クライアントの
サイトを保護するには
〜包括的ガイド〜
KINSTA

常に最新のバージョンについては、
上記のQRコードまたは次のURLにアクセスしてください
https://kinsta.com/jp/ebooks/

発行 KINSTA

クライアントの
サイトを保護するには
～包括的ガイド～

クライアントのサイトを保護する方法包括的ガイド

目次

6
セキュアなWordPressホスティングに投資

7
最新のPHPバージョンを使う

10
賢いユーザー名とパスワードを使用する

11
常に最新バージョンのWordPress、プラグイン、テーマを使用する

14
WordPressログイン画面の守りを固める

17
2要素認証（2FA）を利用する

20
HTTPSを使用して接続を暗号化する（SSL）

20
HTTPSがeコマースサイト以外でも重要である6つの理由

22
XML-RPCを無効にする

22
最新のHTTPセキュリティヘッダーを追加する

24
WordPressセキュリティプラグインを使用する

26
データベースのセキュリティを強化する

27
常に安全な接続を使用する

28
ファイルとサーバーのアクセス権限を確認

29
DDoS攻撃に対する守りを固める

31
常にバックアップを取る

33
WordPressバックアッププラグイン

33
まとめ

クライアントの
サイトを保護するには
～包括的ガイド～

internet live statsによると、100,000を超えるウェブサイトが毎日ハッキングされています。😲 そのため、WordPressのセキュリティ強化のあり方について、少し時間をかけて考えてみ WordPressのセキュリティは包括的な話題です。サイトそのものの保護強化（ちなみに、これについても最善策をご紹介します）にとどまりません。

セキュアなWordPressホスティングに投資

WordPressホストが担うことになるウェブサーバーレベルのセキュリティから始めましょう。クライアントのサイトを「差し出す」ことになるのですから、信頼できるホストを選択することが非常に重要です。

自前のVPSでWordPressをホストしている場合は、これを自分で行うための技術的知識が必要になります。しかし正直なところ、システム管理者になることで月額20ドルを節約しようとするやり方は、事業運営の賢い判断とは言えません。

サーバーの強化は、完全に安全なWordPress環境を維持するための鍵です。WordPressサイトをホストするITインフラストラクチャが物理的、仮想的に高度な脅威に十分に対抗できるように、ハードウェアやソフトウェアレベルのセキュリティ策を複数レイヤー用意することが重要です。

このため、WordPressをホストするサーバーには、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、スキャンすることが求められます。

WordPressのインストール、サイトの構築段階であっても、クライアントのサイトを適切に保護するために、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を用いる必要があります。ただし、最適なパフォーマンスを維持するには、WordPressコンテンツを保護するためにマシンに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必要があります。さらに、安全なネットワークとファイル転送暗号化プロトコル（FTPではなくSFTP）を使用し、悪意のある侵入者から機密コンテンツを隠すようにサーバーを構成する必要もあります。

セキュアなWordPressホスティングであるKinstaではすべてのWordPressユーザーのお客様にGoogle Cloud Platformをご提供しています。セキュリティは当社アーキテクチャの土台に組み込まれており、市場に出回る他の選択肢よりもはるかにセキュアです。

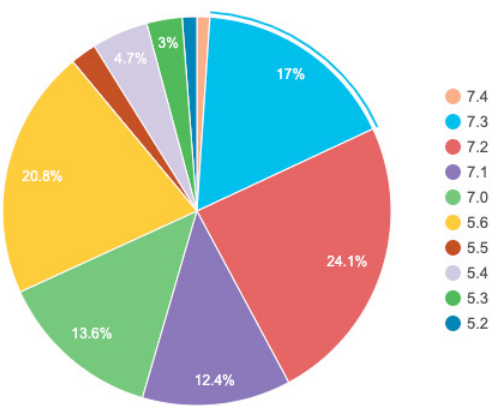
最新のPHPバージョンを使う

PHPはあらゆるWordPressサイトのバックボーンです。クライアントのサイトがサーバー上で最新のバージョンを常に使用するように気を配りましょう。PHPの各メジャーリリースは、通常、リリース後2年間完全にサポートされます。

