（仮訳）

I

規則

規則（EC）No 1060/2009、（EU）No 648/2012、（EU）No 600/2014、（EU）No 909/2014 及び（EU）2016/1011 を改正する、金融セクターにおけるデジタル・オペレーショナル・レジリエンスに関する 2022 年 12 月 14 日の欧州議会及び閣僚理事会規則（EU）2022/2554

EEA 適用文書

（仮訳）

欧州議会及び閣僚理事会は、
欧州連合の機能に関する条約、第 114 条を特に根拠として、
欧州委員会の提案を考慮し、
議会への立法案送付後、
欧州中央銀行の意見を考慮し（[1]）、
欧州連合における経済社会評議会の意見を考慮し（[2]）、
通常の立法手続きに従って行動し（[3]）、
前文として以下を述べる。

[1] OJ C 343、26.8.2021、p.1

[2] OJ C 155、30.4.2021、p.38

[3] 2022 年 11 月 10 日の欧州議会の立場（官報未掲載）および 2022 年 11 月 28 日の閣僚理事会の決定

(1) デジタル時代において、情報通信技術（ICT）は日常生活で使用される複雑なシステムを支えている。ICTは金融セクターを含む主要セクターにおける経済を維持し、域内市場の機能を強化する。一方で、デジタル化と相互接続性の発展によりICTリスクも拡大し、社会全体、特に金融システムがサイバー脅威やICTの障害に対してより脆弱になっている。ICTシステムの広域な利用と高度なデジタル化と接続性は、現在EUの金融事業体の活動における中核的な特徴となっているが、こうした事業体のデジタル・レジリエンスはより適切に対応され、業務全体のフレームワークに統合される必要がある。

(2) 過去十数年にわたり、ICTの活用は金融サービスの提供において重要な役割を担うようになり、現在ではすべての金融機関の日常業務において欠かせない存在となっている。デジタル化は、たとえば、現金や紙ベースの方法からデジタルへ移行が進む決済や、同様に、証券の清算と決済、電子取引やアルゴリズム取引、融資や資金調達、P2Pファイナンス、信用格付け、クレーム管理、バックオフィス業務などに及んでいる。保険業界においてもICTの活用により大きな変革が起きており、InsurTechを活用してオンラインでサービスを提供する保険仲介業者の登場や、デジタルによる保険による引き受けプロセスがその代表例である。金融はセクター全体を通じて大部分でデジタル化に進んだだけでなく、デジタル化が金融セクター内、及びサードパーティインフラやサービスプロバイダーとの相互接続性や依存度を高めている。

(3) 欧州システミックリスク理事会(ESRB)は、2020年の報告書において、システミックサイバーリスクに関する見解を改めて示した。その中で、金融機関・金融市場・金融インフラの間での高度に相互接続されている現在の状況、特にそれらのICTシステム間の相互依存関係が、システミックな脆弱性になり得ると指摘している。これは局地的なサイバーインシデントが、地理的な境界に妨げられることなく、約22,000社のEUの金融機関のいずれかから金融システム全体に急速に広まる可能性があるためである。金融分野で深刻なICT侵害が発生すると、個々の金融機関にとどまらず、金融の波及経路を通じて局所的な脆弱性が拡散され、結果としてEU全体の金融システムの安定性に悪影響を及ぼす可能性がある。また、それらは、局地的な脆弱性が金融市場（チャネル）全体に伝播することを容易にし、流動性の取り付け騒ぎや金融市場への信頼と信用の全体的な喪失など、EUの金融システムの安定性に悪影響をもたらす可能性がある。

(4) 近年、国際機関やEU、各国の政策立案者、規制当局、基準設定機関は、デジタル・レジリエンスの強化、基準の設定、規制や監督上業務の協調取り組みの試みにおいて、ICTリスクに注目している。国際的には、バーゼル銀行監督委員会、決済・市場インフラ委員会、金融安定理事会、金融安定研究所、G7及びG20が、様々な管轄区域の所管当局や市場運営者に、金融システムのレジリエンスを強化するツールを提供することを目指している。その取り組みは、国際金融システムの相互接続性が高い状況の中ICTリスクを十分に考慮する必要があり、関連するベストプラクティスのより高い一貫性を追求する必要性にも後押しされている。

(5) EU及び各国による対象を絞った政策・法制度の取り組みにもかかわらず、ICTリスクは依然として、EUの金融システムのオペレーショナル・レジリエンスやパフォーマンス、安定性に対する課題となっている。2008年の金融危機の後に実施された改革は、主にEUの金融セクターの金融レジリエンス

を強化し、経済、健全性、市場行動の観点でEUの競争力と安定性を防御することを目的とした。しかし、ICTセキュリティやデジタル・レジリエンスは、オペレーショナルリスクの一部であるにも関わらず、金融危機後の規制の中心的なテーマにはならず、EUの金融サービス政策や規制の展望、または限られた加盟国においてのみ進展している状況である。

(6) 2018年3月8日付の「フィンテック行動計画：より競争的で革新的な欧州金融セクターに向けて」欧州委員会の通達において、欧州委員会は、EUの金融セクターのレジリエンスを高めることが最も重要であると強調した。これには、運用面から、技術的な安全性と優れた機能の確保、ICT侵害やインシデントからの迅速な復旧さらにはストレス下でもEU全体で金融サービスの効果的かつ円滑な提供を可能にすること、消費者及び市場の信頼・信用を維持することが含まれる。

(7) 2019年4月、欧州議会及び閣僚理事会規則（EU）No 1093/2010（[4]）により設立された欧州監督機構（欧州銀行監督機構）（EBA）、欧州議会及び閣僚理事会規則（EU）No 1094/2010（[5]）により設立された欧州監督機構（欧州保険・企業年金監督機構）（「EIOPA」）、並びに欧州議会及び閣僚理事会規則（EU）No 1095/2010（[6]）により設立された欧州監督機構（欧州証券市場監督機構）（「ESMA」）（総称して「欧州監督機構(ESA）」と呼ばれる）は、金融における一貫したICTリスクアプローチを求めて、EUのセクター別の取り組みを通じて金融サービス業界のデジタル・オペレーショナル・レジリエンスを強化することを勧告する技術的助言を共同で発出した。

(8) EUの金融セクターは、単一のルールブックによって規制され、欧州の金融監督制度によって管理されている。しかし、デジタル時代において金融の安定性および市場の健全性を確保する上で重要であり、例えば共通の健全性基準や市場行動基準と同等に重要であるにも関わらず、デジタル・オペレーショナル・レジリエンス及びICTセキュリティに関する規定は、現状では完全かつ一貫して統一されていない。そのため、単一のルールブックと監督体制は、デジタル業務レジリエンスにも対応できるように発展させる必要があり、監督当局の権限を強化して、金融分野におけるICTリスク管理を適切に監督できるようにし、域内市場の健全性・効率性を保護し、その秩序ある機能を支えるべきとされている。

(9) ICTリスクに関する法制度の格差や、各加盟国による規制・監督のばらつきは、金融サービスにおける域内市場の円滑な機能を妨げる要因になる。これにより、金融機関が国境を越えて事業を展開する際に、設立の自由やサービス提供の自由が阻害されてしまう。また、異なる加盟国で活動する同種の金融機関の間で、公平な競争が損なわれるおそれもある。特に、EUレベルでの調和が限定的である分野、例えばデジタル・オペレーショナル・レジリエンスのテストや、ICTサードパーティリスクの

---

4 欧州監督機構（欧州銀行監督機構）を設立し、決定 No 716/2009/EC を改正し、欧州委員会決定 2009/78/EC を廃止する、2010 年 11 月 24 日の欧州議会および閣僚理事会規則（EU）No 1093/2010（OJ L 331、15.12.2010、p.12）

5 欧州監督機構（欧州保険・企業年金監督機構）を設立し、決定 No 716/2009/EC を改正し、欧州委員会決定 2009/79/EC を廃止する、2010 年 11 月 24 日の欧州議会および閣僚理事会規則（EU）No 1094/2010（OJ L 331、15.12.2010、p.48）

6 欧州監督機構（欧州証券市場監督機構）を設立し、決定 No 716/2009/EC を改正し、欧州委員会決定 2009/77/EC を廃止する、2010 年 11 月 24 日の欧州議会および閣僚理事会規則（EU）No 1095/2010（OJ L 331、15.12.2010、p.84）

監視のような規定が存在しない分野において、このような問題が顕著である。国レベルで想定される動きから生じる相違は、域内市場の機能に対してさらなる支障をきたし、市場参加者と金融の安定を損なう可能性がある。

(10) 現在に至るまで、ICTリスクに関する規定はEUレベルで部分的にしか対応されていないため、たとえばICT関連のインシデント報告やデジタル・オペレーショナル・レジリエンスのテストといった重要な領域において、規制のギャップや重複が存在している。その結果、各国で異なるルールが生まれたり、重複する規制が非効率に適用されたりするなど、一貫性のない状況が発生している。テクノロジーリスクは国境を持たず、金融サービスはEU域内外で広く国境を越えて展開されているため、各国で異なるルールが生まれたり、重複する規制が非効率に適用されたりすることなどは、ICTに大きく依存する金融セクターにとって深刻な問題である。国境を超えて活動する、あるいは複数の認可（例えば、1つの金融機関が銀行業・投資業・決済業のライセンスをもち、それぞれ1つもしくは複数の加盟国の当局からや加盟国から発行されている）を保有する金融機関は、合理的かつ費用対効果の高い方法で、ICTリスクに対応し、インシデントの悪影響を単独で軽減することが、運用上の課題となっている。

(11) 単一のルールブックには包括的なICTまたはオペレーショナルリスクのフレームワークが付随していないため、全ての金融機関への主要なデジタル・オペレーショナル・レジリエンス要件をさらに整合させる必要がある。これらの主要な要件に基づき、金融機関が業務停止に耐えることを目的にICTケイパビリティAと全体的なレジリエンスを向上させることは、EU金融市場の安定性及び健全性の維持に役立ち、ひいてはEUの投資家及び消費者の高いレベルの保護につながる。本規則は、域内市場が円滑に機能することに寄与することを目的としているため、欧州連合の機能に関する条約（TFEU）第114条の条項に基づき、欧州連合司法裁判所の一貫した判例法に従って解釈されるべきものとする。

(12) 本規則は、これまで様々なEUの法令で個別に扱われてきたオペレーショナルリスク要件の一部であるICTリスク要件を統合・高度化することを目的としている。これらの法令は、金融リスクの主要なカテゴリー（例えば信用リスク、市場リスク、取引先信用リスク・流動性リスク、市場リスク等）を対象としていたが、採択当時は、オペレーショナル・レジリエンスの全ての構成要素に包括的に対処していなかった。また、従来の法令におけるオペレーショナルリスクに関するルールは、（つまりICTリスクに対して資本要件を設定するなどの）従来の定量的アプローチが中心であり、ICTインシデントに対する防御・検知・封じ込め・復旧・修復能力や、インシデント報告・デジタルテスト能力といった質的な対応に関するルールは十分に整備されていなかった。これらの法令は、主に、健全性の監督、市場の健全性、または行動に関する必須規則を対象とし、更新することを目的としていた。本規則はICTリスクに関する様々な規則を統合・高度化することにより、金融セクターのデジタルリスクを扱う全ての条項が、初めて一貫した形で単一の法令にまとめられるべきである。そのため本規則は、その法令で使用されている用語に関連するものを含め、いくつかの以前の法令におけるギャップを埋め、また矛盾を是正するものであり、ICTリスクの管理能力、インシデント報告、オペレーショナル・レジリエンスのテスト、ICTサードパーティリスクの監視に関して対象を絞った規則を通じて、ICTリスクを明示的に言及している。本規則はまた、ICTリスク

に対する意識を高め、ICTインシデントやオペレーショナル・レジリエンスの欠如が金融機関の健全性を脅かす可能性があることと認識を広めることにも寄与するべきである。

(13) 金融機関はICTリスクに対処する際、機関の規模及び全体的なリスクプロファイル、並びに機関のサービス、活動、及び業務の内容、規模、及び複雑性を考慮しながら、同一のアプローチ、及び同一の原則ベースの規則に従うべきである。特にICTシステム、プラットフォーム及びインフラに対する依存度が高い場合は、さらなるデジタルリスクを伴うため、一貫性が金融システムに対する信頼を高め、その安定性を維持することに貢献する。基本的なサイバーハイジーンを遵守することで、ICTの障害の影響とコストを最小限に抑えられ、それにより経済全体への過度な負担を回避することが期待される。

(14) 規則は、規制上の複雑さを軽減し、監督上の調和を促進し、法的な確実性を高めるとともに、特に国境を越えて事業を展開する金融機関にとって、コンプライアンスコストを抑え、競争上の歪みを軽減する役割を果たす。したがって、金融機関のデジタル・オペレーショナル・レジリエンスのための共通フレームワークを構築するために規則を採用することは、金融セクターのICTリスク管理における全ての構成要素を首尾一貫して均質に適用することを保証する最も適切な方法といえる。

(15) 欧州議会及び閣僚理事会指令（EU）2016/1148（[7]）は、EUレベルで制定された初の横断的なサイバーセキュリティフレームワークであり、3業態の金融機関（信用機関、取引所、中央清算機関）にも適用された。しかし、本指令は、国レベルの重要サービス事業者を特定する仕組みを定めていたため、実際には加盟国によって特定された一部の信用機関、取引所、中央清算機関のみがその適用対象となり、ICTセキュリティとインシデント通知の要件に遵守する義務を負った。その後、欧州議会及び理事会の指令（EU）2022/2555（[8]）は、3業態の金融機関を適用範囲に残しつつ、適用範囲に含まれる事業体を判断する統一基準（規模上限規則）を設定している。

(16) しかし、本規則はICTリスク管理およびICT関連のインシデント報告に関して、現行のEU金融サービス法に比べより厳格な要件を導入することで、デジタル・レジリエンスの各要素に関する調和水準を高めている。したがって、本規則は、指令(EU)2022/2555に対して「特別法」としての位置づけを持つ。同時に、加盟国が採択したサイバーセキュリティ戦略との整合性を確保し、当該指令の対象である他のセクターに影響を及ぼすサイバーインシデントを金融監督当局が把握できるようにするために、金融機関とＥＵ横断のサイバーセキュリティに係る枠組みとの間の強固な関係を維持することが重要である。

(17) 欧州連合条約第4条第2項に従い、欧州連合司法裁判所による司法審査を妨げることなく、本規則は、公共の安全、防衛、国家安全保障の確保など、本質的な国家機能に関する加盟国の責任に影響を与え

---

[7] EU 全体での高度な共通水準のネットワークセキュリティおよび情報システムセキュリティに向けた措置に関する 2016 年 7 月 6 日の欧州議会および閣僚理事会指令（EU）2016/1148（OJ L 194、19.7.2016、p.1）

[8] 規則（EU）No 910/2014 および指令（EU）2018/1972 を改正し、指令（EU）2016/1148 を廃止する、EU 全体での高度な共通水準のサイバーセキュリティに向けた措置に関する 2022 年 12 月 14 日の欧州議会および閣僚理事会指令（EU）2022/2555（NIS 2 指令）（本官報の p.80 を参照）

るべきではない。例えば、国家安全保障の確保に反する情報の提供に関しては、加盟国の責任の範囲内である。

(18) サイバー脅威への対処において他のセクターの経験から学びそれを活用するために、指令（EU）2022/2555 に言及される金融機関は、同指令の「エコシステム」（例えば、連携グループやコンピュータセキュリティインシデント対応チーム（CSIRT））の一部であり続けるべきである。ESA及び各国の所管当局は、当該指令の下、連携グループの戦略的政策に関する討議及び技術的作業に参加することができ、指定または設置された単一の連絡窓口と情報を交換してさらに協力を行えるべきである。本規則に基づく主管当局もCSIRTと協議及び連携を行うべきであり、また、指令（EU）2022/2555 に基づき指定または設置された主管当局から技術的助言を求めるほか、効果的かつ迅速な調整メカニズムを確保するための協力体制を構築できるようにすべきである。

(19) 金融機関のデジタル・レジリエンスと物理的レジリエンスの間の強い相互関係を踏まえ、本規則並びに欧州議会及び閣僚理事会指令（EU）2022/2557（[9]）には、重要な事業体のレジリエンスに関する一貫したアプローチが必要である。本規則に定めるICTリスク管理及び報告義務によって、金融機関の物理的レジリエンスが包括的に取り扱われていることを踏まえると、指令（EU）2022/2557の第III章及び第IV章に定められている義務は、同指令の適用範囲に該当する金融機関に適用すべきではない。

(20) クラウドサービスプロバイダーは、指令（EU）2022/2555の対象とされるデジタルインフラストラクチャのカテゴリーの一つである。本規則によって構築されるEU監督フレームワーク(Oversight Framework)は、金融機関にICTサービスを提供するクラウドサービスプロバイダーを含む、全ての重要なICTサードパーティサービスプロバイダーに適用され、指令（EU）2022/2555に従って実施される監督を補完するものである。さらに、EUレベルでデジタル監査当局を定める横断的なフレームワークが存在しない場合には、本規則による監督フレームワークがクラウドサービスプロバイダーを対象とするべきである。

(21) ICTリスクを完全に統制するためには、金融機関は強固かつ効果的なICTリスク管理体制に加え、すべてのICT関連のインシデントの対処及び重大インシデントの報告に具体的な仕組みや方針を整備する必要がある。同様に、金融機関は、ICTシステムのテスト、統制及びプロセスに関する政策、並びにICTサードパーティリスク管理の政策が整備されている必要がある。金融機関のデジタル・オペレーショナル・レジリエンスの基準は引き上げられるべき一方で、特定の金融機関、特に小規模事業者には簡素化されたICTリスク管理のフレームワーク比例的な要件の適用を考慮するべきである。年金基金に関して、割合に応じて効率的に監督を促進し、所管当局の事務負担を軽減するため、こうした金融機関に関する国の監督の準備作業は、欧州議会及び閣僚理事会指令（EU）2016/2341（[10]）の第5条で定められた関連する閾値を超える場合でも、機関の規模及び全体的なリスクプロファイル、

---

[9] 閣僚理事会指令 2008/114/EC を廃止する、重要な事業体のレジリエンスに関する 2022 年 12 月 14 日の欧州議会および閣僚理事会指令（EU）2022/2557（本官報の p.164 を参照）

[10] 職域年金基金機関（IORP）の活動および監督に関する 2016 年 12 月 14 日の欧州議会および閣僚理事会指令（EU）2016/2341（OJ L 354、23.12.2016、p.37）

並びにサービス、活動及び業務の内容、規模及び複雑性を考慮に入れるべきである。特に、監督活動は、ある特定の事業体のICTリスク管理に関連する重大なリスクに対処する必要性に主に焦点を当てるべきである。所管当局は、指令（EU）2016/2341の第31条に従って、資産運用、保険数理計算、会計及びデータ管理等、機関の中核業務をサービスプロバイダーにアウトソーシングしている職域年金基金機関の監督に関して、慎重ながらも割合に応じたアプローチを維持すべきである。

(22) ICT関連のインシデント報告の閾値と分類体系は国レベルで大きく異なる。欧州議会及び閣僚理事会規則（EU）2019/881（[11]）によって設立された欧州連合サイバーセキュリティ機構（ENISA）及び指令（EU）2022/2555に基づく連携グループによる関連作業を通じて共通基盤の構築が図られてはいるものの、基準設定や分類体系の仕様についてのアプローチは依然として金融機関の間で相違し、また今後も新たに生じる可能性がある。これらの相違により、特に複数の加盟国で事業を展開している、または金融グループに属している金融機関においては、順守すべき要件が多岐にわたることとなる。さらに、このような相違は、報告プロセスを迅速化し、所管当局間の迅速かつ円滑な情報交換をサポートするような統一的または一元的なEUレベルでの仕組みの構築を妨げる可能性があり、特に組織的な影響を及ぼすおそれのある大規模攻撃が起きた際にICTリスクに対処するために重要である。

(23) 一部の金融機関における事務的負担及び報告の義務の重複を軽減するため、欧州議会及び閣僚理事会指令（EU）2015/2366（[12]）に準拠したインシデント報告に対する要件を、本規則の適用範囲に該当する決済サービスプロバイダーに適用することを止めるべきである。したがって、同指令第33条（1）に規定するように、信用機関、電子マネー事業者、決済機関及び口座情報サービスプロバイダーは、本規則の適用日から、同指令に従って以前に報告された全ての業務またはセキュリティにおける決済関連のインシデントを、当該インシデントがICT関連であるか否かにかかわらず、本規則に従って報告すべきである。

(24) 所管当局がICTインシデントの性質、発生頻度、重要性および影響について全体像を把握し、また法執行機関や破綻処理機構を含む関連公的機関との情報交換を強化できるようにするために、本規則はＩＣＴ関連インシデントの報告制度について強固な報告体制を定めるべきである。全ての金融機関に対して、本規則に規定された単一かつ合理化されたフレームワークを通じて所管当局に報告することを義務付けることにより、ICT関連のインシデント報告制度を整合化させることが不可欠である。さらに、ESAは、分類形態、時間枠、データセット、報告様式、適用閾値など、ICT関連のインシデント報告のフレームワークに関連する要素を具体的に定める権限を与えられるべきである。また、指令（EU）2022/2555との完全な整合性を確保するため、金融機関はサイバー脅威が金融システム、サービス利用者または顧客に関連性があると判断した場合には、関連する所管当局に重大なサイバー脅威を任意で通知することができるものとすべきである。

(25) デジタル・オペレーショナル・レジリエンスのテスト要件は、ある特定の金融サブセクターで策定さ

---

[11] 規則（EU）No 526/2013（サイバーセキュリティ法）を廃止する、ENISA（欧州連合サイバーセキュリティ機関）および情報通信技術サイバーセキュリティ認証に関する 2019 年 4 月 17 日の欧州議会および閣僚理事会規則（EU）2019/881（OJ L 151、7.6.2019、p.15）

[12] 指令 2002/65/EC、2009/110/EC および 2013/36/EU ならびに規則（EU）No 1093/2010 を改正し、指令 2007/64/EC を廃止する、域内市場の決済サービスに関する 2015 年 11 月 25 日の欧州議会および閣僚理事会指令（EU）2015/2366（OJ L 337、23.12.2015、p.35）

れており、必ずしも完全には整合していないフレームワークが設定されている。これは、国境をまたぐ金融機関にとって潜在的なコストの重複を招く可能性があるほか、デジタル・オペレーショナル・レジリエンステストの結果の相互承認を複雑にし、ひいては域内市場に分断を引き起こす可能性がある。

(26) また、ICTテストが求められていない場合、脆弱性は検出されないままであり、金融機関をICTリスクに晒すことになり、最終的には金融セクターの安定性と健全性へのリスクが高くなる。EUによる介入がなければ、デジタル・オペレーショナル・レジリエンステストは一貫性を欠き、各国・各管轄区間域間でICTテスト結果の相互承認の仕組みも欠如したままである。また、ほかの金融サブセクターが大規模かつ実効的なテスト制度を導入する可能性は低いため、ICTの脆弱性やリスクの発見、防衛能力や事業継続性のテストといった、顧客、サプライヤー、ビジネスパートナーの信頼向上に資するテストフレームワークの潜在的なメリットを享受できなくなってしまう。このような重複、相違、ギャップを是正するために、協調的なテスト制度に関する規則を定め、それによって本規則に定められた基準を満たす金融機関に関して、高度なテストの相互承認を促進するべきである。

(27) 金融機関がICTサービスの利用に依存する一因として、台頭する競争の激しいデジタルグローバル経済に適応し、業務効率を高め、消費者の需要を満たさなければならない必要性がある。こうした依存の性質と程度は近年継続的に進化しており、金融仲介業のコスト削減に拍車をかけ、複雑な内部プロセスを管理するのに幅広いICTツールを提供しながら、金融活動を展開する上でのビジネスの拡大とスケーラビリティを可能にしている。

(28) ICTサービスの広範な利用は、複雑な契約上の取り決めに表れており、金融機関は、適用される健全性基準やその他の規制要件に合わせた契約条件の交渉や、アクセス権や監査権といった特定の権利を行使する上で、例えそのような権利が契約上の取り決めに明記されてしたとしてもしばしば困難に直面している。さらに、これらの契約上の取り決めの多くは、再委託プロセスの完全な監視を可能にするような十分な保護措置を定めておらず、そのため、金融機関は関連するリスクを評価する能力を奪われている。さらに、ICTサードパーティサービスプロバイダーは、様々なタイプの顧客に対して標準化されたサービスを提供することが多いため、こうした契約上の取り決めは必ずしも、金融業界関係者の個別のニーズまたは特定のニーズに対して十分に対応していない。

(29) EUの金融サービス法にはアウトソーシングに関する一定の一般的な規則が含まれているものの、契約面の監視がEU法に完全には組み込まれていない。ICTサードパーティサービスプロバイダーとの契約上の取り決めに適用される明確でニーズに合ったEU基準がないため、ICTリスクの外部ソースは包括的に対処されていないのが現状である。したがって、金融機関がICTサードパーティリスクの管理を行う際の指針となる一定の主要な原則を定める必要がある。これらの原則は、ICTサードパーティサービスプロバイダーに重要または重大な機能の支援を委託する場合に特に重要となる、ICTサードパーティリスクの管理に関する一定の主要原則を定める必要がある。また、こうした原則には、契約履行および終了にかかわる複数の要素に関連する基本的な契約上の権利をセットで定めるべきであり、これによって最低限の保護措置を確保し、金融機関がサードパーティレベルで発生するすべてのICTリスクを効果的に監視できる能力を強化することが目的である。これらの原則は、アウトソ

ーシングに適用されるセクター別の法律を補完するものである。

(30) 現在、ICTサードパーティリスクおよびICTサードパーティへの依存に関する監督の均質性や整合性の欠如が顕著にみられる。2019年のアウトソーシングに関するEBAガイドラインや2021年のクラウドサービスプロバイダーへのアウトソーシングに関するESMAガイドラインなど、アウトソーシングに対処するための取り組みにもかかわらず、限られた数の重要なICTサードパーティサービスプロバイダーに金融セクターが晒されることによって引き起こされる可能性のあるシステミックリスクに対処するという広範な問題は、EU法によって十分に対処されていない。EUレベルでの明確な規則が存在しないことに加え、金融当局がICTサードパーティ依存の実態を正確に把握し、集中リスクから生じるリスクを適切に監視するための権限や手法に関する国内ルールも欠如しており、この課題に拍車をかけている。

(31) アウトソーシングの増加とICTサードパーティの集中に伴う潜在的なシステミックリスクを踏まえ、また、重要なICTサードパーティサービスプロバイダーで発生したICTリスクの影響を定量化し、評価し、是正するための適切なツールを金融監督当局に提供する国のメカニズムが不十分であることに留意して、金融機関以外の顧客の機密性とセキュリティが維持されることを確保しつつ、金融機関にとって重要なICTサードパーティサービスプロバイダーであるICTサードパーティサービスプロバイダーの活動を継続的に監視することを可能にする適切な監督フレームワークを確立することが必要である。金融グループ内部によるICTサービスの提供には特定のリスクと便益が伴うが、グループ外部のプロバイダーによるICTサービスの提供よりもリスクが低いと自動的に判断されるべきではなく、同じ規制フレームワークが適用されるべきである。しかし、同じ金融グループ内部でICTサービスが提供される場合、金融機関はグループ内部のプロバイダーに対してより高い管理権限を持つ可能性があるので、リスク評価全体で考慮されるべきである。

(32) ICTリスクがますます複雑化・高度化する中、ICTリスクの発見と防止において適切な対策は、金融機関間で脅威と脆弱性のインテリジェンスをどのくらい定期的に共有しているかに大きく左右される。情報共有は、サイバー脅威の意識向上に貢献する。これにより、金融機関がサイバー脅威に起因するICT関連インシデントを未然に防止する能力が高まり、ICT関連インシデントの影響をより効果的に抑制し、早期に復旧することが可能となる。しかしながら、EUレベルでのガイダンスの欠如により、そのようなインテリジェンスの共有を阻害している要因がいくつかあるようである。特にデータ保護や反トラスト、責任規則との適合性における不確実性がある。

(33) また、他の市場参加者や、監督当局以外の機関（分析情報に関するENISAや法執行目的に関するユーロポールなど）と共有できる情報の種類についての疑義も、重要な情報の提供を控える原因になっている。そのため、現在のところ、情報共有の範囲と質は限定的かつ断片的なままであり、関連する情報交換の大部分は（各国の取り組みによる）局地的なものであり、統合された金融システムのニーズに合わせて個別に作られたEU全体で整合性の取れた情報共有協定は存在しない。したがって、それらのコミュニケーションチャネルを強化することが重要である。

(34) 金融機関は、情報共有の協定に参加することにより、サイバー脅威を適切に評価し、監視し、防御し、

対応する能力を向上させることを目的に、金融機関間でサイバー脅威に関する情報やインテリジェンスを交換し、戦略的、戦術的及び実務的なレベルで個々の知識や実務経験を共同で活用するよう奨励されるべきである。そのためには、信頼できる環境において情報共有を実施する自発的な仕組みがEUレベルで確率されることが必要である。これは、信頼できる環境で実施されれば、ICTリスクの拡散を迅速に制限し、金融チャネル全体への潜在的な伝播を阻止することによって、金融業界コミュニティがサイバー脅威を予防し、まとめて対応するのに有効である。こうしたメカニズムは、「欧州連合の機能に関する条約の第101条の水平的協調協定への適用に関するガイドライン」と題する2011年1月14日の「欧州委員会からのコミュニケーション」に定められたEUの適用競争法規則、並びにEUのデータ保護規則、特に欧州議会及び閣僚理事会規則（EU）2016/679（[13]）を遵守すべきである。
これらの情報共有は、例えば、同規則第 6 条（1）（f）に言及されているように管理者またはサードパーティによって追求される正当な利益のために必要な個人データの取扱いにおいて、並びに、同規則の第 6 条（1）の（c）及び（e）にそれぞれ言及されるように管理者が負う法的義務の遵守に必要な個人データの取り扱いにおいてまたは公共の利益のために実行される職務の遂行あるいは管理者に付与された公的権限の行使において実行される職務の遂行に必要な個人データの取扱いにおいて、同規則第 6 条に定められている法的根拠の一つ以上を使用し、それに基づいて運用されなければならない。

(35) 金融セクター全体として高いデジタル・オペレーショナル・レジリエンスを維持すると同時に、技術の発展に遅れずについていくために、本規則は、あらゆる種類のICTサービスに起因するリスクに対処すべきである。そのため、本規則におけるICTサービスの定義は、広範な形で理解されるべきであり、1つ以上の内部または外部の利用者に継続的に提供されるICTシステムを通じたデジタルサービスやデータサービスを包含すべきである。その定義には、例えば、電気通信サービスのカテゴリーに含まれる、いわゆる「Over The Top」サービスが含まれるべきであり、これらは電子通信サービスの一種に該当する。定義からは、従来のアナログ電話サービスの限定されたカテゴリー、例えば公衆交換電話網（PSTN）サービス、固定電話サービス、一般電話サービス（POTS）、または固定回線電話サービスとして認められたもののみを除外すべきである。

(36) 本規則で想定されている広範な適用範囲にもかかわらず、デジタル・オペレーショナル・レジリエンス規則の適用に当たっては、各金融機関の規模及び全体的なリスクプロファイルにおける金融機関の間の大きな差異を考慮すべきである。一般原則として、ICTリスク管理のフレームワークを実装するための資源及び能力を配分する際には、金融機関は自らの機関の規模及び全体的なリスクプロファイル、並びにサービス、活動及び業務の内容、規模及び複雑性とICT関連のニーズとの間で適切なバランスをとるべきであり、所管当局はそのような配分のアプローチについて引き続き評価及び見直しを行うべきである。

(37) 指令（EU）2015/2366の第33条（1）に言及されている口座情報サービスプロバイダーは、その活動の具体的な内容及びそれから生じるリスクを踏まえ、本規則の適用範囲に明示的に含まれる。さらに、

[13] 指令 95/46/EC（一般データ保護規則）を廃止する、個人データの取り扱いに係る自然人の保護および当該データの自由な移動に関する 2016 年 4 月 27 日の欧州議会および閣僚理事会規則（EU）2016/679（OJ L 119、4.5.2016、p.1）

