サプライチェーンリスク管理態勢構築のポイント

PwC Japan有限責任監査法人
ガバナンス・リスク・コンプライアンス・アドバイザリー部
ディレクター　**雨宮 弦太**

はじめに

現代のビジネス環境では、企業が多様な委託先や関係会社と協力して業務を進めていく場面が増えています。その中でサプライチェーンに関連する委託先のリスクは、企業の評判や事業継続に大きな影響を及ぼす可能性があります。本稿では、まず委託先管理に関する課題や、委託関係におけるパワーバランスの問題点について紹介します。次にリスクの可視化の手法や、再委託先を含むサプライチェーンを考慮したリスク識別の手法を例示します。また企業全体での評価を通じて重要なリスクを特定し、業務ごとに整理する方法について述べたうえで、委託先管理の実務が形骸化しないようにする管理態勢の構築例について説明します。

なお、文中の意見は筆者の私見であり、PwC Japan有限責任監査法人および所属部門の正式見解ではないことをお断りします。

1 委託先におけるリスク管理の必要性

委託先でのリスク管理が適切に行われない場合、企業はさまざまな危機に直面する可能性があります。近年発生している事案として、次のような例が挙げられます。

- 再委託先によるランサムウェア感染による事業の停止
- 元従業員による営業機密情報の不正持ち出し、転職先への流出
- 納品物の品質管理、プロジェクト管理
- 製品の品質不正
- 特許権や商標権の無断使用

再委託先がランサムウェアに感染した事例では、委託元の主たる事業が一時停止を余儀なくされ、被害拡大を防ぐための緊急対応が必要となりました。また、元従業員による営業機密情報（個人情報）の不正持ち出しの事例では、秘密情報が元従業員の転職先へ流出し、両社の信頼性を大きく損ねました。さらに、納品物の品質管理やプロジェクト管理の不備も無視できないリスクであり、これらの管理の不徹底が最終製品やサービスの品質を低下させ、顧客からの信用を失墜させる事例もありました。加えて、製品の品質不正のほか、特許権や商標権の無断使用といった問題も発生しています。こうした事例は、企業のブランド価値を毀損し、法的な問題に発展する可能性もあります。そのため、委託先におけるリスク管理を強化することは、企業の競争力の維持と向上に欠かせなくなっています。

近年、企業が委託先を管理する環境は急速に変化しており、省庁による関連法令の整備や、新たな制度の検討が進んでいます。例えば、経済安全保障に関わる重要インフラ事業者に対しては事前申請制度が導入され、同制度の下で特定重要設備の重要維持管理業務などへのリスク管理が求め

られるようになりました。同制度は、インフラ事業者が外部のパートナーと連携する際に、より厳格な情報管理面や品質管理面でのリスク評価と管理プロセスを要求しています。さらに、経済産業省はサプライチェーン全体のセキュリティ対策を強化するため、企業間での協力を促進する評価制度の構築を目的としたワーキンググループを立ち上げました。このワーキンググループは、サプライチェーン内の各企業がセキュリティ対策を評価・強化する枠組みを整備し、サイバーリスクなどのさまざまなリスクを未然に防ぐための指針を提供することを目指しています※1。このような動きを踏まえ、各企業は、委託業務の安全性を確保し、安定した事業運営を支援するための基盤を構築することが求められています。

2 委託先管理の難所

委託先管理は、多くの企業にとって非常に難しい課題となっています。その理由の1つは、委託先管理の責任が委託元企業の中で明確になっていないことがあります。これは委託業務の性質に応じて責任部署が異なることが多く、企業の組織体系によって管理部門が変わるため、明確な管理態勢を構築することが容易ではないことが原因として考えられます。例えば、直接原価に関連する委託業務の管理は調達部門が担当するのが一般的です。一方で、その他の業務に関連する委託は、委託元となる各部門が管理することが多くなります。このように、委託先管理の責任部署がばらばらであるため、統一的な管理手法を採用することが難しくなります。

また、委託先管理の範囲を選定や契約といったステージごとに見てみると、委託先選定ルールの制定は調達部が担当し、その後の選定ルールに基づく選定は各委託元部門が行っていることが多いです。具体的な委託内容の管理方法は各委託元部門に委ねられ、さらに、契約条項に関しては法務・コンプライアンス部門が関与します。IT機器の貸与やアクセス権の付与はIT部門が管理し、品質管理については各委託元部門が担うというように、管理の範囲はステージごとに複雑に分かれています。各ステージには異なるリスクが存在し、それらが複合的に影響するため、管理が非常に複雑化します。さらに、組織体系や委託内容によって管理手法が異なるため、委託先管理の標準化を図るのは一層困難となっています。

