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	「インターネット取引における不正アクセス・不正取引を認識次第、速やかに「犯罪発生報告書」にて当局宛て報告を求めるものとする。」とあるが、「犯罪発生報告書」とはどのようなものか。所定様式は定められるか。様式の定めがない（任意様式）であれば、どのような事項を記載する必要があるか。	様式は、提出対象となる金融機関等に別途提示します。
2	(1)顧客の依頼に基づく受動的な URL 送付について 実際の顧客対応においては、顧客がマイページの場所が分からずに電話で問い合わせをしてくるケースや応対中に FAQ の場所を求められるケースが少なからずあるため、手続き可能なマイページや FAQ への URL を付した SMS を送付する運用を行っております。本対応は顧客の能動的な問い合わせに対する応答であり、不特定多数を対象としたフィッシング詐欺とは明確に区別されるべきと考えますし、高齢顧客等では当該手段が無いと手続きページにたどり着けないケースが想定され、代替手段を取ることが困難なケースもあります。顧客の利便性維持の観点から、本運用は問題ないと考えますが、いかがでしょうか。	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。
3	(2)特定の顧客に対する手続き・確認メール内の URL 掲載について 手続完了、中途手続きの再開促進、内容確認等のメールにおいて、マイページへのリンクを案内しております。これらは手続きを要する特定の顧客に限定して送付されるものであり、身に覚えのない顧客を標的とするフィッシング詐欺のリスクは極めて限定的ですし、こちらも	

	(1)同様、高齢顧客等ではリンクが無いと、当該ページにたどり着けないケースも想定されます。顧客が容易に手続きを確認できる利便性維持の観点から、本運用は問題無いと考えますが、いかがでしょうか。	
4	(3)商品・サービス説明画面を経由した誘導について ログイン画面へ直接遷移させず、商品説明やサービス説明画面を介して誘導するURL・バナーについては、顧客の関心に応えるために必要不可欠です。これら説明画面からログイン画面へ遷移可能であることを理由に一律に禁止することは、顧客が必要な情報にたどり着く経路を不当に狭めることになることから、本運用は、問題ないものと考えますがいかがでしょうか。	
5	(4)ID・パスワード入力を伴わない個人情報の取り扱いについて本指針における「パスワード入力を促すページ」という文言に基づき、ID・パスワード入力を伴わない個人情報入力画面への遷移については、本指針の適用対象外であると理解しております。この解釈で相違ないでしょうか。	「ID・パスワード入力を伴わない個人情報入力画面への遷移」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。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。
6	(5)パスワード入力のみのURL掲載について メールやSMSに記載されたURLの遷移先が、顧客のIDやアカウントとは紐づかない、パスワードのみの入力を求めるページである場合、本指針が規制する「ID・パスワードの入力を促すページ」とは性質が異なるものと考えます。当該URLについては本指針の適用対象外と考えますが、いかがでしょうか。	URLの遷移先において実施される操作が、本指針の対象に含まれるかどうかについては、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。

	※個人情報保護の観点から広く普及しているセキュアなファイル転送サービスにおいても、その仕組み上、このようなURLの送信が不可避となっており、顧客とのやりとりにおいても利用実績があることから、確認させて頂いております。	
「保険会社向けの総合的な監督指針」		
全般		
7	本改正の趣旨を踏まえ不断の努力は必要と考えるものの、今般の改正で追記される不正防止策や態勢整備については、画一的な対応が求められているものではなく、各社において、犯罪の発生状況も踏まえリスク評価を行いつつ、当該業務のリスク特性も考慮のうえ、必要と判断する不正防止策等（改正案に記載された方策に限定されない）に取組むことが求められているものと理解しておりますが、認識に相違ないでしょうか。	ご認識の通りです。
8	対策を講じるべき対象として想定されている取引等の範囲は、顧客の資産の移転を伴う取引に限らず、リスクが高い顧客情報や契約情報が含まれる会員サイト等へのログインも対象になると理解しておりますが、認識に相違ないでしょうか。	ご認識の通りです。
Ⅱ－３－１３－２－１－２（５）サイバーセキュリティ管理		
9	本改正で求められる管理態勢の適用範囲は、保険会社に限定され、代理店には適用されないという理解でよいか。	保険会社に限らず保険代理店等についても対象となりますが、規模や業務特性を踏まえ、態勢整備を求めることとなります。
10	「インターネット等の通信手段を利用した非対面の取引」の「取引」は、保険への新規加入や保険料徴収に関わる手続きのみを指すものではなく、「お客様情報の変更」や「補償内容の変更」、「保険金請求」等も含まれるか。また、対象となる範囲は、保険募集に係る取引に限	各社の状況が異なるため一概に申し上げることは困難ですが、当庁といたしましては、顧客が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、よくご検討ください。

	定されているということでよいか。または保険会社が保険募集以外の顧客に提供するサービスを含むか。「取引」が指す手続きや操作の範囲を教えていただきたい。	
11	インターネット取引とは「インターネット等の通信手段を利用した非対面の取引」との定義であるが、web 上で顧客が自身の専用ページにID、パスワード等を用いてログインしたうえで行なう取引ではなく、web サイト上で顧客が手続き内容等を一方的に入力するものである場合、フィッシングに耐性のある多要素認証の実装は義務化されるものではないということでよいか。	「web サイト上で顧客が手続き内容等を一方的に入力するものである場合」の具体的な内容が必ずしも明らかではありませんが、当庁といたしましては、顧客が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、よくご検討ください。
Ⅱ－３－１３－２－２－２（１）内部管理態勢の整備		
12	「リスク分析、セキュリティ対策の策定・実施、効果の検証、対策の評価・見直しからなるいわゆる PDCA サイクル」について、具体的な取り組み方法（PDCA のモデル）などをお示しいただく予定はあるか。	貴重なご意見として承ります。各社の状況が異なるため具体的な取り組みを一概に示すことは難しいと考えております。
13	指針が要請する態勢整備の完了時期については、各保険会社の業務、提供するサービスの特性等に鑑み、「一律にある時期までの完了が必須となる訳ではない」という理解でよいか。	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、可能な限り早期に対応することが望まれます。
Ⅱ－３－１３－２－２－２（２）セキュリティ確保		
14	【原文】 ・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）	貴重なご意見として承ります。

