

# PHPの 脆弱性問題

自社への影響と、企業に必要な対応

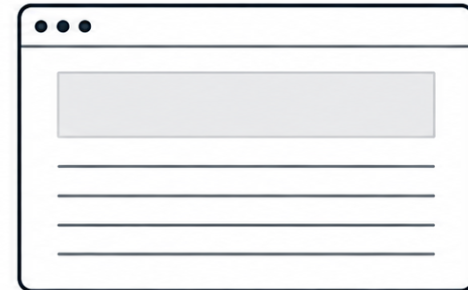
---

脆弱性とは、攻撃者に悪用されるおそれのあるシステムの弱点です。

# PHPは、WordPressなどを動かす技術

ホームページやブログを作るWordPressは、PHPを使って動いています。

記事を開く → ページを作る  
WordPressがPHPを使う → 記事が表示される

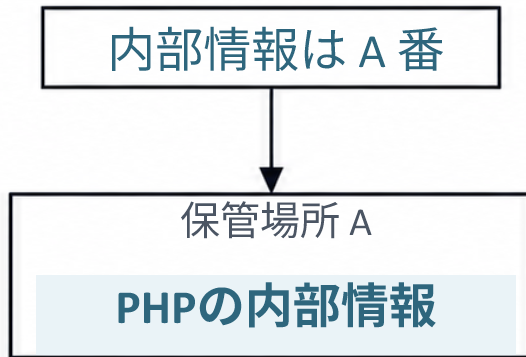


WordPressで作ったサイトの基本的な動き

# 古い記録を使い、別のデータを読み込んでしまう

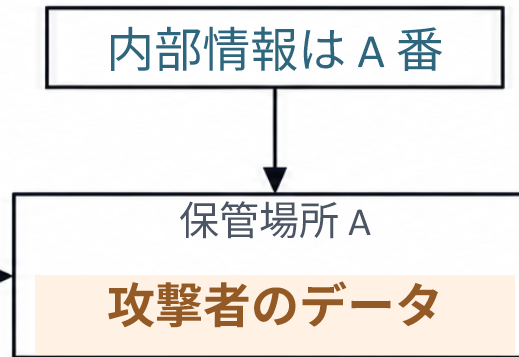
PHPは、処理に使う内部情報を一時的な保管場所（メモリ）に置き、その場所を記録します。古い記録が残ると、同じ場所に入った別のデータを、元の内部情報として扱ってしまいます。

## ① 置き場所を記録する



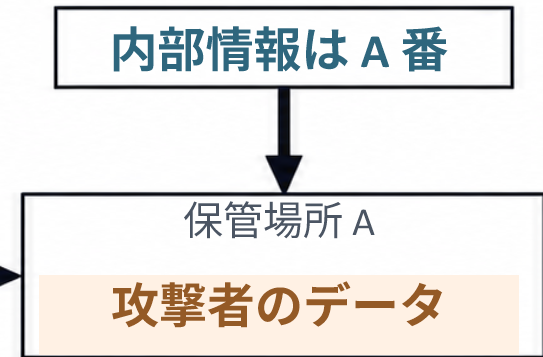
PHPは内部情報を保存し、「A番にある」と記録する。

## ② 中身が入れ替わる



異常終了で記録だけが残ри、空いたA番が再利用されて、攻撃者のデータが入る。

## ③ 古い記録で読み込む



PHPは古い記録を使い、A番の中身を元の内部情報と取り違えてしまう。

**実行する処理を決める情報まで取り違い、不正な操作につながるおそれがあります。**

図は今回の不具合の一例です。攻撃が成功する条件や、操作できる範囲は環境によって異なります。

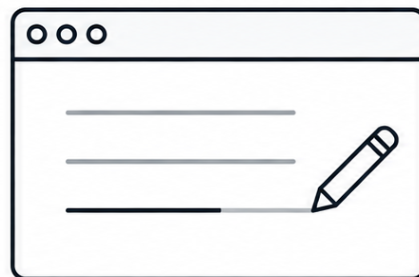
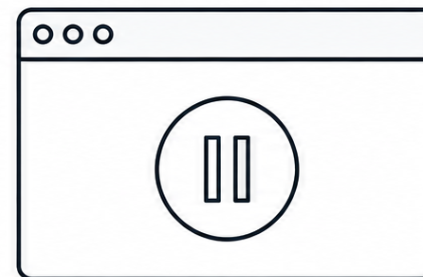
# 弱点を悪用されると、何が起こるのか

条件がそろえば、攻撃者はログインせずに不正な操作を行えるようになります。

情報が盗まれる

内容を書き換えられる

サービスが止まる



起こり得る被害の例です。影響は、PHPのバージョンや設定によって異なります。

# 被害を防ぐため、サービスを一時停止した企業も

一部の企業はサービスを止め、修正と安全性の確認を進めました。

**一時停止**

攻撃を受けるリスクを減らす



**修正と確認**

弱点を直し、安全性を確認する



**再開**

安全を確認して順次再開する

## A社

修正後、10月22日に順次再開しました。  
一部の機能は、同日も停止中でした。

## B社

被害を防ぐために一部サービスを止め、  
PHPの更新後に再開しました。

両社は10月22日、不正アクセスや情報漏えいは確認していないと発表しました。

# 制作や運営を外部に任せていても、確認は必要

自社で開発していなくても、利用中のサービスでPHPが使われていることがあります。

利用しているもの

最初の確認先

自社のホームページ



制作会社・保守会社

---

予約サイト・ネットショップ



運営会社・システム担当者

---

外部の業務サービス



提供会社のサポート窓口

---

自社で管理している場合は、社内の担当者に相談してください。確認先は契約や役割分担によります。

# 管理会社に確認する3つのこと

制作・保守会社やサービス提供元に、次の3点を確認しましょう。

**1** 当社のサイトやサービスは対象ですか。

**2** 修正は完了していますか。

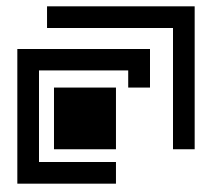
**3** 不正アクセスの形跡はありますか。  
当社で必要な対応も教えてください。



制作・保守会社  
サービス提供元

修正が済んでいても、それ以前に不正な操作がなかったかを確認する必要があります。

# Atlas Supportの診断・改善支援



AIを活用した診断をもとに、改善案の策定から修正・再検証まで支援します。

## 診断

サイトやシステムの  
弱点を洗い出す



## 改善案の策定

事業への影響を踏まえ、  
対策の優先順位を決める



## 改善・再検証

修正を支援し、  
弱点の解消を確認する

## まずは、初回無料のご相談を。

ご利用中のサイトやサービス、  
気になる点をお聞かせください。

**初回無料相談を希望する**

支援内容を見る



[atlassupportai.com/ja/contact](https://atlassupportai.com/ja/contact)