No.06 サービス紹介・全9ページ

1分でわかる

SIMULATE PROTECT ADAPT 早わかり

SIMULATE

PROTECT

ADAPT

リスクの検証、不正操作への対策、修正と再検証。3つのサービスの役割と成果物を1枚ずつ

Securiy

OVERVIEW

いま提供しているのは、SIMULATE と ADAPT

Securiy は「見つける」で終わらせません。見つけたリスクを直し、直した後に確かめます。PROTECT は、確かめた条件を仕組みにするための設計・検証段階のサービスで、SDK の提供時期は未定です。

提供中

SIMULATE

リスクの検証: どの操作で不正が成立するかを確かめる

何を聞くか	**どの操作で不正が成立してしまうか**
何をするか	攻撃者と同じ手順で不正な操作を試し、 合意した検証環境で繰り返す
何が残るか	成立した経路・再現条件・影響範囲・ 修正候補・未検証範囲の一覧

ADAPT

修正・再検証の支援: 直して、両方を確かめる

何を聞くか	**直した後、別の操作が壊れていないか**
何をするか	修正案を作り、拒否されることと 通常操作が通ることの両方を再検証する
何が残るか	修正差分・再検証結果・ 修正候補つきの残課題

設計・検証段階 ／ SDK の提供時期は未定

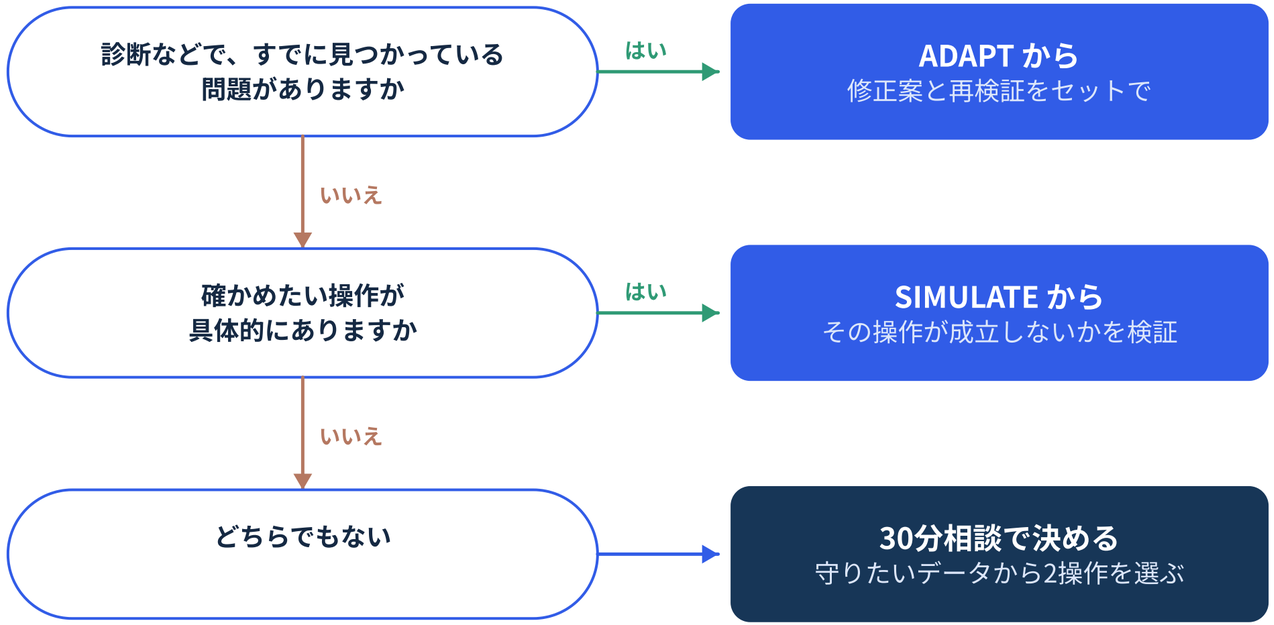
PROTECT

不正操作への対策

SIMULATE と ADAPT で確かめた「誰が・何を・どの条件で」を、要求ごとに照合して範囲外を止める仕組みにする設計。共同検証の中で設計から始めます。

どれから始めるか: 3つの質問で入口が決まる

3つを同時に始める必要はありません。最初の相談で聞く3つの質問で、入口が決まります。



迷ったら、SIMULATE から

守りたいデータと気になる操作を伺い、
初回に検証する2操作を決めます。
見つかったものは、同じ初回スコープの中で
ADAPT が修正案と再検証まで引き受けます。

30分無料相談
守りたいデータと気になる操作を伺う

初回スコープの提案
1アプリ・2操作・10営業日。費用は着手前に提示

PROTECT の設計
SIMULATE の結果をもとに、報告の中で提案

SIMULATE　リスクの検証: 検証記録はこう残る

攻撃者と同じ手順で不正な操作を試し、どの操作で不正が成立するかを、合意した検証環境で確かめます。残るのは「安全」の判定ではなく、再現できる記録です。

こんなときに　「他社のデータが見えないか確かめたい」「新しい API を公開する前に権限の抜けを洗いたい」「取引先に検証結果を示したい」

検証記録 ／ SIM-003（説明のための架空の例）　　対象版 `v2.4.1` ／ 検証環境 `staging`

操作	誰が	何を指定して	結果
顧客一覧の取得	**組織 A の一般ユーザー**	**URL の組織 ID を B に書き換え**	**成立（B 社のデータが返った）**

