ローカルプロキシを用いたクライアント側での CSRF 攻撃検出手法の提案

染川　敦 *，旭　健作，渡邊　晃 (名城大学)

Proposal of CSRF Attack Detection Method Using Local Proxy in Client

Atsushi Somekawa, Kensaku Asahi, Akira Watanabe (Meijo University)

1　はじめに

Cross Site Request Forgeries(CSRF) 攻撃を受けた第三者が，Web サイトの掲示板に犯罪予告を投稿させられ，誤認逮捕されるなど問題となっている．この攻撃はクライアント側で対策をとることは難しいとされている．本稿では，クライアントにローカルプロキシを実装し，クライアント側で CSRF 攻撃を検出する手法の提案を行う．

2　CSRF 攻撃の概要

CSRF 攻撃とは，クライアントが攻撃者の用意した Web サイトにアクセスすると，その応答に含まれる悪意のあるスクリプトを実行させられ，別の脆弱性のある Web サイトに対してクライアント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．

一般に 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 サーバが存在するため，CSRF 攻撃の対策をクライアント側で実施できると有用である．関連研究として，ブラウザのプラグインで 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点に課題がある．

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，クライアント側で CSRF 攻撃を検出する手法を提案する．実際の掲示板への書き込みでは文字を入力するため，送信するために最低でも数秒の時間が必要である．しかし，スクリプトによる書き込みでは即座に書き込みが行われる．この原理を利用して提案方式では，異なるドメイン名のサーバに短い時間間隔で行われる POST メソッドによる通信を検出し，CSRF 攻撃を検出する．

Fig. 1 に提案方式のシーケンス図を示す．クライアントの PC にはローカルプロキシを実装する．攻撃者のサーバと CSRF 攻撃の脆弱性のある掲示板は外部ネットワークにある．攻撃者のサーバはアクセスしてきたクライアントに対して掲示板への書き込みを指示するスクリプトを送り，任意の文字列を掲示板に書き込ませる．攻撃者は事前に脆弱性のある掲示板を知っているものとする．

次に提案方式におけるローカルプロキシの動作を示す．

(1) ブラウザから攻撃者のサーバにアクセスするための HTTP 要求を受信したとき，その宛先のドメイン名を d1 として記録する．

(2) 攻撃者が用意した Web サイトへ HTTP 要求を送信し，攻撃者が用意した Web サイトから悪意のあるスクリプトが付いたレスポンスを受信し，受信した時刻を t1 として記録する．

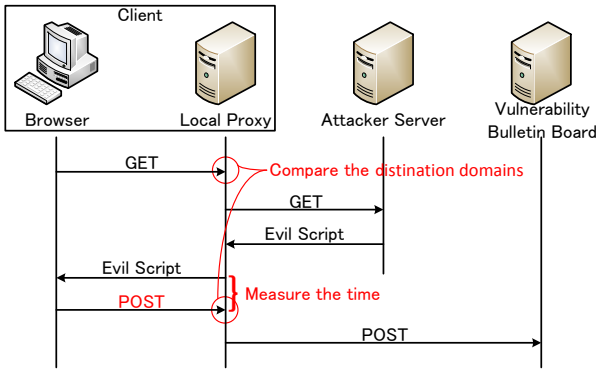


Fig. 1　Sequence of Proposal Method.

(3) スクリプトによってクライアントから POST メソッドでの通信が行われると，ローカルプロキシは宛先のドメイン名 d2，及び受信した時刻 t2 を記録する．

(4) 受信したパケットが POST メソッドで，d1 と d2 が異なり，かつ t2 - t1 が一定時間以下の場合，CSRF 攻撃と判定する．

4　誤検知実験

自身の PC にローカルプロキシを実装し，仮想マシン上に CSRF 攻撃を行う Web サーバと脆弱性のある掲示板を用意する．ローカルプロキシには本提案の CSRF 攻撃検出手法を実装する．また，CSRF 攻撃を行う Web サーバはアクセスがあると，脆弱性のある掲示板に書き込みを行わせるスクリプトを応答として返す．

PC のブラウザからローカルプロキシを介して CSRF 攻撃を行う Web サーバにアクセスし，CSRF 攻撃を発生させたところ，ローカルプロキシで CSRF 攻撃を検出できることを確認した．ローカルプロキシを介して一般の Web サイトや掲示板にアクセスしたが，誤検出は発生しなかったため，本提案は CSRF 攻撃の対策として有用であると判断できる．

5　まとめ

CSRF 攻撃は宛先ドメイン名が違うサーバに POST メソッドでの通信が短い時間間隔で行われる．これを利用して，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，クライアント側で CSRF 攻撃を検出することを提案した．今後は，ローカルプロキシを用いて XSS(Cross Site Scripting) などの他の攻撃手法にも適応可能かどうかを検討する．

文　献

[1] Shahriar.H, et al.: 2010 IEEE 21st Internatioal Symposium on Software Reliability Engineering 2010, pp.358–367, 2010.

