# サードパーティリスク管理関連サービス

## Third-Parties Risk Management (TPRM)related services

株式会社 KPMG FAS

KPMGは、サードパーティによって生じるさまざまなリスクに対応するためのサードパーティリスク管理態勢（TPRM）について「現状の評価」「あるべき姿への移行」「管理の実行」の各フェーズで、各種リスク管理態勢の高度化支援の経験やグローバルネットワークの知見等を活かしてご支援します。

近年、事業の多角化やデジタル化の進展等でビジネスは複雑化し、従来の外部委託の形態にとどまらないクラウドサービス事業者、フィンテック企業、スタートアップ企業等のサードパーティとの連携も増えています。サードパーティとの連携は、多くの企業にコスト削減や顧客サービスの向上などの利益をもたらす一方で、自社のレピュテーションやオペレーションの継続に影響を及ぼすようなインシデントを増加させています。また、コロナ禍や地政学的な問題によるリスク環境の変化や、気候変動等の環境問題、個人情報・プライバシー、労働環境・人権、腐敗・汚職、輸出管理・経済制裁など法規制の強化や社会的要請の高まりから、管理すべきサードパーティのリスク領域は、ますます拡大傾向にあります。

サードパーティのリスク管理は、全てのサードパーティを把握し、リスクベースで対応することが望まれますが、現状では、外部委託先管理や取引先管理といった部分的な管理に留まっているケースが多く見られます。また、多くの企業では、情報管理/プライバシー、贈収賄防止、人権、輸出管理、BCM、経済制裁、マネロン・テロ資金供与防止など、個別テーマでのリスク管理活動がバラバラに行われています。

こうした対応は取組の不整合や不効率を生じさせるため、拡大する管理対象やリスク領域への対応には、組織横断で一元的な管理態勢への変革が求められます。

### 増加するサードパーティに起因するトラブル

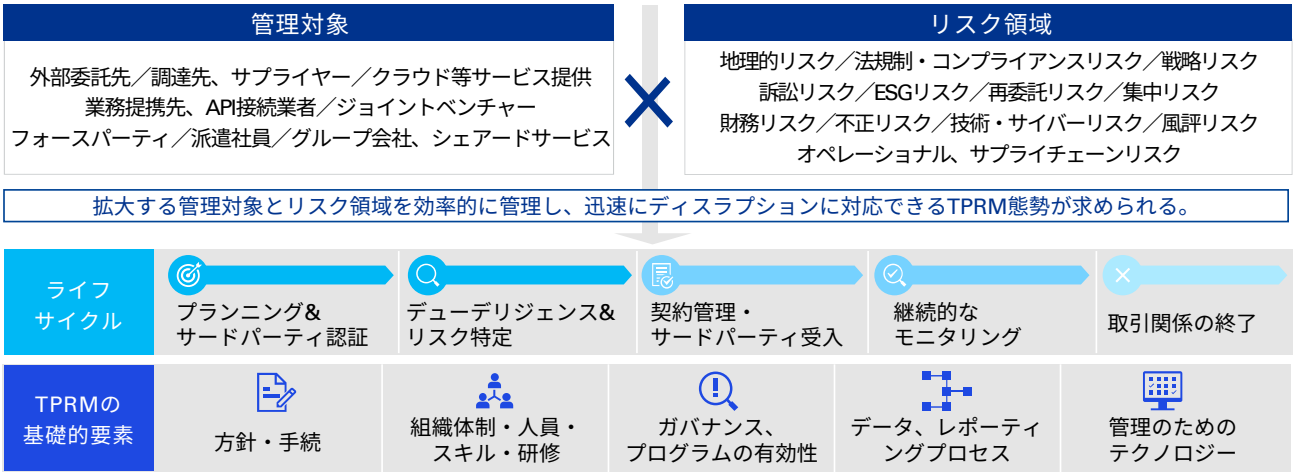
システム運用の委託先でのソフトウェア更新ミスによる大規模システム障害の発生、委託先従業員の不正による顧客資産や個人情報流出など、委託先のミス・不正によるトラブルは従前より発生していました。近年では、サードパーティとの業務連携におけるコントロールの隙をつかれて顧客資産が流出した事案や、取引先へのサイバー攻撃によって自社業務を停止した事案等、委託関係にないサードパーティに起因する事案も増えています。更に、サードパーティとの取引やサプライチェーンにおける、人権問題、経済制裁／輸出入規制等への抵触、贈賄行為等が、各国の規制当局による重大な制裁や処分に繋がるリスクが高まっています。