	【意見】 「パスキーによる認証」と「PKI（公開鍵基盤）をベースとした認証」が並列で記載されていますが、パスキーはPKIを基盤とした認証技術の一種であり、両者は包含関係にあります。この表記では、これらが別の認証方式であるかのような誤解を招きかねません。事業者が具体的な対策を検討する際に、パスキー以外にどのようなPKIベースの認証を指すのか判断に迷い、混乱を招く懸念があります。つきましては、両者の関係性を明確にするため、以下のような記述への修正をご提案します。 【修正案】 「(例：パスキーなど、PKI（公開鍵基盤）をベースとした認証)」	
15	【原文】 ・（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 【意見】 「設定に必要な機器」の例として「スマートフォン等」が挙げられていますが、フィッシングに耐性のある多要素認証、特にパスキーなどは、必ずしもスマートフォン等の別デバイスを必要とするものではありません。この記載は、認証にスマートフォンが必須であるという限定的な印象を与え、実態と異なる解釈をされる可能性があります。認	貴重なご意見として承ります。

	証の可否は、利用するPC等の端末自体が生体認証機能やセキュリティキーに対応しているかどうかに依存する場合もあります。そのため、より正確な表現として、以下のような記述に修正いただくのが適切と考えます。 【修正案】 「顧客が、認証に用いる端末が生体認証やセキュリティキー等のハードウェア要素（所持要素）を備えていない等の理由で…」	
16	「メールやSMS内への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」との記載について、会社が当該実務上の対応を図る中で、その時点でのセキュリティ基準や攻撃手法等も踏まえたリスク評価に基づき、メール等へのログインリンク不記載の実装順序や時期を個別に判断することは、合理的な裁量範囲内であり、「リスクの存在を十分に認識・評価した上での対策の要否・種類の決定」として許容されると理解しておりますが、認識に相違ないでしょうか。	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、可能な限り早期に対応することが望まれます。
17	オンラインによるダイレクト販売の保険会社のビジネスモデルは、オンライン手続きによる徹底したコスト削減を追求し、その経済的メリットを低廉な保険料として顧客に還元することです。 そのようなビジネスモデルの下、銀行や証券と異なり、保険は手続き等におけるアクセス頻度は低いのが実情です。そのため、メールやSMS等で直接的なリンク（ガイド）を提供できない場合、多くの顧客はログイン方法や該当ページへの到達方法がわからず、オンライン手続きを断念せざるを得ません。	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。

	顧客がオンライン手続きを諦めて電話や書面でのやり取りに移行せざるを得ない状況は、ダイレクト販売のビジネスモデルを根底から覆すだけでなく、事務コストの大幅な増大を招きます。結果として、これまで低価格な保険料を維持できていた仕組みが維持困難となり、最終的に顧客利益を損なうことになりかねません。 また、フィッシング詐欺の目的は、①即時に金銭を奪う、②転売・悪用しやすい認証情報を得ることが主なものだと思います。 保険会社の手続きにおいて入手できるものの中には契約者の個人情報や口座情報等もあるので②のリスクは０ではありませんが、保険は即時出金はできず、また通常審査手続きが介在するものであり、証券・銀行と違い①のリスクはないと考えております。	
18	「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」の記載について、保険金・給付金請求や住所変更の等各種手続きのために個人情報を入力してもらうリンク（ログイン不要・パスワード入力不要）については今回のターゲット外という認識でよいでしょうか。 保険においては即時出金が可能な証券・銀行と異なり、保険金・給付金の支払等において通常必ず審査があり、一定程度時間を要しますので、所要時間の削減のためにオンライン手続きの顧客側のニーズがあります。 また、保険は証券・銀行ほど頻繁にアクセスするものではないため、SMS/メール等によるガイドをつけないとオンライン手続き画面へのアクセスが困難であり、電話や書面でのやりとりとしなければならない	「保険金・給付金請求や住所変更の等各種手続きのために個人情報を入力してもらうリンク（ログイン不要・パスワード入力不要)」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。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。

	とすると、顧客利便性の低下が著しく、且つ、デジタル化に逆行することになりかねないと思料します。 加えて、SMS/メール等によるガイドを廃止するとコールセンター等での対応増に伴う、保険会社のコスト増、ひいては顧客の負担増につながりかねないと思料します。	
19	「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。」について、具体的な取り組み方法や事例をお示しいただく予定はあるか。	貴重なご意見として承ります。各社の状況が異なるため具体的な取り組みを一概に示すことは難しいと考えております。
20	第三段落「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（中略）等、提供するサービスの内容に応じた適切な不正防止策を講じているか。」とあるが、事業者から顧客に対して情報発信メールや広告宣伝メールが送信され、メール内に記載された URL やログインリンクを押下してウェブサイト等に遷移するのは業界や商材を問わず一般的な導線設計であり、消費者に広く受け入れられたメンタルモデルであることから、保険会社のみが当該導線設計を止めたとしても悪意をもった攻撃者がフィッシングメール等を配信した際の被害を軽減する効果は限定的と考えられる。全てのユーザーが正規のウェブサイトをブックマークしているないしはブックマーク機能をスムーズに利用できるとは限らず、また、正規のウェブサイトを探す手間を嫌って必要な手続きを先送りするケースや、正規のウェブサイトを探す際に誤って異なるウェブサイトを訪問し必要な手	今般の事案を踏まえ、他業態も同様の改正を行っております。金融業界全体で取り組みを行うことは、業界の信頼性の向上にも資するものと考えます。

