

金融機関の拠点被災を想定した 業務継続計画のあり方

平成 14 年 3 月
日 本 銀 行

1. はじめに

今日の金融機関では、通常の業務体制の維持・継続ができなくなるケースを想定したコンティンジェンシー・プランを整備することが重要な課題となっている。こうした背景には、業務内容の変化に伴い大規模で多様な決済、市場性取引を切れ目なく行う必要性が高まっていること、さらには、決済をはじめとする業務の情報処理システムへの依存度が高まっていること、等を指摘できる。万一、大規模な決済を処理する金融機関において業務が中断した場合、信認の喪失等による当該金融機関への影響が甚大であるほか、金融・決済システムの安定性が脅かされる恐れがあるため、日本銀行でも金融機関の業務継続計画の整備に強い関心を持っている。

既に、多くの金融機関では、主要システムの機器・回線の障害に備えた二重化などの整備が進んでいるが、大規模な災害等を想定した備えについては、最近の決済リスク・プロファイルの変化（日中流動性管理ニーズの高まり等）や事務処理高度化（STP化等）を踏まえて、改めて点検の必要性があるものと考えられる。また、昨年9月の「米国同時多発テロ事件」においても、日頃の業務継続計画整備の重要性が再認識されたといえる。本稿では、コンティンジェン

シー・プランのうち、とくに、重要業務を行う本部ビルや電算センターなどの業務拠点が不慮の事故や災害によって、物理的に機能停止を余儀なくされる状況（拠点被災）を想定した金融機関の業務継続計画のあり方について整理する。

本稿は、金融機関内部で、あるいは考査等の場において、金融機関の健全性維持という観点から議論を深める際の材料との位置づけにある。また、今後の議論や技術環境の変化などを踏まえて修正を加えていくことを想定している。

もとより、金融機関の業務特性やリスク・プロファイルは様々なため、継続すべき業務や必要とされる業務再開までの時間は異なり、業務継続の対応にも多様なアプローチがあり得る。各金融機関においては、本稿の考え方をひとつの材料としつつ、それぞれのリスク・プロファイル、業務の重要度などを踏まえて的確に対応していくことが期待される。

2. 被災想定と影響度の分析

業務継続計画とは、金融機関にとって重要な情報システムや業務機能を予め選定したうえで、それらが中断から円滑かつ速やかに再開・復旧するように備える有事の際の対応プランのこと

である。

業務継続計画の策定に当たっては、①金融機関業務に対する潜在的脅威の洗い出し、②被災の影響度評価と優先的に継続を図るべき業務上の必須項目の特定、などを行ったうえで、③具体的な業務継続手段を整備するのが一般的である。以下では、こうしたステップに沿って対応のポイントを整理する。

まず、金融機関業務に対する潜在的な脅威となりうるリスク・シナリオのうち、「拠点被災」に関連するものとしては、例えば、自然災害（地震、洪水など）、技術的災害（大規模停電、通信途絶）、人的災害（テロ、火事など）が挙げられる。ただ、これら潜在的な脅威は、当該金融機関のおかれている状況等を踏まえて検討する必要がある。

次に、こうした被災想定に基づいて、影響度の分析を行う必要がある。具体的には、拠点被災によって、自社のどの業務がどういう形で中断するのか、それによって生ずる、決済不能、信認の低下、資金繰り逼迫、急なポジション調整等が自社や取引相手先、顧客などにどの程度のダメージをもたらすのか、といった点を評価する。

そのうえで、拠点被災時であっても継続すべき業務を特定する。拠点被災のような異例事態においては、時間制約の強いなかで利用可能な経営資源が限定される。このため、継続を図る業務としては、当然のことながら重要度が高く、短時間での業務再開が求められるものが優先される（例えば、決済や資金繰り業務など）。

3. 業務継続手段の検討

以上を踏まえて、拠点被災時における、重要業務の継続手段について検討する。

まず、電算センターが被災し、情報処理システムの機能が停止した場合、事務量が多く業務処理がシステムに依存している度合いが高いほど、システムを利用せずに業務を継続することは困難である。こうしたケースでは、隔地の電算システム（バックアップ・センター）とバックアップ・データを利用して業務継続を図ることが必要である。ただし、事務量がさほど多くなければ、システムの力を借りなくとも、隔地保管しておいたデータを利用して、手作業などの代替的な手段により、業務の継続が可能な場合もあり得る。

一方、重要な事務拠点（オフィス）の被災時に業務の継続を図るためには、何らかのかたちで代替的なオフィス（バックアップ・オフィス）を利用することが不可欠である。バックアップ・オフィスは、隔地保管されたデータと各種端末や事務機器などを備え、必要に応じて業務要員がメイン・サイトから移動して業務を継続することになる。

