Computer Security Symposium 2017
23 - 25 October 2017

オンラインオークションにおける プライバシーリスクとユーザ認識の調査

長谷川 彩子[1]　秋山 満昭[1]　八木 毅[1]　森 達哉[2]

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ー情報を含んでいる．このため，多くのオークションサイトでは，ユーザの商品購入履歴の漏洩を防ぐために，プライバシー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．本稿では，プライバシー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，標的ユーザの商品購入履歴の推定が可能であることを示した．また，オークションユーザに対してプライバシーに関する意識調査を実施した結果，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オークションサイトを利用しているユーザが多数存在することが明らかになった．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．

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

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) の売買が促進されている．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，ユーザの評価や売買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て，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，購入商品，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．例えば，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匿名化されているため，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，オンラインオークションにおいて標的ユーザの購入履歴を推定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，オンラインオークションのユーザ名と SNS(例えば，Facebook など実名サービス) 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 では成立が難しい．

本稿では，オンラインオークションの主要サービスにおける相互評価システムについてプライバシー保護の観点から比較を行い，前述の購入履歴推測攻撃への耐性を評価した．また，eBay よりも強いプライバシー保護メカニズムを備えるサービスに対しても，相互評価システムに含まれる情報を統合した上で確率的に購入履歴推測攻撃が可能であることを確認した．我々の手法は Minkus らの手法よりも汎用性が高く，eBay を始めとする一般的なオンラインオークションにおいて成立する．このような脅威がある現状において，我々はオンラインオークションユーザのプライバシー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ユー

[1] NTT セキュアプラットフォーム研究所
[2] 早稲田大学
E-mail: hasegawa.ayako@lab.ntt.co.jp

ザが多数存在す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ー問題とユーザの認識の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，終了時間等を設定し出品する．
(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の評価を付ける．

オンラインオークションの特徴の一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等を振り返り，また出品者は落札者の支払いの迅速さ等を振り返り，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 (評価コメント等) 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 商品の購入履歴情報とプライバシーリスク

オンラインサービスにおける商品の購入履歴情報には，その人の属性を間接的に表す様々な情報 (年代，性別，職業，趣味趣向，家族構成，健康状態など) 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，個人の購入履歴が第三者から閲覧されることはない．しかし，Minkus らは，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定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，サービスを跨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挙げられる．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

世界でもっと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，落札日時が記載される．ここでは，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ー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，匿名化された落札者名，落札者の評価スコア，落札日時が記載される．ここでは，落札者のユーザ名が匿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

[*1] 例えば，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，スコアが算出される．

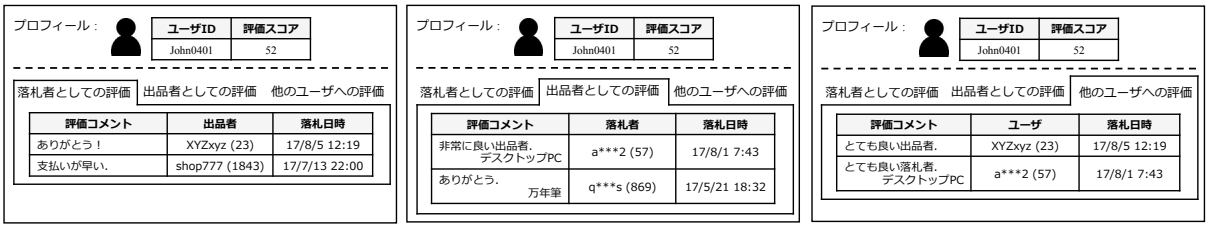

図 1 ユーザのプロフィールページに記載される三種類の評価欄

(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”

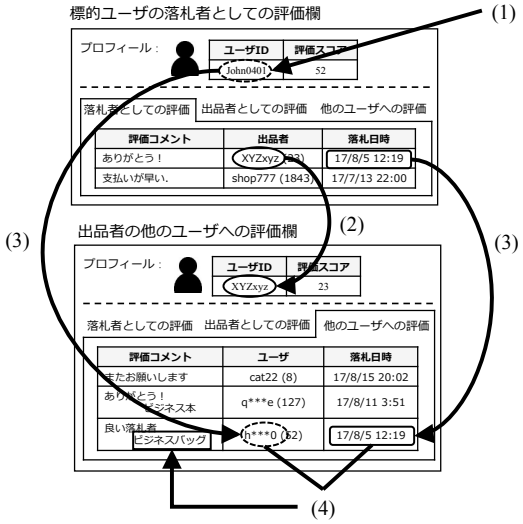

図 2 購入履歴推測攻撃：eBay における標的ユーザの購入表品推測

スコア，落札日時が記載される．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，匿名化された落札者名，落札者の評価スコア，落札日時が記載される．2.5 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

