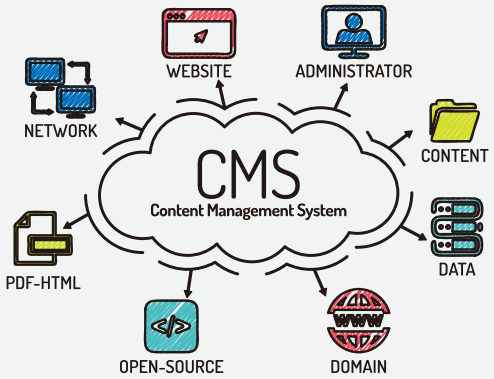
Web サイトの CMS 使用リスク

CMS(Content Management System)

- HTML や CSS などの専門知識不要
- オープンソースや、有料クラウドサービスなどがある
- Web ブラウザやメールで簡単に更新可能
- 低コストで導入できるが、セキュリティリスクもある



WordPress のバージョンアップ

WordPress 本体
PHP
MySQL(SQLite)
テーマ
プラグイン

Web での情報発信を迅速に行えるよう比較的容易に Web サイトの構築や、Web ページの更新を行うことができる CMS (Content Management System) は、Web サイトの約半数を占めるほど成長してきました。
たとえば、世界の Web サイトの約 3 分の 1 は、シェア No.1 である WordPress によって作成されております。
WordPress の良さは、基本無料で使用でき、HTML や CSS の技術ノウハウが無い人でも Web サイトが構築できます。そして、現場の担当者が Web ブラウザやメールから、Web ページの更新ができ、従来専門技術者しかできなかった Web 修正がとても簡単に行えます。
WordPress は、有料もありますが、無料のテーマやプラグインがとても沢山存在しているため、かっこいいデザインや様々な機能追加を自社の Web ページに施すことが簡単にできます。
こうしてみると、良いこと尽くめに見えますが、個人はもちろん多くの企業でも採用されているがゆえ、悪意を持った第三者にも狙われています。今でこそ、WordPress のセキュリティはかなり強化されてきましたが、昔は、ID とパスワードのみの管理だったため、多くの人が" admin" という ID と覚えやすいパスワードで管理者設定してしまい、攻撃者に乗っ取られて大量のスパムメールを送信する踏み台に利用されるなど、様々な被害が増大しました。
WordPress は、MySQL などのデータベースを利用して PHP で開発されたブログ向けのオープンソフトウェアです。そのため、WordPress 本体や、プラグインの脆弱性を悪用して攻撃され、マルウェアに感染して情報漏洩してしまうケースもあります。
脆弱性に対処するためには、WordPress 本体と、テーマやプラグインを最新にしておく必要がありますが、それには、PHP や MySQL も含めたそれぞれのバージョンとの相性も関係し、動かなくなってしまうことが多いです。また、機能追加のために、テーマにある PHP のソースに追加変更をしてしまっている場合なども、テーマをバージョンアップすると Web ページに不具合が出るため、あえてバージョンアップしないまま使用を続けることが多いです。
こうなると、脆弱性があるリスクは避けられないため、他のセキュリティ対策のみに依存することになりかなり危険です。
企業や団体において、マーケティングや E コマースなど Web サイトの重要性はますます高まっておりますが、利便性を求め WordPress などを利用すると、その分セキュリティリスクは高まってしまうということを認識する必要があります。