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

2025年６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（サイバーインシデントを含む）に関して分析した「金融機関のシステム障害に関する分析レポート」を公表してきたが、昨今の地政学リスク、サイバーリスク等の高まりを背景に、政府としてサイバーセキュリティに関する取組みを一層強化する中[1]、金融業界に対して一層のサイバーセキュリティ、オペレーショナル・レジリエンスの強化が求められていることを踏まえ、2024 年度においては、「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」として再構成した。本レポートでは、第一に、例年に続き、2024 年度の金融分野におけるシステム障害の分析について述べた後、第二に、サイバーセキュリティに関し、2024 年 10 月に当庁が策定した「金融分野におけるサイバーセキュリティに関するガイドライン」の要諦及び脅威ベースのペネトレーションテスト（TLPT）に関する取組みと TLPT から得られた示唆について記載している。第三に、金融分野におけるクラウドサービス利用の拡大を踏まえ、その固有のリスクと IT レジリエンス向上に向けた示唆について述べている。最後に、オペレーショナル・レジリエンスについて金融庁が実施しているモニタリングから得られた課題と参考事例についてまとめている。なお、補論として、システム障害の事例集を付けるとともに、耐量子計算機暗号への移行について述べている。

第２編のシステム障害に関する分析については、2024 年度の主なインシデントとして、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による顧客暗号資産の不正流出事案、金融機関の委託先である電子帳票等の発送業者から顧客情報が漏えいした事案、金融機関に対する DDoS 攻撃事案、金融機関が利用しているセキュリティソフトのアップデート不具合によるインシデント事案、証券会社等の顧客口座への不正アクセスによる不正売買事案などを挙げており、こうした事案からは、インシデントが発生していない金融機関においても、サイバーセキュリティを含めた IT リスク（以下、「システムリスク」という。）管理態勢を強化し、障害の未然防止に止まらず、障害発生時の重要業務の継続、顧客影響の軽減及び業務の早期復旧（以下、「IT レジリエンス」という。）の強化をより一層図るべきことが見て取れる[2]。

サイバーセキュリティに関する第３編では、2024 年 10 月に公表した「金融分野におけるサイバーセキュリティに関するガイドライン」（以下、「サイバーガイドライン」という。）と、金融機関のサイバーリスクの可視化のために有用な手段として当庁が実施を促している脅威ベースのペネトレーションテスト（以下、「TLPT」という。）について取り上げている。サイバーガイドラインに関しては、IT レジリエンスの観点から金融機関に求められる対応を、経営

---

[1] 政府では「国家安全保障戦略」（2022 年 12 月 16 日閣議決定）に基づき、サイバー対処能力の向上に向けた取組みを進めており、2025 年５月 23 日に「サイバー対処能力強化法」及び「同整備法」が公布されている。

[2] 例えば、バーゼル銀行監督委員会「オペレーショナル・レジリエンスのための諸原則」（2020 年６月、同委ウェブサイト https://www.bis.org/press/p200806.htm 及び金融庁ウェブサイト https://www.fsa.go.jp/inter/bis/20210402/20210402.html）、金融庁「『オペレーショナル・レジリエンス確保に向けた基本的な考え方』（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」（2023 年４月 27 日、金融庁ウェブサイト https://www.fsa.go.jp/news/r4/ginkou/20230427.html）、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）及び『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』（案）に対するパブリックコメントの結果等について」（2024 年 10 月４日、金融庁ウェブサイト https://www.fsa.go.jp/news/r6/sonota/20241004/20241004.html）。

陣のリーダーシップ、基本的な対策の徹底や侵入を前提とした対応の強化、サードパーティリスク管理、共助の重要性のそれぞれについて記載している。TLPT については、金融機関のサイバーセキュリティに関する意思決定や対策が現実の攻撃に対してどの程度有効かを第三者の視点から検証し、リスクを可視化する上で有効な手段であり、特に、大手金融機関、金融市場インフラ、特定社会基盤事業者、地域社会・経済に重要な役割を果たす金融機関等において、実施することが望ましいものである。当庁では、2023 年度及び 2024 年度において、金融機関が実施した TLPT の分析や、2024 年度において地域金融機関に対する TLPT の実証事業を行った。その結果、TLPT の有効性が確認されたのみならず、リスクを可視化するという目的から見て不可欠な TLPT 実施の前提条件に関して重要な示唆が得られた。

第４編では、当庁がこれまで実施してきたクラウドサービス事業者やその利用者等との対話の結果得られた、金融分野におけるパブリッククラウドサービス利用に関してどのような固有のリスクがあり、リスク管理上又はより IT レジリエンスを向上させ、安全にクラウドを活用する上での留意点は何かといった金融機関のパブリッククラウドサービスの利用に関する示唆について述べている。

第５編では、2023 年４月公表のオペレーショナル・レジリエンスに関するディスカッション・ペーパー及び同６月に改正した主要行等向けの総合的な監督指針のオペレーショナル・レジリエンスに関する規定に基づいて当庁が実施したモニタリングを通じて把握した取組事例及び課題事例についてまとめている。

これらの分析は、共通して、金融業界の IT の複雑化と依存度が増大しており、それに伴ってリスクが顕著に増大し、金融機関の経営ひいては金融システムを揺るがしかねないリスクを内包していること、対策を講じてもインシデントが発生することを前提として IT レジリエンスを強化する必要があること、金融機関の経営層が IT リスク・サイバーリスクをトップリスクとして認識し、内外の事例に照らし、自組織のガバナンス、体制、投資、人材育成について不断に見直し、強化する必要があることを再認識させるものである。当庁としては、金融分野における IT レジリエンス強化を促すため、金融機関の自助、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、対話、情報共有、ガイダンスの提供、サイバーセキュリティ演習等の機会の提供などの公助の取組みを強化していく。

コラム：金融庁におけるサイバーセキュリティの向上のための取組み

金融庁では、本レポート各編に記載の取組み以外にも、以下の関連する取組みを行っている。

（１）サイバーセキュリティセルフアセスメント（CSSA）

サイバーセキュリティ管理態勢の成熟度を評価する点検票（日本銀行及び金融情報システムセンターと共同で開発）に基づく自己評価の実施を地域金融機関等に求め、日本銀行と共同で自己評価の結果を分析し、他の金融機関対比での自組織の位置付けや改善すべき領域に関する情報を還元し、各組織及び業界全体のサイバーセキュリティの強化を促す取組みを

2022 年から実施している[3]。

（２）金融業界横断的なサイバーセキュリティ演習（Delta Wall）

金融業界全体のインシデント対応能力の向上を図るため、最新のサイバー攻撃の脅威動向を反映したシナリオの下、金融業界横断的なサイバーセキュリティ演習（Delta Wall）を 2016 年から毎年実施している[4]。演習結果については、分析の上、業界に還元している。

（３）耐量子計算機暗号（PQC）への移行対応

耐量子計算機暗号（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、関係者と更に検討するための検討会を開催し、同検討会の報告書を 2024 年 11 月に公表した（詳細は補論２参照）。

[3] 初回の 2022 事務年度は、地域金融機関及び新形態銀行に対して実施した。2023 事務年度には保険会社、証券会社及び信託銀行、2024 事務年度には３メガバンク以外の主要行、労働金庫等にも対象を拡大して実施した。

[4] 直近、2024 年 10 月に実施した演習（Delta Wall IX）については、金融庁ウェブサイト参照。
https://www.fsa.go.jp/news/r6/sonota/20241008/deltawall.html

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、事後改善策の報告を受けている。本編では、2024 年４月から 2025 年３月までに受領したシステム障害を分析している。

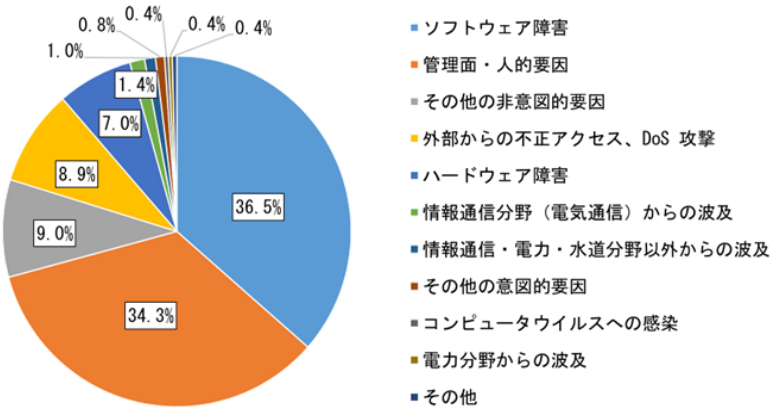
第１章　集計期間及び金融業界全体の障害傾向

2024 年度の業態全体[5]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[6]（図表１）。

「ソフトウェア障害」による障害について、設計時における影響調査の結果やテスト工程における検証観点の十分性を有識者がレビューを実施する体制としなかったことで、プログラムの修正漏れやテスト工程で検証すべき観点の漏れが発生し、ATM が利用不可となる事案が報告されている（本編第２節）。また、サードパーティが提供するセキュリティソフトの製品不具合により、業務用の端末が利用不可となったことで、保険料の支払いが遅延した事案が報告されている（本編第３節第１項）。

「管理面・人的要因」について、設計書の判読性の低さにより、本番環境に影響を与える作業ではないと誤認し、本番稼働中のシステムに対し保守作業を実施した結果、複数の金融機関が利用するインターネットバンキング（以下、「IB」という。）サービスのシステムが停止し、長時間にわたりサービスの利用が不可となる事案が報告されている（本編第４節第１項）。また、IB システムの共同センターにおいて、システム変更時に金融機関間のシステム構成の差異に応じて、適切なレビューアを配置しなかったことで、手順書のレビュー時に誤りを指摘できないまま、システム変更作業を実施した結果、IB システムが起動せず、サービスの利用不可となる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）」



[5] 本集計期間（2024 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 1,800 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、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）。

[6] 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、2025 年３月時点で金融機関にて調査中となっている約 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

2024 年度の主なインシデントとして、標的型ソーシャルエンジニアリング[7]を用いたサイバー攻撃による顧客暗号資産の不正流出事案、金融機関の委託先である電子帳票等の発送業者から顧客情報が漏えいした事案、金融機関に対する DDoS 攻撃事案、金融機関が利用しているセキュリティソフトのアップデート不具合によるインシデント事案、証券会社等の顧客口座への不正アクセスによる不正売買事案などが発生している。

金融機関の経営層は、こうした最新の傾向を踏まえ、自組織の IT レジリエンスを再評価し、トップリスクとしての IT リスク・サイバーリスクの管理態勢の強化を主導すべきだが、その際、対策を講じていたとしてもそれでもなおインシデントが発生し得るという前提に立って対策を講じる必要がある。特に、防御策だけではなく、インシデント発生時の顧客目線での対応、影響の最小化、重要業務の早期復旧等を実現させるための態勢整備といった観点が重要である。

