業務システムへのクラウド・コンピューティング（IaaS）適用の実践的手法

田原 和彦　新栄 俊光　峯田 祐一

Practical method to apply Cloud Computing (IaaS) to Application System

Kazuhiko Tahara, Toshimitsu Shinei and Yuichi Mineta

クラウド・コンピューティングの浸透により，システムのインフラ資源をインターネット経由でサービスとして提供するIaaSが注目を集めている．IaaSは，柔軟で高速な構成変更や従量課金などクラウドならではのメリットがある反面，提供者側で標準化したサービス提供が基本となるため個別のシステム要件や運用の要件に対応することは難しく，標準に準拠することが求められる．筆者ら，IBMが提供するIaaSであるMCCSにオンプレミスのNASとのハイブリッドな環境を付け加えることにより個別のシステム要件に適応したASPシステムを構築した．本論文では標準的なIaaSクラウドの環境を基幹システムの個別運用に適用するための実践的手法を提言する．これにより，クラウドの提供者による標準機能に合致しないシステム要件を持つことのある基幹系システムにおいても，積極的にIaaSクラウドが適用されていくことが期待される．

As the infiltration of Cloud Computing, the Infrastructure as a Service (IaaS) that provides system resources through the network has captured much attention from the market. Although IaaS type of services has some advantages such as flexibility, agility, and “pay as you go “ charging, but there are quite difficult to adopt unique operational requirements on to the IaaS, because the IaaS services are often standardized and fixed. During construction of ASP(Application Service Provider) infrastructure using MCCS which is provided by IBM and customer's on-premises NAS system, we found the way to adopt unique requirements satisfied by building hybrid environment of MCCS with NAS. This paper describes the practical method to apply IaaS to Core Application System. Referring this paper, it is expected to apply IaaS to Core Application Systems with unique requirements.

Key Words & Phrases：クラウド・コンピューティング，IaaS，MCCS，NAS，バックアップ
cloud computing, IaaS, MCCS, network attached storage, backup

1. はじめに

IDCのレポートでは，クラウドは2010年頃からメディアで取り上げられることが多くなり，現在では企業での認知度や理解度は大きく向上していると報告している［1］．クラウドの一形態であるInfrastructure as a Service（IaaS）は，仮想化されたサーバーやストレージといったシステムインフラ資源をネットワーク経由で提供するサービスであり，企業のシステム・インフラ調達の方法として有力な選択肢となっている．IaaSは，企業にとって拡張性，迅速性，柔軟性などのメリットをもたらす一方で，提供者側で標準化されたサービスであるため，個別の運用要件に適応できない可能性がある．特にストレージについては，マルチテナントの共用によるセキュリティーの観点から制約の多い運用となりがちである．そのため，高速コピーなどバックアップ運用に有用なストレージの固有機能が標準メニュー化されていない［2］［3］．

IBMが提供するIaaSであるIBM Managed Cloud Computing Services（MCCS）は，システム・リソースと運用保守を組み合わせたサービスで，高い可用性を持つなど，本番システム稼働を意識したクラウド・サービスである．

筆者らはApplication Service Provider（ASP）であるお客様の本番システムをMCCS上で構築するにあたり，ストレージの個別の運用要件をMCCSの運用制約から切り離し，オンプレミスのNASを並列することで解決した．これによりお客様のデータのバックアップ要件および外部保管要件を満たしつつ，MCCSのシステム資源の柔軟性などのメリットを享受できるシステム構成を実現した．今回直面した課題は，IaaS環境がストレージをマルチテナントで共用していることに起因するため，MCCSに限ったものではなく，IaaSでは一般的な課題であると考えられる．

本論文では，課題解決にあたり考慮した点，工夫した点などを記述し，本番システムのIaaS適用の新たな一手法を示す．

提出日：2011年9月20日　再提出日：2012年6月4日

2. MCCSの特徴

MCCSは，CPU処理能力，メモリー，ディスクを要求に合わせて提供するIBMの従量課金型クラウド・サービスである［4］．MCCSの特徴の中で，本論文で扱う事例でMCCS採用の決め手となった特徴は，主に以下の二点である．

