基本のキ。セキュリティ入門（第4回）

狙われやすいWordPressのセキュリティ対策

2020.03.12

Webサイトやブログを作成・運用するツールとして、「WordPress」は非常に人気があります。誰もが簡単に利用できるツールですが、それだけに狙われやすいことも覚えておかなければなりません。

今回は、WordPressが狙われる理由や被害例を紹介し、WordPressで実施しておくべきセキュリティ対策について解説していきます。

WordPressが狙われやすい理由

まずは、WordPressが攻撃者から狙われる理由や被害例についてご紹介します。

＜WordPressが狙われる理由＞
WordPressが狙われる理由としては、大きく次の3つが考えられます。

・世界中で利用しているユーザーが多い
・オープンソースで脆弱性が見つかりやすい
・管理画面のURLが分かりやすい

WordPressが利用されている割合は、世界中のWebサイトの35.1%です。WordPressと同じCMS（Contents Management System）の中では、61.9%ものシェアを誇ります（W3Techs調べ）。シェア率が高いということは、それだけ利用しているユーザーが多いということであり、攻撃者からすればターゲットとして狙えるWebサイトが多く存在する状態だといえるでしょう。

また、WordPressは誰でもカスタマイズして利用できるオープンソースのツールです。オープンソースとはプログラムのソースを公開しているという意味であり、プログラムのソースはいわば設計書となります。設計書を詳しく見られる状態にあるという

ことは、セキュリティ的に弱い部分（脆弱性）を見つけやすい、ということです。

さらに、WordPressの管理画面のURLはデフォルトでは固定化されています。そのため、WordPressを使ったことのある人なら、簡単にWordPressを利用しているWebサイトの管理画面へアクセスすることが可能です。もちろん、IDとパスワードが分からなければログインできませんが、ログインの入り口となる管理画面へ簡単にアクセスできる点は、WordPressが狙われやすい理由の一つとなります。

＜ターゲットになったときの被害例＞
実際にサイバー攻撃のターゲットとなってしまった場合、具体的にどのような被害を受けるのでしょうか。考えうる被害の例を紹介します。

・アカウントの乗っ取り
・情報の抜き取り
・ページの改ざん
・大量のコメントスパム投稿
など

WordPressは、デフォルトの設定では管理画面のURLが固定化されているため、IDとパスワードを総当たりで試行する「ブルートフォース攻撃」を受けると、アカウントを乗っ取られてしまう可能性があります。アカウントを乗っ取られてしまうと、Webサイトに関連する情報を抜き取られたり、公開しているページを改ざんされたりする危険性があります。WordPressで運用するWebサイトによっては、個人情報をデータベースで管理していることもあるため、大量の個人情報を盗み出される可能性も考えられます。

そのほかにも、WordPressで作成したWebページにはコメント機能が標準搭載されています。読者とコミュニケーションを取るための機能ですが、悪用される可能性も考慮しなければなりません。大量に悪意のあるコメントを投稿するスパム行為や、不正なWebサイトへ誘導する書き込みをされるなど、Webサイトの運用が困難となってしまうこともあるのです。

WordPressのセキュリティ対策方法

ここまで、セキュリティ対策を施さないままWordPressを運用する危険性をご紹介してきました。それでは、具体的にどのような対策方法があるのでしょうか。ここからはWordPressのセキュリティ対策方法として、簡単に行えるものから、導入するべきプラグインについて紹介します。

＜WordPress本体のセキュリティ対策＞
WordPress本体で行うセキュリティ対策としては、次の対策が挙げられます。順番に見ていきましょう。

・最新版へアップデートする
・SSLに対応する
・ベーシック認証を追加する
・接続するIPアドレスを制限する
・「wp-config.php」へのアクセスを禁止する
・バージョン情報を非表示にする
など

最初に、最も重要なこととして、WordPress本体のアップデートが挙げられます。WordPress本体は定期的にアップデートされており、アップデートの内容には脆弱性を修正するものも含まれているため、最新版へアップデートすることがとても大切です。

アップデートを対応した上で、サーバー側でいくつか対策できることがあります。

まずSSLですが、インターネット通信を暗号化する技術のため、IDやパスワード情報を盗まれないように、必ずSSL対応するべきです。

また、ベーシック認証の追加やIPアドレスの制限は、WordPressの管理画面へ接続できる人を制限でき、セキュリティ対策として有効です。ベーシック認証は簡単な認証方式ですが、WordPressの機能とは異なる認証を追加することで、セキュリティ

強度を高められます。サーバーにもよりますが、設定も簡単な場合が多いため、可能であれば設定しておきましょう。

これ以外に「wp-config.php」ファイルの設定も行うと良いでしょう。wp-config.phpファイルはWordPressの重要な設定ファイルであり、IDやパスワードも記載されているため、対策としては、ファイルの属性（パーミッション）を「400」に変更して、所有者以外のアクセスを禁止することになります。

