
フロンティアAI時代

脆弱性対策はどうなる？

進化する攻撃に追従する
これからの防御アプローチとは

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、CSIRTや開発現場でのセキュリティ推進を経て、2020年6月より現職。
AeyeScanカスタマーサクセス責任者として診断の内製化を支援し、2026年度より開発責任者に就任。顧客の声を反映したプロダクトの進化を牽引している。大規模イベント等の講演多数。『セキュリティエンジニアの知識地図』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

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。

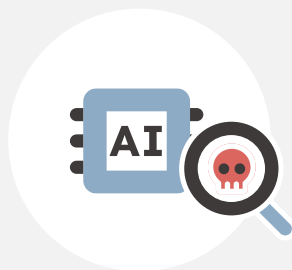


AIの進化がもたらす「セキュリティ常識」の変革

「Claude Mythos Preview」をはじめとするフロンティアAI（自律型AI）の登場により、AIの性能は急速に進化しています。

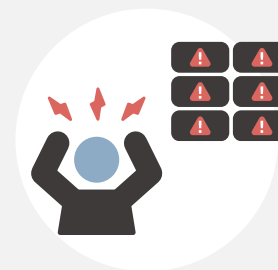
フロンティアAIの進化がもたらす脅威

脆弱性発見から攻撃までの
スピードが劇的にアップ



最新の攻撃手法（ゼロデイ/Nデイ）を取り込み、人間を遥かに凌駕する速度で次々と脆弱性を突き、悪用する能力を持つ。

従来の人間中心の対策では
対応困難な時代へ



少ない工数で攻撃の成否を判断できるため、攻撃サイクルが超高速化。脆弱性を放置できる猶予はゼロに。

攻撃と防御の圧倒的な非対称性が課題に

攻撃側はフロンティアAIを使って一箇所の穴を見つけてきますが、防御側は一箇所の穴が致命傷になるため、「全体」を網羅し続ける必要があります。

