脆弱性対策、どう回していますか？

OWASP Top10 × 実例で学ぶ

回る運用とAI活用

2026
6.30

LIVE リアルタイム配信
火 14:00-14:30

アーカイブ配信
7.9 木 8:00
-7.10 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

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　**関根 鉄平** CISSP

発売中

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、CSIRTや開発現場でのセキュリティ推進を経て、2020年6月より現職。
AeyeScanカスタマーサクセス責任者として診断の内製化を支援し、2026年度より開発責任者に就任。顧客の声を反映したプロダクトの進化を牽引している。
大規模イベント等の講演多数。『セキュリティエンジニアの知識地図』共著。

コミュニティ活動など

- 日本セキュリティオペレーション事業者協議会（ISOG-J）、OWASP Japan 共同ワーキンググループ
- 公益社団法人日本通信販売協会（JADMA）Web・セキュリティ専門部会
- 情報セキュリティ10大脅威 選考会メンバー

OWASPの2大フレームワークの役割

Pick UP

OWASP Top 10：何が問題か

セキュリティリスクの意識向上・啓蒙を目的としたリスト。発生しやすい脆弱性を通じて、「何が危険なのか」と基本的な対策を分かりやすく提示。

セキュリティ意識向上・教育や
リスクの把握に

OWASP ASVS：どう対策すべきか

アプリケーションセキュリティの具体的な要件・検証基準。設計・開発・テストの各段階で「どう作り、何を確認すべきか」をチェックリストとして定義。

開発・テスト・監査のための
具体的なチェックリスト・基準に

どちらもOWASPが提供するセキュリティ関連のフレームワークだが、
組み合わせて使うことが大切

AeyeSecurityLab

OWASP Top 10:2025（2026年1月上旬、正式版公開）

Webアプリの主要リスクをまとめた業界標準レポート「OWASP Top 10」が4年ぶりに改訂。

2021年		2025年	
1位	アクセス制御の不備	1位 →	アクセス制御の不備
2位	暗号化の失敗	2位 ↑	セキュリティの設定ミス
3位	インジェクション	3位 ↑	ソフトウェアサプライチェーンの失敗
4位	安全が確認されない不安な設計	4位 ↓	暗号化の失敗
5位	セキュリティの設定ミス	5位 ↓	インジェクション
6位	脆弱で古くなったコンポーネント	6位 ↓	安全が確認されない不安な設計
7位	識別と認証の失敗	7位 →	認証の失敗
8位	ソフトウェアとデータの整合性の不具合	8位 →	ソフトウェアまたはデータの整合性の不具合
9位	セキュリティログとモニタリングの失敗	9位 →	ロギングとアラートの失敗
10位	サーバーサイドリクエストフォージェリ（SSRF）	10位 NEW	例外的状況の不適切な処理

出典 https://owasp.org/Top10/

2025年版では、ランキングがどう変化した？

Point 1

アクセス制御の不備
（1位）

2021年10位のサーバーサイド
リクエストフォージェリが
集約された

Point 2

セキュリティの設定ミス
（2位）

テスト対象の100%の
アプリケーションに確認され
5位→2位へ**急上昇**

Point 3

ソフトウェア
サプライチェーンの失敗
（3位）

2021年6位の
脆弱で古くなったコンポーネント
から**スコープを拡大**

これを踏まえ、重要な脆弱性とその背景・事例について解説していきます

出典 https://owasp.org/Top10/

Point 1

1位：アクセス制御の不備

ユーザーの権限に応じた、機能やデータへのアクセス制御が不十分な状態のこと。攻撃者が本来許可されていない権限外の情報にアクセスし、改ざん、データの破壊、業務操作を実行するリスクがある。最も発生頻度が高く、システムのセキュリティの根幹に関わる脆弱性として、前回に引き続き1位を維持。

問題の具体例

- 一般ユーザーが管理者ページや管理機能にアクセスできてしまう
- 他人のプロフィールやデータを閲覧・編集できてしまう
- 権限昇格により、本来許可されていない操作（APIの更新・削除など）を実行できてしまう

