専門家ゼロでもできるシフトレフト

AIで回す 脆弱性診断

「実践」ロードマップ

登壇者紹介

株式会社エーアイセキュリティラボ

執行役員兼CX本部長　**関根 鉄平**　CISSP

発売中

セキュリティエンジニアとして大手金融機関等の脆弱性診断に従事。その後、Webアプリケーション検査ツール・サポートチームの立ち上げをしつつ、CSIRTや開発現場でのセキュリティを推進。
2020年6月より現職。AeyeScanのカスタマーサクセスチームの責任者として脆弱性診断の内製化を支援。大規模イベントや大手企業での講演に多数登壇している。
『セキュリティエンジニアの知識地図』を共著。

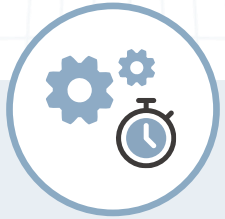
コミュニティ活動など

- 日本セキュリティオペレーション事業者協議会（ISOG-J）、OWASP Japan 共同ワーキンググループ
- 公益社団法人日本通信販売協会（JADMA）Web・セキュリティ専門部会
- 情報セキュリティ10大脅威 選考会メンバー

新体制がスタートする4月、こんな状況になっていませんか？

4月特有の教育コスト

引き継ぎや
オンボーディングで
手一杯に



新体制による加速の歪み

開発の手は増えても
レビュー・テストが
追い付かない

異動で浮彫になる属人化

有識者の不在で
仕様確認や意思決定が
ストップ

品質は落とせないが、これ以上やることは増やしたくない

こうした課題の解決策として広がるキーワード

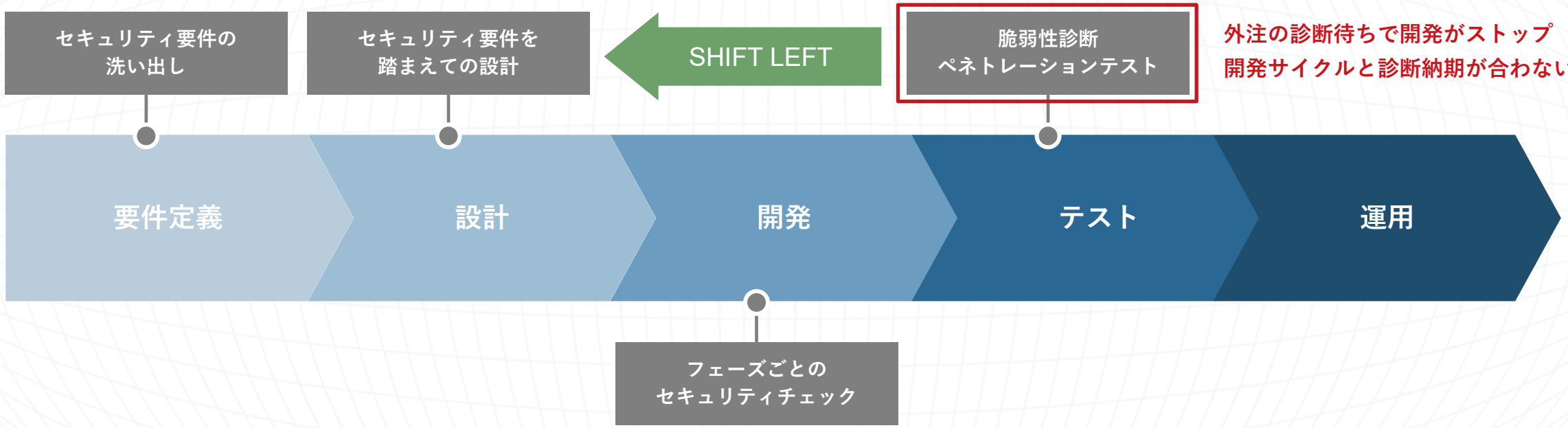
- シフトレフト
- DevSecOps
- 内製化
- セキュリティの自走化

コスト・スピード・リリース頻度の増加を鑑みると

いま開発現場が生き残るための**必須のアプローチ**と言える

診断外注のままシフトレフトを目指す限界

問題を早期発見・修正することで手戻りが減り、スピードアップと品質向上を両立できるはずが…



診断外注のスタイルのままシフトレフトすると

“コスト”と“リードタイム”の壁に突き当たる

かといって、内製化を目指すと――

難しすぎる

ツールの設定が複雑
レポートや用語が読み解けない