	続きを実施できないケースを誘発する可能性もあるなど、利用者利便を著しく損ねる内容なのではないか。	
21	「提供するサービスの内容に応じた適切な不正防止策」は、「フィッシング詐欺への注意喚起を促すガード文言」と「パスワード入力を促すページの URL やログインリンク」を共に記載する、といったことを想定したものとの理解でよいか。	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。
22	「提供するサービスの内容に応じた適切な不正防止策」は、「フィッシング詐欺への注意喚起を促すガード文言」と「パスワード入力を促すページの URL やログインリンク」を共に記載する、といったことを想定したものとの理解でよいか。	
23	メールや SMS におけるログインリンクについて、二要素認証などセキュリティ対策しているページに対するリンクを記載することについても避けるべきとの認識か。	
24	お客さまに送信するメールの「ドメイン認証」を対策実施済みであったとしてもなおメールでのログインリンクの設置は不可か。	
25	「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。）」とあるが、「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」のみならず、顧客の依頼に基づく予約・手続き・照会への返信等については、顧客利便と安全性を両立することを許容する整理とできないか検討いただきたい。	

26	『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』との考え方について、禁止対象が、利用者に認証情報入力を直接促す導線を指すことを明確化いただきたい。あわせて、利用者の能動的な操作を起点とする案内であり、事業者側において送信ドメイン認証、送信文面の定型化、送信目的の明示、アクセス先の限定、一定時間経過後の失効、追加本人認証その他の誤認防止措置を講じる場合における URL 記載の取扱いについて、どのように整理すべきか考え方を示していただきたい。	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。
27	改正案では、不正検知・異常検知に係る通知メール等の機能の提供を求めている一方で、メール・SMS 内へのログインリンク等の不記載を求めている。このため、通知メールにおいて、例えば「ログインがありました」「メールアドレス変更がありました」「心当たりがない場合は公式アプリまたは公式サイトからご確認ください」といった記載がどこまで許容されるのかも整理いただきたい。	当庁といたしましては、顧客が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、よくご検討ください。
28	「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」との記載に関し、DMARC および BIMI の導入を前提とし、フィッシング詐欺リスクの低減と顧客利便性の両立を図る観点から、メールや SMS へパスワード入力を直接促すものではない自社の公式ホームページ URL 等、ログインを必要としない画面であれば上記の条文に該当しないという理解でよいか。	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。
29	事故受付や契約手続き等※においてメールでの URL 案内が不可欠な場面がある。こういったものは、改正案にある「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	インターネット取引に該当するかどうかは、個別具体的に判断する必要がありますが、原則として、メールや SMS（ショートメッセージサービス）

	合」に該当するという理解でよろしいか。それとも、「顧客の財産を安全に管理することが求められる」インターネット取引には該当しないという理解か。 ※事例 ①保険金支払手続きや問い合わせ対応で、保険金支払いの流れや一般的な事故・保険の知識が掲載されたURL が記載されたメールを送信する ②自動車保険の契約更新などの更新日に合わせた手続きご案内メールに、手続き入口ページのURL を記載する ③お客様の行動起点（例：WEB サイトでの申込み手続き完了直後に送るメールなど）で送信する ④顧客との通話中または通話直後に、顧客専用ページへのログインリンクのメール・SMS を送信する	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。 当庁といたしましては、顧客が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、よくご検討ください。
30	保険会社における『重要な操作』の範囲について、財産的影響又はなりすまし被害拡大のおそれの高い手続を中心に、判断要素及び具体例を示していただきたい。例えば、契約者情報の変更、メールアドレス変更、電話番号変更、保険金受取人変更、保険料収納口座変更、支払先口座変更、解約・返戻金請求等がこれに該当するか、考え方を明確化いただきたい。あわせて、閲覧や一般照会等の相対的にリスクの低い操作については、一律ではなくリスクに応じた認証水準の設定が可能であるとの理解でよいか、整理いただきたい。	顧客層、取扱商品、取扱額等は各社で異なることから具体例を一概にお示しすることは困難ですが、各社において、顧客や取扱商品、業務の特性等に応じてリスク評価を行った上で、適切な態勢整備を講じることが重要であると考えます。
31	「フィッシング耐性のある多要素認証の実装・必須化」に当たっては、顧客属性、利用チャネル、商品特性、システム改修時期等を踏ま	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

