# DOM-Based XSS対策の実装

## Implementation of a countermeasure against DOM-Based XSS attacks

折戸洋介・システム分科会・情報セキュリティ大学院大学

Abstract：According Information-technology Promotion Agency and JPCERT/CC, XSS vulnerability accounts for half of web application vulnerability. Further, half of them are not fixed within one month. To do XSS vulnerabilities countermeasure, it is necessary to modify the web application. However, it takes the time to fix. I propose a method to fix the DOM-Based XSS vulnerability that is included in the HTTP response in the web server software. And I was the implement it. This is by applying to the web server software.

**背景**

ウェブアプリケーション脆弱性の半数がXSS
脆弱性発見後，半数は30日以内に修正されない

**問題**

ウェブアプリケーションの修正に時間が掛かる
脆弱性を放置はできないが稼働は止めたくない

ウェブアプリケーションのコードを直接修正せずに脆弱性を防ぎたい

## ウェブサーバソフトウェアのモジュールでウェブアプリケーションのレスポンスに含まれるJavaScriptを書き換えることで、脆弱性を防止

1. ウェブアプリケーションが通常のレスポンスを生成
2. ウェブサーバソフトウェアは、1.に含まれるJavaScriptのコードを書き換えてクライアントに返す
3. クライアントで書き換えられたコードが実行される

DOM操作の関数が呼ばれる直前に
エスケープ処理が行われるよう
標準組込関数を置き換えるコードを挿入

```
(function(){
        var orig = Object.getOwnPropertyDescriptor(Node.prototype,"textContent");
        Object.defineProperty(
                HTMLScriptElement.prototype, "textContent", {
                        set: function() {
                                var text = arguments[0];
                                return orig.set.call(this,sanitize(text));
                        },
                        get: function() {
                                return orig.get.call(this);
                        }
                }
        );
})();
```

HtmlScriptElement.textContentへの実装例

### レスポンス処理遅延