

開発を止めない

シフトレフト実践

－ AI時代の脆弱性診断とは

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



開発を止めない

シフトレフト実践

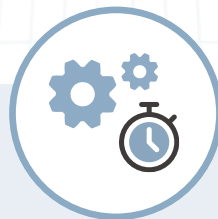
－ AI時代の脆弱性診断とは

4月の新体制スタートから数ヶ月、こんな状況になっていませんか？



新年度特有の教育コスト

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



さらに、もうすぐ夏休みを迎えるいま、
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

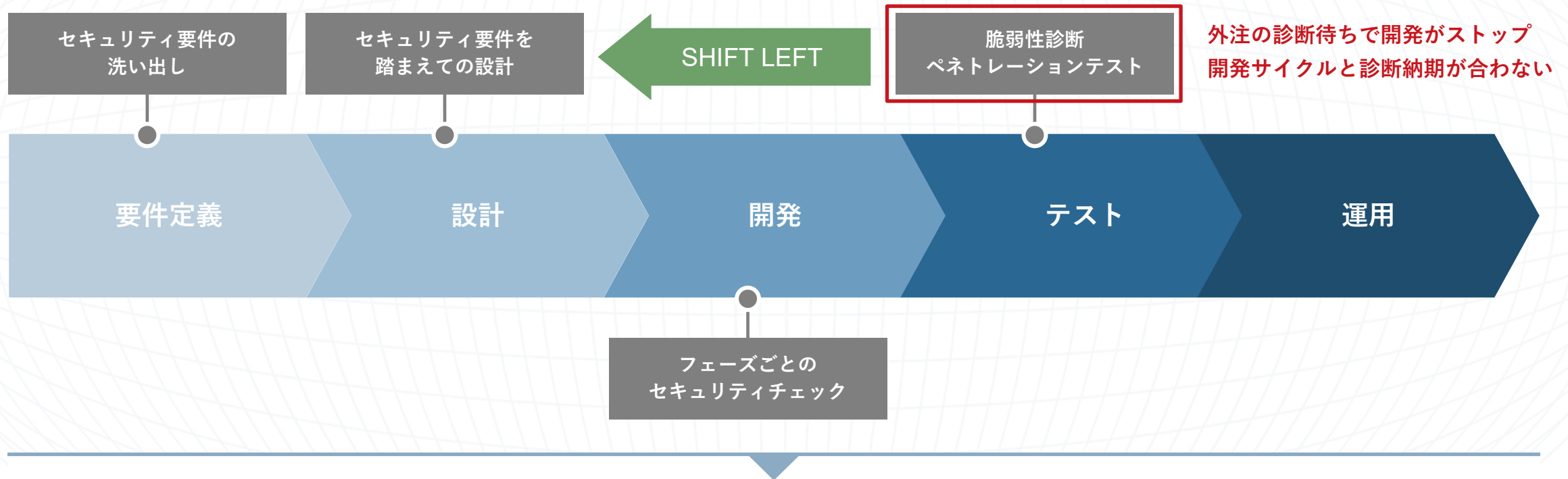
セキュリティの
自走化



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



判断を迫られる

誤検知が混じる
優先度の基準が曖昧



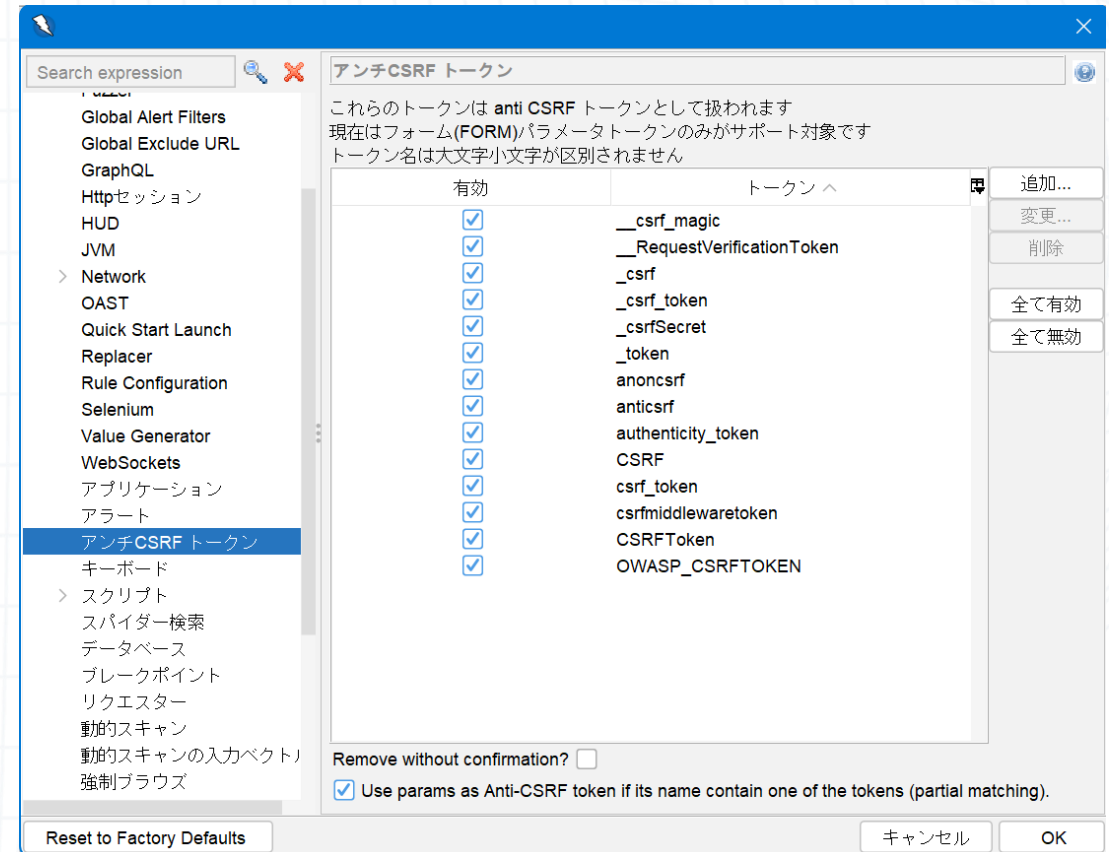
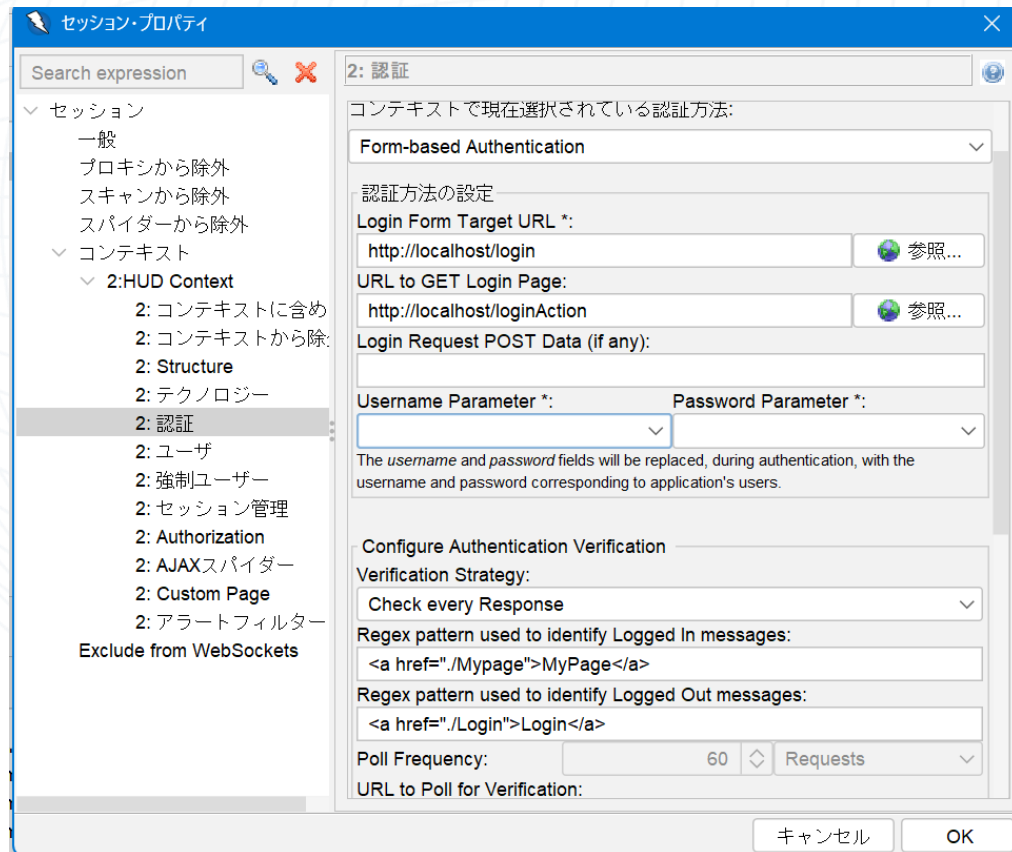
網羅性への不安が残る

