5　オンラインショップにおける個人認証制度

オンラインショップについては、オンラインショップＡ社、オンラインショップＢ社の2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 29　オンラインショップにおける個人認証方式

項番	調査項目		オンラインショップA社	オンラインショップ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		登録メールアドレスへのメール送付、記載のURLにアクセスすることで本人確認 「秘密の質問」と「答え」を登録時に設定	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		メールアドレス または、独立したID	メールアドレス
4	パスワードの実体	第1パスワード	任意の半角英数字6～12桁	任意の半角英数字4～8桁
		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	ショッピングサイトへのログイン チケットの予約、確認、変更 登録情報の変更など	ショッピングサイトへのログイン 購入、確認、変更 決済情報の登録、変更 配送先の登録、変更など
		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 30　オンラインショップにおける ID・パスワードの不正入手を防ぐ対策

項番	調査項目	対策が不十分な場合に想定されるリスク	オンラインショップA社	オンラインショップ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		特になし	画像認証の導入
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		パスワードの一定回数以上の誤入力でサービス停止	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）		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が送付され、メールに記載されたURLにアクセスし本人確認できると、オンライン上でパスワード設定が可能 本人確認のために「合言葉」の入力が必要	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が送付、メールに記載されたURLにアクセスし本人確認できると、オンライン上でパスワード設定が可能 パスワード再設定の際には、画像認証
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	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（30分）以上操作がないと、自動的にログアウト	ログイン時、一定時間以上操作がないと、自動的にログアウト

5.1 オンラインショップ

(1) オンラインショップA社

① 個人認証方式

個人認証方式としては、ID+パスワードが採用されている。

IDは、現在2種類が平行して利用されており、ひとつは、メールアドレスをIDとして利用するタイプである。もうひとつは、独立したIDとなっている。メールアドレスをIDとしている利用者もIDの変更を行うことで、メールアドレスとは異なる独立したIDとすることができる。

また、新規登録の場合は、グループ企業内で利用されている複数のインターネットサービスで使われている個別のIDをひとつにまとめられる「共通のID」を発行した後、ネットショッピングの機能を有効にするための設定（メールマガジンとクレジットカード）を行うという仕組みとなっている。

パスワードは、記号を除く半角・英数6～12文字以内で任意に設定できる。

② 初回登録時の本人確認

会員登録の手続きはインターネットだけで行え、登録後すぐにサービスを利用できる。

まず共通ID取得のための会員登録ページにて、メールアドレスを入力すると、そのアドレスにID取得のメールが送信される。このメールの有効期限は24時間となっている。受信したメールに記載されているURLをクリックすると、個人情報を登録するサイトにアクセスできる。氏名、生年月日、住所、電話番号、自分で設定する「パスワード」、「秘密の質問」とその「回答」を登録すると、「ID」取得できる。「ID」取得完了の際には、登録したメールアドレスにメールが送信される。

続けて、ネットショッピングの新規登録を行う。メールマガジンを配信するメールアドレスと支払いに利用するクレジットカードを登録して完了となる。

会員登録時に本人を確認する書類を求められることはない。

③ パスワード入力が必要な手続き

ログイン時には、「ID」と「パスワード」が必要となる。実際にチケットを購入する際にも、クレジットカードの暗証番号は求められない。ただし、チケットを受け取る際に、利用したクレジットカードをチケット受取機に挿入し、クレジットカードの暗証番号の入力が必要となる。

④ その他新たな個人認証方式の利用

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利用していない。

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

利用者がパスワードを設定する際に、文字数や英数字混在といった制限を行っている

長期間変更されていないパスワードに対するアラーム表示等は行っていない。

⑧ パスワード（または ID）の総当り攻撃

ログイン時に、パスワードを一定回数以上間違えると、ログインできなくなる。

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）

パスワードを忘れた場合は、パスワード再登録を行うと、登録してあるメールアドレスにメールが送付される。そこに記載されている URL にアクセスするとパスワードを再登録することができる。利用者本人である事を確認するために、合言葉の入力を求められる。

⑩ 住所変更時のなりすまし

サイト上から住所変更を行う場合には、ログイン状態であれば、そのまま変更できる。変更後、登録されているメールアドレスに確認メールが送付される。

⑪ インターネット上の経路における盗聴

インターネット上の経路における盗聴を防ぐため、SSL 暗号化通信によりセキュリティ対策を行っている。

⑫ ログイン状態・退席時の他人による操作

ログイン時に、一定時間以上操作がない場合、自動的にログアウトする。時間は約 30 分となっている。

(2) オンラインショップＢ社

① 個人認証方式

個人認証方式としては、ID＋パスワードが採用されている。

「ID」は、メールアドレスをIDとして利用している。

「パスワード」は、記号を除く半角英数字4～8文字以内で任意に設定できる。

② 初回登録時の本人確認

アカウント登録の手続きはインターネットだけで行え、登録後すぐにサービスを利用できる。

アカウント作成時には、氏名、フリガナ、メールアドレス、オプションで誕生日を入力し、任意に設定した「パスワード」も入力する。送付先住所、クレジットカードの情報も入力することで、次回からはIDとパスワードでログインすれば、買い物のたびにクレジットカードや住所等の情報を入力することなく利用できるようになる。

会員登録時に本人を確認する書類を求められることはない。

③ パスワード入力が必要な手続き

ログイン時には、IDとパスワードが必要となる。注文、商品の配送情報の確認、その他アカウント情報の確認の際にも必要となる。

④ その他新たな個人認証方式の利用

パスワード再設定時、画像認証が採用されている。

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利用していない。

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

アカウント作成時に設定するパスワードでは、「1111」「secret」「password」、「letmein」などの推測しやすいパスワードを設定すると「入力されたパスワード

