金融庁
Financial Services Agency

金融分野におけるITレジリエンスに関する分析レポート

2026年7月

目次

第１編　はじめに

金融庁では、2019 年以降、金融機関において発生したシステム障害及びサイバーインシデントに関する分析レポートを継続的に公表してきたが、2025 年６月には、「金融分野における IT レジリエンスに関する分析レポート」として再構成して公表した。2025 事務年度においても、近年の地政学リスク、サイバーリスク及びサードパーティリスク等の高まりに加え、金融機関の業務運営及び顧客サービスが IT・デジタル基盤に一層依存する状況を踏まえ、金融分野における IT レジリエンスの強化に資する観点から、本レポートを取りまとめている。

本レポートの第２編では、2025 年度（2025 年４月～2026 年３月）における金融分野のシステム障害の分析について記載している。2025 年度においては、外部委託先に起因するランサムウェア被害、金融機関が管理するシステムに対する不正アクセス、金融機関を装ったボイスフィッシング詐欺、金融機関等を標的とした DDoS 攻撃等のサイバーインシデントが発生したほか、システム統合・更改、平時の運用・保守及び特殊作業等に起因する重大なシステム障害も引き続き認められた。これらの事案は、未然防止に加え、障害又はインシデント発生時における重要業務の継続、顧客影響の軽減及び業務の早期復旧を実現するための態勢整備、すなわち IT レジリエンスの確保・向上が、金融機関にとって重要な経営課題であることを改めて示している。

第３編では、金融機関における IT ガバナンスについて取り上げている。当庁は、2019 年６月に「金融機関の IT ガバナンスに関する対話のための論点・プラクティスの整理」を公表し、その後も調査結果レポートや事例集の公表等を通じ、金融機関との意見交換を継続してきた。2025 事務年度（2025 年７月～2026 年６月）においては、一部の地域銀行を対象としたアンケート及びヒアリングを通じ、IT 戦略、IT コスト、IT 人材、共同センターの利用実態、共同センター運営におけるガバナンス及び共同化範囲の拡大といった論点について実態把握を行った。実態把握の結果を踏まえると、IT 戦略・IT コスト・IT 人材については、相互に関連する経営課題として、経営陣がリーダーシップを発揮し、方向性や優先順位、資源配分を明確にした上で取組みを主導することが重要であり、システム共同化については、限られた経営資源を有効に活用するための重要な選択肢となり得る一方、障害時の影響波及や集中リスクが高まる可能性もあることから、効率性とレジリエンスの両面を踏まえた検討が求められる。

第４編では、サイバーセキュリティについて、「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（2024 年 10 月）」の公表後に実施したモニタリング等を通じて認められた課題及び参考となる取組みを整理している。さらに、AI によるサイバー脅威の変化への対応及びサードパーティ・サイバーセキュリティリスク管理強化に関する委託調査の結果、顧客口座・アカウントの不正アクセス・不正取引への対策強化について記載している。近年、AI 技術の進展等により脆弱性探索や攻撃手法の高度化・迅速化が懸念される中、金融機関においては、情報資産管理、脆弱性管理、サードパーティリスク管理等の各領域について更なる強化を進めるとともに、単一の対策に依拠するのではなく多層防御の考え方に基づき、侵入を前提とし、レジリエンスを含めた実効的な管理態勢を整備・運用していくことが必要である。また、フィッシング、なりすまし及びその他の手口を通じた不正アクセス・不正取引は、特定業態に限らず金融業界全体の信頼に関わる問題であり、認証の強化、モニタリングの高度化、顧客への注意喚起、業態横断的な情報共有等を含めた対策の強化が重要となっている。

第５編では、金融機関及びパブリッククラウドサービス事業者と当庁で実施した机上演習から得られた知見を整理し、「クラウド演習の進め方」として還元している。これは、パブリッククラウドサービス利用時の障害情報の取扱いに関する実態把握を目的に実施したもので、情報の取扱いに関する特性、演習にあたっての着眼点等を整理している。重要なシステムでパブリッククラウドサービスの利用を検討している金融機関等は、これを参考に、関係者と机上演習に取り組むことを通じて、パブリッククラウドサービス利用時のリスクをあらかじめ確認する等その結果を活用することが望まれる。

なお、本レポートには、補論としてシステム障害の事例集を収録しているほか、バーゼル銀行監督委員会が公表した「健全なサードパーティリスク管理のための諸原則」を取り上げ、その概要を整理するとともに、金融機関との対話を通じて把握した現状及び今後の対応に関する考え方を記載している。また、コラムとして耐量子計算機暗号（PQC）についても記載している。これらはいずれも、IT レジリエンスの確保に向け、各金融機関において計画的な対応が求められる論点である。

これらの分析は、金融業界における IT の複雑化、サードパーティへの依存の高まり、サイバー攻撃の高度化等を背景として、金融機関の経営ひいては金融システムの安定に影響を及ぼし得るリスクが一層高まっていることを改めて認識させるものである。こうした状況を踏まえ、金融機関の経営陣においては、IT リスク及びサイバーリスクを経営上のトップリスクとして認識し、自組織のガバナンス、管理態勢、投資、人材育成並びにサードパーティリスク管理について不断に見直し、その実効性を継続的に高めていく必要がある。また、対策を講じていたとしてもなお障害又はインシデントは発生し得るとの前提に立って、IT レジリエンスを強化する必要がある。当庁としては、金融分野における IT レジリエンスの強化を促す観点から、金融機関の自助及び金融業界の共助を促進するとともに、検査・モニタリングに加え、意見交換、情報共有、ガイダンスの提供、演習等の機会の提供といった公助の取組みを推進していく。

第２編　システム障害に関する分析

金融庁では、法令、監督指針等に基づき、発生したシステムの障害について金融機関から「障害発生等報告書」を受領し、事案に応じ、顧客対応や復旧状況を確認するとともに、障害の真因、事後改善策等の報告を受けている。本編では、2025 年度（2025 年４月～2026 年３月）に受領したシステム障害を分析している。

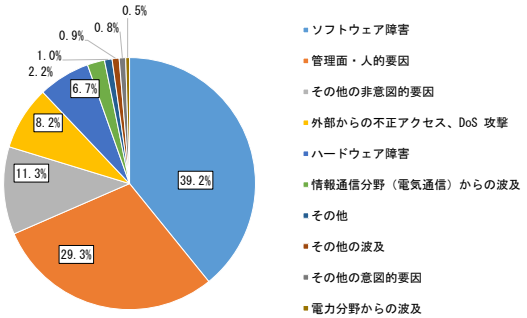
第１章　金融業界全体の障害傾向

2025 年度の業態全体[1]の障害傾向（事象別）として、「ソフトウェア障害」と「管理面・人的要因」による障害が全体の約７割を占めている[2]（図表１）。

「ソフトウェア障害」の一例を挙げると、外国送金に係る新たな電文方式への対応に向けたシステム改修において、仕様の複雑化、関係者間の認識のずれや、網羅的な無影響確認テストが十分ではなかったことから、リリース後、一部の送金処理や対外電文の発信が不能となり、電文処理が滞留する事案が報告されている（本編第２節）。

「管理面・人的要因」について、外部のストレージサービス提供事業者においてハードウェア障害によりストレージサービスの一部が利用不能となったことに起因して、決済の一部が利用できない事案が報告されている（本編第３節第１項）。また、海外データセンターのネットワーク運用を委託している体制の下で、委託元の許可を得ないメンテナンス作業が実施され、冗長構成機器に誤設定が配信されてネットワーク機器が全台通信不能となった事案が報告されている（本編第３節第２項）。さらに、災害対策環境の起動試験においてATM から災害対策環境への通信遮断が未実施であったために一部の ATM 取引に影響を及ぼしたことに加えて、障害対応態勢及び指示系統の不備により、顧客対応が遅延する等の事案が報告されている（本編第４節第１項）。

図表１「障害事象別割合（全業態）」



[1] 本集計期間（2025 年度）に金融機関から報告されたシステム障害の件数は、約 1,600 件であった（金融機関：預金取扱等金融機関（主要行等、地域銀行、信用金庫・信用組合等）、保険会社等、金融商品取引業者等、貸金業者、資金移動業者等（資金移動業者、前払支払手段発行者）、暗号資産交換業者等）。

[2] 障害報告において金融機関が選択した障害事象を集計した結果に基づく。また、2026 年３月時点で金融機関にて調査中・未記入となっている約 100 件については集計の対象外としている。

第２章　主な障害事例

2025 年度の主なサイバーインシデントを端緒としたシステム障害には、外部委託先が不正アクセスを受け、端末・サーバー上のファイルが一部暗号化され個人情報等が窃取されたランサムウェア被害の事案、金融機関が管理するシステムに対する不正アクセスにより数日間にわたり第三者が顧客情報へアクセスできる状態となり情報流出の可能性がある事案、金融機関を騙るボイスフィッシング詐欺[3]事案等がある。

一方、その他の原因によるシステム障害には、送金処理や対外電文の発信が不能となり電文処理が滞留した事案、外部ストレージサービスの電源喪失に起因して決済処理が滞留し支払い処理が不能となった事案、海外データセンターのネットワーク機器に対する未承認メンテナンスを契機として冗長化されている機器へ誤設定が配信されネットワーク機器が全台通信不能となった事案等がある。

金融機関の経営陣は、こうした 2025 年度の傾向も踏まえ、サイバーリスクと IT リスクをトップリスクとして捉え、対策を講じていてもなおインシデントが発生し得るという前提に立ち、重要業務の継続・早期復旧等を実現するための態勢整備を主導して強化する必要がある。

以下では、システム障害を主な端緒（①サイバー攻撃・不正アクセス等の意図的な行為、②システム統合・更改プロジェクト、③システムの日常的な保守・運用、④システムのプログラム更新等の普段と異なる特殊作業）ごとに特徴的な事案を挙げ、それぞれの課題を分析している。

第１節　サイバー攻撃・不正アクセス等の意図的なもの

第１項　マルウェア感染に係る事案

2025 年度においては、金融機関の外部委託先が不正アクセスを受け、外部から侵入した第三者により端末及びサーバーに保存していたファイルが一部暗号化され、個人情報等が窃取されるランサムウェア被害の事案が発生している。本件では、第三者がネットワーク機器の脆弱性を悪用して内部ネットワークへ侵入し、導入していたセキュリティソフトが無効化されていた。

また同じく 2025 年度においては、金融機関が管理するシステムが不正アクセスを受けたことにより、数日間、同システムに侵入した第三者がシステム内の顧客情報にアクセスできる状態になっていたと推測され、外部に漏えいした可能性がある事案が発生している。原因として、システムの脆弱性等が挙げられている。

以上を踏まえ、外部委託先起因のランサムウェア被害が継続して発生していることから、金融機関として、委託先に提供する情報の重要度や漏えい時の影響を踏まえた委託業務の重要度見直し、再委託先を含む統制の実効性確保（実地調査・第三者評価

[3] 電話を起点にフィッシングサイトへ誘導し認証情報を窃取、不正送金に至る手口

等によるチェック体制強化）を進めるとともに、委託契約（覚書等）におけるインシデント報告義務や事業継続対応等の委託先の対応義務を明確化することが必要である。あわせて、VPN／SSL-VPN 等のリモートアクセスを含む脆弱性管理の高度化（迅速なパッチ適用、設定の適正化、ログ確保）、多要素認証や特権アカウント管理の強化、セキュリティ監視・検知能力の強化、インシデント発生時の対応手順の再評価・強化、規程見直しと社内教育、セキュリティ担当部門の強化等により、侵入の防止・早期検知・封じ込め・復旧の各局面における対策の実効性を高めることが重要である。

第２項　ボイスフィッシング詐欺に係る事案

2025 年度において、金融機関を騙るボイスフィッシング詐欺とみられる事案が発生している。ボイスフィッシング詐欺の手口は、①攻撃者が金融機関の担当者をかたり被害者（企業又は顧客）へ電話をかけ、メールアドレス等を聞き出す（自動音声の場合あり）、②当該メールアドレス宛にフィッシングメールを送付し、電話で指示をしながらフィッシングサイトへ誘導してインターネットバンキングの契約者情報、パスワード等を入力させて窃取する、③窃取した認証情報を用いて不正送金を行う、という流れ等で実施されている。背景として、AI による偽音声・偽装技術の高度化、自動音声と偽担当者を組み合わせた二段階の誘導、電話のリアルタイム性に起因する判断ミスの誘発、即時振込機能の悪用等が挙げられる。

こうした事案を踏まえると、金融機関においては、顧客が不審な連絡や誘導に適切に対応できるよう、注意喚起や相談受付態勢の整備を継続的に行うとともに、不正送金の未然防止の観点から、認証・取引時のモニタリングやリスクに応じた取引管理を強化していくことが重要である。あわせて、顧客対応部門を含め、平時からの周知・訓練等を通じて、被害の拡大防止に向けた態勢の実効性を高めることが求められる。

第３項　DDoS 攻撃に係る事案

DDoS 攻撃に係る事案については、2025 年度においても一定数の発生が確認されている。具体的には、IoT ボットネットを利用し、UDP フラッド攻撃や HTTP フラッド攻撃等、複数の攻撃手段が確認されているため、金融機関においても DDoS 対策を見直す必要があり、対策を行っても被害を受ける可能性があることを前提とした備えが必要となる。これらの対応[4]として、金融 ISAC 等を通じた被害事例の情報収集分析及び警戒継続を行い、ボットに感染している端末等が多い国やドメインからのアクセス制限、

[4] 例えば、国家サイバー統括室「DDoS 攻撃への対策について（注意喚起）」、（2025 年２月４日 https://www.cyber.go.jp/pdf/news/press/20250204_ddos.pdf）

DDoS 対策ツール[5]の導入や攻撃元に対するブロック対応の高度化[6]といった防御対策はもとより、相次ぐ攻撃に対して、DDoS 攻撃の早期検知・復旧や業務継続のための態勢整備に関する不断の取組みが課題となっている。また、DDoS 攻撃の通信量の増加に対するリスク低減に向けた対策として、プロバイダ側と連携した態勢整備等が必要である。

第２節　システム統合・更改等に伴って発生したシステム障害

金融機関のシステム統合・更改は、障害が発生した場合の影響が大きく、かつシステムの統合又は更改に必要な知識の専門性が高いため、プロジェクト遂行の難度が高い。こうしたプロジェクト特性を背景に、プロジェクト特性に基づいた再委託先を含むプロジェクト管理態勢の整備、システム仕様書等の開発文書の整備、有識者の適切な配置によるレビュー体制の整備等が金融機関における課題として挙げられる。

2025 年度においては、外国送金に係る新たな電文方式への対応に向けたシステム改修を実施したところ、リリース後に一部の送金処理等に支障が生じ、電文処理が滞留する事案が発生している。

本件では、仕様の複雑化や仕様の見直し対応の中で、関係者間の認識統一が図られず不要な処理が追加され不具合につながった。また、網羅的な無影響確認テストが十分ではなかったことから、当該不具合を事前に検知できなかった。

本件の再発防止に向けては、システム改修に当たり、障害発生時の想定される影響を踏まえたプロジェクト体制構築、無影響確認テスト基準の明確化等を行い、検証態勢を強化することが必要である。

第３節　日常の運用・保守等の過程の中で発生したシステム障害

第１項　サードパーティの提供するサービス等の要因

近年、サードパーティの提供するサービスの障害により、複数の金融機関に影響を及ぼす事案が生じており、こうした障害を想定した代替手段の確保やサードパーティとの継続的な情報連携が求められている。

2025 年度においては、外部のストレージサービス提供事業者においてハードウェア障害によりストレージサービスの一部が利用不可となったことに起因して、決済の一部が利用できない事案が発生している。

---

[5] 例えば、WAF（Web サイト上にあるアプリケーションの通信状態を監視し、異常があればすぐに報告や遮断をすることができるツール。「Web Application Firewall」の略。）や IDS（サーバーやネットワークの外部との通信を監視し、攻撃の侵入や試行等不正なアクセスを検知するツール。「Intrusion Detection System」の略。）、IPS（不正を検知して通信を遮断するシステム。「Intrusion Prevention System」の略。）、UTM（複数の異なるセキュリティ機能を一つのハードウェアに統合し、集中的にネットワーク管理を行うツール。「Unified Threat Management」の略。）といったツール。

[6] 例えば、DDoS 対策ツールのバージョンアップ適用、ネットワークトラフィックを制限するレートリミットの導入等。

サードパーティの提供するサービスに起因する障害であっても、決済処理全体への波及を抑止できるよう、障害発生時に影響箇所を早期に特定可能とする監視設定の見直しを行うとともに、その結果に基づき影響箇所を自動的に切り離す機能を実装するなど、検知から復旧対応までを迅速化する運用・機能面の整備が必要である。

第２項　冗長構成が機能しない等の障害

従前から、勘定系システム等の重要システムにおいて、冗長化設計の実効性確保が不十分なことにより、障害・メンテナンス時にサービス停止へ波及する事案が発生している。

2025 年度においては、海外のデータセンター内に設置されたネットワーク接続用機器が全台通信不能となり、外部との通信が不通となり、さらに、セカンダリーデータセンターへの切替に時間を要したことから、重要なアプリケーションの一部が遅延した事案が発生している。本件では、ネットワーク運用管理をサービス提供ベンダーに委託し、当該ネットワーク機器の管理はサービス提供ベンダーから提携先に再委託している体制のもと、海外の営業時間中に、委託元の許可を得ずに再委託先がメンテナンス作業を実施したところ想定外の挙動が発生し、冗長構成を有する機器の全台に誤った設定情報（初期設定値）が配信され、結果として全台が通信不能となった。

以上を踏まえ、委託先に対する監査・統制を厳格化することによる委託先管理の強化を行うとともに､セカンダリーデータセンターへの切替テストを実施する等により、冗長化設計の実効性を確保することが必要である。

第３項　システム障害発生時の復旧に関する不芳事案

2025 年度においては､国内勘定系システムにおいて入出力装置の不具合による障害が発生した後、待機系への切替や再起動による復旧に時間を要し、結果として後続処理にも影響が生じた事案が発生した。

システム障害発生時においては、障害箇所を早期に把握し、影響範囲の拡大を抑止するための検知・遮断態勢を整備するとともに、障害発生時の切替え・復旧手順について、実効性の検証を含めた見直しを行うことが必要である。

第４節　プログラム更新、普段と異なる特殊作業等から発生したシステム障害

第１項　設定ミス・作業の誤り

2025 年度においては、勘定系システムにおいて、本番稼働中に実施した災害対策環境に関する作業を契機として、一部の ATM 取引に障害が発生したほか、それに対する問い合わせ対応のひっ迫により、顧客対応が遅延し多数の苦情が発生する事案が発生している。

本件では、本番稼働中に実施した災害対策環境に関する作業において、引継ぎ不足

や考慮漏れにより、ATM から災害対策環境への通信遮断が実施されていなかったことに加えて、例年の災害対策訓練と同様との誤認から、本番環境リスクを適切に反映できず、本来は経営承認が必要な案件であったにもかかわらず、部内決裁のみで実施され、十分な検証が行われなかった。さらに、障害対応態勢及び指示系統の不備等により、経営へのエスカレーション、関係者への情報共有及び顧客対応が遅延した。

以上を踏まえ、本番システムへの影響を十分に踏まえた変更管理及びリスク評価を徹底するとともに、障害発生時における役割分担、エスカレーション、情報共有及び顧客対応を含む対応態勢の整備を進め、あわせて、平時から研修・訓練を通じて、その実効性を高めていくことが重要である。

第３編　IT ガバナンス高度化に係る実態把握

金融庁では、2019 年６月に「金融機関の IT ガバナンスに関する対話のための論点・プラクティスの整理」（以下、「IT ガバナンスの論点」という。）を公表した。その後、2020 年から 2022 年にかけて、IT ガバナンス等に関する調査結果レポートと事例集を毎年公表した。2023 年６月には、IT・デジタル技術を活用した金融機関のデジタルトランスフォーメーション[7]（以下、「DX」という。）に関して相応の進展が見られたこと等を踏まえ、DX の考え方・着眼点を盛り込み、その内容を充実させるよう「IT ガバナンスの論点」を改訂した。

これらの取組みをさらに推進するため、2025 事務年度は、一部の地域銀行に対して、（１）IT ガバナンスの主要項目、（２）システム共同化の活用の２つのテーマのもと、６つの論点（①IT 戦略、②IT コスト、③IT 人材、④共同センター[8]の利用実態、⑤共同センター運営におけるガバナンス、⑥共同化範囲の拡大）について、アンケート及び個別ヒアリングを行い、実態把握[9]を行った。

本編は、当庁が実施した一部の地域銀行に対するアンケート及びヒアリング結果等に基づき、IT ガバナンス高度化に資する論点や参考事例を整理したものである。したがって、本編は地域銀行全体の傾向や優劣を示すものではなく、監督上の一律の基準やチェックリストを示すことを意図するものでもない。各金融機関が自らの規模、経営戦略、共同化の状況、リスク特性等を踏まえて、創意工夫を進めていく際の参考として活用してもらうことを想定している。

第１章　IT ガバナンスの主要項目に係る実態把握結果

第１節　IT 戦略

今回当庁が実施したアンケートの全回答において、経営戦略と IT 戦略を紐付けている、あるいは経営戦略の実現・課題解決のため IT 施策を実施しているなど、経営陣が経営戦略の策定において IT 戦略にも関与していることがうかがえた。

一方、課題としては、中期経営計画の３年間の枠組みにとらわれない長期的な IT 戦略の必要性や、IT 投資の検証とリスク管理の両面からシステム案件を評価するスキームの継続的な改善等が挙げられている（図表１）。

---

[7] デジタルトランスフォーメーションとは、デジタル技術を活用して、顧客や社会ニーズをもとにサービスやビジネスモデル等を変革し、競争上の優位性を確立することを指す。

[8] 複数の金融機関が、勘定系システム等について、共同利用型又は共通性の高いシステム基盤・アプリケーション・運用サービス等を利用する枠組みをいう。

[9] 公益財団法人金融情報システムセンターが金融機関等に対して実施している「令和７年度金融機関アンケート（調査基準日 2025 年３月 31 日）」（以下、「FISC アンケート」という。）のデータの一部を当庁で集計して活用。また、当庁が地域銀行に対して 2025 年８月に実施した「共同システム利用に係る契約状況に関するアンケート」も活用。

（図表１）IT 戦略に関する課題例

- 中期経営計画の３年間の枠にこだわらず、より実効性のある長期的な IT 戦略の策定が必要。
- IT 投資検証とリスク管理の両面からシステム案件を検証できるスキームの継続的な改善が課題。
- 現在、システムアーキテクチャを策定し、技術標準化を推進中。今後はクラウド・AI 導入に向けたアーキテクチャの刷新が必要。
- 各部門の要望に沿ったシステム導入が中心で、組織的な IT 戦略・方針が未整備。

IT 戦略を推進するために必要な経営陣によるリーダーシップ発揮の事例としては、DX 戦略ロードマップの策定・公開やシステム投資に係る予算枠の確保等が見られる（図表２）。

（図表２）経営陣のリーダーシップ事例

- DX 戦略ロードマップをグループ共通指針として策定・公表し、技術動向予測を踏まえ環境変化に応じた戦略を策定。
- システム投資・経費予算では、柔軟な対応を可能にする予算枠を確保。
- IT・デジタルを経営に活用してビジネスモデル変革につなげることを目指し、中期経営ビジョン・経営計画を策定。
- IT・デジタル化対応を経営の最重要課題の一つとして位置付け、中期経営計画の中で個別の戦略を立案し、その実行状況を経営会議及び取締役会にてモニタリング。
- IT 戦略、システムリスク管理強化、システム投資等について、経営陣の認識及び関与のもと、適切な対応方針を協議する委員会を設置。

IT 戦略において、DX の推進につながる「生成 AI・データ利活用」や、それを実現するために必要となる「IT 人材の確保・育成」を重点施策として位置付けている地域銀行が多く見られた（図表３）。

（図表３）IT 戦略における重点施策

カテゴリー	重点施策	回答割合
業務効率化	営業店・本部業務の効率化	16.7%
顧客利便性向上	個人向けアプリ・法人ポータルの機能拡充	27.8%
DX・新事業創出	生成 AI・データ利活用	55.6%
	地域社会の DX 支援	22.2%
勘定系システム更改関連	次期システムの検討、システム高度化、共同センター価値拡大	44.4%
システムリスク管理高度化	サイバーセキュリティ	22.2%

IT 人材の確保・育成	IT 人材（デジタル人材を含む）の育成	61.1%

経営層向けの IT に係る報告や勉強会のテーマとしては、「生成 AI」の割合が最も多く、次いで「ブロックチェーン（デジタル証券等）」となっている。また、報告・勉強会の実施割合が高いテーマほど、そのテーマに対応しないことを機会損失リスクとして認識している割合も相対的に高い傾向がうかがえる。これらの結果を踏まえると、経営層が新技術の動向や他社の活用事例に関する情報を把握する機会を持つことは、IT 戦略の検討・論点整理に資する可能性を示唆している（図表４）。

（図表４）経営層向けの IT に係る報告や勉強会のテーマと機会損失リスクの認識

カテゴリー	報告・勉強会の実施割合	機会損失リスクの認識割合
生成 AI	94.4%	38.9%
ブロックチェーン（デジタル証券等）	44.4%	16.7%
地域通貨（地域銀行が発行・運営に関与する電子マネーやポイント等）	38.9%	5.6%
量子コンピュータ	33.3%	16.7%
ステーブルコイン	22.2%	11.1%
その他	50.0%	11.1%

KPI は、IT 戦略に基づく重点施策の実効性を確認するための有効な手段の一つであり、今回当庁が実施したアンケートにおいて KPI を設定している銀行は半数であった。KPI の内容としては、「IT 人材の確保・育成」や「顧客利便性向上」に関する項目を設定している銀行が多く見られた（図表５）。

（図表５）IT 戦略に関する KPI の事例

カテゴリー	KPI の事例
業務効率化	・ 店頭タブレットによる業務の所要時間 ・ 営業店において削減された事務量
顧客利便性向上	・ 法人向け IB 契約者数、個人向けアプリ契約者数 ・ 全振込取引における電子取引利用率 ・ 電子交付サービス利用者数
DX・新事業創出	・ チャットボットによる行内照会業務の削減時間 ・ DX 支援コンサルティング件数

	・ 従業員向けAIチャットの利用者数 ・ 年度予算額に対する戦略的DX投資の実績額 ・ データ分析モデルの開発件数
IT投資の適正配分	・ 競争領域への投資割合
システムリスク管理高度化	・ 金融庁サイバーガイドラインにおける基本的な対応事項の遵守率 ・ システム部門起因の開発ミス件数、運用ミス件数
IT人材の確保・育成	・ IT人材のスキルレベル毎の割合 ・ DX案件従事経験者数 ・ セキュリティ担当者数 ・ 行内研修受講者数

IT戦略の策定に当たっては、各部門の要望に沿った個別案件を積み上げるだけではなく、経営戦略の実現に向けて目指すべきビジネスの姿や、それを支えるデータ・システム基盤、許容するリスクの水準等を整理した上で、中長期的な方向性と重点施策を明確化していくことが有用と考えられる。

また、重点施策の実効性を確保する観点からは、施策の進捗確認にとどまらず、追加投資、計画修正、優先順位の見直し等の経営判断に資するKPIを設定し、継続的に活用していくことが有用と考えられる。

第２節　ITコスト

FISCアンケート結果（2025年）に基づき、地域銀行におけるITコスト[10]の使用目的別割合を見ると、「保守・維持（基幹系システム以外の周辺・サブシステム）」が34.4%を占め、最も高い割合となっている。次いで「保守・維持（基幹系システム）」が22.8%で２番目に高い一方、「新規開発（前向き）」は14.8%であり、相対的に低い水準にとどまっている（図表６）。

また、2022年と2025年を比較してみると、「保守・維持（基幹系システム以外の周辺・サブシステム）」の割合が増加していることが確認できる。周辺領域の拡張は利便性向上や業務高度化に資する一方で、保守・維持費用が継続的に発生することから、コスト増加の要因となっている可能性が示唆される。

一方、新規開発（前向き）、新規開発（ディフェンシブ）、基幹系システムの保守・維持、共同システムセンター分担金は総じて横ばいであった。

[10] P/Lの金額（人件費、物件費（減価償却費を含む）、税金の合計）によるものとする。

（図表６）IT コストの使用目的別割合

目的	2022 年	2025 年	増減
新規開発（前向き）	14.4%	14.8%	0.4%
新規開発（ディフェンシブ）	10.2%	9.1%	▲1.1%
保守・維持（基幹系システム）	23.0%	22.8%	▲0.2%
保守・維持（基幹系システム以外の周辺・サブシステム）	31.4%	34.4%	3.0%
共同システムセンター分担金	21.0%	19.0%	▲2.0%

＜IT コストを目的別に分類する際の参考事例＞

新規開発（前向き）	・売上拡大、コスト削減等の収益拡大につながる新規システム構築・既存システム改修経費
新規開発（ディフェンシブ）	・社内外向けのセキュリティ・安全対策のためのシステム関連経費 ・法改正・規制見直しへ対応するためのシステム関連経費 ・BCP 対策のためのシステム関連経費
保守・維持（基幹系システム）	・システム運用費、ライセンス費用等の定常的に支出される経費のうち、基幹系システムに関する経費
保守・維持（基幹系システム以外の周辺・サブシステム）	・システム運用費、ライセンス費用等の定常的に支出される経費のうち、基幹系システム以外の周辺・サブのシステムに関する経費
共同システムセンター分担金	・共同センター加盟機関が共同センターに支払う関連経費（外部接続先システム（全銀システム、統合 ATM、ANSER 等）、外部センターの利用料等）