また、昨今、外部委託先を含むサードパーティに起因するサイバーインシデントやシステム障害が多数発生していることから、サイバーセキュリティや個人情報管理といった観点を含めて外部委託先・サードパーティのリスク管理の実効性を向上させる必要がある。加えて、顧客口座への不正アクセスの事案は、証券業界に限らず、金融業界の信頼を揺るがしかねない問題であり、認証やモニタリングの強化などを含め、迅速な対応が必要である。

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　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の事案

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）が不正に流出する事案が発生している。

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への対策として、警察庁、内閣サイバーセキュリティセンター及び金融庁が共同で公表している注意喚起[8]に記載されている攻撃グループの手口例及び緩和策等を参考とし、①多要素認証を導入する、②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、③居住地以外の地域や VPN サービスか

[7] ソーシャルエンジニアリングとは、人間の心理的な隙やミスにつけ込み、情報を不正に取得する手口。
[8] 警察庁、NISC、金融庁「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、https://www.npa.go.jp/bureau/cyber/pdf/20241224_caution.pdf）

らと見られる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、④EDR 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。）、⑤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へのアクセスを禁止するなど、標的となり得る組織や事業者は、境界防御のみに頼らずに、多層的なセキュリティ対策を講じていく必要がある。

第２項　マルウェア感染に係る事案

2024 年度においては、外部委託先にて運用されているサーバーが第三者から不正アクセスを受け、個人情報を含む電子ファイルがランサムウェアにより暗号化され、さらに窃取された同電子ファイルの情報がダークウェブ上に公開されたことにより、個人情報の漏えいが生じた事案や、海外支店のプライベートクラウド環境が第三者から不正アクセスを受け、海外支店のサーバーを経由して国内外拠点への水平展開[9]を試みようとしていた事案が発生している。

2023 年度及び 2024 年度において外部委託先におけるマルウェア感染に係る事案が発生していることから、金融機関として、外部委託先へ提供する情報の重要度や情報が漏えいした場合の影響を考慮した委託先業務の重要度の見直しや、クラウドサービス利用時における IaaS[10]等の運用形態による重要度の見直し、重要な外部委託先については、実地調査や第三者評価等によるチェック体制の強化等により、重要な外部委託先の管理の実効性を確保することが課題となっている。海外拠点のサイバーセキュリティ管理態勢の整備においては、各海外拠点のサイバーセキュリティ対策状況を十分に把握し、適切な対策を講じること、サイバーインシデントが発生した際に、速やかな分析と経営陣等への報告が可能となるよう、各海外拠点と CSIRT との役割分担及び報告体制、対応期限等を明確にしておく必要がある。

第３項　DDoS 攻撃に係る事案

金融機関（外部委託先を含む。）を標的とした DDoS 攻撃等のサービス不能攻撃が相次いで発生し、IB にログインしにくいなど一時的にサービスへ繋がりにくくなる事案や、DDoS 攻撃（通信量増加）によりアプリ上で行う決済サービスが利用しづらくなる事案が発生している。

年末年始に行われた DDoS 攻撃においては、IoT ボットネットを利用し、UDP フラッド攻撃や HTTP フラッド攻撃など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、対策してもなお影響が生じる可能性がある

---

[9] 水平展開とは、攻撃者が侵入したネットワーク内で、最初に侵入したシステムから他のシステムへと横方向に移動し、ネットワーク全体への侵入を拡大していく攻撃手法。

[10] クラウドの運用形態には、SaaS（情報通信システムの有する機能をネットワークを通じて提供するサービス）、IaaS（サーバー、ハードディスク、ストレージ等の ASP・SaaS・PaaS に必要なハードウェア資源等を提供するサービス）、PaaS（システム資源、開発・実行資源、ネットワーク資源を提供するサービス）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[11]として、金融 ISAC[12]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、DDoS 対策ツール[13]の導入や攻撃元に対するブロック対応の高度化[14]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４項　不正アクセスに係る事案

金融機関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）や情報を窃取するマルウェア[15]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）の被害に関する事案が急増している。

こうしたことから、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[16]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[17]や BIMI[18]の導入などのなりすまし対策の強化、証券口座と預金口座など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

---

[11] 例えば、内閣サイバーセキュリティセンター「DDoS 攻撃への対策について（注意喚起）」、（2025 年２月４日 https://www.nisc.go.jp/pdf/news/press/20250204_ddos.pdf）

[12] 一般社団法人金融 ISAC（https://www.f-isac.jp/）

[13] 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（サーバーやネット枠の外部との通信を監視し、攻撃の侵入や試行など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。

[14] 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。

[15] 例えば、インフォーメーションスティーラー（Information Stealer）と呼ばれる感染したデバイスから情報を窃取するタイプのマルウェアであり、フィッシングメールの添付ファイルや改ざんされたウェブサイトの閲覧、信頼できないフリーソフトのインストール、OS やソフトウェアの脆弱性を悪用したドライブバイダウンロードなどを通じて感染する可能性がある。

[16] パスキー：FIDO Alliance と World Wide Web Consortium により規格化されているパスワードが不要な認証技術。フィッシングサイト等の正規サイト以外のウェブサイトにおいては、認証が機能しないといった観点から認証技術の漏えいリスクを低減できる効果があるとされている。

[17] DMARC(Domain-based Message Authentication, Reporting, and Conformance)：SPF（※１）・DKIM（※２）の認証結果を利用し総合的に送信ドメイン認証を行う技術。受信したメールが正規の送信元から送られてきたかを検証できる技術の一つ。ドメイン管理者は、認証に失敗したメールの取り扱いを送信側でポリシー（DMARC ポリシー）として宣言できるようになる。これにより、なりすまされているメールは受け取らない、といった強いポリシーを受信側に伝えることができる。

※１　SPF（Sender Policy Framework）：送信側のメールサーバーの IP アドレス等を DNS で宣言することにより、ネットワーク的に認証を実施する技術

※２　DKIM（DomainKeys Identified Mail）：送信側のメールサーバーで作成した電子署名により認証する技術

[18] BIMI（Brand Indicators for Message Identification）：メールを送信した企業のブランドアイコンが受信メールフォルダに表示される技術であり、DMARC の導入を前提としていることから、なりすましメール対策において、DMARC を補完するものと整理できる。（参照：警察庁「キャッシュレス社会の安全・安心の確保に向けた検討会報告書」（令和６年３月 21 日））

強化、手口や対策に関する顧客への注意喚起[19]や顧客からの相談への対応の強化等が必要である。

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、金融機関は、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、レビューアとしての有識者の適切な配置によるレビュー体制等の整備を課題として抱えている。

2024 年度においても、勘定系システム更改時に、外部委託先において別プロジェクトで稼働実績のある ATM 仕様を当該更改時に流用したが、別プロジェクトとの仕様差異の理解不足や影響調査が不十分であったことに起因し、ATM の稼働状況を監視するサーバーと連携する機能の実装が漏れたことにより、一部の ATM が起動しない障害が発生している。また、ATM の稼働日に係る設定も別プロジェクトから流用していたが、仕様差異の理解不足や、レビュー時に有識者を配置していなかったことに起因して、ATM の稼働日に係る設定を誤ったため、稼働日であるにもかかわらず、ATM が稼働しなかったり、ATM における取扱業務が一部利用できなくなったりする事案が発生している。

他プロジェクトから ATM 仕様書等を流用する際の仕様差異に関する影響調査プロセス及びレビューや、テスト観点等に関するレビューにおいて、レビューアとしての有識者（金融機関、委託先等の関係者）の適切な配置によるレビュー体制の整備等が必要である。

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

従前より、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、サードパーティの提供するサービスの障害を想定した代替手段の確保やサードパーティとの不断の情報連携等が求められているが、2024 年度においては、セキュリティソフトウェアのアップデートの不具合により、青い画面になり再起動を繰り返す障害（ブルースクリーン障害）が発生し、一部の金融機関の支払い業務に支障が生じた。セキュリティソフトウェアの欠陥がシステム障害を引き起こすことや、特定の製品・サービス等に依存することのリスクを再認識し、パッチ管理、サードパーティリスク管理、コンティンジェンシープランの検討などを含めた IT レジリエンスの強化が必要である。

[19] 例えば、金融庁「インターネット取引サービスへの不正アクセス・不正取引による被害が急増しています」（2025 年４月、https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html）

第２項　冗長構成が機能しない等の障害

従前、勘定系システムと API を接続するためのシステムでハードウェア障害が発生し、副系への切り替えに失敗してアプリ等が利用できなくなった事案や、勘定系システムにおいて、ハードウェア障害が発生し副系に切り替わったものの、パッチを適用していなかった OS の不具合が顕在化したため、通信が不可となり、勘定系システムに係る全ての取引が不可となる事案が発生している。

2024 年度においては、データベースシステム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マニュアルの不備により誤認し、複数のデータベースシステムが２台の通信機器のうち特定の１台のみに繋がる誤ったネットワーク設定となっていた。こうしたネットワーク構成のもとで、メンテナンスのためデータベースシステムと繋がっている通信機器をシャットダウンしたことにより、サービスが利用不可となる事案が発生している。

以上を踏まえ、冗長構成の設定に関するマニュアル整備を含め、冗長構成が意図どおりに機能するよう実効性の確保や冗長構成が機能しなかった際の業務継続のための態勢整備が引き続き必要である。

第３項　システム障害発生時の復旧に関する不芳事案

2024 年度においては、データセンターにおいてスイッチのポート障害が発生した際に、故障したスイッチのポートが完全に停止しなかったことに起因して、データベースに関するシステムが全面停止する事案が発生した。その際に、データベースに関するシステムの全面停止を想定した復旧手順の整備ができていなかったため、障害発生時に迅速な復旧対応が実施できなかった。

データベース等の重要なシステム停止等の不測の事態を踏まえ、障害発生時の業務継続に係る代替手段の整備や障害シナリオを想定した復旧手順の整備が必要である。

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

2024 年度においては、複数の金融機関が利用する IB の共同センターにおいて、移行環境のハードウェアの予防交換作業を実施した際に、移行環境に保有するディスク装置の一部は本番環境からも参照される構成であったことから、予め本番環境から当該ディスク装置への参照を抑止する作業手順とすべきところ、設計書の判読性の低さによりメンテナンス作業者が誤認し、本来の作業手順は本番環境からの参照を抑止する手順を設けるべきところその考慮が漏れ、誤った手順書をもとに作業（移行環境のシステムの電源断）を実施した。このため、本番環境から移行環境のディスク装置参照が不可となり、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案が発生している。また、移行環境作業へのリスク認識が低く、障害発生時の

態勢整備ができておらず、障害発生時の対象システムの特定や事象解析等に時間を要したことから、迅速な復旧対応が実施できなかった。また、IB の共同センターにおいて、一加盟行向けのシステム基盤構築作業時に、作業手順書のレビューに有識者を配置しなかったため、作業手順の不備を見逃したことに起因して、担当者が誤った作業手順書をもとに作業を実施したことにより、作業終了後にシステムが起動せず、システム基盤構築作業とは関係のない他の共同センター加盟行の IB が利用不可となる事案が発生している。