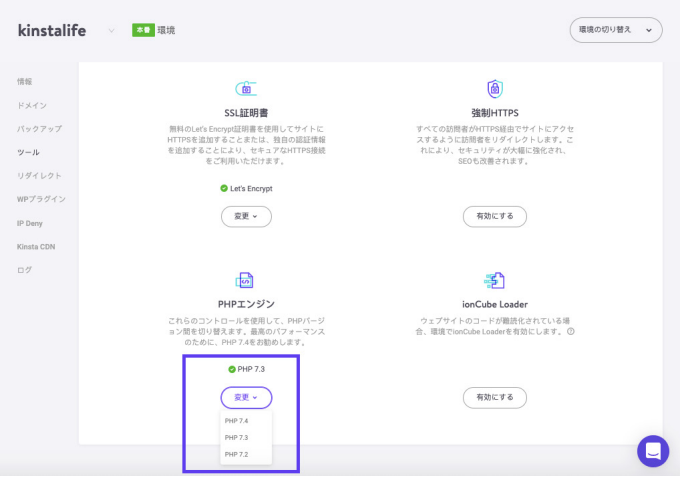
その間、バグとセキュリティの問題が定期的に修正され、パッチが適用されます。現在のところ、バージョンPHP 7.1以前を利用するサイトはセキュリティサポートを受けておらず、パッチの欠如した、セキュリティ面での脆弱性にさらされています。そして、衝撃の事実がこちら。

WordPressの公式統計ページによると、WordPressユーザーの約34%がまだPHP 5.6以前を使用しています。つまり、現在3分の1以上のユーザーが、全くサポートされていないPHPバージョンを使用しているのです。恐ろしい事態です！

PHPバージョン



Kinstaでは、7.2、7.3、7.4という、安定した、そしてサポートのあるバージョンのみの使用をお勧めしています。PHP 5.6、7.0、7.1は段階的に廃止されています。MyKinstaダッシュボード内からボタンをクリックするだけで、PHPバージョンを切り替えることができます。



実際に使ってみるには、demo.kinsta.com からデモをご確認ください。

賢いユーザー名とパスワードを使用する

意外かもしれませんが、WordPressのセキュリティを強化する最良の方法の1つは、巧妙なユーザー名とパスワードを使用することです。とてもシンプルな話だと思えるかもしれません。しかし、そうとも限りません。SplashDataによる2019年を通じて盗まれたトップパスワードのリストをご紹介します（最も多い順に並べられています）。

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

最も多かったパスワードは「123456」です。このような理由から、Kinstaを通じたWordPressインストール時には、wp-adminログインには複雑なパスワードを設定するように強制しています（以下のワンクリックインストールプロセスを参照）。これは、「推奨」ではなく「必須」事項です。

MyKinstaデモでこの機能をご確認ください。

WordPressのwp_hash_password 関数は、phpassパスワードハッシュフレームワークとMD5ベースのハッシュの8つのパスを使用します。また、WordPressのクライアントサイトでデフォルトの「admin」ユーザー名を使用することは避け、管理者アカウントとして一意のWordPressユーザー名を作成するようにしましょう。

また、クライアントサイトごとに異なるパスワードを使用することも重要です。そして、それらをコンピューターの暗号化したローカルのデータベースに保存しましょう。

無料のツールKeePassが便利です。その他には、1PasswordやLastPassなどのオンラインパスワードマネージャーもあります。

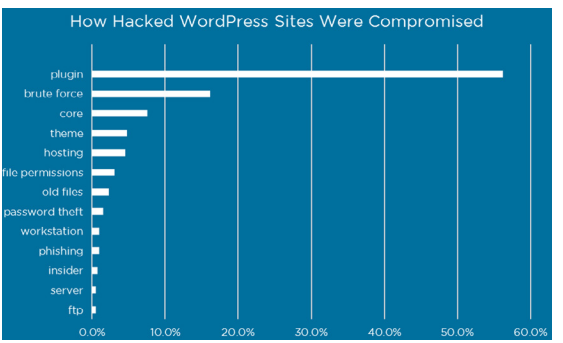
常に最新バージョンのWordPress、プラグイン、テーマを使用する

クライアントのサイトセキュリティを強化するもう1つの非常に重要な方法として、常に最新の状態に保つことが挙げられます。具体的には、WordPressコア、プラグイン、テーマの更新です。更新には大きな価値があります。多くの場合、アップデートのたびにセキュリティが強化され、バグが修正されます。

残念ながら、世界中の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おり、これには「自分の事業は正しい道を進んでいる」という誤解が付随しがちです。「サイトが壊れる」、「コアに施した変更が消える」、「プラグイン○○が機能しなくなる」、「新しい機能は必要ない」などなど、更新を渋る理由が列挙されることでしょう。

