



■ PHP の脆弱性について

週末から現在（2026/10/27）まで、新しく発見された **2 つの PHP の脆弱性（PHP2shell）** によって多くのサイトが閉鎖しています。

常態化してしまった「情報漏洩」 が世間を騒がせている中、政治家が SNS でコメントしたこともあって大変大きな社会問題になっています。



図：IPA による PHP2shell の解説ページ

<https://www.ipa.go.jp/security/security-alert/2026/alert20261022.html>

2 つの脆弱性を簡単な図で説明したものが以下です。

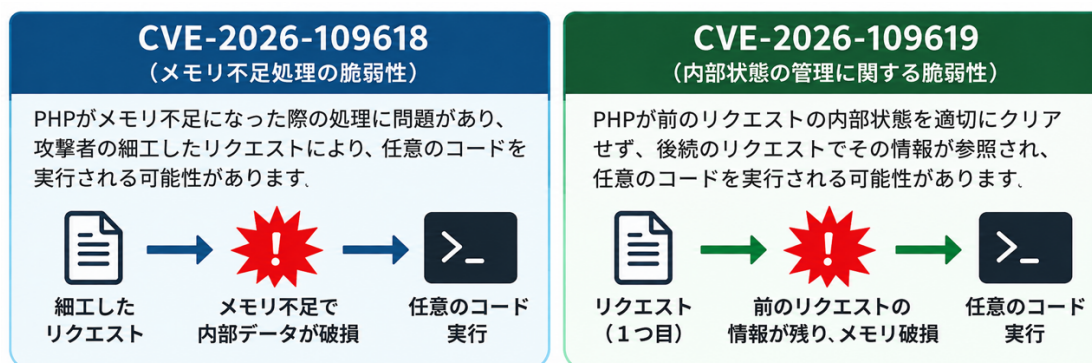
根本的にあるのは

PHP が内部で管理しているメモリの状態と、実際のメモリの状態に不整合が生じ、PHP がメモリ操作の安全性を保証できなくなる

という問題です。

C 言語を扱った経験がある方であれば、メモリーを「利用して解放する」という処理を書いたことがあるかと思います（PHP も C 言語で書かれています）。

PHP を言語としてみると、メモリー管理に気を使う必要はなく、それは PHP の実行部分（エンジンなど）が行います。これらは、利用しているメモリーを完全に管理下に置かなくてはならないのですが、**管理できない状態が存在して、それを悪用される可能性がある**、ということです。



図：CVE-2026-109618、CVE-2026-109619（イーレンジャー、ChatGPT）

このような脆弱性は特別なものではないのですが、**AI が攻撃**に関わるようになってきていること（情報漏洩の大半）を踏まえると、「**どんなことをされるかわからない**」というのが本音ですし、このような事例は増えると思います。