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
報告書

デロイトトーマツサイバー合同会社

2023年11月30日

目次

エグゼクティブサマリ

金融機関のサードパーティ関係が多様化し、ICT[1]サプライチェーン[2]が複雑化している中で、サードパーティによるサイバーインシデントが増加し、ICT サプライチェーン内の脆弱性も明らかになるなどのサードパーティ・サプライチェーンに起因したサイバー攻撃の脅威が増大している。こうした状況から、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[3]/C-SCRM[4]）の重要性が高まっていることを踏まえ、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、本邦金融機関におけるリスク管理などへの示唆について考察した。

調査の結果、米国の大手金融機関は、最近のサイバー攻撃がサードパーティ・サプライチェーンを標的とする傾向があることを踏まえ、TPCRM/C-SCRM に特別な注意を払っており、以下のように、先進事例と認められる対策を推進していることが分かった。

- 組織体制について、TPCRM を専門に担当するチームまたは要員が 1 線部門内に存在し、利用部門である業務部門を牽制する 1.5 線的な役割を果たしている金融機関がある。また、2 線部門でも、オペレーショナルリスク部門に TPCRM の専任者が存在し、1 線部門のリスク評価に場合によっては異議を唱え、または介入するなどの牽制の仕組みが整備されている。このように、米国大手金融機関においては、1 線及び 2 線において牽制機能があるなどの組織的に TPCRM を行うための仕組みがある。
- 人的リソースについて、数千社のサードパーティを管理するために、TPCRM 部門には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、サイバーリスク評価に特化し効率的に業務経験を積ませ、社内トレーニングやメンター制度の活用なども合わせて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。
- リスク管理プロセスについて、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注力する継続的モニタリングを行っている。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。
- 自社が使用するソフトウェアの脆弱性は自社で確認するとの方針の下、技術的評価を実施するチームを持ち、評価を実施している。ソースコードレビューやソフトウェア構成解析（SCA）[5]

---

1 Information and Communication Technology の略。

2 前掲書脚注 1 で「組織が自身の業務を支えるために用いる ICT エコシステムを形成する、サードパーティ間の相互の結び付きからなる。ICT サプライチェーンには、すべての製品、サービス及びインフラに加え、それらの提供者、供給者及び製造業者も含まれる」と定義している。

3 Third Party Cyber Risk Management の略。

4 Cyber Supply Chain Risk Management の略。サイバーリスクに限定されないサードパーティリスク管理は Third Party Risk Management の略である TPRM を使用。

5 Software Composition Analysis の略。ソフトウェアを分析して組込まれているオープンソースソフトウェア（OSS）を検出し、そこに含まれている脆弱性やライセンスの問題などを検出する手法。

などの技術的に可能な手法を積極的に採用し、高度化を進める取組みが認められる。
・ 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）[6]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。

[6] Unified Extensible Firmware Interface（Basic Input/Output System）の略。

I. イントロダクション

1. 調査の背景、目的

国内外で金融機関のサードパーティが多様化・複層化するとともに、ICT サプライチェーンが複雑化している。こうした状況の下、近年、サードパーティに起因するサイバーインシデントが発生し、また、ICT サプライチェーンに内在する深刻な脆弱性が公表されている。このように、サードパーティ・サプライチェーンに対するサイバー攻撃の脅威が増大している。

例えば、我が国において、医療機関が外部委託先を介して侵入されランサムウェア攻撃を受け、基幹システムの復旧まで 1 か月以上を要し、診療にも重大な影響が及んだ事案が発生した[7]。また、金融セクターでも、金融機関が利用するサードパーティに起因するインシデント、また、外部委託先以外にも事業連携先を介したインシデントなどが認められている[8]。

このため、金融機関には、従来の外部委託先管理プロセスの対象である先に限らず、サービス連携先などを含めたサードパーティ全般[9]のサイバーリスクへの対応を強化し、同時に、ソフトウェア・ハードウェアの調達先やその構成要素などの ICT サプライチェーンに内在するサイバーリスクに対応することが求められている。

しかし、現実には、重大な脆弱性が公表された場合のリスクや脅威の度合い（サードパーティ・サプライチェーンにおける影響の有無、影響の範囲、影響の程度など）の判定は容易ではなく、そのため、インシデントが発生した場合の対処も難しい課題となっている。これは、我が国だけではなく、G7 サイバー・エキスパート・グループ（CEG）が 2022 年 10 月に公表した「金融セクターにおけるサードパーティのサイバーリスクマネジメントに関する G7 の基礎的要素」（G7 基礎的要素）[10]で取り上げているように、国際的にも関心が高まっている課題である。

こうした状況を踏まえ、本調査では、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の管理（TPCRM/C-SCRM）について、どのように従来の外部委託先管理の範囲を拡張し、サードパーティ及び ICT サプライチェーンのサイバーリスクに対応しているか、といった点につき、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、我が国（特に本邦金融機関におけるリスク管理と金融監督当局におけるモニタリング）への示唆を得ることを目的とする。

---

7 地方独立行政法人大阪府立病院機構大阪急性期・総合医療センター「情報セキュリティインシデント調査委員会報告書について」（2023 年 3 月 28 日、https://www.gh.opho.jp/important/785.html）

8 金融機関の事業連携先に起因して被害が発生した事例として、株式会社ドコモ（「ドコモ口座を利用した不正利用についてのお問い合わせ窓口設置について」（2020 年 9 月 11 日、https://www.docomo.ne.jp/info/notice/page/200911_00.html））、不正アクセスにより、外部委託業者から顧客情報が漏えいした事例として、チューリッヒ保険会社（「個人情報漏えいに関するお詫びとご報告」（2023 年 1 月 27 日、https://www.zurich.co.jp/customerdata/））やアフラック生命保険株式会社（「個人情報流出に関する再発防止策について」（2023 年 7 月 10 日、https://www.aflac.co.jp/news_pdf/20230710.pdf）などがある。

9 例えば、外部委託先のほか、IT 製品購買先、クラウドサービス事業者、サービス提携先（カード、決済サービス業者など）、関連子会社などを含む。

10 前掲書脚注 1

2. 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など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。

調査期間は 2023 年 6 月 16 日から 11 月 30 日である。

3. 免責事項

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ある。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ある。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いるが、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、留意されたい。

本報告書は、金融庁と当社との間で締結された、2023 年 6 月 16 日付け業務委託契約書に基づいて実施した調査研究の結果を報告するものであり、保証業務として実施したものではない。内容の採否や使用方法については本調査報告書の読者自らの責任で判断を行うものとする。

本調査報告書に記載されている情報は、調査時点のものであり、公開情報を除き、調査対象先から提出を受けた情報を基礎としている。これら入手した情報自体の妥当性・正確性については、当社で責任を持たないものとする。

II. 既存のガイダンス、文献

1. サードパーティ・サプライチェーンサイバーリスクに関するガイダンス

米国大手金融機関における管理手法に関する調査項目を抽出するため、既存のガイダンスや文献において要求、推奨される管理の範囲や内容について調査を行った。ここでは、サードパーティ・サプライチェーンサイバーリスクに関連する、各国当局、国際機関などが発行するガイダンスを紹介する。[11]

金融セクターの TPCRM/C-SCRM に関連するものとしては下記のものが挙げられる。

a. G7 CEG は、「金融セクターにおけるサードパーティのサイバーリスクマネジメントに関する G7 の基礎的要素」[12]において金融機関、金融当局及びサードパーティ向けのガイダンスを提供している。
b. 米国ニューヨーク州金融サービス局は、「金融サービス会社向けのサイバーセキュリティ要件」[13]において、金融機関がサードパーティサービスプロバイダに対して遵守すべきリスク管理の要件を設けている。

金融セクター向けではない一般的なガイダンスとしては、下記のものが挙げられる。

c. 欧州ネットワーク・情報セキュリティ機関（ENISA）は、「サプライチェーン・サイバーセキュリティのための優れた取組み」[14]において、サプライチェーン（サプライヤーとサービスプロバイダ）のリスク管理、脆弱性管理などの取組みのガイドラインを提供している。
d. ソフトウェアサプライチェーンについては、米国国立標準技術研究所（NIST）が「大統領令 14028 セクション 4e に基づくソフトウェアサプライチェーンセキュリティのガイダンス」[15]を発行しており、ファームウェア、OS、アプリケーション及びサービスを対象に、米国連邦政府機関にソフトウェアを納入する開発業者が遵守すべき要件を提示している[16]。この中で参照

---

[11] サードパーティ・サプライチェーンリスクに限らず、金融機関が参照すべきサイバーセキュリティに関する基準・ガイドラインについては、十川基「金融機関における戦略的なサイバーセキュリティ対策の計画立案・推進に関する考察」（金融庁金融研究センターディスカッションペーパーDP2022-4、2022 年 7 月、https://www.fsa.go.jp/frtc/seika/R4.html#DP2022-4）が各基準・ガイドライン・フレームワークなどの特徴を整理している。

[12] 前掲書脚注 1。G7CEG は、2022 年 10 月に G7 基礎的要素を改定し、全体の内容を見直す中で ICT サプライチェーンに関する内容も追加している。

[13] New York State Department of Financial Services, *Cybersecurity Requirements for Financial Services Companies*, March 1, 2017, https://www.governor.ny.gov/sites/default/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23NYCRR500.pdf.

