

データセンターにおける SDN の利用

SDN Use Case in the Datacenter

金田克己

Abstract

クラウドコンピューティングサービスの発展に伴い、データセンターにはこれまで以上にコンピュータリソースが集約されてきている。これら集約したコンピュータリソースを分割して様々なユーザに提供することでリソース全体の利用率を向上させるというのがクラウドコンピューティングの持つ一つの特長である。このとき、リソースをできるだけ細かく分割し、迅速にユーザに割り当てる必要がある。このようなデータセンターの要求に対して、昨今のネットワークオーバレイ技術、SDN のような自動化技術が実用化されることが期待されている。

キーワード：クラウドコンピューティング、データセンター、自動化、マルチテナント

1. はじめに

クラウドコンピューティングサービス（以下、クラウド）の利用が一般的になってきた。これに伴ってこれまでユーザが手元で運用してきたコンピュータシステムをクラウドに移そうとする動きが活発化している。

本稿では、クラウドを提供するデータセンターを題材としてそこで利用されるネットワークの性質と課題を明らかにした上で、SDN に代表されるネットワーク自動化技術の必要性を論ずる。

2. クラウド、データセンター、ネットワーク

2.1 クラウドとデータセンター

本稿で取り扱うデータセンターは、クラウドを提供することに特化したクラウドデータセンターとする。

クラウドデータセンターと言っても、災害を考慮した立地にあり、堅ろうな建屋、自家発電装置、強力な空調設備を備えるといった特性は通常のデータセンターと変わらない。

クラウドデータセンターと通常のデータセンターの違い

いは、通常のデータセンターが多種多様な機器を設置することを想定しているのに対して、クラウドデータセンターにおいては、同一仕様の機器を大量に設置することである。これら機器はクラウドの規模にもよるが、市販されていない特注製品のことも多い。

2.2 クラウドデータセンターのネットワーク

クラウドを提供する設備のように、データセンターに集約して設置されたリソースを相互接続するためのネットワークをデータセンターネットワークと呼ぶ。

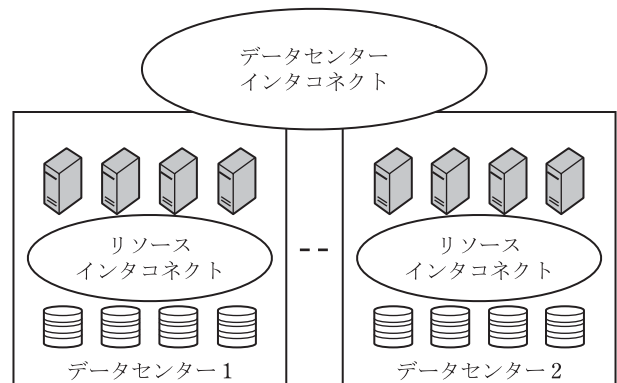


図1 データセンターネットワーク データセンターネットワークは、データセンターに設置されたリソース同士を接続するためのリソースインタコネク トと、データセンター間を接続するためのデータセンターインタコネク トに大別される。

金田克己 (株)インターネットイニシアティブネットワークサービス部
E-mail katz@iij.ad.jp
Katsumi KANEDA, Nonmember (Network Service Department, Internet Initiative Japan Inc., Tokyo, 101-0051 Japan).
電子情報通信学会誌 Vol.96 No.12 pp.921-925 2013年12月
©電子情報通信学会 2013

