資料３－２

共同システムの導入に関する論点

「光ブロードバンドの活用方策検討チーム」でのこれまでの議論や地方銀行等におけるシステムの共同化の現状等を踏まえ、主な論点を整理する。

Ⅰ．期待される効果に係る論点
1. 行政コストの削減
2. 経営戦略の手段（機能強化やサービスの充実）
3. 内部職員の役割
4. システムの安定性の向上（耐障害性・障害復旧速度の向上）

Ⅱ．共同システムの導入の要件に係る論点
1. 業務の標準化とカスタマイズの抑制
2. パッケージ・ソフトの利用
3. データの移行
4. システム開発の迅速化

Ⅲ．ＩＴリスク管理上の論点
1. ＩＴリスク管理全般
2. 安定性・信頼性・安全性等について
3. 共同化における委託先管理手段
4. クラウド・コンピューティングによる共同化の留意点

Ⅳ．次期システム検討体制の確保に係る論点

（参考資料）

金融機関におけるシステム共同化の現状と課題-地域銀行 108 行へのアンケート調査結果から-、日本銀行調査論文、2009.6

「わが国金融機関への期待」、富永　新、生産性出版、2009

「光ブロードバンドの活用方策検討チーム」第一回・第二回の意見　　等

Ⅰ.　期待される効果に係る論点

1.　　行政コストの削減

〇投資効率を最大化するためには、標準化・共通化を通じて使用頻度の低いチャネル・帳票等を廃止や絞り込むことなどにより、業務とシステムの最適化を目指すことが重要。組織だけでなく、システムにも簡素・統合化の余地は大きい。

〇一方、共有度合いが高いほど効率化に伴うコスト削減効果が大きくなり、その反面として自社の独自ニーズを反映したシステム仕様の実現は困難になる。

〇地方銀行における共同システムの実現方式

（システム共同化行は2009年3月時点で約半数、2012 年末時点で７割近くに達する見通し）

データセンターを別々に設置	13%
同一センター内で別々のホストコンピューター	９%
同一のホストを論理分割し、別々のOS・アプリを起動	36%
マルチバンク方式（アプリまで共用、アプリの処理ロジックで各行を区別）	42%

（日本銀行調査論文「金融機関におけるシステム共同化の現状と課題～地域銀行 108 行へのアンケート調査結果から～」（以下、「日銀調査」より）

2.　経営戦略の手段（機能強化やサービスの充実）

○24 時間・365 日稼働、オフサイトバックアップ、チャネル拡充等が容易になるなど、IT はコスト削減の道具ではなく、組織の価値創造の有効な手段ともなり得る。

○アウトソーシングを実施するに当たっては、その組織にとって何がコア・コンピタンスか見極めたうえで、戦略的に経営資源の選択と集中を行う観点から取り組むことが重要。

○「固有の業務は自前、他と共通の業務はアウトソーシング」というのが一つの方針。限りある経営資源を、組織戦略における重要分野に集中投入するため、コア・コンピタンスでない（組織固有性・競争性に乏しく重要度の低い）業務をアウトソーシングするのは、効率的な経営の観点から有効な選択。

○クラウドの導入は業務の標準化を進める契機になるとともに、自治体が複数の選択肢から選べるようになり得る。

○クラウドサービス導入に伴い、遠隔地にバックアップ・センターを持つ効果は大きい。

○金融界でいえば、CRM（ Customer Relationship Management：情報システムを応用して企業が顧客と長期的な関係を築く手法のこと）や ERP（Enterprise Resource Planning：企業全体を経営資源の有効活用の観点から統合的に管理し、経営の効率化を図るための手法・概念のこと。「企業資源計画」）パッケージを入れるのなら、BI（Business Intelligence：業務システムなどから蓄積される企業内の膨大なデータを、蓄積・分析・加工して、企業の意思決定に活用しようとする手法）機能を導入するなどにより、様々な蓄積データをより高度に分析し、経営の意志決定等に活かすことが望ましいとされる。

3. 内部職員の役割

○業務とどう関係して動いているか、リスク管理が効いているかを評価できれば、システムを自分で作らなくても良い。一方、インソースの強化をやらないとブラック・ボックス化が進行してしまうので、IT の選択的・戦略的な活用のためには、全体のデザイナーは内部に必要。

