# 株式会社ツチノコテクノロジー Webシステム脆弱性診断

作成　2021年3月3日

更新　2021年3月3日

目次

# はじめに

昨今、多くの企業が Web システムを独自に開発し、顧客に提供しています。その際に、社内に十分な技術的な知識がないため、多くの企業では外部の会社に制作を委託することが多く見受けられます。その際、必ず問題として浮上するのは、「このシステムはきちんと作成されているのか？」という監査の問題です。どうやってチェックを行えば、顧客に対して「このシステムは安全です」と言えるのでしょうか？

そこでツチノコテクノロジーでは、ツールを使った脆弱性診断をご提案します。診断対象の脆弱性とその想定被害についてのリストをもとに、ご依頼いただいた Web システムに脆弱性があるかどうか審査いたします。利用するツールの設定内容も公開いたしますので、Web システムの制作を委託している場合、この概要資料をもとに、脆弱性診断を実施してもらうことを依頼いただけると思います。世間を賑わす情報漏洩などをみたことがあると思います。脆弱性とは、油断から生まれるのではなく、知らなかったからこそ生まれてしまうものです。開発担当者に最低限の脆弱性のチェック方法を、本書をもってお伝えいただければと思います。

もし、弊社に脆弱性診断をご依頼いただく場合の費用は最後に掲載しております。ご検討のほど、どうぞよろしくお願いいたします。

# 用語の統一

## WEBシステム

- ホームページ
- インターネットショップ（ECサイト）
- 社内システムのうち、サーバーに接続して利用しているもの
- Webサービス
- Webアプリケーション

以上の用語はすべて統一して、「Webシステム」と呼びます。
主に Internet Explorer や Google Chrome 等のブラウザで閲覧するシステムのことです。

## 診断対象脆弱性と想定被害

| No | 診断項目 | 危険度 | 攻撃方法 | 想定被害 | | |
|---|---|---|---|---|---|---|
| | | | | 漏洩 | 改ざん | 妨害 |
| 1 | SQLインジェクション | 高 | 能動的 | ○ | ○ | ○ |
| 2 | クロスサイト・スクリプティング | 中 | 受動的 | ○ | △ | |
| 3 | CSRF（クロスサイト・リクエスト・フォージェリ） | 中 | 受動的 | △ | ○ | ○ |
| 4 | OSコマンド・インジェクション | 高 | 能動的 | ○ | ○ | ○ |
| 5 | ディレクトリ・リスティング | 低～高 | 能動的 | ○ | | |
| 6 | メールヘッダ・インジェクション | 中 | 能動的 | | | ○ |
| 7 | パス名パラメータの未チェック<br>ディレクトリ・トラバーサル | 高 | 能動的 | ○ | △ | |
| 8 | 意図しないリダイレクト | 中 | 受動的 | ○ | | |
| 9 | HTTPヘッダ・インジェクション | 中 | 受動的 | ○ | △ | |
| 10 | 認証 | 低～中 | 能動的 | ○ | ○ | |
| 11 | セッション管理の不備 | 低～高 | 能動的<br>受動的 | ○ | ○ | |
| 12 | 認可制御の不備、欠落 | 高 | 能動的 | ○ | ○ | |
| 13 | クローラへの耐性 | 低～中 | 能動的 | | | ○ |

※ 本診断の診断対象脆弱性は、IPA発表の「ウェブ健康診断 診断内容」を参考に設定されています。

※ 本診断は検査パターンを絞り込んだものです。安全宣言には繋がりません。

※ 診断の結果を確認した後は、より詳細な診断を受けたり、「安全なウェブサイトの作り方」を参考に対策を実装することなどを、検討してください。

# 診断対象脆弱性の概要と一般的な対策

## 1. SQLインジェクション

SQLインジェクションとは、不正なスクリプトをサーバーに送り込み、データベースの内容を不正に取得する行為のこと。または、それを可能にしてしまうサイトの欠陥（脆弱性）のこと。

