

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）

現 行	改 正 後
<p>【本編】</p> <p>Ⅱ－3 事務運営</p> <p>Ⅱ－3－1 (略)</p> <p>Ⅱ－3－1－1 主な着眼点</p> <p>(1)システムリスクに対する認識等</p> <p>① (略)</p> <p>② 経営者は、システム障害の未然防止と発生時の迅速な復旧対応について、経営上の重大な課題と認識し、態勢を整備しているか。</p> <p><u>(新設)</u></p> <p>③ (略)</p> <p>④ 経営陣は、<u>システム障害発生等の危機時において、果たすべき責任やとるべき対応について具体的に定めているか。</u> また、自らが指揮を執る訓練を行い、その実効性を確保しているか。</p> <p>(2) (略)</p> <p>(3)システムリスク評価</p> <p>① システムリスク管理部門は、顧客チャネルの多様化による大量取引の発生や、ネットワークの拡充による<u>システム障害の影響の複雑化・広範化</u>など、外部環境の変化によりリスクが多様化していることを踏まえ、定期的に又は適時にリスクを認識・評価しているか。 また、洗い出したリスクに対し、十分な対応策を講じているか。</p> <p>②・③ (略)</p> <p>(4)安全対策</p> <p>安全対策の基本方針が策定されているか。また、定められた方針、基</p>	<p>【本編】</p> <p>Ⅱ－3 事務運営</p> <p>Ⅱ－3－1 (略)</p> <p>Ⅱ－3－1－1 主な着眼点</p> <p>(1) システムリスクに対する認識等</p> <p>① (略)</p> <p>② 経営者は、システム障害やサイバーセキュリティ事案（以下「システム障害等」という。）の未然防止と発生時の迅速な復旧対応について、経営上の重大な課題と認識し、態勢を整備しているか。</p> <p><u>(注)「サイバーセキュリティ事案」とは、情報通信ネットワークや情報システム等の悪用により、サイバー空間を經由して行われる不正侵入、情報の窃取、改ざんや破壊、情報システムの作動停止や誤作動、不正プログラムの実行やDDoS攻撃等の、いわゆる「サイバー攻撃」により、サイバーセキュリティが脅かされる事案をいう。</u></p> <p>③ (略)</p> <p>④ 経営陣は、システム障害等発生時の危機時において、果たすべき責任やとるべき対応について具体的に定めているか。 また、自らが指揮を執る訓練を行い、その実効性を確保しているか。</p> <p>(2) (略)</p> <p>(3) システムリスク評価</p> <p>① システムリスク管理部門は、顧客チャネルの多様化による大量取引の発生や、ネットワークの拡充による<u>システム障害等の影響の複雑化・広範化</u>など、外部環境の変化によりリスクが多様化していることを踏まえ、定期的に又は適時にリスクを認識・評価しているか。 また、洗い出したリスクに対し、十分な対応策を講じているか。</p> <p>②・③ (略)</p> <p>(4) <u>情報セキュリティ管理</u></p> <p>① <u>情報資産を適切に管理するために方針の策定、組織体制の整備、社</u></p>

