特集論文

イオンモール㈱向けITインフラBCP対策

片谷二郎* 岩崎郁来*
飯塚和貴* 渡辺直之*
加藤美彦*

The Business Continuity Planning in IT Infrastructure for AEONMALL Co.Ltd

Jiro Kataya, Waki Iizuka, Yoshihiko Katou, Ayana Iwasaki, Naoyuki Watanabe

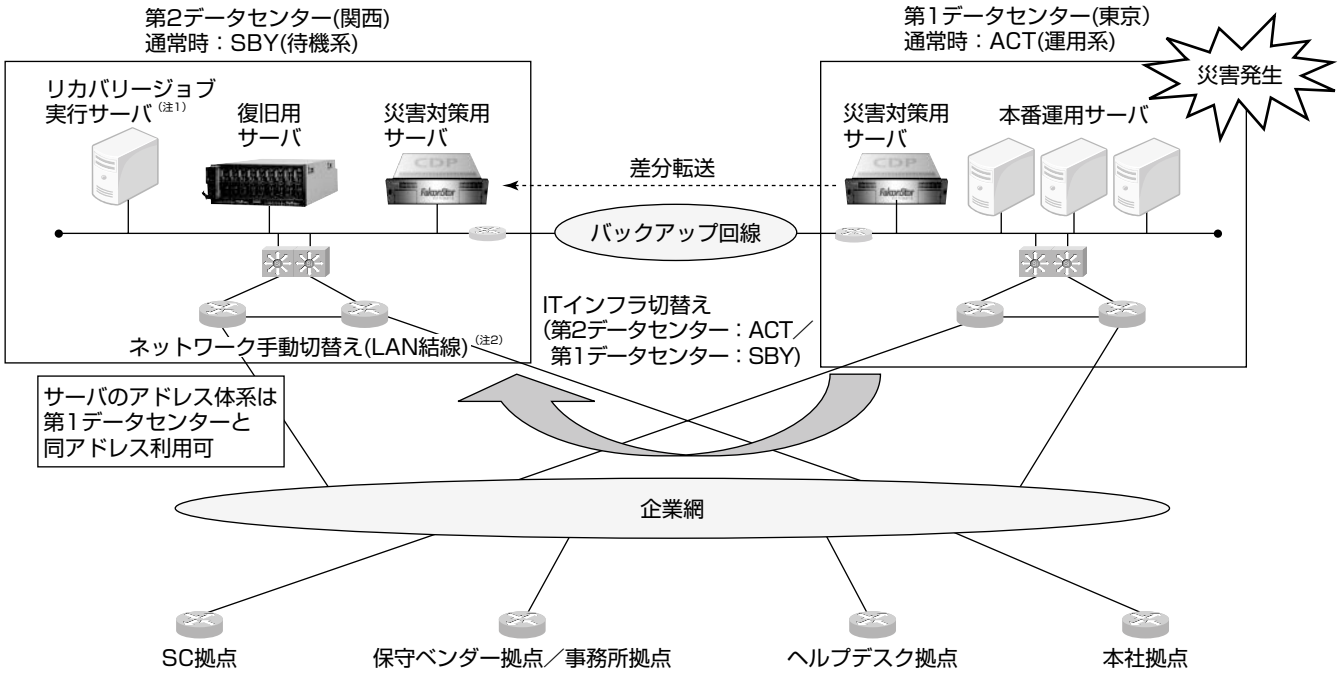
要　旨

東日本大震災以降，各企業で事業継続／災害対策が急務となり，検討・対応が推進されてきている。三菱電機インフォメーションシステムズ㈱(MDIS)の顧客であるイオンモール㈱でも，2011年からBCP(Business Continuity Planning)対策の検討を開始しており，ITインフラ全般にかかわっているMDISが中心となってBCP対策を進めることになった。

都内のデータセンター(以下“第1データセンター”という。)には約60システム(約200サーバ)が集約されており，全国のショッピングセンター(SC)及び関係場所(事務所，保守ベンダー拠点)約90拠点からネットワークを介して業務を行っている。利用規模はパソコン約2,000台，POS(Point Of Sale)端末約15,000台である。

