4 ネットワークシステム運用管理への応用

新　麗
（株）IIJ イノベーションインスティテュート

新しいネットワークシステム

従来，インターネットを図示するときには，図 -1 のように雲のような形が使われてきた．これは，雲の中の詳細は分からないが，雲を通じて接続されているということを示している．インターネット全体を 1 つの雲で表記することもあれば，複数の雲が接続されていることもあり，雲の中にまた雲を描くこともある．インターネット全体を統括する管理主体はないが，その中の雲が表すネットワークの 1 つ 1 つは，分散，独立して管理されている．

インターネットの接続性を示してきたこの雲の中に，インターネット上のアプリケーションやサービス，それと関連するストレージなどまで入れるのが，いわゆるクラウドの 1 つの形として語られているのではないだろうか．雲の中にあるのはインターネットに接続されたシステムであり，中の詳細は分からないが，接続すれば必要なリソースやサービスなどが提供される．利用者は所有する機器，つまり雲の外の機器であれば自分で設定や管理を行わなければならなかったが，雲の中のサービスであれば機器の管理を行う必要はなくなる．

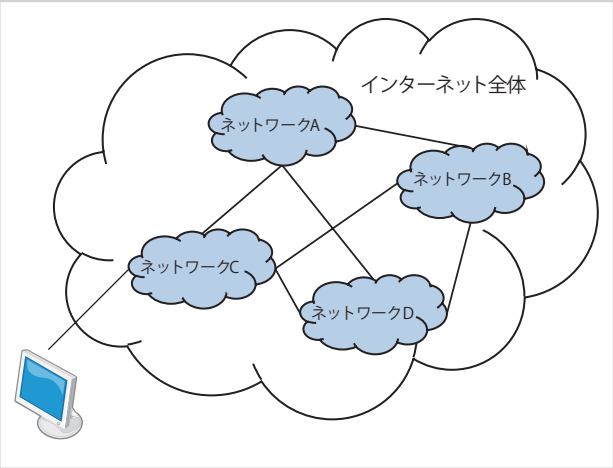

図 -1　インターネットと雲の図

■ ネットワーク運用管理の重要性

一方で雲の中では，接続性だけでなくリソースやサービスまでを統合して提供することになる．一般にサービスを提供するためには，ネットワーク機器だけでなくコンピュータやストレージ，あるいはアプリケーションを組み合わせてシステムを構成しなければならない．したがって，管理対象となる機器の数がこれまでとは比べ物にならないほど膨大になるだけでなく，種類，それも類似の機種というのではなく性質の違う機器を管理する必要がある．これまでも機器の接続や組合せを統合的に管理する研究は行われているが，クラウドの登場により，管理対象となる数や種類が桁違いに増え，新しく接続する機器も増え，関連する情報が変化してきたことで，また新たな課題が出てきたと言えるだろう．

また，ネットワークシステムの管理および運用に関して，特に要求が厳しくなってきているのが信頼性である．ネットワークシステム上にさまざまな種類，分野のサービスが稼働するようになり，1 つのトラブルが与える影響が多岐にわたることもある．まずトラブルがないこと，万が一起こっても迅速に復旧できることが必要条件となる．その点で，ネットワークシステムはすでに社会基盤となっており，いわゆるインフラに相当する信頼性が求められるようになっていると言える．運用管理はインフラとしての信頼性を提供するための重要な技術の 1 つである．

■ システム停止の原因

社会基盤となったネットワークシステムの実体は，サービスを行う会社内から，データセンタのような専用のファシリティを持つ設備へと移行しはじめている．そのため，データセンタに設置される機器は増加の一途をた

どっている．特定のサービス専用のシステムも増加しているが，クラウドのようにハードウェアやアプリケーションを事前に用意し，要求に応じて組み合わせる利用形態も増えている．データセンタの実態は一般に非公開であるが，数千から数万台の機器やアプリケーションが稼働していると言われており[1]，さらに増え続けている[2]．

