情報処理学会論文誌 Vol.59 No.9 1689–1698 (Sep. 2018)

オンラインオークションにおける購入履歴漏洩のリスクとユーザ認識の調査

長谷川 彩子[1,a)] 秋山 満昭[1] 八木 毅[1] 森 達哉[2]

受付日 2017年12月12日, 採録日 2018年6月8日

概要：オンラインでの商品の購入履歴情報は，ユーザの属性を示唆するプライバシ情報を含む．このため，多くのオークションサイトでは，ユーザの購入履歴情報の漏洩を防ぐために，落札者の仮名表示などのプライバシ保護メカニズムを備えた相互評価システムを運用している．しかし先行研究により，特定のオークションサイトにおいて標的ユーザの購入履歴を推測する攻撃が可能であることが示された．本稿では，より強いプライバシ保護メカニズムを備えるオークションサイトにおいても購入履歴推測攻撃が可能であるかを確認するため，標的ユーザの評価スコアと仮名の出現率を用いたより汎用性の高い推測手法を提案した．実サービスでの実験の結果，97.2%のユーザの購入履歴の推測が可能であった．このような脅威がある現状において，オークションユーザに対してプライバシに関する意識調査を実施した．この結果，自身の購入履歴が第三者に閲覧されると困ると答えた回答者が一定数存在し，その多くが，自身の購入履歴が漏洩しうる状態にあることを認識していないことが明らかになった．これらの結果から，オンラインオークションで発生しうる潜在的なプライバシ問題とユーザの認識に差異があることが判明した．最後に，これらの事実に基づき，オークションユーザとサービス提供者が実施可能な対策を検討した．

キーワード：ユーザブルプライバシ&セキュリティ，オンラインオークション，購入履歴情報

A Study of Purchase History Leakage on Auction Sites and Users' Expectations

Ayako Hasegawa[1,a)] Mitsuaki Akiyama[1] Takeshi Yagi[1] Tatsuya Mori[2]

Received: December 12, 2017, Accepted: June 8, 2018

Abstract: An online purchase history is privacy-sensitive information which indirectly indicates who he/she is. To protect buyers from the leakage of their purchase histories, online auction sites have adopted some form of privacy protection mechanisms such as anonymization of buyers' ID. However, Minkus et al. have demonstrated it's possible to reconstruct an online purchase history on a specific online auction site. In this paper, we extend their work and demonstrate that a purchase history attack can also work for other auction sites with more powerful privacy protection mechanism. In our experiment on an actual auction site, we confirmed that our extended attack is able to reveal 97.2% of users' online purchase histories. Additionally we study users' expectations regarding their privacy on online auction sites and reveal that many users aren't aware of the possibility of the leakage of their purchase histories. This result indicates there is a discrepancy between the potential privacy risk in online auction sites and users' expectations. Finally we make recommendations towards better privacy for auction users and service providers respectively.

Keywords: usable privacy and security, online auction, purchase history

1. はじめに

オンラインオークションのユーザ数は増加の傾向にあり，世界で最も有名なオークションサイトである eBay のアクティブユーザ数は 2017 年現在で 1.7 億人にまで増加してい

[1] NTT セキュアプラットフォーム研究所
NTT Secure Platform Laboratories, Musashino, Tokyo 180–8585, Japan
[2] 早稲田大学
Waseda University, Shinjuku, Tokyo 169–8555, Japan
[a)] hasegawa.ayako@lab.ntt.co.jp

る [1], [2]．オンラインオークションでは，ユーザである出品者と落札者の相互評価に基づいてユーザ間の信頼が形成されることにより，Consumer to Consumer（C2C）の取引が促進されている．オンラインオークションにおいて，相互評価における透明性を担保する仕組みとして，ユーザの評価や取引履歴の多くを閲覧できるサービスが普及している．取引を行ったユーザは，取引完了時に取引相手に対し，その取引内容に応じてポジティブ/ネガティブな評価を相互に付与する．過去の取引相手から付与された評価は，将来の取引に際して相手が信用できるユーザであるかを互いに判断する重要な指標として用いられる．この相互評価システムには，取引に関する具体的な情報として，評価コメント，取引された商品，出品者，落札者などの情報が含まれる．このため，オンラインオークションのサービス提供者は，ユーザの購入商品情報の漏洩を防ぐためにシステムに様々な対策を実施している．たとえば，取引された商品の情報は，出品者の評価ページには表示されるが，落札者の評価ページには表示されないことが多い．さらに，出品者の評価ページでは落札者のユーザ名が仮名で表示されるため，商品を購入したユーザを直接特定することができない．

しかし Minkus らによって，相互評価システムに含まれる断片的な情報を統合することにより，eBay において標的ユーザの購入履歴を推測する購入履歴推測攻撃が可能であることが示された [3]．さらに，eBay のユーザ名と SNS（たとえば，Facebook などの実名サービス）のユーザ名が類似もしくは一致する場合が多いことが確認され，オンラインオークションでの購入履歴と実名を紐付けるアカウントリンク攻撃が可能であることが示された．ただし，Minkus らの攻撃手法は，相互評価システムの仕様変更により現在の eBay では攻撃成功率は低下する．

本稿では，eBay よりも強いプライバシ保護メカニズムを備えるオークションサイトにおいても購入履歴推測攻撃が可能であるかを確認するため，標的ユーザの評価スコアと仮名の出現率を用いたより汎用性の高い推測手法を提案した．実サービスにおける実験の結果，97.2%のユーザの購入履歴の推測ができることが明らかになった．このような脅威がある現状において，我々はさらにオンラインオークションユーザのプライバシ意識を把握するためのアンケート調査を実施した．その結果，“自身の購入商品が第三者から閲覧されたら困る” と答えた回答者が約 36%おり，その多くが，“自身の購入商品が第三者から閲覧されうる状態にある” という認識がないままサービスを利用していることが明らかになった．つまり，オンラインオークションで発生しうる潜在的なプライバシ問題とユーザの認識に差異があることが判明した．このような事実に基づいて，オークションユーザとサービス提供者が実施可能な対策を検討した．