| | 業種／発生時期 | 事象の内容 |
|---|---|---|
| 1 | **自動車**<br>2022年3月 | 車の内装に使用する樹脂部品を手掛ける**大手自動車の取引先がサイバー攻撃**を受けた。当該大手自動車では、必要最低限の部品しか保有しない生産管理システムを整えており、当該システムは取引先にも接続されていたため、部品の供給停滞の恐れから、**工場の操業を2日間停止**した。大手自動車本体のみならず、グループ内でトラックや軽自動車を製造する自動車会社にも影響が出た。 |
| 2 | **インターネットサービス**<br>2021年3月 | SNSプラットフォームを提供するインターネットサービス企業が**システム管理を委託する中国の関連会社の技術者が、日本のユーザーの個人情報にアクセス可能な状態**になっていることが判明した。その後調査で、委託先技術者が、当社の個人情報に1年間で139回アクセスしていたことが判明した。本件では、個人情報保護委員会が当社に対して、**業務委託先の監督体制が不十分**だったとして行政指導が行われた。 |
| 3 | **証券**<br>2021年3月 | 証券会社のシステム開発・保守・運用の委託先の担当者が、バックアップファイルの個人アドレス等への不正な転送により、**証券会社の顧客のID、パスワード、暗証番号等を不正に取得**し、顧客になりすまして有価証券を売却する等、**顧客の資金を証券口座から不正に出金**した。被害総額は2億円にのぼる。業務上必要のないファイル転送の検知する適切な仕組みがなく、また個人のメールアドレスへの情報の転送防止する仕組みが機能しなかった。 |
| 4 | **資金移動業・銀行**<br>2020年9月 | 資金移動業者と複数の銀行との口座連携において、顧客以外の第三者が不正に預金口座から顧客の資金が出金された。資金移動業者側は、メールアドレス1つで口座の開設が可能で、**銀行口座情報があれば他人であっても紐づけられたことが原因**となっていた。 |
| 5 | **外貨両替・銀行**<br>2020年1月 | 外貨両替大手が**マルウェアによるサイバー攻撃**を受けて、対応にあたる期間、一時的にウェブサイトを閉鎖した。当社のシステムはその他の複数の銀行のOnline Travel Money Serviceに利用されていたが、サイトの閉鎖の間、同様にシステムが使用できず顧客向けのサービスが停止された。 |

## 求められるサードパーティリスク管理態勢の要素

拡大する管理対象やリスク領域を効率的に管理するためには、組織全体で一貫した方針・手続を採用し、組織体制や責任者の設定、KPI/KRIの設定や報告といった管理の基礎となるガバナンスプログラムを整備した上でサードパーティのオンボーディングから取引終了までのライフサイクルを継続的に管理できる枠組みが必要となります。特に、業務の効率化を図るためには、リスクベースアプローチの採用やテクノロジーの活用が欠かせません。