MDISが推進したイオンモール㈱向けITインフラBCP対策プロジェクトでは首都圏直下型地震等の大震災(震度6以上)によって，関東近郊の社会インフラが途絶することで電源供給断などが発生し，第1データセンターが機能しなくなることを前提としている。MDISはITインフラBCP対策として，他社複数ベンダーが構築した45システム(120サーバ)を対象システムとし，これら全てを改修することなく，かつ同じオペレーションで統一的に関西地区のデータセンター(以下“第2データセンター”という。)に復旧する仕組みを構築した。ITインフラBCP対策システムの構築は2012年4月から約1年をかけて完遂し，運用を開始している。

なお，BCP発動後のITインフラの切替えは，第2データセンター内オペレータによって，“ネットワーク切替え(第1データセンター⇒第2データセンター)”と“システム復旧”を手動で実施する運用としている。



(注1)　仮想環境下でリカバリージョブを実行し，システム復旧を行う。
(注2)　災害時に第2データセンター側の専用ルータにLANケーブルを差しこむ(通常時：未結線)ことで，ネットワーク切替えを実現する。
日々の差分転送はバックアップ回線を通し，第2データセンターの災害対策用サーバに格納される。

ITインフラBCP対策システム

通常時は第1データセンターはACT(運用系)，第2データセンターをSBY(待機系)とし，非同期でデータ連携を行う。災害時は第2データセンターでネットワークの切替えとシステム復旧を手動で行うことでITインフラの切替えを行う。

*三菱電機インフォメーションシステムズ㈱

1. まえがき

MDISはイオンモール㈱(以下“顧客”という。)と2005年にITアウトソーシング契約を締結し，IT全般にかかわる業務を担ってきている。主な業務はデータセンター，ネットワーク(WAN，データセンター内LAN，各拠点)，仮想化を含めたITインフラ，端末管理，システム運用・監視，ヘルプデスク，情報システム企画支援，情報システム管理等である。2010年から2011年には，約20社の各システムベンダーが構築した約50システムのサーバ仮想化統合を推進し，現在までに約60台の物理サーバを仮想化(VMware vSphere(注3))環境へ移行し運用している。

2011年の東日本大震災によってBCP対策の機運が顧客内部で高まる中で，顧客全社に先駆けてシステム部で対策を練ることになり，各システムが災害後も継続利用できる方法を検討することになった。そこで，ITアウトソーシング・物理サーバ仮想化を実現し，顧客ITインフラ全般に携わるMDISがBCP対策を進めることになった。

BCP対策に向けての課題は多種多様なシステムに対して，⑴現行システムへの改修を行わず(同一IPなど)統一的な方式を採用すること，⑵個別要件を満たすRPO(Recovery Point Objective：目標復旧時点)とRTO(Recovery Time Objective：目標復旧時間)を達成すること，⑶運用の簡易化及び拡張性のある構成にすることであった。

本稿ではこれらの課題を踏まえて取り組んだITインフラBCP対策システム構築の内容について述べる。

(注3) VMware vSphereは，VMware，Inc. の登録商標である。

2. 要件定義

2.1 改修を伴わない統一的な方式

BCP対策対象システムのほとんどが他ベンダー構築のシステムであった。そのため，第2データセンターに切り替えて運用する際に，サーバのホスト名，IPアドレスなど固有値を変更することの影響範囲を把握することが難しかった。また，サーバのホスト名，IPアドレスを変更することで，システム利用者が通常通りに利用できなくなってしまう。したがって，現行システムへの改修を行わないことが最善であった。

そして，システムごとにBCP対策方式が異なることは運用を煩雑化させるので，統一的な方式で全対象システムに対してBCP対策を実施する必要もあった。これらの要件から，システムに依存しないバックアップが可能で，サーバ固有値を変更することなく第2データセンターで復旧できるBCP対策システムとして，コスト面なども考慮し，FalconStorCDP(注4)を採用した。

(注4) FalconStorCDPは，FalconStor Software，Inc. の登録商標である。

2.2 RPO／RTOの取り決め

RPO／RTOの設定は，顧客が事業継続に必要とするシステムを把握することと，顧客の要望に応えることが可能かどうかを確認する上で重要な数値となる。

設定にあたっては，第3者的視点を持つために，“顧客影響度”“収益影響度”“業務影響度”“データ重要度”の4項目を定義し，システムごとに数値化(1～3)して，その合計値(最大12)から，RPO／RTO数値を取り決めた。その結果から，各システムを6段階のRPO／RTOレベルにグルーピングし，その中でRPO／RTO数値の降順に優先順位を設定した(**図1**)。