ローカルプロキシを用いたクライアント側でのCSRF攻撃検出手法の提案

名城大学大学院 理工学研究科 情報工学専攻
染川　敦，旭　健作，渡邊　晃

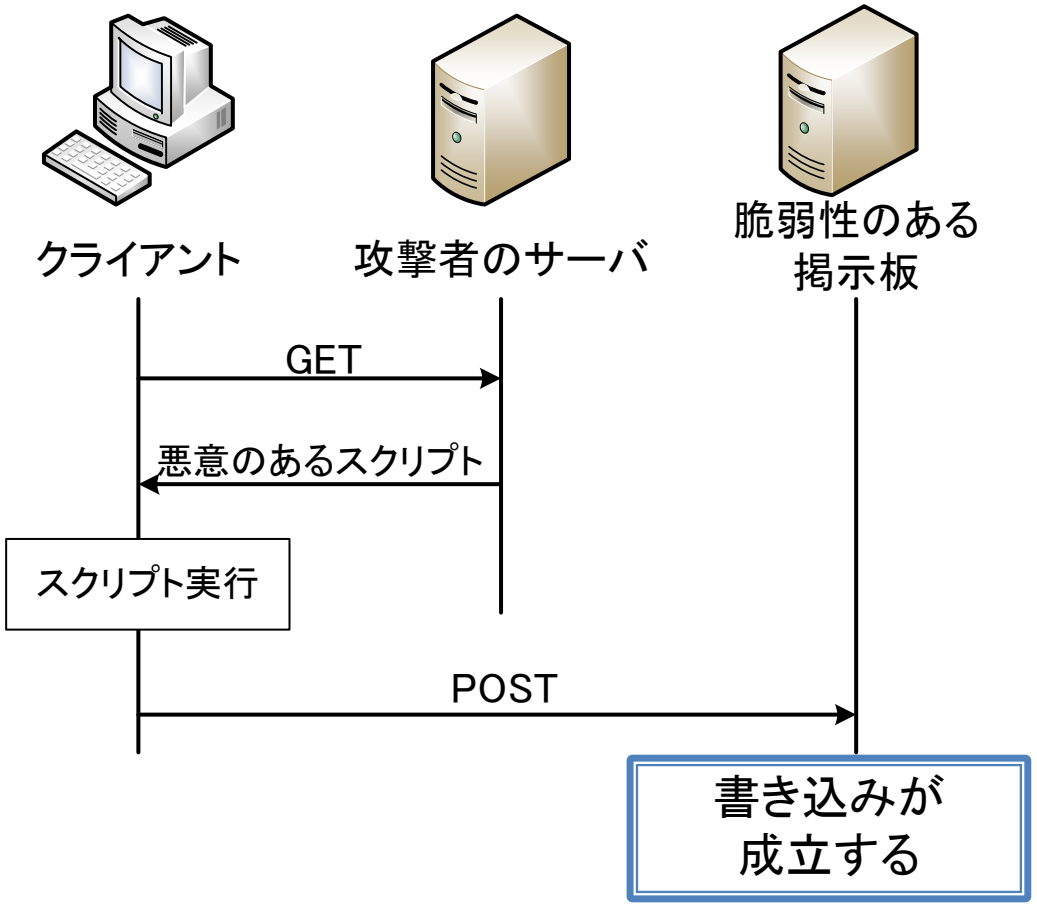
Watanabe Lab.

CSRFとは

- Cross Site Request Forgeries
- クライアントが攻撃者の用意したWebサイトに対してクライアント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. クライアント→攻撃者
   GETリクエスト
2. 攻撃者→クライアント
   GETレスポンス
3. クライアント
   悪意のあるスクリプトの実行
4. クライアント→脆弱性のある掲示板
   意図しない通信が開始

