DEIM Forum 2022 J43-1

プライバシーリスクの範囲と程度を実感させるウェブ検索スニペット

清水　勇祐†　　山本　祐輔†

† 静岡大学大学院総合科学技術研究科　〒 432–8011 静岡県浜松市中区城北 3–5–1
E-mail: †shimizu@design.inf.shizuoka.ac.jp, ††yamamoto@inf.shizuoka.ac.jp

あらまし　本論文ではウェブ検索ユーザに，ウェブ閲覧履歴が誰にどの程度知られる可能性があるのかという情報を提供する，2 つの検索インタフェースを提供する．提案した検索インタフェースがウェブ検索ユーザのプライバシ意識や行動にどのような影響を与えるかをオンラインのユーザ実験を行い検証した．ユーザ実験の結果，実験協力者は単にトラッカーが埋め込まれているかどうかを示す検索結果のインタフェースよりも，提案したインタフェースの方が閲覧履歴の漏洩を知る上で効果的であると感じていることがわかった．本研究で得られた知見によって，ウェブ検索における便益とリスクを考えるための検索インタフェースの設計に寄与することが期待される．

キーワード　プライバシー，トラッキング広告

1 はじめに

ウェブ上でのパーソナライズされた情報配信はますます盛んになっている．一方で，データのプライバシ問題が重要な社会問題になっている．デジタルマーケティング会社は，ユーザの行動や嗜好に応じて，ウェブ検索履歴や閲覧履歴などのユーザの行動ログを追跡し，パーソナライズされた広告を配信している．しかし，パーソナライズされた広告に不信感を抱く人が増えており [1]，自分のデータがどのように使用されるのかについて深刻な懸念を抱いている人も存在する [2]．過度なトラッキングを行うと，健康上の懸念や思想信条など，プライベートな情報を反映したウェブ広告が表示される可能性がある．その結果，人々は自分のプライベートな情報が流出した場合に起こりうる恥ずかしさを懸念している．

このような懸念から個人情報保護の機運が高まっている．例えば，欧州では一般データ保護規則 [1]，米国カリフォルニア州ではカリフォルニア消費者プライバシ法 [2]が制定されている．また，ウェブブラウザ用のトラッキングブロッカーの開発と改良が行われている．現在，多くの人が閲覧履歴の流出を防ぐためにそのようなトラッキングブロッカーを使用しているが，ブロッカーを回避する技術も開発されている．技術的なアプローチのみでは，オンライントラッキングのリスクを完全に回避することは困難である [3] [4]．ウェブ上のプライバシを保護するためには，ユーザ自身がプライバシを保護するための効果的な行動を取る必要がある．

ウェブ検索エンジンは，ウェブ上の情報を取得するための主要なツールとして広く利用されているが，ウェブ検索を行う際に考慮すべきプライバシ上の問題がいくつか存在する．第一に，ウェブ検索エンジンは一般的に，検索エンジン結果ページ（SERP）において，情報ニーズに関連する情報（タイトル，URL，スニペットなど）しか提供していない．そのため，SERP に掲載されているウェブページのプライバシ・リスクを調査・評価することは困難である．第二に，ウェブページのプライバシポリシーを確認するためにはスキルや時間的コストを要する点である [5]．ウェブ検索ユーザがプライバシポリシーを確認すれば，どのような行動データが収集されているのかや，その理由を知ることができる．しかし，そのようなプライバシポリシーの確認には時間がかかる．また，プライバシポリシーを確認するためにウェブページを訪れた際にも，行動データが追跡されてしまう危険性が存在する．

ウェブページ訪問のプライバシリスクは，ウェブ検索ユーザがそのウェブページを閲覧する前に評価できるべきである．本稿では，ウェブ検索ユーザに対して，ウェブ閲覧履歴が誰にどれだけ漏れるかという情報を提供することを目的とし，以下のような検索結果の表現を提案する．その上で，表現されたユーザインタフェース（UI）がウェブ検索ユーザのプライバシ意識や検索行動に与える影響を明らかにする．

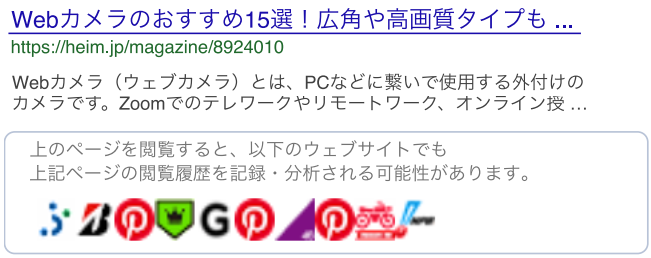
`Icon` UI ：ユーザが検索結果をクリック（閲覧）した際に，その検索結果の閲覧履歴が流出する可能性のあるウェブサイトの具体例をファビコンで表示する．

`Ratio` UI ：ユーザが検索結果をクリック（閲覧）した際に，その検索結果の閲覧履歴が流出する可能性のあるウェブサイトのカテゴリと数を表示する．

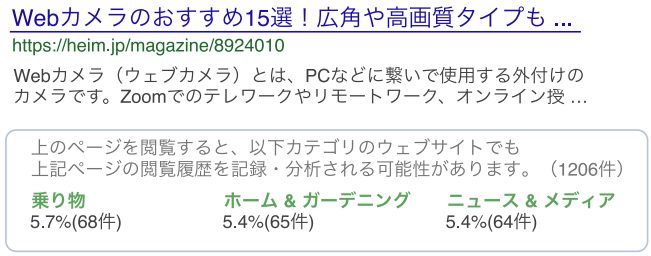
本論文の貢献は以下の通りである．

- ウェブページ閲覧履歴のトラッキングの度合いを伝えるための検索結果 UI「`IconUI`」と「`RatioUI`」を提案した．
- ユーザ実験の結果，実験協力者は単にトラッカーが埋め込まれているかどうかを示す検索結果のインタフェースよりも，提案したインタフェースの方が閲覧履歴の漏洩を知る上で効果的であると感じていることがわかった．
- 検索行動を分析した結果，`RatioUI` を利用した実験協力者は，トラッカーが埋め込まれた検索結果をより積極的に閲覧して有用な情報を探す傾向が見られた．一方，「`IconUI`」ではこのような傾向は見られなかった．