必要な対策

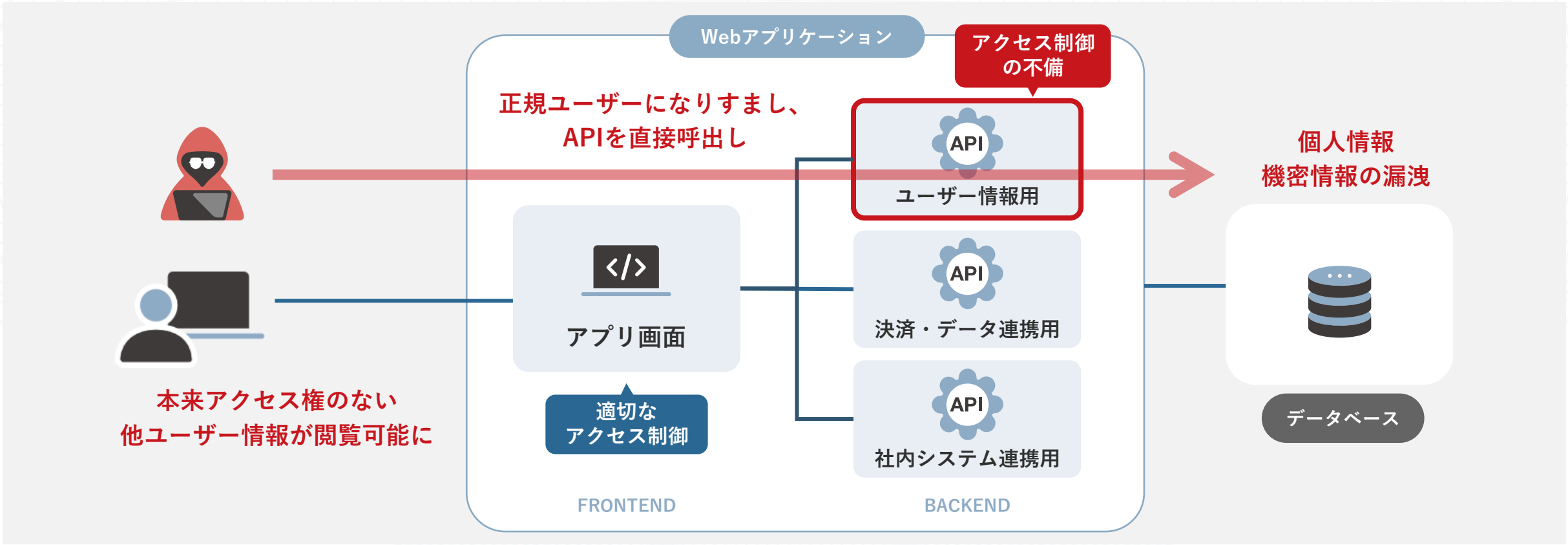
- 設定やコードでアクセス制御を一元管理し、最小権限の原則を適用する
- サーバーサイドでアクセス制御を実装し、クライアント側の制御を信頼しない
- 定期的にアクセス制御のチェックを行い、脆弱性を早期に発見する

出典 https://owasp.org/Top10/

Point 1

【背景】1位：アクセス制御の不備

GUI（画面）とAPIを分離する開発手法の普及により、アクセス制御の実装箇所が増加。GUI側で権限制御を行っていても、API側の認可チェック漏れによる脆弱性が発生しやすくなっている。



Point 2

2位：セキュリティの設定ミス

アプリケーションやクラウド環境において、権限や公開範囲、セキュリティ設定が不適切な状態で運用されている状態。コードに問題がなくても、設定の誤りやデフォルト設定のままの運用によって、重大なリスクが生じる。システムの複雑化と設定管理の重要性が高まったことで、5位から2位に急上昇。

問題の具体例

- デフォルトのアカウント・パスワードや不要なサービスが有効なまま運用されている
- エラーメッセージに機密情報や内部構造が含まれている
- クラウドストレージのアクセス権限が過剰、または暗号化が行われていない

必要な対策

- 適切な設定管理と、定期的なセキュリティチェックを実施する
- 開発・運用チーム全体で設定のセキュリティを意識する
- 自動化された設定管理やセキュリティチェックを導入する

