脆弱性診断サービス

Webアプリケーション脆弱性診断

株式会社神戸デジタル・ラボ

Proactive Defense

Kobe Digital Labo

目次

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。

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。

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。

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。

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。

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。

目次

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

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

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。

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

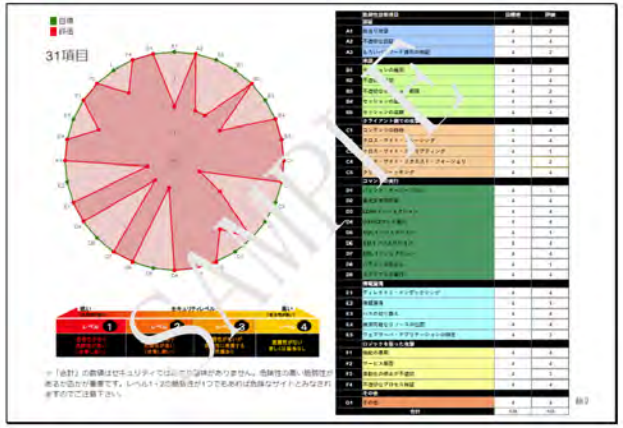
経産省では、「情報セキュリティサービス基準」を策定しています。一定の技術要件及び品質管理要件を満たし、品質の維持・向上に努めているか審査し、審査に通ったサービスのみが『情報セキュリティサービス台帳』へ登録されます。Proactive Defenseの診断サービスは『情報セキュリティサービス台帳』へ登録されています。

Proactive Defense なら**精度の高い診断が可能**です。

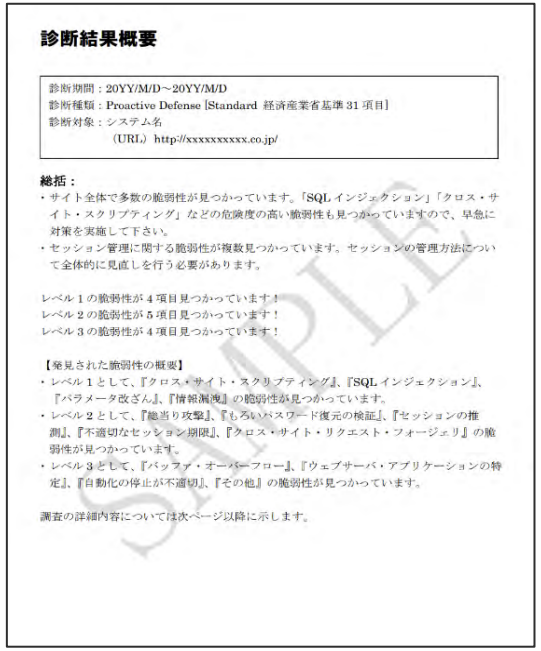
特長2. わかりやすいレポート&アフターフォローも充実

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。

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

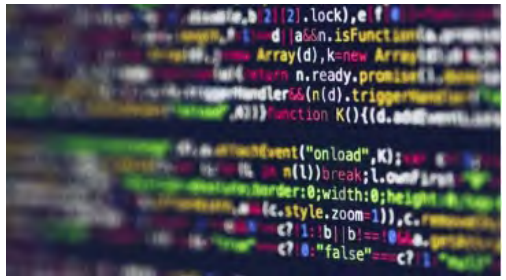
経済産業省事業

「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。

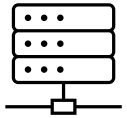
目次

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

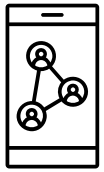
Webアプリケーションの脆弱性診断。発見した脆弱性の内容と脅威を報告し、対策方法をご提案。

