Mythosショックで変わる

脆弱性診断の新常識

登壇者紹介

株式会社エーアイセキュリティラボ

CX本部マーケティングマネージャー　**長谷川　由利子**

生産管理パッケージメーカーにてCSに3年従事。2018年より、Ｓｋｙ株式会社にてセキュリティ製品の研修・セミナーの企画立案や講師を担当。 通算300回以上のセミナー・研修を実施し、組織のセキュリティリテラシー向上を支援。
2023年より株式会社エーアイセキュリティラボに参画。マーケティングマネージャーとして、AIを活用したクラウド型Webアプリケーション脆弱性診断ツール「AeyeScan」の顧客ロイヤリティ向上を牽引。企業の「Webセキュリティ対策」や「脆弱性診断の内製化・自動化」をテーマとしたセミナーの企画を数多く手掛ける。Podcast「ゆるセキュ。」のパーソナリティ兼運営も務める。

＼Podcast「ゆるセキュ。」のフォローをお願いします／

株式会社エーアイセキュリティラボ

CX本部マーケティングマネージャー　長谷川　由利子

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

AeyeSecurityLab

誰でも簡単に

プロさながらの高度な

脆弱性診断を

AeyeScan

Mythosショックで変わる

脆弱性診断の新常識

「Claude Mythos Preview」の衝撃

セキュリティ業界だけでなくビジネス界全体で、Anthropic（アンソロピック）社が発表した最新AI「Claude Mythos Preview（クロード・ミュトス・プレビュー）」が大きな注目を集めています。