2. 背景

2.1 オンラインオークション

オンラインオークションは，サービス上でユーザ登録を行うと誰でも商品の出品/落札を行うことができる，C2C のビジネスとして成立している．オンラインオークションにおける取引の一般的な流れを以下に示す．

(1) 出品者が開始価格，終了時間などを設定し出品する．
(2) 購入を希望するユーザは開始価格以上で入札を行う．
(3) 終了時間で最高価格で入札したユーザが落札者となる．
(4) 落札者は出品者との間で任意の方法により決済を行う．
(5) 出品者は落札者の支払いを確認し，商品を発送する．
(6) 落札者が商品の到着を確認し，取引が完了する．
(7) 出品者および落札者は任意でお互いへの評価を付与する．

オンラインオークションの特徴の 1 つである相互評価システムは，出品者と落札者が取引完了時に相手への評価を付与するシステムであり，取引に際して相手が信用できるユーザであるかを互いに判断する重要な指標として用いられている．落札者は出品者の商品の品質や発送の早さなどを振り返り，また出品者は落札者の支払いの早さなどを振り返り，取引相手にポジティブ/ネガティブな評価コメントを付与できる．このようにして付与された過去の取引における評価に基づいて，各ユーザには評価スコアが付けられる[*1]．各ユーザの評価スコアや過去の評価情報（評価コメントなど）は，各ユーザのプロフィールページに記載され，第三者が自由に閲覧できる．商品の購入を検討しているユーザは，出品者の評価スコアや過去の評価情報を参考にして，信用できる出品者であるかを判断する．また，出品者は，入札者の評価スコアや過去の評価情報を見て，取引を行いたくないと判断した場合には，入札の取り消しを行える．

2.2 購入履歴情報とプライバシリスク

オンラインサービスにおける商品の購入履歴情報には，ユーザの属性（年代，性別，職業，趣味趣向，家族構成，健康状態など）を間接的に表す様々な情報が含まれる．一般的な Business to Consumer（B2C）のオンラインショッピングでは，個人の購入履歴情報が第三者から閲覧されることはない．しかし，Minkus らは，特定のオンラインオークションにおいては，相互評価システムに含まれる評価情報を分析することで，個人の購入履歴情報を第三者が推測する購入履歴推測攻撃が可能であることを明らかにした [3]．

悪意のある第三者によってオンラインオークションのユーザ名とそのユーザの購入履歴が紐付いた際に，様々な

[*1] たとえば，ポジティブな評価コメントが付くと加算され，ネガティブな評価コメントが付くと減算され，評価スコアが算出される．

プライバシリスクが発生すると考えられる．

(1) アカウントリンク攻撃：インターネットユーザは様々なオンラインサービスにおいて自身のアカウントを保有しており，異なるサービス間で同一もしくは類似のユーザ名を利用するユーザも多い．オンラインオークションのユーザ名と同一もしくは類似のものが他のサービスに存在した場合に，サービスをまたがって同一ユーザであることを特定するアカウントリンク攻撃が可能である [12]．特に，eBay のユーザ名のうち Facebook のユーザ名として存在するものが約 17%あることが知られている [3]．

(2) 標的型攻撃：購入履歴に基づいて標的ユーザに対して注意を引く内容のメールを送付する標的型攻撃があげられる．通常のオンラインショッピングでは，サービス提供者がユーザの購入情報を管理し，場合によってはサービス内での適切な広告表示に活用している．しかし，オンラインオークションでは，相互評価システムを悪用することでサービス提供者ではない第三者でもユーザの購入履歴情報が入手できる．標的型攻撃を行うにあたって用いる標的ユーザのコンタクト情報は，標的ユーザと取引を行うことや，アカウントリンク攻撃によって特定した別サービスのアカウント情報を参照することで取得できる．

2.3 オンラインオークションのプロフィールページ

世界で最もユーザ数が多いオンラインオークションである eBay をモデルとして，ユーザのプロフィールページを**図 1** に示し，記載内容を下記で説明する．

落札者としての評価欄（図 1（左））
出品者から付与されたユーザの落札者としての評価欄であり，評価コメント，出品者名，出品者の評価スコア，時間情報が記載される．ここで，落札者としての評価欄には購入商品の記載はなく，ユーザのプライバシに配慮がなされている．

出品者としての評価欄（図 1（中央））
落札者から付与されたユーザの出品者としての評価欄であり，評価コメント，商品情報，仮名化された落札者名，落札者の評価スコア，時間情報が記載される．ここでは，落札者のユーザ名が仮名化されていることから，落札者のユーザ名と商品が直接紐付いて表示されないように配慮されている．

他のユーザに付与した評価欄（図 1（右））
自身が他のユーザ（出品者もしくは落札者）に付与した評価欄である．落札者として出品者に評価を付与した場合には，評価コメント，出品者名，出品者の評価スコア，時間情報が記載される．出品者として落札者に評価を付与した場合には，評価コメント，商品情報，仮名化された落札者名，落札者の評価スコア，時間情報が記載される．3.1 節でも言及するが，この評価欄は eBay では存在するが，Taobao や Yahoo!オークションでは存在しない．

2.4 購入履歴推測攻撃（先行研究）

一般的なオンラインオークションにおいて，プロフィールページにはユーザのプライバシを守るメカニズムが備わっており，ユーザが購入した具体的な商品名は記載されておらず，ユーザと購入商品が直接的に紐付かない仕様になっている（2.3 節）．

しかし，このようなプライバシへの配慮がされているオンラインオークションにおいても，相互評価システムに含まれる情報を利用することで標的ユーザの購入商品を推測する購入履歴推測攻撃が可能であることが示されている [3]．この購入履歴推測攻撃の手順を**図 2** に示すとともに下記で説明する．