	え、代替的な多要素認証の提供、顧客周知及び検知機能の強化を組み合わせながら、段階的に移行することを許容する考え方を明確化いただきたい。	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。
32	多要素認証の要求頻度（有効期間）を決定するに際しては、各社が当該システムで保持する情報の質・量といった重要性、インターネットに面しているといった利用環境等のリスクを総合的に評価し判断することが基本と考えているが、評価にあたってのポイントや、最低限満たすべき基準についてどのように解釈すればよろしいか。 例えば『セッションが継続している間のみ有効』『最低でも1日に1回は要求すべき』『(リスクの低い）システムによっては初回に認証すれば良い』といった想定されている最低限の基準や考え方について伺いたい。 当指針の趣旨である顧客情報保護の実効性確保の観点から、原則としてアクセス（ログイン）の都度要求されるべきものかもしれないが、リスク評価に基づき、一定期間や特定条件下で認証の有効期間の許容範囲があることについて、顧客利便性も踏まえ合理的な安全管理措置が許容されるものであることを確認させていただきたい。	各社の状況が異なるため具体的な評価ポイントや基準を示すことは難しいと考えます。各社において、顧客や取扱商品、業務の特性等に応じてリスク評価を行った上で、適切な要求頻度をご検討ください。
33	フィッシング耐性のある多要素認証の必須化が示されているが、中小法人顧客の中には、個人顧客とは異なる利用形態も多いと認識している。こうした実態を踏まえた代替的な本人確認・認証手段の設計について、当局としての基本的な考え方を示していただきたい。	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。
34	「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)」との記載について、以下の2点を確認したい。	①パスキーには限りませんがフィッシングに耐性のある多要素認証の必須化を今後新たに登録する顧客のみならず、全ての登録顧客に対して求めるものです。

	①認証方式をパスキーのみに限定する趣旨ではなく、今後新たに登録する顧客に対して、パスキーの設定を必須とするという理解でよいか。 ②全ての顧客においてパスキーへの移行が完了するまで、既存のID・パスワード方式にワンタイムパスワード等を組み合わせた多要素認証を引き続き併用するという理解でよいか。	②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。
35	「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、「必須化（デフォルトとして設定）」という表現が、実質的な義務化と読める可能性があり、監督運用上の裁量の余地を明確にしていただきたい。 高齢者・法人顧客・代理店経由取引等、一律必須化が困難な利用者層への配慮や、既存基幹システムや外部委託先との連携制約により、短期対応が困難な会社への取り扱いについて、リスクに応じた段階的導入が許容されるのか、代替的な多要素認証の内容・許容期間を本文または注記で明確化していただくことが望ましいと考える。	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。 導入につきましては、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。
36	「解除率が低くなるよう見直しを検討・実施」という表現は、数値目標の設定を事実上求められているようにも読めるため、解除理由の正当性（端末非保有等）との関係性が不明確と思われる。解除率そのものではなく、解除理由の分析や代替策の妥当性を重視する旨を明確化していただきたい。	端末非保有等の理由で設定を解除する場合であっても、解除率の状況をフォローし、解除率が低くなるような対策を講じる必要があります。一方で必ずしも数値目標の設定を求めるものではなく、各社において、顧客や取扱商品、業務の特性等に応じてリスク評価を行った上で、適切な対策を講じることが重要であると考えます。
37	振る舞い検知、異常検知、ログ保存の強化について、中小法人顧客においては、専門人材確保や外部ベンダー利用コストが大きな負担となると考えられる。「十分な措置」の範囲について、規模・特性に応じた考え方を、より明確に記載していただきたい。なお、自社でのシス	当庁といたしましては、顧客が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、よくご検討ください。

	テム構築を前提とするのか外部委託活用を前提とするのかもお示しいただきたい。	
38	ダイレクト型の正味収入保険料が市場全体の約 1 割を占める自動車保険を代表格として、保険業界ではインターネットを通じた募集が一般化している。こうしたオンライン募集は自動車保険に限らず他種目にも広がっており、ネット専業の各社では、満期日の 2―3 ヶ月前から登録メールアドレス宛に継続手続きを案内することが標準的な運用となっている。 当社においても、自動車保険・ペット保険・家財保険・傷害保険等の満期が近づいた契約者に対し、継続手続用リンクを記載したメールや SMS を送付し、満期日前の手続きを促している。これらのメールや SMS に URL を掲載できない場合、顧客は自ら当社アプリまたはホームページと目的の手続ページを探す必要があり相当の時間を要することが想定されるため、顧客の利便性を損ない、苦情となる可能性がある。更に、場合によっては手続きを断念あるいは後回しとしそのまま失念するおそれもある。結果として無保険状態を引き起こし、事故発生時には被害者救済が困難となるなど、社会的影響が極めて大きいと考えられる。 また、これらの保険は事故による損害や賠償に備えるものであり、解約返戻金や満期保険金を伴う資産性はなく、フィッシング詐欺の標的となるリスクは極めて低い。以上を踏まえると、資産性の高い保険契約を除き、既契約者向けの満期案内メールや SMS に継続手続用 URL や保険会社公式サイトのトップページ URL を掲載することは、合理的であり許容されるべきと考えるがどうか。	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。

39	ダイレクト型の正味収入保険料が市場全体の約 1 割を占める自動車保険を代表格として、保険業界ではインターネットを通じた募集が一般化している。こうしたオンライン募集は自動車保険に限らず他種目にも広がっており、ネット専業の各社では、満期日の 2―3 ヶ月前から登録メールアドレス宛に継続手続きを案内することが標準的な運用となっている。 当社においても、既契約者のクレジットカード決済がエラーとなった場合や、カード有効期限の 2 か月前となった場合に、メールや SMS で保険料支払手続等を案内している。これらの連絡には、当社ウェブサイトの手続ページへ遷移する URL を掲載しており、顧客は ID・パスワードを入力して支払手続等を行っている。これらのメールや SMS に URL を掲載できない場合、顧客は自ら当社アプリまたはホームページと目的の手続ページを探す必要があり相当の時間を要すること が想定されるため、顧客の利便性を損ない、苦情となる可能性がある。更に、場合によっては手続きを断念あるいは後回しとしそのまま失念するおそれもある。結果として保険料未納となり無保険状態を引き起こし、事故発生時には被害者救済が困難となるなど、社会的影響が極めて大きいと考えられる。 また、これらの保険は事故による損害や賠償に備えるものであり、解約返戻金や満期保険金を伴う資産性はなく、フィッシング詐欺の標的となるリスクは極めて低い。以上を踏まえると、資産性の高い保険契約を除き、既契約者に必要な手続きを案内するメールや SMS に手続用	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。

