2026 年 1 月 13 日

金融庁

総合政策局リスク分析総括課ITサイバー・経済安全保障監理官室　御中

一般社団法人全国銀行協会

「主要行等向けの総合的な監督指針」等の一部改正（案）
に対する意見について

2025年12月８日付で意見募集が開始された標題改正案について、別紙のとおり意見を提出いたしますので、何卒ご高配を賜りますようお願い申しあげます。

以　上

別紙

「主要行等向けの総合的な監督指針」等の一部改正（案）に対する意見

【総括】意見提出の趣旨

●今般の改正（案）については、近年増加しているサイバーリスクへの対応を強化するため、①メールやSMS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対策、②ログイン・出金等の重要操作時におけるフィッシング耐性のある多要素認証の実装および必須化の対策等が盛り込まれる改正と認識している。
●当協会の意見は、①の対策について個別顧客等へ送付するWEB会議リンク掲載メール等を対象外とすることおよび②の対策について多要素認証の必須化の見直し等を求める内容としている。

No.	項目	意見等
1	主要行向け：Ⅲ−3−8−2(2) 中小向け：Ⅲ−3−5−2(2)	「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」とあるが、以下のようなケースに、利用者側として受信が想定されるメールやSMSは、フィッシングメールと誤認し難く、本改正の対象とする必要性は無いと思われるため、対象外として明示いただきたい。 例：個別の従業員が、個別の顧客や委託先等とのやり取りにおいて、WEB会議ファイルサーバー等のログインリンクを掲載したメールを送付するもの
2	主要行向け：Ⅲ−3−8−2(2) 中小向け：Ⅲ−3−5−2(2)	「法令に基づく義務を履行するために必要な場合等、その他の代替的手段を採り得ない場合を除く。」とあるが、「その他の代替的手段を採り得ない場合」について、「法令に基づく義務を履行するために必要な場合」に限らず、「実務観点で代替手段がないと判断される場合」も含まれる認識でよいか。
3	主要行向け：Ⅲ−3−8−2(2) 中小向け：Ⅲ−3−5−2(2)	「法令に基づく義務を履行するために必要な場合等、その他の代替的手段を採り得ない場合を除く。」とあるが、業界横断でのガイドライン等を準備する予定はなく、代替手段の有無の判断基準も、監督指針のベースの考え方である個別行ごとにリスクベースでの判断になる認識でよいか。 なお、当該改正案箇所の内容を有効に機能させるためには、メールやSMS上のURLやログインリンクの記載方針を、個別行単位でなく銀行業界や金融業界として、広く周知し利用者の認識を得る必要があると思われるため、金融庁としての広報活動等もご検討が必要ではないかと考える。
4	主要行向け：Ⅲ−3−8−2(2) 中小向け：Ⅲ−3−5−2(2)	「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」と記載があることから、フィッシング詐欺に繋がらないような一般的なマーケティング等で顧客に送られるメールや、パスワード入力を促すページのURLおよびログインリンクでなければ、監督指針改正案の対象外の認識で良いか。監督指針改正案で求めている対象について明確化願いたい。
5	主要行向け：Ⅲ−3−8−2(2) 中小向け：Ⅲ−3−5−2(2)	Google「メール送信者ガイドライン」では、ワンクリック登録解除等のオプトアウトに関する要件が入っているが、当該URLの記載は代替手段を取り得ない場合と解釈されるか。
6	主要行向け：Ⅲ−3−8−2(2) 中小向け：Ⅲ−3−5−2(2)	「メールやSMS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」とあるが、例えば、パスワード入力をしない企業のHP等は記載しても良いという理解で良いか。
7	主要行向け：Ⅲ−3−8−2(2) 中小向け：Ⅲ−3−5−2(2)	「ログイン、出金等、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の実装及び必須化」とあるが、対応端末を保持していない等の理由で、必須化後、解除やむ無しとなる顧客が相当数発生する見込みである。 対応端末を保持しない場合、JPKIやeKYC等一定水準での本人確認が担保できない場合も想定されるが、どのような方法で相当数の顧客の解除手続きを実現させる想定であるか。 必須化された多要素認証を解除できない顧客が相当数発生するとなれば、これを奇貨とした犯罪手口が発生する懸念もあり、各金融機関の事情に応じ、必須化でなく、導入後および利用促進強化でも充足する旨を明示いただきたい。
8	主要行向け：Ⅲ−3−8−2(2) 中小向け：Ⅲ−3−5−2(2)	「ログイン、出金等、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）」の記載について、顧客が取引に利用する機器の都合で多要素認証が設定できない等の場合にやむを得ず解除するケースが想定されことから、デフォルト設定とすれば必須化の要件を充足している認識で良いか。
9	主要行向け：Ⅲ−3−8−2(2) 中小向け：Ⅲ−3−5−2(2)	多要素認証をデフォルト設定する場合、スマートフォン未保有者や生体認証が出来ない一定の顧客は多要素認証を解除しなければインターネット・バンキングを利用できなくなる。加えて、多要素認証解除には認証強度が高い本人確認を実施しなければ犯罪者に悪用されるため、eKYCでの本人確認が必須と考える。しかしながらスマートフォン未保有者はeKYCでの本人確認が実施できないため、多要素認証の解除が出来ずインターネット・バンキングの利用が出来ない。 こういった顧客が多発することが想定されるため、デフォルト設定ではなく、原則顧客に登録いただく仕組みや未選択時の取引制約を課す等の組合せによるリスク軽減を行う方針へ変更いただきたい。
