生成AI時代に必要な“確率論”と“決定論”の脆弱性対策

©AeyeSecurityLab Inc.

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。

©AeyeSecurityLab Inc.

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！



©AeyeSecurityLab Inc.

ととのう、セキュリティ

私たちは、AIの力でセキュリティ対策が無理なく回り続ける仕組みを提供し、専門部門だけに頼らず、チームで安全を支えられる状態をつくります。
本来の業務に集中しながら、事業が前に進み続ける世界を実現していきます。



AeyeSecurityLab

©AeyeSecurityLab Inc.

“確率論”と“決定論”
２つのセキュリティ対策

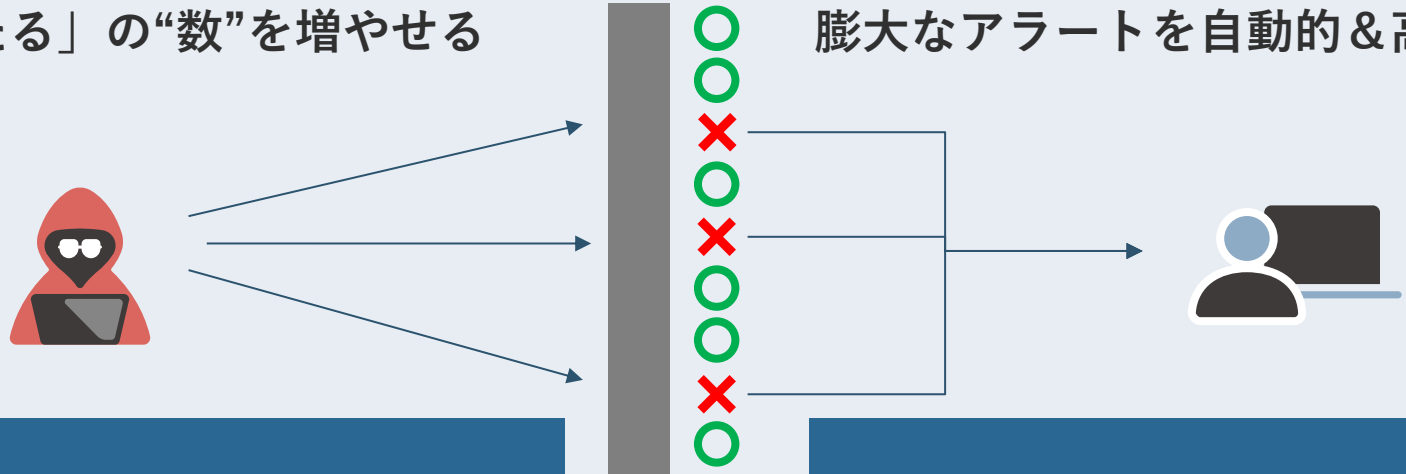
©AeyeSecurityLab Inc.

AIは、攻撃側と防御側のどちらに味方したか

サイバー攻撃の能力が飛躍的に向上した生成AIは、攻撃・防御の生産性を向上させた…？

攻撃側の生産性

「数打ちゃ当たる」の“数”を増やせる



１つでも攻撃が成功すれば “成功”なので
「点(突破口)」を見つけやすくなって嬉しい

防御側の生産性

膨大なアラートを自動的＆高度に分析できる

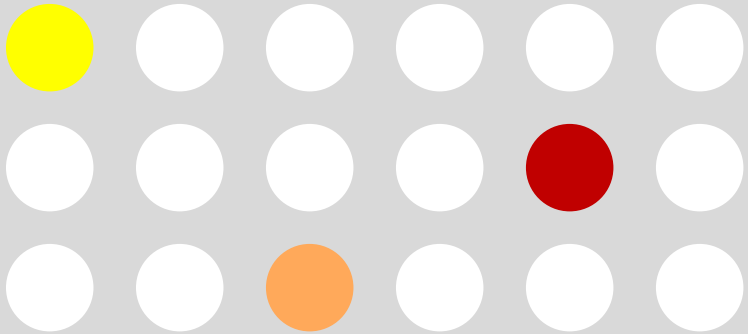
全ての攻撃を防ぎきらないといけないので
「点(異常値)」を見つけやすくなっても…

©AeyeSecurityLab Inc.