○システム共同化を行った地方銀行の 7 割でシステム要員が 30～50%以上削減されている。一方で、共同化後の自行職員のスキル変化をみると、共同化行の７割で委託先管理スキルが向上したとする一方、システム維持管理のためのコアスキル（システム設計スキル等）は、低下したとする行が向上したとする行を上回っている。スキルレベルを維持する方法として、研修・委託先への出向・共同組織の設置と出向・スキルを持つ人材の中途採用などが行われている。
（「日銀調査」より）

⇒課題：システム共同化においては、単独での運営に比べ、各共同化行におけるシステムへの関与が薄くなりがちである。このことがもたらすリスクを十分認識した上で、各共同化行は、平素から主体性をもってシステムの運営や管理に関与していく必要がある。

⇒課題：システム開発時に、ユーザーニーズを適切にシステム設計に反映させるには、要件定義を適切に行うための業務スキルが必要となる。共同化行は、システム開発プロセスにおける業務スキル維持に取り組む必要がある。また、共同システムの運営を主導する銀行（以下、リーダー行、主として共同化システムを最初に導入した銀行）と他の共同化行との間でのシステムスキル格差拡大が示唆されており、各共同化行はスキルをリーダー行に過度に依存することのないよう、普段から共同システム運営に十分に関与することが求められる。

4. システムの安定性の向上（耐障害性・障害復旧速度の向上）

○NGN（次世代ネットワーク）の普及や IPv6 の普及に伴い、インターネットベースでも、よりセキュアなネットワーク構築が可能。

Ⅱ．　共同システムの導入の要件に係る論点

1.　　業務の標準化とカスタマイズの抑制

○画面やイメージについては、個々の歴史があり、一番使いやすい形として運用されているので、標準化に踏み切るのに躊躇する例がある。

○システム調達においては、利用部門は往々にして「あれもこれも欲しい」と「あれば便利」的なことまで要求する。システム部門はこれに応えようと、無理して難しい仕様に挑戦してしまう傾向がある。これらを放任してしまえば、必要性の低い投資が高価なスペックで繰り返され、経営効率が低下していくことになる。従って、経営としての視点から積極的に裁定していく対応が望ましい。

○共同化にあたっては、先ず各組織の個別仕様、すなわち独自性を極力削減し、統一仕様の比率を高めていくのが成功への近道となる。コストが当初の目論見ほどに下がらない原因の多くは個別仕様の割合が高く、結局は個別に開発するのと大差ない工数がかかっているといった面にある。「3 割以上カスタマイズするのであれば、新規開発した方が早くて安い」と言われている。パッケージ・ソフトを利用するのであれば、組織の権限体系等、一切合切をパッケージに合わせ、既存の事務フローを変えてでも仕様を変更しない方が良いのでは。

○システム統合にあたっては、それまでの各組織内での各種のしがらみやシステムと業務のたび重なる迷宮化をこの機会に清算するため、身辺整理と業務の見直し（BPR : Business Process Re-engineering）を行って、「シンプルなシステム構造を目指す」というスタンスが賢明。

○ベンダー主導のアウトソーシングであったとしても業務要件は自分で決め、プロジェクトを管理するスタンスが求められている。

○データの統一化など、ベンダーの立場で標準化を行うわけにはいかない。

○地方銀行のシステム共同化においては、共同化行の約６割がシステム仕様変更の柔軟性に多少なりとも不満。一方、共同化行の約半数が独自カスタマイズを原則自由とされている中で、カスタマイズ率が１割未満に止まる行が約７割に達しており、独自カスタマイズは抑制的に運用。
（「日銀調査」より）

⇒課題：「共同化＝仕様変更の柔軟性低下」は共通認識となっている。その上で共同化に踏

み切るかどうかの判断が分かれるのは、経営戦略との関係で仕様変更の柔軟性確保の重要性や勘定系システムの位置付けについての判断が異なるためと思われる。システム共同化の採否や共同化後の運営に際して、経営陣はシステム共同化の特性を十分に理解し、適切な判断を下す必要がある。

