



# WordPressのセキュリティ対策 セミナー「今すぐ確認できる方 法からここまではやってほしい 対策を解説」

2024.10.30  
プライム・ストラテジー株式会社  
代表取締役 吉政忠志



# 目次

---

- 自己紹介と会社紹介
- サービス紹介
- 新サービス「WordPress簡易脆弱性診断サービス」
- 新製品「KUSANAGI Security Edition」(通称：KUSANAGI SE)
- 市場データ
- セキュリティ対策について
- 事例について
- イベント等のお知らせ

# 本日のハイライト

---

- WordPressのセキュリティ動向（稟議の添付資料や社内資料にご活用ください）
- なぜ、最新版にアップデートできないWordPressが47%も存在するのか
- 手軽に確認する方法のご紹介（今すぐできる簡単な方法もご紹介）
- プライム・ストラテジー新サービス「WordPress簡易脆弱性診断サービス」のご紹介
- プライム・ストラテジー新製品「KUSANAGI Security Edition」（通称：KUSANAGI SE）のご紹介
- 最低限ここまではやってほしいセキュリティ対策について
- プライム・ストラテジーセキュリティ対策ソリューションのご紹介
- セキュリティ対策事例のご紹介

# 会社紹介と自己紹介



# 新代表挨拶

## 代表取締役 吉政 忠志

私たちプライム・ストラテジーは、WordPressのリーディングカンパニーの1社として、Linuxなどのオペレーティングシステム、Apache、Nginx、MySQL、PHPなどのミドルウェア、WordPressなどのアプリケーションを中心とするOSSに関するサービスを提供して参りました。その後、WordPressは大規模のWebシステムで採用されるようになり、表示速度やセキュリティ面、保守面の改善が市場の声として求められるようになりました。そこで、2015年より、超高速CMS実行環境「KUSANAGI」の一般無償提供を開始し、セキュリティ面、保守面を支援するべく、「KUSANAGIマネージドサービス」を展開し、常に顧客課題の解決に向けてサービスの開発を行って参りました。これらの製品やサービスが高く評価され、多くのお客様にご評価をいただけるようになりました。

近年、WordPressの国内CMSシェアは80%を超え、大手企業でのWordPress利用率も大幅に向上し、当社が担う責務もますます重くなってきております。この期待に応えるべく、今後も「KUSANAGI」「WEXAL」「KUSANAGIマネージドサービス」の強化に努め、エンタープライズOSSエコシステムの発展のために全力を尽くして参ります。

より高速に、より安全に、より手離れよくオープンソースソフトウェアをお客様のビジネスでご活用いただくために、私たちは、IT業界におけるユーザーの期待とベンダーの現実のギャップを解消し、エンタープライズOSS（オープンソースソフトウェア）エコシステム発展のために全力を尽くして参ります。一方で当社はAIや自動化を業務の中心で活用する企業という側面もあり、AI・自動化の知見とノウハウが多く蓄積されています。このノウハウを活かし、エンタープライズOSSエコシステム発展に尽力いたします。世界中のお客様、パートナーの皆様、ステークホルダーの皆様、引き続きご支援、ご指導のほど宜しくお願いいたします。



# 業界団体の経歴

- 一般社団法人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
- Rails技術者認定委員会 理事長
- 一般社団法人日本ネットワーク技術者協会 代表理事
  - IPv6検定、Pythonとネットワークの自動化検定を主宰

過去には、IPA専門委員、文部科学省XML教育推進委員、Linuxコンソーシアム副会長、OSSコンソーシアム副会長なども歴任

# プライベートでは

- マイナビニュースなどで月刊連載 15本
- 日本赤十字より受勲しました。
- 自転車で日本縦断中です。(残240km)
- マイナビ出版で企画力と企画書の教科書を出版しました。
- 某大手企業のマーケティング外部職級審査員をしてました。
- 東京パラリンピックの東京都最終ランナーとしてNHK・開会式で流れました。
- 趣味は釣りとお茶です。



ITエンジニアのための 吉政 忠志 [著]

## 企画力と 企画書の 教科書

企画力でエンジニアの人生は変わる！  
やりたい仕事も高い給与も手に入る！

「ロジック」と「鳥瞰力」で  
採用される企画は作れる！  
伝説と言われた給与を獲得した  
筆者が教える、生のノウハウ

増井雄一郎氏推薦！  
エンジニアリングで  
培ったロジックで最強の  
企画を立てよう！

企画ができなければ、  
AIにこき使われる時代へ

# 会社概要

## 社名

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

## 設立年月日

2002年12月2日

## 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）

20名(2024年5月末)

## 資本金

439,796千円（2024年8月31日時点）

## 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」<sup>®</sup>
- 戦略AI「ONIMARU<sup>®</sup> 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

## 連結子会社

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

## 資本業務提携先



株式会社イントラスト 株式会社エアトリ

WEXAL<sup>®</sup>、Page Speed Technology<sup>®</sup>、ONIMARU<sup>®</sup>は当社の登録商標です。  
登録商標であることの告知記号「<sup>®</sup>」は以降省略して記載させていただきます。



# マネジメントチーム



**吉政 忠志** 代表取締役  
マーケティング部管掌

1992年 インテック入社  
2010年 吉政創成株式会社 代表取締役就任  
2011年 PHP技術者認定機構 理事長就任  
2016年 一般社団法人Pythonエンジニア育成推進協会  
代表理事就任  
2018年 一般社団法人日本ネットワーク技術者協会  
代表理事就任  
2024年 プライム・ストラテジー株式会社 代表取締役就任

社外取締役

小舘 亮之  
大崎 理乃  
添田 繁永（監査等委員）  
鈴木 隆之（監査等委員）  
森田 芳玄（監査等委員）



**中山 勝美** 取締役  
経営管理部管掌

1986年 有限会社家庭教師センター学習館入社  
1987年 東京アカウンティング学院株式会社  
（現TAC株式会社）入社  
2012年 学校法人大阪歯科大学入職  
2017年 当社入社 執行役員管理部長  
2023年 当社取締役就任



**池宮 紀昭** 取締役  
クラウドインテグレーション事業部管掌

2008年 株式会社コナミデジタルエンタテインメント入社  
2016年 AppMedia株式会社入社  
2018年 当社入社  
2020年 当社クラウドインテグレーション事業部 部長就任  
2020年 当社取締役就任

# WordPressのリーディングカンパニー

WordPress関連書籍の執筆、監訳など

東京都主催「世界発信コンペティション」で  
東京都革新的サービス特別賞を受賞

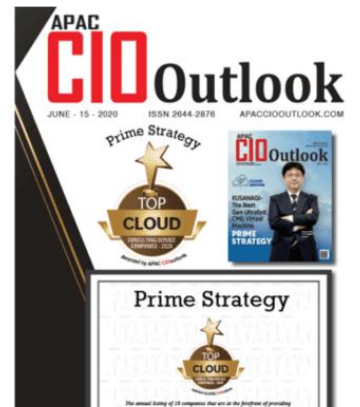
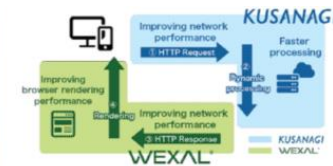


『詳解 WordPress』  
『WordPressによる  
Webアプリケーション開発』  
(出版社：株式会社オライリー・ジャパン)



『WordPressの教科書』シリーズ  
(出版社：SBクリエイティブ株式会社他)