こうしたことから、移行環境作業等のシステム変更作業の影響範囲等に関する設計書の整備や、システム変更の作業手順書に関するレビューアとしての有識者の適切な配置によるレビュー体制の強化が課題となっている。また、電源断等によるシステム停止等の不測の事態を踏まえ、金融機関のみならず、外部委託先を含めた復旧作業手順・体制の整備、不断の情報連携の取組みが課題となっている。

第３編　サイバーセキュリティ

近年のサイバー攻撃の脅威の動向や国内外の情勢、金融庁の検査・モニタリングの経験を踏まえると、金融機関が直面するサイバーリスクが顕著に台頭し、必要なリスク管理態勢と現状の差が拡大していると見られる。そこで、金融庁は 2024 年 10 月に監督指針等を改正するとともに、新たにサイバーガイドライン（「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」）を策定し[20]、当庁の監督上の期待を明確化した。

また、TLPT（脅威ベースのペネトレーションテスト）は、一般的な脅威に止まらず、自組織が抱える固有のリスクを具体的に分析した上で、攻撃者が現実に採用する戦術、手法を再現し、疑似的な攻撃を仕掛けることで、自ら講じた策の有効性や見落とされている点を含め、防御・検知の可否、対応の迅速性・適切性を検証するものである。TLPT は、自組織のリスクを客観的に特定する有効な手法であり、金融機関は、その結果に基づき、効果的にセキュリティ対策を講じることが可能となる。経営陣は、自社のサイバーリスクを正しく認識せずに IT 投資やセキュリティに関わる経営判断をすることで、誤ったガバナンスを構築し、誤った対応を指示してしまう可能性がある。効果的な TLPT を実施することにより、サイバーリスク低減に必要な投資にあたって適切な経営判断の一助とするとともに、単に技術的な対応だけではなく、人・業務上のプロセスの面も含めた組織全体としてのサイバー攻撃対応態勢の実効性向上につなげることが期待される。サイバーガイドラインでは金融機関における TLPT の実施に関する監督上の期待についても明確化しているが、それ以外にも地域金融機関に対する TLPT の実証事業や金融機関が実施した TLPT の事例分析を行うことで、金融機関における TLPT の実施を促進・支援している。

以下では、サイバーガイドラインの要諦及び金融庁の TLPT に関する取組みを概説する。

第１章　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

第１節　経緯・背景等

サイバーガイドラインの策定に当たっては、国内外のフレームワークを参考にするとともに、当庁の検査・モニタリングで発見した事項等を盛り込んだ。サイバーガイドラインでは、特定、防御、検知、対応・復旧についての項目に加え、こうしたフレームワークにおいて近年重要な要素とされる経営陣のリーダーシップを含むガバナンス、サードパーティリスク管理に関する着眼点を盛り込んでいる。

また、サイバーガイドラインでは、各領域において「基本的な対応事項」と「対応が望ましい事項」を明確化した。「基本的な対応事項」は、いわゆる「サイバーハイジーン」と呼ばれる事項その他の金融機関等が一般的に実施する必要のある基礎的な事項を指し、「対応が望ましい事項」は、金融機関等の規模・特性等を踏まえると、インシデント発生時に、地域社会・経済等に大きな影響を及ぼし得る先において実践することが望まし

[20] 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）及び『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』（案）に対するパブリックコメントの結果等について」（2024 年 10 月４日、金融庁ウェブサイト https://www.fsa.go.jp/news/r6/sonota/20241004/20241004.html）。

いと考えられる取組みや、他国の当局又は金融機関等との対話等によって把握した先進的な取組み等の大手金融機関及び主要な清算・振替機関等が参照すべき優良事例を指す。

金融機関の規模・特性は多様であり、「基本的な対応事項」及び「対応が望ましい事項」の双方について一律の対応を求めるものではない。金融機関自らを取り巻く事業環境や経営戦略、リスク許容度等を踏まえ、サイバーセキュリティリスクを特定・評価し、それに見合った低減措置を講ずる「リスクベース・アプローチ」が求められることをサイバーガイドラインに明記している。なお、規模や業態などの要素だけでサイバーガイドライン記載事項の該否を考えるべきではなく、脅威環境などによってリスクは変動し得る点に留意が必要である。

当庁のモニタリングに当たっては、サイバーガイドラインへの対応については金融機関で重要性・緊急性に応じて優先順位を付けた上で、リソースの制約を踏まえ、リスク低減措置に取り組むべきであることに留意することとしている。この優先順位の付け方は一意に存在するものではなく、各金融機関で検討が必要である。

第２節　経営陣の関与の必要性

前述のとおり、サイバーガイドラインではリスクベースでの対応が求められるものの、サイバーリスクは金融機関の経営に重大な影響を及ぼしかねないトップリスクの一つであるため、金融機関においては、その管理態勢の整備及び実効的な運営が喫緊の課題となる。金融機関を取り巻く脅威動向やリスクを踏まえると、形式的な体制整備ではなく、ガバナンスを含めたサイバーセキュリティ管理態勢が、現実にどの程度有効に機能するかという観点からの実質的な対応が求められる。サイバーインシデントによる業務中断や機密情報の漏えいは、金融機関の事業・経営ならびに金融機関に対する信頼を揺るがしかねない重大な影響をもたらし得る。これは金融システムの不安定化をも招きかねない。

サイバーセキュリティの強化には、IT 部門だけではなく、各業務所管部や企画、広報、コンプライアンス、リスク管理、監査などの各部門間の連携が不可欠である。技術的対策だけでなく、いかに組織的な対策も推進できるかは、経営者の認識とイニシアチブによるところが大きい。

サイバーガイドラインでは、経営陣のリーダーシップの下でサイバーセキュリティに関するガバナンスの確立が必要である点を明記している。例えば、経営陣が自らリーダーシップを発揮し、サイバーセキュリティ確保に向けた組織風土を醸成する必要性を記載している。これには、経営陣が担当部署等の特定の部署あるいは特定の職員に対応を任せるのではなく、組織全体（部門、職員のレベルなどを問わず）として、サイバーセキュリティ管理態勢を構築・運用することが含まれる。

また、人材育成に配慮した人事政策や、セキュリティ人材育成計画の策定の必要性について、サイバーガイドラインでは独立した節を設けて記載している。セキュリティ人材は金融分野以外でもひっ迫しており、外部からの調達は容易ではない。こうした中、計画なく短期的な内部人材の配置転換を繰り返せば、人材の確保・育成はますます困難になる。事業継続の上でセキュリティの確保は欠かせない前提であることを認識し、中

長期的な視点で人材の確保・育成に取り組む必要がある。こうした対応は、経営陣が率先して関与しなければ実現は容易でないと考えられる。

第３節　基本的な対策の徹底や侵入を前提とした対応の強化

サイバーガイドラインには、基本的な対策として情報資産管理や脆弱性管理、定期的な脆弱性診断・ペネトレーションテストの実施、ID アクセス権管理などについての着眼点を記載している。これらは、過去の検査・モニタリングにおいて対策が不十分な事例が散見され、対応を促してきた事項でもある。また、本レポートの事例集からも分かるように、基本的な対策の不備に起因する障害事例が依然として散見されており、対策の徹底が必要である。

上記の基本的対策の実施頻度や程度・水準等は画一的には定まらない。例えば、情報資産の台帳をどの程度「最新の状態」に保てばよいのかという点や、脆弱性管理において、他のトラブルやコストを考慮してパッチ適用を速やかに実施しない場合については、リスクベースで判断すべきであり、例えば深刻な脆弱性が明らかになった場合に対応できるかという観点を考慮する必要がある。深刻かつ機密性・可用性・完全性に重大な影響のある脆弱性であるにもかかわらず、他のトラブルがあることをもって代替的な低減措置なしにパッチ適用を否とするかについては慎重な検討が必要である[21]。

また、防御に関する技術的対策の運用・管理を外部ベンダーに委託する場合であっても、サイバーセキュリティに関する最終的な責任を委託先に転嫁することはできない。委託先に対する統制・管理の責任が金融機関にあることを前提として、必要に応じて外部リソースを活用し、自組織のサイバーセキュリティを補完・強化することが考えられる。

さらに、リスク評価に当たっては、境界防御型セキュリティが突破又は迂回されるリスクや、内部不正などの脅威も考慮し、内部ネットワークセグメントに設置したシステムのリスクも対象とする必要がある。当庁は境界防御型セキュリティの限界について、これまで様々な機会を通じて強調しており、サイバーガイドラインでも明確化している。サードパーティやサプライチェーン経由のものを含む内部不正のリスクが現実の脅威となっていることを踏まえた対応も欠かせない。

防御や検知だけでなく対応や復旧についても、様々なケースを想定しておくことが重要である。サイバー攻撃か否かによって、そしてサイバー攻撃の種別によって、インシデント対応や復旧計画は異なると考えられる。例えば、サイバー攻撃はシステム障害とは異なり、復旧や再接続時の再感染リスクの確認において対応に違いがあり得る。また、ウェブサイトのダウンを狙った DDoS 攻撃と、不正送金を引き起こす攻撃では、顧客対応の内容に違いが生じ得る。このように、様々なケースを想定して、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を策定する必要がある。それとともに、これらの実効性を定期的な演習・訓練によって確認し、技術面のみならず態勢面も継続的に改善す

[21] 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）及び『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』（案）に対するパブリックコメントの結果等について」（2024 年 10 月 4 日、金融庁ウェブサイト https://www.fsa.go.jp/news/r6/sonota/20241004/20241004.html）を参照されたい。

ることが重要である[22]。

第４節　サードパーティリスク管理

本レポートでも取り上げているとおり、サードパーティに由来するサイバーインシデントで金融機関の業務や顧客が影響を受ける事例が多発している。サイバーガイドラインでは、サードパーティリスク管理に係る対応事項を詳細に記載している。

サードパーティリスク管理は、チェックリストを用いた形式的な確認によることが多いと考えられる中、リスク管理を実効的なものとしていくことが重要である。リスク管理の目線を揃える観点から、サードパーティリスクを一元的に管理する統括部署の設置や、関係部署間の連携が重要である。ライフサイクル管理（契約前のリスク評価・デューデリジェンス、期中のモニタリング、出口戦略など）も求められる。インシデントの発生を想定してコンティンジェンシープランを整備する際は、様々なシナリオの下で、サードパーティのリスクも考慮することが必要である。

なお、特にサービス提供型のサードパーティの場合、サードパーティからの情報開示に制約があり、リスク管理が困難という意見もある。一般論として、このような場合には、サイバーセキュリティの適切性・十分性について、契約書や第三者保証による報告書、サードパーティから提供される報告書等を活用することが考えられる。さらに、サイバーガイドラインでは、金融機関にサービスを提供するサードパーティが、そのサービスに係るサイバーセキュリティリスクを金融機関が適切に管理する上で必要な支援（リスク管理上必要とする情報の提供など）を金融機関に対して行うべきであることも示している。[23]

