



Androidアプリ診断 徹底解説

Web, API, モバイルの診断を1プラットフォームで

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 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、CSIRTや開発現場でのセキュリティ推進を経て、2020年6月より現職。
AeyeScanカスタマーサクセス責任者として診断の内製化を支援し、2026年度より開発責任者に就任。顧客の声を反映したプロダクトの進化を牽引している。大規模イベント等の講演多数。『セキュリティエンジニアの知識地図』共著。

コミュニティ活動など

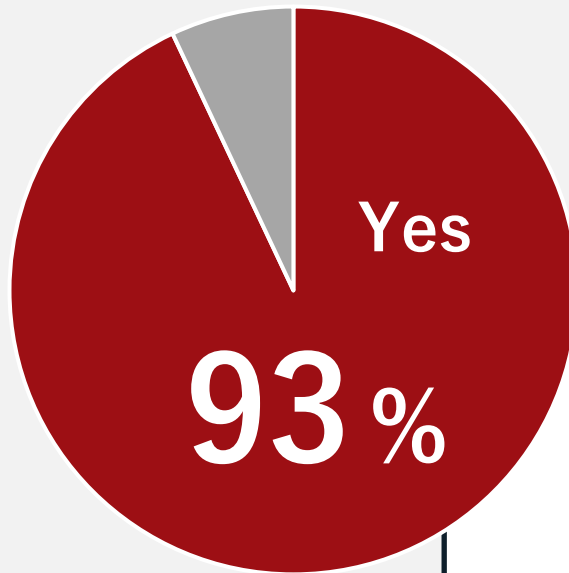
- 日本セキュリティオペレーション事業者協議会（ISOG-J）、OWASP Japan 共同ワーキンググループ
- 公益社団法人日本通信販売協会（JADMA）Web・セキュリティ専門部会
- 情報セキュリティ10大脅威 選考会メンバー

**モバイルアプリのセキュリティ
今のままで大丈夫ですか？**

大丈夫と思っていても、実は危ない

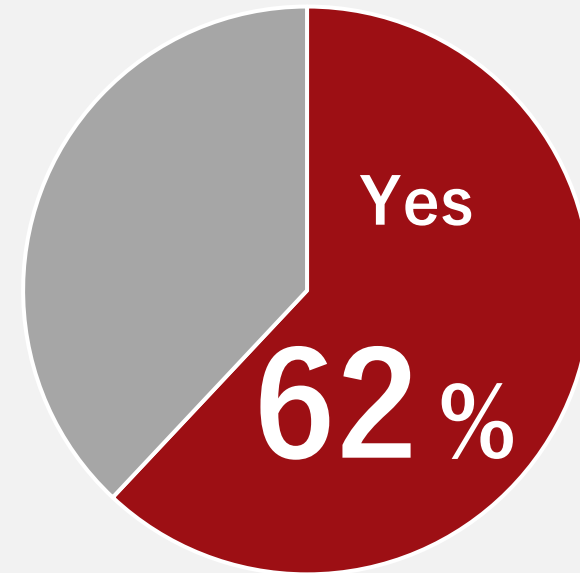
Guardsquare社の調査

自社のモバイルアプリ関連の
セキュリティ対策に自信がある



97%はモバイルアプリの
最新セキュリティポリシーを
定めていた

過去1年にモバイルアプリ関連の
インシデントを経験したことがある



実際に脆弱性が発覚した事例

2025年11月 大手放送局提供の動画配信アプリ

脆弱性	ハードコードされた暗号鍵の使用 (CVE-2025-64304)
状況	アプリ内に暗号鍵が直接書き込まれた状態で配布
リスク	第三者に暗号鍵を取得され、本来保護されるべき情報が解読される可能性

2026年5月 大手通信キャリア提供のフィルタリングアプリ

脆弱性	重要情報の平文送信 (CVE-2026-41281)
状況	通信の一部がHTTPSによって暗号化されず、未保護のまま送信
リスク	中間者攻撃によって、通信内容の盗聴や改ざんが行われる可能性