「APAC CIO Outlook Magazine」にて  
「Top 10 Cloud Solution Companies – 2021」に選出



# 「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」

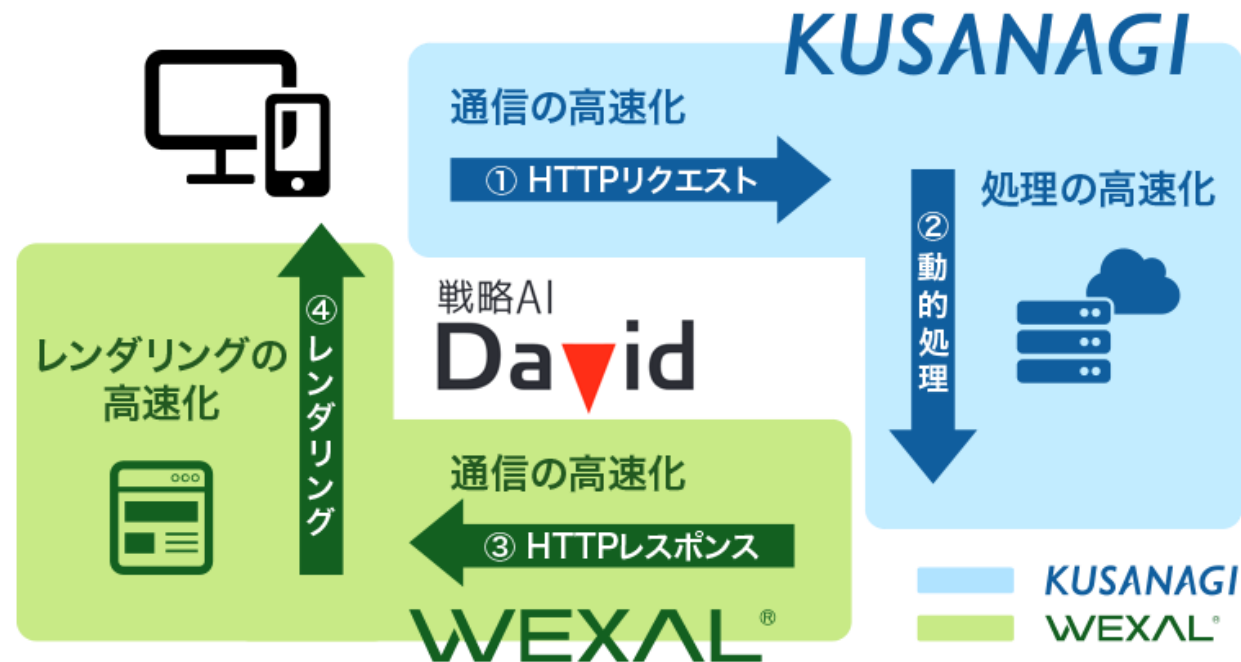


日本国特許第7523733号  
日本国特許第7530383号  
\* 米国特許出願・審査中

28プラットフォームで展開<sup>※1</sup>  
累計稼働台数9万台<sup>※2</sup>

**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



※1：2024年9月現在

※2：2024年7月現在

# 事業内容

「KUSANAGI」などコアとなる基礎技術・プロダクトの開発

AI・自動化などのテクノロジーを最大限活用した各種サービスの展開

## ストック型ビジネスを中心に展開

### ストック型ビジネス

#### ライセンス

##### 有償版ライセンス

KUSANAGIのクラウド事業者を通じた世界販売



##### 知的財産

ブランド/知的財産のライセンス提供



KUSANAGIブランド

GMO INTERNET GROUP

国内特許取得済み  
米国特許申請・審査中  
知的財産

#### KUSANAGIマネージドサービス

##### KUSANAGI+KUSANAGIの開発元 としてのマネージドサービスの付加価値

##### 単一のWebシステム保守運用サービス

顧客の単一のCMS等Webシステムの保守運用サービス

##### CMSプラットフォーム統合サービス

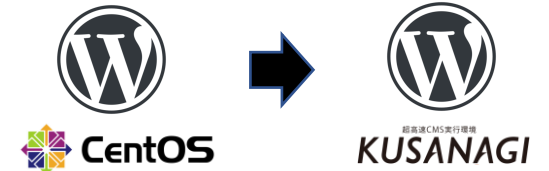
顧客の複数のCMS等Webシステムの統合管理サービス

### フロー型ビジネス

#### クラウドインテグレーションサービス

##### 初期導入時のサービス

KUSANAGIマネージドサービス導入時のシステム移行



##### 保守運用後のサービス

保守運用開始後の顧客Webシステムの追加開発

# 超高速CMS実行環境「KUSANAGI」

超高速CMS実行環境

## KUSANAGI

Powered by  Prime Strategy

WordPress等のCMSやWebシステムを  
高速かつ安全に動作させるための  
OS(オペレーティングシステム)

28プラットフォーム  
37カ国203リージョンで展開<sup>※1</sup>  
累計稼働台数9万台<sup>※2</sup>



※1：2024年9月現在  
※2：2024年9月現在

## フリーミアムモデル

製品を無償提供することでプロダクトの認知度を  
向上させ、運用保守サービスやライセンス販売等の  
有償サービスへ繋げる戦略

無償版



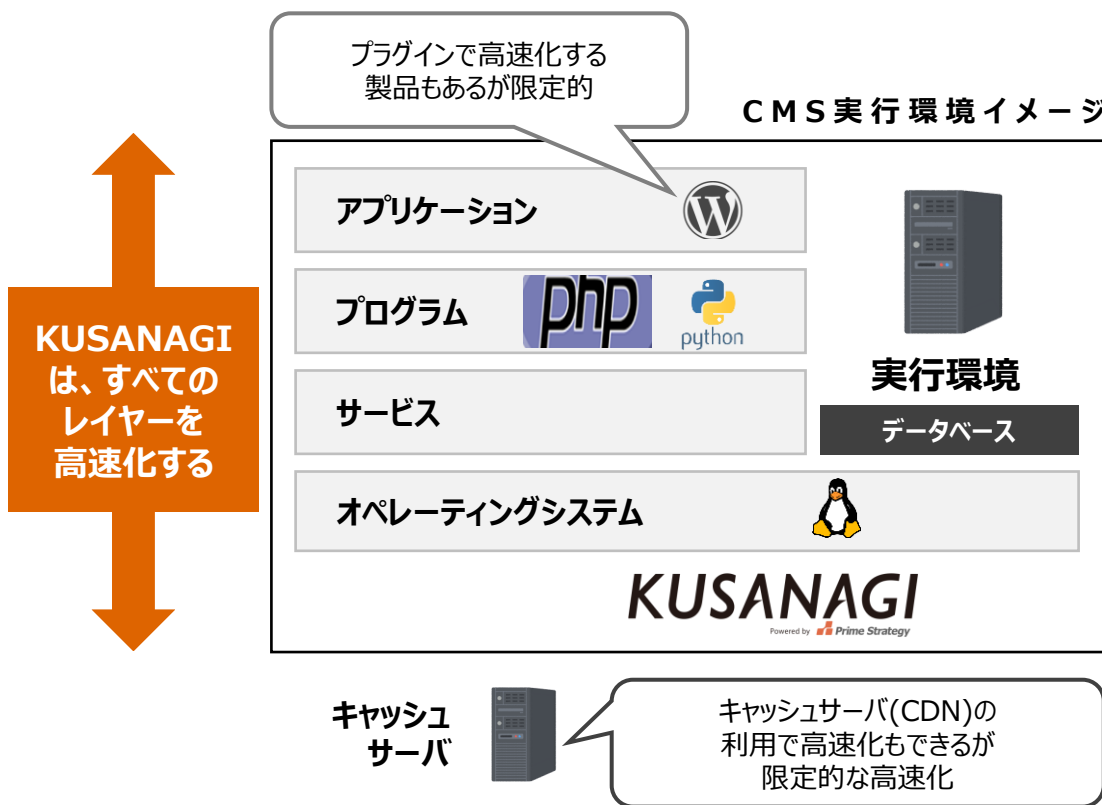
有償版



# 「KUSANAGI」のパフォーマンス

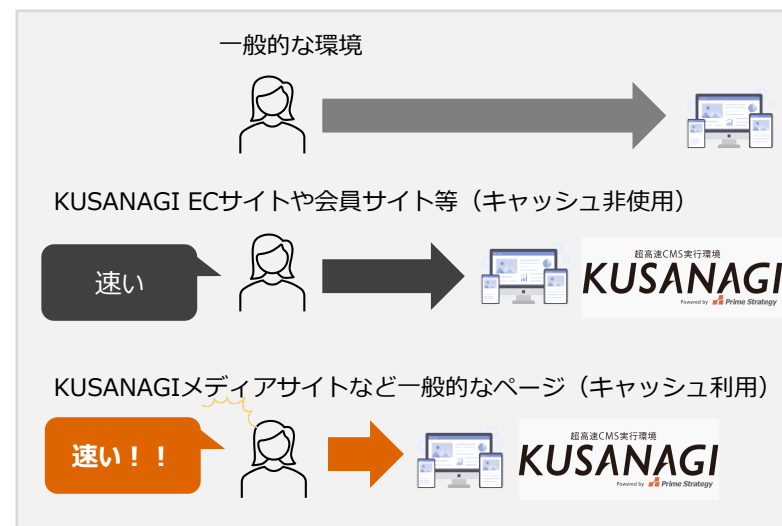
AWS、Microsoft Azure、Googleなどパブリッククラウド等の  
インフラ上で利用する希少性の高いソフトウェア

**差別化された独自性の高い当社の基盤となるプロダクト**



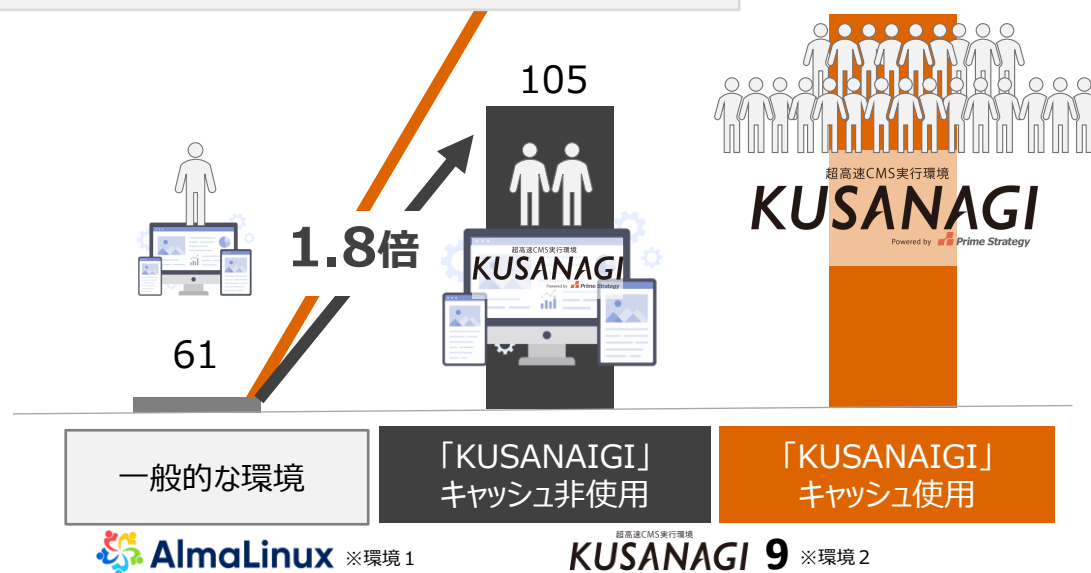
KUSANAGIはすべてのレイヤーを高速化  
ページキャッシュを利用しない場合でも高速化

**1秒あたりの処理可能リクエスト数**



16,046

260倍



# 「WEXAL Page Speed Technology」「David」



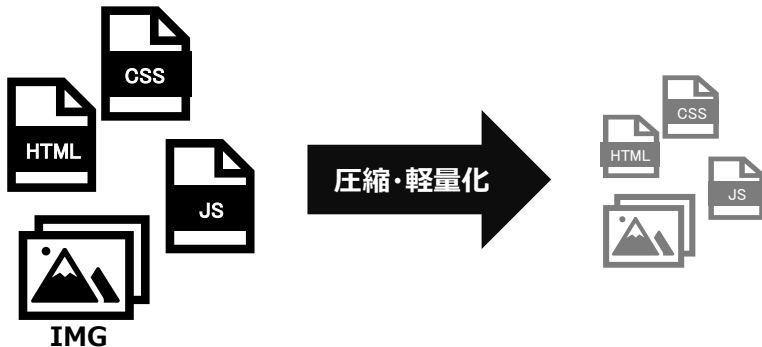
「**WEXAL Page Speed Technology**」は、Webシステムのための「高速化エンジン」。  
ブラウザ表示の自動チューニングを実施し、UX（ユーザー体験）の向上を実現します。

## メリット

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

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

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。



元システムの変更不要  
(導入しやすい)

# 「KUSANAGI」の拡がり

## 世界で利用されるKUSANAGI

グローバルなCMS高速化ソリューションのデファクトスタンダードとして成長

(2024年7月現在)

国内外の主要な28プラットフォーム

37カ国203リージョンで利用可能 (2024年9月現在)



