API悪用の実態と検出手法

モバイルアプリを起点とした攻撃をどう見抜くか

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

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。

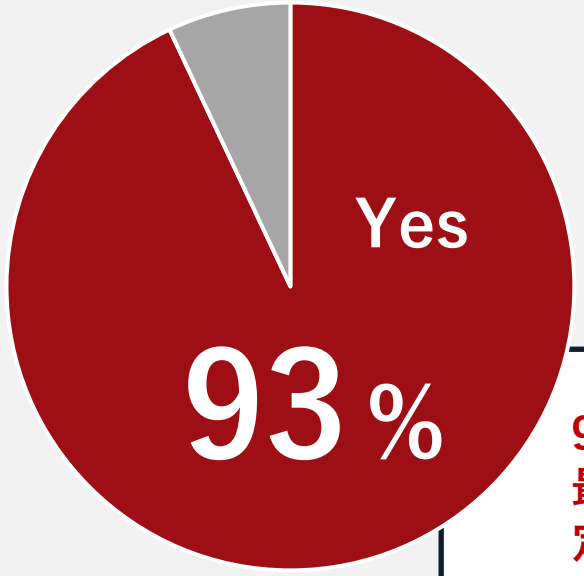
AeyeSecurityLab

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

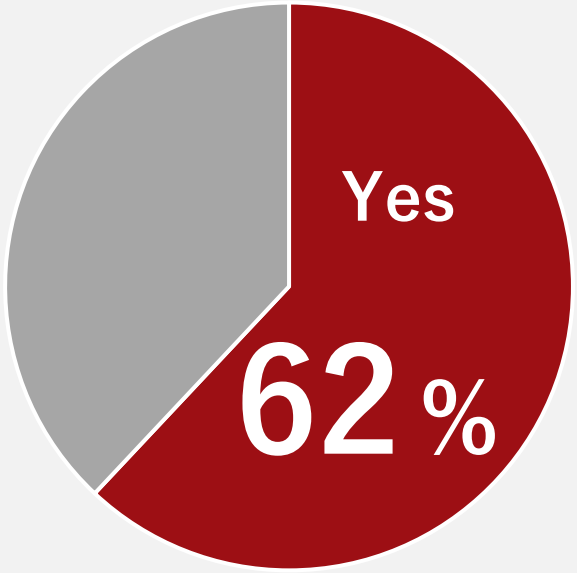
Guardsquare社の調査

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



出典：Guardsquare社調査報告書 https://www.guardsquare.com/report/overconfidence-exposes-mobile-app-security-gaps