理解コストが高い…

判断を迫られる

誤検知が混じる
優先度の基準が曖昧

どこまで直せばいいの…？

網羅性への不安が残る

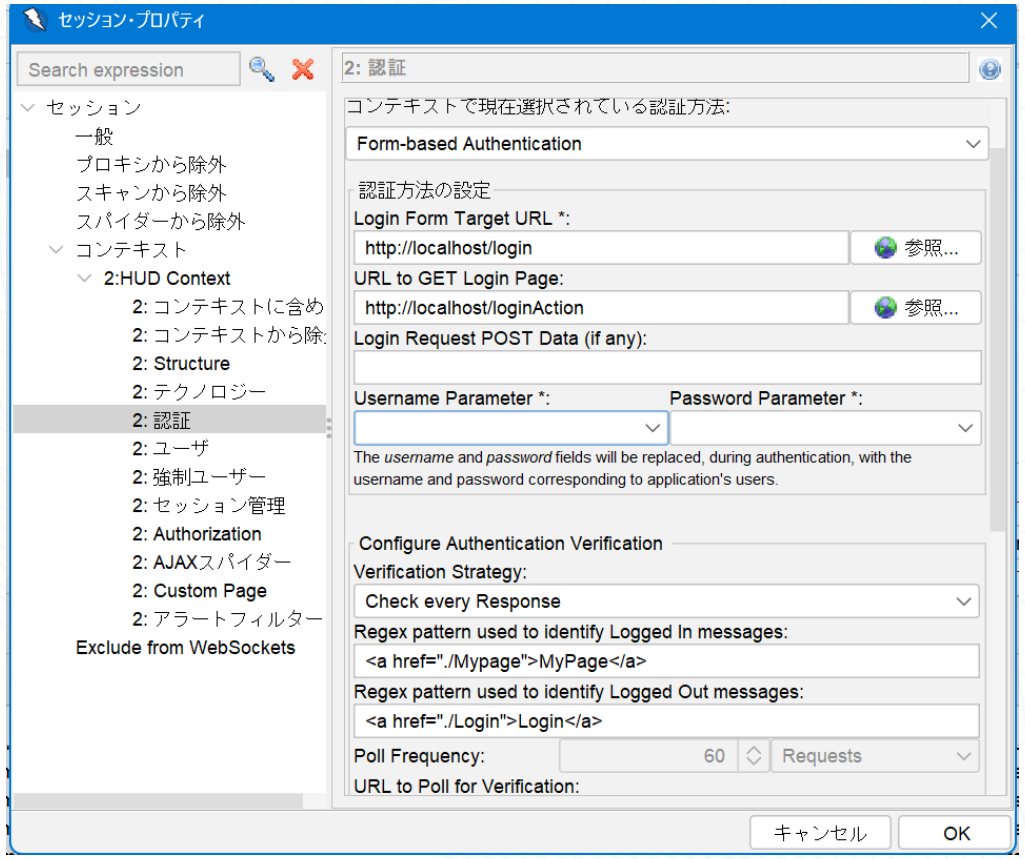
一部のガイドライン準拠のみ
最新脅威を追えているか不明

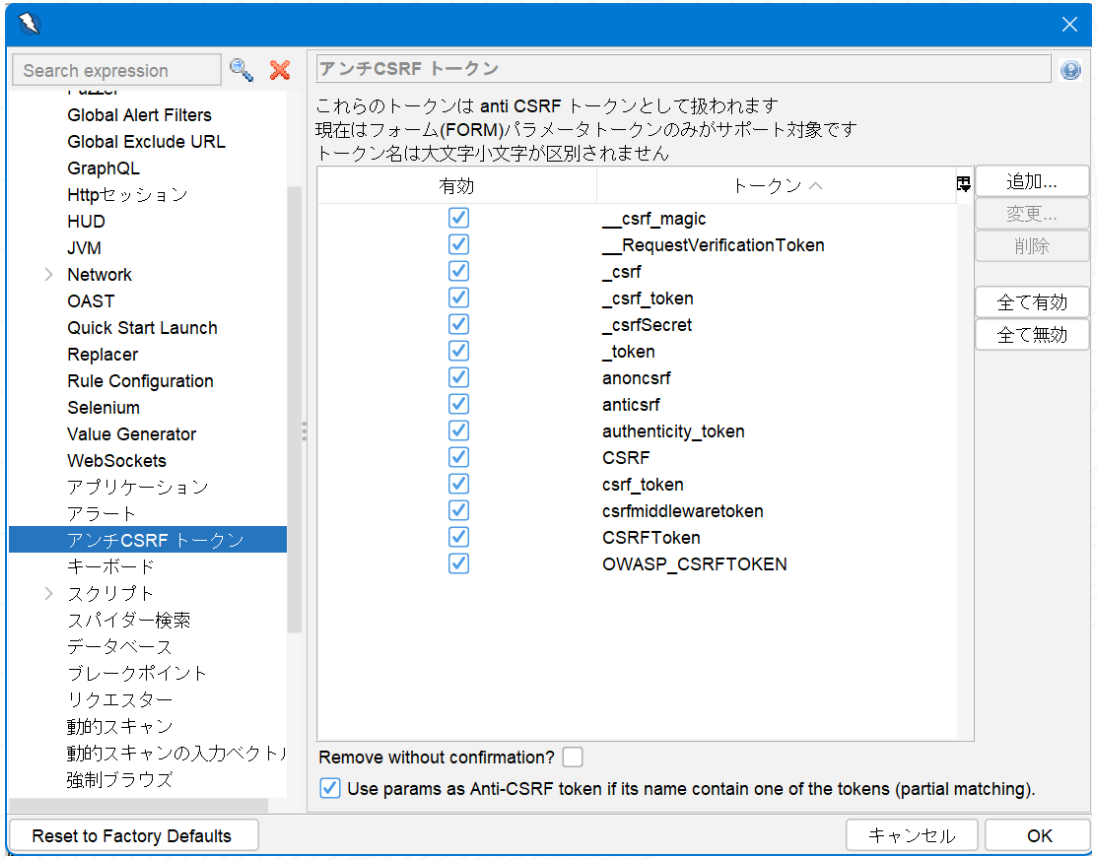
これで本当に守れている…？

世の中で語られている手法の多くは、
『セキュリティの専門知識を持ったエンジニアが潤沢にいること』を前提にしている

例えば、脆弱性診断ツールを導入し内製化しようとすると…

無料脆弱性診断ツールの一例：OWASP ZAP





無料ツールを導入しても、運用できない状態に陥りがち

とりあえず導入したが設定がわからない

マニュアルが英語…

何から直すべきかわからない

アラートが3,000件…

判断できる人に依存しボトルネックに

〇〇さん待ちで延期

いつの間にか放置状態に

誰もログインしなくなった

ツールはある。でも回らない。だから必要なのは“回る設計”

