金融機関のシステム障害に関する
分析レポート

令和３年６月

金融庁
Financial Services Agency

【はじめに】 1
（留意事項） 1
【障害分析概要】 2
１．集計期間 2
２．主な障害傾向 2
（１）システム統合・更改に伴い発生したシステム障害 2
（２）プログラム更新、普段と異なる特殊作業などから発生したシステム障害 2
（作業影響の検討不足） 2
（設定ミス・作業の誤り） 2
（３）日常の運用・保守等の過程の中で発生したシステム障害 3
（サードパーティの提供するサービス等の要因） 3
（冗長構成が機能しない障害（ハードウェア・回線等）） 3
（４）サイバー攻撃、不正アクセス等の意図的なもの 4
（本人確認の設計に係る事案） 4
（クラウド事業者等の提供するサービスのセキュリティに係る事案） 4
３．今後の金融庁の取組 4
（１）システム障害の発生を踏まえたモニタリング 4
（２）システム統合・更改に関するモニタリング 5
（３）サードパーティの提供するサービスなどの新たなリスクへの対応 5
【事例集】 6
１．業態全体の障害傾向（事象別） 6
２．事例 7
（１）システム統合・更改に伴い発生したシステム障害 7
（２）プログラム更新、普段と異なる特殊作業などから発生したシステム障害 13
① ソフトウェアの不具合 13
② 設定ミス・操作ミス等の管理面・人的要因 18
（３）日常の運用・保守等の過程の中で発生したシステム障害 24
① サードパーティの提供するサービス等の要因 24
② ハードウェア・回線等の不具合 28
③ 設定ミス・操作ミス等の管理面・人的要因 31
④ 取引量増加に伴う容量不足等 35
（４）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 39

【はじめに】

金融庁では、監督指針等に基づき、発生したシステム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、各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。

これらの報告等を基に、これまで、2019 年及び 2020 年に「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、近年の IT やデジタライゼーションの進展に伴う特徴的な障害など、分析結果や事例を公表してきている。

昨今、全国に大きく報道されるような障害や不正利用等の事案が発生しており、多くの顧客に影響を及ぼす事案が続いている。また、バーゼル銀行監督委員会から「オペレーショナル・レジリエンスのための諸原則」等が公表され、今後、オペレーショナル・レジリエンスへの取組が加速することも予想され、業務中断の影響をいかに軽減・緩和し、初動・回復に繋げていく対応が重要となる中、組織横断的なシステムリスク管理態勢の整備や高度化の必要性がますます高まってきている。

したがって、本レポートでは、各金融機関がシステムリスク管理に取り組んでいく上で、障害に関する分析結果が参考になるよう、過去に公表した事例も含め障害傾向と事例（事象、原因及び対策）を取りまとめて公表することとした。

各金融機関においては、引き続き、各種ガイドライン等[1]や本文書を活用し、金融システムの安定や利用者保護の観点から、システムリスク管理態勢の整備や高度化に向けた創意・工夫を積み重ねることが期待される。

（留意事項）

本レポートの個々の事例は、2018 年７月から 2021 年３月までに報告された「障害発生等報告書」等のうち、主な事案を事例集として取りまとめたものであるが、掲載されていない事例について、当局としてこれを重視していないことを必ずしも意味するものではない。

本事例は、各金融機関において、自己責任原則の下、創意・工夫を活かし、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することを想定しているものである。

[1] 金融機関に活用されている各種ガイドライン等として、公益財団法人金融情報システムセンター（FISC）の「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」及び「金融機関等のシステム監査基準」、情報システムコントロール協会（ISACA）の「Control Objectives for Information and related Technology (COBIT)」、経済産業省の「システム管理基準」及び「システム監査基準」などが想定される。

【障害分析概要】

１．集計期間

金融機関のシステム障害については、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、本レポートは、「障害発生等報告書」の集計期間を 2020 年４月から 2021 年３月までとし分析したものである。

２．主な障害傾向

（１）システム統合・更改に伴い発生したシステム障害

これまでに公表した分析レポートでは、システム統合・更改に係るプロジェクトについては、大規模かつ専門性が高いものであることから、プロジェクトの特質に基づいたプロジェクト管理態勢の整備や、設計レビュー体制の強化等を課題として取り上げている。

前回のレポート公表後、金融機関の合併に伴うシステム統合をはじめとして、新たな勘定系システムへの移行や現行システムのクラウドサービスへの移行など、様々な大規模プロジェクトが進められている中、システム稼働時に振込の遅延など、顧客の決済に影響を及ぼすような事案が数多くみられた。

これらの障害の原因は、旧システムの仕様の理解不足やテストのパターン不足等が挙げられ、この背景にレガシーシステムの有識者の高齢化等による人材不足があると考えられる。有識者不足によるリスクを低減するため、システム仕様や作業手順書等の「IT 資産の整備」のほか、IT 人材の育成が引き続き課題となっている。

（２）プログラム更新、普段と異なる特殊作業などから発生したシステム障害

（作業影響の検討不足）

本番環境において、様々な特殊作業を行わなければならないプロジェクト等があり、これらの作業に起因する障害が多くみられた。中には、一部システムが停止したことに起因して ATM 等の周辺システムに影響する事例が複数みられた。

