DXを加速させる

「戦略的」セキュリティ対策の要諦

-AIを活用した脆弱性診断の内製化・運用の“いろは”-

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。

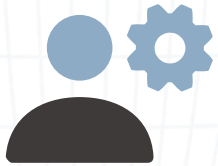
IPAが提言するDXに必要な要素

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



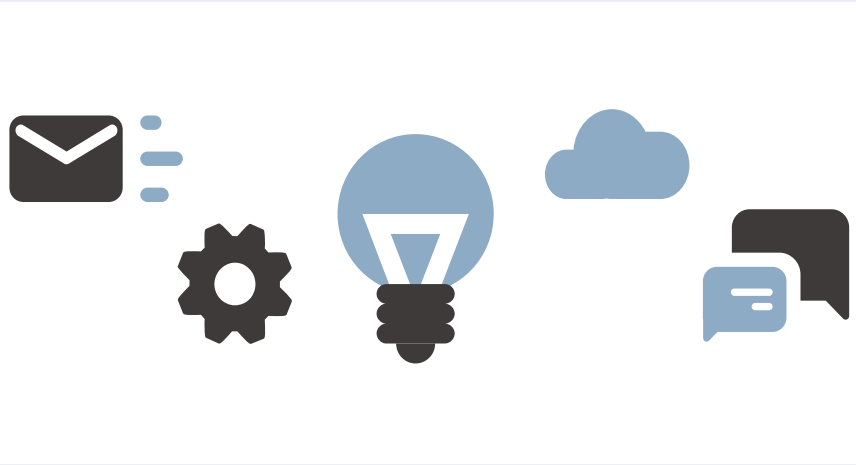
ビジネス上の
ニーズに合致する

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

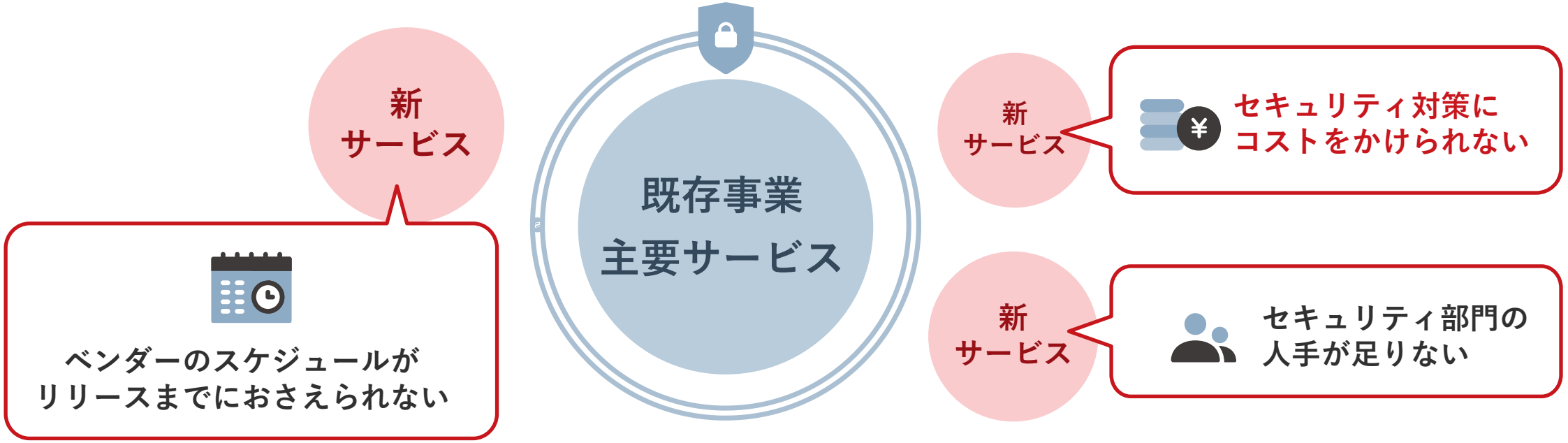
対応範囲は拡大

難易度は上昇

DXの進展に伴う「セキュリティ対策の悩み」

❶ 対応範囲は広がる一方、時間・予算・人材は足りない

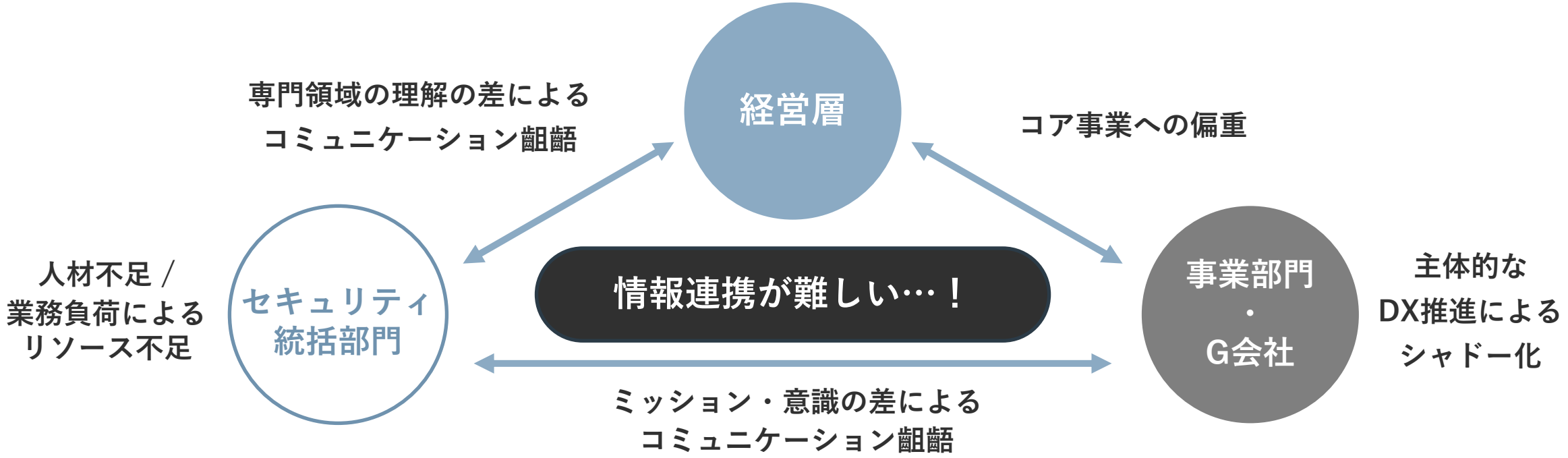
新しいデジタルサービスが次々と生みだされる一方で、事業立ち上げ段階から万全のリソースをかけてセキュリティ対策を行うことは困難であり、事業スピードとの両立が課題化しやすい。



DXの進展に伴う「セキュリティ対策の悩み」

❷ ステークホルダーが増え、連携が難しくなった

セキュリティガバナンス実現のため、部門や役割を超えたコミュニケーションが求められる。



セキュリティ対策の悩みを克服する「戦略的」思考とは

セキュリティ対策の「戦略的」思考

「戦略的な」セキュリティ対策とは・・・

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

濃 ⟷ 淡

戦略的な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

課題①

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

課題②

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・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

