弁護士法人三宅法律事務所

デジタル・ガバナンス／サイバーセキュリティ セミナー

保険会社向けの総合的な監督指針の改正

― インターネット取引の新設、フィッシングに耐性のある認証、
ログインリンクの見直し及び犯罪発生報告 ―

令和8年7月17日 公表・即日適用

※ 本資料は新旧対照表及びパブリックコメント回答（計76件）を踏まえた解説資料です。

AGENDA

本セミナーの構成 — 全6部

本改正は「インターネット取引」を独立の監督項目として新設し、認証・検知・顧客対応・当局報告を一つの管理サイクルとして規定するものです。パブリックコメント回答（計76件）を随所に織り込みながら解説します。

第1部　改正の全体像

削除された例示、新設項目の構造、対象範囲、リスクベースの射程

第2部　ログインリンクの原則禁止

最大の争点。業界要望とその帰結、個別ケースの深掘り

第3部　多要素認証と多層防御

全登録顧客への必須化、解除、要求頻度、多層防御、電決代行

第4部　経営管理・顧客対応・委託

取締役会・PDCA、被害補償、外部委託・代理店

第5部　犯罪発生報告書と行政対応

新様式、時系列管理、法128条・132条、他業態への波及

第6部　実務対応と誤解の整理

優先対応事項、ロードマップ、よくある誤解Q&A

BACKGROUND

改正の背景 — なぜ、いま改正されたのか

フィッシング被害の急増

ID・パスワードを窃取するフィッシング詐欺が高度化・巧妙化し、なりすましによる不正アクセス・不正取引の被害が拡大。

金融業界横断の対応

証券・銀行・貸金業・資金移動業・前払式支払手段発行者等でも同時に同趣旨の改正。業界全体で取り組むことが信頼性向上に資する（項番20）。

公表日から即日適用

令和8年7月17日に公表され、同日から適用。経過措置は設けられていない（項番68）。

パブリックコメントの概要

76件
一部改正に関係する意見の総数

R8.3.30〜4.30
パブリックコメント実施期間

R8.7.17
結果公表・改正指針の適用開始

出典（パブコメ回答）：https://www.fsa.go.jp/news/r8/sonota/20260717-2/20260717.html

01

PART 1

改正の全体像

削除された例示、新設項目の構造、対象範囲、そしてリスクベース・アプローチの射程と限界。

THE SHIFT

改正の本質 — 技術管理から経営管理へ

従来

- 認証方式・不正防止策を個別に例示
- 固定式ID・パスワードに頼らない認証
- 不正なログイン・異常な取引等の検知
- 主としてシステム部門の技術的対策
- 個別的な不正防止策の列挙

改正後

- インターネット取引全体の管理態勢を新設
- 重要な操作時のフィッシング耐性のある多要素認証の実装・必須化
- 振る舞い検知、追加認証、適時遮断、顧客通知、ログ保存
- 取締役会等の関与・全社態勢・PDCA・顧客対応・当局報告
- リスクベースの多層防御と継続的な見直し

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。

CAUTION

見落とされやすい「削除」

従来のシステムリスク管理態勢（旧Ⅱ－３－１３－２－２(5)②③）の例示は、いずれも削除された。

削除された主な例示

- 固定式ID・パスワードのみに頼らない認証方式（可変式パスワード・電子証明書等）
- 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提供、ウィルス感染検知・警告ソフトの導入
- 電子証明書をICカード等の別媒体・機器へ格納する方式

特に重要 ― セーフハーバー的（注）の削除

「出金先口座について顧客と名義が異なる指定・変更を認めず、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（注）が削除された。

→ 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。

STRUCTURE

新設項目の構造 ― Ⅱ－３－１３－２－２

条項	項目	主な内容
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／取締役会等の検討／全社態勢／金融ISAC・JPCERT／CC／PDCA
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
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／迅速な連絡／普及モニタリング／被害補償
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条命令
様式・参考資料編	**犯罪発生報告書**	様式Ⅱ－３－１３－２－２－３(1)（インターネット取引関連）を新設

