Deloitte.
デロイト トーマツ

金融機関のサードパーティ・サイバーセキュリティリスク管理強化
DORA本文に関連するサードパーティ管理規則の概要

デロイト トーマツ サイバー合同会社
2026年2月27日

本資料の各関連規則概要は仮訳となります

本書はDORA本文の補足文書として、以下の構成で作成されています

1．DORA本文と関連規則等の概要

DORA本文はICTリスク管理など金融機関に求める領域および当局向けのフレームワークなどの内容で構成されているほか、技術標準などの仕様が別途定められています

DORA本文の概要と構成

サードパーティ管理に関する規則

DORAの概要	
	• EUの各法令で個別に扱われてきたICTリスクに関する要件を統合し、金融機関のデジタル・レジリエンスを強化することを目指して導入された法令である。 • 2025年1月17日から適用され、銀行、保険会社、投資会社などの金融機関が、サイバー攻撃やシステム障害などのICT（情報通信技術）に関する障害に対して、対応し、復旧できるようにすることを目的としている。

DORAを構成する主な領域	対象	目的
1.ICT risk management	金融機関向け	ICTリスク管理フレームワークの構築、ガバナンス、リスク評価、保護・防御、検知、対応・復旧などのプロセスが含まれる
2.Incident reporting	金融機関向け	サイバー攻撃やシステム障害などのICTインシデントの検知、管理、報告体制。重大インシデントが発生した場合、迅速な報告が求められる。
3.Digital operational resilience testing	金融機関向け	定期的に自社システムのレジリエンスを検証するテストを実施することが求められる。
4.ICT third-party risk	金融機関向け	ICTサードパーティサービスプロバイダーの管理強化、契約、リスク評価、当局による監視などが求められる。
5.Critical Third-Party oversight	金融当局向け	重要なサードパーティプロバイダに対する直接的な監視フレームワークの構築

DORAの施行のために、技術標準などの仕様を策定（次頁以降）

DORA本文を補足する関連規則の概要は以下の通りです

DORA本文と関連規則の関係（1/2）

サードパーティ管理に関する規則

Pillar	関連する主な本文の条項	関連規則の文書番号	ITS/RTS/Guideline（※）	概要
1. ICT Risk-management	15,16[3]	2024/1774	RTS	ICTリスク管理のツール・方法・プロセス及び方針の規則、並びに簡素化されたICTリスク管理の枠組みの技術基準を補足する規則
2. Incident Reporting	20	2025/301	RTS	情報通信に関連する主な事象およびサイバー脅威に対する自主的な通知に関する初期・中間報告及び最終報告の技術基準を補足する規則
	18[3][4]	2024/1772	RTS	ICT関連インシデント及びサイバー脅威の分類基準、重要性の閾値、主要インシデントの報告の技術基準を補足する規則（サードパーティは主に地理的影響の記載）
	20	2025/302	ITS	重大なICTインシデントの報告に関する正確性・安全性を確保するため、標準化されたテンプレート等の技術基準を補足する規則
	11[10][11]	JC/2024/34	Guideline	ICT関連インシデントのコスト・損失や金融回収額を評価し、内訳を事例ごとに報告するために必要な手続き・条件に関するガイドライン
3. Resilience Testing	26[11]	2025/1190	RTS	脅威ベースのペネトレーションテストを実施するための要件、テスト方法や各フェーズのアプローチなどの技術基準を補足する規則
4. Critical Third-Party Risk	28[10]	2024/1773	RTS	ICTサードパーティサービスプロバイダ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の技術基準を補足する規則
	30[5]	2025/532	RTS	重要または重大な機能を担うICTサービスを下請契約する場合の判断・評価する技術基準を補足する規則
	28[9]	2024/2956	ITS	EU域内の金融機関がICTサードパーティサービスプロバイダに関する情報を通知するための標準テンプレートおよびフォーマットを補足する規則

※RTS/ITS/ガイドライン
・Regulatory Technical Standards（RTS：規制技術基準）：DORA本体の要求事項を詳細に定める規制技術基準
・Implementing Technical Standards（ITS：導入技術基準）：DORAの要求事項の報告様式やプロセスの標準化などの導入技術基準
・ガイドライン：DORAの要求事項に対して、具体的な運用やプラクティスを示すガイドライン

DORA本文を補足する関連規則の概要は以下の通りです

DORA本文と関連規則の関係（2/2）

Pillar	関連する主な本文の条項	関連規則の文書番号	ITS/RTS/ Guideline（※）	概要
5.Critical Third-Party oversight	31[2][6]	2024/1502	–	重要なICTサードパーティサービスプロバイダーの指定に関する規則
	41[1][2]	2025/295	RTS	サードパーティへの監督活動を実施するための条件の技術基準を補足する規則
	41[1][2]	2025/420	RTS	共同検査チームの構成に関する技術基準を補足する規則
	32[7]	JC/2024/36	Guideline	所管当局とESAs間の業務配分および重要なサードパーティへの勧告のフォローアップを行うために必要な情報交換の手続き・条件に関するガイドライン
	–	JC/2025/29	Guideline	基本原則、ガバナンス体制、利用可能なツールおよび監督プロセスの概要を示した、重大なサードパーティの監督枠組みに関するガイドライン

2. サードパーティ管理関連規則等の概要

以下の文書の概要について、次頁以降で説明します。

関連規則の文書番号	ITS/RTS/Guideline	概要
2024/1773	RTS	ICTサードパーティサービスプロバイダ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の技術基準を補足する規則
2025/532	RTS	重要または重大な機能を担うICTサービスを下請契約する場合の判断・評価する技術基準を補足する規則
2024/2956	ITS	EU域内の金融機関がICTサードパーティサービスプロバイダに関する情報を通知するための標準テンプレートおよびフォーマットを補足する規則

仮訳

ICTサードパーティサービスプロバイダ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の技術基準を補足する規則

ICTサービスの利用に関する契約上の取り決めの技術基準に係るSupplementing Regulations（2024/1773）の概要

概要	■ DORA28条「ICTサードパーティリスクの健全な管理に関する原則」を補足するRTS ■ ICTサードパーティサービスプロバイダーと契約を締結する前に発生する可能性のあるリスク管理のプロセスやその概要、および契約やその終了に関する項目が記載されています

主な条項		各条項の抜粋
第1条	全体的なリスクプロファイルと複雑性	■ 重要な機能を支援するICTサービスの利用ポリシーは、その規模、リスクプロファイル、サービス、活動、オペレーションの性質、範囲、および複雑性の増減要素を考慮する必要
第3条	ガバナンス体制	■ 経営陣は、ポリシーを少なくとも年に1回見直し、必要に応じて更新する必要 ■ ポリシーにはどのICTサービスが重要な機能を支えるか判定する方法をを含む必要
第4条	契約上の取り決めとライフサイクル	■ 契約上の取り決めのライフサイクルの各主要段階について、要件（規則、責任およびプロセス）を明記しなければならない
第5条	リスク評価	■ 契約上の取り決めを締結する前にリスク評価が実施されなければならない。リスク評価は、DORAおよび他に適用される分野別EU法令に定められた全ての関連要件を考慮する必要
第6条	デューデリジェンス	■ サードパーティの選定と評価について、適切かつ均衡なプロセスを定めなければならない。この際、対象となるサードパーティがICTグループ内サービスプロバイダーか否かを考慮しなければならない
第8条	契約条項	■ 契約上の取り決めに、金融機関が情報へアクセスする権利、検査および監査を実施する権利、ICTに対するテストを実施する権利が含まれることを定めなければならない
第9条	取り決めの監視	■ 契約上の取り決めに、サードパーティのパフォーマンスを継続的に監督するための措置と主要な指標（KPI）を明記しなければならない
第10条	契約の終了	■ 各契約上の取り決めごとに文書化された出口計画を策定すること、並びにその出口計画を定期的に見直しおよびテストすることに関する要件を含める必要

仮訳

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の技術基準を補足する規則

ICTサービスの利用に関する契約上の取り決め（2024/1773）の概要（1/9）

項目		概要
第1条	1	■ 重要または重大な機能を支援するICTサービス（以下「ICTサービス」）の利用に関するポリシー（以下「ポリシー」）は、金融機関の規模および全体的なリスクプロファイル、ならびにそのサービス、活動、オペレーションの性質、範囲、および複雑性の増減要素を考慮しなければならず、これには以下の要素が含まれる： ➢ (a)金融機関とサードパーティ間のICTサービス利用契約に含まれるICTサービスの種類 ➢ (b)サードパーティまたはその親会社の所在地 ➢ (c) ICTサービスが、加盟国内のサードパーティによるものか、第三国によるものか（さらに、ICTサービスの提供元やデータの処理・保存場所も考慮） ➢ (d)サードパーティと共有されるデータの性質 ➢ (e)サードパーティが、サービスを提供される金融機関と同一グループに属しているかどうか ➢ (f)加盟国内の所管当局により認可・登録・監督・監視を受けている、またはDORA第5条第2項の監督枠組みの対象となっているサードパーティの利用状況、またはそれに該当しない事業者の利用状況 ➢ (g)第三国の監督機関によって認可・登録・監督・監視を受けているサードパーティの利用状況、またはそれに該当しない事業者の利用状況 ➢ (h) ICTサービスの提供が、単一または少数のサードパーティに集中しているかどうか ➢ (i)技術的特性等により、ICTサービスを他のサードパーティへ移転可能かどうか ➢ (j) ICTサービスの提供に支障が生じた場合、金融機関の事業継続性やサービス提供可能性への潜在的な影響
第2条	2	■ 本規則が下位連結および連結レベルで適用される場合、グループの連結または下位連結財務諸表の作成を担当する親会社は、グループに属する全ての金融機関においてポリシーが一貫して実施されること、また本規則がグループの全ての該当階層で効果的に適用されるためにポリシーが適切であることを確保しなければならない。

仮訳

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の技術基準を補足する規則

ICTサービスの利用に関する契約上の取り決め（2024/1773）の概要（2/9）

項目		概要
第3条	1	■ 経営陣は、ポリシーを少なくとも年に1回見直し、必要に応じて更新する必要がある。ポリシーの変更は、関連する契約上の取り決めの範囲内で、適時かつ可能な限り速やかに実施する。金融機関は、実施のための予定タイムラインを文書化する。
	2	■ ポリシーには、どのICTサービスが重要または重大な機能を支えるかを判定するための方法を策定または参照を含む必要がある。また、評価の実施と再評価する時期についても明記しなければならない。
	3	■ ポリシーは、関連する契約上の取り決めの承認、管理、統制および文書化に関する内部の責任を明確に割り当てる必要がある。また、これらの取り決め（それに基づき提供されるICTサービスを含む）を効果的に監督するために、金融機関内で適切なスキル、経験および知識が維持されるよう確保しなければならない。
	4	■ ポリシーは、金融機関が関連する契約上の取り決めを効果的に監督する最終的な責任を有することを損なわず、サードパーティが提供されるICTサービスに関して金融機関がすべての法的・規制的要件を遵守できるよう、十分なリソースを有していると評価されることを求めなければならない。
	5	■ ポリシーは、契約上の取り決めの監視に責任を持つシニアマネジメントの役割または担当者を明記する必要がある。また、当該役割または担当者の経営陣との連携方法（該当機能自体に含まれる場合を除く）、経営陣に対する報告ラインの設定、報告する情報や文書の内容及び報告頻度を定めるものとする。
	6	■ ポリシーは、契約上の取り決めが以下のDORAの内容と整合していることを確保しなければならない： ➢ (a) 第6条に言及されているICTリスク管理枠組み ➢ (b) 第9条第4項に言及されている情報セキュリティ方針 ➢ (c) 第11条に言及されているICT事業継続計画 ➢ (d) 第19条で定められているインシデント報告要件
	7	■ ポリシーは、サードパーティが提供するICTサービスが、独立したレビューの対象となり、監査計画に含まれることを求めなければならない。

仮訳

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の技術基準を補足する規則

ICTサービスの利用に関する契約上の取り決め（2024/1773）の概要（3/9）

項目		概要
第3条	8	■ ポリシーは、契約上の取り決めについて以下を明確に定めなければならない： ➢ (a) 金融機関およびその経営陣の規制上の義務や顧客に対する責任を免除しないこと ➢ (b) 金融機関の効果的な監督を妨げず、サービスや活動に対する監督当局の制限に違反しないこと ➢ (c) サードパーティが所管当局と協力することを要求すること ➢ (d) 金融機関、その監査人および所管当局が、ICTサービスの利用に関連するデータおよび拠点に効果的にアクセスできることを要求すること
第4条	1	■ ポリシーは、契約上の取り決めのライフサイクルの各主要段階について、少なくとも以下を含む要件（規則、責任およびプロセス）を明記しなければならない： ➢ (a) 経営陣の責任（必要に応じて、サードパーティが提供するICTサービスの利用に係る意思決定プロセスへの関与を含む） ➢ (b) 契約上の取り決めの計画（リスクアセスメント、第5条および第6条に定めるデュー・ディリジェンス、ならびに第8条4項に定める契約上の取り決めの新規もしくは重要な変更の承認プロセスを含む） ➢ (c) 業務部門、内部統制およびその他関連部門の契約上の取り決めへの関与 ➢ (d) 契約上の取り決めの実施、監督および管理〔必要に応じて、連結および下位連結レベルにおける第7、8、9条に言及する事項を含む〕 ➢ (e) 文書化および記録の保存（DORA第28条第3項で定められている情報の登録簿に関する要件を考慮） ➢ (f) 記事10に定められている出口戦略および契約解除プロセス
第5条	1	■ ポリシーは、契約上の取り決めを締結する前に、金融機関の業務上のニーズを明確にする要件を含めなければならない。

