プログレス・ウェビナー

サードパーティ・リスク・マネジメントの実践ポイント

PwC Japan有限責任監査法人
加藤美保子

Agenda

1 内外の監督当局の動向と期待事項

2 サードパーティ・リスク・マネジメント フレームワーク

3 Appendix　評価項目例

1

内外の監督当局の動向と期待事項

TPRMと、経済安全保障、オペレジ、サイバーとの関係

サードパーティリスクの効果的な管理は、経済安全保障、オペレジやサイバーセキュリティの強化を促し、本邦法令や監督当局の規制の期待値に沿うことにもなります。

経済安全保障管理の向上	オペレジの向上	サイバーセキュリティの向上

外部の脅威や不確実性にさらされない
• 金融インフラ導入時に政府審査
  • 情報処理システム
  • 業務アプリ
  • オペレーティング・システム
  • ミドルウェア、サーバーなど
 	
（金融庁/内閣府：金融分野における経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度/令和6年6月）
	災害等が発生しても重要な業務を最低限維持
	
	• 重要なサードパーティと対話・連携・管理
	
	（金融庁：オペレーショナル・レジリエンス確保に向けた基本的な考え方/令和5年4月）
		金融分野におけるサイバーセキュリティ強化と金融システムの安定
		
		• サプライチェーンに由来するサイバーインシデントにより、金融機関等が多大な影響を受けることを未然に防ぐ
		
		（金融庁：金融分野におけるサイバーセキュリティに関するガイドライン（案）/令和6年7月中パブコメ中）

サード・パーティリスク管理

受入審査、期中モニター、サプライチェーン管理など

- リスクのある先を受け入れない
- 期中のモニター（例、集中リスク）
- サプライチェーンのモニターと管理

（FSB「サードパーティ・リスク管理及び監督の強化）

世界各地の関連規制

金融機関のサードパーティ利用の拡大に伴い、サードパーティのリスクが金融機関の業務に与える影響が増加しています。管理態勢の構築・強化や当局への報告義務を規制化する方針が示されています。

バーゼル銀行監督委員会（BCBS）

- 2020年8月にオペレーショナル レジリエンスとオペレーショナルリスクに関する原則を公表し、各国中銀の関連する取組みを強化するための、原則的なアプローチを紹介。2021年3月に上記の原則文書を改定する形で、「**オペレーショナル レジリエンスのための諸原則**」最終文書を公表
- 2025年12月に**健全なサードパーティリスク管理のための諸原則**を発表。銀行のサードパーティリスク管理について、取締役会等の責任、リスク管理枠組みの実施、リスク評価、デュー・デリジェンス、契約締結、オンボーディング、継続的なモニタリング、業務継続管理、契約終了に言及している。

金融安定理事会（FSB）

- 2020年9月、FSBは、**アウトソーシングやサードパーティとの関係性に関する規制・監督上の問題点**についてのディスカッションペーパーを公表。国境を越えた依存関係を持つ金融機関、監督当局およびサードパーティ間のグローバルな対話を促進することを目的とし、当局間サーベイで特定された実務的課題（金融機関および監督当局からのサードパーティ内部の情報・システムへのアクセス制約、サブコンリスク特定の困難さ、そのためのリソースの不足等）が紹介されている。
- 2023年12月、FSBは、**サードパーティリスクの管理とオーバーサイトの向上：金融機関と金融当局のためのツールキット**を発表。

日本（金融庁）

- 主要行等向けの総合的な監督指針において、**外部委託先管理の整備方針やリスク管理態勢の整備に関する期待事項**を規定している。
- 2023年4月 「オペレーショナル・レジリエンス確保に向けた基本的な考え方」のディスカッションペーパーを発出。サードパーティーリスクについて言及。
- 2024年10月 「金融分野におけるサイバーセキュリティに関するガイドライン」を公表。サイバーセキュリティ管理態勢の強化に加え、サードパーティリスク管理に関する対応事項にも言及。

英国（BOE、PRA、FCA）

- 2021年3月、BOEとPRAは、**アウトソーシングとサードパーティリスク管理**に関する金融機関への期待をまとめた監督声明を公表。同時期に公表されたオペレーショナル・レジリエンスに関する要件と期待を補完するものであり、また、クラウドや新たなテクノロジーのレジリエンスを促進し管理することを目的としている。2021年にオペレーショナルレジリエンスに関する規制化、2022年に効力発生。2025年3月には各行が検討しインパクトトレランス内での活動を行うことを求めている。

米国（FRB, OCC, FFIEC）

- 2013年10月OCCは**サードパーティ利用時のリスク管理に関するガイダンス**を、また同年12月FRBは**アウトソーシングリスク管理に関するガイダンス**を公表。2020年10月には、FRB・FDIC・OCCにより**オペレーションレジリエンス**に関するサウンドプラクティス文書が公表されている。
- FFIECは2019年11月にBusiness Continuity Management bookletを公開し、**サードパーティ管理の在り方**を明記している。あくまでも指針を示すに留まっており、当局への登録や報告の義務はガイダンスに明記されていない。
- 2023年6月、FDIC, FRB, OCCは、レジリエンスの観点を含めた外部委託先管理についての最終ガイダンスを公表

欧州連合（EC、EBA）

- 2019年2月、EBAは**アウトソーシングに関するガイドライン**を公表（同年9月末発効）。Proportionalityへの配慮の必要性に言及しつつ、**アウトソーシング契約前・契約期間中のリスク評価やガバナンスに関する期待事項**を規定している。
- 2023年1月、欧州委員会がデジタルオペレーションレジリエンス法（DORA）を発効。**当局や金融機関がICTサービスの中断に対するレジリエンスを確立することを目的とした規制**として、2025年1月運用開始。2025年11月、クリティカルサードパーティのリストを公表。

BCBS「健全なサードパーティリスク管理のための諸原則」

銀行のサードパーティリスク管理について、銀行に対する9つの原則及び監督当局に対する3つの原則からなる計12の原則を示しています。

ガバナンス、リスク管理、戦略
原則1：取締役会は、銀行のサードパーティリスクの監督について最終的な責任を負い、明確な戦略を承認し、銀行のリスクアペタイトとそれに伴う混乱に対するトレランスを定義する必要がある。
原則2：取締役会は、シニアマネジメントが、銀行のサードパーティ戦略に沿って、サードパーティリスク管理フレームワーク（TPRMF）のポリシーとプロセスを実施していることを確認する必要がある。これには、サードパーティサービスプロバイダーの実績とサードパーティサービスプロバイダー契約に関連するリスクの報告、およびリスク軽減策の取締役会への報告が含まれる。

リスク評価
原則3：銀行は、サードパーティサービスプロバイダー契約を締結する前とサードパーティサービスプロバイダー契約のライフサイクル全体を通じて、特定されたリスクと潜在的なリスクを評価および管理するために、サードパーティリスク管理フレームワークに基づく包括的なリスク評価を実施する必要がある。

デューデリジェンス
原則4：銀行は、契約を締結する前に、将来のサードパーティサービスプロバイダーに対して適切なデューデリジェンスを実施する必要がある。

契約締結
原則5：サードパーティサービスプロバイダー契約は、契約当事者全員の権利と義務、責任、期待を明確に規定した法的拘束力のある書面による契約によって管理されるべきである。

オンボーディングと継続モニタリング
原則6：銀行は、デューデリジェンスや契約条項の解釈中に特定された問題の解決を含め、新しいサードパーティサービスプロバイダーの円滑な導入を支援するために十分なリソースを投入すべきである。
原則7：銀行は、サードパーティサービスプロバイダー契約のパフォーマンス、リスク及びクリティカリティの変化を継続的に評価・監視し、その結果を取締役会及びシニアマネジメントに報告すべきである。銀行は、問題が発生した場合には、適切な対応をとるべきである。
原則8：銀行は、サードパーティサービスプロバイダーサービスの途絶が発生した場合でも業務を継続できるよう、頑健な事業継続管理を維持する必要がある。

