

金融機関のシステム障害に関する 分析レポート

2024 年 6 月

第1部	はじめに	1
第2部	障害分析概要	3
第1章	集計期間	3
第2章	主な障害傾向	3
第1節	サイバー攻撃・不正アクセス等の意図的なもの	6
Ⅰ	マルウェア感染に係る事案	6
Ⅱ	DDoS 攻撃に係る事案	6
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	7
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	7
Ⅰ	冗長構成が機能しない等の障害	7
Ⅱ	システム障害発生時の復旧に関する不芳事案	8
Ⅲ	記憶領域の確保不足による障害	8
Ⅳ	取引量増加に起因する障害	8
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	9
Ⅰ	設定ミス・作業の誤り	9
第3章	今後の金融庁の対応	9
第1節	サイバーセキュリティ管理態勢に関するモニタリング	9
第2節	システム障害の発生を踏まえたモニタリング	10
第3節	システム統合・更改等に関するモニタリング	10
第3部	事例集	11
第1章	業態全体の障害傾向（事象別）	11
第2章	事例	12
第1節	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	12
第2節	システム統合・更改に伴い発生したシステム障害	23
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	36
Ⅰ	ハードウェア・回線等の不具合	36
Ⅱ	設定ミス・操作ミス等の管理面・人的要因	45
Ⅲ	サードパーティの提供するサービス等の要因	57
Ⅳ	取引量増加に伴う容量不足等	63
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	67
Ⅰ	設定ミス・操作ミス等の管理面・人的要因	67
Ⅱ	ソフトウェアの不具合	74
第5節	システム障害後の対応が円滑に行われた事例	79
別紙1	コラム：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）の好事例及び課題	82
別紙2	コラム：オペレーショナル・レジリエンスに係る金融機関との対話等の概要	85

第1部 はじめに

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」を受領するとともに、金融機関に対し障害の復旧状況の確認やヒアリング等を行い、金融機関で分析・検討した障害の真因、事後改善策の報告を受けている。これらの報告等に基づく分析結果や事例をまとめ、2019年以降、「金融機関のシステム障害に関する分析レポート」（以下、「分析レポート」という。）として公表している。

近年、金融機関のITシステムの複雑化、ITシステムの委託関係の複雑化、サイバー攻撃の高度化等により、多くの顧客に影響を及ぼす事案が発生している。

昨年も、資金清算機関にてシステム障害が発生し、為替業務が一部金融機関で不能となり、復旧にも時間を要した事案が生じた。

こうした状況の下、金融機関は、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。）管理態勢を強化する必要があるが、特に、障害の未然防止にとどまらず、障害発生時の重要業務の継続、業務の早期復旧及び顧客影響の軽減（以下、「ITレジリエンス」という。）の強化を図ることがより一層求められている¹。

本レポートでは、障害の端緒ごとに障害事例を分類し、代表的な事例について、発生した事象、障害の原因、再発を防止するうえで取り組むべき課題について分析している。昨年と同様に、今回のレポートでは、ITレジリエンス強化の参考となるよう、障害対応等の好事例も記載した²。

金融機関においては、本レポートに加え、サイバーセキュリティを含むシステムリスク管理に関する各種標準、ガイドライン等³を参照し、自組織の体制及び対策について見直し、求められるITセキュリティ又はITレジリエンスとの差異を特定し、解消することが望ましい。

留意事項

¹ 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』の一部改正（案）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/20230427-2.html>）。

² 第3部第2章第5節参照。

³ 公益財団法人金融情報システムセンター「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」（2024年3月、<https://www.fisc.or.jp/publication/book/006241.php>）及び「金融機関等のシステム監査基準」（2019年3月、<https://www.fisc.or.jp/publication/book/003929.php>）、情報システムコントロール協会「Control Objectives for Information and related Technology」（<https://www.isaca.org/resources/cobit#1>）、経済産業省「システム管理基準」（2023年4月26日、<https://www.meti.go.jp/policy/netsecurity/sys-kansa/sys-kanri-2023.pdf>）、「システム監査基準」（2023年4月26日、<https://www.meti.go.jp/policy/netsecurity/sys-kansa/sys-kansa-2023r.pdf>）及び「サイバーセキュリティ経営ガイドライン Ver. 3.0」（2023年3月24日、https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf）、米国立標準技術研究所「重要インフラのサイバーセキュリティを向上させるためのフレームワーク」（2018年4月16日、<https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>）等。

本レポート第3部事例集は、2018年7月から2024年3月までに報告された「障害発生等報告書」のうち、主な事案を取りまとめたものであるが、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2部 障害分析概要

第1章 集計期間

金融機関のシステム障害については、法令、監督指針等に基づき、金融機関から障害発生等報告書を受領しているが、第2部は2023年4月から2024年3月までに受領したものを分析したものである。

第2章 主な障害傾向

前回のレポートでは、2022年度の主な障害傾向として、以下の点を挙げていた。

- ・ 外部委託先のシステムへの外部からの不正アクセスにより、大量の顧客情報が漏えいするといった重大なインシデントが発生した。
- ・ サポート期限切れの機器を使用したことに起因した脆弱性に対する外部からの不正アクセスによるランサムウェア被害や、なりすましメールに添付されたファイルを開封したことにより、エモテットに感染する事案が発生した。
- ・ 外部委託先を含む金融機関へのDDoS攻撃により、金融機関のホームページの閲覧ができなくなる等の事案が発生した。
- ・ データセンターの障害によるシステムの全面停止や、地域金融機関の共同センターの障害により、同時に複数の金融機関で障害が発生する等、多くの顧客に影響が及んだ。
- ・ 2021年度と同様に、障害発生時に準備していたシステムの冗長構成が機能せず、復旧に想定以上の時間を要した。
- ・ 障害発生時に、顧客対応を迅速に行う等の好事例も認められたが、2021年度と同様に、障害発生時の障害復旧手順・体制の整備が不足（人材不足を含む。）し、復旧に時間を要した。

上記の傾向から、2022年度においては、

- ・ サイバーインシデントについては、外部委託先への不正アクセスによる顧客情報の漏えいが発生していること、外部委託先を含む金融機関へのDDoS攻撃により、金融機関のホームページの閲覧ができなくなる事案が発生していること等から、重要な外部委託先も含めたサイバーセキュリティ対策等の整備状況の把握及びその実効性の検証といったITレジリエンスの向上が必要であることが課題となっていた。
- ・ また、IT資産の適切な管理や不審メール受信時の対応といった基本的な対策を実施するための態勢整備が引き続き課題となっていた。
- ・ システム障害（サイバーインシデントを除く。）関連については、障害発生時に、顧客対応を迅速に行う等の好事例も認められ、金融業界において障害対応への意識が高まっている面も垣間見えたが、他方、引き続き、障害復旧に関する不芳事案も認められた。

- ・ サイバーインシデントやシステム障害（サイバーインシデントを除く。）関連の障害傾向から、経営陣がサイバーセキュリティを含む IT レジリエンスの強化（重要な外部委託先を含む。）を主導すること、その下で、経営上の計画における施策を策定するとともに実施すること、必要なリソース（予算及び人材）を確保するとともに適切に配置すること、インシデント対応においては顧客目線での対応、インシデントの影響の最小化、重要業務の早期復旧等を実現させるための態勢整備を行うことが課題となっていた。

2023 年度の主な障害傾向としては、以下の点が挙げられる。

- ・ 外部委託先が管理する 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るランサムウェア感染により、外部委託先が提供するサービスを金融機関が利用できなくなる事案や、ファイル転送ソフトウェアの脆弱性を悪用した不正アクセスによるマルウェア感染により、金融機関の従業員の個人データが流出する事案、外部委託先の従業員の PC がマルウェアに感染したことにより、社内システムに対して不正アクセスが行われて、大量の情報漏えいに繋がった事案が発生した。
- ・ 外部委託先が提供するクラウドサービスを利用する他企業への DDoS 攻撃により、同サービスを利用する金融機関のインターネットバンキング（以下、「IB」という。）のシステムが長時間にわたって利用不可となる事案や、金融機関への DDoS 攻撃により、スマートフォンアプリを用いた顧客の決済ができなくなる事案が発生した。
- ・ 資金清算機関のシステム更改において、委託元における外部委託先でのレビュー体制・テスト内容の確認等が十分でなかったことや、外部委託先に対する牽制が十分でなかったこと等に起因して、為替業務で必要となる金融機関名に係るテーブルが正しく作成されず、為替業務が一部金融機関で不能となる事案が発生した。また、プロジェクト固有のリスクを踏まえた業務継続計画（以下、「BCP」という。）が整備できていなかったことや、大規模障害を想定した危機管理体制が十分に整備されていなかったことにより、障害復旧対応に時間を要し、多くの顧客に影響が及んだ。
- ・ 2022 年度と同様に、障害発生時に準備していたシステムの冗長構成が意図どおり機能せず、復旧に時間を要する事案が発生した。
- ・ システム障害発生時の復旧に関する不芳事案の新たな傾向として、障害原因を調査するための情報不足により、障害原因の特定に時間を要したことで、復旧に時間を要する事案が発生した。
- ・ スマートフォン等を利用した金融サービスの利用増加に伴う取引量の増加により、取引処理が必要とする記憶領域の確保不足に起因して、決済等のサービスが利用不可となる事案が発生した。また、キャンペーン等による取引量増加に伴うシステム処理能力不足に起因して、決済等のサービスが利用不可となる事案が発生した。

