6　各業界における個人認証制度の比較および評価

(1) 銀行

		銀行	
		都市銀行	地方銀行
個人認証方式		認証方式は、ID＋パスワード＋乱数表＋ワンタイムパスワードが多い。 複数のパスワードを併用させるが、多くが第3パスワードまで利用している。 乱数表による多要素認証が標準で用いられ、ワンタイムパスワードトークンもオプションで導入されている。	認証方式は、ID＋パスワード＋乱数表またはID＋パスワード＋ワンタイムパスワードが多い。 複数のパスワードを併用させるが、多くが第2パスワードまで利用している。 多要素認証では、乱数表かワンタイムパスワードトークンのどちらかを選択している場合が多い。
初回登録時の本人確認		口座開設を必須にすることにより、本人確認するとともに、IDやパスワードを返送不要で郵送している。	口座開設を必須にすることにより、本人確認するとともに、IDやパスワードを返送不要で郵送している。
IDの実体		口座番号とは異なる英数字を付与されることが多い。	口座番号とは異なる英数字を付与されることが多い。
パスワードの実体		任意に設定させるもの、郵送で送付するもの、乱数表、OTPを組み合わせることで高いセキュリティを確保している。	任意に設定させるもの、郵送で送付するもの、乱数表、OTPを組み合わせることで高いセキュリティを確保している。
ワンタイムパスワードの利用		導入されているが、有料オプションが多い。 専用機器が主流である。	上位行では導入率が高い。 導入している場合は、携帯電話で無料オプションが多い。
個人認証制度の課題		インターネット上の個人認証においては、最も高いレベルの方策が実施されている。 セキュリティを高めるために複雑な仕組みを取ることで、利用者のユーザビリティがおざなりになり、実際には利用者がパスワードを紙に書いてしまうというようなことが発生しないような配慮が必要である。 システム的なセキュリティは既に水準を超えており、今後は、アナログ犯罪を防ぐための利用者への啓蒙・教育が重要になる。	銀行の規模と財務状況により、対応にばらつきはあるが、業界ガイドランドが作成されるなどしているため、必要なベースラインはきちんと押さえられている。 多要素認証においても、乱数表かOTPのどちらかが導入されており、高いセキュリティが確保されている。OTPにおいても、専用機器ではなく携帯電話を活用するなど、コストを抑えながらも安全を高める工夫がされている。 都市銀行のようにフルラインナップでセキュリティ施策をする必要はなく、地域ごとに異なる利用者のITリテラシーやニーズにあった施策展開が重要となる。
ＩＤ・パスワードの不正入手等を防ぐための対策	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。 キー配列固定が多い。	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。 キー配列固定が多い。
	パスワード入力時の覗き見	●●●●の暗号化表示に対応している。	●●●●の暗号化表示に対応している。
	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、リスクベース認証、電子署名など先端的な対応が採用されている。	EV SSLサーバ証明書に加えて、サイト上からダウンロードできるフィッシング対策ソフトを無料提供している銀行が多い。
	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や推測しやすいパスワード設定を行わないことなどを利用者へ注意喚起している。 パスワードに有効期限をつけている場合もある。	定期的にパスワードを変更することや推測しやすいパスワード設定を行わないことなどを利用者へ注意喚起している。
	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を停止している場合が多い。 サービス再開には、パスワードや本人確認が必要となっている。	パスワードの一定回数以上の誤入力でサービスを停止している場合が多い。 サービス再開には、パスワードや本人確認が必要となっている。
	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）	重要なパスワードを忘れた場合は、電話または書面による手続きを必要とするところが多い。	重要なパスワードを忘れた場合は、電話または書面による手続きを必要とするところが多い。
	住所変更時のなりすまし	サイト上で手続きできるが、パスワードを求められる。	サイト上で手続きできる場合、書面や窓口での手続きしかできない場合に分かれる。
	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保護を行っている。	128bit SSLの暗号通信方式による通信路保護を行っている。
	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となる。	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となる。
ID・パスワードの不正入手等を防ぐための対策における課題		インターネット上でID・パスワードの不正入手等を防ぐために、最も高いレベルの方策が実施されている。	インターネット上でID・パスワードの不正入手等を防ぐために、高いレベルの方策が実施されている。
総評		◎	○