※1 経済産業省「サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ（概要）」2025年4月14日 https://www.meti.go.jp/press/2025/04/20250414002/20250414002-1.pdf

これらの問題を克服するには、どの部門がどの業務を委託されているかを可視化し、委託時の各ステージにおけるリスクを洗い出すことが重要です。

3 パワーバランスにおける課題

委託先管理において、委託元と委託先のパワーバランスは非常に重要な要素です。競争法や下請法（製造委託等に係る中小受託事業者に対する代金の支払の遅延等の防止に関する法律）の取引の公平性に鑑みると、委託元と委託先の関係は対等であるべきと考えられますが、実際のビジネス上のバランスはそれとは別に存在します。

不健全な関係の例として、委託元が委託先に無理な要求をするケースや、委託元が適切な要望を伝えられず、誤解やコミュニケーション不足が生じ、委託業務の円滑な運用に支障が出るケースがあります。さらに過度な依存関係もパワーバランスをゆがめる一因となり得ます。技術や製品の特殊性、あるいは長年の関係が、依存関係につながる要素として挙げられます。例えば、技術や製品の特殊性によって委託先に依存せざるを得ない場合や、長い付き合いがあると関係の変化に気づかず、適切な判断が難しくなることがあります。

ただし、パワーバランスや依存関係には、必ずしもマイナスだけの側面があるわけではありません。依存関係をうまく生かすことで、強固なパートナーシップを構築できるようになります。そのため、委託管理のリスク評価では、「委託先依存度」も考慮することが重要と考えられます。

4 管理すべき広さと範囲について

委託先管理におけるリスクを評価では、サプライチェーン全体を俯瞰し、リスクの高い部分にリソースを集中していく、リスクベースアプローチの利用が有効です。以下、委託先管理をする際のリスクベースアプローチの手法例を紹介します。

STEP1　サプライチェーンの範囲の広さと深さを識別

まず、委託先管理の対象となるサプライチェーンの全体の「広さ」と「深さ」を識別していく必要があります。実務上、サプライチェーンは複数の企業や組織が連携して構成されている場合が多く、委託先から再委託先へ委託されている場合は再委託の階層が深くなるに従って管理の難易度が上がっていきます。もし委託先や再委託先で問題が発生すると、他の

ステークホルダーにも影響が及び、最終的には製品やサービスの提供に支障をきたす可能性もあります。全体像を把握することで、各段階のリスクや依存関係を明確にし、問題が発生した際の影響範囲を予測しやすくなります。

サプライチェーンにおける「広さ」とは、企業のサプライチェーンに関わる機能領域の範囲を指します。具体的には、調達、技術サービス提供、間接サービス提供といった領域が含まれます。これにより、サプライチェーン全体の透明性を確保し、潜在的なリスクを未然に防ぐことが可能となります。サプライチェーンにおける「深さ」とは、サプライチェーンに関わる子会社、関連会社、委託先、再委託先などがどこまで続いているか、つまり階層（Tier）の深さを指します（**図表1**）。

STEP2　リスクベースアプローチによる管理すべき広さと深さの決定

「広さ」については、リスクが顕在化した際の影響度と発生可能性を考慮した上で絞り込むことが重要です。具体的には、レピュテーションリスクが顕在化した場合の金額的な被害の大きさや、その事象がどのくらいの頻度で発生する可能性があるかを考慮し、管理対象項目を絞り込みます。

