リーディングカンパニーにおける
サードパーティセキュリティリスクマネジメント

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

デジタル変革の加速により、企業のサードパーティへの依存度は前例のない水準に達している。2024年の調査によると、**73%**の組織がサードパーティリスク管理（**TPRM**）プログラムの非効率性により風評リスクに晒されていると報告している。

2024年は多くの重大なサードパーティ関連インシデントが発生した年として記録されており、CrowdStrikeの大規模システム障害、Change Healthcareのランサムウェア攻撃、MOVEitファイル転送ソフトウェアの脆弱性悪用など、いずれも数百万人の顧客と数千の企業に影響を与えた。

本ホワイトペーパーでは、2025年における大規模事業者のサードパーティリスクマネジメントの最新トレンド、主要インシデントの詳細分析、実践的なベストプラクティス、そして新興する規制要件について包括的に分析する。

1. 市場動向とトレンド

1.1 市場規模とベンダーリスク管理の成長

ベンダーリスク管理市場は急速な成長を続けており、2024年には**119**億**8,000**万米ドルに達し、年平均成長率**12.5%**で成長し、2029年には**215**億**9,000**万米ドルに達すると予測されている。

この成長の主要因として以下が挙げられる：

- サプライチェーン攻撃の431%増加（2021-2023年）
- 規制要件の強化（DORA、NIS2、金融庁ガイドライン等）
- AI技術の導入によるリスク評価の高度化
- サードパーティへの依存度の継続的な増加

1.2 2025年のキートレンド

1.2.1 AI駆動型リスク管理の普及

2025年は「統合リスク管理とAIの産業化」が主要テーマとなる。調査によると、2024年に37%の組織がAIリスクを管理していなかったが、2025年にはこの数字が23%に大幅減少し、38%の改善を示している。

1.2.2 サードパーティ依存関係の拡大

AIの導入により、組織のサードパーティ依存関係はさらに拡大している。特に以下の分野で顕著：

- クラウドサービスプロバイダー
- SaaSアプリケーション
- AIプラットフォームとモデル提供者
- サイバーセキュリティベンダー

1.2.3 新たな脆弱性の拡大

サードパーティリスクの範囲は従来のサイバーセキュリティリスクを超えて拡大している：

- 運用継続性リスク
- データプライバシー・主権リスク
- ESG・レピュテーションリスク
- 地政学的リスク

2. 主要インシデント事例分析

2.1 CrowdStrike大規模システム障害（**2024**年**7**月）

インシデント概要

発生日：2024年7月19日
原因：CrowdStrike Falcon Sensorの欠陥のあるコンテンツアップデート
影響範囲：世界規模での航空、銀行、緊急サービス、医療システムの停止

学習ポイント

- 単一ベンダー依存のリスク：重要なサービスにおける単一ベンダーへの過度な依存の危険性
- カスケード障害：一つのソフトウェア更新が業界全体に影響を与える可能性
- 代替手段の重要性：主要ベンダーが利用不可能になった場合の代替戦略の必要性
- 更新管理：自動更新プロセスにおけるリスク評価と段階的展開の重要性

対応策

- 重要システムにおけるマルチベンダー戦略の採用
- 更新プロセスの段階的展開とテスト環境での事前検証

- インシデント対応計画の定期的な見直しと訓練

2.2 Change Healthcare ランサムウェア攻撃（2024年2月）

インシデント概要

発生日：2024年2月21日
攻撃者：ロシア系ランサムウェアグループ
損害額：24億5,700万ドル（2024年第3四半期時点）
影響：全米の医療システムの運用停止、患者データの大規模漏洩

学習ポイント

- 重要インフラへの影響：医療システムのような重要インフラにおけるサードパーティ依存のリスク
- データブリーチの規模：1億人を超える個人情報が影響を受けた
- 復旧期間の長期化：システム復旧に8ヶ月以上を要した
- 経済的影響：史上最大規模のランサムウェア攻撃による損失

2.3 MOVEit ファイル転送ソフトウェア攻撃（2023年）

インシデント概要

発生時期：2023年5月 〜
攻撃手法：Progress Software MOVEit TransferのゼロデイSQL脆弱性悪用
攻撃者：Clopランサムウェアグループ
影響企業：Shell、British Airways、BBC等数千社

学習ポイント

- ファイル転送ソフトウェアのリスク：機密データを扱うファイル転送システムの脆弱性
- ゼロデイ攻撃：事前に知られていない脆弱性を悪用した攻撃の脅威
- サプライチェーン攻撃：一つのソフトウェアベンダーを通じた大規模な被害

