系統金融機関向けの総合的な監督指針　新旧対照表

改　正　後	現　　行
【本編】 **Ⅱ　系統金融機関監督上の評価項目** **Ⅱ－３　業務の適切性** **Ⅱ－３－５　インターネットバンキング** **Ⅱ－３－５－２　主な着眼点【共通】** (1)　(略) (2) セキュリティの確保 ①・②　(略) ③　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。）、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促進等、業務に応じた適切な不正防止策を講じているか。 （注）情報の収集に当たっては、金融関係団体や公益財団法人金融情報システムセンターの調査等のほか、情報セキュリティに関する検討会や金融機関防犯連絡協議会における検討結果、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。	【本編】 **Ⅱ　系統金融機関監督上の評価項目** **Ⅱ－３　業務の適切性** **Ⅱ－３－５　インターネットバンキング** **Ⅱ－３－５－２　主な着眼点【共通】** (1)　(略) (2) セキュリティの確保 ①・②　(略) ③　ウェブページのリンクに関し、利用者が取引相手を誤認するような構成になっていないか。 また、フィッシング詐欺対策については、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等、業務に応じた適切な不正防止策を講じているか。 （注）情報の収集に当たっては、金融関係団体や公益財団法人金融情報システムセンターの調査等のほか、情報セキュリティに関する検討会や金融機関防犯連絡協議会における検討結果、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。

系統金融機関向けの総合的な監督指針　新旧対照表

改　正　後	現　　行
④　業務内容に応じて、以下の不正防止策を講じているか。また、内外の環境変化や事故・事件の発生状況を踏まえ、定期的かつ適時にリスクを認識・評価し、必要に応じて、認証方式等の見直しを行っているか。 ・ログイン、出金など、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） （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、利用者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、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の認証の方法の見直しを検討・実施することとする。 （注２）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利用者に周知するとともに、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。 ・利用者が身に覚えのない第三者による不正なログイン・取引を早期に検知するため、電子メール等により、利用者に	（新設）

系統金融機関向けの総合的な監督指針　新旧対照表

改　正　後	現　　行
通知を送信する機能の提供 ・認証に連続して失敗した場合、ログインを停止するアカウント・ロックの自動発動機能の実装及び必須化 ・利用者のログイン時の挙動の分析による不正アクセスの検知（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の実施 ・不正アクセスの評価に応じて追加の本人認証を実施するほか、当該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等の対応の実施 ・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	
(3) 利用者対応 ① 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（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。）、被害拡大の可能性（対策として、振込限度額の設定等）等、様々なリスクの説明や、利用者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等が利用者に対して十分に行われる態勢が整備されているか。 ②～⑥　（略）	(3) 利用者対応 ① 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、被害拡大の可能性（対策として、振込限度額の設定等）等、様々なリスクの説明や、利用者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等が利用者に対して十分に行われる態勢が整備されているか。 ②～⑥　（略）
(4)　（略）	(4)　（略）

系統金融機関向けの総合的な監督指針　新旧対照表

改　正　後	現　　行
（参考） ・セキュリティ対策向上・強化等に関する一般社団法人全国銀行協会の「申し合わせ」（24 年 1 月、25 年 11 月、26 年 5 月、26 年 7 月等） ・インターネット・バンキングにおいて留意すべき事項について（一般社団法人全国銀行協会） ・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（公益財団法人金融情報システムセンター編） ・情報セキュリティに関する検討会における検討資料 ・預貯金等の不正な払戻しへの対応について（平成 20　年 9 月 1 日：JA バンク） ・法人向けインターネット・バンキングにおける預金等の不正な払戻しに関する補償の考え方（平成 26 年 7 月 17 日：一般社団法人全国銀行協会） ・フィッシング対策ガイドライン（フィッシング対策協議会）	（参考） ・セキュリティ対策向上・強化等に関する一般社団法人全国銀行協会の「申し合わせ」（24 年 1 月、25 年 11 月、26 年 5 月、26 年 7 月等） ・インターネット・バンキングにおいて留意すべき事項について（一般社団法人全国銀行協会） ・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（公益財団法人金融情報システムセンター編） ・情報セキュリティに関する検討会における検討資料 ・預貯金等の不正な払戻しへの対応について（平成 20　年 9 月 1 日：JA バンク） ・法人向けインターネット・バンキングにおける預金等の不正な払戻しに関する補償の考え方（平成 26 年 7 月 17 日：一般社団法人全国銀行協会） （新設）
Ⅱ－３－６　外部の決済サービス事業者等との連携【共通】 **Ⅱ－３－６－２　主な着眼点** （１）（略） （２）セキュリティの確保 ①・②　（略） ③　預貯金口座との連携を行う際に、サービスの内容に応じ	**Ⅱ－３－６　外部の決済サービス事業者等との連携【共通】** **Ⅱ－３－６－２　主な着眼点** （１）（略） （２）セキュリティの確保 ①・②　（略） ③　預貯金口座との連携を行う際に、固定式の ID・パスワー

系統金融機関向けの総合的な監督指針　新旧対照表

改　正　後	現　　行
てⅡ－３－５－２（２）に記載している対策（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）により預貯金者へのなりすましを阻止しているか。	ドによる本人認証に加えて、ハードウェアトークン・ソフトウェアトークンによる可変式パスワードを用いる方法や公的個人認証を用いる方法などで本人認証を実施するなど、実効的な要素を組み合わせた多要素認証等の導入により預貯金者へのなりすましを阻止する対策を導入しているか。
（注）（略） ④～⑨　（略）	（注）（略） ④～⑨　（略）
(参考) （略）	(参考) （略）
（３）（略）	（３）（略）

附　則

この通知の改正は、令和８年２月 27 日から適用する。