

運用の効率化を目的としたネットワーク構成管理 と自動設定の実現

近堂 徹^{1,a)} 田島 浩一¹ 岸場 清悟¹ 吉田 朋彦¹ 岩田 則和¹
大東 俊博¹ 西村 浩二¹ 相原 玲二¹

概要：ネットワークの利用形態が多様化・複雑化するなか、ネットワークインフラの運用管理の効率化が強く求められるようになってきている。しかしながら、管理対象となるネットワーク機器は増加し、人手では対応しきれないケースも多い。機器の設定状況が管理情報として正しく登録されてない場合、障害時の初動対応遅れやヒューマンエラーの発生等が避けられない。本研究では、組織内のネットワークデザインと管理の一元化に加え、ネットワーク機器の構成管理と設定の自動化について考察する。具体的には、広島大学で運用するキャンパス情報ネットワーク (HINET2014) のエッジスイッチ約 450 台に対して、VLAN 情報などの構成管理と設定自動化を実施し、その効果と課題について述べる。

Realization of a Network Configuration Management for increasing Operation Efficiency

TOHRU KONDO^{1,a)} KOICHI TASHIMA¹ SEIGO KISHIBA¹ TOMOHIKO YOSHIDA¹ NORIKAZU IWATA¹
TOSHIHIRO OHIGASHI¹ KOUJI NISHIMURA¹ REIJI AIBARA¹

Abstract: While the growing diversity and complexity of the computer network, the operational efficiency of network management has been required. However, network equipments which should be managed are increasing, and it results in a management cost increase. To improve this issue, in this paper, we think the configuration management and automatic provisioning of the network service. Specifically we describe the effectiveness and problem of the proposed method through the application to a Hiroshima University's campus network system which is consisted by approximately 450 network switches.

1. はじめに

ICT 環境は、今日の情報化社会における社会的基盤のひとつとして人間の生活のあらゆる場面で必要不可欠となった。加えて、それを支えるネットワークも高いセキュリティ・安定性を確保しつつもユーザの利便性を損なわないサービス提供が求められるようになってきている。また、クラウドコンピューティング導入による ICT システムの運用効率化 [1] の動きが顕著になりつつあるなか、俊敏性・柔軟性に優れたネットワーク基盤への要求が明確となっている。

一方、ネットワーク運用管理の面から考えると、管理対

象となるネットワーク機器は増加し、ネットワークの利用形態が多様化していくなかで、組織におけるネットワーク管理の効率化を進めていくことが大きな課題となってきている。

近年では、SDN(Software-Defined Networking) 等の技術開発により、ネットワーク構成をソフトウェアで定義し、柔軟な構成変更を実現することが可能になってきている。ネットワーク仮想化との組み合わせにより、運用自動化や迅速なサービス展開も視野に入れた研究開発も行われている。今後、SDN の利点を活用した柔軟なネットワーク運用の導入が進むことが予想される。これらの技術を導入することで、ネットワーク運用管理コストを削減することが期待できる。一方、コントローラ制御による集中管理による

¹ 広島大学情報メディア教育研究センター, Information Media Center, Hiroshima University

^{a)} tkondo@hiroshima-u.ac.jp

オーバーヘッドやそれに伴うスケーラビリティへの不安、設計・運用思想が従来と大きく異なるため運用ノウハウが蓄積されるまでの運用管理コストの実質的な増加などの課題がある。

広島大学では、2008年度からキャンパスネットワークの管理方法を一新し、全学整備および一元管理によるキャンパスネットワークを構築・運用してきた。さらに2014年8月より運用を行っているキャンパス情報ネットワーク HINET2014 では、エッジスイッチ約450台に対して、VLAN情報などの構成管理と設定自動化を実施している。本稿では、これらの取り組みから得られた知見より、組織内におけるネットワークデザインと管理の一元化に加え、ネットワーク機器の構成管理と設定の自動化による運用の効率化について考える。