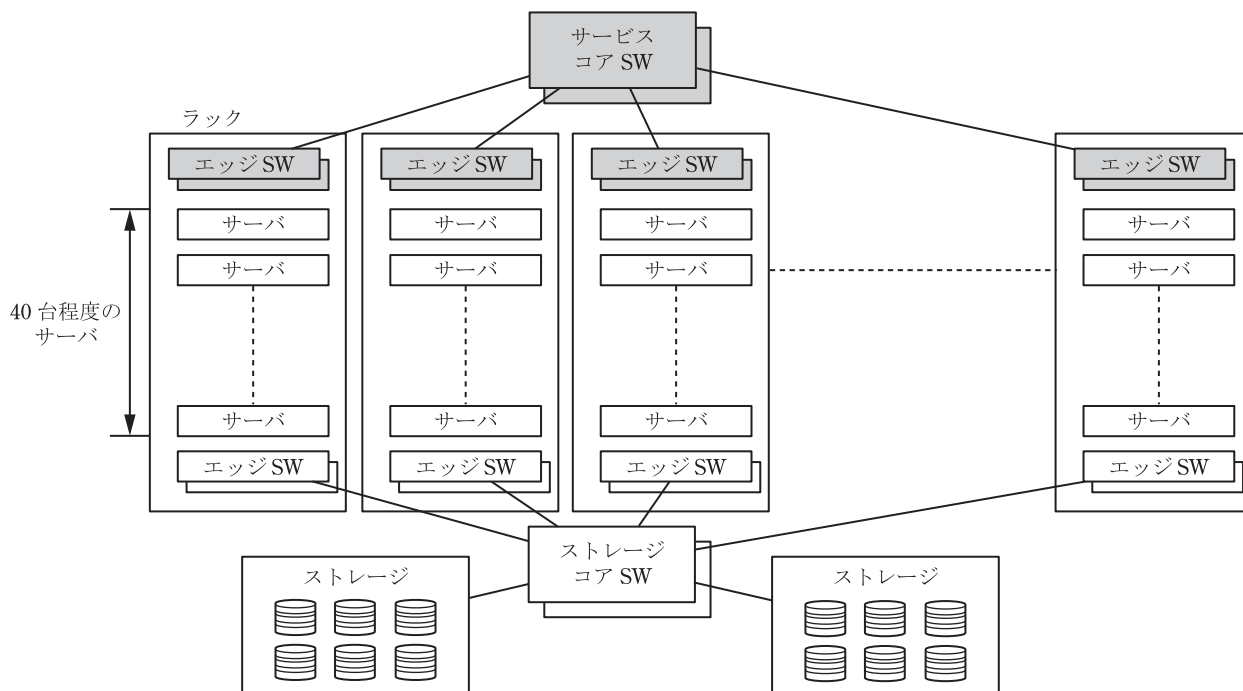


図2 典型的なクラウド提供設備 網かけ部分がデータセンターネットワークを構成する機器である。図中でSWとあるのはイーサネットスイッチの略称である。クラウドを提供する設備では、全てのリソースはあらかじめラックに設置されており物理的な結線は完了している。図面下部のストレージとサーバを接続するストレージネットワークも広義のデータセンターネットワークであるがここでは範囲外とする。

データセンターネットワークは、データセンター内部でリソース同士を相互接続するリソースインタコネクと、複数データセンター間を接続するためのデータセンターインタコネクに大別される (図1)。

本稿ではこのリソースインタコネクに着目して議論を進める。本稿でデータセンターネットワークと言ったときには、このリソースインタコネクを指すものとする。

2.3 データセンターネットワークと自動化

図2に典型的なクラウド提供設備を示す。図ではサーバ同士を接続するネットワーク (図中網掛け部分) とストレージ群とサーバをつなぐネットワークを記述している。広義にはどちらもデータセンターネットワークであるが、ここではサーバ同士を接続するネットワークに限って話を進める。

一般に、クラウドにおいてはそのサービス提供までの

時間を短縮するために、データセンターにサーバ、ストレージ等のリソースをあらかじめ設置しておく。

このとき、ネットワーク機器は設置済みであり、リソースとネットワーク機器の間は結線された状態である。

データセンターネットワークは、このように物理的な構造が固定されている。このような環境で、柔軟なネットワーク構成を可能とするためには、ネットワークを構成する機器に対する設定変更だけで自由にネットワークを構成できるようにする必要がある。ここで、ネットワーク機器に対する設定を、外部のプログラムから可能にすることができれば、人手を介さずネットワークが構成可能となる。このことをネットワークの自動化と言う。

実際には、抽象化したモデルを構築し、論理的にネットワークを取り扱えるように設備を含めて設計することが重要である。3. では、クラウドを例に用いてリソースを抽象化して取り扱うモデルについて論ずる。

