3　インターネット・オークションにおける個人認証制度

インターネット・オークションでは、オークションA社、オークションB社、オークションC社の3社について、個人認証方式およびID・パスワードの不正入手を防ぐための対策に関する調査を行った。

図表 23　インターネット・オークションにおける個人認証方式 1/2

項番	調査項目		オークションA社	オークションB社
1	個人認証方式		ID＋パスワード	ID＋パスワード
2	初回登録時の本人確認		オークションの利用には、会員登録が必須 登録メールアドレスへのメール送付で本人確認 「秘密の質問」と「答え」を登録時に設定 5000円以上の取引には、有料の「プレミアム会員」への登録（決済情報の登録も含む）が必要 オークションに出品するには、配送本人確認への登録が必要	オークションの利用には、会員登録が必須 登録メールアドレスへのメール送付で本人確認 「秘密の質問」と「答え」を登録時に設定 オークションに出品するには、「料金自動引き落としサービス」への登録が必要
3	IDの実体		任意の半角英数字4～31桁 ただし、最初の文字は英字	任意の半角英数字6桁以上 登録メールアドレスをそのままIDとして利用することも可能
4	パスワードの実体	第1パスワード	任意の半角英数字6～32桁	任意の半角英数字6桁以上
		第2パスワード	なし	なし
		第3パスワード	なし	なし
		ワンタイムパスワード	なし	なし
5	パスワード入力が必要な手続き	第1パスワードが必要	オークションサイトへのログイン 入札、出品	オークションサイトへのログイン 入札、出品
		第1～第2パスワードまで必要	なし	なし
		第1～第3パスワードまで必要	なし	なし

図表 24　インターネット・オークションにおける個人認証方式 2/2

項番	調査項目		オークションC社
1	個人認証方式		ID＋パスワード
2	初回登録時の本人確認		オークションの利用には、会員登録が必須 登録メールアドレスへのメール送付で本人確認
3	IDの実体		任意の半角英数字4～20桁 登録メールアドレスをそのままIDとして利用することも可能
4	パスワードの実体	第1パスワード	任意の半角英数字4～20桁
		第2パスワード	なし
		第3パスワード	なし
		ワンタイムパスワード	なし
5	パスワード入力が必要な手続き	第1パスワードが必要	オークションサイトへのログイン 入札、出品 登録情報の変更やシステム利用料の入金の際には再入力
		第1～第2パスワードまで必要	なし
		第1～第3パスワードまで必要	なし

図表 25　インターネット・オークションにおけるID・パスワードの不正入手を防ぐ対策

1/2

項番	調査項目	対策が不十分な場合に想定されるリスク	オークションA社	オークションB社
1	キーロガー等による、キーボード入力履歴、画面情報等の不正入手	ID・パスワードの不正入手、金銭的被害、個人情報漏洩	ソフトウェアキーボードの採用なし	ソフトウェアキーボードの採用なし
2	パスワード入力時の覗き見		●●●●の暗号化表示に対応	●●●●の暗号化表示に対応
3	フィッシングサイト等によるID・パスワードの不正入手		ログインシール（ログイン画面上に設定した任意の文字列または画像を利用者のコンピュータ画面に表示）の導入 画像認証の導入	特になし
4	不適切なID・パスワード設定（IDとパスワードが同一、パスワードが1111等）を悪用した不正入手		簡単に推測されやすいパスワードは登録制限 定期的にパスワードを変更することの利用者への注意喚起	簡単に推測されやすいパスワードは登録制限 定期的にパスワードを変更することの利用者への注意喚起
5	パスワード（またはID）の総当り攻撃		ID、パスワードの一定回数以上の誤入力があると、ログイン画面に画像認証が追加 正しくログインできれば、次回からは通常ログイン	特になし
6	パスワード確認・変更時のなりすまし（他人よる不正なパスワード確認、変更請求等）		IDがわからなくなった場合は、サイト上から生年月日、郵便番号、登録メールアドレスの入力が必要 入力手続き後、登録メールアドレスあてにIDが送付 パスワードがわからなくなった場合は、ID、画像認証、「秘密の質問」の「答え」か登録メールアドレスで本人確認し、サイト上からパスワード再設定	ID、パスワードがわからなくなった場合は、サイトから登録メールアドレスへメールを送付 メールに記載されたURLにアクセスし本人確認できると、画面上にIDが表示され、パスワードの再設定が可能
7	住所変更時のなりすまし		サイト上から手続き可能	サイト上から手続き可能
8	インターネット上の経路における盗聴	ID・パスワードや取引内容の盗聴	SSLの暗号通信方式による通信路の保護	128bit SSLの暗号通信方式による通信路の保護
9	ログイン状態・退席時の他人による操作	他人による不正な振込（金銭的被害）、個人情報漏洩	ログイン時、一定時間以上操作がないと、パスワードの再入力が必要	特になし

