情報処理学会論文誌 Vol.57 No.3 998–1007 (Mar. 2016)

自動構成機能を有する大規模キャンパスネットワーク管理システムの実装と評価

近堂 徹[1,a)] 田島 浩一[1] 岸場 清悟[1] 岩田 則和[1] 相原 玲二[1]

受付日 2015年6月22日, 採録日 2015年12月7日

概要：ネットワークの利用形態が多様化・複雑化するなか，ネットワークをはじめとする情報基盤の運用管理の効率化が強く求められている．大学や企業等の大規模な組織では，管理対象となるネットワーク機器は増加し，複数の機器に対する設定が必要な場合は，異なる操作方法やコマンド体系を意識した設定変更が求められる．また，機器の設定状況が管理情報として正しく登録されていない場合，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．本論文では，大規模組織内ネットワークを対象とする構成管理機能とネットワークスイッチの自動設定機能を持つネットワーク管理システムの設計と実装について述べる．本システムは，ネットワークスイッチに対する設定内容を抽象化することでベンダや機種に依存しない制御を行い，利用者からの申請に基づいた設定の自動化を実現する．さらに，本システムを約 500 台のネットワークスイッチで構成する広島大学キャンパスネットワークに適用した際の実装内容と自動構成機能の動作結果について述べる．

キーワード：キャンパスネットワーク，ネットワーク構成管理，自動設定，運用技術，Software-Defined Networking

Implementation and Evaluation of a Management System for Large-scale Campus Networks Using Auto-configuration Functions

Tohru Kondo[1,a)] Koichi Tashima[1] Seigo Kishiba[1] Norikazu Iwata[1] Reiji Aibara[1]

Received: June 22, 2015, Accepted: December 7, 2015

Abstract: The growing diversity and complexity of computer networks has required the operational efficiency of network management. However, the amount of network devices that should be managed is increasing, and this has resulted in an increase in management costs due to control for each devices. To improve this issue, in this paper, we design the configuration management and automatic provisioning for the network services of large-scale LAN, and implement this method into network management systems. The proposed system can control networks automatically with no dependence on particular switches on the basis of the request of users. We show the effectiveness of the proposed method through its application to Hiroshima University's campus network system that consists of approximately 500 network switches.

Keywords: campus network, network management, auto configuration, operation technology, software-defined networking

1. はじめに

今日の情報化社会において，ICT 環境は社会的基盤の 1 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安全性と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り，柔軟性に優れたネットワーク基盤への要求が高まっている．

[1] 広島大学情報メディア教育研究センター
Information Media Center, Hiroshima University, Higashi-hiroshima, Hiroshima 739–8511, Japan
[a)] tkondo@hiroshima-u.ac.jp

一方，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，運用管理の効率化を進めていくことも重要な課題となっている．従来，ネットワーク管理者は，ネットワーク利用者からの要望に応じて随時ネットワーク機器の設定変更やトラブルシューティング等，ネットワーク全体の維持管理を行ってきた．管理対象の機器が増加し，複数の機器に対する設定が必要な場合は，異なる操作方法やコマンド体系を意識した設定変更が求められる．また，機器の設定状況が管理情報として正しく登録されていない場合，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．これらの課題を解決するために，SDN（Software-Defined Networking）の研究開発では，ネットワークをソフトウェアで一元的に管理し，設定の自動化が進められている [2], [3]．将来的には SDN による柔軟なネットワークの導入が進むことが予想されるが，その利点を活かすには SDN に対応したスイッチでネットワークを構成する必要があり，広く設置されているスイッチの全面的な更新には膨大な費用と時間を要する．

本論文では，大規模組織内ネットワークを対象とし，利用者からの申請に基づくネットワーク構成管理とスイッチの自動設定を行うネットワーク管理システムの設計と実装について述べる．本システムは，ネットワークスイッチに対する設定内容を抽象化することでベンダや機種に依存しない制御を行うとともに，利用者の申請からスイッチ設定までの処理フローを明確化することで設定の自動化を実現する．さらに，本システムを約 500 台のネットワークスイッチで構成する広島大学キャンパス情報ネットワークに適用した際の実装内容と自動構成機能の動作結果について述べる．

以下，2 章では，本論文が対象とするネットワークを定義し，管理運用における問題点を整理するとともに，関連研究についてまとめる．3 章では，2 章の検討をもとにネットワーク構成管理と自動構成手法について述べる．4 章ではキャンパスネットワークを例に本手法の実装とその評価について述べ，5 章で考察する．最後に 6 章でまとめを記す．

2. ネットワーク管理の背景

2.1 管理対象ネットワーク

対象とするネットワークは，研究グループ等の小規模ネットワークを多数接続して構成している，大学や研究機関の大規模ネットワークを想定している．研究グループや部署ごとに管理担当者（サブネット管理者とよばれることが多い）を置くこともあるが，本論文ではすべて「利用者」とよぶ．一方，ネットワーク全体を一元的に管理運用する担当者を「管理者」とよび，少人数の管理者による一元管理を前提とする．

