1.4 その他銀行

その他銀行では、その他A行、その他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 17 その他銀行における個人認証方式

項番	調査項目		その他A行	その他B行
1	個人認証方式		ID＋パスワード+乱数表	ID＋パスワード
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(郵送)、第1パスワード(申込書記入)、第2パスワード(郵送)が必要で、第3パスワードの乱数表を登録	口座開設が必要(本人確認書類添付) ID＋第1パスワード(郵送)、第2パスワード(申込書記入)
3	IDの実体		半角数字10桁(3桁店番号と7桁口座番号)	口座番号とは別の半角数字10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(数字4桁)	パスワード通知書に記載 初回ログイン時に、任意の半角英数字4～11桁に変更
		第2パスワード	デフォルトは、口座開設時に登録された生年月日YYYYMMDD 初回ログイン時に半角英数字6桁～12桁に変更する	半角数字6桁
		第3パスワード	乱数表から、ログイン画面で指定された指示(配置)に従って英数字1桁×3を入力	なし
		ワンタイムパスワード	なし	なし
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ログイン 残高照会 入出金の明細照会	インターネットバンキングへのログイン 残高照会 入出金の明細照会
		第2パスワードが必要	インターネットバンキングへのログイン 残高照会 入出金の明細照会	振込、振替 定期預金への振替など
		第3パスワードが必要	振込、振替 振込限度額変更など	なし

図表 18　その他銀行における 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	その他A行	その他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	ソフトウェアキーボードの採用なし
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	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
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		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 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
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、電話での手続きが必要	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、電話での手続きが必要
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）		第1パスワードがわからなくなった場合は、電話による手続きの上、郵送 第2パスワードがわからなくなった場合は、電話による手続きの上、「初期パスワード」で利用開始登録	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		インターネットバンキングで手続き可能サイトでの手続き後、本人確認書類を郵送	インターネットバンキングで手続きは不可郵送または窓口での手続きが必要
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) その他Ａ行

①　個人認証方式

個人認証方式としては、ID（店番号と口座番号）＋第１パスワード（暗証番号）＋第２パスワード（パワーダイレクトパスワード）＋第３パスワード（セキュリティカード乱数表）が採用されている。

IDとなる「店番号と口座番号」は、10桁（3桁の店番号と7桁の口座番号）となっており、口座開設後に郵送されるキャッシュ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、口座開設時に設定した数字４桁の番号で、キャッシュカードの暗証番号と同じものである。

第２パスワードとなる「パワーダイレクトパスワード」は、「初期パスワード」として、口座開設時に登録された生年月日を西暦 YYYYMMDD 形式で入力する。初回ログイン時に６桁～12桁の英数字に変更を行う。

第３パスワードとなる「セキュリティカード乱数表」は、「セキュリティカード」に記載された乱数表から、ログイン画面で指定された指示（配置）に従って半角英数字１桁を３つ入力する。初回ログイン時には、「セキュリティカード」に記載されている 15 桁の「セキュリティカード番号」をサイト上から登録し、「セキュリティカード」の有効化を行わなければならない。

②　初回登録時の本人確認

インターネットバンキングを利用するには口座開設が必要になる。窓口で口座開設をする場合は、その場で４桁暗証番号の登録をする。

インターネットバンキングをするには、初回ログイン時に、「パワーダイレクトパスワード」と後日郵送される「セキュリティカード」番号の登録を行う。

③　パスワード入力が必要な手続き

ログインには、「店番号」＋「口座番号」、「暗証番号」、「パワーダイレクトパスワード」が必要になる。

ログイン後の取引には、「セキュリティカード乱数表」の数字が要求される。

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

セキュリティの観点から、ソフトウェアキーボードの使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。通常のキーボードで入力をしたい場合は、ソフトウェアキー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

「通知Eメール」に登録すると、通知メールアドレスを登録・変更・削除した時、振込・振替の取引が完了できなかった時（振込エラー）、ATM出金・J-Debitの利用限度額を変更した時、海外ATMで出金した時、振込・振替限度額を変更した時、パワー預金から円普通預金への振替限度額を変更した時、「パワーダイレクトパスワード」を変更した時、「電子お取引レポート」が更新された時、為替レート通知に登録し設定した条件になった時に通知メールが発信される。

