4　オンラインゲームにおける個人認証制度

オンラインゲームでは、オンラインゲームA社、オンラインゲーム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 27　オンラインゲームにおける個人認証方式

項番	調査項目		オンラインゲームA社	オンラインゲームB社
1	個人認証方式		ID＋パスワード	ID＋パスワード＋乱数表+ワンタイムパスワード(メール)
2	初回登録時の本人確認		ゲーム利用にはサービス共通アカウントと個別ゲームアカウントの取得が必要 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 有料サービスや個人情報が必要なサポートを利用するには、個人情報(名前・住所)の登録も必要 サービス共通サイトにログインする時は、ID、第1パスワード、第2パスワード 個別ゲームにログインする時は、個別ID、個別パスワード	ゲーム利用にはサービス共通アカウントと個別ゲームアカウントの取得が必要 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 決済方法がクレジットカードの場合、会員登録後、クレジットカード情報を入力 ログイン時は、ID＋第1パスワード、第2パスワード
3	IDの実体		任意の半角英数字4～32桁	登録時に任意に設定
4	パスワードの実体	第1パスワード	登録時に任意に設定	登録時に任意に設定
		第2パスワード	生年月日	4桁のパスワード32セットからなる乱数表の画像データ 記載された数字のうち、指定された枠内の4桁の数字を入力
		第3パスワード	なし	半角英数10桁 有効期限3時間 第3パスワードが必要な場面で、メールアドレスを入力することで送付
		ワンタイムパスワード	なし	第3パスワードがワンタイムパスワード
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	ゲームサイトへのログイン ゲームアカウント取得	第1パスワードだけの手続きはなし
		第1～第2パスワードまで必要	登録情報の確認・更新 個人情報の確認・変更 利用料金の支払い手続きなど	共通サービスへのログイン ゲームへのログイン 決済情報登録
		第1～第3パスワードまで必要	なし	アカウント登録情報変更 パスワードの変更

図表 28　オンラインゲームにおける 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	オンラインゲームA社	オンラインゲーム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		ひらがな認証（画像に表示されたひらがな8の字を入力）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	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	第2パスワードの3回以上の誤入力で、サービス停止 第2パスワードが記載されている「セキュリティカード」の再発行手続きが必要
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、電話による問い合わせが必要 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	パスワードを忘れた場合は、アカウントと登録メールアドレスを入力すると、登録メールアドレスに認証キーが届く その認証キーを入力してパスワード再発行画面へログイン後、新しいパスワードを設定
7	住所変更時のなりすまし		サイト上から手続き可能 本人確認のために第2パスワードが必要	サイト上から手続き可能 本人確認のために第3パスワードが必要
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	特になし	特になし

(1) オンラインゲームＡ社

① 個人認証方式

個人認証方式として採用されているのは、ID（共通サービスの ID）＋第 1 パスワード（共通サービスのパスワード）＋第 2 パスワード（セキュリティパス）となっている。

ID は、個人情報やＡ社が提供する各ゲームをプレイする上で必要な「ゲームアカウント」の情報を一括管理するための「ID」のことで、「ID」登録の際に任意の英数字（4～32 文字まで）で設定することができる。「ID」登録時に送付される登録完了メールにも記載される。

ひとつの「ID」を登録しておけば、以後、各ゲームの「ゲームアカウント」を登録することができる。

第 1 パスワードも、ID 登録の際に任意で設定することができる。

第 2 パスワードとなる「セキュリティパス（本人認証）」は、個人情報の確認・変更や利用料金の支払い手続きなどの際に入力するパスワードで、ID 登録時に入力した生年月日を使用している。

ID とパスワードを取得後に、A 社が提供する各ゲームをプレイするために必要となる「ゲームアカウント」を取得する。これは、利用するゲームごとに作成が必要となる。「ゲームアカウントのパスワード」は、半角英数 8 文字～16 文字以内で設定できる。

② 初回登録時の本人確認

ID 登録するには、登録者が本人であることを確認するため、通常利用しているコンピュータ用のメールアドレスを入力し、認証を行う。入力されたメールアドレス宛に、ID 登録ページの URL が記載されたメールが届く。メールに記載された URL にアクセスすると本人確認が完了でき、ID 登録ページに進むことができる。

ID 登録に必要な情報は、メールアドレス、任意に設定する「ID」、任意に設定する「パスワード」、生年月日を入力する。

その後、「ひらがな認証」（画像に表示されたひらがな 8 文字を入力）、アバター（インターネット上で利用者の分身として表示されるキャラクター）のニックネームと性別を入力する。ニックネーム、性別は、登録した後で変更することはできない。

登録完了後に、登録メールアドレス宛てに「登録完了メール」が届く。

A 社サイトのゲームで利用できるコイン、アバター利用権、Game カフェのゲーム購入などサービス、期間利用権のクレジットカード決済など、その他全ての有

料サービス、個人情報（名前・住所）が必要なサポート、「ID」忘れ、アカウントハッキングの調査などのサービスを利用するには、「ID」の登録とあわせて、個人情報（名前・住所）の登録が必要となる。

③ パスワード入力が必要な手続き

「ID」、「パスワード」でログインすることにより、「アトラクションセンター」が利用できる。「アトラクションセンター」は、提供されている様々なサービスに関する利用状況や利用料金の支払い状況を一元管理できる窓口となっている。