「新規開発（前向き）」の割合が大きい地域銀行では、中期経営計画において DX 対応等の方針が明確に示されており、予算を確保しやすいとの回答が見られた。一方で、「新規開発（前向き）」の割合の小さい地域銀行では、過去の合併案件に伴う償却費に予算が充当されているほか、「新規開発（ディフェンシブ）」に該当する大規模システム更改案件にコストを要している事例が見られた（図表７）。この点、ディフェンシブ案件や更改案件は、短期的には前向き投資余力を圧迫し得る一方で、中長期的には、システムの安定性確保、システムの複雑化・肥大化の抑止、将来の機動的な開発やデータ利活用を可能とする基盤整備としての側面があると考えられる。

（図表７）新規開発（前向き）案件割合の要因

新規開発（前向き）案件割合が大きくなっている要因	・ 中期経営計画で DX に対する積極投資方針を明確にしているため、予算を確保しやすい。モダナイゼーションを含めた大型案件が増えてきている。 ・ DX 投資や銀行の P／L 向上に資する案件を含めた成長投資に

	ついて前中期経営計画より注力している。 ・ 顧客チャネル並びに業務の高度化・効率化に向けて既存システムのコスト抑制と戦略的なシステム投資を実施している。
新規開発（前向き）案件割合が小さくなっている要因	・ ゼロトラスト PC 端末導入への投資をセキュリティレベル向上の観点からディフェンシブ投資として計上している。 ・ 次期勘定系の更改、大規模システム更改、システム保守等に予算及び工数を要している。

FISC アンケート結果に基づき、地域銀行における IT コストの 2022 年対比 2025 年の増減を見ると、IT コストが増加している銀行が 63.2%となっている。これを「新規開発（前向き）」との関係で見ると、IT コストが増加し「新規開発（前向き）」も増加している銀行の割合が 32.6%と最も多く、次いで IT コストは増加しているが「新規開発（前向き）」が減少した銀行の割合が 29.5%となっている。

一方、IT コストが減少している銀行が 36.8%となっており、そのうち、「新規開発（前向き）」が増加している銀行は 14.7%あり、こうした銀行は非戦略領域の見直し等を通じて、前向き投資余力を捻出している可能性がある。

（図表８）IT コスト増減と新規開発（前向き）増減

IT コスト増減 割合		内：新規開発（前向き）増減 割合	
増　加	63.2%	増　加	32.6%
		不　変	1.1%
		減　少	29.5%
減　少	36.8%	増　加	14.7%
		不　変	1.1%
		減　少	21.1%

IT コスト分析については、新規開発（前向き）等使用目的別の割合やその推移に加え、IT コスト総額の増減、保守・維持費用等の継続的に発生する費用の割合、主要案件の内容及び IT 投資額の状況を合わせて確認し、戦略領域への資源配分の実態を把握することが有用と考えられる。

第３節　IT 人材

地域銀行における IT 人材の確保・育成に関する取組みについて、2021 年と 2025 年の FISC アンケート結果を比較すると、取組みを実施している割合が半数未満であった項目が解消されるなど、一定の進展が見られる（図表９）。

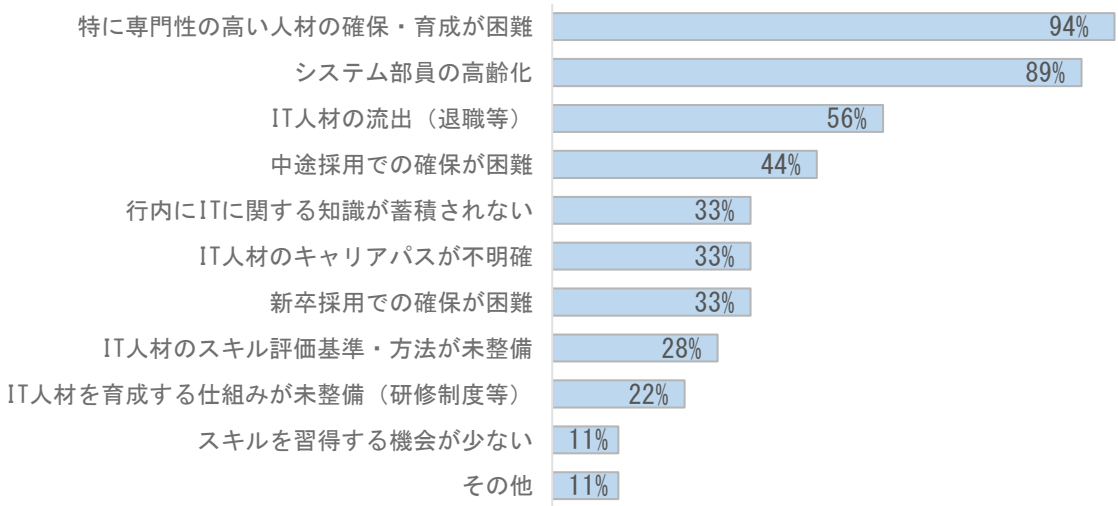
一方で、2023 年と 2025 年を比較すると、複数の項目（中長期計画、キャリアパス等）において、実施割合が横ばいで推移しており、取組みが十分に進展しているとは言い難い状況にあることがうかがわれる。

（図表９）IT 人材の確保・育成に関するアンケート結果

質問事項	2021 年	2023 年	2025 年
IT 人材を確保・育成するための中長期計画を策定しているか	58.0%	64.3%	64.9%
IT 人材のキャリアパスを策定しているか	48.0%	54.1%	56.7%
IT 人材のスキルを評価する基準や方法を定めているか	47.0%	50.0%	59.4%
IT 人材を育成するための研修制度を定めているか	46.0%	50.0%	53.1%
IT 人材を確保するための採用施策（IT 専門職としての採用や IT 部門におけるインターンシップ受入等を含む）を実施しているか	―（アンケート未実施）	63.3%	74.0%
IT 人材を確保するため、IT 専門職としての新卒採用を実施しているか	―（アンケート未実施）	44.9%	52.1%
IT 人材を確保するため、IT 専門職としての中途採用を実施しているか	―（アンケート未実施）	77.6%	85.4%
全社員を対象に IT・デジタルのリテラシー向上のための施策を実施しているか	79.0%	93.9%	93.8%

IT 人材に関する課題として、「専門性の高い人材の確保・育成」「システム部員の高齢化」が多く見られた（図表 10）。

（図表 10）IT 人材に関する課題



「専門性の高い人材の確保・育成」「システム部員の高齢化」への対応として、以下のような取組みが見られる（図表 11）。

専門性の高い人材の確保・育成については、セキュリティ人材やデジタル人材の確保に苦慮しているとの声があり、中途採用だけでは確保できないため自前での育成の強化や、

出向・共同化等を通じた外部と連携した育成に取り組んでいる金融機関も見られる。

また、システム部員の高齢化については、シニアが働き続けられる制度の整備、若手採用による年齢構成の適正化、スキル継承のための体制・仕組みの整備といった取組みが確認された。高齢化への対応は、単に年齢構成を是正するだけでなく、保有スキルの可視化や計画的なスキル移転を通じて、属人的な運営を見直していく観点からも有用である。

（図表 11）IT 人材の課題への取組み

専門性の高い人材の確保・育成が困難	・ サイバー人材は中途採用が難しく、育成に時間を要するため、新卒採用を中心に採用を進めている。デジタル人材については、必要数は確保できているが、当行が提示できる年収では期待するスペックの人材の採用が難しいため、一定程度要件を緩和しつつ広く採用し、育成していく方針としている。 ・ データサイエンティストは中途採用が難しく、現状では外部パートナー（ベンダー、コンサルティング会社等）の支援を活用しつつ、社内育成も進める方針としている。 ・ セキュリティ人材の育成は OJT に加え、外部研修への参加、資格取得の推進を実施している。加盟する共同センターの中でセキュリティ対策に共同で取り組むことで人材不足を補う予定。 ・ デジタル人材はベンダー等と伴走し、CoE（Center of Excellence）組織が中心となり、案件を進めながら育成している。 ・ セキュリティエンジニアは、コンサルティング会社の伴走支援等により、人材育成を進めている。 ・ セキュリティ人材は中途採用も行っているが、有資格の若手人材も含まれ、十分な実務経験を有する専門人材とは言い難いため、募集要領を見直しながら採用を継続。育成は外部出向・研修を中心としている。 ・ サイバーセキュリティ、データサイエンティスト等の人材について、中途採用（オファー型、専門領域型等）に加え、リファラル採用[11]やアルムナイ採用[12]といった多様な採用制度の活用や、金融 ISAC 等の外部専門組織への参加に取り組んでいる。
システム部員の高齢化	・ 55 歳での専任転換制度を段階的に廃止し、処遇に起因した離職の抑制を図っている。 ・ 専門職制度を導入し 55 歳以降も有識者が活躍できる体制を整備するとともに、60 歳以降もスキルを勘案し嘱託再雇用を実施。並行して、ベテランから新規配属者へのスキル移転を計画的に進めている。

[11] 職員からの紹介による採用手法。

[12] 過去に在籍していた元職員を再雇用する採用手法。

	・ 人事ローテーションや中途採用に加え、60 歳以上の嘱託採用でスキル継承を継続して行っている。 ・ 協力会社も含め、社員の若返りを計画。新卒社員の採用枠の拡大も検討している。 ・ 中途採用や若手行員の人事異動により若返りを図っている。更なる若返りのため行内公募を実施する予定としている。 ・ 従来の「一子相伝」的な引継ぎをやめ、業務と担当を紐付けない開発体制へ移行し、幅広い業務対応を可能にする体制を構築している。 ・ 協力会社への外部委託や、自動コーディングの研究を視野に入れて検討を進めている。

FISC アンケート結果に基づき、IT 人材の中途採用実績（過去３年間）を集計した結果、１行当たりの平均は 5.4 名であった。そのうち、７名以上採用している地域銀行では、IT 人材の「中長期計画」「キャリアパス」を策定している割合が高い傾向が見られた（図表 12）。これは、中長期的に必要な人材像や処遇・育成の方向性を明確にしている地域銀行ほど、採用活動を進めやすい可能性があることが示唆される。もっとも、個々の金融機関の規模や戦略、採用市場の状況等によって事情が異なる点に留意が必要である。

（図表 12）過去３年の中途採用者数

中途採用者数	銀行数	IT 人材の中長期計画の策定状況	IT 人材のキャリアパスの策定状況
０～３名	59 行	54.2%	44.1%
４～６名	16 行	62.5%	56.3%
７名以上	23 行	91.3%	87.0%

IT 人材に関する「中長期計画」「キャリアパス」の具体的な内容は、以下のとおりであった（図表 13）。

中長期計画に関しては、経営陣が関与して IT 人材の確保・育成を経営戦略に直結するテーマと位置付け、人材育成制度を整備し、多様な採用やキャリアパスにより人材確保を図ろうとする取組みが見られた。

また、デジタル人材には、新たなビジネスの推進力やデータ活用力等、従来の IT 人材とは異なるスキルが求められる点を踏まえ、デジタル人材認定制度の整備や、従来の IT 人材からデジタル人材へのシフトを計画する地域銀行が確認された。

キャリアパスに関しては、スキルレベル制度の導入等によるキャリアパスの制度化、キャリアパスの多様化の促進、キャリアと育成が紐づいた仕組みの整備といった取組みが見られた。

（図表 13）中長期計画・キャリアパスの内容

中長期計画	・ 中期経営計画策定時に必要な人数を算出し、不足分についてキャリア採用を実施。また、行員が IT 部門へ転籍できる制度があり、応募者の意欲や資質を考慮しながら選考を実施している。 ・ 中期経営計画において、IT 人材に関する KPI（IT 資格保有者比率、中途採用者数等）を設定している。 ・ 経営会議において、システム部門から IT 人材の育成の取組みについて報告している。 ・ デジタル人材（コア・ミドル・ベース）認定制度で育成人数の目標値を定め、育成を実施している。 ・ ①育成実績の把握と計画の策定、②人材の育成に必要な外部研修等を整理した教育研修ロードマップの策定、③ロードマップに基づく実績の評価・計画の見直しの観点で、IT 人材育成の PDCA サイクルを運用している。中途採用だけでなく、新卒採用についても IT・デジタル枠を新設する予定としている。あわせて、DX に係るリーダー人材を４つのカテゴリー（①DX の BPR 企画、②データサイエンス、③DX インフラ整備、④DX 支援）に区分し認定を行っている。 ・ IT 戦略の中で IT 人材に係る中長期計画を策定し、システム企画人材からデータ・AI 活用を企画する人材へのシフトを計画している。
キャリアパス	・ IT マネジメントコースと IT テクニカルコースに分けて、年齢別に習得すべきスキル、役職を整理している。IT 人材のスキルレベル制度の中で必要なスキルや資格取得を明示している。 ・ 経験年数ごとにスキルレベルを設定し、その達成に必要な資格取得や受講研修を整理している。 ・ スキル評価項目を策定し、これに基づく評価を実施している。 ・ ジョブスキルアセスメントを実施し、ジョブごとにスキルレベルチェックシート兼育成計画書を作成している。 ・ IT スキル診断シートを作成し、各人のスキルレベルを評価した上で、配属チームの検討や処遇の参考としている。 ・ システムの内製化を進めており、開発、運用、セキュリティ等、様々な分野においてキャリアパスを準備している。

IT 人材については、IT 専門職としての採用等、人材確保に向けた取組みに一定の進展が見られる一方で、専門性の高い人材の確保・育成や既存人材の高齢化といった課題は依然として残っている。

こうした状況を踏まえると、IT 人材をシステム部門内の課題としてのみ捉えるのではなく、経営戦略及び IT 戦略の実現を支える経営資源として位置付け、経営陣が積極的に関与

する形で、自組織で保有・強化すべき能力と、外部人材、外部委託先、共同センター等との連携により補完すべき能力を整理した「人材ポートフォリオ」を設計する視点で捉えることが期待される。その上で、中長期的に必要となる人材像やスキルを明確化し、計画的な育成・評価・キャリアパスの整備を進めていく必要がある。

その際、全ての開発・運用機能を一律に内製で保有することを目指すのではなく、競争領域か否か、顧客への影響の大きさ、システム改修の頻度、求められる専門性等を踏まえ、自組織で担うべき領域と外部活用が適する領域を見極めることが重要である。

特に、キャリアパスについては、専門分野の高度化や新技術の習得等による専門性の向上を図るルートに加え、IT 企画、投資管理、経営管理等の役割でも活躍できるよう整備することで、IT 人材の活躍の場が広がり、定着や後継者育成の観点からも有用と考えられる。

IT 戦略・IT コスト・IT 人材に関する各論点を総合すると、これらは相互に関連する経営課題であり、個別に対応するのではなく、一体的に検討・推進していくことが望まれる。経営陣がリーダーシップを発揮し、方向性や優先順位、資源配分を明確にした上で取組みを主導することが、IT ガバナンス高度化の観点から重要であると考えられる。

第２章　システム共同化の活用に係る実態把握結果

第１節　共同センターの利用実態

地域銀行では、共同センターへの加盟・利用が９割を超えており、IT コストの削減やリソースの最適化が図られている。一方、共同センター利用のリスクとして、「障害影響の拡大」「開発スキルの低下」「開発自由度の低下」等が挙げられた（図表 14）。

（図表 14）共同センター利用により高まるリスク

障害影響の拡大	・　インシデントが他行にも影響を及ぼすリスク。 ・　委託先の管理体制に起因し、システム障害発生時の対応が遅延するリスク。 ・　銀行別処理（ロジック）に起因する不具合発生のリスク。 ・　緊急事態発生時の対応が遅れるリスク。 ・　共通基盤に対する障害が発生した際に影響範囲が拡大するリスク。
開発スキル低下	・　システムの開発スキルを喪失するリスク（ブラックボックス化の進行）。 ・　自行開発要員の開発力が低下するリスク。
開発自由度低下	・　開発に係る制約事項が増え、各行の自由度が低下するリスク。 ・　加盟行間での仕様調整や意思決定に時間を要するリスク。
その他	・　委託業務における不正や、サービスレベルの低下により、情報資産の安全性や信頼性が損なわれるリスク。

他の共同センターへの乗換えが困難となる技術的要因について確認した結果、過去の実績やシステムの著作権を自行で保有していることから、「特になし」との回答が最も多かった。一方で、「ベンダー仕様の把握」「リソース不足」「データ移行」の観点から困難との回答もあり、仕様の非開示により移行難度が高まるといった実態面での乗換えの難しさがうかがえた（図表 15）。

（図表 15）他の共同センターへの乗換えが困難となる技術的要因

特になし	・ 他の共同センターへ移行した銀行が複数実在している。 ・ システムの著作権を銀行で保有しており、乗換えの際にベンダーがソースコードの開示を拒む懸念はない。 ・ 移行において技術的障壁はない。
ベンダー仕様の把握	・ ミドルウェアにベンダーの独自仕様がある。 ・ 乗換え先のシステム仕様やデータ構成及び業務仕様を完全に把握する必要があり、難度が高い。 ・ ベンダー（乗換え元）の内部仕様が非開示であることによって、ユーザ側から工数やリスクの合理性評価が困難である。
リソース不足（ヒト、カネ）	・ システム市場の価格が高騰している。 ・ 仕様変更・データ移行に伴う事務対応や他サブシステム対応に係る人的リソースの確保が難しい。
データ移行	・ 元帳移行等での乗換え元と乗換え先のデータベース項目のマッピングが難しい。

共同センター利用料金[13]に関するベンダーとの交渉は、一部の地域銀行では、第三者評価による妥当性の検証等、高度な取組みを行っている。一方で、料金の根拠の提示が十分に示されない事例や交渉に当たり調整を要している事例等が見られており、地域銀行間で交渉の進め方や情報把握の程度に違いが生じていることがうかがえる（図表 16）。

（図表 16）利用料金のベンダーとの交渉

・ 更改時に第三者を活用し、費用の妥当性を検証するとともに、加盟行で役割分担を行い、ベンダーと費用を交渉している。 ・ 基盤資源や要員の按分割合は、定期的に資金量や業務量等を確認し、各行で見直している。ベンダーに支払う費用は、更改時に第三者評価を実施するなどして、妥当性を確認している。 ・ 利用料金の推移や各サービスの利用率等から、それらに応じた料金体系となるよう交渉を行っている。 ・ 各システム及びサービスの費用は導入時に必要数・スペック等の交渉を行っている。

[13] 各共同センターのモニタリング対象先に対して、共同センターの利用に係る料金として１年間に支払う金額を確認。対象システムは、共同化の範囲や委託業務の内容により異なる。

- 前回の契約内容と比較し、新技術や新機能によるレベルアップ内容や物価上昇率等の社会要因等も加味し、ベンダーと交渉の上、適切性を判断している。
- ベンダーの要員や作業量等、利用料金算出の基礎となる情報の開示を求め、その適切性について協議している。
- 契約更新の都度、他共同センターとの比較により交渉している。
- 口座数、取引量等に応じた従量部分を固定化している。
- 次期更改費用（HW／SW）の見積りが総額で提示され、各明細が開示されていないため、追加でベンダーに明細を確認し費用の妥当性を検討する必要がある。
- 契約更新に当たりベンダーより利用料金の見直し要請を受けたため交渉を進めているが、今後の選択肢として他の共同センターへの移行可能性を継続的に検討している。

地域銀行では、共同センターの利用により、ITコストの削減やリソースの最適化が進む一方、障害影響の拡大や開発・運用スキルの低下、開発自由度の低下等のリスクも認識されている。とりわけ、開発・運用スキルの低下は、単に開発要員が減少するという問題にとどまらず、仕様の妥当性評価、システム更改時の複数対応案の比較検討、障害発生時の影響把握や対応判断、ベンダー提案に対する根拠説明の要求といった業務を主体的に行う能力の低下につながり得る点に留意が必要である。

共同センターの利用に当たっては、こうしたリスクの性質を踏まえ、自行が利用するシステム・サービスの内容やリスク特性について必要な理解を維持し、障害時や更改時等に適切に確認・判断できる態勢を確保していくことが重要である。

第２節　センター運営におけるガバナンス

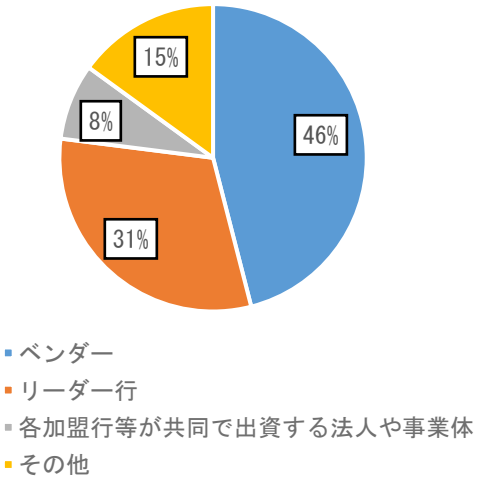
共同センター利用に係る契約状況に関する当庁アンケートでは、共同センターの運営主体は、ベンダー又はリーダー行[14]が多く、リーダー行を設置している共同センターは半数程度となっている（図表17、18）。

共同センター運営における意思決定に関して、リーダー行を設置している共同センターは、加盟行の意見を集約し、加盟行を代表してベンダーと協議している先が多く見られており、リーダー行が共同センター運営における円滑な意思決定に寄与していると考えられる。

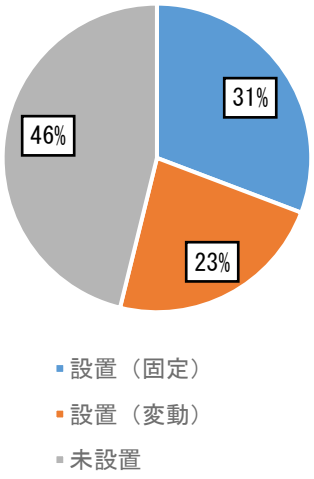
また、意思決定における自行の意見の反映方法については、全加盟行が参加する会議体で提言を行い加盟行の理解を得る、リーダー行に伝達するなどにより自行の意見を反映するとの意見が多く見られた。

[14] 共同センターの運営を主導する銀行（共同化先による持ち回りを含む）。

（図表 17）共同センターの運営主体



（図表 18）リーダー行の設置状況



FISC アンケート結果によると、外部委託先管理において、ベンダー・共同利用先との要件調整等の共同センター運営について「課題あり」と回答した地域銀行は、約３割となっている。

これに対し、今回の当庁アンケートでは、共同センター運営における意思決定に関して、多くの地域銀行が「ベンダー主導の意思決定事項は特になし」と回答し、また、銀行主導で意思決定を行うための取組みとして、リーダー行が調整を主導、全加盟行参加の会議体によるオープンな合意形成、ベンダーと対等な関係の構築等が見られた（図表 19）。一方で、一部の地域銀行においては、ベンダー主導で意思決定が行われている実態も確認された。

要件調整等の共同センター運営に「課題あり」と回答した地域銀行の中には、ベンダー主導で意思決定が行われている先があり、こうした先ではベンダーへの依存が高まっていることが推測される。

（図表 19）銀行主導で意思決定するための取組み

- リーダー行として各行の意見をくみ取り、調整を実施している。
- リーダー行が全体調整を主導し、個別連絡や実務担当者間の調整を行い、意思決定の円滑化を図っている。
- 加盟行とベンダーが対等に運営し、金融機関の意向を強く反映できている。ベンダー側も他行展開を見据え、金融機関の意向をしっかり汲んでいる。
- 開発組織への出向や開発案件の設計レビュー等により、開発・運用に対するスキル維持に努めている。
- ベンダー主導で進める保守期限対応の更改でも、加盟行と合意の上で進めている。

共同センター運営においては、専門性や効率性の観点から、一定の領域においてベンダーが主導的役割を担うこと自体は合理的な場合もある。一方で、投資の方向性、サービス

水準、コスト構造、リスク対応方針等について、加盟行が主体的に関与し、判断できる状態を維持することが重要である。

このため、ベンダーが主導する領域と、銀行が責任を持って判断すべき領域を区分して整理し、投資判断、サービス水準、費用妥当性、リスク対応等に関する加盟行側の関与と説明責任を確保することが、ガバナンス確保の観点から有用と考えられる。

第３節　共同化範囲の拡大

今回当庁が実施したアンケートにおいて、システムの共同化範囲の拡大に向けて取り組んでいると回答した銀行は半数となっている。共同化の対象となっている具体的なシステムとしては、「ATM・営業店システム」や「サブシステム（分散システム）」等が挙げられている（図表 20）。

（図表 20）システム共同化範囲の拡大に向けた取組み

ATM・営業店システム	・ ATM 及び勘定系端末の仕様を共通化。 ・ 営業店のスマート化を加盟行全体に展開。 ・ 近隣他行との店舗外 ATM の共同利用拡大。
サブシステム（分散システム）	・ 融資審査等のシステムを加盟行共同でリリース。 ・ 各加盟行がサブシステム一覧を整理し、システム部門と事務部門が共同化の検討を継続的に実施。 ・ 各加盟行で分散システムの一覧表を整理し、導入等のタイミングで共同導入を検討。

また、システム以外（事務等）の共同化については、共同センターの枠組みを超えた連携や、システム提供行から事務規程の提供を受けるなどの取組みが見られた（図表 21）。

（図表 21）システム以外（事務等）の共同化に向けた取組み

・ 複数の共同センター加盟行が共同で立ち上げたセキュリティ強化のための組織にて、各種セキュリティサービスや機器の共同調達の検討、人材交流（人材育成）等を実施している。
・ 規程等の作成・改正、経営報告や監査対応、脆弱性管理、セルフアセスメント、リスク評価、情報共有機関との窓口等を共同化している。
・ 事務共同化の拡大に向け、共同事務センター（別会社）の設立を検討している。
・ マネロン対策強化のため、AML センター（別会社）を設立し、各加盟行の AML 業務を集約している。
・ システム提供行の事務対応等の運用手続き・通達等の提供を受け、共同化の取組みとして参考にしている。
・ 商品・サービス、規程・基準、書式等を統一している。

こうした共同化を推進する要因としては、各行のシステムを一覧化した上で他行のシステムを把握し、新規導入や更改のタイミングに応じて共同化の可否を議論することで、検討が進めやすくなっている点が挙げられる。また、システム部門に加え、事務部門も含めた横断的な情報共有や検討体制を構築していることで、システム・事務の両面から検討が可能となっている点も挙げられる（図表 22)。

（図表 22）共同化の推進要因

- 各行の分散システムの一覧表を整理し、新規導入や更改のタイミングにおいて、共同での導入が可能か議論している。また、各行の経営戦略を踏まえた上で、システムの共同化が可能な領域について議論している。
- サブシステムの一覧を作成し定期的に情報交換を行うとともに、システム部門だけでなく事務部門も含めて情報を交換している。
- 共同化における先発行を設定し、先発行が責任を持ってベンダーとの交渉を行うとともに、後発行と意見交換等を実施している。また、システムを業務に合わせるのではなく業務をシステムに合わせていくという発想を持ち、そのためにシステム部門だけでなく各行の業務部門を当初から巻き込んでいる。
- 各行が共通の課題認識を持っている。
- 非戦略領域において同一システムを採用し、ボリューム効果でコストダウンを図っている。

地域銀行では、近年の人件費やシステム関連コストの上昇、サイバーセキュリティ対応の高度化等を背景に、現状よりも踏み込んだシステム共同化を進めることで、資金面及び人材面の負担軽減につながる可能性がある。こうした中で、共同化範囲の拡大は単なるコスト削減策にとどまらず、非戦略領域の標準化・効率化を通じて、限られた IT 投資や IT 人材を戦略領域へ再配分するための IT ガバナンス上の取組みとして位置付けることが重要である。

一方で、共同利用先等への依存関係が複層化し、障害時の影響波及や集中リスクが高まる可能性もあることから、効率性の向上とレジリエンス確保の両面を踏まえた検討が求められる。

以上のように、共同センターの利用、共同センター運営におけるガバナンス、共同化範囲の拡大に関する各論点を総合すると、システム共同化は、限られた経営資源を有効に活用するための重要な選択肢となり得る一方で、ベンダーへの依存度を高める側面も併せ持っている。ベンダー主導により加盟行の対応負担が軽減される一方、こうした状況が常態化した場合には、システムに関する判断や対応を自ら行う機能が低下するおそれがある。

このため、効率性の向上とレジリエンス確保の両立を意識しつつ、銀行自らが、共同化の範囲、その運営の在り方、費用の妥当性、システム仕様の理解状況、代替可能性、障害時に自ら判断できる余地等について、継続的に確認しながら、中長期的な視点で共同化の進め方を検討していくことが重要である。

第４編　サイバーセキュリティ

近年、いわゆる「フロンティア AI」の発展に伴い、高度なサイバー攻撃の増加が懸念されている。フロンティア AI は脆弱性の発見や高度な攻撃コードの生成に優れており、従来は発見が困難であった脆弱性が短期間に大量に発見され得ることに加え、脆弱性の発見から攻撃に至るまでの期間が大幅に短縮され得ることが指摘されている。さらに、スキルの低い攻撃者がフロンティア AI を悪用することで、高度なサイバー攻撃が増加することが懸念されている。

これらの脅威は、自組織で開発したシステムに限らず、オープンソースソフトウェア（OSS）[15]を含むサードパーティのソフトウェアやサービスにおいても、同様に及び得ることに留意する必要がある。

