【インターネットバンキング】

フェーズ		リスク			
		項目		本検討会で検討した主なリスクの例	
Ⅰ	金融機関内のシステム・体制の構築	1	事務委託業者・システム構築業者等による口座情報・暗証番号等の流出	①	ID・パスワード等が適切に管理されない
Ⅱ	インターネット・バンキング利用時	1	スパイウェアによりIDと認証情報が漏洩する	①	電子メールの添付ファイルやCD－ROMに含まれていたスパイウェアに感染する
				②	顧客が最新式のアンチ･ウイルス・ソフトを用いていないため、スパイウェアに感染する
		2	フィッシングサイトにおいてIDと認証情報が詐取される	①	金融機関の名を騙ったフィッシングメールにより、フィッシングサイトにアクセスするよう誘導される
		3	IDと認証媒体が盗難にあう	①	ID・パスワードが保存された顧客のパソコンが盗難にあう
				②	キーロガーが仕掛けられたインターネットカフェのパソコンで、ID／認証情報が盗取される
				③	乱数表やID・パスワードが記載されたカードを一箇所に保管していたところ、両方とも盗難にあう
		4	パスワードの再交付過程で漏洩する	①	類推可能なリマインダ登録により、パスワードが盗取される
Ⅲ	被害発生時	1	異常取引を検知しにくい	①	通知先のメールアドレスが勝手に変更され、異常取引に気付くのが遅れる
		2	公表・周知が遅れる	①	事案の公表、顧客への周知等に関する態勢が不十分
		3	手口に係る証拠の確保ができず、原因が究明できない	①	個別のスパイウェアの型が確保できないため、ベンダーがアンチウィルスソフトなどの改良に手間取る
Ⅳ	事後対応	1	金融機関間での適時の情報共有ができず、被害が他金融機関にも拡大する	①	被害状況・手口等に関する情報の共有が遅れる
		2	被害の偽装	①	スパイウエア等の被害にあったと偽装される

【インターネットバンキング】

フェーズ		リスク			
		項目		本検討会で検討した主なリスクの例	
Ⅴ	業務の正常な継続	1	ボットネット(注3)等の外部からのシステム攻撃	①	ボットネットにとりこまれたパソコンから金融機関のサーバーが一斉に攻撃を受ける
		2	障害発生時	①	顧客をATMシステムなどの代替システムに円滑に誘導できない
		3	取引が集中した場合	①	処理能力を超えた取引要求により、長時間のシステム障害を起す

（注1） 上記リスクは、本検討会において検討したリスクの一例であり、検討の全てではない。

（注2） 上記リスクは、国内及び外国において既発生の手口、可能性が指摘されているリスクをもとに列挙したものであるが、将来にわたる全てのリスクを網羅するものでない一方、列挙した全てが顕在化すると限らず、国内の現状においては現実的でないリスクも含まれている。各金融機関は顧客や業務の特性に応じてリスクを選別し、対策を講じることが必要である。

（注3） PCがある種のウィルスに感染することにより、悪意の第三者が遠隔から各PCに対して命令を発し、不正活動を行わせることが可能になる。そのようなウィルスに感染した多数のPCのネットワークを「ボットネット」という。