図 1 に対象とするネットワーク構成を示す．図のように

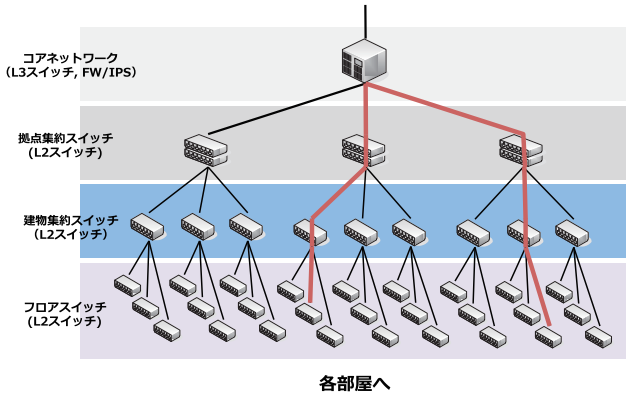

図 1 対象とするネットワーク構成
Fig. 1 Network configuration.

L3 機能（ファイアウォール機能を含むルータ等）を頂点とした多段スター型のスイッチ（L2 スイッチ）構成とし，L2 ループが存在しない構成とする．ただし，スタック接続等のクラスタリング技術により複数台のスイッチを仮想的に 1 台のスイッチとして構成することで，冗長構成をとることも可能である．管理方法の前提を以下に示す．

前提 1) 組織内すべての建物にネットワークが設置されており，500 台以上のネットワークスイッチ（約 15,000 ポート以上）により構成される．

前提 2) ルータ（L3 スイッチ）またはファイアウォールで区切られた小規模 LAN セグメントが 1,000 以上存在する．

前提 3) すべての LAN セグメントは組織内の任意の建物で利用される可能性がある．

前提 4) 利用者からの構成変更等に関する要求をオンライン申請により直接受け付ける．

2.2 運用管理の問題点

大規模ネットワークの構築および運用には，VLAN 技術を利用する方法が広く普及している．図 1 のネットワークにおいて，ある LAN セグメントを指定場所で利用するには赤線で示すような VLAN パスを設定する必要がある．具体的には以下の操作を行う．

- LAN セグメントに VLANID を割り当てる．
- 経由するスイッチを含め，関係するスイッチのポートへ VLAN を設定する．

これを，前提 1) および前提 2) のネットワークで実施すると，複数の機器に対する設定作業が発生する．また，大規模な組織になると組織の再編や活動拠点の追加，変更（削除を含む）等が日常的に発生するため，そのつど管理者の設定作業が発生する．これを管理者自身で実施すると，一定の確率でヒューマンエラーが発生する．さらに一度障害が発覚すると，その対応に多くの時間を費やすことになる．ヒューマンエラーを回避するためには，複数人での確

認体制を構築することが必要で，少ない人員で継続的に管理するのは困難である．広島大学での運用を例にとると，管理者を介した設定に 1 日以上を要することもあった [4]．

また，利用者からの設定要求に早期に対応するためスイッチ設定のみを行い，構成管理情報と不整合状態となる場合もある [5]．ネットワーク機器だけでなく IP アドレスや MAC アドレス等の情報管理も考えると，さらに複雑化する．構成管理や資源管理に関しては文献 [6], [7] 等でも取り組まれ，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，利用者からの申請に基づいた設定の自動化には至っていない．

2.3 関連研究

ネットワーク装置の設定に対する作業コストを軽減するため，各ネットワーク機器ベンダではネットワーク管理ソフトェアを提供しているケースが多い．これは，SNMP [8] や NETCONF [9] 等の標準プロトコルを用いた制御インタフェースやベンダ独自の API を提供し，GUI/GUI による操作を可能とするものである．しかしながら，これらの多くは特定のネットワーク機器に対する制御であり，ネットワーク全体を管理するためには別途フレームワークが必要となる．

ネットワーク全体を対象とした管理手法として，VLAN 等の資源管理機能を備えたソフトウェアによる統合ツール[*1]や VLAN 管理システム [10] が提案されている．文献 [10] では，複数スイッチによって構成される VLAN を一括管理するシステムを開発し，数十台のスイッチに対する制御を実現しているものである．これにより，VLAN 構成の整合性検証が可能となり，複雑な VLAN を構成する場合でも設定ミス等を事前に防げることが示されている．しかしながら，本管理システムは管理者が操作することが前提であり，利用者からの要求に応じて管理者が操作しなければならない点で課題が残る．

利用者および機器の ID や属性に応じて VLANID を切り替える動的 VLAN を用いたネットワーク構成も考えられる．しかしながら，動的 VLAN を利用する場合，VLAN 切替え処理を行う境界スイッチまで VLAN を事前に設定しておく必要がある．管理対象ネットワークの前提 1)〜3) を満たすには，すべてのスイッチを拠点集約スイッチと同等の性能を持つものにしておかなければならず，費用的課題が大きい．

近年，SDN 技術を活用したネットワークの集中管理・制御手法が提案されている [2], [3]．本論文では 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．SDN の利点は，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．SDN 技術には期待が高まっているが，その利用はデータセンタ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．本論文が対象とする大規模ネットワークにおいて，すべてのスイッチを SDN 対応に更新するには，費用以外にも課題が多い．たとえば，スイッチ管理の一元化や制御の集中化によるスケーラビリティの阻害，運用やトラブルシューティングに関するノウハウの不足等である．また，利用者からの設定要求を受け付けるシステムは別途構築しなければならない．

