貸金業者向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
【本編】	**【本編】**
Ⅱ－２－４　システムリスク管理態勢 　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、システムの不備若しくはコンピュータが不正に使用されることにより、資金需要者等又は貸金業者が損失を被るリスクをいう。 　仮に、貸金業務をコンピュータシステムを用いて大量に処理する貸金業者においてシステム障害が発生した場合は、資金需要者等の社会経済生活等に影響を及ぼすおそれがあるほか、その影響は単に一貸金業者にとどまらないことから、システムが安全かつ安定的に稼動することは、これらの貸金業者の信頼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。	Ⅱ－２－４　システムリスク管理態勢 　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、システムの不備若しくはコンピュータが不正に使用されることにより、資金需要者等又は貸金業者が損失を被るリスクをいう。 　仮に、貸金業務をコンピュータシステムを用いて大量に処理する貸金業者においてシステム障害やサイバーセキュリティ事案が発生した場合は、資金需要者等の社会経済生活等に影響を及ぼすおそれがあるほか、その影響は単に一貸金業者にとどまらないことから、システムが安全かつ安定的に稼動することは、これらの貸金業者の信頼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。
（注）ここでいう「貸金業務」とは、金銭の交付・債権の回収（弁済の受領）、貸付けに係る契約の締結、返済能力調査、帳簿の作成、個人信用情報の登録等を含み、貸金業務をコンピュータシステムを用いて大量に処理する貸金業者（以下Ⅱ－２－４において単に「貸金業者」という。）としては以下のようなものが想定される。 ・　自社において自動契約受付機又は現金自動設備を設置している貸金業者 ・　受払等業務委託先（銀行、長期信用銀行、協同組織金融機関及び株式会社商工組合中央金庫を含む。以下Ⅱ－２－４において同じ。）と自動契約受付機又は現金自動設備の利用提携をしている貸金業者	（注）ここでいう「貸金業務」とは、金銭の交付・債権の回収（弁済の受領）、貸付けに係る契約の締結、返済能力調査、帳簿の作成、個人信用情報の登録等を含み、貸金業務をコンピュータシステムを用いて大量に処理する貸金業者（以下Ⅱ－２－４において単に「貸金業者」という。）としては以下のようなものが想定される。 ・　自社において自動契約受付機又は現金自動設備を設置している貸金業者 ・　受払等業務委託先（銀行、長期信用銀行、協同組織金融機関及び株式会社商工組合中央金庫を含む。以下Ⅱ－２－４において同じ。）と自動契約受付機又は現金自動設備の利用提携をしている貸金業者
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貸金業者においてなされていない場合にあっても、当該貸金業者の規模、貸金業務の処理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、資金需要者等の保護の観点から、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、以下の各着眼点に記述されている字義どおりの対応が貸金業者においてなされていない場合にあっても、当該貸金業者の規模、貸金業務の処理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、資金需要者等の保護の観点から、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。
（新設）	（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。

貸金業者向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
（１）主な着眼点 （略） ①　システムリスクに対する認識等 イ．　（略） ロ．経営陣は、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。 ハ．　（略） ニ．経営陣は、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。 ②・③　（略） ④　安全対策の整備 イ．安全対策の基本方針が策定されているか。 ロ．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。 ハ．外部委託先等が占有管理する端末機等（入出力装置等を含む。）については、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、不正アクセス防止対策、資金需要者等のプライバシー保護対策が施されているか。 （新設）	（１）主な着眼点 （略） ①　システムリスクに対する認識等 イ．　（略） ロ．経営陣は、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。 ハ．　（略） ニ．経営陣は、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・③　（略） ④　情報セキュリティ管理 イ．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。 ロ．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。 ハ．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。 ニ．貸金業者が責任を負うべき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。 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

貸金業者向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
	・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 ・現金自動設備（店舗外含む。）等に保存されている取引ログ　等
（新設）	ホ．洗い出した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
（新設）	ヘ．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）	ト．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、暗証番号、パスワード、クレジットカード情報等、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）	チ．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）	リ．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）	ヌ．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。
（⑧ハから移動）	ル．定期的に、データのバックアップを取るなど、データが毀損した場合に備えた措置を取っているか。
（⑧ニから移動）	ヲ．指定信用情報機関に提供する個人信用情報の正確性を確保するための方策を取っているか。
（新設）	⑤　サイバーセキュリティ管理 イ．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