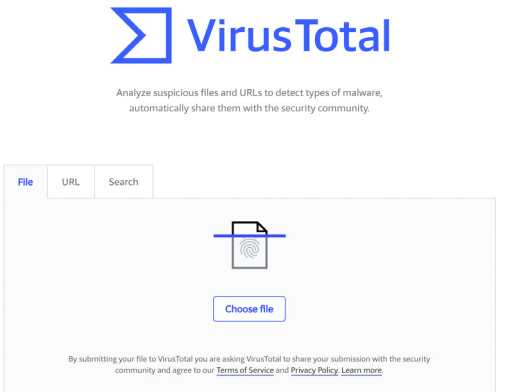
実際、ウェブサイトは主に、古いバージョンのWordPressのバグが原因で壊れるものです。WordPressチームや関連するリスクを理解する開発者は、コアに変更を施すことを推奨しません。また、WordPressのアップデートには、最新のプラグインを実行するために必要な機能とともに、必須のセキュリティパッチが含まれます。

あなたは、プラグインの脆弱性がハッカーの既知のエントリポイントの55.9%を占めるというデータをご存知でしょうか？これは、WordFenceによる、攻撃の被害にあった1,000人以上のWordPressサイト所有者への聞き込みから判明しています。プラグインを更新することで、この被害者たちの一員になることが避けられます。



クライアントサイトには信頼できるプラグインのみをインストールすることもお勧めします。WordPressリポジトリの「注目」カテゴリと「人気」カテゴリを対象とするのがいいでしょう。または、開発者のウェブサイトから直接ダウンロードします。違法公開（有料のものを無料で配布している例など）のWordPressプラグインとテーマを使用することは避けてください。

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確認することができます。



また、WordPressの最新セキュリティアップデートや脆弱性の追跡に使える便利なリソースも多数あります。以下をご活用ください。

- WP Security Bloggers: 20以上のセキュリティフィードを集約
- WPScan Vulnerability Database: 10,000以上のWordPressコア、プラグイン、テーマの脆弱性を掲載
- ThreatPress: WordPressプラグイン、テーマ、WordPressコアの脆弱性についての日々更新型データベース.
- Official WordPress Security Archive

WordPressログイン画面の守りを固める

「隠蔽によるセキュリティ」戦略は、時に、一般的なオンラインビジネスやWordPressサイトにとって効果的になり得ます。ハッカーによる特定のバックドアの発見を難しくすれば、攻撃を受ける可能性を下げることができます。クライアントのWordPressログイン画面の守りを固めることは、セキュリティ強化に一役買います。これを行う方法として、デフォルトのwp-adminログインURLを変更すること、そして、ログインの試行回数を制限することが考えられます。

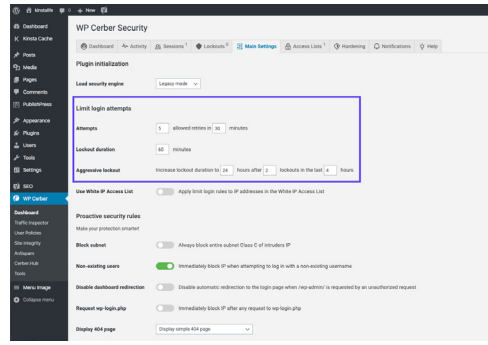
WordPressログインURLを変更する方法

デフォルトでは、WordPressサイトのログインURLはdomain.com/wp-adminです。これの問題点として、ボット、ハッカー、悪意のあるスクリプトのすべてが、このURLを知っています。URLを変更することで、ターゲットになる可能性を下げ、ブルートフォース攻撃から身を守りましょう。ただし、これはあくまでも、万能の解決策ではなく、保護に役立つ小さな技の一つです。

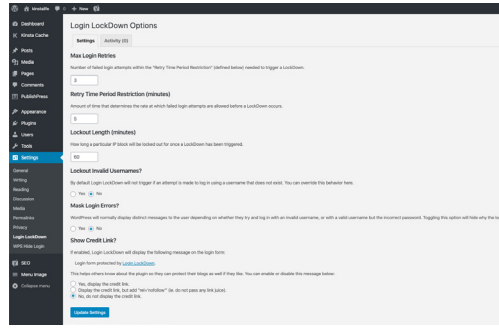
WordPressログインURLを変更するには、無料のWPS Hide Loginプラグインをお勧めします。ボットまたはスクリプトのリストに含まれていないと思われるユニークなものを選択しましょう。

