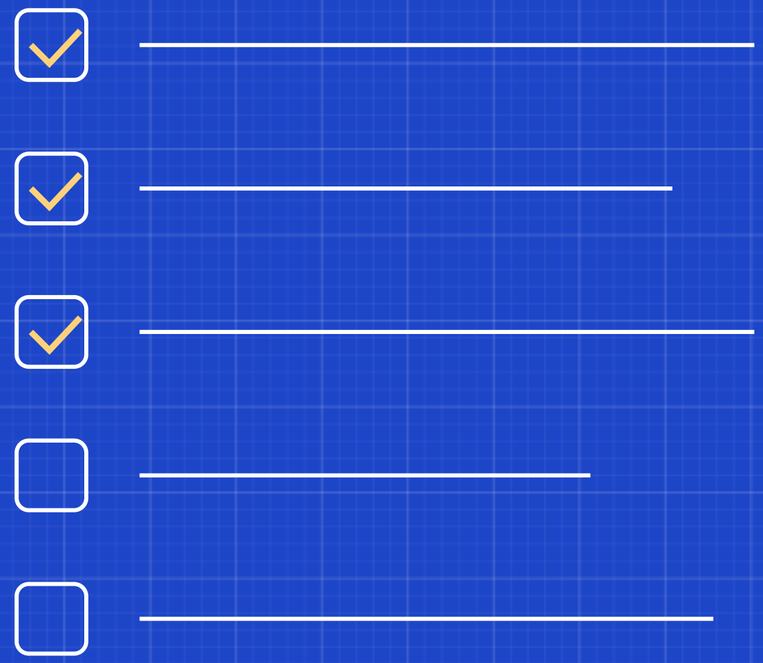
SECURIY DOCS — No.17 選定シート

外に出すときの選び方

セキュリティ検証ベンダー選定シート

実行環境・情報の扱い・修正と再検証・未検証範囲の明記。15の設問と3社比較シート



Securiy

7 PAGES · 2026.10
TEMPURA TECHNOLOGIES

見積りの前に比べるべきは、情報の扱いと修正後の確認

見つける力はどのベンダーも強調するため、見積りの段階では比べにくい項目です。比べやすく、後から差が出やすいのは、預ける情報の扱いと、直して確かめるところまで含まれるかどうかです。

見つける力

どの会社も強調するので、
見積りの段階では比べにくい。

検出数・価格・AI の有無は
前提として確認するにとどめ、
差が出やすい右の4つで比べます。

- 検出数
  対象と期間が違えば比べられない
- AI の有無
  使っているだけでは差にならない
- 価格
  含まれるものが違えば比べられない

見積りの前に比べる4つ

預ける情報
本番の認証情報や実データを求めるか。
保管・削除・公開の取り決めが先にあるか。

直し方
一覧を渡して終わりか、修正案まで出すか。
既存のコードに組み込める粒度か。

確かめ方
直した後に同じ操作を試すか。通常業務が
壊れていないかも見るか。変更のたびに回せるか。

報告の書き方
再現条件が1行で分かるか。確かめていない
範囲を書くか。取引先にそのまま出せるか。

設問15項目: 5つの観点 × 3問

候補のベンダーに見積りを依頼する前に、この15問を送ってください。答え方を比べると、進め方の違いが見えます。

No.	設問	確認したい答え
A-01	**本番環境に無断で攻撃しないか**	検証環境・対象・操作・時間帯を文書で合意する
A-02	**やらないことを言うか**	規制適合審査、基盤全体の監査など対象外を明示する
A-03	**AI と人の役割分担を説明できるか**	AI が広く探し、人がシナリオと妥当性を判断する
B-04	**本番の認証情報・顧客データを預かる必要があるか**	検証環境とテストアカウントだけで実施できる
B-05	**検証に使った情報の保管と削除を決めるか**	保管期間・削除の時期・方法が文書にある
B-06	**結果の共有先と事例公開の可否を事前に決めるか**	報告書の共有範囲、公開の可否を先に合意する
C-07	**修正案まで含むか**	見つけて終わりではなく、直し方まで出す
C-08	**修正後に拒否と正常の両方を再検証するか**	「直った」と「壊れていない」を同じ表で示す
C-09	**変更のたびに再検証する手段があるか**	リリースごと、公開情報が出たときに回せる
D-10	**再現条件が書かれるか**	誰が・何を・どの条件で、が1行で分かる
D-11	**未検証の範囲を明記するか**	「安全」と総合判定せず、見ていない範囲を書く
D-12	**取引先にそのまま出せる粒度か**	チェックシートの設問に対応づけて添付できる
E-13	**担当者の経験と体制を説明できるか**	誰が何を判断するか、経験の種類を示せる
E-14	**費用に含まれるものが明細で分かるか**	再検証・修正支援・報告会の有無が見積りに書かれている
E-15	**実績を確認できるか**	公開できる事例、または公開できない理由と代わりに示せるもの