はB社パスワードの最低要件を満たしていません。」とエラー表示され、6文字以上、大文字と小文字を区別したパスワードを要求される。記号の含めたパスワード設定も可能となっている。

長期間変更されていないパスワードに対するアラーム表示等は行っていない。

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）

「パスワード」を忘れた場合は、パスワード再登録を行うと、登録してあるメールアドレスにメールが送付される。メールに記載されたURLからパスワード設定画面にアクセスし、新しい「パスワード」を入力する。再設定完了後、登録してあるメールアドレスに連絡メールが送付される。

「パスワード」再設定の際には、画像認証が導入されており、登録してあるメールアドレスの入力に加えて、画面上に表示されている画像（数字、アルファベット6文字が含まれる）をキーボードから入力させる。

登録してあるメールアドレスが、現在利用していないもの場合には、新しくアカウントを作成する必要がある。

⑩ 住所変更時のなりすまし

サイト上から住所変更を行う場合には、ログインできていれば、そのまま変更できる。

⑪ インターネット上の経路における盗聴

インターネット上の経路における盗聴を防ぐため、SSL 暗号化通信によりセキュリティ対策を行っている。

⑫ ログイン状態・退席時の他人による操作

ログイン時に、一定時間以上操作がない場合、自動的にログアウトする。

⑬ 特記

サイト上からクレジットカード情報を送ることが心配という場合は、画面にはクレジットカードの下 4 けたと有効期限だけを入力する。注文の確定後、カスタマーサービスに電話し、番号の残りの部分を口頭にて連絡すれば、買い物が可能となっている。

5.2 ヒアリング調査（オンラインショップ）

(1) オンラインショップA社

訪問日時：書面による問い合わせ
対応部門：営業部、A社システム関連会社安全対策室

① オンラインショップの概要

A社では、2001年4月に、航空会社、旅行会社と連携し、チケット予約や宿泊、ツアー予約ができるオンラインショップのサイトを開設した。グループ企業内で展開している複数のインターネットサービスのIDをまとめることができる共通サービスは、2008年2月よりサービスを開始している。

2008年11月末時点で、累計会員数は2,967,225名となっており、そのうち、共通サービスIDとの連携会員数は、526,549名となっている。

会員登録数は、右肩上がりで増加しており、1年で50万人近く会員が増えている。1日あたりの平均登録会員数は、ここ1年の傾向では、平均して1,374人が登録を行っている。

図表 31 会員の各マイルストーンに至るまでの会員登録数／日

会員数	達成日	達成に要した年月	1日あたりの平均登録会員数
～100万人	2004年7月2日	約3年2ヶ月	866人
100万人～150万人	2005年12月2日	約1年5ヶ月	969人
150万人～200万人	2007年1月29日	約1年2ヶ月	1,174人
200万人～250万人	2007年12月30日	約11ヶ月	1,497人
250万人～300万人	2008年12月16日	約12ヶ月	1,374人

注:1ヶ月を30.4日で算出。端数切捨て

A社では、チケット申込サービスや国内ツアー予約等の旅に関する予約・申込サービスの企画を担当している。グループ会社の1つが、オンラインショップのサイトの運営・管理を行い、さらにもう1つのグループ会社で、オンラインショップ関連のシステム開発・運営を行っている。

② 利用者層

登録している会員では、30代～40代の男性が最も多くなっている。

③ 新技術への対応

最新のセキュリティ技術の動向については、システムを担当しているグループ

会社にセキュリティを管理している部門があり、そこから入手している。また、セキュリティ専門会社からの情報提供や意見交換も行っている。

新しい技術では、携帯電話からのアクセスの場合には、携帯電話から送出される固有情報に基づいた本人認証を一部取り入れているが、これ以外の携帯トークンや、ドングル（USB 等に接続するハードウェアキー）などについては、現在は検討していない。

利用者から ID やパスワードの不正入手に対する苦情や問合せも特にない。

④ 利用者が安心して利用できる工夫

パスワードの再登録時に合言葉を採用している。パスワード再登録の手続きをサイト上で行う場合、登録したメールアドレス宛に送信されたメールに記載される URL をクリックすることで本人確認している。しかし、これだけでは、サイト上でメール送信の操作した人とメールを受信した人が同一人物であることは確認できないため、合言葉を入力させることで確認を行っている。

推測しやすいパスワード（誕生日、電話番号、1111 など）については、利用者がパスワードを設定する際に、文字数や英数字混在といった条件をつけている。

チケット購入時の決済は、インターネット上では行わず、チケットを窓口等で発券する際に決済する仕組みが取られている。利用者は、窓口等でクレジットカードを提示し、暗証番号を入力すればよい仕組みとなっている。クレジットカードの情報をインターネット上で入力する必要がなく、利用者の安心感にもつながっている。

⑤ 今後の課題

ネットショッピングという販路は、今後も注力していくべき分野であると考えている。今後、新たに開拓していきたい利用者層としては、携帯電話によるサイト利用者が拡大していることから、携帯ユーザのユーザビリティ向上について検討している。

利用者の使いやすさとセキュリティの高さは、二律背反の面もあるが、セキュリティの確保を基本とし、そのうえで利用者の使いやすさを訴求していく。

利用者が安心してサービスを利用できるように、現在も通信には SSL を使用するなど対策を実施しており、今後もできうる限りの対策を実施していく。