本稿の構成は以下の通りである。まず2章では、ネットワーク構成管理および運用自動化における現状と課題について整理するとともに、SDNによる構成管理手法についてまとめる。3章では、本学のキャンパスネットワークの概要について述べ、本研究で提案するネットワーク構成管理と自動設定手法について述べる。4章では運用における効果と課題について考察し、最後に5章でまとめを記す。

2. ネットワーク管理の背景

本章では組織におけるネットワーク管理の現状とその問題点について整理し、今後、普及が見込まれているSDN技術の活用についてまとめる。

2.1 ネットワーク管理の現状と問題点

大学などの高等学術機関では、大規模な組織においては学部や学科などの単位でサブネットを構成し、サブネット内の運用は各組織の裁量に委ねられているケースも少なくない。しかしながら、多くの部局では対応要員の継続的な確保は不可能であり、その維持が困難となっている。また全学的に一元的な管理運用を行っている組織においても、ネットワーク運用管理のための専任の人員の確保することは難しい状況となっている。

その一方で、ネットワークがライフライン化し大規模になるなか、管理対象となるネットワーク機器は増加し、人手でのネットワーク管理が限界になりつつある。例えば、ネットワーク装置に対する設定投入を考えた場合、ネットワーク全体構成やVLAN等の確認から、コンフィグ生成、さらにヒューマンエラーを回避するための2重、3重のチェックを経て設定投入という手順を考慮すると、少ない人員での運用管理が難しいのは想像に難しくない。それでもなおヒューマンエラーはゼロにすることはできない。さらに、利用者からの設定要求に対する迅速性も求められ、管理情報との整合性が取られないまま設定だけが変更されてしまう恐れもある[2]。このように機器の設定情報と管

理情報との間に乖離があるケースでは、障害時の初動対応遅れやヒューマンエラーの発生によるコスト増は避けられない。さらに、ネットワーク機器だけではなくIPアドレスやMACアドレス等の情報管理も考えると、その範囲は拡大し更に複雑化することも考えられる。資源管理に関しては文献[3],[4]などでも取り扱われ、設定に関するエラー回避や時間短縮に効果があることが示されているものの、設定の自動化までには至っていない。

なお、広島大学でも2008年度から全学整備および一元管理によるキャンパスネットワークを構築・運用している。障害時やセキュリティインシデント時などの迅速な調査・対応に一定の効果が得られているものの、ネットワーク構成変更に伴うネットワーク機器への設定投入は外部委託による設定補助業者で行っていたため、申請から実際に利用できるまでに1~2営業日を要していた[5]。

2.2 ネットワーク運用管理の効率化

近年、ネットワーク運用管理の効率化を目的としてSDN技術を活用する動きが活発になりつつある。本稿ではSDNを「ネットワークの構成や状況の可視化、運用の最適化」という広義の意味での用語として考える。その本質は、統一的な操作が可能な抽象化レイヤを定義することで、ネットワーク機器ごとに異なる処理を隠蔽し、コントローラーによる集中管理とソフトウェアによる柔軟な制御を可能にすることにある。ネットワーク構成や制御を一元管理し、ソフトウェアで制御することにより、ネットワーク運用に人手を掛けず、インフラ維持の低コスト化を狙ったものである。また、利用者からの設定要求に対するリードタイムの短縮も可能となる。

SDN技術等によるネットワーク運用管理の効率化・自動化には強い要望があるものの、その利用はデータセンターや仮想基盤上での適用にとどまっており、組織内であってもエッジスイッチを含めたネットワーク全体で適用されている例は少ない。その理由としては、従前と比較しネットワークデザインや運用ポリシーが大幅な変更を伴う可能性があること、リソース管理の一元化や制御の集中化によるスケーラビリティ、枯れてない技術の不安定さへの懸念、運用やトラブルシューティング時のノウハウの欠如などが考えられる。新しい概念のもとでネットワーク運用を行うには、既存手法からの段階的な移行を検討しつつ、これらの点をひとつずつ解決していく必要がある。