(1) 標的ユーザ（`john0401`）のプロフィールページにアクセスする．

(2) 落札者としての評価欄にある，標的ユーザに商品を販売した出品者（`XYZxyz`）を取得し，その出品者のプロフィールページを確認する．

(3) 出品者（`XYZxyz`）が他のユーザに出品者として付けた評価の中から，標的ユーザの持つ時間情報（`17/8/5 12:19`）と一致するもの，および，標的ユーザの仮名

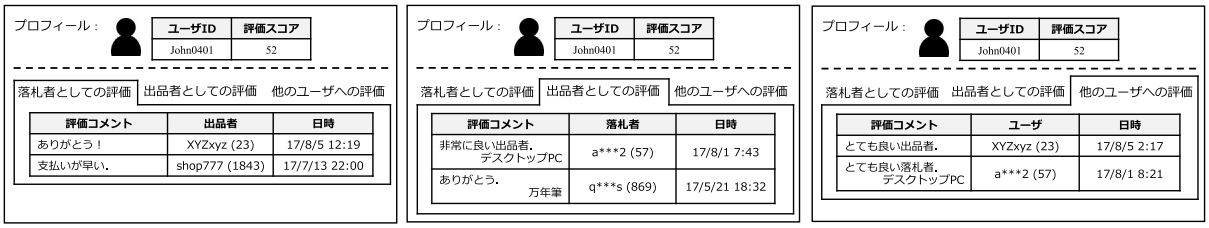

図 1 ユーザのプロフィールページに記載される 3 種類の評価欄（左）出品者から付与された “落札者としての評価欄”，（中央）落札者から付与された “出品者としての評価欄”，（右）当該ユーザが “他のユーザ（出品者もしくは落札者）に付与した評価欄”

Fig. 1 The three types of feedback on profile pages. (Left) Feedback as a buyer, (Center) Feedback as a seller, (Right) Feedback left for others.

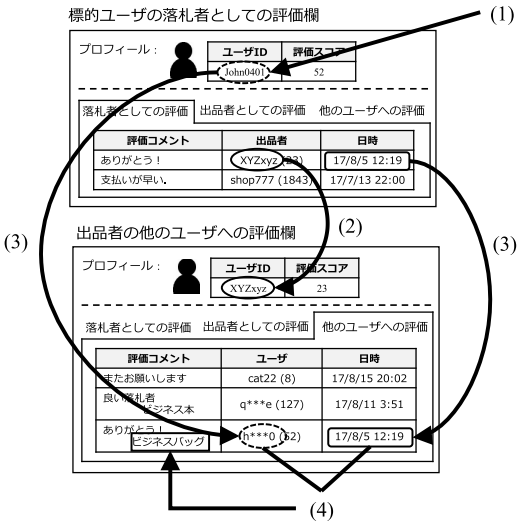

図 2 購入履歴推測攻撃：eBay における標的ユーザの購入商品推測
Fig. 2 Diagram of the purchase history reconstruction attack on eBay.

としてありうるものを探索する．なお，eBay における仮名化は元のユーザ名からランダムに 2 文字抽出してその間にアスタリスク（*）を 3 文字挿入する．よって `john0401` の仮名として `h***0` が予測できる．

(4) 取引の候補が 1 つに絞り込めた場合，その取引における商品が標的ユーザの購入商品（ビジネスバッグ）であると推測する．

手順 (2)〜(4) を標的ユーザの落札者としての評価欄に記載されているすべての取引について繰り返し実施することで，標的ユーザの購入履歴を列挙できる．

3. 購入履歴推測攻撃の改良

3.1 オンラインオークションの比較と攻撃実現可能性

本節では，世の中の主要なオークションサイトの仕様の違いを調査し，購入履歴推測攻撃の実現可能性について検討する．主要なオンラインオークションサービスとその利用者を**表 1** に示す．北米やヨーロッパ各国では eBay が主に利用されており，北米などで用いられる `ebay.com` をはじめとして，ヨーロッパ各国（`.uk`，`.de`，`.fr` などのドメイン）のサイトがある．ただし，アカウントはすべてのサイトで共通的に利用でき，サイトの仕様も同一である．Taobao [5] は主に中国で利用されているが，ユーザ数は世界で最も多い．Yahoo!オークション（以下，ヤフオク！）[4] は日本で最も有名なオンラインオークションであり，ユーザ数も国内のサービスでは最多である．

相互評価システムにおいて，購入履歴の推測に用いられるプロフィールページの情報に基づいて，オークションサービス間の相違点（2017 年 8 月時点）を**表 2** にまとめ，これらに基づき標的ユーザに対する購入商品の推測の難しさを**図 3** に示す．

オークションサービス間において，性質 A：出品者と落札者のリンク，性質 B：ユーザの仮名，性質 C：時間情報，の 3 種類に相違がある．eBay では，あるユーザの “他のユーザ（出品者/落札者）に付与した評価” を閲覧できるため，（性質 A）標的ユーザに付与された “落札者としての評価” は，出品者が “他のユーザ（出品者/落札者）に付与した評価” の中に必ず存在する．この前提に基づいて，（性質 B）元のユーザ名から予測可能な仮名，および（性質 C）時間情報が一致する取引を絞り込むことができる．

一方で，Taobao やヤフオク！では，あるユーザが “他のユーザ（出品者/落札者）に付与した評価” については，そのような評価欄がそもそも存在せず閲覧できない．このため，（性質 A）標的ユーザに付与された “落札者としての評価” と同じ取引を表す評価が，出品者のプロフィールページ内に必ずしも存在するとは限らない．これは，出品者は標的ユーザに評価を付けたものの，標的ユーザが何らかの理由で出品者に評価を付けていない場合があるからである．よって，Taobao とヤフオク！は，落札者（標的ユーザ）が出品者を評価している取引の商品のみが推測攻撃の対象になる．ただし，Taobao の（性質 B）と（性質 C）は eBay と同様のため，標的ユーザに付与された “落札者としての評価” と同じ取引を表す評価が出品者のプロフィールページ

表 1 主要なオンラインオークションサービス
Table 1 Major auction sites.

