Securiy

No.26 ノウハウ・全6ページ

1分でわかる

既存の WAF・診断とどう組み合わせるか

置き換えではなく追加。いま入れている対策の範囲を棚卸しし、診断の見積書で範囲を確かめ、足りない確認だけを決める手順

GUIDE

3つは見ている場所と頻度が違う。重なるのは、診断の認可の項目だけ

「WAF（Web アプリへの通信を境界で見張り、攻撃のパターンに一致する通信を止める仕組み）と年次診断があるのに、まだ要るのか」に最初に答えます。重なるのは、診断の見積りに入れた認可の項目と、確認が同じ操作を試す部分だけ。重なる部分は診断に任せ、確認からは外します（P.05）。このページは、見積書のどこを見れば範囲が分かるかまで扱います。連携キーは、外部のツールがアプリの API を呼ぶためのキーです。

	担う範囲（外さない）	担わない範囲
WAF 常時・境界で	既知の攻撃パターンに一致する通信を遮断 異常な量・頻度の通信を検知	ログインした利用者が、権限外のデータを 正常な形で要求すること（ID の書き換え）
年次の脆弱性診断 年1回・その時点の版で	共通の脆弱性の型を網羅的に検出。認可の項目も ある（渡したアカウントと画面・API の範囲で）	見積りに入れなかった経路（連携キー・AI 機能） 診断後に足した操作、仕様を渡さなかった業務操作
成立しないことの確認 操作を足したリリースごと	決めた操作を「誰として・何を指定して・どの経路で」 試し、成立しないことを記録する	既知の攻撃パターンの遮断、脆弱性の型の網羅 （上の2つの範囲は、この確認では代替しない）

診断の見積書か報告書で確かめる5項目。書いてある範囲は、診断で足りている

- **① 対象の版と日付**
- **② アカウント: 2組織・権限違い**
- **③ 経路: 画面／API／連携／AI**
- **④ 権限表と承認の流れを渡すか**
- **⑤ 診断後の変更の扱い**

書いていない項目が、P.03 の「担わない範囲」の欄に入ります。各製品の範囲の詳しい説明は No.09 P.04 にあります。

いま入れている対策を、1枚に棚卸しする

相談や見積りの前に、この表を埋めます。「版・日付」が埋まらない行、「試せる経路」に連携キー・AI 機能が入らない行が、抜けている場所です。埋めた表は P.05 の判定フローに1行ずつ当てます。薄い字は説明のための記入例で、上書きしてください。

対策	担う範囲	頻度	範囲を最後に見直した版・日付	試せる経路	担わない範囲
WAF	境界の通信 （攻撃パターンの遮断）	常時	例: 2026.09 ルール更新	例: 画面・API（境界を通るもの）	例: ログイン後の権限外の要求
年次の脆弱性診断	共通の脆弱性の型と、渡した範囲の認可	年1回	例: v2.3 ／ 2026.04	例: 見積書の対象一覧で確かめる	例: 診断後に足した操作
認証（IdP）・認可 SDK	ログインと、権限判定の仕組み	常時			例: 判定が全経路で呼ばれているか
監視 ／ SIEM	異常の検知と記録	常時			例: 検知される前に成立しない状態にすること
依存ライブラリの照合	公開済みの脆弱性との照合 （No.10）	毎週			
業務操作の確認 （未実施なら空欄）	自社固有の業務操作				

書き方

年次診断の行は、見積書か報告書の「対象範囲」を写します。対象のリクエスト一覧に守りたい操作の API が入っていて、権限の違うテストアカウント（2組織分）で認可を試す項目があれば、その操作は診断の範囲です。代表の画面だけを選ぶ診断もあるので、操作ごとに確かめます。

用語

IdP: ログインを一元管理する仕組み。認可 SDK: 「この利用者がこの操作をしてよいか」を判定する部品。SIEM: 各システムの記録を集めて突き合わせ、異常を検知する仕組み。
依存ライブラリの照合: 使っているライブラリの版と公開された脆弱性情報を突き合わせること。

