(1) 地銀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（ログインパスワード）＋第2パスワード（確認用パスワード）が採用されている。

IDとなる「ログインID」は、初回のログイン時に、サイト上で登録する。口座番号とは異なるインターネットバンキング専用の番号であり、英数字混在で6～12桁となっている。「ログインID」は、初回ログイン時に、申込書に記載した決済口座の情報（支店番号、口座番号）、「ログインパスワード」、「確認用パスワード」を入力することで取得する。

第1パスワードとなる「ログインパスワード」は、インターネットバンキングの申込後に、郵送で送付される「ログインパスワードのご案内」に記載されている。10桁（英大文字）または9桁（半角数字）となっている。

第2パスワードとなる「確認用パスワード」は、申込書に記入したパスワードで、8桁（英大文字）または7桁（半角数字）となっている。

「ログインパスワード」、「確認用パスワード」は、ともに「ログインID」の取得の際に、英数字混在で6～12桁へ変更を行う。

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。窓口での本人確認には、預金口座の届出印と本人確認資料（運転免許証、健康保険証、パスポート、印鑑証明書、住民票、外国人登録原票記載事項証明書など）が必要となる。郵送による申込の場合も、本人確認資料1点を必ず同封しなければならない。

また、申込後、契約カードは、配達記録郵便または簡易書留にて届け出の住所へ転送不要で郵送される。

③ パスワード入力が必要な手続き

初回ログイン時には、決済口座の情報（支店番号、口座番号）、「ログインパスワード」、「確認用パスワード」が必要となる。その以降のログインでは、「ログインID」と「ログインパスワード」でサービスサイトに入り、取引には、「確認用パスワード」の入力が必要となる。

利用できるサービスは、残高照会/入出金明細照会、振込、振替、定期預金取引、外貨預金取引、税金・各種料金の支払、住所・電話番号の変更となっている。

④ その他新たな個人認証方式の利用

無料オプションで携帯電話を利用したワンタイムパスワードを利用できる。サイト上で、ワンタイムパスワードのトークン発行処理を行う。トークン発行処理には、携帯電話メールアドレス、「利用開始パスワード」、「確認用パスワード」の入力が必要となる。「利用開始パスワード」は、トークン発行時のみに必要なパスワードで、4～8桁の半角数字で任意に設定できる。その際、「サービスID」と「ユーザID」も発行される。

入力した携帯電話メールアドレスに、トークンアプリのダウンロード用URLを記載したメールが送信される。そのURLにアクセスし、トークンアプリのダウンロードを行う。トークンアプリを起動後、「サービスID」、「ユーザID」、「利用開始パスワード」を入力し、「送信」ボタンを押すと、ワンタイムパスワード画面が表示される。ワンタイムパスワードは、数字8桁となっている。

利用開始以後は、ログイン時に「ログインID」、「ログインパスワード」に追加してワンタイムパスワードが要求されるようになる。

新しい携帯電話でワンタイムパスワードを利用するには、初期登録手続きが必要となる。

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」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は、NTTコムウェア株式会社の「PHISHCUT（フィッシュカット）」を導入している。「PHISHCUT」ソフトウェアのダウンロード及び利用は無料で、利用者は銀行のダウンロードサイトからソフトウェアをダウンロードし、自分のコンピュータにインストールする。

「PHISHCUT」ソフトウェアは、自動的にウェブサイトを検証するために、ソフトのインストールが終了すれば、利用者側で特別な操作は必要としない。ウェブサイトに埋め込まれた「専用電子透かし」を利用してフィッシングサイトであるかどうかを検証し、ツールバー上に本物か偽物かを表示する。正しいサイトであると検証できれば青いマーク、認証ができなければ赤いマークが表示されることで、利用者が正しいサイトへ接続しているかどうかを確認できるようになっている。

インターネットバンキングロック機能は、パスワードを盗取されても取引ができないように、インターネットバンキングを利用しない間は、利用者のモバイル

バンキングでインターネットバンキングへのログインをロックしておき、利用するときだけロックを解除し利用するという機能である。インターネットバンキング利用の際には、インターネットバンキングロックの解除後、ログインすることになるが、解除後一定時間（5分程度）を経過すると、また自動的にロックが設定されるようになっている。

