

金融機関に求められる サイバーセキュリティ実務対応 (下)

——サードパーティリスク管理

星野 悠樹

八雲法律事務所 弁護士

岸野 秀昭

シンプルクス株式会社
シニアセキュリティスペシャリスト

本企画は、サイバーセキュリティ法務に精通した弁護士と、企業の実情に即したセキュリティ態勢の設計・高度化を支援するITコンサルタントの2名による解説と対談で構成するものである。第一部ではテーマの前提知識や注目される論点を整理し、第二部では両者による対

第一部 解説

近年、金融機関のITシステムは、外部のクラウドサービスやAPI連携先のシステムなど、多様なサードパーティ(外部組織)のシステムへの依存を急速に深めている。しかし、その反面、サードパーティを起因とするサイバーインシデントが相次いでいる。

こうした状況を踏まえ、金融庁が2024年10月に策定、2025年7月に一部改正した「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」(以下、「金融庁ガイドライン」という)においては、金融機関等は「サプライチェーンのサイバーセキュリティリスクを

談で具体的な考察を加えていく。上編は「経営陣の役割」、中編は「リスクの特定」について解説した。最終回の下編となる本稿では「サードパーティリスク管理(委託先の監督)」を取りあげる。

適切に管理する必要がある」と位置づけ、サードパーティリスク管理を独立した章として体系的に規定している。

また、サプライチェーン全体でのサイバーセキュリティ向上を図る取組みとして、経済産業省および内閣官房国家サイバー統括室による「サプライチェーン強化に向けたセキュリティ対策評価制度」(以下、「SCS評価制度」という)の制度構築も進んでいる。本稿では、金融庁ガイドラインにおけるサードパーティリスク管理に関する事項を解説するとともに、近時のサードパーティリスクに係るインシデント

事例や法的事項、さらにはサプライチェーン対策に関する制度的な動向を踏まえ、金融機関がとるべき実務対応について考察する。

一 サードパーティリスク 管理が注目される背景

金融機関を取り巻くIT環境は大きく変化している。冒頭において述べたように、クラウドサービス提供事業者やAPI連携先等を含むサードパーティへの依存が深まる一方で、近時、金融機関の委託先等のサードパーティがランサムウェアや不正アクセスの被害を受け、結果的に金融機関の顧客情報が漏えいしたり、金融機関の業務に支障が生じたりするサイバーインシデントが頻繁に発生する事態になっている。経済産業省のIT政策実施機関である情報処理推進機構(IPA)の「情報セキュリティ10大脅威2026」[組織]においても「サプライチェーンや委託先を狙った攻撃」が2位に挙げられている。サードパーティリスクが顕在化した近時の事例を挙げると、

近時の不正動向を踏まえた内部監査部門および 監査役・監事による監査手法見直し時の着眼点

オペレーショナルデザイン株式会社取締役・デザイナー/データアナリスト 佐々木城寿

昨年8月に公表された「2025事務年度 金融行政方針主なポイント」には、協同組織金融機関における適切な経営管理および業務運営の確保として「不正融資や重大な法令違反が確認されたことも踏まえ、早期に課題を発見し、的確な対応を行う」旨が明記された。他方、公表後にも不正行為が断続的に報道され、態勢整備の難しさを逆説的に示している。

本稿では、主に内部勤務者の不正防止に寄与する監査手法見直し時の着眼点を概説したい。

一 近時の不正動向から窺える問題点

1 名寄せ

実務上、マネー・ローンダリング等対策のほか相続や預金保険料の計算、さらに一先および同一グループ先への与信限度額管理などを目的に実施される。そうした日常的な対応のうえで、預金保険機構による検査などを見越した整備が加わる。

一方、かねてよりみられる借名預金や迂回融資のほか、近年報じられた無断借名融資などが、名寄せを無効化させるデータの偽装に該当する。近時の不正事象では、与信限度額超過を隠蔽するため、顧客情報ファイル（以下、「CIF」という）

を追加登録（二重登録）して同一先でないよう偽装するなどの手口の巧妙化がみられる。

2 反社会的勢力リスト

反社会的勢力との取引を遮断するために活用される反社会的勢力リスト（以下、「リスト」という）は、金融機関外部によるデータベース等を導入し、それに各金融機関が日常的に収集した情報を加える形で整備される。

他方、警察当局による該当者把握からデータベース更新までには相応のタイムラグがあり、経営資源の多寡などを背景に、各金融機関における追加整備の

実態にも頻度などの差異がみられる。これらの実情が、リストに「穴」をもたらす。

また、リストの活用工程では、システムによる突合だけでなく、人間の目を介した確認がなされるのが一般的だ。この工程でのリストへのアクセスについても、誰でも幅広く利活用を可能としている金融機関と、個人情報保護等を意識し、役職などに応じてアクセス権限を設定している金融機関がみられる。後者の金融機関では、リストの目的外利用などに一定のガードがかかる一方、配置人員絞込みの中での店内検査形骸化や、権限者が限られることによる慢心

2026年の国際情勢の変化と金融システムへの影響 —上期の危機と下期の構造転換を見据えた展望—

国際政治学者

和田 大樹

一 米国・イランの 軍事衝突と国際情勢 秩序への影響

2026年2月末以降、国際社会は第二次世界大戦後に構築された安定的な秩序が大きく変容する、歴史的かつ決定的な瞬間に立ち会うこととなった。

米国とイスラエルによる対イラン大規模軍事作戦「エピック・フューリー」の実施、そしてその混乱の最中に報じられた最高指導者アリ・ハメネイ師の逝去という事態は、単なる一地域における緊張の高まりを意味するものではない。これは、人類が長きにわたる歴史的教訓を経て

到達した主権国家の不可侵および武力行使の原則的禁止という国際法の根幹が、実質的にその拘束力を失いつつあることを示唆している。

軍事的にきわめて厳しい状況に置かれたイランは、国家の存立を維持するための極限の対抗措置として、世界経済の急所であるホルムズ海峡の事実上の封鎖に踏み切った。世界の原油輸送の約3割、液化天然ガス（LNG）の約2割が通過するこの海上交通路（シーレーン）が物理的・軍事的に遮断されたことで、エネルギー供給の途絶を懸念する世界市場には、1970年代のオイルショックを想起さ

せる、あるいはそれを凌駕するほどの深刻な動揺が広がっている。

しかし、この事態が突きつけている本質的な危機は、物理的な衝突やエネルギー価格の暴騰という現象面だけではない。より深刻なのは、国際社会における共通の行動規範が形骸化し、世界がそれぞれの利益のみを唯一の指針とする予測困難な無秩序状態へと回帰しつつあるという冷厳な事実である。

現政権によるこの軍事作戦は、国連憲章が定める武力行使禁止原則、および国際法上の自衛権の要件を著しく逸脱した先制的な行動であるとの指摘を免

れない。本来であれば、国際社会はこれを主権国家に対する重大なルール違反として厳格に指弾すべき局面にある。

それにもかかわらず、欧州や日本といった米国の同盟国は、これを明確に国際法違反として批判することを避けている。各国にとつて、安全保障や経済面での対米関係を維持することは、最優先すべき現実的な国益であるからだ。この文脈において、同盟諸国が維持している戦略的沈黙は、複雑な国際政治の力学における苦渋の選択といえる。