

# 金融機関のシステム障害に関する 分析レポート

令和元年 6 月



## 目次

【はじめに】	1
（留意事項）	1
【障害分析概要】	3
1. 集計期間	3
2. 主な障害傾向	3
（1）業態共通	3
① サードパーティに起因する障害（新たなサードパーティリスクへの対応）	3
② レガシーシステムにおける有識者不足に起因する障害	3
③ システム統合・更改に関する障害	4
④ 取引量増加に起因する障害	4
（2）業態固有	4
① 暗号資産交換業者における障害	4
② 資金移動業者等における障害	5
③ 金融商品取引業者（ネット証券会社）における障害	5
3. 今後の金融庁の取組	6
① デジタライゼーションの進展に伴う新たなサードパーティリスクへの対応	6
② IT人材戦略策定への対応	6
③ システム統合・更改に関するモニタリング結果（事例集）の公表	6
④ システムの安定稼働に向けた継続的なシステム障害対応	6
【事例集】	7
1. 業態全体の障害傾向（事象別）	7
2. 事例	8
① サードパーティに起因する障害	8
② レガシーシステムにおける有識者不足に起因する障害	10
③ システム統合・更改に関する障害	13
④ 取引量増加に伴う障害	16
⑤ 委託先に起因する障害	18
⑥ 作業手順誤りに起因する障害	21
⑦ 固有の商品特性の理解不足に起因する障害	27
⑧ 設計時の基本的な事項の考慮漏れに起因する障害	28

## 【はじめに】

近年の IT やデジタルライゼーションの進展、クラウドサービスの利活用や API<sup>1</sup>によるシステム間連携の増加、サイバー攻撃の高度化等に伴い、業務上の特性から、IT システムを広範囲に利用している金融機関においては、新たなリスクの顕在化が窺われている。

また、銀行法や資金決済法等の関連法規の改正やデジタルライゼーションの進展等により、電子決済等代行業者、資金移動業者や暗号資産交換業者等の金融サービスを提供する新たなプレイヤーが増加するとともに、当該業態におけるシステム障害の発生件数も増加してきており、システムリスク管理態勢の整備や高度化の重要性がますます高まってきている。

金融庁では、監督指針に基づき、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。

これらのシステム障害を分析したところ、デジタルライゼーションの進展等に伴う IT システムへの依存の深化や情報セキュリティを含むシステムリスクの多様化によって、サードパーティ<sup>2</sup>を含めた新たなリスクが顕在化した事例がみられた。

こうした状況を踏まえ、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、システム障害に関する分析結果が参考になると考え、この度、本文書に業態共通・業態固有の主な障害傾向と障害事例（事象、原因、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、今後予定されている金融検査マニュアル廃止後も、引き続き一般に存在する各種ガイドライン等<sup>3</sup>や本文書を活用し、金融システムの安定化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）

本文書の個々の事例は、平成 30 事務年度（平成 30 年 7 月から 31 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。

したがって、本事例のみを活用して、システムリスク管理に取り組むことで、システムリスク管理が適切に機能することを担保するものではないことに留意する必要がある。

このため、本事例は、各金融機関において、自己責任原則の下、創意・工夫を十分に

---

<sup>1</sup> 「API (Application Programming Interface)」とは、あるアプリケーションの機能や管理するデータ等を他のアプリケーションから呼び出して利用するための接続仕様・仕組みをいう。

<sup>2</sup> 「サードパーティ」とは、業務上の関係や契約を有する組織をいう。

<sup>3</sup> 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。

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、あくまで参考とすることを想定しているものである。したがって、個々の事例を形式的に適用したり、チェックリストとして用いたりすることは望ましくない。

なお、金融庁のシステムリスク管理に係るモニタリングにあたっては、令和元年6月公表の「金融機関のITガバナンスに関する対話のための論点・プラクティスの整理」の「V. 従来のシステムリスク管理」に基づき、金融機関の規模・特性等を十分に踏まえた議論を行う。

また、金融機関からの「障害発生等報告書」等の中で得られた有益な事例については、今後も公表可能な範囲で引き続き公表していく。

## 【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、本文書については、「障害発生等報告書」の集計期間を平成30年7月から31年3月までとし分析したものである。

### 2. 主な障害傾向

#### (1) 業態共通

##### ① サードパーティに起因する障害（新たなサードパーティリスクへの対応）

複数の金融機関において、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認証（以下、「OTP 認証」という）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。

その際、ATM や店頭に誘導するといったコンティンジェンシープラン（以下、「CP」という）を発動したものの、実効性が乏しいといった課題が認められた。

また、上記の障害事例のほかにも、サービス提供元のシステム障害により IB が利用できなくなった事例や通信機器のソフトウェア証明書の有効期限切れによる通信障害等、複数の障害が発生しており、デジタルライゼーションの進展に伴い、今後もますます起こり得るものとして、対応策の検討が課題であると考えられる。

