（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