

コンプライアンス InSight 2023年 春号

サードパーティ・リスク管理を “投資”と捉える企業のねらいとは？

～ 経営の安全性を高める手段としての「デューデリジェンス」の意義と価値～

この20年間、汚職や腐敗、不正を世界経済から排除すべく、各国の当局は連携して様々な規制を設けるなど、活発な活動を続けてきた。これは社会的要請に基づくものではあったが、実際にサードパーティへのデューデリジェンスの徹底や報告対象項目の拡大、非財務データの開示といった取り組みを行う企業にとっては、ある種の“負担”とみなされる風潮は少なからずあったと言える。

しかし、ここにきて潮目は大きく変わりつつある。規制遵守は単なるコストではなく、「大きな競争力を得ることに繋がる」との考えが広まっているようだ。

本稿では、なぜそのような意識変革が起これ、実際に規制遵守への取り組みがどのような恩恵を企業にもたらすようになったかについて、リフィニティブ作成のレポート「効果的なサードパーティ・リスク戦略—不確実性の時代における生き残りの鍵」を元に、整理していく。

事業に影響をおよぼすおそれのあるリスクとは？

まず、リスクについて、改めて整理しておこう。サードパーティによって事業に影響がおよぶおそれのあるリスクは、大きく6つに分類できる。

不正行為や反競争的行為、贈収賄・汚職、詐欺といった人に関わるインシデントである「健全性リスク」や、定められた納期までに納品ができるか、供給停止等の可能性とそれによる収益減やブランド毀損が起こるかどうかといった「業務及び品質に関するリスク」、取引相手の財務的健全性や安定性のほか、財務上の不正行為に関する「財務リスク」。これらは、古くから認知されているものだ。

一方、「アイデンティティ・リスク」は、あらゆる段階でオープンな情報共有と説明責任を推進することによって、個人や組織の資金源に関する透明性と明確性を確保し、はじめて回避できるリスクだ。例えば、組織の実質的支配者(UBO)や従業員を含むステークホルダーと外国PEPsや反社会的勢力との繋がりの有無といった、より深い部分も含めた調査を行うことで把握できるリスクとも言えるだろう。

これらに加え、近年注目されているのが、「ESGリスク」と「サイバー及びデータリスク」だ。

ESGリスクの波及力

「ESGリスク」は、指し示す範囲が広いのが特徴だ。経営に直結する内容としては、取締役会や経営陣がESG(環境・社会・ガバナンス)を重視した活動を行っていない場合、投資家らがそれを公然と非難する、あるいは、投資の引き揚げ(ダイベストメント)のような踏み込んだ対応を行うことが挙げられる。企業にとっては到底無視できない問題であることは言うまでもないだろう。

一方、ESGリスクを抱えるサードパーティがサプライチェーンに組み込まれていたとして、その事実が明るみになった場合、たとえ当事者ではなかったとしても批判の矢面に立たされ、長期にわたる風評被害を被るといったことも企業にとってのESGリスクだと言える。

例えば、サプライヤーが気候変動や不平等、人身売買ほかバイオ・ダイバーシティを侵害するような問題に加担している、あるいは放置していることが報道等によって知れ渡ったとすると、その批判の矛先は、サプライチェーン全体を管理する大企業に向けられることが往々にしてある。サプライヤーの先で起きている問題であるため、把握しづらい、という点は非常に悩ましいところだ。

サプライチェーンについては、ドイツの「サプライチェーン・デューデリジェンス法」を例に挙げると、原料採取から最終製品の納入まで、生産プロセスの全体が含まれる、と定義されている。だが、ウクライナがロシアに侵攻されて以降、その定義を拡大し、「上流」だけでなく、販売後どのような団体・個人が製品やサービスを使うかといった「下流」にも十分な配慮が必要だ」とする気運が高まっている。

こうして見るだけでも、今日においてサプライチェーン・マネジメントがいかにESGリスク対策として重要であるか分かるだろう。

加えて、ESGリスクに向き合う上で注目したいのが、日本国内ではE(環境)に対する関心が高いが、海外ではS(社会)やG(ガバナンス)への危機感が強く、取り組みも進んでいるという点だ。

