Deloitte.
デロイト トーマツ

金融機関のサードパーティ・サイバーセキュリティリスク管理強化に関する調査

調査報告概要資料

デロイト トーマツ サイバー合同会社
2026年2月27日

目次

TPCRMに関するガイダンスについて、調査を実施

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のサイバーセキュリティリスク管理（TPCRM）について、その対応が比較的進んでいるとされる米国・EU・英国の大手銀行および大手保険会社（以降、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TPCRMへの示唆について考察する。	
調査アプローチ	米国、EU、英国金融機関のTPCRMの（1）サードパーティの分類と管理方針、（2）重要なサービスや機能等の提供が特定のサードパーティに集中することによるリスク（以降、集中リスク）、（3）サードパーティと契約後の期中のモニタリング、（4）サードパーティに対する監督権の確保・手法、（５）出口戦略・出口計画、（６）インシデント対応を主たる調査項目とし、まず、金融セクターのTPCRMに関連する各法令やガイドラインなどから関連する要素を整理した上で、次に、米国・EU・英国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。また、（７）保険代理店・ブローカーや保険商品・サービスに紐づくサードパーティなど保険業界特有のサードパーティの管理について追加項目として、調査を行った。	
調査領域	（１）サードパーティの分類と管理方針	• サードパーティの分類方法、管理対象とすべきサードパーティ • 管理すべきNthパーティの考え方、サードパーティ・NthパーティのIT資産管理 • 重要度の判定基準、重要なサードパーティの管理手法
	（２）集中リスク	• サードパーティの集中リスク • 集中リスクの測定方法
	（３）サードパーティと契約後の期中モニタリング	• サイバー脅威インテリジェンスモニタリング • 業界における質問票の共有
	（４）サードパーティに対する監督権の確保・手法	• サイバーセキュリティに係る契約書条項 • 監査権と現地調査
	（５）出口戦略・出口計画	• サードパーティの出口戦略・出口計画
	（６）インシデント対応	• サイバーインシデント発生を想定した規定類整備/体制
	（７）保険代理店の管理方針	• 保険代理店・ブローカー、保険商品に紐づくサードパーティの管理方針
調査期間	2025年6月17日から2026年2月28日 （米国、EU、英国銀行へのヒアリングは2025年9月から10月、保険会社は11月から2026年2月に実施）	

TPCRMに関するガイダンスについて、調査を実施

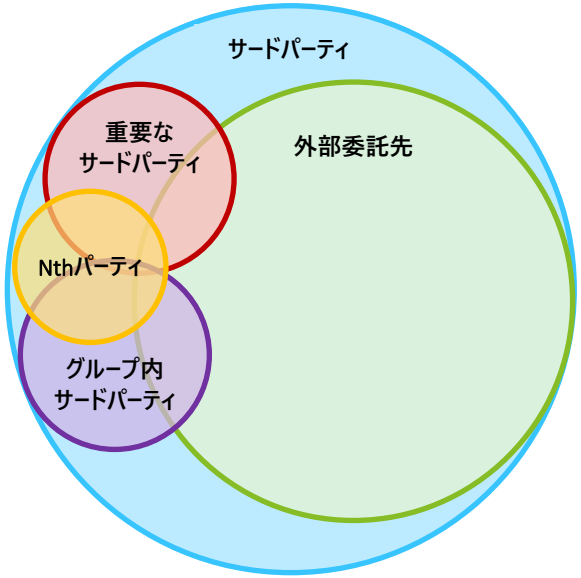
調査結果

- TPCRMの枠組みの前提として、米国、EU、英国の金融機関では、サードパーティリスク管理（TPRM）の枠組みが整備されており、サードパーティのサイバーセキュリティリスクはTPRMでカバーされるリスク領域の一つとして組み込まれている。
- TPRMの一連のプロセス（固有リスク評価・デューデリジェンス・契約・期中モニタリング・終了）を支えるプラットフォームとしてのシステムを構築して、TPRM/TPCRMを実施している。

#	調査領域	調査結果
1	サードパーティの分類と管理方針	• 固有リスク評価に基づくメリハリのある管理を実施。 • 重要なサードパーティの割合は全体数の1%-10%程度であり、重要なサードパーティを対象とした追加的管理（出口戦略・出口計画の策定、集中リスクモニタリング、現地調査等）を実施。
2	集中リスク	• オペレーショナルレジリエンスの観点で集中リスクのモニタリングを実施。 • 単一サードパーティへの集中、特定のNthパーティへの集中、地理的集中、といったカテゴリーをTPRMツールでデータ化し管理。集中度が高い場合のリスク受容可否や代替可否の判定に活用。
3	サードパーティと契約後の期中モニタリング	• サイバー脅威インテリジェンスを活用し客観性・適時性の高いモニタリングを実施。脆弱なインターネット接続機器等の適時検知により、対策の徹底が困難な中小サードパーティにおけるインシデント予防効果を見込む例も見られる。 • 不備が発見された場合に是正実施を要求、未対応の場合解約する例も見られる。
4	サードパーティに対する監督権の確保・手法	• 契約条項にサードパーティに対する監査権（現地調査権限含む）、最低限遵守すべきセキュリティコントロール要件（暗号化、アクセス権限管理、等）を明記。 • 現地調査では物理セキュリティ確認に加え、リモート調査より踏み込んだ証跡収集やプロセスの成熟度確認等を実施。
5	出口戦略・出口計画	• サードパーティのサービス終了時の対応方針や代替手段への切り替え時の移行計画を策定。実効性を高めるため定期的なテストを実施。 • 重要なサードパーティを中心に、契約・更新時に戦略・計画を策定・承認プロセスを整備。
6	インシデント対応	• サードパーティでのインシデント発生を想定した手続き（報告フロー・ネットワーク遮断・再接続などの詳細手順）を整備し、実効性を高めるため演習を実施。 • インシデント発生時は、契約担当部署とサイバーインシデント対応専門チームが協働して対応。
7	保険代理店の管理方針	• 代理店のセキュリティ評価・管理はTPRMとは別プログラムとして行う保険会社が多かったものの、TPRMへの統合（固有リスクの評価・管理基準・管理するデータベース等の統一）を検討する例、TPRMと一体で運用中の例も見られる。

