＼ 膨大な脆弱性は賢く仕分ける！ ／

戦略的 トリアージ & ASM 実践

2025 11.6 (木)

LIVE リアルタイム配信
11:00-11:30

アーカイブ配信
11.13 (木) 8:00 - 11.14 (金) 22:00

AeyeSecurityLab

株式会社エーアイセキュリティラボ
執行役員
関根 鉄平 CISSP

膨大な 脆弱性 は 賢く仕分ける！

― 戦略的「トリアージ&ASM」実践 ―

はじめに

本日は本ウェビナーにご参加いただきありがとうございます

Q&A

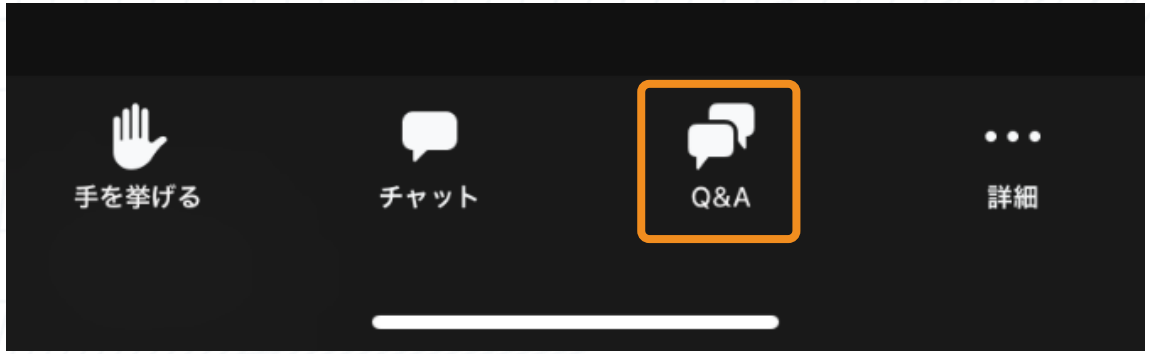
- ウェビナー中、お困り事がありましたらQ&Aにてご連絡ください。
- お客様のQ&A投稿、お名前、音声や画像が他の参加者様に届くことはございません。
- 質疑応答セッションは後に設けておりますが、ご質問はいつでもご投稿いただけます。

アンケート

- ウェビナー終了後、アンケート回答にご協力をお願いいたします。
- 本日の講演内容についてご質問のある方は、Zoom退出時に表示されるアンケート内にコメントをいただければ、後日回答させていただきます。

タイムテーブル

11:00	ご挨拶
11:05	本題
11:25	質疑応答
11:30	終了



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

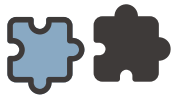
- 情報セキュリティ10大脅威 選考会メンバー
- OWASP/ISOGJ アジャイル開発におけるセキュリティ｜パターン・ランゲージ
- 『脆弱性トリアージガイドライン作成の手引き』共同執筆

