選ばれ続ける制作会社の鉄則！顧客サイトのセキュリティ強化16のコツ

Kinsta

クライアントサイトの保護は最優先事項

仕事で顧客のウェブサイトを扱う人にとって、最優先事項とも言えるのが顧客サイトのセキュリティ。セキュリティを怠れば、顧客の信頼を失い、ビジネスの評判に傷をつけ、結果として収益に打撃を与えます。大切な顧客のウェブサイトは、あらゆる策を講じて徹底的に保護する必要があります。本電子書籍では、セキュリティこだわるKinstaの経験に基づいた、セキュリティ対策を一挙ご紹介します。参考になりましたら幸いです。

業界トップクラスのセキュリティを誇るKinstaのノウハウ

Kinstaは、セキュリティに徹底的にこだわります。積極的かつ受動的な対策により、57億もの悪意のあるリクエストを自動処理。毎月90以上のDDoS攻撃を緩和しています。お客様に安心してサービスをご利用いただけるよう、独立した第三者機関による弊社のセキュリティ慣行の監査を実施。米国公認会計士協会によって考案されたSOC2報告書（Service Organization Control Type 2）を受領し、 国際的なデータセキュリティおよびプライバシー管理に関するISO/IEC認証（ISO 27001、ISO 27017、ISO 27018）も取得。GDPRおよびCCPRのプライバシー基準にも準拠しています。

目次

第1章

セキュアな WordPress サーバーに投資する

顧客のWordPressサイトをサーバーレベルで保護することは非常に重要です。クライアントサイトを託すサーバーの選定は、慎重に行わなければなりません。

自前の仮想専用サーバー（VPS）でWordPressサイトをホスティングするには、技術的な専門知識が求められます。月額20ドル程度を削減するために、自分がシステム管理者（通称シスアド）になってサーバーを管理するのは、賢い判断とは言えません。

サーバーの強化は、安全なWordPress環境の確保に欠かせません。サーバーのインフラストラクチャが物理的、そして仮想的にサイバー攻撃に太刀打ちできるよう、ハードウェアやソフトウェアレベルのセキュリティ強化策を複数の防御層で確立することが重要です。

最新のオペレーティングシステムとセキュリティソフトウェアを使用し、脆弱性とマルウェアを徹底的にテスト・スキャンしてくれるWordPress専用サーバーを利用することを強くお勧めします。

また、WordPressサイトの構築過程であっても、クライアントサイトをしっかりと保護するには、サーバーレベルのファイアウォールと侵入検知システムが必要です。

コンテンツを保護し、サイトのパフォーマンスを最適に保つためには、インストールされているすべてのソフトウェアが最新のデータベース管理システムと互換性があることも重要です。さらに、安全なネットワークとSFTP（FTPは安全性に欠ける）を使用し、悪意のある侵入者から機密データを守ることも必要です。

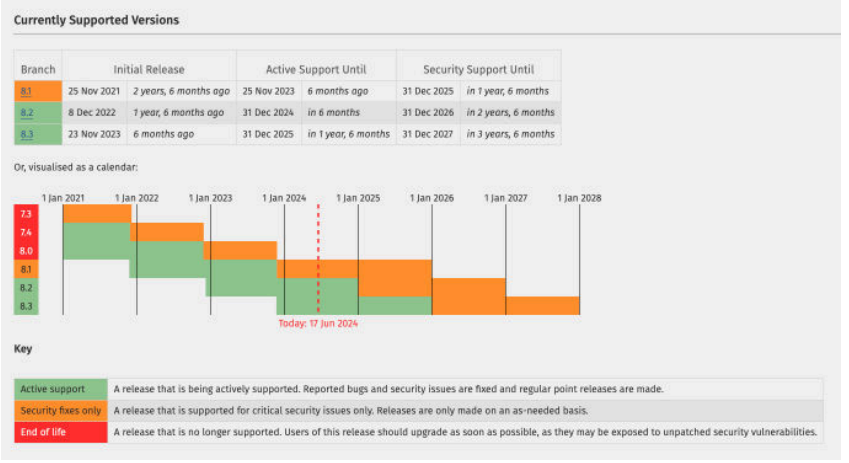
セキュアなWordPress専用マネージドクラウドサーバーを提供するKinstaでは、すべてのプランにGoogle Cloudの最速サーバー（C2およびC3D）およびプレミアムティアネットワークのみを採用。プロビジョニングの整った低遅延Googleグローバルネットワーク上でトラフィックを配信することにより、データの安全な伝送を保証しています。また、ファイル転送プロトコルには、安全性を考慮しSFTPのみをサポート。さらに、コンテナ技術によりすべてのサイトが100%隔離されたコンテナで実行されます。Kinstaのセキュリティに関する詳細はこちらをご覧ください。

