

IT-BCP対策ソリューションへの取り組み

土井 丈志*

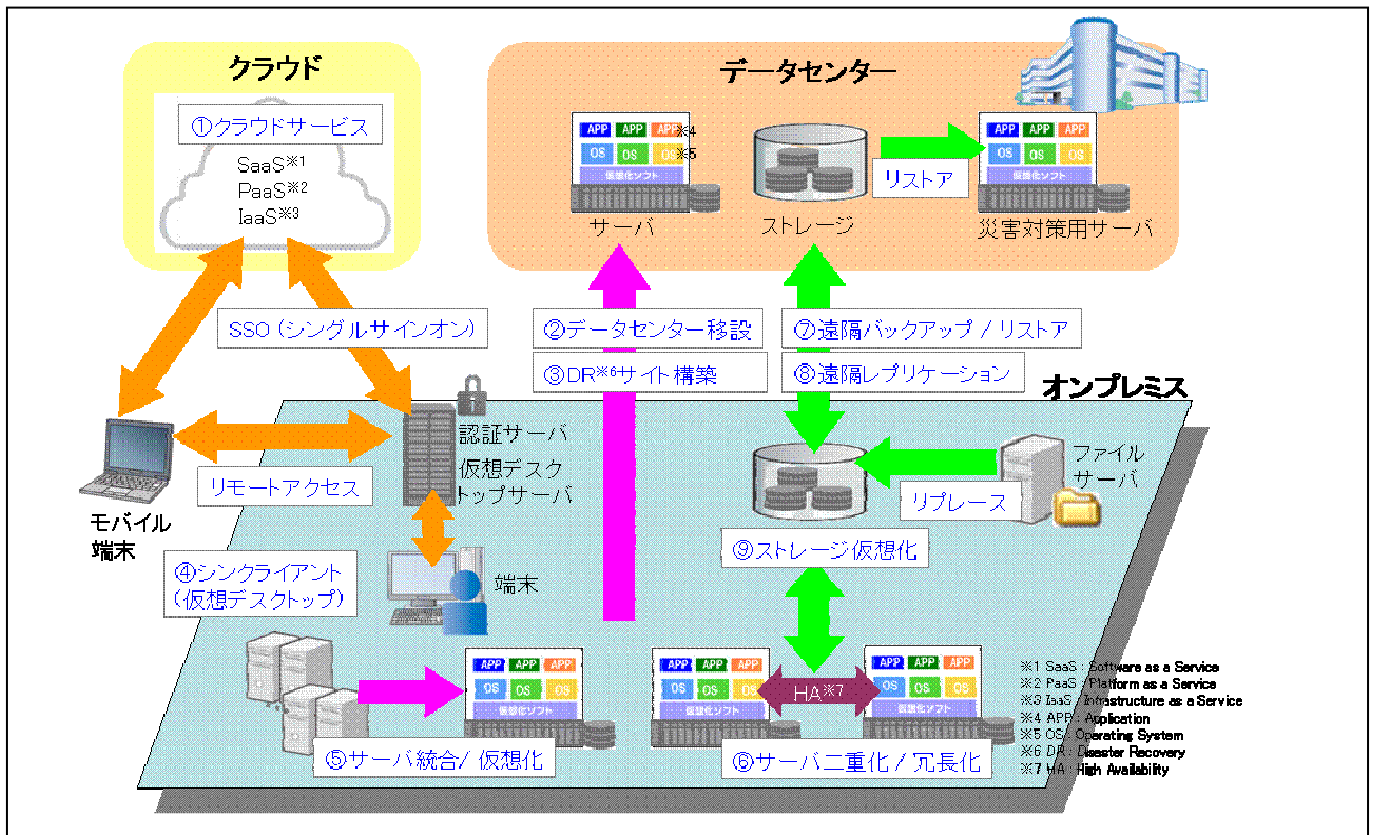
Commitment to IT-BCP recovery solution

要旨

東日本大震災以降、各企業においては災害対策の必要性が認識され、事業継続計画(Business Continuity Plan (BCP))の策定や改善が進められている。情報システムは、企業活動を支える重要な役割を担っているため、情報システムの停止やデータ消失は事業継続に大きな影響を与えることになる。IT-BCPとは災害など予期せぬ事象が発生した場合でも情報システムを継続し、早期復旧を可能とするための行動計画や準備体制のことを指している。情報システムを停止させないための事前対策としてはシステムの2重化、データセンター内へのシステム設備の移設、システムのクラウドサービスへの移行などの予防的措置を講じておくことが有効である。また、計画停電や交通機関の停止などによる間接的被害への