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）

現 行	改 正 後
<p><u>準及び手順に従って安全対策を適正に管理する担当者を設置しているか。</u></p>	<p><u>内規程の策定、内部管理態勢の整備を図っているか。また、他社における不正・不祥事件も参考に、情報セキュリティ管理態勢のPDCAサイクルによる継続的な改善を図っているか。</u></p>
<p><u>（新設）</u></p>	<p>② <u>情報の機密性、完全性、可用性を維持するために、情報セキュリティに係る管理者を定め、その役割・責任を明確にした上で、管理しているか。また、管理者は、システム、データ、ネットワーク管理上のセキュリティに関することについて統括しているか。</u></p>
<p><u>（新設）</u></p>	<p>③ <u>コンピュータシステムの不正使用防止対策、不正アクセス防止対策、コンピュータウィルス等の不正プログラムの侵入防止対策等を実施しているか。</u></p>
<p><u>（新設）</u></p>	<p>④ <u>前払式支払手段発行者が責任を負うべき利用者の重要情報を網羅的に洗い出し、把握、管理しているか。</u></p>
<p><u>（新設）</u></p>	<p><u>利用者の重要情報の洗い出しにあたっては、業務、システム、外部委託先を対象範囲とし、例えば、以下のようなデータを洗い出しの対象範囲としているか。</u></p>
<p><u>（新設）</u></p>	<p>・ <u>通常の業務では使用しないシステム領域に格納されたデータ</u> ・ <u>障害解析のためにシステムから出力された障害解析用データ 等</u></p>
<p><u>（新設）</u></p>	<p>⑤ <u>洗い出した利用者の重要情報について、重要度判定やリスク評価を実施しているか。</u></p>
<p><u>（新設）</u></p>	<p><u>また、それぞれの重要度やリスクに応じ、以下のような情報管理ルールを策定しているか。</u></p>
<p><u>（新設）</u></p>	<p>・ <u>情報の暗号化、マスキングのルール</u> ・ <u>情報を利用する際の利用ルール</u> ・ <u>記録媒体等の取扱いルール 等</u></p>
<p><u>（新設）</u></p>	<p>⑥ <u>利用者の重要情報について、以下のような不正アクセス、不正情報取得、情報漏えい等を牽制、防止する仕組みを導入しているか。</u></p>
<p><u>（新設）</u></p>	<p>・ <u>職員の権限に応じて必要な範囲に限定されたアクセス権限の付与</u> ・ <u>アクセス記録の保存、検証</u> ・ <u>開発担当者と運用担当者の分離、管理者と担当者の分離等の相互牽制体制 等</u></p>
<p><u>（新設）</u></p>	<p>⑦ <u>機密情報について、暗号化やマスキング等の管理ルールを定めているか。また、暗号化プログラム、暗号鍵、暗号化プログラムの設計書等の管理に関するルールを定めているか。</u></p>
<p><u>（新設）</u></p>	<p><u>なお、「機密情報」とは、暗証番号、パスワード、クレジットカード</u></p>

