1.3 ネットバンク

ネットバンクでは、ネットバンクA行、ネットバンクB行の2社について、インターネットバンキングにおける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 15 ネットバンクにおける個人認証方式

項番	調査項目		ネットバンクA行	ネットバンクB行
1	個人認証方式		ID＋パスワード	ID＋パスワード+ワンタイムパスワード(メール)
2	初回登録時の本人確認		口座開設が必要(本人確認書類添付) 初回ログイン時に、ID＋第1パスワード(郵送)＋第3パスワード(郵送)が必要	口座開設が必要(本人確認書類添付) 初回ログイン時に、「支店番号」、「口座番号」、第1パスワード(郵送)が必要で、ID、第2パスワードを登録
3	IDの実体		口座番号とは別の半角数字10桁	任意に設定した半角英数字8～12桁
4	パスワードの実体	第1パスワード	デフォルトでキャッシュカードの暗証番号(半角数字4桁)	半角数字8桁 初回ログイン時に、任意の半角英数字6～12桁に変更
		第2パスワード	初回ログイン時に任意で設定	初回ログイン時に任意で設定する半角数字4～12桁
		第3パスワード	取引用の番号	取引の都度、メールで送信されたセキュリティコードを入力するワンタイム認証
		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	インターネットバンキングへの初回ログイン	インターネットバンキングへのログイン 残高照会
		第2パスワードが必要	インターネットバンキングへの通常ログイン 照会(残高照会、入出金の明細照会、月々の取引明細表、重要通知の一覧)	振込・振替 定期預金取引 外貨預金取引など
		第3パスワードが必要	インターネットバンキングへの初回ログイン 振込(登録済み振込先の削除、振込限度額変更) 定期預金(作成、預入明細照会など) ATM(キャッシュカード暗証番号変更、ATMご利用限度額変更、ATM定期預金解約停止) その他(利用者情報変更、第2パスワード変更、通知メールの受信設定)	IP制限 セキュリティ通知メールの設定変更 定期預金中途解約 モバイルアクセス制限 ログイン制限の一時解除 限度額設定(振込、VISAデビット、ATM出金)

図表 16　ネットバンクにおける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	ネットバンクA行	ネットバンクB行
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（キー配列固定とキー配列を毎回変更が併用）によるパスワード入力手段の提供	セキュリティボード（「数字」と「その数字に対応する英字」の組み合わせを表にしたもの）によるパスワード入力手段の提供
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によるID・パスワードの不正入手		取引や登録情報の変更があった場合、登録メールアドレスに通知	EV SSLサーバ証明書を採用 取引や登録情報の変更があった場合、登録メールアドレスに通知 IP制限サービス（登録したプロバイダ以外からの暗証番号を伴う取引を制限）を提供
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		90日ごとにパスワード変更のアラームを表示 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	パスワードが長期間変更されていない場合にはアラームを表示 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 サービス再開には、サイト上からのパスワード再登録が必要 第1パスワードの入力が必要	パスワードの一定回数以上の誤入力でサービスが一時停止 一時停止後、一定時間経過すると利用可能
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）		第2パスワードがわからなくなった場合は、サイト上から再登録 IDと第1パスワードの入力が必要	IDがわからなくなった場合は、現在利用中のIDを無効化し、支店番号・口座番号、第1パスワードの入力でログインできるように設定可能 パスワードがわからなくなった場合は、電話による手続きが必要
7	住所変更時のなりすまし		テレホンバンキングで本人確認の上、手続き可能 第3パスワードの入力が必要	住所変更は、サイト上で変更した後、本人確認書類を郵送
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	128bit 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	ログイン時に、一定時間以上操作がない場合、自動的にログアウト	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

(1) ネットバンクＡ行

① 個人認証方式

個人認証方式としては、ID（ログインID）＋第1パスワード（キャッシュカード暗証番号）＋第2パスワード（ログオンパスワード）＋第3パスワード（確認ナンバー）が採用されている。

IDとなる「お客さまID」は、半角数字10桁のインターネットバンキング専用の番号で、キャッシュカードの裏面に印刷されている。

第1パスワードとなる「キャッシュカード暗証番号」は半角数字4桁で、口座開設時に銀行より送付される「仮暗証番号のお知らせ」ハガキに記載されている。初回ログイン時に、「仮暗証番号」は変更しなければならない。

第2パスワードとなる「ログオンパスワード」は、インターネットバンキングのログイン時に毎回利用するもので、 初回ログイン時に、「ご利用開始登録」で設定する。

第3パスワードとなる「確認ナンバー」は、インターネットバンキングを利用した取引や変更などを行う際に使用する番号で、キャッシュカードの裏面に印刷されている。

初回ログイン時には、「ご利用開始登録」でインターネットバンキング・モバイルバンキング振込限度額とメールアドレスを登録する。

② 初回登録時の本人確認

インターネットバンキングを利用するには口座開設が必須となっている。口座開設をするには、銀行サイト上で利用者の情報を入力すると、利用者情報が印字された申込書が自宅に郵送される。申込書に捺印し、本人確認書類を添付し、銀行へ返送すると、キャッシュカード、利用ガイドが郵送される。別便で「仮暗証番号のお知らせ」ハガキも自宅に届く。

