WEBSITE SECURITY SELF CHECK｜2026年11月版

ホームページ
脆弱性セルフ診断シート

30項目で、自社のサイトの守りの弱いところが分かる。
二段階認証など「今日できる対策10」つき。

全30項目・60点満点　専門知識がなくても答えられる　今日できる対策10

30 チェック項目　**10** 今日できる対策　**6** 分野

株式会社仁頼　jinrai.co.jp

INTRODUCTION

なぜ今、ホームページの守りを見直すのか

2026年の秋は、ホームページを動かすソフトに、重大な脆弱性（セキュリティの弱点）が続けて見つかりました。

2026年10月21日	WordPressなどを動かすPHPに、重大な脆弱性2件（通称PHP2Shell）。深刻度はCVSS v4.0で9.2。IPAが10月22日に注意喚起を出し、米国CISAは10月26日、実際の攻撃に使われた脆弱性の一覧に加えました。
2026年11月19日	PHPが脆弱性17件を修正（8.5.13・8.4.28・8.3.37・8.2.36）。公開された説明のうち、深刻度が最も高い「Critical」は3件。同じ日に、IPAはWebサーバーのソフト「nginx」の脆弱性についても注意喚起を出しています。

こうした脆弱性の多くは、サーバー会社や制作会社が対応します。一方で、**二段階認証、パスワード、使っていないアカウントの削除、バックアップ**のように、サイトの持ち主にしかできない対策もあります。この診断シートは、その両方を30項目で確かめられるように作りました。

> **この診断シートについて**
>
> 専門の「脆弱性診断」（専門家がプログラムや設定を検査するサービス）の代わりではありません。サイトの持ち主が、自分で確かめられる範囲の点検です。会員情報・決済を扱うサイトや、独自に開発したシステムは、専門の診断もあわせて検討してください。攻撃の方法は書いていません。

HOW TO USE

使い方

1	各項目に、○（**できている**）＝**2点**、△（**一部できている・分からない**）＝**1点**、×（**できていない**）＝**0点**をつけます。
2	分野ごとに小計を出し、合計点（60点満点）を出します。分からない項目は△にして、担当者（制作会社・サーバー会社）に確かめます。
3	最後のページの「点数の目安」で、次にやることを確かめます。×の項目は、「今日できる対策10」から手をつけます。

CHECK LIST 01–10

A ログインとアカウント

乗っ取りを防ぐ、いちばん効果の大きい対策です。

01 **WordPressの管理者アカウントに、二段階認証（2FA）を設定している**
パスワードのほかに、スマホのアプリなどで表示される確認コードを求める仕組み。パスワードが漏れても、それだけではログインされません。

02 **レンタルサーバーの管理画面、ドメインの管理画面、Googleアカウントにも二段階認証を設定している**
サイトの外側の管理画面が乗っ取られると、WordPressの対策は意味をなくします。サイトに関わるすべてのログインが対象です。

03 **パスワードは推測されにくく、ほかのサービスと使い回していない**
パスワード管理のアプリを使うと、長く複雑なパスワードを無理なく使い分けられます。

04 **使っていない管理者アカウント（退職者・制作会社の旧担当など）を削除している**
「誰が使っているか分からないアカウント」は、気づかないうちに悪用される入口になります。

05 **アカウントは一人ひとつで、必要以上に強い権限を与えていない**
記事を書くだけの人は「編集者」や「投稿者」に。全員を管理者にしないことで、被害の範囲を小さくできます。

Aの小計（10点満点）＿＿＿＿ 点

B ソフトウェアの更新

脆弱性の多くは、更新するだけで直ります。

06 **WordPress本体を、最新の版に更新している**
管理画面の「ダッシュボード」→「更新」で確認できます。

07 **プラグインとテーマを最新にし、使っていないものは削除している**
停止しているだけのプラグインも、ファイルが残っていれば狙われることがあります。

08 **サーバーのPHPが、サポート中の版（8.2〜8.5）になっている**
PHP 8.1以前はサポートが終わり、修正版が出ません。8.2も2026年12月31日でセキュリティ修正が終わります。WordPressの「ツール」→「サイトヘルス」→「情報」→「サーバー」で確認できます。

09 **サーバー会社のお知らせ（脆弱性への対応・メンテナンス）を受け取れるようにしている**
共用のレンタルサーバーでは、PHPやWebサーバーの更新はサーバー会社が行います。対応の状況は、お知らせで確認します。

10 **更新の担当者が決まっている（社内か、制作会社・保守会社か）**
「誰かがやっているはず」が、いちばん危険です。保守の契約に更新が含まれているかも確認します。

Bの小計（10点満点）＿＿＿＿ 点

C サーバーと通信

外から見える部分を、必要最小限にします。

11 **サイト全体がHTTPS（鍵マーク）で表示され、http:// で開いても https:// に切り替わる**
証明書の期限切れにも注意します。多くのレンタルサーバーには自動更新の機能があります。

