AIと人間が“賢く”分業する

DX時代の セキュリティ対策

AeyeSecurityLab

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CXチームでの活動に加え、新規プロダクト企画・海外事業
展開など全社横断プロジェクトにも携わる。

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

進む「DX」
増える「セキュリティ対策の悩み」

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%

参考：IPA「DX動向2024： https://www.ipa.go.jp/digital/chousa/dx-trend/eid2eo0000002cs5-att/dx-trend-2024.pdf」

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。

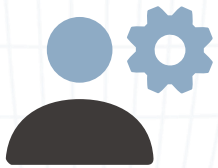
IPAが提言するDXに必要な要素

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



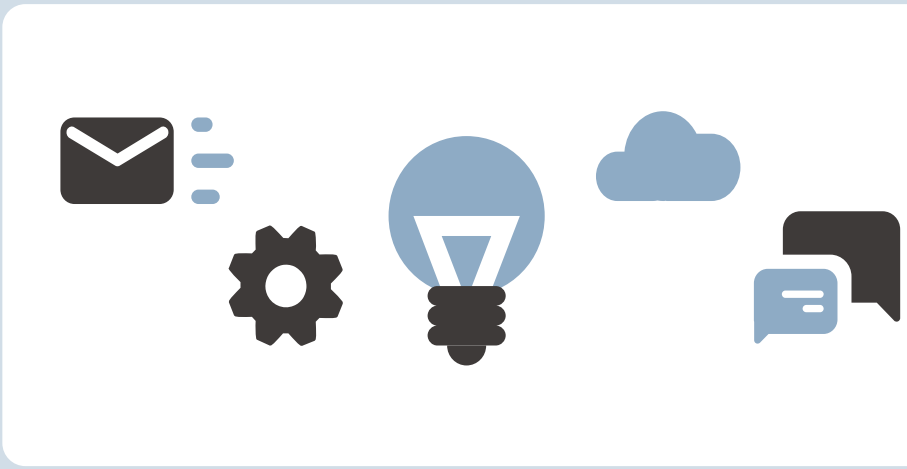
ビジネス上の
ニーズに合致する

データ活用と分析

参考：IPA「DX動向2024： https://www.ipa.go.jp/digital/chousa/dx-trend/eid2eo0000002cs5-att/dx-trend-2024.pdf」

