コメントの概要及びコメントに対する金融庁の考え方

No.	コメントの概要	金融庁の考え方
監督指針全般について		
1	金融会社関係「資金移動業者関係」の改訂は行われないのでしょうか。	「資金移動業者関係」向けの事務ガイドラインの改正につきましては、今後改正の必要性等を検討してまいります。
2	セキュリティの確保として行う不正防止策として、『不正アクセス検知機能の導入』『セッションや取引のモニタリングの強化』自体をより明確に単体として位置付ける記述にすべき。また、民間外部委託事業者等の積極的な活用等を位置付ける記述にすべき。 （理由）金融庁が昨年６月に公表した「金融分野における IT レジリエンスに関する分析レポート」においても、『インシデントが発生していない金融機関においても、サイバーセキュリティを含めた IT リスク管理態勢を強化すべき」「顧客口座への不正アクセスの事案は、証券業界に限らず、金融業界の信頼を揺るがしかねない問題であり、認証やモニタリングの強化などを含め、迅速な対応が必要である。」「セッションや取引のモニタリングの強化が必要」と記述されているなど、貴庁自体が、金融機関全体の底上げと不正アクセス検知導入の必要性を示唆している。	貴重なご意見として承ります。
3	インシデント発生時及びインシデント認識時における即応態勢の整備ができているかを着眼点に明確に位置付けるべきである。 （理由）	貴重なご意見として承ります。

	インシデントの予兆をいかにはやく認識して、インシデントが発生した場合には、「今ここにある危機」のために、外部事業者との連携を含めてあらゆる手段を講ずる態勢が取れているかをきちんと行政として把握しておかないと、投資家・消費者保護が徹底されないことになる。	
4	監督指針やガイドライン等に沿って各金融機関がどのような態勢変更等を行ったかなどのフォローアップの実施とそれに基づいた監督指針やガイドライン等の適宜見直しを行っていくべき。 （理由）今回の監督指針やガイドライン等の改正で打ち出す方向性は金融取引におけるセキュリティ向上や金融犯罪の抑止のために必要であるので、この改正によりどのように各金融機関において実装され、その結果出てくる課題等は何かなどフォローアップをしっかり行い、それを踏まえ、必要に応じて監督指針やガイドライン等も再改正するなどの政策のローリングモデルを構築すべき。	貴重なご意見として承ります。
5	今回の監督指針やガイドライン等の改正内容や改正趣旨そのものを各金融機関において確実に実装させるためには、抜本的な支援措置の強化、必要な技術支援（必要に応じて民間知見の活用）、また、金融機関と外部民間企業との必要な連携の促進（金融機関による有効な外部ツールの積極的な活用へ向けた働きかけ等）などの環境整備など必要な各種政策を金融庁としてパッケージとして明らかにしたうえで政策を進めてもらいたい。	貴重なご意見として承ります。

	（理由）今回の監督指針やガイドライン等の改正は、金融機関からすると、今後対応すべきことがより明確になったあるいはなるということで大変意義深いものである。それゆえに、その内容や趣旨を実現するための各種措置の実施が今後大至急の課題として必要不可欠である。	
6	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。	貴重なご意見として承ります。
7	パスワード忘失時やパスキー登録端末の機種変更時には、「パスワードを忘れた方はこちら」などのダイアログから再登録可能としている金融機関は多い。こうした中、口座番号と生年月日、4 桁のキャッシュカードで再登録可能としているケースも見られるが、新たな攻撃の端緒とならないか？取引認証の堅牢系だけでなく、当人認証の堅牢性についても今後監督指針に盛り込めるように検討と対応をお願いしたい。	貴重なご意見として承ります。ご指摘のとおり、フィッシングに耐性のある多要素認証の導入に際して、前提として、確実に本人の認証情報を登録することは重要と考えます。
8	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のパブリックコメントでは、金融機関に対して対応期限を求めるという性質のものではないとの回答があったが、それを踏まえ、本項で示されている様々な不正防止策についても、リスクベースアプローチの考えのもと、金融機関ごとの特性に応じて必要な対策を選択し、適切な時間	システム開発等その他やむを得ない理由による場合に一定の期間を要する場合があることや顧客規模や取引チャネルに応じて段階的に導入していく場合があることは理解できますが、目下の状況を踏まえ、可能な限り早期に対応することが望まれます。

