



## 賛助会員だより

フォーティネットジャパン株式会社

### キャンパス情報ネットワークを支える 次世代ファイアウォールFortiGate-1500D ～eduroam用のセキュアな無線LANコントローラ としてもFortiGateを活用～

創立110年を迎えた名古屋工業大学は、7万人を超える優れた人材を輩出し、我が国の産業社会の礎を築き、その繁栄を支えてきました。その教育的な特徴は、入学時から専門教育課程を実施し、実践的な工学エリート養成を目指している点にあります。また、「工学で世界の平和と幸福に貢献する研究」を目指し、工学の広い分野で先端的、独創的な研究を創出するイノベーションを喚起し、世界に発信することができる「工学イノベーションハブ」を構築しています。

こうした教育研究活動を支えるキャンパス情報ネットワークや基盤的情報システムの運用管理を行うのが、情報基盤センターです。現在、情報基盤センターではサーバ、ネットワーク、ストレージ、クライアントに至る全面的な仮想化環境を構築しており、シンクライアント用が約250台、各種サーバ群が約150台など約400台の仮想マシンが稼動しています。

また、キャンパス情報ネットワーク「MAINS」(Meikoudai Advanced Information Network System)は、約2万台の機器のMACアドレス認証が可能なVLANを2010年から運用しています。このダイナミックVLAN環境構築の際にFortiGate-3810Aが導入され、仮想UTM機能のVDMを利用して、学外通信およびVDM間を越える学内通信の制御とセキュリティ強化を実現してきました。

運用5年目を迎えた2014年には、FortiGate-1500Dにリプレースされ、10GbpsでSINET(学術情報ネットワーク)に接続する通信や情報基盤サーバ群への安定した通信とセキュリティ確保に寄与しています。

#### ■10Gbpsの外部接続を活かせるIPSスループットを確保

名古屋工業大学のFortiGate運用は、ファイアウォール機能、DoSのアノマリ検知等のIPS(不正侵入防御)、アプリケーション制御(P2P型ファイル交換ソフトの遮断など)、メールのアンチウイルスおよびスパムメ

ール検知などです。

「本学では学外通信だけでなく、情報基盤システムへのアクセスなど内部通信でも仮想UTM機能を運用しており、ウイルス感染した端末の持ち込みなどで、通信の可用性が損なわれる危険性は常にあります。そのためウイルス侵害があってもネットワーク可用性を維持できるCPU性能の高いモデルが求められます」。情報基盤センター長の松尾啓志氏は、FortiGate-1500Dにリプレースした背景をこう説明します。

従来モデルでは4GbpsだったIPSスループットがFortiGate-1500Dで11Gbpsに拡大し、以前は50%を超えていたCPU負荷が、現在は10%以下で稼動しているということです。「学外接続の10Gbpsを活かせるスループットが得られるようになりました」(松尾氏)と、あらためてFortiGateの性能を高く評価しています。

また、工学研究科准教授の打矢隆弘氏は、VDMの管理インタフェースの機能性向上を指摘しています。「従来は各VDMの設定を行う際には、それぞれのVDMに管理画面を切り替える必要がありましたが、1つの画面ですべてのVDM環境が見えるようになり、管理性が向上しました」(打矢氏)。

#### ■eduroamサービス用無線LANをFortiGate/FortiAPで構築

名古屋工業大学はFortiGate-1500Dによる安定性・可用性向上を実現した一方、2012年よりFortiGate-200BとFortiAPによる国際無線LANローミング基盤「eduroam」に対応する無線LAN環境を整備しました。

eduroamは大学など研究機関の間でキャンパス無線LANの相互利用を実現するローミングサービスで、世界規模で展開され、日本では国立情報学研究所(NII)が中心となりeduroam.jpを運用している。2015年3月現在、国内108機関(大学、研究機関)、世界約70か国・地域が参加し、学外からの研究者等にeduroam認証サービスによる無線LANを提供しています。

同大学では主に学生向け無線LANサービスをMACアドレス認証で運用しており、IEEE802.1x認証のeduroamサービスを提供するためには、既存ネットワークと分離した環境が必要でした。「独立型のAPを

利用した無線LANでは、機器の死活監視ができない、ファームウェアのバージョンアップに手間がかかるなどの課題があります。そこで、もともとVPN装置としてFortiGate-200Bを導入・運用していたため、これをコントローラとして無線LAN環境を構築することとしました」(打矢氏)と構築の背景を述べています。

### ■アクセス制御と脅威管理を実現するセキュアな無線LAN環境を実現

FortiGate-200Bをコントローラとするeduroamサービス環境を構築するメリットは、次のような3点だといえます。

第一は、FortiGateシリーズは以前から運用しており、同様の管理インターフェースで運用できるため、管理が容易であることです。第二に、FortiGate-200B自体が通信のフィルタリング機能を有しており、eduroam認証ユーザの学内電子ジャーナルなどへのアクセスを遮断できることでし。第三に、eduroamサービスに必要なポートを開けるなど、通信のプロトコル制御をFortiGate-200Bで集中管理できることだということです。

実際の接続・認証処理では、FortiGate-200Bを介したアクセス端末の認証要求がeduroam用名工大RADIUSサーバに届き、学内者からの認証要求はActive Directoryに転送されます。学外者の認証要求は外部ネットワーク境界のFortiGate-1500Dのeduroam用ファイアウォールを通り他機関のeduroam用RADIUSサーバへ転送されます。

アクセスポイントは、2012年の構築時にFortiAP-220Bが13台導入、その後に順次追加され、現在19台のFortiAP-220B/221Bが導入されました。主に大学会館や講堂、講義室など大小の学術研究会が開かれる会場向けに設置されています。また、主要会議室以外で研究会が行われる際には、可搬タイプのプラグアンドプレイ対応無線APのFortiAP-11Cも利用されています。

松尾氏は「eduroamは学外研究者の利便性を目的としたサービスであり、コストを抑えて構築することが求められます。元々運用していたFortiGateをコントローラ兼アクセス制御機器として利用でき、APの台数ライセンスも不要なFortinetのソリューションは、われわれの要求を満たすものでした」と述べています。今後、隣接する名古屋大学医学部・附属病院で運用するeduroamサービスとのローミングを可能にして学外

研究者の利便性向上も検討し、その際に、国内販売が間もない屋外設置対応APのFortiAP-222Cに期待を寄せています。

eduroam (エデュローム)は、欧州のGÉANT Association (旧TERENA) で開発された学術無線LANローミング基盤です。日本を含む世界76か国・地域で、キャンパス無線LANのデファクト・スタンダードになっています。

<https://www.eduroam.org/>

#### 導入・構築のポイント

- (1) VDOM機能を利用したキャンパス情報ネットワークに、外部接続10Gbpsを活かせる性能と可用性をFortiGate-1500Dで実現
- (2) セキュリティ機能と無線コントローラ機能を備えたFortiGate-200Bにより、セキュアなeduroam用無線LANサービスを提供
- (3) VPN装置として運用してきたFortiGate-200Bを利用することで、コストを抑えた無線LAN環境を実現



名古屋工業大学情報基盤センター前にて  
左から若松慎三氏、梶岡慎輔氏、松尾啓志氏、  
打矢隆弘氏。

#### 問い合わせ先

社名 フォーティネットジャパン株式会社  
担当部署名 市場開発本部  
TEL:03-6434-8533  
E-mail: [public\\_jp@fortinet.com](mailto:public_jp@fortinet.com)  
URL <http://www.fortinet.co.jp/>