国連「ビジネスと人権に関する指導原則」や「労働における基本的原則及び権利に関するILO宣言」といったソフトローをもとに、英国「現代奴隷法」やドイツ「サプライチェーン・デューデリジェンス法」、米国「ウイグル強制労働防止法」といったハードローが立て続けに整備されたことはよく知られている。さらに、日本政府も2022年9月に「責任あるサプライチェーン等における人権尊重のためのガイドライン」を発表した。こうした動きを見ても、「ビジネスと人権」への感度を高めることが最重要であると理解できるだろう。

無視できない世論の圧力

「ESGリスク」については、1990年代の世界的な貿易取引の増大と労働市場の拡大と表裏になっているとも言える。有名ブランドの製品を製造する現場で劣悪な労働慣行が横行していることが問題化して以来、サプライチェーンの問題はNGO団体や人権擁護家を中心に世の中から厳しい視線が向けられるようになった。

特に、世界の購買力を支えるミレニアル世代やZ世代の価値観は、さまざまな調査結果にも示されている通り、ESG原則と密接に結びついている。彼らが問題視するような事柄を放置し、是正しない企業が支持を得られず、競争力を低下させていった例は少なくない。

ミレニアル世代やZ世代は、情報取得のチャネルが他の世代に比べて多い、というのも特徴として挙げられる。例えば、「Millennials and Social Media Statistics: Platforms and Marketing, Writersblocklive.com」が2021年5月に発表した調査結果によると、米国のミレニアル世代の4分の3以上(79%)が毎日1回はソーシャルメディアに触れており、複数のプラットフォームを行き来し、商品やサービスに関する友人の投稿に大きく影響されやすい傾向があるとのことだ。

ソーシャルメディアの影響力は極めて大きく、企業が起こした過去の違反行為や判断ミス、意図せぬ関与といった不都合な内容が投稿されれば、またたく間に拡散する。その過程では、個人の意見や見解が加わっていくことも多く、「友人の意見に同調する、あるいは、反論する」といったより複雑な形で情報が再生産・加工・消費されていくこともある。こうなれば、企業側はほとんど情報を制御できなくなり、リスクがより大きく複雑化してしまう。

このようなことが起こらないよう、自社内のコンプライアンス・ガバナンス体制の強化は当然行われているだろうが、それだけでは取り組みとして不十分と言わざるを得ない。

企業としては、レピュテーションリスクを回避する取り組みとして、サードパーティに対しても、そのようなリスクの発生源となる可能性について、徹底した評価が欠かせない。そうした意図で、取引先についての詳細な実態把握の手段としてスクリーニングやデューデリジェンスの実践が進むようになったことは、自然な流れだと言えるだろう。

サイバー攻撃対策としてのサードパーティの実態把握が重要な理由

ここまで挙げた5つのリスクは、認知も広がっており、次善の措置を講じる企業も増えている。だが、「サイバー攻撃のリスクを低減させるための手段」については、対策に関する知見がまだ十分ではない、と感じているのが多数派ではないだろうか。

一方、コロナ禍によってリモートワークやEコマースが一気に普及するなど、デジタル化は一気に加速した。それに伴い、サイバー攻撃のリスクは増大し、悪質化・高度化も進み、事業に及ぼす経済的な損失や損害も大きくなっている。例えば、インフラ施設を攻撃して日常生活を破綻させたり、病院内の重要な情報を“人質”に身代金を要求したり、といった事件は深刻な社会問題だ。

ランサムウェア攻撃にしても、不正アクセスにしても、攻撃者に対する守りを固めていても新たな脅威が次々出てくるので、「打つ手がない」というのが現状だろう。

だが、手をこまねてはいられない。対策の基本としてできることは全て実践する必要があり、中でもサードパーティのサイバー・セキュリティ感度をしっかりと確認する取り組みは欠かせない。

日本法人の中でもここ数年、サイバー攻撃への懸念が話題になる機会は増えているようだ。日本企業に対しリスク&コンプライアンス領域のガバナンス強化を支援する製品やソリューションを提供しているリフィニティブのカスタマー&サードパーティリスクソリューションセールス・スペシャリスト乳原晶子は、「ある企業では、サイバー攻撃に対抗するため、サードパーティとの取引を始める際には必ず取引先企業に独自のアンケートを実施し、リスクの高低を自社基準に照らして判断するようになった」と話す。

確かに、サードパーティにおける現在のセキュリティ対策の内容を把握したり、社内の情報管理や社員教育のあり方をヒアリングしたり、従業員に付与しているID/パスワードの取り扱いやアクセス権限付与時のルールを確認したり、リモートワーク環境のセキュリティレベルを見ておけば、取引先のサイバー攻撃への対応度を推し測ることはできるだろう。

