事務ガイドライン（第三分冊：金融会社関係　13　指定信用情報機関関係）（新旧対照表）

現　　行	改　正　後
【本編】	**【本編】**
Ⅰ－２－５　システムリスク管理 　システムリスクとは、コンピュータシステムのダウン又は誤作動等のシステムの不備等に伴い加入貸金業者や指定信用情報機関が損失を被るリスクや、コンピュータが不正に使用されることにより加入貸金業者や指定信用情報機関が損失を被るリスクをいう。 　システムが安全かつ安定的に稼動することは指定信用情報機関に対する信頼性を確保するための大前提であり、システムリスク管理態勢の充実強化は極めて重要である。 　指定信用情報機関のシステムリスク管理態勢の監督に当たっては、以下の点に留意する必要がある。	Ⅰ－２－５　システムリスク管理 　システムリスクとは、コンピュータシステムのダウン又は誤作動等のシステムの不備等に伴い加入貸金業者、資金需要者等又は指定信用情報機関が損失を被るリスクや、コンピュータが不正に使用されることにより加入貸金業者、資金需要者等又は指定信用情報機関が損失を被るリスクをいう。 　システムが安全かつ安定的に稼動することは指定信用情報機関に対する信頼性を確保するための大前提であり、システムリスク管理態勢の充実強化は極めて重要である。 　指定信用情報機関のシステムリスク管理態勢の監督に当たっては、以下の点に留意する必要がある。
（１）システムリスクに対する認識等 　①　（略） 　②　代表取締役は、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。 　（新設）	（１）システムリスクに対する認識等 　①　（略） 　②　代表取締役は、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。 （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、サイバー空間を経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。
③　（略） 　④　代表取締役及び取締役（委員会設置会社にあっては執行役）は、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。 　　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。	③　（略） 　④　代表取締役及び取締役（委員会設置会社にあっては執行役）は、システム障害等発生の危機時において、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。
（２）　（略）	（２）　（略）
（３）システムリスク評価 　①　システムリスク管理部門は、ネットワークの拡充によるシステム障害	（３）システムリスク評価 　①　システムリスク管理部門は、ネットワークの拡充によるシステム障害

現　　行	改　正　後
の影響の複雑化・広範化など、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。	等の影響の複雑化・広範化など、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。
②・③　（略）	②・③　（略）
（４）安全対策	（４）情報セキュリティ管理
①　安全対策の基本方針が策定されているか。	①　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。
②　定められた方針、基準及び手順に従って安全対策を適正に管理する安全管理者を設置しているか。安全管理者は、システム、データ、ネットワークの管理体制を統括しているか。	②　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。
③　加入貸金業者が占有管理する端末機やインターネット等を利用して、指定信用情報機関に対して、信用情報の提供又は提供の依頼を行う場合に、コンピュータシステムの事故防止対策、不正使用防止対策及び不正アクセス防止対策等が施されているか。	③　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。
（新設）	④　指定信用情報機関が責任を負うべき加入貸金業者が提供する資金需要者等の重要情報を網羅的に洗い出し、把握、管理しているか。 加入貸金業者が提供する資金需要者等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。 ・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 ・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
（新設）	⑤　洗い出した加入貸金業者が提供する資金需要者等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。 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。 ・情報の暗号化、マスキングのルール ・情報を利用する際の利用ルール ・記録媒体等の取扱いルール　等

現　　行	改　正　後
（新設）	⑥　加入貸金業者が提供する資金需要者等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。 ・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 ・アクセス記録の保存、検証 ・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
（新設）	⑦　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。 なお、「機密情報」とは、信用情報、クレジットカード情報等、加入貸金業者又は資金需要者等に損失が発生する可能性のある情報をいう。
（新設）	⑧　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。
（新設）	⑨　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。
（新設）	⑩　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。
④　災害等に備えた信用情報の安全対策（紙情報の電子化、電子化されたデータファイルやプログラムのバックアップ等）は講じられているか。	⑪　災害等に備えた信用情報の安全対策（紙情報の電子化、電子化されたデータファイルやプログラムのバックアップ等）は講じられているか。
⑤　コンピュータシステムセンター等の安全対策（バックアップセンターの配置、要員・通信回線確保等）は講じられているか。	⑫　コンピュータシステムセンター等の安全対策（バックアップセンターの配置、要員・通信回線確保等）は講じられているか。
⑥　④及び⑤のバックアップ体制は、地理的集中を避けているか。	⑬　⑪及び⑫のバックアップ体制は、地理的集中を避けているか。
（新設）	（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 ・サイバー攻撃を受けた際の報告及び広報体制

現　　行	改　正　後
	・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　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。 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。 ・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　等 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

現　　行	改　正　後
	・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 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。
（５）システム企画・開発・運用管理 ①～⑥　（略）	（６）システム企画・開発・運用管理 ①～⑥　（略）
（６）システム監査 ①～④　（略）	（７）システム監査 ①～④　（略）
（７）外部委託管理 ①　（略） 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。 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。 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。	（８）外部委託管理 ①　（略） 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、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。 ③　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。 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。 ④　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。 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。

現　　行	改　正　後
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。	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。
⑤　（略）	⑤　（略）
（８）データ管理態勢 ①　データについて機密性等の確保のためデータ管理態勢を整備しているか。 ②　データ保護、データ不正使用防止及び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。	（削除）
（９）コンティンジェンシープラン ①～③　（略） ④　コンティンジェンシープランは、他の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。 ⑤　（略） 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、災害、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。	（９）コンティンジェンシープラン ①～③　（略） ④　コンティンジェンシープランは、他の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。 ⑤　（略） 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、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。
(10)　（略）	(10)　（略）
(11) 障害発生時の対応 ①　システム障害が発生した場合に、加入貸金業者及び他の指定信用情報機関等に対し、無用の混乱を生じさせないよう適切な措置を講じることとしているか。 　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。 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。 ③　経営に重大な影響を及ぼすシステム障害が発生した場合に、速やかに代表取締役をはじめとする取締役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	(11) 障害発生時等の対応 ①　システム障害等が発生した場合に、加入貸金業者及び他の指定信用情報機関等に対し、無用の混乱を生じさせないよう適切な措置を講じることとしているか。 　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。 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。 ③　経営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、速やかに代表取締役をはじめとする取締役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

現　　行	改　正　後
ば、加入貸金業者等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、代表取締役等自らが適切な指示・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。 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。 ⑤　システム障害が発生した場合、障害の内容・発生原因及び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、コールセンターの開設等を迅速に行うための態勢整備が講じられているか。 　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。 ⑥　システム障害の発生原因の究明、復旧までの影響調査、改善措置及び再発防止策等を的確に講じることとしているか。 　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。 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るなどのシステム的な仕組みを整備しているか。 （参考）　（略）	えば、加入貸金業者等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、代表取締役等自らが適切な指示・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。 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。 ⑤　システム障害等が発生した場合、障害の内容・発生原因及び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、コールセンターの開設等を迅速に行うための態勢整備が講じられているか。 　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。 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、改善措置及び再発防止策等を的確に講じることとしているか。 　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。 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的な仕組みを整備しているか。 （参考）　（略）