- ・ 勘定系システムのメンテナンス時間を利用したテスト終了後に、作業誤りに起因して、ATM の電源を切断したことにより、翌日、全 ATM が利用不可となる事案が発生した。また、データセンターでの点検作業時に、作業手順書の誤りに起因して、計画と異なる電源を遮断したことで、決済等のサービスが利用不可となる事案が発生した。

上記の傾向から、2023 年度においては、

- ・ サイバーインシデントについては、外部委託先が管理する 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、ランサムウェアに感染して外部委託先が提供するサービスが利用できなくなる事案が発生していること等から、脆弱性に係る最新情報の把握やパッチ適用の徹底、不正な通信を検知するためのシステム・体制の整備等のマルウェア対策の整備はもとより、重要な外部委託先のサイバーセキュリティ管理態勢のリスク評価実施や強化をすることが課題となっている。
- ・ 外部委託先を含む金融機関への DDoS 攻撃により、長時間にわたって IB 利用や一部の決済ができなくなる事案が発生していること等から、DDoS 攻撃の軽減対策の強化や、DDoS 攻撃の早期検知・復旧のための態勢を整備することが課題となっている。
- ・ システム障害（サイバーインシデントを除く。）関連については、過去のシステムの稼働実績を過信することなく、外部委託先の開発におけるレビュー体制の適切性の確認、試験内容の十分性の確認等による外部委託先管理の強化や、プロジェクト固有のリスクを踏まえた BCP の整備、大規模障害を想定した危機管理体制の整備が課題となっている。
- ・ 冗長構成が意図どおり機能するよう実効性を確保することや、障害発生時の業務継続に係る代替手段の整備が課題となっている。また、新たな傾向として、障害原因の特定に時間を要したことから、原因分析に必要な情報の把握や、情報取得手段の確保に予め備えておくことが課題となっている。
- ・ スマートフォン等を利用した金融サービスの利用増加に伴う取引量の増加による記憶領域の確保不足や、システム処理能力不足に対して、記憶領域の使用状況の監視やシステム処理能力の事前検証が課題となっている。
- ・ 作業の誤りや作業手順書の誤りに対して、本番環境を操作することによるリスクを軽視することなく、作業手順書の確認強化や作業実施体制の強化をすることが課題となっている。
- ・ サイバーインシデントやシステム障害（サイバーインシデントを除く。）関連の障害傾向から、改めて障害が発生するという前提に基づき、経営陣がサイバーセキュリティを含む IT レジリエンスの強化（重要な外部委託先を含む。）を主導すること、その下で、経営上の計画における施策を策定して実施すること、特に、サイバーインシデント対応やシステム障害対応においては顧客目線での対

応、インシデントの影響の最小化、重要業務の早期復旧等を実現させるための態勢整備を行うことが引き続き金融業界の重要な課題となっている。また、資金清算機関のシステム障害から、システム障害が発生した場合に備えて、プロジェクト固有のリスクを踏まえた BCP を整備するとともに、訓練による実効性の確保が重要であることが窺える。

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取りまとめ、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

I マルウェア感染に係る事案

以前の分析レポートでは、金融機関、その海外現地法人等において、マルウェアに感染した事案を取り上げた。2023 年度においては、外部委託先が管理する VPN 機器の脆弱性を悪用したと考えられる外部からの不正アクセスにより、ランサムウェアに感染し、外部委託先が提供するサービスを金融機関が利用できなくなる事案や、ファイル転送ソフトウェアの脆弱性を悪用した外部からの不正アクセスによってマルウェアに感染し、金融機関の従業員の個人データが流出する事案、外部委託先の従業員の PC がマルウェア感染し、社内システムに対する不正アクセスにより、大量の情報漏えいに繋がった事案が発生している。

これらの対応として、脆弱性に係る最新情報の把握と脆弱性に対するパッチ適用の徹底、不正な通信を検知するためのシステム・体制の整備や、不正な外部サーバーとの通信制御といったマルウェア対策の整備はもとより、重要な外部委託先のサイバーセキュリティ管理態勢のリスク評価実施や強化が課題となっている。

II 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 攻撃と思われるサービス不能攻撃が発生している。特に、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も影響を受けて IB が長時間利用できなくなる事案や、DDoS 攻撃により、スマートフォンアプリを用いた決済ができなくなる事案が発生している。

これらの対応として、アクセス制限や DDoS 対策ツール⁴の導入といった基本的な対

⁴ 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 IPS（不正を検知して通信を遮断するシステム。「Intrusion Prevention System」の略。）といったツール。

策はもとより、攻撃元に対するブロック対応の高度化⁵や、DDoS 攻撃の早期検知・復旧のための態勢を整備することが課題となっている。

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た。

こうした状況の下、昨年、資金清算機関のシステム更改において、委託元において、外部委託先でのレビュー体制・テスト内容の確認等が十分でなかったことや、外部委託先に対する牽制が十分でなかったこと等により、為替業務で必要となる金融機関名に係るテーブルが正しく作成されず、為替業務が一部金融機関で不能となるとともに、障害復旧対応に時間を要したことにより、多くの顧客に影響を及ぼす事案が見られた。

こうしたことから、外部委託先のレビュー体制・テストの実施状況の把握や、外部委託管理の強化、再委託先を含むリスク評価・管理の強化等を行うことが課題となっている。

また、プロジェクト固有のリスクを踏まえた BCP が整備されていなかったことや、大規模障害時の危機管理体制が整備されていなかったことにより、障害復旧対応に時間を要したことから、プロジェクト固有のリスクを踏まえた BCP の整備や、大規模障害を想定した危機管理体制の整備と訓練による実効性の確保が課題となっている。

さらに、課題解決を図るために必要な IT 人材の確保や第三者目線によるチェック強化が課題となっている。

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

I 冗長構成が機能しない等の障害

これまでに公表した分析レポートでは、障害に備えた冗長構成が意図どおりに機能しない障害について取り上げたが、2023 年度も同様の事案（ハードウェア障害が発生したにもかかわらず副系に切り替わらなかった事案等）が認められた。

例えば、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が認められた。また、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、

⁵ 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。

勘定系システムに係る全ての取引が不可となる事案が認められた。

こうしたことから、冗長構成が意図どおりに機能するよう実効性の確保や、冗長構成が機能不全を起こすような不具合へのパッチについて、適切な管理を行うことが課題となっている。

Ⅱ システム障害発生時の復旧に関する不芳事案

以前の分析レポートでは、外部委託先が運営するデータセンターの電源故障によるシステム停止や、地域金融機関の共同センターの障害により、複数の金融機関において、同時に障害が発生し、復旧手順の未整備や復旧対応を行う有識者の不足等により、復旧までに想定以上の時間を要した事案を取り上げた。

2023 年度においては、新たな傾向として、サーバーの処理能力が一時的に低下し、スマートフォン等による決済等サービスが利用不可となる障害が発生した際に、原因特定に必要な情報が取得できていなかったことから、原因特定に時間を要した事案や、データベースサーバーへのアクセスが不安定となり、レスポンスの大幅な遅延が発生し、バーコード決済が不可となった際に、データベースサーバーの再起動により、一時的に復旧したものの、障害の原因特定に至っていなかったことから、障害が再発した事案が見られた。

こうしたことから、一時的に復旧した場合でも障害原因の特定を実施することはもとより、インシデント対応態勢の整備や、障害原因を早期特定するため、予め障害事象の原因分析に必要な情報の把握、情報取得手段の確保しておくことが課題となっている。

Ⅲ 記憶領域の確保不足による障害

デジタルバンキングの利用増加に伴い、取引処理が利用する記憶領域が不足したことに起因して、サーバーの処理能力が一時的に低下し、アプリ等による決済等のサービスが利用不可となる事案が発生した。

こうしたことから、記憶領域の使用状況を把握し、適時対策を実施するための監視を強化することが課題となっている。

また、記憶領域不足による障害は、システムの処理能力低下や処理停止により、決済等サービスの利用不可といった顧客に影響を及ぼすことがあることから、記憶領域の確保に係る設定については、十分な確認や検証が必要である。

Ⅳ 取引量増加に起因する障害

スマートフォン等を利用した金融サービス利用の普及に伴い、スマートフォン等で利用するアプリケーションにて作成される決済用の QR コードやバーコードを表示して決済を行う顧客が増加している。

こうした状況の下、キャンペーン等によって顧客の利用が集中したことにより、システムの処理能力が不足したため、決済アプリへのログイン不可や QR コード等を用いたチャージ及び決済が行えず、顧客に影響を及ぼす事案が発生した。