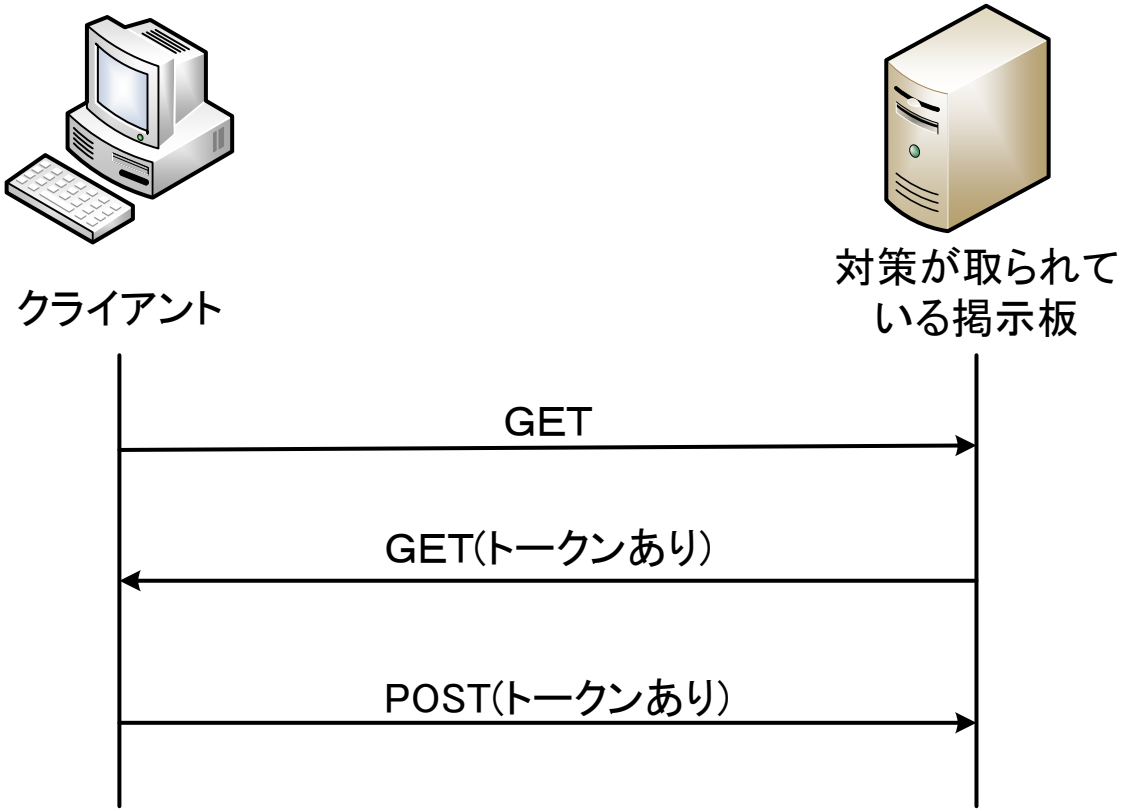


CSRFの特徴

- 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
- クライアント側での対策が困難

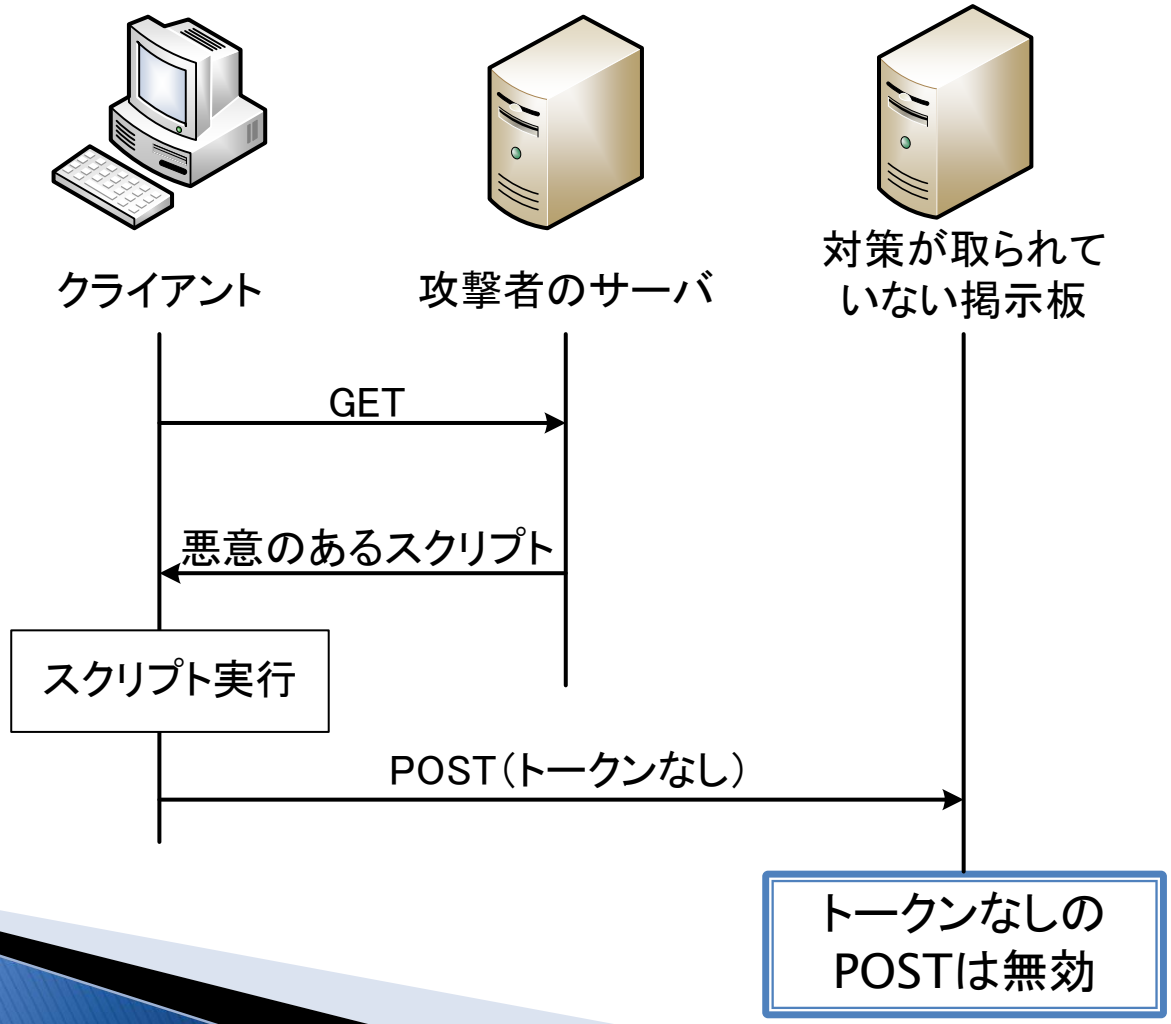
CSRF攻撃の対策

- 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