ORACLE  
Cloud

vmware®



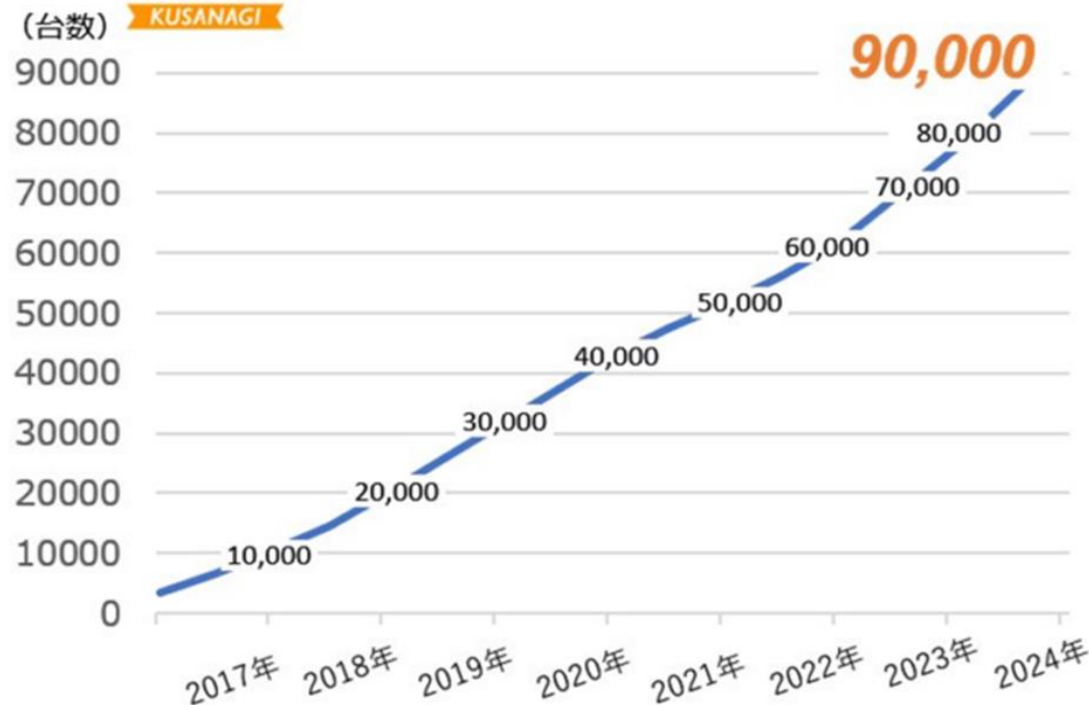
知的財産のライセンス提供

Xserver

GMO  
INTERNET GROUP

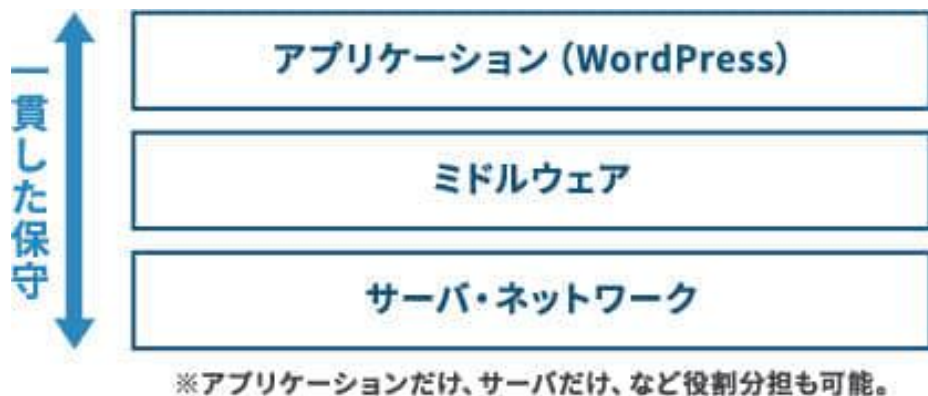


KUSANAGI 累計稼働台数の推移

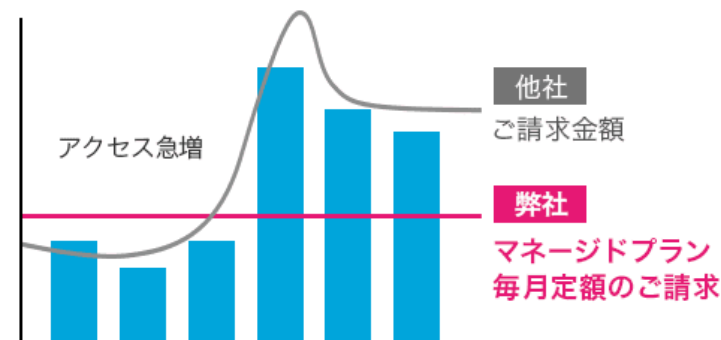




## WordPressなどのCMSからサーバの運用管理までを一貫してサポート



年間予算を立てやすいクラウド料金込みの月額定額制。  
一時的なアクセス増加があっても料金はそのまま。



CMSの運用に必要なものがセットになった  
フルマネージド型のサービス

サーバー費用込み

障害対応24時365日

セキュリティ対応

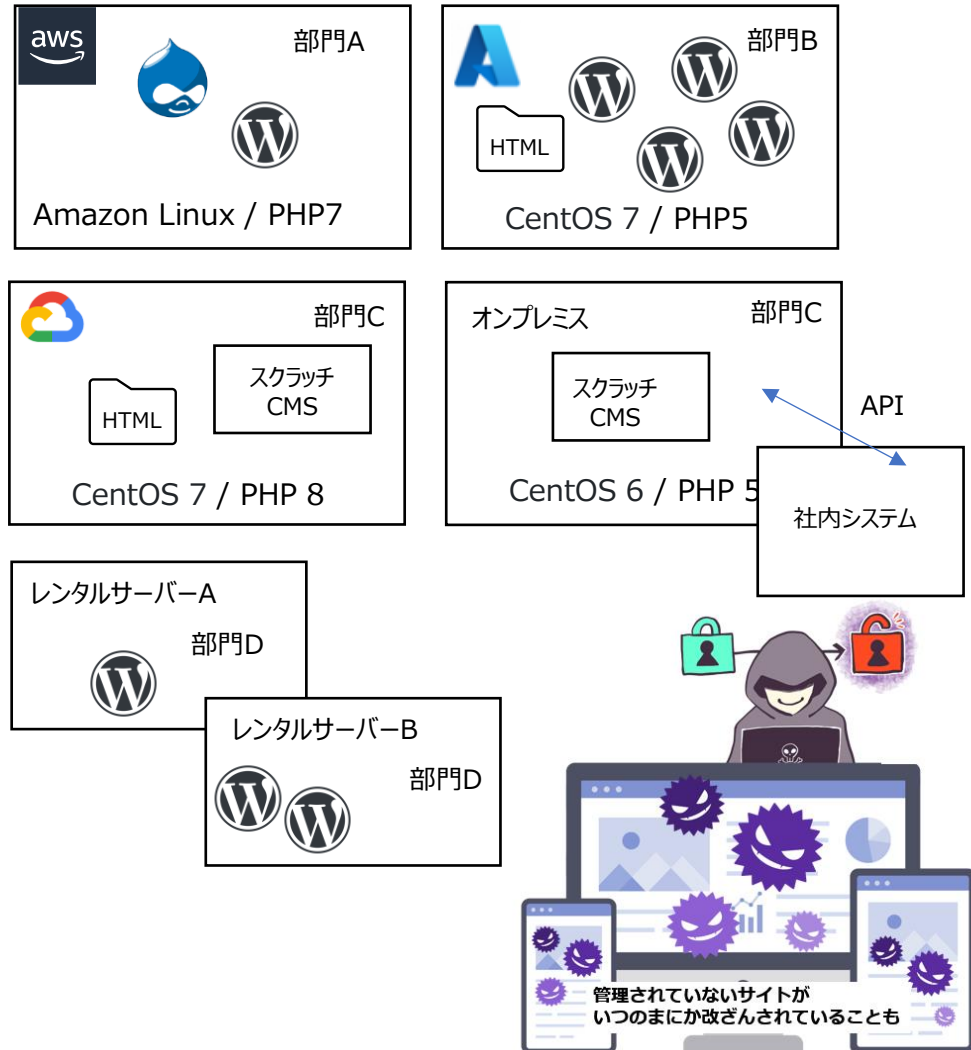
技術サポート

マーケティング・Web担当者様  
情報システム部門の担当者様に

CMSの運用を手離れして  
コンテンツ作成など本来の業務に集中できる

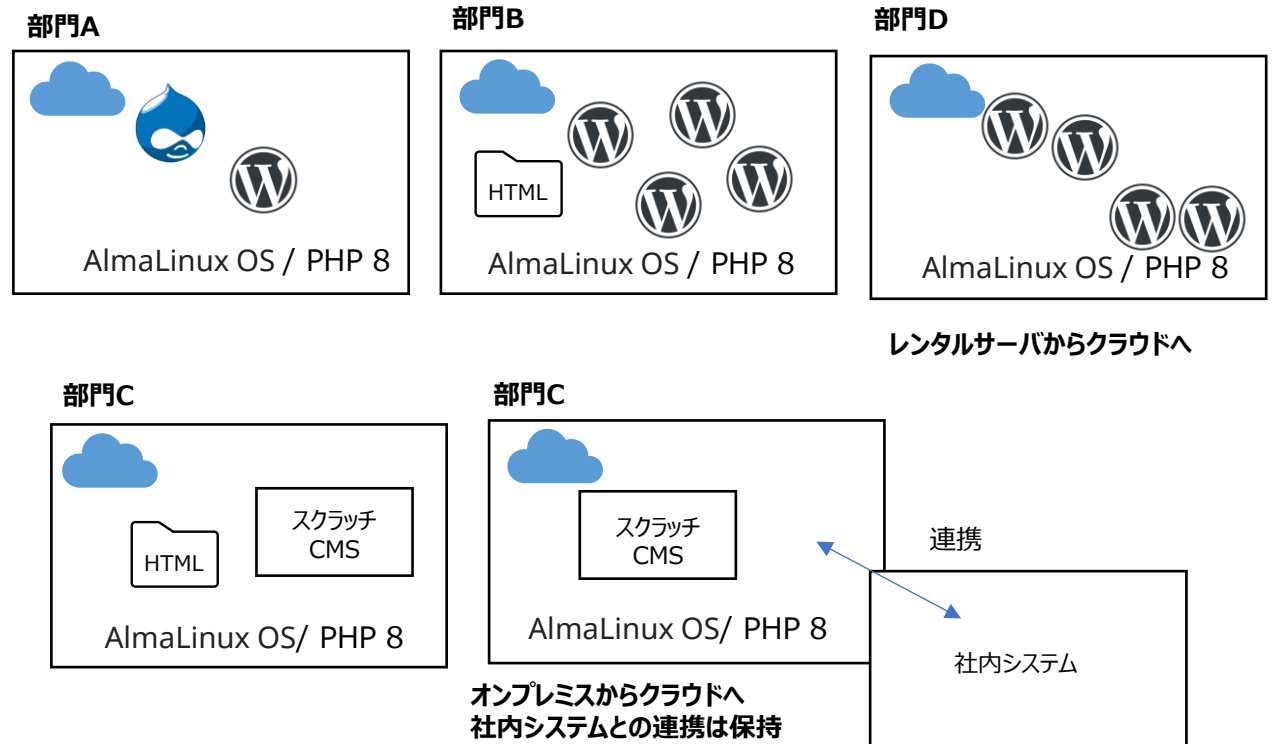
# CMS/Webプラットフォーム統合サービス

乱立するWebサイトが抱えるセキュリティとガバナンスの課題



クラウドプラットフォームを統一  
OSやミドルウェアを最新化し、統一されたルールで運用

統一したセキュリティ環境での運用



# CMS/Webプラットフォーム統合サービス

## プランニング

- ・環境調査
- ・サイトリスト作成
- ・課題点の洗い出し
- ・制作ベンダーとのやりとり
- ・運用ルールの策定

## 移行

- ・サーバ構築
- ・サイト移設
- ・セキュリティサービスの導入
- ・CMSのアップデート

## 運用

- ・障害対応
- ・メンテナンス
- ・セキュリティアップデート
- ・レポートニング
- ・ドメイン・SSLなどのアカウント管理
- ・制作ベンダーとの連携
- ・各種ご相談