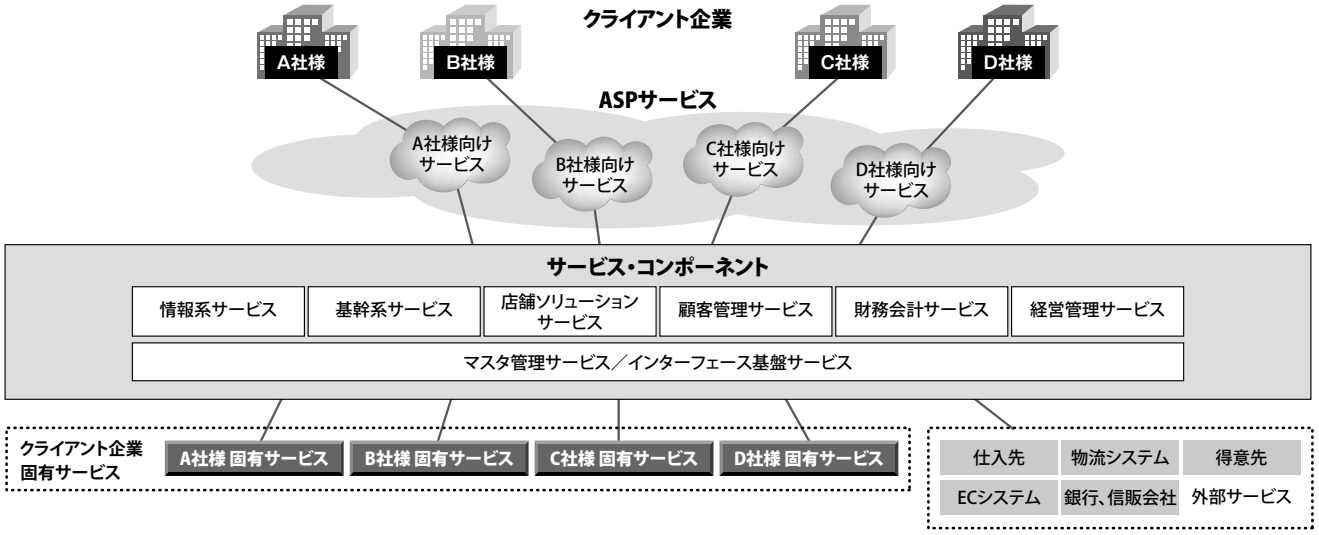


図1. ASPシステム概要

1）本番システム対応の運用と可用性の提供

Amazon EC2 のような単純なリソース提供サービスと大きく異なる点として，MCCS は本番システム稼働を意識したサービスであることが挙げられる． MCCS では Hypervisor（仮想化ソフトウェア）以下の資源にかかわるレイヤーについては，ITIL® に準拠した 24 時間 365 日の運用監視などの運用保守が標準サービスとして提供される.Hypervisorより上のソフトウェアのレイヤーについても，お客様の要件に応じた運用が別途対応可能である．また,ディスクやネットワーク･スイッチなど,サービスを構成する機器は二重化されており，本番システムに耐えうる高可用性を実現したサービスとなっている．

2）柔軟なリソースの課金体系

MCCS が提供する CPU などのキャパシティーは , 月ごとに細かい単位で設定することが可能で月単位の課金となる．このため，必要な時に必要なリソースだけを利用することができ，コストの最適化が実現できる．また MCCS の特徴であるバースト対応により，要求が基準キャパシティーを超えた場合でも，ベスト・エフォートで基準キャパシティーの最大 4 倍のリソースを使用することができ，資源課金の平準化が可能となる．

3. ASPのシステム要件

3.1 システム概要

事例として紹介するシステムは，流通業向けのアプリケーション・サービスを実現するシステムである．MCCS ではお客様のクライアントである企業に対して図 1 で示すように基幹系サービス，情報系サービス，店舗ソリューション・サービスなどをサービス・コンポーネントとして提供するためのシステム・インフラを提供する．

ASP であるお客様はアプリケーションサービスのメニューを用意し，クライアント企業と使用アプリケーション範囲やユーザー数といったキャパシティー条件で個別に契約して月ごとに課金するというビジネス形態をとる．

3.2 MCCS への適合要件

3.2.1 MCCS 適合要件

対象とした ASP システムでは，クライアント企業数やシステム規模を事前に予測することが難しい．システム機器を購入した場合では，事前に大規模な機器を用意すると過大な投資となる可能性があり，逆に小さすぎる機器ではクライアント企業と契約を獲得した時にシステムが用意できずに機会を損失する恐れがある．

その点，前述した MCCS の拡張性と柔軟な従量課金という特性を生かすことができれば，初期投資を最低限に抑えられ，かつクライアント企業の契約獲得時に即座にリソースが用意できる．もちろん課金についても使用分だけで済ませることができるかが重要となる．

また，クライアント企業の基幹業務が稼働するため安定した運用が必要であるが，この点においても本番システム稼働を意識した MCCS の運用保守サービス仕様が合致した．