第2章

最新のPHPバージョンを使用する

PHPはWordPressサイトの中核となる技術。クライアントサイトで常に最新バージョンのPHPを使用することが大切です。PHPの各メジャーリリースは、通常リリース後、2年間サポートされます。

その間、バグとセキュリティに関する問題が継続的に修正され、パッチが適用されます。2023年11月にはPHP 8.0のセキュリティサポートが終了しており、これは8.0以下のバージョンにはセキュリティ修正やパッチが提供されず、脆弱性にさらされている可能性があることを意味します。



Currently Supported Versions

Branch	Initial Release		Active Support Until		Security Support Until	
8.1	25 Nov 2021	*2 years, 6 months ago*	25 Nov 2023	*6 months ago*	31 Dec 2025	*in 1 year, 6 months*
8.2	8 Dec 2022	*1 year, 6 months ago*	31 Dec 2024	*in 6 months*	31 Dec 2026	*in 2 years, 6 months*
8.3	23 Nov 2023	*6 months ago*	31 Dec 2025	*in 1 year, 6 months*	31 Dec 2027	*in 3 years, 6 months*

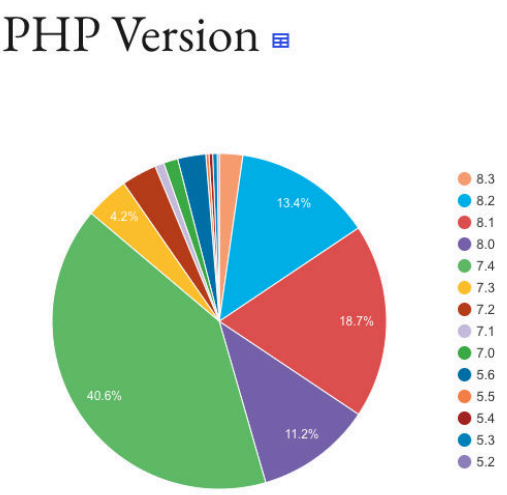
Or, visualised as a calendar:

Key

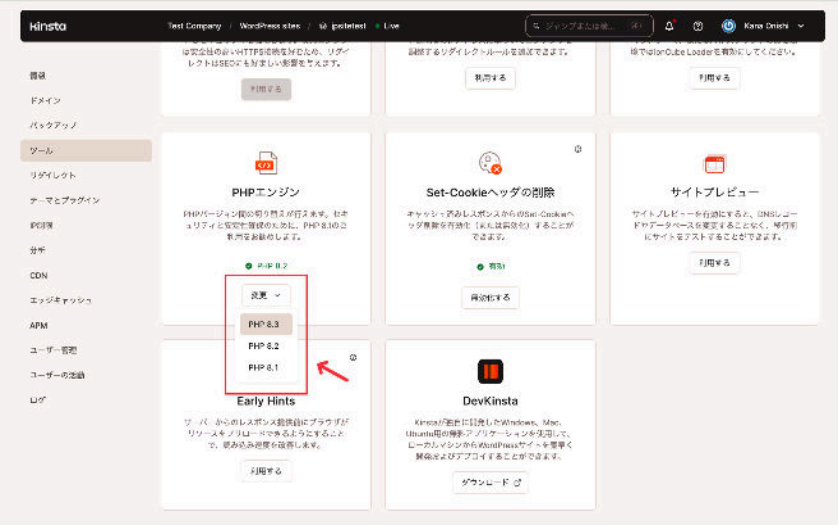
Active support	A release that is being actively supported. Reported bugs and security issues are fixed and regular point releases are made.
Security fixes only	A release that is supported for critical security issues only. Releases are only made on an as-needed basis.
End of life	A release that is no longer supported. Users of this release should upgrade as soon as possible, as they may be exposed to unpatched security vulnerabilities.

現在サポートされているPHPバージョン（2024.06）

WordPressの公式統計ページによると、半数以上のWordPressユーザーがいまだにPHP 8.0以下を使用している現状（最も使用されているのは、2024年6月現在PHP 7.4で40.60%）。半数以上のWordPressサイトでサポートの終了したPHPを使用しているというのは由々しき事態です。



Kinstaでは現在（最終更新日：2024年7月）、PHP 8.0、8.1、8.2、および8.3をサポート（切り替え選択可能なのは安全性を考慮し8.1以降のみ）しており、常に最新バージョンの使用を推奨しています。PHPのバージョンは、専用コントロールパネル「MyKinsta」からワンクリックで変更可能です。多数のクライアントサイトを抱えている場合も、一括操作機能で一度に変更することができるため非常に効率的です。



MyKinstaのツール画面

第3章

強力なユーザー名とパスワード

WordPressのセキュリティを強化する効果的な対策の1つは、強力なユーザー名とパスワードを使用することです。これは一見かなり初歩的なヒントに思えますが、SplashDataの調査によると、最もよく使われているパスワードは以下のようなものです。

- 123456
- 1234567
- 111111
- 123456789
- 12345678
- 123123
- qwerty
- 12345
- password
- iloveyou