SCOPE

対象範囲 — 資産移転取引に限られない

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）。

各社が該当性を検討すべき操作（候補）

- 顧客専用ページへのログイン
- 新規加入・契約更新
- 住所・電話番号・メールアドレスの変更
- 補償内容・契約内容の変更
- 保険金・給付金請求
- 解約・返戻金請求
- 保険金受取人・支払先口座の変更

金融庁の回答姿勢

- 「重要な操作」の具体例は示されていない（項番10・11・30）
- 各社が顧客層・取扱商品・取扱額等に応じてリスク評価を行い、対象を定義する
- 列挙した操作は「金融庁が該当と回答したもの」ではなく、あくまで検討候補
- **インターネットバンキング相当機能に限らず、契約上の権利関係に重大な影響を与える操作を横断的に棚卸し**

RISK-BASED

リスクベース・アプローチの射程と限界

各社の裁量が認められる領域

- 画一的対応は求められない（項番7）
- 例示された対策の全網羅は不要。リスク評価に基づき選択的に実施すれば足りる（項番57）
- 列挙事項と異なる独自手法で十分な対策を講じていれば趣旨を満たす（項番58）
- 独自対策への重点配分も尊重（ただし列挙項目以外も速やかに実施が望ましい／項番59）

原則的な最低線（見送りは不可）

- パスワード入力を促すURL・ログインリンクの不記載
- 重要な操作時のフィッシング耐性のある多要素認証の実装・必須化
- 未実装期間中の代替的多要素認証／スケジュール周知／検知機能の強化
- 不正ログイン・異常取引の検知、顧客通知及びログ保存

裁量が認められるのは「方向性を採るか否か」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。

02

PART 2 | 最大の争点

メール・SMSの
ログインリンクの原則禁止

顧客に「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る。

LOGIN LINKS

フィッシング詐欺対策の原則

原則：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

あわせて求められる対策

正規サイトの
ブックマーク・
正規アプリからの
ログインを促す

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

唯一の明示的例外：メール配信の解除手続きなど、法令に基づき電子メール本文への記載が義務付けられている場合など（＝代替的手段を採り得ない場合）に限られる。

PUBLIC COMMENT

業界からの例外要望は、ほぼ全て斥けられた

回答はいずれも「原則として…記載すべきではない」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	項番	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・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（直接遷移しない）	項番4	例外とせず
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）実施済みメール	項番24・28・53	例外とせず
注意喚起のガード文言を併記する運用	項番21・22	例外とせず
満期・継続手続案内、カード決済エラー案内（無保険回避）	項番38・39	例外とせず
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
ダイレクト販売モデル上の必要性／即時出金がなくリスク低	項番17	例外とせず

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・資産性の低さは、いずれも単独では例外事由とならない。

PUBLIC COMMENT

射程はメール・SMSに限られない

法令例外でも「遷移先」を問う（項番47）

特定電子メール法に基づく受信拒否の通知先URLは例外として認めつつ、「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。法令例外でも遷移先がログイン可能画面となる設計は避ける。

公式アカウントも同様（項番64）

RCS・LINE等の企業公式アカウントからの送信も、「URLやログインリンクの送付は極力控え、代替的手段の導入を検討することが望ましい。ログイン可能画面へ遷移するURLも記載すべきでない」。棚卸し対象はアウトバウンド・チャネル全般。

検知通知メールとの整合（項番27）

「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」といった記載の許容範囲を問う意見に対し、回答は「よくご検討ください」にとどまった。

実務上は、通知にリンクを付さず、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、通知文面の定型化と事前周知を併せて行う。

CASE STUDY

ケース深掘り — ダイレクト型・満期案内

「即時出金がなくリスクが低い」「無保険状態を招く」という強い反論も、例外として認められなかった。

業界の主張（項番17・38・39）

- ダイレクト型は徹底したコスト削減を低廉な保険料として還元するモデル。リンクを送れないと手続を断念
- 保険は即時出金ができず審査も介在。フィッシングの主目的（即時の金銭奪取）のリスクは低い
- 満期・継続手続の案内メールにURLを載せられないと、無保険状態を招き被害者救済が困難に
- カード決済エラー・有効期限切れ時の支払手続案内も同様