各国の法令・ガイドラインでは外部委託先に限らず、金融機関の業務やビジネス上の契約等の取り決めが持つリスクを評価・識別し、適切に管理する必要があるとしている

補足：各国の法令・ガイドラインで求められるサードパーティ管理



■　サードパーティと外部委託先の定義※1

項目	定義
サードパーティ	サードパーティとは、自組織がサービスを提供するために、業務上の関係や契約等を有する他の組織をいう（例：システム子会社やベンダー等の外部委託先、クラウド等のサービス提供事業者、資金移動業者等の業務提携先、API 連携先）。
外部委託先	業務を委託している組織をいう（金融機関等が金融サービスを提供するために外部委託するシステム（共同センター等を含む）のベンダーなど。形式上、外部委託契約が結ばれていなくともその実態において外部委託と同視しうる場合や当該外部委託された業務等が海外で行われる場合も含む）。

※1：金融庁2024年10月 4 日「金融分野におけるサイバーセキュリティに関するガイドライン」より引用

■　リスクを評価・識別すべきサードパーティの分類と概要※2

項目	概要
重要なサードパーティ	提供するサービスの停止が、金融機関の業務に対して重大な影響を与えるサードパーティを指す。
Nthパーティ	サードパーティによる金融機関へのサービス提供を間接的に支援する事業者や個人を指す。重要なサービスを提供するサードパーティを支える場合は重要なNthパーティになる。
グループ内サードパーティ	金融機関グループ内でサービスを提供するサードパーティであり、親会社、姉妹会社、子会社など共通の所有・支配下にあるサードパーティを指す。

※2：Appendixに記載の文献を基に整理

米国、EU、英国の金融機関ではリスク管理上の優先事項としてTPRM/TPCRMに継続的に注力しており、以下のような取り組みを行っていることが確認された

補足：TPCRMの高度化に向けて確認された取り組み

TPRMの一部としてのTPCRMの実施	• TPCRMの枠組みの前提として、米国、EU、英国の金融機関では、サードパーティリスク管理（TPRM）の枠組みが整備されており、サードパーティのサイバーセキュリティリスクはTPRMでカバーされるリスク領域の一つとして組み込まれている。 • サードパーティリスクの専門部署の一つとしてサイバーセキュリティ部署が組み込まれ、対策を推進している • TPRM/TPCRMの体制としては、1線として契約担当部署がTPRMプログラムの対応および最終的な責任を持ちつつ、サイバーセキュリティ部門がサードパーティのサイバーセキュリティリスク評価を担当し、購買部門または2線としてのリスク管理部署がTPRM/TPCRMプログラムを監督し、それぞれが協働してTPRM/TPCRMを実行している。
テクノロジーとデータの活用	• TPRMの一連のプロセスを支えるプラットフォームとしてのシステムを構築して、TPRM/TPCRMを実施している。 • 関連するデータ（サードパーティの基本情報や取引内容に関する情報、案件ごとのリスク評価結果、指摘事項の改善状況等）も当該システム上で管理されていることから、データの分析・可視化が容易になっている。また、サードパーティの基本情報や契約情報が一元化されていることから、新たな契約を行う際のデューデリジェンスプロセスにて、サードパーティの集中状況の確認や、代替可能なサードパーティがいるかの判断など集中リスクの管理や対応も実施可能となっている。
サイバー脅威インテリジェンスの活用	• サイバーセキュリティ観点では、サイバー脅威インテリジェンスの活用が普及している。 • リスクスコアリングツール、オープンソースインテリジェンス（OSINT）、アタックサーフェスマネジメント（ASM）、ダークウェブモニタリングといった手法を活用することで、「サードパーティの回答に依拠しない客観的なリスク評価」「リスク顕在化状況のタイムリーな検知」「インシデント発生時の情報漏えい等の影響把握」等をプロアクティブに実施している。 • サードパーティ専門のサイバー脅威インテリジェンスチームを組織し、サードパーティにリスクの兆候が見られた際に深堀調査を実施しているなどの先進的な取り組みも見られた。 • なお、規程や整備されているプロセスなど統制の成熟度はサイバー脅威インテリジェンスでは判断できないため、質問票などによるリスク評価はいずれの金融機関でも実施されていた。

調査結果概要

米国、EU、英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策を考察した

（1）サードパーティの分類と管理方針

調査項目	本邦金融機関の課題仮説	調査結果	本邦金融機関における改善策の考察
サードパーティの分類方法と、管理対象とすべきサードパーティの考え方	• 従来の外部委託等に限定していた管理から範囲の拡大を検討しているが、TPCRMで管理対象とすべきサードパーティ分類の整理に悩んでいる。	• **サードパーティの分類方法**については、各社とも**サービスの重要度やリスクレベル、サービスの種類等で分類**していた。**管理対象とすべきサードパーティ**の考え方については、各社とも**すべてのサードパーティを対象**としていたが、主に米国の一部金融機関においては当局の監督下にあるサードパーティ（例えば、FMIなどの規制対象サードパーティ）も、TPRMの管理対象に含めていた。	• 分類方法は現行の購買カテゴリ分類や既存の取引データに含まれるサードパーティサービス、取引内容も活用しながら、その重要度や区分を見直し、整理する。 • リスクベースで軽重を付け、重点的に管理が必要なサードパーティにリソースを割り当てることを実現できる仕組みを検討する。
管理すべきNthパーティの考え方 **サードパーティ・NthパーティのIT資産の管理**	• 直接契約関係のない再委託先をどのように管理すべきか、海外のベストプラクティスも参考にしたい。 • サードパーティから規定類の情報提供依頼を拒否されるなど、IT資産管理に係るリスク管理状況の把握が難しい。	• **管理対象とすべきNthパーティ**は各社とも**サービスプロバイダーを対象**に、**リスクベースで判断**していた。 • 多くの金融機関がNthパーティの管理の取り組みとして、**再委託先までを可視化**し、また直接的な契約関係のないNthパーティのリスクは、**サードパーティの委託先管理能力を評価**し、間接的に低減していた。 • **サードパーティ、NthパーティのIT資産管理**は、各社ともサードパーティの**規程類の整備状況など**を確認していた。 • SBOMの利用は試験的に取組を開始している金融機関もあったが、SBOMの入手はサードパーティの協力が得られないため当局による主導を要望する金融機関もあった。	• サードパーティの委託先管理のポリシーや規程類の整備状況など、統制状況を確認する評価手続きも考慮したプロセス設計を検討する。 • IT資産管理などの規程類については、必要に応じてサイバー担当者同席のもと、規程類に加えシステムやネットワーク構成図などの具体的な資料の提出を求め、管理方針等を確認する。

