

安心してウェブサイトを運営するための WordPressセキュリティの基礎知識



自己紹介

- 久野 晃司 (岐阜県岐阜市在住)
- [オレインデザイン](#)
- フリーランス ウェブ制作者
- [WordPress コントリビューター](#)
- Snow Monkey/unitone
- [hook wp_ メンバー](#)
- [本、書きました \(TT4本\)](#)

最近、メルマガはじめました

アジェンダ

- 前提認識・知識
- WordPress セキュリティの考え方
- 入り口を固める
- WordPress 本体・テーマ・プラグインのアップデート
- 「アップデートしない」は無い
- バックアップという保険
- プラグインの活用
- ユーザー管理と権限設定
- セキュリティに対する意識向上
- まとめ

前提認識・知識

想定

- 一般的な WordPress の利用方法を想定
- WordPress.org（インストール型）を想定

WordPress とは

- コンテンツマネージメントシステム（CMS）の1つ
- グローバルシェアは約43%
- 日本国内シェアは82%以上

一般の皆さんの利用方法例

- 独自ドメイン利用、レンタルサーバーで稼働
- 専門家ではない個人（社内web担当者含む）が管理、または専門家に委託

システムであり、ソフトウェアである

- CMS:コンテンツを管理するシステム
- "WordPress is open source software."
 - 引用：[About – WordPress.org](#)

WordPress セキュリティの考え方

WordPress は自分の家

- 自分が責任を持って管理する
- 自分が責任を持って運営する
- 自分が責任を持って守る

守れなかつたら…

- 泥棒に入られる
- 何かを盗まれる
- 乗っ取られる
- 悪い人の拠点にされる
- 他の家に迷惑をかける

なぜセキュリティ対策をするのか

- 自身のウェブサイトの情報を守るため
- 自身のウェブサイトが他に悪影響を及ぼさないため

対策対象は大きく分けて2つ

- 入り口（ログイン画面）
- WordPress本体（コア）・テーマ・プラグイン

入り口を固める

一意のアカウント名

- ブルートフォース攻撃では一般的なユーザー名とパスワードの組み合わせ辞書を使用する
- `admin` は使わない
- ユーザー名は公開情報
- ユーザー名は推測されやすい

強力なパスワード

- 20文字以上
- 小文字と大文字を使用
- 数字を含む
- 特殊文字を含む !"#\$%&'()*)+, -./:; <=>?@[]^_{}|~
- 適切なパスワード例： As32!KoP43??@ZkI??L0d

絶対に避けるべきパスワード

- パートナーや子供、ペットの名前
- 会社名
- 好きなスポーツチームや車の名前
- 生まれた年
- あなたの誕生日

これらはすべて公開情報→簡単に推測される

WordPress で自動生成する



ダッシュボード

投稿

メディア

固定ページ

コメント

外観

プラグイン

ユーザー

ユーザー一覧

新規ユーザーを追加

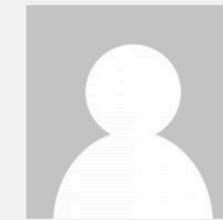
プロフィール

ツール

設定

メニューを閉じる

プロフィール写真

[Gravatar でプロフィール画像の変更が可能です。](#)

アカウント管理

新しいパスワード

[新しいパスワードを設定](#)

セッション

[他のすべての場所でログアウト](#)

この場所のみでログインしています。

アプリケーションパスワード

アプリケーションパスワードを使用すると、実際のパスワードを入力しなくても XML-RPC や REST API などの非対話型システムを介した認証が可能になります。アプリケーションパスワードは簡単に取り消すことができます。サイトへの従来のログインには使用できません。

新しいアプリケーションパスワード名

アプリケーションパスワードの作成に必要ですが、ユーザーの更新には不要です。

ブラウザのパスワードマネージャーを利用する

- Chrome, Safari, Firefox など主要ブラウザで利用可能
- パスワードを自動生成して保存をサポートしてくれる
- パスワードを覚える必要がない
- 共有する場合はアプリを利用する
 - [1Password](#) など色々とある

How Secure Is My Password?