金融庁の結論

- 法令上の記載義務がある場合などを除き、原則としてURL・ログインリンクを記載すべきでない
- 資産性の低さ・ビジネスモデルへの影響は、例外を基礎づけない
- 公式ホームページのトップページURLの掲載も、原則として認められない
- **システム開発等に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**

CASE STUDY

「技術で担保できる」という主張の帰結

ディープリンク・中間ページ・パーソナライズ表示・ドメイン認証等を挙げてURL記載を認めるべきとの意見（項番52・26・28・53）も斥けられた。

ディープリンクで公式アプリを直接起動

ブラウザ上の偽サイト誘導を物理的に排除できると主張

中間ページ（スピードバンプ）を設置

「ここから先はログインが必要」と警告し能動的確認を促す

遷移先にパーソナライズ情報を表示

本人しか知り得ない情報でトラストシグナルを提示

送信ドメイン認証（SPF/DKIM/DMARC）

なりすましメールを技術的に排除できると主張

結論：いずれも「原則として…記載すべきではない」との回答が維持された。技術的補完は、URL記載を正当化する事由とはされていない。

ACTION

実務上の棚卸し — 導線の区分と対応

ログイン画面への直接リンク	原則廃止し、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。説明画面経由でも例外とならない
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
法令上リンク記載が必要なもの	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
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

03

PART 3

多要素認証と多層防御

全登録顧客への必須化、解除の可否、要求頻度、そして「認証だけでは足りない」多層防御。

MFA

フィッシングに耐性のある多要素認証

重要な操作時

ログイン・出金・出金先口座の指定変更等に実装及び必須化（デフォルト設定）

全登録顧客が対象

新規登録顧客のみならず、既存の全登録顧客に求める（項番34）

パスキーに限定せず

PKIベース認証や回線認証等、耐性を合理的に説明できる方式も可（項番72）

移行期間中の代替措置（注２）— ID・パスワードの継続だけでは足りない

- 代替的な多要素認証の提供
- 実装・必須化に向けた具体的スケジュールの顧客周知（概算での足切りは不可／項番55）
- 振る舞い検知・ログイン通知等の検知機能の強化

PUBLIC COMMENT

顧客要望による解除 — 同意しても正当化されない

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、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（項番33・35）。

やむを得ず解除する場合（注１）

- 代替的な多要素認証を提供する
- 解除率の状況をフォローする
- 認証技術・規格の発展も勘案し、解除率が低くなるよう認証方法の見直しを検討・実施

ただし数値目標までは不要（項番36）

- 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い
- 各社が顧客・取扱商品・業務特性に応じてリスク評価を行い、適切な対策を講じる
- **管理指標としては、解除率に加え、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**

DEFENSE IN DEPTH

認証だけでは足りない — 多層防御

予防 ▶ 検知 ▶ 追加認証・遮断 ▶ 顧客通知 ▶ ログ事後検証

改正指針が列挙する不正防止策

- 不正なログイン・取引・出金・保険金受取人の変更等の顧客通知
- 認証連続失敗時のアカウント・ロックの自動発動（実装・必須化）
- ログイン時の振る舞い検知＋ログイン・取引情報の保存
- 追加の本人認証／不審アクセスの適時遮断／不正アクセス元のブロック
- 検知後、速やかに利用者へ連絡する体制と仕組み
- 他の銀行口座との連携サービス提供時の多要素認証

要求頻度に一律の最低基準はない（項番32）。保有情報の質・量、露出、顧客属性等を踏まえ、設定頻度の合理性を説明できる根拠資料を整備。

FREQUENCY & TIMELINE

要求頻度・移行スケジュールの考え方

多要素認証の要求頻度（項番32）

- 「都度要求すべきか」「最低1日1回か」といった一律の最低基準は示されていない
- 各社が、保有情報の質・量、インターネットへの露出、顧客属性、商品・業務特性を総合評価
- セッション継続中のみ／一定期間有効等の設計も、リスク評価に基づく合理的な範囲で許容され得る
- **設定した頻度の合理性を説明できる根拠資料の整備が不可欠**