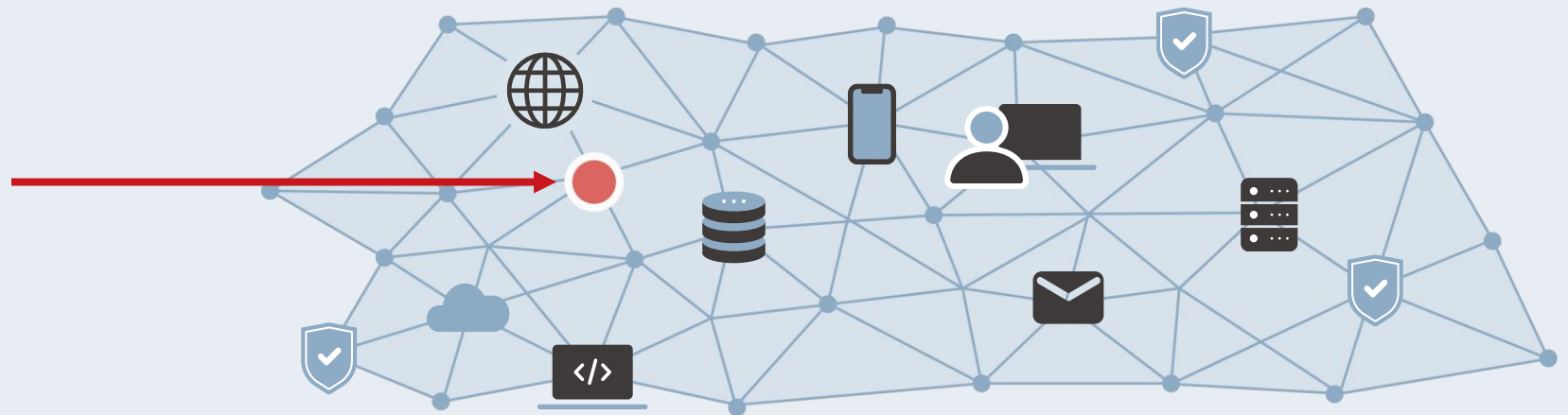
攻撃側

「点（脆弱性）」を
ピンポイントで突き抜ける
能力が高度化



防御側

「面（システム全体）」を常に取り続けなければならない



この「網羅性の欠如」こそが、フロンティアAI時代における防御の最大の弱点となっています



では、防御側も
フロンティアAIを使えばいいのでは？

フロンティアAIで高性能な防御ができるという誤解

フロンティアAIは脆弱性検知を高速化しますが、「網羅性の向上（穴をゼロにする）」は構造上難しいのが現状。

誤解 1

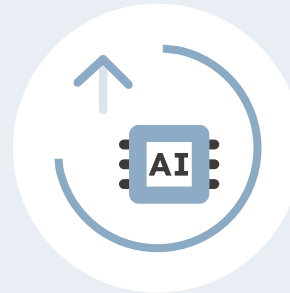


脆弱性がなくなるまで
全自動で診断してくれる？

フロンティアAIが知っているのは、
世界で公開済みの脆弱性や攻撃手法のみ。
自ら全自動で脆弱性がなくなるまで
診断計画を立ててはくれない。

※「AIが未知の脆弱性を発見」というニュースは、AIを駆使して「専門家が」発見しています

誤解 2



フロンティアAIモデルが
進化すれば網羅性も高まる？

システム全体の「網羅性」は学習で
強化できず、“AIモデルの進化”とは
無関係。AIが進化しても、
診断の網羅性は100%にならない。

米国の主要なセキュリティ研究※の
結果から見ても、フロンティアAI
単体で「穴をゼロ」にするのは困難

※LLMを用いた自動脆弱性診断の評価テスト等

脆弱性発見率 約50～70%
→ 3～5割は見落とす可能性

誤検知（偽陽性）も多く発生
→ 人による確認・仕分けが必要

フロンティアAIによる脆弱性診断の限界

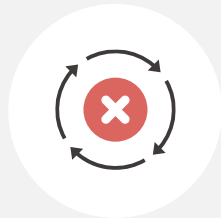
フロンティアAIのベースである大規模言語モデル（LLM）は、「ふさわしいテキストを確率で選んで返す」仕組みであるため、診断の正しさを担保する上でも限界があります。