 **The #1 Password Strength Tool. Trusted and used by millions.**

 ENTER PASSWORD

Entries are 100% secure and not stored in any way or shared with anyone. Period.

AS SEEN ON

The New York Times

THE VERGE

Entrepreneur

nerdwallet.

G

the bloodline of data and online security, but our research on the [password habits in the U.S.](#) shows that less than half of Americans are confident that their password is secure. Is your password secure? We built this password checker tool to help you find out, so try it out now!

Pro Tip: We recently rolled out a new [password generator](#) tool that will help you create super secure, unique passwords in a snap!

安心してウェブサイトを運営するためのWordPressセキュリティの基礎知識

2要素認証 (2FA:Two-Factor Authentication)

2つの異なる要素を使って認証する（以下のうち2つを組み合わせる）

1. 知識要素（パスワードやPIN）
2. 所持要素（スマホなど）
3. 生体要素（指紋や顔認証）

WordPress 本体・テーマ・プラグインの アップデート

アップデートとは

- 機能の追加
- バグの修正など

最適な状態を保つための取り組み



ホーム

更新 1

投稿

メディア

固定ページ

コメント

外観

プラグイン

ユーザー

ダッシュボーダー

安心してウェブサイトを運営するためのWordPressセキュリティの基礎知識

サイトヘルスステータス

まだ情報がありません...

アップデート対象

- WordPress本体（コア）
- テーマ
- プラグイン

概要

1件の投稿

1件のコメント

コアアップデートの種類

種類	主な内容	頻度	バージョン番号の変化
メジャーアップデート	新機能の追加、パフォーマンス向上など	年に3回（2023年の事例）	6.6 → 6.7
マイナーアップデート	バグ修正、セキュリティ修正など	不定期	6.6.1 → 6.6.2

アップデートを躊躇する理由

- 画面が真っ白になるかもしれない
 - エラーが出るかもしれない
 - 表示が崩れるかもしれない
-
- これらの情報を見聞き（または体験して）して恐る

アップデートをしなかったら？

- 脆弱性を抱えた状態で公開される可能性
- サイトが乗っ取られる可能性
- 踏み台にされる可能性（他への攻撃につながる）

僕がお勧めするアップデートに対する考え方は…

アップデートは可能な限り早期に実施する

- 画面が真っ白になつたら対処する
- エラーが出たら対処する
- 表示が崩れたら対処する

--

- 脆弱性を抱えて誰かに迷惑をかけてしまう or 表示が崩れる
- 見えにくい問題を抱える or 見える問題を抱える

どちらを選ぶ？

何かに対処することは運用の一部

- 日々の運用で改善を繰り返すのがウェブサイト運用
- 課題・問題→対処→効果測定などの繰り返し
- アップデートもその一貫だと考える

アップデートで問題が起きにくい作りを考える

- WordPressへの理解
- 見た目（テーマ）と機能（プラグイン）の分離
- 繼続的メンテナンスができない機能追加は慎重に検討する

「アップデートしない」は無い

テスト環境でアップデートを試す

1. 稼働ウェブサイトと全く同じものを壊れても良い環境に用意する
2. 実際にアップデートを行う
3. 管理画面や実際の表示に問題がないか確認する
4. 問題がなかったら or 問題を解決したら本番環境でアップデートを行う

自動アップデートを適切に活用する

例えば…

- WordPress マイナーアップデートは有効化する
- ユーザーから情報入力があるプラグインは有効化する
- 表示（フロント側）に影響がないプラグインは有効化する

などなど

..。「本業ではないので簡単に言わないでください」)