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。

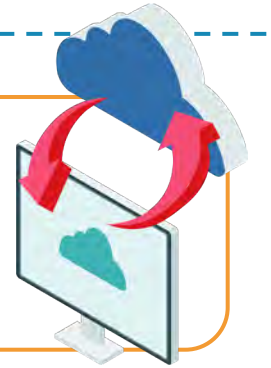
脆弱性診断の概要：各脆弱性診断の範囲

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）

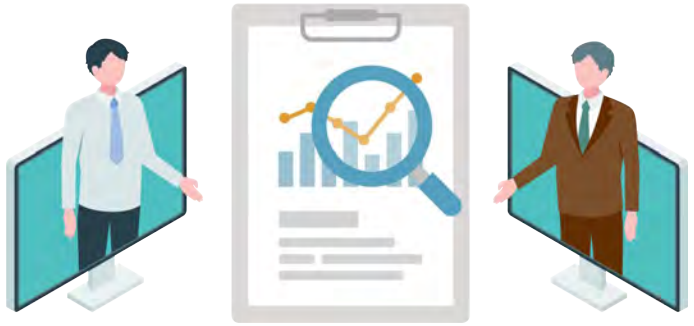
クラウド環境（AWS）のセキュリティ設定に関する診断については、クラウドセキュリティ設定診断の範囲となります。（別途説明資料あり）



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。



Webアプリケーション脆弱性診断：診断プラン

２つの診断プランをご用意しています、サイト特性や目的に応じてお選びください。

◆ スタンダードプラン（ 22 項目診断 ）

- ✓ **Webサイトの基本的な安全性を確認したい方におすすめのプラン**
  総当たり攻撃や認証まわりの不備、XSS・SQLインジェクションなど、代表的な脆弱性を中心に22項目の診断を行います。
- ✓ **コーポレートサイト、キャンペーンページなど、比較的シンプルな構成のWebサイトに最適**
  「まずは現状を把握したい」「最低限の安全性を確認したい」という場合におすすめです。

◆ アドバンスドプラン（ 31 項目診断 ）

- ✓ **より高いセキュリティ対策が求められるWebサービス向けのプラン**
  スタンダードの内容に加え、LDAP／XMLインジェクション、サービス拒否（DoS）、スクリプト実行などを含む31項目を診断します。
- ✓ **ログイン機能や会員情報の管理、決済処理、外部APIとの連携などを含むWebサービスや、個人情報・業務データを扱うシステムに最適**
  高い信頼性や法令順守が求められるサイト、事業の中核となるサービスにはこのプランをおすすめします。

Webアプリケーション脆弱性診断：診断項目（1/3）

診断メニュー	診断内容	脆弱性が存在することによって被る被害	22項目	31項目
認証（Authentication） ※認証を使用しているウェブサイトで適切に認証が実施されているか診断を行います。	総当たり攻撃 （Brute Force）	IDやパスワードが簡単に推測可能であり、管理者や他のユーザに成りすまされてしまいます。	○	○
	不適切な認証 （Insufficient Authentication）	正常なログイン処理を介さずにログイン後の画面にアクセスされてしまうため、成りすましや情報漏えいの危険性があります。	○	○
	もろいパスワード復元の検証 （Weak Password Recovery Validation）	ユーザがパスワードを忘れた際の回復方法に問題があり、パスワードの情報が外部に漏えいしてしまいます。	○	○
承認（Authorization） ※認証後のセッション管理やパスワード管理に問題が無いか診断を行います。	セッションの推測 （Session Prediction）	セッション情報が推測しやすい値の場合、攻撃者は正しい値を推測し、管理者やユーザに成りすますことができます。	○	○
	不適切な承認 （Insufficient Authorization）	承認が不適切だと、アクセス権限の高いコンテンツや機能へのアクセスを認めてしまいます。これにより、攻撃者が他のユーザや管理者に成りすます危険性があります。	○	○
	不適切なセッション期限 （Insufficient Session Expiration）	セッション期限が不適切である場合、ユーザのセッション情報を盗用しやすくなり、攻撃者が管理者やユーザに成りすますことができます。	○	○
	セッションの固定 （Session Fixation）	攻撃者が任意のセッション情報を使って管理者やユーザに成りすますことができます。	○	○
	セッションの盗難 （Session Hijack）	SSL等を使用して暗号化をしていない場合、攻撃者はセッション情報を容易に取得することができ、管理者やユーザに成りすますことができます。	○	○