「アトラクションセンター」で、「ID」、「パスワード」などの登録情報の確認・更新、個人情報の確認・変更や利用料金の支払い手続きなどを行うには、本人確認のための「セキュリティパス」が必要となる。

「ゲームアカウント」取得にも、「ID」、「パスワード」でログインすることが必要になる。実際にゲームにログインする時には、「ゲームアカウント」と「ゲームアカウントパスワード」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

利用者が入力したパスワードをセキュリティ保護のため、「●」または「*」で表示している。

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

不正な登録を防ぐために、画像に表示されたひらがな 8 文字を入力させる「ひらがな認証」を導入している。

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

同じ文字が 4 文字以上連続しているパスワード、数字のみのパスワード、英字のみのパスワードは設定することができない。

⑦ パスワード（または ID）の総当り攻撃

特になし。

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）

ID を忘れた場合は、電話による問い合わせが必要になる。

パスワードを忘れた場合は、「パスワード再発行」画面からパスワードを再発行できる。ID と「登録のメールアドレス」を入力すると、「ご本人確認メール」が送信される。再発行の手続きを本人が行っていることの確認が取れ次第、新しいパスワードを再設定することができる。

「ゲームアカウントパスワード」を忘れた場合は、「アトラクションセンター」にログイン後、利用登録をしているゲームの「ゲームアカウント設定」からパスワードを再発行することができる。

⑨ 住所変更時のなりすまし

住所等の登録情報を変更する場合には、「アトラクションセンター」にログインし、登録情報を変更する。その際には、本人確認のための「セキュリティパス」が必要となる。

⑩ インターネット上の経路における盗聴

個人情報の送信を行うページには SSL を採用している。

⑪ ログイン状態・退席時の他人による操作

特になし。

(2) オンラインゲームＢ社

① 個人認証方式

個人認証方式としては、ID（B社アカウント）＋第1パスワード（パスワード）＋第2パスワード（セキュリティカードパスワード）＋第3パスワード（認証キー）が採用されている。

IDとなる「B社アカウント」は、提供する全てのサービスを一つにまとめた総合ゲーム&コミュニティサイトのアカウントで、登録すれば一つのアカウントで全てのサービスを利用することが出来る。

第1パスワードとなる「パスワード」も、ID登録の際に任意で設定する。

第2パスワードとなる「セキュリティパス（本人認証)」は、4桁のパスワード32セットからなる乱数表の画像データで、ゲームにログインする際、セキュリティカードに記載された数字のうち、指定された枠内の4桁の数字を入力することで、アカウントの不正使用を防止することが可能となる。

第3パスワードとなる「認証キー」は、アカウント登録画面にログインするためのパスワードで、入力されたメールアドレスが利用できる状態にあるかを確認するため、入力されたメールアドレスに送付される。半角英数10桁の認証キーの有効期限は3時間で、有効時間が経過した認証キーは利用できないため、3時間を経過した場合は、再発行を行わなければならない。アカウント登録情報変更やパスワードの変更を行う場合は、その都度、新しい認証キーが発行される。

② 初回登録時の本人確認

新規登録の際には、登録画面よりメールアドレスを入力し、入力されたメールアドレスが利用できる状態にあるかを確認するために、そのメールアドレス宛に「認証キー」を送付される。受け取った「認証キー」で、会員登録画面にログインし、必要な情報を入力する。個人情報登録が完了すれば、完了メールが登録したメールアドレスに送付され、「セキュリティカード」が添付される。

決裁に利用する方法がクレジットカードの場合、支払窓口からB社アカウントとパスワードでログインし、クレジットカード情報を入力する。

③ パスワード入力が必要な手続き

個別のゲームを利用するには、「B社アカウント」、「パスワード」、「セキュリティパス（本人認証)」でログインする。

アカウント登録情報変更やパスワードの変更を行う場合は、その都度、新しい認証キーが発行される。

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

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。

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

特になし。

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

パスワードは、キャラクター名やアカウント名から容易に推測ができるパスワードは利用しないよう、また、定期的なパスワードの変更が勧められている。

⑦ パスワード（または ID）の総当り攻撃

「セキュリティパス」を 3 回連続で誤入力した場合は、ゲームにログインできなくなり、「セキュリティカード」の再発行が必要となる。

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）

「パスワード」を忘れた場合は、「マイアカウント」ページから、再発行を行うことができる。アカウントと登録メールアドレスを入力すると、登録メールアドレスに認証キーが届く。その認証キーを入力してパスワード再発行画面へログイン後、新しいパスワードを設定する。

⑨ 住所変更時のなりすまし

「会員情報変更」ページから、住所などの登録情報の変更が行える。アカウントとパスワードを入力すると、登録メールアドレスに「個人情報変更」画面にログインするための認証キーが送信される。メールに記載の「認証キー」を入力し、「個人情報変更」画面から個人情報を変更できる。

⑩ インターネット上の経路における盗聴

登録された個人情報を保護するため、SSL によるセキュリティ及び、TURSTe のライセンシーとして管理を行っている。

⑪ ログイン状態・退席時の他人による操作

特になし。