[14] European Union Agency for Cybersecurity (ENISA), *Good Practices for Supply Chain Cybersecurity*, June 13, 2023, https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity.

[15] National Institute of Standards and Technology (NIST), *Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e*, February 4, 2022, https://csrc.nist.gov/pubs/other/2022/02/04/software-supply-chain-security-guidance-eo-14028-s/final.

[16] 最終的には連邦政府機関を対象とするが、民間部門においても利用可能と言及されている。NIST, *Improving the Nation's Cybersecurity: NIST's Responsibilities Under the May 2021 Executive Order*, July 11, 2022, https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity.

されているソフトウェア開発実務におけるリスク管理のガイダンスとして、NIST SP800-161 Rev.1「連邦政府情報システムと組織のためのサイバーセキュリティサプライチェーンリスク管理の慣行」[17]がある。

e. ファームウェアの不正な変更を防止するための技術的なガイドライン及び推奨事項を提供している文書として NIST SP800-147「BIOS 保護ガイドライン」[18]、改ざん保護、検出、復旧機能を含めたものとして、NIST SP800-193「プラットフォームファームウェアのレジリエンスに関するガイドライン」[19]がある。また、部品やファームウェアの出所と完全性の検証を可能にする「プラットフォーム証明書」が TCG（Trusted Computing Group）で定義され、NIST SP1800-34「コンピューティングデバイスの完全性検証」[20]でそのユースケースが示されている。

f. ハードウェア管理については、米国国土安全保障省のサイバーセキュリティ・社会基盤安全保障庁が「ベンダーSCRM テンプレート」[21]において、サプライヤーの製品提供ライフサイクル、サプライチェーンの完全性やレジリエンスのリスク管理について論じているほか、ハードウェア部品表（HBOM）に関するガイドライン[22]も発行している。

g. ENISA は「調達のための必須セキュリティ要件」[23]を発行し、製品のライフサイクルを通じた正当性、完全性の確保について、サプライヤーが情報提供することについて言及している。

また、必ずしもサイバーセキュリティに焦点を当てているわけではないが、金融セクターのサードパーティリスク管理（TPRM）について取り上げたものとして下記が挙げられる。

h. 金融安定理事会「サードパーティリスクの管理とオーバーサイトの向上：金融機関と金融当局のためのツールキット―市中協議文書」[24]

i. 米国通貨監督庁ほか「サードパーティとの関係に関する省庁間ガイダンス：リスク管理」[25]

---

[17] NIST, *SP 800-161 Rev.1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, May 2022, https://doi.org/10.6028/NIST.SP.800-161r1.

[18] NIST, *SP 800-147, BIOS Protection Guidelines*, April 2011, https://doi.org/10.6028/NIST.SP.800-147.

[19] NIST, *SP 800-193, Platform Firmware Resiliency Guidelines*, May 2018, https://doi.org/10.6028/NIST.SP.800-193.

[20] NIST, *SP 1800-34, Validating the Integrity of Computing Devices*, December 2022, https://doi.org/10.6028/NIST.SP.1800-34.

[21] Cybersecurity & Infrastructure Security Agency (CISA), *ICT SCRM Task Force Vendor Template*, April 12, 2021, https://www.cisa.gov/resources-tools/resources/ict-scrm-task-force-vendor-template.

[22] CISA, *Hardware Bill of Materials (HBOM) Framework for Supply Chain Risk Management*, September 25, 2023, https://www.cisa.gov/resources-tools/resources/hardware-bill-materials-hbom-framework-supply-chain-risk-management.

[23] ENISA, *Indispensable Baseline Security Requirements for the Procurement of Secure ICT Products and Services*, January 21, 2017, https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services.

[24] Financial Stability Board, *Enhancing Third-Party Risk Management and Oversight: A Toolkit for Financial Institutions and Financial Authorities Consultative Document*, June 22, 2023, https://www.fsb.org/2023/06/enhancing-third-party-risk-management-and-oversight-a-toolkit-for-financial-institutions-and-financial-authorities-consultative-document/.

[25] The Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Department of the Treasury, *Interagency Guidance on Third-Party Relationships: Risk Management*, June 9, 2023, https://www.federalregister.gov/documents/2023/0/09/2023-

j. 英国健全性規制機構「SS2/21 アウトソーシングとサードパーティリスク管理」[26]

これらの文書は TPRM プロセスにおける考慮事項を示しており、G7 基礎的要素（特に、要素 2 サードパーティのサイバーリスクに対するリスクマネジメントプロセス）にも共通点がみられる（II.3 参照）。

2. サードパーティ・サプライチェーンサイバーリスク管理のスコープ

先に述べたとおり、本件調査におけるサードパーティ・サプライチェーンの定義は G7 基礎的要素によるが、このうち「サードパーティ」は、いわゆる業務委託やアウトソーシングといった形態だけではなく、例えば、金融機関がサービスの利用者としてサービスの提供を受ける相手方、IT サービスの提供を受けて業務上の連携を行う相手方、購買先、調達先なども含まれ得る。業務委託はサードパーティの代表的形態ではあるが、委託契約以外の契約のある先や、報酬のないサードパーティも存在し得る。また、金融機関に物、サービスを提供する子会社や関連会社も含まれる。

さらに、金融機関にサイバーリスクをもたらすものとしては、いわゆる再委託先など、サードパーティとの関係と同様に連なる関係を構成する先（4th パーティ及びそれ以降の先）、ICT によって構成されるネットワークや一体となってサービスを提供するシステム及びそれらのサプライヤーといった要素も考慮に入れる必要があり、これらの要素により ICT サプライチェーンが構成される。

これらを踏まえて金融機関におけるサードパーティ・サプライチェーンの範囲を例示すると、下記図 1 のようになる。4th パーティ以降にも連なるサードパーティサービス関係、それぞれの組織が利用する ICT インフラ、それらを構成する ICT 機器、そのサプライヤーを含めて ICT サプライチェーンが構成される。

12340/interagency-guidance-on-third-party-relationships-risk-management.

[26] Prudential Regulation Authority, *Supervisory Statement, SS2/21 Outsourcing and Third Party Risk Management*, March 2021, https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss221-march-21.pdf.