2025年7月 スマートホームデバイス用アプリ

脆弱性	ログファイルへの機微な情報の出力 (CVE-2025-53649)
状況	パスワード等の重要情報が、端末内の動作ログに含まれている
リスク	ログファイルを取得された場合、パスワード等の機微情報が漏えいする可能性

2026年5月 大手外食チェーン公式アプリ

脆弱性	プッシュ通知に関する通信における証明書検証不備 (CVE-2026-41872)
状況	通信先サーバの証明書検証が適切に行われていない
リスク	悪意ある第三者によって偽サーバへ誘導され、認証情報等が窃取される可能性

| モバイルアプリのセキュリティ対策の実態

セキュア設計・開発 (コードレビュー、SAST)

作る段階で
安全にする



ガイドラインやレビュー文化
があり比較的实施されている

通信・認証の検証 (API通信/トークン管理)

動かしたときの挙動を
確認する



一部に留まり網羅的に
検証されているケースは少ない

実環境での検証 (動的テスト)

実際の利用環境を
想定して検証する



Webほど
標準化・普及していない

対策の抜け漏れがあると、どうなるのか…？

**アプリが
解析される**



API使用や内部ロジックが
解析される

**通信が
観測・改ざんされる**



正規アプリを装った
不正リクエストが成立する

**トークンが
抜かれる**



セッションを使いまわされ
なりすましが成立する



「解析・改ざん・奪取」の成立は、実被害の直接的な原因に

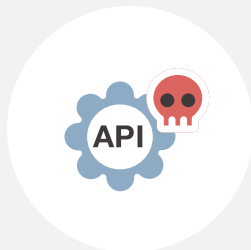
さまざまな甚大なリスクが起こりうる

アプリが
解析される



不正API利用

本来想定していない操作
(ポイント不正取得など)



