

脆弱性診断サービスのご案内

攻撃者より先に、自社システムの弱点を把握する。

OSSツール活用 × 金融グレードの実装経験で、コストと精度を両立した脆弱性診断をご提供します。

株式会社ASH（大阪市北区） | www.ash.osaka | 2026年6月

FOR EXECUTIVES — 経営者の皆様へ（このページだけで概要がわかります）

■ なぜ今、脆弱性診断か

数時間で標的に

Webサイトは公開直後から自動スキャンボットの標的になります。「うちは狙われない」は通用しません。

約190億ドル市場

セキュリティ&脆弱性管理のグローバル市場規模（2026年）。年6〜7%成長。対策は世界標準の経営課題です。

取引条件化が進行

親会社・取引先から「診断レポートの提出」を求められるケースが急増。商談・契約継続の前提になりつつあります。

■ 診断で得られる効果

① インシデントの未然防止

情報漏えい事故が起きてからの対応費用（調査・復旧・賠償・信頼回復）は、事前診断費用の数十倍規模になり得ます。「事後対応」より「事前診断」が圧倒的に安価です。

② 取引先・規制要請への対応力

診断レポートは取引先・監査・規制対応の客観的なエビデンスに。取引先チェックシートの回答支援（オプション）も提供します。

③ リスクの可視化と投資判断

「どこが、どれだけ危ないか」をリスクレベル付きで一覧化。限られたIT予算をどこに使うべきか、優先順位を持って判断できるようになります。

■ 費用・期間・成果物（概要）

費用

20万円～

規模・深度により変動（税別）

期間

2〜4週間

標準的なWebサイト診断の場合

成果物

日本語報告書

リスク評価＋具体的な対策案

業務影響

原則ゼロ

ステージング・低負荷時間帯で実施

■ ASHを選ぶ理由（採用判断のポイント）

金融グレードの診断実績

コーポレートサイトに加え、証券・デリバティブ系オンライン取引システムの診断実績。高可用性が要求される環境での無停止診断のノウハウがあります。

OSS活用による低コスト構造

OWASP ZAP・OpenVAS等のOSSツールを主軸とし、ライセンス費を抑制。費用の中心は専門エンジニアの工数のみ。大手の同等診断より割安です。

ホワイトボックス診断に対応

多くのベンダーが外部診断のみの中、ソースコードまで踏み込む内部診断に対応。受託開発で実装側を熟知しているからこそその確度の高い指摘が可能です。

「直し方」まで提案＋再診断1回込み

修正コード例を含む対策案まで提供。修正後の確認再診断（1回）を標準費用に含み、

「直った状態」までを成果物

とします。

▶ ご判断いただきたいこと：①診断の対象 ②深度 ③時期

まずは**無料のヒアリング（30分）**で対象を整理し、お見積りと**匿名化サンプルレポート**をご提示します。

※ 顧問契約（FDE）でご支援中の企業様は、**準備工数を圧縮した特別条件・短納期**で実施できます（詳細は8章）。

1. 診断の種類と対象レイヤー SERVICE LINEUP

システムは複数の層で構成され、層ごとに脆弱性の性質と診断手法が異なります。ASHは各層に最適なツールと手法を使い分けます。

Webアプリ層	自社開発のWebアプリ・フォーム・API 検出対象：SQLインジェクション、XSS、認証・セッション管理不備、アクセス制御不備、CSRF	OWASP ZAP (DAST/動的解析)
ソースコード層	プログラム内部の実装 検出対象：認可チェック漏れ、危険な関数利用、機密情報のハードコード、入力検証・エスケープ漏れ	Semgrep ほか (SAST+手動レビュー)
プラットフォーム層	OS・ミドルウェア・サーバ・ネットワーク機器 検出対象：既知の脆弱性 (CVE)、設定不備、不要ポート/サービス、パッチ未適用	OpenVAS / Nessus (認証スキャン対応)