米国、EU、英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策を考察した

（1）サードパーティの分類と管理方針

調査項目	本邦金融機関の課題仮説	調査結果	本邦金融機関における改善策の考察
重要度の判定基準と、重要なサードパーティの管理手法	• 重要なサードパーティの判定基準や管理手法に関する明確なガイダンスもなく、整備に悩んでいる。	• **サードパーティの重要度の判定基準**については、**主に米国では業務の固有リスク評価結果から、EUと英国では主に法規制対応の観点から判定**していた。いずれも業務が停止した場合の影響が、金融機関の業務継続に致命的な場合、重要と整理していた。 • サイバーセキュリティの観点では、例えば、サードパーティと自社のシステム/ネットワークへの接続有無を固有リスク評価の項目の1つとして確認をしていた。 • **重要なサードパーティの管理手法**については、各社とも追加的な対応として重点的なモニタリングによる深堀調査等を行っていた。	• サードパーティが担うサービスの内容、取り扱うデータの性質、およびサードパーティが提供する業務が停止した場合の業務継続に基づく重要度の判定基準を整備する。 • 重要なサードパーティに対して重点的なモニタリング等により、リスク低減されていることを継続的に監視する。

米国、EU、英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策を考察した

（2）集中リスク

調査項目	本邦金融機関の課題仮説	調査結果	本邦金融機関における改善策の考察
サードパーティの集中リスク	• TPCRMで管理すべき集中リスクの分類が定義できていない。	• **サードパーティの集中リスク**については、各社とも**オペレーショナルレジリエンスの観点で、サードパーティ集中、Nthパーティの集中、地理的集中**（サービスが提供される国、地域など）を管理していた。	• 現行の取引先マスタやデータベースを確認し、どのサードパーティや地域にサービスが依存・集中しているかの分析のための台帳・データベースを整備、最新化することが考えられる。
集中リスクの測定方法	• 何をもって集中しているかを判断するための測定方法に悩んでいる。 • サードパーティの集中リスクを限られたリソースでどのように効率的に管理・モニタリングできるか悩んでいる。	• **集中リスクの測定方法の軸**としては、**そのサードパーティや関連する特定の再委託先への総委託数や総支出金額、サービスの提供元の地域**などを対象としていた。測定軸となるサードパーティ関連データは、TPRMを実施する際に利用されるTPRMツール上に登録されているデータ（例えば、契約担当者がTPRMの対応を行う際に入力するサードパーティや契約内容に係る情報（サードパーティの住所や契約金額、サービスの提供元となる地域の情報等）など）が活用されていた。 • TPRMツールを用いて、サードパーティデータを一元管理し、ダッシュボード機能やアラート機能を実装して効率的にサードパーティの集中リスクを識別・分析していた。	• データベースを整備し、登録されている情報の正確性、網羅性が確認できたうえで、測定する集中度のカテゴリの検討を行う。 • TPRMに関するプロセスやデータの一元的な管理を実現する観点からは、TPRMツールの導入に向けた情報収集やその検討を行うことも選択肢である。

米国、EU、英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策を考察した

（２）集中リスク（調査結果の補足）

セクターレベルの集中

集中リスクの種類	概要
システミックレベルの集中リスク	• 単一または限られた数のサードパーティが提供する1つ以上のサービスへの依存から生じる金融セクター全体のリスクを指す • システミックな集中リスクは各国当局により管理されるものとしている（金融機関は、当局への情報提供をする一貫で、金融機関においてもシステミックな集中を意識すべきと示している）
金融機関レベルの集中リスク	• 金融機関が１つ以上のサービスを単一または限られた数のサードパーティに依存している状況から生じるリスクを指す • 金融機関レベルの集中リスクは、金融機関により管理されるものとしている

管理項目（例）

単一サードパーティへの集中	重要なNthパーティの集中	地理的集中
• 単一のサードパーティへの依存から生じる集中リスクであり、サードパーティがサービス停止した際に金融機関の多くの業務が影響を受ける • 測定方法：特定カテゴリに対する総支出金額、契約件数の割合、等	• 直接取引する重要なサードパーティが単一の再委託先に依存していることから生じる集中リスクであり、単一サードパーティへの集中や地理的集中と同様の影響がある • 測定方法：特定カテゴリに対する総支出金額や契約件数全体に対する特定再委託先の割合、等	• 単一の国・地域等への依存から生じる集中リスクであり、当該国・地域で自然災害、政情不安、制裁、規制変更などが発生した際に、金融機関の多くの業務が影響を受ける • 測定方法：高リスクと分類される特定の国や地域における契約数、等（例えば、サードパーティや契約内容の基本情報などに含まれる地理的情報を活用）

TPRMツールで可視化、管理

※BCBS：「Principles for the sound management of third-party risk」やBoE/PRA：「SS2/21 Outsourcing and third party risk management」を基に整理

