ローカルプロキシを用いたCSRF攻撃検出手法の検討

Researches on CSRF Attacks Detection Method Using Local Proxy

染川 敦[1] 鈴木 秀和[1] 旭 健作[1] 渡邊 晃[1]
Atsushi Somekawa Hidekazu Suzuki Kensaku Asahi Akira Watanabe

名城大学大学院理工学研究科[1]
Graduate School of Science and Technology, Meijo University

1 はじめに

クロスサイトリクエストフォージェリ (Cross Site Request Forgeries，以下 CSRF) 攻撃とは，ユーザが攻撃者の用意した Web サイトにアクセスすると，別の脆弱性のある Web サイトに対してユーザの意図しないリクエスト (例えば掲示板への書き込み) が送信される攻撃である．本稿では，ローカルプロキシを用いたユーザ側での CSRF 攻撃検出手法の検討を行った．

2 CSRF 攻撃の概要

図 1 に CSRF 攻撃の概要を示す．ユーザが攻撃者の用意した Web サイトに HTTP でアクセスし，その応答を受け取ると，端末内で悪意のあるスクリプトが実行され，ユーザの端末から脆弱性のある Web サイトへユーザの意図しない通信が行われる．

CSRF 攻撃は攻撃者が用意した Web サイトへのリンクをクリックすることで起こる攻撃であり，攻撃者の用意した Web サイトへのリンクと正常な Web サイトへのリンクの判別は難しい．ゆえに，一般的に CSRF 攻撃の対策はトークンを発行するなどの方法で，Web サーバ側で行われる．しかし，このような対策がとられていない Web サーバが存在することも考えられるため，CSRF 攻撃の対策をユーザ側で実施できると有用である．関連研究として，ブラウザにプラグインとして CSRF 攻撃の検出をする方法 [1] があるが，ブラウザごとにプラグインを開発しなければならない．

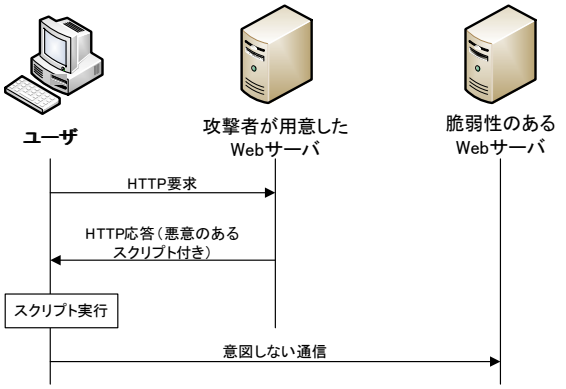


図 1 CSRF 攻撃の概要

3 提案方式

本稿では，ブラウザと Web サーバ間の通信を自端末内に置かれるローカルプロキシで監視することにより，ユーザ側で CSRF 攻撃を検出する手法を提案する．図 2 に提案方式の概要を示す．ブラウザは攻撃者が用意した Web サイトにアクセスするための HTTP の要求をローカルプロキシへ送信する．ローカルプロキシは攻撃者が用意した Web サイトへ HTTP の要求を送信する．そして，攻撃者が用意した Web サイトからローカルプロキシへ悪意のあるスクリプトが付いた HTTP の応答が送信される．

