サードパーティリスク・
パートナー企業財務リスクトレンドレポート

Librus株式会社
コンサルティングサービス事業部

エグゼクティブサマリー

2024年は、サードパーティリスクが企業経営に与える影響が過去最大となった年として記録される。特に、パートナー企業の財務悪化による連鎖倒産件数が74件と過去30年で最多を記録し、負債1,000万円未満の小規模倒産も534件に達した。サードパーティを介したサイバー攻撃の割合は30%に倍増し、日本における第三者リスクは世界平均を大幅に上回る水準となっている。

本レポートでは、サードパーティリスクの基本概念から実践的管理手法まで、2024年の最新インシデント事例とトレンドを踏まえた包括的な分析を提供する。

第1章 サードパーティリスクの基本概念

1.1 サードパーティリスクの定義

サードパーティリスク（第三者リスク）とは、企業が外部組織（サードパーティ）との関係から生じる潜在的な脅威を指す。これには、ベンダー、サプライヤー、業務委託先、クラウドサービスプロバイダー、パートナー企業などとの取引関係に起因するリスクが含まれる。

1.2 サードパーティリスクの分類体系

1.2.1 リスクカテゴリー別分類

- オペレーショナルリスク：サービス中断、品質低下、納期遅延
- 財務リスク：取引先倒産、信用悪化、連鎖破綻
- コンプライアンスリスク：法規制違反、監査不備、規制変更対応
- セキュリティリスク：データ漏洩、サイバー攻撃、情報セキュリティ侵害
- 戦略リスク：事業継続性、競争力低下、技術的陳腐化
- レピュテーションリスク：風評被害、ブランド価値毀損、顧客信頼失墜

1.2.2 関係性による分類

- 直接取引先：一次ベンダー、主要サプライヤー
- 間接取引先：二次・三次サプライヤー、サブコントラクター

- 重要インフラ提供者：クラウドプロバイダー、通信事業者
- 規制対象サービス：金融サービス、個人情報取扱業務

1.3 2024年のサードパーティリスク環境

2024年 主要統計データ

- 第三者経由のデータ漏洩：30%（前年15%から倍増）
- サプライチェーン攻撃：431%増（2021-2023年比）
- 連鎖倒産件数：74件（過去30年で最多）
- 平均データ漏洩コスト：$4.88million（過去最高額）
- クラウド障害による年間ダウンタイム：77時間

第2章 パートナー企業の財務リスク分析

2.1 財務リスクの要因と影響

2.1.1 主要な財務リスク要因

パートナー企業の財務悪化は、以下の要因により発生する：

- 経済環境の悪化（インフレ、金利上昇、景気後退）
- 業界固有の構造変化（デジタル化、規制変更）
- 財務管理の不備（過剰債務、キャッシュフロー悪化）
- 経営戦略の失敗（過度な拡張、投資ミス）
- 外部ショック（自然災害、パンデミック、地政学リスク）

