No.24 ノウハウ・全10ページ

WEEKLY

RELEASE

継続検証のロードマップ

一度きりの診断から継続検証へ

公開情報の取り込み、照合、再検証を回し続けるために、最初に決めておく運用の形

NOTIFY

VERSION

Securiy

この資料でわかること

年1回の診断は、その時点の版を確かめたものです。毎週リリースするアプリでは、診断の翌週からずれ始めます。この資料は、検証を「回し続ける」ために最初に決めておくことを整理します。自動化の仕組みがなくても回せる手順と運用の形を扱います。カード業界の基準（PCI DSS）も、年1回に加えて重要な変更の後の試験と、修正後の再試験を求めています。

想定読者

年次診断の報告書が「古い」と言われた開発責任者

リリースが毎週〜毎月あり、取引先から「変更時の確認」を求められる SaaS・Fintech・EC 事業者。

扱うこと

3つのループと、先に決める3つ

公開情報の照合・リリースごとの再検証・定期の深掘り。許可・版の一致・通知の決め方。手動から半自動へのロードマップ。

扱わないこと

自動化ツールの選定、CI の設定手順

特定の CI（コードを取り込むたびにテストを自動で走らせる仕組み）や監視製品の設定は扱いません。「何を回すか」を決める資料です。

1 なぜ回し続けるか

診断から離れるほど、ずれが積み上がる P.03

回すのは3つのループ P.04

2 先に決める3つ（許可・版・通知）

許可: 誰が、どこまでの検証を認めるか P.05

版の一致: 検証した版と本番の版 P.06

通知: 何を・誰に・いつ P.07

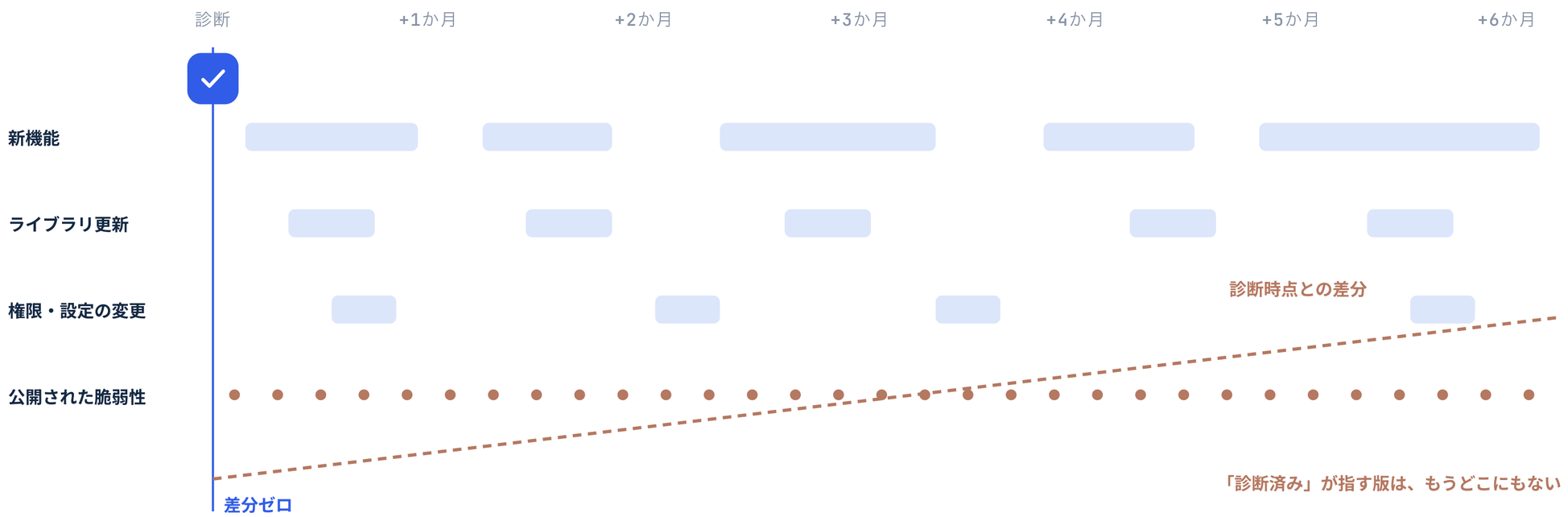
3 回し始める

手動 → 半自動 → 自動のロードマップ P.08

点検表 P.09

診断から離れるほど、ずれが積み上がる

診断の翌週から、新機能・ライブラリ更新・権限の変更・新しく公開された脆弱性が積み上がります。半年後の「診断済み」は、もう存在しない版の話です。



報告書は正しい。ただし指しているのは診断時点の版です。半年後の本番は、機能も依存関係も権限も別物になっています。

回すのは3つのループ

継続検証といっても、全部を毎日やるわけではありません。頻度の違う3つのループを、それぞれ回せる大きさで持ちます。



年次診断を捨てるのではなく、3つ目のループとして残します。足すのは左の2つ。どちらも手順書とスプレッドシートで始められます。

操作の選び方は No.25 P.03、候補の洗い出しは No.19 P.05。

3つのループの記録を同じ表に集めると、取引先への「変更時の確認」「既知脆弱性の確認」「診断の実施」に1枚で答えられます。

許可: 誰が、どこまでの検証を認めるか

