小規模校における全館 Wi-Fi 化と学内 LAN のセキュリティ対策

田中　健吾 [1)2)]

1) 香蘭女子短期大学 情報センター
2) 香蘭女子短期大学 ライフプランニング総合学科

tanaka@koran.ac.jp

Implementation of Whole Building Wi-Fi and Security Measures for Campus LAN in Small College

Kengo Tanaka [1)2)]

1) Information Technology Center, Koran Women's Junior College
2) Department of Comprehensive Studies for Life Planning, Koran Women's Junior College

概要

2021 年度に香蘭女子短期大学では一部のエリアにしか導入されていなかった Wi-Fi 環境を，全館へと拡張する工事を行った．それに伴い，Wi-Fi 環境も教育・研究・業務の基盤として利用されるようになり，それらの用途に耐えられるネットワーク構成，セキュリティ対策，安定稼働性，効率的なネットワーク管理などを担保できるように設計・施工を行ったので，本稿ではその内容について報告する．Wi-Fi 環境を含めた学内 LAN 管理の低コストかつ高効率な運用方法の事例として，本学と同規模程度の小規模校に参考になる事例であると考えている．

1　はじめに

GIGA（Global and Innovation Gateway for All）スクール構想は，2019 年 12 月に閣議決定を経て文部科学省により発信された小学校，中学校，高等学校を対象とした ICT 環境の実現構想である．Society5.0 時代到来へ対応するために，高速大容量の通信環境を校内 LAN として整備し，児童生徒に 1 人 1 台の端末環境を配備することで，児童生徒に個別最適化され，創造性を育む教育 ICT 環境の実現を目指したものである，と述べられている[1].

GIGA スクール構想を IT インフラの観点から簡潔にまとめると，校内に高速無線 LAN を導入し，クラウド活用や大容量の動画視聴やオンラインテストを快適に行える校内 LAN の整備をする，と説明される．その際，工事に用いる UTP ケーブルは CAT6A 以上，ハブやスイッチ，ルーターなどは 1Gbps の普及モデルを使用する，というガイドラインが提示されている[2]．この仕様の記述は解釈の差異を残す表現となっているが，各フロアのスイッチと教室のアクセスポイント（以下，AP）や LAN ポートまでの間は，理論値 1Gbps 程度の通信速度を，他方，各フロアのスイッチもしくは各校舎の主幹スイッチから上位の主幹スイッチまで，くわえて WAN 側のインターネット接続部分までは理論値で 10Gbps 程度の通信速度を想定していると概ね理解される．

2020 年にパンデミックを起こした新型コロナウィルスの影響で，日本全国の教育現場は遠隔授業への対応を迫られることになり，GIGA スクール構想の計画も福岡県については前倒しで進行することになった．本学でも 2020 年度は通常の対面授業の他に，遠隔授業ならびに対面・遠隔の両方を行うハイブリッド型授業の実施を行った．また，パソコン室の授業も本学 Firewall への VPN 接続とリモートデスクトップ接続を組み合わせることで，一部遠隔授業を実施した[3].

上記の様にして 2020 年度の授業を終えた結

果，様々な問題が明確になってきた．その一つとして，1 日の時間割に対面授業と遠隔授業の両方が混在する場合，遠隔授業を学内で受講しようとすると，校舎内に AP がある場所が限定されており，その周辺に密を招くという問題があるということが認識された．

学内での密対策や教育・研究・業務の情報化の推進，GIGA スクール構想を基盤とした教育からの連続性への対応などのために，本学では 2021 年度に全館 Wi-Fi 化を行った．それ以前は，学内の一部のエリアにしか Wi-Fi 環境を備えておらず，その用途は主として学生のインターネット利用であった．この度の全館 Wi-Fi 化では，用途を学生・教職員の教育・研究ならびに業務の基盤へと拡張したことで，それらに耐えられるネットワーク構成，セキュリティ対策，安定稼働性，効率的なネットワーク管理などを担保できるように設計・施工を行った．本稿ではこれらの内容について報告を行う．