出典 https://owasp.org/Top10/

Point 2

【背景】2位：セキュリティの設定ミス

クラウド・SaaS・コンテナの普及により、アプリケーションの挙動が「コード」ではなく「設定」に依存する割合が増加し続けている。設定項目の複雑化に伴い、設定ミスによるセキュリティ事故が日常的に発生。

必要な設定

- Webサーバー設定
- API設定
- クラウド設定
- 権限設定
- コンテナ設定
- CDN設定
- WAF設定
- ：

OWASPの最新調査において

テストされたアプリケーションの100%に検出

- ✓ 公開不要なクラウドストレージ
- ✓ デフォルト設定の放置
- ✓ 不要な管理画面の公開
- ✓ 過剰なアクセス権限付与

Point 3

3位：ソフトウェアサプライチェーンの失敗

※コミュニティ調査では1位にランクイン

開発から配布までの一連のプロセス（サプライチェーン）に存在する脆弱性やリスクのこと。

これまでは「脆弱で古くなったコンポーネント」に焦点を当てていたが、2025年版では、依存関係やビルド環境、配布インフラなど、より広い範囲のリスクを含んだうえで、6位から3位へ上昇。

問題の具体例

- 利用しているOSSや外部ライブラリ、依存関係を把握・管理できていない
- 脆弱性のあるライブラリを更新せず、古いバージョンを使い続けている
- 改ざんされたライブラリやビルド環境を経由して不正コードが混入する

必要な対策

- 依存関係を可視化・管理し、脆弱性情報を継続的に確認する — SBOM
- ライブラリやCI/CDなど開発基盤の信頼性・権限を適切に管理する — CI/CD セキュリティ
- 依存関係やビルド工程を含めた定期セキュリティチェックを行う — DAST

出典 https://owasp.org/Top10/

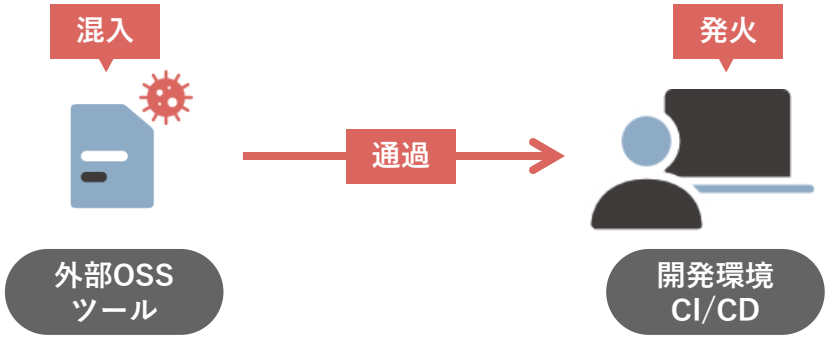
Point 3

【事例】3位：ソフトウェアサプライチェーンの失敗

2026年3月、Trivy、LiteLLM、Telnyx、axiosなど、開発者が日常利用する主要なOSS・ツールが相次いで侵害。
CI/CD等の配布経路に悪性コードが混入し、APIキー、SSH鍵、クラウド認証情報などが窃取対象となるリスクが顕在化。

被害の流れ

信頼済みツールから
攻撃が開発環境へ流れ込む



信頼済みツールが攻撃経路になる時代へ

1. **開発ツール・OSSパッケージが侵害**
   Trivy、LiteLLM、Telnyx、axiosなどに悪性コードが混入
2. **CI/CD・開発環境で実行**
   ビルド、インストール、importなど通常の処理で発火
3. **認証情報・設定情報を収集**
   APIキー、SSH鍵、クラウド認証情報などが標的に
4. **盗まれた権限で侵害が連鎖**
   リリース権限やパッケージ配布経路が悪用される
5. **利用企業側にも影響が波及**
   バックドア、C2通信、情報流出の確認が必要に