通信が観測・改ざん
される



認証バイパス

ログインせずに機能を
利用・権限昇格



トークンが
抜かれる

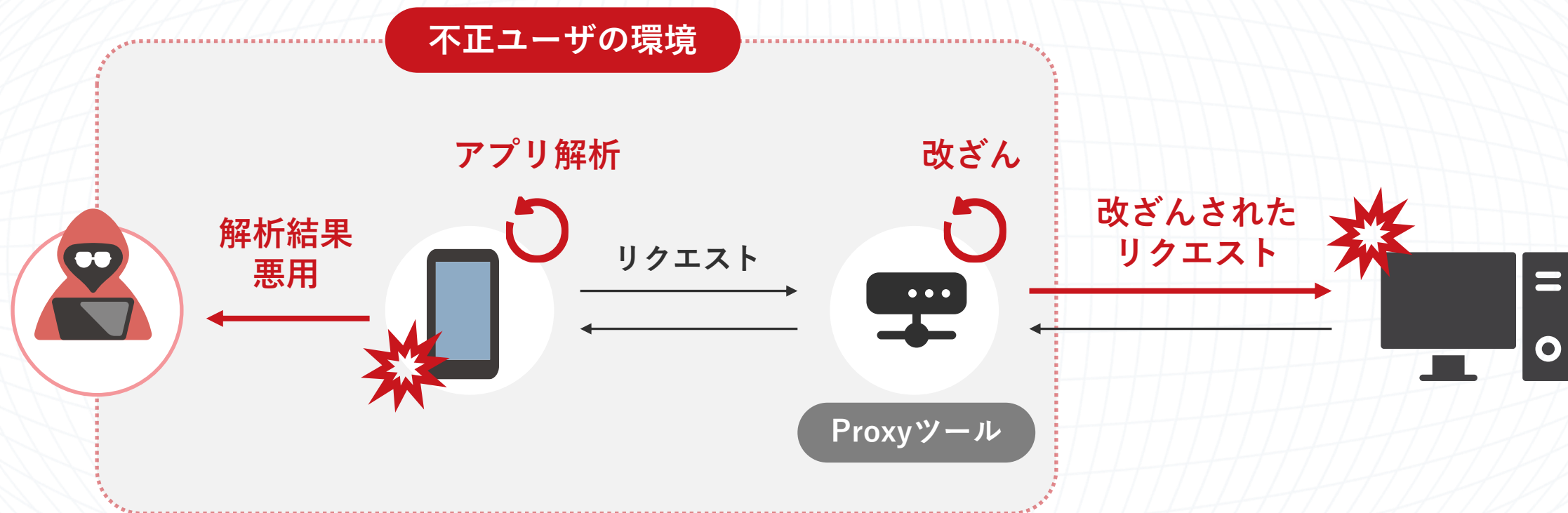


情報漏洩

他ユーザーの
データ取得



モバイルアプリに対する代表的な攻撃手法



攻撃者の手元（クライアント）で完全にコントロールされる

| モバイルは、Webと同じ守り方では防げない

クライアントは
想定通りに動く前提

防御は
サーバー中心



Web

サーバーを守る世界観

クライアントは
攻撃者に操作される

防御をクライアント
に置くと破られる



Mobile

クライアントが信用できない世界観

Webよりも攻撃対象は広いのに、守りは開発段階に偏っている

なぜWebよりモバイルのセキュリティは遅れているのか

モバイルのセキュリティ対策 3つの課題

スキル依存



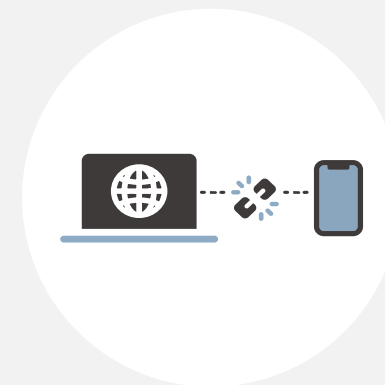
高度な解析・検証
スキルが必要

標準化不足



ツールは存在するが
自動化・運用が難しい

Webとの分断



既存の診断プロセスに
