データの取り扱い方法ならびに セキュリティ の取り組みについて

― AeyeScanのWeb-ASM機能・生成AI機能・Androidアプリ診断機能 ―

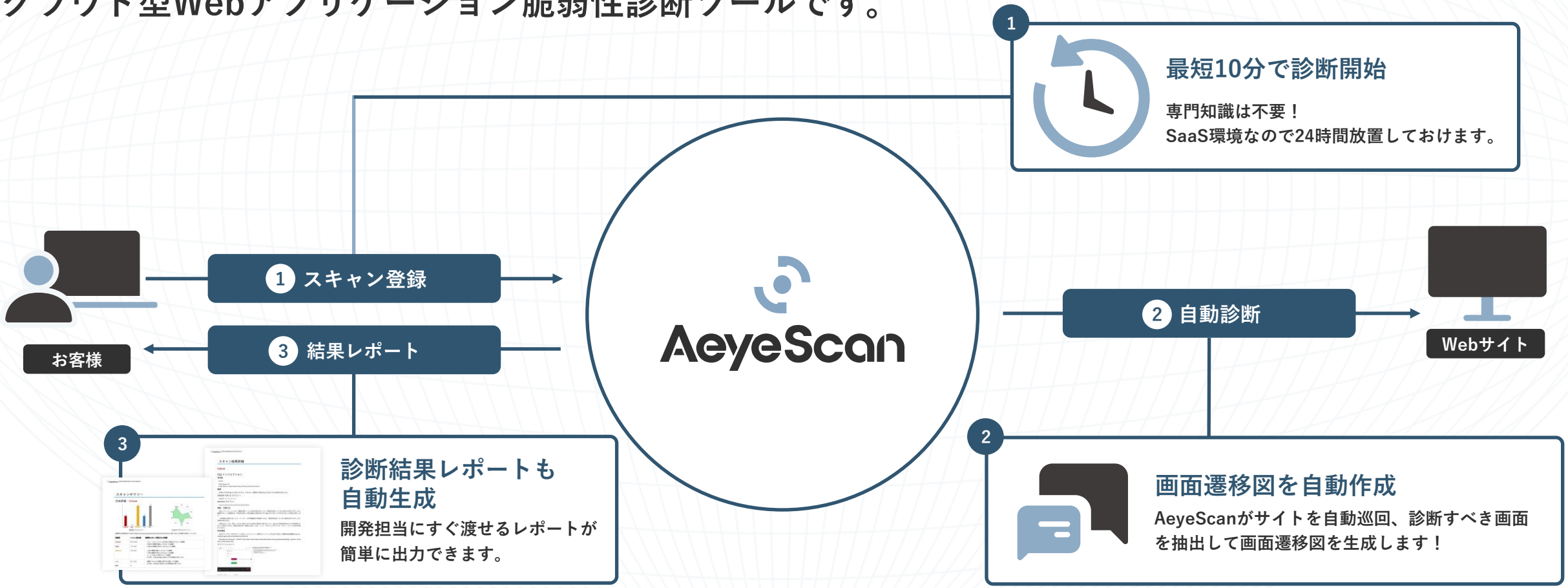
本資料は 生成AI、Androidアプリ診断 それぞれのオプション機能のセキュリティ対応状況の説明資料です。
コンプライアンス評価の参考資料としてご活用ください。

©AeyeSecurityLab Inc.

AeyeSecurityLab

AeyeScanとは？

生成AI等の最先端技術の活用による自動化で、いつでも誰でも簡単に、高精度な診断を実現する、クラウド型Webアプリケーション脆弱性診断ツールです。



©AeyeSecurityLab Inc.