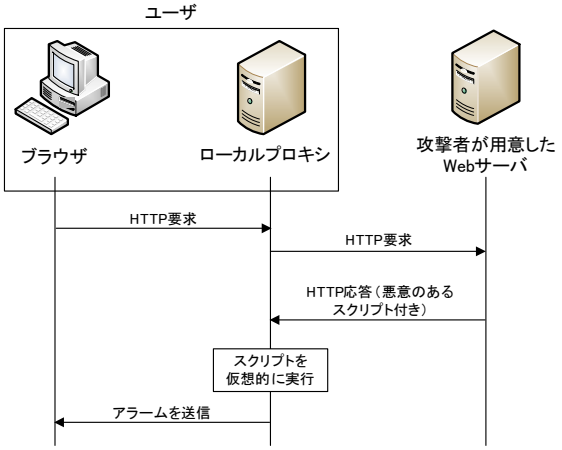


図 2 提案方式の概要

本提案ではブラウザと Web サーバ間の通信をローカルプロキシで監視し，HTTP 応答に含まれるスクリプトを仮想的に実行し，通信している Web サーバと異なるドメインの Web サーバへリクエストを送信するような処理が行われた場合，ブラウザに CSRF 攻撃が行われる可能性があるとして，ローカルプロキシからブラウザへアラームを送信する．

4 まとめ

ブラウザと Web サーバ間の通信をローカルプロキシで監視し，HTTP 応答に含まれるスクリプトを仮想的に実行することにより，ユーザ側で CSRF 攻撃を検出する手法を提案した．今後は，実装方法について検討する．さらに，本提案が XSS（Cross Site Scripting）などの他の Web サイトへの攻撃手法にも適応可能かどうかを検討する．

参考文献

[1] Shahriar, H. , Zulkernine, M. : 2010 IEEE 21st Internatioal Symposium on Software Reliability Engineering, 2010, 358-367

ローカルプロキシを用いたCSRF攻撃検出手法の検討

名城大学大学院　理工学研究科
染川 敦，鈴木 秀和，旭 健作，渡邊 晃

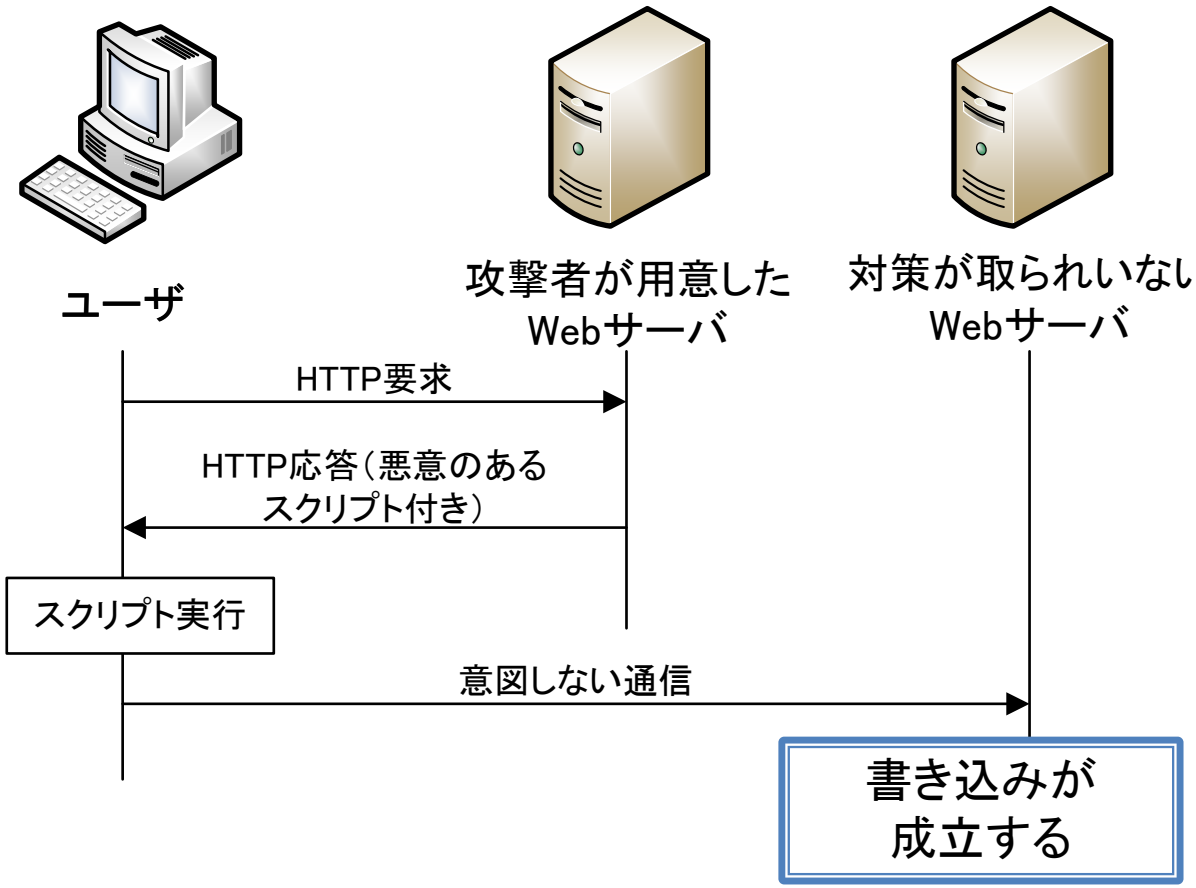
Watanabe Lab.