第５節　業界団体や共助組織・中央機関の役割

特に規模が小さい金融機関において、最新の脅威や攻撃手法などの情報収集・分析や対応のノウハウ蓄積を単独で行うことには限界がある。そのために金融 ISAC などの「共助」の組織が設立され、技術的な課題への対応やベストプラクティスの提供、最新のサイバー攻撃の動向、脆弱性情報の分析、実践的な演習の実施等に関し、積極的な情報共有その他の協力が行われている。また、協同組織金融機関の場合、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る。中央機関には、サイバーセキュリティに関する業務補完･支援の充実を通じて､業態内の相互扶助の充実を図ることが期待されている。金融機関にとってサイバーセキュリティは、競争分野ではなく協調分野である。さらなる共助の余地があると考えられ、こうした共助組織、中央機関、業界団体やその活動の果たす役割は大きく、サイバーガイドラインにおいてもその旨記載している。

---

[22] 本編第２章「金融機関における脅威ベースのペネトレーションテスト（TLPT）」も参照されたい。

[23] 金融機関がパブリッククラウドサービスを利用する場合、障害（サイバー攻撃によるものを含む）対応上、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が留意すべき点については、第４編「クラウドサービス事業者との対話」を参照されたい。

仮に自らの組織のサイバーセキュリティが強固なものであったとしても、他の金融機関の脆弱性が明らかとなれば、業界全体が標的とされ得るほか、業界全体の信頼が損なわれる事態に発展することもあり得る。サイバーセキュリティは、業界、ひいては金融サービスの利用者、当局を含めたステークホルダーが、エコシステム全体で強化すべく努める必要がある。

第２章　金融機関における脅威ベースのペネトレーションテスト(TLPT)[24]

第１節　TLPT に関する金融庁の取組み

金融庁では、2024 年度、TLPT に関して大きく２つの施策を実施している。１つ目の施策が、「TLPT 実証事業」である。これは、地域金融機関の実態を把握するため、幾つかの金融機関に対して TLPT を実施し、判明した脆弱性について、よく認められるものを地域金融機関に還元するとともに、地域金融機関において TLPT が実行可能で有用であることを示すことにより、地域金融機関において TLPT の実施を促す取組みである。２つ目の施策が、「TLPT 事例分析」である。これは、金融機関における TLPT の実施事例を収集し、主な好事例及び課題を整理し、匿名化・一般化した上で、その結果を業態全体に共有する取組みであり、2023 事務年度に銀行を対象に実施した[25]ことに引き続き、2024 事務年度は保険会社を対象に実施した。

第２節　TLPT を実施するにあたっての推奨事項

本章では、TLPT 実証事業を通じて得られた、TLPT を実施するにあたっての推奨事項を記載する。推奨事項としては、主に以下の６点が挙げられる。

①　テスト目的の認識合わせ

TLPT の最終的な目的は、自組織におけるリスクを可視化し、必要な対策を講じ、サイバー攻撃に備えることである。まず、リスクを可視化した上で、次に、検知力・対応力の評価を行うべきである。TLPT 実施ベンダーの中には、テスト期間の中で段階を分け、まずは検知がされにくい手法を優先して行い、リスクを可視化した後、検知がされやすい手法を用いて検知力・対応力の検証をすることにより、両者を効率的に進めているケースもある。

②　スコープの設定とテスト内容

TLPT では、脆弱性診断やペネトレーションテストと異なり、特定のシステム単体にスコープを絞らず、組織全体をスコープとすることが望ましい。例えば、クラウド環境上に格納している顧客情報を攻撃目標とした際、実際のサイバー攻撃は、従業員が使用している端末等を経由する可能性がある。そのため、クラウド環境のみにスコープを絞らず、従業員が使用している端末等の組織全体をスコープに含める

---

[24] Threat-Led Penetration Testing の略。脅威ベースのペネトレーションテスト。自組織が抱えるリスクを個別具体的に分析した上で、攻撃者が採用する戦術、手法を再現し疑似的な攻撃を仕掛けることで、侵入・改ざんの可否や検知の可否、対応の迅速性・適切性を検証する、より実践的なテストを指す。レッドチームテストとも呼ばれる。

[25] 概要については 2024 年６月に公表した「金融機関のシステム障害に関する分析レポート」にコラムとして掲載している。(https://www.fsa.go.jp/news/r5/sonota/20240626/20240626.html)

ことが望ましい。また、個別システムの技術的な脆弱性を評価したい場合は、脆弱性診断やペネトレーションテストの活用が適している。

リスクの可視化のためには、導入している対策や製品の強度といった技術的な側面だけではなく、フィッシングメールへの対応や物理侵入への対応といった「人」や「プロセス」のリスクを可視化することが不可欠である。テスト環境では実際の人の振る舞いや対応のプロセスを検証できないため、本番環境においてテストを実施することを推奨する。

テスト内容に関しては、事前に決定する検証項目は最低限実施する内容として定義しつつ、テスターがテスト中に得られた情報に応じて柔軟に実施内容の拡張をする形が望ましい。

③　経営層の関与

TLPT の業務影響を最小限のものとするためのリスク管理計画の策定のためには部門横断的な調整が求められることなどから、TLPT の実施を経営陣が主導することが重要である。経営陣の関与不足などにより、テストの制限事項が多くなり、TLPT の目的が達成されなくなる事例が認められている。なお、テスト結果の活用に関し、経営層が TLPT で攻撃が成功した原因について現場担当者等の責任を問う姿勢を取るのではなく、テストの結果判明したリスクに対応するための施策推進や追加的なリソースの投入をサポートする姿勢を取ることが有用である。

④　関係者との連携・通知

ブルーチーム[26]には非通知でテストを実施することが望ましい。比較的小規模な金融機関などにおいてホワイトチーム[27]の組成が難しいケース場合は、ブルーチームの責任者がホワイトチーム役を務めることも考えられる。その場合も、他のブルーチーム担当者に対しては、非通知でテストをすることが望ましい。

一方、不測の事態に備え、テスト実施に関する事前の通知をしておいた方がよい関係者として、経営層、情報システム部門の責任者、広報部門の責任者などが挙げられる。

⑤　TLPT 実施中に求められるホワイトチームの対応

TLPT 実施中にホワイトチームに求められる主な対応としては、TLPT とサイバー

[26] ブルーチームは、攻撃者に扮したグループ（すなわちレッドチーム）に対して、金融機関等のセキュリティ状況を維持することにより情報システムの安全な運用に責任を有するグループである。なお、通常は CSIRT（SOC、NOC、システムの運用担当等を含む場合もある）が担当する。

[27] ホワイトチームは、攻撃者に扮するレッドチームと、金融機関等の情報システム利用の実際の防御者であるブルーチームの関与を調整する責任を有する。テストにおいて、ホワイトチームはルールの実効性を確保し、テストの実施を監視し、起こり得る問題を解決し、すべての情報要求や質問を受け付け、意図された方法でテストが確実に実行されるようにする。

攻撃によって発生するアラート等を切り分けること、関係者等からの各種照会に対応すること、一度成功した攻撃の再実行を省略する等の効率的なテスト推進を検討することなどが挙げられる。これらの対応を円滑に行うため、ホワイトチームは、レッドチーム[28]との連絡手段を整備しておく必要がある。なお、ホワイトチームからレッドチームへの連絡は、テストの進行を妨げることになる他、レッドチームに不必要な情報を与えてしまい、テスト結果の妥当性を損なうリスクがあるため、必要最小限にすることが望ましい。

⑥　共同利用システムへのテスト

複数の金融機関で共同利用しているシステムにおいても、重要なシステムについては、テストの対象とするように調整することが望ましい。関係組織との調整の結果、テストの実施が難しい場合は、共同利用システムの中で、自社が利用する範囲に限定したテストを検討することが望ましい。共同利用システムへのテスト自体が難しい場合は、監査証跡等のセキュリティが担保されていることを確認すべきである。

第３節　TLPT として望ましい事例、不十分な事例

本章では、本年度において分析した保険会社における TLPT の事例から抽出した望ましい事例と不十分な事例を下表のとおり記載している（前述の TLPT 実証事業での取組み事例も踏まえて記載している）。金融機関においては、これらの事例を参考にして TLPT を実施することが望ましい。

なお、TLPT としては不十分なテストであっても、サイバーセキュリティの強化に資する側面がないわけではないため、そうした金融機関の取組み自体が否定されるものではない。

（図表２）TLPT として望ましい事例と不十分な事例

望ましい事例	不十分な事例
１．経営陣の承認、テストの実施体制	
・ 経営者が TLPT の目的を理解し、予算、実施方法（本番環境での実施等）及びリスク管理計画を含め、テスト計画を承認し、テストの実施を推進している。 ・ ホワイトチームとレッドチームが連携し、状況を確認しながらテストを実施している。	【課題事例】 ・ 本番環境ではなく、テスト環境でテストを実施している。また、予算が過少で、予算内に収まるようにテストスコープを狭めている。 【考えられる対応】 ・ TLPT は、技術的な側面だけでなく、攻撃予兆の検知や、攻撃発生時のインシデント対応といった「人」や「プロセス」の評価も行うことで、より現実的なセキュリティリスクの可視化が可能になる。開発環境では、人

[28] レッドチームは、テスト実施者のグループであり、金融機関等のセキュリティ状況に対して、攻撃者が実施する可能性のある攻撃を行うことや、侵入能力を模倣する権限が与えられ、組織されている。通常、ペネトレーションテストプロバイダーのメンバーにより組織される。

	員や業務プロセスが本番環境と異なることが多く、現実のリスクを正確に評価することが困難であるため、本番環境に対して疑似攻撃テストを実施することが望ましい。また、特定のシステムやシナリオだけにスコープを限定すると TLPT の目的を達成できないため、組織全体を対象になるべくスコープを制限せずにテストを実施する。（本編第２章②「スコープの設定とテスト内容」も参照） 【課題事例】 ・ レッドチームとブルーチームだけが定義され、ホワイトチームの体制や役割が不明確なままテストを実施している。 【考えられる対応】 ・ TLPT 全般のコントロールやテスト結果の評価等を行うホワイトチームを明確に定義する。（本編第２章⑤「TLPT 実施中に求められるホワイトチームの対応」も参照）
２．脅威インテリジェンス	
（１）脅威情報の調査・分析	
・ 自組織を標的とすることが想定される攻撃グループの調査と自組織に対する攻撃の糸口となり得る情報をインターネット上で取得可能かについての調査の両方を実施している。 ・ 自組織の公開情報に基づく脅威情報を収集・評価し、潜在的な脆弱性やリスクの洗出し、アタックサーフェスとなる特定システム領域に関する情報を収集し、分析している。	【課題事例】 ・ 脅威情報の調査・分析を省いており、自組織に対して考えられる脅威アクターや攻撃手法を評価・分析できていない。 ・ 自組織の脅威環境を考慮しないまま、予め設定されたシナリオのみの下でテストを実施している。 【考えられる対応】 ・ 自組織にとっての脅威だけではなく、金融業界やサイバー空間全般を取り巻く脅威を分析し、最新の攻撃動向（脅威アクターや攻撃手法等）を踏まえてテストを実施することが望ましい。
（２）想定する攻撃者（脅威アクター）	
・ 保険業界だけではなく、過去に金融業界に対する攻撃を行った実績がある攻撃グループを想定して想定攻撃者を選定している。 ・ 脅威インテリジェンス結果から攻撃者グループの手法や技術を MITRE ATT&CK のフレームワークに基づいて可視化・整理し、脅威シナリオに取り込んでいる。	【課題事例】 ・ 具体的な攻撃者を想定していない。 【考えられる対応】 ・ 上記２（１）に同じ。
３．評価	
（１）テスト結果の評価	
・ テストベンダーがしかけた攻撃が成功せず、一定水準の対策がなされていることを確認したが、それに止まらず侵入された前提で更にテストを進め、自社のリスクを可視化し、改善が必要な点を特定し、改善を進めている。	【課題事例】 ・ 外部から侵入を試みるテストを実施し、攻撃が不成立であったことだけが結果として報告されており、侵入された前提での更なる調査を試みていない。 【考えられる対応】 ・ サイバー攻撃への対策の考え方として、多層防御が重要である。仮に外部からの侵入が成功した場合に、どのような防御策が有効であるのかを検証し、リスクの可視化をすることが望ましい。
（２）検知・対応能力の評価	
・ ブルーチーム（SOC）は、TLPT とは知らされずに発生した脅威に対応し、検知・対応能力の評価が行われている。 ・ テスト終了後、レッドチームとブルーチームが連携して要改善事項の対応方針を協議している。	【課題事例】 ・ ブルーチームへの情報開示を行った上で TLPT を実施しており、リアルタイムの検知・対応能力の評価ができていない。 【考えられる対応】

