1　銀行における個人認証制度

1.1　都市銀行

都市銀行では、都銀 A 行、都銀 B 行、都銀 C 行、都銀 D 行の 4 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 1　都市銀行における個人認証方式 1/2

項番	調査項目		都銀A行	都銀B行
1	個人認証方式		ID＋パスワード＋乱数表＋ワンタイムパスワードトークン（有料オプション）	ID＋パスワード＋乱数表＋ワンタイムパスワードトークン（有料オプション）
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） 初回ログイン時には、ID（郵送）、第1パスワード（申込書記入）、第2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） インターネット、モバイル、電話での利用申込の際は、「暗証カード」が届いたところで有効化が必要 ログインには、ID（郵送）、第1パスワード（郵送）が必要
3	IDの実体		口座番号とは別の8桁または10桁の半角数字	口座番号とは別の10桁の半角数字
4	パスワードの実体	第1パスワード	申込時に任意に設定した半角数字4桁（キャッシュカード暗証番号でも可） インターネットバンキング専用の暗証番号（4桁）に変更可能	デフォルトでキャッシュカードの暗証番号 インターネットバンキング専用の暗証番号（4桁）に変更可能
		第2パスワード	6桁の数字の中から、指定された4つの数字を入力	乱数表の1回限りの箇所の数字の組合せ（2+2＝4桁）
		第3パスワード	任意に設定した半角英数字6～32桁	乱数表の特定箇所の数字（2桁）
		ワンタイムパスワード	（有料オプション）パスワードが30秒毎に更新される専用機器（トークン） 第2パスワードの代わりに利用可能	（有料オプション）パスワードが1分毎に更新される専用機器（トークン） 第1パスワードと併用して利用可能
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・入出金明細の閲覧 登録済の振込先への振込 登録情報の閲覧
		第2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・振替 外貨預金取引 投資信託など	新規の振込先への振込 カードローンの申込
		第3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 残高照会	定期・積立預金の中途解約 振込上限額の引上げ 住所変更

図表 2　都市銀行における個人認証方式 2/2

項番	調査項目		都銀C行	都銀D行
1	個人認証方式		ID＋パスワード＋乱数表	ID＋パスワード＋乱数表＋ワンタイムパスワードトークン（有料オプション）
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） 口座があれば、オンラインでインターネットバンキングの申込可能 初回ログイン時には、ID、第1パスワード（申込書記入）、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） 口座開設には店舗での申込が必要
3	IDの実体		口座番号とは別の10桁の半角数字	申込書に記載の番号
4	パスワードの実体	第1パスワード	申込時に任意に設定した半角数字4桁	メイン口座の口座番号7桁とキャッシュカード暗証番号4桁を組合せた半角数字11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	初回ログイン時に登録する半角英数字記号8～16桁	乱数表の指定された場所の数字を入力
		第3パスワード	乱数表の指定された枠の半角数字2桁をを入力	なし
		ワンタイムパスワード	なし	（有料オプション）パスワードが30秒毎に更新される専用機器（トークン） 第2パスワードの代わりに利用可能
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 振込、振替 定期預金 外貨預金 投資信託など	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 預金残高照会 明細照会	振込、振替 定期預金 外貨預金 登録情報の変更など
		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、振替 定期預金 外貨預金 投資信託など	なし