一定時間（5分程度）が経過しても、ログイン後であれば利用を続けることができ、ロックの解除は必要ない。ログアウトし、改めてインターネットバンキングを利用する場合は、ロックの解除が必要となる。

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ID」、「ログインパスワード」、「確認用パスワード」は、初回ログイン時にそれぞれ異なるものに変更しなければならない。

また、定期的にパスワードを変更することへの注意喚起も行われている。

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て入力された場合は、サービス利用が停止される。この際、銀行から利用停止を知らせるメールが送られる。サービスの利用停止は30分後に解除されるが、引き続き誤ったパスワードが一定回数連続して入力された場合は、再度サービスの利用を停止される。この場合、再び利用するためには、申込書による「パスワード再登録」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）

セキュリティを高めるため、ログインIDやパスワードは照会できない仕組みとなっている。申込書による「パスワード再登録」の手続きが必要となる。

⑩ 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。

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、センターと利用者のコンピュータとの間の通信を暗号化技術（128bit SSL）により保護している。

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。

(2) 地銀B行

① 個人認証方式

個人認証方式としては、ID（会員番号）＋第1パスワード（暗証番号）＋第2パスワード（第2暗証番号）＋第3パスワード（ログインパスワード）が採用されている。

IDとなる「会員番号」は、口座番号とは異なるインターネットバンキング専用の番号であり、半角数字10桁となっている。利用申込後に郵送されてくる「会員カード」に記載されている。

第1パスワードとなる「暗証番号」は、インターネットバンキングを申込した際に、申込書に記入した半角数字4桁となっている。

第2パスワードとなる「第2暗証番号」は、利用申込後に郵送されてくる「会員カード」に記載されている10桁の番号のうち、コンピュータ画面上に指定される番号4桁を入力する。

第3パスワードとなる「ログインパスワード」は、初回ログイン時に半角英数字4～10桁で任意に設定できる。「ログインパスワード」は、「会員番号」や「暗証番号」と同じ番号で登録することはできない。

② 初回登録時の本人確認

インターネットバンキングを利用するには、口座開設が必要となっている。窓口または郵送で利用申込ができる。

初回ログイン時には、申込書に記入した「暗証番号」と郵送で送付される「会員カード」に記載されている「会員番号」「第2暗証番号」が必要となる。

③ パスワード入力が必要な手続き

「会員番号」、「暗証番号」、「ログインパスワード」でログインし、残高照会等は、ログインしていれば可能であるが、利用者情報の変更（メールアドレスの登録など）や振込・振替などの取引には「第2暗証番号」が必要となる。

④ その他新たな個人認証方式の利用

利用料無料で携帯電話を利用した「ワンタイムパスワード」のサービスを提供している。利用にあたっては、インターネットバンキングへログインし、「ワンタイムパスワード開始・解除」ボタンから利用手続きを行う。

サイト上で、ワンタイムパスワードのトークン発行処理を行う。トークン発行処理のため、携帯電話メールアドレス、「利用開始パスワード」を登録する。入力した携帯電話メールアドレスに、トークンアプリのダウンロード用URLが記載されたメールが送信される。そのURLにアクセスし、トークンアプリのダウンロー

ドを行う。トークンアプリを起動後、利用設定を行うとワンタイムパスワード画面が表示される。ワンタイムパスワードは、数字8桁となっている。

利用開始以後は、ログイン時に「会員番号」、「暗証番号」、「ログインパスワード」に追加してワンタイムパスワードが要求されるようになる。

新しい携帯電話でワンタイムパスワードを利用するには、初期登録手続きが必要となる。

「ワンタイムパスワード」には有効期限の設定があり、ワンタイムパスワードアプリ画面に表示されている。有効期限の30日前からワンタイムパスワードアプリ画面上に更新の案内が表示され、利用者はワンタイムパスワードアプリ上（携帯電話画面上）で期限更新の操作をする必要がある。

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」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の提供を行っている。キーボードの文字配列は固定である。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

フィッシング詐欺から、利用者の情報を保護するために、EV SSLサーバ証明書によりサイトの正当性が簡単に確認できるようになっている。

また、RSAセキュリティ株式会社が提供するフィッシングサイト閉鎖サービス「RSA FraudAction」を導入している。

振込・振替、税金・各種料金の払込み、「暗証番号」、「ログインパスワード」の変更、住所変更といった取引が行われた場合には、事前に登録されているメールアドレスに取引の受付結果が送付される。