3. HINET2014におけるネットワーク管理手法

広島大学ではネットワーク運用管理の効率化を実現するために、ネットワーク設定の自動化機能を取り入れた新しいキャンパスネットワーク(HINET2014)[6]を2014年8月より運用している。本章では、HINET2014の概要とそ

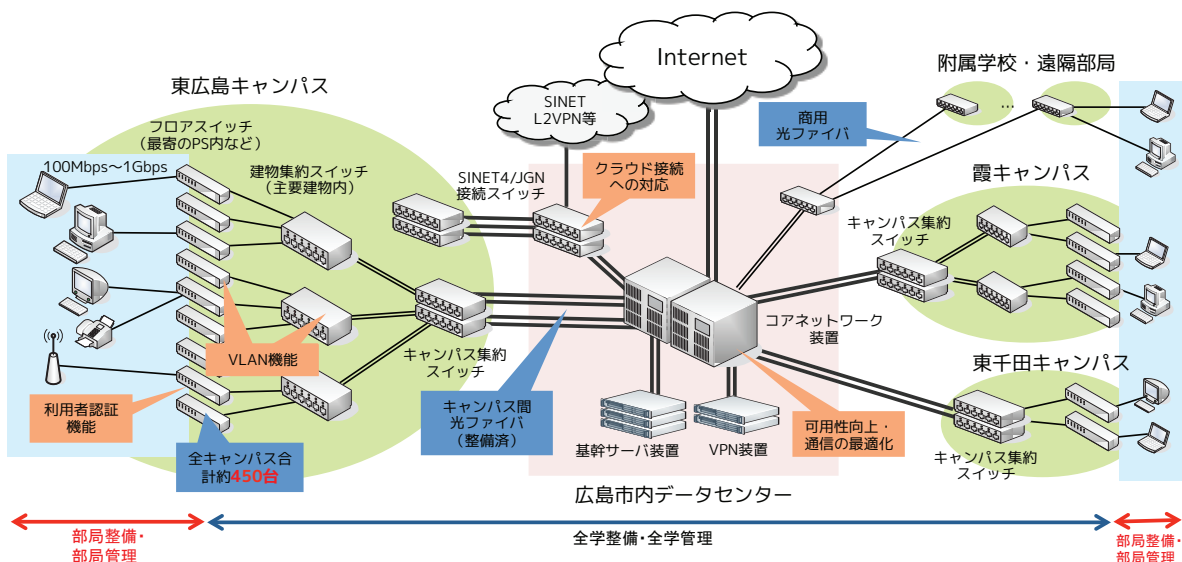


図 1 HINET2014 の概要

の管理手法について述べる。

3.1 キャンパス情報ネットワーク HINET2014

3.1.1 概要

ネットワーク概要を図 1 に示す。HINET2014 は主要 3 キャンパス（東広島，霞，東千田）および附属学校，呉・竹原などの小規模遠隔部局に整備されており，データセンターに設置するコアネットワーク装置を最上位に，スター型のネットワークとなっている。全学整備の範囲を基幹ネットワークからフロアスイッチまでとし，約 450 台のフロアスイッチの各ポートの設定までを一元管理としている。ポート総数としては，18,000 ポートとなる。フロアスイッチから各部屋までのフロア配線は部局が整備および管理を担当する。

各ポートには，図 3 に示すコネクタ ID とよび識別番号（ラベル）を情報コンセントに対応する形で割当てている。コネクタ ID はフロアスイッチに割り当てられたスイッチ ID とポート番号の連結によって表現されている。スイッチ ID はフロアスイッチの物理的な位置情報から決められることから，トラブル対応時の問い合わせ項目としたり，後述するネットワーク利用申請サービスによる申請時情報として，利用者が一般的に利用する識別番号となっている。

次にネットワーク構成について説明する。HINET では学内外からのアクセス可否パターンおよび利用形態により区別される「ゾーン」という概念を導入している。図 2 に主要なゾーン構成を示す。ゾーンのアクセス制限は VLAN 毎に設定可能な個別ファイアウォール（ゾーン C 用），および全学ファイアウォール（ゾーン B，ゾーン D 用）によって実現している。構成員の多くが研究室単位でゾーン C を申請し，その中に PC やプリンタ，NAS 等を設置して管理・運用するのが一般的な利用形態となっている。学外公