現　　行	改　正　後
	必要な態勢を整備しているか。 ロ．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 ・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 ハ．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） ニ．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 ホ．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。 ヘ．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。 ト．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

現　　行	改　正　後
	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 ・同一ユーザーIDからの同時ログインの禁止措置 ・リスクベース認証やキャプチャー認証　等
	チ．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 ・取引時におい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利用者への提供 ・利用者のパソコンのウィルス感染状況を貸金業者側で検知し、警告を発するソフトの導入 ・利用者の口座に振り込む方法による貸付けに当たっては、利用者の本人名義の口座に限定するなど、貸付金の詐取を防ぐ措置の導入 ・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　等
	リ．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。
	ヌ．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	⑥　システム企画・開発・運用管理
イ．～へ．　（略）	イ．～へ．　（略）
⑥　システム監査	⑦　システム監査
イ．～ハ．　（略）	イ．～ハ．　（略）
⑦　外部委託管理	⑧　外部委託管理
イ．　（略）	イ．　（略）
ロ．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、提供されるサービス水準等を定めているか。	ロ．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、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。
ハ．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	ハ．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

現　　行	改　正　後
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。	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。
ニ．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資金需要者等に係る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。	ニ．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。 さらに、外部委託先における資金需要者等に係る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。
ホ．・ヘ．　（略）	ホ．・ヘ．　（略）
⑧　データ管理態勢	（削除）
イ．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。	（削除）
ロ．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。	（削除）
ハ．定期的に、データのバックアップを取るなど、データが毀損した場合に備えた措置を取っているか。	（④ルに移動）
ニ．指定信用情報機関に提供する個人信用情報の正確性を確保するための方策を取っているか。	（④ヲに移動）
⑨　コンティンジェンシープラン	⑨　コンティンジェンシープラン
イ．～ニ．　（略）	イ．～ニ．　（略）
ホ．コンティンジェンシープランは、他の貸金業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。	ホ．コンティンジェンシープランは、他の貸金業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。
へ．　（略）	へ．　（略）
ト．貸金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。	ト．貸金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　障害発生時の対応	⑩　障害発生時等の対応
イ．システム障害が発生した場合に、資金需要者等に無用の混乱を生じさせないための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、	イ．システム障害等が発生した場合に、資金需要者等に無用の混乱を生じさせないための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、

現　　行	改　正　後
必要な対応を行う態勢となっているか。 ロ．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。 ハ．貸金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、資金需要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、経営陣自らが適切な指示・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。 ニ．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。 ホ．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、資金需要者等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を設置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。 ヘ．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。 　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。 ト．システム障害が発生した場合に、書面交付義務違反や指定信用情報機関への個人信用情報提供義務違反等の法令違反が発生していないかを検証する態勢となっているか。 　また、法令違反が認められるときには、真正な書面の再交付や指定信用情報機関に提供した個人信用情報の訂正など、速やかに問題が解消される態勢となっているか。 チ．システム障害の影響を極小化するためのシステム的な仕組みを整備しているか。 ⑪・⑫　（略）	必要な対応を行う態勢となっているか。 ロ．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。 ハ．貸金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、資金需要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、経営陣自らが適切な指示・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。 ニ．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。 ホ．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、資金需要者等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を設置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。 ヘ．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。 　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。 ト．システム障害等が発生した場合に、書面交付義務違反や指定信用情報機関への個人信用情報提供義務違反等の法令違反が発生していないかを検証する態勢となっているか。 　また、法令違反が認められるときには、真正な書面の再交付や指定信用情報機関に提供した個人信用情報の訂正など、速やかに問題が解消される態勢となっているか。 チ．システム障害等の影響を極小化するためのシステム的な仕組みを整備しているか。 ⑪・⑫　（略）