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

「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。

また、簡単に推測されやすい暗証番号（生年月日の年年年年・年年月月・月月日日）、電話番号（「03」「06」ではじまる電話番号の中の連続4桁）、連続した番号（「0123」「1234」「2345」等）、同一の番号（「0000」「1111」「2222」及び「0111」など）は登録が制限されている。

⑦ パスワード（またはID）の総当り攻撃

セキュリティ確保のため、一定回数以上にパスワードの入力を間違えると、サービスが停止される。その場合は、電話にて「パスワードリセット」の手続きを依頼し、リセット後は、「パワーダイレクトパスワード」入力欄に、「初期パスワード」として、利用者の生年月日を西暦8桁のYYYYMMDD形式で入力の上、再度、利用開始登録を行う必要がある。

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）

「暗証番号」を忘れた場合、利用者のセキュリティを守るため銀行では調べることができない仕組みとなっている。電話にて依頼し、再度、仮暗証番号を送付してもらう。

「パワーダイレクトパスワード」を忘れた場合も、銀行では調べることができない仕組みとなっている。電話にて依頼し、「パワーダイレクトパスワード」をリセットし、「初期パスワード」（利用者の生年月日を西暦8桁のYYYYMMDD形式）を入力の上、再度、利用開始登録を行う。

⑨ 住所変更時のなりすまし

住所変更は、インターネットバンキングでは行えない。サイト上で届出事項変

更届を印刷し、記入・捺印する。新住所・氏名・生年月日が確認できる本人確認書類を用意し、届出事項変更届と本人確認書類を同封の上、銀行まで郵送する。

⑩ インターネット上の経路における盗聴

128bit SSL により暗号化している。

⑪ ログイン状態・退席時の他人による操作

利用者のセキュリティ確保のため、一定時間操作をされない状態が続いた場合自動的にログアウトされる。再度取引を行う場合は、もう一度ログインから始める。

(2) その他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（ログインパスワード）＋第2パスワード（確認暗証番号）が採用されている。

IDとなる「契約者番号」は、郵送で送られる「パスワード通知書」に記載されている10桁の数字である。

第1パスワードとなる「ログインパスワード」も、「パスワード通知書」に記載されている。初回ログイン時に、ログインパスワードを4～11桁に変更する必要がある。

第2パスワードとなる「確認暗証番号」は、申込書類に記載した6桁の数字となる。

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場合には、口座開設が必要となる。

③ パスワード入力が必要な手続き

ログインには、「契約者番号」と「ログインパスワード」が必要となる。定期預金への振替等の取引の際には、「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

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

メールアドレスを登録すると、資金の移動が伴う取引の結果をメールにて知らせるサービスを提供している。

また、不正アクセスを利用者自身が事後的に確認できるよう、ログイン時に3回前までのアクセス時間を表示している。

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

利用者に対して、定期的にパスワードを変更すること推奨している。

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」、「確認暗証番号」を一定回数以上間違えると、パスワ

ードが無効になる。再発行手続きが必要であり、電話で依頼する。

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）

銀行では、利用者のパスワードを調べることはできない。「ログインパスワード」、「確認暗証番号」を忘れた場合は再発行手続きが必要であり、電話で依頼する。

⑨ 住所変更時のなりすまし

住所変更は、郵送または窓口での書面による手続きが必要となる。

⑩ インターネット上の経路における盗聴

128bit SSL 暗号化通信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

第三者に勝手に操作されることを防止するため、ログイン後、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。

1.5 ヒアリング調査（銀行）

(1) 都銀 A 行

訪問日時：2008 年 11 月 26 日
対応部門：広報部、営業開発部

① 個人向けインターネットバンキングの概況

現在の形の個人向けのインターネットバンキングサービスは、2003 年 3 月から開始されているが、3 行の合併により誕生した銀行であるため、それぞれの銀行におけるインターネットバンキングはそれより以前に開始されている。

個人向けのインターネットバンキングは、営業開発部の中に組織されたチームが担当となっている。銀行のホームページ自体は、個人業務部が担当しているが、その中で法人向けのバンキングについては、E ビジネス業務部が、個人向けのバンキングについては、営業開発部のインターネットバンキング担当チームが業務を担当している。6~7 名の陣容で業務を行っているため、かなり多忙となっている。

インターネットバンキングの契約を行っている利用者は、約 750 万人。1 人の利用者が、複数の口座を持っている場合も、インターネットバンキングの契約は 1 つで利用できるようになっている。個人向けの契約口座数の半分程度はインターネットバンキングの契約も行っている。但し、実際の利用率はそのうちの 1 割程度であり、まだまだ利用者は拡大できる可能性が高い。