10	主要行向け：Ⅲ−3−8−2(2) 中小向け：Ⅲ−3−5−2(2)	当行では、生体認証を利用する場合、スマホ1端末に対し1口座の管理となる。このため、複数口座に紐づく複数のインターネット・バンキング契約を持つ顧客や未成年口座を管理する親権者等は多要素認証をデフォルト設定した場合、インターネットバンキングを利用できなくなるため、デフォルト設定するのではなく顧客に登録いただく仕組みや未選択時の取引制約を課す等の組合せによるリスク軽減を行う方針へ変更いただきたい。
11	主要行向け：Ⅲ−3−8−2(2) 中小向け：Ⅲ−3−5−2(2)	多要素認証のデフォルト設定は、インターネット・バンキングを利用できない顧客が多発するため、原則は顧客に登録いただく仕組みや未選択時の取引制約を課す等の組合せによるリスク軽減を行う方針へ変更いただきたい。このうえで、多要素認証未利用者に対して定期的な周知や利用者拡大に向けた対応を行っていくことが望ましいと考える。
12	主要行向け：Ⅲ−3−8−2(2) 中小向け：Ⅲ−3−5−2(2)	パスキーやPKI基盤等、例示されている多要素認証方式は、顧客や自社が自社以外の第三者（OSプラットフォーマーや認証局等）が提供するデバイスや基盤を信頼することを前提とした認証と認識している。これは自社が独自に提供する認証手段に依存するのではなく、顧客自身が利用する認証基盤を選択・管理できる柔軟性を重視する考え方とも受け取れるが、この認識でよいか。
13	主要行向け：Ⅲ−3−8−2(2) 中小向け：Ⅲ−3−5−2(2)	金融機関としてパスキー等の利用を推進しても顧客側の端末環境や手続きの煩雑性等の事情によりパスキー等の多要素認証を登録しない意向の顧客が一定数存在することが想定されるため、こうした顧客まで一律パスキー等の利用を強制するのではなく、パスキー等を利用する顧客と利用しない顧客に分けて統制上の差異を設けること（パスキー等を利用しない顧客について検知の閾値を上げる、または送金額上限に差異を設ける等）も1つの解になると考えているが、認識に相違ないか。
14	主要行向け：Ⅲ−3−8−2(2) 中小向け：Ⅲ−3−5−2(2)	昨年7月28日付「顧客口座・アカウントの不正アクセス・不正取引対策の強化について（要請）」の文書において、例えばパスキー等では「導入」までが求められているところ、監督指針改正案では「必須化」と記載ぶりが異なっている。同要請に合わせ改定される予定の監督指針改正案の各項目について、同要請文以上の対応が求められているものでは無い認識で良いか。また認識に相違無ければ、記載の平仄を合わせていただきたい。
15	主要行向け：Ⅲ−3−8−2(2) 中小向け：Ⅲ−3−5−2(2)	「ログイン、出金等、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」との記載について、「フィッシング対策ガイドライン」における多要素認証の考慮点（23～24頁）と照らし、「ユーザー情報や多要素認証等の設定変更等」との対象の追記・明確化を行った方が良いのではないか。
16	主要行向け：Ⅲ−3−8−2(2) 中小向け：Ⅲ−3−5−2(2)	「ログイン、出金等、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）」の記載について、（注2）の注記事項の趣旨と比較した場合、既存顧客に対しては実装対応後に一定の移行期間等を設定したうえでの一律適用・移行を要請するものと考えるが認識に相違ないか。
17	主要行向け：Ⅲ−3−8−2(2) 中小向け：Ⅲ−3−5−2(2)	インターネット・バンキングをPCブラウザのみ、かつワンタイムパスワードカード（ハードウェアトークン）で利用している顧客は、多要素認証をデフォルト設定した場合インターネット・バンキングが利用できなくなる。 デフォルト設定するのではなく顧客に登録いただく方針へ変更いただきたい。
18	主要行向け：Ⅲ−3−8−2(2) 中小向け：Ⅲ−3−5−2(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」とあるが、顧客に周知するということは犯罪者側にも情報提供することに繋がる。本件周知は犯罪者に犯行・悪意のある攻撃（例えば、銀行を騙り「認証方法の変更のために必要」、「認証が使えなくなる」といった騙り口で顧客から情報を騙し取る手法等）を実施するタイミングを惹起する懸念があるため、「具体的なスケジュールについて顧客に周知する」ことは避けたく、周知の記述は回避いただきたい。
19	全般	本件を実施するのであれば、国民の金融機関取引において利便性を大きく損なう対応であり、各金融機関が個別で顧客対応することは極めて負荷が大きい。本件は金融機関取引に対する国民の理解が必須であり、金融庁・警察庁・政府から金融機関取引においては多要素認証が必須である旨、国民に対して報知を行うことについてご検討いただきたい。
20	その他	ボイスフィッシング対策について、クローキングによる詐欺サイト閉鎖に時間を要しているが、銀行だけの対応には限界があり、海外のホスティング事業者に対する政府からの要請や、警察・通信事業者連携による不正電話番号の即時利用停止仕組みを整備し、通信経路を断つ対策等を是非お願いしたい。 また、海外犯罪組織に関する政府間のさらなる連携強化をお願いしたい。

以　上