Securiy

No.25 ノウハウ・全7ページ

1分でわかる

初回相談で決まること

対象の操作・試す立場・試す環境・完了条件

30分で決まる4つと、持ち帰るもの

相談前に埋める1枚つき

FIRST CALL

30分で決まる4つ

初回相談の30分は、サービスの説明ではなく、検証の対象を決めることに使います。守りたいデータと気になる操作を伺い、次の4つを決めます。終わったときに手元に残るメモは、右のようなものです。

0分 **現状を伺う**
事業・アプリ・気になっていること

5分 **守りたいデータと、気になる操作**
事故になる操作を2つに絞る

15分 **試す立場と、試す環境**
どのロールで、どこで試すか

25分 **完了条件と、次の一手**
何が残れば終わりか

30分

初回相談メモ（記入例）

説明のための架空の例 ／ オンライン 30分

1. 対象の操作	**顧客一覧の取得と CSV 出力（他組織のデータが見えないか）／送金先の変更（承認なしで通らないか）**
2. 試す立場	**一般ユーザー ／ 組織の管理者 ／ 外部連携の API キー**
3. 試す環境	**ステージングあり。テスト用の組織 A・B と各1アカウントを御社で用意（来週中）**
4. 完了条件	**2操作が拒否される記録が版・日付つきで残る ／ 見つかった分の修正差分と再検証結果がある**
次の一手	**Securiy からスコープ案と見積りを送付 → 御社で検討 → 合意書の案を確認**

4つが決まると、初回スコープ（1アプリ・2操作・準備完了後10営業日）と費用を着手前にお出しできます。

初回に検証する2操作の選び方

全部を一度に確かめる必要はありません。起きたら事故になる操作で、かつ検証環境で今すぐ試せるものから2つ。残りの操作は、初回の結果と手順書をもとに、御社で足すか外部に出すかを決めます。



選ぶ基準 1

起きたら事故になる操作

他社のデータが見える、承認なしで金額や宛先が変わる、権限が勝手に上がる。取引先や利用者に説明が必要になる操作です。

選ぶ基準 2

検証環境で今すぐ試せる操作

ステージングとテストアカウントで再現できること。ステージングがなくても、本番とは別のテスト用の組織とアカウントを用意する方法から一緒に決めます。

対象外

先に決めておくもの

金融の規制適合審査、決済基盤全体の監査、カード不正判定は対象外です。EC プラットフォームの標準機能だけで運営している場合は、提供事業者への確認をお勧めします。

3 ／ 相談の前に

相談前に埋める1枚

4つの欄を埋めてお持ちいただくと、初回で対象の操作まで決まります。手ぶらでも構いません。本番の認証情報や顧客データは書かないでください。

1 ／ 守りたいデータ

漏れたり書き換えられたりすると困るもの

例: 顧客の氏名・連絡先、取引先の口座、注文・配送先、契約プラン、API キー

2 ／ 気になる操作

「これが通ったら事故」という操作

例: 他組織の顧客一覧の取得・CSV 出力、承認なしの送金先変更、返金、権限の付与、外部連携からの一括操作

3 ／ 権限の種類

誰がどこまでできるか

例: 一般ユーザー ／ 組織の管理者 ／ システム管理者 ／ 購入者・出店者・運営者 ／ 外部連携の API キー

4 ／ 既存の対策と環境

いま入れているものと、試せる場所

例: WAF（境界で攻撃の通信を見張る仕組み。製品名）、年次の脆弱性診断（最終実施月）、認可 SDK（権限判定の部品）・IdP（ログインの一元管理）、監視。ステージング・テストアカウントの有無

あると早いもの、お持ちにならないでほしいもの

手ぶらでも相談できます。あると早いものと、お持ちにならないでほしいものを分けました。本番の認証情報や実データは、相談でも検証でも受け取りません。

あると早いもの（なくても相談できます）

機能の一覧か、主な画面
何ができるアプリか。画面のスクリーンショットでも可

権限の種類
一般・管理者・外部連携など、誰がどこまでできるか

検証環境の有無
ステージング・テストアカウントの有無と用意できる時期

既存の対策
WAF・監視・年次の脆弱性診断など、いま入れているもの

気になっていること
取引先の指摘、過去のヒヤリ、リリース前の不安

お持ちにならないでください

本番の認証情報
本番のパスワード・API キー・トークン。検証でも受け取りません

顧客データ
実データの複製やサンプル。検証は検証環境用のテストデータで行います

本番環境へのアクセス
合意した検証環境で実施します

ソースコードについて

初回相談では不要です。修正案を作る段階では、対象の操作に関わるコードを合意した範囲と方法（画面共有、期限つきの読み取り権限など）で拝見します。

相談の内容は、ご了承なく社外に出しません。

ご希望があれば、相談の前に秘密保持契約を結びます。

相談のあとに起きること

相談が終わると、こちらから初回スコープ案と見積りをお送りします。進めるかどうかは、それを見てから決めていただけます。
費用は、検証する操作の数、検証環境の準備状況、修正案の件数で決まります。



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・合計40時間（修正案と再検証は2件・12時間まで）。報告会は10営業日の最終日に行います。

守りたいデータと、気になる操作をひとつ。

決めた条件で画面と API から試すところまでは自社でできます（No.09 P.09）。外に出す価値があるのは、まだ決めていない条件と経路（承認内容の書き換え・連携キー・AI 機能）を広く洗い出して試し、試さなかったものも未検証範囲として書いた、取引先に出せる記録にするところです。守りたいデータと気になる操作を伺えば、30分で初回スコープの目安まで決まります。P.04 のシートを埋めてお持ちいただくと早いですが、手ぶらでも構いません。本番の認証情報や顧客データは不要です。

お申し込み・お問い合わせ　**securiy-preview.pages.dev**　のフォームから
Tempura technologies株式会社

※ 初回スコープの条件は共同検証プログラムのものです。すべての攻撃の網羅や「安全」の総合判定は保証しません。金融の規制適合審査、決済基盤全体の監査、カード不正判定は対象外です。

無料相談

30分無料相談

オンラインで30分。守りたいデータ、気になる操作、試す立場、試す環境を伺い、初回に検証する2操作を一緒に決めます。

相談を申し込む →

共同検証プログラムとは

検証テーマを一緒に作る企業に、初回スコープで提供する枠組み

1アプリ・1検証環境・2操作、準備完了後10営業日・合計40時間（修正案と再検証は2件・12時間まで）。費用は着手前に提示します。

次に読む

早わかり「SIMULATE／PROTECT／ADAPT」

どのサービスから始めるかの判定と、初回の組み合わせ方、質問と答えはこちら。