1：https://gdpr-info.eu/
2：https://https://oag.ca.gov/privacy/ccpa



(a)IconUI



(b)RatioUI

図 1　提案手法の概観図

2　関 連 研 究

2.1　ウェブ閲覧におけるトラッキング

オンライン行動追跡（OBT）は，ユーザの好みや行動に応じて，情報提供を最適化する上で重要な役割を果たしている．例えば広告のターゲッティングやウェブ検索のパーソナライゼーションなどが挙げられる．複数のウェブサイト間の行動を追跡するために，様々な手法が開発されてきた．一般的なアプローチの 1 つは，サードパーティクッキーを使用するものである．例えば，Englehardt らは，サードパーティクッキーを使用した行動追跡により，IP アドレスを使用するよりも効率的にウェブ上のユーザの閲覧遷移を明らかにできることを発見した [6]．Libert らは，多くの Web サイト，特にニュースサイトは，収益化やウェブサイトの管理のためにサードパーティクッキーに依存しており，不透明なトラッキングを行うことが多いと報告している [7]．

サードパーティクッキーに対する懸念から，Apple は Intelligent Tracking Prevention[3]を，Google は Privacy Sandbox[4]を導入し，ウェブ上でのトラッキングをブロックしている．しかしリンクデコレーション [5]，CNAME クローキング [6]，ブラウザフィンガープリントなど，ウェブ上でユーザを識別・追跡する新しい手法が開発され始めている [8] [9]．Levia らは，マウスの動きの情報でも，合理的な精度でユーザの属性を推測できると報告している [10]．

3：https://www.apple.com/privacy/features/
4：https://www.chromium.org/Home/chromium-privacy/privacy-sandbox
5：https://webkit.org/blog/8828/intelligent-tracking-prevention-2-2/
6：https://webkit.org/blog/11338/cname-cloaking-and-bounce-tracking-defense/

ウェブにおけるプライバシ保護のためには，ユーザがウェブ上のプライバシリスクを評価できるようにすることが重要である．本研究では，どのようなプライバシリスクの表現方法が，閲覧履歴の流出先や流出範囲に関する情報をウェブ検索ユーザに提供できるかを検討する．本研究では，検索エンジンからウェブサイトに移動する前に，ウェブサイト上のトラッキング行為を検出する方法として，サードパーティクッキーに注目している．

2.2　プライバシ意識の強化

一般に，人々がウェブ上のプライバシを守りたいと思っていても，プライバシリスクを具体的に理解させ，プライバシを守るための行動をとらせることは困難である [11]．そこで，先行研究では，プライバシリスクの評価やプライバシを意識した行動を支援する手法が開発されている．例えば，Harkous らは，ウェブサイトのプライバシポリシーを分析し，ウェブサイトを訪問した際に収集される個人情報の種類を可視化するツールを提案している [12]．また，Kelly らは，食品の栄養表示にヒントを得て，ウェブサイト上のプライバシリスクを分かりやすく表現することを検討している [13]．Kelly らの研究と同様に，Naeini らは，IoT デバイスを購入する際にセキュリティリスクやプライバシリスクを評価するのに役立つラベルの表現を提案している [14]．

ウェブ検索やウェブ閲覧におけるプライバシ意識を高めるためのツールも提案されている．例えば，Zimmerman らは，ウェブ検索において，与えられたクエリに対する各ウェブ検索結果のプライバシリスクのレベルを示すプライバシナッジを提案している [15]．また，DuckDuckGo Inc. は，閲覧したウェブサイトのプライバシリスクレベルを表示するブラウザ拡張機能 *Privacy Essentials*[7]を公開している．また，Privacy Essentials に類似したツールとして，*Privacy Badger*[8]が存在する．我々は，Zimmerman の研究のようなプライバシリスクの指標に基づいて，`IconUI` と `RatioUI` を提案する．これは，ウェブ検索ユーザに，閲覧履歴がどの第三者にどのくらい漏れる可能性があるかについての情報を提供するものである．

3　提 案 手 法

本研究では，ウェブ検索ユーザがウェブ検索を行う際に，ウェブページの閲覧前にプライバシリスクを評価できるように，SERP におけるスニペット表現を検討する．提案された検索スニペットは，ウェブ検索ユーザが SERP 上のウェブページをクリックする前に，自分の行動データを監視している対象を直感的に知るのに役立つ．ここでは，ウェブページの閲覧履歴が漏洩する可能性のあるウェブサイトを漏洩先と定義する．

提案手法では，まず SERP 上のどのウェブページがユーザの行動を追跡しているかを検出し，潜在的な漏洩先を検出する．そして，一般的なウェブ検索結果スニペットを拡張するこ