これらに共通する問題点として、作業に起因してどのような障害が発生し得るのか想定できていないなど適切にリスクを認識するに至っていないことや、コンティンジェンシープラン（以下、「CP」という。）の整備が不十分なまま作業が実施されたことが挙げられる。

また、作業自体については、システム全体を見渡すことができる有識者参加のもとでレビューを行うなどにより、品質を確保することが重要である。

（設定ミス・作業の誤り）

本番環境のシステムにおける作業誤りや、委託先における作業の誤りを看過するな

どの管理面・人的側面に起因する障害が多くみられた。特に、委託先における作業の実態を把握していなかったような事例もみられており、いかに委託先の作業を適切に管理するかが課題となっている。

また、導入したデータベース等の製品に対する知見不足により、設定不備が発生するといった事案もみられ、機器等を導入する際の選定手順等も適切なものにしていく必要がある。

さらに、障害発生時の作業が適切に行われず、障害の時間を長引かせるような事例など、あらかじめ作業手順を確立できていないことにより問題が大きくなるような事例も複数みられた。

様々な事態を想定し作業手順書等の充実を図るとともに、それらの内容に効率性も含めて問題がないか定期的に点検を行うなど、作業品質を向上させていくことが課題となっている。

（３）日常の運用・保守等の過程の中で発生したシステム障害

（サードパーティの提供するサービス等の要因）

これまでに公表した分析レポートでは、複数の金融機関に影響を及ぼしたインターネットバンキング（以下、「IB」という。）に関するワンタイムパスワード（以下、「OTP」という。）認証システムの障害を取り上げ、CP の実効性の向上を課題としてきた。

前回のレポート公表後においても、サードパーティの提供するサービスの障害によって、多くの金融機関に影響を及ぼす事例が複数みられた。

特に、金融機関だけで障害を未然防止することが困難なクラウドサービス等の障害も増加しており、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の取組が必要となる。

（冗長構成が機能しない障害（ハードウェア・回線等））

昨年の分析レポートにおいて、障害に備えた冗長構成[2]が意図どおりに機能しない障害について取り上げたが、その後も同様の事例（障害が発生したにも係わらず副系に切替わらなかったなど）が複数みられた。冗長構成は、特に可用性が求められるシステムで用いられているため、障害が発生した場合、顧客に大きな影響を及ぼすなど、重大な障害となるケースがある。

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に実効性を確保することはもとより、意図どおりに機能しないことも想定し重要な業務が継続できるような方策の準備や、障害検知及び対応の早期化に係る取組が課題である。

[2] システム障害に備えて設備や装置を複数用意しておき、一部障害が発生しても運用が継続できるようにしたシステム構成。

（４）サイバー攻撃、不正アクセス等の意図的なもの

（本人確認の設計に係る事案）

スマートフォンを用いて、インターネット口座振替サービス等の方法により預金口座と連携させる決済サービスを提供する事業者が多数登場しているが、この仕組みを悪用し、連携を行う預金口座の預金者になりすまして不正な取引を行う事案が発生した。

また、金融商品取引業者を中心にインターネットを通じた株取引ツール等への不正アクセスが行われる事案が発生している。特に、フィッシングサイトを含む別のサイト等から過去に流出したIDやパスワードで様々なサイトへのログインを試みるリスト型攻撃と呼ばれる手口がみられた。

これらへの対応として、補償方針の策定・実施や利用者相談に真摯に対応するための態勢整備に加え、実効的な認証方式の導入等不正防止対策が急務である。また、パスワード等の漏えいに備え、利用するサービスの内容及びリスク特性に応じて、多要素認証等を用いて安全性を確保することが課題となっている。[3]

（クラウド事業者等の提供するサービスのセキュリティに係る事案）

クラウド事業者をはじめとする外部委託先等の提供するサービスについては、当該サービスへの不正アクセスに起因して多くの金融機関に影響を及ぼす事例が複数みられただけでなく、クラウドサービス内に保存されている情報が、設定不備等により第三者にアクセスできる状態となり、漏えいするといった事案も複数みられた。

クラウドサービスにおけるシステム開発を外部ベンダーに委託しているようなケースも多く、クラウドサービスの仕様やアップデート情報等に関する知識習得や情報収集を含め、十分な態勢整備が行われないまま、クラウドサービスを利用している事例もみられた。

サービス品質等の管理が行き届かなくなるリスクやセキュリティ面のリスクが考えられる中、アウトソーシング可能な業務範囲の明確化といった対策も含めて、全体の態勢を整備していくことが課題となっている。

３．今後の金融庁の取組

金融庁は、各金融機関のシステムリスク管理態勢の整備等の取組が円滑に進められるよう以下の取組を実施する。

各金融機関においては、金融システムの安定や利用者保護の観点からシステムリスク管理態勢の整備や高度化に向けた創意・工夫を積み重ねることが期待される。

（１）システム障害の発生を踏まえたモニタリング

デジタライゼーションの進展やコロナ禍による IT サービスの利用増加等の顧客の動

[3] 金融庁では、サイバーセキュリティ管理や外部サービスとの連携時に必要となる対策等を整理し、「事務ガイドライン（第三分冊：金融会社関係）」、「主要行等向けの総合的な監督指針」等の一部を改正した。