一般的なオンラインオークションにおいて，ユーザのプロフィールページには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ー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の推測が可能である購入履歴推測攻撃が示されている [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，標的ユーザの落札時間 (`17/8/5 12:19`) が一致するもの，および，標的ユーザの匿名としてありうるものを探索する．なお，eBay における匿名化は元のユーザ名からランダムに二文字抽出してその間にアスタリスク (*) を三文字挿入する．よって `john0401` の匿名化ユーザ名として `h***0` が推測できる．

(4) 売買の候補が一つに絞り込めた場合，その売買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) をすべての売買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．

表 1 主要なオンラインオークションサービス

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

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) ユーザの匿名化表示	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

2.5 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，購入履歴の推定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

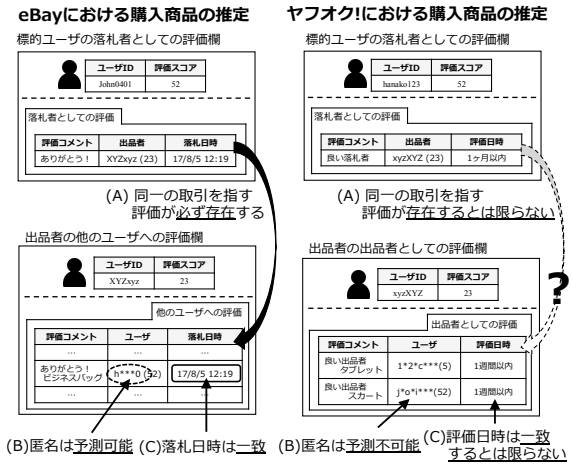

図 3 購入商品推測の困難さ

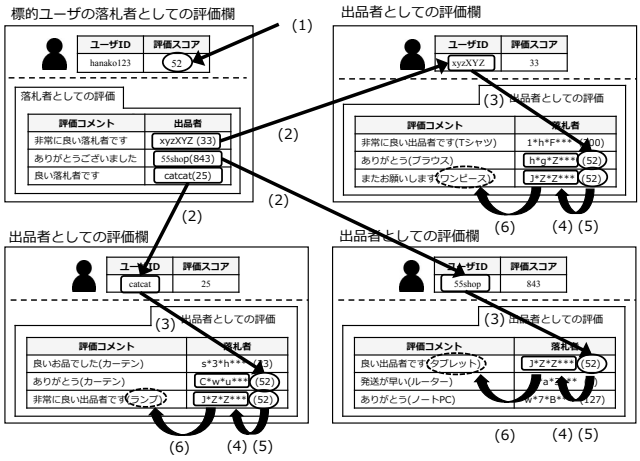

図 4 改良した購入履歴推定アルゴリズム

サービス間の相違点を**表 2** にまとめ，これらに基づいて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：ユーザの匿名化表示，性質 C：時間情報，の三種類に相違がある．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” の中にかならず存在する．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匿名，および (性質 C) 落札時間が一致する売買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内に存在した場合 (つまり，その売買に関して，落札者が出品者を評価した場合) は，購入商品を推定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) 標的ユーザの匿名化表示は完全にランダム化されていて予測できないものである上，(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，プライバシー保護メカニズムが強固であり，購入履歴推定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落札時間は相対時間表記 (“1 週間以内”，“半年以内” など) に変更されており，2.4 節 (3) において時間の一致する売買が多数出現しやすくなることから，eBay においては Minkus らの手法の適用が困難になった．

3. 購入履歴推定攻撃の改良

Minkus らの提案した購入履歴推定攻撃は, eBay, Taobao, ヤフオク！などの主要なオンラインオークションでは成立が困難であることを 2.5 節において示した．特に，ヤフオク！はこれらのオンラインオークションの中で最もプライバシー保護メカニズムが強固であった．

しかし我々は，相互評価システムに含まれる情報を統合することで確率的に購入履歴の推定が依然として可能であることを本節で示す．

3.1 改良した購入履歴推定アルゴリズム

我々のアイデアは，標的ユーザと売買をした出品者に関する過去の売買において，その売買において出現頻度のもっとも高い匿名を標的ユーザのものであると推定することである．これにより，2.5 節の表 2 で列挙した性質の違いである，売買のエントリーの欠損，予測不可能な匿名化，落札時間の不一致や早退時間表記，に影響されない攻撃が実現できる．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`)

