（１）中小・地域金融機関向けの総合的な監督指針

| 改正案 | 現行 |
| --- | --- |
| Ⅱ　銀行監督上の評価項目<br>Ⅱ－３　業務の適切性等<br>Ⅱ－３－５　インターネットバンキング<br>Ⅱ－３－５－２　主な着眼点<br>（１）略<br>（２）セキュリティの確保<br>情報セキュリティに関する検討会の検討内容等を踏まえ、体制の構築時及び利用時の各段階におけるリスクを把握した上で、自らの顧客や業務の特性に応じた対策を講じているか。また、個別の対策を場当たり的に講じるのではなく、効果的な対策を複数組み合わせることによりセキュリティ全体の向上を目指すとともに、リスクの存在を十分に認識・評価した上で対策の要否・種類を決定し、迅速な対応が取られているか。<br><br>インターネットバンキングに係る情報セキュリティ全般に関するプログラムを作成し、各種犯罪手口に対する有効性等を検証した上で、必要に応じて見直す態勢を整備しているか。また、プログラム等に沿って個人・法人等の顧客属性を勘案しつつ、「金融分野におけるサイバーセキュリティに関するガイドライン」や全国銀行協会の申し合わせ等も踏まえ、取引のリスクに見合ったセキュリティ対策を講じているか。その際、犯罪手口の高度化・巧妙化等（「中間者攻撃」や「マン・イン・ザ・ブラウザ攻撃」など）　を考慮しているか。<br><br>また、フィッシング詐欺対策については、メールやSMS（ショートメッセージサービス）内にパスワード入力を促すページのURLやログインリンクを記載しない（法令に基づく義務を履行するために必要な場合など、その他の代替的手段を採り得ない場合を除く。）、利用者に対して正規のウェブサイトのブックマークや正規のアプリからログインすることを促す、送信ドメイン認証技術の計画的な導入、フィッシングサイトの閉鎖促進等、業務に応じた適切な不正防止策を講じているか。<br><br>（注）情報の収集に当たっては、金融関係団体や金融情報システムセンターの調査等のほか、情報セキュリティに関する検討会や金融機関防犯連絡協議会における検討結果、金融庁・警察当局から提供された犯罪手口に係る情報などを活用することが考えられる。<br><br>（参考）<br>・セキュリティ対策向上・強化等に関する全国銀行協会の「申し合わせ」（平成24年１月、25年11月、26年５月、26年７月等）<br>・インターネット・バンキングにおいて留意すべき事項について（全国銀行協会）<br>・金融機関等コンピュータシステムの安全対策基準・解説書（金融情報システムセンター）<br>・情報セキュリティに関する検討会における検討資料<br><br>業務内容に応じて、以下の不正防止策を講じているか。また、内外の環境変化や事故・事件の発生状況を踏まえ、定期的かつ適時にリスクを認識・評価し、必要に応じて、認証方式等の | Ⅱ　銀行監督上の評価項目<br>Ⅱ－３　業務の適切性等<br>Ⅱ－３－５　インターネットバンキング<br>Ⅱ－３－５－２　主な着眼点<br>（１）略<br>（２）セキュリティの確保<br>情報セキュリティに関する検討会の検討内容等を踏まえ、体制の構築時及び利用時の各段階におけるリスクを把握した上で、自らの顧客や業務の特性に応じた対策を講じているか。また、個別の対策を場当たり的に講じるのではなく、効果的な対策を複数組み合わせることによりセキュリティ全体の向上を目指すとともに、リスクの存在を十分に認識・評価した上で対策の要否・種類を決定し、迅速な対応が取られているか。<br><br>インターネットバンキングに係る情報セキュリティ全般に関するプログラムを作成し、各種犯罪手口に対する有効性等を検証した上で、必要に応じて見直す態勢を整備しているか。また、プログラム等に沿って個人・法人等の顧客属性を勘案しつつ、「金融分野におけるサイバーセキュリティに関するガイドライン」や全国銀行協会の申し合わせ等も踏まえ、取引のリスクに見合ったセキュリティ対策を講じているか。その際、犯罪手口の高度化・巧妙化等（「中間者攻撃」や「マン・イン・ザ・ブラウザ攻撃」など）　を考慮しているか。<br><br>ウェブページのリンクに関し、利用者が取引相手を誤認するような構成になっていないか。また、フィッシング詐欺対策については、利用者がアクセスしているサイトが真正なサイトであることの証明を確認できるような措置を講じる等、業務に応じた適切な不正防止策を講じているか。<br><br>（注）情報の収集に当たっては、金融関係団体や金融情報システムセンターの調査等のほか、情報セキュリティに関する検討会や金融機関防犯連絡協議会における検討結果、金融庁・警察当局から提供された犯罪手口に係る情報などを活用することが考えられる。<br><br>（参考）<br>・セキュリティ対策向上・強化等に関する全国銀行協会の「申し合わせ」（平成24年１月、25年11月、26年５月、26年７月等）<br>・インターネット・バンキングにおいて留意すべき事項について（全国銀行協会）<br>・金融機関等コンピュータシステムの安全対策基準・解説書（金融情報システムセンター）<br>・情報セキュリティに関する検討会における検討資料<br><br>（新設） |