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

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…

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



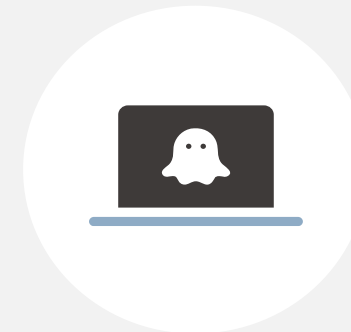
アラートが3,000件…

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

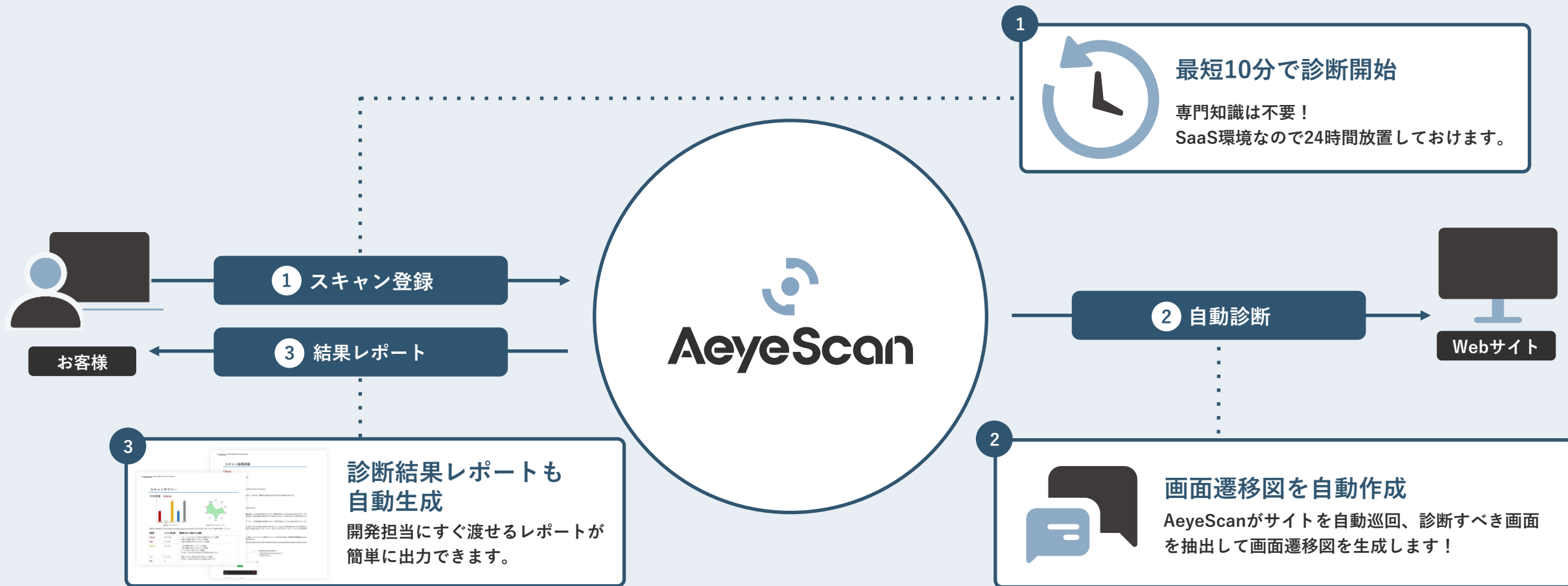
いつの間にか
放置状態に



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



| AeyeScanの設計思想

開発のついでに
“診断を日常化”する仕組み



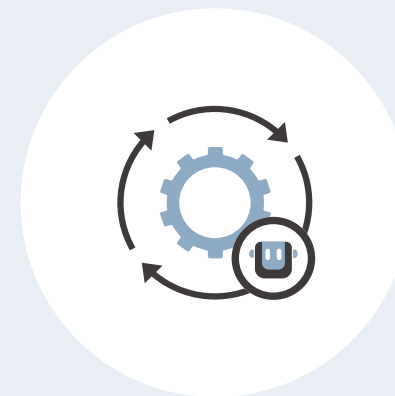
CI/CDツールと連携し
自動で診断

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

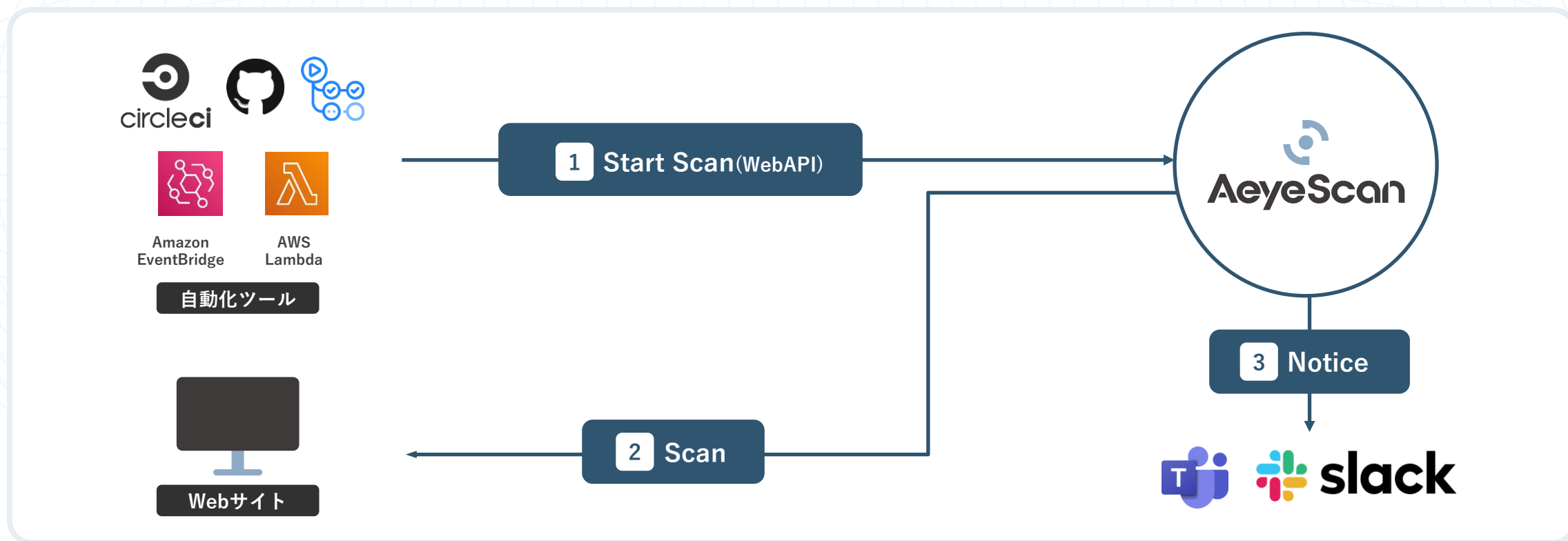


ほとんどの工程を自動化
開発者が本来の仕事に集中できる

設計思想①：診断を日常化する「CI/CD連携」

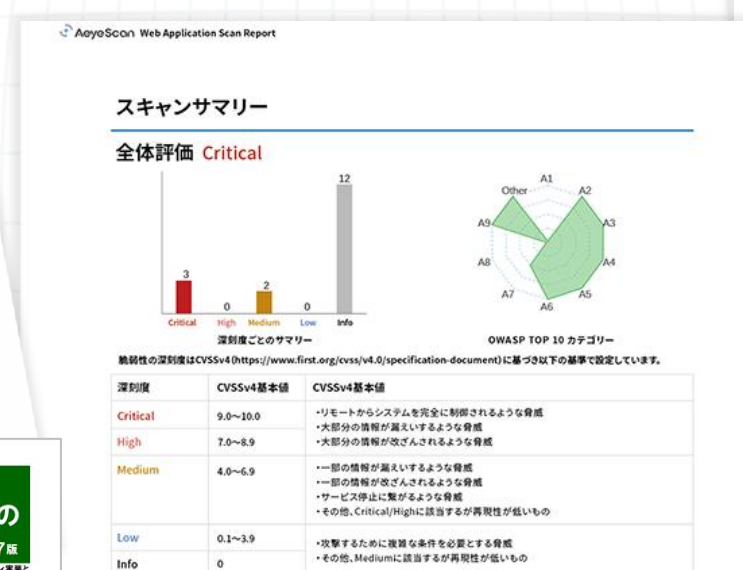
リリースのたびに手動で回す必要はありません。

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。



スキャン結果詳細

Critical

SQLインジェクション

深刻度

Critical

CVSS Score: 9.3

CVSS Vector: CVSS4.0(AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)