インターネットバンキングの利用に際しては、はじめに「ご利用開始登録」が必要となる。

③ パスワード入力が必要な手続き

ログイン時には、「お客さまID」と「ログオンパスワード」が必要となる。

また、振込やお届け情報の変更などの際には、「確認ナンバー」で二重の本人確認を行う。

照会（残高照会、入出金の明細照会、月々の取引明細表、重要通知の一覧）はログイン時には閲覧できる。

振込（登録済み振込先の削除、インターネット・モバイルバンキング振込限度

額変更)、定期預金（作成、預入明細照会、満期取扱変更、解約)、ATM（キャッシュカード暗証番号変更、ATM ご利用限度額変更、ATM 定期預金解約停止)、その他（利用者情報変更、「ログオンパスワード」変更、通知メールの受信設定）の取引では「確認ナンバー」が必要となる。

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

インターネットバンキングの安全性を高めるため、「お客さま ID」「キャッシュカード暗証番号」「ログオンパスワード」「確認ナンバー」の入力は、セキュリティキーボードの利用を標準設定としている。数字の配置はログインのたびにランダムな並びとなり、アルファベットの配置は固定となっている。通常のキーボード入力をしたい場合は、セキュリティボードの利用を解除して利用する。

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による ID・パスワードの不正入手

不正取引を直ちに検知するために、振込取引、登録情報の変更などが行われた場合は、登録メールアドレスに通知が送付される。

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

「暗証番号」は、仮暗証番号、現在の暗証番号、同一の数字 4 桁（「0000」、「9999」など)、生年月日（月日・西暦 4 桁）および届け出している電話番号は登録できない。

「ログオンパスワード」では、90 日ごとにパスワード変更を推奨するメッセージが表示される。

「ログオンパスワード」も登録制限があり、届け出している電話番号の中で、連続する組み合わせ（電話番号が「123-4567-8901」の場合、1234567、23456789 など)、生年月日（生年月日が 2007 年 8 月 1 日、平成 19 年 8 月 1 日の場合は、200708、190108 など)、同一数字（1111、2222222 など）が登録できないようになっている。

⑦ パスワード（または ID）の総当り攻撃

誤った「暗証番号」、「ログオンパスワード」、「確認ナンバー」が所定の回数以上繰り返して入力されると失効となる。

「ログオンパスワード」が失効になった場合は、インターネットバンキングのログイン画面の下方にある「ログオンパスワードが失効となった方」ボタンから「ログオンパスワード」の再登録を行うことで、サービスを再開できる。その際

には、「お客さまID」と「暗証番号」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）

「ログオンパスワード」を忘れた場合は、インターネットバンキングのログイン画面の下方にある「ログオンパスワードを忘れた方」ボタンを押して、「ログオンパスワード」の再登録を行うことでパスワードを再発行できる。その際には、「お客さまID」と「暗証番号」が必要となる。

⑨ 住所変更時のなりすまし

サイト上から手続きが可能となっており、第3パスワードの入力が必要となっている。

⑩ 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、128bit SSLによる暗号化技術で保護している。

⑪ ログイン状態・退席時の他人による操作

所定の時間、入力操作がなかった場合は、強制的にログアウトされる。

また、不正取引を直ちに検知するために、前回ログアウトした時間が、毎回、ログイン時に表示される。

(2) ネットバンクＢ行

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（ログインパスワード）＋第 2 パスワード（暗証番号）＋第 3 パスワード（セキュリティコード）が採用されている。

ID となる「ユーザ ID」は、初回ログイン時に、初期ユーザ ID（口座開設時に郵送される「ThankYou レター」に記載されている「支店番号」と「口座番号」をつなげた 10 桁の数字）から、利用者の任意の「ユーザ ID」に変更する。「ユーザ ID」は、半角英数字 8～12 桁（英字のみ可、数字のみ不可）で設定できる。

第 1 パスワードとなる「ログインパスワード」は、口座開設時に郵送される「ThankYou レター」に記載の仮ログインパスワード（数字 8 桁）から変更する。利用者の任意の半角英数字 6～12 桁（英字のみ不可、数字のみ不可）で設定できる。

第 2 パスワードとなる「暗証番号」は、ログイン後の取引で利用するもので、初回ログイン時に、「ユーザ ID」「ログインパスワード」と一緒に「ご利用開始登録」で設定する。半角数字 4～12 桁で任意に設定できる。

初回ログイン時には、「ワンタイム認証」のための「セキュリティ通知メール」の設定も行う。「セキュリティ通知メール」を受信するメールアドレスを登録すると、そのメールアドレス宛に、「セキュリティコード」が送信されるようになる。