向変化は、情報システムへの依存による利便性の向上と引き換えに、システムリスク管理の重要性が高まる要因となり、大規模な障害が頻繁に発生すれば、金融機関に対する信頼性が揺らぎかねない。

金融庁では、金融機関のシステムの安定稼働に向けて、障害発生時には、必要に応じ原因・事後改善策のヒアリングなど、モニタリングを中心に実施してきたところである。

昨今の状況を踏まえ、今後も、こうした取組を継続するとともに、障害発生の重要度や管理態勢上のリスクが認められる場合には、検査を含めた更に深度ある検証を行うなど、実効的かつ効果的なモニタリングを進めていく。

（２）システム統合・更改に関するモニタリング

経営統合に伴うシステム統合だけでなく、将来を見据えた大規模なシステム更改も行われるなど、大規模なプロジェクトがいくつもの金融機関において予定されている。

こうした経験の少ない大規模プロジェクトに関するモニタリングにおいては、単に進捗状況の把握にとどまらず、過去の事例も踏まえて、問題となりやすい事項について詳細に検証・議論するなど、対話を通じて金融機関の自律的な改善を促すことに力点を置いてきた。

今後も、こうした取組を継続するとともに、リスクの高いプロジェクトには検査を含めた更に深度ある検証を行うなど、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。

（３）サードパーティの提供するサービスなどの新たなリスクへの対応

デジタライゼーションへの対応について、適切な IT マネジメントの下でリスクを踏まえつつ、柔軟かつ迅速に取り組んでいくことが重要となる。特に、クラウド等のサードパーティが提供するサービスを利用する金融機関が増加する中、導入・運用時に適切にリスク管理ができるような態勢を整備することが必要となる。

サードパーティの提供するサービスに関するリスクへの対応は、以前より公益財団法人金融情報システムセンター（以下、「FISC」という。）等と連携し対応を進めてきたところであるが、今後も新たな事案が認められた場合には、各金融機関の取組の参考とするため、事例等の公表を行っていく。金融機関側でのコントロールが難しいリスクとその対策については、引き続き、FISC 等と連携の上、調査検討を進めていく。

【事例集】

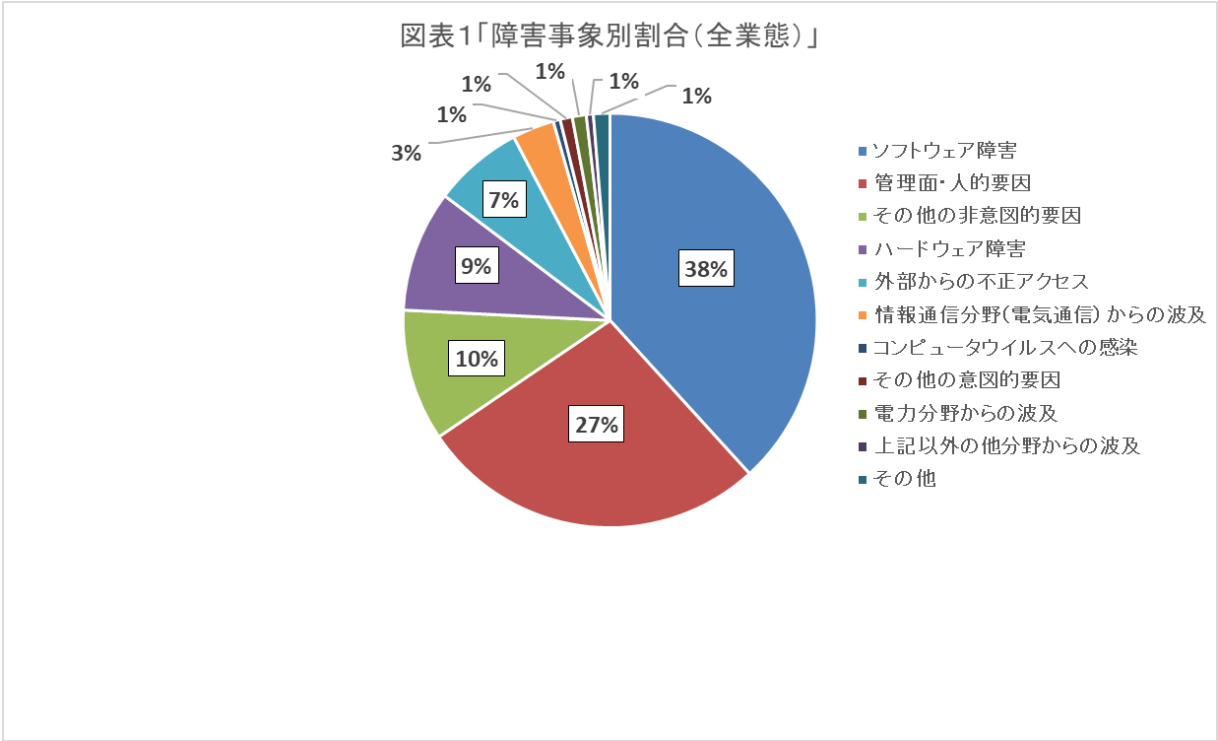
１．業態全体の障害傾向（事象別）

業態全体[4]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３分の２を占めている[5]。

「ソフトウェア障害」について、主要行等や資金移動業者等においては設計時の考慮不足や事前の負荷テスト項目の漏れに起因して IB が利用不可となるなどの障害が多く報告されている。また、地銀や金融商品取引業者においては、システム開発の委託先に起因する障害が多く報告されている。