2つの混同が、AI投資・AIを利用したセキュリティ対策の失敗につながる

確率論的セキュリティ対策

当たりを探す・異常を見つける



最悪、ある程度は間違っていてもいいので
とにかく「当たり」「異常」を検知したい

➡ AIの得意領域

決定論的セキュリティ対策

問題ないことを確かめる



結果のブレや抜け漏れがあるとマズい
再現性・網羅性・説明可能性を担保したい

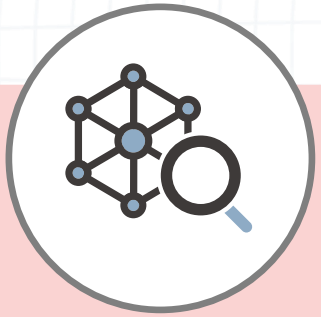
➡ AIの苦手領域

©AeyeSecurityLab Inc.

確率論的セキュリティ対策が「効く」領域

予測母数が巨大で、ノイズが多い領域：確率論的セキュリティ対策

AIが人間の能力を上回り、強みを発揮する➡AIに任せていきやすい



ASM

未把握の資産も含めて
自社資産を幅広く探索・監視



EDR/XDR

大量のイベント・ログから
怪しい動きを見つける



WAF/Bot検知

アクセスの特徴を分析し
Botらしさを判定する

©AeyeSecurityLab Inc.

決定論的セキュリティ対策が「必要」な領域

網羅性・再現性、証跡や説明が必要な領域：決定論的セキュリティ対策

AIを活用しながら、再現性・証跡を担保する仕組みが必要



脆弱性診断

疑似的な攻撃により
脆弱性の有無を確認する



SBOM

構成情報と脆弱性情報を
照らし合わせる



CSPM

権限・設定の誤りがないか
確認する

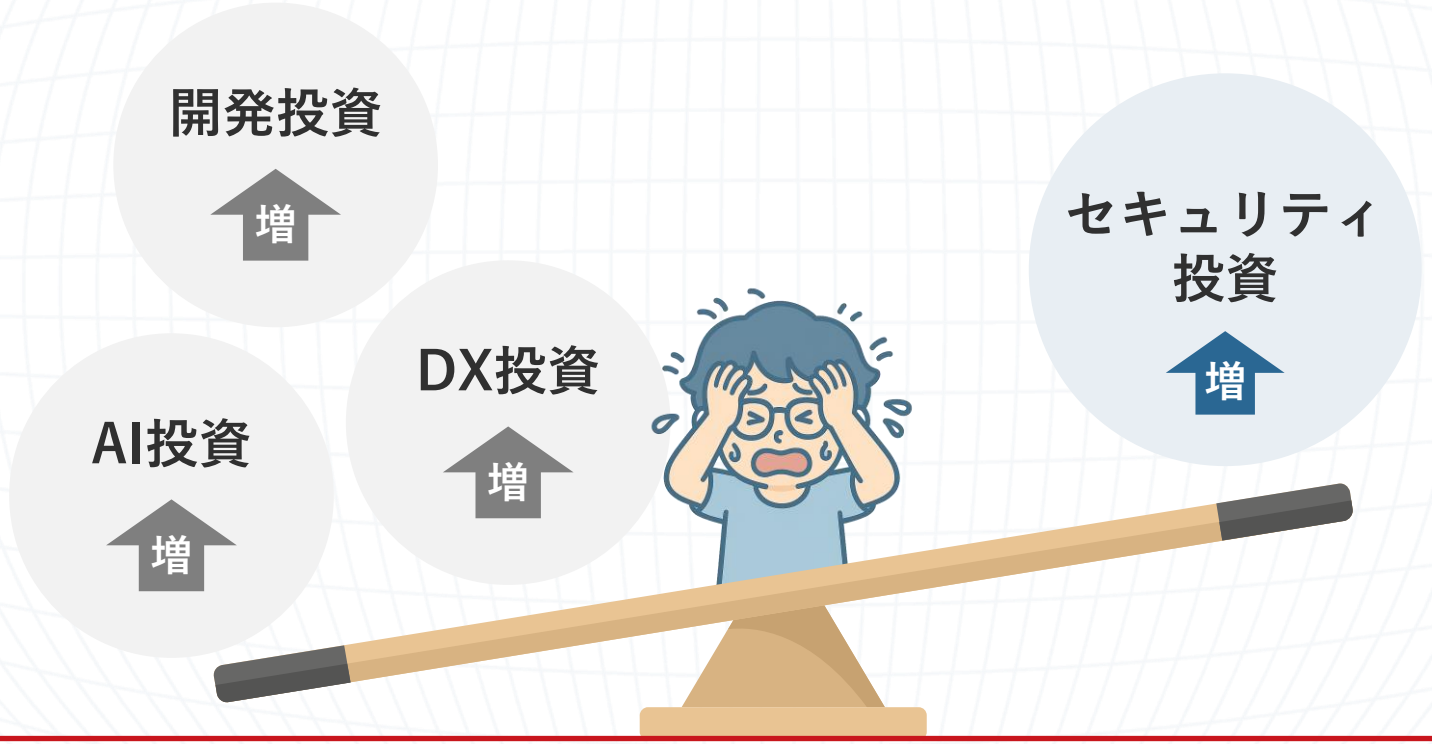
©AeyeSecurityLab Inc.

