GMO PRIME STRATEGY

初心者向けWordPressの改ざん傾向と原因と今すぐできる対策

GMOプライム・ストラテジー株式会社

代表取締役社長　吉政 忠志

GMO INTERNET GROUP

代表取締役 吉政忠志のプロフィール

GMOプライム・ストラテジー株式会社　代表取締役 社長

OSSコミュニティ活動

Python エンジニア育成推進協会　代表理事

PHP技術者認定機構　理事長

主な職歴

- Linuxコンソーシアム副会長（7期）
- 経済産業省外郭団体IPA専門委員（2期）
- 文部科学省XML教育推進委員（2期）
- Novell Japan、SAP Japan、Asteria社などでマーケティング・営業部門の責任者を歴任

その他

- 日本赤十字社より勲章を授与
- 東京パラリンピック　東京都最終聖火ランナー
- ロードバイクの旅、47都道府県走破　2025年4月
- ロードバイクの旅、日本縦断3418km走破　2025年8月

GMOプライム・ストラテジーとは

GMO PRIME STRATEGY

当社はインターネット上でコンテンツを提供する
サーバ（Webサーバ）のOS「KUSANAGI」を開発するメーカーです。

「KUSANAGI」は超高速の性能を持ち、セキュリティの高さが評価され、
世界の主要なクラウドサービス上で利用されており累計稼働台数は10万台に達しています。

「KUSANAGI」は全世界のWebサーバの61.0%*で稼働しているCMS
（WordPressは全体の43.5%で稼働*）に強いOSです。

＊引用元 https://w3techs.com/technologies/overview/content_management (2025/7/9現在)

会社概要

社名

GMOプライム・ストラテジー株式会社
英文社名：GMO PRIME STRATEGY CO., LTD.

設立年月日

2002年12月2日

インターネット系の
会社としては老舗です

所在地

〒102-0082
東京都千代田区一番町８番地 住友不動産一番町ビル１階

代表取締役

代表取締役　吉政忠志

従業員数（連結）

28名（2025年11月末）

スタンダード市場上場企業としては
かなりコンパクトな社員数です

資本金

453,798千円（2025年11月末）

AIや自動化で業務が効率化
されている会社です

事業領域

KUSANAGI Stackの開発と提供
- 超高速CMS実行環境「KUSANAGI」
- 高速化エンジン「WEXAL Page Speed Technology」®
- 戦略AI「ONIMARU® David」

KUSANAGI Stack事業
- KUSANAGIマネージドサービス
- クラウドインテグレーションサービス
- ライセンス販売

KUSANAGIはWebサーバーを
超高速化しセキュリティを高めるOSです。

主要株主

GMOインターネットグループ株式会社

連結子会社

PRIME STRATEGY NEW YORK, INC.
（米国ニューヨーク州）

お知らせ

■KUSANAGIサミット　6月27日開催

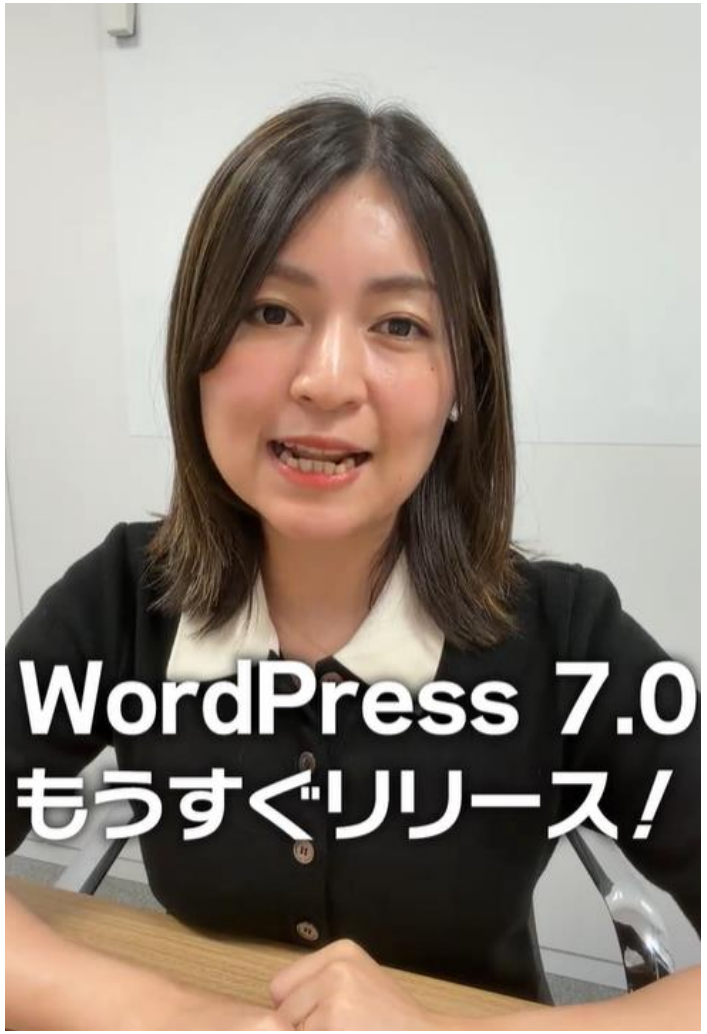
写真撮影どうぞ！

学べるすんごいYouTubeチャンネル登場

www.youtube.com/@WebTipsChannel_KUSANAGI

TikTokはじめました

https://www.tiktok.com/@gmoprimestrategy/



WordPressを260倍高速化し
コストを最大で1/4にする
KUSANAGIとは

「KUSANAGI Stack」

すべての過程で高速化する市場唯一の製品群

KUSANAGI Stack

超高速CMS実行環境「KUSANAGI」
高速化エンジン「WEXAL Page Speed Technology」
戦略AI「ONIMARU David」

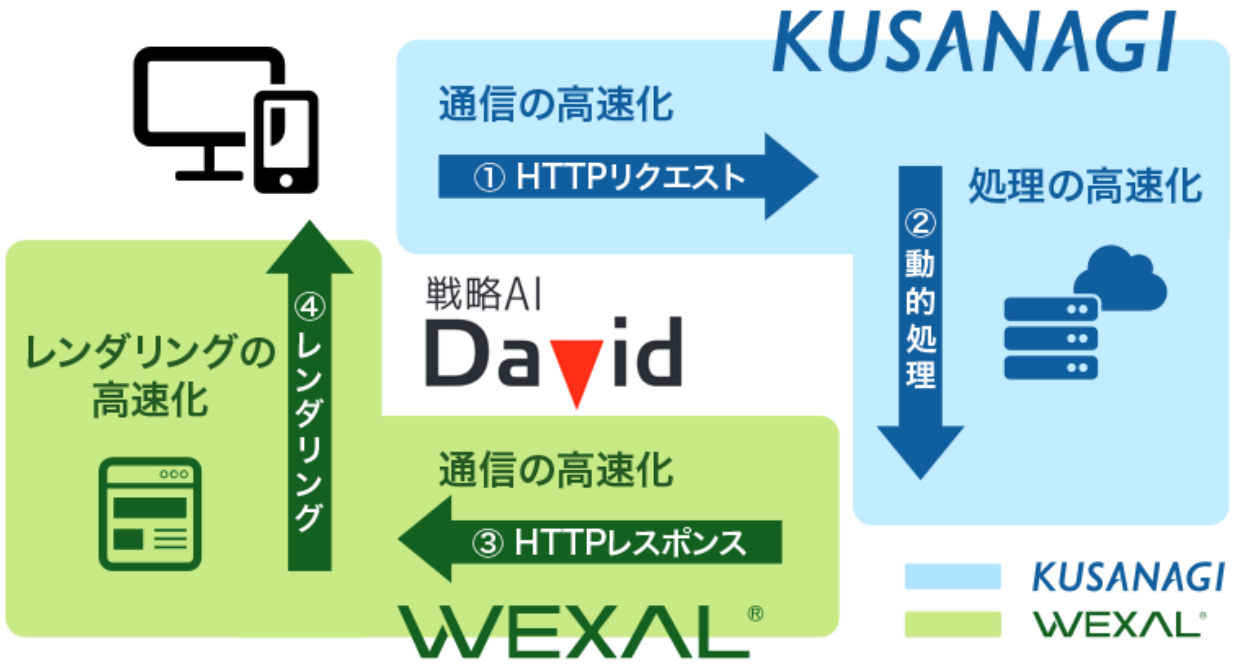
日本国特許第7523733号
日本国特許第7530383号
米国特許 US 12,111,876 B2
＊米国特許出願・審査中

