診断ツールだけで本当に安全？

ー専門家診断との使い分けを整理

株式会社神戸デジタル・ラボ

はじめに

近年のサイバー攻撃は高度化・多様化しており、企業のセキュリティ対策は経営課題として重要性を増しています。その対策として、以下のようなセキュリティチェック用のツールやサービス導入が進んでいます。

- 脆弱性診断ツール - システムやアプリケーションのセキュリティ上の弱点（脆弱性）を自動で探し出すツール
- 自動セキュリティスキャン - 定期的にシステムを自動でチェックし、セキュリティ上の問題がないか継続的に監視する仕組み

一方、多くの企業が以下のような疑問を抱いています。

- ツール導入だけで本当に安全なのか
- 専門家による診断は本当に必要なのか
- 自社でツールを運用すれば十分ではないのか

本資料では、これらの疑問に対して、実際の診断経験を踏まえた見解を紹介します。

本資料でわかること

本資料を読むことで、以下の4つのポイントが理解できます。

✓ 脆弱性診断ツールの仕組みと特徴

自動でセキュリティチェックを行うツールの基本的な動作原理や、得意な範囲、苦手な部分を解説します

✓ ツール診断のメリットと限界

低コストで高速な診断が可能である一方、誤検知や見落としが発生しやすいといったツールの長所と短所を理解できます

✓ ツールでは検出できない脆弱性の種類

ロジックの欠陥やビジネスプロセスに関わるような、専門家による手動診断でしか発見が難しい脆弱性の具体例を紹介します

✓ 最も効果的で安全な診断方法

ツール診断と専門家診断を組み合わせ、それぞれの強みを活かした、実践的かつ網羅的なセキュリティ診断のアプローチを提案します

実際の診断経験から、ツール診断と専門家診断の違いを具体的に解説します。

脆弱性診断ツールとは

脆弱性診断ツールとは、システムやWebアプリケーションに存在するセキュリティ上の弱点を自動で検出するソフトウェアです。
数百から数千の検査パターンを自動実行し、効率的に発見します。