米国、EU、英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策を考察した

（3）サードパーティと契約後の期中モニタリング（1/2）

調査項目	本邦金融機関の課題仮説	調査結果	本邦金融機関における改善策の考察
サイバー脅威インテリジェンスモニタリング	• 契約更新時および年次などの定期点検にて再評価しているが、よりタイムリーなリスクを検出するための手法について悩んでいる。 • インシデントの検知がサードパーティからの事後報告となっている。	• **サイバー脅威インテリジェンスの活用**については、サードパーティのアタックサーフェスを評価・モニタリングすることで**客観的なリスク評価とタイムリーなリスク検知**を実現していた。また**リスクスコアリングツール（アタックサーフェスマネジメント機能を含む）を活用することで業務負荷の低減**を果たしている金融機関が多くあった。ツールの活用には過検知等の観点からアウトプット情報の精査・取捨選択が必要といった声もあった。 • 重要なサードパーティに絞ってモニタリングを実施している例のほか、先進的な金融機関の事例では、**全サードパーティを対象としたモニタリング**や、**サードパーティに特化した脅威インテリジェンスチームを組織**している例も見られた。 • サイバー脅威インテリジェンスによるモニタリングは、契約前にサードパーティリスク評価時の追加的なインプットとして活用したり、契約後の継続モニタリングとしてそのサードパーティのリスクに著しい変動がないことの確認に活用していた。 • リスク予兆（脆弱なインターネット接続機器等）の適時検知により、セキュリティ対策の徹底が困難な中小TPにおけるインシデント予防にも効果を見込む例も見られた。 • モニタリングの結果不備が発見された場合は、サードパーティに是正計画の提出を求め、改善が見られない場合は契約を終了している例も見られた。	• サードパーティのリスク評価及び期中モニタリングにおいてサイバー脅威インテリジェンスの活用を検討する。 • 中小金融機関など人材や予算等の制約がある場合は、自社の保有する情報の処理を委託する先など期中モニタリングで重点的に監視するサードパーティの検討や、継続的なデューデリジェンスの再実施、サードパーティが自社に対して実施するサイバーに係る監査状況の確認、といった代替手段を検討する。

米国、EU、英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策を考察した

（３）サードパーティと契約後の期中モニタリング（2/2）

調査項目	本邦金融機関の課題仮説	調査結果	本邦金融機関における改善策の考察
業界における質問票の共有	• 変化するサイバーの外部環境に合わせたリスク評価項目の作成・見直しの効率的な手法や、多数あるサードパーティを管理するための効率的な手法や高度化の実現方法について悩んでいる。	• サードパーティのリスク評価のための質問票を各金融機関が個々に整備してリスク評価を実施することは、金融機関・サードパーティの双方に負担が発生することから、海外ではコミュニティ等の参加組織間で設計した**業界共通の質問票テンプレート**や、**業界共通のコミュニティ型プラットフォーム上で評価（調査）結果を共有する枠組み**が存在する。本調査対象となった金融機関においても、**自社で設定したリスクアペタイトと照らし合わせた上**で、業務効率化等を目的として、こうした枠組みを活用している事例も見られた。 • 業界共通の質問票テンプレートの活用方法については活用していた金融機関毎に異なり、質問項目を参考程度に参照しているケースや、業界共通の質問票テンプレートをそのまま、もしくはその質問票をベースに独自の設問項目の追加等カスタマイズして利用しているケースが確認された。 • 評価（調査）結果の共有の枠組みについては、業界共通のコミュニティ型プラットフォームに参加している他の組織が、共通の質問票を用いて実施した直近のサードパーティの評価結果について、リスクベースで活用している事例が見られた。コミュニティに参加しているが共通の質問票を利用していない金融機関においても、自社のリスク評価質問票の確認観点と整合性の高い項目のみ、他社が直近で行った評価結果を参照する場合があるといった声もあった。	• 業務効率化の観点からは、業界共通の質問票テンプレートや結果を共有する枠組みを活用することは有用と考えられる。 • ただし、サードパーティを評価する目的は「自社と同等のリスク管理がサードパーティにおいても担保されるか」を評価することにある。そのため、金融機関それぞれでリスクアペタイトを設定した上で、その範囲内で活用することが前提となる。

米国、EU、英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策を考察した

（３）サードパーティと契約後の期中モニタリング（調査結果の補足）

活用されているテクノロジー等の例

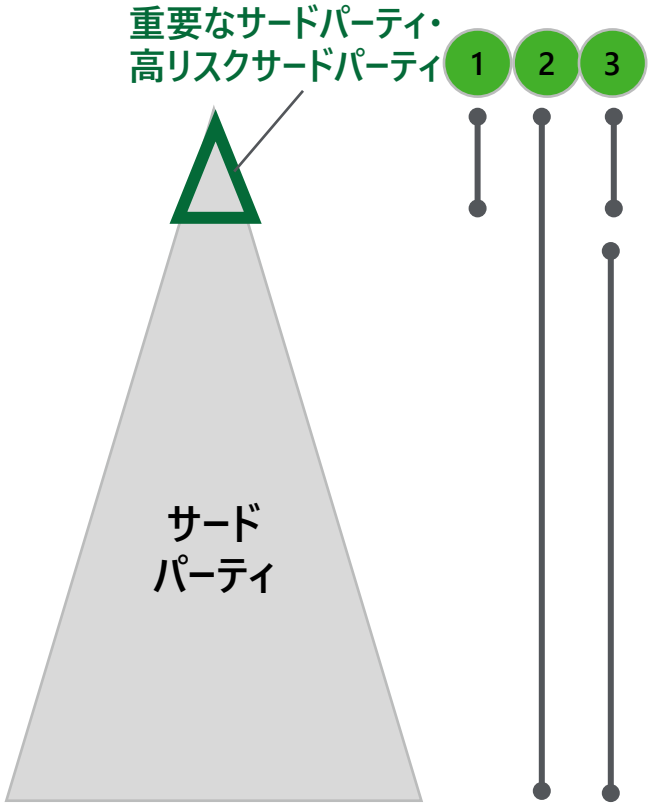
- **リスクスコアリングツール　※調査先の多くが利用**
  企業や組織のサイバーセキュリティの状態を外部から定期的に評価し、スコアやランクとして可視化するツール・サービス
- **オープンソースインテリジェンス（OSINT）**
  インターネット上の情報など、合法的に入手できる情報を調べ、組織の脆弱性や攻撃の糸口となりえる情報を収集、組み合わせて分析する調査手法
- **ダークウェブモニタリング**
  一般の検索エンジン等からはアクセスできない特定のネットワーク上に存在するウェブサイト等において、情報の流通状況や不正取引等の動向を把握するための監視・調査活動
- **アタックサーフェスマネジメント（ASM）※調査先の多くが利用**
  外部（インターネット）からアクセス可能なIT資産の情報を調査し、それらに存在する脆弱性を継続的に評価する仕組み

