金融サービス仲介業者向けの総合的な監督指針　新旧対照表（案）

改正案	現行
Ⅲ－２－１３　システムリスク管理態勢 Ⅲ－２－１３－２　主な着眼点 システムリスク管理態勢の検証については、金融サービス仲介業者の規模・業務の特性等に応じて、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 ①　経営上責任を負う立場の者は、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）	Ⅲ－２－１３　システムリスク管理態勢 Ⅲ－２－１３－２　主な着眼点 システムリスク管理態勢の検証については、金融サービス仲介業者の規模・業務の特性等に応じて、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 ①　サイバーセキュリティについて、経営上責任を負う立場の者は、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 ・　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

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）	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。
（削除）	⑦　サイバー攻撃を想定したコンティンジェンシープラン（緊急時対応計画）を策定し、訓練や見直しを実施し、高度化を図っているか。
（６）～（１１）　（略）	（６）～（１１）　（略）