“てんやわんや”な脆弱性対応から抜け出せ！

AIを活用した効率的な

トリアージ & ASM とは

AeyeSecurityLab

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CXチームでの活動に加え、新規プロダクト企画・海外事業
展開など全社横断プロジェクトにも携わる。

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。

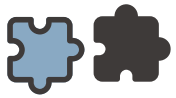
AeyeSecurityLab

いまや、脆弱性が「山積み」の時代

環境変化に伴い脆弱性が増加する一方、リソース不足で対応しきれなくなっている

攻撃対象の拡大

Webアプリケーション、API、
モバイル、クラウド…
診断対象の範囲が広がり
脆弱性が増加



新しい技術の台頭

マイクロサービスや
SaaS連携など、
新しい開発スタイルが
生まれるごとに
新しいリスクも生まれる

既知の脆弱性の放置

修正リソース不足や
診断待ちにより、
既知の脆弱性が
解消されないまま
積み上がっている

濃淡をつけないと、対応しきれない…

優先度：脆弱性の危険度、資産の重要性、ビジネスインパクト

時間とお金をかけて対応

限られたリソースで対応

限られたリソースを最適配分するために「脆弱性トリアージ」が必要

脆弱性トリアージはどのように進める？

脆弱性トリアージができる体制をつくる

「脆弱性の影響分析」、「リスク判定基準」、「対応の要否と期限を決める」といった
対応基本方針を策定することで、迅速に最低限のトリアージが可能な体制が構築できます。

1. 関係者の役割と責任を明確にする
2. トリアージガイドラインの適用範囲を決める
3. 脆弱性の影響範囲の調査
4. トリアージで決めるべきこと
5. 対応の要否と期限を決める
6. 脆弱性の管理方法

参考： 「脆弱性トリアージガイドライン作成の手引き 」 「1章 トリアージガイドラインの作成 」https://wg1.isog-j.org/TriageGuidelines/docs/chapter1/

トリアージで決めるべきこと　（1）対象資産の重要度の評価

資産の種類	影響度の規模 （例：利用者数）	利用者・顧客
高　金融データ、顧客情報、特許性を有する製品や技術情報	高　利用者数 1万人以上	高　官公庁利用者 （政府調達等）
中　業務データ、 従業員の勤怠情報	中　利用者数 1000人以上	中　技術者（開発者） システム管理者 企業の担当者
低　ホームページ等で既に公開されている情報	低　利用者数 1000人未満	低　一般の利用者 （BtoCのサービス等）

参考：「脆弱性トリアージガイドライン作成の手引き」「1章 トリアージガイドラインの作成」https://wg1.isog-j.org/TriageGuidelines/docs/chapter1/

トリアージで決めるべきこと　（2）脆弱性の危険度の評価

評価方針の設定

CVSS基本値や、脆弱性診断事業者が
提供する危険度評価を参考に分類

CVSSでは「攻撃元区分」「攻撃条件の複雑さ」
「攻撃前の認証要否」など、複数の要素を元に
最終的な値が算出されますが、特に重視する項目が
あれば基準の一つとしてもOK

危険度評価の定義例（3段階の場合）	
高	CVSS: 7.0 - 10.0
中	CVSS: 4.0 - 6.9
低	CVSS: 0.0 - 3.9

危険度評価の定義例（5段階の場合）	
Critical	CVSS: 9.0 - 10.0
High	CVSS: 7.0 - 8.9
Medium	CVSS: 4.0 - 6.9
Low	CVSS: 0.1 - 3.9
Info	CVSS: 0.0

参考：「脆弱性トリアージガイドライン作成の手引き 」「1章 トリアージガイドラインの作成 」https://wg1.isog-j.org/TriageGuidelines/docs/chapter1/

対応の優先度の決め方

対象の重要度評価と脆弱性の危険度評価から、マトリクスを作成して優先度・対応期間を決めます。

		資産重要度		
		低	中	高
CVSS	高	中 (30日以内)	高 (10日以内)	緊急 (5日以内)
	中	低 (90日以内)	中 (30日以内)	高 (10日以内)
	低	低 (90日以内)	低 (90日以内)	中 (30日以内)

参考：「脆弱性トリアージガイドライン作成の手引き」「1章 トリアージガイドラインの作成」https://wg1.isog-j.org/TriageGuidelines/docs/chapter1/

自社資産と脆弱性を把握するには？

ASM・脆弱性診断・トリアージは内製でできる

Web資産の把握（ASM）	脆弱性診断	トリアージ
ASMツールを活用し 未把握のWeb資産を発見する	脆弱性診断ツールを活用し 脆弱性を発見する	自社トリアージガイドライン を作成し、優先度付け