2 ネットワーク構成

この度の全館 Wi-Fi 化は，有線ネットワークを主とした既存の学内 LAN を拡張する形式で設計・施工を行った．2.1 ではそのネットワーク構成について，2.2 では AP の無線部分の構成について，いずれもその概略を簡潔に説明する．

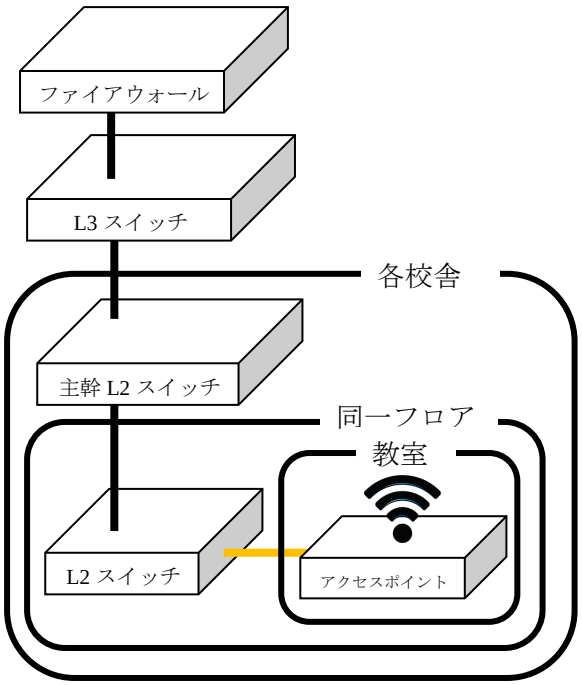

図 1　ネットワーク構成の概略図

2.1 ネットワーク機器構成

図 1 に今回の全館 Wi-Fi 化工事に関するネットワーク構成の概略を示す．本学のファイアウォールの配下には L3 スイッチが配備されて，そこから下位にある各校舎と各パソコン室の主幹 L2 スイッチへ光ファイバーケーブルで接続されている．各棟の主幹 L2 スイッチから配下の各フロアの L2 スイッチに，さらには各教室等に設置されている AP までは，いずれも階層的にスター型のネットワークで，UTP ケーブルで接続されている．

AP には IEEE 802.11ac（Wave2）に対応し，2.4GHz 帯では最大で 400Mbps，5GHz 帯では 867Mbps の通信速度のものを採用した．また，PoE+（IEEE 802.3at）に対応した L2 スイッチを採用し，その配下に設置された AP には UTP ケーブルで給電することにした．そのために，PoE+に非対応の L2 スイッチしかないフロアでは，PoE+に対応した L2 スイッチでリプレースもしくは追加するか，給電ポート数分の PoE+インジェクターを用いた．即ち，図 1 において，同一フロア内の L2 スイッチから AP までは，PoE+で給電しており，オレンジ色の線は UTP ケーブルで給電していることを意味している．

2.2 VLAN と無線部分の構成

学内のネットワークは「学生用 VLAN」「PC 室用 VLAN」「職員用 VLAN」「教員用 VLAN」他で構成されている．今回導入した AP には VAP（Virtual Access Point）の機能を備えており，1 台の AP に複数の VLAN を収容可能である．

「学生用 VALN」は主に学生のインターネット接続のための用途であり，同 VLAN に対応する VAP を AP に設定し，SSID を公開設定して発信している．また，「PC 室用 VLAN」はパソコン室用であり，対応する SSID を隠蔽設定している．授業時に学生端末をパソコン室用の VLAN に接続するための用途を想定している．

「教員用 VLAN」「職員用 VLAN」に接続するために指定する SSID は，認証時にユーザ・端末に応じた VLAN 情報が AP へ提供され，所属 VLAN が決定される．したがって，「教員用 VLAN」「職員用 VLAN」に対応する SSID は統一した SSID で運用することにした. 表 1 では，学内 LAN でユーザが主に使用する VLAN とそれに対応する VAP･SSID の設定の概略についてまとめた.