[*1] 株式会社イイガ，VLAN.Config（2015-6-10 参照），http://www.iiga.jp/solution/config/vlan.html

3. ネットワーク構成管理と自動設定手法

3.1 システムに求められる要件

本論文では，組織内ネットワークの構成管理およびスイッチ自動設定を可能とするシステムを設計するにあたり，以下の 3 点を要件として定める．

要件 1) スイッチのポート設定や VLANID 等の資源を一元的に管理し，利用者の要求（申請）に応じて割当てができること

要件 2) 利用者からの申請に対して，処理開始から 3 分以内で設定処理が完了するとともに，管理者が設定内容を把握できること

要件 3) ネットワークスイッチに対する操作内容を抽象化し，機種依存の操作手順をモジュール化することで，ネットワーク機器の機種に依存しない制御を実現できること

要件 1) は，資源割当ての自動化およびスイッチに対する設定投入時のミスを防ぐために必要である．スイッチ間の接続関係や各ポートの情報，また VLANID の割当てルールは管理者により定義し，たとえば身分や設定場所に応じた資源割当てができなければならない．要件 2) は，1 つの申請に対する処理時間を定めたものである．広島大学における 2013 年度のネットワーク運用において，1 カ月間の処理依頼件数の最大値は 442 件（2013 年 9 月）であり，これは 1 日平均 14.7 件である．仮に 1 日の依頼を 20 件とし，それが集中した場合でも 1 時間以内で処理が完了することを目標に定め，1 つの申請あたり 3 分以内と設定した．なお，エラー等により設定が正常に完了しない場合には管理者による手動設定に移行することとする．一方，利用者からの問合せ等のために，申請内容および機器への設定変更内容は管理者がいつでも参照できなければならない．このためには，権限に基づくロール設定とそれをもとにした申請，承認フローが必要となる．要件 3) は，ネットワークスイッチに対する設定内容（VLAN 追加，VLAN 削除，ウェブ認証設定，MAC アドレス認証設定）と操作内容を，

表 1 設定内容の抽象化の例（VLAN 追加の場合）
Table 1 Example of configuration abstraction (In the case of VLAN addition).

設定内容 [引数]	操作内容 [引数]	コマンド展開例
VLAN 追加	ログイン [IPaddr]	ssh -l user [IPaddr]
[IPaddr, Port, VLANID, Description]	特権モード移行	enable
	コンフィグモード移行	configure terminal
	VLAN 定義追加 [VLANID]	vlan [VLANID] name ”VLAN[VLANID]”
	インタフェース指定 [port]	interface gigabitethernet [Port]
	VLAN 設定 [VLANID] (アクセスポートの場合)	switchport access vlan [VLANID]
	VLAN 設定 [VLANID] (タグ VLAN の場合)	switchport trunk allowed vlan add [VLANID]
	説明文更新	description ”[Description]”
	ログアウト	save exit

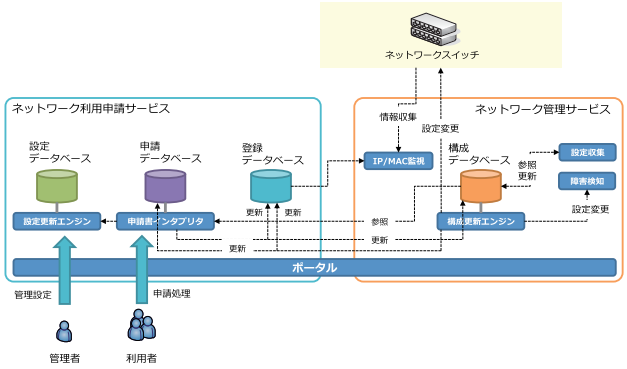

図 2 システム概要
Fig. 2 System configuration.

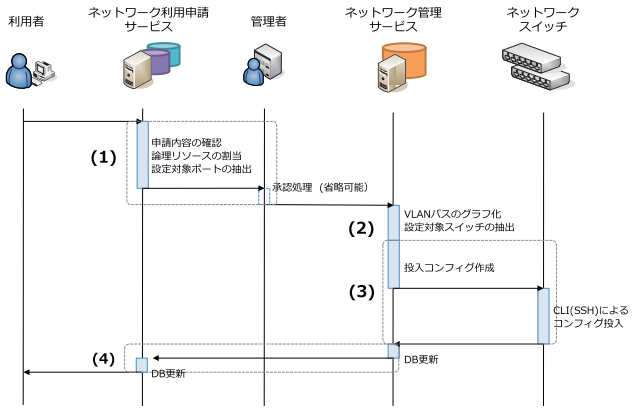

図 3 申請および設定処理の流れ
Fig. 3 Application and configuration procedures.

