人手不足のEC現場をAIが救う！

セキュリティ診断“義務化”対応の自動化術

AeyeSecurityLab

登壇者紹介

株式会社エーアイセキュリティラボ

執行役員兼CX本部長 **関根 鉄平** CISSP

セキュリティエンジニアとして大手金融機関等の脆弱性診断に従事。その後、Webアプリケーション検査ツール・サポートチームの立ち上げをしつつ、CSIRTや開発現場でのセキュリティを推進。
2020年6月より現職。AeyeScanのカスタマーサクセスチームの責任者として脆弱性診断の内製化を支援。大規模イベントや大手企業での講演に多数登壇。
『セキュリティエンジニアの知識地図』を共著。

コミュニティ活動など

- 情報セキュリティ10大脅威 選考会メンバー
- OWASP/ISOGJ アジャイル開発におけるセキュリティ｜パターン・ランゲージ
- 『脆弱性トリアージガイドライン作成の手引き』共同執筆

クレジットカード・セキュリティを取り巻く状況

- クレジットカード番号等の非保持化に対応していても、
  ECサイト自体が改ざんされることで
  クレジットカード番号等が流出する事案が発生

- オープンソースにより構築されている、適切なアップデートを行わないなど、**十分なセキュリティ対策を講じていない**
  ECサイトが攻撃の対象になりやすい

出典：経済産業省　商務・サービスグループ 商取引監督課 「最近の主な漏洩事案」

クレジットカードの不正利用被害額は年々増加

2025年のカード不正利用被害額

1月～9月時点ですでに**416.6億円**

↓

そのうち**93.3%**が

クレジットカード番号の盗用被害

クレジットカード不正利用被害の発生状況

（単位：億円、%）

期間	クレジットカード不正利用被害額	クレジットカード不正利用被害額の内訳					
		偽造カード被害額		番号盗用被害額		その他不正利用被害額	
		被害額	構成比	被害額	構成比	被害額	構成比
2020年（1月～12月）	253.0	8.0	3.2%	223.6	88.4%	21.4	8.5%
2021年（1月～12月）	330.1	1.5	0.5%	311.7	94.4%	16.9	5.1%
2022年（1月～12月）	436.7	1.7	0.4%	411.7	94.3%	23.3	5.3%
2023年（1月～12月）	540.9	3.1	0.6%	504.7	93.3%	33.1	6.1%
2024年（1月～12月）	555.0	5.9	1.1%	513.5	92.5%	35.6	6.4%
（1月～3月）	124.1	0.7	0.6%	115.1	92.7%	8.3	6.7%
（4月～6月）	135.9	0.9	0.7%	126.3	92.9%	8.7	6.4%
（7月～9月）	132.7	2.1	1.6%	121.4	91.5%	9.2	6.9%
（10月～12月）	162.3	2.2	1.4%	150.7	92.8%	9.4	5.8%
2025年（1月～9月）	416.6	6.2	1.5%	388.8	93.3%	21.6	5.2%
（1月～3月）	193.2	1.8	0.9%	182.9	94.7%	8.5	4.4%
（4月～6月）	121.4	1.1	0.9%	113.3	93.3%	7.0	5.8%
（7月～9月）	102.0	3.3	3.2%	92.6	90.8%	6.1	6.0%

出典：クレジットカード不正利用被害の発生状況

クレジットカード番号の盗用による被害は2021年以降常態化

不正利用は、“カード会社の問題”ではなく“すべてのEC事業者の経営リスク”

EC事業者が実施すべきセキュリティ対策とは？

非保持化

- カード情報保護のための取組として「非保持化」を推進

PCI DSS 準拠

- 業態、システム・ネットワーク構成に適した要求事項に対応

NEW 脆弱性対策

- 全てのEC加盟店は、5つの具体的な脆弱性対策をすべて実施

クレジットカード・セキュリティガイドライン【 6.0版 】において、
「EC 加盟店のシステム及び Web サイトの**脆弱性対策**を講じる。」という記述が追加された。
つまり、**義務化**されたといえる

参考：https://www.meti.go.jp/press/2024/03/20250305002/20250305002.html

義務化された「脆弱性対策」の具体的な内容とは？

クレジットカードの情報漏えいを防ぐ5つの脆弱性対策

1. システム管理画面のアクセス制限と管理者のID／パスワード管理
2. データディレクトリの露見に伴う設定不備への対策
3. Webアプリケーションの脆弱性対策
4. マルウェア対策としてウイルス対策ソフトの導入、運用
5. 悪質な有効性確認、クレジットマスターへの対策