セーフガードにより
診断が制限される



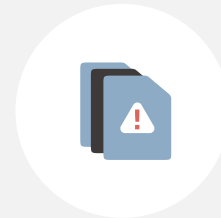
攻撃と判定される処理は、
モデルによっては拒否・
制限される場合がある。

再現性がなく
精度が担保できない



診断手法が正しいかを検証
してはならず、診断のたびに
手法がブレる。

コンテキストに
誤りが蓄積する



指示修正が追記で行われる
ため、必要な記憶が抜け、
結果に影響を及ぼす。

情報収集（巡回）に
限界がある

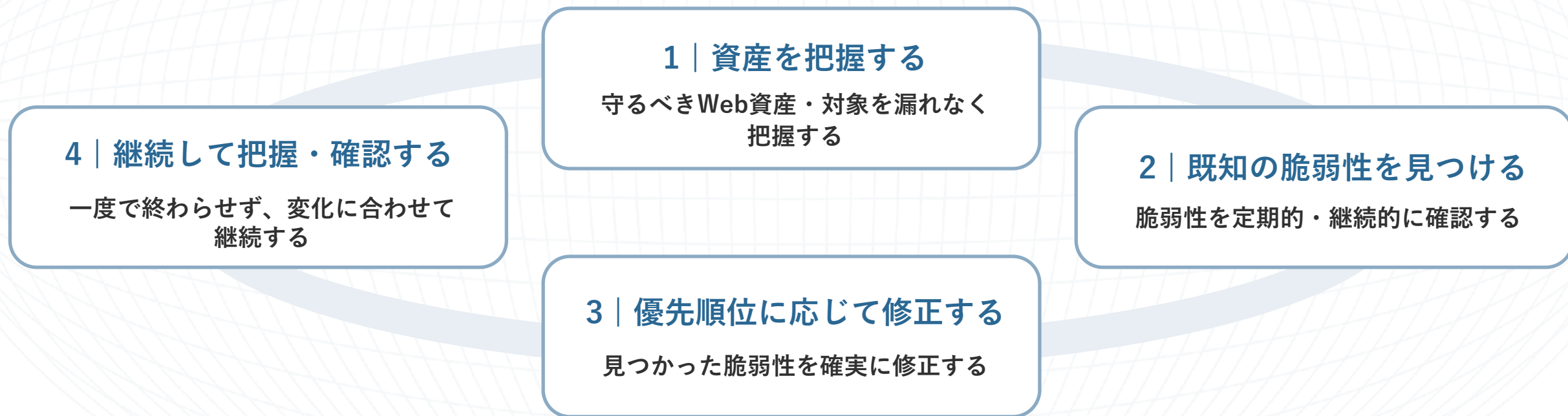


確率任せなので、巡回が早ず
ぎる切り上げ(見落とし)や堂々
巡り(時間切れ)に陥りやすい。

無理に現場で使おうとすると、かえって専門家の補完＝属人化が発生

「フロンティアAI時代だからこそ立ち返るべき「基本の徹底」

新しい攻撃手法への対応や高度な防御策に目を奪われがちですが、まず重要なのは、すでに分かっている脆弱性を確実に残さないという「当たり前の対策」です。



新しい攻撃手法を追いかける前に、まずは既知のリスクを残さない仕組みづくりを

必要な防御とは、「網羅的で地道な継続診断」

これから防御に必要なのは、フロンティアAIモデルの進化ではなく、システム全体を網羅的に潰す地道で継続的な診断だと言えます。

網羅性

全画面・全サイトを
網羅的に診断



認証後の画面も含め、
診断対象を漏れなく確認

再現性

同じ基準で
繰り返し診断



担当者や実施タイミングによらず、
一定の基準で実施

継続性

低コスト・低工数で
継続



人に依存せず、必要なタイミングで
繰り返し実施

「網羅性・再現性・継続性」のある診断を、攻撃に追従させる仕組みが必要

診断対象の拡大による「コスト増」への対抗策

攻撃が高速化・自動化するAI時代においては、「すべてのサイト・すべての画面」を網羅的に診断する（面で対策する）ことが必須となり、それだけセキュリティコストや手間が嵩む時代に突入しています。

AI時代に備えた「セキュリティ体制・予算」をつくる

「かかる費用の理解」とコストの最適化

AI活用による自動化で
脆弱性診断のコストと工数を抑える



予算や人材には限りがあるため、既存対策である
「脆弱性診断」は自動化し、コストを最適化

限られた予算と人材を
未知のリスクへの備えに集中投資



脆弱性診断のコストを抑えることで、限られた
予算と人材を本当に必要なところに回す

【結論】 防御に必要なのは、セキュリティ専用AI

フロンティアAI時代の防御に必要なのは、汎用的なフロンティアAIで対抗することではなく、Web巡回・脆弱性診断に特化し、「網羅性・再現性・継続性」を仕組みで担保できるセキュリティ専用AIです。