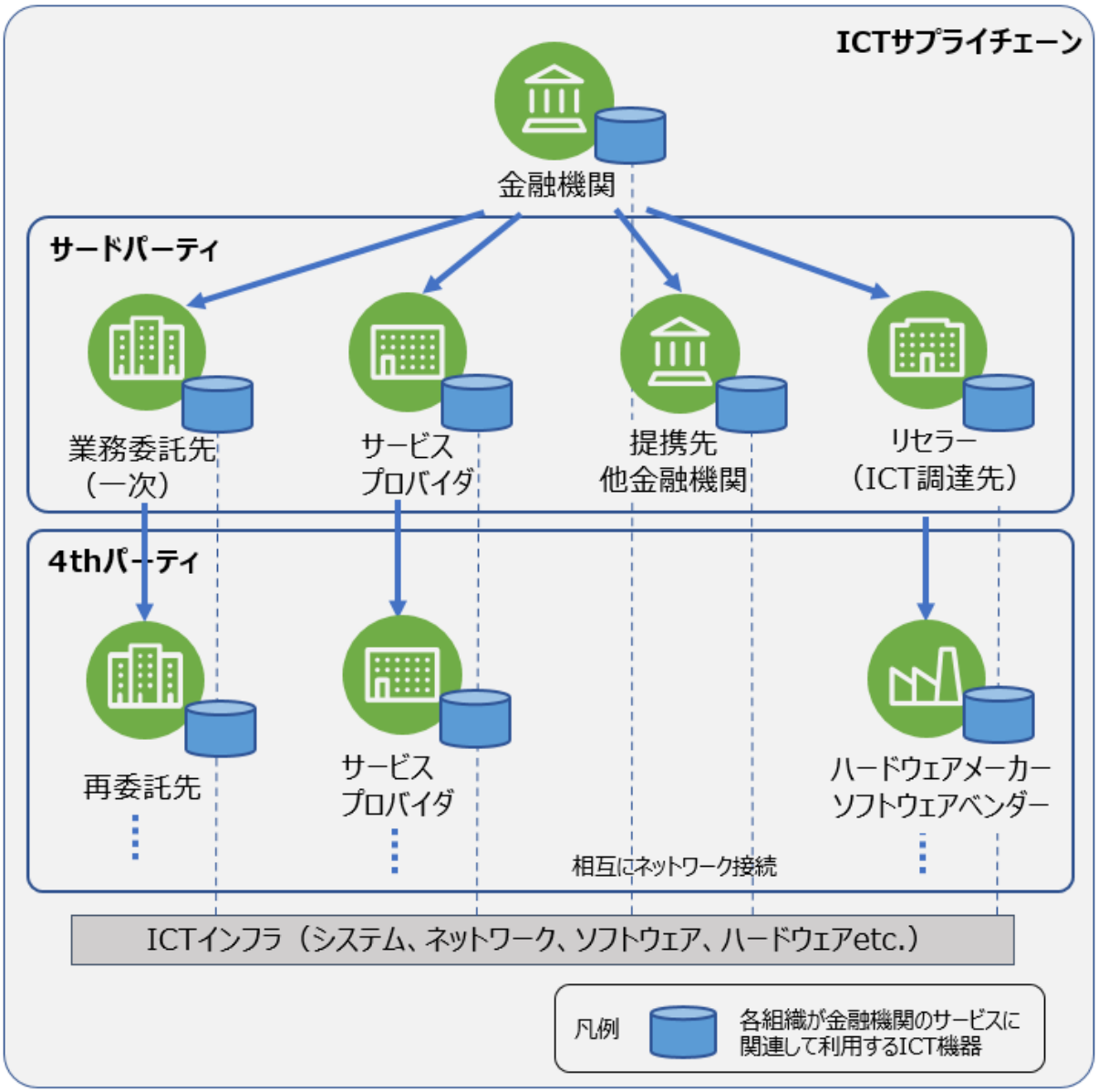

図 1　サードパーティと ICT サプライチェーンの概念

3. ガバナンス及びリスク管理プロセス

G7 基礎的要素は、サードパーティ・サプライチェーンのライフサイクル全体を通じ、サードパーティ・サプライチェーンサイバーリスクを管理するための有効なプロセスとして下記を示している（図 2 及び参考 1 参照）[27]。

・ガバナンス
・サードパーティと重要性の特定
・サイバーリスクの評価とデューディリジェンス
・契約の構成
・継続的なモニタリング
・インシデント対応
・コンティンジェンシープランと出口戦略

また、G7 基礎的要素では、金融機関は、自らの観点から特定のサードパーティへの集中リスクを特定、評価、監視し、当局と情報を共有すること、出口戦略は実行可能な範囲でテストすること、また、自らのコンティンジェンシープラン及び出口戦略に加え、特に重要なサードパーティについてはそのコンティンジェンシープランも検証することなどが推奨されている[28]。

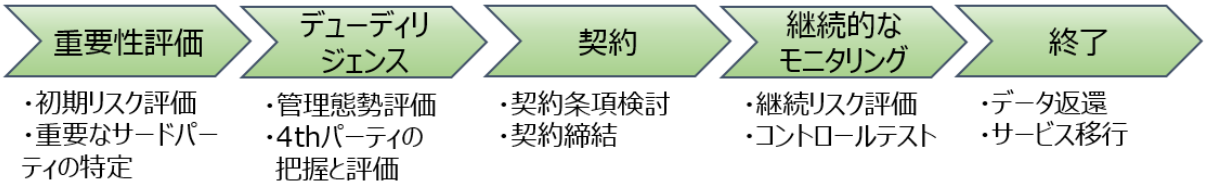

図 2　リスク管理プロセス

[27] G7 基礎的要素 1、2、3 及び 4 参照。これらは、II.1 において参照した金融セクターにおける TPRM に関するガイダンスに共通する項目である。
[28] G7 基礎的要素 4 及び 5 参照。

【参考 1】各ガイダンスにおける共通要素の概要

重要性評価

サードパーティとの関係の内容や複雑さの程度に応じてリスク管理の実務を調整することを前提に、プロセスの最初の段階（契約前の選定段階）でサードパーティの重要性評価を実施し、リスクの高い、重要なサードパーティを特定することを求めている。サイバーリスクに関連する重要性評価指標としては、下記のような例がある[29]。

・金融機関のシステム、ネットワークや金融機関が保有する機密情報へのアクセス
・データの機密性、完全性または可用性が損なわれた場合の影響

デューディリジェンス

金融機関が期待する活動を遂行する能力をサードパーティが有しているかを評価することを目的として、サードパーティとの契約締結前に、重要性評価結果に基づいて範囲や方法を選択した上で実施することを求めている。デューディリジェンスプロセスにおける考慮事項のうちサイバーリスクに関連するものとしては、下記のような例がある[30]。

・ICT コントロールとセキュリティ、サイバーリスク管理
・4th パーティ（以降）のモニタリング状況
・金融機関の情報セキュリティプログラムとの整合性
・ディザスタリカバリー及び事業継続計画
・サイバーセキュリティ保険への加入状況

契約

契約についても、サードパーティのリスクに応じて契約条項を調整することを求めており、考慮すべき要素の例を示している。サードパーティが標準契約書を提示し、変更が困難な場合の対応について言及している例もある[31]。

契約条項における考慮事項のうちサイバーリスクに関連するものとしては、下記のような例がある。

・サードパーティから継続的なモニタリングとして受け取る報告書（コントロール評価、セキュリティなど）の種類と頻度の指定
・サイバーインシデントの報告や対応に関する責任
・サプライチェーンリスク管理に関する情報を含む関連情報にアクセスし、監査し、サードパーティ

[29] 前掲書脚注 25、3.1. Identification of critical services and assessment of criticality
前掲書脚注 26、B. Risk Management

[30] 前掲書脚注 25、3.2. Onboarding and ongoing monitoring of service providers
前掲書脚注 26、C. Third-Party Relationship Life Cycle 2. Due Diligence and Third-Party Selection
前掲書脚注 27、5.18-5.20 Due Diligence, 9.3-9.8 Firms' oversight of sub-outsourcing

[31] 前掲書脚注 25、3.2. Onboarding and ongoing monitoring of service providers
前掲書脚注 26、C. Third-Party Relationship Life Cycle 3. Contract Negotiation
前掲書脚注 27、6.4-6.5 Material outsourcing agreements 8.6-8.8 Pooled audits and third party certificates and reports

から入手する権利
・事業継続、危機管理計画、災害復旧など、オペレーショナルレジリエンスに関するコミットメント

継続的なモニタリング

モニタリングについてもデューディリジェンスと同様、サードパーティのリスクレベルや性質の変化を確認し、リスクに応じた内容や頻度を選択することを求めており、考慮事項の例を挙げている。必ずしもサイバーリスクに特化した内容ではないが、関連するモニタリング活動の例として下記のような要素が挙げられている[32]。

・サードパーティのリスクが継続して許容可能か評価
・サードパーティの管理態勢の有効性に関する報告書の入手とレビュー
・サードパーティとの定期的な協議
・金融機関によるコントロールの定期的なテスト

終了

サービスを終了する、他のサードパーティに移行する、委託をやめ組織内に引き戻すなどのケースを想定し、終了または移行が円滑に行われるよう、契約時点での考慮を求めている。サイバーリスクに関連する考慮事項としては、下記のような例がある[33]。

・サービスを移行可能な代替サードパーティ候補の考慮
・サードパーティが保持していたデータの消去、破壊、返却、ネットワーク切断
・関係終了後の追加のモニタリング

[32] 前掲書脚注 25、3.2. Onboarding and ongoing monitoring of service providers
前掲書脚注 26、C. Third-Party Relationship Life Cycle 4. Ongoing Monitoring
前掲書脚注 27、5.21-5.23 Risk assessment

