保険会社向けの総合的な監督指針（別冊）　（少額短期保険業者向けの監督指針）　新旧対照表

改　正　案	現　行
Ⅱ－3－12 システムリスク	Ⅱ－3－12 システムリスク管理態勢
Ⅱ－3－12－1　システムリスク管理態勢	（新設）
Ⅱ－3－12－1－1 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、顧客や少額短期保険業者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少額短期保険業者が損失を被るリスクをいう。システムが安全かつ安定的に稼動することは少額短期保険業者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、少額短期保険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－3－12－1 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、顧客や少額短期保険業者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少額短期保険業者が損失を被るリスクをいう。システムが安全かつ安定的に稼動することは少額短期保険業者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、少額短期保険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。
（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）
Ⅱ－3－12－1－2 主な着眼点 「総合指針Ⅱ－3－13－2－1－2 ＜システムリスク管理態勢＞ 主な着眼点」に準じて取扱うものとする。	Ⅱ－3－12－2 主な着眼点 「総合指針Ⅱ－3－13－2－2 ＜システムリスク管理態勢＞ 主な着眼点」に準じて取扱うものとする。
Ⅱ－3－12－2　インターネット取引	（新設）
Ⅱ－3－12－2－1　意義 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。）は、少額短期保険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。 少額短期保険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、少額短期保険業者においては、利用者利便を確保しつつ、少額短期保険業者の規模や業務特性に応じて、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	（新設）

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。	
Ⅱ－3－12－2－2　主な着眼点 「総合指針Ⅱ－3－13－2－2－2 ＜インターネット取引＞ 主な着眼点」に準じて取扱うものとする。	（新設）
Ⅱ－3－12－3 監督手法・対応	Ⅱ－3－12－3 監督手法・対応
(1) 問題認識時 システムリスク管理態勢について、問題があると認められる場合、必要に応じて法第 272 条の 22 に基づき報告を求め、重大な問題があると認められる場合には、法第 272 条の 25 又は法第 272 条の 26 に基づき行政処分を行うものとする。	（新設） システムリスク管理態勢について、問題があると認められる場合、障害発生時及びシステム統合時において、必要に応じて法第 272 条の 22 に基づき報告を求め、重大な問題があると認められる場合には、法第 272 条の 25 又は法第 272 条の 26 に基づき行政処分を行うものとする。
(2)障害発生時 ① コンピュータシステムの障害やサイバーセキュリティ事案の発生を認識次第、直ちに、その事実について当局宛て報告を求めるとともに、「障害発生等報告書」（様式集 別紙様式Ⅰ-49）にて当局宛て報告を求めるものとする。ただし、ＤＤｏＳ攻撃事案の場合は「ＤＤｏＳ攻撃事案共通様式」（「サイバー攻撃による被害が発生した場合の報告手続等に関する申合せ」（令和７年５月 28 日関係省庁申合せ（以下、「関係省庁申合せ」という。））別添様式１）、ランサムウェア事案の場合は「ランサムウェア事案共通様式」（関係省庁申合せ 別添様式２）による報告も可能とする。なお、ランサムウェア事案の報告においては、同様式により個人データ等の漏えい等の報告を兼ねることも可能であることに留意する（「金融機関における個人情報保護に関するＱ＆Ａ」参照）。 また、復旧時、原因解明時には改めてその旨報告を求めることとする。 ただし、復旧原因の解明がされていない場合でも 1 ヵ月以内に現状について報告を求めることとする。 （注）報告すべきシステム障害等 その原因の如何を問わず、少額短期保険業者が現に使用しているシステム・機器（ハードウェア、ソフトウェア共）に発生した障害であって、 ア．保険金等の支払いに遅延、停止等が生じているもの又はそのおそれがあるもの イ．資金繰り、財務状況把握等に影響があるもの又はそのおそれがあるもの ウ．その他業務上、上記に類すると考えられるものをいう。 ただし、一部のシステム・機器にこれらの影響が生じても他のシステム・機器が速やかに交替することで実質的にはこれらの影響が生じない場合を除く。 なお、障害が発生していない場合であっても、サイバー攻撃の予告がなされ、又はサイバー攻撃が検知される等により、顧客や業務に影響を及ぼす、又は及ぼす可能性が高いと認められる時は、報告を要するものとする。	（新設）