上記の点はこれまでの ASP 向けのシステムでは実現できなかったメリットであり，お客様の経営層からも重要視されたシステム化の必須要件となっていた．

お客様のシステム要件と MCCS の特徴の対応を図 2 に示す．

3.2.2 MCCS 非適合要件

3.2.1 に記述したクラウド適合要件が必須要件である一方

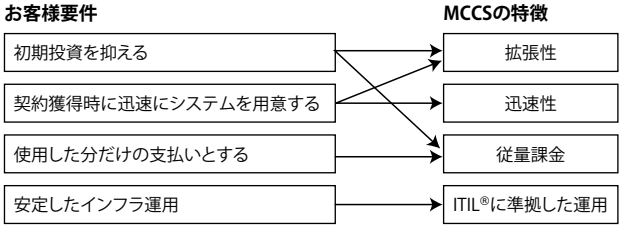


図2. クラウド適合要件

で，MCCS の運用上の制約により以下に示すバックアップおよび外部保管に関する要件は MCCS に非適合であった．

• バックアップ要件

クライアント企業のデータのバックアップを完全に行い，その上で朝のサービス開始時刻を順守する．そのため夜間のバックアップは短時間で終わらせる必要がある．この要件を満たすために，業務の夜間バッチ処理完了直後にデータの静止点を設けて，その間にストレージ・レベルの高速コピー機能によりバックアップを取得する必要がある．しかし，MCCS ではストレージの高速コピー機能は提供されているものの，外部からのジョブ連携による高速コピー機能は実施できないという制約があった．外部からコピー実施はデータの不正取得につながりかねないなどのセキュリティー保護上の配慮による制約である．

• 外部保管要件

アプリケーション・サービスのオプションとしてバックアップ・データの外部保管というメニューが用意されていたため，外部保管サービスが必要だった．しかし，MCCS ではテープ装置など外部メディアへのバックアップ運用は用意されていない．

上記の MCCS の制約により実現できない非適合要件は，データを保持する DB サーバーに関する要件である．DB サーバーのみをクラウド環境ではなく個別サーバーとしてストレージ機器およびテープ装置を配備して個別に構築することで解決することも検討された．しかし，個別のサーバーでは 3.2.1 で記述したシステム要件を満たすことができなくなる．本プロジェクトではすべての CPU 資源は MCCS から提供するものとして，ストレージ資源のみを Network Attached Storage（NAS）形式で個別に構築し，MCCS 適合要件と非適合要件の両立を図った．**表 1** に記載した構成パターンのパターン 3 である．この解決策の実現にあたり発生した考慮点などを次章に記述する．

4. xMCCSと専用ストレージにおける設計

4.1 専用ストレージ設計

xMCCS は MCCS が提供している System x 上に構築された VMware による仮想化システムである．本論文では，xMCCS 上の仮想インスタンスである DB サーバーと個別に構築された NAS ディスク装置を接続する場合の設計ポイントとして以下の 3 点を指摘する．

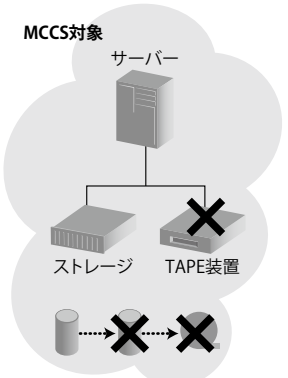
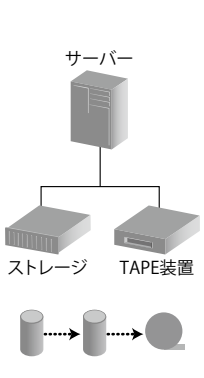
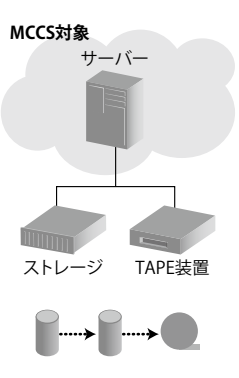
（1）使用するディスク装置の選択

ジョブ連携が必須であるという要件からプロジェクト専用のストレージとして，SAN 接続する DS8000 シリーズ［5］，または NAS 接続する IBM N シリーズを検討対象とした．xMCCS ではストレージ仮想化技術である IBM System Storage SAN ボリューム・コントローラー［6］によるストレージを SAN 経由で提供している．そのため xMCCS サーバーとプロジェクト個別のディスク装置を SAN 接続させることは当時できなかった．そのため，選択肢は NAS に絞られたが，個別にカスタマイズ可能である NAS を採用することで，複雑な運用要件に対応する事が容易になった．また，仮想化サーバーの IO システムと NAS の親和性は高く，IaaS 環境で異なる運用環境をサポートする NAS 型ストレージを組み合わせる優位性は明らかである．

