貸金業者向けの総合的な監督指針　新旧対照表（案）

改正案	現行
Ⅱ．貸金業者の監督に当たっての評価項目 Ⅱ－２　業務の適切性 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。 　また、貸金業者のIT戦略は、近年の金融を巡る環境変化も勘案すると、今や貸金業者のビジネスモデルを左右する重要課題となっており、貸金業者において経営戦略をIT戦略と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、貸金業者の規模や業務特性に応じて、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仕組みである「IT ガバナンス」が適切に機能することが極めて重要となっている。	Ⅱ．貸金業者の監督に当たっての評価項目 Ⅱ－２　業務の適切性 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。 　また、貸金業者のIT戦略は、近年の金融を巡る環境変化も勘案すると、今や貸金業者のビジネスモデルを左右する重要課題となっており、貸金業者において経営戦略をIT戦略と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、貸金業者の規模や業務特性に応じて、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仕組みである「IT ガバナンス」が適切に機能することが極めて重要となっている。

改正案	現行
（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。 （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。	（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。 （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。

改正案	現行
（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）	（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）
（１）主な着眼点 システムリスク管理態勢の検証については、貸金業者の業容に応じて、例えば以下の点に留意して検証することとする。 ①～④　（略） ⑤　サイバーセキュリティ管理 イ．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） （削除）	（１）主な着眼点 システムリスク管理態勢の検証については、貸金業者の業容に応じて、例えば以下の点に留意して検証することとする。 ①～④　（略） 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 ・　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。

改正案	現行
	・　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）
（削除）	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
（削除）	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。
（削除）	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。
ロ.　（略）	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を用いるなど、複数経路による取引認証

改正案	現行
ハ．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 （参考） ・　インターネット取引サービスにおける不正取引等防止に関するガイドライン（令和３年 10 月 29 日：日本貸金業協会）	・　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
（削除）	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。

改正案	現行
（削除）	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。
⑥～⑩　（略）	⑥～⑩　（略）
⑪　現金自動設備に係るセキュリティ対策 現金自動設備に係るシステムは、簡単・迅速に金銭の交付及び債権の回収（弁済の受領）を可能にするものであり、資金需要者等にとって利便性が高く、広く活用されている。一方で、現金自動設備に係るシステムを通じた取引は、非対面で行われるため、異常な取引態様を確認できないなどの特有のリスクを抱えている。 したがって、資金需要者等の利便を確保しつつ、資金需要者等の保護の徹底を図る観点から、貸金業者には現金自動設備に係るシステムのセキュリティ対策を十分に講じることが要請される。 また、他の貸金業者等と現金自動設備の利用提携をしている場合において、セキュリティ対策が脆弱な現金自動設備に係るシステムを放置している貸金業者が存在したときは、他の貸金業者等に影響が及ぶことにも留意する必要がある。	⑪　現金自動設備に係るシステムのセキュリティ対策 現金自動設備に係るシステムは、簡単・迅速に金銭の交付及び債権の回収（弁済の受領）を可能にするものであり、資金需要者等にとって利便性が高く、広く活用されている。一方で、現金自動設備に係るシステムを通じた取引は、非対面で行われるため、異常な取引態様を確認できないなどの特有のリスクを抱えている。 したがって、資金需要者等の利便を確保しつつ、資金需要者等の保護の徹底を図る観点から、貸金業者には現金自動設備に係るシステムのセキュリティ対策を十分に講じることが要請される。 また、他の貸金業者等と現金自動設備の利用提携をしている場合において、セキュリティ対策が脆弱な現金自動設備に係るシステムを放置している貸金業者が存在したときは、他の貸金業者等に影響が及ぶことにも留意する必要がある。
イ．　（略）	イ．　（略）
ロ．セキュリティの確保 ローンカードや現金自動設備に係るシステムについて、セキュリティ・レベルを一定の基準に基づき評価するとともに、当該評価を踏まえ、セキュリティ・レベルを維持・向上するために適切な対策を講じているか。セキュリティの確保に当たっては、「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」も参照すること。	ロ．セキュリティの確保 ローンカードや現金自動設備に係るシステムについて、セキュリティ・レベルを一定の基準に基づき評価するとともに、当該評価を踏まえ、セキュリティ・レベルを維持・向上するために適切な対策を講じているか。

<table>
<tr><th>改正案</th><th>現行</th></tr>
<tr><td>（参考）セキュリティに関する基準としては、「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」のほか、「金融機関等コンピュータシステムの安全対策基準・解説書」（公益財団法人金融情報システムセンター編）などがある。
ハ．～ニ．　（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）</td><td>（参考）セキュリティに関する基準としては、「金融機関等コンピュータシステムの安全対策基準・解説書」（公益財団法人金融情報システムセンター編）などがある。
ハ．～ニ．　（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）</td></tr>
<tr><td>
<table>
<tr><th>適否</th><th>審　査　内　容</th></tr>
<tr><td>（略）</td><td>（略）</td></tr>
<tr><td colspan="2">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））</td></tr>
<tr><td>（略）</td><td>（略）</td></tr>
<tr><td>□</td><td>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。</td></tr>
<tr><td>（削除）</td><td>（削除）</td></tr>
<tr><td>（削除）</td><td>（削除）</td></tr>
</table>
</td><td>
<table>
<tr><th>適否</th><th>審　査　内　容</th></tr>
<tr><td>（略）</td><td>（略）</td></tr>
<tr><td colspan="2">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））</td></tr>
<tr><td>（略）</td><td>（略）</td></tr>
<tr><td>□</td><td>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。</td></tr>
<tr><td>□</td><td>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。</td></tr>
<tr><td>□</td><td>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。</td></tr>
</table>
</td></tr>
</table>

改正案		現行	
（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）