どうすれば回るか？という設計思想から生まれた診断ツールのご紹介

1

最短10分で診断開始

専門知識は不要！
SaaS環境なので24時間放置しておけます。

お客様

1 スキャン登録

3 結果レポート

AeyeScan

2 自動診断

Webサイト

3

診断結果レポートも自動生成

開発担当にすぐ渡せるレポートが簡単に出力できます。

2

画面遷移図を自動作成

AeyeScanがサイトを自動巡回、診断すべき画面を抽出して画面遷移図を生成します！

AeyeScanの設計思想

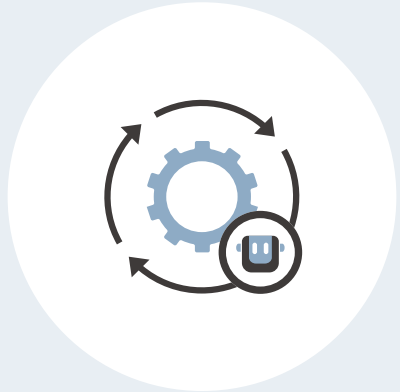
開発のついでに“診断を日常化”する仕組み

CI/CDツールと連携し
自動で診断

判断の負荷を取り除く仕組み

誰もが読み解ける
説明付きレポートで属人化解消

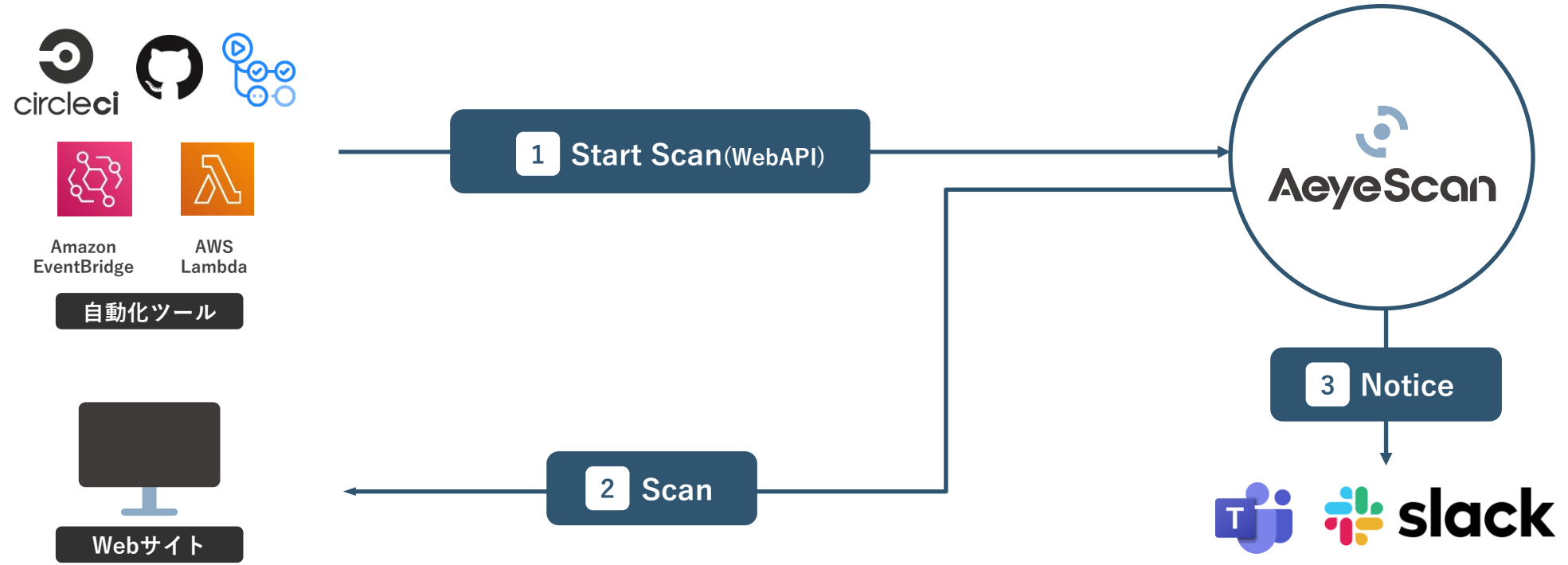
人が操作する工程の最小化



ほとんどの工程を自動化
開発者が本来の仕事に集中できる

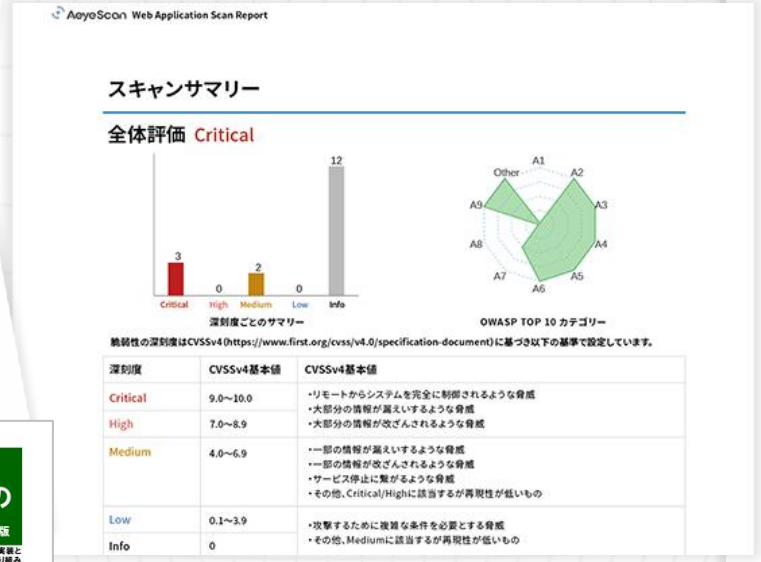
設計思想①：診断を日常化する「CI/CD連携」

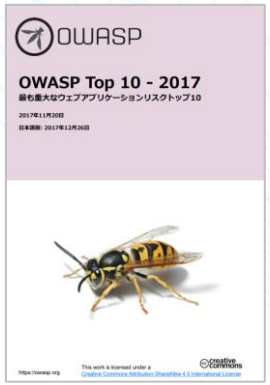
リリースのたびに手動で回す必要はありません。
有識者が不在でも、開発サイクルの中でセキュリティチェックが自動的に完結します。