進化するAIに後れ(おく)を取らない「前提」となるセキュリティ対策

©AeyeSecurityLab Inc.

限界あるセキュリティ投資、際限ない「攻撃面」の増加

生成AI投資により開発が加速し、システムも複雑化。守るべき攻撃面は際限なく拡大している。



追加のセキュリティ投資には限界がある一方で、
攻撃面・脆弱性は際限なく広がっていく

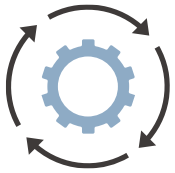
©AeyeSecurityLab Inc.

AI活用そのものが、脆弱性の混入機会を増やしている

AIによる開発の高速化

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

生成AIが作成したコードに
脆弱性が含まれている割合 **45%**

出典：https://www.veracode.com/blog/spring-2026-genai-code-security/

リファクタリングされている
コードの割合は直近4年間で **-70%**

出典：https://www.gitclear.com/the_ai_code_quality_maintainability_gap

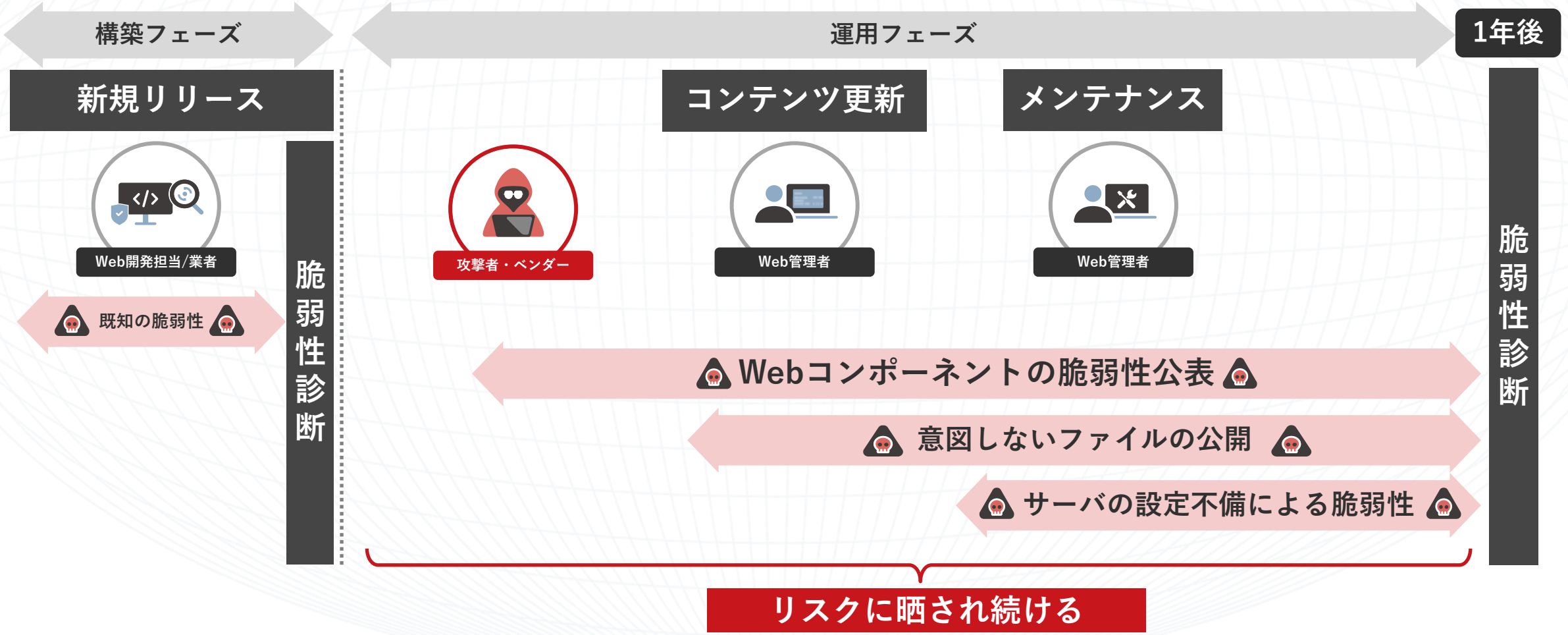
生成AIが作成したコードが
欠陥を含む可能性は人間の **2.74倍**

出典：https://forbesjapan.com/articles/detail/94209

©AeyeSecurityLab Inc.

年1回の脆弱性診断では追いつかない

開発リリースごと・脆弱性発見ごとにリスクは積み重なり、攻撃の隙を与え続けてしまう

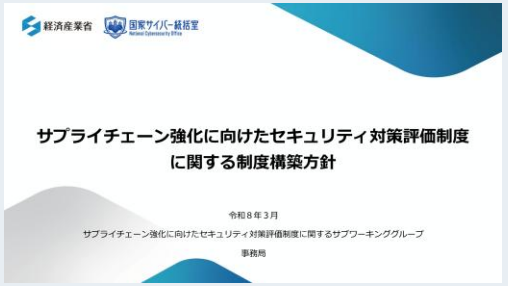


©AeyeSecurityLab Inc.

継続的なセキュリティ対策は「任意」から「前提」へ

セキュリティ対策は、“やるかどうか”ではなく“どう継続するか”が問われる段階に移行している

制度・ガイドライン



