

サイバーレジリエンス強化の

一丁目一番地

資産とリスクの「特定」を内製化する方法とは

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。



主な著書

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。

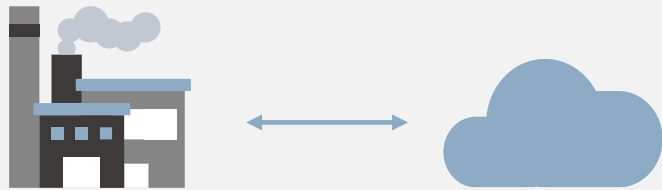
世界も驚くような、技術の力で。

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。

DX/AI時代は「攻撃される前提」でのリスク管理が重要

DXの進展

ITとOTが融合し、
ビジネスとデジタルが直結



**サイバー攻撃は
事業存続のリスクに**

AIの進化

サイバー攻撃のコモディティ化



**攻撃されるのが
当たり前の世界へ**

DXが進むほど、リスク管理は「復旧力」が問われる

さらにAIの活用も広がる中で、セキュリティリスク管理の重要度が増している。



AIが事業に組み込まれ
部分障害が全体停止に
つながりやすい



早く復旧できないと
事業の改善スピードが
低下してしまう



サービス停止や
その後の対応次第で
顧客の信頼低下を招く

事業継続のためには「サイバーレジリエンス強化」が欠かせない

あらためて、DX/AI時代に必要なサイバーレジリエンスとは

攻撃されても、業務やサービスを継続し、被害を最小化しながら素早く復旧できる体制

NIST CSF 2.0のモデルと、対応する対策・ソリューション

← ガバナンス (Govern) : 経営層と戦略の統合 →

特定

資産とリスクの
可視化

ASM、脆弱性管理
ID/アクセス管理

防御

権威の
侵入・拡散を阻止

EPP/EDR、DLP
ネットワーク
セキュリティ

検知

脅威の早期発見
分析

SIEM
脅威インテリジェンス

対応

インシデントの
迅速な封じ込め

SOAR
インシデント
レスポンスサービス

復旧

事業継続の
確保

サイバーレジリエンス強化のために
まず、始めたい2つのこと

レジリエンス強化に必要なこと① 資産とリスクの「可視化」

攻撃される前提で考えた時に、資産とリスクを把握していることが重要



「見えないものは守れない」

攻撃対象を**可視化**（把握）することが、サイバーレジリエンス強化の第一歩

レジリエンス強化に必要なこと② セキュリティ対策の「自動化」

脆弱性診断もASMも、人手だけで実施しては追いつかない。

診断対象の多様化

クラウド

SaaS

API

サーバ

開発環境の変化

アジャイル

CI/CD

高速リリース

短期サイクル

「人だけでは守れない」

自動で回る仕組みづくりが、レジリエンス強化に求められている

どうやってリスクを可視化する？
どこまで自動化できる？

| 孫子曰く…

敵を知り、己を知れば、百戦殆(あやう)からず

己を知る = **ASM(攻撃面管理)**

自分たちの資産(城砦、兵糧、武器…)を予め把握し、
弱いところ・守るべきところを押さえておく

敵を知る = **脆弱性診断**

攻撃者がどのように攻めてくるか予め知っておき、
それに備えられるよう訓練しておく



| お客様から伺う「ASMツール」活用のお悩み

探せない

探索のための手がかりがない

ASMを使って探索したいのに、ヒントが必要って…

わからない

本当に自社の資産なのか怪しい

類似する他社サイトが紛れ込み、精査が必要…

選べない

どれから対応すべきかわからない

資産の検出はできても、リスク評価までは行えない…

高度な生成AI活用により、効率的かつ信頼性の高い探索が可能



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



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



発見経路/理由 が分かる

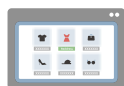
生成AIが攻撃面を見つけるまでに
辿ったルートの説明



リスク対応の優先順位付けに必要な情報を自動判別

Web資産の重要度

各Web資産の属性
(サイト用途、保持データなど)



製品情報サイト

重要度：中



ECサイト

クレジットカード
情報保持

重要度：高



ヘルプサイト

WordPress使用

重要度：低

リスクの深刻度

ミドルウェアやライブラリの悪用観測脆弱性*

※既にサイバー攻撃で悪用が確認された脆弱性

2件



ミドルウェアA CVE-xx 深刻度：高
ミドルウェアA CVE-xx 深刻度：中

1件



ライブラリB CVE-xx 深刻度：低

10件



ミドルウェアC CVE-xx 深刻度：高
ライブラリD CVE-xx 深刻度：高
:

お客様から伺う「脆弱性診断」のお悩み

公開するWebサイトや
提供するWebサービス
が増えている



開発規模・サイト規模
が大きくなっている
(100画面以上ある)