またハードウェアの進歩により，複数のシステムやアプリケーションを1台の機器に収容できるようになった．たとえばネットワーク危機の処理能力が向上して，数十台のサーバが1台のネットワーク機器を共有することができる．またサーバの高機能化および仮想化技術により，1台のサーバ上に複数の OS やアプリケーションを動作させることも一般的になりつつある．これらの技術は，データセンタに設置された機器を効率的に利用し，稼働するアプリケーションの数や種類を増やすことで，サービス向上に貢献するが，運用管理はますます複雑になる．

ある報告[3]によれば，データセンタの停止時間の78% は設定ミスによるものだという．つまり，運用管理上の人為的ミスである．機器の故障やバグなどが原因での停止のほうが圧倒的に少ないということになる．また，情報漏えいなどのセキュリティ事故の 95% は，パッチが適用されていなかったり，サーバに設定ミスがあったりすることが原因ということである．設定ミスを減らすための対策の1つは，人手による設定を減らすことであり，自動的な運用管理への移行である．

■監視からシステム制御へ

クラウドのような大規模なネットワークシステム運用管理を行うためには，従来の監視中心のネットワーク管理手法から，ネットワーク制御を可能にすることが必要である．その上でネットワーク管理の自動化による省力化を行って大規模かつ複雑なシステムへの対応ができるようにし，かつ信頼性も向上させなければならない．この実現には多くの課題があるが，以下にその主なものを述べる．

現在のインターネット管理は，SNMP（Simple Network Management Protocol）を中心として行われている．SNMP によって行う管理はネットワーク機器の監視が主であり，クラウドで必要とされるような大規模システムの管理にとって十分とは言えない．

ネットワーク機器の設定を行うには，CLI（Command Line Interface）を利用するのが一般的である．CLI 機器を操作するためのコマンド群であり，管理者が入力することを想定して設計されている．CLI はネットワーク機器ベンダごとに規定されており，相互互換性がないのが現状である．たとえ IP アドレスを設定するだけであっても，コマンド名やパラメータの数や順番が異なったり，指定するインタフェースの表現方法が異なっていたりする．この差異はベンダごとにだけではなく，同じベンダであってもモデルやバージョンによって，あるいは，ルータかスイッチかのような機能の違いによっても異なる．ネットワークシステムを構成する機器は数年単位で入れ替えるのが一般的である．また拡張も頻繁に起こるため，常にすべて同一の機器で構成することは困難である．さらに，機器は入れ替わっても提供するサービスは維持しなければならない．そのために，機器ごと，バージョンごとの差異はシステム構築時に吸収する必要があり，現状では管理者が個別に対応している．

管理体制についても新たな課題が出てきている．システムの規模が大きくなるにつれて，管理が分業していくのは必至である．しかし前述したように，ネットワークシステムは機器を共有していることが多く，また機器の管理者とアプリケーションの管理者とでは，必要となる管理対象，範囲が異なっている．つまり，管理者によってさまざまな視点での管理が必要となってきている．

■アーキテクチャとモデル

以上のような状況において，ネットワークとコンピュータ，ストレージ等の各種機器を組み合わせ，システムとして管理するためには，新しい管理アーキテクチャとモデル化が必要となる．インターネット技術に関しては SNMP を中心とした管理モデルがあり，コンピュータデバイスと管理インタフェースに関しては，DMTF[4]（Distributed Management Task Force, Inc.）において，CIM（Common Information Model）として議論されているが，双方を統合したアーキテクチャの設計はこれからである．また，SNMP には監視情報についての情報モデルは MIB（Management Information Base）として定義されているが，CLI による設定についてはまだ共通モデルはなく，標準化もされていなかった．そこで，設定に関しての標準化として登場したのが NETCONF である．

NETCONF が IETF（Internet Engineering Task Force, インターネットプロトコルの標準化団体）において 2006 年に標準化された後，NETCONF を実装したネットワーク機器やネットワーク管理機器ソフトウェアが増えてきた．現在はまだプロトコルを実装したという段階であり，NETCONF の本格的な利用とまでは至っていない．しかし，実装が進んだことで運用管理システムへ応用する準備が整ったので，今後利用および応用が広がっていくと期待される．