AeyeSecurityLab

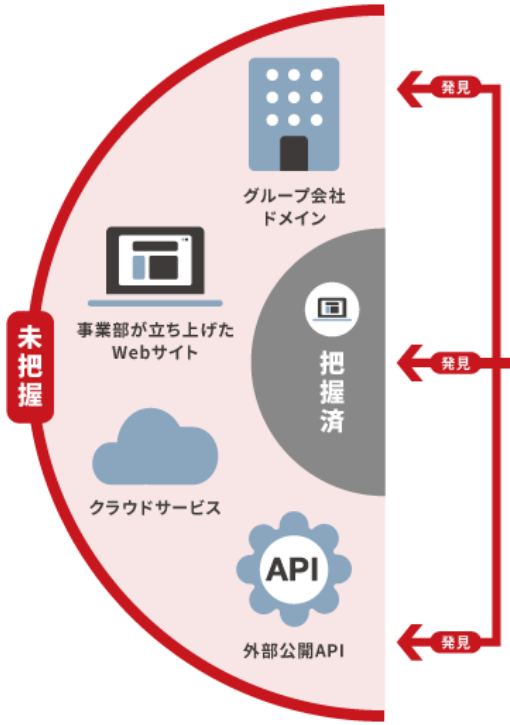
生成AI活用で、工数をかけずにWeb-ASMを実現

オプション機能

Web-ASMとは？

未把握な攻撃面の継続的な発見・リスク評価※

※リスク評価：AeyeScanのスキャンによる



特許取得実績のある
生成AI活用の技術により、
効率的・網羅的に攻撃面を発見。



生成AI

Web-ASMの実施ステップ

1 攻撃面の発見



Web-ASM機能

自社が保有している
ドメイン一覧を抽出

2 攻撃面の情報収集



自動巡回

未把握のドメインを
巡回対象に追加

3 攻撃面のリスク評価



脆弱性診断

管理対象の全ドメインに
脆弱性診断を実施

AeyeScan ひとつで、
より網羅的な脆弱性診断とリスクマネジメントが可能に！

©AeyeSecurityLab Inc.