CSRFとは

- Cross Site Request Forgeries
- ユーザが攻撃者の用意したWebサイトに対して
  ユーザの意図しないリクエストが送信される攻撃
  - 例：掲示板への書き込み
- 2006年から継続的に脆弱性に関する届け出がある

CSRF攻撃の概要

1. ユーザ→攻撃者
   HTTP要求
2. 攻撃者→ユーザ
   HTTP応答
3. ユーザ
   悪意のあるスクリプトの実行
4. ユーザ→脆弱性のあるWebサーバ
   意図しない通信が開始

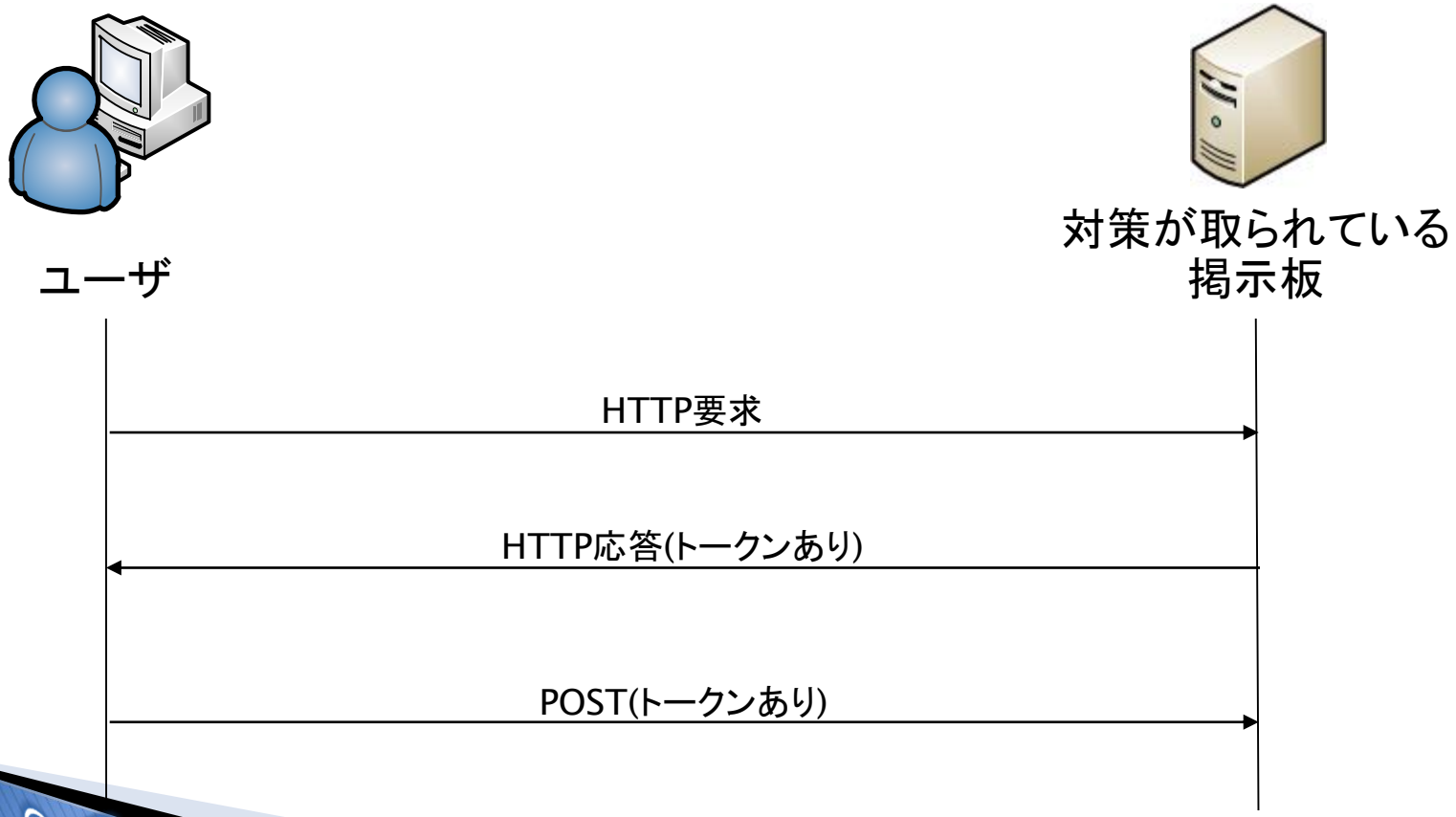


CSRFの特徴

- 攻撃者が用意したWebサイトへのリンクをクリックするだけで成立する攻撃
- リンク先のURLで攻撃を判別することは困難
- ユーザ側での対策が困難

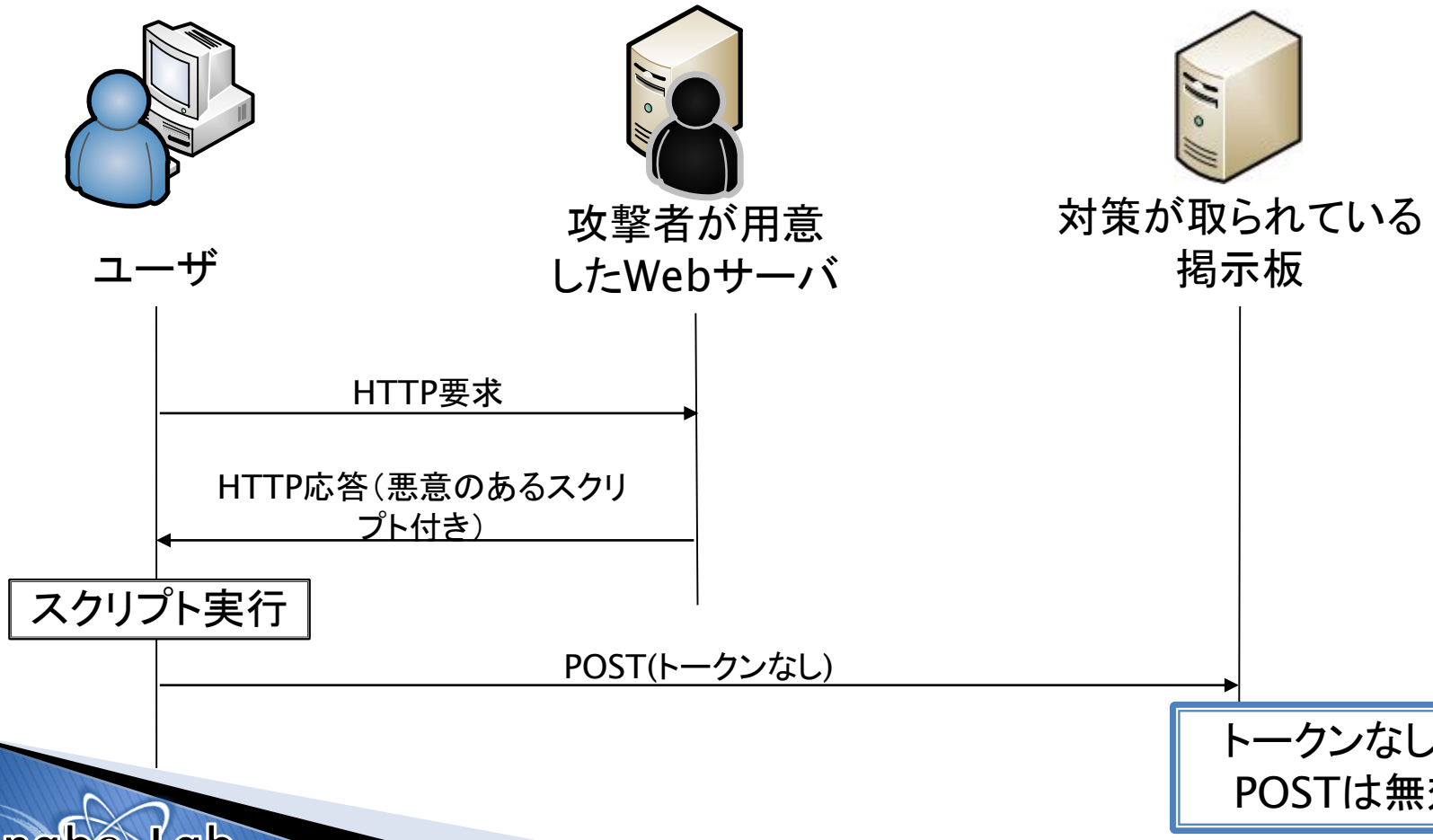
CSRF攻撃の対策

- Webサイトがトークンを発行



CSRF攻撃の対策

- トークンを発行している場合



研究目的

ユーザ側でCSRF攻撃を検出

- 本研究での検出対象は掲示板への書き込み