また、「もし同じことを自社内で行った場合、問題になるかどうか」というように、自社ルールと照らし合わせてみれば、自ずと「取引を行っても問題ないか、是正を依頼するべきか、取引は見送るか」ふるいに掛けることができる。

並行して、過去に情報漏洩やIT障害等の問題を引き起こしていないか、報道や当局への報告等の事実確認も進めれば、かなりの精度でリスク判定ができそうだ。

この時、サードパーティから寄せられた回答の内容が正確かつ詳細であればあるほど良いが、一方で、アンケートの回答者が必ずしもITリテラシーが高いとも限らないし、自社のセキュリティ事情に詳しいわけでもない、ということも想定される。質問の内容や意図を正確に理解しないまま不正確な回答をされてしまえば、こちら側の判断にも影響が出てしまうだろう。

「そのようなことがないよう、こうした取り組みをする際には、事前のレクチャーやいつでも簡単に質問ができるような環境を整備しておくことが望ましい」と、前出の乳原。加えて、「回答を自社のリスク判定基準に照らして『スコアが芳しくない』と評価された企業に関し、『World-Check One』のようなデータベースでシームレスに追加調査を実施できれば、よりスマートに取引可否を判断できるだろう。またこのような仕組みがあれば、追加調査の結果、取引を見送らざるを得ないとの結論が出たとしても、そのことを新規取引や取引継続の申請を上げた部署に説明がしやすく、一連の取り組みそのものがガバナンス意識の向上にも繋がると期待できる」と続けた。

さらに乳原は、「上述のような調査を行なっているうちに、例えば、『相手方企業が自社に対するサイバー攻撃の“踏み台”になるおそれがないか脆弱性に関するチェックをしていたところ、別の懸念される事柄も見つかった』といったケースに遭遇することも考える。そうなれば、より詳細なデューデリジェンス・リサーチを行う必要も生じるだろう。このような場面で、アナリスト・チームを活用して調査対象の評判に関するバックグラウンドや情報をより詳細に追加収集してレポートする『Refinitiv Due Diligence Report (リフィニティブ・デューデリジェンス・レポート)』のようなサービスを活用することで、企業にとって避けるべきリスクを未然かつ大きく低減させることも期待できる」と、提案する。

リスクを効果的に特定し、管理するための要点

サードパーティにおけるサイバー攻撃への対応の度合いやESGリスクへの対応ぶり、伝統的な財務や健全性に関する状態把握など、今日、コンプライアンスを徹底するには、広く複合的な知識と最新の問題への高い理解が求められる。もはや、法務部門のような一部の部門だけでリスク対応をするのはほとんど現実的ではなく、部門横断的な連携と複合的なリスク感度で多角的なステップからなる包括的な対応策が不可欠だ。

では、どのようなあり方が考えられるか？ レポートでは、次のような内容が紹介されていた。

1: 情報収集

未知の情報やリスクを特定することは、スクリーニングやデューデリジェンスのプロセスと同じくらい重要である。ロシアに対する制裁で明らかになったように、サプライヤーや顧客企業の所有構造を知ることが、変化し続ける義務を管理する上で欠かせない。