欧州議会及び閣僚理事会指令2009/110/EC（[14]）の第9条（1）及び指令（EU）2015/2366の第32条（1）によって免除される電子マネー事業者及び決済機関は、指令2009/110/ECに従い電子マネーを発行する権限を付与されていない場合、または指令（EU）2015/2366に従い決済サービスを提供・実行する権限を付与されていない場合でも、本規則の適用範囲に含まれる。ただし、欧州議会及び閣僚理事会指令2013/36/EU（[15]）の第2条（5）の（3）に言及されている郵便振替取扱機関は、本規則の適用範囲から除外される。指令（EU）2015/2366に従って免除されている決済機関、指令2009/110/ECに従って免除されている電子マネー事業者、及び指令（EU）2015/2366の第33条（1）に言及されている口座情報サービスプロバイダーの所管当局は、指令（EU）2015/2366の第22条に従って指定された所管当局とする。

(38) より大規模な金融機関は、より広範なリソースを有し、また、ガバナンス構造の構築や様々な企業戦略の策定に迅速に資金を投入することができるため、本規則の意味する小規模事業者ではない金融機関のみが、より複雑なガバナンス体制の構築を要求されるべきである。具体的には、ICTサードパーティサービスプロバイダーとの取り決めを監督したり、危機管理に対応したりするための専門管理機能の設置、3線防御モデルによるICTリスク管理の体系化、内部リスク管理・コントロールモデルの構築、ICTリスク管理のフレームワークの内部監査への提出などが挙げられる。

(39) 一部の金融機関は、適用除外の恩恵を受けているか、関連するセクター別のEU法の下で非常に軽い規制枠組みの対象となっている。このような金融機関には、欧州議会及び閣僚理事会指令2011/61/EU（[16]）第3条（2）に言及されているオルタナティブ投資ファンドの運用者、欧州議会及び閣僚理事会指令2009/138/EC（[17]）第4条に言及されている保険及び再保険会社、並びに合計加入者数が15人以下の年金制度を運営する職域年金基金機関が含まれる。これらの適用除外に照らして、そのような金融機関を本規則の適用範囲に含めることは規模に見合わないであろう。さらに、本規則は、保険仲介市場構造の特殊性を認めており、その結果、小規模事業者または中小企業としての資格を有する保険仲介業者、再保険仲介業者及び補助保険仲介業者は、本規則の適用範囲から外すべきである。

(40) 指令2013/36/EUの第2条（5）の（4）から（23）に言及されている事業体は同指令の適用範囲から除外されるため、加盟国は、結果的に、自国のテリトリーに所在する当該事業体を本規則の適用から除外することを選択できるべきである。

---

[14] 指令 2005/60/EC および 2006/48/EC を改正し、指令 2000/46/EC を廃止する、電子マネー事業者の事業の開始、遂行、健全性の監督に関する 2009 年 9 月 16 日の欧州議会および閣僚理事会指令 2009/110/EC（OJ L 267、10.10.2009、p.7）

[15] 指令 2002/87/EC を改正し、指令 2006/48/EC および 2006/49/EC を廃止する、信用機関の業務へのアクセスおよび信用機関の健全性の監督に関する 2013 年 6 月 26 日の欧州議会および閣僚理事会指令 2013/36/EU（OJ L 176、27.6.2013、p.338）

[16] 指令 2003/41/EC および 2009/65/EC ならびに規則（EC）No 1060/2009 および（EU）No 1095/2010 を改正する、オルタネイティブ投資ファンドの運用会社に関する 2011 年 6 月 8 日の欧州議会および閣僚理事会指令 2011/61/EU（OJ L 174、1.7.2011、p.1）

[17] 保険および再保険の事業の開始および遂行に関する 2009 年 11 月 25 日の欧州議会および閣僚理事会指令 2009/138/EC（ソルベンシー II）（OJ L 335、17.12.2009、p.1）

(41) 同様に、欧州議会及び閣僚理事会指令2014/65/EU（[18]）の適用範囲に本規則を合わせるために、同指令2014/65/EUに基づいた認可を取得する必要がなく、投資サービスを提供することが認められている同指令の第2条及び第3条に言及されている自然人及び法人を本規則の適用範囲から除外することも適切である。しかしながら、指令2014/65/EUの第2条はまた、証券集中保管機関、集団投資スキーム、保険・再保険事業など、本規則の適用の目的で金融機関としての資格を有する事業体を同指令の適用範囲から除外している。同指令の第2条及び第3条に言及されている個人及び事業体を本規則の適用範囲からの除外に、そうした証券集中保管機関、集団投資スキームまたは保険・再保険事業を含むべきではない。

(42) セクター別のEU法の下では、一部の金融機関は、その規模や提供するサービスに関連する理由から、より軽い要件や免除の対象となっている。その金融機関のカテゴリーには、小規模の非相互接続投資会社、指令（EU）2016/2341の第5条に規定された条件に基づき関係加盟国により同指令の範囲から除外されることができ、かつ合計加入者数が100人以下の年金制度を運営する小規模の年金基金、並びに指令2013/36/EUに従って免除される機関が含まれる。　したがって、比例原則に従い、また、セクター別のEU法の理念を維持するために、これらの金融機関を本規則に基づく簡素化されたICTリスク管理のフレームワークの対象とすることも適切である。これらの金融機関を対象とするICTリスク管理のフレームワークの比例的な特徴は、ESAによってこれから策定される規制技術基準によって変更されるべきではない。さらに、比例原則に従い、指令（EU）2015/2366の第32条（1）に定める決済機関及び指令2009/110/ECの第9条に言及されている電子マネー事業者もこれらのEU法を組み込んだ国内法に従って免除されているが、本規則に基づいて簡素化されたICTリスクの管理フレームワークに従うことが適切である一方、セクター別のEU法を組み込んだそれぞれの国内法に従って免除されていない決済機関及び電子マネー事業者は、本規則に定める一般的なフレームワークに従うべきである。

(43) 同様に、小規模事業者に該当する金融機関または本規則に基づく簡素化されたICTリスク管理のフレームワークの対象となる金融機関は、以下を要求されるべきではない。ICTサービスの利用に関してICTサードパーティサービスプロバイダーと締結した取り決めを監視する役割を定めること、あるいは関連するリスクの影響範囲及び関連文書の監督について責任を負う上級管理職のメンバーを指名すること、利益相反を回避するためにICTリスクを管理・監督する責任をコントロール部署に割り当て、当該コントロール部署において適切な独立性を確保すること、ICTリスク管理のフレームワークを最低年1回文書化しレビューすること、ICTリスク管理のフレームワークを定期的な内部監査の対象にすること、ネットワークや情報システムのインフラやプロセスを大幅に変更した後に詳細な評価を実施すること、レガシーICTシステムのリスク分析を定期的に実施すること、ICT対応・復旧計画の実施を独立内部監査レビューの対象とすること、危機管理機能を持ち一次ICTインフラと余剰設備の切り替えシナリオを把握するために事業継続及び対応・復旧計画のテストを拡大すること、ICT能力の冗長性を維持するために、所管当局の要請に応じて、主要なICT関連インシデントによって引き起こされる年間総コストと損失の見積もりを報告すること、ICT関連インシデン

---

[18] 指令 2002/92/EC および指令 2011/61/EU を改正する、金融商品市場に関する 2014 年 5 月 15 日の欧州議会および閣僚理事会指令 2014/65/EU（OJ L 173、12.6.2014、p.349）

トレビュー後に実施された変更を国の所管当局に伝えること、関連する技術動向を継続的に監視すること、本規則に定めるICTリスク管理のフレームワークの不可欠な部分として包括的なデジタル・オペレーショナル・レジリエンステストプログラムを確立すること、またはICTサードパーティリスクに関する戦略を採択し定期的に見直すこと。

また、小規模事業者は、自社のリスクプロファイルに基づいて冗長な ICT 能力を維持する必要性を評価することのみが求められるべきである。小規模事業者は、デジタル・オペレーショナル・レジリエンステストプログラムに関して、より柔軟な制度からメリットを得るべきである。実施するテストの種類と頻度を検討する際には、高いデジタル・オペレーショナル・レジリエンスを維持するという目的、利用可能なリソース、自社の全体的なリスクプロファイルのバランスを適切にとるべきである。

本規則の簡素化された ICT リスク管理のフレームワークの対象となる小規模事業者及び金融機関は、脅威ベースのペネトレーションテスト（TLPT）に基づいて ICT ツール、システム及びプロセスの高度なテストを実施する要件から免除されるべきであり、本規則で定める基準を満たす金融機関のみにそのようなテストの実施を義務付けるべきである。その限られた能力に踏まえ、小規模事業者は、金融機関のアクセス、検査、監査の権利を ICT サードパーティサービスプロバイダーが任命した独立サードパーティに委任することに ICT サードパーティサービスプロバイダーと合意できるべきである。ただし、金融機関は、いつでも、当該独立サードパーティから ICT サードパーティサービスプロバイダーのパフォーマンスにおける全ての関連情報及び保証を要求することができる。

(44) 高度なデジタル・レジリエンステストの目的で特定された金融機関のみが脅威ベースのペネトレーションテスト脅威ベースのペネトレーションテストの実施を求められるべきである。そのため、そのテストの実施に伴う管理プロセスと財務コストは、少数の金融機関によって負担されるべきである。

(45) 金融機関の事業戦略とICTリスクの経営との完全で全体的な整合性を確保するためには、金融機関の経営陣が、ICTリスク管理のフレームワークとデジタル・オペレーショナル・レジリエンス戦略全体の指導と適応において中心的かつ積極的な役割を担うことが求められるべきである。経営陣が取るべきアプローチは、ICTシステムのレジリエンスを確保する手段にとどまらず、企業の各組織階層や全職員に対してサイバーリスクに対する強い意識を養い、あらゆるレベルにおいて厳格なサイバーハイジーンを守るというコミットメントを醸成する一連の方針を通じて、人とプロセスにまで及ぶべきである。金融機関のICTリスクを管理する上での経営陣の最終的な責任は、その包括的アプローチの最重要原則であるべきであり、さらに言えば、ICTリスク管理の監視のコントロールに経営陣が継続的に関与すべきである。

(46) また、金融機関のICTリスク管理に対して全面的かつ最終的な責任を経営陣が負うという原則は、金融機関が高いレベルのデジタル・オペレーショナル・レジリエンスを達成できるように、金融機関が一定レベルのICT関連投資や全体予算を確保する必要性と密接に関連している。

(47) 本規則は、関連する国際、国内及び業界のベストプラクティス、ガイドライン、勧告及びサイバーリスク管理へのアプローチに着想を得て、ICTリスク管理の全体構造を促す一連の原則を奨励している。したがって、金融機関が備えている主要な機能によって本規則で規定されているICTリスク管理の諸機能（識別、保護と防止、検出、対応と復旧、教訓と発展、コミュニケーション）が対応されている限り、金融機関は異なるフレームワークや分類のICTリスク管理モデルを自由に使用することができ

る。

(48) 進化するサイバー脅威の状況に対応するためには、金融機関は、サービスに必要なデータの処理を保証するだけでなく、市場環境の悪化やその他の悪条件による追加的な処理ニーズに適切に対応することを可能にする十分な技術的レジリエンスを確保するために、高い信頼性と機能を備えた最新のICTシステムを維持する必要がある。

(49) 金融機関が、サイバー攻撃をはじめとするICT関連インシデントにおいて、バックアップ方針に基づき、被害を食い止め、業務の再開や復旧を優先して迅速に対応するためには、効率的な事業継続・復旧計画が必要である。しかしながら、そのような業務の再開は、ネットワークや情報システムの完全性及びセキュリティ、またはデータの可用性、真正性、完全性あるいは機密性を決して危険にさらしてはならない。

(50) 本規則は、金融機関が、関連する機能の性質と重要性、及び特定のビジネスニーズを十分に考慮して、柔軟な方法で目標復旧時間（RTO）及び目標復旧時点（RPO）を決定して、それらの目標を設定することを認めている。しかしながら、当該目標を決定する際には、市場の効率性に与える潜在的な全体的影響を評価することを金融機関に求めるべきである。

(51) サイバー攻撃の実行者は、攻撃元で金銭的利益を直接的に追求する傾向があり、その結果、金融機関が重大な影響を受ける可能性がある。ICTシステムが完全性を失ったり、利用できなくなったりすることを防ぎ、データ漏洩やICTインフラの物理的損傷を回避するために、金融機関による主要なICT関連インシデントの報告を大幅に改善し、合理化する必要がある。ICT関連のインシデント報告は、全ての金融機関が関連所管当局に直接報告するという要件の導入を通じて整合化されるべきである。金融機関が複数の国の所管当局による監督の対象となる場合、加盟国は、当該報告先として単一の所管当局を指定すべきである。閣僚理事会規則（EU）No 1024/2013（[19]）の第6条（4）に従って重要と分類された信用機関は、当該報告を各国の所管当局に提出すべきであり、所管当局はその後、その報告を欧州中央銀行（ECB）に伝達すべきである。

(52) 重大なICT関連のインシデントについての直接報告は、金融監督当局が該当インシデントに関する情報へ即時にアクセスできるようにするものである。金融監督当局は、同様に、主要なICT関連インシデントの詳細を公の非金融当局（例えば、指令（EU）2022/2555に基づく所管当局や単一の連絡窓口、国のデータ保護当局、及び犯罪の性質を有する主要なICT関連インシデントに関する法執行当局など）に伝え、これらの当局が当該インシデントへの意識を高めるように、CSIRTの場合には、必要に応じて金融機関に提供される可能性のある迅速な支援を促すようにすべきである。さらに、加盟国は、金融機関が当該情報を金融サービス分野以外の公的機関に提供すべきであると決定できる必要がある。こうした情報の流れによって、金融機関が当該当局から、関連する技術的情報、救済策に関する助言、及びその後のフォローアップを得て、迅速にメリットを得られるように

---

[19] 信用機関の健全性の監督に関連する政策について欧州中央銀行に特定の任務を与える 2013 年 10 月 15 日の閣僚理事会規則（EU）No 1024/2013（OJ L 287、29.10.2013、p.63）

すべきである。主要なICT関連インシデントに関する情報は相互に伝達されるべきである。すなわち、金融監督当局は金融機関に必要なフィードバックやガイダンスを全て提供すべきであり、ESAはより広範な集団防衛を支援するために、インシデントに関連するサイバー脅威や脆弱性に関する匿名化されたデータを共有すべきである。

(53) 全ての金融機関がインシデント報告の実施を求められるべきであるが、その要件が全ての金融機関に同じように影響を与えるとは想定されていいない。実際、ESAによって今後策定される規制技術基準に基づく委任法令において、重要性の閾値や報告期限は、主要なICT関連インシデントのみを対象とするという観点から、適切に調整されるべきである。さらに、報告義務の期限を設定する際は、金融機関ごとの特性を考慮すべきである。

(54) 本規則は、信用機関、決済機関、口座情報サービスプロバイダー及び電子マネー提供機関に対し、以前に指令（EU）2015/2366に基づき報告された全ての業務上またはセキュリティ上の決済に関連するインシデントを、インシデントのICT内容にかかわらず報告することを義務付けるべきである。

(55) ESAは、EUレベルでICT関連インシデント報告の一元化について実現可能性及び条件を評価する任務を負うべきである。そのような一元化は、以下のいずれかによる主要なICT関連インシデント報告のEU共通の情報ハブで構成することができる。関連報告を直接受け取り、自動的に各国の所管当局に通知する方式か、あるいは単に各国の所管当局から送られた関連報告を一元化し、取りまとめの役割を果たす方式かである。ESAは、ECBとENISAと協議の上、EU共通の情報ハブの設立の実現可能性を探る共同報告書を作成する任務を負うべきである。

(56) 高水準のデジタル・オペレーショナル・レジリエンスを達成するために、関連する国際基準（例えば、脅威ベースのペネトレーションテストに関するG7の基礎的要素）及びTIBER-EU等のEUの適用フレームワークに沿って、金融機関は、潜在的なICTの脆弱性を発見・対処するために、ICTシステム及びICT関連の責任を有する職員の防止力、検知力、対応力及び復旧力の有効性に関して定期的にテストするべきである。金融機関のサイバーセキュリティへの準備態勢レベルに関して、様々な金融サブセクター間や金融サブセクター内の相違を反映するために、テストには、基本要件の評価（例えば、脆弱性評価及びスキャン、オープンソース分析、ネットワークセキュリティ評価、ギャップ分析、物理的セキュリティレビュー、アンケート及びスキャンソフトウェアソリューション、実現可能な場合はソースコードレビュー、シナリオベースのテスト、互換性テスト、パフォーマンステスト、エンドツーエンドテストなど）からTLPTによる高度なテストまで、幅広いツールと措置が含まれるべきである。そのような高度なテストは、ICTの観点からそれを合理的に実施できるほど十分に成熟した金融機関にのみ要求されるべきである。したがって、本規則で要求されるデジタル・オペレーショナル・レジリエンステストは、本規則に定められた基準を満たすこれらの金融機関（例えば、大規模でシステミックかつICTの成熟度が高い信用機関、証券取引所、証券集中保管機関、清算機関）に対して、他の金融機関よりも要求の厳しいものである必要がある。同時に、TLPTによるデジタル・オペレーショナル・レジリエンステストは、中核的な金融サービスサブセクターで事業を行い、システミックな役割を果たしている金融機関（例えば、支払い、銀行取引、清算、決済）に対してはより関連性が高く、他のサブセクター（例えば、資産運用会社や信用

格付け会社）に対しては関連性がより低くあるべきである。

(57) 国境を越えた業務に関与し、EU域内で設立の自由またはサービス提供の自由を行使する金融機関は、自国の加盟国において高度なテストの一連の要件（すなわちTLPT）を遵守するべきである。この要件には、国境を越えた金融グループがEU域内で運用する全ての管轄区域のICTインフラが含まれるべきであり、それにより、このような国境を越えた金融グループは、1カ所の管轄区域においてのみ関連するICTテスト費用を負担することが可能になる。

(58) ある特定の所管当局が既に獲得した専門知識、特にTIBER-EUフレームワークの実施に関する専門知識を活用するため、本規則は、加盟国が、国家レベルで金融セクターにおける全てのTLPTに関する事項を担当する単一の公的機関を指定することを認めるべきであり、また、そのような指定がない場合は、所管当局がTLPT関連業務の遂行を国の他の金融所管当局に委任することを認めるべきである。

(59) 本規則は、1回の脅威ベースのペネトレーションテストで全ての重要または重大な機能をカバーすることを金融機関に求めていないため、金融機関は、当該テストの範囲にどの重要または重大な機能をどれだけ含めるかを自由に決定できるものとすべきである。

(60) 本規則の意味におけるプールテスト ― 複数の金融機関がTLPTに参加し、ICTサードパーティサービスプロバイダーが外部テスターと直接契約を締結できるテスト ― は、本規則の適用範囲外の事業体である顧客に対してそのICTサードパーティサービスプロバイダーが提供するサービスの品質またはセキュリティ、または当該サービスに関連するデータの機密性が悪影響を受けることが合理的に予想される場合にのみ許可されるべきである。プールテストは、本規則に基づいたTLPTの目的を満たす参加金融機関に関して厳格なテストの実施を確保するため保護措置（指定された1社の金融機関による指示、参加金融機関の数の調整）の対象とすべきである。

(61) 企業レベルで利用可能な内部リソースを活用するために、本規則は、TLPTにおける脅威インテリジェンスのプロバイダーが常に金融機関の外部者であることを求めながら、監督当局の承認があり、利益相反がなく、内部テスターと外部テスターの定期的な交代（3回ごとのテスト）があることを条件として、TLPT実施の目的での内部テスターの使用を金融機関に認めるべきである。TLPTの実施責任は、全面的に金融機関にあるものとする。当局によって提供されるアテステーションは、相互承認のみを目的とするものであり、金融機関がさらされているICTリスクに対処するために必要なフォローアップ措置を妨げるものではなく、また、当該金融機関のICTリスク管理及び緩和能力を管理当局が承認・補償したことを意味するものではない。

(62) 金融セクターにおけるICTサードパーティリスクの健全な監視を確保するためには、特に重要または重大な機能を支えるICTサービスについて、ICTサードパーティサービスプロバイダーにアウトソーシングされた機能に関連して発生するリスク、そしてより一般的にはICTサードパーティへの依存に関連して発生するリスクを金融機関が監視する際の指針となる一連の原則ベースのルールを規定する必要がある。

(63) 金融サービスの円滑な提供を可能にする技術的ソリューションのプロバイダーの多さと多様さを考慮しつつ、ICTリスクの様々な発生源の複雑さに対処するため、本規則は、クラウドサービス、ソフトウェア、データ分析サービスのプロバイダー、データセンターサービスのプロバイダーなど、広範なICTサードパーティサービスプロバイダーを対象とすべきである。同様に、金融機関は、金融グループ内で調達されるICTサービスにおける文脈を含め、あらゆる種類のリスクを効果的かつ筋道を明確にして正しく特定・管理する必要があるため、金融グループの一員であり、ICTサービスを主に親会社または親会社の子会社若しくは支店に提供する企業、及び他の金融機関にICTサービスを提供する金融機関も、本規則にしたがいICTサードパーティサービスプロバイダーとみなされることを明示すべきである。最後に、進化する決済サービス市場が複雑な技術的ソリューションにますます依存するようになっていること、また新たな種類の決済サービス及び決済関連ソリューションが出現していることを踏まえると、決済処理業務を提供するまたは決済インフラを運営する決済サービスエコシステムの参加者も、中央銀行が決済または証券決済システムを運営する場合、及び政府当局が国の機能を果たす上でICT関連サービスを提供する場合を除き、本規則の下ではICTサードパーティサービスプロバイダーとみなされるべきである。

(64) 金融機関は、本規則に定める義務を遵守することについて、常に全面的な責任を負うべきである。金融機関は、ICT関連の依存の性質、規模、複雑性及び重要性、契約上の取り決めの対象となるサービス、プロセスまたは機能の重要性を十分に考慮することにより、また、最終的には、必要に応じて、個人レベル及びグループレベルで金融サービスの継続性及び質に与える潜在的影響の慎重な評価に基づいて、ICTサードパーティサービスプロバイダーのレベルで生じるリスクの監視に比例的アプローチを適用すべきである。

(65) このような監視は、全てのICTサードパーティへの依存の継続的な審査に基づき、金融機関の経営陣が専用ICTサードパーティリスク戦略の採択を通じて正式なものとなったICTサードパーティリスクへの戦略的アプローチに沿って実施されるべきである。ICTサードパーティへの依存に関する監督上の意識を高めるために、また、本規則によって設立された監督フレームワークの下での業務支援を強化する観点から全ての金融機関は、ICTサードパーティサービスプロバイダーから提供されるICTサービスの利用に関する全ての契約上の取り決めについて、情報の登録簿に記録することが求められるべきである。金融監督当局は、金融機関のICTへの依存をより広範に把握するために必要な情報を入手するため、登録簿全体を要求したり、特定の箇所を要求したりできるようにすべきである。

(66) 特に、想定されるICT契約によってサポートされるサービスの重要性、必要な監督上の承認若しくはその他の条件、それに伴う可能性のある集中リスクといった要素に焦点を当てるとともに、ICTサードパーティサービスプロバイダーの選定と評価の過程でデューデリジェンスを適用し、潜在的な利益相反を評価することによって、徹底的な契約前分析は、正式な契約締結の根拠となり、契約に先立って行われるべきである。重要または重大な機能に関する契約上の取り決めについては、金融機関は、ICTサードパーティサービスプロバイダーによる最新かつ最高の情報セキュリティ基準の使用を考慮に入れるべきである。契約上の取り決めの終了は、少なくとも、ICTサードパーティサービスプロバイダーレベルでの欠陥を示す一連の状況、特に法律または契約条件の重大な違反、契約上の取り決めに規定された機能の遂行の潜在的な変更を明らかにする状況、全体的なICTリスク管理における

ICTサードパーティサービスプロバイダーの弱点の証拠、または関連する所管当局が金融機関を効果的に監督できないことを示す状況によって促される可能性がある。

(67) 厳格な上限や厳しい制限を課すことは事業の遂行を妨げ、契約の自由を制約する可能性があるため、本規則ではICTサードパーティ集中リスクのシステミックな影響に対処するために、そのような集中リスクに対して柔軟かつ段階的なアプローチをとることでバランスのとれたソリューションを推進している。金融機関は、特に第三国で設立されたICTサードパーティサービスプロバイダーと締結する場合、再委託契約の詳細な分析などを含め、想定される契約上の取り決めを徹底的に評価し、そのようなリスクが発生する可能性を特定すべきである。現時点では、契約上の自由の保護と金融の安定性の保証とのバランスを考慮すると、ICTサードパーティのエクスポージャーに対して厳格な上限と制限を設けることは適切ではないと考えられる。監督フレームワークに関しては、本規則に従って任命された主監督者は、重要なICTサードパーティサービスプロバイダーに関しては、相互依存関係の大きさを十分に把握することに注意を払い、EUにおける重要なICTサードパーティサービスプロバイダーの集中度が高くなりすぎることがEUの金融システムの安定性と健全性に負担をかける可能性がある具体的な事例を発見し、具体的なリスクが特定された場合には重要なICTサードパーティサービスプロバイダーとの対話を維持するべきである。

(68) 金融機関のデジタル・オペレーショナル・レジリエンスに悪影響を及ぼすことなく金融機関に安全にサービスを提供するICTサードパーティサービスプロバイダーの能力を定期的に評価・監視するためには、ICTサードパーティサービスプロバイダーとの間でいくつかの主要な契約要素について整合性を取る必要がある。その整合性を取る範囲は、金融機関がデジタル・レジリエンスを確保する必要性の観点から、ICTサードパーティサービスプロバイダーから生ずるリスクを金融機関が十分に監視できるようにするのに最低でも不可欠な分野を対象とするべきである。なぜなら、デジタル・レジリエンスは、金融機関が受けるICTサービスの安定性、機能性、可用性及びセキュリティに深く依存しているからである。

(69) 本規則の要件との整合性を確保するために契約上の取り決めについて再交渉する場合、金融機関及びICTサードパーティサービスプロバイダーは、本規則に規定されている主要な契約上の条項を必ず適用範囲に含めるべきである。

(70) 本規則に定める「重要または重大な機能」の定義は、欧州議会及び閣僚理事会指令2014/59/EU（[20]）の第2条（1）、（35）に定義された「重要な機能」を含む。したがって、指令2014/59/EUに従って重要とみなされる機能は、本規則の意味での重要な機能の定義に含まれる。

(71) ICTサービスによってサポートされる機能の重要性を問わず、契約上の取り決めには、特に、機能及びサービスの完全な内容、当該機能が提供される場所及びデータが処理される場所、並びにサービスレベルの内容の記載を規定すべきである。金融機関によるICTサードパーティリスクの監視を

---

[20] 閣僚理事会指令 82/891/EEC、ならびに欧州議会および閣僚理事会指令 2001/24/EC、2002/47/EC、2004/25/EC、2005/56/EC、2007/36/EC、2011/35/EU、2012/30/EU および 2013/36/EU、ならびに欧州議会および閣僚理事会規則（EU）No 1093/2010 および（EU）No 648/2012 を改正し、信用機関および投資会社の再建と破綻処理に関する枠組みを設定する、2014 年 5 月 15 日の欧州議会および閣僚理事会指令 2014/59/EU（OJ L 173、12.6.2014、p.190）

可能にするためのその他の必須要素は以下のとおりである。ICTサードパーティサービスプロバイダーが個人データのアクセシビリティ、可用性、完全性、セキュリティ及び保護をどのように確保するかを規定する契約条項、ICTサードパーティサービスプロバイダーの倒産、破綻または事業停止の場合におけるデータへのアクセス、復旧及び復元を可能にするための当該保証を規定する条項、並びに提供されるサービスに関連してICTインシデントの場合に追加費用なしまたは事前に決定された費用で協力することをICTサードパーティサービスプロバイダーに要求する条項、ICTサードパーティサービスプロバイダーが金融機関の所管当局及び破綻処理機構と十分に協力する義務に関する条項、また、所管当局及び破綻処理機構の期待に従って、契約上の取り決めの契約終了権及び関連する最低通知期間に関する条項。

(72) このような契約条項に加え、また、金融機関が自社のICTセキュリティを損なう可能性のあるサードパーティレベルで発生する全ての事態を完全に管理し続けることを確保する観点から、重要または重大な機能を支援するICTサービスの提供に関する契約では、以下についても規定すべきである。合意されたサービスレベルが遵守されていない場合に不当な遅滞なしに適切な是正措置をとることを可能にするために、正確な定量的及び定性的な成果目標を記載したサービスレベルの全内容を定めること、ICTサードパーティサービスプロバイダーが効果的にICTサービスを提供する能力に重大な影響を及ぼす可能性のある事態が発生した場合の当該ICTサードパーティサービスプロバイダーの通知期間及び報告義務、そして、ビジネスコンティンジェンシープランを実施・テストし、サービスの安全な提供を可能にするICTセキュリティ対策、ツール、ポリシーを有し、金融機関が実施するTLPTに参加し全面的に協力することをICTサードパーティサービスプロバイダーに対して求めること。

(73) また、重要または重大な機能をサポートするICTサービスの提供に関する契約には、金融機関または指定されたサードパーティによるアクセス、検査、及び監査を行う権利、及びコピーをとる権利を可能にする条項を含めるべきである。これらの権利は、サービスプロバイダーによる調査への全面的な協力と相まって、金融機関がICTサードパーティサービスプロバイダーのパフォーマンスを継続的に監視する際の重要なツールとなる。同様に、金融機関の所管当局は、秘密情報の保護を条件として、通知に基づき、ICTサードパーティサービスプロバイダーを調査し、監査する権利を有するべきである。

(74) このような契約上の取り決めは、特に、金融機関のレベルでの中断リスクを軽減するために、ICTサードパーティサービスプロバイダーが当該サービスの提供を継続する必要がある義務的な移行期間を可能にする、または、提供されるICTサービスの複雑さに応じて、金融機関が他のICTサードパーティサービスプロバイダーへの切り替えや社内ソリューションに切り替えることを認める専用の出口戦略も規定すべきである。さらに、指令2014/59/EUの適用範囲内にある金融機関は、ICTサービスに関する当該契約が強固で外因に影響をうけないものであり、金融機関が破綻になった場合に完全に執行可能であることを確保すべきである。したがって、これらの金融機関は、破綻処理機構の期待に応え、ICTサービスに関連する契約が破綻に対して耐性があるにすべきである。これらの金融機関は、支払義務を履行し続ける限り、ICTサービスに関連する契約に、再編または破綻を理由とする契約の終了、停止及び変更の禁止の条項が含まれるよう、他の要件とともに確保すべきで

ある。

(75) さらに、公的機関またはEU機関が策定した標準契約条項の自主的な利用、特に欧州委員会が策定したクラウドサービスに関する契約条項を自主的に使用することで、EUの金融サービス法が定める要件及び期待に完全に合致し、金融セクターにおけるクラウドサービスの利用に関する法的確実性のレベルを高めることにより、金融機関及びICTサードパーティサービスプロバイダーにさらなる安心感を与えることができる。標準契約条項の策定は、2018年のフィンテック行動計画で既に想定されている措置を土台としている。同計画では、委員会が金融セクターの関与に助けられて推進してきた、セクター横断的なクラウドサービスの利害関係者の取り組みを利用して、金融機関によるクラウドサービスのアウトソーシングの利用に関する標準契約条項の策定を奨励し、促進させたいという委員会の意向が発表された。

(76) 金融セクターにおけるICTサードパーティリスクへの対応において監督アプローチのコンバージェンスと効率性を促進するとともに、金融サービスの提供を支えるICTサービスの提供を重要なICTサードパーティサービスプロバイダーに依存する金融機関のデジタル・オペレーショナル・レジリエンスを強化し、それによってEUの金融システムの安定性と金融サービス域内市場の健全性の維持に資することを目的として、重要なICTサードパーティサービスプロバイダーはEUの監督フレームワークの対象となるべきである。監督フレームワークの設定は、EUレベルで措置を講じるという付加価値と、金融サービスの提供におけるICTサービス利用の固有の役割と特殊性によって正当化されるが、同時に、このソリューションは、特に金融セクターのデジタル・オペレーショナル・レジリエンスを扱う本規則の文脈においてのみ適切であると思われることも留意すべきである。しかし、このような監督フレームワークは、金融サービスや活動のその他の分野におけるEUの新たな監督モデルとみなされるべきではない。

(77) 監督フレームワークは重要なICTサードパーティサービスプロバイダーだけに適用されるべきである。したがって、金融セクターの当該ICTサードパーティサービスプロバイダーへの依存の側面と性質を考慮した指定メカニズムが必要である。同メカニズムには、監督フレームワークに含めるための基礎として、重要度パラメータを設定するための一連の定量的及び定性的基準が含まれるべきである。その判断の正確さを確保するため、ICTサードパーティサービスプロバイダーの企業構造にかかわらず、より広範なグループに属するICTサードパーティサービスプロバイダーの場合には、当該基準は、ICTサードパーティサービスプロバイダーの全体のグループ構造を考慮すべきである。一方で、当該基準の適用によって自動的に指定されない重要なICTサードパーティサービスプロバイダーは、自主的に監督フレームワークに参加できる可能性が与えられるべきであり、他方で、TFEU第127条（2）で言及されている欧州中央銀行制度の任務遂行を支える監視メカニズムのフレームワークの対象に既になっているICTサードパーティサービスプロバイダーは除外されるべきである。