「Claude Mythos Preview」の概要

目的

未知の脆弱性発見を人力からAI主体へ転換

従来は人間のスキルと長時間の手動検証が必要だった

従来のAIとの違い

生成AIから、“自律型サイバーAI”へ進化

人間の指示待ちではなく、自ら探索・判断・検証を行う

性能

人間を凌駕する速度で発見・検証

何十年も潜んでいた未知の脆弱性（ゼロデイ）を高速・自律的に見つける

高性能AIによって、サイバー攻撃は大きく変化する

「Claude Fable 5」公開・停止・再開が示した現実

高性能AIモデルの公開・停止・再開が短期間で起きるなど、AIの能力向上は安全対策や規制のあり方にも影響を与え始めています。

Anthropic社の高性能AI「Claude Fable 5」をめぐるドタバタ

公開

高性能モデル
「Claude Fable 5」を公開

高度な推論・開発支援を行う
高性能モデルとして公開

停止

安全保障上の懸念から
全ユーザー利用停止に

安全対策をすり抜ける
手口の報告を受け停止

再開

安全対策を強化し
再び提供を開始

報告された手口を検知する
改良版の分類器を開発

AIの進化は、モデルの性能だけでなく「どう安全に使わせるか」まで問う段階へ

高性能AIを悪用した攻撃は、過去の「延長線」にある

AIを使って脆弱性を発見する取り組みは数年前から存在しており、「AIを悪用したサイバー攻撃」も過去から着実に進化を続けてきた歴史の延長線にあります。

Phase1

AI＝効率化ツール

- フィッシングメール自動作成
- マルウェア量産
- ディープフェイク詐欺

攻撃作業の自動化

Phase2

AI＝探索支援

- 脆弱性候補の洗い出し
- コード解析支援
- 攻撃シナリオ生成

攻撃判断の高速化

Phase3

自律型サイバーAI

- AIによる自律的な探索
- 脆弱性の発見/検証
- 攻撃まで高速実行

攻撃そのものの自律化

高性能AI時代、セキュリティは「継続運用」が前提に

高性能 AI が攻撃者に悪用されることにより、脆弱性の発見から悪用までの時間は急速に短縮。
企業には継続運用を前提とした防御体制が求められています。

攻撃者×高性能AI

- 脆弱性発見が高速化
- 悪用までの時間が短縮
- 同時多発的な攻撃が増加

AIにより攻撃サイクルが高速化

企業×継続運用

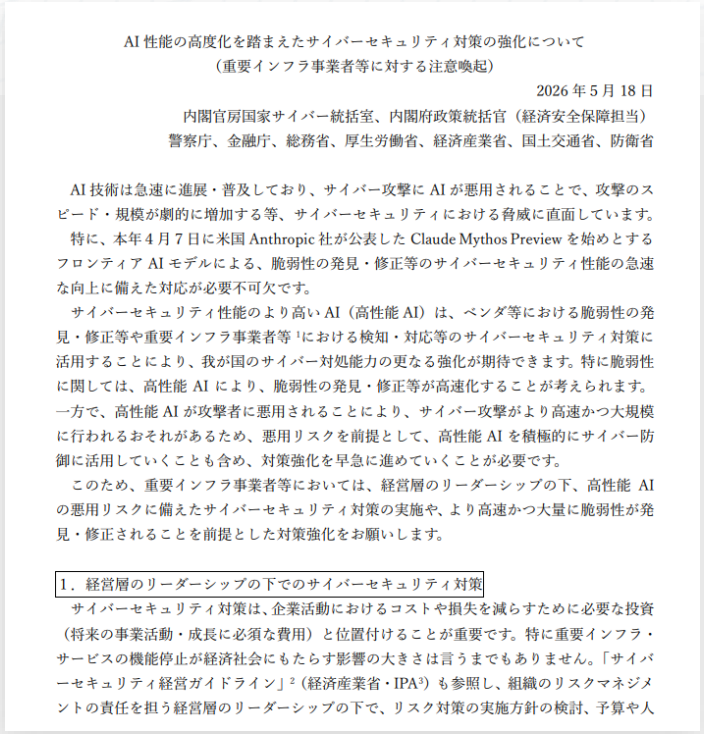
- 継続的な資産管理
- 脆弱性情報の収集
- リスク評価
- 優先順位付け
- 継続的な修正対応

継続的な脆弱性管理体制が必要

参考：「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_Critical_Infrastructure.pdf

政府も高性能AI時代への前提変更を始めている

内閣官房の「国家サイバー統括室」は、 Anthropic社の「Claude Mythos Preview」の登場を念頭に、政府全体の対策パッケージ『Project YATA-Shield』を取りまとめました。



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
（重要インフラ事業者等に対する注意喚起）

2026 年 5 月 18 日
内閣官房国家サイバー統括室、内閣府政策統括官（経済安全保障担当）
警察庁、金融庁、総務省、厚生労働省、経済産業省、国土交通省、防衛省

AI 技術は急速に進展・普及しており、サイバー攻撃に AI が悪用されることで、攻撃のスピード・規模が劇的に増加する等、サイバーセキュリティにおける脅威に直面しています。
特に、本年 4 月 7 日に米国 Anthropic 社が公表した Claude Mythos Preview を始めとするフロンティア AI モデルによる、脆弱性の発見・修正等のサイバーセキュリティ性能の急速な向上に備えた対応が必要不可欠です。
サイバーセキュリティ性能のより高い AI（高性能 AI）は、ベンダ等における脆弱性の発見・修正等や重要インフラ事業者等[1]における検知・対応等のサイバーセキュリティ対策に活用することにより、我が国のサイバー対処能力の更なる強化が期待できます。特に脆弱性に関しては、高性能 AI により、脆弱性の発見・修正等が高速化することが考えられます。
一方で、高性能 AI が攻撃者に悪用されることにより、サイバー攻撃がより高速かつ大規模に行われるおそれがあるため、悪用リスクを前提として、高性能 AI を積極的にサイバー防御に活用していくことも含め、対策強化を早急に進めていくことが必要です。
このため、重要インフラ事業者等においては、経営層のリーダーシップの下、高性能 AI の悪用リスクに備えたサイバーセキュリティ対策の実施や、より高速かつ大量に脆弱性が発見・修正されることを前提とした対策強化をお願いします。