契約終了
原則9：銀行は、サードパーティサービスプロバイダー契約の計画的な終了に関する終了計画と、計画外の終了に関する終了戦略を維持すべきである。

監督当局の役割
原則10：監督当局は、銀行の継続的な評価の不可欠な一部として、サードパーティリスク管理を評価すべきである。
原則11：監督当局は、銀行セクターにサービスを提供する1つまたは複数のサードパーティサービスプロバイダーの集中によってもたらされるリスクを含め、潜在的なシステミックリスクを特定するために入手可能な情報を分析すべきである。
原則12：監督当局は、銀行にサービスを提供するクリティカル・サードパーティサービスプロバイダーがもたらすシステミックリスクを監視するために、セクター横断的および国境を越えた調整と対話を促進すべきである。

出所：Principles for the sound management of third-party risk, Basel Committee on Banking Supervision, 2025年12月

FSB「サードーパーティリスク管理および監督の強化」

FSBは、2023年12月に金融機関・監督当局のためのサードパーティリスク管理強化への包括的かつ具体的なプログラム（Toolkit)を発表しました。特に金融機関には、以下の8つの項目の強化を求めています。

1. 重要な業務の特定と重要性の評価

- 重要な業務の特定には以下を考慮すること
  - 業務の戦略上の重要性と当行のコアビジネスとは何か？
  - 特定のビジネス停止の銀行経営への影響は何か？など
- 重要性の評価を常に最新の状態に保ち、陳腐化を防ぐこと

2. サービスプロバイダー（SP)の受入審査と期中モニター

- 受入審査は、SPのリスクレベルに応じて深度を変え、審査ポイントは
  - SP受け入れによる便益、コストとリスク
  - SPのサービス提供と継続能力、など
- 期中モニターはリスクレベルに応じて経常又は定期モニター等を実施

3. 金融機関への事務事故報告

- 金融機関は、適時の事務事故の当局報告及び改善計画の策定が求められ、SPとの契約に以下の事務事故報告の基準等を考慮する
  - 事故の種類や影響とその内容
  - 必要最低限の速報情報、など

4. サードパーティ相互連関マッピング

- 有効なサードパーティのマッピングは、明確・整合性があり以下を含む
  - サードパーティのリスクレベル
  - オペレジ目的で、重要な業務のend to endのグループ会社及び外部のサードパーティを含めた内部・外部相互依存関係

5. サービスプロバイダーのサプライチェーンの管理

- 金融機関は、重要な業務に影響する場合、以下も考慮する
  - SPのサプライチェーンに関わるリスクの特定
  - SPのサプライチェーン・リスクをモニター・管理・低減する方策

6. 業務継続

- サードパーティ・サービスプロバイダーに以下をコミットさせる
  - 金融機関にとって重要な業務に関わる適切なBCP
  - テスト計画と実施結果（学び、脆弱性、対応計画を含む）
  - 金融機関のBCPテストへの参加

7. 出口戦略

- 重要な業務に関わるサードパーティ・サービスプロバイダーの不測の事態（例、サービス低下、業務停止）の出口戦略は、以下を考慮
  - 影響を最小限にする契約書上の合意
  - 有形及び無形資産返還のプロセス、など

8. 集中リスクの管理

- 集中リスクの特定方法としては、以下があり、低減・管理を考慮する
  - 1つのSPまたはSPグループがサポートする当社の業務数
  - 1つのSPまたはSPグループがサポートする当社の重要業務数
  - 地理的集中

出所：「Enhancing Third-Party Risk Management and Oversight - A toolkit for financial institutions and financial authorities」FSB発行（2023年12月）をもとに、PwCが作成

BCBS「オペレーショナルレジリエンスに関する諸原則」

2021年の改訂版では、重要な業務の提供に関わるサードパーティやグループ内組織への依存度を管理するべきと述べており、オペレーショナルリスク管理のフレームワークと整合したリスクアセスメントを行うことや、重要なオペレーションを提供するサードパーティーに関するBCPの策定を求めています。

1. ガバナンス

- リスクアペタイト、リスクキャパシティ、リスクプロファイルを考慮したレジリエンスレベルの設定
- リスク強度は強いが蓋然あるシナリオ（“Severe but plausible”）の想定

2. オペレーショナルリスク管理

- PSMORのフレームワークの上にレジリエンスを確立
- オペレーショナルレジリエンスに関連する管理フレームワークの協調の必要性（例：BCP、サードパーティ管理、RRP等）
- 脅威と脆弱性の特定・評価および改善プロセスの必要性
- チェンジマネジメントの強化、拡張

3. BCPとテスティング

- 重要業務（Critical operations）の特定
- 重要な依存関係の特定
- 相互連関と相互依存を考慮したBCPの策定と管理
- RRP（再建・処理計画）との整合

4. 重要業務に係る相互連関と相互依存の把握

- 重要業務に関連する人材、テクノロジー、プロセス、情報、ファシリティ、サードパーティ、グループ会社（機能提供会社）とその関連性の把握（マッピング）

5. サードパーティー管理

- 重要業務の提供に関わるサードパーティやグループ会社のレジリエンス能力の評価と管理
- 上記について自社と同等の水準の管理を有しているか検証する必要

6. インシデント管理

- インシデントのライフサイクル管理（インシデントの影響度評価とリソース配分、インシデント管理プロセス、コミュニケーション）

7. 情報通信技術（ICT）のレジリエンス

- 情報資産、インフラの管理
- サイバーセキュリティ

出所：「オペレーショナルレジリエンスの諸原則」協議文書（2020年8月）をもとに、PwCが作成

デジタルオペレーショナルレジリエンス法（DORA）

EUの金融業界のデジタルオペレーショナルレジリエンスに関する規制であり、日本企業であってもEU内に拠点を置いている金融機関、EUの金融機関にサービスを提供しているICTサービスプロバイダーも対象となります。

1. 目的

DORA（デジタルオペレーショナルレジリエンス法）は、EUレベルでデジタルオペレーションレジリエンスのための詳細かつ包括的な規制を定義しています。

目的:

EU加盟国間の金融分野における現地規制を調和させ、それによって:

- 金融機関およびICTサードパーティ（TPP）が、あらゆる種類のICT関連の混乱に適時かつ適切に対応し、回復することを確保する
- ICTリスクマネジメントの向上
- 金融監督当局が、金融機関とそのICTサードパーティをより厳格に監視・監査する権限を付与する
- ナレッジシェアを含めた統一的な事故報告の仕組みの導入

