『開発を止めるな！』を地で行く

セキュリティ・バイ・デザイン な

脆弱性対策とは

登壇者紹介

株式会社エーアイセキュリティラボ

事業企画部 ディレクター　**阿部 一真**（あべ かずま）

新卒でNTTデータに入社し、Salesforceビジネス推進部門で
コンサルティングセールス・カスタマーサクセスを経験。
その後、AIベンチャー企業・SaaSスタートアップ企業にてCS責任者
およびプロダクトマネージャー・事業統括責任者を歴任し、エーアイ
セキュリティラボに入社。
現在は、新規プロダクト企画・事業開発をリードしながら、
各種セミナー・講演への登壇などエバンジェリストとしても活動。

登壇者紹介

株式会社エーアイセキュリティラボ

事業企画部 ディレクター　阿部 一真（あべ かずま）

フォローお願いします！

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。

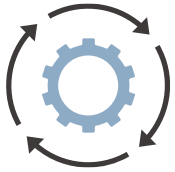
AeyeSecurityLab

AIが“開発”と“攻撃”の速度を同時に変えた

開発の高速化

AI駆動

Cursor / Copilot / Devin



実装・改修が高速化
小規模リリースが常態化

誰でも開発

ノーコード＋生成AI

作るハードルが低下
現場主導でサービス増加

攻撃の高速化

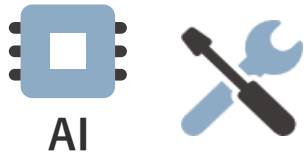
常時スキャン

24時間365日

公開直後から探索
AIが継続監視

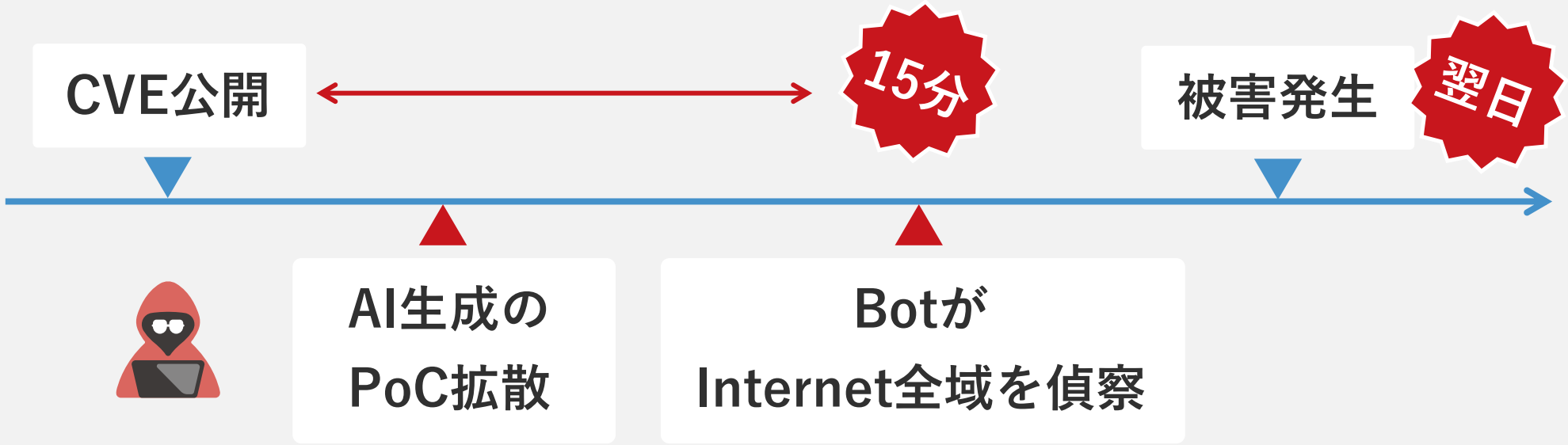
自動化

PoC / フィッシング生成



攻撃の作成コスト低下
誰でも攻撃可能な時代へ

“AI＆Bot”が攻撃を始めるまでの時間が短くなっている



2026年
現実の記録

- スキャン開始時間：CVE公開から「**15分**」以内が常態化 ※1
- 悪用開始までの平均：2024年の56日→2026年は「**10時間**」に短縮 ※2
- 実例：LiteLLM（CVE-2026-42208）公開から「**36時間**」で実攻撃を確認 ※3