いまや、脆弱性が「山積み」の時代

環境変化に伴い脆弱性が増加する一方、リソース不足で対応しきれなくなっている

攻撃対象の拡大

Webアプリケーション、API、
モバイル、クラウド…
診断対象の範囲が広がり
脆弱性が増加



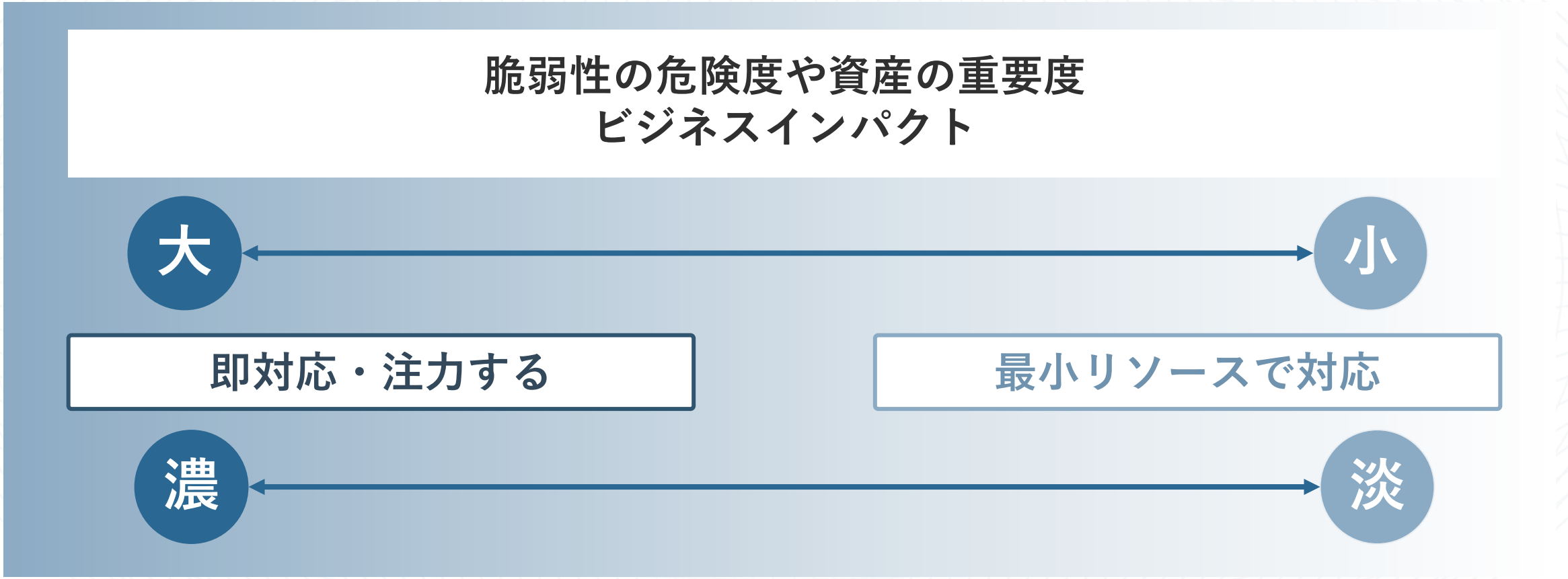
新しい技術の台頭

マイクロサービスや
SaaS連携など、
新しい開発スタイルが
生まれるごとに
新しいリスクも生まれる

既知の脆弱性の放置

修正リソース不足や
診断待ちにより、
既知の脆弱性が
解消されないまま
積み上がっている

濃淡をつけて対応しないと、捌き切ることができない



限られたリソースを最適配分するために「脆弱性トリアージ」が必要

脆弱性トリアージ体制はどのようにつくる？

脆弱性トリアージ体制をつくるには

脆弱性トリアージ体制の作成は、「脆弱性トリアージガイドライン作成の手引き」の「1章 トリアージガイドラインの作成 」を参考にして下さい。

「脆弱性の影響分析」、「リスク判定基準」、「対応の要否と期限を決める」といった
対応基本方針を策定することで、迅速に最低限のトリアージが可能な体制が構築できます。

1. 関係者の役割と責任を明確にする
2. トリアージガイドラインの適用範囲を決める
3. 脆弱性の影響範囲の調査
4. トリアージで決めるべきこと
5. 対応の要否と期限を決める
6. 脆弱性の管理方法

参考： 「脆弱性トリアージガイドライン作成の手引き 」 「1章 トリアージガイドラインの作成 」https://wg1.isog-j.org/TriageGuidelines/docs/chapter1/

トリアージで決めるべきこと　（1）対象資産の重要度の評価

まず重要度の評価基準の選定から始めましょう。以下は、評価分類の一例です。

資産の種類に基づく分類		影響度の規模(利用者の規模)に基づく分類		利用者層に基づく分類	
高	金融データ、顧客情報、特許性を有する製品や技術情報	高	利用者数1万人以上	高	官公庁利用者(政府調達等)
中	業務データ、従業員の勤怠情報	中	利用者数1000人以上	中	技術者、システム管理者、企業の担当者
低	ホームページ等で既に公開されている情報	低	利用者数1000人未満	低	一般の利用者(BtoCのサービス等)

参考：「脆弱性トリアージガイドライン作成の手引き」「1章 トリアージガイドラインの作成」https://wg1.isog-j.org/TriageGuidelines/docs/chapter1/

トリアージで決めるべきこと　（2）脆弱性の危険度の評価

次に脆弱性の危険度を確認し、対応の緊急性を評価する基準を設けます。

評価方針の設定

CVSS基本値や、脆弱性診断事業者が提供する危険度評価を参考に分類

CVSSでは「攻撃元区分」「攻撃条件の複雑さ」「攻撃前の認証要否」など、複数の要素を元に最終的な値が算出されますが、特に重視する項目があれば基準の一つとしてもOK

危険度評価の定義例（3段階の場合）	
高	CVSSが7.0 - 10.0
中	CVSSが4.0 - 6.9
低	CVSSが0.0 - 3.9

危険度評価の定義例（4段階の場合）
Critical
High
Medium
Low

※3段階の場合と同様、それぞれの段階で定義を記載

参考：「脆弱性トリアージガイドライン作成の手引き」「1章 トリアージガイドラインの作成」https://wg1.isog-j.org/TriageGuidelines/docs/chapter1/

