ご確認事項⑤

ー	種類	内容
1	悪用	プログラムが潜在的に抱えている問題を悪用し、作者の意図しない方法で使用する。
2	書き換え（置き換え）	プログラムが潜在的に抱えている問題を悪用し、作者の意図しない方法を用いてプログラムを書き換える。
3	破壊	プログラムが潜在的に抱えている問題を悪用し、作者の意図しない方法を用いてプログラムを破壊し、使用できない状態にする。

どのような手法を使って悪用するのか？

コメントスパム

公開している内容と関係のない文字列がコメント欄に投稿され、ホームページへ大量に登録されてしまうことをコメントスパムと呼びます。
コンテンツそのものへの影響はありませんが、1 ページへの登録件数が万単位になると、サーバ負荷が高まり、自身だけではなく同サーバを利用しているユーザのコンテンツの表示も遅延することがあります。

管理画面の悪用

WordPress の管理画面は wp-login.php というプログラムファイルを中心に構成されています。悪意のある第三者は不正な文字列をサーバへ送信することでプログラムの脆弱性(ぜいじゃくせい)を利用し、管理画面へログインします。このような状態となった場合、悪意のある第三者は WordPress のすべての機能を使用することができます。

プラグインの悪用

WordPress は「プラグイン」と呼ばれる拡張機能があり、有志や愛好家が公開しているプログラムを追加することができます。悪意のある第三者は不正な文字列をプラグインとなるプログラムに対して送信することでプログラムの脆弱性(ぜいじゃくせい)を利用し、不正なアクセスを行います。影響度は脆弱性の程度によって差があるものの、多くの場合、管理者が意図しないファイルを設置されます。

Pingback 機能の悪用

WordPress には自身のホームページに対する言及を第三者のホームページ上で行われた場合、そのことを通知する、「Pingback」という仕組みがあります。この仕組みを悪用されたとしても、自身のホームページを書き換えられることはありませんが、知らないうちにどこかのサーバへの攻撃に加担してしまう可能性があります。

ブルートフォースアタック / 辞書攻撃

ランダムな文字をプログラム的に作り出して何度もアクセスを試み、認証を突破することを「ブルートフォースアタック」もしくは「辞書攻撃」と呼びます。突破された場合、管理者が意図して公開を制限しているファイルを閲覧されたり、WordPress のすべての機能を使用することができてしまいます。

対策

『All In One WP Security & Firewall(AIOWPS)』を使ってセキュリティを強化する

「さくらのレンタルサーバ」や「さくらのマネージドサーバ」の「クイックインストール」からインストールを行った WordPress はいくつかのプラグインを予めインストールしていますが、そのうちのひとつである『All In One WP Security & Firewall(AIOWPS)』はセキュリティ強化に効果的です。
以下、『All In One WP Security & Firewall』の中でも比較的容易に導入可能な項目をご紹介します。

(1)WordPress のセキュリティの脆弱性について

サイト公開後の更新や機能の追加がしやすいことから、内容や規模の大小問わずさまざまなサイトに使われている WordPress。
オープンソースの CMS である性質が利便性という大きな恩恵を生む反面、セキュリティ面で大きなリスクを背負っています。

それはなぜでしょうか。
オープンソースとはソースコードが一般に公開されている状態を指します。
コードが理解できれば誰にでも新たなプログラムが開発できます。
インストールをしただけのデフォルト状態では味気ないサイトでも、いくらでもカスタマイズを加えら

れます。
これらはつまり、悪意のある第三者が簡単にサイトを不正に改ざんしてしまえる危険性をはらんでいるとも言えます。

DDoS 攻撃、サイトを構成するファイルの改ざん、アカウント乗っ取り、スパムコメントの投稿など、脆弱性が多く見られることから、ハッカーなどの標的にされやすいことから、WordPress にはセキュリティ面でリスクが高いとされています。

(2)WordPress サイトのセキュリティ対策ポイント・基本編

WordPress でサイトを構築するにあたり、最低限やっておきたいセキュリティ対策のポイントを挙げます。

・バックアップをとっておく
最悪、サイトが書き換えられてしまった時のために、元の状態に戻せる状態にしておくことです。
改ざん被害に遭わなくても、サーバ障害に見舞われることもあります。
WordPress を利用する・しないに関わらず、最新の状態のバックアップをとっておくことは基本中の基本です。

・利用するテーマやプラグインは、WordPress 公式のものを利用する
開発者や出処が不明なサードパーティーからリリースされるものは極力使わないのが賢明です。
どうしても利用したいのであれば、評判をよくリサーチし、安全性を確認してからにしましょう。

・WordPress 本体、テーマ・プラグインは、最新版にしておく
どのソフトや OS でもそうであるように、WordPress も脆弱性が見つかればその対策を施したアップデートを行います。
常に最新の状態に保っておくことで、第三者の改ざんや乗っ取りを極力防げます。

(3)WordPress サイトのセキュリティ対策ポイント・応用編

基本的なセキュリティ対策を施したとしても、WordPress サイトがオープンソースである以上、常にハッカーが隙を狙っていると考え、改ざんや乗っ取りに対して万全な対策を講じることが求められます。
ここでは応用編として、さらにセキュリティを強固にする代表的な対策方法を挙げます。

・手動インストールしよう
レンタルサーバなどの提供する「簡単インストール」はできれば避けましょう。
便利な機能のひとつではあるのですが、自動でインストール作業が行われるため、データベース名やサイトを構成するファイルがどのサイトとも共通となってしまうのです。
これはハッカーに書き換えてくださいと言っているようなもので、ハッキングのお膳立てをしてしまうのと同じです。

・データベースのテーブル名の頭につく接頭辞を変更しよう
手動インストール作業の途中で、データベースのテーブル名に任意の接頭辞を付けることができます。
独自のテーブル名をつけることにより、データベースを書き換えられる可能性がぐっと低くなります。
インストール後もテーブル名を変更するプラグインを使うことで対応可能です。(もちろん安全な公式プラグインです)

・「wp-config.php」を、アクセスに制限をかけておこう
「wp-config.php」とはインストール作業の過程で作成されるファイルで、サイトのさまざまな設定の詳細、やデータベースへの接続情報など、WordPress サイトの肝となるものです。
これに第三者がアクセスできる状態は好ましくありませんので、アクセス不可の設定を施しましょう。