脆弱性診断サービス

プラットフォーム脆弱性診断

株式会社神戸デジタル・ラボ

目次

Copyright © Kobe Digital Labo , Inc. All rights Reserved

セキュリティ対策の必要性

DX化やクラウド化が進み、サイバー攻撃が増えている

あらゆるロケーション・モノがネットワークにつながりはじめ、今までセキュリティ対策を実施してこなかった
企業内のシステムに対してもセキュリティ対策の必要性が問われるように。

個人情報保護に関する法整備が進んでいる

EUでのGDPRをきっかけに国内においてもマイナンバー法、改正個人情報保護法など、法整備が進み、
個人情報を扱う企業にはより厳重な管理体制が求められ罰則も課せられるようになってきた。

サプライチェーンなどを狙った攻撃が増えている

サプライチェーン攻撃により、自社のみならず取引先の大企業にまで被害が及ぶような事態も。

上記のような環境の変化により、セキュリティ対策は
以前にも増してその必要性が高まっています。

Copyright © Kobe Digital Labo , Inc. All rights Reserved

脆弱性診断が必要な理由：情報漏えい等の可能性を低減

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。

脆弱性診断によるリスク低減

脆弱性の有無を検査し、見つかった問題点を改修することで、顧客情報や機密情報の漏えい、Webサイトの改ざん・乗っ取り・データ破壊、正規会員への成りすまし、などのリスクを低減することができます。

情報の安全性確保のために、脆弱性診断は必要です。

Copyright © Kobe Digital Labo , Inc. All rights Reserved

脆弱性診断が必要な理由：セキュリティ対策におけるコスト削減

セキュリティインシデントが発生した場合のコスト

事故調査、システム対策、調査や対策のための内部コスト、被害を受けたユーザへの損害賠償などにより、莫大な損失コストが必要となる可能性があります。

脆弱性診断により効率の良い対策が可能に

脆弱性診断は対象システムの規模によって数十万円から実施することができます。事前に脆弱性を把握し、危険度の高い部分から修正していくことで、効率良く問題を解決することができます。脆弱性診断を実施せずにインシデントが発生してしまうと、一から対処しなければならなくなるため作業工数が増えコスト増に繋がります。

脆弱性診断を実施することが、**結果的にセキュリティ対策における**
コスト削減となる可能性があります。

Copyright © Kobe Digital Labo , Inc. All rights Reserved

脆弱性診断が必要な理由：社会的な信用

自社の社会的な信用を守るためにも必要

脆弱性診断などのセキュリティ対策を実施せずに情報漏洩などを起こした場合、顧客や取引先からの信用を失う原因になります。1度でも情報漏洩を起こすと、その事実はインターネットを介して簡単に確認できてしまいます。顧客に安心して自社サービスを使ってもらったり、お取引していただけるよう、脆弱性診断を実施することが必要です。

新規顧客を獲得しづらくなったり、取引先に契約を見直されたりと、
さまざまなリスクにつながり得ます。

Copyright © Kobe Digital Labo , Inc. All rights Reserved

脆弱性を放置することによって被る代表的な攻撃例

✓ **個人情報、機密情報の漏えい・改ざん・データ破壊等**

Webサイトで管理している個人情報や社内の重要な情報が漏えいします。

✓ **会員や管理者への成りすまし**

Webサイトの会員に成りすまして発注をされたりします。
また、管理者に成りすまし、Webサイトを乗っ取られてしまいます。

✓ **誤情報を掲載される**

Webサイトを勝手に改ざんされて、誤情報を掲載されてしまいます。

✓ **他サーバを攻撃する踏み台にされる**

サーバのセキュリティ・ホールを悪用され、スパムメールの発信元になったり、
不正行為を行うための中継点として利用されてしまいます

脆弱性診断はセキュリティ対策の第一歩
まずは**自社システムの現状を把握**するところから始めてみませんか。

Copyright © Kobe Digital Labo , Inc. All rights Reserved

脆弱性診断サービスを選ぶ際の留意事項

point 1

予算とスケジュールの確保

脆弱性診断には、ある程度のコストと完了までにある程度の時間が必要ですので、あらかじめ予算とスケジュールの確保をしておくことが重要です。

point 2

報告会やアフターフォローの有無 （ 対応）

脆弱性診断は一度実施して終わりではありません。診断結果をもとに問題箇所の改修などを行って初めて対策したということになりますので、選定時にアフターフォローの有無を確認するのもポイントです。