主な特徴

数百～数千の検査を自動実行

手動では発見が難しい多様な脆弱性を効率的に洗い出します

AIやルールベースの診断エンジン

最新の脅威パターンや過去の脆弱性データベースに基づき、高度な分析を行います

自動巡回による継続的なスキャン

新機能追加やコード変更後も自動で再検査し、常に最新のセキュリティ状態を維持します

構造化されたレポート生成

検出された脆弱性の詳細、深刻度、修正方法などを明確に提示し、迅速な対応を支援します

これにより、手動では実施困難な大規模な検査を短時間で完了できます。

主な診断ツールの例

市場には多くの脆弱性診断ツールが存在します。対象システムの種類によって、適切なツールが異なります。

Webアプリケーション診断

Burp Suite

世界的に広く使われている多機能な統合型診断ツール

Vaddy

国内初のクラウド型Webアプリケーション脆弱性診断サービス

AeyeScan

AIによる自動巡回で高速かつ高精度な診断を実現

ZAP

OWASPが提供するオープンソースのWebアプリケーション脆弱性診断ツール

プラットフォーム診断

Nessus

サーバーやネットワーク機器の脆弱性を網羅的に検出するツール

InsightVM

リアルタイムで脆弱性を可視化し、リスクベースの優先順位付けを行うプラットフォーム

Vuls

Linux/FreeBSDなどのOSやミドルウェアの脆弱性を日本語で通知するオープンソースツール

これらのツールは、それぞれ異なる検査対象と検査方法を持っており、組織のニーズに応じて選択・組み合わせて使用されます。

診断ツールのメリット

脆弱性診断ツールには、以下の4つの大きなメリットにあります。

✓ 大量の検査パターンを実施可能

人手では多くの時間要する膨大な検査パターンで、システムを検査することができます。

✓ 短時間で広範囲を検査

人手に比べ、数時間で効率的に検査できます。

✓ 定期診断に適している

システムの更新や変更のタイミングで自動的に診断を実行し、継続的なセキュリティ監視を実現します。

✓ 最新の脅威情報の基づく検査パターン

専門的な知識がなくとも、最新の脅威情報に基づいた膨大な検査パターンで検索を実施することができます。

これらのメリットにより、ツール診断はセキュリティ対策として注目されています。

ツールで検出できる主な脆弱性

脆弱性診断ツールは、最新の脅威情報に基づく検査パターンに基づいて検査を実施します。以下は、ツールによってよく検出する代表的な脆弱性です。

代表的な検出項目

SQLインジェクション

悪意のあるSQLコマンドが実行され、データベースの内容が閲覧・改ざんされたり、システムが不正に操作されたりする攻撃です。

クロスサイトスクリプティング（XSS）

ユーザーが入力した内容を正しく処理せずにそのまま表示してしまうことで、悪意あるスクリプトが実行される脆弱性です。Cookie情報の盗み取りや不正な操作につながります。

OSコマンドインジェクション

システム内部でOSのコマンドを実行する処理に、外部から不正な命令を混ぜ込まれる脆弱性です。サーバ上のファイル操作や不正プログラムの実行が行われる危険があります。

ツールで検出できる主な脆弱性（続き）

その他の重要な脆弱性

CSRF（クロスサイトリクエストフォージェリ）

ログイン中のユーザーに、意図しないリクエストを送らせてしまう攻撃です。例えば、『ログイン中の銀行サイトで知らぬ間に送金される』といったケースがこれにあたります。

セキュリティヘッダ設定不備

Webサイトの通信を保護したり、不要な情報を外部に漏らさないようにするための設定が不十分なケースです。『クリックジャッキング防止』や『HTTPS通信の強制』などを行わないと、思わぬ攻撃リスクが残ってしまいます。

ディレクトリトラバーサル

URLやファイルパスの指定を悪用して、本来アクセスできないファイルを閲覧されてしまう脆弱性です。『../』といった記号を使い、サーバ内の重要情報（設定ファイルなど）を盗まれることがあります。

こツール診断で検出することは、セキュリティ対策の第一歩として重要です。

特に『インジェクション』は、診断ツールでも比較的高い精度で検出可能です。

よくある誤解

ツール診断の有効性が認識される一方で、その能力を過信する企業も少なくありません。

以下は、セキュリティ対策において陥りやすい誤解です。

誤解①：ツール診断だけで十分だと過信

ツール診断は脆弱性を効率的に検出できますが、ビジネスロジックの欠陥には対応できません。重要度の高いシステムでは、専門家による手動診断が不可欠です。

誤解②：AIが診断するから正確だと過信

ツールは、誤検知、過検知がつきものです。検知されたものをトリアージする必要があります。

誤解③：レポートが出るなら専門家はいらないと過信

検出結果の精査と正確な評価が必要です。診断ツールは機械的にパターンマッチングを行うため、実際には問題がない箇所を『脆弱性』と誤検知することがあります。

誤解④：安く済むならツールだけで良いと過信

見落とされる脆弱性が多く存在します。特に重要度の高いシステムでは、専門家による詳細な診断が不可欠です。

これらの誤解が、セキュリティ対策の不十分さにつながるケースが多く見られます。

診断ツールの死角

ツール診断には、見つけられない脆弱性が存在します。

これは、ツールが『人間の意図やシステムの利用文脈』を十分に理解できないからです。

主な理由

サイトの仕様を理解できない

ツールは定義されたルールのみで動作するため、ユーザー固有の複雑なサイト構造や、特定のデータを事前に登録しておく必要があるケースに対応できません。

ビジネスロジックを理解できない

業務フローの矛盾を検出できません。例えば、複雑な認証フローやカートに商品を入れてから購入画面に進むといった一連の操作を必要とする場合、自動化のシナリオを正しく組まないと診断が途中で止まってしまいます。