図表 26　インターネット・オークションにおけるID・パスワードの不正入手を防ぐ対策

2/2

項番	調査項目	対策が不十分な場合に想定されるリスク	オークションC社
1	キーロガー等による、キーボード入力履歴、画面情報等の不正入手	ID・パスワードの不正入手、金銭的被害、個人情報漏洩	ソフトウェアキーボードの採用なし
2	パスワード入力時の覗き見		●●●●の暗号化表示に対応
3	フィッシングサイト等によるID・パスワードの不正入手		特になし
4	不適切なID・パスワード設定（IDとパスワードが同一、パスワードが1111等）を悪用した不正入手		簡単に推測されやすいパスワードは登録制限 定期的にパスワードを変更することの利用者への注意喚起
5	パスワード（またはID）の総当り攻撃		特になし
6	パスワード確認・変更時のなりすまし（他人よる不正なパスワード確認、変更請求等）		ID、パスワードがわからなくなった場合は、サイトから登録メールアドレスへメールを送付 メールに記載されたURLにアクセスし本人確認できると、画面上にID、パスワードが表示
7	住所変更時のなりすまし		サイト上から手続き可能
8	インターネット上の経路における盗聴	ID・パスワードや取引内容の盗聴	SSLの暗号通信方式による通信路の保護
9	ログイン状態・退席時の他人による操作	他人による不正な振込（金銭的被害）、個人情報漏洩	ログイン時、一定時間（2時間）以上操作がないと、自動的にログアウト

(1) オークションA社

① 個人認証方式

個人認証方式としては、ID（A社 ID）＋第1パスワード（パスワード）が採用されている。

ID となる「A社 ID」は、最初の文字を英字にした 4～31 文字までの英数字となっており、ID 取得時に任意に設定できる。

第1パスワードとなる「パスワード」は、6～32 文字までの半角の英数字、記号の組み合わせで設定する。こちらも、ID 取得時に任意に設定できる。

② 初回登録時の本人確認

オークションの利用には、「A社 ID」の取得が必要となる。ID の取得では「A社 ID」、「パスワード」、「表示名」を任意に設定し、ID やパスワードを忘れた場合の本人確認のために、郵便番号、性別、生年月日、メールアドレス、業種、職種を入力する。

また、「秘密の質問」として、指定された質問（あなたのペットの好物は？ 旅行に行きたい場所は？ 子ども時代のヒーローは？ 嫌いな食べ物は？ 応援しているチームは？ 名前を変えるとしたら何？ 卒業した学校のアイドルは？ よくドライブした場所は？ 一番好きな映画は？）からを 1 つ選択し、「秘密の答え」を登録する。その際に、ID の不正な自動登録を防ぐため画像認証を行う。画像認証では、画像で表示されている少し見えにくい数字を半角で入力する。

4,999 円までの入札は、この設定により可能となるが、5,000 円以上で入札する場合や、特定カテゴリ（自動車車体、トラック車体、バス車体、オートバイ車体、不動産、船体）の商品に入札するには、「プレミアム会員への登録」が必要になる。プレミアム会員は、月額 346 円（税込）の有料サービスで、インターネットで支払手続きや報酬の受け取りができる「A社ウォレット」というサービスに、利用者のクレジットカード等の決済のための情報を登録する必要がある。これにより、支払い情報（クレジットカード番号など）を毎回入力する必要がなくなり、簡単な手続きで購入できるようになる。受取口座情報を登録すれば、対応サービスからの報酬も受け取れる。

出品する場合は、「配送本人確認」という手続きが必要である。出品を希望する利用者には、「A社ウォレット」で登録した住所および氏名宛てに指定配達業者によって暗号を記した配送物が送付され、指定配達業者に本人確認書類を提示の上で配送物が手渡される。利用者は配送物に記載された暗号をサイト上で入力することで、初めて出品が可能となる。

