あみだくじを用いた対話的なブラウザ履歴漏洩の研究

笹　航大†　　清水　雄太†　　菊池浩明†

明治大学総合数理学部　先端メディアサイエンス学科‡

1　はじめに

近年，利用者が気付かないうちに自分のブラウザ履歴を第三者に知らせてしまうブラウザ履歴盗聴攻撃の危険性が高まっている．Weinberg らは，チェスを模した Captcha を提案している[1]．不正ボットを防止するための Captcha を偽装し，チェスの駒をユーザにクリックさせることにより，ブラウザの履歴を盗聴する．全ての駒には URL が一意に設定されており，すでに訪問したサイトの駒は背景と同色で表示されるため，ユーザは気づかないままクリックした URL が既訪問であることを取得されてしまう．しかし，Weinberg らの提案した Captcha では１クリックで１履歴を盗聴することしかできない．

そこで，本稿では，１クリックで複数のブラウザ履歴を同時に盗聴することが出来る，あみだくじを用いたブラウザ履歴盗聴システムを提案する．本研究は履歴盗聴サイトのリスクについて報告する．

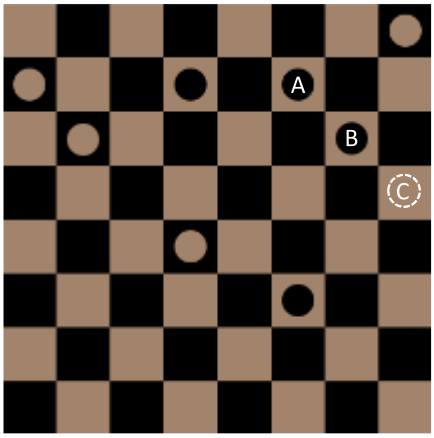

図１：chessboard 方式[1]の原理図

2　ブラウザ履歴盗聴の方法

2.1　chessboard 方式[1]

Weinberg らの提案する chessboard[1]では，HTML の A タグと CSS の visit タグを使用する．未訪問 URL を指定した A タグは背景と同色に，既訪問 URL は背景と違う色に CSS で設定することにより，対象者の履歴に応じて表示結果が変化することを利用する．

図１に示す chessboard の原理図において，A に設定した URL は既訪問である．背景は茶色なので，駒の色は背景と異色の黒になっている．B も同様である．一方，C に設定した URL は未訪問で，駒は背景と同色の茶色になっているため，存在しないように見える．Captcha として利用者に駒をクリックさせることにより，その対象者が A，B のサイトを訪問したことがサーバにわかる．

2.2　提案方式

あみだくじの横線を複数の URL に対応した A タグとすることで，指定した URL が未訪問か既訪問かによって，たどり着くゴールが変化するシステムを提案する．ゴールをクリックさせることで履歴を盗聴する．このシステムの利点はあみだくじの組み方により，１クリックで同時に複数の履歴を盗聴することが可能という点である．しかし同時に盗聴できる履歴が増えるにあたり，あみだくじの本数が増え，複雑さが増すため，その効果を明らかにするために３節の実験を行った．

図２の４本のあみだくじ方式の実行画面を使用してシステムの説明を行なう．

まず，一意の URL A，B に対応する複数の枝を設定する．①の場合，A，B 両方の URL を未訪問のため，図の N がゴールとなる．②③④も同様である．ここで，g を１クリックで同時に取得できる URL 履歴盗聴数と定義する．よって図２の①は g=0，②，③は g=1，④は g=2 である．また g=0 の場合，あみだくじとして不自然である．よって実験用ではどのサイトの閲覧履歴がなくとも表示されるダミーの横線を配置した．

チェスボード方式およびあみだくじ方式は，HTML と CSS，PHP，SQL を用いてウェブブラウザ上での動作を確認した．

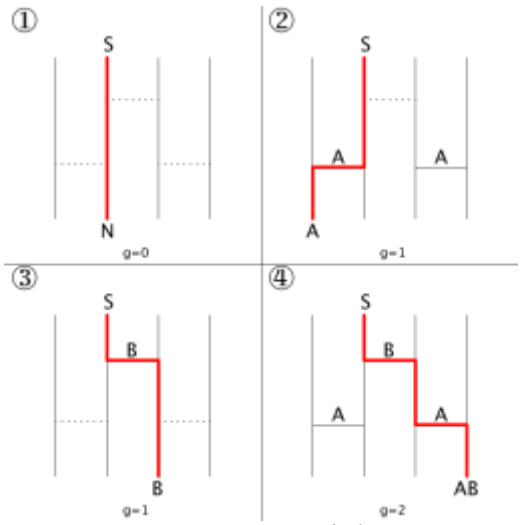

図２：あみだくじ方式

3.　実験

3.1　概要

chessboard 方式では g=1 の時間を計測すること，あみだくじ方式では g=0～3 の時間を計測することで，単位時間当たりの履歴盗聴数を明らかにすることを実験目的

†Study on Interactive browser history sniffing using Amida Lottery , Kota Sasa , Yuta Shimizu
School of Interdisciplinary Mathematical Sciences, Meiji Uni-Versity