A 環境と範囲 ／ B 情報の扱い ／ C 修正と再検証 ／ D 報告の書き方 ／ E 体制と費用

答えの読み方: 確認したい答えと、注意したい答え

同じ「はい」でも中身が違います。設問4つを例に、どこを見分けるかを示します。正解は一つではなく、自社の優先度に合うかで決めます。

A-01　本番環境に無断で攻撃しないか

確認したい答え

検証環境・対象の機能・試す操作・時間帯を事前に文書で合意します。本番に触れる場合も範囲と時間を限定し、合意なく広げません。

注意したい答え

「本番で試したほうが実態に近いので、全体に対して実施します」。範囲と時間の合意がない。

B-04　本番の認証情報・顧客データを預かる必要があるか

確認したい答え

検証環境とテストアカウントで実施します。本番の認証情報や実データは受け取りません。

注意したい答え

「管理者アカウントと本番データの複製をいただければ早いです」。預かる理由が「早いから」だけ。

C-08　修正後に拒否と正常の両方を再検証するか

確認したい答え

修正後、不正操作が拒否されることと、通常操作がそのまま通ることを同じ表で示します。

注意したい答え

「修正後の確認は対象外です。再診断は別途お見積りです」。直した後に同じ操作を試す手段が用意されていない。

E-15　実績を確認できるか

確認したい答え

公開できる事例を示すか、公開できない場合はその理由と、代わりに報告書のサンプル・合意書の雛形を事前に見せます。

注意したい答え

「実績は多数ありますが、守秘義務で何も出せません」。代わりに示せるものがない。

3 ／ 比較シート

1枚で3社を比べる

自社の優先度（◎必須／○あれば／△不要）を先に1回だけ決め、候補ごとの答えを ○・△・× と一言で書きます。◎の設問で「注意したい答え」が出た候補は外します。

No.	設問	自社の優先度	候補 A	候補 B	候補 C
A-01	本番環境に無断で攻撃しないか	◎ ○ △			
A-02	やらないことを言うか	◎ ○ △			
A-03	AI と人の役割分担を説明できるか	◎ ○ △			
B-04	本番の認証情報・顧客データを預かる必要があるか	◎ ○ △			
B-05	検証に使った情報の保管と削除を決めるか	◎ ○ △			
B-06	結果の共有先と事例公開の可否を事前に決めるか	◎ ○ △			
C-07	修正案まで含むか	◎ ○ △			
C-08	修正後に拒否と正常の両方を再検証するか	◎ ○ △			
C-09	変更のたびに再検証する手段があるか	◎ ○ △			
D-10	再現条件が書かれるか	◎ ○ △			
D-11	未検証の範囲を明記するか	◎ ○ △			
D-12	取引先にそのまま出せる粒度か	◎ ○ △			
E-13	担当者の経験と体制を説明できるか	◎ ○ △			
E-14	費用に含まれるものが明細で分かるか	◎ ○ △			
E-15	実績を確認できるか	◎ ○ △			

候補 A: _____　候補 B: _____　候補 C: _____　記入日: _____／____／____

4 ／ Securiy の回答

同じ15問に、Securiy はこう答えます

自社に都合のよい設問だけを並べたと読まれないよう、◯だけでなく△も書きます。△の3つは、初回相談で現状をそのままお伝えします。

No.	設問	回答	内容
A-01	**本番環境に無断で攻撃しないか**	◯	検証環境・対象の機能・試す操作・時間帯を文書で合意します。本番環境には無断で触れません。
A-02	**やらないことを言うか**	◯	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。先に示します。
A-03	**AI と人の役割分担を説明できるか**	◯	AI エージェントが経路を広く探して繰り返し、専門家がシナリオの設計と妥当性・影響の判断を担います。
B-04	**本番の認証情報・顧客データを預かる必要があるか**	◯	本番の認証情報・実データは受け取りません。検証環境用のテストアカウントだけで実施します。
B-05	**検証に使った情報の保管と削除を決めるか**	◯	検証ログの保管期間と削除の時期・方法を、始める前に合意書に書きます。
B-06	**結果の共有先と事例公開の可否を事前に決めるか**	◯	報告書の共有先と、事例としての公開可否を、始める前に決めます。公開は任意です。
C-07	**修正案まで含むか**	◯	修正案を出します。初回スコープでは2件・12時間までを含みます。
C-08	**修正後に拒否と正常の両方を再検証するか**	◯	不正操作が拒否されることと、通常操作がそのまま通ることを、同じ表で再検証します。
C-09	**変更のたびに再検証する手段があるか**	△	自動で回す仕組み（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。現在は手順書と記録の雛形をお渡しし、再検証は都度ご相談です。
D-10	**再現条件が書かれるか**	◯	誰が・何を・どの条件で、を1行で書きます。再現手順は開発者がそのまま追えるように書きます。
D-11	**未検証の範囲を明記するか**	◯	確かめた操作と、確かめていない範囲を分けて書きます。「安全」の総合判定はしません。
D-12	**取引先にそのまま出せる粒度か**	◯	取引先のチェックシートの設問番号に対応づけて添付できる粒度で書きます。
E-13	**担当者の経験と体制を説明できるか**	△	少人数の体制です。誰が何を判断するか、担当の経験は初回相談でお伝えします。
E-14	**費用に含まれるものが明細で分かるか**	◯	見積りに、検証・修正案・再検証・報告会の有無と範囲を明細で書きます。初回は合計40時間の枠です。
E-15	**実績を確認できるか**	△	導入企業名は公開していません。代わりに、報告書のサンプルと範囲・情報の扱いの合意書の案を事前にお見せします。

シートを持って、3社に同じ質問を。

どの候補にも同じ15問を送ると、答え方の違いがそのまま進め方の違いになります。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。Securiy の回答は P.06 のとおりです。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

※ 本資料は選定の観点を整理したものです。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

このシートをお持ちください。△の3項目の現状と、初回に検証する2操作・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

課題編「AI攻撃時代のセキュリティ対策のススメ」

自社で回すと何が止まるか、外に出すときの4つの確認はこちら。