（2）xMCCS サーバーと NAS の接続方式

ジョブ連携したバックアップを行うためには実行環境である DB サーバーまたはバックアップ・サーバーから NAS のコントローラーに対してバックアップ要求を出す必要がある．しかし，3.2.2 で述べた MCCS のセキュリティーの制約により，NAS と xMCCS の管理している VMware の Hypervisor である ESX サーバー［7］とはネットワーク上分離しなくてはならず，直接の接続はできない．**図 3**（左）に示すように一般的に用いられる ESX サーバーから NAS に対して Network File System（NFS）や iSCSI 接続させる方法では，NAS が ESX のネットワーク上に配備され，ネットワーク上分離されてしまうと要件を満たせない．そこで，**図 3**（右）に示すように仮想インスタンスである DB サーバーから直接 NAS のボリュームを NFS もしくは iSCSI によって接続すると，仮想インスタンスと NAS の間にゲストネットワークとして導通が得られ，かつ NAS コントローラーに対する制御も実現できる．NFS もしくは

表1. MCCSおよび個別の構成パターン

	パターン1：すべてMCCS	パターン2：すべて個別	パターン3：サーバーのみMCCS
サーバー・リソースの従量課金	○	×	○
データ・バックアップ要件	×	○	○
構成概要			

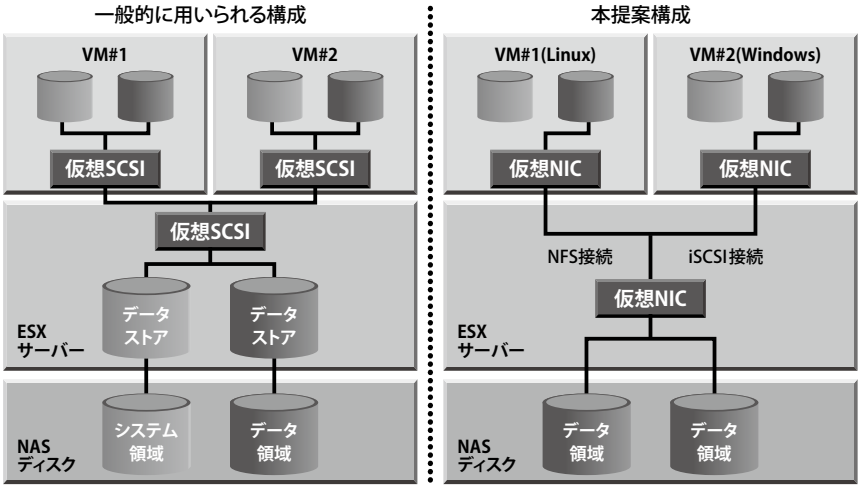


図3. NASの接続方式

表2. バッチ処理に必要なスループット予測値

全データ容量	51,116 GB
目標バッチ処理時間	3時間（10,800秒）
Read I/Oスループット	970 MB/sec
Write I/Oスループット	189 MB/sec

iSCSIの接続については S/W のサポートの観点で,DB サーバーが Linux の場合は NFS 接続とし，Windows サーバーの場合には iSCSI 接続の方式を採用した.

（3）NAS 使用時のパフォーマンス

MCCS 上に構築される DB サーバーのパフォーマンス要件を満足するために考慮した 3 つの点を以下に示す.

a）最大スループットに対する帯域の確保

NAS にはネットワーク経由のアクセスとなるため，最大スループットがどの程度あるかを要件定義時点で得られている全クライアント企業の DB サイズの情報を基に算出した．特に負荷の高いと考えられるバッチ処理の処理時間目標に対して，どれだけの I/O スループットが必要となるかを重要視した．ここではバッファー・プールなどの予測値を前提においた上で表 2 のように I/O スループットを予測した.

これによると 10Gbps（1Gpbs のポート 10 個分）が確保できれば Read と Write の処理が同時に発生した場合でもネットワーク帯域としてパフォーマンスの影響が出ない．本システムで想定される仮想 OS 数は 135 ノードとかなりの数であったため，他システムと共有することなく，xMCCS のサーバー数台を占有して使用でき，ネットワーク・インターフェースも十分な数占有できることが確定していた．このことから，上記スループットを物理的に担保できることが確認できた．他方で要求される仮想サーバーの数が少なく，かつ I/O スループットが大きいなど，本論文で扱ったケースとは異なる I/O のボリューム・バランスになるシステムにおいては，ネットワーク・インターフェースの確保が課題となる場合もあるため注意が必要である.