Point

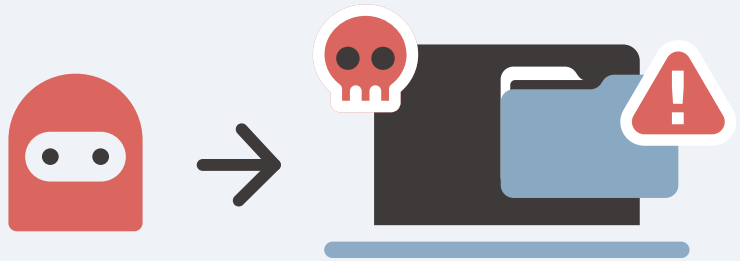
システムだけでなく、

商品・サービス・金額等が掲載され消費者が閲覧するWebサイトやLPなどのWebページも対象となる

【出展】クレジットカード・セキュリティガイドライン【6.0版】 改訂ポイント

そもそも、脆弱性診断（セキュリティ診断）とは？

脆弱性を突いた攻撃を受けた際に、被害につながる可能性がないか検証すること



システムやアプリケーションに潜む
脆弱性を放置していると、
サイバー攻撃を受けて企業の機密情報や
個人情報が漏えいする危険性が高まる。

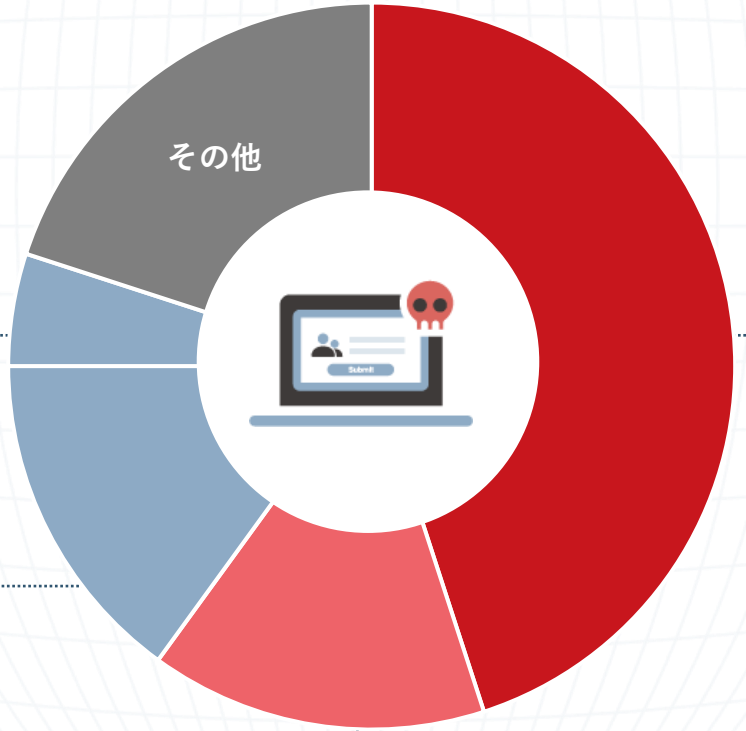
脆弱性診断は、Webサイト・サーバ・ネットワークに実施する必要がある。
中でも頻繁に改修がなされ、攻撃対象として狙われやすいWebサイトには定期的な診断が必要。