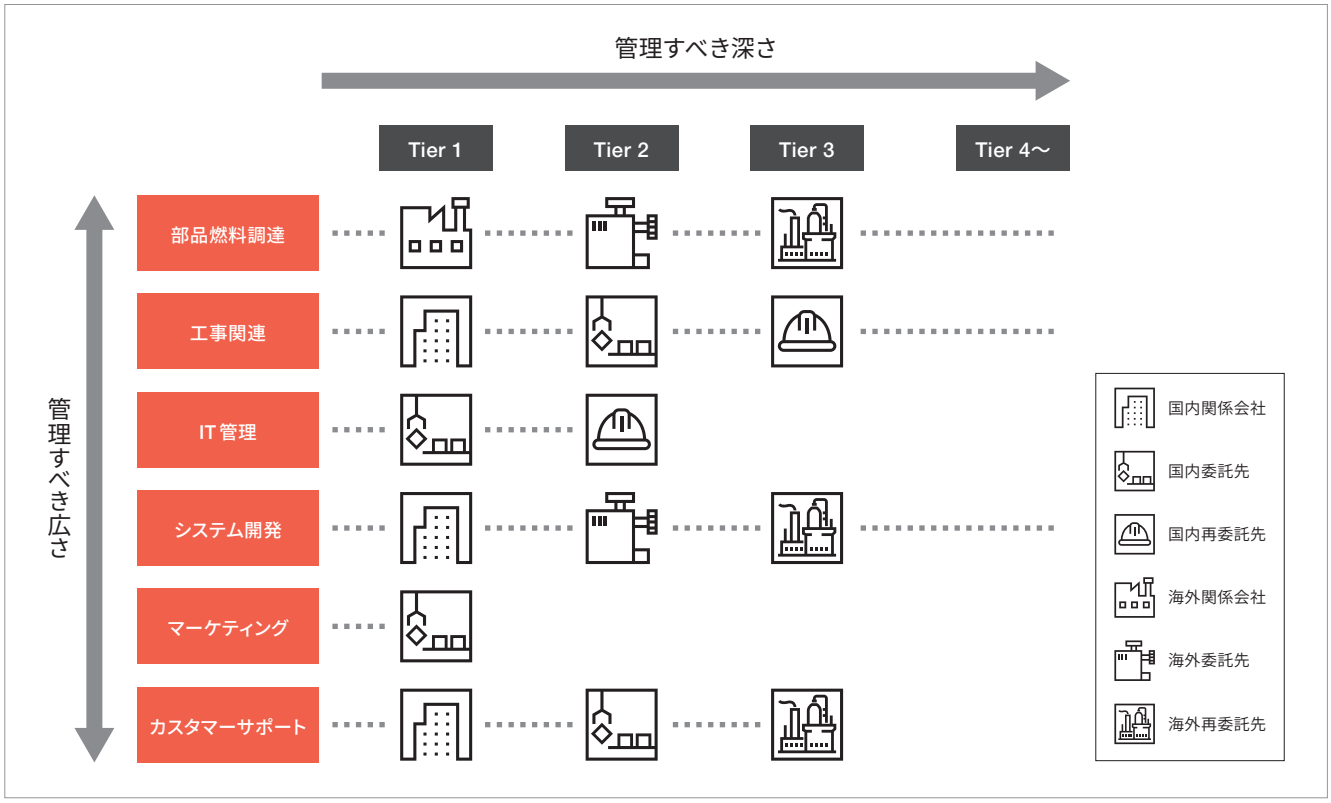
「深さ」については、委託先への管理状況をもとに、そのリスクの大きさによって決定します。また、委託先から再委託先への管理も含め、リスクの程度に応じて監督するレベルや頻度を調整することで、効率的なリスク管理を実現します。このリスクベースアプローチにより、社内資源を有効に活用し、リスクの高い部分に重点的に対応することが可能です。

以上のように、サプライチェーンリスク管理における委託先管理は、まず全体を識別し可視化した上でリスクベースアプローチを活用し、リスクの高い範囲の管理に重きを置く方式が、効果的かつ効率的な手法と考えられます。

5　委託先管理の方向性

リスクベースアプローチで管理すべき重要な委託先および委託業務を識別した後は、当該委託先をどこまで管理すべきかを決定します。例えば、サプライチェーンをたどると再委託先、再々委託先と複数の階層がありますが、全てを管理するのは簡単ではありません。しかし、直接契約関係にない再委託先で問題が起きた際は、委託元の経済的、運営的、信用面に直接影響を与え得る可能性があります。また、委託業務の責任は委託元にあります。

図表1：管理すべき委託先の「広さ」と「深さ」の識別イメージ



出所：PwC作成

以下では、法令などで再委託先管理をどこまで求めているかを見ていきます。「個人情報の保護に関する法律についてのガイドライン（通則編）」では、次のように再委託先の監督に関する方針が明確に示されています（「3-4-4 委託先の監督（法第25条関係）」を参照）。