ログイン試行回数を制限する方法

上記の管理者ログインURLを変更する方策には、不正なログイン試行の大部分を未然に防ぐ効果がありますが、さらに制限を設けることも非常に効果的です。無料のCerber Limit Login Attemptsプラグインを使えば、ログイン再試行不能期間、ログイン試行回数、IPホワイトリスト、ブラックリストを簡単に設定できます 。



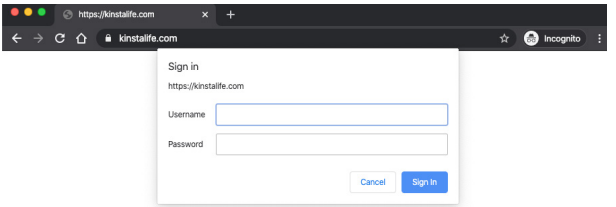
もっとシンプルなWordPressセキュリティソリューションをお探しであれば、優れた代替策として（同じく無料の）Login Lockdownプラグインもあります。



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ます。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た場合には、その範囲からのすべての要求に対しログイン機能が無効になります。また、前述のWPS Hideログインプラグインと完全に互換性があります。

ちなみに、クライアントのサイトをKinstaに移行する際には、プラットフォームがデフォルトで制限をかけ、悪意のあるログインを自動的にブロックするので、このためのプラグインを個別にインストールする必要はありません。

基本的なHTTP認証を追加する方法（htpasswd保護）管理者画面の守りを固めるもう1つの方法として、HTTP認証を追加することもできます。これを実装すると、WordPressログインページにアクセスする 。



MyKinstaデモでこの機能をご確認ください。

重要：通常、eコマースサイトやメンバーシップサイトでは使用しないでください。しかし、ボットによるサイトへのアクセスを防ぐには非常に効果的な手法です。

Kinstaでクライアントのサイトをホストしている場合は、MyKinstaダッシュボードから簡単にパスワード保護（htpasswd）ツールを使用できます（無料のMyKinstaデモアカウントで実際に動作をご確認ください）。サイトの「ツール」セクションにあります。「有効にする」をクリックし、ユーザー名とパスワードを入力するだけで準備完了です。

MyKinstaデモでこの機能をご確認ください。

有効にすると、WordPressサイトにアクセスする際に、毎回、認証が要求されます。ログイン情報はいつでも変更でき、不要になった場合は無効にできます。

2要素認証（2FA）を利用する

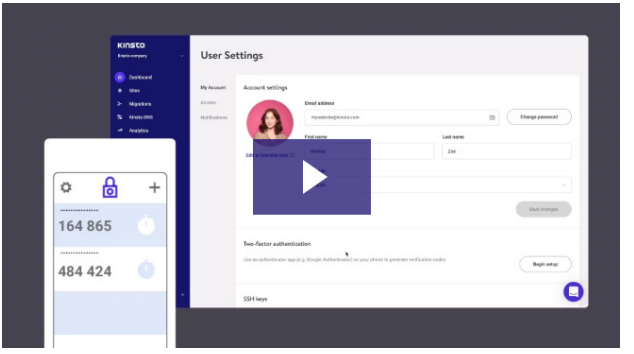
2要素認証を利用すると、ログインプロセスが2段階になり、パスワードだけでなく2つ目の要素もログインに必要になります。ほとんどの場合、これはクライアントのWordPressサイトへのブルートフォース攻撃を防ぐという意味で非常に効果的です。

クライアントサイトを扱う場合には、2要素認証は2つの部位に分けて考えることができます。

1つ目は、お使いのウェブホスティングプロバイダーで使用しているアカウントまたはダッシュボードです。誰かがこれにアクセスすると、クライアントのすべてのパスワードの変更、ウェブサイトの削除、DNSレコードの変更など、あらゆる恐ろしいことが起こり得ます。Kinstaでは、MyKinstaダッシュボードにAuthenticatorベースの2FAを使用しています。

- Authenticatorベースの2FAは、携帯電話番号に紐づけられないので、従来のSMS依存型よりも安全です。結果的に、Authenticatorベースの2FAはSIM入れ替えによるアクセス手法に耐性があります。
- Authenticatorベースの2FAは、1Passwordなどのパスワードマネージャーアプリと併用できさらに便利です。2FA情報をパスワードマネージャーに追加すると、MyKinstaへのログインに外部デバイスを使用する必要がなくなります 。