本稿では，NETCONF をネットワークシステム運用管理に応用し，さまざまな機器の組合せによるネットワークシステムの管理を実現するためのアーキテクチャや

モデルの 1 つの形態を定義し，またそれに基づいて小規模な環境で行った実証実験について報告する．

ネットワークシステム管理アーキテクチャ

クラウド等の大規模かつさまざまな種類の機器が相互接続されるネットワークシステムには，まだ確立したアーキテクチャがない．さまざまな機器やアプリケーションが関係することを考慮すると，単一ではなく複数の管理ドメインが相互接続する形態になると考えられる．このような管理アーキテクチャを設計するにあたって重要なことは，(1) 従来の機器主導でなくユーザ主導の管理モデルであること，(2) トランスポートプロトコルに非依存であること，(3) ネットワークサービスに対して水平垂直方向にさまざまな事業者が存在することを前提としていること，を考慮することである．これを実現するために，まず，ネットワーク機器，サーバ，およびストレージをまとめて扱うネットワークリソースと，それに対して適用する機能とを分離する．次に，ネットワークリソースに対して，ユーザの要求を実現するシナリオ，トランスポート非依存のネットワーク構成情報，および機能モデルの 3 つを分離し，それぞれのクラスからなる，ネットワーク管理アーキテクチャを以下のように定義する．

■ シナリオ

ネットワークシステムに対して行う管理作業を手順化したものを指す．現状では人手で行っている手順を解析するが，最終的にはユーザは選択するだけとするか，あるいは何らかの条件の下で自動的に適切なシナリオが起動して，自動的に動作することを目指す．

■ システム構成情報

管理対象となるネットワークシステムの構成情報．構成している機器や接続，そのシステムを実現するための設定情報やネットワーク構成情報も含む．システムのモデル化が必要となる．具体的には，ネットワーク接続情報や設定情報，稼働する OS やアプリケーションなどの情報となる．設定情報は具体的なコマンドではなく，機能モデルに基づいて規定されたパラメータ情報等である．

■ 機能モデル

ネットワークシステムを実現するために必要な機器のモデル．要求事項からの実現を目指し，ベンダに依存しない機能のまとまりを定義する．具体的には，VLAN や VPN などの機能単位でのモデル化となる．

■ 各クラスの相互作用

これらの 3 つのクラスは相互に関係しあってシステムを構成し，管理制御も行われる．基本的にはユーザに見えるのはシナリオであり，ここにネットワークシステムの実現にあたっての要求事項が含まれる．たとえば，Web サーバを立ち上げたい，という大きな要求があり，それに対して規模の検討などが行われた結果，必要なネットワークシステムが選択される．

システム構成情報はユーザからの要求を具体化し，それらを実現する技術的検討を行う．たとえば，Web サーバを立ち上げる場合に，マシンに必要な性能や，ネットワークの帯域，あるいはネットワークをローカルに設定するなどの構成に関する検討が行われた結果，その実現に必要な機能が選択される．

ネットワーク機器は機能モデルと設定情報に従って実際に設定が行われる．このインタフェースが NETCONF であれば機器ごとに差異はないが，現在はまだ NETCONF 対応機器と CLI で設定する機器とが混在しているのが現状である．ネットワーク管理アーキテクチャの概念図を図 -2 に示す．

マルチドメイン環境における ネットワークシステム管理

複雑に連携するネットワークシステムにおいて，共有される機器などのリソースを必要に応じて管理するためには，管理者が必要とする情報をグループ化する必要がある．一般にネットワークシステムは，複数の閉じたシステムから構成されていることから，本アーキテクチャではこのような閉じたシステムをドメインと定義する．