委託元の責任（再委託時）

- 委託先が再委託を行う際、再委託先の監督が適切に行われるよう確認する。
- 再委託先が法第23条で要求される水準の安全管理措置を講じることを、委託先が確実に確認するよう指導する。
- 必要に応じて、再委託先に対する監査を実施する。

委託先の責任（再委託時）：

- 再委託が必要な場合には、委託元に事前に報告し、承認を得る。
- 再委託先にも法第23条に基づく安全管理措置を講じさせる。
- 自身が再委託先を適切に監督し、個人データの適切な取り扱いを確保する。
- 委託元の監督を受ける立場にあることを理解し、再委託に関連する手続きや監査を受け入れる。

また、「組織の内部不正防止ガイドライン」（独立行政法人情報処理推進機構）の「対策のヒントとなるQ&A14」を参照すると、例えば個人情報の場合、委託元の責任として、委託先が再委託先を適切に管理監督しているところまでを管理対象とすることが望ましいと言えます（**図表2**）。

6 委託先リスク管理の手順

次に、委託先リスク管理のプロセスを説明します（**図表3**）。

①全社的なリスク評価

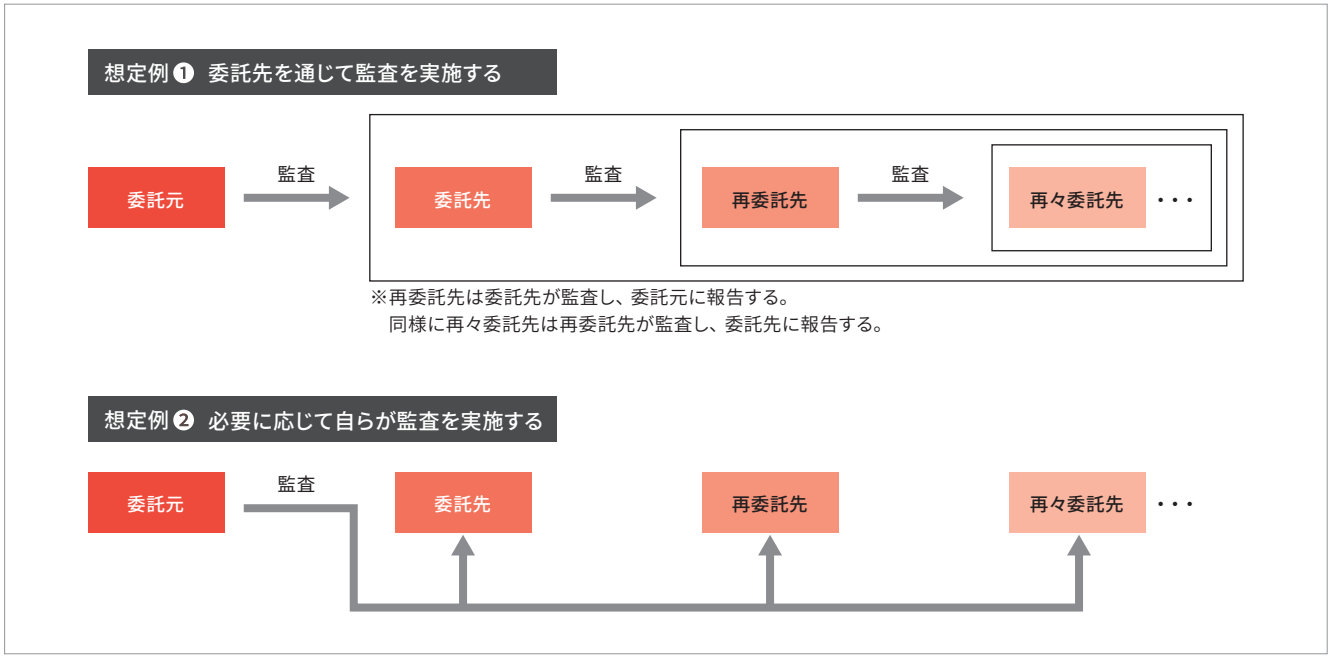
①-1　管理すべき重要なリスクの特定

すでに全社的なリスク管理の仕組みが整備されている場合は、固有リスクが高いと評価される項目を、サプライチェーン全体で管理すべきリスクの参考にすることができます。また、固有リスクが高く、リスク低減策を委託先が実施している場合には、委託元がコントロールできない、もしくはコントロールすることが難しい箇所を、管理すべき重要なリスクとして捉えるべきです。