表 1　各 VLAN と対応する VAP･SSID の設定

VLAN	VAP・SSID	SSID 公開／隠蔽
学生	2.4GHz 帯 SSID 5GHz 帯 SSID	公開
PC 室	2.4GHz 帯 SSID 5GHz 帯 SSID	隠蔽
教員	2.4GHz 帯 SSID 5GHz 帯 SSID SSID を「教員」「職員」で統一	隠蔽
職員		

学内には 2.4GHz 帯にしか対応していない端末・周辺機器が存在するし，5GHz 帯に比べて 2.4GHz 帯の方が, 障害物などがある場合でも広範囲まで伝播する傾向があるため，両方の帯域の SSID を使用することにした．また，SSID の隠蔽（ステルス）設定はパッシブスキャンとしてビーコンを発信しなくなる，もしくは，実際の SSID 名で発信しなくなる，というだけで，アクティブスキャン時には端末から AP に向けて実際の SSID 名が発信されることになる．したがって，本質的なセキュリティ向上には繋がらないが，非専門家には一定の効果が期待できるので，「PC 室用 VLAN」「職員用 VLAN」「教員用 VLAN」に対応する SSID は隠蔽した.

電波干渉を極力抑えるために, AP 間で使用するチャンネルや電波の出力を自動調整するためのコントローラも導入した．また，IP アドレスを DHCP サーバから端末へリースする速度が遅いと, ネットワークの利用開始が遅滞するので，リース速度が高速な専用の DHCP 機器の導入も行った.

3 セキュリティ対策

この節では，この度の全館 Wi-Fi 化に伴い，高いセキュリティ強度を要する VLAN へのアクセス許可は IEEE802.1X 認証を構成することにしたので，その内容について述べたい．3.1 では認証システムの構成について，3.2 では主な VLAN へのユーザ・端末ごとのアクセス制御について，それぞれの概略を簡潔に説明する.

3.1 認証システムの構成

「教員用 VLAN」「職員用 VLAN」に対応する SSID に端末が接続する際の認証には，高いセキュリティ強度を実現するために，EAP-TLS の認証方式を採用することにした．そのために，IEEE 802.1X に対応した AP（authenticator）と RADIUS サーバ（authentication サーバ）の機能を有する認証機器を導入した．その認証システムの概略図を図 2 に示す.

この認証機器は RADIUS サーバに加えて，プライベート認証局の機能を内蔵した専用機器であり，プライベート認証局から RADIUS サーバへのルート証明書とサーバ証明書のインストールが自動化されている．図 2 の上部にある認証機器の図はプライベート認証局と RADIUS サーバが一体となって描かれており，プライベート認証局からルート証明書とサーバ証明書が RADIUS サーバへ自動的に配備されることをオレンジ色の矢印は示している.

また，水色の矢印は，プライベート認証局で発行されたクライアント証明書とルート証明書が，プライベート認証局から物理的に外部へ移動し，教職員端末へ配備されることを意味している．ここまでは，端末が認証と通信を行う前段階の準備である.

図 2 の①～⑫は,「教職員端末」を「教職員用 SSID」を指定して接続開始をしてから，認証され，認証情報に対応する VLAN へ通信開始となるまでの処理順序の概略を示している.