AeyeSecurityLab

生成AIの活用による高度な自動化を実現

オプション機能

1 診断設定がさらにカンタンに

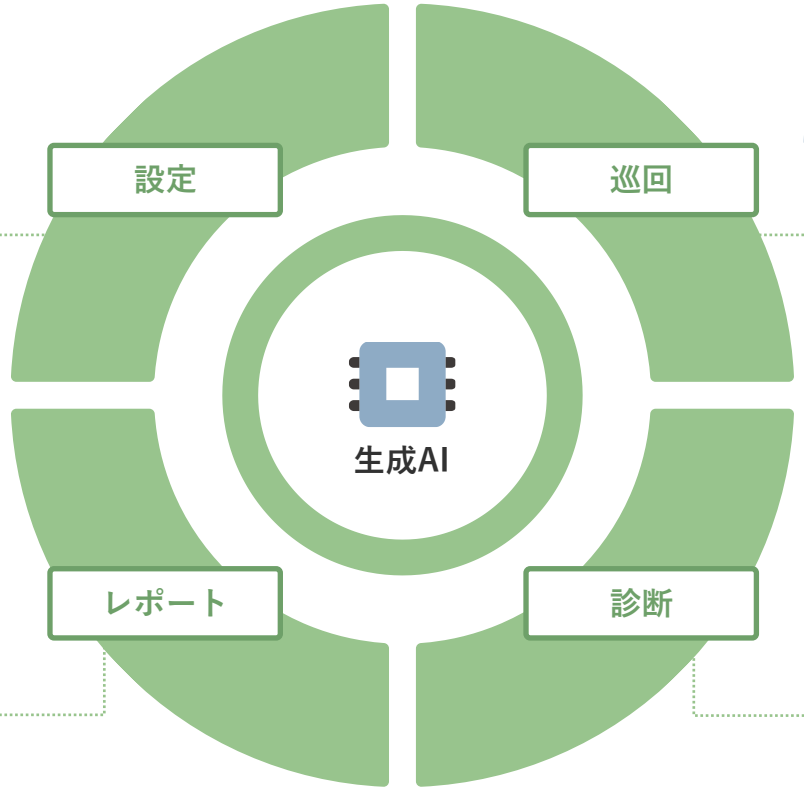
- フリーフォーマットでの指示

特許 第7320211号

2 巡回がより柔軟に進化

- 多言語対応
- フリーフォーマットでの指示
- 画面の自動類似判定

特許 第7348698号



3 手動で診断していた項目にも対応

- パラメータの用途を推測
- セッションIDの規則性を解析

特許 第7344614号

4 高度なレポート出力も可能に

- 診断結果を元に総評を生成

©AeyeSecurityLab Inc.

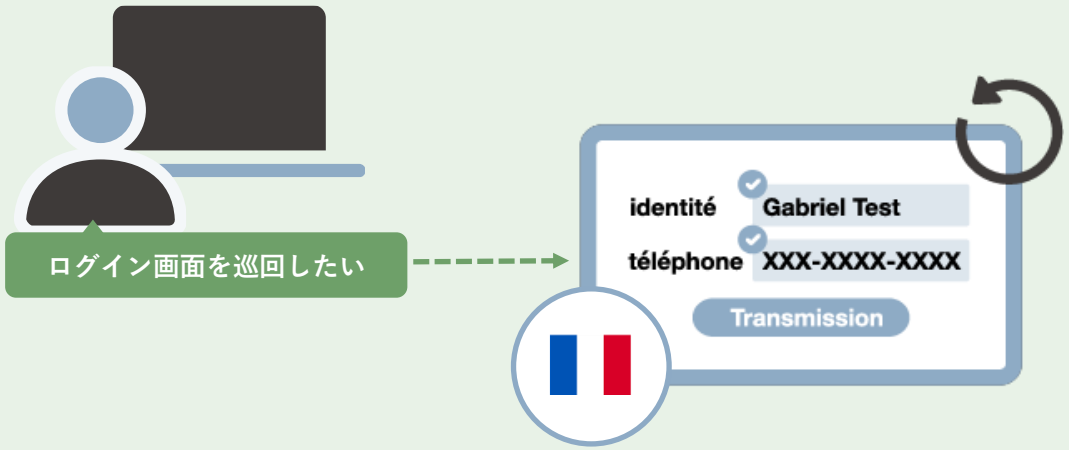
AeyeSecurityLab

巡回もより柔軟に！フリーフォーマットでの指示に対応

巡回 オプション機能

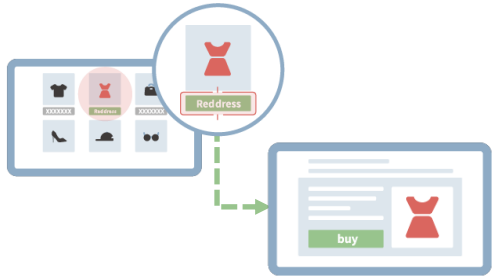
巡回も自然言語での指示が可能に

巡回してほしい画面の機能などを入力すると
指示した箇所のみ巡回



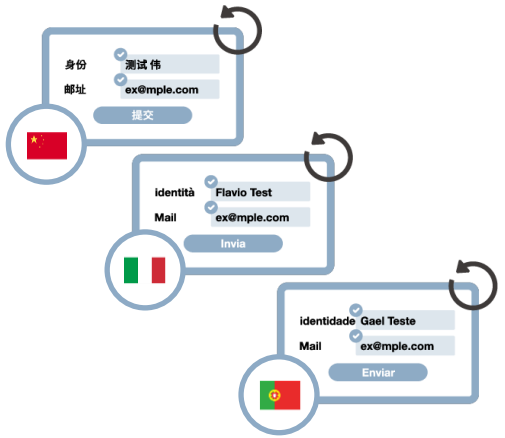
多言語対応により、
日本語以外のWebサイトも幅広く巡回

多言語サイトの把握が可能



日本語サイトと同じように
ボタンやリンクを認識して遷移

フォーム入力も多言語に対応



日本語・英語に加え、フランス語、中国語、韓国語、オランダ語、ドイツ語、イタリア語、
ポーランド語、スペイン語、ポルトガル語、ロシア語、スウェーデン語、アラビア語に対応予定

©AeyeSecurityLab Inc.