SQLとはデータベースの情報を取り扱うためのコンピュータ言語。SQLを（不正に）注ぎ込む＝インジェクションするので、SQLインジェクション。

一般的な対策

クライアントから送信された内容をそのままSQL（の一部）として使用しない。SQL文の構築にはプレースホルダーの機能を使用する。

## 2. クロスサイト・スクリプティング

クロスサイト・スクリプティング（XSS）とは、悪意あるスクリプトを公開し、閲覧者を危険サイトへと誘導する行為のこと。または、それを可能にしてしまうサイトの欠陥（脆弱性）のこと。

サイトを越えて（＝クロス）スクリプトを仕込むので、クロス・サイト・スクリプティング。略称は、IT用語でCSSが既に存在する（カスケード・スタイルシート）のと、英語圏の略語の技法によりXSSとなっている。

一般的な対策

投稿フォームの内容はそのままHTMLとして表示せず、タグの無効化を行って投稿する。一部タグを使用可能にしたい場合は、先に一律で無効化してから、必要なタグだけを有効化して表示する。

## 3. CSRF（クロスサイト・リクエスト・フォージェリ）

CSRFとは、サイトに不正スクリプトを設置し、閲覧者に実行させることで、閲覧者が権限を持つ操作を乗っ取る行為のこと。または、その手法が有効であるという脆弱性のこと。

例えば、SNSの非公開記事を不正スクリプトにより勝手に公開させられる、閲覧者のアカウントで勝手に買物をされる等。サイトを越えて（＝クロス）操作（＝リクエスト）を捏造する（＝フォージェリ）ので、クロス・サイト・リクエスト・フォージェリ。

一般的な対策

サイト構造を、サイト外の処理が起点になっている操作（POST）を基本的に受け付けないような作りにする。

## 4. OSコマンド・インジェクション

投稿型サイトにスクリプトを混ぜた投稿を行い、サーバー上でコマンドを不正に実行する行為のこと。または、それを可能にしてしまうサイトの欠陥（脆弱性）のこと。

OSのコマンドを（不正に）注ぎ込む＝インジェクションするので、OSコマンド・インジェクション。

一般的な対策

投稿フォームの内容をそのままOSコマンド（の一部）として使用しない。

## 5. ディレクトリ・リスティング

サーバー上のURLを任意に入力して、指定したパス（ディレクトリ）内のファイル一覧を表示すること。または、それを可能にしてしまうサイトの欠陥（脆弱性）のこと。

標準的なWebサーバーでは、Index.html などのインデックスファイルが無い場合にディレクトリの中身をリスト公開するDirectory Index機能が備わっているが、特に必要としない場合はoffにすることが推奨される。意図してDirectory Index機能を使いディレクトリ公開しているのであれば問題は無い。

一般的な対策

各フォルダに index.html などのインデックスファイルを設置する。もしくはDirectory Index機能を解除する。

## 6. メールヘッダ・インジェクション

メールフォームにて不正な投稿を行い、メールヘッダを書き換えることで、件名やメール送信先などを操作する行為のこと。または、それを可能にしてしまうサイトの欠陥（脆弱性）のこと。SPAM投稿などに悪用される危険性がある。

一般的な対策

投稿フォームの内容をそのまま使用せず、改行削除などのエスケープ処理をする。メールフォームに使用するライブラリを最新化する。

## 7. パス名パラメータの未チェック ディレクトリ・トラバーサル

ディレクトリ・トラバーサルとは、不正なURL指定を行って、公開を意図しないディレクトリ一覧やファイルを取得する行為のこと。または、それを可能にしてしまうサイトの欠陥（脆弱性）のこと。

一般的な対策

標準的なWebサーバー（Apache、nginx）で、かつ静的なアクセス（＝CGIやPHPなどを使わない）であれば問題は無い。そうでない場合、URLを含めたパラメータのチェックを徹底する。

## 8. 意図しないリダイレクト

HTTPレスポンスの300番台やHTMLによるリダイレクトで、意図しないページ移動を行うこと。クロスサイト・スクリプティングの1手法として悪用される場合がある。

一般的な対策

クロスサイト・スクリプティングの対策に準ずる。

## 9. HTTPヘッダ・インジェクション

クロスサイト・スクリプティングの一種で、通信パラメータであるHTTPヘッダを不正に書き換えて、サーバーに不正な挙動を起こさせること。または、それを可能にしてしまうサイトの欠陥（脆弱性）のこと。

