生成AIにより高度化する攻撃
今、API が狙われている

― APIリスクの可視化と診断体制の作り方 ―

APIセキュリティは世界的な最優先課題となっている

生成AIがビジネス現場をはじめ多様な分野で技術革新を後押しする一方、それらの技術を悪用したサイバー攻撃の自動化・効率化が急速に進んでいる。APIも最優先ターゲットの１つ。

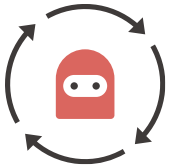
高度な攻撃の自動化

APIの構造を生成AIが解析
パラメータの特徴を推測し
複雑な攻撃を自動実行

脆弱性発見の効率アップ

APIの通信だけでなく、
APIリファレンスなどの
公開情報も統合し
短時間で弱点を推測

連鎖的な被害の拡大



他の攻撃者のノウハウを
高速で取得・学習することで
対策がとられる前に大量攻撃

見落とされがちな「API」の存在

Webサイト・アプリと同様のリスクがあるにも関わらず、APIは「目に見えない」状態で
利用されることが多いため、管理者が存在に気づきにくく、リスクが放置されやすい。

ユーザー操作画面がない

利用者・管理者の目に触れる
機会がないので関心が低い

更新頻度が高い

追加や変更が多く
管理・棚卸が間に合わない

ドキュメントが未整備

今ここにあるAPI=現物のみで
仕様書・設計書を確認できない

内部通信が多い

システム間連携で利用されるAPI
は管理対象として把握しにくい

公開範囲が複雑

公開APIと内部限定APIが混在し
把握漏れや誤設定のリスクも

攻撃者はAPIを狙っている

APIは魅力的な攻撃経路であり、被害規模が大きくなる傾向があるため標的になりやすい。
2022年Gartner社が「API攻撃がWebアプリ最大の攻撃経路になる」と予測、2023年以降現実に。

出典：Level Blue社 https://levelblue.com/blogs/security-essentials/gartner-predicted-apis-would-be-the-1-attack-vector-two-years-later-is-it-true

API攻撃のリアルな被害数字

公開API・認証情報漏洩による大規模データ流出

- Dellにて、APIの脆弱性により4,900万件の顧客レコードに影響のある被害が発生（2024年5月）
- Trelloにて、公開されたAPIにより1,500万人以上のユーザーデータが漏洩（2024年1月）

出典：Salt Security https://salt.security/blog/its-2024-and-the-api-breaches-keep-coming

APEC企業の85%が直近12ヶ月でAPIインシデントを経験（2025年5月）
平均被害額は58万USD→約8,550万円

出典：Akamai社 プレスリリース https://www.akamai.com/newsroom/press-release/2025-api-security-impact-study

Web診断だけでは「APIリスク」に対応しきれない

典型的なWeb診断（画面遷移時に発生するHTTP通信の診断）では、API固有の脆弱性の検知が難しい。

典型的なWeb診断	API固有の診断項目（技術課題）
パラメータ操作はWeb画面内で操作できるHTML要素の範囲で検証	APIリクエスト単体でのID指定操作などWeb画面を介さないロジックの検証
Web画面上で人が操作できるリンクやフォームのみ探索	モバイルアプリや内部通信APIなど非公開エンドポイントの検出
単発リクエストのレスポンス確認のみ	連続リクエストによるビジネスロジック連携による挙動変化を検証

APIリスクに対応できる診断体制の構築が欠かせない

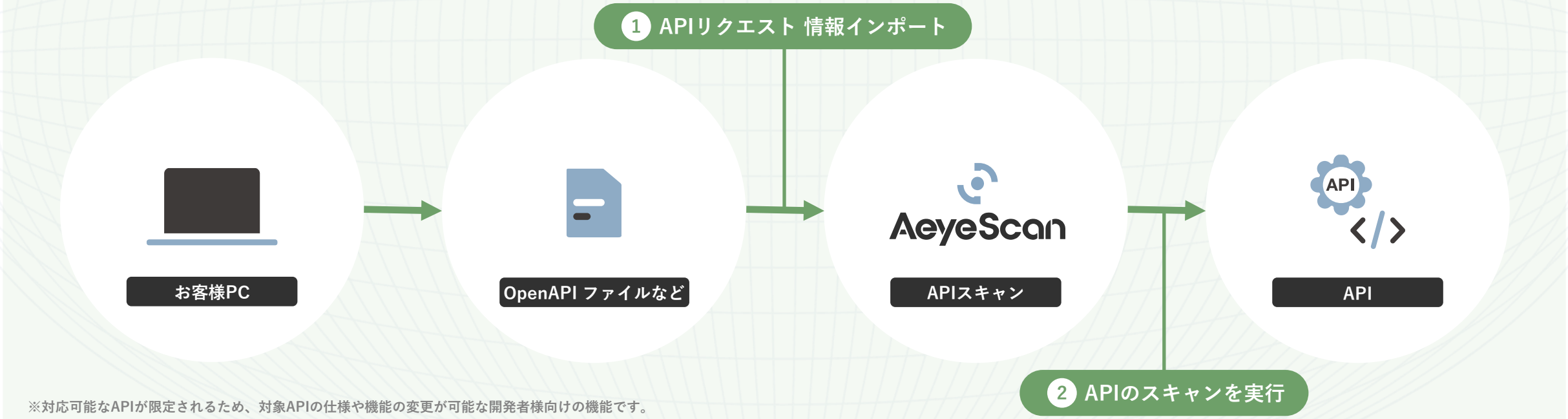
AeyeScanの「APIスキャン機能」は どのような開発環境でもAPIリスクを 防ぐ診断体制が構築できます