①-2　特定したリスクにおける業務ストリームごとの整理

管理すべきリスクを特定した後、業務フローごとにどのような委託が発生しているのかを詳細に洗い出します。このステップでは、業務フローの各段階で委託が行われている対象を明確にすることが重要です。次に、部門ごとにどのような

図表2：再委託先への監査



出所：独立行政法人情報処理推進機構（IPA）「組織の内部不正防止ガイドライン」をもとにPwC作成

サプライチェーンが存在しているのかを確認しつつ、業務がどのように委託されているのか評価します。これにより、各部門が依存しているサプライチェーンの輪郭が見えてきます。この情報は、サプライヤーマスタもしくは委託先管理リストと連携すると、情報の統合管理が可能となり、より体系的なリスク管理が実現します。

続いて、当該業務の特性に基づき、管理すべきリスクの発生頻度やその影響度を簡易評価します。ここでは、リスクがどれほどの頻度で発生し得るのか、発生した場合にどれほどの影響を及ぼすのかを見極めます。最後に、リスクの高い部門や業務、すなわち優先度の高い業務ストリームに紐付く重要な委託先を特定します。

①-3　再委託先を含むサプライチェーンの可視化

重要な委託先が特定できたら再委託の状況を確認します。まずは、委託先が再委託先と締結している契約書を確認します。情報管理における条項やモニタリング・監査の条項がついているかなど、再委託先への管理レベルを改めて把握するためです。委託先へのインタビューを通して、再委託先への依存度や実務上のコミュニケーションやモニタリングの実態を聞き取ることも、管理レベルを理解するうえで有用です。また、委託元と委託先との契約書の条項に、再委託の事前申請もしくは承認を義務付けることも重要です。

②委託先ごとのリスク評価

②-1　委託先と再委託先の管理態勢を評価（成熟度）

委託先の管理状況を測定する指標を準備し、評価することが重要です。つまり、委託元として、どこまでリスクについて許容できるかを考慮したものさしを準備することを意味します。ここではPwC Japanグループのナレッジである成熟度を利用し、定量的に管理状況を可視化した例を紹介します（**図表4**）。

委託先のリスク管理態勢を確認した次に、再委託先に対する管理状況についても確認する必要があります（**図表5**）。委託先におけるリスク管理態勢が適切に行われていても、業務の大部分を再委託している場合は、再委託先への管理状況も留意する必要があるためです。