こうしたことから、顧客の利用量増加を踏まえたシステムの処理能力設計に係る品質強化や、システムの処理能力の事前検証による実効性の確保が課題となっている。

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

I 設定ミス・作業の誤り

勘定系システムのメンテナンス時間帯を利用したテスト終了後、手順書に記載がない ATM の電源切断を担当者のみの判断で誤って行ったことに起因して、翌日、ATM がサービス開始時間になっても起動せず、全 ATM が長時間にわたって利用不可となる事案が発生した。また、データセンターの電源点検作業時に、作業手順書の誤りに起因して、計画とは異なる電源を遮断したことにより、チャージ等の一部のサービスが利用不可となる事案が発生した。

こうしたことから、ATM の電源に係る作業やデータセンターの電源点検作業等の本番システムに影響する作業を行うことによるリスクを軽視することなく、作業手順書の確認強化や作業実施体制の強化が課題となっている。

第3章 今後の金融庁の対応

金融機関は、創意・工夫をもって、サイバーセキュリティを含めたシステムリスク管理態勢を強化する必要があるが、特に、サイバーインシデントやシステム障害の未然防止にとどまらず、IT レジリエンスの強化が一層求められている。

金融庁としては、金融システムの安定及び利用者保護の観点から、以下のとおり、検査・モニタリングを通じ、サイバーセキュリティを含む金融機関のシステムリスク管理態勢の強化を促していく。

第1節 サイバーセキュリティ管理態勢に関するモニタリング

昨今、サイバー攻撃の高度化・巧妙化により、金融機関において、大規模な顧客情報の漏えい、顧客資産の不正出金及びランサムウェア攻撃によるデータの暗号化・業務の停止といった重大なインシデントが発生している。こうしたサイバーリスクのすう勢を踏まえ、引き続き、金融機関のサイバーセキュリティ管理態勢の実効性⁶について検査を通じて検証するとともに、地域金融機関、証券会社、保険会社等に対しては、

⁶ 実効性を検証する有効な手法として脅威ベースのペネトレーションテスト（TLPT）が挙げられる。TLPT の好事例及び課題については、別紙 1 「コラム：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）の好事例及び課題」参照。

サイバーセキュリティに関する自己評価の実施を求める。加えて、金融業界横断的なサイバーセキュリティ演習を実施し、金融業界のインシデント対応能力の向上を図る。

第2節 システム障害の発生を踏まえたモニタリング

IT・デジタル技術の進展とともに、金融機関はITシステムへの依存度を高めており、商品・サービスが拡大し、ITシステムが益々複雑化する中、外部委託への依存度も高めている。こうした状況の下、システムリスクはさらに多様化しており、大規模なシステム障害が頻繁に発生する事態になれば、金融機関に対する信頼が揺らぎかねない。そのため、金融機関におけるシステムリスク管理の重要性は一層高まっている。

金融庁では、重大な顧客被害の発生や金融機関のシステムリスク管理態勢（外部委託先を含む。）に重大な問題が認められる場合、機動的に検査・モニタリングを行い、その実態を検証し、金融機関に改善を促している。今後もこうした取組を継続するとともに、2023年4月に公表した「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」⁷に基づく対話⁸を進めていることから、障害の未然防止にとどまらず、利用者目線に立った早期復旧や影響範囲の最小化が図られるよう、金融機関にオペレーショナル・レジリエンスの取組を促していく。

第3節 システム統合・更改等に関するモニタリング

金融機関の経営統合、経営戦略・IT戦略を踏まえた利用共同システムの変更などに伴い、複数の金融機関において、システム統合、システム移行等の大規模かつ難度が高いプロジェクトが進められている。

金融庁では、こうした金融機関のシステム統合・移行に係るモニタリングにおいて、進捗状況等の実態を把握の上、過去の事例も踏まえて、問題となりやすい事項を検証・議論することとしており、対話を通じて金融機関の自律的な改善を促している。

今後もこうした取組を継続するとともに、リスクが高いと考えられるプロジェクトに対しては、検査を行うほか、計画段階から対話を行うことや、集中ヒアリングなどを通じて深度ある検証を行うことなどにより、リスクに応じた効果的かつ効率的なモニタリングを進めていく。

⁷ <https://www.fsa.go.jp/news/r4/ginkou/20230427.html>

⁸ 別紙2「コラム：オペレーショナル・レジリエンスに係る金融機関との対話等の概要」参照。

第3部 事例集

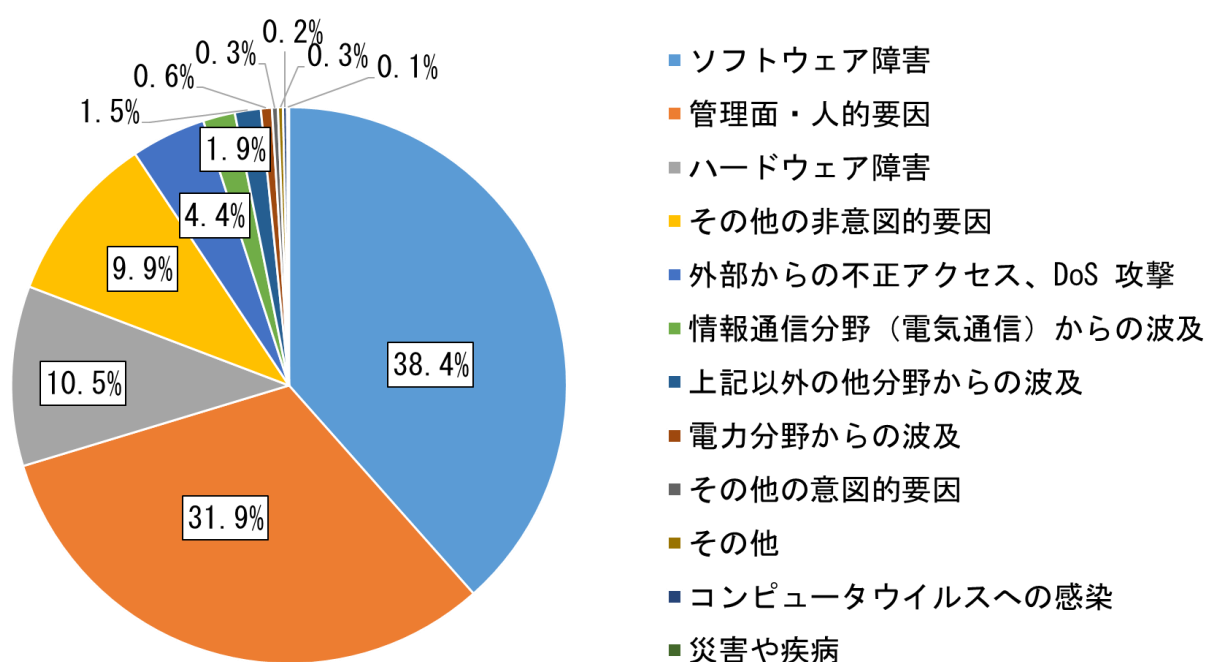
第1章 業態全体の障害傾向（事象別）

2023年度の業態全体⁹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¹⁰。

「ソフトウェア障害」による障害について、設計時の考慮不足により、誤った仕様の下でプログラムを作成し、IB利用や決済が不可となる事案、レビューの観点の網羅性が不十分なものとなり、プログラムの誤りを検出できず、その結果、二重振込や入金金先が誤って取り引きされる事案が報告されている。

「管理面・人的要因」について、本番環境の運用・保守作業時に、本番環境を操作することのリスクを軽視し、担当者の単独作業となり、作業結果の再鑑を行う体制を構築していなかったことにより、ATMの停止や決済が不可となる事案が報告されている。また、外部委託先のレビュー体制が不十分であったため、プログラムの修正誤りや作業手順書の記載誤りが発生し、その結果、長時間にわたりサービスの利用が不可となる顧客に大きな影響を及ぼす事案が報告されている。

図表1 「障害事象別割合（全業態）」



⁹ 本集計期間（2023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1,900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）。

¹⁰ 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、2024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 事例

システム障害の事例については、2019 年以降公表しているが、本事例についてこれまで公表した主な事例を障害発生の端緒別等に整理した上で¹¹、前回公表時に取りまとめた以降に発生した障害事例を追加（初めて掲載した事例には「新規」と表示）したものである。

第1節 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サービス停止「新規」

<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 ASM¹²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

2 マルウェア感染による個人データ流出「新規」

<業態>

金融商品取引業者等

¹¹ 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。

¹² サイバー攻撃の対象となりうる IT 資産や攻撃経路を把握・管理する取り組みや技術。「Attack Surface Management」の略。

＜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¹³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）

3 DDoS 攻撃による決済不可新規

＜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¹⁴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）

4 外部委託先が提供するサービスへの DDoS 攻撃新規

＜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

¹³ 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中で、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

¹⁴ 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。

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

5 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。

＜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

6 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

7 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

8 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

9 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

10 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

11 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

12 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

1 3 開発環境に対する不正アクセス

＜業態＞

主要行等

＜事象＞

- 外部委託先がパブリッククラウド上に構築した開発用サーバーにおいて、リモートアクセスするための接続箇所に、悪意をもった第三者から不正アクセスされランサムウェアに感染した。