組み込みにくい

**これらの課題は
生成AIで解決できます！**



生成AI時代の脆弱性診断なら

AeyeScan

クラウド型Webアプリケーション
脆弱性検査ツール

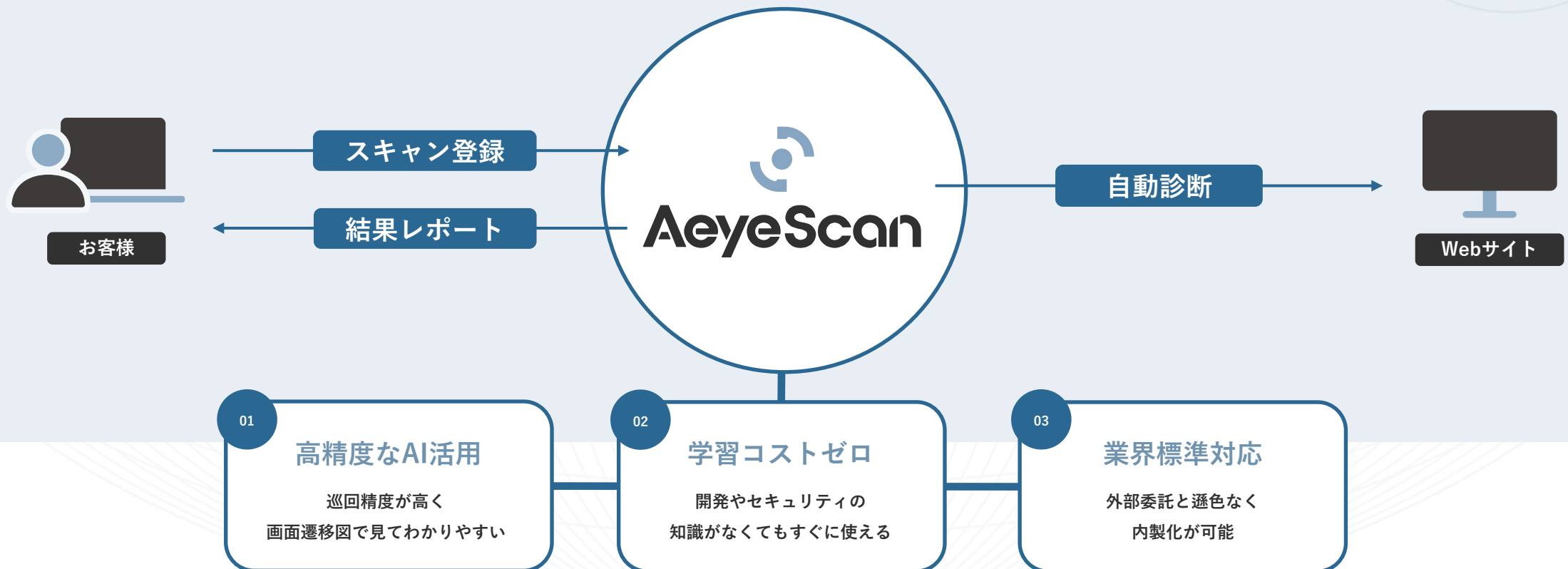
国内市場シェア

No.1※

※ 富士キメラ総研調べ「2025 ネットワークセキュリティビジネス調査総覧 市場編」
Webアプリケーション脆弱性検査ツール ベンダーシェア（2024年度実績）

※ ITR調べ「ITR Market View：サイバー・セキュリティ対策市場2026」SaaS型Web
アプリケーション脆弱性診断・管理市場：ベンダー別売上金額シェア（2024年度実績）

有償契約
300社以上





AeyeScan が Androidアプリ診断を 近日提供

Web、API、そしてモバイルの診断を
1プラットフォームで

POINT

生成AIが「見て、判断する」—高精度な画面認識

高度なVision AIが人間のように画面を認識。コード構造に依存しないため、難読化されたコードや独自のUIフレームワークを採用したアプリでも正確な認識・操作が可能です。