診断メニュー	内容	こんな場合に
Webアプリケーション診断	OWASP ZAP による動的解析 (Active/Passive Scan、Ajax Spider)。フォーム入力・多段遷移・認証付き画面に対応し、OWASP Top 10 系の脆弱性を網羅的に検出。	公開サイト・Webサービスの定期点検、リリース前確認
プラットフォーム診断	OpenVAS / Nessus によるネットワーク・サーバ診断。CVEベースの既知脆弱性、設定不備、開放ポートを検出。認証スキャンによる深度のある診断も可能。	専用サーバ・オンプレ・VPC内リソースの棚卸し
ホワイトボックス診断	ソースコードを受領し内部から精査。SAST (Semgrep等) + 専門エンジニアの手動コードレビューで、外部から見えないサーバ側処理の欠陥を検出。	自社開発システムの根本確認、フォーム・決済処理の精査
ハイブリッド診断	ブラックボックス+ホワイトボックスを併用し、重複工程を圧縮しつつ外部・内部の両面から網羅評価。	金融系・個人情報を扱う重要システム

2. ブラックボックス vs ホワイトボックス METHODOLOGY

外部から攻撃者視点で検査する「ブラックボックス」と、ソースコードを直接読む「ホワイトボックス」。**見えるものが本質的に異なる**ため、対象の重要度に応じて使い分け・併用します。

ブラックボックス診断 (DAST)

外部から攻撃リクエストを送信 ▼

対象システム (中身は見えない)

公開URL・画面・APIエンドポイント

▲ 応答・挙動から脆弱性を判定

検出できるもの：実際に攻撃可能な脆弱性 (XSS・SQLi・認証不備等)、設定ミス、既知CVE。**攻撃者と同じ視点**で実害リスクを確認できる。

限界：サーバ内部の処理 (認可ロジック、DB操作、機密情報の扱い) は応答に現れない限り見えない。

ホワイトボックス診断 (SAST+レビュー)

ソースコード一式を受領 (NDA締結) ▼

コード内部を直接解析

サーバ側処理・設定ファイル・DBアクセス

▲ 自動SAST+手動レビューで精査

検出できるもの：認可チェック漏れ、入力検証・エスケープ漏れ、CSRF対策不備、機密情報のハードコード、危険な実装パターン。**該当コード行と修正例**まで特定。

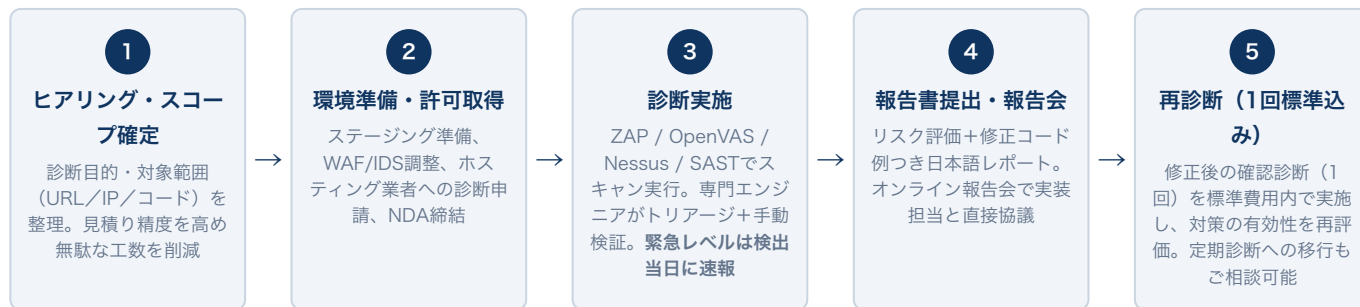
限界：運用環境の設定不備・ネットワーク経路の問題は対象外 (ブラックボックスで補完)。

▶ ASHの強み：ホワイトボックスまで一貫対応

国内の診断サービスの多くはブラックボックスのみの提供です。ASHは受託開発企業として実装側を熟知しているため、**コードに踏み込んだ確度の高い指摘と、修正例の提示**まで可能です。フォームや決済処理など「作り込んだ独自機能」の根本確認に最も効果を発揮します。

