

インターネット・バンキングにおけるセキュリティ対策事例

1. 銀行が講じるセキュリティ対策事例

- (1) ワンタイムパスワード(ハードウェアトークン、ソフトウェアトークン、お客さまが取引に利用しているパソコンのブラウザとは別の携帯電話等の機器への電子メール通知等)の採用
- (2) お客さまが取引に利用しているパソコンのブラウザとは別の、携帯電話等の機器を用いる取引認証の導入
- (3) お客さまのパソコンのウィルス感染状況を検知し、警告を発するソフトの導入と、場合により取引を遮断する対処
- (4) お客さまに対するセキュリティ対策ソフトの無償配布
- (5) トランザクション認証(ハードウェアトークン等でトランザクション署名を行うもの)の導入
- (6) リスクベース認証の導入・強化 等

2. 個人のお客さまに実施していただきたいセキュリティ対策事例等

- (1) 不正な払戻し被害を防止するために各銀行が導入し、または推奨しているセキュリティ対策に関するサービスを積極的に利用すること
- (2) パソコンの基本ソフト(OS)やウェブブラウザ等、インストールされている各種ソフトウェアを最新の状態に更新しておくこと
- (3) セキュリティ対策ソフトを導入するとともに、最新の状態に更新しておくこと
- (4) 万が一、ウィルスに感染した場合等でも被害を最小限度に抑えることができるように、振込・払戻し等の限度額を必要な範囲内でできるだけ低く設定すること
- (5) インターネットカフェやホテルなど複数の人が利用する共用のパソコンを使用したり、公衆Wi-Fiを使用して、インターネット・バンキングを利用することは極力避けること
- (6) ID・パスワード等について、次のような事項に留意していただくこと
 - ① ID・パスワード等は慎重に管理し、お客さま以外の第三者には教えない
 - ② ID・パスワード等を、パソコン、スマートフォンやクラウドサービス等にファイルや画像(写真)などで入力・保存しない
 - ③ パスワード等は定期的に変更するとともに、第三者から類推されやすいものに設定しない
 - ④ ID・パスワード等の入力を求めるメールを受信しても無視する

補償減額または補償せずの取扱いとなりうる事例について

・個人のお客さまにおけるインターネット・バンキングの不正な払戻しについて、「預金者過失あり・重過失」の場合には「個別対応」としているところ、当協会の会員銀行(一部)を対象に実施したアンケート調査によれば、各行の補償対応実務上、以下のような事例は補償を減額するまたは補償をしない取扱いとされている。

- (1) 銀行が複数回にわたり、個別的・具体的に注意喚起していたにもかかわらず、注意喚起された手口により騙されて、ID・パスワード等を入力してしまった場合
- (2) 警察や銀行等を騙る者に対し、安易に ID・パスワード等を回答してしまった、または安易に乱数表(暗証カード)を渡してしまった場合。その他、正当な理由もなく、ID・パスワード等を他人に教えてしまった場合
- (3) お客さまが ID・パスワード等を手帳等にメモしていたり、携帯電話等の情報端末等に保存しており、お客さまの不注意により当該手帳や携帯電話等が盗難等に遭う等して当該情報が盗取された場合
- (4) 以下のような事実があるにもかかわらず、取引先の銀行への通報を怠っていた間に犯行が行われた場合
 - ① 上記(1)～(3)の事例にあるようなケースに該当すること
 - ② 通帳記帳やインターネット・バンキングサービスへのログインなどにより、身に覚えのない預金残高の変動があることを認識していたこと
 - ③ お客さまのパソコン等がウィルス感染するなどにより、インターネット・バンキングで不正な払戻しが行われる可能性を認識していたこと