- ユーザが開いているブラウザはひとつのみ

先行技術

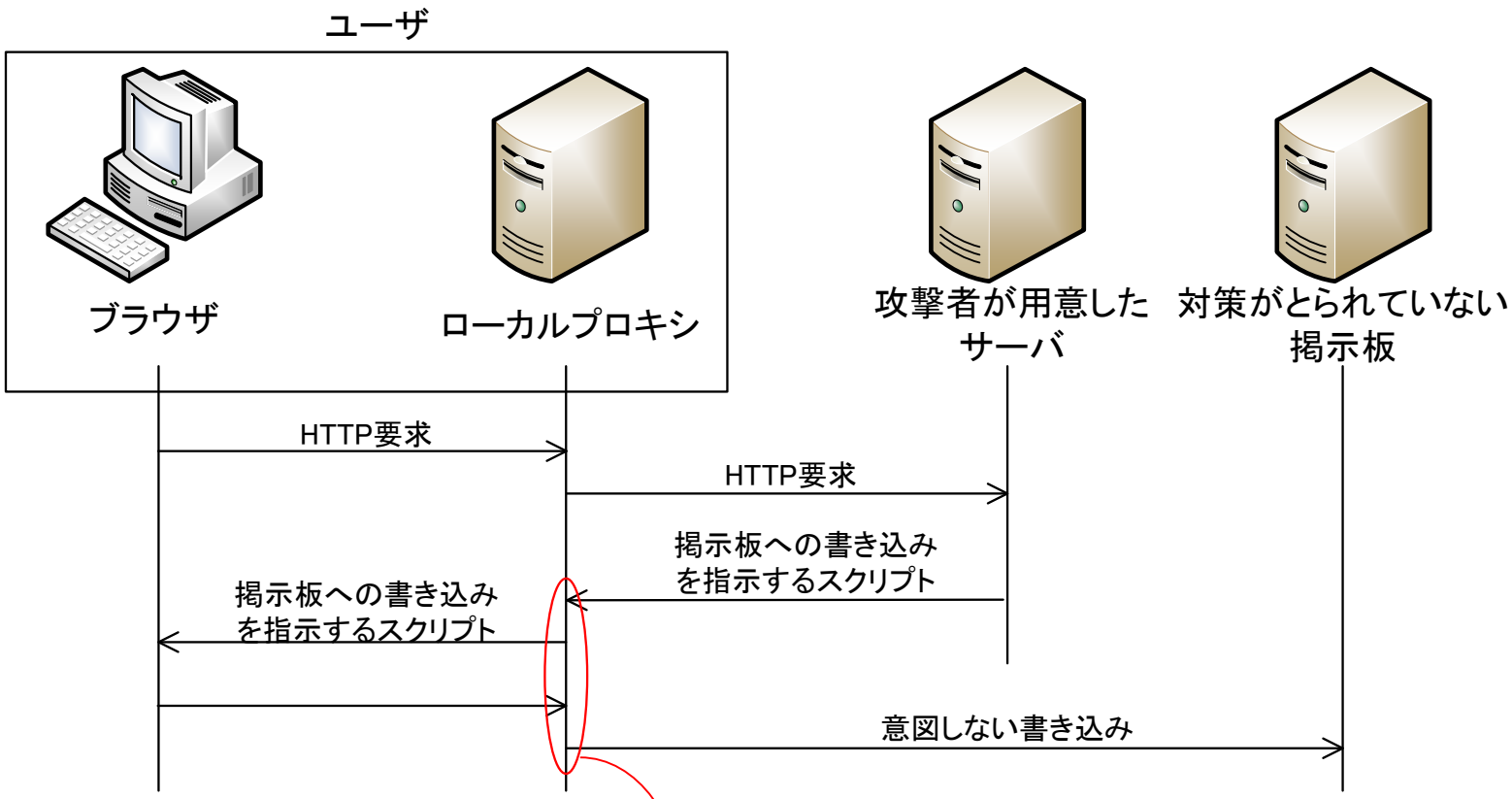
- ブラウザにCSRF攻撃を検出するためのプラグインでCSRF攻撃を検出する手法
  - 宛先ドメインのページ（書き込み先）が実際に開いているウィンドウにあるかどうか
  - フォームの有無の一致
  - ブラウザごとにプラグインを作成する必要がある

Shahriar, H. , Zulkernine, M. : 2010 IEEE 21st International Symposium on Software Reliability Engineering, 2010, 358-367

提案方式

- ユーザのコンピュータにローカルプロキシを設置し，ブラウザと攻撃者が用意したサーバとの通信を監視することでユーザ側でCSRF攻撃を検出する
  - ローカルプロキシ
    - 自身のコンピュータ内に設置するプロキシ
    - FQDN（Fully Qualified Domain Name）と，フォームが作成されるスクリプトを検出
- ブラウザごとに開発する必要がない．