各端末（supplicant）にインストールされたクライアント証明書と RADIUS サーバにインストールされているサーバ証明書を，相互にルート証明書を用いて認証する．この際，クライアント証明書は RADIUS サーバが端末を認証するために，ルート証明書は端末が RADIUS サーバを認証するのに使用される．

AP はダイナミック VLAN で「教職員用端末」を，端末ごとに適切な VLAN へ所属させるように運用している．RADIUS サーバで「教職員用端末」の認証が成功すると，認証情報に紐づいた VLAN ID がリプライアイテムとして AP へ返

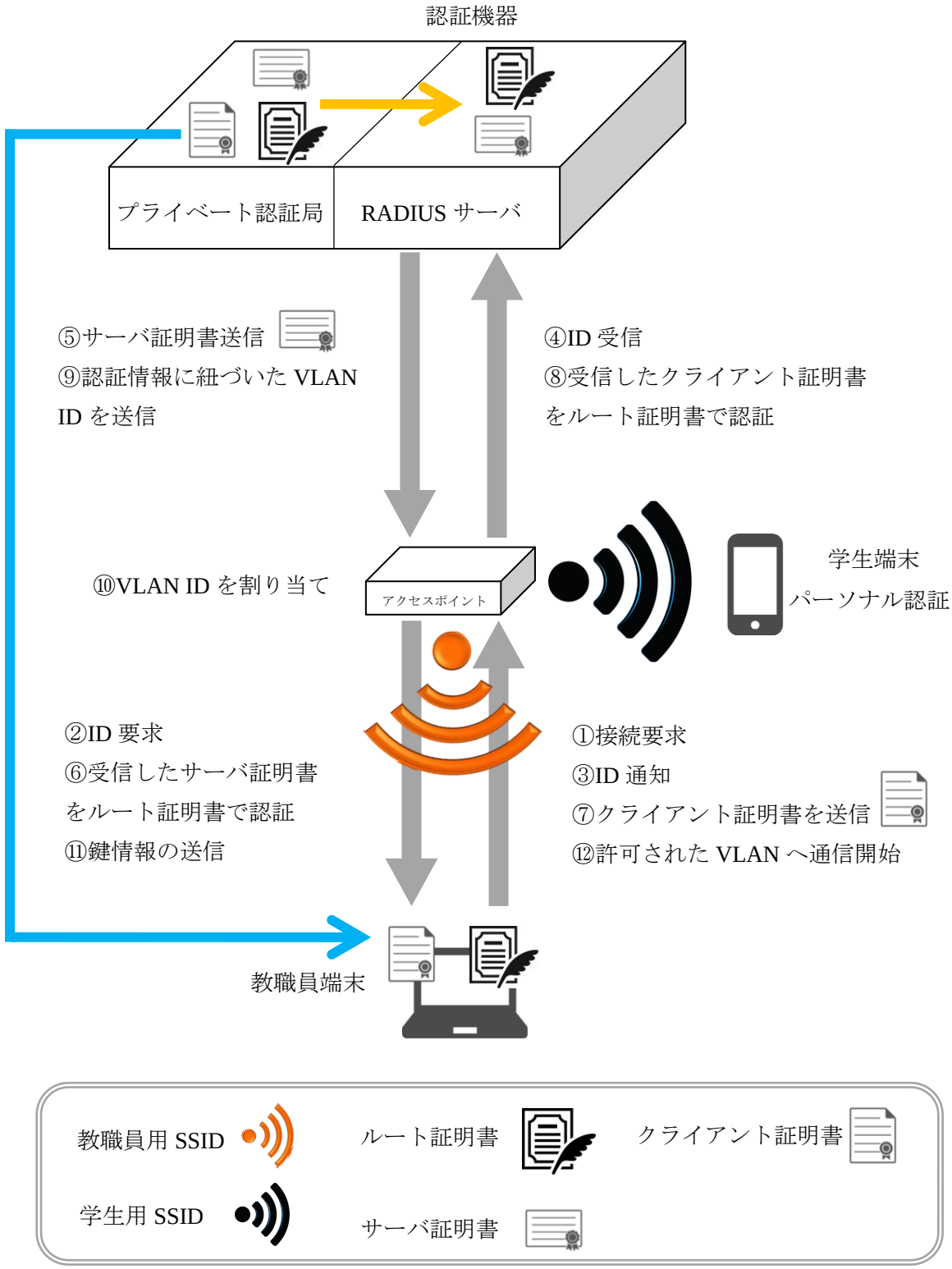

図 2　IEEE802.1X 認証の構成と通信開始までの処理

される．そして，端末が AP へ無線通信を行うと，AP の有線ポート部分で VLAN 情報が付加され，適切な VLAN へ参加することになる．

他方，図 2 の右部分にはスマホのアイコンで「学生端末」が図示されている．「学生用 SSID」はパーソナル認証で運用されており，共通のパスワードで「学生用 VLAN」へ通信許可される．

3.2 ユーザの認証と VLAN へのアクセス制御

図 3 には，図 2 の認証システムの配下で，「ユーザ・端末」「SSID」「認証方式」「VLAN へのアクセス制御」の関係性がまとめられている．

「教員端末」「職員端末」は「教職員用 SSID（オレンジ色の電波のアイコン）」で AP へ接続し，インストールされているクライアント証明書が RADIUS サーバに EAP-TLS 認証されると，認証情報に対応した VLAN へ通信許可されることを緑色の丸は意味している．

また，「学生用 SSID」を指定して接続してきた「教員端末」「職員端末」は，AP が持つ MAC アドレスのブラックリストで「学生用 VLAN」への通信がブロックされている．そのことを赤色の禁止マークは意味している．

「教職員用周辺機器」はクライアント証明書をインストールすることができないので，パーソナル認証と MAC アドレス認証を併用することにした．RADIUS サーバにあらかじめ MAC