26プラットフォームで展開 ※1
累計稼働台数10万台 ※2

※1：2025年５月現在
※2：2025年６月現在

SPEED & SECURITY & COST

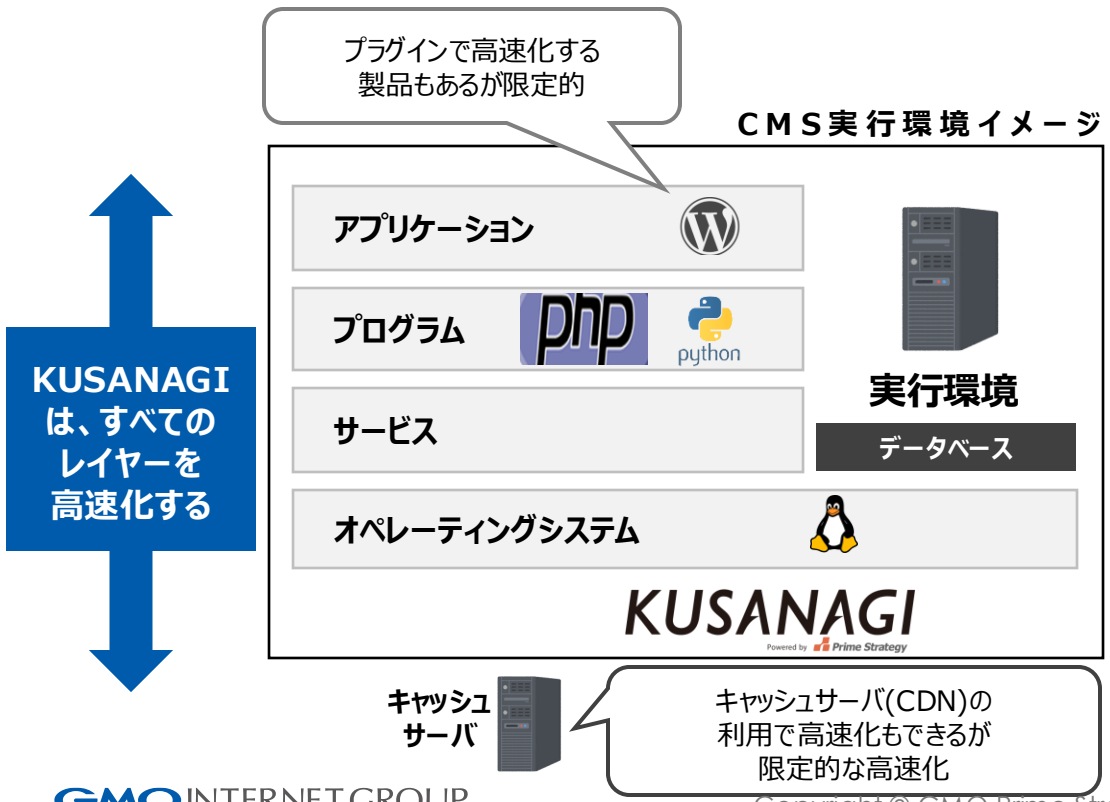
画面表示するまでのすべての過程を高速にチューニング

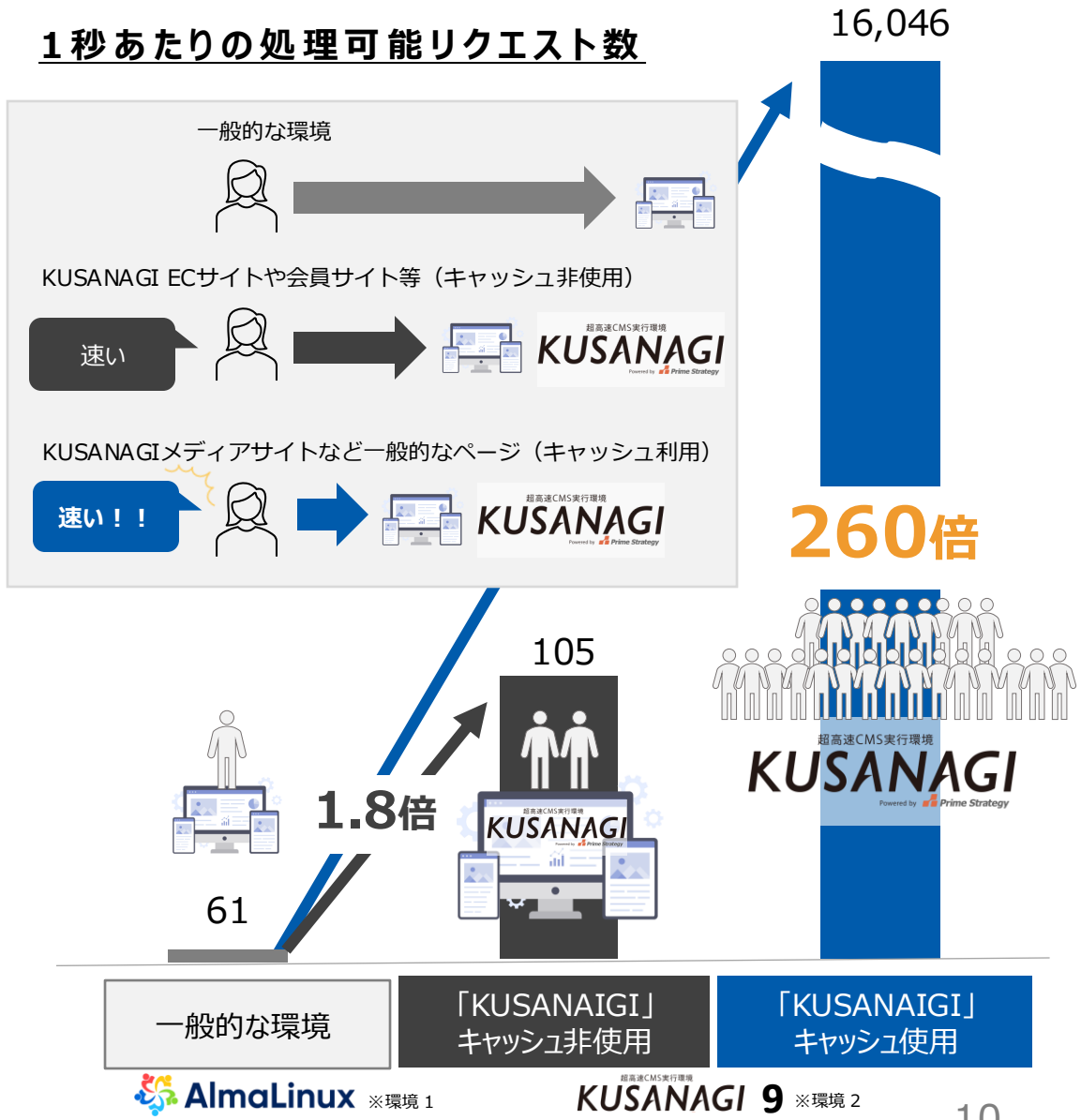


「KUSANAGI」のパフォーマンス

GMO PRIME STRATEGY

WordPress/CMSに特化した
超高速チューニングと
セキュリティ強化のチューニングを
以下の組み合わせで行っているOSが
「KUSANAGI」です。





GMO INTERNET GROUP

※環境1 AlmaLinux 8.8
Microsoft Azure Standard D4as_v5インスタンス (3.24Ghz AMD EPYC 7763 プロセッサ 4vCPU, 16GiB), Premium SSD LRS, 東日本リージョン, PHP 8.0.30, Nginx 1.20.1, MariaDB 10.5.22, WordPress 6.4.2
*環境2 KUSANAGI 9.4.8-1
Microsoft Azure Standard D4as_v5インスタンス (3.24Ghz AMD EPYC 7763 プロセッサ 4vCPU, 16GiB), Premium SSD LRS, 東日本リージョン, PHP 8.0.30, Nginx 1.25.3, MariaDB 10.5.23, WordPress 6.4.2

