事務ガイドライン（第三分冊：金融会社関係　５　前払式支払手段発行者関係）　新旧対照表

改正後	現行
Ⅱ　前払式支払手段発行者の監督上の評価項目	Ⅱ　前払式支払手段発行者の監督上の評価項目
Ⅱ－３－１　システム管理	Ⅱ－３－１　システム管理
前払式支払手段の発行の業務を行うに当たっては、コンピュータシステムのダウンや誤作動等、システムの不備等により、又は、コンピュータが不正に使用されることにより利用者や前払式支払手段発行者が損失を被るリスク（以下「システムリスク」という。）が存在することを認識し、適切にシステムリスク管理を行う必要がある。	前払式支払手段の発行の業務を行うに当たっては、コンピュータシステムのダウンや誤作動等、システムの不備等により、又は、コンピュータが不正に使用されることにより利用者や前払式支払手段発行者が損失を被るリスク（以下「システムリスク」という。）が存在することを認識し、適切にシステムリスク管理を行う必要がある。
特に、IC カードを用いた前払式支払手段やサーバ型前払式支払手段については、発行者が使用するシステムに障害が発生した場合には、発行額、回収額、未使用残高の把握ができなくなるおそれや、前払式支払手段の発行業務が継続不可能となるなど利用者に多大な損害を及ぼすおそれがあることから、特にシステムリスク管理を適切に行う必要がある。	特に、IC カードを用いた前払式支払手段やサーバ型前払式支払手段については、発行者が使用するシステムに障害が発生した場合には、発行額、回収額、未使用残高の把握ができなくなるおそれや、前払式支払手段の発行業務が継続不可能となるなど利用者に多大な損害を及ぼすおそれがあることから、特にシステムリスク管理を適切に行う必要がある。
また、IC カードを用いた前払式支払手段やサーバ型前払式支払手段発行者の IT 戦略は、近年の金融を巡る環境変化も勘案すると、今や当該前払式支払手段発行者のビジネスモデルを左右する重要課題となっており、当該前払式支払手段発行者において経営戦略と IT 戦略を一体的に考えていく必要性が増している。こうした観点から、当該前払式支払手段発行者の規模や特性に応じて、経営者がリーダーシップを発揮し、IT と経営戦略を連携させ、企業価値の創出を実現するための	また、IC カードを用いた前払式支払手段やサーバ型前払式支払手段発行者の IT 戦略は、近年の金融を巡る環境変化も勘案すると、今や当該前払式支払手段発行者のビジネスモデルを左右する重要課題となっており、当該前払式支払手段発行者において経営戦略と IT 戦略を一体的に考えていく必要性が増している。こうした観点から、当該前払式支払手段発行者の規模や特性に応じて、経営者がリーダーシップを発揮し、IT と経営戦略を連携させ、企業価値の創出を実現するための

改正後	現行
仕組みである「IT ガバナンス」を適切に機能させることが極めて重要となっている。 以下の着眼点は IC カードを用いた前払式支払手段やサーバ型前払式支払手段の発行者を想定しているが、字義どおりの対応がなされていない場合にあっても、当該前払式支払手段発行者の規模、前払式支払手段の発行の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。 なお、磁気型・紙型の前払式支払手段を発行する場合にあっても、システム障害により前払式支払手段の発行の業務に支障を来たすおそれがある場合には、必要に応じたシステム管理に係る態勢整備を行う必要がある。 （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）	仕組みである「IT ガバナンス」を適切に機能させることが極めて重要となっている。 以下の着眼点は IC カードを用いた前払式支払手段やサーバ型前払式支払手段の発行者を想定しているが、字義どおりの対応がなされていない場合にあっても、当該前払式支払手段発行者の規模、前払式支払手段の発行の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。 なお、磁気型・紙型の前払式支払手段を発行する場合にあっても、システム障害により前払式支払手段の発行の業務に支障を来たすおそれがある場合には、必要に応じたシステム管理に係る態勢整備を行う必要がある。 （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）
Ⅱ－３－１－１ 主な着眼点 ⑴～⑷ （略） ⑸ サイバーセキュリティ管理 ① 経営陣は、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）	Ⅱ－３－１－１ 主な着眼点 ⑴～⑷ （略） ⑸ 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、経営陣は、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。

改正後	現行
	・サイバー攻撃に対する監視体制 ・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
（削除）	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）
（削除）	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状態 ・システムの全部又は一部の一時的停止　等

改正後	現行
（削除）	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。
（削除）	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。
②　（略）	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機能　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。

改正後	現行
③　（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、連絡可能な利用者に対して速やか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。
（削除）	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。
（中略）	（中略）
第三者型発行者登録審査事務チェックリスト （この章の規定を順守するために必要な体制）	第三者型発行者登録審査事務チェックリスト （この章の規定を順守するために必要な体制）
（略）	（略）
適否　審　査　内　容	適否　審　査　内　容

改正後		現行	
（略）	（略）	（略）	（略）
システム管理（Ⅱ－3－1）		*システム管理（Ⅱ－3－1）*	
（略）	（略）	（略）	（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。	□	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。
（削除）	（削除）	□	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。
（削除）	（削除）	□	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。
（削除）	（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。
（削除）	（削除）	□	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。
（略）	（略）	（略）	（略）
（略）	（略）	（略）	（略）