(78) 同様に、本規則ではICTサードパーティサービスプロバイダーのカテゴリーに属しているが、他の金融機関にICTサービスを提供する金融機関も、関連するEU金融サービス法で構築された監督メカニズムの対象に既になっているため、監督フレームワークから除外されるべきである。該当する場合には、所管当局は、自局の監督活動において、ICTサービスを提供している金融機関によってもたらさ

れる金融機関へのICTリスクを考慮に入れるべきである。同様に、グループレベルでの既存のリスク監視メカニズムを理由として、主に自らのグループの事業体にサービスを提供するICTサードパーティサービスプロバイダーに対しても、同様の免除を導入すべきである。1加盟国のみで事業をしている金融機関に、同加盟国のみでICTサービスを提供しているICTサードパーティサービスプロバイダーについても、その活動が限定的であり、国境を越える影響がないことから、指定制度から除外すべきである。

(79) 金融サービスが経験したデジタルトランスフォーメーションによって、ICTサービスの利用と依存度がかつてない水準に達している。クラウドサービス、ソフトウェアソリューション、データ関連サービスを利用せずに金融サービスを提供することは考えられなくなったため、EUの金融エコシステムは、ICTサービスサプライヤーが提供する特定のICTサービスに本質的に共依存する構造となっている。これらのサービスプロバイダーの中には、ICTベースの技術の開発と応用におけるイノベーターとして、金融サービスの提供において重要な役割を果たす企業や、金融サービスのバリューチェーンに統合されるようになった企業もある。このように、EUの金融システムの安定性と健全性にとって不可欠な存在になっている。こうした重要なICTサードパーティサービスプロバイダーによって提供されるサービスへの依存の広まりは、様々な市場運営者の情報システムの相互依存と相まって、重要なICTサードパーティサービスプロバイダーが業務中断や重大なサイバーインシデントの影響を受けた場合、EUの金融サービスシステムと金融サービスの提供の継続性に直接的で潜在的に深刻なリスクをもたらす。サイバーインシデントは、金融セクターで監視される他の種類のリスクよりもかなり速いペースで金融システム全体に増殖し波及する独特な特性を有しており、セクター間や地理的境界を越えて拡大する可能性がある。サイバーインシデントは、金融システムが耐えられないレベル、または強力なショック吸収策を講じなければならないようなレベルに達し、実体経済を支える機能の混乱または多額の財務損失により金融システムへの信頼が損なわれるようなシステム危機に発展する可能性がある。このような事態が実際に起こり、それによってEUの金融の安定性と健全性が脅かされることを防ぐために、特に重要なICTサードパーティサービスプロバイダーに対するEUの監督を可能にする新たな規則を通じて、金融におけるICTサードパーティリスクに関する監督業務のコンバージェンスを図ることが不可欠である。

(80) 監督フレームワークは、金融サービスの提供に影響を及ぼすサービスを金融機関に提供する重要なICTサードパーティサービスプロバイダーと、主監督者との間の連携の度合いに大きく依存している。監督の成功は、とりわけ、重要なICTサードパーティサービスプロバイダーが用いる規則、管理策、及びプロセスを評価する主監督者の能力、またそれらの活動が金融の安定性及び金融システムの健全性に及ぼす潜在的な累積的影響を評価するための監視任務及び査察を効果的に実施する主監督者の能力にかかっている。同時に、重要なICTサードパーティサービスプロバイダーが主監督者の勧告に従い、その懸念事項に対処することが重要である。金融サービスの提供に影響を及ぼすサービスを提供する重要なICTサードパーティサービスプロバイダーが、例えば施設への立入りや情報提供の拒否のような協力が得られない場合、最終的には主監督者がICTサードパーティリスクを評価するための重要な手段を失うことになり、金融の安定性や金融システムの健全性に悪影響を及ぼす可能性があるため、相応の制裁措置も定める必要がある。

(81) このような背景から、重要なICTサードパーティサービスプロバイダーに本規則に定める透明性とアクセス関連の義務を遵守させるために主監督者が罰金を課す必要性は、第三国に設立された重要なICTサードパーティサービスプロバイダーに関連して罰金を課すことで生じる困難によって脅かされるべきではない。このような罰則の執行可能性を確保し、指定メカニズムと勧告の発行において、重要なICTサードパーティサービスプロバイダーの弁明権を速やかに確保できるようにするため、金融サービスの提供に影響を及ぼす金融機関にサービスを提供する重要なICTサードパーティサービスプロバイダーは、EU内で十分なビジネスプレゼンスを維持することが求められるべきである。監督の性質上、また、他の法管轄区域に同等の取り決めが存在しないため、第三国に設立された重要なICTサードパーティサービスプロバイダーとして認定された、システミックなICTサードパーティサービスのプロバイダーがもたらすデジタルオペレーショナルリスクによる影響の監視に関して、第三国の金融監督当局と効果的に協力することにより、この目的を確実に達成する適切な代替メカニズムは存在しない。したがって、EU域内の金融機関にICTサービスを提供し続けるために、第三国に設立され、本規則に従って重要と指定されたICTサードパーティサービスプロバイダーは、指定後12カ月以内に、EU法（Union *acquis*）で定義される子会社、すなわち欧州議会及び閣僚理事会指令2013/34/EU（[21]）で定義される子会社を設立することによって、EU域内での法人化を確実に実施するために必要な取り決めを全て行う必要がある。

(82) EU域内での子会社の設立という要件が、重要なICTサードパーティサービスプロバイダーがEU域外に所在する施設及びインフラからICTサービス及び関連技術支援を提供することを妨げるものであってはならない。本規則は、EU域内でのデータの保管または処理を求めていないため、データローカライゼーションの義務を課していない。

(83) 重要なICTサードパーティサービスプロバイダーは、必ずしもEU域内の施設からのみでなく、世界のどこからでもICTサービスを提供できるべきである。監督活動は、まずは連合に所在する事業所で実施されるべきであり、本規則に従って重要なICTサードパーティサービスプロバイダーによって設立された子会社を含め、連合内に所在する事業体とのやり取りを通じて行われるべきである。しかしながら、EU域内でのそのような措置では、主監督者が本規則に基づいて自身の職務を完全かつ効果的に履行するには不十分かもしれない。したがって、主監督者は、第三国においても関連する監視権限を行使できるようにする必要がある。第三国においてこうした権限を行使することにより、主監督者は、重要なICTサードパーティサービスプロバイダーがICTサービスまたは技術支援サービスを実際に提供または管理している施設を調査できるようになり、主監督者が重要なICTサードパーティサービスプロバイダーのICTリスク管理について包括的かつ実務的な理解を得ることができる必要がある。主監督者がEU機関として、EUのテリトリー外で権限を行使する可能性は、関連する条件、特に関係する重要なICTサードパーティサービスプロバイダーの同意を得て適切に決められるべきである。同様に、第三国の関係当局は、主監督者の活動が自国の領域内で実施されることについて通知されるべきであり、異議を唱えないことが求められる。しかしながら、効率的な実施を確保するために、また、EU機関及び加盟国のそれぞれの権限を侵害することなく、当該権限

[21] 欧州議会および閣僚理事会指令 2006/43/EC を改正し、閣僚理事会指令 78/660/EEC および 83/349/EEC を廃止する、特定種類の企業の年次財務諸表、連結財務諸表および関連報告書に関する 2013 年 6 月 26 日の欧州議会および閣僚理事会指令 2013/34/EU（OJ L 182、29.6.2013、p.19）

が、関係する第三国の関係当局との行政協力協定の締結にも完全に根差している必要がある。したがって、本規則は、ESAが第三国の関係当局と行政協力協定を締結することを可能にするものであり、EU及びその加盟国に関して法的義務を課すものであってはならない。

(84) 主監督者とのコミュニケーションを円滑にし、十分な代表性を確保するために、グループの一員である重要なICTサードパーティサービスプロバイダーは、調整窓口として一法人を指定すべきである。

(85) 監督フレームワークは、本規則の下で重要と指定されていないが、国家レベルで重要とみなされているICTサードパーティサービスプロバイダーに関して各加盟国が監督職務または監視職務を行う権限を損なわないものであるべきである。

(86) 金融サービス分野における多層的な制度構造を活用するため、ESA合同委員会は、サイバーセキュリティに関する任務に基づき、ICTリスクに関連する全ての事項に関して、全体的にセクター横断的な連携を引き続き確保するべきである。同委員会は、重要なICTサードパーティサービスプロバイダーに対する個別の決定の準備作業及び、特に、重要なICTサードパーティサービスプロバイダーに対する監視プログラムのベンチマーキング及びICT集中リスク問題に対処するためのベストプラクティスの特定に関する集合的な推奨事項の発行の準備作業を行う新たな小委員会（監督フォーラム）によって支援されるべきである。

(87) 重要なICTサードパーティサービスプロバイダーがEUレベルで適切かつ効果的に確実に監督されるようにするため、本規則は、3つのESAのいずれかを主監督者として指定することができると定めている。重要なICTサードパーティサービスプロバイダーを3つのESAのいずれかに個別に割り当てる際には、当該ESAが管轄する金融セクターで事業を展開する金融機関の優位性を評価し、その上で決定すべきである。このアプローチにより、監督機能を遂行するという観点から、3つのESA間の業務と責任のバランスのとれた配分が実現し、3つのESAそれぞれで利用可能な人的資源と技術的専門知識を最大限に活用することにつながるべきである。

(88) 主監督者は、調査を実施し、重要なICTサードパーティサービスプロバイダーの施設及び拠点において現場査察及びオフサイト査察を実施し、完全かつ最新の情報を入手するのに必要な権限が与えられるべきである。これらの権限により、主監督者は、金融機関、ひいてはEUの金融システムに与えるICTサードパーティリスクの種類、規模、影響について実質的な洞察を得ることができるようになるべきである。ESAに主監督の役割を委託することは、金融におけるICTリスクの組織的側面を理解し、対処するための前提条件である。重要なICTサードパーティサービスプロバイダーがEUの金融セクターに与える影響とICT集中リスクによって引き起こされる潜在的な問題に対処するには、EUレベルでの共同アプローチが求められる。多数の所管当局が、ほとんどまたは全く連携を取らずに複数の監査とアクセス権を同時に実施すれば、金融監督当局がEU域内のICTサードパーティリスクについて完全かつ包括的な概要を取得することの妨げになるだけでなく、重要なICTサードパーティサービスプロバイダーが多数の監視調査の要請を受けた場合、そのプロバイダーにおいて冗長性、負担、複雑性が生じることになる。

(89) 重要と指定されることの重大な影響を踏まえ、本規則は、監督フレームワークの実施の全期間、重要なICTサードパーティサービスプロバイダーの権利が尊重されることを確保すべきである。当該プロバイダーは、重要と指定される前に、例えば、指定に関する評価を目的として、一切の関連情報を含む陳述書を主監督者に提出する権利を有するべきである。主監督者は、ICTリスク問題に関する勧告及びそれに対する適切な救済策を提出する権限（金融機関または金融システムの安定に最終的には影響を与える特定の契約上の取り決めに反対する権限を含む）を与えられるべきであるため、重要なICTサードパーティサービスプロバイダーには、これらの勧告が最終決定される前に、勧告で想定される解決策が本規則の適用範囲外の事業体である顧客に与えると予想される影響に関する説明を行い、リスクを軽減するための解決策を策定する機会を与えられるべきである。勧告に同意しない重要なICTサードパーティサービスプロバイダーは、勧告を支持しない意向について理由を付した説明を提出すべきである。その理由を付した説明が提出されない場合または不十分とみなされる場合、主監督者は、不遵守である本件を要約した公告を発出すべきである。

(90) 所管当局は、金融機関の健全性監督に関する機能に、主監督者が発行した勧告に対する実質遵守を検証する業務を正式に含めるべきである。所管当局は、主監督者の勧告で特定されたリスクに対処するための追加的な措置を講じるよう金融機関に求めることができるべきであり、しかるべき時期にその旨の通知を発行すべきである。主監督者が指令（EU）2022/2555に基づいて監督されている重要なICTサードパーティサービスプロバイダーに対して勧告を行った場合、所管当局は、当該重要なICTサードパーティサービスプロバイダーへの対応において連携の取れたアプローチを促すために、自主的に、追加的措置を採択する前に、当該指令に基づき所管当局と協議できるようにするべきである。

(91) 監督の実施は、次の3つの運用原則を指針とするべきである。同原則は以下の確保を目指している。（a）共同監督ネットワーク（JON）を通じた、ESAの主監督者としての役割における緊密な連携、（b）指令（EU）2022/2555によって確立された枠組みとの一貫性（重要なICTサードパーティサービスプロバイダーに対する措置の重複を避けるため、当該指令の下に設置された機関との自主的な協議を通じて）重要なICT、（c）重要なICTサードパーティサービスプロバイダーが本規則の適用範囲外の事業体である顧客に提供するサービスが中断されるという潜在的リスクを最小限に抑えるための努力が払われること。

(92) 監督フレームワークは、重要なICTサードパーティサービスプロバイダーとの契約上の取り決めを継続的に監視する義務を含め、金融機関がICTサードパーティサービスプロバイダーの利用に伴うリスクを自ら管理するという要件に代わるものではなく、いかなる形であれ、いかなる部分においても取って代わるべきではない。同様に、監督フレームワークは、本規則及び関連する金融サービス法に定められた全ての法的義務を遵守し、果たす金融機関の完全な責任に影響を与えるべきではない。

(93) 重複や二重を避けるために、所管当局は、重要なICTサードパーティサービスプロバイダーのリスクを監視することを目的とした措置を個別に取ることを一切控えるべきであり、この点に関しては、関連する主監督者の評価に依拠すべきである。監督フレームワークにおける任務の遂行に関して、いかなる措置も、いかなる場合にも、主監督者と事前に連携し、合意を得るべきである。

(94) ICTサードパーティサービスプロバイダーのデジタルリスク管理のレビュー及び監視のベストプラクティスの利用に関し、国際レベルでの収束を促すために、ESAは第三国の関連する監督当局及び規制当局と協力協定の締結が奨励されるべきである。

(95) 所管当局、3つのESA、及び任意で指令（EU）2022/2555に基づく所管当局内において、運用リスク及びICTリスクを専門とするスタッフの特定の能力、技術スキル、専門知識を活用するために、主監督者は、国の監督能力と知識を活用し、一般調査及び重要なICTサードパーティサービスプロバイダーの調査を含む監督業務の準備や遂行をサポートするために、またそれに対する必要なフォローアップを行うために、多分野にわたるチームをプールし、重要なICTサードパーティサービスプロバイダーごとに専門調査チームを設置すべきである。

(96) 監視業務から発生する費用は、重要なICTサードパーティサービスプロバイダーに課される手数料で全額賄われるが、ESAは、監督フレームワークの開始前に、専用のICTシステムを事前に開発・導入する必要があるため、今後の監視をサポートする専用ICTシステムの導入費用が発生する可能性がある。したがって、本規則は、監督フレームワーク自体は全額手数で賄われる一方で、ESAのICTシステムの開発費用はEUと各国の所管当局の拠出金から賄われるという、ハイブリッド型の資金調達モデルを規定している。

(97) 所管当局は、本規則に基づく職務を確実に遂行するために必要な全ての監督、調査及び制裁の権限を有するべきである。原則として、所管当局が課す行政処分に関する通知を公表すべきである。金融機関及びICTサードパーティサービスプロバイダーは、別々の加盟国に設立され、別々の所管当局によって監督される可能性があるため、本規則の適用は、一方では、理事会規則（EU）No 1024/2013によってECBが与えられた特定の任務を含む所管当局間の緊密な協力によって促進されるべきであり、他方では、関連する監督業務において、相互の情報交換及び支援の提供を通じたESAとの協議によって促進されるべきである。

(98) ICTサードパーティサービスプロバイダーを重要と指定する基準を定量化・定性化するため、また監督手数料を整合化するために、TFEU第290条に従って法令を採択する権限を欧州委員会に委任し、ICTサードパーティサービスプロバイダーの障害または業務停止がICTサービスを提供する金融機関に与えうるシステムへの影響、当該ICTサードパーティサービス事業者に依存するグローバルなシステム上重要な機関（G-SIIs）またはその他のシステム上重要な機関（O-SIIs）の数、ある特定の市場で活動しているICTサードパーティサービスプロバイダーの数、データとICTワークロードを他のICTサードパーティサービスプロバイダーに移行するコスト、並びに監視手数料の額とその支払い方法をさらに規定することによって、本規則を補足すべきである。特に、委員会が準備作業を行う際には、専門家レベルも含めて適切な協議を実施し、その協議が2016年4月13日付「より良い法制定に関する機関間合意」の原則に従って行われることが重要である[22]。さらに、委任法令の作成への平等な参加を確保するために、欧州議会及び閣僚理事会は、加盟国の専門家と同時に全ての文書を受領すべきであり、また、それらの専門家は、委任法令の作成を扱う欧州委員会の専門家グループの会合に

[22] OJ L 123、12.5.2016、p.1

体系的に参加できるようにするべきである。

(99) 規制技術基準は、本規則に定められた要件の一貫した整合化を確保すべきである。高度に専門的な専門知識を有する機関としての役割において、ESAは、政策決定を伴わない規制技術基準案を作成し、欧州委員会に提出すべきである。規制技術基準は、ICTリスク管理、主要なICT関連インシデント報告、テストの分野において、並びにICTサードパーティリスクの健全な監視に関する主要な要件に関連して策定されるべきである。欧州委員会及びESAは、これらの基準及び要件が、全ての金融機関において、各機関の規模と全体的なリスクプロファイル、並びにサービス、活動、業務の性質、規模、複雑さに委任法令により比例した形で適用できることを確保すべきである。欧州委員会は、TFEU第290条に従った委任法令によって、また規則（EU）No 1093/2010、（EU）No 1094/2010及び（EU）No 1095/2010の第10条から第14条に従って、これらの規制技術基準を採択する権限が与えられるべきである。

(100) 主要なICT関連インシデントや主要な運用上またはセキュリティ上の決済関連インシデントに関する報告書の比較を容易にし、ICTサードパーティサービスプロバイダーが提供するICTサービスの利用に関する契約上の取り決めについて透明性を確保するために、ESAは、金融機関が主要なICT関連インシデントや主要な運用上またはセキュリティ上の決済関連インシデントを報告するための標準化されたテンプレート、フォーム及び手順、並びに情報登録のための標準化されたテンプレートを確立する実施技術基準案を策定すべきである。これらの基準を策定する際、ESAは、金融機関の規模及び全体的なリスクプロファイル、並びにそのサービス、活動及び業務の性質、規模及び複雑性を考慮に入れるべきである。欧州委員会は、TFEU第291条に従った実施法令により、並びに規則（EU）No 1093/2010、(EU) No 1094/2010及び（EU）No 1095/2010の第15条に従って、実施技術基準を採択する権限を与えられるべきである。

(101) さらなる要件は、欧州議会及び閣僚理事会規則（EC）No 1060/2009（[23]）、（EU）No 648/2012（[24]）、（EU）No 600/2014（[25]）及び（EU）No 909/2014（[26]）の技術規制基準及び実施技術基準に基づく委任法令及び実施法令によって既に規定されているため、ESAが個別にまたは合同委員会を通じて共同で、規制及び実施技術基準を委員会に提出し、既存のICTリスク管理規則を継承・更新する委任法令及び実施法令を採択させることが適切である。

(102) 本規則は、欧州議会及び閣僚理事会指令 (EU) 2022/2556 ([27]) と共に、規則 (EU) No 1060/2009、

---

[23] 信用格付機関に関する 2009 年 9 月 16 日の欧州議会および閣僚理事会規則（EC）No 1060/2009（OJ L 302、17.11.2009、p.1）

[24] OTC デリバティブ、中央清算機関、および取引情報蓄積機関に関する 2012 年 7 月 4 日の欧州議会および閣僚理事会規則（EU）No 648/2012（OJ L 201、27.7.2012、p.1）

[25] 規則（EU）No 648/2012 を改正する、金融商品市場に関する 2014 年 5 月 15 日の欧州議会および閣僚理事会規則（EU）No 600/2014（OJ L 173、12.6.2014、p.84）

[26] 指令 98/26/EC および 2014/65/EU ならびに規則（EU）No 236/2012 を改正する、欧州連合および証券集中保管機関における証券決済の改善に関する 2014 年 7 月 23 日の欧州議会および閣僚理事会規則（EU）No 909/2014（OJ L 257、28.8.2014、p.1）

[27] 金融セクターのデジタル・オペレーショナル・レジリエンスに関する指令 2009/65/EC、2009/138/EC、2011/61/EU、2013/36/EU、

（EU）No 648/2012、（EU）No 600/2014及び（EU）No 909/2014、並びに（EU）2016/1011（[28]）を含む、連合の金融サービスに関する複数の規則及び指定にわたるICTリスク管理条項の統合を伴うものであるため完全な一貫性を確保するために、これらの規則を改正して、適用ICTリスク関連条項が本規則に定められていることを明確にする必要がある。

(103) したがって、規則（EU）No 1060/2009、規則（EU）No 648/2012、規則（EU）No 600/2014、規則（EU）No 909/2014及び規則（EU）2016/1011に定められていた権限付与が委任法令及び実施法令の採択を義務づけていたオペレーショナルリスク関連条項の範囲は、現在こうした規則の一部となっているデジタル・オペレーショナル・レジリエンスの面に関する全ての条項を本規則に引き継ぐという観点から絞り込まれるべきである。

(104) 決済システムの運用及び決済処理業務の提供を可能にするICTインフラの利用に関連する潜在的なシステミックサイバーリスクは、整合性の取れたデジタル・レジリエンス規則によってEUレベルで適切に対処されるべきである。このため、欧州委員会は、本規則の適用範囲の見直しの必要性を迅速に評価し、その見直しを指令（EU）2015/2366の下で想定されている包括的見直しの結果と合致するようにすべきである。過去10年間に起きた数多くの大規模攻撃は、決済システムがいかにサイバー脅威にさらされているかを示している。決済システムと決済処理業務は、決済サービスチェーンの中核に位置し、金融システム全体との強力な相互接続性を示しており、そのため、EU金融市場の機能にとって重要な意味を獲得した。このようなシステムに対するサイバー攻撃は、決済の円滑化など、主要な経済機能に直接的な影響を及ぼすとともに、関連する経済プロセスに間接的な影響を及ぼすなど、事業に運営上の深刻な混乱を引き起こす可能性がある。制度の統一並びに決済システム運営会社及び処理会社の監督がEUレベルで導入されるまで、加盟国は、同様の市場プラクティスを適用する観点から、自国の管轄区域下で監督されている決算システム運営会社及び処理会社に規則を適用する際、本規則に定めるデジタル・オペレーショナル・レジリエンスの要件を参考にすることができる。

(105) 本規則の目的、すなわち、規制対象の金融機関に関して高水準のデジタル・オペレーショナル・レジリエンスを実現することは、EU域内の様々な規則及び各国の法令の整合化が求められるため、加盟国だけでは十分に達成できないが、その規模と影響を考慮すると、むしろEUレベルの方がより適切に実現することができるため、EUは欧州連合条約第5条に規定された補完性原則に従って措置を取ることができる。同条に規定された比例性原則に従って、本規則は、当該目的を達成するのに必要な範囲を超えない。

(106) 欧州データ保護監督官は、欧州議会及び閣僚理事会規則（EU）2018/1725（[29]）の第42条（1）に

---

[28] 指令 2008/48/EC および 2014/17/EU ならびに規則（EU）No 596/2014 を改正する、金融商品および金融契約のベンチマークとして、または投資ファンドのパフォーマンスの測定のために使用される指数に関する 2016 年 6 月 8 日の欧州議会および閣僚理事会規則（EU）2016/1011（OJ L 171、29.6.2016、p.1）

[29] 規則（EC）No 45/2001 および決定 No 1247/2002/EC を廃止する、EU 機関、組織、独立部局および専門行政機関による個人データの取り扱いに係る自然人の保護ならびに当該データの自由な移動に関する 2018 年 10 月 23 日の欧州議会及び閣僚理事会規則（EU）2018/1725（OJ L 295、21.11.2018、p.39）

従って協議を受け、2021年5月10日（[30]）に意見書を提出した。

[30] OJ C 229、15.6.2021、p. 16

（仮訳）

第 1 章

総則

第 1 条

主題

1. 規則は、デジタル・オペレーショナル・レジリエンスの高い共通水準を達成するため、金融機関のビジネスプロセスを支援するネットワーク及び情報システムのセキュリティに関する統一要件を以下のように定めている。

(a) 次の事項に関する金融機関に適用される要件

(i) 情報通信技術（ICT）リスク管理

(ii) 重大なICT関連のインシデントの報告、及び重大なサイバー脅威に関する所轄当局への自主的な通知

(iii) 第2条第1項（a）～（d）に規定される金融機関が所管当局に対して行う、運用又は証券決済に関連するインシデントの報告

(iv) デジタル・オペレーショナル・レジリエンステスト

(v) サイバー脅威と脆弱性に関する情報及びインテリジェンスの共有

(vi) ICTサードパーティリスクの堅牢な管理のための措置

(b) ICTサードパーティサービスプロバイダーと金融機関との間で締結される契約上の取り決めに関する要件

(c) 金融機関にサービスを提供する際の重要なICTサードパーティサービスプロバイダーの監督枠組みの設立及び運営に関する規則

(d) 所管当局間の協力に関する規則、及び本規則の対象となる全ての事項に関連して所管当局が行う監督及び執行に関する規則

2. 指令（EU）2022/2555第3条が適用された国内法に従って、不可欠又は重要な事業体として特定された金融事業体に関連し、本規則は当該指令第4条の目的上、分野別EU法とみなされる。

3. 本規則は、EU法に基づく公衆の安全、防衛及び国家安全保障に関わる重要な国家機能に関する加盟国

（仮訳）

の責任を妨げない。

（仮訳）

第 2 条

範囲

1. 本規則は、第3項及び第4項を妨げることなく以下の事業体に適用される。

信用機関

(a) 決済機関(指令（EU）2015/2366に従って除外される決済機関を含む)

(b) 口座情報サービスプロバイダー

(c) 電子マネー事業者(指令2009/110/ECに従って除外される電子マネー事業者を含む)

(d) 投資会社

(e) 暗号資産市場、及び規則（EU）No 1093/2010並びに（EU）No 1095/2010、指令2013/36/EU並びに（EU）2019/1937（「暗号資産市場規制」）の改正に関する欧州議会及び閣僚理事会規則に基づいて認可された暗号資産サービスプロバイダー、及びアセット参照型トークンの発行者

(f) 証券集中保管機関

(g) 中央清算機関

(h) 取引所

(i) 取引情報蓄積機関

(j) オルタナティブ投資ファンド運用者

(k) 運用会社

(l) データ報告サービスプロバイダー

(m) 保険及び再保険事業者

(n) 保険仲介業者、再保険仲介業者、及び付帯保険仲介業者

(o) 年金基金

(p) 信用格付機関

(q) クリティカルベンチマークの管理者

(r) クラウドファンディングサービスプロバイダー

(s) 証券化情報蓄積機関

(t) ICTサードパーティサービスプロバイダー

2. 本規則の目的上、第1項（a）～（t）に規定される事業体は、「金融機関」と総称するものとする。

3. 本規則は以下には適用されない。

(a) 指令2011/61/EU第3条第2項が定めるオルタナティブ投資ファンド運用者

(b) 指令2009/138/EC第4条が定める保険及び再保険事業者

(c) 合計加入者数が15人以下の年金制度を運営する職域年金基金

(d) 指令2014/65/EU第2条及び第3条に従って除外される自然人又は法人

(e) 小規模事業者又は中小企業である保険仲介業者、再保険仲介業者、及び付帯保険仲介業者

(f) 指令2013/36/EU第2条第5項(3)が定める郵便振替取扱機関

4. 加盟国は、それぞれの領土内に所在する指令2013/36/EU第2条第5項（4）～（23）が定める事業体を本規則の適用範囲から除外することができる。加盟国がかかるオプションを利用する場合、その旨及びその後の変更を欧州委員会に通知するものとする。欧州委員会は、その情報を欧州委員会のウェブサイト又はその他の容易にアクセス可能な手段で公衆への利用を可能とするものとする。

（仮訳）

第 3 条

定義

本規則の目的上、以下の定義が適用される。

(1) 「デジタル・オペレーショナル・レジリエンス」とは、業務の完全性及び信頼性を構築し、保証し、及びレビューする金融機関の能力を指し、ICTサードパーティサービスプロバイダーが提供するサービスの利用を通じて、金融機関が使用するネットワーク及び情報システムの安全性に対処するため、かつ金融サービス及びその品質の継続的な提供を支援するために必要なあらゆるICT関連の能力を直接的、又は間接的に確保することによって確保できるものを指す。

(2) 「ネットワーク及び情報システム」とは、指令（EU）2022/2555第6条（1）に定義されたネットワーク及び情報システムを指す。

(3) 「レガシーなICTシステム」とは、ライフサイクルの終了（EOL）に達したICTシステムであって、技術的又は商業的な理由からアップグレード又は修理に適さないICTシステム、或いはサプライヤー又はICTサードパーティサービスプロバイダーによる支援が終了した後も使用されており、金融機関の機能を支えているICTシステムを指す。

(4) 「ネットワーク及び情報システムのセキュリティ」とは、指令（EU）2022/2555第6条（2）に定義されたネットワーク及び情報システムのセキュリティを指す。

(5) 「ICTリスク」とは、ネットワーク及び情報システムの使用に関連して合理的に識別可能な状況であって、実際に発生した場合に、デジタル環境又は物理的環境に悪影響を及ぼすことによって、ネットワーク及び情報システム、技術に依存するツール又はプロセス、運用及びプロセス、或いはサービス提供の安全性を損なうおそれのあるものを指す。

(6) 「情報資産」とは、有形無形を問わず、保護する価値のある情報の集合体を指す。

(7) 「ICT資産」とは、金融機関が使用するネットワーク及び情報システムにおけるソフトウェア又はハードウェア資産を指す。

(8) 「ICT関連のインシデント」とは、ネットワーク及び情報システムのセキュリティを侵害し、データの可用性、真正性、完全性若しくは機密性、又は金融機関が提供するサービスに悪影響を及ぼす、金融機関が想定していない単独の事象又は一連の関連する事象を指す。

(9) 「運用又は証券決済に関連するインシデント」とは、第2条第1項（a）～（d）までに規定される金融機関によって計画されていない単一の、又は一連の関連事象であって、ICT関連であるか否かを問わず、決済関連データの可用性、真正性、完全性若しくは機密性、又は当該金融機関が提供する決済関連サービスに悪影響を及ぼす事象を指す。

(10)「重大なICT関連のインシデント」とは、金融機関の重要または重大な機能を支えるネットワーク及び情報システムに大きな悪影響を及ぼすICT関連のインシデントを指す。

(11)「運用又は証券決済に関連する重大なインシデント」とは、提供される決済関連サービスに大きな悪影響を及ぼす運用又は証券決済に関連するインシデントを指す。

(12)「サイバー脅威」とは、規則（EU）2019/881第2条（8）に定義された「サイバー脅威」を指す。

(13)「重大なサイバー脅威」とは、重大なICT関連のインシデント、又は運用又は証券決済に関連する重大なインシデントを引き起こす可能性があることを示す技術的特性を持つサイバー脅威を指す。

(14)「サイバー攻撃」とは、脅威アクターによる資産の破壊、暴露、改ざん、無効化、窃取若しくは認可されていないアクセス若しくは使用の試みによって引き起こされる、悪意のあるICT関連のインシデントを指す。

(15)「脅威インテリジェンス」とは、意思決定に必要な文脈を提供し、またICT関連のインシデント又はサイバー脅威の影響を緩和するために適切かつ十分に把握できるようにするために、集約、変換、分析、解釈又は強化された情報を指す。この情報には、サイバー攻撃の技術的詳細、その攻撃の実行者と手口、および動機が含まれる。

(16)「脆弱性」とは、資産、システム、プロセス又は制御の弱点、脆弱性或いは欠陥であって、悪用されるおそれがあるものを指す。

(17)「脅威ベースのペネトレーションテスト（TLPT）」とは、実際のサイバー脅威をもたらすとされる現実の脅威アクターの戦術、手法、及び手順を模倣したフレームワークを指す。この枠組みでは、金融機関の重要な稼働中システムに対して、統制され、組織別に調整されたインテリジェンス主導（レッドチーム）のテストが実施される。