KUSANAGIはなぜ速くて、コストが低減できるのか？

1 OS・ミドルウェアの徹底最適化

- **OS層**
  不要サービス停止・リソース最適化
- **PHP**
  OPcache・JITで処理高速化
- **Nginx + PHP-FPM**
  Brotli圧縮・HTTP/2,3対応
- **MariaDB**
  Query Cache・メモリ活用でI/O削減
- **WordPress特化**
  翻訳・テーマアクセラレーター

2 重層的なキャッシュ戦略

fcache（Nginxレイヤー）

PHP・DBアクセスを完全バイパス
秒間 **80,000件以上** の処理対応
レスポンス **8ms以下**

bcache（WordPressレイヤー）

DBにキャッシュ格納・クエリ削減
別サーバー分離でスケールアウト対応

3 実測パフォーマンス

最大 **260倍**
キャッシュ利用時
標準OS比のスループット向上

約 **2倍**
キャッシュなし
最適化設定のみでも高速化

TCO最大 **1/4**
インフラコスト削減
CPU 1/2・メモリ 1/4のVMで
ハイエンドサーバー同等性能

「WEXAL Page Speed Technology」「David」

［ウェクサル］
WEXAL®
Page Speed Technology

「**WEXAL Page Speed Technology**」は、Webシステムのための「高速化エンジン」。
ブラウザ表示の自動チューニングを実施し、UX（ユーザー体験）の向上を実現します。

メリット 1

戦略AI Davidによる最適化戦略の自動生成

戦略AI Davidがエンジニアに代わってブラウザの環境に合わせてページごとに最適化戦略を自動生成

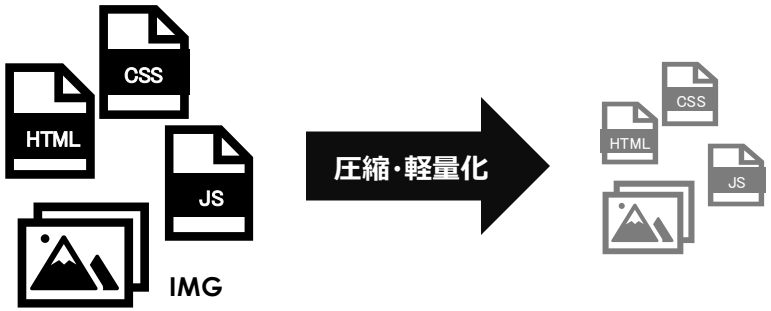
戦略AI David
自動最適化

エンジニアが最適化に悩む必要はない

メリット 2

リソース最適化による高速化と転送量の削減

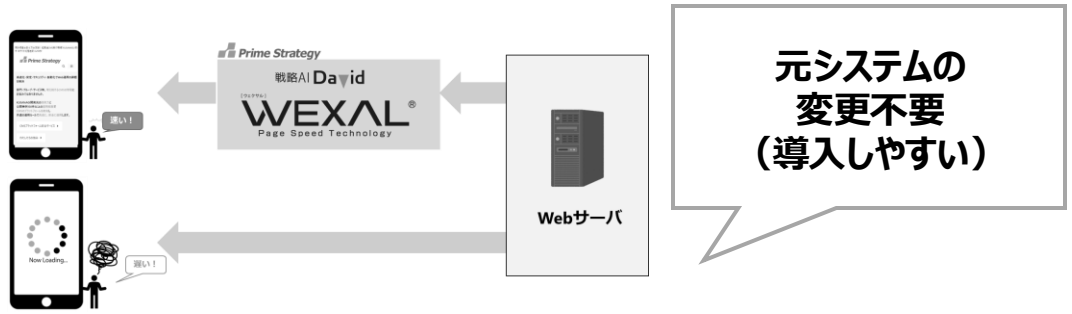
画像やJS、CSSのリソースを圧縮し、軽量化する。リソースの最適化により、表示の高速化だけではなく転送量を削減します。



メリット 3

オリジナルデータの改変なし

オリジナルのリソースやプログラム、データベースに保存されているデータなどの改変は行わない。



KUSANAGI＋WEXAL＝KUSANAGI Premium Edition

GMO PRIME STRATEGY

■特徴

> WordPressだけでなく、LinuxベースのWebならなんでも爆速
> CDN、チューニング、KUSANAGI Premium Edtionの3択へ

■詳細は

> https://kusanagi.tokyo/edition_and_upgrade/kusanagi-premium-edition/

■主な稼働環境

> AWS、Azure、さくらVPS　に加え、、、、

■どれだけ速くなるかの確認サイト

> https://www.o20.jp/

お勧めは！

写真撮影どうぞ！

手順解説動画

■このとおり行えば15分で世界最速クラスのWordPress爆誕

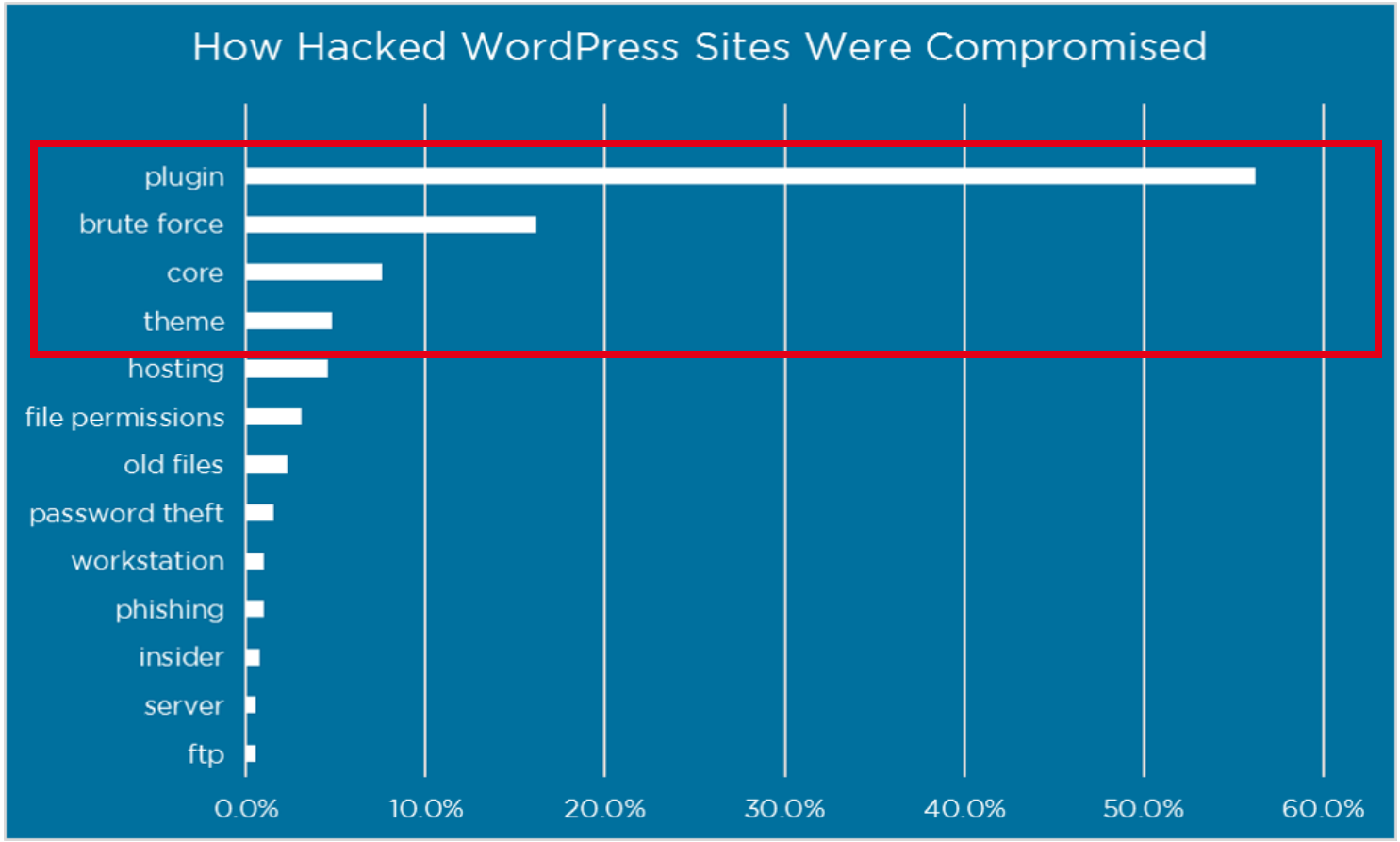
https://youtu.be/k0R4jV0J6Zs

写真撮影どうぞ！

ハッキングの原因と
今すぐできる対策

WordPressサイトのハッキングの原因

WordPressサイトのハッキングの原因の60%以上が、プラグインやテーマの脆弱性によるもの
WordPress本体（Core）、プラグインやテーマの脆弱性対策をすることで、**ハッキングのリスクを大幅に軽減**できる
あわせてブルートフォース攻撃（管理画面への総当たり攻撃）への対策をおこなうことも有効



https://www.wordfence.com/blog/2016/03/attackers-gain-access-wordpress-sites/

最新版を利用しているのはわずか47%

14. 47% of WordPress installations use the latest version of WordPress.