実装スケジュールの周知（注2・項番55）

- 施行時点で未完了でも直ちに不適切とはされない（項番54）
- ただし可能な限り早期の対応が望まれ、計画と進捗の合理性が問われる
- 「〇年度中を目指す」といった概算・暫定目標での足切りは是認されていない
- **顧客の安心のため、スケジュールはできる限り明らかにすることが重要**

API & AGGREGATION

電子決済等代行業者との連携という論点

口座情報の一覧化サービス等では、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、スクレイピング方式による連携が困難になるとの意見（項番76）。

参照系（読取のみ）

まずは参照系と更新系を分別し、当面の連携を確保すべきとの提案

更新系（取引・出金・変更）

重要な操作に対してのみ、先行してフィッシング耐性のある認証を導入

中長期はAPI整備へ

金融機関がAPIを整備し、参照系連携でも耐性のある認証へ移行する計画的アプローチ

金融庁の回答：段階的導入が理解される場合はあるが、目下の状況を踏まえ、可能な限り早期の対応が望まれる（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。

04

PART 4

経営管理・顧客対応・外部委託

取締役会等の関与とPDCA、被害発生後の顧客対応・補償、そして委託先・代理店の管理。

GOVERNANCE

内部管理態勢・取締役会等・PDCA

不正アクセス・不正取引対策を「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。

取締役会等に期待される役割

- 重要なサービス・操作の特定／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

「取締役会等」は会議体に限定されず、各社のガバナンス態勢に応じた体制で足りる（項番71）。

文書化すべき管理プロセス（PDCA）

1. 対象サービス・操作の棚卸し
2. 不正手口・脅威情報の収集（金融ISAC・JPCERT/CC）
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・解除率のモニタリング
7. 対策の見直し／取締役会等への報告

PDCAの具体的モデルは「各社の状況が異なるため一概に示すことは難しい」（項番12・19）。

CUSTOMER & OUTSOURCING

顧客対応・被害補償／外部委託・代理店

顧客対応・被害補償

- リスク説明・セキュリティ対策事例の周知を含む注意喚起
- 顧客が取引内容を適時に確認できる手段
- 届出の速やかな受付／容易に理解できる形での周知
- 被害のおそれがある顧客への迅速な連絡による被害抑制
- 普及状況の定期モニタリング＋追加施策（普及率だけでは免責されない）
- 被害補償を含む真摯な被害回復対応
- 記録の適切な保存／顧客・捜査当局への誠実な協力

外部委託・代理店・少短・仲立人

- 取引時確認は犯収法に限らず「取引の際のあらゆる確認」（項番41）
- 管理態勢は保険代理店等も対象（規模・業務特性を踏まえる／項番9）
- 委託先にも同様の不正防止策を講じさせる（項番70）
- 点検対象：代理店の募集システム、委託CC、SaaSポータル、認証サービス、配信・監視事業者等
- **委託契約で責任分界を明確化（認証方式・リンク送信ルール・ログ・通知・当局報告への協力）**
- 少額短期保険業者・保険仲立人も規模・特性に応じ準じた対応

05

PART 5 | 新様式の新設

犯罪発生報告書と行政対応

改正対応の状況が、事故報告の一部として制度的に可視化される構造が完成した。

CRIME REPORT

報告義務と様式の記載事項

報告対象：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（項番43）。確定を待たず、認識次第、速やかに報告。想定される不正取引＝保険契約者へのなりすましによる保険金の不正受給（項番42）。

(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)	**多要素認証の導入状況 ★**	ログイン時／出金・出金先口座変更時／保険受取人変更時／その他の操作時。必須化（デフォルト設定）の状況がわかるように記載
(3)	**事案の形態・概要**	不正アクセスのみ発生／不正取引の発生
(4)(5)	**被害件数・被害金額**	
(6)	**発生要因**	不正アクセス又は不正取引の発生要因
(7)	**再発防止策**	
(8)	**被害者対応・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)欄が決定的に重要：未導入の場合、その理由・代替措置・導入計画の説明が当然に想定される。

