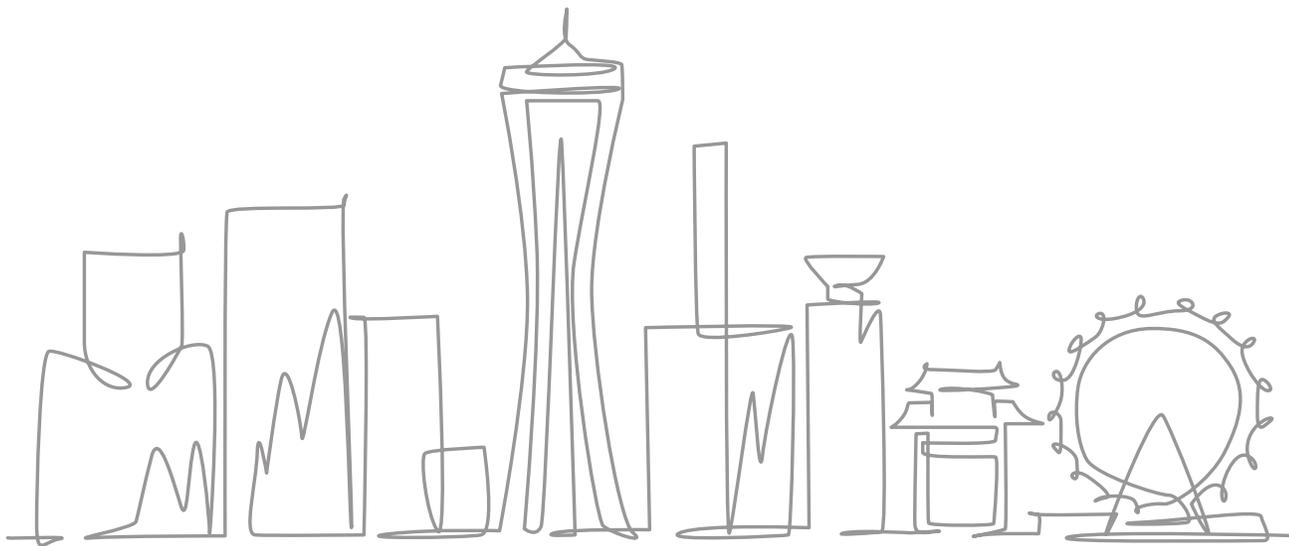


定期診断のご提案



株式会社神戸デジタル・ラボ



目次

1. 定期診断は必要なのでしょうか
 - 1-1 定期診断が必要な理由①
 - 1-2 定期診断が必要な理由②
 - 1-3 定期診断が必要な理由③
2. 企業にとって定期診断が必要な理由
3. 特に診断が必要なタイミング
4. 会社紹介

定期診断は必要なのでしょうか

お客様の声

脆弱性診断は一度実施すればよいものではないことはなんとなく知っているけれど、
実際予算やスケジュールの兼ね合いもあり難しい場合もある。
定期診断は本当に必要？おすすめの頻度や実施すべきタイミングはある？



理由① 新たな脆弱性



新たな脆弱性が日々
発見されています

理由② 攻撃手法の進化



攻撃手法が日々
進化しています

理由③ ガイドラインの推奨



ガイドラインでも定期診
断が推奨されています



上記のような理由から**年に1回程度の定期診断を推奨**します。
次ページ以降で詳しく解説します。

定期診断が必要な理由①：新たな脆弱性

脆弱性とは

コンピュータやネットワークなどの情報システムにおいて、第三者が悪意のある攻撃に利用できる可能性のある、Webサイト上の欠陥や問題点の事です。脆弱性はセキュリティホールとも呼ばれ、放置すると脆弱性を狙ったサイバー攻撃による不正侵入などを招き、重大な被害を受ける恐れがあります。

日々発見される新たな脆弱性

脆弱性を発見して対策を取ったとしても、毎日のように世界中で新たな脆弱性が発見されています。そこで、定期的に診断を受け、脆弱性を確認し、対策を取り続けることが必要です。

定期診断が必要な理由②：攻撃手法の進化

日々進化するサイバー攻撃

サイバー攻撃は日々進化しています。そのためセキュリティ対策ツールなどの利用によりサイバー攻撃から防御できていた社内システムや社内ネットワークが、攻撃手法の進化により防御できなくなるようなケースがあります。