2.4 SolarWinds サプライチェーン攻撃（2020年）継続的な教訓

継続的な影響と教訓

SolarWinds攻撃から4年が経過した現在も、その教訓は2025年のサードパーティリスク管理において重要な指針となっている：

- ソフトウェア更新プロセスの セキュリティ強化
- ゼロトラストアーキテクチャの採用
- 継続的監視とアノマリー検出
- ベンダー評価プロセスの強化

2.5 Log4jの脆弱性（CVE-2021-44228）の継続的な影響

2025年における継続的なリスク

2021年末に発見されたLog4jの脆弱性は、2025年現在でも多くの組織にとって課題となっている：

- レガシーシステムでの未修正の脆弱性
- サードパーティソフトウェアに組み込まれた隠れたLog4jコンポーネント
- ベンダー管理におけるソフトウェア部品表（SBOM）の重要性

対応策

- すべてのサードパーティソフトウェアのSBOM要求
- 脆弱性スキャンの定期実行
- ベンダーとの脆弱性対応に関する明確な契約条項

3. ベストプラクティスとフレームワーク

3.1 TPRM最適化のための10の重要要素（KPMG推奨）

1. 明確なインシデント報告プロトコルの確立
   サードパーティがセキュリティ侵害やコンプライアンス問題を報告する方法と時期を明確に定義
2. リスクスチュワードの任命
   組織全体のサイロを超えてリスク管理要件の優先順位付けを行う専任担当者の設置
3. 企業レベルでの統合的アプローチ
   調達、サイバーセキュリティ、サプライチェーン管理を統合したホリスティックな視点
4. **AI**導入準備への投資
   データ品質改善、標準化、ガバナンス体制の整備
5. 継続的リスク監視
   ベンダーのリスクプロファイルの定期的な評価と更新
6. 契約条項の標準化
   セキュリティ要件、インシデント対応、データ保護に関する標準契約条項
7. 複数層防御の実装
   単一の防御策に依存しない多層的なセキュリティ対策
8. 定期的な評価とテスト
   ペネトレーションテスト、脆弱性評価、インシデント対応訓練

9. ベンダー関係の多様化
   重要なサービスにおける単一ベンダー依存の回避
10. 出口戦略の準備
    主要ベンダーとの関係終了時の代替手段と移行計画

3.2 NIST サイバーセキュリティフレームワーク 2.0 対応

NIST CSF 2.0では、サプライチェーンサイバーセキュリティリスク管理がより重点的に扱われている：

機能	カテゴリ	主要要件
GOVERN	サイバーセキュリティサプライチェーンリスク戦略	組織のコンテキスト理解、戦略確立
IDENTIFY	ID.SC-4	サプライヤーとサードパーティパートナーの定期的評価
PROTECT	サプライチェーン保護	適切な保護措置の実装
DETECT	継続的監視	サプライチェーン内の異常検知
RESPOND	インシデント対応	サプライチェーンインシデントへの迅速な対応
RECOVER	復旧計画	サプライチェーン中断からの復旧

3.3 EY推奨：AI活用による変革的TPRM

EYの2025年サードパーティリスク管理調査によると、以下の3つのアクションがTPRM変革を加速する：

3.3.1 企業レベルでの統合的アプローチ

- 規制要件、取締役会指令、投資家要求の統合理解

- 組織サイロを超えたメトリクス統合
- エンタープライズレベルでの意思決定最適化

3.3.2 AI準備態勢への投資

- 既存TPRMプロセス、ツール、データ管理慣行の包括的評価
- データ品質改善と標準化
- 従業員のスキルギャップ解消と訓練
- 新興AIトレンドの継続的監視

3.3.3 前提条件の見直しとティッピングポイントの加速

- 技術の非線形変化への適応
- コストベネフィット計算の見直し
- 組織構造の再編

4. 規制環境とコンプライアンス

4.1 欧州：**DORA**（**Digital Operational Resilience Act**）

施行日：2025年1月17日
対象：EU内の金融機関とその重要なサードパーティサービスプロバイダー

主要要件

- ICTリスクマネジメントフレームワークの確立
- サードパーティサービスプロバイダーの継続的監視
- インシデント報告とリスク管理
- デジタル運用レジリエンステスト
- ICTサードパーティリスクの包括的管理

4.2 日本：金融庁サイバーセキュリティガイドライン

公表日：2024年10月4日
対象：国内金融機関

サードパーティリスク管理の着眼点

- 契約開始時およびその後の継続的なリスク評価
- サードパーティのサイバーセキュリティ態勢の定期的確認
- インシデント発生時の報告・対応体制
- SaaSリスク管理の強化（SSPM: SaaS Security Posture Management）

