
AIをフル活用した

次世代Webセキュリティとは

-安全と効率を両立させる脆弱性診断の最新アプローチ-

自己紹介



株式会社エーアイセキュリティラボ

経営企画部 ディレクター **瀧沢 翼** (たきざわ つばさ)

外資系戦略コンサルティングファームにて、全社戦略立案、業務効率化、DX推進、M&Aデューデリジェンスなど、多岐にわたるプロジェクトを経験後、2024年9月より現職の経営企画部の立ち上げメンバーとして参画。全社戦略や予算の策定、人事評価制度の設計など、経営上流の意思決定支援を担う一方で、バックオフィス業務フローの標準化・管理の実務にも着手し、組織全体の効率化と競争力向上に向けた仕組みづくりを推進。

| 本日本話したいこと

- ✔ DXの進展がもたらすセキュリティへの影響
 - ✔ セキュリティ対策の実行における主要課題の洗い出し
 - ✔ デモンストレーションや導入事例を通じた、弊社プロダクト「AeyeScan」のご紹介
-

| やらないと死ぬDX、年々高まる人材需要

DXの推進は、多くの組織において取り組むべき重要課題とされている一方、DX人材の不足が慢性化している状況にある。

DXの戦略立案や統括を行う
人材が不足している

69.2%

DXを現場で推進、実行する
人材が不足している

65.4%

DXを取り巻く状況

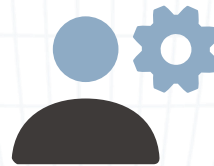
DXの進展に伴い、ITシステムの連携・整備やデータ活用が新たな価値創出の源泉となった結果、デジタルサービス・システムの開発機能の内製化が加速している。

