セキュリティは“対処”から“運用”の時代へ

ランサムウェア事例

から考える、継続的なリスク管理

AeyeSecurityLab

本資料の目的

ランサムウェア被害は、もはや一部の企業や特定の業界に限った話ではありません。
システムや業務のデジタル化が進むにつれ、どの企業にとっても現実的なリスクとなっています。

インシデントが発生すると「防げたのか」「どこに問題があったのか」が注目されがちです。
しかし実務の現場では、それ以上に重要な問いが存在します。
それは、インシデント発生後、組織としてどのように対応し、
その後の運用をどう立て直していくのかという点です。

本資料では、公開されているランサムウェア被害の事例をもとに、
特定の企業や対応を評価・批評するのではなく、
インシデント対応後の運用にて、多くの組織が直面する共通課題に焦点を当てています。

「完全に防ぐこと」が難しくなった今、組織に求められているのは、
インシデントを前提とした上で、いかに継続的に判断し、運用を回し続けられるかだと言えるでしょう。
本資料が、その視点を整理する一助となれば幸いです。

ランサムウェア被害の調査報告資料から見えてくるもの

2025年10月に発生したランサムウェア被害。12月に入り、調査結果および対応状況について、
外部に向けた報告資料が公開されました。資料には、以下のような内容が記載されています。

- ランサムウェア感染が確認された経緯

- 被害が確認されたシステム / 影響範囲

- 初動対応 / 調査・復旧に向けた 取り組み

- 再発防止に向けた対応方針

これらは、インシデント対応の全体像を把握する上で非常に参考となる情報です。

本書では、公開されている事実のみを前提とし、対応の良否や背景についての評価・推測は行いません。
その上で、報告資料から、**現在のインシデント対応において何が重視されているのか**考えてみましょう。

インシデント対応の評価軸は変化している

公開資料を読み進めると、対応の過程が丁寧に整理されていることが分かります。
このことは、インシデント対応において重視される評価軸が変化していることを示しています。

これまで

- 脆弱性を事前に把握／対策できていたか
- セキュリティ対策が十分だったか
- 攻撃を受ける前に侵入を阻止できていたか

事前に防げたか（防御力）

これから

- 早期に異常を検知できたか
- 影響範囲を適切に把握できたか
- 事業継続や顧客対応の判断を迅速に行えたか

適切に対応できたか（対応力）

すべての組織が向き合うべき課題は

“ 防げなかった場合に、どこまで対応できるか ”

対応後にはじまる「運用負荷の増加」

インシデント対応が一段落した後、多くの組織が直面するのが運用負荷の増加です。
これは一時的なものではなく、長期的に影響を及ぼします。

⚠ 今まで通りの運用が許容されなくなり、より慎重・確実な運用が求められる

運用負荷が増加

システムやWeb資産の
点検・確認頻度の増加

社内外への
報告 / 説明業務の増加

経営層や監査部門など
関係者調整の複雑化

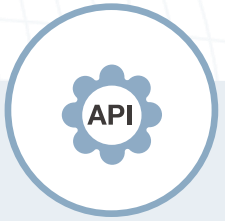
情シスやセキュリティ部門、開発部門だけでなく、事業部門など複数部署にも影響が

運用負荷の増加で露呈する不安要素

いざ点検や棚卸しを進めると浮き彫りになるのが、自分たちの環境を把握しきれていないという現実です。
時間の経過とともに管理対象から外れ、「未把握」の状態になっている資産はありませんか？

