

株式会社ゆうちょ銀行のガバナンス等に係る検証結果の概要

2021/1/29 横田

第 1 検証対象事案

- 1 即時振替サービス不正利用事案
- 2 mijica 不正利用事案
- 3 SBI 証券不正出金事案

第 2 検証体制

当職が、補助弁護士と共に、2020 年 10 月下旬から 2021 年 1 月 20 日までの約 3 か月にわたり実施

第 3 検証作業の概要

- 1 関係資料の精査・分析等
- 2 ゆうちょ銀行及び日本郵政の社員等合計 24 人のヒアリング
- 3 役員合計 20 人との意見交換会
- 4 視察：ゆうちょ銀行のエリア本部及び直営店等 合計 9 か所

第 4 検証の視点

- 1 「顧客本位の業務運営」の観点から、顧客保護に向けたセキュリティ対策を適切に講じていたか（視点①）
- 2 リスク管理態勢としての 3 線ディフェンスが機能していたか（視点②）
- 3 顧客の苦情に含まれる重大なリスクの検知、分析を通じて、顧客の声を経営において適切に活用していたか（視点③）
- 4 内部統制の要素の一つである「情報と伝達」の状況、すなわち、ゆうちょ銀行が、リスク情報を、どのように認識・評価し、内部で伝達し、日本郵政に報告したか（この視点は、危機管理対応としての広報対応も含む。）（視点④）

第 5 検証結果の概要

- 1 「顧客本位の業務運営」の観点から、顧客保護に向けたセキュリティ対策を適切に講じていたか（視点①）
 - (1) 即時振替サービス不正利用事案
 - ① 決済事業者との間で即時振替サービス契約を締結するに先立ち、即時振替サービスの所管部署のみで決済事業者の接続承認基準への適合性を判断していた。

- ② 即時振替サービス導入時に「新商品等審査」¹を実施しておらず、本人確認の認証セキュリティを含めたリスクの評価及び管理を行う機会を逸した。
- ③ 即時振替サービス導入後、本人確認の認証セキュリティ対策としての「IVR 認証」²の導入が遅れた。
- ④ 決済事業者に対し二要素認証の導入に向けて必ずしも積極的な働きかけまでは行っていなかった結果、一部の決済事業者による導入が進まなかった。

(2) mijica 不正利用事案

- ① mijica に送金機能を追加した 2017 年 11 月の新商品等審査において、セキュリティ面の脆弱性を検知できなかった。
- ② 年次の「システムリスク評価」³においても、入力試行防止機能⁴の有無についてログイン時と送金時のフェーズごとの検証を行っていなかったため、セキュリティ面の脆弱性を発見できなかった。
- ③ 委託先におけるログイン監視状況に対する実態把握が不十分であった。
- ④ システムやセキュリティに関する専門的知見を有する人材が 1 線に不足しており、深度あるリスク評価及び管理ができていなかった。

2 リスク管理態勢としての 3 線ディフェンスが機能していたか（視点②）

(1) 1 線による自律的管理がなされていなかったこと、及び 2 線による牽制が有効に機能していなかったこと

ア 即時振替サービス

- ① 決済事業者の接続承認基準への適合性の判断を 1 線のみで行っていた。
- ② リスク管理の一環としての新商品等審査が行われなかったため、1 線のリスク管理に対し、2 線が適切な牽制を行う機会が失われた。
- ③ 即時振替サービスに係るセキュリティリスクについて、これを取り巻く環境変化等を踏まえ、2 線が継続的に管理を行う仕組みが構築されていなかった。

イ mijica サービス

- ① 1 線である mijica サービスの所管部署によるシステムリスク評価に対し、2 線によるチェックが不十分であった。
- ② 委託先におけるセキュリティ対策の整備に関する 1 線によるモニタリングに際して

¹ ゆうちょ銀行において、新商品及び新規業務を導入する前に、リスク管理統括部が事務局となり、関連する部署を通じ、新商品等に内在するリスク等を特定・評価し、管理体制の適切性及び有効性を確認することをいう。

² 即時振替サービスの申込時に「電話番号」を入力させ、ゆうちょ銀行の顧客原簿に登録された電話番号と一致するか認証を行い、一致した場合、その電話番号に架電し、自動音声でワンタイムパスワードを通知するものである。

³ システムリスク評価とは、システムごとに内在するコンピュータシステムのダウン又は誤作動等、システムの不備等に伴い損失を被るリスク、更にコンピュータが不正に使用されることにより損失を被るリスクを特定し、頻度と影響度により評価を行い、重要度に応じてコントロールを設定し、モニタリングを行い、必要に応じた対応策を実施することをいう。

⁴ パスワード等を一定回数誤入力するとアカウントがロックされる機能。

の2線による支援が不十分であった。

(2) 3線が有効に機能していなかったこと

3 顧客の苦情に含まれる重大なリスクの検知、分析を通じて、顧客の声を経営において適切に活用していたか（視点③）

(1) 苦情の検知

① 苦情として取り扱うべき申出に該当するか否かを判断する基準の周知が不十分であったことから、顧客からの申出のうち、即時振替サービスに関する苦情の一部が事故報告システムに入力されていなかった。

② mijica デスクに寄せられた苦情について、委託先からその一部のみの報告を受けて事故報告システムに入力していたことから、mijica デスクに寄せられた苦情の全容を把握していなかった。