2. コントロールエリア

ガバナンス要件：特にマネジメントボードの役割

ICTリスク管理：識別、保護・予防、検知、対策・復旧、学習、高度化・コミュニケーション

ICT関連インシデントを当局に報告する

デジタル運用のレジリエンステスト：少なくとも年に1回実施される独立したテストに使用される評価基準、テスト、方法、手順、ツールの定義

ICTサードパーティのリスク管理：金融機関によるICTサードパーティのリスク監視の要件、重要なICTサードパーティへの監督的枠組みの適用

情報共有：サイバー脅威に関する情報を金融機関間で共有すること

3. 対象事業者

信用機関、保険会社、職業的退職金提供機関、資本管理会社、市場インフラなどを含む**EU内の約22,000の金融会社**、およびICTサービスプロバイダーなど

金融庁「オペレーショナルレジリエンス確保に向けた基本的な考え方」1/2

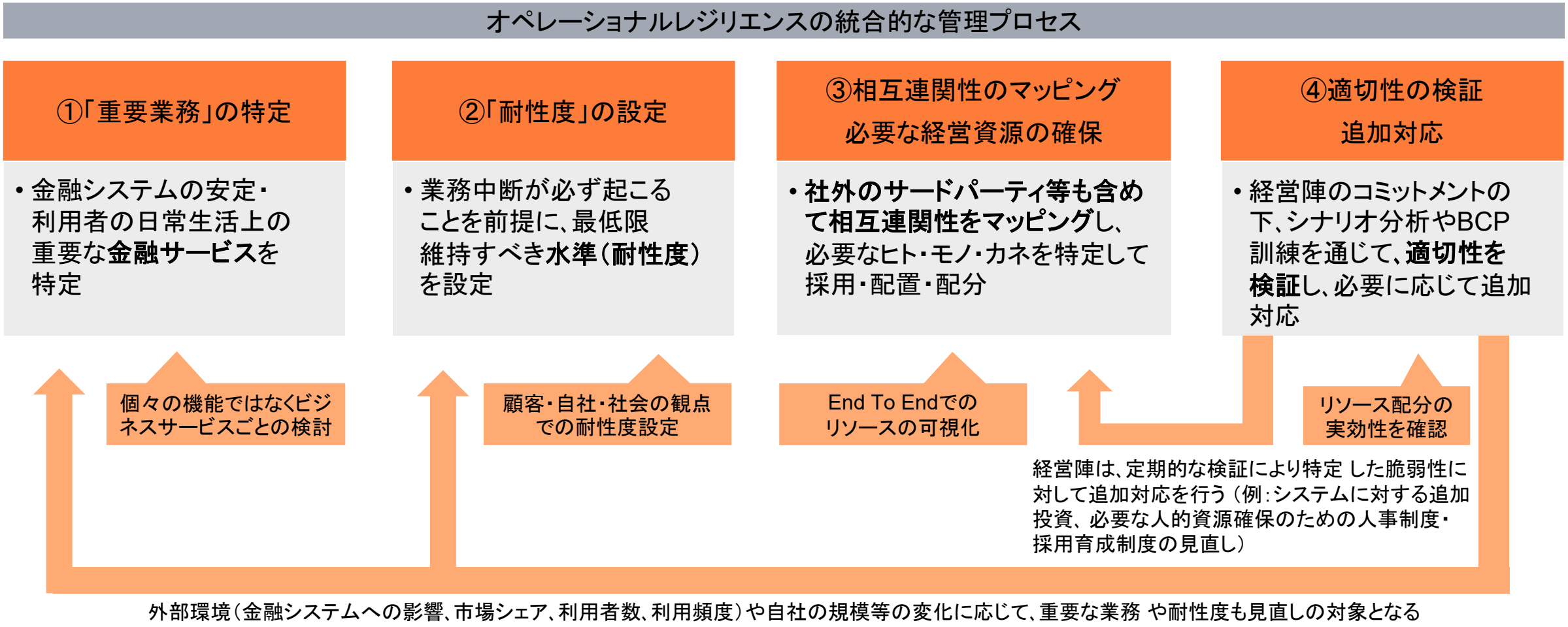
金融庁は、2022年8月「2022事務年度金融行政方針」において、オペレーショナルレジリエンスの対応について言及し、2023年4月「オペレーショナル・レジリエンス確保に向けた基本的な考え方」のディスカッションペーパーを発出しました。

金融庁による オペレジの定義	システム障害、テロやサイバー攻撃、感染症、自然災害等の事象が発生しても、金融機関が重要な業務を、最低限維持すべき水準（耐性度）において、提供し続ける能力
ディスカッションペーパー の概要	• オペレーショナルレジリエンスとして求められる対応はBCBSや英国の要請事項と凡そ、共通。 • サードパーティリスク、サイバーセキュリティに触れるのは当然として、オペレーショナルリスク、BCP／BCM、再建・処理計画（RRP）、更にはコンプライアンスリスク（コンダクトリスク）についても言及。 • 主たる対応として4つのステップに係るプロセスを提示。 ① 「重要な業務」の特定 ② 「耐性度」の設定 ③ 相互連関性のマッピング、必要な経営資源の確保 ④ 適切性の検証、追加対応 • 社内外の経営資源の相互連関性のマッピングにより、重要な業務の最低限維持すべき水準（耐性度）で提供するために重要なサードパーティを特定した後は、そのサービス品質を確認・維持することや、代替手段の確保、出口戦略の策定などの依存度の管理が必要となることに言及。

出所: オペレーショナルレジリエンス確保に向けた基本的な考え方, 金融庁, 2023年4月

金融庁「オペレーショナルレジリエンス確保に向けた基本的な考え方」2/2

特定した「重要業務」であるビジネスサービスを支える重要なリソースの一つとして、社外のサードパーティーを捉えています。



出典: 金融庁「オペレーショナルレジリエンス確保に向けた基本的な考え方」（概要）

経済安全保障推進法

2022年5月に成立した「経済安全保障推進法」の4つの制度のうち、「基幹インフラ役務の安定的な提供の確保」においては、基幹インフラの重要設備が我が国の外部から行われる役務の安定的な提供を妨害する行為の手段として使用されることを防止するため、重要設備の導入・維持管理等の委託の事前審査、勧告・命令 等を措置している。

特定社会基盤役務の安定的な提供の確保に関する制度（基幹インフラ制度）

- 銀行、証券（第一種金融商品取引業者）、保険会社等が一定のシステムを導入、維持管理の委託を行う場合、政府が、安全保障の見地から、あらかじめ、その内容やベンダーの情報を審査し、必要な措置の実施または導入・維持管理の委託の中止を勧告・命令することが可能となり、2024年5月から施行された

  →内閣府：「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」
  →金融庁：対象事業者となる銀行等の指定など

- 目的は、日本が直面する多様なリスクに対処し、国の経済と安全保障を強化するため

- 以下の「導入」や「重要な維持管理の等の委託」には金融庁に事前の届け出が必要
  - 情報処理システム
  - 業務アプリ
  - オペレーティング・システム
  - ミドルウェア、サーバーなど

- 届け出の内容は
  - 導入や維持を支援する業者・機器の供給業者の役員や議決権保有者のバックグラウンド
  - 構成設備の製造工場など

IIA 専門職的実施の国際フレームワーク（IPPF）トピック別要求事項

内部監査人協会（IIA）は、「トピック別要求事項（Topical Requirements）」"第三者" を公表

- 本要求事項は、「専門職的実施の国際フレームワーク®（IPPF）」を構成する要素の一つであり、「グローバル内部監査基準™」と併せて、内部監査の必須事項に関するものと位置づけられている
- 「第三者」に関するトピック別要求事項は、内部監査部門が、ベンダー、サプライヤー、請負業者、下請業者、外部委託サービス・プロバイダなどに対するアシュアランス業務を実施する際の基準を示している

IPPFを構成する３つの要素

- グローバル内部監査基準
- トピック別要求事項
- グローバル・ガイダンス

専門職的実施の国際フレームワーク®（IPPF）

出所：トピック別要求事項（Topical Requirements）」"第三者"（日本語版）, The Institute of Internal Auditors - Japan, 2025年9月

2

サードパーティリスクマネジメントフレームワーク

内部監査に期待される役割

サードパーティーリスクマネジメントについて、内部監査は監査やモニタリングを通じて、組織に価値を提供することが期待されます。

リスクアセスメント、年度監査計画

- 監査ユニバースに、サードパーティリスクマネジメントや重要業務（重要ビジネス・サービス）を取り込む。少なくとも〇年に一度は、保証を提供する。

個別監査

- 重要業務（重要ビジネス・サービス）を対象とする監査において、End to Endで監査スコープを設定する。プロセスフローチャート等を作成する際には、重要なリソースとして、重要なサードパーティーもカバーする。
- サードパーティに関する残余リスクが、リスクアペタイトの範囲内に収まっているかを確認する（監査評定、意見に反映）。

