D6-3

名工大における大規模ダイナミック VLAN ネットワークの管理・運用

打矢 隆弘, 松井 俊浩, 齋藤 彰一, 山本 大介, 内匠 逸, 松尾 啓志

名古屋工業大学　情報基盤センター

t-uchiya@nitech.ac.jp

概要：名古屋工業大学では 2010 年 4 月から 2 万台の端末認証が可能なダイナミック VLAN ネットワーク：新 MAINS(Meikoudai Advanced Information Network System)を稼働している．新 MAINS ではネットワーク機器更新と各種システム開発により利便性・可用性の向上，セキュリティと利便性の両立，およびユビキタス環境の充実を実現した．本稿では，新 MAINS におけるネットワーク運用実績や利用状況の推移について報告する．

1　はじめに

約6,700人の学生・院生と550人の教職員が所属する名古屋工業大学では，これまで1万台を超える大規模ダイナミックVLANネットワーク(MAINS: Meikoudai Advanced Information Network System)を運用し，MACアドレスベースの端末認証手法や管理・運用方式に関する多数のノウハウを蓄積してきた．また，2010年3月末にネットワーク機器を更新し，可用性，信頼性，保守容易性，安全性，利便性をさらに向上させたネットワークシステムとして，新MAINSを稼働している．本稿では，2011年10月時点の新MAINSの構成，本学で開発したシステム，及び，新MAINSにおけるネットワーク運用実績や利用状況の推移について報告する．

2　新 MAINS の導入

2.1 旧 MAINS の問題点

旧 MAINS では MAC アドレス認証によるダイナミック VLAN を使ったネットワーク(図 1)を構築していた．このネットワークでは，サブネット作成時にサブネットと VLAN の紐付けをネットワーク管理者が設定している．その後，端末利用者が MAC アドレスの登録作業により MAC アドレスとサブネットを一度紐付けするだけで，以降は大学内のどの建物でその端末を情報コンセントに接続しても，紐付けしたサブネットの端末として自動的に認識され，場所を問わずに研究室サブネットのリソースを利用できる．

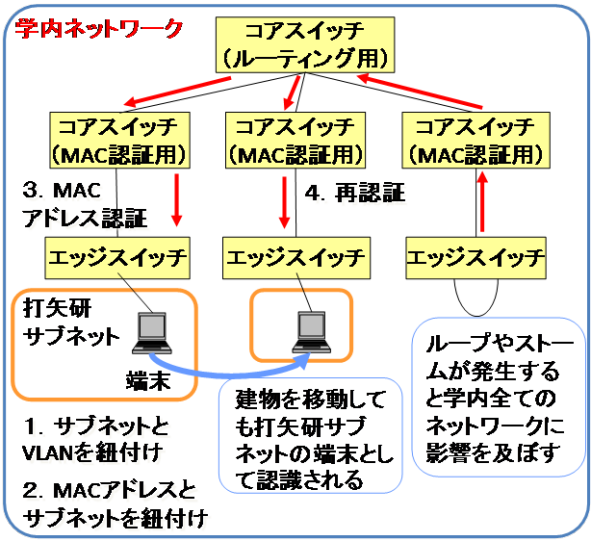

図 1：旧 MAINS の MAC アドレスベース ダイナミック VLAN

この利便性の一方で，教職員・学生の不注意によるケーブル誤接続に伴うネットワークループや，持ち込み PC からのウイルス攻撃によるトラフィックの急激な増加が発生すると，学内ネットワークが全てダウンしており，学内の教育・研究活動に大きな支障をきたしていた．また，SSH 経由の外部からの侵入，研究室無線 LAN 基地局の安易な設置によるセキュリティ低下，電波混信による性能低下が発生していた．さらに，個々の端末毎のセキュリティポリシの設定が不可能，P2P ファイル交換ソフトの利用制限やアプリケーションレベルでのフィルタリングができないなどのセキュリティ上の課題もあった．

そこで，これらの問題点を解決する新しいネットワークシステムとして，新 MAINS を導入した．

2.2 新 MAINS の概要(2011 年 10 月時点)

新 MAINS は旧 MAINS 最大の特徴である MAC アドレスベースのダイナミック VLAN を継承するとともに以下の改善を行ったネットワークである.