出典：※1 Palo Alto Networks「2026 Unit 42 Global Incident Response Report」 ※2 Cyber Unit「CVE-to-Exploit Window Drops to 10 Hours in 2026」 ※3 SC Media「LiteLLM exploited within 36 hours of disclosure via SQL injection bug」

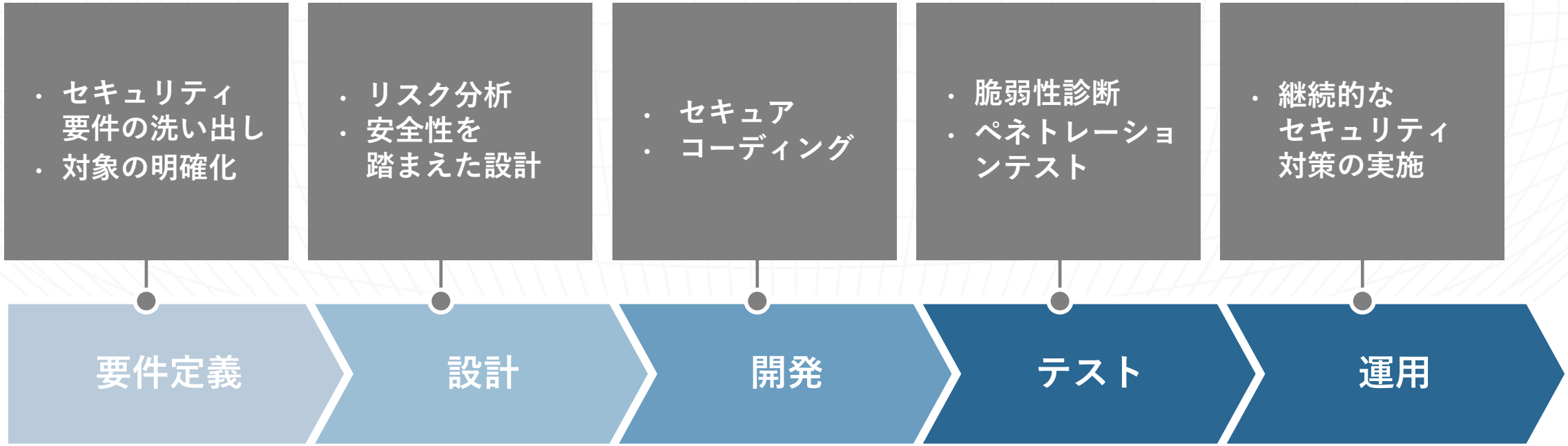
“セキュリティ”に求められていること

AeyeSecurityLab

システム開発にはセキュリティ・バイ・デザインが求められている

> *情報システムの企画工程から設計工程、開発工程、運用工程まで含めた*
> *全てのシステムライフサイクルにおいて、一貫したセキュリティを確保する方策*

参考：政府情報システムにおけるセキュリティ・バイ・デザインガイドライン（2024，デジタル庁）
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7e3e30b9/20240131_resources_standard_guidelines_guidelines_01.pdf

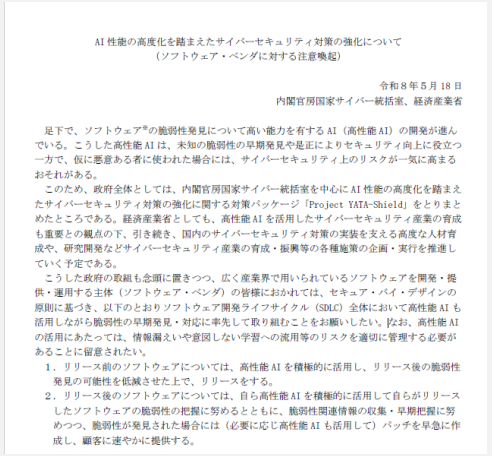


AeyeSecurityLab

政府指針でもセキュリティ強化の重要性が示されている

ソフトウェアを開発・提供・運用する主体は、
セキュア・バイ・デザインの原則に基づき、
開発ライフサイクルにおいて高性能AIも活用しながら
脆弱性の早期発見・対応に率先して取り組むこと