新規に口座を開設する際には、インターネットバンキングの申込書もセットになっており、同時に申し込めるようになっている。「新生活キャンペーン」などにより、新しく大学生や社会人になった人々への利用を推進している。現在は「ネットで投資信託キャンペーン」により、インターネットバンキングで対象となる取引が行われた場合には手数料を一部キャッシュバックするなど利用者の拡大にも取り組んでいる。

月ベースで 10 万前後の利用者が新たにインターネットバンキングへの申込を行っており、新規口座開設の 8 割から 9 割は同時に申し込んでいる。

② 利用者層

幅広い年代で利用されているが、30 代～40 代の男性が最も多い。一般的に 20 代のインターネット利用率は高いが、インターネットバンキングの利用では、30 代に比べると少ない。

モバイルバンキングも同時に利用している人が多く、外出先ではモバイルバンキング、家ではインターネットバンキングと使い分けている。

高齢者は、操作に関する問い合わせが多い。

③ 新技術への対応

全国銀行協会の申し合わせで、インターネットバンキング等の不正利用での損害金に対して原則補償を打ち出している[1]。そのため、インターネットバンキング利用におけるさらなる安全性を求めて、2008年3月から専用トークンによるワンタイムパスワードが導入された。まだ開始して間もないため、専用トークンは何千という単位ででているだけである。ワンタイムパスワードは、月額の利用料は無料であるが、契約手数料を取っている。専用トークンの原価を考えると、採算ぎりぎりであり、契約手数料を無料化するまでは難しい。このような高いセキュリティを求める利用者は、セキュリティにうるさいというよりも、利用頻度が高く、利用金額も大きい人々であるため、付加的なサービスとしている。

また、不正利用による損害は、通常で50万円、会員になっている場合は100万円まで補償される保険が適用される。

合言葉と画像によるリスクベース認証も導入し、利用の安全を高めている。業界内での評判は高い。利用者からは「めんどくさい」「そこまでやらなくてもいいのでは」といった意見もあったが、セキュリティに対してそのような意見も持つ利用者は必ずいることから、想定の範囲内であった。

銀行からのメールに電子署名を付加することについては検討中である。フィッシング対策ガイドライン[2]でも「電子署名は顧客に送信する全てのメールに付与することが望ましい」とされているが、電子署名自体が、利用者への浸透が進んでおらず、電子署名をサポートしていないメーラーがあることや、電子署名に対する知識のない利用者にとっては、署名されたメールは怪しく感じるといったこともある。

現状では、インターネットバンキングの利用において、銀行側から利用者に電子メールを送るのは受付メールだけであり、URLのリンクなども貼る必要がない。そのため、電子署名の優先度は低く、慎重に検討しているところである。

PKIや生体認証は、個人向けサービスでは適さない技術と考える。セキュリティのレベルでいっても、ワンタイムパスワードとどちらが上か比較しづらく、使い勝手を考えると、ワンタイムパスワードを選択することになる。

新技術の情報収集は、セミナーやカンファレンスへの出席、セキュリティベンダーからの情報提供などで行っている。

---

[1]全国銀行協会より2008年2月に出された「預金等の不正な払戻しへの対応について」では、インターネットバンキングによる預金等の不正払戻しについて、銀行に過失がない場合でも、利用者自身の責任によらずに遭った被害については補償を行うこととしている。
http://www.zenginkyo.or.jp/news/entryitems/news200219_1.pdf（2008年12月25日取得）

[2]全国銀行協会も加盟するフィッシング対策協議会により2008年9月に出されたガイドライン。
http://www.antiphishing.jp/antiphishing_guide.pdf（2008年12月25日取得）

④ 問い合わせの多い内容

操作に関する問い合わせ、パスワードの失念に関する問い合わせが多い。ログインパスワードを失念したという問い合わせは、日に何百件と発生している。

パスワードを定期的に変更することを推奨しているが、長期間変更のない利用者に対してアラームを出したり、強制的に変更しないと利用できなくなるといったようなことはしていない。強制変更にしてしまうと、利用者はパスワードを覚えきれなくなり、結局、紙にメモしてしまうということが発生しやすいためである。