2.1.2 財務悪化の兆候

兆候カテゴリー	具体的指標	警告レベル
収益性	売上高営業利益率	3期連続悪化
流動性	流動比率	100%未満
安全性	自己資本比率	20%未満

効率性	総資産回転率	業界平均の50%未満
成長性	売上高成長率	3期連続マイナス

2.2 2024年の連鎖倒産事例分析

事例1：テックコーポレーション破綻による連鎖倒産

概要：2024年3月、広島のテックコーポレーション（負債191億9400万円）が破産。不自然な手形取引の末の破綻により、1ヶ月で取引先の連鎖倒産が発生。

影響範囲：直接取引先10社以上、債権者445名、推定被害額約10億円

教訓：手形取引の実態確認、取引先の財務状況の継続的監視の重要性

事例2：小規模事業者の連鎖倒産急増

概要：2024年度の負債1,000万円未満倒産534件のうち、「他社倒産の余波」が74件（64.4%増）と急増。

特徴：親会社や主要取引先への売上依存度が高い小・零細企業が多数被害

業種別影響：サービス業236件、建設業80件、小売業72件

2.3 業界別財務リスク分析

業界	主要リスク要因	2024年倒産予測ランキング	対策優先度
電子部品製造業	複数年赤字、設備投資過多	1位	極高
宿泊業	コロナ後遺症、人材不足	2位	高

農業	気候変動、原材料コスト増	3位	高
運輸業	2024年問題、燃料費高騰	4位	中
建設業	資材価格上昇、人件費増	5位	中

第3章 2024年重大インシデント事例

3.1 サイバーセキュリティ関連インシデント

株式会社イセトー ランサムウェア攻撃

発生日：2024年5月26日

被害規模：約150万件の個人情報漏洩可能性

影響範囲：銀行、保険会社、自治体など150以上の組織

原因：VPN経由の不正アクセス、データ管理体制の不備

経済損失：数十億円規模の対応コスト

学んだ教訓：サプライチェーン全体のセキュリティ管理、データ保管ルールの徹底、VPN機器の脆弱性管理

CrowdStrike グローバル障害

発生日：2024年7月19日

被害規模：全世界850万台のWindows端末

影響範囲：航空、金融、医療、小売業界

経済損失：$5.4billion（米国のみ）

学んだ教訓：クリティカルシステムの冗長化、段階的アップデート、ベンダー依存度の分散

3.2 クラウドサービス障害

発生日	サービス	障害時間	主要影響	原因
2024年1月18日	Atlassian Jira	4時間	プロジェクト管理停止	データベース更新失敗
2024年2月22日	AT&T	12時間	通信サービス全般	ネットワーク設定ミス
2024年7月30日	Microsoft Azure	9時間	クラウドサービス全般	DDoS攻撃とシステム障害
2024年9月30日	Verizon	10時間	モバイル通信	ネットワーク機器障害

3.3 業務委託先起因のインシデント

2024年 業務委託先関連インシデント統計

- 総件数：213件（全インシデントの36.3%）
- 情報漏洩件数：約2,164万件
- 最多業種：製造業（18社）、サービス業（14社）
- 平均復旧期間：23日
- 平均対応コスト：$4.1million

第**4**章 サードパーティリスク管理フレームワーク

4.1 TPRM（**Third Party Risk Management**）の基本構造

TPRMライフサイクル管理

1. 計画（**Planning**）
    - 事業要件の明確化
    - リスク評価の実施
    - 予算・リソース計画
2. デューデリジェンス（**Due Diligence**）
    - 財務状況調査
    - セキュリティ評価
    - コンプライアンス確認
3. 契約交渉（**Contract Negotiation**）
    - SLA/SLO設定
    - 責任分担明確化
    - 終了条項整備
4. 継続監視（**Ongoing Monitoring**）
    - パフォーマンス監視
    - 財務状況追跡
    - インシデント管理
5. 契約終了（**Termination**）
    - 移行計画実行
    - データ返却・削除
    - 知的財産権整理

4.2 財務リスク評価手法

4.2.1 定量的評価指標

評価項目	主要指標	健全性基準	警告基準	危険基準
収益性	営業利益率	5%以上	2-5%	2%未満
安全性	自己資本比率	40%以上	20-40%	20%未満
流動性	流動比率	150%以上	100-150%	100%未満
効率性	総資産回転率	1.0以上	0.5-1.0	0.5未満

成長性	売上成長率	5%以上	0-5%	マイナス成長

4.2.2 定性的評価項目

- 経営陣の質：経営経験、業界知識、危機管理能力
- 事業モデル：競争優位性、市場地位、収益構造
- ガバナンス：内部統制、コンプライアンス体制、透明性
- 市場環境：業界動向、競合状況、規制環境
- オペレーション：品質管理、効率性、技術力

4.3 リスク軽減策

4.3.1 予防的対策

- 多様化戦略：複数ベンダーの活用、地理的分散
- 契約条項強化：SLA設定、ペナルティ条項、保険要求
- 継続的監視：定期的財務確認、早期警戒システム
- エスクロー制度：ソースコード預託、データバックアップ

4.3.2 事後対応策

- 事業継続計画：代替ベンダー確保、内製化準備
- 損失軽減措置：保険活用、法的措置、債権回収
- 顧客対応：情報開示、代替サービス提供、補償検討
- 学習・改善：事後分析、プロセス見直し、予防策強化

第**5**章 規制動向と業界標準

5.1 国内規制動向

5.1.1 金融業界

金融庁は2024年5月、「第三者リスク管理ガイダンス」を発行し、金融機関に対してより厳格なTPRM体制構築を求めている。特に、以下の要件が強化された：

- 重要業務の特定と分類
- 第三者の財務健全性評価
- 継続的監視体制の確立
- 事業継続計画の策定

5.1.2 個人情報保護

個人情報保護委員会は、委託先管理に関するガイドライン改正を検討中。主なポイント：

- 委託先の選定基準明確化
- 再委託管理の強化
- データ移転時の安全管理措置
- インシデント時の報告体制

5.2 国際規制動向

5.2.1 EU規制

- **DORA**（**Digital Operational Resilience Act**）：金融機関のデジタル運営レジリエンス要求
- **NIS2**指令：重要インフラの第三者リスク管理義務化
- **CSRD**：企業持続可能性報告指令における供給網リスク開示