＜原因＞

- ◆ 接続箇所の認証方法が ID・パスワードのみであり、総当たりの解析を行われ特定された。

＜対策＞

- 開発環境のリモートアクセスに関するセキュリティ対策（二要素認証や端末認証等）のルール徹底

1 4 脆弱性情報の収集およ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つ

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

15 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

16 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＞

- インターネットを經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¹⁵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¹⁶に感染した。

¹⁵ 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。

¹⁶ 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。

<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

17 悪意のある第三者からの不正アクセスによる顧客資産の流出

<業態>

金融商品取引業者等

<事象>

- 身に覚えのない取引があったとの顧客からの申し出を端緒に、悪意のある第三者による不正アクセスにより顧客資産が流出したことが判明した。悪意のある第三者は、何らかの方法で取得したログイン ID やパスワード等の情報を用いて、証券会社 Web サイトで出金先銀行口座等を不正な銀行口座に変更した上で出金を行った。

<原因>

- ◆ ログイン ID やパスワードが不正入手されたことを前提とした対策が不足していた。

<対策>

- 不正アクセス（不正ログイン）に対するモニタリングの強化
- 本人認証の強化

18 外部委託先従業員による不正送金

<業態>

金融商品取引業者等

<事象>

- 外部委託先の従業員が不正取得した認証情報を使い、委託元の証券会社の顧客資産の売却を行い、その売却金等を不正に取得した。当該職員は、業務上付与された権限を不正に使用し、顧客 ID やパスワード等を不正に取得していた。

<原因>

- ◆ 悪意のある内部不正を前提とした権限管理やモニタリングが不足していた。

<対策>

- 権限管理及びモニタリングの強化
- 外部委託先の管理強化

19 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。

<対策>

- 最新の事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

20 スマホ ATM 機能の悪用に関する不正アクセス

<業態>

貸金業者

<事象>

- フィッシングサイト等を経由して窃取された会員のスマートフォンサイトの ID・パスワード等の情報をもとに、スマホ ATM 機能を悪用されキャッシングされた。

<原因>

- ◆ 顧客の秘匿情報が漏えいしたことを想定した対策が不足していた。

<対策>

- 多要素認証等の実効性ある認証方式の採用
- 取引発生時等に真の利用者に対する通知機能の実装
- 不正取引等に対するモニタリングの強化

21 パブリッククラウドサービスのバージョンアップに起因した個人情報等の

不正アクセス

<業態>

資金移動業等

<事象>

- パブリッククラウドサービスのアクセス権の設定不備により、悪意の第三者が、収集された個人情報等に不正アクセスできる可能性があった。

<原因>

- ◆ パブリッククラウドサービスのバージョンアップ時、アクセス権限の見直しの必要性を理解していなかった。
- ◆ パブリッククラウドサービス導入時のリスク評価が未実施であった。

<対策>

- パブリッククラウドサービス利用時の管理態勢の強化
- 有識者によるアクセス権限設定の確認（必要に応じて第三者機関によるセキュリティ評価・脆弱性診断の実施）

2.2 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

2.3 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節 システム統合・更改に伴い発生したシステム障害

1 メモリ領域不足に起因した為替取引不可^{新規}

<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¹⁷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不十分であった。
- ◆ 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

¹⁷ 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

<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）の妥当性検証が不十分であった。
- ◆ 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不十分であった。
- ◆ 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对外告知等の対応事項の整備が不十分であった。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、障害対応力が不十分であった。

<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对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。

2 長期間にわたるシステム停止による ATM 非稼働新規

<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。

3 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

4 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

5 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

6 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

7 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

8 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

9 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

10 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の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

1 1 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

1 2 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

13 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

14 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より起因して、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

15 大規模プロジェクトに係る知見、経験等の不足による ATM 停止及び残高情報 の誤更新

<業態>

主要行等

<事象>

- ATM 取引不能及び勘定不整合が発生した。

<原因>

- ◆ 勘定系システムと ATM の間で発生したネットワーク障害（障害に対する考慮不足によりネットワークのログを保存していなかったため詳細不明）により勘定系システムからの応答（下り電文）が ATM へ届かなかったため、取引が不能となった。
- ◆ ネットワーク障害が発生し応答が正常にできていないことを検知していたにもかかわらず、勘定系システム内では ATM から続々と要求され続ける取引（上り電文）の処理を続けたため、取引が完結していないにもかかわらず勘定系システム内の残高情報が更新された。

<対策>

- 重要システムでの障害発生時に原因を正確に特定するため、ログの保存を開始
- ネットワーク障害を検知した場合には即時に取引を停止し再起動するよう勘定系システムを改修

16 システムリスク管理態勢の整備不足によるサービス停止

<業態>

主要行等

<事象 1>

- 新システム稼働後、大量の処理に伴うサーバーリソースの高負荷、データロック（滞留）の長期化が発生し、IB やデビット機能、ATM 取引が利用不可となった。

<原因 1>

- ◆ システム開発時に想定した以上のトランザクション件数が発生した。
- ◆ システム開発時におけるパフォーマンスやキャパシティに係るテストが不足していた。

<対策1>

- サーバーリソースの高負荷を回避するようシステムレスポンスを改善
- 長時間のデータロックを回避するよう処理ロジックを変更
- サーバーの高負荷を防止するよう商品ルールを変更し、アプリケーションを改修

<事象2>

- 勘定系データベースサーバーがダウンし、ATMで取引エラーが発生した。

<原因2>

- ◆ 基本ソフトウェアの不具合により、勘定系データベースサーバーがダウンした。また、待機系への手動切替え手順の認識（手順実施の必要性、関連ドキュメントの所在等）不足により対応が遅れ、サービス回復までに時間を要した。

<対策2>

- 基本ソフトウェアのバージョンアップ
- 障害対応態勢の整備（知識の共有を含む）
- 障害対応に係るドキュメントの参照環境の整備（検索性向上等）

<事象3>

- 各種処理の実行タイミングの競合等により、他行宛振込や定額自動振込の実行不可、デビット機能の利用不可が発生した。

<原因3>

- ◆ 各種処理（オンライン取引・バッチ処理・顧客操作等）やデータの影響範囲・利用範囲の把握が十分ではなく、処理の競合に係る考慮が漏れており、テストが不足していた。

<対策3>

- 網羅的なテストケース設定のためのドキュメント（システム関連図等）の作成
- オンライン取引等の競合防止のための禁止事項・ルールの整備

<事象4>

- 他行宛振込実施時に、複数行の特定支店が振込先として表示されない障害が発生した。また、データパッチ¹⁸により対処を実施したところ、振込画面に遷移するとシステムエラーとなる2次障害が発生した。

¹⁸ 「データパッチ」とは、不具合の修正を行うために、データベースに適用し、一部の更新データをデータベースに適用すること。

＜原因４＞

- 支店の住所変更等に係る日付のプログラム誤りにより、当該特定支店が無効となっていた。
- データパッチ適用作業実施時のルールが未整備であり、再鑑も行われていなかった。

＜対策４＞

- チェックリストに日付や曜日の観点を加え、設計レビューやテスト等を実施
- 本番環境におけるデータパッチ適用等の作業時のルールを整備し、上長による承認フローを徹底

１７ システム更改時の設計漏れに起因する被仕向送金障害

＜業態＞

地域銀行

＜事象＞

- 被仕向送金のうち、一部振込に関して、振込資金の入金遅延・仕向銀行への資金の誤返却する障害が発生した。

＜原因＞

- ◆ 受取人口座番号の変更処理プログラムの誤りで、口座番号相違となった。
- ◆ 設計担当者・レビュー担当者双方の被仕向為替における口座番号変換処理仕様に関して理解が不足しており、口座番号の桁数バリエーションまで含めたテストケース設定ができていなかった。

＜対策＞

- 業務機能・システム処理方式に関する設計ドキュメントの整備
- 周辺システムを意識した勘定系システムの設計レビュー、テスト等の充実

１８ コアタイムからモアタイム切替え遅延に伴う為替未送信

＜業態＞

地域銀行

＜事象＞

- 障害発生時間帯（約 15 分間）に受け付けた他行宛振込が全銀センターでエラーとなり、当行内に滞留、為替未送信となる事象が発生した。

＜原因＞

- ◆ 修正プログラムをリリースした際、為替送信処理ステータスがエラーとなり、同時時間帯に受付した他行宛振込が滞留した。
- ◆ 運用担当者における修正プログラムの反映タイミングの理解や経験が不

足していた。

<対策>

- 周辺システムを意識した勘定系システムの設計レビュー・テスト等の充実

19 新旧システムの特性等に対する考慮不足による誤った引落し

<業態>

地域銀行

<事象>

- 新旧システムの機能差異の比較不足のため、誤って口座引落としされる事象が発生した。

<原因>

- ◆ 解約等によって口座引落としを行わない明細の扱いが新旧システムで異なることを、設計時やデータ移行時に新旧比較や有識者レビューの不足のため認識できなかった。

<対策>

- 設計時の新旧システムの各有識者による相互レビューの徹底

20 プログラムの修正漏れによる振込不可

<業態>

信用金庫・信用組合等

<事象>

- IB や ATM 等から振込を行う際の取引電文を書き出す為替発信用ファイルに関するプログラムに修正漏れがあり、先日付振込が当初予定の期日に行われない事象が発生した。