スイッチの機種に依存しないように抽象化する．**表 1** に VLAN 追加における抽象化の例を示す．このように設定に対する操作内容を定義し，ネットワーク機器に対して設定を行う際には，抽象化した操作内容から各機種のフォーマットに従ったコマンドラインへ展開する．これは，ネットワークをすべて単一ベンダ機器，単一機種で揃えるのは困難であるため必要である．

これらの要件を満たすことで汎用性のあるシステム構築が可能になると考えらえれる．

3.2 管理システム設計

3.2.1 概要

図 2 にシステム概要図を示す．本システムは，ネットワーク利用申請サービスとネットワーク管理サービスの 2 つのサービスから構成される．

ネットワーク利用申請サービスでは，各種申請状況を管理する申請データベース，申請により割り当てられた IP アドレスや VLANID 等の資源情報（以下，論理リソース）を管理する登録データベース，システム利用者のロール設定を管理する設定データベースを有する．これらのデータベースに対して申請書インタプリタや設定更新エンジンを実装することで，申請に基づく情報更新や登録内容の参照が行われる．ネットワーク管理サービスでは，申請・登録された情報から生成されるネットワーク構成を管理する構成データベースを有し，構成更新エンジンを実装することで申請に基づいたネットワーク構成の更新が行われ，スイッチへの設定反映が行われる．このように，申請処理と設定処理を独立した異なるサービスで提供し，両サービスが連携して動作する設計としている．

また，両サービスと制御対象のネットワークスイッチは，一般用途のネットワークとは異なる VLAN の制御用ネットワークで接続され，このネットワークを介して管理，設定を行う．

申請から設定までの処理の流れを**図 3** に示す．なお，本システムでは，複数の設定処理が同時に動作することによるネットワークスイッチへの重複設定を避けるために，ネットワーク利用申請サービスでキューによる設定処理の排他制御を行う．次項以降で手順に従い，申請に対する処理内容を述べる．

3.2.2 利用申請と資源割当て：区間（1）

ネットワーク利用申請サービスは，まずログイン時にシステム利用者（利用者および管理者）の権限設定に基づき，申請の可否を判断する．これはシングルサインオンによる

表 2 スイッチ設定のテーブル構造
Table 2 Table structure of switch configuration.

属性	名称	型	出現回数	内容
swichID	スイッチ ID	文字列	1	スイッチを一意に表す ID
ipAddress	管理 IP アドレス	IPv4 アドレス	1	管理用の IP アドレス
productType	製品種別	文字列	1	スイッチの製品型番
serial	シリアル番号	文字列	1	該当スイッチの個体を一意に表す文字列
switchType	スイッチ種別	文字列	1	スイッチの種別 (階層) [campus, building, floor]
location	設置場所	文字列	1	スイッチの設置場所
autoConfiguration	自動設定変更対象フラグ	ブール	1	自動設定変更対象を表すフラグ
connectorID	コネクタ ID	文字列	0..*	該当スイッチが保持するポートの ID
vlanId	VLAN ID	数値	0..*	該当スイッチで利用可能な VLAN

表 3 ポート設定のテーブル構造
Table 3 Table structure of port configuration.

属性	名称	型	出現回数	内容
connectorID	コネクタ ID	文字列	1	該当スイッチが保持するポートの ID
swichID	スイッチ ID	文字列	1	該当ポートが所属するスイッチ ID
port	ポート番号	文字列	1	該当コネクタ ID が示すポート
vlanId	VLAN ID	数値	0..*	該当のポートで利用可能な VLAN
tagVlanEnabled	タグ VLAN 使用フラグ	ブール	1	該当ポートでタグ VLAN を利用するかを表す
status	利用状態	文字列	1	ポートの利用状態 [上流, 下流, アクセス, 予約]
neighborConnectorID	隣接コネクタ ID	文字列	0..1	隣接するコネクタ ID

認証・認可機能の利用を前提とする．利用者は VLANID と設定対象となるスイッチのポート情報，およびタグ VLAN 利用の有無をパラメータとして申請を行う．このとき，利用者はネットワーク構成を意識することはなく，ネットワーク機器を直接接続するエッジスイッチのアクセスポートのみを指定すればよい．なお，VLANID の割当てルールについてはシステム内で管理者が定義する必要があるため，ここではルールを定義できる機能のみを提供し，割当てルールについては言及しない[*2]．申請書インタプリタでは，与えられたパラメータをもとに申請データベースと登録データベース内の論理リソースの情報更新を行う．本システムでは，新規の論理リソース割当てに対して管理者の承認処理を行うが，割当てルールや利用状況に応じて承認フローを省略（自動承認）することも可能である．

3.2.3 ネットワーク構成管理：区間（2）

ネットワーク管理サービス内の構成更新エンジンでは，ネットワーク利用申請サービスの申請書インタプリタから引き継ぐ形で処理が行われる．構成データベースでは，スイッチ設定とポート設定の情報から，各スイッチの識別子やポート情報，隣接関係，スイッチ種別，管理用 IP アドレス，製品種別等を保持する．スイッチ設定とポート設定のデータ構造例を**表 2**，**表 3** に示す．なお，本データ構造は VLAN 設定に必要な項目のみを列挙しており，たとえばスイッチでの認証機能等を利用する場合にはこれらの情報を追加することも可能である．本システムは，図 1 に示すスター型のネットワークを対象としているため，構成データベースの情報を利用することでスイッチ間の接続関係をグラフで表現する．生成するスイッチ間接続の有向グラフ例を**図 4** に示す．この有向グラフを利用することで，利用者が申請したスイッチのアクセスポートから最上位のスイッチまでの VLAN パスを探索し，制御対象スイッチを抽出することができる．