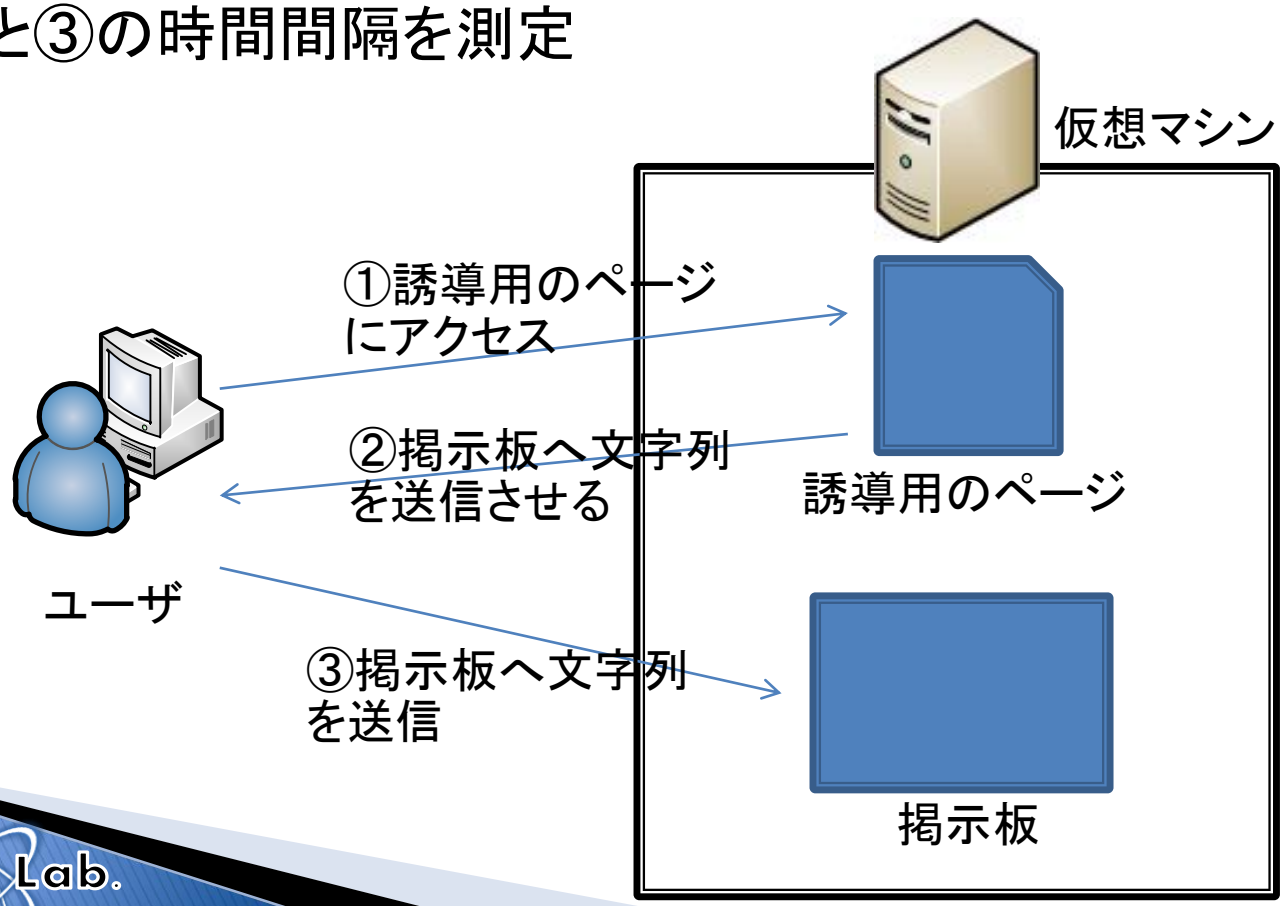
提案方式



FQDN
フォームの作成（formをsubmit）
時間間隔

実験

- 提案手法が有効かどうかローカルなネットワークでCSRF攻撃を行った
  - ②と③の時間間隔を測定



実験結果

時間間隔[s]				
0.015	0.016	0.015	0.016	0.017
0.015	0.015	0.016	0.017	0.015

- 受け取ったパケットと異なるFQDNへの書き込みが短い時間間隔で発生する.
- 実験では時間間隔が0.016[s]前後だが，実環境では結果よりも長くなることが考えれられる.

まとめ

- CSRFとはユーザが攻撃者が用意したWebサイトに対してユーザの意図しないリクエストが送信される攻撃
- ローカルプロキシを設置することでブラウザに依存することなくCSRFの検出が可能

- 今後の課題
  - ローカルプロキシへの実装
  - 誤検知実験
  - XSS(Cross Site Scripting)などの他の攻撃への応用