BOJ
Reports & Research Papers

2015年1月

リスク管理と金融機関経営に関する調査論文

重要な顧客情報のセキュリティ強化に向けて

― コンピュータ・システムのリスク管理上の留意点 ―

日本銀行金融機構局

2015 年 1 月

日本銀行金融機構局

重要な顧客情報のセキュリティ強化に向けて
― コンピュータ・システムのリスク管理上の留意点 ―

[目　次]

【本件に関する照会先】

日本銀行金融機構局　考査企画課システム・業務継続グループ

伊藤　琢、中井　大輔、三木　康次

E-mail : csrbcm@boj.or.jp

１．重要な顧客情報の取扱いと環境変化

金融機関は、預金や証券売買、資金の貸付けや振込み・引落し等、様々な金融取引を通じて、個人や企業等、顧客の情報を数多く取り扱っている。なかでも、預金口座や証券口座の口座番号、キャッシュカードの暗証番号、インターネット取引のログイン ID・パスワード等は、仮にこれらが不正に利用された場合には、顧客や金融機関に直接的な金銭被害等が生じるおそれがある、極めて重要な情報（以下、重要情報）であり、特に厳格な管理が求められる。

金融機関の業務の多くは、コンピュータ・システム（以下、システム）を用いて処理されているため、重要情報を取り扱うシステムのセキュリティを確保し、不正利用から守ることは、金融機関にとって非常に重要である。また、近年、金融機関のシステムやその開発・運用作業では、以下のような変化がみられており、金融機関は、こうした環境変化も十分考慮して対応する必要がある（図表１）。

（１）システム構成のさらなる複雑化

パソコンのほか、スマートフォンやタブレット端末を利用し、インターネットを介して行う外貨預金や国債、投資信託等の取引サービスが広がる等、金融機関が顧客に提供するサービスや取引チャネルは、年々、多様化している。

これらへの対応に伴い、金融機関は、取引の当事者や利用する端末の正当性を確認する認証システムや、それぞれの取引を実行・管理するシステム、それらの取引の売買代金の決済や証券の受け渡しを行い、残高を管理する勘定系システム等、より多くのシステムを開発・運用している。同時に、通信回線や各種ネットワーク機器、中継システム等で相互にそれらのシステムを接続する等、金融機関のシステムやネットワークの構成はさらに複雑なものとなってきている。

この結果、システムやネットワーク内のデータの流れ（データフロー）も複雑化しており、重要情報がどのシステムやネットワークを経由し、どのシステム・機器でどのように処理され、あるいは保存されているかを注意深く調査し、正確に把握することが、従来にもまして重要になってきている。