これまで手動でしか診断できなかった項目にも対応

診断 オプション機能

セカンドオーダーインジェクションによる クロスサイトスクリプティング（XSS）

検出手順

1. 登録/更新した値が表示されそうな画面を生成AI（ChatGPT）に推測させる
2. 値が表示されているか、巡回データを基に判定する
3. 判定結果がTrueの場合、セカンドオーダーインジェクションによるXSSスキャンの対象として診断を実施する



認可の不備の脆弱性

検出手順

1. サイト巡回時に「どの画面が管理者機能であるか」を生成AI（ChatGPT）に推測させる
2. 一般ユーザ権限でログインした際に「推測した画面へのボタンやリンクがない」場合に管理者機能であると判定する
3. スキャン時に、一般ユーザで管理者メニューを表示できるか検証する



管理者メニュー



一般ユーザーメニュー

©AeyeSecurityLab Inc.

診断結果をもとにしたエグゼクティブサマリも自動生成

レポート

オプション機能



©AeyeSecurityLab Inc.

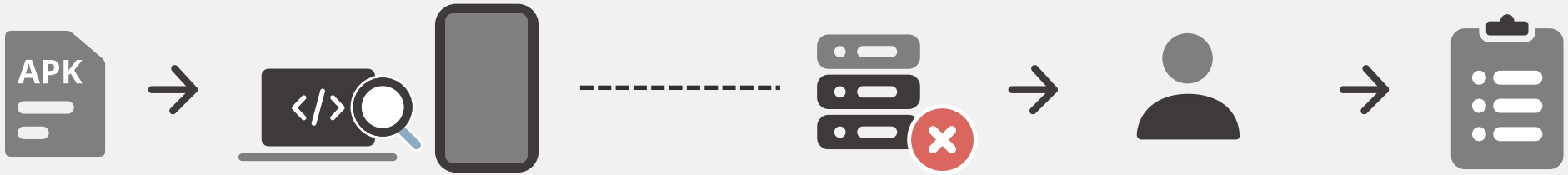
AeyeSecurityLab

Androidアプリの巡回・スキャンもかんたん操作で実現

オプション機能

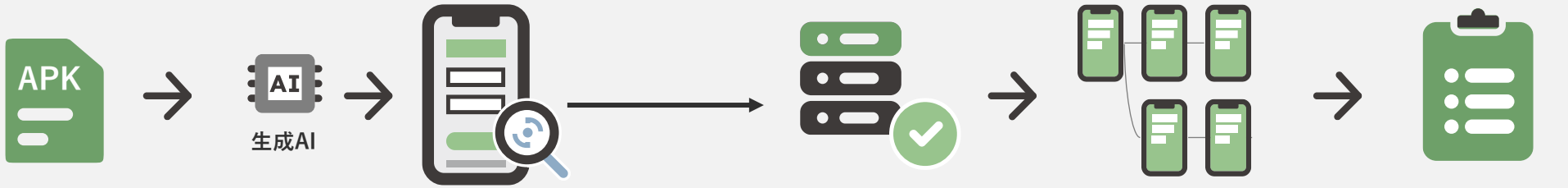
違いは、アプリを実際に動かして診断すること。攻撃者が実際に突く、通信や認証の弱点まで見つかります。