(18)「ICTサードパーティリスク」とは、アウトソーシングの取り決めを通じたものを含め、ICTサードパーティサービスプロバイダー又はその下請業者によって提供されるICTサービスの利用に関連して金融機関に発生する可能性のあるICTリスクを指す。

(19)「ICTサードパーティサービスプロバイダー」とは、ICTサービスを提供する事業者を指す。

(20)「ICTグループ内サービスプロバイダー」とは、金融グループの一部であり、かつ、同一グループ内の金融機関又は同一の機関保護スキームに属する金融機関（親事業者、子会社、支店、又は共通の所有若しくは支配下にあるその他の事業体を含む）に対して、主としてICTサービスを提供する事業体を指す。

(21)「ICTサービス」とは、ICTシステムを通じて1つ以上の内部又は外部の利用者に継続的に提供され

るデジタルサービス及びデータサービスを指し、ハードウェアアズアサービス、及びハードウェアプロバイダーによるソフトウェア又はファームウェアの更新による技術支援の提供を含む。ただし、従来のアナログ電話サービスを除く。

(22)「重要または重大な機能」とは、中断すると金融機関の財務実績、又はそのサービスや活動の健全性若しくは継続性が著しく損なわれるおそれがある機能、又はその機能の中断、欠陥又は履行不能によって、金融機関が認可の条件及び義務、或いは適用される金融サービス法に基づくその他の義務を継続的に遵守することが著しく困難になる可能性がある機能を指す。

(23)「重要なICTサードパーティサービスプロバイダー」とは、第31条に従って重要であると指定されたICTサードパーティサービスプロバイダーを指す。

(24)「第三国に設立されたICTサードパーティサービスプロバイダー」とは、第三国に設立された法人であって、金融機関との間でICTサービスの提供に関する契約を締結しているICTサードパーティサービスプロバイダーを指す。

(25)「子会社」とは、指令2013/34/EU第2条（10）及び第22条で規定された意味の範囲内における子会社事業を指す。

(26)「グループ」とは、指令2013/34/EU第2条（11）に定義されたグループを指す。

(27)「親事業者」とは、指令2013/34/EU第2条（9）及び第22条に規定された意味の範囲内における親事業者を指す。

(28)「第三国に設立されたICT下請事業者」とは、第三国に設立された法人であって、ICTサードパーティサービスプロバイダー、又は第三国に設立されたICTサードパーティサービスプロバイダーとの間で契約を締結しているICT下請事業者を指す。

(29)「ICT集中リスク」とは、関連する個別又は複数の重要なICTサードパーティサービスプロバイダーに対するエクスポージャーであって、当該プロバイダーに依存した結果、当該プロバイダーのサービス利用不可、破綻、或いはその他収益の未達によって重要または重大な機能を提供する金融機関の能力が脅かされる可能性や、金融機関が多額の損失を含む異なる種類の悪影響を被る可能性、又はEU全体の金融の安定性が脅かされる可能性を指す。

(30)「経営陣」とは、指令2014/65/EU第4条第1項（36）、指令2013/36/EU第3条第1項（7）、欧州議会及び閣僚理事会指令2009/65/EC第2条第1項（S）（[31]）、規則（EU）No 909/2014第2条第1項（45）、規則（EU）2016/1011第3条第1項（20）、及び暗号資産市場規則の関連条項に定義される経営機関、又は関連するEU法若しくは国内法に従って事業体を実質的に運営する、若しくは主要な

---

31 譲渡有価証券 (UCITS) への集団投資を行う企業に係る法律、規則及び行政規定の調整に関する 2009 年 7 月 13 日付欧州議会及び閣僚理事会指令 2009/65/EC (OJ L 302, 17.11.2009, p. 32)。

機能を有する同等の自然人を指す。

(31)「信用機関」とは、欧州議会及び閣僚理事会規則（EU）No 575/2013第4条第1項（1）（[32]）に定義された信用機関を指す。

(32)「指令2013/36/EUに従って除外される機関」とは、指令2013/36/EU第2条第5項（4）～（23）に規定される事業体を指す。

(33)「投資会社」とは、指令2014/65/EU第4条第1項（1）に定義された投資会社を指す。

(34)「小規模非連結投資会社」とは、欧州議会及び閣僚理事会規則（EU）2019/2033第12条第1項[33]に定める条件を満たす投資会社を指す。

(35)「決済機関」とは、指令（EU）2015/2366第4条（4）に定義された支払機関を指す。

(36)「指令（EU）2015/2366に従って除外される決済機関」とは、指令（EU）2015/2366第32条第1項に従って除外される支払機関を指す。

(37)「口座情報サービスプロバイダー」とは、指令（EU）2015/2366第33条第1項に規定される口座情報サービスプロバイダーを指す。

(38)「電子マネー事業者」とは、欧州議会及び閣僚理事会指令2009/110/EC第2条（1）に定義された電子マネー事業者を指す。

(39)「指令2009/110/ECに従って除外される電子マネー事業者」とは、指令2009/110/EC第9条第1項に記載された権利放棄の恩恵を受ける電子マネー事業者を指す。

(40)「清算機関」とは、規則（EU）No 648/2012第2条（1）に定義された中央清算機関を指す。

(41)「取引情報蓄積機関」とは、規則（EU）No 648/2012第2条（2）に定義された取引情報蓄積機関を指す。

(42)「証券集中保管機関」とは、規則（EU）No 909/2014第2条第1項（1）に定義された証券集中保管機関を指す。

(43)「取引所」とは、指令2014/65/EU第4条第1項（24）に定義された取引所を指す。

---

[32] 信用機関の健全性要件及び規則 (EU) No 648/2012 の改正に関する 2013 年 6 月 26 日付欧州議会及び閣僚理事会規則 (EU) No 575/2013 (OJ L 176, 27.6.2013, p. 1)。

[33] 投資会社の健全性要件及び規則（EU）No 1093/2010、（EU）No 575/2013、（EU）No 600/2014 の改正に関する 2019 年 11 月 27 日付欧州議会及び閣僚理事会規則欧州議会及び閣僚理事会規則(EU) 2019/2033 (OJ L 314, 5.12.2019, p. 1)。

(44)「オルタナティブ投資ファンド運用者」とは、指令規則2011/61/EU第4条第1項（b）に定義されたオルタナティブ投資ファンド運用者を指す。

(45)　「管理会社」とは、指令2009/65/EC第2条第1項（b）に定義された管理会社を指す。

(46)「データ報告サービスプロバイダー」とは、規則（EU）No 600/2014第2条第1項（34）～（36）が定める意味の範囲内におけるデータ報告サービスプロバイダーを指す。

(47)「保険事業者」とは、指令2009/138/EC第13条（1）に定義された保険事業者を指す。

(48)「再保険事業者」とは、指令2009/138/EC第13条（4）に定義された再保険事業者を指す。

(49)「保険仲介業者」とは、指令（EU）欧州議会及び閣僚理事会指令（EU）2016/97第2条第1項（3）[34]に定義された保険仲介業者を指す。

(50)「付帯保険仲介業者」とは、指令（EU）2016/97第2条第1項（4）に定義する付帯保険仲介業者を指す。

(51)「再保険仲介業者」とは、指令（EU）2016/97第2条第1項（5）に定義された再保険仲介業者を指す。

(52)「年金基金」とは、指令（EU）2016/2341第6条（1）に定義する職域年金基金を指す。

(53)「小規模年金基金」とは、合計加入者数が100人未満の年金制度を運営する職域年金基金を指す。

(54)「信用格付機関」とは、規則（EC）No 1060/2009第3条第1項（b）に定義された信用格付機関を指す。

(55)「暗号資産サービスプロバイダー」とは、暗号資産市場規則の関連規定に定義される暗号資産サービスプロバイダーを指す。

(56)「アセットトークン発行者」とは、暗号資産市場規則の関連条項に定義されるアセット参照型トークンの発行者を指す。

(57)「クリティカルベンチマークの管理者」とは、規則（EU）2016/1011第3条第1項（25）に定義された「クリティカルベンチマーク」の管理者を指す。

(58)「クラウドファンディングサービスプロバイダー」とは、欧州議会及び閣僚理事会規則（EU）

---

[34] 保険の流通に関する 2016 年 1 月 20 日付欧州議会及び閣僚理事会指令（EU）2016/97 (OJ L 26, 2.2.2016, p. 19)。

2020/1503第2条第1項（e）[35]に定義するクラウドファンディングサービスプロバイダーを指す。

(59)「証券化情報蓄積機関」とは、欧州議会及び閣僚理事会規則（EU）2017/2402第2条（23）（[36]）に定義された証券化情報蓄積機関を指す。

(60)「小規模事業者」とは、雇用する従業員数が10人未満であり、年間売上高及び／又は年間総資産が200万ユーロを超えない金融事業体であって、取引所、清算機関（CCP）、取引情報蓄積機関又は証券集中保管機関以外のものを指す。

(61)「主監督者」とは、本規則第31条第1項(b)に従って任命された欧州監督機構（ESA）を指す。

(62)「合同委員会」とは、規則（EU）No 1093/2010、（EU）No 1094/2010及び（EU）No 1095/2010の第54条に規定される委員会を指す。

(63)「小規模事業者」とは、雇用する従業員数が10人以上50人未満であり、年間売上高及び／又は年間総資産が200万ユーロ超1,000万ユーロ以下の金融機関を指す。

(64)「中規模事業者」とは、雇用する従業員数が250人未満であり、年間売上高が5000万ユーロ以下及び／又は年間総資産が4,300万ユーロ以下の、小規模事業者ではない金融機関を指す。

(65)「公共機関」とは、政府、又は中央銀行を含むその他の行政機関を指す。

---

35 ビジネス向けのクラウドファンディングサービスプロバイダー及び規則 (EU) 2017/1129 並びに指令 (EU) 2019/193 7 (OJ L 347, 20.10.2020, p. 1)の改正に関する 2020 年 10 月 7 日付欧州議会及び閣僚理事会規則 (EU) 2020/1503。

36 証券化に関する一般的な枠組みを定め、単独、透明かつ標準化された証券化に向けた特定の枠組みを創出すること、並びに指令 2009/65/EC、2009/138/EC、2011/61/EU、規則 (EC) No 1060/2009、 (EU) No 648/2012 (OJ L 347, 28.12.2017, p. 35)の改正に関する 2017 年 12 月 12 日付欧州議会及び閣僚理事会規則 (EU) 2017/2402。

（仮訳）

第 4 条

比例原則

1. 金融機関は、その規模及び全体的なリスク特性、並びにそのサービス、活動及び業務の性質、規模及び複雑性を考慮しつつ、比例原則に従って、第2章に定める規則を遂行するものとする。

2. さらに、金融機関による第3章、第4章及び第5章第1節の適用は、これらの章の関連規則に具体的に定めるとおり、金融機関の規模及び全体的なリスク特性、並びに金融機関のサービス、活動及び業務の性質、規模及び複雑性に比例したものでなければならない。

3. 所管当局は、第6条第5項及び第16条第2項の規定に従って所管当局の要請に応じて提出される報告書を基に、ICTリスク管理の枠組みの一貫性を審査するにあたっては、金融機関による比例原則の適用を考慮するものとする。

第 2 章

ICT リスク管理

第 1 節

第 5 条

ガバナンスと組織

1. 金融機関は、高水準のデジタル・オペレーショナル・レジリエンスを達成するため、第6条第4項に従い、ICTリスクの効果的かつ慎重な管理を担保する内部ガバナンス及び管理フレームワークを整備するものとする。

2. 金融機関の経営陣は、第6条第1項に規定されるICTリスク管理の枠組みに関連する全ての取り決めを定め、承認し、監督し、その実施に責任を負うものとする。

第 1 サブパラグラフの目的上、経営陣は以下を行うものとする。

(a) 金融機関のICTリスクを管理する最終責任を負う

(b) 高水準のデータの可用性、真正性、完全性及び機密性を維持することを目的とする方針を導入する

(c) 全てのICT関連部門の明確な役割と責任を設定し、これらの部門間の効果的かつタイムリーなコミュニケーション、協力及び調整を確保するための適切なガバナンスの取り決めを確立する

(d) 第6条第8項(b)が定める金融機関のICTリスクの適切なリスク許容水準の決定を含め、第6条第8項が定めるデジタル・オペレーショナル・レジリエンス戦略を設定し承認する全体的な責任を負う

(e) 金融機関のICT事業継続方針及びICT対応・復旧計画の実施を承認し、監督し、定期的にレビューする。これらは、第11条第1項及び第3項にそれぞれ規定されており、金融機関の全体的な事業継続方針及び対応・復旧計画の不可欠な部分を形成する専用かつ特定の政策として採用することができる

(f) 金融機関のICT内部監査計画、ICT監査及びそれらの重要な修正を承認し、定期的にレビューする

(g) 関連するICTセキュリティ意識向上プログラム、並びに第13条第6項に規定されるデジタル・オ

ペレーショナル・レジリエンス研修及び全職員のICTスキルを含むあらゆる種類のリソースに関する金融機関のデジタル・オペレーショナル・レジリエンスのニーズを満たすために、適切な予算を配分し、定期的にレビューする

(h) ICTサードパーティサービスプロバイダーが提供するICTサービスの利用に係る取り決めに関する金融機関の方針を承認し、定期的にレビューする

(i) 企業レベルで、次の事項について適切に情報を得ることができるように報告経路を整備する

(i) ICTサービスの利用に関するICTサードパーティサービスプロバイダーとの取り決め

(ii) ICTサードパーティサービスプロバイダーに関する計画上の重要な変更

(iii) かかる変更の影響を評価するためのリスク分析の概要、少なくとも重要または重大なICT関連のインシデント及びその影響、並びに対応・復旧・是正措置を含む、当該取り決めの対象となる重要または重要な機能にかかる変更が及ぼす潜在的な影響

3. 小規模事業者以外の金融機関は、ICTサービスの利用に関するICTサードパーティサービスプロバイダーとの間で締結した取り決めを監視するための役割を確立する、又は関連するリスクの影響範囲及び関連文書を監督する責任者として上級管理職メンバーを指名するものとする。

4. 金融機関の経営陣のメンバーは、管理されているICTリスクに応じた特定の研修を定期的に受けるなどして、ICTリスク及び金融機関の業務に対するその影響を理解し、評価するための十分な知識及び技能を積極的に最新の状態に保たなければならない。

第 2 節

第 6 条

ICT リスク管理の枠組み

1. 金融機関は、全社的なリスク管理システムの一環として、健全で包括的かつ十分に文書化されたICTリスク管理の枠組みを備えていなければならない。そうすることで、金融機関は迅速、効率的かつ包括的にICTリスクに対処し、高水準のデジタル・オペレーショナル・レジリエンスを確保できる。

2. ICTリスク管理の枠組みには、コンピュータソフトウェア、ハードウェア、サーバーを含む全ての情報資産及びICT資産を正当かつ適切に保護するため、また、プレミス、データセンター、機密指定区域等の全ての関連する物理的構成要素及びインフラを保護するために必要な戦略、方針、手続、ICTプロトコル及びツールを少なくとも含めるものとし、全ての情報資産及びICT資産が損害及び不正アクセス又は不正使用を含むリスクから適切に保護されなければならない。

3. 金融機関は、ICTリスク管理の枠組みに従い、適切な戦略、方針、手続、ICTプロトコル及びツールを実装することにより、ICTリスクの影響を最小限に抑えるものとする。また、所管当局の要請に応じて、ICTリスク及びICTリスク管理の枠組みに関する完全かつ最新の情報を所管当局に提供するものとする。

4. 小規模事業者以外の金融機関は、利益相反を回避するために、ICTリスクを管理し監督する責任をコントロール機能に割り当て、そのコントロール機能の適切な水準の独立性を確保するものとする。金融機関は、3線防御モデル又は内部リスク管理及びコントロールモデルに従って、ICTリスク管理機能、コントロール機能及び内部監査機能の適切な分離及び独立性を確保するものとする。

5. ICTリスク管理の枠組みは、重大なICT関連のインシデントの発生時に加え、少なくとも年1回、若しくは小規模事業者の場合には定期的に文書化し、レビューするものとする。これは、監督者による指示又は関連するデジタル・オペレーショナル・レジリエンステスト若しくは監査プロセスから得られた結論に従って実施するものとし、また、実施及び監視から得られた教訓に基づき、継続的に改善していかなければならない。ICTリスク管理の枠組みのレビューに関する報告書は、所管当局の要請に応じて提出するものとする。

6. 小規模事業者以外の金融機関のICTリスク管理の枠組みは、金融機関の監査計画に沿って、監査人による内部監査を定期的に受けるものとする。監査役は、ICTリスクに関する十分な知識、技能、専門性及び適切な独立性を有するものとする。ICT監査の頻度及び焦点は、金融機関のICTリスクに見合っていなければならない。

7. 金融機関は、内部監査レビューの結論に基づき、重要なICT監査所見の適時の検証及び是正に関する規則を含む正式なフォローアッププロセスを確立するものとする。

8. ICTリスク管理の枠組みには、フレームワークの実施方法を定めたデジタル・オペレーショナル・レ

ジリエンスの戦略を含めるものとする。そのためには、デジタル・オペレーショナル・レジリエンスの戦略に、ICTリスクに対処して特定のICT目標を達成すべく以下の方法を盛り込むものとする。

(a) ICTリスク管理の枠組みが金融機関の事業戦略と目標をどのように支援しているかを説明する

(b) 金融機関のリスクアペタイトに応じたICTリスクのリスク許容度を設定し、ICTの障害の影響許容度を分析する

(c) 重要業績評価指標と重要なリスクメトリクスを含む明確な情報セキュリティ目標を設定する

(d) ICTリファレンスアーキテクチャ及び特定のビジネス目標を達成するために必要な変更について説明する

(e) ICT関連のインシデントの検出と影響の防止、保護を目的として導入された様々なメカニズムの概要を示す

(f) 報告された主なICT関連のインシデントの件数と予防措置の有効性に基づき、デジタル・オペレーショナル・レジリエンスの現状を示す

(g) 本規則第4章に従ってデジタル・オペレーショナル・レジリエンステストを実施する

(h) 第14条に従って開示が要求されるICT関連のインシデントが発生した場合のコミュニケーション戦略の概要を示す

9. 金融機関は、第8項に規定されるデジタル・オペレーショナル・レジリエンス戦略の文脈において、包括的なICTマルチベンダー戦略をグループ又は事業体レベルで定義することができる。そうすることで、ICTサードパーティサービスプロバイダーへの主要な依存関係を示し、ICTサードパーティサービスプロバイダーの複数の調達手法の背後にある理論的根拠を説明することができる。

10. 金融機関は、EU法及び分野別国内法に従って、ICTリスク管理要件の遵守を検証する業務をグループ内又は外部の事業者にアウトソーシングしてもよい。アウトソーシングをする場合、金融機関はICTリスク管理要件の遵守を検証する完全な責任を常に負うものとする。

（仮訳）

第 7 条

ICT システム、プロトコル及びツール

ICT リスクに対処して管理するため、金融機関は次のような ICT システム、プロトコル及びツールを使用し、最新の状態に維持するものとする。

(a)
第 4 条に規定される比例原則に従い、自社活動の遂行を支援する業務の規模に対して適切である

(b) 信頼性がある

(c) 業務の遂行及び適時のサービスの提供に必要なデータを正確に処理し、ピーク時の注文、メッセージおよび取引量に対処するため、必要に応じて新しい技術が導入された場合を含め、十分な能力を備えている

(d) 緊張下にある市場環境又はその他の不利な状況下で必要とされる追加的な情報処理ニーズに適切に対処するために、技術的な回復力がある

（仮訳）

第 8 条

識別

1. 第6条第1項に規定されるICTリスク管理の枠組みの一環として、金融機関は、ICTが支援する全ての事業機能、役割と責任、それらの機能を支援する情報資産とICT資産、及びICTリスクとの関係におけるそれらの役割と依存関係を識別、分類し、適切に文書化するものとする。また必要に応じて、少なくとも毎年、この分類及び関連文書の妥当性を検討するものとする。

2. 金融機関は、継続的に、全てのICTリスクの発生源、特に他の金融機関との間のリスクの影響範囲を特定し、ICTが支援する事業機能、情報資産及びICT資産に関連するサイバー脅威及びICTの脆弱性を評価するものとする。金融機関は、自社に影響を及ぼすリスクシナリオを定期的に、少なくとも年1回レビューするものとする。

3. 小規模事業者以外の金融機関は、ICTに支援されている自社の事業機能、情報資産又はICT資産に影響を及ぼすプロセス又は手続において、ネットワーク及び情報システムインフラへの大きな変更がある都度、リスク評価を実施するものとする。

4. 金融機関は、ネットワーク資源及びハードウェア機器を含む、全ての情報資産及びICT資産を遠隔地にあるものも併せて検知、重要とみなされるものをマッピングするものとする。また、情報資産とICT資産の構成、及び異なる情報資産とICT資産の間の関連性と相互依存性をマッピングするものとする。

5. 金融機関は、ICTサードパーティサービスプロバイダーに依存する全てのプロセスを特定して文書化し、重要または重大な機能を支援するサービスを提供するICTサードパーティサービスプロバイダーとの相互接続を洗い出すものとする。

6. 第1、4、5項の目的上、金融機関は関連する台帳を維持し、定期的に及び第3項に規定される重要な変更が生ずる都度、当該資産を更新するものとする。

7. 小規模事業者以外の金融機関は、全てのレガシーICTシステムについて定期的に（少なくとも年次で）特定のICTリスク評価を実施する必要があり、また、技術、アプリケーション、またはシステムを接続する前後にも必ずこの評価を行うものとする。

（仮訳）

第 9 条

保護と防止

1. ICTシステムを適切に保護する目的上、また、対応措置を整備する観点から、金融機関はICTシステム及びツールのセキュリティ及び機能を継続的に監視し制御しなければならず、また、適切なICTセキュリティツール、方針及び手続の実装を通じてICTリスクがICTシステムに与える影響を最小限にするものとする。

2. 金融機関は、ICTシステム（特に重要または重大な機能を支援するシステム）の回復力、継続性及び可用性を担保することを目的とするICTセキュリティ方針、手続、プロトコル及びツールを設計、調達及び実施しするものとし、また、保管中、使用中又は移動中のデータの可用性、真正性、完全性及び機密性について高水準を維持するものとする。

3. 第2項が定める目的を達成するため、金融機関は第4条に従って以下に挙げる適切なICTソリューション及びプロセスを使用するものとする。

   (a) データ転送手段のセキュリティを確保する

   (b) データの破損又は損失、不正アクセス、及びビジネス活動を妨げる可能性のある技術的欠陥のリスクを最小限に抑える

   (c) 可用性の欠如、真正性及び完全性の侵害、機密性の違反及びデータの損失を防止する

   (d) 不十分な管理、処理に関するリスク及びヒューマンエラーを含む、データ管理から生じるリスクからデータを保護する

4. 第6条第1項に規定されるICTリスク管理の枠組みの一環として、金融機関は以下を行わなければならない。

   (a) データ、情報資産及びICT資産（該当する場合には顧客の資産を含む）の可用性、真正性、完全性及び機密性を保護するための規則を定めた情報セキュリティ方針を策定し、文書化する

   (b) サイバー攻撃の際に影響を受ける情報資産を隔離するための自動メカニズムの実装を含む適切な技術、方法及びプロトコルを用いて、健全なネットワークとインフラの管理構造をリスクベースアプローチに従って確立する

   (c) 情報資産及びICT資産への物理的又は論理的なアクセスを正当で承認された機能及び活動に必要なもののみに制限する方針を実施し、その目的のためにアクセス権の設定と健全な運用を行う一連の方針、手続及び管理を確立する

(d) 関連する基準と専用の制御システムに基づく強力な認証メカニズムの方針とプロトコルを実施し、かつ、データ分類の承認とICTリスク評価プロセスの結果に基づいてデータを暗号化する暗号鍵の保護対策を実装する

(e) ICTシステムに対する全ての変更を管理された方法で記録、テスト、評価、承認、実施、検証するために、リスク評価アプローチに基づき、かつ、金融機関の全体的な変更管理プロセスの不可欠な部分であるICT変更管理（ソフトウェア、ハードウェア、ファームウェアコンポーネント、システム又はセキュリティパラメータの変更を含む）に関して文書化された方針、手続及び管理を実施する

(f) パッチ適用及びアップデートに関する適切で包括的な文書化された方針を有する

第 1 サブパラグラフ（b）の目的上、金融機関は、特に相互接続された金融プロセスにおいて危機の伝搬を最小限に抑えて阻止するため、ネットワーク接続インフラを瞬時に切断又は分割できるように設計するものとする。

第 1 サブパラグラフ（e）の目的上、ICT 変更管理プロセスは適切な管理部門によって承認されるものとし、特定のプロトコルを設定しなければならない。

（仮訳）

第 10 条

検出

1. 金融機関は、第17条に従って、ICTネットワークのパフォーマンスの問題及びICT関連のインシデントを含む逸脱した活動を迅速に検出し、潜在的に重大な単一障害点を特定するための仕組みを整備するものとする。

   第 1 サブパラグラフに規定される全ての検出メカニズムは、第 25 条に従って定期的にテストするものとする。

2. 第1項に規定される検出メカニズムは、複数の制御層を稼働させ、ICT関連のインシデント対応プロセスを起動し開始するためのアラート閾値及び基準を決定するものとする。同プロセスには、ICT関連のインシデント対応の担当者向けの自動アラートメカニズムが含まれる。

3. 金融機関は、利用者の活動、ICTの異常及びICT関連のインシデント、特にサイバー攻撃の発生を監視するために十分なリソース及びケイパビリティを投入するものとする。

4. さらに、データ報告サービスプロバイダーは、取引報告の完全性を効果的に確認し、漏れや明らかな誤りを特定し、それらの報告の再送信を要求できるシステムを有するものとする。

第 11 条

対応と復旧

1. 第6条第1項に規定されるICTリスク管理の枠組みの一環として、また、第8条に定める識別要件に基づき、金融機関は包括的なICT事業継続方針を実施するものとする。これは、金融機関の事業継続方針全体の不可欠な部分を形成しており、特化した具体的な方針として採用することができる。

2. 金融機関は、以下を特定の目的とした適切かつ文書化された取り決め、計画、手続及び仕組みを通じてICT事業継続方針を実施するものとする。

   (a) 金融機関の重要または重大な機能の継続性を確保する

   (b) 被害を限定化し、活動の再開と復旧活動を優先させる方法で、全てのICT関連のインシデントに迅速、適切かつ効果的に対応し、解決する

   (c) ICT関連のインシデントの各種類に応じた封じ込め措置、プロセス及び技術を実現し、被害の拡大防止に特化した計画、並びに第12条の規定に従って定められた個別の対応及び復旧手続を遅滞なく発動する

   (d) 事前に影響、損害及び損失を見積もる

   (e) 第14条に従って、最新の情報が全ての関連する内部スタッフ全員と外部利害関係者に伝達されるためのコミュニケーションと危機管理活動を定め、第19条に従って所管当局に報告する

3. 第6条第1項に規定されるICTリスク管理の枠組みの一環として、金融機関は関連するICT対応及び復旧計画を実施するものとし、小規模事業者以外の金融機関である場合、かかる計画は独立した内部監査レビューの対象となる。

4. 金融機関は、特に、ICTサードパーティサービスプロバイダーとの取り決めを通じてアウトソーシングされた重要または重大な機能に関しては、適切なICT事業継続計画を策定して維持し、定期的にテストするものとする。

5. 全体的な事業継続政策の一部として、金融機関は、重大な事業の中断に対するエクスポージャーについてビジネスインパクト分析（BIA）を実施するものとする。BIAの下では、金融機関は、必要に応じて内部及び外部のデータ及びシナリオ分析を用いて、重大な事業中断の潜在的な影響を定量的及び定性的な基準によって評価するものとする。BIAは、特定され、マッピングされたビジネス機能、支援プロセス、サードパーティの依存関係及び情報資産、並びにそれらの相互依存関係の重要性を考慮するものとする。金融機関は、特に全ての重要な構成要素の冗長性を適切に確保することに関して、ICT資産及びICTサービスがBIAと完全に整合する形で設計され、利用されるように取り計らうもの

とする。

6. 包括的なICTリスク管理の一環として、金融機関は以下を行わなければならない。

(a) 全機能を支援するICTシステムに関するICT事業継続計画、ICT対応・復旧計画を少なくとも年に1回テストするとともに、重要または重大な機能を支援するICTシステムに実質的な変更があった場合にもテストする

(b) 第14条に従って策定されたクライシスコミュニケーションの計画をテストする

第 1 サブパラグラフ（a）の目的上、小規模事業者以外の金融機関は、サイバー攻撃のシナリオ、及び第 12 条に定める義務を満たすために必要な主要な ICT インフラと冗長化、バックアップ及び冗長化設備との間の切り替えをテスト計画に含めるものとする。

金融機関は、第 1 サブパラグラフに従って実施されたテストの結果、及び監査チェック又は監督上のレビューから得られた勧告を考慮しつつ、ICT 事業継続方針及び ICT 対応・復旧計画を定期的にレビューするものとする。

7. 小規模事業者以外の金融機関は、危機管理機能を備えている必要があり、ICT事業継続計画又はICT対応・復旧計画が発動された場合には、特に、第14条に従って内外のクライシスコミュニケーションの計画を管理するための明確な手続を定めなければならない。

8. 金融機関は、ICT事業継続計画及びICT対応・復旧計画が発動される際に、事業中断の発生前及び発生中の活動の記録を容易にアクセス可能な状態で保存するものとする。

9. 証券集中保管機関は、ICT事業継続テスト又は同様の演習の結果の写しを所管当局に提供するものとする。

10. 小規模事業者以外の金融機関は、所管当局の要請に応じて、重大なICT関連のインシデントによって生じた年間の総費用及び損失の見積金額を報告するものとする。

11. 規則（EU）No 1093/2010、（EU）No 1094/2010及び（EU）No 1095/2010の第16条に従って、ESAは合同委員会を通じて第10項に規定される年間の総費用及び損失の見積金額に関する共通ガイドラインを2024年7月17日までに策定するものとする。

（仮訳）

第 12 条

バックアップ方針と手続、復元・復旧の手続と方法

1. ICTリスク管理の枠組みの一環として、金融機関はダウンタイムを最小限に抑え、事業中断と損失を最小限に抑えてICTシステムとデータを確実に復元するために、以下を策定し文書化するものとする。

   (a) 情報の重要度又はデータの機密性レベルに基づいて、バックアップの対象となるデータの範囲及びバックアップの最小頻度を指定するバックアップ方針及び手続

   (b) 復元・復旧の手続と方法

2. 金融機関は、バックアップ方針と手続、並びに復元・復旧手続と方法に従って起動可能なバックアップシステムを構築するものとする。バックアップシステムの起動によって、ネットワーク及び情報システムのセキュリティ又はデータの可用性、真正性、完全性若しくは機密性が損なわれてはならない。バックアップ手続並びに復旧・復元手続及び方法のテストは、定期的に行うものとする。

3. 金融機関は、自社システムを用いてバックアップデータを復元する場合、当該ICTシステムは、元のICTシステムから物理的及び論理的に分離されたICTシステムを利用する。ICTシステムは、不正アクセスやICTの破損から安全に保護されている必要があり、また必要に応じてデータやシステムのバックアップを利用して、サービスを迅速に復元できるようにしなければならない。

   中央清算機関については、復旧計画によって事業中断の発生時に全ての取引を復旧させることで、中央清算機関が確実に業務を継続し、予定日に決済を完了できるようにするものとする。

   さらに、データ報告サービスプロバイダーは、常に自社サービスを提供し維持するために、十分な資源を維持し、バックアップ施設及び復元施設を整備するものとする。

4. 小規模事業者以外の金融機関は、ビジネスニーズを確保するのに十分なリソース、ケイパビリティ及び機能を備えたICTの冗長性を維持するものとする。小規模事業者は、かかるICTの冗長性を維持する必要性をリスク特性に基づいて評価するものとする。

5. 証券集中保管機関は、ビジネスニーズを確保するために十分なリソース、ケイパビリティ、機能及び人員配置を備えたセカンダリーサイトを少なくとも1カ所維持するものとする。

   セカンダリーサイトは、以下を満たすものとする。

   (a) 明確なリスク特性を確保し、プライマリーサイトに影響を与えた事象の影響を受けないようにするため、プライマリーサイトから地理的に離れた場所に配置されること

(b) プライマリーサイトと同様に重要または重大な機能の継続性を確保できる、又は金融機関が復旧目標の範囲内で重要な業務を確実に遂行できるようにするために必要なレベルのサービスを提供できること

