TRUSTORIGIN

Webサイト改ざん検知サービス

正しい状態を、原本で持つ。



検知し、証拠を保全し、元に戻すまで。

TRUSTORIGIN DVE は、公開サーバーのファイルを「原本」と比較します。既知のパターンを探す方式ではないため、未知の攻撃でも差分として現れ、検知できます。

なぜ、改ざんに気づけないのか

改ざんは、サイトが正常に見えたまま進行します。攻撃者は目立つ痕跡を残さず、気づいたときには検索結果から除外されていた、という形で表面化します。従来の方式には、次の限界があります。

従来の改ざん検知の、3つの限界

- ✕ **既知のパターンに無い攻撃は、検知できない**
- ✕ **検知できても、元に戻すのは手作業のまま**
- ✕ **復旧を急ぐと、原因を追う証拠が消えてしまう**

SOLUTION — 解決のアプローチ

「正しい状態」を手元に持ち、定期的に突き合わせる

DVEは公開サーバーとは別の場所に原本（ベースライン）を保管し、定期的に公開サーバーと比較します。原本に無い変更はすべて差分として現れるため、攻撃手法を知らなくても検知できます。そして原本があるということは、元に戻せるということでもあります。

DVEがもたらす、3つの価値

原本との比較で検知

既知のパターンに頼らないため、未知の攻撃も検知できます。

証拠を保全してから復旧

改ざんファイルを保全した上で戻します。原因を追う材料が残ります。

原本から自動で復旧

改ざんされたファイルを、正しい状態へ自動で戻します。

仕組みと、対応環境

TRUSTORIGIN DVE　総合案内

TRUSTORIGIN

改ざん検知の流れ

① **原本を保管**
公開サーバーとは別の場所に保管

② **定期的に比較**
スケジュールに従い差分を抽出

③ **検知・証拠保全**
改ざんファイルを先に保全する

④ **原本から復旧**
正しい状態へ自動で戻す

対応環境

多様な接続方式

SSH（rsync）／FTP／FTPS／SFTP に対応。サーバーから折り返す接続方式も選べ、受け口を開けずに導入できます。

SaaS・オンプレ両対応

クラウドでの提供に加え、自社環境に設置しての運用も可能です。データを外部に出さない構成が選べます。

複数サイトを一元監視

1つの管理画面で、複数サーバー・複数サイトをまとめて監視できます。サイトごとに検査周期や除外設定を変えられます。

主な機能

1. **原本配信**
原本に置いたファイルを公開サーバーへ配信。原本が唯一の正しい状態になります。
2. **通知**
メール／Slack／Webhook に対応。検知時に外部システムへ連携することもできます。
3. **誤検知対策**
頻繁に変わるファイルの除外設定と、更新作業中に検知を止めるメンテナンス機能。
4. **モニター権限**
閲覧のみのユーザーを作成し、担当サイトだけを開放。顧客や他部署への共有に。
5. **監査ログ**
誰がいつ、どの設定を変更し、どの操作を実行したかを記録します。

用途に応じた、専用の機能

それぞれ専用のご案内をご用意しています。詳しくはブースでお申し付けください。

WordPress対応

正当な更新と改ざんを見分ける。DBの監視も

サプライチェーンスキャン

脆弱性・既知の悪性コード・公式版との照合

AI一次調査

検知の先へ。原因と対処案を数分後に

導入方式

穴を開けない接続とリアルタイム検知

→　検知して終わりにしない。戻せるところまでが、改ざん対策です。

お問い合わせ　アットシグナル株式会社
TEL　073-499-6588　／　E-mail　sales@at-signal.jp

TRUSTORIGIN

WordPress対応 — Webサイト改ざん検知サービス

「正しい更新」と「改ざん」を、見分ける。



更新はそのまま、改ざんだけを見逃さない。

WordPressサイトの改ざんを検知し、原本から自動で元に戻します。ファイルだけでなく、データベース上の改ざんも監視します。

なぜ、WordPressの改ざん検知は難しいのか

WordPressは毎日更新されます。記事の投稿、プラグインの更新、自動アップデート――正当な変更が絶え間なく発生するため、「ファイルが変わった＝改ざん」と単純に判定できません。

従来の改ざん検知の、3つの限界

- ✕ **正当な更新と改ざんの区別がつかない**
- ✕ **誤検知が多く、アラートが形骸化してしまう**
- ✕ **自動で復旧できず、復旧作業は手作業のまま**