IPAが提言するDXに必要な要素

ビジネス環境の変化に
迅速に対応できる
ITシステムの整備



競争領域を
強化するための
社内外システムの連携



ビジネス上の
ニーズに合致する
データ活用と分析



DXの進展がもたらすセキュリティへの影響

自社で管理すべきデジタルサービス・資産の増加に伴い、セキュリティ対策の対象範囲は劇的に拡大し、対策の複雑性と実現難易度も一層高まっている。

DX

デジタルサービスの開発・提供
自社で管理すべきデジタル資産

増

=

×

急速な技術の進化

セキュリティ

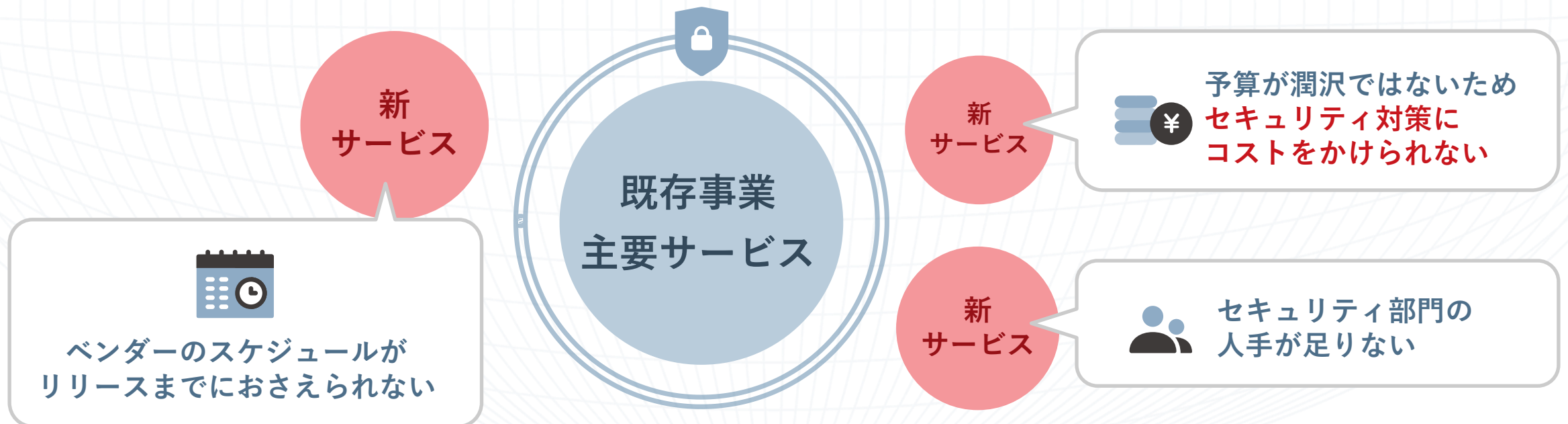
必要なセキュリティ対策の
対応範囲は広く…
難易度も高く…

DXの推進にセキュリティ強化は不可欠だが、その実現には多くの課題が存在

DXの進展によって生じた課題

① 時間・予算・人材の不足

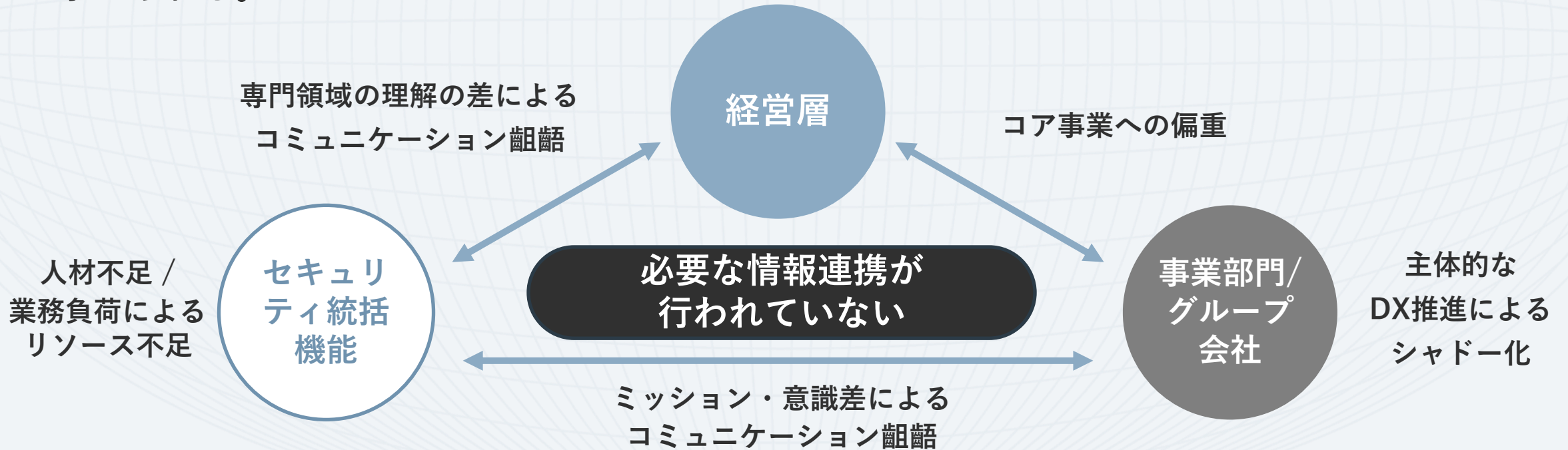
新しいデジタルサービスが次々と生みだされる一方で、事業立ち上げ段階から万全のリソースをかけてセキュリティ対策を行うことは困難であり、事業スピードとの両立が課題化しやすい。



DXの進展によって生じた課題

② 部門間での連携の難化

組織全体でセキュリティガバナンスを効かせるために、部門や役割を超えたコミュニケーションが求められる。



DXの進展によって生じた課題

③ セキュリティ対策の必要量も急増

例えばWebサイトのセキュリティ対策を例にとっても、求められる対策の量は膨大であり、あらゆる項目をすべての対象に徹底して実施することは容易ではない。

Webアプリケーションの セキュリティ対策

- ① ファイルの公開設定
- ② Webページの公開設定
- ③ 脆弱性への対策
- ④ ソフトウェアの脆弱性対策
- ⑤ エラーメッセージの設定
- ⑥ ログ管理
- ⑦ 暗号化
- ⑧ 不正ログインへの対策