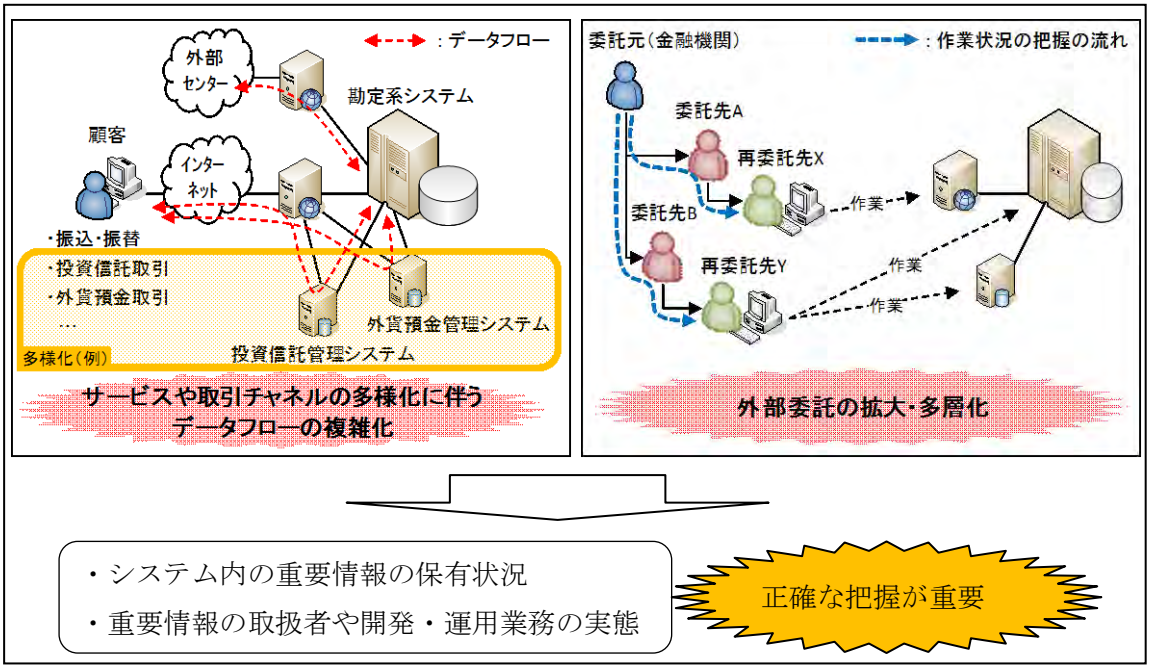
（２）外部委託化の一層の進展

多くの金融機関では、経費削減等の観点から、システムの開発・運用業務の外部委託化が一段と進められてきている。例えば、地域銀行では、複数の銀行が同じ勘定系システムを利用する[1]共同システムの利用先が全体の約 7 割に達している[2]。システムの開発・運用業務の外部委託では、委託形態が、再委託や再々委託を含む多層構造となっているケースが少なくない。また、金融機関によっては、複数のベンダーの機器やソフトウェアを併用したり、数多くのベンダーのサポートを受けたりしている先もみられる。

従って、金融機関では、システムの開発・運用業務の外部委託化が一層進展する下で、多層構造の委託関係や複数のベンダーの併用状況も含めて、重要情報を取り扱うシステム開発・運用業務の実態を正確に把握することが、より重要になってきている。

本稿では、これらの点を踏まえ、特に、システム面のリスク管理に着目して、重要情報のセキュリティ強化に向けた対応の留意点――具体的には、①重要情報の保有状況の把握、②重要情報を取り扱う業務の把握、③リスク対策の実施状況の把握に関する留意点等――を整理する。

（図表１）システムを巡る環境変化と重要情報の正確な把握



[1] ここでは、コンピュータや業務アプリケーションを共用するか否かにかかわらず、複数の金融機関が勘定系システムの開発または運用を共同で外部委託することを指す。

[2]「地域金融機関におけるシステム外部委託先管理に関するアンケート（2013 年 11 月）調査結果」（2014 年 3 月）日本銀行ホームページ（http://www.boj.or.jp/）参照。

２．システム面のリスク管理強化に向けた留意点

２－１．重要情報の保有状況の把握　～ログ情報にも内在し得る重要情報

システムにおける重要情報のリスク管理を強化するためには、まず重要情報の保有状況――具体的には、重要情報がシステムのどの部分に、どのようなかたちで、どのくらいの期間にわたって保有されているか等――を正確に把握する必要がある。

システム内部でデータが保存される場所としては、一般に、勘定系システムのデータベースやファイルシステム等（以下、データベース等）が注目されやすい。実際、金融機関が、システムで保有するデータのセキュリティのリスクを評価する場合、これらのデータベース等を対象にしていることが多い。