TIMELINE

報告の時系列管理 — 「翌々営業日」が要諦

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。平時からの規程化が必要。

初回報告

事案の概要が判明した時点で報告（発生要因・再発防止策は調査中でも可）。概要不明でも、認識した日の翌々営業日までに現状報告。

▼

更新報告

状況変化があれば都度更新。変化が無くても、初回報告から1か月以内に現状報告。

▼

最終報告

「処理・補償の進捗状況」が「補償事由の発生なし」又は「完結」となった時点で最終報告。

案件単位：発覚から「完結」までを一つの案件として案件識別番号を付す（形式は任意）。最終報告以降、同様の事案が生じた場合は別事案として初回報告。

ENFORCEMENT

報告徴求・業務改善命令との関係

犯罪発生報告書

インターネット取引の不正アクセス・不正取引を認識次第

▶

法128条 追加報告

検査結果・報告書等により業務運営に疑義が生じた場合

▶

法132条 業務改善命令

必要な検討がなされず被害が多発する等、契約者保護上問題がある場合

三系統の並行管理（項番67：共通様式化は「参考意見」にとどまる）

① 犯罪発生報告書

様式Ⅱ－３－１３－２－２－３(1)

② 障害発生等報告書

様式Ⅱ－３－１４(1)

③ 個人情報の漏えい等報告

個人情報保護委員会宛て

なりすまし事案では同時にトリガーされ得る。報告要否判定を一枚のフローに統合しておくことが有用。

FORM IMAGE

犯罪発生報告書の様式イメージ

金融庁長官宛て。案件識別番号で管理し、初回・更新・最終の別を記載する。

宛先	金融庁長官　殿 *金融機関名／代表者名／担当者情報（所属・氏名・電話・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) 多要素認証の導入状況 ★	ログイン時／出金・出金先口座変更時／保険受取人変更時／その他の操作時 *※必須化（デフォルト設定）の状況がわかるように記載*
(3) 事案の形態・概要	□不正アクセスのみ発生　□不正取引の発生
(4)(5) 被害件数・被害金額	
(6) 発生要因　／　(7) 再発防止策	
(8) 被害者対応・補償方針	□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	

