(5) 地銀E行

① 個人認証方式

個人認証方式としては、ID（利用者ID）＋第1パスワード（利用者パスワード）＋第2パスワード（確認パスワード）が採用されている。

IDとなる「利用者ID」は、利用者本人の確認に使用する識別名で、インターネットバンキングにログインする時に入力が必要となる。初回ログイン時に、利用者が6～12桁の半角英数字で任意に設定を行う。口座番号とは別のものとなっている。

第1パスワードとなる「利用者パスワード」は、申込時に利用申込書に記載した6桁の半角英数字となっている。初回ログイン時に、変更が求められる。英数混在が必須で、「利用者ID」と同じ設定はできない。利用者パスワードには、無料オプションでワンタイムパスワードトークンも利用できる。ワンタイムパスワードトークンは数字8桁となっている。

第2パスワードとなる「確認パスワード」も、申込時に利用申込書に記載した利用者パスワードとは異なる6桁の半角英数字となっている。初回ログイン時に、変更が求められる。英数混在が必須で、「利用者ID」と同じ設定はできない。

② 初回登録時の本人確認

利用登録に先立ち、店頭での口座開設が必要となっており、犯罪収益移転防止法の定めに従った本人確認を行っている。

インターネットバンキングを利用するには、事前に書類による申込が必要で、申込は本支店の窓口または郵送にて受付している。

初回ログイン時には、店番号（3桁）、普通・当座等の科目、口座番号（7桁）、「利用者パスワード」、「確認パスワード」を入力し、「利用者ID」を取得する。「利用者ID」取得のあと、2つのパスワードの変更画面が現れ、変更した後にインターネットバンキングを利用することができる。

③ パスワード入力が必要な手続き

ログインは、「利用者ID」と「利用者パスワード」で行い、ログイン時には、残高照会等が行える。

振込・振替、定期預金預入・解約および各種変更届等の取引は、加えて、「確認パスワード」が必要となる。

④ その他新たな個人認証方式の利用

無料オプションでワンタイムパスワードを提供している。利用する場合は、利

用申込を別途行い、携帯電話にパスワード生成用のアプリケーションソフトをダウンロードする。携帯電話にはパスワードが1分毎に更新され、「利用者パスワード」と併用して利用する。

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

ソフトウェアキーボードも利用できる。キー配置は固定である。

パスワード入力時の覗き見防止で、入力したパスワードの文字を●●●●のように暗号化表示することにも対応をしている。

⑥ フィッシングサイトによるID・パスワードの不正入手

フィッシング詐欺等によるパスワード盗難を防ぐために、ネットムーブ株式会社のセキュリティツール「nProtect Netizen（エヌプロテクト・ネチズン）」が無料提供されている。利用者は、銀行サイトからダウンロードし利用できる。インストール後、銀行サイトへアクセスすると「nProtect Netizen」が自動的に起動し、利用者のコンピュータを監視する。

利用者が照会以外の取引（振込・振替等）を行った場合や、ロックアウト時などに、登録してあるアドレスに確認メールが送信される。全ての電子メールに電子署名を付与するサービスは検討中である。

また、利用履歴（最近3回のログイン日時）を表示している。

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

パスワードの有効期限は1年間で、有効期限が切れた場合には、アラームを表示するが、「変更しない」を選択し、そのまま同じパスワードを利用することもできる。

パスワードとして、誕生日や電話番号など推測しやすい番号は登録しないように推奨しているが、登録制限は行っていない。

⑧ パスワード（またはID）の総当り攻撃

誤ったパスワードが一定回数連続した場合、一定時間ログインができなくなる「ロックアウト」の状態になる。「ロックアウト」が、一定回数連続した場合は、当該口座は利用できなくなる。