一方で、英国 AISI（AI 安全性評価機関）の報告書 [16] によれば、現時点ではフロンティア AI は、十分に防御された IT システムに対しては、攻撃を達成できるとは言えないと報告されている。これを踏まえれば、金融庁の「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、「サイバーガイドライン」という）」に基づく基本的な対策をより迅速かつ着実に実行していくことが引き続き重要である。

また、ランサムウェア攻撃による被害が依然として続いており、金融業界以外ではあるものの、長期にわたりビジネスや顧客に影響を及ぼした事案も複数発生するなど、その脅威は益々高まっている。金融業界においても、複数の金融機関が利用するサードパーティにおいてランサムウェア被害が発生するなど、同様に脅威が高まっている。

近年、金融機関においては、業務の高度化・多様化やデジタル技術の進展を背景として、外部委託や他事業者との連携を通じた業務遂行が拡大している。これに伴い、金融機関の業務やサービス提供に関与する主体は、従来の外部委託先にとどまらず、サービス提供事業者、システム連携先、業務提携先等へと拡大し、サードパーティが多様化している。こうした中、足元では、サードパーティがサイバー攻撃を受けたことを端緒として、金融機関の業務に支障が生じる事案や、顧客情報の漏えい又は漏えいのおそれが生じる事案が発生している。サードパーティリスク管理については、後述する第１章第６節及び第３章並びに補論２で詳細に記載しているところであるが、金融業界においても重要な課題となっている。

また、金融業界においては、2025 年春頃から実在する証券会社のウェブサイトを装った偽サイト等で窃取した顧客情報（ログイン ID やパスワード等）によるインターネット取引サービスでの不正アクセス・不正取引の被害が急増し、足元は低水準で推移しているが、現在も被害が継続している [17]。インターネットバンキングにおいても、2025 年通期（2025 年１月～12 月）で約 104 億円（昨年同期比で約 1.2 倍）の不正送金が発生し、

---

[15] 利用者の目的を問わず、ソースコードを利用、調査、修正、拡張、再頒布等が可能なソフトウェアのこと。「Open Source Software」の略。

[16] AI Security Institute (AISI), Our evaluation of Claude Mythos Preview’s cyber capabilities, https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities

[17] 金融庁：「インターネット取引サービスへの不正アクセス・不正取引にご注意ください」（2026 年７月）https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html

そのうち約９割がフィッシングによるものであった[18]。

第１章　モニタリング等で認められた課題と参考となる取組み

当庁は、2024 年 10 月に「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」を策定・公表し、当庁の監督上の期待を明確化し、サイバーガイドラインに基づき、金融機関との間においてサイバーセキュリティ確保に関する検証や議論を実施してきたところである。サイバーガイドライン公表後に実施した各種モニタリング等で認められた課題及び参考となる取組みについて以下のとおり記載する。

第１節 サイバーセキュリティ管理態勢の構築

サイバーセキュリティについては、経営陣の主体的な関与の下、リソースを適切に配分することが求められるとともに、インシデントが起きてから態勢を見直すという受け身の対応ではなく、平時から能動的に態勢を見直す必要がある。また、サイバーセキュリティは、サイバーセキュリティ担当部署や IT 担当部署だけでは確保できないため、経営陣をはじめとして、組織全体で態勢構築と運営を行う必要がある。こうしたサイバーセキュリティ管理態勢に係る事項については、サイバーガイドラインに明記しているところである。

大手金融機関では、システムが大規模かつ複雑で、その設計・開発・運用等に多くの職員が関与することから、部門ごとにサイロ化が生じ、サイバー部門、システム部門、リスク管理部門等、複数部門に跨るプロジェクトの統制は、難度が高くなる傾向がある。また、金融機関等がグループ（海外拠点等を含む）を形成している場合には、各拠点や子会社が独自の IT 運用を行い、個別の予算に基づく独自の対応を実施している例も見られる。このため、サイバーセキュリティ管理態勢に係る事項について、傘下のグループ会社及び各拠点の規模・特性・サイバーセキュリティ対策状況等を十分に把握した上で、グループ全体として整合性のある適切な態勢を整備することが重要である。加えて、サイバーインシデント発生時に迅速な分析及び経営陣等への報告が可能となるよう、各海外拠点を含め CSIRT との役割分担及び報告体制、対応期限等をあらかじめ明確化しておく必要がある。これらを通じ、グループ全体のサイバーセキュリティを確保することが求められる。

中小規模の金融機関では、サイバーセキュリティに関わる人員及び予算の規模が相対的に限られていることに加え、サイバーセキュリティに関する知見を有する人材が、技術者のみならず、ガバナンス、リスク管理、コンプライアンスを担う各機能において不足している傾向がある。こうした中、各協同組織金融機関においては、中央機関による経営支援機能を活用することも考えられ、また、中央機関等においては、サイバーセキュリティに関する業務補完・支援の集約及び充実を通じ、業態内の相互扶助の充実を図ること

[18] 警察庁：「2025 年におけるサイバー空間をめぐる脅威の情勢等について」（2026 年３月）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf

が期待されている。

金融機関の規模による傾向を上述したが、組織全体・グループ全体での態勢構築と管理運営、サイバーセキュリティに係る人材不足等は、金融業界共通としての課題でもある。金融機関は、退職者の代替人員の確保に加え、進展する技術に対応できるような持続可能な人事施策や教育・研修制度の検討を行っていくことが重要である。

＜課題点＞

- 経営陣は、サイバーセキュリティを経営の重要課題の一つとして認識しているとしているものの、自社のサイバーセキュリティ管理態勢について定期的なレビューが実施されていない事例や、形式的なレビューにとどまり、必要な予算や人員の配分等に関し、十分な情報に基づく実質的な検証・議論が行われていない事例等、経営陣の主体的な関与が不足している事例が認められた[19]。
- 自社のシステムについて残存するリスクを経営陣が適時・的確に把握できていないことから、当該リスクに応じた適切なリソース配分がなされず、結果として適切な未然防止策が講じられていないおそれがある事例が認められた。

＜参考となる取組み＞

- グループ会社や海外拠点におけるサイバーセキュリティ責任者を明確化することに加え、サイバーセキュリティ部門だけでなく、経営資源配分を所管する経営企画部門等も参画させた上で、定期会議等を開催し、親会社からの指示や支援を行えるように体制を整備するとともに、必要に応じて現地拠点の実態評価を実施するなど、グループ全体のサイバーセキュリティ対策を親会社の経営陣が主導している取組み。
- ビジネスモデルや規模等に照らして、自社と類似する固有リスクを抱える金融機関のサイバーセキュリティ対策の情報を収集し、その社と比較検討することにより、自社とのギャップや、そのギャップによるリスクを認識し、自社のサイバーセキュリティ対策の向上に活かしている取組み。
- グループ全体における規程や共通的なコントロールの整備に加え、横断的な分析の実施を目的として、傘下のグループ会社及び各拠点で分散していたセキュリティ監視やログ管理の仕組みを、共通のプラットフォーム上で一元的に運用する高度化の取組み。
- 新卒採用の募集段階において、主にシステム・サイバーセキュリティ等のデジタル部署への配属が中心となるコースを設けている取組み。入社前に将来のキャリアパスを示すことで、情報系をはじめとする幅広い人材の採用を行っている取組み。CISO 等将来的な経営層育成に向け、インシデント対応や資源配分の高度な判断ができる人材を自社内で育成していく取組み。

第２節 サイバーセキュリティリスクの特定

[19] サイバーセキュリティに関する取組みが遅延するなどして、未実施の施策や長期間未解決の課題が散見されるにもかかわらず、経営陣が、対策の進捗状況の管理、問題や原因の把握（人材・予算の問題か、組織体制上の問題かなど）といったモニタリングが不十分で、追加対策の指示を適切に行っていない事例も認められた。

脆弱性管理については、その前提として、情報資産（ハードウェア／ソフトウェアを含めたIT資産）及びネットワーク構成・データフロー（どのようなデータがどの経路を通過するか）の可視化を行い、最新の状態に維持することが、サードパーティリスク管理の観点を含めて重要である。

一般的に、攻撃者は脆弱な箇所や経路を狙って攻撃を行うことを踏まえれば、金融機関においては、自社のシステム全体を網羅的に把握した上で、リスクに応じた優先順位付けを行い、対象範囲、手法（脆弱性診断、ペネトレーションテスト、脅威ベースのペネトレーションテスト（TLPT）等）、実施時期等を計画的に定め、脆弱性を把握する必要がある。また、これらの結果は、経営陣がリスクの受容・低減・移転の判断を行うための基礎情報として適切に活用される必要がある。

また、フロンティアAIにより、従来は高度な専門性や一定の時間を要していた脆弱性の探索や攻撃手法の検討、実行といった工程が、大幅に効率化・高速化され得る可能性が指摘されている。こうした変化を前提に、迅速かつ優先度に応じたパッチ適用が可能な態勢をあらかじめ整備しておくことが重要であり、脆弱性公表からパッチ適用までのスピードアップを可能とする運用態勢の構築や、中長期的な自動化への移行に向けた取組みが求められる。

＜課題点＞

- リスク評価については、年に１回の評価となり、机上演習等様々な活動から認識されたリスクが適時に反映されていない事例が認められた。また、リソース制約等を理由として、インターネットに直接接していないセグメントについては、一律にリスク評価の対象外とするなどの運用が行われている事例も認められた。
- 脆弱性管理については、情報システム及びハードウェア・ソフトウェア等に関する台帳等に基づき、影響を受ける情報システム等を特定し、速やかなパッチ適用等の対応要否を判断する必要があるが、情報システム及びハードウェア・ソフトウェア等に関する台帳等にて、対象とすべきIT資産が網羅的に管理されていない、もしくは脆弱性管理に必要な項目が含まれていない事例が認められた。

＜参考となる取組み＞

- 経営陣が、自社のサイバーセキュリティに係るリスクの大きさを適時・的確に理解し、そのリスクに応じた投資計画やリスク受容等の適切な経営判断が行えるように、技術的なリスク情報を、そのシステムが侵害された場合に予想される業務影響等、経営陣が理解しやすい経営情報に変換して報告している取組みや、自社の固有リスクを踏まえ、セキュリティ対策の進捗やリスクの高まりを継続的に把握するための指標（KPI、KRI）[20]を設定し、その実効性を確認している取組み。

[20] KPI（Key Performance Indicator）、KRI（Key Risk Indicator）こうした指標は、経営陣がリスクを迅速かつ的確に把握するためのものであり、その目的を十分に踏まえた上で継続的に見直すことが重要である。指標の設定自体が目的化しないよう留意すべきである。

- リスク評価に当たり、サイバーガイドラインや CRI プロファイル[21]等のフレームワークを用いた網羅的なギャップ分析に加えて、その組織を取り巻く脅威情報やネットワーク構成等を踏まえたシナリオの発生可能性や影響を加味することで、個別組織の特性を踏まえたリスク評価を行う取組み。
- 情報資産管理を標準化・自動化し、その情報と脆弱性情報を自動的に紐付けることで、脆弱性管理やパッチ適用をより高度化する取組み。

第３節 サイバー攻撃の防御

AI 技術の発展を踏まえると、ゼロデイ攻撃の増加や、脆弱性の発見から攻撃に至るまでの期間の大幅な短縮の可能性があり、従来のパッチマネジメント手法では十分に対応できないおそれがある。金融機関においては、ソース自体が公開されているオープンソースソフトウェア（OSS）の利用に関するサプライチェーンリスクの再評価[22]が必要であるとともに、従来から進めている多要素認証の導入等による認証の強化や、アクセス権限の最小化や職務分離の徹底といったアクセス管理の強化等について、加速させる必要がある。また、ゼロトラストの考え方に基づく対策としてマイクロセグメンテーション等を検討し、多層防御を講じることが重要である。

＜課題点＞

- 重要なシステムにおいて、ランサムウェア攻撃のリスクを考慮した十分なバックアップの期間や頻度の確保、改ざん耐性のあるバックアップシステムの利用、組織内ネットワークから切り離した複数の環境での保管や媒体等へのバックアップの実施等の対策を十分に検討していない事例が認められた。
- 内部ネットワークセグメントに設置した重要なシステムにおいて、重大な脆弱性が残存している状況を認識しているにもかかわらず、境界防御型セキュリティが突破されるリスクを十分に考慮していない事例が認められた。また、サポート期限の終了に伴うハードウェアやソフトウェアの廃止・更改について、計画的かつ安全に実施するための更新計画が十分に整備されていない事例が認められた。

＜参考となる取組み＞

- 組織全体での厳格な ID・アクセス制御基盤を構築し、権限昇格や不正な水平移動を防止する取組み。また、マイクロセグメンテーション等を活用して、隔離・遮断・停止の自動化範囲を拡大することにより、マルウェア侵入後においても影響の拡大を抑止する高度化の取組み。
- 組織全体を俯瞰して、業務上重要な主要システム（サーバーや機器等を含む）を選定し

[21] CRI プロファイルとは、Cyber Risk Institute（CRI）が策定した金融機関向けのサイバーセキュリティ管理フレームワークであり、NIST 等の国際的基準をベースに、金融機関のリスク管理や統制項目を体系的に整理・標準化したもの。

[22] SBOM 整備等による OSS（依存関係を含む）の可視化、当該 OSS に係る脆弱性の把握と対応、悪意あるコード混入への対策等、これらを含めた網羅的な視点でのリスク評価等。

た上で、ネットワークの配置状況とサイバー防御対策の実装状況をマッピングするなど可視化し、防御対策の漏れがないか、追加で対応すべき点がないか、外部専門家（第三者評価）が点検している取組み。

- 従来のシステム単位毎のリスク評価にとどまらず、攻撃種別ごとのサイバー攻撃やその影響の波及経路等に関するシナリオを踏まえ、リスク管理部門や外部専門家も交え、システム全体を可視化した俯瞰図をもとに防御対策の実装状況を確認し、優先的に実装すべき防御対策を洗い出している取組み。

第４節 サイバー攻撃の検知

サイバー攻撃の経路（アタックサーフェス等）は、金融機関が従来から認識しているインターネットに直接接続している経路に加え、DX の進展により新たに導入されたモバイル端末の経路、SaaS[23]等のクラウドサービスの経路、職員のリモートワークの経路、さらにはベンダー保守等に伴うリモートアクセス時に利用されるインターネット VPN 機器の経路等、多様化している。また、サードパーティ経由の不正アクセスも考慮する必要があるほか、セキュリティ機器を回避する手口や、ソーシャルエンジニアリングや内部不正等による内部ネットワークへの不正アクセスにも留意が必要である。このように金融機関のアタックサーフェスは拡大し続けていることに加え、通常の通信プロセスの中にマルウェアが潜伏している可能性も否定できない。EDR[24]、IPS、SOAR[25]等様々なセキュリティ機器を利用しインシデント発生前の不正アクセスの試行を的確に検知し、即時に対応できる態勢を整備することは重要である。検知態勢の巧拙は、金融機関におけるサイバーセキュリティ確保の水準を大きく左右するものとなっている。

＜課題点＞

- クラウドサービスの契約時に、アラートの重要度に基づくクラウド事業者からの通知方法やクラウド事業者と金融機関の役割分担について明確にしていなかったため、拠点内で発生した不審な通信に起因するアラートに対応できなかった。また、拠点間のネットワークにおいて不審な通信を検知したものの、インシデント発生時の連絡プロセスを決めていなかったことから、組織全体としてインシデントとして認識するまでに時間を要した事例が認められた。

＜参考となる取組み＞

- エンドポイントセキュリティ強化の一環として、役職員の端末に加え、内部ネットワークセグメントに設置されたシステムのうち、特に重要なシステムに対しても、EDR 等の計

[23] SaaS とは、ソフトウェアをインターネット経由でサービスとして提供する形態であり、インフラやソフトウェアの管理を主に提供事業者が担うため、利用者の管理範囲が限定されるクラウドサービス。
[24] EDR（Endpoint Detection and Response）とは、端末やサーバーの動作を監視することで不審な挙動（振舞い）を検知し、迅速な対応を支援する仕組みをいう。
[25] SOAR（Security Orchestration, Automation and Response）とは、セキュリティ対策の統合・自動化により、インシデント発生時の自動遮断等の対応を実施するシステムをいう。

画的な導入を進めている取組み。リスクベース・アプローチにより優先順位付けの上、相対的にリスクが低いと評価されたシステムにおけるセキュリティ対策の実装を、次回のシステム更改と同時に実施するといった対応計画を策定し、人員・コスト等の平準化を行った上で計画的に実施している取組み。

- 各種ログを個別に取り扱うのではなく相互に関連づけて分析することによりサイバー攻撃の兆候を多角的に検知する取組み。サードパーティリスク管理を含む統合的リスク管理の高度化の一環として、脅威情報やシステム上の検知結果等を連動させ、定量的な基準に基づくリスク評価を実施することにより、リスクの高まりを定量的に把握し、インシデントの未然防止に向けた対応を高度化する取組み。
- サイバー攻撃を検知する SOC[26]について、グローバルでの一元化を目指す取組み。日本や海外拠点等、地域別に SOC を運用し、各 SOC 間で情報連携する取組み。
- 実環境のアラートログ情報等を活用し、マルウェアの侵入を SOC やレッドチーム等と連携させることにより、検知漏れの把握や対応力の向上を図る取組み。外部脅威情報を活用し、未検知となっている可能性のある脅威を、レッドチームによりハンティングする取組み。

第５節 サイバーインシデント対応及び復旧

経営陣は、迅速かつ的確に現状を把握し、様々なリスクを勘案の上、ネットワークの切り離し、再接続等の経営判断を実施することが肝要である。サイバーセキュリティに係る技術的な観点に加え、インシデント対応においては、法務リスクや顧客保護、事業継続、レピュテーションリスクを踏まえた対外説明等様々な観点から経営判断が必要であり、平時から経営主導で必要な準備を進め、有事において BCP が機能するように IT 部門だけでなく経営陣や関係部門等を含め、練度を高めておくことが重要である。

＜課題点＞

- インシデント対応計画及びコンティンジェンシープランが、初動対応のみに範囲が限定された内容となっており、攻撃を想定した対応から復旧に至るまでの一連のプロセスが欠落していた事例や、重要なシステムが更改されているにもかかわらず、インシデント対応計画等を更新していないなど、実効性を欠く事例が認められた。
- 国内外の拠点及びサードパーティにおいてサイバーインシデントが発生しているにもかかわらず、原因分析及び再発防止策の検討・実施が十分でないことから、必要なセキュリティ対策の見直しやインシデント対応に係るプロセスと完了基準の見直しが行われていない事例が認められた。

＜参考となる取組み＞

[26] Security Operation Center（セキュリティオペレーションセンター）の略で、組織の IT 環境において不審な通信やログの監視、攻撃の兆候の検知、インシデント発生時の初動対応、被害拡大の防止等を行う、サイバー攻撃に対する監視・検知・初動対応を担うチーム又は体制。

- インシデント発生時に経営判断に必要なグループ全体の情報が迅速に集約可能となる仕組みの構築に向けた取組み。
- 構成管理データベース（CMDB）[27]を活用して資産・業務・権限の関係性を一元管理して可視化するとともに、脅威インテリジェンス情報を加味した上で SOAR 等の自動化ツールを組み合わせることで、インシデント発生時の状況把握と優先順位付けの効率化を図る取組みや、AI を活用したインシデント対応の迅速化に向けた取組み。
- EDR で検知できない潜伏期間を考慮した多世代保管・分散保管とともに、改ざん耐性を備えることで、攻撃者の長期潜伏にも耐え得るようにバックアップデータの取得を行う。また、バックアップデータ保全の高度化（バックアップ 3-2-1 ルールの実装）や、バックアップデータからの復旧迅速化に向けた高度化の取組み。
- 業務やシステム機能に大きな変更があった場合に、復旧計画の有効性を検証するため、目標復旧時間（RTO）等の定量的な指標に基づく復旧訓練を実施し、復旧目標の達成に役立つプロセスと復旧のための技術基盤を検証するといった取組み。インシデント発生時に役職員が適時に必要な判断を確実に行うため、昨今の攻撃者の TTPs（Tactics（戦術）、Techniques（技術）、Procedures（手順））等を踏まえ、具体的なサイバーインシデントシナリオを設定した研修・訓練を実施している取組み。
- グループ横断でサイバー演習の年間計画を立て、拠点毎に課題を設定し演習を実施する取組み。

第６節 サードパーティリスク管理

サードパーティにおいて発生した事案であっても、金融機関の業務継続や顧客への影響に係る最終的な責任は金融機関自身に残ることから、サードパーティを起点とするサイバーリスクは、金融機関自身のサイバーリスクとして捉える必要がある。

現状、サードパーティリスク管理においては、契約締結時における一定の確認や、必要最小限の事項をチェックリスト形式で点検することにとどまるケースも見られるが、サイバーインシデントの未然防止や、発生時における影響最小化・早期復旧といった観点から、こうした対応のみでは必ずしも十分とは言えなくなってきている。もっとも、金融機関がサードパーティから情報資産や脆弱性管理の実施状況等に関する情報を十分に取得できない場合があることに加え、金融機関側のリソース不足により十分に把握できない場合もあるなど、様々な課題が存在することにも留意が必要である。

このため、効率的かつ効果的なサードパーティリスク管理に向けては、金融機関がリスクベースで第三者保証による報告書（SOC2[28]等）や外部評価の枠組み、契約書等を活用し、サードパーティへのモニタリングの実効性を高めるとともに、必要に応じてヒアリ

[27] CMDB（Configuration Management Database）とは、システムを構成するハードウェア、ソフトウェア、ネットワーク等の構成要素とその関係性を一元的に管理するためのデータベース。

[28] SOC2 とは、System and Organization Controls 2 の略であり、サービス提供事業者のセキュリティ、可用性、処理の完全性、機密性及びプライバシーに関する内部統制の整備・運用状況について、第三者監査人が評価・報告する枠組み及びその報告書。

ングを実施するほか、ASM[29]ツール等を活用して外部に晒されている脆弱性を把握するなど、複数の手段の組合せによる確認を実施することや確認の頻度を変更する等の工夫が求められる。

さらに、金融機関においては、サードパーティを含むインシデント対応計画及びコンティンジェンシープランの整備状況を、あらかじめ検証し実効性を高めておくなどサードパーティにおけるインシデント発生を前提とした態勢整備をしておくことが重要である。

＜課題点＞

- サードパーティのサイバーセキュリティの確保状況を把握するためのチェックリストの設問が「はい」「いいえ」で回答する形式となっており、その実効性には疑義がある中で、必要に応じて回答に関するエビデンスを徴求して確認できていない、または、重要なサードパーティの実査を実施していないなど、その実効性を高められていない事例が認められた。
- サードパーティで発生したインシデントの原因やサイバーガイドラインの内容を踏まえ、チェックリストの項目について必要な見直しを実施していない事例が認められた。
- 重要情報を管理する情報システムを保有しているサードパーティの点検や、サードパーティとの契約継続の判断について、サイバーセキュリティに知見のある部署を関与させていなかった事例が認められた。
- 攻撃者からの脅威を低減するためには、情報資産管理、ネットワーク構成、脆弱性管理の対応状況等の理解が必要であるが、サードパーティが提供するサービスに関しては、サードパーティ任せとなる傾向が強く、サードパーティ経由の感染等を含めたリスクの特定が不足している事例が認められた。

＜参考となる取組み＞

- 管理プロセスの自動化を通じて、外部委託先等、サプライチェーン全体のリスクの可視化対象を拡大するとともに、継続的なリスク低減を図る取組み。
- 代替ソリューションを特定するとともに、実効性を確保するために、代替ソリューションへの切替対応プロセスを文書化する。また、契約条件の未遵守先に対しては取引停止措置を講じられるよう契約上の手当を検討する取組み。

第２章　AIによるサイバー脅威の変化への対応

AI技術が急速に進展する中、サイバー攻撃の速度・規模が劇的に加速・拡大するなど、サイバーセキュリティを巡る脅威が急速に高まっている。こうした中、短期的に脆弱性やパッチが集中して発見・提供される可能性を踏まえ、2026年５月22日、金融庁は日本銀行と連名で各金融機関等に対して、経営トップを含めた経営層の直接関与の下、以下

[29] サイバー攻撃の対象となり得るIT資産や攻撃経路を把握・管理する取組みや技術。「Attack Surface Management」の略。

に掲げる対応に取り組むよう要請した。要請文の全文は金融庁ホームページ[30]をご確認いただきたい。なお、本要請は要請文発出時点での状況を前提とするものであり、金融機関等においては、今後の AI を巡る動向の変化を踏まえ、不断かつ機動的に対応を見直すことが求められる。また、AI 脅威に対しても基本的な対応が有効なため、「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」に基づく対策についても、より迅速かつ着実に実行していくことが引き続き重要である。

① フロンティア AI への対応を経営課題として扱う

経営トップは、フロンティア AI への対応を IT 部門にとどまらない全社的な経営課題として位置づけ、関係部門が横断的に連携して対応できるようにする。その上で、経営トップのリーダーシップの下、CIO や CISO をはじめとする経営層が直接関与する。

② 優先的に対応すべきサービス／IT システムを特定する

優先的に対応すべきサービス／IT システムを特定し、リソースを重点的に配分するなど、リスクベースでの対応を行う。（例：インターネットバンキング）また、当該システムが共同運営形態で提供される場合は、利用側・提供側双方において十分な認識共有を行い、責任分担を明確化する必要がある。

③ 特定した資産の技術負債を解消しておく

特定した資産については、脆弱性発見時にパッチ適用対象を即時に特定できる状態を確保する。加えて、特権 ID の削除や未対応パッチの適用等により技術負債を極力解消し、迅速なパッチ適用が可能な状態を確保する。特に、サポートが終了している製品は、サポート対象のバージョンへ更新する。

④ パッチ適用に係る人的リソースを追加する

増加が見込まれる脆弱性への対応力を向上させるため、金融機関等やベンダーにおいて、パッチ適用に係る人的リソースの追加を検討する。また、脆弱性の優先度判断に係る評価体制についても、同様に人的リソースを確保する。

⑤ ベンダーとの維持保守契約の内容を確認する

パッチ適用作業が現行の維持保守契約に含まれていること及び役割分担が明確であることを確認する。さらに、緊急にパッチ適用作業が必要な場合に、夜間・休日等も含めて適時に対応可能な契約内容となっていることを確認する。加えて、ベンダー側で必要なリソース確保状況を確認しつつ、リソースがひっ迫すること等も想定し、パッチ適用の遅延に係るリスク受容等のプロセスを整備する。

⑥ パッチ適用プロセスをリスクベースにする

発見された脆弱性が自組織のサービス／IT システムに及ぼし得る影響と攻撃が成

[30] 金融庁は４月 24 日に「AI 脅威に対する金融分野のサイバーセキュリティ対策強化に関する官民連携会議」を開催した。その議論を踏まえ、金融業界と IT 事業者、政府・日本銀行等が AI 技術の進展による脅威について共通の理解を持ち、対応を検討していくため、実務者レベルの作業部会（第１回）を５月 14 日に実施した。当該作業部会において取りまとめた「フロンティア AI による脅威変化を踏まえた金融機関等の短期的な対応」について要請したもの。
https://www.fsa.go.jp/news/r7/sonota/20260522-5/20260522.html

立する蓋然性も踏まえて評価する。その上で、リスクベースで優先順位付けを行い、よりリスクの高い脆弱性から対応する。さらに、パッチ適用作業に係る事前のテストについては、想定されるリスクを総合的に勘案し、テスト実施内容の合理的な縮小等の対応も検討する。

⑦ パッチ適用以外の対策も強化する

パッチ適用そのものが困難である場合等は、仮想パッチの適用やボット対策の導入等、多層防御の強化を図る。また、ネットワーク分離の実施、特権 ID への多要素認証の導入等による防御能力の強化や内部侵入後の横展開への対策等を講じる。あわせて、パッチが適用できないことによる残存リスクを評価した上で、パッチ適用に要する期間を踏まえた適切なリスク受容手続を講じる。

⑧ 優先サービス／IT システムの停止に備える

サイバー攻撃により IT システムが停止する場合を想定する。また、システムを能動的に停止させざるを得ない場合も、あらかじめ選択肢として検討する。その上で、BCP の有効性や顧客等への対応手順、緊急時の連絡体制等を点検するとともに、能動的なサービス／IT システム停止の判断基準及び手順を明確にしておく。さらに、サードパーティが提供するソフトウェアやサービスの停止にも備える。

⑨ 外部との連携を維持・強化する

金融 ISAC や各業界団体･コミュニティ､当局等からの情報に積極的にアクセスし、必要な情報収集を行う。あわせて、自組織での取組みを金融 ISAC 等の共助コミュニティで積極的に共有し、金融分野全体の強靭性の向上に努める。

第３章　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委託調査

第１節　調査の背景及び目的

金融庁では、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（以下、「TPCRM」という。）について、諸外国の金融機関における管理手法を調査し、その知見を整理・公表することで、本邦金融機関における TPCRM の強化につなげることを目的として、委託調査を実施した。

第２節　調査概要

本委託調査では、金融分野における TPCRM の強化に資する国際的なガイダンスや諸外国の制度・基準・ガイダンス等を対象とした文献調査を行うとともに、米国、欧州及び英国の銀行・保険会社を対象に、質問票調査及びヒアリングを実施した。調査項目については、金融機関との意見交換等を通じて寄せられた課題や懸念事項を踏まえ、サードパーティ管理のライフサイクル全体を俯瞰する観点から、主に以下の事項を対象とした。