例えば、本事案では、CP の課題としては、2つの側面があると考えられる。

- ・ IB 等の新しいサービスの重要性や特性に応じた CP になっていない（IB のみ利用する顧客が増えていることや店舗が周辺にないために IB を利用する顧客がいるといった点を考慮せず、単純に IB が復旧するまで待つ、あるいは、店舗誘導という代替案があるからよしとするといった実効性のない CP になっている）。
- ・ 委託先の使用するシステムのパーツの特殊開発やパスワード等の把握困難な事象による障害発生が常に起き得ることを想定した CP になっていない。

したがって、新たなサービスの重要性や特性を取り込んだ CP の見直しや管理掌握が困難な事象による障害発生を見込んだ CP の見直し、また、このようなデジタルライゼーションの進展に伴う新たなサードパーティリスクへの対応が課題であると考えられる。

##### ② レガシーシステム<sup>4</sup>における有識者不足に起因する障害

---

<sup>4</sup> 「レガシーシステム」とは、技術革新による代替技術が広く普及している中、旧来の技術により構築されているコンピュータシステムをいう。

今事務年度において、システム障害の復旧作業やシステム環境の変更作業等に関する本番システムでの作業手順誤りにより、システム停止やオンライン開始時間の遅延等、顧客に影響を及ぼすシステム障害が複数認められた。

これらの障害の原因には、勘定系システムの共同化やレガシーシステムの有識者の高齢化等による有識者不足が背景にあることが見受けられ、有識者不足を補完するための作業手順書の改善や有識者の育成等が今後の課題であると考えられる。

特に、障害復旧等に関する手順については、障害対応機会も少なく、かつ、より専門的なノウハウを必要とするため、有識者に依存しているケースが多いことが推察される。こうした中、既存の手順書の見直しの必要性を十分に検討し、既存の手順書では不十分である場合は、見直しを実施することや手順を見直した場合は、実効性確保のため、可能な限り訓練を実施すること等が課題であると考えられる。

### ③ システム統合・更改に関する障害

システム統合・更改は、大規模プロジェクトであること、専門性が非常に高いこと、日常的に経験できるものではないこと等の特質が考えられ、経験不足やプロジェクト管理態勢の整備が不十分のままプロジェクトを開始したこと等に起因し、ネット銀行等において、新システム稼働後に多くの障害が発生し、ATMの取引不能、残高情報の誤更新といった顧客サービスに影響を及ぼすシステム障害も認められた。このため、今後、システム統合・更改を進める金融機関において、プロジェクト開始前に、事前にプロジェクト管理態勢の整備等を行うことが課題であると考えられる。

### ④ 取引量増加に起因する障害

スマートフォン等のスマートデバイスによる資金決済、全銀システム接続時間拡大対応等の利便性向上やキャンペーン等のイベントによる取引量の増加に伴い、システムカウンターの上限值超過、システムの処理能力不足により、システム停止等の顧客サービスに影響を及ぼすシステム障害が複数認められた。このため、今後、2020年東京オリンピック・パラリンピック競技大会等のイベントによる一時的な取引量の増加も考慮した上で、システムカウンター上限値、システムの処理能力、データ保存容量等について、事前検証を行うことが課題であると考えられる。

また、貸金業において、不正オーソリ<sup>5</sup>の大量集中によるエラーデータ容量の超過が発生しており、このような非意図的要因による不測の事態へのシステム対処やCPの実効性の検証等も課題であると考えられる。

## (2) 業態固有

### ① 暗号資産交換業者における障害

---

<sup>5</sup> 「オーソリ」とは、オーソリゼーションのことで、クレジットカード加盟店がカードで決済処理を行う際に、取引金額に対して当該カードが利用可能かカード発行会社に確認し、その金額の利用枠を確保する手続きをいい、「不正オーソリ」とは不正なカード情報を含むオーソリをいう。

暗号資産交換業者の障害を事象別に分析したところ、プログラムの誤りや作業ミス等により、取引ができなくなるなど顧客サービスに影響を及ぼすシステム障害が複数認められた。暗号資産技術特有の問題点に起因する事案は少なく、設計考慮漏れといった、一般的なシステムの品質管理態勢が不十分であることに起因するものが大半を占め、業容に比べてシステム担当者が不足していた事例もみられた。適正な人員の確保、設計・製造におけるレビュープロセスの改善、障害の真因分析や再発防止策の立案といった、システム品質に関わる管理態勢の改善が課題であると考えられる。

## ② 資金移動業者等における障害

資金移動業者等の障害を事象別に分析したところ、作業ミス等により、決済サービスが利用できなくなるなど顧客サービスに影響を及ぼしており、以下のような傾向や課題であると考えられる事項が認められた。