短期施策のために
一時的に作られたサイト

外部ベンダーに委託して
構築したシステム



役割を終えても
残り続ける機能

インシデント後の運用では、こうした状態が大きな不安要素として顕在化

未把握な資産の中でも、数が多く管理から漏れやすい「フォーム」

顧客やパートナー向けの
会員登録・問い合わせフォーム

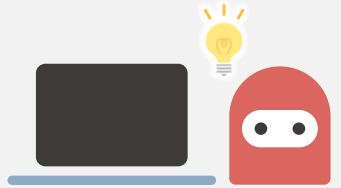
商品やサービスごとに設置する
資料請求・デモ申込フォーム

採用強化で拡大する
求人応募・エントリーフォーム

現場

施策を打つたびに増えていく
広告・キャンペーンLP

定期開催で毎月立ち上がる
ウェビナー申込サイト



攻撃者

現場の管理が煩雑になる一方で、攻撃者にとっては狙いやすい“入口”に

環境の複雑化により、人手による管理は限界へ

複雑化した環境を人手だけで把握・管理し続けることには限界があります。特に、役割分担が進んだ組織ほど、全体を横断的に把握しづらくなりがちです。

工数・時間がかかり続ける

日常的な運用だけで
多くの工数と時間を要し、
改善や対策検討に
十分なリソースを割けなくなる

対応品質にばらつきが出る

属人化により
担当者の経験に依存してしまい、
判断や対応スピード・内容に
差が生じてしまう

抜け漏れが発生しやすくなる

対象の増加や変更の
把握・管理が追いつかず、
確認漏れや見落としが
起こりやすくなる

初動対応までに時間がかかる

状況把握や影響範囲の
確認に時間を要し、
初動対応が遅れることで、
被害や影響が拡大する

“作業”を自動化し、人は“判断”に集中

これからは人が抱え込むのではなく、ツールや仕組みで自動化できる作業を切り分けることが重要です。

自動化する領域

- 定期的な状態の把握
- 変更点や差分の検知
- 一次的なリスクの洗い出し

反復的な作業は自動化

×

人がやる領域

- 対策の優先順位づけ
- 方針や戦略の策定
- 改善や最適化の意思決定

人は判断 / 意思決定に集中

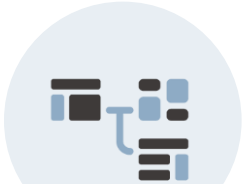
自動化による日常的な環境・資産の把握が

インシデント発生時の「対応力」を向上させる

自動化と相性のよい、Webサイトの脆弱性診断

Webサイトは、リリースや改修を重ねる中で、画面や入力項目、構成が継続的に変化していきます。
そのため、人手による運用では特に限界が生じやすく、自動化を検討すべき領域です。

**Webサイトの脆弱性診断は、自動化との親和性が高く
ツールによって仕組み化しやすい**

未把握の Web資産の検出	診断画面の 自動抽出	脆弱性診断の 実行	リスク深刻度の ランク付け
			

脆弱性診断ツールの役割は「攻撃対策」から「継続把握」へ

インシデントは一度対応して終わるものではありません。セキュリティを点ではなく線で捉え、日常運用に組み込んでいく視点が求められています。その中で、脆弱性診断ツールが果たす役割も変化しています。

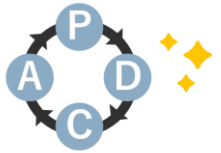
これまで

防げたか

攻撃対策

脆弱性を発見・対応し
侵入を防ぐためのツール

これから



適切に対応できたか

継続把握

継続的なリスク管理を行い
判断・対応を支えるツール

AI活用により「継続把握」を日々の運用の中に組み込むことができる

クラウド型Webアプリケーション脆弱性診断ツール「AeyeScan」

（エーアイスキャン）

AeyeScan なら、セキュリティ運用をAIで自動化・仕組み化

誰でも簡単に社内で脆弱性診断が行えます

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（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