[33] 前掲書脚注 25、h. 3.7. Exit Strategies
前掲書脚注 26、C. Third-Party Relationship Life Cycle 3. Contract Negotiation, 5. Termination
前掲書脚注 27、10.10-10.16 Stressed exits

III. 米国大手金融機関へのヒアリング調査

1. 調査項目

既存ガイダンスの記載や、想定される金融機関の状況を踏まえて抽出した調査項目の要約を表 1 に示す。この調査項目に基づき質問票を作成し、各金融機関に事前に記載を依頼した上でヒアリングを実施した。

(1) 組織体制、人的リソース、管理の仕組み、ツール

- 組織体制に関し、サードパーティ・サプライチェーンサイバーリスクのモニタリングのうち、何をどの部署でどのように行っているか（例えば、サードパーティ利用部門、サイバーセキュリティ部門、TPRM 部門、オペレーショナルリスク管理部門の関係、サプライチェーンサイバーリスクの取扱いなど）について、どのような先進事例がみられるか、分業・専門化が進んでいるか（サイバーセキュリティ部門に加え、TPRM/SCRM 担当部門の中にもサイバーセキュリティの専門部隊が存在するかなど）といった点について調査した。また、牽制やグループ管理のあり方に本邦と違いがみられるか（TPCRM/C-SCRM について、2 線はどのように 1 線を牽制しているのか、グループ会社の TPCRM/C-SCRM をどのように統括し、管理しているのか、各拠点におけるグループポリシーの遵守をどのように確保しているのかなど）についても調査した。
- 人的リソースに関し、TPCRM/C-SCRM の各関連業務にどのような資質を持った人材を何名充てているのか（人員数、専門性・スキルなど）、どのように人材を確保・育成しているか、といった点について調査した。
- リスク管理の仕組みやツールに関し、各拠点で分散管理が行われているというよりは、グローバルに共通の枠組みの下でコントロールされていると想定されるが、その枠組み、ルール、手順はどのようなものか、グローバルで統一された管理を実現する上で、自動化、効率化がどの程度進んでいるかといった点について調査した。

(2) リスク管理プロセス

- サードパーティに起因するサイバーリスクについては、サードパーティの契約前評価から出口（契約終了）まで、サードパーティのライフサイクル全体にわたる管理が行われていると想定されるが、それがどのように行われているか、サイバーセキュリティに関する契約条項はどのようなものか、遵守状況はどのようにモニタリングしているか、サードパーティからインシデント報告をどのように求めているか、どのような脆弱性管理をサードパーティに求めているのか、出口戦略はどのような形で定められているのか、特定のサードパーティへの依存度が高まる集中リスクをどのように管理・モニタリングしているのかといった点を調査した。
- TPCRM/C-SCRM 上、4th パーティ以降に起因するサイバーリスクへの対処はどのように行われているかについても調査した。

(3) ソフトウェア管理

- オープンソースソフトウェア（OSS）として広く使われるソフトウェアライブラリに深刻な脆弱性が

発見されるなど、その影響が広範に及び、かつ、脆弱性の有無の特定が難しい事案が発生しており[34]、ソフトウェアサプライチェーンのサイバーリスク管理の難度は高まっている。ソフトウェア構成解析（SCA）[35]やソフトウェア部品表（SBOM）[36]などの管理手法が出現する中、米国大手金融機関がこれらの手法を活用しているか、またこれらの手法によりどのようにリスクを管理しているかについて調査した。

（4） ハードウェア管理

- 近年、ファームウェアや UEFI（BIOS）に対するサイバー攻撃が現実のものとなりつつある[37]。NIST SP800-193 では、不正なファームウェアの導入防止、検知だけでなく、リカバリする仕組みについても言及があり、ファームウェアの改ざんを検知、復旧するソリューションも出現している。一方、不正なハードウェアの混入による情報漏えいのリスクも指摘されている[38]。こうした攻撃は OS レイヤー以上で起動するセキュリティソリューションでは検知が困難であり、対応が十分に取られないおそれがある。意図しない不正な動作や通信を行うハードウェアを混入させ、情報漏えいなどを狙う攻撃のリスクへの対応について、米国大手金融機関がどのようにリスクを管理しているかについて調査した。
- また、不正なハードウェアの混入防止を目的としたセキュア調達関連のガイドラインや業界標準が利用されているかといった点についても調査した。

表 1　ヒアリング調査項目

大項目	中項目	小項目
（1）組織体制、人的リソース、管理の仕組み、ツール	組織体制	• 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ついて、組織体制はどのようになっているか。どの部署で何をどのように行っているか（例えば、サードパーティ利用部門、リスク管理やサードパーティ・サプライチェーンサイバーリスクのモニタリング部門などの組織構成）。 • 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ついて、2 線はどのように 1 線を牽制しているのか。グループ会社におけるサードパーティのサイバーリスク管理をどのように統括し、管理しているのか。各拠点におけるサードパーティのサイバーリスク管理に関するグループポリシーの遵守をどのように確保しているのか。

[34] 独立行政法人情報処理推進機構「Apache Log4j の脆弱性対策について」（2021 年 12 月 27 日、https://www.ipa.go.jp/security/security-alert/2021/alert20211213.html）

[35] Software Composition Analysis の略。ソフトウェアを分析して組込まれている OSS を検出し、そこに含まれている脆弱性やライセンスの問題などを検出する手法。

[36] Software Bill Of Material の略。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。相互運用性を高めるために共通フォーマットが開発されており、SPDX（Software Package Data eXchange）、CycloneDX、SWID タグ（Software Identification タグ）などがある。

[37] New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) Alert, *APT28 First Group to Embed Rootkit in UEFI*, October 4, 2018, https://www.cyber.nj.gov/alerts-advisories/apt28-first-group-to-embed-rootkit-in-uefi.

[38] ENISA, *ENISA Threat Landscape for Supply Chain Attacks*, July 29, 2021, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

大項目	中項目	小項目
	人的リソース	• 各関連業務にどのような資質を持った人材を何名充てているのか。サイバーセキュリティの管理からサードパーティを検証できる人材をどのようにして確保しているのか。
	管理の仕組み、ツール	• どのようなツールを導入し、どのように活用しているのか。ツールの利点と問題点・限界は何か。
（2）リスク管理プロセス	リスク管理手法	• ライフサイクルに沿ってどのように管理しているか。継続的なモニタリングの手法は何か。4th パーティ以降の管理はどのように行われているか。
	契約管理	• 契約管理、契約遵守のモニタリングはどのように行われているか。
	サイバー脅威の監視	• サードパーティ・サプライチェーンサイバーリスク管理の観点から、どのような監視目的が設定、実施されているか。監視体制はどのようになっているか。
	出口戦略	• 契約終了や他サービスへの移行を事前に想定した出口戦略は策定されているか、またこれらの対応について契約上の考慮はされているか。
	集中リスクへの対応	• サードパーティ・サプライチェーンサイバーリスク管理の観点から、特定のサードパーティへの依存度が高まる集中リスクをどのように管理・モニタリングしているか。
（3）ソフトウェア管理		• サードパーティ・サプライチェーンサイバーリスク管理の観点から、ソフトウェア管理がどのように行われているか。
（4）ハードウェア管理		• サードパーティ・サプライチェーンサイバーリスク管理の観点から、機器の真正性、ファームウェアの不正書換え防止管理がどのように行われているか。 • 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はどうか。

2. 調査結果及び考察

本節では、前節で述べた調査項目について、米国大手金融機関を対象とした調査結果を記載する。加えて、調査結果に基づく本邦金融機関への示唆について考察する。

調査結果及び考察の要約を表 2 に示す。

(1) 組織体制

① 調査結果

- 組織の機能としては、サードパーティの利用部門（業務部門）、TPRM 部門、サイバーセキュリティ部門が存在し、このうち TPRM 部門内に TPCRM を専門に担当するチームが存在するケースと、サイバーセキュリティ部門が TPCRM を担当し、その結果を TPRM 部門に連携する形で TPRM 部門が TPCRM を統括しているケースがある。いずれの部門も、3 線モデルの下、リスクを所有し、管理する 1 線に位置付けている。
- サイバーリスクの評価は、地域毎に TPCRM 部門を配置して実施するケース、本社がグローバルで一元的に実施するケースの双方がある。いずれも、グローバル共通のポリシー、プロセスで管理している。
- 2 線では、オペレーショナルリスク部門にサイバーセキュリティ担当チームが存在し、1 線による統制の十分性を検証している。1 線の判断に 2 線が異議を申し立てた場合、1 線が疎明しない限りサードパーティを利用できないなど、2 線の介入権限を明確に設け、2 線による牽制機能を担保しているケースがある。このケースでは、必要に応じて 1 線、2 線がそれぞれの担当役員に 1 線の検討結果をエスカレーションすることとなっている。