■ 用語解説

仮想アプライアンス ルータ、ファイヤウォール、NASのように物理的なアプライアンスをVMで動作するようにしたソフトウェア。

ネットワーク自動化 人手を介さずネットワーク機器の設定を実施すること。更に、ネットワークそのものをプログラム可能とすること。

3. データセンターネットワークの実際

クラウドはその提供形態によって様々な分類があるが、ここでは、アメリカ国立標準技術研究所 (NIST) のクラウドモデル定義⁽¹⁾に基づいて不特定多数の利用者に対して事業者がサービスを提供するパブリッククラウド

ド、その中でも IT インフラストラクチャを提供する IaaS を題材として話を進める。

3.1 本稿における IaaS の定義

IaaS というサービスモデル分類は存在するが、コンセンサスを得た仕様が存在するわけではない。解説に先立って、本稿で用いる IaaS の仕様を定義する。

- 複数のユーザに対してリソースを提供するサービスであり、ユーザが契約したリソースは、それぞれ論理的に分離されている。これをクラウドのマルチテナント利用と呼ぶ。
- IP アドレスを持つ論理インスタンス、論理イーサネットセグメント、及び、インターネットとの接続をサービスとして提供する。
- 論理インスタンスとは、Linux や Windows のような OS、または、ルータやファイヤウォールのようなネットワーク機能とする。
- 論理インスタンスは全て仮想マシン (VM) を用いて実装されることとする。OS は VM にインストールすることで提供し、ネットワーク機能は仮想アプライアンス^(用語)を VM にインストールすることで提供する。物理的なルータ、ファイヤウォール等は提供しない。
- ユーザは、サービスを契約することで、論理インスタンスと論理イーサネットセグメントを自由に組み合わせ、望んだシステムを構築することができる。

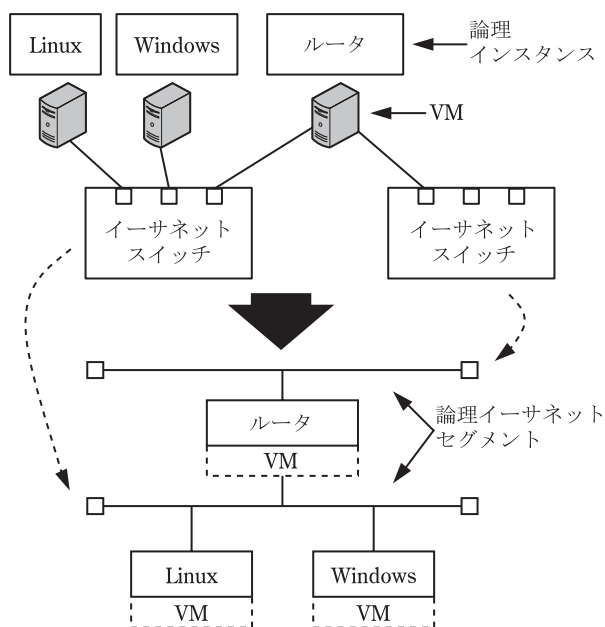


図3 論理インスタンスと論理イーサネットセグメントを用いたシステム間の対応 物理的なシステムと論理インスタンス、論理イーサネットセグメントの対応を示す。図中のルータは仮想アプライアンスを想定している。

- 論理イーサネットセグメントは互いに分離されており通信ができないこととし、ユーザが構築したシステムのセキュリティはこれをもって担保される。

図3に物理的なシステム、論理インスタンス、及び論理イーサネットセグメントを用いたシステムの対応を示した。この図では、イーサネットスイッチと論理イーサネットセグメントが1対1で対応している。図に示したように、VMにインストールされた論理インスタンスのみに着目すれば、論理イーサネットセグメントと論理インスタンスのみでシステムを表現することが可能である。この論理表現を用いて IaaS を説明したのが図4である。

3.2 IaaS の仕組み

それでは、図2に示したような設備に一定の手順で操作を加えることで、図4に示したようなシステムが構成可能なことを説明しよう。

論理インスタンスを生成するのにサーバ仮想化ソフトウェアを用いて構成したVMを用いることとする。また、論理イーサネットセグメントはイーサネットスイッチ(以下、スイッチ)のIEEE 802.1Q VLAN 機能を用いて実現するものとする。ストレージの仮想化については紙幅の関係で省略する。