ドメインは，システムが提供するサービスの性質や範囲などで構成される場合と，ネットワーク機器や機能のレベルなどで構成される場合とがある．前者はユーザ主導，後者は機器主導と言うことができる．現在は，ユーザ主導の要求事項を受けて，運用管理者が機器ごとの設定を行うという運用が一般的であり，ドメインはまったく独立しておりその間は人が対応することで一貫性を維持しようとしている．このような運用は，小規模なシステムであれば可能だが，クラウドのような大規模で複雑なシステムには対応できない．そこで，ユーザ主導のドメインと機器レベルのドメインとが混在しているのを問題とし，特にユーザ主導のドメインを「ポリシードメイン」と定義する．

■ ユーザとシステム

大学や会社などで情報共有のシステムを構築する場合，夏休みのおしらせなど組織内の誰もが見られる情報もあ

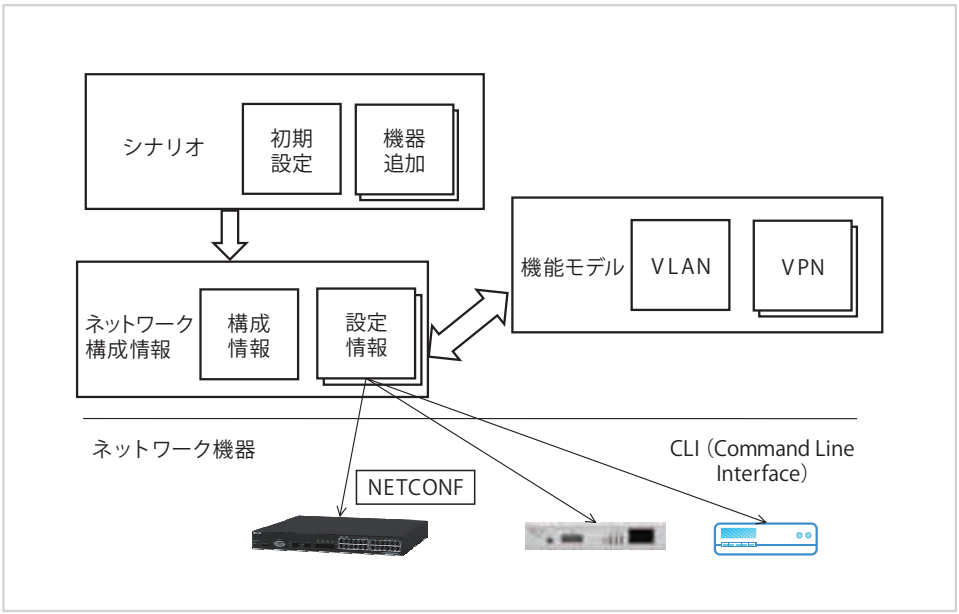

図 -2　ネットワークシステム管理アーキテクチャ

れば，成績や顧客情報などアクセス制限をかけるべき情報もある．つまり，どの情報に対して誰がアクセスできるのかというポリシーを定義する必要がある．この定義はネットワークシステムとは関係なく情報管理の問題であり，本来のユーザ要求ということになる．現状では，情報に対してパスワード等でアクセス制限をかけることが多いが，システムとして切り分けられるほうがより安全である．

またこのようなシステムを実際に構築する際に，アクセス方法によってネットワーク構成が違うことがある．たとえば，同じ情報を組織内からアクセスする場合と，支社など組織外からアクセスする場合である．ネットワークの機能から見ると，組織内のネットワークとインターネットを経由した VPN などは別のネットワーク構成を持つ別のドメインである．管理方針も方法も違っているため，一般的には管理も別になっている．しかし，ユーザ要求を実現するためには，ネットワークの機能が異なる，つまり機能レベルのドメインが異なっても，同一ポリシーで扱う必要がある．現在はこのようなポリシーからネットワーク機器への実装は，設計者や運用者が対応することで実現している．

ポリシードメインは，ユーザ要求によるポリシーに従って決められる範囲として定義し，この範囲での管理を実現するための機器やアプリケーションなどをグループ化するものである．ユーザの権限によって属するドメインを決め，そのサービスに対応するネットワークリソースとの対応付けを行う．階層構造ではなくドメインによって定義すれば，複数のドメインに属することも可能であり，複数の権限を持つユーザの定義も行うことができる．