12 **サーバー会社が提供するWAF（Webアプリケーションファイアウォール）を有効にしている**
不正な通信を入口で止める仕組みです。管理画面で有効・無効を切り替えられることが多く、無料で使える場合もあります。

13 **公開しているフォルダに、バックアップのファイルや古いサイト、設定ファイルの写しを置いていない**
「一時的に置いたまま」のファイルから、情報が漏れることがあります。

14 **本番のサイトで、エラーの詳細を画面に表示していない**
開発用の設定（WordPressのデバッグ表示など）が本番で有効のままだと、サーバーの内部の情報が見えてしまいます。

15 **WordPressの管理画面から、テーマやプラグインのファイルを直接編集できないようにしている**
乗っ取られたときに、プログラムを書き換えられる被害を防げます（wp-config.php の設定で無効にできます）。

Cの小計（10点満点） ＿＿＿＿ 点

D フォームと外部サービス

問い合わせと、外部の仕組みとのつなぎ目を守ります。

16 **問い合わせフォームに、迷惑な送信への対策がある**
自動で送られてくる大量の送信は、通知メールの見落としや、配信の停止につながります。

17 **問い合わせフォームや資料請求のフォームを、月に1回はテスト送信して、通知が届くことを確かめている**
フォームは、壊れても画面上は普通に見えることがあります。気づかないまま、問い合わせを取りこぼす原因になります。

18 **APIキーやパスワードを、ページの中（HTMLやJavaScript）に書いていない**
ページの中に書いた値は、誰でも見ることができます。メール配信や地図などのサービスのキーは、サーバー側で管理します。

19 **サイトに入れている外部のタグ（解析・広告・チャットなど）を把握し、不要なものを外している**
使っていないタグも、外部のプログラムを読み込む入口になります。

20 **プラグインやテーマは、公式の配布元や信頼できる開発元からだけ入れている**
有料のものを無料で配っているような配布物には、不正なプログラムが仕込まれていることがあります。

Dの小計（10点満点） ＿＿＿＿ 点

E バックアップと復旧

「戻せる」状態にしておくことが、最後の備えです。

21 **ファイルとデータベースの両方を、自動でバックアップしている**
サーバー会社の自動バックアップの範囲（何日分か、データベースも含むか）を確認します。
○ □ △ □ × □

22 **バックアップを、サイトと同じサーバー以外の場所にも保管している**
サーバーごと被害を受けた場合にも、戻せるようにするためです。
○ □ △ □ × □

23 **バックアップから戻す手順を、一度は試したことがある**
取っているだけで、戻せないバックアップは少なくありません。
○ □ △ □ × □

24 **数週間前までさかのぼって戻せる（複数の世代を残している）**
改ざんに気づくのが遅れると、直近のバックアップも汚れていることがあります。
○ □ △ □ × □

25 **戻すときに、誰が何をするか（サーバー会社への連絡を含む）を決めている**
緊急のときに、手順を調べるところから始めずに済みます。
○ □ △ □ × □

Eの小計（10点満点）＿＿＿＿点

F 監視と体制

早く気づき、迷わず動けるようにします。

26 **ファイルの改ざんや、不審なファイルを検知する仕組みがある**
セキュリティのプラグインや、サーバー会社の検知の機能を使います。
○ □ △ □ × □

27 **管理画面へのログインの記録（いつ・誰が）を確認できる**
身に覚えのないログインに気づくための備えです。
○ □ △ □ × □

28 **IPA（情報処理推進機構）やJPCERT/CCの注意喚起を、確認する担当がいる**
重大な脆弱性は、これらの機関が日本語で注意を呼びかけます。
○ □ △ □ × □

29 **緊急時の連絡先（社内の責任者、制作会社、サーバー会社）を一覧にしている**
夜間や休日でも連絡がつくかを、あわせて確認します。
○ □ △ □ × □

30 **サイトを一時的に止める基準と、再開する基準を決めている**
止めるかどうかで迷う時間が、被害を広げることがあります。
○ □ △ □ × □

Fの小計（10点満点）＿＿＿＿点

QUICK WINS

今日できる対策10

専門知識がなくても、今日中に進められるものを、効果の大きい順に並べました。右の時間は、作業のおおよその目安です。

- [ ] **1. WordPressの管理者に二段階認証を設定する** — 30分
  公式のプラグイン配布サイトにある二段階認証のプラグインを使うのが一般的です。①バックアップを取る、②プラグインを入れる、③管理者が一人ずつ、スマホの認証アプリで登録する、④予備のコード（バックアップコード）を安全な場所に保管する、⑤全員の設定が済んだかを確認する、の順に進めます。

- [ ] **2. サーバー・ドメイン・Googleアカウントに二段階認証を設定する** — 各10分
  各サービスの管理画面の「セキュリティ」や「アカウント設定」から設定できます。会社で共有しているアカウントは、誰の端末で認証するかを決めておきます。