従来の静的診断ツール



AeyeScan Androidアプリ診断

アップロードするだけ



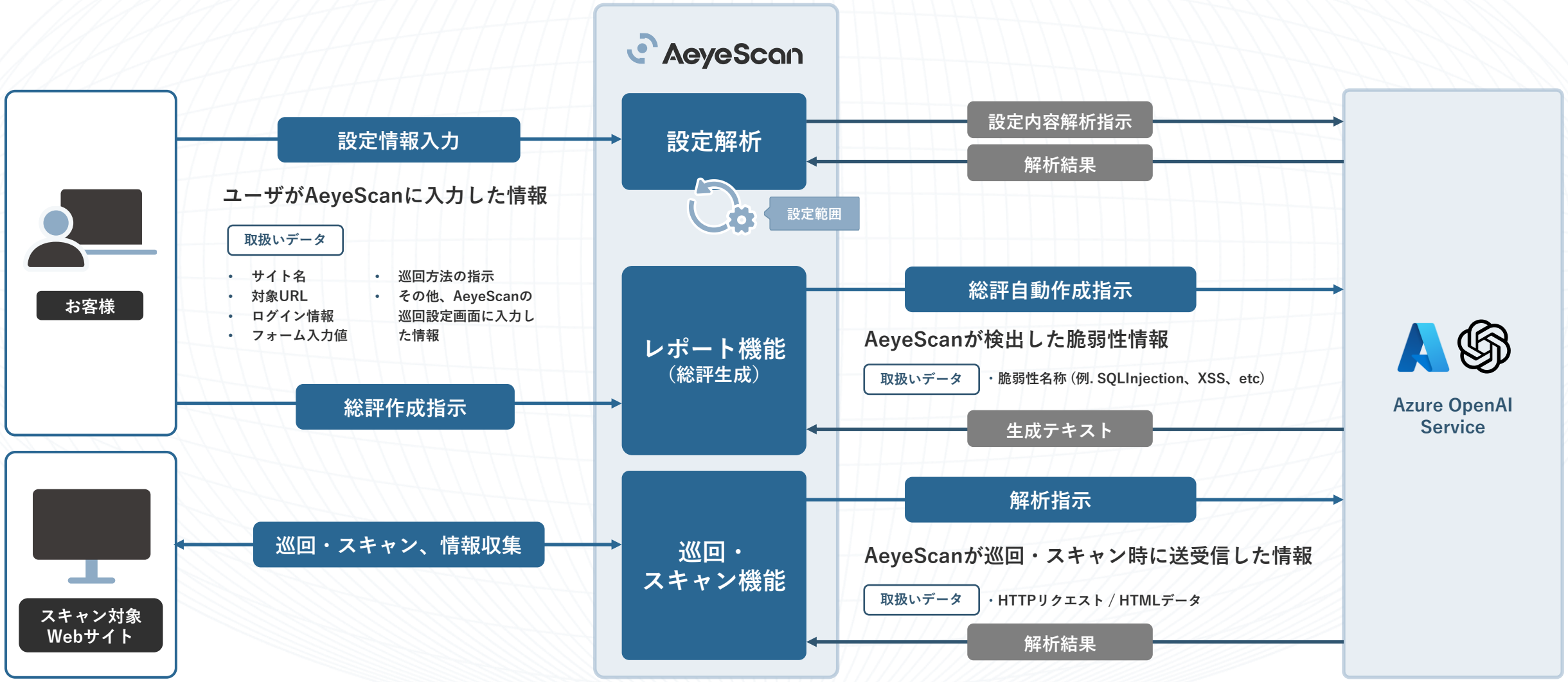
©AeyeSecurityLab Inc.

Web-ASM機能・生成AI機能の
データ取り扱いとセキュリティへの取り組み

©AeyeSecurityLab Inc.

AeyeSecurityLab

生成AI機能の主な取り扱いデータと流れ



©AeyeSecurityLab Inc.