図表 3　都市銀行における ID・パスワードの不正入手を防ぐ対策 1/2

項番	調査項目	対策が不十分な場合に想定されるリスク	都銀A行	都銀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によるパスワード入力手段の提供	ソフトウェアキーボード(マウス操作、キー配列を毎回変更)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		EV SSLサーバ証明書を採用 リスクベース認証を導入 フィッシングサイト閉鎖サービスを導入	EV SSLサーバ証明書を採用 自社の画面設計ガイドラインを作成し、自サイトが正当なサイトであることを容易に確認可能な仕組みを提供 フィッシングサイト閉鎖サービスを導入 全ての電子メールに電子署名を付与
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の登録制限 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 第3パスワードがサービス停止になった場合は、電話による第1パスワード、第2パスワードの確認でサービス再開	パスワードの一定回数以上の誤入力でサービス停止 申込書に署名・捺印の上、本人確認資料を添えて、郵送で申込を行うことでサービス再開 ワンタイムパスワードの一定回数以上の誤入力の場合は、サービス再開には窓口での手続きが必要
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、申込書による再発行手続きが必要 再発行手続きに伴い、第1パスワード、第2パスワードも変更 第1パスワード、第2パスワードがわからなくなった場合も、申込書により新しい暗証番号を設定 ID、パスワードが記載された書類は配達記録で送付	第2～第3パスワードの確認・変更には、申込書に署名・捺印の上、本人確認資料を添えて、郵送での申込が必要 パスワードを記載した書類は、配達記録郵便またはヤマト運輸のセキュリティパッケージにて送付
7	住所変更時のなりすまし		インターネットバンキングで手続き可能 第2パスワードかワンタイムパスワードの入力が必要	インターネットバンキングで手続き可能 第1～第3パスワードまでの入力が必要
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	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、一定時間以上操作がないと、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 パスワードの自動入力は不可

図表 4　都市銀行における ID・パスワードの不正入手を防ぐ対策 2/2

項番	調査項目	対策が不十分な場合に想定されるリスク	都銀C行	都銀D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の採用なし	ソフトウェアキーボード(キー配列固定)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		EV SSLサーバ証明書を採用 一部の電子メールに、電子署名を付与	EV SSLサーバ証明書を採用 リスクベース認証を導入 フィッシング対策ソフトを無料提供
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		簡単に推測されやすいパスワードの登録制限 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 第1パスワードを連続して誤入力した場合は、電話または書面による手続きが必要 第2パスワードを連続して誤入力した場合は、インターネット上で再度の初回登録	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、約1時間で改めて正しいパスワードを入力することで利用可能 一時停止が一定回数発生した場合は、登録されているパスワードが無効になり、サービスが停止 第1パスワード、「秘密の質問」が無効になった場合は、パソコンから初期化手続きすることでサービスの再開 第2パスワードが無効となった場合は、郵送か店舗で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(他人による不正なパスワード確認、変更請求等)		第1パスワードがわからなくなった場合は、電話または書面による手続きが必要	IDがわかなくなった場合は、サイト上で生年月日などの必要事項を入力することで、登録電子メールアドレスへID送付
7	住所変更時のなりすまし		インターネットバンキングで手続き可能	インターネットバンキングで手続き可能
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	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、一定時間以上操作がないと、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(約10分)

(1) 都銀Ａ行

① 個人認証方式

個人認証方式としては、ID（お客様番号）＋第１パスワード（第１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「お客様番号」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８桁または 10 桁となっている。

第１パスワードとなる「第１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１暗証番号」は、キャッシュカードの暗証番号と同じ数字を利用することもできる。誕生日などの推測しやすい数字は避けるようにという注意喚起を行っており、1111 などの単純な数字の組み合わせは設定できないようになっている。

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「ご利用開始のお知らせ(ご利用カード)」に記載されている６桁の半角数字の中から、指定された４つの数字を入力することとなる。「第２暗証番号」に関しては、有料オプションにてワンタイムパスワードトークンを利用することもできる。

第３パスワードとなる「ログインパスワード」は、初回ログイン時に登録を行う。「ログインパスワード」は、半角英数字６～32 桁で利用者が任意に設定することができるが、英数が混在した組み合わせでなければ登録できないようになっている。

② 初回登録時の本人確認

インターネットバンキングを利用するには、口座開設が必要となっている。郵送による口座開設の申込もできるが、犯罪による収益の移転防止に関する法律（以下、「犯罪収益移転防止法」という）に基づく本人確認資料２点の提示が必要となる。

初回ログイン時には、申込書に記入した「第１暗証番号」と速達記録郵便（転送付加）で発送される「ご利用カード」に記載された「お客様番号」、「第２暗証番号」で本人確認を行う。

③ パスワード入力が必要な手続き

初回ログイン時には、「お客様番号」、「第１暗証番号」、「第２暗証番号」が必要となる。その以降のログインでは、「お客様番号」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、外貨預金取引、投資信託などの取引には、追加的に「第２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