(c) プライマリーサイトが利用できなくなった場合に重要または重大な機能の継続性を確保するために、金融機関の職員が直ちにアクセス可能であること

6. 各機能の目標復旧時間（RTO）及び目標復旧時点（RPO）を決定するに当たり、金融機関は、当該機能が重要または重大な機能であるか否か、また市場の効率性に対する全体的な影響の可能性を考慮するものとする。かかる時間的な目標は、合意されたサービスレベルが極端なシナリオにおいて確実に満たされるようにしなければならない。

7. 金融機関は、ICT関連のインシデントから復旧する際に、最高水準のデータの完全性が確実に維持されるようにするため、多重チェックや調整をはじめ、必要なチェックを行う。こうしたチェックは、外部の利害関係者からのデータを再構築する際にも、全てのデータの一貫性がシステム間で保たれているようにするために実施するものとする。

（仮訳）

第 13 条

学習と発展

1. 金融機関は、脆弱性やサイバー脅威、ICT関連のインシデント、特にサイバー攻撃に関する情報を収集し、デジタル・オペレーショナル・レジリエンスへの影響を分析するケイパビリティとスタッフを有するものとする。

2. 金融機関は、重大なICT関連のインシデントによって中核的な活動が中断した後にICT関連のインシデント事後レビューを実施する。そして中断の原因を分析し、ICT業務又は第11条に規定されるICT事業継続方針において必要とされる改善点を特定するものとする。

   小規模事業者以外の金融機関は、要請に応じて、第 1 サブパラグラフに規定される ICT 関連のインシデント事後レビューの後に実施された変更を所管当局に通知するものとする。

   第 1 サブパラグラフに規定される ICT 関連のインシデント事後レビューでは、以下に関連するものを含め、確立された手続が随従されたか否かや、取られた措置が効果的であったかどうかを決定するものとする。

   (a) セキュリティアラートへの迅速な対応、ICT関連のインシデントの影響度及び重大度の判断

   (b) 適切とみなされる場合に実施するフォレンジック分析の質及び速度

   (c) 金融機関内でのインシデントエスカレーションの有効性

   (d) 社内外のコミュニケーションの有効性

3. 第26条及び第27条に従って実施されたデジタル・オペレーショナル・レジリエンステストから得られた教訓、及び実際のICT関連のインシデント、特にサイバー攻撃から得られた教訓、並びにICT事業継続計画及びICT対応・復旧計画の発動時に直面した課題は、相手先金融機関と交換し、監督レビューにおいて評価された関連情報とともに、ICTリスク評価プロセスに継続的かつ適切に組み込まれなければならない。これらの所見は、第6条第1項に規定されるICTリスク管理の枠組みの関連構成要素の適切なレビューの根幹を成すものとする。

4. 金融機関は、第6条第8項が定めるデジタル・オペレーショナル・レジリエンス戦略の実施の有効性を監視するものとする。特に、重要または重大な機能に関連するICTリスクの影響範囲の水準を把握するために、ICTリスクの経時的な変化をマッピングし、ICT関連のインシデント、特にサイバー攻撃の頻度、種類、規模及び変化とそのパターンを分析し、金融機関のサイバーセキュリティの成熟度や体制(準備状況)を強化するものとする。

5. ICT上級職員は、第3項に規定される所見を少なくとも年に1回経営陣に報告し、勧告を提出するものとする。

6. 金融機関は、職員研修制度の必須モジュールとしてICTセキュリティ意識向上プログラムとデジタル・オペレーショナル・レジリエンス研修を開発するものとする。これらのプログラム及び訓練は、全ての従業員及び上級管理職に適用されなければならず、また、職務の権限に見合った複雑性レベルを有するものとする。適切な場合には、金融機関は、第30条第2項（i）に従って、関連する研修制度にICTサードパーティサービスプロバイダーも含めるものとする。

7. 小規模事業者以外の金融機関は、かかる新技術の実装がICTセキュリティ要件及びデジタル・オペレーショナル・レジリエンスに及ぼす可能性のある影響を把握するためにも、関連する技術開発を継続的に監視するものとする。また、現在又は新たな形態のサイバー攻撃に効果的に対抗するために、最新のICTリスク管理プロセスを最新の状態に保たなければならない。

（仮訳）

第 14 条

コミュニケーション

1. 第6条第1項に規定されるICTリスク管理の枠組みの一環として、金融機関は少なくとも重大なICT関連のインシデント又は脆弱性について、顧客及び相手先金融機関並びに適宜公衆に対しても、責任ある開示を可能にするクライシスコミュニケーションの計画を策定するものとする。

2. ICTリスク管理の枠組みの一環として、金融機関は、内部職員及び外部利害関係者に対するコミュニケーション方針を実施するものとする。職員のためのコミュニケーション方針は、ICTリスク管理に関与する職員、特に対応・復旧に責任を負う職員と、情報提供を必要とする職員とを区別する必要性を考慮に入れなければならない。

3. 金融機関において、少なくとも職員1人以上にICT関連のインシデントのためのコミュニケーション戦略を実施する任務が課され、その目的のために公共機能及びメディア機能を果たすものとする。

第 15 条

ICT リスクの管理ツール、方法、プロセス、方針の整合化

欧州監督機構（ESA）は、欧州連合サイバーセキュリティ機関（ENISA）と協議の上、以下の目的のために合同委員会を通じて共通の規制技術基準の草案を作成するものとする。

(a) ネットワークのセキュリティを確保するために、第9条第2項が定めるICTセキュリティ方針、手続、プロトコル及びツールに含めるべきさらなる要素を規定する。侵入及びデータの誤用に対する適切な保護措置を可能にする。暗号技術を含むデータの可用性、真正性、完全性及び機密性を維持する。また、重大な中断及び不当な遅延のない正確かつ迅速なデータ伝送を保証する

(b) 第9条第4項（c）に規定されるアクセス管理権の管理のさらなる構成要素、及びそれに関連する人的資源方針を策定する。これには、アクセス権、権利の付与及び取消の手続、（ネットワーク利用パターン、時間、IT活動、未知のデバイスに関する指標を含む）適切な指標を用いたICTリスク関連の逸脱した行動の監視を明記する

(c) 逸脱した活動を迅速に検知することを可能にする第10条第1項に規定されたメカニズム、及びICT関連のインシデントの検知及び対応プロセスを起動させる第10条第2項に規定された基準の策定を進める

(d) 第11条第1項が定めるICT事業継続方針の構成要素をさらに具体化する

(e) 第11条第6項が定めるICT事業継続計画のテストをさらに具体化する。かかるテストは、重要または重大な機能の提供の質が許容できないレベルに低下したり、かかる提供が失敗したりするシナリオだけでなく、関連するICTサードパーティサービスプロバイダーの倒産やその他の破綻の潜在的な影響と、関連する場合にはそれぞれのプロバイダーの国における政治的リスクを十分に考慮したものにする

(f) 第11条第3項に規定されるICT対応・復旧計画の構成要素をさらに具体化する

(g) 第6条第5項に規定されるICTリスク管理の枠組みのレビューに関する報告書の内容と形式をさらに具体化する

規制技術基準の草案を作成する際には、ESA は、金融機関の規模及び全体的なリスク特性、並びにそのサービス、活動及び業務の性質、規模及び複雑性を考慮するとともに、異なる金融サービス分野にわたる活動の異なる性質から生じる特定の特徴を十分に考慮するものとする。

ESA は、上記の規制技術基準の草案を 2024 年 1 月 17 日までに欧州委員会に提出するものとする。

規則（EU）No 1093/2010、（EU）No 1094/2010 及び（EU）No 1095/2010 第 10 条から第 14 条に従い、

第 1 項に規定される規制技術基準を採択することによって本規則を補足する権限が欧州委員会に委任される。

第 16 条

ICT リスク管理の枠組みの簡素化

1. 本規則第5条から第15条は、相互関連性のない小規模投資会社、指令（EU）2015/2366に従って除外される決済機関、指令2013/36/EUに従って除外された機関であって、加盟国が本規則第2条第4項により定められたオプションを適用しないことを決定した機関、指令2009/110/ECに従って除外された電子マネー事業者、及び年金を提供する小規模機関に適用しないものとする。

第 1 サブパラグラフの規定を害することなく、第 1 サブパラグラフに掲げる事業体は以下を満たすものとする。

(a) 関連する物理的構成要素及びインフラの保護を含め、ICTリスクの迅速、効率的かつ包括的な管理を目的としたメカニズム及び措置を詳述する、健全で文書化されたICTリスク管理の枠組みを整備・維持する

(b) 全てのICTシステムのセキュリティと機能を継続的に監視する

(c) 事業体の活動の遂行及びサービスの提供を支援するのに適切で、回復力があり、かつ最新のICTシステム、プロトコル及びツールを利用することで、ICTリスクの影響を最小化する、並びに、ネットワーク及び情報システムにおけるデータの可用性、真正性、完全性及び機密性を適切に保護する

(d) ICTリスクの発生源や、ネットワーク、情報システム内の異常を早期に識別して検知し、ICT関連のインシデントに迅速に対応する

(e) ICTサードパーティサービスプロバイダーへの主な依存関係を特定する

(f) 事業継続計画、少なくともバックアップ及び復旧措置を含む対応・復旧措置を通じて、重要または重大な機能の継続性を確保する

(g) （f）に規定される計画及び措置、並びに（a）及び（c）に従って実施されたコントロールの有効性を定期的にテストする

(h) 適宜、（g）に規定されるテスト及びインシデント事後分析から得られた運用上の結論をICTリスク評価プロセスに導入し、ニーズ及びICTリスク特性に応じて職員及び管理職向けのICTセキュリティ意識向上プログラム及びデジタル・オペレーショナル・レジリエンス研修を策定する

2. 第1項第2サブパラグラフ（a）に規定されるICTリスク管理の枠組みは、監督上の指示に従って、定期的に及び重大なICT関連のインシデントの発生時に文書化し、レビューするものとする。また、実

施及び監視から得られた教訓に基づいて継続的に改善するものとする。ICTリスク管理の枠組みのレビューに関する報告は、所管当局の要請に応じて提出するものとする。

3. ESAは、ENISAと協議の上、以下の目的のために合同委員会を通じて共通の規制技術基準の草案を作成するものとする。

(a) 第1項第2サブパラグラフ（a）に規定されるICTリスク管理の枠組みに含めるべき要素をさらに具体化する。

(b) ネットワークのセキュリティを確保し、侵入及びデータの誤用に対する適切な保護措置を可能にし、並びにデータの可用性、真正性、完全性及び機密性を維持することを目的として、第1項第2サブパラグラフ(c)が定めるICTリスクの影響を最小限にするためのシステム、プロトコル及び手段に関する要素をさらに具体化する

(c) 第1項第2サブパラグラフ（f）に規定されるICT事業継続計画の構成要素をさらに具体化する。

(d) 事業継続計画のテストに関する規則をさらに規定し、かかるテストでは、第1項第2サブパラグラフ（g）に規定されるコントロールの有効性を担保し、重要または重大な機能の提供の質が容認できないレベルまで低下したり、かかる提供が失敗したりするシナリオを十分に考慮する。

(a) 第2項に規定されるICTリスク管理の枠組みのレビューに関する報告の内容及び様式をさらに具体化する。

規制技術基準案を作成する際には、ESA は、金融機関の規模及び全体的なリスク特性、並びにそのサービス、活動及び業務の性質、規模及び複雑性を考慮するものとする。

ESA は、上記の規制技術基準の草案を 2024 年 1 月 17 日までに欧州委員会に提出するものとする。

規則（EU）No 1093/2010、（EU）No 1094/2010 及び（EU）No 1095/2010 の第 10 条から第 14 条に従い、第 1 サブパラグラフに規定される規制技術基準を採択することによって本規則を補足する権限が欧州委員会に委任される。

第 3 章

CT 関連のインシデント管理、分類及び報告

第 17 条

ICT 関連のインシデント管理プロセス

1. 金融機関は、ICT関連のインシデントを検出、管理、通知するためのICT関連のインシデント管理プロセスを定め、確立し実施するものとする。

2. 金融機関は、全てのICT関連のインシデント及び重大なサイバー脅威を記録するものとする。そして、ICT関連のインシデントの一貫した統合的な監視、処理及びフォローアップを実施するための適切な手続及びプロセスを確立し、かかるインシデントの発生を防止すべく根本原因を特定し、文書化し、対処するものとする。

3. 第1項に規定されるICT関連のインシデント管理プロセスでは、次の事項を実施するものとする。

   (a) 早期警戒指標を導入する。

   (b) 第18条第1項に定める基準に従い、ICT関連のインシデントをその優先度と重大度、及び影響を受けるサービスの重要度に応じて特定、追跡、記録、分類及び分類するための手続を確立する。

   (c) ICT関連のインシデントの種類やシナリオに応じて、活用されるべき役割と責任を割り当てる。

   (d) 第14条に基づく職員、外部利害関係者及びメディアとのコミュニケーション、顧客への通知、ICT関連の顧客からの苦情を含む内部エスカレーション手続、並びに相手先金融銀行として適宜行動する金融機関への情報提供に関する計画を策定する。

   (e) 重大なICT関連のインシデントは少なくとも関連する上級管理者に報告し、また、少なくとも重大なICT関連のインシデントは経営陣に報告し、かかるICT関連のインシデントの結果確立される影響、対応及び追加的なコントロールについて説明する。

   (e) 影響を軽減し、サービスが適時に運用可能かつ安全となったことを保証するためのICT関連のインシデント対応手順を確立する。

（仮訳）

第 18 条

ICT 関連のインシデント及びサイバー脅威の分類

1. 金融機関は、以下の基準に基づいてICT関連のインシデントを分類し、その影響を判断する。

(a) ICT関連のインシデントの影響を受けた顧客又は相手先金融機関の数及び／又は関連性、また該当する場合には、ICT関連のインシデントの影響を受けた取引額又は件数、及びICT関連のインシデントがレピュテーションに及ぼした影響の有無

(b) サービス停止時間を含むICT関連のインシデントの継続時間

(c) 特にICT関連のインシデントが2カ国以上の加盟国に影響を及ぼす場合のICT関連のインシデントの影響を受ける地域に関する地理的広がり

(d) データの可用性、真正性、完全性又は機密性に関連するICT関連のインシデントに伴うデータ損失

(e) 金融機関の取引及び業務を含む、影響を受けるサービスの重要度

(f) ICT 関連のインシデントの絶対的及び相対的な経済的影響、特に直接的及び間接的な費用及び損失

2. 金融機関は、リスクにさらされているサービスの重要性(当該金融機関の取引及び業務、対象となる顧客又は相手先金融機関の数及び／又は関連性、及びリスクにさらされている地域の地理的広がりを含む)に基づいて、サイバー脅威を重大な脅威として分類するものとする。

3. ESAは、ECB及びENISAと協議の上、以下をさらに具体化する共通の規制技術基準の草案を、合同委員会を通じて作成するものとする。

(a) 第1項に定める基準（第19条第1項に定める報告義務の対象となる重大なICT関連のインシデント、又は該当する場合は業務若しくは証券決済に関連する重大なインシデントを判断するための重要性の閾値を含む）

(b) 重大なICT関連のインシデント、又は該当する場合には、業務若しくは証券決済に関連する重大なインシデントの重大度を評価する目的上、所管当局が他の加盟国の関連所管当局に適用する基準、及び第19条第6項及び第7項に従って他の所管当局と共有される重大なICT関連のインシデント、又は該当する場合には、業務若しくは証券決済に関連する重大なインシデントの報告の詳細

(c) 本条第2項に定める基準; 重大なサイバー脅威を判断するための高い重要性の閾値を含む

4. 本条第3項に規定される共通規制技術基準の草案を作成する場合、ESAは、第4条第2項に規定される

（仮訳）
基準並びにENISAが策定し公表する国際基準、ガイダンス及び仕様（適切な場合には、他の経済分野の仕様を含む）を考慮に入れるものとする。第4条第2項に定める基準を適用する目的上、ESAは、小規模事業者及び中小企業がICT関連のインシデントに迅速に対処するにあたって十分なリソース及びケイパビリティを結集する必要性を十分に考慮するものとする。

ESA は、上記の共通規制技術基準の草案を 2024 年 1 月 17 日までに欧州委員会に提出するものとする。

規則（EU）No 1093/2010、（EU）No 1094/2010 及び（EU）No 1095/2010 第 10 条から第 14 条に従って、第 3 項に規定される規制技術基準を採択することによって本規則を補足する権限が委員会に委任されるものとする。

（仮訳）

第 19 条

ICT 関連の主要なインシデントの報告及び重大なサイバー脅威についての自主的な通知

1. 金融機関は、本条第4項に従い、重大なICT関連のインシデントを第46条に規定される関係所管当局に報告するものとする。

   金融機関が第 46 条に規定される複数の所管当局による監督の対象となる場合、加盟国は、本条で規定された機能及び義務を遂行する責任を有する所管当局として単一の所管当局を指定するものとする。

   規則（EU）第 1024/2013 号第 6 条第 4 項に従い「重要」と分類された信用機関は、指令 2013/36/EU 第 4 条に従って指定された関連する国内の主管当局に、重大な ICT 関連インシデントを報告しなければならない。その主管当局は、直ちにその報告を ECB（欧州中央銀行）へ送付しなければならない。

   第 1 サブパラグラフの目的上、金融機関は、全ての関連する情報を収集し及び分析した後、第 20 条が定めるテンプレートを用いて、第 4 項に規定される初期通知及び報告を作成し、所管当局に提出するものとする。ただし、技術的な理由で提出が不可能な場合に金融機関は、代替手段を通じてその旨を所管当局に通知するものとする。

   第 4 項に規定される初期通知及び報告には、所管当局が重大な ICT 関連のインシデントの重篤度を決定し、国境を越えて影響が及ぶ可能性を評価するために必要な全ての情報を記載するものとする。

   金融機関が第 1 サブパラグラフに従って該当する所管当局に報告することを妨げることなく、加盟国は、一部又は全ての金融機関が第 20 条に規定されるテンプレートを用いた本条 4 項に規定される初期通知及び各報告も、所管当局、又は指令（EU）2022/2555 に従って指定又は設置されたコンピュータセキュリティインシデント対応チーム（CSIRT）に提供しなければならない旨を追加的に決定することができる。

2. 金融機関は、重大なサイバー脅威が金融システム、サービス利用者又は顧客に関連すると判断した場合には、自主的に重大なサイバー脅威を関連する所管当局に通知することができる。該当する所管当局は、第6項に規定される他の関係当局にかかる情報を提供することができる。

   規則（EU）第 1024/2013 号第 6 条第 4 項に従い「重要」と分類された信用機関は、任意で、指令 2013/36/EU 第 4 条に従って指定された関連する国内の主管当局に、重大なサイバー脅威を通知することができる。その主管当局は、直ちにその通知を ECB（欧州中央銀行）へ送付しなければならない。

   加盟国は、第 1 サブパラグラフに従って自主的に通知する金融機関がその通知を指令（EU）2022/2555 に従って指定又は設立された CSIRT にも伝達することができる旨を決定することができる。

3. 金融機関は、重大なICT関連のインシデントが発生し、顧客の金融上の利益に影響を及ぼす場合には、当該インシデントを認識した時点で遅滞することなく、その発生状況及び影響を緩和するために講じた措置について顧客に通知するものとする。

重大なサイバー脅威の場合、金融機関は、該当する場合に影響を受ける可能性のある顧客に対し、当該顧客が実施を検討することが可能な適切な保護措置を通知するものとする。

4. 金融機関は、第20条第1項（a）、（ii）に従って設定される期限内に、関連する所管当局に以下を提出するものとする。

(a) 初期通知

(b) （a）に規定される初期通知の提出後、当初のインシデントの状況が大きく変化した場合、又は新たに入手した情報に基づいて重大なICT関連のインシデントの対応が変化した場合に行う中間報告。続いて、適切な状況が更新された都度及び所管当局からの具体的な要請があった場合に行う更新後の通知

(c) 根本原因分析が完了した際に提出される最終報告書。これは、改善措置がすでに実施されているかどうかに関わらず、また、概算値に代わる実際の影響データが利用可能になった場合に提出されるものとする。

5. 金融機関は、EU法及びセクター別国内法に従い、本条の規定に基づく報告義務をサードパーティサービスプロバイダーにアウトソーシングすることができる。アウトソーシングする場合、金融機関はインシデント報告要件を満たすことに完全な責任を負う。

6. 所管当局は、第4項に規定される初期通知及び各報告を受領した際には、以下の受領者に対し、該当する場合にそれぞれの権限に応じて重大なICT関連のインシデントの詳細を適時に提供する。

(a) EBA、ESMA又はEIOPA

(b) ECB（第2条第1項（a）、（b）及び（d）に規定される金融機関の場合）

(c) 所管当局、指令（EU）2022/2555に従って指定又は設置された単一の連絡窓口又はCSIRT

(d) 破綻処理機構、並びに欧州議会及び閣僚理事会規則（EU）No 806/2014第7条第2項[37]に規定される事業体に関して、かつ、規則（EU）No 806/2014第7条第4項（b）及び（5）に規定される事業体及びグループに関しては（その内容が指令2014/59/EU第2条第1項（35）の意味の範囲内における重要な機能の確保にリスクをもたらすインシデントに関連する場合）、指令2014/59/EU第3条に規定される単一破たん処理委員会（SRB）

(e) 国内法に基づくその他の関連公的機関

---

37 単一破綻処理メカニズム及び単一破綻処理基金の枠組みにおける、信用機関及び特定の投資会社の破綻処理のための統一規則・手順を制定し、規則 (EU) No 1093/2010 (OJ L 225, 30.7.2014, p. 1)を改正する 2014 年 7 月 15 日付欧州議会及び閣僚理事会規則 (EU) No 806/2014。

7. 第6項に従って情報を受領した後、EBA、ESMA又はEIOPA及びECBは、ENISAと協議し、関連所管当局と協力して、重大なICT関連のインシデントが他の加盟国の所管当局に関連するか否かを評価するものとする。この評価後に、EBA、ESMA又はEIOPAは、できるだけ速やかに他の加盟国の関連所管当局にその旨を適宜通知するものとする。ECBは、決済システムに関連する問題を欧州中央銀行制度の加盟国に通知するものとする。所管当局は、この通知に基づき、必要に応じて金融システムの当面の安定を保護するために必要な全ての措置を講じるものとする。

8. 証券集中保管機関が加盟主催国内で国境を越えた重要な活動を行っている場合、関連する重大なICT関連のインシデントが加盟主催国内の金融市場に深刻な影響を及ぼす可能性がある場合及び金融機関の監督に関連する所管当局間の協力体制がある場合には、本条7項に従ってESMAが行う通知は、当該重大なICT関連のインシデントの詳細を加盟主催国内の関係当局に緊急に伝達するという所管当局の責任を妨げてはならない。

（仮訳）

第 20 条

報告内容及びテンプレートの整合化

ESA は、ENISA 及び ECB と協議の上、合同委員会を通じて次の事項を策定するものとする。

(a) 以下を目的とした共通規制技術基準の草案

(i) 第18条第1項に定められた基準を反映するために、重大なICT関連のインシデントに関する報告の内容を確立し、他の加盟国に対する報告の関連性を確立するための詳細や、かかるインシデントが運用又は証券決済に関連する重大なインシデントであるか否かなどの追加的な要素を組み込む

(ii) 初期通知及び第19条第4項が定める各報告の期限を決定する

(iii) 重大なサイバー脅威に関する通知の内容を確立する。

ESA は、規制技術基準の草案を策定する際には特に本項（a）及び（ii）の目的上、本規則及び指令（EU）2022/2555 に準拠した ICT 関連のインシデント報告に対する一貫したアプローチの維持を妨げることなく、異なる期限に金融分野の特殊性を適宜反映させる観点から、金融機関の規模及び全体的なリスク特性並びにそのサービス、活動及び業務の性質、規模及び複雑性を考慮に入れるものとする。また、該当する場合、かかる指令の文脈において採用されたアプローチから逸脱した際にはその正当性を示すものとする。

(b) 金融機関が重大なICT関連のインシデントを報告し、重大なサイバー脅威を通知する際に使用できる標準的な様式、テンプレート及び手続を確立するための共通の実施技術基準の草案。

ESA は、第 1 項（a）に規定される共通の規制技術基準の草案、及び第 1 項（b）が定める共通の実施技術基準の草案を 2024 年 7 月 17 日までに欧州委員会に提出するものとする。

規則（EU）No 1093/2010、（EU）No 1094/2010 及び（EU）No 1095/2010 の第 10 条から第 14 条に従って、第 1 項（a）に規定される共通の規制技術基準を採択することによって本規則を補足する権限が欧州委員会に委任される。

規則（EU）No 1093/2010、（EU）No 1094/2010 及び（EU）No 1095/2010 の第 15 条に従い、第 1 項（b）に規定される共通の実施技術基準を採択する権限が欧州委員会に与えられる。

（仮訳）

第 21 条

重大な ICT 関連のインシデント報告の一元化

1. ESAは、合同委員会を通じてECB及びENISAと協議の上、金融機関による重大なICT関連のインシデント報告のためのEU共通の情報ハブの設立を通してインシデント報告をさらに一元化することが実現可能であるかを評価する共同報告書を作成する。共同報告書は、監督の一貫性を強化する観点からICT関連のインシデント報告の流れを促進し、関連コストを削減し、テーマ別分析を支える方法を調査するものとする。

2. 第1項に規定される共同報告書は、少なくとも次の要素から構成されるものとする。

   (a) EU共通の情報ハブ設立の前提条件

   (b) 利点、制約および機密性の高い情報の集中に伴うリスクを含むリスク

   (c) 他の関連する報告制度との相互運用性を確保するために必要なケイパビリティ

   (d) 運用管理の要素

   (e) 加盟条件

   (f) 金融機関及び各国の所管当局がEU共通の情報ハブにアクセスするための技術的な取り決め

   (g) 必要な専門知識を含む、EU共通の情報ハブを支える運用プラットフォームを構築するために発生する財務コストの予備的評価。

3. ESAは、第1項に規定される報告書を2025年1月17日までに欧州議会、閣僚理事会及び欧州委員会に提出するものとする。

（仮訳）

第 22 条

監督上のフィードバック

1. 指令（EU）2022/2555に基づくCSIRTにより、該当する場合には国内法に従って提供される技術的なインプット、助言、救済及びその後のフォローアップを妨げることなく、所管当局は、第19条第4項に規定される初期通知及び各報告を受領した時点で受領を確認し、実行可能な場合には、特に同様の脅威に関する匿名化された関連情報及びインテリジェンスを利用可能にすることにより、適切かつ相応なフィードバック又はハイレベルのガイダンスを適時に金融機関に提供することができ、金融機関レベルで適用される救済策及び金融セクター全体にわたる悪影響を最小化及び軽減する方法について議論することができる。金融機関は、受領した監督上のフィードバックを妨げることなく、第19条第1項に従って報告されたICT関連のインシデントの処理及び結果について引き続き完全な責任を負う。

2. ESAは、合同委員会を通じて重大なICT関連のインシデントを匿名及び集計ベースで毎年報告するものとし、少なくとも重大なICT関連のインシデントの件数、その性質及び金融機関又は顧客の業務への影響、講じた是正措置及び発生したコストを記載した報告内容は、所管当局が第19条第6項に従って提供しなければならない。

ESA は、ICT 脅威及び脆弱性の評価を支援するために警告を発し、詳細な統計を作成するものとする。

（仮訳）

第 23 条

信用機関、決済機関、口座情報提サービスプロバイダー及び電子マネー事業者に係る運用又は証券決済関連のインシデント

本章に定める要件は、信用機関、支払機関、口座情報サービスプロバイダー及び電子マネー事業者に関する場合には、運用又は証券決済関連のインシデント並びに運用又は証券決済関連の重大なインシデントにも適用する。

第 4 章

デジタル・オペレーショナル・レジリエンステスト

第 24 条

デジタル・オペレーショナル・レジリエンステストの実施に関する一般要件

1. ICT関連のインシデントに対処するための準備状況を評価し、デジタル・オペレーショナル・レジリエンスにおける弱点、欠陥及びギャップを特定し、是正措置を迅速に実施する目的上、小規模事業者以外の金融機関は、第4条第2項に定める基準を考慮しつつ、第6条に規定されるICTリスク管理の枠組みの不可欠な部分としての健全かつ包括的なデジタル・オペレーショナル・レジリエンステストプログラムを確立し、維持し、レビューするものとする。

2. デジタル・オペレーショナル・レジリエンステストプログラムには、第25条及び第26条に従って適用される一連の評価、テスト、方法論、演習及びツールを含めるものとする。

3. 本条第1項に規定されるデジタル・オペレーショナル・レジリエンステストプログラムを実施する場合、小規模事業者以外の金融機関は、第4条第2項に定める基準を考慮に入れたリスクベースアプローチに従うものとし、ICTリスクの状況の変化、当該金融機関が現在又は将来さらされる可能性のある特定のリスク、情報資産及び提供されるサービスの重要性並びに当該金融機関が適切とみなすその他の要因を十分に考慮する。

4. 小規模事業者以外の金融機関は、独立した当事者が内部者であるか外部者であるかに拠らず、かかる当事者がテストを実施するように取り計らうものとする。内部のテスト実施者がテストを実行する場合、金融機関は十分なリソースを投入し、テストの設計及び実施段階を通じて利益相反を回避するものとする。

4. 小規模事業者以外の金融機関は、テストの実施を通じて明らかになった全ての問題に優先順位を付け、分類し、改善するための手続と方針を確立しなければならず、特定された全ての弱点、欠陥又はギャップが完全に対処されていることを確認するための内部検証方法を確立するものとする。

5. 小規模事業者以外の金融機関は、重要または重大な機能を支援する全てのICTシステム及びアプリケーションについて、適切なテストが少なくとも年に1回実施されるようにする。

（仮訳）

第 25 条

ICT ツール及びシステムのテスト

1. 第24条が定めるデジタル・オペレーショナル・レジリエンステストプログラムは、第4条第2項に定める基準に従って、脆弱性評価及びスキャン、オープンソース分析、ネットワークセキュリティ評価、ギャップ分析、物理的セキュリティレビュー、アンケート及びスキャニングソフトウェアソリューション、実現可能な場合はソースコードレビュー、シナリオベースのテスト、互換性テスト、パフォーマンステスト、エンドツーエンドのテスト及び侵入テストなどの適切なテストの実施を提供するものとする。

2. 証券集中保管機関及び中央清算機関は、新規又は既存のアプリケーション及びインフラコンポーネント、並びに金融機関の重要または重大な機能を支援するICTサービスの実装又は再実装の前に、脆弱性評価を実施するものとする。

3. 小規模事業者は、本条に規定されるICTテストに配分されるリソースの規模及び時間との間でバランスのとれたアプローチを維持する必要性と、一方では、リスクの緊急性、種類、提供される情報資産及びサービスの重要性並びに算出されたリスクを引き受ける金融機関のケイパビリティを含む他の関連する要素を適切に考慮しつつ、リスクベースアプローチをICTテストの戦略的計画を組み合わせることにより、第1項に規定されるテストを実施するものとする。

（仮訳）

第 26 条

TLPT に基づく ICT ツール、システム、プロセスの高度なテスト

1. 第16条第1項第1サブパラグラフに規定される事業体以外の金融機関、及び本条第8項第3サブパラグラフに従って特定される小規模事業者以外の金融機関は、脅威ベースのペネトレーションテスト（TLPT）によって少なくとも3年ごとに高度なテストを実施するものとする。所管当局は、金融機関のリスク特性に基づき、かつ、業務の状況を考慮しつつ、必要に応じて、金融機関に対して当該テストの頻度の増減を要請することができる。

2. 各TLTPは、金融機関の重要または重大な機能の一部又は全てを対象とし、かかる機能を支援する実稼働システムで実行するものとする。

   金融機関は、重要または重要な機能及び ICT サービスを支援する全ての関連する基盤となる ICT システム、プロセス及び技術を特定するものとする。これには、ICT サードパーティサービスプロバイダーにアウトソーシングしている重要または重大な機能を支援するものが含まれる。

   金融機関は、どの重要または重大な機能を TLPT の対象とする必要があるかを評価する。この評価の結果は、TLPT の正確な適用範囲を決定し、所管当局によって検証されなければならない。

3. ICTサードパーティサービスプロバイダーがTLPTの適用範囲に含まれる場合、金融機関は、当該ICTサードパーティサービスプロバイダーをTLPTに参加させるために必要な措置及び保護措置を講じなければならず、また、本規則の遵守を徹底させるための完全な責任を常に負うものとする。