AI時代とともにさらに高度化する恐れも

生成AIの悪用により、なりすまし等が容易になりサイバー攻撃がしやすくなる可能性があります。これによりサイバー攻撃はさらに高度化・多発化する可能性が危惧されます。デジタル化が進む現代世界において、サイバーセキュリティは企業や組織にとって重要な課題であり、リスクヘッジとしての定期診断の必要性が高まっています。



脆弱性診断は実施時点での状態を確認する**健康診断**のようなもの。
新たな脆弱性や攻撃手法の進化に対応する為、
定期的に診断を行い対策を取る必要があります。

定期診断が必要な理由③：ガイドラインの推奨（JPCERT/CC）

ガイドラインの例：

JPCERT/CC 注意喚起「サイバー攻撃に備えてWebサイトの定期的な点検を」

<https://www.jpccert.or.jp/pr/2016/pr160004.html>

Webアプリケーションのセキュリティ診断

- ◆ 目的：自社のWebアプリケーションに脆弱性や設定の不備が存在しないか確認するため
- ◆ 対象：Webアプリケーション
- ◆ 頻度：1年に1回程度、および機能追加などの変更が行われた時

またWebサーバ上のファイルの確認については週に1回程度、ログインIDとパスワードの確認については年に1回程度との記載があります。



Webアプリケーションの脆弱性診断については、
年に1回程度の定期診断が推奨されています。

定期診断が必要な理由③：ガイドラインの推奨（IPA）

ガイドラインの例：

IPA 「ECサイト構築・運用セキュリティガイドライン」

<https://www.ipa.go.jp/security/guide/vuln/ps6vr7000000acvt-att/000109337.pdf>

ECサイトを構築後、新たな脆弱性が発見される・新たな脆弱性を作り込む可能性があるため、定期的及びカスタマイズを行った際に脆弱性診断を実施することが重要です。

- ◆ 新機能の開発・追加やシステム改修等のカスタマイズを行ったときには、その都度Webアプリケーション診断を実施することが重要です。
- ◆ 上記のような新機能の開発・追加やシステム改修等のカスタマイズ等を行っていない場合でも、OSやミドルウェア等の脆弱性は継続的に発見されているため、四半期に1回の頻度でプラットフォーム診断を実施することが重要です。



以下の頻度で定期診断が推奨されています。

- ✓ Webアプリケーションの脆弱性診断：システム改修等の都度
- ✓ プラットフォームの脆弱性診断：四半期に1回

企業にとって定期診断が必要な理由

以下を継続的に実現するためには、定期的な診断が必要です。

point

1

安全なサービスを提供するため

顧客情報などの適切な管理、堅牢なシステムの維持管理により安全なサービスを顧客や取引先に提供する。

定期診断により情報漏洩、システム破壊、サービス停止などのリスクを低減することができる。



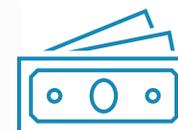
point

2

想定外のセキュリティ対策コストを撲滅するため

サイバー攻撃の被害を受けた場合の損害賠償や再発予防などのコストを撲滅する。

定期診断によりセキュアな状態を保ち続けることで結果的にセキュリティ対策コストを抑えることができる。



point

3

自社への信頼度を高めるため

サイバー攻撃の脅威から身を守るとともに顧客や取引先も守ることで自社への信頼度を高める。

定期診断の実施を自社のポリシーとすることで顧客や取引先からの信頼度を高めることができる。



特に診断が必要なタイミング

定期診断に加えて以下のケースにおいては、[その都度診断をご検討ください](#)。

case

1

システムの改修が発生した

大幅なシステム改修や重要機能の改修が発生した場合

新たな脆弱性が作り込まれている可能性がある。



case

2

システムで取り扱う情報が増えた

顧客情報や機密情報など、
システムで取り扱う情報の量や種類が増えた場合

サイバー攻撃によるインシデントが発生した場合、
甚大な被害や損害に発展する可能性がある。



case

3

新たなサービスの提供を開始した

サービスの提供開始を最優先にするため、
脆弱性診断を後回しにした場合

サービス提供後、脆弱性に起因するインシデントが
発生した場合、世間の信頼を失い、そのサービス
による事業の継続が困難になる可能性がある。



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
- オブテックス・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

- 東急リゾート&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

本資料は、貴社内関係者のみによって使用されるものとし、本資料のいかなる部分について、株式会社神戸デジタル・ラボの事前の承諾を得ずに、外部への頒布・引用・改変を実施してはならないものとさせていただきます。

