特集

クラウドコンピューティング時代の大規模運用技術

～次世代ネットワーク機器管理プロトコル NETCONFとその応用～

編集にあたって

黒崎芳行
アラクサラネットワークス(株)

新　麗
(株) IIJ イノベーションインスティテュート

概況

コンピュータやネットワーク（以下 ICT（Information & Communication Technology）基盤）は，各種の産業ライフサイクル（販売，生産，物流，研究，開発，等）にエコシステムとして取り入れられているため，ICT 基盤の停止は，単に一部の障害ということだけでなく，関連する企業や個人，社会システムに対しても大きな影響を与える状況にあり，ある意味，私どもの生活にとって，水や空気，電気，ガス，等と同様に必要不可欠なインフラになってきている．

今後ますます ICT 基盤を利用したサービスの利用が普及，促進するにつれて，そのリスクを踏まえての対応というものがますます重要となってきている．

ICT 基盤を利用したシステムは大きく分ければ，アプリケーションを処理するサーバシステム，アプリケーシ

ョンやアプリケーション実行のためのデータを格納するストレージシステム，アプリケーションの実行を要求するクライアントと，サーバシステムをシームレスに接続するネットワークから構成されており，その中でも，昨今の SaaS，クラウド，等として言われている，各種の物理リソースを仮想化技術を利用して，効率的に活用する ICT の利用形態において，複数の拠点間を接続するルータやスイッチなどのネットワーク機器は，情報システムの発達とともにますます重要な役割を果たすようになっている．

特に，「いつでも，どこでも，だれとでも」に表されるように，高速，高帯域のネットワークインフラが整備されることで，アプリケーションもさらに提供するサービスが高度化することとなり，直感的で分かりやすい画面を持ったアプリケーションが登場し，ユーザにとっての利便性は向上することになる反面，対象リソースの大規模化（数，容量），障害対策の複雑化（関連する機器の増加による対応能力の限界，機能の高機能化によるオペレータの対処能力の限界，等）による運用操作への課題の増大といった問題が顕在化してきている．

ICT システムは，メインフレームの時代から，ダウンサイジング，Web コンピューティングと，時代時代に応じた変遷をしてきており，今回の「クラウド」もその変遷の一環であるが，変遷の 1 つとして確立されるためには，単にコストメリットがあるというだけでなく，利便性や安全性等においても，従来技術を凌駕するにいたらなければ，単なるファッションで終わってしまうことになる．

ここでは，やや乱暴かもしれないが，「クラウド」を「サーバからクライアントまでのプラットフォーム仮想化技術」として捉え，コスト，利便性，安全性，についての現状と課題，および将来の可能性について，考えてみたい．

クラウド環境の変遷

クラウド環境は，膨大な数のサーバが占める物理的な面積を削減したいという動機と，飛躍的に向上してきた CPU パワーの有効活用として，サーバの仮想化というかたちから発展してきた．

クラウドをその技術的構成から考えると，3 段階に分けることができる．現在のクラウド環境は第 2 段階の機能の充足を図っている状況といえるだろう．一部では第 3 段階に差しかかっている状況にある．

(1) 初期のクラウド（～ 2007 年頃）

物理サーバ上に複数の論理サーバを立ち上げた VM（Virtual Machine）サーバ集約型クラウド．ネットワークも単一なフラットなもの．

VM の移動などの高度な利便性の提供はなし．

(2) 利便性の向上したクラウド（現在）

論理サーバをクラウド上の任意の場所へ移動することが可能となり，高可用なサーバ利用環境が実現する．

この機能の実現にはサーバ側だけではユニークな場所への移動はできないが，VLAN を利用することでネットワーク面での連携を実現することが可能であり，VLAN のいくつかの活用（DynamicVlan，MacVlan，認証 VLAN 等）により，位置透過性の実現の目処がたってきた状況．

(3) End-End でのクラウド（今後）

VLAN（＝論理サーバ収容）をさらに上位概念であるユーザ収容に向けた仮想ネットワーク技術，End-End にわたった仮想環境を高いセキュリティを保ったかたちで提供する仮想通信路の提供，等サーバ，ストレージ，ネットワーク（イントラ，エクストラ）にわたったコンピューティング環境を仮想化技術を使って提供されることが期待される時期．

仮想化することでの課題

次に，よく知られたことではあるかもしれないが，仮想化をしたことでの失敗事例を挙げ，そこから課題を抽出してみたい．

(1) 利便性に潜むセキュリティ問題

VM 化する目的の 1 つに，障害対応が挙げられる．

VM 化により論理的なサーバは，どこででも動けることができるようになっており，また簡単に動作する場所を引っ越せる技術（ライブモーション等）も実現されており，サーバ環境にとってもはや「場所」は問題ではなくっている．しかし，移動した先のセンタのネットワーク環境が異なっていると，移動した先のサーバはインターネットからのアタックをまともに受けてしまい，動作不能になることがある．元のセンタでは，ネットワークからアプリケーションまでの FW（FireWall）が完備し，各種のプロトコルを使ったアタックやウィルスに対する UTM（Unified Threat Management）があり……という環境を前提にしているサーバが手違いで，ネットワークレベル（例：レイヤ 3 のアクセスリストくらい，など）の FW しかないサイトに移動してしまったとすると，これは最悪な事態を招いてしまう．