定期的な脆弱性診断を阻む要因のほとんどは「人材不足」と「コスト」

ECサイトへの継続的なセキュリティ対策が実施できない理由

5%

前任者が退職し、後任者における
セキュリティ対策の引継ぎや知見の
キャッチアップが不十分であった



45%

EC サイトの運営で主に
セキュリティ対策の**必要性を認識**
している人員がいなかった

15%

外部委託先にセキュリティ対策を
依頼しているつもりであったが、
認識されていなかった

15%

事業全体の売上高に比較して、EC事業
による売上高の割合が低い(5%以下)
ため、**費用を掛けられなかった**

出典：ECサイト構築・運用セキュリティガイドライン

定期的な脆弱性診断を継続していくために

脆弱性診断を外部委託する

コストが高い

自社にノウハウが残らない

脆弱性診断を内製化する

専門人材がいない

どのツールを選べばいいか
わからない

コストを抑えつつ、専門人材がいなくても実施できる脆弱性診断ツール

AeyeScanをご紹介させてください！

AeyeSecurityLab

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！

Demonstration

製品デモ

AI活用のレベルが高いので、自動巡回が高精度で範囲が広い

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…**

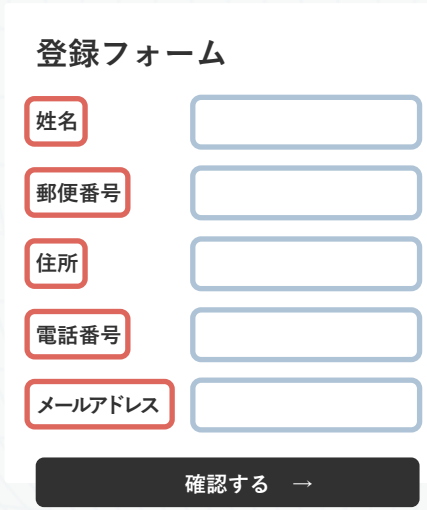
AeyeScanなら、
正確に入力値を推測して巡回！

ココがポイント

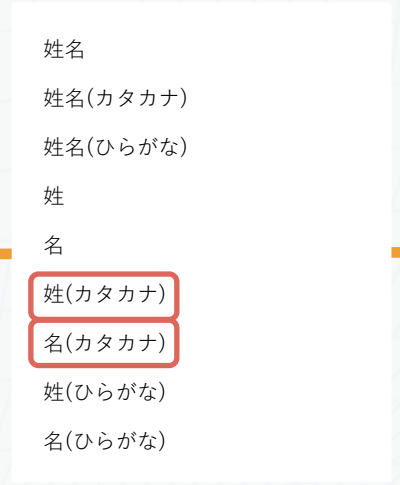
名前や住所など決まった項目だけでなく、
どんな項目にも対応！

例えば
- クレジットカード
- 画像アップロード

フォームを自動認識しラベル化



自動認識したラベル(赤枠)に応じ
適切な入力値を設定



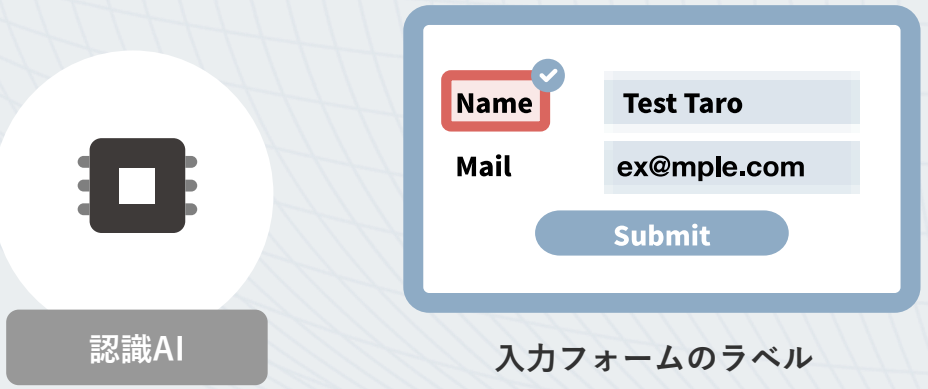
正常遷移

適切な値を入力

生成AIを使えば、巡回はここまで進化できる

認識AIができること

画面上の入力フォームのラベル（氏名など）を
認識AIが判断することでフォームに入力する



生成AIができること

生成AIを使うことで、人が画面を見るように
「これは商品画面」「これはお知らせ画面」と
判断できる！

生成AIの活用による高度な自動化を実現

生成AI機能

1 診断設定がさらにカンタンに

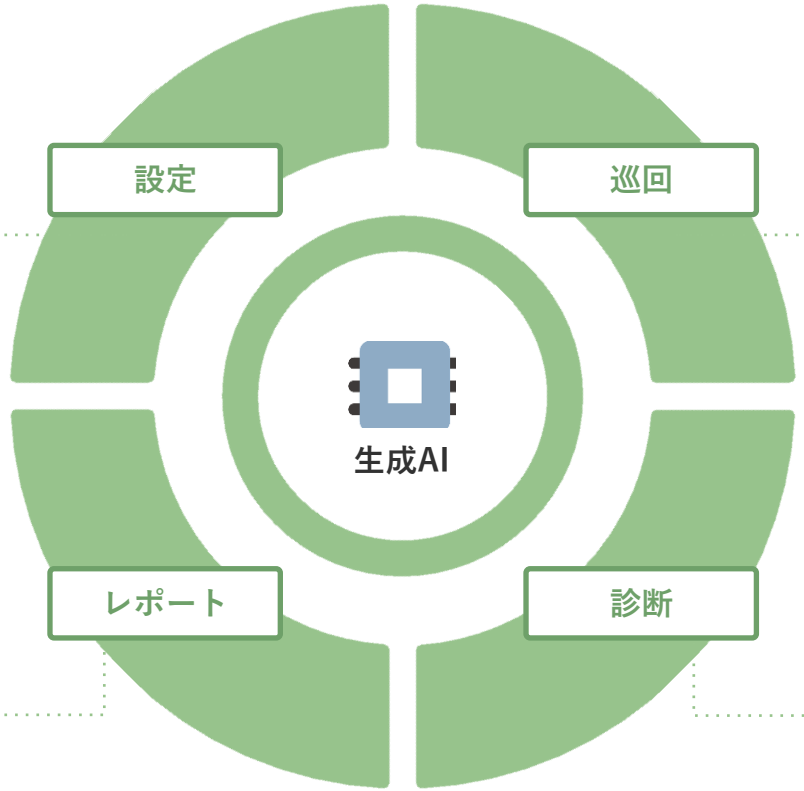
- フリーフォーマットでの指示

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



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

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

各種セキュリティガイドラインの自動化可能な項目に対応

OWASP TOP10

日本語版PDFはこちら

OWASP アプリケーション
セキュリティ検証標準

OWASP github

IPA 安全なWebサイトの作り方

PDFはこちら

ココがポイント

- 経済産業省が策定した「情報セキュリティサービス基準」に適合している脆弱性診断サービスとして、AeyeScanが「情報セキュリティサービス台帳」に登録
- 独立行政法人情報処理推進機構（IPA）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

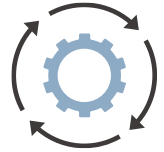
023-0026-20

ドメインごとの課金ではなく「定額プラン」

複数のWebサイトを運営していても診断し放題だから…

リリース直前の診断や、
継続的な再診断も
負担なく実施できる

診断を運用サイクルに
組み込みやすく、
チームで取り組める



継続的かつ高頻度な診断により、セキュリティ強化を実現

