WordPress Meetup

はじめての
セキュリティプラグイン選び

Wordfence・SiteGuard・CloudSecure・XO Security
4つを比べて、自分のサイトに合うものを見つけよう

今日のゴール

1

セキュリティプラグインが「何から守るのか」がわかる

2

人気の4つのプラグインの違いが、ざっくりわかる

3

自分のサイトに合うものを選べるようになる

なぜ対策が必要なの？

WordPressは使っている人が多いぶん、攻撃する側からも狙われやすいソフトです。よくある被害はこの3つです。



パスワードの総当たり

ログイン画面で、パスワードを機械的に何千回も試される



古いプラグインの弱点

更新していないプラグインの「穴」をねらって侵入される



サイトの改ざん

悪いコードを仕込まれ、見に来た人にまで被害が広がる

守り方は大きく2種類



入口を固める

ログイン画面や管理画面に、悪い人が入れないようにする

家でいえば「玄関の鍵」



侵入に気づいて直す

怪しいファイルを見つけて、元の状態に戻す

家でいえば「防犯カメラと修理屋さん」

これだけ覚えればOK 用語ミニ辞典

用語	ひとことで言うと
ログイン試行の制限	何度もパスワードを間違えた相手を締め出す
ログインURL変更	ログイン画面の「住所」を変えて見つかりにくくする
2段階認証（2FA）	パスワードに加えて、スマホのコードでも本人確認
画像認証（CAPTCHA）	文字を読んで入力させ、ロボットでないか確かめる
WAF	怪しいアクセスを入口で止める「門番」
マルウェアスキャン	サイトの中に悪いファイルがないか点検する

今日比べる4つのプラグイン

Wordfence

世界でいちばん使われている多機能型

500万＋

開発：Defiant（米国）
料金：無料＋有料プラン

SiteGuard

国内の定番。ログインまわりをシンプルに

60万＋

開発：EGセキュアソリューションズ
料金：無料

CloudSecure

国産で機能が幅広い、2023年公開の新顔

10万＋

開発：エックスサーバー
料金：無料

XO Security

どのサーバーでも動きやすい軽量型

3万＋

開発：ishitaka 氏（個人）
料金：無料

大きな数字は有効インストール数（WordPress.org、2026年10月31日時点）

海外製 ・ 無料＋有料プラン

Wordfence Security

侵入を「防ぐ」だけでなく、「見つけて直す」までできる多機能型

得意なこと

- WAF（門番）で怪しいアクセスを遮断
- マルウェアスキャンと、改ざんされたファイルの修復
- 2段階認証とパスキー（無料版でも使える）
- 複数サイトをまとめて管理（Wordfence Central）

気をつけたいこと

- 無料版はWAFのルール更新が30日遅れ
- 機能が多く、設定項目も多い
- 海外製（画面は日本語に翻訳）

最新版 9.0.2 ・ 最終更新 2026-09-30

国産 ・ 無料

SiteGuard WP Plugin

有効化するだけで、ログイン画面と管理画面をしっかり守る

得意なこと

- ログインURLを自動で変更（新しいURLはメールで届く）
- 画像認証（ひらがなも選べる）
- 管理画面に入れる人をIPアドレスで制限
- フェールワンス：正しいパスワードでも1回目はわざと失敗させる

気をつけたいこと

- 2段階認証がない
- マルチサイトに非対応
- ログインURLが変わるので、チームに必ず共有

最新版 1.8.10 ・ 最終更新 2026-10-27

国産 ・ 無料

CloudSecure WP Security

国産で、2段階認証や簡易WAFまで1つでそろう

得意なこと

- 2段階認証（スマホアプリ／メール）
- シンプルWAFで、よくある攻撃を遮断
- サーバーエラー（500エラー）をメールで通知
- 各機能はオン／オフを切り替えるだけ

気をつけたいこと

- 2023年公開と新しく、レビューはまだ少ない
- Apacheサーバーが前提（Nginxは公式対応外）
- マルチサイトに非対応

最新版 1.4.18 ・ 最終更新 2026-10-14

国産 ・ 無料

XO Security

サーバーの設定ファイルを書き換えないので、どこでも動きやすい

得意なこと

- Nginx・LiteSpeedなど、いろいろなサーバーで動く
- ほかのプラグインとぶつかりにくい
- ユーザー名が外に漏れない工夫が細かい
- WooCommerceのログイン保護、メンテナンスモードも

気をつけたいこと

- 個人が開発しているプラグイン
- WAF、管理画面のIP制限、更新通知はない

最新版 3.11.0 ・ 最終更新 2026-07-19

機能をざっくり比べると

機能	Wordfence	SiteGuard	CloudSecure	XO Security
WAF（門番）	◎	×	○	×
マルウェアスキャン	◎	×	×	×
ログイン試行の制限	○	○	○	○
ログインURL変更	×	○	○	○
2段階認証	◎	×	○	○
画像認証	○	○	○	○
管理画面のIP制限	△	○	○	×
更新のお知らせ	△	○	○	×
マルチサイト	◎	×	×	△

◎ 特に強い　○ ある　△ 一部だけ・別の方法で代用　× ない

いちばん大きな違い

Wordfenceだけが「侵入されたあと」まで面倒を見てくれる

国産の3つは「入口を固める」タイプ。
侵入に気づいたり、元に戻したりする機能はありません。

こんなサイトなら、これ

ECサイト・会員サイト、複数のサイトを運用している	→ **Wordfence**
国産でシンプルに。2段階認証やWAFも1つで済ませたい	→ **CloudSecure**
Nginx・LiteSpeedのサーバー、ほかのプラグインと共存させたい	→ **XO Security**
サーバーにSiteGuardのWAFが入っている、管理画面の制限を重視	→ **SiteGuard**

注意 その1

同じ機能を、2つのプラグインでオンにしない

たとえば「ログインURL変更」を両方でオンにすると…

- ログインURLが2つできてしまう
- ログイン画面が開かなくなる

こうすれば安心

重なる機能は、どちらか**片方だけ**で有効にする

出典：SiteGuard WP Plugin 公式サイトの注意事項

注意 その2

どれを使っても「最新版」が前提

この1年で、4つとも「ログインまわり」のセキュリティ修正を出しています。

SiteGuard
ログインURL保護やXSSの修正

CloudSecure
2段階認証をすり抜けられる問題を修正

XO Security
2段階認証をすり抜けられる問題を修正

Wordfence
2段階認証の流れを強化

プラグインと一緒にやっておきたい3つ

こまめに更新

WordPress本体・テーマ・プラグインを最新に保つ

強いパスワード

使い回さない長いパスワードと、2段階認証を組み合わせる

バックアップ

もしものときに戻せるよう、定期的に保存しておく

まとめ

- ✓ 守り方は「入口を固める」と「侵入に気づいて直す」の2種類
- ✓ 侵入後まで見たいならWordfence、入口をシンプルに固めるなら国産3つ
- ✓ サーバーの種類と、ほかのプラグインとの機能の重なりを確認する
- ✓ どれを選んでも、最新版に保つことがいちばん大事

出典：WordPress.org プラグインページ、各プラグイン公式サイト（2026年10月31日調査）