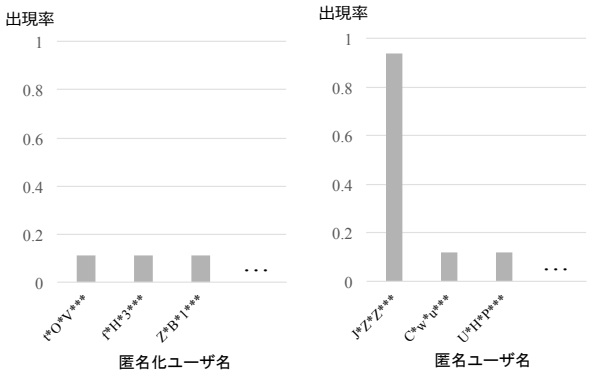

図 5 出現率のヒストグラム．(左) 標的ユーザの匿名を 1 つに絞れない，(右) 標的ユーザの匿名を 1 つに絞れる

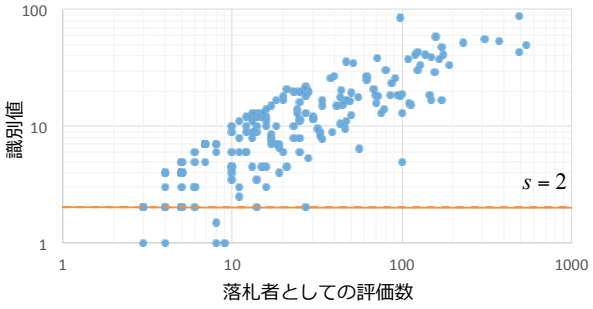

図 6 識別値の分布

(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匿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) 各匿名の，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) 最大出現率の匿名を標的ユーザの匿名として選択する．
(J*Z*Z***)

(6) (5) で選択した匿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)

3.2 手法の評価

標的ユーザの匿名の特定ができれば，一意に購入商品を特定できる (3.1 節の (6)) ことから，3.1 節の (5) における標的ユーザの匿名推定について評価する．

標的ユーザの匿名推定の精度の指標として，3.1 節 (4) における最大出現率を f_1，二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もつ匿名が複数存在することを意味するため，標的ユーザの匿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，標的ユーザの匿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，ある標的ユーザの商品売買における匿名の出現頻度を**図 5** に例示する．図 5(左) は，s が 1.0 に近く，標的ユーザの匿名を単一の候補に絞れない場合の 3.1 節 (4) における匿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，標的ユーザの匿名を単一の候補に絞れるときの，匿名の出現率のヒストグラムの例である．本稿では，$s \geq 2.0$ の場合に，最も出現率の高い匿名が標的ユーザであるとみなす．

3.3 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，最もプライバシー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，改良手法による匿名推定を行った．各ユーザがもつ落札者としての評価の数 (横軸) と，各ユーザの匿名の識別値 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，匿名推定が可能であった．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匿名推定が可能であった．つまり，ヘビーユーザであるほどに匿名の推定が容易である傾向にあることが判明した．

また，改良手法が実際に購入履歴を復元できることを検証するため，著者らが所有する二つのヤフオク！ユーザアカウントに改良手法を適用した．両アカウントについて $s \gg 2.0$ となるような最大出現率をもつ匿名を推定でき，その匿名が購入した商品を復元したところ，実際に著者らが購入した商品と完全に一致することを確認した．

3.4 手法の考察と制約事項

従来の購入履歴推定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ーがそもそも存在しないため，商品の推定ができない．

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．落札者の行動に関わらず，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ーが存在しない．これが匿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匿名が判明したとしても，前

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

毎回 (100%)	61.9%
80%〜99%	19.8%
60%〜79%	3.7%
40%〜59%	6.0%
20%〜39%	2.0%
〜19%	0.9%
一度もない (0%)	5.7%

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通りである．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．これらユーザに対しては，かならず取引のエントリー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．アンケートは 2〜3 分程度で完了する簡易な質問 10 問であり，報酬は 35 円としたところ，349 人から有効回答を得た．アンケートでは，回答者の属性調査 (性別・年代等) 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，二回に一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わかる.

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，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関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巡回することにより，“アカウントの有無に関わらず誰もが閲覧できる”状態となる．“アカウントの有無に関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復元されうる状態にあるというプライバシー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わかった.

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

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%
全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関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

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%
全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関わらず誰もが閲覧できる	19.2%

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

全く困らない	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%

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.

“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挙げられた.

