令和6年10月更新

資金移動業のしおり＜第７版＞　【正誤表】

資金移動業のしおりをご購入いただき、誠にありがとうございます。
本書で扱う法令及びガイドラインにつきまして、以下の通り一部改正が行われました。

改正対象	改正の主な内容等	施行・適用日
事務ガイドライン第三分冊金融会社関係 14 資金移動業関係	「金融分野におけるサイバーセキュリティに関するガイドライン」が別途制定されたことに伴い、事務ガイドライン内の重複する内容を削除する改正	令和6年10月４日

これにより、本書の内容にも影響がございましたので、以下の表の通り、本文を読み替えてご利用ください。
また、本書の一部に、編集時の誤りがございました。お詫びして訂正いたします。誤りも改正と併せて以下の表に記載しております。

【解説編】

ページ	訂正個所	訂正後	訂正前
115	Ⅵ 雑則 ２ 廃止の届出等 (1) 財務(支)局等への届出等 ポイント	ポイント　**電子公告の方法により公告を行う場合** 資金移動業の廃止の公告を電子公告の方法により行う場合、資金移動業者は、ホームページにおいて、廃止日まで継続して公告を掲載しなければなりません(資金決済法第61条第6項、政令第19条の2、会社法第940条第1項第1号)。 また、**資金移動業者が**資金移動業の廃止の公告を電子公告の方法により行う場合は、法務大臣の登録を受けた電子公告調査機関に調査を委託し、公告期間中、当該公告の内容である情報が不特定多数の者が提供を受けることができる状態に置かれているかどうかについて、調査を受けることが義務付けられています**(会社法第941条(外国資金移動業者である資金移動業者については資金決済法第61条第7項により準用))**。具体的には、①あらかじめ提出された公告情報と実際のホームページに掲載された電子公告の情報が一致しているか、②公告アドレスまでのリンクが途切れておらず、無償かつパスワード等が不要でアク	ポイント　**電子公告の方法により公告を行う場合** 資金移動業の廃止の公告を電子公告の方法により行う場合、資金移動業者は、ホームページにおいて、廃止日まで継続して公告を掲載しなければなりません(資金決済法第61条第6項、政令第19条の2、会社法第940条第1項第1号)。 また、**外国資金移動業者である資金移動業者が**資金移動業の廃止の公告を電子公告の方法により行う場合は、法務大臣の登録を受けた電子公告調査機関に調査を委託し、公告期間中、当該公告の内容である情報が不特定多数の者が提供を受けることができる状態に置かれているかどうかについて、調査を受けることが義務付けられています**(資金決済法第61条第7項、会社法第941条)**。具体的には、①あらかじめ提出された公告情報と実際のホームページに掲載された電子公告の情報が一致しているか、②公告アドレスまでのリンクが途切れておらず、無償かつパスワード等が不要でアクセスできるか、③公告掲載期間中、公

資金移動業のしおり＜第7版＞ 【正誤表】

令和6年10月更新

ページ	訂正個所	訂正後	訂正前
		セスできるか、③公告掲載期間中、公告を調査できる状態が継続しているか、また公告が改ざんされていないかなどが調査の対象となります。電子公告調査機関は、電子公告調査の終了後速やかに、調査結果を電子公告を委託した会社等に対し通知しなければならないこととされています。 なお、登録された電子公告調査機関は5社となっています（法務省HP参照）。	告を調査できる状態が継続しているか、また公告が改ざんされていないかなどが調査の対象となります。電子公告調査機関は、電子公告調査の終了後速やかに、調査結果を電子公告を委託した会社等に対し通知しなければならないこととされています。 なお、登録された電子公告調査機関は5社となっています（法務省HP参照）。

【資料編】

ページ	変更個所	変更後	変更前
268	Ⅱ－2－3－1	**Ⅱ－2－3－1 システムリスク管理** （中略） なお、以下の各着眼点に記述されている字義どおりの対応が資金移動業者においてなされていない場合にあっても、当該資金移動業者の規模、資金移動業務におけるコンピュータシステムの占める役割などの特性からみて、利用者保護の観点から、特段の問題がないと認められれば、不適切とするものではない。 （参考）金融機関の IT ガバナンスに関する対話のための論点・プラクティスの整理**第2版**（令和**5**年6月）	**Ⅱ－2－3－1 システムリスク管理** （中略） なお、以下の各着眼点に記述されている字義どおりの対応が資金移動業者においてなされていない場合にあっても、当該資金移動業者の規模、資金移動業務におけるコンピュータシステムの占める役割などの特性からみて、利用者保護の観点から、特段の問題がないと認められれば、不適切とするものではない。 （参考）金融機関の IT ガバナンスに関する対話のための論点・プラクティスの整理（令和**元**年6月）
270	Ⅱ－2－3－1－1 主な着眼点	**Ⅱ－2－3－1－1 主な着眼点** (1) ～ (4) （略） (5) サイバーセキュリティ管理 **① 取締役会等は、サイバーセキュリティの重要性を認識し、「金融分野におけるサイバーセキュリティに関するガイドライン」を踏まえ、必要な態勢を整備しているか。** **（削除）**	(1) ～ (4) （略） (5) サイバーセキュリティ管理 **① サイバーセキュリティについて、取締役会等は、サイバー攻撃が高度化・巧妙化していることを踏まえ、サイバーセキュリティの重要性を認識し必要な態勢を整備しているか。** **② サイバーセキュリティについて、組織体制の整備、社内規程の策定のほか、以下のようなサイバーセキュリティ管理態勢の整備を図っているか。** **・サイバー攻撃に対する監視体制**