「管理面・人的要因」による障害について、前年までの傾向に変わりなく、業態に偏りなく報告されており、委託先を含む本番システムにおける作業手順誤りや、誤った作業を看過したことによるシステム停止及び運用における業務処理の重複に伴うデータベースの過負荷等によって顧客サービスに影響を及ぼす障害が報告されている。

金融商品取引業者においては、証券取引所が 2020 年 10 月 1 日にシステム障害を受けて全銘柄の取引を終日とりやめたことに起因して、こうした想定でシステムが構築されていない先もあり、翌日のシステム稼働における障害が複数報告されている。



[4] 本集計期間（2020 年度）に金融機関から報告されたシステム障害の件数は、前年度（2019 年度）と同じく約 1,500 件であった。（金融機関：預金取扱金融機関、保険会社、金融商品取引業者、貸金業者、前払式支払手段発行者、資金移動業者、暗号資産交換業者等）

[5] 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もの。

２．事例

システム障害の事例については、2019 年及び 2020 年に公表しているが、本事例については、これまで公表した主な事例を障害発生の契機別等に整理した上で[6]、前回公表時に取りまとめた以降に発生した障害をアップデート（初めて掲載した事例には新規と表示）したものである。

（１）システム統合・更改に伴い発生したシステム障害

➢ 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

➢ 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＞
○ 新システム稼働後、大量の処理に伴うサーバリソースの高負荷、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＞

[6] 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。

◆ 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＞

● サーバ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＞

○ 勘定系データベースサーバがダウンし、ATM で取引エラーが発生した。

＜原因＞

◆ 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がダウンした。また、待機系への手動切替手順の認識（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＞

● 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＞

○ 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＞

◆ 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＞

● 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＞

○ 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[7]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。

＜原因＞

◆ 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。

[7] 「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、一部を更新するデータをいう。

◆ 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＞

- 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

➢ システム更改時の設計漏れに起因する被仕向送金障害 新規

＜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・仕向銀行に対する資金の誤返却が発生した。

＜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基幹系システムの設計レビュー、テスト等の充実

➢ コアタイムからモアタイム切替遅延に伴う為替未送信 新規

＜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基幹系システムの設計レビュー、テスト等の充実

➢ **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、誤って口座引落しされる事象が発生した。
＜原因＞
◆ 解約等によって口座引落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

➢ **新旧システムの特性等に対する考慮不足による ATM での一部取引不可**

＜業態＞
地域銀行
＜事象＞
○ 新旧システムの機能に対する比較検討不足のため、ATM で古いキャッシュカードと通帳を併用した一部の取引ができない事象が発生した。
＜原因＞
◆ 関係先間（ATM の開発委託先、新システム開発委託先、当行）における認識相違のため、旧システムにおいては、古いキャッシュカードを用いた取引時、店番と口座番号を旧システムで読替えたが、新システムにおいては、通帳の改ページが発生した場合読替えを行わない仕様であった。
◆ テストのパターン不足で、このような組合せを試していなかった。
＜対策＞
● 関係先全てを招集したレビューの徹底による認識相違の防止
● マトリクス表を用いた、テストパターンの網羅性確認

➢ **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

➢　新旧システムの各担当者間の連携不足に起因した移行漏れによる IB 利用不可

＜業態＞

信用金庫、信用組合等

＜事象＞

○　仕向先金融機関の属性を判定する管理テーブルのデータ移行が漏れたことによって、IB による取引が利用不可となる事象が発生した。

＜原因＞

◆　新システムの更改担当は、新システムでは管理テーブルによる判定は不要と誤認し、データ移行の必要性を認識しておらず、旧システムの保守担当は、新システムの設計レビューに関与しなかった。

＜対策＞

●　個別チームの誤認を防ぐため、個々の案件に対するチーム合同のレビューを必須化及びテーブルデータの取扱いの明確化

➢　ネットワーク接続変更作業の管理ミスによる取引障害

＜業態＞

貸金業者

＜事象＞

○　開発中のシステムを誤って本番ネットワークに接続したことにより一部出金取引不可等が発生した。

＜原因＞

◆　当社は新システムの開発を複数のシステム開発会社に委託して推進しており、新システムのテストをＡ社、ネットワーク接続設定の変更作業をＢ社が担当。

◆ 新システムはネットワーク接続設定に加え、通信制御機能により外部システムとの接続を制御しており、本来、本番リリースまで本機能を停止しておく必要があったが、Ａ社は開発中のシステムを本番疑似環境に接続してテストを実施するために通信制御機能を起動。再テストを実施する可能性を考慮してテスト後も当該機能を停止せず、また、当該機能を停止していないことについてＢ社との間で情報共有していなかった。