次に、バックアップ・サイト（バックアップ・センターとバックアップ・オフィスを総称したもの）の機能について、カバーする業務の緊要性（当日中の処理が必要か）、事務量、人的資源の活用度合等を勘案して、業務再開までの時間、再開後の業務処理の所要時間、バックアップ・サイトの稼働期間、等を想定する必要がある。

例えば、被災から業務再開までの時間についてみると、バックアップ・サイトに設置してある機器が即座に利用可能な状態であれば、短時間で業務を再開することが可能だが、すぐに設置機器を利用できない場合（被災後に、コンピュータを立ち上げたり、機器を運び込むケースなど）、業務の再開は遅くなる。また、バッ

クアップ・データの取得頻度が低いと（業後に1日分をまとめて取得する等）、被災時のデータ逸失により、業務の再開が困難になる。高度なバックアップ体制は維持コストが大きい、被災時の影響と業務の重要性を踏まえて、適切な業務継続体制を構築することが求められる。

また、バックアップ・サイトの運営方式については、様々な選択肢を十分検討すべきである。自前でビルやシステム等を設置する方法のほか、既存設備（僚店、事務センター等）を有効利用する、外部業者にアウトソースする、他社と相互にバックアップ・サイトを提供し合う、バックアップ・サイトを共同運営する、などの選択肢があり得る。各々の選択肢にはそれぞれメリット、デメリットがあるが、これらを適宜活用していくことで、効率的にバックアップ体制を構築していくことが重要である。

4. 留意点

次に、拠点被災対応を検討する場合にとくに留意を要する点について、述べることにしたい。

第1に、バックアップ・サイトの所在地については、メイン・サイトと共倒れにならないよう、同一のリスク・ファクター（火災、停電、地震等）を共有しない程度にメイン・サイトから離れて設置すべきである。拠点被災が発生する状況では、その周辺地域一帯も同時に機能停止する可能性が否定できないので、至近距離にバックアップ・サイトを設けることは適当ではない。もっとも、メイン・サイトから要員が駆け付けることを計画している場合には、あまりに遠隔地であると業務の再開までに時間を要することとなるので、適度に近い距離であることも求められる。こうした様々な要請を踏まえ、バランスの取れた判断を行うことが重要である。

第2に、拠点被災時の対応が実効性を発揮するために、業務継続体制の整備を具体的に行うべきである。例えば、緊急時を認定し、バックアップ・サイトへの移行を決断する責任者などの意思決定・指揮命令系統の明確化や、連絡体制の整備が必要である。また、業務処理手順（メイン・サイトへの再移行の手順も含む）を分かりやすい形で書面化しておくことも、組織全体で業務継続計画を共有するためには不可欠である。さらに、緊急時には通常と大きく異なる業務処理を行うケースが多いので、日頃から定期的（少なくとも年1回）に訓練を実施して、要員の習熟を図っておくべきであろう。また、こうした訓練は、業務処理手順の適切性を確認し、必要に応じて改善を図るうえでも役立つものと思われる。

第3に、拠点被災の検討には、何よりも経営陣の関与が不可欠である。被災対応の検討およびその実施には、多くの経営資源の投入が必要になるため、経営の強いコミットメントがない限り、プロジェクトは円滑に進まない。また、想定する拠点被災の範囲、継続すべき重要業務、バックアップ・サイトの場所・機能・運営形態などについても、経営レベルでの高度な判断をする必要がある。

5. おわりに

米国同時多発テロ事件の際には、大半の金融機関はバックアップ・サイトを利用して業務を継続したため、業務の中断は最小限に止まり、決済不能の影響が資金や証券の受取をあてにしていた他の主体にシステミックに拡大するなどの事態を回避することができた。わが国においても、拠点被災による業務中断の影響がシステミックに拡大しないよう、十分な備えが望まれる。

日本銀行では、経営の健全性を維持するためのリスク管理という観点から金融機関に適切な対応を期待しているほか、決済システムの安定性を維持するという面からも金融機関の業務継続計画が重要であると考えている。こうしたことから、今後ともオフサイト・モニタリングや考査の場を通じて、拠点被災対応を含めたコンティンジェンシー・プランのあり方やその高度化に向けた施策について、金融機関と議論していくこととしたい。

(本件に関する照会先)

日本銀行 考査局

リスクアセスメントグループ

| | |
|----|------------------------------|
| 鎌田 | 03-3277-2513 |
| | sawaichirou.kamata@boj.or.jp |
| 荒井 | 03-3277-2005 |
| | takashi.arai@boj.or.jp |
| 和瀬 | 03-3277-1728 |
| | koutarou.wase@boj.or.jp |