金融機関のシステム障害に関する分析レポート

2022 年６月

金融庁
Financial Services Agency

第１部　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、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。

これらの報告等をもとに、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、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いる。

昨今、全国的に大きく報道されるような障害もあり、多くの顧客に影響を及ぼす事案が発生している。また、障害の未然防止にとどまらず、障害発生時の業務の早期復旧や顧客影響の軽減につなげていく対応が重要となる中、実効性のある組織横断的なシステムリスク管理態勢の整備や高度化に取り組む必要性は引き続き高い状況にある。[1]

したがって、本レポートでは、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。

金融機関においては、引き続き、各種ガイドライン等[2]や本レポートを活用し、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2022年３月までに報告された「障害発生等報告書」のうち、主な事案を事例集として取りまとめたものであるが、掲載し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、金融機関において、自己責任原則の下、創意・工夫し、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] バーゼル銀行監督委員会は「オペレーショナル・レジリエンスのための諸原則」等を公表しており、オペレーショナル・レジリエンスへの取組みが今後加速することが予想される。
https://www.fsa.go.jp/inter/bis/20210402/20210402.html

[2] 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」等が想定される。

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、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2021年４月から2022年３月までとして分析したものである。

第２章　主な障害傾向

昨今、システム障害により、広範囲にわたりATM等が利用できなくなるなど、多くの顧客に影響を及ぼす事案が発生している。特に、障害発生時に、準備していたシステムの冗長構成[3]が機能しないことや、障害復旧手順・体制（人材不足含む）を整備していないこと等の問題が顕在化し、復旧に想定以上の時間を要する事案が複数見られた。

こうしたことから、現状を過信することなく、経営陣の積極的な関与の下、障害発生時を想定した顧客目線での対応態勢を整備することが課題となっている。さらに、障害発生の未然防止にとどまらず、システム障害のパターンを十分に想定した上で、冗長構成に係る実効性の確保や、障害復旧手順・復旧体制の見直し、訓練等によるシステムリスク管理態勢の高度化についても課題となっている。

システム障害の発生の端緒ごとに主な事例を取りまとめ、課題を分析した結果は以下のとおりである。

第１節　システム統合・更改等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を踏まえ、プロジェクト特性に基づいたプロジェクト管理態勢の整備、旧システムの仕様に係る理解、テストケース不足に係る対応強化等を課題として取り上げている。

昨今も、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に関する障害が発生し、顧客の決済に影響を及ぼすような事例が見られた。

また、レガシーシステムにおける機能追加において、テスト不足等に起因したプログラムの不具合により、勘定系システムが停止し、顧客に影響を及ぼすような事例が見られた。

これらの障害の原因は、旧システムの仕様に係る理解不足やテストケース不足等が挙げられ、この背景としてレガシーシステムに係る有識者の高齢化等による人材不足や経営陣における現場実態の把握不足があると考えられる。

---

[3] 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。

このような背景を踏まえ、経営陣が開発現場の実態を十分に把握した上で開発を進めることや、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。

第２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

本番環境のシステムにおける設定ミス等の管理面・人的側面に起因する障害が複数見られた。特に、製品導入時におけるシステム機器の仕様に係る確認不足や、設定変更箇所の洗い出しの漏れ等による設定ミスにより、ATM等での取引ができなくなる事例も見られており、いかに設定ミスを防止するかが課題となっている。

こうしたことから、あらかじめ定めていた作業目的や業務要件を正しく作業手順に反映していること等を確認するための態勢の整備や、本番環境の実態に即したテストの実施、人事異動等で担当者を変更した場合であっても作業の誤りが発生しない仕組みの整備等により、システムの設定作業の品質を向上させること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、その後も同様の事例（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例等）が複数見られた。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。しかしながら、十分な実効性の検証を行わず、冗長構成が意図どおりに機能しなかった結果、復旧に時間を要し、顧客に大きな影響を及ぼす事例が見られた。また、トラフィックの経年的な増加やハードウェアの経年的な劣化など、障害の予兆があるにもかかわらず、こうした予兆を把握できておらず、障害を未然に防ぐことができなかった事例も見られた。

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に実効性を確保しているか、現状を過信することなく、障害の発生に備えあらかじめ検証することはもとより、障害の予兆を捉えた未然防止策を導入する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

システム障害の復旧時において、障害パターンの想定不足による復旧手順が

未整備であった事例や、システム機器の操作ミス等により、復旧までに想定以上の時間を要し、当日取引のために必要な処理の時限に間に合わず、翌営業日の処理となった事例、取り扱うデータを誤ったことなどにより、決済サービス利用時に支払が二重となるなどの顧客に影響を及ぼす事例が見られた。