認証・権限の挙動を理解できない

複雑な権限制御の欠陥を見落とし、重要な部分の検査が抜け落ちることがあります。

ツールでは見つかりづらい脆弱性

専門家による手動診断では、ツールでは見つけづらい脆弱性を発見できます。以下は、その代表例です。

代表例

認証の不備

ログイン機構の設計上の欠陥。例えば、セッションの有効期限が設定されていない、パスワードリセット機能に脆弱性があるなど。

認可の不備

アクセス権限の不適切な設定。一般ユーザーが管理者機能にアクセスできるなど、権限制御の欠陥。

格納型XSS

データベースに保存された悪意あるコンテンツが、後で他のユーザーの画面で実行される脆弱性。

DOM型XSS

クライアント側のJavaScript処理の脆弱性。ユーザーの入力がDOM操作を通じて実行される。

機密情報漏えい

意図しない情報の露出。例えば、エラーメッセージに機密情報が含まれている、キャッシュに機密データが残っているなど。

これらの脆弱性は、システムの仕様やビジネスロジックを深く理解した専門家だからこそ発見できるものです。

ビジネスロジックの脆弱性

ビジネスロジックの脆弱性とは、システムの設計や業務フローの不備によって発生するセキュリティ問題です。

一般的な攻撃パターンとは異なり、システムの仕様や業務の流れを理解しないと発見が難しいという特徴があります。

実例：あるECサイトの診断で、次のような問題が見つかりました。

購入数量を「－1」にすると、購入金額が増えてしまう

本来、商品の数量は「1以上」である必要がありますが、システム側で入力値のチェックが不十分だったため、数量「－1」を入力金額計算が正しく処理されない結果として金額が増えてしまうという不具合が発生していました。

なぜツールでは見つからないのか？

このような問題は、次の理由からツールでは検出が難しい場合があります。

- ✓ 業務仕様を理解する必要がある
  （数量がマイナスになること自体が不正）
- ✓ 実際の操作手順を試す必要がある
  （商品選択 → カート → 数量変更）
- ✓ 複数画面の処理を確認する必要がある
  （入力 → 計算 → 決済処理）

ビジネスロジックの問題は自動スキャンでは見つからないケースが多く、専門家による手動診断で発見されることが多い脆弱性です。

診断ツールの正しい使い方

ツール診断は、適切に活用すれば非常に効果的です。以下は、ツール診断が最も効果を発揮するケースです。

ツールが向いているケース

定期診断

継続的な脆弱性チェックに最適。数カ月に一度の定期的な確認に適しており、システムの更新や変更のたびに自動的に診断を実行し、継続的なセキュリティ監視を実現します。

開発途中の検査

開発サイクルに組み込める。軽微な変更後の確認や早期のリスク発見に効果的です。

コーポレートサイト

静的ページの多いサイトなど、比較的重要度の低いシステムの健康診断的なチェック。

ツール診断は、短時間で自動的にスキャンできるため、『早期発見・早期対応』を目的とした日常的な運用に向いています。安価で気軽に診断を実施でき、24時間自動で診断を回すことも可能です。そのため、一度に大規模なサイトや多くの検査パターンを効率よくチェックすることができます。

専門家診断が必要なケース

以下のようなシステムでは、ツール診断だけでは不十分です。専門家による手動診断が必須となります。

ECサイト

金銭取引に関わるビジネスロジックの検証が必須です。複雑な決済フローや価格計算ロジックに潜む欠陥を検出するには、専門家の深い知見と手動検証が不可欠となります。

個人情報を扱うサイト

情報漏えいリスクが高く、高度な診断が必要です。初期リリース前には必ず実施することを強く推奨します。

金融システム

規制要件と高いセキュリティレベルが要求されます。複雑な認証フローや権限制御の検証が必須です。

業務システム

複雑なビジネスロジックと権限制御の検証が必要です。大幅な機能追加や設計変更があった場合、ツール診断では再現できない複雑な挙動を人の目で確認する必要があります。

これらのシステムでは、ビジネスロジックの脆弱性やアクセス制御の欠陥が、重大な被害につながる可能性があります。そのため、専門家による詳細な診断が不可欠です。専門家は診断ツールのスキャン結果をもとに『どの脆弱性が本当に危険なのか』『どう対策すべきか』といった判断やアドバイスも行います。