設計思想②：判断負荷を取り除く「レポート」

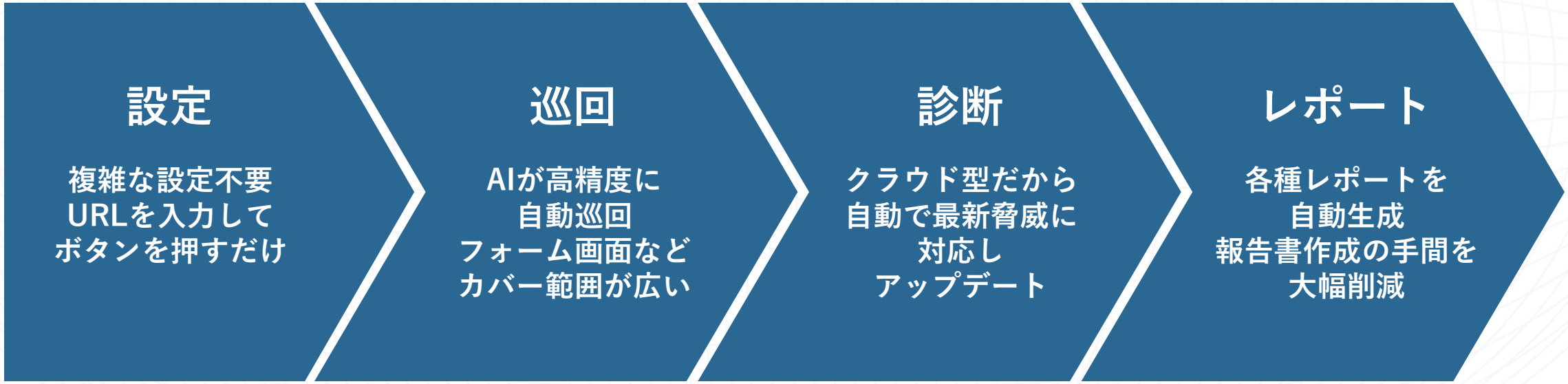
専門知識がなくても、どこをどう直すべきかが一目でわかるレポートを自動出力。
ガイドラインに紐づいた根拠のある説明付きで、属人化を解消します。





設計思想③：現場工数を最小化する「診断工程の自動化」

設定から巡回・診断・レポート出力まで、人手が必要だった工程を自動化で置き換え。
複雑なマニュアル作成や教育は不要で、新任担当者の方でも即日診断を開始できます。



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※

EPARK / AIRE / HIS / H2O RETAILING / NTT EAST / odakyu / 近鉄情報システム株式会社 / GEO / SymEnergy / 水ing / Suzuyo / TOYOTA HOME / NANKAI / 日本調剤 / JARMeC / HITOWA GROUP / BOOK・OFF / ベルーナ / grow up together MEDIA / Looop / Loyalty Marketing, Inc.

エンタメ

イープラス / CAPCOM / GungHo Online Entertainment, Inc. / とらラボ! / BookLive

メディア

集英社 / 中日新聞 / 東海テレビ / NIKKEI / Media Do

製造

AICA / AISIN / KITZ / KOSÉ / SAKI / TIGER / TEIJIN / Denkei / House / Mizuno / ユーグレナ

金融

セブン-イレブン / UPSIDER / MS&AD / MS&ADインターリスク総研 / JOBPAY / SOMPOひまわり生命 / DMM FinTech / Tokyo Century / Net Protections

人材・教育

OHSAWA DRIVING SCHOOL / 河合塾 / Junion / JINSOKEN / ZENKIGEN / Direct Sourcing / PERSOL / 立教大学 / Leverages / workport

SaaS

Advanced Media, Inc. / Lexica / エアトリ / M-aid / エムティーアイ / OZ INTERNATIONAL / giftee / Classi / COACH A Co.,Ltd. / cybozu / Speee / SecureNavi / Diamond head / DMM Boost / TAL / Digital Garage / TEMONA / NAVITIME / KNOCK ON THE DOOR / BATONZ / VALUE HR / freee / vector / porters / hokan / Money Forward / RUN.EDGE / RVSTA / Rescuenow

SI・IT企業

Rworks / アクモス株式会社 / AVANT GROUP / Insight Edge / Infcurion / 80&Co. / SBWorks / NTT Integration / NTT DATA / NTTビジネスソリューションズ / OMRON / Globalway / KDDI Agile Development Center / circlace / さくら情報システム / SUNDAY SYSTEMS / CEC / GA TECHNOLOGIES / Simplex Inc. / 777WORKS / SOFT CREATE / SOLTEC / 高千穂交易株式会社 / TDI / 電通総研 / TOPPAN / JOPS / JAST / PCNET / Human Interactive Technology inc. / FUJISOFT / FUJITSU / MACROMILL / MITSUBISHI ELECTRIC / YONA / リピスト / Y!