Webアプリケーション脆弱性診断：診断項目（2/3）

診断メニュー	診断内容	脆弱性が存在することによって被る被害	22項目	31項目
クライアント側での攻撃 （Client-side Attacks） ※クライアント側から行われる攻撃に対する診断を行います。	コンテンツの詐称 （Content Spoofing）	偽のコンテンツをあたかも正式なものであるかのように装ってウェブサイトに表示し、ユーザを欺きます。これにより、パスワードを抜き取られたり、フィッシング詐欺サイトへ誘導されたりする危険性があります。	○	○
	クロス・サイト・トレーシング （Cross Site Tracing）	ウェブのヘッダ情報を不正に読み出されてしまいます。これにより、他の脆弱性を利用して管理者や他のユーザに成りすまされてしまいます。	○	○
	クロス・サイト・スクリプティング （Cross Site Scripting （XSS））	サイトをまたがって不正な要求を送り、ユーザが意図していないスクリプトを実行させられてしまいます。その結果、例えば偽ページを表示することが可能になり、フィッシング詐欺などに悪用されてしまいます。	○	○
	クロス・サイト・リクエスト・フォージェリ （Cross Site Request Forgery（CSRF））	サイトをまたがって不正な要求を送り、ユーザが意図していない操作を実行させられてしまいます。例えば、ユーザが意図しないままオンラインショップで買い物をさせられたりしてしまいます。	○	○
	クリックジャッキング （ClickJacking）	ログインしているユーザ向けに提供されている機能のうち、マウス操作のみで実行可能な機能をユーザは意図せず実行させられてしまいます。	○	○
コマンドの実行 （Command Execution） ※コマンド実行により行われる攻撃に対する診断を行います。	バッファ・オーバフロー （Buffer Overflow）	アプリケーションの予期しないデータを送り、アプリケーションを異常終了させられてしまいます。これにより、ウェブサーバのサービスを停止させられたり、ウェブサーバを乗っ取られる危険性があります。	○	○
	書式文字列攻撃 （Format String Attack）	入力された文字列を書式加工する際にプログラムをクラッシュさせたり、不正なコードを実行させられてしまいます。これにより、ウェブサーバのサービスを停止させられたり、ウェブサーバを乗っ取られる危険性があります。		○
	LDAP インジェクション （LDAP Injection）	LDAPコマンドを不正に使用されてしまいます。これにより、ウェブサイトからの情報漏えい、改ざん等の危険性があります。		○
	OS のコマンド実行 （OS Commanding）	サーバ内のOSのコマンドを不正に実行されてしまいます。これにより、ウェブサイトからの情報漏えい、改ざん等の危険性があります。	○	○
	SQL インジェクション （SQL Injection）	DBサーバへのアクセスを不正に実行されてしまいます。これにより、ウェブサイトからの情報漏えい、改ざん等の危険性があります。	○	○
	SSI インジェクション （SSI Injection）	SSIコマンドを不正に実行されてしまいます。これにより、ウェブサイトからの情報漏えい、改ざん等の危険性があります。		○
	XMLインジェクション （XML Injection）	XMLデータにスクリプト等を混入して攻撃されてしまいます。これにより、ウェブサイトからの情報漏えい、改ざん等の危険性があります。		○
	パラメータ改ざん （Parameter Manipulation）	パラメータを不正に改ざんされてしまいます。その結果、管理者や他のユーザに成りすまされてしまいます。	○	○
	スクリプトの実行 (Script Execution)	許可していないスクリプトを実行されてしまうため、情報の漏えいやウェブサイトの改ざんを許してしまいます。		○