回し続ける検証は、毎回「やっていいか」を聞いていたら止まります。最初に範囲と方法を決めて許可を取り、その中では自由に回せるようにします。ここでいう許可は検証の許可で、業務の承認とは別です。

決めること	内容	誰が認めるか	残すもの
検証の対象	どのアプリ・どの環境・どの操作を試してよいか	開発責任者	**対象の操作の一覧（2〜3操作から）**
試す方法	正当なアカウントで範囲外の操作を試す。攻撃の手口は使わない	開発責任者	**手順書（誰として・何を・期待する結果）**
本番への影響	原則は検証環境のテストアカウントだけ。本番に検証用の組織を作る場合は、他の顧客のデータに触れない範囲と時間帯を決める	開発責任者・情シス	**環境と認証情報の分離の記録**
結果の扱い	成立した操作は誰に知らせ、いつまでに直すか	開発責任者	**通知先と期限（P.07）**
外部に出すとき	共同検証など外部に任せる範囲、情報の保管と削除	開発責任者・法務	**範囲と取り扱いの合意書**

最初の許可は、1アプリ・1検証環境・少数の操作の小さな範囲で取ります。回り始めてから広げるほうが、許可も取りやすくなります。業務の「承認」（送金の承認など）とは別の話です。

版の一致: 検証した版と、本番の版

検証記録があっても、本番で動いている版と一致していなければ、取引先には「古い版の確認」としか言えません。デプロイの手順に1行足すだけで、一致は保てます。



版の一致を保つ最小の形

1. 検証記録に「対象の版」を必ず書く（Git のタグやコミット ID）
2. デプロイ手順の最後に「この版の検証記録はあるか」を1行入れる
   なければデプロイ前に決めた操作を試して追記する
3. 記録がない版を本番に出すときは、理由を書く（緊急修正など）
4. 月に1回、本番の版と記録の版が一致しているかを見る

「検証した」と「本番で動いている」が同じ版を指していること。継続検証の信頼は、ここで決まります。

通知: 何を・誰に・いつ

回し続ける仕組みは、結果が誰にも届かなければ止まります。通知は5種類で足ります。多すぎると読まれなくなるので、増やしません。

何を	誰に	いつ	何を添えて
不正操作が成立した	開発責任者・該当機能の担当	即時	**操作・再現条件・影響の範囲・暫定対応（上限を下げる等）**
修正が必要（期限つき）	担当者・開発責任者	判断した日	**対象・期限・担当。期限超過で再通知**
再検証で拒否を確認した	開発責任者・（取引先担当の営業）	リリース判断の前	**版・日付・拒否と正常の両方の結果**
公開情報に該当があった	照合の担当	週次の照合時	**脆弱性 ID・該当箇所・優先度（KEV・EPSS＝悪用される見込みの推定）**
記録がない版が本番に出た	開発責任者	デプロイ時	**版・理由・いつ検証するか**

