社内ウェブサイトの脆弱性を悪用したXSSを防止するシステムの構築

川内　英主†　千葉　雄司‡　土居　範久†
中央大学　理工学部　情報工学科†
中央大学大学院　理工学研究科‡

1 はじめに

スクリプティング(Scripting)と呼ばれる攻撃のひとつにXSS(Cross-Site Scripting)がある[1]．スクリプティングとは，悪意のあるスクリプトを含むコンテンツを被害者に参照させ，スクリプトを実行させる攻撃だが，その中でもXSSでは，悪意のあるスクリプトを含むコンテンツを作成する手段として，第三者が公開している動的コンテンツを利用する．このため，動的コンテンツを公開しているユーザは，動的コンテンツ[1]をXSSに悪用されないよう対策をとる必要がある．

現在，社外へ公開するウェブサイトでのXSS脆弱性対策をとる企業が増えてきているが[2]，XSS脆弱性対策は社内だけに公開するウェブサイト(社内ウェブサイトと略す)にも適用する必要がある．社内ウェブサイトは社外から参照できないが，それでも，2章で詳述するように，社内ウェブサイトの脆弱性を悪用して社外からXSSを仕掛けることは可能であり，対策が必要になる．

社内ウェブサイト向けの脆弱性対策では，社外向けと同様に，ウェブコンテンツを1つ1つ人手で修正することもできるが[3]，それでは修正漏れの恐れがある．そこで本論文では，修正漏れのおきない対策を提案する．本論文の構成は次に示すとおりである．まず，2章で対策する攻撃を明らかにし，3章で対策手法を示す．4章では対策に伴って生じるオーバヘッドの大きさを評価した結果を示す．5章は結論である．

2 社内ウェブサイトの脆弱性を悪用したXSS

社内ウェブサイトは，社外のユーザからは参照できないので，社外のユーザは社内ウェブサイトの脆弱性を悪用したXSSの被害にあうことはない．しかしながら社内のユーザは，社内外のウェブサイトを参照できる状況にあると社外からのXSS攻撃にあうことがある．社内ウェブサイトの脆弱性を悪用して社外からXSS攻撃を仕掛ける手順を次に示す(図1参照)．

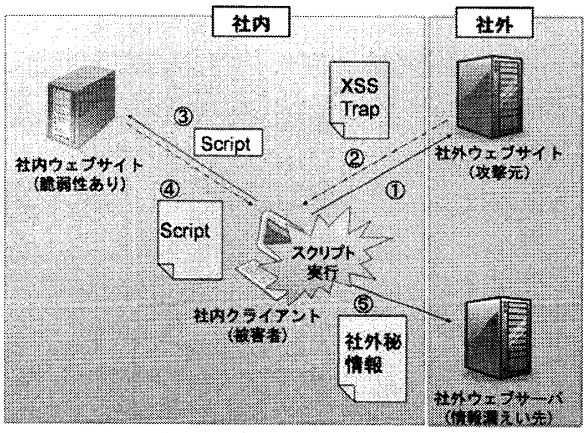

図1　社外からのXSS

① 社内にいるクライアント(社内クライアントと略す)が，社外にあるウェブサイト(社外ウェブサイトと略す)へ，リクエストを送る．
② 社外ウェブサイトは社内クライアントへ悪意のある参照を含むコンテンツを送る．
③ 社内クライアントが悪意のある参照をたどると，脆弱な社内ウェブサイトは，悪意のある参照から，悪意のあるスクリプト入りのページを作成してしまう．
④ このページを社内クライアントに送り返すと，社内クライアントがページ内のスクリプトを実行してしまう．
⑤ スクリプトの内容によっては，社外秘情報の漏えいといった被害にあう．

この攻撃にあたって，攻撃元のウェブサイトは必ずしも社外にある必要はない．しかしながら社外にあると，社内システムの管理者がコンテンツを制御できない点で対策し難い．そこで本論文では攻撃元が社外にある場合向けの対策を提案する．

3 提案するシステム

本研究で提案する対策は，プロキシサーバを用いて，社外のウェブサイトから送られてきたコンテンツを走査し，その中に社内ウェブサイトへの参照があるか否かを調べ，参照があったらそのコンテンツを遮断するというものである．社内ウェブサイトは，社内だけに公開するものなので，社

Preventing XSS attacks to intranet web sites
Hideyuki KAWAUCHI†, Yuji CHIBA‡, Norihisa DOI†
†Department of Information and System Engineering, Faculty of Science and Engineering, Chuo University
‡Graduate School of Science and Engineering, Chuo University