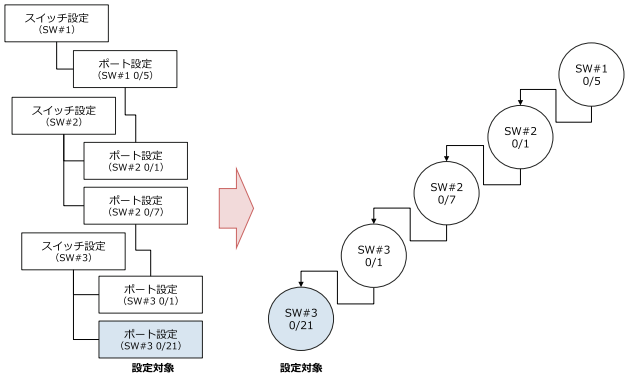

図 4 スイッチ間接続の有向グラフ化
Fig. 4 Directed graph for connecting switches.

各ポート設定には [上流, 下流, アクセス, 予約] の 4 つの状態を保持するようにし，上流/下流の場合は，それぞれの隣接するスイッチのポート情報を持つ．また，アクセスの場合は，本システムでの VLAN 設定が可能な状態を意味する．

なお，建物の更新により，スイッチ ID およびそれに紐づくコネクタ ID が変更になる場合，管理者がネットワー

[*2] 広島大学における運用例を 4 章で述べる．

図 5　ネットワーク利用申請サービスの画面
Fig. 5　Display of network application service.

ク利用申請サービスおよびネットワーク管理サービスの各データベースの更新を行う．更新はウェブブラウザによるGUI で行い，表 2 および表 3 で示す各フィールドの書き換えが行われる．

3.2.4　スイッチ自動設定：区間（3）

前述のネットワーク構成データベースから制御対象となるスイッチを抽出することができるため，対象のスイッチに対して，順次スイッチ設定処理を実行する．スイッチ設定の実行途中でエラーを検出した場合には，その時点で処理を中断し，管理者に対して通知を行い，手動での設定を行う．なお，ツリー構造のリーフのスイッチ（エッジスイッチ）のアクセスポートに対しては申請をもとに Tagged/Untagged のいずれかの設定が行われるが，エッジスイッチから上流のポートは Tagged で VLAN 追加を行う．

本システムではスイッチへの設定についてはコマンドラインインタフェース（CLI）による設定投入を行う．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，同種の変更内容であっても機器の種類によって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（コンフィグファイル）の生成を行う．自動設定の終了後，処理結果に応じて構成情報をデータベースへ保存する．

4.　実運用ネットワークへの適用と評価

前章で設計したシステムをベースに，広島大学では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，以下 HINET）を 2014 年 8 月より運用している [11]．本章では，HINET における導入，

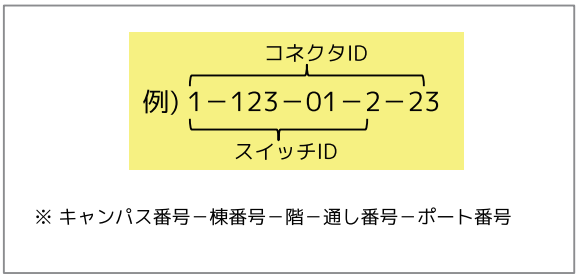

図 6　コネクタ ID の例
Fig. 6　Example of connector ID.

適用とその評価について述べる．

4.1　広島大学キャンパスネットワーク HINET2014

4.1.1　概要

まず本システムの導入規模を示すために，キャンパスネットワークの概要について説明する．HINET は主要 3 キャンパス（東広島，霞，東千田）および附属学校，呉・竹原等の小規模遠隔部局に整備されており，データセンタに設置するコアネットワーク装置を最上位に，図 1 に示したようなスター型のネットワークとなっている．また，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 500 台のスイッチの各ポートの設定までを一元管理している．管理対象ポート数は約 18,000 ポートとなる．

HINET では各アクセスポートには，**図 6** に示すコネクタ ID とよぶ識別番号（ラベル）を情報コンセントに対応する形で割り当てている．コネクタ ID はスイッチに割り当てられたスイッチ ID と物理ポート番号の連結によって表現されており，スイッチ ID はスイッチが設置されている物理的な位置情報から一意に決められる．スイッチ ID およびコネクタ ID は表 2，表 3 で示した構成データベース内の各属性値に対応付けられる．

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 7** にゾーンの概要と各ゾーンで利用する VLANID の範囲を示す．利用者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．ゾーンのアクセス制限は全学ファイアウォールおよび個別ファイアウォールをコアネットワーク装置で一元的に提供する．各ゾーンで利用する VLANID の範囲を一元的に定義，管理することで，利用者からの申請により VLANID の自動割当てを可能にしている．2015 年 6 月時点で，自動割当て対象の VLAN 約 2,000 のうち約 1,200 が使用中である．

4.1.2　自動設定機能の導入

図 8 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，ログ管理サービス，本システム（ネットワーク利用申請サービス，ネットワーク管理サービス）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，各サービスごとに二重化して異なる筐体に分散配置することにより負荷分散と耐障害性を向上させている．

