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

改正後	現行
Ⅰ．指定信用情報機関の指定・監督に当たっての評価項目	Ⅰ．指定信用情報機関の指定・監督に当たっての評価項目
Ⅰ－２　業務の適切性	Ⅰ－２　業務の適切性
Ⅰ－２－５　システムリスク管理	Ⅰ－２－５　システムリスク管理
（１）～（４）　（略）	（１）～（４）　（略）
（５）サイバーセキュリティ管理 ①　取締役会等は、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。	（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。
（削除）	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 ・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
（削除）	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。

改正後	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）	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
	・システムの全部又は一部の一時的停止　等
（削除）	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。
（削除）	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。
②　（略）	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

改正後	現行
③　（略）	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 ・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
（削除）	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。
（削除）	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。