しかも簡単にこの機能を有効にできます。



2要素認証の2番目の部位は、クライアントのWordPressサイトそのものです。これを実装できるお勧めのプラグインをいくつかご紹介します。

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

上のプラグインのいずれかをクライアントサイトにインストールし設定すると、WordPress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追加フィールドが表示されるようになります。また、Duoプラグインであれば、最初にアカウント情報を使ってログインし、次にDuoプッシュ、通話、パスコードなどの認証方法を選択するよう求められます 。

HTTPSを使用して接続を暗号化する（SSL）

WordPressセキュリティ強化の際に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可能にするメカニズムです。「クライアントのサイトにクレジットカードでの支払い機能がなければ、SSLは必要ない」というのはよくある誤解です

では、eコマースサイト以外でもHTTPSが重要である理由をいくつかご紹介します。Kinstaを含む多くのホストでは、Let's Encryptを用いた無料のSSL証明書が利用できます。

HTTPSがeコマースサイト以外でも重要である6つの理由

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であることは、言うまでもありません。それでは、ユーザーがログインをするたびに、その情報がプレーンテキストでサーバーに渡されるという事実はご存知でしょうか。HTTPSは、サイトとブラウザ間の安全な接続を維持するために不可欠です。これを用いることで、ハッカーや部外者がクライアントのサイトにアクセスするのを防ぐことができます。

2. SEO
Googleは公式にHTTPSがランキング上昇を助ける要素であることを発表しました。クライアントのサイトで、SEOやSERPの面から競合他社の先を行くことにつながるため、導入しない手はありません。

3. 信頼性
GlobalSignの調査によると、訪問者の28.9%がブラウザで緑色のアドレスバーを積極的に探すとのことです。また、77%がオンラインでデータが傍受されたり誤用されたりすることを心配しています。緑色の南京錠のマークが目に入ると、ユーザーは自分のデータがより安全であることを瞬時に理解し安心感を得ることができます。

4. 参照データ
HTTPSからHTTPへの参照データがGoogleアナリティクスでブロックされることを知っている人は、あまり多くありません。ブロックされた参照データのほとんどは、「ダイレクト（direct）トラフィック」セクションに一緒にまとめられます。逆に誰かがHTTPからHTTPSへ移動した場合、リファラーは正常に渡されます。

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以外のすべてのサイトに「Not Secure（安全ではない）」という文言が表示されています。そして、2020年から、従来のTLSバージョンのサポートが非推奨になっています。WordPressサイトを含むウェブサイトで安全な接続が確立されていない場合にはそれをユーザーに知らせる、というGoogleの明確な姿勢がわかります。だからこそ、HTTPSがこれまで以上に重要な意味を持っているのです！

6. パフォーマンス
多くの場合、HTTP/2プロトコルの恩恵で、HTTPSを介し適切に最適化されたサイトでは、読み込み速度の向上さえ見られます。ブラウザのサポートのため、HTTP/2ではHTTPSが必要になり

ます。HTTP/2が優れた多重化、並列処理、ハフマン符号によるHPACK圧縮、ALPN拡張、サーバープッシュをサポートするなど、さまざまな理由により、パフォーマンスの向上が実現します 。

また、TLS 1.3を使用すると、HTTPS接続がさらに高速になります。Kinstaは、すべてのサーバーとKinsta CDNでTLS 1.3をサポートしています 。

詳細は、WordPress HTTPS移行ガイド、そして、TLSとSSLの比較記事をご覧ください。

XML-RPCを無効にする

ここ数年間、XML-RPCは以前にも増して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プラグインはいくつかありますが、ほとんどの場合これは必要ではなく、単純にアクセスを無効化するという策を講じることができます 。

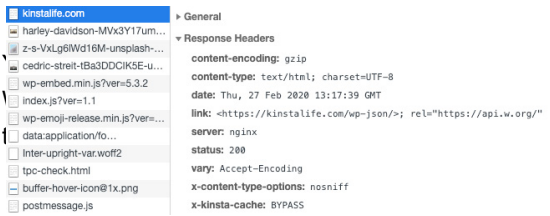
Kinstaをお使いであれば、攻撃や悪意ある行いに対する能動的、受動的な策を講じているため、ご心配は要りません。具体的には、XML-RPCを介した攻撃が検出されると、スニペットをNginx構成ファイルに追加し、403エラーの生成を阻止します。