有料オプション（発行手数料 2,100 円、月々の利用料は無料）で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申込した利用者にはワンタイムパスワード専用端末であるトークンが送付され、インターネットバンキング等を利用する際に、従来の「第 2 暗証番号」の代わりにトークンに表示されるワンタイムパスワードを入力する。約 30 秒ごとに異なる新しいパスワード（ワンタイムパスワード）が生成され、数字 6 桁で液晶画面に表示される。生成されたパスワードは、ボタンを押したときのみ液晶画面に表示される仕組みとなっている。

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

「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。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、EV SSL 証明書、リスクベース認証、RSA セキュリティ株式会社が提供する「RSA FraudAction」によるフィッシングサイト閉鎖サービスを導入している。これは、偽の Web サイトを探知し、閉鎖するサービスで、世界各国のインターネットサービスプロバイダとの協力により、24 時間 365 日体制で国内外のフィッシングサイトを閉鎖する対応が可能となっている。

リスクベース認証は、利用者がインターネットバンキングにアクセスする環境（コンピュータやネットワーク等）を分析し、コンピュータ環境（コンピュータの OS やブラウザの種類が異なる、cookie がない等）や利用している IP アドレス情報等のネットワーク環境を総合的に検証し、通常利用している状況と異なると判定された場合は、従来の「ログインパスワード」による認証にくわえて、「合言葉」による追加認証を行うものである。

利用者は、初回のログイン時に、3 つの合言葉と画像を登録する。3 つの合言葉は、3 つの質問グループ（1 つの質問グループには 10 の質問が含まれており、その中から任意に 1 つ選択）からそれぞれ 1 問、合計 3 問を選択し、その回答（全角 10 文字以内）が合言葉として登録される。質問は、「最も好きな歌手の名前は何ですか？」「最も好きな飲み物は何ですか？」といった内容になる。画像については、約 600 種類の中から 1 つ選択し、登録しておく。通常利用している状況と異なると判定された場合は、「お客様番号」の後に、「合言葉」の入力が必要となる。

登録した画像は、ログイン時のログインパスワードの入力画面で表示されるこ

とになる。これによりログインするサイトが正規のサイトであることを画面上で確認することができる。

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

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が、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

パスワードの一定回数以上の誤入力があった場合は、サービスが停止される。

誤入力したパスワードが「ログインパスワード」の場合、電話にて「第1暗証番号」、「第2暗証番号」を伝えることでサービスを再開できる。

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）

「お客さま番号」がわからなくなった場合には、申込書により「ご利用カード」の再発行手続きが必要となる。再発行手続きに伴い、「第1暗証番号」、「第2暗証番号」も変更となる。手続き終了後、再発行された「ご利用カード」が配達記録郵便で届けられる。

「第1暗証番号」がわからなくなった場合や「第1暗証番号」の変更を希望する場合は、申込書により新しい「第1暗証番号」を設定する。電話等による「第1暗証番号」の照会はできない。「第1暗証番号」が変更されると、同時に「第2暗証番号」も変更となるため、新しい「第2暗証番号」が記載された「ご利用カード」が配達記録郵便で届けられることになる。

「第2暗証番号」がわからなくなった場合も、「第1暗証番号」と同様に申込書により新しい「第2暗証番号」を設定する。電話等による「第2暗証番号」の照会はできない。

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、「第2暗証番号」もしくはワンタイムパスワードの入力が必要である。

⑪ インターネット上の経路における盗聴

128bit SSLの暗号通信方式によって通信路の保護を行っている。

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。

(2) 都銀 B 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（第 1 暗証）＋第 2 パスワード（第 2 暗証）＋第 3 パスワード（第 3 暗証）が採用されている。

ID となる「契約者番号」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。

第 1 パスワードとなる「第 1 暗証」は、デフォルトでキャッシュカードの暗証番号となっているが、インターネットバンキング専用の暗証番号（4～8 桁）に変更可能である。「第 1 暗証」に関しては、有料オプションにてワンタイムパスワードを併用できる。

第 2 パスワードとなる「第 2 暗証」は、インターネットバンキングの利用申込後に郵送されてくる「暗証カード」に記載されている乱数表から、指定された 2 箇所の枠内にある 2 桁の半角数字を入力する（2+2＝4 桁）。

第 3 パスワードとなる「第 3 認証」も、インターネットバンキングの利用申込後に郵送されてくる「暗証カード」に記載されている乱数表から、指定された 1 箇所の枠内にある 2 桁の半角数字を入力する（2 桁）。