1. 可用性の向上

エッジスイッチによる L2 ループ検知機能を用い，スイッチ配下の HUB でループ構成になった場合にポートのシャットダウンにより障害影響範囲の局所化を図る．またエッジスイッチのストームコントロール機能を用い，ポート毎にパケットの流量を監視し，ストームが発生した場合に当該トラフィックを廃棄する．これらの機能により，ループやストーム発生時のネットワーク全体のダウンを防ぐことに成功した.

2. 通信速度の向上

中央スイッチと各建物・フロアのエッジスイッチの回線を 100Mbps から 1Gbps に増速した．無線 LAN も IEEE11n 方式により最大 300Mbps に対応した．さらに透過型 WEB プロキシを導入することで WEB の閲覧速度を向上した．加えて，2011 年 3 月に SINET3 から SINET4 に移行し，対外接続を従来の 1Gbps から 10Gbps に増速し対外向けの通信速度を向上した.

3. セキュリティと利便性の両立

統合脅威管理機器(UTM)を用い，セキュリティポリシを IP アドレス・ポート毎に設定可能とした．これにより学外に公開しなければならないサーバ群を最小限にしている．また，異常検知や外部攻撃の自動遮断を行う侵入防止システム, WEB サイトや P2P ファイル交換を遮断するアプリケーションレベルのフィルタリング機能も導入した.

端末の認証関連では，従来の端末認証方式である MAC アドレス認証に加え， エッジスイッチによる WEB 認証を新たに導入した．これにより，端末の MAC アドレス登録作業無しに学内認証アカウントである基盤 ID で利用端末をネットワークに接続できる．さらに, WEB 認証時でも研究室の VLAN に接続可能な，利便性の高い環境を構築した.

4. ユビキタス環境の充実

2.4GHz/5GHz 対応，かつ IEEE802.11 a/b/g/n に対応した無線 LAN アクセスポイント(以降，無線 AP)を 400 台以上設置し，学内ほぼ全ての場所で高速にインターネットにアクセス可能な学内ユビキタス環境を実現した.

また学外者の無線 LAN 利用のため，ゲスト用無線 LAN アカウント発行システムを開発した．加えて，2011 年 3 月に国際無線 LAN ローミング基盤(eduroam)に参加した．これにより，学外者が所属機関のアカウントを用いてユーザ認証を行い, 無線 LAN を利用できる環境が整いつつある.

なお，本学では無線 AP への接続ログを常時保存しており，紛失したモバイル端末の早期発見や各無線 AP の利用状況の把握に活用している.

2.3 導入機器一覧

導入した機器は以下の通りである．また，図 2 に新 MAINS のネットワーク構成を示す.

- 中央スイッチ L3 AlaxalA AX6708S 1 台
- サーバスイッチ, 集約スイッチ, エッジスイッチ: L2 AlaxalA AX3640S 120 台 (MAC 認証, WEB 認証, IEEE802.1X 認証対応, ループ検知やストームコントロール機能を備え，1 台あたり 1000 端末の同時認証／ダイナミック VLAN が利用可能)
- 無線 AP: HP ProCurve MSM422 Access Point 400 台
- 無線 AP Controller: HP ProCurve MSM760 Access Controller 3 台
- UTM(Firewall, IPS): Fortigate3810A 2 台(IP アドレス単位のポリシ設定やアプリケーションレベルフィルタリングが可能)
- HP BladeSystem c7000: (mail サーバ, mail gateway サーバ, traffic capture サーバ, DNS/DHCP サーバ, SNMP サーバ, MAINS データベースサーバ, RADIUS サーバ) 1 台
- SIP サーバ, VPN コンセントレータ