ユーザ	eBay	Taobao	ヤフオク！
ユーザの多い地域	北米/欧州	中国	日本
ユーザ数	1.7 億人 [2]	4 億人 [10]	1,600 万人 [11]

表 2 オークションサイトのプロフィールページの比較
Table 2 Comparison of profile pages.

性質	eBay	Taobao	ヤフオク！
(A) 出品者と落札者のリンク	完全	不完全	不完全
(B) ユーザの仮名	予測可能	予測可能	予測不可能
(C) 時間情報	一致	一致	不一致

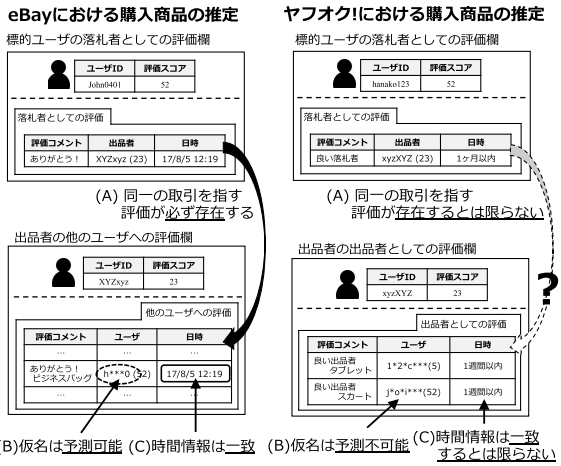

図 3 購入商品推測の困難さ
Fig. 3 The difference between eBay and Yahoo! Auction.

内に存在した場合（つまり，その取引に関して，落札者が出品者を評価した場合）は，購入商品を推測することが可能である．しかしヤフオク！では，標的ユーザに付与された“落札者としての評価”と同じ取引を表す評価が出品者のプロフィールページ内に存在したとしても，（性質 B）標的ユーザの仮名は完全にランダム化されていて元のユーザ名から予測できないものであるうえ，（性質 C）評価を付ける時間は出品者と落札者（標的ユーザ）で異なる場合があるため，標的ユーザの購入商品を絞り込むのは困難である．

これらの観点から，ヤフオク！，Taobao，eBay の順に，プライバシ保護メカニズムが強固であり，購入履歴推測攻撃が成功しにくいことが明らかになった．さらに，2017 年 8 月現在，eBay のプロフィールページの時間表記は相対時間表記（“1 週間以内”，“半年以内”など）に変更されており，2.4 節 (3) において時間情報の一致する取引が多数出現しやすくなることから，現在の eBay の仕様では Minkus らの攻撃手法の攻撃成功率は低下する．

3.2 改良した購入履歴推測アルゴリズム

我々のアイデアは，標的ユーザと過去に取引をした複数の出品者の出品者としての評価欄において，出現率の最も高い仮名を標的ユーザのものであると推測することである．これにより，3.1 節の表 2 で列挙した性質の違いである，取引のエントリの欠損，元のユーザ名から予測不可能な仮名化，時間情報の不一致や相対時間表記に影響されない汎用的な攻撃を実現できる．改良した手法の手順を**図 4** に示す．また，改良手法のアルゴリズムを以下に記す．

(1) 標的ユーザ（`hanako123`）の評価スコアを確認する．
(52)
(2) 標的ユーザに“落札者としての評価”を付与した各出品者のプロフィールページにアクセスする．
(`xyzXYZ`, `55shop`, `catcat`)
(3) 各出品者の“出品者としての評価欄”から，標的ユーザの評価スコアと同じスコアの仮名をそれぞれ抽出する．
(((`h*g*Z***`, `J*Z*Z***`), (`J*Z*Z***`), (`C*w*u***`, `J*Z*Z***`)))
(4) 各仮名の，出品者間の出現率を算出する．出現率の分母は (2) のユーザ数，分子は (3) の出現数とする．
(`h*g*Z***` $= 1/3$, `J*Z*Z***` $= 3/3$, `C*w*u***` $= 1/3$)
(5) 最大出現率の仮名を標的ユーザの仮名として選択する．
(`J*Z*Z***`)
(6) (5) で選択した仮名が購入した商品を抽出し，これらを標的ユーザの購入商品とする．
(ワンピース, タブレット, ランプ)

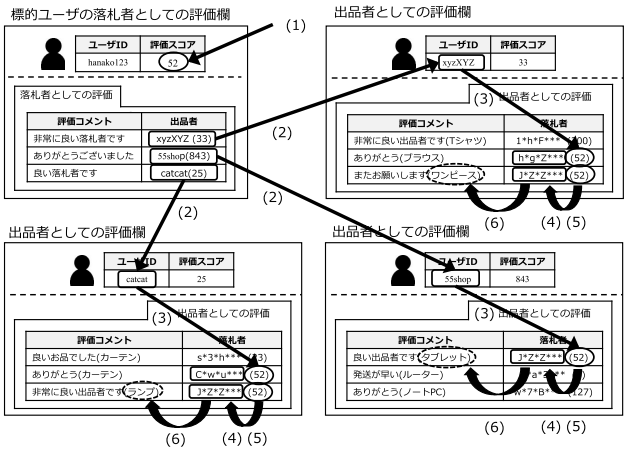

図 4 改良した購入履歴推測アルゴリズム
Fig. 4 Diagram of the extended purchase history reconstruction attack.