7：https://duckduckgo.com/app
8：https://privacybadger.org/

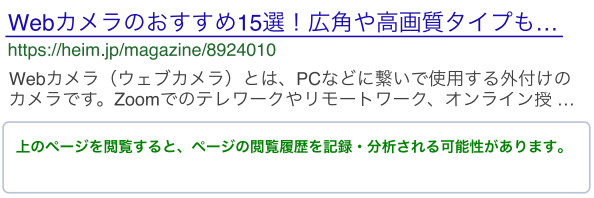


図 2　シンプルなトラッキングインジケータ（ControlUI）を用いたウェブ検索結果の概観図

とで，スニペットを生成する．本研究では，閲覧行動の漏洩範囲を説明するために，3 つのスニペットを検討した．以下に詳細を示す．

3.1　スニペットの設計

3.1.1　IconUI: 漏洩先の具体例の表示

図 1(a) に示すように，IconUI はウェブ検索結果の漏洩先のファビコンのリストを表示する．この UI により，ユーザはウェブページの閲覧履歴が漏洩する可能性のあるウェブサイトの例をいくつか知ることができ，トラッキングの可能性があることも知ることができる．なお，IconUI は Wang の研究 [16] [17] を参考に考案した．Wang らは，SNS 上で共有されている写真を見ることができる人物をパーソナライズされた例として特定し，SNS ユーザが予期せぬ人物に写真を見られる可能性を理解できるようにすることを提案している．また，Wang らの研究では，SNS 上で写真を共有する際のプライバシリスクを直感的に理解することができることが明らかになった．提案する IconUI は，Wang らの研究とは異なり，ウェブ検索ユーザにパーソナライズされた例を表示しない．その代わりに，IconUI はウェブ検索ユーザに，自分の閲覧履歴がどのようなウェブサイトに流出する傾向があるかを，流出先の例として表示する．

3.1.2　RatioUI: 漏洩先のカテゴリ別の数値の表示

図 1(b) に示すように，RatioUI は，漏洩先のウェブサイトの上位 3 つのカテゴリとその規模を示している．RatioUI は，ユーザがウェブ検索結果をクリックした際に，そのウェブ検索結果ページの閲覧履歴がどのようなカテゴリのウェブサイトに流出するのかをユーザに知らせる．また，RatioUI では，ウェブサイトのカテゴリに応じて，何件のウェブサイトに履歴が流出するかの情報も表示する．IconUI とは異なり，RatioUI では流出先のウェブサイトの具体例ではなく，流出先の数と流出先のウェブサイトカテゴリの割合が表示される．IconUI のデメリットとして，ファビコンで表現されたウェブサイトを知らないユーザが存在することが考えられる．RatioUI は，ウェブ検索ユーザが各漏洩先サイトの詳細を知らない場合にも，漏洩先の範囲や種類を理解できることを期待している．

3.1.3　ControlUI: 単純なトラッキング警告

図 2 に示すように，DuckDuckGo Privacy Essentials や Privacy Badger と同様に，ウェブページのトラッキングの可能性のみをユーザに表示するベースラインの UI を ControlUI とする．ControlUI は，IconUI や RatioUI とは異なり，漏洩先に関する情報を表示するものではない．ここでは，検索結果からリンクされたウェブページにサードパーティクッキーによるトラッカーが埋め込まれていると仮定する．この場合，ユーザがウェブページにアクセスすると，そのページの閲覧履歴が保存され，分析される可能性があることだけを示す．この ControlUI により，ユーザは SERP 上のどのウェブページがトラッキングリスクを伴う可能性があるかを，簡単な方法で特定することができる．

表 1　実験協力者の割り当て

	検索 UI		
検索トピック	Control	Icon	Ratio
買い物	68	76	71
健康	62	67	61
合計	130	143	132

3.2　仮　　説

本研究では，提案するスニペットが，ユーザのプライバシリスクに対する理解やウェブ検索時の検索行動に与える影響を調査した．具体的には，以下の仮説を検証することに焦点を当てた．

- H1　ウェブ検索ユーザに対して，どのような第三者が閲覧履歴を監視できるかという情報を事前に表示することで，単にトラッキングの有無を表示するよりも，プライバシリスクを意識するようになる．
- H2　どのような第三者が閲覧履歴を監視できるかという情報を事前に表示することで，ウェブ検索ユーザは，プライバシを保護するためにウェブ検索結果のリストをより注意深く探索する．

4　実　　験

オンラインユーザ調査において，提案したスニペットの有効性を，ウェブ検索における行動データの漏洩に関するリスクを説明する能力の観点から評価した．ユーザ調査は，2021 年 8 月 14 日と 15 日に日本語で行った．

4.1　タ　ス　ク

今回のユーザ調査では,「ショッピング」と「健康」という 2 つのトピックで 4 つの検索タスクを用意した.「ショッピング」では，2 つの検索タスクを用意し，自分が購入したいと思うウェブカメラやイヤホンのメーカーを検索させた.「健康」のカテゴリでは，糖尿病やメニエール病の代表的な症状を検索させた．それぞれの検索タスクでは，実験協力者は用意されたウェブ検索結果のリストを検索し，回答を報告した．ここでは，各実験協力者はショッピングカテゴリまたは健康カテゴリのいずれかのみで 2 つの検索タスクを行った．

4.2　実 験 手 順

募集サイトの同意書に同意した後，実験協力者をユーザ調査用のサイトに誘導した．そして，各実験協力者に検索 UI 条件

と検索トピックを無作為に割り当てた．表 1 に UI 条件とトピックの割り当てを示す．

はじめに，実験協力者に対し，タスクの流れと検索システムの説明を行った．また，データ収集の方針についても説明した．なお，実験協力者は，検索タスク中に収集したデータを使用してもよいと同意した場合にのみ，ユーザ調査を進めた．実験協力者は，各検索タスクを実行する前に，事前アンケートに回答した．事前アンケートでは，ウェブ検索におけるプライバシリスクの認識について質問した（セクション 4.4）．その後，各実験協力者は,「買い物」または「健康」のいずれかのトピックについて，2 つの検索タスクを行った．なお，タスクの順番は実験協力者ごとにランダムに割り当てた．また，検索タスクを実行する前に，タスクのシナリオを提示した．そして，各実験協力者が「検索開始」ボタンをクリックすると，検索結果のリストが表示される．実験協力者はそのリストを閲覧して，回答をまとめた．そして，その結果と理由をウェブサイトで報告した．すべての検索タスクが完了した後，実験協力者に事後アンケートを実施した．事後アンケートでは，実験協力者のウェブ検索におけるプライバシ意識の変化を調べ，検索 UI に対する主観的な評価を尋ねることを目的とした．