[1] CGI(Common Gateway Interface)などで動的に作られるウェブページ

外ウェブサイトのコンテンツが社内ウェブサイトへの参照を含んでいることは不自然である．そこで，社外から送られてきたコンテンツが社内ウェブサイトへの参照を含んでいたら，XSS と判断し，攻撃を防ぐためにコンテンツを遮断する．

4 性能評価

提案技法では，プロキシサーバでコンテンツの検査をおこなうが，検査に伴う性能劣化があまりに著しいと，実用に耐えなくなってしまう．そこで我々は，提案技法の実用性を評価するために，提案技法を導入する前後のプロキシサーバの性能(スループット)を測定，比較した．

4.1 評価方法

評価環境を図 2に示す．

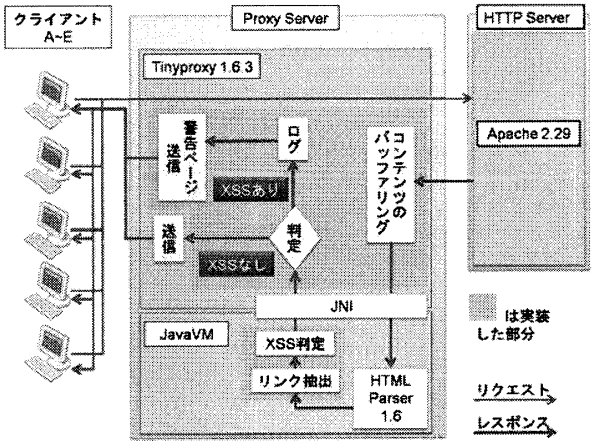

図 2　評価環境

性能評価にあたっては，5 台のクライアントからプロキシサーバを中継して HTTP サーバにリクエストを送り，プロキシサーバにおいて 10000 回の中継処理にかかった時間とリクエスト先のウェブページのサイズからスループットを算出した．HTTP サーバに配置するウェブページは実際にインターネット上に公開されているものを用いた．なお，本研究で利用したプロキシ(TinyProxy-1.6.3[4])はコンテンツをキャッシュしないので，リクエストごとにコンテンツの走査をおこなう．キャッシュをおこなう場合に生じる性能劣化は本論文に示す評価結果よりも小さくなる．

なお，走査にあたっては，コンテンツからのリンクの抽出に HTML Parser 1.6[5]を用いた．評価に使った計算機の詳細は次に示す通りである．

- Proxy Server(OS Fedora 7,CPU Pentium4 2.8GHz, Memory 512MB,JDK JDK-1.5.0_16)
- HTTP Server(OS CentOS 4.7,CPU Celeron 2.4GHz,Memory 768MB)
- Client A～E (OS WindowsXP Professional SP2)
  - A (CPU Pentium4 2.8GHz,Memory 2GB)
  - B (CPU Pentium4 3.0GHz,Memory 1GB)
  - C (CPU Pentium4 2.8GHz,Memory 1GB)
  - D (CPU Pentium4 2.8GHz, Memory 512MB)
  - E (CPU Xeon 2.13GHz,Memory 1GB)

4.2 評価結果

10KB から 50KB までのウェブページを用いて，ページサイズごとに性能劣化率を評価した．評価結果を図 3に示す．

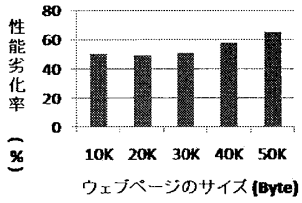

図 3　プロキシサーバの性能劣化率

図 3から，提案するシステムを導入することによるプロキシサーバの性能劣化率は，ページサイズに比例して大きくなる傾向にあり，50KB のウェブページでは 60%ほどになることがわかった．

5 まとめ

本研究では，社内ウェブサイトの脆弱性を悪用した社外からの XSS を防止する手法を提案し，その利用にともなう実行時オーバヘッドを評価した．

今後の課題としては，Squid などのキャッシュを利用するプロキシ上に実装することで，より現実的な評価をおこなうことがあげられる．

参考文献

[1] CRET Coordination Center, Malicious HTML Tags Embedded in Client Web Requests, http://www.cert.org/advisories/CA-2000-02.html, 2000.2

[2] 独立行政法人情報処理推進機構, ソフトウェア等の脆弱性関連情報に関する届出状況[2008 年第 3 四半期(7～9 月)] http://www.ipa.go.jp/security/vuln/report/vuln2008q3.html

[3] 独立行政法人情報処理推進機構, セキュア・プログラミング講座 (新版), https://www.ipa.go.jp/security/awareness/vendor/programmingv2/web.html

[4] BANU, tinyproxy, https://www.banu.com/tinyproxy/

[5] SourceForge, HtmlParser, http://htmlparser.sourceforge.net/