2: 潜在的リスクのスクリーニング

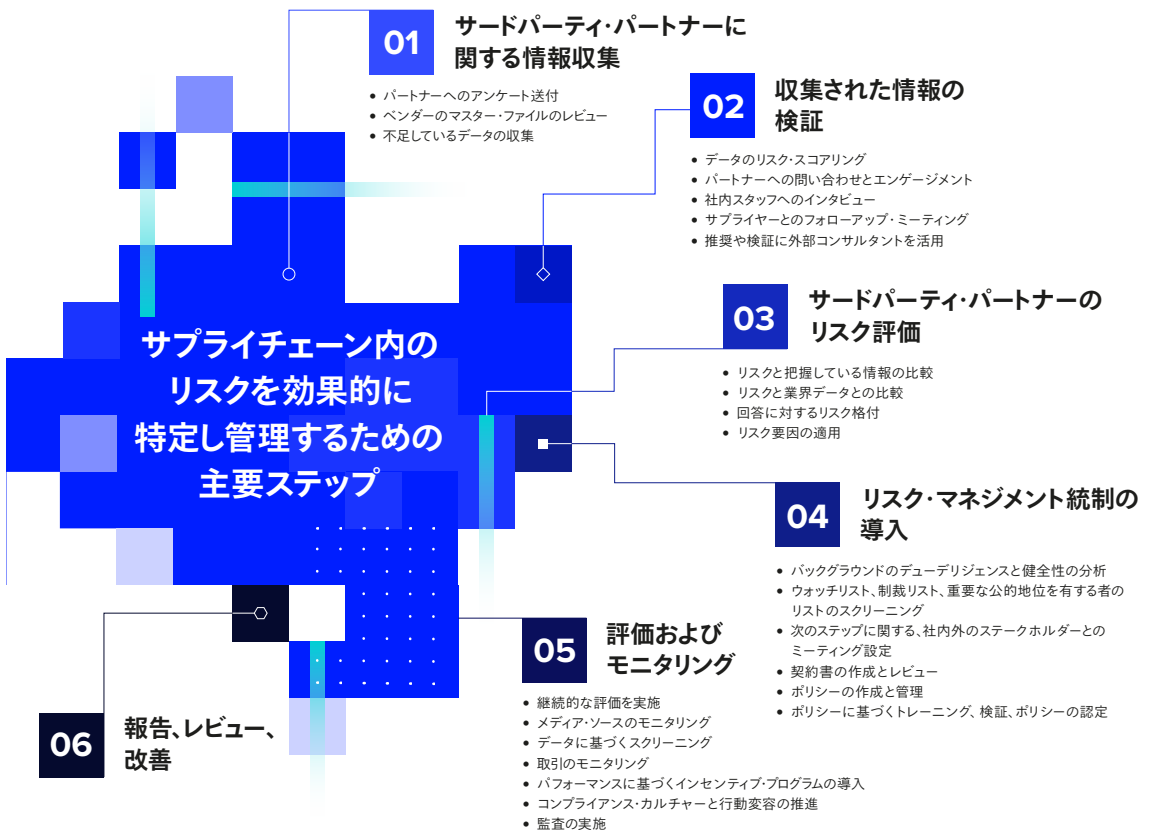
スクリーニングは効果的なデューデリジェンスをサポートし、取引関係を低・中・高リスクに分類できるため、リスク軽減のために必須の取り組みである。

3: 適切なデューデリジェンスの実施

スクリーニングによってリスクが高いことが検知、または、その疑いがあると分かったら、さらなる調査が必要となる。その際、いくつかの方法が考えられるが、例えばWeb検索で知り得る範囲の情報には正確性の問題があり、専門家による実地調査を行うとなればコストや調査期間の長期化等の別の問題が生じかねない。

そうした意味では、適正なコストを支払って、正確性や更新性、信頼性、網羅性が担保されたデータベースを照会して詳細な調査を行う、という取り組み方はリーズナブルな選択肢になりうる。

特に、海外企業や重要人物等に関わる情報を精査する際には、データベースの精度や更新性や網羅性のほか、深度にも着目する必要がある。この点について、例えば、調査および政策提言を行う国際的な団体「The Sentry」*1が提供するデータは、オープンソースデータや実地調査の結果だけでなく、現地や国際的な市民社会団体、ジャーナリスト、各国政府と連携して得られたものであり、武力紛争と残虐行為に対する資金提供や支援、その収益化の実態を追跡・分析するなど、入手しづらい情報が蓄積されている点で高く評価されている。このようなデータを活用することは、間違いなく企業にとって思わぬリスクを回避するひとつの手段だ。



出所:リフィニティブ・グローバル・レポート「効果的なサードパーティ・リスク戦略」(日本語翻訳版)

*1 <https://www.refinitiv.com/ja/risk-and-compliance/financial-crime-risk-management/risk-advocacy#t-the-sentry>

リスク対策は競争力にもなり得る

最後に、サードパーティ・リスクを管理することが事業継続性を保つことに繋がっているという事実について、興味深いデータを示したい。

レポートによると、「株主だけでなくすべてのステークホルダーに利益をもたらす長期的価値を築くことを重視する『ステークホルダー資本主義(包括的資本主義)』への支持は高まりつつある。新型コロナウイルスの感染拡大を契機に、ESG原則と密接に結びつくステークホルダー資本主義は、企業のレジリエンスと長期的な成功にとって不可欠であるとみなされるようになり、その流れを加速させている」というのだ。

実際に、リフィニティブが作成した「GETTING PERSONAL: HOW WEALTH FIRMS CAN ATTRACT AND RETAIN THE MODERN INVESTOR」*2で紹介している調査結果によると、グローバルに調査した投資家の半数以上(51%)がサステナブル投資になじみがあると回答し、そのうち29%がすでにポートフォリオに組み入れている、とのことだ。

