「保険会社向けの総合的な監督指針」等の一部改正（案）の公表について

No	該当箇所	意見提出
1	II-3-13-2-1-2(5)	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
2	II-3-13-2-1-2(5)②	「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。
3	II-3-13-2-2	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。
4	II-3-13-2-2-1	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。
5	II-3-13-2-2-2	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。
6	II-3-13-2-2-2(1)	「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。
7	II-3-13-2-2-2(2)	「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。
8	II-3-13-2-2-2(2)	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。 なお、「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。
9	II-3-13-2-2-2(2)	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。
10	II-3-13-2-2-2(2)	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。
11	II-3-13-2-2-2(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。
12	II-3-13-2-2-2(2)	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。

13	II-3-13-2-2-2(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。
14	II-3-13-2-2-2(2)	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
15	II-3-13-2-2-2(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（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。
16	II-3-13-2-2-2(2)	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。
17	II-3-13-2-2-2(2)	「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。
18	II-3-13-2-2-2(2)	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。
19	II-3-13-2-2-2(2)	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。
20	II-3-13-2-2-2(2)	「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。

21	II-3-13-2-2-2(2)	「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。
22	II-3-13-2-2-2(2)	「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。
23	II-3-13-2-2-2(2)	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。
24	II-3-13-2-2-2(3)	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。
25	II-3-13-2-2-2(4)	「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。
26	II-3-13-2-2-3(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」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。また、「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。