AeyeSecurityLab

AeyeScanなら、APIインポート～スキャン操作がかんたん

オプション機能

- OpenAPIファイル(API定義ファイル)のインポートが可能
- harファイル(http通信ログのアーカイブ)のインポートが可能
- cURLコマンドでAPIリクエストの登録が可能
- OpenAPI 3.0、3.1に対応

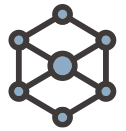


※対応可能なAPIが限定されるため、対象APIの仕様や機能の変更が可能な開発者様向けの機能です。

AeyeScanの「APIスキャン機能」が選ばれる理由

API固有の脆弱性を含むガイドライン
OWASP API Security Top 10に
準拠した診断項目

REST・SOAP・GraphQLなど
幅広いAPI方式に対応



Bearerトークン継承と
共通ヘッダー設定で、
APIの認証設定がかんたん

インポート対応フォーマットが
多く、診断用のスクリプトを
手動作成不要

かんたん操作で手間がかからず、開発環境を選ばないため
APIリスクを防ぐ診断体制を、開発工程に自然に組み込めます

AeyeScanを使った「API診断」の理想的な運用例

診断対象となるAPIの管理・棚卸

- Web-ASM機能（オプション）を使って、
  公開中のAPIエンドポイントを自動で一覧化
- Web診断のレポートに
  「APIカバレッジ率」を表示

未診断のAPIが存在するギャップを可視化

継続的に診断できる運用体制の構築

- CI/CDと連携し
  APIの新バージョンごとに自動スキャン
- 運用中のAPIは
  「90日ごとの定期再診断」＋「差分だけ再検査」
- スキーマ変更・認証方式変更などの
  重大変更トリガーで随時診断

開発の流れに組み込みながら、自動で最新の状態を診断できる

成功事例

約60プロダクトを定期診断できる体制を構築

某金融系サービス企業さまの事例

課題

- 事業拡大により、内部・外部問わずAPIを活用したプロダクトが急増
- API診断に必要な事前設定が多く、担当者の負担が大きかった

解決策

- 複雑な設定が不要で、簡単な操作でAPI診断ができるAeyeScanを導入
- 専用画面の作成なしで、ファイルのインポートだけでAPI診断が可能に

効果

- 診断にかかる工数・負担が減ることで、網羅的なAPI診断が実現できた
- 診断対象の洗い出し時に、APIも一緒に棚卸しすることで、セキュリティカバレッジが向上

その他にも…

体制移行によって APIを含む全てのWebサービスを診断できるようになったA社

CI/CD連携によって アップデートの度に、ほぼ自動で診断できる状態を実現されたB社　など

多数プロダクトの診断効率化に向け、API診断体制の構築と同時実行数の最適化も支援します

まとめ

攻撃者の主戦場となっているAPIは、脆弱性対策の盲点になりがちです。
APIリスクに備えるには、Web診断だけでは不十分なため、API診断が欠かせません。

AeyeScanのオプション機能「APIスキャン機能」を活用することで、
APIリスクに備えた診断体制を開発環境に組み込むことが可能になります。
体制づくりや運用方法も含めてご相談を承りますので、お気軽にご連絡ください。

本資料の内容に関連するAeyeScan機能

ご興味がございましたら、ぜひ弊社担当までお声がけください！

APIスキャン機能

トライアル受付中

運用方法についても、弊社カスタマーサクセス担当者がご相談を承ります

セキュリティに、確かな答えを。