1．経営層のリーダーシップの下でのサイバーセキュリティ対策
サイバーセキュリティ対策は、企業活動におけるコストや損失を減らすために必要な投資（将来の事業活動・成長に必須な費用）と位置付けることが重要です。特に重要インフラ・サービスの機能停止が経済社会にもたらす影響の大きさは言うまでもありません。「サイバーセキュリティ経営ガイドライン」[2]（経済産業省・IPA[3]）も参照し、組織のリスクマネジメントの責任を担う経営層のリーダーシップの下で、リスク対策の実施方針の検討、予算や人

ポイント

1. **経営層のリーダーシップの下でのサイバーセキュリティ対策**
   セキュリティを必要投資と捉え、予算・人材確保・リスク管理を実施
2. **基本的なサイバーセキュリティ対策の確実な実施及び更なる対策の強化**
   基本対策に加え、ゼロトラスト・脅威検知・AI活用など対策を強化
3. **高性能AIにより高速化する脆弱性の発見・修正等への対応**
   継続的な脆弱性対応と資産管理、リスク評価・優先順位付けを実施

参考：「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_Critical_Infrastructure.pdf

攻撃者がAIを使うなら、守る側もAIを使うのは「当然の前提」

人間の手作業や、年1～2回の定期的な脆弱性診断（手動）だけで、24時間365日休みなく進化・巡回し続ける攻撃者に対抗することは、物理的に不可能です。

攻撃者×高性能AI

- 24時間365日の攻撃
- 自律的に探索/攻撃

企業×継続運用

- 年1、2回の定期診断
- 人力で時間をかけて作業

人力前提の防御は、すでに限界を超えている

では、汎用AIによる社内診断で防御はできるのか