クラウド型Webアプリケーション脆弱性診断ツール「AeyeScan」とは

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

1

最短10分で診断開始

専門知識は不要！
SaaS環境なので24時間放置しておけます。

お客様

1 スキャン登録

3 結果レポート

AeyeScan

2 自動診断

Webサイト

3

診断結果レポートも自動生成

開発担当にすぐ渡せるレポートが簡単に出力できます。

2

画面遷移図を自動作成

AeyeScanがサイトを自動巡回、診断すべき画面を抽出して画面遷移図を生成します！

テストシナリオ作成不要、最短10分で診断開始

フォーム特有の入力・遷移パターンを自動認識。面倒なパラメータ設定やシナリオ作成は不要で、
URLを入力すればすぐに診断を開始できます。

従来のツール
URLの設定
パラメータ・セッションの手動設定
テストシナリオの手動作成

AeyeScan
URLを入力するだけ！
 1週間かかっていた準備が3、4時間で 終わるようになったというお声も！

AeyeSecurityLab

複雑なフォーム構造も高精度に網羅

高度なAI活用技術により、従来のツールでは対応が難しかった**複雑なフォーム構造も自動巡回**できます。

例： AIによるフォーム入力値の判断処理

課 題

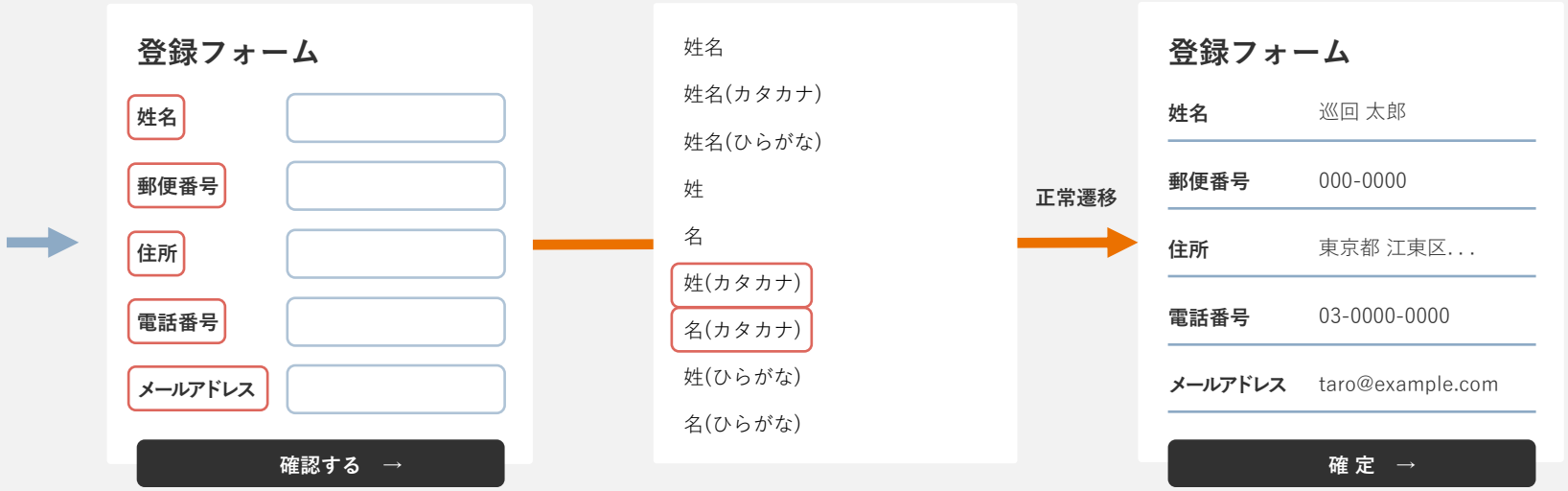
フォーム入力は正しい値を入力する必要がある。
間違えると、**入力エラーとなり遷移できず診断が進まない…**