point 3

実績のある企業に依頼する （ 対応）

多くの診断実績がある会社であればノウハウが蓄積されているため、より精度の高い診断結果が期待できます。

Copyright © Kobe Digital Labo , Inc. All rights Reserved

目次

Copyright © Kobe Digital Labo , Inc. All rights Reserved

Proactive Defense について

KDLのセキュリティサービス「Proactive Defense（プロアクティブディフェンス）」は、**西日本で情報セキュリティ分野の専門サービスがほとんど無かった2008年からいち早くサービス提供を開始**。
2015年、都道府県警で初の事例として、民間から兵庫県警サイバー犯罪対策課へ任期付警察官としてセキュリティエキスパート派遣を実現するなど、各方面から高い信頼を獲得しています。

Proactive Defense

高い信頼性

サイバー犯罪解決への
協力等数々の実績

確かな技術力

資格保有者で構成された
プロフェッショナルチーム

網羅的な対応

予防対策から事故対応まで
一気通貫のサービス

Copyright © Kobe Digital Labo , Inc. All rights Reserved

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

Copyright © Kobe Digital Labo , Inc. All rights Reserved

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。

Copyright © Kobe Digital Labo , Inc. All rights Reserved

特長1.精度の高いマニュアル診断

ツール診断とマニュアル診断の違い

ツール診断とは市販されている自動診断ツールやASPサービスなどを利用して、診断作業を全てツールが行う診断です。一方マニュアル診断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います。 マニュアル診断はWebサイトの特性に合わせた精度の高い結果を得る為の診断サービスです。Proactive Defenseではマニュアル診断を行っております。

品質保証：経産省「情報セキュリティサービス基準」登録

経産省では、「情報セキュリティサービス基準」を策定しています。一定の技術要件及び品質管理要件を満たし、品質の維持・向上に努めているか審査し、審査に通ったサービスのみが『情報セキュリティサービス台帳』へ登録されます。Proactive Defenseの診断サービスは『情報セキュリティサービス台帳』へ登録されています。