b）DB サーバーの物理配置

物理サーバーと NAS の間のネットワーク帯域を増やすためにはサーバーおよび NAS のネットワーク接続を複数ポートでチーミングする．一方で仮想 OS はその複数のポートのうち 1 つを利用するために,負荷バランスを整える必要がある．つまり，xMCCS サーバー上の仮想 DB サーバーの物理配置を負荷バランスの観点で実施することになる．1 社のクライアント企業が全サブシステムを利用すると 8 台の DB サーバーが必要になる，これらを負荷が高いものからソートして負荷バランスのよい組み合わせを考え物理サーバー上の配置を計画した．この組み合わせを配置ルールとして定義することで，リソースの自動分散配置機能などの働きにより他の組み合わせとなっている仮想 DB サーバーが，同一の物理

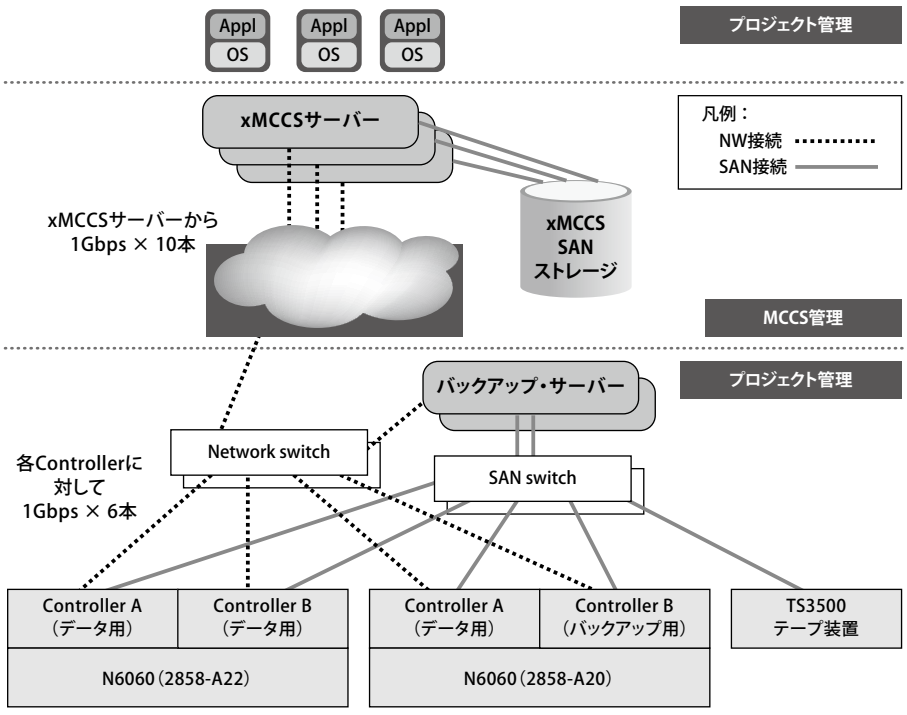


図4. ネットワーク接続構成

サーバーに配置されないようにすることで，クライアント企業が増加しても I/O パフォーマンスのバランスが崩れないように配慮した．

c）NAS のネットワーク接続の負荷バランス

xMCCS 側の仮想 DB サーバーの負荷バランスだけではなく，ネットワーク接続されている NAS 側においても同様にネットワークの負荷バランスを考慮した構成を作成する必要がある．NAS は NAS コントローラー 1 台当たり 6 つの 1Gbps イーサーネット・ポートで動的マルチモードの Virtual Interface（VIF）と呼ばれるチーミングを行い，ネットワーク・インターフェースを束ねて利用できるように構成した．ネットワークのトラフィックは二種類あり，サーバーからの I/O のトラフィックと SnapMirror 等で使用するバックアップ用の帯域である．パフォーマンスを維持するために，これらのトラフィックを VLAN によって分割せずに 1 つのセグメントとして混流させる．これは個別にトラフィックを制御して制限を持たせるよりも全体の利用可能な帯域幅を増やし，ネットワークの利用効率を高めることが狙いであった．一方で束ねられた 6 本のイーサネット・ポートのうち特定のポートのみ負荷が高くなることを避ける必要がある．VIF のロード・バランスを IP ベースとして DB サーバーの IP アドレスによりトラフィックが分散するように設定し，SnapMirror のトラフィックはマルチパス SnapMirror 機能を使うことですべてのポートにバランスよくトラフィックが流れるように構成した．運用面では夜間に終了すべき SnapMirror が朝のサービス開始時点までに完了しない場合には SnapMirror が使用する帯域を動的に絞り，オンラインのパフォーマンスを優先するなどの運用設計も行った．図 4 に実装したネットワーク接続構成図を示す

4.2 バックアップ・リストア設計

4.2.1 バックアップ設計

3.2.2 で MCCS では実現できないバックアップ要件の時間的制約を述べているが，NAS に実装する DB サーバーのバックアップ・リストア要件は**表 3** の通りである．