① サードパーティの分類と管理方針
② 集中リスク
③ サードパーティ選定時におけるデューデリジェンス

④　契約後の期中モニタリング及び監査権の確保
⑤　サードパーティのサービス停止等を想定した出口戦略・出口計画
⑥　サードパーティにおけるサイバーインシデント発生時の対応

第３節　主な調査結果

以下に調査結果の概要を記載する。調査結果の詳細は金融庁ホームページ[31]をご確認いただきたい。

①　サードパーティの分類と管理方針

調査対象となった金融機関では、サードパーティを外部委託先のみに限定せず、金融機関と取引のある全ての組織を管理対象として整理している例が多く見られた。その上で、提供されるサービスの重要度、取り扱う情報の性質、金融機関のシステムやネットワークとの接続の有無等を踏まえ、固有リスクに基づく分類を行っていた。こうした分類の結果、全サードパーティのうち 1～10%程度を「重要なサードパーティ」とし、これらに対して重点的に管理を行うリスクベースのアプローチが採用されていた。重要なサードパーティの割合は全体の一部にとどまる一方、これらに対しては、追加的なモニタリングや出口戦略・出口計画の策定、現地調査等、管理の深度を高める対応が講じられ、限られたリソースを実効的に配分するための工夫が確認された。また、管理対象とすべき Nth パーティについては、全てを一律に管理対象とするのではなく、提供されるサービスの重要度や固有リスクを踏まえ、リスクベースで判断している例が確認された。具体的には、直接契約関係にあるサードパーティに対し、再委託先等をどのように管理しているかといった管理能力を評価することにより、間接的に Nth パーティのリスク低減を図る対応が取られていた。

②　集中リスク

集中リスクについては、「金融セクター全体に係るシステミックレベルの集中リスク」と「金融機関レベルの集中リスク」が挙げられるが、本委託調査は「金融機関レベルの集中リスク」について調査した。調査対象となった金融機関では、集中リスクの把握はオペレーショナル・レジリエンス確保の観点から重視されており、単一のサードパーティへの依存にとどまらず、特定の国・地域への依存による地理的集中等も含めて管理が行われていた。また、集中の有無を把握することに加え、当該サービスが停止した場合の代替先の有無や、当該代替先への切替えの実行可能性といった点についても含めて評価が行われていた。これにより、平時から代替手段の検討を進め、有事における迅速な意思決定につなげる取組みが認められた。集中リスクの測定方法としては、「サービス集中」、「地理的集中」、「Nth パーティの集中」等の種類ごとに指標を置き、ツールを活用し集中リスクを測定していた。

③　サードパーティ選定時におけるデューデリジェンス

調査対象となった金融機関では、サードパーティ選定時におけるデューデリジェ

[31] 金融庁：「『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』報告書等の公表について」（2026 年４月３日）https://www.fsa.go.jp/common/about/research/20260403/20260403.html

ンスについて、金融機関及びサードパーティ双方の負担を踏まえつつ、重要度に応じて確認項目や深度を調整するリスクベースの運用が確認された。こうした取組みの一環として、効率化を目的に、参加企業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にてサードパーティのリスク評価結果を共有する枠組みが存在した。業界共通の質問票を活用することで一定のベースラインを効率的に確認した上で、重要なサードパーティについては個別の追加確認を行うといった取組みも見られた。また、契約書等において、最低限実施すべきサイバーセキュリティ対策（例えば、データの暗号化、情報漏洩防止策、アクセス制御等に関する要求事項）に関する条項を設けることで、これを充足できない場合は契約を見送る対応が取られている例も確認された。加えて、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要件を金融機関のホームページ等で公開しているケースも確認した。

④　契約後の期中モニタリング及び監査権の確保

調査対象となった金融機関では、契約締結後の期中モニタリングにおいては、定期的な質問票による確認に加え、サイバー脅威インテリジェンス等を活用し、サードパーティのリスク状況の変化を把握する取組みが行われていた。また、期中モニタリングにあたってはリスクスコアリングツールやアタックサーフェスマネジメント等のテクノロジーを活用しているケースを確認した。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サードパーティ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。これにより、リスクの顕在化を早期に捉え、是正対応を促すなど、実効性を意識した運用が確認された。不備が是正されない場合にはサードパーティとの契約解除も検討するなど、形式的な管理にとどまらない対応が行われていた。また、監査権を契約条項に含めて確保し、必要に応じて現地調査を実施する態勢が整備されていた。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。こういったケースにおいては、業界団体に加盟している金融機関に監査結果が共有されていた。

⑤　サードパーティのサービス停止等を想定した出口戦略・出口計画

調査対象となった金融機関では、重要なサードパーティについて、サービス停止や事業撤退等を想定した出口戦略・出口計画を事前に整備している例が多く見られた。出口戦略と出口計画の定義を明確にしていない金融機関も見られたが、そのような金融機関においても、サードパーティが提供するサービスの終了または中断時における対応の基本方針及び全般像（対応方針や選択肢、発動条件等）を整理した文書（出口戦略）や、業務やサービスの維持に向けた移行計画の詳細をまとめた文書（出口計画）を整備していた。重要なサードパーティとの初回の契約及び契約更新時に、出口戦略・出口計画が策定・承認される仕組みをプロセスに実装していた。また事前に策定した出口計画については定期的なテストが実施されており、その実施方法としては、現時点では机上テストの範囲で検証している金融機関が多くみられる。こうした定期的な見直しや机上テストを通じて、計画の形骸化を防止する取組みが行われていた。

⑥　サードパーティにおけるサイバーインシデント発生時の対応

調査対象となった金融機関では、サードパーティにおけるサイバーインシデント発生を前提に、報告フロー、エスカレーション手順、ネットワーク遮断や再接続の条件等を明記した対応手順（プレイブック）が整備されていた。インシデント対応に当たっては、サイバーセキュリティインシデントの対応チームが技術的な対応を実施し、契約所管部や法務等の関係部門等がビジネス観点の対応を担い、相互に連携するなど、サイバーセキュリティインシデント対応の専門チームと契約部署と連携する態勢が構築されており、役割分担の明確化が図られていた。また、重要なサードパーティとは平時から共同演習を実施し、対応手順の確認や課題抽出を行うことで、有事対応力の向上につなげている例も確認された。

第４章　顧客口座・アカウントの不正アクセス・不正取引への対策強化

証券会社のインターネット取引サービスについては、2025 年春頃に第三者による不正アクセス・不正取引の被害が急増した。こうした不正アクセス・不正取引による被害は、証券業界にとどまらず、金融業界全体の信頼に直結する問題である。

金融庁は、2025 年７月に顧客口座・アカウントの不正アクセス・不正取引への対策強化を全所管金融機関に対して要請した。要請文では、①フィッシングに耐性のある多要素認証の導入及びモニタリング等、②ウェブサイト・メールのなりすまし等への対策、③口座連携におけるリスクへの対応、④金融機関間の情報共有、⑤顧客への注意喚起・相談対応の５点について要請を行った。

加えて、証券会社において被害が発生していることを踏まえ、2025 年 10 月 15 日に「金融商品取引業者等向けの総合的な監督指針」を改正し、その後その他の業態についても、業態ごとの業務内容やリスク特性を踏まえ、段階的に監督指針及び事務ガイドラインの改正を実施した（図表１参照）。

当庁としては、改正後の監督指針等に基づき、国民が安心して金融取引を行うことができる環境を確保する観点から、モニタリングを行っていく。

（図表１）顧客口座・アカウントの不正アクセス・不正取引への対策強化に関する監督指針及び事務ガイドラインの改正一覧

改正日	監督指針及び事務ガイドライン
令和７年 10 月 15 日 [32]	・　金融商品取引業者等向けの総合的な監督指針
令和８年 ２月 27 日 [33]	・　主要行等向けの総合的な監督指針 ・　中小・地域金融機関向けの総合的な監督指針

[32] 金融庁：「『金融商品取引業者等向けの総合的な監督指針』等の一部改正（案）に対するパブリックコメントの結果等の公表について」（2025 年 10 月 15 日）
https://www.fsa.go.jp/news/r7/shouken/20251015/20251015.html

[33] 金融庁：「『主要行等向けの総合的な監督指針』等の一部改正（案）に対するパブリックコメントの結果等の公表について」（2026 年２月 27 日）https://www.fsa.go.jp/news/r7/sonota/20260227/20260227.html

	・ 事務ガイドライン第三分冊：金融会社関係「16 暗号資産交換業者関係」 ・ 事務ガイドライン第三分冊:金融会社関係「17 電子決裁手段等取引業者関係」 ・ 系統金融機関向けの総合的な監督指針 ・ 漁協系統信用事業における総合的な監督指針
令和８年 ７月 17 日 [34]	・ 保険会社向けの総合的な監督指針 ・ 少額短期保険業者向けの監督指針 ・ 貸金業者向けの総合的な監督指針 ・ 金融サービス仲介業者向けの総合的な監督指針 ・ 主要行等向けの総合的な監督指針（電子決済等代行業） ・ 中小・地域金融機関向けの総合的な監督指針（電子決済等代行業） ・ 事務ガイドライン第三分冊：金融会社関係「5 前払式支払手段発行者関係」 ・ 事務ガイドライン第三分冊：金融会社関係「14 資金移動業者関係」

[34] 金融庁：「『保険会社向けの総合的な監督指針』等の一部改正（案）に対するパブリックコメントの結果等の公表について」（2026 年７月 17 日）https://www.fsa.go.jp/news/r8/sonota/20260717-2/20260717.html

第５編　クラウド演習の進め方

国内の金融分野においてもクラウドサービスの利用が進む中、当庁ではクラウドサービス事業者と意見交換を行っている。その意見交換を通じて抽出されたものとして、昨年のレジリエンスレポートにおいて、金融機関のパブリッククラウドサービスの利用にあたり、金融機関、クラウドサービス事業者及びクラウドサービスを利用して金融機関にサービスを提供する事業者は、以下の点に留意すべきとした。

- 銀行法等の業法上、クラウドサービスの利用は委託（二段階以上の委託を含む）に該当するため、金融機関はクラウドサービスを外部委託として管理するとともに、クラウドサービスの特性に由来するリスクを考慮した対策を講じる必要があること。
- 特に、パブリッククラウドサービスを利用する場合には、金融機関は、障害対応に必要な情報をオンプレミスの場合と同程度に迅速に取得し、かつ十分な情報を取扱い可能か、あらかじめ確認する必要があること。
- 確認のためには、金融機関とクラウドサービス事業者がともに机上演習等を行い、障害時の情報の取扱いに関する実態を把握することが有効であること。[35]

2025 事務年度においては、障害情報の取扱いに関する実態把握を目的に、金融機関、パブリッククラウドサービス事業者とともに机上演習を実施した。今般、演習で得られた知見を、他金融機関でも参考可能な形で整理した上で、「クラウド演習の進め方」として還元する。

演習を行った金融機関は、特定のパブリッククラウドサービスを複数の業務で利用していることから、障害情報の取扱いに加えて、特定のサードパーティへの集中リスクも念頭に、演習を行った。

パブリッククラウドサービスの利用対象範囲の拡大を予定している金融機関、あるいは、重要なシステムでパブリッククラウドサービスの利用を検討している金融機関は、以下を参考に、関係者と机上演習に取り組むことを通じて、パブリッククラウドサービス利用時のリスク（障害情報の取扱いに加えて、利用実態によっては集中リスクも含む）をあらかじめ確認するとともに、その結果を、パブリッククラウドサービス利用に関する意思決定あるいは利用開始後のレジリエンス確保のために活用することが望ましい。

---

[35] 金融機関は、その業務を第三者に行わせる限りにおいて、当該第三者がクラウドサービス事業者であるか否かを問わず、当該第三者を外部委託管理態勢の中で管理することとなる。
したがって、金融機関は、クラウドサービスに起因するシステム障害に備えて、クラウドサービス事業者を含めた報告態勢、指揮・命令系統を明確にし、ノウハウ・経験を有する人材をクラウドサービス事業者等から速やかに招集するため応援体制を明確にするとともに、システム障害発生時には、発生原因の究明、復旧までの影響調査、改善措置、再発防止策等を的確に講じ、特に経営に重大な影響を及ぼすシステム障害が発生した場合には、取締役に最悪のシナリオの下で生じうる最大リスクを報告する必要がある（例えば、主要行等向けの総合的な監督指針ではⅢ－３－７－１－２（10））。
加えて、障害対応を通じて、クラウドサービス事業者の業務運営態勢等に問題が認められる場合等においては、特に必要があると認められる場合（クラウドサービス事業者に対して多数の金融機関が同種の外部委託を行っている場合や決済システム全体に影響を及ぼしかねない場合など）に、クラウドサービス事業者に対して、事実関係や発生原因分析及び改善・対応策等必要な事項について、業法に基づき報告を求めることがある（例えば、主要行等向けの総合的な監督指針ではⅢ－３－３－４－３（２）②）。

第１章　プロセスの全体像

障害情報の取扱いに関する机上演習に取り組むプロセスとして、例えば、以下のプロセスが考えられる。目的次第でシナリオや演習の重点が変わり得ることから、「目的の設定」「目的の共有」が最も重要なプロセスとなる。

＜プロセス例＞

プロセス	内容
目的の設定	流通する情報の速度・情報の深度・情報の経路を検証すること 過去のオンプレ障害時と比較
参加者の確定	社内外で障害対応に関わる関係者の特定、参加承諾
目的の共有	目的を参加者と共有するとともに必要に応じて修正
シナリオづくり	既存のインシデント対応計画やコンティンジェンシープランの確認 障害事例を参考に「想定以上に深刻なものだが、起こり得るシナリオ」を設定
机上演習	業務影響の確認（集中リスクの確認）関係者間で流通する情報の速度の確認 社会的な情報発信のタイミングの確認、情報の源泉の確認
リスク評価 対応可能性検証	オンプレ障害時とのギャップ分析に基づきパブリッククラウドサービス利用時のリスクを評価、リスクへの対応可能性を検証
整備 （課題の特定）	リスク顕在化時の事後対策整備 リスク対応にかかる意思決定、リスク対応策の検討、課題の担い手の設定

第２章　目的の設定

特定のパブリッククラウドサービスを既に多くの業務で利用している金融機関の場合、以下の目的が考えられる。

＜金融機関＞

パブリッククラウドサービスを利用する場合、障害対応に必要な情報をオンプレミスの場合と同程度に迅速に取得し、かつ十分な情報を取扱い可能か、確認すること。確認された結果を踏まえ、パブリッククラウドサービスに起因する障害時に適切に対応可能かを金融機関において検証し、インシデント対応計画やコンティンジェンシープランを整備し、必要に応じて更新すること。

＜パブリッククラウドサービス事業者＞

本邦において、パブリッククラウドサービス障害時に、金融機関は、どのような情報共有を求めているか理解を深めること。確認された結果を踏まえ、金融機関に対する情報共有の方法等を必要に応じて見直すこと。

第３章　セッション

演習を実施するにあたり、関係者間で、少なくとも以下の３回のセッションを実施することが考えられる。

（１）準備セッション
参加者で目的の共有、シナリオ作りのほか、シナリオの前提となるリスクを共有する。
（２）本番セッション
机上演習をタイムラインに沿って実施し、情報流通経路・流通速度・流通する情報の内容等を確認する。
（３）まとめセッション
振り返り討議の実施により、リスク評価と対応可能性を検証し、課題を特定する。

第４章　演習シナリオ

パブリッククラウドサービスに起因する障害として、「想定以上に深刻なものだが、起こり得るシナリオ」を具体的に設定するにあたり、例えばフェーズを「初動」「業務継続確保」「復旧」「真因分析・再発防止」に区分し、フェーズ毎で情報の取扱いを確認することが考えられる。

（１）初動
リージョンの全てのサービスが突然停止（オフライン）する。ソーシャルネットワーキングサービス（SNS）等を通じて障害情報が拡散する。
（２）業務継続確保
SNS 等を通じて、障害情報が更に拡散する。クラウドサービス事業者が障害原因の特定に至らない中で、金融機関は業務継続確保に向けた意思決定を行う。
（３）復旧
クラウドサービス事業者は障害原因を特定し復旧を進め、サービスが徐々に再開する。金融機関は、停止していたクラウドサービスへの再接続（オンライン化）の意思決定を行う。
（４）真因分析・再発防止
金融機関は、クラウドサービス事業者とともに、障害の原因分析と再発防止策を検討。

更にストレスを高める場合には、障害発生時間を対応の難度が最も高いと考えられる時間帯に設定するほか、「切り替え後にバックアップサイトの機能が低下する」といったシナリオを追加することが考えられる。

第５章　本番セッションの進行

当庁が参加した演習では以下の進行で行った。

（１）机上演習

参加者間の情報流通の実践「どのような要請・報告・回答を行うこととなるか、あるいは、受けることとなるか」

・シナリオは事前に参加者へ開示しておく。

・参加者はそれぞれの組織毎で部屋を分ける。

・メールを使用するなど情報流通の記録が残るように行う。

（２）振り返り

組織の内部的な情報流通・意思決定の共有「なぜ、そのような要請・報告・回答を行ったか、あるいは、受けることとなったか」

・記録した情報流通をもとに、それぞれの組織内部的な動きを共有し理解を深める。

（３）質疑応答

・例えば、情報の取扱いに関するオンプレミスとのギャップの有無（クラウドサービス事業者が行う統制に関する情報を含む）に関して、意見交換を行う。

＜机上演習　「初動」進行例＞

	事象・アクション
1	障害発生
2	金融機関が障害検知、クラウドサービス事業者が障害情報を公表
3	金融機関が、クラウドサービス事業者へ情報提供要請
4	クラウドサービス事業者が、金融機関へ情報提供
5	金融機関が、監督当局へ障害報告（初報）
6	監督当局が、金融機関とクラウドサービス事業者へ情報提供要請
7	金融機関とクラウドサービス事業者が、それぞれ監督当局へ情報提供

第６章　着眼点

一般的に、パブリッククラウドサービスにおける情報の取扱いに関する特性として以下が考えられる。

・パブリッククラウドサービス事業者にすれば、設備を共同利用させている多数の利用者からの情報提供要請に対応することは現実的ではないことから、利用者であるか否かを問わず、一斉に公表することとなる[36]。

・その際、障害情報公表のタイミングは、パブリッククラウドサービス事業者が独自に決定し、また、公表の内容についても、自らの責任範囲として明確な、技術的部分に限定されることとなる。

[36] 公表に加えて、顧客向けに、顧客が利用しているサービスへの影響を通知する場合もある。

これは、自社専用設備であるオンプレミスを利用する場合や、設備の共同利用相手が明らかな共同センターを利用する場合とは異なることから、金融機関は、この特性から生じうる情報の取扱いを確認し、従来のオンプレミス等とのギャップから生じるリスクについて、あらかじめ評価しておくことが重要である。

以上の評価観点を踏まえつつ、演習にあたっては、金融機関は、自社の意思決定（例えばバックアップサイトへの切替）や対応（例えば広報・当局対応）に必要十分な情報を収集することができるか、そのために、誰からどういう情報を受け取って誰に渡すのか、あるいは、どれぐらいのタイミングで受け取れるのか、という点に着眼して、確認を進めることが必要である。その他に、例えば、金融機関は、以下のような点に着眼することも考えられる。

・パブリッククラウドサービス事業者が公表する障害情報を、速やかに収集分析しているか
・影響を受けうるシステムを速やかに特定しているか（サードパーティへの集中リスク、Nth パーティへの集中リスクの管理を含む）。
・パブリッククラウドサービスを利用する他事業者（金融機関に加え他産業分野の事業者を含む）の特定及び他事業者から受ける影響の分析に努めているか（パブリッククラウド事業者からの情報収集を含む）。
・顧客からの問い合わせ・苦情に加え、SNS 等を通じたパブリッククラウドサービス事業者や金融機関の風評拡大状況といった情報収集分析に努めているか。
・パブリッククラウドサービス事業者からの情報提供（クラウドサービス事業者の責任範囲に関する情報）を契約で担保しているか。

＜バックアップサイトを手当てしている場合＞

・バックアップサイトへの切替を行う場合、あらかじめ必要な情報処理資源の確保はできているか[37]。

第７章　留意点

金融機関のクラウドサービス利用実態は区々であることから、実態に応じてリスクベースで、演習の実施要否や内容を検討すればよく、ここで例示した演習の形式的な実施自体が目的化されるべきではない。また、クラウドサービス事業者を含むサードパーティリスクの観点からは、障害情報の取扱い、特定のサードパーティへの集中リスク以外にも、地理的集中リスクをはじめ様々なリスクが想定される。このため、本演習を実施すれば十分とすることなく、クラウドサービス利用にあたり、金融機関のリスクの実態に応じたシナリオを用意した上で、クラウドサービス事業者を交えて演習を行い、継続的にレジリエンス向上に取り組むことが必要である。

[37] その他に、サイバー攻撃に起因する障害であることが確認された場合には、バックアップサイトの汚染可能性を考慮すること、復旧したとするクラウドサービスに対して再接続する際に第三者による復旧状況の検証の要否を検討することが考えられる。

補論１　システム障害に関する分析（事例集）

システム障害に関する分析（事例集）は、2022 年４月から 2026 年３月までに報告された「障害発生等報告書」のうち、主な事案を障害発生の端緒別等に整理し[38]、取りまとめたものである（今回初めて掲載した事例には新規と表示している）。なお、掲載していない事例を当局として重視していないということを必ずしも意味するものではない。

本事例集が、金融機関において、自己責任原則の下、創意工夫をもって、それぞれの規模・特性等に応じたシステムリスク管理を行う際の参考となることを期待している。

第１章　サイバー攻撃・不正アクセス等の意図的な要因から発生したシステム障害

１ 委託先へのランサムウェア攻撃新規

＜業態＞

保険会社等

＜事象＞

- 金融機関の外部委託先への不正アクセスにより外部から第三者に侵入され、端末及びサーバーに保存していたファイルが一部暗号化され、個人情報等が窃取されるランサムウェア被害が発生した。

＜原因＞

- 第三者がネットワーク機器の脆弱性を悪用して不正アクセスを行い、内部ネットワークに侵入したことが判明。また、導入していたセキュリティソフトが当該第三者により無効化されている。

＜対策＞

- セキュリティ関連規程等の見直し及び社内教育の推進
- 悪用されたネットワーク機器の排除
- ネットワーク管理体制やアクセス制限の強化
- インシデント発生時の対応策の強化
- セキュリティ担当部門の強化

２ システムへのサイバー攻撃新規

＜業態＞

保険会社等

＜事象＞

- 社内システムが不正アクセスを受けたことにより、数日間、同システムへ侵入した第三者が顧客情報にアクセスできる状態になっていたと推測され、外部に漏えいした可能性があることが判明した。

＜原因＞

[38] 過去に掲載した事例については、分かりやすさの観点から記載を修正している場合がある。また、本文に記載されている報告期間以前の事例であっても、業態の状況等を踏まえ、掲載を継続しているものがある。

- システムの脆弱性等

＜対策＞

- 他システムに同様の脆弱性が無いことの確認
- 不正アクセスの監視・検知能力の強化

3 システムへの不正アクセス新規

＜業態＞

保険会社等

＜事象＞

- システムへの不正アクセスにより、外部から侵入した第三者が顧客等に関する情報を抜き取ろうとしていた可能性があると推測され、外部に漏えいした可能性があることが判明した。

＜原因＞

- システムの脆弱性管理の不備等

＜対策＞

- セキュリティインシデント管理の強化
- 脆弱性管理の強化
- 攻撃に対する防衛策と異常検知の仕組みの強化

4 証券サイトにおける不正ログイン・不正売買新規

＜業態＞

金融商品取引業者等

＜事象＞

- 実在する証券会社のウェブサイトを装った偽のウェブサイト（フィッシングサイト）等で窃取した顧客情報（ログイン ID やパスワード等）によるインターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害が発生している。

＜原因＞

- 証券会社を装ったメールや SMS によって偽のウェブサイト（フィッシングサイト）に誘導し、ログイン情報や取引パスワードを不正取得している。メールや SMS のメッセージは「口座凍結」「本人確認」等の緊急性を煽る内容が多く、心理的に動揺させて入力を誘導している。
- 多要素認証（MFA）を迂回するリアルタイムフィッシング等の高度な手法も確認されている。

＜対策＞

- フィッシングに十分な耐性のある多要素認証（特に生体認証を用いたパスキーによるもの）の必須化及びセッションや取引のモニタリングの強化、DMARC や BIMI の導入等のなりすまし対策の強化、証券口座と預金口座等の口座連携におけるリスクへの対応、金融 ISAC 等において手口や対策に関する情報共有の強化、手口や対策に関する顧客への注意喚起や顧客からの相談への対応の強化　等

５ ボイスフィッシング詐欺新規

＜業態＞

地域銀行

＜事象＞

- 地域銀行を装ったボイスフィッシング詐欺[39]とみられる事案が複数確認された。
- 銀行の担当者をかたる者が企業または個人に電話をかけ、その後の電子メール等を通じて偽のウェブサイトへ誘導し、インターネットバンキングに関する情報を不正に取得した上で、資金を第三者口座へ送金する手口が確認されている。

＜原因＞

- AI 技術を用いた偽音声やなりすまし手法の高度化
- 自動音声と銀行担当者を装った通話を組み合わせた二段階手法
- 電話対応中に判断を迫ることによる被害者の冷静な確認行動の阻害
- 即時振込機能の悪用

＜対策＞

- 顧客が不審な連絡や誘導に適切に対応できるよう、注意喚起や相談受付態勢の整備を継続的に行う
- 不正送金の未然防止の観点から、認証・取引時のモニタリングやリスクに応じた取引管理を強化する
- 顧客対応部門を含め、平時からの周知・訓練等を通じて、被害の拡大防止に向けた態勢の実効性を高める

６ 不正なモバイルアプリ（マルウェア）を介したフィッシング攻撃新規

＜業態＞

資金移動業者等

＜事象＞

- 不正なモバイルアプリ(マルウェア)のインストール誘導を目的とした当社を騙る Web サイトが確認された。
- 同アプリをインストールしたユーザが、同アプリ上でログイン情報を入力したことにより、第三者による不正ログイン・不正決済が行われた。

＜原因＞

- 当社を騙る Web サイトを通じたマルウェア配布・フィッシング攻撃

＜対策＞

- 当社 Web サイト等を通じて、本事案と同様の手口（不審なアプリのインストール誘導等）に対する注意喚起文の掲載を実施
- アプリ配信プラットフォーム事業者への情報提供による同アプリの配信停止対応
- マルウェア配布 Web サイト発見時の Web サイト差し止め要請の迅速化
- パスキーによる認証の推進　等

[39] 音声通話を起点とするフィッシング詐欺

7 モバイルアプリサーバーのマルウェア感染新規

＜業態＞

資金移動業者等

＜事象＞

- グループ会社が運営するモバイルアプリのサーバーが外部からの不正アクセスを受けた。同アプリは、利用者の同意に基づき、グループ会社側システムから API を通じて当社サーバーに保存された顧客情報へアクセスできる仕様となっていた。
- 不正アクセス者により当該 API が実行された結果、当社サーバーに保存されていた一部顧客のメールアドレス等が漏えいしたおそれがあるほか、一部のアプリ会員登録が不正に解約される事象が発生した。

＜原因＞

- モバイルアプリの認証機能において、認可制御に不備があり、認証パラメータが再利用可能となっていた
- セッションキー生成方法のランダム性が不十分で推測可能性が高い等、安全でない方式が用いられていた

＜対策＞

- 認証パラメータに対する改ざん防止措置の導入やアプリ側で取得できない情報を追加パラメータとして付与するなど、認可制御の不備を是正
- セッションキーの生成方法を、十分にランダムで推測不能な方式へ変更するなど、モバイルアプリ認証に係る安全性を強化

8 開発者ＰＣのマルウェア感染新規

＜業態＞

暗号資産交換業者

＜事象＞

- 開発者がシステム開発で利用しているツールを起動したところ、ツールの拡張機能が自動アップデートし、開発者ＰＣがマルウェア感染した。

＜原因＞

- ツールの拡張機能で利用しているＯＳＳパッケージの配布元が改ざんされ、ＯＳＳパッケージにマルウェアが仕込まれていた。

＜対策＞

- 外部の攻撃情報、脆弱性情報の収集を継続する。
- マルウェア感染発生時の対応（感染の早期検知、検知時の対応、被害状況の把握、関係者への報告、全役職員への注意喚起、復旧方針等）を適切に実施できるようにしておく。

9 ソーシャルネットワーキングサービスで利用している公式アカウント乗っ取りによる、フィッシングサイトへの誘導新規

＜業態＞
暗号資産交換業者
＜事象＞
- 第三者によってソーシャルネットワーキングサービスで利用している公式アカウントへ不正ログインされ、ユーザーアカウントへのログインページを装ったサイトへ誘導する投稿が行われた。
- システム自体の不具合等は発生していないものの、顧客へのフィッシング被害の発生及び拡大を防止するため、全てのサービスを一時停止した。

＜原因＞
- 担当者は、キリル文字を利用した偽装メールアドレスから届いたメールに記載されたリンクをクリックし、フィッシングサイトに遷移した後、ID・パスワード・二要素認証情報を入力した。

＜対策＞
- ソーシャルネットワーキングで利用する公式アカウントの認証をフィッシングに耐性のあるパスキー認証へ移行。
- 不正ログイン時のリスクが高い外部サービスを全社的に洗い出し、リスク評価及び認証状況の再点検を実施。