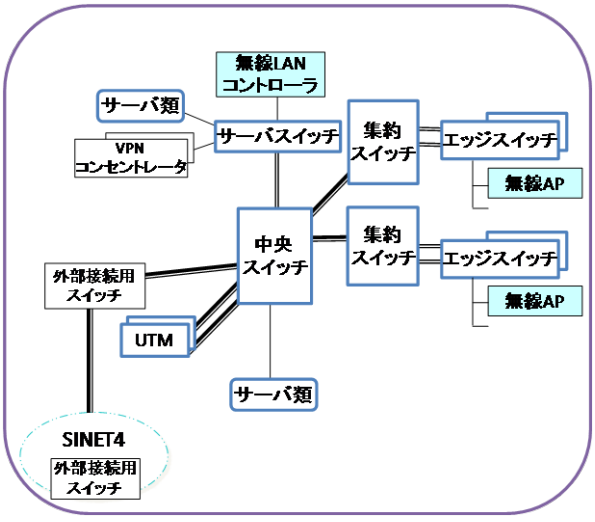

図 2：新 MAINS のネットワーク構成

3 本学で開発したシステム

3.1 MAINS データベース

MACアドレス認証では，事前に利用端末のMACアドレスを**MAINSデータベース**(図3)に登録する方式を用いている．MAINSデータベースでは，サブネットとVLANの紐付け情報や，MACアドレスとサブネットの紐付け情報が管理されている．

図3：MAINSデータベースの端末登録画面

3.2 WEB 認証時の接続先 VLAN 設定システム

VLANネットワークにおいてWEB認証を実現する場合，認証後の接続先VLANを任意に変更できることは利用者の利便性向上に大きく寄与する．本学では，利用者毎に接続先VLANを「WEB認証既定VLAN」または「研究室VLAN」のどちらかに変更可能なシステム(図4)を開発した．これにより，「研究室VLAN」が接続先に設定されていれば，WEB認証時でも認証成功後に研究室のプリンタ・共有フォルダなどのリソースが活用できる．

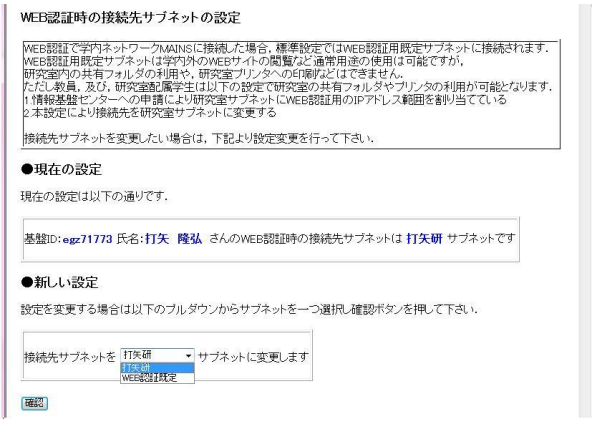

図4：WEB認証時接続先VLANの設定画面

3.3 学外公開ホスト参照システム

利用者は，本システムを用いて自身が学外に公開しているWebサーバ，SSHサーバ等の外部公開用サーバの設定状況を参照できる(図5)．開放しているポートの一覧も確認可能である．

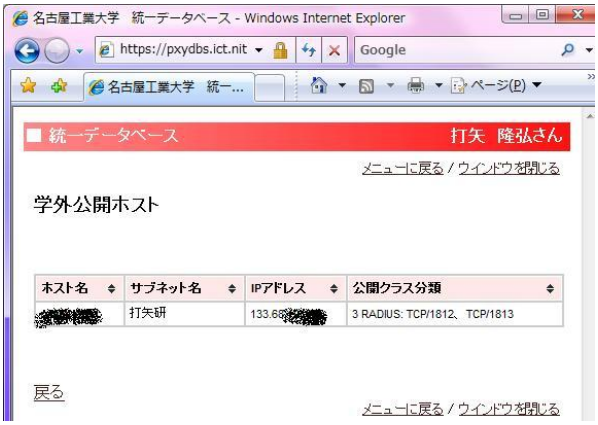

図5：学外公開ホストの設定状況確認画面

3.4 サブネット管理情報参照システム

研究室のネットワーク管理者は，本システムを用いて自身の管理サブネットの設定状況(サブネット基本情報，MACアドレス用IPアドレス範囲，WEB認証用IPアドレス範囲)を確認できる(図6)．