		銀行	
		ネットバンク	その他の大手、準大手
個人認証方式		認証方式は、ID＋パスワードまたはID＋パスワード＋ワンタイムパスワードが多い。 複数のパスワードを併用させるが、多くが第3パスワードまで利用している。 多要素認証の導入は、バラツキがある。	認証方式は、ID＋パスワードまたはID＋パスワード＋乱数表が多い。 複数のパスワードを併用させている。 多要素認証の導入は、バラツキがある。
初回登録時の本人確認		口座開設を必須にすることにより、本人確認するとともに、IDやパスワードを返送不要で郵送している。	口座開設を必須にすることにより、本人確認するとともに、IDやパスワードを返送不要で郵送している。
IDの実体		口座番号とは異なる英数字を付与されることが多い。	口座番号とは異なる英数字を付与されることが多い。
パスワードの実体		任意に設定させるもの、郵送で送付するもの、OTPを組み合わせることで高いセキュリティを確保している。	任意に設定させるもの、郵送で送付するもの、乱数表を組み合わせることで高いセキュリティを確保している。
ワンタイムパスワードの利用		専用機器だけでなく、セキュリティコードをメール送信するワンタイム認証を行っている銀行もある。	導入率は高くない。
個人認証制度の課題		ネットバンクという特性から、セキュリティを重視しているものとユーザビリティを重視しているものに分かれるが、多要素認証までいたっていない銀行においても、パスワードを複数入力させるなど、セキュリティを高める工夫がされている。 セキュリティを確保しながらも、ネットバンクというインターネット上で気軽利用できる銀行としての特性を失わないような配慮が必要である。	インターネットバンキングに注力している銀行、そうでない銀行で対応がわかれる。 ネットでのチャネルを強化している銀行では、複数のパスワードや乱数表で多要素認証を行っているが、そうでない場合は、最低限の対策となっている。セキュリティ対策が遅れている銀行の底上げが重要となる。
IDパスワードの不正入手等を防ぐための対策	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	キー配列を毎回変更する新型ソフトウェアキーボードやセキュリティボードなど新技術が導入されている	ソフトウェアキーボードによるパスワード入力手段を提供している。 キー配列固定が多い。
	パスワード入力時の覗き見	●●●●の暗号化表示に対応している。	●●●●の暗号化表示に対応している。
	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サーバ証明書に加えて、メールにて、取引実行や登録情報の変更などを通知している場合が多い。	メールにて、取引実行や登録情報の変更などを通知している場合が多い。
	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や推測しやすいパスワード設定を行わないことなどを利用者へ注意喚起している。	定期的にパスワードを変更することや推測しやすいパスワード設定を行わないことなどを利用者へ注意喚起している。
	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を停止している場合が多い。 サービス再開には、パスワードや本人確認が必要となっている。	パスワードの一定回数以上の誤入力でサービスを停止している場合が多い。 サービス再開には、パスワードや本人確認が必要となっている。
	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)	重要なパスワードを忘れた場合は、電話または書面による手続きを必要とするところが多い。	重要なパスワードを忘れた場合は、電話または書面による手続きを必要とするところが多い。
	住所変更時のなりすまし	サイト上で手続きできる場合、書面や窓口での手続きしかできない場合に分かれる。	サイト上で手続きできる場合、書面や窓口での手続きしかできない場合に分かれる。
	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保護を行っている。	128bit SSLの暗号通信方式による通信路保護を行っている。
	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となる。	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となる。
ID・パスワードの不正入手等を防ぐための対策における課題		インターネット上でID・パスワードの不正入手等を防ぐために、高いレベルの方策が実施されている。	インターネット上でID・パスワードの不正入手等を防ぐための方策は、銀行によってバラツキがある。セキュリティ対策が遅れている銀行の底上げが重要となる。
総評		○	○／△