	URL や保険会社公式サイトのトップページ URL を掲載することは、合理的であり許容されるべきと考えるがどうか。	
Ⅱ－３－１３－２－２－２（３）顧客対応		
40	改正案では、顧客へのリスク説明や注意喚起、啓発が求められているが、中小法人顧客に対しては、「必要十分な説明水準（簡潔さ・実務負荷を抑えた形）」が重要と考えられる。当局として想定する「十分な説明・周知」とは、どの程度の内容・頻度を想定しているか。	各社の状況が異なるため一概に申し上げることは困難ですが、当庁といたしましては、顧客が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、よくご検討ください。
Ⅱ－３－１３－２－２－２（４）その他		
41	「インターネット取引が非対面取引であることを踏まえた、取引時確認等の顧客管理態勢の整備が図られているか」の「取引時確認」は犯罪収益移転防止法上の取引時確認のことという理解でよいか。	犯収法の取引時確認だけに絞っているという意図はなく、取引の際のあらゆる確認に関して顧客管理態勢の整備を図られているかという意図で記載しています。
Ⅱ－３－１３－２－２－３（１）犯罪発生時		
42	「インターネット取引における不正アクセス・不正取引を認識次第」当局報告を求めるとある。インターネット取引における「不正アクセス」は、主にインターネットの非対面取引という特性を悪用し、権限外にアクセスするものであり、具体的には ID・PW の盗用などによるなりすましといったことと理解できるが、「インターネット取引における不正取引」といった場合に、具体的にどのような不正取引を想定しているのか、当局として、何か想定しているものがあれば確認したい。例えば、そもそも最初から人格を偽って取引を開始した、といったことを想定したものか。	保険契約者になりすまし、保険金を不正に受給することなどを想定しています。
43	「犯罪発生報告書」とあるので、報告すべき不正アクセス・不正取引とは、不正アクセス・不正取引のうち、犯罪に該当するものが発生した場合に、報告するという理解でよいか。	報告すべき対象としては、不正アクセス・不正取引のうち、犯罪に該当する恐れがあるものを想定しております。

少額短期保険業者向けの総合的な監督指針		
Ⅱ－３－１２－１－２　主な着眼点		
44	少短指針の II-3-12-1-1（システムリスク管理態勢）および II-3-12-2-1（インターネット取引）のそれぞれの意義において、少額短期保険業者の規模や業務特性に応じた態勢の整備が求められている。 少短指針の II-3-12-1-2 および II-3-12-2-2 の主な着眼点については、それぞれ総合指針の II-3-13-2-1-2 および II-3-13-2-2-2 に準じて取り扱うとされている。 この場合、少短指針の II-3-12-1-1 および II-3-12-2-1 の趣旨を踏まえ、少短指針の II-3-12-1-2 および II-3-12-2-2 の主な着眼点に係る態勢の整備は、少額短期保険業者の規模や業務特性に応じて行うとの理解で良いか。	ご認識の通りです。
貸金業者向けの総合的な監督指針		
Ⅱ－２－４－２（１）主な着眼点		
45	「ログイン、出金、出金先銀行口座の変更など、重要な操作時」に該当する操作の範囲については、各貸金業者が自社の取引内容、顧客属性、リスク評価結果等を踏まえて判断するとの理解で差し支えないでしょうか。	ご認識の通りです。
46	令和 7 年 10 月 15 日公表の「金融商品取引業者向けの総合的な監督指針」等の一部改正（案）のパブリックコメントNo.14 では、インターネット取引サービス外であり、かつ顧客の口座・資産に影響を及ぼさない、例えば「リサーチレポートの閲覧や WEB セミナー視聴用のシステムにログインするために、顧客に ID 及びパスワード（インターネット取引サービスのシステムにログイン時に使用するものとは	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。

	別のもの）の入力を促すページの URL が記載されたメールを送付すること」については、本規制の対象外である旨がコメントされております。 本改正案の「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」について、新規契約審査の本人確認や契約手続き等のため、顧客毎に特定画面に遷移させ、例えば受付番号や顧客属性（顧客の携帯電話番号等）の入力で遷移させる方法は、口座開設や貸付取引等のインターネット取引に必要な ID やパスワードと別のものであれば、当該方法に係る URL の記載は許容されるとの理解で良いか。 （理由）契約締結前の顧客であり、かつインターネット取引における ID とパスワードとは別のデータによる認証であり、フィッシング詐欺のリスクは低いと考えられる	
47	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の件について、法令に基づく義務を履行するために必要な場合は除く旨記載いただいております。 特定電子メール法に基づく受信拒否の通知先（URL 等）を記載する場合、当該 URL がログインを要する会員サイトへ遷移する構成であっても、『法令に基づく義務を履行するために必要な場合』として認められると解釈してよろしいでしょうか。	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。
48	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の件について、本指針における『適切な不正防止策』は、各社がリスクベースアプローチに基づき、送信ドメイン認証	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