SCS評価制度



AI事業者ガイドライン

継続的な対策を前提に、
企業に求められる取り組みが具体化。

脅威・実務基準


情報セキュリティ10大脅威 2026

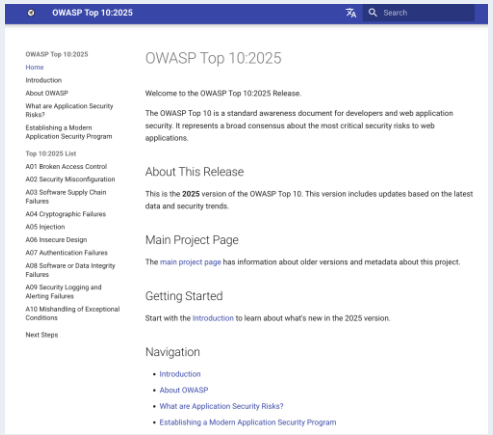
公開日：2026年1月29日
最終更新日：2026年5月21日

「情報セキュリティ10大脅威 2026」は、2025年に発生した社会的に影響が大きかった情報セキュリティの事故や攻撃の状況などから、IPAが脅威候補を選定し、情報セキュリティ分野の研究者、企業の実務担当者など約250名のメンバーからなる「10大脅威選考会」が審議・投票を経て決定したものです。
「組織」向け脅威については順位を併記し、「個人」向けでは脅威名のみを五十音順で記載しています。複数の脅威にまたがる事案もあるため、各自の環境に照らし退出された脅威については、相力もれなく対策を行うことが求められます。

◢ 情報セキュリティ10大脅威 2026［組織］

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサム攻撃による被害	2016年	11年連続11回目
2	サプライチェーンや委託先を狙った攻撃	2019年	8年連続8回目
3	AIの利用をめぐるサイバーリスク	2026年	初選出
4	システムの脆弱性を悪用した攻撃	2016年	6年連続9回目
5	機密情報を狙った標的型攻撃	2016年	11年連続11回目
6	地政学的リスクに起因するサイバー攻撃（情報戦を含む）	2025年	2年連続2回目
7	内部不正による情報漏えい等	2016年	11年連続11回目
8	リモートワーク等の環境や仕組みを狙った攻撃	2021年	6年連続6回目
9	DDoS攻撃（分散型サービス妨害攻撃）	2016年	2年連続7回目
10	ビジネスメール詐欺	2018年	9年連続9回目

情報セキュリティ
10大脅威2026



OWASP Top 10
2025

変化する脅威にあわせ、
確認すべきリスクも継続的に更新。

©AeyeSecurityLab Inc.