参考：「脆弱性トリアージガイドライン作成の手引き」 https://wg1.isog-j.org/TriageGuidelines/

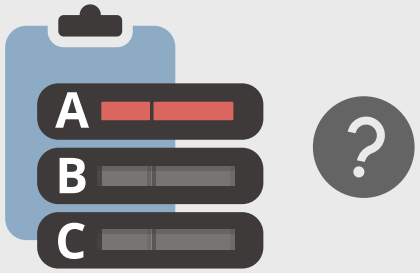
Web資産を把握する難しさ

人力で探索・精査が必要

広範囲から検出することはできるが、
不要なものも多く紛れ込んでおり、
人手による精査が必要。

リスク評価が困難

リスクをどう評価するか悩ましい。
システム観点からだけでなく、
事業観点での優先順位付けが必要。

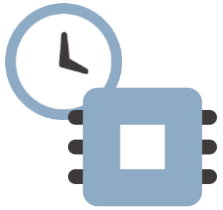


「困った時の生成AI」はASMにも使える

生成AIをASMに活用することで…！

会社名だけで攻撃面を探索

検索結果に上がってきた
組織名(文字列)を解読



発見経路/理由が分かる

生成AIが攻撃面を見つけるまでに
辿ったルートを説明

膨大な情報源から総合的に判定

- SSL証明書の情報
- IR情報(Web公開済み)など

重要度を自動でランク付け

Webサイトの属性を自動判定し
ビジネス上の重要度をもとにランク付け

脆弱性診断を内製化するときに考えること

「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？

脆弱性診断を内製化するときに考えること

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

ASM×脆弱性診断の「内製化」をご支援します

生成AI時代の脆弱性診断なら AeyeScan

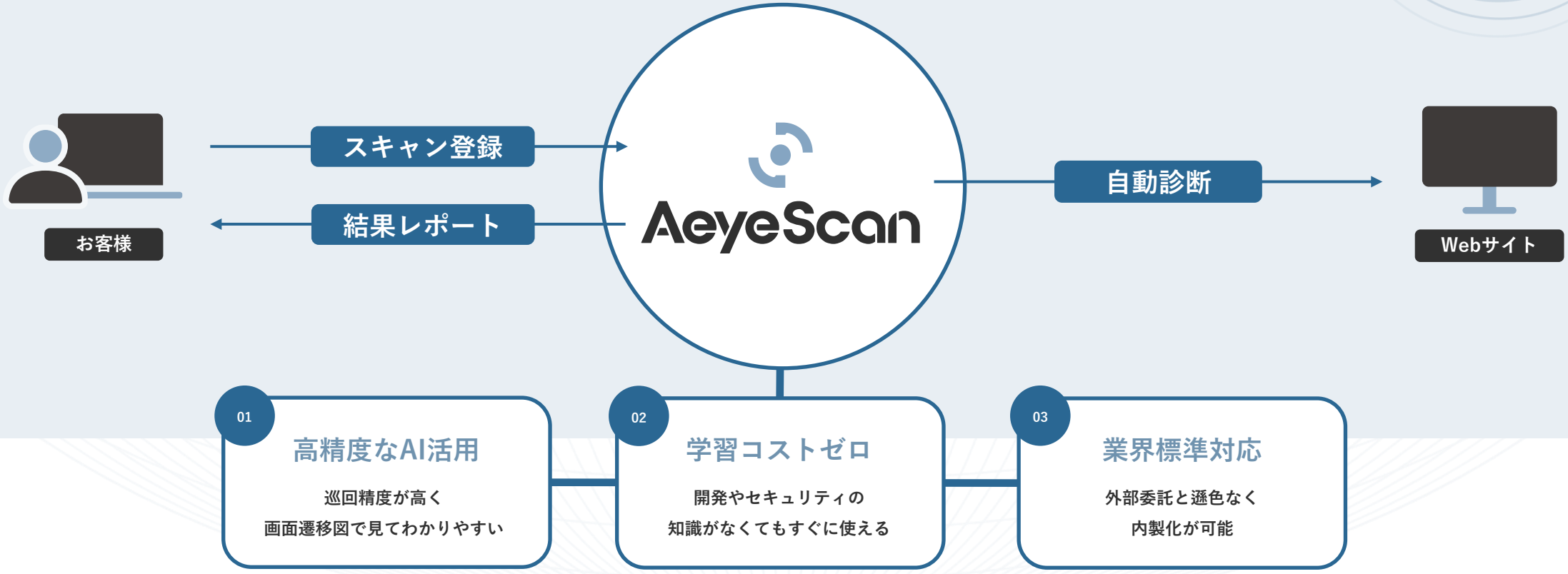
クラウド型Webアプリケーション
脆弱性検査ツール

国内市場シェア
No.1※

※ 富士キメラ総研調べ「2024 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〈クラウド〉2023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（2024年度実績）

