WordPress公式が推奨しているセキュリティ対策方法

結論から言うと、WordPress公式が強く案内しているのは、**特定の監査ログ製品そのもの** ではなく、**セキュリティを強化するための基本原則と運用方法** です。したがって、実務で説明する際は、**「公式推奨の考え方」と「その実装手段」** を分けて示すのが正確です。[1][2]

まず押さえるべき公式推奨事項

WordPress公式文書から見ると、優先順位が高いのは、**最新状態の維持**、**信頼できる入手元の利用**、**強い認証**、**バックアップ**、**ログと監視**、そして **サーバー・ファイル・管理画面のハードニング** です。[1][2]

推奨方法	公式上の位置づけ	実務でやること
WordPressを最新に保つ	最重要。古い版は安全更新されないため更新継続が重要	コア、プラグイン、テーマの更新を徹底する
自動更新を使う	3.7以降の自動更新を活用して最新維持を容易にする	セキュリティ・マイナー更新を自動化し、必要に応じてプラグイン・テーマも自動更新する
信頼できる配布元だけを使う	非信頼ソースのテーマ・プラグインを避ける	WordPress.org や著名ベンダーに限定する
強いパスワードと多要素認証	管理者保護の基本	強固なパスワード、可能なら2段階認証を有効化する
バックアップを取る	侵害や更新失敗に備える準備として重要	DBとファイルの定期バックアップ、復元テスト
ログ取得と監視	フォレンジックと早期検知に重要	アクセスログ、変更ログ、ファイル変更監視を整える
管理画面・設定ファイルの保護	侵入口の削減	`/wp-admin/` 保護、`wp-config.php` 保護、ファイル編集無効化
HTTPS と権限制御	通信と権限の保護	SSL化、不要権限の削減、適切なファイル権限設定

公式寄りに言うなら、この順番が妥当です

WordPress公式の内容に忠実に並べるなら、最初に提示すべき方法は **更新の継続** です。公式ハードニング文書では、古いバージョンはセキュリティ更新が提供されず、3.7以降は自動更新を使って最新状態を保ちやすくなっていると説明しています。[1] また、プラグインとテーマについても、5.5以降は個別に自動更新を有効化でき、通常は1日2回自動更新が走り、結果通知メールも送られます。[2]

次に重要なのが、**バックアップと復旧可能性の確保** です。WordPress公式は、自動更新を前提にするなら、失敗時に戻せるよう定期バックアップを取るべきだと案内しています。[2] これは単なる保険ではなく、セキュリティ運用の一部です。

その次に来るのが、**ログと監視** です。WordPress公式の *Hardening WordPress* では、ログは何が起きたかを理解するうえで重要であり、侵害後の調査や異常把握に役立つと説明されています。[1] ただし、ここでの公式姿勢は **「ログ・監視を行うべき」** というレベルであり、**WP Activity Log を公式標準として指定しているわけではありません。**[1]

つまり、あなたに提示すべき「推奨方法」

実務でそのまま提案するなら、私は次のように整理します。これは **WordPress公式の考え方に沿った順番** です。

優先度	推奨方法	理由
1	WordPressコアを常に最新に保つ	既知脆弱性への露出を減らすため
2	プラグイン・テーマの自動更新を有効化する	攻撃対象になりやすい周辺部品の更新漏れを防ぐため
3	定期バックアップと復元手順を整える	更新失敗や侵害時に戻せるようにするため
4	強いパスワードと多要素認証を導入する	アカウント侵害を防ぐため
5	信頼できる配布元のテーマ・プラグインだけを使う	サプライチェーン起点のリスクを減らすため
6	ログ取得と監視を導入する	侵害や不正操作の早期発見と事後調査のため
7	`wp-admin`、`wp-config.php`、ファイル編集権限を保護する	攻撃面を減らすため

8	必要に応じて監査ログプラグインを使う	変更追跡の実装手段として有効だが、製品名指定は公式推奨ではないため

WP Activity Log の位置づけ

したがって、**WP Activity Log は「公式が推奨している方法」そのものではなく、公式が重要だと述べる『ログ取得・監視』を実装するための一つの選択肢** と表現するのが最も正確です。[1][3] もし説明文を安全に書くなら、次の言い方が適切です。

> WordPress公式は、ログ取得・監視・バックアップ・更新継続などの基本対策を重視しています。その実装手段として、監査ログ系プラグインを導入するのは実務上有効です。

ひとことで言うと

公式が推奨しているのは「WP Activity Log」という製品名ではなく、更新・認証強化・バックアップ・ログ監視・ハードニングという方法論です。 WP Activity Log は、そのうち **ログ監視・変更監査を実現する実装候補の一つ** です。[1][2][3]

References

[1] Hardening WordPress – Advanced Administration Handbook
[2] Plugin and themes auto-updates – Documentation – WordPress.org
[3] WP Activity Log – WordPress plugin