AeyeScanなら、
正確に入力値を推測して巡回！

ココがポイント

名前や住所など決まった項目だけでなく、
どんな項目にも対応！

例えば
- クレジットカード
- 画像アップロード



巡回時に自動で「画面遷移図」を生成

ページやリンク構造を自動で可視化。診断対象リストの手動作成が不要で、再診断もスムーズに行えます。

参照： AeyeScan コントロールパネル

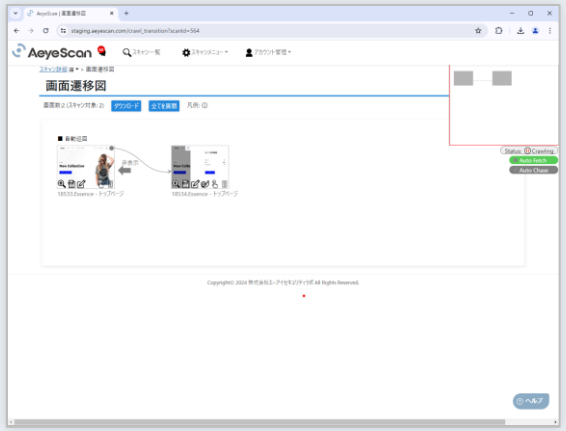
課 題

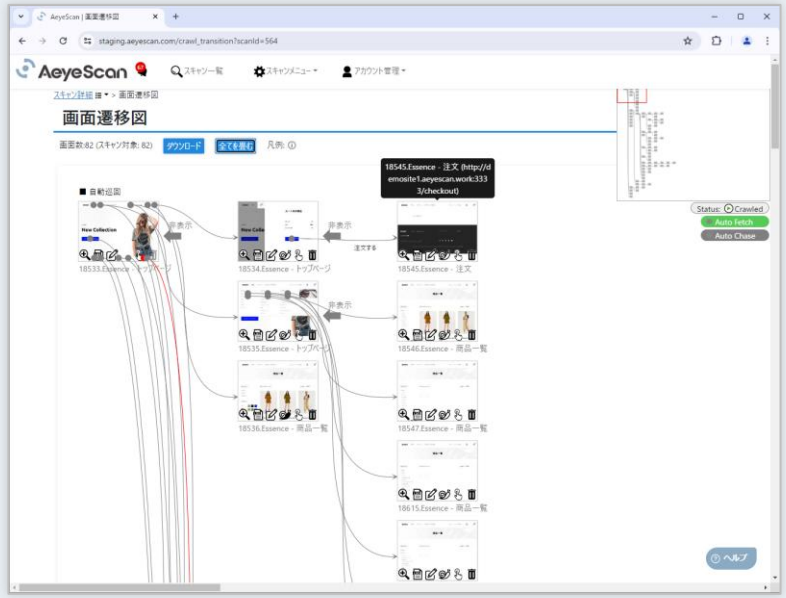
遷移が正しくできていないと、
どこからリンクされている画面か分からなかった

AeyeScanなら、
自動作成された画面遷移図でエラーも瞬時に把握！

ココがポイント

存在しないページなどの404エラーも
すぐに発見できる





簡易診断ではない、本格的なガイドライン準拠

主要なセキュリティガイドラインの自動化可能な項目に対応。フォーム入力検証や認可不備など、**実被害につながる脆弱性を的確に検出**します。

OWASP TOP10

OWASP アプリケーション
セキュリティ検証標準

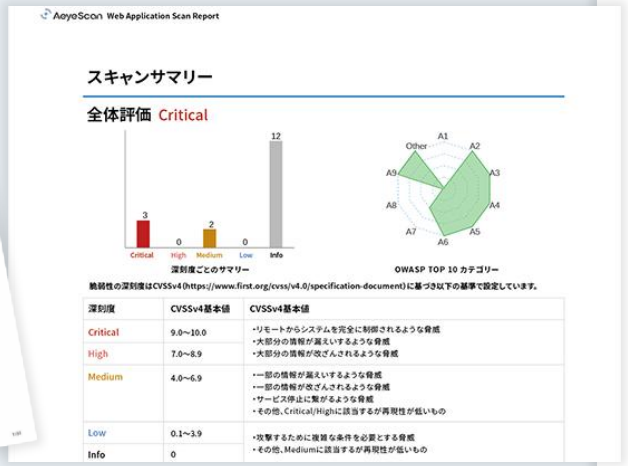
IPA 安全なWebサイトの作り方

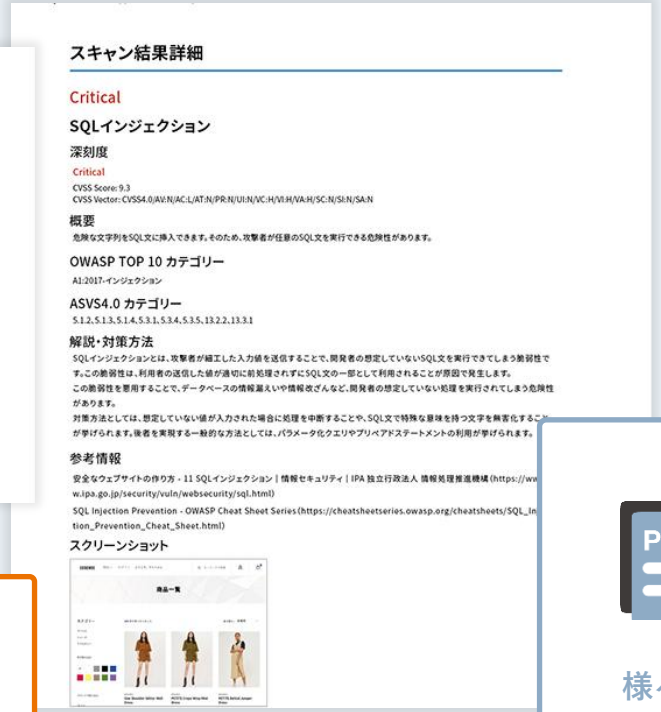
ココがポイント

独立行政法人情報処理推進機構（IPA）が実施した2021年度セキュリティ製品の有効性検証において、
有識者会議による審査の結果、AeyeScanが選定されました。

国内製品ならではの「わかりやすい日本語レポート」

専門知識がなくても理解できる日本語のレポートを自動生成。社内共有や報告工数を大幅に削減できます。





ココがポイント

- どのガイドラインに準拠して検出された項目かがわかる
- どう修正すべきかも記載してあり、そのまま開発者に渡せる
- エグゼクティブサマリも簡単に作成可能

PDF DOC CSV

様々な形式でカンタンに
自動生成ができる！

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

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

インフラ

EPARK
AIRE
HIS
NTT EAST
odakyu
近鉄情報システム株式会社
SymEnergy
水ing
Suzuyo
NANKAI
日本調剤
JARMeC
HITOWA GROUP
