NET ASSIST
24/7 Guardian Deity

2024.11 #42

# NEWS LETTER

TOPICS



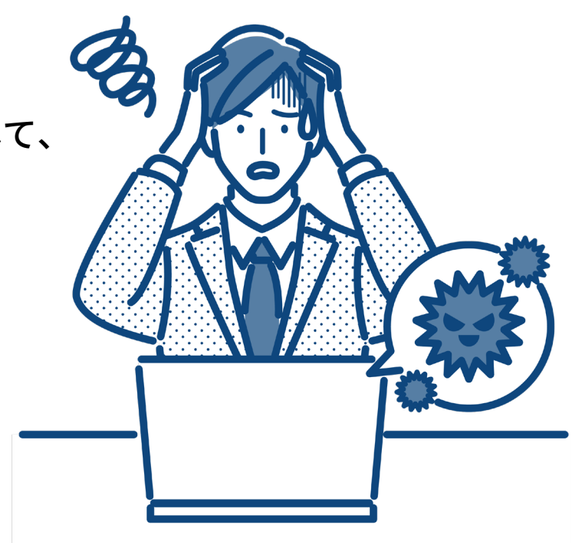
＊ TOPICSの各タイトルをクリックすると該当の記事へ飛びます

## #1 セキュリティ診断の種類と診断の選定基準

世界的なコロナウィルスの流行が始まった2020年を節目に、不正アクセス等のサイバー攻撃は年々増加の一途を辿っており、その技術や手法はますます多様化・巧妙化している状況です。
それに伴い、セキュリティサービスのお問合せが占める割合も年々増えてきました。特に、ここ数年は「脆弱性診断サービス」の需要が伸びています。
こちらのニュースレターでも「脆弱性診断についてのおはなし」として計2回、脆弱性診断の必要性をお伝えいたしました。
今回は、脆弱性診断と混同されやすいペネトレーションテストなどの、セキュリティ診断の種類とその比較、また脆弱性診断の手法や選定基準についてご案内いたします。

### そもそも脆弱性とは

「脆弱性」とは、WebアプリケーションやOS／ミドルウェア、ネットワーク等のシステムプラットフォームに潜在する**セキュリティ上の弱点や欠陥のことです。**
これらの脆弱性を悪用すると、外部の第三者がシステムに侵入できたり、本来は閲覧できないはずの重要な情報を見る事ができてしまいます。
実際に被害が報告されているサイバー攻撃は、これら脆弱性を悪用したものが殆どであり、**良く知られている既知の脆弱性に対する対策が不充分だった為**に引き起こされています。
しっかりとした対策が出来ていれば、それら事故の85%は未然に防げたとの調査結果（※）も出ています。
IPA（独立行政法人情報処理推進機構）によって毎年公開されるセキュリティ10大脅威などの情報も参考として、定期的な確認を意識しましょう。
※出展：ベライゾンジャパン　2016年度データ漏洩／侵害調査報告書（DBIR）より



### セキュリティ診断の種類と違い

WEBアプリケーションやシステムプラットフォームに関するセキュリティ診断は、大別して３種類に分類できます。

#### ①システムに潜在するリスクを可視化する「脆弱性診断」

WEBアプリケーションのソースコードや、システムプラットフォームに使われているOS／ミドルウェア、ネットワークに潜在する「脆弱性を可視化」するものです。
可視化された脆弱性は適切な対策を施す事により、セキュリティインシデントのリスクを大幅に減らす事が可能です。

#### ②セキュリティ対策の有効性を検証する「ペネトレーションテスト（侵入テスト）」

脆弱性診断があくまでもリスクの可視化であるのに対し、ペネトレーションテストは、専門のエンジニアが実際の攻撃に用いられる手法を使い、対象システムへの侵入を試みる疑似攻撃を実施します。
現時点でのセキュリティ対策の有効性や、脆弱性診断で可視化されたリスクへの対処状況などを把握する事が可能となり、システムの堅牢性が明確になります。

次ページへ

前ページより

## ③クラウドサービス利用等における「コンプライアンス診断」

クラウドサービスの急速な普及に伴い、設定ミスによるセキュリティインシデントの発生も増加の一途を辿っています。
ID／PWの設定不備や、クラウドストレージの閲覧権限設定不備等に起因する重要情報の漏洩等が代表的な被害です。このような事故を未然に防ぐ為に、各クラウドサービスにはそれぞれベストプラクティスとされているガイドラインが存在します。コンプライアンス診断は、それらの著名なガイドラインとの照合を実施し、その適合状況を可視化するものです。

| | 脆弱性診断 | ペネトレーションテスト | クラウドセキュリティ設定診断 |
|---|---|---|---|
| 目的 | 潜在する脆弱性やリスクの可視化 | システムへの侵入可否の確認 | クラウド利用時のセキュリティ設定状況の可視化 |
| 診断方法 | ツール診断と手動診断の組み合わせが主流 | 主にエンジニアによる手動診断が主流 | 主にツール診断が主流 |
| 効果 | 診断結果に基づいた適切な対処が可能 | セキュリティ対策の有効性確認、明確化 | クラウド利用におけるガイドラインとの適合状況把握 |