2.3 容易な復旧方法と継続的な運用

首都圏直下型地震等の大震災(震度6以上)発生時に，MDISがシステムの復旧操作を実施できない可能性を考慮し，誰でも容易に復旧操作を実施できることが重要である。実際にBCPが発動され，システム復旧を実施する場合，非被災場所である第2データセンターのオペレータが統一した手順に沿って復旧操作を行うことになる。

さらに，BCP対策には終わりはなく継続的運用をするために，バックアップデータを保護するストレージと復旧用のサーバを追加することが容易な構成とした。

3. ITインフラBCP対策設計

3.1 第2データセンター選定

第2データセンター選定もMDISの作業範囲にあり，最初に地震，原子力，水害等の災害リスクの低いエリアから耐震構造，給電方式，自家発電の対応時間等をベースに8つのデータセンターを候補として選定した。その上で，ネットワーク設備のキャリアフリー対応，運用サービス形態等に加え，顧客グループ全体で利用できるキャパシティを考慮するなど，グループ会社全体のBCP対策を考え，最終的に関西地区にあるデータセンターに決定した。

	A	B	C	D	E	F
RPO	1時間前	半日前	2日前	2日前	2日前	指定なし
RTO	1時間	半日	2日	1週間	2週間	2週間～
1	A1システム	B1システム	C1システム	D1システム	E1システム	F1システム
2	A2システム	B2システム	C2システム	D2システム	E2システム	F2システム
3	A3システム	B3システム	C3システム	D3システム	E3システム	F3システム
4	A4システム	B4システム	C4システム	D4システム	E4システム	F4システム
5	－	－	－	D5システム	E5システム	F5システム
6～	－	－	－	D6システム …	E6システム …	F6システム …

(高) 優先順位 (低)

RPO：データを戻す時点，RTO：システム復旧にかかる時間

RPO 災害発生時点 RTO

図1．RPO／RTO一覧

3.2 データ連携方式の検討

⑴ データセンター間データ連携方式

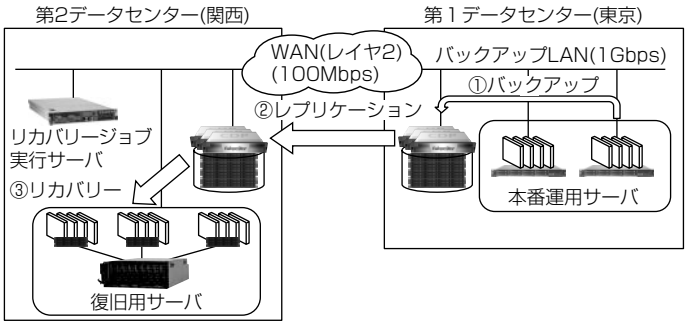
第2データセンターで運用するシステムは，第1データセンター内にバックアップ取得したデータを用いて復旧を行う。データセンター間のデータ連携方式として，①第1データセンター・第2データセンターをACT（運用系）・ACTにした双方向レプリケーションでのリアル同期方式，②第1データセンターはACT，第2データセンターをSBY（待機系）とする非同期の方式，そして③データ部のみを第2データセンターへバックアップする方式を検討した。結果，コスト面，運用，復旧時間等の要件から方式②を顧客のBCPデータ連携方式に決定した（**図2**）。

⑵ アプリケーション非改修及びバックアップ方法

複数システムのBCP対策で，バックアップを行うためにシステムごとにアプリケーションを改修することは膨大なコスト増につながる。そのため今回は，アプリケーションを改修することなく，システムごとに，OSを含むシステム全体をアーカイブとしてバックアップし，レプリケーションする方式を採用した。また，このバックアップデータを用いることでサーバ固有値を変更することなくシステムを復旧させることが可能である。

⑶ システム単位のデータ同期方法

第1データセンターと第2データセンターのデータ連携を非同期としたため，第1データセンターのバックアップ後にレプリケーションが実行されるようにするなど，決められたスケジュールでデータの同期を行える仕組みが重要である。 バックアップ，レプリケーションの回線の負荷を平準化させつつ，帯域内でシステムごとに異なるRPOを満たすデータ同期のスケジュールを設定した。



①バックアップ：システムをOSを含むDISK単位でCDPサーバへバックアップ
②レプリケーション：第1データセンターのCDPサーバから第2データセンターのCDPサーバへバックアップデータを転送する
③リカバリー：復旧用サーバへシステムを復旧させる
CDP：Continuous Data Protection