3.3 予備実験

提案手法の有効性を確認するために，著者らが所有するアカウントを用いて予備実験を行う．

落札者としての評価数が 2〜6 である 5 つのヤフオク！アカウントに対して改良した購入履歴推測攻撃を実施した．これらのアカウントにおいて，最大出現率を持つ仮名はただ 1 つに絞ることができ（3.2 節の (5)），復元した購入商品はすべて実際に著者らが購入した商品と一致した．これにより，ヤフオク！のように強いプライバシ保護メカニズムを持つオークションサイトであっても，改良手法により購入履歴復元が十分に可能であることを確認した．

3.4 手法の評価

標的ユーザの仮名の特定ができれば標的ユーザの購入商品を特定できる（3.2 節の (6)）ことから，3.2 節の (5) における標的ユーザの仮名推測の精度について評価する．

標的ユーザの仮名推測の精度の指標として，3.2 節 (4) における最大出現率を f_1，2 番目に大きい出現率を f_2 としたときの比率である $s = f_1/f_2$ の値を識別値 s として導入する．s が 1.0 に近い場合は，最大出現率と同程度の出現率を持つ仮名が複数存在することを意味するため，標的ユーザの仮名を単一の候補に特定できない．s が 1.0 に比べて十分に大きいときには，標的ユーザの仮名を単一の候補に特定できる．

実際のオークションサイトにおいて，ある標的ユーザの仮名の出現率を**図 5** に例示する．図 5（左）は，s が 1.0 に近く，標的ユーザの仮名を単一の候補に絞れない場合の 3.2 節 (4) における仮名の出現率のヒストグラムの例である．また，図 5（右）は，s が 1.0 に比べて十分に大きく，標的ユーザの仮名を単一の候補に絞れる場合の，仮名の出現率のヒストグラムの例である．

3.3 節の予備実験において購入履歴復元が成功した 5 つのアカウントの s の値が $s = 2.0, 2.0, 3.0, 3.0, 5.0$ であったことから，本稿では，$s \geq 2.0$ の場合に，最も出現率の高

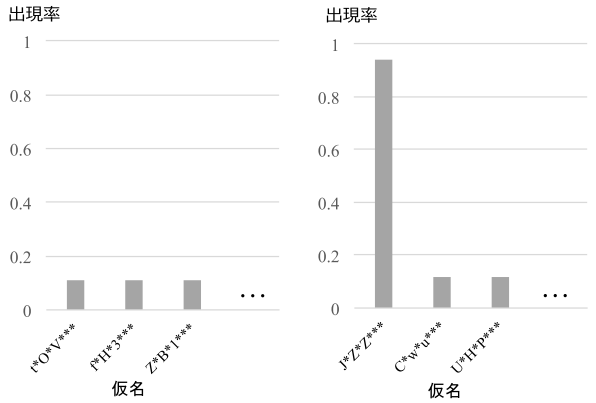

図 5 出現率のヒストグラム（左）標的ユーザの仮名を 1 つに絞れない，（右）標的ユーザの仮名を 1 つに絞れる

Fig. 5 Histogram of the frequency. (Left) the pseudonym is NOT identified uniquely, (Right) the pseudonym is identified uniquely.

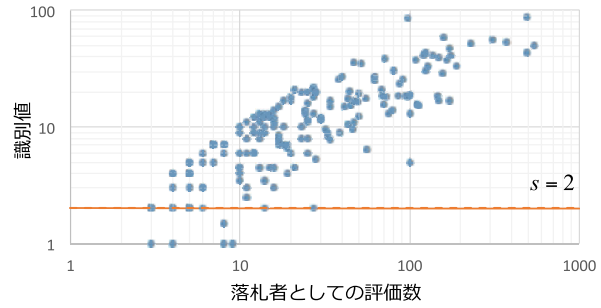

図 6 識別値の分布

Fig. 6 Distribution of the distinguishability score.

い仮名を標的ユーザの仮名として十分に特定できると見なして本実験を行う．

3.5 本実験

評価指標を用いた検証は実際のオンラインオークションで実施する．オンラインオークションの中でも，最もプライバシ強度の高かったヤフオク！に対して実験を行う．ヤフオク！においてランダムで 180 ユーザを抽出し，改良手法による仮名推測を行った．各ユーザが持つ落札者としての評価の数（横軸）と，各ユーザの仮名の識別値 s（縦軸）の分布を**図 6** に示す．97.2%（175/180）のユーザにおいて $s \geq 2.0$ となり，仮名の特定が可能であった．さらに，図 6 から，落札者としての評価の数が多いほど s の値が大きくなる傾向があり，落札者としての評価数が 10 件以上のすべてのユーザで仮名の特定が可能であった．つまり，相互評価システムを積極的に活用して取引を行うヘビーユーザであるほど仮名の特定が容易である傾向にあることが判明した．

3.6 手法の考察と制約事項

従来の購入履歴推測攻撃や我々の改良手法は，出品者と落札者の双方が評価をしていない取引については，相互評価システム上に取引のエントリがそもそも存在しないため，商品の推測ができない．

eBay では，出品者が落札者を評価した段階で，落札者の “落札者としての評価” と，出品者の “他のユーザへの評価” に同じ評価情報が記載される．落札者の行動にかかわらず，落札者と出品者の情報が相互につながり，これにより従来の購入履歴推測攻撃が成立した．

しかし，Taobao やヤフオク！は，“他のユーザへの評価欄” がそもそも存在しないため，落札者が出品者を評価していない取引は，出品者の “出品者としての評価” に当該取引のエントリが存在しない．これが仮名の出現率が低下する要因であり，識別値の低下に影響する．また，他の取引から確率的に標的ユーザの仮名が判明したとしても，前述の商品は特定できない．