4. 第2項第1及び第2サブパラグラフを妨げることなく、第3項に規定されるICTサードパーティサービスプロバイダーのTLPTへの参加が、ICTサードパーティサービスプロバイダーが本規則の適用範囲外の事業体である顧客に提供するサービスの品質若しくはセキュリティ、又は当該サービスに関連するデータの機密性に悪影響を及ぼすことが合理的に予想される場合、金融機関とICTサードパーティサービスプロバイダーは、1つの指定金融機関の指示の下で、ICTサードパーティサービスプロバイダーがICTサービスを提供する複数の金融機関が関与する合同のTLPT（合同テスト）を実施するために、ICTサードパーティサービスプロバイダーが外部のテスト実施者と契約上の取り決めの直接締結を書面で合意することができる。

   この合同テストは、金融機関がそれぞれの ICT サードパーティサービスプロバイダーと契約した重要または重大な機能を支援する ICT サービスの関連範囲を対象とする。合同テストは、合同テストに参加する金融機関によって実施される TLPT とみなされるものとする。

   合同テストに参加する金融機関の数は、関連するサービスの複雑さと種類を考慮して適切に調整するものとする。

5. 金融機関は、ICTサードパーティサービスプロバイダー及び、監督当局を除くその他の関係者の協力を得て、金融機関自体や相手先金融機関又は金融セクターにおけるデータへの潜在的な影響、資産の損傷、及び、重要または重大な機能、サービス又は業務の中断のリスクを軽減するために、効果的なリスク管理策を適用するものとする。

6. テストの終了時に報告及び改善計画が合意された後、金融機関及び該当する場合には外部のテスト実施者は、関連する調査結果の要約、改善計画及びTLPTが要件に従って実施されたことを証明する文書を第9項又は10項に従って指定された当局に提出するものとする。

7. 当局は、所管当局間でのTLPTに関する相互認識を実現するために、文書で証明しているとおりに要件に従ってテストが実施されたことを確証するアテステーションを金融機関に提供するものとする。金融機関は、アテステーション、関連する調査結果の概要及び是正計画を関連する所管当局に通知するものとする。

   金融機関は当該アテステーションを妨げることなく、第 4 項に規定されるテストの影響について常に完全な責任を負うものとする。

8. 金融機関は、第27条に従ってTLPTを実施することを目的とした契約をテスト実施者と締結するものとする。金融機関は、TLPTを実施する目的で内部テスト実施者を利用する場合、テストを3回実施するごとに外部テスト実施者と契約するものとする。

   規則（EU）第 1024/2013 号第 6 条第 4 項に従い「重要」と分類された信用機関は、第 27 条第 1 項(a)から(e)までの規定に従ってのみ、外部テスターを利用しなければならない。

   所管当局は、第 4 条第 2 項に定める基準を考慮しつつ TLPT を実施することが要求される金融機関を以下の評価に基づいて特定するものとする。

   (a) 影響に関連する要因、特に金融機関が提供するサービス及び実施する活動が金融セクターに与える影響の程度

   (b) 金融機関の連合レベルまたは国内レベルでのシステミックな性質を含む、考えられる金融安定性への懸念（該当する場合）

   (c) 具体的なICTリスク特性、金融機関のICT成熟度レベル、又は関連する技術特性。

9. 加盟国は、金融セクターにおけるTLPT関連事項に国レベルで責任を負う、単独の公的機関を金融セクターにて指定することができ、その責任を完遂するための全ての権限と業務を当該公的機関に委任するものとする。

10. 本条第9項に従った指定がなされない場合には、所管当局はTLPTの実施を要求される金融機関を特定する権限を妨げることなく、本条及び第27条に規定される業務の一部又は全部の実施を金融セクタ

ーにおける他の国家当局に委任することができる。

11. ESAは、ECBとの合意の下でTIBER-EUの枠組みに従い、以下をさらに具体化するための共同規制技術基準の草案を作成するものとする。

(a) 第8項第2サブパラグラフを適用する目的で使用される基準

(b) 社内テスト実施者の利用に関する要求事項及び基準

(c) 以下に関する要件

(i) 第2項に規定されるTLPTの適用範囲

(ii) テストプロセスの特定の段階ごとに従うべきテスト方法及びアプローチ

(iii) テストの結果、終了及び修復段階

(d) 複数の加盟国で運営する金融機関のコンテキストにおいて、TLPTの実施及びTLPTテストの相互承認の促進のために必要とされる監督及びその他の関連する協力の種類。これにより、適切なレベルの監督上の関与及び金融サブセクター又は現地金融市場の特殊性に対応する柔軟な実施が可能となる。

この規制技術基準の草案を作成する際には、ESA は、異なる金融サービスセクターにわたる活動の異なる性質から生じる特定の特徴を十分に考慮するものとする。

ESA は、この規制技術基準の草案を 2024 年 7 月 17 日までに欧州委員会に提出するものとする。

規則（EU）No 1093/2010、（EU）No 1094/2010 及び（EU）No 1095/2010 の第 10 条から第 14 条に従い、第 1 サブパラグラフに規定される規制技術基準を採択することによって本規則を補足する権限が欧州委員会に委任される。

（仮訳）

第 27 条

TLPT 実施に関するテスト実施者の要件

1. 金融機関は、TLPTを実施するにあたって以下に該当するテスト実施者のみを利用するものとする。

   (a) 最高レベルの適合性及び評判を持つ

   (b) 技術的能力及び組織的能力を有し、脅威インテリジェンス、侵入テスト、レッドチームのテストに関する専門知識を有する

   (c) 加盟国の認定機関によって認定されている、又は正式な行動規範若しくは倫理的枠組みを遵守している

   (d) 金融機関の秘密情報の適切な保護及び金融機関の事業リスクの是正を含め、TLPTの実施に伴うリスクの健全な管理に関して独立した保証又は監査報告を提供する

   (e) 関連する専門職業人賠償責任保険により、正当かつ完全に補償されている（不正行為及び過失のリスクに対する補償を含む）。

2. 金融機関は内部テスト実施者を利用する場合、第1項の要件に加えて以下の条件が満たされていることを保証するものとする。

   (a) 当該利用が、関連する所管当局又は第26条第9項及び第10項に従って指定された単独の公的機関によって承認されている

   (b) 当該所管当局は、当該金融機関が十分な専門リソースを有していることを検証し、かつ、テストの設計及び実施段階の全般にわたって利益相反が回避されていることを保証している

   (c) 脅威インテリジェンスプロバイダーは、金融機関外の事業者である。

3. 金融機関は、外部テスターと締結する契約において、TLPTの結果が適切に管理されること、またその結果の生成、保存、集約、作成、報告、伝達、廃棄を含むいかなるデータ処理も、金融機関にリスクを生じさせないことを確保しなければならない。

（仮訳）

第 5 章

ICT サードパーティリスクの管理

第 1 節

ICT サードパーティリスクの健全な管理に関する原則

第 28 条

一般原則

1. 金融機関は、第6条第1項に規定されるICTリスク管理の枠組みの中で、かつ以下の原則に従って、ICTサードパーティリスクをICTリスクの不可欠な構成要素として管理するものとする。

   (a) ICTサービスを利用して事業を運営するための契約上の取り決めを締結している金融機関は、本規則及び適用される金融サービス法に基づく全ての義務の遵守及び履行について常に完全な責任を負うものとする

   (b) 金融機関のICTサードパーティリスク管理は、以下の事項を考慮しつつ、比例原則に照らして実施されるものとする

      (i) ICT関連の依存関係の性質、規模、複雑性及び重要性

      (ii) 個々のサービス、プロセス、又は機能の重大性又は重要性、並びに個人及びグループレベルにおける金融サービスと金融活動の継続性及び可用性に対する潜在的な影響を考慮しつつ、ICTサードパーティサービスプロバイダーとの間で締結したICTサービスの利用に関する契約上の取り決めから生じるリスク

2. ICTリスク管理の枠組みの一環として、第16条第1項第1サブパラグラフに規定される事業体以外及び小規模事業者以外の金融機関は、該当する場合に第6条第9項に規定されるマルチベンダー戦略を考慮に入れつつICTサードパーティリスクに関する戦略を採択し、定期的に見直すものとする。ICTサードパーティリスクに関する戦略には、ICTサードパーティサービスプロバイダーが提供する重要または重大な機能を支援するICTサービスの利用に関する方針が含まれ、個別ベース、及び関連する場合には下位連結ベースと連結ベースで適用される。経営陣は、金融機関の全体的なリスク特性並びにビジネスサービスの規模及び複雑性の評価に基づき、重要または重大な機能を支援するICTサービスの利用に関する契約上の取り決めに関して識別されたリスクを定期的に見直すものとする。

3. ICTリスク管理の枠組みの一環として、金融機関は、ICTサードパーティサービスプロバイダーが提供するICTサービスの利用に関する全ての契約上の取り決めに関する情報の登録簿を事業体レベル、下位準連結及び連結レベルで維持し更新するものとする。

第 1 サブパラグラフに規定される契約上の取り決めは、重要または重大な機能を支援する ICT サービスを対象とするものとそうでないものとを区別して、適切に文書化されなければならない。

金融機関は、少なくとも年に 1 回、ICT サービスの利用に関する新たな取り決めの件数、ICT サードパーティサービスプロバイダーの区分、契約上の取り決めの種類及び提供されている ICT サービスと機能について所管当局に報告するものとする。

金融機関は、所管当局の要請に応じ、当該金融機関による効果的な監督を可能にするために必要とみなされる情報とともに、完全な情報の登録簿、又は要請に応じてその特定の部分を所管当局が入手できるようにしなければならない。

金融機関は、重要または重大な機能を支援する ICT サービスの利用に関して計画中の契約上の取り決めがある場合や、ある機能が重要または重大な機能になった場合には適時に所管当局に通知するものとする。

4. 金融機関は、ICTサービスの利用に関する契約上の取り決めを締結する前に、下記を行わなければならない。
   (a) 契約上の取り決めが重要または重大な機能を支援するICTサービスの利用を対象としているかどうかを評価する

   (b) 契約に関する監督上の条件が満たされているかどうかを評価する

   (c) 契約上の取り決めが第29条で定めるICT集中リスクの強化に寄与する可能性を含め、当該契約上の取り決めに関連する全てのリスクを特定し、評価する

   (d) ICTサードパーティサービスプロバイダーの候補に対して全てのデューデリジェンスを実施し、選定及び評価プロセス全般においてICTサードパーティサービスプロバイダーの適切性を保証する

   (e) 契約上の取り決めが引き起こす可能性のある利益相反を特定し、評価する。

5. 金融機関は、適切な情報セキュリティ基準に準拠したICTサードパーティサービスプロバイダーとのみ契約上の取り決めを締結することができる。これらの契約上の取り決めが重要または重大な機能に関するものである場合、金融機関は取り決めを締結する前に、ICTサードパーティサービスプロバイダーが最新かつ最高品質の情報セキュリティ基準を使用していることを十分に考慮するものとする。

6. 金融機関は、ICTサードパーティサービスプロバイダーに対するアクセス権、検査権及び監査権を行使するにあたり、一般的に公正妥当と認められている監査基準の使用と採用に関する監督指示とともに、一般的に公正妥当と認められている監査基準を遵守することにより、監査及び検査の頻度並びに監査すべき分野をリスクベースアプローチに基づいて事前に決定するものとする。

   ICT サービスの利用に関して、ICT サードパーティサービスプロバイダーと締結した契約上の取り決めが

高度な技術的複雑性を伴う場合には、金融機関は、監査人が内部監査人か外部監査人か、又は監査人の集団かどうかにかかわらず、関連する監査及び評価を効果的に実施するための適切な技能及び知識を監査人が有していることを検証するものとする。

7. 金融機関は、次のいずれかの状況においてはICTサービス契約を終了できることを保証しなければならない.

(a) ICTサードパーティサービスプロバイダーが適用法令、規制または契約条項に重大な違反をした場合

(b) ICTサードパーティリスクの監視により、契約に基づく機能のパフォーマンスに影響を与える可能性のあり事情(契約内容やICTサービスプロバイダーの状況に重大な変化があった場合)

(c) ICTサードパーティサービスプロバイダーのICTリスク管理全般に関する弱点、特に個人データやその他の機密データ、非個人データを問わず、データの可用性、真正性、完全性、機密性を保証する方法に関する弱点が判明した場合

(d) それぞれの契約上の取り決めの条件又はそれに関連する状況の結果として、所管当局がもはや金融機関を効果的に監督することが不可能な場合

8. 重要または重大な機能を支えるICTサービスについて、金融機関は出口戦略を策定するものとする。出口戦略は、ICTサードパーティサービスプロバイダーのレベルで発生する可能性のあるリスク、特にICTサードパーティサービスプロバイダーの側で起こり得る破綻、提供されるICTサービスの質の低下、ICTサービスの不適切な提供又はかかる提供の失敗による事業の中断、又はそれぞれのICTサービスの適切かつ継続的な展開に関連して生じる重要なリスク、又は第7項に列挙されたいずれかの状況下でのICTサードパーティサービスプロバイダーとの契約上の取り決めの終了を考慮したものでなければならない。

金融機関は、次の状況を生じさせることなく契約上の取り決めを終了できるものとする。

(a) 事業活動の中断

(b) 規制要件の遵守に対する制限

(c) 顧客に提供するサービスの継続性及び質の低下

出口計画は、包括的かつ文書化されたものでなければならず、第 4 条第 2 項に定める基準に従って十分にテストし、定期的に見直さなければならない。

金融機関は代替の解決策を検知、契約した ICT サービス及び関連するデータを ICT サードパーティサービスプロバイダーから排除し、代替のプロバイダーに安全かつ一体的に移行又は金融機関内に再統合できるようにするための移行計画を策定するものとする。

金融機関は、第 1 サブパラグラフに規定される事態が発生した場合に事業継続を維持するための適切な危機管理措置を講じなければならない。

9. ESAは、合同委員会を通じて、第3項が定める情報（情報通信技術サービスの利用に関する全ての契約上の取り決めに共通する情報を含む）の登録を目的とした標準的なテンプレートを作成するための実施技術基準の草案を作成する。また、この実施技術基準の草案を2024年1月17日までに欧州委員会に提出するものとする。

   規則（EU）No 1093/2010、（EU）No 1094/2010 及び（EU）No 1095/2010 の第 15 条に従い、第 1 サブパラグラフに規定される実施技術基準を採択することによって本規則を補足する権限が欧州委員会に与えられる。

10. ESAは、ICTサードパーティサービスプロバイダーが提供する重要または重大な機能を支援するICTサービスの利用に関する契約上の取り決めに関連して第2項に規定される方針の詳細な内容をさらに具体化するため、合同委員会を通じて規制技術基準の草案を作成するものとする。

    規制技術基準の草案を作成する際には、ESA は、金融機関の規模及び全体的なリスク特性、並びにサービス、活動及び業務の性質、規模及び複雑性を考慮するものとする。ESA は、この規制技術基準の草案を 2024 年 1 月 17 日までに欧州委員会に提出するものとする。

    規則（EU）No 1093/2010、（EU）No 1094/2010 及び（EU）No 1095/2010 第 10 条から第 14 条に従って、第 1 サブパラグラフに規定される規制技術基準を採択することによって本規則を補足する権限が委員会に委任される。

（仮訳）

第 29 条

事業体レベルでの ICT 集中リスクの予備的評価

1. 第28条第4項（c）が定めるリスクの特定及び評価を行う場合には、金融機関は、重要または重大な機能を支援するICTサービスに関連して想定している契約上の取り決めの締結によって、下記のいずれかが結果としてもたらされるかどうかも考慮するものとする。

   (a) 代替が困難なICTサードパーティサービスプロバイダーと契約していること、又は

   (b) 重要または重大な機能を支援するICTサービスの提供に関して、同一のICTサードパーティサービスプロバイダー、又は密接に関連するICTサードパーティサービスプロバイダーと複数の契約上の取り決めを締結していること

   金融機関は、想定している解決策が自社のデジタル・レジリエンス戦略に定められたビジネスニーズ及び目標に合致するか否か、また、合致するとしたらどのように合致するのかを考慮しつつ、様々な ICT サードパーティサービスプロバイダーの利用などの代替の解決策の便益及びコストを比較検討するものとする。

2. 重要または重大な機能を支えるICTサービスの利用に関する契約上の取り決めにおいて、重要または重大な機能を支えるICTサービスをICTサードパーティサービスプロバイダーが他のICTサードパーティサービスプロバイダーに再委託する可能性が含まれる場合には、金融機関は特に第三国に設立されたICT再委託事業者の場合に当該再委託に関して生じ得る便益及びリスクを比較検討するものとする。

   契約上の取り決めが重要または重大な機能を支援する ICT サービスに関連する場合、金融機関は、ICT サードパーティサービスプロバイダーが破産した場合に適用される倒産法の規定及び金融機関のデータの緊急復旧に関して生じる可能性のある制約を十分に考慮するものとする。

   重要または重大な機能を支援する ICT サービスの利用に関する契約上の取り決めが、第三国に設立された ICT サードパーティサービスプロバイダーと締結される場合、金融機関は第 2 サブパラグラフに規定される考慮事項に加え、当該第三国における EU データ保護規則の遵守及び法律の効果的な執行についても考慮するものとする。

   重要または重大な機能を支援する ICT サービスの利用に関する契約上の取り決めにおいて、再委託が規定されている場合、金融機関は、潜在的に長い又は複雑な再委託の連鎖が、契約上の機能を十分に監視する自らの能力、及びその点において金融機関を効果的に監督する所管当局の能力に影響を及ぼすか否か、また影響を及ぼす場合にはどのような影響があるのかを評価するものとする。

（仮訳）

第 30 条

主要な契約条項

1. 金融機関及びICTサードパーティサービスプロバイダーの権利及び義務は、明確に配分され、書面に記載されなければならない。完全な契約にはService Level Agreement（SLA）を含めるものとし、当事者が紙で入手できる1つの文書、又はダウンロード可能で耐久性がありアクセス可能な別の形式の文書にて文書化するものとする。

2. ICTサービスの利用に関する契約上の取り決めには、少なくとも次の要素を含めるものとする。

(a) ICTサードパーティサービスプロバイダーが提供する全ての機能及びICTサービスの明確かつ完全な記述であって、重要または重大な機能を支援するICTサービスの再委託又はその重要な部分が許可されているか否かを示し、許可されている場合には当該再委託に適用される条件を示すもの

(b) 契約又は再委託した機能及びICTサービスが提供され、保存場所を含むデータが処理される場所、すなわち地域又は国、及びICTサードパーティサービスプロバイダーがその場所を変更する場合には、事前に金融機関に通知することを定めた要件

(c) 個人データを含むデータの保護に関する可用性、真正性、完全性及び機密性に関する規定

(d) ICTサードパーティサービスプロバイダーの倒産、破綻処理若しくは事業活動の停止が発生した場合、又は契約上の取り決めが終了した場合に、金融機関が処理した個人データ及び非個人データへのアクセス、同データの回復及び容易にアクセス可能な形式での返却を保証するための規定

(e) 更新及び改訂を含むサービスレベルの記述

(f) 金融機関に提供するICTサービスに係るICTインシデントが発生した場合は追加費用を請求することなく、又は事前に定められた費用にて金融機関を支援するというICTサードパーティサービスプロバイダーの義務

(g) ICTサードパーティサービスプロバイダーが、主管当局および金融機関の破綻処理当局、その指名した者を含む関係者と全面的に協力する義務

(h) 解約権、及び所管当局と破綻処理機構の想定に基づいて契約上の取り決めを解約するにあたっての最低通知期間

(i) ICTサードパーティサービスプロバイダーが、第13条第6項に基づいて金融機関のICTセキュリティ意識向上プログラム及びデジタル・オペレーショナル・レジリエンス研修に参加するための条件。

3. 重要または重大な機能を支援するICTサービスの利用に関する契約上の取り決めには、第2項に規定される要素に加え、少なくとも次の事項を含めるものとする。

(a) 更新と改定されたものを含んだ完全なサービスレベルの記述と、明確な定量的・定性的パフォーマンス目標を含むこと。これにより、金融機関がICTサービスの監視を有効に行い、合意されたサービスレベルが達成されなかった場合に速やかに是正措置が取れるようにする。

(b) 金融機関に対するICTサードパーティサービスプロバイダーによる通知期間及び報告義務。合意されたサービスレベルに沿って重要または重大な機能を支援するICTサービスを効果的に提供するICTサードパーティサービスプロバイダーの能力に重大な影響を及ぼす可能性のある事象の通知を含む

(c) ICTサードパーティサービスプロバイダーが、規制の枠組みに沿ってビジネスコンティンジェンシープランを実施・テストし、金融機関によるサービスの提供に適切なレベルのセキュリティを提供するICTセキュリティ対策、ツール及び方針を整備するための要件

(d) 第26条及び第27条に規定される金融機関のTLPTに参加し、全面的に協力するというICTサードパーティサービスプロバイダーの義務

(e) ICTサードパーティサービスプロバイダーのパフォーマンスを継続的に監視する権利。これには以下が含まれる。

(i) 金融機関又は指定されたサードパーティ及び所管当局による無制限のアクセス権、検査権及び監査権、並びにICTサードパーティサービスプロバイダーの業務にとって重要である場合に関連文書の写しを現地で入手する権利であって、その効果的な行使が他の契約上の取り決め若しくは実施方針によって妨げられたり制限されたりすることのない権利

(ii) 他の顧客の権利が影響を受ける場合に代替的な保証レベルに合意する権利

(iii) 所管当局、主監督者、金融機関、又は指定されたサードパーティが実施する現地調査及び監査において全面的に協力するというICTサードパーティサービスプロバイダーの義務

(iv) 当該検査及び監査の範囲、従うべき手続及び頻度に関する詳細を提供する義務

(f) 特に次のような義務的かつ適切な移行期間を設定する出口戦略

(i) 金融機関における事業中断のリスクを軽減する、又は金融機関が破綻処理及び再編を効果的に実施できるようにするために、ICTサードパーティサービスプロバイダーがそれぞれの機能又はICTサービスの提供を継続する期間。

（ii）金融機関が提供されるサービスの複雑さに応じて別のICTサードパーティサービスプロバイダーに移行したり、社内ソリューションに切り替えたりすることが可能である期間。

（e）の例外として、ICT サードパーティサービスプロバイダーと小規模事業者である金融機関は、金融機関のアクセス権、検査権及び監査権を ICT サードパーティサービスプロバイダーによって指名された独立したサードパーティに委任すること、かつ、金融機関は常に ICT サードパーティサービスプロバイダーのパフォーマンスに関する情報及び保証をサードパーティに要求することが可能であることに同意することができる。

4. 金融機関及びICTサードパーティサービスプロバイダーは、契約上の取り決めを交渉する際には特定のサービスについて公的機関が作成した標準的な契約条項を使用することを考慮するものとする。

5. ESAは、第2項（a）に規定される要素をさらに具体化するため、合同委員会を通じて規制技術基準の草案を作成するものとし、かかる要素は、金融機関が重要または重大な機能を支援するICTサービスを再委託する際に決定し評価する必要がある。

この規制技術基準の草案を作成する際には、ESA は、金融機関の規模及び全体的なリスク特性並びにそのサービス、活動及び業務の性質、規模及び複雑性を考慮するものとする。

ESA は、この規制技術基準の草案を 2024 年 7 月 17 日までに欧州委員会に提出するものとする。

規則（EU）No 1093/2010、（EU）No 1094/2010 及び（EU）No 1095/2010 第 10 条から第 14 条に従い、第 1 サブパラグラフに規定される規制技術基準を採択することによって本規則を補足する権限が欧州委員会に委任される。

（仮訳）

第 2 節

重要な ICT サードパーティサービスプロバイダーの監督フレームワーク

第 31 条

重要な ICT サードパーティサービスプロバイダーの指定

1. ESAは、合同委員会を通じて、かつ、第32条(1)に従って設置された監督フォーラムの勧告に基づき、次のことを行う。

(a) 第2項に規定する基準を考慮した評価を経て、金融機関にとって重要なICTサードパーティサービスプロバイダーを指定する。

1. 重要なICTサードパーティサービスプロバイダーそれぞれに対し、規則(EU) No 1093/2010、(EU) No 1094/2010又は(EU) No 1095/2010に従って、当該金融機関の個々の貸借対照表の合計により立証されるように、各ESAが責任を負う金融機関の総資産額を合計した場合に、当該重要なICTサードパーティサービスプロバイダーのサービスを利用している全ての金融機関の総資産額に占める割合が最大となるESAを主監督者として任命する。

2. 第1項(a)にいう指定は、ICTサードパーティサービスプロバイダーが提供するICTサービスに関して、以下の全ての基準に基づくものとする。

(a) 当該ICTサードパーティサービスプロバイダーがサービスの提供に大きな支障をきたすこととなった場合、当該ICTサードパーティサービスプロバイダーがサービスを提供する金融機関の数及び金融機関の資産の総額等を勘案し、当該金融サービスの提供の安定性、継続性又は品質にもたらされるシステミックな影響

(b) 以下のパラメータに従って評価された、当該ICTサードパーティサービスプロバイダーに依存する金融機関のシステミックな性質又は重要性

(i) 各ICTサードパーティサービスプロバイダーに依存するグローバルなシステム上重要な機関（G-SII）又はその他のシステム上重要な機関（O-SII）の数

(ii) (i)にいうG-SII又はO-SIIと他の金融機関との間の相互依存関係（G-SII又はO-SIIが他の金融機関に対して金融インフラサービスを提供する場合を含む）

(c) 金融機関が再委託協定を通じて直接的又は間接的に当該サービスに依存しているか否かを問わず、最終的に同ICTサードパーティサービスプロバイダーが関与する金融機関の重要または重大な機能に関連して、当該ICTサードパーティサービスプロバイダーが提供するサービスに金融機関が依存していること

(d) 以下のパラメータを考慮したICTサードパーティサービスプロバイダーの代替性の程度

(i) 特定の市場で活動しているICTサードパーティサービスプロバイダーの数が限られていること、当該ICTサードパーティサービスプロバイダーの市場シェア、独自技術に関連するものを含む技術的複雑さ又は高度さ、ICTサードパーティサービスプロバイダーの組織又は活動に特有の特徴に起因する、部分的でも真の代替の欠如

(ii) 移行プロセスに伴う多額の財務コスト、時間若しくはその他の資源、又はそのような移行を通じて金融機関がさらされる可能性のあるICTリスク等のオペレーショナルリスクの増加により、関連するデータ及びワークロードの一部又は全部を、当該ICTサードパーティサービスプロバイダーから他のICTサードパーティサービスプロバイダーに移行することが困難であること

3. ICTサードパーティサービスプロバイダーがグループに属する場合には、第2項にいう基準は、グループ全体が提供するICTサービスに関連して考慮されるものとする。

4. グループの一部である重要なICTサードパーティサービスプロバイダーは、主監督者との適切な表明及びコミュニケーションを確保するため、調整窓口となる者を一人指名する。

5. 主監督者は、第1項(a)にいう指定に至る評価の結果をICTサードパーティサービスプロバイダーに通知するものとする。ICTサードパーティサービスプロバイダーは、通知日から6週間以内に、評価のための関連情報を記載した陳述書を主監督者に提出することができる。主監督者は、陳述書を検討するものとし、当該陳述書の受領から30暦日以内に追加情報を提出するよう要請することができる。

ESA は、重要な ICT サードパーティサービスプロバイダーとして指定した後、合同委員会を通じて、その指定及び実質的に監督活動の対象となる開始日を同 ICT サードパーティサービスプロバイダーに通知するものとする。開始日は、通知後 1 ヶ月以内とする。同 ICT サードパーティサービスプロバイダーは、サービスを提供する金融機関に対して、重要な ICT サードパーティサービスプロバイダーとして指定された旨を通知しなければならない。

6. 欧州委員会は、2024年7月17日までに、本条第2項にいう基準をさらに詳細に定めることによって本規則を補足するために、第57条に従って委任法令を採択する権限を与えられる。

7. 第1項(a)にいう指定は、欧州委員会が第6項に従って委任法令を採択するまで使用してはならない。

8. 第1項(a)にいう指定は、以下には適用しないものとする。

(a) 他の金融機関にICTサービスを提供する金融機関

(b) EUの機能に関する条約第127条(2)で言及されている任務を支援する目的で設立された監督フ

レームワークの対象となるICTサードパーティサービスプロバイダー

(c) グループ内ICTサービスプロバイダー

(d) ある加盟国においてのみ活動する金融機関に対して、その加盟国においてのみICTサービスを提供するICTサードパーティサービスプロバイダー

9. ESAは、合同委員会を通じて、EU全体での重要なICTサードパーティサービスプロバイダーの一覧表を毎年作成し、公表し、及び更新するものとする。

10. 第1項(a)の規定の適用上、所管当局は、第28条(3)第3サブパラグラフにいう報告書を年1回まとめ、第32条に従って設置された監督フォーラムに送付するものとする。監督フォーラムは、所管当局から入手した情報に基づいて、金融機関のICTサードパーティ依存関係を評価する。

11. 第9項にいう一覧表に含まれていないICTサードパーティサービスプロバイダーは、第1項(a)に従って重要なICTサードパーティサービスプロバイダーとして指定されるよう要請することができる。

第 1 サブパラグラフの規定の適用上、ICT サードパーティサービスプロバイダーは、理由を付した申請書を EBA、ESMA 又は EIOPA に提出しなければならず、EBA、ESMA 又は EIOPA は、合同委員会を通じて、第 1 項(a)に従って当該 ICT サードパーティサービスプロバイダーを重要な ICT サードパーティサービスプロバイダーとして指定するか否かを決定しなければならない。

第 2 サブパラグラフにいう決定は、申請の受領から 6 ヶ月以内に採択され、ICT サードパーティサービスプロバイダーに通知されなければならない。

12. ICTサードパーティサービスプロバイダーが、指定後12ヶ月以内にEU域内に子会社を設立した場合、金融機関は、第三国に設立され、第1項(a)に従って重要なICTサードパーティサービスプロバイダーと指定されたICTサードパーティサービスプロバイダーのサービスを利用しなければならない。

13. 第12項にいう重要なICTサードパーティサービスプロバイダーは、EU域内に設立された子会社の経営組織の変更について主監督者に通報しなければならない。

（仮訳）

第 32 条

監督フレームワークの構造

1. 合同委員会は、規則(EU) No 1093/2010、(EU) No 1094/2010及び(EU) No 1095/2010の第57条(1)に従って、金融セクターを横断するICTサードパーティリスク分野において、合同委員会及び第31条(1)(b)にいう主監督者の取組みを支援する目的の小委員会として、監督フォーラムを設置するものとする。監督フォーラムは、当該分野における合同委員会の共同見解及び共通行為の草案を作成する。

監督フォーラムは、ICT リスク及び脆弱性に関連する進展について定期的に議論し、EU 全体での ICT サードパーティリスクの監督に対する一貫したアプローチを促進する。

2. 監督フォーラムは、毎年、全ての重要なICTサードパーティサービスプロバイダーについて実施された監督活動の結果及び所見の総合的な評価を行い、金融機関のデジタル・オペレーショナル・レジリエンスを向上させ、ICT集中リスクに対処するためのベストプラクティスを発展させ、並びにセクター間のリスク移転の緩和策を検討するための調整措置を促進する。

3. 監督フォーラムは、規則(EU) No 1093/2010、(EU) No 1094/2010及び(EU) No 1095/2010の第56条(1)に従ってESAの共同見解として合同委員会が採択すべき重要なICTサードパーティサービスプロバイダーに関する包括的ベンチマークを提出するものとする。

4. 監督フォーラムは、次のものから成る。

(a) ESAの議長

(b) 各加盟国の、第46条にいう関連所管当局の現職の職員のうち、上級代表者1名

(c) 各ESAの理事及び、欧州委員会、ESRB、ECB、ENISAから代表者各1名がオブザーバーとして参加

(d) 必要に応じて、各加盟国から、第46条にいう所管当局の追加代表者1名がオブザーバーとして参加

(e) 該当する場合には、指令(EU) 2022/2555の対象となる不可欠な事業体又は重要な事業体であって、重要なICTサードパーティサービスプロバイダーに指定されたものの監督について責任を有する、当該指令に従って指定され、又は設立された所管当局の代表者1名がオブザーバーとして参加

監督フォーラムは、必要に応じて、第 6 項の規定に従って任命された独立した専門家の助言を求めることができる。

5. 各加盟国は、第4項第1サブパラグラフ(b)にいう上級代表者となる職員が所属する関連所管当局を指定し、主監督者に通知するものとする。

   ESA は、加盟国が指名した関連所管当局の現職の職員から選出された上級代表者の一覧表を ESA のウェブサイトで公表するものとする。

6. 第4項第2サブパラグラフにいう独立した専門家は、監督フォーラムが、公的かつ透明性のある申請手続に従って選定された専門家の集団の中から任命するものとする。

   独立した専門家は、金融の安定性、デジタル・オペレーショナル・レジリエンス及び ICT セキュリティに関する専門知識に基づいて任命される。EU 全体の利益のためだけに独立してかつ客観的に行動しなければならず、また、EU の機関又は団体、加盟国の政府又はその他の公私の団体から指示を求めたり受けたりしてはならない。