高いセキュリティレベルを保ったシステム運用を実現するためには、これら3種類の診断を組み合わせて適切な診断を定期的に実施することが重要です。

# 適切な診断手法とは

診断サービスを検討する際は、守るべき情報資産や企業価値などを考慮し、万が一セキュリティ事故が発生した際の損害等を見据えた内容で実施する事が推奨されます。
現状のアセスメントをしっかりと実施し、想定される被害や想定損害額などを把握し、それらを未然に防ぐために必要な診断を、適正な費用で実施する事が重要です。

## ①エンジニアによる手動診断、ペネトレーションテスト

高度な専門性を持ったエンジニアが、対象システムの診断を手動で実施し、実際の脆弱性を悪用した攻撃が可能かどうか確認します。
対象システムの規模にもよりますが、熟練のエンジニアが担当する為、費用も高額になる事が多いですが、ECサイトのようなクレジットカード情報を扱うシステムや、大量の個人情報を保有しているようなシステムの場合は、必ず実施する事が推奨されます。新規に開発したシステム等に関しても、初回公開前には手動での診断を実施する事が望ましいと考えます。

## ②ツールによる自動診断

対象システムによって向き不向きはありますが、安価に費用対効果の高い診断を実施したいような際はツールによる自動診断もおすすめです。
システムの規模やサイトの画面数等に依存せず、定額での診断が可能です。且つ、手動診断と比較すると短納期で診断結果を得る事が出来ます。
急に診断が必要になった際にまずは実施してみるという場面や、過去に手動診断を実施したシステムへの定期診断等でのご利用にも最適です。
ただし、手動診断と比較した場合、ツールではカバーしきれない項目もあり、複雑な構成のシステム等においては、細部までの診断が出来ない事もあります。