AI開発者/提供者にはセキュア・バイ・デザインを、
AI利用者には適切なセキュリティ対策を推奨



AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化について
（ソフトウェア・ベンダに対する注意喚起）

令和８年５月 18 日
内閣官房国家サイバー統括室、経済産業省

足下で、ソフトウェア※の脆弱性発見について高い能力を有する AI（高性能 AI）の開発が進んでいる。こうした高性能 AI は、未知の脆弱性の早期発見や是正によりセキュリティ向上に役立つ一方で、仮に悪意ある者に使われた場合には、サイバーセキュリティ上のリスクが一気に高まるおそれがある。

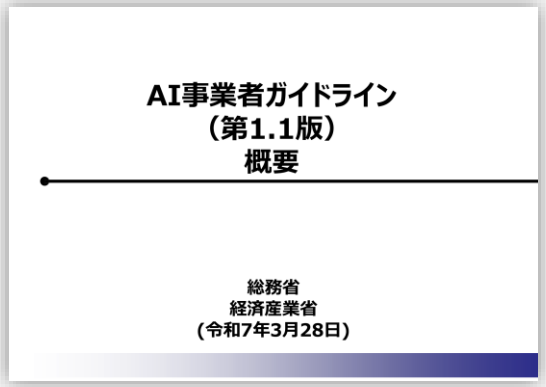
このため、政府全体としては、内閣官房国家サイバー統括室を中心に AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化に関する対策パッケージ「Project YATA-Shield」をとりまとめたところである。経済産業省としても、高性能 AI を活用したサイバーセキュリティ産業の育成も重要との観点の下、引き続き、国内のサイバーセキュリティ対策の実装を支える高度な人材育成や、研究開発などサイバーセキュリティ産業の育成・振興等の各種施策の企画・実行を推進していく予定である。

こうした政府の取組も念頭に置きつつ、広く産業界で用いられているソフトウェアを開発・提供・運用する主体（ソフトウェア・ベンダ）の皆様におかれては、セキュア・バイ・デザインの原則に基づき、以下のとおりソフトウェア開発ライフサイクル（SDLC）全体において高性能 AI も活用しながら脆弱性の早期発見・対応に率先して取り組むことをお願いしたい。なお、高性能 AI の活用にあたっては、情報漏えいや意図しない学習への流用等のリスクを適切に管理する必要があることに留意されたい。

1．リリース前のソフトウェアについては、高性能 AI を積極的に活用し、リリース後の脆弱性発見の可能性を低減させた上で、リリースをする。
2．リリース後のソフトウェアについては、自ら高性能 AI を積極的に活用して自らがリリースしたソフトウェアの脆弱性の把握に努めるとともに、脆弱性関連情報の収集・早期把握に努めつつ、脆弱性が発見された場合には（必要に応じ高性能 AI も活用して）パッチを早急に作成し、顧客に速やかに提供する。

国家サイバー統括室など

AI性能の高度化を踏まえた
サイバーセキュリティ対策の
強化について
（ソフトウェア・ベンダに対す
る注意喚起）



AI事業者ガイドライン
（第1.1版）
概要

総務省
経済産業省
（令和7年3月28日）

経産省・総務省

AI事業者ガイドライン
第1.1版 概要

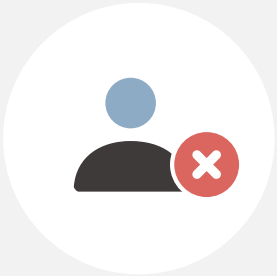
参考：国家サイバー統括室ほか「AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化について」：https://www.cyber.go.jp/pdf/press/20260518_AI_CS_software_vendor.pdf
総務省・経済産業省「AI事業者ガイドライン （第1.1版） 概要」：https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20250328_2.pdf