<原因>

- ◆ システム開発時における先日付振込を含むテストケースが不足していた。

<対策>

- IB や ATM 等を含む対外接続に係る開発において、オンラインで作成されるデータ、センターカットにて作成されるデータ等テストケースを網羅的に洗い出した上でテスト実施

21 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

I ハードウェア・回線等の不具合

1 障害原因未特定による障害の再発新規

<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

2 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新規

<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

3 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

4 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

5 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

6 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

7 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

8 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

9 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＞

- リカバリ対応が完了するまでの間の影響把握、復旧手順の整備

10 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出来なかった。

＜対策＞

- ネットワーク機器故障の予兆検知実施

11 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

1 2 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、对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）

1 3 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もとづく予兆管理の徹底

1 4 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

15 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もとづく対応手順の整備と訓練の実施

16 電源供給停止に伴う通信障害による ATM 等の利用不可

＜業態＞

主要行等

＜事象＞

- 台風の影響で回線を収容する通信会社の収容局に対する電力供給が途絶え、加えて非常用電力の枯渇によって通信障害が発生した際、利用回線を経由したサービスが停止する事象が発生した。

＜原因＞

- ◆ 利用回線は冗長構成であったが、正副回線とも同一地域を通過しており、広域で電力供給が途絶えたことで冗長構成が機能しなかった。

＜対策＞

- 正副回線が切断された場合の CP の準備とともに、通信障害リスクの低減に向けたキャリア分散による冗長構成の見直し

17 電源喪失に伴う勘定系システム停止

＜業態＞

主要行等

＜事象＞

- 勘定系システムを設置しているデータセンターにおいて、メンテナンス作業時の電源機器の障害で電源供給が絶たれたことによって、勘定系システムが停止、併せて関連するサーバーのハードウェアも故障する事象が発生した。また、待機系サイトへの切替え判断や作業にも時間を要した。

＜原因＞

- ◆ 外部委託先での電源設備の保守点検作業の手順に不備があった（単一障害点のある手順となっていた）。
- ◆ 必要なメンバーの招集から障害対応までを対象とした災害対策サイトへの切替え訓練を行っていなかった。

＜対策＞

- 保守点検作業においても、単一障害点が発生しない電源設備への移行
- 切替え決定からの必要メンバーの招集や作業ドキュメントの準備等のより実態に即したシステム切替え訓練の実施

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

19 ハードウェアの障害による終日株式売買の停止

<業態>

証券取引所

<事象>

- 共有ディスク装置のメモリに故障が発生した際、冗長構成になっていたにもかかわらず、もう一つの装置に切り替わらず一部業務に異常が発生し、売買を停止せざるを得ない状況となった。
- 日中にシステムを再起動した場合の市場の混乱を懸念し、終日売買停止することとなった。

<原因>

- ◆ 故障した製品のマニュアルに不備があり、自動切替えがされない設定になっていた。また、当該設定に係る実際の稼働テストが不十分であった。
- ◆ システム障害による売買停止後の再開に向けたルールが整備されていなかった。

<対策>

- 冗長構成が正常に動作することの確認
- システム障害発生時の業務再開に向けた手順やルールの整備

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

Ⅱ 設定ミス・操作ミス等の管理面・人的要因

1 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^{新規}

<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

2 パッチ未適用により冗長機能が機能しない^{新規}

<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、主システムから副システムに切り替わったが、副システム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>

- ◆ 副システムに切り替わった際、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

3 業務時間帯で実施した保守作業による ATM 利用不可^{新規}

<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

4 設定誤りにより冗長構成が機能せずアプリ利用不可^{新規}

<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

5 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新規

<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

6 設定誤りにより冗長構成が機能せず取引不可新規

<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

7 システムへのデータ取り込み漏れ^{新規}

＜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、テスト内容が不十分であった。
- ◆ 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不十分であった。

＜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

8 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）

9 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值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

10 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

1 1 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

1 2 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

13 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

14 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＞

- ◆ リグレーションテスト¹⁹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ーションテストの確認観点到追加

15 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

¹⁹ 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

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

1 6 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

1 7 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

18 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

19 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）

20 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 にログインしづらい事象が発生した。

＜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

2 1 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

2 2 高負荷な検索作業に起因した IB におけるエラー出力

＜業態＞

主要行等

＜事象＞

- IB のデータベースに対する検索作業に起因して、IB に対するアクセスが高負荷となり約 3 時間断続的にエラーが発生した。
- 復旧作業のため対象サーバーを再起動した際に用いた手順書に不備があり復旧までに時間を要した。

＜原因＞

- ◆ 参照系の検索作業は開発及び運用組織による事前報告やテストを実施していなかった。
- ◆ 過去に実施したシステム変更時に手順書を改訂していなかった。

＜対策＞

- テスト環境による確認と開発及び運用組織による事前承認のプロセス徹底
- システム変更作業におけるレビュー時に、運用に対する影響確認や対応結果の確認をルール化

2 3 社内の他組織との連携不足に起因した IB アクセス不可

＜業態＞

主要行等

＜事象＞

- Web サイトに掲載する広告の定型的な登録作業で、外部委託先から提供された、誤りを含むプログラムを登録したことで IB にアクセスできない事象が発生した。また、対応にも時間を要した。

＜原因＞

- ◆ 登録作業において事前のテスト等を行わなかったため、プログラム誤りに気付くことができなかった。
- ◆ プログラムの登録作業を特定の部署のみで完結したため、障害対応を担当した関連部署が登録作業を認識できず、原因特定に時間を要した。

＜対策＞

- 登録作業に関する、検証やテストの手順確立
- 作業依頼からテストや本番作業等のプロセスにおける関連部署の役割を定義

2 4 各システム及び処理の連携・前後関係の認識不足によるサービス開始遅延

＜業態＞

主要行等

＜事象＞

- システムの定例保守作業における作業ミス起因とし、夜間バッチ処理が異常終了。異常終了した処理の復旧に関する手順を誤り、更に影響が拡大。その後の復旧に想定以上の時間を要し、顧客サービスの開始遅延等が生じたほか、通常作業と復旧作業を並行して行う必要から作業量が積み上がり、完全復旧までに相当な日数を要した。

＜原因＞

- ◆ 定例保守作業において作業順序を誤った。また、再鑑が不十分であり、再鑑者が作業順序相違を看過した。
- ◆ 一時的に抑止したシステムの再実行の管理が不十分であり、必須処理が漏れたままとなっていた。
- ◆ 影響範囲の広い大規模障害を想定した CP が策定されていなかった。

<対策>

- 作業手順書において作業工程を細分化、作業順序を明確化し、再鑑タイミングも細分化後の工程ごとに実施するよう変更
- 必須処理の漏れがシステムの的に検知できる機能の追加、一時的に抑止したシステムの再開時には開発及び運用部門の有識者によりタイミングの確認と再開前の必須処理が完了済みかどうかの点検を実施することを手順へ明記
- 大規模障害発生時にも顧客サービスへの影響を回避できる CP の作成、それにもとづく訓練の実施

2 5 定期メンテナンス後の確認不足による信用情報機関への情報提供遅延

<業態>

貸金業者

<事象>

- 一部データベースが使用不可状態となったままオンラインサービスを開始したため、信用情報機関に提供すべきデータが一部作成できず情報提供遅延となる事象が発生した。

<原因>

- ◆ データベースの定期メンテナンス後、システムを立ち上げる際に、データベースの状態を確認する運用を定めていなかった。

<対策>

- 定期メンテナンスの確認項目に、システムを再立ち上げる際、データベースの状態を確認し、異常が発生していないことを確認することを追加

2 6 連携先におけるシステム障害後の対応不備に起因した二重引き落とし

<業態>

資金移動業者等

<事象>

- カード会社から連携される残高引落処理用のデータが機器故障により正常に受信されず、誤って前日処理済みのデータで再度処理が行われたことから、カード利用者において二重の支払いが発生した。

＜原因＞

- ◆ リカバリー対応において、前日分のデータをシステムの確認をせずに取り込んだ。
- ◆ 当社はカード会社から正常にデータを受信していない旨の連絡を受けていたが、システムの運用管理を行う部署に連携していなかった。

＜対策＞

- 処理対象データについて前日データとの差分チェックを行う等、データの二重処理を防止する機能の実装
- データ連携ができなかった際の関連部署や関連会社との情報連携体制の強化

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

Ⅲ サードパーティの提供するサービス等の要因

1 外部サービスでのシステム障害により利用者資産の出金が遅延^{新規}

＜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

2 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

3 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

4 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

5 サードパーティの提供するサービスの障害によるサービス提供不可（１）

＜業態＞

主要行等、地域銀行、信用金庫・信用組合等

＜事象＞

- 複数の金融機関において、IB に関するワンタイムパスワード認証システムのエラーにより個人 IB 及び法人 IB のログインが不可となる事象が発生した。

＜原因＞

- ◆ サービス提供元のシステム障害が原因（サービス提供元がプログラム修正を行い対処）。

＜対策＞

- 認証エラー時の代替手段の構築
- 障害時の連絡体制強化

6 サードパーティの提供するサービスの障害によるサービス提供不可（２）

＜業態＞

主要行等、地域銀行

＜事象＞

- エンドユーザー側端末の OS アップデートによって、端末とシステム間の暗号化通信仕様が変更された結果、負荷分散装置で必要なリソースを確保できなくなったことで、法人 IB にログイン不可となる事象が発生した。また、事象検知や対応にも時間を要した。