| | |
|---|---|
| 見直しを行っているか。<br><br>・ログイン、出金など、重要な操作時におけるフィッシングに耐性のある多要素認証（例：パスキーによる認証、PKI（公開鍵基盤）をベースとした認証）の実装及び必須化（デフォルトとして設定）<br>（注１）フィッシングに耐性のある多要素認証の実装及び必須化以降、顧客が設定に必要な機器（スマートフォン等）を所有していない等の理由でやむを得ずかかる多要素認証の設定を解除する場合には、代替的な多要素認証を提供するとともに、解除率の状況をフォローした上で、認証技術や規格の発展も勘案しながら、解除率が低くなるよう多要素の認証の方法の見直しを検討・実施することとする。<br>（注２）フィッシングに耐性のある多要素認証を実装及び必須化するまでの暫定的な対応として、代替的な多要素認証を提供する場合には、当該実装及び必須化に係る具体的なスケジュールについて顧客に周知するとともに、それまでの期間においても、振る舞い検知やログイン通知等の検知機能を強化する必要がある。<br>・顧客が身に覚えのない第三者による不正なログイン・取引を早期に検知するため、電子メール等により、顧客に通知を送信する機能の提供<br>・認証に連続して失敗した場合、ログインを停止するアカウント・ロックの自動発動機能の実装及び必須化<br>・顧客のログイン時の挙動の分析による不正アクセスの検知（ログイン時の振る舞い検知）及び事後検証に資するログイン・取引時の情報の保存の実施<br>・不正アクセスの評価に応じて追加の本人認証を実施するほか、当該不正が疑われるアクセスの適時遮断、不正アクセス元からのアクセスのブロック等の対応の実施<br>・不正なログイン・異常な取引等を検知し、速やかに利用者に連絡する体制と仕組みの整備<br><br>（参考）<br>・金融機関等コンピュータシステムの安全対策基準・解説書（金融情報システムセンター）<br>・フィッシング対策ガイドライン（フィッシング対策協議会） | |
| （３）顧客対応<br>インターネット上での暗証番号等の個人情報の詐取の危険性、類推されやすい暗証番号の使用の危険性（認証方式においてパスワードを利用している場合に限る。）、被害拡大の可能性（対策として、振込限度額の設定等）等、様々なリスクの説明や、顧客に求められるセキュリティ対策事例の周知を含めた注意喚起等が顧客に対して十分に行われる態勢が整備されているか。<br><br>顧客自らによる早期の被害認識を可能とするため、顧客が取引内容を適時に確認できる手段を講じているか。<br><br>顧客からの届出を速やかに受け付ける体制が整備されているか。また、顧客への周知（公表を含む。）が必要な場合、速やかにかつ顧客が容易に理解できる形で周知できる体制が整備されているか。特に、被害にあう可能性がある顧客を特定可能な場合は、可能な限り迅速に顧客 | （３）顧客対応<br>インターネット上での暗証番号等の個人情報の詐取の危険性、類推されやすい暗証番号の使用の危険性、被害拡大の可能性（対策として、振込限度額の設定等）等、様々なリスクの説明や、顧客に求められるセキュリティ対策事例の周知を含めた注意喚起等が顧客に対して十分に行われる態勢が整備されているか。<br><br>顧客自らによる早期の被害認識を可能とするため、顧客が取引内容を適時に確認できる手段を講じているか。<br><br>顧客からの届出を速やかに受け付ける体制が整備されているか。また、顧客への周知（公表を含む。）が必要な場合、速やかにかつ顧客が容易に理解できる形で周知できる体制が整備されているか。特に、被害にあう可能性がある顧客を特定可能な場合は、可能な限り迅速に顧客に連絡するなどして被害を最小限に抑制するための措置を講じることとしているか。 |

| | |
|---|---|
| に連絡するなどして被害を最小限に抑制するための措置を講じることとしているか。<br><br>不正取引を防止するための対策が利用者に普及しているかを定期的にモニタリングし、普及させるための追加的な施策を講じているか。<br><br>不正取引に係る損失の補償については、預貯金者保護法及び全国銀行協会の申し合わせの趣旨を踏まえ、利用者保護を徹底する観点から、個人顧客及び法人顧客への対応方針等を定めるほか、真摯な顧客対応を行う態勢が整備されているか。<br><br>不正取引に関する記録を適切に保存するとともに、顧客や捜査当局から当該資料の提供などの協力を求められたときは、これに誠実に協力することとされているか。<br><br>（４）略 | 不正取引を防止するための対策が利用者に普及しているかを定期的にモニタリングし、普及させるための追加的な施策を講じているか。<br><br>不正取引に係る損失の補償については、預貯金者保護法及び全国銀行協会の申し合わせの趣旨を踏まえ、利用者保護を徹底する観点から、個人顧客及び法人顧客への対応方針等を定めるほか、真摯な顧客対応を行う態勢が整備されているか。<br><br>不正取引に関する記録を適切に保存するとともに、顧客や捜査当局から当該資料の提供などの協力を求められたときは、これに誠実に協力することとされているか。<br><br>（４）略 |