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の技術基準を補足する規則

ICTサービスの利用に関する契約上の取り決め（2024/1773）の概要（4/9）

項目		概要
第5条	2	■ ポリシーは、契約上の取り決めを締結する前に、金融機関レベルで、必要に応じて連結および下位連結レベルでリスク評価が実施されなければならない。リスク評価は、DORAおよび他に適用される分野別EU法令に定められた全ての関連要件を考慮する。特に、ICTサービスがサードパーティによって提供された場合の金融機関への影響や、そうしたICTサービスの提供によってサードパーティにより生じるすべてのリスク（下記を含む）を考慮しなければならない： ➢ (a) オペレーショナルリスク ➢ (b) 法的リスク ➢ (c) ICTリスク ➢ (d) 風評リスク ➢ (e) 機密データや個人データの保護に関するリスク ➢ (f) データの可用性に関するリスク ➢ (g) データが処理・保存される場所に関するリスク ➢ (h) サードパーティの所在地に関するリスク ➢ (i) 金融機関レベルにおけるICT集中リスク

仮訳

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の技術基準を補足する規則

ICTサービスの利用に関する契約上の取り決め（2024/1773）の概要（5/9）

項目		概要
第6条	1	■ ポリシーは、将来のサードパーティの選定と評価について、適切かつ均衡なプロセスを定めなければならない。この際、対象となるサードパーティがICTグループ内サービスプロバイダーか否かを考慮しなければならない。また、金融機関は契約上の取り決めを締結する前に、当該サードパーティについて以下を評価することを求めなければならない： ➢ (a) 信頼できるかつ専門的な方法でICTサービスを提供するための、事業評判、十分な能力、専門性、適切な財務資源・人的資源・技術資源、情報セキュリティ基準、適切な組織構造、リスク管理および内部統制、そして該当する場合は必要な認可や登録を有しているか ➢ (b) 関連する技術的な進展を監視し、ICTセキュリティの先進的な実践を特定・導入する能力を有し、効果的かつ健全なデジタルオペレーショナルレジリエンスの枠組みを持っているか ➢ (c) ICTサービスの全てまたは重要部分の実施に際し、ICT下請事業者を利用している又は利用しようとしているか ➢ (d) 第三国に所在又は第三国でデータを処理・保存している場合に当該状況がオペレーショナルリスクや風評リスク、または制限措置（禁輸や制裁含む）によりICTサービス提供や金融機関によるサービス受領に影響を及ぼすリスクにどう影響するか ➢ (e) 金融機関自身、指名されたサードパーティ、および所管当局による現地監査を含む監査が効果的に実施できる契約上の取り決めに同意するか ➢ (f) 倫理的かつ社会的責任をもって行動し、人権・児童の権利や環境保護の原則を順守し、適切な労働条件を保証しているか
	2	■ ポリシーは、サードパーティが提供するICTサービスについて、当該プロバイダーのリスク管理体制の有効性に関する必要なレベルの保証についても明確に定める必要がある。また、ポリシーはデュー・デリジェンスがリスク軽減策および事業継続手段の存在および、それらが実際にICTサードパーティサービスプロバイダー内でどのように機能しているかについて評価することを求めなければならない。

仮訳

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の技術基準を補足する規則

ICTサービスの利用に関する契約上の取り決め（2024/1773）の概要（6/9）

項目		概要
第6条	3	■ ポリシーは、サードパーティの選定および評価のためのデュー・ディリジェンスプロセスを定め、サードパーティのパフォーマンスに必要なレベルの保証を得るために、以下のいずれの要素を利用するかを明示しなければならない： ➢ (a) 金融機関自らまたは代理で実施する監査または独立したアセスメント ➢ (b) サードパーティの要請に基づき作成された独立監査報告書の利用 ➢ (c) サードパーティの内部監査部門による監査報告書の利用 ➢ (d) 適切な第三者認証の利用 ➢ (e) 金融機関が入手可能なその他関連情報またはサードパーティが提供するその他情報の利用
	4	■ 金融機関は、第3項(a)から(e)に挙げられた要素を考慮し、サードパーティのパフォーマンスに関して適切なレベルの保証を確保しなければならない。必要に応じて、これら複数の要素を併用する。
第7条	1	■ ポリシーは、サードパーティの利用により生じる実際または潜在的な利益相反を特定し、防止および管理するために、関連する契約上の取り決めを締結する前に、取るべき適切な措置を明記しなければならない。また、その利益相反について継続的なモニタリングを行うことを規則しなければならない。 ■ ポリシーは、ICTサービスがICTグループ内サービスプロバイダーによって提供される場合、ICTサービスの条件（財務条件を含む）が客観的に決定されることを明記しなければならない。

仮訳

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の技術基準を補足する規則

ICTサービスの利用に関する契約上の取り決め（2024/1773）の概要（7/9）

項目		概要
第8条	1	■ ポリシーは、関連する契約上の取り決めが書面で作成され、DORA第30条第2項および第3項のすべての要素を含むことを定めなければならない。また、方針にはDORA第1条第1項(a)に定める要件や、必要に応じてその他の関連するEU法及び国内法に関する要素も含めなければならない。
	2	■ ポリシーは、関連する契約上の取り決めに、金融機関が情報へアクセスする権利、検査および監査を実施する権利、ICTに対するテストを実施する権利が含まれることを定めなければならない。そのために、ポリシーは金融機関が以下の方法を利用することを求めつつ、最終的な責任が金融機関にあることに影響を与えないものとする： ➢ (a) 金融機関自身による内部監査または指名されたサードパーティによる監査 ➢ (b) 必要に応じて、他の契約金融機関や同一サードパーティを利用する企業と共同で組織する合同監査およびICTテスト（脅威ベースのペネトレーションテストを含む）。これらの監査やテストは、当該金融機関や企業、または彼らから指名されたサードパーティによって実施されるものとする。 ➢ (c) 必要に応じて、第三者認証 ➢ (d) 必要に応じて、サードパーティが提供する内部監査または第三者監査報告書

仮訳

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の技術基準を補足する規則

ICTサービスの利用に関する契約上の取り決め（2024/1773）の概要（8/9）

項目		概要
第8条	3	■ 金融機関は、時間の経過とともに第2項の(c)の第三者認証や(d)の監査報告書のみに依拠してはならない。方針では、第2項の(c)及び(d)の方法については、金融機関が以下を満たす場合にのみ利用を許可しなければならない： ➢ (a) その契約上の取り決めに対するサードパーティの監査計画に満足している ➢ (b)第三者認証や監査報告の範囲が、金融機関が特定したシステムや主要な統制項目をカバーし、関連する規制要件が遵守されていることを確保している ➢ (c)第三者認証や監査報告の内容を継続的に評価し、報告書や認証が陳腐化していないことを検証している ➢ (d) 将来の認証や監査報告において主要なシステムや統制がカバーされていることを確保している ➢ (e)第三者認証・監査を行う者の適性に満足している ➢ (f)第三者認証は広く認められている関連専門基準に基づいて発行され、監査は同基準に基づいて行われ、主要な統制の運用効果についてテストが含まれていることに満足している ➢ (g) 金融機関が、リスク管理の観点から合理的かつ正当な頻度で、第三者認証や監査報告書の範囲の変更を他の関連システムや統制へ要求できる契約上の権利を有している ➢ (h) 契約上の取り決めに関して、金融機関が独自または合同監査を随時実施する契約上の権利を有し、その権利を合意された頻度で行使できること
	4	■ ポリシーは、契約合意の重要な変更が、日付入りかつ全当事者の署名を備えた書面によって正式に記録されることを確保しなければならない。また、契約上の取り決めの更新手続きについても定めなければならない。
第9条	1	■ ポリシーは、契約上の取り決めに、サードパーティのパフォーマンスを継続的に監督するための措置と主要な指標（KPI）を明記しなければならない。これには、データおよび情報の機密性、可用性、完全性、真正性に関する要件の遵守状況、およびサードパーティが金融機関の関連方針や手順に準拠しているかを監督するための措置が含まれる。また、サービス水準契約（SLA）が遵守されない場合に適用される措置（必要に応じて契約上のペナルティを含む）についても定めなければならない。
	2	■ ポリシーは、金融機関が、ICTサービスに利用されるサードパーティが、契約上の取り決めと金融機関自体の方針に照らして、適切な性能および品質

仮訳

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の技術基準を補足する規則

ICTサービスの利用に関する契約上の取り決め（2024/1773）の概要（9/9）

項目		概要
第9条	1	■ 基準を満たしているかどうかをどのように評価するかについて定める必要がある。特に以下を確保しなければならない： ➢ (a) サードパーティが、定期報告書、インシデント報告書、サービス提供報告書、ICTセキュリティに関する報告書、事業継続計画およびテストに関する報告書等について、活動およびサービスに関する適切な報告を金融機関に提出すること ➢ (b) ICTリスク管理枠組みに沿って、KPI（重要業績指標）、重要統制指標、監査、自己適合証明、独立レビューによってパフォーマンスが評価されること ➢ (c) 金融機関がサードパーティから他の関連情報も受領できること ➢ (d) ICT関連のインシデントや業務・セキュリティ・決済に関するインシデントについて、適切に通知を受けること ➢ (e) 法的および規制要件、方針への適合性を検証するための独立レビューや監査が実施されること
	2	■ ポリシーは、第2項に基づく評価が文書化され、その結果が第6条に定める金融機関のリスク評価の更新に活用されることを明記しなければならない。
	3	■ ポリシーは、金融機関が、ICTサービスの提供、契約上の取り決めまたは法的要件の遵守に関して、サードパーティに不備があると認識した場合（ICT関連のインシデントや業務・セキュリティ・決済関連のインシデントを含む）、採用すべき適切な措置を定め、措置の実施が、定められた期間内にその重要性を勘案しつつ、効果的に遵守されるようモニタリングする方法も明示しなければならない。
第10条	1	■ ポリシーは、各契約上の取り決めごとに文書化された出口計画を策定すること、並びにその出口計画を定期的に見直しおよびテストすることに関する要件を含めなければならない。出口計画を策定する際には、以下の事項を考慮する必要がある： ➢ (a) 想定外かつ持続的なサービス中断 ➢ (b) 不適切またはサービス提供の失敗 ➢ (c) 契約上の取り決めの予期しない終了
	2	■ 出口計画は、現実的かつ実行可能で、あり得るシナリオおよび合理的な仮定に基づき作成されなければならず、契約上の取り決めに定められた終了および解除条件と整合する実施スケジュールを含めなければならない。

仮訳

重要または重大な機能を担うICTサービスを下請契約する場合の判断・評価する技術基準を補足する規則

下請契約する場合の判断・評価する技術基準に係るSupplementing Regulations（2025/532）の概要

概要	■ DORA30条「主要な契約条項」を補足するRTS ■ 金融機関が重要または重大な機能を担うICTサービスを下請契約する場合は、以下の要求事項を基に判断・評価することが記載されています

主な条項		各条項の抜粋
第1条	全体的なリスクプロファイルと複雑性	■ 金融機関は、そ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、複雑性の増減要因を考慮しなければならない
第3条	下請契約に係るDDおよびリスク評価	■ 金融機関は、サードパーティとの契約上の取り決めを締結する前に、当該サードパーティがICTサービスを再委託可能かどうかを決定しなければならない
第4条	下請契約の条件	■ 金融機関とサードパーティとの間で締結される契約上の取り決めは、ICTサービスのうち、どのサービスが再委託の対象となりうるか、またその条件を明確に定めなければならない
第5条	ICTサービスの委託契約の重要な変更	■ 契約上の取り決めには、サードパーティが再委託に関する重要な変更を行う意向がある場合に、金融機関が評価するために十分な時間的余裕をもって通知することを定めなければならない
第6条	契約の終了	■ 金融機関は、サードパーティとの契約上の取り決めにおいて、再委託を許可されていないICTサービスを下請事業者に委託した場合など、契約を解除できる権利を有する旨を定めること

