弁護士法人　三宅法律事務所

Mivake　& Partners

デジタル・ガバナンス／サイバーセキュリティニュース　No.1

保険会社向けの総合的な監督指針の改正のご報告

― メール・SMS へのログインリンク記載の原則禁止、全登録顧客に対する多要素認証の必須化及び犯罪発生報告書の新設 ―

平素より大変お世話になっております。

金融庁は、令和8年7月 17 日、「保険会社向けの総合的な監督指針」等の一部改正（案）に対するパブリックコメントの結果等を公表し、**改正後の監督指針を同日から適用**いたしました[1]。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の改正であり、一部改正に関係するものとして計 76 件の意見が寄せられています。**経過措置は設けられておらず、既に適用済みである**点にご留意ください。

本改正は、保険会社向けの総合的な監督指針に「インターネット取引」（Ⅱ－3－13－2－2）を独立の監督項目として新設し、**内部管理態勢の整備、セキュリティの確保、顧客対応及び監督手法・対応を一体として規定するもの**です。あわせて、様式・参考資料編に**「犯罪発生報告書（インターネット取引関連）」**が新設されました。なお、本改正は保険会社のみを対象とするものではなく、少額短期保険業者、貸金業者、金融サービス仲介業者、主要行等及び中小・地域金融機関（いずれも電子決済等代行業関係）、前払式支払手段発行者並びに資金移動業者の各監督指針・事務ガイドラインについても、同日、同趣旨の改正が行われています。本ニュースレターは保険会社向けの改正を中心に取り上げますが、パブリックコメント回答には他業態向けの改正に関する回答も含まれており、同一文言の解釈の手がかりとなることから、適宜あわせて紹介いたします。

本改正は、単に新たな認証技術の導入を求めるものではありません。**従来の顧客導線をフィッシング対策の観点から見直し、予防・検知・遮断・顧客通知・被害回復・当局報告を一つの管理サイクルとして運営する態勢への転換**を求めるものです。特に、メール・SMS 内のログインリンクという従来一般的であった顧客導線については、業界から多数の例外要望が提出されましたが、金融庁はそのほぼすべてを認めませんでした。

本ニュースレターでは、新旧対照表及びパブリックコメントに対する金融庁の考え方を踏まえ、改正の内容と実務上の留意点を整理いたします。末尾には理解度チェック（〇×問題 10 問）を付しておりますので、社内研修等にもご活用いただけますと幸いです。

令和8年7月 18 日
弁護士法人三宅法律事務所

＊本ニュースレターに関するご質問・ご相談がありましたら、下記にご連絡ください。
弁護士法人三宅法律事務所
弁護士　渡邉雅之（執筆者）
TEL 03-5288-1021　FAX 03-5288-1025
Email: m-watanabe@miyake.gr.jp

[1]金融庁「「保険会社向けの総合的な監督指針」等の一部改正（案）に対するパブリックコメントの結果等の公表について」（令和8年7月 17 日）（https://www.fsa.go.jp/news/r8/sonota/20260717-2/20260717.html）。パブリックコメントは令和8年3月 30 日から同年4月 30 日にかけて実施された（https://public-comment.e-gov.go.jp/pcm/1040?CLASSNAME=PCM1040&id=225026021&Mode=1）。以下、本文中の「項番」は、同ページ別紙1「コメントの概要及びコメントに対する金融庁の考え方」の項番を指す。

保険会社向けの総合的な監督指針の改正のご報告
― メール・SMS へのログインリンク記載の原則禁止、全登録顧客に対する多要素認証の必須化及び犯罪発生報告書の新設 ―

【目次】

1　改正の全体像――個別の例示から「インターネット取引管理」へ

(1) 見落とされやすい「削除」

今回の改正では、従来のシステムリスク管理態勢（旧Ⅱ－３－１３－２－２(5)②③）に置かれていた次の例示が、いずれも削除されている。

- 可変式パスワードや電子証明書などの、固定式の ID・パスワードのみに頼らない認証方式
- 複数経路による取引認証、ハードウェアトークン等によるトランザクション認証
- セキュリティ対策ソフトの利用者への提供、ウィルス感染状況の検知・警告ソフトの導入
- 電子証明書を IC カード等、取引に利用しているパソコンとは別の媒体・機器へ格納する方式
- **（注）出金先口座について顧客と名義が異なる指定・変更を認めないこととし、更に転送不要郵便により書面を送付する等の措置を講じている場合には、取引のリスクに見合った対応がなされているものと考えられる旨の記述**

特に最後の（注）は、従来、多くの会社が「取引のリスクに見合った対応」を説明する際の拠り所としてきた記述である。これが姿を消し、新設のインターネット取引の章に統合された以上、**旧（注）に依拠して「対応済み」と整理していた会社は、リスク評価の枠組みそのものを組み直す必要がある**。改正後のサイバーセキュリティ管理（Ⅱ－３－１３－２－１－２(5)②）は、インターネット取引を行う場合に新章の規定に基づく適切な取扱いを確保する態勢を整備しているかを問う参照規定に置き換えられた。