＜原因＞

- ◆ システム監視におけるエラー検知がなく、接続エラーの問い合わせが通常時より増加するまで障害として認知できなかった。
- ◆ システム運用側で、検証環境の機器が本番環境と同等ではなく、障害対応のために負荷分散装置メーカーから提供された修正プログラムの妥当性確認ができなかった。

＜対策＞

- 障害状況の適時把握を目的とした監視項目の追加や問い合わせ状況の連携強化

- システム運用側での本番環境と同等以上の検証環境構築と修正プログラムの検証

7 サードパーティの提供するサービスの障害によるサービス提供不可（3）

<業態>

主要行等

<事象>

- 新規の口座開設等の機能を提供するサードパーティの提供するサービスにおいて、ハードウェア障害に対する冗長構成が機能せず、利用不可となる事象が発生した。また、復旧作業時に意図しない振る舞い等が発生し復旧に時間を要した。

<原因>

- ◆ サービス提供事業者において、障害時の作業手順や環境整備方法、外部有識者への連携等の基本的な態勢が整備されていなかった。

<対策>

- サービス品質を維持するための態勢確立や監査によるプロセスの改善
- 業務委託元として、委託業務に対する代替手段の整備及び可用性や影響度を考慮した外部委託先の決定

8 サードパーティが提供するサービス仕様の理解不足による Web アクセス不可

<業態>

主要行等

<事象>

- サードパーティがサービスとして提供するサーバー証明書²⁰の有効期限に対する自動更新機能が、意図しないタイミングで実施され、スマートフォンアプリに保持された情報との不整合によって、サービスが利用できない事象が発生した。

<原因>

- ◆ サーバー証明書の期日を管理していたサーバー運用部門が、自動更新機能による更新タイミングを把握できていなかった。

<対策>

- 利用するサービスの設定や仕様に関する関係者間での必要な確認と周知

9 サードパーティの提供するサービスの障害によるスマートフォンアプリケーション、一部 Web サービス提供不可

²⁰ 「通信の暗号化」「Web サイトの運営者・運営組織の实在証明」の2つの役割をもつ電子証明書のこと

<業態>

地域銀行

<事象>

- データ記憶装置が停止状態になった結果、スマートフォンアプリケーションによる口座開設新規開設、スマホ・PCによる住宅ローン申し込みができない事象が発生した。

<原因>

- ◆ 共同利用しているデータ記憶装置にて機器故障交換を契機に潜在的な不具合が発生し、データ記憶装置がスローダウンし最終的には停止状態になった。
- ◆ データ記憶装置のベンダー出荷時に設定初期不良があった。

<対策>

- データ記憶装置の監視項目にパフォーマンス傾向「応答速度」を追加
- ベンダー製品の各種初期設定値の開示、機器増強時に設定値の精査

10 サードパーティの提供するサービスの障害によるサービス提供不可

<業態>

地域銀行

<事象>

- サードパーティ側のメンテナンス作業において設定不備があり、IB（クラウドサービス利用）にログインしづらい状態となる事象が発生した。

<原因>

- ◆ サードパーティ側の設定不備によって発生するシステム障害を想定していなかった。

<対策>

- 障害発生箇所をスムーズに特定するためのシステム構成及びリソース監視項目の見直し

11 サードパーティの提供するサービスの障害による復旧対応遅延

<業態>

資金移動業者等

<事象>

- サービス提供に必要なサードパーティの利用システムが設置されているデータセンターでシステム障害が発生した。事前に準備していた冗長構成が機能せず、障害復旧に時間を要し、決済等取引に影響を及ぼす事象が発生した。

<原因>

- ◆ 冗長構成を事前に検証する等の対策の実効性確保ができていなかった。
- ◆ 復旧手順の整備、訓練等が実施できていなかった。

<対策>

- 冗長構成の事前検証の実施
- 復旧手順の整備、訓練等の実施

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

Ⅳ 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^{新規}

＜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^{新規}

＜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 カウンター上限値超過によるシステム停止

＜業態＞

主要行等、資金移動業者等

＜事象＞

- 取引量の増加（キャンペーン等のイベントによる一時的な取引量増加を含む。）により、システムで保有する取引件数等のカウンターやメールのファイル格納数等のシステムカウンターが上限値を超過し、システムが停止したため、顧客がサービスを利用できない事象が発生した。また、システム設定値の上限を超過した場合の対応を備えていたが機能しなかった事象も発生した。

＜原因＞

- ◆ システムで保有する取引件数カウンターやメールのファイル格納数等のシステム設定値の上限の把握や監視ができていない。
- ◆ 取引量等の増加（キャンペーン等のイベントによる一時的な取引量増加を含む）によるシステム設定値の上限の事前検証、見直しができていない。また、システム設定値の上限を超過した場合の対応が正しく動作するかの検証ができていない。

＜対策＞

- システムで保有する取引件数カウンターやメールのファイル格納数等のシステム設定値と上限の洗出し
- カウンターの監視、取引量等の増加（一時的な取引量増加を含む）によるシステム設定値の上限（システム設定値の上限を超過した場合措置を含む）の事前検証、見直し実施

6 システムの処理能力不足による決済不可

＜業態＞

資金移動業者等

＜事象＞

- 取引量の増加（キャンペーン等のイベントによる一時的な取引量増加を含む。）によるシステムの負荷予測を行い、システムの処理能力等の事前検証を行っていたが、検証範囲が適切に設定されておらず、決済が不可となる事象が発生した。

＜原因＞

- ◆ 取引量の増加に伴うシステムの負荷予測、システムの処理能力等の事前検証が必要な外部接続先等の範囲の認識が誤っていた。

＜対策＞

- システムの負荷予測、システムの処理能力等の事前検証を行う先の選定に関して、決済事業者や販売店（POS 会社）の外部接続先を含めた網羅的な検討の実施

7 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>

- ◆ 想定取引量にもと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もと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

I 設定ミス・操作ミス等の管理面・人的要因

1 本番作業時の作業誤りによる ATM 稼働不可^{新規}

<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う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

2 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^{新規}

<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

3 利用予定の外部サービスに関する技術調査内容の誤り^{新規}

<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

4 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

5 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

6 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）

7 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

8 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

9 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²¹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）

10 製品知識の不足に起因する障害に伴う IB の利用不可

<業態>

²¹ 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。

主要行等

<事象>

- 勘定系システムと周辺システムとを接続するハブ機能をもつシステムにおいて、冗長構成の設定不備に起因し、ハードウェア障害時にシステムが停止し IB が利用不可となった。システム改修時にそれまで利用していた製品とは別製品を採用したことに起因し、製品固有の設定についてメーカーに対する確認漏れが発生した。

<原因>

- ◆ 過去の開発実績を踏まえて設計・設定を行った。
- ◆ 切替えのテスト工程について、利用実績のある製品をもとにしたテストのみを行ったため、設定誤りに気づけなかった。

<対策>

- 導入実績のないハードウェアやソフトウェアを利用する際の製品メーカーのテクニカルレビューを義務化し、確認漏れを発生させないプロセスを整備

1 1 口座情報の更新作業の障害に伴う ATM の利用不可

<業態>

主要行等

<事象>

- 口座情報の更新作業時にメモリ容量不足が発生し、勘定系システムの一部機能が停止したことに起因して、多くの ATM が停止し顧客の通帳等が取り込まれる事態が発生した。

<原因>

- ◆ 作業時に直接的な変更箇所以外の影響確認を実施していなかった。
- ◆ 作業に起因して発生する業務影響の把握が不足したことによって事前準備が不足し障害対応に時間を要した。

<対策>

- 変更作業に対するチェックやレビュープロセス改善と影響箇所を把握するための有識者の育成
- 限定された作業箇所の障害がシステム全体としてどのような影響範囲（最大リスク）になるのか特定し対策する態勢の整備

1 2 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

1 3 本番作業時の同時処理考慮漏れに起因するオンライン取引不能

＜業態＞

地域銀行

＜事象＞

- 月次定例処理と随時処理におけるデータベースアクセスが競合し、一部店舗の口座（元帳）オンライン取引が不能となり、取引不能時間帯に利用された自動機（ATM、通帳繰越機）がタイムアウトし自動機が停止する障害が発生した。

＜原因＞

- ◆ 運用担当者は定例処理と随時処理を同時実行するときのリスクを正しく認識できておらず、また開発担当者においても処理が競合するリスクに気付くことができなかった。

＜対策＞

- 定例処理と随時処理の競合時における問題発生処理の洗い出しと処理可能時間の明確化
- 「実施タイミング」、「処理実施システム」、「参照先データベース」等に問題がないことを事前にチェックする手順の整備