サーバ費用込みの  
定額料金



技術サポート



24時間365日  
障害対応



セキュリティ  
対応



メンテナンス



バックアップと  
復旧

# 新サービス「WordPress簡易脆弱性診断サービス」



# WordPress簡易脆弱性診断サービス

---

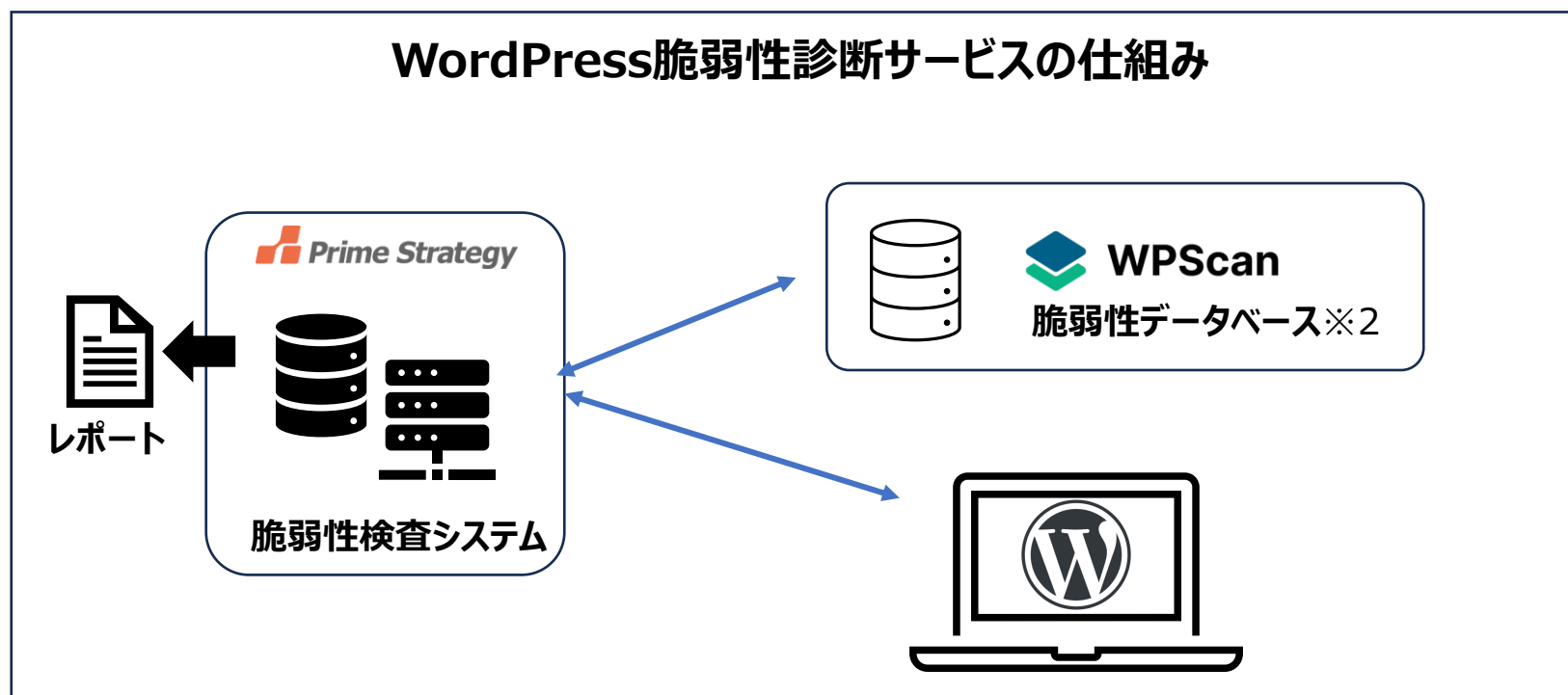
WordPressサイトを健全に保つには、現在のサイトの**潜在的なリスク**を知り、**必要なアクション**につなげていくことが大切です。



WordPress簡易脆弱性診断サービスは、**攻撃の対象となるリスクが高い**WordPress本体、プラグイン、テーマの脆弱性と、ご利用のサーバに含まれる脆弱性を診断し、**対応方法とともにレポートニング、コンサル**がご説明いたします。

# WordPress簡易脆弱性診断サービス

外部からWebサイトにアクセスして診断するため、サーバやWordPressの管理画面へのログインは不要です。運用サイトの状況を知っていただく第一歩としてお気軽に始めていただけるサービスです。



- ①外部からアクセスし、HTML等を解析※1
- ②WordPress・プラグイン・テーマのバージョンを解析し、脆弱性の有無を確認
- ③現在のバージョンが取得できなかった場合は、過去のバージョンの脆弱性情報から脆弱性の可能性をレポート

※1 外部からアクセスできるサイトのみを対象とさせていただきます。

※2 [WPScan](#) は歴史あるWordPressセキュリティスキャナーです。WordPress Core（WordPress本体）、プラグイン、テーマに関する28,000件以上の脆弱性データベースを提供し、WordPressセキュリティの第一人者によって管理されています。

# WordPress簡易脆弱性診断サービス

1サイト（WordPress）あたり

**3** 万円 + 消費税



お問い合わせはダイワボウ情報システム株式会社からお願いします。  
当社から直接販売もできます。

- ・診断結果に対するアップデートなどの対応は含んでおりません。
- ・より詳細な脆弱性診断をご希望の場合はご相談ください。

# 新製品「KUSANAGI Security Edition」





2024年12月 主要クラウドマーケットプレイスから提供開始予定

# KUSANAGI Security Edition



セキュリティ対策を強化 OS・ミドルウェアの自動アップデートを段階的に実現



OS・ミドルウェアの  
自動アップデート



マルチクラウド・マルチOSの  
セキュリティ基準



実用的なレポートイング



既存の運用フローとの  
インテグレーション

# KUSANAGI Security Edition

セキュリティ対策によるコストの増大とリソースの圧迫

- 複数のセキュリティ管理ツールやレポーティングツールからのアラートへの対応
- アップデートによる脆弱性への対応
- 一部では形骸化も

標準化した運用環境

## KUSANAGI



- 標準的なセキュリティ対策の設定の提示
- アップデート作業の効率化
- 効率的で柔軟性の高い運用をサポート

セキュリティ特化の運用環境として、企業やCMS・Webシステムの構築運用を提供するSIer・制作会社等に標準的に選択される基盤

2024年12月 主要クラウドマーケットプレイスから提供開始予定



# 激化するサイバー攻撃～社会課題

- ・ランサムウェア攻撃による事業活動への影響
- ・ソフトウェアの脆弱性を悪用された不正アクセスによる個人情報の流出



【NEWS RELEASE】

2024年7月29日  
株式会社KADOKAWA

## 【第4報】KADOKAWAグループの事業活動の回復状況について

株式会社KADOKAWA（本社：東京都千代田区、取締役 代表執行役社長 CEO：夏野剛）は、6月8日に発覚した当社グループのデータセンター内のサーバーへのサイバー攻撃の影響により、読者やユーザー、作家・クリエイター、取引先、株主・投資家をはじめ、関係するすべての皆様へ、多大なるご心配とご迷惑をおかけしておりますことを深くお詫び申し上げます。

当社は本事業発生以降、事業活動の根幹である経営機能の立て直しと、売上規模が大きい出版事業の回復を最優先事項として取り組んでまいりました。経営機能については、アナログ対応も含め既に平常状態に復旧していることに加え、出版事業につきましても、8月から段階的に出荷ボリュームが回復し、8月中旬以降は1日当たりの出荷部数が概ね平常時の水準に回復する見込みとなりましたことを報告いたします。

### ①出版事業

6～7月	<ul style="list-style-type: none"><li>・ 6月8日に、複数サーバーにアクセスできない障害が発生。出版製造・物流システムが停止</li><li>・ 新刊の製造・出荷は平常時水準を維持。既刊の出荷部数は平常時の3分の1程度に</li></ul>
8月	<ul style="list-style-type: none"><li>・ 段階的に出荷ボリュームが回復</li><li>・ 中旬以降は既刊の1日当たりの出荷部数は平常時水準に回復の見込み</li></ul>
9月～	<ul style="list-style-type: none"><li>・ DOTを再稼働、販売施策を強化し、出荷・販売を増強</li><li>・ 事業発生以降の出荷保留分や、店頭で品薄となっているタイトルの埋め合わせを図る</li></ul>

シャープ公式オンラインストア「COCORO STORE」・食材宅配サービス「ヘルシオデリ」における不正アクセスによる個人情報流出についてのお詫びとお願い

2024年07月29日

シャープ公式オンラインストア「COCORO STORE」および食材宅配サービス「ヘルシオデリ」への第三者による不正アクセスにより、これらのサービスをご利用いただいた一部のお客様の個人情報が外部へ流出していたことが判明しました。また、「COCORO STORE」のウェブサイトへアクセスいただいたお客様を、悪意のあるサイトへ誘導する不正な改ざんがなされていたことも判明しました。