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）

現 行	改 正 後
<u>（新設）</u>	<u>情報等、利用者に損失が発生する可能性のある情報をいう。</u>
<u>（新設）</u>	⑧ <u>機密情報の保有・廃棄、アクセス制限、外部持ち出し等について、業務上の必要性を十分に検討し、より厳格な取扱いをしているか。</u>
<u>（新設）</u>	⑨ <u>情報資産について、管理ルール等に基づいて適切に管理されていることを定期的にモニタリングし、管理態勢を継続的に見直しているか。</u>
<u>（8）③から移動）</u>	⑩ <u>セキュリティ意識の向上を図るため、全役職員に対するセキュリティ教育（外部委託先におけるセキュリティ教育を含む。）を行っているか。</u>
<u>（新設）</u>	⑪ <u>定期的に、データのバックアップを取るなど、データがき損した場合に備えた措置を取っているか。</u>
<u>（新設）</u>	⑫ <u>定期的に、データのバックアップを取るなど、データがき損した場合に備えた措置を取っているか。</u>
<u>（新設）</u>	⑬ <u>定期的に、データのバックアップを取るなど、データがき損した場合に備えた措置を取っているか。</u>
<u>（新設）</u>	⑭ <u>定期的に、データのバックアップを取るなど、データがき損した場合に備えた措置を取っているか。</u>
<u>（新設）</u>	⑮ <u>定期的に、データのバックアップを取るなど、データがき損した場合に備えた措置を取っているか。</u>
<u>（新設）</u>	⑯ <u>定期的に、データのバックアップを取るなど、データがき損した場合に備えた措置を取っているか。</u>
<u>（新設）</u>	⑰ <u>定期的に、データのバックアップを取るなど、データがき損した場合に備えた措置を取っているか。</u>
<u>（新設）</u>	⑱ <u>定期的に、データのバックアップを取るなど、データがき損した場合に備えた措置を取っているか。</u>
<u>（新設）</u>	⑲ <u>定期的に、データのバックアップを取るなど、データがき損した場合に備えた措置を取っているか。</u>
<u>（新設）</u>	⑲ <u>定期的に、データのバックアップを取るなど、データがき損した場合に備えた措置を取っているか。</u>
<u>（新設）</u>	⑲ <u>定期的に、データのバックアップを取るなど、データがき損した場合に備えた措置を取っているか。</u>
<u>（新設）</u>	⑲ <u>定期的に、データのバックアップを取るなど、データがき損した場合に備えた措置を取っているか。</u>
<u>（新設）</u>	⑲ <u>定期的に、データのバックアップを取るなど、データがき損した場合に備えた措置を取っているか。</u>
<u>（新設）</u>	⑲ <u>定期的に、データのバックアップを取るなど、データがき損した場合に備えた措置を取っているか。</u>
<u>（新設）</u>	⑲ <u>定期的に、データのバックアップを取るなど、データがき損した場合に備えた措置を取っているか。</u>
<u>（新設）</u>	⑲ <u>定期的に、データのバックアップを取るなど、データがき損した場合に備えた措置を取っているか。</u>
<u>（新設）</u>	⑲ <u>定期的に、データのバックアップを取るなど、データがき損した場合に備えた措置を取っているか。</u>
<u>（新設）</u>	⑲ <u>定期的に、データのバックアップを取るなど、データがき損した場合に備えた措置を取っているか。</u>
<u>（新設）</u>	⑲ <u>定期的に、データのバックアップを取るなど、データがき損した場合に備えた措置を取っているか。</u>
<u>（新設）</u>	⑲ <u>定期的に、データのバックアップを取るなど、データがき損した場合に備えた措置を取っているか。</u>

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）

現 行	改 正 後
<p>(5)システム企画・開発・運用管理 ①～⑤ (略)</p> <p>(6)システム監査</p>	<p>・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</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>・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 ・取引に利用しているパソコンのブラウザとは別の携帯電話等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 等</p> <p>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。</p> <p>・不正な IP アドレスからの通信の遮断 ・利用者に対してウイルス等の検知・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 ・前回ログイン（ログオフ）日時の画面への表示 等</p> <p>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。</p> <p>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。</p> <p>(6) システム企画・開発・運用管理 ①～⑤ (略)</p> <p>(7) システム監査</p>

現 行	改 正 後
<p>①～③ （略）</p> <p><u>(7)外部委託管理</u></p> <p>① （略）</p> <p>② 外部委託契約において、外部委託先との役割分担・責任、監査権限、再委託手続き、提供されるサービス水準等を定めているか。</p> <p>③ システムに係る外部委託業務について、リスク管理が適切に行われているか。 特に外部委託先が複数の場合、管理業務が複雑化することから、より高度なリスク管理が求められることを十分認識した体制となっているか。 システム関連事務を外部委託する場合についても、システムに係る外部委託に準じて、適切なリスク管理を行っているか。</p> <p>④ 外部委託した業務について、委託元として委託業務が適切に行われていることを定期的にモニタリングしているか。 また、外部委託先任せにならないように、例えば委託元として要員を配置するなどの必要な措置を講じているか。 さらに、外部委託先における顧客データの運用状況を、委託元が監視、追跡できる態勢となっているか。</p> <p>⑤ （略）</p> <p><u>(8)データ管理態勢</u></p> <p>① <u>データについて機密性等の確保のためデータ管理者を置いているか。</u></p> <p>② <u>データ保護、データ不正使用防止、不正プログラム防止策等について適切かつ十分な管理態勢を整備しているか。</u></p> <p>③ <u>定期的に、データのバックアップを取るなど、データがき損した場合に備えた措置を取っているか。</u></p> <p><u>(9)コンティンジェンシープラン</u></p> <p>①～③ （略）</p>	<p>①～③ （略）</p> <p><u>(8) 外部委託管理</u></p> <p>① （略）</p> <p>② 外部委託契約において、外部委託先との役割分担・責任、監査権限、再委託手続き、提供されるサービス水準等を定めているか。また、<u>外部委託先の役職員が遵守すべきルールやセキュリティ要件を外部委託先へ提示し、契約書等に明記しているか。</u></p> <p>③ システムに係る外部委託業務<u>（二段階以上の委託を含む。）</u>について、リスク管理が適切に行われているか。 特に外部委託先が複数の場合、管理業務が複雑化することから、より高度なリスク管理が求められることを十分認識した体制となっているか。 システム関連事務を外部委託する場合についても、システムに係る外部委託に準じて、適切なリスク管理を行っているか。</p> <p>④ 外部委託した業務<u>（二段階以上の委託を含む。）</u>について、委託元として委託業務が適切に行われていることを定期的にモニタリングしているか。 また、外部委託先任せにならないように、例えば委託元として要員を配置するなどの必要な措置を講じているか。 さらに、外部委託先における顧客データの運用状況を、委託元が監視、追跡できる態勢となっているか。</p> <p>⑤ （略）</p> <p><u>(削除)</u></p> <p><u>(削除)</u></p> <p><u>(削除)</u></p> <p><u>((4)⑪に移動)</u></p> <p><u>(9) コンティンジェンシープラン</u></p> <p>①～③ （略）</p>