クライアント側で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

先行研究

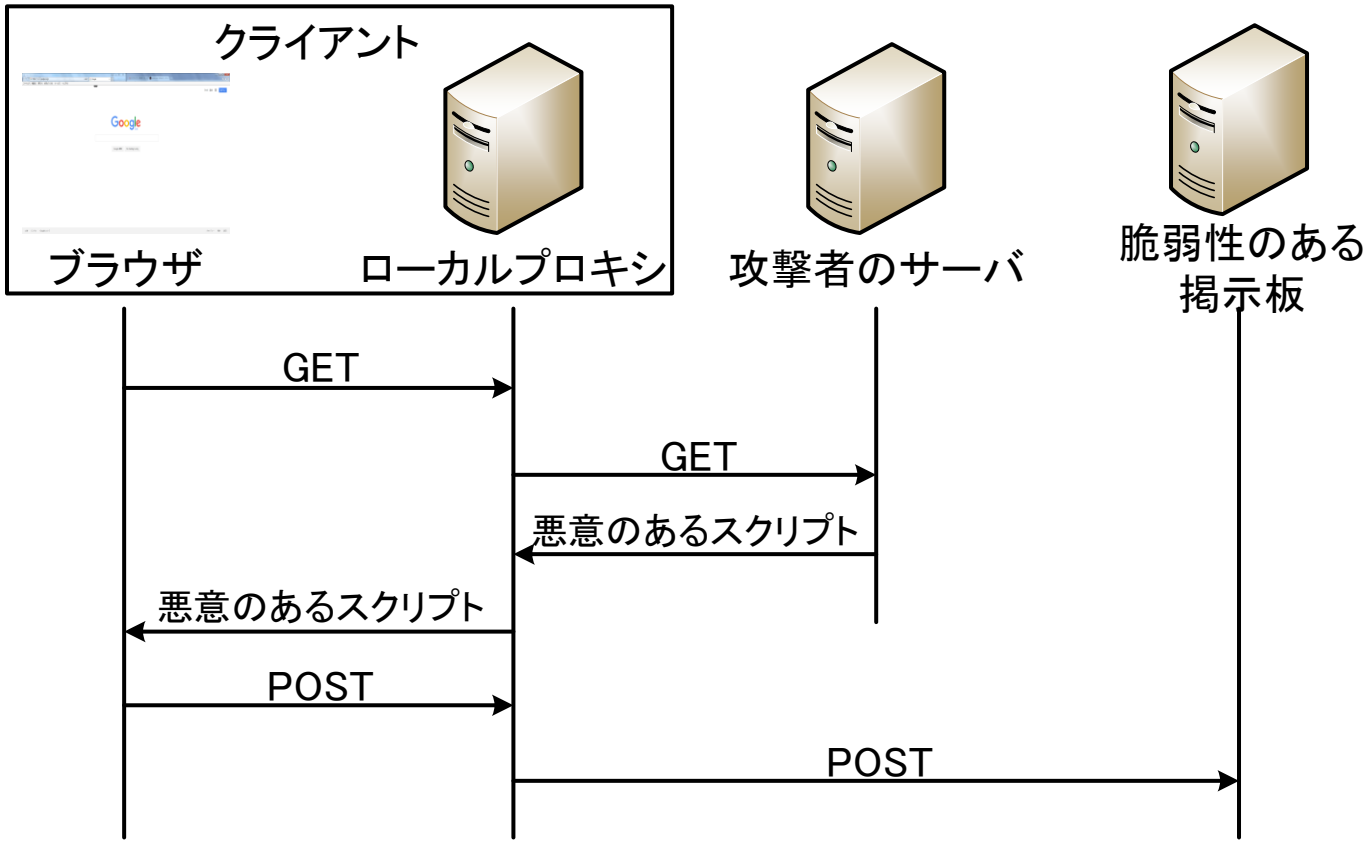
- ブラウザにCSRF攻撃を検出するためのプラグインでCSRF攻撃を検出する手法
  - 宛先ドメインのページ（書き込み先）が実際に開いているウィンドウにあるかどうか
  - URLにパラメータが存在しているかどうか
  - ブラウザごとにプラグインを作成する必要がある