(2) 新設項目の構造

条項	内容
Ⅱ－３－１３－２－２－１	意義（非対面取引特有のリスク、顧客の財産の安全な管理、利用者利便の確保と利用者保護の徹底）
同－２－２(1)	内部管理態勢の整備（最優先の経営課題の一つとしての位置付け、取締役会等における検討、全社態勢、金融 ISAC・JPCERT／CC 等の活用、PDCA サイクル）

条項	内容
同－２－２(2)	セキュリティの確保（方針の作成・検証、多層防御、フィッシング詐欺対策、重要な操作時の多要素認証等）
同－２－２(3)	顧客対応（注意喚起、取引内容の適時確認、届出受付、迅速な顧客連絡、普及状況のモニタリング、被害補償、記録保存・捜査協力）
同－２－２(4)	その他（取引時確認等の顧客管理態勢、外部委託）
同－２－３	監督手法・対応（(1)犯罪発生時＝犯罪発生報告書、(2)問題認識時＝法 128 条報告・法 132 条業務改善命令）
Ⅴ－５－７	保険仲立人（規模・業務特性を踏まえ、保険会社における取扱いを参考に適切な措置）
様式・参考資料編	様式Ⅱ－３－１３－２－２－３(1) 犯罪発生報告書（インターネット取引関連）を新設

(3)改正の本質

従来	改正後
認証方式・不正防止策を個別に例示	インターネット取引全体の管理態勢を新設
固定式 ID・パスワードのみに頼らない認証	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
不正なログイン・異常な取引等の検知	振る舞い検知、追加の本人認証、適時遮断、顧客通知、ログ保存
主としてシステム上の対策	取締役会等の関与、全社態勢、PDCA、顧客対応、当局報告
個別的な不正防止策	リスクベースの多層防御と継続的な見直し

改正の本質は、サイバー対策を、システム部門の技術管理から、**顧客保護と業務運営に関する全社的な経営管理**へ引き上げた点にある。

2 対象範囲――資産の移転を伴う取引に限られない

対策を講じるべき対象が、保険料の収納、保険金の支払、解約返戻金の請求等、顧客の資産の移転を直接伴う取引に限られるかが問われたが、金融庁は、**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となる**との理解を明確に肯定した（項番 8）。

もっとも、「インターネット取引」及び「重要な操作」の範囲について、具体例は示されていない。

「取引」に顧客情報の変更、補償内容の変更、保険金請求等が含まれるか、保険募集に係る取引に限られるかという問いに対する回答は、「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。この点を踏まえ、よくご検討ください」というものであった（項番 10）。ログインを伴わず、ウェブサイト上で顧客が手続内容等を一方的に入力する類型について多要素認証は義務化されないかという問いにも同旨の回答にとどまり、対象外とは明言されていない（項番 11）。

契約者情報・メールアドレス・電話番号・保険金受取人・保険料収納口座・支払先口座の変更、解約・返戻金請求等が「重要な操作」に当たるかについても、顧客層、取扱商品、取扱額等が各社で異なることから具体例を一概に示すことは困難であり、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された（項番 30）。

したがって、これらの手続は、**あくまで各社が対象該当性を検討すべき候補**であって、金融庁が該当すると回答したものではない点に留意を要する。実務上は、インターネットバンキング相当の機能のみを念頭に置くのではなく、**顧客情報又は契約上の権利関係に重大な影響を与えるオンライン操作を横断的に棚卸しし、なりすましが生じた場合の影響度に基づいて対象を定義すること**が出発点となる。

3 リスクベース・アプローチの射程と限界

今回の改正で追記される不正防止策や態勢整備について、**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）に取り組むことが求められている**との理解は、「ご認識の通りです」と肯定されている（項番 7）。

同一の文言を有する他業態向け監督指針に関する回答も、解釈の手がかりとなる。例示された各種対策はすべてを網羅的に実施することを求めるものではなく、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れば足りるとされ（項番 57）、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には、列挙事項を必ずしも実施していなくても趣旨を満たすとされた（項番 58）。独自対策へのリソースの重点配分についても、「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」と、留保付きで是認されている（項番 59）。

ただし、リスクベース・アプローチであることは、各社が自由に対策を見送れることを意味しない。回答全体からは、少なくとも次の各点について、金融庁が**原則的な最低線**として求めていることが読み取れる。

- パスワード入力を促すページの URL・ログインリンクの不記載
- 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
- 未実装期間中の代替的な多要素認証の提供、スケジュールの顧客周知及び検知機能の強化
- 不正なログイン・異常な取引等の検知、顧客への通知及びログの保存

各社の裁量が認められるのは、**これらの方向性を採用するか否かではなく、対象・方法・導入順序・要求頻度をどう設計するか**の局面である、と整理すべきである。

4 最大の争点――メール・SMS のログインリンク

(1) 改正指針の内容

改正指針は、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こと（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。）を求め、あわせて、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こと、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を挙げている。