	軸のもとで対応していくべきという理解でよいか。それとも、インターネットバンキングというサービスを提供するにあたっては、リスクベースアプローチ上これらの対策は必須であり、達成時期はともあれ必ず具備すべきという趣旨なのか。	
9	「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」について、当該 URL がたとえ金融機関の公式サイトトップページであったとしても、同トップページにインターネットバンキングへのリンクボタンがある場合には不適切であり、メールや SMS への同トップページの URL の記載は避けるべきか。	メール配信の解除手続きなど、法令に基づき電子メールの本文に記載が義務付けられている場合などを除き、原則として、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すべきではないと考えます。 また、利用者に対して、各社のウェブサイトにアクセスする際は、事前に正規のウェブサイトの URL をブックマーク登録しておきブックマークからアクセスしたり、正規のアプリからアクセスしたりするよう周知することが望ましいと考えます。 以上を踏まえると、ログインすることが可能な画面へ遷移するページの URL についても記載すべきではないと考えます。
主要行等向けの総合的な監督指針		
全般について		
10	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。	貴重なご意見として承ります。
Ⅲ―３―８―２　主な着眼点（２）セキュリティの確保		

11	「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	原則として、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すべきではないと考えます。
12	上記指針における「多要素認証の実装及び必須化」について、個人向けインターネットバンキングのみならず、法人向けインターネットバンキングについても同様に適用される想定であるかを確認したい。 （意見の理由・背景） 法人向けインターネットバンキングにおいて、パスキー等を用いたフィッシング耐性のある多要素認証を導入する場合、利用者である法人の役職員それぞれの個人端末（スマートフォン等）において、認証情報の設定・管理が必要となることが想定される。 一方で、法人利用においては、業務用端末と私物端末の峻別、端末管理や人事異動時の対応、複数担当者による権限管理等の観点から、個人端末への認証情報の設定を前提とする方式が、必ずしも法人の業務管理体制や内部統制に適合しない場合もあると考えられる。	当庁といたしましては、顧客がフィッシング被害に遭うリスクを低減するための適切な措置を講じていただくことが重要であると考えております。この点を踏まえ、各事業者におかれましては、代替手段の検討等を含め、よくご検討ください。
13	「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	「実務観点で代替手段がないと判断される場合」の具体的な内容が必ずしも明らかではありませんが、原則として、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すべきではないと考えます。

	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。	
14	「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。	ご認識の通りです。 広報活動については、貴重なご意見として承ります。
15	「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。	ご認識の通りですが、顧客へ送付するメール又は SMS にリンク先の URL を載せ、そこから遷移させることは極力控え 、代替的な手段の導入を検討することが望ましいと考えます。また、ログインすることが可能な画面へ遷移するページの URL についても記載すべきではないと考えます。
16	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。	個別製品に関するご回答は難しいですが、メール配信の解除手続きなど、法令に基づき電子メールの本文に記載が義務付けられている場合などを除き、原則として、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すべきではないと考えます。

17	「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。	ご認識の通りですが、顧客へ送付するメール又は SMS にリンク先の URL を載せ、そこから遷移させることは極力控え 、代替的な手段の導入を検討することが望ましいと考えます。また、ログインすることが可能な画面へ遷移するページの URL についても記載すべきではないと考えます。
18	「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。	ご指摘のとおり、フィッシングに耐性のある多要素認証の導入に際して、前提として、確実に本人の認証情報を登録することは重要と考えます。 当庁といたしましては、顧客がフィッシング被害に遭うリスクを低減するための適切な措置を講じていただくことが重要であると考えております。 この点を踏まえ、各事業者におかれましては、代替手段の検討等を含め、よくご検討ください。
19	「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。	インターネット取引においては、提供するサービスの内容に応じた不正防止策を講じることを求めております。 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については、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といった場合にやむを得ず解除するケースが想定されます。 上記のケースであっても、当該顧客の状況（全顧客に占める割合の推移、不正アクセス等の状況等）をフォローし、また、認証技術や規格の発展も勘案しながら、当該顧客の割合が低くなるよう対策の見直しを検討する必要があると考えます。

