

予算は？体制は？

DX推進で後回しにできない

Web診断のはじめ方

あらたな答えを、つぎつぎと。

変化の激しいサイバーセキュリティの世界。

私たちは、未知の課題が生まれるたび、培った知見と経験・実績をもとに、
「あらたな答え」を世の中に提供し続けていきます。

世界も驚くような、技術の力で。

そして、サイバーセキュリティの進化を通して、
人は、人にしかできない、創造性を活かした仕事に注力できる、
社会の進化にも貢献していきます。

誰でも簡単に

プロさながらの高度な
脆弱性診断を



予算は？体制は？

DX推進で後回しにできない

Web診断のはじめ方

| DXの進展でセキュリティ対策の需要は高まっている



デジタルサービスの開発・提供
自社で管理すべきデジタル資産

増

×

急速な技術の進化

||

必要なセキュリティ対策の

対応範囲は
拡大

難易度は
上昇

「セキュリティちゃんとしておいて」と言われても…



何をどこまでやればいいか
わからない

外注まかせで提案が最適か
判断できていない

診断のたびにコストがかさみ
継続が難しい



結果を受け取っても
どこまで修正すべきか迷う

本来の業務に追われ
対応が後回しになっている

正解が見えないまま、手探りで進めざるを得ない状況になっていませんか？

なぜ今、脆弱性診断が「不可欠」とされているのか？

Webアプリケーションに潜む『セキュリティ上の欠陥』を突いた攻撃が、深刻なビジネスリスクとなっています。

重要情報の漏洩

クレジットカード情報や
個人情報、社外秘データの
外部流出

改ざん・データ破壊

Webサイトの書き換えや
データベース内の
重要データの消失・損壊

マルウェアの踏み台

サイト閲覧者への感染、
他社攻撃の「加害拠点」
としての悪用

なりすまし

盗まれた認証情報による
意図しない操作や
決済の実行

DXの加速や開発スピードの向上により、脆弱性の混入リスクはかつてないほど増大

被害に遭えば、サービス停止や信用の失墜、多額の経済的損失は避けられません

診断方法を整理する「2つの軸」

自社に合った方法を見極めるために、まずは代表的な手法の全体像を整理してみます。

Who

誰がやるか

外部委託

プロへ依頼



内製化

自社で実施

How

どうやるか

手動診断

人の目で深くチェック



自動診断

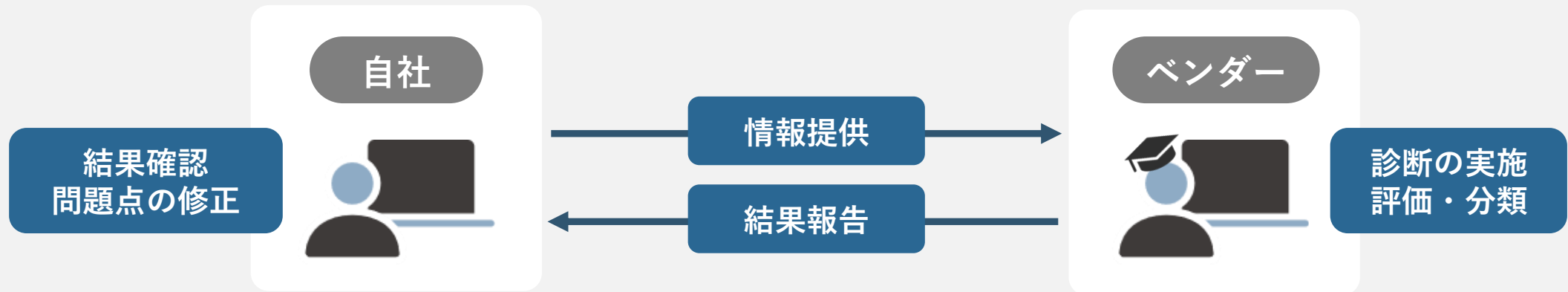
ツールで素早くスキャン

| かつての「正解」は、この組み合わせでした

外部委託
プロへ依頼

+

手動診断
人の目で深くチェック



理由

「開発工程そのものが外注」 「第三者診断が必須要件」 「高度な専門性が要求される領域」

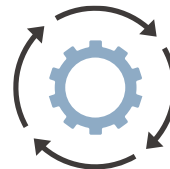
「外部委託100%」モデルは、いま限界を迎えています

セキュリティ人材や 予算の不足



採用・育成は難易度が上昇し
外注先でも同じくリソース不足で
診断できない／リリースできない

アジャイル開発 (開発の高速化)