2. パッケージ・ソフトの利用

〇旧来のメインフレーム型では特定のベンダーにシステム全体を囲い込まれ、コントロールが効きにくい可能性がある。この結果、「システム部門が IT ベンダーとなれ合い関係になり、高いものを買わされているのではないか」との経営層の不信感が底流に生まれた。これを打破するため、オープン化の旗の下に、システムを部品化し「それぞれに最適なベンダーから最善の商品を安く買おう」との発想が現れ、パッケージ・ソフトの導入が拡大。

〇マルチベンダー化と併せ、最近は既成のパッケージ・ソフトを組み合わせて利用することが多い。

〇標準化作業には長い時間がかかるので、いち早くどういうアプリでどういうことをやればクラウドの機能を発揮できるのかを検証しながら、同時に標準化ということをやらないと国際的には通用しない。

〇パッケージ・ソフトは汎用的に作られているだけに、それらを組み合わせた場合の「相性問題」から逃れることは難しい。

〇オープン系技術もある程度の標準化やベンダーの淘汰が進んでいるが、親和性の難点は依然として残る。パッケージ・ソフトは基本的に単独動作環境を前提に作られており、他のソフトと組み合わさるとメーカー保証外となる場合もある。

〇個別の製品としては完成度が高くても組み合わせや利用条件によって、潜在していたバグにぶつかるケースもある。

3.　データの移行

〇データの移行は、現行システムから必要なデータを取り出して、新システムに投入する作業であるが、以下のような膨大で緻密さを要する課題がある。

(1)　新システムに移すデータを選び、形式を決める。

(2)　データを変換する移行用プログラムを作る。

(3)　移行当日の限られた時間内に全部のデータを間違えずに引っ越す。

データ以外にも移行に関連した機器の設置やネットワークの張替え等、諸作業は数多く、連関している。

4.　システム開発の迅速化

〇システム共同化を行った地方銀行の約６割はシステム開発のスピードが低下したと感じているが、リーダー行の存在、業務アプリにパラメーター設定等（金利・満期日の設定・商品ごとの独自設定が可能）により開発の迅速性向上が図られている。（「日銀調査」より）

〇システムの統合においては、まず価値観とゴールの共有化を行った上で、それに適合したシステム統合方式を選択する。システム統合方式には下記のようなものがある。

(1)　全面再構築型（新たなシステムの構築）
制約なく最適なシステムを構築できる。時間・費用がかかり、障害リスク大。

(2)　片寄せ型（一方のシステムの規模を拡張し、データを移行）
比較的早く統合でき、リスク小。利用を停止する側の優れた機能がなくなる。

(3)　良い所取り型（業務別・システム別等に選択して組み合わせる）
両者の優れた機能を残せる。選択に軋轢が生じやすい。複雑化によるリスク増

(4)　ブリッジ中継型（両者のシステムを存続し、中継システムでデータを受け渡す）
すばやく統合でき、リスク小。業務処理が個別のため、合理化効果が出にくい。

Ⅲ．　ＩＴリスク管理上の論点

1.　　ＩＴリスク管理全般

○IT リスクとは、コンピューター・システムの不具合や運用ミス、外部からの攻撃等により、システムがダウンしたり誤作動、ないし情報漏洩することにより、業務上の影響を被る可能性を指す。

○リスク管理上の条件は、むしろ最低限必要なことを定めることにより、利活用を強力に推進すべきである。

○SLA（サービスレベル管理：Service Level Agreement）の考え方と障害発生時の免責事項と責任事項の明確化が必要。

○メインフレームを中心にネットワーク接続が可能な利用者を限定した「クローズドシステム」が主流であった。こうした環境の下では、以下のようなセキュリティ対策でリスクを回避してきた。

(1) データ・センターへの入退館管理や専用回線利用による物理的な隔離
(2) 独自性の高い基本ソフトや通信プロトコルの使用
(3) 防犯ビデオ等による不正監視

こうした体制下では、外部からのセキュリティ侵害の可能性は低く、内部者による不正行為の防止等に力点が置かれてきた。

○オープン・ネットワーク化の進展は、なりすましやネットワークを流れる情報の盗取・改竄等といったリスクを高めている。加えて、外部からの不正侵入やアクセスを集中することによる業務妨害といったオープン・ネットワークに固有の新たなリスクも現実のものとなっている。