② 考察

米国大手金融機関では、サードパーティ・サプライチェーンのサイバーリスク管理を専門に担当するチームまたは要員が 1 線内に存在し、サードパーティ・サプライチェーンの利用部門である業務部門を牽制する 1.5 線的な役割を果たしている。

また 2 線においても、1 線のモニタリングを実質的、効果的に行うためには高度な専門性が要求されるため、2 線にもサイバーリスク管理の専担者を配置し、グローバルで一元的な管理、牽制を行っている。加えて、1 線の判断に 2 線が介入する権限が与えられている。

本邦金融機関においても、1 線における自律的な統制強化や 2 線による牽制の強化のため、1 線または 2 線に TPCRM 専担者を置くこと、2 線にサイバーリスク管理専担者を置くこと、2 線の介入権限を強化したり、リスク受容に関してエスカレーションを含めて管理プロセスを明確化したりすることは検討に値する。

本領域の改善のステップとして、例えば、以下が挙げられる。

i. 自組織内の現状の TPCRM 体制を評価する。
ii. 1 線の統制、2 線による牽制といったチェックアンドバランスの関係の明確さ、各部門の機能の十分性に不備がある場合、その要因を分析する（組織体制上の不備、専門知識の不足、人員不足など）。

iii. 上記の例を参考に、1 線内の統制機能の強化や 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などの体制強化を検討する。

（2） 人的リソース

① 調査結果

- TPRM 部門にサイバーセキュリティ専門家を 100 名程度配置し、グローバルで一元的に管理する体制としている。
- TPCRM 業務に要求されるスキル・経験として、情報セキュリティ領域の技術、リスクまたはコントロール評価などの関連業務のいずれかを数年間経験していることを求めている。
- TPCRM 専門家としての技術は、社内トレーニングや経験の浅い職員により経験のある者をメンターとして配置する制度の活用によって身に付けさせている。さらに、効率的に業務経験を積ませるため、サイバーリスク評価に特化させている。
- サイバーリスク評価の一部を委託し、外部のリソースを活用するケースもある。

② 考察

今般、アウトソース先に限らず、多様なサードパーティ・サプライチェーンがサイバーリスクを呈している状況などを勘案し、米国大手金融機関では、契約形態に関わらず全てのサードパーティ・サプライチェーンを直接的または間接的なリスク管理対象としており、管理対象の拡大に見合う人的リソースが必要となっている。加えて、サードパーティ・サプライチェーンのサイバーリスク評価に、より専門的な知識が必要になっており、質の面でもその管理を支える人的リソースが必要となっている。今回の調査で確認した限りにおいて、直接の管理対象のサードパーティは、10,000 社以上になるケースもあり、この管理に対応する TPCRM 部門に 100 人程度の専門家が配置されている。

スキル面では、サイバー部門の職務記述書（Job Description）において求められるサイバーセキュリティに関する専門性に加え、TPRM の経験まで要求するケースもあったが、TPCRM 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ることなどにより、TPCRM 関連スキルを身に付けさせ、組織としての専門性を高め、人的リソースを強化する工夫をしている。

本邦金融機関においても、スコープの拡充をはじめとして TPCRM/C-SCRM の高度化が求められているが、その実現には人的リソースの強化が不可欠である。

本領域の改善のステップとして、例えば、以下が挙げられる。

i. 自組織内にて TPCRM 業務に携わる現時点での人員数及びスキルセット、他業務との兼任などの人的リソースの状況を整理する。
ii. 現時点及び将来的な TPCRM 業務の実施内容及び作業量に比べ、現時点での人的リソースで対応可能かどうかを判断する。その際、上述した米国大手金融機関における管理の状況も参考にする。
iii. 現在の人的リソースの状況では不十分である場合、人材確保・育成計画の策定及び実施並びに各種ツールの活用を検討する。
※各種ツールの活用に関する具体的な検討アプローチは「（3） 管理の仕組み、ツール ②考察」に記載。

（3） 管理の仕組み、ツール

① 調査結果

・ リスク管理プロセスは国や地域に関わらず共通としているが、評価ツールや評価項目のレベルでは、各地の法規制に対応するためのカスタマイズが行われている。
・ 内製ツールまたは市販ツールを活用することで、多数に上るサードパーティの管理の効率化を図っている。市販ツールを利用する場合も、各金融機関のプロセスに合わせたカスタマイズを実施している。
・ 評価項目の設定、サードパーティとのアンケートのやり取り、回答結果の集約に市販の TPRM アンケートツールを活用し、社内での回答結果の分析や評価では内製ツールを活用する傾向がある。
・ 導入当時は市販ツールの選択肢が限られていたために内製せざるを得なかったが、現在も市販ツールよりも充実した機能を維持し、内製ツールの利用を継続するケース、内製ツールがサイロ化したため、市販ツール導入により統合を目指したケースの双方があった。
※脅威のモニタリングのためのツールの活用については、後出の「（6）サイバー脅威の監視② 考察」に記載。

② 考察

サードパーティ・サプライチェーンのサイバーリスク評価実施先として、米国大手金融機関では多いところで 10,000 社を超えるサードパーティに対して直接管理している。このように広範なサードパーティ・サプライチェーンに対するリスク評価や、評価時における管理対象先とのやり取りは、スプレッドシートや電子メールを使った手作業では担当者に多大な負担が生じることから、米国大手金融機関では内製ツールまたは市販ツールを活用し、効率化している。

本邦金融機関においても、広範なサードパーティ・サプライチェーンを管理対象とし、全社一元的に管理することを考慮すると、効率化は不可欠であるといえる。本領域の改善のステップとしては、望ましい業務プロセスと現在の業務プロセスのギャップ分析などを実施した上で、ツール導入の要否を検討することが挙げられる。

（4） リスク管理手法

① 調査結果

・ 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、自社と同じセキュリティ水準を要求している。コントロール評価など、リスクに応じた評価手法を選択し継続的にモニタリングを実施している。
・ 企画、デューディリジェンス、選定、契約、継続的なモニタリング、契約終了といった、ライフサイクル管理が行われている。
・ デューディリジェンスまたは選定段階で重要度の分類を行い、契約以降のモニタリングの軽重を決定している。例えば、重要度の分類に応じ、継続評価の初回実施タイミング、継続評価の頻度、実地調査の要否や深度を決定している。
・ 4th パーティを直接の管理対象とはしないが、サードパーティの 4th パーティに対する管理におい

て、自社と同水準のコントロール評価を実施するか、自社と同水準のコントロールの実施を契約上求めることで、間接的に管理している（脆弱性管理を含む）。ただし、4th パーティが取扱っているデータの特定や保管場所の確認のために、金融機関が自ら 4th パーティの情報を取得したり、4th パーティの固有リスク評価を行ったりするケースがある。

・ 継続的なモニタリングの手法について、複数金融機関が共同で開発に関与した質問票を含む TPRM ツール（サイバーセキュリティを含む）の活用が進んでいる。

② 考察

米国大手金融機関では、サードパーティに自社と同じセキュリティ水準を要求していること、必要に応じて金融機関が自ら 4th パーティ（とそれ以降）のリスク評価を行うケースがあることのほか、リスクレベルに応じたモニタリング手法を用いている点が着目に値する。例えば、低リスクと判断された評価対象先に対しては定期的なリスク評価の頻度を減らし、高リスクのサードパーティの管理により焦点を当てるといったリスクベースの手法が採られている。

本邦金融機関における本領域の改善のステップとして、例えば、以下が挙げられる。

a. 4th パーティ以降のサイバーリスク管理について
   i. 自組織において 4th パーティ以降のサイバーリスクを自組織においてどのように管理しているか、自組織と同水準のサイバーセキュリティを求めているかを再確認する。
   ii. 4th パーティ以降がリスク管理対象外、またはその管理が不十分な場合、サードパーティとの契約の中で 4th パーティ以降のサプライチェーンをサードパーティが管理することを求める、または必要に応じて自ら評価することを検討する。

b. 対象範囲及び継続的なモニタリングについて
   i. リスク評価対象のモニタリング頻度がリスクベースの観点から適切か、再確認する。
   ii. 評価頻度の見直しが必要と判断する場合は、管理の仕組み、ツール、人的リソースの再配分なども併せて検討する。