◆ Ｂ社は開発中のシステムで使用する通信制御機能の起動状態を確認せず（停止しているものと誤認し）、ネットワーク接続設定をシミュレータから本番ネットワークへ変更。誤って開発中のシステムが本番ネットワークに接続された。

◆ 通信制御機能の起動やネットワーク接続設定の変更を行う際の承認プロセスが機能せずに本番ネットワークへの誤接続の可能性を看過した、プロジェクト管理上の不備。

＜対策＞

● 本番環境への変更を行う場合には、双方のシステム開発会社の担当者が必ず事前説明に参画し、本番ネットワークに誤接続されないことを確認の上、承認するプロセスを明確化

（２）プログラム更新、普段と異なる特殊作業などから発生したシステム障害

①　ソフトウェアの不具合

➢　新規プログラムの設計不備及びリリース認証不可　新規

＜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、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

➢　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　新規

＜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生じた。

○　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、本年１月の更改時の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生じた。

＜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

➢ **システム開発におけるレビューの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って、当該システムが停止し、窓口での現金受払、ATM、IB 等の取引ができない事象が発生した。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って、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態勢の再検証、大規模障害の訓練の定期的な実施

➢ **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

➢ 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が高負荷の状態で実行さ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

➢ 実機でのテスト未実施による ATM を利用した出金不可

＜業態＞
資金移動業者等
＜事象＞
- ○ プログラムの改修誤りによって、ATM を利用した出金ができなくなる事象が発生した。

＜原因＞
- ◆ プログラムの改修に伴いコードレビューは実施していたが、リリース規模から実機を利用したテストを実施していないため、プログラムの改修誤りを検出することができなかった。

＜対策＞
- テストツールの導入による実機と同等のテストの実施

➢ 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＞
- ◆ 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

➢ プログラミングミスによる取引失敗及びその後の不正な残高更新

＜業態＞
資金移動業者等
＜事象＞
- ○ 基幹系システムに追加した新機能におけるプログラミングミスによりカード決済処理が遅延し、タイムアウトが発生したため取引が失敗した。また、その際に自動で発動したタイムアウト防止機能の不備により、取引失敗にもかかわらず残高が減算された。

＜原因＞
- ◆ 新機能リリース前の無影響確認テスト不足により、プログラミングミスを発見できなかった。
- ◆ タイムアウト防止機能として、加盟店側のデータと同期しないまま、失敗した取引を自動取消する機能を実装していたため、残高の不整合を招いた。

＜対策＞
- ● 本番同等の開発環境を構築し、新機能リリース前の無影響確認テストを強化
- ● 決済処理プロセスを、加盟店側からの応答結果に基づき処理を行うよう変更

➢ システム設計不備による顧客情報表示の誤り

＜業態＞
暗号資産交換業者
＜事象＞
- ○ 外部事業者のプラットフォーム上で稼働するシステムの設計ミスによって、複数の顧客間で表示すべき情報が入れ替わる事象が発生した。また、本事象発生後もサービスを継続したため、同様の事象が複数回発生した。

＜原因＞
- ◆ 開発担当者が外部の事業者の提供するシステム仕様を正しく理解せず、設計ミスが発生した。また、テストケースの考慮が不足していたため、バグを発見することができなかった。
- ◆ システムの表示誤りを想定したサービス停止基準を整備していなかった。

＜対策＞
- ● 外部事業者の提供するシステムの仕様に関する情報の収集・把握
- ● システムの表示誤りを想定したサービス停止基準の整備

➢ 本番環境とテスト環境の相違に起因する設計不具合の検出漏れによる取引不可

＜業態＞
暗号資産交換業者
＜事象＞
- ○ 修正プログラムの本番適用後、取引システムへのアクセスが不可となった。

＜原因＞
- ◆ 修正プログラムに誤りが含まれていたが、所定のテストプロセスでは検出されなかった。
- ◆ テスト環境と本番環境の設定が相違していたことに起因し、テスト環境では不具合が発現しなかった。

＜対策＞
- ● テスト環境と本番環境の差異を特定し、定期的に確認
- ● 設定差異を踏まえたテストケースを策定・実施

（２）プログラム更新、普段と異なる特殊作業などから発生したシステム障害

②　設定ミス・操作ミス等の管理面・人的要因

➢　製品知識の不足に起因する障害に伴う IB の利用不可　新規

＜業態＞

主要行等

＜事象＞

○　基幹システムと周辺システムとを接続するハブシステムにおいて、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。

◆　切替のテスト工程について、利用実績のある製品を基にしたテストのみを行ったため、設定誤りに気付けなかった。

＜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

➢　口座情報の更新作業の障害に伴う ATM の利用不可　新規

＜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、基幹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