影響の範囲

顧客一覧・CSV 出力・検索 API の3経路で同じ条件が成立。画面からは拒否される。

再現手順

```
01 組織 A の一般ユーザーでログイン
02 GET /api/customers?org=B を直接要求
03 200 OK で B 社の顧客 128 件が返る
```

修正候補

要求の org をセッションの所属組織と照合し、不一致は 403 を返す

確かめていない範囲

管理者ロール、外部連携 API キー経由の取得、バッチ処理

複数の経路を広く試すのは AI エージェント、成立したものの妥当性と影響を判断するのは専門家です。

成果物: この記録が、成立した経路の数だけ1冊にまとまります。取引先に出せる粒度で書きます。

PROTECT　不正操作への対策: 要求ごとに3つの関門で止める

要求ごとに、権限・承認・上限を1カ所で照合し、範囲外の操作を止める仕組みを設計します。画面でも API でも AI 機能でも、同じ関門を通します。

設計・検証段階 ／ SDK の提供時期は未定。共同検証の中で、操作ごとの許可条件を設計書にまとめるところから始めます。

1つの要求

返金 ¥120,000
組織 A の担当者 ／ 注文 #4411
画面・API・AI 機能・外部連携の
どこから来ても同じ



権限
担当者は返金できる

承認
上長の承認済み

上限
1件 ¥100,000 を超えている

範囲外のため停止
拒否の理由と要求の内容を記録し、申請に回す

こんなときに

「承認された内容と実行内容を一致させたい」
「AI 機能や外部 API にも同じルールを掛けたい」
「返金・送金先変更に上限を付けたい」

いまできること

操作の棚卸し → 許可条件の設計 → 例外処理の定義 → 導入時の検証項目。
この4つを設計書にまとめ、既存コードに組み込む形で提案します。
仕組みへの組み込みは御社の開発で行います。SDK として提供する時期は未定です。

ADAPT　修正・再検証の支援:「直った」と「壊れていない」を同じ表で

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。

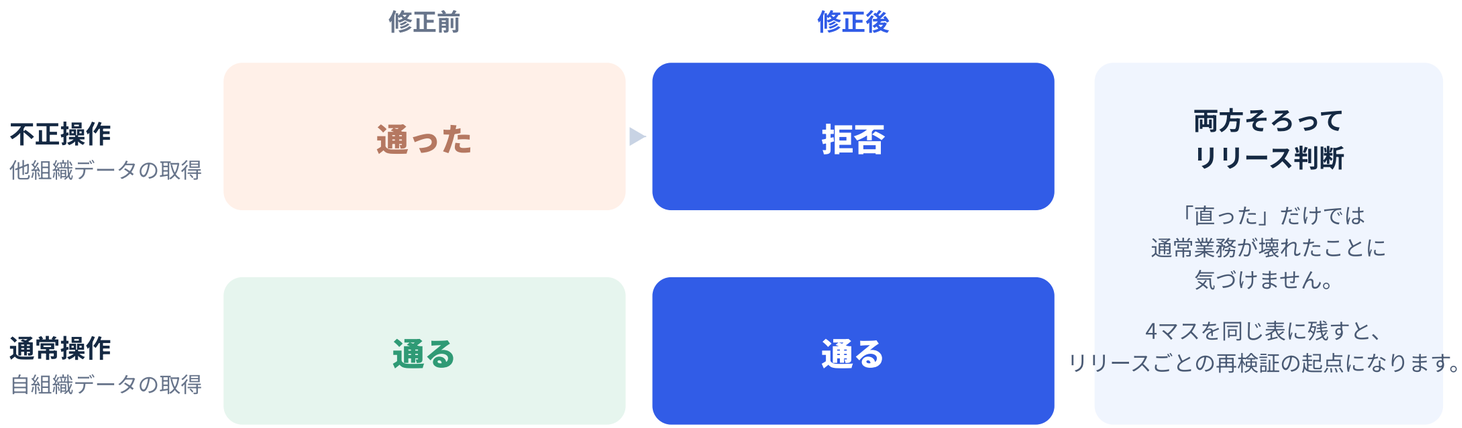
修正差分（例）

```
def customers(request):
- org = request.GET['org']
+ org = request.user.org_id
+ if request.GET.get('org') != org:
+ return forbidden()
return Customer.filter(org=org)
```