お客様や関係者の皆様には、多大なるご迷惑とご心配をおかけすることとなり、深くお詫び申し上げます。

「COCORO STORE」および「ヘルシオデリ」のウェブサイトは、不正アクセスの判明後、すみやかに一時停止しております。個人情報が流出したお客様および、該当期間に「COCORO STORE」のウェブサイトへログインの上アクセスされたお客様には、本日より電子メールにてご連絡を開始しております。

現時点におきまして、流出した個人情報の不正利用などの二次被害は確認されておりませんが、個人情報保護委員会への報告や警察への届出をしており、引き続き調査を進めてまいります。

[https://tp.kadokawa.co.jp/.assets/240729\\_release\\_e8codpsX.pdf](https://tp.kadokawa.co.jp/.assets/240729_release_e8codpsX.pdf)

<https://corporate.jp.sharp/info/notices/240729-a.html>

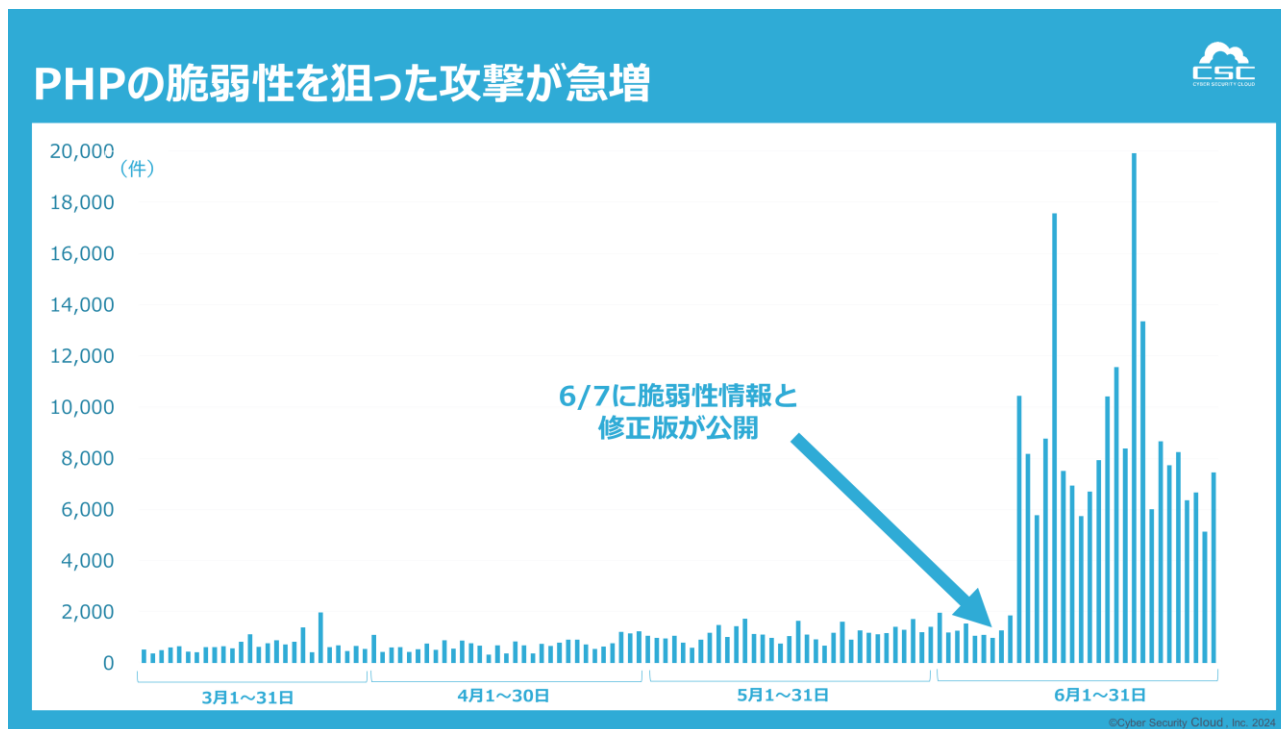
# アップデートの重要性の高まり

脆弱性が発表されると、その脆弱性を狙った攻撃が一気に増加  
攻撃が開始されるまでの期間が非常に短い

[PHPの脆弱性 \(CVE-2024-4577\) を狙う攻撃について](https://www.ipa.go.jp/security/security-alert/2024/alert_20240705.html)

[https://www.ipa.go.jp/security/security-alert/2024/alert\\_20240705.html](https://www.ipa.go.jp/security/security-alert/2024/alert_20240705.html)

[【注意喚起】PHPの脆弱性を狙った攻撃が6月7日以降で約10倍に急増！ ダークウェブへの不用意なアクセスにもご注意を](#)



<https://www.cscloud.co.jp/news/press/202407057263/>

# 開発の背景

---

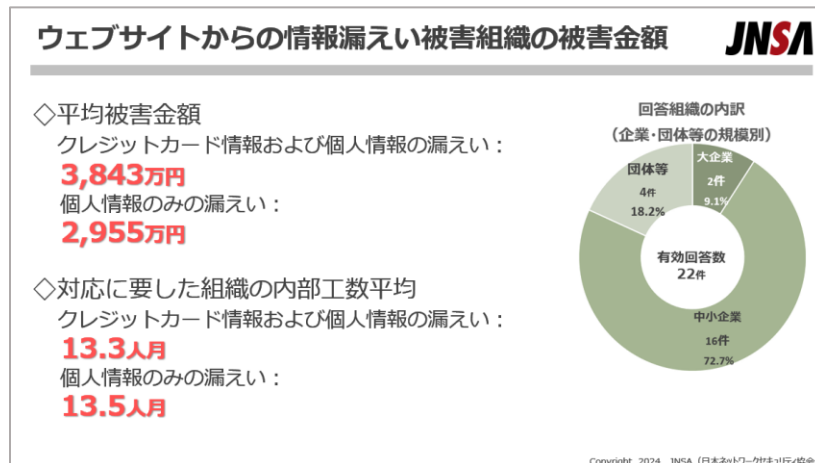
# セキュリティに、よりコストをかける時代に

攻撃され続けるWebサイト

セキュリティインシデントは企業経営を揺るがす

- 企業の信頼、ブランドの毀損
- サービス停止による事業継続性への影響
- 膨大な対策費用

事故対応の費用だけで数千万



# セキュリティ対策によるコスト増大と業務の圧迫

---

セキュリティ対策には限りがない

標準的な運用ルールの策定や対応の有無を判断する難しさ

- 必要以上の対策によるコストの増大
- 複数のセキュリティ管理ツールやレポーティングツールなどからのアラートへの対応によるリソースの圧迫
- アップデート作業によるリソースの圧迫
- 一部ではセキュリティ疲れや形骸化も課題に

企業・顧客を守るためのセキュリティ対応が事業活動を圧迫

# KUSANAGIによる課題の解決

---

CMSの運用と自動化で培った知見

- 標準的なセキュリティ対策ツールと設定の提示
- アップデート作業の効率化
- 効率的で柔軟性の高い運用をサポート

## KUSANAGI Security Edition



# 開発方針

---

# 開発方針

- OS・ミドルウェアの自動アップデート - 運用コストの削減
  - AIによるテスト・巻き戻し（レポートイング）機能
- 統一したセキュリティ基準の提供 - マルチクラウド・マルチOS
  - 対応するOSをRed Hat系のLinuxに拡大
  - オンプレミス環境へ提供
- 効率的で効果の高いレポートイング
  - 具体的な対応方法をレコメンド
  - WordPressに特化した監査
- APIの提供 - 既存の運用フローとの連携
  - 既存のフローや監査・レポートイングツールとの連携
- 外部セキュリティ製品との連携



OS・ミドルウェアの自動アップデート



マルチクラウド・マルチOSの  
セキュリティ基準



実用的なレポートイング



既存の運用フローとの  
インテグレーション

# OS・ミドルウェアの自動アップデート - 運用コストの削減

---

## アップデート

- セキュリティに関する運用で最も基本的で重要
- 専門的な知識・工数が必要

## OS・ミドルウェアの自動アップデート

1. アプリケーションに影響の少ないアップデートの自動化
2. AIによるテスト、巻き戻し（レポーティング）機能の提供と適用範囲の拡大

# 統一したセキュリティ基準の提供 – マルチクラウド・マルチOS

---

- 複数のクラウドやオンプレミスなど様々な環境で運用
- BCP対策などにより異なる環境が必要になることも

複数の基盤で統一したセキュリティ基準と運用を実現

1. 対応するOSをRed Hat系のLinuxに拡大
2. オンプレミス環境へ提供

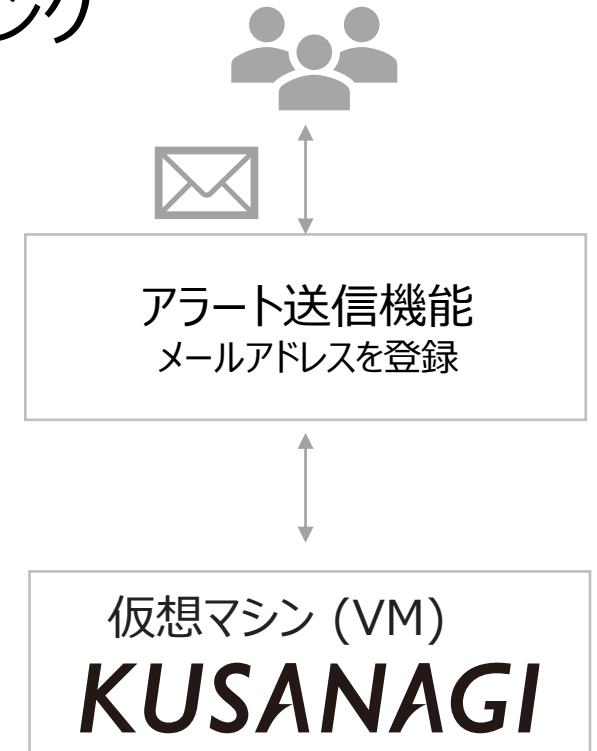
# 効率的で柔軟性の高い運用をサポート

## 効率的で効果の高いレポートイング

- リスク分析機能「KUSANAGI Analyze」のセキュリティ監査を強化
- WordPressに特化した監査
- 具体的な指示を提示する効率的で効果の高いレポートイング
- アラートを送信するための機能を提供予定