3. 診断の進め方（5ステップ） PROCESS

初回ヒアリングから報告書提出まで標準2～4週間。本番影響を避けるための事前調整は当社が伴走します。



4. 成果物：診断報告書 DELIVERABLES

「検出して終わり」ではなく、**経営報告に使えるサマリー**と**実装者がそのまま動ける対策案**の両方を1冊にまとめます。**匿名化したサンプルレポート**を商談時にご提供しますので、報告書の品質は発注前にご確認いただけます。

章構成	内容	主な読者
1. エグゼクティブサマリー	総合リスク評価、重大な検出事項、推奨対応の優先順位を1～2ページに凝縮	経営層・管理職
2. 診断概要	対象範囲、診断手法・使用ツール、実施期間、制約事項	管理職・担当者
3. 検出事項一覧	脆弱性ごとのリスクレベル（CVSS準拠）・影響・再現手順	担当者
4. 対策提案	脆弱性ごとの具体的な修正方法。ホワイトボックス診断では該当コード行と修正例を明記	開発者
5. 付録	スキャン生データ、参考情報（CVE/CWE等へのリンク）	開発者

検出事項のリスク評価基準（CVSS準拠）

レベル	定義	対応の目安
緊急	外部から容易に悪用可能で、情報漏えい・改ざん・システム停止に直結する	即時対応（暫定対処含む）
高	悪用には条件があるが、成立すれば重大な影響がある	1～2週間以内に修正
中	単体での実害は限定的だが、他の脆弱性と組み合わせて悪用され得る	次回リリースで修正
低	直接的な実害の可能性は低いが、堅牢化のため対応が望ましい	計画的に対応
情報	脆弱性ではないが、把握しておくべき構成情報・推奨設定	参考情報として活用

※ 緊急レベルの即日速報：診断期間中に「緊急」レベルの脆弱性を検出した場合は、報告書の完成を待たず**検出当日に速報**し、暫定対処をご案内します。

▶ オプション：取引先セキュリティチェックシートの回答支援

親会社・取引先・監査から求められるセキュリティチェックシート（質問票）への回答を、診断結果をもとに当社が作成支援します。「診断レポートの提出」だけでなく、**チェックシートに回答できる状態**までを伴走します。

5. 推奨する運用モデル OPERATION

単発で終わらず、「定期的なツール診断+要所での手動診断」の組み合わせが、コストと精度を両立する業界の王道です。

定期ツール診断（ベース）

四半期～月次でZAP / OpenVASによる自動スキャンを実施し、新たなCVE・設定変更によるリスクを継続監視。低コストで反復可能。

+

手動診断（要所）

大型リリース前・重要機能追加時・年1回の定期点検で、専門エンジニアによる手動診断・コードレビューを実施。ツールで出ないロジック欠陥を捕捉。

※ リリースサイクルへの組み込み（CI/CDでの自動スキャン連携=DevSecOps）のご相談も承ります。

6. 診断実績 TRACK RECORD

コーポレートサイトから、ミッションクリティカルな金融取引システムまで、複数の実環境で診断と対策提案を行ってきました。

コーポレートサイト診断

公開Webサイトに対するブラックボックス診断。フォーム・認証・共用ホスティング環境の制約を踏まえたスコープ設計と、検出後の対策提案までワンストップで対応。

OWASP ZAP

OpenVAS

オンライン取引システム診断

金融グレードのオンライン取引システム（証券・デリバティブ系）の脆弱性診断。高可用性・低レイテンシ要件下での無停止診断、ステージングでの網羅診断、リリース前最終チェックを実施。

OWASP ZAP

OpenVAS

Nessus

ホワイトボックス診断

カスタム開発のWebアプリ・APIについて、ソースコード受領のうえSASTと手動コードレビューを併用。フォームのサーバ側処理、認可制御、機密情報の取り扱いを内部から検証。