○共同センターでの障害は、一つのプログラムの不具合や運用ミスが複数機関の業務を同時に停止させたり、誤処理を引き起こすことに繋がるため、影響が大きい。

○IT リスク管理とは、システムの安定性（可用性）・信頼性（完全性）・安全性（機密性）を適切な水準にコントロールするため、リスクを分析・評価し、適切な対応を図る活動である。リスクに対しては、回避するだけでなく、移転・低減・受容といった対応もある。

2.　安定性・信頼性・安全性等について

〇IT リスク管理の要点は「安定性・信頼性・安全性・有効性・効率性・遵守性」に整理される。特に安定性・信頼性・安全性が重要な三本柱となる。

(1)　安定性

・ISO（国際標準化機構）の 3 区分（CIA）で言えば A（Availability）＝可用性

・障害や災害等からシステムを保護すること

・典型的なリスクは、システム・ダウンによる業務の停止

(2)　信頼性

・CIA で言えば I（Integrity）＝完全性

・システムが提供する情報や機能の正確性を確保すること

・典型的なリスクは、システムが提供する情報の誤りによる業務トラブルの発生

(3)　安全性

・CIA で言えば C（Confidetiality）＝機密性

・犯罪や不正行為等からの情報やシステムを保護すること（いわゆる情報セキュリティ）

・典型的なリスクは、内部不正による顧客情報の漏洩やハッカーによる不正アクセス

〇システムの安定性を確保するためには、テストの充実による品質向上策が大事だが、その上で障害発生時の連絡体制や、原因究明と復旧のための対応を確立していくことになる。障害対策の基本は以下の 4 点に尽きる。

(1)　予防する＝障害を発生させない。

(2)　局所化する＝影響を広げない。

(3)　回復する＝迅速に復旧対応を実施する。

(4)　再発させない＝原因を究明し横展開(他のシステムに反映)する。

〇障害には、影響度合い等に着目した重要ランクをつける必要がある。例えば

(1)　対外的な影響度

(2)　決済への直結度

(3)　システム停止時間

(4)　代替手段の有無

(5)　レピュテーション（評判）毀損度合い

〇ユーザーは、前提となる事務量等、特にピーク時事務量や同時並行処理される事務の重複度合い等を的確に申告するほか、せめて最終的な負荷テストだけでも主体的に関与する必要がある。

レスポンスタイム（端末に入力してから応答が帰るまでの時間）やスループット（単位時間あたりの処理能力）といったパフォーマンスはシステム評価上の重大なポイントである。

〇何らかのデータが特定のファイル（本来の業務処理とは直接関係しない、いわば裏方ファイルの場合も多い）に溜まりすぎ、オーバーフロー（限界値超え）によりダウンしたり、その結果、他のデータを壊してしまうといった事例もある。

〇情報セキュリティ（安全性）対策の基本線は以下の 5 点である。

(1)　情報資産のうち何を守るべきかを決める。
(2)　どのような脅威があるのかを分析する。
(3)　脆弱性は何かを見極める。
(4)　どの程度の損失が発生するかを見積もる。
(5)　それに応じた防御策を考え、実行する。

〇情報セキュリティ対策のレベルを維持・向上させるためには、IT リスク管理の基本とも共通するが、PDCA の運用サイクルを確立することがきわめて重要である。すなわち

(1)　情報セキュリティ面でのリスク（どこに何がどの程度）を分析する。
(2)　把握したリスクについて技術・運用両面からの対応策を検討・実施する。
(3)　職員（派遣職員、パートやアウトソーシング先職員を含む）の教育・啓蒙を行う。
(4)　情報セキュリティに係る監査により運用状況を確認する。
(5)　監査結果を次回のリスク分析に反映する。

3.　バックアップ・センターと障害対応

〇重要業務を継続するために必須となるバックアップデータの取得・確保も重要なポイント。要員と執務場所がそろっても、肝心の取引データが消失すると業務の継続は不可能になる。失った後に再入手する難度からは「データが何より重要」と言える。

〇バックアップ・センターへの切り替え基準や権限者、手順等をあらかじめ明確に定めておくことは当然である。またカバーする対象業務の範囲や処理能力が、通常時のどの程度なのか、それによって、どのような業務上の制約や変化が発生するのか（例えば、いつもと同じ帳票の出力ができない等）については十分に洗い出した上で、事務処理部門や経営層と認識を共有しておく必要がある。