4.3 検索システムのプロトタイプ

我々は，3 種類のプライバシを考慮したスニペットを提供する検索システムのプロトタイプを開発した． ウェブ検索ユーザがプロトタイプシステムにクエリを発行すると，システムは SERP 上の各ウェブ検索結果に対して以下のようにスニペットを生成する．

（1） 従来のウェブ検索エンジン（Google や Bing など）の API を使用して検索結果を取得する．
（2） SERP 上の各検索結果に，サードパーティクッキーが含まれているかどうかを分析する．
（3） 対象となる検索結果にサードパーティクッキーが含まれている場合，そのクッキーの発行ドメインが，事前に人気のあるウェブサイトに対して検出されたドメインのリストに含まれているかどうかを確認する．
（4） 検索結果 X が人気サイト Y と同じサードパーティドメインのクッキーを含んでいる場合，X の閲覧履歴が Y に漏洩する可能性がある（Y が漏洩先である）と判断する．
（5） 漏洩先ページのリストを用いて，3.1 節で述べたスニペットを生成する．

手順 3 では，ウェブサイトのトラフィックを網羅的に分析するウェブサービスである SimilarWeb.com[9]を用いてウェブページを取得した．24 の主要なカテゴリについて，日本のウェブサイトで最もアクセス数の多い 100 のウェブページを取得した．手順 2，3 では，オープンソースツールの webXray [18] を用いて，ウェブページのトラフィックやコンテンツを分析し，ウェブページ内のサードパーティクッキーを検出・分析する．このシステムは，表示される漏洩先の数を制限するために，漏洩先の逆文書頻度（IDF）を計算した．与えられたクエリに対するウェブ検索結果の文章数を N とし，漏洩先 d に閲覧履歴が漏洩する可能性のある検索結果の数を $df(d)$ とする．すると，d の IDF $idf(d)$ は以下のように定義される．

$$idf(d) = log\frac{N}{df(d)}$$

`Icon`UI は，各ウェブ検索結果に対して，漏洩先として上位 5 件の IDF 値を持つウェブサイトに加えて，その検索結果特有の漏洩先として下位 5 件の IDF 値を持つウェブサイトを表示する．`Ratio`UI は，SimilarWeb.com のカテゴリに従って，各検索結果の漏洩先の数を集計する．`Ratio`UI では，各ウェブ検索結果について，上位 3 件のカテゴリと漏洩先ウェブサイトの数，および全体に対する比率を表示する．`Control`UI では，ウェブ検索結果に漏洩先がある場合，警告文のみを表示する．

すべての検索 UI において，奇数順位のウェブ検索結果にのみリスク指標を表示するようにした．これは，リスク指標のあるウェブ検索結果とないウェブ検索結果をできるだけ均等に表示するための操作である．この操作により，リスク指標のある検索結果とない検索結果のクリック数を比較することができると期待した．

4.4 アンケート項目

ユーザ実験では，事前アンケートに 1 件の質問，事後アンケートに 9 件の質問および人口統計学的質問を用意した．実験協力者は以下の質問（Q0〜Q8）に 5 段階のリッカート尺度で回答した．

Q0：プライバシリスクの認識

実験協力者に対し，検索タスクの前後すなわち，タスク前と終了時のアンケートで，ウェブ検索においてどの程度のプライバシリスクを感じているかを確認した.（「1：全くリスクを感じない」〜「5：非常にリスクを感じる」）．そして，検索タスクの前後でこの質問に対する実験協力者のスコアの差を分析した.

Q1：プライバシリスクを気にせずに検索できるかどうか

割り当てられた UI が，プライバシリスクを気にせずに検索を行うことに対して，どの程度役に立ったかを尋ねた（「1：全く役に立たない」〜「5：非常に役に立つ」）.

Q2：トラッカーが含まれている検索結果の見つけやすさ

ウェブ検索結果にトラッカーが埋め込まれているかどうかを知るという点で，割り当てられた UI の有用性について尋ねた（「1：全く役に立たない」〜「5：非常に役に立つ」）.

Q3：データ漏洩の範囲を知る上での有用性

ウェブ検索結果をクリックした際に，そのウェブ検索結果の閲覧履歴が流出する可能性のあるウェブページを特定するという点で，割り当てられた UI がどの程度有用であったかを尋ねた（「1：全く有用ではない」〜「5：非常に有用である」）.