従来型の診断フロー・期間では
2～4週間のリリースサイクルに
柔軟に対応できない

ローコード開発 (コモディティ化)



PaaS/IaaS/SaaSの普及により
開発のハードルが下がったことで
診断対象サイトが急増している

診断対象・診断回数が増え、外部診断だけでは到底カバーできない

| 高品質ゆえの「小回りの利かなさ」がボトルネックに

委託先との連携に
余計な工数がかかる



診断タイミングを
柔軟に調整できない



追加の依頼ができず
リスクを潰しきれない



無理して続けると、調整工数ばかり増えて
肝心のリスクが残ってしまう…

IPAからも脆弱性診断内製化ガイドが公開されています

※独立行政法人情報処理推進機構

公開の背景

脆弱性の早期発見が ますます重要に

- ・ 事業継続
- ・ 信頼性維持の観点



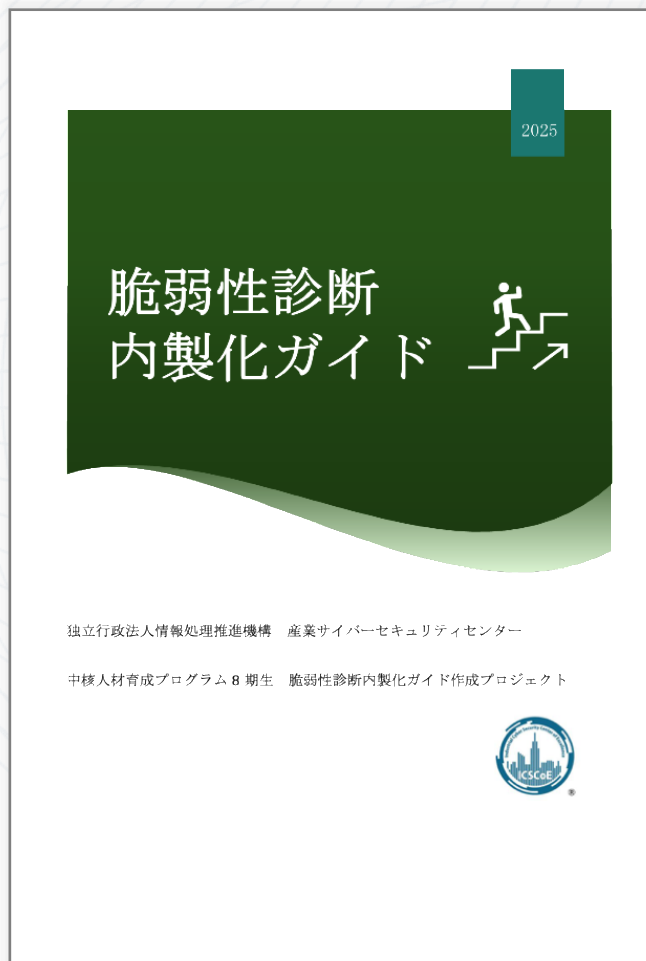
内製化への関心が高まっている

- ・ 新たな脆弱性の増加
- ・ リリースサイクルの高速化



主な内容

- ・ 外部発注と内製の違い
- ・ 内製化に必要な組織体制と人材
- ・ 内製化の進め方と継続的改善プロセス
- ・ 関係組織との連携とセキュリティ意識の醸成
- ・ ツール選定におけるポイント