利用方法とデータの取り扱い

生成AIの利用方法について

- ベースライセンスで提供している基本機能には利用しておらず、オプション機能として提供している、Web-ASM機能、生成AI機能およびAndroidアプリ診断機能にて、生成AIを利用しています。ご利用の際は、別途お申込みが必要です。
- Web-ASM機能・生成AI機能では、Microsoft社のAzure OpenAI Serviceを使用していますが、お客様が直接Azure OpenAI Serviceに入力したり、応答を受け取るような使い方はできません。Androidアプリ診断機能については次ページをご覧ください。

Web-ASM機能・生成AI機能で取り扱うデータおよび利用目的

	取り扱うデータ	利用目的
巡回設定機能	お客様がAeyeScanに入力した情報 （対象サイトのURL、認証情報など）	巡回対象の解析
巡回・スキャン機能	AeyeScanが巡回・スキャン時に送受信した情報 （HTTPリクエスト、HTMLや画面データ）	巡回精度向上やスキャン実施
レポート機能	AeyeScanが検出した脆弱性情報 （脆弱性の名称）	総評（エグゼクティブサマリ）作成

©AeyeSecurityLab Inc.

プロンプトデータおよび生成データの取り扱い

データの学習について

お客様がAeyeScanに入力した情報をもとに作成したプロンプトデータ（以下、お客様のプロンプトデータという）や出力した生成データを、**学習に利用したりファインチューニングに利用することはありません**。Azure OpenAI Serviceも同様です※1。

※1. 参考文書：Data, privacy, and security for Azure OpenAI Service

データへのアクセスについて

お客様のプロンプトデータは、悪用／誤用を監視する目的のためAzure上に保存します。保存したデータは、管理者権限をもったエーアイセキュリティラボ社の社員または、資格をもったMicrosoft社の社員がレビューすることがあります。

データの秘密保持について

Microsoft Azure OpenAI Service の利用にあたっては、「Microsoft 製品およびサービスに関するデータ保護付録（Microsoft Products and Services Data Protection Addendum：DPA）」が適用されます。本契約により、Microsoft 社は顧客データの機密保持義務を負っており、法令による要請などの例外を除き、**第三者への開示やアクセスを認めないことが明記されています**。
また、AeyeScanのご利用に際しても、当社は利用規約に基づき、**機密保持義務を遵守いたします**。

データの保存期間について

お客様のプロンプトデータの保存期間は、サービスの利用規約（データ削除期限日等）の通りです。
Azure OpenAI Serviceでは、30日と規定されています※2。

※2. 参考文書：Data, privacy, and security

©AeyeSecurityLab Inc.

ガイドラインやポリシーへの対応状況



生成AI利用（ChatGPT）時の
セキュリティ対策を実施しています

OWASP Top 10 for Large Language Model Applicationsの
ガイドラインを基に、プロンプトインジェクションや機密情報の
漏洩に関する対策を行っています。



AeyeScanの提供・運用組織として
各種認証を取得しています

情報セキュリティマネジメントシステム（ISMS） IS 752963 / ISO 27001
ISMSクラウドセキュリティ認証 CLOUD 790050 / ISO 27017
情報セキュリティサービス基準適合サービスリスト 023-0026-20