ユーザが出品者を評価する頻度が識別値に影響することは前述のとおりである．ユーザがどれくらいの頻度で出品者を評価しているかを直接把握できないため，実際にユーザが落札時にどの程度の頻度で出品者を評価するかをアンケートにより質問した．その結果，“毎回評価する” と回答したユーザが 61.9%存在した．これらのユーザに対しては，必ず取引のエントリが相互評価システム上に存在するため，高い識別値が得られる．このアンケート結果の詳細は 4.1 節に示す．

4. ユーザ認識の調査

相互評価システムに対するユーザの理解度の調査と，購入履歴情報に関する意識調査を実施した．クラウドソーシングサービス [6] を用いて，ヤフオク！を利用したことがある人を対象として募集を行った（2017 年 8 月に実施）．アンケートは 2〜3 分程度で完了する簡易な質問 10 問からなり，報酬 35 円で回答者 350 人を募集したところ，349 人から有効回答[*2]を得た．アンケートでは，回答者の属性（性別・年代など）やサービスの利用頻度（詳細は付録を参照）に加えて，相互評価システムの利用頻度，相互評価システムに関するユーザの理解，購入履歴情報に関する意識の調査を行った．

4.1 相互評価システムの利用頻度

ユーザが相互評価システムをどの程度利用しているかを調査するために，落札時に出品者に対してどの程度の頻度で評価を付与するか質問した．選択肢と回答結果を**表 3** に示す．落札時に出品者に対して毎回評価を付与すると回答したユーザは 61.9%であった．一方で，2 回に 1 回程度かそれ以下のユーザは 14.6%程度であった．これにより，多くのユーザがオンラインオークションにおいて積極的に相互評価システムを活用していることが分かる．

[*2] ヤフオク！の利用頻度を問う質問に対し “1 度も利用したことがない” を選択した 1 人を無効回答として除去した．

表 3 落札時に出品者にどの程度の頻度で評価を付けるか
Table 3 Frequency of leaving feedback for sellers.

毎回（100%）	61.9%
80%～99%	19.8%
60%～79%	3.7%
40%～59%	6.0%
20%～39%	2.0%
～19%	0.9%
1 度もない（0%）	5.7%

表 4 質問 1：自身に付いた評価コメントは誰にまで閲覧される可能性があると思うか
Table 4 Who can see the feedback you received?

誰も閲覧できない	0.9%
自身のみが閲覧できる	3.2%
自身に評価を付けた出品者のみが閲覧できる	4.3%
すべての出品者が閲覧できる	20.3%
アカウントを持つ全員が閲覧できる	37.8%
アカウントの有無にかかわらず誰もが閲覧できる	33.5%

表 5 質問 2：自身の購入商品は誰にまで閲覧される可能性があると思うか
Table 5 Who can see your purchase items?

誰も閲覧できない	2.6%
自身のみが閲覧できる	23.2%
自身に評価を付けた出品者のみが閲覧できる	11.7%
すべての出品者が閲覧できる	13.8%
アカウントを持つ全員が閲覧できる	29.5%
アカウントの有無にかかわらず誰もが閲覧できる	19.2%

4.2 相互評価システムへの理解

ユーザが相互評価システムについてどのように理解しているのかを調査するために，自身への評価および購入商品の閲覧範囲についてどのように考えているのかを質問した．選択肢と回答結果を**表 4** および**表 5** に示す．

質問 1 の正答は “アカウントの有無にかかわらず誰もが閲覧できる” であるが，正しく理解している人は 33.5%であった．また，質問 2 に関しては，表層的には “自身に評価を付けた出品者のみが閲覧できる” のように見えているが，実際には，本稿の改良アルゴリズムのように相互評価システムを悪用することにより，“アカウントの有無にかかわらず誰もが閲覧できる” 状態となりうる．“アカウントの有無にかかわらず誰もが閲覧できる” と答えた人は 19.2%であり，約 8 割のユーザは自身の購入履歴が閲覧されうる状態にあるというプライバシリスクを把握しないままサービスを利用していることが分かった．

4.3 購入履歴のセンシティビティに関する調査

購入履歴情報についてどのように考えているかを調査するため，自身の購入履歴情報が第三者から閲覧されたら困るかどうかを質問した．選択肢と回答結果を**表 6** に示す．

表 6 質問 3：自身の購入履歴情報が第三者から閲覧されたら困るか
Table 6 Do you have a problem if a third party see your purchase items?

まったく困らない	37.2%
どちらかというと困らない	26.9%
どちらかというと困る	27.8%
非常に困る	8.0%

“どちらかというと困る” もしくは “非常に困る” と回答した人は合計 35.8%存在した．これらを回答した人の理由として以下のような意見があげられた．

- 男性，女性のどちらなのか，子供がいるのかなど，大まかにどんな人なのか分かりそうだから．
- 買物情報もプライバシとして保護されるべきだと思うから．
- 購入履歴は個人情報であり，他人に全商品の履歴が見られると詐欺などの犯罪にも巻き込まれかねないと思うから．
- 自身の趣味趣向や購買傾向，家族構成などが不特定多数に分かってしまう可能性があるので怖いと感じる．

商品の購入履歴から，自身の属性（性別，年代，家族構成，職業，趣味趣向など）を推測されうると考えている回答者が多数存在した．また，質問 3 で “どちらかというと困る” ないしは “非常に困る” と回答した人で，質問 2 で “アカウントの有無にかかわらず誰もが閲覧できる” と答えた人は 11.2%のみであった．これらの結果から，購入履歴情報を見られたら困ると感じているユーザが一定数存在するが，彼らのうちの大部分が実際に購入履歴情報を第三者に見られうる状態にあることを認識していないことが判明した．さらに，センシティブなアイテム（医療用品やアダルト商品など）を購入したことがある人は全体の 2%存在した．