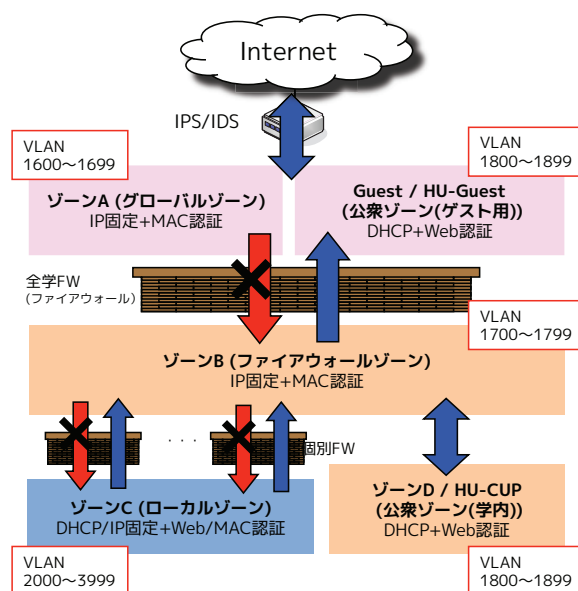


図 2 HINET で提供する主要ゾーン構成

開が前提となるサーバはゾーン A，複数のゾーン C やゾーン D から利用する可能性のあるプリンタや NAS 等の学内限定ホストはゾーン B に設置する形で運用している。なお，どのゾーンに接続する場合でも利用者には Web 認証または MAC アドレス認証のいずれから適用される。認証方式はゾーンにより異なるが，いずれの認証もフロアスイッチで行っている。

3.1.2 基幹サービス構成

図 4 に基幹サービス構成を示す。基幹サービスでは，Web 認証/MAC アドレス認証/シングルサインオン認証を担う認証サービス，DHCP サービス，ネットワーク構成管理サービス，ログ管理サービス，ネットワーク利用申請サービスの 5 つのサービスを 3 台の基幹サーバ装置に仮想化して動作させている。そのうえで，各サービス毎に二重化し

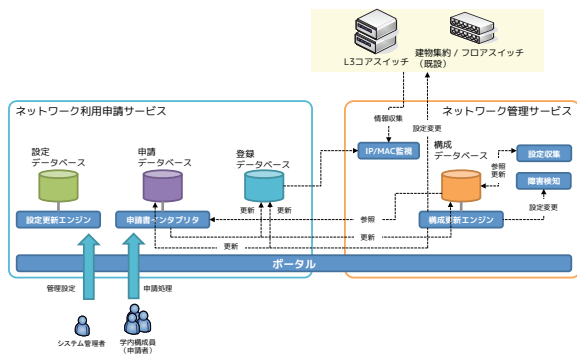


図 6 ネットワーク管理サービス/利用申請サービスのデータベース

ベースの情報を利用することで、エッジスイッチまでの接続関係をグラフで表現することができる。その一部を図7に示す。この有向グラフを利用することで、利用者からの申請に基づき、VLANのパスを追加・削除することが可能となる。

各スイッチのポートには { 上流, 下流, アクセス, 予約 } の4つの状態を保持できるようにし、上流/下流の場合は、それぞれの隣接するスイッチIDのポート情報をもつ。また、アクセスの場合は、ネットワーク利用申請でのコネクタID申請やゾーン申請によるアクセス用VLANの設定が可能な状態を意味する。

3.3 フロアスイッチの設定自動化

次に、図5のネットワーク利用申請サービスを利用して、構成員が申請を行った場合の設定自動化の手順について説明する。本稿では、割当済のコネクタIDに対して、新規でゾーンAホストを1台申請する場合を考える。なお、本システムでは利用するVLANはコアネットワーク装置から各キャンパス集約スイッチまでは事前に設定しており、設定自動化の対象としては主要3キャンパスの各キャンパス集約スイッチ配下のフロアスイッチ群に対して適用される。表1に2015年2月1日時点の自動化対象のスイッチの機器一覧を示す。