こうしたことから、障害パターンを十分に想定[4]し、障害の発生箇所に着目した上で、手動切替え等の対策[5]の整備や訓練といった対応を行うことはもとより、障害発生時の顧客影響の確認方法の整備[6]や、顧客目線に立った復旧対応の早期化に係る取組み[7]が課題となっている。

Ⅲ　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障害事例を取り上げ、コンティンジェンシープラン（以下、「CP」という。）の整備や実効性の確保を課題としてきた。

昨今においても、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見られており、引き続き、サードパーティの提供するサービスの障害を想定した代替手段の確保やサードパーティとの不断の情報連携等の取組みが必要である。

第４節　サイバー攻撃、不正アクセス等の意図的なもの

金融機関やその海外現地法人等から、ランサムウェアの感染等が報告されている。金融庁では、昨今の情勢を踏まえ、本レポートの集計期間において、金融機関におけるサイバーセキュリティ対策の強化に関する注意喚起を合計３回発出しているが[8]、これらの注意喚起で求めているような基本的な対策の不備に起因する事例が見られる。連携サービスや外部委託の拡大等により、IT資産管理の範囲が拡大し、複雑化する中、基本的な対策を着実に実施するための態勢強化（いわゆるサイバーハイジーン）[9]が、引き続き課題となっている。

---

[4] 例えば、設計時の冗長構成では対応できないシステム障害（ハードウェアの多重障害等）が発生する想定も含む。

[5] 例えば、システムの強制的な切離しや副系の単独起動等の対策。

[6] 例えば、システムが複雑化・高度化する中、各システム障害がどの提供サービスに影響し、顧客利便にどのように影響するのか、連携の必要な関連部署や委託先はどこなのかといった情報を可視化する方法等の整備。

[7] 例えば、ATMにおける媒体等のくわえ込みの設定を見直す、ATM停止を想定した職員による駆け付けやその際の掲示物の事前準備、暫定払いのオペレーションの整備等の取組み。

[8] 2022年2月23日「昨今の情勢を踏まえた金融機関におけるサイバーセキュリティ対策の強化について」。
https://www.fsa.go.jp/news/r3/cyber/0224oshirase.html
2022年3月1日「金融機関におけるサイバーセキュリティ対策の強化について」。
https://www.fsa.go.jp/news/r3/cyber/0301oshirase.html
2022年3月25日「現下の情勢を踏まえたサイバーセキュリティ対策の強化について」。
https://www.fsa.go.jp/news/r3/cyber/0324oshirase.html

[9] 「金融分野におけるサイバーセキュリティ強化に向けた取組方針(Ver. 3.0)」においても新たなリスクへの備えとして言及している。https://www.fsa.go.jp/news/r3/cyber/torikumi2022.html

一方、未然防止が困難なサイバー攻撃に対して、業務や顧客への影響を許容水準内に収めるよう、経営陣も含めた訓練・テスト等を通じて、業務やサービスのレジリエンスを高める取組みも引き続きの課題である。

Ⅰ　基本的なサイバー対策の不備に係る事案

コンテンツマネジメントシステム[10]（CMS）やファイアウォールに存在する外部から悪用可能な脆弱性に起因し、複数の金融機関のウェブサイトで、不正なファイルの配置やホームページの閲覧不可、顧客情報の漏えい等の事案が発生している。

また、システム管理者が利用する情報系システムに対して、適切なセキュリティ対策を施さずインターネットに公開されていたことに起因し、ランサムウェアの被害や個人情報を窃取されるといった事案も報告された。

これらの対応として、利用する製品やソフトウェアのバージョンといった構成情報やシステム環境を平時から把握し、脆弱性の有無と外部からの悪用可否等を確認することに加え、不正アクセス発生時の対処手順をあらかじめ備え、定期的な訓練等による対応の実効性を確保することが引き続き課題となっている。

Ⅱ　マルウェア感染に係る事案

金融機関がエモテット[11]に感染する事例が非常に多く発生している。

これらの対応として、マクロ実行の無効化、不正な外部サーバーとの通信制御等のマルウェア対策、不審メール受信時等の対応態勢整備はもとより、定期的な訓練等による対応に係る実効性の確保が引き続き課題となっている。

第３章　今後の金融庁の取組み

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

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。

---

[10] ウェブサイトのコンテンツを統合的に管理し構築するシステム。

[11] マクロ付きのExcelやWordファイル、あるいはこれらをパスワード付きZipファイルとしてメールに添付する形式等で配信され、ファイルを開封後に、マクロを有効化する操作を実行することで感染につながるマルウェア。感染後はメールやメールアドレス等の情報を外部に送信する。悪意ある攻撃者は窃取した情報をもとに、当該金融機関の組織内外に当該金融機関をかたったメールを送信することで、新たな受信者による二次感染が発生する。