POINT

| 生成AIが「考えて、動く」—網羅的な自律巡回

戦略的な自律走行
Planner

AIが次の一手を判断
独自の仕組みで網羅的な
画面遷移を可能に

文脈を読み取った
テストデータ生成

文脈から入力値を動的生成
本物に近いデータ入力で
複雑なフォームも突破

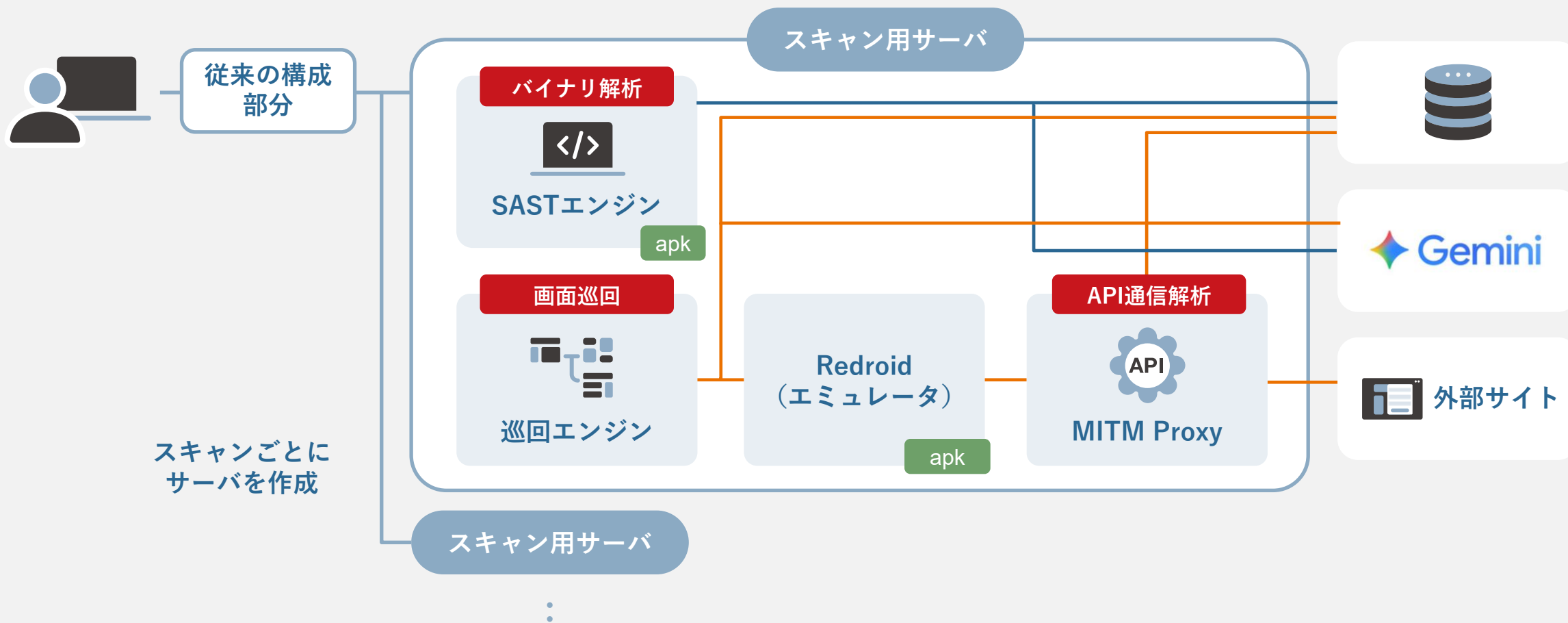
三位一体による
総合スキャン

API・バイナリ・巡回を統合
サーバーと端末側の
双方を一括でスキャン

Webと同じ手軽さで、モバイルアプリ診断を開発の標準プロセスに

POINT

三位一体を実現するシステムアーキテクチャ



POINT

三位一体を実現するシステムアーキテクチャ

アプリの「中身」を徹底解析

バイナリ解析

</>

SASTエンジン

apk

画面巡回



巡回エンジン

サーバーとの「通信」をキャッチ

API通信解析



MITM Proxy

Redroid
(エミュレータ)

apk

外部サイト

従来の構成
部分スキャンごとに
サーバを作成

実際の「画面」を網羅解析

デモ画面リファレンス

AIが自律的に画面を巡回

画面遷移図 (24. eccense)

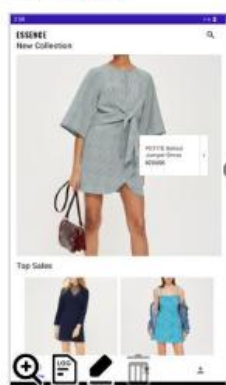
画面数: 11 (スキャン対象: 11画面, リクエスト数: 8リクエスト)

ダウンロード

全てを展開

凡例: ①

■ 自動巡回



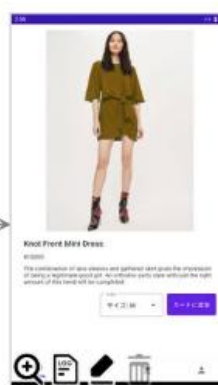
87.Home

↔ 非表示



89.検索_form

↔ 子画面(6)表示



90.検索結果_form

! ココがポイント

画面を自動で巡回し
遷移図を生成

Status: ① Crawling

Auto Fetch

Auto Chase



デモ画面リファレンス

| 手動巡回と自動巡回の組み合わせも可能

リモートAndroid手動巡回 (eccense)

6:24



PETITE Crepe Wrap Mini Dress

¥20000

Even though the dress is stylish, the long flared skirt is strikingly feminine.
The fluttering hem leaves a beautiful afterglow as you move.

size

サイズ: M

カートに追加

画面遷移図に反映

リセット

中止

画面遷移状態

操作で確定した画面がここに表示されます

! ココがポイント

AIが突破できない
2段階認証の壁も突破

取得できた通信

[除外されている通信](#)