② 初回登録時の本人確認

利用登録に先立ち、口座開設が必要であり、犯罪収益移転防止法に基づく本人確認資料 2 点の提示が求められる。利用申込後、「暗証カード」が郵送されるが、書面ではなく、インターネット、モバイル、電話にて利用申込が行われた場合は、安全のため「暗証カード」は利用できない状態で送付され、手元に「暗証カード」が届いた時点で有効化手続きが必要になる。有効化手続きは、「契約者番号」と「第 1 暗証」でログインした後、「暗証カードを有効にする手続きを行う」メニューで申込時に届けた電話番号を確認し、その電話番号にシステムから自動で電話がかかってくる。利用者は電話を受け、画面に表示されている確認番号を電話機のボタンで入力することで、「暗証カード」を有効にすることができる。

③ パスワード入力が必要な手続き

「第 1 暗証」のみで実行可能な手続きは、

- インターネットバンキングへのログイン
- 残高・入出金明細の閲覧
- 登録済の振込先への振込
- 登録情報の閲覧

「第１暗証」、「第２暗証」が必要な手続きは、
・新規の振込先への振込
・カードローンの申込
「第１暗証」、「第２暗証」、「第３暗証」が必要な手続きは、
・定期・積立預金の中途解約
・振込上限額の引上げ
・住所変更
となっている。

④　その他新たな個人認証方式

有料オプション（発行手数料は無料、月々の利用料は 105 円）でワンタイムパスワードが利用できる。ワンタイムパスワードを申込した利用者には専用機器であるトークンが郵送される。1分毎に新しいパスワードが表示される専用機器（トークン）を「第１暗証」と併用して利用することができる。

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（マウス操作、キー配列を毎回変更）によるパスワード入力手段が提供されている。画面上でソフトウェアキーボードからマウスが離れているとキーが表示され、クリックするためマウスが近づくとキーが非表示になるため、クリックと同時に画面情報を盗み取るタイプのスパイウェアからの防御が可能な新型ソフトウェアキーボードとなっている。

⑥　フィッシングサイトによる ID・パスワードの不正入手

画面設計ガイドラインを作成し、正しいサイトであることを容易に確認可能な仕組みを提供している。

また、EV SSL サーバ証明書により正しいアドレスの際にはアドレスバーが緑色に変化する仕組みを取り入れ、「ブラウザのアドレスバーの色」と「サイトを運営する企業名の表示」の 2 点をチェックすることにより、正しいサイトであることを確認できるようになっている。

フィッシング詐欺時に作成される偽サイトを迅速に閉鎖させるために、RSA セキュリティ株式会社が提供する「RSA FraudAction」を採用している。

また、銀行からの電子メールには、全て電子署名を付与している。

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

パスワードが長期間変更されていない場合には、ログイン時（パスワード入力時）にアラームが表示される。しかし、強制変更のシステムにはなっておらず、

アラーム画面を確認すれば、現在のパスワードで利用が可能となっている。

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でサービスが停止される。サービスの再開には、申込書に署名・捺印の上、本人確認資料（氏名と住所を証明するもの）を添えて、郵送での申込が必要である。パスワードを記載した書類は、配達記録郵便またはヤマト運輸のセキュリティパッケージにて郵送される。

ワンタイムパスワードを一定回数以上誤入力した場合、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）

「第2暗証」と「第3暗証」の確認・変更には、申込書に署名、捺印の上、本人確認資料を添えて、郵送での申込が必要となる。パスワードを記載した書類は、配達記録郵便またはヤマト運輸のセキュリティパッケージにて郵送される。

⑩ インターネット上の経路における盗聴

128bit SSLの暗号通信方式によって通信路の保護を行っている。

⑪ ログイン状態・退席時の他人による操作

ログイン時、一定時間以上、操作がないと、自動的にログアウトする。

パスワードの自動入力は不可となっている。

(3) 都銀C行

① 個人認証方式

個人認証方式としては、ID（ご契約番号）＋第1パスワード（ダイレクトパスワード）＋第2パスワード（確認番号）＋第3パスワード（IBログインパスワード）が採用されている。

