 すべての攻撃を防げるようになりますか？

保証はしません。対象・予算に合わせたモデルと手順を選び、確認できた事項と未確認の事項を分けて報告します。新しい手法は継続検証に取り込みます。

Q3 費用はいくらですか？ 無償の条件は？

対象・操作・検証環境を決めた時点で、着手前に見積りを提示します。共同検証プログラムの参加条件に合う場合は無償です。〔要確定: 参加条件の文言（例: 匿名化した結果を手法の改善に使うことへの同意、報告後のフィードバック）〕 事例としての公開は条件に含みません。

Q4 年次の脆弱性診断とは何が違いますか？

診断は、決めた期間に広い範囲を調べ、指摘を出すところまでが中心です。共同検証は対象を2操作に絞り、貴社の業務ルール（誰が・何を・どの条件で）を RULE として書き出して試します。そのうえで修正案を作り、直ったことと通常の操作が止まらないことを再検証して、次の変更時に再実行できるテストとしてお渡しします。診断で認可を見ている場合は、その指摘の修正と再検証を担う分担もできます。

Q5 何を預ける必要がありますか？

検証環境への接続情報、テストアカウント、対象部分のソースコードの閲覧権限をいただきます。本番の認証情報と実データは受け取りません。結果の共有先・保管期間・公開可否も事前に合意します。

共同検証プログラムに参加しませんか。

初回の2操作で、検証・修正・再検証の結果を記録としてお渡しします。続けるかどうかは、その記録を見てから決めてください。

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

JOINT VERIFICATION

30分無料相談を予約する

守りたいデータと気になる操作を伺い、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 ／ 03 検証記録の作り方

業種別の検証シーンは 01、記録の残し方と提出先への説明は 03 へ。