一般的な対策

クロスサイト・スクリプティングの対策に準ずる。

## 10. 認証

サーバーが、閲覧者に所定の操作をさせることで、ユーザーの特定、およびアクセスの正当性を確認する処理のこと。

この機能に問題があるとアカウントの乗っ取りが発生する可能性があり、アクセスとは比較にならないほど容易に情報漏洩などのIT事故を起こす危険がある。

一般的な対策

認証ページは必ずhttpsで公開し、認証情報を含む通信は必ずhttpsで行う。暗号化していないパスワードをデータベースに保存したり、メールで送信することを避ける。（メールで送信を行った場合、そのユーザーが次回アクセス時にパスワード変更を強要する等）

## 11.セッション管理の不備

セッションとは、ページを移動しても閲覧者が同じであることを把握するためのサーバーの機能。この機能に不備があると、閲覧者の個々の特定が怪しくなり、アカウントの乗っ取りなどの問題が起こる可能性がある。

例：ショッピングサイトにAさんがログインすると、たまたま同じタイミングでサイトアクセスしたBさんが何故かAさんのアカウントでログイン状態になってしまう。

## 12.認可制御の不備、欠落

認可制御（パーミッション）とは、各アカウントに権限を設け、閲覧可能な範囲と閲覧不能な範囲を策定する機能。

例：ショッピングサイトの買物客はログインしても管理画面にアクセスすることはできない。

この機能に不備があると、本来アクセスする権限の無い人が、アクセスしてはいけないページにアクセスできてしまう、ということが起こりうる。

## 13.クローラへの耐性

クローラとは、各サイトの情報を収集するための自動システム。Googleなどの検索エンジンでWeb検索するための情報を収集するクローラが最も一般的。クローラを適切に受け入れることはCSR的にも重要。

一般的な対策

近年では公開情報を根こそぎスクレイピングする悪質なクローラーもあり、同一サーバーからのアクセスを制限するなどの設定を行う。

## 脆弱性診断費用

**お見積り　　無料**
**診断費用　　１サービスあたり、40万円〜（税別）**

お気軽にご相談ください。

貴社・貴店のIT部門

# 株式会社ツチノコテクノロジー

住所：　509-1302
岐阜県加茂郡東白川村神土3131-2(本社)※ 従業員は在宅勤務です。
電話：　050-5371-8644
mail：　tt@tutinoko.tech (全社員共通メール)
LINE：　@tutinokotech ツチノコテック
URL:　https://tutinoko.tech

# 株式会社ツチノコテクノロジーのご紹介

## 合言葉は「貴社・貴店のIT部門」です。

「システム」って聞いただけで難しそうだと拒否反応！！！そんな方々にも、わかりやすく解説しながらITをうまく使った効率の良いビジネスをお手伝いをします。 社内にIT部門がある会社・店舗はごくまれです。わたしたちは、みなさんのIT部門になります！ぜひ、アウトソーシングをご検討ください！

私たちの作るシステムは、お客様の業務を自動化します。システムだからこそできる24時間365日の確実な作業。お客様が寝ている間も安心して業務をお任せください。私たちが作りだすのは、お客様が安らかに手を休められる「安心」です。

## 東京での実務経験(15年)による最先端の技術が強みです。

クレジットカード決済、権限管理、メールやCSVやプリンターの出力、各種SNSに対応できます。
子会社(株)RedoITの仕組みを利用して、大きなシステムも請け負うことができます。

《実務実績》　大企業の社内勤怠管理・給与・手当ての算出システム
特殊な現場で働く社員に対する出退勤の記録、給与・特別手当ての算出をおこなうシステムを制作・運用しています。 現在、全国40店舗でアルバイト・パートを含む社員数約1000人が、毎日利用しています。

## 料金は安心の月額定額制。業務の実態に合わせて作業内容をすぐに変更いたします。

長期のご契約はすべてラボ型契約 月額80万円/人です。月曜日から木曜日まで、お客様の売上向上、業務安定のためにシステムのあらゆる対応をいたします。

※ もしご依頼が1名分だとしても、必ず3人チームで対応させていただきます。一人の IT エンジニアに全部を管理させないチェック体制を作るためです。
※ 都度ご依頼のお客さまは、ご依頼内容のお見積もりをさせていただき、期間中の月額料金を提案させていただきます。