7. 規則(EU) No 1093/2010、(EU) No 1094/2010及び(EU) No 1095/2010の第16条に従って、ESAは、本節の規定の適用上、ESAと所管当局との間の協力に関するガイドラインを重要なICTサードパーティサービスプロバイダー宛てに2024年7月17日までに発行しなければならない。このガイドラインには、所管当局とESAとの間での任務の分担及び遂行に関する詳細な手順及び条件、並びに第35条(1)(d)に基づく勧告のフォローアップを所管当局が確保するために必要な情報交換に関する詳細について記載する。

8. 本節に定める要件は、指令(EU) 2022/2555及びクラウドサービスプロバイダーに適用される監督に関する他のEU規則の適用を妨げるものではない。

9. ESAは、合同委員会を通じて、監督フォーラムが実施する準備作業に基づき、毎年、本節の適用に関する報告書を欧州議会、閣僚理事会及び欧州委員会に提出するものとする。

（仮訳）

第 33 条

主監督者の任務

1. 第31条(1)(b)に従って任命された主監督者は、割り当てられた重要なICTサードパーティサービスプロバイダーの監督を行うものとし、監督に関連する全ての事項に関して、当該重要なICTサードパーティサービスプロバイダーの主要な連絡先となるものとする。

2. 主監督者は、第1項の規定の適用上、各重要なICTサードパーティサービスプロバイダーが、金融機関にもたらされる可能性のあるICTリスクを管理するための包括的、健全かつ効果的な規則、手続、仕組み及び取り決めを有しているか否かを評価する。

   第 1 サブパラグラフにいう評価は、主に、金融機関の重要または重大な機能を支援する重要な ICT サードパーティサービスプロバイダーが提供する ICT サービスに焦点を当てるものとする。関連するリスク全てに対処するために必要な場合には、その評価は、重要または重大な機能以外の機能を支援する ICT サービスにも及ぶものとする。

3. 第2項にいう評価は、以下を対象とする。

   (a) 金融機関に提供される重要なICTサービスのセキュリティ、可用性、継続性、拡張性および品質を確保するためのICT要件、ならびにデータの可用性・真正性・完全性・機密性の高い水準を常時維持できる能力

   (b) 敷地、施設、データセンターのセキュリティを含む、ICTセキュリティの確保に寄与する物理的セキュリティ

   (c) ICTリスク管理方針、ICT事業継続方針、ICT対応・復旧計画を含む、リスク管理プロセス

   (d) 効果的なICTリスク管理を可能にする、明確で透明性のある一貫した責任・説明責任体制を備えた組織構造を含む、ガバナンスの取り決め

   (e) 重大なICT関連インシデントの特定、監視及び金融機関への迅速な報告、これらのインシデントの管理及び解決、特にサイバー攻撃への対応

   (f) 金融機関による解約権の効果的な行使を確保する、データポータビリティ、アプリケーションポータビリティ及び相互運用性のための仕組み

   (g) ICTシステム、インフラ、統制のテスト

   (h) ICT監査

(i) 金融機関へのICTサービスの提供に適用される、国内及び国際的な関連基準の利用。

4. 第2項にいう評価に基づき、かつ第34条(1)にいう共同監督ネットワーク（JON）と連携して、主監督者は、各重要なICTサードパーティサービスプロバイダーについて計画された、年次監督目標及び主な監督行動を記載した、明確、詳細かつ合理的な個別の監督計画を導入するものとする。この計画について、毎年、重要なICTサードパーティサービスプロバイダーに伝達するものとする。

主監督者は、監督計画の導入に先立ち、監督計画の草案について重要な ICT サードパーティサービスプロバイダーに伝達する。

重要な ICT サードパーティサービスプロバイダーは、監督計画の草案を受領次第、15 暦日以内に、本規則の適用範囲外にある事業体である顧客への予想される影響を証明し、適切な場合にはリスクを軽減するための解決策を説明する陳述書を提出することができる。

5. 第4項にいう年次監督計画が導入され、重要なICTサードパーティサービスプロバイダーに通知された後、所管当局は、主監督者との合意がある場合にのみ、当該重要なICTサードパーティサービスプロバイダーに関する措置をとることができる。

（仮訳）

第 34 条

主監督者間の運営上の連携

1. 監督活動に対する一貫したアプローチを確保するため、また、協調的な総合的監督戦略並びに統一性のある業務アプローチ及び作業方法を可能にするため、第31条(1)(b)に従って任命された主監督者3機関は、準備段階において相互に連携し、それぞれの監督対象である重要なICTサードパーティサービスプロバイダーに対する監督活動の実施について連携するため、並びに第42条により必要とされる措置の過程において、JONを設立するものとする。

2. 第1項の規定の適用上、主監督者は、日常的な連携を実施し並びに迅速なやり取り及び対応を確保するために従うべき詳細な手続を定める共通の監督プロトコルを作成するものとする。プロトコルは、運営上の必要性、特に実際的な監督体制の進展を反映するために、定期的に改訂されなければならない。

3. 主監督者は、適宜、ECB及びENISAに対し、技術的助言の提供、実務経験の共有、JONの特定の連携会議への参加を要請することができる。

（仮訳）

第 35 条

主監督者の権限

1. 主監督者は、本節に定める義務を遂行するため、重要なICTサードパーティサービスプロバイダーに関し、次の権限を有するものとする。

(a) 第37条に従って全ての関連情報及び文書を要請すること

(b) 第38条及び第39条それぞれに従って総合的な調査及び査察を行うこと

(c) 監督活動の完了後に、本項(d)にいう勧告に関連して重要なICTサードパーティサービスプロバイダーがとった措置又は実施した改善策を記載した報告書を要請すること

(d) 第33条(3)にいう分野、特に以下に関する勧告を出すこと

(i) 特定のICTセキュリティ及び品質要件又はプロセスの利用であって、特に、金融機関に提供されるサービスのICTセキュリティを確保するために、主監督者が適切と考えるパッチ、アップデート、暗号化及びその他のセキュリティ対策のロールアウトに関連するもの

(ii) 主要監督官によって関連性があると認められた条件や条項およびその技術的な実装に基づき、重要なICTサードパーティサービスプロバイダーが金融機関にICTサービスを提供する際、単一障害点の発生やその拡大を防止し、ICT集中リスクが発生した場合にもEUの金融セクター全体へのシステミックな影響を最小限に抑えられるようにすること。

(iii) 再委託の計画であって、主監督者が、第37条及び第38条に従って収集された情報の検討に基づき、重要なICTサードパーティサービスプロバイダーが第三国で設立されたICTサードパーティサービスプロバイダー又はICT再委託業者との間で締結することを計画している再委託協定を含む再委託の追加的な取り決めが、金融機関によるサービスの提供に対するリスク又は金融の安定性に対するリスクを引き起こす可能性があると判断するもの

(iv) 以下の累積的な条件が満たされる場合には、再委託の追加的な取り決めを締結してはならない。

— 想定される再委託先が第三国に所在する ICT サードパーティサービスプロバイダー又は ICT 再委託業者である場合

— 再委託が金融機関の重要または重大な機能に関係するものである場合

— 主監督者が、そのような再委託の使用が、金融機関が監督上の要件を遵守する能力を含め、EUの金融の安定性又は金融機関に対して明白かつ重大なリスクをもたらすと判断する場合。

本号(iv)の規定の適用上、ICT サードパーティサービスプロバイダーは、第 41 条(1)(b)にいうテンプレートを用いて、再委託に関する情報を主監督者に送付しなければならない。

2. 主監督者は、本条にいう権限を行使するに当たり、次のことを行うものとする。

(a) JON内での定期的な連携を確保し、特に重要なICTサードパーティサービスプロバイダーの監督に関しては、必要に応じて一貫したアプローチを追求する

(b) 指令(EU) 2022/2555の規定に従って重要なICTサードパーティサービスプロバイダーに適用される可能性のある技術的及び組織的措置との重複を避けるため、同指令により制定された枠組みを十分に考慮し、必要な場合には、同指令に従って指定され又は設立された関連所管当局と協議する

(c) 本規則の適用範囲外の事業体である顧客に対して重要なICTサードパーティサービスプロバイダーが提供するサービスが中断されるリスクを可能な限り最小化するよう努める。

3. 主監督者は、第1項にいう権限を行使する前に、監督フォーラムと協議するものとする。

第 1 項(d)に従って勧告を出す前に、主監督者は、ICT サードパーティサービスプロバイダーに対し、30 暦日以内に、本規則の適用範囲外の事業体である顧客に予想される影響を証明する関連情報を提供し、適切な場合にはリスクを軽減するための解決策を説明する機会を与えなければならない。

4. 主監督者は、第1項(a)及び(b)にいう権限の行使の結果をJONに伝達するものとする。主監督者は、第1項(c)にいう報告書をJON及び当該重要なICTサードパーティサービスプロバイダーのICTサービスを利用する金融機関の所管当局に対し、不当に遅滞することなく送付する。

5. 重要なICTサードパーティサービスプロバイダーは、主監督者と誠実に協力し、その任務の遂行を援助する。

6. 第1項(a)、(b)及び(c)に基づく権限の行使に従ってとることを要求される措置の全部又は一部が遵守されない場合において、重要なICTサードパーティサービスプロバイダーが各措置の通告を受領した日から少なくとも30暦日の期間が経過した後、主監督者は、重要なICTサードパーティサービスプロバイダーに当該措置を遵守させるための期間的な制裁金の支払いを科す決定を採択するものとする。

7. 第6項にいう期間的な制裁金の支払いは、遵守が達成されるまで毎日、期間的な制裁金の支払いを科す決定が重要なICTサードパーティサービスプロバイダーに通報された後、最長6か月の範囲で科されるものとする。

8. 期間的な制裁金の支払いを科す決定に定める日から換算される期間的な制裁金の支払額は、重要なICTサードパーティサービスプロバイダーの前事業年度の日平均世界売上高の1%を上限とする。主

監督者は、制裁金の支払額を決定するにあたり、第6項にいう措置の不遵守に関する次の基準を考慮する。

(a) 不遵守の重大性及び期間

(b) 不遵守が故意によるものか過失によるものか

(c) ICTサードパーティサービスプロバイダーと主監督者との連携の程度

第 1 サブパラグラフの規定の適用上、一貫したアプローチを確保するため、主監督者は、JON 内で協議を行う。

9. 制裁金の支払いは、行政的性質のものとし、強制力を有するものとする。執行は、査察及び立入りが実施される地域の加盟国で施行されている民事訴訟規則に準拠するものとする。当該加盟国の裁判所は、執行の不正行為に関する苦情について管轄権を有するものとする。制裁金の支払額は、EUの一般予算に配分されるものとする。

10. 主監督者は、科された全ての期間的な制裁金の支払いを一般に開示するものとする。ただし、その開示が金融市場を著しく危険にさらし、又は関係当事者に不均衡な損害を与える場合は、この限りでない。

11. 主監督者は、第6項に基づく期間的な制裁金の支払いを科す前に、手続の対象となる重要なICTサードパーティサービスプロバイダーの代表者に対し、調査結果について聴聞を受ける機会を与えるものとし、手続の対象となる重要なICTサードパーティサービスプロバイダーが意見を述べる機会が与えられた調査結果のみに基づいて決定を行う。

手続の対象となる者の被告の権利は、手続において十分に尊重される。手続の対象となる重要な ICT サードパーティサービスプロバイダーは、他者の営業秘密の保護に対する正当な利益に従うことを条件として、ファイルを閲覧する権利を有する。ファイルを閲覧する権利は、機密情報又は主監督者の内部準備文書には及ばないものとする。

（仮訳）

第 36 条

EU 域外における主監督者の権限の行使

1. 第31条(12)の目的のために設立された子会社との対話によって、又はEU域内に所在する施設において監督活動を行うことによって監督目標を達成することができない場合には、主監督者は、重要なICTサードパーティサービスプロバイダーがEUの金融機関にサービスを提供する目的で所有し又は何らかの方法で使用している第三国に所在する施設で、その事業運営、機能又はサービスに関連して、次の規定に定める権限を行使することができる。このような施設には、管理、事業若しくは運営上の事務所、施設、土地、建物その他の財産が含まれる。

(a) 第35条(1)(a)

(b) 第35条(1)(b)、第38条(2)(a)、(b)及び(d)、並びに第39条(1)及び(2)(a)

第 1 サブパラグラフにいう権限は、次の全ての条件を満たした場合にのみ、行使することができる。

(i) 第三国における査察の実施が、主監督者が本規則に基づく義務を十分かつ効果的に履行うえで必要だと考えていること

(ii) 第三国での査察がEU域内での金融機関へのICTサービスの提供に直接関係していること

(iii) 当該重要なICTサードパーティサービスプロバイダーが第三国における査察の実施に同意していること

(iv) 当該第三国の関係当局が主監督者から正式に通知を受け、異議を申し立てていないこと。

2. EBA、ESMA又はEIOPAは、EUの機関及び加盟国のそれぞれの権限を害することなく、第1項の規定の適用上、主監督者及びその指定する当該第三国での任務のためのチームによる当該第三国における査察の円滑な実施を可能とするため、当該第三国の関係当局と行政協力に関する取り決めを締結する。これらの協力の取り決めは、EU及びその加盟国について法的義務を生じさせるものではなく、また、加盟国及びその所管当局がこれらの第三国及びその関係当局と二国間又は多国間の取り決めを締結することを妨げるものではない。

これらの協力の取り決めは、少なくとも次の要素を規定するものとする。

(a) 本規則に基づいて実施される監督活動と当該第三国の関係当局が行う金融セクターにおけるICTサードパーティリスクの類似の監視を連携するための手続（主監督者及びその指定チームが第1項第1サブパラグラフにいう総合的な調査及び現地査察をその管轄の下にある地域において実施することを認める当該第三国の同意を伝達するための詳細を含む）

(b) EBA、ESMA又はEIOPAと当該第三国の関係当局との間の関連情報、特に第37条に基づき主監督者が要請することができる情報の伝達の仕組み

(c) 第三国で設立され、第31条(1)(a)に従って重要なICTサードパーティサービスプロバイダーに指定されたICTサードパーティサービスプロバイダーが、当該第三国の金融機関にサービスを提供する際に当該第三国の適用法に従って遵守することが義務付けられている要件に違反したとみなされた場合に、当該第三国の関係当局がEBA、ESMA又はEIOPAに速やかに通知する仕組み、並びに適用される是正措置及び処罰

(d) 当該第三国の金融機関のICTサードパーティリスクに対する監視に関する規制又は監督の進展に関する最新情報の定期的な伝達

(e) 必要な場合には、主監督者及びその指定チームが実施する査察に、関連する第三国当局の代表者1名の同行を認めるための条件

3. 主監督者が第1項及び第2項にいうEU域外での監督活動を実施できない場合には、主監督者は、次のことを行う。

(a) 入手可能な全ての事実及び文書に基づいて第35条に基づく権限を行使する。

(b) 本条にいう想定される監督活動を実施することができない場合に生じる結果を文書化し、説明する。

第 35 条(1)(d)に従って出される主監督者の勧告においては、本項(b)にいう潜在的結果を考慮に入れるものとする。

（仮訳）

第 37 条

情報の要請

1. 主監督者は、単純な要請又は決定により、重要なICTサードパーティサービスプロバイダーに対し、主監督者が本規則に基づく義務を遂行するために必要な全ての情報の提供を要求することができる。このような情報には、全ての関連する事業又は業務に関する文書、契約、方針、書類、ICTセキュリティ監査報告書、ICT関連インシデント報告書、並びに重要なICTサードパーティサービスプロバイダーが業務上の機能又は活動をアウトソーシングした者に関する情報が含まれる。

2. 主監督者は、第1項に基づいて情報の単純な要請を行う場合には、次のことを行う。

(a) 要請の法的根拠として本条を参照する

(b) 要請の目的を記載する

(c) 必要な情報を指定する

(d) 情報提供の期限を設定する

(e) 情報の要請先である重要なICTサードパーティサービスプロバイダーの代表者に対し、情報を提供する義務はないが、要請に対して自発的に応える場合には、提供する情報は不正確であってはならず、また誤解を招くものであってはならない旨を記載する。

3. 主監督者は、第1項に基づいて情報の提供を決定により要求する場合には、次のことを行う。

(a) 要請の法的根拠として本条を参照する

(b) 要請の目的を記載する

(c) 必要な情報を指定する

(d) 情報提供の期限を設定する

(e) 要求された情報の提出が不完全である場合、又は当該情報が本項(d)にいう期限内に提供されない場合に生じる、第35条(6)に規定された期間的な制裁金の支払いについて記載する

(f) 規則(EU) No 1093/2010、(EU) No 1094/2010及び(EU) No 1095/2010の第60条及び第61条に従って、当該決定についてESA審判部に上訴する権利、並びに当該決定について欧州司法裁判所（欧州司法裁判所）による再審理を受ける権利について記載する。

（仮訳）

4. 重要なICTサードパーティサービスプロバイダーの代表者は、要請された情報を提供するものとする。正当に権限を与えられた弁護士は、依頼人に代わって情報を提供することができる。重要なICTサードパーティサービスプロバイダーは、提供された情報が不完全、不正確又は誤解を招く場合には、継続して全面的な責任を負うものとする。

5. 主監督者は、関連する重要なICTサードパーティサービスプロバイダーのサービスを利用する金融機関の所管当局及びJONに対し、情報を提供する旨の決定の写しを遅滞なく送付するものとする。

第 38 条

総合的な調査

1. 主監督者は、本規則に基づく義務を遂行するため、必要な場合には、第40条(1)にいう共同検査チームの支援を受けて、重要なICTサードパーティサービスプロバイダーの調査を行うことができる。

2. 主監督者は、次の権限を有する。

(a) 任務の遂行に関連する記録、データ、手順その他の資料を、それらが保存されている媒体のいかんを問わず、調査すること

(b) かかる記録、データ、文書化された手順その他の資料の認証された写し又は抜粋を取得又は入手すること

(c) 重要なICTサードパーティサービスプロバイダーの代表者を召喚し、調査の対象及び目的に関連する事実又は文書について口頭又は書面による説明を求め、その回答を記録すること

(d) 調査の対象に関する情報を収集する目的で面談することに同意するその他の自然人又は法人と面談すること

(e) 電話及びデータ通信の記録を要請すること

3. 第1項にいう調査のために主監督者から委任を受けた職員その他の者は、調査の対象及び目的を明記した委任状を提示して、その権限を行使するものとする。

委任状にはまた、要求された記録、データ、文書化された手順若しくはその他の資料の提出、又は ICT サードパーティサービスプロバイダーの代表者への質問に対する回答が得られない、又は不完全である場合に生じる、第 35 条(6)に規定される期間的な制裁金の支払いについて記載しなければならない。

4. 重要なICTサードパーティサービスプロバイダーの代表者は、主監督者の決定に基づいて調査に応じる必要がある。決定には、調査の対象及び目的、第35条(6)に規定される期間的な制裁金の支払い、規則(EU) No 1093/2010、(EU) No 1094/2010及び(EU) No 1095/2010に基づいて利用可能な法的救済措置、並びに決定について欧州司法裁判所の再審理を受ける権利を明記しなければならない。

5. 主監督者は、当該重要なICTサードパーティサービスプロバイダーのICTサービスを利用する金融機関の所管当局に対し、調査予定及び委任を受けた者の身元を調査開始前の適切な時期に通知するものとする。

主監督者は、第 1 サブパラグラフの規定に従って送付される全ての情報を JON に伝達するものとする。

第 39 条

（仮訳）

査察

1. 本規則に基づく業務を遂行するために、主要監督官は第40条第1項で言及されている合同調査チームの支援を受け、ICTサードパーティサービスプロバイダーの本社、運用センター、支店などの事業所、土地、財産に立ち入り、必要な現地調査をすべて実施できるほか、遠隔による調査も行うことができる。

   第 1 サブパラグラフにいう権限を行使する目的で、主監督者は、JON と協議するものとする。

2. 現地査察の実施について、主監督者から委任を受けた職員その他の者は、次のことを行う権限を有する。

   (a) 当該事業施設、土地又は財産に立入ること

   (b) 査察の期間中及び査察に必要な範囲において、当該事業施設への立入りや帳簿又は記録へのアクセスを禁止すること

   主監督者から委任を受けた職員及びその他の者は、当該重要な ICT サードパーティサービスプロバイダーの代表者が査察を受け入れない場合には、査察の対象及び目的並びに第 35 条(6)に規定する期間的な制裁金の支払いを明記した委任状を提示して、その権限を行使する。

3. 主監督者は、査察の開始前に適切な時期に、当該ICTサードパーティサービスプロバイダーを利用する金融機関の所管当局に通知するものとする。

4. 査察は、金融機関へのICTサービスの提供に使用され、又は貢献する関連ICTシステム、ネットワーク、機器、情報及びデータの全範囲を対象とする。

5. 主監督者は、予定されている現地査察の前に、重要なICTサードパーティサービスプロバイダーに対して合理的な通知を行うものとする。ただし、緊急事態若しくは危機的状況のために当該通知を行うことができない場合、又は当該通知によって査察若しくは監査がもはや有効でなくなるような状況をもたらす場合は、この限りでない。

6. 重要なICTサードパーティサービスプロバイダーは、主監督者の決定により命じられる現地査察を受け入れるものとする。決定には、査察の対象及び目的を明記し、査察の開始日を定め、第35条(6)に規定される期間的な制裁金の支払い、規則(EU) No 1093/2010、(EU) No 1094/2010及び(EU) No 1095/2010に基づいて利用可能な法的救済措置、並びに当該決定について欧州司法裁判所の再審理を受ける権利について記載するものとする。

7. 重要なICTサードパーティサービスプロバイダーが本条の規定に基づいて命じられた査察に異議を申し立てたと主監督者からの委任を受けた職員その他の者が認める場合には、主監督者は、そのような

（仮訳）
異議によって生じる結果（関連する金融機関の所管当局が金融機関に対し当該重要なICTサードパーティサービスプロバイダーと締結した契約の取り決めを解除するよう要求する可能性を含む）を重要なICTサードパーティサービスプロバイダーに伝達するものとする。

（仮訳）

第 40 条

継続的な監督

1. 主監督者は、監督活動、特に総合的な調査又は査察を行う際に、重要なICTサードパーティサービスプロバイダーごとに設置される共同検査チームの支援を受けるものとする。

2. 第1項にいう共同検査チームは、次の機関の職員から成る。

   (a) ESA

   (b) 重要なICTサードパーティサービスプロバイダーがICTサービスを提供する金融機関を監督する関連所管当局

   (c) 第32条(4)(e)にいう各国の所管当局（任意）

   (d) 重要なICTサードパーティサービスプロバイダーが設立されている加盟国の各国の所管当局（任意）

   共同検査チームの構成員は、ICT 及びオペレーショナルリスクに関する専門知識を有するものとする。共同検査チームは、指名された主監督者職員（「主監督者コーディネーター」）の連携の下で活動するものとする。

3. 主監督者は、監督フォーラムと協議した後、調査又は査察の終了後3ヶ月以内に、第35条にいう権限に従って重要なICTサードパーティサービスプロバイダーに対して出す勧告を採択するものとする。

4. 第3項にいう勧告は、重要なICTサードパーティサービスプロバイダー及び同サービスプロバイダーがICTサービスを提供する金融機関の所管当局に直ちに伝達するものとする。

   監督活動を遂行する目的で、主監督者は、関連するサードパーティ認証、及び重要な ICT サードパーティサービスプロバイダーが公開している ICT サードパーティ内部又は外部監査報告書を考慮に入れることができる。

（仮訳）

第 41 条

監督活動の実施を可能にする条件の整合化

ESA は、合同委員会を通じて、以下を規定する規制技術基準の草案を作成するものとする。

(a) 第31条(11)に基づいて、重要なICTサードパーティサービスプロバイダーに指定されることを自発的に要請するための申請においてICTサードパーティサービスプロバイダーが提供すべき情報

(b) 第35条(1)の規定によりICTサードパーティサービスプロバイダーが提出、開示又は報告を行う情報の内容、構成及び様式（再委託契約の取り決めに関する情報を提供するためのテンプレートを含む）

(c) ESAsおよび関係する管轄当局の職員がバランスよく参加することを確保するための、共同調査チームの構成要件、および任命方法・任務・業務運営の詳細。

(d) 第42条(3)の規定による主監督者の勧告に基づいて重要なICTサードパーティサービスプロバイダーがとった措置に関する所管当局の評価の詳細。

1. ESAは、これらの規制技術基準の草案を2024年7月17日までに欧州委員会に提出するものとする。

規則(EU) No 1093/2010、(EU) No 1094/2010 及び(EU) No 1095/2010 の第 10 条から第 14 条に規定された手順に従って、第 1 項にいう規制技術基準を採択することによって本規則を補足する権限を欧州委員会に委任する。

（仮訳）

第 42 条

所管当局によるフォローアップ

1. 第35条(1)(d)に従って主監督者が出した勧告を受領してから60暦日以内に、重要なICTサードパーティサービスプロバイダーは、主監督者に対し、当該勧告に従う意思を通知するか、又は当該勧告に従わない理由を提供するものとする。主監督者は、この情報を直ちに関連する金融機関の所管当局に伝達する。

2. 主監督者は、重要なICTサードパーティサービスプロバイダーが第1項の規定に従って主監督者に通知しなかった場合又は重要なICTサードパーティサービスプロバイダーが提供した説明が十分でないと認められる場合には、これを公表する。公表される情報は、重要なICTサードパーティサービスプロバイダーの身元並びに不遵守の種類及び性質に関する情報を開示するものとする。だたし、公表が関係者に過度の損害を与える場合や、金融市場の秩序ある機能や統合性、またはEU全体または一部の金融システムの安定性を著しく危険にさらす可能性がある場合は除く。

   主監督者は、その情報開示について ICT サードパーティサービスプロバイダーに通知する。

3. 所管当局は、第35条(1)(d)に従って重要なICTサードパーティサービスプロバイダーに対して出された勧告で特定されたリスクを、関連する金融機関に通知するものとする。

   金融機関は、ICT サードパーティリスクを管理する際に、第 1 サブパラグラフにいうリスクを考慮に入れなければならない。

4. 所管当局は、金融機関がICTサードパーティリスクの管理において勧告で特定された特定のリスクを考慮しておらず、又は十分に対処していないと認める場合には、所管当局は第 6 項に基づく決定が取られる可能性を通知し、適切な契約上の取り決めがない場合は通知を受けてから60暦日以内にその決定が行われる可能性を示す。

5. 所管当局は、第35条(1)(c)にいう報告書を受領した後、本条第6項にいう決定を下す前に、任意で、指令(EU) 2022/2555に従って指定され又は設立された所管当局であって、当該指令の対象となる不可欠な事業体又は重要な事業体であって重要なICTサードパーティサービスプロバイダーとして指定されたものの監督に責任を有するものと協議することができる。

6. 所管当局は、最後の手段として、第50条の規定に従い、本条第4項及び第5項に規定する通知並びに適当な場合には協議の後、重要なICTサードパーティサービスプロバイダーに対する勧告において特定されたリスクに対処するまでの間、同重要なICTサードパーティサービスプロバイダーが提供するサービスの利用又は展開を部分的に又は完全に一時的に停止することを金融機関に要求する決定を下すことができる。必要な場合には、~~同~~重要なICTサードパーティサービスプロバイダーとの間で締結された関連する契約上の取り決めの一部又は全部を解除するよう金融機関に要求することができる。

7. 重要なICTサードパーティサービスプロバイダーが、主監督者が助言したアプローチとは異なるアプローチに基づいて勧告を受け入れることを拒否し、そのような異なるアプローチが多数の金融機関又は金融セクターの大部分に悪影響を及ぼす可能性があり、かつ、所管当局によって発行された個別の警告が、金融の安定性に対する潜在的なリスクを軽減する一貫したアプローチにつながらなかった場合、主監督者は、監督フォーラムと協議した後、適宜、一貫した統合的な監督上のフォローアップ措置を促進するために、所管当局に対して拘束力のない、非公開の意見を出すことができる。

8. 第35条(1)(c)にいう報告書を受領した後、所管当局は、本条第6項にいう決定を下す際に、以下の基準を考慮に入れて、重要なICTサードパーティサービスプロバイダーが対処していないリスクの種類と程度、並びに不遵守の重大性を考慮するものとする。

(a) 不遵守の重大性及び期間

(b) 不遵守によって重要なICTサードパーティサービスプロバイダーの手続、管理体制、リスク管理及び内部統制に重大な弱点があることが明らかになったか

(c) 金融犯罪が不遵守によって助長された、若しくは引き起こされたか、又はその他の形で不遵守に起因するものであったか

(d) 不遵守が故意によるものか過失によるものか

(e) 契約の一時停止または終了が金融機関の事業運営の継続にリスクをもたらすかどうか、ただし金融機関がサービス提供の中断を回避する努力を行っている場合

(f) 該当する場合には、指令（EU）2022/2555に従って指定または設立され、その指令の対象となる重要または本質的な事業体の監督を担当し、かつ重要なICTサードパーティサービスプロバイダーとして指定された事業体に関する主管当局の意見を、当該条項第5項に基づき任意で求めることができる。主管当局は、金融機関がデジタル・オペレーショナル・レジリエンスへの悪影響を回避し、記事28で言及されている出口戦略や移行計画を実施できるよう、重要なICTサードパーティサービスプロバイダーとの契約上の取り決めを調整するために必要な期間を金融機関に与えなければならない

10. 本条第6項にいう決定は、第32条(4)(a)、(b)及び(c)にいう監督フォーラムのメンバー並びにJONに通知されるものとする。

第 6 項に規定する決定の影響を受ける重要な ICT サードパーティサービスプロバイダーは、影響を受ける金融機関と、特に契約上の取り決めの停止又は解除の過程において、十分に協力する。

11. 所管当局は、主監督者に対し、主監督者が重要なICTサードパーティサービスプロバイダーに対して出した勧告の一部又は全部を同サービスプロバイダーが受け入れていない場合に、その監督任務において金融機関に関連してとったアプローチ及び措置並びに金融機関が締結した契約上の取り決めにつ

いて、定期的に伝達するものとする。

12. 主監督者は、要請に応じ、出した勧告について更なる説明を行い、フォローアップ措置について所管当局に指針を提供することができる。

（仮訳）

第 43 条

監督手数料

1. 主監督者は、本条第2項で言及される委任法に従い、重要なICTサービスプロバイダーに対し、本規則に基づく監督業務の実施に関連する必要経費を完全にカバーする手数料を請求する。この経費には、第40条で言及される合同調査チームによる作業に起因する可能性のある費用の償還、および第32条(4)第2サブパラグラフで言及される独立専門家による助言の費用（直接監督活動の範囲に該当する事項に関連するもの）も含まれる。

   重要な ICT サードパーティサービスプロバイダーに課される手数料の額は、本節に規定する義務の履行から生じる全ての費用をカバーし、かつ、同サービスプロバイダーの売上高に相応するものとする。

2. 欧州委員会は、2024年7月17日までに手数料の額及びその納付方法を決定することにより、本規則を補足するために第57条に従って委任法令を採択する権限を有する。

（仮訳）

第 44 条

国際協力

1. 第36条を損なうことなく、EBA、ESMA及びEIOPAは、規則(EU) No 1093/2010、(EU) No 1095/2010及び(EU) No 1094/2010のそれぞれ第33条に従って、第三国の規制及び監督当局と行政取り決めを締結することができる。特にICTリスクの管理の実施及び統制、緩和措置並びにインシデント対応の見直しに関するベストプラクティスを開発することにより、様々な金融セクターにわたるICTサードパーティリスクに関する国際協力を促進する。

2. ESAは、合同委員会を通じて、第1項にいう第三国の当局との間で行われた関連協議の結果を要約した共同機密報告書を5年ごとに欧州議会、閣僚理事会及び欧州委員会に提出するものとする。この報告書は、ICTサードパーティリスクの発展並びに金融の安定性、市場の健全性、投資家の保護及び域内市場の機能に対する影響に焦点を当てるものとする。

（仮訳）

第 6 章

情報共有の取り決め

第 45 条

サイバー脅威情報及びインテリジェンスに関する情報共有の取り決め

1. 金融機関は、サイバー脅威情報及びインテリジェンス（侵害の痕跡（IoC）、戦術、技術及び手順、サイバーセキュリティアラート及び設定ツールを含む）を相互に共有することができる。ただし、当該情報及びインテリジェンスの共有が次の条件を満たす場合に限る。