③　パスワード入力が必要な手続き

オークションサービスを利用するには、「A 社 ID」と「パスワード」でログインする。

④　キーロガー等による、キーボード入力履歴、画面情報等の不正入手

パスワード入力時の覗き見を防止するために、入力したパスワードの文字を●●●●のように暗号化表示する技術的対応を行っている。

⑤　フィッシングサイト等による ID・パスワードの不正入手

「ログインシール」は、ログイン画面上に設定した任意の文字列または画像を利用者のコンピュータ画面に表示させる無料のサービスである。ログインしている時は、設定したログインシールが表示されているか確認し、表示されているメッセージや画像、色が利用者の設定したものであれば、正しいサイトにアクセスしていることを確認できる。

⑥　不適切な ID・パスワード設定（ID とパスワードが同一、パスワードが 1111 等）を悪用した不正入手

第三者から推測されやすい文字列を使用しないよう推奨されているが、パスワードの登録に制限はない。

⑦　パスワード（または ID）の総当り攻撃

「A 社 ID」や「パスワード」を間違えるなど、連続してログインに失敗した場合、セキュリティへの配慮からログイン画面に画像認証の数字が表示される。

正しい「A 社 ID」と「パスワード」に加えて、ログイン画面の下の画像内に表示されている数字を半角文字で入力し、ログインが成功すれば、次回からは画像認証の数字は表示されない。

⑧　なりすまし（他人よる不正なパスワード確認、変更請求等）

「A 社 ID」を忘れた場合、パスワード再設定サイトより、本人確認を行うために、登録時に入力した生年月日、郵便番号、登録メールアドレスを入力する必要がある。入力後、登録メールアドレス宛てに、「A 社 ID」が記載されたメールが届く。

「パスワード」を忘れた場合は、「A 社 ID」と画像認証（表示されている画像と同じ英字や数字を半角で入力）、本人確認のための「秘密の質問の答え」か「登録メールアドレス」のいずれかを入力する。本人確認ができた場合は、パスワードの再設定ページが表示され、パスワードを再設定できる。

⑨ 住所変更時のなりすまし

住所変更は、オンライン上で行える。

⑩ インターネット上の経路における盗聴

SSLで、インターネット上の情報を暗号化して送受信している。

⑪ ログイン状態・退席時の他人による操作

利用者になりすましてサービスを悪用することを防ぐために、ログイン後に一定の時間が経過すると、パスワードの再入力を求める仕組みを採用している。

(2) オークションＢ社

① 個人認証方式

個人認証方式としては、ID（ユーザ ID）＋第１パスワード（パスワード）が採用されている。

ID となる「ユーザ ID」は、半角英数字 6 文字以上で、会員登録時に任意に設定できる。ただし、登録メールアドレスをそのままユーザ ID として利用することも可能である。

第１パスワードとなる「パスワード」は、半角英数字 6 文字以上で、会員登録時に任意に設定できる。「ユーザ ID」と同じものは登録できない。

② 初回登録時の本人確認

オークションの利用には、会員登録が必要となる。会員登録には、必須項目として、メールアドレス、「ユーザ ID」、「パスワード」、氏名、氏名フリガナを登録する。必須ではないが、パスワード再設定のための「秘密の質問（両親の結婚記念日、卒業した学校名、好きなチーム名、ペットの名前、両親の旧姓、免許証の下４桁、好きな映画の題名など）」と「答え」も登録できる。最後に、クレジットカード情報を登録して、会員登録が完了する。

オークションに出品するには、料金自動引き落としサービスへの登録が必要となる。

③ パスワード入力が必要な手続き

オークションサービスを利用するには、「ユーザ ID」と「パスワード」でログインする。ログインしていれば、そのまま入札、出品が可能となっている。

④ その他新たな個人認証方式

特になし。

⑤ キーロガー等による、キーボード入力履歴、画面情報等の不正入手

パスワード入力時の覗き見を防止するために、入力したパスワードの文字を●●●●のように暗号化表示する技術的対応を行っている。

⑥ フィッシングサイト等による ID・パスワードの不正入手

特になし。

⑦ 不適切な ID・パスワード設定（ID とパスワードが同一、パスワードが 1111 等）を悪用した不正入手

利用者に対して、定期的にパスワードを変更することや推測しやすいパスワード設定を行わないことなどを注意喚起している。

⑧ パスワード（または ID）の総当り攻撃

特になし。

⑨ なりすまし（他人よる不正なパスワード確認、変更請求等）

「ユーザ ID」、「パスワード」を忘れた場合は、「ユーザ ID の確認・パスワードの再設定ページ」で、会員登録したメールアドレスと氏名を入力すると、メールが送付される。メールに記載されている URL にアクセスして、再度メールアドレスを入力すると、「ユーザ ID」が表示され、「パスワード」を再設定できる。