仮訳

重要または重大な機能を担うICTサービスを下請契約する場合の判断・評価する技術基準を補足する規則

ICTサービスを下請け契約する場合の技術基準（2025/532）の概要（1/5）

項目		概要
第1条	1	■ 金融機関は、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、及び業務の性質、規模、複雑性の増減要因を考慮しなければならない。これには以下の要素が含まれる： ➢ (a) 金融機関とサードパーティとの契約上の取り決めにより、ICTサービスの種類 ➢ (b) サードパーティと、その下請事業者との契約上の取り決めで対象となるICTサービスの種類 ➢ (c) ICTサービスを提供するICT下請事業者、あるいはその親会社の所在地 ➢ (d) サードパーティが利用する、ICTサービスを提供する再委託の連鎖の長さおよび複雑さ ➢ (e) ICTサービスを提供するICT下請事業者と共有されるデータの性質 ➢ (f) ICTサービスの実際の提供場所およびデータの実際の処理・保存場所を含む、ICTサービスの提供が、下請事業者によって行われているかどうか、また、その下請事業者が加盟国内又は第三国に所在しているか、 ➢ (g) ICTサービスを提供するICT下請事業者が、提供先である金融機関と同一グループに属しているかどうか ➢ (h) ICTサービスを提供するICT下請事業者が、加盟国の認可・登録・監督当局による監督・監視を受けているか、またはDORA第5章第2項の監督フレームワークの対象であるかどうか ➢ (i) ICTサービスを提供するサードパーティが、第三国の監督当局による認可・登録・監督・監視を受けているかどうか ➢ (j) ICTサービスの提供が、サードパーティの特定の一つの下請け業者または少数の下請事業者に集中しているかどうか ➢ (k) ICTサービスの下請事提供が、それらICTサービスを他のサードパーティへ移転する際の可搬性に影響を与えるかどうか ➢ (l) サードパーティが下請事業者を利用する場合、ICTサービスの継続性や可用性に、障害が与える潜在的な影響
第2条	1	■ この規則が下位連結および連結ベースで適用される場合、グループの下位連結または連結財務諸表の作成を担当する親会社は、ICTサービスの利用に関して、再委託が契約上許可されている場合に、その再委託に関する条件がグループ内のすべての金融機関において一貫して実施され、本規則があらゆる関連レベルで効果的に適用されるのに十分なものであることを確保しなければならない。

重要または重大な機能を担うICTサービスを下請契約する場合の判断・評価する技術基準を補足する規則

ICTサービスを下請け契約する場合の技術基準（2025/532）の概要（2/5）

項目		概要
第3条	1	■ 金融機関は、サードパーティとの契約上の取り決めを締結する前に、当該サードパーティがICTサービスを再委託可能かどうかを決定しなければならない。金融機関は、以下のすべての条件が満たされていると評価した場合にのみ、そのような契約上の取り決めを締結することができる。 ➢ (a) サードパーティに対するデュー・デリジェンス手続きが、サードパーティが潜在的なICT下請事業者の業務的および財務的能力を選定し評価できることを確保しており、これには、必要に応じて金融機関の要求により、DORA第4章で言及されるデジタル・オペレーショナル・レジリエンステストへの参加が含まれていること。 ➢ (b) サードパーティが、ICTサービスを提供するすべての下請事業者を特定し、それら下請事業者について金融機関に通知・情報提供を行い、本条における条件の評価に必要なあらゆる情報を金融機関に提供できること。 ➢ (c) サードパーティが、ICTサービスを提供する下請事業者との契約上の取り決めにより、金融機関がDORAおよび適用されるEU法令及び国内法に基づく自らの義務を履行できるようにしていること。 ➢ (d) 下請事業者が、金融機関および監督・決済当局に対し、サードパーティによって付与されているものと同等のアクセスおよび監査の契約上の権利を与えていること。 ➢ (e) 金融機関の法令および規制上の義務を遵守する最終責任を損なうことなく、サードパーティ自体が、下請先レベルでのICTリスクを適切な情報セキュリティ基準の適用や、適切な組織構造、リスク管理、内部統制、インシデント報告・対応などを含む十分な能力、専門性、財務的・人的・技術的資源を有して監督できること。 ➢ (f) 金融機関自体が、再委託されたICTサービスに関するICTリスクを適切に管理するため、適切な情報セキュリティ基準の適用や、適切な組織構造やリスク管理、インシデント対応、事業継続管理、内部統制などを含む十分な能力、専門性、財務的・人的・技術的資源を有していること。 ➢ (g) 金融機関は、ICTサービスを提供する下請事業者の障害が、当該金融機関のデジタル・オペレーショナル・レジリエンスおよび財務の健全性に及ぼし得る影響を評価していること。 ➢ (h) 金融機関は、ICTサービスの提供に関連し、サードパーティが利用する潜在的な下請事業者の所在地によるリスクを評価していること。 ➢ (i) 金融機関は、DORA第29条に従い、企業レベルでのICT集中リスクを評価していること。 ➢ (j) 金融機関は、所管当局、破綻処理機構、又は金融機関自身（及び機関により指名された者）がアクセス権、検査権、監査権を行使する上で、障害となるものが存在しないかを評価していること。

仮訳

重要または重大な機能を担うICTサービスを下請契約する場合の判断・評価する技術基準を補足する規則

ICTサービスを下請け契約する場合の技術基準（2025/532）の概要（3/5）

項目		概要
第3条	2	■ ICTサービスを再委託するサードパーティを利用する金融機関は、事業環境の変化、支援対象となる事業機能の変化、ICTの脅威、ICT集中リスク、地政学リスクを含むリスク評価の変化等に対して、第1項(f)から(j)に言及されているリスク評価を定期的に実施しなければならない。
	3	■ 本条に定める義務を遵守するために、サードパーティがその下請事業者に対して実施したリスク評価の結果に依拠した場合であっても、DORAに基づく法的および規制上の義務を遵守する最終的な責任が金融機関にあることは変わらない。

重要または重大な機能を担うICTサービスを下請契約する場合の判断・評価する技術基準を補足する規則

ICTサービスを下請け契約する場合の技術基準（2025/532）の概要（4/5）

項目		概要
第4条	1	■ 金融機関とサードパーティとの間で締結される契約上の取り決めは、ICTサービスのうち、どのサービスが再委託の対象となりうるか、またその条件を明確に定めなければならない。その契約には、以下の事項が明記されるものとする。 ➢ (a) サードパーティが下請事業者によって提供されるサービスについて責任を負うこと。 ➢ (b) サードパーティが再委託されたすべてのICTサービスを監督し、金融機関との契約上の義務が継続的に履行されることを確保する義務を負うこと。 ➢ (c) ICTサービスを提供する下請事業者に関して、サードパーティが金融機関に対して負う監督および報告の義務を負うこと。 ➢ (d) サードパーティが、ICTサービスを現在または将来的に提供する下請事業者やその親会社、および当該ICTサービスが実際に提供される場所に関連するすべてのリスクを評価すること。 ➢ (e) 該当する場合には、下請事業者によって処理または保存されるデータの所在。 ➢ (f) サードパーティが、下請事業者との契約において、当該下請事業者がサードパーティおよび、合意がある場合は金融機関に対して負う監督および報告の義務を明記すること。 ➢ (g) ICT下請事業者が契約上の義務を履行できない場合にも、サードパーティが下請事業者の連鎖全体にわたりICTサービスの継続性を確保すること。 ➢ (h) サードパーティとその下請事業者の契約上の取り決めが、DORA第30条第3項(c)で言及されているビジネスコンティンジェンシープランに関する要件を含み、これらの計画に関するICT下請事業者が遵守すべきサービスレベルを明示していること。 ➢ (i) サードパーティと下請事業者間の契約が、DORA第30条第3項(c)で言及されているICTセキュリティ基準および追加的なセキュリティ要件を明記していること。 ➢ (j) 下請事業者が、DORA第30条第3項(e)で言及されているものと同様のアクセス権、検査権及び監査権を、金融機関および該当する監督・破綻処理機構に付与すること。 ➢ (k) サードパーティが、再委託に関する取り決めに重要な変更が生じた場合、金融機関に通知すること。 ➢ (l) 規則本体の第6条またはDORA第28条第7項で定められた条件が満たされた場合、金融機関がサードパーティとの契約を解除する権利を有すること。

重要または重大な機能を担うICTサービスを下請契約する場合の判断・評価する技術基準を補足する規則

ICTサービスを下請け契約する場合の技術基準（2025/532）の概要（5/5）

項目		概要
第4条	1	■ この規則を遵守するために必要となる、金融機関とICTサービスを提供するサードパーティとの間の契約上の取り決めに関する変更は、適宜、可能な限り速やかに実施しなければならない。金融機関は、その実施に関する予定されたタイムラインを文書化しなければならない。
第5条	1	■ 契約上の取り決めには、サードパーティが再委託に関する重要な変更を行う意向がある場合には、金融機関が次の事項を評価するために十分な時間的余裕をもって通知しなければならない旨が定めなければならない。 ➢ (a) 金融機関が現に直面している、または直面し得るリスクへの影響 ➢ (b) 重要な変更が金融機関への契約上の義務の履行能力に影響を及ぼす可能性があるかどうか
	2	■ 契約上の取り決めには、金融機関が変更を承認または異議を申し立てるための合理的な通知期間を設けることが盛り込まれていなければならない。
	3	■ サードパーティは、金融機関が通知期間の終了までに当該変更を承認した、または異議を申し立てなかった場合に限り、再委託に関する重要な変更を実施するものとする。
	4	■ 金融機関が、第1項に言及されている重要な変更が自身のリスク許容度を超えると判断した場合、金融機関は通知期間の終了前に以下を行わなければならない。 ➢ (a) その旨をサードパーティに通知すること ➢ (b) 変更に対して異議を申し立て、実施前にその変更の修正を要求すること
第6条	1	■ 金融機関は、サードパーティとの契約上の取り決めにおいて、以下の場合に契約を解除できる権利を有する旨を定めることができる。 ➢ (a) 金融機関が重要または重大な機能を支える下請に関する重要な変更に対して異議を申し立て、修正を要求したにもかかわらず、サードパーティがその重要な変更を実施した場合。 ➢ (b) サードパーティが金融機関の承認を得ずに、通知期間終了前に重要または重大な機能またはその重要部分を支える下請に関する重要な変更を実施した場合。 ➢ (c) サードパーティが、金融機関とサードパーティとの契約で明示的に再委託を許可されていないICTサービスを下請事業者に委託した場合。

仮訳

EU域内の金融機関がICTサードパーティサービスプロバイダーサービスプロバイダに関する情報を記録するための標準テンプレートおよびフォーマットを補足する規則

ICTサードパーティサービスプロバイダーサービスプロバイダに関する情報の登録に係るSupplementing Regulations（2024/2956）の概要

概要 ■ DORA28条[3]「サードパーティが提供するサービスの契約上の取り決めに関連する情報の登録」を補足するITS

主な条項		各条項の概要（抜粋）
第1条	定義	■ ICTサードパーティサービスプロバイダー、ICTサプライチェーン、ランクの定義
第2条	サードパーティのランク	■ 各サードパーティにランクを付与しなければならない。付与されたランクの数値が小さいほど、金融機関により近い取り決めである
第3条	情報登録のテンプレート	■ 金融機関は、テンプレートに含まれる情報が正確かつ一貫性を持つことを確保する必要
第5条	情報登録の内容	■ 情報登録に含める内容
第6条	情報登録の範囲	■ グループに属するすべての金融機関およびICTグループ内サービスプロバイダーを含める必要

仮訳

EU域内の金融機関がICTサードパーティサービスプロバイダに関する情報を登録するための標準テンプレートおよびフォーマットを補足する規則

ICTサービスプロバイダの情報を登録するためのテンプレートを補足する規則（2024/2956）の概要（1/6）

項目		概要
第1条	1	■ 「直接のICTサードパーティサービスプロバイダーサービスプロバイダー」とは、以下のいずれかの契約上の取り決めを締結したサードパーティまたはICTグループ内サービスプロバイダーを指す。 ➢ (a) 金融機関と契約し、その金融機関に対して直接ICTサービスを提供する者 ➢ (b) 金融機関または非金融機関と契約し、同一グループ内の他の金融機関にサービスを提供する者
	2	■ 「ICTサービスサプライチェーン」とは、直接のサードパーティが金融機関にICTサービスを提供することに関連し、直接のサードパーティを起点として、その相手方（下請事業者）として一者または複数の他のサードパーティが関与する、一連の契約上の取り決めの流れを意味する。
	3	■ 「ランク」とは、ICTサービスサプライチェーンにおけるサードパーティの位置を指す。
第2条	1	■ 金融機関は、各サードパーティにランクを付与しなければならない。ランクは「1」以上の任意の自然数であり、付与されたランクの数値が小さいほど、金融機関により近い取り決めであることを意味する。 ICTサービスサプライチェーンにおける直接のサードパーティのランクは常に「1」となる。 ICTサービスサプライチェーンにおける下請事業者のランクは常に「1」より大きな数となる。

仮訳

EU域内の金融機関がICTサードパーティサービスプロバイダに関する情報を登録するための標準テンプレートおよびフォーマットを補足する規則

ICTサービスプロバイダの情報を登録するためのテンプレートを補足する規則（2024/2956）の概要（2/6）

項目		概要
第3条	1	■ 金融機関は、DORA第28条第3項に従い、情報の登録簿を、各機関レベルまたは下位連結および連結レベルで維持・更新するために、別添IからIVで定められた様式を使用しなければならない。
	2	■ 金融機関は、前項で言及されている様式に以下のすべてが含まれていることを確実にしなければならない。 ➢ (a) 直接のICTサードパーティサービスプロバイダープロバイダーによって提供されるすべてのICTサービスに関する関連情報 ➢ (b)重要または重大な機能またはその重要部分を支えるICTサービスを実質的に下支えするすべての下請事業者に関する情報
	3	■ 金融機関は、前項で言及されている様式に含まれる情報が正確かつ一貫性を持つことを確保しなければならない。金融機関は、様式に含まれる情報を定期的に確認し、発見された誤りや不一致を速やかに訂正しなければならない。グループの場合、下位連結および連結レベルで情報の登録簿の維持・更新を担当する金融機関は、連結内の機関レベルに関する情報が正確かつ下位連結および連結レベルの情報と一致と一致していることを確保しなければならない。
	4	■ 金融機関は、前項で言及されている様式に含まれる情報が、以下のデータ品質原則に従っていることを確保しなければならない。 ■ (a) 正確性 (b) 網羅性 (c) 一貫性 (d) 完全性 (e) 均一性 (f) 妥当性
	5	■ 金融機関は、すべてのICTサードパーティサービスプロバイダーサービスプロバイダー（法人格を有する者、但し事業者として行動する個人を除く）を特定するために、適格かつ有効な法人識別コード（LEI）、または指令（EU）2017/1132第16条に記載された欧州固有識別子（EUID）、そしてこれらが両方とも利用可能な場合には両方の識別子を使用しなければならない。
	6	■ 直接のサードパーティが金融機関の重要または重大な機能を支えるICTサービスを提供する場合、金融機関は、前項の(b)に従い情報の登録簿に記載された直接のICTサードパーティサービスプロバイダーサービスプロバイダー、すべての下請事業者が、事業者として行動する個人を除き、重要または重大な機能を支えるICTサービスを実質的に下支えしている場合、有効なLEIまたはEUID、そして利用可能な場合は両方の識別子を使用することを確実にしなければならない。

