



WORDPRESS + LINUX HOST PROTECTION

侵入の兆候を、 暗号化の前後で捉える。

WordPressとLinuxホストを二層で監視する
ランサムウェア早期警戒システム。

不審アクセス、Web shell、権限変更、Canary破壊、大量改変、未知拡張子、身代金要求文書、Agent停止までを相関。単一イベントではなく「一連の攻撃兆候」として評価します。

● WordPress Monitoring

● Linux Agent

● Emergency Lockdown

● Signed Heartbeat

Detect

HTTP・認証・Web shell・ファイル改変・OS
側兆候を継続監視。

Correlate

複数の兆候をスコアリングし、HIGH /
CRITICALへ段階評価。

Contain

必要時のみ段階的Lockdown。自動隔
離は安全側に初期OFF。

WordPress / Linux 二層監視。

アプリケーション層・OS層・外部監視を分離。WordPressが停止した場合でも、OSが稼働していればAgentが監視を継続できます。



WordPress停止 ≠ 監視停止

WordPress/PHPが停止してもLinux Agentが稼働していれば、OS側監視とローカルイベント保持を継続できます。外部Heartbeatを併用すれば、死活監視をさらに強化できます。

役割を明確に分離

Pluginはアプリケーション層、Agentはホスト層。どちらか一方に依存しすぎない設計です。

単発イベントではなく、 「攻撃の流れ」を相関して判定。

正常な管理操作と攻撃兆候を同列に扱わず、複数シグナルの組み合わせでSeverityを上げます。v2.0.2ではWeb shell検知にrequest-taint / data-flow判定を導入し、正規callbackコードの誤検知を抑制しています。



WS

Web shell heuristic

v2.0.2

外部入力が可変call targetや実行引数へ実際に到達したかを簡易追跡。単なる同一ファイル内共存では強く加点しません。

FI

File integrity + Canary

重要ファイルをSHA-256で監視。通常操作では触れないCanaryの変更・削除を高確度シグナルとして扱います。

RX

Ransomware correlation

大量変更、同一未知拡張子付加、ファイルヘッダー破壊、身代金要求文書などを組み合わせてCRITICAL化します。

AU

Auth / privilege monitoring

ログイン失敗集中、管理者作成、権限昇格、プラグイン・テーマ操作など、侵入後の足場形成も監査します。

Severity & Risk Score

NOTICE		20+
WARNING		40+
HIGH		70+
CRITICAL		100

※ ルールにより直接HIGH / CRITICALへ昇格する場合があります。

Response by design

1 Alert

HIGH / CRITICALを管理画面・メール・Heartbeatで通知。

2 Restricted

更新・追加・削除などコード変更経路を停止。

3 Hard Lockdown

投稿・メディア・REST書き込み等を含め読取り優先へ。

4 Safe default

Auto Lockdownは初期OFF。運用確認後に段階的に有効化。

安全側に導入し、 監視結果を見ながら段階的に強化。

初日から自動遮断を強制する設計ではありません。まずDetect / Observeで環境固有の正常挙動を把握し、必要に応じてContainへ進めます。

1

WordPress Pluginを導入

既存サイトへZIPでインストール。初期状態は自動遮断OFF。

2

Deep Scanで初期確認

Baseline、Web shell、Canary、変更傾向を確認。

3

Linux Agentを追加

Python 3標準ライブラリのみ。systemdでホスト側監視を継続。

4

Heartbeatを外部へ

別障害ドメインへ死活を送り、WordPress停止も監視対象へ。

5

必要に応じてLockdown

RESTRICTED / HARDを段階設定。自動化は十分な観察後に。

Full Bundle

- ☐ WordPress Plugin ZIP
- ☐ Linux Agent / Python 3
- ☐ systemd service / install scripts
- ☐ Agent sample JSON
- ☐ Architecture / Communication Spec
- ☐ Regression Test / Fix Notes

安全境界

- ✓ 遠隔シェルを搭載しない
- ✓ 任意コマンド実行をしない
- ✓ 自動process killをしない
- ✓ iptables/nftablesを自動変更しない
- ✓ Webサーバを自動停止しない
- ✓ 不審ファイルを自動削除しない

こんな環境に

- WordPressを業務・予約・会員導線に利用しているサイト
- プラグインやテーマ更新が多く、改変監視を強化したい環境
- Web shell・大量暗号化・不審ログインを一つの監査画面で追いたい環境
- WordPressだけでなくLinuxホスト側の兆候も把握したい環境

Detect before damage spreads.

Ransomware Sentinelは、アンチウイルスやEDR、バックアップを置き換える製品ではありません。WordPressとLinuxホストの「早期警戒センサー」として、攻撃兆候を見逃さないための観測層を追加します。

RANSOMWARE SENTINEL v2.0.2
WordPress + Linux Host Ransomware Detection System