	等の技術的対策を講じることで補完し合う関係にあると理解しております。URL 記載の可否についても、一律禁止ではなく、上記対策との組み合わせによりリスクが低減されていると判断できる場合は、柔軟な運用が許容されるという理解で相違ないでしょうか。	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。
49	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の件について、法令に基づく義務を履行するために必要な場合は除く旨記載いただいております。 「法令に基づく義務」とは具体的にどの範囲を指しますでしょうか。例えば、貸金業法上の書面交付義務に関連する通知、および特定電子メール法上の義務履行に関連する通知は、本例外の範囲に含まれるという理解でよろしいでしょうか。	具体的な範囲を全てご回答するのは困難ですが、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。
50	「期間ごとの借入上限を顧客が設定できる機能の提供」との要件について、本機能については、システム上で顧客がリアルタイムかつ能動的に上限額を変更・設定できる機能を想定されているものと理解しております。 一方で、実務上、顧客からの申請を受け付け、弊社にて審査のうえ増枠・減枠を行う運用も存在します。この「顧客からの申請に基づく個別の増枠・減枠対応」をもって、本指針が求める「機能の提供」を満たすものと解釈してよろしいでしょうか。それとも、審査を介さない顧客自身による即時設定機能の実装が必須となりますでしょうか。	期間ごとの借入上限を顧客が設定できる機能が提供されていれば、審査を介さない顧客自身による即時設定機能の実装は必ずしも必要ではありません。
51	【改正内容】 （中略） 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	貴重なご意見として承ります。

	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依頼等、提供するサービスの内容に応じた適切な不正防止策を講じているか。 （以下略） 【意見 1】 本改正案の趣旨であるフィッシング詐欺対策の強化には強く賛同する。他方で、当該記載が、ログインリンクや認証誘導 URL にとどまらず、返済確認、契約内容確認、書面確認、延滞回避、本人に対する重要なお知らせ確認等のための安全な導線まで広く抑制するものとして運用される場合、利用者保護に反する副作用が大きいとも考えられる。 フィッシング対策の必要性は理解するものの、正規の登録貸金業者によるメール・SMS 配信を実質的に廃止するような運用は、利用者の確認機会を損ない、利便性及び利用者保護の両面で問題がある。むしろ、正規の登録貸金業者については、送信者認証や公的に確認可能な識別表示等により真正性を判別できる仕組みを整備し、安全な通知配信を継続可能とすべきである。あわせて、システム改修・顧客周知・運用見直しに要する期間を踏まえ、十分な経過措置を設けるべきである。	
52	【意見２】	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

	本改正案において、メールやSMS等へのURL記載が制限される趣旨は、悪意ある第三者がなりすましサイトへ誘導し、顧客の認証情報（ID・パスワード等）を窃取するフィッシング被害の防止にあると理解している。 リスクベース・アプローチの考えに基づけば、実務においてフィッシングリスクを低減し、顧客のセキュリティを高度に担保できる以下の技術的または手法的な方策を講じる場合、本指針の求める「セキュリティの確保」の要件を満たすものとして、URLの記載が一律に制限されるものではないと理解して差し支えないか。 (1)ディープリンクを用いた公式アプリへの直接遷移 内容：メールやSMSから、ブラウザではなくアプリケーションを直接起動させる技術（ディープリンク）を使用する。 趣旨：端末内のアプリを確実に起動させることで、ブラウザ上の偽サイトへ誘導されるリスクを物理的に排除し、安全な正規アプリケーション内での取引を保証するため。 (2)セキュリティ啓発を兼ねた中間ページの設置 内容：「ここから先はログインが必要です」といった警告とともに、正規ドメインであることを確認させるメッセージを表示する中間ページを挟み、その後ログイン画面へ遷移させる。 趣旨：ユーザーに「今、自分がどこにアクセスしているか」を再確認させる「スピードバンプ（心理的ブレーキ）」を設けることで、機械的なリダイレクトに頼らず、ユーザーの能動的なドメイン確認を促し、フィッシング被害を未然に防止するため。 (3)遷移先におけるパーソナライズ情報の表示	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。

	内容：メールや SMS の文面または遷移先ページに、ユーザー本人しか知り得ない情報（氏名の一部伏字等）を表示する。 趣旨： ユーザーに対して「当該ページが公式なものである」という強力な信頼シグナル（トラストシグナル）を提示することで、偽サイトとの判別を明確化し、安全性を高めるため。 また、認証を必要としない自社 Web サイトのトップページや、お知らせ・キャンペーン情報等の閲覧用ページへのリンクは、フィッシングリスクが低いものとして制限されるものではないと理解して差し支えないか。	
53	【意見３】 本改正案において、メールや SMS にログインページへの URL を記載しないことが制限されている趣旨は、フィッシング詐欺被害の防止にあると理解している。 一方で、送信ドメイン認証技術（SPF、DKIM、DMARC 等）の導入も対策として求められており、送信ドメイン認証技術を導入することで、なりすましメールを技術的に排除することが可能となる。 ついては、高いセキュリティ水準を担保する送信ドメイン認証技術を導入している場合、顧客の利便性を考慮し、当該メール・SMS 内にログインページ等の URL を記載することは許容されるのか、あるいは技術的対策の有無にかかわらず、一律に記載を控えるべきなのか、指針における解釈を明確にされたい。	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。
54	システム開発の規模や人的・費用的リソースを踏まえると、改正施行時点において「フィッシングに耐性のある多要素認証」の実装が段階	ご認識の通りです。