It's important to check what version of WordPress you're using. Outdated version of WordPress can leave you vulnerable to exploits. According to statistics on WordPress.org only 47% of users are using the latest WordPress version of WordPress.

Operating on an outdated version means missing out on new features and critical security updates. These updates often fix vulnerabilities that hackers could exploit, securing your site.

Thus, if you're not using WordPress's latest version, you must update immediately. Doing so gives you the latest features for optimal website performance and strengthens your site's security.

Always keep WordPress updated for website security. For a smooth and safe user experience, your website must be reliable and have the latest features.

https://smartwp.com/wordpress-statistics/

なぜ最新にアップデートできないのか

GMO PRIME STRATEGY

■主に以下の原因があります

- > カスタマイズがあり、バージョンアップにコストと手間がかかる
- > プラグインが多すぎて、バージョンアップにコストと手間がかかる
- > 詳しい人がいなくなり、バージョンアップを行うにはまず調査から行わないといけなく、さらにバージョンアップにコストと手間がかかる
- > 責任分担が不明確な個所があり、調整が必要になり、さらにバージョンアップにコストと手間がかかる
  - > OSやミドルウェアはA社が保守をしているが、WordPressはコンテンツ管理しか依頼していなく、WordPressの保守やカスタマイズ部分やプラグインの保守までは担当している人がいない
- > 構築時はチェックしていても、その後のバージョンアップを担当する担当が不在（意外に多いです）

KUSANAGIマネージドサービス、KUSANAGI Security Editionにお任せください！

バージョンアップは月何回が良いのか

GMO PRIME STRATEGY

■バージョンアップは月1回というところが多いです。

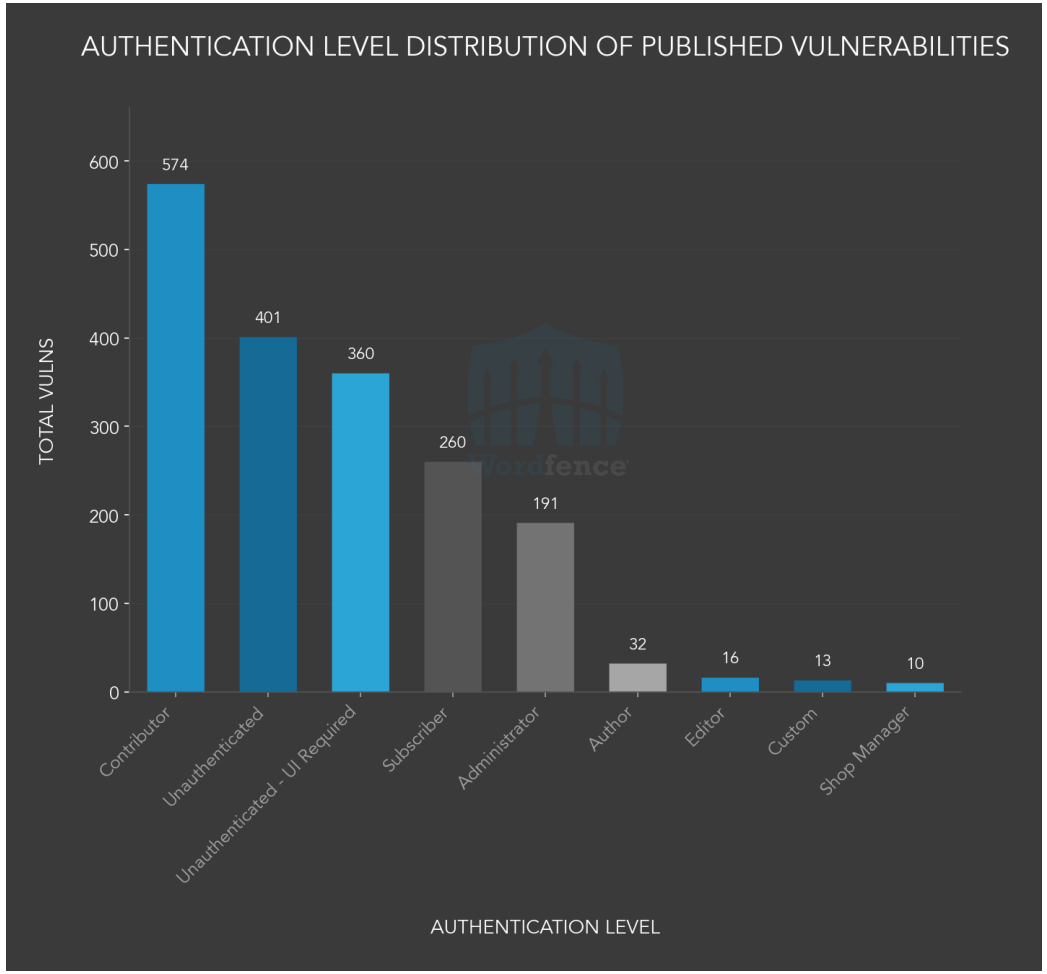
■月1回もしていない会社もあります。

■数世代前のOS、ミドルウェア、WordPress、プラグイン、テーマの状態から最新版にアップするのは、かなりのリスクとコストがかかります。

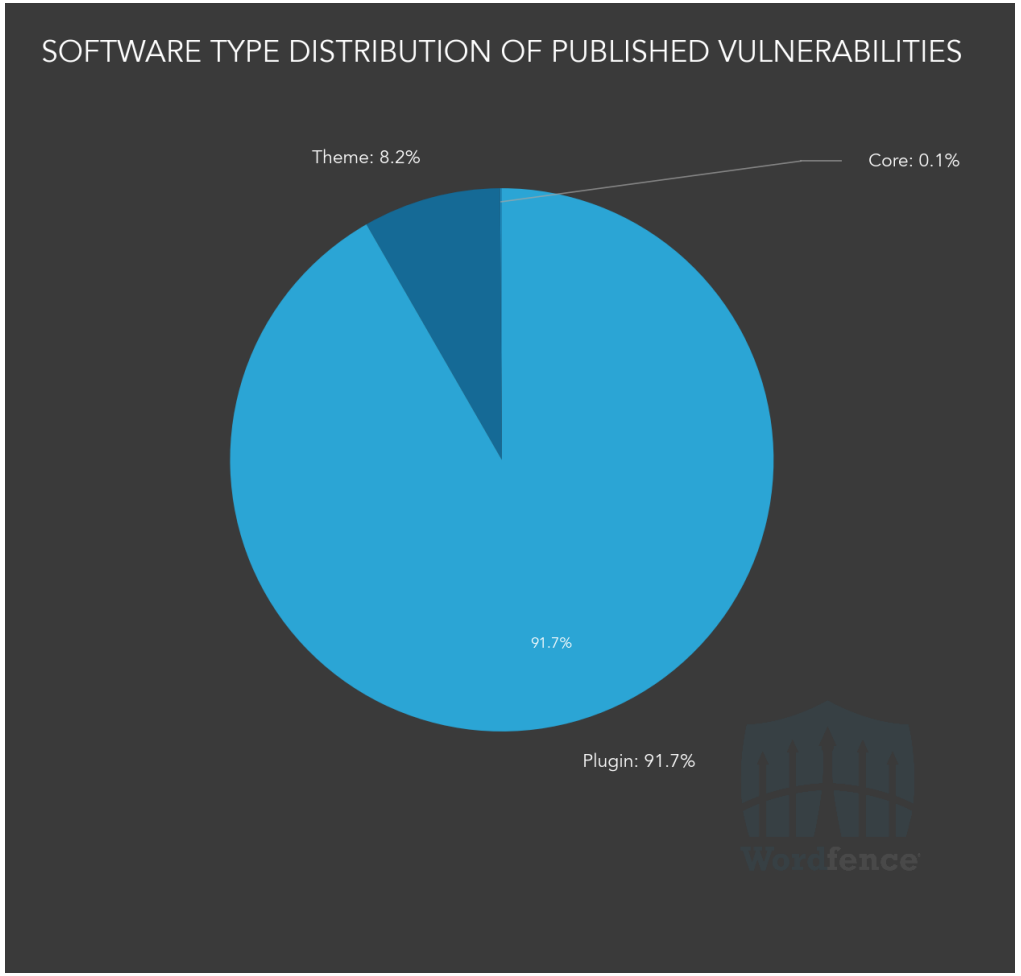
Wordfence2025年3Qのレポートを読み解く

https://www.wordfence.com/blog/2025/10/quarterly-wordpress-threat-intelligence-report-q3-2025/