**確実なロジックで
脆弱性診断を自動化**

攻撃速度に追従し
自ら探索・診断・判断できる



**URLを設定するだけで
自動巡回**

Web巡回・認証突破・動的診断に
対応した知識と機能を持つ



**専門知識や
プロンプトスキル不要**

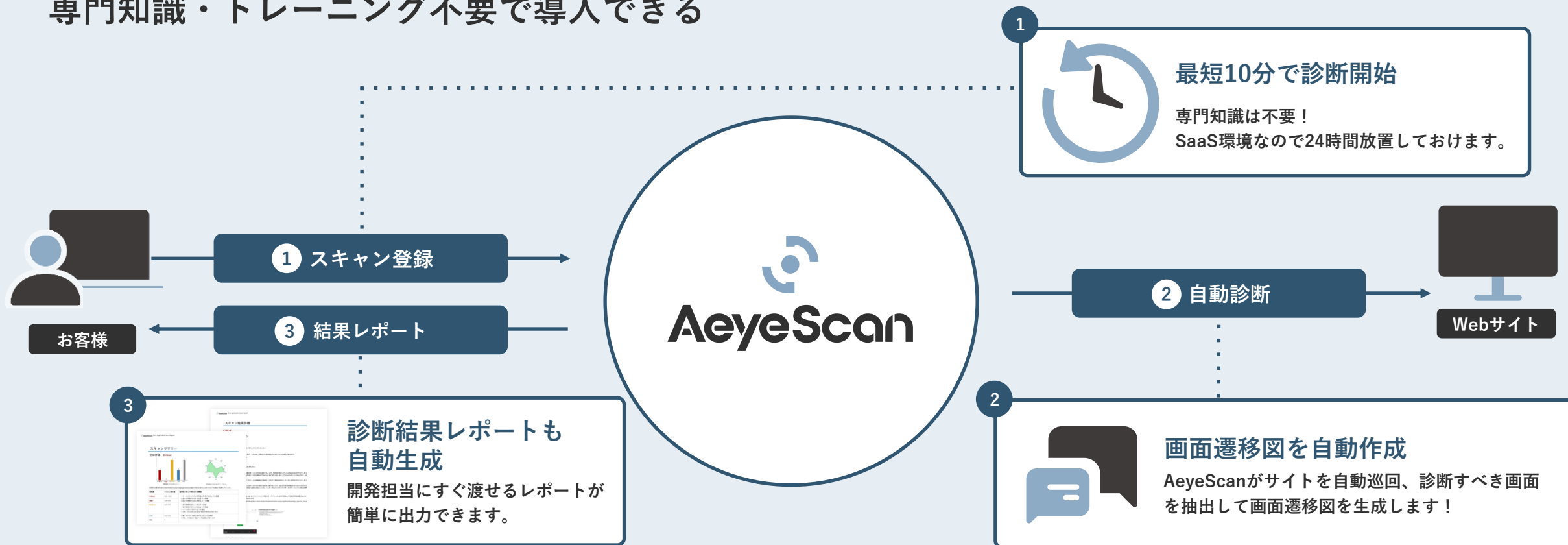
学習コストゼロで現場で使え
継続運用できる

基本の対策を自動化することで、コストの最適化ができる

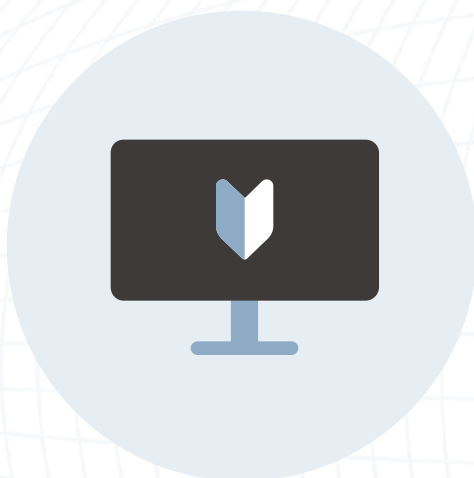
セキュリティ専用AIなら クラウド型Webアプリケーション脆弱性診断ツール「AeyeScan」

学習コストゼロ！

専門知識・トレーニング不要で導入できる



| 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。

 **AeyeScan** (エーアイスキャン) により
セキュリティ対策にかかる **コストを削減!**



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※



有償契約
300社以上

※ 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）

プロが認める品質・精度

セキュリティベンダーやSIerでも
顧客向けサービスとして活用



ブラウザ上での直感的な操作

専任エンジニア不要、情シスや開発部門でも
安定した運用が可能

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※



エンタメ



メディア



製造



金融



人材・教育



SaaS



SI・IT企業



セキュリティ企業



※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

フロンティアAI時代に必要な「面」の防御を、迅速かつ低コストで実施

専門家品質の高精度な脆弱性診断を、仕組みとして自動化。

フロンティアAIでは難しい網羅的・再現性のある自動診断が、社内に必要なタイミングに実施できます。

網羅的な「面」の
防御ができる



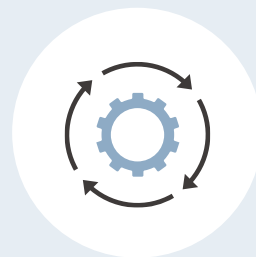
認証機能のある画面も
自動巡回して網羅性を担保

属人化せず、現場で
運用できる



非エンジニアでも
簡単な操作で実施できる

仕組み化で
無理なく継続できる



開発プロセスに組み込み
自然に実行される仕組みへ

コストと工数を
最適化できる



外注による診断と比較して
コスト・工数を削減

＼無料・定期開催中／

さまざまなテーマで情報収集をしたい方へ



事例と対策ノウハウをご紹介します！
毎月あたらしいテーマで学べるウェビナーをご用意

AeyeScanにご関心をお寄せいただいた方へ



いつでも見られるデモ動画を公開中！
オンサイトで実際に体験できるセミナーも

詳細はこちらから！気になるテーマをぜひお探しく下さい

詳細・お申し込みはこちら



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か？
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





AeyeScan

セキュリティに、確かな答えを。