サードパーティの評価

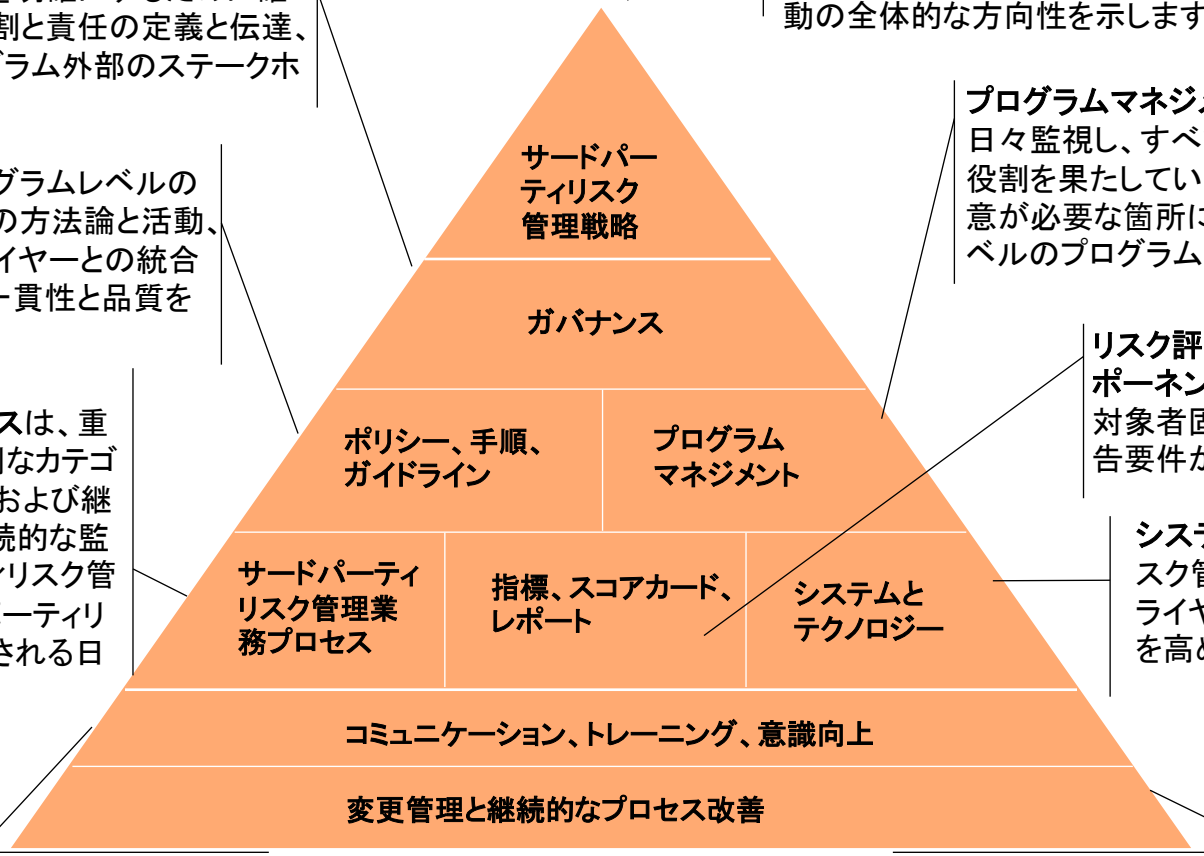
- BAUとしてのサードパーティーリスクマネジメントのライフサイクルにおいて、重要なサードパーティの評価、監査を行うことでビジネス部門を支援する。

Third-party Risk Management program framework

ガバナンスは、サプライヤーリスク管理活動を実施するための組織的枠組みとガバナンスモデルを明確にするために確立されます。これには、報告体制、役割と責任の定義と伝達、プログラムの組織的適用範囲、プログラム外部のステークホルダーとの連携が含まれます。

ポリシー、手順、ガイドラインは、プログラムレベルの要件、プログラムの監視、リスク評価の方法論と活動、リスク許容レベル、および他のサプライヤーとの統合ポイントを定義し、プログラム活動の一貫性と品質を確保します。

サードパーティリスク管理運用プロセスは、重要なサードパーティ関係の管理、特別なカテゴリのサードパーティの取り扱い、初期および継続的なデューデリジェンス、契約、継続的な監視、アクティブ/パッシブサードパーティリスク管理、および出口戦略を含む、サードパーティリスク管理活動を促進するために実施される日常的なプロセスと管理です。



サードパーティリスク管理戦略は、サードパーティリスク管理機能とサポート役割の要件と活動の全体的な方向性を示します。

プログラムマネジメントは、機能しているプログラムを日々監視し、すべての主要な関係者が求められている役割を果たしていることを確認し、プログラム領域で注意が必要な箇所には是正措置を講じます。あらゆるレベルのプログラム関係者との連携も含まれます。

リスク評価活動およびプログラムの運用コンポーネントには、データの品質と正確性、および対象者固有の報告を確保するための指標と報告要件が存在します。

システムとテクノロジーは、グループが共通のリスク管理プロセスを使用することを促進し、サプライヤーリスク管理プログラムの有効性と効率性を高めます。

コミュニケーション、トレーニング、および意識向上により、サプライヤーのリスク機能とプログラムのビジネス価値を関係者に通知するためのチャネルが作成されます。

変更管理と継続的なプロセス改善により、企業全体でプログラムを効果的に導入し、関係者のフィードバックを通じて継続的なプログラム改善を組み込むための基盤が確立されます。

日本の金融機関におけるサードパーティリスク管理の課題

最近のサードパーティが関係する事案の発生や、海外における当局の規制強化に鑑み、日本の金融機関におけるサードパーティリスク管理の課題としては、以下のようなものがあげられます。

- **管理すべきサードパーティの範囲**：管理対象とすべきサードパーティの範囲をどこまで広げるか。業務委託先以外のアライアンス先やJV先など、どこまでを含むべきか。
- **再委託先及び再々委託先の管理**：サプライチェーンを構成するサードパーティについてどこまで（再委託先、再々委託先等）を管理すべきか。またその管理手法はどのようにするべきか。特定の再委託先への集中リスクをどのように評価し、管理するのか。
- **管理対象リスク**：管理対象リスクとして、コンプライアンスやサードパーティ側の業務継続性等に加え、どこまでを含めるべきか。特に業務回復力を含むレジリエンスや、人権・ESGなど、新しいリスク領域についてどこまで含めるか。
- **管理の担い手**：サードパーティの種類や管理すべきリスクが多様化しているため、契約所管部署によるリスクの管理には限界がある。社内のどの部署でサードパーティリスクを管理すべきか。また自社でサードパーティに関するすべてのリスクを適時適格に捕捉し続けるのは限界があるので、管理の効率性を高めるためにどのように外部サービスを活用することができるのか。
- **重要度に応じた管理手法**：サードパーティの重要度をどのような基準で判定し、メリハリをつけた管理手法を実現していくのか。重要先にはどこまで踏み込んだリスク評価を行うべきか。
- **ガバナンス**：サードパーティリスク管理のレポートラインをどう設計するのか。またグループ全体、およびグローバルでの管理態勢をどのように設計し、本社にどこまでの情報を集約すべきか。

管理対象のサードパーティと管理対象リスク

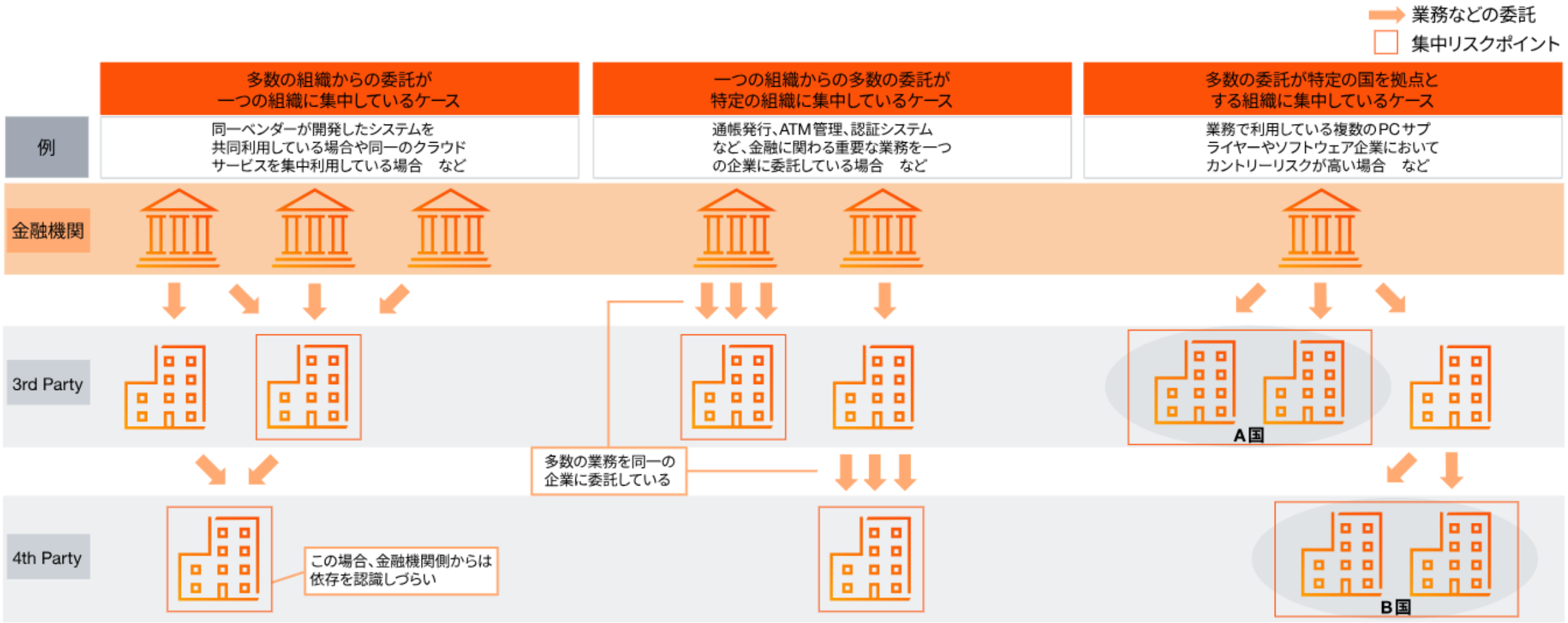
一般的に金融機関が管理するサードパーティ及びその対象リスクを概観すると、下表のようなものがあります。この中から自社のビジネスモデルや市場特性を踏まえ、最適な管理項目を特定していきます。