Q4：プライバシリスクのある検索結果の避けやすさ

ウェブ検索でトラッカーが埋め込まれているページを避けるという点で，割り当てられた UI がどの程度役に立ったかを尋

9：https://www.similarweb.com

ねた（「1：全く役に立たない」〜「5：非常に役に立つ」）．

Q5：リスクはあるが価値のある検索結果を見つけることができるという点での有用性

ウェブ検索でトラッカーが埋め込まれているが，価値あるウェブページを見つけるという観点から，割り当てられた UI がどの程度有用であるかを尋ねた（「1：全く有用でない」〜「5：非常に有用である」）．

Q6：検索のしやすさ

提案された UI の使いやすさを検討するために，実験協力者に，割り当てられた UI がウェブ検索タスクに対してどの程度妨げになるかを尋ねた（「1：全く妨げにならない」〜「5：非常に妨げになる」）．分析のために，この質問に対する実験協力者の回答の逆数を集計した．

Q7：表現のわかりやすさ

ユーザビリティの観点から，検索結果のプライバシリスクを知る上で，割り当てられた UI がどの程度わかりやすいかを尋ねた（「1：まったくわからない」〜「5：非常にわかりやすい」）．

Q8：利用への積極性

もし割り当てられた UI が実用化された場合に，日常的に使用したいと思うかを尋ねた（「1：全く使用したくない」〜「5：非常に使用したい」）．

人口統計情報

実験協力者の性別，年齢などの人口統計学的情報を収集した．また，実験協力者の持つプライバシ意識を調査するため，過去 1ヶ月間にウェブブラウザのプライベートブラウジングモードを利用したかどうかを尋ねた．

4.5 実験協力者

クラウドソーシングサービスである CrowdWorks.jp[10]で 424 名の実験協力者を募集した．事前にデータ収集の方針を説明し，検索タスクで収集したデータを使用することに同意してもらった上で，ユーザ調査を実施した．なお，19 名の実験協力者は，タスクを完了しなかったか，タスクの実行に異常に時間がかかったため，外れ値として分析から除外した [11]．このようにして，合計 405 名の実験協力者の回答を分析した．実験協力者の属性を表 2 に示す．タスクを完了した実験協力者には，報酬として 150 円を支払った．実験協力者は平均して，2 つのタスクを 429.8 秒で完了した．

5 結　　果

405 人の実験協力者の回答を分析し，3 つのプライバシリスク指標がウェブ検索結果に与える影響を調べた．収集したデータが正規分布に従わなかったため，3 つの UI についてノンパラメトリック一元配置分散分析 (Kruskal–Wallis 検定) を採用した．事後解析では，Benjamini–Hochaberg FDR test [19] を用いて多重比較を行った．ここでは，有意水準を $\alpha = 0.05$ とした．

表 2　実験協力者のデモグラフィック情報

	人数	割合
実験協力者の合計	405	
性別		
男性	229	56.5%
女性	173	42.7%
無回答	3	0.7%
年齢		
20 歳未満	4	1.0%
20–29 歳	71	17.5%
30–39 歳	124	30.6%
40–49 歳	117	28.9%
50–59 歳	62	15.3%
60 歳以上	26	6.4%
無回答	1	0.3%
過去 *1*ヶ月以内のプライベートブラウジング機能の使用の有無		
あり	178	44.0%
なし	227	56.0%

5.1 アンケート

9 つの質問に対する回答の平均値と，検定結果を表 3 に示す．Q0 では，検索タスクの前後で，プライバシリスクに対する意識についての質問に対する回答のスコア差を計算した．平均値が高いほど，UI に対して肯定的な結果を示している．事後解析における 3 つの UI のペアワイズ比較を表 4 に示す．

Q1〜Q8 の平均値が 3 より大きいことから，実験協力者は 3 つの UI に対して概ね肯定的に感じていることがわかる．いくつかの質問については，UI 間，特に `Ratio`–`Control` の UI 間で統計的有意差が見られた．

プライバシに関する Q1，Q2，Q4 については，3 つの UI の間に有意な差があることがわかった（Q1：$p < 0.01$，Q2：$p < 0.01$，Q4：$p < 0.01$）．また，事後解析の結果，Q1，Q2，Q4 において，`Ratio`UI の平均回答は `Control`UI の平均回答よりも少ないことがわかった．`Ratio`UI を使うと，`Control`UI を使った場合に比べて，ウェブ検索時にプライバシリスクに対する不安を感じやすいことがわかった（Q1 平均：3.45 vs 3.88; $p < 0.01$）．また，`Ratio`UI では，`Control`UI（Q2 平均：3.60 vs. 3.99; $p < 0.01$），`Icon`UI（Q2 平均：3.60 vs. 3.87; $p < 0.05$）に比べて，トラッカー付きの検索結果を見つけることに困難を感じていることがわかった．同様に，`Ratio`UI は `Control`UI に比べて，プライバシリスクのある検索結果を回避するという点で，あまり役に立たないと感じられているが，`Ratio`UI の平均的な回答は中立的なスコアを上回っていた（Q4 平均：3.58 vs. 4.02; $p < 0.01$）．

なお，Q3 では 3 つの UI の間には有意な差が見られた（$p < 0.05$）．しかし，Q1，Q2，Q4 に比べ，`Ratio`UI（平均：3.64）と `Icon`UI（平均：3.75）は `Control`UI（平均：3.32）よりも高く評価されていた（Q3; Control-Ratio:$p < 0.05$; Control-

10：https://crowdworks.jp

11：タスクのセッション時間を対数変換した値の IQR（四分位範囲）を算出した．対数変換したセッション時間が $Q3 + 1.5IQR$ 以上または $Q1 - 1.5IQR$ 以下の実験協力者を外れ値として除外した．

表 3　事後アンケートの質問に対する平均値，標準偏差（SD），および統計的有意差（有意水準は*：0.05，**：0.01，***：0.001）．Q1〜Q8 は，5 段階のリッカート尺度（1：強く否定的，3：中立，5：強く肯定的）で回答．