機能改修・追加など
リリース頻度が高く
間隔も短くなっている

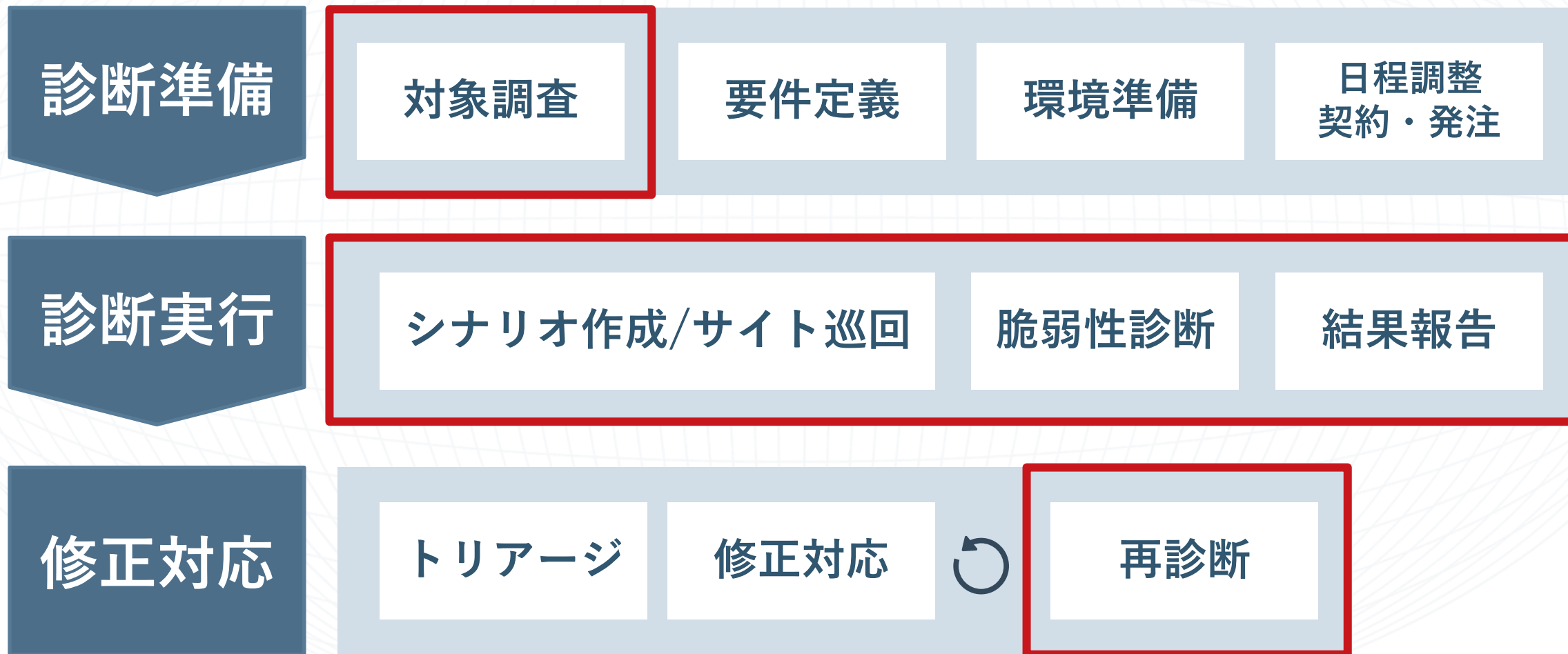


でも…

予算が限られている

人員も限られている

AI活用で、脆弱性診断プロセスの大部分を自動化・省力化できる

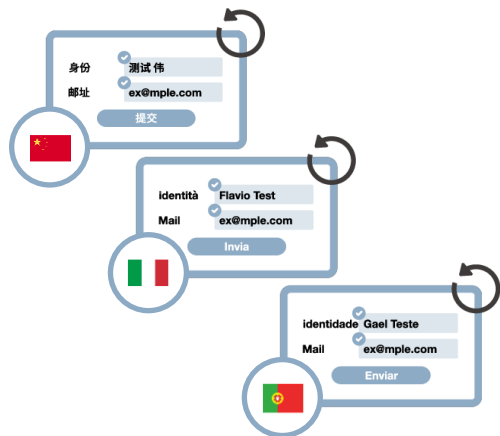


生成AIを組み込むことで、多様なWebサイト・多様な脆弱性に対応

多言語対応

日英以外のWebサイトも幅広く巡回・診断

多言語でのフォーム入力

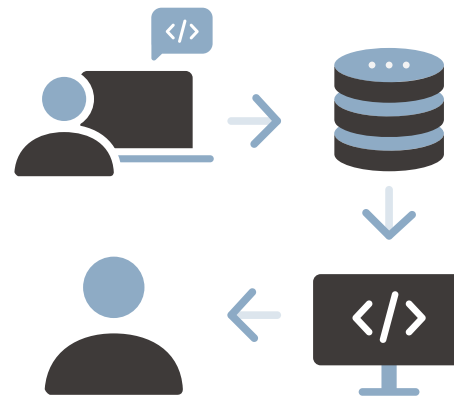


日本語	ポーランド語
英語	スペイン語
フランス語	ポルトガル語
中国語	ロシア語
韓国語	スウェーデン語
オランダ語	アラビア語
ドイツ語	...
イタリア語	

診断項目の拡張