仮訳

EU域内の金融機関がICTサードパーティサービスプロバイダに関する情報を登録するための標準テンプレートおよびフォーマットを補足する規則

ICTサービスプロバイダの情報を登録するためのテンプレートを補足する規則（2024/2956）の概要（3/6）

項目		概要
第4条	1	■ 別段の指示がない限り、情報の登録簿を構成する各様式は、あらかじめ定められた列数と無制限の行数を持つ表でなければならない。
	2	■ 金融機関は、各データ項目を単一の値で記入しなければならない。特定のデータ項目について複数の値が有効となる場合、金融機関は各有効な値ごとに対応する様式に追加の行を加えなければならない。
	3	■ 金融機関は、該当する場合は、機関レベル、下位連結および連結レベルにおいて、情報の登録簿のすべてのデータ項目を記入しなければならない。

仮訳

EU域内の金融機関がICTサードパーティサービスプロバイダに関する情報を登録するための標準テンプレートおよびフォーマットを補足する規則

ICTサービスプロバイダの情報を登録するためのテンプレートを補足する規則（2024/2956）の概要（4/6）

項目		概要
第5条	1	■ 金融機関は、別添Iに定められた指示に従い、情報の登録簿に以下の情報を含めなければならない。 ➢ (a) 機関レベル、下位連結レベル、連結レベルごとに情報の登録簿を維持・更新する金融機関に関する一般情報 ➢ (b) 連結内の企業に関する一般情報 ➢ (c) 様式B_01.02に記載された本国以外に所在する金融機関の支店の特定 ➢ (d) 契約上の取り決めに関する一般情報 ➢ (e) 契約上の取り決めに関する詳細情報 ➢ (f) ICTサービスサプライチェーンの一部が社内グループの場合、契約参照番号を用いたグループ内契約上の取り決めとグループ外ICTサードパーティサービスプロバイダーサービスプロバイダーとの契約上の取り決めとの関連情報 ➢ (g) ICTサービスの受領のためまたはICTサービス利用企業の代理として直接のICTサードパーティサービスプロバイダーサービスプロバイダーと契約を締結した企業に関する情報 ➢ (h) ICTサービスの提供を目的に契約を締結したICTサードパーティサービスプロバイダーサービスプロバイダーの特定 ➢ (i) 連結内の他の企業にICTサービスを提供するために契約を締結した企業の特定 ➢ (j) ICTサードパーティサービスプロバイダーサービスプロバイダーによって提供されるICTサービスを利用する企業に関する情報 ➢ (k) 直接のICTサードパーティサービスプロバイダーサービスプロバイダーおよび下請事業者に関する情報 ➢ (l) ICTサービスサプライチェーンに関する情報 ➢ (m) 機能の特定に関する情報 ➢ (n) 重要または重大な機能またはその重要部分を支えるICTサードパーティサービスプロバイダーサービスプロバイダーによって提供されたICTサービスの評価に関する情報 ➢ (o) 金融機関で使用されている用語、および様式記入時に使用される閉じたリストや分類体系に含まれる用語に関する情報

仮訳

EU域内の金融機関がICTサードパーティサービスプロバイダに関する情報を登録するための標準テンプレートおよびフォーマットを補足する規則

ICTサービスプロバイダの情報を登録するためのテンプレートを補足する規則（2024/2956）の概要（5/6）

項目		概要
第6条	1	■ リスク管理または契約管理上適切である場合、金融機関は目的に最もふさわしい形式で追加情報を情報の登録簿に含めることができる。
	2	■ グループの場合、親会社は、情報の登録簿に含めるべき企業を決定する際に、関連する分野別EU法令を考慮しなければならない。
	3	■ 下位連結および連結レベルで維持・更新される情報の登録簿には、その下位グループおよびグループに属するすべての金融機関およびICTグループ内サービスプロバイダーを含めなければならない。

EU域内の金融機関がICTサードパーティサービスプロバイダーサービスプロバイダに関する情報を記録するための標準テンプレートおよびフォーマットを補足する規則

ICTサービスプロバイダの情報を登録するためのテンプレートを補足する規則（2024/2956）の様式（6/6）

様式	概要
B_01.01	機関レベル、下位連結レベル、連結レベルごとに情報の登録簿を維持・更新する金融機関に関する一般情報
B_01.02	連結内の企業に関する一般情報
B_01.03	上記以外の国に所在する金融機関の支店の特定
B_02.01	契約上の取り決めに関する一般情報
B_02.02	契約上の取り決めに関する詳細情報
B_02.03	ICTサービスサプライチェーンの一部が社内グループの場合、契約参照番号を用いたグループ内契約上の取り決めとグループ外サードパーティとの契約上の取り決めとの関連情報
B_03.01	ICTサービスの受領のためまたはICTサービス利用企業の代理として直接のサードパーティと契約を締結した企業に関する情報
B_03.02	ICTサービスの提供を目的に契約を締結したサードパーティの特定
B_03.03	連結内の他の企業にICTサービスを提供するために契約を締結した企業の特定
B_04.01	サードパーティよって提供されるICTサービスを利用する企業に関する情報
B_05.01	直接のサードパーティおよび下請事業者に関する情報
B_05.02	ICTサービスサプライチェーンに関する情報
B_06.01	機能の特定に関する情報
B_07.01	重要または重大な機能またはその重要部分を支えるサードパーティによって提供されたICTサービスの評価に関する情報
B_99.01	金融機関で使用されている用語、および様式記入時に使用される閉じたリストや分類体系に含まれる用語に関する情報

Appendix.
重要なサードパーティの監督に係る規則等の概要

以下の文書の概要について、次頁以降で説明します。

文書番号	ITS/RTS/ Guideline	概要
JC/2025/29	Guideline	DORA監督活動および各組織の役割の概要などが記載されたガイドライン、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に関するガイドライン
2024/1502	–	重要なICTサードパーティサービスプロバイダーの指定に関する規則
2025/295	RTS	サードパーティへの監督活動を実施するための条件の技術基準を補足する規則
2025/420	RTS	共同検査チームの構成に関する技術基準を補足する規則
JC/2024/36	Guideline	所管当局とESAs間の業務配分および重要なサードパーティへの勧告のフォローアップを行うために必要な情報交換の手続き・条件に関するガイドライン

DORAの監督活動の枠組みやプロセスに関するガイドライン

DORAの監督活動の枠組みやプロセスに関するガイドライン（JC 2025 29）の概要（1/2）

概要	■ DORA監督活動に関するガイドライン ■ 監督活動の目的、基本原則、構造、活動、実施プロセスなどについて記載されています

DORA監督活動の概要		
重要なICTサードパーティサービスプロバイダーの指定		情報の登録簿を含むすべてのデータをもとにESAが指定する年次プロセス
リスクアセスメント		ICTサードパーティサービスプロバイダー監視活動の強度を定義し、優先順位を設定する年次プロセス
計画	個別（年次）	ICTサードパーティサービスプロバイダーに共有される文書、目的と監視で実施される主な行動を概説
	複数年計画	ESAとCAの3か年計画
検査	定期的なモニタリング	定期的な情報収集、新たな問題(例：運用上の事故や新たな脅威)等に関するCサードパーティPとの継続的な対話
	一般的な調査	特定のリスク領域に対する水平的または的を絞ったレビュー
	検査	CサードパーティPがFEにもたらすリスクの対象を絞った詳細な状況を確認、すべての関連文書を請求する権利を伴う
	情報の要求	監督当局が一般的な調査や査察を開始することなく、情報を要求
推奨事項		評価分野で特定された発見事項への対応。フォローアップは、継続的な定期的モニタリングの一環、または改善策を明記した報告を通じて実施

DORAの監督活動の枠組みやプロセスに関するガイドライン

DORAの監督活動の枠組みやプロセスに関するガイドライン（JC 2025 29）の概要（2/2）

ESA（EBA、EIOPA、ESMA）	監視の役割と概要
Joint Committee （JC：合同委員会）	-JCは、ICTサードパーティサービスプロバイダー指定を含む3つのESAを調整する。 -ESAの監視活動に関する共同立法機関への報告
Oversight Forum （OF：監督フォーラム）	● JCの小委員会: ✓ 3つのLOの共同意思決定を準備 ✓ 重要なICTサードパーティサービスプロバイダー指定を勧告 ✓ 年1回の監視評価を提供 ✓ ICTサードパーティサービスプロバイダーリスク、FEレジリエンスの調整と低減、集中リスクと部門横断的リスクのモニタリングにおける一貫性を促進する。 ✓ 欧州当局に提出するJC年次報告書の作成
Joint Oversight Network （JON：共同監督ネットワーク）	● 監督業務を監視・舵取り ✓ 監視活動の一貫性の確保 ✓ ESA全体の監視戦略と方法論を調整する
Joint Examination Team （JET：共同検査チーム）	JETがLOの監督業務を行う (一般調査・検査等)
Lead Overseers （LOs：主監督者）	監督責任者 割り当てられたICTサードパーティ、JETによるサポート

当局が指定するICTサードパーティサービスプロバイダの指定基準に関する規則の概要

重要なICTサードパーティサービスプロバイダの指定基準に係るSupplementing Regulations（2024/1502）の概要

概要

- DORA31条「重要なICTサードパーティサービスプロバイダの指定」を補足する規則
- ICTサードパーティサービスプロバイダが金融市場を混乱させる単一の障害点とならないよう、金融機関に与えるリスクを識別・分類・管理するための詳細な評価基準と手続きについて記載されています

STEP1（定量的評価）
サービスの提供範囲、取引量、リスクの集中度等を評価

評価基準	考慮すべき小基準
第31条(2)[a]	■ 1.1：金融機関の総数に占める割合 ■ 1.2：金融機関の総資産価値に占める割合
第31条(2)[b]	■ 2.1：G-SIIおよびO-SIIの数 ■ 2.2：2.1以外の金融機関かつDORA本文46条で定める当局が認定する金融機関の数
第31条(2)[b]	■ 4.1：同一のICTサービスを提供する能力を有する他のサードパーティが存在しない金融機関の総数に占める割合 ■ 4.2：同一のICTサービスを提供する他のサードパーティに移行することが極めて困難な金融機関の総数に占める割合

STEP2（定性的評価）
システミックリスクの影響、オペレーショナルレジリエンス、相互接続性、プロバイダの代替の容易さ等を評価

評価基準	考慮すべき小基準
第31条(2)[a]	■ 1.3：サードパーティが提供するICTサービスの廃止により、金融機関の活動及び業務に及ぼす影響の強さ及び金融機関の数 ■ 1.4：サードパーティが提供する重要な機能を支援するICTサービスの同じ下請事業者への依存
第31条(2)[b]	■ 2.3：G-SIIもしくはO-SIIおよびSTEP1の他の金融機関が相互以前関係にある
第31条(2)[c]	■ 3.1：金融機関の重要な機能を支援する同一のサードパーティによって最終的に提供されるICTサービスは、金融機関の活動にとって重要な性質のものである
第31条(2)[d]	■ 3.1：特定の市場で活動しているサードパーティの数が限られていること、当該サードパーティの市場シェア、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、サードパーティ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

金融機関が利用するICTサードパーティサービスプロバイダーの指定基準に関する規則

Supplementing Regulations2024/1502の概要（1/5）

項目		概要
前文	評価アプローチ	• ESAは、第31条（２）に定める条件を考慮し、二段階アプローチ評価（※）における小基準を使用する必要 • 重要なICTサービスとそれらを利用する金融機関の多様性と数を考慮すると、評価の第1ステップの一部として、定量的フィルタリングをしたのちに、評価の第2ステップの一部として、定性的基準に照らし詳細な分析を実施する必要 • ESAは、サードパーティを重要サービスとして指定すべきか否かを評価する際に、規則 (EU) 2022/2554の第28条(3) の情報の登録簿のデータ及びその他の容易に入手可能な情報に依拠することが重要
	評価対象のサードパーティの分類	• 第31条 (3) に基づくグループに属する場合には、サードパーティのグループごとに実施されるべきである • ICTサードパーティサービスプロバイダーのICT下請事業者もESAによる評価の対象とすべきであり、該当する場合には、重要なICTサードパーティサービスプロバイダーとして指定されるべき
	評価項目および評価の考慮事項	• 当該サードパーティのサービスに依存する金融機関及び金融システムに与えるシステミックな影響の程度及び性質を明確に把握することが最も重要なため、当該ICTサービスを利用している金融機関の数や資産価値を考慮 • 金融サービス提供に対するサードパーティのシステミックな重要性や相互連関性、サービスの安定性や継続性を考慮した重要性について定性的な評価の必要 • G-SIIs及びO-SIIs、又は「システミック」と特定される金融機関が、重要または重大な機能をサポートするために同一のICTサービスに依存している場合、当該サービスを提供するサードパーティがEU金融セクターにとって重要であるか否かを評価 • 金融機関が業務を支障なく遂行するために必要な種類及び重要性の観点から重要または重大な機能を支えるICTサービスを評価 • サードパーティの代替性の判断は、ESA評価の一環として、特定の市場で活動するサードパーティの数、同一のICTサービスの代替ソリューションの存在、及び他のサードパーティへのデータ・ワークロードの移行コストを考慮する必要