(2) 業界からの例外要望は、ほぼすべて斥けられた

パブリックコメントでは、顧客利便性や保険業務の特性を理由として、多数の例外要望が提出された。しかし金融庁の回答は、いずれも**「原則として、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すべきではないと考えます」**という定型の反復であり、包括的な例外は一切認められなかった。

業界からの主な要望	金融庁の結論
顧客からの電話問合せに応じたマイページ・FAQ の URL 送付（項番 2）	例外とせず
手続完了・中途手続再開・内容確認メール内のマイページリンク（項番 3）	例外とせず
商品・サービス説明画面を介した誘導（ログイン画面へ直接遷移しない）（項番 4）	例外とせず
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（項番 5、18）	対象外と明言せず。極力控え、代替的手段の導入を検討することが望ましい
ID と紐づかない、パスワードのみの入力ページ（セキュアファイル転送等）（項番 6）	例外とせず
フィッシング詐欺への注意喚起を促すガード文言の併記（項番 21、22）	例外とせず

業界からの主な要望	金融庁の結論
二要素認証が実装されたページへのリンク（項番 23）	例外とせず
送信ドメイン認証（DMARC・BIMI 等）を実施済みのメール（項番 24、28、53）	例外とせず
顧客の能動的操作を起点とし、失効措置・追加本人認証等を講じる場合（項番 26）	例外とせず
満期・継続手続案内、カード決済エラー時の案内（無保険状態の回避）（項番 38、39）	例外とせず
認証を要しない公式ホームページのトップページ URL（項番 28、38、39）	例外とせず
通話中・通話直後の SMS、顧客の行動起点のメール、事故受付・保険知識の案内（項番 29）	個別具体的に判断するとしつつ、原則として記載すべきでない
ダイレクト販売のビジネスモデル上の必要性、保険は即時出金がなくリスクが低いこと（項番 17）	例外とせず
保険会社のみが導線を変更しても被害軽減効果は限定的であること（項番 20）	他業態も同様の改正を行っており、金融業界全体で取り組むことは業界の信頼性の向上に資する
経過措置・準備期間の設定（項番 66、68）	システム開発等により期間を要することは理解するが、可能な限り早期の対応が望まれる

顧客からの依頼、二要素認証、送信ドメイン認証、注意喚起文言、資産性の低さ。これらはいずれも、単独では例外事由とならない。

（3）例外はどこまで狭いか

金融庁が例外として繰り返し挙げるのは、**「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」**に限られる。

しかも、特定電子メール法に基づく受信拒否の通知先 URL については、これを例外として認めつつ、**「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。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」**と付言された（項番 47）。法令上の例外に該当する場合であっても、遷移先がログイン可能画面となる設計は避けるべきである。「法令に基づく義務」の具体的範囲は示されていない（項番 49）ため、例外に依拠する場合には、根拠法令・条項と代替不能性を文書化して残す必要がある。

（4）射程はメール・SMS に限られない

見落としやすい点として、RCS・LINE 等の企業公式アカウントからの送信についても、**「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。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」**とされている（項番 64）。

すなわち改正指針は、ログイン画面への直接リンクだけでなく、**顧客に「送られてきたメッセージ内のリンクを踏む」習慣を形成させること自体をフィッシングリスクとして捉えている**と評価すべきである。棚卸しの対象は、メール・SMS にとどまらず、アプリのプッシュ通知、公式メッセージングアカウント等を含む、顧客向けアウトバウンド・チャネル全般に及ぶ。

（5）検知通知メールとの整合

改正指針は、不正なログイン・取引・出金・保険金受取人の変更等を早期に検知するため、電子メール等により顧客に通知を送信する機能の提供を求めている。他方でリンクの記載は制限されるため、通知メールの文面設計が問題となる。

この点、「ログインがありました」「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かという問いに対する回答は、「よくご検討ください」にとどまった（項番 27）。実務的には、通

知にはリンクを付さず、公式アプリ・公式サイト（ブックマーク）からの確認を促す文面を原則とし、なりすまし通知を警戒する顧客の混乱を招かないよう、通知文面の定型化と事前の周知を併せて行う設計が穏当である。

（6）実務上の棚卸し

区分	主な対応
ログイン画面への直接リンク	原則として廃止し、代替導線へ移行
ログインにつながる手続入口（説明画面経由を含む）	遷移経路を含めて評価。説明画面を経由しても例外とならない
ログイン不要の個人情報入力画面	極力控え、代替的手段を検討
商品説明・FAQ 等の一般ページ	認証画面への導線の有無を個別に評価
法令上リンクの記載が必要なもの	根拠法令・代替不能性を記録。遷移先がログイン可能画面とならない設計に
顧客の操作を起点とする通知	例外とならない。通知内容・送信時期を個別に評価
異常検知・取引通知	リンクを付さず、公式アプリ・公式サイトでの確認を案内
RCS・LINE 等の公式アカウント、プッシュ通知	メール・SMS と同様に極力控える

5 フィッシングに耐性のある多要素認証

（1）重要な操作時の実装及び必須化

改正指針は、ログイン、出金、振込先金融機関口座（出金先口座）の指定・変更等の手続きなど、**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）**を求めている。