まとめ

義務化したWeb脆弱性診断を適切な頻度で行うべく

ツール活用による「自動化」に、
積極的に取り組んでいきましょう！

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

製造

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

インフラ

EPARK
ARE
HIS
H2O RETAILING
NTT EAST
odakyu
近鉄情報システム株式会社
GEO
SymEnergy シン・エナジー
水ing Swing Corporation
Suzuyo
NANKAI 南海システムソリューションズ
HITOWA GROUP
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

人材・教育

Junion
JINSOKEN
ZENKIGEN
Direct Sourcing
PERSOL
Leverages
workport

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
estie
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
DMM Boost
TAL
Digital Garage
TEMONA
NAVITIME
KNOCK ON THE DOOR
BATONZ
VALUE HR
Finovo
freee
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.
SB Technology
SBWorks
NTT DATA
NTT ビジネスソリューションズ
OMRON
Globalway
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 TAKACHIHO KOHEKI CO.,LTD.
電通総研
TOPPAN
JOPS
JAST
NHC
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

AeyeSecurityLab

導入事例紹介

ベルーナ 様

企業名　株式会社ベルーナ

事業内容　アパレル・雑貨事業、プロパティ・ホテル事業など

従業員数　連結 3,884名(2025年3月31日現在)

課題

事業の多角化で増加する
数十ものWebサイトに対し
均質な診断を実施するのが難しい

具体的な課題

1. 外部委託ではコストがかさみ、診断範囲を限定せざるを得ないことも
2. 全体で一定水準以上の品質を保ちたい
3. 毎回異なる事業者に依頼しており調整の手間もかかる

多様な事業を展開する中、Webサイトは重要な顧客接点だが、増え続けるWebサイト全体に同一レベルの対策ができていなかった。内製のほうがコスト効率がよく、セキュリティ面でもよい選択ができると考えた。

導入

サブスクリプション形式で
使い勝手や診断品質にも優れた
AeyeScanを採用

導入の背景

1. シナリオ作成から診断の実施、レポート作成まで簡単にできる
2. 画面遷移図で診断中の箇所やスキャン結果がわかりやすく示される
3. 診断品質も十分なレベルに達している

AIを活用した他の診断ツールも試した上で、設定の簡単さなど、使いやすさを評価。トライアルを行い、以前受けたベストエフォート型診断サービスと比較しても診断品質が十分だと判断し、AeyeScanを採用。

効果

すべての事業に均質な診断を実現
診断回数を増やしながら
コストが半減

具体的な効果

1. 網羅的な定期診断と、改修時のスポット診断を内製で実現
2. 修正、再診断までのスピードが向上
3. セキュリティを標準化しつつ、費用、時間、工数の最適化が実現

導入後は、事業全体で横断的な診断が可能に。分かりやすいレポートにより改修スピードが向上し、診断回数を増やしつつ、コストは半分以下に削減。セキュリティの標準化とリソース最適化を実現できた。

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

セキュリティに、確かな答えを。