金融機関が利用するICTサードパーティサービスプロバイダーの指定基準に関する規則

重要なサードパーティの指定基準に係るSupplementing Regulations（2024/1502）の概要（2/5）

項目		概要
第1条	1	• 金融機関にとって重要なサードパーティを指定するために、規則 (EU) 2022/2554の第31条 (2) に定める基準を検討する場合、ESAは、以下のアプローチを適用する必要 ➢ ステップ１ ：サードパーティが本文書の第2条 (1)、第3条 (1)および第5条 (1) の小基準をすべて満たしているかどうかを評価 ➢ ステップ２ ：ステップ１の小基準を満たすサードパーティについて、本文書の第2条 (5)、第3条 (4)、第4条 (1) および第5条 (5) で言及されている「ステップ2」の小基準に照らして評価を実施
	2	• 第31条 (5) の陳述書の提出期間（サードパーティへの通知から6週間以内）の終了後、ESAは、合同委員会を通じて、「ステップ1」の小基準をすべて満たし、かつ、「ステップ2」の小基準の評価結果に基づいてサードパーティを指定
第2条	1	※評価STEP1参照（P38）
	2	• 第2条1(a)に規則された小基準は以下の通り計算する ➢ 同一サードパーティが重要または重大な機能を支えるICTサービスを提供する本文第2条 (1) に規則する金融機関分類の金融機関数 ➢ 本文第2条 (1) に規則された金融機関分類の金融機関数の総数
	3	• 第2条1(b)に規則された小基準は以下の通り計算する ➢ 同一サードパーティが重要または重大な機能を支えるICTサービスを提供する本文第2条 (1) に規則する金融機関分類の金融機関の総資産価値 ➢ 本文第2条 (1) に規則された同じ分類の全EU金融機関数の資産総額
	4	• 第2項及び第3項に従って計算された割合の両方が、本文第2条 (1) に規則された少なくとも1つの分類の金融機関の総数の少なくとも10%を占める場合、第1項で言及された「ステップ1」の下位基準を満たしている
	5	※評価STEP2参照（P39）

金融機関が利用するICTサードパーティサービスプロバイダーの指定基準に関する規則

重要なサードパーティの指定基準に係るSupplementing Regulations（2024/1502）の概要（3/5）

項目		概要
第3条	1	※評価STEP1参照
	2	• サードパーティの提供するサービスが少なくとも次のいずれかによって使用されている場合、第1項[a]に定める下位基準を満たしている ➢ [a]：G-SII ➢ [b]：少なくとも3つのO-SII ➢ [c]：指令2013/36/EUの第131条 (3) に従って計算したO-SIIスコアが3000を超える少なくとも1つのO-SII
	3	• サードパーティの提供するサービスが少なくとも次のいずれかによって使用されている場合、第1項[b]に定める下位基準を満たしている ➢ 本文第2条 (1) (g)、(h)、(i) 又は (j) に分類され、所管当局がシステミックと指定する金融機関 ➢ 信用機関および上記に該当しない少なくとも3つの金融機関へのサービス提供
第4条	1	※評価STEP2参照（P39）
第5条	1	※評価STEP2参照（P39）
	2	• 第5条1(a)に規則された小基準は以下の通り計算する ➢ 同一のICTサービスを提供する能力を有する他のサードパーティが存在しない金融機関数
	3	• 第5条1(b)に規則された小基準は以下の通り計算する ➢ 同一のICTサービスを提供する他のサードパーティに移行もしくは再統合することが極めて困難な金融機関数数
	4	• サードパーティは、以下のいずれかを満たす場合、第1項に定める下位基準を満たしている ➢ 1項[a]の総数に占める割合が、本文第2条 (1) の金融機関の区分に係る金融機関の総数の10%以上であること ➢ 1項[b]の総数に占める割合が、本文第2条 (1) の金融機関の区分に係る金融機関の総数の10%以上であること
	5	※評価STEP2参照（P39）

金融機関が利用するICTサードパーティサービスプロバイダーの指定基準に関する規則

重要なサードパーティの指定基準に係る2段階アプローチ評価の概要：STEP1（4/5）

STEP1	第2条（1）	• 第31条 (2)[a]の基準（金融サービス提供の安定性、継続性、品質に係るシステミックな影響）を評価 本文第2条 (1) の金融機関の分類基づき、重要または重大な機能を支えるICTサービスが同一のサードパーティによって提供されている、 ➢ 小基準1.1：金融機関の総数に占める割合 ➢ 小基準1.2：金融機関の総資産価値に占める割合
	第3条（1）	• 第31条 (2)[b]の基準（サードパーティに依存する金融機関のシステミックな性質、重要性）を評価 重要または重大な機能を支えるICTサービスが同一のサードパーティによって提供されており、信用機関（Credit Institution）である、 ➢ 小基準2.1：G-SIIおよびO-SIIの数 ➢ 小基準2.2：2.1以外の金融機関かつDORA本文46条で定める当局が認定する金融機関の数
	第5条（1）	• 第31条 (2)[b]の基準（サードパーティに依存する金融機関のシステミックな性質、重要性）を評価 本文第2条 (1) の金融機関の分類基づき、重要または重大な機能を支えるICTサービスについて、 ➢ 小基準4.1：同一のICTサービスを提供する能力を有する他のサードパーティが存在しない金融機関の総数に占める割合 ➢ 小基準4.2：同一のICTサービスを提供する他のサードパーティに移行することが極めて困難な金融機関の総数に占める割合

金融機関が利用するICTサードパーティサービスプロバイダーの指定基準に関する規則

重要なサードパーティの指定基準に係る2段階アプローチ評価の概要：STEP2（5/5）

STEP2	第2条（5）	第31条 (2)、(a) 項に定める基準を考慮する際に以下の小基準を考慮する必要 ➢ 小基準1.3：サードパーティが提供するICTサービスの廃止により、金融機関の活動及び業務に及ぼす影響の強さ及び金融機関の数 ➢ 小基準1.4：サードパーティが提供する重要または重大な機能を支援するICTサービスの同じ下請事業者への依存
	第3条（4）	第31条 (2)、(b) 項に定める基準を考慮する際に以下の小基準を考慮する必要 ➢ 小基準2.3：G-SIIもしくはO-SIIおよびSTEP1の他の金融機関が相互以前関係にある
	第4条（1）	第31条 (2)、(c) 項に定める基準を考慮する際に以下の小基準を考慮する必要 ➢ 小基準3.1：金融機関の重要または重大な機能を支援する同一のサードパーティによって最終的に提供されるICTサービスは、金融機関の活動にとって重要な性質のものである
	第5条（5）	第31条 (2)、(d) 項に定める基準を考慮する際に、第31条 (2)、(d) (i) に定められた代替性に係る小基準を考慮する必要 ➢ 特定の市場で活動しているサードパーティの数が限られていること、当該サードパーティの市場シェア、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、サードパーティ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

サードパーティへの監督活動を実施するための条件の技術基準を補足する規則

サードパーティへの監督活動を実施するための条件の技術基準（2025/295）の概要（1/9）

概要	■ DORA41条「サードパーティへの監督活動を実施するための条件の技術基準」を補足するRTS ■ 所管当局がサードパーティへの監督活動を実施するための条件の技術基準について記載されています

主な条項		各条項の抜粋
第1条	重要なICT指定の申請に必要な情報	■ ICTサードパーティサービスプロバイダーは、重要なサードパーティとして指定を希望する自主申請において、各情報を申請書に記載する
第2条	重要な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情報	■ 重要なICTサードパーティサービスプロバイダーは、監督義務を遂行するために主任監督官が必要とする情報を、主任監督者の要求に応じて、主任監督者に提供する
第3条	是正勧告発効後の重要なICTサードパーティサービスプロバイダーからの情報	■ 重要なICTサードパーティサービスプロバイダーは、主監督者に対して、勧告で特定されたリスクを軽減するために実施を計画している勧告及び改善策に関する改善計画を含む報告書を提供する
第6条	監督者の勧告で取り上げたリスクに対する所管当局の評価	■ 金融機関に対する監督の一環として、所管当局は比例性の原則に従い、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が金融機関に及ぼす影響を評価する

サードパーティへの監督活動を実施するための条件の技術基準を補足する規則

サードパーティへの監督活動を実施するための条件の技術基準（2025/295）の概要（2/9）

項目		概要
第1条	1	■ ICTサードパーティサービスプロバイダーは、DORA第31条第1項(a)に従い、重要なサードパーティとして指定を希望する自主申請（同規則第31条第11項）において、以下の情報を理由付き申請書に記載しなければならない： a. 法人名 b. 法人識別コード c. 連絡担当者名およびクリティカルICTサードパーティサービスプロバイダーの連絡先 d. 法人の登記上の所在国 e. 企業構造の説明（少なくとも親会社やEU金融機関向けにICTサービスを提供する関連事業体の情報を含む）該当する場合、以下の情報を含むこと： i. 法人名 ii. 法人識別コード iii. 法人の登記上の所在国 f. EU金融セクターにおけるサードパーティの推定市場シェア、及びDORA第2条第1項で参照された金融機関の種類ごとの市場シェア（申請年および前年の推計） g. 以下の内容を含む、サードパーティの事業内容及びEU域内の金融機関に提供する各ICTサービスの説明 i. 金融機関に提供される事業の内容およびICTサービスの種類の説明 ii. ICTサービスによって支援される金融機関の機能の一覧（あれば） iii. ICTサービスが金融機関の重要または重大な機能を支援している情報（あれば） h. 以下の内容を含む、サードパーティが提供するICTサービスを利用している金融機関の一覧（あれば、各金融機関について以下の情報を含む） i. 法人名 ii. サードパーティが把握している場合は法人識別コード iii. DORA第2条第1項に規則される金融機関の種類 iv. ICTサービスが提供されている法人の所在地（あれば）

サードパーティへの監督活動を実施するための条件の技術基準を補足する規則

サードパーティへの監督活動を実施するための条件の技術基準（2025/295）の概要（3/9）

項目		概要
第1条	1	i. 申請者であるサードパーティが提供するサービスに依存している、DORA第31条第9項に基づき欧州監督機関（ESA）が公表した最新の重要なサードパーティリストに掲載されている重要なサードパーティの一覧（あれば） j. 以下の内容を含む、サードパーティによる自己評価： i. (i)以下の観点を考慮した、各ICTサービスについての代替可能性の程度： i. EU金融セクターにおけるサードパーティの市場シェア ii. ICTサービスの種類またはグループごとの既知の競合他社の数 iii. 提供されるICTサービスの特性に関する説明（独自技術や、サードパーティの組織または業務の特徴に関する事項を含む） ii. 申請を提出するサードパーティと同じICTサービスを提供可能な代替サードパーティの利用可能性に関する知見 k. EU域内の金融機関へのICTサービス及びインフラ提供に関する今後の戦略及び投資計画に関する情報（グループや経営体制の変更、新規市場又は新規事業への参入を含む） l. 重要なサードパーティとして指定された下請事業者に関する情報 m. 重要なサードパーティとしての指定申請に関連するその他の理由
	2	■ サードパーティが企業グループに属する場合、第1項の情報提供はグループ全体として提供されるICTサービスに関連して記載する。

サードパーティへの監督活動を実施するための条件の技術基準を補足する規則

サードパーティへの監督活動を実施するための条件の技術基準（2025/295）の概要（4/9）

項目		概要
第2条	1	■ 1. 重要なICTサードパーティサービスプロバイダーは、規則(EU)2022/2554の要件に従って、監督義務を遂行するために主任監督官が必要とする情報を、主任監督者の要求に応じて、主任監督者に提供するものとします。
	2	■ 第1項に規則する情報には、特に次のものが含まれます。 (a)次のものの間の取り決めに関する情報及び契約書類の写し (i)重要なICTサードパーティサービスプロバイダー及び規則 (EU) 2022/2554の第2条 (1) に言及されている金融機関; (ii)EU域内の金融機関に提供されるICTサービスの技術的バリューチェーンを把握するために、重要なICTサードパーティサービスプロバイダーとその下請業者; (b)EU域内の金融機関にICTサービスを直接又は間接的に提供する同一グループに属するすべての機関の特定を含む、重要なICTサードパーティサービスプロバイダーの組織及びグループ構造に関する情報; (c)次に掲げるいずれかの主要株主の構成及び地理的分布その他の主要株主に関する事項 (i)重要なICTTの資本又は議決権の25%以上を単独又は関連事業者と共同で保有する事業者; (ii)重要なICTサードパーティサービスプロバイダーの運営、経営又は監督機関の構成員の過半数を選任又は解任する権利を有する者; (iii)契約に基づき、重要なICTサードパーティサービスプロバイダーの株主又は社員の議決権の過半数を支配している事業者; (d)重要なICTサードパーティサービスプロバイダーが事業を展開する関連市場におけるサービスの種類ごとの市場シェアに関する情報; (e)重要なICTサードパーティサービスプロバイダーの内部ガバナンス体制に関する情報 (ガバナンス責任と説明責任に関する規則の系統を持つ構造を含む); (f)重要なICTサードパーティサービスプロバイダーの経営管理機関その他の内部の関連する委員会の議事録であって、域内金融機関の機能を支援するICTサードパーティサービスプロバイダーサービスに関する活動及びリスクに何らかの形で関連するもの;