最も安全な診断方法

脆弱性診断として最も効果的で安全な方法は、**ツール診断**と**専門家診断**を組み合わせることです。

ツール診断の役割

- ✓ **よくある脆弱性の検出**：一般的なセキュリティ問題や過去に報告された弱点を効率的に見つけ出します。
- ✓ **基本的なセキュリティレベルの確認**：日常的にサイトの健康状態をチェックする役割を果たし、軽微な変更後の確認や早期のリスク発見に効果的です。
- ✓ **継続的な監視**：24時間自動で診断を回すことで、常に最新のセキュリティ状態を維持します。

専門家診断の役割

- ✓ **複雑な脆弱性の発見**：ビジネスロジックの欠陥やなどの脆弱性を発見し、より高度なセキュリティレベルを実現します。
- ✓ **深い掘り下げ**：システム全体を深く掘り下げ、表面化していない潜在的なリスクや設計上の問題まで洗い出します。
- ✓ **実践的なアドバイス**：発見した脆弱性に対して、実際にどのように対処すべきかまで踏み込んだアドバイスを得ることができます。

理想的なセキュリティ対策のサイクルは『ツール診断で定期的に確認し、重要なタイミングで専門家が深掘りする』というアプローチです。この2つをバランスよく使い分けることで、コストを抑えつつも堅牢なセキュリティ体制を維持することが可能です。

まとめ

本資料で述べた内容をまとめると、以下の3つのポイントが重要です。

診断ツールは有効

脆弱性（例：OSコマンドインジェクション、クロスサイトスクリプティングなど）を効率的に検出し、基本的なセキュリティレベルを確保するのに優れています。低コストで広範囲をカバーできます。

しかし死角がある

ビジネスロジックの不備などには対応不可です。ツール診断だけでは、重大なセキュリティリスクを見落とす可能性があります。

Webアプリ診断では手動診断が重要

特に重要度の高いシステムでは、専門家による詳細な診断が不可欠です。ツール診断と専門家診断を組み合わせることで、より強固なセキュリティ体制を構築できます。

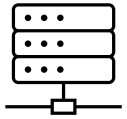
セキュリティ対策の成功は、ツールと専門家の両方を活用し、バランスの取れた診断戦略にあります。

Proactive Defense がご提供する脆弱性診断

Webアプリケーション脆弱性診断

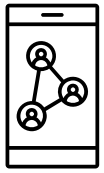
Webアプリケーションの脆弱性診断。発見した脆弱性の内容と脅威を報告し、対策方法をご提案。

プラットフォーム脆弱性診断



サーバ・プラットフォームの脆弱性診断。検出されたセキュリティ上の問題点と対策方法をご提案。

WebAPI脆弱性診断



Webアプリやスマートフォンアプリの通信先WebAPIに対する脆弱性診断。

クラウドセキュリティ設定診断

AWS 環境のセキュリティ設定に対する診断。 AWS Security Hub を用いて診断を実施。

脆弱性診断は対象によって診断の手法や内容が異なります。
Proactive Defense では**長年に渡る経験と最新の知見に基づき、診断対象に合わせた最適な診断をご提案**しております。

Proactive Defense の診断サービスを選ぶ理由

特長1. 精度の高いマニュアル診断

Proactive Defenseではプロの診断員が手動診断ツールを使い、診断箇所の特定・レスポンスの検証・証跡取りなど手動で行っています。

特長2. わかりやすいレポート&アフターフォローも充実

見つかった脆弱性についてはレベルわけしてご報告。問題点レベル、発生箇所、問題内容の詳細、リスク、対策方法など詳しくレポートします。また報告会も無料で開催しております。