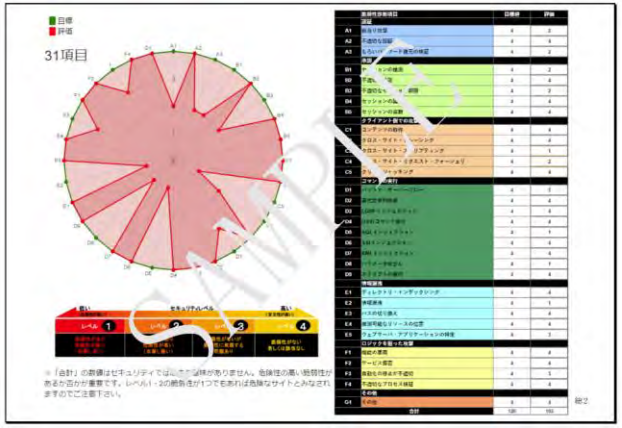
Proactive Defense なら**精度の高い診断が可能**です。

Copyright © Kobe Digital Labo , Inc. All rights Reserved

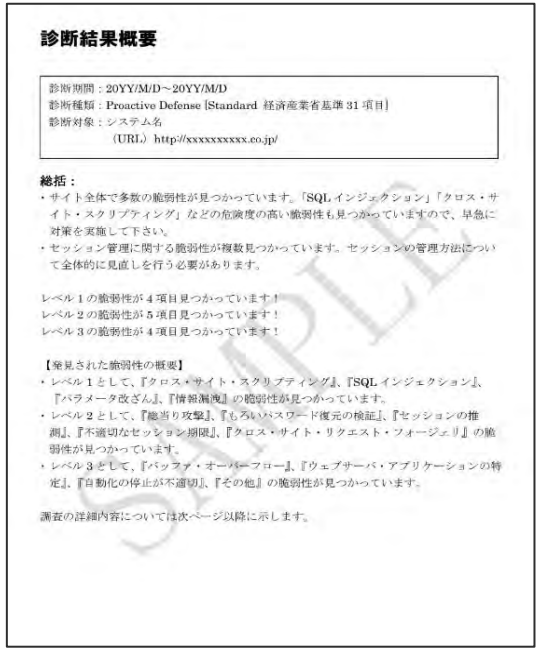
特長2. わかりやすいレポート&アフターフォローも充実

レポートの内容が充実、診断後の報告会・オンライン相談も無料！

診断結果を分かりやすく図解レポート。Webサイトの現状と問題点を徹底的に調査・解析し、さらに、分かりやすい解説によって説明、脆弱性の対策についてもご提案致します。すべて弊社診断員が記述しますので、ツールが自動的に生成した説明とは、分かりやすさが違います。また**診断結果のご報告やオンライン相談も無料で提供**しています。



冒頭に診断の総括をテキストならびに図化し、まとめています。ご多忙な経営層様へのご報告にお使いいただけます。



診断結果概要

診断期間：20YY/M/D～20YY/M/D
診断種類：Proactive Defense [Standard 経済産業省基準 31 項目]
診断対象：システム名
（URL）http://xxxxxxxxxx.co.jp/

総括：
・サイト全体で多数の脆弱性が見つかっています。「SQL インジェクション」「クロス・サイト・スクリプティング」などの危険度の高い脆弱性も見つかっていますので、早急に対策を実施して下さい。
・セッション管理に関する脆弱性が複数見つかっています。セッションの管理方法について全体的に見直しを行う必要があります。

レベル 1 の脆弱性が 4 項目見つかっています！
レベル 2 の脆弱性が 5 項目見つかっています！
レベル 3 の脆弱性が 4 項目見つかっています！

【発見された脆弱性の概要】
・レベル 1 として、『クロス・サイト・スクリプティング』、『SQL インジェクション』、『パラメータ改ざん』、『情報漏洩』の脆弱性が見つかっています。
・レベル 2 として、『総当り攻撃』、『もろいパスワード復元の検証』、『セッションの推測』、『不適切なセッション期限』、『クロス・サイト・リクエスト・フォージェリ』の脆弱性が見つかっています。
・レベル 3 として、『バッファ・オーバーフロー』、『ウェブサーバ・アプリケーションの特定』、『自動化の停止が不適切』、『その他』の脆弱性が見つかっています。

調査の詳細内容については次ページ以降に示します。

診断項目ごとに
以下をご報告

- ✓ 問題点レベル
- ✓ 発生箇所
- ✓ 問題内容の詳細
- ✓ リスク
- ✓ 対策方法

Proactive Defense

A. 認証
A.1 総当り攻撃
A.1.1 パスワードの文字数に関する問題
A.1.1.1 問題点レベル
レベル 2（危険度 中）
A.1.1.2 発生箇所
・○○○画面
（http://xxxxxxxxxx.co.jp/xxx/xxx）
A.1.1.3 問題点
上記の画面にてパスワードの登録を行う際、パスワードとして登録可能な文字数の下限が 6 文字となっています（参照）。そのため、文字数の短い脆弱なパスワードが設定されやすくなっています。

図 1 ○○○画面

A.1.1.4 リスク
文字数が短すぎるパスワードや使用されている文字種が少ないパスワードは、ツールによる解析で簡単に見破られてしまいます。パスワードが見破られると第三者がそのユーザになりすまし、そのユーザの権限で利用可能な様々な機能を悪用することができます。パスワードの解析に必要な時間に関して、以下のような検証結果も存在しています。

Copyright © Kobe Digital Labo , Inc. All rights Reserved

特長3.導入実績多数

株式会社 ytvメディアデザイン様

月間PV1,000万を突破した
Webメディアを脆弱性診断

芝浦工業大学 情報工学科様

自動運転セキュリティ基盤検証
プロジェクトにて、評価実験を支援

経済産業省事業

「開発段階のIoT機器に対する脆弱性検証
事業促進事業」に参加

大手インフラ事業グループ会社様

新機能リリース前の脆弱性診断による
セキュアなWEBサイト構築サポート

大手SI企業様

Webサイトのリニューアルにあたり、
リリース前に脆弱性診断を実施

その他、多数実績ございます

- ✓ **業界最大手 総合アパレルファッション事業**
  ブランドサイト(30サイト)、採用サイト
- ✓ **業界最大手 製造業**
  各事業部毎の見積依頼、問合せBtoBサイト
- ✓ **財務・会計ソフト・経営システム 開発、販売事業**
  コーポレートサイト、経営情報サイト、
  ビジネスノウハウ共有サイト（国内利用者数最大級）
- ✓ **クロスメディアマーケティング企業（大阪ガス関連会社）**
  ファイル転送サービスサイト（国内利用者数最大級）、
  料理レシピ検索サイト