- デューデリジェンス時などに実施するサードパーティへの質問票への回答結果に依拠しない、客観的かつタイムリーなモニタリングを実現できる効果を重視
- リスク評価プロセスの自動化・負荷軽減・範囲拡大といった効果を期待
- モニタリング先に影響を及ぼさない方式で実施

米国、EU、英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策を考察した

（３）サードパーティと契約後の期中モニタリング（調査結果の補足）

脅威インテリジェンスの適用対象と活用例



	脅威インテリジェンスの活用対象	脅威インテリジェンスの活用例
1	重要なサードパーティ・高リスクサードパーティに限定	• リスクスコアリングツール・ASM等でモニタリングを実施 • 固有リスク評価により識別した重要なサードパーティに限定し、インシデントや重要な変更がないかをモニタリング
2	全サードパーティに同等に活用	• リスクスコアリングツール・ASM等を活用し効率化 • リスク顕在化時・インシデント識別時の深堀調査やダークウェブモニタリングには外部ベンダーに調査を委託する事例もある • ダークウェブモニタリングを全TPに実施しているケースも見られた
3	全サードパーティに活用するが重要サードパーティには重点的に活用	• 自社内のインテリジェンスチームによって直接OSINTやダークウェブモニタリング等によるモニタリングおよび深堀調査を実施 • 重要なサードパーティ以外にはリスクスコアリングツール・ASM等を活用し効率化する事例もある

米国、EU、英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策を考察した

（4）サードパーティに対する監査権の確保・手法

調査項目	本邦金融機関の課題仮説	調査結果	本邦金融機関における改善策の考察
サイバーセキュリティに係る契約条項	• サイバーセキュリティに係る契約条項を契約書等に設けられていないことから、最低限必要となるセキュリティ対策が不十分となる懸念がある。	• 各金融機関はサードパーティとの**契約に標準契約書を整備しており、その条項には関連する法令やサードパーティの義務として最低限実施すべきサイバーセキュリティの条項（例えば、データの暗号化、漏洩防止策、ネットワークセキュリティ、アクセス制御、等に関する要求事項）を設けていた。** • 契約交渉において、最低限実施すべきサイバーセキュリティの条項を**充足できない場合は、そのサードパーティとは契約しない**といった対応が見られた。 • また、取引の条件としてサードパーティに求めるコントロール条項をウェブページ上で公開しているケースも確認した。	• 現行の契約書のひな型を見直し、追加で必要な条項がないかを検討する。 • 既存サードパーティとの契約を、重要なサードパーティから順に見直しを行い、その際、サードパーティを適切に管理できる条項が無い場合は追加を検討する。 • ひな形の見直しにあわせて、既存の契約書の更新タイミングについても検討する（期中で変更、次回契約更新時のタイミング等で変更、等の方針を検討）。 • 契約条項の変更の検討や対内外向けの周知説明が可能な体制を構築する（複数部門の連携等）。
サードパーティの監査権と現地調査	• 質問票によるリスク評価や現地調査等を併用しているものの、現地調査の実施を拒むなど調整が難航するサードパーティに対する監査権の確保に向けた手法について、海外のベストプラクティスも参考にしたい。	• **サードパーティに対する監査権と現地調査**の実施権ついては、各金融機関ともサードパーティに対して**監査権を契約条項に含めて確保していた。** • 一方で現地調査については、かつては現地で直接証跡等の閲覧や観察することを重視していたものの、コロナ禍を経てリモート会議に移行し、画面投影から証跡を確認して評価を行っている金融機関も見られた。ただし、そのような場合でも物理セキュリティ等の直接確認が必要な領域は現地調査を行っていた。また、現地調査ではリモート調査より踏み込んだ証跡収集やプロセスの成熟度確認等が可能と評価する金融機関も見られた。 • 大手のクラウドサービスプロバイダーに対しては業界団体と共に共同監査を行っているケースも見られた。結果は業界団体に加盟している金融機関に共有されていた。	• 現地調査の要否については、評価すべきリスク・目的や、そのサードパーティが金融機関にとってどの程度重要か等に応じて検討する。 • クラウドなど自社では監査権の取得や行使が難しい場合は、SOC2レポートなど第三者評価など代替策の検討のほか、業界内での共同監査などの管理の枠組みを検討することも一案。

米国、EU、英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策を考察した

（5）出口戦略・出口計画

調査項目	本邦金融機関の課題仮説	調査結果	本邦金融機関における改善策の考察
サードパーティの出口戦略・出口計画	• サードパーティの出口戦略・出口計画に含めるべき内容や、それぞれの使い分け方法について明確化されていない。	• **サードパーティの出口戦略・出口計画**は、**各金融機関とも重要なサードパーティを優先して策定していた**。重要なサードパーティ以外であっても策定を求めている金融機関では、項目に記載する情報量の粒度に軽重をつけて対応していた。 • 重要なサードパーティに該当する場合は、必ず出口戦略・出口計画が策定・承認される手続きをTPRMプロセスに組み込んでいた。 • それぞれの文書の定義に統一的な基準はないものの、**サードパーティが提供するサービスの終了や中断時にどのように対応するかの基本方針を出口戦略**として策定し、**代替手段（代替案への切り替えなど）への移行手順の詳細をまとめた文書を出口計画**として策定していた • 各金融機関とも、策定した出口計画の内容については定期的な内容の見直しや机上テストを行い、発動の際の実効性を高めるための維持管理をTPRMプロセス上で実施していた。	• まずは、出口戦略・出口計画策定の対象とする自社にとって重要なサードパーティのカテゴリを整理する。 • 「戦略」と「計画」で文書を必ずしも分ける必要はないが、それぞれの要素となる対応の基本方針、移行計画の詳細など必要な項目を整理する。項目検討の際、事業継続計画（BCP）等の既存の社内文書と整合させて管理できるようにすることは一案。 • 出口計画の定期的な見直しの実施及び結果の記録等等による実効性を担保するための仕組み構築を検討する。 （例えばTPRMプロセスの期中管理）