(2) 仮想化によってサーバが増えてしまう問題

通常サーバは，機能単位に立てられ，DB ファーム，Web フロントファーム，AP ファームなどサーバリソースを共同利用する前提で構築をするのであるが，一部の企業や自治体等では「予算」ベースでサーバを立てること

がある．つまり，予算化された単位でサーバが乱立することがある．

昨今さすがに，物理的なサーバを立てるのは効率面で排除される傾向にはあるが，仮想化により簡単に論理サーバを構築できることになると，一見アプリケーション（ソフトウェア）の予算だけを取っているようで，その実態は前提のサーバ（VM）を含めて構築をすることになるので，気がつくとサーバが乱立することになる．物理サーバの構築は，忘れた頃に「物理リソースの圧迫」を理由に増設することになるので，気がつくと管理するサーバの数が予想外に増え，コスト（ソフトライセンス費）増，運用負荷増，DB 項目の発散（ローカル DB 化による項目の発散）等を招くことになり，隠れ費用の増大につながってしまう．

(3)ネットワークの隠れ島問題

ハイパーバイザー機能が高度化し，論理サーバ間の通信路の制御を行う仮想スイッチ機能が高度化してくると，従来のネットワーク管理の手法では管理できない「隠れ島」ができてしまう可能性がある．論理サーバ間の通信を仮想スイッチや，NIC（ネットワークインタフェースカード）内の制御機構が独自の転送機能を働かせてしまうと，従来のネットワーク管理システムが使っている監視手法（SNMP，Syslog，netconf，ospf/bgp のプロトコル解析，etc）では検知ができない事態となる（仮想スイッチ同士が独自の手法で転送，管理，制御を行ってしまったり，同一物理サーバ内の論際サーバの転送をハイパーバイザーが行ってしまい，外部のネットワークには情報が渡らないことがあるため）．

一番怖いのは，「管理のできない隠れ島ができていることを知らずにいること」で，アプリケーション的には障害を検知できても（クライアント側のエラーで発覚，など），実態として，どこに問題があるのかを追求できなくなる事態を招いてしまう．

クラウドを「ICT の変遷の歴史」に残していくためには

冒頭でも述べたが，クラウド（クラウド技術）を ICT 変遷の歴史上の 1 ページに残していくためには，既存技術を凌駕し，利便性や安全性もきちんと担保され，適切なコストで利用できることが必要である．

そのための方向性を少し考えてみた．

(1)新しいプロトコルや標準へのチャレンジ

2009 年初頭に Cisco 社が UCS（Unified Computing System）を発表し，オールインワン型の新しいコンセプトを発表した．

この中には，配線系のオールイーサネット化，ハイパーバイザーと連携した動的ネットワーキングの実現，等，IEEE802.1 標準[☆1] で議論されている技術が取り込まれている．

この製品が成功するかどうかは未知数であるが，時代の変遷期には従来技術を踏襲するとしても，新しい効率的な技術にチャレンジをすることが必要であり，今後もそういった技術を踏まえて成長をしてゆく必要がある．

(2)仮想化されたクライアント

家庭の中の 1 台の PC に家族全員の環境があったとしたら？

料理の献立を考えるお母さん，学校の宿題やネットサーフィンして楽しんでいる子供たち，町内会の行事のアレンジをしているお爺さん，……それぞれの個人環境はきちんと守られていないと安心してクライアントを使うことはできない（ネットサーフィンしているお兄さんの画面をお母さんが覗けたりしたら……ちょっと困る）．

家庭の中のクライアント環境がクラウド化されたことを考えると，暗号化された VLAN や VPN，クライアント OS の認証強化やアクセス制御の強化，などが考えられる．

(3)適材適所のリソース割り当て

一般的になるが，インターネットで世界の津々浦々まで接続可能なリッチな環境は必ずしも必要ない（極論をいうと，ネットバンキングするときは，銀行にだけつながってくれればよい）にもかかわらずネットワークリソースの設計はどこでもつながる事態を想定した上で用意されている．

また，ネットワークを利用するということは多種多様なセキュリティ問題と向かいあう必要性が出てくる．特に家庭環境においては，そういったことを個々に実施することは現実的ではない．