Proactive Defense には、**1000サイト以上の豊富な導入実績**がございます。

Copyright © Kobe Digital Labo , Inc. All rights Reserved

目次

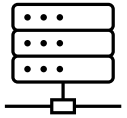
Copyright © Kobe Digital Labo , Inc. All rights Reserved

脆弱性診断の概要：ご提供する脆弱性診断の種類

Webアプリケーション脆弱性診断

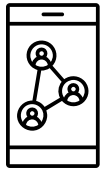
Webアプリケーションの脆弱性診断。発見した脆弱性の内容と脅威を報告し、対策方法をご提案。

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。

Copyright © Kobe Digital Labo , Inc. All rights Reserved

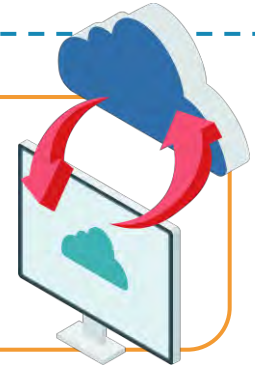
脆弱性診断の概要：各脆弱性診断の範囲

Webアプリケーション脆弱性診断
で洗い出せる範囲

プラットフォーム脆弱性診断
で洗い出せる範囲

Webアプリやスマートフォンアプリの通信先WebAPIの診断については、WebAPI診断の範囲となります。（別途説明資料あり）

クラウド環境（AWS）のセキュリティ設定に関する診断については、クラウドセキュリティ設定診断の範囲となります。（別途説明資料あり）



Copyright © Kobe Digital Labo , Inc. All rights Reserved

脆弱性診断の概要：脆弱性診断の実施イメージ

①弊社よりインターネット経由でアクセスし、攻撃者視点で脆弱性の有無を洗い出します。

②診断結果についてはレポートにまとめてご報告します。

Copyright © Kobe Digital Labo , Inc. All rights Reserved

プラットフォーム脆弱性診断：診断の種類

標準価格	概要	診断対象	実施条件
ブラックボックス診断	サーバに弊社から**インターネット経由でアクセスして診断**します。 インターネットまたはLAN内の特定セグメントより、**ネットワーク経由で把握できるプラットフォームの脆弱性や設定の問題有無を調査**します。	**弊社がアクセスできるサーバ** • ログインは不要です。 • FWなどのネットワーク機器に関しては、ポートスキャンのみの対応となります。	• 弊社が用意した端末を使用して診断できる • 診断の対象をホスティングしている会社から診断の許可を得ている • 診断の対象へ接続できる経路をご提供いただける • 診断の対象がサーバレスでない
ホワイトボックス診断	サーバに**管理者権限でログインして診断**します。 サーバの内部から診断を実施するため、**ブラックボックスの診断では確認できない脆弱性を網羅的に調査**できます。	**弊社がログインできる以下のサーバ** **Linux ・ Unix ・ Windows** • 対応範囲はOS、ミドルウェア、ネットワークです。 • Linux および Unix は SSH のポートを開放する必要があります。 • Windows は135,139,445のポートを開放する必要があります。	上記に加えた以下の条件 • 管理者権限を付与したアカウントをご提供いただける(※)、Linux および Unix の場合 sudo 権限でも可 • ログインに必要なポートを開放していただける • 診断の対象がコンテナで稼働しているサーバでない