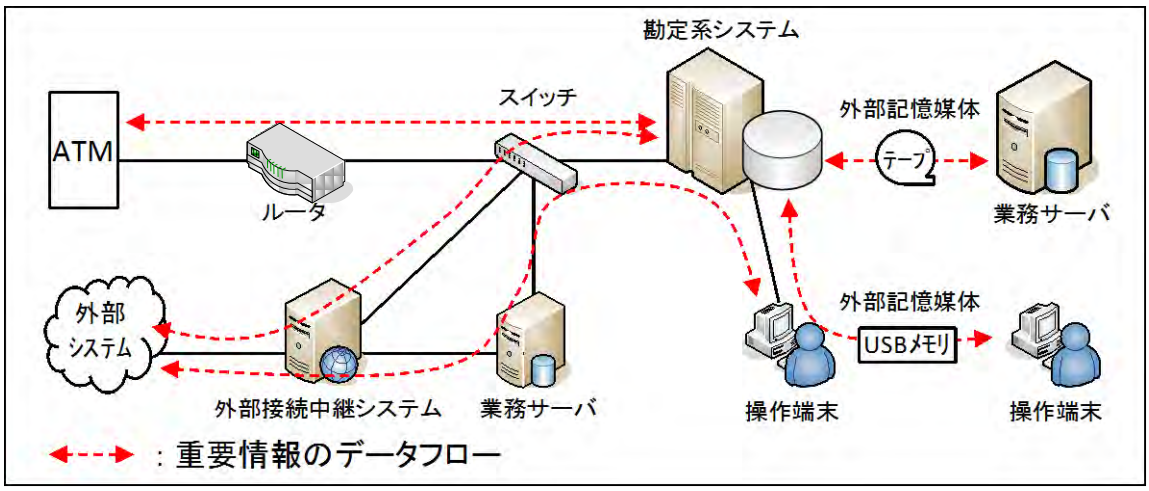
しかし、①顧客や金融機関の職員がデータを入力するATMや窓口端末等でも、データが保存される場合がある。さらに、障害が発生した場合の原因分析等の目的から、②スイッチやルータといったネットワーク機器では、その内部に詳細なログが保存されることがあるほか、③データベース等を保有しないプログラムでも、エラー処理の際には通常よりも詳細なログを出力する仕組みとなっている場合がある。そして、これら①～③にも重要情報が含まれる場合がある点には、特に留意が必要である。

通常、勘定系システムのデータベース等は、大量のデータをまとまったかたちで保有しているという意味で、セキュリティ上の潜在リスクは小さくないが、他方で、比較的設置台数が限られ、また設計書等でもデータの保有状況を確認しやすい。これに対し、入力端末やネットワーク機器、連動する各種のプログラムについては、保有する情報の量や種類は相対的に限られたものとなっている可能性がある一方、その数と所在は、多数かつ多岐にわたる傾向にある。

従って、システム内における重要情報の保有状況を正確に把握するためには、まず、重要情報を取り扱う業務を特定したうえで[3]、金融機関のシステム全体を対象に、それらの重要情報のデータフローを把握し、重要情報を保有する可能性のあるシステム・機器を特定することが重要である。データフローの把握にあたっては、図表２のようなデータフロー図を作成することも考えられる。

[3] 重要情報を取り扱う業務の特定に際して、入出金取引や振込・振替取引といった業務面からの切り口のほかに、バックアップデータ保管やバッチ処理といったシステム運行にかかる業務についても特定することが重要である。

（図表２）重要情報のデータフロー（例）



次に、重要情報を保有する可能性のあるシステム・機器について、保有の有無や、図表３に示すような保有の形態を確認する。この際、ATM や、スイッチやルータ等のネットワーク機器、外部への接続を中継するシステム等では、上述のとおり、当該システム・機器の内部で、重要情報をログの形態で保有している可能性がある点、留意する必要がある。

（図表３）重要情報の保有の形態（例）

確認項目	想定される保有の形態
保有場所	データベースとして格納／ログ等の中だけに保有　等
保有期間	一時的保有／長期的保有　等
加工状況	平文／暗号化／マスキング　等

２－２．重要情報を取り扱う業務の把握　～障害対応にも留意が必要

システムにおける重要情報のリスク管理の強化に向けた第二のステップは、重要情報を取り扱うシステム開発・運用業務を正確に把握することである。

重要情報を取り扱う開発・運用業務を正確に把握するためには、重要情報のデータフローに沿って、①各業務に関与する取扱者と②各システム・機器で発生し得る業務の内容を特定することが重要である。

このうち、取扱者に関しては、システムの開発・運用業務の外部委託が一層進展している中で、再委託先や再々委託先等の外部委託先の取扱者を把握し、それらの外部委託先において重要情報の取扱ルールの設定や取扱いの実態が適

