情報システムのディザスターリカバリへの取り組み

１．はじめに

企業活動において，コンピュータシステムの利用が不可欠な中，東日本大震災クラスの地震やその他の自然災害によりシステムが被災し，長期間利用できない，重要データが復旧できないなどの状況となった場合，業務に大きな支障をきたすことになる．

本稿では，このような自然災害時のシステムリスク低減を図るために取り組んだ対策，いわゆるディザスターリカバリ（Disaster Recovery）への取り組みについて述べる．

２．概要

今までの「コンピュータ安全対策」は予備装置を配置するなどして「いかにシステムダウンを回避するか」を求めていたのに対し，「ディザスターリカバリ」は，逆にシステムダウンを前提とし，「いかに速く確実に復旧するか」を目指している．

このため，ディザスターリカバリの計画策定にあたり，検討の初期段階から，実際にリカバリできることをどのようにして担保するかを念頭に置く必要があった．

実現性の高い計画を策定するため，各検討事項に対し，どのような考え方で方針を決め，リカバリ計画および手順を作成したかについて紹介する．

３．ディザスターリカバリの方針

計画の策定にあたり，以下の４つのカテゴリについて，検討を行い，方針を決定した．

３．１　復旧対象・復旧範囲・復旧レベル

ディザスターリカバリの計画において，「全てを守ることに固執すると，究極の事態では，かえって何も守れない状況に陥る危険性が高まる」と言われている．

この考えに基づき，復旧対象は，もっとも重要な基幹システムに限定した．復旧範囲は，利用者の業務に直結する機能のみに絞り，サーバの稼働監視機能などは範囲外とした．復旧レベルは，早期復旧を優先し，システムの拡張性や可用性などは現行と同レベルを求めないと決めた．

３．２　復旧時点のデータ・復旧時間

復旧時点のデータについては，システム被災前のどの時点のデータに復旧できれば業務を再開できるかという視点で検討した．過去の障害事例から業務再開が可能な時点を分析し，復旧データは被災日の前日時点のデータとすることとした．

復旧時間の検討にあたり，まず，システムが全損した場合の復旧時間を試算した．その結果，サーバなどの機器調達やシステムの再構築が伴うことから，復旧に２ヶ月半程度の時間を要し，業務に大きな支障をきたすことが判明した．このため，早期の業務再開という方針のもと，復旧時間の目標を７日と設定し，これを実現できる計画の策定に取り組んだ．

３．３　復旧に使用する技術

復旧にどのような技術を使用するかの判断基準の一つが，費用対効果である．

代表的なリカバリ方式には，本番システムのダウンと同時に待機システムへ切り替わる「フェイルオーバー方式」やデータを常に同期させて別サイトへバックアップを行う「レプリケーション方式」などがあるが，これらの方式を使用する場合，新たな技術の導入と高額な投資が伴う．

このため，本計画では，既に導入実績のある技術について検討し，「仮想化技術」を使用することとした．

この技術は１台のサーバを何台もサーバがあるかのように使える技術であり，これまでサーバの台数削減やシステムの延命対策に使用してきたが，本計画では復旧時間の短縮に使用する．

３．４　自社固有資産の保護

復旧には，システム要員，データ，自社開発プログラム，ソフトウエア製品，ハードウエア製品，ネットワーク設備，電源・空調設備を用いるため，これらの全てを保護しなければならない．

特に，自社固有の資産であるデータと自社開発プログラムについては，外部調達できないことから，確実に保護できる仕組みが求められる．このため，本計画では，自社固有資産の保護対策を強化する方針で，これらの資産を本社サーバ室と別サイトの２箇所に保管するというバックアップの二重化を決めた．

４．ディザスターリカバリの計画および手順

前述の方針決定をもとにリカバリ計画を作成し，その具体的な手順を確立した．

４．１　計画

あらゆる被災状況に対応した復旧計画を立てようとすると，復旧方法や復旧手順が複雑になり，早く確実に復旧できないおそれがある．このため，もっとも重度な被災状況に対する復旧方法を計画し，それ以外の状況に対しては，その復旧方法を応用し対処することとした．

今回計画した被災状況と復旧方法の概要は次の通りである．

《被災状況》

本社サーバ室が被災を受け，サーバや通信機器が全損し，電源・空調設備まで使用不能に陥った．

《復旧方法》

① 本復旧を終えるまでの繋ぎとして，７日間で仮設のシステムを社外データセンターに構築する．

② 仮設のシステムを使い，重要業務から優先的に再開し，業務への支障を最低限におさえる．

③ 本復旧を終えた後に仮設システムから本システムへ切り替え，全ての業務を本格的に再開する．

４．２　手順

計画した復旧方法を確実なものにするには，事前に復旧手順を確立させる必要がある．この計画で特に重要なポイントは，仮設システムを７日間で構築できるかである．

図１に仮設の基幹システムの具体的な構築手順を示す．構築作業では，随所で仮想化技術を使用することとしたが，有事の際はベンダーの支援が受けられず，自社で全て対応せざるをえない状況が想定される．このため，実際に仮設システムを構築し，手順を確立させた．