管理対象サードパーティ
業務委託先（重要ビジネスサービスに係る者）
業務委託先（上記以外）
アライアンス先
ジョイント・ベンチャー（JV）
データ提供先（Data Aggregator）
情報ベンダー（例：Bloomberg、Reuters）
クラウドサービス業者
ソフトウェアベンダー
ブローカー
カストディアン
専門家事務所（法律、会計等）
広告代理店
サプライヤー
金融市場インフラ（FMI）
ユーティリティ（電力会社）
カウンターパーティ/コルレス銀行
グループ企業
政府系機関

管理対象リスク		
サービスに関するリスク	オペレーショナルレジリエンス	事業継続性（BCM/BCP）
		IT/ システムリスク
		サイバーセキュリティ
	情報セキュリティ	データプライバシー
		データインテグリティ
	物理的セキュリティ	
	カントリーリスク	
	コンプライアンス	
	代替可能性	
	集中リスク（サービス/地理的）	
サードパーティーに関するリスク	組織構造・所有関係	
	財務状態	
	専門性・能力(災害対応等含む)	
	許認可・資格（該当する場合）	
	利益相反	
	倫理基準	
	汚職・贈収賄	
	AML/KYC	
	税務コンプライアンス	
	集中リスク（特定サードパーティへの集中）	
	Environmental , Social and Governance (ESG)	
	レピュテーションリスク	
	リーガルリスク	
	再委託リスク	

集中リスクの例

ICTサードパーティーのリスク管理の一環として、金融機関からの依存度の高い一つの組織等で発生した問題が原因となり、金融機関の業務に影響を与える「集中リスク」の重要性が高まっています。



サードパーティリスクマネジメントのガバナンス

欧米系のG-SIBsでは、専門性の確保とコスト削減の観点から、1線内にTPRM管理部署を有し業務を集約する傾向がみられます。TPRM管理部署に対しては、オペレーショナルリスク専門部署が2線として監督します。

TPRMガバナンス構造の例

TPRM管理部署の機能の例:
- プログラムの遵守状況の日々のモニタリング
- TPRMプログラムの関係者（委託元部署、調達、リスク専門部署）との調整（リスクアセスメント、期中モニタリング含むライフサイクル管理）
- プログラムの改善と報告の監督
- TPRMに関する手続き、テンプレート、評価基準、およびツールをビジネスユニットに提供

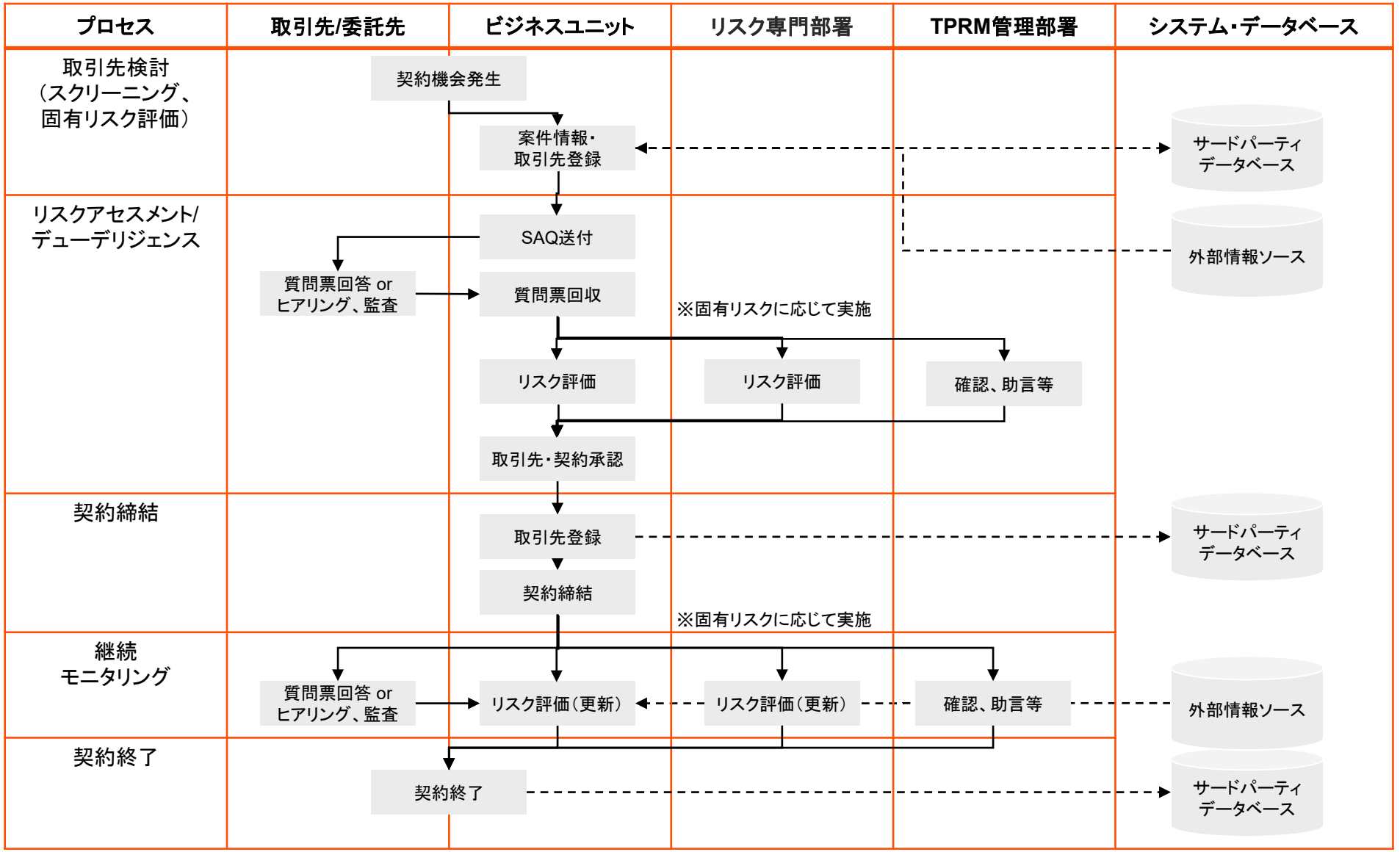
1線、2線の役割・責任の例

2線
- ガバナンス機関であるリスク管理等の委員会は、サードパーティのリスクポリシーとリスクプロファイルの許容範囲を承認する責任を負う。また、重要なサードパーティの承認や、TPRMプログラムの有効な整備についての最終責任を負う。
- オペレーショナルリスクの所管組織は、2線として、1線のTPRM管理部署が中心となって管理するTPRMプログラムおよび運用について監督および支援する。