未だかつてないほどセキュリティが重要視されている2024年の現在でも、最も使用されているパスワードは「123456」であるから驚きです。これを踏まえ、KinstaではWordPressのインストール後、管理画面へのログインで強力なユーザー名とパスワードの設定を強制しています。

WordPressのwp_hash_password関数は、パスワードのハッシュ化においてphpassというライブラリを使用しています。また、顧客のWordPressサイトではユーザー名の「admin」をそのまま使用することは避け、管理者

アカウントとして一意のWordPressユーザー名を必ず作成するようにしてください。

また、クライアントサイトごとに異なるパスワードを設定することも重要です。各パスワードは、暗号化したローカルのデータベースに保存してください。あるいは、無料でオープンソースのパスワードマネージャーであるKeePass、1PasswordやLastPassなどのオンラインパスワードマネージャーを使用することもできます。

第4章

WordPressコア プラグインとテーマは 常に最新の状態に

クライアントサイトのセキュリティを強化するもう1つの重要なヒントは、WordPressコア、プラグイン、そしてテーマを常に最新の状態に保つことです。更新はセキュリティ強化の鍵。通常、更新がリリースされるたびにセキュリティが強化され、バグの修正が行われています。

しかしながら、世界中で何百万もの企業が古いバージョンのWordPressソフトウェアやプラグインを使用しています。「サイトが壊れる」「コアに施した変更が消えてしまう」「特定の機能が使えなくなる」「新機能は特に求めていない」などの理由から、多くの企業が更新を後回しにしているのが現状です。

ウェブサイトが壊れる大きな原因は、古いバージョンのWordPressのバグにあります。また、WordPressチームやそのリスクを理解する開発者は、WordPressコアに触接手を加えることはそもそも推奨していません。WordPressの更新には、最新のプラグインを実行するのに必要な機能とともに、必須のセキュリティパッチも含まれています。

astra社の調べによると、WordPressサイトの脆弱性の52%は更新されていない古いプラグインが原因です。そのため、プラグインを常に最新の状態に保つことで、攻撃の標的になるリスクを抑えることができます。

クライアントサイトには、多くのユーザーに評価され信頼できるプラグインのみを使用してください。WordPressプラグインディレクトリの「Featured plugins」（注目）カテゴリや「Popular plugins」（人気）カテゴリから必要なプラグインを探すのが堅実です。あるいは、プラグイン開発者のサイトから直接ダウンロードすることもできます。無断で配布されているプラグインとテーマの使用は控えてください。

VirusTotalなどのオンラインツールを使用して、プラグインやテーマのファイルをスキャンし、マルウェアが検出されるかどうかを確認するのもおすすめです。

VirusTotal

また、WordPressの公式セキュリティアーカイブやWPScan Vulnerability DatabaseなどでWordPressの最新セキュリティアップデートや脆弱性の追跡を行うことも可能です。

（Kinstaは）セキュリティが高いのでとても安心できています。専門性が求められるため、 その面を担ってくれるのが非常に大きいです。弊社のように管理をする立場になると、セキュリティのリスクを背負うことになります。Kinstaにしてからは、WordPressで何か脆弱性の発表があった時にはすぐメールが来ますし、そのあたりの対応が早いことがわかります。それに対してのこちらでのリカバリーとかもすぐに対応できるので、Kinstaのセキュリティというのは選ぶ第一の理由になりますね。

奥田浩一 様
株式会社文化工房

導入事例を読む

第5章

WordPressのログイン画面を保護する

ログイン画面などの「守りを固める」ことも、オンラインビジネスやWordPressサイトにとって効果的なセキュリティ戦略です。ハッカーによるバックドアの設置を困難にすれば、攻撃を受けるリスクを減らすことができます。クライアントサイトのログイン画面を保護するには、デフォルトのログインURL「/wp-admin」を変更し、ログインの試行回数を制限することが重要です。

WordPressログインURLを変更する方法

WordPressサイトのログインURLは、デフォルトで「domain.com/wp-admin」と決まっており、悪質なボットやスクリプト、ハッカーも把握済み。URLを変更することで、不正ログインを困難にし、ブルートフォース攻撃からサイトを守ることができます。万能の解決策というわけではありませんが、セキュリティを強化する「小技」として機能します。