1 4 データベース容量拡張時の作業手順誤りによる入金取引不可

＜業態＞

貸金業者

＜事象＞

- データベース容量拡張時の作業手順誤りにより、一部ローンサービスにおける入金取引が不可となる事象が発生した。

＜原因＞

- ◆ データベース容量拡張作業において、作業手順を誤り、データ移行が正

常に実施できなかった（テストは実施したが、本番との作業手順に相違があった）。

＜対策＞

- テストにおける作業手順の確認は、本番と同一手順でのテスト実施を徹底

15 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

Ⅱ ソフトウェアの不具合

1 設定ミスにより複数回の同一注文が発注可能^{新規}

<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

2 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

3 想定を超えた注文数により時間優先での原則が適用されず約定が行われたシステム障害

<業態>

暗号資産交換業者

<事象>

- 同一価格で一定件数を超える指値買いの新規注文が蓄積した場合、約定対象の買い注文に時間優先の原則が適用されず、後から注文した指値の買い注文から約定した。

<原因>

- ◆ 当社取引所システムの板寄せ処理は、指値の買い注文を一定件数ずつ取得し売り注文とのマッチングを行っているが、一定件数を超える同一価格での指値の買い新規注文が発生した場合、直近の一定件数が優先される仕様となっていたため、先に注文した買い注文が後回しにされた。

<対策>

- 想定以上の注文を受けた際に時間優先の原則が適用されているかというテスト確認の徹底
- 新規取扱銘柄に対する注文増加予測と事前のシステム影響調査

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）

5 新規プログラムの設計不備及びリリース認証不可

<業態>

主要行等

<事象>

- 生体認証プログラムの新規リリース後に、誤ったソフトウェア設計に起因して処理が間に合わず大量の認証エラーが発生した。その後システムの切戻しを実施したが、復旧までに時間を要した。

＜原因＞

- ◆ 新規プログラム開発時に行った負荷テストが、そもそもシステム要件に合致していなかった。
- ◆ システムの安全性に配慮したリリース手順ではなかった。

＜対策＞

- 開発委託先の負荷テストの検証結果を確認するプロセスの追加
- システムリリース時における手順の品質向上

6 システム更改（機能追加）時の、仕様の理解不足等によるプログラムミス

＜業態＞

信用金庫・信用組合等

＜事象＞

- 共同センター（個人向け IB）において、機能追加による更新時に設計書の記載が不正確であったことにより、プログラムミスによるエラーが発生し、約 10 金庫の個人向け IB において、ログインできない事象が発生した。
- 共同センター（法人向け IB）において、機能追加による更新時に仕様変更を把握していなかったことにより、データベースのレコード作成に誤りがあり、約 90 金庫の法人向け IB において、取引画面が操作できない事象が発生した。

＜原因＞

- ◆ 機能追加による更新時に、設計書の記載が不正確であった。
- ◆ 更改時の仕様変更を把握していなかった。

＜対策＞

- 設計書の再点検
- データ構成を変更する際に既存データが変更後の仕様に合致しているかの全件チェックを実施することをルール化
- 機能追加・変更があった設定の再検証
- レコード作成要領の整備
- システム更改時の仕様変更について、理解度向上のための講習会を実施

7 システム開発におけるレビュー不足によるサービス提供不可

＜業態＞

信用金庫・信用組合等

＜事象＞

- 勘定系システムの通信状況を監視するプログラムの不備により、当該システムが停止し、窓口での現金受払、ATM、IB等の取引が不可となる事象が発生した。また、システムを運用する外部委託先から金融機関への報告に時間を要した。

＜原因＞

- ◆ プログラムの不備により、ホストコンピュータのリソースが枯渇し、システムが正常に稼働しなくなった。
- ◆ プログラムの初期導入時、検証者によるレビューが有効に機能しなかった。
- ◆ 夜間・早朝に障害が発生した際の連絡手段に不備があり、また、定義されたCPが不徹底であった。

＜対策＞

- ホストコンピュータのリソース監視強化、本番リリース時のチェックリストの見直し、本事象と同様の不備有無の点検
- 大規模障害発生時の連絡体制の再検証、大規模障害の訓練の定期的な実施

8 外部ベンダーのパッケージ製品の仕様確認不足による取引処理遅延

＜業態＞

金融商品取引業者（ネット証券会社）

＜事象＞

- 改修した口座振替サービスのリリース直後、口座振替処理が遅延した。

＜原因＞

- ◆ 改修に伴い、利用していたパッケージ製品の仕様確認を自社でしか行わなかった結果、確認に誤りがあり、パッケージ製品が本来対応していない処理方式へと改修してしまった。

＜対策＞

- 今後の改修時の影響調査においては、製品ベンダーへ確認し、確認結果の証跡を残すようプロセスを変更
- リリースまでに本番同等の環境にてテストを行えるよう開発環境を整備

9 ログ出力仕様の誤りによる取引開始遅延

＜業態＞

金融商品取引業者（ネット証券会社）

＜事象＞

- データベースサーバーが高負荷の状態で行われた定期バックアップ処理に時間を要し、FX 取引サービスの開始が遅延。また、復旧作業を行った影響により、取引報告書閲覧開始が遅延。

＜原因＞

- ◆ 障害発生の数日前にリリースした改修プログラムにおいて、本来はログ出力が不要にもかかわらず、一部のログを高頻度に出力する不具合が内在していた。
- ◆ ログ出力がないとの思い込みによりテストでのログ出力確認を実施せず、また、テストでは本番よりも負荷の少ないテストデータ使用したことにより不具合の発見に至らなかった。

＜対策＞

- 設計時にログ出力頻度やリソースへの影響について確認することを開発時のチェックシートへ明記
- サイクルテスト実施時に不要なログ出力のないこと、予期せぬ性能劣化のないことを確認することを開発時のチェックシートへ明記

10 外部委託先が招いた設計不備、自社によるテスト不足による送金不可

＜業態＞

資金移動業者等

＜事象＞

- 性能改善のためリリースした修正プログラムに設計不備があり、送金先へ接続できず、送金不可となる事象が発生した。

＜原因＞

- ◆ 外部委託先において設計書等の成果物の整備が不十分で知識が属人化しており、また、担当者の異動時の引継ぎが不十分であったため、リリース前に設計不備に気付けなかった。
- ◆ 当社による受入テストにおいてもテスト項目が不十分であり、設計不備を検知できなかった。

＜対策＞

- 知識の属人化防止のための成果物の確実な作成、担当者の異動に備えた体制の整備
- システム変更箇所を考慮した十分なテスト計画を作成の上、受入テストを実施

第5節 システム障害後の対応が円滑に行われた事例²²

1 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^{新規}

＜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。

2 事後改善策における障害発生時の顧客周知の迅速化^{新規}

＜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。

3 アプリへのログイン不可時の円滑な顧客対応の実施^{新規}

＜業態＞

主要行等

＜事象＞

- 銀行アプリが繋がりにくい状態となり、システムへのログインが不可等

²² 改善が適切に行われた事例を含む。

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 や店頭その他チャネルへ誘導した。

4 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。

5 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 CTM²³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。

6 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

²³ 郵便貯金、簡易保険の業務で使用する係員操作の端末機。「カウンター・ターミナル・マシン」の略。

態となった。

＜対応＞

- 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。

7 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。

以 上

別紙 1

コラム： 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の好事例及び課題

1 国内金融機関における TLPT の現状

サイバー攻撃の脅威が高まる中、技術的な対策だけではなく、人及びプロセスも含めた対応が必要だが、技術、人及びプロセスを含めた対応態勢の実効性を検証する有効な手法として TLPT が挙げられる²⁵。近年、我が国の金融機関において、TLPT を実施する例が増えており、好事例も認められるものの、TLPT の内容や活用方法に改善の余地がある事例も認められる。

金融庁では、2023 事務年度金融行政方針の行動計画において、「金融機関のサイバーレジリエンスを強化するため、金融機関において実施した TLPT を収集・分析し、共通する課題及び好事例等を還元する」ことを掲げている。この計画にもとづき、銀行等における 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・一般化したうえで、その結果を銀行と共有した²⁶（概要は以下のとおり²⁷）。

2 分析結果の概要

まず、TLPT に重要な要素として、以下の 2 点が挙げられる。

- ・ 一般的な脅威だけではなく、自組織に特有の脅威を分析し、現実の攻撃を模した攻撃を実施する（具体的には、脅威インテリジェンスの導出結果を踏まえ、自組織を標的とし得る攻撃者、及び、それらの攻撃者が現

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。

²⁵ 「金融機関等における TLPT 実施にあたっての手引書」（公益財団法人金融情報システムセンター、2019 年 9 月、<https://www.fisc.or.jp/publication/book/004197.php>）では、「システムを対象とした対策だけでなく、人、対応プロセスも含めて総合的に実施する必要性が高まってきている。」（p2）、「システムへの侵入に関する防御能力のみに焦点を当てたペネトレーションテストのみならず、システムへの侵入後の『人』の対応などにも焦点を当てている TLPT は、サイバーレジリエンスを高めるうえで、より有効な手段であると考えられる。」（p5）としている。