2つの対策、どう使い分けるか決めるのは「事業・経営」サイド

顧客や取引先、株主への説明責任がある以上、事業部門・経営層がリスク選好度を決める必要

どこまで「確率論」のリスクを許容できるか、明確に定める



事業リスクや影響度を踏まえ、どこまで「確率論的な対策」で効率化するのか、不確実性を許容するのか、決める。

説明可能性の担保が必要な領域を明確にして「決定論」を採る



取締役会・監査・顧客・取引先への説明責任を果たすには「決定論的な対策」による再現性・証跡が必要となる。

©AeyeSecurityLab Inc.

「決定論的セキュリティ対策」の条件
解決策としての“内製化”

©AeyeSecurityLab Inc.

決定論的なセキュリティ対策の3条件

網羅性

すべての対象を
漏れなく診断できる



再現性

誰でも実施できて、誰でも
同じ結果が得られる



証跡

第三者に提示可能な
客観的記録を残せる





限りある予算・人員・時間の中で
これらの条件を全て満たすには、どうすればいいのか？

©AeyeSecurityLab Inc.

「いつでも・誰でも・好きなだけ」診断できる環境をつくれば解決する

時・人・量の制約が解消できて、はじめて、決定論的セキュリティ対策は運用に乗る。

「内製化できればいいんだけどな…」



診断の**品質を維持**できるだろうか？

診断員を**育成・確保**できるだろうか？

コスト(費用・時間)を削減できるか？

©AeyeSecurityLab Inc.

「いつでも・誰でも・好きなだけ」診断できる環境をつくれば解決する

診断の**品質を維持**できるだろうか？

診断員を**育成・確保**できるだろうか？

コスト(費用・時間)を削減できるか？

プロ級の機能・性能



誤検知・過検知が少なく
外部委託（手動診断）に近い性能

誰でも使える操作性



ツール習得コストがかからず
すぐに・簡単に利用できる

利用範囲・回数が無制限

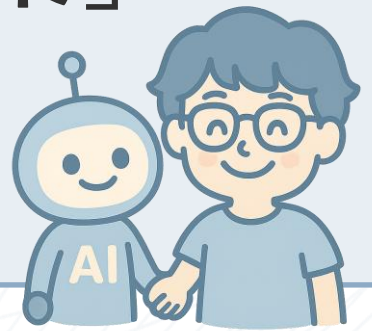


画面数やサイト数に制限がなく
いつでも・いくらでも使える

©AeyeSecurityLab Inc.

AIと

Web診断の内製化で「決定論的サイバーセキュリティ対策」の実現を支援します！



©AeyeSecurityLab Inc.