（5） 契約管理

① 調査結果

・ 契約書の標準ひな型に、関連する法令への対応、自社のセキュリティポリシーと同水準のコントロールの実施を求める条項が含まれる。その中には、例えば、サードパーティから金融機関へのインシデント報告義務、サードパーティにおける脆弱性への対応及び対応状況の報告義務などが含まれる。また、セキュリティを含め、サードパーティが遵守すべき各種要件を記した付属書をウェブ上で公開し、契約を結ぶにあたってどのような対応が必要かをサードパーティが事前に確認できるようにしているケースもある。
・ 契約書または付属書に要件を詳細に記載して遵守を要求し、継続的なモニタリングを行っている。
・ サードパーティに対する再委託先管理義務を要件に含め、4th パーティに対してサードパーティと同などのセキュリティ要件を課すことを求めている。

② 考察

米国大手金融機関では、契約書の標準ひな型においてサードパーティに自社と同などのセキュリティ水準を要求し、サードパーティが遵守すべき要件を詳細に記載しているケース、サードパーティが遵守すべきセキュリティを含む各種要件を記した付属書をウェブ上で公開し、各社と契約を結ぶにあたってどのような対応が必要かをサードパーティが事前に確認できるようにしているケースなどは、サードパーティのセキュリティレベルを契約上の要求事項として明確化するという点で着目すべき事例である。

本邦金融機関における本領域の改善のステップとして、例えば、以下が挙げられる。

i. 現在自組織で使用しているサードパーティとの契約書ひな型を確認し、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が含まれているか、再確認する。
ii. ひな型にサイバーセキュリティ要件が含まれていない、または内容や粒度が不十分である場合、新規契約要項の追加や付属書の新規作成などの対応を検討する。
iii. サードパーティに対する要求事項をウェブサイトで公開するなど、サードパーティが容易に確認できるようにする。

(6) サイバー脅威の監視

① 調査結果

・ 直接の管理権限が及ばない 4th パーティ以降も含めた ICT サプライチェーンへのサイバー脅威の監視として、サイバー脅威インテリジェンスの手法を用いたモニタリングを実施している。市販の脅威インテリジェンス分析ツールや ASM[39]ツールを活用し、モニタリングを実施しているケースや OSINT[40]に基づいて自社内で情報収集、分析を実施しているケースがある。また、監視をサイバーセキュリティ部門が実施するケースと、TPRM 部門に所属するサイバーリスク関連チームが実施するケースがある。
・ 監視により脅威や脆弱性を認めた場合は、サードパーティにその情報を共有し、説明を求め、必要に応じて是正を求めている。インシデントが発生した際の自組織への影響の度合いに応じて、アラートの緊急度レベルに差をつけているケースもある。

② 考察

米国大手金融機関では、サードパーティ及び ICT サプライチェーンについて脅威インテリジェンスをモニタリングに活用しており、本邦金融機関においても検討に値すると考えられる。

本領域の改善のステップとして、例えば、以下が挙げられる。

i. 現在自組織で運用している脅威インテリジェンスのスコープにサードパーティ・サプライチェーンも含まれているか、再確認する。
ii. サードパーティ・サプライチェーンがスコープ外の場合、TPCRM における継続的なモニタリングの手段として脅威インテリジェンスを含めることを検討する。併せて、脅威インテリジェンスの

[39] Attack Surface Management の略。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。

[40] Open-Source Intelligence の略。主に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し、組み合わせて分析する調査手法のこと。

対象となるサードパーティ・サプライチェーンのスコープが十分かどうかを検討する。

iii. TPCRM/C-SCRM に脅威インテリジェンス分析ツール、ASM ツール、OSINT を活用することを検討する。脅威や脆弱性を認めた場合、対象への情報を共有し、是正を求める。自組織への影響度が高い先には緊急度レベルを上げて対応する。

(7) 出口戦略

① 調査結果

・ 契約終了時には、サードパーティが契約に基づいて保有が許可されていた機密情報を返却または削除することが契約上求められている。これに関しては、契約を終了したことによる金融機関業務への影響や、データの返還がなされたか否かなどを評価するケースがある。また、サードパーティのサービス終了に関連して、自社に関連する全ての機密情報（及び関連する記録及びファイル）の返却などに必要な協力・支援を自社に提供すること（例えば、自社からの要請に応じて一定期間サービスの提供を継続させること、など）も併せて取り決めているケースもある。

・ サードパーティにおいて自社または顧客に深刻な影響を及ぼすインシデントが発生することを想定し、サードパーティからのサービス提供の拒絶（アクセス遮断など）や契約の解除を実行するプロセスを事前に定めている。当該プロセスの発動において、インシデントの深刻度（中断するサービスの重要度、中断期間など）を検討要素としている。併せて平常時の対策としてサービスの代替先候補をリスト化しているケースがあるが、サービスの代替先がない場合においてもインシデントにより自社へ波及する影響が深刻かつ明白である場合には当該プロセスを発動させている。

・ なお、サードパーティにおいてインシデントが発生した場合には原則、速やかに金融機関に伝えることを契約上取り決めている。加えて、インシデントが発生した場合、封じ込め対策として、サードパーティからのアクセス遮断を行う、インシデント後の対策の評価を実施するといった対応を行うケースもある。これらの対応に関するプロセスは事前に計画・準備されている。

② 考察

米国大手金融機関では、重要なサードパーティサービスの利用終了や代替先への移行、インシデントに起因してサービスの遮断、契約解除や切り替えを行う事態を想定し、事前、事後の対応を定義している。

本邦金融機関における本領域の改善のステップとして、例えば、以下が挙げられる。

i. 機密情報の返却や削除など、サードパーティとの契約終了時におけるサイバーセキュリティ観点の対応要求事項について、追加の要否などを検討する。

ii. 自社のサイバーインシデント対応手順などを確認し、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対応、インシデント終息後の対応など、上述した米国大手金融機関における参考となる取組みが含まれているかを確認の上、含まれていない場合は追加の必要性の検討を実施する。

（8） 集中リスクへの対応

① 調査結果

・ 代替可能性、地理的集中、クラウドサービスなど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。
・ 評価結果は経営層に共有され、集中リスクが重大であると判断された場合は、追加でデューディリジェンスを行うといった対応を取る。

② 考察

米国大手金融機関では、個別のサードパーティに対する管理だけでなく、代替可能性、地理的集中、自社のサードパーティであり、かつ、4th パーティ以降のサービスプロバイダでもある同一の先への集中などを考慮した横断的な管理を行うことは本邦金融機関においても検討に値する。

本領域における改善のステップとしては、自組織におけるリスク管理の観点に、上述の観点が考慮されているか再確認し、必要に応じて集中リスクの評価手法を検討することが挙げられる。

（9） ソフトウェア管理

① 調査結果

・ 自社開発ソフトウェア、ベンダー開発ソフトウェアなどの形態に関わらず、受入時のソフトウェアの脆弱性評価を実施している。サイバーセキュリティ部門の中の技術的評価を担当するチームが対応している。
・ ソースコードレビュー、ソフトウェア構成要素解析（SCA）を実施しているケースもある。

② 考察

ICT サプライチェーンの脆弱性管理という観点から、昨今、OSS の利用状況などのソフトウェアの構成要素管理の重要性が高まっている。SCA などによるソフトウェア構成要素の把握は、OSS などを通じて混入する脆弱性を可視化し、早期の対応につなげることを目的としている。本来はサードパーティ及び 4th パーティ以降の ICT サプライチェーンも脆弱性管理のスコープに入るが、米国大手金融機関においても、現状 ICT サプライチェーンに存在する脆弱性を網羅的に把握、管理するための手法が確立されているとはいえず、発展途上の領域であると考えられる。

従前より、ソフトウェアの脆弱性管理に関しては、ソフトウェアベンダーがセキュアな開発体制を構築しているかをサイバーリスク評価の一環として確認する、といった実務がある。しかし、米国大手金融機関ではこれに留まらず、自社が使用するソフトウェアの脆弱性は自社で確認するとの方針の下、技術的評価を実施するチームを持ち、評価を実施している。ソースコードレビューや SCA など、技術的に可能な手法を積極的に採用し、高度化を進める姿勢がみられた[41]。