〇リカバリーのキーポイントは「データの確保」にある。ハードやソフトは再調達可能だが失ってしまったデータは取り返しがつかない。バックアップの方法は大きく３つある。

（１） 磁気（ないし電子）媒体に記録して遠隔地に運ぶ（データ・バックアップ型）
（２） 遠隔地のストレージに一定間隔毎にまとめて送信する。（バッチ型）
（３） データ発生の都度（リアルタイムで）、送信する。（逐次バックアップ型）

〇金融機関について見ると、大規模障害等が発生した際の BCP（業務継続計画）については、用意されている金融機関が多いが、BCM（業務継続管理）は弱い。BCM の実効性を確保するには「テスト」や「訓練」による実地での確認のみであるが、「テスト」と「訓練」が峻別されていない例が多い。「テスト」とは本当に業務が回るかの検証であり、「訓練」はその上で各人が事務手順を身につけるための練習である。テストによりフィージビリティ（実現可能性）を確認できていないのに漫然と訓練を繰り返しても意義が乏しい。

4. 共同化における委託先管理手段

〇委託先との役割分担や責任範囲は、契約書やサービス仕様書によって明確に定めておく必要がある。さらには SLA の締結と定期的な見直しを通じ、具体的なレベルでも取りきめていくことが適当である。

〇委託先の監査の方法には以下のような選択肢がある。自社がおかれた状況とシステムの重要性に照らして、必要十分なチェックを実施できるように決めることが適当である。
⑴ アウトユーサー（受託者）の社内外監査結果を開示してもらう。
⑵ ユーザー自らが監査に立ち入る。
⑶ 第三者の専門家等に監査してもらって、結果の報告を受ける。

〇地方銀行のシステム共同化における各種委託先管理手段の導入率は高く、共同化行の約８割で、委託先が実施した外部・内部監査結果の入手や定期的な立入検査を実施 （「日銀調査」より）

⇒課題：各種委託先管理手段の導入が奏功して、多くの共同化行が委託先管理のスキルは向上したと考えている。もっとも、個別金融機関ごとの外部委託と比較すると、システム共同化は、委託先との関係の希薄化に伴う委託先管理の実効性低下のリスクがある。各共同化行は、委託先管理の実効性を常に検証することが重要である。

5.　クラウド・コンピューティングによる共同化の留意点

○クラウド・コンピューティングの場合、委託先管理の実効性を確保することが難しくなることは事実である。しかし、システム構築・運営への関与度が少なく、提供されたサービスを利用するだけであっても、契約による役割分担と責任関係の明確化が必要なことは同じである。

○クラウドについて、特に海外法人に預ける際には、情報の取り扱いに関する日本の法律が全く適用されないので、何か問題が起きても把握できず保護・救済されないリスクをチェックしておく必要がある。国が変わり、複数の企業をまたいだ場合に、問題判別や情報漏洩時の責任は誰が負えるのか。問題を指摘しても否認されればおしまいということになりかねない。さらには「廃業されたら自社の事業も終了という事態にならない担保」を確認しておきたい。実際、多くの企業から重要業務を多数引き受けたクラウドシステムがダウンした場合の世界的な影響の大きさは、計り知れない。

○システムの開発や運用を外部に委託している場合には、委託先に対する管理がリスク管理の要となる。例えば ASP、SaaS のようなシステム利用の色彩が濃い形態であっても、SLA に基づく報告書面や監査結果の入手等、モニタリングに活用可能の管理手段は存在する。委託形態にふさわしい管理手段を採用して、委託先管理の実効性向上に努めることが重要である。

Ⅳ.　次期システム検討体制の確保に係る論点

○共同化した地方銀行の約６割は次期システムの検討に着手しておらず、うち約半数は現行システムの更改時期を想定していない。共同化を予定していない行の約８割が、業務運営の自由度を損なう懸念やシステム開発の迅速性・機動性低下をその理由として挙げている。（「日銀調査」より）

⇒課題：共同システムの稼働後、これを支える技術の変化や顧客サービス拡充の必要性等により、いずれシステムの更改を見込むべき時期が到来するが、共同化行の過半が次期システムの検討に着手していない。次期システムに向けた更改内容検討に際しては、共同行間での調整等に時間がかかることが予想され、検討体制の適時な立ち上げや、必要な人材確保が求められる。