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

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

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
があり比較的実施されている

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

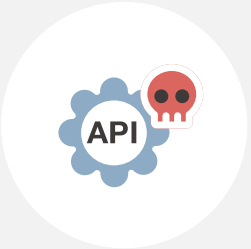
アプリが
解析される

通信が観測・改ざん
される

トークンが
抜かれる

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）

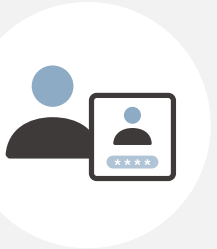


認証バイパス

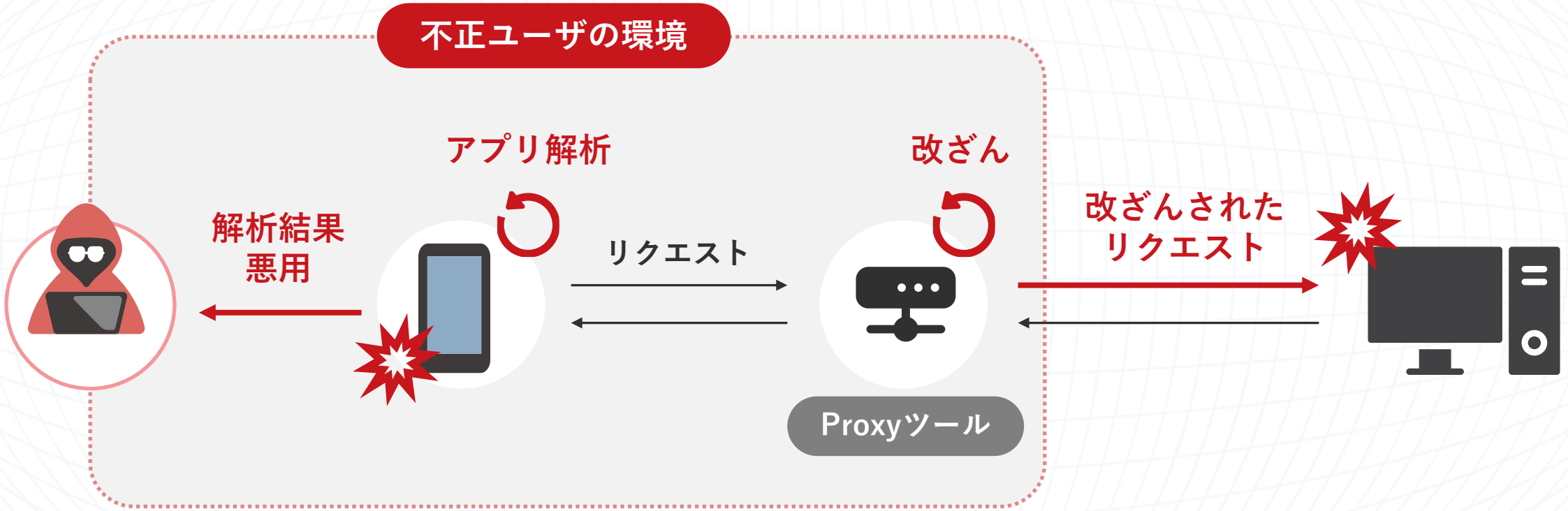
ログインせずに機能を
利用・権限昇格

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

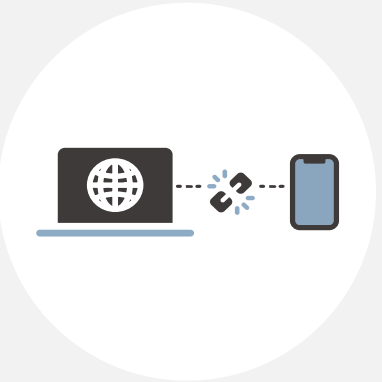
スキル依存

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2025」SaaS型
Webアプリケーション脆弱性管理市場：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

01
高精度なAI活用
巡回精度が高く
画面遷移図で見てわかりやすい

02
学習コストゼロ
開発やセキュリティの
知識がなくてもすぐに使える

03
業界標準対応
外部委託と遜色なく
内製化が可能

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

AeyeSecurityLab

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。

AIが要素を解析

- 要素を検出
- 文脈を理解
- コードを生成

```
[
 {
  "name": "Search",
  "role": "icon",
  "point_y": 91,
  "point_x": 892,
  "bbox_ymin": 78,
  "bbox_xmin": 865,
  "bbox_ymax": 104,
  "bbox_xmax": 919
 },
 {
  "name": "PETITE Crepe Wrap Mini
Dress #10000",
  "role": "link",
  "point_y": 453,
  "point_x": 696,
  "bbox_ymin": 393,
  ....
```