セキュリティ・バイ・デザインの実現を阻む 3つの課題

基準やルールが明確でない

概念自体が新たしく、規格やガイドライン等が少ない。
特に企画・設計段階では、何をどのくらいやれば十分なのか？を定義するのが難しい

専門人材の不足



施策全体を設計するためには、セキュリティ技術の専門性だけでなく、システム開発のライフサイクルなど幅広い知識・経験が必要。
適合する人材がなかなかいない

社内・関係者の理解が得にくい

既存の開発プロセスを大幅に変更する必要があり、特に開発ベンダー等が多重構造になっている等多くのステークホルダーが関わるシステムへの適用が大変

できることから「セキュリティ・バイ・デザイン」を始めるのも良い

← 何をすればいいか分かりづらい →　← 「できること・やるべきこと」が比較的分かりやすい →

ライフサイクルの後工程から、徐々に「セキュリティ・バイ・デザイン」を組み込んでいく

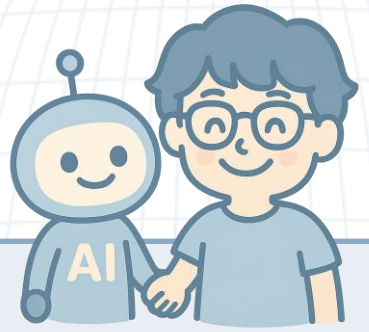
例えば、脆弱性対策なら…

“シフトレフト”で「セキュリティ・バイ・デザイン」を加速する

要件定義	設計	開発	テスト	運用
開発標準(コード規約) セキュリティ要件	データ保護設計 認証・認可設計	SAST(静的コード解析) SBOM/SCA 構成管理	DAST(動的脆弱性診断) ペネトレーション テスト	パッチ管理/適用 ログ監視/分析 ASM(攻撃面管理)