   (a) 特にサイバー脅威に関する意識の向上、サイバー脅威の拡散能力の制限又は阻害、防衛能力、脅威検知技術、緩和戦略又は対応及び復旧段階の支援を通じて、金融機関のデジタル・オペレーショナル・レジリエンスを強化することを目的とすること

   (b) 金融機関の信頼できるコミュニティ内で行われること

   (c) 共有される情報の潜在的な機密性を保護し、かつ、ビジネスの機密性を完全に尊重する行動規則、規則(EU) 2016/679に従った個人データの保護、及び競争政策に関するガイドラインに準拠する情報共有の取り決めによって実施されること。

2. 第1項(c)の規定の適用上、情報共有の取り決めは、参加条件を定めるものとし、また、適切な場合には、公的機関の関与及び公的機関が情報共有の取り決めに関与することができる立場、ICTサードパーティサービスプロバイダーの関与並びに専用のITプラットフォームの利用を含む運用上の要素に関する詳細を定める。

3. 金融機関は、第1項にいう情報共有の取り決めへの参加について、加入又は、適当な場合には、脱退の認証の効力が生じた後直ちに、所管当局に通知するものとする。

第 7 章

所管当局

第 46 条

所管当局

本規則第 5 章第 2 節にいう重要な ICT サードパーティサービスプロバイダーの監督フレームワークの規定を害することなく、本規則の遵守は、以下の所管当局により、それぞれの法令により与えられた権限に従って確保されるものとする。

(a) 信用機関及び指令2013/36/EUに従って適用を免除される機関については、当該指令の第4条に従って指定される所管当局、規則(EU) No 1024/2013の第6条(4)に従って重要と分類された信用機関については、同規則によって与えられた権限及び任務に従うECB

(b) 指令(EU) 2015/2366に従って適用を免除される決済サービス機関を含む決済サービス機関、電子マネー事業者指令2009/110/ECに従って適用を免除される機関を含む電子マネー事業者、及び指令(EU) 2015/2366の第33条(1)にいうアカウント情報サービスプロバイダーについては、指令(EU) 2015/2366の第22条に従って指定される所管当局

(c) 投資会社については、欧州議会及び閣僚理事会の指令(EU) 2019/2034[38]の第4条に従って指定される所管当局

(d) 暗号資産市場及びアセット参照型トークンの発行者に関する規則に基づいて認可された暗号資産サービスプロバイダーについては、同規則の関連規定に従って指定される所管当局

(e) 証券集中保管機関については、規則(EU) No 909/2014の第11条に従って指定される所管当局

(f) 中央清算機関については、規則(EU) No 648/2012の第22条に従って指定される所管当局

(g) 取引所及びデータ報告サービスプロバイダーについては、指令2014/65/EUの第67条に従って指定される所管当局、及び規則(EU) No 600/2014の第2条(1)(18)に定められる所管当局

(h) 取引情報蓄積機関については、規則(EU) No 648/2012の第22条に従って指定される所管当局

(i) ファンド運用者については、指令2011/61/EUの第44条に従って指定される所管当局

---

[38] 指令 2002/87/EC、2009/65/EC、2011/61/EU、2013/36/EU、2014/59/EU 及び 2014/65/EU を改訂する、投資会社の健全性監督に関する 2019 年 11 月 27 日付欧州議会及び閣僚理事会の指令(EU) 2019/2034（OJ L 314、5.12.2019、p.64）

(j) 運用会社については、指令2009/65/ECの第97条に従って指定される所管当局

(k) 保険及び再保険事業者については、指令2009/138/ECの第30条に従って指定される所管当局

(l) 保険仲介業者、再保険仲介業者及び補助保険仲介業者については、指令(EU) 2016/97の第12条に従って指定される所管当局

(m) 職域年金基金については、指令(EU) 2016/2341の第47条に従って指定される所管当局

(n) 信用格付業者については、規則(EC) No 1060/2009の第21条に従って指定される所管当局

(o) クリティカルベンチマークの運営機関については、規則(EU) 2016/1011の第40条及び第41条に従って指定される所管当局

(p) クラウドファンディングサービスプロバイダーについては、規則(EU) 2020/1503の第29条に従って指定される所管当局

(q) 証券化情報蓄積機関については、規則(EU) 2017/2402の第10条及び第14条(1)に従って指定される所管当局

第 47 条

指令(EU) 2022/2555 により設立された組織及び当局との協力

1. 本規則に基づいて指定される所管当局と指令(EU) 2022/2555の第14条によって設立される連携グループとの間の協力を促進し監督上の交流を可能にするため、ESA及び所管当局は、金融機関に関連する監督活動に関する事項について、連携グループの活動に参加することができる。ESA及び所管当局は、指令(EU) 2022/2555の適用を受ける不可欠な事業体又は重要な事業体であって、本規則第31条により重要なICTサードパーティサービスプロバイダーとして指定されているものに関する事項について、連携グループの活動に招待されるよう求めることができる。

2. 適切な場合には、所管当局は、指令(EU) 2022/2555に従って指定され又は設置された単一の連絡窓口及びCSIRTと協議し、情報を共有することができる。

3. 適切な場合には、所管当局は、指令(EU) 2022/2555に従って指定され又は設立された所管当局に対し、関連する技術的助言及び援助を要請することができ、また、効果的かつ迅速な対応のための連携の仕組みを設けるための協力体制を確立することができる。

4. 本条第3項にいう取り決めは、特に、指令(EU) 2022/2555の適用を受ける不可欠な事業体又は重要な事業体であって、本規則第31条により重要なICTサードパーティサービスプロバイダーとして指定されたものに関する監視及び監督活動の連携のための手続を定めることができる。これには、国内法に従った調査及び現地査察の実施に関する手続、並びに本規則に基づく所管当局と当該指令に従って指定され又は設立された所管当局との間の情報交換のための仕組みが含まれ、後者の主管当局が求める情報へのアクセスも含まれる。

（仮訳）

第 48 条

当局間の協力

1. 所管当局は、所管当局間において、また、適当な場合には主監督者と緊密に協力するものとする。

2. 所管当局及び主監督者は、本規則に基づくそれぞれの義務を遂行するために必要な重要なICTサードパーティサービスプロバイダーに関するすべての関連情報、特に主監督者の監督任務の一環として特定されたリスク、並びにとられたアプローチ及び措置に関する情報を適時に相互に交換するものとする。

第 49 条

金融セクター横断的な演習、コミュニケーション及び協力

1. ESAは、合同委員会を通じて、所管当局、指令2014/59/EUの第3条にいう破綻処理機構、ECB、規則(EU) No 806/2014の適用対象となる主体に関する情報については単一破たん処理委員会、ESRB及びENISAと適宜協力して、金融セクター間で効果的な慣行の共有を可能にし、状況把握を向上し、セクター間に共通するサイバー上の脆弱性及びリスクを特定するための仕組みを構築することができる。

   これらの機関は、コミュニケーションチャネルを開発し、EU の金融セクター全体にシステマティックな影響を及ぼす重大な国を超える ICT 関連インシデント又は関連する脅威が発生した場合に、EU レベルでの効果的な協調的対応を段階的に可能にすることを目的として、サイバー攻撃シナリオを含む危機管理及び緊急時対応演習を開発することができる。

   これらの演習は、必要に応じて、金融セクターの他の経済セクターへの依存度をテストすることもできる。

2. 所管当局、ESA及びECBは、第47条から第54条までの規定に基づく義務を遂行するため、相互に緊密に協力し、情報を交換するものとする。本規則への違反を特定して是正し、ベストプラクティスを策定して促進し、協力を促進し、解釈の一貫性を確保し、意見の相違がある場合には管轄権を越えた評価を提供するために、監督を緊密に連携しなければならない。

第 50 条

行政罰及び是正措置

1. 所管当局は、本規則に基づく義務を履行するために必要な全ての監督、調査及び制裁の権限を有するものとする。

2. 第1項にいう権限は、少なくとも次の権限を含む。

(a) 所管当局がその義務の遂行に関連すると認める文書又はあらゆる形式で保有されているデータにアクセスし、その写しを受領し又は取得すること

(b) 現地査察又は調査を実施すること。これには、次の事項を含むが、これらに限定されない。

(i) 金融機関の代表者を召喚し、口頭又は書面により調査の対象及び目的に関連する事実又は文書について説明を求め、その回答を記録すること

(ii) 調査の対象に関する情報を収集する目的で面談することに同意するその他の自然人又は法人と面談すること

(c) 本規則の要件への違反に対する是正措置及び改善措置を要求すること

3. 第52条に従って加盟国が刑事処罰を科す権利を損なうことなく、加盟国は、本規則への違反に対する適切な行政罰及び是正措置を定める規則を制定し、その効果的な実施を確保するものとする。

これらの処罰及び措置は、効果的、均衡的かつ抑止的なものでなければならない。

4. 加盟国は、所管当局に対し、本規則への違反に対して少なくとも以下の行政罰又は是正措置を適用する権限を与えるものとする。

(a) 当該自然人又は法人に対し、本規則に違反する行為の停止及び当該行為の反復の中止を要求する命令を発すること

(b) 所管当局が本規則の規定に反するとみなす慣行又は行為の一時的又は恒久的な停止を要求すること、及び当該慣行又は行為の繰り返しを防止すること

(c) 金融機関が引き続き法的要件を遵守することを確保するために、金銭的な措置を含むあらゆる種類の措置を採用すること

(d) 本規則への違反について合理的な疑いがあり、かつ、当該記録が本規則への違反に関する調査に関連する可能性がある場合には、国内法で認められている限りにおいて、通信事業者が保有する

既存のデータ通信の記録を要求すること

(e) 当該自然人又は法人の身元及び違反の性質を記載した公表文を含む公告を発すること。

5. 第2項(c)及び第4項が法人に適用される場合、加盟国は、国内法に規定された条件に従い、経営陣及び国内法に基づき違反に責任を負うその他の個人に対して、行政罰及び是正措置を適用する権限を所管当局に与えるものとする。

6. 加盟国は、第2項(c)に規定される行政罰又は是正措置を科す決定が正しく道理にかなっており、上訴権の対象であることを確保するものとする。

（仮訳）

第 51 条

行政罰及び是正措置を科す権限の行使

1. 所管当局は、適当な場合には、自国の法的枠組みに従い、第50条にいう行政罰及び是正措置を科す権限を次のとおり行使する。

(a) 直接

(b) 他の当局と協力して

(c) 他の当局への委任により、自己の責任の下で、または

(d) 所轄の司法当局への申請によって

2. 所管当局は、第50条に基づいて科される行政罰又は是正措置の種類及び程度を決定する際に、違反がどの程度故意によるものであるか又は過失に起因するものであるか、また適当な場合には、次の事項を含む他の全ての関連する状況を考慮しなければならない。

(a) 違反の重要性、重大性及び期間

(b) 違反に責任を負う自然人又は法人の責任の程度

(c) 責任を有する自然人又は法人の経済力

(d) 利益または損失を判断できる限りにおいて、責任を有する自然人又は法人が得た利益又は回避した損失の重要性

(e) 損失を判断できる限りにおいて、違反によって生じたサードパーティの損失

(f) 責任を有する自然人又は法人の所管当局に対する協力の程度。ただし、当該自然人又は法人が得た利益又は回避した損失の返還を確保する必要性を損なうものではない。

(g) 責任を負う自然人又は法人による過去の違反。

（仮訳）

第 52 条

刑事処罰

1. 加盟国は、自国の法制度において刑事罰の対象となる違反行為に関しては行政制裁または是正措置に関する規定を設けないことを選択することができる。

2. 加盟国が本規則への違反に対して刑事処罰を定めることを選択した場合、加盟国は、所管当局が、本規則への違反に対して開始された刑事捜査又は手続に関連する特定の情報を受領するために管轄内の司法当局、訴追当局又は刑事司法当局と連絡を取るために、また、本規則の目的のために協力する義務を果たす目的で他の所管当局並びにEBA、ESMA又はEIOPAに同じ情報を提供するために必要な全ての権限を有することができるよう、適切な措置が講じられていることを確認するものとする。

（仮訳）

第 53 条

通知義務

加盟国は、2025 年 1 月 17 日までに、関連する刑法規定を含め、本章を実施する法律、規則及び行政規定を欧州委員会、ESMA、EBA 及び EIOPA に通知するものとする。加盟国は、欧州委員会、ESMA、EBA 及び EIOPA に対し、その後の改訂を不当に遅滞することなく通知するものとする。

（仮訳）

第 54 条

行政罰の公表

1. 所管当局は、行政罰を科す決定であって、被処罰者が当該決定の通知を受けた後に不服申立てを行わなかったものについて、不当に遅滞することなく、その公式ウェブサイトにおいて公表するものとする。

2. 第1項にいう公表には、違反の種類及び性質、責任を有する者の身元並びに科される処罰に関する情報を含める。

3. 所管当局は、個々の事案ごとに評価を行った上で、法人については身元情報を、自然人については身元情報及び個人情報を公表することが、個人データの保護に関連するリスクを含めて不相応であり、金融市場の安定性若しくは進行中の犯罪捜査の遂行を危うくし、又は損害を判断できる限りにおいて関係者に不相応な損害を与えると認める場合には、行政罰を科する決定に関し、次のいずれかの解決策を採用するものとする。

   (a) 不公表の理由がなくなるまで公表を延期する

   (b) 国内法に従って匿名で公表する、または

   (c) (a)及び(b)に定める選択肢が、金融市場の安定性に対していかなる危険ももたらさないことを保証するには不十分であると考えられる場合、又はそのような公表が科された処罰の~~寛大さ~~軽微さに相応しないと考えられる場合には、公表を差し控える。

4. 第3項(b)に従って匿名で行政罰を公表する決定の場合は、関連する情報の公表を延期することができる。

5. 所管当局が行政罰を科す決定を公表し、それに対する不服申立てが関係司法当局に提起されている場合には、所管当局は、当該情報及び、その後の段階で、当該不服申立ての結果に関するその後の関連情報を直ちにその公式ウェブサイトに追加するものとする。行政罰を科す決定を無効とする判決についても公表するものとする。

6. 所管当局は、第1項から第4項までにいう公表が、本条の規定を適用するために必要な期間に限り、その公式ウェブサイトに掲載されることを確保するものとする。この期間は、公表後5年を超えてはならない。

（仮訳）

第 55 条

職業上の守秘義務

1. 本規則に従って受領、交換又は伝達される機密情報は、第2項に定める職業上の守秘義務の条件に従うものとする。

2. 職業上の守秘義務は、本規則に基づく所管当局のために、又はこれらの所管当局がその権限を委任した当局若しくは市場事業者又は自然人若しくは法人のために働いている又は働いたことのある全ての者に対しても適用される。これには、主管当局が契約した監査人や専門家も含まれる。

3. 職業上の守秘義務の対象となる情報は、本規則に基づく所管当局間及び指令(EU) 2022/2555に従って指定又は設立された所管当局間での情報交換を含めて、EU又は国内法の規定による場合を除き、その他の者又は当局に開示してはならない。

4. 本規則に基づいて所管当局間で交換される全ての情報のうち、事業又は経営の状況及びその他の経済的又は個人的な事項に関するものは、機密情報とみなされ、職業上の守秘義務の要件に従うものとする。ただし、所管当局が、情報伝達時に当該情報を開示する可能性について述べている場合又は当該開示が法的手続のために必要である場合は、この限りでない。

（仮訳）

第 56 条

データ保護

1. ESA及び所管当局は、本規則に基づくそれぞれの義務及び責務を遂行するために必要な場合に限り、特に、調査、査察、情報の要請、伝達、公表、評価、検証、査定及び監督計画の立案のために、個人データを取り扱うことが認められる。個人データは、規則(EU) 2016/679又は規則(EU) 2018/1725のいずれか該当する方に従って取り扱うものとする。

2. 他のセクター別法令に別段の定めがある場合を除き、第1項にいう個人データは、適用される監督義務から免責されるまで、また、係属中の裁判手続が当該データを引き続き保持することを求める場合を除き、いかなる場合も最長15年間保存されるものとする。

第 8 章

委任法令

第 57 条

委任の行使

1. 欧州委員会に与えられる委任法令を採択する権限は、本条に定める条件に従う。

2. 第31条(6)及び第43条(2)にいう委任法令を採択する権限は、2024年1月17日から5年間、欧州委員会に与えられるものとする。欧州委員会は、5年間の期間が終了する遅くとも9ヶ月前までに、権限の委任に関する報告書を作成するものとする。権限の委任は、各期間の終了の3ヶ月前までに欧州議会又は閣僚理事会がその延長に反対しない限り、同じ期間を期限として、黙示的に延長されるものとする。

3. 第31条(6)及び第43条(2)にいう権限の委任は、欧州議会又は閣僚理事会によりいつでも取消すことができる。取消しの決定は、その決定に明示された権限の委任を終了させる。取消しの効力は、欧州連合官報に当該決定が公表された日の翌日又は当該決定において指定されたそれ以降の日に発生するものとする。この決定は、既に発効している委任法令の効力には影響しない。

4. 委任法令の採択に先立ち、欧州委員会は、2016年4月13日付のより良い立法についての機関間協定に定められた原則に従って、各加盟国が指定する専門家と協議するものとする。

5. 欧州委員会は、委任法令を採択したら直ちに、欧州議会及び閣僚理事会に同時に通知するものとする。

6. 第31条(6)及び第43条(2)に従って採択された委任法令は、同法令が欧州議会及び閣僚理事会に通知されてから3ヶ月以内に欧州議会又は閣僚理事会のいずれからも反対が表明された場合に限り、又はその3ヶ月の期間終了前に欧州議会及び閣僚理事会の双方が反対する意思がない旨を欧州委員会に通知した場合に限り、効力を生じるものとする。この期間は、欧州議会又は閣僚理事会からの発議があればさらに3ヶ月延長するものとする。

（仮訳）

第 9 章

経過規定及び最終規定

第 1 節

第 58 条

見直し条項

(1) 2028年1月17日までに、欧州委員会は、必要に応じてESA及びESRBと協議した後、見直しを行い、欧州議会及び閣僚理事会に報告書を提出するものとする。適切な場合には、報告書に法制度の提案を添付する。見直しには、少なくとも以下を含めるものとする。

(a) 第31条(2)に従った重要なICTサードパーティサービスプロバイダーの指定の基準

(b) 第19条にいう重要なサイバー脅威の通知の任意性

(c) 第三国に設立された重要なICTサードパーティサービスプロバイダーの効果的な監督の確保に関する当該規定の有効性を評価することを目的として、第31条(12)にいう制度、及び第35条(1)(d)(iv)第1インデントに規定された主監督者の権限、並びにEU域内に子会社を設立する必要性。

本項目第 1 サブパラグラフの適用上、見直しには、第三国のサービスへの EU の金融機関のアクセス及び EU 市場における当該サービスの利用可能性という観点を含めて、第 31 条(12)にいう制度の分析を含めるものとし、また、本規則の適用範囲であるサービスの市場における更なる発展、当該制度の適用及び監督それぞれに関する金融機関及び金融監督当局の実際的な経験、並びに国際的なレベルでの関連規制及び監督の進展を考慮しなければならない。

(d) 営業支援自動化システムを利用する、第2条(3)(e)にいう金融機関について、そのようなシステムの利用に関する将来的な市場動向に照らして、本規則の適用範囲に含めることの妥当性

(e) 監督フレームワーク内の監視の一貫性及び情報交換の効率性を支援する上でのJONの機能及び有効性。

(2) 指令(EU) 2015/2366の見直しという文脈において、欧州委員会は、決済システム及び決済処理活動のサイバーレジリエンスを高める必要性、並びに本規則の適用範囲を決済システム運営者及び決済処理活動に関与する事業体に拡大することの適切性を評価するものとする。この評価を踏まえて、欧州委員会は、指令(EU) 2015/2366の見直しの一環として、2023年7月17日までに欧州議会及び閣僚理事会に報告書を提出するものとする。

その見直し報告書に基づき、また ESA、ECB 及び ESRB と協議した上で、欧州委員会は、必要に応じて、指令(EU) 2015/2366 の第 108 条第 2 項に従って採択する法律の提案の一部として、中央銀行による既存の監督を考慮しつつ、全ての決済システム運営者及び決済処理活動に関与する事業体が適切な監督の対象となることを確保する提案を提出することができる。

(3) 2026年1月17日までに、欧州委員会は、ESA及び欧州監査監督機関委員会と協議した上で、見直しを行い、欧州議会及び閣僚理事会に報告書を提出するものとする。適切な場合には、報告書に、法定監査人及び監査法人を本規則の適用範囲に含めることによって、又は欧州議会及び閣僚理事会の指令 2006/43/EC[39]
の改訂によって、デジタル・オペレーショナル・レジリエンスに関する法定監査人及び監査法人の要件を強化することの適切性についての法律の提案を添付する。

第 2 節

改訂

第 59 条

規則(EC) No 1060/2009 の改訂

規則(EC) No 1060/2009 を以下のとおり改訂する。

(1) 附属書I、セクションA、第4項目の第1サブパラグラフを以下のとおり置き換える。

「信用格付業者は、欧州議会及び閣僚理事会規則(EU) 2022/2554 [(*1)] に従って、健全な経営手続及び会計手続、内部統制の仕組み、効果的なリスク評価手続、ICT システム管理のための効果的なコントロール及びセーフガードを有していなければならない。

---

[39] 欧州理事会指令 78/660/EEC 及び 83/349/EEC を改訂し、閣僚理事会指令 84/253/EEC を廃止する、年次会計及び連結会計の法定監査に関する 2006 年 5 月 17 日付欧州議会及び閣僚理事会の指令 2006/43/EC（OJ L 157、9.6.2006、p.87）

※1 (EC)No1060/2009、(EU)648/2012、(EU)600/2014、(EU)909/2014、並びに(EU)2016/1011 を改定する、欧州議会および閣僚理事会による 2022 年 12 月 14 日付け(EU)2022/2554 金融セクターによるデジタル・オペレーション・レジリエンスに関する規則（OJL 333、2022/12/27、p1）

(2) 附属書IIIの第12項目を以下のとおり置き換える。

「12.当該信用格付業者は、規則(EU) 2022/2554 に従って、健全な経営手続若しくは会計手続、内部統制の仕組み、効果的なリスク評価手続、又は ICT システム管理のための効果的なコントロール若しくはセーフガードを有していない場合、又は、その時点で必要とされる意思決定手順若しくは組織体制を導入又は維持していない場合、附属書 I、セクション A、第 4 項目と併せて、第 6 条(2)に違反する。」

第 60 条

規則(EU) No 648/2012 の改訂

規則(EU) No 648/2012 を以下のとおり改訂する。

(1) 第26条を以下のとおり改訂する。

(a) 第3項を以下のとおり置き換える。

「3. CCP は、そのサービス及び活動の実施において継続性及び秩序ある機能を確保する組織体制を維持し、運用しなければならない。また、欧州議会及び閣僚理事会規則(EU) 2022/2554 [(*2)] に従って管理される ICT システムを含む、適切かつ均衡のとれたシステム、資源及び手続を採用しなければならない。

※2 (EC)No1060/2009、(EU)648/2012、(EU)600/2014、(EU)909/2014、並びに(EU)2016/1011 を改定する、欧州議会および閣僚理事会による 2022 年 12 月 14 日付け(EU)2022/2554 金融セクターによるデジタル・オペレーション・レジリエンスに関する規則（OJL 333、2022/12/27、p1）

(b) 第6項を削除する。

(2) 第34条を以下のとおり改訂する。

(a) 第1項を以下のとおり置き換える。

「1. CCP は、その機能の保全、適時の業務復旧及び同 CCP の義務の履行を確保することを目的として、適切な事業継続方針及び災害復旧計画を確立し、実施し、維持しなければならない。これには、規則(EU) 2022/2554 に従って導入し、実施する ICT 事業継続方針並びに ICT 対応及び復旧計画が含まれる。」

(b) 第3項の第1サブパラグラフを以下のとおり置き換える。

「3. 本条の一貫した適用を確保するため、ESMA は、ESCB の構成員と協議の上、事業継続方針及び災害復旧計画（ICT 事業継続方針及び災害復旧計画を除く）に最低限含むべき内容及び要件を定める規制技術基準の草案を作成するものとする。」

(3) 第56条(3)の第1サブパラグラフを以下のとおり置き換える。

「3. 本条の一貫した適用を確保するために、ESMA は、第 1 項にいう登録申請の詳細（ICT リスク管理に関連する要件の詳細を除く）を定める規制技術基準の草案を作成するものとする。」

(4) 第79条の第1項及び第2項を以下のとおり置き換える。

「1. 取引情報蓄積機関は、オペレーショナルリスクの発生源を特定し、また、規則(EU) 2022/2554 に従って管理される ICT システムを含む適切なシステム、コントロール及び手続の開発を通じて、オペレーショナルリスクを最小化しなければならない。」

「取引情報蓄積機関は、その機能の維持、適時の業務復旧及び同取引情報蓄積機関の義務の履行を確保することを目的として、適切な事業継続方針及び災害復旧計画を確立し、実施し、維持しなければならない。これには、規則(EU) 2022/2554 に従って確立される ICT 事業継続方針並びに ICT 対応及び復旧計画が含まれる。」

(5) 第80条の第1項を削除する。

(6) 附属書Iのセクション II を以下のとおり改訂する。

(a) (a)及び(b)を以下のとおり置き換える。

「(a) 取引情報蓄積機関は、オペレーショナルリスクの発生源を特定しない場合、又は規則(EU) 2022/2554 に従って管理される ICT システムを含む適切なシステム、コントロール及び手続の開発を

通じてオペレーショナルリスクを最小化しない場合、第 79 条(1)に違反する。

「取引情報蓄積機関は、その機能の維持、適時の業務復旧及び同取引情報蓄積機関の義務の履行を確保することを目的として、規則(EU) 2022/2554 に従って確立される適切な事業継続方針及び災害復旧計画を確立、実施又は維持しない場合、第 79 条(2)に違反する。」

(b) (c)を削除する。

(7) 附属書IIIを以下のとおり改訂する。

(a) セクションIIを以下のとおり改訂する。

(i) (c)を以下のとおり置き換える。

「(c) Tier 2 CCP は、そのサービス及び活動の実施において継続性及び秩序ある機能を確保する組織体制を維持若しくは運用しない場合、又は規則(EU) 2022/2554 に従って管理される ICT システムを含む適切かつ均衡のとれたシステム、資源若しくは手続を採用しない場合、第 26 条(3)に違反する。」

(ii) (f)を削除する。

(b) セクションIIIの(a)を以下のとおり置き換える。

「(a) Tier 2 CCP は、その機能の保全、適時の業務復旧及び同 CCP の義務の履行を確保することを目的として、規則(EU) 2022/2554 に従って設けられる適切な事業継続方針並びに対応及び復旧計画を確立、実施又は維持し、CCP が確実に業務を継続して決済予定日に決済を完了できるように、少なくとも障害発生時における全取引を復旧可能にしない場合、第 34 条(1)に違反する。」

第 61 条

規則(EU) No 909/2014 の改訂

規則(EU) No 909/2014 の第 45 条を以下のとおり改訂する。

(1) 第1項を以下のとおり置き換える。

「1.CSD は、内部及び外部双方のオペレーショナルリスクの発生源を特定し、また、欧州議会及び閣僚理事会規則(EU) 2022/2554 [*3] に従って設定され、管理される適切な ICT ツール、プロセス及び方針の展開を通して、並びに、CSD が運営する全ての証券決済システムを含む、様々な種類のオペレーショナルリスクに対するその他の関連する適切なツール、コントロール及び手続を通じて、その影響を最小化しなければならない。

(2) 第2項を削除する。

(3) 第3項及び第4項を以下のとおり置き換える。

「3.CSD は、提供するサービス及び運営する各証券決済システムについて、業務を混乱させる重大なリスクをもたらす事象の発生時に、そのサービスの保全、適時の業務復旧、及び同 CSD の義務の履行を確保することを目的として、適切な事業継続方針及び災害復旧計画を確立し、実施し、維持しなければならない。これには、規則(EU) 2022/2554 に従って確立される ICT 事業継続方針並びに ICT 対応及び復旧計画が含まれる。

第 3 項にいう計画は、CSD の参加者が確実に業務を継続して決済予定日に決済を完了できるように、障害発生時における全取引及び参加者のポジションの復旧を規定しなければならない。これには、規則(EU) 2022/2554 の第 12 条(5)及び(7)に規定されるとおり、重要な IT システムが障害発生時点から業務を再開できることを確保することも含まれる。」

(4) 第6項を以下のとおり置き換える。

「6.CSD は、自らが運営する証券決済システムの主要な参加者だけでなく、サービスプロバイダー及びユーティリティプロバイダー、その他の CSD 又はその他の市場インフラが自らの業務にもたらすリスクを特定し、監視し、管理しなければならない。要請に応じ、所管当局及び関係当局に対し、特定されたリスクに関する情報を提供しなければならない。また、ICT リスクに関連するものを除き、そのようなリスクから生ずるオペレーショナルインシデントについて、遅滞なく所管当局及び関係当局に通報する。」

(5) 第7項の第1サブパラグラフを以下のとおり置き換える。

※3 (EC)No1060/2009、(EU)648/2012、(EU)600/2014、(EU)909/2014、並びに(EU)2016/1011 を改定する、欧州議会および閣僚理事会による 2022 年 12 月 14 日付け(EU)2022/2554 金融セクターによるデジタル・オペレーション・レジリエンスに関する規則（OJL 333、2022/12/27、p1）

（仮訳）

「7. ESMA は、ESCB の構成員と緊密に協力して、第 1 項及び第 6 項にいうオペレーショナルリスク（ICT リスクを除く）並びにこれらのリスクを検証し、対処し又は最小化する方法を定める規制技術基準の草案を作成するものとする。これには、第 3 項及び第 4 項にいう事業継続方針及び災害復旧計画並びにこれらの評価方法を含むものとする。

第 62 条

規則(EU) No 600/2014 の改訂

規則(EU) No 600/2014 を以下のとおり改訂する。

(1) 第27条gを以下のとおり改訂する。

(1) 第4項を以下のとおり置き換える。

「4. APA は、欧州議会及び閣僚理事会規則(EU) 2022/2554 [*4] に規定されているネットワーク及び情報システムのセキュリティに関する要件を遵守しなければならない。

(2) 第8項の(c)を以下のとおり置き換える。

「(c) 第 3 項及び第 5 項に規定する具体的な組織的要件」

(2) 第27条hを以下のとおり改訂する。

(a) 第5項を以下のとおり置き換える。

「5. CTP は、規則(EU) 2022/2554 に規定されるネットワーク及び情報システムのセキュリティに関する要件を遵守しなければならない。」

(b) 第8項の(e)を以下のとおり置き換える。

「(e) 第 4 項に規定する具体的な組織的要件」

(3) 第27条iを以下のとおり改訂する。

第 3 項を以下のとおり置き換える。

「3. ARM は、規則(EU) 2022/2554 に規定されるネットワーク及び情報システムのセキュリティに関する要件を遵守しなければならない。」

(a) 第5項の(b)を以下のとおり置き換える。

「(b) 第 2 項及び第 4 項に規定する具体的な組織的要件」

※4 (EC)No1060/2009、(EU)648/2012、(EU)600/2014、(EU)909/2014、並びに(EU)2016/1011 を改定する、欧州議会および閣僚理事会による 2022 年 12 月 14 日付け (EU)2022/2554 金融セクターによるデジタル・オペレーション・レジリエンスに関する規則（OJL 333、2022/12/27、p1）

（仮訳）

第 63 条

規則(EU) 2016/1011 の改訂

規則(EU) 2016/1011 の第 6 条に、以下の項を追加する。

「6.クリティカルベンチマークについて、運営者は、欧州議会及び閣僚理事会規則(EU) 2022/2554 [*5] に従って、ICT システムを管理するための健全な経営手続及び会計手続、内部統制の仕組み、効果的なリスク評価手続、効果的なコントロール及び安全策を有していなければならない。

※5 (EC)No1060/2009、(EU)648/2012、(EU)600/2014、(EU)909/2014、並びに(EU)2016/1011 を改定する、欧州議会および閣僚理事会による 2022 年 12 月 14 日付け (EU)2022/2554 金融セクターによるデジタル・オペレーション・レジリエンスに関する規則（OJL 333、2022/12/27、p1）

（仮訳）

第 64 条

効力の発生及び適用

本規則は、欧州連合官報において公表された日から 20 日目に効力が生じる。

本規則は、2025 年 1 月 17 日から適用される。

本規則は、その全体において拘束力を有し、全ての加盟国で直接適用される。

2022 年 12 月 14 日、ストラスブールにて調印。

欧州議会	閣僚理事会
議長	議長
R. METSOLA	M. BEK