4.3 日本：経済産業省サプライチェーンセキュリティ対策

制度開始予定：2026年10月（予定）
対象：サプライチェーン企業

評価制度の概要

- 5段階のセキュリティ対策レベル評価
- 星の数による可視化システム
- 基本的対策の導入認証
- サイバー攻撃リスクの約80%低減効果

4.4 米国:連邦規制動向

NIST SP 800-161 Rev. 1

- サイバーサプライチェーンリスク管理の包括的ガイダンス
- C-SCRM（Cyber Supply Chain Risk Management）の実装
- ベンダー選定と管理のベストプラクティス

SEC サイバーセキュリティ開示規則

- 重大なサイバーインシデントの4日以内報告
- 年次サイバーセキュリティリスク管理開示
- サードパーティリスクの透明性要求

5. 業界別リスク特性

5.1 金融サービス業

主要リスク

- フィンテックパートナーのサイバーリスク
- クラウドサービスプロバイダーの集中リスク
- 決済処理業者の運用継続性リスク
- データプロセッサーの規制コンプライアンスリスク

対応戦略

- 金融業界固有のリスク評価フレームワーク
- レジリエンス要件の契約化
- 定期的なストレステスト
- 規制当局との連携強化

5.2 ヘルスケア業界

主要リスク

- 電子健康記録（EHR）システムの脆弱性
- 医療機器メーカーのセキュリティリスク
- クラウドストレージプロバイダーのデータ保護
- 医療用IoTデバイスの管理

5.3 製造業

主要リスク

- 産業制御システム（ICS/SCADA）の脆弱性
- サプライヤーの製造停止リスク
- 知的財産の保護
- IoTセンサーとエッジデバイスのセキュリティ

6. 技術トレンドとイノベーション

6.1 AI・機械学習の活用

現在の応用領域

- リスクスコアリング：ベンダーのリスクレベル自動評価
- 異常検知：サードパーティ行動の異常パターン検出
- 予測分析：将来のリスク発生確率予測
- 自然言語処理：契約書の自動レビューとリスク条項抽出

2025年の新興技術

- エージェンティック**AI**：自律的なリスク評価と対応
- マルチモーダル**AI**：テキスト、画像、データの統合分析
- 推論**AI**：複雑なリスクシナリオの分析
- 自己改善**AI**：継続的学習による評価精度向上

6.2 ブロックチェーンとサプライチェーン透明性

- サプライチェーンの完全なトレーサビリティ
- 改ざん不可能な取引記録
- スマートコントラクトによる自動コンプライアンス
- デジタル身元証明とゼロトラスト統合

6.3 ゼロトラストアーキテクチャ

サードパーティリスク管理における適用

- 「信頼するが検証する」から「決して信頼せず、常に検証する」へ
- 継続的な認証と認可
- 最小権限アクセス原則
- マイクロセグメンテーション

7. 財務影響と**ROI**分析

7.1 サードパーティリスクの財務インパクト

インシデント種類	平均損失額（**USD**）	復旧期間	追加影響
データブリーチ	4.45 million	287日	規制罰金、訴訟
システム停止	5.6 million	24時間	顧客信頼失墜
サプライチェーン攻撃	2.4 billion	8ヶ月	業界全体影響
ランサムウェア	1.85 million	23日	風評被害

7.2 TPRM投資のROI

コスト削減効果

- インシデント予防：平均70%のセキュリティインシデント削減
- コンプライアンス効率化：規制対応コスト40%削減
- 契約交渉力向上：ベンダー費用15-20%削減
- 運用効率化：手作業による評価時間80%短縮

投資回収期間

- 大規模企業：18-24ヶ月
- 中規模企業：12-18ヶ月
- 金融機関：6-12ヶ月（規制要件により）

8. 業界ベンチマークと成熟度評価

8.1 TPRM成熟度モデル

レベル	特徴	組織の割合	主要課題
レベル1：基本的	基本的なベンダー管理	35%	標準化されたプロセスの欠如

レベル2:管理された	文書化されたプロセス	40%	自動化の不足
レベル3:定義された	標準化されたTPRMフレームワーク	20%	継続的監視の限界
レベル4:量的に管理された	メトリクス駆動型管理	4%	予測分析の制限
レベル5:最適化された	継続的改善とAI統合	1%	組織全体での一貫性

8.2 業界別成熟度

- 金融サービス:平均レベル 2.8(規制要件により高い)
- ヘルスケア:平均レベル 2.3(データ保護重視)
- 製造業:平均レベル 2.1(物理的セキュリティ重視)
- 小売業:平均レベル 2.0(顧客データ保護)
- 公共セクター:平均レベル 1.9(予算制約)