**＜求められるサードパーティリスク管理態勢＞**




## KPMGのサードパーティリスク高度化のご支援

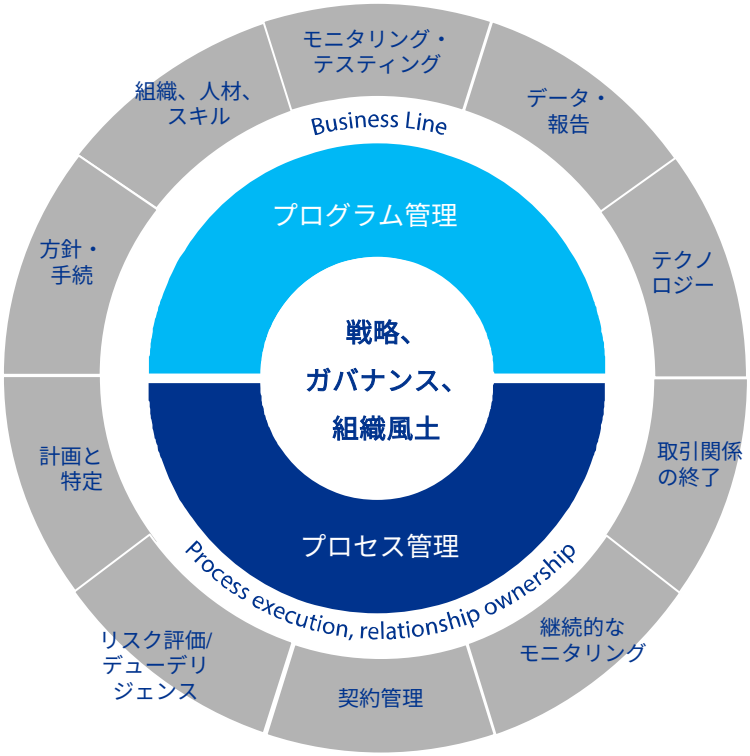
**TRPM成熟度評価**

KPMGは、欧米当局のガイドラインや先行的なプラクティスを基に、以下の2つの主要なセクションに焦点を当てて、効果的なTPRMプログラムのための主要な要素を整理しています。

- プログラム管理：サードパーティリスクに対応するための基礎的な要素
- プロセス管理：サードパーティリスクを低減するためのプロセス

KPMGは、サードパーティ管理に係る各所管部門とのワークショップを通して、企業のTPRMプログラムの成熟度評価を行い、高度化のための方向感・ロードマップの整理を支援します。

**＜TPRMの構成要素＞**



### サードパーティのマッピング支援

オペレーショナル・レジリエンスはTPRMプログラムが最も効力を発揮するリスク領域であり、事業継続の耐性を強化するためには、集中リスクへの対応が欠かせません。集中リスクへの対応の最初のステップは、既存のサードパーティとの関係を整理し、サードパーティ、場所、システム/情報、人材等の関連事項を棚卸し、相互依存関係を把握することです。KPMGは、サードパーティのマッピングを行い、業務、情報、スキル等の集中ポイントの把握を支援します。

### サードパーティの背景調査（Astrus）

サードパーティ起用前のリスク評価やデューデリジェンスのための情報収集を支援します。KPMGは、30,000を超える情報ソースを対象に、調査対象に関連する情報を収集します。情報ソースは一般的なコンテンツプロバイダーが提供するデータベース以外にも、KPMG独自で調査した情報ソース、一般的な検索エンジンでは届かない深層にあるウェブサイト等もカバーしています。