米国、EU、英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策を考察した

（５）出口戦略・出口計画（調査結果の補足）

出口戦略	
サードパーティが提供するサービスの終了もしくは中断時に、金融機関がどう対応するかの基本方針や全般をまとめた文書	• 発動条件（例：サードパーティの倒産、サイバーインシデント発生、等） • 社内外連絡先 • サードパーティに依存しているサービスの終了・継続（代替案判断方針 • 代替案への切り替え方針（内製化、代替先への切り替え） • 代替先業者リスト　などを含む

出口計画	
金融機関が業務やサービスを維持できるようにするための移行計画の詳細をまとめた文書	• 代替案への切り替えスケジュール • 代替案への切り替えにおける役割と責任、リソース • 代替案への移行コスト • 社内外のコミュニケーション戦略 • 代替先とのインターオペラビリティ • 移行手順 • データの返却・廃棄手順　などを含む

※FSB：「Enhancing Third-Party Risk Management and Oversight – A toolkit for financial institutions and financial authorities」やインタビュー結果を基に整理

米国、EU、英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策を考察した

（6）インシデント対応

調査項目	本邦金融機関の課題仮説	調査結果	本邦金融機関における改善策の考察
サイバーインシデント発生を想定した規定類整備/体制	• サードパーティにサイバーインシデントが発生した際、対応する部署が不明確で対応に遅れが生じてしまう懸念がある。 • 契約担当は1線であるものの、サイバーセキュリティ部門に対応が集中することで、平時の活動やリソースへの影響が懸念される。	• 各金融機関ともサードパーティにサイバーインシデントが発生した際の報告フローなどの**インシデント発生時の対応計画や具体的な対応手順（ネットワークの遮断の手続きや再接続の際のリスク評価など）**が整備されていた。 • インシデント発生時には、契約を所管する**契約担当部署とサイバーインシデント対応チームが協働**し対応する体制となっていた。また、サードパーティーの類型に依拠せず、自社とシステム・ネットワーク接続されているサードパーティに対しては、インシデント発生時にネットワーク遮断など必要な手続きが実施可能な体制を整備しているケースも見られた。 • また、インシデント発生時の実効性を高めるため、**重要なサードパーティと共同訓練を実施**しているケースも見られた • 各金融機関とも、金融市場インフラ（FMI）などは主に業界団体が主催する訓練に参加していた。	• サードパーティのインシデント発生を想定したインシデント対応計画の策定や具体的な対応手順を整備する。 • 上記の実効性を高めるため、定期的に自社での机上訓練を実施する（サードパーティの契約窓口となる契約担当部署も含めた演習の実施）。 • 重要なサードパーティの特定と、共同での演習実施の検討する。

米国、EU、英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策を考察した

（６）インシデント対応（調査結果の補足）

サイバーインシデント対応		
平時の運用	サイバーインシデント発生時の対応計画や手順の整備	➢ サイバーインシデント発生時の対応計画に含まれる項目例は以下の通り • サードパーティにサイバーインシデントが発生した場合の報告フロー • 当局へのエスカレーションフロー • インシデントの原因と漏洩した情報の確認結果を含む報告手順 • 代替先、および代替先への切り替え方法、承認プロセス（サイバーコンティンジェンシープラン対応） • ネットワーク再接続条件および手順
	サードパーティとの共同訓練	➢ サイバーインシデント対応計画を基に少なくとも年次で机上演習などを実施 ➢ 重要なサードパーティ等と共同訓練を実施 ➢ FMIなどは自社での訓練企画および実施ではなく、業界団体などが主催する訓練に参加
有事の運用	インシデント発生時の対応	➢ インシデント発生時は、契約の担当となる部門がサードパーティとの対応窓口を担当 ➢ 契約書には、サードパーティからのサイバーインシデント発生時の通知義務等を明記 ➢ サイバーインシデントレスポンスチームは、脅威インテリジェンスの活動によるサイバーインシデントの早期検知や、専門家としての知見を提供 ➢ 契約担当部署とサイバーインシデントレスポンスチームが協働して対応

米国、EU、英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策を考察した

（7）保険会社の代理店・ブローカーの管理方針

調査項目	本邦金融機関の課題仮説	調査結果	本邦金融機関における改善策の考察
代理店・ブローカーの管理方針	• 代理店・ブローカーは過去から管理プログラムを策定し点検を実施しているものの、サイバー脅威が広がっている動向から、代理店・ブローカーや保険商品に付帯するサービス提供先などが重要情報などを保持しており、リスク管理に悩んでいる。	• 代理店・ブローカは、**TPRMとは別のプログラムで管理している事例が多く見られた。**海外では商習慣の違いから代理店・ブローカーは仲介機能を中心とした取引のため、**代理店・ブローカーは保険契約者の情報を保持しておらず固有リスクを「低」と評価**するケースが多く見られた。 • 一方、**保険の更新などで保険契約者の情報にアクセスする代理店・ブローカーも一部存在し、**このような場合はTPRMとは別プログラムであるものの、**代理店・ブローカーのセキュリティ対策についても保険会社による評価・管理が行われていた。**先進的な事例では、サイバー脅威インテリジェンスによるモニタリングやTPRMの管理範囲を代理店・ブローカーにも拡大（固有リスクの評価、TPRMの管理データベースによる管理、等）している事例も見られた。 • **契約管理や保険金支払いなどを行うTPA（Third Party Administrator）は、TPRMの枠組み**で管理する保険会社もみられた。**ブローカーはTPRMのスコープに含めるか検討中**といった事例も存在していた。	• 管理対象も多数になることが想定されるため、海外の保険会社の例のように固有リスクを評価することでリスクベースで軽重を付け、重点的に管理が必要なサードパーティ等にリソースを割り当てることを実現できる仕組みを検討する。（TPRMの取り組みを部分的に代理店・ブローカーの管理に拡大することを検討する） • リアルタイムにサイバー脅威のリスクを把握することは従来の質問票による評価だけでは対象数も多く難しいことが想定されるため、サイバー脅威インテリジェンスの活用を検討する。
保険商品に付随するサービスの提供先の管理方針		• 医療のセカンドオピニオンの提供など**保険商品に付随するサービスプロバイダーは、保険会社により対応が分かれた。**保険会社はサービスプロバイダーに仲介をするのみに留まり、保険契約者が直接サービスプロバイダーに連絡をすることから、**管理の対象外としているケース**も見られた。一方、保険契約者に仲介することでサービス提供会社が自社の契約者の情報を扱うことから、**TPRMの枠組みで管理するケース**も見られた。 • IoT機器（カメラ）から収集したデータをサードパーティが処理する場合に、TPRMと同様の管理していたケースが見られた。個人情報保護の観点から、自社データセンターへの管理に移行していた。	• 保険商品に付随するサービスプロバイダー（例えば、カメラなどのIoTデバイスなどをそのサードパーティが提供し、かつ、機器から収集した情報をサードパーティが処理する場合などのケース）は、扱う情報や自社、サードパーティ、契約者との関係性を鑑みて、管理方針を検討する。