Webサーバの セキュリティ対策

- ⑨バージョンアップを行う
- ⑩ 不要なサービス・アプリケーションの停止
- ⑪ 不要なアカウントの削除
- ⑫ 安全なパスワードの設定
- ⑬ アクセス制御
- ⑭ ログ管理

ネットワークの セキュリティ対策

- ⑮ 不要な通信の遮断
- ⑯ 通信のフィルタリング
- ⑰ 不正な通信の検知・遮断
- ⑱ ログ管理

その他の セキュリティ対策

- ⑲ クラウドサービスへのセキュリティ対策
- ⑳ Webアプリケーション・Webサーバ・ネットワークへの定期的な脆弱性診断

では、どうするべきか…？

DXとセキュリティを両輪で進めるために必要な「AI活用」

人手やコスト・時間が限られる中でセキュリティを担保するためには、対応に濃淡をつけつつ、リソースを効率良く配分する方法を考える必要がある。その方法のひとつが、AI活用といえる。

手間と時間をかけて
専門家が対応する

濃

淡

人的リソースを最小化
しつつ対応する

専門人材は限られているが、技術的に人間が対応しなければいけない範囲が広い

継続的・網羅的に対応する必要があるが、割ける人的・金銭的リソースは限定的

AIを活用した「自動化」も必要

セキュリティ領域におけるAI活用



法令遵守

- デジタル関連法令対応
- コンプライアンス対応
- 業界のセキュリティガイドラインへの準拠

…etc



ミスができない領域
人が考えて対応すべき



ガバナンス強化

- 事業特性に応じたセキュリティポリシーやガイドライン作成
- セキュリティ対応マニュアルの整備と実行管理

…etc



関係者が多く影響範囲が広い
人の精緻な設計が必要



具体的な対策

- セキュリティ製品やサービスの導入
- システム面のサイバー攻撃対策
- 脆弱性診断

…etc



目的と方法を決めれば
対策にAIを組み込める

「では、具体的になにをすればいいのか？」



まずは、
脆弱性診断から「AIをフル活用」し、
セキュリティ対策に濃淡をつけませんか？



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「2023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)2022年度実績)

※ITR調べ「ITR Market View：サイバー・セキュリティ対策市場2024」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 (2022年度実績)

有償契約
200社以上



導入事例紹介

アイフル様



企業名 アイフル株式会社

事業内容 リテール金融サービス

従業員数 単体 1,229人 (2024年3月31日現在) 連結 2,470人 (2024年3月31日現在)

課題

診断の外部委託ではコストがかさむ上
調整に手間がかかり
開発スタイルにそぐわなかった

具体的な課題

- 1 セキュリティの深い知識までは持っていない
- 2 外注では全体で数百万単位のコストがかかる
- 3 外注だと日程調整などに手間がかかる

高いセキュリティが求められるため診断を外部委託していたが、コストと手間がかかる状態だった。日程も融通がきかず、アジャイル方式の開発スタイルとは相性がよくなかった。

導入

レポートの分かりやすさ、
診断項目・精度、コストなど
総合的に見て導入を決定

導入の背景

- 1 エンジニアにとって分かりやすく、使い勝手がよい
- 2 スキャンが高精度で、どう修正すべきかも分かる
- 3 サポート体制がしっかりしている

エンジニアにとっての分かりやすさ、使いやすさを重視。画面遷移図が自動生成される点や、『問診票』が用意されていて事前の準備が容易な点も評価。

効果

コスト・工数削減を実現し、
スピーディな開発と
セキュリティの担保を両立

具体的な効果

- 1 診断会社との調整の手間がなくなった
- 2 好きなタイミングで何回でも診断が可能に
- 3 クライアントやユーザー部門にも安心材料を提示できる

スタートガイドを参照することで、予想以上にスムーズに導入できた。画面遷移で詰まるところが出てきた際も、サポートに連絡し、スピーディーに更新対応がなされたことが好印象。