5. 考察

5.1 対策

我々が実施したオンラインオークションおよびユーザ認識の調査結果に基づいて，プライバシ保護の観点からユーザおよびサービス提供者が実施可能な対策を検討する．

5.1.1 ユーザ

現状では多くのオークションサイトにおいて本稿で示したような購入履歴推測攻撃が起こりうるため，ユーザ側も注意を払いながら利用するのが望ましい．

購入したことを第三者に知られたくない商品を落札した際は，出品者に評価を付与しないことで回避できる．Taobao およびヤフオク！では，これによって相互評価システム上に当該取引のエントリが掲載されることはない．しかし eBay では，自身が出品者に対して評価を付与するかにかかわらず，出品者が自身に評価を付与した際に，出

品者の “他のユーザへの評価” に当該取引のエントリが掲載される．よって，eBay においては出品者に対して自身への評価を付与しないよう指示することで，自身のユーザ名とその商品が紐付くのを回避できる．

ユーザの認識調査（4 章）では，そもそも自身の購入履歴が第三者に閲覧されうることを認識していないユーザが存在した．また，センシティブな商品を購入するユーザも少なからず存在した．ユーザは，自身の取引情報が第三者に閲覧されうることを認識したうえで取引を行うべきである．また，第三者に購入履歴と実名とを紐付けられると困る場合は，ユーザ名に個人情報（名前・誕生日など）に関する文字列を含めないこと，他の SNS とユーザ名の使い回しをしないことでこのようなリスクを回避できる．

5.1.2 サービス提供者

本稿で示したような購入履歴推測攻撃を実現させない，つまり，落札者とその購入商品が紐付くことを防ぐための対策が必要である．

購入商品名の表示の有無を設定する機能があれば，センシティブな商品の売買において落札者のプライバシを保護することができる．これは eBay において “Private Listing” という機能として出品者が表示の有無を選択できるよう実装されている．これにより，入札前にユーザに選択を与えることができる．しかし，過度に購入商品名の非表示が実施された場合，出品者の出品履歴情報が不足することで，ユーザが入札時に出品者が信用に足るユーザであるか判断ができない可能性がある．

最も有効な対策は “出品者としての評価欄” における落札者の仮名を非表示にすることである．これにより購入履歴推測攻撃の成功率を大幅に低減できる．さらに，“出品者としての評価欄” における落札者の評価スコアの粒度を粗くすることで攻撃成功率をさらに低下させることができる．

5.2 サービスの透明性とユーザのプライバシ保護

オンラインオークションにおいて，サービス提供者は，サービスの透明性を高め，取引におけるユーザ間の信頼を形成するため，相互評価システムにおいて多くの評価情報を公開している．しかし，実験の結果（3.5 節図 6）から，プライバシ保護がなされているオンラインオークションであっても購入商品の推測が可能であり，さらに，落札者としての評価数が多いユーザほど購入履歴復元の攻撃が容易になることが判明した．

プライバシ保護の観点から考えると，利用頻度によらず攻撃を受けにくいような相互評価システムをサービス提供者が構築すべきである．プライバシ保護を強力にするには現在公開されている取引情報などを隠蔽・加工する必要が出てくる．一方で，このような処理を加えることで，相互評価システムの透明性が少なからず低下する．

サービス提供者による過度な情報の制御は，サービスの透明性の低下を招き，ユーザ間の評価情報に基づいて取引を判断するエコシステムが阻害される危険性がある．我々は今後，プライバシ保護のための情報の制御に対するユーザの認識の関係をさらに調査し，透明性とプライバシ保護を高い水準で両立させる手段を検討する予定である．

5.3 研究倫理

本研究は Menlo Report に記載されている研究倫理の原則に基づいて，実験の設計・実施と実験データの管理を行った [7]．オンラインオークションを対象にするにあたり，実際のサービス上での実験を実施した．その際に，ユーザが攻撃に巻き込まれることによる被害が新たに発生しないように配慮した．実験では，特定のアカウントに対する購入商品の列挙はしておらず，また特定のアカウントと他のサービスのアカウントを紐付けることもしていない．またユーザへのアンケートにおいては，個人情報の収集は実施しておらず，回答結果の統計情報を中心に回答者が特定されない形で利用した．

6. 関連研究

6.1 オンラインオークションにおけるトラスト形成

インターネットが普及する以前，オフラインでの商取引における取引相手に対するトラストは，過去の個人的な経験や，人伝てによる評判情報に基づいていた．オンラインでの商取引においては，過去の取引情報や評判情報を可視化し流通させることを担う相互評価システムがトラスト形成を促進しており，オンラインオークションや Q&A フォーラムなどに広く適用されている．Resnick らは，このような相互評価システムが利用者に対して “誰が信頼できるかを判断し，信頼できる行動を助成することを助けるとともに，スキルのないもしくは不誠実なユーザの参加を抑制する効果がある” と論じている [13]．また，文献 [8], [9] では，評価が取引価格に及ぼす影響を分析し，出品者の評価と取引価格に相関がある（たとえば，評価の高い出品者は商品の取引価格が上昇する）ことが示されている．オンラインオークションにおいて，評価情報はトラスト形成と意思決定における重要な役割を果たす一方で，本研究では評価情報の悪用によるプライバシリスクがあることを示した．

6.2 オンラインオークションとプライバシ

オンラインオークションでのユーザの購入履歴情報についての実践的なプライバシリスクの研究は文献 [3] が初めてであり，彼らは eBay において購入履歴推測攻撃が可能であることを明らかにした．我々はこの手法を改良し，より強いプライバシ保護メカニズムを備えるオークションサイトであっても購入履歴推測攻撃が成立することを確かめた．また，Diaz らは，オンラインオークションを含めたオ

ンラインショッピングサービス全般について，購入時，支払時，配達時，購入完了時の 4 つのフェーズにおけるユーザのプライバシ漏洩の脅威をまとめている [14].

