ＩＴ－ＢＣＰ対策ソリューションへの取り組み

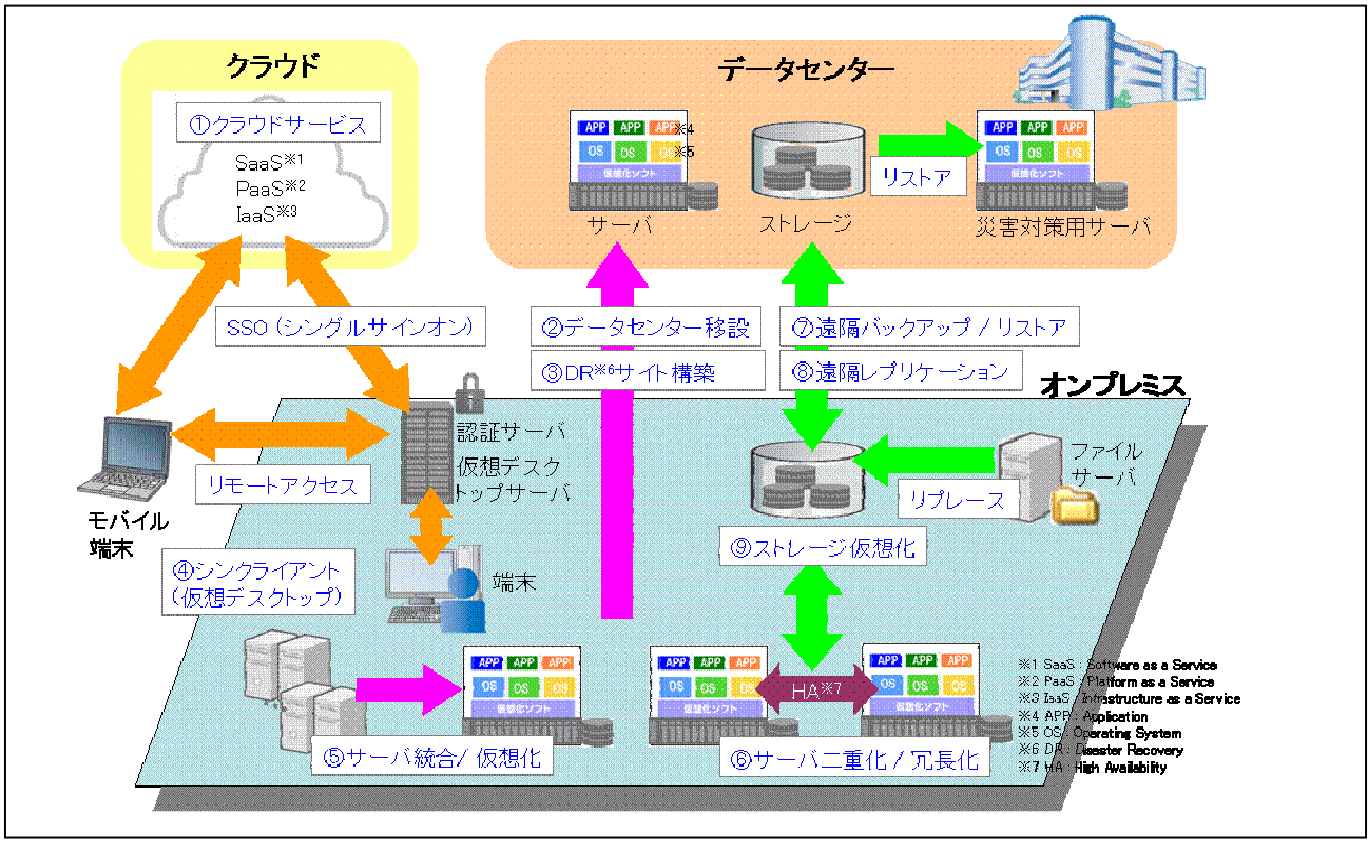
土井丈志*

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しての検討，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、⑨ストレージ仮想化によるコスト削減や，⑥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⑦遠隔バックアップや⑧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