	・ 現場のブルーチーム担当に対しては、可能な限り非通知でテストをすることが望ましい。（本編第２章④「関係者との連携・通知」も参照） 【課題事例】 ・ EDR 等のセキュリティ製品の有効性を評価するにとどめており、「人」や「プロセス」の評価が行われていない。 【考えられる対応】 ・ TLPT は、セキュリティ製品の有効性の評価だけではなく、「人」や「プロセス」も評価する事が望ましい。（本編第２章②「スコープの設定とテスト内容」も参照）

第４編　クラウドサービス事業者との対話

国内外で、クラウドサービスの利用が進む中、我が国金融分野では８割を超える金融機関でクラウドサービスが利用され、基幹系システムへのクラウドサービスの採用や検討も進んでいる[29]。

こうした背景には、金融機関が AI の利活用上クラウドサービスの利用を進めている[30]ほか、国内の IT ベンダーが金融機関の勘定系システム用に提供してきたメインフレームの事業から撤退することを公表する中、金融機関が勘定系システムの更改を迫られており、メインフレームの代替選択肢としてクラウド上に勘定系システムを移行させる事例が出てきていることなどがある。こうした昨今の傾向を踏まえると、今後も、金融機関の重要なシステムにおけるクラウドサービスの利用が拡大していく可能性がある。

こうした状況を踏まえ、金融庁では、クラウドサービス事業者との対話を行っており、特に金融機関のクラウドサービスの利活用において認められるリスクや論点（集中リスク、クラウドサービスとオンプレミスの比較、勘定系システムへのクラウドサービス利用の趨勢、人材、インシデント対応等）について取り上げた[31]。

第１章　パブリッククラウドサービス利用時の留意事項

上記の対話を通じ、金融機関のパブリッククラウドサービスの利用について、障害対応上、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が留意すべき点として抽出されたものは以下のとおりである。

（１）クラウドサービスの利用は委託に該当すること

銀行法等の業法上、クラウドサービスの利用は委託に該当する（二段階以上の委託を含む）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必要がある。また、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[32]。

---

[29] 公益財団法人金融情報システムセンター「令和６年度金融機関アンケート調査結果」（2024 年 11 月）参照。

[30] 金融庁「AI ディスカッションペーパー（第 1.0 版）」（2025 年３月、https://www.fsa.go.jp/news/r6/sonota/20250304/aidp.html）

[31] 金融庁「金融分野におけるサイバーセキュリティ強化に向けた取組方針」（2022 年２月、https://www.fsa.go.jp/news/r3/cyber/torikumi2022.html）において「金融機関でクラウドサービスの利用が拡大する中、クラウドサービスの特性や仕様の理解不足等に起因するアクセス権限の設定不備による顧客情報の漏えいなど、多くの金融機関に影響を及ぼす事案が発生した。金融機関は、クラウドサービスの利点を活かすうえで、クラウドサービスの仕様、特性に伴うリスクも適切に評価し、システム稼働の安定性や顧客情報の適切な管理を確保する必要がある。過去のインシデントを踏まえると、金融機関がクラウドサービスを活用するうえで、サイバーセキュリティが確保されているかを確認するためには、例えば、インシデント発生時のコンティンジェンシープランの整備や演習の実施を通じて、システムの可用性やデータの機密性を確認することが有効である。（改行）金融庁においても、金融機関のクラウドサービスの利用実態やそれに伴うサイバーセキュリティ管理態勢の把握を進めるほか、クラウドサービス事業者との対話を行う」とされている（３（２）②）。

[32] 例えば銀行法第 12 条の２第２項。また、金融機関・クラウドサービス事業者・ベンダー等が会員となっている公益財団法人金融情報システムセンターが策定した「金融機関等コンピュータシステムの安全対策基準・解説書第 13 版」（2025 年３月）参照。

（２）障害発生時の状況把握

パブリッククラウドサービスを利用する場合、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について、予め確認する。例えば、パブリッククラウドサービスに起因した障害が発生した場合、金融機関が得られる障害対応に必要な情報は、クラウドサービス事業者がインターネット上に独自のタイミングと内容で公表・通知する情報に留まる可能性があることから、金融機関が誤った復旧対応を行ったり、業務復旧のための対応が遅れたりするリスクについて予め確認する[33]。

（３）演習の実施

上記（２）のリスクを評価するため、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で、起こり得るシナリオを具体的に設定し、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。また、こうした取組みを同一のパブリッククラウドサービスを利用する複数の金融機関が共同で実施することも有効である。

（４）インシデント対応計画・コンティンジェンシープランの整備・更新

上記のような取組みを通じ、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[34]。

第２章　今後の金融庁の取組み

上記のような取組みを通じ、金融機関において、クラウドサービスが金融システムの安定に貢献する形で利用され、また、イノベーションを支える基盤として利活用されることが期待される。当庁としては、クラウドサービスに限らず、IT レジリエンスの向上の観点から、関係者が共同で行う取組みに、必要に応じて協力していく。

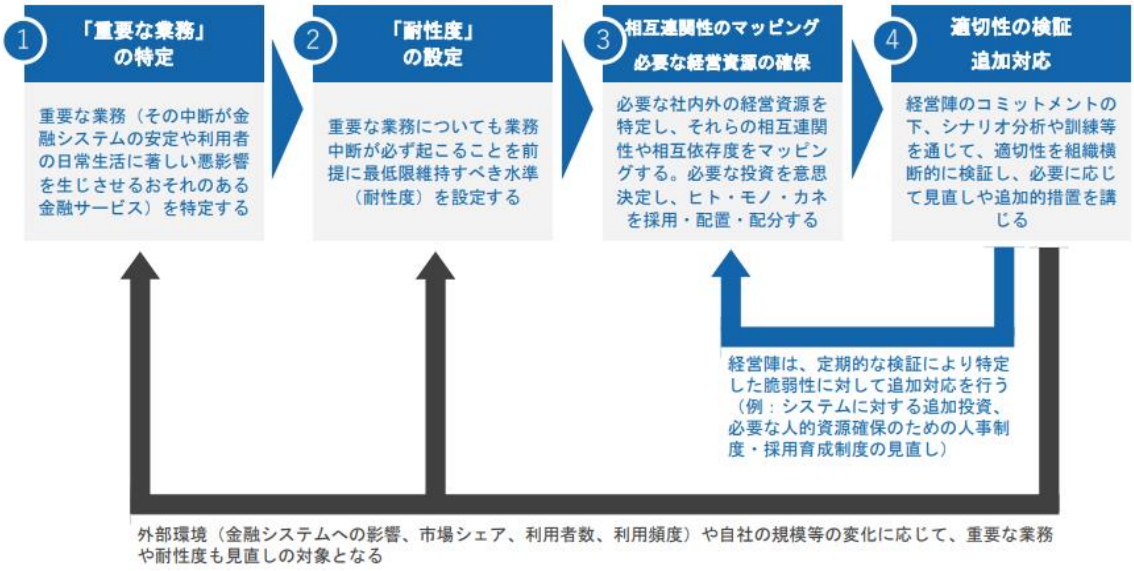
[33] 復旧対応以外の障害対応として、発生原因の究明・復旧までの影響調査・改善措置・再発防止策等が的確に講じられていることの確認、金融機関等が行う顧客への説明・当局への報告が考えられる。

[34] 金融庁「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、https://www.fsa.go.jp/news/r6/sonota/20241004/20241004.html）では、クラウドサービス利用時の対策として、「多岐にわたる関係主体等を把握し、情報共有体制・インシデント対応態勢を構築すること」を挙げている（2.3.4.5.）。

第５編　金融機関におけるオペレーショナル・レジリエンス

金融庁では、「オペレーショナル・レジリエンス確保に向けた基本的な考え方」（オペレーショナル・レジリエンス（オペレジ）に関するディスカッション・ペーパー）を 2023 年４月に公表しているが、その中で、金融機関におけるオペレジ確保に向けた基本動作を４つのステップで整理している（図表３）。

（図表３）オペレジの基本動作



第１章　オペレーショナル・レジリエンスに関する金融庁の取組み

金融庁では、上記ディスカッション・ペーパーの趣旨を踏まえ、2023 年６月に主要行等向けの総合的な監督指針[35]（以下、「監督指針」という。）を改正しており、同ディスカッション・ペーパー、監督指針に基づき、2023 事務年度から一部の金融機関を対象にオペレジに関するモニタリングを実施している。

第２章　　金融機関の取組事例・課題事例

モニタリングの結果に基づき、オペレジの基本動作ごとに取組事例、課題事例をまとめると以下のとおりである（各基本動作の考え方、取組事例、課題事例の定義は図表４参照）。なお、これらの事例は、アンケートやヒアリングの結果に基づいた一般的な傾向や金融機関にとって参考となると考えられる事例をまとめたものであり、金融庁として個別の金融機関及び業界全体の進展度について認定するものではない点や、本文書で紹介する取組事例を実施することでオペレジの確保が完了することを担保するものではない点に留意が必