概要

危険な文字列をSQL文に挿入できます。そのため、攻撃者が任意のSQL文を実行できる危険性があります。

OWASP TOP 10 カテゴリー

A1:2017-インジェクション

ASVS4.0 カテゴリー

5.1.2, 5.1.3, 5.1.4, 5.3.1, 5.3.4, 5.3.5, 13.2.2, 13.3.1

解説・対策方法

SQLインジェクションとは、攻撃者が修正した入力値を送信することで、開発者の想定していないSQL文を実行できてしまう脆弱性です。この脆弱性は、利用者の送信した値が適切に前処理されずにSQL文の一部として利用されることが原因で発生します。この脆弱性を悪用することで、データベースの情報漏えいや情報改ざんなど、開発者の想定していない処理を実行されてしまう危険性があります。対策方法としては、想定していない値が入力された場合に処理を中断することや、SQL文で特殊な意味を持つ文字を無害化することが挙げられます。後者を実現する一般的な方法としては、パラメータ化クエリやプリペアドステートメントの利用が挙げられます。

参考情報

安全なウェブサイトの作り方・11 SQLインジェクション | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構 (<https://www.ipa.go.jp/security/vuln/websecurity/sql.html>)

SQL Injection Prevention - OWASP Cheat Sheet Series (https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html)

スクリーンショット



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。





脆弱性診断ツールを検討するにあたり、
こんなお悩みはありませんか？

まずは無料のものから