ユーザの権限によってシステムアクセスを制限する方法は，コンピュータセキュリティにおける，ロールベースアクセス制御と類似している[5]．本概念は，情報アクセスだけでなく，関連するシステムとの関係までを記述できるように拡張する．これによって，ユーザ要求とシステムとを一貫して扱うようにする．

■ ネットワークシステムの共有

ネットワークシステムの実装を詳細化すると，1 台の機器が複数のドメインに属している場合も多い．たとえば図 -3 に示すように，情報群 I を提供するシステムと情報群 J を提供するシステムがルータやスイッチなどのネットワーク機器を共有する場合である．当該のネットワーク機器は，回線が接続されているポート，あるいは仮想ポートごとに異なるドメインに属することになる．このような形態ではシステムの管理者とネットワーク機器の管理者が別であることも多い．このような場合は，管理者の視点に対応するように各ドメインを定義する．たとえば，情報群 I 提供システム，情報群 J 提供システムのほかに，ネットワーク機器の管理あるいは監視用のドメインを定義する．

ネットワークシステム管理制御システム

以上のようなアーキテクチャとモデルに基づき，ネットワークシステム管理制御システムの試作を行う．システム管理ツールは，管理者が監視や状態確認を行ったり，構成変更を行ったりするため，ユーザインタフェースの作りも重要となる．本システムでは，使いやすさという視点でのユーザインタフェースに関しては追及しないが，

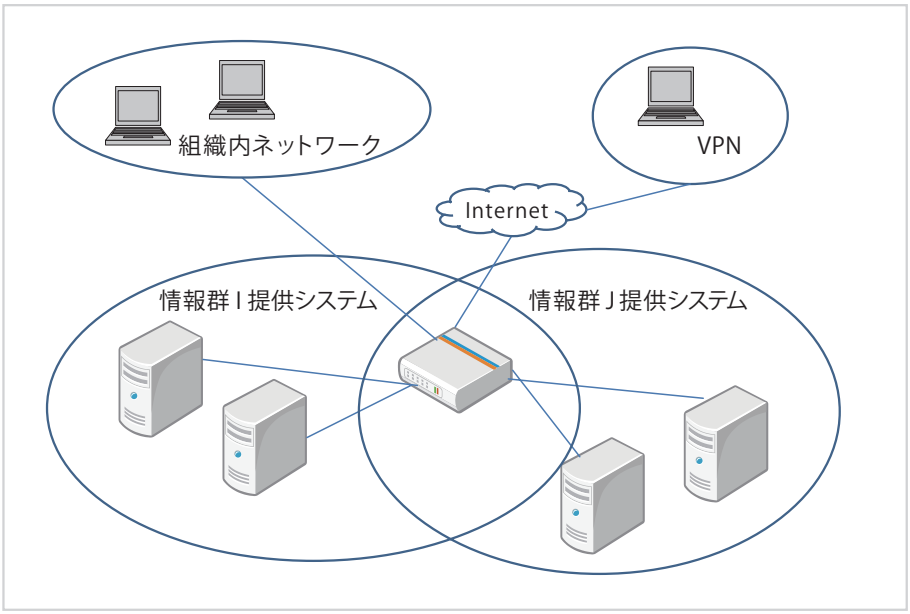

図 -3　ネットワークシステム構成と共有の例

水平垂直にさまざまな利用者・事業者がいることを考慮し，利用者や事業者，あるいは管理担当ごとに必要な情報を提示できるように設計する．さらに，ポリシードメインに対してあるシナリオを実行することによってネットワークシステムの管理制御を自動的に行う機能を実装する．

■ 視点に応じた表示

まず，水平垂直に関係するさまざまな利用者・事業者に対し，提供されているサービスや視点に対応した表示やシナリオを提供するため，どのように情報や機能が共有されるのか整理を行う．複数のネットワークシステムにより利用されるネットワーク機器の管理・制御を行うためには，サービスシステムからの要求を受けてネットワークシステムの設計を行う設計者，設計を受けてネットワーク機器の設定を行う設定者，また設定されたネットワーク機器の運用を継続して行うネットワーク管理者，さらに各サービスシステムの管理を行うシステム管理者など，さまざまな人々が携わっている．