	的対応となる場合も想定されますが、その場合であっても、施行時点で未完了であることをもって直ちに不適切と評価されるものではない、との理解で差し支えないでしょうか。	
55	改正案の注釈（注 2）に記載されている「具体的なスケジュール」の周知について、開発内容の詳細が未確定な段階において、「〇年度中の実装を目指す」といった概算レベル又は暫定的な目標の公表であっても、要件を満たしていると認められるでしょうか。	スケジュールについては、顧客の安心のために、できる限り明らかにすることが重要と考えます。
56	暫定的な対応として求められている「振る舞い検知やログイン通知等の検知機能の強化」についても、一定のシステム改修を伴うことから、これらの対応について施行日以降に順次対応を開始するスケジュールとすることは差し支えないでしょうか。	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。
57	本文中に「例えば、以下のような」として例示されている各種対策は、すべてを網羅的に実施することを求めているものではなく、各社が自社のリスク評価に基づき、適切な対策を選択的に実施することで足りる、との理解でよいでしょうか。	ご認識の通りです。
58	「顧客や業務の特性に応じた検討」や「リスクの存在を評価した上で対策の要否を決定」することが求められていますが、自社の分析に基づき、列挙事項とは異なる独自の手法により十分な対策を講じている場合、結果として列挙されている事項を必ずしも実施していなくても、本指針の趣旨を満たしていると評価されるでしょうか。	
59	特定の列挙項目が自社のサービス形態において実効性が低いと判断される場合において、より効果が高いと考えられる独自の対策にリソースを重点的に配分する判断は、監督上尊重されるものと理解してよいでしょうか。	ご認識のとおりですが、当該列挙項目以外の対策についても速やかに実施することが望まれます。

60	重要な操作時の対策例として記載されている「パスキーによる認証」について、監督上想定されている具体的な技術仕様や要件等があればご教示ください。	各社の状況が異なるため一概に申し上げることは困難ですが、当庁といたしましては、顧客が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、よくご検討ください。
61	「PKI をベースとした認証」や「パスキー」以外の技術であっても、事業者において「フィッシング耐性がある」と判断のうえ導入した場合、その有効性や妥当性はどのような観点で評価されるのでしょうか。	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。
62	不正防止策を講じているか否かの判断（具体的内容や水準）については、各社のリスク評価等に基づき判断するものと理解してよいでしょうか。	ご認識の通りです。
63	対策内容の具体的な設計や実装方法については、各社の判断に委ねられているとの理解で差し支えないでしょうか。 （例：URL やログインに関する記載方法についても、同等以上の不正防止策を講じている場合には、必ずしも一律の対応を求められないとの理解で相違ないでしょうか。）	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。
64	RCS・LINE など企業公式アカウントからの送信が明白なコミュニケーションツールについても、URL を含む連絡が同様に制限の対象となるのでしょうか。	顧客へ URL やログインリンクを送付し、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。
65	督促時に使用しているリンク付き SMS についても、今回の改定の対象となるか確認したい。なお、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されている点を踏まえ、リンク先に遷移しても、書面で送付している督促状や和解提案等	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。

	が表示されるのみで、認証情報等の入力を要しない場合には、対象外と整理されるとの理解で相違ないでしょうか。	
66	「フィッシング詐欺対策として、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する点」について、新規申込から契約締結に至る手続においては、利用者利便性の観点から、メール又は SMS に記載した URL を起点として手続きを行っている貸金業者も多い。当該運用について、現時点で同等の利便性を確保し得る代替手段が存在しない場合に、一律に不可と整理されることは、利用者利便性への影響が大きいと考えられる。そのため、本改正案における「代替的手段を採り得ない場合」の考え方の中に、新規申込・契約手続に係る連絡を含めて整理可能であるかについて、監督上の考え方を伺いたい。併せて、見直しに当たっては、一定の経過措置期間を設けた段階的対応とすることを要望する。	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。 システム開発等その他やむを得ない理由により、対応に一定の期間を要する場合があることは理解しますが、不正取引を防止するための対策であることから、可能な限り早期に対応することが望まれます。
Ⅱ－２－４－２（２）監督手法・対応		
67	「犯罪発生報告書」のフォーマットについて、内閣官房国家サイバー統括室が報告を収集する DDOS 攻撃事案共通様式、ランサムウエア攻撃事案共通様式と共通書式にしていただき、障害発生等報告、個人情報漏えい等の報告と兼ねることについてもご検討をお願いしたい。 （理由） 事業者負担（報告業務や対応負荷）軽減するため。	貴重なご意見として承ります。
その他		
68	本指針の適用開始時期について、配信システムの改修や顧客への周知期間を考慮し、一定の準備期間や経過措置を設ける予定はありますで	システム開発等その他やむを得ない理由により、対応に一定の期間を要する場合があることは理解しますが、不正取引を防止するための対策であることから、可能な限り早期に対応することが望まれます。

	しょうか。また、施行日以前に設定済みのメール配信設定についても即時変更が求められるのでしょうか。	
事務ガイドライン（第三分冊：金融会社関係　５　前払式支払手段発行者関係）		
Ⅱ－３－１－２－ ２ 主な着眼点（２） セキュリティの確保		
69	【該当箇所】 インターネット取引に係る情報セキュリティ全般に関する方針を作成し、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。 【意見】 「インターネット取引に係る情報セキュリティ全般に関する方針を作成し」とありますが、各事業者が業務内容・リスク特性に応じた方針や内部規程等を整備する趣旨との理解でよいでしょうか。 また、監督上の確認は、定期的な提出・報告を一律に求めるものではなく、必要に応じて態勢整備状況を確認する趣旨との理解で相違ないでしょうか。	ご認識の通りです。
70	【該当箇所】 さらに、例えば、以下のような不正防止策を講じているか。 ・取引時や他の銀行口座との連携サービス提供時におけるフィッシングに耐性のある多要素認証の提供 【意見】一部のサービスではプリペイドの新規入金に係る収納代行を委託しており、口座振替やクレジットカードによる入金ができるようになっております。	ご認識の通りです。