自社に最適な「診断スタイル」を見極めるための比較表

診断方法	特徴	方法	メリット	課題
外部委託	専門業者に依頼	手動診断が多いが 直近では自動診断も登場	専門性が高く高精度 多くの場合「人の目」で チェックが入っている	相対的にコストが高く 各種調整の負担が大きい
内製化（自社実施）	社内セキュリティ部門や 開発チームが診断	脆弱性診断ツールを 利用することが多い	低コストかつ 柔軟な対応が可能 ノウハウも蓄積される	一定レベルの社内人材や 業務フロー/ルールが必要
ハイブリッド	一部を外部委託するが 残りは自社で診断する	複数手法を組み合わせる	外部の専門性と 内製の機動力を両立	方法の混在によって 管理工数が増加しやすい

「外部委託か内製化か」の二択ではなく、
両者の強みを活かす“ハイブリッド型”という選択肢が、いま注目されています

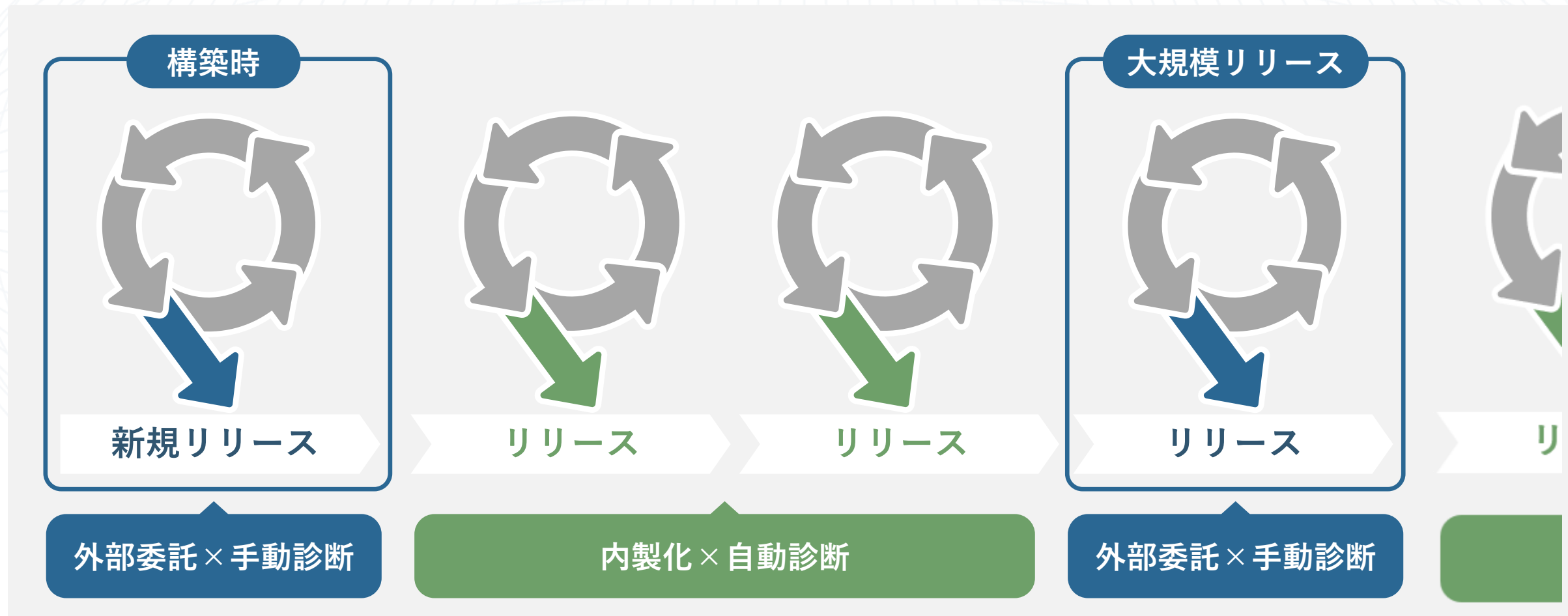
重視する「優先順位」で決まる、3つの選択肢

「品質」「速度」「コスト」のどこに重心を置くかによって、目指すべきスタイルは明確になります。



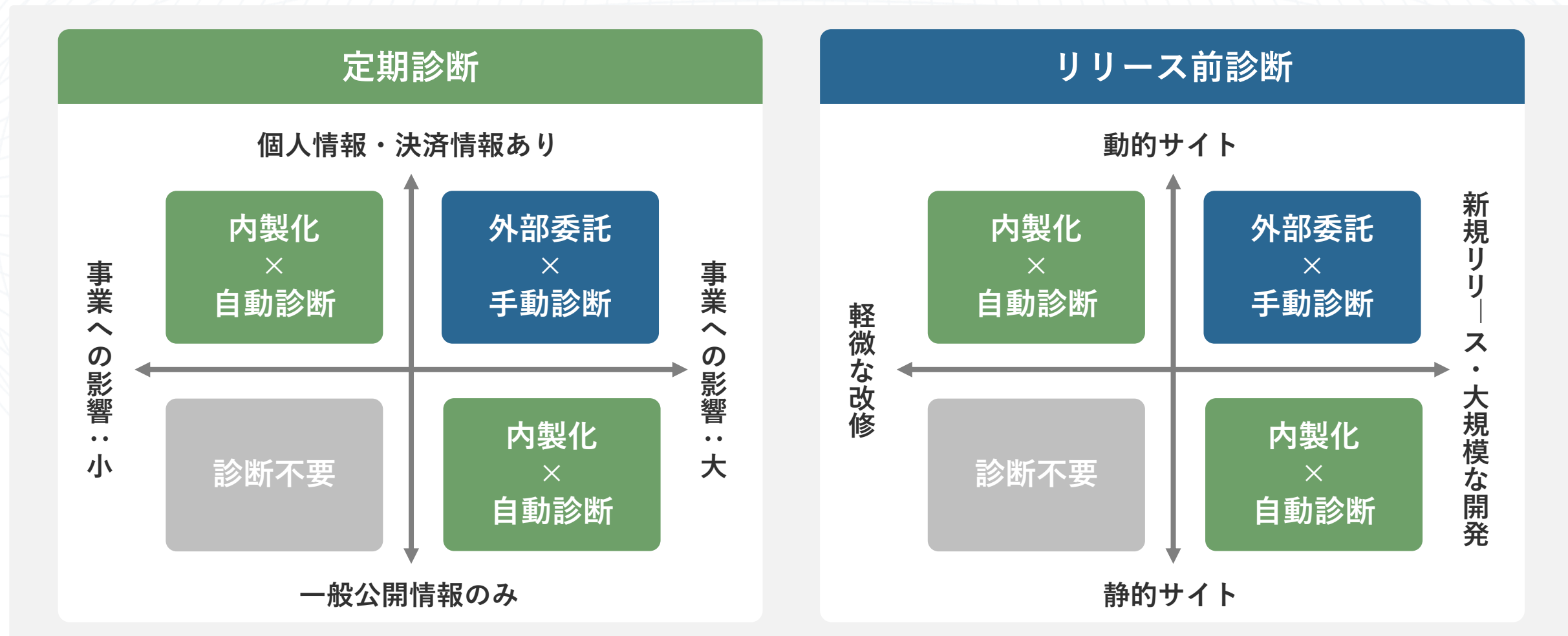
開発サイクルと診断手法の連動イメージ

リリースの規模やタイミングに応じて、外部委託と内製化を使い分ける、実務的な運用モデルをご紹介します。



「定期」と「リリース前」で異なる判断軸

一律にせず、「定期的なリスク確認」と「リリース前の安全検証」で判断の軸を切り分けることがポイントです。



「ハイブリッド診断」を取り入れるための検討項目

守るべき対象の特性と開発現場の実情を掛け合わせることで、無理なく継続できる診断体制が定義されます。

診断対象サイトの重要度

- 取り扱っている情報の重要度
- ビジネス上・業務上の重要度
- 監督官庁・業界団体ガイドライン
- リリース・アップデート頻度



開発内容・体制・タイミング

- 大規模な開発 or 軽微な修正
- 外部ベンダーが開発 or 内製開発
- 部分的に診断 or 全体を診断
- リリース前の診断 or 定期診断

カプコン 様の事例

高頻度な診断を、現場主体で「当たり前」に。

診断スタイル： **ハイブリッド**

(外部ベンダーによる手動診断と、AeyeScanによる自動診断を使い分け)