現 行	改 正 後
<p>④ コンティンジェンシープランは、他の前払式支払手段発行者におけるシステム障害事例や中央防災会議等の検討結果を踏まえるなど、想定シナリオの見直しを適宜行っているか。</p> <p>⑤ （略）</p> <p>⑥ 業務への影響が大きい重要なシステムについては、オフサイトバックアップシステム等を事前に準備し、<u>災害、システム障害が発生した場合等に</u>、速やかに業務を継続できる態勢を整備しているか。</p> <p>(10)障害発生時の対応</p> <p>① システム障害が発生した場合に、利用者に対し、無用の混乱を生じさせないよう適切な措置を講じているか。 また、システム障害の発生に備え、最悪のシナリオを想定した上で、必要な対応を行う態勢となっているか。</p> <p>② システム障害の発生に備え、外部委託先を含めた報告態勢、指揮・命令系統が明確になっているか。</p> <p>③ 業務に重大な影響を及ぼすシステム障害が発生した場合に、速やかに経営陣に報告するとともに、報告に当たっては、最悪のシナリオの下で生じうる最大リスク等を報告する態勢（例えば、利用者に重大な影響を及ぼす可能性がある場合、報告者の判断で過小報告することなく、最大の可能性を速やかに報告すること）となっているか。 また、必要に応じて、対策本部を立ち上げ、経営者自らが適切な指示・命令を行い、速やかに問題の解決を図る態勢となっているか。</p> <p>④ システム障害の発生に備え、ノウハウ・経験を有する人材をシステム部門内、部門外及び外部委託先等から速やかに招集するために事前登録するなど、応援体制が明確になっているか。</p> <p>⑤ システム障害が発生した場合、障害の内容・発生原因、復旧見込等について公表するとともに、利用者からの問い合わせに的確に対応するため、必要に応じ、コールセンターや相談窓口の設置、認定資金決済事業者協会の協会員の場合には同協会に対応を依頼するなどの措置を迅速に行っているか。 また、システム障害の発生に備え、関係業務部門への情報提供方法、内容が明確になっているか。</p> <p>⑥ システム障害の発生原因の究明、復旧までの影響調査、改善措置、再発防止策等を的確に講じているか。</p>	<p>④ コンティンジェンシープランは、他の前払式支払手段発行者におけるシステム障害等の事例や中央防災会議等の検討結果を踏まえるなど、想定シナリオの見直しを適宜行っているか。</p> <p>⑤ （略）</p> <p>⑥ 業務への影響が大きい重要なシステムについては、オフサイトバックアップシステム等を事前に準備し、<u>災害、システム障害等が発生した場合に</u>、速やかに業務を継続できる態勢を整備しているか。</p> <p>(10) 障害発生時等の対応</p> <p>① システム障害等が発生した場合に、利用者に対し、無用の混乱を生じさせないよう適切な措置を講じているか。 また、システム障害等の発生に備え、最悪のシナリオを想定した上で、必要な対応を行う態勢となっているか。</p> <p>② システム障害等の発生に備え、外部委託先を含めた報告態勢、指揮・命令系統が明確になっているか。</p> <p>③ 業務に重大な影響を及ぼすシステム障害等が発生した場合に、速やかに経営陣に報告するとともに、報告に当たっては、最悪のシナリオの下で生じうる最大リスク等を報告する態勢（例えば、利用者に重大な影響を及ぼす可能性がある場合、報告者の判断で過小報告することなく、最大の可能性を速やかに報告すること）となっているか。 また、必要に応じて、対策本部を立ち上げ、経営者自らが適切な指示・命令を行い、速やかに問題の解決を図る態勢となっているか。</p> <p>④ システム障害等の発生に備え、ノウハウ・経験を有する人材をシステム部門内、部門外及び外部委託先等から速やかに招集するために事前登録するなど、応援体制が明確になっているか。</p> <p>⑤ システム障害等が発生した場合、障害の内容・発生原因、復旧見込等について公表するとともに、利用者からの問い合わせに的確に対応するため、必要に応じ、コールセンターや相談窓口の設置、認定資金決済事業者協会の協会員の場合には同協会に対応を依頼するなどの措置を迅速に行っているか。 また、システム障害等の発生に備え、関係業務部門への情報提供方法、内容が明確になっているか。</p> <p>⑥ システム障害等の発生原因の究明、復旧までの影響調査、改善措置、再発防止策等を的確に講じているか。</p>