対応など多くの課題に対する検討、対策が必要である。

多岐にわたるIT-BCPにおいて最優先で準備・実施しておくべき対策は、情報システムが停止した時の早期復旧、再開を目的とした災害復旧(Disaster Recovery (DR))対策である。株式会社三菱電機ビジネスシステム(MB)では、最重要となるデータの消失を回避するためのバックアップデータの遠隔地保管や、早期復旧を目的としたDRサイト構築による2拠点化などの対策ソリューションを中心として、仮想化をはじめとする効果的な技術を活用しながら、顧客のニーズに応えられるIT-BCP対策ソリューションの提供に取り組んでいる。



仮想化とデータセンター活用による情報システムのIT-BCP対策

①クラウドサービスや②データセンターへの移設、③DRサイト構築で情報システムの停止を回避する事前対策。④デスクトップ仮想化による在宅勤務環境の構築。仮想化で⑤サーバ統合、⑥ストレージ仮想化によるコスト削減や、⑦サーバ二重化による可用性向上。システムが停止した時の復旧を目的とした災害対策としてDRサイト内のストレージに⑧遠隔バックアップや⑨レプリケーションによるデータ転送を行い災害対策サーバにてシステムの早期復旧・再開を実現。

1. ま え が き

東日本大震災後、企業のIT-BCP対策に対する取り組みに変化が起きている。理由としてはBCPに対する意識が高まったことや、技術の進化による対策ソリューションの多様化などが挙げられる。特に震災後は予防的措置だけで災害全てに対応することは困難という認識からシステムが停止した場合のDR対策への取り組みが注目されている。本稿では多岐にわたるIT-BCP対策の中からDR対策に焦点を置き、早期復旧するためのDR対策ソリューションの特長やDR対策に効果的な技術について紹介し、最後に導入事例について触れる。

2. IT-BCP対策の概要

IT-BCP対策は災害などが発生した場合でも情報システムを停止させないための事前対策と、停止した時の復旧・再開のためのDR対策に大別される。

2.1 事前対策

事前対策には情報システム設備のデータセンターへの移設やシステムのクラウドサービスへの移行などがある。また、震災後に発生した計画停電や交通機関の停止による間接的被害に対応するためのリモートアクセスやデスクトップ仮想化などの在宅勤務環境の整備も事前対策の一つである。

2.2 DR対策

DR対策でのデータ復旧方法には技術の進歩もあり、多くの方法があるが大きく分けると以下の3つに分類できる。

- (1) バックアップ媒体の輸送による遠隔地保管
 - (2) レプリケーションによる遠隔地保管
 - (3) DRサイト構築によるサイト間フェイルオーバー
- (1)のバックアップ媒体の遠隔保管はDR対策では一般的な方法でデータ消失を防ぐためには有効な対策であるが、この方法は復旧に多くの時間が必要となり早期復旧を要する場合には不向きである。早期復旧を実現するには(2)のレプリケーション技術による遠隔地保管や(3)のDRサイトを構築してサイト間でシステムを切り替えるといった対策が必要である。

2.3 災害発生時の情報システムの復旧目標

DR対策は復旧すべき情報システム毎に災害発生からいつまでにシステムを再稼働すべきかの目標時間 (Recovery Time Objective (RTO)) や、災害から遡っていつの時点のデータに復旧するか(Recovery Point Objective (RPO)) を定める必要がある (図1)。

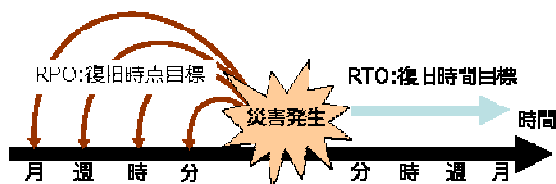


図1. DR対策におけるRPOとRTOの関係

3. 早期復旧を目的としたDR対策モデル

災害時の早期復旧を目的としたDR対策は、レプリケーション技術を使って遠隔地にデータを保護する方法と、これに加えてDRサイトを構築しシステムを切り替え再開する方法がある。この2つの方法を組み合わせたDR対策ソリューションを目標復旧時間別に3つにモデル化 (表1) して、それぞれの機能や特長を説明する。