開発できたところから
早め・こまめに脆弱性診断

設計段階から
攻撃面の最小化を検討



人とAIの協働で「できることから」始める
セキュリティ・バイ・デザインを

生成AI時代の脆弱性診断なら AeyeScan

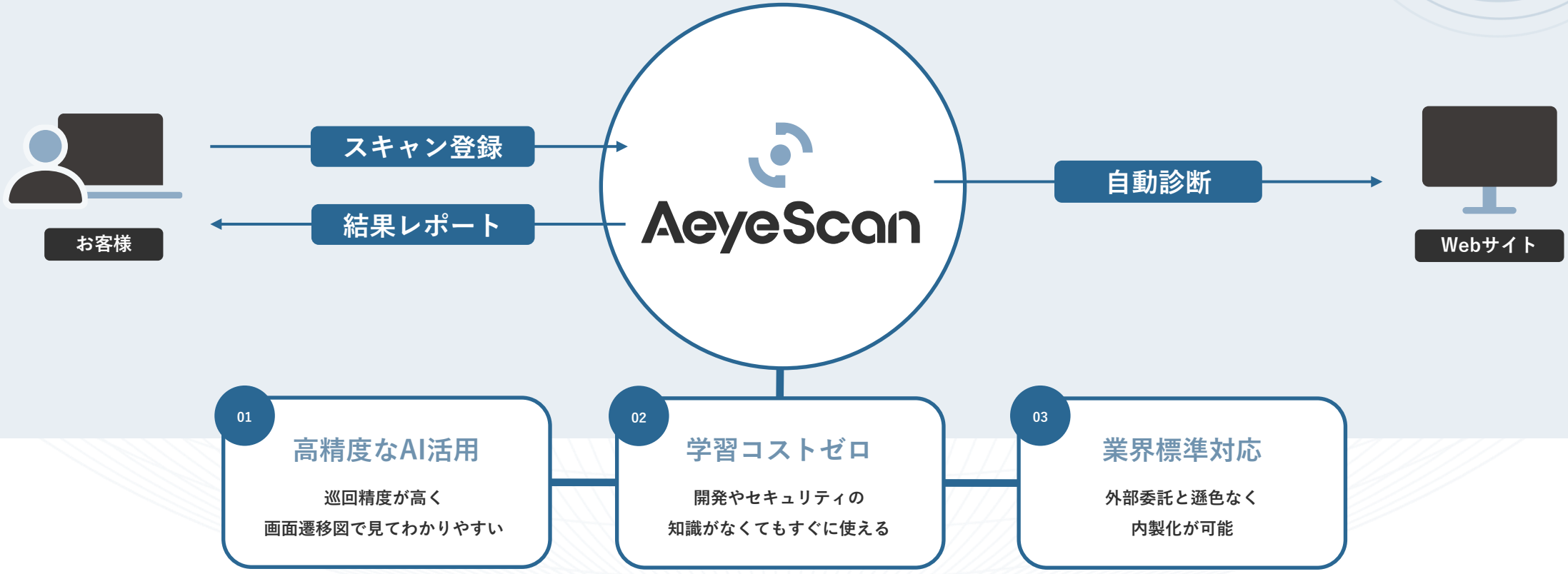
クラウド型Webアプリケーション
脆弱性検査ツール

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（2023年度実績）

有償契約
300社以上

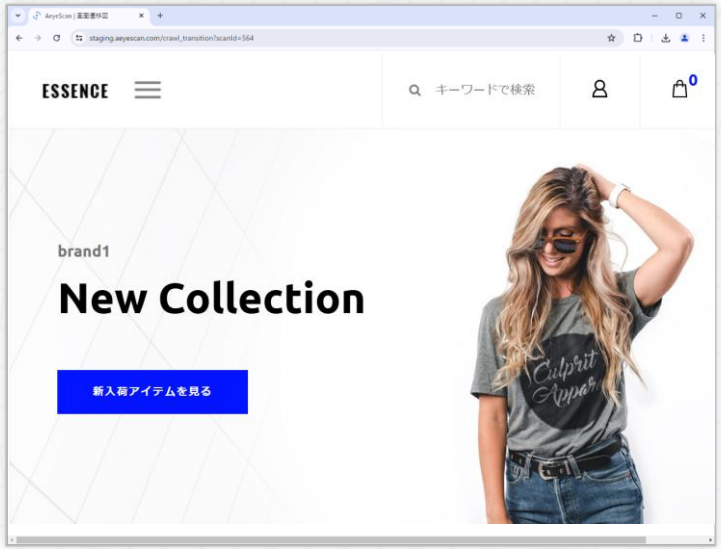


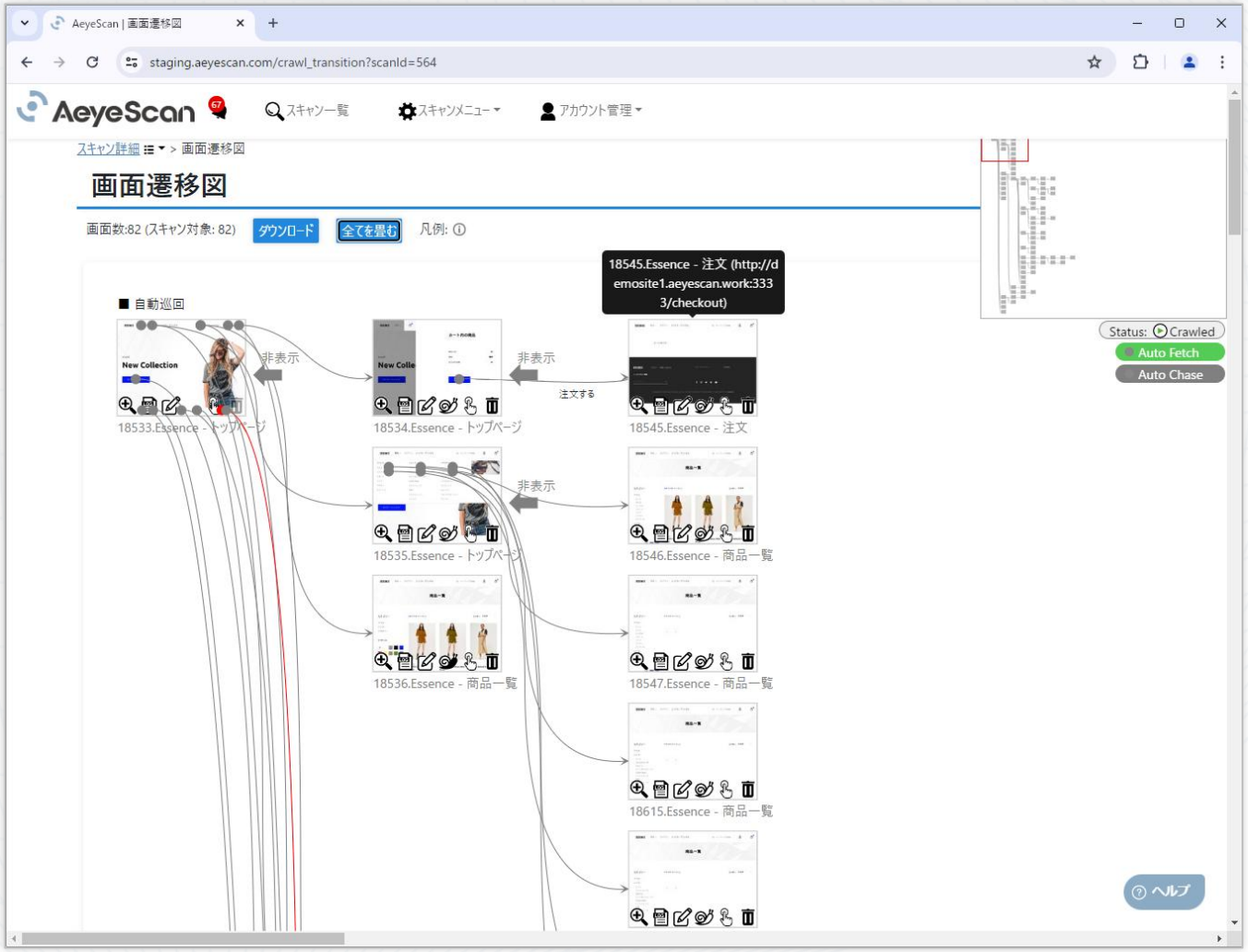
01
高精度なAI活用
巡回精度が高く
画面遷移図で見てわかりやすい

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

巡回時に、自動で画面遷移図を生成





AeyeSecurityLab

結果がわかりやすく、すぐさま修正作業に取り組めるレポート

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 / NTT EAST / odakyu / 近鉄情報システム株式会社 / GEO / SymEnergy / 水ing / Suzuyo / TOYOTA HOME / NANKAI / 日本調剤 / JARMeC / HITOWA GROUP / BOOK・OFF / ベルーナ / MEDIA / Looop / Loyalty Marketing, Inc.

エンタメ

イープラス / CAPCOM / GungHo / とらラボ! / BookLive

メディア

集英社 / 中日新聞 / NIKKEI / Media Do

製造

AICA / AISIN / KITZ / KOSÉ / SAKI / TIGER / TEIJIN / Denkei / House / Mizuno / ユーグレナ

金融

SOMPOひまわり生命 / MS&AD / MS&ADインターリスク総研 / JOBPAY / 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. / Lexica / M-aid / 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 / 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 / Human Interactive Technology inc. / FUJISOFT / FUJITSU / MACROMILL / YONA / リピスト

セキュリティ企業

NEC NECセキュリティ / NTT DATA / GSX / 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）