5.2.2 米国規制

- 連邦準備制度理事会ガイダンス：コミュニティ銀行向けTPRM指針
- **SEC**要求事項：サイバーセキュリティインシデントの迅速報告
- **CISA**推奨事項：重要インフラの供給網セキュリティ強化

第**6**章 **2025**年以降の展望

6.1 新興リスクとトレンド

6.1.1 AI・自動化リスク

- AIサービス依存度増加に伴う新たなリスク
- アルゴリズムの透明性と説明責任
- AI判断エラーの組織全体への波及
- 学習データの品質・バイアス問題

6.1.2 地政学リスク

- 国際制裁によるサプライチェーン分断
- データローカライゼーション要求
- 技術移転制限と知的財産保護
- クロスボーダー取引の複雑化

6.1.3 環境・社会リスク

- 気候変動による物理的影響
- ESG要求事項の厳格化
- 人権デューデリジェンス義務化
- サステナビリティ報告要求

6.2 推奨対応策

2025年に向けた戦略的対応

短期対応（**6**ヶ月以内）

- 既存第三者の財務健全性緊急チェック
- 重要業務の特定と影響度評価
- インシデント対応体制の見直し
- 契約条項の最新化

中期対応（**6-18**ヶ月）

- TPRM統合プラットフォーム導入
- リスクベース監視システム構築
- 代替ベンダー戦略策定
- デジタル化による効率性向上

長期対応（**18**ヶ月以上）

- エコシステム全体の最適化
- 予測分析による先制的管理
- ゼロトラスト原則の完全実装
- レジリエント組織への変革

第**7**章 実践的管理手法

7.1 組織体制の構築

7.1.1 ガバナンス構造

役割	責任者	主要職務	報告関係
戦略策定	取締役会	方針決定、予算承認	株主・規制当局
統括管理	CRO	全社リスク管理	CEO・取締役会

実務運営	TPRMオフィサー	日常的監視・評価	CRO・各部門長
専門支援	法務・IT・調達	専門知識提供	TPRMオフィサー

7.1.2 三線防御モデル

- 第一線：事業部門によるリスクオーナーシップ
- 第二線：リスク管理部門による独立監視
- 第三線：内部監査による客観的保証

7.2 技術的ソリューション

7.2.1 統合リスク管理プラットフォーム

- ベンダー情報の一元管理
- リアルタイムリスク監視
- 自動アラート機能
- ダッシュボード・レポート機能

7.2.2 AIを活用した予測分析

- 財務悪化の早期予測
- 異常検知アルゴリズム
- シナリオ分析・ストレステスト
- 自動リスクスコアリング

7.3 測定・評価指標（**KPI**）

指標カテゴリー	**KPI**名称	目標値	測定頻度
予防効果	高リスクベンダー比率	5%以下	月次
検知能力	インシデント早期発見率	90%以上	四半期
対応効率	平均復旧時間	24時間以内	インシデント毎

コスト効果	TPRM投資回収率	3:1以上	年次
業務継続	サービス可用性	99.9%以上	月次

結論

2024年は、サードパーティリスクが企業経営の中核課題として浮上した転換点となった。パートナー企業の財務悪化による連鎖倒産、サイバー攻撃の第三者経由侵入、クラウドサービス障害による業務停止など、従来のリスク管理の枠組みを超える事象が多発している。

これらの課題に対処するためには、従来の契約ベースの管理から、継続的監視と予測分析を組み合わせた動的なリスク管理への転換が不可欠である。また、組織内の縦割りを排し、全社横断的なガバナンス体制の構築が求められる。

2025年以降は、AI・自動化の進展、地政学リスクの高まり、環境・社会要求の厳格化により、サードパーティリスクはさらに複雑化することが予想される。企業は、これらの変化を先取りし、レジリエントな組織への変革を進めることで、持続可能な成長を実現していかなければならない。

本レポートは2025年6月時点の公開情報に基づいて作成されております。
最新の動向については、各企業・機関の公式発表をご確認ください。

監修者:
鎌田光一郎:青山学院大学法学部卒業。SMBC日興証券株式会社にて証券営業、経営管理業務に従事したのちPwCコンサルティンク゛合同会社に転籍。金融機関に対するコンサルティンク゛業務に従事。その後、Librus株式会社を設立、代表取締役に就任。

お問い合わせ先
Librus株式会社（代表取締役 鎌田光一郎）
105-0004東京都港区新橋6丁目13-12 VORT新橋Ⅱ 4F
03-6772-8015
お問い合わせフォーム
https://librus.co.jp/contact