また、障害原因の分析が十分でないため、適切な再発防止策となっていない事例がみられた。このため、障害の真因分析を行い、再発防止策を立案することが必要である。

- ・ システム移行時等に作業手順書を作成しておらず作業ミスに繋がった事案やシステム能力増強のためのサーバー追加時の本番移行作業ミス等、作業手順書未作成や再鑑不足を主な原因とする障害が認められた。したがって、システム移行時等の作業手順書作成、作業手順再鑑の徹底といった作業品質確保への取組みが課題であると考えられる。
- ・ 要件の考慮不足やプログラミングミス等、設計・製造時の不備に起因する障害が認められた。それぞれの工程でのレビューや埋め込んだ不具合を未然に発見するために本番同等の環境で網羅的なテストを実施するなどのテストの強化が課題であると考えられる。
- ・ 委託先の対応漏れによるシステム障害を起因とし、顧客サービスに影響を及ぼす障害も認められたため、今後、委託先管理の強化が課題であると考えられる。

また、子会社が親会社のシステムを活用し、金融サービスを提供しているため、本来であればグループとしてシステムリスク管理態勢等を整備すべきところ、グループとしてのリスクアセスメントを実施しておらず、システムリスク管理態勢が十分でない可能性がある先も見受けられた。今後、金融サービスを提供するために利用しているシステム（機能）を網羅的に把握し、グループとして、システムリスク管理態勢の整備等を行うことが課題であると考えられる。

## ③ 金融商品取引業者（ネット証券会社）における障害

金融商品取引業者の障害を事象別に分析したところ、ソフトウェア障害、管理面・人的要因による障害が太宗であった。特にネット証券会社からの報告件数が多く、これは、日頃から頻繁に新機能の追加や機能改修を行っており、取り扱う商品に複雑な特性をもったものが多いことなどの背景が考えられるものの、一方で、作業ミスや設計誤りによる障害も認められており、手順書の一部未整備や再鑑の未実施、システム変更の影響調査漏れ等に課題があると考えられる。

### 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みを実施する。

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 デジタライゼーションの進展に伴う新たなサードパーティリスクへの対応

「2. 主な障害傾向」に記載した新たなサードパーティリスクへの対応について、関係団体等と連携し、サードパーティリスクへの対応に関する CP 見直しについて検討を進める。また、デジタライゼーションの進展に伴い潜在する新たなサードパーティに関するシステムリスクとその対策の調査検討を行っていく。

#### ② IT 人材戦略策定への対応

有識者不足への対策として、例えば、これまで有識者に依存していた障害復旧手順を「見える化」し、有識者不足を補完する代替手段の検討や IT 人材の確保・育成をどのように行っていくかなど、IT 人材戦略の策定・実行が重要である。こうしたことから、IT ガバナンスの対話等を通じて、デジタライゼーション進展も視野に入れた IT 人材戦略に係る取組について議論していく。

#### ③ システム統合・更改に関するモニタリングレポートの公表

各金融機関が経験の少ない中で大規模なシステム統合・更改に取り組んでいく上で、金融庁のシステム統合・更改に関するモニタリングで金融機関が気付いた課題事例（業態等、課題事項、原因、対策）が参考になると考え、取りまとめて公表する。

#### ④ システムの安定稼働に向けた継続的なシステム障害対応

システムの安定稼働に向け、継続的に障害対応を行うとともに、業態特性やシステム障害による顧客への影響度等を踏まえ、必要に応じ原因・事後改善策のヒアリングや事後改善策の実施状況等のモニタリングを実施する。



