

「中小・地域金融機関向けの総合的な監督指針」の一部改正(案)に対するご意見・ご質問

一般社団法人全国地方銀行協会

項番	該当箇所(頁、項番等)	意見
1	Ⅱ-3-5-2 全般	昨今のボイスフィッシング事案の発生等、犯罪者の手口が巧妙化する中で、金融機関が対策を講じていくことができるよう、新たな手口の発生時等に、金融機関が取り得る有効な対応策を示していただきたい。
2	Ⅱ-3-5-2(2)	今回の改正箇所ではないが、「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。」の記載がある。現在において、「中間者攻撃」や「マン・イン・ザ・ブラウザ攻撃」よりも喫緊の脅威となっている攻撃手法もあることから、例示を更新いただきたい。
3	Ⅱ-3-5-2(2)	「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」について、利用者への連絡手段としては、電話やメール等が考えられる。具体的にどのような連絡手段を採用するかは各行の実態に即して判断すべきものと理解してよいか。
4	Ⅱ-3-5-2(3)	今回の改正案において「(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。)」と追記した理由を示していただきたい。 「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」と記載されており、パスワードを利用していることが自明であると考えられるため。
5	Ⅱ-3-6-2(2)③	改正案では「預金口座との連携を行う際に～(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」とあるが、必ずしも金融機関側のシステムで「フィッシング耐性のある多要素認証」を行う必要があるわけではなく、預金口座との連携を行う際の一連の手続きフローの中で「フィッシング耐性のある多要素認証」が行われていることを確認することでも問題ないか。

以 上