## 既存の運用フローとの連携

- 既存の運用フロー、レポートイングツール等との連携、自動化を容易にするためのAPIの提供
- 外部セキュリティ製品との連携



# 主な機能

---

# ピックアップ

---

## マルウェア・アンチウイルス対策機能

- マルウェアスキャンを構成に合わせて設定し、負荷を軽減
- スキャンの間隔などの推奨設定と、カスタマイズ
- メールやAPIでのレポート

## IP制限・Basic認証

WordPressの管理画面やドキュメントルートにIP制限・Basic認証を簡単に設定

- 設定ファイルの記載ミスを軽減
- IPのリストによる制限設定に対応し、運用を容易化

# 機能一覧（予定）

---

## ■ セキュリティツール

- マルウェア・アンチウイルス対策機能
- Bot対策

## ■ セキュリティ運用

- ミドルウェア・OSの自動アップデート（テスト・巻き戻し）

## ■ 監査・レポーティング

- 監査 / WordPress専用監査
- レポート(対策のレコメンド)
- API・メール送信・PDFダウンロードなど

## ■ 脆弱性管理

RPMの脆弱性情報の提供

## ■ KUSANAGIの標準的なセキュリティ機能

- 最新版ミドルウェアをKUSANAGIのリポジトリより提供
- WAF
- SELinux対応
- TLS 1.3対応
- TLS 1.1以下の無効化
- DoS攻撃対策
- WordPress向けセキュリティ機能（KUSANAGI専用プラグイン）

などを予定



ロードマップ・ご利用方法など

---

# ロードマップ

## 初版（2024.12）

- マルウェア対策機能
- IP制限・Basic認証
- ミドルウェア・OSの自動アップデート  
（DB・OSのカーネルを除くマイクロまで）\*
- 監査・レポート

## アップデート

- レポーティング機能の拡充
  - メールのアラート送信
  - 監査・レポート項目の拡充
- ミドルウェア・OSの自動アップデート
  - マイナーアップデート
  - テスト（レポート）
  - 巻き戻し機能
- 提供プラットフォームの拡充

\*自動アップデートは機能に影響の少ないものから順次提供

# ご利用方法など

---

## ■ご利用方法

KUSANAGIを提供している主要クラウドの  
マーケットプレイスから順次提供開始

(その他)

- プライベートオファアでの利用
- オンプレミスへの提供  
を検討

## ■ライセンス料金

未定

(VM単位の料金体系を予定)

## ■サポート

専用の導入・運用サポートを提供予定

※提供中のBusiness/Premium Editionからのアップグレードの提供は予定していません。移行機能を提供予定です。  
※新パートナープログラムでのお取り扱い、プラットフォームでの新規提供についてはお問い合わせください。

# より詳しい説明を聞かれたい方、評価版について

---

- 評価版については現在検討中です。
- より詳しい説明を聞かれたい方、評価版を希望される方は、アンケートに希望を記載ください。
- 法人名でのアンケート送信の方に限定させていただきます。

# 稟議に使える市場データ集



# 日本のCMS市場シェア

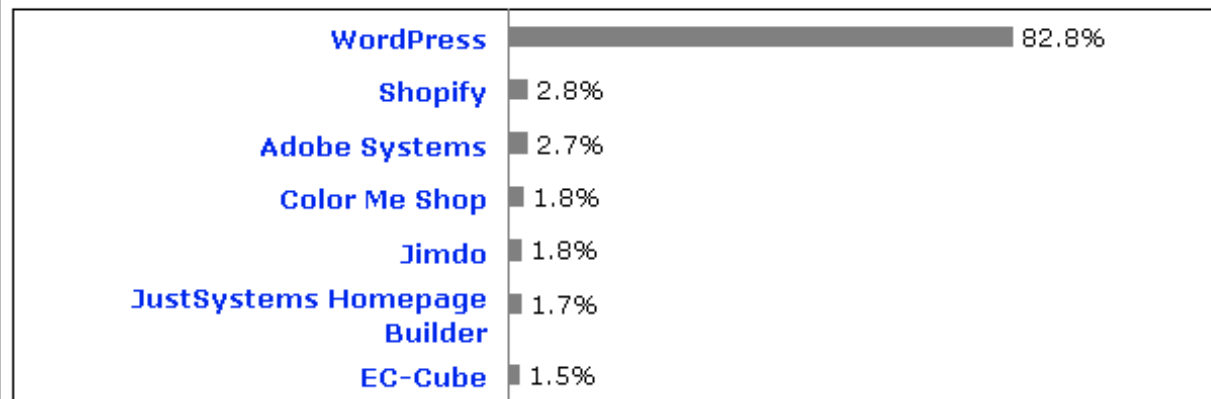
- 国内のCMSの82%はWordPressが稼働
  - [Distribution of Content Management Systems among websites that use Japanese \(w3techs.com\)](http://w3techs.com)

## Distribution of content management systems among websites that use Japanese

This diagram shows the percentages of websites using various content management systems among the sites that use Japanese. See [technologies overview](#) for explanations on the methodologies used in the surveys.

How to read the diagram:

WordPress is used by 82.8% of all the websites whose content management system we know and **that use Japanese as content language.**



# ご参考：上場企業のWordPress利用状況

- 上場企業 3821社（総URL数18,559）でWordPressが使用されているドメイン数は4343サイト（前年比944サイト増）
  - 株式会社DataSign 2023年8月調査
  - [https://oshiete-url.jp/report/cms/2023\\_8/](https://oshiete-url.jp/report/cms/2023_8/)

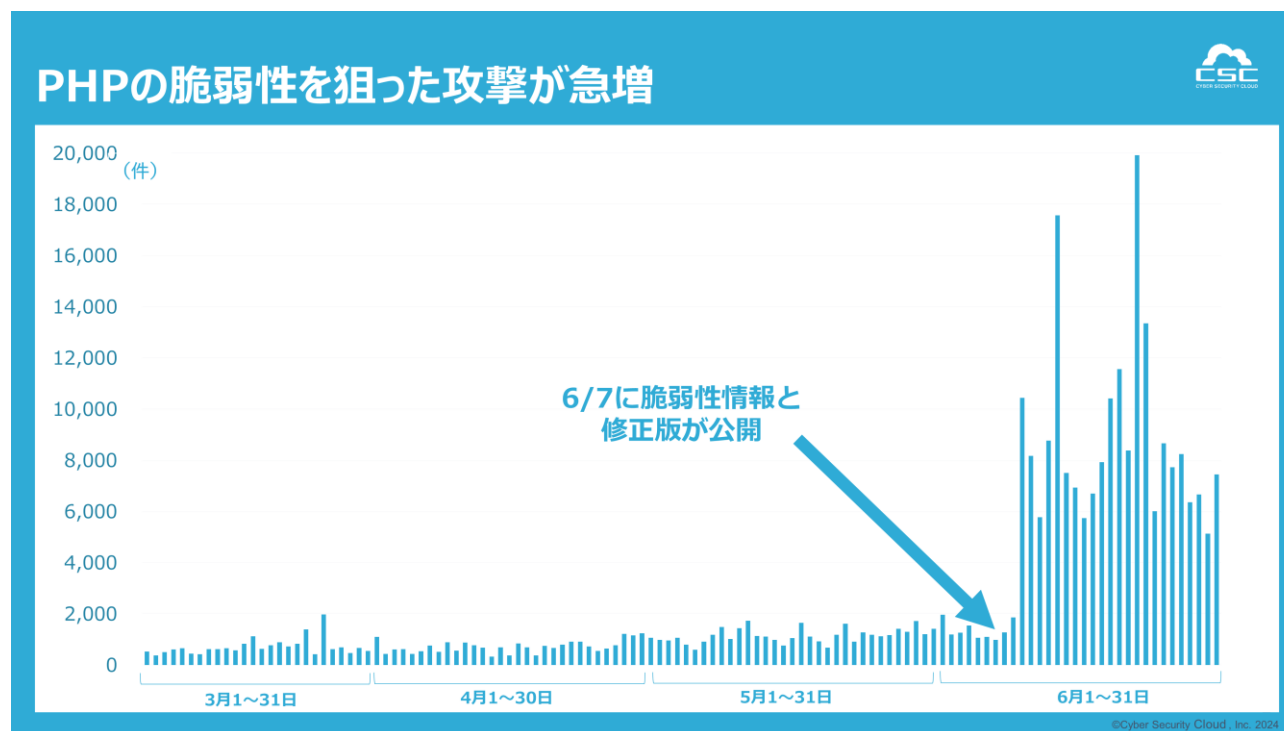
	2023年8月	2022年8月	前年比	増減率
WordPress	4343	3399	944	127.8%
ShareWith	185	165	20	112.1%
Drupal	130	95	35	136.8%
Movable Type	111	118	-7	94.1%
Blue Monkey	92	70	22	131.4%

# 公開された脆弱性を狙った攻撃の増加

脆弱性が発表されると、その脆弱性を狙った攻撃は一気に増加する  
攻撃が開始されるまでの期間が非常に短い

PHPの脆弱性 (CVE-2024-4577) を狙う攻撃について

【注意喚起】PHPの脆弱性を狙った攻撃が6月7日以降で約10倍に急増！ ダークウェブへの不用意なアクセスにもご注意を



<https://www.cscloud.co.jp/news/press/202407057263/>



# 企業としての顧客（閲覧者）を保護する責任

## 情報セキュリティ10大脅威 2024

### ▲ 情報セキュリティ10大脅威 2024 [個人]

「個人」向け脅威（五十音順）	初選出年	10大脅威での取り扱い (2016年以降)
インターネット上のサービスからの個人情報の窃取	2016年	5年連続8回目
インターネット上のサービスへの不正ログイン	2016年	9年連続9回目
クレジットカード情報の不正利用	2016年	9年連続9回目
スマホ決済の不正利用	2020年	5年連続5回目
偽警告によるインターネット詐欺	2020年	5年連続5回目
ネット上の誹謗・中傷・デマ	2016年	9年連続9回目
フィッシングによる個人情報等の詐取	2019年	6年連続6回目
不正アプリによるスマートフォン利用者への被害	2016年	9年連続9回目
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	2019年	6年連続6回目
ワンクリック請求等の不当請求による金銭被害	2016年	2年連続4回目