サードパーティへの監督活動を実施するための条件の技術基準を補足する規則

サードパーティへの監督活動を実施するための条件の技術基準（2025/295）の概要（5/9）

項目		概要
第2条	2	(g)重要なICTサードパーティサービスプロバイダーのICTセキュリティに関する情報。これには、関連する戦略、目的、ポリシー、手順、プロトコル、プロセス、機密データを保護するための制御手段、アクセス制御、暗号化の実施、インシデント対応計画、および関連するすべての規制や国内および国際基準 (該当する場合) の遵守に関する情報が含まれる。 (h)個人データ及び非個人データを含むデータ保護及びデータ機密性を確保するための技術的及び組織的措置、機密データを保護するために実施された管理措置、アクセス制御、暗号化、データ侵害対応計画に関する情報;個人データの処理に関して、ICTサードパーティサービスプロバイダーが第三国の法律 (第三国政府のアクセス要求、国のリストおよび適用される法律を含む) の適用を受ける場合: (i)重要なICTサードパーティサービスプロバイダーが、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および相互運用性のためにEU金融機関に提供するメカニズムに関する情報; (j)金融機関にサービスを提供する目的で使用されるデータセンター及びICT生産センターの所在地に関する情報 (EU域外を含む重要なICTサードパーティサービスプロバイダーの全ての関連施設及び施設のリストを含む); (k)重要なICTサードパーティサービスプロバイダーによる第三国からのサービス提供に関する情報 (当該ICTサードパーティサービスプロバイダーが取り扱う個人データ及び非個人データに適用される関連法規に関する情報を含む); (l)重要なICTサードパーティサービスプロバイダー及びその第三国の下請業者によるICTサービスの提供から生じるリスクに対処するためにとられた措置に関する情報; (m)リスク管理の枠組み及びインシデント管理の枠組みに関する情報。これには、重要なICTサードパーティサービスプロバイダー及びその下請業者のポリシー、手順、ツール、仕組み及びガバナンスの取り決めが含まれる。これには、EU域内の金融機関に直接的又は間接的な影響を及ぼす主要なインシデントのリスト及び説明が含まれる。これには、金融機関に対するインシデントの重要性を判断し、国境を越えた影響の可能性を評価するための関連する詳細が含まれる。 (n)重要なICTとその下請け業者のポリシー、手順、コントロールを含む、変更管理フレームワークに関する情報;

サードパーティへの監督活動を実施するための条件の技術基準を補足する規則

サードパーティへの監督活動を実施するための条件の技術基準（2025/295）の概要（6/9）

項目		概要
第2条	2	(o)重要なICTサードパーティサービスプロバイダーの全体的な対応と復旧の枠組みに関する情報。これには、事業継続計画と関連する取り決めと手順、ソフトウェア開発ライフサイクルポリシー、対応と復旧計画と関連する取り決めと手順、バックアップポリシーの取り決めと手順が含まれる。 (p)パフォーマンス監視、セキュリティ監視、およびインシデント追跡に関する情報、ならびにサービスパフォーマンス、インシデント、および重要なICTサードパーティサービスプロバイダとEU域内の金融機関との間で合意されたサービスレベルアグリーメント (SLA) およびサービスレベルオブジェクト (SLO) または同様の取り決めの遵守に関する報告メカニズムに関する情報; (q)戦略、ポリシー、手順、プロセス及びコントロールを含む、重要なICTサードパーティサービスプロバイダーサービスプロバイダーのICTサードパーティサービスプロバイダー管理フレームワークに関する情報。これには、重要なICTサードパーティサービスプロバイダーサービスプロバイダーが下請業者と契約を締結する前に下請業者に対して実施したデュー・ディリジェンス及びリスク評価の詳細を含み、全ての関連するICTリスク及びカウンターパーティ・リスクをカバーする関係を監視する。 (r)ネットワーク監視、サーバ監視、アプリケーション監視、セキュリティ監視、脆弱性スキャン、ログ管理、パフォーマンス監視、インシデント管理、SLOなどの信頼性目標に対する測定を含むが、これらに限定されない、重要なICTサードパーティサービスプロバイダーおよびその下請け業者の監視およびスキャンシステムからの抽出; (s)EU域内の金融機関に直接又は間接的にサービスを提供するために、重要なICTサードパーティサービスプロバイダー及びその下請業者が使用する本番、本番前及びテストシステム又はアプリケーションからの抽出; (t)関連当局との協力協定が情報交換を規則している場合には、EU域内及びEU域外の国家当局によって実施された監査を含む、コンプライアンス及び利用可能な監査報告書並びに関連する監査結果、又は重要な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達成された認証 (内部及び外部の監査人からの報告書、認証、又は業界固有の基準に対するコンプライアンス評価を含む) 。これには、重要なICTサードパーティサービスプロバイダーのICTシステムの耐障害性に関する利用可能な任意の種類の独立したテストに関する情報が含まれます。これには、ICTサードパーティサービスプロバイダーが実施するあらゆる種類の脅威ベースペネトレーションテストが含まれます。

サードパーティへの監督活動を実施するための条件の技術基準を補足する規則

サードパーティへの監督活動を実施するための条件の技術基準（2025/295）の概要（7/9）

項目		概要
第2条	2	(u)重要なICTサードパーティサービスプロバイダーの要請に応じて、又は重要なICTサードパーティサービスプロバイダーのために、重要なICTサードパーティサービスプロバイダー内の重要な地位にある個人の適性及び誠 実性を評価するために重要なICTサードパーティサービスプロバイダーが実施する評価に関する情報; (v)第3条に基づく勧告に対処するための是正計画に関する情報、および是正措置が実施されたことを確認するための関 連情報; (w)利用可能な従業員訓練スキームとセキュリティ意識向上プログラムに関する情報。これには、重要なICTサードパーティサービスプロバイダーが、機密性 の高い財務データを取り扱い、高いレベルのセキュリティを維持するためのスタッフの訓練に必要な投資、資源、方法に 関する情報が含まれる。 (x)ICTとセキュリティに関連する予算と資源に関する情報を含む、重要なICTサードパーティサービスプロバイダーの活動に関する情報と財務諸表。

サードパーティへの監督活動を実施するための条件の技術基準を補足する規則

サードパーティへの監督活動を実施するための条件の技術基準（2025/295）の概要（8/9）

項目		概要
第3条	1	■ 重要なICTサードパーティサービスプロバイダーはDORA第35条第1項(d)に言及されている勧告で特定されたリスクを軽減するために、重要なICTサードパーティサービスプロバイダーが実施を計画している勧告および是正措置に関する是正計画を盛り込んだ報告書を主監督者に提出しなければならない。この報告書は、それぞれの勧告ごとに主監督者が定めたタイムラインと整合していなければならない。
	2	■ 重要なICTサードパーティサービスプロバイダーが受領した勧告に対応して講じた措置や実施した是正措置の進捗を主監督者がモニタリングできるよう、重要なICTサードパーティサービスプロバイダーは主監督者の要請に応じ、以下を共有しなければならない。 ➢ (a) 主監督者が定めたタイムライン内で、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に提出した報告書に記載の実施行動や措置の進捗状況を明示した中間進捗報告書および関連する裏付け資料 ➢ (b) 受領した勧告で特定されたリスクを軽減するために重要なICTサードパーティサービスプロバイダーが講じた措置または実施した是正措置を明示する最終報告書および関連する裏付け資料
第4条	1	■ 重要なICTサードパーティサービスプロバイダーは、主監督者の依頼に記載された専用の安全な電子チャネルを通じ、主監督者が定めた様式で要求された情報を主監督者へ提出しなければならない。
	2	■ 主監督者に情報を提供する際、重要なICTサードパーティサービスプロバイダーは以下を遵守しなければならない： ➢ (a) 主監督者の情報依頼に示された構成に従うこと ➢ (b) 提出書類の中で該当情報を明確に特定できるようにすること
	3	■ 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へ提出、開示、報告する情報は、国際金融分野で慣習的に使用される言語で記載されなければならない。
第5条	–	■ 下請け契約に関する情報の共有が求められる重要なICTサードパーティサービスプロバイダーは、付属書に定められたテンプレートに従い、主監督者へ情報を提出しなければならない。

サードパーティへの監督活動を実施するための条件の技術基準を補足する規則

サードパーティへの監督活動を実施するための条件の技術基準（2025/295）の概要（9/9）

項目		概要
第6条	1	■ 所管当局は、金融機関の監督の一環として、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基づき実施した措置が金融機関に与える影響について、比例性の原則に従い評価しなければならない。
	2	■ 第1項に定める評価を実施する際、所管当局は以下すべてを考慮しなければならない。 ➢ (a) 勧告で特定されたリスクを軽減するために金融機関が実施した是正・補正措置の適切性および一貫性 ➢ (b) 勧告で特定されたリスクに対する、所管当局の監督下にある金融機関のエクスポージャーに影響を及ぼす場合の、重要なICTサードパーティサービスプロバイダーの報告書内措置・行動への準拠性に関する主監督者の評価 ➢ (c) DORA第42条第5項に従い協議された他の所管当局の見解 ➢ (d) 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行動および是正措置を、監督下の金融機関のリスクエクスポージャー軽減に十分であるとみなしているかどうか
	3	■ 主監督者からの要請があった場合、所管当局は第1項で定める評価結果を適切な期間内に提供しなければならない。主監督者が評価結果の提出を要請する際は、比例性の原則および勧告に関連するリスクの大きさ、さらに複数の加盟国で業務を行う金融機関に影響が及ぶ場合のリスクの越境的影響を考慮しなければならない。
	4	■ 必要な場合、所管当局は第1項の評価を遂行するために必要な情報を金融機関に提供するよう要請しなければならない。

共同検査チームの構成に関する技術基準を補足する規則

共同検査チームの構成に関する技術基準（2025/420）の概要（1/5）

概要	■ DORA41条「サードパーティへの監督活動を実施するための条件の技術基準」を補足するRTS ■ 共同検査チームの設置やメンバーに関して記載されています

主な条項		各条項の抜粋
第1条	共同検査チームのメンバーの任務	■ 共同検査チームのメンバーは、主監督者コーディネーターの指揮の下で、第1条に記載の業務を遂行する
第2条	共同検査チームの設置	■ 重要なICTサードパーティサービスプロバイダを指定した後、主監督者は共同監督ネットワークと合意して、監視活動を実施する責任を負う共同検査チームを設立する
第3条	共同検査チームのメンバー	■ 主監督者は、共同監督ネットワークと合意し、監視フォーラムと協議の上、共同検査チームの人数およびその構成を決定する
第5条	共同検査チームのメンバーの作業体制	■ 共同検査チームのメンバーは、主監督者の指示に従って、相応の技能、注意および勤勉さをもって、偏りなく、個別の年間監督計画に特定された自らの任務を遂行する

共同検査チームの構成に関する技術基準を補足する規則

共同検査チームの構成に関する技術基準（2025/420）の概要（2/5）

項目		概要
第1条	1	■ 共同検査チームのメンバーは、主監督者コーディネーターの指揮の下で業務を遂行しなければならない。これらの業務には、主監督者が実施する活動の継続的な支援および特定の業務の実行が含まれる。具体的な業務は以下のとおりである。 ➢ (a) DORA第33条第4項で言及されている個別の年次監督計画の作成・起草において主監督者を補助すること。 ➢ (b) DORA第33条第2項で言及されている評価の実施において主監督者を補助すること。 ➢ (c) DORA第37条および委任規則（EU）2025/295第II章に基づき、主監督者がサードパーティから取得した情報を評価すること。 ➢ (d) DORA第38条で言及されている重要なサードパーティに関する一般的な調査を実施すること。 ➢ (e) DORA第39条第1項で言及されている検査を実施すること。 ➢ (f) DORA第35条第1項(d)で言及されている勧告の起草。 ➢ (g) 委任規則（EU）2025/295第4条で言及されている是正計画および進捗報告書の評価。 ➢ (h) DORA第35条第6項、第37条第1項、第38条第4項、第39条第6項で言及されている要求および決定の作成・起草。 ➢ (i) DORA第32条第3項で言及されている包括的ベンチマークの策定など、主監督者による横断的な監督活動への貢献において主監督者を補助すること。 ➢ (j) 重要なサードパーティが提供するサービスを利用する金融機関に関連する情報を主監督者と共有することを確実にすること。 ➢ (k) 監督の目的のために主監督者が必要と判断した計画外の臨時活動において主監督者を補助すること。
	2	■ 「ICTサービスサプライチェーン」とは、直接のサードパーティが金融機関にICTサービスを提供することに関連し、直接のサードパーティを起点として、その相手方（下請事業者）として一者または複数の他のサードパーティが関与する、一連の契約上の取り決めの流れを意味する。