本邦金融機関における本領域における改善のステップとして、例えば、以下が挙げられる。

---

[41] NIST SP 800-161 Rev.1（前掲書脚注 18）では、高度なテストの実施、文書化やセキュリティ機能の要求によって製品の価格は上昇し、最終的には調達側のコスト増要因となることから、サイバーセキュリティリスク対応によって得られる便益とコストのバランスを考慮すべきと指摘している。

i. ICT サプライチェーンのサイバーリスクの観点から重要なソフトウェアを識別し、これらが脆弱性評価の対象となっていることを再確認する。その上で、受入時並びに継続的な脆弱性評価に、上述のソフトウェア構成要素分析やソースコードレビューが含まれているかを確認し、含まれていない場合は追加対策の必要性を検討する。
ii. ソフトウェアコンポーネントの出所や OSS の利用状況を把握し、対処が必要な脆弱性が報告、公表された場合に、自社及びサードパーティにおいて迅速な対応が行えるような体制の構築を検討する。

（10） ハードウェア管理

① 調査結果

・ 端末のファームウェアに関しては、Hardware Root of Trust（Trusted Platform Module など）を内蔵した製品であることを調達基準とし、順次入れ替えを進めている。
・ サーバのファームウェアについても同様に Hardware Root of Trust を内蔵した製品であることを調達基準とし、不正なファームウェアや UEFI（BIOS）の導入防止並びに改ざん検知を実施しているケースもある。
・ 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おり、これに従った調達を実施している。

② 考察

ソフトウェア管理と同様に、ICT サプライチェーン上のハードウェアの脆弱性管理の重要性は高まっているが、不正、あるいは意図しない動作をするハードウェアが混入していないか、といった問題を含め、網羅的に把握、管理する手法が確立されているとはいえず、発展途上の領域であると考えられる。

上記のように、ハードウェアやファームウェアの脆弱性管理は発展途上ではあるが、脅威が顕在化した場合の影響の大きさや検知の困難性を踏まえ、特に大規模な金融機関においては、より高度な攻撃手法を想定した先進的な対策として検討が望まれる領域である。また、規模に関わらず不正なハードウェアやファームウェアの混入を防ぐセキュアな調達の推進が望まれる。

本邦金融機関における本領域における改善のステップとして、例えば、以下が挙げられる。

i. 自社の ICT サプライチェーンのサイバーリスク評価において、ハードウェアに対する不正なファームウェアの導入のリスクが評価対象となっていることを再確認する。
ii. 対応策として、上述した米国大手金融機関における参考となる取組みが含まれているかを確認の上、含まれていない場合は追加の必要性を検討する。
iii. 調達に関するビジネス、倫理、法規制などのポリシーとの整合を図り、NIST のガイドラインなどを参考にし、必要に応じて調達基準や取引基準などへの組込みを検討する。

表 2 調査結果及び考察の要約

No.	調査項目	調査結果の要約	改善のステップ例示
1	組織体制	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、グローバル一元的に管理、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。	自組織内の現状の TPCRM 体制を評価し、1 線の統制、2 線による牽制といったチェックアンドバランスの関係に不備がないか分析する。 必要に応じ、1 線内の統制機能の強化や 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などの体制強化を検討する。
2	人的リソース	管理対象は数千社、これに対応するサードパーティサイバーリスク管理の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。	自組織内にて TPCRM 業務に携わる人的リソースの状況を整理し、現時点及び将来的に必要な TPCRM 業務に対応可能か分析する。 必要に応じ、人材確保・育成計画の策定及び実施並びに各種ツールの活用を検討する。
3	管理の仕組み、ツール	サードパーティとのアンケートのやり取り、回答結果の集約に内製ツールまたは市販ツールを活用し、効率化している。	望ましい業務プロセスと現在の業務プロセスのギャップ分析などを実施した上で、ツール導入の要否を検討する。
4	リスク管理手法	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ている。 4th パーティ以降を直接の管理対象とはしないが、サードパーティの 4th パーティに対する管理を要求し、間接的に管理している。 リスクレベルに応じたモニタリング手法を用いている。	a. 4th パーティ以降のサイバーリスク管理について 4th パーティ以降の管理状況を再確認し、必要に応じ、サードパーティとの契約の中で 4th パーティ以降のサプライチェーンの管理を求める、または自ら評価することを検討する。 b. 対象範囲及び継続的なモニタリングについて モニタリング手法がリスクベースの観点で適切なものとなっているかを分析し、必要に応じて管理の仕組み、ツール、人的リソースの再配分などを検討する。

No.	調査項目	調査結果の要約	改善のステップ例示
5	契約管理	契約書の標準ひな型において遵守すべき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。サードパーティに対する再委託先管理義務を要件に含め、サードパーティと同など要件の遵守を求めている。	契約書ひな型に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が適切に含まれているかを再確認し、必要に応じ新規契約要項の追加や付属書の新規作成などの対応を検討する。
6	サイバー脅威の監視	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が適切かを分析し、必要に応じてスコープの拡大を検討する。 脅威インテリジェンス分析ツール、ASM ツール、OSINT の活用を検討する。
7	出口戦略	契約終了、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。	契約終了時におけるサイバーセキュリティ観点の対応要求事項、サイバーインシデント発生時の対応についてサードパーティとの取り決めの状況を再確認し、必要に応じ追加の対応を検討する。
8	集中リスクへの対応	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。 集中リスクが重大であると判断された場合は、追加でデューディリジェンスを行うといった対応を取る。	現状のリスク管理手法における集中リスクの考慮状況を再確認し、必要に応じ、集中リスク評価手法を検討する。

No.	調査項目	調査結果の要約	改善のステップ例示
9	ソフトウェア管理	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など、受入時のソフトウェアの脆弱性評価を実施している。	ICT サプライチェーンのサイバーリスクの観点から重要なソフトウェアを識別し、これらの脆弱性評価が適切に行われているか再確認し、組込まれているOSSなども含め、ソフトウェアに脆弱性が識別された際に迅速な対応が行えるよう、脆弱性評価範囲や内容の高度化、構成要素管理などの対応を検討する。
10	ハードウェア管理	端末、サーバがファームウェア改ざん防止機能など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。	自社の ICT サプライチェーンのサイバーリスク評価において、ハードウェアに対する不正なファームウェア導入のリスクの考慮状況を再確認し、必要に応じ調達基準の見直しなどを検討する。 調達に関するビジネス、倫理、法規制などのポリシーとの整合を図り、必要に応じて調達基準や取引基準などへの組込みを検討する。

IV. 結語

本調査では、深刻性の高まるTPCRM/C-SCRMに関し、米国大手金融機関における先進事例を調査することを通じ、本邦金融機関への示唆を考察した。

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。

本調査で考察した主な示唆は以下のとおりである。

- 組織体制面及び人的リソース面では、TPCRM/C-SCRMに従事する要員の規模もさることながら、TPCRM 専担者が存在すること、グローバルで共通の管理プロセスを採用し、サイバーセキュリティの専門性を持つ専担者がグローバルにリスク管理を行っている。
- リスク管理の仕組み、ツールに関しては、多数のサードパーティの管理を内製、市販ツールの活用により効率化している。
- リスク管理プロセスについて、高リスクの評価対象に焦点を当てた継続的モニタリングを実施し、必要に応じて自ら4thパーティ（とそれ以降）のリスク評価も行っている。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。
- ソフトウェアサプライチェーンリスク管理面では、構成要素分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。

本邦金融機関においては、高度化するサイバー攻撃の脅威に適切に対応するため、自組織のサードパーティ・サプライチェーンサイバーリスクを適切に評価した上で、本調査から得られる示唆も参考にしてTPCRM/C-SCRMを高度化していくことが望ましい。