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

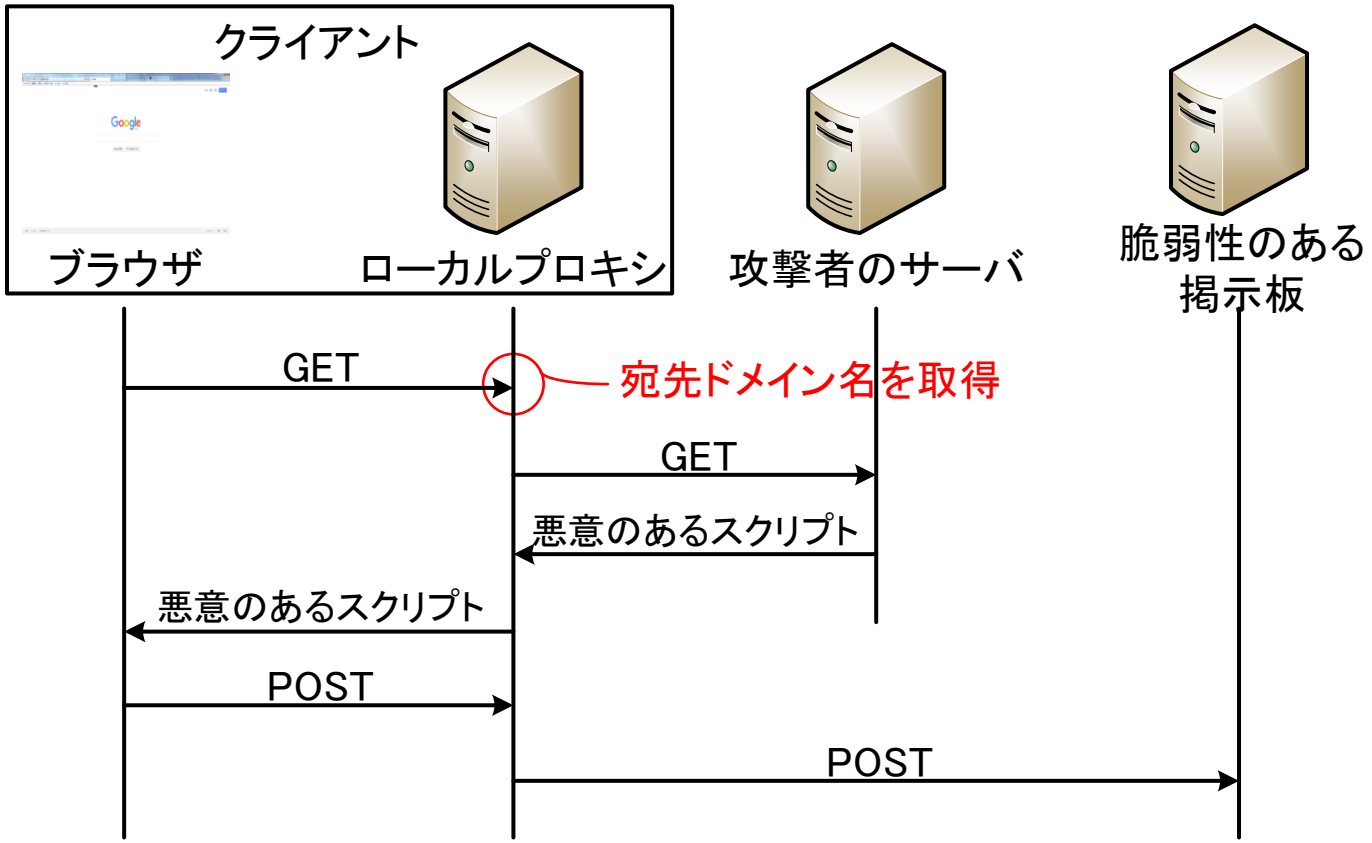
提案方式

- クライアント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クライアント側で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
- ブラウザごとに開発する必要がない.