対応の優先度の決め方

対象の重要度評価と脆弱性の危険度評価から、マトリックスを作成して対応の優先度を決めます。

CVSS				
	高	中 (30日以内)	高 (10日以内)	緊急 (5日以内)
	中	低 (90日以内)	中 (30日以内)	高 (10日以内)
	低	低 (90日以内)	低 (90日以内)	中 (30日以内)
		低	中	高
		資産重要度		

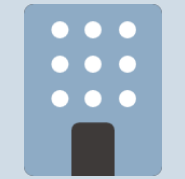
参考：「脆弱性トリアージガイドライン作成の手引き」「1章 トリアージガイドラインの作成」https://wg1.isog-j.org/TriageGuidelines/docs/chapter1/

ビジネスインパクトを考慮した結果優先度が下がった事例

トリアージ対象の脆弱性：CVE-2022-3080(CVSSスコアは7.5)

BIND 9と呼ばれるDNSサーバーの実装に発見された脆弱性。クライアントからフルサービスリゾルバとして動作するBIND 9のDNSサーバーに対し、細工された問い合わせを送信することにより、特定の条件下でサービス不能（DoS）にさせることができる。

トリアージを実施するA社の状況



A社

- 複数のブログやWebメディアを運営する企業
- ページ上に掲載される広告を主な収益源

2種類の用途でそれぞれ独立したDNSサーバーを運用

権威DNSサーバー
ブログやWebメディアのドメインの問い合わせに応答する

フルサービスリゾルバ
社内業務に利用するオフィス端末のインターネットアクセスに利用する。

参考：「脆弱性トリアージガイドライン作成の手引き 」「5章 事例」https://wg1.isog-j.org/TriageGuidelines/docs/chapter5/section2/

トリアージする脆弱性はどうやって見つける？

トリアージする脆弱性の発見は、まず「ASM」から始めるべき

DXの推進に伴い、未把握のWeb資産が増加している。
脆弱性対策の抜け漏れを防ぐためにも、ASM（Attack Surface Management）と
脆弱性診断は合わせて行うのが望ましい。

未把握のWeb資産の一例

事業部門がアジャイル開発で
構築・運用するWebサイト

PoCで作ってみた
SaaS/IaaS/PaaS上のアプリ

スクラップ＆ビルドの連続で
誰も管理できていないAPI

ASM・脆弱性診断・トリアージは内製でできる

外部委託する方法以外に、内製で行うこともできる。

Web資産の発見（ASM）	脆弱性診断	トリアージ
ASMツールを活用し未把握のWeb資産を発見する	脆弱性診断ツールを活用し脆弱性を発見する	「脆弱性トリアージガイドライン作成の手引き」を参照しながら行う

参考：「脆弱性トリアージガイドライン作成の手引き」 https://wg1.isog-j.org/TriageGuidelines/

内製する上での課題

ASM・脆弱性診断・トリアージを内製する上では、それぞれ以下のような課題がある。

Web資産の発見（ASM）	脆弱性診断	トリアージ
探索に必要な 手がかりがわからない	専門知識のないメンバーで 対応できない	リソース不足 人によって認識が異なる
誤検知の精査に 手間や時間がかかる	ツールを導入しても 使いこなせず工数がかかる	ビジネス上の優先度や 修正容易性を加味しづらい
発見経路や 検出理由まではわからない	診断の精度やカバー範囲など 品質に不安がある	CVSSだけでは 自社環境まで考慮できない

内製でのASM・脆弱性診断・トリアージの課題を解決するAeyeScan

AI・RPA活用により、脆弱性診断を自動化するクラウド型Webアプリケーション診断ツール

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

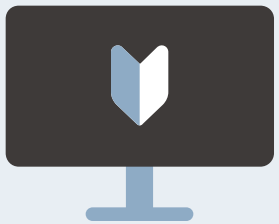
AeyeScanがサイトを自動巡回、診断すべき画面を抽出して画面遷移図を生成します！