(2) 受け付けた苦情の分析状況等

ア 苦情受付等担当部署による苦情の分析等

苦情受付等担当部署は、週次で所管部署に提供する苦情や各所管部署に改善を依頼する苦情について、リスク情報把握の観点からの抽出・分析を行っていなかった。

イ 各所管部署による苦情の分析等

上記苦情受付等担当部署から提供を受けた各所管部署が、苦情の内容を十分に精査しなかったため、顧客の苦情から本件不正利用事案に係るリスクを把握できなかった。

(3) 経営陣に対する苦情の報告等

顧客の苦情を経営に活かすための報告態勢等が整備されていなかった。

4 内部統制を構成する主たる要素としての「情報と伝達」の状況等（視点④）

(1) 即時振替サービス不正利用事案における「情報と伝達」の状況等

① コンプライアンス統括部内における情報の伝達等に不備があった。

② 営業部門の所管部署とコンプライアンス統括部の間にコミュニケーション不全が生じていた。

③ 経営陣に対しリスク情報が適時に報告されていなかった。

5 危機管理対応としての「情報と伝達」の状況等（視点④）

(1) 2020年8月下旬以降、日本郵政グループは、「信頼回復に向けた業務運営の開始」に向けた準備を進めるなど、グループ全体としての信頼回復に向けた活動に取り組んでいたため、顧客に被害が生じた本件キャッシュレス決済サービス不正利用事案について、ゆうちょ銀行は、平時以上にリスク感度を高め、危機管理として対応することが求められていた。

(2) 即時振替サービス不正利用事案及び mijica 不正利用事案のいずれについても、危機管理対応がなされておらず、社内での情報の共有や経営陣への報告が遅れ、日本郵政

への報告も可能な限り速やかに行われたとはいえない。

第6 ガバナンス強化の観点からの課題

1 組織風土に関わる課題

(1) 日本郵政グループが信頼回復の途上にある中で、ゆうちょ銀行は、顧客本位の理念に反する事象が自行の信用やサービスに対する顧客の信頼及び社会的信用の毀損、ひいてはグループ全体の信頼回復を阻害するおそれのある事態であるとの認識が不十分であった。

(2) 顧客の視点に立ち、被害を受けた顧客の迅速な救済を図るという意味での「顧客本位の業務運営」が実行できていなかった。

2 「顧客本位の業務運営」の観点から、即時振替サービス及びmijica サービスに関し、預金者保護に向けた適切なサイバーセキュリティ対策を講じていなかったこと

3 即時振替サービス及びmijica サービスの顧客の苦情等を漏れなく正確に収集・分析し、速やかに対応し、経営に活用する仕組みに不備があったこと

4 ゆうちょ銀行の内部統制としての情報伝達等に不備が認められたこと

5 ゆうちょ銀行に対する顧客の信頼及び社会的信用が毀損されるおそれのある事象をリスク情報として早期に探知し、危機管理対応に移行する態勢及び手続が定められていなかったこと

6 グループ全体の企業価値が毀損されるおそれのあるリスク事象について、日本郵政内に、ゆうちょ銀行を含む事業子会社から情報提供を受け、一元的に対応するという機能が整備されていなかったこと

第7 ガバナンス強化に向けた改善策の提言

1 ゆうちょ銀行は、預金者が「お客さま」であることを再認識し、真の「顧客本位の業務運営」を実現するための組織風土改革を実行すべきであること

2 実務を担う役職者による部門横断的なリスク情報共有の機会を定期的に設け、「顧客本位の業務運営」が実務面で実行されているのかを評価・検討し、課題や解決策を洗い出すとともに、責任部署を明確に定めて、その進捗状況を定期的に確認し、経営陣に適時に報告する仕組みを構築すること

3 社外取締役を含む外部人材の知見を一層活用すること

4 部門をまたいだ人事異動・交流等の活性化を図ること

5 リスク管理態勢の強化を図ること

(1) いかなるリスクカテゴリーに該当するのかが明確ではないリスク事象が生じることも想定し責任部署を明確にしたリスク管理態勢を構築すること

(2) 新商品等審査において、2線が多角的・多面的なリスク評価を行うことができるような仕組みとプロセスを構築すること

(3) 顧客に被害を生じさせるリスクが潜在する商品やサービスの導入後も、これを取り巻く環境変化等を踏まえた継続的かつ定期的なリスク評価の洗い替えを多角的・多面的に行う仕組みを構築すること

(4) 1線におけるサイバーリスクを含むリスク評価の高度化に向けた態勢を強化すること

(5) 2線である管理部門の機能強化に向けた態勢整備として、所掌事務等を抜本的に見直すこと

(6) 3線である内部監査部門のリスク評価機能を強化すること

6 苦情を含む顧客の声を収集・分析して活用するなどし、その状況をモニタリングするというPDCAサイクルを回すことにより、顧客の声を経営において適切に活かす態勢を再構築し、着実に実行すること

7 顧客に被害を生じさせ、ゆうちょ銀行に対する顧客等の信頼が毀損されるおそれのある事態を、リスク事象として早期に探知し、危機管理対応に移行するために、現行の複線的なレポーティングラインを確保しつつ、リスク事象に係る情報伝達のルール及び責任部署等を明確に定め、周知徹底すること

8 グループの企業価値が毀損されるおそれのある事業子会社のリスク情報が日本郵政に迅速かつ確実に伝達され、より早い段階からグループとしての一体的な対応を可能と

すべく、日本郵政において、現行の複線的なレポーティングラインを確保しつつ、子会社からのリスク情報を第一次的に受け付け、日本郵政の経営陣に対する報告及び関係部署との共有等を迅速に行う機能及び態勢を整備すること

9 グループガバナンス、特に内部統制強化の観点から、「コンダクト・リスク」に係る情報を早期に探知し適切に対応するための日本郵政による方策の検討と実行を通じて、子会社であるゆうちょ銀行のガバナンス強化を図ること

以上