生成AI時代の脆弱性診断なら AeyeScan

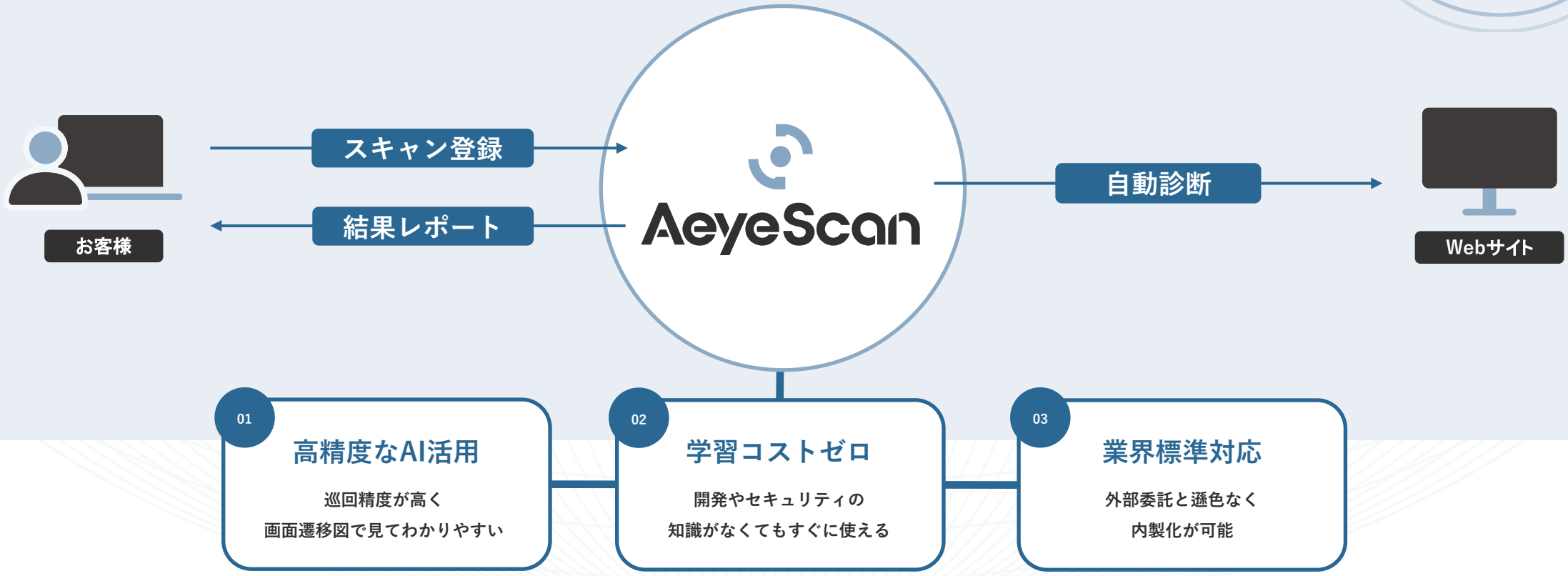
クラウド型Webアプリケーション
脆弱性検査ツール

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
500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

©AeyeSecurityLab Inc.