さらに「今、ESG投資を以前よりも積極的に検討したい理由は何か?」という問いへの回答として、「ESG投資への理解が深まった(50%)」「危機時におけるESG投資のパフォーマンス(42%)」「投資プロセスの仕組みに関する情報が現在は増えた(41%)」といった反響も紹介している。また、レポートでは、「多くの投資家が、自分の投資資金が企業の意思決定にどのように影響しているかを知らされ、またその実情に関心を寄せるようになっていく」との分析がなされている。投資家にとって、投資によるリターン獲得はもちろん、社会的責任を果たせるか否かは投資行動をする上での重要な判断要素になっている、と分かるだろう。

他方、ESG原則を不可欠な基準としてサステナブル投資を強く支持した国連「責任投資原則(PRI)」に賛同する投資会社は、2006年当初は63社、運用資産残高(AUM)合計6.5兆ドルだったが、2019年6月には2,450社 AUM 合計80兆ドル超にまで成長している。

また、「ESG関連のパフォーマンスを高めることは、それをしない企業よりもリスクが低く、長期的な成長において優位性があり、不確実な状況をうまく乗り切ることができると評価されている」との事実もある。

これらを見ると、リスクへの対応は、企業にとって「投資家からの支持を得、投資を呼び込むことになる」と言え、商品やサービスを向上させることと同じくらい競争力として評価される、との期待もできる。

これまでの日本市場では、企業同士が強固な相互関係を構築していたため、双方が取引先について、「十分に理解している。サードパーティ・リスクに類する問題は起きづらい」との認識があったと推察される。だが、変化に富み、海外企業のM&Aやグローバルなサプライチェーン展開、海外市場での売上割合の増加が進む今日のビジネス環境において、その考え方はもはや通じそうにない。

規制遵守をはじめ、あらゆるリスクに対策するための“コスト”を“成長のための投資”と考え直し、取り組みを加速させられるかどうか? これは、不確実性の時代における生き残りの道を切り拓けるかどうかと同義だと考えられるだろう。

*2 <https://www.refinitiv.com/en/resources/special-report/getting-personal-in-wealth-management>

ウェブサイト [refinitiv.com/ja](https://www.refinitiv.com/ja) |  @RefinitivJP  @RefinitivJP

LSEG(ロンドン証券取引所グループ)傘下のRefinitiv(リフィニティブ)は、金融市場のデータとインフラストラクチャの提供で世界をリードしています。リフィニティブは、190カ国にわたって4万以上の企業や40万を超えるお客様にサービスを提供しながら、世界中の金融市場に関わる人々を支援しています。また、重要な投資や取引、リスク判断をお客様に自信をもって行っていくための情報やインサイト、テクノロジーを取り揃えています。独自のオープン・プラットフォームと業界をけん引するデータおよび専門的な知識を組み合わせることで皆様に取引機会と選択肢を提供し、お客様とビジネス・パートナーの皆様のパフォーマンス、革新、成長を促進してまいります。 <https://www.refinitiv.com/ja>

© Refinitiv 2023. All rights reserved.

本文および本文の内容(以下、「本内容」)は、あくまでも一般的な情報提供を目的としたもので、筆者の本主題に係る過去の経験に基づくものであります。記載された内容はRefinitivの見解を反映するものではありません。なお、無断での複製、転送等を行わないようにお願いします。

本内容は、如何なる法域又は領域においても、投資助言(及びその他の如何なる助言)を提供するものではなく、また金融商品の売買の申し込み又はその勧誘とみなされるべきではありません。記載された意見や予測等は作成時点のものであり、Refinitivは、本内容に含まれる情報の正確性、最新性、適切性及び完全性、また本内容の利用結果について如何なる保証も行わず、本内容に起因して生じた損失や損害について一切責任を負いません。Refinitivは予告なくいつでも本内容を変更、削除する権利を留保します。

発行元: リフィニティブ・ジャパン株式会社

Webサイト: [refinitiv.com/ja/governance-risk-compliance-solution](https://www.refinitiv.com/ja/governance-risk-compliance-solution)

お問い合わせ先

URL: [refinitiv.com/ja/ask](https://www.refinitiv.com/ja/ask)

電話: 03-6743-6515

An LSEG Business

REFINITIV® 