ワンタイムパスワードを一定回数以上誤入力した場合も、同様の「ロックアウト」、利用停止があり、サービス再開には窓口での手続きが必要となる。

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）

「利用者ID」の再発行はできず、失念した場合には、解約・新規申込の手続き

が必要になる。

2つのパスワードを失念し、確認する場合は、窓口にてパスワード変更の手続きを行い、新たなパスワードを設定する。

⑩ 住所変更時のなりすまし

インターネットバンキングの住所変更の受付サービスにより、住所変更の届出も可能である。住所変更の際には、「確認パスワード」が求められる。

⑪ インターネット上の経路における盗聴

インターネット上での盗聴、改ざんを防ぐため、利用者との送受信にSSL128bitによる暗号技術を採用している。また、24時間のアクセス監視も行われている。

⑫ ログイン状態・退席時の他人による操作

本人以外の第三者の利用を防止するため、一定時間操作がない場合、自動的にログアウトされる。

(6) 地銀F行

① 個人認証方式

個人認証方式としては、ID（ご契約者番号）＋第1パスワード（ログインパスワード）＋第2パスワード（確認番号）が採用されている。

IDとなる「ご契約者番号」は、10桁のインターネットバンキング専用の番号となる。申込後、登録住所に配達記録郵便で送付される「ご利用カード」に記載されている。

第1パスワードとなる「ログインパスワード」は、申込書に記入したパスワードで、半角英数字6桁となっている。

第2パスワードとなる「確認番号」は、振込や振替等を行う際に使用する番号で10桁のうち2桁を利用する。申込後、送付される「ご利用カード」に記載されている。

② 初回登録時の本人確認

インターネットバンキングの申込は、口座を持っていることを条件に窓口および郵送にて可能となる。

郵送された「ご利用カード」に記載の「ご契約者番号」と申込書に記載した「ログインパスワード」でログインする。

③ パスワード入力が必要な手続き

ログイン時には、「ご契約者番号」と「ログインパスワード」でサービスサイトに入り、振込、振替等の取引の際には「確認番号」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

「ログインパスワード」の入力の際には、ソフトウェアキーボードによるパスワード入力手段が提供されている。キーボードの文字は固定となっている。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

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

「ログインパスワード」の有効期限は1年となっている。

⑦ パスワード（またはID）の総当り攻撃

「ログインパスワード」の入力を 6 回連続して間違えるとログインができなくなる。ログインできなくなった場合は、銀行のヘルプセンターに連絡し、テレフォンバンキングで本人確認の上、ログインが可能となる。テレフォンバンキングで本人確認ができなかった場合は、「暗証番号変更届」が必要となり、申込書により新しい暗証番号を記入し、捺印の上、申込代表口座店へ提出する。

同様に、「確認番号」の入力を 3 回連続して間違えるとログインができなくなる。この場合も、「ログインパスワード」と同様の手続きが必要となる。

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）

「ログインパスワード」を忘れてしまった場合は、「暗証番号変更届」が必要となる。申込書により新しい暗証番号の記入し、届出印捺印の上、窓口へ提出する。

⑨ 住所変更時のなりすまし

ログイン時には、サイト上から住所変更を行うことができる。

⑩ インターネット上の経路における盗聴

インターネットでの情報の漏洩、盗聴、データの偽造・改ざんを防ぐため、128bit SSL 暗号化方式を採用している。

⑪ ログイン状態・退席時の他人による操作

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。

(7) 地銀G行

① 個人認証方式

個人認証方式としては、ID（ご契約者番号）＋第1パスワード（ログオンパスワード）＋第2パスワード（確認パスワード）が採用されている。

IDとなる「ご契約者番号」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、申込後、登録住所へ配達記録郵便で郵送される「ネットバンクご利用カード」に記載されている。

第1パスワードとなる「ログオンパスワード」は、サービス画面にログインする際に使用し、初期値は、申込書に記載した6桁の半角数字となっている。初回利用時に変更を行う。

第2パスワードとなる「確認用パスワード」は、振込、振替、定期預金の預け入れ等をする際に使用し、申込後、登録住所へ配達記録郵便で郵送される「ネットバンクご利用カード」に記載されている。数字10桁から、取引の都度指定される2桁を入力する。