Semgrep

手動コードレビュー

使用する主なツール

ツール	区分	概要
OWASP ZAP	Webアプリ診断（DAST）	OWASP公式のWebアプリケーション診断ツール。Active/Passive Scan、Ajax Spiderに対応し、認証付き画面も含めた動的解析を実施。
OpenVAS / Greenbone	プラットフォーム診断	OSSの脆弱性スキャナ。CVEデータベースを基盤に、OS・ミドルウェアの既知脆弱性、設定不備、開放ポートを検出。
Nessus	プラットフォーム診断	商用スキャナのデファクトスタンダード。エンタープライズグレードの検出力で、認証スキャン、コンプライアンス監査（CIS等）にも対応。
Semgrep ほか SAST	ソースコード診断	静的解析ツール。PHP / TypeScript / Python等の主要言語のセキュリティルールを実行し、危険な実装パターンを検出。

7. 費用の目安 PRICING

対象規模・診断深度・レポート要件により変動します。下記は市場相場をベースとした概算（税別）で、正式見積りはヒアリング後にご提示します。

診断種別	費用目安（税別）	標準期間	備考
Webアプリ診断 （小規模）	20万～50万円	1～2週間	WordPress等、フォーム数が少ない構成
Webアプリ診断 （中規模）	40万～80万円	2～3週間	100画面前後、フォーム複数系統
プラットフォーム 診断	1IPあたり 5万～20万円	1～2週間	OpenVAS / Nessus。専用サーバ向き
ホワイトボックス 診断	50万～150万円	2～4週間	カスタムコード量に依存（SAST+手動）
ハイブリッド診断	80万～200万円	3～5週間	重要システム・金融系向け。重複工程を圧縮
再診断（修正後確認）	1回まで標準込み	3～5営業日	修正箇所に絞った確認診断。2回目以降は初回費用の20～30%
チェックシート回答支援	5万～15万円	3～5営業日	取引先・親会社のセキュリティ質問票への回答作成を支援（診断とセットでのご提供）

※ OSSツール（OWASP ZAP / OpenVAS / Semgrep）を主軸とするためライセンス費は実質ゼロ。費用の大部分は専門エンジニアの工数です。Nessus使用時はライセンス費を別途ご提示します。

※ 市場相場：Webアプリ手動診断 30万～150万円、ペネトレーションテスト 200万円～が一般的なレンジです（2026年6月時点の公開情報に基づく）。

▶ コストを抑える3つのポイント

- ・「**テンプレート重複の除外**」：ブログ等の量産ページは代表ページのみ診断し、全URL個別診断を回避（見積りが数倍変わることも）
- ・「**スコープの優先順位付け**」：個人情報・決済を扱う機能を深く、静的ページは浅く。全部を最高深度でやらない
- ・「**定期化による効率化**」：2回目以降は環境・設定を流用できるため、初回より2～3割低コストで実施可能

8. 顧問契約（FDE）企業様向け：FDEが診断を行うメリット FOR FDE CLIENTS

ASHと顧問契約を締結し、FDE（Forward Deployed Engineer）として開発・運用をご支援中の企業様は、**外部ベンダーに新規依頼する場合と比べて大幅に有利な条件**で脆弱性診断を実施できます。

① ヒアリング・環境調査が実質ゼロ

FDEはシステム構成・コード・運用を既に把握しています。外部診断で必須となるスコープ確定・環境調査の工数（1～2人日）がほぼ不要になり、**費用と納期を圧縮**できます。

② 検出 → 修正 → 再診断がワンループ

通常は「診断ベンダーの報告書 → 開発ベンダーへ修正依頼 → 再診断手配」と3者間の調整が必要ですが、FDEなら**検出した本人がそのまま修正し、即再診断**。対応完了までの期間が数分の一になります。