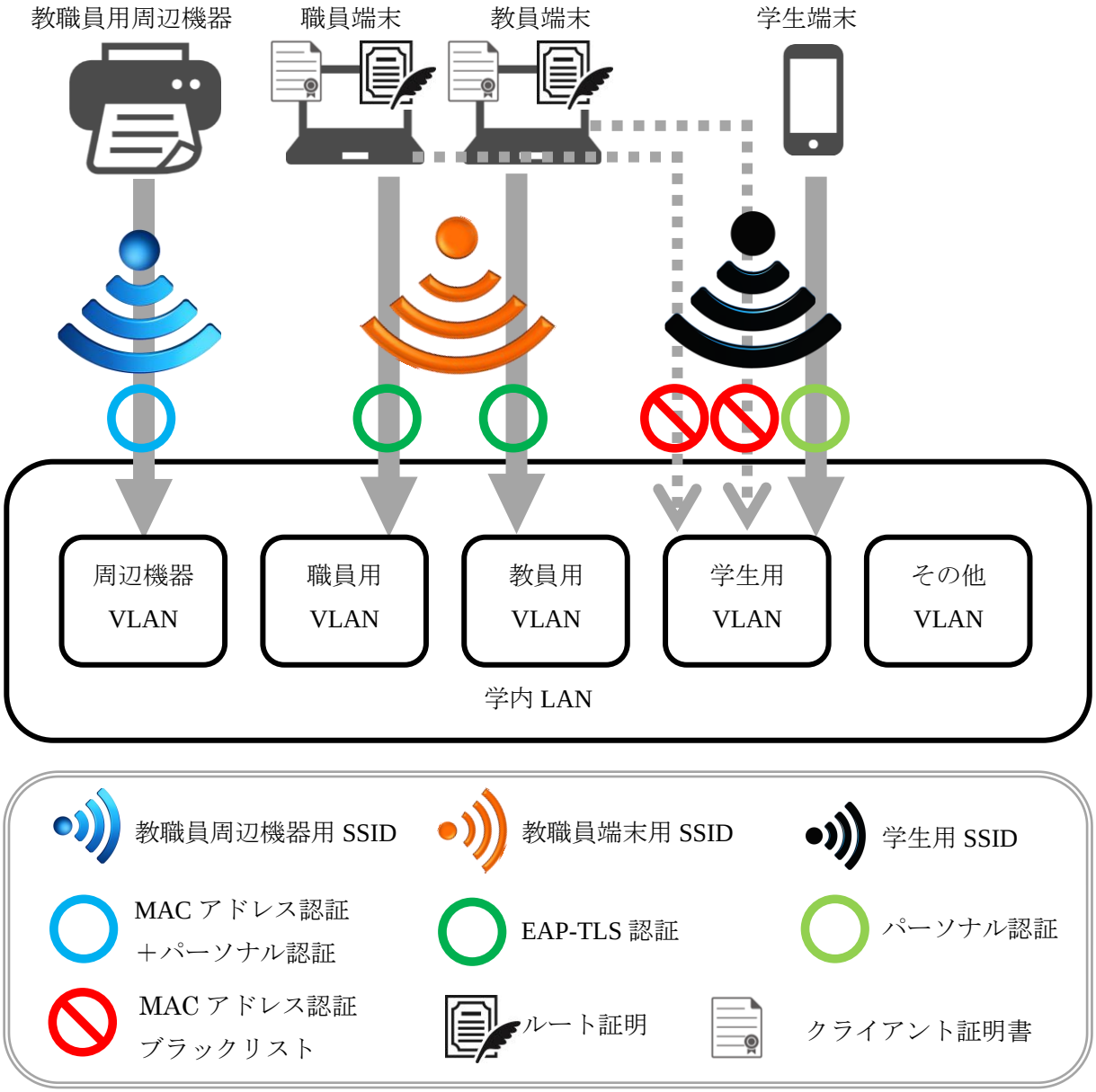

図 3　ユーザ・SSID・VLAN へのアクセス制御の概略

アドレスが登録されている周辺機器が認証後，「周辺機器用 VLAN」へ通信可能となる．今回導入した AP の仕様により，単一の SSID で，EAP-TLS 認証と MAC アドレス認証を同時に収容できなかったことより，「教職員用 SSID」とは別に「教職員周辺機器用 SSID（青色の電波のアイコン)」を設定する必要があった．

「教職員周辺機器用 SSID」を指定して接続要求してきた周辺機器は，パーソナル認証後，AP が MAC アドレスを RADIUS サーバへ問い合わせて認証されると，「周辺機器 VLAN」へ通信許可されることを青色の丸は意味している．また，図 3 には示していないが，「職員用 VLAN」「教員用 VLAN」からは「周辺機器 VLAN」へ通信許可している．したがって，「教職員用端末」は「教職員用 SSID」を指定して各 VLAN へ参加し，そこから「周辺機器 VLAN」に所属している「教職員用周辺機器」を利用可能である．

他方，「学生端末」は「学生用 SSID」を指定して AP へ接続し，パーソナル認証され，「学生用 VLAN」へ通信許可されることを黄緑色の丸は意味している．

4 運用コスト

この度の全館 Wi-Fi 化に伴い，AP は既設の台数と併せて 125 台となった．また，L2 スイッチの台数も増加している．ネットワーク機器の管理台数は急増し，従来の学内 LAN の運用方法では維持管理が困難であり，効率的な運用方法が求められる．4.1 ではネットワークの設計およびネットワーク機器の設定管理の観点から，4.2 ではネットワークの安定稼働性やトラブル時の対応という観点から，運用コスト全般について説明したい．

4.1 ネットワークの設計とネットワーク機器の設定管理

AP では，パーソナル認証に関する定期的なパスワード変更や SSID 等に関する設定変更が必要になる．また，電波干渉を避けるために出力や使用するチャンネルを AP 間で調整する必要もある．

しかし，100 台を超える AP の設定変更を 1 台ずつ行うのは，現実的ではない．一括した AP の設定変更ができることや，使用するチャンネルや出力を自動調整してくれる機能が運用コスト全般を大幅に引き下げてくれる．