バックアップ設計では，7 世代という世代保管の保管場所が課題となった．4.1 で検討した SAN 接続の DS8000 ではディスク･コピー先に同じ容量を確保する FlashCopy によるバックアップ方法が現在も主流である．この場合，Disk-Disk-Tape（D2D2T）のバックアップを実施し，テープ装置上にあるテープに 7 世代を保管し，バックアップ･ソフトウェアによって管理する．

しかし，本システムではバックアップ容量が大きく，日次でテープ・バックアップを行うにはテープ装置のドライブ数が 35 ドライブも必要となり，また大量の保管用テープも必要となり，コストを圧迫してしまう．このような SAN 構成に対して，N シリーズを用いた NAS 構成では Snapshot でリポジトリー情報を管理することで複数世代を同一ボリューム上に保管でき，さらにボリューム単位の SnapMirror により Snapshot も含めたディスク･コピーができる．その機能を利用して 7 世代のバックアップをテープ装置上に保管するのではなくオンラインのディスク上に保管する設計とした．7 世代のバックアップ要件はディスク上で実装したが，テープが一世代のみでは緊急時に不安がある．そのためテープ装置へのバックアップ［8］は，週次で 3 世代保管することにしたが，全体としてはリポジトリー保管によるスペース削減やテープ･ドライブの削減などでコスト削減につなげることができた．

外部保管時の暗号化については当初，すべての DB データのテープ・バックアップを暗号化することを検討した．テー

表3.バックアップ･リストア要件

バックアップ要件	
1. オンライン／オフライン	オフライン
2. 差分／増分／フル	フル･バックアップ
3. 取得頻度	日次
4. バックアップ対象	DB全体
5. 世代･日数管理	7世代
6. 取得要件	･バッチ前後に短時間（30分程度）で取得 ･バッチ後をテープに取得
7. 外部保管有無	現時点ではないがオプションとして用意する
8. 外部保管時の暗号化	個人情報が含まれるため必要
リストア要件	
9. Recovery Time Objective（RTO）	最大24時間以内
10. Recovery Point Objective（RPO）	24時間以内
11. その他	バッチ処理の失敗時にリカバリーから再実行が可能

表4. テープ･バックアップの暗号化

バックアップ方法	NDMP バックアップ（Fiber 経由）	TSM バックアップ（一部 NW 経由）	併用バックアップ（Fiber と一部 NW の併用）
1. 暗号化方法	ライブラリーで暗号化を設定する LME を使用	TSM のデバイス・クラスで暗号化を設定する AME を使用	TSM のデバイス・クラスで暗号化を設定する AME を使用
2. 鍵管理	TKLM サーバー	TSMDB	TSMDB
3. 暗号化対象	すべてのバックアップが対象	すべてのバックアップが対象	必要な DB のみ
4. バックアップ／リストア時間	20 時間	167 時間	35 時間
5. リストア方法	直接ソース・ボリュームにリストア可能	TSM にソース・ボリュームをマウントする必要あり	TSM にソース・ボリュームをマウントする必要あり
6. 必要な HW/SW	TKLM 用サーバー危機と TKLM のライセンスが必要	NAS の FlexClone ライセンスが必要	なし