脆弱性の傾向



第3四半期に公開された脆弱性のほとんどは、
悪用するためにコントリビューターレベルのアクセスが必要

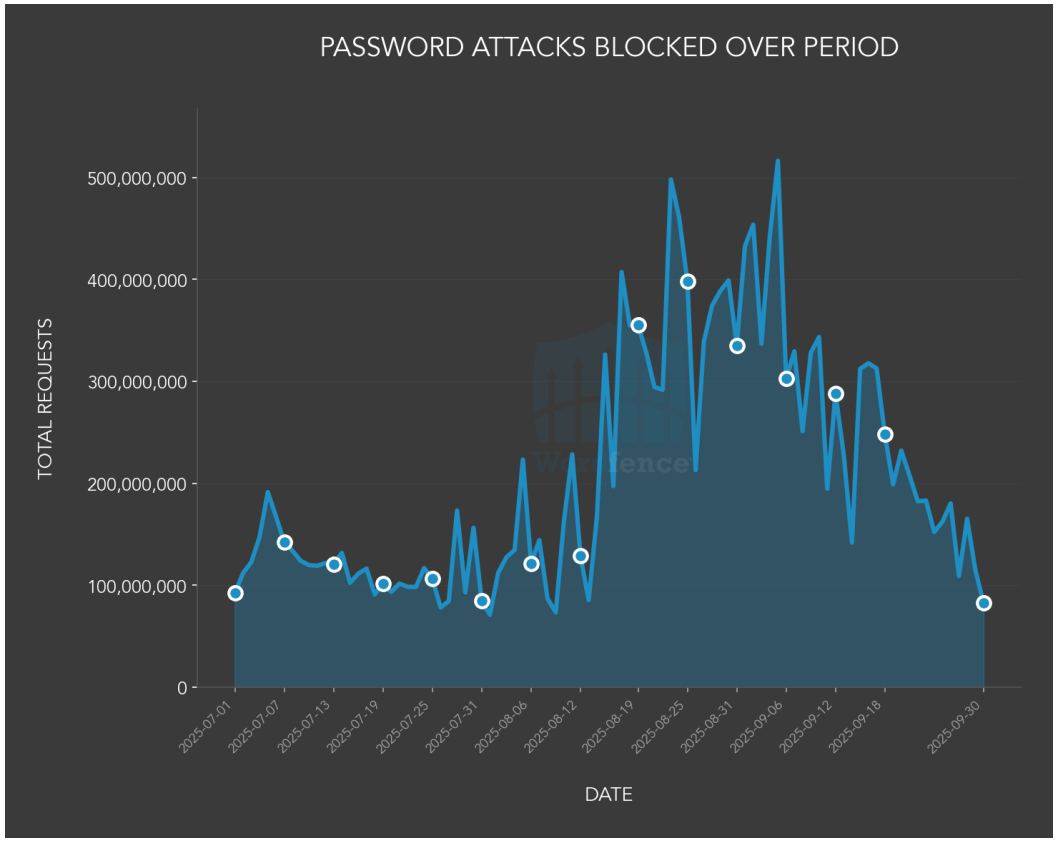


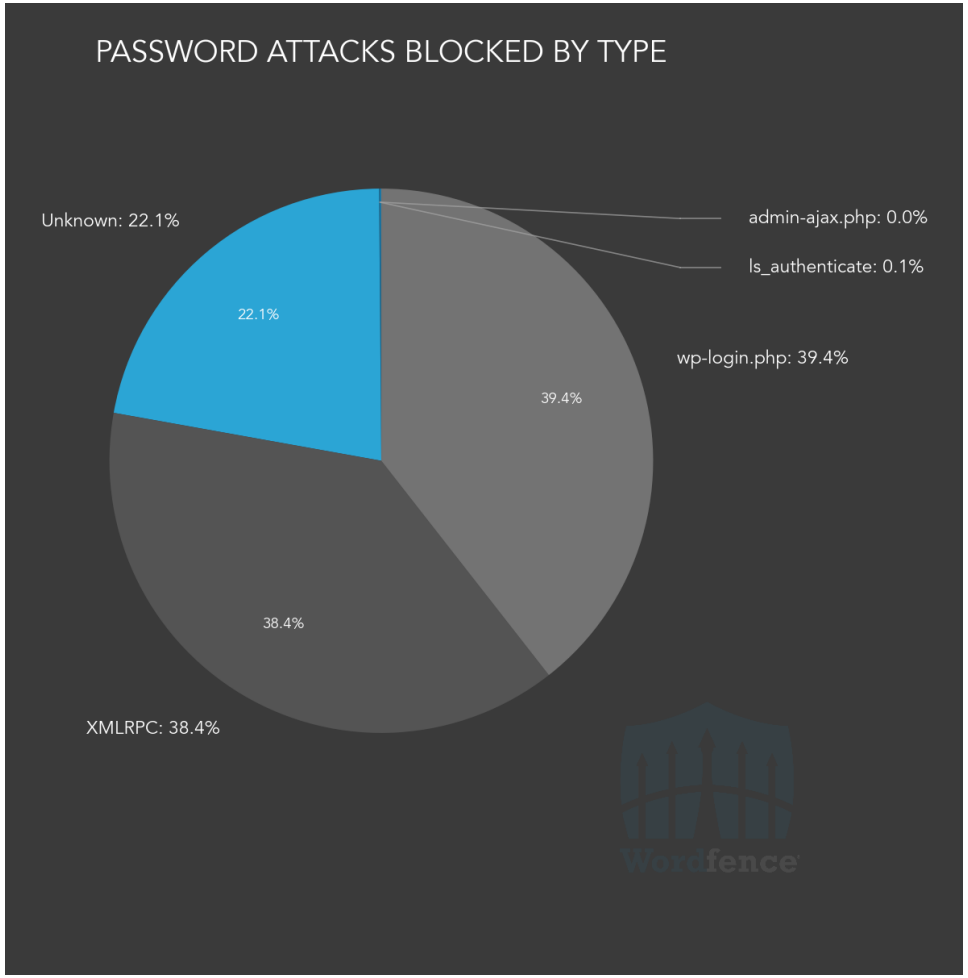
脆弱性の大部分はプラグイン関連の脆弱性

パスワード攻撃

ブロックしたブルートフォース攻撃

192億

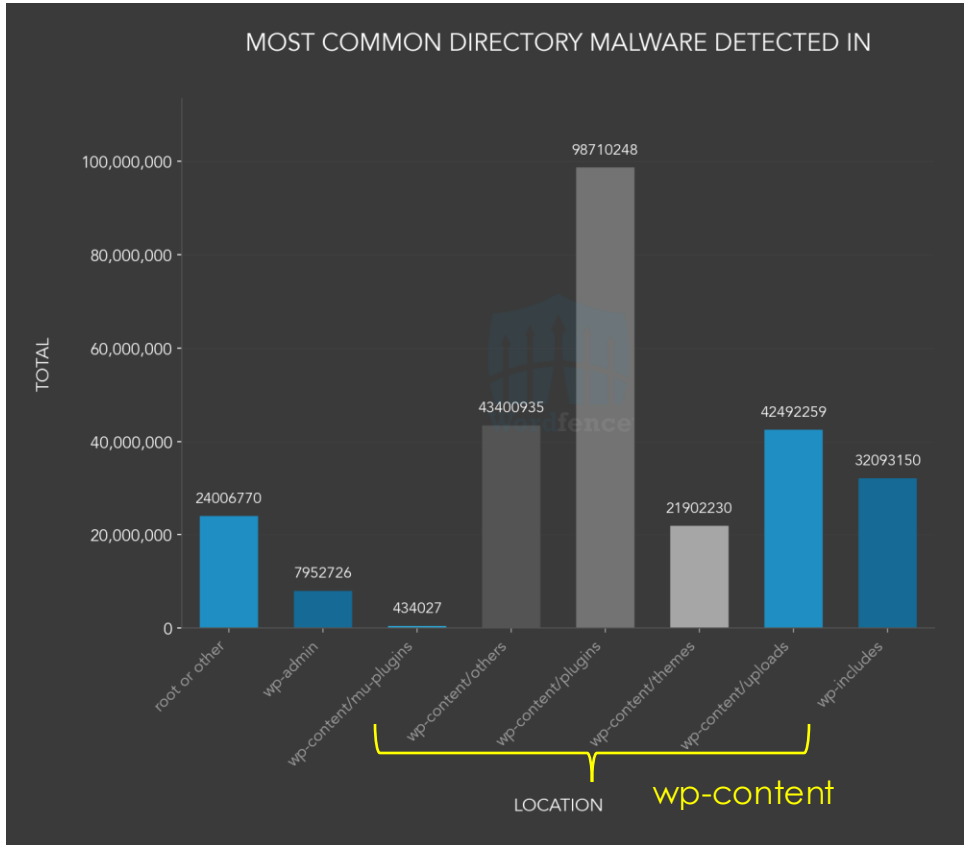




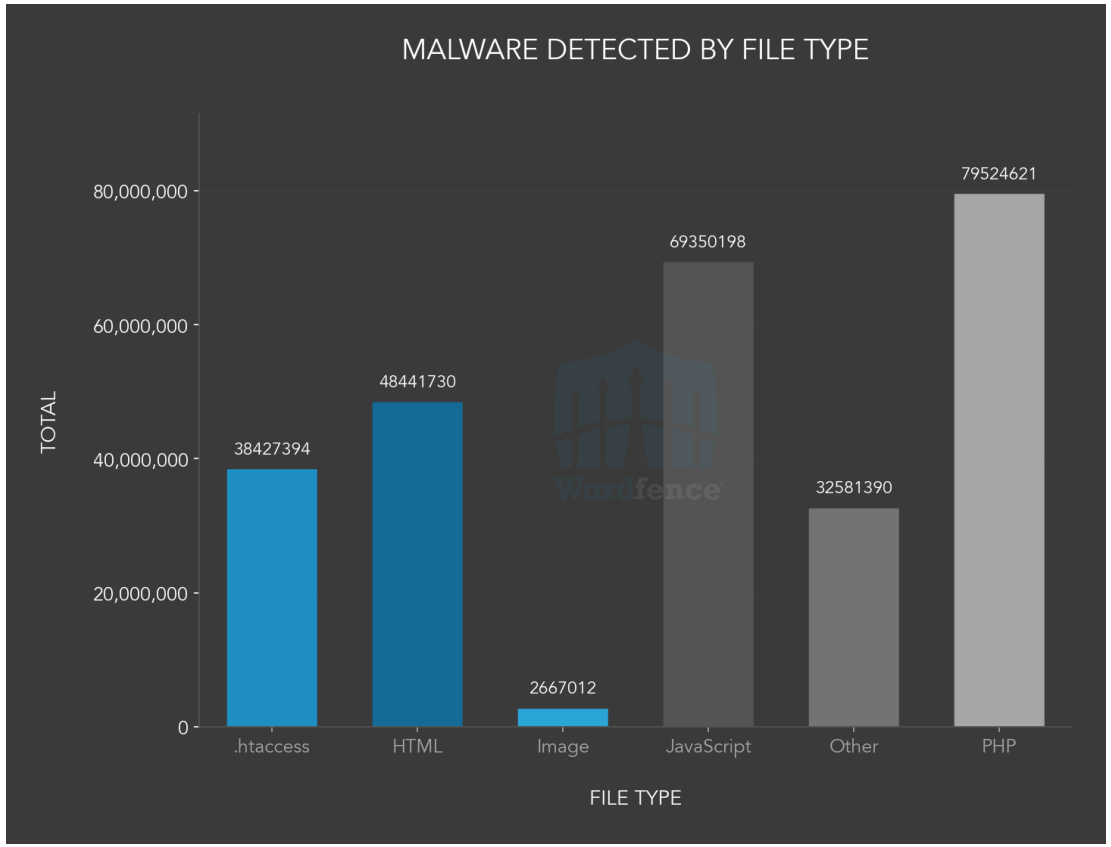
管理画面を隠すだけでは不十分
wp-login.phpとXMLRPCに対する攻撃は同じくらい

マルウェア攻撃

マルウェアの見つかったサイト　**495K**
サイトあたりの平均感染ファイル数　**62.2**
サイトあたりの平均マルウェアのバリエーション　**2.6**