⑤ セキュリティとユーザビリティ

セキュリティを高めると、利用者の利便性が低くなるということはどうしても起こってしまう。現在の状況から、リスクベース認証までは利用者全員必須とし、トークンによるワンタイムパスワードは選択としている。

金融庁や全国銀行協会からの通達については、対応していかなくてはならないと考えている。銀行の足並みを揃えるためにも一定のガイドラインは必要である。

⑥ 利用者の安心を高める工夫

技術的には、利用者に安心してインターネットバンキングを利用してもらう環境は整えられている。今後は、利用者自身のセキュリティ意識も重要となってくる。ホームページにも4コマ漫画で表現したセキュリティガイドを掲載するなど、利用者自身のセキュリティ意識を高めるための普及啓蒙に力を入れている。

(2) 都銀 B 行

訪問日時：2008 年 11 月 28 日
対応部門：マスリテール事業部

① 個人向けインターネットバンキングの概況

個人向けのインターネットバンキングは、1997 年 1 月から開始され、現在の形でのサービスは 2000 年 11 月から開始されている。合併後、サービス名は変更されたが、サービス内容は変更されていない。

個人向けの口座は約 2700 万～2800 万口座の契約がある。その中で、インターネットバンキングの契約数は約 900 万となっている。インターネットバンキングの契約数の伸びは右肩あがりで、年間 90 万近く増加している。

個人向けのインターネットバンキングは、マスリテール事業部の中に組織されているインターネットバンキング担当グループが担当しており、12 名という陣容で業務を行っている。

② 利用者層

利用者層は、20 代、30 代、40 代が中心となっている。日本全体の高齢化に伴い、高齢の利用者も増えてきている。

従来は、ネットの知識がある人々がインターネットバンキングを利用していたが、利用者層が多様化し、窓口を経由しない新たな利用者の流れから、ネットの知識が低い人々に裾野が拡大している。

③ 新技術への対応

新しい技術に対する情報収集のために、カンファレンスやセミナーなどに積極的に出席している。また、社内の情報システム企画部からも技術動向についての情報を入手している。

PKI は、利用者のリテラシーがある程度必要であり、利用者自身での作業も必要となる。個人向けのサービスにおいては、利用者側で作業が必要なセキュリティ対策は実際には導入しづらいと考えている。

携帯を利用したトークンについては検討を行ったが、モバイルバンキングの利用者にとっても利用できるという観点から専用トークンが採用された。

リスクベース認証は、時間や場所に対するリスクを軽減するが、取引のリスクには効果が薄い。B 行では、既に乱数表による第 2 暗証、第 3 暗証を採用しており、リスクベース認証は、セキュリティ対策の方向性が異なる技術であるため採用していない。

④ セキュリティとユーザビリティ

セキュリティ対策と利便性は、バランスが必要である。リテラシーが高い層は、自分でセキュリティ対策ができるため、銀行側から提供するものはなるべく少なくし利便性を高める方がいい。反対に、リテラシーの低い層では、利便性も高いがセキュリティも高いワンタイムパスワードといった新しい技術が必要となる。リテラシーの高い層、低い層、その中間の層と 3 つの層を満足させることが重要である。

⑤ 利用者の安心を高める工夫

銀行側のシステムのセキュリティは厳しく、利用者側のコンピュータのセキュリティも高くなってきたため、昨今のネット犯罪は技術だけでは対応できない、アナログ犯罪というものが増加してきている。保険会社を名乗り、インターネットバンキングに契約していない人をターゲットにして「保険の還付に必要だから」などと理由をつけ、インターネットバンキングに申込をさせ、暗証情報が載ったカードが届いた時点でその情報を聞き取るといったように、手の込んだ犯罪も報道されるようになっている。

システム的な対策だけでなく、利用者に何が起こっているかを知ってもらい、わかりやすい対策を講じることがポイントとなっていく。利用者の普及啓蒙が今後重要になってくる。ホームページに啓発コンテンツ「やさしいセキュリティ教室」を掲載し、漫画の利用や新聞記事の引用で、手口を明確に記載し、利用者自身で対策を考えられるように工夫している。

(3) 地銀 E 行

訪問日時：2008 年 11 月 21 日
対応部門：個人営業部

① 個人向けインターネットバンキングの概況

個人向けのインターネットバンキングは、利用者からの要望もあり、1999 年 5 月から開始している。法人向けのインターネットバンキングのサービスは、これより遅れて 2006 年から開始している。