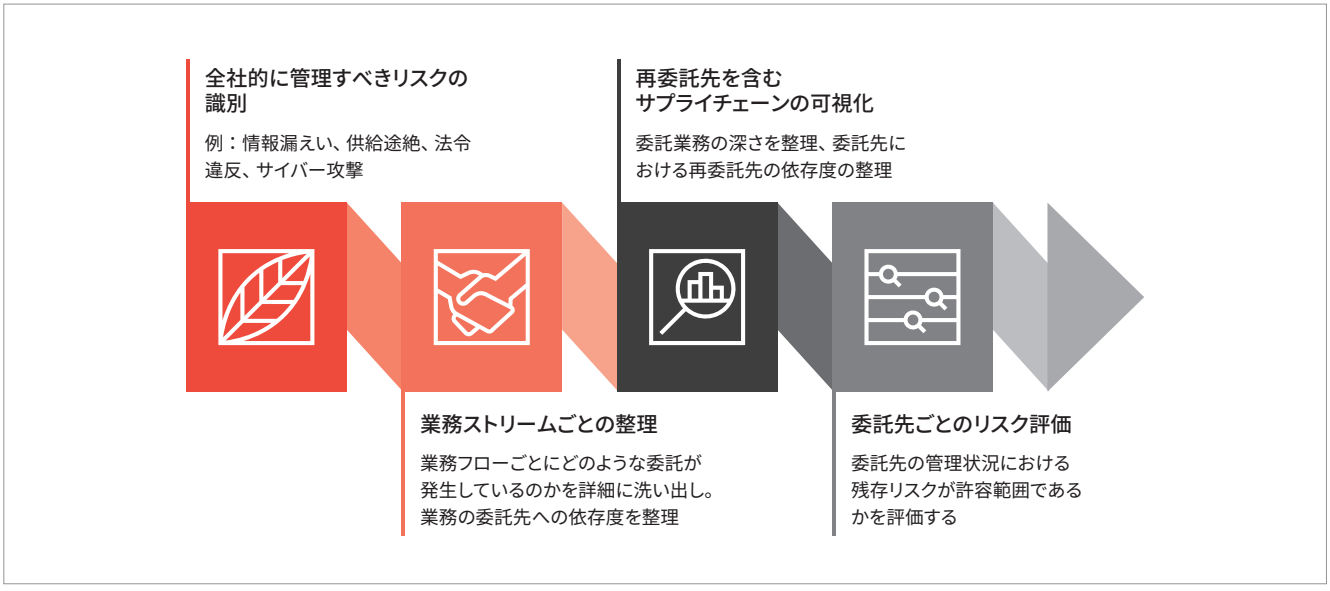
7 委託先リスク管理の実務例

ここまで委託先のリスクを可視化して、より管理すべき箇所を特定する評価方法について紹介してきました。それを踏まえて、具体的なリスク管理の実務例を以下に示します。

① 委託先モニタリング

委託先のリスク評価の結果は、継続的なモニタリングの判断に活用できます。例えば、リスクの強弱に応じて、現場でのモニタリングの要否、頻度を判断できます。情報漏えいリスクなどの管理を例にすると、重要な委託先の業務については、年に1回、現場を訪問して、インタビューや現場での情報管理状況、再委託先へ監督状況を確認することで、社内

図表3：委託先リスク評価のプロセスイメージ



出所：PwC作成

のリソースをリスクの高い箇所へ集中させられます。また、リスクレベルが高くない委託先については、自主評価シートで管理状況の回答を依頼し、確認する方法が考えられます。また、委託先管理項目には専門性が求められる領域も数多くあることから、第三者による定期的な客観的評価を通じて、現行の管理状況をモニタリングすることも、持続可能な管理手法の1つになります。