[35] https://www.fsa.go.jp/news/r4/ginkou/20230623-2.html

要である。

金融機関においては、これらの事例を参考として、オペレジ対応における課題の解決やそれぞれの規模・特性を踏まえたベストプラクティスの探求を行うことが望ましい。

（図表４）基本動作ごとの取組事例と課題事例の定義

考え方	ディスカッション・ペーパーに記載している基本動作の考え方
取組事例	先行事例を含めた金融機関の取組事例
課題事例	金融機関が認識する課題又はその事例

①「重要な業務」の特定

＜考え方＞

- 「重要な業務」（その中断が金融システムの安定や利用者の日常生活に著しい悪影響を生じさせるおそれのある金融サービス）を特定すること。

＜取組事例＞

- 「公共的使命」「金融市場」「自社の健全性」の観点で各業務を評価した上で選定している。
- BIA[36]（ビジネスインパクト分析）を行い、（金銭的）資産の損失、対外（顧客、取引先）関係の損失、社会的影響等の観点で評価し、重要な業務を特定している。
- 「代替可能性」「市場シェア・利用者数」について他項目より重み付けを大きくし、より利用者目線に沿うような選定方法を検討している。
- 自社の商品・サービス一覧等から、既存の BCP[37]における重要な業務、利用者の資金決済・資金調達等に関連する業務を抽出し、重要な業務の候補を選定。その後、「代替可能性」「利用頻度」等の項目で重要性評価を行い、評価結果と経営陣の意見等を踏まえ重要な業務を特定している。
- 決済業務を中心に選定した BCP 上の重要な業務をベースに、海外当局の重要業務評価項目を参考に選定基準を設定している。
- 「重要レベル（業務の優先度）」と「時限性」の２軸でリスクを評価し重要な業務を特定している。
- 「代替可能性」と「影響度」の２軸で評価。影響度は顧客の利用頻度、市場シェア・利用者数、金融システムへの影響度、中断時の最大損失等の観点で評価している。

＜課題事例＞

- 評価対象業務の洗い出しにおける網羅性確保の難度が高い。

②「耐性度」の設定

[36] Business Impact Analysis の略。
[37] Business Continuity Plan の略。

＜考え方＞

- リスク選好度（リスクアペタイト）を設定した上で、重要な業務と特定した金融サービスについて、未然防止策を尽くしてもなお、業務中断が必ず生じることを前提に最低限維持すべき水準を「耐性度」（Tolerance for disruption）として設定すること。

＜取組事例＞

- 耐性度として、既存の BCP における RTO[38]（目標復旧時間）を利用することを検討している。
- RTO を「完全復旧」と「暫定復旧（暫定的な事業継続策を実施するまでの時間）」の２段階にしている。
- 既存の BCP における事務処理時限（カットオフ）をベースに耐性度を設定。代替手段により処理可能時限が後ろ倒し可能な場合は、後ろ倒し後の時限を耐性度として設定している。
- 業務の特性に合わせて最大停止許容時間や取引時限等の指標を選択して耐性度を設定している。
- 既存の「いつまでに復旧するか」の指標である RTO に加え、「RTO の時点で平時と比較してどの程度の業務量を復旧しなければならないか」の指標である RLO[39]（目標復旧レベル）を耐性度として新たに設定している。
- 耐性度については、「時間（いつまでに）」と「復旧水準（どの程度まで）」を基準に設定。「時間」は顧客・金融システム・自社への影響度の定量評価等を踏まえ設定し、「復旧水準」はシェアと代替可能性のマトリックスを作成し設定している。
- 重要な業務ごとに、「顧客影響」「金融システム影響」「最大損失」等のそれぞれの観点で、許容可能な最大限の業務中断時間を決め、そのうち最も短い時間を当該業務の耐性度として設定している。
- 年次で BIA を行い、その結果を受けて RTO の見直しを行っている。見直しの結果を受けて、耐性度を高める施策を実施している（拠点における耐震性・確保電力の冗長化（非常用発電機設置等）、代替オフィスの整備等）。

＜課題事例＞

- 耐性度の設定にあたっては、考慮すべき条件が多岐にわたり、条件次第で耐性度が変わるため、条件の設定に苦慮している。設定する業務範囲と粒度次第で想像以上に業務負担が大きくなる。

③相互連関性のマッピング・必要な経営資源の確保

[38] Recovery Time Objective の略。
[39] Recovery Level Objective の略。

＜考え方＞

- 重要な業務の耐性度での提供に必要な社内外の経営資源（ヒト・モノ・カネ）を端から端まで（end to end の業務プロセス全体で）特定し、それらの相互連関性や相互依存度をマッピングすること。その上で、必要なスキル・専門性を持った役職員を採用・配置し、適切な施設、システム、サードパーティ等を調達・確保し、保守・改善のための十分な投資を行うこと。

＜取組事例＞

- 商品･サービスを顧客接点から終了までの各工程と関係者を可視化した業務フロー図をベースとして、不足しているシステムや施設等のリソース（経営資源）を追加している。
- end to end の業務フローを作成し、業務の各プロセスでどの経営資源（人員・施設・システム・サードパーティ）が必要となるかを特定。業務フローにて特定した経営資源について、業務遂行において何名の人員が必要か、関連システムは何か、再委託先はどこかなどの粒度で記載し、相互連関性のマッピングを実施している。
- end to end で業務フロー図を整備し、通常時の業務体制・使用拠点・システム等について実地調査を実施。重要な業務の社内外関係者・関係業務・使用システムをフローチャートで一覧化。重要な業務同士の前後関係から、業務目標復旧時間・システム目標復旧時間の整合性を確認している。
- 各ユーザ部門・システム部門が連携し、重要な業務単位でフローチャートを新規に作成。これに基づき、リソースに応じたリスク・脆弱性を特定するため、質問票を作成し各ユーザ部門・システム部門に回答してもらうとともに、重要な業務単位で関係者に個別ヒアリングを行っている。
- 相互連関性のマッピングは、サマリーシートと詳細版シートで構成。サマリーシートは、業務フローの概要、業務の重要性評価結果、代替手段、人員、システム、サードパーティの概要等を記載し、詳細版シートは、業務フローを業務の開始時点から終了時点まで end to end で記載。サマリーシートを作成することで、経営陣が業務を俯瞰できるようにしている。
- 重要ビジネス・サービスに関する業務目線の全体像を最も簡略化する「概要」シートと、その概要に沿ってリソースマッピングの詳細を含めた「詳細」シートに分け、経営層と現場が同じ情報に基づいて会話できるよう工夫。また、現場実務層との詳細確認においては、各関連部署の有識者を個別訪問するなど、社内に散在する情報を繋ぎ合わせるような地道な活動を行っている。
- 各業務のプロセスにおけるフロー図をエクセルベースで作成していたが､システムツールを活用したデータベース化に着手している。
- J-SOX 関連文書をドラフトとして活用し、不足するリソースの情報を他文書にて補完して、リスク・脆弱性を可視化。現状、致命的な経営資源不足は見受けられ

ないものの、今後、「適切性の検証」結果を踏まえ、不足リソース有無を検証の上、経営資源の追加投資要否を協議する予定としている。

※ 金融機関が相互連関性のマッピングにおいて、重要なサードパーティを特定するにあたって、フォースパーティ、クラウドサービス事業者への依存状況を把握・管理するための取組みとして以下の事例が見られた。

- 外部委託の開始時及び定期評価時において、再委託先（２次委託以降を含む）への委託内容や、クラウドの利用状況を確認している。
- 外部委託先調査票を用いて委託先・再委託先のリスク状況を把握している。
- 外部委託契約を対象にサードパーティリスク管理（TPRM[40]）による把握・評価を実施し、TPRM システムにて一元管理された契約、サードパーティ等のデータを用いて、依存度の高い先を特定している。
- 現状、再委託先やクラウドサービス事業者に対して年次でのリスク評価を実施した上で、Excel ベースで集計し、把握・管理を行っている。将来的には CSA[41]で利用予定のシステムツールを活用し、特定のサードパーティへの依存状況の可視化を図る方針としている。
- 外部委託の一連の流れ（リスク評価、契約、モニタリング等）と外部委託先に関する情報を一元的に管理する台帳の構築に取り組んでいる。その台帳に再委託の状況やクラウドの利用有無等の項目を入れて管理することを想定している。

＜課題事例＞

- 現段階で具体的なマッピング手法は未定となっている。
- 現状、サンプルとして数業務をマッピングした段階であり、今後は業務所管部の主導で、社内外の経営資源を端から端まで特定し、マッピングできるかが課題と認識している。
- システム情報（重要な業務を構成するシステム間の関係性等）の整理と粒度、外部委託先の全量調査（現状サンプリング調査に留めている）が課題と認識している。
- 業務プロセスと必要な経営資源の図示を行ったものの、相互連関性を示すまでには至っておらず、今後マッピング方法を改善する予定としている。
- マッピングの対象となる経営資源の情報については今後更なる拡充が必要と認識している。

④適切性の検証・追加対応

＜考え方＞

[40] Third-party Risk Management の略。
[41] Control Self-Assessment の略。

- 経営陣のコミットメントの下、極端だが起こり得るシナリオを想定した分析や訓練等を通じて、リスク選好度、重要な業務、耐性度、必要な経営資源に関する設定及び配分が適切であるかを定期的かつ組織横断的に検証し、必要に応じて見直しや追加的措置を講じること。

＜取組事例＞

- 極端だが起こり得るシナリオを想定して、耐性度までに復旧できるのかについて複数のストレスケースを用いて定量的に検証を実施。検証の結果、耐性度までに復旧できない場合は、課題や補強すべきポイントを明確化し、対応の優先順位等を検討している。適切性の検証にあたって、ストレステスト用の汎用的な「検証シート」を作成している。
- 経営資源ごとに極端だが起こり得るシナリオを設定し、当該シナリオが発生した場合の耐性度の充足度を検証し、リスク評価を実施。リスク評価結果を踏まえ「追加対応」又は「リスク受容」の方針について、関係部署間で審議・決定。適切性の検証にあたって、過去の取引データ等の定量情報を用いることでリスク評価の精緻化を推進している。
- 検証の観点として、「①耐性度までにサービス復旧できるか」「②代替手段開始までの時間は妥当か」「③顧客影響を十分に軽減する代替手段の処理能力があるか」などを予定している。
- 適切性の検証は、机上でのストレステストを実施。シナリオ設定については、経営資源ごとに最も厳しい結果事象となる危機事象を特定し、適切性検証のシナリオとして設定している。
- 各部の対応可能人数や処理量、過去最大の取引件数等を加味した上で、定量的に耐性度までに復旧できるのか、机上によるストレステストを実施している。

＜課題事例＞

- 「極端だが起こり得るシナリオ」として大規模震災を設定しているが、他のシナリオを含めるなどのブラッシュアップが必要と認識している。
- 既存の BCP の考え方に基づく「自然災害」「システム障害」「パンデミック」という特定シナリオからのアプローチだけでなく、ヒト・モノ・システム等の経営資源が毀損した場合を想定したアプローチでの検証が必要と認識している。
- リスクシナリオの設定にあたっては、同時多発を想定し複合的なリスクシナリオの設定が必要と認識している。
- 「複数リソースの制約が同時に発生する場合にどういう想定となるのか」「その想定に関する情報をどのように捕捉していくのか」などは検討課題として捉えている。
- 検証作業に掛かる時間・負荷の軽減のため、より効率的に検証する方法の模索が課題と認識している。

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、2021 年４月から 2025 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[42]、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 外部委託先のランサムウェア感染による情報漏えい新規

＜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など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

[42] なお、過去に掲載した事例については、できる限り判りやすくするため記載を修正している場合がある。

２ 年末年始の DDoS 攻撃新規

＜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など、対策マニュアルや BCP を策定

３ 委託先クラウドのマルウェア感染事案新規

＜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

4 DDoS 攻撃による外部委託先サービス停止新規

＜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

5 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新規

＜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、当該の 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