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）

現 行	改 正 後
<p>また、システム障害の原因等の定期的な傾向分析を行い、それに 応じた対応策をとっているか。</p> <p>⑦ システム障害の影響を極小化するために、例えば障害箇所を迂回す などのシステムの仕組みを整備しているか。</p> <p>(参考) (略)</p> <p>Ⅱ－３－１－２ 監督手法・対応 (1) (略)</p> <p>(2)障害発生時</p> <p>① 財務局が別途通知する前払式支払手段発行者のIC型又はサーバ型前 払式支払手段についてコンピュータシステムの障害発生を認識した場 合、直ちに、その事実を当局宛てに報告を求めるとともに、「障害等発 生報告書」(別紙様式1の1)にて当局宛てに報告を求めものとする。 また、復旧時、原因説明時には改めてその旨報告を求めることとす る。 ただし、復旧原因の解明がされていない場合でも1か月以内に現状 について行うこととする。 なお、財務局は前払式支払手段発行者より報告があった場合は直ち に金融庁担当課室宛て連絡することとする。</p> <p>(注) 報告すべきシステム障害等 その原因の如何を問わず、前払式支払手段発行者が現に使用してい るシステム・機器(ハードウェア、ソフトウェア共)に発生した障害 であって、 イ. 前払式支払手段の発行若しくは利用の停止等が生じているもの又 はそのおそれがあるもの ロ. その他業務上、上記に類すると考えられるもの をいう。</p> <p>ただし、一部のシステム・機器にこれらの影響が生じても他のシス テム・機器が速やかに交替することで実質的にはこれらの影響が生じ ない場合(例えば、一部の店舗においてシステム障害により前払式支</p>	<p>また、システム障害等の原因等の定期的な傾向分析を行い、それに 応じた対応策をとっているか。</p> <p>⑦ システム障害等の影響を極小化するために、例えば障害箇所を迂回 するなどのシステムの仕組みを整備しているか。</p> <p>(参考) (略)</p> <p>Ⅱ－３－１－２ 監督手法・対応 (1) (略)</p> <p>(2) 障害発生時</p> <p>① 財務局が別途通知する前払式支払手段発行者のIC型又はサーバ型前 払式支払手段についてコンピュータシステムの障害やサイバーセキュ リティ事案の発生を認識した場合、直ちに、その事実を当局宛てに報 告を求めるとともに、「障害等発生報告書」(別紙様式1の1)にて当 局宛てに報告を求めものとする。 また、復旧時、原因説明時には改めてその旨報告を求めることとす る。 ただし、復旧原因の解明がされていない場合でも1か月以内に現状 について行うこととする。 なお、財務局は前払式支払手段発行者より報告があった場合は直ち に金融庁担当課室宛て連絡することとする。</p> <p>(注) 報告すべきシステム障害等 その原因の如何を問わず、前払式支払手段発行者が現に使用してい るシステム・機器(ハードウェア、ソフトウェア共)に発生した障害 であって、 イ. 前払式支払手段の発行若しくは利用の停止等が生じているもの又 はそのおそれがあるもの ロ. その他業務上、上記に類すると考えられるもの をいう。</p> <p>ただし、一部のシステム・機器にこれらの影響が生じても他のシス テム・機器が速やかに交替することで実質的にはこれらの影響が生じ ない場合(例えば、一部の店舗においてシステム障害により前払式支</p>