有償契約
300社以上

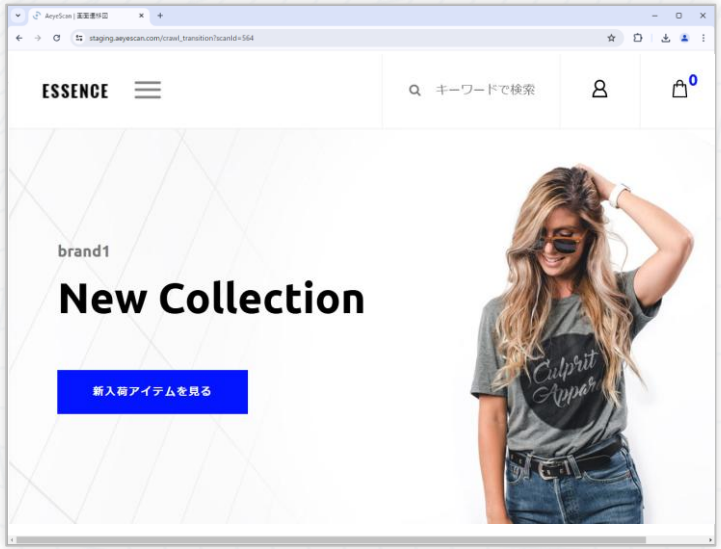


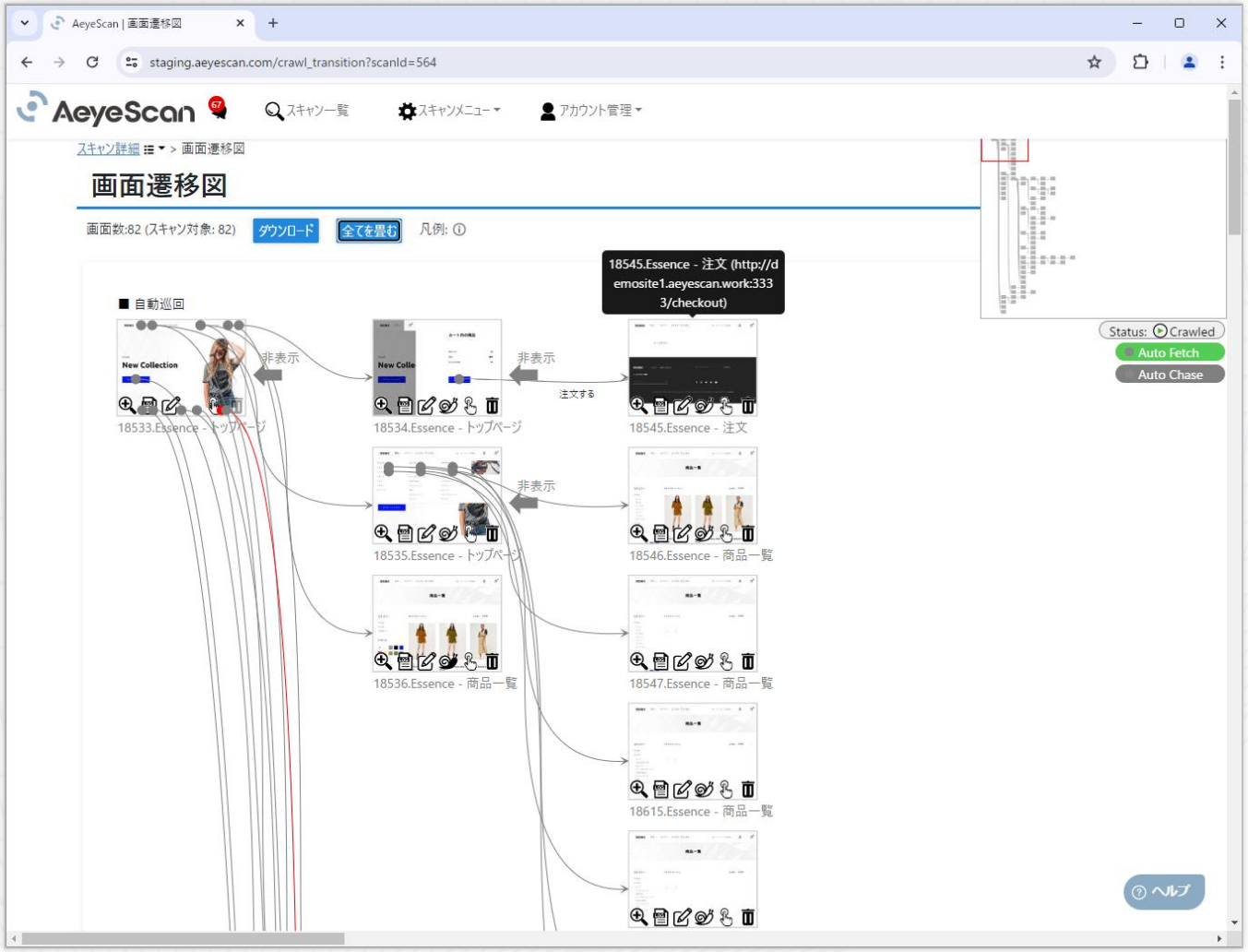
01
高精度なAI活用
巡回精度が高く
画面遷移図で見てわかりやすい

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

AeyeSecurityLab

生成AIを活用したWeb-ASM機能で Web資産の把握・定期監視を実現

Web-ASMの実施ステップ

1 攻撃面の **発見**

Web-ASM機能

自社が保有している
ドメイン一覧を抽出

2 攻撃面の **情報収集**

自動巡回

未把握のドメインを
巡回対象に追加

3 攻撃面の **リスク評価**

脆弱性診断

管理対象の全ドメインに
脆弱性診断を実施

AeyeScan とあわせて
より網羅的な脆弱性診断とリスクマネジメントが可能に！

ビジネス観点＆技術観点でリスクを評価

サイト用途

Medium

- ECサイト
- 製品情報サイト
- サービスサイト

など

Low

- ブログ系サイト
- 外部SaaSサイト
- テストサイト

など

保持データ

High

- 個人情報
- クレジット情報

など

簡易スキャン

Low

- TLS暗号スイートの不備
- HTTPSが強制されていません
- Cache-Controlヘッダの不備

など

Info

- 期限切れ間近のサーバ証明書
- Referrer-Policyヘッダの不備

など

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

人材・教育

HSAWA DRIVING SCHOOL / 河合塾 / Junion / JINSOKEN / ZENKIGEN / Direct Sourcing / PERSOL / Leverages / workport

インフラ

EPARK / AIRE / HIS / H2O RETAILING / NTT EAST / odakyu / 近鉄情報システム株式会社 / G-gio / SymEnergy / 水ing Swing Corporation / Suzuyo / NANKAI 南海システムソリューションズ / 日本調剤 / HITOWA GROUP / ベルーナ / grow up together MEDIA / Looop / Loyalty Marketing, Inc.

金融

アイフル / 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

メディア

集英社 / 中日新聞 / NIKKEI / Media Do