1.5線
- 各リスク専門部署は、契約、財務状況の評価等、必要な専門知識を提供し、TPRM管理部署を支援する。
- 各リスク専門部署は、各領域のリスク管理について専門知識を提供し、ビジネスユニットのリスク評価の実施を支援する場合もある（オペレーショナルリスク、情報セキュリティ、法務等）。

1線
- TPRM管理部署は、TPRMプログラムの管理・運用に責任を負う。
- 調達部門は、調達方針の策定、コスト分析・戦略立案、購買プロセスの整備、サプライヤーの管理等を実施
- ビジネスユニットは、サードパーティリスクのオーナーとして、TPRMポリシーに従ってリスクを管理する責任を負う。サービス提供状況のモニタリング、検出された問題・懸念の報告を含む。

サードパーティリスクマネジメントの運営プロセス例



サードパーティリスクの固有リスクスコアリング例

リスクレーティング	財務インパクト 事業1	事業2	事業3	顧客影響	レピュテーション影響	法的・規制上の影響	情報の機密性	サービス影響
Low	100万ドル未満	25万ドル未満	10万ドル未満	顧客への潜在的な損害はない	影響は局所的で、パブリシティは限定的	会社および顧客、市場への影響はほとんど、またはまったくなく、 規制当局の関心を引く可能性も低い	公開情報	サービス障害は 1 つのビジネス関係に限定される
Medium Low	100万～200万ドル	25万～100万ドル	10万～50万ドル	顧客に損害を与える可能性は低い	影響は地域レベルで、パブリシティは限定的	会社および顧客、市場への影響は限定的だが、 規制当局の関心を引く可能性はある	社内利用に限定	長期にわたる業務停止 または 特定の顧客グループまたはサービス種別に影響
Medium High	200万～1000万ドル	100万～500万ドル	50万～250万ドル	損害を引き起こす可能性があるが、 影響は小規模な顧客グループ／人口に限定される	影響は地域レベルで広く報道される または 影響はグローバルだが、関係者は限定された少数に限られる	会社および／または個々の従業員に対する規制当局による精査の可能性があり、 顧客および／または市場への影響もある	機密	重大なサービス障害 または 主要な顧客グループまたはサービス種別に影響
High	1000万ドル超	500万ドル超	250万ドル超	大規模な顧客グループに対する重大な損害	影響はグローバルで、広く報道される	会社および／または個々の従業員に対する 重大な規制当局の精査の可能性があり、 顧客および／または市場への重大な影響が生じる	極めて機密性が高い	深刻なサービス障害 または すべての顧客またはサービス種別に影響

デューデリジェンスおよび契約締結

サードパーティ リレーションシップの固有リスクに基づきリスクレーティング・区分を決定するだけではなく、契約締結前のデューデリジェンスの結果を踏まえて、契約上どのような保護を定めるかを決定する必要があります。

デューデリジェンス評価の例

1. オペレーショナルコンピテンシー
2. 財務
3. レピュテーション
4. コンプライアンス
5. 情報セキュリティ・プライバシー
6. 技術
7. 業務継続・レジリエンス
8. 物理的セキュリティ
9. 再委託先
10. カウントリーリスク

結果

指摘事項

問題点

契約条項の例

1. サービスの内容および範囲
2. 実施基準
3. 再委託先およびフォースパーティ
4. ダイバーシティ
5. 補償
6. デフォルトおよび終了
7. 秘匿性＆セキュリティ
8. 規制要件
9. 所有権、ライセンス、アクセス
10. 業務継続およびコンティンジェンシープランニング
11. 内部統制の検証
12. 通知および報告手続き
13. 責任限度
14. 保険
15. 監査権
16. 記録管理
17. 価格設定
18. コストおよび補償
19. 支払条件
20. 扮装解決
21. 経営情報システム報告および責任
22. 顧客苦情対応
23. 内容変更

サードパーティの継続的モニタリング

リスクのプロファイルに合わせた内容で、契約締結中のモニタリング、再評価を行う必要があります。

初期評価

- 監査
- 財務諸表
- 評判、苦情、訴訟
- 資格
- 内部統制
- 経営情報システム（MIS）の適切性
- 事業継続計画（BCP）/災害対策（DR）
- 開発、導入、サポート費用
- 第三者機関の活用
- 保険

オンゴーイングモニタリング

- 財務状況統制の監視
- 監査報告書
- サプライヤーポリシー
- オンサイト訪問
- コンプライアンスリスク
- BC/DR計画とテスト結果
- サービスとサポートの品質
- SLA報告
- イシューマネジメント
- 組織戦略との整合性
- 顧客からの苦情
- 顧客満足度調査
- サプライヤーとの定期的なミーティング

再評価

- 戦略目標との一致
- 専門性
- 費用対効果
- 顧客の期待
- 情報セキュリティ
- 物理的セキュリティ
- 事業継続計画
- 財務デューデリジェン
- スレピュテーションデューデリジェンス

ダッシュボード

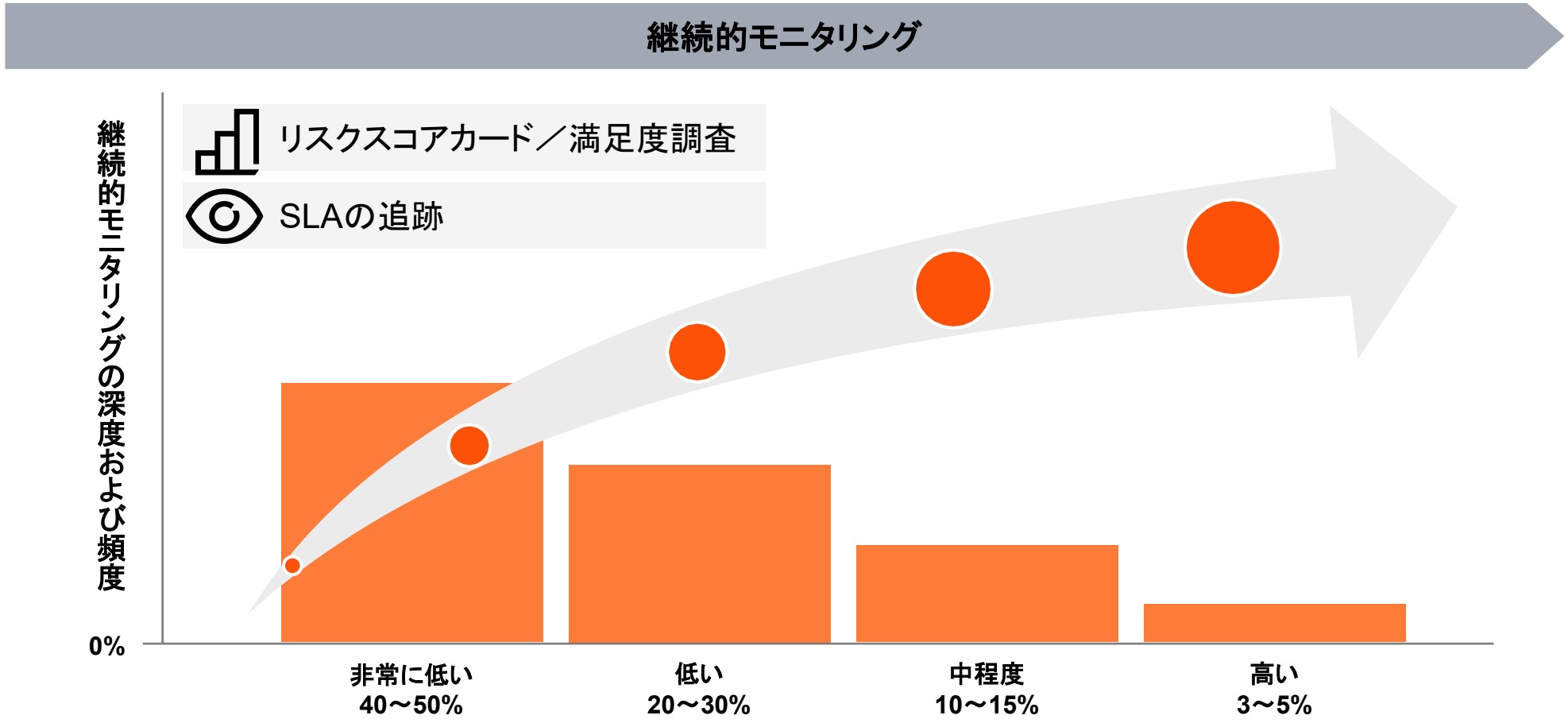
- サプライヤーサービス情報を集約
- サプライヤープロフィール

スコアカード

- パフォーマンスとリスクの監視
- 個々のサプライヤーのパフォーマンス

サードパーティの継続的モニタリング

リスクに応じてモニタリングの深度、頻度を調節し、効率的にモニタリングを行います。



サードパーティリスクマネジメント　ダッシュボード

ダッシュボードを活用することで、サードパーティーに関する潜在的なリスクについての示唆を提供したり、管理状況を可視化することが可能となります。

サードパーティリスクマネジメント管理指標例

Key Performance and Risk Indicators (KPIs and KRIs)の例として、サードパーティリスク（潜在的、顕在）を示す指標、統制に関する指標、等があります。