BOOK・OFF
ベルーナ
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
KOSÉ
SAKI
TIGER
TEIJIN
Denkei
House
Mizuno
ユーグレナ

エンタメ

イープラス
CAPCOM
GungHo
とらラボ!
BookLive

SaaS

Advanced Media, Inc.
Lexica
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
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
tdi 情報技術開発株式会社
Simplex Inc.
777WORKS
SOFT CREATE
SOLTEC
高千穂交易株式会社
電通総研
TOPPAN
JOPS
JAST
PCNET
Human Interactive Technology inc.
FUJISOFT
FUJITSU
MACROMILL
YONA
リピスト

セキュリティ企業

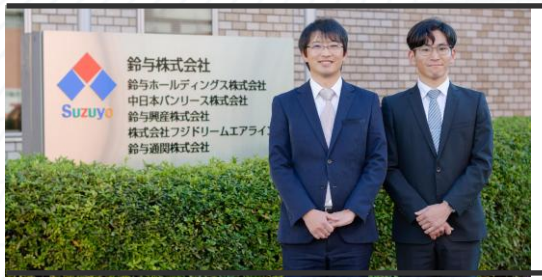
NEC
NECセキュリティ
NTT DATA
GSX
cybertrust
LAC

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

AeyeSecurityLab

導入事例紹介

鈴与 様



企業名	鈴与株式会社
事業内容	総合物流事業
従業員数	1,146人（2024年8月31日時点）

課題

外部ベンダーに診断を依頼していたが、
対象となるWebシステムが増えるほど
コストと時間がボトルネックに

具体的な課題

1. 社外向けWebシステムの開発が増え、診断にかかるコストが膨らんでいた
2. 外部ベンダーに依頼すると、見積もりや契約だけで1か月かかるなど、時間を要してしまう
3. コスト・時間の制約から頻度高く診断を行うことができない

これまで社内向け業務システムの開発が中心だったが、物流データを活用した新たな価値提供を推進するため、社外向けWebシステムを積極的に開発する方針へ転換。しかし、診断にかかるコストと時間がボトルネックになっていた。

導入

セキュリティ専門家でなくても扱える上、
外部ベンダーの診断と同等の品質も評価

導入の背景

1. 診断開始までの工数が少なく、UI含めて誰でも使いやすい
2. OWASPなど業界標準の脆弱性をカバーしており、外注と同等の診断ができる
3. 専門家でなくても、レポートを見れば問題点と必要な対策が理解できる