それらの重要な役割を果たしてくれるのが，AP のコントローラであり，今回導入した AP に対応したコントローラは上記の機能を備えている．また，同コントローラは L2 スイッチの VLAN に関する簡易的な設定機能を拡張して搭載することができる．L2 スイッチに対して一括して新しい VLAN を作成したり，個別の L2 スイッチに対してアクセスポートやトランクポートに，VLAN を追加したりすることが，GUI の画面上でマウス操作により可能である．コントローラが有している設定機能に限定されるが，大幅に設定変更作業が迅速化されることを実感できる．その際，VLAN 構成を可視化する機能もあり，管理業務を効率的にアシストしてくれる．

今回の工事でプライベート認証局と RADIUS サーバの機能を有する認証機器が導入されたことで，ダイナミック VLAN の実装が可能となり，「教員用 VLAN」「職員用 VLAN」などの重要なセグメントへのアクセスは端末にインストールされたクライアント証明書に紐づく VLAN ID で管理されるようになった．他方，有線 LAN 主体だったこれまでは，タグ VLAN で管理しており，部屋の用途が変更になると，L2 スイッチのアクセスポートの所属 VLAN を変更する作業が生じていた．もちろん，有線 LAN の利用は継続されるので，有線部分もダイナミック VLAN への移行が必要になるが，それが完了すれば，定期的な L2 スイッチの設定変更作業は格段に少なくなり，クライアント証明書に紐づける VLAN ID を管理すればよい状態に概ね移行することになる．L2 スイッチの設定作業は専門的な知識・技術を要するが，それに

比べると今回導入した認証機器はいわゆる専用機器であり，クライアント証明書の発行業務は単純作業のレベルに簡単化されている．したがって，属人的な業務から誰でも担える業務へと移行したことになり，ネットワークの運用コストを軽減できたと言える．

4.2 ネットワークの安定稼働性と障害時の復旧対応

本学には著者を含めてネットワーク管理をする専任スタッフは不在である．ネットワーク障害が発生すると，途端に障害切り分けや復旧作業への対応が必要になり，それ以外の業務を圧迫する．また，学内 LAN は教育・研究・業務の基盤であるので，何よりもその安定稼働が重要であり，障害時の対応は想定する必要があるが，それ以前に冗長構成やホスティングサービスの積極的利用等で安定稼働を担保することがきわめて重要であると長年考えてきた．

今回導入した IEEE802.1X 認証を構成する図 2 の認証機器は，プライベート認証局と RADIUS サーバを内蔵しており，同機器に障害が発生すると途端に「教職員用端末」は学内 LAN へアクセスできなくなるために，冗長構成をすると共に 2 台の認証機器間でデータの同期をしており，片方の機器に障害が発生したとしても，もう片方の機器で認証を担保することができる構成となっている．

また，今回導入した DHCP サーバも障害が発生すると途端に端末へ IP アドレスがリースされなくなるため，これも 2 台での冗長構成を採用している．また，同機器は DNS サーバの機能も内蔵しており，ゾーン転送による同期と冗長構成で DNS サーバの安定稼働性も向上した．

L2 スイッチについては，今回導入した AP のコントローラと L3 スイッチが連携して設定データを保存する機能を有している．障害時には L2 スイッチをリプレースして配線を元通りに接続すると，設定が自動復旧する仕組みになっており，障害時の復旧作業の軽減と復旧までの迅速化に大きく貢献してくれることになる．

AP については，リプレースが困難な場所に設置されているものもあり，障害時の復旧作業が困難なケースも予想されるが，その場合は隣接している AP の出力を増大させるなどして，カバーすることで対応しつつ，復旧作業を急ぎたい．