➢ 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　新規

＜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

➢ リリース作業ミスによる ATM、IB 障害

＜業態＞
地域銀行
＜事象＞
- ○ 本番環境にリリースしたプログラムに一部古いプログラムが混入。その後の再リリース作業時に必要なパラメータの設定を誤り、一部顧客の ATM、IB による残高照会が利用できなくなった。

＜原因＞
- ◆ 前回リリース作業後の作業漏れにより、削除すべき古いプログラムが放置され、今回のリリース作業において混入。リリースプログラムの不整合を示すチェックリストの確認が漏れ、事前に検知できなかった。
- ◆ 再リリース作業時に必要となるパラメータ設定方法が手順書から漏れており、誤ったパラメータを設定したことにより、一部の顧客を管理する情報が欠落した。

＜対策＞
- ● 手順書の整備により、リリース作業後の古いプログラムの削除手順や設定すべきパラメータを明確化し、作業手順書に沿った作業結果の記録、再鑑を行う態勢を構築

- リリース前作業時の不整合チェックリストの確認を修正した担当業務の担当者のみが行うのではなく、全業務の担当が確認し、管理者が最終確認する態勢を整備

➢ 本番環境と開発環境の取違えによる送金障害

＜業態＞
地域銀行
＜事象＞
○ API 連携基盤を通じて連携するスマートフォンアプリにおいて他行への送金、他行から当行への送金ができない。
＜原因＞
◆ クラウド上に構築したオープン API 連携基盤の本番環境と開発環境を取り違え、誤って本番環境の認証・認可機能に対し、外部からの接続を許可しないように設定してしまった。
◆ 開発担当者個人のアカウントに本番環境・開発環境双方の API 連携基盤の操作権限が付与されており、同一の管理コンソールから双方の環境への操作が行え、操作する環境を間違いやすい環境にあった。また、管理コンソールを操作するための具体的な運用ルールや手続きが整備されていなかった。
◆ API 連携基盤を構築するプロジェクトにおいて、サービスイン後の運用手続きを策定する作業を漏らしていた。また、クラウドという新技術による構築であることに目が向き、運用ルールや手続きに対する意識が希薄になっていた。
＜対策＞
- 本番環境への操作に関しては共通アカウントを通じて行い、作業申請書による上長の承認を受ける等、管理コンソールでの業務に関する手続きを整備
- 新たな技術を活用したプロジェクトにおいて、本番環境・開発環境のシステム運用に関する必要な作業に漏れがないかチェックする態勢を整備

➢ リリース作業の引継ぎ誤りによるサービス開始遅延

＜業態＞
金融商品取引業者（ネット証券会社）
＜事象＞
○ システムリリース後、最初の取引開始が遅延した。
＜原因＞
◆ 改修対象プログラムのリリース日が担当者間で誤って引き継がれリリース作業が行われたため、稼働すべきプログラムが稼働しなかった。

◆　リリース作業の再鑑手順にも不備があり、作業ミスを検知でなかった。

＜対策＞

- 作業者・再鑑者の役割を明確に定義
- 再鑑漏れ防止のため、作業引継ぎが必要な場合は作業者・再鑑者等の関係者による会議を開催し、メンバー全員が共通理解を持てる体制を整備

➢ **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って、一部ローンサービスにおける入金取引ができなく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

➢ **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**　**新規**

＜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

➢ **アップグレード作業未完による暗号資産の取引停止　新規**

＜業態＞
暗号資産交換業者
＜事象＞
○　当社が取り扱っている暗号資産のノード[8]のアップグレードがなされたにも関わらず、それと接続する委託先のノードのアップグレードがなされなかったため、暗号資産のノードと委託先のノードにバージョン差異が発生し、顧客資産の入出庫が実施できなくなった。
＜原因＞
◆　委託先はノードのアップグレードの期日を認識していたものの、作業依頼者が作業期限を明記しなかったため、アップグレードの期日までに作業実施者によるアップグレード作業が完了しなかった。
◆　当社はノードのアップグレード期日を認識しておらず、委託先の作業状況も把握していなかった。
＜対策＞
●　委託先による作業管理（期限設定、完了確認等）の徹底
●　当社による暗号資産のノードのアップグレードに関する情報の定期的な収集及びアップグレードに係る作業状況の管理

➢ **共通プログラムのリリースミスによる取引サービスの停止**

＜業態＞
暗号資産交換業者
＜事象＞
○　複数のシステムで共通的に利用しているプログラムを修正した際に、一部のシステムに対するリリースが漏れたまま、ネットワーク切替え作業を行ったため、クライアント側から当該システムへの通信ができなくなり、暗号資産による店頭決済ができなくなる事象が発生した。
＜原因＞
◆　複数のシステムで担当者が異なっており、システム切替え前に本プログラムのリリースが必要であることを担当者間で共有できていなかった。
◆　影響範囲の誤認識があったため、当該システムとの結合テストが漏れていた。
＜対策＞
●　共通プログラムを修正した際の修正内容、影響範囲の共有の徹底