申請者は、システムを利用してコネクタIDと申請台数、ホストのMACアドレス等を入力し申請を行うと、VLANIDやIPアドレスなど設定情報が自動で割当てられる。VLANIDとコネクタIDが決まると、前節で述べた構成管理情報より、VLANが定義されるスイッチ(VLANパス)と機器を接続するポート(コネクタID)が把握できるため、VLANの設定および認証設定を自動で行っていく。現在の実装では、CLI(Command Line Interface)にて各スイッチに設定を投入するようになっている。また、設定日時を指定することも可能にしており、この場合は指定された日時までは保留状態となる。なお、設定の投入にあたっては複数種の機器を対象とする可能性があるため、機器の種類によって同種の変更内容であっても異なるコマンドを

実行しなければならない可能性がある。そのため、本システムでは、各機器で実行すべきコマンドのテンプレート定義ファイルを用意し、設定投入時には、更新対象スイッチの製品種別をキーとして、テンプレート定義ファイルから実行すべきコマンドのテンプレート文字列を取得し、投入コマンドの生成を行っている。

本システムを用いることで、ネットワーク利用単位をゾーニングにより細かな単位で柔軟に設定できるメリットを活かし、IPアドレスやVLANID等の資源の一元管理を行いつつ、構成員からの申請に基づき、エッジスイッチを含めたネットワーク構成の自動化が可能になる。

4. 実運用からみた効果と課題

本システムを導入した効果と課題について考察する。まず申請からVLAN設定完了までに要した時間について述べる。自動化導入後からこれまでに行われた申請からランダムに10件分を抽出し、処理時間の平均値を求めたところ、1件あたり1分27秒であった。比較のために、自動化導入以前の場合の時間を求めたところ、1件あたり25時間50分30秒であった。これは、構成員からの利用申請をWebインタフェースにて受付し、メディアセンター管理者によるチェックの後、ポートに対するVLANパス設定作業を契約する設定業者(外部委託)へアウトソーシングしていたケースである。この結果から大幅なリードタイムの短縮につながっていることがわかる。また日時指定の申請の場合でも、確実に指定された時間で設定が行われることになり、これまでに人手による作業によるコストがかかっていた部分を自動化により改善できたことも大きな成果である。

今後検討して行くべき点としては、申請・設定変更処理内容の把握がある。トラブル・障害時など利用者からの問い合わせに対して、設定処理に起因するものかどうかを調べるためには、設定内容を管理者自身で把握でき、後からでも容易に変更箇所を追従できるようにしておかなければならない。人手を介さず自動化することと管理をしないことはイコールにはならず、設定変更に関する情報を正確に把握・追従できることがより重要となると考えられる。

本システムは自動設定対象スイッチに対しCLIコマンド投入による設定を行っているため、ベンダ依存性及び機種依存性がある。コマンドのテンプレートを定義することで、依存性を吸収しているものの、常にテンプレートの保守が必要であるなどの課題がある。しかしながら、標準化されたSDNプロトコル対応スイッチによるネットワーク構築を行ったとしても、ベンダ依存の拡張機能を使っていたり、発展途上時にはプロトコルのバージョンアップが頻繁に実施されるため、結果的に機種依存となることがある。SDNプロトコルの開発が安定し、対応スイッチが低価格で安定的に供給されるようになるまでは、本提案方式の優位