通知の宛先に「取引先担当の営業」を入れておくと、チェックシートの回答期限が来たときに、最新の記録がどこにあるかを営業が自分で探せます。

3 ／ 回し始める

手動 → 半自動 → 自動のロードマップ

最初から自動化する必要はありません。手動で3か月回ると、何を自動化すべきかが見えてきます。自動で回す仕組みは設計・検証段階で、いまあるのは左の2段階です。



今日から

- 対象の2〜3操作を決め、手順書に書く
- リリース前に同じ手順で試し、1操作1行で記録
- 週次30分で公開情報を照合し、1件1行で記録
- 記録に版を書く。デプロイ手順に1行足す

ツールの費用は掛かりません。
人の時間は週1時間程度が目安です。

手動が3か月回ったら

- 手順書の2〜3操作を、API のテストとして書く
- CI のリリース前ジョブに入れ、失敗で止める
- 結果を記録の表に自動で追記
- 公開情報の照合は通知機能に任せ、判断だけ人が

人の作業は「判断」と「新しい操作の追加」だけに。

自動化するときに決めること

- 公開情報の取り込みと構成の照合を自動で回す
- リリースのたびに操作を自動で試す
- 許可・版・通知を仕組みに組み込む

自社で作るか、外部の仕組みを使うかは、
手動と半自動の記録が揃ってから決めます。

この資料の許可・版・通知の設計は、
どの段階でもそのまま使えます。

自動化は後からで構いません。先に決めるのは、許可・版の一致・通知。この3つがあれば、手動でも継続検証は成立します。

点検表: 手動で回し続けられる状態か

7つが揃えば、手動でも継続検証は回ります。Q1・Q2・Q3 の3つがあれば、今週から始められます。「2〜3操作」は自社で回す場合の目安で、共同検証プログラムの初回スコープは2操作です。

No.	点検すること	区分	状態	担当
Q1	**検証の対象・方法・本番への影響を、誰が認めるか決めた**	許可	ある ／ 一部 ／ ない	
Q2	**リリースごとに試す2〜3操作と手順書がある**	許可	ある ／ 一部 ／ ない	
Q3	**検証記録に対象の版（タグ・コミット ID）が書いてある**	版の一致	ある ／ 一部 ／ ない	
Q4	**デプロイ手順に「この版の検証記録はあるか」の1行がある**	版の一致	ある ／ 一部 ／ ない	
Q5	**通知5種類の宛先と期限が決まっている**	通知	ある ／ 一部 ／ ない	
Q6	**週次の公開情報の照合が回っている（No.10）**	ループ1	ある ／ 一部 ／ ない	
Q7	**定期の深掘り（四半期〜年1回）で、新しい機能の操作を検証対象に足している**	ループ3	ある ／ 一部 ／ ない	

自社で回るもの

許可・版・通知を決め、決めた操作を手順書で繰り返すところまでは、この資料の手順で自社で回せます。

外に出す価値があるもの

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記録にするところ。
共同検証プログラムの初回スコープで、手順書と記録の型を作ります。

手順書と記録の型から、一緒に回し始める。

許可・版の一致・通知を決め、決めた操作を決めた条件で画面と API から繰り返し試すところまでは自社で回せます（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。共同検証プログラムの初回スコープでは、選んだ2操作の手順書と記録の型を作ります。手順書があれば、3つ目からの操作は自社で足していけます。自動で回す仕組みは設計・検証段階です。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

※ 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。本資料の運用の形は、Securiy のサービスを使わなくても成立します。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

いまの診断の頻度とリリースの頻度を伺い、最初に回す2操作と、検証の許可の取り方を一緒に決めます。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。手順書と記録の雛形をお渡しします。

次に読む

No.10 既知の脆弱性が放置される3つの壁
No.12 エンプラ顧客に提供するための3つの観点

ループ1の回し方と、記録を取引先に示す方法はこちら。