「パスキーは PKI を基盤とする認証技術の一種であり、両者の並列表記は誤解を招く」との意見、「パスキーは必ずしもスマートフォン等の別デバイスを要しない」との意見は、いずれも「貴重なご意見として承ります」との回答にとどまり、文言は修正されていない（項番 14、15）。

認証方式はパスキーに限定されない（項番 34）。他業態向けの回答では、携帯電話会社の回線認証など例示以外の方式であっても、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された（項番 72）。もっとも、その有効性・妥当性の評価観点については「個々の事情や各社の方針に応じて判断が必要」とされており（項番 61）、フィッシング耐性の説明責任は各社が負う構造である。

（2）既存顧客を含む全登録顧客が対象

金融庁は、フィッシングに耐性のある多要素認証の必須化について、**今後新たに登録する顧客のみならず、すべての登録顧客に対して求めるもの**と明言した（項番 34）。「新規顧客から順次」という設計は、それ自体では改正の要求を満たさない。

（3）導入時期――改正指針は既に適用済み

改正後の監督指針は、**令和8年7月 17 日から適用されており、経過措置は設けられていない**。適用開始時期について一定の準備期間や経過措置を設ける予定はあるかとの意見に対しても、「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」との回答にとどまった（項番 68）。

完了時期は一律でないとの理解を求める複数の意見に対する回答は、いずれも、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るが、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る、というものであった（項番 13、16、31、34、35、56）。

他方、**施行時点において実装が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**との理解は、「ご認識の通りです」と肯定されている（項番 54）。

すなわち、**「施行時点未完了＝直ちに不適切」ではないが、計画と進捗の合理性が問われる**構造である。裏を返せば、計画も進捗管理もないまま未実装である状態は正当化されない。

(4)移行期間中の代替措置（注2）

完全実装までの間、従来の ID・パスワード方式を継続するだけでは足りない。改正指針は、次を求めている。

- 代替的な多要素認証の提供
- 実装及び必須化に向けた具体的なスケジュールの顧客への周知
- 振る舞い検知やログイン通知等の検知機能の強化

スケジュールの粒度について、「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足りるかという問いに対しては、「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」とされ、概算での足切りは是認されていない（項番 55）。

(5)顧客要望による解除（注1）

高齢者、法人顧客、スマートフォンを保有しない顧客等への配慮を求める意見に対し、金融庁は、次の立場を明示した（項番 33、35）。

> **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。**

顧客が同意していても、それ自体は解除を正当化しない。やむを得ず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、解除率の状況をフォローした上で、認証技術や規格の発展も勘案しながら、解除率が低くなるよう多要素認証の方法の見直しを検討・実施する必要がある。

もっとも、解除率について一律の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とされている（項番 36）。管理指標としては、解除率そのものに加え、解除理由の分析と代替策の妥当性を記録することが実務的である。

(6)要求頻度

多要素認証の要求頻度（有効期間）について、「アクセス（ログイン）の都度要求すべきか」「最低でも 1 日に 1 回か」といった最低限の基準の提示を求める意見に対し、金融庁は、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し、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、適切な要求頻度を検討すべきとした（項番 32）。各社には、保有情報の質・量、インターネットへの露出、顧客属性、商品特性等を踏まえ、設定した頻度の合理性を説明できる根拠資料の整備が求められる。

6 認証だけでは足りない――多層防御

改正指針は、**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**を問うている。列挙されている不正防止策は、次のとおりである。

- 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
- 顧客が身に覚えのない第三者による不正なログイン・取引・出金・保険金受取人の変更などを早期に検知するための、電子メール等による顧客への通知機能の提供
- 認証に連続して失敗した場合のアカウント・ロックの自動発動機能の実装及び必須化

- ログイン時の振る舞い検知及び事後検証に資するログイン・取引時の情報の保存
- 不正アクセスの評価に応じた追加の本人認証、不正が疑われるアクセスの適時遮断、不正アクセス元からのアクセスのブロック
- 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
- 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

参考として、金融情報システムセンター「金融機関等コンピュータシステムの安全対策基準・解説書」及びフィッシング対策協議会「フィッシング対策ガイドライン」が掲げられている。

すなわち、改正指針が求めるのは、**予防 → 検知 → 追加認証・遮断 → 顧客通知 → ログによる事後検証**という一連の管理であり、多要素認証を導入すれば足りるという発想は採られていない。

なお、電子決済等代行業者との機能連携（スクレイピング方式）への影響を指摘し、参照系業務と更新系業務を分別して段階的に導入すべきとの意見に対しても、回答は「可能な限り早期に対応することが望まれます」にとどまった（項番 76）。API 整備を含む中長期的な連携設計は、各社の課題として残されている。

7 内部管理態勢・取締役会等・PDCA サイクル

改正指針は、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う**ことを求めている。

ここでいう「取締役会等」については、他業態向けの回答において、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が確認されている（項番 71）。

取締役会等に期待される役割としては、次のものが考えられる。

- 重要なサービス・操作の特定及びリスク評価結果の確認
- 対策方針及び導入計画の承認
- 段階的導入に伴う残存リスクの把握
- 対策の有効性及び不正被害状況の確認
- 顧客周知及び被害補償方針の監督