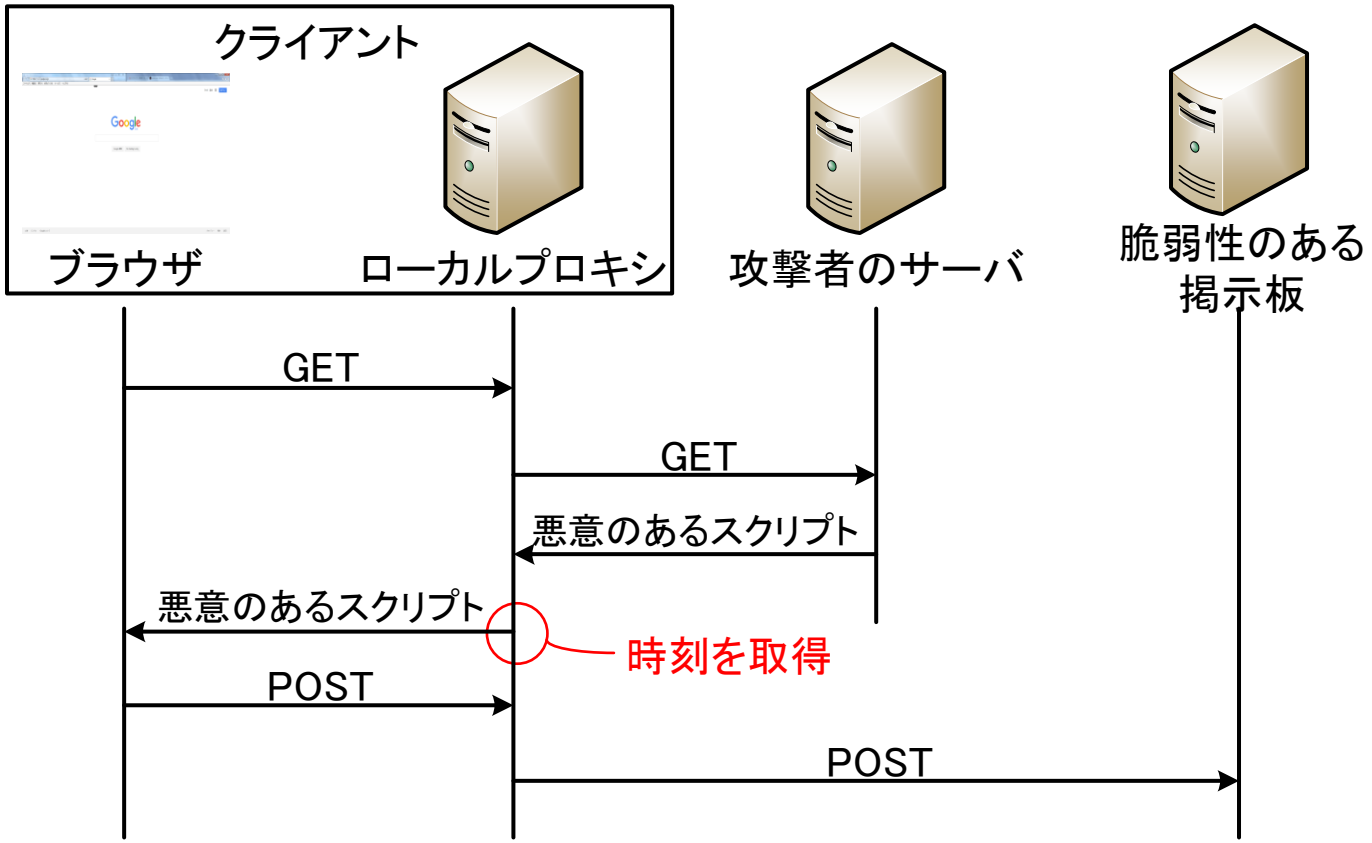
ローカルプロキシの動作



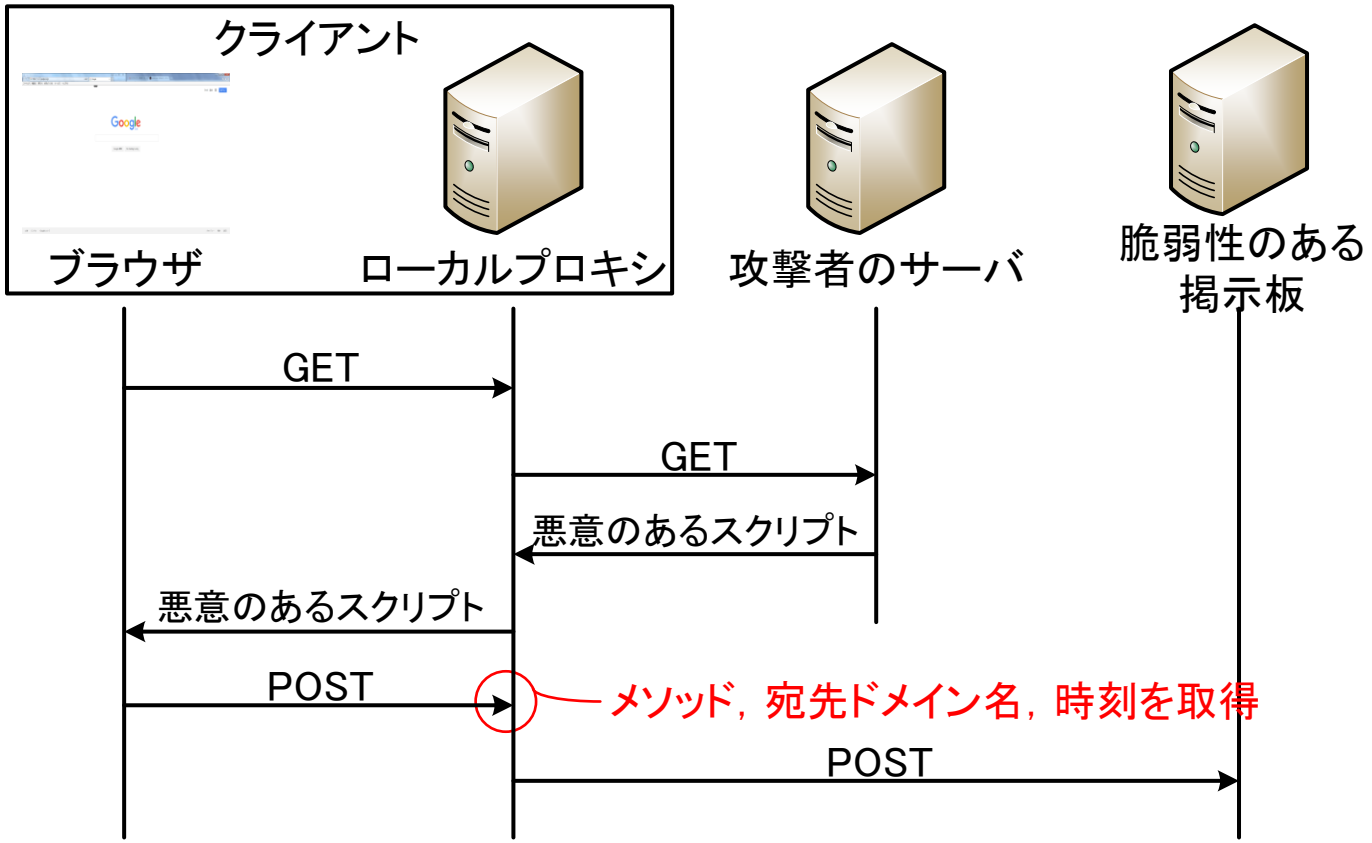
ローカルプロキシの動作①



ローカルプロキシの動作②

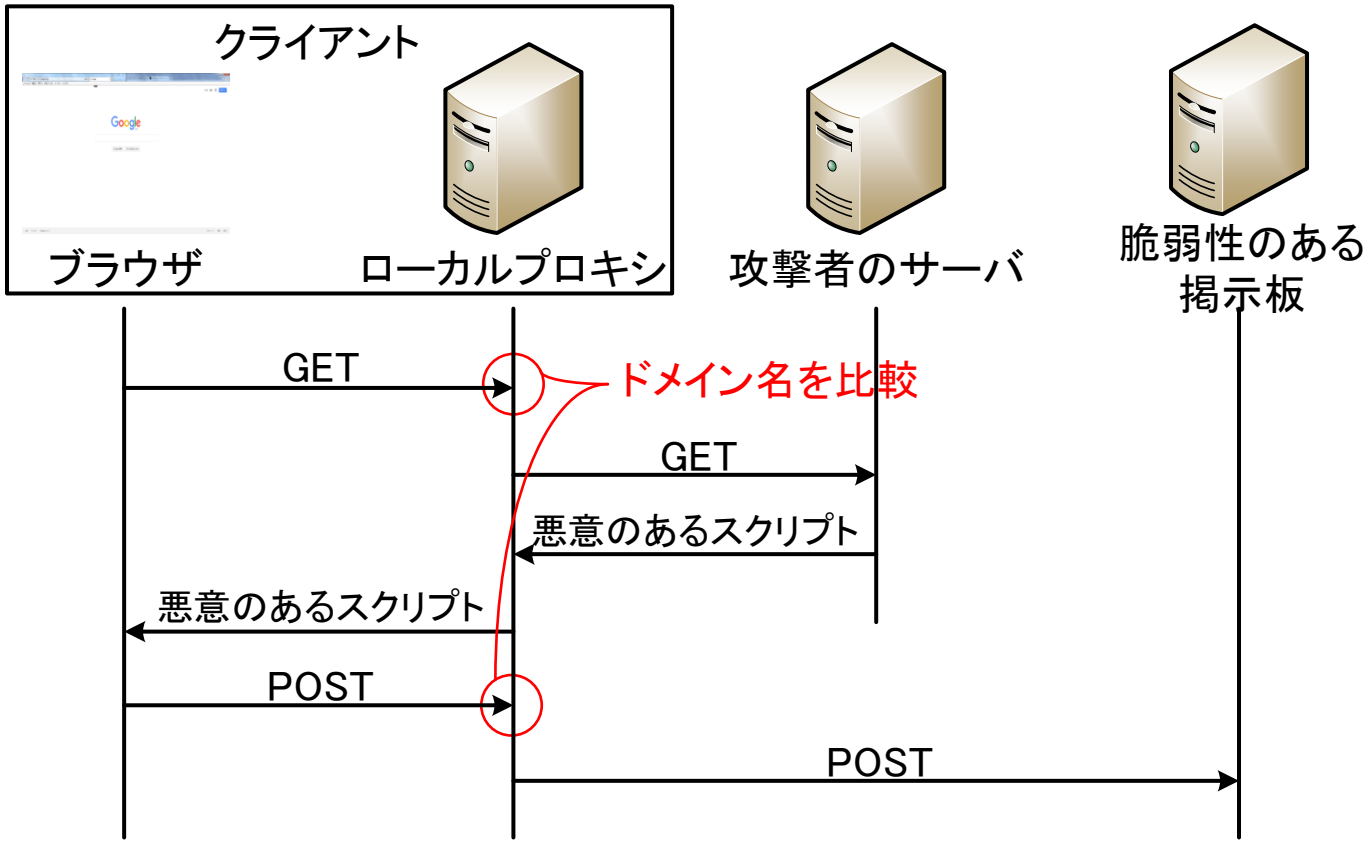


ローカルプロキシの動作③



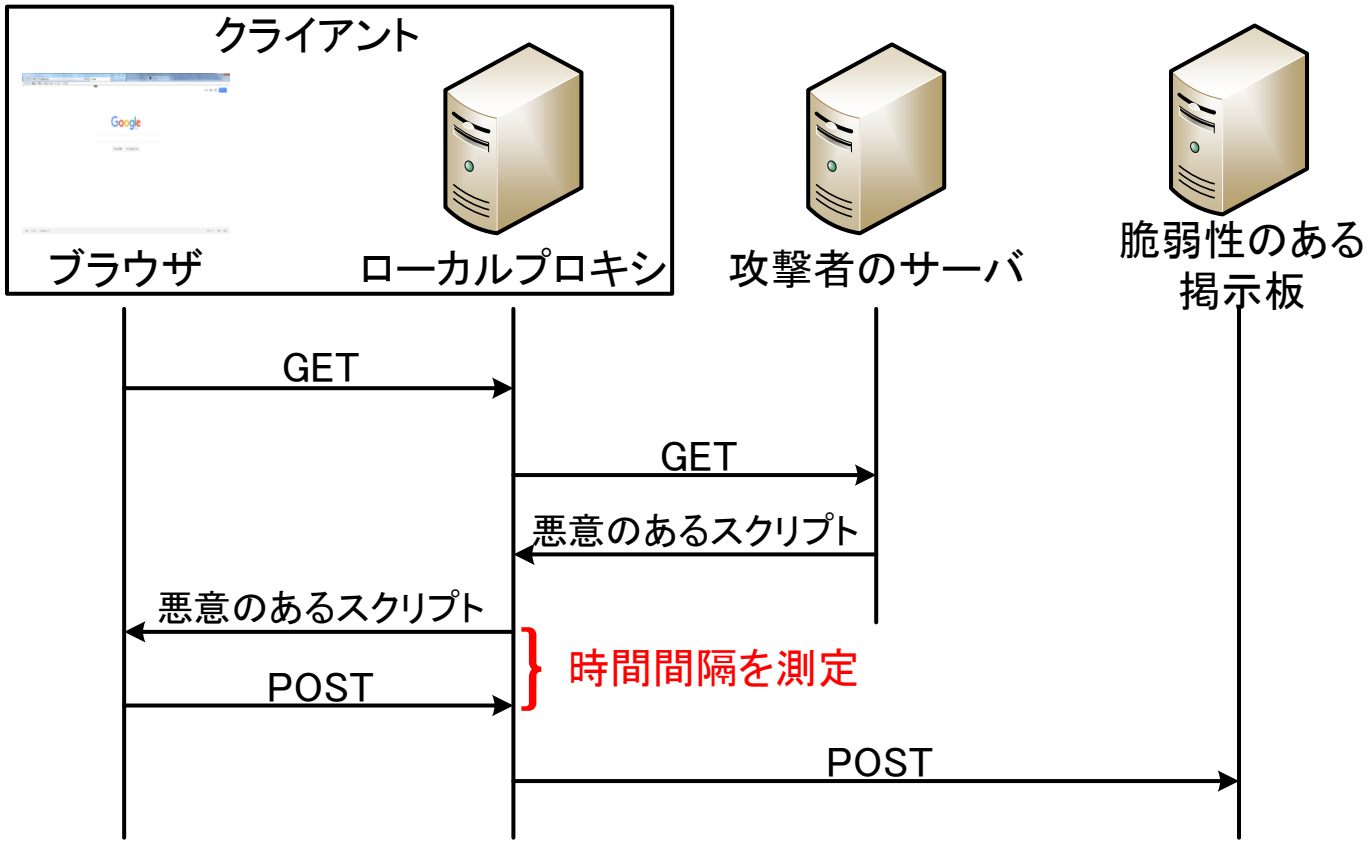
メソッドがPOSTならば次の処理へ

ローカルプロキシの動作④



ドメイン名が異なれば次の処理へ

ローカルプロキシの動作⑤