令和6年10月更新

ページ	変更個所	変更後	変更前
271		②（略） （削除） ③（略）	・サイバー攻撃を受けた際の報告及び広報体制 ・組織内 CSIRT（Computer Security Incident Response Team）等の緊急時対応及び早期警戒のための体制 ・情報共有機関等を通じた情報収集・共有体制 等 ③ サイバー攻撃に備え、入口対策、内部対策、出口対策といった多段階のサイバーセキュリティ対策を組み合わせた多層防御を講じているか。 ・入口対策（例えば、ファイアウォール、WAF の設置、抗ウィルスソフトの導入、不正侵入検知システム・不正侵入防止システムの導入等） ・内部対策（例えば、特権 ID・パスワードの適切な管理、不要な ID の削除、特定コマンドの実行監視、本番システム（サーバー間）のセキュア化（パケットフィルタや通信の暗号化）、開発環境（テスト環境を含む。）と本番システム環境のネットワークの分離、利用目的に応じたネットワークセグメント分離等） ・出口対策（例えば、通信ログ・イベントログ等の取得と分析、不適切な通信の検知・遮断等） ④ サイバー攻撃を受けた場合に被害の拡大を防止するために、以下のような措置を講じているか。 ・攻撃元の IP アドレスの特定と遮断 ・DDoS 攻撃に対して自動的にアクセスを分散させる機能 ・システムの全部又は一部の一時的停止 等 ⑤ システムの脆弱性について、OS の最新化やセキュリティパッチの適用など必要な対策を適時に講じているか。 ⑥ サイバーセキュリティについて、ネットワークへの侵入検査や脆弱性診断等を活用するなど、セキュリティ水準の定期的な評価を実施し、セキュリティ対策の向上を図っているか。 また、国内外でサイバーセキュリティ侵害事案が発生した場合には、適宜リスク評価を行うなど自社への影響を検討しているか。 ⑦ インターネット等の通信手段を利用した非対面の取引

令和6年10月更新

ページ	変更個所	**変更後**	変更前
			を行う場合には、例えば、以下のような取引のリスクに見合った適切な認証方式を導入しているか。 　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、認証方式の見直しを行っているか。 ・可変式パスワード、生体認証、電子証明書等実効的な要素を組み合わせた多要素認証などの、固定式のID・パスワードのみに頼らない認証方式 ・取引に利用しているパソコン・スマートデバイス等とは別の機器を用いるなど、複数経路による取引認証 ・ログインパスワードとは別の取引用パスワードの採用（同一のパスワードの設定を不可とすること等の事項に留意すること。） ・特定の端末のみを利用可能とする端末認証 等 （注）電話番号、メールアドレス、パスワードなど認証に利用され る情報の登録・変更に堅牢な認証方式が導入されている必要 がある点に留意する
		④（略）	⑧ インターネット等の通信手段を利用した非対面の取引を行う場合には、例えば、以下のような業務に応じた不正防止策を講じているか。 ・不正な IP アドレスからの通信の遮断 ・利用者に対してウィルス等の検知・駆除が行えるセキュリティ対策ソフトの導入・最新化を促す措置 ・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の整備 ・不正が確認された ID の利用停止 ・前回ログイン（ログオフ）日時の画面への表示 ・取引時の利用者への通知 等
		（削除）	**⑨ サイバー攻撃を想定したコンティンジェンシープランを策定し、訓練や見直しを実施しているか。また、必要に応じて、業界横断的な演習に参加しているか。** **⑩ サイバーセキュリティに係る人材について、育成、拡充するための計画を策定し、実施しているか。**

資金移動業のしおり＜第7版＞【正誤表】

令和6年10月更新

ページ	変更個所	変更後	変更前
326	資金移動業者登録審査事務チェックリスト（資金移動業を適切かつ確実に遂行する体制・この章の規定を順守するために必要な体制）	システムリスク管理に関する社内規則等（ガイドラインⅡ－2－3－1－1） （略） □ サイバーセキュリティの重要性を認識し、「金融分野におけるサイバーセキュリティに関するガイドライン」を踏まえ、必要な態勢を整備しているか。 （削除）	システムリスク管理に関する社内規則等（ガイドラインⅡ－2－3－1－1） （略） □ サイバーセキュリティについて重要性を認識した上で、組織体制の整備や社内規程の策定等、必要な態勢を整備しているか。 □ サイバー攻撃に備え、入口・内部・出口といった多段階のサイバーセキュリティ対策を組み合わせた多層防御を講じているか。 □ サイバー攻撃を受けた場合に被害の拡大を防止するための措置を講じているか。
		□ システムの脆弱性について、OSの最新化やセキュリティパッチの適用など必要な対策を適時に講じているか。また、脆弱性及び脅威情報の定期的な情報収集・分析・対応を組織的に実施しているか。 （注）電子決済手段の発行及び償還に係る業務において、ブロックチェーン等の技術を利用する場合、関連する周辺技術を含めた幅広い情報収集の必要性があることに留意する。 （削除）	□ システムの脆弱性について、OSの最新化やセキュリティパッチの適用など必要な対策を適時に講じているか。また、脆弱性及び脅威情報の定期的な情報収集・分析・対応を組織的に実施しているか。 □ サイバーセキュリティ水準の定期的な評価を実施し、セキュリティ対策の向上を図っているか。また、国内外でサイバーセキュリティ侵害事案が発生した場合には、適宜リスク評価を行うなど自社への影響を検討しているか。 （略）