脆弱性診断プロセスの大部分を省力化できる

診断準備

- 対象調査
- 要件定義
- 環境準備
- 日程調整
  契約・発注

診断実行

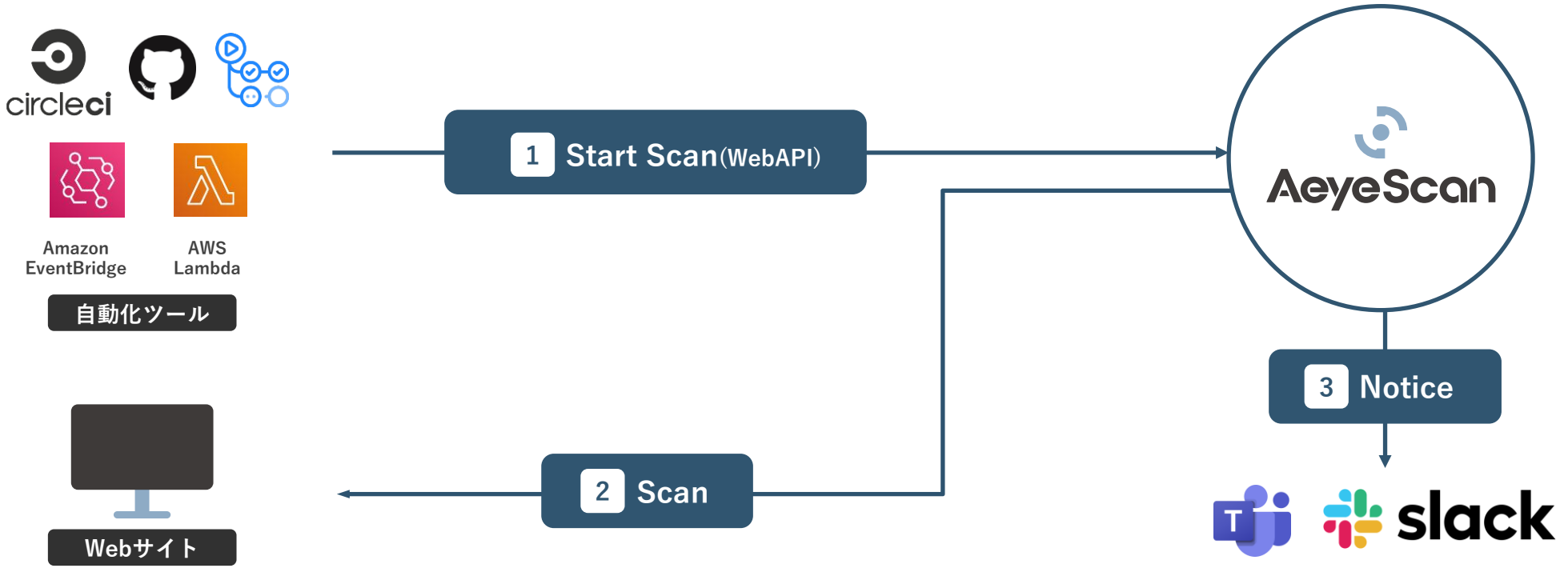
- シナリオ作成/サイト巡回
- 脆弱性診断
- 結果報告

修正対応

- トリアージ
- 修正対応
- 
- 再診断

アジャイル開発・高頻度リリースでも漏れなく診断

CI/CDに組み込むことで、リリースのたびに自動で診断が実行される仕組みづくりが可能に。
属人化を排除し、誰が開発しても一定のセキュリティを担保できる。



診断工数ほぼ半減を実現できたDevSecOps事例（Webサービス展開事業Rさま）

前提情報

- Webサービスを自社開発し、toC/toBで提供している
- 自社サービスのセキュリティ対策も、基本的には自社内で実施してきた
- 直近、新規事業領域に幅広くチャレンジしており、多角化が進んでいる

課題・きっかけ

- 事業拡大・システム数の増加に対して、セキュリティ対策の整備が追いつかない
- セキュリティテストの実施方法が部署ごとに異なり、全社共通の基準が存在していなかった
- 「性善説に基づいた運用」でセキュリティを度外視していたことも…

診断工数ほぼ半減を実現できたDevSecOps事例（Webサービス展開事業Rさま）

海外製のDASTツールを導入!!