DXの進展でセキュリティ対策の需要は高まっている

DX



セキュリティ

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

=

必要なセキュリティ対策の

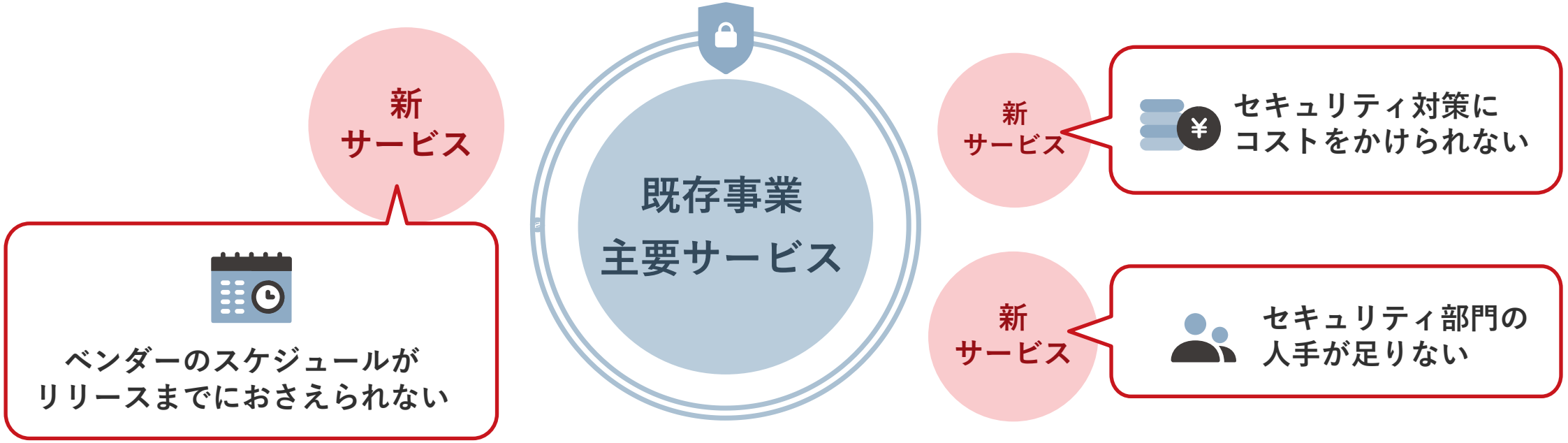
対応範囲は拡大

難易度は上昇

DXの進展に伴う「セキュリティ対策の悩み」

対応範囲は広がる一方、時間・予算・人材は足りない

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時代のセキュリティ対策
カギは「人間とAIの分業」

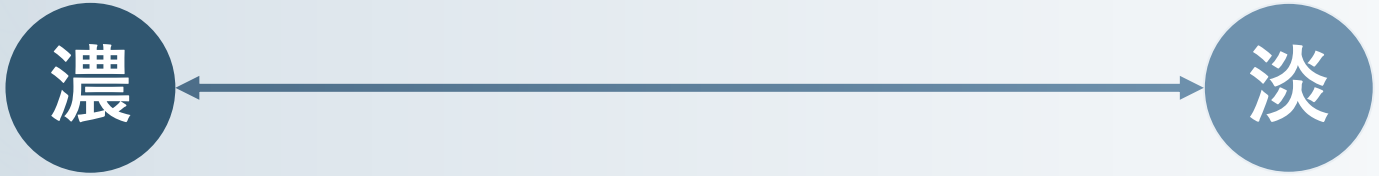
DX時代のセキュリティ対策の考え方

限られたリソースを、どのように配分するか？

濃淡をつける・取捨選択する・選択と集中

手間と時間をかけて専門家が対応する

人的リソースを最小化しつつ対応する

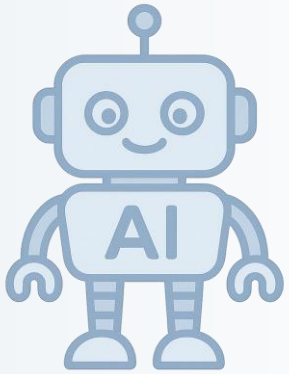


DX時代のセキュリティ対策を実行する上での課題

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



AIを活用した「自動化・内製化」で解決できないか？

個別のセキュリティ対策・施策から「まずAIを使ってみる」

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

AIと相性の良いセキュリティ対策：脆弱性診断

継続的・永続的に対策が必要	⟷ 人力では**生産性が上がらない**
網羅的に診断することが望ましい	⟷ 網羅性を高めると**費用も増える**

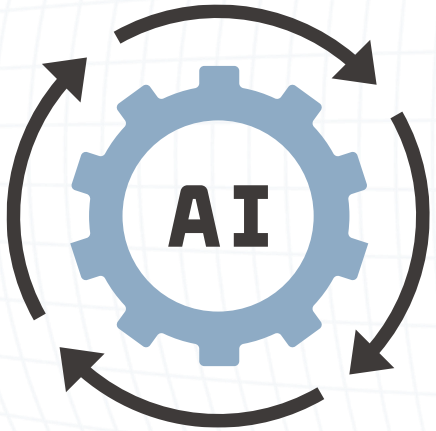
AIによる自動化・内製化ができれば