IDとなる「ご契約番号」は、口座番号とは別の番号であり、半角数字10桁となっている。

第1パスワードとなる「ダイレクトパスワード」はインターネットバンキングを申込した際に指定した4桁の半角数字となっている。

第2パスワードとなる「IBログインパスワード」は、初回ログイン時に登録する。半角英数字と半角記号8桁以上16桁以内で組み合わせることが必須となっている（英字と記号、数字と記号、もしくは英字と数字と記号）。

第3パスワードとなる「確認番号」は、利用申込後郵送されてくる「ご契約カード」に記載された乱数表で、指定された枠の数字2桁を入力する（半角数字2桁）。

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る。口座を持っていれば、インターネットから申込が完了する。

インターネットでの申込の際には、店番（半角数字3桁）、預金種類、口座番号（半角数字7桁）、名前（全角カタカナ）、生年月日（半角数字）に加えて、通帳の最終残高を入力する必要がある。

申込完了後、「スタートキット」が配達記録郵便で発送される。

③ パスワード入力が必要な手続き

初回ログイン時には、「ご契約番号」、「ダイレクトパスワード」、「確認番号」が必要となる。次回以降のログインは、「ご契約番号」と「IBログインパスワード」で利用できるようになる。振込、振替等の取引には、「ダイレクトパスワード」と「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

ソフトウェアキーボードへの対応は行われていない。

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によるID・パスワードの不正入手

フィッシングサイトによる不正なIDやパスワードの入手を防止するために、EV SSLサーバ証明書を採用している。これにより、コンピュータのOSがWindows XP SP2またはWindows Vista、ブラウザがInternet Explorer 7.0の利用者は、利用時の画面が正しいものであることの確認がわかりやすくなっている。

他人の不正なアクセスを利用者本人が事後的に確認できるよう、利用者がログインした時刻を記録しており、ログイン時に前回のログイン時刻を画面上に表示している。

また、銀行から送付する電子メール（一部）に、電子署名をつけている。

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

「IBログインパスワード」は、記号を組み合わせることは必須となっており、数字だけの組み合わせではなく、英字と記号、数字と記号、もしくは英字と数字と記号という組み合わせでパスワードを設定しなければならない。

利用者に対して、定期的にパスワードを変更することへの注意喚起も行っている。

⑦ パスワード（またはID）の総当り攻撃

不正な取引防止策として、パスワードを一定回数以上誤って入力すると、サービスが停止される。

「ダイレクトパスワード」を連続して誤入力した場合は、電話または書面による手続きが必要となる。

「IBログインパスワード」の誤入力よりサービスが停止された場合は、「契約カード」があれば、インターネット上で初回登録を再度行うことで利用できるようになっている。

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）

「ダイレクトパスワード」を忘れた場合は、電話か書面による手続きが必要となる。

⑨ 住所変更時のなりすまし

サイト上で手続き可能であり、書面による申込は不要となっている。

⑩ インターネット上の経路における盗聴

128bit SSLの暗号通信方式によって通信路の保護を行っている。

⑪　ログイン状態・退席時の他人による操作

ログイン後に、コンピュータ等から離席し、その間に第三者に勝手に操作されることを防止するため、一定時間操作がない場合には自動的にログアウトし、取引を終了する。

(4) 都銀 D 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（ご利用カード乱数表）が採用されている。

ID となる「ログイン ID」は、申込書に記載したもので、利用申込後に郵送されてくる「ご利用カード（乱数表）」にも記載されている。ログイン ID は変更が可能で、アルファベットと数字を必ず組み合わせて設定することが推奨されているが、数字のみでも設定できる。

第 1 パスワードとなる「ログインパスワード」は、デフォルトでメイン口座の口座番号 7 桁とキャッシュカード暗証番号 4 桁を組合せた 11 桁となっている。初回ログイン時に変更を行い、半角英数字 6～12 桁の設定を行う。

第 2 パスワードは、「ご利用カード（乱数表）」に記載されている数字となり、指定された場所の数字を入力する。有料オプションのワンタイムパスワードを代わりに利用することもできる。