図2．データ連携方式

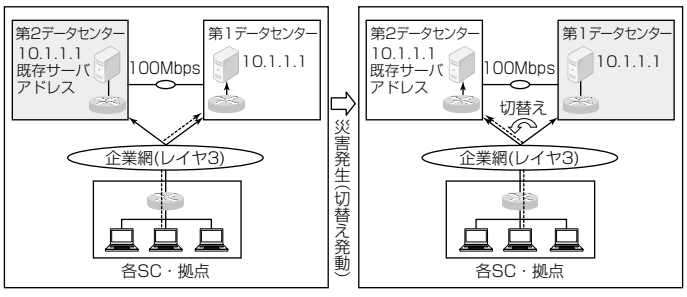


図3．ACT／SBY側によるネットワーク切替え

3.3 ネットワーク設計

⑴ 拠点ネットワーク

当初，第1データセンターと第2データセンターのネットワークアドレス体系は別とし，サーバのIPアドレスを同一とするために，各拠点にNAT（Network Address Translation：IPアドレス変換）用のファイアウォールを導入し，BCP発動時に各拠点でNAT用のファイアウォールに切り替えることで，異なったネットワークアドレス体系を意識することなくサーバへのアクセスを可能とする案で検討を進めていた。しかし，各拠点の作業者への教育やBCP発動時の連絡体制などに対する問題から，別の案を検討することとなった。

検討を重ねた結果，動的ルーティング（Border Gateway Protocol：BGP）を利用できる新ネットワーク網にネットワーク全体を変更し，第1データセンターと第2データセンターのネットワークアドレス体系を同一にすることに決定した。サーバIPアドレスを変更せず，かつ自動でネットワーク全体を切り替えることが可能となったため，第1データセンターが利用不能となった際，全拠点を一斉に第2データセンターに切り替えることができることになった（**図3**）。なお，既存ネットワーク網を新ネットワーク網に変更する作業として約3か月間，全国約90拠点の現場に赴き，夜間帯の工事で動的ルーティングに対応したネットワークへの変更を実施した。

⑵ データセンターネットワーク

第1データセンター内にバックアップLAN（1Gbps）を新設し，新設したLANを通してバックアップを行うことで，既存のネットワークに影響を与えない設計とした。

また，データセンター間にバックアップ回線（100Mbps）を新設し，新設したバックアップ回線を通してレプリケーションを実施する設計とした。

4. 工　夫　点

4.1 バックアップ・レプリケーションのスケジュール

リカバリーに使用するバックアップデータはレプリケーション終了後のデータとなる（**図2**）。そのため，レプリケーションが終了するまで，第2データセンターでは最新のバックアップデータを利用できない。したがって，バックアップ終了からレプリケーション終了までの間に災害が発生した場合，最新のバックアップ時点に復旧することができず，1つ前のバックアップデータが復旧時点となる。そのため，バックアップ及びレプリケーションのスケジュールは，バックアップ開始からレプリケーション終了を