技術者以外のメンバーでも操作できる診断ツールを活用し、開発現場が主体となって高頻度に診断を実施。工数を抑えながら、セキュリティを開発の一部として根付かせることを目指している。

このスタイルが
マッチするケース

- 開発プロセスにセキュリティ診断を組み込みたい
- 外注コストを抑えつつ、診断のスピードと頻度を上げたい
- 個人情報や決済処理のある社外向けサイトを運営している

詳細はこちら⇒

<https://www.aeyescan.jp/case/capcom/>

NTT東日本 様の事例

リリースサイクルを緩めず、セキュリティを強化

診断スタイル： **ハイブリッド**

（AeyeScanによるリリース前の診断と、外部委託による年1回の定期診断）



開発を内製に移行したタイミングで採用したアジャイル開発のスピードを維持するため、脆弱性診断の内製化を決意。リリース前に自分たちで診断を行うことで、リリースを止めることなく、セキュリティも担保できる体制を構築した。

このスタイルが
マッチするケース

- リリース前の診断を必須にしてセキュリティを強化したい
- 一方、開発サイクル・スピードは落とせない
- 診断については、品質とコストのバランスを重視したい

詳細はこちら⇒

<https://www.aeyescan.jp/case/ntt-east/>

とはいえ、診断の内製化ってどうやるの・・・？

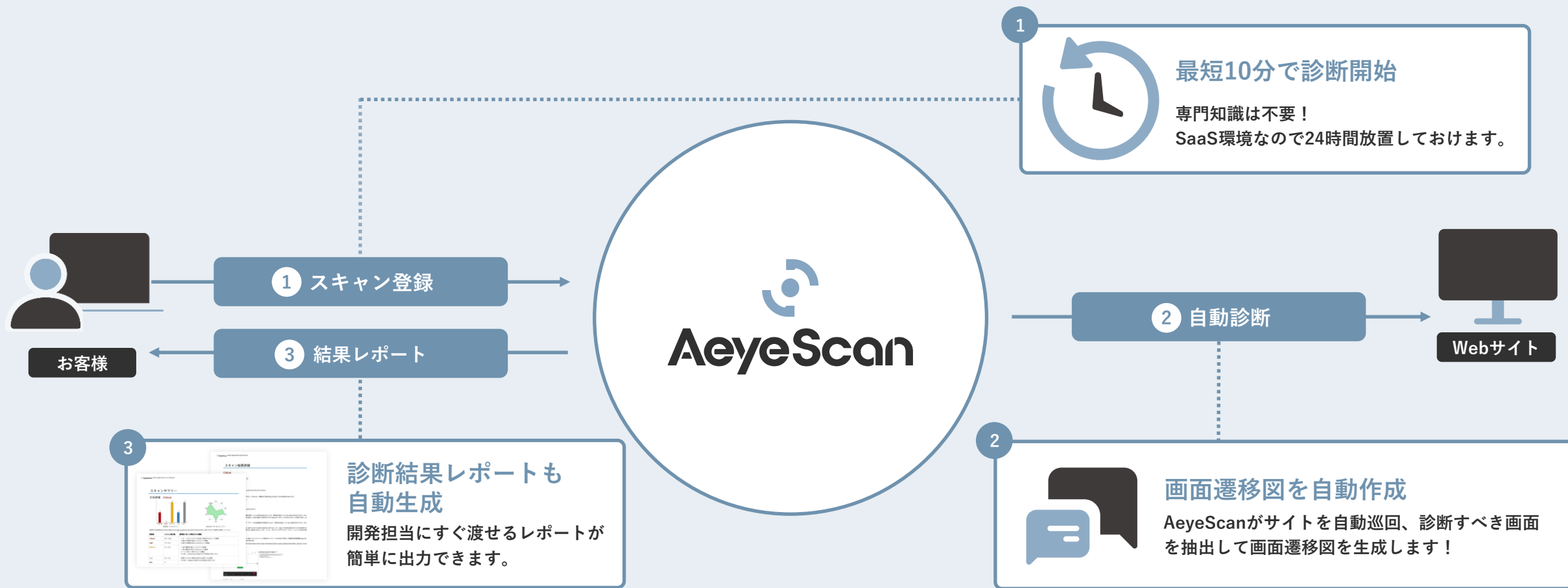
具体的に、診断内製化に踏み出そうとしたとき、課題になりやすいのは「人材」「知識不足」「管理工数」です。