[8]ノード：暗号資産のネットワークを構成するサーバや端末などのこと。

- 連携先システム担当者との結合テストの実施確認の徹底

（３）日常の運用・保守等の過程の中で発生したシステム障害

①　サードパーティの提供するサービス等の要因

➢　サードパーティの提供するサービスの障害による自社サービス提供不可

＜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 OTP 認証システムのエラーにより、個人 IB、法人 IB のログインが不可となる障害が発生した。
＜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
●　障害時の連絡態勢強化

➢　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＞
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

➢ **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　新規**

＜業態＞
主要行等
＜事象＞
○　新規口座開設等の機能を提供するサードパーティのサービスにおいて、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、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可否の決定

➢ **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 SSL 証明書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齟齬によって、サービスが利用できない事象が発生した。
＜原因＞
◆　サーバ証明書の期日を管理していたサーバ運用部門が、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

➢ **サードパーティの提供するサービスの障害によるスマホアプリ、一部 Web サービス提供不可　新規**

＜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、スマホアプリによる新規口座開設、スマホ・PC による住宅ローン申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

➢ **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　新規**

＜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

➢ **IB 共同センターの作業手順不備による IB 障害**

＜業態＞

地域銀行

＜事象＞

○　個人 IB、法人 IB のログインやオンライン取引ができない事象が発生。

＜原因＞

◆　IB 共同センターの中継サーバにおいて、ログファイルの容量が枯渇し、正常に稼動しなかったため。

◆　サービス提供元が行ったログファイル調査作業の手順不備により、使用可能な領域が少なくなっており、枯渇を招いた。

＜対策＞

●　ログファイル調査作業の手順見直し（調査後に容量を確保する手順を追加）

- ● ログファイルの定例メンテナンス処理のタイミングを変更
- ● ログファイルの利用可能領域の常時監視態勢の構築

➢ **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。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。
- ◆ 復旧手順の整備や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
- ● 復旧手順の整備と訓練等の実施

（３）日常の運用・保守等の過程の中で発生したシステム障害

②　ハードウェア・回線等の不具合

➢　ディスク障害に起因した送金処理等の遅延　新規

＜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

➢　OTP 認証システムの待機系切替え不良に伴う IB の利用不可

＜業態＞

主要行等

＜事象＞

○　OTP 認証システムでハードウェア障害を起因とした待機系システムへの自動切替えに失敗し IB にログインできない状態が長時間継続する事象が発生した。

＜原因＞

◆　自動切替え失敗後に対応すべき強制切替えの適用条件を明示しておらず、委託先が実施するまでに時間を要した。

＜対策＞

●　委託先における強制切替え判断手続の整備と訓練実施の徹底

➢　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

➢ **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＞

◆　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

➢ **ハードウェアの障害による終日株式売買の停止**　**新規**

＜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。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、自動切替がされない設定になっていた。また、当該設定にかか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

（３）日常の運用・保守等の過程の中で発生したシステム障害

③　設定ミス・操作ミス等の管理面・人的要因

➢　高負荷な検索作業に起因した IB におけるエラー出力　新規

＜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。

○　対象サーバの再起動に係る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

➢　社内の他組織との連携不足に起因した IB 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、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

➢ **高負荷のプログラム実行に伴う IB 利用不可**

＜業態＞
主要行等
＜事象＞
○ 高負荷のバッチプログラム実行で DB サーバの負荷が増大したことで、一部 ATM の利用不可等の事象が発生した。
＜原因＞
◆ 対象のバッチプログラムは社内レビューを行っていたが、一部の有識者の知見に依存したレビューであったため、他処理に影響する負荷の高いバッチプログラムであることを事前に認識することができなかった。
＜対策＞
● 他処理への影響、バッチプログラムの方式及び作業態勢を含む、バッチプログラム実行における網羅的なレビューの徹底

➢ **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を起因とし、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、さらに影響が拡大。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毎に実施するよう変更
● 必須処理の漏れがシステム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、それに基づく訓練の実施

➢ **委託先におけるガバナンスの欠如、自社による委託先管理の不足によるサービス停止**

＜業態＞
主要行等
＜事象＞
○ 使用している製品の不具合により、インターネットサービス、提携 ATM サービス、API 提供サービス等が利用不可となる事象が発生した。
＜原因＞
◆ 当不具合は既知のものであったが、当社との取り決め（サービス継続に影響を及ぼし得る事象の報告、対応等）に反し、ベンダーから当社に報告がされておらず、対応がなされていなかった。
◆ ベンダー側のガバナンスや体制が不十分、かつ、マネジメント層のプロジェクト管理が不十分であり、当社へ報告していない不具合があることをベンダーのマネジメント層が認識していなかった。
＜対策＞
- 不具合の影響度に応じた対応の基本方針をベンダーとともに作成。動作に影響のある不具合判明後直ちに全量を当社へ報告させ、基本方針を踏まえ、都度対応を当社と協議する運用へ変更。また、その検討結果を当社担当役員が出席する月次会議で報告
- ベンダー側において、縦割りとなっていた組織に全領域横断的に管理する役員クラスの責任者を設置