② 初回登録時の本人確認

インターネットバンキングの申込は、口座を持っていることは条件に窓口および郵送にて可能となる。口座開設時には、窓口での本人確認が必要となっている。

口座を開設済みであれば、窓口および郵送でインターネットバンキングの申込ができる。届出印による捺印と自署が必要となっている。

③ パスワード入力が必要な手続き

ログイン時には、「ご契約者番号」と「ログオンパスワード」が必要となる。

残高照会、入出金明細照会、住所変更等はログイン状態で行える。振込、振替、定期預金取引等の取引には、「確認用パスワード」の入力が必要となる。

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

ソフトウェアキーボードによるパスワード入力手段が提供されている。「ログオンパスワード」の入力の際には、キーボードの文字は固定となっているが、「確認パスワード」入力時のソフトウェアキーボードは、利用の都度、数字の表示順を並び替える。

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

フィッシング詐欺への対策として、日本ベリサイン株式会社のEV SSLサーバ

証明書を採用している。

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

「ログオンパスワード」および「確認パスワード」の有効期限はないが、パスワードの定期的な変更を推奨している。

⑦ パスワード（または ID）の総当り攻撃

「ログオンパスワード」および「確認パスワード」を連続して一定回数以上間違えた場合は、サービスが利用できなくなる。再度、サービスを利用するには、窓口にて「ご利用カード」の再発行手続きを行う。手続きの際には、「ネットバンクご利用カード」、代表口座の届出印、本人確認書類（運転免許証等）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）

セキュリティを高めるため、「ログオンパスワード」および「確認パスワード」は照会できない仕組みとなっている。パスワードがわからなくなった場合は、窓口にて「ご利用カード」の再発行手続きを行う。手続きの際には、「ネットバンクご利用カード」、代表口座の届出印、本人確認書類（運転免許証等）が必要となる。

⑨ 住所変更時のなりすまし

ログイン時には、サイト上から住所変更を行うことができる。

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、センターと利用者のコンピュータとの間の通信を 128bit　SSL により暗号化している。

⑪ ログイン状態・退席時の他人による操作

ログインしたまま離席した場合など、一定時間操作がなかった場合には自動的にログアウトし、第三者の不正使用を防ぐよう配慮されている。

Internet Explorer のオートコンプリート機能を、インターネットバンキングでは使用できないように制限している。

(8) 地銀H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（ログインパスワード）＋第2パスワード（確認パスワード）が採用されている。

IDとなる「ログインID」は、半角英数字6～12桁のインターネットバンキング専用の番号となっている。初回ログイン時にサイト上で任意の英数字で設定する。

第1パスワードとなる「ログインパスワード」は、初期値は、サービス申込時の申込書に記載した8桁の英数字となっている。初回利用時に6～12桁の半角英数字に変更しなければならない。

第2パスワードとなる「確認用パスワード」は、振込、振替等をする際に使用し、初期値は、サービス申込時の申込書に記載した8桁の半角英数字となっている。初回利用時に6～12桁の半角英数字に変更しなければならない。「ログインパスワード」と「確認用パスワード」は必ず異なるものにしなければならない。

② 初回登録時の本人確認

インターネットバンキングの申込は、口座を持っていることを条件に窓口および郵送にて可能となる。口座開設時には、窓口での本人確認が必要となっている。

初回ログイン時に、「代表口座の店番・口座番号」、申込書に記載した「ログインパスワード」、「確認用パスワード」を入力し、「ログインID」（任意の半角英数字6～12桁）とメールアドレスを設定する。

③ パスワード入力が必要な手続き

ログイン時には、「ログインID」と「ログインパスワード」が必要となる。

残高照会、入出金明細照会はログイン状態で閲覧できる。振込、振替、限度額変更、利用者登録情報の変更には、「確認用パスワード」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