あわせて、金融 ISAC や JPCERT／CC 等の情報共有機関等を活用して、犯罪の発生状況や犯罪手口に関する情報の提供・収集を行うとともに、有効な対応策等を共有し、自らの顧客や業務の特性に応じた検討を行った上で、今後発生が懸念される犯罪手口への対応も考慮することが求められる。情報の収集に当たっては、金融関係団体や金融情報システムセンターの調査等、金融庁・警察当局から提供された犯罪手口に係る情報などを活用することが考えられる旨が注記されている。

さらに、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 サイクルが機能しているかが問われる。PDCA の具体的な取組方法（モデル）や事例の提示を求める意見に対しては、各社の状況が異なるため具体的な取組を一概に示すことは難しいと回答された（項番 12、19）。

したがって、各社は少なくとも次の各項目を、自社の管理プロセスとして文書化する必要がある。

① 対象サービス・操作の棚卸し（メール・SMS・公式アカウント等の導線を含む。）

② 不正手口・脅威情報の収集

③ リスク分析・評価

④ 対策の選択・導入

⑤ 効果検証

⑥ 不正件数、認証普及率、解除率等のモニタリング

⑦ 対策の見直し

⑧ 取締役会等への報告

なお、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の作成については、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であり、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であることが確認されている（項番 69）。

8 顧客対応・被害補償

改正指針は、システム上の予防策のみならず、被害発生後の顧客対応も監督上の着眼点としている。

- ID・パスワード等の個人情報の詐取の危険性、類推されやすいパスワードの使用の危険性、被害拡大の可能性等のリスクの説明及び顧客に求められるセキュリティ対策事例の周知を含めた注意喚起
- 顧客自らによる早期の被害認識を可能とするための、顧客が取引内容を適時に確認できる手段
- 顧客からの届出を速やかに受け付ける体制及び顧客が容易に理解できる形での周知（公表を含む。）の体制
- 被害にあう可能性がある顧客を特定可能な場合における、可能な限り迅速な顧客への連絡等による被害の最小限の抑制
- 不正取引を防止するための対策の利用者への普及状況の定期的なモニタリング及び追加的な施策
- 被害状況を十分に精査し、顧客の態様やその状況等を加味した上での、被害補償を含む被害回復に向けた真摯な顧客対応
- 不正取引に関する記録の適切な保存並びに顧客及び捜査当局からの資料提供等の要請への誠実な協力

説明の水準・頻度についての具体的な基準は示されていない（項番 40）。もっとも金融庁は、本年 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同庁ホームページに掲載しており[2]、顧客説明等の際に活用することが案内されている（項番 75）。

普及状況のモニタリングについては、パスキー等の新たな認証手段の普及は事業者の努力だけで実現できるものではないとの意見が出されたが、「貴重なご意見として承ります」との回答にとどまった（項番 75）。**普及率が上がらないこと自体は免責事由とならず、モニタリングと追加施策の実施記録が問われる**と理解すべきである。

このため、不正アクセス・不正取引対策は、システム部門のみで完結する問題ではない。法務、コンプライアンス、リスク管理、カスタマーサービス、保険金支払、広報、代理店管理及び経営層を含む横断的なインシデント対応態勢が必要となる。

9 取引時確認・外部委託・代理店・少額短期保険業者・保険仲立人

(1)取引時確認

改正指針は、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を求めている。ここでいう「取引時確認」について、金融庁は、**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る**と回答した（項番 41）。犯収法対応のみをもって足りるとする整理はできない。

(2)外部委託・代理店

インターネット取引に関し外部委託がなされている場合には、外部委託に係るリスクを検討し、必要なセキュリティ対

[2]金融庁ホームページ（https://www.fsa.go.jp/news/r7/sonota/20260416-2/20260416-2.html）。

策が講じられているかが着眼点とされている。管理態勢は保険会社に限らず保険代理店等についても対象となり、規模や業務特性を踏まえて態勢整備が求められる（項番 9）。また、他業態向けの回答では、収納代行等を委託している場合に、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ることが確認されている（項番 70）。

点検の対象としては、次のものが考えられる。

- 代理店のオンライン募集システム
- 委託コールセンターによるメール・SMS の送信
- SaaS 型顧客ポータル、本人認証サービス
- メール配信事業者、不正検知・監視事業者
- 保険金請求・契約変更の受付サービス

委託契約においては、認証方式、リンク送信ルール、ログの保存・提供、インシデント通知、原因調査への協力、再委託、顧客対応及び**当局報告への協力**について、責任分界を明確にする必要がある。

（3）少額短期保険業者・保険仲立人

少額短期保険業者向けの総合的な監督指針の主な着眼点は、総合指針の該当規定に準じて取り扱われるが、その態勢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が肯定されている（項番 44）。保険仲立人についても、規模や業務特性を踏まえ、保険会社における取扱いを参考に適切な措置を講じる必要がある（Ⅴ－5－7）。