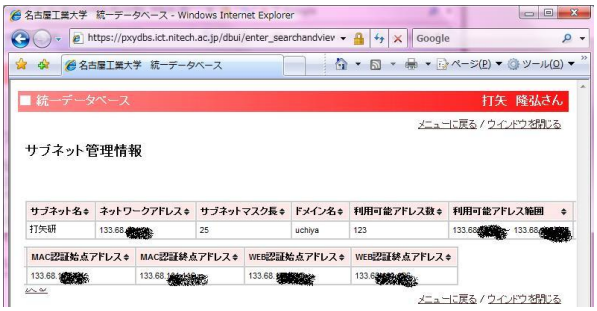

図6：管理サブネットの設定状況確認画面

3.5 ゲスト用無線 LAN アカウント発行システム

本システムでは，来学者が少数の場合に利用する「アカウント個別発行」と，学会開催などで来学者が多数の場合に利用する「アカウント一括発行」の2種類の発行方式を利用できる(図7)．アカウントの有効期間は開始日を含め最大4日まで設定可能である．発行手続きを行うと，認証用のアカウントとパスワードが利用者に提供される．

図7：ゲスト用無線LANアカウント発行システム

4 ネットワーク運用実績・利用状況

4.1 ネットワーク全体のダウン回数の大幅減

エッジスイッチによる L2 ループ検知機能やストームコントロール機能が有効に働いた結果，新 MAINS を導入した 2010 年 4 月から 2011 年 10 月までのネットワーク全体のダウン回数は 0 回であった．さらに，L2 ループ/ストーム発生源の特定等のネットワークの保守・管理が容易になった．

4.2 セキュリティ向上

統合脅威管理機器(UTM)の各機能が有効に働いた結果，ウイルス攻撃によるネットワークの全面停止や大幅な速度低下の発生は 0 回であった．また，外部からの攻撃による計算機への進入や，進入された計算機から外部への踏み台攻撃も皆無となった．

4.3 MAC アドレス認証回数と WEB 認証回数の推移

表 1 に 2010 年 11 月から 2011 年 9 月までの MAC アドレス認証の成功回数と WEB 認証の成功回数を示す．また，図 8 に月別の認証成功回数のグラフを示す．本学では 1 カ月に 100 万回以上の認証処理が行われていることがわかる．認証回数は非常に多いが，認証関連のトラブルは皆無であった．特に，認証処理の大部分は MAC アドレス認証であるが，本学では認証サーバである RADIUS サーバと MAINS データベースの連携により，認証処理を自動化している．そのため，接続端末が増え認証回数が大幅に増加しても管理者負担がない，スケーラビリティの高い構成となっている．

表 1：MAC 認証回数と WEB 認証回数

年月	MAC認証回数	WEB認証回数	合計
2010年11月	1082293	19111	1101404
2010年12月	1141615	16771	1158386
2011年1月	1136628	17434	1154062
2011年2月	1045914	16147	1062061
2011年3月	1084752	11525	1096277
2011年4月	1140352	21519	1161871
2011年5月	1175321	24082	1199403
2011年6月	1174159	24676	1198835
2011年7月	1173967	24939	1198906
2011年8月	1070801	15435	1086236
2011年9月	1057077	12937	1070014

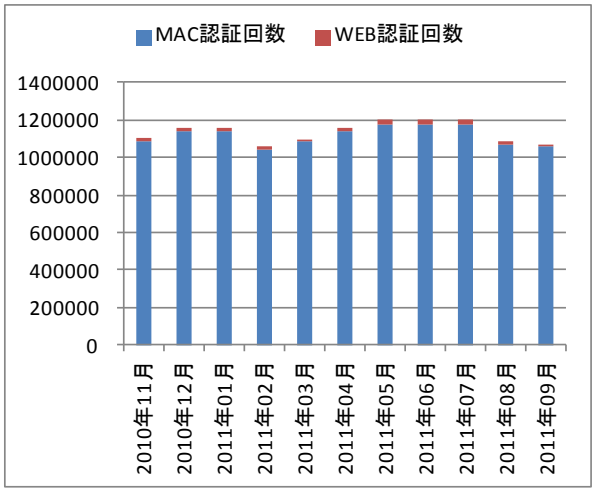

図 8：月別の認証成功回数

4.4 無線 AP の接続状況

表 2 に 2011 年 9 月 19 日から 2011 年 10 月 16 日までの無線 AP の接続状況を示す．当該数値は無線 AP コントローラに記録されているセッション確立ログを基に算出した．休日・祝日と比較すると，平日は 2～3 倍程度の接続があるのがわかる．また，前半 2 週と比較して，後半 2 週の接続数が増加している．これは後期開始となり，無線 LAN