修正案はレビューを反映して御社で適用。
適用後に、下の4マスを同じ手順で確かめます。

こんなときに

「修正案まで欲しい」
「直した後に別の操作が壊れていないか不安」
「リリース判断の根拠を残したい」



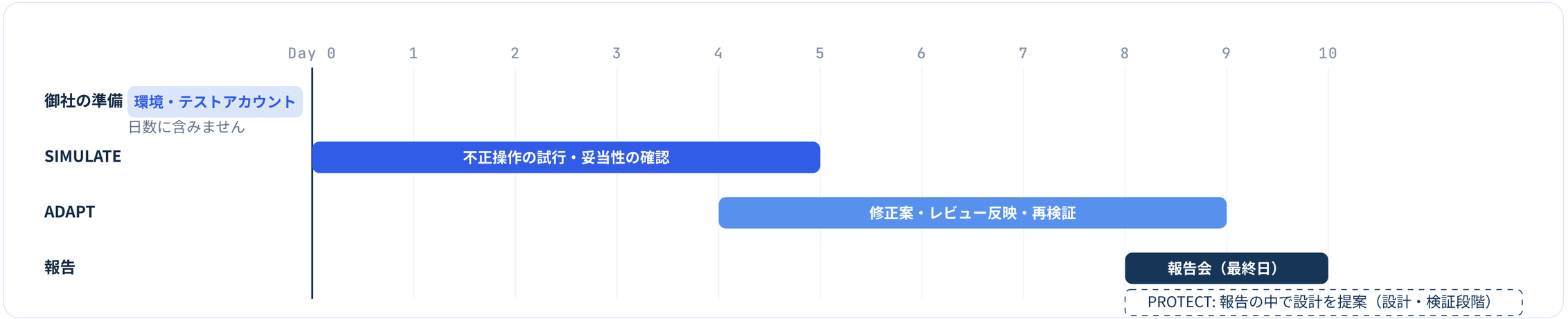
成果物

修正差分 ／ 通常操作と不正操作の再検証結果（上の4マス） ／ 修正候補つきの残課題 ／ 判断の記録（誰が・いつ・何を根拠に）

初回スコープでは、修正案と再検証を2件・12時間まで含みます。

初回はこう組み合わせます

小さく始めます。2操作を SIMULATE で検証し、見つかったものを ADAPT で直して再検証。準備が整ってから10営業日で報告会まで。
費用は対象と操作を決めた時点で、着手前に提示します。



対象

1アプリ・1検証環境・2操作

たとえば「顧客データの取得」と「送金先の変更」。事故になる操作から選びます。

期間と工数

10営業日・合計40時間

検証・修正案・再検証・報告の合計。修正案と再検証は2件・12時間まで含みます。週次で進捗を共有。

含まれるもの

検証から報告会まで

シナリオ設計、不正操作の試行、報告書、修正案、再検証、報告会。

費用

着手前に提示

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。見積りは無料で、お断りいただいても構いません。

先にお答えしておくこと

検討の段階で確かめておきたいことを先に書きます。ここに書けないことは、初回相談でそのままお答えします。

AI にうちの環境を触らせて大丈夫ですか。データを外部の AI に送るのでは。

試す操作・環境・時間帯は事前に文書で合意し、合意した操作以外は実行しません。検証で得た応答やコードを外部の AI サービスに送るかどうか、送る場合の学習利用の有無は、範囲の合意書に明記します。いつでも止められる窓口を決めてから始めます。

導入実績はありますか。

導入企業名は公開していません。代わりに、検証の前に範囲と情報の扱いを文書で合意し、報告書のサンプルと合意書の案を事前にお見せします。

WAF と年1回の診断で十分では。

WAF（Web アプリへの通信を境界で見張る仕組み）は既知の攻撃パターンに一致する通信を遮断し、ログインした利用者の権限外の要求は見ません。年次診断は渡したアカウントと画面・API の範囲で認可も試しますが、診断後に足した操作や見積りに入れなかった経路（連携キー＝外部ツール用の API キー・AI 機能）は残ります。重なる部分は提案せず、足りない検証だけを提案します。判定の手順は No.26 P.05 にあります。

PROTECT（SDK）はいつ使えますか。

設計・検証段階で、提供時期は未定です。いまは共同検証の中で、操作ごとの許可条件を設計書にまとめ、既存コードに組み込む形で提案します。

費用はいくらですか。

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。初回スコープは合計40時間・修正案と再検証2件までの枠で見積もり、着手前に明細つきで提示します。見積りは無料です。

ステージング環境がありません。

相談できます。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など、用意の仕方から一緒に決めます。本番環境に無断で触れることはありません。

最初の一手は、
気になる操作をひとつ。

3つ全部を決める必要はありません。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、初回に検証する2操作と入口のサービスが決まります。初回のご相談は30分・無料です。

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

※ PROTECT（不正操作を防ぐ SDK）と継続検証システムは設計・検証段階で、提供時期は未定です。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

どのサービスから始めるか、初回スコープと費用の決まり方をご説明します。
本番の認証情報や顧客データは不要です。

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

紹介編「Securiyのご紹介」／初回相談で決まること

仕組みの全体像と報告書の書き方、30分の相談で決まる4つはこちら。