診断方法	特徴	方法	メリット	課題
外部委託	専門業者に依頼	手動診断が多いが 直近では自動診断も登場	専門性が高く高精度 多くの場合「人の目」で チェックが入っている	相対的にコストが高く 各種調整の負担が大きい
内製化（自社実施）	社内セキュリティ部門や 開発チームが診断	脆弱性診断ツールを 利用することが多い	低コストかつ 柔軟な対応が可能 ノウハウも蓄積される	一定レベルの社内人材や 業務フロー/ルールが必要
ハイブリッド	一部を外部委託するが 残りは自社で診断する	複数手法を組み合わせる	外部の専門性と 内製の機動力を両立	方法の混在によって 管理工数が増加しやすい

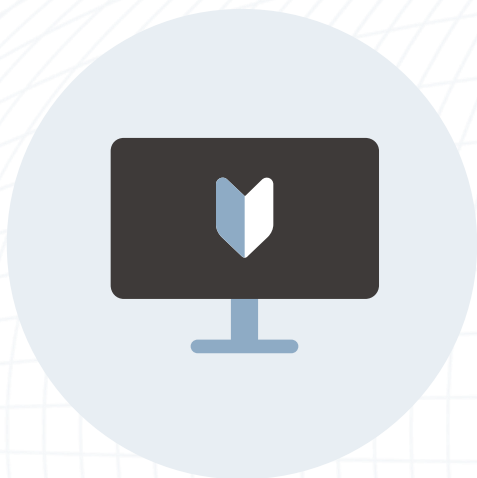
それを解決するのが **AeyeScan** です！

| AeyeScanとは？

AI・RPA活用により、脆弱性診断を自動化するクラウド型Webアプリケーション診断ツールです。



| AeyeScanが選ばれている理由



誰でもかんたん操作



開発やセキュリティの知識がなくても、
トレーニングなしで診断可能。



AIによる自動診断



圧倒的な巡回精度で
24時間自動で診断。
画面遷移図で状況を可視化。



わかりやすいレポート



各種ガイドラインに準拠した
プロ仕様のレポート出力、