個人の口座数が約 120 万口座あるが、そのうちインターネットバンキングの利用契約がされているのは 3 万 8 千口座で 3%程度となっている。

法人向けのインターネットバンキングは、県内の中小企業を対象としているが、こちらもあまり普及していない。昨年の eTAX による税金支払の関係で契約する企業が増加し、現在は約 1000 社が利用している。

個人向けインターネットバンキングを担当している部署は、個人営業部で 1～2 人の陣容で企画、推進を行っている。テレフォンバンキングについては、別の組織が担当している。

個人向けのインターネットバンキングと、法人向けのインターネットバンキングでは、それぞれ担当する部門が異なる。利用者が異なるため、それぞれの部署に位置づけられているが、混乱することもある。

インターネットバンキング自体の利便性はあるが、県内でこのサービスが認知されていないことも普及が進まない要因のひとつになっている。全体の認知度を上げていくことが普及につながるといえる。

また、個人利用者の利便性ということでも、オンライントレードを行っているような利用者であれば、資金移動等で利用頻度も高いが、普通の個人利用者では振込といった取引は、月に 1～2 度あるかないかといった程度である。

インターネットバンキングの契約率を上げるため、サービス開始当初はパワーセールスを行い、現在もスポットで促進を行っている。しかし、インターネットバンキングの契約はするもの、実際には利用しないという契約者が増えてしまうという側面もある。

② 利用者層

地域全体の高齢化もあり、銀行の利用者層も全体的には高齢化しているが、インターネットバンキングの利用者に関しては、30 代～40 代が比較的多い。高齢の利用者は、テレフォンバンキングを利用する傾向がある。

今後の展開としては、若年層の利用者を増やしていきたい。新規口座開設の際には、インターネットバンキングの申込をセットにするなど工夫している。

③ 新技術への対応

個人向けのインターネットバンキングは、NTT データのシステムを利用している。

携帯電話を利用したワンタイムパスワードを 2007 年 5 月から導入している。現在は、利用は任意となっている。ワンタイムパスワードの利用申込はインターネットバンキングの利用者の半分程度で、実際に利用しているは 1 万人弱程度である

しかし、ワンタイムパスワードに対する利用者の関心は高く、若い層で問い合わせが多かった。シニア層でも、セキュリティに関心の高い利用者の関心が高かった。

新しい技術の関する情報収集は、インターネットバンキングのシステムを依頼しているベンダーから、そのシステムの付加サービスの案内ということでくる。銀行側では、そのサービスを追加するか検討し、最終的に判断している。

現在、導入しているセキュリティツール「nProtect Netizen（エヌプロテクト・ネチズン）」もベンダーからの紹介で導入を検討した。

東北地方の地銀 3 社とは、同じインターネットバンキングのシステムを利用しているということもあり、個人的にではあるが情報交換を行っている。

④ セキュリティとユーザビリティ

金融機関は、利用者の資産や情報を守ることが一番であるが、セキュリティでがんじがらめにしてしまうということではない。銀行側が、セキュリティを高めるサービスを提供する中で、利用者にサービスを選別してもらうということが必要になる。

例えば、ATM ロックという、通常は ATM が利用できない状態にし、利用するときだけ、携帯電話でロックを解除するというサービスがあるが、セキュリティは高いが利用しづらい面もある。メール通知サービスでは、妻が昼間、口座からお金を下ろしただけであっても、メールで通知が入り、かえって心配になるという面もある。

セキュリティの高さと利用しやすさのバランスは、銀行側で押し付けるのでなく、利用者に選別していってもらうことが重要であると考える。

金融庁、全国銀行協会などからもインターネットバンキングのセキュリティについては厳しくしていく方向性が示されている。

⑤ 利用者の安心を高める工夫

本人確認はしっかりと行っている。インターネットバンキングの利用は、口座開設していることが前提となる。口座開設の際の本人確認に加えて、インターネ

ットバンキングを利用する際にも、本人確認と意思確認を行っている。郵送による申込でも、本人確認書類のコピー添付が必要である。窓口でも申込では、その場で本人確認書類を確認し、返送不要で実住所に郵送することで確認をとっている。

⑥ 地銀としてのインターネットバンキング

地銀は、地域を基盤にしており、インターネットバンキングのいつでも、どこからでも、といったサービスとはうまく合致しない部分もある。しかし、インターネットバンキングは、既にチャネルのひとつとなっており、ホームページの情報提供も含めて、有効であると考えている。