Stand out for the right reason
金融サービスにおけるリスクと規制

PRAによる外部委託およびサードパーティ・リスク管理規則案の公表

HOT TOPIC
2019年12月

ハイライト

PRAは、EBAアウトソーシングガイドラインを実施する、銀行・保険会社・第三国支店向けの監督上のステートメント（Supervisory Statement）に係る市中協議案を公表した。また、PRAのオペレーショナルレジリエンス方針との整合性の確保を推進するとともに、外部委託契約以外の幅広いサードパーティ契約の金融機関による管理に対する期待事項を明確化している。

概要

2019年12月5日、英国規制当局は、オペレーショナルレジリエンスに関する数々の市中協議文書（CP：Consultation Paper）を公表した（「オペレーショナルレジリエンスに関するHot Topic」を参照）。

これらに加え、PRA（Prudential Regulation Authority）は、外部委託およびサードパーティ・リスク管理に関する監督上のステートメント（Supervisory Statement）案であるCP30/19を公表した。同ステートメント案は、あらゆる形態の外部委託およびサードパーティ・リスク管理に係るミクロプルーデンスの枠組みを、以下の方法で強化し、高度化することを目的としている。

- CP29/19「重要なビジネスサービスに係るオペレーショナル・レジリエンスの影響許容度（Operational resilience impact tolerances for important business services）」におけるオペレーショナル・レジリエンスに関する政策案を補完する。
- クラウドやその他の新技術のレジリエンスを強化し、導入を推進する。
- EBA（欧州銀行監督機構）アウトソーシングガイドライン（EBA Outsourcing Guidelines）を実施する（PwCの「At a Glance」を参照）。
- クラウドサービス業者への外部委託に関するEIOPA（欧州保険・年金監督局）ガイドライン（EIOPA Guidelines on Outsourcing to Cloud Service Providers）案、およびICT・セキュリティリスク管理に関するEBA（欧州銀行監督機構）によるアウトソーシングガイドライン（EBA Guidelines on ICT and security risk management）案を考慮する。

監督上のステートメント案は、以下のすべてに関連する。

- 英国の銀行、住宅金融組合、PRA指定の投資会社（「銀行等」）
- ソルベンシーIIの適用対象である保険会社・グループ、再保険会社・グループ（「保険会社等」）
- 海外の銀行等・保険会社等の英国支店

主な英国固有の分野

当市中協議文書（CP）は、EBAアウトソーシングガイドラインを実施するにあたっての要件の追加、強化、または要件の明確化を提案している。主な提案の概要は、以下のとおりである。

比例性の原則：外部委託およびサードパーティ・リスク管理に対する企業の対応は、その規模、内部組織、リスク特性および業務の内容・範囲・複雑性に見合ったものであるべきである。これには、システミックな重要性も含まれる。例えば、当局対応担当者が自社の影響度区分を1または2であると示した企業は、自社が「重要性（significant）」があり、より高い期待事項の適用対象となると考えるべきである。

マテリアリティ対クリティカリティ：クリティカルな機能または重要な機能の外部委託を表すためによく用いられていた「クリティカルな外部委託（critical outsourcing）」という用語に代わって、「マテリアルな外部委託（material outsourcing）」という用語が採用されている。これは、「クリティカルな機能（critical function）」や「クリティカル・サービス（critical service）」といった、異なるが部分的に重複する用語と混同しないようにするためである。

オペレーショナルレジリエンス、および重要なビジネスサービスの重視：外部委託のマテリアリティを判断する基準には、運用上の不備や障害が企業のオペレーショナルレジリエンス（すなわち、重要なビジネスサービスの提供を継続する能力）を著しく損なう可能性があるかを考慮することが追加された。

より幅広い「サードパーティ契約」を対象：企業は、外部委託契約だけではなく、あらゆるサードパーティ契約から生じるリスクを特定・管理・報告するための適切なガバナンスおよび内部統制を整備することが期待されている。企業は、外部委託契約以外の契約がPRAの基本規則（Fundamental Rules）、事業継続、ガバナンス、オペレーショナルレジリエンスおよびリスク管理に関する一般的な要件・期待事項の適用対象であることに留意する必要がある。このような契約の例として、特定のソフトウェア製品や技術ソリューションの購入、サードパーティとのデータ共有を伴う契約が挙げられている。

グループ間取引に関するガイダンス：グループ間取引が本質的に外部のサードパーティ（「ベンダー等」）との取引に「劣らずリスキーである（no less risky）」というEBAの見解を支持しつつ、統制・影響のレベルやグループ規程類への依存状況を検討することによって、リスク管理業務についてより比例的なアプローチを実施することができるという追加ガイダンスが提供されている。これには、実施したデューデリジェンスの変更、契約書の修正、監督業務の頻度・強度の調整が含まれる。

リスク選好をサポートするための許容度の導入：CPは、取締役会の責任を定めており、これには、(1) リスク管理態勢および戦略が適切かつ実効的であることを確保する、(2) 外部委託に係るリスク選好および（EBAによるものに加えて）許容度を設定する、(3)「クリティカルなサービスプロバイダー」への企業の依存状況を理解する、等が含まれる。

