# HTMLエスケープとXSS

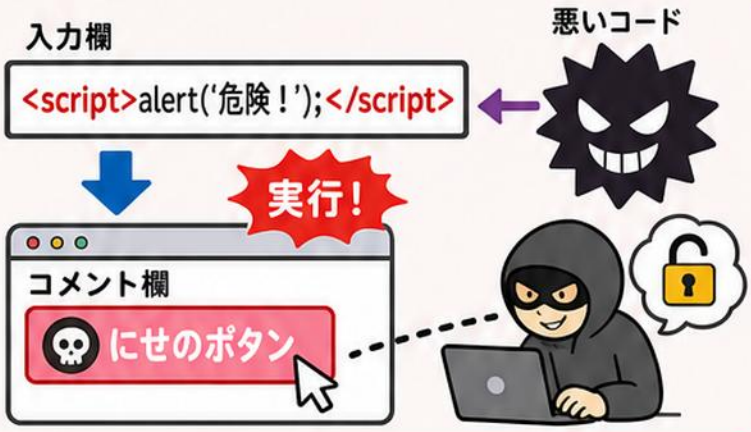
## ✦ Webを安全に保つ工夫 ✦

入力をそのまま表示すると、悪いプログラムが動くことがある（XSS）。
特殊文字を変換して防ぐ。

## 1 XSSってなに？

危険な攻撃のひとつ。

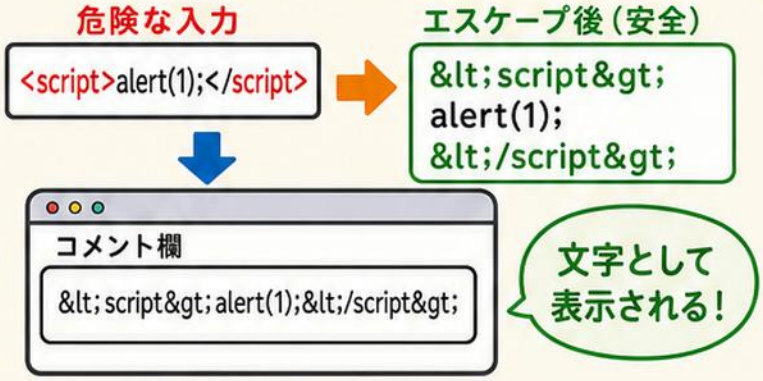
- 入力がHTMLとして実行される
- にせのボタンや盗み見
- コメント欄などが狙われる




## 2 HTMLエスケープ

特殊文字を変換。

- 山かっこ・引用符などを変換
- 文字として表示され実行されない
- 例：< を < にする




## 3 何を守る？

守りたいもの。

- 利用者の情報
- なりすまし防止
- サイトの信頼

## 4 対策

あわせて行う。

- 表示するときにエスケープ
- フレームワークの自動機能
- CSPなども併用


## ★ 特殊文字を変換して悪用を防ぐ