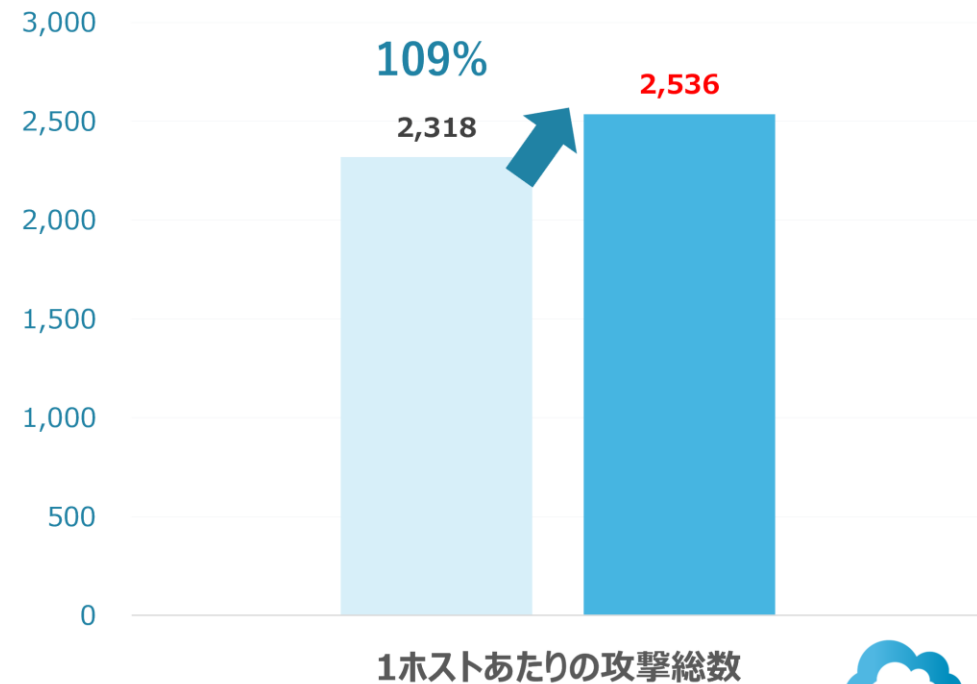
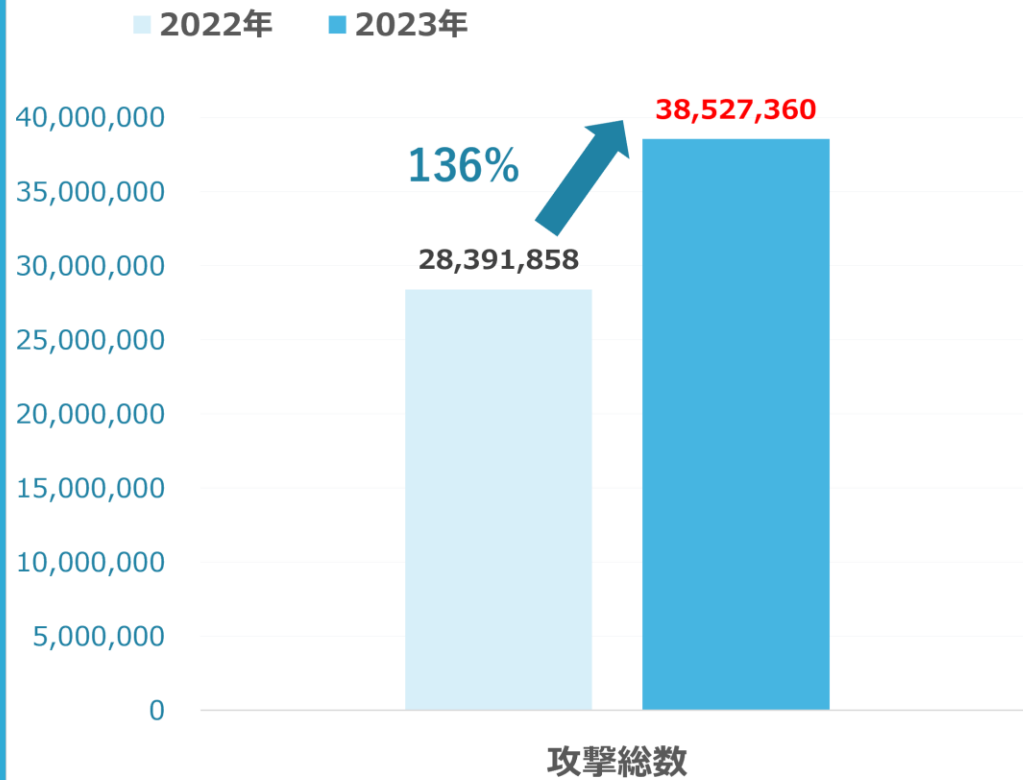
### ▲ 情報セキュリティ10大脅威 2024 [組織]

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い (2016年以降)
1	ランサムウェアによる被害	2016年	9年連続9回目
2	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目
6	不注意による情報漏えい等の被害	2016年	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目