設計者，設定者，管理者はその役割ごとにそれぞれ部分的にネットワークシステムの管理にかかわっている．各役割間で連携してネットワークシステムを管理するためには，ネットワークシステムの構成情報を共有することが重要である．構成情報の共有にあたっては，ネットワーク機器の設定に習熟していなくても構成情報を理解できるようにネットワーク機器の設定ファイルや CLI など各機器の設定方式に依存した形式でなく，ネットワーク機器の機能を共通化してより共有しやすくすることが重要である．つまり，さまざまに関連しあう役割によって，共有される情報とそれを基礎として必要な情報だけにアクセスできるようにする必要がある．

現在行われている一般的な管理への応用を考慮するとたとえば図 -4 のように，物理結線，VLAN などの OSI モデルでの 2 層にあたるデータリンク層，IP などの 3 層にあたるネットワーク層，および全体管理を行うビューを表示することが考えられる．

■ 管理システムの構成

試作したシステムの構成図は図 -5 の通りである．構成はデータモデル，機能，機能モデルの大きく 3 つに分けられている．

データモデルは，ネットワークリソースとネットワークシステムの構成情報を管理するための要素で，リソースデータベースと構成情報データベースとからなる．機能は，コントローラからネットワーク管理の要求を受けるための要素で，リソース管理と設定管理とからなる．機能モデルは，シナリオデータベースであり，ユーザの要求事項を実現するための要素である．ネットワークシステムへの要求を，ネットワークシステムに対して行う管理作業として手順化し，それをシナリオとして管理プロトタイプにおいて実行するように設計を行った．

■ 管理システムの実行

実験のための実データを作成するため，まず対象となる小規模なネットワークシステムを構成するネットワーク構成情報を定義する．さらにこのシステムに適用するサービスシナリオを作成することも必要となる．