業務の効率化・費用の最適化につながりやすい

脆弱性診断にAIを活用する方法

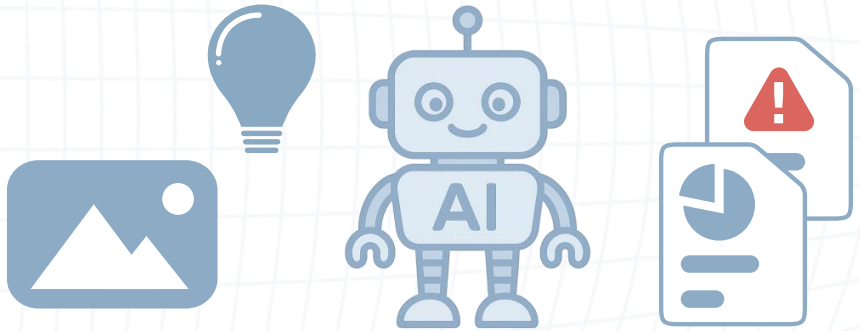
改めて…AIは何ができる？何が得意？

今までのAI



繰り返しの作業
ルールベースの作業

これからのAI



その場に応じて判断が必要な作業
文脈（前後関係）を考慮した作業

AIを活用して、脆弱性診断を自動化・内製化できるのか…？

？

診断の**品質を維持**できるだろうか？

？

コスト（費用・時間）を抑えられるか？

？

社内メンバーで対応できるだろうか？

AIを活用して、脆弱性診断を自動化・内製化できるのか…？

？

診断の**品質を維持**できるだろうか？

ルールベースの診断は
人間と同等の品質

文脈・判断が必要な診断も
どんどん対応可能に

？

コスト（費用・時間）を抑えられるか？

人間がやるより何倍も速い

費用も工数に依存せず
一定範囲に抑えられる

？

社内メンバーで対応できるだろうか？

もはや診断自体には
人間が介在しない

人間は、サイト・アプリの
理解を助けてあげる存在

AI活用で、どこまで脆弱性診断を自動化・内製化できるのか…？

診断準備

- 対象調査
- 要件定義
- 環境準備
- 日程調整
  契約・発注

診断実行

- シナリオ作成/サイト巡回
- 脆弱性診断
- 結果報告

修正対応

- トリアージ
- 修正対応
- 再診断

脆弱性診断にAIを活用して
“DX時代のセキュリティ対策”を実現！

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「2024 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〉2023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）