③ ビジネス文脈に基づく優先順位付け

どの機能が売上・個人情報・基幹業務に直結するかを理解しているため、機械的なCVSSスコアだけでなく、**貴社の実態に即したリスク評価と対応順**を提示できます。

④ 機密情報が外部に出ない

新たなNDA締結・ソースコードの社外提供が不要。既存の顧問契約の枠内で、システム内部情報・検出された脆弱性情報を**追加の開示先を増やさずに**扱えます。

項目	外部ベンダーに新規依頼	FDE（ASH顧問契約）が実施
事前ヒアリング・環境調査	1～2人日（別途費用）	ほぼ不要（システム既知）
契約・NDA	新規締結が必要	既存の顧問契約内で対応
検出後の修正	別途、開発ベンダーへ依頼・調整	FDEがそのまま修正（即着手）
再診断	別途見積り・日程調整	修正後即時に再スキャン
費用感	市場相場どおり（フル工数）	準備・調整工数の圧縮分、 相場より低コスト 。小規模なら顧問稼働内での実施もご相談可
継続診断	都度契約	リリースサイクルに組み込み、 DevSecOpsとして常時運用可

※ 取引先・監査から「第三者による独立した診断」を明示的に求められている場合は、自社開発部分について外部ベンダー診断の併用をご提案します（FDEが窓口・伴走することで、その場合も調整コストを圧縮できます）。

9. ご担当者様向け：事前準備チェックリスト PREPARATION

以下を事前にご準備いただくと、**見積り精度が上がり、診断がスムーズに進み、費用も抑えられます**。すべて揃っていないなくても構いません — 不明点はヒアリングで一緒に整理します。

A. 対象の棚卸し（見積り精度に直結）

☐ 診断対象のURL・ドメイン一覧

本番／ステージングの別、サブドメインも含めて。サイトマップがあれば共有ください

☐ 画面数・フォームの一覧

特に入力フォーム（問い合わせ・会員登録・決済等）は診断の重点対象。多段ステップの有無も

☐ サーバ・IPアドレスの一覧

プラットフォーム診断の対象。クラウド（AWS等）／専用サーバ／共用ホスティングの別も

☐ APIエンドポイントの一覧（ある場合）

REST/GraphQL等。API仕様書（OpenAPI等）があれば診断効率が大幅に向上します

B. 環境・権限の確認（診断の前提条件）

☐ ステージング環境の有無

本番影響を避けるため原則ステージングで診断。ない場合は低負荷時間帯での実施を調整します

☐ ホスティング事業者の診断ポリシー確認

共用ホスティングは事前申請が必須場合があります。無断スキャンは規約違反・遮断のリスク。申請は当社が支援します

☐ WAF / IDS / IPS の有無と管理者

診断時に一時調整（診断元IPの除外設定等）が必要になる場合があります

☐ テスト用アカウントの準備

認証付き画面の診断に必要。一般ユーザー＋管理者の2種類あると権限昇格の検査も可能

C. ホワイトボックス診断を行う場合

☐ ソースコード一式の提供準備

Gitリポジトリへの読み取りアクセス、またはアーカイブでの受け渡し。NDAは事前に締結します

☐ カスタム開発部分の特定

フレームワーク本体・市販プラグインは対象外とし、自社開発部分に集中することで費用を抑制できます

☐ 構成図・DBスキーマ・環境情報

システム構成図、使用ライブラリ一覧（package.json / composer.json等）があると解析が効率化します

D. 社内調整

☐ 診断窓口担当者の決定

技術的な質疑、緊急時連絡（重大な脆弱性発見時の即時報告）の窓口を1名決めてください

☐ 関係者への事前周知

診断中はアクセスログにスキャン痕跡が残ります。運用・監視チームへ実施期間を共有してください

☐ 直近バックアップの確認

診断による障害は原則発生しませんが、万一に備えてバックアップの取得状況をご確認ください

☐ 修正体制の確保（推奨）

報告書受領後に修正を行う開発リソースをあらかじめ想定しておく、対応がスムーズです。当社での修正支援も可能です

10. お問い合わせ CONTACT

社名	株式会社ASH
所在地	大阪市北区同心
Web	https://www.ash.osaka/security/ （本サービスの紹介ページ・問い合わせフォーム）
初回ヒアリング	無料（30分・オンライン）。対象システムの概要をお聞かせいただければ、概算見積りと推奨プランをご提示します。

本資料の市場データ・費用相場は2026年6月時点の公開情報に基づく目安です。正式な費用は対象の規模・複雑性を確認のうえ個別にお見積りします。

© 2026 ASH Inc. All rights reserved.