質問項目	UI			p-value
	Control	Icon	Ratio	
Q1. プライバシリスクを気にせずに検索できるかどうか	3.88 (0.95)	3.66 (1.00)	3.45 (1.06)	**
Q2. トラッカーが含まれている検索結果の見つけやすさ	3.99 (0.93)	3.87 (0.93)	3.60 (1.01)	**
Q3. データ漏洩範囲を知る上での有用性	3.32 (1.16)	3.75 (1.02)	3.64 (0.99)	*
Q4. プライバシリスクのある検索結果の避けやすさ	4.02 (0.94)	3.87 (0.97)	3.58 (1.11)	**
Q5. リスクはあるが価値のある検索結果を見つける上での有用性	3.75 (1.04)	3.59 (1.08)	3.54 (1.07)	0.25
Q6. 検索のしやすさ	3.93 (0.82)	3.82 (0.79)	3.86 (0.89)	0.52
Q7. 表現のわかりやすさ	4.02 (0.80)	3.80 (0.99)	3.55 (1.03)	***
Q8. 利用への積極性	3.82 (0.84)	3.57 (0.94)	3.47 (0.99)	**
Q0. プライバシ意識の変化	0.12 (0.69)	0.20 (0.61)	0.11 (0.63)	0.71

表 4　多重比較を行った際の統計的有意差の有無（有意水準は，*: 0.05; **: 0.01; ***; 0.001）．

質問項目	組み合わせ		
	Control-Icon	Control-Ratio	Icon-Ratio
Q1	0.092	**	0.108
Q2	0.224	**	*
Q3	*	*	0.403
Q4	0.177	**	0.058
Q5	NA	NA	NA
Q6	NA	NA	NA
Q7	0.093	***	0.058
Q8	*	**	0.338
Q0	NA	NA	NA

Icon:$p < 0.05$）．つまり，実験協力者は，検索結果をクリックした場合にどのウェブサイトに閲覧行動が漏れるのかがわかりやすいという点で，RatioUI と IconUI がより有用であると判断する傾向が見られた．Q5 では，3 つの UI の間に統計的な違いは見られなかった（$p = 0.25$）．

また，Q7 と Q8 については，3 つの UI 間で有意な差が見られた（Q7：$p < 0.001$，Q8：$p < 0.01$）．RatioUI は，ControlUI（平均 4.02）に比べて，ネガティブなスコアをあまり獲得していないにもかかわらず，RatioUI（平均 3.55）は ControlUI（平均 4.02）に比べて，情報を理解するのが難しいと感じていることがわかった．また，ControlUI（平均：3.82）の方が RatioUI（平均：3.47）や IconUI（平均：3.57）よりも使用したいと考えていることがわかった（Q8; Control-Ratio:$p < 0.01$; Control-Icon:$p < 0.05$）．Q6（検索のしやすさ）については，3 つの UI の間に統計的な違いは見られなかった（p=0.52）．

Q0 については，3 つの UI とも，平均してウェブ検索におけるプライバシリスクに対する実験協力者の意識をわずかに改善した（Q0:Icon=0.20,Ratio=0.11,Control=0.12）．しかし，3 つの UI の間で有意な差は見られなかった（$p = 0.71$）．

5.2 行動分析

5.2.1 SERP 閲覧時間

表 5 に示すように，3 つの UI の間に有意な差は見られなかった（$p = 0.49$）．また，実験協力者がウェブ検索結果のリストをどれだけ注意深く閲覧したかを調べるために，検索タスク中に SERP 上の検索結果を初めてクリックするのに要した時間を分析した．これを「初回クリックまでの時間」と定義する．表 5 に示すように，初回クリックまでの時間に 3 つの UI の間で有意な差は認められなかった（$p = 0.66$）．

5.2.2 最大クリック深度

検索結果のリストを読み取るため，実験協力者がどの程度の労力を必要とするかを調べるために，実験協力者がクリックした検索結果の順位を調べ，最も深い検索結果の順位を分析した．ここでは，最大クリック深度が大きいほど，実験協力者は検索結果リストのより深いところにある検索結果を見たと解釈する．表 5 に示すように，最大クリック深度に 3 つの UI の間で有意な差は見られなかった（$p = 0.98$）．

5.2.3 ページ閲覧数

各 UI が実験協力者に検索結果リストのウェブページをクリックする意欲を与えたかを調べるために，実験協力者が検索タスク中に検索結果リストのウェブページをどれだけ閲覧したかを分析した．表 5 に示すように，ページ閲覧数については 3 つの UI の間に有意な差は認められなかった（$p = 0.23$）．

6 考　　察

5.1 節で述べたように，アンケート結果によると，3 つの UI は，8 つの質問に対して平均的に高い評価を得た（Q1-Q8 で 3 以上（表 3））．このことから，実験協力者の多くは 3 つの UI がプライバシを意識したウェブ検索やユーザビリティに何らかの役に立つと考えていることがわかった．

また，プライバシリスクに対する意識の向上という点では，3 つの UI の間に有意な差は見られず，プライバシリスクに対する意識はそれほど向上していないことがわかった（表 3 の Q0）．一方で，プライバシリスクを気にせずにウェブを検索するとい

表 5　ユーザの検索行動の結果（かっこ内は標準偏差，*: 0.05）

Metric	UI condition			p-value
	Control	Icon	Ratio	
SERP 閲覧時間 (秒)	343.9 (259.9)	376.0 (299.1)	416.6 (333.7)	0.49
初回クリックまでの時間 (秒)	32.5 (48.7)	32.9 (90.3)	27.6 (26.6)	0.66
最大クリック深度	6.87 (6.01)	7.76 (8.15)	7.77 (8.15)	0.98
ページ閲覧数	2.88 (2.10)	3.16 (2.25)	3.25 (2.19)	0.23
拡張された検索結果の閲覧数	1.21 (1.26)	1.28 (1.29)	1.54 (1.26)	*
拡張されていない検索結果の閲覧数	1.66 (1.34)	1.88 (1.59)	1.70 (1.48)	0.50