有償契約
300社以上

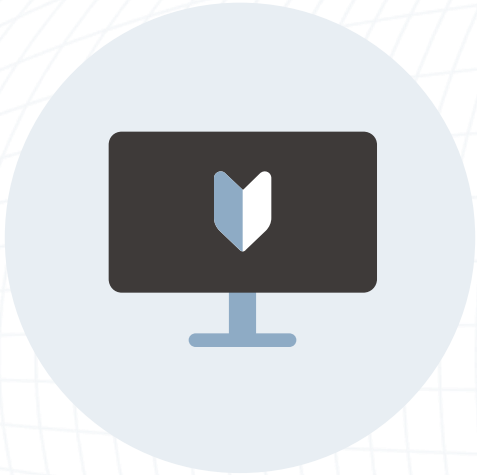
01
高精度なAI活用
巡回精度が高く
画面遷移図で見てわかりやすい

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

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。

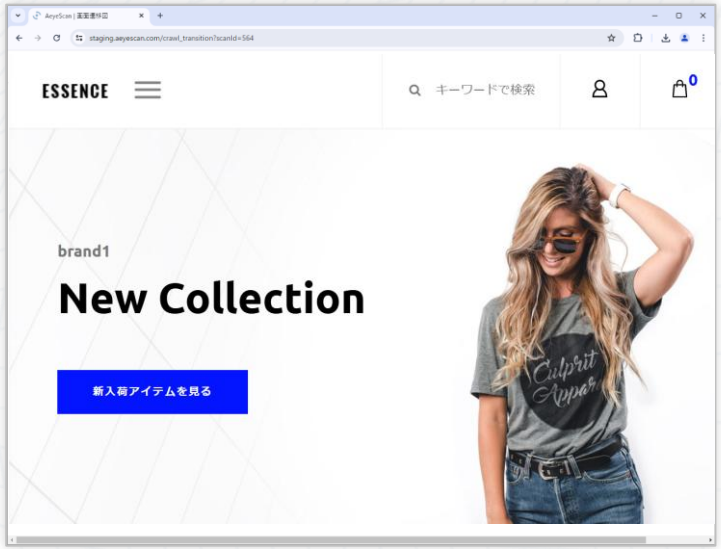
AIによる自動診断

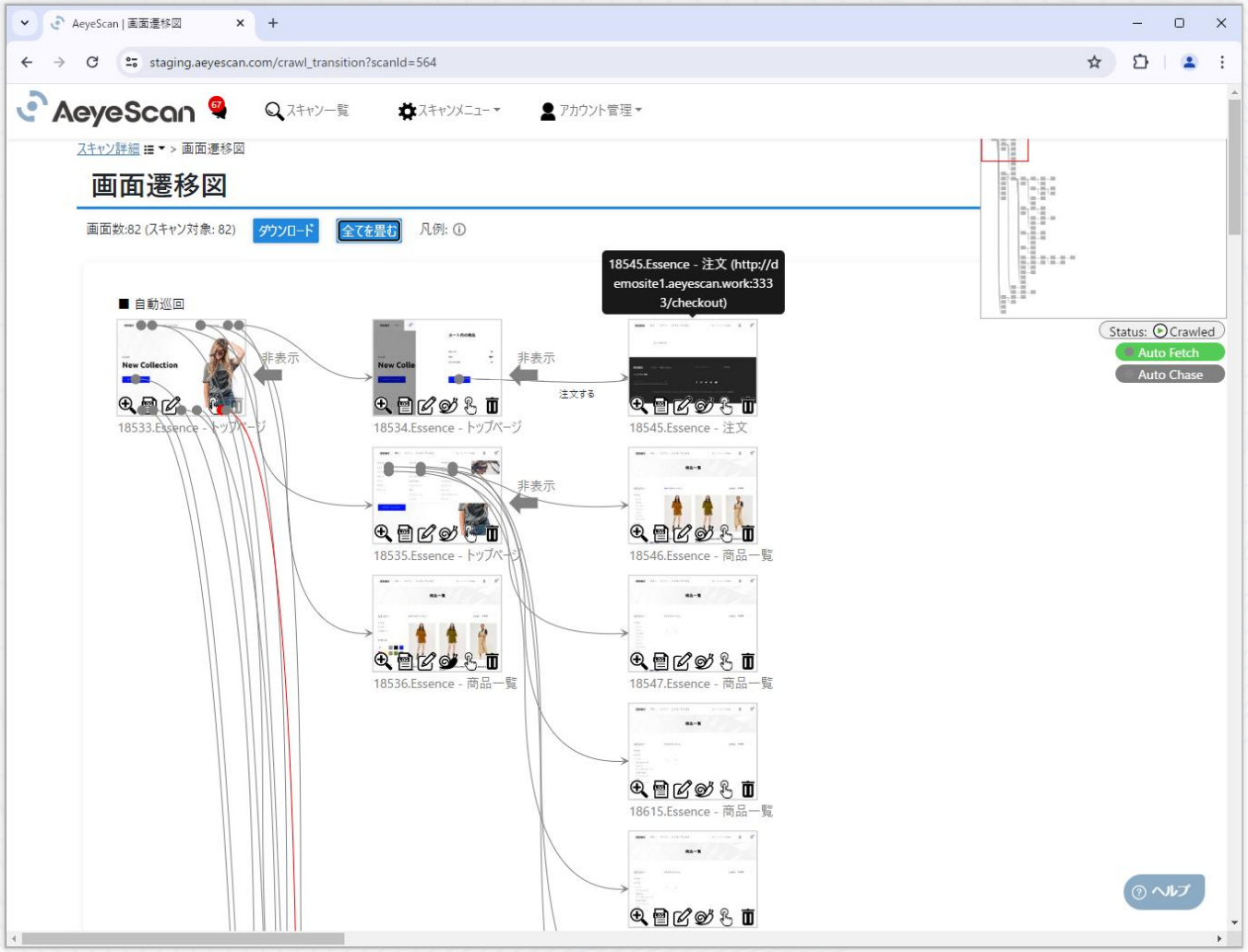
圧倒的な巡回精度で
24時間自動で診断。
画面遷移図で状況を可視化。

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。

巡回時に、自動で画面遷移図を生成





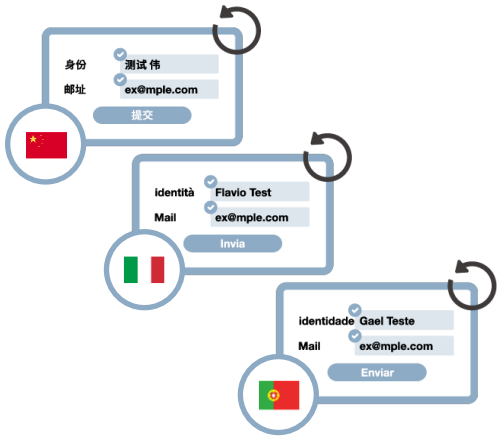
AeyeSecurityLab

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

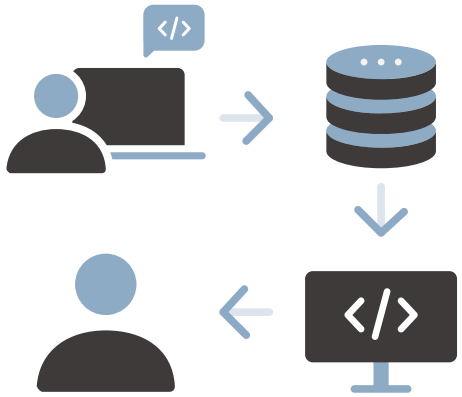


- 日本語
- 英語
- フランス語
- 中国語
- 韓国語
- オランダ語
- ドイツ語
- イタリア語
- ポーランド語
- スペイン語
- ポルトガル語
- ロシア語