表1. 早期復旧を目的としたDR対策モデル

対策モデル	モデル1	モデル2	モデル3
対策ソリューション	バックアップレプリケーション	ソフトウェアレプリケーション	ストレージ統合レプリケーション
目標RTO	数日	1日	数時間
目標RPO	1日	数分～数時間	数分～数時間
保護対象データ	バックアップデータ	本番データ	本番データ・OSアプリケーション
導入コスト	低	中	高

3.1 対策モデル1：バックアップレプリケーション

各サーバのバックアップをバックアップストレージに集約し、ネットワーク経由でバックアップデータをDRサイト側のストレージにレプリケーションする (図2)。

災害発生時にはOSやアプリケーションなどの環境構築済みの代替機にバックアップデータをリストアする。バックアップストレージは、レプリケーションソフトウェアをインストールしたストレージや、レプリケーション機能を持った専用ストレージを使用する。この方法の特長はメインサイト側サーバのバックアップの運用を変えずに追加する形で対策を施すことが可能な点である。

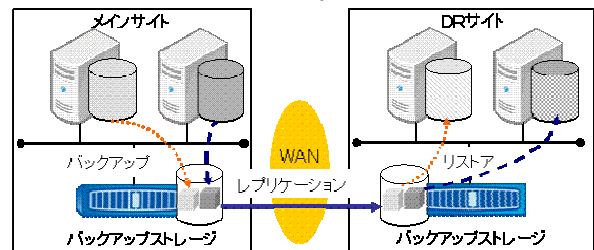


図2. バックアップレプリケーション

3.2 対策モデル2：ソフトウェアレプリケーション

メインサイト側サーバとDRサイト側サーバにレプリケーションソフトウェアをインストールしてサーバ間でレプリケーションを行う。メインサイト側サーバで更新された業務データをネットワーク経由でDRサイト側サーバのディスクへ直接レプリケーションする (図3)。災害発生時にはDRサイト側サーバでシステムの切り替えを実施する。バックアップからのリストアが必要ないため比較的短時間でシステムを再開することが可能である。このモデルの特長はサーバ1台だけの災害対策にも採用できる点である。ただし、レプリケーション対象は業務データだけのため、メインサイト側サーバでOSやアプリケーションなどの更新を行った場合にはDRサイト側サーバも手動更新をする必要がある。

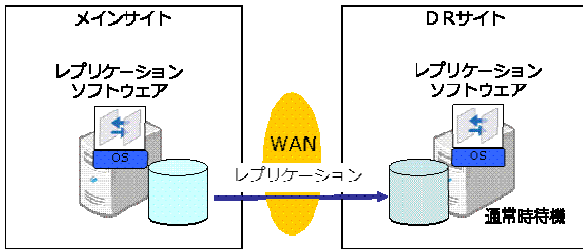


図3. ソフトウェアレプリケーション

3.3 対策モデル3：ストレージ統合・レプリケーション

レプリケーション機能を持ったストレージ間でレプリケーションを行う。メインサイト側で複数サーバのストレージ統合環境を構築し、ストレージには各サーバのOSやアプリケーションを含めたデータが保管される。メインサイト側ストレージ内で更新されたデータをDRサイト側ストレージへレプリケーションする（図4）。

災害発生時には、DRサイト側の各サーバでシステム切り替えを実施する。このモデルの特長は、ストレージ統合された複数サーバのOSやアプリケーションを含めた更新データがDRサイト側ストレージに同期されるため、短時間で複数サーバのシステムの再開が可能となる点である。また、複数サーバを同一の方法でレプリケーションするため運用の統一化を図ることができる。ただし、複数サーバのデータを全てストレージに格納するため高信頼のストレージが必要となり導入コストは割高となる。

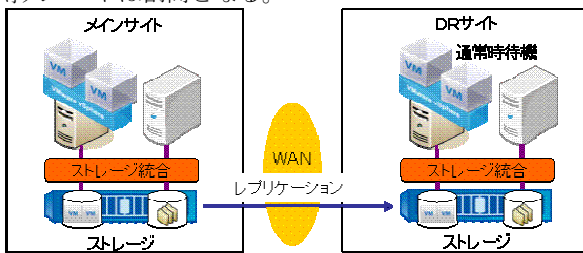


図4. ストレージ統合・レプリケーション

4. DR対策に効果的な技術

DR対策で必要となるバックアップやWAN（Wide Area Network）でのデータ転送を実現するために効果的であると思われる技術や、DRシステム構築時にコスト削減効果を得ることができる仮想化技術について紹介する。

