さらば！“ヒト”まかせの脆弱性対策

AIとつくる

新しいセキュリティ運用のカタチ

登壇者紹介

主な著書

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。

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

サイバー攻撃が高度化し、セキュリティ対策が難しくなっている

攻撃者

AIや自動化ツールの活用により
攻撃が容易化・高度化

企業

必要なセキュリティ対策の
対応範囲・難易度が上昇

脆弱性対策の継続的な運用はますます困難に。
しかし、人手・予算はなかなか増えない

多くの現場で「判断が追いつかない」問題が起きている

アラート対応

どこまで無視していい？

脆弱性対応

自社環境で本当に危ない？

優先順位づけ

どこまでやれば合格？

説明責任

「安全です」と言えるか？

事業継続

サービス止めてまで直す？

セキュリティ対策の課題として「人手不足」が挙げられがちだが…

「人を増やしても、意外と楽にならない」が現場の実感？

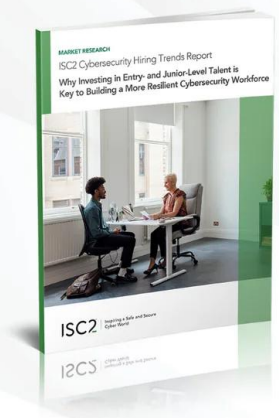
問題の本質は「人手不足」ではないところにある

問題の本質は、「人手不足」ではなく「スキル不足」…？

ISC2：2025年版「サイバーセキュリティ人材調査」

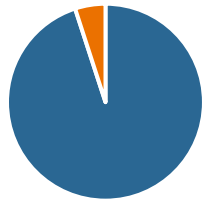
ISC2™ RESEARCH

2025 Cybersecurity Hiring Trends



何らかのスキル不足を抱えている

→ **Yes.** 世界の回答者の **95%**



内、自組織でスキル不足に起因する
重大インシデントを少なくとも1回経験 **88%**

では、解決策は「スキルの補充/スキルを持った人材の補充」なのか…？

出典：ISC2：2025年版「サイバーセキュリティ人材調査」 https://prtimes.jp/main/html/rd/p/000000024.000103584.html

「スキルの補充」では解決しない3つの理由

処理能力の限界

**判断に必要な情報が多すぎて
人間が処理しきれない**

人員を増やしても情報処理の
「複雑さ」は解消されない

**個人の能力には
物理的な限界がある**

属人化

**高度なセキュリティ判断は
ベテランの頭の中にしかない**

訪れるのは
“質のバラつき”と“教育コスト”