Webアプリケーション脆弱性診断：診断項目（3/3）

診断メニュー	診断内容	脆弱性が存在することによって被る被害	22項目	31項目
情報漏洩 （Information Leakage） ※ウェブサーバから情報が漏えいする可能性が無いか診断を行います。	ディレクトリ・インデックシング （Directory Indexing）	ウェブサーバ内のファイルを閲覧されることにより、ウェブサーバ攻撃の足がかりとされてしまいます。		○
	情報漏洩 （Information Leakage）	ウェブサーバから意図していない内部情報が外部に漏えいしてしまいます。	○	○
	パスの切り換え （Path Traversal）	ウェブブラウザのアドレスバーやファイル名を指定するパラメータなどの箇所から任意のパスを受け付けてしまうため、機密情報などが保管されているパスを指定されることにより情報漏えいにつながります。	○	○
	推測可能なリソースの位置 （Predictable Resource Location）	フォルダ名やファイル名が推測可能な簡単な名称になっているなど、内部のリソースの配置が推測可能な場合、重要な情報や機能が外部に漏えいする危険性があります。	○	○
	ウェブサーバ・アプリケーションの特定 （Fingerprinting）	ウェブサーバ、ウェブアプリケーションの種類やバージョン情報から脆弱性が探り出され、攻撃の足がかりとされてしまいます。	○	○
ロジックを狙った攻撃 （Logical Attacks） ※ウェブサーバやウェブアプリケーションの持つ機能を狙った攻撃が可能か診断を行います。	機能の悪用 （Abuse of Functionality）	ウェブサーバ、ウェブアプリケーションの持つ機能を不正に実行されてしまいます。その結果、SPAM（メールを大量配信すること）の中継地点に使われるなど、悪用されてしまいます。	○	○
	サービス拒否 （Denial of Service）	ウェブサーバのサービスを停止、もしくは低下させられてしまいます。		○
	自動化の停止が不適切 （Insufficient Anti-automation）	ロボットなどによるウェブサーバへの連続攻撃を受け、正しいIDやパスワードを探られたり、ウェブサーバに負荷をかけられたりしてしまいます。		○
	不適切なプロセス検証 （Insufficient Process Validation）	正常な画面遷移を無視して特定の画面にアクセスされてしまうため、成りすましや情報漏えいの危険性があります。		○
その他	上記以外の診断方法で問題があれば報告致します。		○	○

Webアプリケーション脆弱性診断：ご提供内容/価格

ご提供内容（各プラン共通）	
1	ツール疑似攻撃診断
2	マニュアル脆弱性診断
3	報告（速報・報告書・報告会） ※速報は最も危険度の高いレベル1限定で標準価格に含みます

標準価格	①スタンダードプラン（22項目診断）	②アドバンスドプラン（31項目診断）
基本料金	275,000円	330,000円
機能単価（診断対象機能の1機能あたり）	49,500円	55,000円

オプション価格	実施内容	価格
再診断	発見した脆弱性に対して再診断を実施し、セキュリティレベルを向上する	初回診断の3割（1サイトあたり）
速報	最も危険度の高いレベル1より低いレベルの脆弱性についても速報	11,000円（1日あたり）
休日対応	診断期間が限られる場合、ご要望に応じて休日対応可能	55,000円（1日あたり）

※価格はすべて税抜き表記となります

- 【2機能のWebサイトを①スタンダードプラン（22項目診断）で診断する場合の費用例 】
  ①の基本料金:275,000円 + ①の機能単価:49,500円 × 2機能 = 374,000円

EC加盟店様向けサービス

一般社団法人日本クレジット協会が定める「クレジットカード・セキュリティガイドライン」の改訂（6.0版）に伴い、2025年4月以降すべてのEC加盟店様に対して、脆弱性対策や不正利用対策の実施が義務付けられました。