ダッシュボードにて可視化し、リスクへの対応状況を把握し、改善に繋げます。

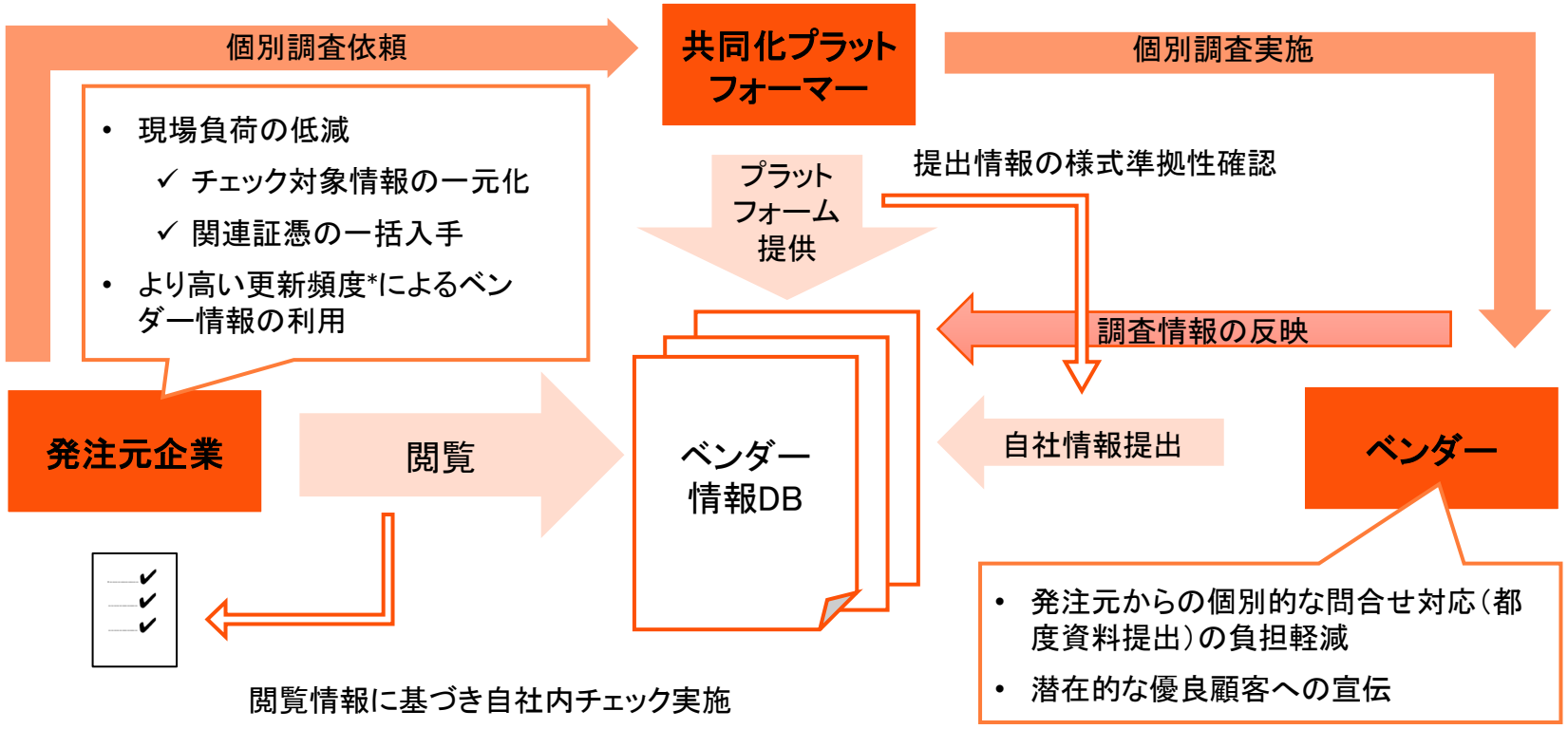
- サードパーティ別の課題件数
- 管理しているサードパーティ数
- 業績指標および報酬にリスク管理目標が反映されている従業員の割合
- 発生頻度と影響度の期待される低減効果が追跡されているリスク課題の割合
- 能動的なリスク管理に関する研修を受けたスタッフの割合
- アクションプランの完了までの進捗管理

  等

共同化例 – コンソーシアムによる更なる効率化

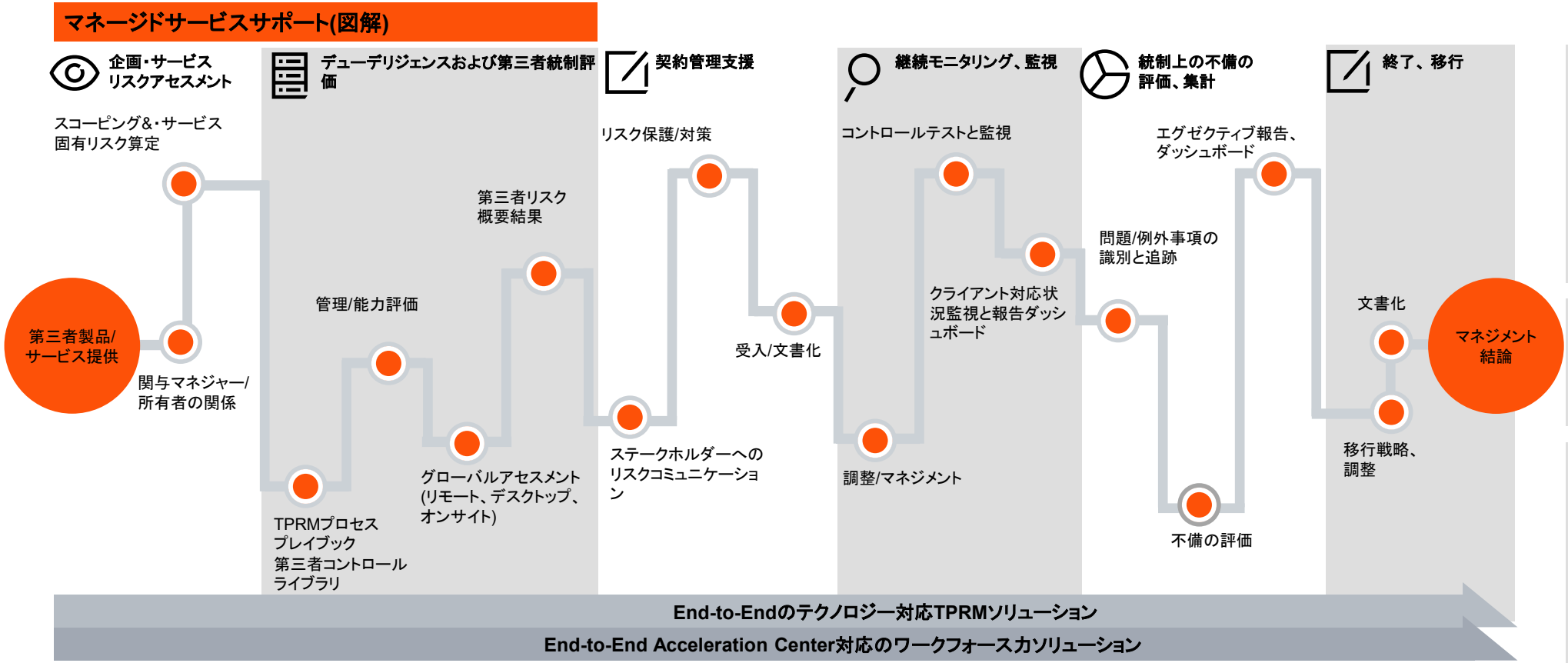
ベンダーの基本情報に加え、内部管理の状況や取引の実績等、他社も同様の情報を求めています。
プラットフォームを通じてサードパーティーの情報を共有することで、業務の重複を省き、より効率的に