20	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。	顧客要望による例外を認めることは、顧客がそのリスクを認識していたとしても不正アクセスの隙を与えることにつながりかねず、不正ログイン・不正取引防止の観点においては、原則としてフィッシングに耐性のある多要素認証を必須化することが適切と考えます。
21	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。	
22	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。	
23	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。	
24	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。	
25	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。	本改正は、昨今の事案の被害状況・手口等を踏まえ、利用者保護の観点から有効と考えられる対策を追加したものです。 自社独自の認証手段を提供する場合、第三者が提供する認証手段をサービスに組み込む場合のいずれにおいても、導入することによるリスクの評価、残存するリスクの管理について、よくご検討ください。
26	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	要請文は、目下の状況を踏まえ、あらゆる金融機関において講ずべき対策を列挙しております。 一方、主要行等向けの総合的な監督指針等は、検査・監督に関する基本的考え方、事務処理上の留意点、監督上の評価項目等を体系的に整理したものであり、金融庁担当課室においては、本監督指針に基づき主要行等の検査・監督事務を実施するものです。

	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。	そのため、各社の顧客や業務の特性、提供するサービスの内容等を踏まえながら、その時々のセキュリティ水準や犯罪手法等に応じて、要請文に記載のある対策も含めて、不断にセキュリティ対策を見直していくことが重要と考えます。
27	「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。	貴重なご意見として承ります。
28	「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。	ご認識の通りです。
29	「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	貴重なご意見として承ります。

	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。	
30	「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」とあるが、予め顧客と銀行間で合意がとれている状態で、合意した通りの内容（件名やＵＲＬ等）と顧客が個別判断できるメールやＳＭＳを送付する場合は問題ないとの理解でよいか。 具体的には、以下のような事例を想定しているが問題ないか。 ・顧客からの問い合わせを受け、必要な手続きを行うために、合意した通りの内容で送信されるメールやＳＭＳ。 ・ＵＲＬを記載したメール等の送付について、送付タイミング（例えばお電話でご了承を得てから一定時間後等）・送付方法・件名・ＵＲＬからの入力内容等をあらかじめ顧客と銀行間で合意したうえでご案内するメールやＳＭＳ。	メール配信の解除手続きなど、法令に基づき電子メールの本文に記載が義務付けられている場合などを除き原則として、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すべきではないと考えます。
31	「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、ログインリンクであっても、顧客があらかじめスマートフォンにインストール済みの正規アプリへのリンク（インストール後、顔認証やパスキーで自動ログインできるものに限る）であれば、アクセス時に何らパスワードや個人情報の入力は要求されないものであり、同ログインリンクを記載したメールや当該アプリへのログインリンクが記載されたページへ誘導するＵＲＬを記載したメールは、いずれも問題ないと考えてよいか。	今回の監督指針改正で求めているのは、「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」ことになります。また、顧客へ送付するメール又は SMS にリンク先の URL を載せ、そこから遷移させることは極力控え 、代替的な手段の導入を検討することが望ましいと考えます。
Ⅲ―３―９―２　主な着眼点（２）セキュリティの確保		