そうなると，適材適所のリソース割り当てを行うネットワークの機能や，アウトソーシングの活用をシームレスに行える技術，用途に応じた回線の選択（ネットバンキングは NGN，ネットサーフィンはインターネット等）等，選択可能で，かつ容易に利用できるサービスの活用が必要になってくると考える．

まだまだクラウドは「活用」途上（発展ではなく，まずは活用をして発展するとして）にある技術であり，いろいろな応用が出てくるものと考えられ，そのときにはあ

☆1 IEEE802.1 で標準化されている技術
DCB：Data Center Bridging（イーサネットの上に LAN 系，ストレージ系の接続を集約する）
EVB：Edge Vitulaize Bridging（サーバの仮想化と連携したネットワーク（主に VLAN）の仮想化連携対応）

らたな技術的な壁も出てくるものと想像する．

ネットワークの自動運用に向けて

こういったクラウド環境が普及するには，何よりも「自動化」がどこまで実現できるのか？が課題となる．

従来，ネットワーク機器は熟練した技術者が管理操作することを前提としてきたが，このような ICT 基盤活用の広がりに対応するためには，人的な対応によらずに自動化が容易に行える機能（インタフェース）を具備し，サーバ，ストレージ，ネットワーク，さらにはアプリケーションとの連携を可能とすることで，有機的な管理が行える，管理技術がその時代時代に対応したかたちで求められている．

1990 年頃から TCP/IP による通信のオープン化，Web（HTML）技術による異機種環境での接続の容易性（特にアプリケーションの接続容易性，部品利用化，等）が進行すると，サーバやストレージを中心に XML を利用した管理基盤の整備がされてきた．サーバ系では，DMTF や OASIS が，ストレージでは SNIA が中心となり異機種連携のデータモデルやプロトコルの相互接続実験が行われシステム相互接続の検証が行われてきた．この間，ネットワークは，拡大するトラフィックと網の整備に着目し，ネットワーク自身の耐障害性の向上を充実してきた（機器自身のフォールトトレラント機能やネットワークプロトコルとしての冗長化対応（Link Aggregation や Gracefull Restart 等））．反面，規模の拡大に対する対応として，サーバやストレージのような自動化を目指した対応については出遅れの感があった．

このような背景から，2002 年頃から IETF の場でネットワーク管理の新しい標準として，NETCONF の議論が開始され，2006 年にプロトコルが，2008 年には一部であるがデータモデルが RFC として制定された．

現在はベンダごとに操作方法が異なるが，XML を利用することで手順を共通化することを目的にしており，遠隔からの操作も可能となるため，サーバやアプリケーションと連携して動作することも可能となるに至っている．

本特集では，NETCONF の概要とその目指すもの，さらに現在取り組まれている応用技術について紹介する．

1 編，2 編では，NETCONF の技術の現状について標準化と実際の製品適用について取り上げる．「NETCONF の標準化状況（東村）」では，IETF における NETCONF の標準化の状況と日本からの貢献について紹介するとともに，2009/10 に標準採択された rfc5831（データモデルの実装）について解説する．「NETCONF 製品化と API/SDK（木村）」では世界初の NETCONF 対応製品の開発と，それを利用するために提供した API の構想および内容について解説する．

3 編，4 編では実際に NETCONF（および NETCONF を利用するための API）を利用した実証システムについて取り上げる．「ダイナミックネットワーク制御技術（千装）」では，NETCONF 対応製品を利用し，ネットワーク機能を切り替えることで柔軟にサービスを提供できるシステムの一例を紹介する．VLAN 技術を応用することで，通信先（通信範囲）の切り替えが行えるのであるが，これを動的に変更することにより，従来では複数台必要であった装置を複数のユーザでシェア（通信内容は VLAN で分離）したり，あるいは特定のユーザには FW などを使わないで直接接続をしたり（それによってセキュリティ脅威にさらされる環境での研究を行う）といったことをアプリケーションから制御することで柔軟なネットワークシステムを構築することが可能となる．「ネットワークシステム運用管理への応用（新）」では，データセンタのような非常に多数のサーバが接続された環境におけるサーバの割り当てに対応したネットワークの開通制御について解説する．データセンタには多数のサーバがあり，それを利用するユーザも長期間利用するユーザからスポット的に短期間で利用をやめるユーザまでいろいろであり，もともと共通リソースでもあるネットワークを停止することなく，また誤設定なく設定を行うには，サーバの割り当てと連携したネットワークの開通制御を自動化することで，迅速かつ正確な設定が可能となる．

NETCONF によるネットワーク制御は，それ自身がネットワークの新しい進化ではあるが，新しいコンピューティング環境である SaaS，クラウド，等の仮想化環境を統合して利用することにつながる技術であり，今後も IETF や OASIS 等の場で議論が進んでいくものと考える．本特集が ICT 運用関連に従事し，次世代の運用・管理技術を検討されている諸氏の参考になることにつながれば，幸いである．

（平成 21 年 10 月 14 日）