「ログインパスワード」の入力の際には、ソフトウェアキーボードによるパスワード入力手段が提供されている。キーボードの文字は固定となっている。

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。

⑥ フィッシングサイトによるID・パスワードの不正入手

フィッシング詐欺への対策としてEV SSLサーバ証明書を採用し、無料で「フィッシング詐欺検知機能」が利用できる。

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」および「確認パスワード」の有効期限はないが、パスワードの定期的な変更を推奨している。

⑧ パスワード（またはID）の総当り攻撃

「ログインパスワード」および「確認用パスワード」を連続して一定回数以上間違えた場合は、サービスが停止される。再度、サービスを利用するには、窓口でパスワードの再登録手続きを行う必要がある。

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）

「ログインパスワード」、「確認用パスワード」を忘れた場合は、申込書にてパスワード変更届けを提出しなければならない。申込書に必要事項の記入、捺印の上、窓口に郵送する。

⑩ 住所変更時のなりすまし

住所変更は、「変更届」により窓口での手続きとなる。手続きには、届出印および本人確認書類が必要となる。

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、128bit SSLによる暗号化で保護している。

⑫ ログイン状態・退席時の他人による操作

ログインしたまま離席した場合など、一定時間操作がなかった場合には自動的にログアウトし、第三者の不正使用を防ぐ仕組みが取られている。

Internet Explorer のオートコンプリート機能を、インターネットバンキングでは使用できないように制限している。

(9) 地銀1行

① 個人認証方式

個人認証方式としては、ID（契約者番号）＋第1パスワード（ログオンパスワード）＋第2パスワード（取引確認番号）が採用されている。

IDとなる「契約者番号」は、インターネットバンキング専用の番号で、半角数字10桁となる。利用申込後にハガキで利用者に通知される。

第1パスワードとなる「ログオンパスワード」は、初期値は、サービス申込時の申込書に記載した6桁の半角英数字となっている。初回利用時に6～12桁の半角英数字に変更しなければならない。

第2パスワードとなる「取引確認番号」は、振振込等の資金移動取引時に、取引確認の証明として画面上で入力する番号となっている。

初回のログオン時には、メールアドレスを必ず登録する。

インターネットバンキングの利用には月額210円の基本手数料がかかる。

② 初回登録時の本人確認

窓口で総合口座(普通預金口座)を契約後、インターネットバンキングの利用申込を行う。代表口座のある支店の窓口に利用申込書と本人確認資料を持参するか、メールオーダー式の申込書の郵送にて手続きが行える。

③ パスワード入力が必要な手続き

ログイン時には、「契約者番号」と「ログオンパスワード」が必要となる。

口座情報照会サービス（残高照会、入出金明細照会、定期預金明細照会）は、ログイン時に閲覧できる。

振替サービス（事前登録口座間振替、処理状況照会、予約取消）、振込サービス（事前登録先振込、都度指定先振込、処理状況照会、予約取消）、定期預金取引（預入・解約）、国庫金納付などの資金移動には「取引確認番号」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

「ログオンパスワード」の入力の際には、ソフトウェアキーボードによるパスワード入力手段が提供されている。キーボードの文字は固定となっている。

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。

⑥ フィッシングサイトによる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

定期的にパスワードを変更することが推奨されている。

⑧ パスワード（またはID）の総当り攻撃

「ログオンパスワード」、「取引確認番号」をいずれか6回連続して誤入力した場合、本人確認できなかったとして、サービスメニュー画面へのログインができなくなる。サービス再開には、本人確認資料を窓口に持参し、「ログオンパスワード」の変更手続が必要となる。

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）

「ログオンパスワード」、「取引確認番号」がわからなくなった場合は、変更の申込書を窓口へ提出しなければならない。署名・捺印により本人確認した上で、申込書に記載した新しい「ログオンパスワード」が利用できるようになる。

⑩ 住所変更時のなりすまし

住所変更は、サイト上から行えず、窓口または郵送による手続きとなる。

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、128bit SSLによる暗号化技術で保護している。

⑫ ログイン状態・退席時の他人による操作

一定時間操作がなかった場合には自動的にログアウトする。