以上

Appendix

付表 1 参照文献一覧

No.	発行者（発効日）	文書名（上段　日本語訳（当社仮訳）／原題 下段　参照 URL）
1	G7 サイバー・エキスパート・グループ （2022 年 10 月 13 日改訂）	金融セクターにおけるサードパーティのサイバーリスクマネジメントに関する G7 の基礎的要素／G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector https://www.fsa.go.jp/inter/etc/20221021/contents.html
2	米国ニューヨーク州金融サービス局 （2017 年 3 月 1 日）	金融サービス会社向けのサイバーセキュリティ要件／Cybersecurity Requirements for Financial Services Companies https://www.governor.ny.gov/sites/default/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23NYCRR500.pdf
3	欧州ネットワーク・情報セキュリティ機関 （ENISA） （2023 年 6 月 13 日）	サプライチェーン・サイバーセキュリティのための優れた取組み／Good Practices for Supply Chain Cybersecurity https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity
4	米国国立標準技術研究所（NIST） （2022 年 2 月 4 日）	大統領令 14028 セクション 4e に基づくソフトウェアサプライチェーンセキュリティのガイダンス／Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e https://csrc.nist.gov/pubs/other/2022/02/04/software-supply-chain-security-guidance-eo-14028-s/final
5	NIST （2022 年 5 月 5 日）	NIST SP800-161r1：連邦政府情報システムと組織のためのサイバーセキュリティサプライチェーンリスク管理の慣行／Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations https://doi.org/10.6028/NIST.SP.800-161r1
6	NIST （2011 年 4 月 29 日）	NIST SP800-147：BIOS 保護ガイドライン／BIOS Protection Guidelines https://doi.org/10.6028/NIST.SP.800-147
7	NIST （2018 年 5 月 4 日）	NIST SP800-193：プラットフォームファームウェアのレジリエンスに関するガイドライン／Platform Firmware Resiliency Guidelines https://doi.org/10.6028/NIST.SP.800-193

No.	発行者（発効日）	文書名（上段　日本語訳（当社仮訳）／原題 下段　参照 URL）
8	米国国家安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA） （2021 年 4 月 12 日）	ベンダーSCRM テンプレート／Vendor SCRM Template https://www.cisa.gov/resources-tools/resources/ict-scrm-task-force-vendor-template
9	CISA （2023 年 9 月 25 日）	SCRM のためのハードウェア部品表（HBOM）フレームワーク／Hardware Bill of Materials (HBOM) Framework for Supply Chain Risk Management https://www.cisa.gov/resources-tools/resources/hardware-bill-materials-hbom-framework-supply-chain-risk-management
10	ENISA （2017 年 1 月 21 日）	調達のための必須セキュリティ要件／Indispensable Baseline Security Requirements for the Procurement of Secure ICT Products and Services https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services
11	金融安定理事会 （2023 年 6 月 22 日）	サードパーティリスクの管理とオーバーサイトの向上：金融機関と金融当局のためのツールキット（市中協議文書）／Enhancing Third-Party Risk Management and Oversight: A Toolkit for Financial Institutions and Financial Authorities - Consultative Document https://www.fsb.org/2023/06/enhancing-third-party-risk-management-and-oversight-a-toolkit-for-financial-institutions-and-financial-authorities-consultative-document/
12	米国連邦準備制度理事会、連邦預金保険公社、通貨監督局、財務省 （2023 年 6 月 9 日）	サードパーティとの関係に関する省庁間ガイダンス：リスク管理／Interagency Guidance on Third-Party Relationships: Risk Management https://www.federalregister.gov/documents/2023/0/09/2023-12340/interagency-guidance-on-third-party-relationships-risk-management

No.	発行者（発効日）	文書名（上段　日本語訳（当社仮訳）／原題 下段　参照 URL）
13	イングランド銀行 健全性規制機構 （2021 年 3 月 29 日）	監督文書 SS2/21 外部委託とサードパーティのリスク管理／ Supervisory Statement SS2/21 | Outsourcing and Third Party Risk Management https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss221-march-21.pdf

付表 2 用語集

個別に特記していないが、いずれの用語もサイバー（セキュリティ）の文脈で使用される場合の用語の定義として記載している。

用語	初出ページ	定義
サードパーティ	1	その組織がグループ内企業であるか外部組織であるかに関わらず、組織に対し特定の製品またはサービスを提供する相手先。代表的な形態としては業務委託先。
ICT サプライチェーン	1	組織が自身の業務を支えるために用いる ICT エコシステムを形成する、サードパーティ間の相互の結び付きからなる。ICT サプライチェーンには、すべての製品、サービス及びインフラに加え、それらの提供者、供給者及び製造業者も含まれる[42]。
4th パーティ	1	サードパーティに対しサービスなどを提供する（サードパーティサービス関係にある）組織。代表的な形態としては再委託先。 4th パーティ及びそれ以降の再委託先を 5th, Nth パーティなどの用語を用いて表記することがあるが、本報告書では、「4th パーティ以降」と記載する。
SCA	2	ソフトウェア構成分析（Software Composition Analysis） ソフトウェアを分析して組込まれている OSS を検出し、そこに含まれている脆弱性やライセンスの問題などを検出する手法。
OSS	2	オープンソースソフトウェア（Open-Source Software） 利用者の目的を問わずソースコードを使用、調査、再利用、修正、拡張、再配布が可能なソフトウェア。多くの場合、その利用が無保証であることの誓約や、利用者の制約事項を含めた汎用的なオープンソースライセンス（例　GNU GPL、Apach-2.0、MIT）を採用している。
ファームウェア	2	システムを構成するハードウェアを制御するためのソフトウェアのうち、ハードウェアに密接に結び付いていて、むやみに書換えることのない媒体（多くの場合不揮発性メモリ（ROM）などの集積回路）に書き込まれたもの。PC、サーバでは BIOS（Basic Input/Output System）や UEFI（Unified Extensible Firmware Interface）と呼ばれている。
デューディリジェンス	9	調査対象組織のサイバーセキュリティ対策がどのように実施されているかを調査、分析すること。管理態勢のほか、インシデントの発生状況、システムの脆弱性評価などを含むことがある。

[42] 前掲書脚注 1、G7 基礎的要素より引用。

出口戦略	9	一般的には、軍事行動や投資活動などで損失・被害を最小限に留めて撤退する作戦のことを指すが、TPCRM の文脈では、サードパーティサービスの提供が中断するなどして組織のサービスに影響が出ている状況で、サードパーティとの関係を終了させ、内製もしくは他のサードパーティサービスに移行するための計画を指す。
集中リスク	9	一般には、機能が特定の領域に集中することで、その領域に異常があった場合に組織全体の機能維持が困難になるリスクのことを指すが、TPCRM の文脈では、特定のサードパーティサービスプロバイダへの依存度が高い場合に、そのプロバイダにサイバーインシデントが発生しサービスが利用できなくなった場合に組織全体のサービス継続や事業継続が困難になるリスクを指す。
SBOM	13	ソフトウェア部品表（Software Bill Of Material） 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。相互運用性を高めるために共通フォーマットが開発されており、SPDX（Software Package Data eXchange）、CycloneDX、SWID タグ（Software Identification タグ）などがある。
3 線モデル	15	米国に本部を置く内部監査人協会（IIA）が提唱する組織モデルで、以下 3 つのラインが相互に調整、コミュニケーション、連携、協働することで強力なガバナンスとリスク管理を促進することができるとする[43]。 第 1 ライン（1 線）：顧客に対する製品やサービスの提供と、リスクの管理 第 2 ライン（2 線）：リスクに関連する事項について、専門知識、支援、モニタリングの提供と異議申し立て 第 3 ライン（3 線）：目標の達成に関するすべての事項について、独立した客観的なアシュアランスと助言
脅威インテリジェンス	19	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。オープンソースインテリジェンス（OSINT)、シグナルインテリジェンス（SIGINT）、ソーシャルメディアインテリジェンス（SOCMINT)、ヒューマンインテリジェンス（HUMINT）などからなる。

[43] The Institute of Internal Auditors, *The IIA's Three Lines Model : An Update of the Three Lines of Defense*, July 2020, https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf.
日本語訳　https://www.iiajapan.com/leg/pdf/data/iia/2020.07_1_Three-Lines-Model-Updated-Japanese.pdf

ASM	19	アタックサーフェス（攻撃対象領域）の把握・管理（Attack Surface Management） 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。
OSINT	19	オープンソースインテリジェンス（Open-Source Intelligence） 主に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し、組み合わせて分析する調査手法のこと。
Hardware Root of Trust	22	信頼の基点（Root of Trust）を格納しているハードウェア。暗号鍵が格納されており、コンピュータの起動プロセスなどで実行されるコードの完全性を確認する機能を有する。この機能を改ざんが困難なハードウェアにより提供することで、高度なセキュリティを確保しようとするもの。これを基点に信頼の連鎖を形成することで、コンピュータ全体の信頼性を確保する。国際標準規格（ISO/IEC 11889）に則る Trusted Platform Module や、Apple 社が自社製品に採用する Secure Enclave などがある。