★ 多要素認証の導入状況欄により、改正対応の状況が事故報告の一部として当局に開示される。

CROSS-INDUSTRY

他業態への波及 — 同日に横並びで改正

本改正は保険会社に限られない。パブコメ回答には各業態向けの回答が含まれ、同一文言の解釈の手がかりとなる。

少額短期保険業者

主な着眼点は総合指針に準じるが、規模・業務特性に応じた態勢整備で足りる（項番44）

貸金業者

「重要な操作」の範囲は各社が判断（項番45）。督促SMS等も対象（項番65）。借入上限設定機能の提供（項番50）

資金移動業者

「取締役会等」は会議体に限定されない（項番71）。回線認証等、耐性を説明できれば可（項番72）

前払式支払手段発行者

委託先（収納代行等）にも同様の不正防止策を講じさせる（項番70）

電子決済等代行業者

参照系・更新系の分別と段階導入の提案。中長期はAPI整備へ（項番76）

保険仲立人

規模・業務特性を踏まえ、保険会社の取扱いを参考に適切な措置（Ⅴ－５－７）

06

PART 6

実務対応と誤解の整理

優先対応事項、対応ロードマップ、そして現場で生じやすい誤解の整理。

ACTION PLAN

保険会社における優先対応事項

第1　顧客導線の棚卸し

全アウトバウンド・チャネル（メール・SMS・RCS・LINE・プッシュ通知）のURL・リンクを洗い出し、用途・遷移先・認証有無・代替手段・法令義務を整理

第2　重要な操作の定義

影響度・なりすまし被害の拡大可能性を踏まえて定義し、判断過程を記録（定義の合理性の説明責任は各社）

第3　多要素認証の実装計画

既存を含む全登録顧客を対象とする導入計画・段階順序・完了時期・移行期間中の代替認証を定め、取締役会等の承認を取得

第4　多層防御の実装

振る舞い検知・自動ロック・追加認証・適時遮断・顧客通知・ログ保存を組み合わせ。通知は公式アプリ・公式サイトでの確認を促す文面に

第5　インシデント・当局報告フロー

「翌々営業日／1か月」を前提に、認識日特定・判断者・提出責任者・期限管理・採番を規程化。三系統の報告要否判定を統合

第6　取締役会・委託先管理

進捗・残存リスク・被害件数・普及率・解除率・周知状況を定期報告。代理店・委託先にも同等対応を求め、責任分界を見直す

ROADMAP

対応ロードマップ ― 3つのフェーズ

既に適用済みである以上、「棚卸し・応急対応」から着手し、恒久対応へ移行する。

フェーズ1
即時（～数か月）

- 導線の棚卸し（メール・SMS・公式アカウント）
- ログイン画面への直接リンクの停止
- 検知通知の文面見直し（リンク不記載）
- インシデント・当局報告フローの規程化

フェーズ2
短期（～1年）

- 重要な操作の定義とリスク評価の文書化
- 多要素認証の実装計画・スケジュール周知
- 移行期間中の代替認証・検知機能の強化
- 委託先・代理店の契約・責任分界の点検

フェーズ3
恒久（継続）

- 全登録顧客への多要素認証の必須化
- 多層防御の実装と有効性検証
- 普及率・解除率のモニタリング
- 取締役会等への定期報告とPDCA

FAQ

よくある誤解の整理

誤解 ドメイン認証や二要素認証済みページなら、リンクを載せてよい	**正** 単独では例外事由とならない。原則として記載すべきでない（項番23・24・28・53）
誤解 資産移転を伴わない会員サイトのログインは対象外	**正** 対象となり得る。リスクの高い顧客情報・契約情報を含むログインも対象（項番8）
誤解 多要素認証の必須化は新規顧客から順次でよい	**正** 既存を含む全登録顧客が対象（項番34）
誤解 顧客が希望すれば多要素認証を解除してよい	**正** 顧客が同意しても原則は必須化。解除時も代替認証と解除率のフォローが必要（項番33・35）
誤解 施行時点で未実装なら直ちに不適切	**正** 直ちに不適切ではない（項番54）。ただし計画・進捗・代替措置の合理性が問われる
誤解 犯罪発生報告は原因が判明してから提出すればよい	**正** 認識日の翌々営業日までに現状報告。調査中でも差し支えない

まとめ

求められるのは「画一性」ではなく「説明可能性」

- 本改正は、個別の認証手段の例示から、顧客の行動変容・多層防御・経営管理・顧客救済・当局報告を統合した「インターネット取引管理」への移行。
- メール・SMSのログインリンクという従来の導線そのものをリスクと捉え、利便性・技術的補完・顧客の依頼による例外を一切認めなかった。
- 犯罪発生報告書に多要素認証の導入状況欄が設けられ、報告が法128条・132条の入口として明示。改正対応の遅れが事故発生時に制度的に可視化される。
- リスクベースである以上、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が重要。

※ 既に適用済み。「これから準備する」ではなく「未対応部分の計画と代替措置を示せるか」が問われる局面。

弁護士法人三宅法律事務所

Miyake & Partners

本セミナー・ニュースレターに関するお問い合わせ

執筆・講演　　弁護士　渡邉 雅之

TEL　03-5288-1021　／　FAX　03-5288-1025

Email　m-watanabe@miyake.gr.jp

本資料は一般的な情報提供を目的とするものであり、個別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。

出典：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日公表・即日適用）。新旧対照表（本編・様式／参考資料編）及び別紙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」を含む。

https://www.fsa.go.jp/news/r8/sonota/20260717-2/20260717.html　（本文中の「項番」は同ページ別紙１の項番を指す）