松浦研究室

[オブジェクト指向のWebアプリケーションに対するXSS攻撃脆弱性の静的解析]

生産技術研究所　情報・エレクトロニクス部門
Department of Informatics and Electronics
http://kmlab.iis.u-tokyo.ac.jp

情報理工学系研究科
電子情報学専攻

情報セキュリティ

クロスサイトスクリプティング（XSS）攻撃

Cross Site Scripting (XSS) Attack

クロスサイトスクリプティング（XSS）攻撃とは、主にWebアプリケーションでユーザーからの入力に対してサーバーサイド側での入力処理が不適切であることを利用して、攻撃者が悪意のあるスクリプティングを注入する攻撃である。

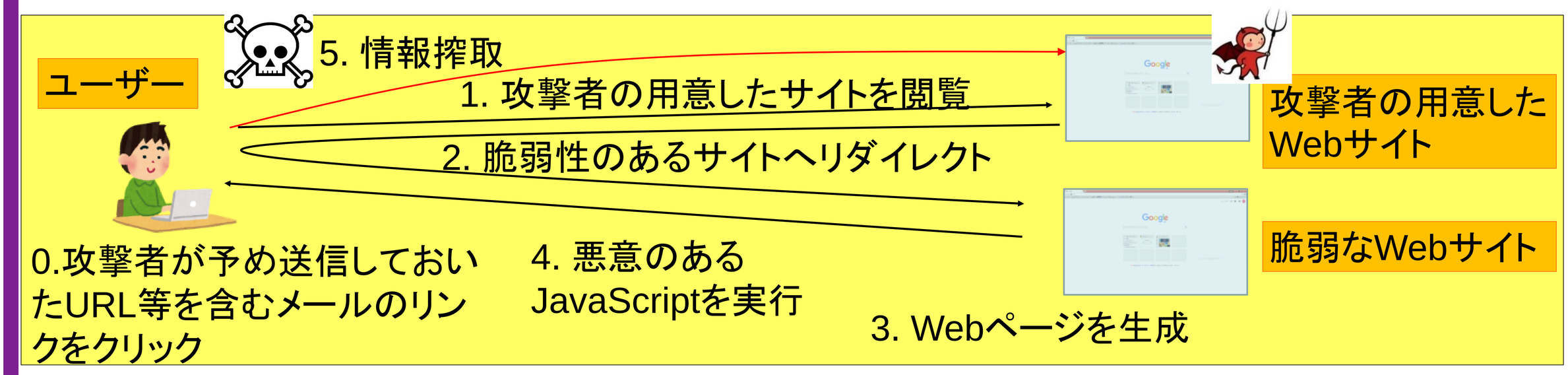


図１：　反射型XSS攻撃。

オブジェクト指向スクリプト言語のアプリケーション

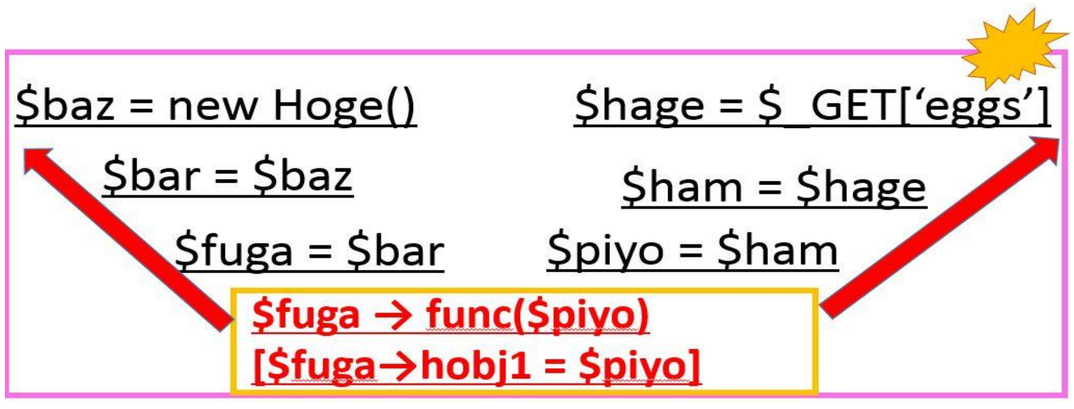
Application implemented with object oriented Script Language

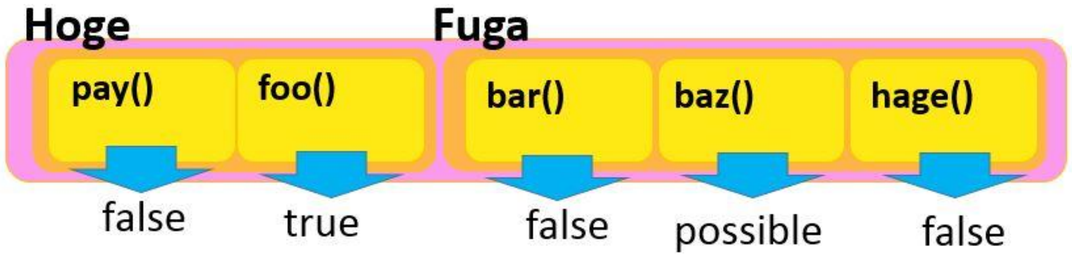
◇オブジェクト指向の静的解析について、JavaやC++といったプログラミング言語では型情報を基に静的解析するといった研究があるが、型情報を持たないスクリト言語において、このような手法は適用できない。

検知のアプローチ

How to detect

◆本研究では、オブジェクト指向で実装されたスクリプト言語のWebアプリケーションの脆弱性検知を反射型XSSと蓄積型XSSを対象。
◆アプローチとして、2方向後方脆弱性分析とクラスキャッシュの概念を導入。





◆予めクラスキャッシュで脆弱性情報を保持しておき、2方向後方脆弱性分析をすることでXSS攻撃の検知率を大幅に上げたことを確認。