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

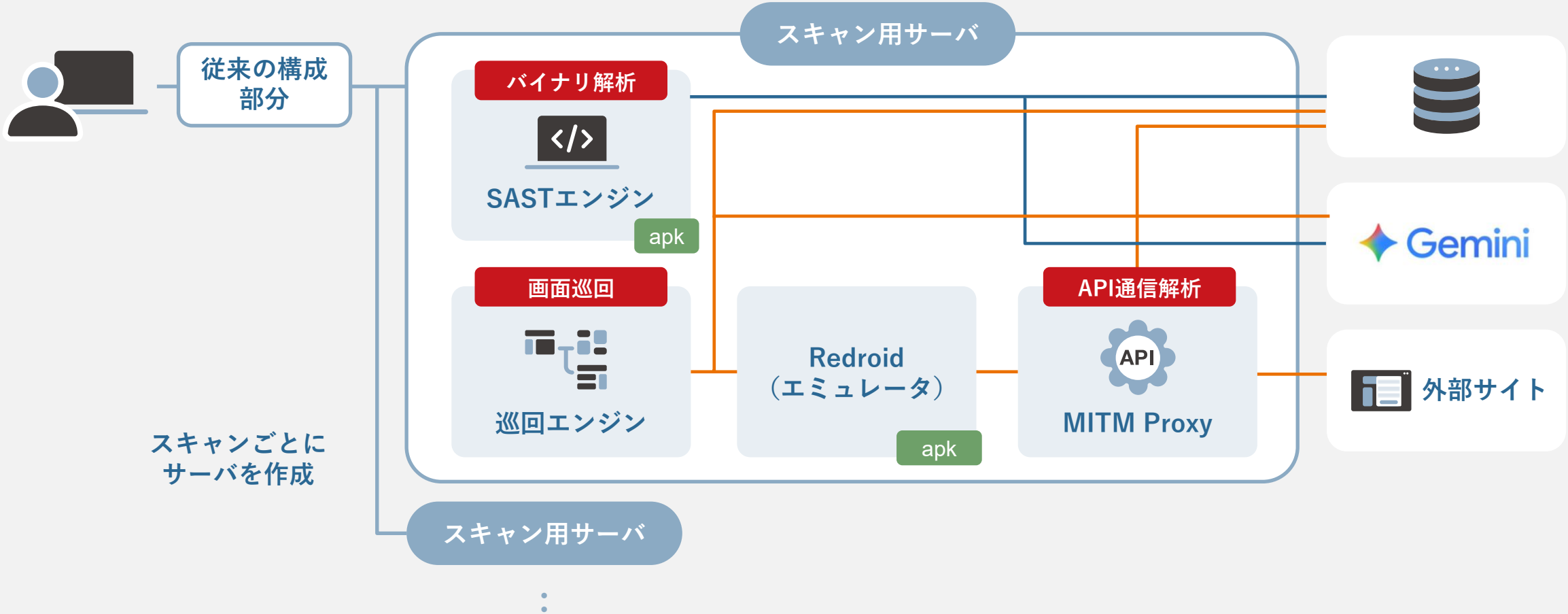
文脈から入力値を動的生成
本物に近いデータ入力で
複雑なフォームも突破

三位一体による
総合スキャン

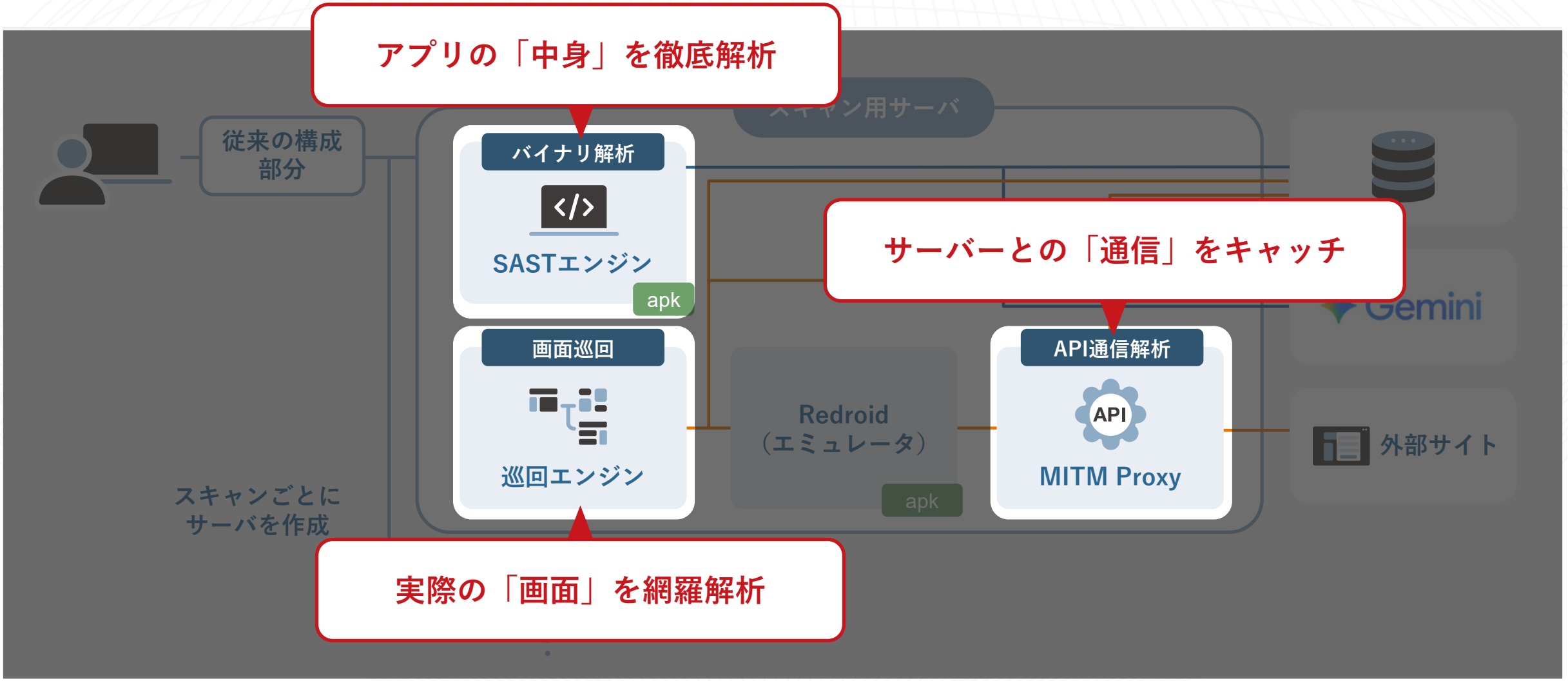
API・バイナリ・巡回を統合
サーバーと端末側の
双方を一括でスキャン

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

三位一体を実現するシステムアーキテクチャ

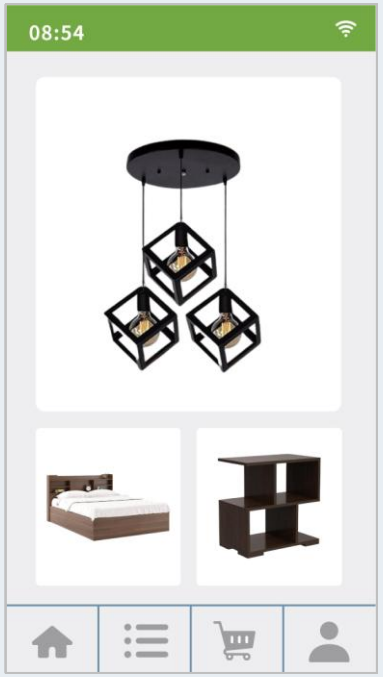


三位一体を実現するシステムアーキテクチャ



手動×自動巡回 ―AIが突破できない「2段階認証の壁」も解決

AeyeScan



入力イベント

{"event":"screen","name":"login"}
{"state":"ready"}

{"event":"input","field":"email"}
{"valid":true,"length":16}

{"event":"input","field":"password"}
{"valid":true,"masked":true}

{"event":"tap","target":"login"}
{"action":"authenticate"}