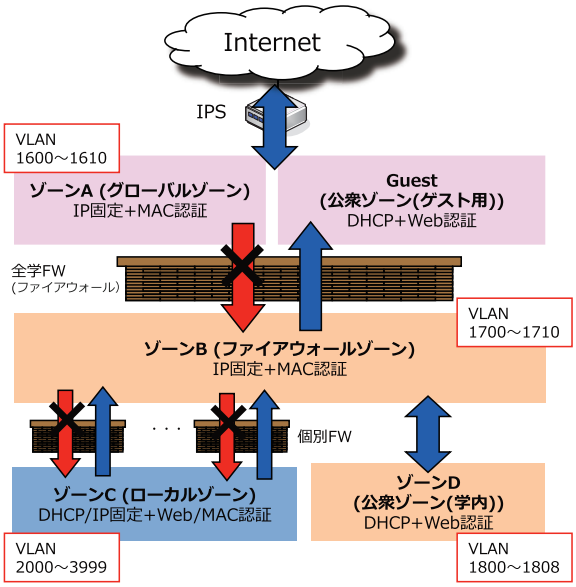

図 7　HINET で提供する主要ゾーン構成
Fig. 7　Configuration of HINET's zone.

次に，申請権限を有する利用者が本システムを利用して申請を行う場合の設定自動化の手順について説明する．本論文では，あるコネクタ ID をゾーン C（特定の VLANID）に所属させる場合を考える．なお HINET 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事前に設定しており，設定自動化の対象としては各キャンパス集約スイッチ配下の建物集約・フロアスイッチ群に対して適用される．建物集約・フロアスイッチは最大でも 3 階層以内で到達するように構成している．

利用者は，ウェブインタフェースを利用して，コネクタ ID 等の必要な情報を入力し申請を行うと，VLANID 等の論理リソースの割当てが行われる．HINET では，4.1.1 項で示したとおり，VLANID を一元的に管理しているため，現時点では管理者の承認は不要とし，自動処理を行っている．VLANID とコネクタ ID が決まると，前章で述べたネットワーク構成管理情報より，VLAN を定義するスイッチ（VLAN パス）と利用するポート（コネクタ ID）が把握できるため，スイッチの設定を自動で行っていく．なお，HINET では L2 スイッチの機能を利用して，すべてのアクセスポートで Web 認証もしくは MAC アドレス認証による利用者認証を行っている．したがって，本システムでは VLAN の設定に加えて認証設定も同時に行われる．また，設定日時を指定することも可能で，この場合は指定された日時までは設定保留状態となる．500 台のスイッチのうち，自動設定対象スイッチは約 450 台（2015 年 6 月時点）であり，内訳を**表 4** に示す．また，本システムの主な申請処理実績を**表 5** に示す．

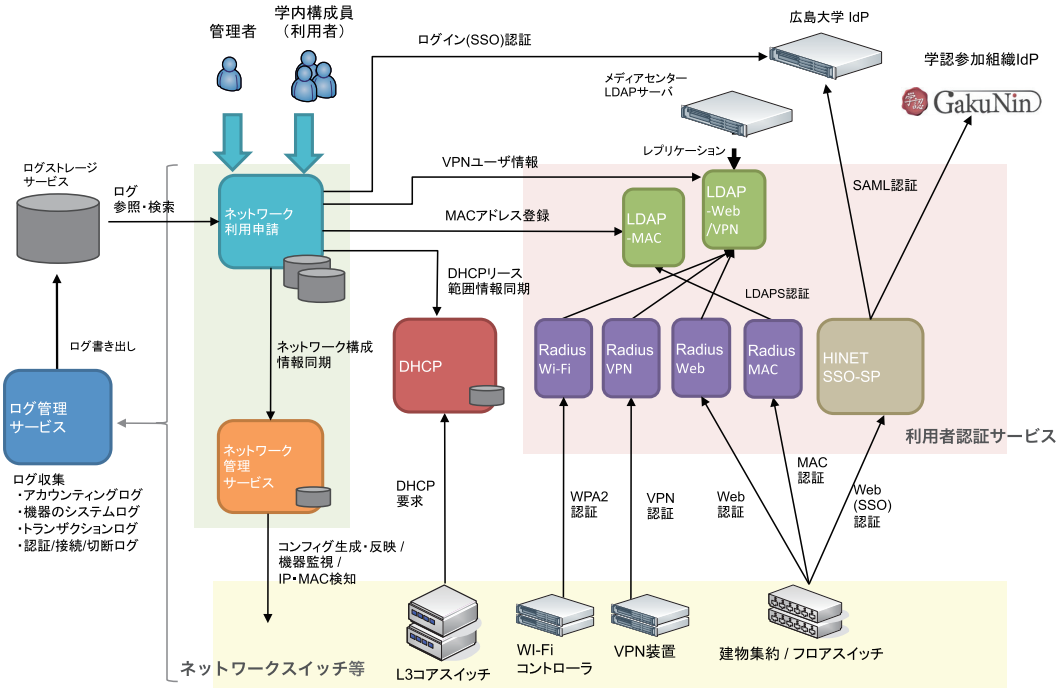

図 8　基幹サービス構成
Fig. 8　Configuration of HINET servers.

表 4 設定自動化対象のスイッチ一覧
Table 4 Auto configuration supported network switches.