(2) 証券会社

		証券会社	
		大手、準大手証券会社	ネット証券会社
個人認証方式		認証方式は、ID＋パスワードが多い。 多要素認証の導入は低い。	認証方式は、ID＋パスワードが多い。 多要素認証の導入は低い。
初回登録時の本人確認		口座開設を必須にすることにより、本人確認するとともに、IDやパスワードを返送不要で郵送している。	口座開設を必須にすることにより、本人確認するとともに、IDやパスワードを返送不要で郵送している。
IDの実体		口座番号がIDとなることが多い。	口座番号とは異なる英数字を付与されることが多い。
パスワードの実体		任意に設定させるもの、郵送で送付するものを組み合わせることで高いセキュリティを確保している。	任意に設定させるもの、郵送で送付するものを組み合わせることで高いセキュリティを確保している。
ワンタイムパスワードの利用		ほとんど導入されていない。	ほとんど導入されていない。
個人認証制度の課題		株取引というタイミングが重要なサービスを提供しているため、利便性を重視しているところが多く、多要素認証の導入も進んでいない。利用者の利便性を失うことなく、セキュリティを高めることができるような施策を展開することが必要である。	株取引というタイミングが重要なサービスを提供しているため、利便性を重視しているところが多く、多要素認証の導入も進んでいない。利用者の利便性を失うことなく、セキュリティを高めることができるような施策を展開することが必要である。
ID・パスワードの不正入手等を防ぐための対策	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を提供をしている。 キー配列は、固定と変動のどちらも存在する。	ソフトウェアキーボードによるパスワード入力手段を提供をしている。 キー配列は、固定と変動のどちらも存在する。
	パスワード入力時の覗き見	●●●●の暗号化表示に対応している。	●●●●の暗号化表示に対応している。
	フィッシングサイトによるID・パスワードの不正入手	特に対策していない。	特に対策していない。
	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や推測しやすいパスワード設定を行わないことなどを利用者へ注意喚起している。	定期的にパスワードを変更することや推測しやすいパスワード設定を行わないことなどを利用者へ注意喚起している。
	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利用が一時停止されるが、一定時間が経過すれば解除されることが多い。	パスワードの一定回数以上の誤入力でサービス利用が一時停止されるが、一定時間が経過すれば解除されることが多い。
	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）	重要なパスワードを忘れた場合は、電話または書面による手続きを必要とするところが多い。	重要なパスワードを忘れた場合は、電話または書面による手続きを必要とするところが多い。
	住所変更時のなりすまし	サイト上で手続きできない場合が多い。	サイト上で手続きできない場合が多い。
	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保護を行っている。	128bit SSLの暗号通信方式による通信路保護を行っている。
	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となる。	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となる。
ID・パスワードの不正入手等を防ぐための対策における課題		銀行に比べて、フィッシング対策については非常に遅れている。証券業界全体の底上げが必要となる。	銀行に比べて、フィッシング対策については非常に遅れている。証券業界全体の底上げが必要となる。
総評		△	△