Appendix

調査対象の各法令・ガイドライン等の一覧

No	文書名	発行機関	管轄・区分	概要
1	Consultative Document Principles for the sound management of third-party risk	• バーゼル銀行監督委員会（BCBS/Basel Committee on Banking Supervision）	国際機関	✓ 銀行、監督当局向けに、銀行業界におけるサードパーティリスクの健全な管理のための原則を示した協議文書である。
2	Enhancing Third-Party Risk Management and Oversight A toolkit for financial institutions and financial authorities	• 金融安定理事会（FSB/Financial Stability Board）	国際機関	✓ 金融当局、金融機関、サービスプロバイダー向けのサードパーティリスク管理、監督のためのツールキットである。
3	FCA Handbook - SYSC 8 Outsourcing	• 英国金融行為規制機構（FCA/Financial Conduct Authority）	英国当局	✓ 英国金融行為規制機構の法令やその他の規定などをまとめたFCAハンドブック（手引き）の中の「SYSC/Senior Management Arrangements, Systems and Controls」を構成するセクションの一つである。本セクションでは、金融機関（銀行、証券会社、投資会社など）がアウトソーシングなどの体制をどのように設計・運用すべきかを規定している。
4	Supervisory Statement | SS2/21 Outsourcing and third party risk management	• イングランド銀行（BoE/Bank of England） • 健全性規制機構（PRA/Prudential Regulation Authority）	英国当局	✓ 金融機関が、アウトソーシングおよびサードパーティリスク管理に関連する規制要件・期待事項をどのように遵守すべきかについて、健全性規制機構の期待事項が示された文書である。
5	Supervisory statement | SS6/24 Operational resilience: Critical third parties to the UK financial sector	• 英国金融行為規制機構（FCA/Financial Conduct Authority） • イングランド銀行（BoE/Bank of England） • 健全性規制機構（PRA/Prudential Regulation Authority）	英国当局	✓ 重要なサードパーティが金融サービス・市場法2000（Financial Services and Markets Act 2000 (FSMA) as amended）および規制当局の規則により課された義務および責任をどのように遵守すべきかについて、規制当局の期待を示した文書である。

調査対象の各法令・ガイドライン等の一覧

No	文書名	発行機関	管轄・区分	概要
6	Final Report on EBA Guidelines on outsourcing arrangements	• 欧州銀行監督機構（EBA/European Banking Authority）	欧州当局	✓ 欧州銀行監督機構の権限範囲に含まれる全ての金融機関に対して、アウトソーシングの取決めに関するガバナンス体制や、関連する管理上の期待・プロセスに関して規定している文書である。
7	Consultation Paper on EBA Draft Guidelines on the sound management of third-party risk			✓ EBAの「Guidelines on outsourcing arrangement」からの更新版として策定されており、アウトソーシング契約に限定せず、より広域なサードパーティとの契約等に関する、金融機関や所管当局が実施すべきリスク管理の手法や基準、役割などを示している文書である。
8	Digital Operational Resilience Act (DORA)	• 欧州委員会（European Commission） • 欧州議会（European Parliament） • EU理事会（Council of the European Union）	欧州政策決定機関	✓ EUの各法令で個別に扱われてきたICTリスクに関する要件を統合し、金融機関のデジタル・レジリエンスを強化することを目指して導入された法令である。ICTリスク管理能力、インシデント報告、オペレーショナルレジリエンステスト、ICTサードパーティリスクの監視などのルールを定めている。
9	Interagency Guidance on Third-Party Relationships: Risk Management	• 米国連邦準備制度理事会（FRB/Board of Governors of the Federal Reserve） • 連邦預金保険公（FDIC/Federal Deposit Insurance Corporation） • 通貨監督局（OCC/Office of the Comptroller of the Currency）	米国当局	✓ 銀行組織に向けた、サードパーティとの関係に関するリスク管理のガイダンスである。リスク管理を実施するための基本原則や考慮事項、サードパーティリスク管理のライフサイクルの各段階において必要となる活動や考慮事項、組織的な監視体制と責任、当局による監督のフレームワークについて示している。
10	Third-Party Risk Management A Guide for Community Banks			✓ 「Interagency Guidance on Third-Party Relationships: Risk Management」を基に中小銀行（コミュニティバンク）向けに作成されたガイダンスである。

調査対象の各法令・ガイドライン等の一覧

No	文書名	発行機関	管轄・区分	概要
11	Solvency ii Directive	• 欧州議会（European Parliament） • EU理事会（Council of the European Union）	欧州政策決定機関	✓ 欧州議会（European Parliament）、欧州理事会（European Council）による、EUにおける保険会社および再保険会社のための健全性規制である。本規制は保険契約者や受益者が十分に保護されることを目的としており、EU内の保険会社および再保険会社に適用されるさまざまな要件を定めている。
12	Draft Application Paper on operational resilience objectives and toolkit	• 保険監督者国際機構（IAIS）	国際機関	✓ 保険会社向けのオペレーショナルレジリエンスの目標とそれを支援するプラクティスやツールキットに関するガイダンスである。具体的には、オペレーショナルレジリエンス・ガバナンス・オペレーショナルリスクの関係性、オペレーショナルレジリエンスを推進するための重要な要素および保健会社の監督の目標について示す構成となっている。
13	NAIC Insurance Data Security Model Law	• 全米保険監督官協会（NAIC）	米国当局	✓ 米国各州の保険局から認可を受けている保険会社等への情報セキュリティプログラムの策定などに関する州レベルの法律のモデル法である。具体的には、情報セキュリティプログラムの策定・実施、サイバーセキュリティイベント発生時の調査、州保健委員への通知、保険委員の監督権限などについて示す構成となっている。
14	Industry Letter：Guidance on Managing Risks Related to Third-Party Service Providers	• ニューヨーク州金融機関サービス局（NYDFS）	米国当局	✓ ニューヨーク州金融サービス局の監督下にある銀行や保険会社などの金融機関宛てに、新たに規制要件を課すものではなく、サードパーティサービスプロバイダーの利用に伴うサイバーリスクの適切な管理のために、サイバーセキュリティ規則（23 NYCRR Part 500）のSection500.11の遵守を推進することを目的としベストプラクティスを例示したガイダンスである。