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る。口座開設には店舗での申込が必要となる。

③ パスワード入力が必要な手続き

ログイン時には、「ログイン ID」と「ログインパスワード」が必要となる。

振込・振替、定期預金、外貨預金といった取引や「ログインパスワード」等の変更の際には、「ご利用カード（乱数表）」に記載の数字の入力が必要となる。

④ その他の新たな個人認証方式の利用

有料オプション（利用手数料は 2,000 円）でワンタイムパスワードが利用できる。振込、ペイジー払込、「ログインパスワード」変更などを行う際に、「ご利用カード（乱数表）」の代わりに利用する。

ワンタイムパスワードを申込した利用者には、ワンタイムパスワード生成するトークンが送付される。トークンは、ボタンを押下するたびに異なる 6 桁の数字を表示する。続けて使用する場合は、32 秒経ってからボタンを押下する必要がある。

トークンの有効期限は、トークンの電池切れにより、ワンタイムパスワードが表示されなくなるまでとなっている。電池切れ後も引続きワンタイムパスワードを利用する場合は、トークンの再発行手続きが必要となる。再発行の際にも、利用手数料 2,000 円がかかる。但し、通常の利用で 5 年以内にトークンが電池切れ

になった場合は、無償で交換してくれる。

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（キー配列固定）を利用して、「ログインID」と「ログインパスワード」を入力することができる。入力した文字は、「●●●●」で表示され、パスワード入力時の覗き見を防止する技術的対応が行われている。

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、リスクベース認証を導入している。セキュリティ向上のため、ログイン時に利用者の利用環境や利用パターンなどを自動的に認識して、普段とは異なる状況でログインがなされた場合に、「秘密の質問」による認証を追加する本人認証方式をとっている。

初期設定時に質問と回答を3つずつ登録する。質問は、全角20文字以内で漢字・カナ等の制限はない。回答は、全角ひらがなで3～10文字以内で設定する。

同様に、初期設定時に、「秘密の画像」として好みの画像を1つ選択し、ログインパスワード入力画面、およびログイン後のトップページに選択した画像を表示することで、正しいサイトであることを確認しやすくしている。自分で撮影したオリジナル画像（2MB以下）を登録することも可能である。

任意ではあるが、「秘密の画像」と一緒に、「秘密のフレーズ」を登録することができる。「秘密の画像」と組み合わせることで、偽サイトに対するセキュリティをより高めることができる。

SSLによる暗号化通信が行われるページにはサーバ証明書が発行され、EV SSL対応ブラウザでアクセスした場合アドレスバーが緑色になり、そのサイトが正しいサイトであることが確認できる仕組みがとられている。

不正取引への対策ツールとして、「nProtect Netizen（エヌプロテクト・ネチズン）」も導入されている。インターネットバンキングの利用前に、このソフトウェアを起動することで、スパイウェア等の不正取引をガードする。

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

パスワードが長期間変更されていない場合には、ログイン時（パスワード入力時）にアラームが表示される等、定期的にパスワードを変更することへの注意喚起が行われている。

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連続して一定回数入力されると、一定時間の間サービスが利用できなくなり「ロックアウト」する。「ロックアウト」中は利用することがで

きないが、1時間程経ってから改めて正しいパスワードを入力することで利用可能となる。「ロックアウト」になった際は、登録されている電子メールに連絡される。

さらに、「ロックアウト」が一定回数発生した場合は、登録されているパスワードが無効になり、サービスが停止される。サービス停止の際にも、電子メールにて連絡される。「ログインパスワード」、「秘密の質問」が無効になった場合は、コンピュータから初期化手続きすることでサービスを再開できるが、第2パスワードの乱数表によるパスワードが無効となった場合は、郵送か店舗で「ご利用カード（乱数表）」の再発行手続きが必要なる。

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」を失念した場合は、支店名、科目、口座番号、カナ氏名、生年月日、メールアドレスを入力することで、登録してある電子メールアドレスへ「ログインID」が送付される。

⑩ **住所変更時のなりすまし**

サイト上で手続き可能であり、書面による申込は不要となっている。

⑪ **インターネット上の経路における盗聴**

128bit SSLの暗号通信方式による通信路の保護を行っている。

⑫ **ログイン状態・退席時の他人による操作**

他者からの悪用を防止するため、一定時間操作が行われないと自動的にログアウトする。その時間は、約10分間となっている。自動的にログアウトした場合は、再度ログインすることで利用することができる。