保険会社向けの総合的な監督指針　新旧対照表（案）

改正案	現行
Ⅱ－３　統合的リスク管理態勢	Ⅱ－３　統合的リスク管理態勢
Ⅱ－３－13　オペレーショナル・リスク管理態勢	Ⅱ－３－13　オペレーショナル・リスク管理態勢
Ⅱ－３－13－２　システムリスク管理態勢	Ⅱ－３－13－２　システムリスク管理態勢
Ⅱ－３－13－２－１　意義	Ⅱ－３－13－２－１　意義
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のシステムの不備等に伴い、顧客や保険会社が損失を被るリスクやコンピュータが不正に使用されることにより顧客や保険会社が損失を被るリスクを言う。特に、合併や持株会社化による経営統合等の経営再編に伴うシステム統合や新商品・サービスの拡大等に伴い、保険会社の情報システムは一段と高度化・複雑化し、さらにコンピュータのネットワーク化の拡大に伴い、重要情報に対する不正なアクセス、漏洩等のリスクが大きくなっている。システムが安全かつ安定的に稼動することは保険会社に対する信頼性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。	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のシステムの不備等に伴い、顧客や保険会社が損失を被るリスクやコンピュータが不正に使用されることにより顧客や保険会社が損失を被るリスクを言う。特に、合併や持株会社化による経営統合等の経営再編に伴うシステム統合や新商品・サービスの拡大等に伴い、保険会社の情報システムは一段と高度化・複雑化し、さらにコンピュータのネットワーク化の拡大に伴い、重要情報に対する不正なアクセス、漏洩等のリスクが大きくなっている。システムが安全かつ安定的に稼動することは保険会社に対する信頼性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、金融機関の IT 戦略は、近年の金融を巡る環境変化も勘案すると、今や金融機関のビジネスモデルを左右する重要課題となっており、金融機関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、経営者がリーダーシップを発揮し、IT と経	また、金融機関の IT 戦略は、近年の金融を巡る環境変化も勘案すると、今や金融機関のビジネスモデルを左右する重要課題となっており、金融機関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、経営者がリーダーシップを発揮し、IT と経

改正案	現行
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。 （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） Ⅱ－３－13－２－２　主な着眼点 (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。 （削除） （削除）	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。 （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） Ⅱ－３－13－２－２　主な着眼点 (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、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。 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機能
	・　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

改正案	現行
	・　ハードウェアトークン等でトランザクション署名を行うトランザクション認証　等 （注）　不正アクセスによる顧客口座からの不正出金を防止するための措置を講じている場合（例えば、保険金振り込み金融機関口座（出金先口座）の指定・変更手続きにおいて、顧客口座と名義が異なる出金先口座への指定・変更を認めないこととし、さらに転送不要郵便により顧客の住所地に口座指定・変更手続きのための書面を送付するなどにより、顧客口座と名義が異なる出金先口座への振込みを防止する措置を講じている場合）は、取引のリスクに見合った対応がなされているものと考えられる。
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。 ・　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保険会社側で検知し、警告を発するソフトの導入 ・　電子証明書を IC カード等、取引に利用しているパソコンとは別の媒体・機器へ格納する方式の採用 ・　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）	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。

改正案	現行
（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。