	今回の改正による不正防止策の実装について、委託先に対しても同様の不正防止策を講じさせることが求められているとの理解でよいでしょうか。	
事務ガイドライン（第三分冊：金融会社関係　１４　資金移動業者関係）		
Ⅱ－２－３－１－ ２－２ 主な着眼点（１） 内部管理態勢の整備		
71	【該当箇所】 インターネット等の不正アクセス・不正取引等の犯罪行為に対する対策等について、犯罪手口が高度化・巧妙化し、被害が拡大していることを踏まえ、最優先の経営課題の一つとして位置付け、取締役会等において必要な検討を行い、セキュリティ・レベルの向上に努めるとともに、利用時における留意事項等を顧客に説明する態勢が整備されているか。 【意見】 インターネット等における不正アクセス・不正取引対策を経営上の重要課題として位置付け、経営陣が適切に関与することは重要であると考える。 その上で、「取締役会等において必要な検討を行い」との記載については、必ずしも取締役会という会議体に限定するものではなく、各事業者において、その組織体制・ガバナンス態勢に応じた適切な体制の下で、必要な検討及び意思決定が行われることを含む趣旨であることを確認させていただきたい。	ご認識の通りです。
Ⅱ－２－３－１－ ２－２ 主な着眼点（２） セキュリティの確保		
72	【該当箇所】	ご認識の通りです。

	ログイン、出金、出金先銀行口座の変更など、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） 【意見】 例示の方法以外に、携帯電話会社の回線認証のように、フィッシングに耐性のある多要素認証は存在しております。例示の方法以外の認証手法を活用する場合であっても、その安全性やフィッシング耐性を合理的に説明できるものであれば、ガイドライン改正の趣旨にかなうとの理解でよいでしょうか。	
73	【該当箇所】 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間は、代替的な多要素認証を提供するとともに、当該実装及び必須化に向けた具体的なスケジュールについて顧客に周知する必要がある。また、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。 【意見】 「振る舞い検知やログイン通知等の検知機能」とあるが、この記載の趣旨は、事業者・利用者の双方またはいずれかがが不正の兆候に適時に気づき、対応し得る態勢を整備することを求めるものであるとの理解でよいか。	ご認識のとおりです。
74	【該当箇所】 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間は、代替的な多要素認証を提供するとともに、当該実装及び必須化に	各社で状況が異なることから具体例を一概にお示しすることは難しいと考えます。

	向けた具体的なスケジュールについて顧客に周知する必要がある。また、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。 【意見】 振る舞い検知については、現時点においても各種の手法が存在する一方、その導入方法や有効性、適用場面には幅があり、サービス特性等によって期待される効果も異なるものと考えられる。 そのため、振る舞い検知により想定される検知対象や考え方について、一定の例示をお示しいただけると、各事業者における実務対応の明確化に資すると考える。	
Ⅱ－２－３－１－２－２ 主な着眼点（３） 顧客対応		
75	【該当箇所】 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。 【意見】 不正取引防止策の利用者への普及を進めることは重要であり、事業者としても継続的な周知・導入促進に取り組む必要があると考える。もっとも、パスキー等の新たな認証手段の普及状況は、事業者の努力だけで実現できるものではなく、世の中全般で一定程度利用が広がることにより、加速度的に普及が進む可能性もある。 そのため、「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。」との文言については、普及状況のみをもって一律に評価するのではなく、各事業者によるモニタリング、利用者への周知、導	貴重なご意見として承ります。なお、3 月に各種媒体において、動画広告を実施したほか、理解促進のためのリーフレットを金融庁 HP に掲載しておりますので、顧客説明等の際にご活用ください。 《https://www.fsa.go.jp/news/r7/sonota/20260416-2/20260416-2.html》

	入促進のための追加的な施策その他の取組状況を踏まえて評価される趣旨であることを明確化いただきたい。 また、こうした対策の普及促進に当たっては、政府・当局による周知・広報等の後押しも重要であると考える。	
主要行等向けの総合的な監督指針等		
Ⅹ－３－２（３）サイバーセキュリティ管理		
76	電子決済等代行業者は銀行法に基づき、取得した銀行口座の情報をユーザーに提供する等の業務を行っていますが、銀行以外の金融機関（保険会社様、前払式支払手段発行者様、資金移動業者様を含む）にも機能連携を行い、複数の口座に跨る情報の一覧化等を行うことにより、適切な資産管理を行うサービス等も提供しています。 電子決済等代行業者が金融機関との機能連携を行う際に、金融機関への「ログイン」時にフィッシング耐性のある認証が要求されると、いわゆるスクレイピングと呼ばれる手法での機能連携を行うことが困難となり、電子決済等代行業者の既存の業務に、大きな支障が生じることが予想されます。 まずは短期的に、参照系の（金融機関のデータの読取のみを行う）業務と、取引・出金・譲渡等の変更等の重要な操作の連携が可能な更新系の業務とを分別し、後者の重要な操作に対してのみフィッシング耐性のある認証手段を導入していくことを提案いたします。 また、中長期的には金融機関（本件においては保険会社様、前払式支払手段発行者様、資金移動業者様）においてAPIを整備していただき、そのタイミングで参照系業務での機能連携時にも、フィッシング	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。

	耐性のある認証手段を導入していくという、計画的なアプローチが必要だと考えます。	