システム設計にあたって，データモデル，ネットワーク構成情報の記述には XML スキーマ，実際に利用するデータの記述には XML，情報管理には XML データベ

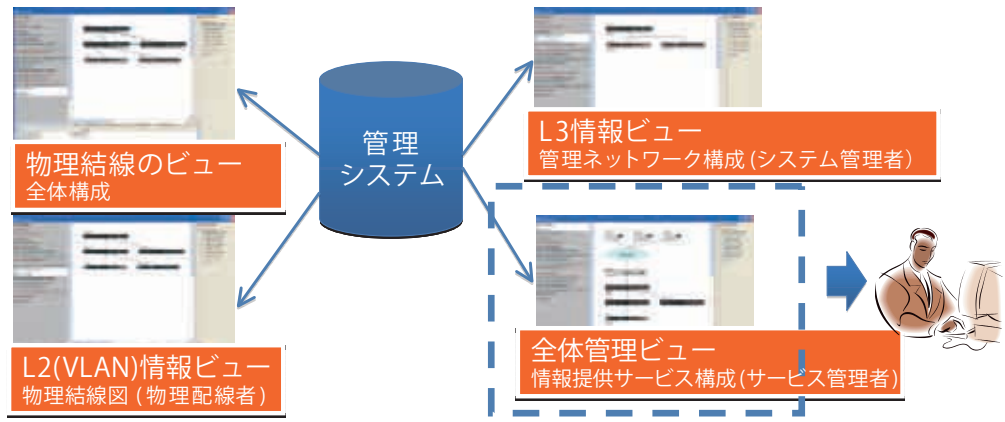

図 -4　各視点における表示ビュー

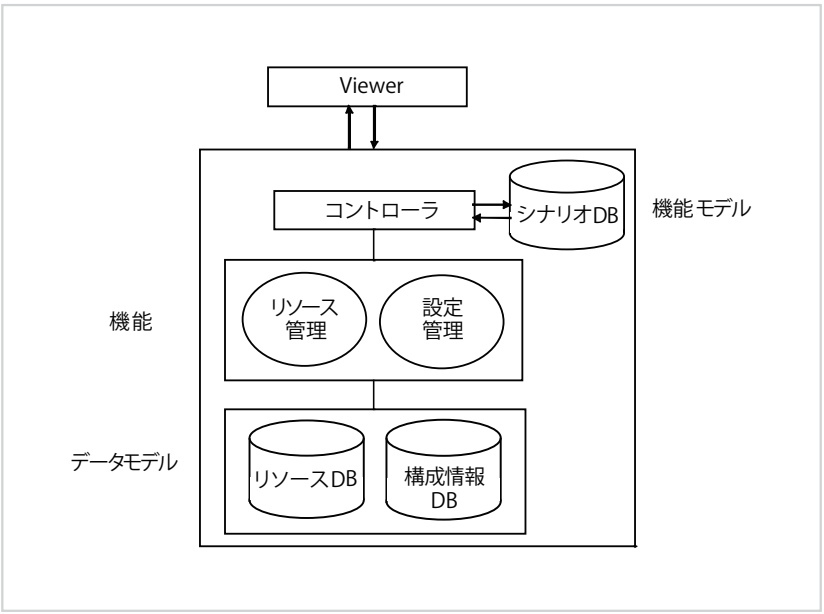

図 -5　ネットワークシステム管理プロトタイプ構成

ースを利用した．ネットワーク機器の設定に関しては，データモデルに従って設定情報を記述し，本試作に関しては，実際の設定には NETCONF プロトコル対応であり Java インタフェースを持つアラクサラネットワークス社製の ON-API を使用した．

図 -6 にシステムの実行画面例を示す．画面中央にネットワーク構成を表示し，左のタブによってビューを切り替え，物理結線，VLAN などの接続を見ることができる．右側にはこのシステムに対して実行できるシナリオのリストがあり，状況に応じて，たとえばサーバ機器を 1 台追加したり，VLAN を作成したりという作業を行うことができる．実行されたシナリオに対応してデータベースが書き換えられ，表示画面にはシナリオ実行後の構成が表示される．また実際のネットワーク機器に対しても設定が行われ，システムも更新される．

データモデルを設計したことで，ネットワーク構成情報およびネットワーク機能と実際の設定を分離することが可能となる．ネットワーク構成や機能を追加する場合には，対応するデータモデルを設計して拡張することも可能である．実際のネットワーク機器設定については，現状では各機器に対応してプログラムやコマンド発行などをしなければならないが，システム自動化を行う場合には，他のプログラムとの連携ができるかどうかが鍵となってくる．今回の試行でも，機器設定に対する NETCONF のプログラムインタフェースは必須ともいえるものであり，今後ネットワーク機器などでの実装が進むことを期待する．