切であるか否かを、委託者である金融機関が十分に把握することが一段と重要になっている。

また、業務の内容のうち、特に運用業務については、図表４のように、定期的かつ計画的に実施される通常時運用と、突発的な事象に伴い臨時で実施される臨時運用に分けて実態を把握することが適当である。臨時運用は、作業内容がほぼ定型化している通常時運用に比べ、予め十分な管理体制を確保しないまま、意図せず重要情報を取り扱ってしまうリスクが懸念される（図表５）。こうした場合に備えて、過去の障害発生時の対応や保守作業の内容を参考に、臨時運用で取り扱う可能性のある重要情報やその取扱者を確認することが重要である。

（図表４）システム運用の分類（例）

システム運用の分類	想定される作業
通常時運用	システム起動・停止、システム監視、ジョブの実行、データバックアップ、定期保守点検
臨時運用	障害対応（ログ収集、障害分析、障害復旧）、臨時保守

（図表５）留意が必要な臨時運用（例）

臨時運用	想定される運用事例
障害対応[4]	・ネットワーク機器での電文の取得 ・本番作業エリア外（外部委託先の執務エリア等）での障害分析作業
臨時保守	・機器交換

２－３．リスク対策の実施状況の把握

～　重要情報に対するアクセス制御の実施状況等

システムにおける重要情報のリスク管理の強化に向けた第三のステップとして、２－１．および２－２．で把握した重要情報の保有状況や取扱状況に対して、リスク対策を実施しているか否か、また実施している場合には、具体的に

[4] 機器やソフトウェアによっては、通常時運用では使用しない可能性のある管理ツール（データベース管理システムに標準搭載されているコマンドラインツール等）が搭載され、こうしたツールの機能により、重要情報の取得が可能となっている状況も想定される。このため、機器やソフトウェアに搭載されている機能については、十分に把握することが重要である。

どのような対策が講じられているかを確認する必要がある（図表６）。

（図表６）リスク対策（例）

項　目	内　容
重要情報を保有する機器における対策	・重要情報の暗号化やマスキング ・重要情報を保有する機器でのアクセス制御、不要な機能の無効化、重要情報アクセス時のアラーム発報　等
重要情報を取り扱う運用における対策	・特権 ID の管理、複数名での運用、操作ログの取得・検証、作業権限の分離、カメラ等での監視　等

２－４．リスク評価を踏まえた対策の強化

２－１．から２－３．までで示した確認内容を改めて整理すると、図表７のようになる。これらの作業を通じて把握された重要情報の所在と対策の実施状況――すなわち、重要情報に関するリスク管理の実状――については、例えば、図表８のように、重要情報のデータフローに沿った一覧表に整理することで、全体像をより把握しやすくなると考えられる。

（図表７）重要情報のデータフローにおける確認項目・内容

確認項目	確認すべき内容
重要情報を取り扱う業務	・業務のプロセスと重要情報
重要情報の保有状況	・重要情報を保有するシステム・機器 ・保有の形態 ―　保有場所（データベースとして格納／ログ等の中だけに保有　等） ―　保有期間（一時的保有／長期的保有　等） ―　加工状況（平文／暗号化／マスキング　等）
重要情報を取り扱う運用	・上記機器毎の取扱者（金融機関役職員／外部委託先）、運用内容　等
リスク対策	・アクセス制御や、データの暗号化等のリスク対策の内容　等