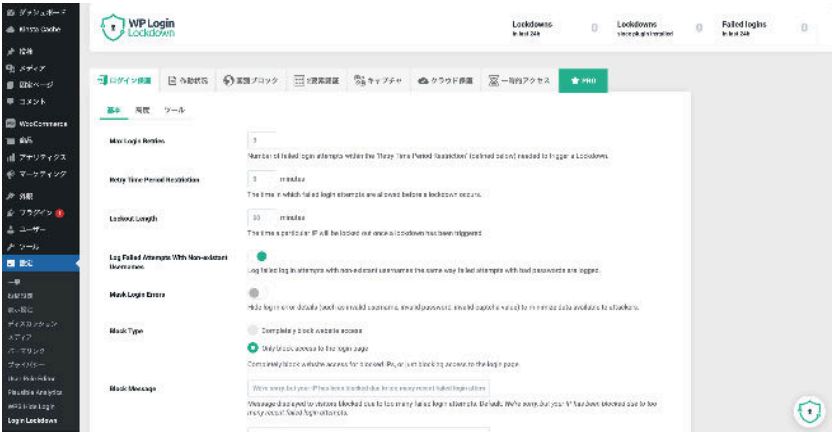
WordPressのログインURLを変更するには、無料のWPS Hide Loginプラグインが便利です。ボットまたはスクリプトの攻撃対象リストに含まれていないような一意のURLに変更してください。

WPS Hide Loginプラグインの設定画面

ログイン試行回数を制限する方法

ログインURLを変更することで、不正なログインの試行を防ぐことができますが、試行回数にログインを設けることも非常に効果的です。無料のLimit Login Attempts Reloaded、またはLogin Lockdownプラグインを使用すると、ログイン再試行を制限する期間やログイン試行回数の上限を簡単に設定することができます。

たとえばLogin LockDownは、失敗したすべてのログインのIPアドレスとタイムスタンプを記録し、同じIPの範囲から一定の回数を超える試行が短期間に検出されると、その範囲からの要求に対しログイン機能が無効になります。また、WPS Hide Loginプラグインとも互換性があります。



Login Lockdownの設定画面

Kinstaのプラットフォームでは、セキュリティ上の理由からデフォルトでログイン試行回数に制限がかかり、不正の疑われるログイン試行が自動的にブロックされます。したがって、Kinstaをご利用の場合は、別途プラグインをインストールする必要はありません。

Basic認証（htpasswd保護）を追加する方法

また別の方法として、HTTPが定義するBasic認証を追加することも効果的です。これは、WordPressのログインページにアクセスする前にユーザー名とパスワードを要求する認証方式です。

注）ボットによるアクセスを非常に効果的に防ぐことができますが、ECサイトや会員制サイトでは使用を控えてください。

Kinstaでクライアントサイトをホスティングする場合は、MyKinstaのパスワード保護（htpasswd）機能を使用することができます。手順はサイトの「ツール」画面にある「パスワード保護」の「利用する」をクリックし、ユーザー名とパスワードを入力するだけと非常にシンプルです。

Basic認証を追加すると、WordPressサイトにアクセスするたびに認証が必要になります。ログイン情報はいつでも変更可能で、不要になれば無効にすることができます。

第6章

二要素認証を使用する

二要素認証（2FA）を利用するとログインプロセスが2段階になります。パスワードに加えて、スマホの認証アプリ（Authenticatorなど）や電話番号など別の認証要素が必要になることで、WordPressサイトへのブルートフォース攻撃を効果的に阻止することができます。

クライアントサイトを扱う際には、以下2つのプラットフォームで二要素認証を設定することを心がけてください。

1つ目は、利用しているサーバーのアカウントやコントロールパネル。悪意のあるユーザーがアカウントに侵入すると、クライアントサイトのパスワードの変更、サイトの削除、DNSレコードの変更など、最悪の事態が起こりかねません。たとえば、Kinstaのコントロールパネル「MyKinsta」では、Authenticatorベースの二要素認証をワンクリックで有効にすることができます。

Authenticatorベースの二要素認証は、携帯電話番号に紐付けられないため、従来のSMS認証よりも安全です。また、SIM入れ替えによるアクセス手法にも耐性があります。

また、1Passwordなどのパスワードマネージャーアプリと併用すると、自分自身もより効率的に二要素認証を行うことができます。二要素認証情報

をパスワードマネージャーに追加すると、MyKinstaへのログインに別のデバイスを使用する必要がなくなります。使い方も簡単です。

2つ目は、顧客のWordPressサイトの管理画面です。WordPressサイトで二要素認証を実装するには、以下のプラグインがおすすめです。

- Duo Two-Factor Authentication
- Google Authenticator
- Two Factor Authentication

いずれかのプラグインをインストールして設定すると、WordPressのログインページにセキュリティコードを入力するためのフィールドが表示されるようになります。例えばDuo Two-Factor Authenticationであれば、最初にアカウント情報を使ってログインし、プッシュ、通話、パスコードなどの中から任意の認証方法を選択します。

第7章

HTTPSで接続を暗号化する

WordPressサイトのセキュリティ強化策として見落とされがちなものに、SSL証明書を用いたHTTPS接続があります。HTTPS（Hypertext Transfer Protocol Secure）は、ブラウザやウェブアプリケーションによるサイトへの安全な接続を保証する技術です。クレジットカード情報のような機密データを扱わないサイトでも、今日SSL証明書の導入は欠かせません。