AeyeSecurityLab

AeyeScanが選ばれている理由



誰でもかんたん操作

開発やセキュリティの知識がなくても、
トレーニングなしで診断可能。



AIによる自動診断

圧倒的な巡回精度で
24時間自動で診断。
画面遷移図で状況を可視化。

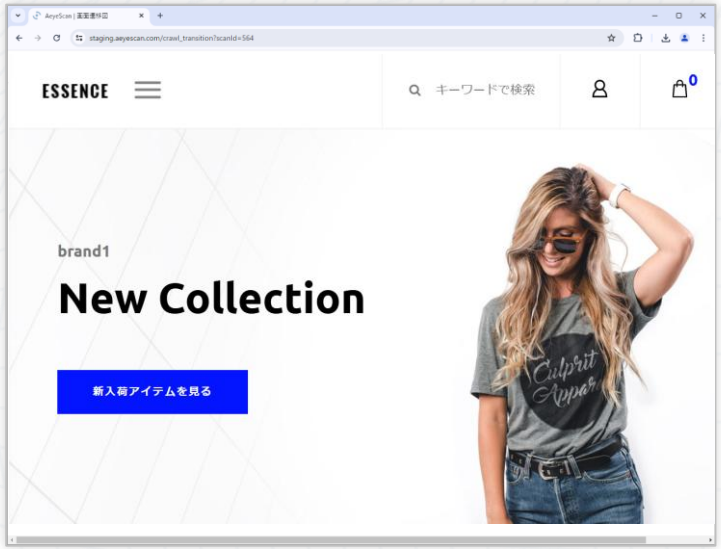


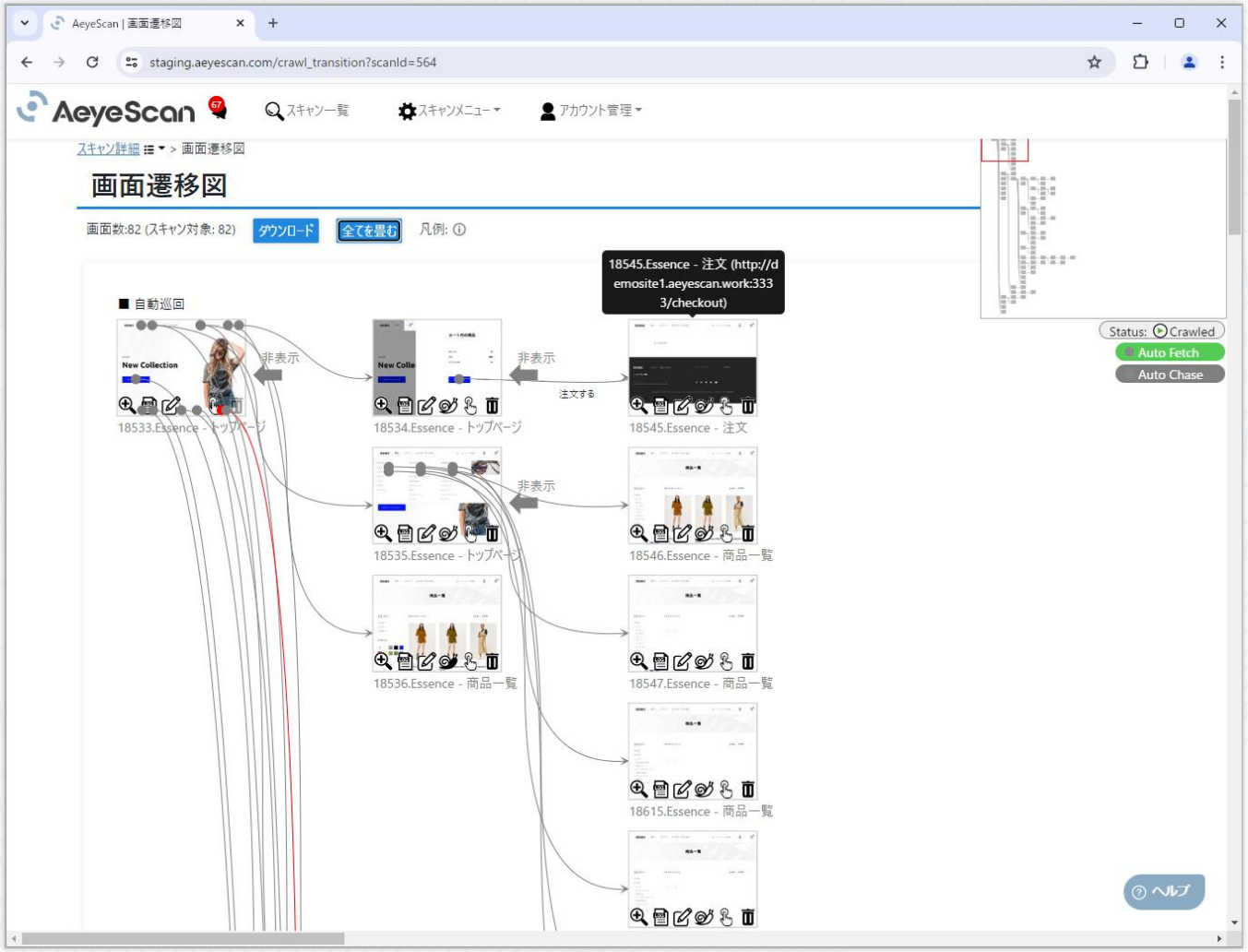
わかりやすいレポート

各種ガイドラインに準拠した
プロ仕様のレポート出力、
日本語と英語に対応。

©AeyeSecurityLab Inc.

巡回時に、自動で画面遷移図を生成





©AeyeSecurityLab Inc.

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





©AeyeSecurityLab Inc.

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

©AeyeSecurityLab Inc.

AeyeSecurityLab

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 / H.I.S. / 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 / 東海テレビ / NIKKEI / Media Do

製造

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

金融

セブン-イレブン / UPSIDER / 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. / Lexica / エフアンドエムネット株式会社 / 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 / 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）

会社名及びロゴは各社の商標または登録商標です

©AeyeSecurityLab Inc.

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 Inc.

AeyeSecurityLab

定期開催中！ AeyeScanがよく分かるデモ動画・セミナー

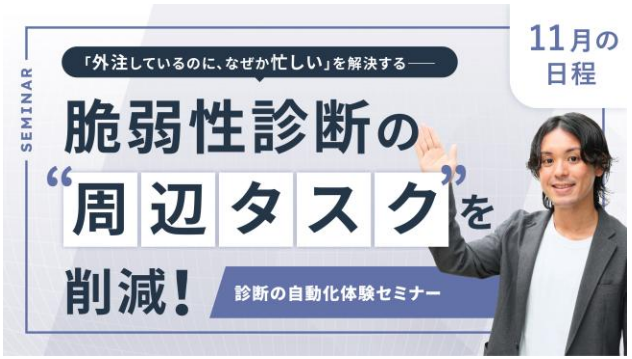
AeyeScanを検討してみたい方へ



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！

デミセミナーの日程を確認

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。

ハンス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

©AeyeSecurityLab Inc.



セキュリティに、確かな答えを。

©AeyeSecurityLab Inc.