マルウェアが最も頻繁にアップロードされる場所は
プラグインディレクトリ

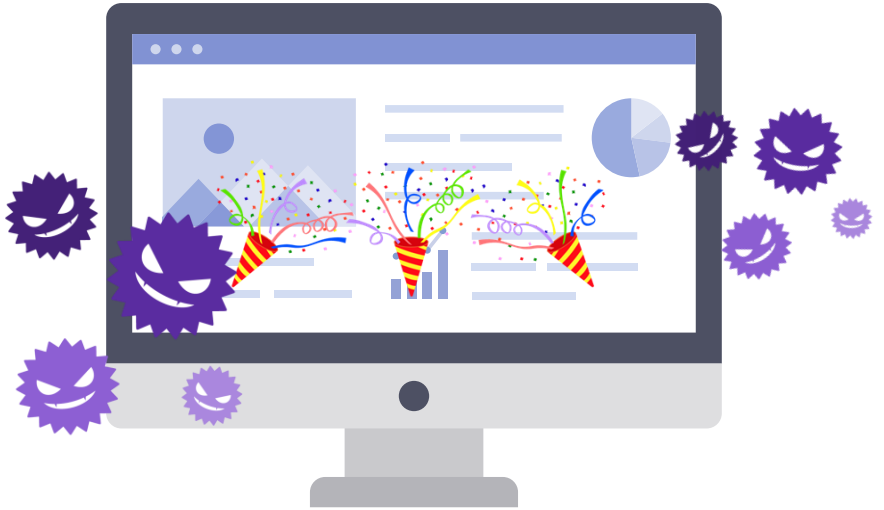


PHPファイルはWebシェル、バックドアなどと関連付けられることが多く、JavaScriptやHTMLなどのファイルはスパムと関連付けられることが多い

WordPress×企業セキュリティの落とし穴
～実録ヒヤリハット事例～

インシデント事例 - 改ざんの実態

WordPress管理画面への侵入



■攻撃者が管理画面から侵入
■ヘッダーなどにコードを挿入するプラグインを設置
■不正なサイトへ誘導したり
　不正な広告を表示したりするスクリプトを挿入

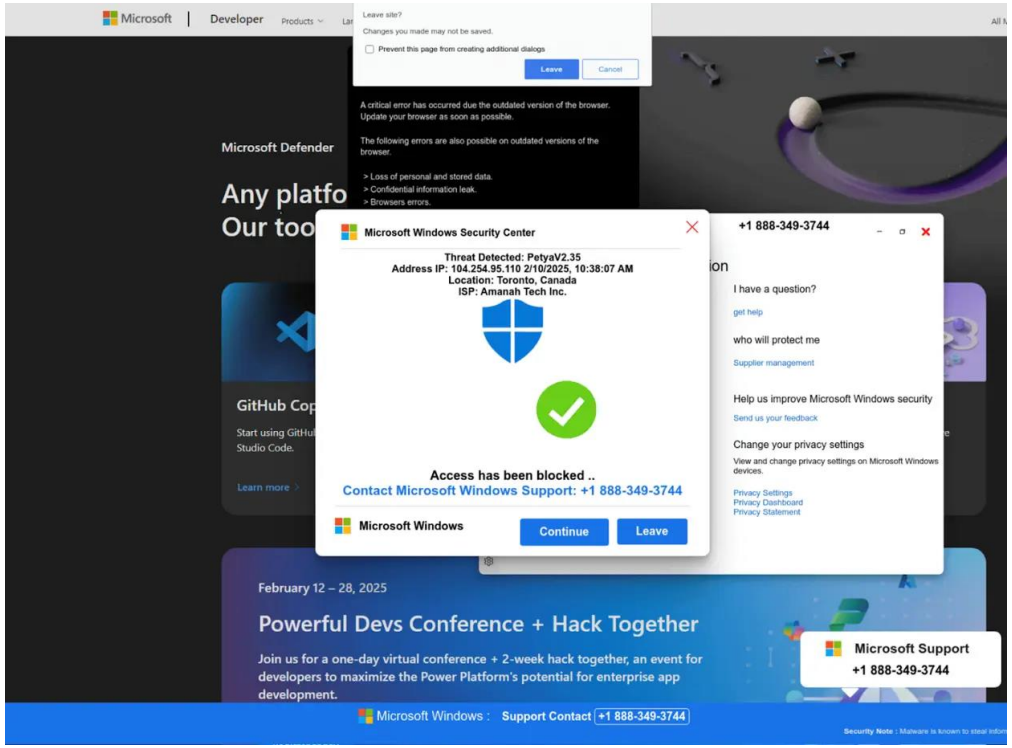
既存ユーザーを利用し実際の運用に近い動きで改ざんが行われた。
さらに不正な表示もランダムだったため、発見まで時間がかかった。