共同検査チームの構成に関する技術基準を補足する規則

共同検査チームの構成に関する技術基準（2025/420）の概要（3/5）

項目		概要
第2条	1	■ DORA第31条第1項(a)に従い、サードパーティが初めて「重要」と指定された後、DORA第34条第1項に定める共同監督ネットワーク（Joint Oversight Network）との合意のもと、主監督者は、その重要なサードパーティに対する監督活動を実施する責任を有する共同検査チームを設置しなければならない。
	2	■ 重要なICTサードパーティサービスプロバイダーの状況に重要な変更が生じた場合、主監督者は共同監督ネットワークとの合意のもと、その重要なICTサードパーティサービスプロバイダーに対する監督活動を担う共同検査チームの構成を更新することができます。この目的における重要な変更とは、以下のいずれかに関するものとします。 ➢ (a) 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 ➢ (b) 重要なICTサードパーティサービスプロバイダーのICTサービスにより支援を受けている金融機関が行う活動 ➢ (c) DORA第31条第9項に言及されているEUレベルの重要なICTサードパーティサービスプロバイダーのリスト
	3	■ DORA第40条第2項に定める当局は、その職員の中から1名以上を共同検査チームのメンバーとして指名し、任命しなければならない。個人は、1つまたは複数の共同検査チームのメンバーとして指名・任命される場合がある。
	4	■ 主監督者は、指名された個人を共同検査チームのメンバーとして、利用可能状況、主監督者の特定のニーズ、および指名当局と主監督者の合意により、フルタイムまたはパートタイムで任命しなければならない。
	5	■ 当局（規則（EU）2022/2554第40条第2項）は、共同検査チームのメンバーを指名する際、ICTおよび関連分野の技術的専門知識、資格、技能、コミュニケーションと協働能力、監査および監督能力を評価しなければならない。
	6	■ 主監督者は、正当な理由がある場合、かつ指名された個人の能力が必要な人材の要件に合致しない場合に限り、指名当局に指名内容の修正を求めることができる。
	7	■ 主監督者および当局は、年間個別監督計画に従い、共同検査チームの十分な人員確保のために、あらゆる適切かつ可能な措置を講じなければならない。

共同検査チームの構成に関する技術基準を補足する規則

共同検査チームの構成に関する技術基準（2025/420）の概要（4/5）

項目		概要
第3条	1	■ 主監督者は、DORA第34条第1項に定める共同監督ネットワークと合意し、かつ同規則第32条第1項に定める監督フォーラムと協議したうえで、共同検査チームのメンバー数およびその構成を決定しなければならない。
	2	■ 主監督者は、共同検査チームの設置プロセスの一環として、また必要に応じて、その人数を以下を考慮して決定しなければなりません。 ➢ (a) 共同検査チームが監督する各重要なサードパーティごとに作成された個別の年次監督計画に含まれる業務 ➢ (b) すべての共同検査チームが監督するすべての重要なサードパーティを対象とした複数年の監督計画の戦略的目標
	3	■ 共同検査チームの人数および構成を決定する際、主監督者は少なくとも下記の事項を考慮しなければなりません。 ➢ (a) すべての重要なICTサードパーティサービスプロバイダーに関連して行われる監督活動の想定される強度 ➢ (b) 共同検査チームおよびESAs（欧州監督機関）が主監督者として監督するICTサードパーティサービスプロバイダーの規模および複雑性 ➢ (c) 主監督者が評価した特定の重要なICTサードパーティサービスプロバイダーに関連する個別の監督ニーズ ➢ (d) 適切な知識の維持を確保するための共同検査チームの構成の安定性 ➢ (e) 共同検査チームが業務を遂行するために必要な技術的および非技術的なICT知識要件を考慮した必要なスキル ➢ (f) 重要なICTサードパーティサービスプロバイダーが、金融機関の重要または重大な機能を支えるICTサービスを提供する加盟国および、それらのサービス利用金融機関を監督する所管当局 ➢ (g) 重要なICTサードパーティサービスプロバイダーが、重要または重要な機能を支えるICTサービスを提供する金融機関の種類、規模および数 ➢ (h) 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サービスへの依存度が最も高い金融機関を監督する所管当局 ➢ (i) 共同検査チームの指名当局の部門横断的かつ均衡のとれた代表性
	4	■ DORA第40条第2項で言及される当局が共同検査チームのメンバーを指名する際には、第3項の(c)、(d)、(e)、(g)、(h)を少なくとも考慮しなければならない。

共同検査チームの構成に関する技術基準を補足する規則

共同検査チームの構成に関する技術基準（2025/420）の概要（5/5）

項目		概要
第4条	1	■ 定期的に、または主監督者が交代した場合、あるいは第2条第2項で定められた重要な変更が生じた場合、主監督者は共同検査チームのメンバーと協議したうえで、共同検査チームのメンバーの成果を評価しなければならない。指名当局および主監督者の双方は、その評価結果をもとに、共同検査チームのメンバー構成を変更することが適切かどうかを判断しなければならない。
第5条	1	■ 共同検査チームのメンバーは、個別の年次監督計画で定められた業務を、十分な技能、注意、勤勉さをもって、いかなる偏見もなく、かつDORA第40条第2項第2文に定める主監督者コーディネーターの指示に従って遂行しなければならない。
	2	■ 監督業務を実施する際、共同検査チームのメンバーは、監督活動および関連するおオペレーショナル分野の実施に関し、欧州監督機構が共同で策定した監督手続きに従わなければならない。これには、ITツールや機器の使用や時間管理に関する仕様も含まれる。
	3	■ 共同検査チームのメンバーは、DORA第40条第2項第2文で言及されている主監督者コーディネーターから与えられた情報・データの取り扱いに関する仕様や指示に従い、また欧州監督機構の機密保持制度を遵守しなければならない。
	4	■ 主監督者および指名当局は、本規則で定められた要件を実施するための仕組みを確立しなければならない。これには、共同検査チームによる監督活動に要する時間・見積もりコスト、トレーニング、そして共同検査チームのメンバーの役割に関連する倫理や行動規範に関する取り決めが含まれる。
	5	■ 主監督者および指名当局は、第4項で言及された取り決めが、適時に実施・見直しされ、常に最新の状態となるようにしなければならない。

所管当局とESAの協力および情報交換に関するガイドライン

所管当局とESAの情報交換に関するガイドライン（JC/GL/2024/36）の概要（1/11）

概要	■ 所管当局とESAとの間の業務の配分及び実施に関する手続等のガイドライン ■ 監督にあたって交換される情報やICTサードパーティサービスプロバイダーに向けられた勧告のフォローアップにおいて実施される当局間の情報交換について記載されています

主なガイドライン（GL）		各条項の抜粋
GL5	所管当局がESAに提出する情報	■ 所管当局は情報の登録簿を受領した後、遅滞なくその全文をESAに提供する。要請があれば、所管当局は監督活動で取得した追加の情報をESAに提供する
GL6	ESAが所管当局に提出する重要なICTサードパーティの情報	■ 所管当局に対し、指定申請を行ったICTサードパーティサービスプロバイダーの法的名称、識別コード、本店所在地国を提供
GL7	監督計画	■ 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提供するICTサービスを利用する金融機関の所管当局へ、年次監督計画案を提供する
GL11	フォローアップのための監督者と所管当局の情報交換	■ 主監督者は、重大なサードパーティが提供するICTサービスを利用する金融機関の所管当局に対し、改善策を明記したサードパーティの報告書などの情報を提供する
GL12	サービスの利用・停止を求める決定	■ 所管当局は、金融機関が主監督者の勧告で特定された固有リスクに対処する適切な契約条件を採用しない場合、金融機関に対して通知する意向を主監督者に連絡する

所管当局とESAの協力および情報交換に関するガイドライン

所管当局とESAの情報交換に関するガイドライン（JC/GL/2024/36）の概要（2/11）

項目		概要
第1節	一般的な目的と原則	■ 本ガイドラインの目的は、DORA第32条第7項に従い、ESAsおよび所管当局が以下を確保することである。 ➢ 所管当局とESAsの間で協力や情報交換が必要となる分野の全体像の把握 ➢ 監督活動の効率性と一貫性を確保し、重複を避けるため、ESAsと所管当局の間の情報交換および協力において調整され、統一されたアプローチ ➢ 協力と情報交換に関する手続き規則およびタイムライン、役割・責任、協力・情報交換方法に関する共通のアプローチ ■ 本ガイドラインは、DORA第32条第7項の文脈におけるESAsと所管当局間の監督協力および情報交換に関し、一貫性のある、効率的かつ効果的な実務を構成する。本ガイドラインは、ESAsと所管当局間でさらなる情報交換や拡張された監督協力を妨げない。また、ESAsと所管当局間の協力や情報共有の実務的詳細は、個別のターゲット運営モデルの対象となり得る。 ■ 本ガイドラインで定められた協力と情報交換は、予防的かつリスクベースのアプローチを考慮すべきである。その結果、三つのESAsと所管当局間で業務と責任がバランスよく配分され、各ESAsおよび所管当局の人的資源および技術的専門知識が最大限に活用されるべきである。 ■ 本ガイドラインに別段の定めがない限り、ESAsとは、三つの欧州監督機構（主監督者を含む）を指す。

所管当局とESAの協力および情報交換に関するガイドライン

所管当局とESAの情報交換に関するガイドライン（JC/GL/2024/36）の概要（3/11）

項目		概要
第1節	スコープ	■ 本ガイドラインの適用範囲は、DORA第V章第II節（第31条～第44条）のみに関連している。以下に関係する条文は対象外である。 ➢ 特定の所管当局またはESAのみが対象となる業務（例：監督料に関する第43条は主監督者（LO）のみの業務）や、金融機関および重要なICTサードパーティサービスプロバイダーが対象となる業務（例：第35条第5項では重要なICTサードパーティサービスプロバイダーが誠実に主監督者と協力し、その業務遂行を支援することが求められる）。 ➢ 所管当局間の協力（例：第48条第1項では所管当局が相互に密接に協力すべきこと）、ESAs間の協力（例：第35条第2項(a)では主監督者が共同監督ネットワーク内で定期的な調整を確保すること）、および他のEU当局との協力（例：第34条第3項では主監督者がECBやENISAに技術的助言を求めることができる）。 ➢ ESAの手続規則の適用対象となるガバナンス体制（例：第32条ではESAsが監督フォーラムを設立する必要があり、第34条では主監督者が共同監督ネットワークを設立する必要がある）。 ➢ 個別の法的権限に基づく業務（例：JET（共同検査チーム）の構成、指名、業務、運営体制の基準は、ESAsが策定する別の規制技術基準で定められている〔第41条第1項(c)〕）。

所管当局とESAの協力および情報交換に関するガイドライン

所管当局とESAの情報交換に関するガイドライン（JC/GL/2024/36）の概要（4/11）

項目		概要
第1節	ガイドライン①	■ 1.1　協力と情報交換の目的のため、ESAsおよび所管当局は、別途合意がある場合を除き、英語でコミュニケーションを取るべきである。 ■ 1.2　ESAsおよび所管当局は、本ガイドラインで言及される情報を、別途合意がある場合を除き、電子的手段で提供するべきである。 ■ 1.3　ESAsおよび所管当局は、機構専用・機能的なメールアドレスの形で単一の連絡窓口を設置し、ESAsと所管当局間の情報交換に用いるべきである。 ■ 1.4　この単一の連絡窓口は、機密性のない情報の交換にのみ使用すべきである。ESAsおよび所管当局は、単一の連絡窓口を介した情報の安全な伝達に関する要件（例：認証された者による電子署名の要件等）について、二者間や多者間で追加合意することができる。 ■ 1.5　単一の連絡窓口の情報はESAsによって所管当局へ提供されるべきである。所管当局は、単一の連絡窓口に関する情報を、ESAsが定める運用指示に従い、遅滞なく提供・更新すべきである。 ■ 1.6　ESAsおよび所管当局は、双方が機密性および安全性を確保して情報を共有できる専用のセキュアなオンラインツールを利用すべきである。そのオンラインツールには、サードパーティによる不正アクセスからデータの機密性を保証する技術的な情報セキュリティ対策が施されている必要がある。 ■ 1.7　専用セキュアオンラインツール経由で交換される情報は、ポイント5～12及び主監督者および所管当局がDORAの業務遂行に必要な追加情報に限定すべきである。 ■ 1.8　ESAsおよび所管当局は、関係者間のコミュニケーションおよび情報交換のアクセシビリティやインクルージョン（利用しやすさ・包括性）を確保すべきである。これには、言語障壁やアクセシビリティ上のニーズを持つ者も含まれる。その場合、ESAsおよび所管当局は翻訳サービスや字幕付きビデオ会議ソフトなどのアクセシブルなコミュニケーションツールを利用することができる。ただし、データが第三者による不正利用から保護されている必要がある。