導入事例紹介

マネーフォワード様



企業名 株式会社マネーフォワード

事業内容 PFMサービスおよびクラウドサービスの開発・提供

従業員数 2,400人 (2024年5月末日現在)

課題

事業が拡大しプロダクトが増えるにつれ、脆弱性診断の間隔が空いてしまうことが懸念材料だった

具体的な課題

- 1 外注だとナレッジが蓄積されない
- 2 外注だと画面数に応じた料金体系で網羅的な診断を受けづらい
- 3 開発が遅れた場合、ベンダーとのスケジュール調整が困難

新機能の追加や大規模な改修の際には脆弱性診断を実施していたが、それ以外はプロダクト側の判断に委ねていた。小さな改修のたびに診断を外注するのではなく、内部で迅速に診断する選択肢も持ちたかった。

導入

診断ツールを導入し
継続できなかった経験から、
使いやすさを重視

導入の背景

- 1 自動巡回のカバー率が高く、主要な脆弱性を確実に検出できる
- 2 グループ会社のプロダクトも診断できるライセンス体系
- 3 API診断が可能

外国籍エンジニアも多く在籍するため、英語にも対応していること、Slackをはじめとする外部サービスとの連携性も要件だった。複数のツールの比較検討を進め、いくつかのプロダクトを対象に検証を実施した上で選定。

効果

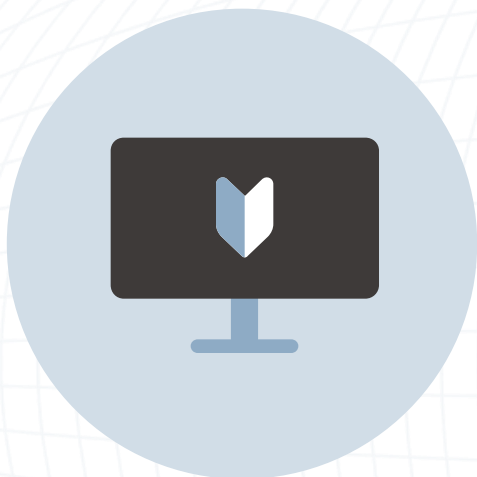
約60プロダクトに診断を実施できた
今後、最低年1回の診断を計画

具体的な効果

- 1 画面遷移図により、CISO室がプロダクトの画面を把握できるように
- 2 開発者のセキュリティ意識が高まった
- 3 グループ統一のセキュリティスタンダード適用にも活用予定

ほぼすべてのサービスを内製で開発する中、「セキュリティスペシャリストの活動をAeyeScanがサポートしてくれている」とCISOも評価。セキュリティエンジニア以外に、QAチームでも使用を開始している。

| 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
200社以上

※富士キメラ総研調べ「2023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)2022年度実績)

※ITR調べ「ITR Market View:サイバー・セキュリティ対策市場2024」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(2022年度実績)