日本語と英語に対応。

【簡単＆自動】サイト巡回 → 画面遷移図 → 診断＆レポート作成

画面遷移図

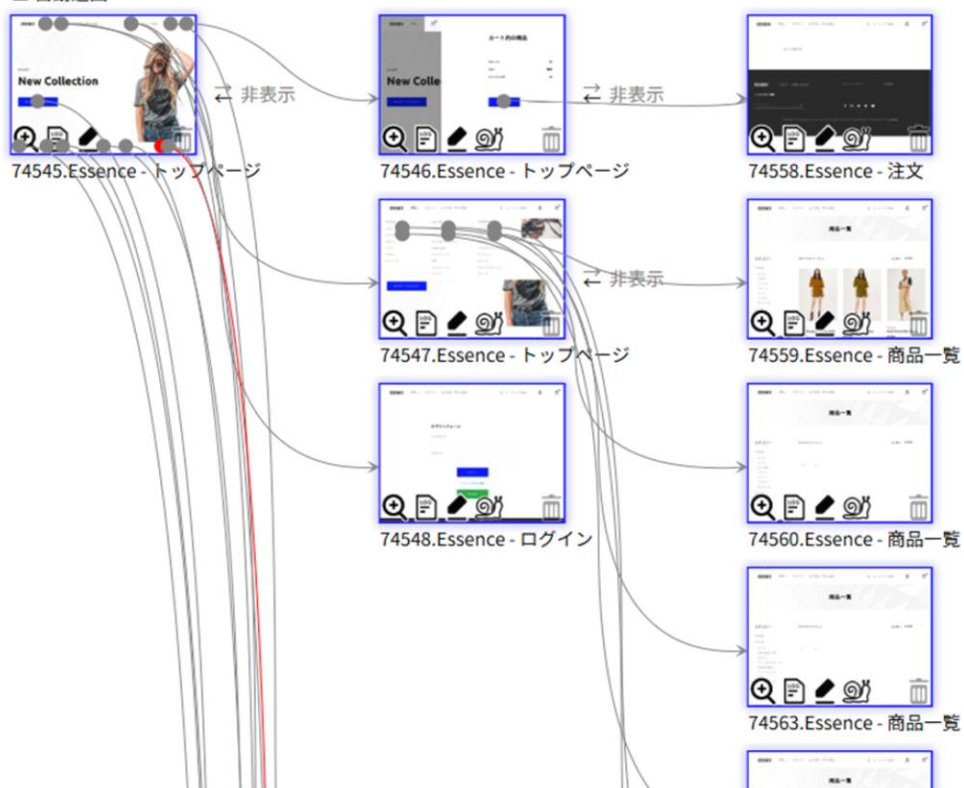
画面数: 86 (スキャン対象: 86)

ダウンロード

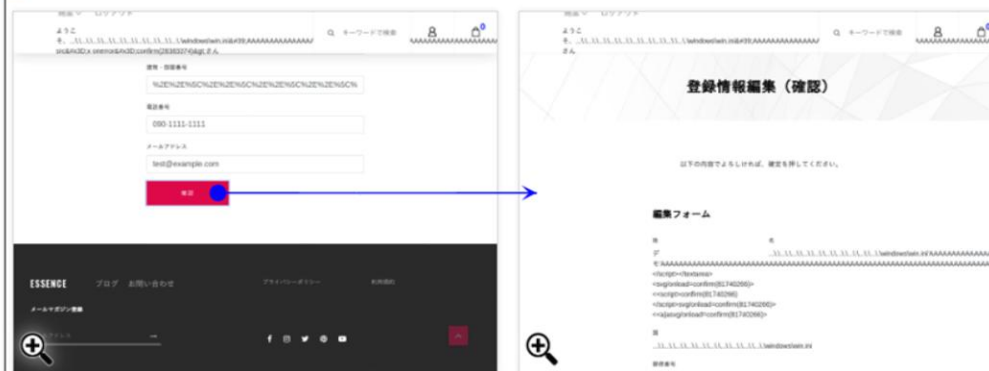
全てを展開

凡例: ⓘ

■ 自動巡回



スクリーンショット



パラメータ情報

タイプ:	POSTパラメータ
パラメータ名:	last_name
正常パラメータ値:	%E3%83%87%E3%83%A2
検知時パラメータ値:	%E3%83%87%E3%83%A2"></script></textarea><svg/onload=confirm(81740266)><<script>confirm(81740266)</script>svg/onload=confirm(81740266)><<a svg/onload=confirm(81740266)>

検知理由

パラメータの送信後に他のページ「Essence - 登録情報編集 (<http://demosite2.aeyescan.work:3333/my-page/user-edit>)」にアクセスしたところ、「81740266」を含んだダイアログが表示されました。

