# 実効性を重視する米国インターネットバンキングの認証対策

米国の金融当局は、インターネットバンキングの認証には、利用者の認識情報、所持装置、生体特性のうちの2つを併用する方法（複数要素認証）を導入することを求めているが、実際の運用はかなり柔軟なものとなっている。本稿では、実効性を重視する米国の認証強化の取り組みについて紹介する。

## 個人認証強化を進める米国金融当局

インターネットバンキングやインターネット取引における不正アクセスが多いのは、米国も日本と同様である。ユーザーIDやパスワードが盗まれ、赤の他人が不正な取引をする事件が後を絶たないのである。そこで米国の金融当局では、本人認証（本人であることの確認）を利用者の認識情報（その代表がパスワード）だけに頼らないよう金融機関に要請することが検討された。それにより発表されたのが、連邦準備制度理事会（FRB）や連邦預金保険公社（FDIC）など金融当局5機関で構成される連邦金融機関検査委員会（FFIEC）による「インターネットバンキング環境での認証方式に関するガイドライン」（2005年10月）である。

ガイドラインでは、「金融機関がインターネットを使ってサービスを提供する場合、そのWebサイトへのアクセスはパスワードなどの単一認証だけでは不十分」であり、「複数要素認証、多重認証などの方式を採用してリスクを軽減する必要がある」と記されている。そして、金融機関に対して2006年12月末までの対応を求めたのである。

## 複数要素認証の導入に向けた課題

複数要素認証の技術として最も普及しているのは、利用者の所持装置を利用する「ハードウェアトークン認証」であろう。利用者が金融機関のWebサイトへアクセスする際に、ユーザーIDと従来からの「利用者の認識情報」であるパスワードとともに、キーホルダーサイズの画面に表示されるワンタイムパスワードを入力する。利用者の所持装置を使うものには、このほかにソフトウェアの暗号鍵を事前に利用者のPCにダウンロードしておく「ソフトウェアトークン認証」がある。また、利用者の「生体特性」を使う方式では、指紋などを読取装置で認識して認証するものなどがある。

以上の方式に比べてより簡易なものでは「イメージ双方向認証」がある。利用者は事前にイメージ情報と本人確認用の質問と回答を登録しておく。登録に使ったPCからログインすると、入力されたユーザーIDからPCの識別情報を金融機関側で認識し、事前に登録されたイメージ情報が画面に表示される。利用者はこれにより金融機関の本物のWebサイトであることを確認できる。

NRIアメリカ
社長
**南　博通**（みなみひろみち）

**専門は金融サービスの事業戦略、IT戦略の調査・コンサルティング**

複数要素認証を実現する方式の多くは、一般顧客へ導入しようとすると、モノ（ハードウェアトークン、生体情報読み取り装置）を配付する場合にはコストがかかり、顧客が紛失した場合のリスクもある。ソフトウェアを配付する場合には顧客説明の手間がかかり、また顧客のITリテラシーの差も大きく、どのレベルに合わせるかといった問題もある。

## 柔軟に運用されるガイドライン

では実際に米国の金融機関はどのようにガイドラインを適用しているのだろうか。マネーセンターバンクと呼ばれる米銀ビッグ3についてその状況をみてみよう。

預かり資産規模で全米1位のシティバンクでは、法人顧客および超富裕層（プライベートバンキング）顧客と、一般個人顧客では異なった対応をしている。すなわち、前者では全顧客にハードウェアトークンを配付し、ワンタイムパスワードによる複数要素認証を実現しているが、後者に対しては従来の単一要素認証のままである。

バンクオブアメリカでは、2005年からすでにイメージ双方向認証を導入している。ただし強制はしておらず、この方式を利用するかどうかは顧客側の判断に委ねられている。

JPモルガン・チェース銀行では、複数要素認証の紹介などは行っていないが、顧客が通常ログインするPCを認識し、それと異なるPCからアクセスがあった場合は追加的な認証を行うことがあると、Webサイトで通知している。

このような柔軟な運用は当局も追認している。ガイドラインで設定された期限が近づいた2006年8月に、FFIECに対する代表的な質問とそれに対する回答が発表された。その回答のなかで、「多くの銀行業務の場合、単一要素だけの認証では不十分」としながらも、「多重認証やその他の手段よりも複数要素認証を推奨しているのではなく、リスクを軽減できればどのような方法でもよい」と述べられている。

## 実効性のある普及を重視する米国

米国の大手銀行では、少なくとも一般個人顧客に対しては複数要素認証を一律に導入することをしていない。当局も、複数要素認証にこだわらず多重認証でも問題ないとし、また銀行が導入・通知していれば、全顧客の利用徹底までは求めないとしている。セキュリティ方式の厳格さよりも効果を重視しようということであろう。ハードウェアの配付はコストの割に効果が小さいとみられている。銀行によっては、多額の振り込みが行われた場合には電話をかけて本人確認を行う。ITと人間系の組み合わせでITリテラシーの差を埋めようとするわけである。米国では、複数要素認証の導入・普及に実効性をもたせるために、文化や習慣に合わせた柔軟な対応を図っていると言うべきであろう。 ■