ShadowCaptcha：WordPress悪用キャンペーン

改ざんされた WordPress サイトから偽の CAPTCHA ページへ誘導し、ユーザー操作を利用してランサムウェア・情報窃取・暗号通貨マイナーを感染させる攻撃。

1. WordPress サイトに悪意のある JS を埋め込み。
   偽 CAPTCHA へリダイレクト
2. 「確認のためクリック／保存・実行」を誘導
3. 実行によりマルウェア配布

ソーシャルエンジニアリング中心。
ユーザーの自己判断操作を悪用。



対策

- WordPress／プラグインを常に最新に
- 管理者アカウントに MFA を導入
- 改ざん検知・WAF の活用
- 「偽 CAPTCHA」等の注意喚起と実行制御

ShadowCaptcha Exploits WordPress Sites to Spread Ransomware, Info Stealers, and Crypto Miners
https://thehackernews.com/2025/08/shadowcaptcha-exploits-wordpress-sites.html

インシデント事例 - 見逃されたバックドア

GMO PRIME STRATEGY

不正に作成されたユーザーを削除したにもかかわらず繰り返される改ざん

■バックドアユーザーを作成するプラグインの設置
■テンプレートにバックドアユーザーを作成する
　コードの埋め込み

```
function create_admin_account(){
$user = 'xxxxx';
$pass = 'xxxxxx';
$email = 'xxxxxx';
if ( !username_exis
&& !email_exists(
$user_id = wp_crea
$email );
$user = new WP_User( $us
$user→set_role( 'admin
 } }
add_action('init','cre
```

WordPressの正式なコードで書かれていたため、
クリーニング作業時にも見逃され、再侵入を許す事になった。

WordPress「mu-plugins」悪用のリスク

GMO PRIME STRATEGY

■攻撃者が WordPress サイトに侵入後、mu-plugins フォルダ内にマルウェアを設置
■自動実行され、管理画面では見えない。
■永続的なバックドアやスパム拡散に悪用される
■バックドア、web シェル、SEO スパム、トラフィックのリダイレクトなど、幅広い悪用
■多くのセキュリティツールがこのフォルダを監視対象外としているため、検知が遅れやすい。

対策

- mu-plugins フォルダを定期的に監査
- 不要ならフォルダごと削除・再生成されないよう管理
- セキュリティスキャン対象に mu-plugins を含める設定
- ホスティングや運用担当者は、この仕組みを把握して対処

「見えない場所に仕込まれる」ことが最大のリスク。

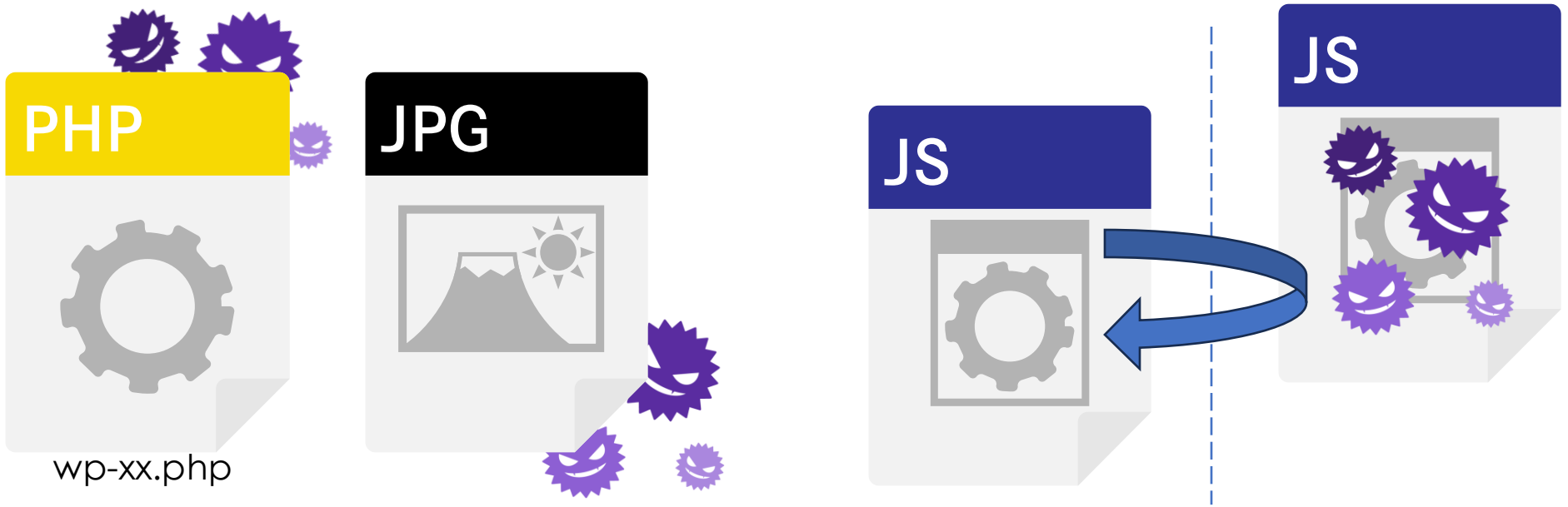
Risky Bulletin: Hackers abuse secret WordPress feature you'll probably want to disable
https://news.risky.biz/risky-bulletin-hackers-abuse-secret-wordpress-feature-youll-probably-want-to-disable/

インシデント事例 - 偽装ファイルの設置

GMO PRIME STRATEGY

単純な検索ではわかりにくい偽装ファイルの設置

■CMSを構成するファイル名に酷似したファイルを設置
■画像（jpg）拡張子の偽装ファイルを設置し、スクリプト（PHP)から読み込む
■PHPやJSなどに外部のJSをインクルードするコードを設置