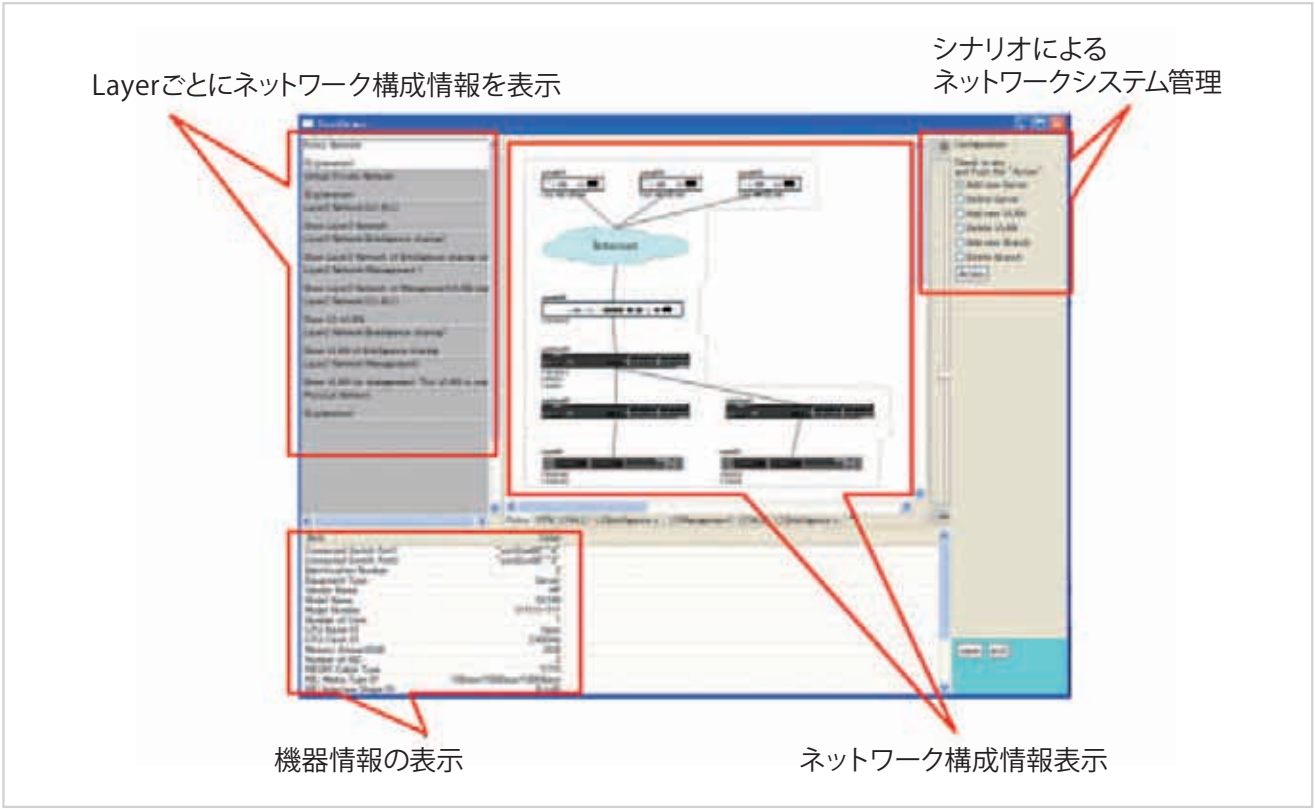

図 -6　管理システムの実行画面例

今後の課題

これまでにもネットワーク管理，システム管理の研究，製品は多くあるが，両者を連携させる例はあまり存在しない．この分野は研究よりも製品が多いこともあり，内部のデータ構造などが非公開である傾向が強く，連携が難しい構成になっていることが多い．しかしクラウドなどの大規模システムにおいては，関連する機器の連携管理が必須である．そのための全体アーキテクチャの設計や公開されたデータモデルの検討は，まだごく一部で問題が認識された程度である．これまでどちらかといえばシステムありきの管理が行われる傾向があったが，理論も含めたモデル化を考える時期にきていると言えるだろう．モデル化には計算機科学の成果を応用するべきであることは言うまでもない．

参考文献

1) Inside Microsoft's $550 Million Mega Data Centers, http://www.informationweek.com/news/hardware/data_centers/showArticle.jhtml?articleID=208403723
2) Microsoft : Datacenter Growth Defies Moore's Law, http://www.pcworld.com/article/130921/microsoft_datacenter_growth_defies_moores_law.html
3) BladeLogic Sets Standard for Data Center Automation and Provides Foundation for Utility Computing with Operations Manager Version 5, http://findarticles.com/p/articles/mi_m0EIN/is_2003_Sept_15/ai_107753392/?tag=content;col1
4) Distributed Management Task Force, Inc., http://www.dmtf.org/.
5) Ferraiolo, D. F. and Kuhn, D. R. : Role Based Access Control (PDF), 15th National Computer Security Conference, pp.554-563 (Oct. 1992).

（平成 21 年 11 月 2 日受付）

新　麗（正会員）
ray@iijlab.net

電気通信大学博士前期課程修了．奈良先端科学技術大学院大学博士後期課程修了．博士（工学）．現在，（株）IIJ イノベーションインスティテュートにて NETCONF およびネットワークシステム管理の研究開発に従事．