最新のHTTPセキュリティヘッダーを追加する

クライアントのWordPressサイトのセキュリティを強化するために、その他には、HTTPセキュリティヘッダーを利用することができます。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とき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様々な種類がありますが、最も重要なのは、以下の通りです。

- 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 DevToolsを使い、サイトの最初の応答のヘッダーを確認することができます。

以下は、kinstalife.com（デモサイト）の例です。x-content-type-optionsヘッダーを利用していることがわかります。

実際のクライアントサイトについて言えば、例にあるように、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は必要な場合にのみ設定されます。

クライアントのサイトをスキャンする必要がある場合には、Scott Helme氏提供の無料ツールsecurityheaders.ioが便利です。

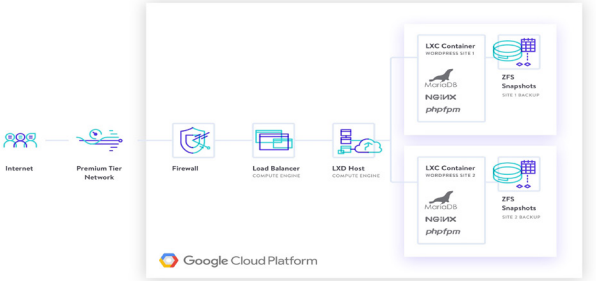
また、HTTPセキュリティヘッダーを実装する場合、これがWordPressサブドメインにどのように影響するかを知っておくことも重要です。たとえば、Content Security Policyヘッダーを追加し、ドメインごとにアクセスを制限する際には、自分のサブドメインも追加する必要があります。これの実装方法が不明な場合には、ホストに問い合わせをするのが得策でしょう。

WordPressセキュリティプラグインを使用する

WordPressサイト保護に便利な優れたソリューションを提供するすばらしい開発者や企業はたくさん存在します。注目すべき例を挙げると次のとおりです。

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

Kinstaには、ハードウエアファイアウォール、能動的・受動的セキュリティ、分単位のアップタイムチェック、その他多数の高度な機能があり、攻撃者によるデータへのアクセスを防ぎます。そして万が一サイトが危険にさらされた際には、無料でのサイト修正サービスをご利用頂けます。

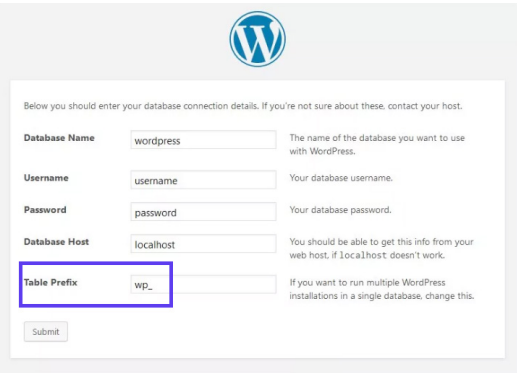


多くのセキュリティプラグインに含まれる非常に重要な機能に、チェックサムユーティリティがあります。これは、クライアントのWordPressデータを検査し、（APIを介して）WordPress.org提供のコアファイルに何かしらの変更が加えられていないかチェックしてくれます。コアファイルの変更や修正はハッキングの危険信号です。

WP-CLIを使用して、自らチェックサムを実行することもできます。こちらのWordPressセキュリティプラグイン各種も是非ともご確認ください。

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ます。1つ目は、データベース名を賢く決めることです。データベース名を分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で、サイトを保護することができます。

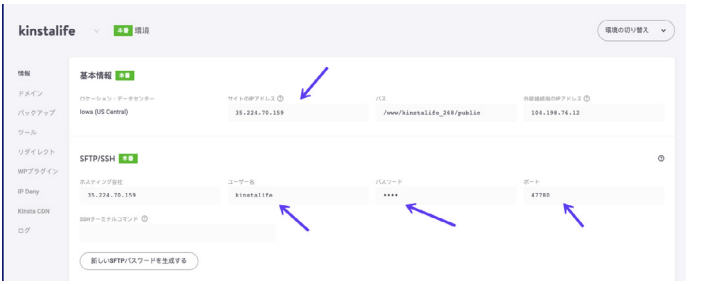


2つ目の方法は、別のデータベーステーブルプレフィックスを使用することです。WordPressをインストールすると、テーブルプレフィックスが要求されます。 デフォルトでは、WordPressはwp_を使用します。これを39xw_のようなものに変更すると、はるかに安全になります。