ウェブサイトの運用・運営は以下の3つに絞れる

- 自分で運用・運営する
- 専門家に委託する
- 適材適所で依頼・委託する

本業ではない方は、困った時に相談できる専門家を見つけておくと良いかも

バックアップという保険

バックアップは何か問題が起きた場合の重要な備え

- アップデートで問題が発生した場合に利用
- ハッキングされた場合のロールバックに利用
- その他、想定外の問題が発生した際に復元に利用

バックアップ取得の頻度

- ウェブサイトにより最適解が変わる
- ウェブサイトの更新頻度によって最適解を探る必要がある

バックアップ取得方法

- プラグインで行う（推奨）
 - [UpdraftPlus](#)
 - [BackWPup](#)
 - [All-in-One WP Migration](#) など
- 自身で手動で行う
 - データベースの書き出し
 - `/wp-content/` ディレクトリのコピーなど

意外と盲点！

バックアップからの復元方法の確認

- バックアップを取得するだけでなく、復元方法も確認しておく
- いざという時はトラブルが発生している状態
- そんな時にも適切に対応できるように準備しておく

プラグインの活用

よく聞くセキュリティ系プラグイン

- [Wordfence](#)
- [Sucuri Security](#)
- [XO Security](#)
- [SiteGuard WP Plugin](#)

などたくさんある

セキュリティ系プラグイン利用について（個人的な意見）

- プラグインを入れる前にやるべき対策があることを理解
- それらが完璧に対応された上での利用を推奨する
 - ログイン周りが弱いと総合的なセキュリティレベルを上げられません

「セキュリティ系プラグインを入れたから安心」という考え方は危険

サーバーのセキュリティ

SSLの導入

- インターネット通信の暗号化するセキュリティ機能
- SSL 証明書は上記の情報暗号化通信に加え、そのウェブサイトが信頼できるものであることを証明する
- 多くのレンタルサーバーで無料で導入・設定が可能
- SEO の観点からもメリットがある

サーバー内のファイル権限設定

- ファイルの読み書き権限を適切に設定する
- レンタルサーバーが用意する簡単 WordPress インストール機能を使っておけば問題ない

ユーザー管理と権限設定

ユーザーアカウントは一人につ

- ユーザーアカウントを複数人で共有しない
- 誰がいつどんな操作をしたのか特定できなくなる
- 一人がパスワードを変更した場合、他の人がログインできなくなる

必要最小限の権限を与える

- ユーザー毎に適切な権限を最小限で与える
- WordPress に詳しくない人には管理権限を普段使いさせない
 - 普段は最低限の権限を提供し、必要な場合のみ管理者権限を利用するなどの方法もあり

ユーザーの活動監視

- 各ユーザーの WordPress 内での活動内容を記録・監視する
- 問題が発生した場合に、実行者の特定と以後の改善方法共有などが可能になる

--

- [Simple History](#)
- [WP Activity Log](#)

セキュリティに対する意識向上

対策実行とアップデートの大切さを知る

- 自身の環境と照らし合わせて、必要な対策を速やかに実施する
- アップデートの重要性を理解し、適切なタイミングで実施する

セキュリティに関する情報を定期的にチェック

- 信頼できる情報源を見つける
- WordPress Meetup などのコミュニティに参加し情報収集する
- セキュリティに関する情報収集は立派な「保守」の一部

まとめ

- WordPress セキュリティは自身の家を守ることと同じ
- 基本的な点をしっかり対策する
- アップデートは実施する前提で WordPress を使う
- 情報収集を継続的に行う

おまけ

僕の基本セキュリティ対策

- パスワードを強固なものにする
- ログイン画面にひらがな画像認証を導入
- 1時間におけるログイン試行回数制限
- 二要素認証の導入
- コメント機能の無効化
- WordPress コアはマイナーアップデート自動化
- テーマ・プラグインは可能な限り自動アップデート有効化
- バックアップは毎日取得し、稼働サーバーとは別の場所に保存

参考資料一覧

- [Password Best Practices](#)
- [Updatiing WordPress](#)
- [Usage statistics and market share of WordPress](#)
- [Changing File Permissions – Advanced Administration Handbook](#)
- [サイバーセキュリティ初心者のための三原則](#)
- [安全なパスワードの設定・管理 | 国民のためのサイバーセキュリティサイト](#)
- [インターネットの安全・安心ハンドブック - NISC](#)