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）

現 行	改 正 後
<p>払手段の利用ができなくなった場合であっても、近隣店舗によって対応が可能な場合）を除く。</p> <p>なお、障害が発生していない場合であっても、サイバー攻撃の予告がなされ、又はサイバー攻撃が検知される等により、<u>上記のような障害が発生する可能性が高いと認められるときは、報告を要するものとする。</u></p> <p>② （略）</p> <p>③ 特に、<u>大規模な障害</u>の場合や障害の原因の解明に時間を要している場合等には、直ちに、障害の事実関係等についての一般広報及び店頭等における利用者対応等のコンティンジェンシープランの発動状況をモニタリングするとともに、迅速な原因解明と復旧を要請し、法第 24 条に基づき速やかな報告を求める。</p>	<p>払手段の利用ができなくなった場合であっても、近隣店舗によって対応が可能な場合）を除く。</p> <p>なお、障害が発生していない場合であっても、サイバー攻撃の予告がなされ、又はサイバー攻撃が検知される等により、<u>利用者や業務に影響を及ぼす、又は及ぼす可能性が高いと認められるときは、報告を要するものとする。</u></p> <p>② （略）</p> <p>③ 特に、<u>大規模なシステム障害等</u>の場合や障害の原因の解明に時間を要している場合等には、直ちに、障害の事実関係等についての一般広報及び店頭等における利用者対応等のコンティンジェンシープランの発動状況をモニタリングするとともに、迅速な原因解明と復旧を要請し、法第 24 条に基づき速やかな報告を求める。</p>