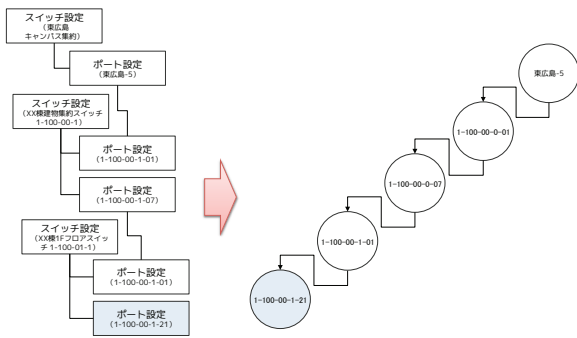


図 7 スイッチ接続構造のグラフ化

表 1 設定自動化対象のスイッチ一覧

スイッチ名称	製品種別	台数
東広島キャンパス集約	AX3830S-44X4QW	2 (スタック構成)
霞キャンパス集約	AX2530S-24S4X	2 (スタック構成)
東千田キャンパス集約	AX2530S-24S4X	2 (スタック構成)
建物集約スイッチ	AX2430S-24T	12
	AX2430S-48T	32
	AX2530S-48T	2
フロアスイッチ	AX2430S-24T	187
	AX2430S-48T	194
	AX2530S-24T	6
	AX2530S-48T	15

性は高い。

5. まとめ

本稿では、運用の効率化を目的としたネットワーク機器構成管理とスイッチの自動設定の取り組みについて述べた。ネットワークがインフラ化し、迅速かつ安定的なネットワーク提供が必須となる一方、人手によるネットワーク管理に対するコスト増が避けられなくなり、SDN 技術等を用いた新たなネットワーク運用管理が求められるようになってきている。広島大学では、2007 年度から IP アドレスや VLAN ID 等の資源の管理一元化をしながら、ネットワーク利用に関する手続きの整理・手順化を進めてきた。これまでの運用で手順を明確にできたことで、申請処理を機械化し、申請からネットワーク機器設定までを自動化するに至った。

自動化による効果として最も大きい点は迅速なサービス展開にある。HINET はコアネットワーク装置を集約し、キャンパス内は多数のレイヤ 2 ネットワークを利用者の申請に応じて設定している。この枠組を利用することで、SINET クラウドサービス^{*1} による商用クラウドのような外部サービスとのオンデマンド L2 接続を任意のフロアスイッチに設定することは、本自動化の仕組みを利用して通常の運用として容易に実現可能となる。今後は、外部サービスとのオンデマンド連携も視野に入れたより柔軟かつ迅速なネットワークサービス提供の基盤として有効性を検証

^{*1} http://www.sinet.ad.jp/service/other/cloud_services

していく。

謝辞 本キャンパスネットワークの構築および運用に尽力頂いている情報メディア教育研究センター、ネットワークシステムズ株式会社、株式会社プロキューブの関係者に感謝致します。

参考文献

- [1] 文部科学省, "教育研究の革新的な機能強化とイノベーション創出のための学術情報基盤整備について-クラウド時代の学術情報ネットワークの在り方-(審議まとめ)", 2014.
- [2] 須藤侑一, 佐藤聡, 櫻井孝一, 新城靖, "ネットワーク構成変更を追跡可能とするネットワーク管理支援システム", 情報処理学会研究報告 2013-IOT-20, pp.1-6, 2013.
- [3] 宮本貴朗, 田村武志, 鈴木亮司, 平岡大樹, 松尾英普, 泉正夫, 福永邦雄, "大規模ネットワークにおける VLAN 管理システム", 情報処理学会論文誌 41(12), pp.3234-3244, 2000.
- [4] 吉澤政洋, 沖田英樹, 上原敬太郎, 垂井俊明, "仮想ネットワークに関する文書作成を支援するネットワーク管理システムの実装および評価", 情報処理学会論文誌 52(3), pp.1334-1347, 2011.
- [5] 大東俊博, 近堂徹, 岸場清悟, 田島浩一, 岩田則和, 西村浩二, 相原玲二, "広島大学における新キャンパスネットワークへの移行手法", 情報処理学会研究報告 2008-IOT-3, pp.31-36, 2008.
- [6] 近堂徹, 田島浩一, 岸場清悟, 吉田朋彦, 岩田則和, 大東俊博, 西村浩二, 相原玲二, "クラウドコンピューティング活用のための大規模キャンパスネットワーク", 情報処理学会インターネットと運用技術シンポジウム (IOTS)2014 論文集, pp.101-108, 2014.