Deloitte.
デロイト トーマツ

金融セクターのサードパーティ・サプライチェーンのサイバーリスク管理に関する調査

報告概要資料

デロイト トーマツ サイバー合同会社

2023年11月30日

調査対象とした米国大手金融機関では、先進事例と認められる対策を推進していた

エグゼクティブサマリ

今回調査対象とした米国大手金融機関では、サードパーティ・サプライチェーンに対するサイバーリスクを認識し、専門家の育成、人的リソースの確保、部門相互が密に連携する体制を敷くことで対応していた。相談して解決策を見出すカルチャーの醸成、情報の蓄積や連携を効率化するツールの活用も進められていた。
これらはいずれも新たな脅威を重要なリスクとして認識し、これに適切に対応するための仕組み作りや体制作りが進められてきた結果と考えられる。

組織体制	サードパーティサイバーリスク管理（TPCRM※）の専担者が**グローバルにリスク管理を行っている**。また、1線及び2線において牽制機能があるなど**組織的にTPCRMを行うための仕組み**がある。
人的リソース リスク管理ツール	数千社のサードパーティを管理するために、TPCRM部門に百人規模でサードパーティのサイバーリスク管理の専門家を配置し、**人材の量と質の向上に努めて**いる。 リスク管理に関わる作業は**内製、市販ツールの活用により効率化**している。
リスク管理手法	評価対象を**リスクレベルで分類し、高リスクの評価対象に対するモニタリングに注力する**継続的モニタリングを実施している。 必要に応じ、4thパーティ（とそれ以降）のリスク評価も金融機関が自ら行っている。 自社と同レベルのセキュリティ水準をサードパーティに求めるため、**契約や要綱に詳細を明記**している。
ソフトウェア管理 ハードウェア管理	ソフトウェアサプライチェーンリスク管理面では、**ソフトウェア構成解析などの利用可能な手法を組み合わせて**可能な限りリスクを把握するとともに必要な対策を進めている。 ハードウェアセキュリティについては、ファームウェアやUEFI（BIOS）の真正性を確保するための対策の導入などにより、**セキュアな調達を実現する取組み**が認められる。

※　Third Party Cyber Risk Managementの略。

サードパーティ・サプライチェーンサイバーリスク管理に関する既存ガイダンスや想定される金融機関の状況を踏まえ、調査を実施した

調査概要

調査目的		重要性が高まっているサードパーティ・サプライチェーンサイバーリスク管理（TPCRM/C-SCRM※）について、その対応が比較的進んでいるとされる米国の大手金融機関における管理手法（先進事例）を調査し、特に本邦金融機関におけるリスク管理等への示唆について考察する。
調査のアプローチ		米国大手金融機関のTPCRM/C-SCRMの（1）組織体制、リソース（人材、専門性など）及び仕組み（管理枠組みやツールなど）、（2）契約による管理をはじめとしたリスク管理プロセス、（3）TPCRM/C-SCRMの観点から、金融機関が課題として認識すべきソフトウェア管理、並びに（4）ハードウェア管理を主たる調査項目とし、まず、金融セクターのTPCRM/C-SCRMに関連する基準やガイダンス等から関連する要素を整理した上で、次に、米国大手金融機関数社を対象に、質問票への回答を依頼するとともにヒアリングを行った。
調査領域	**組織体制 人的リソース 管理の仕組み、ツール**	• TPCRM/C-SCRMの管理体制 • 関連業務に充てる人員数、専門性・スキル及びその確保、育成 • ツールの導入、活用状況、利点と問題点
	リスク管理プロセス	• ライフサイクル管理、継続的モニタリングや4thパーティ以降の管理手法 • 契約管理、契約遵守のモニタリング • サイバー脅威の監視体制 • 契約終了や他サービスへの移行を想定した出口戦略の策定 • 集中リスクの管理、モニタリング
	ソフトウェア管理	• ソフトウェアの脆弱性管理
	ハードウェア管理	• 機器の真正性、ファームウェアの不正書換え防止管理 • セキュアな調達のためのガイドラインや業界標準の利用状況
調査期間		2023年6月16日から11月30日（米国大手金融機関へのヒアリングは2023年8月実施）

※　TPCRM: Third Party Cyber Risk Managementの略。
　　C-SCRM: Cyber Supply Chain Risk Managementの略。