オンラインストア以外もHTTPSが重要になる理由をいくつかご紹介します。多くのサーバーでは、Let's Encryptの無料SSL証明書を利用でき、Kinstaでは、Cloudflareのワイルドカード対応SSL証明書をすべてのプランで無料にて提供しています。

HTTPSが重要な理由

1. **セキュリティの強化**—クライアントのログイン情報が機密データであることは言うまでもありません。ログイン情報は、ユーザーがログインするたびにプレーンテキスト（平文）でそのままサーバーに渡されます。HTTPSは、サイトとブラウザ間の安全な接続を確立し、データの送受信を暗号化してくれるため、ハッカーや部外者から大切な情報を保護することができます。

2. **SEO**—HTTPSは、Googleが検索結果の表示順位を決定する要因の一つです。検索エンジン最適化（SEO）や検索エンジン結果ページ（SERP）の面から競合他社サイトと差をつけることができるため、HTTPSを導入しない手はありません。
3. **信頼性**—GlobalSignの調査によると、インターネットユーザーの28.9%が訪れたサイトの接続が保護されているかどうかを気にしており、77%がデータの傍受や誤用を懸念しています。アドレスバーに「この接続は保護されています」というメッセージを表示できると、サイト訪問者に安心感を与えることができます。

Google Chromeのアドレスバー

4. **参照データ**—HTTPSからHTTPへの参照データは、Google アナリティクスでブロックされており、多くは「Direct（ダイレクト）」トラフィックにまとめられます。逆にHTTPからHTTPSに移動した場合、リファラー情報が正常に渡されます。
5. **Chromeの警告**—2018年7月24日以降、Chrome 68以上のバージョンでは、HTTPSを使用していないサイトのアドレスバーに「保護されて

いない通信」というメッセージが表示されます。そして2020年からは、従来のTLSバージョンのサポートが非推奨に。安全な接続が確立されていないサイトでは、訪問者にその潜在的な危険性を明示するというGoogleの取り組みが伺えます。

6. **パフォーマンスの向上**—HTTP/2プロトコルの恩恵により、HTTPSを使用し適切に最適化されたサイトでは、通常読み込み速度も向上します。ブラウザのサポートのため、HTTP/2ではHTTPS接続が必要です。優れた多重化、並列処理、ハフマン符号によるHPACK圧縮、ALPN拡張、サーバープッシュなどにより、パフォーマンスの改善が期待できます。

また、TLS 1.3を使用すると、HTTPS接続がさらに高速化されます。Kinstaでは、サーバーとCDNでTLS 1.3をサポ ートしています。

詳しくは、WordPressサイトのHTTPからHTTPSへの切り替え方法、およびTLSとSSLの違いをご覧ください。

第8章

XML-RPCを無効にする

XML-RPCは、WordPressが採用するプロトコルの1つであり、近年これまで以上にブルートフォース攻撃の標的となっています。Jetpackなど、XML-RPCに依存するWordPressプラグインもありますが、多くの場合は不要であり、単にアクセスを無効化することでサイトのセキュリティを強化することができます。

Kinstaでは、攻撃や悪意のある行為に対して能動的かつ受動的な強化策を講じています。XML-RPCを介した攻撃が検出されるとスニペットをNginxの設定ファイルに追加し、403エラーの生成を阻止します。

> Kinstaの技術スタックとセキュリティのベストプラクティスを実装しているおかげで、セキュリティはもはや懸念事項ではなくなりました。ソフトウェアベースの制限、DDoS攻撃検出、ハードウェアファイアウォール、継続的な監視などは、Kinstaの素晴らしいサービスのほんの一部に過ぎません。加えて、ウェブサイトは毎日バックアップされており、これはサイトを常に編集して改善する企業にとって不可欠な機能です。Kinstaの1時間ごとの自動バックアップにはどれほど感謝していることか！おかげで、1ビットのデータも失わずに済みました。
>
> **Tom Potanski 氏**
> DevsData 創業者

第9章

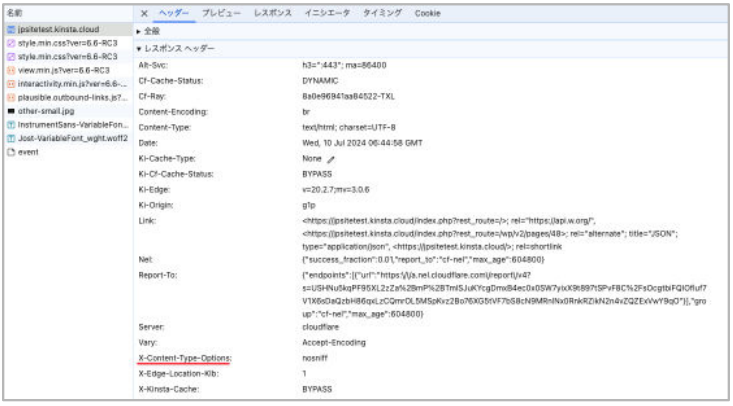
HTTPセキュリティヘッダーを追加する

クライアントのWordPressサイトを確実に保護するには、HTTPセキュリティヘッダーも活用しましょう。これは通常、ウェブサーバーレベルで設定するもので、クライアントサイトのコンテンツを処理する際の動作についてブラウザに指示を出します。HTTPセキュリティヘッダーにはさまざまな種類がありますが、主要なものは以下のとおりです。