10 犯罪発生報告書（インターネット取引関連）の新設

（1）報告義務

改正指針は、**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」により当局宛て報告を求める**ものとしている。

「不正取引」として想定されているのは、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である（項番 42）。報告すべき対象は、不正アクセス・不正取引のうち、犯罪に該当する「恐れ」があるものとされており（項番 43）、犯罪該当性が確定してからの報告では足りない。記載要領上、ここでいう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による顧客口座等における保険契約に関する手続き等を指す。

（2）様式の記載事項

欄	内容
宛先・提出者	金融庁長官宛て。金融機関名、代表者名、担当者情報（所属・氏名・電話番号・E-mail）
管理欄	案件識別番号、発覚日、初回報告日、更新日（第二報以降）、最終報告日
(1)	発覚の端緒（顧客からの申し出／顧客以外からの連絡／システムによる検知／その他）
(2)	ログイン時・出金時・保険受取人の変更時等の多要素認証の導入状況（ログイン時／出金時及び出金先銀行口座の変更時／保険受取人の変更時／その他の操作時（銀行口座との連携サービス提供時、メールアドレス変更時など））※必須化（デフォルトとして設定）の状況がわかるように記載
(3)	事案の形態（不正アクセスのみ発生／不正取引の発生）及び事案の概要
(4)(5)	被害件数、被害金額
(6)	不正アクセス又は不正取引の発生要因
(7)	再発防止策
(8)	被害者への対応の状況・補償方針、処理・補償の進捗状況（補償事由の発生なし／調査・検討中／完結）
(9)	その他特筆すべき事項

(2)欄の存在が決定的に重要である。事案が発生した場合、当該会社における多要素認証の実装・必須化の状況が、

操作類型ごとに当局へ開示される構造となっている。未導入であった場合には、その理由、代替措置及び導入計画について説明を求められることが当然に想定される。**改正への対応状況が、事故報告の一部として制度的に可視化される**点は、従来の障害発生等報告にはなかった特徴である。

(3)報告の時系列管理——「翌々営業日」が実務上の要諦

記載要領は、次のとおり明確な時限を定めている。**事故発生後に初めて様式を確認するのでは間に合わない。**

段階	内容
初回報告	事案の概要が判明した時点で報告し、発生要因、再発防止策等は調査中であっても差し支えない。ただし、事案の概要が判明していない場合でも、事案を認識した日の翌々営業日までに現状の報告を行う
更新報告	状況の変化等がある場合は、記載内容を更新して報告を行う(追加報告の都度、更新日を更新する。)。ただし、状況の変化等が無い場合でも、初回報告から 1 か月以内に現状の報告を行う
最終報告	被害者への対応状況・補償方針の「処理・補償の進捗状況」が「補償事由の発生なし」又は「完結」となった場合に、最終報告を行う(最終報告日欄に日付を記入)
案件単位	発覚から「補償事由の発生なし」又は「完結」となるまでを一つの案件として「案件識別番号」を付す(番号の形式は任意)
再発時	最終報告以降、同様の事案が生じた場合には、別事案として初回報告を行う

したがって、平時から、インシデント対応規程に次の事項を定めておく必要がある。

- 初回報告の要否の判断者(「犯罪に該当する恐れ」の判断基準を含む。)
- 認識日の特定ルール(誰の認識をもって起算するか)——翌々営業日という時限に直結する
- 金融庁への提出責任者及び連絡窓口
- 情報収集を行う各部門と情報集約フロー
- 確認済み事実と推測・調査中事項の区分(初回報告は調査中で差し支えないため、確定を待つ運用は誤りである。)
- 更新報告の期限管理——状況の変化等が無くても 1 か月以内に報告義務が生じる
- 最終報告の完了基準(補償の「完結」の判断基準)
- 案件識別番号の採番ルール及び顧客ごとの被害状況の管理方法

なお、記載要領上、報告は顧客ごとの被害状況等について行うものとされる一方、案件識別番号は発覚から完結までを一つの案件として付すものとされている。同一の手口による複数顧客の被害を 1 案件として扱うか、顧客ごとに採番するかは記載要領上明示されておらず、各社において運用を整理し、社内のインシデント管理と当局報告を整合させる必要がある。

(4)他の報告制度との関係

犯罪発生報告書の様式について、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・ランサムウェア攻撃事案の共通様式と共通書式にし、障害発生等報告や個人情報漏えい等の報告と兼ねることの検討を求める意見に対しては、「貴重なご意見として承ります」との回答にとどまった(項番 67)。

したがって実務上は、①犯罪発生報告書、②障害発生等報告書、③個人情報保護法上の漏えい等報告(個人情報保護委員会宛て)を並行して管理する必要がある。なりすましによる不正アクセス事案では、これらが同時にトリガーされ得るため、報告要否の判定を一枚のフローに統合しておくことが有用である。なお、様式については「提出対象となる金融機関等に別途提示します」との回答もあり(項番 1)、運用上の細目が追って示される可能性がある。

