

# サードパーティリスク管理の 高度化に向けて



言うまでもなく、企業活動においては自社グループの組織のみならず、外部の事業者、すなわちサードパーティとの協業が不可欠ですが、近年のグローバル化や事業活動の複雑化、そして経営効率の追求に伴い、企業のサードパーティへの依存度はますます高まっています。一方で、サードパーティによるトラブルや不祥事が自社のビジネスにこれまで以上に多大な影響を及ぼすことも懸念されており、実際にサードパーティに起因する重大なコンプライアンス事案が多発しています。このような背景からも、自社を取り巻くサードパーティをより精緻に、より効率的に管理することがますます重要となってきていると言えます。

本レポートでは、サードパーティリスク管理の考え方と、その高度化に向けたアプローチについて解説します。

## 1. サードパーティおよびサードパーティリスクとは

一般に、サードパーティとは、商品やサービスを提供するために業務上の契約関係を有する組織、また、当該商品・サービスの提供に必要な事業者を指します。具体的には、サプライヤー、製造委託先、物流業者、販売代理店や製造設備ベンダー等、バリューチェーンの維持において自社と関係する事業者のほか、ITベンダー、弁護士等、自社の管理機能の一部を委託する事業者も含まれます（なお、本レポートでは自社の顧客は含めないものとして進めます）。

サードパーティリスクとは、これらサードパーティが自社の事業や収益等に影響を与え得る潜在的な脅威を指します（図表1参照）。

従来のサードパーティ管理は、与信の観点によるリスク管理が中心でしたが、近年は製造委託先による品質不正事案や、ITベンダーからの情報漏洩事案等により、製品・サービスの品質リスクや情報セキュリティリスク管理の重要性も高まっています。

【図表1 サードパーティリスク例】

分類	サードパーティリスク例
信用リスク	サプライヤー等の倒産による供給不能 等
贈収賄リスク	販売代理店による公務員への贈賄、通関業者による税関職員へのファシリテーションペイメント、サプライヤーによる取引先等からのキックバックの受け取り 等
知的財産リスク	製造委託先による知的財産の侵害行為、販売代理店による商号の侵害 等
情報セキュリティリスク	外部からのサイバー攻撃による製造委託先のシステム障害に起因した生産ライン停止、製造委託先従業員による製造に係る営業秘密の情報漏洩 等
自然災害リスク	自然災害・パンデミックの発生による、サプライヤー・製造委託先での製造中断・停止、物流会社の被災による物流の寸断による販売網への影響 等
人事・労務リスク	サプライヤー・製造委託先における人権侵害、児童労働、強制労働 等
製品・サービス品質リスク	サプライヤー・製造委託先における商品製造上の品質不備・不正、サプライヤーによるサイレントチェンジ（無断での仕様変更）、販売後の安全性上の欠陥によるリコール、製造物責任問題 等
その他法令違反リスク	サプライヤー・製造委託先による環境・化学物質等に関する規制違反（違法伐採、化学物質規制違反等）、物流業者による輸出入規制に係る規制違反 等

## 2. ESG・SDGsを意識したサードパーティ管理の 必要性の高まり

昨今のESGへの意識の高まりを受け、ESGの要素も踏まえた責任あるサプライチェーンの構築や、サプライヤーをはじめとするサードパーティの管理が求められるようになってきています。また国際的なNGOやNPO等、ESGに係る問題に取り組む団体の存在感が増大しています。このような団体は、自社のサプライチェーン上における人権侵害や環境問題等に関し、根本的な解決や再発防止策を強く要請するケースが多く、時として大規模なデモや不買運動にまで発展することもあります。

特に近年重要視されている贈収賄リスクと人権コンプライアンスについて、以下に解説します。

### (1) 贈収賄リスク

米国当局をはじめ、贈収賄規制違反に対する執行件数や制裁金額が増加する中、特に、サードパーティを介した贈賄の摘発事例が頻発しています。実際、OECDによる統計によれば、外国公務員に対する贈収賄事案の75%が、エージェントや販売代理店等のサードパーティを経由した支払いとされています。こうした状況を受け、アメリカのFCPAガイドライン（A Resource Guide to the U.S. Foreign Corrupt Practices Act）やイギリスのBribery Actでは、サードパーティに対するリスクベースでのデューデリジェンスの必要性を規定するなど、サードパーティによる贈収賄リスク対応に係る規制を強化しています。

## (2) 人権コンプライアンス

国連による「ビジネスと人権に関する指導原則」をはじめとした国際的な枠組みのほか、主に欧米諸国においてサプライチェーンにおける人権規制の整備が進展するなど、自社グループのサプライチェーンにおける人権への配慮がますます求められるようになっていきます。これは、企業自身が直接人権侵害を引き起こした場合だけでなく、サプライヤーが引き起こした場合においても、責任を追及される可能性があることを示しています。