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）

現 行		改 正 後	
第三者型発行者登録審査事務チェックリスト（この章の規定を遵守するために必要な体制） （略）		第三者型発行者登録審査事務チェックリスト（この章の規定を遵守するために必要な体制） （略）	
適否	審 査 内 容	適否	審 査 内 容
	前払式支払手段の発行の業務に関する社内規則その他これに準ずるもの （内閣府令第16条第8号）など		前払式支払手段の発行の業務に関する社内規則その他これに準ずるもの （内閣府令第16条第8号）など
（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）
<input type="checkbox"/>	システム障害の未然防止と発生時の迅速な復旧対応について、態勢を整備しているか。	<input type="checkbox"/>	システム障害等の未然防止と発生時の迅速な復旧対応について、態勢を整備しているか。
（略）	（略）	（略）	（略）
<input type="checkbox"/>	システム障害発生等の危機時において、とるべき対応について具体的に定めているか。	<input type="checkbox"/>	システム障害等発生等の危機時において、とるべき対応について具体的に定めているか。
（略）	（略）	（略）	（略）
<input type="checkbox"/>	安全対策の基本方針が策定されているか。また、安全対策を適正に管理する担当者を設置しているか。	<input type="checkbox"/>	情報資産を適切に管理するため、情報セキュリティ管理態勢を整備し、PDCAサイクルによる継続的な改善を図っているか。
（新設）	（新設）	<input type="checkbox"/>	情報セキュリティに係る管理者を定め、その役割・責任を明確にした上で情報を管理しているか。
（新設）	（新設）	<input type="checkbox"/>	網羅的に洗い出した利用者の重要情報について、重要度判定やリスク評価を実施した上で、それぞれに応じた情報管理ルールの策定、情報漏えい等を防止する仕組みの導入等を行っているか。
（新設）	（新設）	<input type="checkbox"/>	機密情報について、業務上の必要性を十分に検討し、より厳格な取扱いをしているか。
（新設）	（新設）	<input type="checkbox"/>	情報資産について、管理ルール等に基づいて適切に管理されていることを定期的にモニタリングし、管理態勢を継続的に見直しているか。
（移動）	（移動）	<input type="checkbox"/>	データが毀損した場合に備えた措置を取っているか。
（新設）	（新設）	<input type="checkbox"/>	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。

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）

現 行		改 正 後	
(新設)	(新設)	<input type="checkbox"/>	<u>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。</u>
(新設)	(新設)	<input type="checkbox"/>	<u>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。</u>
(新設)	(新設)	<input type="checkbox"/>	<u>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。</u>
(新設)	(新設)	<input type="checkbox"/>	<u>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。</u>
(新設)	(新設)	<input type="checkbox"/>	<u>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、取引のリスクに見合った認証方式の導入及び業務に応じた不正防止策を講じているか。</u>
(略)	(略)	(略)	(略)
(新設)	(新設)	<input type="checkbox"/>	<u>外部委託契約において、外部委託先との役割分担・責任、監査権限、再委託手続等を定めた上、外部委託先の役職員が遵守すべきルールやセキュリティ要件を契約書等に明記しているか。</u>
<input type="checkbox"/>	システムに係る外部委託業務について、リスク管理が適切に行われているか。	<input type="checkbox"/>	<u>システムに係る外部委託業務(二段階以上の委託を含む。)について、リスク管理が適切に行われているか。</u>
(略)	(略)	(略)	(略)
<input type="checkbox"/>	外部委託した業務について、委託元として委託業務が適切に行われていることを定期的にモニタリングしているか。	<input type="checkbox"/>	<u>外部委託した業務(二段階以上の委託を含む。)について、委託元として委託業務が適切に行われていることを定期的にモニタリングしているか。</u>
<input type="checkbox"/>	データ管理態勢として、以下の事項が整備されているか。 ① <u>データ管理者を置いているか。</u> ② <u>データ保護、データ不正使用防止、不正プログラム防止策等について適切かつ十分な管理態勢を整備しているか。</u> ③ <u>データがき損した場合に備えた措置を取っているか。</u>	(削除)	(削除) (削除) (削除)
(略)	(略)	(略)	(略)
<input type="checkbox"/>	業務への影響が大きい重要なシステムについては、災害、 <u>システム障害が発生した場合等に、速やかに業務を継続できる態勢を整備しているか。</u>	<input type="checkbox"/>	<u>業務への影響が大きい重要なシステムについては、災害、システム障害等が発生した場合に、速やかに業務を継続できる態勢を整備しているか。</u>

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）

現 行		改 正 後	
<input type="checkbox"/>	システム障害の発生に備え、外部委託先を含めた報告態勢、 <u>式・命令系統等</u> が明確になっているか。	<input type="checkbox"/>	システム障害等の発生に備え、外部委託先を含めた報告態勢、 <u>指揮・命令系統</u> が明確になっているか。
<input type="checkbox"/>	システム障害発生時の利用者対応について定めているか。	<input type="checkbox"/>	システム障害等発生時の利用者対応について定めているか。
(略)	(略)	(略)	(略)