所管当局とESAの協力および情報交換に関するガイドライン

所管当局とESAの情報交換に関するガイドライン（JC/GL/2024/36）の概要（5/11）

項目		概要
第1節	ガイドライン②	■ 特定の事情により迅速な対応が求められる場合や、関連する業務の完了に追加の時間が必要となる場合には、主監督者は、関係する所管当局と協議のうえ、ポイント5から12で定められた期限を短縮または延長することができる。主監督者は、その変更内容および理由を記録しなければならない。
	ガイドライン③	■ 3.1 監督協力および情報交換に関して見解の相違が生じた場合、ESAsおよび所管当局は相互に合意できる解決策の実現に努めるべきである。合意に至らない場合は、主監督者が共同監督ネットワーク（Joint Oversight Network）と協議のうえ、意見の相違を監督フォーラム（Oversight Forum）に提示し、監督フォーラムは相互合意に資する見解を示す。
	ガイドライン④	■ 4.1　可能な場合には、所管当局および主監督者は、同指令（NIS2）に基づき重要または本質的な主体を監督するNIS2当局との対話から得た関連情報を、相互に提供し合うべきである。これには、重要なICTサードパーティサービスプロバイダーサービスプロバイダーとして指定された者に関する情報が含まれる。

所管当局とESAの協力および情報交換に関するガイドライン

所管当局とESAの情報交換に関するガイドライン（JC/GL/2024/36）の概要（6/11）

項目		概要
第2節	ガイドライン⑤	■ 5.1 DORA第31条第1項(a)に基づき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目的のため、所管当局は、DORA第28条第3項で言及される情報の登録簿を受領した後、遅滞なくその全文をESAsに対して、ESAsが定める書式および手順に従い提供するべきである。 ■ 5.2 また、所管当局は、DORA第31条第2項に規則される重要性評価を円滑に進めるため、ESAsが利用できる、関連する定量的・定性的な情報を、所管当局が保有する範囲でESAsに提供するべきである。この際、DORA第31条第6項の委任法（delegated act）を考慮するものとする。 ■ 5.3 要請があれば、所管当局は監督活動で取得した追加の情報をESAsに提供し、重要性評価を支援するべきである。
	ガイドライン⑥	■ 6.1　ESAsは、ICTサードパーティサービスプロバイダーからの受領後10営業日以内に、ICTサービスを利用する金融機関の所管当局に対し、DORA第31条第11項に従って重大（クリティカル）指定申請を行ったICTサードパーティサービスプロバイダーおよび、グループに属している場合は親グループの法的名称、識別コード、本店所在地国を提供すべきである。 ■ 6.2　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提供するICTサービスを利用している金融機関の所管当局と以下の情報を共有すべきである： ➢ a) DORA第31条第13項に従い、EU域内に設立された子会社の経営体制に構造変化があった旨の重要ICTサードパーティサービスプロバイダーから通知を受け取った後、10営業日以内にその内容を共有すること。 ➢ b) DORA第31条第5項及び第11項に従い、重要ICTサードパーティサービスプロバイダーへの重要指定決定を通知した後10営業日以内に、重要指定されたICTサードパーティサービスプロバイダーの法的名称、識別コード、本店所在地国、およびグループに属する場合は親グループの情報、さらにDORA第31条第5項に従って実際に監督業務の対象となる開始日を共有すること。

所管当局とESAの協力および情報交換に関するガイドライン

所管当局とESAの情報交換に関するガイドライン（JC/GL/2024/36）の概要（7/11）

項目		概要
第3節	ガイドライン⑦	■ 7.1　DORA第33条第4項で言及される年次監督計画の最終化前に、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提供するICTサービスを利用する金融機関の所管当局へ、年次監督計画案を提供すべきである。 ■ 7.2　年次監督計画案には、予定されている総合的な調査又は査察に関する以下の情報を含めるものとする。 ➢ a)監督活動の種類（総合的な調査又は査察） ➢ b)ハイレベルな範囲および目的 ➢ c)概算の実施期間 ■ 7.3　所管当局は、年次監督計画案の受領後30営業日以内にコメントを提出することができる。 ■ 7.4　主監督者は、年次監督計画および複数年度監督計画を採択後10営業日以内に、所管当局へこれらを提供すべきである。 ■ 7.5　主監督者は、年次監督計画および複数年度監督計画の重要な更新が行われた場合、更新の採択後遅滞なく所管当局へ重要な更新内容を提供すべきである。所管当局は、年次監督計画の重要な更新の受領後30営業日以内にコメントを提出することができる。
	ガイドライン⑧	■ 8.1　DORA第38条第5項、第39条第3項および第36条第1項に基づく総合的な調査又は査察の開始の少なくとも3週間前、または総合的な調査又は査察の場合は可能な限り速やかに、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提供するICTサービスを利用する金融機関の所管当局に対して、当該総合的な調査又は査察を担う委任を受けた者の身元を通知すべきである。 ■ 8.2　委任を受けた者には、以下が含まれる： ➢ 主監督者の関連職員 ➢ DORA第40条第2項に定められた共同検査チームのうち、当該総合的な調査又は査察のために任命された職員 ■ 8.3　主監督者は、委任を受けた者が重要なICTサードパーティサービスプロバイダーによる検査への抵抗（不当な条件付け等を含む）があったことを発見した場合、そのICTサービスを利用する金融機関の所管当局に対してその旨を通知すべきである。

所管当局とESAの協力および情報交換に関するガイドライン

所管当局とESAの情報交換に関するガイドライン（JC/GL/2024/36）の概要（8/11）

項目		概要
第3節	ガイドライン⑨	■ 9.1　重要なICTサードパーティサービスプロバイダーへの情報提供依頼が採択されてから10営業日以内に、主監督者は、共同監督ネットワーク（Joint Oversight Network）およびそのICTサービスを利用する金融機関の所管当局に対し、DORA第36条第1項6および第37条第1項に基づき重要なICTサードパーティサービスプロバイダーに提出された情報提供依頼の関連範囲について提供すべきである。 ■ 9.2　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報告した場合、以下の事項について、重要なICTサードパーティサービスプロバイダーが提供するICTサービスを利用する金融機関の所管当局に通知すべきである。 ➢ 金融機関に対して欧州連合内で直接または間接的に影響を及ぼした主要インシデント（関連の詳細を含み、インシデントの重要性および国境を越えた影響の評価に必要な情報を含む） ➢ 重要なICTサードパーティサービスプロバイダーのICTサードパーティサービスプロバイダーリスク戦略に関する重要な変更 ➢ ICTサービス提供の継続性および持続可能性に重要なリスクとなる可能性がある事象 ➢ 重要なICTサードパーティサービスプロバイダーが提出する、監督計画案の顧客（DORAの対象外事業者）への予想される影響、および必要に応じてDORA第33条第4項に言及されたリスクを緩和するための解決策を提示する根拠付きの声明 ■ 9.3　重要なICTサードパーティサービスプロバイダーが監督に関する事項で所管当局と直接連絡を取る場合、所管当局はその通信内容を主監督者に提供し、主監督者が監督業務に関する全ての事項の主たる連絡窓口であることを、重要なICTサードパーティサービスプロバイダーに改めて周知すべきである。
第4節	ガイドライン⑩	■ 10.1　主監督者が発出した勧告のフォローアップに関しては、以下の一般原則が適用される。 ➢ 所管当局は、自らが監督する金融機関に対する主たる連絡窓口であり、重要なサードパーティのサービスを利用している金融機関に関して、勧告で指摘されたリスクへのフォローアップについて責任を負う。 ➢ 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対する監督事項全ての主たる単一の連絡窓口であり、重要なICTサードパーティサービスプロバイダーに向けた勧告のフォローアップについて責任を負う。

所管当局とESAの協力および情報交換に関するガイドライン

所管当局とESAの情報交換に関するガイドライン（JC/GL/2024/36）の概要（9/11）

項目		概要
第4節	ガイドライン⑪	■ 11.1　主監督者は、重大なサードパーティが提供するICTサービスを利用する金融機関の所管当局に対し、以下の情報を提供しなければならない： ➢ a. 主監督者が受領後10営業日以内に： • 主監督者が発出した勧告の遵守を通知する重大なサードパーティからの通知および当該サービスプロバイダーによる是正計画 • 勧告を遵守しない旨の重大なサードパーティによる根拠付き説明 • DORA第35条第1項(c)に従い重大なサードパーティが実施した措置や是正策を記載した報告書 ➢ b. DORA第42条第1項に定める60暦日が満了した後10営業日以内に： • DORA第35条第1項(d)に基づき、勧告の発出後60暦日以内に重大なサードパーティから通知が送付されなかった場合の事実 ➢ c. 主監督者が採択後10営業日以内に： • 主監督者の勧告に従わない重大なサードパーティの説明が十分であるかどうかの評価、および十分と認められた場合の勧告修正に関する主監督者の決定 • DORA第35条第1項(c)に従い重大なサードパーティが実施した対応策の評価。もし十分に措置が実施されていない場合には、少なくともDORA第42条第8項のa～d基準をカバーするものとする • DORA第35条第6項に基づき、重大なサードパーティに対して定期的な制裁金の支払いを科す決定。ただし、主監督者がDORA第35条第10項に従い制裁金の公表を行わないことを選択した場合、情報を受け取った所管当局も公表しないこと • 主監督者の助言と異なる方針に基づき勧告の承認を拒否した重大なサードパーティーの行為が、多数の金融機関または金融分野の重要な部分に悪影響を及ぼす可能性があるかどうかの評価

所管当局とESAの協力および情報交換に関するガイドライン

所管当局とESAの情報交換に関するガイドライン（JC/GL/2024/36）の概要（10/11）

項目		概要
第4節	ガイドライン⑪	■ 11.2　DORA第42条第10項に従い、重要なサードパーティが主監督者からの勧告を部分的または全面的に承認しなかった場合、所管当局は以下の情報を主監督者へ提供しなければならない： ➢ a. 所管当局による採択後10営業日以内に： • DORA第42条第4項に従い、金融機関が主監督者から発出された勧告で特定されたICTサードパーティサービスプロバイダーリスクに十分対応しなかったと判断した場合、意思決定がなされる可能性について金融機関へ通知 • DORA第42条第7項に基づく所管当局による個別警告と、主監督者がこうした警告によって金融の安定性への潜在的リスクが一貫して緩和されたかどうかを評価するために必要な関連情報 ➢ b. 協議後10営業日以内に： • DORA第42条第5項に記載された意思決定前のNIS2当局との協議結果（可能な場合） ➢ c. 金融機関から情報受領後10営業日以内に： • 主監督者の勧告に対応するために金融機関が重要なサードパーティとの既存契約に加えた重要な変更 • DORA第28条第8項に記載された、金融機関の出口戦略及び移行計画の実施開始 ■ 11.3　ESAsは、所管当局と協議の上、11.2で定義された情報の伝達を円滑にするためのテンプレートを作成するものとする。

所管当局とESAの協力および情報交換に関するガイドライン

所管当局とESAの情報交換に関するガイドライン（JC/GL/2024/36）の概要（11/11）

項目		概要
第4節	ガイドライン⑫	■ 12.1　所管当局は、金融機関が主監督者の勧告で特定された固有リスクに対処する適切な契約条件を採用しない場合、その金融機関に対して「意思決定がなされる可能性がある」旨を通知する意向を主監督者に連絡しなければならない（DORA第42条第4項参照）。12.2の適用目的のため、所管当局は、可能な決定に関するあらゆる関連情報を主監督者に提供し、緊急の決定を採用する意向がある場合はその旨を明確に伝えるべきである。 ■ 12.2　情報を受領後、主監督者は、その決定がサービスの一時停止または終了となる重要なサードパーティにどのような影響を与える可能性があるかを評価しなければならない。情報受領後10営業日以内、または所管当局が緊急決定を採用する意向がある場合は可能な限り速やかに、主監督者はその評価を関係する所管当局に提供すべきである。所管当局は、その評価が拘束力のないものであることを考慮しつつ、12.1で言及された通知の発出の是非を決定する際に参考にするものとする。 ■ 12.3　同一の重要なサードパーティのICTサービスを利用している金融機関に対し、2つ以上の所管当局が決定を行う、または行う予定の場合、主監督者は、加盟国間で金融機関が同一サービスを利用する際に監督アプローチの不整合や相違が生じ、それが競争条件の不均衡につながる可能性がある場合は、その事実を当該所管当局に通知するものとする。

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーである合同会社デロイト トーマツならびにそのグループ法人（有限責任監査法人トーマツ、デロイト トーマツ サイバー合同会社、デロイト トーマツ税理士法人、DT弁護士法人および合同会社デロイト トーマツ グループを含む）の総称です。デロイト トーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従いプロフェッショナルサービスを提供しています。また、国内約30都市に2万人超の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト、www.deloitte.com/jp をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイトネットワーク”）のひとつまたは複数を指します。DTTL（または“Deloitte Global”）ならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTLおよびDTTLの各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。DTTLはクライアントへのサービス提供を行いません。詳細は www.deloitte.com/jp/about をご覧ください。
デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ベンガルール、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、ムンバイ、ニューデリー、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、最先端のプロフェッショナルサービスを、Fortune Global 500®の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促進することで、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来180年の歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をパーパス（存在理由）として標榜するデロイトの約46万人の人材の活動の詳細については、www.deloitte.com をご覧ください。

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301

IS/BCMSそれぞれの認証範囲はこちらをご覧ください
htサードパーティ://www.bsigroup.com/clientDirectory