初期登録時に「秘密の質問」と「答え」を設定している場合は、会員登録したメールアドレスと氏名に加えて、「秘密の質問」に対する「答え」を入力すると、「ユーザ ID」が表示され、「パスワード」が再設定できる。

⑩ 住所変更時のなりすまし

住所、電話番号、メールアドレス、クレジットカードなどの登録情報を変更するには、登録情報の変更ページから手続きを行う。

⑪ インターネット上の経路における盗聴

128 ビット RC4 や 168 ビット Triple-DES など、SSL3 で規定されているすべての暗号化に対応しており、通信内容を保護することができる。クレジットカード番号の入力画面、店舗編集画面や受注確認画面などで対応している。

⑫ ログイン状態・退席時の他人による操作

特になし。

(3) オークションC社

① 個人認証方式

個人認証方式としては、ID（ニックネーム）＋第1パスワード（パスワード）が採用されている。

IDとなる「ニックネーム」は、半角英数字4文字以上20文字以内で、会員登録時に任意に設定できる。ただし、登録メールアドレスをそのままユーザIDとして利用することも可能である。

第1パスワードとなる「パスワード」は、半角英数字4文字以上20文字以内で、会員登録時に任意に設定できる。

② 初回登録時の本人確認

オークションの利用には、会員登録が必要となる。会員登録には「ニックネーム」と「パスワード」を任意に設定し、必須項目として、名前、フリガナ、自宅住所、郵便番号、都道府県、市区郡町村、番地、電話番号、Eメールアドレス、生年月日、性別を入力する。会員登録をすると、登録されたメールアドレスが利用者のアドレスとして正しいのか、メールの送受信が可能かどうかを確認するため、「会員登録確認メール」が送信され、「会員登録確認メール」に記載の確認用のURLをクリックすることで会員登録が完了する。

③ パスワード入力が必要な手続き

オークションサービスを利用するには、「ニックネーム」と「パスワード」でログインする。ログインしていれば、そのまま入札、出品が可能となっている。

登録情報の変更やシステム利用料の入金の際には、再度パスワードを入力する仕組みになっている。

④ その他新たな個人認証方式

特になし。

⑤ キーロガー等による、キーボード入力履歴、画面情報等の不正入手

ソフトウェアキーボードは採用されていない。

パスワード入力時の覗き見を防止するために、入力したパスワードの文字を●●●●のように暗号化表示する技術的対応を行っている。

⑥ フィッシングサイト等によるID・パスワードの不正入手

特になし。

⑦ 不適切な ID・パスワード設定（ID とパスワードが同一、パスワードが 1111 等）を悪用した不正入手

「ニックネーム」、「パスワード」は、現在、ともに 6 文字以上の半角英数字で、それぞれ固有の文字列を登録することとなっている。以前に登録した会員で 5 文字以下のユーザ ID やパスワードを設定されている場合や、ユーザ ID とパスワードを同じ文字列で設定されている場合には、アラームが表示され、変更が必要となる。

⑧ パスワード（または ID）の総当り攻撃

特になし。

⑨ なりすまし（他人よる不正なパスワード確認、変更請求等）

「ニックネーム」や「パスワード」を忘れた場合、会員登録してあるメールアドレスを入力すると、メールアドレス宛にメールが送付される。メールに記載された URL をクリックし、再度メールアドレスを入力すると、登録されている「ニックネーム」、「パスワード」が表示される。

⑩ 住所変更時のなりすまし

住所、電話番号、メールアドレス、クレジットカードなどの登録情報を変更するには、登録情報の変更ページから手続きできる。

⑪ インターネット上の経路における盗聴

サイトの安全性を高めるために、個人情報を送信するページには SSL を採用している。

⑫ ログイン状態・退席時の他人による操作

ログイン後、一定時間（2 時間）ページへのアクセスがない場合、自動的にセッションを切断するためメッセージが表示される。画面の指示に従って、再度ログインする必要がある。