さて、図2からエッジイーサネットスイッチに接続された2台のサーバを抜き出して詳述したものが図5である。

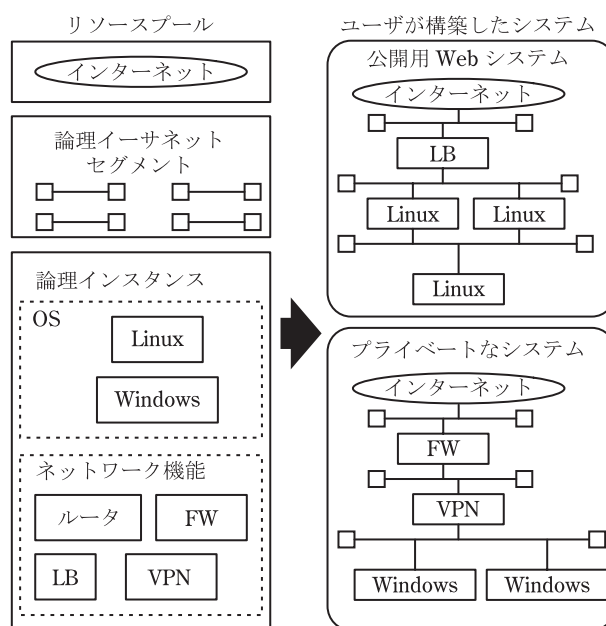


図4 IaaS の説明図 ユーザは、図中左方にあるリソースプールにあるリソースを使って、望んだシステムを構築することができる。

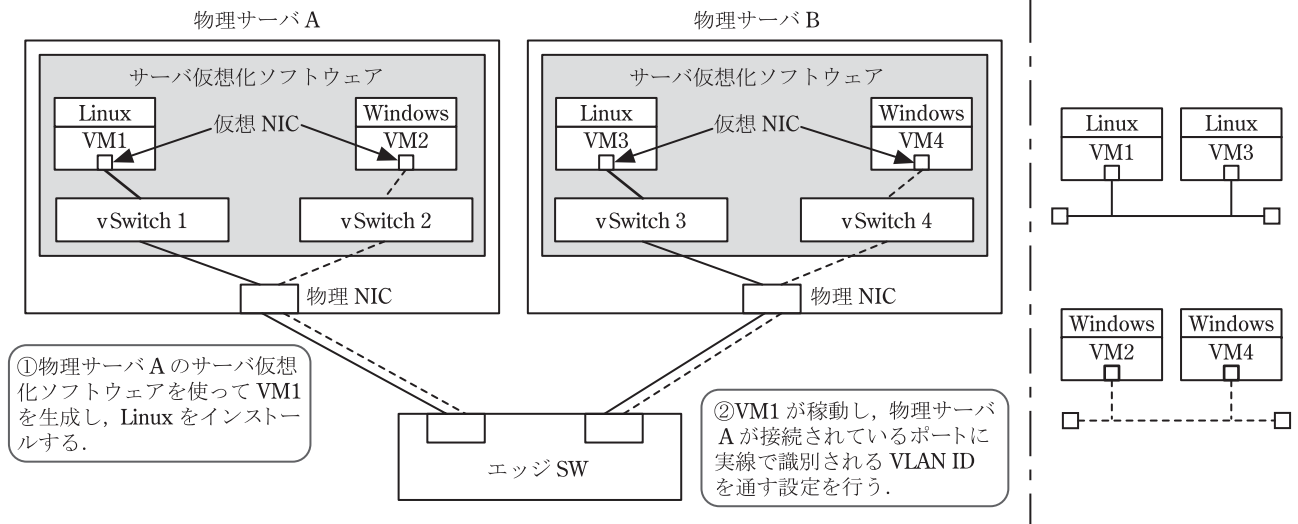


図 5 IaaS の仕組み 一点鎖線の左方が物理的な設備を表し、右方はそこから構成したシステムである。図中の vSwitch はサーバ仮想化ソフトウェア内で動作する仮想的なイーサネットスイッチである。