- 男性、女性のどちらなのか，子供がいるのか等大まかにどんな人なのかわかりそうだから.
- 買物情報もプライバシー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わ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

ウントの有無に関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，プライバシー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

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売買のエントリー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関わらず，出品者が落札者に評価を付与した際に，出品者の “他のユーザへの評価”に当該売買のエントリーが掲載される．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を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，自身の売買情報が第三者に閲覧されうることを認識した上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・誕生日等) 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

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ー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．

また，“出品者としての評価欄”における落札者の匿名を非表示にすることで，推測攻撃の成功率を大幅に低減できる．しかし，これも同様に，ユーザ間の信頼性を低下させてしまう恐れがある．入札する側のユーザからすると，出品者の評価の透明性が著しく低下するため，宣伝目的の評価等により不当に高く付与されたものでないかという疑念をもたらしうる．

5.2 サービスの透明性とユーザのプライバシー保護

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 (3.3 節 図 6) から，プライバシー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定が可能であり，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．

プライバシー保護の観点から考えると，利用頻度に依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．プライバシー保護を強力にするには現在公開されている取引情報等を隠蔽・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売買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，プライバシー保護のための情報の制御に対するユーザの売買に関する認識の関係をさらに調査し，透明性とプライバシー保護を高い水準で両立す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．またユーザスタディ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，回答項目の統計情報のみを利用した．

6. 関連研究

6.1 匿名によるオンライン取引

取引相手だけでなくサービスプロバイダからもアイデンティティを隠蔽しつつ商取引を実現する分散型匿名マーケットプレイスが存在する．分散型匿名マーケットプレイスは，ネットワークにおける匿名技術 (Tor や I2P など) や支払いにおける匿名技術 (Bitcoin など) の技術を組み合わせて実現されている．しかしながら，分散型匿名マーケットプレイスには信頼できる相互評価システムの構築などに課題があり，その多くは残念ながらアンダーグラウンド市

場における違法商品の売買に利用されている [8], [9].

6.2 非匿名化

オンラインサービスにおけるユーザの活動はプライバシーを多分に含むため，様々なデータセット (アクセスログや通信パターンなど) からユーザを特定する攻撃に晒されてきた．Wondracek らは，アクセス先 URL の組み合わせから標的ユーザの SNS のアカウントを特定できることを示した [13]．Schuster らは，暗号化された通信経路を用いたとしても，どのビデオコンテンツを閲覧しているかを通信のバースト値のパターンで特定できることを示した [14]．オンラインオークションにおける実践的な非匿名化手法とプライバシーリスクの研究は，文献 [3] が初めてであり，我々はこの手法を改良してより強くプライバシー保護された相互評価システムであっても攻撃が成立することを確かめた．

このような非匿名化攻撃に対して，データの匿名性を保証する手法が提案されている．k-匿名化は，同一の属性を持つデータが k 個以上存在するようにデータセットを加工することで，個人が特定される確率を $1/k$ 以下に低減させる手法である [15].

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売買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売買情報は，一方で，ユーザのプライバシー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ー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 35%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探索を検討した．

謝辞

本研究を進めるにあたり貴重なご意見とアドバイスをいただきましたヤフー株式会社の大神渉様に感謝いたします．

参考文献

[1] eBay, *https://www.ebay.com/*
[2] Statista, Number of eBay's active users from 1st quarter 2010 to 2nd quarter 2017 (in millions), *https://www.statista.com/statistics/242235/number-of-ebays-total-active-users/*
[3] T. Minkus et al, I Know What You ' re Buying: Privacy Breaches on eBay, Privacy Enhancing Technologies (PETS), 2014.
[4] ヤフオク！, *https://auctions.yahoo.co.jp/*
[5] Taobao, *https://www.taobao.com/*
[6] ランサーズ, *http://www.lancers.jp/*
[7] Menlo Report, *https://www.caida.org/publications/papers/2012/menlo_report_actual_formatted/*
[8] N. Christin et al. Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace, WWW Conference, 2013.
[9] K. Soska et al. Beaver: A Decentralized Anonymous Marketplace with Secure Reputation, *https://eprint.iacr.org/2016/464.pdf*
[10] DMR. 21 Amazing Taobao Statistics (February 2017), *http://expandedramblings.com/index.php/taobao-statistics/*
[11] 数字で見るヤフオク！, *https://auctions.yahoo.co.jp/topic/promo/infographic/#users*
[12] D. Perito et al. How unique and traceable are usernames?, Privacy Enhancing Technologies (PETS), 2011.
[13] G. Wondracek et al. A practical attack to de-anonymize social network users. IEEE Symposium on Security and Privacy (S&P), 2010.
[14] R. Schuster et al. Beauty and the Burst: Remote Identification of Encrypted Video Streams, USENIX Security Symposium, 2017.
[15] L. Sweeney. k-anonymity: A model for protecting privacy, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10(05):557570, 2002.

付　　録

A.1 回答者の内訳

ユーザスタディにおける 349 人の回答者の男女比・年代・利用頻度の内訳は以下の通りである．

表 A·1 回答者の男女比

男性	44.4%
女性	55.6%

表 A·2 回答者の年代

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

1 週間に 1 回以上	0.9%
1 ヶ月に 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)

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%