１０ 外部委託先のランサムウェア感染による情報漏えい

＜業態＞
主要行等、地域銀行、金融商品取引業者等、信用金庫・信用組合等、保険会社等、貸金業者
＜事象＞
- 金融機関に情報サービスを提供している会社のファイルサーバーがランサムウェア感染したことにより、委託元の金融機関が同社へ取り扱わせていた個人情報の漏えいに繋がった。
- リークサイトにおいて窃取されたと思われる情報のダウンロードURLが出現し、流出した情報の中には顧客の個人情報が含まれていることが判明した。

＜原因＞
- 委託先においてVPN接続における多要素認証等のセキュリティ対策不足、パスワードポリシーの脆弱さ、特権アカウントの管理不備等、サイバー攻撃への対策が十分でなかった。
- 委託先においてアクセスセキュリティの不備、個人情報保管についての認識不足、社内ルールから逸脱したファイルサーバー利用の常習化等個人情報管理が十分でなかった。
- 委託元においても、委託先のサイバーセキュリティ対策状況の確認、再委託先の管理、個人情報保護の監視・チェック体制の確認等における外部委託先評価の形骸化が見られた。

＜対策＞

- 委託先へのサイバーセキュリティ評価の高度化（チェック項目・評価対象の見直し、第三者によるセキュリティ態勢評価等）
- 委託先の対応義務明確化（委託契約覚書等にインシデントの報告義務・事業継続への対応を明文化等）
- 委託先におけるインシデント発生時対応手順を再評価

１１ 年末年始の DDoS 攻撃

＜業態＞

主要行等、地域銀行、金融商品取引業者等

＜事象＞

- 年末年始の DDoS 攻撃により主要行や地銀等で一時的にサービスへ繋がりにくくなる事案が発生した。

＜原因＞

- 犯罪組織等による重要インフラ事業者等に対する DDoS 攻撃。

＜対策＞

- 金融 ISAC 等を通じた被害事例の情報収集分析及び警戒継続
- DDoS 攻撃はボットからの攻撃によって実施されることが多いため、ボットに感染している端末等が多い国やドメインからの通信拒否を検討
- WAF（Web Application Firewall）、IDS/IPS、UTM（Unified Threat Management）、DDoS 攻撃対策専用アプライアンス製品等の導入
- 必要性に応じて事業継続に重要なシステムはその他のシステムとネットワークの分離を検討
- サーバーやインターネット回線が使用不能となった場合の代替手段やユーザ向けのサービスが提供不可となった場合のユーザへの周知手段の確保等、対策マニュアルや BCP を策定

１２ 委託先クラウドのマルウェア感染事案

＜業態＞

主要行等

＜事象＞

- 海外支店のプライベートクラウド環境への不正アクセスが発生した。
- 海外支店のサーバーを経由し、国内外拠点へのポートスキャンと見られる不正通信が発生した。

＜原因＞

- プライベートクラウドにおける運用再委託先で動作していたリモートアクセス用ツールが不正侵入の起因であり、パスワードのセキュリティ強度も十分でなかった。
- 自給自足型攻撃（システム内に元から存在する正規のツールや機能を悪用して行われるサイバー攻撃）等が利用されているため、ふるまい検知機能がないエンドポイントプロテクションでは、攻撃の検知が十分ではなかった。

- 海外拠点からの照会連絡等の対応態勢が十分でなかったため、インシデントへの対応が遅れた。

＜対策＞

- 委託先管理としてPaaS／IaaSの利用の重要度・影響度を上方に修正。委託先・再委託先のクラウド運用体制の確認を掘り下げて実施できる態勢の整備
- 特権ID管理、パスワードポリシー強化。アクセス管理として最小権限の付与とネットワーク防御の対策を検討
- 昨今の攻撃事象の事例や情報収集を踏まえたリスク分析によるセキュリティ対策の検討
- 照会連絡等の体制強化のため、拠点からの連絡を組織的に確認、適時に判断するプロセスを整備。海外拠点の環境・コンディションの把握、セキュリティ強化

１３ DDoS攻撃による外部委託先サービス停止

＜業態＞

主要行等、地域銀行、資金移動業者等

＜事象＞

- 委託先データセンターのファイアウォールがDDoS攻撃を受けた。
- 各銀行が委託先から提供を受けているサービスに対しての攻撃ではなかったが、DDoS攻撃の緩和処理が作動するまでの間にファイアウォールが高負荷となり、営業店で顧客に対しカード等の媒体を発行するサービスが一時利用不可となった。

＜原因＞

- 委託先のデータセンターでのDDoS攻撃緩和機能を上回る通信が継続した。

＜対策＞

- データセンターにおいて他サービスを狙ったDDoS攻撃の影響が銀行のサービスに及ばないよう、システム間で共有しているファイアウォールをシステムごとに分割

１４ DDoS攻撃によりアプリ上でのサービスが利用しにくい状況

＜業態＞

資金移動業者等

＜事象＞

- アプリ上で行うサービス（チャージ、ネット決済等）に利用しにくい状況が発生した。

＜原因＞

- 不特定多数のIPアドレスから、アプリのサーバーに対するDDoS攻撃を受けた。

＜対策＞

- 一定の通信量を超えた送信元IPアドレスに対し、当該IPアドレスからの通信を遮断する機能の閾値の見直し
- 海外のIPアドレスからの通信帯域の制限
- 他システムとファイアウォールを共用している箇所について、専用のファイアウォールを割り当てるよう構成変更

- ロードバランサーのアップグレードによる性能向上

１５ 標的型ソーシャルエンジニアリングを用いたサイバー攻撃

＜業態＞

暗号資産交換業者

＜事象[40]＞

- 当社で利用するウォレットソフトウェア提供会社の従業員に対して、北朝鮮を背景とするサイバー攻撃グループによる標的型ソーシャルエンジニアリングを用いた攻撃にて同従業員になりすまし、正規取引のリクエストを改ざんしたことにより、顧客暗号資産（ビットコイン）が不正に流出した。

＜対処例と緩和策[41]＞

- 多要素認証を導入する。
- 事前申請又は通常の業務時間帯・曜日ではない期間に行われたアクセスに関する認証ログ、アクセスログがないか監視する。（例：時差の大きい地域に居住する従業員が、通常は日本時間の夜や早朝にアクセスしているにもかかわらず、ある時期から日本時間の日中もアクセスしているなど。）
- EDR[42]や PC 内のログと矛盾がないか監視する。（例：PC が電源 OFF している期間にアクセスしていないか。）
- PC のログ保存期間や、マルウェアに感染した後にログが消去されるリスクを考慮し、ログを集中的に保存・検索できる仕組みを構築し、異常の把握と速やかな対処ができるようにしておく。
- 事前に許可されている場合を除き、私用 PC で機微な業務用システムにアクセスしない。

１６ 外部委託先のランサムウェア感染によるサービス停止

＜業態＞

地域銀行、信用金庫・信用組合等

＜事象＞

- 再委託先が提供するクラウドサービスのサーバーに対する VPN 機器の脆弱性を悪用したと考えられる不正アクセスにより、再委託先がランサムウェアに感染した。このため、金融機関の利用者がサーバーにアクセスできなくなり、外部向けファイル転送システムが利用不可となった。

＜原因＞

---

[40] 「北朝鮮を背景とするサイバー攻撃グループ TraderTraitor による暗号資産関連事業者を標的としたサイバー攻撃について」（2024 年 12 月 24 日、警察庁、https://www.npa.go.jp/bureau/cyber/koho/caution/caution20241224.html）より抜粋。

[41] 「北朝鮮を背景とするサイバー攻撃グループ TraderTraitor によるサイバー攻撃について（注意喚起）」（2024 年 12 月 24 日、警察庁・国家サイバー統括室・金融庁、https://www.fsa.go.jp/news/r6/sonota/20241224/tyuuikanki.pdf）より抜粋。

[42] 端末やサーバーの動作を監視することで不審な挙動（振舞い）を検知し、迅速な対応を支援する仕組み。「Endpoint Detection and Response」の略。

- 再委託先において、脆弱性情報を収集していたが、脆弱性に対するバージョンアップの適用状況の管理が十分ではなかった。また、サイバー攻撃に対する技術的な対策や検知後の対応態勢が脆弱であった。
- 外部委託先の選定時にサイバーセキュリティ管理態勢の評価が十分でなかった。

＜対策＞

- 再委託先における脆弱性情報の把握と脆弱性に対するバージョンアップ適用状況の管理体制の強化
- 再委託先におけるサイバー攻撃に対する技術的な対策の強化及び検知後の対応態勢の強化
- 外部委託先の選定時に ASM[43]等の技術的な評価を活用したサイバーセキュリティ管理態勢評価の強化

１７ マルウェア感染による個人データ流出

＜業態＞

金融商品取引業者等

＜事象＞

- ファイル転送サービスシステムのサーバーが、不正アクセスによりマルウェアに感染し、システムで転送されるファイルへのアクセス及びダウンロード権限を有するアカウントが作成されたことから、従業員の個人データが流出した。

＜原因＞

- ファイル転送サービスのサーバーがゼロデイ脆弱性 [44]を悪用した攻撃者によって侵害された。

＜対策＞

- ファイル転送システムのサーバーに対するサイバーセキュリティ管理について全面的な見直しの実施（サイバーセキュリティの専門家による影響を受けたサーバーのサイバーセキュリティ評価の実施）

１８ DDoS 攻撃による決済不可

＜業態＞

資金移動業者等

＜事象＞

- DDoS 攻撃により、サーバーへの負荷が急増し、リクエストを処理できず、決済に影響が生じた。

＜原因＞

- 複数あるインターネット上の入り口（ドメイン）の一部に対し、特定 IP アドレスより通常時の 3,000 倍以上のアクセスが発生したため、サーバーへの負荷が増加し、リ

[43] サイバー攻撃の対象となり得る IT 資産や攻撃経路を把握・管理する取組みや技術。「Attack Surface Management」の略。

[44] ソフトウェア等に見つかったセキュリティ上の脆弱性のうち、その存在が公表される前や、修正用プログラムやパッチがリリースされる前の脆弱性

クエストを処理できなかった。

＜対策＞

- 異常なリクエストを自動で制御するためのドメインレベルでの主要経路に対するレートリミット[45]の導入
- ブロック対応の高度化（IP ブラックリストの適用、HTTP ヘッダーを用いたブロックルールの適用）

１９ 外部委託先が提供するサービスへの DDoS 攻撃

＜業態＞

地域銀行

＜事象＞

- 同じクラウドサービスを利用する他企業への DDoS 攻撃により、同クラウドサービスを利用する金融機関の IB が長時間にわたり利用不可となった。

＜原因＞

- DDoS 攻撃を受けたことで、負荷分散サーバーの TCP 接続が許容量を超えたため、新たな TCP 接続を確立できなくなった。また、タイムアウトまで接続状態を解除できなかった。
- 正常性監視において、TCP 接続テーブルの接続数が許容量を超えていることを検知できなかった。
- 外部委託先内における部署間の連携不備により、復旧対応に時間を要した。

＜対策＞

- 早期復旧を図るための接続タイムアウト値の短縮の実施及び負荷軽減を図るための負荷分散サーバーへの流用制限適用の実施
- 障害原因を特定できるよう、接続数が許容量を超えた場合の検知実施
- 外部委託先における DDoS 攻撃に対する早期検知・復旧作業迅速化のための態勢整備

２０ 外部委託先における認証設定の不備による情報漏えい

＜業態＞

保険会社等

＜事象＞

- 再委託先による、サーバーの認証を不要とする誤った設定に起因して、外部からの不正アクセスを受け、個人情報漏えいが発生した。

＜原因＞

- 再委託先において、使用目的を達成後、本来削除すべき個人情報が残存していた。
- 委託先において、再委託先の情報セキュリティ管理態勢の実効性確認が十分に行われていなかった。
- 委託元において、委託先・再委託先に対する情報セキュリティ管理態勢の実効性の検証が十分行われていなかった。

[45] 一定期間内に許可されるリクエストの数を制限する技術。

＜対策＞

- 委託する個人情報のデータ管理（データへのアクセス権限、データ保管場所、データ保管期限等）に関する確認項目の詳細化と証跡による検証の実施
- 委託先における情報セキュリティ管理態勢の変更（システム変更含む）に関する要件の詳細化
- 委託先（再委託先含む）の情報セキュリティ管理態勢の委託元（金融機関）における委託開始前評価及び委託中の定期点検の強化　等

２１ 外部委託先への DDoS 攻撃

＜業態＞

信用金庫・信用組合等

＜事象＞

- ホームページが閲覧不可となり、IB、電子記録債権サービス、投信インターネットサービス及び外為 Web サービスへホームページからログインできなくなる事象が発生した。
- 当金庫が提供するアプリが利用不可となる事象が発生した。

＜原因＞

- 外部委託先が運営するホスティングサービス上で稼働している特定のサイトに大量のトラフィックが流入したため、回線帯域が逼迫し、ホスティングサービス全体のインターネット接続に影響が発生した。その結果、ホームページ及びアプリも閲覧不可、利用不可となった。

＜対策＞

- 障害発生時の連絡体制、復旧が長期化した場合の対応策等、障害対応に係るマニュアル見直しの実施
- 外部委託先における大量通信発生サイト特定の迅速化

２２ 金融機関のエモテット感染の疑い

＜業態＞

信用金庫・信用組合等

＜事象＞

- 経営企画部にて受信した Web メールに添付されているファイルを開封したところ、不審な画像が表示され、エモテット感染の疑いが発生した。

＜原因＞

- メールで受信したファイルを信用金庫内環境に取り込む場合、無害化できないものは、担当者と上席者がクロスチェックをした上で無害化せずに取り込むこととしているところ、受信メールの本文をよく確認しなかったこと、無変換でのファイル取込みを担当者のみで行ってしまったこと等が重複した。

＜対策＞

- 取り込むファイルの無害化・無変換に関するルールの再周知及び徹底
- PC のデスクトップ画面に、不審なファイルを開いた場合の初期対応を表示

２３ 多数の IP アドレスを使用した DDoS 攻撃

＜業態＞

金融商品取引業者等

＜事象＞

- サービスを提供するシステム共通基盤のネットワーク機器の CPU 負荷が増大し、各サービスの接続に通常より時間を要する、エラーとなるなどの事象が発生した。
- DDoS 攻撃の検知から対応方針の確定及び IP アドレス遮断によるネットワーク機器の CPU 負荷低下の効果確認完了までに時間を要した。

＜原因＞

- サービスを提供するシステムの IP アドレスに対する DDoS 攻撃により、想定以上のアクセスが集中した。
- サイバー攻撃を受けた際の連携体制が十分に理解されていなかった。
- IP アドレス遮断に係る手順が不明確だった。

＜対策＞

- 攻撃内容を分析し、導入済みの DDoS 攻撃対策サービスを補完する追加機能等の実装
- 速やかに対応するための部署間の連携体制、会議体の役割の再確認
- IP 遮断対応の手順改善の実施

２４ 他社システムへの DDoS 攻撃の波及によるホームページ利用不可

＜業態＞

地域銀行

＜事象＞

- 外部委託先がホームページのシステム基盤をホスティングサービスとして複数の事業者や業態に提供している。そのサービスを利用する他社のホームページに対し、大量の通信が発生しシステムの負荷が高騰したことにより、長時間にわたりホームページへのアクセスが不可となった。

＜原因＞

- 外部委託先の提供するサービスを利用する他社のホームページへの大量通信

＜対策＞

- 外部委託先において、トラフィック流入元のサイトの早期特定のための分析機能を改善すること、特定した流入元サイトを速やかに停止するための手順や連絡体制等の態勢整備
- 迅速に顧客周知を行う方法及び顧客に対して代替手段へ誘導する方法の確立

２５ ランサムウェア感染に伴う情報漏えい

＜業態＞

信用金庫・信用組合等

＜事象＞

- ファイアウォールの脆弱性を悪用した外部からの不正アクセスにより、ファイルサーバーがランサムウェアに感染し、データが暗号化されて身代金を要求されるとともに、情報漏えいが発生した。

＜原因＞

- ファイルサーバーへの接続元を制限する設定としていなかった。
- サポート期限切れの古いサーバーを利用していた。

＜対策＞

- 認証強化（二要素認証）、ネットワーク機器の接続先 IP アドレス等制御の実施
- サポート期限切れのサーバーの利用中止
- ツール導入による脆弱性管理の実施

２６ 署名鍵の災害・障害復旧に関する情報を悪用した暗号資産の流出

＜業態＞

暗号資産交換業者

＜事象＞

- 暗号資産を管理するウォレットシステムへの不正アクセスにより、当社の自己保有暗号資産が流出した。

＜原因＞

- 自己保有暗号資産を管理する署名鍵の災害・障害復旧に関する情報を用いて不正な資産移転が行われた。
- 当該情報に対する十分なアクセス管理が行われていなかった。

＜対策＞

- 署名鍵の災害・障害復旧に関する情報に対するセキュリティ管理態勢（情報の暗号化及び分散、職務分掌によるけん制機能等を含む）の整備
- 外部からの不正アクセス及び内部不正リスクを考慮したアクセス権限管理の徹底、モニタリング態勢の整備

２７ ドメイン名登録情報への不正アクセスを端緒とした情報漏えい

＜業態＞

暗号資産交換業者

＜事象＞

- ドメイン管理事業者へアクセスする際の認証方式の設定不備により、第三者のなりすましにより当社のドメイン名登録情報が書き換えられたため、顧客等からの電子メールが漏えいした。
- 窃取されたドメイン登録情報を用いて、当社システムに不正に侵入され、当社の顧客情報が漏えいした。

＜原因＞

- ドメイン管理事業者のドメイン管理サイトには、ログイン時の二要素認証の機能があったにもかかわらず、それを設定していなかった。

- 当社システムにアクセスする認証設定も不十分であった。

＜対策＞

- 外部サービス利用時の認証機能の強化とセキュリティの評価
- 当社システムのアカウントへの二要素認証の設定及びアクセス制御の強化

第２章　システム統合・更改に伴い発生したシステム障害

１ 新たな送金電文方式への対応に伴う外国送金トラブル新規

＜業態＞

主要行等

＜事象＞

- 外国送金に係る新たな電文方式への対応に向けてシステム改修を実施したところ、リリース後、一部の送金処理や関連処理、対外電文の発信ができなくなる事象が発生し、電文処理が滞留したもの。

＜原因＞

- 新旧の電文方式が併存する移行対応に伴い、送信する電文方式を判別するための設定を追加していたところ、条件分岐が複雑化していたもの。
- その後の仕様見直しや変更対応の過程で、関係者間の認識にずれが生じ、不要な処理が実装されたもの。また、テストにおいて無影響確認が十分でなかったことから、不具合を事前に検知できなかったもの。

＜対策＞

- 案件立上げ時のレビューを強化し、想定される障害影響を踏まえた確認を徹底
- 無影響確認テストの基準を明確化し、テスト項目として整備
- 不具合発生時の電文除去やプロセス再起動に係る手順を整備

２ 振込予約処理の考慮不足に伴う障害新規

＜業態＞

主要行等

＜事象＞

- 全銀為替システムにおける予約仕向取引について、システム更改の影響により、更改作業後の営業初日における振込予約件数が、ピーク実績の約 3 倍となった。
- 同日営業開始前より遅延が発生し、コアタイム内に振込予約処理を全件完了できない見込みとなったため、未処理の振込予約をモアタイムで発信するべく、実行中の振込予約バッチ処理の強制停止を試みた。しかしながら、当該バッチ処理に対して強制停止手順が機能せず、処理が継続した。その結果、コアタイム中に発信できなかった振込が、コアタイムとモアタイムにおける処理日の相違に伴う日付整合性チェックに抵触し、エラー判定となった。顧客宛てには、振込エラー通知メール等が送信され、振込は実行されなかった。

＜原因＞

- 件数が３倍程度に増加することは、準備段階で見込みが立っていたが、振込予約実行処理のタイムアウトや処理性能への考慮が不足していたもの。
- 障害対応時には既存の強制停止手順を適用したものの、本障害では強制停止の適用対象外であったことが事後的に判明している。事象発生時点では、「強制停止手順を適用すれば全てのバッチ処理を停止できる」という認識が共有されており、処理パターンごとの適用可否が整理・文書化されていなかった。

＜対策＞

- 件数の増加傾向分析に基づき、「テスト計画の方針」及び「通常と振る舞いが異なる取引の有無とその影響」を整理・記載する欄を新設し、改修有無に関わらず影響を受ける可能性のあるシステムを網羅的に整理するルールを追加
- 稼働中のバッチ処理について、処理パターン（実装方式・中断可否等）を一覧化し、適用可能な強制停止手順との対応関係を明確化。不足が判明した範囲については、新たな強制停止手順の策定または安全に停止可能な設計の導入可否を検討　等

３ ステーキング[46]の報酬付与に係る計算ロジックの誤認により、本来付与されるべき報酬額よりも少ない報酬額を付与している状況が発生 新規

＜業態＞

暗号資産交換業者

＜事象＞

- ステーキングの報酬付与に係る計算ロジックの誤認により、付与対象者への報酬額が実際に付与すべき報酬額より少なく付与されていた。
- 「報酬付与原資に付与割合を乗算済みの値」に対し、再度付与割合を乗じる計算ロジック（付与割合を二重で計算するロジック）になっていた。

＜原因＞

- 要件定義書に計算ロジックの内容を正しく反映していないことから、複数部署間で誤認が発生し、二重で手数料を控除することになった。
- 計算ロジックに係る重要な機能部分を要件定義書に記載していないことを見過ごしていた。
- 要件追加時に、要件定義書の再レビューを実施していなかった。
- 機能要件に係るテスト項目の網羅性に不足があった。

＜対策＞

- 要件定義書において確認すべき項目の明確化及び責任者によるレビューの必須化。
- 要件の追加・変更発生時の再レビュー・再承認プロセス、また、再テストを実施したか確認するプロセスを追加。
- 機能要件を網羅的にテストしていることを確認する基準を設定。

４ 勘定系システム更改に関連する ATM 障害

[46] Proof of Stake を採用している暗号資産を預入し、ブロックチェーンの安定稼働（ネットワークの維持やセキュリティ）に貢献することで、報酬を得ることができる仕組み。

＜業態＞

地域銀行

＜事象＞

- 勘定系システムの老朽化に伴い、勘定系システムの更改を実施した。稼働直後より、ATM の稼働日に係る設定誤りや ATM の取扱を開始する上で必要な機能が未実装、ATM に関する設定変更内容が未確認であったことにより、ATM の利用が不可となる障害が複数回にわたり発生した。

＜原因＞

- 要件定義や設計工程等の上流工程において、別プロジェクトで使用した資産・機能を流用した際に別プロジェクトの実績を過信し、銀行のレビュー不足や委託先が影響調査やその結果の妥当性を確認するプロセスが明文化していなかった。
- テスト工程では、テスト計画策定時に、主担当である委託先に任せ、銀行や関連する委託先とのレビューやテスト環境に関する認識合わせが十分にできておらず、有効なテストが実施できていなかった。
- システム変更前の確認作業において、銀行がシステムの運用方法を変更するにあたり、委託先へ変更する内容や問題有無について確認していなかった。
- 稼働後の障害対応に追われ、リリース判定時に変更する対象のプログラムを確認していなかったことで誤った資産をリリースした。

＜対策＞

- 要件定義・設計工程における影響調査プロセス及びレビュー体制の整備
- テスト工程におけるテスト観点やテストを実施する環境について、銀行や主担当の委託先、その他のテストに関連する委託先間での認識合わせ・レビューの実施
- 銀行主体でシステム変更する際は、委託先に問題有無や影響確認を必須化
- リリース判定会議においてリリース対象プログラムの確認と委託先担当者の会議への参加を必須化

5 システム統合における ATM の通帳取り込み

＜業態＞

地域銀行

＜事象＞

- ATM において、通帳を利用して取引を行った際に、再振替の情報が付与されている口座への入金後、残高不足により再振替が未成立となった場合、ATM が通帳を取り込んだまま休止する障害が発生した。

＜原因＞

- 委託先担当者は、現行システムである他社の仕様書との差異を検知したが、修正は不要と誤認し、そのまま開発及びテストを行った。
- 当行は仕様書の差異の確認を委託先に任せ、調査結果を確認していなかったため、当行による受入テストにおいてテスト項目として設定していなかった。

＜対策＞

- ATM 等の重要システムに対し、委託先で実施した仕様差異の確認結果について内容や妥当性を確認
- 確認結果を基にした受入テストのテスト計画・テスト項目の作成

６ 第三者型ＩＣＯ[47]上場直後からログインしにくい状況と、暗号資産取引所及び販売所において取引しにくい状況が発生

＜業態＞

暗号資産交換業者

＜事象＞

- 第三者型ＩＣＯとして新規銘柄上場直後から当社サービスへのログインしにくい状況と、暗号資産取引所及び販売所において取引しにくい状況が発生。
- アプリのトップページで上場銘柄の価格を表示する際に、当社販売所の価格を取得する仕様としており、上場前は価格情報が生成されていないことから、データベースのフルスキャンが行われ、データベースサーバーの負荷が増大してログイン不可となった。

＜原因＞

- 新規銘柄上場時にトップページの価格表示方法が通常とは異なることについて考慮から漏れていた。
- 新規銘柄上場前に販売システムの負荷テストは実施していたが、上記の考慮漏れによりトップページの性能テストを実施していなかった。

＜対策＞

- 価格情報が生成されていない状態でのデータベース検索方法を改修
- 新規銘柄上場時における性能テストの範囲を見直し

７ メモリ領域不足に起因した為替取引不可

＜業態＞

資金清算機関

＜事象１＞

- システム更改による OS の非互換対応 [48]において、テーブル生成プログラムの考慮漏れによるメモリ領域不足に起因して、テーブル更新作業過程でテーブルの内容が一部破損したことにより、移行後初日の営業日にシステムがダウンして移行対象の加盟行との間における為替取引が行えなかった。

＜原因１＞

- 外部委託先のレビュー体制及び試験内容の確認が十分でなかった。
- 再委託先の人員体制やスキル習熟状況を把握しておらず、システム開発に関する外部

[47] 業等がトークンと呼ばれるものを電子的に発行して、公衆から法定通貨や暗号資産等の調達を行う行為の総称。「Initial Coin Offering」の略。トークンの発行者が販売を行う自社型ＩＣＯと、暗号資産交換業者がトークンの発行者に代わって販売を行う第三者型ＩＣＯがある。

[48] OS のバージョン変更に伴い、旧バージョンからの互換性がない対象を洗い出して開発・修正を行い、新バージョンの OS に対応できるようにする対応

委託先全体の業務遂行能力の評価・検証を十分に実施していなかった。

＜対策１＞

- 外部委託先の開発時の各工程におけるレビュー体制の適切性確認及び試験内容の十分性確認の実施
- 再委託先を含む外部委託先に対する業務遂行能力の評価・検証の実施

＜事象２＞

- 障害復旧対応に時間を要し、障害発生日当日にシステムを復旧させることができなかった。また、代替手段による処理を円滑に行うことができなかった。

＜原因２＞

- システムの移行に関して、リスクに応じた移行方法（両センター同時移行）・移行時期（移行対象銀行・移行時期分散、繁忙日・連休明け）の妥当性検証が十分でなかった。
- 障害復旧対応において、復旧に係る暫定対処の適切性の判断や復旧対応に係るタイムマネジメントが十分でなかった。
- 本プロジェクトのリスクを想定した固有の BCP が未整備であった。
- BCP の発動基準や代替手段を実施する際の具体的なルールや手順が未整備であった。
- BCP に基づく訓練が不足しており、BCP の実効性（障害復旧対応に係る作業等の所要時間、加盟銀行ごとの BCP に係る習熟度等）の把握・検証を実施しておらず、BCP の実効性を確保していなかった。
- 大規模障害発生時の対外告知等の対応事項の整備が十分でなかった。また、大規模障害時の対応体制等も明確にされていなかった。
- 平時からの実践的な訓練も不足しており、障害対応力が十分でなかった。

＜対策２＞

- 両センター同時障害発生等のリスクや加盟金融機関の影響を踏まえた適切な移行方法・時期の検討方法に関するマニュアルの整備
- 障害復旧対応における優先順位の整備、復旧方法の決定に当たっての複数プランの比較検討及び適切なタイムマネジメントの実施方法に関するマニュアルの整備
- システム開発案件の特性を踏まえたプロジェクト固有の BCP 整備
- 平時からの備えとしての BCP・代替手段の運用ルールの整備・強化による実効性の確保
- 大規模障害発生時の対外告知等の対応事項の明確化及び大規模障害時の対応体制・役割分担の明確化
- システム障害対応研修の実施及び今回の障害を踏まえた実践的な訓練の実施

＜事象１、２に係る共通の課題と対策＞

- システムに関する専門性や経験値が十分に蓄積されず、上記障害の対策を検討するためのシステム人材が不足しているため、システム人材の育成・確保を図る。

- システム開発・運用に関する検討を実施する委員会等の役割も不明確で、知見も十分に活用されていなかったため、CIO 設置による事務局体制の強化、銀行知見活用による各検討体制の強化及び外部目線によるチェック強化を行うことにより、組織全体の体制の強化を図る。

８ 長期間にわたるシステム停止による ATM 非稼働

＜業態＞

地域銀行

＜事象＞

- 年末年始を利用した新システムへの移行において、ATM を停止していたが、新システムの稼働時に ATM 内部の機器のエラーを検知し、一部の ATM が利用不可となった。