たとえば、英国の現代奴隷法では、英国で事業を展開し、世界での売上が一定額以上の英国内外の企業を対象として、事業とサプライチェーンにおける人権デューデリジェンスのプロセスを「奴隷と人権取引声明」に記載するよう要請しています。

また、米国カリフォルニア州のサプライチェーンにおける透明性を確保する法律では、全世界における売上が1億ドル以上で、カリフォルニア州で事業を行う小売業者および製造業者に対し、サプライチェーンにおける強制労働や人身取引に対する関与の有無について確認・監査を行うほか、サプライヤーに対して強制労働や人身取引に関する規制の遵守を義務付けた上で、その結果を自社のウェブサイトで開示するよう求めています。

そのほか、2020年4月には、欧州委員会がEU加盟国の企業に対し、人権デューデリジェンスを義務付ける方向で立法を進めていることを公表しており、自社のサプライチェーンに関係するサードパーティについて、ESGの観点から管理することはますます重要になるものとみられます。

## 3. サードパーティリスク管理における課題

サードパーティリスク管理には実務上の難しさもあります。以下、項目別に解説します。

### (1) サードパーティの管理主体のあいまいさ

グローバル化が進むなか、自社を取り巻くサードパーティは数千社～数万社に及ぶ場合があり、すべてのサードパーティをくまなく管理することは、社内リソースの観点からまず難しいと言えます。そのため、多くの企業においては、直接材や間接材、また、製造委託先や生産設備ベンダー等、それぞれのサードパーティが、委託元のさまざまな部門により個別に管理されているのが実情であり、自社のサードパーティ管理の全容を可視化できているケースは少ないのが現状です。各部門がそれぞれ個別にサードパーティを管理する状況下では、サードパーティリスクについての部門がどのような責任を負うのかが不明瞭となる恐れがあります。

### (2) 手作業を中心とした管理

委託元部門とサードパーティとのやり取りは、Eメールによることがほとんどですが、その中でさまざまなリスク管理を行うことは委託元部門における負担を大きくする可能性があります。たとえば、取引前や取引後の継続的モニタリングの際に、Eメールを介して質問票の授受を行い、手作業で集計しているケースが多く見られます。こうした管理を行っている場合、自社が委託するサードパーティの件数が増加すればするほど、確認作業がますます煩雑になってしまいます。また、サードパーティに係る情報集計の手間が増える

と、サードパーティに内在するリスクの全容の可視化と継続的な追跡による是正措置の策定や、購買の最適化を行うための十分な時間とリソースの確保が難しくなります。

### (3) 施策実行の難しさ

自社とサードパーティのビジネス上の関係性、特に調達量や製造量、市場占有率等によっては、サードパーティに対する管理施策の強化を要請しづらい場合も想定されます。また、施策の内容や実施方法によっては、サードパーティに一方的な義務を負わせる可能性があり、自社とサードパーティとの企業規模の差や力関係によっては、独占禁止法や下請法上の問題が生じる恐れもあります。

## 4. サードパーティリスク管理の高度化に向けたポイント

ここまで述べてきたように、サードパーティのサービスや製品が自社にもたらし得るさまざまなリスクを適切に評価し、管理するためには、新たな管理体制や仕組みを構築することが必要です。そのためにはフレームワークの活用が有効です。フレームワークを企業の組織と実務に落とし込むにあたって、特に考慮すべき4つのポイントを説明します。

### ポイント (1) サードパーティの分類

まず自社にとって重要なサードパーティを見極め、自社の管理リソースを集中させることが重要です。管理の対象とすべきサードパーティを把握するため、基準を設けてサードパーティを分類することが必要となります。

<基準例>

- ・当該サードパーティが自社のクライアントと接触するか
- ・当該サードパーティは、自社の知的財産やクライアントのデータにアクセスする機会があるか
- ・当該サードパーティのサービスは、規制当局による監視の対象となる領域か
- ・当該サードパーティのサービスは、他のサードパーティによって代替され得るものか 等

### ポイント (2) サードパーティリスクの特定

次に、法規制の動向や、自社の業界を取り巻く環境等を踏まえたサードパーティリスクの洗い出しを行います（具体的なリスク例については図表1を参照ください）。一方、自社のリソース等の制約から、すべてのサードパーティリスクに対し一度に対応することは困難なため、実務上は、過去に自社や他社において発生したサードパーティリスク発現事案等を踏まえ、特に直近で対処すべき重要リスクを数項目抽出するケースが多く見られます。

### ポイント (3) 各部門の役割・責任の明確化

一般的にサードパーティの管理主体については、主に以下の3つの類型に分けられ、現状、多くの日系企業においては、個別管理型または部分的管理型に該当するケースが大半を占めています。なお、一部の外資系企業においては、集約型を採用するケースも見られます。