## 【事例集】

### 1. 業態全体の障害傾向（事象別）

業態全体の障害傾向（事象別）として、「ソフトウェア障害」と「管理面・人的要因」による障害が約6割を占めた。

「ソフトウェア障害」について、クレジットカード業務を営む貸金業者において、クレジットカード発行元のソフトウェア障害により同時に複数の障害が報告されている。

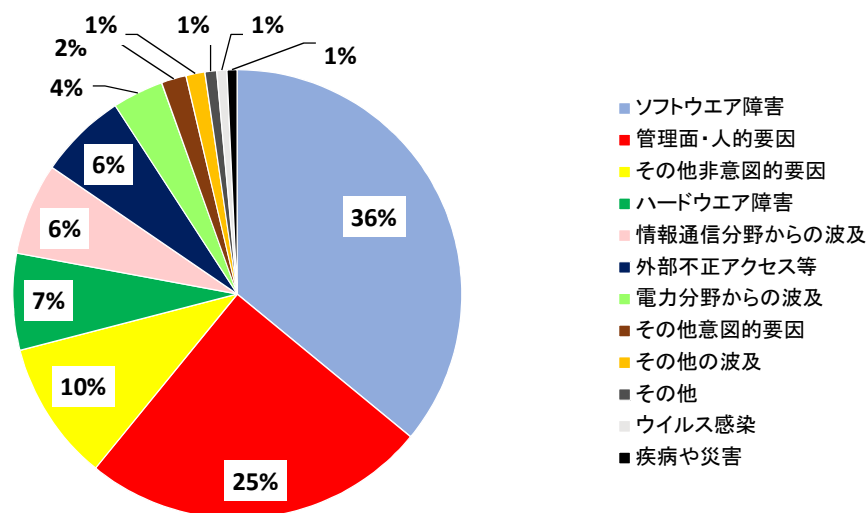
また、ネット証券会社において、常に値が動く有価証券を扱うため、わずかな取引遅延等が顧客影響につながり得ることや新機能の開発が盛んであり日常的に新規リリースを行っていることから、時価情報の表示誤り等の軽微な障害が複数報告されている。

その他、今事務年度において、預金取扱金融機関で大規模制度案件（全銀システムの稼働時間拡大）があり、ほとんどの預金取扱金融機関が対応を行ったことから、本件に関連した障害が複数報告されている。

「管理面・人的要因」による障害について、システムリソースの追加やシステムへのデータ登録作業等の本番システム作業時に、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等、顧客サービスに影響を及ぼした障害が報告されている。

その他の障害事象の傾向について、「その他非意図的要因」による障害として、貸金業において不正オーソリの集中発生によるソフトウェア障害により、同時に複数の障害が報告されている。

図表1 「障害事象別割合（全業態）」



## 2. 事例

### ① サードパーティに起因する障害

#### ➤ サードパーティサービスの障害による自社サービス提供不可

##### <業態等>

主要行等、地域銀行、信用金庫及び信用組合

##### <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
- 障害時の連絡体制強化

#### ➤ リスクベース認証<sup>6</sup>サービス提供元のミスによる個人IBログイン障害

##### <業態等>

地域銀行

##### <事象>

- 個人IBログイン時に、リスクベース認証を導入したが、ログインできない事象が発生。

##### <原因>

- ◆ リスクベース認証のサービス提供元から配信された、アクセス元の機器(PC、スマートフォン、携帯電話)を判定するための情報を格納するファイルの形式不備。
- ◆ サービス提供元の人的ミスにより、ファイル形式を誤った。

##### <対策>

- サービス提供元におけるファイル作成プロセスの見直し(作業マニュアル、確認手順の見直し)
- 配信されたファイルの本番適用前の事前検証

<sup>6</sup> 「リスクベース認証」とは、利用者の環境、IPアドレス、取引時の行動パターン等を分析し、普段と異なる環境からのアクセスである等、リスクが高いと判断された場合に追加認証を行う認証方式をいう。

➤ IB 共同センターの作業手順不備による IB 障害

＜業態等＞

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ーにおいて、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

## ② レガシーシステムにおける有識者不足に起因する障害

### ➤ 有識者不足による振込等のサービス提供不可

#### <業態等>

地域銀行

#### <事象>

- システム開発における設計ミスによるソフトウェア障害のため、振込等のサービスができなくなった。

#### <原因>

- ◆ 主な原因としては、設計レビューを行う有識者が不足しており、有識者を設計レビュー体制に組み込むことができず、設計誤りを摘出できなかった。
- ◆ また、有識者が参画していない状況で設計レビューを実施、完了としており、レビュー体制等に関するプロジェクト管理が不十分であった。

#### <対策>

- 資金決済等の重要機能のレビュー時に有識者を参画させることを規定（有識者の作業状況（作業負荷等）を上位管理職が適切に管理徹底することが前提）
- 有識者不足により、不足するスキル領域を明確にするとともに、システム開発要員等のスキル評価を行い、不足するスキル領域等をカバーするための人材育成計画の見直しを実施

### ➤ 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

#### <業態等>

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
- 必須処理の漏れが系統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

➤ システム及び処理に係る仕様の認識不足、ドキュメント化の不足による振込遅延

<業態等>

主要行等

<事象>

- 使用している製品の不具合を起因として、振込サービスの遅延等が発生した。

<原因>

- ◆ 製品不具合に係る障害回復にあたり、手順書に複数の不備があり、監視システムの停止、滞留データの未処理を発生させてしまった。
- ◆ リカバリ対象データの抽出にあたり、設計や実装状況を確認することなく、抽出してしまった結果、対象に漏れが発生した。

<対策>

- 手順書の記載詳細化、作業順序や禁止事項等の留意事項の明記
- 本障害の発生箇所において発生し得る他の障害ケースも含め、リカバリ対象データの抽出等の対応手順を整備