9. 2025年予測と推奨事項

9.1 2025年の**7**つの重要予測

1. サイバー犯罪者のターゲット変化:医療、金融、教育等の高価値業界のサードパーティが主要標的に
2. ビジネスレジリエンスの重視拡大:2025年は透明性とサステナビリティに重点を置いたビジネスレジリエンスが焦点
3. **AI**統合の加速:関連技術との組み合わせによるTPRMのゲームチェンジャー化
4. 規制要件の強化:DORA、NIS2等の本格運用開始による大幅な規制強化
5. サードパーティ依存関係の複雑化:第4・第5次パーティまでのリスク管理必要性
6. リアルタイム監視の標準化:継続的リスク監視がデフォルトに
7. 業界特化型ソリューションの普及:汎用ソリューションから業界特化型へのシフト

9.2 経営陣への推奨事項

戦略レベルの推奨事項

1. サードパーティリスクの取締役会議題化：四半期ごとの取締役会でのサードパーティリスク報告制度化
2. **Chief Risk Officer**（**CRO**）の権限強化：サードパーティリスクに関する意思決定権限の明確化
3. 年間予算の**5-8%**を**TPRM**に配分：適切なリソース配分によるプログラム強化
4. クライシス管理体制の確立：サードパーティインシデント専用の危機管理チーム設置
5. 保険戦略の見直し：サイバー保険・サードパーティ賠償責任保険の拡充

9.3 運用レベルの推奨事項

即座に実行すべき施策

1. サードパーティ台帳の完全化：全てのベンダー・サプライヤーの網羅的リスト作成
2. 重要度に基づく分類（**Tier**分け）：ビジネスインパクトに基づくベンダー分類システム導入
3. 契約条項の標準化：セキュリティ・プライバシー・インシデント対応に関する標準条項策定
4. 定期評価スケジュールの確立：リスクレベルに応じた評価頻度の設定
5. インシデント対応計画の策定：サードパーティ起因インシデント専用の対応計画
6. 従業員訓練プログラム：サードパーティリスク認識向上のための定期訓練
7. メトリクス・**KPI**の設定：TPRM効果測定のための定量指標確立

9.4 技術投資の優先順位

2025年の技術投資ロードマップ

第**1**四半期：基盤整備

- 統合GRC（Governance, Risk, Compliance）プラットフォーム導入
- ベンダー管理システム（VMS）の実装
- リスク評価自動化ツールの導入

第**2**四半期：監視強化

- 継続的監視ソリューション導入
- 脅威インテリジェンス統合
- ダッシュボードとレポーティング機能強化

第**3**四半期：**AI**統合

- AI駆動型リスクスコアリング導入
- 機械学習ベースの異常検知

- 予測分析機能の実装

第4四半期：最適化

- プロセス自動化の拡張
- 統合レポーティングシステム
- 次年度戦略策定とシステム評価

10. 結論

2025年は、大規模事業者にとってサードパーティリスクマネジメントが戦略的重要性を増す転換点となる。CrowdStrike、Change　Healthcare、MOVEitといった2024年の重大インシデントは、サードパーティリスクがもはや「IT部門の課題」ではなく、「経営リスク」であることを明確に示している。

特に注目すべきは、単一のソフトウェア更新が世界規模での業務停止を引き起こす現実と、一つのファイル転送ソフトウェアの脆弱性が数千の企業に影響を与えるサプライチェーン攻撃の脅威である。これらのインシデントは、従来のリスク管理アプローチでは対処できない新たな現実を浮き彫りにしている。

2025年に向けて、組織は以下の変化に適応する必要がある：

- 規制環境の大幅変化：DORA（2025年1月施行）、日本の金融庁ガイドライン強化、経済産業省のサプライチェーンセキュリティ評価制度等
- **AI**技術の本格導入：手作業から自動化されたインテリジェントなリスク管理へ
- リスク範囲の拡大：サイバーリスクから運用継続性、ESG、地政学的リスクまで
- ステークホルダー期待の向上：投資家、規制当局、顧客からの透明性要求

成功する組織は、TPRMを単なるコンプライアンス活動から戦略的競争優位性の源泉へと変革する必要がある。これには、経営層のコミットメント、適切なリソース配分、技術投資、そして組織文化の変革が不可欠である。

最終的に、2025年のサードパーティリスクマネジメントは、組織のレジリエンス、信頼性、持続可能性を決定する重要な要素となる。先進的な組織は既にこの変化を予見し、必要な投資と変革を実行している。残された時間は限られており、今こそ行動を起こすべき時である。

最重要アクションアイテム

本ホワイトペーパーを読了した経営陣は、以下の3つの質問に90日以内に回答できる体制を構築することを強く推奨する：

1. 当社の最も重要なサードパーティ10社が明日利用不可になった場合、事業継続は可能か？
2. 当社のサードパーティがサイバー攻撃を受けた場合、24時間以内にその影響を評価できるか？
3. 2025年の新たな規制要件に対して、当社のTPRMプログラムは準拠しているか？

これらの質問に明確に答えられない場合、直ちにTPRM強化プログラムの開始を検討すべきである。

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