<https://www.ipa.go.jp/security/10threats/10threats2024.html>

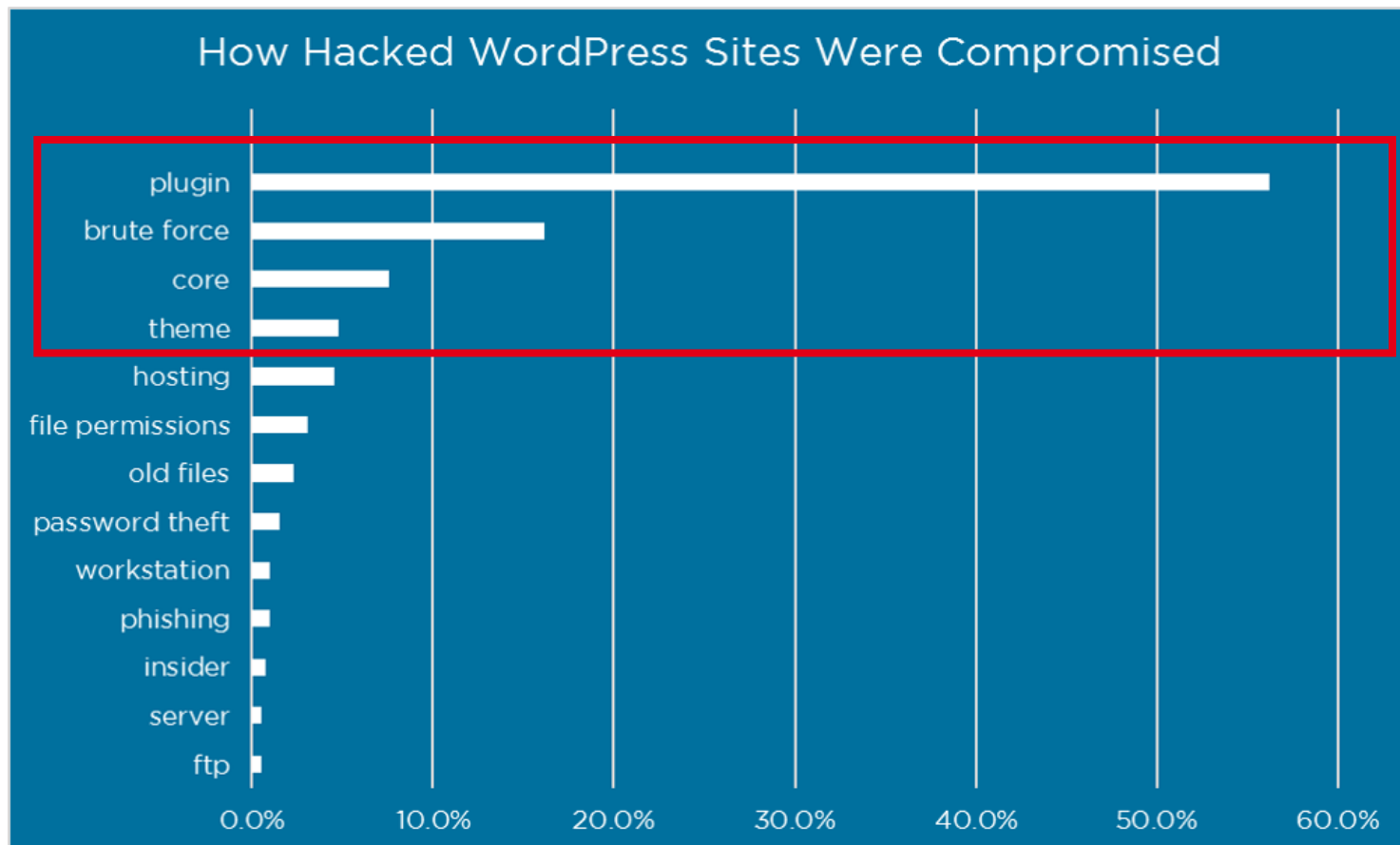
# WordPressの攻撃の増加

## WordPress



# 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



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/>

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

# なぜ最新にアップデートできないのか

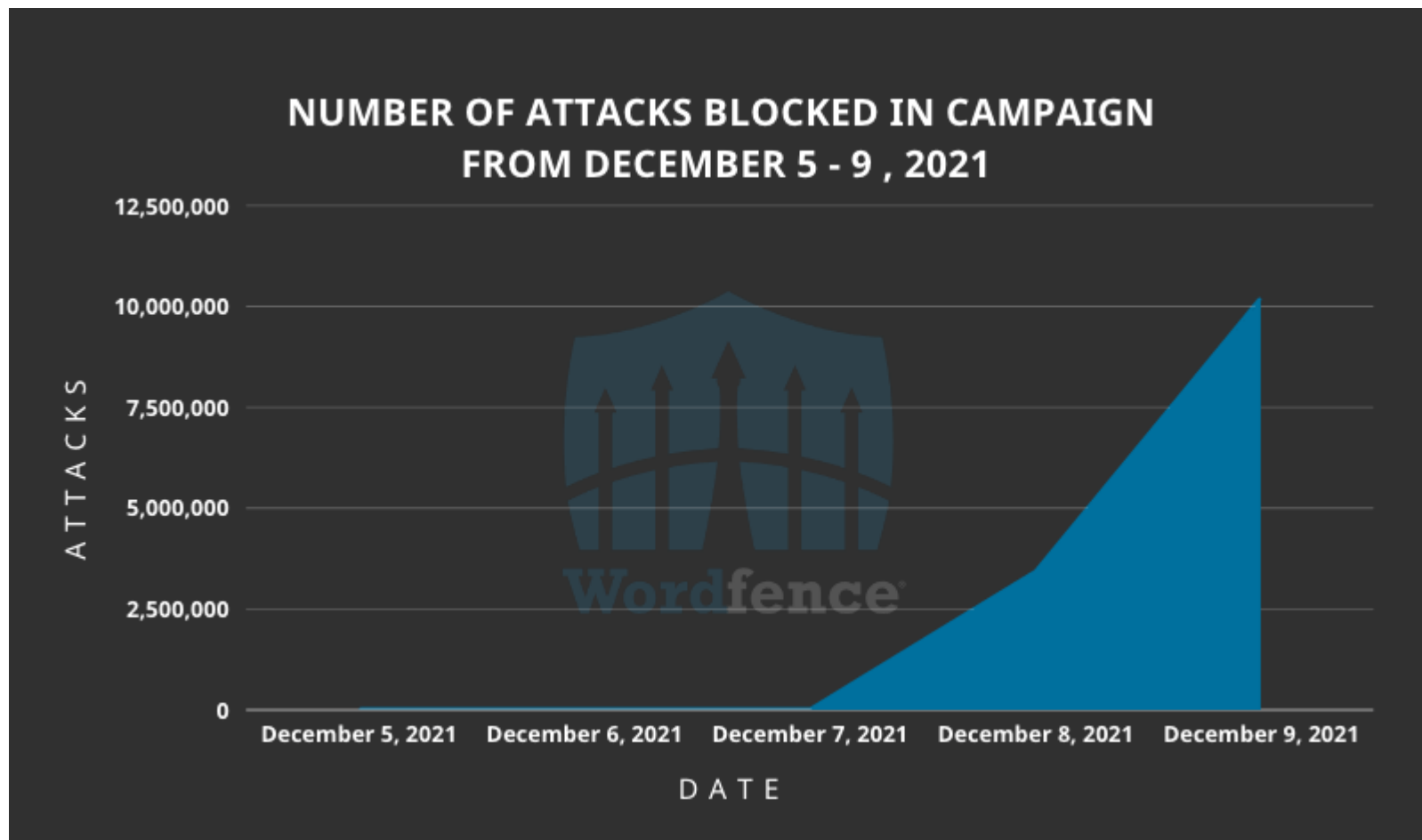
- 主に以下の原因があります。
  - カスタマイズがあり、バージョンアップにコストと手間がかかる
  - プラグインが多すぎて、バージョンアップにコストと手間がかかる
  - 詳しい人がいなくなり、バージョンアップを行うにはまず調査から行わないといけなく、さらにバージョンアップにコストと手間がかかる
  - 責任分担が不明確な個所があり、調整が必要になり、さらにバージョンアップにコストと手間がかかる
    - OSやミドルウェアはA社が保守をしているが、WordPressはコンテンツ管理しか依頼していなく、WordPressの保守やカスタマイズ部分やプラグインの保守までは担当している人がいない
  - 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！**

# 増加するWordPressサイトへの攻撃

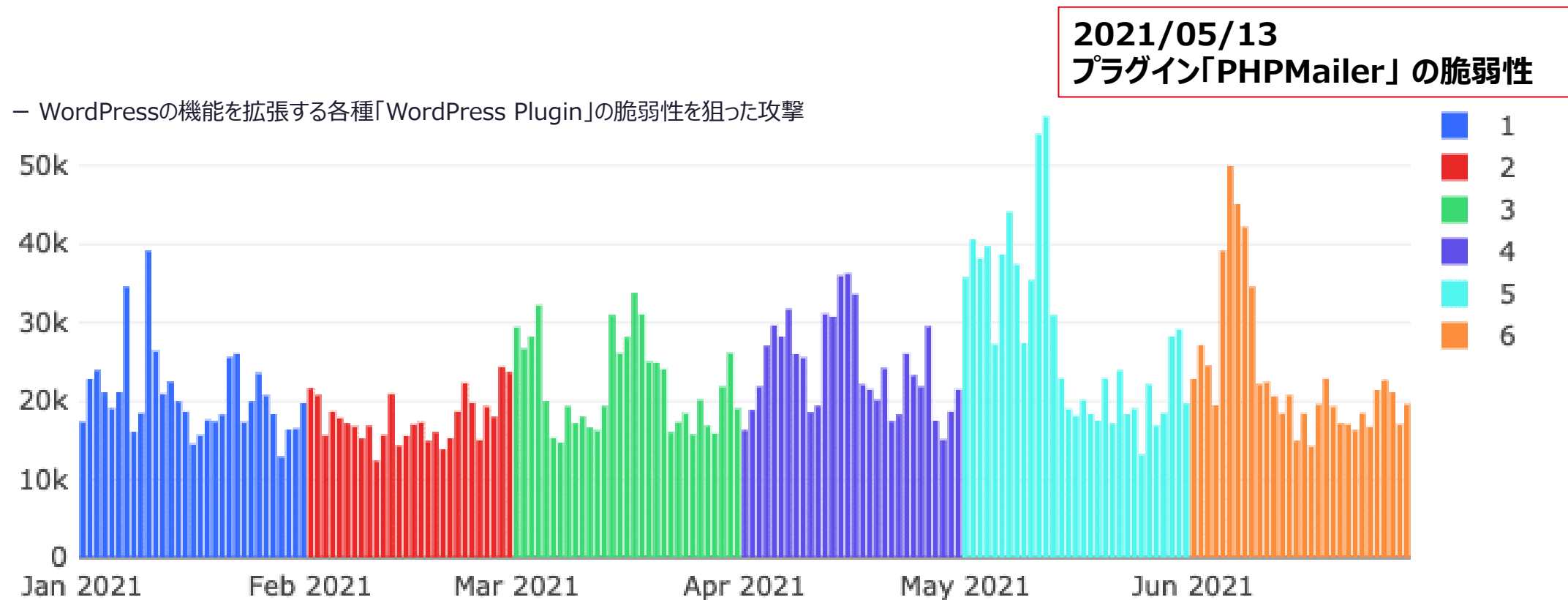
## 短期間・大量攻撃のリスク

**36時間の間に160万のWordPressサイト**が16,000のIPから**1,370万回の攻撃**を受けた



# 増加するWordPressサイトへの攻撃

プラグインの脆弱性が見つかったタイミングで攻撃が増加していることから、早急なアップデートが必要なことがわかる。



# バージョンアップは月何回が良いのか

---

- 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。
- KUSANAGI Security Editionで安全に自動アップデートがお勧めです！

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

どこまで守るか、どうやって守るか





# どうやって守るのか

- 侵入されない（サーバ・アプリケーション）
  - IP制限・basic認証
  - アカウントの管理（多要素認証など）
  - 複雑なパスワード・使いまわしをしない
  - IPS/IDS
- 適切なアップデート
  - ミドルウェアのアップデート
  - アプリケーションのアップデート
- セキュリティツールの導入
  - WAF
  - マルウェア・アンチウイルス対策
  - 改ざん検知
  - 定期的な脆弱性検査
- 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）
  - ドメインやSSLもセキュリティに係る大事な資産



**自社サイトの  
管理状況を  
把握するところから**



# 今すぐできる対策

---

- 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。
- 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。

# どうやって守るのか

- 管理画面の保護
  - **強固なパスワード** (WordPressがレコメンド)
  - **IP制限・basic認証** (ログインURLを変更しても安心しない)
  - シングルサインオン
- **WordPress本体・プラグイン・テーマのアップデート** (自動アップデート機能の活用)
- ユーザー管理
  - 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)
- 不要なプラグイン・テーマの削除
- ファイルパーミッションの適切な設定
- 設定ファイル (wp-config.php) の位置
- XML-RPCの無効化
- 個人情報の外部DB化



**アップデートと  
管理画面の保護で  
多くの脅威は防げる**



KUSANAGI開発メンバーのエンジニアブログ

## 小さなプラグインを作り、 WordPressのXML-RPCを 停止する方法

「小さなプラグインを作り、WordPressのXML-RPCを停止する方法」by福田拓朗  
[https://www.prime-strategy.co.jp/column/archives/column\\_8952](https://www.prime-strategy.co.jp/column/archives/column_8952)

# こんなお客様も

---

- 「専門の業者にフルサポートいただくことで、リスクヘッジをしています。」というお客様が多いです。
- プライム・ストラテジーはWordPressの国内屈指の技術力を持つ会社であり、技術力が高いフルスタックエンジニアが多く在籍しています。
- ウェブセキュリティに関しても経験が豊富で、国内屈指の技術力を持っていると自負しています。

**是非、当社にお任せください！**

# 事例集



# 豊富なWordPress構築・運用実績



ヤマハWeb音遊人 (みゅーじん)



メルセデスベンツ日本



りそな銀行



住友不動産



新潮社



扶桑社





お知らせ



# KUSANAGIマナーズドサミット

KUSANAGIサミット2024オンライン無料開催

業界トップランナーによる、  
Webセキュリティと収益性と



市場動向を学ぶWebの祭典

12月4日開催、徳丸本・Python本の抽選あり



<https://enterprise-wordpress.doorkeeper.jp/events/178505>

# Web担当者フォーラム

超高速CMS実行環境「KUSANAGI」の  
プライム・ストラテジーが登壇します。



「Web改ざん匿名事例解説、  
セキュリティはどこまでやれば十分なのか」  
～稟議に使える市場データとCMSセキュリティ対策事例を紹介～

創刊18周年



## Web担当者Forum ミーティング 2024 秋

11.19(火) » 20(水) 10:30-17:15

虎ノ門ヒルズフォーラム5階(リアル開催)

#webtan



聴講無料  
(事前登録制)

主催：株式会社インプレス / Web担当者Forum

<https://webtan.impress.co.jp/events/202411>

※初日の基調講演の後です。

# MTDDC Meetup TOKYO 2024



- 私達はみた！ Webサイトに潜むヒヤリハット & アップデートはセキュリティ対策の大事な第1歩 Room C 13:25 - 14:10
  - 登壇者 相原知栄子、吉政忠志
- ブースでは、特製Tシャツのプレゼント抽選会を行う予定です。

# パートナープログラムを刷新しました

---

- 大きな改善点
  - マーケティング支援がかなり強化されました。
  - グレードによって再販ができるようになりました。
  - グレードによって共同の営業目標を設定でき、協業を強化できるようになりました。
- 興味がある方は、アンケートでお申し付け下さい。
  - 是非、私にお声がけください。協業戦略の立案の支援をさせてください。

情報源



# KUSANAGIの各種情報

---

- KUSANAGI公式サイト : <https://kusanagi.tokyo>
- はじめてのKUSANAGI : <https://kusanagi.tokyo/readme/>
- KUSANAGI Tech Column : <https://www.prime-strategy.co.jp/column/>
- KUSANAGIユーザーフォーラム : <https://users.kusanagi.tokyo/>
- WEXAL公式サイト : <https://www.wexal.jp/>
- 草薙沙耶公式X [https://twitter.com/kusanagi\\_saya](https://twitter.com/kusanagi_saya)



# Thanks!



本資料に掲載されている社名、製品名などは、各社の登録商標または商標です。

© Prime Strategy Co., Ltd.