AIを活用した
脆弱性診断の自動化・内製化

脆弱性診断を自動化・内製化するときに考えること

「内製化できればいいんだけどな…」

？

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？

脆弱性診断を自動化・内製化するときに考えること

？

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？

＋

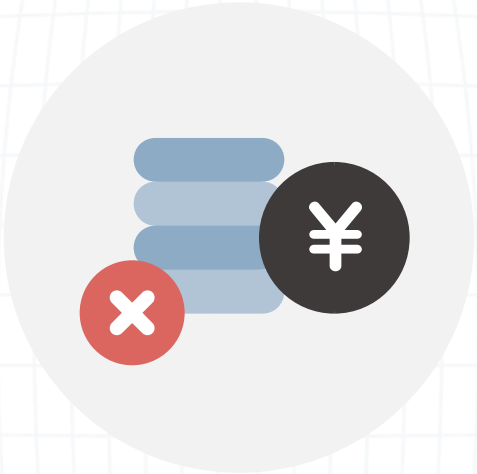
事業部門・開発部門に内製化の協力を得られるか？

実際に事業部門と向き合う中で直面する「壁」

課題 1

稼働を割きたくない

診断に時間を取られたくない
スケジュール調整したくない
なるべく対応したくない



課題 2

コストをかけたくない

計画にセキュリティコストを含めていない
診断環境を用意したくない

課題 3

セキュリティ意識が低い

診断とは何をするものなのかがわからない
セキュリティを意識しようと思っていない

脆弱性診断の自動化・内製化に必要な要素とは？

① 脆弱性診断のプロセスに
事業部門を巻き込む

② AIを活用した脆弱性診断
ツールの導入

脆弱性診断の自動化・内製化に必要な要素とは？

① 脆弱性診断のプロセスに事業部門を巻き込む

事業部門とセキュリティ部門で一緒に脆弱性診断を行うことのメリットを訴求

早期に脆弱性を発見することで
開発終盤での手戻りを最小化できる
（シフトレフト）

業務やサービス仕様に詳しいチームが
診断に参加することで
診断の精度・網羅性が上がりやすい

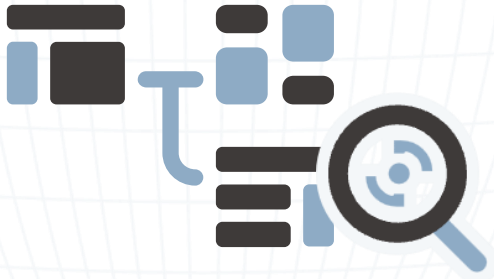
脆弱性診断の自動化・内製化に必要な要素とは？

② 脆弱性診断ツールの導入

事業部門を巻き込む前提で考えた場合、ツール選定に必要なポイントは…

1 誰でも使える操作性

2 利用範囲に制限がない



3 結果がわかりやすい

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。

脆弱性診断の内製化によって「戦略的」セキュリティ対策を実現する

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
