貸金業者向けの総合的な監督指針　新旧対照表

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 Ⅱ－２－４－１　システムリスク管理 （１）主な着眼点 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。 ロ．インターネット等の通信手段を利用した非対面の取引（以下「インターネット取引」という。）を行う場合には、Ⅱ－２－４－２の規定に基づく適切な取扱いを確保するための態勢を整備しているか。	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 （新設） （１）主な着眼点 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。 ロ．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 ・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 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

改正案	現行
	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）
⑥～⑫（略） （２）、（３）（略）	⑥～⑫（略） （２）、（３）（略）

改正案	現行
Ⅱ－２－４－２　インターネット取引 　インターネット取引は、貸金業者にとっては低コストのサービス提供を可能とするものであるとともに、利用者にとっては利便性の高い取引ツールとなり得るものである。一方、インターネット取引は、非対面で行われるため、異常な取引態様の確認が困難であることなどの特有のリスクを抱えている。 　貸金業者が顧客にサービスを提供するに当たっては、顧客の財産を安全に管理することが求められる。従って、貸金業者においては、利用者利便を確保しつつ、利用者保護の徹底を図る観点から、インターネット取引に係るセキュリティ対策を十分に講じるとともに、顧客に対する情報提供、啓発及び知識の普及を図ることが重要である。 （１）　主な着眼点 ①内部管理態勢の整備 　インターネット等の不正アクセス・不正取引等の犯罪行為に対する対策等について、犯罪手口が高度化・巧妙化し、被害が拡大していることを踏まえ、最優先の経営課題の一つとして位置付け、経営陣等において必要な検討を行い、セキュリティ・レベルの向上に努めるとともに、利用時における留意事項等を顧客に説明する態勢が整備されているか。 　また、インターネット取引の健全かつ適切な業務の運営を確保	（新設）

改正案	現行
するため、貸金業者内の各部門が的確な状況認識を共有し、貸金業者全体として取り組む態勢が整備されているか。 　その際、金融ＩＳＡＣやＪＰＣＥＲＴ／ＣＣ等の情報共有機関等を活用して、犯罪の発生状況や犯罪手口に関する情報の提供・収集を行うとともに、有効な対応策等を共有し、自らの顧客や業務の特性に応じた検討を行った上で、今後発生が懸念される犯罪手口への対応も考慮し、必要な態勢の整備に努めているか。 　加えて、リスク分析、セキュリティ対策の策定・実施、効果の検証、対策の評価・見直しからなるいわゆるＰＤＣＡサイクルが機能しているか。 ②セキュリティの確保 　セキュリティ体制の構築時及び利用時の各段階におけるリスクを把握した上で、自らの顧客や業務の特性に応じた対策を講じているか。また、個別の対策を場当たり的に講じるのではなく、効果的な対策を複数組み合わせることによりセキュリティ全体の向上を目指すとともに、リスクの存在を十分に認識・評価した上で対策の要否・種類を決定し、迅速な対応が取られているか。 　インターネット取引に係る情報セキュリティ全般に関する方針を作成し、各種犯罪手口に対する有効性等を検証した上で、必要に応じて見直す態勢を整備しているか。また、当該方針等に沿って個人・法人等の顧客属性を勘案しつつ、「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」等も踏まえ、提供するサービスの内容に応じた適切なセキュリティ対策を講じてい	

改正案	現行
るか。その際、犯罪手口の高度化・巧妙化等（「中間者攻撃」や「マン・イン・ザ・ブラウザ攻撃」など）を考慮しているか。 　また、フィッシング詐欺対策については、メールや SMS（ショートメッセージサービス）内にパスワード入力を促すページの URL やログインリンクを記載しない（法令に基づく義務を履行するために必要な場合など、その他の代替的手段を採り得ない場合を除く。）、利用者に対して正規のウェブサイトのブックマークや正規のアプリからログインすることを促す、送信ドメイン認証技術の計画的な導入、フィッシングサイトの閉鎖依頼等、提供するサービスの内容に応じた適切な不正防止策を講じているか。 （注）情報の収集に当たっては、金融関係団体や金融情報システムセンターの調査等、金融庁・捜査当局から提供された犯罪手口に係る情報などを活用することが考えられる。 　インターネット取引を行う場合には、提供するサービスの内容に応じて、以下の不正防止策を講じているか。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、認証方式等の見直しを行っているか。 ・　ログイン、出金、出金先銀行口座の変更など、重要な操作時におけるフィッシングに耐性のある多要素認証（例：パスキーによる認証、PKI（公開鍵基盤）をベースとした認証）の実装及び必須化（デフォルトとして設定） （注１）フィッシングに耐性のある多要素認証の実装及び必	