第１節　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新型コロナウイルス感染症の影響によるITサービスを利用する顧客の増加等といった顧客の動向変化は、利便性の向上と引き換えに情報システムへの依存度を高めており、大規模なシステム障害が頻繁に発生すれば、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高まっている。

金融庁では、金融機関のシステムの安定稼働に向けて、重大な顧客被害や金融機関のシステムリスク管理態勢に問題が見られる場合は、検査を含め、重点的に検証するなど、実効的かつ効果的なモニタリングを進めてきたところである。

昨今の状況を踏まえ、今後も、こうした取組みを継続するとともに、障害の未然防止にとどまらず、障害発生時の業務の早期復旧や顧客影響の軽減に向けた対応が行われるようモニタリングを実施していく。

第２節　システム統合・更改等に関するモニタリング

2022年度も、将来を見据えた大規模なシステム更改やクラウド環境への移行等のプロジェクトが金融機関において進められる予定である。

これまで、大規模プロジェクト等に関する経験が少ない金融機関の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、こうした取組み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。

第３節　サードパーティの提供するサービス等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は、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、金融機関の取組みの参考とするため、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。

第３部　事例集

第１章　業態全体の障害傾向（事象別）

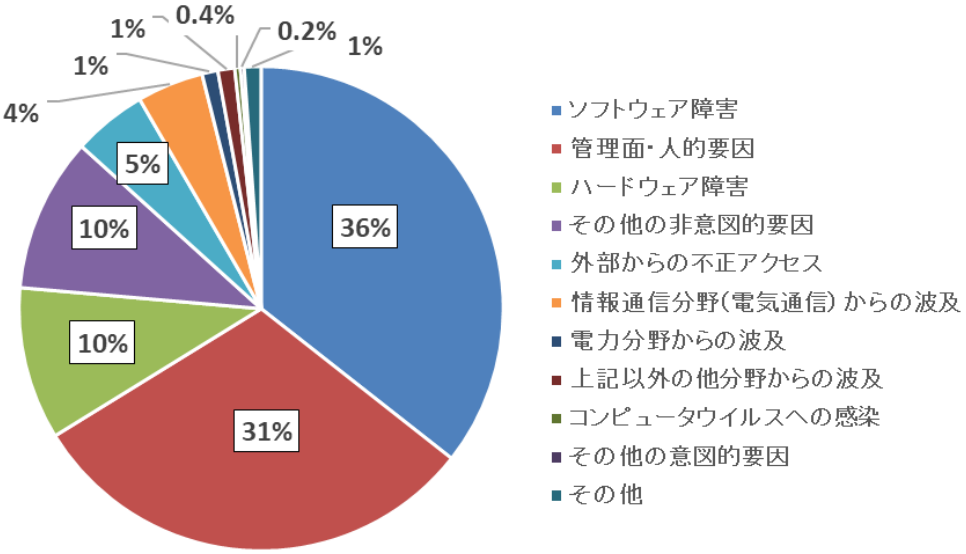
業態全体[12]の障害傾向（事象別）として、「ソフトウェア障害」と「管理面・人的要因」による障害が全体の３分の２を占めている[13]。

「ソフトウェア障害」について、金融機関から、設計時の考慮不足やテスト観点・項目不足等に起因するインターネットバンキング（以下、「IB」という。）　障害や決済遅延等の報告が行われている。

「管理面・人的要因」による障害について、金融機関から、委託先を含む本番システムでの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、トラフィックの経年的な増加といった障害の予兆を把握できず顧客サービスへの影響を未然に防げなかった障害等の報告が行われている。

なお、「ハードウェア障害」については、金融機関から、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いなど、冗長構成が意図どおりに機能しなかった障害等の報告が行われている。

図表1「障害事象別割合（全業態）」



---

[12] 本集計期間（2021 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 1,700 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）。前回集計期間（2020 年度）の約 1,500 件から増加した一因として、当局からのサイバー攻撃に関する注意喚起等の発出を踏まえ、金融機関において障害対応や報告に対する意識が高まったことがあると考えられる。

[13] 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。

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、本事例については、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[14]、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　システム統合・更改に伴い発生したシステム障害

１．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新規

＜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

２．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新規

＜業態等＞

主要行等

＜事象＞

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

＜原因＞

◆　データベースの設計内容（型指定等）を誤認したまま開発を進めたこと

---

[14] 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。

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

３．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

４．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＞

〇　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[15]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