プロが認める品質・精度

×

ブラウザ上での直感的な操作

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

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

製造



インフラ



金融



メディア



エンタメ



SaaS



SI・IT企業



セキュリティ企業



生成AIの活用による高度な自動化を実現

オプション機能

1 診断設定がさらにカンタンに

- ・フリーフォーマットでの指示



特許 第7320211号

2 巡回がより柔軟に進化

- ・多言語対応
- ・フリーフォーマットでの指示
- ・画面の自動類似判定



特許 第7348698号

4 高度なレポート出力も可能に

- ・診断結果を元に総評を生成



3 手動で診断していた項目にも対応

- ・パラメータの用途を推測
- ・セッションIDの規則性を解析



特許 第7344614号

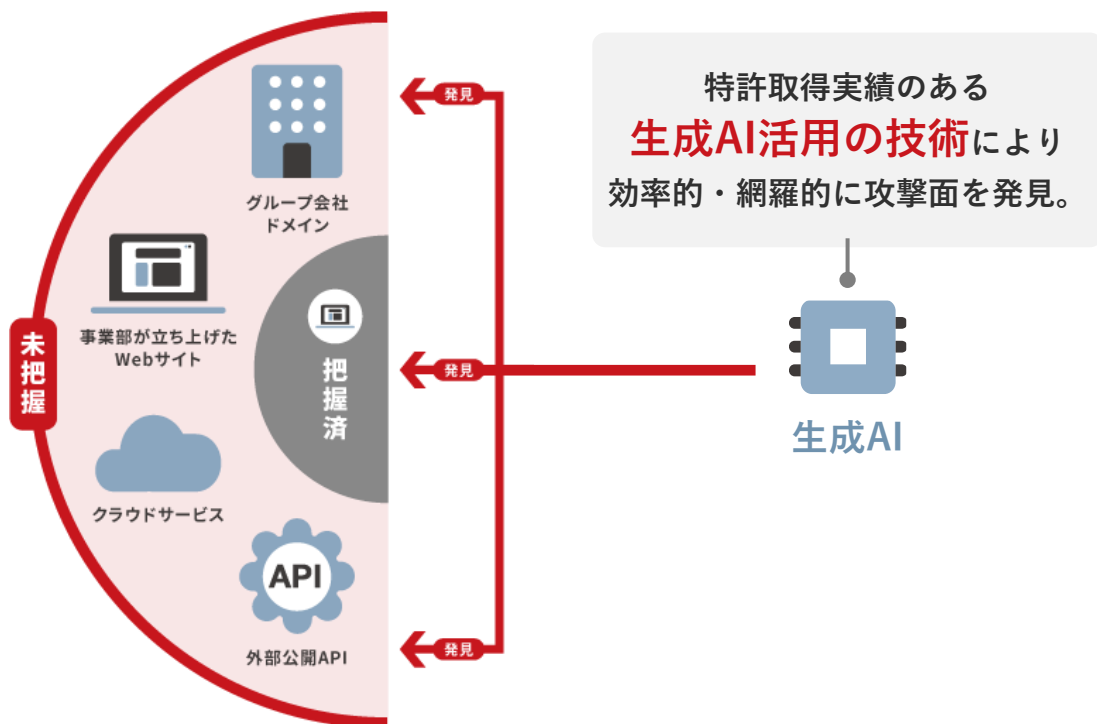
生成AI活用で、工数をかけずにWeb-ASMを実現

オプション機能

Web-ASMとは？

未把握な攻撃面の継続的な発見・リスク評価※

※リスク評価：AeyeScanのスク্যানによる



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 ひとつで、

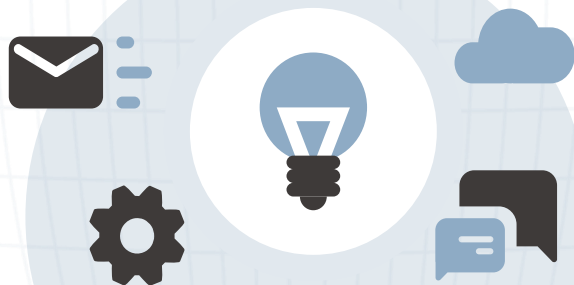
より網羅的な脆弱性診断とリスクマネジメントが可能に！

| まとめ

DXとセキュリティを両輪で進めるために、
AIに任せられる業務は積極的に任せ、
安全と効率を両立しましょう！



スピード感のある
事業展開



DX推進



セキュリティ
ガバナンスの
推進



期間
限定

Web-ASM機能オプション 利用料金50%OFFキャンペーン

内容

Web-ASM機能オプション利用料金を初回契約分50%OFFでご提供いたします。

適用対象

- 2025年3月31日(月)までに株式会社エーアイセキュリティラボにご発注いただいたものが対象です。
- AeyeScan Businessライセンスをご契約中または2025年3月31日(月)までに新規で利用開始いただいていることが前提となります。

申込方法

「Web-ASM機能」お問い合わせフォームまたは弊社担当までご相談ください。

▶ お問い合わせフォームはこちら <https://www.aeyescan.jp/form/web-asm/>

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。