SOLUTION — 解決のアプローチ

解決のカギは、WordPress内に置く「キーパー（門番）」

DVE専用プラグインをWordPressに導入します。プラグインが管理画面での操作や更新を見張り、「これは正当な変更」とDVEへ伝達。DVEは、プラグインが正当と伝えていない変更だけを「改ざん」と判定できます。

DVEがもたらす、3つの価値

改ざんだけを検知

正当な更新は自動で除外。本当に危険な変更だけを通知します。

自動で復旧

改ざんされたファイルを、原本から元の状態へ自動で戻します。

運用はそのまま

WordPressをいつも通り更新するだけ。特別な作業は不要です。

仕組みと、ファイルの監視

TRUSTORIGIN DVE　WordPress対応

TRUSTORIGIN

改ざん検知の仕組み

WordPress サーバー
WordPress ＋ DVEプラグイン（キーパー）

↓ ① プラグインが「正当な変更」をDVEへ登録

DVE 管理サーバー
原本（ベースライン）と照合し、登録されていない変更＝改ざんを検知

↓ ② 改ざんと判定

改ざんファイルを自動で復旧　／　管理者へ即時通知

プラグインが捕捉する「正当な変更」

- ✓ メディアの追加（サムネイル含む）
- ✓ 記事・固定ページの投稿・更新
- ✓ プラグイン／テーマ／コアの追加・更新
- ✓ 管理画面のファイルエディタでの編集

誤検知を防ぐ、3つの仕掛け

除外設定

キャッシュやログなど、頻繁に変わるファイルをあらかじめ対象外にします。

メンテナンスウィンドウ

プラグインやコアの更新中は検知を止め、更新の完了とともに自動で再開します。

学習モード

導入直後は観測のみ。実際に変わるファイルを見てから除外設定を決められます。

ファイル監視の主な機能

1. **正規変更の自動登録**
   プラグインが捕捉した正当な変更を、原本（ベースライン）へ自動で反映。
2. **改ざんの検知**
   原本に登録されていない変更を、改ざんとして検知し管理者へ通知。
3. **自動復旧**
   改ざんされたファイルを、原本から元の状態へ自動で復元。

検知できる脅威の例（ファイル）

- Webシェル・不正PHPファイルの設置
- 既存ファイルへの不正コード埋め込み
- アップロード領域への実行ファイル設置
- ファイルの不正な削除・差し替え

▶ 情報システム担当者の方へ

改ざんを見逃さず、復旧まで自動化。日々の監視・運用の負担を増やしません。

▶ サイト制作者の方へ

通常の更新やカスタマイズはそのまま。あなたの正当な作業が改ざん扱いされることはありません。

データベースの監視と、導入

TRUSTORIGIN DVE　WordPress対応

TRUSTORIGIN

ファイルには現れない改ざんがある

SQLインジェクションや管理画面の乗っ取りによる改ざんは、データベースの中だけで完結し、ファイルには一切現れません。ファイルの監視では原理的に検知できない領域です。DVEはここも監視します。

1 DB値監視

サイトURL・管理者メールアドレス・有効なテーマ／プラグイン・管理者アカウント一覧などを定期的に報告し、正常値とのズレを検知します。

2 コンテンツ注入監視

投稿の本文・タイトル・抜粋や、カスタムHTMLウィジェット等に埋め込まれたスクリプト・iframe・不正リダイレクトを検知します。

3 記事変更検知

記事・固定ページ・カスタム投稿の追加／更新／削除を通知。本文はサーバーへ送らず、サイト側で計算したハッシュだけで判定します。

検知できる脅威の例（データベース）

- **サイトURL・管理者権限の不正変更**
- **投稿へのスパムスクリプト埋め込み**
- **不正な管理者アカウントの追加**
- **身に覚えのない記事の書き換え・削除**

キーパー自身を、守る

管理画面を乗っ取った攻撃者がプラグインを止めて検知を無力化する手口に、三層で備えます。

● **停止時の通知**	プラグインが停止されるとき、沈黙する前にDVEへ通知します。
● **設定変更の通知**	接続設定やAPIトークンの変更を通知。通知先はDVE側のため書き換えられません。
● **沈黙検知**	報告の途絶をDVE側が検知。WordPressの外側で動くため止められません。

導入は、4ステップ

1. **WordPressにプラグインを導入**
2. **APIキーとDVEのURLを設定**
3. **学習モードで実際の変更を観測**
4. **除外設定を整えて本稼働へ切り替え**