| AeyeScanが選ばれている理由

プロが認める機能・性能

×

誰でも使える操作性

さまざまな企業さまに導入いただいております

ユーザー企業

インフラ※



エンタメ



メディア



製造



金融



人材・教育



SaaS



SI・IT企業



セキュリティ企業



※公共および社会・生活基盤までを包含

社名五十音順（導入いただいた企業様の一部です）会社名及びロゴは各社の商標または登録商標です

| AeyeScanなら！



ガイドライン準拠で
「何をどこまで」が明確に

専門知識不要で
迷わず「内製化」スタート

限られた予算内で
納得感のある継続が可能に



結果から「直すべき優先度」
が分かり、迷わない

自動化で工数を削り、
本来の業務に集中できる

根拠があるから、もう迷わない。セキュリティを、チームの「自信」に変えていく

AeyeScanにご興味をお持ちいただいた方へ、 トライアルをご用意しています

トライアルとは？

「AeyeScanで自社のWebサイトを適切に診断できそうか」を検証いただくための取り組みです。

- 自動化したい箇所がうまく診断できず、導入後すぐに診断を開始できないケースがございます。
→検討初期段階であっても、まずはトライアルをお試しいただくことを推奨しています。
- トライアルでは、操作支援などのサポートも行います。
- トライアル開始に必要なのは以下の3点のみ。お気軽にお申し込みください！
 - ・ 検証するサイトの選定
 - ・ AeyeScanのIPアドレス許可設定
 - ・ 問診表のご一読と社内周知

AeyeScanの導入を検討してみませんか？

操作性の確認、実際に利用してみたい方へ

AeyeScan の 無料トライアル

トライアルにかかる費用は不要。実際の操作性はどうか？
またどのように脆弱性が発見されるのか？
などの疑問は無料トライアルで解消しましょう。

無料トライアルの申し込み



お見積りの希望・導入をご検討している方へ

AeyeScan への お問い合わせ

お見積りの希望・導入をご検討してくださっている方は
お問い合わせフォームよりご連絡ください。
当日もしくは遅くとも翌営業日にはご連絡を差し上げます。

お問い合わせフォーム



＼8月 | 納涼ビアバッシュイベントを開催します／

ビール片手に、Webセキュリティの“リアルな悩み”を共有しませんか？

納涼ビアセキュ

参加無料

操作体験もOK!

～ビール片手にカジュアルに語る、Webセキュリティ交流会～

8.26 WED

KANDA SQUARE 11F WeWork
〒101-0054 東京都千代田区神田錦町二丁目2番地1

株式会社エーアイセキュリティラボ
事業企画ディレクター 阿部 一真

株式会社エーアイセキュリティラボ
CX本部プリセールスリーダー 高橋 貴弘

AeyeScan

お悩み解決のヒントが得られる
トークセッションも!

エーアイセキュリティラボ初の試みとして、
Webセキュリティに関する課題や疑問を持つ皆さまが
集まり、冷たいビールやドリンクを片手にカジュアルに
語り合う情報交換会「BeerBash」を開催します！

お申し込みはこちら



スマートフォンからも
お申込みいただけます



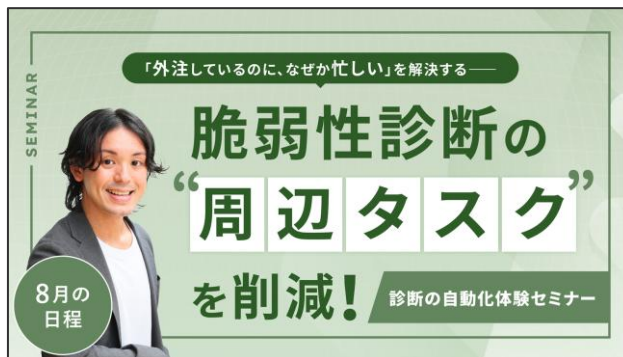
定期開催中！

AeyeScanがよく分かるデモ動画・セミナー

AeyeScanを
検討してみたい方へ

AeyeScanがどんなものか知りたい方に、
デモを交えてわかりやすくご紹介。
まずは気軽に使い勝手をチェック！

デミセミナーの日程を確認

AeyeScanの操作を
体験してみたい方へ

実際の操作を通して、一連の機能を体感。
導入前の不安や疑問をまるごと解消。
“わからないまま”をなくすセミナーです。

ハンスオンセミナーの日程を確認

セキュリティ対策に
お悩みの方へ

最新の事例や対策ノウハウをテーマ別に紹介。
月替わりで学べる無料ウェビナーを開催中。
お気軽にご視聴いただけます！

ウェビナーの日程を確認





AeyeScan

セキュリティに、確かな答えを。