う点で，実験協力者は RatioUI は ControlUI よりも有用性が低いと感じていることがわかった（Q1）．この結果は RatioUI が ControlUI に比べて，ウェブ検索におけるプライバシリスクへの意識をより高めていることを意味している．プライバシリスクのある検索結果を回避する上では，RatioUI は IconUI に比べて有用性が低いと評価された（Q2）．また，トラッカーが含まれている検索結果の見つけやすさ（Q2），プライバシリスクのある検索結果の避けやすさ（Q4），表現のわかりやすさ（Q7），利用したいかどうか（Q8) の観点で ControlUI の方が RatioUI よりも高い評価を得ていることがわかった．

これらの結果から，SERP 上の各ウェブ検索結果にトラッカーが含まれているかどうかを評価する上で，RatioUI と比較して ControlUI はウェブ検索ユーザにとってより便利で使いやすいものになると考えられる，ControlUI は，ウェブページのトラッキングの可能性をウェブ検索ユーザに伝えるだけで，データ漏洩先の範囲などの追加情報を提示しない．したがって，ControlUI は RatioUI に比べて単純である．このことが実験協力者の印象を良くしたと考えられる．

IconUI と RatioUI は，ControlUI と同じように慎重にウェブ検索結果のリストを探索することを促すと予想した．しかし，プライバシ保護のための慎重なウェブ検索に対する実験協力者の行動に関して，ControlUI，IconUI，RatioUI の間に有意な差は見られなかった（SERP での滞在時間，最初のクリックまでの時間，最大クリック深度，総閲覧数など）．したがって，H2 は支持されないと結論づけた．

ウェブページのトラッキング可能性を明らかにするという点では ControlUI の方が有用であると評価された．一方で，行動データの漏洩の程度を把握するという点では，IconUI と RatioUI の方が高い評価を得た（Q3；5.1 節）．この結果から，IconUI と RatioUI は，ウェブ検索ユーザが潜在的な漏洩先を知るために有用であることがわかる．しかし，ControlUI と比較して，この 2 つの UI は，トラッカーが設置されたウェブページの見つけやすさの点でやや劣ることがわかった．

また，行動分析の結果 RatioUI を利用した実験協力者は ControlUI よりもトラッカーが埋め込まれた検索結果を積極的に閲覧する傾向が見られた（表 5 の「拡張された検索結果の閲覧数」を参照）．一方，トラッカーが付いていない検索結果の閲覧数（表 5 の「拡張されていない検索結果の閲覧数」を参照）については，3 つの UI の間に有意な差は見られなかった．これらの結果から，RatioUI を使用した実験協力者は，トラッキングリスクのあるウェブページを意図的に多く閲覧できたと考えられる．つまり，RatioUI は ControlUI と比較して，検索結果のリストを見ながら，トラッキングリスクとウェブページ閲覧のメリットのトレードオフを考えることを実験協力者に促すことができたと考えられる．

行動分析の結果，IconUI は RatioUI と同様の効果がみられなかった．その原因として，以下のことが考えられる．IconUI では流出先の例が示されたが，一部の実験協力者にとってはそれらのウェブサイトが馴染みのないものであった可能性が存在する．一方，RatioUI では，流出先のウェブサイトがカテゴリ別に表示されていた．RatioUI では，検索結果の閲覧履歴がどのようなウェブサイトに流出するのか，具体的な情報がなくても想像することが可能だった．そのため，IconUI は RatioUI に比べてユーザの行動に影響を与えないことが考えられる．

6.1 結　　論

以上のことから，主観アンケートでは，ウェブ検索における閲覧履歴の漏洩先を把握するという点で，RatioUI が有用であることがわかった．行動分析では，RatioUI がタスクに役立つ情報を得るために，トラッキングリスクのあるウェブページの閲覧を促していることが分かった．このように，ウェブ検索者が SERP 上の閲覧履歴の流出先のカテゴリで閲覧履歴の流出数を知ることができれば，トラッキングリスクを効果的に検討させることが可能となる．

6.2 研究の限界点

本研究の限界は，トラッカーや閲覧履歴の流出先の検出に関するものである．提案システムでは，検索結果にトラッカーが含まれているかどうかを判断するためにサードパーティクッキーを使用した．サードパーティクッキーへの規制は強まっており，ブラウザフィンガープリントなど他の方法が普及しつつある．本研究では，プライバシリスクの表現に焦点を当てており，提案した UI はトラッカーの検知方法に依存しないが，今後は最新のトラッキング技術を用いて閲覧履歴の漏洩を検知する効果的な方法を検討する予定である．

第二に，トラッキングの目的の特定に関するものである．ユーザ実験で使用したシステムでは，トラッカーが含まれているウェブサイトは，広告代理店と閲覧履歴を共有することを前提とした．しかし，ウェブサイトによっては，アクセス解析のた

めだけにトラッカーを利用している場合も存在する．したがって，ウェブページのプライバシリスクの程度を把握するためにトラッキングの目的を特定する必要がある．

第三に，実験協力者の募集条件である．本研究ではクラウドソーシングサービスを利用し，提案インタフェースがウェブ検索ユーザのプライバシ意識や行動にどのような影響を与えるかを調査した．しかし，提案したシステムを使用している間実験協力者が何を考えていたかについては詳細に調査していない．オンラインでの調査のみでは，プライバシの理解度を検証することは困難であるため，今後はより効果的な分析のために実験室での研究を行う必要がある．