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

「暗証番号」、「ログインパスワード」は180日間有効で、180日間経過後にログインすると、「暗証番号」、「ログインパスワード」の変更を勧める画面が表示される。

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）

セキュリティ保護のため、「暗証番号」、「ログインパスワード」は銀行で調べる

ことができない仕組みとなっている。失念した際には、「暗証番号」の場合は、インターネットバンキングの申込書を、「ログインパスワード」の場合には、再利用登録依頼書を提出しなければならない。

「会員カード」の紛失の場合も、再利用登録依頼書を提出しなければならない。

⑩ 住所変更時のなりすまし

サイト上から利用者情報を変更するには「第2暗証番号」が必要となる。

⑪ インターネット上の経路における盗聴

利用者の情報を保護するために、128ビットSSL暗号化通信方式を採用し、情報の盗聴・書換えを防いでいる。

⑫ ログイン状態・退席時の他人による操作

ログインしたまま一定時間以上端末の操作をせずに放置していると、自動的に「ログアウト」し、取引を終了する。

(3) 地銀C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（確認用パスワード）が採用されている。

IDとなる「ログインID」は、口座番号とは異なるインターネットバンキング専用の番号であり、6～12桁（半角英数字）で初回ログイン時に任意に設定できる。数字のみ、英字のみの登録も可能となっている。

第1パスワードとなる「ログインパスワード」は、6～12桁（半角英数字）で任意に設定できる。「ログインID」とは異なるものを設定しなければならない。インターネットバンキングの申込書に記載した「仮ログインパスワード」を初回ログイン時に「ログインパスワード」に変更する。

第2パスワードとなる「確認用パスワード」も、6～12桁（半角英数字）で任意に設定できる。「ログインID」、「ログインパスワード」とは異なるものを設定しなければならない。インターネットバンキングの申込書に記載した「仮確認用パスワード」を初回ログイン時に「確認用パスワード」に変更する。

利用手数料は月額105円となっているが、初年度は無料となっており、代表口座のポイントサービスにおけるポイント数が50ポイント以上の利用者は無料で利用できる。

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、口座開設が必要となっている。郵送および窓口で申込が可能となっている。

初回ログイン時には、代表口座番号、申込書に記載した「仮ログインパスワード」と「仮確認パスワード」を初回登録サイトに入力し、「ログインID」の取得を行う。

③ パスワード入力が必要な手続き

初回ログイン時には、代表口座番号、「仮ログインパスワード」、「仮確認パスワード」が必要となる。その以降は、「ログインID」と「ログインパスワード」でログインできる。

残高照会、入出金明細照会は、ログインした状態であれば閲覧できる。振込・振替、投資信託取引、定期預金取引、税金・各種料金払込み、公共料金口座振替契約、住所変更届などは、「確認用パスワード」の入力が求められる。

④ その他新たな個人認証方式の利用

携帯電話を利用したトークンのワンタイムパスワードを利用できる。ワンタイ

ムパスワードを利用するには、サイト上からトークンの発行手続きを行い、トークン発行手続きが完了すると利用者が指定した携帯電話機の電子メールアドレスへ電子メールが送信される。電子メールに記載されたURLよりアプリケーションソフトをダウンロードし、トークンの設定を行う。8桁の数字のワンタイムパスワードが約1分ごとに新しく生成され、表示される。

トークンには有効期限があり、有効期限が近づいた場合は、トークンの起動時に更新画面が表示され、更新手続きが必要となる。

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」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。キーボードの文字位置は固定である、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

フィッシングサイト対策としては、株式会社セキュアブレインのフィッシング対策ソフト「PhishWall（フィッシュウォール）」を無料提供している。銀行サイトより利用者自身でダウンロード、インストールを行うが、インストールは約30秒と簡単であり、利用者が設定を行う必要もない。利用者が銀行サイトにアクセスする際、ブラウザのツールバーに緑のシグナルを表示し、アクセス中のサイトが本物であることを簡単に確認できる。

また、EV SSL サーバ証明書が導入され、利用者のブラウザが Internet Explorer7.0 であれば、インターネットバンキングのサイトが正当なものかどうかを、アドレスバーが緑色に変わることで確認できる。

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

パスワードは登録してから90日間有効で、90日間経過後にログインするとパスワードの変更を勧める画面が表示される。従来のパスワードを継続して使用することも可能であるが、セキュリティ上の観点からも定期的な変更を促している。