11 報告徴求・業務改善命令との関係

改正指針は、検査結果、犯罪発生報告書等により、保険会社のインターネット取引に係る健全かつ適切な業務の運

営に疑義が生じた場合には、必要に応じ、保険業法 128 条の規定に基づき追加の報告を求めるとし、さらに、犯罪防止策や被害発生後の対応について必要な検討がなされず、被害が多発するなどの事態が生じた場合など、契約者等の保護の観点から問題があると認められる場合には、同法 132 条に基づき業務改善命令を発出する等の対応を行うと明記している。

犯罪発生報告書が、法 128 条報告及び法 132 条命令への入口として明示的に位置付けられた点は、本改正の重要な特徴である。本監督指針は単なる推奨事項ではなく、検査・監督上の評価、報告徴求及び行政処分に直結する実務基準である。

事故発生後には、被害を補償したか否かにとどまらず、次の各点が問われることになる。

- 事前のリスク評価は適切であったか
- 改正指針を踏まえた対策計画が存在したか(「施行時点未完了＝直ちに不適切ではない」との整理は、計画の存在を前提とする。)
- 対策の導入が遅れた理由は合理的か
- 未実装期間中の代替措置(代替的な多要素認証、スケジュールの周知、検知機能の強化)を講じていたか
- 顧客への通知・被害抑制が迅速であったか
- 取締役会等が適切に監督していたか

12 保険会社における優先対応事項

第 1 顧客導線の棚卸し

メール・SMS に加え、RCS・LINE 等の公式アカウント、プッシュ通知を含む顧客向けアウトバウンド・チャネル全般について、記載しているすべての URL 及びログインリンクを洗い出し、用途、リンク先、遷移先での認証の有無、代替手段の有無、法令上の義務の有無を整理する。法令上の例外に依拠する場合には、根拠条項と代替不能性を文書化する。

第 2 重要な操作の定義

顧客情報・契約内容・保険金受取人・収納口座・支払先口座等への影響度及びなりすまし被害の拡大のおそれを踏まえ、フィッシングに耐性のある多要素認証を求める「重要な操作」を定義し、その判断過程を記録する。金融庁が具体例を示していない以上、定義の合理性の説明責任は各社にある。

第 3 多要素認証の実装計画

既存顧客を含む全登録顧客を対象とする導入計画、段階的導入の順序と完了時期、移行期間中の代替認証・スケジュールの顧客周知・検知機能の強化策を定め、取締役会等の承認を得る。

第 4 多層防御の実装

振る舞い検知、アカウント・ロックの自動発動、追加の本人認証、不審なアクセスの適時遮断・ブロック、顧客への通知及びログの保存を組み合わせる。通知は、リンクを付さず、公式アプリ・公式サイトでの確認を促す文面とする。

第 5 インシデント・当局報告フローの整備

「認識日の翌々営業日」「初回報告から 1 か月」という時限を前提に、認識日の特定、初回報告の判断者、提出責任者、更新・最終報告の期限管理、案件識別番号の採番ルールを規程化する。障害発生等報告及び個人情報漏えい等報告との報告要否の判定を統合したフローとする。

第 6 取締役会・委託先管理

進捗、残存リスク、不正被害件数、認証普及率、解除率及び解除理由、顧客周知状況等を取締役会等へ定期的に報告する。代理店・外部委託先にも同等の対応を求め、委託契約における責任分界、特に当局報告への協力を見直す。

13 おわりに

新旧対照表及びパブリックコメント回答を併せて読むと、本改正の本質は、従来の個別的な認証手段・不正防止策の例示から、顧客の行動変容、フィッシングに耐性のある認証、多層防御、経営管理、顧客救済及び当局報告を統合した「インターネット取引管理」へ移行したことにある。

特に重要なのは、金融庁が、**メール・SMS 内のログインリンクという従来一般的であった顧客導線そのものをフィッシングリスクの一部として捉え、利便性、技術的補完（送信ドメイン認証、二要素認証）、顧客からの依頼といった事情による例外を一切認めなかった**点である。「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」との回答（項番 20）は、この点に関する金融庁の姿勢を端的に示している。

同時に、犯罪発生報告書に多要素認証の導入状況欄が設けられ、当該報告が法 128 条・法 132 条への入口として明示されたことにより、改正対応の遅れが、事故発生時に制度的に可視化される構造が完成した。

リスクベース・アプローチが採用されている以上、求められるのは対応の画一性ではなく、**なぜその対象・方式・導入時期を選択したのかを、リスク評価と証拠に基づいて説明できること**である。裏を返せば、リスク評価も計画も存在しないまま従来の運用を継続することは、リスクベース・アプローチによって正当化されない。

14 理解度チェック（〇×問題 10 問）

本改正の理解度を確認するため、〇×問題を 10 問用意した。社内研修等にご活用いただきたい。まず【問題】に解答した上で、【解答・解説】をご確認いただきたい。

【問題】次の記述は正しいか（〇×）。

第 1 問 今回の改正により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、保険料の収納、保険金の支払、解約返戻金の請求など、顧客の資産の移転を伴う取引に限られる。