7. まとめ

オンラインオークションを特徴付ける相互評価システムはユーザ間の取引を促進する重要な役割を果たしている．相互評価システムに含まれる取引情報は，一方で，ユーザのプライバシに関わるものも含まれている．我々は主要なオンラインオークションに対して汎用性の高い購入履歴推測攻撃が可能であることを実際のサービスを用いて示した．このようなプライバシの潜在的な脅威が存在するにもかかわらず，オンラインオークションにおける購入履歴が第三者から閲覧されると困るとするユーザは約 36%存在した．このように我々の調査によってサービスの実態とユーザの認識に差異があることが判明した．また我々は，この差異を解消するために，ユーザおよびサービス事業者双方に対して実施可能な対策を検討した．

参考文献

[1] eBay, available from ⟨https://www.ebay.com/⟩.
[2] Statista, Number of eBay's active users from 1st quarter 2010 to 2nd quarter 2017 (in millions), available from ⟨https://www.statista.com/statistics/242235/number-of-ebays-total-active-users/⟩.
[3] Minkus, T. et al.: I Know What You're Buying: Privacy Breaches on eBay, *Privacy Enhancing Technologies* (*PETS*) (2014).
[4] ヤフオク！, 入手先 ⟨https://auctions.yahoo.co.jp/⟩.
[5] Taobao, available from ⟨https://www.taobao.com/⟩.
[6] ランサーズ, 入手先 ⟨http://www.lancers.jp/⟩.
[7] Menlo Report, available from ⟨https://www.caida.org/publications/papers/2012/menlo_report_actual_formatted/⟩.
[8] Houser, D. et al.: Reputation in auctions: Theory, and evidence from eBay, *Journal of Economics & Management Strategy*, Vol.15, No.2, pp.353–369 (2006).
[9] Lucking-Reiley, D. et al.: Pennies from eBay: The determinants of price in online auctions, *The Journal of Industrial Economics*, Vol.55, No.2, pp.223–233 (2007).
[10] DMR, 21 Amazing Taobao Statistics (Feb. 2017), available from ⟨http://expandedramblings.com/index.php/taobao-statistics/⟩.
[11] 数字で見るヤフオク！, 入手先 ⟨https://auctions.yahoo.co.jp/topic/promo/infographic/#users⟩.
[12] Perito, D. et al.: How unique and traceable are usernames?, *Privacy Enhancing Technologies* (*PETS*) (2011).
[13] Resnick, P. et al.: Reputation systems, *Comm. ACM*, Vol.43, No.12, pp.45–48 (2000).
[14] Diaz, J. et al.: Privacy Threats in E-Shopping (Position Paper), *International Workshop on Data Privacy Management* (2015).

付　　録

A.1 回答者の内訳

ユーザスタディにおける 349 人の回答者の性別・年代・利用頻度の内訳は以下のとおりである．

表 A·1 回答者の性別
Table A·1 Gender of participant.

男性	44.4%
女性	55.6%

表 A·2 回答者の年代
Table A·2 Age of participant.

10 代	1.1%
20 代	24.9%
30 代	41.5%
40 代	24.6%
50 代以上	6.0%

表 A·3 ヤフオク！の利用頻度
Table A·3 Frequency of use of Yahoo! Auction.

1 週間に 1 回以上	0.9%
1 カ月に 1 回以上	17.2%
半年に 1 回以上	38.7%
それ以下	43.3%

表 A·4 購入したことのある商品（複数選択可）
Table A·4 Which items have you bought on Yahoo! Auction? (Multiple choice).

趣味に関する商品	63.0%
本や映画	36.5%
衣類	26.6%
電化製品	22.3%
生活用品	13.5%
医療用品/アダルト商品	2.0%
その他	11.7%

表 A·5 センシティブな商品（医療用品やアダルト商品など）を買う場所（複数選択可）
Table A·5 Where do you buy the sensitive items (ex: health care items, adult goods)? (Multiple choice).

実店舗	51.3%
オンラインショッピング（オークションを含まない）	43.3%
ヤフオク！	10.9%
ヤフオク！以外のオークション	1.7%
メルカリなどのフリーマーケット	3.2%
その他	3.7%

長谷川 彩子

平成 25 年お茶の水女子大学理学部情報科学科卒業．平成 27 年同大学大学院修士課程修了．同年日本電信電話（株）入社．サイバー攻撃対策技術に関する研究開発に従事．

秋山 満昭 （正会員）

平成 17 年立命館大学理工学部情報学科卒業．平成 19 年奈良先端科学技術大学院大学情報科学研究科修士課程修了．同年日本電信電話（株）入社．平成 25 年奈良先端科学技術大学院大学情報科学研究科博士課程修了．平成 28 年より日本電信電話（株）セキュアプラットフォーム研究所特別研究員．サイバー攻撃対策技術に関する研究開発に従事．工学博士．電子情報通信学会，IEEE 各会員．

八木 毅

平成 12 年千葉大学工学部電気電子工学科卒業．平成 14 年同大学大学院自然科学研究科修士課程修了．同年日本電信電話（株）入社．平成 25 年大阪大学大学院情報科学研究科博士課程修了．平成 26 年より日本電信電話（株）セキュアプラットフォーム研究所主任研究員．サイバー攻撃対策技術に関する研究開発に従事．情報科学博士．電子情報通信学会，電気学会，IEEE 各会員．

森 達哉 （正会員）

平成 9 年早稲田大学理工学部応用物理科卒業．平成 11 年同大学大学院修士課程修了．同年日本電信電話（株）入社．平成 19 年から 20 年にかけて米国ウィスコンシン州立大学マディソン校客員研究員．平成 25 年より早稲田大学基幹理工学部情報通信学科准教授．平成 30 年より同教授．情報セキュリティ・プライバシに関する研究に従事．情報科学博士．平成 21 年電子情報通信学会英文 B 誌論文賞，平成 22 年電気通信普及財団テレコムシステム技術賞受賞．電子情報通信学会，IEEE，ACM，USENIX 各会員．