時間間隔が一定時間以内ならばCSRFと判定

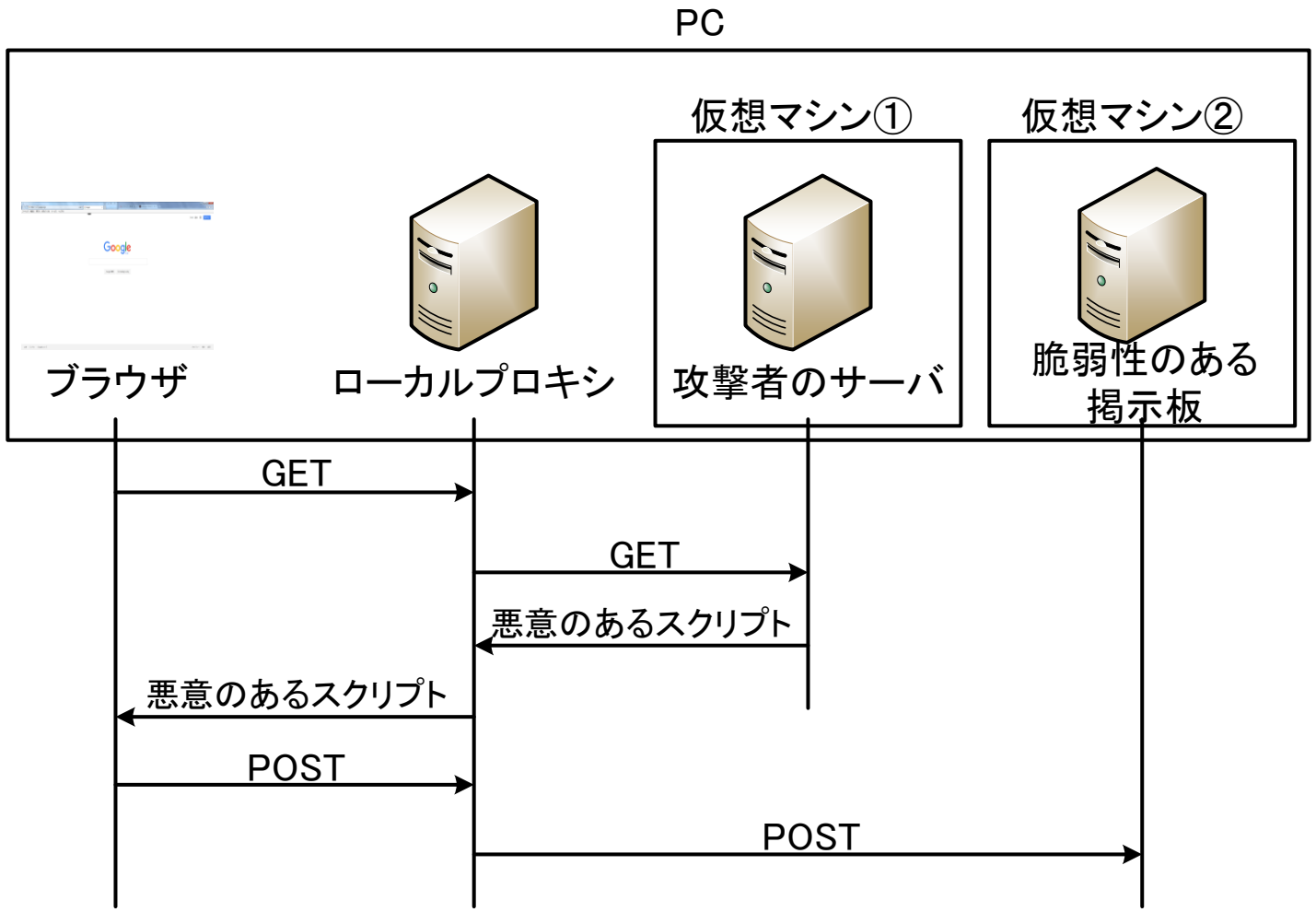
検出実験

- PCに提案方式が実装されたローカルプロキシを実装し，仮想マシン上にCSRF攻撃を行うWebサーバと脆弱性のある掲示板を用意する.

- 実際にCSRF攻撃を発生させ検出できるかどうかを確認する．また、その際に時間間隔を測定する.

- 一般のWebサイトや掲示板にアクセスした際の挙動を確認する.

実験環境


PC
仮想マシン①
仮想マシン②
ブラウザ
ローカルプロキシ
攻撃者のサーバ
脆弱性のある
掲示板
GET
GET
悪意のあるスクリプト
悪意のあるスクリプト
POST
POST

実験結果

- 本環境でCSRF攻撃を発生させたところローカルプロキシでCSRF攻撃を検出できることが確認できた.

- 時間間隔
  - 試行回数:10回
  - 13ms – 17ms

- 一般のWebサイトや掲示板にアクセスした際にCSRFと判定されることはなかった.

まとめ

- CSRFとはクライアントが攻撃者が用意したWebサイトに対してクライアント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
  - XSS(Cross Site Scripting)などの他の攻撃への応用