- スウェーデン語
- アラビア語
- …

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

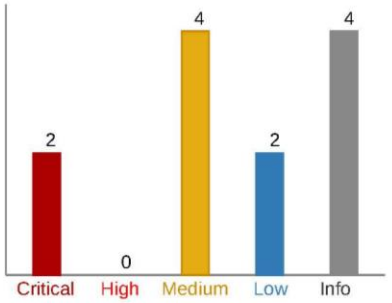


認可の不備・権限昇格

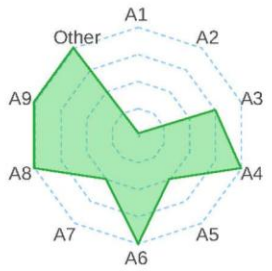
結果がわかりやすく、すぐさま修正作業に取り組めるレポート

スキャンサマリー

全体評価　Critical



深刻度ごとのサマリー



OWASP TOP 10 カテゴリー

脆弱性の深刻度はCVSSv3 (https://www.ipa.go.jp/security/vuln/CVSSv3.html) に基づき以下の基準で設定しています。

深刻度	CVSSv3基本値	脆弱性に対して想定される脅威
Critical	9.0～10.0	・リモートからシステムを完全に制御されるような脅威 ・大部分の情報が漏えいするような脅威 ・大部分の情報が改ざんされるような脅威
High	7.0～8.9	
Medium	4.0～6.9	・一部の情報が漏えいするような脅威 ・一部の情報が改ざんされるような脅威 ・サービス停止に繋がるような脅威 ・その他、Critical/Highに該当するが再現性が低いもの
Low	0.1～3.9	・攻撃するために複雑な条件を必要とする脅威 ・その他、Mediumに該当するが再現性が低いもの
Info	0	

