香港で進む銀行の不正アクセス対策

ますます巧妙化する不正アクセスに対する対策が、金融機関に強く求められている昨今、世界的金融センターのひとつである香港では、政府主導で踏み込んだ対策を銀行に求めている。本稿では、2005年５月の指針で求められることになった２要素認証の内容について、主要各行の採用事例に基づいて紹介する。

義務づけられた2要素認証

香港では、香港金融管理局、香港銀行公會、香港警察がインターネットバンキングへの不正アクセス対策について議論を続けてきたが、その三者が共同で2005年５月に指針を発表した。それは、ユーザーIDとパスワードに加えて、以下の３つの方法のいずれかの証認手続きを、６月から１年以内に各銀行が採用することを求めるものであった。

①セキュリティデバイスを使用したワンタイムパスワード

②SMS（携帯電話でのショートメッセージサービス）を利用したワンタイムパスワード

③香港政府が発行する電子証明による本人確認

従来のユーザーID・パスワードに、もう１つの認証要素を加えるという意味で、これを２要素認証という。なお、ワンタイムパスワードとは一時的に設定されるパスワードという意味である。

香港金融管理局副局長のW・ライバック氏は、指針の発表にあたり次のような声明を出している。「２要素認証の採用により、インターネットバンキングのセキュリティを強固とし、不正行為から銀行顧客を保護する。香港は、インターネットバンキングが安全で堅実な環境の下で繁栄し続けることができる規定を満たす、高度に発展した金融都市の最初の場所のひとつである」。近年、上海の台頭により香港の金融中心地としての地位が脅かされているなかで、官民一体で金融サービスの品質を向上し、その地位を堅持しようという決意がうかがわれる（http://www.info.gov.hk/hkma/eng/press/index.htm。5月30日の記事）。

各認証方式の事例と特徴

求められている新たな認証方式については、すでに採用事例がある。

①セキュリティデバイスの採用

セキュリティデバイスの採用事例としては、2005年６月から香港上海銀行で使われているハードウェアトークンがある。初回ログイン時には、郵送されたトークンの裏面に記載してある番号と、トークンに表示された乱数を入力し、さらに口座開設時に提示した本人確認書類である香港IDカード番号、もしくはパスポート番号の指定された数桁を入力してはじめて認証が行われる。この処理は、

NRI香港
グローバルシステムズディビジョン
マネージャー
廣井和紀（ひろいかずのり）
専門は証券バックオフィスシステムの開発

初回のログイン画面に表示される期間内に行わなければならず、トークンの誤配送、盗難や紛失の被害から顧客を保護している。次回からは、ユーザーID・パスワードと、トークンに表示されるワンタイムパスワードでログインが可能となる。セキュリティデバイスは、携帯すれば世界中どこからでもアクセスが可能で利便性が高いが、故障・紛失時の費用負担が利用者に求められる。

②SMSの利用

SMSによる認証は2005年6月からシティバンク香港で採用されている。ログインはこれまでと同様にユーザーIDとパスワードだけで可能だが、送金などリスクの高い手続きを行う際には、事前に登録した携帯電話にメールで送信された30分間有効のワンタイムパスワードが必要となる。

香港の携帯電話の普及率は、2005年7月時点で694万の人口に対して加入数が842万件あり、121%と非常に高い（電訊管理局の資料による）。SMSを利用した認証は、香港では受け入れられやすい仕組みと言えるであろう。ただし、日本のようにSMSの規格が異なる国ではワンタイムパスワードが受信できないという不便さもある。

③電子証明の利用

電子証明による証認方式は、2005年6月から東亜銀行で採用されている。香港では香港郵政発行のe-Certと呼ばれる電子証明が普及している。e-Certは、香港IDカードのメモリーチップに埋め込む方式が一般的だが、メモリーチップのない旧式のカード保持者のために、i-Keyと呼ばれるUSBメモリーやフロッピーディスクによる発行も行っている。東亜銀行でも、シティバンク香港と同様にリスクの高い手続き時が対象で、カードリーダーで読み取った香港IDカード上のe-Certと、そのe-Certのパスワードで本人確認を行う。

e-Certは、住所変更や自動車免許更新などの公共サービスや、オンラインショッピングでの本人確認などにも利用できる汎用性の高さがメリットだが、e-Certの発行・維持のために、毎年利用者に費用負担が生じる。

先行事例の行方に注目

香港では、緊急性の高い問題に対し、制度としては枠組みのみを標準化し、個別採用技術は各社の裁量に任せることで、短期間での導入を可能としている。結果として、主要各行が別々の方式を採用することとなった。ユーザーIDとパスワードのみの認証方法から、多要素認証が主流となりつつあるが、巧妙化していく不正アクセスの抜本的な解決策となり得るのか注目すべきところである。また、利用者の利便性、安全性、コストなどから、各国、各企業がどのような技術を採用するのか興味深い。日本においても、金融庁が多要素認証の検討を進めているようである。香港の一歩踏み込んだ取り組みはその参考となるはずである。 ■