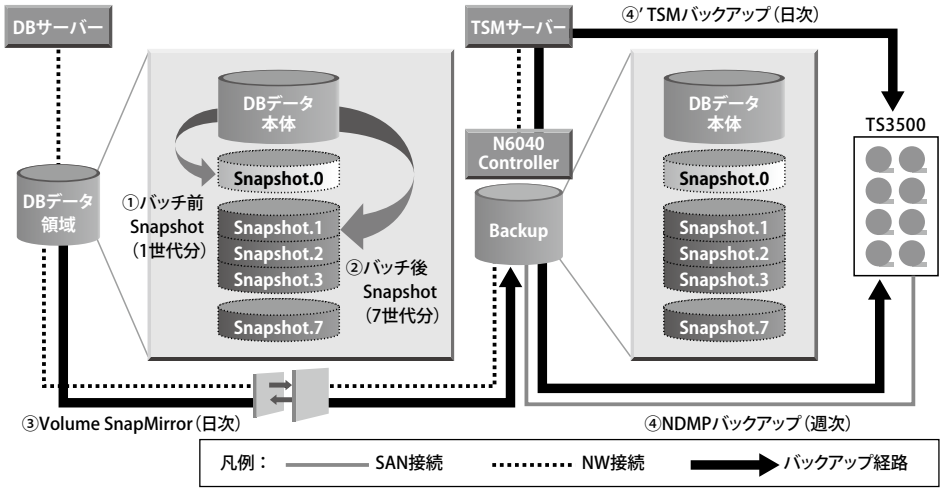


図5. バックアップ方式

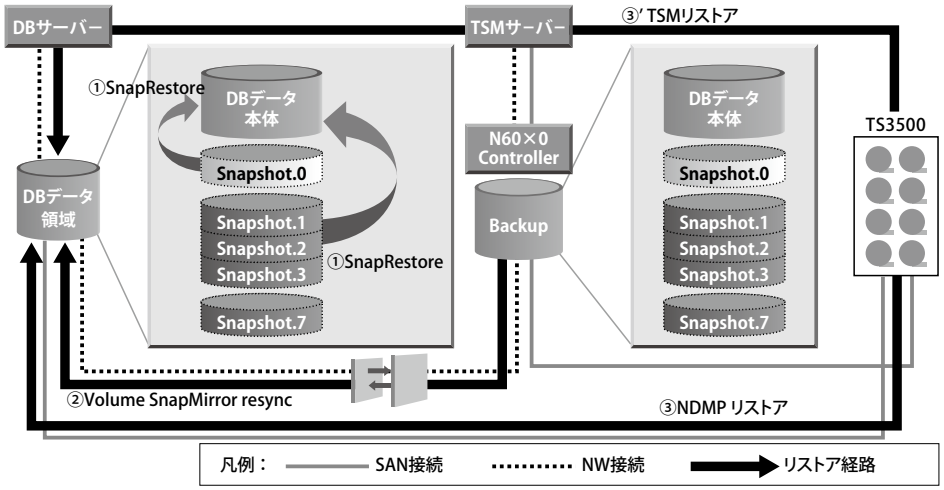


図6. リストア方式

プの暗号化方法により，表 4 のような考慮点がある［9］.

暗号化要件が個人情報を含む情報のみであることから，個人情報を含むデータのみを選択して暗号化対象とすることで，暗号化の不要なものは Network Data Management Protocol（NDMP）によるバックアップを用い，暗号化の必要なものは Tivoli Storage Manager（TSM）バックアップを併用することで短時間にバックアップおよびリストアが実現可能なバックアップ方法を実現した.

4.2.2 バックアップ・リストア方式

本システムで採用したバックアップ・フローは図 5 のような手順となった.

① バッチ前の Snapshot（1 世代保管）
② バッチ後の Snapshot（7 世代保管）
③ 別筐体の NAS に Volume SnapMirror を取得
④ テープへの NDMP バックアップ

暗号化ありの場合，図 5 のバックアップの④が TSM 経由でのバックアップ（④'）へと変更する．本システムにおいて暗号化が必要な DB サーバーは Linux であったため，TSM 経由でバックアップを行う際にはバックアップサーバーから SnapMirror 先のボリュームを NFS マウントして，テープに取得した．もしも DB サーバーが Windows サーバーであった場合には，NAS との接続が iSCSI 接続の Logical Unit Number（LUN）という構成をとらなくてはならない．その場合，SnapMirror 先をバックアップサーバーにマウントするには FlexClone という機能を使う必要があり，オプションのライセンスが必要となることは注意が必要である.

なお，TSM 経由でバックアップする場合は NDMP と異なり，Snapshot 含めたボリューム全体の取得ができないため，個人情報を含む暗号化対象のデータについてはバックアップ容量を勘案した上で，全体のバックアップリストア計画方針から除外して日次で 7 世代テープに保管する設計とした.

リストアは，図 6 に示すような 3 つの方式となった.

① バッチ前後の Snapshot からの SnapRestore
② SnapMirror の逆同期による Resync
③ ソース・ボリュームへの NDMP リストア

暗号化対象データの場合，図 6 におけるリストア手順の③が TSM 経由のリストア（③'）に変更する．バックアップ・サーバーにソース・ボリュームを NFS マウントすることで直接ソース・ボリュームにリストアできるような設計とした.

5. おわりに

これまでは DB のデータ管理のバックアップやバッチ再起動などの運用要件を考慮すると標準運用しかサポートされないクラウドの IaaS 適用は困難と考えられがちであった．本論では IaaS クラウド上の業務アプリケーション・システム実装課題をオンプレミスで設置した Network 経由の NAS の運用を個別カスタマイズする，すなわちデータ管理の個別運用要件をオンプレミスの NAS 側で吸収するという現実的で実

装可能な手法を導いた.