＜原因＞

- 長期間にわたり低温環境下で ATM を停止していたことで機器内の部品が正常に動作しなくなった。

＜対策＞

- ATM を長期間停止させるなどの重要イベントを実施する際は、事前に想定リスクを提示するように機器の提供会社や委託先に申し入れを行う。

９ 復旧手順の不備による障害対応時間の長期化

＜業態＞

主要行等

＜事象＞

- ネットワーク機器の不具合により、総合振込のエラーが発生した。社内関係各部への情報共有の遅延や複雑な BCP により、時限内に対応が行えなかった。

＜原因＞

- 提供するサービスの障害発生時における初動対応の手順が不明確だった。
- 総合振込のエラーをカバーする BCP の網羅性が不足し、BCP が有効に機能しなかった。
- 復旧作業にあたり、BCP で定めていない作業手順から検討したため、所要時間の見積りを正しく評価できず、時限を過ぎても対応を終えることができなかった。

＜対策＞

- サービスごと（総合振込、口座振替等）の復旧対応手順の整備
- BCP の見直しと訓練の実施
- 復旧目標時刻までにシステム復旧が見込めない場合の対応方針の明確化

１０ 性能の仕様の理解不足による一部 ATM 停止

＜業態＞

主要行等

＜事象＞

- ATM を利用したキャッシング取引でのタイムアウトにより、一部の ATM でキャッシング取引が不可となり、当該 ATM が停止した。

＜原因＞

- 設計書やテストケースのレビュー時に有識者がレビューに参画していなかった。
- 勘定系システムと ATM 等を中継するシステムの性能に関する仕様の理解が不足していた。
- 本番同等の ATM の取引量を想定した負荷テストを実施していなかった。

＜対策＞

- 開発時におけるレビューアの適切な配置
- 設計書の記載の充実
- 本番稼働を想定した高負荷テストの実施

１１ リリース作業誤りによる仕向振込・被仕向入金一部不可

＜業態＞

主要行等

＜事象＞

- プログラムのリリース作業誤りにより、全銀システム関連機能が意図せず二重起動したことに起因し、当該機能がダウンと再起動を繰り返し、全銀システムとの通信が不安定な状態となった。これにより、仕向振込及び被仕向入金が一部不可等となった。また、復旧方法を誤り、仕向振込の二重送信等が発生した。

＜原因＞

- 本番環境に準じたテスト環境を構築した上でのリリース作業手順確認を実施していなかった。
- 外部委託先からリリース作業が遅延しているという報告を受けていたものの、リリース時間が全銀システムに与える影響を認識しないままリリースを承認してしまった。
- 全銀システムとの接続復旧後に電文を送信する際に電文ごとに不整合の発生有無を確認していなかった。

＜対策＞

- 本番環境に準じたテスト環境の構築とリリース作業手順確認の実施
- リリースプロセス見直しの実施
- 障害復旧時の手順の整備

１２ メモリ管理不具合による取引遅延

＜業態＞

主要行等

＜事象＞

- 新システム稼働後に大量データの入出力が発生した際、メモリを確保できずサーバー全体がスローダウンしたことにより、仕向振込、被仕向入金が遅延した。

＜原因＞

- バックアップ処理において、不要なファイルをコピーして必要以上の入出力が発生したことにより、データを一時的に保管するメモリを確保できなかった。
- サーバーがスローダウンした際にアラートを送信する仕組みがなかった。

＜対策＞

- バックアップ処理を必要なファイルのみコピーするよう変更
- メモリの開放要求が発生したタイミングでアラートを発出する処理の追加

１３ IB サービス提供側の対応漏れによる法人 IB 上の取引不可

＜業態＞

信用金庫・信用組合等

＜事象＞

- 法人 IB 上の取引が不可となる事象が発生した。

＜原因＞

- 事前に実施された勘定系システム更改にあたり、IB サービス提供者側の開局・閉局処理プロセスに対応漏れがあった。

＜対策＞

- IB サービス提供者側における死活監視・再起動機能の導入
- 開局・閉局要求を送信するタイミングが他の信用金庫と重ならないよう調整
- IB サービス提供者側における複数要員確保、連絡体制等の整備

１４ システム更改時のプログラム誤りによる取引エラー

＜業態＞

信用金庫・信用組合等

＜事象＞

- ATM の他行カード振込取引を行った際、振込金額の支払取引のみが成立し、振込自体がエラーとなる事象が発生した。

＜原因＞

- 勘定系システム更改の対応において、通帳振込機能のプログラムに誤りがあり、他行カードを利用した振込処理の際、他行宛振込支払応答処理でカードを利用した振込実行処理を実施すべきところ、通帳を利用した振込実行処理を実施し、当該振込実行処理で業務エラーが発生した。

＜対策＞

- 委託責任者としての各種検証、テスト実施
- システム更改期間中の緊急時における信用金庫内及び外部委託先を中心とした外部関係機関との情報連携強化

１５ システム更改時のプログラム誤りによる取引エラー②

＜業態＞

信用金庫・信用組合等

＜事象＞

- 一部地域のクレジット会社のカードを利用した ATM 取引がエラーとなる事象が発生した。

＜原因＞

- 勘定系システム更改にあたり、外部委託先が開発した地域クレジット会社のカード種別を判別するプログラムに不備があった。
- 外部委託先において、クレジット会社のカードの利用に係るテストの実施対象を全国的なクレジット会社のカードに限定し、地域クレジット会社のカードに対するテストを行わなかったため、本件不備が検知されなかった。
- 外部委託先から修正プログラムのテスト結果が良好との報告を受け、修正プログラムのリリースを了承し一時復旧したと認識したが、実際はテスト環境で実施していないカード情報の復号処理プログラムに不備が内包されていたため、再度不備が発生した。

＜対策＞

- システム更改時における網羅性のあるテストの実施
- 本番環境とテスト環境の差異の整備

１６ システム更改時のプログラム誤りによるキャッシュカード使用不可

＜業態＞

信用金庫・信用組合等

＜事象＞

- ATM で生体認証 IC キャッシュカードが使用不可となる事象が発生した。

＜原因＞

- 勘定系システムの更改における IC 認証に関するプログラムに不備があった。
- 生体認証 IC キャッシュカード発行開始当初、IC チップ内の一部データ項目が未設定の状態で発行されたものがあり、当該カードも問題なく利用できるよう更改前のシステムのプログラムに改修を加えていたが、更改後のシステムには想定したプログラムが反映できていなかった。
- 今回不具合が発生する条件のテスト用の生体認証 IC キャッシュカードが手元になく確認テストができていなかったため、事前に不具合の検出ができなかった。

＜対策＞

- 新しいキャッシュカードを発行する際、将来のプログラム改修に備え、テストで使用するキャッシュカード等を準備及び厳格に保管し、テスト実施を徹底

１７ 仕様の把握ミスに起因した入金金額相違

＜業態＞

金融商品取引業者等

＜事象＞

- 営業店でのリアルタイム口座振替指示（取引明細指定）において、振替指示画面上の

受渡日の前日基準残高が誤って表示されていたことにより、誤った振替指示が実行された。

＜原因＞

- 前日基準残高の算出は外部委託先が提供する共同利用型システムの既存仕様にあるロジックを用いて構築したが、旧システムの類似したロジックと利用用途が同様であると思い込んだため、調査・設計の不足があることに気づくことができなかった。
- パターンの網羅性を考慮したテストを実施することができなかった。

＜対策＞

- 新旧システムの仕様に関する差分等の検証態勢の強化

１８ 旧銀行カードによるATM利用不可

＜業態＞

地域銀行

＜事象＞

- 共同センターへの移行において、ATMによる他行宛振込処理で旧銀行の廃止店発行のキャッシュカードを使用した場合、廃止店のためテーブルに登録がなく異動明細作成処理が異常終了したことにより、他行宛てATM振込不可となった。

＜原因＞

- 共同センターの仕様に、当行では不要なテーブルを参照する処理が含まれていたが、事前にその処理の必要性を確認していなかった。

＜対策＞

- 共同センターのカード取引における機能変更時、廃止店番に対する仕様の確認

第３章　日常の運用・保守等の過程の中で発生したシステム障害

第１節　ハードウェア・回線等の不具合

１　海外データセンターにおけるネットワーク障害新規

＜業態＞

金融商品取引業者等

＜事象＞

- 海外データセンター内にあるネットワーク接続用機器が全て通信不能となるシステム障害が発生した。
- また、復旧に際しても、当該データセンターが外部と通信不能となり、セカンダリーデータセンターへの切替に時間を要したことから、重要なアプリケーションの一部が遅延した。

＜原因＞

- ネットワークの運用管理をサービス提供ベンダーに委託し、ネットワーク機器はサービス提供ベンダーの提携先が提供している。

- 本障害は海外の営業時間中にデータセンター内に設置された当該ネットワーク機器に対して、委託元の許可を得ずにサービス提供ベンダーの提携先エンジニアがメンテナンス作業として順次再起動したところ、想定外の挙動が発生し、冗長構成を持つネットワーク機器全てに誤った設定情報（初期設定値）が配信され、通信不能となる障害が発生した。
- また、別の委託先が過去に実施したファイルサーバーの移管作業において、一部の重要なアプリケーションに関するファイルを冗長性のあるセカンダリーデータセンターへ複製・同期できていなかったため、本障害時において復旧に必要な構成ファイルが存在せず、セカンダリーデータセンターへの切替に時間を要し、復旧が遅延した。
- さらに、当社も過去に実施したデータセンター切替テストにおいて、テストの対象を限定していたことから上記不備の発見につながらなかった。

＜対策＞

- 外部委託している主要サービス等の見直しや委託先に対する監査・統制を厳格化
- 重要なアプリケーションの依存関係を見直してリスク低減を実施。また、レガシーファイルの利用を見直し、構成ストレージを最新化
- 年次で切替テストを実施

２　ハードウェア障害に起因する障害後の処理遅延新規

＜業態＞

主要行等

＜事象＞

- 国内勘定系システムにおいて、データ授受を行う入出力装置の不具合によりシステム設定ファイルが破損し、ホストが停止したもの。

＜原因＞

- 障害発生後、待機系への切替や再起動による復旧を試みたが、復旧に時間を要したもの。
- この結果、バッチ処理の開始が遅延し、後続処理にも影響が生じたもの。

＜対策＞

- 障害箇所を早期に検知し、影響範囲を限定するための検知機能の高度化
- 待機系切替時に必要ファイルへ不具合が生じた場合の修復手順の整備・自動化
- 入出力装置の障害がシステム設定ファイルの破損につながらないよう、装置面での対策を検討

３　電源回路の異常に伴う送金システムの障害新規

＜業態＞

主要行等

＜事象＞

- ハードウェア故障により、他行への送金（仕向）の一部取扱いができない事象が発生

した。
- また、障害の影響で、他行からの送金（被仕向）の一部取扱いに着金遅延が発生した。

＜原因＞
- 送金システムにおいて、一部スイッチカードの電源回路の異常が発生したもの。
- 電源回路の異常によるハードウェア故障の場合、一般的なハードウェア故障と異なり、ホスト間の通信パスが切断され、手動で通信パスを復旧する仕様（製品仕様）であったが、切断パスの特定及び手動による通信パスの復旧手順の整備が不十分であった。

＜対策＞
- ハードウェア故障による復旧手順の選択に必要な「ホスト間の通信パスの切断事象及び切断パスの特定をメッセージから迅速に把握する手順」及び「切断パスの復旧手順」の整備

４　ハードウェア障害に起因する為替業務の復旧対応遅延新規

＜業態＞

信用金庫・信用組合等

＜事象＞
- ハードウェア障害を起因としたファームウェア不具合により、オンライン取引や為替業務の開始遅延、各種バッチ処理の遅延等が発生。この結果、為替業務が利用不可となり、一部の振込取引に遅延が生じた。
- 上記の遅延に対する影響把握と対応に長時間を要したことから、対外公表及び関係者への情報共有を迅速に実施できなかった。

＜原因＞
- 本番環境に影響を及ぼす可能性のある機器交換作業において、リスク評価及び影響分析が不十分であったため、作業後に生じた通信の不安定化を重大障害の予兆として認識できなかった。
- 障害の深刻度評価基準及び運用ルールが不明確であったため、関係者の招集やエスカレーションが迅速に行われず、初動対応が遅延した。
- 設計書・ドキュメントが不足しており、緊急対応手順やコンティンジェンシープランの整備も不十分であった。
- 障害対応拠点の分散による指揮系統の曖昧さや口頭中心の情報共有、情報発信基準の未整備により、適切な判断・情報連携が行われなかった。

＜対策＞
- 障害対応態勢、設計書・ドキュメント、緊急対応手順及びコンティンジェンシープランの整備
- 障害対応における統括責任者、意思決定プロセス、情報集約窓口及び情報発信基準の明確化
- 委託先との役割分担、承認プロセス及びエスカレーションルールの整理、定期的な障害訓練の実施

５　ハードウェア故障による光量低下時の対応不備

＜業態＞

主要行等

＜事象＞

- データセンターにおいてハードウェアの故障が発生した。当該ハードウェアが完全に停止しなかったことに起因してシステム全体が不安定な状態となり、サービスへのログインできない事象が長時間継続した。該当時間帯の全取引が不可となった。

＜原因＞

- SAN（Storage Area Network）スイッチのポート障害（光量低下）を起因としてシステム全体が不安定となった。結果として SAN スイッチ障害が全体のサービス停止に至る（DB サーバー停止）。
- SAN スイッチ障害に起因する DB サーバー全面停止を想定した復旧手順の整備がされていなかったため復旧に時間を要した。

＜対策＞

- 光量低下時のアラート検出基準の閾値の設定。定期的な光量チェックにて、閾値を下回ったらエラーを出す仕組みを導入
- スイッチポートの光量低下時に、特定の条件下ではコントローラにまで影響を与えてしまう事象が発生したことを踏まえ、コントローラの通信経路を見直し。SAN スイッチからストレージへの通信経路上に 2 台のコントローラの通信経路が完全に独立する構成に変更
- 本障害の復旧時の問題点も踏まえた手順を策定

６　ネットワーク回線のハードウェア故障に対する復旧対応遅延

＜業態＞

地域銀行

＜事象＞

- 銀行とデータセンターの間にあるネットワーク機器でハードウェア障害が発生したが、機器が完全に停止しなかったことでバックアップ回線への切り替え動作が正常に行われず、切り替えと切り戻しを繰り返す不安定な状態となったことで ATM の取引や外部接続先のシステムとの通信が不能となった。
- 回線復旧後に外部接続先のシステムとの通信を復旧させるには、手動での再接続作業が必要であったため、全システムが利用可能になるまでに時間を要した。

＜原因＞

- 機器の挙動の監視や、異常状態を検知するシステム構成としていなかった。
- 複数の外部接続先システムが同時に通信不能となることを想定していなかった。

＜対策＞

- 切り替えと切り戻しを繰り返すような不安定な通信状態を検知し自動で切り替えや切り離しを行えるようシステム構成を変更

- 複数の外部接続先との通信不能を想定した復旧手順の整備と訓練の実施

7　障害原因未特定による障害の再発

＜業態＞

資金移動業者等

＜事象＞

- データベースサーバーの製品不具合により、決済アプリを利用した取引ができない状況が発生した。
- データベースサーバーの再起動により、事象が解消したが、翌日に同様の障害が発生した。

＜原因＞

- 直前にリリースした案件により、特定の SQL の実行が急増し、データベースサーバーのリソースが枯渇した。
- データベースサーバーの再起動により、正常に動作したため復旧したと判断したが、障害原因の特定及び対処ができていなかった。

＜対策＞

- データベースサーバーの不具合を引き起こす SQL の実行条件の見直し
- 開発工程における性能検証の強化
- 製品パッチ適用運用の見直し

8　システムの依存関係の認識不足による出金サービス利用不可

＜業態＞

資金移動業者等

＜事象＞

- 決済する際にポイントを付与・利用するために、ポイントシステムに API 接続している。ポイントシステムのデータベースで障害が発生したため、復旧作業の一環で API サーバーの再起動を実施したが、再起動の手順に漏れがあり、滞留していた取引データを決済システムに連携ができず、出金サービスが利用できなくなった。

＜原因＞

- サーバーの再起動手順に不備があり、データ連携機能の再起動が漏れたため、機能が停止した。
- API サーバーを再起動した際の作業の依存関係の認識が不足していた。

＜対策＞

- 作業手順書の作成段階におけるチェック体制の強化
- 再起動時の対応手順の自動化
- 決済システムとポイントシステムの依存関係をまとめた資料整備

9　データセンターの障害による勘定系システム停止

＜業態＞

主要行等、地域銀行

＜事象＞

- 外部委託先が運営する共同センターのデータセンター内の設備が点検作業中に故障したことに起因し、共同センターの全加盟行の勘定系システムへの給電が停止し、その復旧に時間を要したことで、ATM や営業店等での全取引が長時間利用不可となった。また、通帳等の取込みも多数発生した。

＜原因＞

- 全加盟行のシステム一斉停止を想定したシステムの復旧対応に関する態勢を整備していなかった。
- データセンター内の設備に対する点検作業の安全性等の評価やチェック態勢が十分ではなかった。

＜対策＞

- 全加盟行のシステム停止、複数のシステムの停止を想定した各種復旧手順の作成や有識者の育成、障害訓練の実施等の復旧態勢の整備
- 点検作業のリスクや作業プロセスの確認・評価態勢の整備

１０ ネットワーク機器の故障に起因する決済業務の復旧対応遅延

＜業態＞

主要行等

＜事象＞

- 外部委託先によるネットワーク設定変更作業に誤りがあったためネットワークが高負荷となり、約４時間、顧客の決済がエラーとなった。

＜原因＞

- 本番環境に影響があるにもかかわらず、影響を過小評価して本番環境稼働中にネットワーク設定変更作業を行ってしまった。
- 作業手順を整備していなかった。
- システム復旧手順を整備していなかった。

＜対策＞

- 本番環境に対する設定変更作業等の禁止事項・ルールの整備
- 作業手順の整備
- システム復旧手順の整備

１１ ネットワーク機器の故障に起因する未処理取引の復旧対応遅延

＜業態＞

主要行等

＜事象＞

- 全銀システムと勘定系システムとの間の一部経路切断により、取引が滞留し、仕掛り中の処理が発生した。当該ネットワークの一部経路が一時切断していたため、顧客の仕向取引及び被仕向取引の電文が滞留し、未処理の取引が発生した。また、未処理の

取引が発生した際の業務影響有無の特定に時間を要した。

＜原因＞

- 未処理の有無を確認する作業手順を整備していなかった。
- 未処理発生時の対応手順を整備していなかった。

＜対策＞

- 未処理有無の確認手順の整備
- 未処理発生時の対応手順の整備

１２ ネットワーク機器の故障に起因するサービス復旧対応遅延

＜業態＞

主要行等

＜事象＞

- 交換を予定していたネットワーク機器が故障したにもかかわらず、通信が断続的に正常応答したため、他系統への自動切替えが行われず、法人向けサービスの一部で取引エラーが発生した。また、ネットワーク機器のエラー解消後にサービスを早期に復旧できなかった。

＜原因＞

- 機器交換までに期間が空くことを踏まえ、交換実施までの間にエラーが発生した場合の対処方針を策定していなかった。
- ネットワーク機器のエラー時に電文破棄や処理待ち状態が発生する際の対応手順をあらかじめ準備していなかった。

＜対策＞

- 予兆点検における交換対象機器のエラー発生時に向けた対応手順の整備
- 電文破棄や処理待ち状態発生時の対応手順の整備

１３ ネットワーク機器の故障に起因する決済業務の復旧対応遅延

＜業態＞

主要行等

＜事象＞

- ベンダーが提供するプライベートクラウドのネットワーク機器の間欠障害により、自動で副系統に切り替わらなかったことに起因し、決済業務が不可となった。また、当該機器の故障により、データベースサーバーに不要なトランザクションが蓄積し、その原因特定に手間取ったことから勘定系システムの復旧まで時間を要した。

＜原因＞

- ネットワーク機器の予兆監視を十分に実施していなかった。
- ネットワーク障害時の復旧手順書を整備していなかった。
- データベースサーバーの不要なデータの蓄積状況を確認していなかった。

＜対策＞

- ネットワーク機器を予兆監視対象として追加

- ネットワーク障害時の復旧手順の整備
- ネットワーク障害時にデータベースサーバーの状態を確認・対処する手順の整備

１４ ソフトウェア（OS）の不具合により冗長構成が機能せずATMが停止

＜業態＞

地域銀行

＜事象＞

- 勘定系システムと接続しているネットワーク機器が故障した際、当該ネットワーク機器のOSの不具合により、待機系に制御機能が引き継がれず、勘定系システムとの通信が停止し、ATMやIBが利用不可となった。

＜原因＞

- 購入したネットワーク機器のOSの不具合であり、導入時のテストや検証では、製品そのもののテストは行わないため、不具合を発見できなかった。

＜対策＞

- 重要ネットワーク機器の特定、OSのバージョン管理の実施

１５ ネットワーク機器の異常によるIB利用不可

＜業態＞

地域銀行

＜事象＞

- ネットワーク機器がハードウェアの異常を検知し、待機系への自動切替えが発生した。その影響を受けてIB等で利用しているネットワーク一部経路が閉塞し、該当経路でのIB等が利用不可となった。

＜原因＞

- ネットワーク機器が待機系に切り替わるまでの時間だけでなく、その後のリカバリー対応が完了するまでの間、一部のIB等が停止したままになってしまう影響を把握できておらず、復旧手順の整備ができていなかった。

＜対策＞

- リカバリー対応が完了するまでの間の影響把握、復旧手順の整備

１６ ネットワーク機器故障によるATM利用不可

＜業態＞

地域銀行

＜事象＞

- 勘定系システムと対外センターと接続するネットワーク機器にハードウェア障害が発生し、予備機への切替えが行われたものの、通信状態が不安定となり予備機が閉塞し、ATMが利用不可となった。

＜原因＞

- 上記とは異なる上位のネットワーク機器の故障が原因で通信が不安定になったが、事

象が発生した際にその原因の特定ができなかった。

＜対策＞

- ネットワーク機器故障の予兆検知実施

１７ 障害発生時のバックアップ回線への切替え失敗

＜業態＞

信用金庫・信用組合等

＜事象＞

- メイン回線用のルータ故障により、一部支店の全てのオンライン取引が停止する事象が発生した。本来であれば即時バックアップ回線へ切替え運用可能となるところ、バックアップ回線への切替えに失敗したため不通の状態となり、復旧までに時間を要した。

＜原因＞

- ルータと通信アダプタが接触不良の状態のままバックアップ回線への切替えを実施し、切替えに失敗した。

＜対策＞

- 全店舗にバックアップ回線機器のランプ状態の確認及び再起動手順を整備
- 定期点検保守時に毎回メイン・バックアップ回線通信機器のランプ状態を確認し、保守記録に掲載

第２節　設定ミス・操作ミス等の管理面・人的要因

１ 資金決済ネットワーク関連システム障害の復旧作業誤り新規

＜業態＞

地域銀行

＜事象＞

- 資金決済ネットワークに接続する中継システムでソフトウェアバグによる障害が発生し、送受信される一部の為替電文に滞留が生じた。その後、滞留電文の復旧作業を実施する過程で、電文管理上の誤りが発生し、一部取引において二重送信、二重着金及び未着金が生じる事象が確認された。

＜原因＞

- 障害復旧作業における人的対応の誤り

＜対策＞

- 訓練及び教育の強化による障害対応力の向上
- 本番環境作業前における開発環境での検証・確認手順の明確化及び徹底

２ 送金再開処理に係る対応不備等による送金遅延新規

＜業態＞

資金移動業者等

＜事象＞

- 顧客からの依頼に基づく送金に際し、当社側の送金用口座に残高不足が発生したため、残高不足を解消の上、送金再開処理を実施した。しかしながら、再開処理の対応に不備があったため、送金は再開されなかった。
- また、担当者は再開処理後の動作確認を行っておらず、かつ、システム側で送金が正常に再開していないことを警告する機能を有していなかったため、顧客からの問い合わせにより発覚するまで、送金が停止したままとなっていた。

＜原因＞

- 担当者がマニュアルの読み取りを誤り、送金再開処理の手順に対応漏れがあった。
- 再開処理後の動作確認が徹底されていなかった。
- 送金が正常に再開していないことを警告する機能を有していなかった。

＜対策＞

- 送金再開処理に係るマニュアルを誤認しない内容に修正
- 再開処理後の動作確認の徹底や第三者の立会いについてマニュアルに明記
- 再開処理が実施されていない場合、一定時間毎に繰り返し警告する機能を既存の検知システムに追加

３ メンテナンス作業における作業不備

＜業態＞

主要行等、地域銀行

＜事象＞

- 複数の金融機関が利用するシステム基盤の移行環境のハードウェア交換作業において、誤った作業手順でメンテナンス作業を実施したことに起因し、本番環境の外接系等のシステムが停止し、IB において口座振替等のサービスが利用不可となる事象が発生した。
- また、上記障害の復旧までに長時間を要したことに加え、銀行から顧客への障害状況の周知が適時に行われていなかったこと等に起因して、顧客からの苦情が複数件発生した。

＜原因＞

- メンテナンス作業を実施したシステムは、本番昇格前の筐体であったが、将来的に本番環境として運用を開始する想定の環境であったため、一部ストレージを本番環境と共用する構成となっていた。
- 本メンテナンス作業において、設計書の判読性の低さにより作業者が誤認したため、移行環境と本番環境が一部ストレージを共用していることに気づけず、本番環境からの移行環境への参照を抑止する手順が漏れた状態で移行環境の筐体の電源切断を行ったことにより、本番環境のファイルシステムが破損した。
- また、ファイルシステムの破損を想定した障害マニュアルが準備されていなかったことが、復旧に長時間を要する一因となった。

＜対策＞

- メンテナンス作業のリスクを適切に識別するためにシステム環境を熟知した有識者によるレビューの実施を徹底
- 設計書の誤認防止のためのレビュー体制強化のほか、リスクに応じて作業実施時間帯を定め、本番稼働に影響を及ぼす作業については原則計画停止かつメンテナンスモードで実施
- 移行環境を本番昇格前までは物理的にも分割される構成に変更
- 同様の事象発生時の復旧時間短縮を図るため、最重要システムにおいてファイルシステム破損を想定した障害マニュアルを整備
- 復旧までの対応早期化を目的とし、障害発生時の連絡体制・運用を改善し、ホームページにおける顧客告知方法を整備

４ ネットワークの冗長化構成の設定誤り

＜業態＞

主要行等

＜事象＞

- DB サーバーと通信機器を接続するネットワークの冗長化構成の設定を誤り、２台の DB サーバーが通信機器のうち特定の１台のみに繋がるネットワーク構成になっていた。メンテナンス時に、１台の通信機器をシャットダウンしたことによりシステムを利用する全ての取引・サービスが利用不可となる事象が発生した。

＜原因＞

- 仮想サーバー環境の場合、ネットワークの冗長化はクラウドサービスとして保証されているが、ベアメタルサーバー環境[49]の場合、物理的な機器・ネットワークはクラウド側で準備されるものの、各種設定はユーザ側が実施する役割分担となっていた。この役割分担はマニュアルに記載されていなかったため、クラウド側でネットワークの冗長化まで行うものと誤認していた。
- DB サーバーがダウンした場合の冗長化テストは実施していたが、ネットワークの冗長化はクラウドサービス側で保証されているとユーザ側が誤認していたため、通信機器の冗長化テストを実施していなかった。

＜対策＞

- メンテナンス・更改等の設計時に考慮漏れが発生しないよう、ベアメタルサーバー環境においては通信機器のハードウェア設定はクラウド側が担当し、OS 等ソフトウェアの通信パラメータ設定はユーザ側が担当することをマニュアルと設計時のチェックリストに記載

５ レビュー観点不足に起因したプログラム誤りによる誤入出金

＜業態＞

主要行等

＜事象＞

[49] ベアメタルサーバー環境とは、クラウドサービスにおいて物理サーバーを提供している環境。

- ATM において、QR コードを用いた入出金を行った際、別 ATM で同時刻に同様の操作を行った別顧客の口座に入出金される事象が発生した。

＜原因＞

- QR コードの生成において、全ての取引の取引キーが重複しないよう一意となる必要があるが、要件定義の内容が後続の設計書やプログラムまで反映されているかという観点でのレビューが不足していた。
- プログラム設計・担当者が要件を正しく理解できる記載となっているかという観点でのレビューが不足していた。

＜対策＞

- 設計書やプログラムのレビュー時の要件定義反映に係るレビュー観点の追加
- プログラム設計・担当者が要件を正しく理解できる記載となっているかという観点での有識者による確認実施と第三者（品質保証部門担当者等）による客観的な確認の実施

６ パッチ未適用により冗長機能が機能しない

＜業態＞

地域銀行

＜事象＞

- 勘定系システムでハードウェア障害が発生し、主系統から副系統に切り替わったが、副系統で通信が不可となり、勘定系システムに関する全ての取引が不可となった。

＜原因＞

- 副系統に切り替わった際、パッチを適用していなかった OS の不具合が顕在化した。
- 外部委託先において、パッチの適用について緊急性の高さのみで判断しており、外部委託先に対しパッチ未適用と判断した根拠まで確認していなかった。
- 委託元として、パッチを適用しない判断を行った場合の影響等を確認していなかった。