➤ 手順書記載の不足及び障害対応不備による表示不正

<業態等>

金融商品取引業者（ネット証券会社）

<事象>

- 夜間バッチ処理とオンライン取引が競合し、オンライン取引側でタイムアウトが発生。その復旧作業を誤ったことで、約定通知等が遅延。また、復旧作業に時間がかかったことにより、残高等に誤った金額が表示され、その誤った情報に基づき一部顧客が返済等を行ったため、原状回復等の対応が必要となった。

<原因>

- ◆ 特定の条件下において一部の夜間バッチ処理に時間を要する場合があります、競合したもう一方の処理における排他制御の解放待ちが長時間に及んだ。
- ◆ 復旧作業手順に考慮不足があり、オンライン取引の復旧前に一部サービスを再開したことで、約定データ等に不整合が発生した。
- ◆ システム障害に対する CP の整備が不十分であった。

<対策>

- 特定条件下の夜間バッチ処理の性能改善
- インシデント発生時の意思決定系統の見直し、関係者間の情報共有方法の改善
- リスクの高いシステム処理タイミングの洗出し、システム障害に対する CP の整備・訓練

### ③ システム統合・更改に関する障害

#### ➤ 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

<業態等>

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

<業態等>

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>

- ◆ 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>

- 勘定系データベースサーバーがダウンし、ATMの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ーがダウンした。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（ナレッジの共有を含む）
- 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<sup>7</sup>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次障害が発生してしまった。

<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。
- ◆ 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>

- チェックリストに実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

<sup>7</sup> 「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。



## ➤ ネットワーク接続変更作業の管理ミスによる取引障害

### <業態等>

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、承認するプロセスとすることを明確化

#### ④ 取引量増加に伴う障害

##### ➤ カウンター上限値超過によるシステム停止

###### <業態等>

主要行等、資金移動業者

###### <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

##### ➤ システムの処理能力不足による取引処理遅延

###### <業態等>

資金移動業者、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

➤ 業容拡大に伴い急増した事務作業の漏れによる支払不可

＜業態等＞

資金移動業者

＜事象＞

- 新たな支払先の追加に伴う事務作業の一部が漏れたことで、それらの支払先への支払が不可となる事象が発生した。

＜原因＞

- ◆ 業容拡大に伴い、行うべき事務作業が大量に積み上がっていた中、システムへの支払先の新規登録作業を失念した。また、再鑑及び一連の作業の完了確認を行っていなかったため、登録作業が行われていないことに気付けなかった。

＜対策＞

- 支払先の新規登録のための一連の作業工程が完了したことを確認するチェックリストの作成及び再鑑を必須化
- 連携してサービスを提供している外部サービス企業へ作業完了時に連絡を行う運用とし、当社と外部サービス企業の双方でチェック体制を整備

➤ 不正オーソリの大量集中発生によるキャッシングサービス利用不可

＜業態等＞

貸金業者

＜事象＞

- 不正なショッピング取引を含む大量の不正オーソリが発生し、キャッシング取引が利用できなかった。

＜原因＞

- ◆ 大半が不正なカード情報を含むオーソリであったため、大量の取引エラーが発生。取引エラーデータを一時格納するデータベースの容量超過によりタイムアウトが発生し、オーソリ判定処理が遅延。
- ◆ オーソリ処理遅延・停止の場合、ショッピング取引は一定条件での代行判定を行っているが、キャッシング取引は代行判定は行っておらず、キャッシング取引のみ利用不可となった。

＜対策＞

- 取引エラーデータを一時格納する容量を拡張

## ⑤ 委託先に起因する障害

委託先において、製品上の既知の不具合を修正する必要があったが、委託先で修正要否の判断等を行う態勢が的確に機能しておらず、不具合を修正できていなかったことにより、インターネットサービスやATMサービスが利用できなくなるシステム障害が認められた。このため、委託元において、委託先のシステム管理態勢等が整備され、的確に機能しているかについて、継続的に確認を行うことが課題であると考えられる。

また、委託先のシステムを利用等している場合において、委託先のシステム障害により、委託元の顧客サービスに影響を及ぼしている障害が複数認められている。委託先のシステムを利用する場合は、事前に委託先管理について十分な検討を行うことや委託先のシステム障害により顧客サービスに影響を及ぼした場合等におけるCPの策定等が課題であると考えられる。

### ➤ 委託先における基本ソフトウェアの既知の不具合対処漏れによるサービス停止

#### <業態等>

資金移動業者

#### <事象>

- 委託先のシステムの既知の不具合（データベースマネジメントシステム等不具合）への修正対応漏れにより、利用していたシステムが障害となり、入金、残高照会等のサービスができなくなる事象が発生した。