【図表2 管理主体の集約化の類型】

	個別管理型	部分的集約型	集約型
イメージ			
特徴	<ul style="list-style-type: none"> <li>各部門が個別対応でサードパーティのリスク管理を実施している。</li> </ul>	<ul style="list-style-type: none"> <li>管理部門（コンプラ、品質部門等）が購買時のガイドラインやマニュアルを提示するが、実際の管理は各部門任せ（または、管理部門と各部門同士で個別に連携）</li> </ul>	<ul style="list-style-type: none"> <li>集約部門が一括して、データを集約するとともに、リスクが高いサードパーティを中心に、一括してリスク評価・モニタリングを行う。</li> </ul>
留意点	<ul style="list-style-type: none"> <li>管理方法につき、部門間での重複等がある恐れがある。</li> <li>委託によるスケールメリットやコスト削減効果は享受しにくい。</li> </ul>	<ul style="list-style-type: none"> <li>各部門が適宜管理部門と連携するため、漏れがある恐れがある。</li> </ul>	<ul style="list-style-type: none"> <li>一元管理されているため管理上の重複はない。</li> <li>集約には、集約部門のリソースや社内における発言力が必要となる。</li> </ul>

集約型における集約部門の役割のあり方については、さまざまなケースが存在します。たとえば、自社のサードパーティのデータを集約し可視化するため、各部門がサードパーティと取引する際には必ず当該部門を通す業務プロセスとするケースもあれば、当該部門は、重要なサードパーティについてのみデータを集約し、リスクアセスメントやモニタリングプロセスにおいて、委託元部門に対する助言等を行っているケースもあります。一元的な管理を実施する集約型の体制を整備し、委託元部門や集約部門等の役割・責任を明確化することが理想的ですが、これは、各部門が個別に行っていたサードパーティの管理業務を、その重要性に応じて集約部門に統合することで、各部門の管理上の負荷を低減するだけでなく、リスクベースアプローチによる管理を実現することが期待できるためです。

ただし、集約型の場合、一元管理主体となる部門（調達部門等）のリソースやスキルが充足していることや、社内における十分な訴求力が必要となることから、実務上は、現状のリソース等を踏まえ、自社に適した管理体制を検討することが重要です。

また、部分集約型や集約型の場合は、個別管理型に比べて集約部門や管理部門の負荷が増加することが想定されます。そのため、分類上重要度が低いと考えられるサードパーティについては、従来どおり各部門が契約～モニタリングを行う一方、重要度が高いサードパーティについては、特定の部門が、コンプライアンス部門や情報セキュリティ部門等の各管理部門と連携しながら、自部門に係るリスク分析やモニタリングを行うことを推奨します。

#### ポイント（4）サードパーティ管理方法の効率化

従来のような手作業による管理では、サードパーティの増加や複雑化するリスクへの対応において限界があることは明白です。そのため、契約～契約終了までの一連の流れに合わせ、管理手法の効率化を図るためのさまざまな取組みを行うことが考えられます。

- ・ITツールを用いたデータの可視化、一元化

サードパーティリスク管理に係るITツールを導入することで、サードパーティとの契約前や契約後の定期的モニタリングにおけるリスクアセスメント結果の可視化やサードパーティに係るデータの一元化を行うことができます。KPMGが世界のグローバル企業約1100社を対象として行った[サードパーティリスク管理に関する調査](#)によれば、サードパーティリスク管理に関して行っている投資として、多くの企業がITツール導入を挙げており、関心の高さがうかがえます。

- ・イニシアティブへの参加

グローバルなイニシアティブや業界団体に加盟するケースも増加しています。こうしたイニシアティブに加盟している企業は、加盟企業同士でサプライヤーのアセスメント結果を共有することができるため、サプライヤー評価の効率化を図ることが期待できます。

## 5. まとめ

今後、自社のさらなる進展やグローバル化の深化に伴い、サードパーティに係るリスクはより複雑化・多様化していくことが想定されます。また、日本企業によるサードパーティリスク管理の高度化の動きも、ますます進んでいくものと考えられます。このようななか、サードパーティの役割を正確に理解した上で、サードパーティリスク管理の体制を構築していくことがより重要となると考えられます。

最後に本レポートが貴社の取組みの一助となれば幸いです。

## 執筆者

サプライチェーンリスク管理チーム



パートナー  
足立 桂輔



ディレクター  
土谷 豪



マネジャー  
佐藤 悠花子

## KPMGコンサルティング株式会社

03-3548-5111

kc@jp.kpmg.com

[home.kpmg/jp/kc](https://home.kpmg/jp/kc)

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供できるよう努めておりますが、情報を受け取られた時点及びそれ以降における正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査した上で提案する適切なアドバイスをもとにご判断ください。

© 2020 KPMG Consulting Co., Ltd., a company established under the Japan Companies Act and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.