人間しか診断できなかった脆弱性も検出

セカンドオーダー系XXS

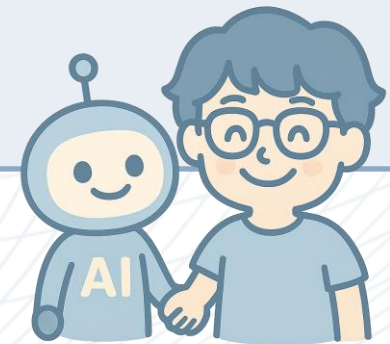


認可の不備・権限昇格



予算・人員が
限られている中で

人とAIの協業モデルによる「可視化」で
サイバーレジリエンスを強化しましょう





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



スキャン登録

結果レポート

AeyeScan

自動診断

Webサイト

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。

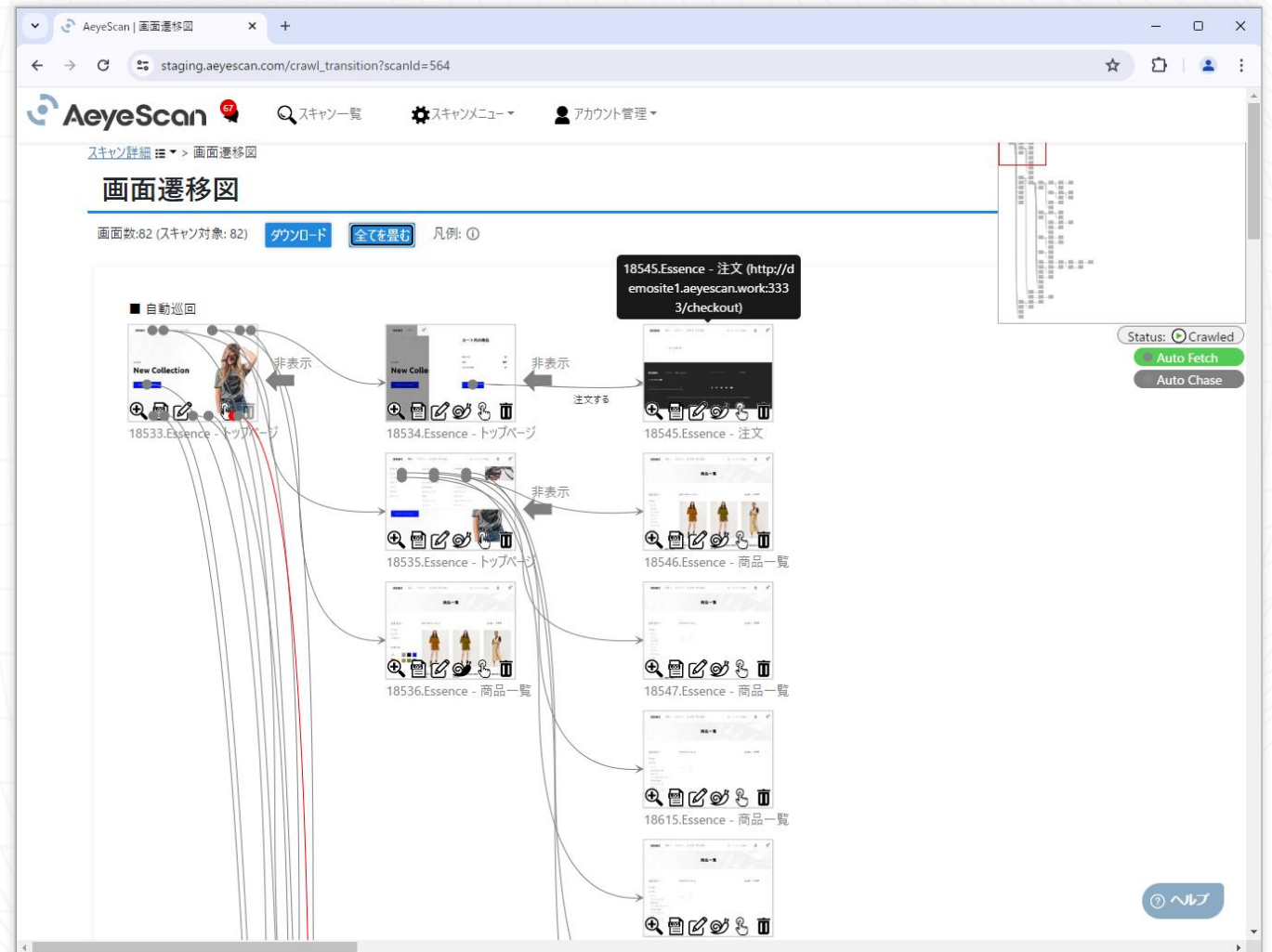
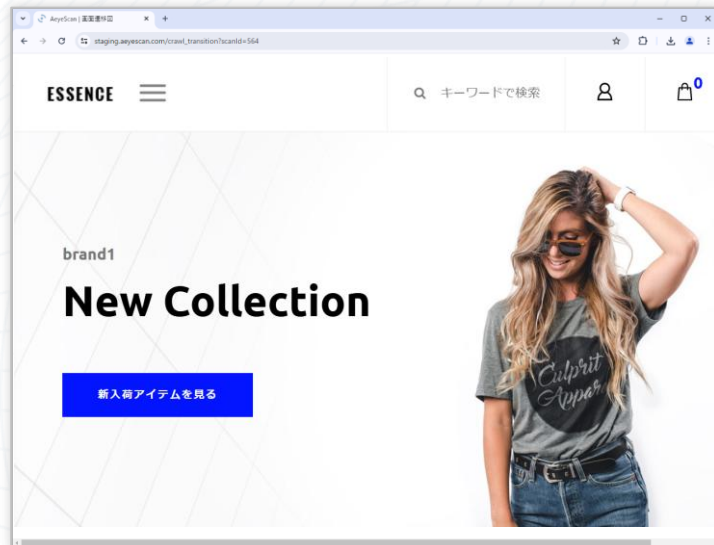