改正案	現行
須化以降、顧客が設定に必要な機器（スマートフォン等）を所有していない等の理由でやむを得ずかかる多要素認証の設定を解除する場合には、代替的な多要素認証を提供するとともに、解除率の状況をフォローした上で、認証技術や規格の発展も勘案しながら、解除率が低くなるよう多要素の認証の方法の見直しを検討・実施することとする。 （注２）フィッシングに耐性のある多要素認証を実装及び必須化するまでの暫定的な対応として、代替的な多要素認証を提供する場合には、、当該実装及び必須化に向けた具体的なスケジュールについて顧客に周知するとともに、それまでの期間においても、振る舞い検知やログイン通知等の検知機能を強化する必要がある。 ・ 顧客が身に覚えのない第三者による不正なログイン・取引・出金・出金先口座変更を早期に検知するため、電子メール等により、顧客に通知を送信する機能の提供 ・ 認証に連続して失敗した場合、ログインを停止するアカウント・ロックの自動発動機能の実装及び必須化 ・ 顧客のログイン時の挙動の分析による不正アクセスの検知（ログイン時の振る舞い検知）及び事後検証に資するログイン・取引時の情報の保存の実施 ・ 不正アクセスの評価に応じて追加の本人認証を実施するほか、当該不正が疑われるアクセスの適時遮断、不正アクセス	

改正案	現行
元からのアクセスのブロック等の対応の実施 ・ 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と仕組みの整備 ・ 期間ごとの借入上限を顧客が設定できる機能の提供 （参考） ・ フィッシング対策ガイドライン（フィッシング対策協議会） ・ 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（日本貸金業協会） ・ 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（金融情報システムセンター） ③顧客対応 インターネット上での ID・パスワード等の個人情報の詐取の危険性、類推されやすいパスワードの使用の危険性（認証方式においてパスワードを利用している場合に限る。）、被害拡大の可能性等、様々なリスクの説明や、顧客に求められるセキュリティ対策事例の周知を含めた注意喚起等が顧客に対して十分に行われる態勢が整備されているか。 顧客自らによる早期の被害認識を可能とするため、顧客が取引内容を適時に確認できる手段を講じているか。 顧客からの届出を速やかに受け付ける体制が整備されているか。また、顧客への周知（公表を含む。）が必要な場合、速やかにかつ顧客が容易に理解できる形で周知できる体制が整備されているか。特に、被害にあう可能性がある顧客を特定可能な場合は、	

改正案	現行
可能な限り迅速に顧客に連絡するなどして被害を最小限に抑制するための措置を講じることとしているか。 　不正取引を防止するための対策が利用者に普及しているかを定期的にモニタリングし、普及させるための追加的な施策を講じているか。 　不正取引による被害があった場合には、被害状況を十分に精査し、顧客の態様やその状況等を加味したうえで、顧客の被害補償を含め、被害回復に向けて真摯な顧客対応を行う態勢が整備されているか。 　不正取引に関する記録を適切に保存するとともに、顧客や捜査当局から当該資料の提供などの協力を求められたときは、これに誠実に協力することとされているか。 ④その他 　インターネット取引が非対面取引であることを踏まえた、取引時確認等の顧客管理態勢の整備が図られているか。 　インターネット取引に関し、外部委託がなされている場合、外部委託に係るリスクを検討し、必要なセキュリティ対策が講じられているか。 （２）監督手法・対応 　①犯罪発生時 　インターネット取引における不正アクセス・不正取引を認識次第、速やかに「犯罪発生報告書」にて当局宛て報告を求めるもの	

改正案	現行
とする。 　なお、財務局は貸金業者から報告があった場合は直ちに金融庁担当課室に連絡すること。 　②問題認識時 　検査結果、犯罪発生報告書等により、貸金業者のインターネット取引に係る健全かつ適切な業務の運営に疑義が生じた場合には、必要に応じ、法第 24 条の６の 10 に基づき追加の報告を求める。その上で、犯罪防止策や被害発生後の対応について、必要な検討がなされず、被害が多発するなどの事態が生じた場合など、資金需要者保護の観点から問題があると認められる場合には、法第 24 条の６の３第 1 項に基づき業務改善命令を発出する等の対応を行うものとする。	