５．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＞

〇　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

６．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＞

---

[15] 「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。

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

７．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

８．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

９．IT 部門と業務部門の連携不足による祝日設定の誤り 新規

＜業態等＞

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２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．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新規

＜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[16]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、設定項目の明確化や再鑑観点の具体化等についての多層的なチェック態勢の構築

２．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＞

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

---

[16] 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。

を整備

３．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

４．ネットワーク機器の設定ミスに起因した自行ATMの停止新規

＜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

５．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

６．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

７．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

８．アップグレード作業未完による暗号資産の取引停止

＜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[17]のアップグレードがなされたにもかかわらず、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

---

[17] 暗号資産のネットワークを構成するサーバーや端末等のこと。

第２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．本番環境を想定したテストケースの不足に起因するIBの利用不可新規

＜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又は対応が難しい場合は実効性あるテストケースでの検証を実施

２．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

３．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

４．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体制の再検証、大規模障害の訓練の定期的な実施

５．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

６．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

７．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

８．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

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．復旧手順の準備不足による障害対応時間の長期化新規

＜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、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の策定などを通じて、対外告知や顧客対応を整備

２．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の利用不可新規

＜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

３．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

新規

＜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の、監視内容の見直し

４．ディスク障害に起因した送金処理等の遅延

＜業態＞

主要行等

＜事象＞

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

＜原因＞

◆　サービス復旧手順や対応態勢を構築していなかった。

◆　システムを横断した障害シナリオを想定しておらず、業務面の影響範囲を特定できなかった。

＜対策＞

●　システムの重要度に応じた復旧態勢と手順の確立

●　障害発生のタイミングや影響する業務等を考慮した精緻な障害シナリオにもとづく対応手順の整備と訓練の実施

５．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

６．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＞
◆　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

７．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新規

＜業態＞
地域銀行

＜事象＞

○　法人 IB の委託先において、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

８．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。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．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新規

＜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）

２．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新規

＜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

３．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新規

＜業態＞

信用金庫・信用組合等

＜事象＞

○　口座振替の処理停止に起因し、一部為替発信処理ができない事象が発生した。

＜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

４．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

５．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、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

６．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、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

７．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

８．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 新規

＜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的な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など、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．様々なネットワーク障害を想定した冗長構成の未整備新規

＜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

２．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、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
●　障害時の連絡体制強化

３．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

４．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の決定

５．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＞

〇　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[18]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

６．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

＜業態＞

地域銀行

＜事象＞

〇　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

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

＜業態＞

地域銀行

＜事象＞

---

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

○　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

８．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

９．バージョンアップの影響評価不十分による取引システムへのログイン不可

新規

＜業態等＞

暗号資産交換業者

＜事象＞

○　クラウドサービス上の構成管理ツールに内在した欠陥（バグ）によって、取引システムの再起動処理が失敗したため、顧客がログインできない状態となった。

＜原因＞

◆　構成管理ツールに欠陥があること、及び当該欠陥の修正バージョンが提供されていることを認識していたにもかかわらず、影響評価を行うため

の情報収集が不十分であった。そのため、影響がないと誤った判断をし、当該ツールの入替えを実施していなかった。

＜対策＞

- パッケージ製品や外部サービスのバージョンに関する幅広い情報収集と評価プロセスの見直し

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．取引集中に備えた対策の不備による送信の時限超過新規

＜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

２．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

３．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

４．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

５．新規暗号資産販売時の負荷検証不足による処理停止新規

＜業態等＞

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　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．開発環境に対する不正アクセス

＜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

２．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新規

＜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って第三者による不正アクセスを受け、ホームページが閲覧不可となった。

＜原因＞

◆　利用ソフトウェアの脆弱性情報の収集や対応を適時に実施していなかった。

◆　インターネットに公開する必要のないプログラムが公開状態であった。

＜対策＞

●　脆弱性情報の収集や対応（脆弱性試験やパッチ適用等）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

３．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

おそれ新規

＜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

４．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新規

＜業態等＞

金融商品取引業者等

＜事象＞

○　インターネットを経由して顧客のシステムが接続して利用するサービスにおいて、運用上不要であるRDP機能[19]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[20]に感染した。

＜原因＞

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

＜対策＞

---

[19] 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。

[20] 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。

- 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

５．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

＜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

６．業務委託先従業員による不正送金

＜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

７．マルウェア被害対策の不備に起因したエモテット感染新規

＜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＞

- ● 最新の実例等を踏まえた訓練及び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

８．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

９．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起因して、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）

10. 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 新規

＜業態等＞

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

11. 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

以上