貸金業者向けの総合的な監督指針（新旧対照表）

現　　行	改　正　後
（２）監督手法・対応 ①　（略） ②　システム障害発生時 イ．コンピュータシステムの障害の発生を認識次第、直ちに、その事実についての当局あて報告を求めるとともに、「障害発生等報告書」（別紙様式１）にて当局あて報告を求めるものとする。 また、復旧時、原因解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報告を行うこと。）。 なお、財務局は貸金業者から報告があった場合は直ちに監督局金融会社室に連絡すること。 （注）報告すべきシステム障害等 その原因の如何を問わず、貸金業者又は貸金業者から業務の委託を受けた者等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（受払等業務委託先が設置した自動契約受付機又は現金自動設備に係るシステムにおいて発生した障害を除く。）であって、借入れ・返済、契約の締結、書面の交付その他資金需要者等の利便等に影響があるもの又はそのおそれがあるもの。 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・機器が速やかに代替することで実質的にはこれらの影響が生じない場合を除く。 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、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時は、報告を要するものとする。 ロ．　（略） ③　（略）	（２）監督手法・対応 ①　（略） ②　障害発生時 イ．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次第、直ちに、その事実についての当局あて報告を求めるとともに、「障害発生等報告書」（別紙様式１）にて当局あて報告を求めるものとする。 また、復旧時、原因解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報告を行うこと。）。 なお、財務局は貸金業者から報告があった場合は直ちに監督局金融会社室に連絡すること。 （注）報告すべきシステム障害等 その原因の如何を問わず、貸金業者又は貸金業者から業務の委託を受けた者等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（受払等業務委託先が設置した自動契約受付機又は現金自動設備に係るシステムにおいて発生した障害を除く。）であって、借入れ・返済、契約の締結、書面の交付その他資金需要者等の利便等に影響があるもの又はそのおそれがあるもの。 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・機器が速やかに代替することで実質的にはこれらの影響が生じない場合を除く。 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、資金需要者等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時は、報告を要するものとする。 ロ．（略） ③　（略）

貸金業者向けの総合的な監督指針（新旧対照表）

現　　行		改　正　後	
（中略）		（中略）	
貸金業者登録審査事務チェックリスト（貸金業を的確に遂行するための必要な体制） （略）		貸金業者登録審査事務チェックリスト（貸金業を的確に遂行するための必要な体制） （略）	
適否	**審　査　内　容**	**適否**	**審　査　内　容**
貸金業の業務に関する社内規則（施行規則第４条第３項第１２号）		***貸金業の業務に関する社内規則（施行規則第４条第３項第１２号）***	
（略）	（略）	（略）	（略）
システムリスク管理に関する社内規則等（監督指針Ⅱ－２－４（１））		*システムリスク管理に関する社内規則等（監督指針Ⅱ－２－４（１））*	
（略）	（略）	（略）	（略）
□	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。	□	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）
□	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。	□	システム障害等発生の危機時において、とるべき対応について具体的に定めているか。
（略）	（略）	（略）	（略）
□	安全対策の基本方針が策定されているか。	□	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。
□	安全管理者とその権限を定めているか。	□	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）	□	網羅的に洗い出した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）	□	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）	□	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）	（移動）	□	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）	（移動）	□	指定信用情報機関に提供する個人信用情報の正確性を確保するための方策を取っているか。

貸金業者向けの総合的な監督指針（新旧対照表）

現　　行		改　正　後	
（新設）	（新設）	□	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。
（新設）	（新設）	□	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。
（新設）	（新設）	□	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。
（新設）	（新設）	□	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。
（新設）	（新設）	□	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。
（新設）	（新設）	□	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、取引のリスク及び業務に応じた不正防止策を講じているか。
（略）	（略）	（略）	（略）
（新設）	（新設）	□	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。
□	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る体制が定められているか。	□	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る体制が定められているか。
（略）	（略）	（略）	（略）
□	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。	□	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。
（略）	（略）	（略）	（略）
□	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データ管理者を置いているか。 ②データ保護、データ不正使用防止、不正プログラム防止等について適切かつ十分な管理態勢を整備しているか。 ③データが毀損した場合に備えた措置を取っているか。 ④指定信用情報機関に提供する個人信用情報の正確性を確保するための方策を取っているか。	（削除）	（削除） （削除） （削除） （移動） （移動）
（略）	（略）	（略）	（略）

貸金業者向けの総合的な監督指針（新旧対照表）

現　　行		改　正　後	
□	貸金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。	□	貸金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。
□	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・命令系統等が明確になっているか。	□	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。
□	システム障害発生時の資金需要者等への利用者対応について定めているか。	□	システム障害等発生時の資金需要者等への利用者対応について定めているか。
（略）	（略）	（略）	（略）
（略）	（略）	（略）	（略）