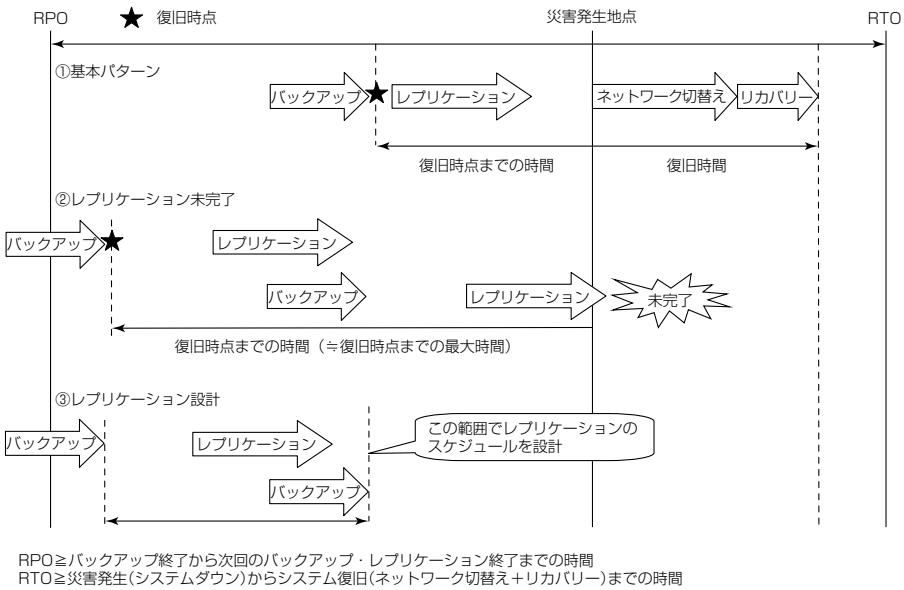


図4．バックアップ・レプリケーション設計

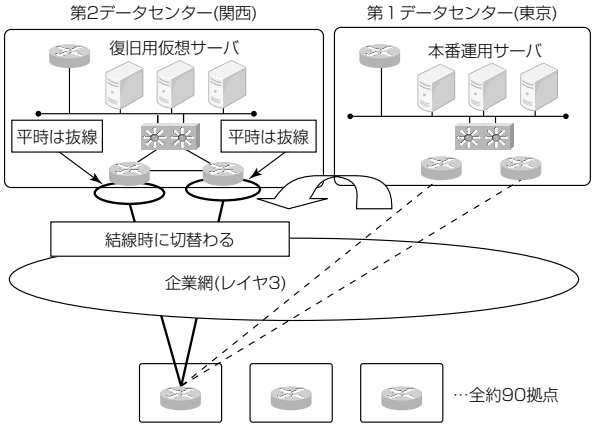


図5．新ネットワーク網によるネットワーク切替え

RPO内に収める設計をするのではなく，バックアップ終了から次回のバックアップを対象とするレプリケーションが終了するまでをRPO内に収める設計が必要である(**図4**②)。

また，レプリケーションは次回バックアップ終了時までに終了すればよいため，レプリケーションを行う回線の負荷分散を考慮したスケジュールを組んだ(**図4**③)。

全システムのスケジュールを1つの表にまとめることで時間帯ごとのレプリケーション数を数値として可視化し，時間帯ごとのレプリケーション数を均等とすることで，レプリケーションを行う回線の1日の負荷を均一とした。

4.2 BCP発動時のネットワーク切替え

当初，新ネットワークは通信の優先順位を第1データセンター＞第2データセンターとし，第1データセンターのネットワークが利用不能となった場合に，自動切替えで第2データセンターがACTになる方式としていた。しかし，この方式には，2つの課題があることが分かった。1つ目は，災害ではない通常障害でも自動で第2データセンターに切り替わってしまうこと，2つ目は，関東近郊の社会インフラが途絶し対象システムが利用できなくなったにも関わらず，第1データセンターのネットワークが落ちなかった場合に，自動切替えが発生しないことである。

そこで，通信の優先順位を第1データセンター＜第2データセンターとし，第2データセンターのネットワークが有効となった場合に，自動切替えで第2データセンターがACTになる方式として，第2データセンターのLANケーブルを通常時は抜いておく運用とした。

これらのことから，ネットワーク網が誤って自動で切り替わることがなく，BCP発動時には，非被災地の第2データセンターのオペレータがLANケーブルを結線するだけで，“ネットワーク切替え(第1データセンター⇒第2データセンター)”を実施できる仕組みを構築した(**図5**)。

5. むすび

BCP対策は費用対効果の観点から，被災によるビジネスに対する影響と，対策を講じるための費用のバランスをとることが重要であり，対象システム範囲とRPO／RTOを定量的に導き出すことが鍵となる。

今回の事例では，提案(2011年)から2年を掛け，顧客とMDISが一体となってITインフラBCP対策システムを構築した。BCPとは本来企業内の各組織が一体化して取り組む施策であり，システムごとのBCP対策では，設計思想のずれやコストのオーバーヘッドが大きくなることが懸念されるが，このプロジェクトでは，長年にわたるITアウトソーシング業務やサーバ仮想化を遂行したノウハウを活用したこと，汎用的なBCPシステムを採用したことによって，個々のシステム要件(RPO／RTO，データ量，仮想化サーバ可否，データベース有無等)を満たした上で，運用の統一，コスト抑制等の“全体最適”を実現することができた。

特に，今回採用したBCPシステムは，ディスク単位でのバックアップやリカバリーが可能なため，一般的なバックアップシステムに代わるものとしても非常に有効である。

MDISは今後もBCP対策機器の追加・変更，運用見直し等による各種マニュアルの改訂や定期訓練等，BCM(Business Continuity Management)の観点で，アウトソーサーの立場として継続的に対応し続ける。また，このプロジェクトを通して得たノウハウや，この事例のバックアップ方式をバックアップ提案例の1つとし，今後とも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。