５．おわりに

東日本大震災の発生以降，ディザスターリカバリの重要性を強く認識した企業は，自然災害に耐えうる堅牢なデータセンターの活用や自然災害の少ない地域へデータをバックアップするなどの対策を施した．

当社においても，今回，ディザスターリカバリ計画を策定して一定の対策を施したが，コンピュータシステムの重要性がさらに高まる中で，近い将来，復旧対象の拡大や復旧時間のさらなる短縮が求められると考えている．

従って，2019 年を目標に基幹システムのデータセンター移設を計画するなど，災害に強いシステム作りに今後も取り組んでいく．

中川　淳一（情報システム部）

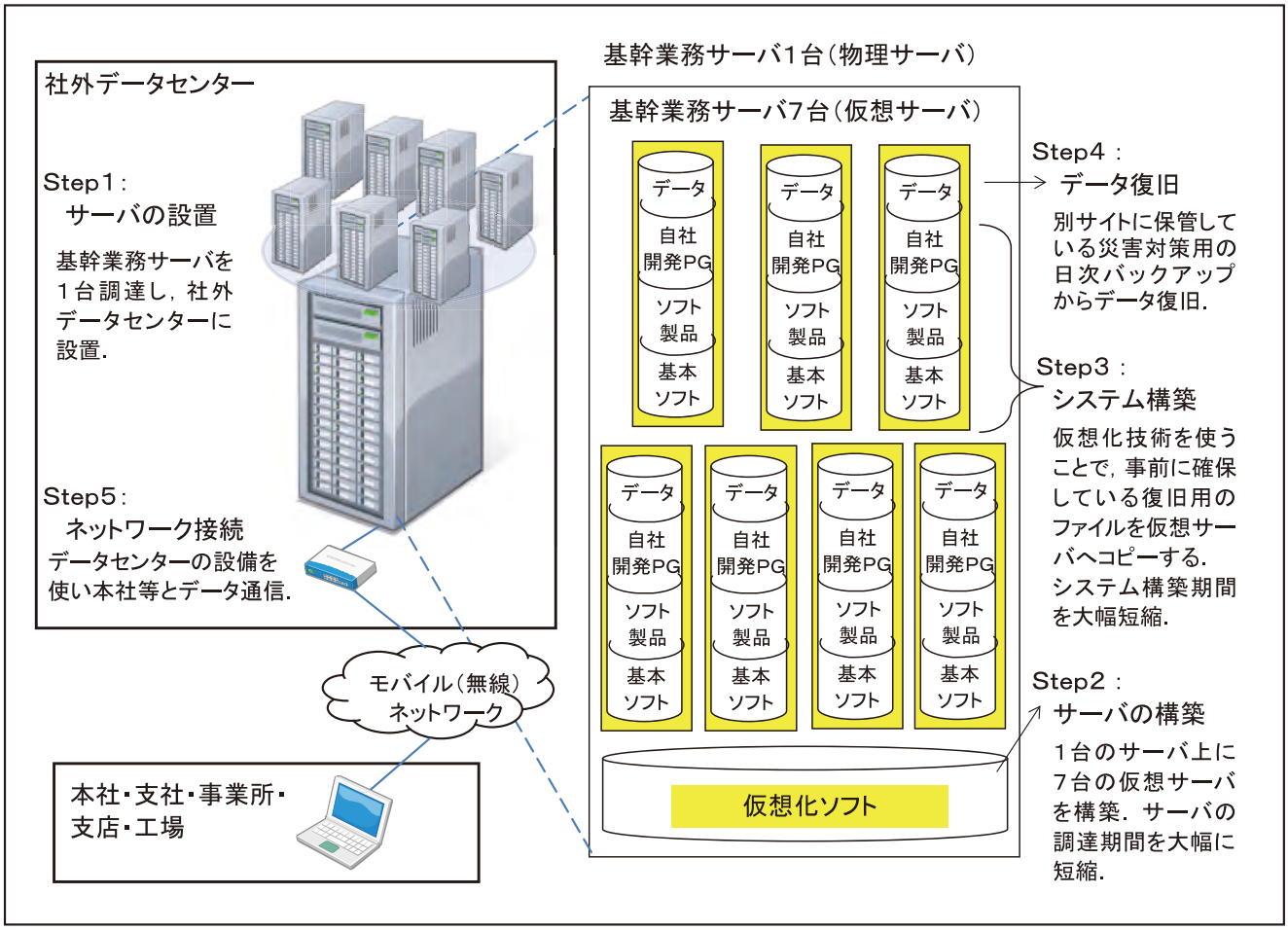

図１　仮設の基幹システム構築手順