(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）。

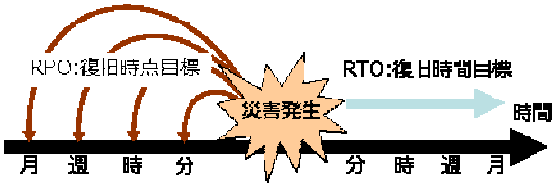


図１．ＤＲ対策におけるＲＰＯとＲＴＯの関係

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。

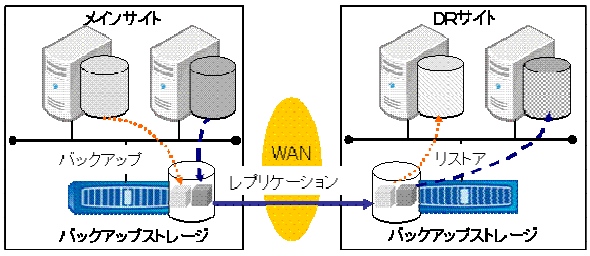


図２．バックアップレプリケーション

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。

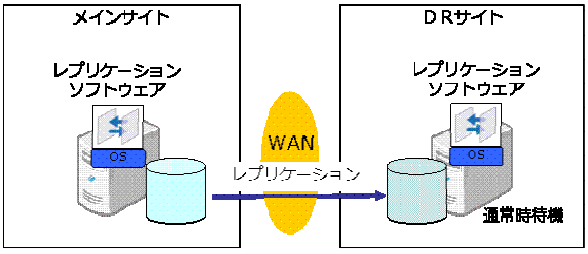


図３．ソフトウェアレプリケーション

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な点である。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。

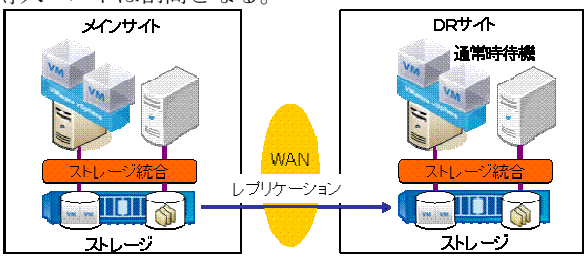


図４．ストレージ統合・レプリケーション

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。

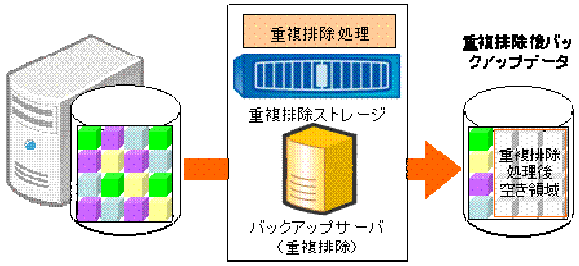


図５．重複排除イメージ

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動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。

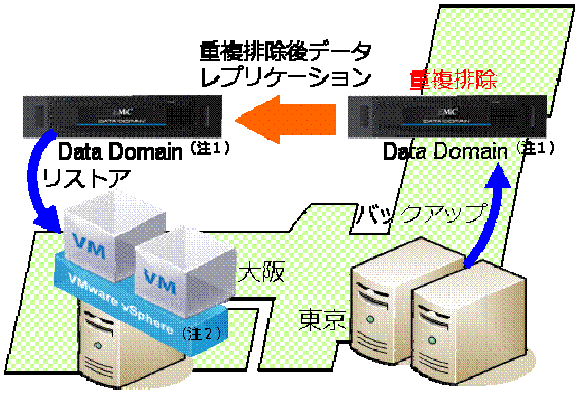


図６．バックアップデータレプリケーション

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。

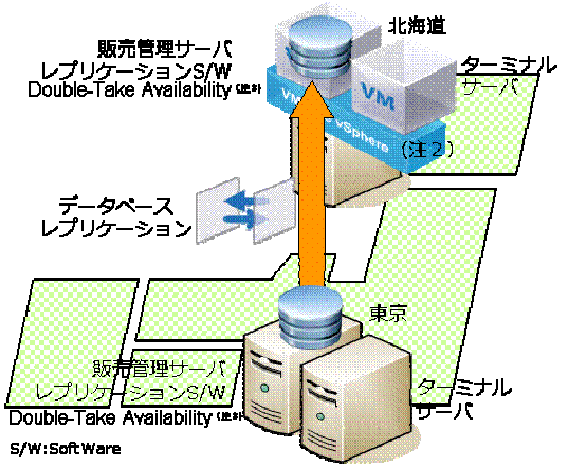


図７．ソフトウェアレプリケーションによる２拠点化

(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