→　**あとは、WordPress をいつも通り更新するだけ。**

キーパーは自動で最新に保たれます

プラグインの更新作業は不要です。DVEサーバーから配信され、キーパー自身が自動で更新されます。

動作要件

WordPress 5.6 以上　／　PHP 7.4 以上　／　動作確認済み WordPress 6.7

お問い合わせ　アットシグナル株式会社

TEL　073-499-6588　／　E-mail　sales@at-signal.jp

TRUSTORIGIN

サプライチェーンスキャン ― Webサイト改ざん検知サービス

改ざんされていなくても、危険な状態はある。



公式版のまま、脆弱性は公表される。

原本と一致していても、そのソフトウェア自体に穴があれば攻撃は成立します。導入されているコンポーネントを棚卸しし、照合することで、改ざん検知だけでは見えない危険を見つけます。

「原本と一致している」＝安全、ではない

改ざん検知は「正しい状態から変わったか」を見ます。ところが攻撃の多くは、ファイルを書き換えずに成立します。正規のまま公表された脆弱性を突かれる、配布元で汚染されたものを掴まされる――いずれも差分としては現れません。

改ざん検知だけでは見えない、3つの危険

- ✕ **公式版のまま、後から脆弱性が公表される**
- ✕ **正規のプラグインやテーマを装って、改変されている**
- ✕ **既知のマルウェアやWebシェルが紛れ込んでいる**

SOLUTION ― 解決のアプローチ

「何が、どの版で入っているか」を正確に持つ

DVEは原本から、導入されているコンポーネントとそのバージョンを棚卸しします。推測ではなく実物からの一覧なので、「このサイトに何が入っているか」を断定できます。この一覧を公式配布物・既知の悪性コード・脆弱性情報と突き合わせます。

サプライチェーンスキャンの、3つの価値

公表と同時に気づく

脆弱性が公表された時点で通知。ファイルが変わっていなくても届きます。

正規を装った改変を見抜く

公式配布物とハッシュを突き合わせ、中身が違うものを検知します。

対処の順番がつく

深刻度と悪用の実績から優先度を算出。どれから手を付けるか判断できます。

3つの照合と、対応範囲

TRUSTORIGIN DVE　サプライチェーンスキャン

TRUSTORIGIN

3つの照合で、危険を洗い出す

1 公式配布物との照合

コア・プラグイン・テーマが、公式に配布されているものと一致するかをファイル単位で突き合わせます。正規を装って中身だけ差し替えられたものを検知します。

2 既知の悪性コードの検知

Webシェルの署名、既知マルウェアのハッシュ、難読化された動的コード、不自然に高いエントロピーの文字列――複数の観点から悪性の痕跡を探します。

3 脆弱性・評判の照合

棚卸ししたバージョンを脆弱性情報と突き合わせます。既知の悪性パッケージや、正規に似せた名前のパッケージも照合します。

ファイルが変わっていなくても、通知が届く

脆弱性の照合は、ほかの検査と性質が違います。

サイトに何も起きていなくても、アドバイザリが公表された瞬間に「該当します」と判定されます。つまり、攻撃される前に手を打てるということです。深刻度は、脆弱性そのものの評価に加えて、実際に悪用されている実績と悪用されやすさを加味して算出するため、対処の順番をつけられます。

対応範囲

WordPress

コア／プラグイン／テーマ

パッケージ管理

npm／PyPI／Packagist
Go／Maven／RubyGems／NuGet

検知できる例

- 公式版のまま公表された脆弱性
- 正規を装って改変されたプラグイン
- 紛れ込んだWebシェル・既知マルウェア
- 難読化された動的実行コード

運用の考え方

重大度で仕分けて渡します

確度の高い検知と、念のため挙げたレビュー候補を分けて提示します。すべてを同じ重さで通知することはありません。

改ざん検知とあわせて1画面で

改ざんのアラートと同じ管理画面で確認できます。通知先も既存の設定をそのまま使えます。

→　改ざんされてから気づくのではなく、狙われる前に塞ぐ。

お問い合わせ　アットシグナル株式会社
TEL　073-499-6588　／　E-mail　sales@at-signal.jp

※ 脆弱性情報は各アドバイザリデータベースを参照しています。出典および著作権表示は、DVEの管理画面および通知に記載しています。

TRUSTORIGIN

開発中
本機能は現在開発中の機能です

AI一次調査 — Webサイト改ざん検知サービス

検知して、終わりにしない。



改ざんの「原因」まで、検知の数分後に。

どのコンポーネントに穴があるのか。他に何が置かれたのか。次に何をすべきか。

なぜ、改ざん対応は「検知」で止まるのか

改ざんが検知されても、その先は人の仕事です。担当者がサーバーに入り、ログを追い、どのプラグインのどのバージョンが入っていたかを調べ、対処を決める。深夜のアラートなら、その数時間がまるごと発生します。