＜対策＞

- パッチ適用に対する評価や影響に関する確認の強化
- パッチを適用する判断基準の明確化
- パッチ適用を見送った際の、障害の顕在化を想定した復旧手順の整備や訓練の実施

７ 業務時間帯で実施した保守作業による ATM 利用不可

＜業態＞

地域銀行

＜事象＞

- システム運用作業を業務時間帯に実施し、勘定系システムに係る通信がタイムアウトして一部 ATM が利用不可となった。

＜原因＞

- システムの運用者と勘定系システムが使用する WAN 回線は、同一の回線を使用してお

り、システム運用者が行う作業がネットワークに過大な負荷を与えた。
- システム運用者が行う作業の実施時間について、その妥当性を確認していなかった。

＜対策＞
- 業務時間中に実施する運用作業の洗い出しとリスクの確認
- 上記を基に運用作業時間の変更

８ 設定誤りにより冗長構成が機能せずアプリ利用不可

＜業態＞

信用金庫・信用組合等

＜事象＞
- メイン基盤で障害が発生した際、バックアップ基盤への切替えが実施されたが、バックアップ基盤が作動せずにアプリにて取引照会等が行えなくなった。

＜原因＞
- バックアップ基盤内の通信設定にメイン基盤向けの IP アドレスが設定されていた。
- テスト工程でフェールオーバーができることを確認した際、テスト後の環境戻しが十分ではなく、誤った設定が残ったままリリースしてしまった。

＜対策＞
- 機器更改時等に設定内容を確認するツールの作成とツールによる確認

９ 平時サービスで障害発生時に代替サービスへの自動切替えが失敗

＜業態＞

暗号資産交換業者

＜事象＞
- 当社のサービスに対し利用者がログイン等で使用する２段階認証のうち SMS 認証において、外部サービスで発生したシステム障害により、利用者へ認証コードが配信されない状態となった。
- 代替手段として準備していた他社サービスへ自動的に切替えが行われず、手動での切替え作業が完了するまでの間、２段階認証で SMS を選択している利用者がログイン、日本円の出金、暗号資産の送付等の操作を行うことができなかった。

＜原因＞
- 当社の SMS 認証で利用している外部サービスにおいて、当該サービスを利用する他社で特定の利用者が許容量を超えるリクエストを繰り返し実行したため、一時的にデータベースの負荷が高まり認証コードが配信できない障害が発生した。
- 当社において、利用サービスの自動切替えを判断する処理の不具合によりサービスの自動切替えが行われなかった。
- 当社内で手動切替えの手順が周知徹底されていなかったため、復旧まで時間を要した。

＜対策＞
- 外部サービス提供元事業者にて実施される再発防止策の確認

- 自動切替え処理に関する設計段階での検討体制の強化
- サービスを手動切替えする手順の周知徹底

１０ 設定誤りにより冗長構成が機能せず取引不可

＜業態＞
金融商品取引業者等
＜事象＞
- 日本株取引システムと証券取引所とのプライマリゲートウェイサーバーにおいて、ハードウェア障害が発生した際、セカンダリゲートウェイサーバーに切替わらず、証券取引所との接続が切断されて日本株取引を行うことができなかった。

＜原因＞
- グローバルのゲートウェイサーバー開発部署がプライマリゲートウェイサーバーとセカンダリゲートウェイサーバーのデータ同期を行う際、当社独自の同期設定を行う必要があったものの、その必要性を認識していなかったことから、グローバル版ゲートウェイサーバーにおける同期設定と同様の設定を行い、一部のデータが同期されずセカンダリゲートウェイサーバーがデータ紛失の可能性があると判断して立ち上がらなかった。
- セカンダリゲートウェイサーバーへの切替えテストは行っていたものの、休日に実施していたため、平日の運用で切替えできるか確認していなかった。

＜対策＞
- グローバル版ゲートウェイサーバーへの移行の検討
- 実運用に沿った切替えテストの実施

１１ システムへのデータ取り込み漏れ

＜業態＞
金融商品取引業者等
＜事象＞
- 証券取引所から受領したデータを売買審査システムに送信するシステムにおいて、システム変更で授受データ内容が変更になった際、売買審査システム側のデータ取り込み条件に該当しなくなり、データの取り込み漏れが発生した。

＜原因＞
- プロジェクトに業務部門が含まれておらず、IT 部門のみでテストケースを作成したことから、テスト内容が十分でなかった。
- 委託元、外部委託先の役割分担が明確でなく、システム仕様の確認が十分でなかった。

＜対策＞
- システム開発における業務部門の関与と業務部門によるテスト実施
- 委託元、外部委託先との役割分担明確化

１２ システム開発の検証・管理体制の不足による勘定不突合

＜業態＞

主要行等

＜事象＞

- 勘定系システムと外部接続先を接続するシステムにおいて、外部委託先及び再委託先が設計した電文作成処理が不要な電文を検索するロジックとなっていた。このため、当該処理が遅延して特定取引の電文が滞留し、当該システムを経由する取引の一部が約７時間にわたって利用しにくい状態となり、勘定不突合の事象が発生した。

＜原因＞

- 設計時の影響調査内容を検証する態勢が不十分だった。
- 外部委託先及び再委託先の体制面の検証や開発に対する検証態勢が不十分だった。
- 休日に障害が発生したため、開発要員が開発拠点に駆付ける必要があり、連絡に時間を要したことからシステム障害の状況等の詳細な調査を行うまでに時間を要した。

＜対策＞

- 設計時の影響調査検討状況と当該検討に係る検証態勢のチェック強化
- 外部委託先及び再委託先の検証・管理態勢のチェック強化
- 休日・夜間に顧客影響が大きいシステムで障害が発生したことを想定した障害訓練のバリエーション追加（一斉同報ツールやメーリングリストを活用した連絡の実施、本番環境へのリモートアクセス環境等を活用した調査の実施等）

１３ 勘定系システムの仕様把握不足による一部取引不可

＜業態＞

主要行等

＜事象＞

- 勘定系システムで管理している各種取引単位で採番される取引通番がシステムの上限値を超過したことにより、超過後のカードローン約定返済処理やデビットカード未精算顧客の銀行取引等が不可となった。
- 上記の影響を受けた顧客を特定してから影響範囲を特定するまでに時間を要し、顧客に迅速な連絡が実施できなかった。

＜原因＞

- 取引通番の採番方法を誤認していたことにより、取引通番の増加状況をモニタリングの対象から外していた。
- 発生事象（商品・サービス）によって顧客対応判断部署が分かれており、全社共通の統一された対応が確立されていなかった。

＜対策＞

- システム制約（システム上限値、閾値、桁数のある項目等）の明確化
- 勘定系システムの有識者育成
- システム障害発生時の顧客影響の範囲を再確認した上で、公開チャネル、タイミング、告知内容、顧客対応方法を整理

１４ 社内の関係部署との連携不足による作業誤りに起因したATM停止

＜業態＞
主要行等
＜事象＞
- 本番リリース作業時に本来再起動が不要なサーバーの再起動を行ったことに起因して、全てのカードローン専用のATMが利用不可となった。

＜原因＞
- システム開発担当からシステム運用担当へ本番リリース作業の際にサーバー再起動不要の連絡を行っていなかった。
- 本番リリース作業の障害による影響（ATM利用不可等）の把握ができておらず、本番リリース作業に係るテストを実施していなかった。

＜対策＞
- 本番リリース作業を行う際の作業手順の整備、作業手順の研修実施
- 本番リリース作業の対顧客業務への影響確認実施の徹底、対顧客業務に影響を与える時間帯での本番リリース作業禁止の徹底

１５ バージョンアップ方法誤りによる送金取引不可

＜業態＞
主要行等
＜事象＞
- 勘定系システムのデータベース（外部委託先提供）のバージョンアップの影響で、IBが利用不可となった。

＜原因＞
- データベースをバージョンアップする際、バージョンアップ前後のデータ属性、桁数の変更がないものと誤認し、必要なテストを実施していなかった。

＜対策＞
- データベースのバージョンアップやメンテナンス時におけるデータ属性の変更に伴う桁数増加についてテストケースの追加

１６ ネットワーク機器の故障に起因する出金取引エラー

＜業態＞
主要行等
＜事象＞
- ネットワーク機器の故障により、他系統に通信経路が切り替わったが、他系統にルート定義情報が設定されていなかったことにより、振込及び振替取引が不可となる事象が発生した。

＜原因＞
- 冗長構成として正系と副系で同様のルート定義情報が設定されるべきところ、作業指示書に不備があったことにより、副系のルート定義情報が正しく設定されていなかっ

た。

＜対策＞

- ネットワーク設計時にルート定義情報の作業指示書として定型化したテンプレートを活用した属人的なミスの抑制対策の実施

１７ 作業ミスによる誤ったプログラムを本番環境に反映したことに起因する金額表示の誤り

＜業態＞

金融商品取引業者等

＜事象＞

- オンライントレードサービスの注文時に確認画面に表示される金額が誤って表示された。

＜原因＞

- プログラムを本番環境に反映する際の手順ミスにより、テスト工程で不備を検知したプログラムを誤って本番環境に反映してしまった。

＜対策＞

- プログラムのバージョン管理及び本番反映手順の見直し
- プログラムのバージョン管理及び本番反映手順遵守の徹底

１８ テスト観点不足による金額表示の誤り

＜業態＞

金融商品取引業者等

＜事象＞

- スマートフォン用取引アプリの決済注文画面において、遷移前の画面で指定した建玉の評価損益が表示されるべきところ、建玉情報リスト取得ロジックの不具合により、顧客が保有する建玉が複数ある場合に正しい評価損益を表示することができなかった。

＜原因＞

- リグレッションテスト[50]において、決済注文画面に遷移する前の画面で指定した条件が正しく表示されることの確認を実施していなかった。

＜対策＞

- 遷移前の画面で指定した条件が正しく表示されることをリグレッションテストの確認観点に追加

１９ システム部門以外の有識者をアサインしないことによる設計工程の考慮漏れ

＜業態＞

金融商品取引業者等

＜事象＞

[50] プログラムの一部を変更・修正した際に、その変更によって予想外の影響が現れていないか確かめるテスト。

- 設計工程における口座紐付けパターンの考慮漏れにより、オンライントレードサービスの取引報告書、運用報告書等で一部の取引を表示できなかった。

＜原因＞

- 設計工程で要員をアサインする際、商品所管部の有識者をアサインせず、商品所管部であれば指摘できた現場事務やパターンを考慮できなかった。

＜対策＞

- 商品所管部門を含めた有識者のアサイン実施

２０ 機能追加による法人 IB 利用不可

＜業態＞

地域銀行

＜事象＞

- IB の共同センターにおいて新機能を導入したが、その影響で利用者端末の電子証明書検証処理がエラーとなり、法人 IB へのログインが不可となった。

＜原因＞

- 機能追加によるクライアント環境での検証が不足していた。
- 障害発生の可能性の把握及び障害が発生した場合の顧客への代替手段等の周知が不足していた。

＜対策＞

- 金融機関も含めた検証項目の十分性の確認と検証結果の確認
- 障害発生時のリスク認識の把握と不具合発生時の代替策の顧客周知

２１ 誤った復旧手順を実施したことによる ATM 停止

＜業態＞

地域銀行

＜事象＞

- 外部委託先において、ATM と接続するシステムを起動した際、バックアップ用アプリにおいてエラーが発生し、エラーの復旧対応を実施したが、作業手順の誤りにより、一部の ATM が開局不可となった。

＜原因＞

- 外部委託先からは、マニュアルに基づき復旧を実施との報告を受けていたが、本事象に合致するマニュアルはなく、復旧手順の整備を行っていなかった。

＜対策＞

- 復旧に関する外部委託先と委託元との対応範囲の明確化及び復旧手順の整備

２２ 証明書有効期限切れによるスマホアプリ利用不可

＜業態＞

地域銀行

＜事象＞

- スマホアプリを利用する IB（クラウドサービス上に構築。）のサーバーの正当性を証明するドメイン証明書の有効期限切れにより、サービスが利用不可となった。

＜原因＞

- クラウドサービスを提供する事業者がドメイン証明書の更新方法を変更したが、変更の事実を把握していなかった。

＜対策＞

- クラウドサービスにおいて有効期限設定されている項目の管理
- 管理項目の定例確認の実施

第３節　サードパーティの提供するサービス等の要因

１ 外部サービスでのハードウェア障害新規

＜業態＞

資金移動業者等

＜事象＞

- 外部のストレージサービス提供事業者のハードウェア障害に起因し、決済の一部が利用できない事象が発生した。

＜原因＞

- ストレージサービス提供事業者におけるハードウェアの主電源及び二次電源の電源喪失により、ストレージサービスの一部が利用不可となった。
- その結果、決済アプリから受け取るトランザクション処理が滞留し、支払い処理が不可能となった。

＜対策＞

- 障害影響を軽減させるため、今回と同様の事象が生じた際、早期の障害箇所の特定を可能とする監視設定の見直しを行う。
- 上記の監視設定のもと、自動で影響箇所の切り離しを行う機能を実装する。

２ クラウドサービス障害による業務サービスの利用不可新規

＜業態＞

地域銀行

＜事象＞

- 地域銀行が共同利用するクラウド基盤において、認証機能を提供するサービスで高負荷状態が発生し、新規の認証処理を受け付けることができなくなる障害が発生した。この影響により、認証の再取得が必要となったタイミングで一部の業務アプリケーションやインターネットバンキング等が利用できない状態となった。

＜原因＞

- クラウドサービスの機能改善を目的とした変更を実施した結果、認証システムとの間で想定外の通信が発生した。これにより、認証システムが急速に高負荷状態となり、クラウドサービス全体へのアクセスに影響が生じた。

＜対策＞

- 変更前の状態への復元
- 認証システムの予防的リソース増強

3 不正侵入防御システムの設定変更に起因するインターネットバンキングの利用支障 新規

＜業態＞

地域銀行

＜事象＞

- 複数銀行がインターネットバンキングを運用委託しているシステムセンターにおいて、不正侵入防御システム（IPS）の設定変更が行われた結果、正常な通信が攻撃通信と誤って判定され、通信が遮断される事象が発生した。この影響により、一部のインターネットバンキングサービスにおいて利用不可またはログインしづらい状態が生じた。

＜原因＞

- システム設定の変更に起因する不具合により、不適切な設定情報が生成・配布された。その結果、システムリソースが逼迫し、通信処理に支障が生じた。

＜対策＞

- 不適切な設定情報の生成・配布を停止。
- コアダンプやその他のエラーレポートがシステムリソースを圧迫する可能性の排除。

4 セキュリティソフト不具合への対応

＜業態＞

保険会社等

＜事象＞

- 業務で使用する端末において、セキュリティソフトの不具合により、画面がシステム異常停止時の青い画面になり再起動を繰り返す障害が発生した。復旧対応を行ったが解約払戻金等の支払いに一部遅延が発生した。

＜原因＞

- システム障害による業務影響の把握に関する対応が十分に整備されていなかった。
- システム停止による解約処理・期日支払処理の影響が把握できず、対象契約を至急扱いの人的処理とするプロセスがなかった。

＜対策＞

- 正確な業務影響の把握（業務影響把握フォーマットの改善等）
- 支払をシステム処理で行う契約の影響把握プロセスの構築
- 支払期日が迫っている契約の特定・優先処理の運用見直し

5 外部サービスでのシステム障害により利用者資産の出金が遅延

＜業態＞

暗号資産交換業者

＜事象＞

- 当社がサービスを利用している外部の暗号資産入金スクリーニングサービスでシステム障害が発生し、約 16 時間の間、利用者の暗号資産の出庫及び日本円での出金に遅延が生じた。

＜原因＞

- 当社では外部事業者が提供する入金スクリーニングサービスを利用し、スクリーニングが完了した暗号資産に対して出庫及び日本円での出金を許可していたところ、外部サービスにてデータベース障害が発生した影響を受け、利用者の暗号資産の出庫及び日本円での出金が遅延した。

＜対策＞

- サービス利用先で障害が発生した場合の手動によるワークフローの確立及び障害訓練の実施

６ 外部委託先の提供するサービス等の要因

＜業態＞

資金移動業者等

＜事象＞

- 接続先である外部委託先の冗長化されたシステムにおいて、稼働系サーバーで異常を検知し、待機系サーバーへの自動接続が行われたものの、接続に失敗し手動での切戻しを実施した。その際に、顧客アカウントの一部に排他ロックがかかり、当該顧客がサービスを利用できなくなった。

＜原因＞

- 稼働系サーバーのハード故障によるパケットロス（通信障害）が発生していた。パケットロスにより、死活監視の通信が途絶したため自動切替えに失敗した。
- 排他ロックされたアカウントは手動でロック解除する必要があり、復旧に時間を要した。

＜対策＞

- 外部委託先の対応として、迅速な待機系への切替え確保、復旧体制の改善、排他ロック解除の円滑化
- 資金移動業者等の対応として、外部委託先の実施状況のフォローアップ、各対応策の完了確認の実施

７ 外部委託先の提供するサービス等の影響を受け決済不可

＜業態＞

資金移動業者等

＜事象＞

- 外部委託先（SaaS 型の決済サービス）が利用しているデータセンターで実施されたネットワーク機器の増設作業の不備により、障害が発生し、当該サービスを利用する複

数の資金移動業者等でサービス全般が利用不可となった。
- 当該ネットワーク機器の増設作業は、データセンター側判断による実施であり、外部委託先への事前のメンテナンス告知等も行っていなかった。

＜原因＞
- データセンターが外部委託先のネットワーク環境を誤認したまま作業を実施した。

＜対策＞
- 外部委託先への原因追及及び再発防止策の報告依頼
- サービス障害時の対応マニュアルの整備

第４節　取引量増加に伴う容量不足等

１ 記憶領域の確保不足による IB やスマートフォンアプリ利用不可

＜業態＞
主要行等
＜事象＞
- 取引量等の増加により、一部のサーバーの処理能力が低下したため、IB やスマートフォンアプリでの決済等のサービスが利用できない状態となった。また、影響が生じた全てのサービスの復旧までに長時間を要した。

＜原因＞
- 設計時のドキュメント等への記載不備により、取引処理に必要な記憶領域内の再利用領域の監視やサーバーの定期的な再起動の必要性を認識していなかった。

＜対策＞
- 記憶領域内の再利用領域の使用量監視の実施
- サーバーの定期的な再起動実施による記憶領域内の再利用領域の確保
- 設計時のドキュメント等の記載見直し

２ システムの処理能力不足によるアプリのログイン・決済不可

＜業態＞
資金移動業者等
＜事象＞
- キャンペーン等による取引量の増大により、データベースサーバーの処理能力を超えたため、決済アプリのログイン、バーコード等を用いた決済及びチャージができなくなった。

＜原因＞
- トラフィック量の増加により、流量制限機能が動作する前にデータベースサーバーの性能限界を超過した。

＜対策＞
- データベースサーバーの性能限界に達する前に流量制御機能が働くようトラフィック量定義の見直し

３ ピーク日の処理による法人 IB へのログイン困難

＜業態＞

主要行等

＜事象＞

- 月末ピーク日に処理負荷が高い入出金明細照会を法人 IB で集中的に受け付けたことにより、サーバーの処理能力を超えたため、法人 IB にログインしにくくなる事象が発生した。また、復旧までに時間（約８時間）を要した。

＜原因＞

- メモリの負荷検証が不十分であった。
- 障害発生時の復旧手順の整備が不十分であった。

＜対策＞

- リソース（メモリ、CPU）増強及び処理性能検証の実施
- 障害発生時の復旧手順の整備

４ 新規暗号資産販売時の負荷検証不足による処理停止

＜業態＞

暗号資産交換業者

＜事象＞

- 新規暗号資産販売時において、顧客から大量の発注申込が発生。発注処理遅延からサーバーが一定時間内に応答しないタイムアウトが発生したため、処理が失敗した。
- さらに、この処理遅延解消のためにプログラム修正を行ったところ、プログラムミスによって処理誤りが生じ、復旧までに１週間以上を要した。

＜原因＞

- 想定取引量に基づく負荷検証が不十分であった。
- 障害対応として実施した、処理遅延解消のためのプログラム修正の検証が不十分であった。

＜対策＞

- 想定取引量の適切な見積り並びに想定取引量に基づく処理時間計測及びシステム負荷の観点での検証態勢の整備
- 障害対応時におけるプログラム修正に対する検証態勢の整備

第４章　プログラム更新、普段と異なる特殊作業等から発生したシステム障害

第１節　設定ミス・操作ミス等の管理面・人的要因

１ 災害対策環境への誤接続による ATM 取引不可新規

＜業態＞

信用金庫・信用組合等

＜事象＞

- 勘定系システムにおいて、一部の ATM が災害対策環境へ誤接続したことにより取引エラーが発生し、通帳及びキャッシュカード（以下、「媒体」という。）の取り込みや過払い等が生じた。
- さらに、ATM のオートホンに顧客からの問い合わせが殺到し、繋がらない状態となった結果、媒体を取り込まれた顧客が長時間その場で待たされる事態となり、多数の苦情が発生した。

＜原因＞

- 本番稼働中における災害対策環境 DNS[51]の起動試験において、引継ぎ不足や考慮漏れにより、ATM から災害対策環境への通信遮断が未実施であった。
- 例年の災害対策訓練と同様との誤認から、DNS 起動に伴う本番影響リスクを適切に評価できず、本来は経営承認が必要な案件が部内決裁のみで実施され、十分な検証が行われなかった。
- 障害対応態勢及び指示系統の不備、並びに規程間の不整合により、経営層へのエスカレーション、関係者への情報共有及び顧客対応が遅延した。

＜対策＞

- 災害対策環境における試験及び環境変更の承認ルールを明確化し、リスクを踏まえた設計・試験計画レビュー用チェックリストを作成
- 休日・夜間の障害対応態勢及び障害対応規程類の整備
- 危機管理、障害対応に係る研修・訓練の実施
- IT 人材の配置及び育成計画策定

２ 有識者のレビュー未実施による作業誤り

＜業態＞

地域銀行

＜事象＞

- システムの変更作業を定期メンテナンス時間帯に実施したが、誤った手順で作業を実施したことにより、DB サーバーの１号機と２号機で不整合が生じ、サーバーが起動せず、IB が利用不可となった。

＜原因＞

- システム環境の理解が不十分な担当者が誤った手順で作業を実施し、かつ事前の作業手順のレビューにおいて有識者ではない管理者がレビューしたため作業手順の不備を見逃した。
- システムの変更作業実施後に動作確認を実施していなかった。

＜対策＞

- 作業手順作成時のチェックリストの整備とレビューに有識者を配置
- 管理者に加えプロジェクト責任者によるレビューの実施と確認観点の明確化

[51] DNS（Domain Name System）：ドメイン名（例：xxx.co.jp）と IP アドレスを対応付ける仕組み（名前解決）を提供するシステム。

- システム変更作業後は動作確認の実施を必須とし、その手順を整備

3 本番環境と検証環境の分離ができていなかったことに起因する障害

＜業態＞

資金移動業者等

＜事象＞

- ポイントシステムのロードバランサーの交換を実施したところ、交換後のロードバランサーに検証環境で設定していた IP アドレスが誤って再利用された。その結果、検証環境へのトラフィックが本番環境に流れ込み、一部のリクエストが二重に処理されてしまった。

＜原因＞

- 本番環境と検証環境の分離ができていなかった。

＜対策＞

- 検証環境と本番環境のネットワークセグメントの分離
- ロードバランサー群へのアクセス制御を設定
- ポイントシステムの全てのネットワーク環境の設定の見直し
- 検証環境を含むロードバランサー等の廃止時手順、チェックリストの整備

4 本番作業時の作業誤りによる ATM 稼働不可

＜業態＞

地域銀行

＜事象＞

- 勘定系システムのメンテナンス時間に新システムのリリースに向けて事前に試験を実施していたが、試験終了後に作業者が本来不要な ATM の全台電源切断処理を誤って実施したことで全 ATM が営業時間になっても起動しなかった。

＜原因＞

- 作業量が少なく、難度も低い作業だったため、作業担当者１名で対応する体制としたことから、作業時のチェック体制が十分ではなかった。

＜対策＞

- 本番作業時の作業誤りで発生し得る顧客影響を踏まえた作業手順・作業結果の確認態勢の強化

5 データセンター保守作業時の操作ミスによる決済サービス停止

＜業態＞

資金移動業者等

＜事象＞

- データセンターでの夜間の電源作業において、サーバーの電源がつながったブレーカーを誤って遮断したことにより、決済システムが停止した。
- 稼働中のサーバーが電源強制切断となったため、サーバーの立ち上げや動作確認を行

う必要があったことから、復旧までに時間を要した。

＜原因＞

- データセンターでの電源作業において、作業手順書に誤りがあった。

＜対策＞

- 作業手順書作成段階におけるチェック体制の強化

６ 利用予定の外部サービスに関する技術調査内容の誤り

＜業態＞

暗号資産交換業者

＜事象＞

- 当社が新しくリリースした入庫スクリーニングシステムの不具合により、暗号資産の入庫が長時間反映されなかった。

＜原因＞

- 当社は、スクリーニングで利用を予定していた外部サービスについて、担当者が単独で実施した技術調査の結果を他メンバーが確認していなかった。そのため技術調査内容の誤りに気づくことができず、誤った調査内容をもとに要件定義と実装を行った。
- 当社は入庫処理の遅延を監視プログラムの対象としていなかったため、リリース後に入庫処理が遅延していることをシステムで検知することができず、発見までに時間を要した。

＜対策＞

- 技術調査の結果についての確認体制の見直し
- 要件定義段階における監視プログラムの対象についての検討

７ 送信元の設定誤りによる IB 等利用不可

＜業態＞

主要行等

＜事象＞

- クラウド環境へ移行する際、本来許可すべき送信元の IP アドレスのセグメント設定を誤り、接続エラーとなったことに起因し、一部の顧客が個人用 IB やホームページを利用できない事象が発生した。また、顧客からの問い合わせがあるまで当該障害を発見できなかった。

＜原因＞

- 担当者の作業確認漏れにより、許可すべき IP アドレスのセグメントが本番環境に反映されていなかった。
- 接続エラーが発生した際にアラートを検知する機能を実装していなかった。

＜対策＞

- レビュー体制の整備
- 接続エラーのアラート検知機能の構築

８ 設定誤りによるチャージ不可

＜業態＞

資金移動業者等

＜事象＞

- 銀行口座からのチャージを行った際、銀行口座残高の引落しは行われたが、資金移動業者等での残高反映がされていなかった。

＜原因＞

- 銀行口座からのチャージは外部システム連携をしており、トランザクション負荷を軽減するため処理の改修を実施したが、外部システム連携に係る仕様の理解不足があり設定が間違っていた。
- 資金移動業者等は、外部システム連携による作業手順書が未整備だったため、テスト環境で資金移動業者等からの応答要求の動作確認は行ったが、外部システムからの応答要求の動作確認を行っていなかった。

＜対策＞

- 外部システム連携に係る処理変更時の時の標準作業手順書の整備
- 当該手順書及び外部システム連携仕様の周知

９ テーブルの最新化作業誤りによる被仕向取引不可

＜業態＞

地域銀行

＜事象＞

- 外部委託先において、新店追加に伴う為替関連テーブルの更新作業を誤り、他行宛振込等の取引が不可となった。

＜原因＞

- テーブルを更新した開発担当者とテーブルのバージョン管理担当間で情報連携が行われていなかった。
- 為替関連テーブルの更新作業手順が不明確であった。

＜対策＞

- 為替関連テーブルの最新化に関する作業手順の整備
- 外部委託先管理の強化（本番リリース前の銀行での事前検証等）

１０ 計画停止中の作業誤りによる ATM 利用不可

＜業態＞

地域銀行

＜事象＞

- メンテナンスのためシステムの計画停止を実施したところ、一部の機器の停止手順を誤ったことにより、システムが正常に立ち上がらず ATM 取引等が不可となった。

＜原因＞

- 作業手順書の記載が不十分であり、再鑑者によるチェックも行われていなかったこと

により、システム停止の際に誤ったオペレーションを行ってしまった。
- エスカレーションに時間を要したことから有識者の駆付けが遅れ、システムの再起動手順を正しく作成できなかった。

＜対策＞
- システム基盤有識者による運用担当者への研修内容の最新化及び研修の定期的実施
- 障害時のエスカレーションの的確なタイミングでの実施

１１ ネットワーク機器の交換手順誤りによる IB 取引不可

＜業態＞

地域銀行

＜事象＞
- IB の共同センターにおいてネットワーク機器の予防交換の作業を誤り、個人 IB 及び法人 IB のオンライン取引が一時不可となった。

＜原因＞
- 手順書の変更管理ルールが徹底されていなかったことにより、メンテナンス作業の手順書が修正されなかった。

＜対策＞
- 変更管理ルールの徹底、作業手順書作成に関する適切な作業者やレビューアのアサインの徹底

１２ 開発メンバーの引継ぎ不十分に伴う仕様の理解不足によるログイン不可

＜業態＞

暗号資産交換業者

＜事象＞
- 顧客からの依頼により、当社担当者の操作による利用者情報の変更の際、変更の承認を得るための電子メールの送信先が誤っていたため、変更手続きが完了せず、顧客がログインできない事象が発生した。

＜原因＞
- 利用者情報変更のプログラムについて、顧客操作によるものと当社担当者操作によるもので同一のプログラムが利用されるという認識がなかったため、前者のみを対象に仕様変更した際、後者への影響を考慮できず、電子メールの送信先の仕様が変更されてしまった。
- 同一プログラムが利用される認識がなかったのは、開発メンバー変更の際の引継ぎ不十分に伴う業務仕様の理解不足である。