Kinstaですべてのクライアントのサイトをホストしている場合には、これを必要する必要はありません。サイトとデータベースへのアクセスロックはKinstaが行います！

常に安全な接続を使用する

安全な接続を使用することの重要性は強調してもしきれません。お使いのWordPressホストがSFTPやSSHの提供といった予防策を講じているかどうか、是非とも確認してください。SFTPまたはセキュアファイル転送プロトコル（SSHファイル転送プロトコルとも）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す。これは、標準のFTPよりも安全性の高い選択肢です。



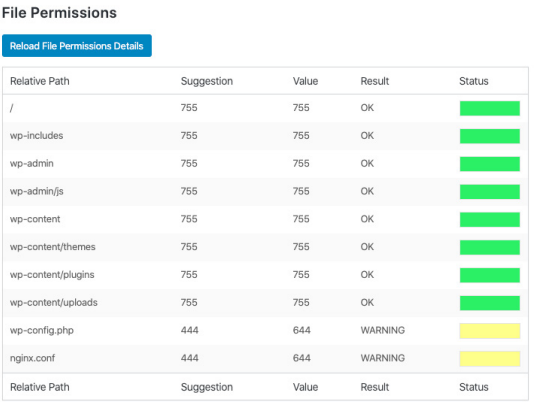
MyKinstaデモでこの機能をご確認ください。

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ホストは通常、SFTPにポート22を使用します。しかしKinstaでは、これをさらに一歩進め、どのサイトのポートもランダムに割り振られます（MyKinstaダッシュボードで確認可能）。

ファイルとサーバーのアクセス権限を確認

クライアントのサイトとサーバーの両方におけるファイルアクセス権限がセキュリティを強化するために重要です。権限が緩すぎると、部外者が簡単に自分のサイトにアクセスして大混乱を引き起こす危険性があります。一方、権限が厳しすぎると、サイトの機能が損なわれる可能性があります。そのため、全体にわたって正しい権限を設定することが重要です。

iThemes Securityなどの無料のプラグインを使用して、クライアントのWordPressサイトの権限をスキャンすることができます。


File Permissions

Reload File Permissions Details

Relative Path	Suggestion	Value	Result	Status
/	755	755	OK	
wp-includes	755	755	OK	
wp-admin	755	755	OK	
wp-admin/js	755	755	OK	
wp-content	755	755	OK	
wp-content/themes	755	755	OK	
wp-content/plugins	755	755	OK	
wp-content/uploads	755	755	OK	
wp-config.php	444	644	WARNING	
nginx.conf	444	644	WARNING	
Relative Path	Suggestion	Value	Result	Status

WordPressのファイルとフォルダのアクセス権限に関して、一般的な推奨事項は以下の通りです。

- すべてのファイルは644または640にする（例外：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読めないようにする必要があります）

- すべてのディレクトリを755または750にする
- たとえ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を設定するのは避けるべき

より詳細な説明については、ファイルのアクセス許可の変更に関するWordPress Codexの記事をご参照ください。

DDoS攻撃に対する守りを固める

DDoS攻撃はDOS攻撃の一種であり、複数のシステムを使用し単一のシステムをターゲットとして、サービス拒否（DoS）を引き起こします。DDoS攻撃は目新しいものではありません– Britannicaによると、最初に記録されたケースは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ことはなく、数時間や数日間のダウンが発生します 。

この脅威から身を守るためには、CloudflareやSucuriなどの信頼できるサードパーティによるセキュリティサービスを使用することをお勧めします。

高度なDDoS保護を使用して、UDP、ICMPプロトコルをターゲットとするものを含むすべての種類とサイズのDDoS攻撃、さらに、SYN/ACK、DNS Amp、レイヤー7攻撃を緩和できます。さらに、本来のIPアドレスを隠すのに力を発揮するプロキシも使用されますが、これは完全な策とは言えません。

ウェブホストが使用するプロバイダーも見落としてはなりません。これも非常に重要です。

Kinstaでは、Google Cloud Platform Firewallを採用し、クライアントのサイトを保護するためのソフトウェアベースの非常に厳しい制限を設け、DDoS攻撃が発生したときにそれを検出するソフトウェアを導入しています。

つまり、御社（ひいては御社のクライアント様）には、15年をかけて築き上げてきた、そして、現在Gmailや検索などの製品・サービスの保護を担っているセキュリティモデルならではの強みを享受して頂けるということです。