セキュリティ企業

NEC NECセキュリティ / NTT DATA / GSX / cybertrust / LAC

※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）

導入事例紹介

SOMPOひまわり
生命保険 様

企業名　SOMPOひまわり生命保険株式会社

事業内容　国内生保事業

従業員数　2,650名（2023年度末時点）

課題

外注だと手間と時間がかかり、
2週間の開発サイクルに合わせた診断が困難

具体的な課題

1. アジャイル開発のため外部委託だと契約や調整の手間、時間がかかる
2. 開発の早い段階で脆弱性対策をする「シフトレフト」を目指したい
3. 家族情報や病歴などを含む個人情報を扱うため、セキュリティ意識の底上げが必要

「健康応援企業」を目指し、アジャイル開発によりアプリ・サービスをスピーディーに提供する中、脆弱性対策が課題になっていた。外部診断ではコストや時間がかかる一方、人材育成も非現実的なため、診断ツール導入を検討することになった。

導入

他社ツールと比較検証した上で、
検知能力、操作性などを評価し選定

導入の背景

1. 他ツールと比較し、高い検知能力があると判断
2. 操作性がよく、開発チーム自ら診断できる
3. レポート内容がわかりやすい

最初にピックアップした11製品の中から、まずはDAST製品である3製品に絞ってPoCを実施。脆弱性のあるサイトを用意して検証した検知能力、操作性、機能・運用性、パフォーマンスの点でAeyeScanが優れていると判断し、導入を決定。

効果

開発者が自分たちで手軽に診断できるようになり、ガイドや勉強会と組み合わせることで
シフトレフトの考え方も浸透

具体的な効果

1. 改修などのタイミングに合わせた、月に1本程度の診断が実現
2. ボタンを押すだけで手軽に診断できると、開発者側から感謝の声が上がっている
3. シフトレフトの考え方が理解され、開発者のセキュリティ意識が向上

AeyeScanの導入とともに開発者向けのガイドを作成し、開発プロセスに無理なく取り入れていった。コストや工数・時間といった課題が解決されたことに加え、開発者のセキュリティ意識も向上。グループ会社からも導入に興味を示されている。

導入事例紹介

カプコン 様

企業名　株式会社カプコン

事業内容　ゲームコンテンツ事業

従業員数　連結 3,531名／単体 3,186名（2024年3月時点）

課題

共通アカウント管理サービスや
ゲームのプロモーションサイトなどに対し
高頻度な診断ができない状況だった

具体的な課題

1. 年々サイト数が増えており、外部ベンダーに依頼すると診断するたびにコスト・工数・時間がかかる
2. 頻度高く診断ができない

共通アカウント管理サービス「CAPCOM ID」を展開するほか、ゲームタイトルごとのプロモーションサイトが年々増え続けており、脆弱性診断のすべてを外注でまかなうにはコスト・工数・時間の観点で課題があった。

導入

技術者でなくても操作できるUI/UXと
従量課金ではない料金体系が決め手に

導入の背景

1. 技術者ではない現場メンバーも使える
2. 従量課金ではなく同一料金
3. 国産ツールのため日本語でサポートしてもらえる

現場主導の診断体制を目指す中で、誰でも使えるUI/UXであることと、FAQやドキュメント、サポートが日本語である点を評価。最適な運用ルールの策定支援など手厚いサポートにより、スムーズに運用を開始。

効果

現場主導の高頻度な診断を実現。
診断工数は1/10と大幅な削減に繋がった

具体的な効果

1. コスト・時間・工数が大幅に削減
2. 再診断にかかるコストを気にせず、気軽に実施できる
3. セキュリティリスクの低いサイトへの診断頻度も増加

AeyeScanの活用により、セキュアなWebサイト運営とコストや時間、工数の大幅な削減を実現。導入後は、外注時と同等レベルのレポート品質や、実際に巡回・診断したかどうかを画面遷移図で確認できる安心感も評価。

まとめ

重要なのは、“導入すること”ではなく
開発の中で“自然に回る仕組み”を作ること

新人や異動者でも、初日から同じ精度で
セキュリティを担保できる
属人化しない“シフトレフトが回る仕組み”を、
今期一緒に作りませんか？

＼最終週もぜひご参加ください／

詳細はこちらから

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なの？
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

セキュリティに、確かな答えを。