Azure OpenAI Serviceの対応方針は、以下ドキュメントで確認できます

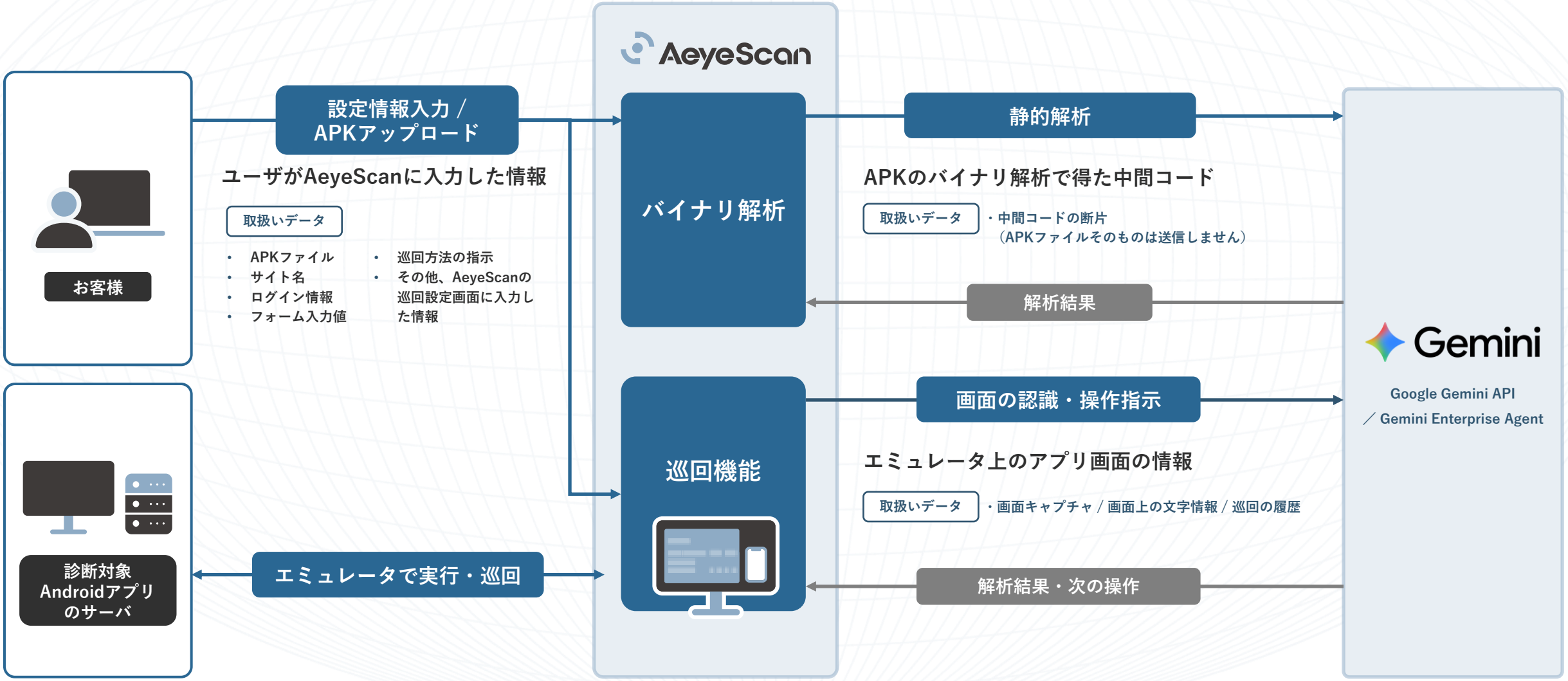
- 制限付きアクセス：Limited access
- 倫理規定：Code of conduct
- わかりやすさに関するメモ：Use cases for Azure OpenAI Service
- データ、プライバシー、セキュリティ：Data, privacy, and security

©AeyeSecurityLab Inc.

Androidアプリ診断機能の
データ取り扱いとセキュリティへの取り組み

©AeyeSecurityLab Inc.

Androidアプリ診断機能の主な取り扱いデータと流れ



©AeyeSecurityLab Inc.

利用方法とデータの取り扱い（Androidアプリ診断機能）

生成AIの利用方法について

- Androidアプリ診断機能では、Google社のGemini API（Google AI Studio）またはGemini Enterprise Agentを使用しています。お客様が直接入力したり、応答を受け取るような使い方はできません。
- アップロードいただいたアプリケーションファイルは、お客様の脆弱性診断の目的にのみ利用し、サービス利用規約に定める範囲で取り扱います。

Androidアプリ診断機能で取り扱うデータおよび利用目的

	取り扱うデータ	利用目的
バイナリ解析	APKファイルのバイナリ解析で得た中間コードの断片 （APKファイルそのものは送信しません）	静的解析（脆弱性の検出）
巡回機能	エミュレータ上でアプリを操作した際の画面キャプチャ （画面上の文字情報、巡回の履歴を含む）	画面の認識と巡回の操作判断

©AeyeSecurityLab Inc.