| Ⅱ－３－５－３（略） | Ⅱ－３－５－３（略） |
| Ⅱ－３－６（略） | Ⅱ－３－６（略） |
| Ⅱ－３－６－２ 主な着眼点<br>（１）（略）<br><br>（２）セキュリティの確保<br>①、②略<br>③ 預金口座との連携を行う際に、サービスの内容に応じてⅡ－３－５－２（２）に記載している対策（フィッシング詐欺対策やフィッシング耐性のある多要素認証）を実施すること等により預金者へのなりすましを阻止しているか。<br><br>（注）実効的な認証方式についてはⅢ－３－７－１－２（５）②を参照。なお、実効的な認証方式などのセキュリティ対策は、情報通信技術の進展により様々な方式が新たに開発されていることから、定期的又は必要に応じて見直しを行う必要があることに留意。<br><br>④～⑨（略）<br><br>（参考）<br>・「資金移動業者等との口座連携に関するガイドライン」（令和２年 11 月 30 日：全国銀行協会）<br><br>（３）（略） | Ⅱ－３－６－２ 主な着眼点<br>（１）（略）<br><br>（２）セキュリティの確保<br>①、②略<br>③ 預金口座との連携を行う際に、固定式の ID・パスワードによる本人認証に加えて、ハードウェアトークン・ソフトウェアトークンによる可変式パスワードを用いる方法や公的個人認証を用いる方法などで本人認証を実施するなど、実効的な要素を組み合わせた多要素認証等の導入により預金者へのなりすましを阻止する対策を導入しているか。<br><br>（注）実効的な認証方式についてはⅢ－３－７－１－２（５）②を参照。なお、実効的な認証方式などのセキュリティ対策は、情報通信技術の進展により様々な方式が新たに開発されていることから、定期的又は必要に応じて見直しを行う必要があることに留意。<br><br>④～⑨（略）<br><br>（３）（略） |

| | |
|---|---|
| Ⅳ－２　電子決済等取扱業<br>Ⅳ－２－３　システムリスク<br>Ⅳ－２－３－１　主な着眼点<br>（１）～（２）（略）<br>（３）<br>①サービスの内容に応じてⅡ－３－５－２（２）に記載している対策（フィッシング詐欺対策やフィッシング耐性のある多要素認証の実装及び必須化など）を実施しているか。<br>②Ⅱ－３－４－１－２（６）の事項に加え、システム設計／開発段階では、以下のような事項を含むセキュリティに係る措置を講じているか。<br>・具体的なセキュリティ要件の明確化<br>・セキュアコーディングの実施など脆弱なポイントが生じないための対策・他社のシステムと連携する場合、連携する部分を含めサービス全体を踏まえたセキュリティ設計　等 | Ⅳ－２　電子決済等取扱業<br>Ⅳ－２－３　システムリスク<br>Ⅳ－２－３－１　主な着眼点<br>（１）～（２）（略）<br>（３）<br>①Ⅱ－３－４－１－２（５）②の事例のほか、例えば、以下のような取引のリスクに見合った適切な認証方式を導入しているか。<br>イ．可変式パスワード、生体認証、電子証明書等、実効的な要素を組み合わせた多要素認証などの、固定式の ID・パスワードのみに頼らない認証方式<br>ロ．ログインパスワードとは別の取引用パスワードの採用（同一のパスワードの設定を不可とすること等の事項に留意すること。）<br>また、内外の環境変化や事故・事件の発生状況を踏まえ、定期的かつ適時にリスクを認識・評価し、必要に応じて、認証方式の見直しを行っているか。<br>②　Ⅱ－３－４－１－２（５）③に加え、例えば、以下のような業務に応じた不正防止策を講じているか。<br>・不正な IP アドレスからの通信の遮断<br>・利用者に対してウィルス等の検知・駆除が行えるセキュリティ対策ソフトの導入・最新化を促す措置<br>・不正なログイン・異常な取引等を検知し、速やかに利用者に連絡する体制の整備<br>・不正が確認された ID の利用停止<br>・前回ログイン（ログオフ）日時の画面への表示<br>・取引時の利用者への通知　等<br>③Ⅱ－３－４－１－２（６）の事項に加え、システム設計／開発段階では、以下のような事項を含むセキュリティに係る措置を講じているか。<br>・具体的なセキュリティ要件の明確化<br>・セキュアコーディングの実施など脆弱なポイントが生じないための対策・他社のシステムと連携する場合、連携する部分を含めサービス全体を踏まえたセキュリティ設計　等 |