Demonstration

デモ

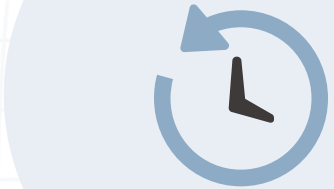
AeyeSecurityLab

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

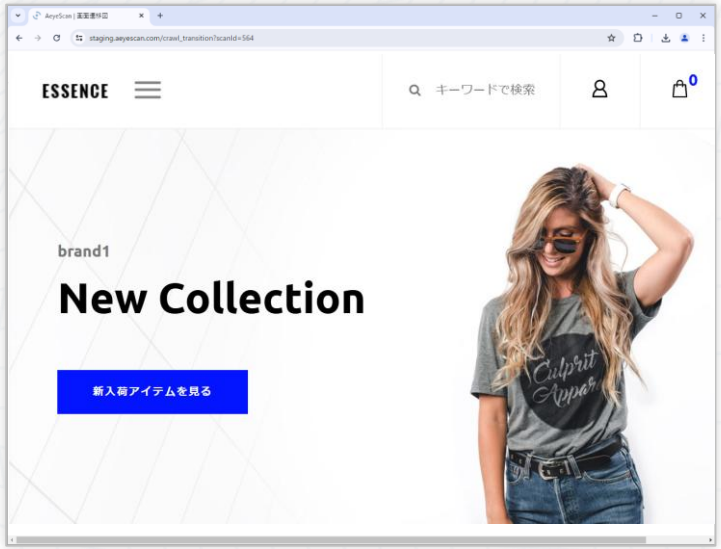
圧倒的な巡回精度で
24時間自動で診断。
画面遷移図で状況を可視化。

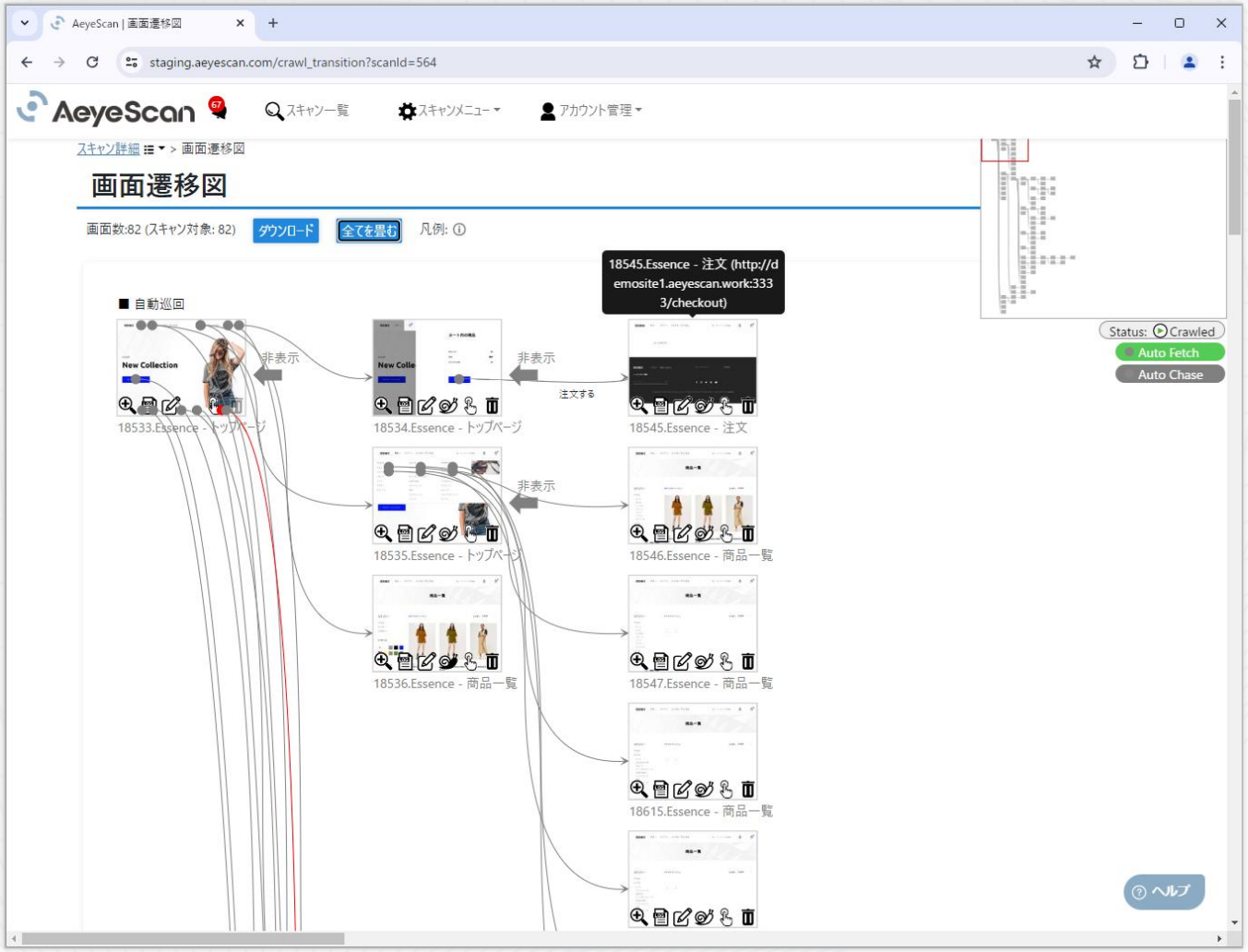
わかりやすいレポート

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。

AeyeSecurityLab

巡回時に、自動で画面遷移図を生成

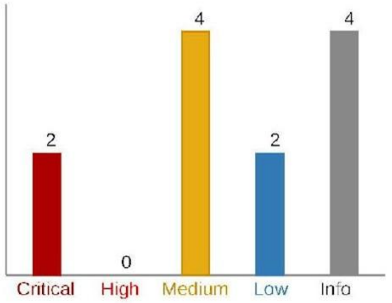




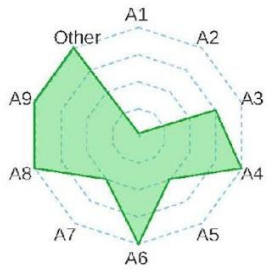
診断結果がわかりやすく、どう修正すべきかまでわかるレポート

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

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 / Denkei / Mizuno / ユーグレナ

インフラ

AIRE / HIS / odakyu / 近鉄情報システム株式会社 / SymEnergy / 水ing / Suzuyo / NANKAI / NTT東日本 / HITOWA GROUP / MEDIA / Looop / Loyalty Marketing, Inc.

金融

アイフル / 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 / Schoo / ZENKIGEN / Direct Sourcing / PERSOL / Leverages / workport

エンタメ

イープラス / CAPCOM / GungHo / とらラボ! / BookLive

SaaS

Advanced Media, Inc. / 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 / 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 / SUNDAY SYSTEMS / CEC / GA TECHNOLOGIES / tdi / Simplex Inc. / 777WORKS / SOFT CREATE / SOLTEC / 森平建交株式会社 / 電通総研 / TOPPAN / JOPS / JAST / NHC / 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

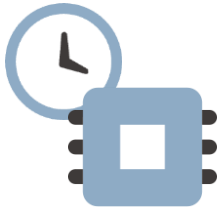