基幹業務の運用要件は，データ管理やバッチ処理実行にかかわるものが多く，その多くはストレージの運用によって実現可能であるというのが本論における発見である．この発見に基づいて標準化されたクラウド環境と自由に運用要件が決定できるオンプレミスの環境をハイブリッドに構成することで，基幹業務における運用を実現できるという結果を導いた．パフォーマンス，バックアップ・リストアにかかわる要件，そして暗号化などの特殊なデータ管理要件に関して考察することで，実現可能でかつ堅ろうなデータ管理運用の仕組みを構築することができた.

ただし，残った課題も存在している．本論においてはDBサーバーのスループット確保に必要なネットワーク帯域はサーバーのノード数が多い事で解決された．しかし，クラウドの占有ノードが少ない場合には帯域不足に陥りやすい．これはNASを使用する場合に一般的に発生する課題であり，今後IaaSにおいて10GbpsイーサネットやInfinibandなどといった多様な高速ネットワークによるデータセンター・ファブリックが使用できる構成であることが望まれる.

今後，本論文で適用したような，データ管理の運用をメニュー化し，従量課金とすることで，クラウド環境と個別環境両者のメリットを生かせるサービスの提供が可能となることに期待したい.

本論が基幹業務にIaaSクラウド環境を適用することに躊躇(ちゅうちょ)されている企業にとって検討を開始される弾みとなることを望むとともに，今後もさらに基幹業務システムのIaaSクラウド適用で課題が想定される，運用・性能品質要件課題に取り組む必要があると考えている.

謝辞

MCCS構成検討にあたり，MCCS Lead Architectの沢橋 松王氏には大変貴重なご助言をいただきました．また，本論文の執筆にあたり，プロジェクト・メンバーにも数多くの助言をいただきました．改めて深謝いたします.

参考文献

［1］ IDC Japan: “国内クラウド市場ユーザー動向調査結果を発表 ,” http://www.idcjapan.co.jp/Press/Current/20110726Apr.html（2011.7.26）.

［2］ 情報処理推進機構 : “中小企業のためのクラウドサービス安全利用の手引き ,” http://www.ipa.go.jp/security/cloud/documents/cloud_tebiki_V1.pdf

［3］ 経済産業省 : “クラウドサービス利用にかかわるリスク ,” http://www.meti.go.jp/press/2011/04/20110401001/20110401001-7.pdf

［4］ IBM Japan : “IBM マネージド･クラウド･コンピューティング･サービス ,” http://www.ibm.com/services/jp/ja/it-services/jp-of-so-managed-cloud-computing-services.html

［5］ Bertrand Dufrasne et al., “IBM System Storage DS8000: Architecture and Implementation,” IBM Redbooks Form No. SG24-8886-01（2011）.

［6］ Jon Tate et al., “Implementing the IBM System Storage SAN Volume Controller V6.3,” IBM Redbooks Form No. SG24-7933-01（2012）.

［7］ VMware, Inc. : “VMware ESXi および VMware ESX の Info Center,” http://www.vmware.com/jp/products/datacenter-virtualization/vsphere/esxi-and-esx/overview.html

［8］ Alex Osuna et al., “Using the IBM System Storage N series with IBM Tivoli Storage Manager,” IBM Redbooks Form No. SG24-7243-01（2010）.

［9］ Alex Osuna et al., “IBM System Storage Open Systems Tape Encryption Solutions,” IBM Redbooks Form No. SG24-7907-00（2010）.

日本アイ・ビー・エム株式会社
テクニカル・リーダーシップ
エンタープライズ・クライアントIT推進
アドバイザリー・IT スペシャリスト

田原 和彦 Kazuhiko Tahara

［プロフィール］
2001年，日本IBM入社．電機のお客様の担当SEとしてお客様の生産管理システムや社内基幹システムの主にインフラ基盤の設計・構築に従事．2011年より流通のお客様の担当SEとして小売のお客様を担当.
ktahara@jp.ibm.com

日本アイ・ビー・エム株式会社
テクニカル・リーダーシップ
製造クライアントIT推進
アドバイザリー・アーキテクト

新栄 俊光 Toshimitsu Shinei

［プロフィール］
1990年，日本IBM入社．自動車メーカーのお客様の研究・設計・開発・販売・サービス業務を支援するIT提案・構築を担当．近年は，電機・電子メーカーのお客様を担当.
E24272@jp.ibm.com

日本アイ・ビー・エム株式会社
インダストリアル・サービス
エレクトロニクス・システム部
アドバイザリー・IT スペシャリスト

峯田 祐一 Yuichi Mineta

［プロフィール］
2003年，日本IBM入社．電機のお客様の担当SEとして生産管理システムや基幹システムのインフラ基盤の設計や構築に従事．近年は，災害対策やクラウド案件における提案活動や基盤設計・構築を担当.
mineta@jp.ibm.com