アプローチを代替可能性（substitutability）までに拡大：CPは、EBAのアプローチを代替可能性までに拡大し、デューデリジェンスを実施するにあたって、代替サービスプロバイダーを特定することまで含めるよう要求している。

重要なビジネスサービスの提供を含む再委託：再委託先によってもたらされる追加的なリスクも評価することが求められている。このため、監視活動は、重要なビジネスサービスの提供に関与する再委託先（会社の影響許容度内に収まることができるかも含む）にまで拡大される。

リスク評価をすべてのサードパーティ契約について実施：CPは、マテリアリティに関係なく、外部委託契約を含め、すべてのサードパーティ契約に係る潜在的リスクを評価すべきであることを企業に再確認している。リスク評価はマテリアリティに応じて行うべきであるが、その際、以下についても検討すべきである。

- 深刻であるが、蓋然性の高いシナリオ分析に基づくオペレーショナルリスク
- 「ステップイン」リスクを含む、金融リスク

集中リスクおよび「ベンダーロックイン」の概念：CPは、個社およびグループの両レベルで、サードパーティへの過度の依存と集中リスクを管理することの重要性を強調している。また、このような過度の依存および集中リスクが、同一または「密接な繋がりのある（closely connected）」サービスプロバイダーまたは代替が困難なサービスプロバイダーとの複数の契約（「ベンダーロックイン（vendor lock-in）」）によって生じるものであるとし、二つの新たな概念を導入している。

データセキュリティのさらなる重視：CPは、クラウド契約のための「責任共有モデル（shared responsibility model）」に関する追加ガイダンス、データ分類、保存データ・使用中のデータ・実行データに対するリスク・ベース・アプローチに係る期待事項など、データセキュリティをより重点的に取り扱っている。

届出要件：CPは、企業に対し、既存の届出要件を再確認させるとともに、「マテリアルな外部委託契約を締結する、または大幅に変更する」場合には、PRAに事前かつ適時に届け出ることを明確に要求している。

事業継続およびコンティンジェンシー：CP29/19に定められているとおり、CPは、ビジネス・コンティンジェンシー・プランの実施・検証を、企業の重要なビジネスサービスに係る影響許容度に応じて実施するよう求めている。企業はまた、業務中断や緊急事態が発生した場合に、関連する社内外のすべてのステークホルダーに情報を提供するための「実効的な危機コミュニケーション手段」が整備されていることを確保すべきである。

出口戦略・計画：企業はすべてのシナリオに備えた出口戦略を策定すること（また、新たな技術ツールなどイグジットの実行可能性に影響を与える可能性のある開発を踏まえて、これらを定期的に更新すること）が期待されているが、CPでは、業務中断が他の事業継続策では対応できないような場合の「リスク軽減の最終手段（risk mitigation of last resort）」として、ストレス状況における出口計画に重点を置いている。

外部委託の取決めの明確化：外部委託の取決めはすべて、書面に定められるべきである。また、マテリアルな外部委託契約については、最低限記載すべき事項を定めており、特に以下に掲げる項目に関する要件に重点を置いている。

- データセキュリティ
- アクセス、監査および情報に係る権利
- 再委託
- 事業継続計画および出口計画

アクセス、監査および情報に係る権利にリスクベースおよび成果ベースのアプローチを適用：マテリアルな外部委託における無制限のアクセス、監査、情報に係る権利は、以下に適用されるべきである。

- データ、デバイス、情報、システム、ネットワーク
- 会社・財務情報
- 外部監査人、職員、敷地

企業は、オンサイト監査および一括監査（pooled audit）に加えて、オフサイト監査の実施、サードパーティの証明書・報告書の利用など、監査および情報収集に成果ベースのアプローチを適用することができる。

外部委託のレジストリに関する詳細：監督上のステートメント案の付属文書には、EBAアウトソーシングガイドラインに準拠して外部委託のレジストリを構築するための追加の指針が提供されている。これには、取引主体識別子によるサービスプロバイダーの把握、マテリアリティに関する記述の文字制限、代替可能性の拡大が含まれる。契約はサービスごとに把握すべきであり、PRAは、外部委託のレジストリの対象を拡大し、サードパーティ契約を含めることに対する意見も募集している。

今後のステップ

企業は、監督上のステートメント案が既存の枠組みならびにEBAおよび（または）EIOPAに係る現行の取り組みに与える影響を評価し、市中協議文書にコメントを提供すること（期限は2020年4月3日）が奨励されている。

PRAは、2020年後半に（オペレーショナルレジリエンスに係る方針に沿って）最終方針を公表する予定である。企業は、PRAと期限の延長について、（個別に）合意に至らなかった場合には、2020年12月31日までに遵守することが期待されている。

なお、EIOPAクラウドガイドライン案の適用対象である契約については、遵守期限が2022年7月1日に後ろ倒しとなる可能性がある。

お問い合わせ先　**辻田　弘志**
パートナー
T：090 1424 3247
E：hiroshi.tsujita@pwc.com