第 2 問 顧客からの電話による問合せに応じてマイページの URL を SMS で送付する運用や、送信ドメイン認証（DMARC・BIMI 等）を導入したメールにログインリンクを記載する運用は、フィッシングリスクが低いため、例外として許容される。

第 3 問 特定電子メール法に基づく受信拒否の通知先 URL をメール本文に記載することは「法令に基づく義務を履行するために必要な場合」に当たるが、当該 URL の遷移先がログインすることが可能な画面である場合には、なお記載すべきではないとされている。

第 4 問 RCS・LINE 等の企業公式アカウントからの送信であることが明白なコミュニケーションツールについては、URL を含む連絡は本改正の制限の対象とならない。

第 5 問 フィッシングに耐性のある多要素認証の必須化は、今後新たに登録する顧客を対象とすれば足り、既存の登録顧客は対象とならない。

第 6 問 顧客が、そのリスクを認識した上で自らの希望により多要素認証の設定解除を求める場合には、保険会社はこれに応じることが原則として適切である。

第 7 問 やむを得ず多要素認証の設定を解除する場合、保険会社は、解除率について具体的な数値目標を設定することが求められる。

第 8 問 改正指針の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完了していないことをもって、直ちに不適切と評価されるものではない。

第 9 問 改正指針にいう「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」の「取引時確認」は、犯罪収益移転防止法上の取引時確認を指すものである。

第 10 問 犯罪発生報告書による報告の対象は、不正アクセス・不正取引のうち、犯罪に該当することが確定したものに限られ、事案の概要が判明していない段階での報告は要しない。

【解答・解説】

問	解答	解説（根拠）
第 1 問	×	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となる（項番 8）。会員ページへのログインや契約内容の変更等を含め、横断的な棚卸しが必要である（本文 2）。
第 2 問	×	いずれも例外とされていない。顧客からの依頼に基づく受動的な URL 送付（項番 2）、送信ドメイン認証済みのメール（項番 24、28、53）、二要素認証実装ページへのリンク（項番 23）、注意喚起文言の併記（項番 21、22）のいずれについても、「原則として…記載すべきではない」との回答が維持された（本文 4(2)）。
第 3 問	〇	「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。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」とされている（項番 47。本文 4(3)）。
第 4 問	×	「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。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」とされている（項番 64）。棚卸しの対象はメール・SMS に限られない（本文 4(4)）。
第 5 問	×	「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

問	解答	解説（根拠）
		客のみならず、全ての登録顧客に対して求めるもの」とされている（項番 34。本文 5(2)）。
第 6 問	×	「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、…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」とされている（項番 33、35。本文 5(5)）。
第 7 問	×	「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」とされている（項番 36）。もっとも、端末非保有等の理由による解除であっても、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る（本文 5(5)）。
第 8 問	○	「ご認識の通りです」と回答されている（項番 54）。もっとも、改正後の監督指針は令和8年7月 17 日から適用されており、経過措置は設けられていない（項番 68）。可能な限り早期の対応が望まれ（項番 13、16、31、34、35、56）、未実装期間中は代替的な多要素認証の提供、スケジュールの顧客周知及び検知機能の強化が求められる。計画も進捗管理もないまま未実装である状態は正当化されない（本文 5(3)(4)）。
第 9 問	×	「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」とされている（項番 41。本文 9(1)）。
第 10 問	×	報告すべき対象は、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」である（項番 43）。また、記載要領上、事案の概要が判明していない場合でも、事案を認識した日の翌々営業日までに現状の報告を行う必要があり、発生要因・再発防止策等は調査中であっても差し支えない。さらに、状況の変化等が無い場合でも、初回報告から 1 か月以内に現状の報告を行う必要がある（本文 10(3)）。

主な参照資料

⑨　金融庁「保険会社向けの総合的な監督指針」の一部改正（新旧対照表）

⑩　金融庁「保険会社向けの総合的な監督指針（様式・参考資料編）」の一部改正（新旧対照表）――様式Ⅱ－3－1 3－2－2－3(1)　犯罪発生報告書（インターネット取引関連）及び記載要領

⑪　金融庁「「保険会社向けの総合的な監督指針」等の一部改正（案）に対するパブリックコメントの結果等の公表について」（令和8年7月 17 日）（https://www.fsa.go.jp/news/r8/sonota/20260717-2/20260717.html）――別紙1「コメントの概要及びコメントに対する金融庁の考え方」、別紙2・3（保険会社向け監督指針及び様式・参考資料編の新旧対照表）、別紙4～10（少額短期保険業者、貸金業者、金融サービス仲介業者、電子決済等代行業関係、前払式支払手段発行者、資金移動業者関係の新旧対照表）

⑫　金融情報システムセンター「金融機関等コンピュータシステムの安全対策基準・解説書」

⑬　フィッシング対策協議会「フィッシング対策ガイドライン」

なお、本ニュースレターは一般的な情報提供を目的とするものであり、個別の事案への対応については別途ご相談ください。改正指針の適用に当たっては、金融庁から示される様式の細目等の最新情報を適宜ご確認ください。

以上