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

表 5 申請処理数（2014 年 10 月 1 日～2015 年 5 月 31 日）
Table 5 The number of transactions for application processing (From Oct. 2014 to May 2015).

申請内容	申請処理数
コネクタ ID 申請	116
ゾーン A 申請	53
ゾーン B 申請	46
ゾーン C 申請	365
ゾーン D 申請	9

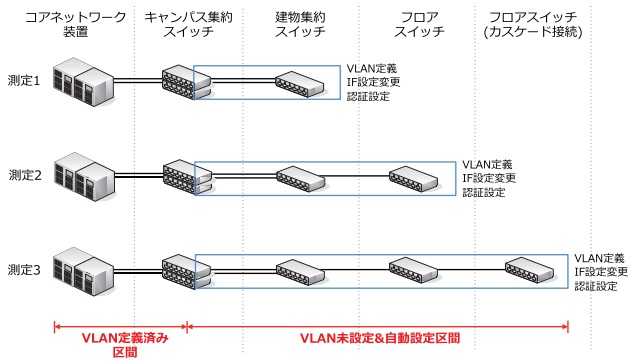

図 9 評価実験の構成
Fig. 9 Configuration of evaluation experiment.

4.2 評価実験

実際に運用中のシステムを用いて，単一の設定処理に要する時間について測定し，3.1 節で示した要件 2) について評価を行った．実験では，**図 9** の枠線で示すとおり，コアネットワーク装置からの深さが異なるスイッチのアクセスポートに対する，申請から設定完了までの時間と各処理の内訳について計測した．設定内容は，VLAN パス設定（追加，削除）に加え，アクセスポートに対する認証設定（Web 認証，MAC アドレス認証併用）となっている．

計測結果を**表 6** に示す．各測定は 3 回の平均値を代表値として記している．なお，測定区間は図 3 における各区間を表している．この結果から，若干のばらつきはあるものの，設定追加と設定削除の場合で設定時間に大きな差異はないことが確認できた．ばらつきの原因としては，申請

表 6 計測結果（単位：秒）
Table 6 Measurement results (Unit: sec).

測定項目		測定区間 (1)	(2)	(3)	(4)	合計
測定 1	設定追加	22.42	10.52	54.71	0.43	88.06
	設定削除	20.73	11.22	54.37	0.36	86.69
測定 2	設定追加	23.81	11.68	66.15	0.52	102.17
	設定削除	23.37	10.82	62.97	0.48	97.64
測定 3	設定追加	23.30	11.80	76.45	0.39	111.94
	設定削除	23.10	11.83	73.54	0.36	108.82

書インタプリタや設定構成エンジンの処理におけるデータベース検索や VLAN パスの有向グラフの生成処理で処理時間に差が生じたためと考えられる．

設定追加の結果に着目すると，設定対象となるスイッチの台数に応じて所要時間が増加し，1 台の追加に対して 10 秒から 15 秒の時間増となっており，区間（3）の時間が増加している．これはコンフィグファイル生成と投入に要する時間であるため，妥当な結果であるといえる．この結果から，設定対象が 4 台に及ぶ場合でも，本システムでは申請から設定完了まで 110 秒で自動設定処理が実現できていることが分かる．

5. 考察

本システムの運用を通して，提案手法の効果と課題について考察する．

3.1 節で，ネットワーク構成管理と自動設定を実現するためにシステムに求められる要件についてまとめた．ここでは，本システムにおける実現方法について述べる．要件 1) については，ネットワーク利用申請サービスにより，VLANID や IP アドレス，スイッチのポート情報等の資源を一元管理し，利用者の権限をもとに申請可否を判断する機構を導入した．要件 2) については，4.2 節の評価実験から，1 つの申請に対する設定を処理開始から 3 分以内で実現しながらも，利用者や管理者が申請データベース内の申請履歴を閲覧できるユーザインタフェースを提供している．また，必要に応じて承認フロー機能も付与している．要件 3) については，ネットワーク管理サービスの構成変更エンジンでコマンドテンプレートを定義したコンフィグ生成を実現している．以上のことより，目的を達成するためのシステム構築および運用が実現できているといえる．

一方，設定処理中に新たな申請が行われた場合には，システムの排他制御により，システム内のキューによる待ち状態となる．また，スイッチ設定の実行途中でエラーを検出した場合は，その時点で処理を中断し，ネットワーク管理者に対して通知を行い，管理者による手動設定を必要とする．具体的には以下の場合が該当する．

- 登録データベース，構成データベースの情報とネットワークスイッチの設定に不一致がある場合

- 途中のスイッチを含む設定対象のスイッチが停止している場合

これらは意図しない VLAN 設定や自動設定エラーによる通信断等の副次的な障害発生のリスクを軽減するためにも必要な処理であると考えている．

次に，本システムの適用範囲について述べる．4 章では広島大学での適用例を示したが，本システムは 2.1 節で示した管理対象ネットワークへの適用を前提としたシステム設計を行っている．図 1 で示したネットワーク構成で，かつ VLANID やスイッチのポート情報等の論理リソースを一元管理できるネットワークであれば適用が可能であり，ネットワーク機器のベンダや機種に依存しない汎用性のある制御が実現できると考えられる．