※ Active Directory サービスに対する脆弱性診断はプラットフォーム診断の診断範囲には含まれません。

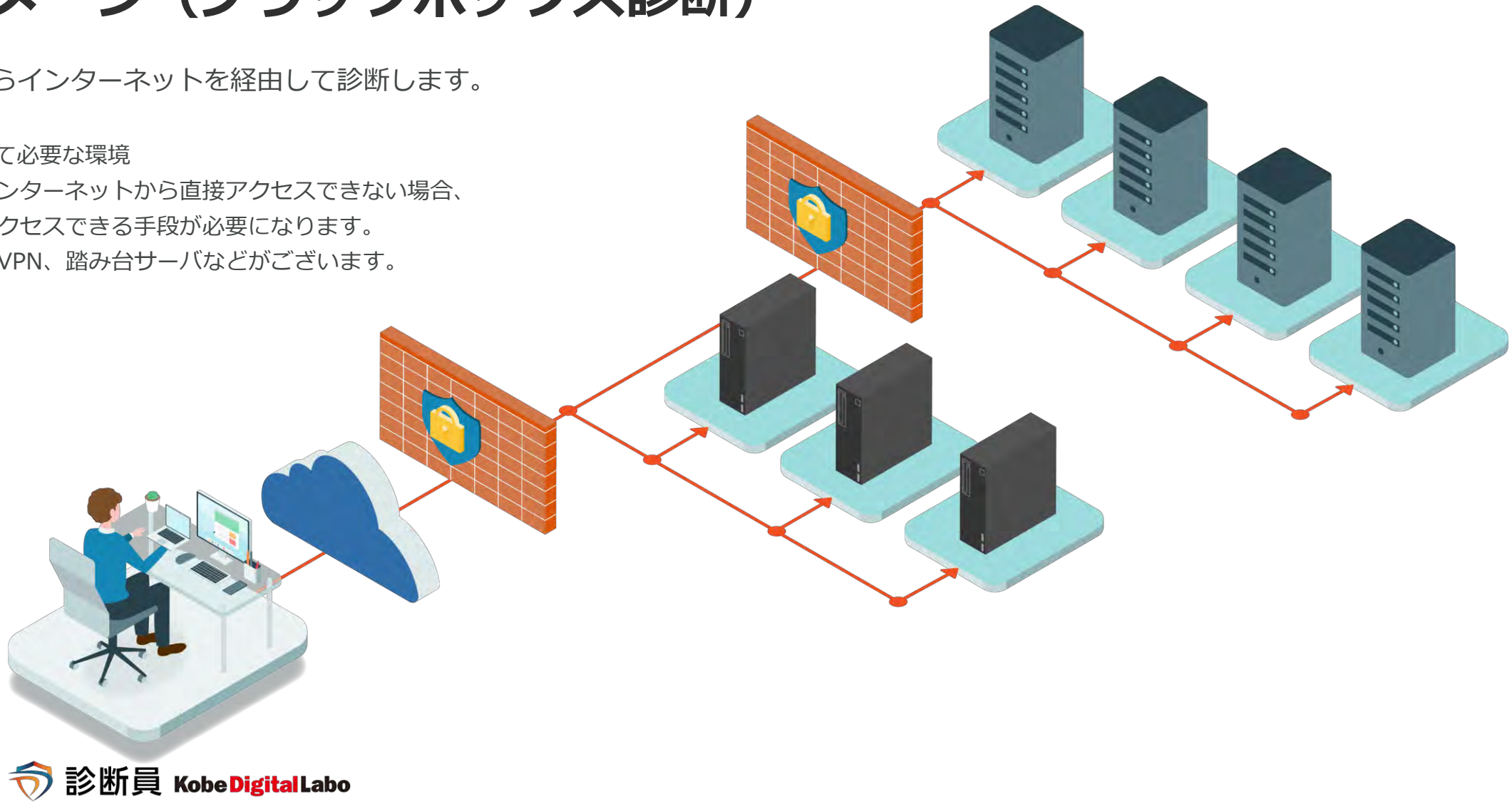
Copyright © Kobe Digital Labo , Inc. All rights Reserved