300社以上

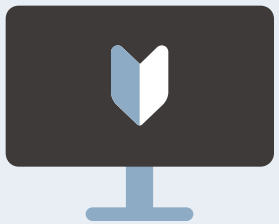
01
高精度なAI活用
巡回精度が高く
画面遷移図で見てわかりやすい

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

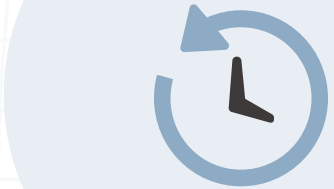
AeyeSecurityLab

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。



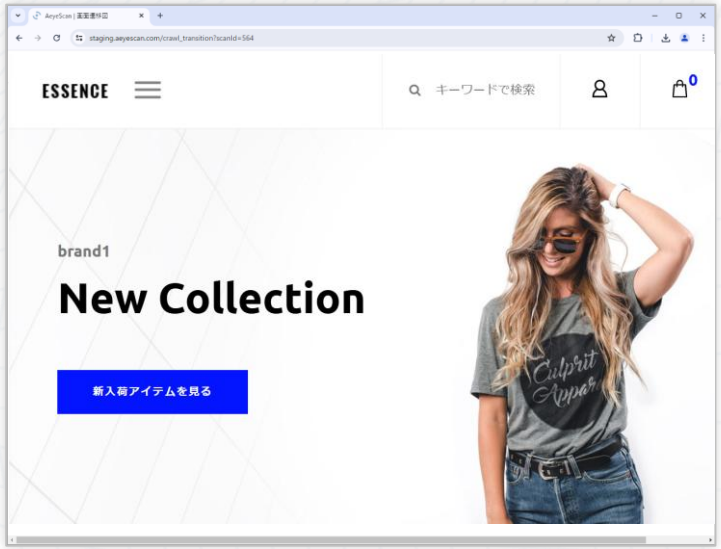
AIによる自動診断

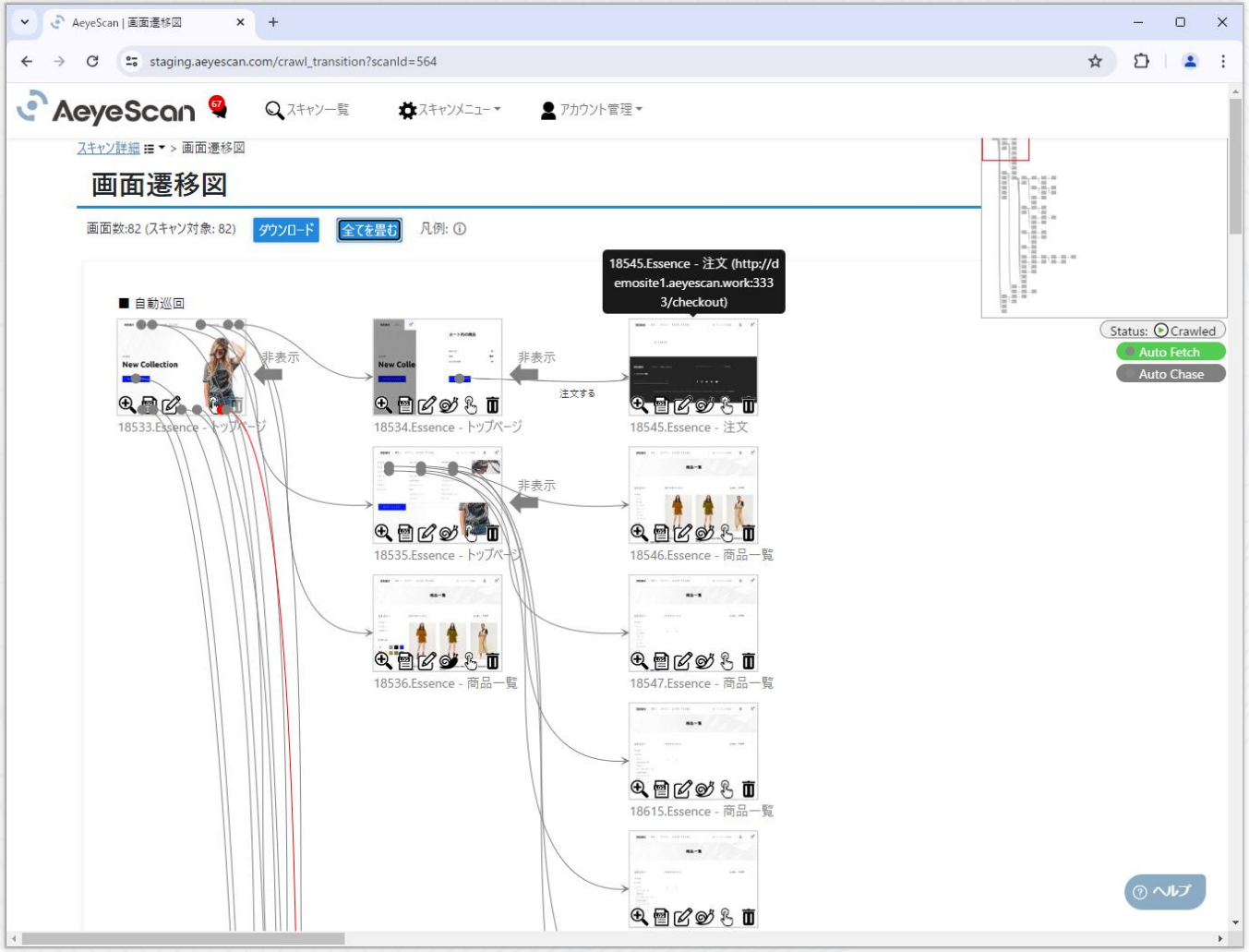
圧倒的な巡回精度で
24時間自動で診断。
画面遷移図で状況を可視化。

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

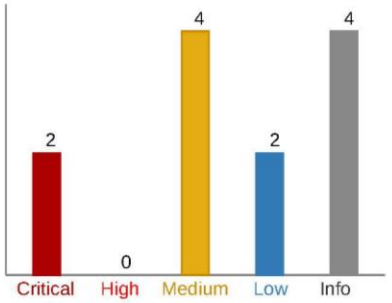




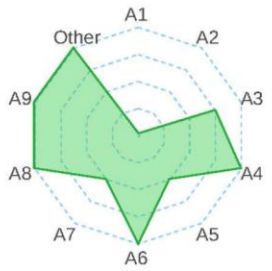
結果がわかりやすく、すぐさま修正作業に取り組めるレポート

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

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

AeyeSecurityLab

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!

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 三菱電機デジタルイノベーション株式会社 / YONA / リピスト / Yeti

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）会社名及びロゴは各社の商標または登録商標です

本日のまとめ

AIで実現する戦略的なセキュリティ対策

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。