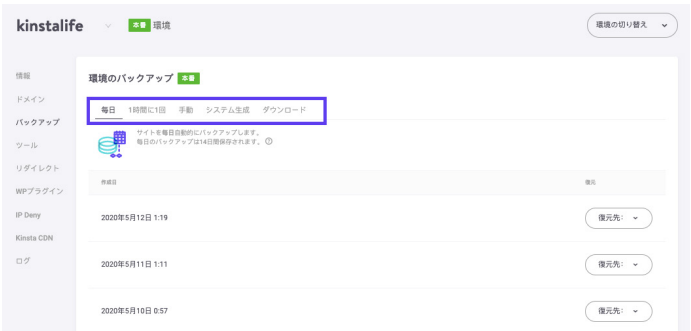
Kinstaでは、Google Cloud Platformに加えて、Linuxコンテナ（LXC、LXD）を使用した調整も行っています。これにより、各アカウントだけでなく各WordPressサイトが完全に分離されます。

それでも、時に問題が発生する可能性はあります。しかしそんな時には、Kinstaの無料ハッキング復旧とマルウェア除去をご利用ください。万が一クライアントのサイトが感染してしまっても、サポートチームがサイトのクリーンアップを行います。

Kinstaがセキュリティをどれだけ真剣に考えているのか、詳細をご覧ください！

常にバックアップを取る

サイトの安全性をどれだけ高めようと、100%安全はあり得ません。だからこそ、最悪の事態が発生した場合に備えてバックアップを取ることが重要です。バックアップとは、誰もが必要だと感じているのに、忘れられがちなもの。今回ご紹介している推奨事項はすべて、クライアントのサイトとビジネスを適切に保護するために効果を発揮します。しかし、バックアップも欠かせません。



この機能を、MyKinstaデモからご確認ください！

ほとんどのマネージドWordPressホスティングプロバイダーがバックアップを提供しています。Kinstaには5種類のバックアップがあります。

- 24時間ごと：Kinstaは24時間ごとにすべてのクライアントのサイトの自動バックアップを作成します。夜には安心してご就寝頂けます。

- 1時間ごと：より頻繁なバックアップスケジュールが必要な場合は、対象とするサイトの6時間または1時間ごとの自動バックアップ作成機能を有効化できます（これは毎月のホスティングプランに追加するかたちでご利用頂けます）。
- 手動：自動バックアップだけでは不十分な場合は、管理するサイトごとに手動でバックアップを取り、データを14日以上保持（ホスティングプランにより上下します）することができます。
- システム生成：MyKinstaの検索置換ツールの使用、ステージング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の大きなタスクの実行前に、Kinstaがシステム生成バックアップを実行します。
- ダウンロード用アーカイブ：上記のすべてが不十分な場合は、週に1度まで、各クライアントサイトのzipファイル（ウェブ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。

Kinstaでは、ワンクリックで簡単に任意のサイトを復元できるため、バックアップオプションの使い勝手も確保されています。非常に便利ですね 。

MyKinstaでバックアップを作成するのがいかに簡単か、無料でご確認ください！

お使いのホストにバックアップ機能がない場合、WordPressプラグインを使ってプロセスを自動化することもできます。

WordPressバックアッププラグイン

WordPress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ソースと統合したりできます。使用するリソースが少なくなるように、増分ソリューションを使用することを強くお勧めします。

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

Kinstaは、パフォーマンスに支障をきたすため、差分バックアッププラグインの使用を許可していません。当社がサーバーレベルでこのすべてを処理するため、クライアントのサイトが遅くなることはありません。

まとめ

セキュリティは層で実施するものです。セキュリティの層を正しく積み重ねるほどに、クライアントのサイトは安全になります。このすべては、賢いパスワードを使用し、コアとプラグインを最新の状態に保ち、今回取り上げた他のセキュリティのベストプラクティスに従うことから始まります 。

しかし、クライアントサイトがハッキングされる可能性を下げるために

できることは他にもあります。KinstaのようなマネージドWordPressホストを選択することで、ほとんどのセキュリティ対策が自動的に行われ、クライアントサイトの(そして御社の)未来を守るための強固でスケーラブルな基盤が構築できます。

Kinstaでクライアントサイトの管理がいかに簡単になるか試してみませんか？

demo.mykinsta.comをご覧ください！
KINSTA