最後に、WordPressには、「バージョン4.x.x」「バージョン5.x.x」などが存在しています。バージョン情報を知られると、脆弱性情報を知られることにつながります。そのため、バージョン情報は隠す設定に変更しましょう。

＜アカウントのセキュリティ対策＞
WordPressで利用するアカウントでは、次の点に注意することでセキュリティ対策となります。

・adminは利用しない
・アカウント名、パスワードを複雑にする
・管理者権限アカウントは最小限にする

adminアカウントはデフォルトのアカウントで、WordPressを利用したことのある人なら誰もが知っています。誰もが知るアカウントを利用すると、アカウントの乗っ取りリスクが高まるため、adminアカウントは利用しないようにしましょう。

WordPressでは任意にアカウントを追加できますが、アカウント名やパスワードは複雑なものを設定しなければなりません。なぜなら、簡単なアカウント名やパスワードは推測できるため、アカウントの乗っ取りリスクが高まるからです。

管理者権限のアカウントは、WordPress上での操作に制限がありません。管理者権限アカウントを乗っ取られると、あらゆる不正を許してしまうことになります。管理者権限アカウントが多くなるほど管理が難しくなるため、必要最小限の作成を心掛けましょう。

＜プラグイン・テーマのセキュリティ対策＞
WordPressの魅力の一つに、プラグインやテーマを導入すれば、簡単で自由にカスタマイズできることが挙げられます。これらの利用で、あなただけのWebサイトを作成できますが、プラグインやテーマを利用するときも、セキュリティ対策は意識しなければなりません。

・最新版へアップデートする
・公式サイトから公開されているものを利用する
・使用していないプラグインは削除する

WordPress本体と同様に、プラグインやテーマは定期的にアップデートされます。もちろん、その中には脆弱性に対応したアップデートも含まれているため、最新版へアップデートしましょう。

プラグインやテーマは、WordPressの公式サイト以外から入手することも可能です。公式サイトで入手できないものが公開されているので魅力的ではありますが、一方で不正なものも含まれているリスクがあります。そのため、利用する際は信頼できるWebサイトか確認する必要があります。セキュリティの観点からは、WordPressの公式サイトで公開されているものを利用するほうが望ましいでしょう。

WordPress本体だけでなく、プラグインにも脆弱性は含まれます。定期的にアップデートを行うことは当然ですが、使用していないプラグインは削除することも大切です。プラグインの数が増えるほど管理が大変になるため、できるだけプラグインの数を減らしてセキュリティ対策を行いましょう。

＜セキュリティ対策にお勧めのプラグイン＞
WordPressのプラグインの中には、セキュリティ対策を行うためのプラグインも存在しています。導入するだけでセキュリティ対策ができるものもあるため、お勧めのプラグインを紹介します。

All In One WP Security & Firewall
All In One WP Security & Firewallは、WordPressの総合的なセキュリティ対策ができるプラグインです。ログイン画面の変更やスパムコメントの制御などが行えます。

SiteGuard WP Plugin
SiteGuard WP Pluginは、WordPressの管理画面を強力に守るプラグインです。設定項目がすべて日本語で使いやすい特徴があり、ログイン画面の変更や接続元IPアドレス制限、日本語によるログイン認証が行えます。

Akismet
Akismetは、スパムコメントを制御するプラグインです。WordPress導入時に初めから導入されているプラグインです。スパムコメントだけでなく、不正なWebサイトへ誘導するようなコメントもブロックしてくれます。

紹介したプラグイン以外にも、セキュリティ対策として利用できるプラグインは存在しています。まずは、紹介したプラグインから導入し、さまざまなプラグインを試してみてはいかがでしょうか。

WordPressは狙われやすいのでセキュリティ対策を検討しよう

WordPressは世界中で利用されており、Webサイトの作成・運用を協力にサポートするツールです。しかし、ユーザーが多いことやオープンソースであることなどを理由に、攻撃者から狙われやすいツールでもあるため、セキュリティ対策が欠かせません。

あなたが作成・運用するWebサイトが被害に遭わないためにも、この記事で紹介したセキュリティ対策を試してみてはいかがでしょうか。

WordPressを安全に運用するためにはセキュリティ対策が必要なように、パソコンを安全に利用するためにはセキュリティ対策ソフトが欠かせません。

NTT西日本では、進化し続ける脅威に対して、セキュリティ対策を複合的に組み合わせた「セキュリティおまかせプラン」をご用意しています。このプランでは、ゲートウェイでの防御や、企業向けセキュリティ対策ツール、サポートセンターでの通信監視・復旧支援など、手厚いサポートで脅威から企業を守ります。

「セキュリティおまかせプラン」の詳細はこちらをご確認ください。

※本機能はセキュリティに対するすべての脅威への対応を保証するものではありません
※掲載している情報は、記事執筆時点のものです