プロンプトデータおよび生成データの取り扱い（Androidアプリ診断機能）

データの学習について

Androidアプリ診断機能で作成したお客様のプロンプトデータや出力した生成データを、**学習に利用したりファインチューニングに利用することはありません**。Gemini APIおよびGemini Enterprise Agentも同様です※1。

※1. 参考文書： Gemini API 利用規約／Google Cloud サービス固有規約

データへのアクセスについて

お客様のプロンプトデータは、悪用／誤用を監視する目的でGemini上に保存します。保存したデータは、Google社の権限をもった担当者がレビューすることがあります。

データの秘密保持について

Gemini APIの利用にあたっては「Google Data Processing Addendum」が、Gemini Enterprise Agentの利用にあたっては「Cloud Data Processing Addendum」が適用されます。本契約により、Google社は顧客データの機密保持義務を負っており、法令による要請などの例外を除き、**第三者への開示やアクセスを認めないことが明記されています**。
また、AeyeScanのご利用に際しても、当社は利用規約に基づき、**機密保持義務を遵守いたします**。

データの保存期間について

お客様のプロンプトデータの保存期間は、サービスの利用規約（データ削除期限日等）の通りです。
Gemini APIでは55日、Gemini Enterprise Agentでは利用規約違反の疑いがある場合に限り最大90日と規定されています※2。

※2. 参考文書： Gemini API 不正利用の監視／Gemini Enterprise Agent 不正行為の監視

©AeyeSecurityLab Inc.

ガイドラインやポリシーへの対応状況（Androidアプリ診断機能）



生成AI利用（Gemini）時の セキュリティ対策を実施しています

OWASP Top 10 for Large Language Model Applicationsの
ガイドラインを基に、プロンプトインジェクションや機密情報の
漏洩に関する対策を行っています。



AeyeScanの提供・運用組織として 各種認証を取得しています

情報セキュリティマネジメントシステム（ISMS） IS 752963 / ISO 27001
ISMSクラウドセキュリティ認証 CLOUD 790050 / ISO 27017
情報セキュリティサービス基準適合サービスリスト 023-0026-20

Gemini API・Gemini Enterprise Agentの対応方針は、以下ドキュメントで確認できます

■ Gemini API（Google AI Studio）

- 利用規約：Gemini API Additional Terms of Service
- 不正利用の監視：Abuse monitoring
- データ処理規約：Google Data Processing Addendum

■Gemini Enterprise Agent

- 学習の制限：サービス固有規約（トレーニングの制限）
- 不正行為の監視：不正行為の監視
- データ処理規約：Cloud Data Processing Addendum

©AeyeSecurityLab Inc.

会社概要

商号	株式会社 エーアイセキュリティラボ	
役員	代表取締役社長	青木 歩
	取締役副社長	安西 真人
	取締役	杉山 俊春　角田 茜
	執行役員 CTO	浅井 健
	執行役員	関根 鉄平
事業内容	情報セキュリティ関連事業（調査・コンサルティング） クラウド型Web診断サービス「AeyeScan」提供	
設立	2019年4月	
拠点	東京都千代田区神田錦町2-2-1 KANDA SQUARE 11F WeWork内	
資本金	1億円	
社員数	70名	
Webサイト	https://www.aeyesec.jp/	
取得認証	情報セキュリティマネジメントシステム（ISMS） ISMSクラウドセキュリティ認証（ISO27017） 情報セキュリティサービス基準適合サービスリスト	

AeyeSecurityLab

セキュリティに
「あらたな答え」を提供し続ける
プロ集団

IS 752963 /
ISO 27001

CLOUD 790050 /
ISO 27017

023-0026-20

©AeyeSecurityLab Inc.



セキュリティに、確かな答えを。

©AeyeSecurityLab Inc.