とする．実験は 20 代から 50 代の男女 20 名に対して，2015 年 10 月 1 日から 1 か月の間に行った．

3.2 実験方法

実験 1　あみだくじの方式の比較

Processing を用いてランダムなあみだくじを表示する．1 回目は g が 0～2，2 回目は g が 0～3 の提案方式で，それぞれのあみだくじを解きゴールをクリックするまでの応答時間を計測する．（これ以降，g が[0,2]からランダムに選ばれることを，g=[0,2]と表記する．）

実験 2　chessboard 方式とあみだくじ方式の比較

8×8 マスのチェス盤にランダムに茶色と黒の駒を 5 個ずつ配置し，計 10 個表示して，そのすべてをクリックするのにかかる時間を計測する．

3.3 実験 1 の結果

実験 1 の結果を表 1 および図 3 に示す．g=[0,2]と[0,3]の平均応答時間を公平に比較するため，g=6 にそろえて，それぞれの平均応答時間を g=[0,2]は 3 倍，g=[0,3]は 2 倍する．その結果，g=[0,3]の方法がより平均応答時間が短くなった．

よって，g=3 を chessboard 方式と比較する．あみだくじの同時履歴盗聴数 g について線形回帰したところ，

$$T_A(g)=2306.9+503.9g$$

であった．g が小さい場合，応答時間の分散は小さいが，g が大きくなるにつれて増加している．この原因は，あみだくじを解く個人差にあると考える．

また図 3 の「amida」の傾きは 503.9，「chess」の傾きは 1334.3 となった．従って，3<g のとき，「amida」の方が「chess」よりも経過時間が短くなると推測する．

表 1．あみだの本数 n についての処理時間

n	4	8
g	[0,2]	[0,3]
1 クリックの平均達成時間[ms]	2805.9	3273.7
標準偏差	966.5	1449.6

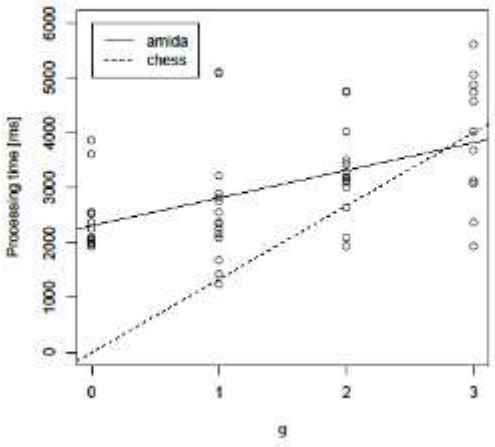

図 3：取得履歴数 g ごとのあみだくじ方式の処理時間

3.4 実験 2 の結果

実験 2 の結果を表 2 および図 4 に示す．平均応答時間は「amida」が 3.27 秒，「chess」が 1.33 秒である．ただし，あみだくじ方式と chessboard 方式を公平に比較するために，同時履歴盗聴数 g=3 にそろえて考える．**chessboard 方式は g に比例して時間がかかるので，$T_C(g)=1.33g$ と予測する．**この $T_C(g)$ を図 3 の上に重ねてプロットする．**図 4 に，両方式のクリックあたりの応答時間**の分布を示す．以上より，あみだくじ方式の方が 1 履歴を取得する際にかかる時間の平均が短いと結論づける．

表 2．chessboard 方式とあみだくじ方式の応答時間

方式	g	1 クリックの平均応答時間[ms]	標準偏差
chessboard	1	1334.3	503.87
あみだくじ	0～3	3273.7	1449.6

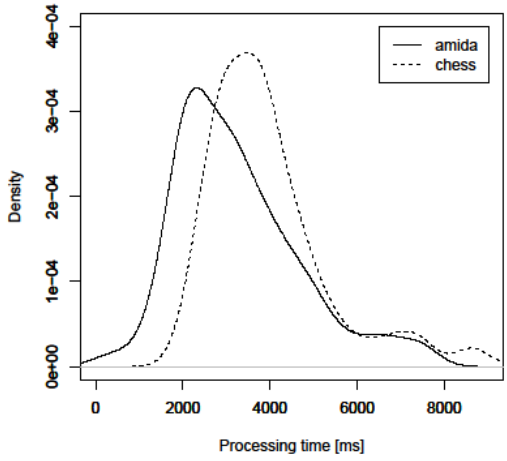

図 4：chessboard 方式とあみだくじの応答時間分布

7. まとめ

本研究では，あみだくじを用いた対話的なブラウザ履歴盗聴システムの提案を行った．また，評価実験によりブラウザ履歴盗聴システムとの効率を評価した．

あみだくじを用いたシステムの効率が予想以上に低かった理由として「応答時間の長さ」が挙げられる．chessboard 方式は視覚で捕え，反射的に応答できるのに対して，あみだくじ方式は線をなぞらなければならないためより時間を要する．

今後の課題として，あみだくじの本数を増やした場合の効率，従来の対話的なブラウザ履歴盗聴システムの単位時間あたりの履歴盗聴数を調べることが挙げられる．

参考文献

[1] Zachary Weinberg, Eric Y. Chen, Pavithra R. Jayaraman and Collin Jackson, “I Still Know What You Visited Last Summer”, 2011 IEEE Symposium on Security and Privacy, pp. 147-161, 2011.