使ってみるべき？

どれが自分たちの
ニーズを満たしている？

正直、どれも同じに
見える…



どの脆弱性診断ツールを選べばいいんだろう…？

なぜ脆弱性診断ツールの選定は難しいの？



多様な
診断ツールが存在

数多くのツールがあるが、
専門性が高いため
違いを理解しづらい



自社のニーズとの
合致が重要

他社にとっての正解が
自社にとっての正解に
なるとは限らない



運用を見据えた
選定が必要

せっかく導入しても、
運用に負荷がかかると
導入効果は損なわれる

コストを抑えて導入しても、実際に運用するといくつかの課題が…

コスト優先でツールを導入した際に起こりがちな課題

✓
コスト



操作性
(工数)

- ・ 設定や準備に時間がかかる
- ・ レポートに手間がかかる



診断項目

ガイドラインに準拠するため
ツールごとの差は少ないが、
自社の基準を満たしているか
確認が必要



精度
(誤検知の少なさ)

- ・ 過検知や誤検知が発生
- ・ 重複巡回が発生

最も注目したいのは「操作性(工数)」と「精度(誤検知の少なさ)」

| 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

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？

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
CX本部プリセールスリーダー 高橋貴弘

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

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



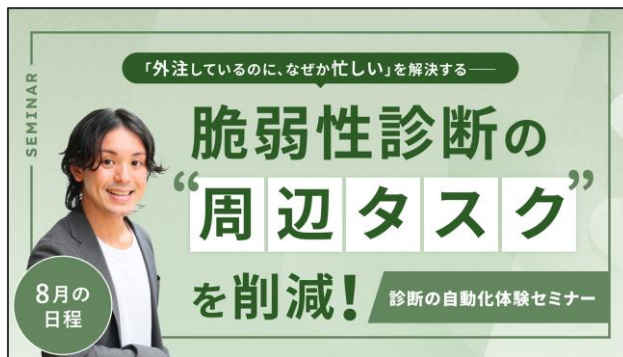
定期開催中！

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。