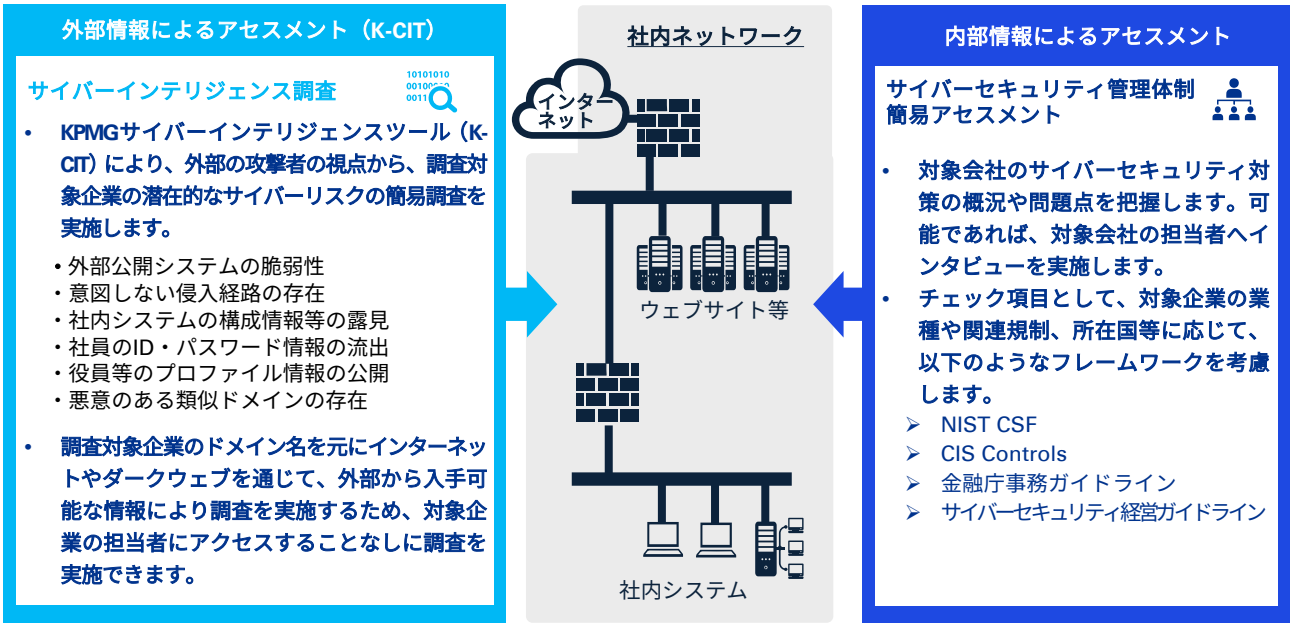
**＜Astrusの主な調査項目＞**

| | |
|---|---|
| 法人の背景情報 | 登記情報、企業識別情報、登録、上場等の状況、経営者や主要株主の情報 |
| 個人の背景情報 | 国籍、学歴、職歴等 |
| メディア情報 | 対象会社、個人に係る不利益なニュース記事等 |
| 訴訟記録 | 調査対象に係る過去10年間の訴訟記録（該当地域で検索可能なものに限る。調査対象が日本の場合、入手可能な情報は限定的） |
| 制裁記録 | 対象会社、個人に係る罰則や制裁、PEP（重要な公的地位を有する者）該当の有無 |

### サードパーティにおけるサイバーリスク簡易評価

サードパーティに対するサイバー攻撃は、企業の事業継続やセキュリティ上のリスクに影響を与えます。KPMGはサードパーティのサイバーセキュリティ管理体制や潜在的なサイバーリスクを簡易的に評価します。サードパーティのビジネス形態（ECサイトの保有有無等）や、対象企業の担当者へのアクセス可否等に応じて2種類のアプローチを用意してます。

- 外部から取得可能な情報に基づく「サイバーインテリジェンス調査」（K-CIT）
- 入手可能な内部情報（委託先チェックリストや契約書、業務報告書、等）による「サイバーセキュリティ管理体制簡易アセスメント」



KPMGは「評価」「移行」「実行」の各フェーズでさまざまなご支援を提供します。

## 評価

- **成熟度評価**
  TPRM機能の現状の簡易レビュー（発見事項と推奨を提供する）
- **規制レビュー**
  関連する規制要件に対するギャップ分析（発見事項と推奨を提供する）
- **ビジネス・ケースとロードマップ**
  機能強化の優先順位付けと、プログラムの展開に必要な活動規模の測定
- **内部監査**
  3つの防衛線（3 Lines of Defense）のコソース

## 移行

- **フレームワーク設計**
  TPRMプログラムとプロセスコンポーネントの確立または強化（プログラムの文書化、ライフサイクルテンプレート、およびテクノロジーのビジネス要件の策定）
- **テクノロジーの有効化**
  ワークフロー・テクノロジー、リスク・インテリジェンス・ソフトウェア、サードパーティ・ユーティリティの設定と導入
- **チューニングと最適化**
  TPRMプログラムおよびプロセスの構成要素の高度化（測定指標やレポート、データ分析、TPRMのリスク選好度など）

## 実行

- **シナリオテスト**
  サードパーティの事業継続および撤退計画
- **マネージド・サービス**
  契約前および契約後のサードパーティのスクリーニングやモニタリングのための、エンド・ツー・エンドプロセスの実行。先進的なテクノロジーとデータ・ソースの先行プラクティス・プロセスへの組込み
- **サードパーティの評価**
  契約前および契約後のリスク評価およびコントロール評価のポートフォリオの実行

**株式会社 KPMG FAS**

〒 100-0004
東京都千代田区大手町1丁目9番5号
TEL : 03-3548-5770
FAX : 03-3548-5740

FAS-Forensic@jp.kpmg.com
kpmg.com/jp/fas

本リーフレットで紹介するサービスは、公認会計士法、独立性規則及び利益相反等の観点から、提供できる企業や提供できる業務の範囲等に一定の制限がかかる場合があります。詳しくは株式会社 KPMG FASまでお問い合わせください。