#### <原因>

- ◆ 委託先において、データベースマネジメントシステム等の製品上の既知の不具合を修正する必要があったが、委託先で修正要否の判断等を行う態勢が未整備であり、委託元において、委託先管理（委託先のシステム管理態勢等）が不十分であった。

#### <対策>

- 委託先管理の強化（委託先のシステム管理状況の把握と委託業務の遂行状況の確認等）

### ➤ 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

#### <業態等>

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体制に全領域横断的に管理する役員クラスの責任者を設置

➤ 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

<業態等>

資金移動業者

<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

➤ システムインフラ提供元との連携不足によるウェブサイトアクセス不可

＜業態等＞

資金移動業者

＜事象＞

- システム更改における考慮漏れの結果、移行後のウェブサイトへアクセスできなくなる事象が発生した。

＜原因＞

- ◆ システム更改のための影響調査、移行作業等において、ウェブサイトのインフラ提供元である親会社との連携不足により、調査結果の誤りに気付かないまま移行を実施してしまった。

＜対策＞

- ウェブサイト更改における開発手順（影響調査、体制整備、移行作業等）の文書化
- 親会社及び開発委託先との情報共有の実施

## ⑥ 作業手順誤りに起因する障害

システムリリース時の資材（プログラム等）のバージョン管理不備、システム登録作業時の再鑑漏れ等に起因する障害が複数認められ、システム部門だけでなく業務部門によるものも散見された。システム作業時の不備抑制や障害発生時の迅速で的確な対応のための、運用マニュアル、障害発生時の対応手順書、CP等の整備や再鑑の実施等が課題であると考えられる。

### ➤ 各種作業手順誤りによるサービス停止

#### <業態等>

資金移動業者、暗号資産交換業者

#### <事象>

- システムリソースの追加やシステムへのデータ登録作業の作業手順誤りにより、システムの停止や振込が行えなくなる事象が発生した。

#### <原因>

- ◆ システムリソースの追加やシステムへのデータ登録作業に関する作業手順書を作成していない。また、作業手順の再鑑を実施していなかった。

#### <対策>

- 作業手順書作成、作業手順の再鑑の徹底

### ➤ ジョブスケジュールの設定誤りによる ATM 利用不可

#### <業態等>

資金移動業者

#### <事象>

- 累積データがディスク容量を占有し、データベース処理が停止したことで、ATMの利用ができなくなる事象が発生した。

#### <原因>

- ◆ 累積データのメンテナンスを行うジョブのスケジュール設定を作業者が誤った。
- ◆ データベース処理の異常を事前に検知する手段がなかった。

#### <対策>

- 作業時に作業内容の再鑑を行う運用へ変更
- データベース処理の動作を監視し事前にアラートを発報する機能を追加

➤ システム環境変更作業時の事前の作業手順検証不足による ATM 開局遅延

＜業態等＞

信用金庫及び信用組合

＜事象＞

- 基幹系システムの環境変更作業の際に、ATM 停止に係る手順を誤り、作業翌日の ATM の開局が遅延した。

＜原因＞

- ◆ システム環境変更作業の実施にあたり、事前の作業手順検証が不十分であった。

＜対策＞

- 作業手順書の事前検証及び記載内容の詳細化の徹底

➤ リリース作業の引継ぎ誤りによるサービス開始遅延

＜業態等＞

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もてる体制を整備

➤ リリース資材のバージョン管理不備による約定金額不正

＜業態等＞

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、特定の時間帯にのみ取引金額が二重計上された状態となり、それに伴い、売却金額が過剰あるいは買付金額が不足する状態となった。

＜原因＞

- ◆ リリースする資材のバージョン管理のために資材に付与する ID の採番に不備が



あり、新資材の ID として、既にリリース済みの別資材の ID を付与してしまった結果、別資材が上書きされた。

<対策>

- 資材 ID を一元管理するシステムを構築・運用することで ID の不備を防止
- 委託先に資材の差分確認結果やリリース手順等のレビュー記録を作成させ、当社自身もそのレビュー結果の確認を徹底

➤ SSL 証明書<sup>8</sup>の期限管理不備によるウェブサイト表示不可

<業態等>

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>

- 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

➤ ネットワーク機器増設時の作業ミスによる Web システム全面停止

<業態等>

貸金業者

<事象>

- ネットワーク機器増設時の作業ミスによりインターネットを介した顧客サービスを含む Web システムが全面停止した。

<原因>

- ◆ ネットワーク機器増設作業において作業手順書に沿った作業について、再鑑を行わず、誤りを看過。LAN ケーブルの接続を誤り、ループが発生した。
- ◆ 障害発生後、あらかじめ定めた復旧作業により復旧しないことが判明した時点で作業員が上席への報告を行わず、独断で復旧作業を継続し、復旧に時間を要した。