EC加盟店様は「ECサイトのセキュリティ対策実施状況申告書」を加盟店契約を結んでいるクレジットカード会社や決済代行会社に提出する必要があります。

「ECサイトのセキュリティ対策実施状況申告書」の実施状況を
チェックすることができます。

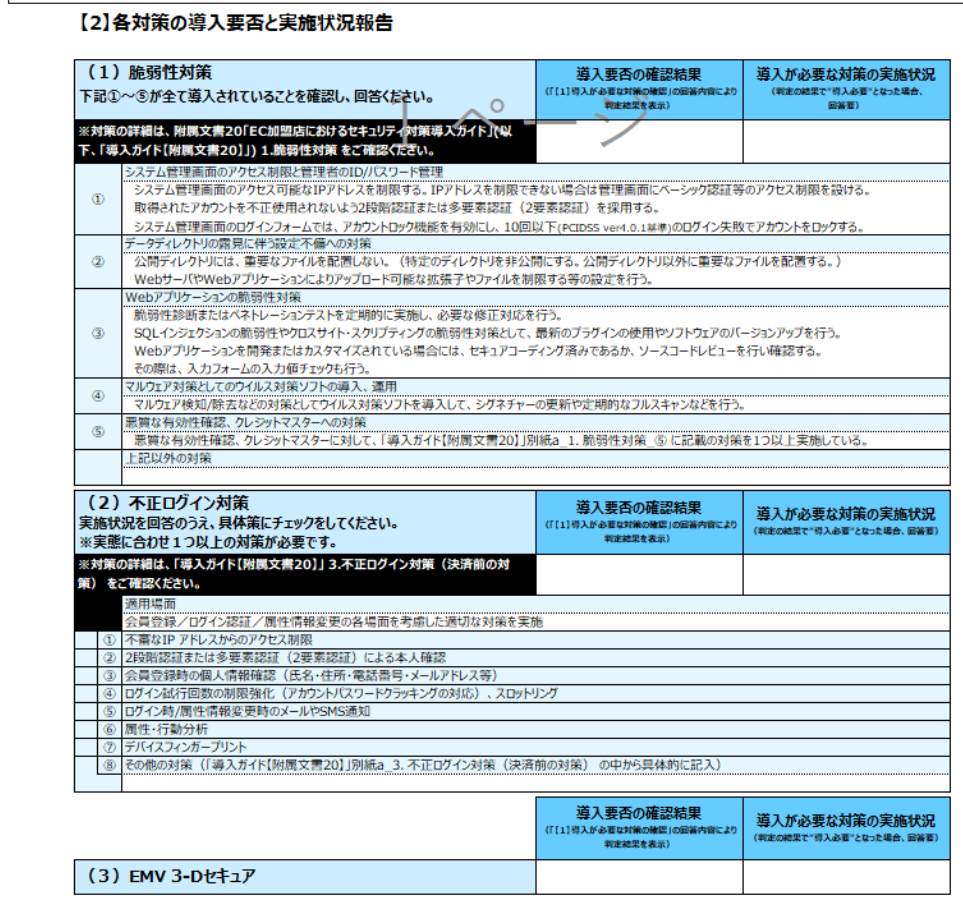
EC加盟店様向けサービス

1. **EC加盟店様向け第三者チェックサービス**
   セキュリティ対策実施状況申告書の「脆弱性対策」、「不正ログイン対策」および「EMV 3-Dセキュア」の実施状況について確認しご報告します。

2. **ECアドバイザリーサービス**
   ECサイトセキュリティ対策の相談に対する助言やアドバイスを実施します。

ECサイトのセキュリティ対策実施状況申告書（イメージ抜粋）

※この様式は新規EC加盟店の契約時調査及び既存加盟店の定期調査における指針対策の導入状況調査として加盟店から申告して頂く内容を例示したものであり、実際の様式については加盟店契約を結んでいるクレジットカード会社や決済代行会社へご確認ください



【2】各対策の導入要否と実施状況報告

（1）脆弱性対策 下記①～⑤が全て導入されていることを確認し、回答ください。		導入要否の確認結果 （「【1】導入が必要な対策の確認」の回答内容により判定結果を表示）	導入が必要な対策の実施状況 （判定の結果で"導入必要"となった場合、回答要）
※対策の詳細は、附属文書20「EC加盟店におけるセキュリティ対策導入ガイド」（以下、「導入ガイド【附属文書20】」）1.脆弱性対策 をご確認ください。			
①	システム管理画面のアクセス制限と管理者のID/パスワード管理 システム管理画面のアクセス可能なIPアドレスを制限する。IPアドレスを制限できない場合は管理画面にベーシック認証等のアクセス制限を設ける。 取得されたアカウントを不正使用されないよう2段階認証または多要素認証（2要素認証）を採用する。 システム管理画面のログインフォームでは、アカウントロック機能を有効にし、10回以下(PCIDSS ver4.0.1基準)のログイン失敗でアカウントをロックする。		
②	データディレクトリの露見に伴う設定不備への対策 公開ディレクトリには、重要なファイルを配置しない。（特定のディレクトリを非公開にする。公開ディレクトリ以外に重要なファイルを配置する。） WebサーバやWebアプリケーションによりアップロード可能な拡張子やファイルを制限する等の設定を行う。		
③	Webアプリケーションの脆弱性対策 脆弱性診断またはペネトレーションテストを定期的に実施し、必要な修正対応を行う。 SQLインジェクションの脆弱性やクロスサイト・スクリプティングの脆弱性対策として、最新のプラグインの使用やソフトウェアのバージョンアップを行う。 Webアプリケーションを開発またはカスタマイズされている場合には、セキュアコーディング済みであるか、ソースコードレビューを行い確認する。 その際は、入力フォームの入力値チェックも行う。		
④	マルウェア対策としてのウイルス対策ソフトの導入、運用 マルウェア検知/除去などの対策としてウイルス対策ソフトを導入して、シグネチャーの更新や定期的なフルスキャンなどを行う。		
⑤	悪質な有効性確認、クレジットマスターへの対策 悪質な有効性確認、クレジットマスターに対して、「導入ガイド【附属文書20】」別紙a 1. 脆弱性対策 ⑤ に記載の対策を1つ以上実施している。		
	上記以外の対策		