サードパーティーの情報を管理することができます。



マネージドサービスの活用

以下の図では、TPRMの手法と能力のライフサイクルの概要を示しています。TPRMライフサイクルのすべてのフェーズにおいて、マネージドサービスを活用して効率化します。



主なサービス:
- アセスメントの実施
- 問題/リスク改善
- クライアントアセスメント対応プログラム(reverse TPRM)
- プログラムの管理と調整
- TPRMプログラム監査支援

お客様の責任:
- 最終評価報告書のレビュー、承認
- エスカレーションの役割(必要に応じて)

主な効果:
- コスト削減
- 付加価値活動への活用できる時間の増加/時間削減
- 効率性の向上
- 範囲の拡大
- 品質の向上
- 拡張性と機敏性

第三者の活用が増えるなか、PwCはこの課題を認識し、監査の補完的支援やお客様のコントロール要求への対応(reverse TPRM)に加え、専門知識、経験、スキルを必要な時に必要な場所で提供し、クライアントをサポートしています。

3

Appendix
評価項目例

サードパーティリスクマネジメントにおける実務例

評価項目一覧

評価項目		観点
リスクアペタイトとの整合	対象リスク	• リスクアペタイト設定（RAS）に基づくサードパーティのリスクの範囲と定義
	対象サービス・業務 / サードパーティー	• 重要ビジネスサービスや重要業務機能に基づいた管理すべきサードパーティーの範囲と定義
ガバナンス・組織体制	取締役会、委員会によるオーバーサイト	• TPRMプログラムの監督機関、担当役員
	3線モデルにおける役割・責任、 アカウンタビリティ	• TPRMプログラム管理組織、責任者 • モニタリングの実施組織、程度・深度、役割分担
	他のリスク管理の枠組みとの関係	• オペレーショナルリスクおよびサブリスクカテゴリーの所管部署の位置づけ、役割
	レポーティング	• 報告主体、報告先
ライフサイクル	プランニング	• 実施組織、実施方法
	デューデリジェンス	• デューデリジェンス、リスクアセスメントの実施組織、程度・深度、役割分担 • 外部機関、Utility（コンソーシアム）等の活用
	契約	• 実施組織、重要な条項
	継続モニタリング	• モニタリング・オーディティングの実施組織、程度・深度、役割分担 • 外部機関、外部レポート等の活用など実施方法
	契約終了	• 実施組織、実施方法
情報システム	システム	• システムの機能、使用範囲（GRC、サードパーティ情報サービス）

サードパーティリスクマネジメントにおける実務例

評価項目ごとの実務例 1/3

評価項目		観点	実務例
リスクアペタイトとの整合	対象リスク	• リスクアペタイト設定（RAS）に基づくサードパーティのリスクの範囲と定義	・評価対象のリスクは自社のリスクアペタイト、リスクタクソノミーにもとづき設定されている。（当局ガイドラインも参考にしている） 対象リスク例： 【サービスレベル】 • ITリスク、サイバーリスク、データプライバシー、情報セキュリティー、物理的セキュリティー、リーガル・コンプライアンス、サプライチェーン、事業継続・レジリエンス、パフォーマンスリスク（業務遂行能力）、レピュテーションリスク、カントリーリスク 【サードパーティーレベル】 • 組織構造とオーナーシップ、財務状況、専門知識と能力、認可/認定、利益相反、贈収賄、金融犯罪・AML、倫理基準（例：現代奴隷法、CSR、ESG）、集中
	対象サービス・業務 / サードパーティー	• 重要ビジネスサービスや重要業務機能に基づいた管理すべきサードパーティーの範囲と定義	・リスクベースアプローチにもとづき、重要ビジネスサービス、重要業務の観点から管理すべきサードパーティの対象を定義する。 対象サードパーティ例： 外部委託先（代理店含む）、情報ベンダー、クラウドベンダー、データアグリゲーター、サプライヤー、プロフェッショナルサービスファーム、アライアンス先（ジョイントベンチャー、提携先）、FMI（取引所、決済機関、保管機関）、ブローカー、間接金融業者、公共事業者（例：電気、ガスの供給会社）

サードパーティリスクマネジメントにおける実務例（続き）

評価項目ごとの実務例 2/3

評価項目		観点	実務例
ガバナンス・組織体制	取締役会、委員会によるオーバーサイト	• TPRMプログラムの監督機関、担当役員	・戦略・業務計画を実現するためのキーとなるサードパーティ、外部委託・提携業務が特定されている ・サードパーティの集中・分散に関する方針を定めている ・アウトソースしたサービスのコンチプラン（インハウスへのシフトを含む）を策定している
	3線モデルにおける役割・責任、アカウンタビリティ	• TPRMプログラム管理組織、責任者 • モニタリングの実施組織、程度・深度、役割分担	・TPRMに係る基本方針（TPRMフレームワーク・プログラム）、リスクアペタイトについて取締役会において監督 ・TPRMに係る管理委員会を1線に設置（COO）している ・TPRMオフィスを1線内に設置しサードパーティを一元管理（TPRMが設置されていない場合は調達部門が役割を担うケースが多い）（TPRMオフィスはCOOにレポート、調達部門はCFOにレポート） ・TPRMオフィス（Head of TPRM)のレポートラインはCOO ・TPRMオフィスは各リスク領域の専門部署と連携してリスク管理を実施する ・TPRMのフレームワーク及び各リスクに係る基準・ルールは2線のリスク管理部署（オペレーショナルリスク管理部署）が所管
	他のリスク管理の枠組みとの関係	• オペレーショナルリスクおよびサブリスクカテゴリーの所管部署の位置づけ、役割	・オペレーショナルリスク管理部署がTPRMに係るフレームワーク、基準・ルールを設定し、その機能状況について監督する ・TPRMに係る個別リスク（サブリスクカテゴリー）についてはサブリスクカテゴリー所管部署が基準・ルールを設定
	レポーティング	• 報告主体、報告先	・TPRMオフィス（Head of TPRM)のレポートラインはCOO

サードパーティリスクマネジメントにおける実務例（続き）

評価項目ごとの実務例 3/3

評価項目		観点	実務例
ライフサイクル	デューデリジェンス	• デューデリジェンス、リスクアセスメントの実施組織、程度・深度、役割分担 • 外部機関、Utility（コンソーシアム）等の活用	・ハイリスクのサードパーティにフォーカスしてデューデリジェンスを実施している ・リスク評価の観点に、サードパーティが提供するサービスの自社戦略上の重要性や顧客への影響が含まれる ・システムプラットフォーム上でサードパーティのリスク評価を実施 ・リスクスコアに応じDDの依頼をシステム上で実施（外部ベンダーへの依頼）
	契約	• 実施組織、重要な条項	・デューデリジェンスの結果に基づき契約条項への追加が行われている （例）オンサイトを含むモニタリング、オーディティング条項の追加　等
	継続モニタリング	• モニタリング・オーディティングの実施組織、程度・深度、役割分担 • 外部機関、外部レポート等の活用など実施方法	・契約所管部署が一義的には継続モニタリングの責任を負う ・TPRMオフィスがリスク情報を集約管理しモニタリングの支援を実施 ・上記を支援するためのシステムプラットフォームを保持（リスク情報の自動収集、アラート機能）
情報システム	システム	• システムの機能、使用範囲（GRC、サードパーティ情報サービス）	・グループで導入済みのシステムプラットフォームを利用している

ご清聴ありがとうございました。

Thank you

pwc.com