²⁶ G7 サイバー・エキスパート・グループが策定した「脅威ベースのペネトレーションテストに関する G7 の基礎的要素」の要素 6 では、TLPT について、当局は、「類型化したデータとして、セクターに共通する発見事項や脆弱性を特定すべき」であり、この「類型化したデータを当局と金融機関の間で共有すること」が金融セクターのサイバーレジリエンスの改善にとって重要な手段であるとしている（<https://www.fsa.go.jp/inter/etc/20181015/02.pdf>）。

²⁷ テスト結果に関する機微な情報が含まれるため、本資料上では詳細な内容に関する記載を差し控える。

実に用いている攻撃手法を想定し、テスト計画へ反映する等)

- ・ システム、IT 資産、技術的な対策のほか、人、対応プロセスも評価する（例えば、導入されているセキュリティ製品の有効性にとどまらず、インシデント対応を担うブルーチーム²⁸の能力を評価する）

上記の点を踏まえ、本調査で銀行等から提供された事例を分析した結果、以下のような TLPT として望ましい事例と不十分な事例が認められた。なお、TLPT としては不十分であっても、なおサイバーセキュリティの強化に資する側面があると考えられるため、そうした金融機関の取組そのものが否定されるものではない。

	望ましい事例	不十分な事例
脅威インテリジェンス	・ 自組織に特有の脅威インテリジェンスを導出し、シナリオ選定している。	・ 脅威インテリジェンスが一般的な脅威情報の分析にとどまっている。
評価	・ ブルーチームに対して事前予告せずに TLPT を実施し、その検知・対応能力を評価している。 ・ SOC²⁹における検知・対応能力だけでなく、フィッシングメールを起点とした職員から CSIRT³⁰へのエスカレーションと、CSIRT の対応状況も評価している。	・ TLPT の計画を事前にブルーチームに伝え、ブルーチームが、疑似攻撃が発生することを把握しているため、その検知・対応能力が適正に評価されていないおそれがある。 ・ 攻撃者が考え得る複数の経路からの侵入や迂回攻撃を試みていないため、事前に想定した攻撃手法・経路で検証対象の脆弱性を検証する脆弱性診断と実質的に異ならないものとどまっている。
経営陣への報告・経営陣の対応	・ サイバーセキュリティ担当部署は、TLPT の結果から判明した全社的な影響を生じさせ得るリスクを経営陣に報告している。 ・ 経営陣は、TLPT の結果報告を受け、課題への対応を指示するだけでなく、テスト範囲の拡大や	・ 業務や顧客に重大な影響を及ぼし得る類似の課題が繰り返し検出されており、対策が十分ではなく、重要なリスクが残存している可能性を推測すべきであるにもかかわらず、過去の発見事項と類似していることをもってサイバーセキュリティ担当部署が経営陣への報告を省略している。 ・ TLPT によって検出された課題のう

²⁸ 模擬的な攻撃者グループに対してセキュリティ態勢を維持することにより、組織の情報システムにおけるセキュリティを確保する責任を負うグループを指す。

²⁹ Security Operation Center の略。ネットワークやシステムの監視、分析により、サイバー攻撃をリアルタイムで検知し、対処等を行う組織を指す。

³⁰ Computer Security Incident Response Team の略。セキュリティインシデントが発生した際に対応するために設置される専門チームを指す。

	事前に予告せずにテストを実施することを通じて、TLPT の高度化を図るように指示している。	ち、金融機関の経営に重要な影響を及ぼし得るものについて経営陣に報告したり、具体的なリスクについて報告したりせず、単に「良好な結果であった」と報告している。
発見事項の活用	・サイバーセキュリティ担当部署は、TLPT で検出された課題と同様の課題が TLPT の対象でなかったシステムにおいても認められないかどうかを確認し、報告するよう、社内の他のシステム担当者及びグループ会社のシステム担当者に対して指示している。	・TLPT で検出された課題が他のシステムでも認められないかどうかを確認していない。その結果、それ以降、他のシステムに対して実施した TLPT でも類似した課題が検出されている。
その他	・犯罪集団、国家が関与する主体、内部犯行者などの様々な主体の攻撃が生じさせる脅威に応じ、複数のシナリオを設定し、TLPT を実施している。	・TLPT の趣旨・目的に沿った十分な予算が確保されておらず、脅威インテリジェンスやブルーチームの評価が省かれ、結果として、TLPT としては不十分なテストとなっている。

3 金融機関に求められる対応

金融機関は、上記の TLPT に重要な要素、望ましい事例及び不十分な事例を参考として TLPT を実施することが望ましい。

経営陣は、攻撃者の目線から組織的な態勢と技術的対策を検証し、抽出された課題への対策を講じることにより、経営上のリスクを低減させるという TLPT の意義を踏まえたうえで、TLPT で重要な課題が検出されれば、躊躇なく現場から報告がなされるような組織文化を築くべきである。また、経営陣は、現場とのコミュニケーションを厚くすることなどを通じ、TLPT によって判明した課題の経営上の重要性及び緊急性、課題の根本原因、課題の解決に必要なリソース及び時間などを含め、課題の全体像を把握したうえでその解決に臨むべきである。

別紙 2

コラム： オペレーショナル・レジリエンスに係る金融機関との対話等の概要

金融庁では、2023 年 4 月に公表した「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）及び同ディスカッション・ペーパーの趣旨を踏まえて同年 6 月に改正した主要行等向けの総合的な監督指針³¹に規定する基本動作及び主な着眼点等について、主要行等及び国際統一基準金融機関を対象にアンケートを実施した上で一部の金融機関と対話を行った。その結果の概要は、以下のとおり。

（なお、本コラムの内容はアンケートやヒアリングの結果をまとめたものであって、これをもって当庁が各金融機関におけるオペレジの確保が完了したと認識していることを必ずしも意味するものではない。）

1 「重要な業務」の特定

対象金融機関のうち大半の先が、重要な業務の特定を完了済みもしくは 2025 年 3 月までに完了させる予定としている。

重要な業務の選定にあたっては、既存の BCP³²（事業継続計画）の対象業務を選定することを検討しつつも、それだけではなく、新たな基準を設けて、重要業務の範囲を見直している先が多い。具体的には、顧客目線に立った業務中断時の影響を重視するとともに、特定業務の市場シェア、金融市場への影響、業務が中断した場合の自行への影響（取引数・取引額などの観点からなど）、業務の特性（取引時限があるか否かなど）等も加味しながら選定を行っている。定量的な基準を設けつつも、最終的には定性的な判断によって重要業務を特定する傾向が認められた。

2 「耐性度」の設定

対象金融機関のうち大半の先が、耐性度の設定を完了済みもしくは 2025 年 3 月までに完了させる予定としている。

既存の BCP の RT0³³（目標復旧時間）を活用して耐性度を設定するとしている先が多かった。一部の金融機関においては、影響を受ける取引数、取引額及び利用者数に加え、苦情数を考慮している事例、業務特性に応じた時限を考慮し

³¹ <https://www.fsa.go.jp/news/r4/ginkou/20230623-2.html>

³² Business Continuity Plan の略。

³³ Recovery Time Objective の略。

ている事例、RTOにRLO³⁴（目標復旧レベル）を組み合わせている事例が認められた。また、利用者の厳しい目線を意識しつつ、引き続き試行錯誤を続けていくとしている先もあった。

3 相互関連性のマッピング・必要な経営資源の確保

対象金融機関のうち半分程度の先が、相互関連性のマッピングを完了済みもしくは2025年3月までに完了させる予定としている。

重要業務の遂行に必要な経営資源として、人員、システム、施設、サードパーティなどの関連性・依存度をマッピングしている先が多く、マッピングの範囲や粒度について試行錯誤している先が多い。こうした状況の下、マッピングにおいて重要業務単位でフローチャートを用いて経営資源（人員、システム、施設など）を可視化している事例、特定した経営資源のマッピングを管理・維持するために一元管理ツールの開発を検討している事例が認められた。

また、対象金融機関のうち半分程度の先が、相互関連性のマッピングの過程において、重要業務の提供に不可欠なサードパーティの特定を完了済みもしくは2025年3月までに完了させる予定としている。

既にサードパーティを特定している金融機関でも、フォースパーティ以降への対応は、外部委託先を通じて管理する既存の枠組みにとどまっており、オペレジの観点による重要業務の提供に不可欠なフォースパーティ以降の関係先の特定や管理の高度化を今後の課題としている。

4 適切性の検証・追加対応

対象金融機関のうち半分未満の先が、適切性の検証を完了済みもしくは2025年3月までに完了させる予定としている。

重要な業務の特定、耐性度の設定、必要な経営資源の配分などが適切であることを検証するシナリオの検討に時間を要している先がみられる中、システム停止が長期化するなどのストレスシナリオの検証を行っている事例、業務停止の原因を問わず、システム、要員などの経営資源が棄損したという結果事象を想定したシナリオによる検証を進めている事例が認められた。

2024年3月末時点では、一部の金融機関がオペレジの基本動作を一巡させている一方、その取組が途上の先も多い。金融機関においては、利用者目線に立った重要業務の早期復旧や影響範囲の最小化のため、経営陣のコミットメントの下、ロードマップを立て、オペレジの確保を計画的に進めることが望ましい。

³⁴ Recovery Level Objective の略称。RTO 時点で平時と比較してどの程度の業務・サービスを復旧するかの指標。