特長3. 導入実績多数

業界最大手 総合アパレルファッション事業、業界最大手 製造業さまをはじめ、1000サイト以上の豊富な導入実績がございます。

脆弱性診断は Proactive Defense にお任せください。

Proactive Defense について

Proactive Defense

https://www.proactivedefense.jp/

Proactive Defenseは、脆弱性診断以外にもセキュリティ分野で幅広くサービスをご提供しています。

セキュリティコンサルティング

企業セキュリティの課題解決、そして意思決定。網羅性と深さのある知見で迅速にサポート

脆弱性診断（セキュリティ診断）

自社サイトの危険度を知る。それがセキュリティ対策、はじめの一歩

セキュリティトレーニング

一人ひとりのセキュリティ意識の底上げと、脆弱性診断の内製化をご支援

セキュリティプロダクト

セキュリティをもっと簡単に。様々なセキュリティ製品と導入支援をご提供

デジタルフォレンジック&インシデントレスポンス

起こってしまった事故の被害拡大を食い止め、事後対応をスピーディに図るために

会社紹介：会社概要

会社名	株式会社 神戸デジタル・ラボ
所在地	神戸市中央区京町72番 新クレセントビル
設立	1995年10月
資本金	5,000万円
売上高	19.5億円（2023年9月期）
従業員数	156名（2023年10月現在）

会社紹介：お取引先・パートナー

お取引先

- 株式会社 アイ・エム・ジェイ
- 株式会社 アシックス
- 株式会社 インターネットイニシアティブ
- オプテックス・エフエー 株式会社
- 川崎重工業株式会社
- 京都大学
- シーシーエス 株式会社
- 株式会社 ジェイ・エス・ビー
- 一般社団法人 JPCERTコーディネーションセンター
- 株式会社 じほう
- 株式会社 シュゼット・ホールディングス
- 国立研究開発法人 情報通信研究機構(NICT)
- 住友ゴム工業 株式会社
- ソフトバンク・テクノロジー 株式会社
- 中電不動産 株式会社
- 株式会社 デアゴスティーニ・ジャパン
- 東急リゾーツ&ステイ株式会社
- 日揮ホールディングス株式会社
- 日本マイクロソフト 株式会社
- 株式会社 ノーリツ
- 株式会社 ハースト婦人画報社
- 株式会社 バリュープランニング
- バンドー化学 株式会社
- 兵庫県立大学
- 株式会社 ファミリア
- フクダ電子 株式会社
- マガシーク株式会社
- 株式会社 ミツエーリンクス
- 株式会社 モリサワ
- 株式会社 山善
- 株式会社 ワールド

他

パートナー、提携

- アシアル　Monaca開発パートナー
- アステリア　ASTERIA Warpサブスクリプションパートナー
- ウイングアーク1st　WARPパートナー
- AWS セレクトティアサービスパートナー
- ELTRES IoTネットワークサービス パートナープログラム
- 京セラコミュニケーションシステム　Sigfoxパートナー
- クラスメソッド　SIパートナー
- サイボウズ　サイボウズシルバーパートナー
- ソニーネットワークコミュニケーションズ
- ソラコム　SPS 認定済インテグレーションパートナー
- Microsoft　Mixed Reality パートナープログラム
- LINE　Technology Partner/コミュニケーション
- 兵庫県警察（テクニカルサポーター）
- Cantho University Software Center （オフショア）
- 株式会社 リッケイ（オフショア）
- 株式会社 Omi Medical （オフショア）　他

Kobe Digital Labo

Proactive Defense 専用サイト
https://www.proactivedefense.jp/

〒650-0034　神戸市中央区京町72番 新クレセントビル
https://www.kdl.co.jp / 078-327-2280

CONFIDENTIAL