改ざん検知の、その先にある3つの壁

- ✕ **検知は自動でも、原因の調査は手作業のまま**
- ✕ **「どこから入られたか」が分からないまま復旧し、再び改ざんされる**
- ✕ **ログの読み方・脆弱性の調べ方が、特定の担当者に属人化している**

SOLUTION — 解決のアプローチ

AIは、お客様の管理下で動かします

DVEは「何が・いつ変わったか」を確定して渡します。AIは「それが誰の仕事で、どこに穴があるのか」を、お客様の環境で判断します。DVEは全ファイルの原本、導入バージョンの正確な一覧、改ざんできない検知区間、保全済みの検体を持っている——人が手作業で集めるより速く、正確な材料です。

DVEのAI一次調査が、ほかと違う点

数分後に、一次所見

脆弱なコンポーネントの名指し、影響範囲、対処案まで。担当者は「判断」から始められます。

AIにサーバーの鍵を渡さない

AIが本番サーバーでコマンドを実行することはありません。監査ログつきの読み取りのみです。

ファイルの中身は外に出ない

改ざんファイルの内容がベンダーのAIに渡ることはありません。お客様ご自身のAI契約の中で完結します。

一次調査の中身

TRUSTORIGIN DVE　AI一次調査

TRUSTORIGIN

検知から、一次所見まで

① 改ざんを検知（DVE） → ② 調査を起動（GitHub） → ③ 材料を受け取る（DVEから） → ④ 不足分を収集（DVE経由・読取専用） → ⑤ 一次所見を提示（根拠つき）

※ 改ざんされたファイルの中身や差分が GitHub 上に書き込まれることはありません。実体はAIがDVEから直接取得します。

一次所見の例

検証環境の実データ（WordPressサイト1件）に対し、実際に生成された所見を要約して掲載しています。

判定

改ざんの可能性が高い ／ 確信度：高

uploads 配下に置かれた **icon.png.php** が既知Webシェル「WSO Shell」とハッシュ一致。画像を装った二重拡張子です。同種の痕跡が計4か所にあり、定着した足場です。

推定される経路

確信度：中

本サイトは WordPress 7.0.2。**CVE-2026-65640（CVSS 8.8／ファイルアップロード経由の RCE）**の影響下。Webシェルの設置場所が、この脆弱性が生む痕跡と一致します。

ただし

当該CVEは Author 権限以上の認証が前提です。この経路ならアカウントが既に奪われています。version.php も公式配布物とハッシュ不一致で、バージョン表記自体が偽装の可能性も残ります。

推奨アクション

いずれも実行前に承認が必要です。

1. **認証情報の全面ローテーション**（WP管理者・投稿者／FTP／DB／管理パネル）—— 最優先
2. **更新**　WordPress 7.0.2 → 7.0.4以降　ほか2件
3. **入口を塞いだ後に、4か所を順に除去**

判定不能

情報が外部に漏洩したかどうかは判定できません。可能性の否定もできません。

CVE が実際に使われたかの確定もできません（POST の本文はログに残らないため）。

分かること、分からないこと

○　分かること

- 脆弱なコンポーネントの名指し
- サーバー上に他に何が置かれたかの網羅
- 過去に仕込まれ眠っていたファイルの発見
- Web経由か認証情報の窃取かの切り分け
- 同じ場所が繰り返し狙われていることの指摘
- 復旧・対処の具体的な手順
- 改ざんが起きた時間帯の絞り込み

×　分からないこと

- **情報が漏洩したかどうか**
  原理的に判定できません。否定もできません。
- **侵入に使われた具体的なリクエスト**
  POST の本文はログに残らないためです。
- **攻撃者の特定**
  本機能の目的ではありません。

