(参考)

2014年7月17日　一般社団法人全国銀行協会「法人向けインターネット・バンキングにおける預金等の不正な払戻しに関する補償の考え方」から

お客さまに講じていただくセキュリティ対策事例

1　法人のお客さまに実施していただくセキュリティ対策
(1) 銀行が導入しているセキュリティ対策の実施 **銀行が導入しているセキュリティ対策を着実に実施していただくこと**
(2) インターネット・バンキングに使用するパソコン（以下、単に「パソコン」という。）に関し、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いただくこと
(3) パソコンにインストールされている各種ソフトウェアで、メーカーのサポート期限が経過した基本ソフトやウェブブラウザ等の使用を止めていただくこと
(4) パソコンに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たうえで、稼動していただくこと
(5) インターネット・バンキングに係るパスワードを定期的に変更していただくこと
(6) 銀行が指定した正規の手順以外での電子証明書の利用は止めていただくこと
2　法人のお客さまに推奨するセキュリティ対策
(1) パソコンの利用目的として、インターネット接続時の利用は、インターネット・バンキングに限定していただくこと
(2) パソコンや無線ＬＡＮのルータ等について、未利用時は可能な限り電源を切断していただくこと
(3) 取引の申請者と承認者とで異なるパソコンを利用していただくこと
(4) 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していただくこと
(5) 不審なログイン履歴や身に覚えがない取引履歴、取引通知メールがないかを定期的に確認していただくこと

補償減額または補償せずの取扱いとなりうるケースについて

1　以下のような対応がお客さまに実施されていないケース
(1) 上記 1「法人のお客さまに実施いただくセキュリティ対策」の導入
(2) 身に覚えのない残高変動や不正取引が発生した場合の、一定期間内の銀行への通報
(3) 不正取引が発生した場合の、一定期間内の警察への通報
(4) パソコンに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たうえで、稼動していただくこと
(5) インターネット・バンキングに係るパスワードを定期的に変更していただくこと
(6) 銀行が指定した正規の手順以外での電子証明書の利用は止めていただくこと
2　お客さまに過失があると考えられる以下のような事象が認められたケース
(1) 正当な理由なく、他人にID・パスワード等を回答してしまった、あるいは、安易に乱数表やトークン等を渡してしまった場合
(2) パソコンや携帯電話等が盗難に遭った場合において、ID・パスワード等をパソコンや携帯電話等に保存していた場合
(3) 銀行が注意喚起しているにも関わらず、注意喚起された方法で、メール型のフィッシングに騙される等、不用意にID・パスワード等を入力してしまった場合
3　その他、以下のような事例に相当するケース
(1) 会社関係者の犯行であることが判明した場合
(2) その他、上記 2. の場合と同程度の注意義務違反が認められた場合