（2）不正ログイン対策 実施状況を回答のうえ、具体策にチェックをしてください。 ※実態に合わせ１つ以上の対策が必要です。		導入要否の確認結果 （「【1】導入が必要な対策の確認」の回答内容により判定結果を表示）	導入が必要な対策の実施状況 （判定の結果で"導入必要"となった場合、回答要）
※対策の詳細は、「導入ガイド【附属文書20】」3.不正ログイン対策（決済前の対策） をご確認ください。			
	適用場面		
	会員登録／ログイン認証／属性情報変更の各場面を考慮した適切な対策を実施		
①	不審なIP アドレスからのアクセス制限		
②	2段階認証または多要素認証（2要素認証）による本人確認		
③	会員登録時の個人情報確認（氏名・住所・電話番号・メールアドレス等）		
④	ログイン試行回数の制限強化（アカウントパスワードクラッキングの対応）、スロットリング		
⑤	ログイン時/属性情報変更時のメールやSMS通知		
⑥	属性・行動分析		
⑦	デバイスフィンガープリント		
⑧	その他の対策（「導入ガイド【附属文書20】」別紙a 3. 不正ログイン対策（決済前の対策） の中から具体的に記入）		

	導入要否の確認結果 （「【1】導入が必要な対策の確認」の回答内容により判定結果を表示）	導入が必要な対策の実施状況 （判定の結果で"導入必要"となった場合、回答要）
（3）EMV 3-Dセキュア		

EC加盟店様向けサービス：ご提供内容/価格

項目	実施内容	価格
EC加盟店様向け 第三者チェックサービス	セキュリティ対策実施状況報告書の項目について対応状況をヒアリング等で確認します。	100,000円
ECアドバイザリーサービス	ECサイトセキュリティ対策の相談に対する助言、提案を行う ※EC加盟店様向け第三者チェックサービスご契約者さまのみ	150,000円（契約期間中10件まで）

※価格はすべて税抜き表記となります

（補足）Webアプリケーション脆弱性診断：見積に必要な情報

- ✓ **診断対象ドメイン**
  - 実際に対象Webサイトにアクセスして診断対象画面を洗い出します
    (システム規模にもよりますが洗い出しに1～2週間程度いただきます)
- ✓ **Webサイトの情報**
  - ログイン機能がある場合は、診断対象範囲が網羅的に確認できるユーザアカウントをご提供ください
  - 機能一覧や画面一覧など、Webサイトの持つ機能がわかる資料があればご提供ください
  - 総リクエスト数・画面ごとのリクエスト数・パラメーター一覧のいずれかを提供いただければ、
    Webサイトの確認無しで見積もりが可能です
- ✓ **ご希望の診断プラン**
  - スタンダードプラン or アドバンスドプラン
- ✓ **オプションの要否**
  - 再診断
- ✓ **スマホ・携帯サイトの診断要否**
- ✓ **リモートアクセスの可否（オンサイト診断要否）**
- ✓ **テスト環境の有無**

開発中またはインターネットアクセスができないWebサイトの場合、資料ベースでのお見積りとなります。
資料ベースでのお見積りの場合は、2～3営業日でご提示可能です。

導入の流れ

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。

目次

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