3 ／ 組み合わせ方

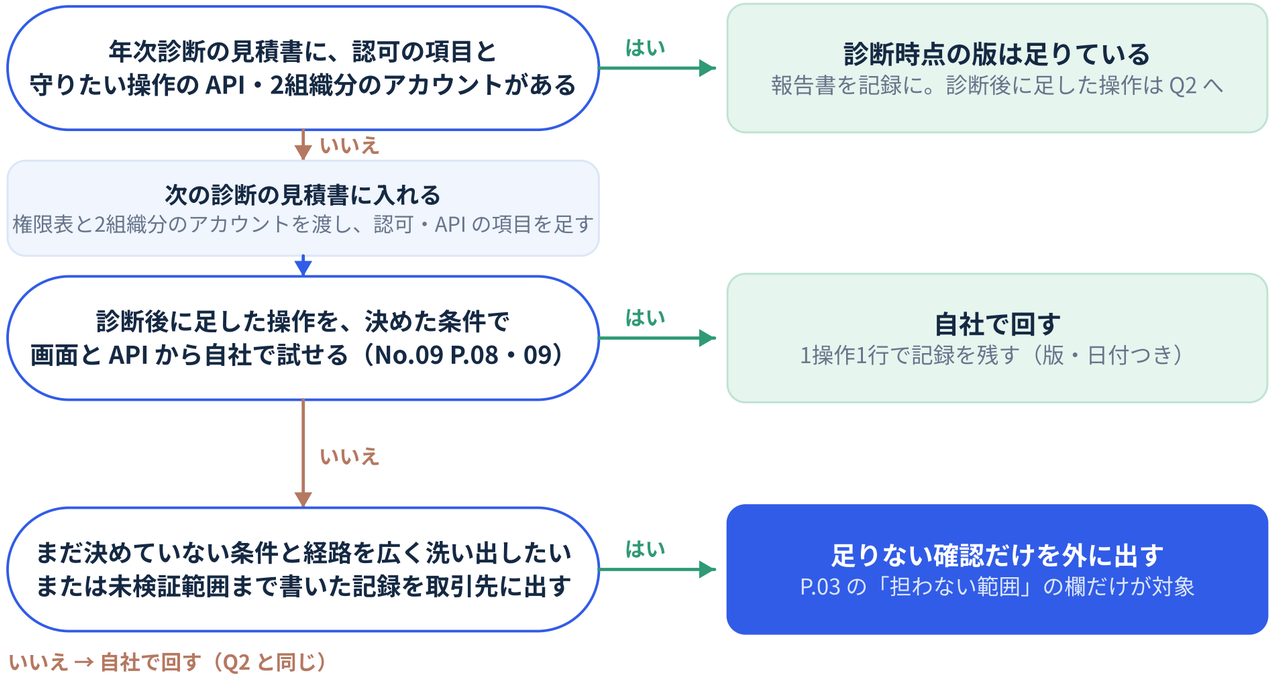
年間でどう並べるか: 診断の前に権限表、診断の後に残った操作

3つを同じ年表に置きます。診断の前に業務操作の一覧と権限表を作るのは、権限表と2組織分のアカウントがないと診断員は組織をまたぐ操作を試せないから。診断の後に確認を置くのは、報告書が出るまで何が試されたか分からないからです。リリースごとの回し方は No.24 にあります。



足すか、足さないか: 棚卸しの1行ごとに3つの質問を当てる

出口は4つ。診断に入れる・足りている・自社で回す・外に出す。同じ会社でも、行によって分かれます。診断会社に API も認可も見てもらえば済みますが、年1回の版に限ります。リリースのたびに足した操作は、診断を毎回頼むか、自社で回すか、外に出すかの3つから選びます。



外に出すときも、重ねて頼まないもの（どの事業者でも）

- ✕ WAF の置き換え・ルールの運用
- ✕ 年次診断の置き換え（網羅的な検出）
- ✕ IdP・認可 SDK の導入や設定
- ✕ 監視・SIEM の導入や運用
- ✕ 診断で足りている範囲を、別の事業者に重ねて頼む
- ✕ AI 機能の診断（注入の検知）の代わり

外に出すのは P.03 の「担わない範囲」に書いた経路だけ。
見積りを比べるときも、この欄と照らします。

外す対策はない。
抜けている確認だけを足す。

棚卸しの表を埋め、診断の見積書で範囲を確かめ、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）。P.05で「診断に入れる」「自社で回す」になった行は、外に出す必要はありません。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。作った人が自分の設計を試すと、設計の前提の外にある条件を思いつきにくいためです。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

※ 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

P.03の棚卸しの表と、診断の見積書（範囲のページ）をお持ちください。外に出す必要がない行はそうお伝えします。そのうえで、足りない確認から初回の2操作を決めます。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。

次に読む

No.09 「診断済み」でも事故が起きる理由
No.24 一度きりの診断から継続検証へ

製品が担う範囲の詳しい表と、リリースごとの回し方はこちら。