各法令・ガイドラインで確認した内容サマリ

サードパーティと契約後の期中モニタリング

項目	概要
期中モニタリングのプロセスに求められる内容	■ サードパーティとの契約などの取り決めに即したサービス提供能力のパフォーマンスやリスクの継続的評価・監視の実施 ■ 取締役会や経営陣への定期的な報告、および重要な問題の識別やインシデントが発生した際の上位者への報告・対応プロセスの構築 ■ 重要なサードパーティとの取り決めに対しては、より包括的で頻度の高いモニタリングの実施
期中モニタリングの実施項目の例	■ サードパーティのパフォーマンス（サードパーティの業務遂行状況やSLAの履行状況など）および重要な問題や懸念事項の発生状況の確認 例：重大または繰り返し発生する指摘事項、財務状況の悪化、データ損失・漏洩、　サービス中断といったインシデントや、コンプライアンス違反、集中、その他リスクの顕在化を示す指標のモニタリング ■ 定期的な訪問やサードパーティの担当者との会議を通じたパフォーマンスおよび運用上の課題に関する議論 ■ データ及び情報の可用性、完全性、機密性が確保されていることの確認

各法令・ガイドラインで確認した内容サマリ

サードパーティに対する監査権

項目	概要
金融機関の 契約条項に含める 監査権の例	■ サードパーティへの監査権や情報取得権、サービスプロバイダーの関連施設（本社や業務センター）、業務提供に使用される機器等（システム、ネットワーク、データ）へのアクセス権 ■ サービスのパフォーマンス指標やKPI ■ 重要サービスに関する正確な情報を金融機関が適時に受け取る権利 （例：インシデントやサービス内容、重要な変更に関する情報など） ■ オペレーショナルレジリエンスに関する条項 （例：事業継続、緊急時対応計画、最大停止時間、目標復旧時間（RTO）、目標復旧時点（RPO）） ■ コンプライアンス違反、法執行措置、規制手続き、金融機関や顧客に重大なリスクをもたらす事象が発生した際の金融機関への通知義務 ■ 合併、買収、事業売却、主要な人員の変更、関与する活動に影響を及ぼす可能性のある重要な変更に関する通知義務 ■ サードパーティから受領する報告書の種類と頻度 （例：業務報告書、財務報告書、セキュリティ報告書、統制評価結果など） ■ 継続的なモニタリングの権利 ■ 再委託先への再委託を規定する条件
監督当局による 金融機関のサードパーティ 管理状況の確認事項の 例	■ 金融機関の経営陣がサードパーティとの関係を管理する能力の評価 ■ サードパーティとの関係が金融機関のリスク特性や財務・事業運営の主要側面（関連法令・規制の遵守を含む）に与える影響の評価 ■ サードパーティとの取引・業務内容のテスト・検査（取引テスト・トランザクションテスト）の実施、または金融機関が実施したテスト結果・関連法令・規制の遵守状況の評価結果のレビュー ■ 必要に応じた金融機関のリスク管理プロセスにおける重大なリスクや不備に関する経営陣や取締役会との協議、指摘状況の評価 ■ 特に重要な活動を伴うサードパーティの監査に関連した不備について、金融機関が適切かつ持続可能な是正策を策定しているかの評価 ■ 金融機関が、関連するすべてのリスクを特定し、管理しているかどうかの評価 ■ 金融機関が、アウトソーシングの契約などの取り決めに関して、利益相反を特定し、評価し、適切に管理しているかどうかの評価

用語集

	用語	概要
1	期中モニタリング	サードパーティとの契約期間中に、サービス提供状況やリスクの変化を継続的に監視・評価する活動。
2	サイバー脅威インテリジェンスモニタリング	サイバー攻撃における動向と技術を調査し対策につなげることを目的に、情報を収集し、組み合わせて分析する調査手法のこと。
3	固有リスク評価	サードパーティが提供するサービス・業務に内在するリスク（例：機密データ取扱、システム接続状況等）を評価すること。リスクベース管理の起点となる。
4	FMI（Financial Market Infrastructure）	証券取引所、決済機関等、金融システムの基盤となるインフラ。TPRMの対象外とされる場合もある。
5	SBOM（Software Bill of Material）	ソフトウェア部品表。ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リスト。
6	オペレーショナルレジリエンス	金融機関が外部・内部のショック（サイバー攻撃、自然災害等）に対して業務継続性を確保できる能力。
7	デューデリジェンス	サードパーティ選定時に、財務状況、サービス内容、リスク管理能力等を調査・評価する活動。
8	BCP（Business Continuity Planning）	事業継続計画。サードパーティ障害時等に業務継続性を確保するための計画・体制。
9	システミックリスク	金融セクター全体や社会経済に重大な影響を及ぼし得るリスク。例えば、複数金融機関が依存している重要なサードパーティの障害等による金融システム全体への影響等。
10	SLA（Service Level Agreement）	サードパーティとの契約において定めるサービス品質・可用性等の基準・合意事項。
11	KPI（Key Performance Indicator）	企業や組織が目標を達成するために、その進捗状況や成果を定量的に測定・評価する指標

Deloitte.
デロイト トーマツ

本件調査は、米国、EU、英国大手銀行および大手保険会社における先進的な取り組みを抽出し、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。調査対象先の多くは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銀行および保険会社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

IS/BCMSそれぞれの認証範囲はこちらをご覧ください
http://www.bsigroup.com/clientDirectory

Member of
Deloitte Touche Tohmatsu Limited