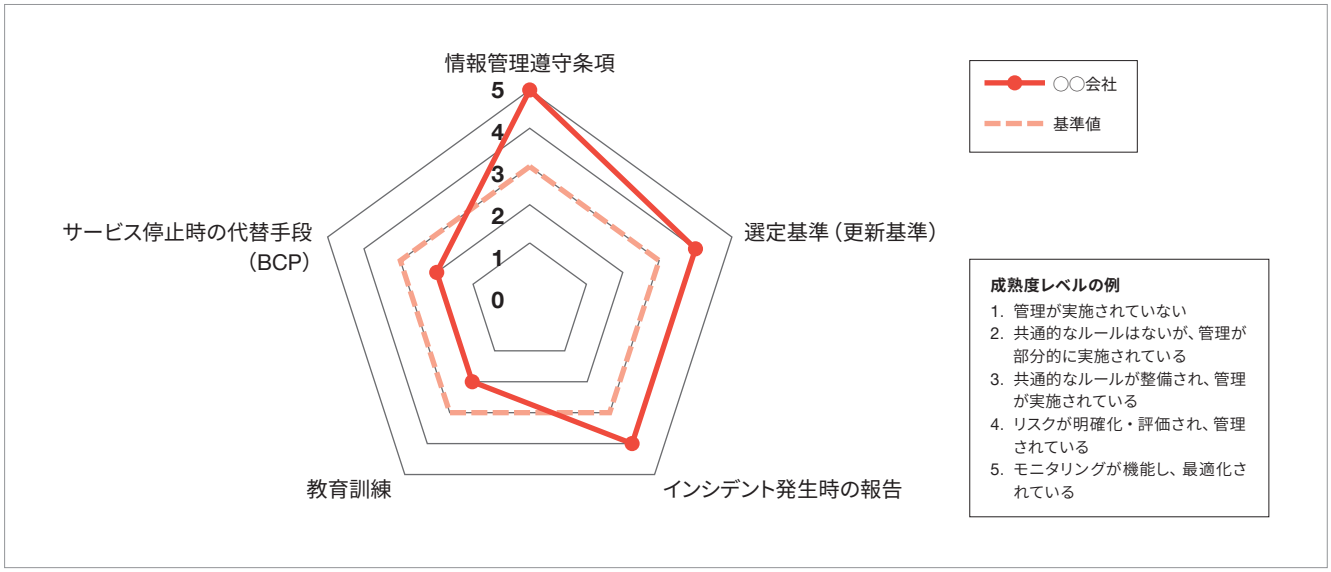
② インシデント情報の横展開

リスク管理態勢を強化していても、委託先でインシデントが発生してしまう可能性はあります。そこで、発生したインシデントの真因を詳細に分析し、その学びを他の関連する部門や委託先に展開することで、全体的なリスクを低減できます。これにより、他部門でも同様の問題の再発を防ぎ、組織全体で品質を向上させられます。また、類似業種の他社におけるインシデント情報を積極的に収集し、これを社内の委託先管理に関与する部門と共有する仕組みを整備することで、業界全体の動向を反映した能動的なリスク管理が可能になります。

③ 全社的なリスク管理の枠組みとの連動

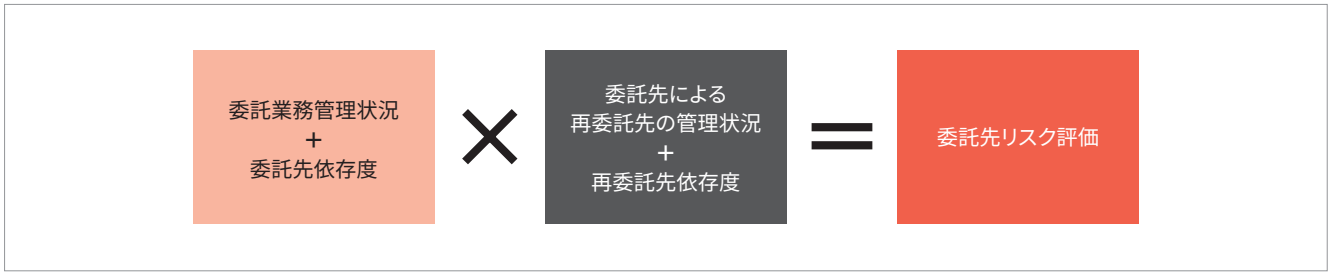
既存の全社的なリスク管理枠組みがある場合、その取り組みと連動させることで、組織全体で統一的なリスク管理が実施できます。これにより、リスク管理のオーナーが明確になり、委託先管理が単一部門による孤立した活動とならず、組織全体の戦略的ゴールと一致した形で運営できるようになります。また、リスク管理をより効果的に運用するためには、第1線（業務部門）、第2線（リスク管理・コンプライアンス部門）、第3線（内部監査部門）が、それぞれリスクの発生を予防、発見、改善する役割を担う「3線管理態勢」を構築し、全社的に管理するのがより有効な手法です。それぞれの部門が専門性を発揮することにより、実効性を持った運用が実現され、リスク管理業務の形骸化を防ぎます。

図表4：委託先リスク成熟度評価のイメージ



出所：PwC作成

図表5：委託先リスク評価のイメージ



出所：PwC作成

8 おわりに

これまで見てきたとおり、委託先、再委託先を含むサプライチェーンのリスク管理は企業の持続的な発展に不可欠な要素です。もしリスク管理が不十分な場合、情報漏えい、品質不正といった深刻な危機が発生し、企業の評判や事業継続に重大な影響を及ぼします。

また、サプライチェーンに関わるリスクは影響範囲が広く、継続的に取り組まなければ抑えることが難しい場合が多いため、継続的な対応が必要です。その際には、効率的な管理手法を導入し、管理の負担を軽減しながら持続可能な管理策を整備する必要があります。

さらに、リスクを最小化するための企業の社内体制としては、各部門の責任を明確にした3線管理態勢を構築し、全社的にリスクを管理していくことが、より実効性の高い手法であると考えられます。

雨宮 弦太（あめみや げんた）
PwC Japan有限責任監査法人　ガバナンス・リスク・コンプライアンス・アドバイザリー部　ディレクター
会計税務アドバイザリー業務、上場会社での内部監査室長を経て現職。上場準備企業におけるリスクマネジメントシステム構築支援、エネルギー関連企業へのグループ内部監査・内部統制高度化支援に従事、経済安全保障に関わる制度対応支援、情報管理セキュリティを含めた体制構築の業務等に幅広く従事している。
メールアドレス：genta.amemiya@pwc.com