- Content-Security Policy
- X-XSS-Protection
- Strict-Transport-Security
- X-Frame-Options
- Public-Key-Pins
- X-Content-Type

各WordPressサイトで使用されているヘッダーを把握するには、Chromeのデベロッパー ツールを使用して、サイトの最初のレスポンスヘッダーを確認します。デベロッパー ツールを開いたら、「ネットワークタブ」を開き、ページを再読み込みします（Ctrl+RまたはCmd+R）。該当のサイトを選択して「ヘッダー」タブの「レスポンス ヘッダー」を確認します。

例えば、次のデモサイト（jpsitetest）では、「X-Content-Type-Options」ヘッダーを利用していることがわかります。



デモサイト（jpsitetest）のレスポンスヘッダー

実際のクライアントサイトでも、X-Content-Type-Optionsは常にデフォルトで追加されますが、X-Frame-OptionsとStrict-Transport-Securityは必要な時にのみ設定されます。クライアントサイトのスキャンには、無料ツールのsecurityheaders.ioがお勧めです。

また、HTTPセキュリティヘッダーを実装する場合、WordPressのサブドメインに与える影響を理解しておくことも重要です。例えば、Content Security Polic（CSP）ヘッダーを追加して、ドメインごとにアクセスを制限する場合、自分のサブドメインも許可リストに追加する必要があります。実装方法が不明な場合は、レンタルサーバー等のご利用のサーバーに問い合わせてみてください。

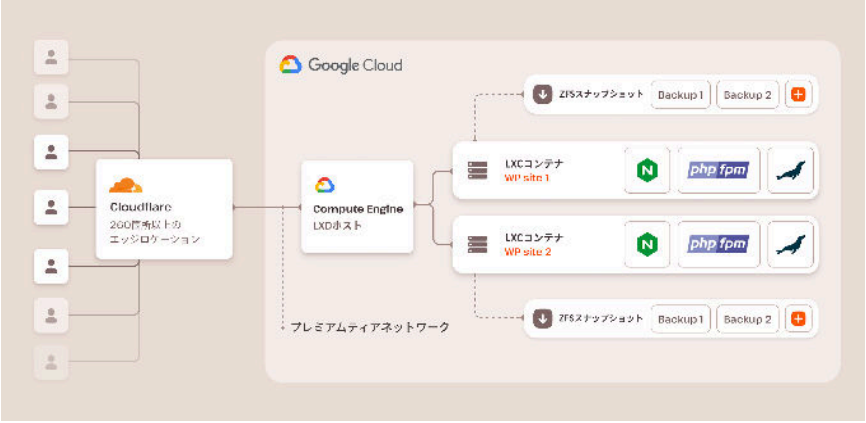
第10章

セキュリティプラグインを使用する

数々の開発者や企業が、WordPressサイト保護に役立つソリューションを提供しています。特に以下の選択肢がお勧めです。

- Sucuri Security
- iThemes Security
- Wordfence Security
- WP Security Audit Log
- WP fail2ban
- All In One WP Security & Firewall
- SecuPress
- BulletProof Security
- VaultPress
- Google Authenticator
- Security Ninja
- Defender
- Astra Web Security
- Shield Security
- Hide my WP
- WebARX

Kinstaは、ハードウェアファイアウォール、3分ごとの死活監視をはじめとする多数のセキュリティ機能を揃え、攻撃者によるデータへのアクセスを阻止します。また、万が一サイトがハッキングなどの被害に遭った場合には、無料でサイトの復旧をお手伝いしています。



KinstaのWordPress専用マネージドクラウドサーバーのアーキテクチャ

セキュリティプラグインに欠かせない重要な機能に「チェックサムユーティリティ」というものがあります。これは、ファイルの整合性の確認やデータの一貫性を確認するもので、（APIを介して）WordPress.orgのコアファイルに何かしらの変更が加えられていないかを検証してくれます。コアファイルの変更や修正は、ハッキングの危険を示すサインです。

WP-CLIを使用して、チェックサムを自分で実行することも可能です。おすすめのWordPressセキュリティプラグインはこちらでご紹介しています。

第11章

データベースのセキュリティを強化する

WordPressデータベースのセキュリティを強化する方法はいくつかあり、基本的なものとしては、まず賢いデータベース名の設定です。データベース名をわかりづらいものに変更し、ハッカーによるデータベースの情報の識別やアクセスを困難にすることが、サイト保護につながります。