➢ **SSL 証明書[9]の期限管理不備によるウェブサイト表示不可**

＜業態＞
金融商品取引業者（ネット証券会社）、暗号資産交換業者
＜事象＞
○ 取引向けのウェブサイトが表示されない。
＜原因＞
◆ 委託先が管理する SSL 証明書の有効期限切れとなっていた。
＜対策＞

[9] 「SSL 証明書」とは、接続先のサイト運営組織の実在を証明し、Web ブラウザと Web サーバ間で暗号化通信を行うための電子証明書をいう。

- 管理対象として当該 SSL 証明書を追加し、定期的に棚卸しを行う運用を整備
- 委託先から重要情報の通知等を受動的に得るだけでなく、当社の業務計画等を委託先へ共有し、当社サービスに影響が生じる可能性のあるイベントを早期に検知する体制を整備

➢ **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する際、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

（３）日常の運用・保守等の過程の中で発生したシステム障害

④　取引量増加に伴う容量不足等

➢　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

➢　新たなサービスの特性に応じた取引量の監視対応不足によるチャージ不可

＜業態＞

地域銀行

＜事象＞

○　コード決済サービスに係る取引件数が上限値を超えたことによって、口座からのチャージができない事象が発生した。

＜原因＞

◆　キャンペーン等を起因とした急激な取引件数の増加等の、コード決済サービスの特性を考慮した上限値設定の検討や取引件数の監視を行っていなかった。

◆ コード決済サービス事業者との間で、取引件数の増加等に関するコミュニケーションを取っていなかった。

＜対策＞

- 取引件数の上限値超過の予兆に関するアラート設定
- 急激な取引数の増加が想定されるイベント時の取引件数に関する情報共有

➢ **個別の決済ルートに対する負荷テスト漏れに伴う障害　新規**

＜業態＞

資金移動業者等

＜事象＞

○ 顧客からのアクセス集中に起因して、特定の ASP サービスを経由する決済が取引エラーとなり、障害が長時間継続した。直接原因は、プログラムの不具合で、特定の決済が重なった際にデータベースがロックする事象であった。

＜原因＞

◆ 導入時のテストにおいて、原因となった特定の決済に関するテストを実施していなかった。

◆ ASP サービスの特定の決済のみを閉塞する手順が確立していなかった。

＜対策＞

- ASP サービスを含めた全てのケースの負荷テストの実施
- 障害を想定した個別決済ルートの閉塞手順や顧客周知方法の確立

➢ **システムの処理能力不足による取引処理遅延**

＜業態＞

資金移動業者等、暗号資産交換業者

＜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、システムの処理能力が不足し、取引等に時間を要する事象が発生した。

＜原因＞

◆ 取引量の見積りやシステム処理能力の事前検証が不十分であった。

＜対策＞

- 取引量の見積り方法の見直し、システム処理能力の事前検証の強化

➢ **データ格納領域不足に伴う決済等不可**

＜業態＞
資金移動業者等
＜事象＞
○ データの追加・削除等の増加に伴い、データ格納領域不足となり、決済等が不可となる事象が発生した。
＜原因＞
◆ データの追加・削除等により隙間領域が発生すること（断片化）への対応が不足していた。
＜対策＞
● 断片化を考慮したデータ格納領域設計実施
● データ格納領域の監視徹底と空き容量不足の予兆がみられた場合の対応態勢整備

➢ **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や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や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

➢ **システムの処理能力不足による取引処理遅延**

＜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。）によって、システムの処理能力が不足し、取引等に影響を及ぼす事象が発生した。

＜原因＞

◆　システムの処理能力の事前検証が足りなかった。

＜対策＞

- システムの処理能力の事前検証の徹底
- 緊急時に即時対応ができるよう体制の整備

➢ **トランザクション件数の急上昇による取引停止　新規**

＜業態＞

暗号資産交換業者

＜事象＞

○　トランザクション件数の急上昇に伴い、システムに不具合が発生したため、顧客が入庫した暗号資産を当社システムへリアルタイムに反映できなかった。暫定対応として、策定済みのリカバリ手順により当社システムへの反映を実施したものの、手順書の一部誤りによりリカバリ作業に時間を要した。

＜原因＞

◆　トランザクション件数の急上昇を見据えたキャパシティプランニングが十分でなかった。

◆　リカバリ手順書の一部に実効性が不足している点があった。

＜対策＞

- 将来の暗号資産の相場動向を予測したキャパシティプランニング方法の見直し
- 容易でかつ迅速なリカバリ対応に向けた手順書等の整備

（4）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

➢ 開発環境に対する不正アクセス　新規

＜業態＞
主要行等
＜事象＞
- ○ 委託先がパブリッククラウド上に構築した開発サーバにおいて、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

➢ 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　新規

＜業態＞
金融商品取引業者
＜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

➢ 業務委託先従業員による不正送金　新規

＜業態＞

金融商品取引業者

＜事象＞

○　業務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

➢ スマホ ATM 機能の悪用に関する不正アクセス　新規

＜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基に、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＞

●　二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

➢ 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　新規

＜業態＞

資金移動業者等

＜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起因して、悪意の第三者により、収集された個人情報等に不正アクセスされる可能性があった。

＜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）

➢ **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** **新規**

＜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関わらず、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

以上