スキャン結果詳細

Critical

SQLインジェクション

深刻度

Critical

CVSS Score: 9.8
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

概要

危険な文字列をSQL文に挿入できます。そのため、攻撃者が任意のSQL文を実行できる危険性があります。

OWASP TOP 10 カテゴリー

A1:2017-インジェクション

ASVS4.0 カテゴリー

5.1.2,5.1.3,5.1.4,5.3.1,5.3.4,5.3.5,13.2.2,13.3.1

解説・対策方法

SQLインジェクションとは、攻撃者が細工した入力値を送信することで、開発者の想定していないSQL文を実行できてしまう脆弱性です。この脆弱性は、利用者の送信した値が適切に前処理されずにSQL文の一部として利用されることが原因で発生します。

この脆弱性を悪用することで、データベースの情報漏洩や情報改ざんなど、開発者の想定していない処理を実行されてしまう危険性があります。

対策方法としては、想定していない値が入力された場合に処理を中断することや、SQL文で特殊な意味を持つ文字を無害化することが挙げられます。後者を実現する一般的な方法としては、パラメータ化クエリやプリペアードステートメントの利用が挙げられます。

参考情報

安全なウェブサイトの作り方 - 1.1 SQLインジェクション | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構 (https://w

生成AIが効率的かつ信頼性の高い探索を可能に

生成AIを活用したWeb-ASM機能

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
辿ったルートを説明

発見したWebサイトの属性を自動判定し＆重要度をランク付け

サイト用途

Medium

- ECサイト
- VPN管理サイト

Low

- 外部SaaSサイト
- テストサイト

保持データ

High

- 個人情報
- クレジットカード情報

利用技術

Low

- WordPress
- EC-CUBE
- 旧式技術
  （JSP/PHP/CGIなど）

技術スタックだけでなく「ビジネス上の重要度」をもとに判定することで

効率的なリソース配分・戦略的セキュリティ対策を実現

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

製造

AISIN
KOSÉ
SAKI
TIGER
TEIJIN
Mizuno
ユーグレナ

インフラ

HIS
H.I.S. RETAILING
odakyu
近鉄情報システム株式会社
水ing Swing Corporation
Suzuyo
NTT東日本
HITOWA GROUP
grow up together MEDIA
Looop
Loyalty Marketing, Inc.

金融

アイフル
JOBPAY
SOMPOひまわり生命
DMM FinTech
Tokyo Century

メディア

集英社
中日新聞
NIKKEI

人材・教育

Junion
JINSOKEN
Schoo
ZENKIGEN
Direct Sourcing
PERSOL

エンタメ

イープラス
CAPCOM
とらラボ! TORANOANA LABORATORY

Leverages

SaaS

Advanced Media, Inc. 株式会社アドバンスト・メディア
estie
M-aid
エムティーアイ
OZ INTERNATIONAL
Classi
COACH A Co.,Ltd.
cybozu
Speee
SecureNavi
DMM Boost
TAL
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 AT
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
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
電通総研
TOPPAN
JOPS
NHC
Human Interactive Technology Inc.
FUJISOFT
FUJITSU
MACROMILL
MITSUBISHI ELECTRIC
YONA
リピスト

セキュリティ企業

NEC NECセキュリティ
NTT DATA NTTデータ先端技術株式会社
GSX
cybertrust
LAC

社名五十音順（導入いただいた企業様の一部です）

本日のまとめ

AIで実現するDX時代のセキュリティ対策

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

＼AIの活用／ → 脆弱性診断の
自動化・内製化

AIを活用して「攻め」と「守り」を両立しましょう！

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。