社名五十音順（導入いただいた企業様の一部です）会社名及びロゴは各社の商標または登録商標です

高度な生成AI活用により、効率的かつ信頼性の高い探索が可能

生成AIをASMに活用することで…！

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



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

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

重要度を自動でランク付け

Webサイトの属性を自動判定し
ビジネス上の重要度をもとにランク付け

脆弱性トリアージ体制の構築とともに
脆弱性診断の内製化・WebサイトのASMを

検討される方には、AeyeScan をご紹介させてください！

このあと表示されるアンケートで「デモを希望する」をご選択いただければ
お打合せを調整いたします。

ぜひ、デモで実際の機能をご覧ください。

AeyeSecurityLab

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

Q&A

お気軽にご質問ください

こちらから質問をお送りください

定期開催中！ AeyeScanがよく分かるデモ動画・セミナー

AeyeScanを検討してみたい方へ

AeyeScanがどんなものか知りたい方に、
デモを交えてわかりやすくご紹介。
まずは気軽に使い勝手をチェック！

デミセミナーの日程を確認

AeyeScanの操作を体験してみたい方へ

実際の操作を通して、一連の機能を体感。
導入前の不安や疑問をまるごと解消。
“わからないまま”をなくすセミナーです。

ハンスオンセミナーの日程を確認

セキュリティ対策にお悩みの方へ

最新の事例や対策ノウハウをテーマ別に紹介。
月替わりで学べる無料ウェビナーを開催中。
お気軽にご視聴いただけます！

ウェビナーの日程を確認

AeyeSecurityLab

期間限定アーカイブ配信

＼ 膨大な脆弱性は賢く仕分ける！ ／

戦略的 トリアージ & ASM 実践

2025 11.6

LIVE リアルタイム配信
木 11:00-11:30

アーカイブ配信 11.13 木 8:00 - 11.14 金 22:00

AeyeSecurityLab

株式会社エーアイセキュリティラボ
執行役員
関根 鉄平 CISSP

次回予告

サプライチェーンを揺るがす DX推進の死角

AI活用で実現する、抜け目ない脆弱性対策とは

2025
11.12

LIVE リアルタイム配信
水 16:00-16:30

アーカイブ配信
11.20 木 8:00
-11.21 金 22:00

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

AeyeSecurityLab

アンケート

ご回答いただいた皆さまへ

本ウェビナーのPDFデータと

をプレゼント

セキュリティに、確かな答えを。