防御側も、AIを使わなければ太刀打ちできなくなっていはいるものの、汎用AI（LLM）を使った社内診断だけでWebアプリケーションを守ることは不可能といえます。

汎用AIによる社内診断の限界

静的ソースコードしかレビューできない

実際の攻撃は
動的環境で行われる

嘘や誤検知・見落としがある

誤った回答を
出力することがある

プロンプトスキルが属人化する

専門家による
チューニングが必要

認証・画面巡回に壁がある

ログインや認証が必要な
画面を突破できない

汎用AIではなく、Web巡回・診断に特化したセキュリティ専用AIによる「AI活用型防御」が必要

生成AI時代の脆弱性診断なら AeyeScan

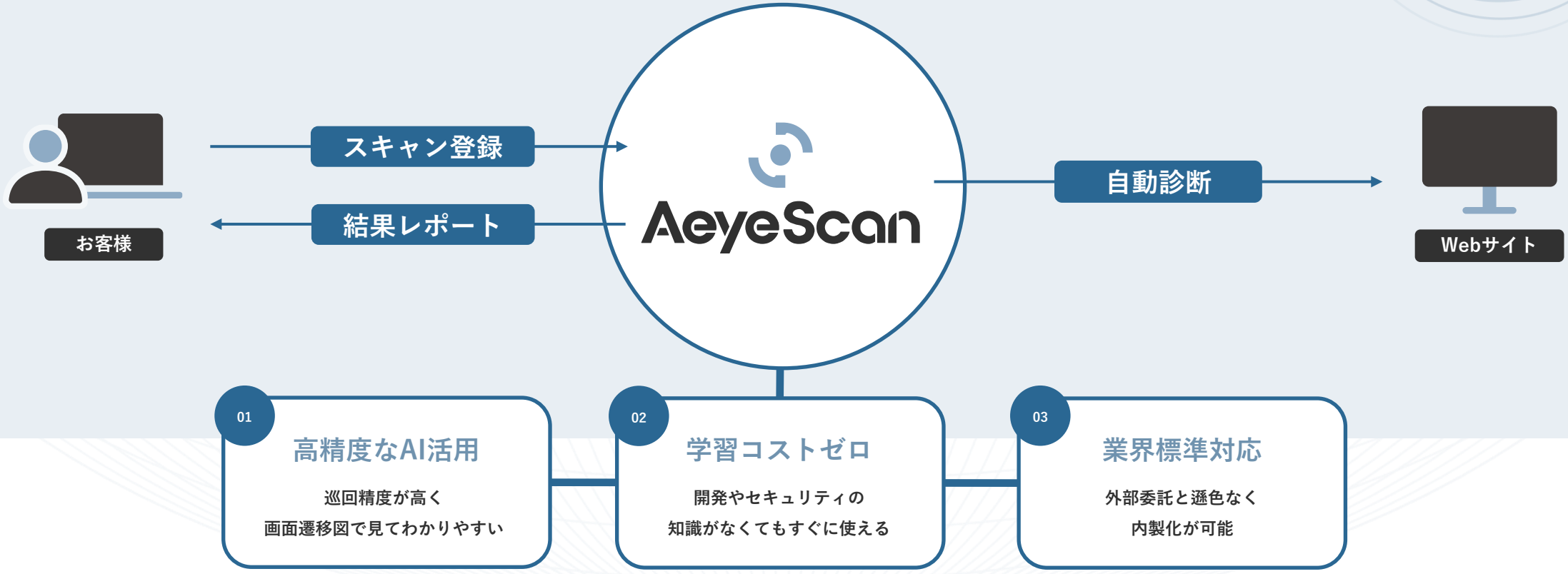
クラウド型Webアプリケーション
脆弱性検査ツール

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

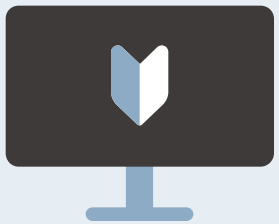


01
高精度なAI活用
巡回精度が高く
画面遷移図で見てわかりやすい

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

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。

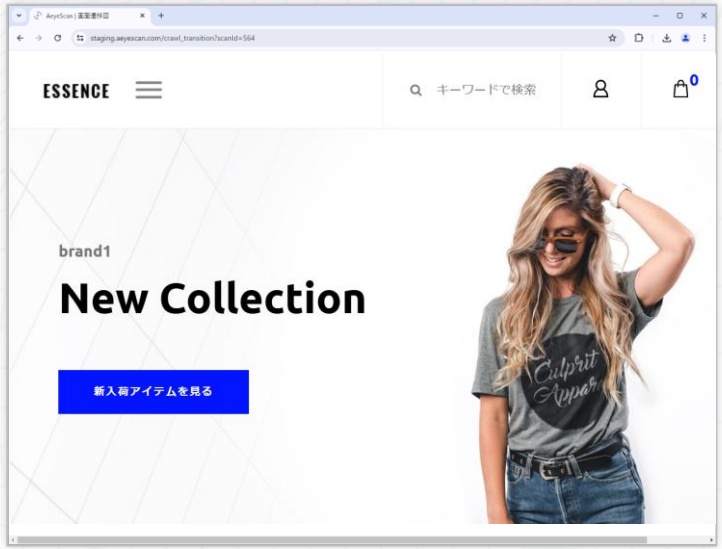
AIによる自動診断

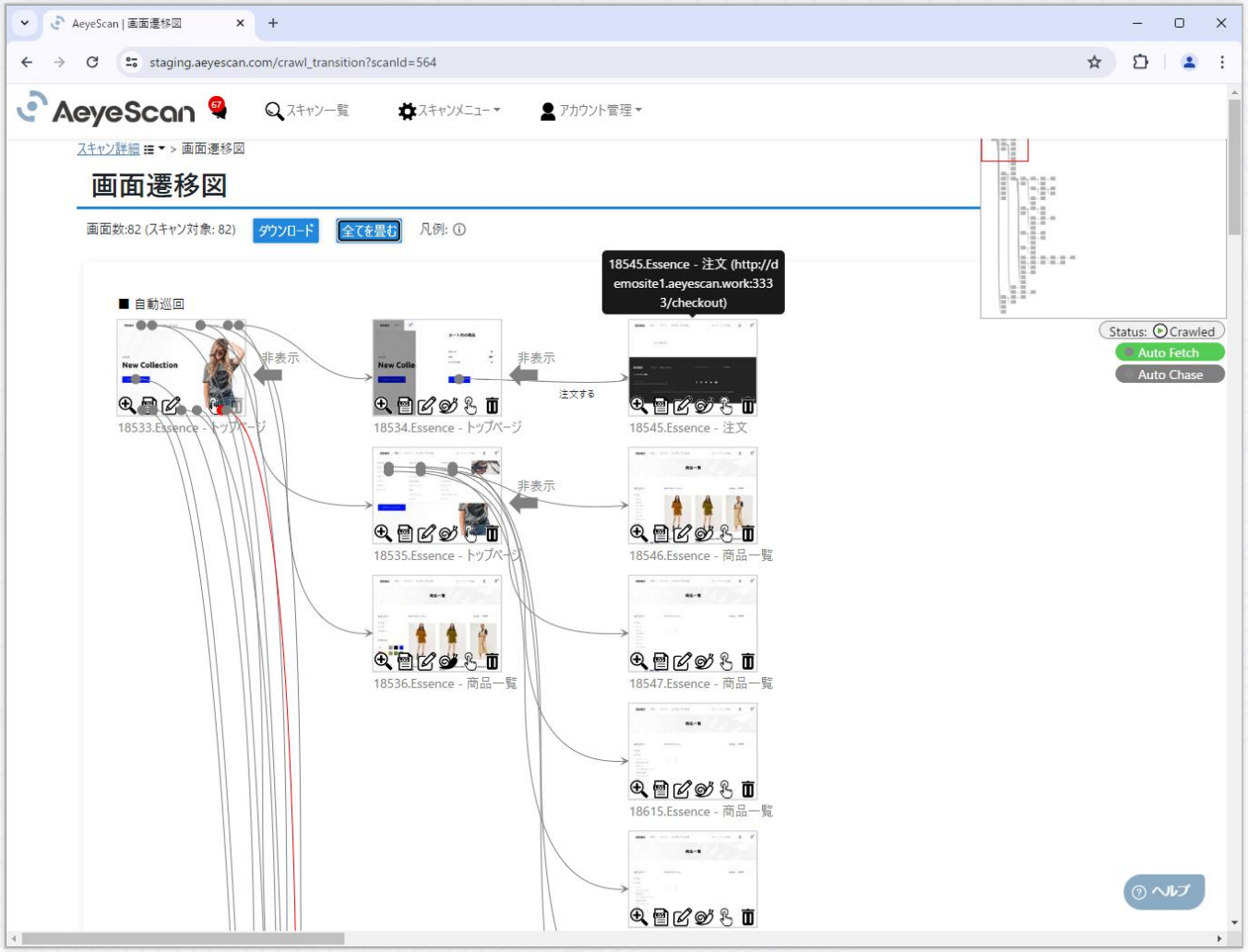
圧倒的な巡回精度で
24時間自動で診断。
画面遷移図で状況を可視化。

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。

巡回時に、自動で画面遷移図を生成





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

AeyeScanが選ばれている理由

プロが認める機能・性能 × 誰でも使える操作性

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 / ANA / HIS / H.I.S. / NTT EAST / odakyu / 近鉄情報システム株式会社 / G&O / 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

アイフル / 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 / 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 / MITSUBISHI ELECTRIC / YONA / リピスト / Yahoo!

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）

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

＼8月｜納涼ビアバッシュイベントを開催します／

ビール片手に、Webセキュリティの“リアルな悩み”を共有しませんか？

エーアイセキュリティラボ初の試みとして、
Webセキュリティに関する課題や疑問を持つ皆さまが
集まり、冷たいビールやドリンクを片手にカジュアルに
語り合う情報交換会「BeerBash」を開催します！

お申し込みはこちら

スマートフォンからも
お申込みいただけます

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