2つ目は、別のデータベースのテーブル接頭辞を使用すること。WordPressをインストールすると、テーブル接頭辞が要求され、デフォルトでは「wp_」が適用されます。この接頭辞をたとえば「39xw_」などに変更するだけで、安全性が大きく向上します。

Wordpressのデータベース設定

Kinstaをご利用の場合、サイトとデータベースへのアクセスロックは自動的に行われるため、この操作は不要です。

第12章

常に安全な接続を使用する

安全な接続を確保することの重要性は、いくら強調してもしきれません。利用中のWordPress向けサーバーが、SFTPやSSHなどに対応しているかどうかを必ず確認してください。SFTP（SSH File Transfer Protocol、またはSecure File Transfer Protocol）は、ファイル転送に使用されるネットワークプロトコルで、標準のFTPよりも安全性に優れています。

Kinstaでは、データの安全性と暗号化のために、SFTP接続のみをサポートしています。また、ほとんどのWordPress向けサーバーは、SFTPに22番ポートを使用していますが、Kinstaでは、さらなるセキュリティを確保するため、ポートがランダムに割り当てられるようになっています（ポート番号はいつでもMyKinstaで簡単に確認可能）。

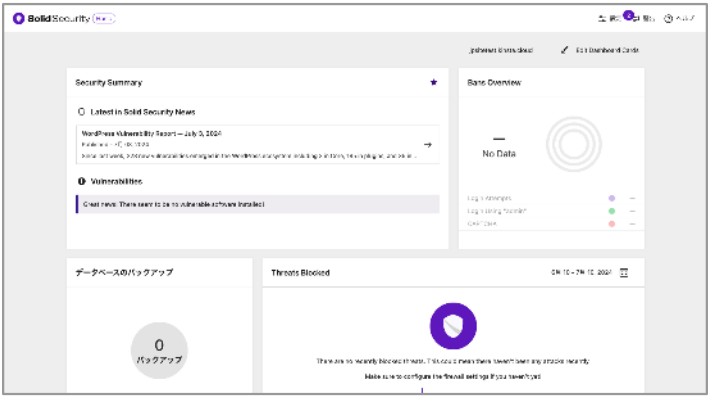
MyKinstaでSFTP/SSH情報を確認

第13章

ファイルとサーバーのアクセス権限を見直す

クライアントサイトおよびウェブサーバーのファイル権限もまた、セキュリティを強化する上で重要です。権限の設定が甘いと、部外者が簡単にサイトに侵入することができてしまい、大惨事が起きる可能性があります。とはいえ、逆に権限を過剰に厳しく設定してしまうと、サイトの機能が損なわれる可能性も。したがって、バランスを見て適切に権限を設定することが重要です。

iThemes Securityなどの無料プラグインを使用して、クライアントのWordPressサイトの権限を確認することができます。



iThemes Securityの設定画面

WordPressのファイルとフォルダのアクセス権限に関する一般的な推奨事項は以下のとおりです。

- すべてのファイルを644または640にする（注：wp- config.phpは440または400にして、サーバー上の他のユーザーがファイルを閲覧できないようにする必要がある）
- すべてのディレクトリを755または750にする
- アップロードディレクトリであっても、ディレクトリに777は設定しない

より詳細な情報については、ファイルのアクセス許可の変更に関するWordPress Codexの記事をご覧ください。

第14章

DDoS攻撃対策を講じる

DDoS攻撃はDoS攻撃の一種であり、複数のシステムを利用して単一のシステムを標的にサービス拒否（DoS）を引き起こします。Britannicaによると、最初に記録されたDDoS攻撃は2000年の初頭にまで遡ります。サイトのハッキングとは性質が異なり、通常サイトが乗っ取られるということはなく、サイトが数時間や数日間ダウンするというのが特徴です。

この脅威からサイトを保護するには、CloudflareやSucuriなどの信頼性に優れるサードパーティのセキュリティサービスを利用することをお勧めします。

高度なDDoS対策を講じれば、UDP、ICMPプロトコルを標的とするものを含むあらゆる種類・規模のDDoS攻撃、さらにSYN/ACK、DNS Amp、レイヤー7（L7）DDoS攻撃を緩和することができます。他にも、万能の策とは言えませんが、本来のIPアドレスを隠すプロキシサーバーを利用するのも1つの手です。

利用するサーバーが採用するソリューションを確認することも重要です。Kinstaが採用するGoogle Cloud Platformのファイアウォールは、サイトを保護するためのソフトウェアベースの厳重な制限を設けており、DDoS攻撃を即座に検出するソフトウェアを導入しています。

Kinstaを選択すると、Googleが15年の年月をかけて構築し、現在はGmailやGoogle 検索などの業界トップクラスの製品・サービスの保護に利用しているセキュリティモデルの恩恵を受けることができます。