6 証券サイトにおける不正買付注文新規

＜業態＞
金融商品取引業者等
＜事象＞
- 正当な顧客ではない者（不正アクセス者）から証券サイトにおける顧客口座への不正なアクセスにより、株式の買付注文が不正に発注され約定する事案が発生した。

＜原因＞
- フィッシング等に起因した不正アクセス。

＜対策（2025 年３月 31 日時点では事後改善策検討中のため一部対策のみ記載）＞
- フィッシングサイトのモニタリングによる検出及びテイクダウン
- 不審な電子メール等に関する注意喚起

7 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新規

＜業態＞
暗号資産交換業者
＜事象[43]＞
- 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[44]＞
- 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等。）
- EDR[45]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。

---

[43] 「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。

[44] 「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・内閣サイバーセキュリティセンター・金融庁、https://www.fsa.go.jp/news/r6/sonota/20241224/tyuuikanki.pdf）より抜粋。

[45] 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。

８ 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＞

- 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[46]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

９ 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[47]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）

[46] 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。

[47] 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

１０ 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[48]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）

１１ 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

１２ 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＞

[48] 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。

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。

＜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

１３ 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

１４ 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
- パソコン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

１５ 顧客口座に対する不正アクセス

＜業態＞

金融商品取引業者等

＜事象＞

- 悪意を持った第三者から顧客口座への不正アクセスがあり、各種保有商品一覧画面や入出金画面等を参照された（不正な取引、入出金、属性変更等はなし。）。

＜原因＞

- 顧客の端末がマルウェアに感染したことにより、認証情報が漏えいしていた。

＜対策＞

- 他の顧客口座へのアクセス有無の確認実施
- 不正アクセスの際に利用された端末識別情報について、不正アクセスの早期検知を実現するためのモニタリングシステムのブロックリストへの登録
- 顧客本人によるログインID及びパスワード変更の実施

１６ 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、エラーとなる等の事象が発生した。
- 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

１７ 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

１８ 二要素認証設定未済利用者への不正アクセスによる暗号資産不正出庫

＜業態＞

暗号資産交換業者

＜事象＞

- 現物取引サービスに対し、攻撃者が不正に得たと思われる大量のメールアドレスとパスワードでログインを試行するリスト型攻撃が発生した。
- 利用者の一部で第一認証が突破され、二要素認証設定が未済であった利用者において、攻撃者による暗号資産の不正出庫が行われた。

＜原因＞

- 利用者が口座開設後、銀行口座連携済みでかつ二要素認証設定が未済の状態における不正利用リスクを検討しておらず、攻撃者が不正ログイン後に二要素認証を設定できるようになっていた。

＜対策＞

- 利用者の状態遷移を考慮した不正利用リスクシナリオの検討
- 重要な登録情報を変更する際は、二要素認証の導入等により、本人認証を厳格化すること
- 不正利用リスクを踏まえた暗号資産出庫時の取引内容の確認

１９ 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

２０ 脆弱性情報の収集及び対応の不備に起因したホームページの閲覧不可

＜業態＞
信用金庫・信用組合等
＜事象＞
- ホームページを更新する際に利用するプログラムの脆弱性により、第三者による不正アクセスを受け、ホームページが閲覧不可となった。

＜原因＞
- 利用ソフトウェアの脆弱性情報の収集や対応を適時に実施していなかった。
- インターネットに公開する必要のないプログラムが公開状態であった。

＜対策＞
- 脆弱性情報の収集や対応（脆弱性試験、パッチ適用等）に関する態勢の整備
- 公開するソフトウェアの精査と基本的なセキュリティ対策の実施

２１ インターネット利用に関する基本的な対策の不備による個人情報漏えいのおそれ

＜業態＞
金融商品取引業者等
＜事象＞
- ホームページの管理者用ページに対して本来設定されるべきアクセス制限機能が長期間解除されていたことにより、保存されていた個人情報が窃取されるおそれがあった。

＜原因＞
- 管理者はブラウザに記憶された ID、パスワードを利用していると誤認し、認証していないことに長期間気付かなかった。

- 認証機能自体は存在することから、ホームページのセキュリティは十分であると誤認し、定期的なシステムリスクアセスメントが実施されていなかった。

＜対策＞

- ログイン時の認証手順の見直し、IP アドレスの指定等によるホームページ管理用ページへのアクセス制限
- インターネットに接するシステムに対する定期的なシステムリスクアセスメントの実施

２２ 要件変更時の対応不備等に起因したランサムウェア感染

＜業態＞

金融商品取引業者等

＜事象＞

- インターネットを経由して顧客のシステムが接続して利用するサービスにおいて、運用上不要である RDP 機能[49]が設定ミスにより開放されていたことに起因し、顧客の利用システムがランサムウェア[50]に感染した。

＜原因＞

- 本サービスは、当初インターネット接続を不要とする環境を前提としていたが、機能追加の結果、インターネット接続することとなった。その際に行った構成変更のレビューが不十分であったため、必要な通信制御の設定や外部からの不正アクセス監視等を実施していなかった。

＜対策＞

- 本番リリース時の判定基準に、インフラ構成やセキュリティ機能を確認する項目を追加

２３ マルウェア被害対策の不備に起因したエモテット感染

＜業態＞

保険会社等

＜事象＞

- マルウェア（エモテット）に感染し、個人情報等のメール情報が窃取された。

＜原因＞

- 標的型攻撃メール訓練は行っていたが、最新のサイバー攻撃の実例等を踏まえた訓練シナリオになっていなかった。また、全役職員への最新のサイバー攻撃に関する教育が不十分であった。
- システム運用において、休日にマルウェア感染の警告メッセージを確認する体制を整備していなかったことから、感染端末のネットワークからの隔離が翌営業日となり初動対応が遅れたことで、二次被害が発生した。

[49] リモートデスクトップ機能。コンピュータのデスクトップ画面を、ネットワーク経由で他のコンピュータに転送し、遠隔から操作する機能。

[50] 悪意のあるソフトウェア（＝マルウェア）の一種で、感染したコンピュータを正常に利用できない状態に置き、復元のために金品の支払いを要求するもの。

＜対策＞

- 最新の実例等を踏まえた訓練や注意喚起の実施や全役職員への教育の徹底
  緊急時における社内外の連絡体制の整備や定期的な見直し

２４ 秘密鍵の災害・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秘密鍵の災害・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＞

- 秘密鍵の災害・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

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 勘定系システム更改に関連する ATM 障害新規

＜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

2 システム統合における ATM の通帳取り込み新規

＜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

3 第三者型ＩＣＯ[51]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新規

＜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

[51] 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。

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

4 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[52]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。

[52] 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

- 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。

５ 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等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。

6 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

7 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

8 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

９ 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

１０ 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

１１ 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

１２ 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

１３ 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

１４ 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

１５ 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

１６ プログラム更改時のテスト不足等に起因するオンライン処理の停止

＜業態＞

主要行等

＜事象＞

- 通帳レス対応に関する営業店オペレーター向けプログラムの改修時の不具合に起因して、オンライン処理で共通的に利用するデータベースの更新等が不可となり、プログラムを切り戻すまでの間、全営業店におけるオンライン処理等が利用不可となった。

＜原因＞

- プログラムの品質チェックにおいて、担当者の思い込みや誤りによって再鑑が機能していなかった。
- プログラム改修が小規模な予算のプロジェクトであったため、テストによる検証が簡易的に行われていた。

＜対策＞

- レガシーシステムの暗黙知を設計書等に明記
- 最大リスクに応じた深度あるテストやチェックリストによる確認

１７ 仕様の把握ミスに起因したスマートフォンアプリケーションのログイン不可

＜業態＞

主要行等

＜事象＞

- 新勘定系システムに移行後に、旧勘定系システムの仕様を誤認したことに起因して、スマートフォンアプリケーションで約１時間、利用不可となった。

＜原因＞

- データベースの設計内容（型指定等）を誤認したまま開発を進めたことで、連携するシステムとの間で不整合が発生した。
- 旧仕様を踏襲する設計であったため結合テスト等の工程で試験内容が不足した。

＜対策＞

- 連携するシステム側の仕様を確認する点を開発ガイドラインに明記
- 旧仕様を踏襲する設計であっても境界値試験等を実施

１８ IT 部門と業務部門の連携不足による祝日設定の誤り

＜業態＞
暗号資産交換業者
＜事象＞
- 取引システムを更改後、本来取引時間外としている祝日において取引が可能な状態となった。

＜原因＞
- 取引システムの祝日設定を誤っていた。
- 取引システムを更改した際、IT 部門と業務部門による仕様確認やテストの分担や手順が不明確であった。

＜対策＞
- 業務に関連するシステムの設定に対する業務部門の確認・指示や IT 部門の作業等のプロセス整備
- システム更改における業務部門の主体的な関与、IT 部門と業務部門との運用に関する役割分担の明確化

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　ハードウェア故障による光量低下時の対応不備新規

＜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

2 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新規

＜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

3 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

4　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

5　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

６　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

７　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

８　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

９　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

１０　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

１１ 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

１２ 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

１３ 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

１４ 復旧手順の準備不足による障害対応時間の長期化

＜業態＞

主要行等

＜事象＞

- 営業店端末と接続するサーバーで複数のハードウェアが故障し、バックアップサーバーへの切替えも不可であったため、結果として復旧が業務開始時刻に間に合わず、災害対策用システムを代替活用し、運用を再開した。
- 来店予定の顧客に、業務開始の直前まで告知できなかったため混乱を招いた。

＜原因＞

- バックアップサーバー単独での起動手順に不備があり、調査等に時間を要した。
- 最悪のケースを想定した復旧対応の時限管理を実施していなかった。

＜対策＞

- 実態に即した（実効性ある）システム障害の訓練
- 影響が顕在化していない初期段階において、最大影響を想定し、対外告知や顧客対応を整備（システムやチャネルを軸とした、影響する業務の把握と業務横断的な BCP の策定）

１５ ネットワーク機器のハードウェア不良に起因する一部 ATM の利用不可

＜業態＞

主要行等

＜事象＞

- ATM システムに関連するネットワーク機器について、既知のバグに起因したログの継続出力による CPU 使用率の高騰やハードウェアエラーに伴う通信の断続的な停止によって、一部の ATM が停止した。

＜原因＞

- 重要システムを構成する機器の状態を収集、監視していなかった。

＜対策＞

- リソースやハードウェアエラーの監視に基づく予兆管理の徹底

１６ 障害箇所等の状態把握に関する対応不備に起因した障害対応時間の長期化

＜業態＞

主要行等

＜事象＞

- ATM とデータセンターを接続するネットワーク機器のハードウェア故障により一部の ATM が停止した。故障箇所の切替えが自動で行われたが、以降も通信の遮断・

接続が繰り返される不安定な状態が継続し、対象機器の切離し等の対処によって復旧するまで数時間を要した。

＜原因＞

- 対象機器の特定等の把握や対応策の検討に時間を要した。

＜対策＞

- ネットワーク機器における発生事象を早期に把握するため、監視内容を見直し

１７ ディスク障害に起因した送金処理等の遅延

＜業態＞

主要行等

＜事象＞

- 様々な業務システムと連携するシステムにおいて、ディスク障害が発生したにもかかわらず冗長構成が機能せず、送金処理等が遅延した。直接原因はディスク装置とサーバー間の通信を担うプログラムの不具合であったが、復旧に手間取り、ディスク交換作業が完了するまで障害が継続した。