診断の内製化にあたり、複数ツールをトライアル導入して比較検討。セキュリティの専門家でなくても扱えることや診断品質、レポートのわかりやすさや、画面遷移図で巡回が抜け漏れなく行われているか見えることなどが決め手となり導入。

効果

約3割の診断コスト削減を実現。
診断頻度も増やすことができ、
セキュリティレベルがアップ。

具体的な効果

1. シナリオ作成も1日かからず終えられ、1週間以内には診断開始まで実行できる
2. コスト・時間が削減できただけでなく、開発サイドのセキュリティ意識も向上
3. 従量課金ではないので、今後診断対象の増加に伴いコストメリットも増えると実感

以前までは診断開始までに長いと1か月ほど時間を要していたが、コストを削減しながらスピード感のある診断が実現できるようになった。緊急度の高い脆弱性が見つかった際にはすぐ改修を依頼できるなど、セキュリティレベルの向上につながっている。

AeyeSecurityLab

導入事例紹介

ミズノ 様

企業名　ミズノ株式会社

事業内容　スポーツ用品の開発・販売ほか

従業員数　3,584人（2024年3月31日現在）

課題

国内だけでも約20 Webサイトを運営する中、
定期的な脆弱性診断ができていなかった

具体的な課題

1. サイト立ち上げ時や大規模改修時だけしか診断ができていない
2. 外部ベンダーによる脆弱性診断だと多額のコストがかかる
3. 内部の人材のスキル不足・業務負荷が高くなる

グローバル全体でセキュリティポリシーを見直し、その中に定期的な脆弱性対策を含めたものの、外部ベンダーによる脆弱性診断だとコストがかかる。内製化を検討するもスキル不足や業務過多といった課題があることから、自分たちでも使える診断ツールの導入を検討。

導入

定額で複数サイトに外部ベンダーによる
脆弱性診断と変わらないクオリティの診断が
できると評価

導入の背景

1. 専門知識を持たなくても簡単に操作できる
2. サイト数に比例して費用が増加しない
3. 外部ベンダーによる脆弱性診断と同等の品質で診断できる

AeyeScanのトライアルを行い、簡単に操作できることを実感。また、同一サイトに対して、外部ベンダーによる脆弱性診断による診断とAeyeScanによるスキャンを並行して行いレポートを比較。AeyeScanの方が同レベル以上・検知項目が多かったことから、導入を決めた。

効果

定期的な診断が可能な体制が整った。
時間短縮により、
診断後の対策、チェックもスムーズに

具体的な効果

1. 内製化により、診断にかかる時間が数ヶ月単位から数週間に短縮
2. 診断、対策、チェックの運用がきれいに回せている
3. 開発ベンダーとのコミュニケーションもスムーズになった

外部ベンダーによる脆弱性診断では脆弱性への対応も含めて数ヶ月単位の時間がかかっていたが、数週間で診断を終えてすばやく対策できるようになった。レポートに具体的な修正方針も示されるため、開発ベンダーとのコミュニケーションもとれ、対策もスムーズになった。

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

会社概要

商号	株式会社 エーアイセキュリティラボ	
役員	代表取締役社長	青木 歩
	取締役副社長	安西 真人
	取締役	杉山 俊春　角田 茜
	執行役員 CTO	浅井 健
	執行役員	関根 鉄平
事業内容	情報セキュリティ関連事業（調査・コンサルティング） セキュリティ診断クラウドサービス「AeyeScan」提供	
設立	2019年4月	
拠点	東京都千代田区神田錦町2-2-1 KANDA SQUARE 11F WeWork内	
資本金	1億円	
社員数	57名	
Webサイト	https://www.aeyesec.jp/	
取得認証	情報セキュリティマネジメントシステム（ISMS） ISMSクラウドセキュリティ認証（ISO27017） 情報セキュリティサービス基準適合サービスリスト	

AeyeSecurityLab

セキュリティに
「あらたな答え」を提供し続ける
プロ集団

IS 752963 / ISO 27001

CLOUD 790050 / ISO 27017

023-0026-20

セキュリティに、確かな答えを。