Google Cloud Platformに加えて、Linuxコンテナ（LXC、LXD）を使用した調整も行い、各アカウントはもちろん、すべてのWordPressサイトが完全に隔離されます。

万が一問題が発生した場合は、ハッキングの復旧とマルウェアの除去を無料で承っています。クライアントサイトがマルウェアに感染しても、サポートエンジニアがすぐにサイトのクリーンアップにあたります。

第15章

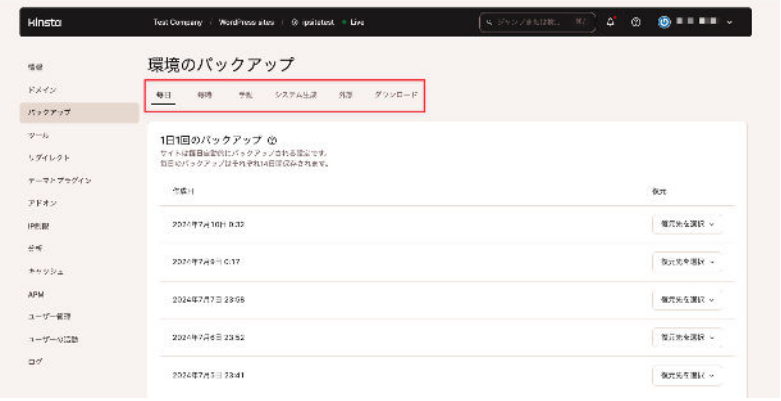
常にバックアップを忘れない

残念ながら、サイトの安全性をどれほど追求しても「100%安全」はありえません。だからこそ、最悪の事態を想定してバックアップを作成することもセキュリティ強化策の1つと言えます。バックアップは基本的な作業ですが、見落とされがちです。本書でご紹介したセキュリティのヒントに加えて、定期的なバックアップも必ず実行してください。

WordPress向けのマネージドサーバーでは、コントロールパネルにバックアップ機能が組み込まれているのが一般的です。Kinstaでは、以下6種類のバックアップをご用意しています。

- **毎日（自動）のバックアップ**：毎日自動でサイトのバックアップを行います。
- **手動バックアップ**：サイトごとに最大5個のバックアップを手動で作成し、14日間保持できます。
- **システム生成バックアップ**：検索と置換ツールの使用、ステージング環境から本番環境への移行、本番環境でのバックアップ復元など、重要なタスクを実行する際には、事前にバックアップが作成されます。
- **ダウンロード可能なバックアップ**：週に一度、サイトのZIPファイル（サイトファイルを格納）とSQLファイル（サイトデータベースのコンテンツを格納）をダウンロードできます。

- **外部バックアップ**（アドオン）：AWSやGoogle Cloudのアカウントを使って外部バックアップを設定することができます。
- **毎時バックアップ**（アドオン）：24時間よりも頻繁にバックアップが必要になる場合は、6時間または1時間ごとの自動バックアップを設定することができます。



MyKinstaのバックアップ画面

また、バックアップはワンクリックで復元可能です。ご利用中のサーバーにバックアップ機能がない場合は、WordPressプラグインを使って自動化すると効率的です。

第16章

バックアッププラグインを使用する

WordPressのバックアッププラグインを使用すると、FTP経由でバックアップを取得したり、Amazon S3、Google Cloud Storage、Google ドライブ、Dropboxなどの外部ストレージサービスと統合したりすることができます。消費リソースを削減できることから、以下のような増分バックアッププラグインがお勧めです。

- DDuplicator
- WP Time Capsule
- BackupBuddy
- UpdraftPlus
- BackUpWordPress
- BackWPup
- WP BackItUp

注意点として、Kinstaではパフォーマンスへの影響を考慮し、差分バックアップの使用を禁止しています。Kinstaでは、サーバーレベルですべての処理を行うため、クライアントサイトの速度が低下することはありませんのでご安心ください。

まとめ

セキュリティは、複数の防御層を重ねて強化することが重要です。層を適切に重ねれば重ねるほど、クライアントサイトの安全が確保されます。一意の強力なパスワードを設定すること、WordPressコアとプラグインを常に最新の状態に保つことなど、本電子書籍でご紹介したセキュリティのベストプラクティスに従うことで、セキュリティを劇的に改善することができます。

そしてクライアントサイトがハッキングなどの被害に遭うリスクを最小限に抑えるには、マネージドに分類されるWordPressサーバーの利用をお勧めします。Kinstaでは、WordPress専用マネージドクラウドサーバーをぜひ一度お試しください。セキュリティ強化策が自動的に実施されるため、クライアントサイト管理の負担を軽減しながら、ビジネスの成長に欠かせない強固でスケーラブルな基盤を確保することができます。

Web制作業を営むお客様向けには、エージェンシープログラムもご用意しています。ご興味がございましたら、お気軽にお問い合わせください。