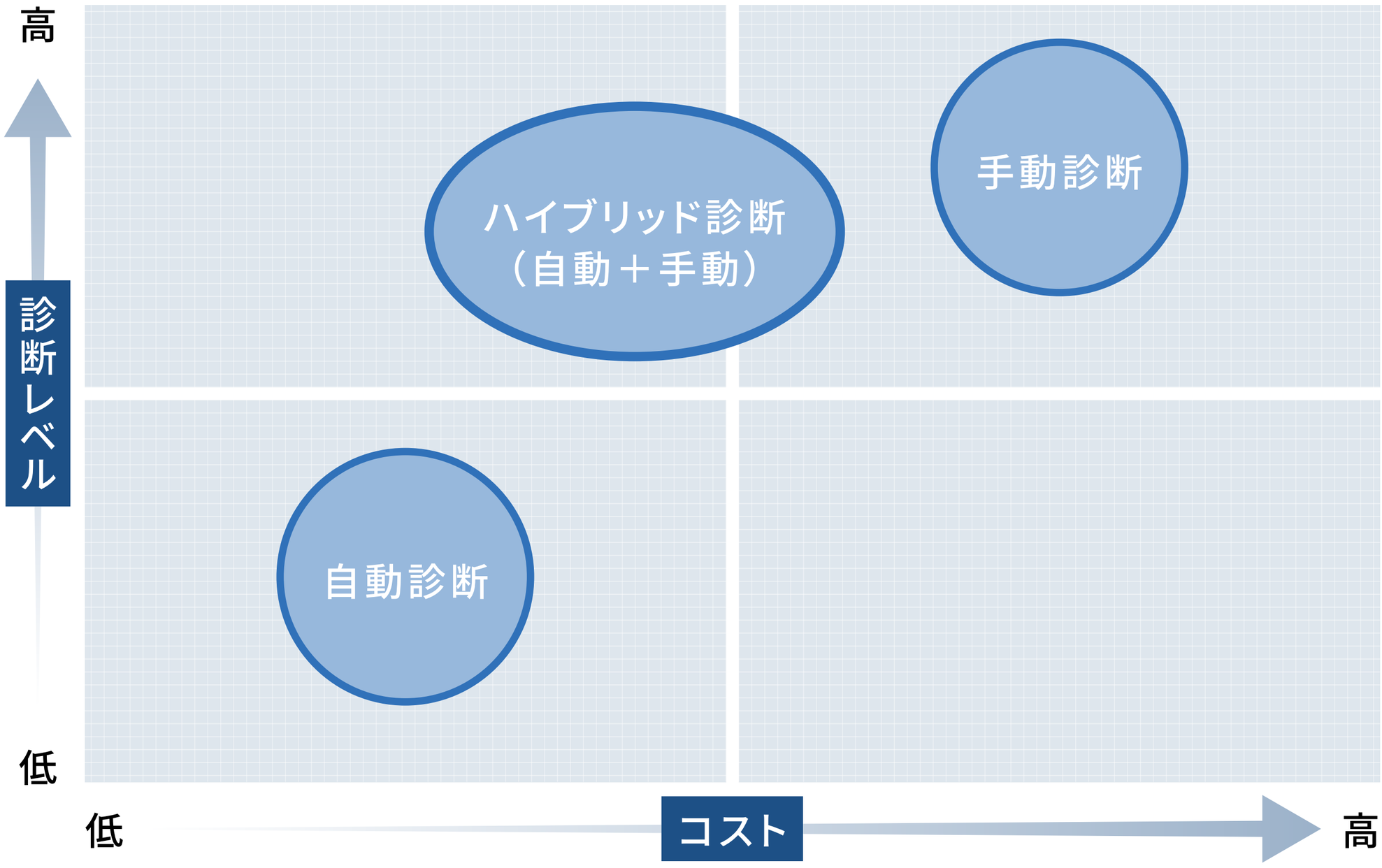
◎各手法のメリットデメリット

| | エンジニア手動診断 | ツール自動診断 |
|---|---|---|
| 推奨される診断対象 | ・ECサイト<br>・大量の個人情報を扱うシステム<br>・医療/金融関連システム<br>・新規公開前のシステム<br>・ログイン機能の有効性確認<br>・セッション管理機能の有効性確認 | ・企業のコーポレートサイトなど、攻撃による影響が小規模と想定されるサイト<br>・静的なコンテンツのみのサイト<br>・定期的な継続診断利用 |
| メリット | ・細部まで精度の高い診断が可能<br>・実施の攻撃手法に沿った診断により、セキュリティ対策の有効性が確認可能 | ・安価で網羅的な診断が可能<br>・オンデマンドでいつでも実施可能<br>・診断期間が短い（数時間から1日程度）<br>・診断結果が即時出力可能 |
| デメリット | ・エンジニアが稼働する為、費用が高額になるケースが多い<br>・診断期間が長い（数日から数週間） | ・診断項目に制限があり、細部まで診断できない事がある |

次ページへ

前ページより

◎診断レベルとコストによる最適な診断の選び方




## ネットアシストの脆弱性診断サービス

弊社では総合セキュリティ事業者である株式会社M&K社と提携し、SecurityBlanketという脆弱性診断サービスをご提供しております。
診断対象はWebアプリケーション、ネットワーク（OS/ミドルウェア）ともに可能であり、診断手法も手動・自動・ハイブリッドの3つから、ご予算や診断対象によってご選択頂けます。また、ペネトレーションテストの実施も可能です。

◎診断プラン料金

| 診断対象 | 手法 | 回数 | 料金 |
|---|---|---|---|
| ネットワーク | 自動 | 1回 | 70,000円/1IP |
| | 自動 | 無制限（1年間） | 210,000円/1IP |
| | 手動 | 2回（2回目は再診断） | 660,000円/3IPまで |
| WEB アプリケーション | 自動 | 1回 | 100,000円/1FQDN |
| | 自動 | 無制限（1年間） | 300,000円/1FQDN |
| | 手動 | 2回（2回目は再診断） | 980,000円～/1FQDN<br>※11URL以上は追加費用 |
| | ハイブリッド | 2回（2回目は再診断） | 660,000円～/1FQDN<br>※手動診断ページ分追加費用 |
| ペネトレーション テスト | 手動 | 1回 | 1,450,000円～/1IP<br>※2IP以上は追加費用 |
| コンプライアンス 診断 | 自動 | 1回 | 240,000円 |

※脆弱性診断の費用は、来年以降価格改定を予定しております。何卒ご了承ください

# #2 【12月11日（水）】セキュリティセミナーを開催いたします！

この度、Webサイト制作会社様や自社サイトの管理や運営をされている企業のご担当者様を対象に、セキュリティのスペシャリストであるサイバーセキュリティクラウド社と合同でセミナーを開催いたします。ご参加お待ちしております！


リスクと手間を最小限に！

## 脆弱性対策の効率化とサーバーセキュリティの強化

### セミナー概要

インターネット上の攻撃でまず狙われるのは、Webサイトやサーバーの安全上の弱点や情報セキュリティ上の欠陥と言われる『脆弱性』です。
脆弱性は1日に平均約50件も報告されており、Webサイトを安全に運用するためには脆弱性が潜んでいないかを定期的に確認することが重要です。
今回のセミナーでは、セキュリティのスペシャリストであるサイバーセキュリティクラウド社とサーバーインフラ企業ネットアシストが共催して、効率的な脆弱性管理の方法について解説いたします。

**日　程** 2024年12月11日（水）
15:00~16:00

**費　用** 無料（事前登録制）

**開催場所** オンライン開催
（GoogleMeet）

詳細の確認・お申込みは下記URLからお願いいたします。

https://www.netassist.ne.jp/1211_sidfmvm_webinar/

NET ASSIST 24/7 Guardian Deity
株式会社 ネットアシスト

TEL 03-3985-6780
mail sales@netassist.ne.jp
web https://www.netassist.ne.jp