<対策>

<sup>8</sup> 「SSL 証明書」とは、接続先のサイト運営組織の存在を証明し、Web ブラウザと Web サーバー間で暗号化通信を行うための電子証明書をいう。

- 作業手順書に沿った作業結果の記録、再鑑を行う態勢の構築
- 障害発生時の上席への報告基準を明確化

#### ➤ リリース作業ミスによる ATM、IB 障害

##### <業態等>

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

#### ➤ 作業指示書の記載ミスによる ATM 提携サービスの誤停止

##### <業態等>

地域銀行

##### <事象>

- クレジットカード取引の提携先から ATM 提携サービスの停止の依頼を受け、システム変更作業を行ったが、誤って別のクレジットカード取引の提携先の ATM 提携サービスを停止し、ATM でのキャッシング、残高照会が取扱不可となった。

##### <原因>

- ◆ 依頼文書を基に作業指示書を記載したが、異なる提携先を記載した。
- ◆ 作業指示書の承認者が依頼文書を確認しておらず、また、依頼者が依頼内容と作業結果の整合性を確認せず、誤りを看過した。

<対策>

- 作業指示書に依頼文書を添付し、作業内容と依頼文書の突合を必須とする態勢を構築
- システム変更作業の管理台帳を整備し、依頼から結果確認までの作業を管理

➤ **本番環境と開発環境の取違いによる送金障害**

<業態等>

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い、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え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

➤ **業務部門の為替レート登録誤りによる取引金額不正**

<業態等>

金融商品取引業者（ネット証券会社）

<事象>

- 毎日登録を行う為替取引や海外株式決済等に使用される為替レートの登録内容に誤りがあり、受渡金額が本来と異なる金額となった。

<原因>

- ◆ 為替レート登録の担当部門が誤って本来の値から乖離した金額を登録した。

<対策>

- 登録する為替レートの値が適正レートから一定以上乖離している場合に表示させるアラートの基準を厳格化し、小幅な誤りでも検知できるよう修正

➤ 業務部門の銘柄情報の登録不備による預り区分不正

<業態等>

金融商品取引業者（ネット証券会社）

<事象>

- 特定の債券の銘柄情報の登録内容に不備があり、当該債券を買付けしたすべての顧客において一般口座預りとなった。

<原因>

- ◆ マニュアルに記載不備があり、銘柄情報の特定項目の登録が漏れた。

<対策>

- 銘柄情報登録時に当該項目の登録内容に注意するようマニュアルに明記
- 銘柄情報登録後の登録内容の再鑑についてマニュアルに追記

## ⑦ 固有の商品特性の理解不足に起因する障害

複雑な特性をもった商品を取扱う場合において、システム開発時に一部の取引パターンが考慮できていなかったため発生してしまった障害が認められた。まずはユーザー部門が商品特性を正確に理解した上で、システム開発部門へ詳細な要件提示を行い、その後の設計工程やテスト工程においても、委託先を含むシステム開発部門が抱いた疑問点や出てきた不明点等を確実に潰し込めるよう、ユーザー部門がしっかりとシステム開発部門をサポートする体制の構築に課題があるのではないかと考えられる。

### ➤ NISAの商品特性の理解不足による各種取引処理の不備

#### <業態等>

金融商品取引業者（ネット証券会社）

#### <事象>

- NISA 固有の取引パターン発生時の口座開設不備・ロールオーバー不備・約定と受渡の間に年末年始を跨ぐ取引への誤課税等が発生した。

#### <原因>

- ◆ NISA 固有の商品特性の理解不足による取引パターン考慮が不足（口座開設パターン・ロールオーバー申請パターン等）していた。
- ◆ 商品特性の理解不足によるオペミス（ロールオーバーによる残高移行作業ミス・年末年始を跨ぐ取引へのオペミス等）が発生した。

#### <対策>

- NISA 固有の取引パターンの再整理・設計書への明記
- 作業ミスを抑止するシステム機能の追加、正確で詳細な手順書の作成、再鑑体制の整備、ユーザー部門とシステム開発部門の連携強化・再教育

## ⑧ 設計時の基本的な事項の考慮漏れに起因する障害

システム開発における設計時の影響調査漏れや各種レビューでの確認観点不足等に起因する障害が認められた。システム開発時のガイドラインやチェックリスト等の規定類の整備が不十分であり、過去の障害等から得られた教訓等をその後の開発に十分に活かしてきていないという課題があるのではないかと考えられる。