② 初回登録時の本人確認

インターネットバンキングを利用するには口座開設が必要になる。銀行サイトから口座開設の申込を行うと、銀行から申込受付の確認メールが送信される。これに本人確認書類を 1 点添付して、ファクシミリ、郵送、携帯電話による書類送付アプリで送付する。銀行での本人確認書類照合が完了したら、利用者宛に本人確認書類照合完了のメールが送信される。

郵送で、「ThankYou レター」が送付され、同封されている台紙に、利用者の支店番号、口座番号、「仮ログインパスワード」等の情報が記載されている。「ThankYou レター」は、転送不要の配達記録郵便で送られる。

インターネットバンキングを利用するには、支店番号、口座番号、「仮ログインパスワード」を入力し、「ユーザ ID」、「ログインパスワード」、「暗証番号」を設定する。

③ パスワード入力が必要な手続き

ログインには、「ユーザ ID」と「ログインパスワード」が必要になる。

ログイン後の取引には、「暗証番号」が要求される。

IP 制限、セキュリティ通知メールの設定変更、定期預金中途解約、モバイルアクセス制限、ログイン制限（一時解除）、振込限度額設定、VISA デビット利用限度額設定、ATM 出金制限サービスはワンタイム認証でセキュリティコードが必要となる。

④ その他新たな個人認証方式

「セキュリティコード」は、「ワンタイム認証」を行うために必要なコードで、IP 制限の一時解除や定期預金中途解約等など「ワンタイム認証」を必要とする取引にはこのコードを利用する。「ワンタイム認証」が必要となる取引の都度に登録したアドレス宛てに自動送信される。

通常のログインは「ログインパスワード」のみの本人認証であるが、不正利用を防止するためにログイン制限を設定することができる。ログイン制限を設定した口座にログインするには「ログインパスワード」の他に「クイックログイン登録済携帯電話」か「ワンタイム認証」が必要となり、二重の本人認証で利用者の口座を防御する。

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

「ログインパスワード」や「暗証番号」をキーボードから直接入力しない「セキュリティボード」が採用されている。セキュリティボードは、「数字」と「その数字に対応する英字」の組み合わせを表にしたもので、利用者は「セキュリティボード」を参照し、「ログインパスワード」や「暗証番号」を英字で入力する。「セキュリティボード」に表示される「数字」と「その数字に対応する英字」の組み合わせは、ログインパスワードや暗証番号の入力ごとに変更される。例えば、数字の「1234」が、「セキュリティボード」では、英字の「phmv」に対応すれば、暗証番号の入力欄に英字の「phmv」と入力するか、英字の「phmv」をクリックすることになる。

⑥ フィッシングサイトによる ID・パスワードの不正入手

フィッシング詐欺のセキュリティ対策として、日本ベリサイン株式会社の EV SSL サーバ証明書が採用されており、アドレスバーを確認するだけで、正規サイトであることが確認できる。ログイン画面およびログイン後のインターネットバンキングサイト、口座開設の申込画面、問い合わせフォーム入力画面が対象となっている。

IP 制限サービスでは、利用者のプロバイダ（ドメインネーム/IP アドレス）を事前に登録しておく事で、登録先以外からの暗証番号を伴う取引を制限することができる。自宅や勤務先など普段利用になるプロバイダ（ドメインネーム/IP アドレ

ス）を、最大5つまで登録ができ、「ログインパスワード」、「暗証番号」が盗まれた場合の不正取引を防止する。

口座に入金、出金、自動引落などがあった場合には、登録のメールアドレスに、取引内容をメールで通知する。

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

「ログインパスワード」の有効期限はないが、設定後一定時間を過ぎると変更を推奨するメッセージが表示される。

⑧ パスワード（またはID）の総当り攻撃

第三者の不正利用を防ぐため、一定回数以上に「暗証番号」を誤って入力すると、ロックがかかりサービスが利用できなくなる。一定時間経つと、サービス利用が再開される。

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）

「ユーザID」を忘れた場合は、現在利用中の「ユーザID」を無効化し、支店番号、口座番号でログインできるように設定する。その際には、支店番号、口座番号、「ログインパスワード」が必要となる。

「ThankYouレター」を紛失した場合、また支店番号、口座番号、「ログインパスワード」が不明の場合は、メールでの受付はできない。カスタマーセンターまで電話で問い合わせを行う必要がある。

⑩ 住所変更時のなりすまし

住所変更は、ログイン後、「登録情報の変更」→「お客さま情報の変更」から変更できる。サイト上で変更した後、銀行より返信用封筒を郵送され、同封の本人確認貼付台紙に変更後の住所が確認できる本人確認書類を貼り付け、返送する。政令指定都市移行に伴う行政区設置による変更、または市区町村の合併で町域名以下に変更がない場合は、本人確認書類の送付は必要ない。

⑪ インターネット上の経路における盗聴

128bit SSLにより暗号化を行っている。

⑫ ログイン状態・退席時の他人による操作

一定時間応答がなかった場合は他者からの悪用を防止するため、自動的にログアウトする。ログアウト状態になってしまった場合は、再度ログインからやり直しとなる。