る。この図では説明を簡略化するために物理サーバ A, B にはサーバ仮想化ソフトウェアがインストールしてあるものとする。サーバ、ネットワークそれぞれに対して、以下のような操作を行う。

サーバ仮想化ソフトウェアに対して、① VM の生成、② VM への OS インストール、③ vSwitch への VLAN ID の割当、④ vSwitch と VM の仮想 NIC の論理的な接続を実施する。ここで、vSwitch はサーバ仮想化ソフトウェアで提供される仮想イーサネットスイッチのことである。

ネットワークに対して、対象となる VM が稼動する物理サーバが接続されているエッジイーサネットスイッチのポートに、VM が必要とする VLAN ID を通すように設定する。

簡略化しているが、上記のような操作を加えることで論理的にシステムを構成することが可能である。

4. データセンターネットワークの課題

IaaS の 1 モデルを提示し、このモデルがサーバ仮想化と IEEE 802.1Q VLAN を用いたネットワーク仮想化を利用することで実現可能であることを示した。ここで利用した技術は古くからあるもので、市販製品で実現可能である。ところが、これらを商用の環境に適用しようとしたときに大きな課題がある。それは、リソースの分割数の上限と自動化の困難さである。例として用いた IEEE 802.1Q VLAN によるネットワークの分割数には上限があり、サービス提供を自動化しようとしたときにプログラム可能な API を備えたスイッチが、余り市販されていないという現実である。

ネットワーク分割数の上限はサービス提供可能数に制

限を設けるため、売上げに影響を及ぼす。プログラム可能な API を備えたスイッチが余り市販されていないという事実は、サービス提供の自動化を阻み運用コストの削減に影響を及ぼす。

いずれもクラウド提供事業者にとっては切実な課題である。

5. データセンターネットワークと SDN

ここまで述べてきたように、データセンターネットワークには、その物理構成が固定されており、ほとんど変更がないという特性がある。また、仮想化技術の進展により、ネットワークのみならず、そこに接続されるサーバ、ストレージ等についても、物理的な機器を仮想化して論理分割することで論理的なインスタンスとして取り扱うことが可能となっている。これらの状況を踏まえて、3. において説明したとおり、適切に論理的なモデルを定義してやれば、物理機器の設定を変更するだけで、一つの共通設備から、複数ユーザに対して、様々なシステムを提供することが可能である。

もし、この共通設備に適切な API が備えられていたとすると、この共通設備はプログラム可能なインフラストラクチャとなり、ソフトウェアで制御可能である。

さて、このような API を考えたときに、サーバとストレージについては、サーバ仮想化ソフトウェアを用いて VM の生成、ストレージの割当、OS のインストール等のオペレーションを、公開された API により外部から実行させることが可能となっている。翻ってネットワークについては、4. で述べたように API を備えたスイッチが余り市販されていないという事実があり、このような用途においてネットワークが課題であるとされる

原因の一つとなっている。

このような事実を踏まえ、SDNはプログラム可能なデータセンターネットワークを実現するものとして期待されている。一例として、OpenFlow互換のvSwitchを使って、VXLANでオーバレイするデータセンターネットワークを構築すれば、ネットワーク分割数の課題、ネットワーク自動化^(用語)の課題も解決可能である。

このようにネットワーク機器の持つ機能をソフトウェアとして実装する、あるいは、ネットワーク構成をソフトウェアで直接制御するといった、これまでユーザができなかったことを可能にすることこそSDNの本質である。

SDNに関してはまだまだ発展途上であり、未成熟な

部分も多いのだが、ネットワーク技術に新たな活力を与えるものとして歓迎したい。

文 献

- (1) The NIST Definition of Cloud Computing, National Institute of Standards and Technology (編), 2011.

(平成25年7月8日受付 平成25年9月17日最終受付)



かなだ かつみ
金田 克己

平3長岡技科大・工・電気・電子システム卒。平5同大学院修士課程了。平22(株)インターネットイニシアティブ入社。以来、クラウドインフラストラクチャの研究・開発に従事。現在、同社ネットワークサービス部シニアテクニカルマネージャー。