32	（２）３の注書きに「実効的な認証方式については III－３－７－１－２（５）２を参照。」とあるが、本監督指針上に該当する項目はないため、「II－３－４－１－２（５）２」の誤植ではないか。	ご指摘の通り修正いたしました。
中小・地域金融機関向けの総合的な監督指針		
Ⅱ―３―５―２　主な着眼点		
33	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。	ご指摘のとおり、サイバー攻撃手法は日々変化し、高度化していきますので、各社の顧客や業務の特性、提供するサービスの内容等を踏まえながら、その時々のセキュリティ水準やサイバー攻撃手法等に応じて、不断にセキュリティ対策を見直していくことが重要と考えます。例えば、自社で収集している情報や当庁から発信している情報だけではなく、同業態でも意見交換等を実施し、知見を共有し、被害防止・対策強化を図ることが対応策として考えられます。
Ⅱ―３―５―２　主な着眼点（２）セキュリティの確保		
34	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。	貴重な御意見として承ります。
35	「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。	ご認識の通りです。
Ⅱ―３―５―２　主な着眼点（３）顧客対応		

36	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。	パスワードを利用しない認証方式についても言及していることから、明確化の観点で記載しております。
Ⅱ―3―6―2　主な着眼点（2）セキュリティの確保③		
37	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。	ご認識の通りです。
事務ガイドライン（第三分冊：金融会社関係　16　暗号資産交換業者関係）		
Ⅱ―2－3－1－2－3　不正取引が発生した場合の対応		
38	Ⅱ－2－3－1－2－3で、「速やかに「不正取引発生報告等」にて当局宛て報告を求めるものとする。」とありますが、ここで言う「報告」が、金融商品取引業者等向けの総合的な監督指針（Ⅲ-2-8-2-3(1)）で示す「犯罪発生報告書」 と同じものにて報告可能なのか、別の様式があるのかが不透明と思われますので明示いただけますと幸いです。	趣旨は同様ですが、様式は異なります。様式は、提出対象となる金融機関等に別途提示します。
Ⅱ－2－3－1－2－2　主な着眼点（2）セキュリティの確保		
39	「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」は金商法の監督指針とあわせて	金融商品取引業者等向けの総合的な監督指針と同様に修正いたしました。

	「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」とするのが望ましいと考えます。 金商法の監督指針ではパブリックコメント No.27 で変更されたと認識しております。 https://www.fsa.go.jp/news/r7/shouken/20251015/01.pdf	
40	フィッシングサイトの閉鎖依頼等とあるが、ブラウザベンダーへのフィッシングサイト報告も含まれていると思ってよいか？	当該ブラウザ以外のブラウザからはアクセスできることや、ブラウザベンダーが対応完了までに時間を要する可能性があること等を踏まえ、リスクに応じた閉塞依頼手段をご検討ください。
41	フィッシングに耐性のある多要素認証に例示しているパスキーやPKIの認証は、法人において1IDを複数名で利用する場合への対応が困難である。法人利用については、顧客からフィッシングリスクがあることを受容する旨の同意をオプトインで得た上でパスキーを必須としない対応をすることはできないか？	当庁といたしましては、顧客がフィッシング被害に遭うリスクを低減するための適切な措置を講じていただくことが重要であると考えております。この点を踏まえ、各事業者におかれましては、代替手段の検討等を含め、よくご検討ください。
Ⅱ－２－３－１－２－２　主な着眼点（３）顧客対応		
42	不正取引による被害があった場合の顧客の被害補償について記載があるが、顧客が自作自演による不正取引による被害の申告（わざとIPアドレスを変えて第三者からアクセスされているように見せかける等）と、本当に第三者による不正取引による被害の申告か、事業者側のログ等だけでは判断がつかない。本人確認の強度が強いパスキーの実装を必須としていることを旨に、補償対象外とすることはよいのか？（第三者がパスキーを攻略することは、利用者が端末を窃取された上で端末のパスコードも合わせて漏洩した場合や、パスキーのバックアップが窃取された場合しかなく、顧客側の過失が強いと考えられる）	事務ガイドラインは監督上の着眼点や留意点等を記載するものであり、金融機関が顧客に対して行う補償の実施や手法について規定する権能はありませんが、個々の事情や各社の方針に応じて、判断が必要なため、一概に申し上げる事は難しいと考えます。