わかりやすいレポート



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

Web-ASM | スキャン一覧 | スキャンメニュー | 組織設定

スキャン一覧 > スキャン詳細 > スキャン結果(カテゴリ)

スキャン結果(カテゴリ)

● 会社概要アップデート (<http://demosite1.aeyescan.work:3333/>)

レポートダウンロード

Severity	Count
Critical	11
High	0
Medium	23
Low	1
Info	17

● OWASP TOP 10の結果

- > A1:2017-インジェクション: 11件
- > A2:2017-認証の不備: 1件
- > A3:2017-機微な情報の露出: 1件
- > A4:2017-XML 外部エンティティ参照(XXE): 1件
- > A5:2017-アクセス制御の不備: 0件
- > A6:2017-不適切なセキュリティ設定: 17件
- > A7:2017-クロスサイトスクリプティング(XSS): 18件
- > A8:2017-安全でないデシリアライゼーション: 1件
- > A9:2017-既知の脆弱性のあるコンポーネントの使用: 1件

ヘルプ

概要 | 脆弱性情報 | 詳細ログ | 再スキャン実行

クロスサイトスクリプティング

スキャン情報

81. 会社概要アップデート (<http://demosite1.aeyescan.work:3333/>)

対象ページ

1777.Essence - 新規登録 (確認) (<http://demosite1.aeyescan.work:3333/register>)

画面遷移図で表示

深刻度

Medium

CVSS: 5.1 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N)

スクリーンショット

ESSENCE ログイン forgot password

ESSENCE ログイン

登録フォーム

氏名
Eメール
パスワード
パスワード (確認)

登録

以下は内容ではありません。 確認を併せてください。

ESSENCE ブログ お問い合わせ

ESSENCE ログイン

氏名
Eメール
パスワード
パスワード (確認)

登録

| 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

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

セキュリティ診断のお悩み・お困りごとをお聞かせください！

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。

トライアル



お見積りの希望・導入をご検討している方へ

AeyeScan に関する 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



セキュリティ診断のお悩み・お困りごとをお聞かせください！

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 に関する 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



各種セミナーも開催中

AeyeScanをもっと知りたい方向け

＼診断ツールの違いを知り、AeyeScanを体験／

6/03 水 オンライン@Zoom

6/09 火 オンライン@Zoom

6/26 金 神田スクエア

詳細・お申し込みはこちら



色々な角度から情報収集したい方向け

＼市場のトレンドを軸に様々な情報をお届け／

5/26 木 脆弱性対策の新しい進め方

6/18 木 Web資産管理の実践知を解説

6/30 火 OWASP Top 10×実例を学ぶ

詳細・お申し込みはこちら





AeyeScan

セキュリティに、確かな答えを。