Point 3

【事例】3位：ソフトウェアサプライチェーンの失敗

2026年3月、Trivy、LiteLLM、Telnyx、axiosなど、開発者が日常利用する主要なOSS・ツールが相次いで侵害。
CI/CD等の配布経路に悪性コードが混入し、APIキー、SSH鍵、クラウド認証情報などが窃取対象となるリスクが顕在化。

例：axiosでは何が起きたか？

門番（メンテナ）を騙した

攻撃者は2週間かけて創業者になりすまし、
ソーシャルエンジニアリングで
axiosのメンテナを油断させ、
メンテナのアカウント奪取に成功

ソースコードは「正常」だった

ソースコード自体は改変せず、
設定ファイルに悪意ある依存関係を挿入。
インストール時に自動実行される
仕掛けを構築

動的なふるまいを乗っ取られた

実行時にバックドアが配置され
外部通信が発生。
痕跡は自動削除されるため、
静的ファイル確認では検知不可能

ここまでのまとめ

OWASP Top10上位リスクから見える脆弱性対策の方向性

資産・構成の可視化

ライブラリ・OSS、開発ツール
CI/CD、依存関係など

サプライチェーンリスクや
構成変化を把握

×

実環境での検証

Webアプリケーション
API、設定値など

実際の挙動を確認し、アクセス
制御不備や設定ミスを発見

変化し続けるシステムと攻撃に対応するため、継続的な実施が重要

増える管理×高頻度な診断要求――現場の限界

やるべきことの拡大

必要な取り組みの増加
Web資産の増加

診断の高頻度化

開発サイクル高速化
攻撃の加速化

継続的に回る運用に向け、AI活用で**診断を自動化**しませんか？

AeyeSecurityLab

診断の全工程を圧倒的に自動化する「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です。

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

AI活用で実現する、破綻しない「回る運用」とは

脆弱性診断のベストな頻度

1 Webサイト構築時

まず、Webサイトの設計・開発時に
可能な限り脆弱性を解消しておく。

2 Webサイト運用時

運用中に発生する問題に対応し、
Webサイトの安全性を維持する。

対応に濃淡をつけ、AIで自動化できる部分は徹底的に任せる

年に1回の
定期診断

＋

リリースや
機能改修時

プロによる手動診断
ペネトレーションテスト

AI活用による自動化で
開発プロセスへ組み込む

AeyeScanが選ばれている理由

OWASP Top10:2025にも即時に対応！

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

インフラ※

EPARK / AIRE / HIS / H2O RETAILING / NTT EAST / odakyu / 近鉄情報システム株式会社 / GEO / SymEnergy / 水ing Swing Corporation / Suzuyo / TOYOTA HOME / 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.

エンタメ

イープラス / CAPCOM / GungHo Online Entertainment, Inc. / とらラボ! TORANOANA LABORATORY / BookLive

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

金融

7&i / UPSIDER / 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

人材・教育

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

SaaS

Advanced Media, Inc. 株式会社アドバンスト・メディア / Lexica E-Retailing Platform / エフアンドエムネット株式会社 / M-aid / MTエムティーアイ / OZ INTERNATIONAL / giftee* / 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 株式会社パソフィックネット / 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

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

※公共および社会・生活基盤までを包含

社名五十音順（導入いただいた企業様の一部です）

AeyeScanを操作してみませんか？

詳細はこちらから

SEMINAR

「外注しているのに、なぜか忙しい」を解決する——

脆弱性診断の“周辺タスク”を削減！

診断の自動化体験セミナー

7月の日程

7/8 水

7/29 水

12:00～
オンライン

期間限定アーカイブ配信

詳細はこちらから

脆弱性対策、どう回していますか？

OWASP Top10 × 実例で学ぶ

回る運用とAI活用

2026
6.30

LIVE リアルタイム配信
火 14:00-14:30

アーカイブ配信
7.9 木 8:00
- 7.10 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

詳細はこちらから

デモ初公開

AeyeScan「Androidアプリ診断」徹底解説

Web、API、そしてモバイルの診断を1プラットフォームで

2026
7.7 (火)

LIVE リアルタイム配信
16:00-16:30

アーカイブ配信
7.16 (木) 8:00
-7.17 (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

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。