(3) インターネット・オークション、オンラインゲーム、オンラインショップ

		インターネット・オークション	オンライングーム
個人認証方式		認証方式は、ID＋パスワードが多い。 多要素認証の導入は低い。	認証方式は、ID＋パスワードが多い。 共通サービスの個人認証に、個別ゲームの個人認証と二階建てにしている企業が多い。 多要素認証の導入はバラツキがある。
初回登録時の本人確認		会員登録が必須となっている。 登録メールアドレスへのメール送付でメールアドレス確認し、本人確認を行っている。	会員登録が必須となっている。 登録メールアドレスへのメール送付でメールアドレス確認し、本人確認を行っている。
IDの実体		任意の英数字を登録するか、メールアドレスをそのままIDとすることが多い。	任意の英数字を登録するか、メールアドレスをそのままIDとすることが多い。
パスワードの実体		オンライン上ですべて取得できる。	オンライン上ですべて取得できる。
ワンタイムパスワードの利用		ほとんど導入されていない。	ほとんど導入されていないが、メールによるワンタイム認証を行っている企業もあり、対応にバラツキがある。
個人認証制度の課題		利便性を重視しているところが多く、パスワードの複数利用も、多要素認証の導入も進んでいない。利用者の利便性を失うことなく、セキュリティを高めることができるような施策を展開することが必要である。	利便性を重視しているところが多く、パスワードの複数利用も、多要素認証の導入も企業によってバラツキが大きい。オンラインゲームというサービスの特性から、利用者の属性も若年層から幅広く対応する必要があると思われる。利用者の利便性を失うことなく、セキュリティを高めることができるような施策を展開することが必要である。
ＩＤ・パスワードの不正入手等を防ぐための対策	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していない。	ソフトウェアキーボードは採用していない。
	パスワード入力時の覗き見	●●●●の暗号化表示に対応している。	●●●●の暗号化表示に対応している。
	フィッシングサイトによるID・パスワードの不正入手	特に対策していない。	特に対策していない。
	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や推測しやすいパスワード設定を行わないことなどを利用者へ注意喚起している。	定期的にパスワードを変更することや推測しやすいパスワード設定を行わないことなどを利用者へ注意喚起している。
	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を停止している場合が多い。 サービス再開には、パスワードや本人確認が必要となっている。	パスワードの一定回数以上の誤入力でサービスを停止している場合が多い。 サービス再開には、パスワードや本人確認が必要となっている。
	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）	オンライン上で手続きできる。 メール送付、記載のURLにアクセスすることで本人確認することが多い。	オンライン上で手続きできる。 メール送付、記載のURLにアクセスすることで本人確認することが多い。
	住所変更時のなりすまし	住所変更は、サイト上で行える。	住所変更は、サイト上で行える。
	インターネット上の経路における盗聴	SSLの暗号通信方式による通信路の保護を行っている。	SSLの暗号通信方式による通信路の保護を行っている。
	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となる。	特になし。
ID・パスワードの不正入手等を防ぐための対策における課題		フィッシング対策については、バラツキがある。 業界全体の底上げが必要となる。	フィッシング対策については、バラツキがある。 業界全体の底上げが必要となる。
総評		（企業間の違いが大きく一概に評価できない。）	（企業間の違いが大きく一概に評価できない。）

		オンラインショップ
個人認証方式		認証方式は、ID＋パスワードが多い。 多要素認証の導入は低い。
初回登録時の本人確認		会員登録が必須となっている。 登録メールアドレスへのメール送付でメールアドレス確認し、本人確認を行っている。
IDの実体		任意の英数字を登録するか、メールアドレスをそのままIDとすることが多い。
パスワードの実体		オンライン上ですべて取得できる。
ワンタイムパスワードの利用		ほとんど導入されていない。
個人認証制度の課題		利便性を重視しているところが多く、パスワードの複数利用も、多要素認証の導入も進んでいない。利用者の利便性を失うことなく、セキュリティを高めることができるような施策を展開することが必要である。
ID・パスワードの不正入手等を防ぐための対策	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していない。
	パスワード入力時の覗き見	●●●●の暗号化表示に対応している。
	フィッシングサイトによるID・パスワードの不正入手	特に対策していない。
	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や推測しやすいパスワード設定を行わないことなどを利用者へ注意喚起している。
	パスワード（またはID）の総当り攻撃	特に対策していない。
	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）	オンライン上で手続きできる。 メール送付、記載のURLにアクセスすることで本人確認することが多い。
	住所変更時のなりすまし	住所変更は、サイト上で行える。
	インターネット上の経路における盗聴	SSLの暗号通信方式による通信路の保護を行っている。
	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となる。
ID・パスワードの不正入手等を防ぐための対策における課題		フィッシング対策については、バラツキがある。 業界全体の底上げが必要となる。
総評		（企業間の違いが大きく一概に評価できない。）