### ➤ 通貨の補助単位に係る設計不備による手数料誤り

#### <業態等>

資金移動業者

#### <事象>

- 日本円の補助単位の扱いに係る設計不備により、海外 ATM からの日本円引出し時に手数料を誤徴収した。

#### <原因>

- ◆ 日本円に補助単位はないが、複数のシステム間で日本円の補助単位の扱いに差異があり、データ連携時に不整合が生じた。
- ◆ 海外 ATM から日本円を出金するケースがそれまでなかったため、そのようなケースのテストが実施されておらず、事前に発見できなかった。

#### <対策>

- 外部設計工程の完了条件として、システム間のデータ連携がある場合はその後の連携テストの要否を検討するプロセスを追加

### ➤ 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

#### <業態等>

資金移動業者

#### <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

#### ➤ 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

##### <業態等>

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

#### ➤ ウェブサイトの画面入力チェック不備による不正取引実行

##### <業態等>

金融商品取引業者（ネット証券会社）

##### <事象>

- ウェブサイトにおいて、買付を停止したはずの商品の買注文を受注してしまった。

##### <原因>

- ◆ 買付を停止した商品の買注文を行える画面へは遷移できないような画面構成とされていたものの、当該画面の URL を直接指定した場合にはアクセスできてしまい、入力チェックがウェブサイト開設当初からの不十分な状態のままであったため、注文が可能であった。

##### <対策>

- 買付停止後は注文できないよう、当該画面の入力チェックを強化
- システム開発時のガイドラインに、入力チェックに関する共通ルールを追加

## ➤ プログラムの修正不備による買付余力金額不正

### <業態等>

金融商品取引業者（ネット証券会社）

### <事象>

- 買付余力計算処理の性能改善のためのシステム改修をリリース後、制度信用取引の建玉決済及び品受品渡の際、買付余力が不正となる。

### <原因>

- ◆ プログラムの修正時に、本来修正対象ではない部分を誤って修正した。
- ◆ 本来の修正対象部分に限定してレビュー・テストを実施したため、誤修正を発見できなかった。

### <対策>

- 修正対象部分以外も含め、修正前後のプログラムの差分を全量抽出する運用へ変更
- 差分が認められた部分の全量を対象とした修正内容・テストパターン・テスト結果等の有識者レビューの実施・レビュー記録の作成をルール化し、レビュー結果を当社自身も確認する運用へ変更

## ➤ ログ出力仕様の誤りによる取引開始遅延

### <業態等>

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



## ➤ 取引パターンの一部考慮漏れによる取引処理順序の誤り

### <業態等>

金融商品取引業者（ネット証券会社）

### <事象>

- 取引の処理順序の制御に不備があったことにより、特定のタイミングで取引注文を行い、その後の特定のタイミングで当該注文の取消や訂正を行った場合に、取消ができない、あるいは訂正が不正な内容となる。

### <原因>

- ◆ 各注文に対し処理順序を制御する情報を付与する処理の設計に不備があった。
- ◆ 注文パターンの洗出し不足及びテストの網羅性不足による不具合を見逃していた。

### <対策>

- 注文タイミングのパターンを網羅的に再確認し、設計書へ明記
- 無影響確認テストでの網羅性担保のための検証ツールの導入・テスト項目書の作成

## ➤ 外部接続先の仕様変更への対応漏れによる金額計算不備

### <業態等>

金融商品取引業者（ネット証券会社）

### <事象>

- 外部接続先から受信するファイルの取り込み時にエラーが発生し、それをもとに行う値洗い処理が遅延したほか、証拠金の計算結果誤りが生じ、一部顧客が不正に証拠金不足と判定された。

### <原因>

- ◆ 外部接続先から受信するファイルのレイアウトが事前周知された上で変更されていたものの、外部接続先からのインターフェース変更等の情報を収集し対応する体制が未整備であり、当該レイアウト変更に対応できていなかった。

### <対策>

- 外部接続先からのインターフェース変更等の情報を収集する担当部門や対応を検討する会議体を定めるなどの体制整備を実施

➤ 設計における要件漏れによる信用情報の誤提供

＜業態等＞

貸金業者

＜事象＞

- 貸金支払の遅延有無は、本来貸金支払残高を参照し判断すべきところ、誤って割賦販売・貸金合計の支払残高を参照したことで、信用情報機関に誤った信用情報を提供していた。

＜原因＞

- ◆ 設計担当者が業務要件を誤認したことによる設計ミス。設計書を有識者がレビューしたが、レビュー時に要件書を確認せず、設計ミスを抽出できなかった。
- ◆ 誤った設計書に基づきテストを実施したため、テスト工程においても抽出できなかった。

＜対策＞

- 要件書に基づく設計書、テスト仕様書等のレビュー時に、有識者を含めた複数名によるレビュー会議を実施し、要件書どおりの設計となっていることを確認する態勢を整備
- テスト結果はユーザー部門、システム部門がシステム設計書だけではなく、要件書も加えて検証

➤ 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

＜業態等＞

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

以上