初期設定が
複雑で
意図通りに
動作しない

診断結果の
精査が複雑

- 専門知識が必要
- 現場の負担が大きい

サポート窓口
の返信が
1か月かかる

▼

「内製化」に方針転換、「手動診断」をすすめるも新たな課題が

検知精度は高まる一方
多くの時間と人手を必要

全システムを1度診断するのに
１年半もかかってしまう状況

アジャイル開発体制では
人手に依存した運用には限界

➡ 担当者の工数負担が非常に大きいため、再度ツールの選定に乗り出す

診断工数ほぼ半減を実現できたDevSecOps事例（Webサービス展開事業Rさま）

「検知精度」が選定の決め手となり、「AeyeScan」を導入

- 他社製品と比べて検知精度が2倍ほどよかった
- ハッカーが仕掛けるような、実際の現場で発生し得る攻撃を疑似的に再現でき、効果的な診断が可能
- 従量課金制ではないため「いつでも・誰でも・好きなだけ」診断できる

AeyeScan導入の効果

診断結果を開発部門へ共有しやすくなった

・画像付きで検出箇所を表示
・対応策も記載されている

自動化により診断工数が約50%削減

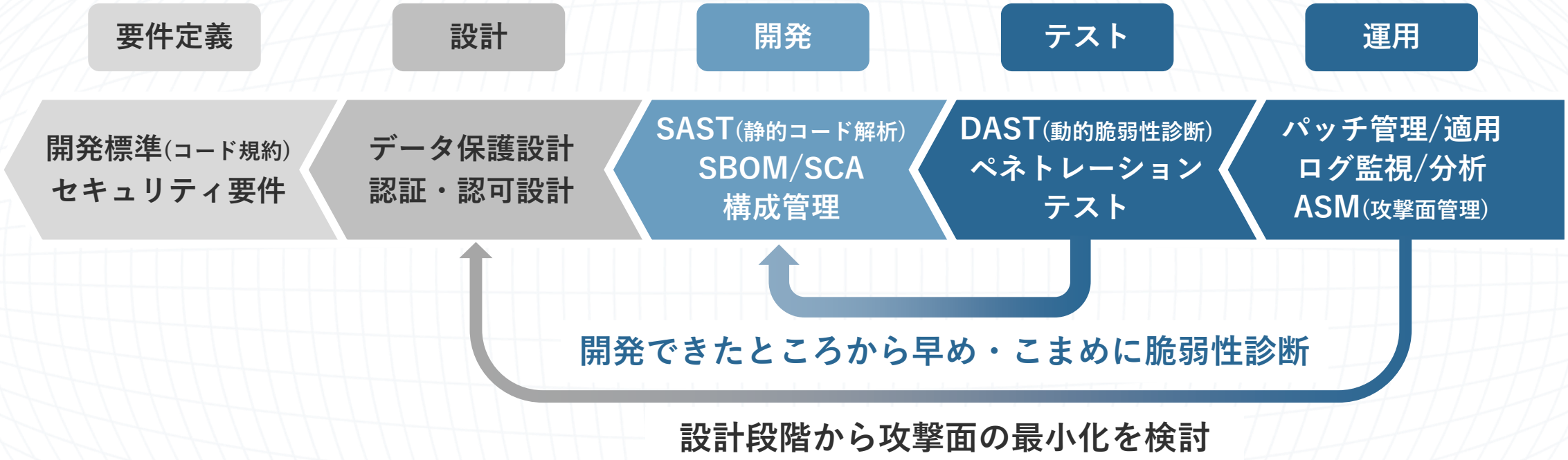
・複雑な初期設定が不要
・レポート精査の工数も削減

顧客への説明力が向上した

・主要なセキュリティ指標に対応
・継続的な実施も説明可能に

AeyeSecurityLab

できるところから「セキュリティ・バイ・デザイン」で“シフトレフト”



診断を自動化し、人はより創造的な業務へ。
現場で回す仕組みづくりを支援します。

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

AeyeSecurityLab

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向けに、
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！

AeyeScanデモ動画を視聴

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。

ハンズ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

セキュリティに、確かな答えを。