**属人化は、組織としての
新たな脆弱性を生む**

戦略の不在

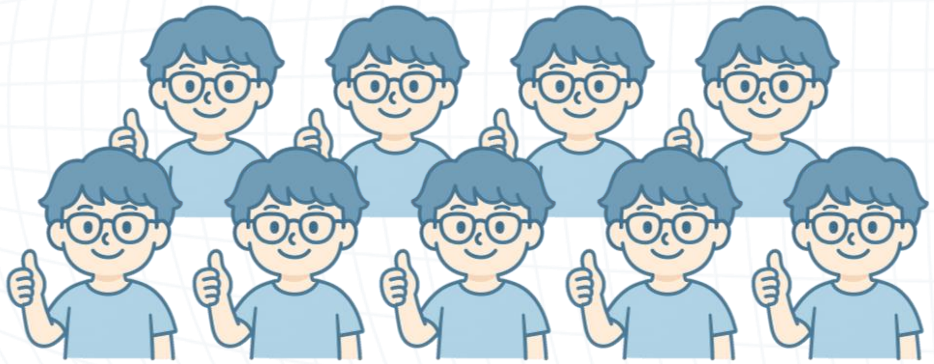
**目の前の現場対応に追われ
中長期的な設計が後回しに**

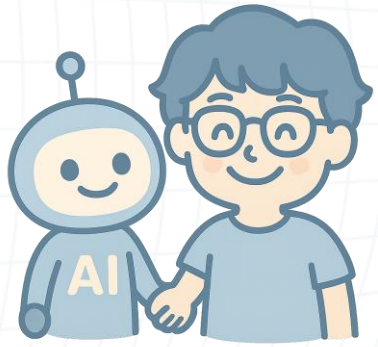
スキルを磨くほど職人技に依存し
仕組み化から遠ざかる

**実務（How）を極めても
構造は変えられない**

「誰でも判断・対応できる仕組みづくり」が必要

これまで	これから
人が頑張る・人が判断する	仕組みを作る・仕組みで判断する





セキュリティ判断を「スキルに依存した作業」から「設計されたプロセス（仕組み）」に変える

発想の転換 が必要

仕組みに転換するための「３つのステップ」

まずは「ちゃんぽん」で考えてみましょう。

Step1

材料を分解する

Step2

レシピ化する

Step3

機械と人間で役割分担し
再現可能な形にする

AIとの協働で「判断を仕組み化する」ための具体的な取り組み

例）脆弱性管理のプロセスを仕組み化する場合

判断を「分解」する

「この脆弱性は危険か？」ではなく、
構成要素に分解する

- 悪用可能性（Exploit）
- 到達可能性（Exposure）
- 事業影響（Impact）

AIと人間が協働して
判断材料を集約する

判断を「形式知化」する

CVSS（数値）だけでなく、
業務文脈をルール化する

- ビジネス観点の重要度は？
- システム停止時の影響範囲は？
- 業務継続の代替手段はある？

判断の「観点」をルール化し
組織の判断能力を「複製」する

判断を「仕組み化」する

AIと役割分担し、
人は設計と例外処理に注力する

AI

- 情報収集
- 情報整理
- 反復作業

人間

- 例外処理
- 経営判断
- 仕組みの設計

人を「作業」から解放し
本来の「戦略」に注力させる

まずは、脆弱性診断から「判断の仕組み化」に着手しませんか？

脆弱性診断は…

情報処理が重い

脆弱性情報・
資産情報・ログなど
判断材料が膨大

判断の再現性が重要

属人化により
優先度がぶれると
対応品質が安定しない

説明できる判断が必要

対策方針の理由を
言語化できないと
経営の合意が得られない

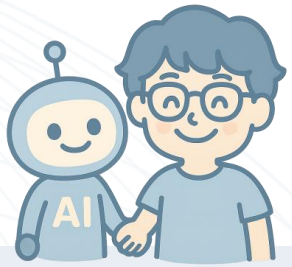
継続運用が前提

一度きりではなく
日々発生し続けるため
仕組み化が必要

だから、AI活用によって「品質」を維持しながら「効率」を高められる！

AeyeSecurityLab

AIとの協業で効率的なセキュリティ対策を実現する脆弱性診断プラットフォーム「AeyeScan」



未把握のWeb資産の可視化・リスク評価から脆弱性診断まで、各工程で自動化を実現。
持続可能なセキュリティ運用の仕組みをご提供します。

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。

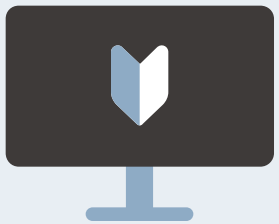
2

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！

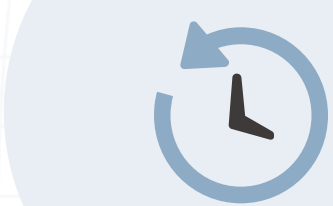
AeyeSecurityLab

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
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（2023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

人材・教育

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

インフラ

EPARK
AIRE
HIS
H.O RETAILING
NTT EAST
odakyu
近鉄情報システム株式会社
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
JARMeC 日本動物高度医療センター
HITOWA GROUP
BOOK・OFF
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
エアアドエムネット株式会社
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 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 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
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

導入事例紹介

エイチ・アイ・エス 様

企業名　株式会社エイチ・アイ・エス

事業内容　総合旅行会社

従業員数　10,849名（2023年6月時点）

課題

セキュリティの内製化が困難。
診断の外注コストを削減したい

具体的な課題

1. 社内からの診断依頼が増え続けていた
2. 診断対象が多く外部委託せざるを得ない
3. 外注による診断コスト増

内製・外製含め100を超えるWebアプリケーションがあり、内部の体制だけでは全ての診断実施に対応できず、一部を外部に委託。コスト削減と体制整備が課題だった。

導入

情報処理推進機構（IPA）の検証結果と
「7割以上自動化」という点が決め手

導入の背景

1. 手動の診断では対応が追い付かず自動化を検討していた
2. 自動化できても性能が落ちない製品を探していた

手動作業を伴う診断では対応が困難になり、診断の自動化を検討。AeyeScanは、IPAの検証結果が高評価だったことと、「7割以上の自動化が可能」という点が決め手で導入。

効果

診断・レポート作成工数を大幅に削減。
さらなる内製化比率の向上を目指す

具体的な効果

1. 診断の大部分を自動化し工数を削減
2. レポート機能により大幅に時間を短縮
3. リリース前に診断と脆弱性改修が完了

「脆弱性が発覚しても、リリースまでに修正が間に合わない」という悩みも解消され、脆弱性を潰してからアプリをリリースできるように。

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名（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。

AeyeSecurityLab

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 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／

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

自席で視聴可能！お気軽にご参加ください

詳細・お申し込みはこちら

セキュリティに、確かな答えを。