初回ログイン時に登録するパスワードも、半角英数字であること、6～12文字であること、「ログインパスワード」と「確認用パスワード」が異なるものであること、「ログインID」と異なるものであることを満たさない場合は、エラーが表示され登録ができない。

⑧ 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があった場合は、一定時間サービスを利用

できなくなる「ロックアウト」の状態になる。「ロックアウト」が一定回数発生するとサービスが停止される。サービス停止後の再開にあたっては、申込書によりパスワードの変更手続を行わなければならない。

「ログインパスワード」の場合は、連続6回入力エラーで「ロックアウト」し、連続3回「ロックアウト」が続くとサービス停止となる。

ワンタイムパスワードの場合は、連続10回の入力エラーでサービスが停止され、ワンタイムパスワード機能解除依頼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）**

「ログインID」を忘れてしまった場合は、窓口または郵送による「ログインID」の初期化が必要となる。

パスワードを忘れてしまった場合は、窓口または郵送で、利用申込書による「利用停止再開（パスワード変更）」の手続きが必要になる。「ログインパスワード」、「確認パスワード」のどちらか一方を忘れても、両方のパスワード変更が必要となる。

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、「確認用パスワード」の入力が求められる。

⑪ **インターネット上の経路における盗聴**

インターネット上の経路における盗聴を防ぐため、128bit SSLによる暗号化などの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**

サービス利用中に画面を開いたまま一定時間（約 5 分）放置した場合、自動的にログアウトされる。

(4) 地銀D行

① 個人認証方式

個人認証方式としては、ID（契約番号）＋第1パスワード（パスワード）＋第2パスワード（確認番号）＋第3パスワード（確認暗証番号）が採用されている。

IDとなる「契約番号」は、口座番号とは異なるインターネットバンキング専用の番号であり、インターネットバンキング申込後送付される「契約者カード」に記載されている数字10桁となっている。

第1パスワードとなる「パスワード」は、インターネットバンキングの申込後送付される「パスワード・確認暗証番号通知書」に記載されている「仮パスワード」を変更して利用するもので、半角英数6～10桁で任意に設定できる。

第2パスワードとなる「確認番号」は、インターネットバンキング申込後送付される「契約者カード」に記載されている2桁の数字で、画面で指定された場所に記載されている数を入力する。

第3パスワードとなる「確認暗証番号」は、インターネットバンキングの申込後送付される「パスワード・確認暗証番号通知書」に記載されている数字で、振込み等の取引時入力する4～6桁の半角数字である。初回ログイン時に変更して利用する。

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、口座開設が必要となっている。

初回ログイン時には、「契約者カード」に記載された「契約者番号」「確認番号」と「パスワード・確認暗証番号通知書」に記載されている「仮パスワード」が必要となる。

③ パスワード入力が必要な手続き

「契約者番号」と「パスワード」でサービスサイトに入り、振込、振替、外貨預金取引、投資信託などの取引には、「確認暗証番号」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

「パスワード」「確認番号」「確認暗証番号」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。キーボードの文字配置は固定されている。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

株式会社セキュアブレインのフィッシング対策ソフト「PhishWall（フィッシュウォール）」が無料提供されている。銀行サイトからソフトをダウンロードし、インストールすることで利用できる。インストール後は、銀行サイトにアクセスした際、正しいサイトであれば、ブラウザのツールバーに緑色のシグナルが表示され、アクセスしているサイトが本物であることを確認することができる。

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

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が行われている。

⑦ 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があった場合は、「パスワードロック」がかかる。解除するには、窓口での手続きが必要で、本人確認書類、届出印も必要となる。ロック解除手続き完了後、「パスワード・確認暗証番号通知書」が郵送され、新しい「パスワード」または「確認暗証番号」で利用を再開する。

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」、「確認暗証番号」を忘れた場合は、「パスワード・確認暗証番号再発行」の届けが必要になる。本人確認書類、届出印が必要となるため窓口でのみ扱う。暗証番号の変更手続き完了後、「パスワード・確認暗証番号通知書」が郵送され、新しい「パスワード」または「確認暗証番号」で利用する。

⑨ 住所変更時のなりすまし

インターネットバンキングのサイト上から住所変更を行うことはできない。

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による暗号化が行われている。

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。