＜原因＞

- サービス復旧手順や対応態勢を構築していなかった。
- システムを横断した障害シナリオを想定しておらず、業務面の影響範囲を特定できなかった。

＜対策＞

- システムの重要度に応じた復旧態勢と手順の確立
- 障害発生のタイミングや影響する業務等を考慮した精緻な障害シナリオに基づく対応手順の整備と訓練の実施

１８ 想定を超えたハードウェア障害に伴う復旧時間の長期化

＜業態＞

地域銀行

＜事象＞

- 法人 IB の外部委託先において、断続的に複数のディスクが故障し、ディスクの三重障害が発生したことに起因し、副系システムへの自動・手動切替えに失敗したことで、約５時間、利用不可となった。

＜原因＞

- ディスクの三重障害が発生することを想定していなかったため、対応手順を準備しておらず、また三番目のディスク故障に対する迅速な検知ができなかった。

＜対策＞

- 想定した二重障害に対する対応手順で復旧しない場合のリカバリープランの整備

第２節　設定ミス・操作ミス等の管理面・人的要因

１ メンテナンス作業における作業不備新規

＜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

２ ネットワークの冗長化構成の設定誤り新規

＜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すべての取引・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[53]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

３ 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＞

- 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

４ 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

[53] 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。

＜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

５ 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

６ 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

7 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

8 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

９ 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

１０ 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）

１１ 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

１２ 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

１３ 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

１４ 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

１５ 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

１６ 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[54]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

１７ 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＞

- 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

[54] 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。

１８ 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

１９ 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

２０ 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

２１ 冗長構成が機能しなかったことに起因する障害対応時間の長期化

＜業態＞

主要行等

＜事象＞

- 法人向け IB で、ハードウェア障害に起因して、平日日中の約５時間、利用不可となり、一部取引が翌営業日の処理となった。冗長構成が機能せず最終的に作業員がデータセンターに移動する必要が生じた。

＜原因＞

- 自動切替えが行われなかった場合の作業に慣れておらず作業ミスが発生した。

＜対策＞

- 強制的な手動起動の手順と当該作業に関する訓練の実施（様々な障害パターンの想定と訓練の実施）

２２ 監視対象漏れに起因した、開局直後の一部ログイン不可事象

＜業態＞

主要行等

＜事象＞

- 週次のシステム定例作業後に実施された、開局に必要な起動処理が正常終了しなかったため、開局直後から法人向け IB にログインしにくい事象が発生した。

＜原因＞

- 開局時に必要となる処理のエラー状態を監視していないことで、原因特定に時間を要し、速やかに対処できなかった。

＜対策＞

- 監視するシステムエラーの対象の見直し

２３ システム障害における影響範囲の把握不備に起因した為替取引不可

＜業態＞

信用金庫・信用組合等

＜事象＞

- 口座振替の処理停止により、一部為替発信処理が不可となる事象が発生した。

＜原因＞

- 口座振替の処理停止は検知し対応したが、並行処理される為替発信処理の監視機能がなかったため、担当者は正常に処理されていると誤認した。
- 口座振替の処理停止が為替発信処理に影響するとの認識が無く、為替発信処理に対する影響を確認する手段や資料を整備していなかった。また、システム障害発生初期に組織内部での連携が取れていなかった。

＜対策＞

- 顧客影響や時限性のある処理に対する、監視機能の実装

- 顧客影響や時限性のある処理に対する、停止時の影響確認手順や関係者との連絡体制の整備

第３節　サードパーティの提供するサービス等の要因

１ セキュリティソフト不具合への対応新規

＜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

２ 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

３ 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

4 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

5 様々なネットワーク障害を想定した冗長構成の未整備

＜業態＞
主要行等　地域銀行　ほか
＜事象＞
- オンプレミスで構築した勘定系システムとクラウドシステム間の通信不良に起因

して、IB へのログイン等が断続的に不可となり、各種取引に影響した。

＜原因＞

- 別ルートの通信手段を用意していなかった。

＜対策＞

- 様々な箇所のシステム障害を想定した冗長構成の実現と切替え訓練の実施

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 取引集中に備えた対策の不備による送信の時限超過

＜業態＞

主要行等

＜事象＞

- 外為送金のアンチ・マネー・ローンダリング用システムにおいて、取引の集中に伴う滞留状態に起因して大量のタイムアウトが発生した。結果として外為送金の処理期限までに一部処理が完了しなかった。

＜原因＞

- 取引量増加に伴う電文滞留に対してシステム増強等の対策を取らなかった。
- 電文滞留時の対応に誤りがあり、タイムアウトの発生を誘発する結果となった。

＜対策＞

- リソースの使用率や発生したエラー等のリスク事象を捉えた対策の実施
- タイムアウト等の不芳事象を把握し対応する態勢の構築

５ 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 有識者のレビュー未実施による作業誤り新規

＜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
- 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

２ 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新規

＜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

3 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

4 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

5 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

6 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

7 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

８ 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）

９ 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

１０ 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

１１ モアタイムへの切替えに関する設定ミスに起因した振込エラー

＜業態＞

主要行等

＜事象＞

- 全銀システムとの接続設定に係る人為ミス（コアタイムシステムからモアタイムシステム[55]への切替え時刻の設定ミス）により、他行向けの振込がエラーとなった。

＜原因＞

- 作業実施者に向けた切替え時刻に関する伝達内容が不明瞭であった。また再鑑も機能していなかった。

＜対策＞

- 維持メンテナンス作業における多層的なチェック態勢の構築（設定項目の明確化、再鑑観点の具体化等）

１２ ネットワーク機器の設定ミスに起因した自行 ATM の停止

＜業態＞

地域銀行

＜事象＞

- 委託先サービスと接続するための作業における設定誤りに起因して自行 ATM が停止した。ATM 稼働時間帯に作業したため、数十件の取引が不可となり、現金やキャッシュカードのくわえ込みが発生した。

＜原因＞

- ネットワーク機器の仕様を誤認した状態で構築しており、レビューは書面のみであった。
- 作業リスクを見誤り ATM 稼働時間帯に作業を実施した

＜対策＞

- 実機によるテストとレビューの徹底
- 顧客影響のリスクを考慮した作業時間帯の設定

[55] 全国銀行データ通信システムの内国為替取引を処理するオンラインシステムのサブシステムのこと。平日８時半から 15 時半までの即時入金を実現する「コアタイムシステム」と平日夜間・土日祝日の「モアタイムシステム」がある。

１３ 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 API インターフェース仕様書の確認不足新規

＜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

２ 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

３ 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

４ 本番環境を想定したテストケースの不足に起因する IB の利用不可

＜業態＞

主要行等

＜事象＞

- 法人向け IB に関する新規プログラムのリリースに起因して、約３時間、利用不可

となる障害が発生した。

＜原因＞

- 本番ピーク時相当の負荷テストと組み合わせたテストケースの検証を実施していなかった。

＜対策＞

- 取引が発生しない時間帯でのリリース（対応が難しければ実効性あるテストケースでの検証を実施）

第５章　システム障害後の対応が円滑に行われた事例[56]

１ システム障害時における円滑な初動対応の実施新規

＜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 など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。

２ 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新規

＜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。
- 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＞

[56] 改善が適切に行われた事例を含む。

- 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。

３ 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などなく 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。

４ 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。

５ 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。

６ 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。

７ 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[57]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。

８ 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＞

[57] 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。

9 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　耐量子計算機暗号（PQC）への移行

量子コンピュータの実用化は早ければ 2030 年代半ばと想定されている。これによって現在の暗号技術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情報システムの安全性が根底から覆される可能性がある。そのため、すべての金融機関は顧客や自身の情報・財産を守るため、規模・特性に関わらず、耐量子計算機暗号への移行などのリスク低減策を講ずる必要があるが、その対応には長期にわたり多大なリソースを要するため、経営層がリスクや移行の期限などを正しく認識する必要がある。金融庁では検査・モニタリングなどを通じて、金融機関に早期かつ着実な移行を促していく方針である。

第１章　耐量子計算機暗号への移行の必要性

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[58]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など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「HNDL」（Harvest Now Decrypt Later）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など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。加えて国外では重要なシステムは 2030 年代の早期に移行すべきと推奨されている[59]。これらの背景を踏まえると、金融機関においては直ちに PQC への移行に着手する必要があると考えられる。

第２章　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

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」[60]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

[58] 例えば、素因数分解が困難な巨大な素数の積を利用したＲＳＡ暗号や、容易に逆算できない楕円曲線上の離散対数問題を利用した楕円曲線暗号といったもの。

[59] National Cyber Security Centre (NCSC)「Timelines for migration to post-quantum cryptography」(2025 年３月 20 日)、The White House「National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems」(2022 年５月４日)、The White House「Sustaining select efforts to strengthen the nation's cybersecurity and amending Executive Order 13694 And Executive Order 14144」(2025 年６月６日) 等を参照されたい。

[60] 金融庁「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」、https://www.fsa.go.jp/singi/pqc/index.html

号への対応に関する検討会報告書」（以下、「報告書[61]」という。）として公表している（同年 11 月）。

報告書の主要メッセージは以下の８点である。金融機関においては、報告書を参考に、IT ベンダーと協力しながら、自社運用のシステムだけでなく、運用を委託している重要システムに関するインベントリの作成を含め、可能な限り早期に移行に着手すべきである。

① 金融機関は、まず、自らの情報資産を網羅的に把握した上で、それぞれの情報資産の重要性を評価し､どのような暗号が用いられているかをリスト化したインベントリ（台帳・目録）を作成すること
② その際、自らが運用するシステムだけではなく、サードパーティに運用を委託している重要システムの情報資産と暗号に関するインベントリも作成すること
③ インベントリの作成作業にはかなりの労力を要するので、早い段階から IT ベンダーの協力を得ること
④ インベントリに基づき、量子コンピュータが実現すると脆弱性にさらされる情報資産のうち、影響が大きいシステムから順に PQC への移行を進めること
⑤ 検討の開始から移行までの一連の作業に関して、ロードマップを作成すること
⑥ 実務的には大規模システム更改などに合わせて PQC への移行を進めることを踏まえると、量子コンピュータの実用化（30 年代半ば）までに残された時間は少ないため、速やかに移行への対応を開始すること
⑦ PQC 自体も脆弱性が明らかとなる恐れがあるため、特定の暗号に固定することを前提とするのではなく、それが脆弱になった場合に暗号を差し替えやすいシステムにしておく、いわゆるクリプト・アジリティを確保しておくこと
⑧ 移行には長い期間と多くの経営資源の投入が必要であるため、経営陣の強いコミットメントが求められること

以　上

[61] 金融庁「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」、https://www.fsa.go.jp/singi/pqc/houkokusyo.pdf