- [ ] **3. 使い回しているパスワードを変える** — 20分
  管理者のパスワードから先に変えます。パスワード管理のアプリを使うと、変えたあとも困りません。

- [ ] **4. 使っていないアカウントを削除する** — 10分
  WordPressの「ユーザー」の一覧で、退職者や旧担当者のアカウントを削除します。投稿は別のユーザーに引き継げます。

- [ ] **5. WordPress・プラグイン・テーマを更新する** — 30分
  先にバックアップを取ります。更新のあと、トップページ、問い合わせフォーム、管理画面へのログインを確認します。使っていないプラグインは削除します。

- [ ] **6. PHPの版を確かめる** — 5分
  「ツール」→「サイトヘルス」→「情報」→「サーバー」で確認します。8.1以前なら、移行の計画を立てます。

- [ ] **7. バックアップの有無と、保管期間を確かめる** — 10分
  サーバー会社の管理画面で、自動バックアップの設定と、何日分を戻せるかを確認します。

- [ ] **8. サーバー会社のお知らせを受け取れるようにする** — 5分
  登録しているメールアドレスが、いまも読まれているかを確認します。

- [ ] **9. 問い合わせフォームをテスト送信する** — 10分
  自分のアドレスで送り、通知メールと自動返信が届くかを確かめます。資料請求のフォームがあれば、それも確かめます。

- [ ] **10. 緊急時の連絡先を1枚にまとめる** — 20分
  社内の責任者、制作会社、サーバー会社の連絡先と、契約の内容（保守に何が含まれるか）を書き出します。

RESULT

点数の目安と、次にやること

合計点（60点満点）　　A＿＿＋B＿＿＋C＿＿＋D＿＿＋E＿＿＋F＿＿＝＿＿＿＿**点**

50〜60点	**守りの基本はできています。**△の項目を担当者と確かめ、半年に1回、この診断をやり直してください。会員情報や決済を扱う場合は、専門の脆弱性診断も検討します。
35〜49点	**弱いところがあります。**×の項目のうち、A（ログインとアカウント）とB（ソフトウェアの更新）を先に直します。この2つは、乗っ取りと脆弱性の悪用に直結します。
0〜34点	**早めの対応が必要です。**まず「今日できる対策10」を上から進めてください。更新の担当者がいない場合は、保守を任せられる相手を決めることが先決です。

分野ごとの小計が4点以下なら

合計点が高くても、その分野は優先して見直します。たとえばE（バックアップと復旧）が弱いと、ほかの対策が破られたときに元に戻せません。

「うちの場合はどこから？」をご相談ください

株式会社仁頼は、WordPressサイトの制作・改善と、検索・AI検索からの集客を支援しています。この診断シートの結果をもとに、二段階認証の設定、PHPやプラグインの更新、バックアップの確認、サーバー会社への確認、更新のあとの動作確認まで、サイトの状況に合わせてお手伝いします。

電話　080-4416-5161（平日10:00〜18:00）

フォーム　https://jinrai.co.jp/contact/ （1営業日以内に返信します）

相談・見積もりは無料です。営業電話やしつこい勧誘はしません。

REFERENCES

出典

- PHP「Supported Versions」（2026年11月19日確認）
  https://www.php.net/supported-versions.php
- PHP「News Archive 2026」（2026年10月21日・11月19日のセキュリティリリース）
  https://www.php.net/archive/2026.php
- IPA「PHPの脆弱性対策について(CVE-2026-109618、CVE-2026-109619：PHP2shell)」（2026年10月22日）
  https://www.ipa.go.jp/security/security-alert/2026/alert20261022.html
- CISA「CISA Adds Two Known Exploited Vulnerabilities to Catalog」（2026年10月26日）
  https://www.cisa.gov/news-events/alerts/2026/10/26/cisa-adds-two-known-exploited-vulnerabilities-catalog
- IPA「NGINXの複数の脆弱性対策について（CVE-2026-123007、CVE-2026-123633等）」（2026年11月19日）
  https://www.ipa.go.jp/security/security-alert/2026/alert20261119.html
- php-src「Security Advisories」（2026年11月19日公開分）
  https://github.com/php/php-src/security/advisories

本資料は2026年11月20日時点の公開情報にもとづいて作成しています。ソフトウェアのサポート期間や、各サービスの画面・機能は変わることがあります。作業の前に、公式の情報と、お使いのサーバー会社・制作会社の案内をご確認ください。本資料の内容を実施したことによる損害について、弊社は責任を負いかねます。

発行：株式会社仁頼（神奈川県横浜市）｜https://jinrai.co.jp

関連記事：PHPの脆弱性17件を修正｜8.5.13・8.4.28・8.3.37・8.2.36の内容と対応
https://jinrai.co.jp/blog/2026/11/19/php-security-release-2026-11/