4.1 レプリケーション

レプリケーションとは本番サーバのデータを待機サーバやストレージに複製しデータを同期する技術である。レプリケーションにはリアルタイムに同期する方式と非同期方式、一定間隔で差分データをまとめて転送する方式がある。DR対策の基本である遠隔地へのデータ複製には欠かせない技術である。レプリケーション環境は、システム規模、対象データ量、コストなどを勘案して適切なレプリケーションソフトウェア製品を選定し、必要なストレージを準備し構築する。

4.2 重複排除

重複排除とは、データの中で重複している部分をあらかじめ

め排除し、実際にディスクに格納するデータ量を小さくする技術である（図5）。重複排除に対応したバックアップソフトウェア製品を利用することによりバックアップディスクの使用量削減、バックアップ時間の短縮といったメリットが期待できる。ネットワークで遠隔地にデータを送る場合に、事前に重複排除処理を行い送るべきデータ量を縮小することで回線の帯域幅を抑えることが可能である。重複排除はDR対策では非常に有効な技術であり今後も進化していく技術と考えられる。

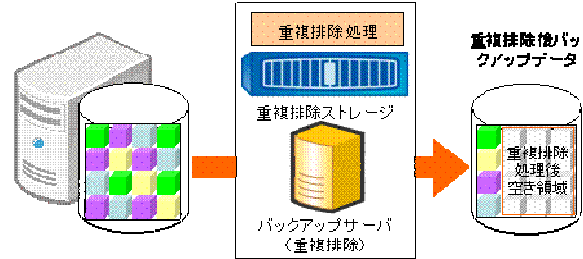


図5. 重複排除イメージ

4.3 イメージバックアップ

イメージバックアップとは、ディスクのビット列をそのままバックアップする方式で、ディスクをまるごとイメージでバックアップする。リストアは専用のリカバリCDでサーバを起動後、バックアップイメージ全てをディスクにリストアする。従来のデータバックアップからの復旧方法に比べて圧倒的に速く手順もシンプルなため、復旧時間の短縮を目的とするバックアップとして有効である。

4.4 仮想化技術

DR対策に有効な仮想化技術としてサーバ仮想化が挙げられる。サーバ仮想化により、1台の物理サーバ上に複数の仮想サーバを稼働させることができる。DRサイトの構築には基本的に本番サーバと同数の待機サーバを用意する必要があるが、待機サーバを仮想化で構築することにより物理サーバ数を減らすことができ、ハードウェア費用や省スペース化といったコスト削減が可能である。さらに、仮想化はシステムのハードウェア依存性を排除することが可能なため本番サーバと同等の機器でなくても待機サーバ環境を構築することが可能である。また、仮想化の特長であるカプセル化によりハードウェア構成、OS、アプリケーション、データをファイルとしてディスクに格納される。仮想サーバ全体がファイル化されるため、そのファイルをバックアップやレプリケーションを活用し遠隔地へ保管すれば仮想サーバ全体の保護が可能となる。

5. 導入事例

3章のDR対策モデルをベースにしたIT-BCP対策ソリューションの導入事例を2例紹介する。

5.1 バックアップレプリケーションDR対策事例

5.1.1 概要

複数サーバのデータ消失回避と低コストが要件であった

ため、3.1項の対策モデル1：バックアップレプリケーションを採用し、かつ待機サーバを仮想化で1台に集約している事例である。メインサイトは東京にあり大阪にDRサイトを新規に構築し、バックアップ保管に重複排除バックアップストレージData Domain^(注1)を採用し両拠点に設置した(図6)。東京側のストレージで重複排除処理によりバックアップデータの重複している部分をあらかじめ除去しバックアップデータサイズを縮小し、ストレージのレプリケーション機能で大阪側のサイトへバックアップデータの複製を実施する。