米国大手金融機関への調査より得られた知見から本邦金融機関における改善のステップを例示した

調査結果要約（1/2）

調査項目	調査結果	本邦金融機関における改善ステップの例示
組織体制 人的リソース 管理の仕組み ツール	組織体制については、**1線部署内にTPCRM担当**が置かれ、業務部門を牽制する1.5線的な役割を果たしている。 2線部署にもTPCRM担当が置かれ、**グローバルで一元的な管理**、牽制を行っている。 1線の判断に2線が介入する権限が与えられている。 人的リソースについては、管理対象数千社に対し**サイバー専門家を百人規模で配置**している。業務関連スキル向上のための社内トレーニングやメンター制度を設けている。 管理の仕組み、ツールについては、サードパーティとのアンケートのやり取りや回答結果の集約に**内製、市販ツールを活用し、効率化**している。	• 1線内の統制機能の強化 • 2線の専門性及び介入権限の強化 • リスク受容のエスカレーション手続きの明確化等の体制強化 • 現時点及び将来的に必要な人的リソース状況の整理 • 人材確保・育成計画の策定及び実施 • 各種ツールの活用検討
リスク管理 プロセス	ライフサイクル管理については、**契約形態に関わらず全てのサードパーティサービス関係を管理対象**とし、リスクに応じたモニタリング手法を用いている。4thパーティ以降に対しては、自社と同水準のコントロールの実施を契約上求めるなど間接的に管理するが、必要に応じて金融機関が自らリスク評価を行うケースもある。 契約管理については、契約書や付属書に**要件を詳細に規定して遵守を要求**し、継続的なモニタリングを行っている。	• サードパーティ及び4thパーティ以降の管理範囲、管理手法検討 • リスクベースのモニタリング手法検討 • 管理の仕組み、ツール、人的リソースの再配分 • サードパーティが遵守すべきサイバーセキュリティ要件の契約条項への盛り込み、付属書の新規作成を検討

米国大手金融機関への調査より得られた知見から本邦金融機関における改善のステップを例示した

調査結果要約（2/2）

調査項目	調査結果	本邦金融機関における改善ステップの例示
リスク管理プロセス（続き）	**サイバー脅威の監視**については、サードパーティ及びICTサプライチェーンにおけるサイバー脅威や脆弱性のモニタリングに、**サイバー脅威インテリジェンスを活用**している。	• サードパーティ及びICTサプライチェーンを対象としたサイバー脅威インテリジェンスのスコープや内容の見直し • 脅威インテリジェンス分析ツール、ASMツール、OSINTの活用検討
	出口戦略については、契約解除、インシデントに起因する**代替サービスへの移行に関するプロセスを事前に計画**、準備している。 契約終了時の機密情報の返却や必要な支援を提供することを契約上取り決めている。	• 左記要素を踏まえた契約終了時、サイバーインシデント発生時の対応プロセスの検討
	集中リスクについては、代替可能性、地理的集中、複数のサードパーティが共通に利用している4thパーティといった要素を検討し、**定期的に集中リスクの評価を実施**している。	• 左記要素を踏まえた集中リスク評価手法の検討
ソフトウェア管理 ハードウェア管理	**ソフトウェア管理**については、脆弱性検査、ソフトウェア構成要素分析、ソースコードレビュー等、**受入時のソフトウェアの脆弱性評価**を実施している。	• 脆弱性評価、構成要素管理等、組み込まれたOSS等の脆弱性対応も想定した脆弱性管理手法の検討
	ハードウェア管理については、端末、サーバが**ファームウェア改ざん防止機能等を有していることを調達基準**としている。 会社の倫理基準や法令の遵守などの要件に基づいた制裁対象国及び制裁対象サプライヤーリストを維持している。	• 不正なファームウェア導入のリスク等を考慮した調達基準の見直し • 調達に関するビジネス、倫理、法規制等のポリシーとの整合を図り、調達基準や取引基準等への組込み検討

Deloitte.
デロイト トーマツ

本件調査は、米国大手金融機関における先進的な取組みを抽出し、本邦金融機関に対する示唆を得ることを目的に実施されたものです。調査対象先はいずれも全世界に拠点を持ち、従業員数は数万から数十万人規模の組織です。本報告書ではこれらの金融機関における実務に言及しておりますが、特に組織体制や人的リソースに係るものはこの規模を前提としており、必ずしも全ての業態や規模の金融機関にそのままあてはまるものではない点につき、ご留意ください。

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301

Member of
Deloitte Touche Tohmatsu Limited