提案手法の課題について述べる．1 つ目にリソースの厳密な管理の必要性がある．本手法は，従来の運用で VLAN が部署ごとに独自管理されている場合やネットワーク機器の管理が分散している場合は，これらを集約し一元化したうえでの管理が前提となる．2 つ目に VLAN 数の制約がある．IEEE802.1Q の仕様上 VLANID は 12 ビットに制限されるため，理論上で最大 4,094 までの数にしか対応できない．4 章で示した本学の適用例では実用上問題のない範囲で運用可能となっているが，より大規模な組織やより細かいネットワーク構成を採用する場合は問題となる可能性がある．しかしながら今後，ネットワーク機器への VXLAN [12] の普及により，利用できる ID 範囲が拡大した場合には，システム側による対応で回避できると考えられる．3 つ目に多種多様なスイッチへの対応がある．本システムは，自動設定対象スイッチに対し，SSH で接続して CLI コマンド投入による設定を行っているため，ベンダ依存性およ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，異なるファームウェアで動作する複数機種への対応を実運用で確認できているものの，機種の追加に応じたテンプレートの保守等の課題は残る．ただし，管理者自身によるネットワーク機器の設定作業と比較すると，その作業コストは十分に小さいと考えられる．

6. まとめ

本論文では，大規模キャンパスネットワークの組織内 LAN を対象とした，一元的なネットワーク構成管理とネットワーク自動設定について述べた．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，運用管理の効率化を進めていくことも重要な課題となっている．このような課題に対して，本論文では，ネットワークスイッチに対する設定内容を抽象化することで機種に依存しない制御を行い，利用者からの申請に基づいた設定の自動化を実現した．実運用ネットワークに対する実装および評価実験から，システム要件として定めた，申請あたり処理開始から 3 分以内での設定が可能であることも示した．

今後の課題としては，商用クラウドサービスや学外サービス等の対外サービスとの連携により，柔軟でかつ迅速なネットワークサービス提供の基盤として活用していくことを検討している．

謝辞 本システムの研究開発に全面的なご協力をいただいた，東海大学情報通信学部の大東俊博氏，広島大学情報メディア教育研究センターの西村浩二氏，吉田朋彦氏に深謝いたします．また日々の運用にご尽力いただいている情報メディア教育研究センター，ネットワンシステムズ株式会社，株式会社プロキューブの関係者各位に感謝いたします．

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 (2014).
[2] Kim, H. and Feamster, N.: Improving Network Management with Software Defined Networking, *IEEE Communication Magazine*, Vol.51, No.2, pp.114–119 (2013).
[3] 岡部寿男，津崎善晴，新 麗，林 達也：ネットワーク仕様定義による広域分散ネットワークの運用管理，信学技報，IA2013-59, pp.13–18 (2013).
[4] 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).
[5] 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).
[6] 新 麗，二宮 恵，加藤雅彦：ネットワークシステム管理のための構成情報データモデルの設計，信学技報，IA2008-45, pp.25–30 (2008).
[7] 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，Vol.52, No.3, pp.1334–1347 (2011).
[8] Case, J., Fedor, M., Schoffstall, M. and Davin, J.: Simple Network Management Protocol (SNMP), RFC1157 (1990).
[9] Enn, R., Bjorklund, M., Schoenwaelder, J. and Bierman, A.: Network Configuration Protocol (NETCONF), RFC6241 (2011).
[10] 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，Vol.41, No.12, pp.3234–3244 (2000).
[11] 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).
[12] Mahalingam, M., Dutt, D., Duda, K., Agarwal, P., Kreeger, L., Sridhar, T., Bursell, M. and Wright, C.: Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks, RFC7438 (2014).

近堂 徹 （正会員）

2001 年広島大学工学部第二類（電気系）卒業．2006 年同大学大学院工学研究科博士課程修了．現在，広島大学情報メディア教育研究センター准教授．博士（工学）．コンピュータネットワーク，リアルタイムマルチメディア通信，仮想化技術に関する研究に従事．電子情報通信学会会員．

田島 浩一 （正会員）

1994 年宮崎大学工学部電子工学科卒業．2000 年同大学大学院工学研究科博士課程後期修了．現在，広島大学情報メディア教育研究センター助教．博士（工学）．コンピュータネットワークの管理に関する研究に従事．電気学会会員．

岸場 清悟 （正会員）

1988 年京都大学理学部卒業．1994 年同大学大学院理学研究科博士後期課程単位取得退学．現在，広島大学情報メディア教育研究センター助教．京都大学博士（理学）．情報システム運用，システム評価，コンピュータネットワークに関する研究に従事．日本物理学会，日本流体力学会各会員．

岩田 則和

1984 年広島大学理学部物性学科卒業．現在，広島大学情報メディア教育研究センター講師．医療情報の 2 次利用に関する研究，システム運用に関する研究に従事．日本医療・病院管理学会，日本医療情報処理学会各会員．

相原 玲二 （正会員）

1981 年広島大学工学部第二類（電気系）卒業．1986 年同大学大学院工学研究科博士課程後期修了．同大学助手，同大学集積化システム研究センター助教授を経て，現在，同大学情報メディア教育研究センター教授．工学博士．コンピュータネットワークに関する研究に従事．電子情報通信学会，IEEE Communications Society 各会員．