プラットフォーム脆弱性診断：
診断イメージ（ブラックボックス診断）

弊社環境からインターネットを経由して診断します。

診断にあたって必要な環境

✓ サーバがインターネットから直接アクセスできない場合、
サーバへアクセスできる手段が必要になります。
接続方法はVPN、踏み台サーバなどがございます。

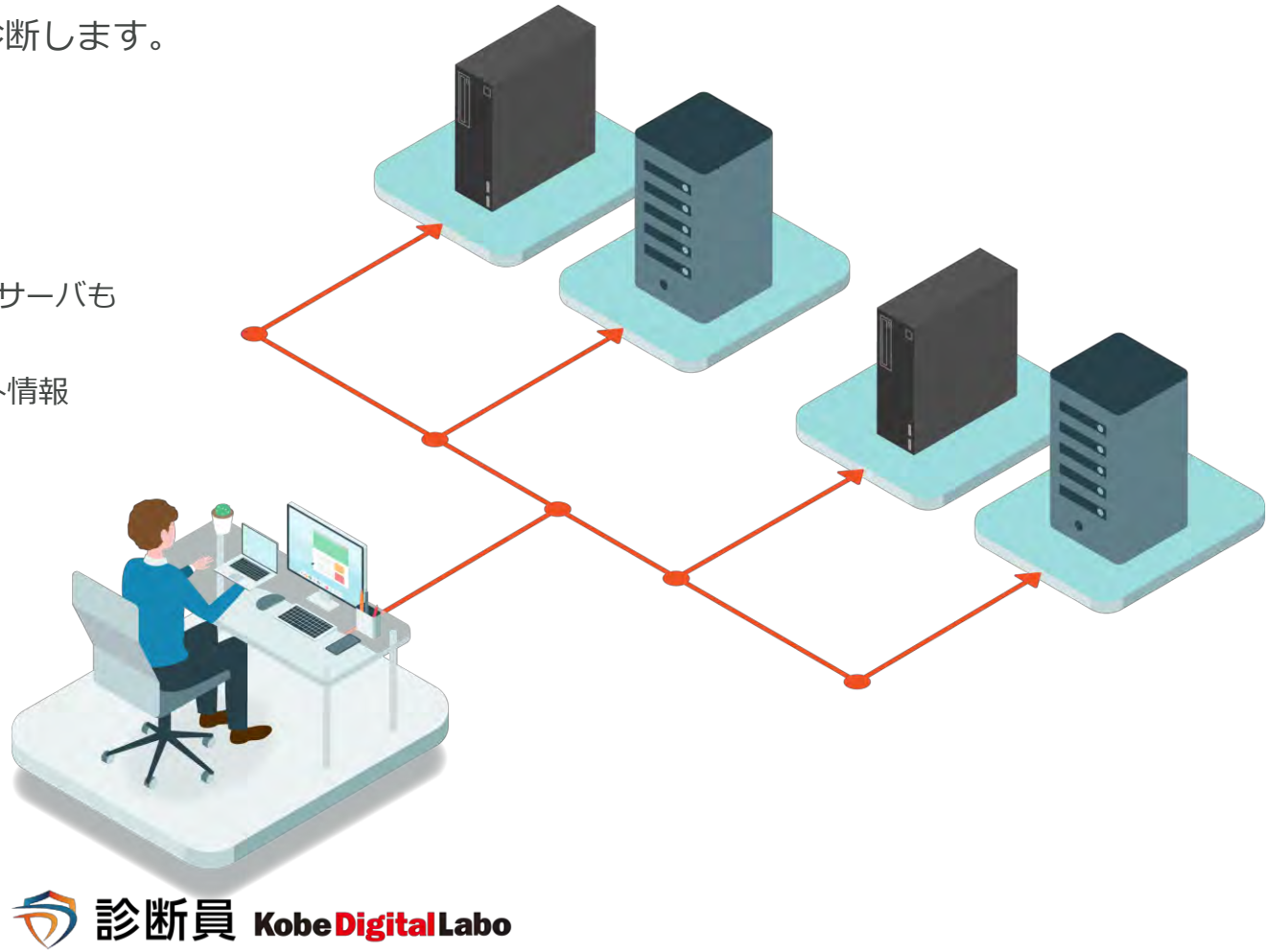


Copyright © Kobe Digital Labo , Inc. All rights Reserved

プラットフォーム脆弱性診断：
診断イメージ（ホワイトボックス診断）

サーバにログインし、内部からセキュリティ上の問題を診断します。
潜在的な脆弱性を洗い出します。

診断にあたって必要な環境
✓ サーバへアクセスできる手段
　　インターネット経由、VPN、プロキシ、必要に応じて踏み台サーバも
　　オンサイトでの診断も可能
✓ サーバに管理者権限（sudoも可）でログインする為のアカウント情報