専門のフォレンジック調査でも同じ結論になります。

導入とご提供物

GitHub をご利用の環境で動きます。構築手順とテンプレートは当社がご提供します。

GitHub リポジトリの構築手順書

受け口をどこに、どう作るかを手順化してご提供します。

GitHub Actions のテンプレート

権限を最小化した参照ワークフロー。改善にも追従します。

判定基準のひな形

作業時間帯やサイトの重要度など、運用に合わせて編集できます。

ご利用の前提　GitHub／GitHub Actions をご利用いただける環境と、AI（LLM）のご契約が必要です。AIの利用料はお客様のご契約に基づきます。

お問い合わせ　アットシグナル株式会社

TEL　073-499-6588　／　E-mail　sales@at-signal.jp

※本資料に記載のAI一次調査機能は現在開発中です。内容・仕様は予告なく変更される場合があります。
※本機能が提示するのは自動生成された一次所見であり、専門家による判断を代行するものではありません。

TRUSTORIGIN

導入方式 — Webサイト改ざん検知サービス

穴を開けずに、
待たずに気づく。

アウトバウンド通信だけで、監視が成立します。

ファイアウォールに受け口を作らずに導入する方式と、検査の間隔を待たずに変更へ反応する方式。どちらもサーバー側から「出ていく」通信だけで動きます。

導入時に、必ず出てくる2つの壁

改ざん検知そのものに納得いただいても、導入の段になると別の話が出てきます。「監視のためにサーバーへ接続を受け入れるのか」という話と、「その方式だと、気づくまでにどれだけかかるのか」という話です。

よくある、2つの障壁

- ✕ **サーバーに、外からの接続を受け入れたくない**
- ✕ **固定IPが無い／NATの内側にあって、外から届かない**
- ✕ **検査の間隔が空くほど、気づくのが遅れる**

SOLUTION — 解決のアプローチ

通信の向きを、サーバー側から出ていく形にする

DVEから接続しに行くのではなく、サーバー側からDVEへ接続する方式を選べます。ファイアウォールに受け口を作る必要がなく、固定IPも要りません。同じ考え方で、ファイルの変更をサーバー側から知らせる方式も用意しています。

2つの方式

1

折り返し接続

サーバーからDVEへ接続を張り、その経路でDVEが検査します。受け口を開けず、固定IPも不要です。

2

リアルタイム検知

サーバー上のエージェントがファイルの変更を捉え、DVEへ知らせます。検査の間隔を待ちません。

2つの方式の、中身

TRUSTORIGIN DVE　導入方式

TRUSTORIGIN

① 折り返し接続　—　受け口を開けずに導入する

対象サーバー
受け口なし・固定IP不要

→

DVE 管理サーバー
この経路で検査する

アウトバウンド接続

受け口を作らない
ファイアウォールに着信を許可する設定が不要です。

固定IPが不要
NATの内側や、IPが変わる環境でも導入できます。

経路は1本だけ
許可するのは、サーバーからDVEへの通信1本です。

② リアルタイム検知　—　検査の間隔を待たない

① **変更を捉える**
サーバー上のエージェントがファイルの変更を検知

→

② **DVEへ知らせる**
変わったパスだけをDVEへ通知

→

③ **その場で検査**
通知されたパスだけを原本と突き合わせ

定期検査では「次の検査まで」が待ち時間になります。リアルタイム検知は変更そのものをきっかけにするため、その待ち時間がありません。変更されたパスだけを検査するので、サイト全体を検査し直す負荷もかかりません。

2つの方式に共通すること

✓ **通信はアウトバウンドのみ**
どちらの方式も、サーバー側から出ていく通信だけで成立します。外からの着信を許可する必要がありません。

✓ **サーバーに置くものは最小限**
常駐するのは軽量なプログラムだけです。サーバー上で任意のコマンドが実行されることはありません。

✓ **既存の運用はそのまま**
検知後の通知・証拠保全・原本からの復旧は、これまでと同じ管理画面と同じ通知先で行えます。

どちらを選ぶか

▶ 折り返し接続が向くケース
セキュリティポリシー上、着信を許可できない／固定IPが無い／NATや閉域に近い環境にサーバーがある

▶ リアルタイム検知が向くケース
改ざんに気づくまでの時間を短くしたい／更新の頻度が高く、検査の間隔を長く取れない

両方を組み合わせることもできます。ご利用環境に合わせてご提案します。

→　監視のために、サーバーを開ける必要はありません。

お問い合わせ　アットシグナル株式会社
TEL　073-499-6588　／　E-mail　sales@at-signal.jp