利用者が増加したためと考えられる．接続数は全体的に予想より多いものであったが，約 400 台の無線 AP が有効活用されていることが確認できた．

表 2：無線 AP の接続状況

期間	月	火	水	木	金	土	日	合計
09/19–09/25	4571	13445	6340	11129	4938	4740	4256	49419
09/26–10/02	13985	14099	14624	15832	14728	6339	5450	85057
10/03–10/09	16104	22154	19181	21023	17506	5291	5152	106411
10/10–10/16	5852	26029	20985	28391	29484	14782	14492	140015
合計	40512	75727	61130	76375	66656	31152	29350	380902

4.5 WEB 認証における研究室 VLAN への接続状況

表 3 に研究室 VLAN を WEB 認証接続先に設定しているユーザ数を示す．学生数の推移を確認すると，4 月から 10 月にかけて，設定ユーザは増加傾向にあることがわかる．この傾向は翌年 3 月まで継続することが予想される．一方年度が変わると設定ユーザが減少することも確認できた．これは本設定を行っているのが主に研究室配属された 4 年次以上の学生であり，学生の卒業により設定ユーザが減少してしまうためだと考えられる．一方，教員数の推移から本設定の利用教員数は増加傾向にあることがわかる．昨年度と比較して今年度の利用教員数は微増であるが，今後さらに利用教員数を増やすためには，「研究室 VLAN」を接続先に設定するメリットを教員に周知していくことが重要である．

表 3：研究室 VLAN を WEB 認証接続先に設定しているユーザ数

年月	学生	教員	合計
2010年4月	30	19	49
2010年10月	90	46	136
2011年4月	47	46	93
2011年10月	103	47	150

4.6 ゲスト用無線 LAN アカウント発行システムの利用状況

表 4 に 2010 年 4 月から 2011 年 9 月までのゲストアカウント発行状況を示す．「アカウント個別発行」では発行件数は少ないものの，ほぼ毎月利用されていることがわかった．また，「アカウント一括発行」は学会シーズンである 8 月～9 月，3 月の利用が多く，特に 2010 年 9 月には 2,357 アカウントの発行があったことから，来学者の無線 LAN 利用に本システムが大いに貢献したことがわかる．

表 4：ゲスト用無線 LAN アカウント発行システムの利用状況

年	月	個別発行回数	一括発行回数	発行アカウント数（一括発行）
2010	4	6	2	55
	5	2	0	
	6	9	1	100
	7	0	3	20
	8	9	2	20
	9	8	5	2357
	10	3	0	
	11	4	0	
	12	5	2	115
2011	1	5	2	17
	2	3	0	
	3	6	3	67
	4	1	1	10
	5	2	0	
	6	7	0	
	7	0	1	20
	8	2	1	10
	9	2	1	30

5 おわりに

本稿では，名古屋工業大学における大規模ダイナミック VLAN ネットワークの管理・運用方式に焦点を当て，新 MAINS の構成，開発したシステム，及び，新 MAINS におけるネットワーク運用実績や利用状況の推移について報告した．今後はネットワーク管理の効率化とアクセスログ解析システムの構築・運用を進めてゆきたい．

参考文献

[1] キャンパス情報ネットワーク（MAINS）
http://www.cc.nitech.ac.jp/mains.html
[2] “大規模な認証ネットワークシステムの構築”, 西日本電信電話株式会社お客様事例紹介パンフレット, 2010.
[3] “新キャンパス情報ネットワークの利便性と高度なセキュリティの両立に寄与する FortiGate”, フォーティネットジャパン株式会社, 2010.
http://www.fortinet.co.jp/doc/cases_nitech.pdf
[4] “1 万 1000 台の機器を MAC 認証と Web 認証によるダイナミック VLAN で使用”, アラクサラネットワークス株式会社, 2010.
http://www.alaxala.com/jp/introduce/case12/