Copyright © Kobe Digital Labo , Inc. All rights Reserved

プラットフォーム脆弱性診断：診断項目

診断項目	概要	ブラック ボックス	ホワイト ボックス
ポートスキャン	TCP及びUDPに対してポートスキャンを実施し、サーバの運用目的に合致しないポートが開放されていないか調査します。 • TCPポートスキャン（IPv4） • UDPポートスキャン（IPv4）	○	○
ネットワークサービス調査	サーバで稼働しているサービス（HTTP・SSH・SMTP・DNS・FTPなど）ごとに下記の項目について確認し、公開すべきでない情報の公開や設定の不備がないか調査します。 • バナー情報の開示 • バージョン情報の開示 • 暗号化の不備 • 認証の不備 • アクセス権の不備 • 機能の悪用 • ネットワーク設定の不備	△	○
サーバ内部調査	サーバにログインした上で下記項目について確認し、設定の不備や不正なサービスが存在していないか調査します。 • OSの設定 • ユーザ関連の設定 • ネットワークの設定 • 稼働中のサービス	×	○
脆弱性調査	サーバで使用されている各種ソフトウェアのバージョンを確認し何らかの脆弱性を抱えていないか調査します。 • 特定されたバージョンでの既知の脆弱性調査	△	○
その他	上記のいずれにも該当しない問題	○	○

Copyright © Kobe Digital Labo , Inc. All rights Reserved

プラットフォーム脆弱性診断：ご提供内容/価格

ご提供内容		ブラックボックス診断	ホワイトボックス診断
1	ツール疑似攻撃診断	○	○
2	マニュアル脆弱性診断	-	
3	報告（報告書・報告会） ※報告書には対策方法を含みます	○	○

標準価格	ブラックボックス診断	ホワイトボックス診断
基本料金	220,000円	440,000円
診断対象単価	110,000円（1IPあたり）	330,000円（1台あたり）

再診断（オプション価格）	ブラックボックス診断	ホワイトボックス診断
基本料金	110,000円（1IP分含む）	220,000円（1台分含む）
追加料金	55,000円（1IP追加あたり）	165,000円（1台追加あたり）

※価格はすべて税抜き表記となります

- 【 3IP・ブラックボックス診断で3IPを対象に診断する場合の費用例 】
  （基本料金）220,000 円 +（診断対象単価）110,000 円　× 3 IP = 550,000 円
- 【 3IP・ブラックボックス診断で3IPを対象に再診断する場合の費用例 】
  （基本料金）110,000 円 +（追加料金）55,000 円　× 2 IP = 220,000 円

Copyright © Kobe Digital Labo , Inc. All rights Reserved

導入の流れ（共通）

Step.1	Step.2	Step.3	Step.4	Step.5	Step.6
サービス申込	**スケジュール調整**	**診断実施**	**報告書作成**	**納品・ご報告会**	**再診断** **（オプション）**
✓機密保持契約 ✓情報提供 ✓お見積り ✓ご発注	✓日程調整 ✓問題発生時の連絡体制確認 ✓ヒアリングシートへのご記入 ✓(必要に応じて)お客様にてサーバ会社へ診断申請	✓専門チームが診断（KDL） ✓深刻な問題が発見された場合は速報として報告（KDL）	✓報告書作成（KDL）	✓報告書の納品（KDL） ※基本的には診断最終日にデータ提出 ✓報告会開催	✓システム改修後、再診断範囲確定 ✓再診断日程調整 ✓再診断実施

報告会はオンラインにて開催します。**実際に診断した診断員が問題点と改修方法まで詳しくご説明**します。
関係各位への詳細なご報告、Q&Aなど、万全のサポート体制で対応させて頂きます。

Copyright © Kobe Digital Labo , Inc. All rights Reserved

目次

Copyright © Kobe Digital Labo , Inc. All rights Reserved

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）

Copyright © Kobe Digital Labo , Inc. All rights Reserved

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

Copyright © Kobe Digital Labo , Inc. All rights Reserved

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。

22000044(06)

Copyright © Kobe Digital Labo , Inc. All rights Reserved