確認結果のイメージ

（図表８）重要情報のデータフローにおける確認項目・内容（一覧表の例）

［ 業務名 ： 自行宛送金 ］

機器	営業店端末	スイッチ	ルータ	外部ネットワーク	中継サーバ	スイッチ	勘定系サーバ
設置場所	営業店			外部	システムセンター（本番環境）		
重要情報の保有場所（保有期間）	システムログ(1カ月)、ジャーナル(1カ月)	電文中継	電文中継	電文中継	システムログ(3カ月)、アプリケーションログ(3カ月)、エラーログ(3カ月)	電文中継	データベース(無期限)、システムログ(3カ月)、アプリケーションログ(3カ月)、エラーログ(3カ月)
保有する重要情報（加工状況）	口座番号（暗号化）、暗証番号（マスキング）	口座番号（平文）、暗証番号（暗号化）	口座番号（平文）、暗証番号（暗号化）	口座番号（通信暗号化）、暗証番号（通信暗号化）	口座番号（平文）、暗証番号（平文）	口座番号（平文）、暗証番号（暗号化）	口座番号（暗号化）、暗証番号（暗号化）
取扱者	端末管理担当者、○○社保守要員	ネットワーク管理者、××社保守要員	ネットワーク管理者、××社保守要員	△△社保守要員	□□社運用要員、○○社保守要員	ネットワーク管理者、××社保守要員	運用担当者、□□社運用要員、○○社保守要員
運用内容	通常時：ログ取得 臨時：ログ・ジャーナル取得、設定変更、機器交換	通常時：なし 臨時：設定変更、パケットキャプチャ、機器交換	通常時：なし 臨時：ログ取得、設定変更、パケットキャプチャ、機器交換	通常時：ログ取得 臨時：ログ取得、パケットキャプチャ、機器交換	通常時：なし 臨時：ログ取得、設定変更、機器交換	通常時：なし 臨時：ログ取得、設定変更、パケットキャプチャ、機器交換	通常時：設定変更、プログラムリリース　等 臨時：ログ取得、設定変更、プログラムリリース、機器交換
リスク対策	・監視カメラ ・特権ID管理 ・アクセス制限 ・無線機能無効化 ・複数人作業 ・外部記憶媒体利用ログ取得・ログ監査	・特権ID管理 ・施錠管理 ・複数人作業 ・作業証跡確認 ・不要なサービス・ポートの停止	・特権ID管理 ・施錠管理 ・複数人作業 ・作業証跡確認 ・不要なサービス・ポートの停止	・監視カメラ ・入退室管理 ・特権ID管理 ・作業証跡確認 ・複数人作業	・入退室管理 ・特権ID管理 重要情報を不正取得される、リスクあり	・監視カメラ ・入退室管理 ・特権ID管理 ・作業証跡確認 ・複数人作業 ・不要なサービス・ポートの停止	・監視カメラ ・入退室管理 ・特権ID管理 ・作業証跡確認 ・複数人作業 ・外部記憶媒体利用ログ取得・ログ監査
備考				対策状況は、外部ネットワーク提供先に確認			

こうした整理に基づき、現在のリスク対策の十分性を評価し、必要に応じて脆弱性が判明した項目のリスク対策を強化する。リスク対策の評価にあたっては、金融機関の役職員や外部委託先による正当な作業に乗じた不正行為の防止または検知に有効か、といった視点も重要である。また、重要情報の暗号化やマスキング等が困難な場合には、例えば、作業権限の分離や作業証跡の確認等の運用面での対策を組み合わせることで、金融機関が必要と考える牽制体制を確保していくことが重要である。

なお、ATM やカード決済、インターネットバンキング等、外部機関が提供するサービスについても、金融機関の重要情報のデータフローの中に当該サービスが関与する場合には、上記と同様の確認をすることが重要である。

３．状況変化に応じた見直しの実施

２．で述べたような、システム面における重要情報のリスク管理の実態把握と改善に向けた取組みは、一時的なものに止まらず、システム構成や提供するサービスの変化等に応じて、適時適切に見直すことが重要である。そのためには、図表９に示したような体制を整備することが考えられる。

（図表９）管理体制の整備方針（例）

体制整備	具体的内容
開発標準への反映	システムの新規構築時や改修時には、リスクプロファイルの変化が想定されるため、開発時に使用する開発標準へ重要情報にかかるリスク評価項目を設定する。
既存のリスク評価プロセスへの反映	既存システムについても、環境変化や利用状況の変化によるリスクプロファイルの変化が想定されるため、既存のリスク評価プロセスへ重要情報にかかるリスク評価項目を設定する。

４．おわりに

重要な顧客情報の管理を厳格に行うことは、不正使用に伴う金銭的な被害の防止にとどまらず、金融機関の業務運営に対する信頼確保の面でも重要である。本稿でみたように、金融機関の業務の多くがシステムを用いて処理され、またシステム構成や運用等の環境変化が生じる中で、システム面でも重要情報のリスク管理強化に向けた取組みを継続的に行っていくことが、一段と重要になってきている。日本銀行としては、金融機関やその外部委託先が、本稿で述べたシステムリスク管理上の留意点も踏まえ、引き続き、システムのセキュリティ確保に向けた対策に取り組んでいくことを期待している。

以　上