インシデント事例 - 管理画面の甘い設定が命取り

守るべき管理画面はCMS以外にもある

■クラウドの管理画面に侵入、複数のサーバを立ち上げられ、金銭的な打撃

■レンタルサーバやクラウドの提供するファイルマネージャーやコンソール。
侵入されることはサーバに侵入されたことと同じ

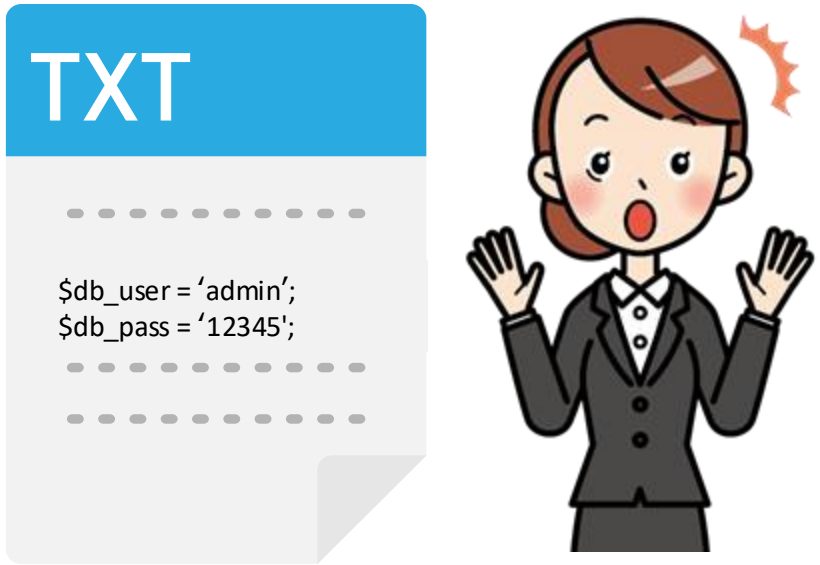
インシデント事例 - 平文で保存された情報

GMO PRIME STRATEGY

重要情報の漏洩

■DB情報や認証情報が平文で保存され、閲覧・ダウンロード可能な状態

■重大インシデントにつながった可能性



インシデント事例 - 知られざる改ざん

GMO PRIME STRATEGY

把握されていないサイトが改ざん

■キャンペーンサイトなど一時的に制作したサイトを放置

■担当者からの引き継ぎがなく把握できていないサイトがそのまま

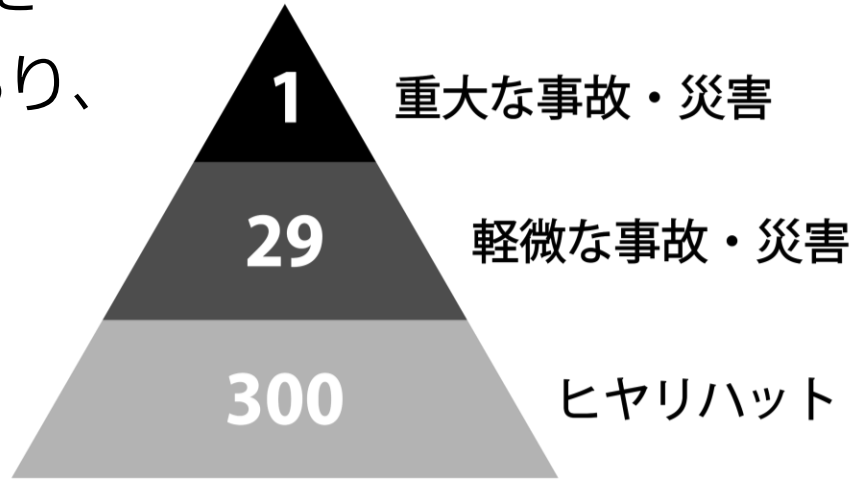
■野良サイト

インシデント事例 - 日々の保守作業に潜む危険

GMO PRIME STRATEGY

「めんどくさい」「これくらい」に潜む重大インシデントの危険

■不特定多数がログインするメディアで、管理画面のアクセス制限を省略
■パスワードの使いまわし、共通パスワードによる運用
■退職者や契約終了したベンダーのユーザーの削除忘れ
■閉鎖したサイトのドメインを手放し、スパムサイトに
■PHPのバックアップの拡張子が不適切で閲覧可能に
■ドキュメントルート配下にDBのバックアップがあり、
ダウンロード可能な状態に



チェックリスト（本日解説しません）

侵入されない　-　WordPress管理画面の保護

GMO PRIME STRATEGY

■強固なパスワード 必須
> WordPressがレコメンドするもの
> 使いまわし・共用を避ける

■adminなどのよく使われるユーザー名を避ける 必須

■IP制限・basic認証 必須

■ログイン試行回数の制限 better

■多要素認証・シングルサインオン +a

※ログインURLの変更は動作に影響を及ぼすリスクがある。ログインURLを変えたからと安心して他の施策をしないことが問題

侵入されない – サーバ

■ファイアウォール（SSHなどのIP制限）必須

■管理画面（コンソールやファイルマネージャーなど）の保護 必須

・多要素認証・権限管理などのプラットフォームが提供する施策

■phpMyAdminなどのデータベース管理ツール better 必須

・使わない

・どうしても使うなら厳重なアクセス制限・短期利用

■IPS/IDS +α

WordPress　その他の対策

GMO PRIME STRATEGY

■XML-RPCの無効化 重要

■設定ファイル（wp-config.php）の位置 重要

■ファイルパーミッションの適切な設定 必須

■不要なプラグイン・テーマの削除 必須

■ユーザー管理 必須

・適切なユーザー権限の設定

・不要なユーザーの削除（無効化）

■個人情報の外部DB化 +α

セキュリティツールの導入 better +a

GMO PRIME STRATEGY

■防御

迷ったらWAF（必須に近くなっている）

> WAF

- ホスティングにWAFがプランに組み込まれていることも増えている
- クラウド・VPSでも導入しやすいプラン（ツール）から検討

■発見

> マルウェア・アンチウィルス検知

> 改ざん検知

> 定期的な脆弱性検査

体制・情報収集 better 必須

GMO PRIME STRATEGY

なにか起こってから慌てるのではなく、日頃から備えておくことが大事

■体制の構築

> セキュリティ対策チーム・外部相談口

> バックアップと復旧（体制と訓練）

■資産管理

> ドメインやSSLもセキュリティに係る大事な資産

■脆弱性情報の収集

> Security Advisory for WordPress
https://kusanagi.tokyo/releases/tag/wp-security-advisory/

> Security Advisory

> https://kusanagi.tokyo/releases/tag/security-advisory/

今すぐできる対策

今すぐできる対策　その１

■まず、WordPressサイトヘルスをご覧ください。
■管理画面の左側の「ツール」⇒「サイトヘルス」で閲覧ください。
■サイトヘルスの中に「ステータス」タブがあり、その中にある「致命的な問題」や「おすすめの改善」を中心にご確認の上、システム担当者や外部の委託先に対応を依頼してください。
　＞ バージョンアップで対応できるものも多いです。
■WordPress本体やプラグイン、テーマを最新版にしてください。
　ただし、正常に行えない場合があるため、システム担当者や外部の委託先に対応を依頼してください。

今すぐできる対策　その2

■脆弱性情報をチェックしてください。

■当社が提供しているSecurity Advisory for WordPress
もご活用ください。

https://kusanagi.biz/wordpress-security-advisory/

今すぐできる対策　その３

■IDとログインURLがネット上で見えていないかを確認する

■確認方法

> ID/パスワードを記憶させていない通常の運用に利用していないブラウザやブラウザのシークレットモードを利用し、管理画面にアクセスしてみてください。Basic認証が表示されず、直接ログインフォームが表示される場合は、管理画面にアクセス制限がかかっていない可能性があります。
> また、ユーザーIDがインターネット上で閲覧できるかどうかを確認する方法の一例をご紹介します。
> 対象となるWebサイトのURLの後に「/?author=1」や「/?author=2」や「/?author=3」を続けて入力して、エンターキーを押してください。ユーザーIDが閲覧できてしまう状態にある場合は、そのユーザーIDが含まれるユーザーページが表示されます。

今すぐできる対策　その４

GMO PRIME STRATEGY

■対策

> Basic認証を設定ください。

> ログインURLを別のURLに変更してください。

> 例として、　「?author=1」も著者アーカイブページ
（/author/username/）も完全に非公開にする

WordPressの法則
皆さんが困っていることは、世界中のWordPressユーザーも困っていることです。
ネットで検索すれば大概の対処方法がでてきます。（いつのコンテンツかを確認してください。）
古いコンテンツはバージョンが違っていてその通り動かないことも。
セキュリティ関連のことは当社のようなWebセキュリティに強い専門の業者に依頼された方が安全です。

プラグインを監視管理するプラグイン作りました

GMO PRIME STRATEGY

KUSANAGI Business Edition/Premium Editionを使っている方のみ利用できる無料プラグインです。動作互換性、メンテナンスが止まっているか、ファイルが改ざんされているかを一覧で確認可能で、AIのアドバイスをもらえます

個人事業主、法人の皆様を無料で支援します

GMO PRIME STRATEGY

■KUSANAGIライセンスパートナー　本日オープン！
■目的：KUSANAGI有償ライセンスでWebサイト構築してくれる
　個人事業主、法人の皆様を支援します
■参加費無料
■支援内容
　> 販促資料提供
　> ロゴ使用権
　> 技術支援（マニュアルサポート）
　> オンラインセミナーの講師無料派遣
■お申し込みと詳細は以下よりお願いします。
　> https://partner.kusanagi.tokyo/

すべての人にインターネット