＜対策＞
- 業務を考慮した影響確認に向けたチェック観点及びテスト項目の整備
- 開発メンバーによる業務に係る仕様の再確認

第２節　ソフトウェアの不具合

１ 残高チャージ等のサービスが利用しにくい状況新規

＜業態＞

資金移動業者等

＜事象＞

- Web アプリケーションフレームワークを別のフレームワークに変更・リリースしたところ、Web サーバーからセッション管理サーバーへの接続数が急増・上限に達し、システムのスローダウンが発生した。
- その結果、利用者が Web サイトに接続しにくい事象が発生したほか、モバイルアプリにおいても Web サイトを介した残高チャージ等のサービスが利用しにくい状態となった。

＜原因＞

- フレームワークの移行前は、当該フレームワークにおいてセッション管理サーバーへの接続数を制御していたが、移行後のフレームワークには当該制御が存在せず、Web アプリのフロントシステムにおいて実装する必要があった。しかしながら、フレームワーク移行に係るギャップ分析が不十分であったことやセッション管理サーバーに接続数の上限が存在していることを開発者が認識していなかったことから、当該制御が実装されないままリリースされた。
- セッション管理サーバーのリソース不足に係る監視閾値を設定していなかった。

＜対策＞

- Web サーバーからセッション管理サーバーへの接続処理について、セッション確立を初回のみ行うよう修正。
- セッション管理サーバーの接続数上限について開発メンバーに周知。
- セッション管理サーバーのリソース不足を事前に検知できるよう監視閾値を設定。監視用のダッシュボードに追加。
- インフラ側の変更等リソース変化が考えられるリリースは週の前半に実施。またリリース作業の経過観察期間を十分に設ける。

２ API インターフェース仕様書の確認不足

＜業態＞

資金移動業者等

＜事象＞

- リリースした改善機能の仕様バグにより、エラー処理が増加、送金依頼人による再度の送金指示を実施する必要が生じた。その結果、受取人への着金が最大翌営業日まで遅延した。

＜原因＞

- 預り金保証会社が提供している送金指示をする API インターフェース仕様書の当社内での確認不足から影響の範囲を見誤ったこと。

＜対策＞

- 外部接続先に対して設定値を変更する際は、開発担当者による仕様書での確認だけでなく、預り金保証会社に対して直接当該変更による影響の確認を徹底
- 要件定義・設計時のチェックリストに上記事項を追加し、預り金保証会社側に確認したことを業務部門の開発担当チームで確認。また、リリース時にはシステム基盤担当部門で再確認し、チェック漏れがない運用を構築
- 送金時のエラー率を定期的にチェックし、異常値の場合アラート検知する仕組みを構築

３ 設定ミスにより複数回の同一注文が発注可能

＜業態＞

暗号資産交換業者

＜事象＞

- 当社が提供するスマートフォン向け取引アプリにおいて、注文操作から注文完了画面表示までの間に複数回タップをすると同一内容の注文が重複発注されてしまう障害が発生した。
- 重複発注を検知する仕組みがなかったため、取引アプリの実装からシステム改修が完了するまでの長期間にわたり発覚が遅れた。

＜原因＞

- 設計段階では利用者が注文操作を行った後、即座にステータスを「注文中」に変更する仕様としていたところ、実装段階では注文操作を行い注文完了の画面が表示されるまでのステータスを「未注文」として処理をしたため、利用者が同一注文を重複発注できる状態となっていた。

＜対策＞

- 特異な操作（連続タップや連続スワイプ）に対するテストシナリオの追加
- 重複発注を検知する仕組みの構築

４ プログラム誤りによる ATM 停止

＜業態＞

地域銀行

＜事象＞

- 勘定系システムと ATM を接続するシステムにおいて、過去に発生した障害対応を行うため、勘定系システムと ATM の接続状況を確認するプログラムをリリースしたが、そのプログラムの接続状況を確認する処理の不具合により、一部の ATM や通帳繰越機が利用不能となった。

＜原因＞

- ATM と接続するシステムの起動処理の挙動についてプログラムを開発した外部委託先が、ATM を開発した外部委託先への確認を怠り、誤った認識の下でプログラムを作成してしまった。

- 新たに導入するプログラムに関するレビューやテストが十分でなかった。

＜対策＞

- 外部委託先共通のプログラムの開発プロセス策定とレビュー体制の確保

第５章　システム障害後の対応が円滑に行われた事例[52]

１ 障害分析ＡＩの活用新規

＜業態＞

地域銀行

＜対応＞

- 障害の再発防止策として障害分析ＡＩを活用。過去の障害事例を学習させることで、テスト漏れ等に起因する同種の障害を未然に防止することを目的として、当行が独自に開発したツール。

２ システム障害時における円滑な初動対応の実施

＜業態＞

地域銀行

＜事象＞

- 勘定系システムと外部接続先を接続するシステムにおいて、プログラムのエラー処理不備により当該システムが停止した。これにより ATM、IB 等の他行宛て振込が不可となった。

＜対応＞

- 委託先において、障害発生箇所の特定作業が早期に完了したため、障害発生から約 40 分で復旧作業が完了し、発生から約１時間後に外部接続先との再接続及びサービスの復旧が行えた。
- 初動対応の訓練を半年に１度実施しているため、障害を検知後、顧客対応部門も含め、システム部門と委託先でオンライン会議を実施し円滑な情報共有と顧客対応方針の決定が行えた。
- 当行ホームページの掲出は銀行端末から可能なため、障害発生から約 30 分で掲出が行えた。

３ 事後改善策における ATM 停止時のシステム対応態勢の整備

＜業態＞

地域銀行

＜事象＞

- 勘定系システムでディスク障害が発生し、冗長構成の機能により、障害が発生したサーバーの切離しを行ったが、切離し処理中に発生した取引がエラーとなり、複数台の ATM が停止した。

[52] 改善が適切に行われた事例を含む。

- 複数台の ATM が停止したことで、停止中の ATM の把握や委託先との作業連携が遅れ、ATM の復旧に時間を要した。

＜対応＞

- 店舗内の ATM が全台取扱中止となった店舗を優先し復旧させるため、ATM 稼働状況を把握するドキュメントを整備し、当行と委託先間で共有している。
- 委託先との円滑な情報連携・連絡態勢の整備をするため、金融機関と委託先間でオンライン会議システムの導入や、導入したオンライン会議システムを用いた委託先との障害訓練の実施、委託先内で障害訓練を３か月に１度実施することとしている。

４ 新システム稼働後の大規模障害を想定した対応態勢の整備

＜業態＞

地域銀行

＜事象＞

- 年末年始を利用した新システムへの移行において、ATM を停止していたが、新システム稼働時に ATM 内部の機器のエラーを検知し、一部の ATM が利用不可となった。

＜対応＞

- 稼働直後の大規模障害を想定し、全営業店との連絡態勢を整備していたことで、店内 ATM を利用する顧客の誘導を円滑に行えた。
- 店外 ATM へ駆け付ける担当者をあらかじめ決めていたことで大きな遅滞等なく ATM へ駆けつけ顧客の誘導を行えた。
- 障害発生後のホームページ等への顧客周知の手順整備と訓練していたことで円滑な対応を実施した。

５ 事後改善策における障害発生時の顧客周知の迅速化

＜業態＞

地域銀行

＜事象＞

- 法人向け IB において、ソフトウェア障害に起因し、決済等が不可となった。また、障害発生後、ホームページでの顧客周知に時間を要した。

＜対応＞

- 障害発生時のホームページへのシステム障害に関する告知作成は、外部委託していたが、緊急時は自行内でホームページの作成ができるよう仕組みを構築し、手順書を整備した。
- システム障害の影響範囲を迅速に把握することやシステム障害対応の迅速な対応が行えることが可能となるように、コンティンジェンシープランのブラッシュアップ及び障害訓練を実施した。

６ アプリへのログイン不可時の円滑な顧客対応の実施

＜業態＞

主要行等

＜事象＞

- 銀行アプリが繋がりづらい状態となり、システムへのログインが不可等となる障害が発生した。

＜対応＞

- 障害における顧客対応について、コンティンジェンシープランに基づき障害情報のホームページへの掲載及び ATM や店頭の他チャネルへ誘導した。

7 システム障害対応に係る手続きの明確化

＜業態＞

主要行等

＜事象＞

- ハードウェア故障によってネットワーク機器が使用不能となったことにより、別経路に自動で切り替わったものの、自動で経路が切り替わるまで一時的に接続が切断されたことで IB 及び ATM での顧客取引や外為被仕向送金等がエラーとなった。

＜対応＞

- システム障害時における取引エラー内容確認、仕掛取引有無の確認、顧客対応の必要性有無の確認に係る手続きを事前に定めていたため、顧客影響を把握のうえ取引の時限内に対応を完了した。

8 ATM 停止時の円滑な顧客対応の実施

＜業態＞

信用金庫・信用組合等

＜事象＞

- 勘定系ネットワーク機器の不具合により、ATM 機器及び CTM[53]端末による全取引が約１時間、停止する事象が発生した。

＜対応＞

- ATM 取引中に取引が中断した顧客が 13 名いたが、職員による説明、取引の確認、他金融機関への誘導等を実施し、ATM 利用に関する苦情等は発生しなかった。

9 コンティンジェンシープランに則った円滑な顧客対応の実施

＜業態＞

地域銀行

＜事象＞

- 通信回線業者の通信障害により、店舗外 ATM とホスト間の通信が休止状態となった。

＜対応＞

[53] 郵便貯金、簡易保険の業務で使用される係員操作の端末機。「カウンター・ターミナル・マシン」の略。

- 障害における顧客対応等について、コンティンジェンシープランに基づき店舗外 ATM に担当者を出動させ、ATM 利用者に対して最寄りの店舗内 ATM や提携先の ATM へ誘導を実施した。また、ATM 利用に関する苦情等は発生しなかった。
- 今後、より迅速な顧客対応等を可能とすべく、休日における障害発生時の訓練について実施することとしている。

１０ コンティンジェンシープランに則った円滑なシステム復旧の実施

＜業態＞

地域銀行

＜事象＞

- クラウドサービスのデータセンター内で通信ネットワーク障害により、ATM 利用不可等となった。

＜対応＞

- 顧客が利用中で自動復旧できなかった店舗内 ATM は、コンティンジェンシープランに基づき行員による手動リセットにより、復旧対応を実施し、店舗外 ATM は、リモート対応あるいは行員の手動リセットにて復旧対応を実施した。
- また、通帳等の取込みが生じ、翌日以降に事後の顧客対応が必要となった事象は、店舗外 ATM 管理店行員が返却等の対応を実施した。
- さらに、店舗外 ATM の対策として、事前に指定した駆付け担当者以外が ATM 駆付けする事態を想定し、手動リセットを実施する手順の訓練及びマニュアルの設置を実施した。
- 休日の大規模障害発生を想定した対応について、ATM 駆付け訓練を実施した。

補論２　バーゼル銀行監督委員会による「健全なサードパーティリスク管理のための諸原則」

第１章　概要

2025 年 12 月、バーゼル銀行監督委員会（以下、「バーゼル委」という。）は、「健全なサードパーティリスク管理のための諸原則」[54]（以下、「諸原則」という。）を最終化・公表した。諸原則は、サードパーティリスク管理に関する取締役会等の責任を明確化した上で、台帳の整備・更新を含むリスク管理枠組みの実施、サードパーティとの取決め締結前のデューデリジェンス、契約締結、オンボーディング及び継続的なモニタリング、業務継続管理、サードパーティとの取決め終了という「出口」に至るまでの一連のライフサイクル全体を通じたリスク管理のあり方が示されている。金融機関におけるリスク管理態勢の整備・運用にあたっては、サードパーティのリスクや重要性等に応じたリスクベース・アプローチのもとでの対応が期待されている。

諸原則は、銀行向けの９原則及び監督当局向けの３原則から構成されている。これらのほか、数十の細目が示されている[55]。

（図表１）諸原則の概要

対象	原則	項目	概要
銀行	1	取締役会等の責任	取締役会は、銀行のサードパーティリスクの監督に対して最終的な責任を負い、明確な戦略を承認し、銀行のリスクアペタイトとサービス中断（disruption）に対する許容度を定義すべき。
	2	リスク管理枠組みの実施	取締役会は、上級管理職が、銀行のサードパーティ戦略に沿ったサードパーティリスク管理枠組みに基づく方針及びプロセスを実施することを確実にすべき。これらの方針及びプロセスには、サードパーティサービス提供者（TPSP）の実績・TPSP との取決め[56]に関連するリスク・低減措置について、取締役会へ報告することが含まれる。
	3	リスク評価	銀行は、TPSP との取決めを締結する前及びライフサイクル全体を通じて、特定されたリスク及び潜在的なリスクを評価し管理するために、サードパーティリスク管理の枠組みの下で包括的なリスク評価を行うべき。
	4	デューデリジェンス	銀行は、TPSP との取決めを締結する前に適切なデューデリジェンスを行うべき。
	5	契約締結	TPSP との取決めは、全ての当事者の権利・義務、責任及び期待を明確に記述した法的拘束力のある書面による契約によって管理されるべき。
	6	オンボーディング	銀行は、デューデリジェンスや契約条項の解釈の過程で特定されたあらゆる問題解決への対応を含め、新たな TPSP のオンボーディングを円滑に進めるための十分な資源を投入すべき。
	7	継続的なモニタリング	銀行は、TPSP との取決めのパフォーマンス、リスク及び重要性の変化を継続的に評価・モニタリングし、その結果を取締役会や上級管理職に報告し、必要に応じて問題に対応すべき。
	8	業務継続管理	銀行は、サードパーティのサービスが中断した場合に業務を継続する能力を確保するために、堅固な業務継続管理を維持すべき。
	9	契約終了	銀行は、サードパーティとの取決めの計画的な終了のための出口計画及び計画外の（予期せぬ）終了のための出口戦略を維持すべき。

[54] 本件に関する金融庁公表資料：https://www.fsa.go.jp/inter/bis/20251217/20251217.html
[55] 細目のポイントについては、本件に関する金融庁・日本銀行作成説明資料（https://www.fsa.go.jp/inter/bis/20251217/01.pdf）も必要に応じて参照いただきたい。
[56] 諸原則において、TPSP との取決めは、銀行と TPSP の間で、１以上のサービス、業務、機能、プロセス、又は作業を銀行に提供するための正式な取決めを指すとされており、外部委託に限られない概念である。また、グループ内サービス提供者による銀行へのサービス提供に係る取決めも含まれるとされている。

監督当局	10	監督当局の役割	監督当局は、銀行に対する継続的な評価の不可欠な要素として、サードパーティリスク管理を評価すべき。
	11		監督当局は、銀行セクターにサービスを提供する一つ又は複数の TPSP の集中によってもたらされるものを含め、潜在的なシステミック・リスクを特定するため、入手可能な情報を分析すべき。
	12		監督当局は、銀行にサービスを提供する重要な TPSP によってもたらされるシステミック・リスクを監視するため、分野横断的かつ国境を越えた連携及び対話を促進すべき。

ここ数年、ソフトウェアの変更管理に起因する問題で我が国を含めて金融業界が大きな影響を受けた事例があるほか、国内でもサードパーティへのサイバー攻撃を通じた深刻な個人情報漏洩事案等が発生しており、サードパーティリスクは金融機関にとって経営上の重大なリスクとなっているため、サードパーティリスク管理態勢の強化は喫緊の課題となっている。我が国の銀行等においては、従前から、法令・監督指針等に基づき、委託先管理やサードパーティリスク管理について適切な対応が求められており、一部の内容は、諸原則をはじめとする、国際的な基準設定主体により策定されたサードパーティリスク管理、オペレーショナル・レジリエンス等に係る文書とも整合したものとなっている。一方で、一般に、サードパーティは、外部委託先に加え、例えば購買・調達先やデータ・サービス連携先[57]を含む点で外部委託よりも幅広い概念と言える。また、サードパーティリスク管理は、サイバーセキュリティや、オペレーショナル・レジリエンスと密接に関連した論点であるが、例えば事業者に預託する機密情報の管理の適切性の観点等では、より幅広い論点を包含し得る。このため、今回新たに策定された諸原則が、多くの金融機関において、さらなるリスク管理の高度化に活用されることが期待される。

（図表２）我が国の法令・監督指針等において求められる対応（例）

法令・監督指針等	内容
銀行法・同施行規則	委託に関し、銀行に対して、委託業務の的確な遂行を確保するための措置を求めている（法第 12 条の２、施行規則第 13 条の６の８）ほか、委託先に対する当局の権限として資料徴求権（法第 24 条）、立入検査権（法第 25 条）を規定。 外部委託に関し、顧客保護の観点からの態勢整備、及び健全性の確保の観点からの総合的な検証・必要な態勢整備（III－３－３－４）。また、システムリスクに関連して、外部委託に係る適切なリスク管理等（III－３－７－１）について規定。
主要行等向けの総合的な監督指針	サードパーティに関しては、オペレーショナル・リスク管理において重要なサードパーティ等への依存度の管理（III－２－３－７）、オペレーショナル・レジリエンスに関する態勢整備に関して、サードパーティ等の社外の経営資源も含めた重要な業務の耐性度での遂行に必要な経営資源の相互連関性や相互依存度の特定・マッピング（III－３－６）について規定。
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	サイバーセキュリティの観点から、金融機関におけるサードパーティリスク管理に関するガバナンスやライフサイクル全体を通じたリスクベースの対応について規定。

[57] 必ずしもこれらの類型に限られるものではない点には留意が必要。

第２章　金融機関との対話を通じて把握した現状

金融庁では、従前から、オペレーショナル・レジリエンスに関するモニタリング等を通じて金融機関のサードパーティリスク管理に係る実態把握に努めてきたほか、主要金融機関との定期的な面談を通じ、サードパーティリスク管理に関する共助の取組みを促してきた。また、最近では、諸原則の内容も踏まえた対応の検討の一助とする観点から、一部の国際統一基準金融機関を対象に本分野に関し、各社における課題認識に関する意見交換や実務の把握のための対話を実施した。

我が国金融機関では、既存の法令・監督指針や諸原則等の国際的な文書の内容も踏まえながら、従来の外部委託先管理の枠組みを、サードパーティリスク管理の枠組みに置換する取組みを進めていることがうかがわれる。こうした取組みにおいては、管理対象を、外部委託先だけではなく、購買・調達先やデータ・サービス連携先等へと拡大するとともに、これらの類型や金融機関グループを横断する形で、ライフサイクルを通じたリスクベースの対応を進めることが志向されている。こうした中、一部の金融機関では、国内・海外拠点及び子会社を幅広く適用対象とするサードパーティリスク管理の方針を経営レベルで定め、システム化を通じてサードパーティの情報とリスク評価の結果を合わせて統合的に可視化するなど、一定の進捗を生んでいる先もみられた。

他方、諸原則の内容にも照らすと、以下の点については、引き続き既存の枠組み、実務を高度化する余地が見受けられる。

- 重大なリスク発現事象が発生していることを踏まえると、取締役会や経営会議によるサードパーティリスク管理の基本的事項の策定・運用への関与を強化する余地がみられる。同様に、傘下のリスク管理委員会等における審議内容を充実させる余地や、実務担当部署による取組状況のモニタリングの強化を図る余地がみられる。また、経営層が関与するもとで明確なロードマップ（目的、目標水準、スケジュールを含む）を策定し、サードパーティのリスクに応じて優先度の高い先・課題から管理またはその高度化に着手する余地がみられる。

- 銀行以外の子会社や海外拠点を含めたグループ横断的な観点や、外部委託先、購買・調達先やデータ・サービス連携先や非 ICT 分野で取引関係にある先といった、サードパーティの類型横断的な観点からみると、統一的なリスク管理戦略・方針の策定、台帳の整備や相互依存性・相互連関性（グループ各社及びサードパーティ間の依存関係と影響の波及関係）のマッピングには高度化の余地がみられる。

- リスクの重大性が増していることと比してサードパーティリスク管理にあたる人材・リソースが不足している。特に、グループ・サードパーティの類型を横断した管理を強化するにあたっては、３線管理における第２線のリスク統括部署等の負荷が増大する。また、本来は業務所管部署（第１線）における自律的なリスク管理が重要であると認識されつつも、現状ではその機能の十分な発揮には高度化の余地がみられる。

- 特に、台帳の整備やリスク評価の実務においては、システム化によりサードパーティとの関係をグループ・類型横断的に可視化すること、サードパーティの情報に基づく

リスク評価等を自動化･標準化することで実務を効率化することが必要と考えられる。こうした取組みは業務所管部署における作業品質の向上やリスク所管部署・統括部署における管理実務の工数削減にも繋がり得るが、多くの先で取組みは緒に就いたばかりである。こうした中、台帳の情報やマッピングの結果に基づいて行うべき集中リスクの分析に関しても、持株会社のリスク統括部署における把握には高度化の余地がみられる。

- デューデリジェンス、リスク評価、継続的なモニタリングの評価方法について、契約締結･継続、取引や業務上の関係継続の可否に係る判断や、サードパーティのリスク・重要性に応じた追加的対応の要否に係る判断を統一的に行うための基準が明確でない事例や、画一的なチェックリストに基づくモニタリングにとどまり、リスクベースでの実態把握に十分に対応できていない事例が見受けられる。

- 契約、業務継続計画（BCP）及び出口戦略に関しては、特に標準化されたサービスを提供する大手事業者や寡占度の高いサービスを提供する事業者、グローバルな事業者等との関係において、金融機関が監査権や情報取得、個別の対応内容等について契約条項の見直しや調整を行うことが困難な場合があるほか、現実的な代替先の確保や実効的な出口戦略の策定に制約が生じている事例がみられる。

第３章　今後の対応に関する考え方

サードパーティリスクが顕在化している状況にあり、また、既存の法令・監督指針や諸原則等の国際的な文書の内容、これまでのモニタリング・対話を通じて把握した課題を踏まえると、各金融機関において取り組むことが想定される基本的な対応事項について、まずは、経営層が関与するもとで明確な全社的ロードマップ（目的、目標水準、スケジュールを含む）を策定し、サードパーティのリスクに応じて優先度の高い課題から着実に管理の高度化を進めていくことが肝要と考えられる。具体例としては、以下の点が挙げられる。

- 取締役会等が積極的に関与し､グループやサードパーティの類型を横断するかたちで、サードパーティリスク管理に係る基本方針を定めるとともに、その運用状況を適切にモニタリングすること。

- 実務レベルにおいては、全社的な基本方針のもと、サードパーティのライフサイクルを通じた評価、契約締結・継続、取引や業務上の関係継続の可否、ならびに統制強化の要否の判断に資する観点から、具体性と判読性を備えた基準を策定し、必要な態勢を整備すること。その際、リスク管理実務が画一的・形式的な手続きにとどまることなく、サードパーティのリスクや重要性に応じ、オペレーショナル・レジリエンスの観点も踏まえて実効的なリスクベース・アプローチの運用が確保されるようにすること。また、こうした取組みにあたっては、近時の特徴的なインシデントやリスク管理上有効な考え方や手法について、外部の動向・知見を積極的に把握し、必要に応じて継続的な態勢・運用の高度化に活用すること。

- 経営陣は、リスク管理実務を特定の部署に依存させるのではなく、まず、調達・契約・

サービス利用の当事者となる部署（主として第１線）による自律的な管理を構築・強化するとともに、リスク統括機能（第２線）や内部監査（第３線）を含めた役割分担を明確にした上で統制機能を強化し、サードパーティリスクに関する認識を組織全体に浸透させ、強化していくこと。必要に応じて外部の目線による検証を行い、その結果をリスク管理の改善に活用すること。

- 外部委託先に限らず、購買・調達先やデータ・サービス連携先等を含めたサードパーティを対象として、台帳の整備・更新を進めるとともに、相互連関性・相互依存性の把握・マッピングを通じて、リスクの可視化を図っていくこと。また、こうした取組みを通じて、特定のサービスや事業者への集中や、オペレーショナル・レジリエンスを確保する上での課題について、サードパーティのリスクや重要性に応じた対応につなげていくこと。

こうした取組みが進むよう、金融庁では、サードパーティリスク管理に関する監督の考え方の整理や明確化に向け、必要に応じて検討を進める方針である。

また、個別金融機関では対応に難しさを伴う論点も多いことから、金融機関横断での協調的な対応が重要な役割を果たし得るところであり、金融 ISAC 等における取組みが見られる。このような共助の取組みは、リスクに関する知見の共有や実務の標準化を通じて、各金融機関のリスク管理の底上げにつながることが期待される。金融機関においても、こうした取組みに主体的に関与し、知見の提供や議論への参加を通じて、業界全体としての対応力の向上に貢献していくことが望まれる。

金融庁としても、業界における共助の取組みを後押ししていく。また、モニタリングや対話を通じて把握した先進的な取組み事例や共通課題について、今後も様々な機会を通じて業界と共有するほか、クラウドサービス事業者との対話を含め、サードパーティとなり得る事業者との相互理解を深め、実務の実態を踏まえた建設的な関与を進めていく。当局間の連携についても、国内外の関係当局との協議・意見交換や、バーゼル委をはじめとする国際的な議論への参加を通じて、積極的に取り組んでいく考えである。

コラム　耐量子計算機暗号（PQC）

1.　量子計算機を巡る環境変化と耐量子計算機暗号（PQC）の必要性

量子コンピュータの実用化と普及は社会を革新する可能性を秘める一方で、現在の公開鍵認証基盤で広く用いられる暗号技術が短時間で解読されてしまう危険をもたらす。暗号技術は、社会生活を支える重要インフラである金融機関の情報システムを情報漏えいや改ざん等から防ぐ手段として重要な役割を果たしている。これらが破られることになれば、インターネットバンキングをはじめとする金融サービスに用いられる情報システムの安全性が根底から覆される。特定の暗号技術に的を絞れば、量子コンピュータの実用化前でも短時間で現在の暗号が解読可能になるとも言われている。足元では、すでにHarvest Now Decrypt Later（HNDL）と呼ばれるサイバー攻撃が潜行しているともいわれる。これは現在の暗号技術で保護されたデータを収集し、量子コンピュータの実用化の後にそのデータを解読して本格的な攻撃を仕掛けるものである。量子コンピュータに耐え得るPQCへの移行は、５～10年サイクルの大規模システム更改等に合わせて実施することが現実的である。多数のステークホルダーが関与するシステムであれば、調整にも時間を要する。これらの背景を踏まえると、金融機関においては直ちに耐量子計算機暗号（以下、「PQC」という）への移行に着手する必要があると考えられる。金融庁ではモニタリングや実証実験等を通じて、金融機関に早期かつ着実な移行を引き続き促していく方針である。

2.　政府全体及び諸外国におけるPQCを巡る動向

我が国政府においては、2025年6月30日、「政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議[58]」が設置され、2025年11月、「政府機関等における耐量子計算機暗号（PQC）への移行について（中間とりまとめ）[59]」が公表された。同中間とりまとめでは、公開鍵暗号を現実的な時間で解くための量子計算機の実現時期を正確に予測することは困難である一方、暗号解読が近い将来に実現する可能性は否定できない点に留意が必要であることが記載されている。

また、我が国のサイバーセキュリティの確保等のため、政府機関等におけるPQCへの移行について、原則として、2035年までに行うことを目指し、2026年度に工程表（ロードマップ）を策定する旨が示されている。これは政府機関等のPQCへの移行を念頭にしたものであるが、PQCへの移行については、政府機関等に限るものではなく、重要インフラ事業者等や民間事業者等においても考慮しなければならない課題であるため、関係府省庁の連携の下、必要な対応について検討を進め、円滑な移行を後押ししていく旨も記

[58] 政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議の開催について
https://www.cas.go.jp/jp/seisaku/pqc/pdf/konkyo.pdf
[59] 政府機関等における耐量子計算機暗号（PQC）への移行について（中間とりまとめ）
https://www.cas.go.jp/jp/seisaku/pqc/pdf/report_202511.pdf

載されている。これらの方向性については、2025 年 12 月に閣議決定された「サイバーセキュリティ戦略[60]」にも盛り込まれている。

3. 金融庁における PQC への取組み

金融分野においては、多くの重要業務やシステムが暗号技術に依存しており、PQC への移行は IT レジリエンスやオペレーショナル・レジリエンスの観点からも重要な課題である。こうした認識の下、金融庁では 2024 年 7 月から 10 月にかけ、「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会」を開催し、預金取扱金融機関が PQC への移行を検討する際の推奨事項、課題及び留意事項について検討し、その結果を「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会報告書」として公表している（同年 11 月）。しかしながら、PQC への対応は、従来の暗号技術とは異なる新しい技術領域であり、その具体的な進め方や優先順位の設定に課題があるとされている。このため、現時点では対応に十分に着手できていない金融機関も少なくないと考えられる。

こうした背景を踏まえ、金融庁では、金融機関における PQC への円滑な移行を促進するため、複数の金融機関を対象として、PQC 移行の前提作業となるクリプト・インベントリ（各システムの暗号利用箇所や利用アルゴリズム等の情報を一覧化した資料）の構築を行うとともに、当該プロセスを通じた金融機関への技術移転としての伴走支援に関する実証実験を進めている。また、本事業を通じて得られた知見である作業手順、ベストプラクティス、課題への対応方法等を整理・公表することにより、業界全体における PQC 移行の促進を図る。

以　上

[60] サイバーセキュリティ戦略
https://www.cyber.go.jp/pdf/policy/kihon-s/cs_strategy2025.pdf