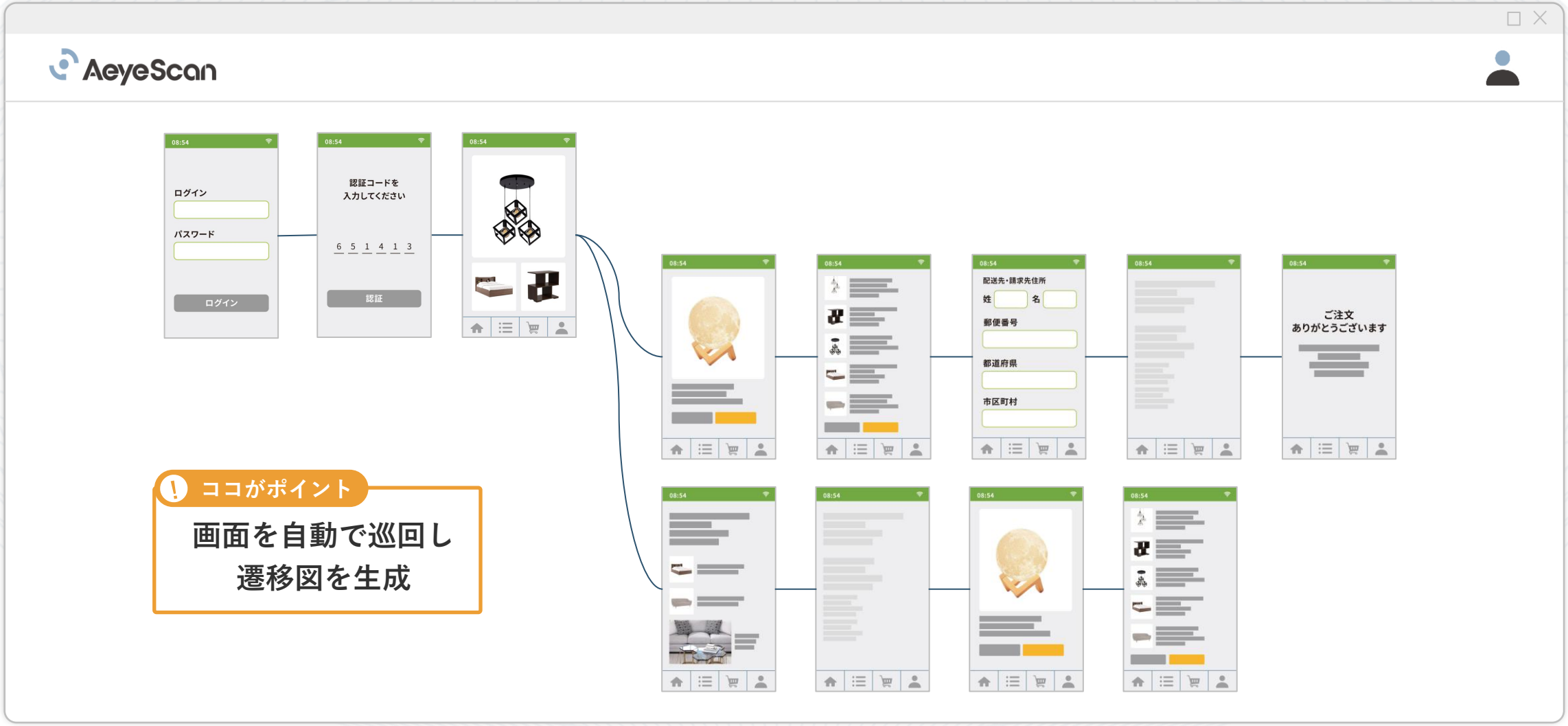
{"event":"screen","name":"verification"}
{"otp":"generated"}

{"event":"input","field":"otp"}
{"digits":6,"complete":true}

{"event":"verify","status":"success"}
{"session":"authenticated"}

登録

AIが自律的に巡回し、画面遷移図を自動で生成



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※

EPARK / AIRE / HIS / H2O RETAILING / NTT EAST / odakyu / 近鉄情報システム株式会社 / GEO / SymEnergy / 水ing Swing Corporation / Suzuyo / TOYOTA HOME / NANKAI 南海システムソリューションズ / 日本調剤 / JARMeC 日本動物高度医療センター / 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! TORANOANA LABORATORY / BookLive

メディア

集英社 / 中日新聞 / NIKKEI / Media Do

製造

AICA / AISIN / KITZ 株式会社キッツ / KOSÉ / SAKI / TIGER / TEIJIN / Denkei / House / Mizuno / ユーグレナ

金融

セブン銀行 / 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. 株式会社アドバンスト・メディア / Lexica E-Retailing Platform / エフアンドエムネット株式会社 / M-aid / MT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 株式会社リバスタ / 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 株式会社パソフィックネット / Human Interactive Technology Inc. / FUJISOFT / FUJITSU / MACROMILL / 三菱電機デジタルイノベーション株式会社 / YONA / リピスト

セキュリティ企業

NEC NECセキュリティ / NTT DATA 株式会社NTTデータ先端技術 / GSX GLOBAL SECURITY EXPERTS / 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）

本日のまとめ

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

＼本講演内容を、より詳しく解説／

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。