製造

AICA / AISIN / KITZ 株式会社キッツ / KOSÉ / SAKI / TIGER / TEIJIN / Denkei / House / Mizuno / ユーグレナ

エンタメ

e+ イープラス / CAPCOM / GungHo Online Entertainment, Inc. / とらラボ! TORANOANA LABORATORY / BookLive

SaaS

Advanced Media, Inc. 株式会社アドバンスト・メディア / Lexica E-Retailing Platform / estie / エアアンドエムマット株式会社 / M-aid / エムティーアイ / OZ INTERNATIONAL / 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 株式会社リバスタ / 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 KDDI Agile Development Center / circlace / さくら情報システム / SUNDAY SYSTEMS / CEC / GA TECHNOLOGIES / tdi 情報技術開発株式会社 / Simplex Inc. / 777WORKS 株式会社スリーセブンワークス / SOFT CREATE / SOLTEC / 高千穂交易株式会社 / 電通総研 / TOPPAN / JOPS / JAST / PCNET 株式会社パシフィックネット / Human Interactive Technology inc. / FUJISOFT / FUJITSU / MACROMILL / 三菱電機デジタルイノベーション株式会社 / YONA / リピスト

セキュリティ企業

NEC NECセキュリティ / NTT DATA 株式会社NTTデータ先端技術 / GSX GLOBAL SECURITY EXPERTS / cybertrust / LAC

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

脆弱性トリアージ体制の構築とともに

脆弱性診断の内製化・WebサイトのASM

検討される方は AeyeScan もお見逃しなく！

来期の脆弱性診断・ASMどうしようかな…という方は、アンケートで

トライアルしたい **デモが見たい** **担当者に相談したい**

をお選びください。

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

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。