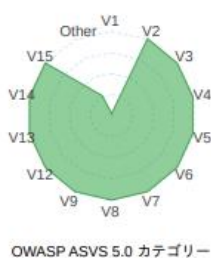
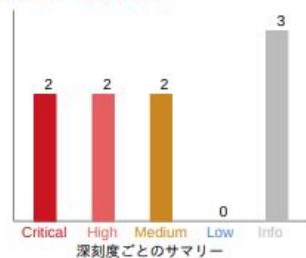
15:24:48 GET https://demosite1.aeyescan.work:13333/api/product/4
15:24:39 GET https://demosite1.aeyescan.work:13333/api/search?keyword...
15:24:08 GET https://demosite1.aeyescan.work:13333/api/home

デモ画面リファレンス

脆弱性の詳細や対処法までわかる、日本語レポート

スキャンサマリー

全体評価 Critical

脆弱性の深刻度はCVSSv4 (<https://www.first.org/cvss/v4.0/specification-document>) に基づき以下の基準で設定しています。

深刻度	CVSSv4基本値	脆弱性に対して想定される脅威
Critical	9.0～10.0	・ リモートからシステムを完全に制御されるような脅威 ・ 大部分の情報が漏えいするような脅威 ・ 大部分の情報が改ざんされるような脅威
High	7.0～8.9	・ 一部の情報が漏えいするような脅威 ・ 一部の情報が改ざんされるような脅威 ・ サービス停止に繋がるような脅威 ・ その他、Critical/Highに該当するが再現性が低いもの
Medium	4.0～6.9	・ 一部の情報が漏えいするような脅威 ・ 一部の情報が改ざんされるような脅威 ・ サービス停止に繋がるような脅威 ・ その他、Critical/Highに該当するが再現性が低いもの
Low	0.1～3.9	・ 攻撃するために複雑な条件を必要とする脅威 ・ その他、Mediumに該当するが再現性が低いもの
Info	0	

基本情報

サイトタイプ	Mobile向けサイト
トップURL	http://android.example.com:18080
スキャンルールセット	APIスキャン
画面数	10 (スキャン対象: 6)

● APK解析 (AndroidManifest.xml)

概要

脆弱性情報

詳細ログ

デバッグ可能なアプリ

スキャン情報

20. permission (<http://android.example.com:18080>)

検出箇所

AndroidManifest.xml

深刻度

High

CVSS: 7.3 (CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N)

検知理由

android:debuggable="true" が設定されています。本番ビルドでは無効にしてください。

補足

Android Gradle Plugin の release ビルドタイプはデフォルトで debuggable=false ですが、build.gradle で android.buildTypes.release.debuggable = true と書き換えていないか、また AndroidManifest.xml の <application> タグに android:debuggable="true" が直接書かれていないかを確認してください。検出時の典型的な攻撃シナリオは、(1) 端末を USB 接続し adb で対象アプリを起動、(2) adb shell run-as <package> でアプリのプライベートディレクトリにアクセス、(3) Android Studio のデバッガで JDWP に接続して任意のメソッド呼び出し・変数書き換え、というものです。CI で逆コンパイルツール等で AndroidManifest.xml を抽出し、application 要素の debuggable 属性が含まれていないことをチェックする運用を推奨します。

| まとめ

Webより遅れがちで、課題の多いモバイルのセキュリティ対策…

生成AIを活用すれば、専門家不要
リリース前の『早く・安く・確実な』
モバイル診断が可能に！

AIにより、
スキル・コスト・工数の壁を解消

開発の中で
継続的に回るセキュリティへ

| AeyeScanが選ばれている理由

誰でも使える操作性 × プロが認める機能・性能

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

／最終週もぜひご参加ください／

詳細はこちらから



**8月
限定**

脆弱性対策 まるわかり月間

最終週! Week4 この機会に、診断ツールを見てみませんか?

診断ツールを知る

8月24日(月)～8月28日(金)

セキュリティ診断のお悩み・お困りごとをお聞かせください！

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





AeyeScan

セキュリティに、確かな答えを。