（別添１）

平成 26 年 7 月 17 日

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

一般社団法人全国銀行協会

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ついては、個人のお客さまのみならず、法人のお客さまにも被害が拡大していることから、今年 5 月、法人向けインターネット・バンキングに関するセキュリティ対策の強化ならびにお客さまへの注意喚起等について、申し合わせを行ったところである。その際、セキュリティ対策強化の継続的な検討に加え、被害補償の取り扱いについても、当協会の検討部会に外部有識者を招聘し検討することとした。

このような検討を通し、今般、当協会では、重要な金融インフラであるインターネット・バンキングの信頼性を高め、お客さまに安心してご利用いただくために、法人のお客さまに対する被害補償に関する考え方ならびに銀行とお客さまのセキュリティ対策事例等について、あらためて下記の通り申し合わせる。各会員銀行は、これらの申し合わせを踏まえ、インターネット・バンキング・サービスの不断の改善に努めていく。

記

これまで当協会は、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への補償については、「偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護等に関する法律」（以下、「預金者保護法」）の対象が個人であること等を踏まえ、個人のお客さまに関する申し合わせを行った。すなわち、銀行に過失がない場合でも、個人のお客さまがご自身の責任によらず遭われた被害は、銀行は補償を行うこととした（平成 20 年２月 19 日「預金等の不正な払戻しへの対応について」）。

しかしながら、最近は犯罪の手口が高度化・巧妙化し、法人のお客さまにも被害が拡大している。このため、インターネット・バンキングに関して、銀行ならびに法人のお客さまが一般的に必要とされるセキュリティ対策を実施しているにもかかわらず、サービスに内在するリスクの発現、すなわち正当な権限者が成りすまされる、あるいは送金情報が改ざんされる等の事態が生じる可能性があることを、あらためて認識したところである。

このような事態が生じるなか、銀行は、法的責任はないと考えられる場合であっても、継続的なサービスの提供や銀行の経営戦略等の観点から合理性があるとして、法人のお客さまの被害を補償するとの判断があると考えられる。

したがって、今後、会員銀行は、インターネット・バンキングの信頼性を高め、お客さまに安心してご利用いただくために、法人のお客さまの被害に対する補償を個別行の経営判断として検討するものとする。

ただし、預金者保護法の対象が個人のお客さまであることに示されている通り、一般に法人のお客さまによるセキュリティ対策等への対応力は、個人のお客さまに比べれば相対的に高いと考えられる。お客さまの利用環境やセキュリティレベルを原因として不正利用される可能性があるなかでは、サービスの提供者である銀行のセキュリティ対策に加え、サービスの利用者である法人のお客さまにもセキュリティ対策を講じていただき、サービスの提供者と利用者の双方が不正利用被害の防止に努めていくことが重要であると考えられる。

すなわち、銀行は、必要なセキュリティ対策を自ら講じていくとともに、法人のお客さまへの補償を具体的に検討する際には、以下の点を考慮することが考えられる。

- 法人のお客さまが別紙1に記載したセキュリティ対策を自ら講じ、不正利用被害の防止に努めていただいていること。なお、別紙2に事例として記載したようなケースが確認された場合には、補償を減額する、もしくは補償をしない取り扱いがあり得ること。
- 法人のお客さまの属性やセキュリティ対策への対応力等に応じて、補償の対象先や上限等を個別に決定すること。

以　上

（別紙 1）

銀行および法人のお客さまに求められ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) 銀行が講じるセキュリティ対策として、現時点では以下のような事例が挙げられ、各会員銀行は、これらを複数組み合わせて万全の対策を講じていく。

① 電子証明書のセキュリティ強化策

ａ．電子証明書を IC カード等、取引に利用しているパソコンとは別の媒体・機器へ格納する方式の採用

ｂ．電子証明書の権限情報付き再発行を不可とする方式の採用

② 認証方法の強化策

✓ 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）、または、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 資金窃取を防止する運用

✓ 事前登録先以外の振込先への受付日当日送金の不実施（ただし、お客さまが取引に利用しているパソコン画面で事前登録先の変更は不可とすることが前提）

④ セキュリティ対策ソフトの提供

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

⑦ 不正なログイン・取引等の検知

⑧ お客さまのセキュリティレベルに応じたサービスの提供

✓ サービス導入時にお客さまのセキュリティレベルを確認し、それに応じたサービス内容の提供を行う。

⑨ 上記のほか、会員銀行が有効と考えるセキュリティ対策

(2) 各会員銀行では上記の対策を実施し、お客さまに講じていただきたいセキュリティ対策に関する説明・周知や、不正利用が発生した際のお客さまへの連絡や問い合わせ・相談等に対するサポート対応などの必要な態勢を整備する。

2. お客さまに講じていただくセキュリティ対策事例

- お客さまに講じていただくセキュリティ対策として、現時点では以下のような事例が挙げられる。銀行は、法人のお客さまに(1)に挙げる対策を実施していただくよう周知するとともに、(2)の対策についても実施を推奨する。

(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 ✓ 上記 1.に記載のものを含め、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

- 以下のようなケースでは、会員銀行はそれぞれの事情を個別に判断したうえで、補償を減額する、もしくは補償をしない取り扱いとすることが考えられる。

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) （別紙１） ２．（１）の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) 不正取引が発生した場合の、銀行による調査および警察による捜査への協力
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