災害発生時は、大阪のData Domain^(注1)から待機サーバへリストアを行い業務再開する。

5.1.2 導入効果

メインサイトの東京側で重複排除にてバックアップデータ量の削減をおこなうことによりバックアップ時間の短縮とネットワーク負荷低減を実現した。なお、待機サーバを仮想化で1台に集約することによりコスト削減が図られている。

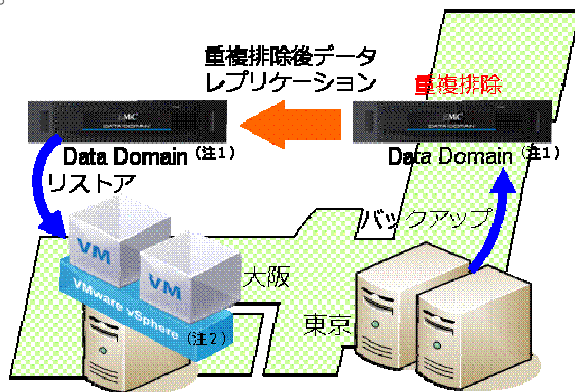


図6. バックアップデータレプリケーション

5.2 ソフトウェアレプリケーションDR対策事例

5.2.1 概要

販売管理システムの1日以内の業務再開と可能な限り災害発生前の最新データへの復旧が要件であったため、3.2項の対策モデル2：ソフトウェアレプリケーションを採用し、かつ待機サーバを仮想化で1台に集約している事例である。メインサイトは東京にあり北海道にDRサイトを新規に構築し、販売管理サーバのデータベースのデータをレプリケーションソフトウェアDouble-Take Availability^(注3)にて北海道側の待機サーバへ非同期レプリケーションを行う(図7)。災害発生時は北海道側の待機サーバに手動で切り替えを行い業務を再開する。

5.2.2 導入効果

データベースの更新データを即時に北海道側待機サーバへレプリケーションを行うため、災害直前のデータに復旧可能なこととリストア作業が不要なため短時間で業務の再開が可能である。なお、待機サーバを仮想化で1台に集約することによりコスト削減が図られている。

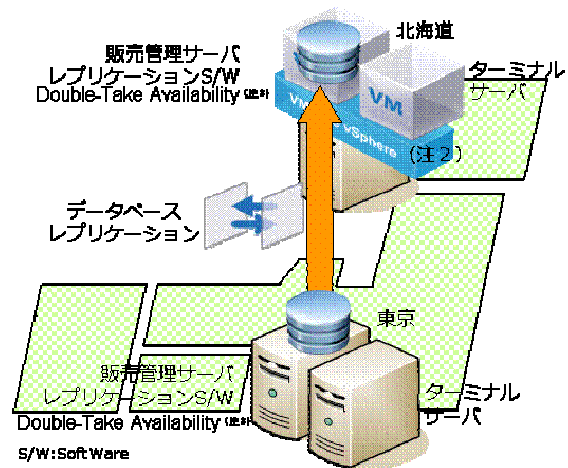


図7. ソフトウェアレプリケーションによる2拠点化

(注1)Data DomainはEMC Corporationの登録商標である。

(注2)VMwareはVMware, Inc.の登録商標である。

(注3)Double-TakeはVision Solutions, Inc.の登録商標である。

6. むすび

現在の企業活動には情報システムは不可欠であり、不測の事態による情報システムの停止は企業活動に大きな影響を与える。IT-BCP対策は一度実施すれば終わりではなく、システムの更新や技術の変化によって対策の見直しや改善を継続的に行っていく必要がある。

情報システムを停止させないための予防対策や災害発生時の事前対策は保険的要素が多く、顧客は必要最低限の投資コストで安心を得られる対策ソリューションを望んでいる。

今後も時代に応じた技術や製品を取り入れながら、顧客ニーズに対応できるIT-BCP対策ソリューションの提供に取り組んでいく所存である。

参考文献

- (1) 巻頭特集 3.11の教訓を生かした災害に強いBCP策定のポイントとITソリューションとは、MELTOPIA, 2012年4月号 (No.175)
- (2) 独立行政法人 情報処理推進機構：事業継続のための高回復力システム基盤導入ガイド (概要編)
- (3) 独立行政法人 情報処理推進機構：情報システム基盤の復旧に関する対策の調査報告書 2012年7月
- (4) 経済産業省：ITサービス継続ガイドライン改訂版 平成24年