7 まとめ

本稿では，ウェブ検索中のユーザのプライバシリスクへの意識づけを支援するウェブ検索インタフェースを提案した．提案インタフェースは，ウェブ検索結果のリンク先と，ユーザが過去に閲覧したウェブページに含まれるサードパーティクッキーを比較し，第三者に知られる可能性のある閲覧履歴の具体例を表示する．提案インタフェースが，ウェブ検索ユーザのプライバシリスクへの意識づけを高めることができるかを評価するため，ユーザ実験を行った．実験の結果，提案システムは，単純な警告のみを表示するインタフェースよりも，閲覧履歴の漏洩を知る上で効果的であると評価された．今後は計測する情報などの実験設計を見直した上で再度実験を行い，提案手法を表示した際のユーザの検索行動の理解を深める必要がある．

謝　辞

本研究は JSPS 科研費 JP18H03244，21H03554，21H03775 の助成を受けたものです．ここに記して謝意を表します．

文　献

[1] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. Smart, useful, scary, creepy: Perceptions of online behavioral advertising. In *Proceedings of the 8th USENIX Symposium on Usable Privacy and Security (SOUPS 2012)*, pp. 1–15, 2012.

[2] Farah Chanchary and Sonia Chiasson. User perceptions of sharing, advertising, and tracking. In *Proceedings of the 11th USENIX Symposium On Usable Privacy and Security (SOUPS 2015)*, pp. 53–67, 2015.

[3] Steven Englehardt and Arvind Narayanan. Online tracking: A 1-million-site measurement and analysis. In *Proceedings of the 2016 ACM Conference on Computer and Communications Security (CCS 2016)*, pp. 1388–1401, 2016.

[4] Arunesh Mathur, Jessica Vitak, Arvind Narayanan, and Marshini Chetty. Characterizing the use of browser-based blocking extensions to prevent online tracking. In *Proceedings of the 14th USENIX Symposium on Usable Privacy and Security (SOUPS 2018)*, pp. 103–116, 2018.

[5] Joshua Gluck, Florian Schaub, Amy Friedman, Hana Habib, Norman Sadeh, Lorrie Faith Cranor, and Yuvraj Agarwal. How short is too short? implications of length and framing on the effectiveness of privacy notices. In *Proceedings of the 12th USENIX Symposium on Usable Privacy and Security (SOUPS 2016)*, pp. 321–340, 2016.

[6] Steven Englehardt, Dillon Reisman, Christian Eubank, Peter Zimmerman, Jonathan Mayer, Arvind Narayanan, and Edward W. Felten. Cookies that give you away: The surveillance implications of web tracking. In *Proceedings of the 24th International Conference on World Wide Web (WWW 2015)*, pp. 289–299, 2015.

[7] Timothy Libert and Reuben Binns. Good news for people who love bad news: Centralization, privacy, and transparency on us news sites. In *Proceedings of the 10th ACM Conference on Web Science (WebSci 2019)*, pp. 155–164, 2019.

[8] Gunes Acar, Christian Eubank, Steven Englehardt, Marc Juarez, Arvind Narayanan, and Claudia Diaz. The web never forgets: Persistent tracking mechanisms in the wild. In *Proceedings of the 2014 ACM Conference on Computer and Communications Security (CCS 2014)*, pp. 674–689, 2014.

[9] Antoine Vastel, Pierre Laperdrix, Walter Rudametkin, and Romain Rouvoy. Fp-stalker: Tracking browser fingerprint evolutions. In *Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP 2018)*, pp. 728–741, 2018.

[10] Luis A. Leiva, Ioannis Arapakis, and Costas Iordanou. My mouse, my rules: Privacy issues of behavioral user profiling via mouse tracking. In *Proceedings of the 2021 ACM Conference on Human Information Interaction and Retrieval (CHIIR 2021)*, pp. 51–61, 2021.

[11] Joseph Phelps, Glen Nowak, and Elizabeth Ferrell. Privacy concerns and consumer willingness to provide personal information. *Journal of public policy & marketing*, Vol. 19, No. 1, pp. 27–41, 2000.

[12] Hamza Harkous, Kassem Fawaz, Rémi Lebret, Florian Schaub, Kang G. Shin, and Karl Aberer. Polisis: Automated analysis and presentation of privacy policies using deep learning. In *Proceeedings of 27th USENIX Security Symposium (USENIX Security 2018)*, pp. 531–548, 2018.

[13] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. *Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach*, pp. 1573–1582. 2010.

[14] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. Ask the experts: What should be on an iot privacy and security label? In *Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP 2020)*, pp. 447–464, 2020.

[15] Steven Zimmerman, Alistair Thorpe, Chris Fox, and Udo Kruschwitz. Privacy nudging in search: Investigating potential impacts. In *Proceedings of the 2019 ACM Conference on Human Information Interaction and Retrieval (CHIIR 2019)*, pp. 283–287, 2019.

[16] Yang Wang, Pedro Giovanni Leon, Kevin Scott, Xiaoxuan Chen, Alessandro Acquisti, and Lorrie Faith Cranor. Privacy nudges for social media: An exploratory facebook study. In *Proceedings of the 22nd International Conference on World Wide Web (WWW 2013)*, pp. 763–770, 2013.

[17] Yang Wang, Pedro Giovanni Leon, Alessandro Acquisti, Lorrie Faith Cranor, Alain Forget, and Norman Sadeh. A field trial of privacy nudges for facebook. In *Proceedings of the 2014 ACM Conference on Human Factors in Computing Systems (CHI 2014)*, pp. 2367–2376, 2014.

[18] Timothy Libert. Exposing the hidden web: An analysis of third-party HTTP requests on 1 million websites. *International Journal of Communication*, pp. 1–10, 2015.

[19] David Thissen, Lynne Steinberg, and Daniel Kuang. Quick and easy implementation of the benjamini-hochberg procedure for controlling the false positive rate in multiple comparisons. *Journal of educational and behavioral statistics*, Vol. 27, No. 1, pp. 77–83, 2002.