5 まとめ・考察・課題

本稿では 2021 年度に行った本学での全館 Wi-Fi 化に関する設計･施工内容の概要について報告を行った．以下，2 節，3 節，4 節について，その内容をまとめると共に，いくつかの考察や今後の課題について述べたい．

2 節ではこの度の全館 Wi-Fi 化について施工後のネットワーク構成と AP の無線部分の構成について，図 1 および表 1 にまとめ，それぞれの概要について説明を行った．主幹 L2 スイッチから各フロアの L2 スイッチ，さらには AP までは CAT6 の UTP ケーブルで接続しており，GIGA スクール構想と同程度の帯域を保証するネットワーク構成となっている．

他方，図 1 の主幹 L2 スイッチから上位の L3 スイッチまでは工事を行っていない．「主幹 L2 スイッチ」－「L3 スイッチ」－「ファイアウォール」の間は，それぞれの両端に SFP モジュールを収容しており，その間を光ファイバーケーブルで接続しているという既存設備のままである．GIGA スクール構想ではネットワークの幹線部分は 10Gbps の帯域を想定しているので，これらの部分は GIGA スクール構想の仕様には見合っていないことになる．今後，大容量の動画視聴などの用途が拡大していけば，それに伴い，求められる帯域も拡大していくことになり，主幹 L2 スイッチからファイアウォールまでの帯域だけではなく，インターネット接続回線についても見直しが必要になる可能性がある．

無線部分の構成については，「学生用 SSID」は，利便性を優先して公開し，それ以外は隠蔽しているが，現在のところ，教職員についてはそのことが利用の障壁を押し上げている感触を

持ってはいない．現状，AP のみダイナミック VLAN で運用しているが，将来的には有線部分にも拡張し，利用の障壁をさらに低減したい．

今回採用した AP は 11ac の規格に対応しており，通常のインターネット接続が快適に利用できるのは, 1 台の AP に接続する端末台数の上限を 40～50 台と想定している．しかし，1 台の AP に接続可能な台数の上限を論理的に制限していないので，複数台の AP を設置している大教室では，特定の AP に接続台数が偏重する可能性がある．その点については，今後，コントローラで端末の接続台数を観察しつつ，設定の必要性を検討したい．

3 節では全館 Wi-Fi 化に伴って導入した認証システムの構成と各ユーザ・端末のアクセス制御について，図 2 および図 3 にまとめ，それぞれの概略について説明した．教職員は各自の業務端末を AP へ接続するには，クライアント証明書の発行申請をし, 証明書を受け取った後は, 各自でインストールする必要がある[4]．しかし, 業務用端末を「教職員用 SSID」を指定して学内 LAN へ接続しなくても当面，業務に支障がない場合は，「学生用 SSID」を指定して「学生用 VLAN」へ接続し続けることも想定される．このような事態を回避するために，図 3 で示すように教職員の業務用端末は MAC アドレス制御で「学生用 VLAN」へのアクセスは論理的に禁止している．

4 節では, この度の全館 Wi-Fi 化で拡大したネットワークの運用コストとそれを低減するための工夫について述べた. コントローラによる AP の一括管理・調整機能やその拡張機能による L2 スイッチの効率的な VLAN 管理機能について言及した．例えば，全ての AP に新しい VLAN に対応した SSID を作成しようと思うと, AP はコントローラで一括して設定変更可能だが，それに連動して，AP が接続されている上位のネットワーク機器全台にタグ設定も必要になり, AP の台数増加に比例して，工数も必然的に多くなるため，効率的に設定変更できるツールが不在だと柔軟なネットワークの運用が担保できなくなる．

また，認証局・認証サーバと DHCP サーバの機能を二つの専用機器で担い，冗長構成した．専用機器は機能性や他の機器との連携性は柔軟さには欠けるものの，設定作業や運用作業が平易化されているという優位性がある．今回導入した DHCP 機器は DNS サーバの機能も内蔵しており，既存の DNS サーバの役割も同機器に統合することができたことで，更なるコスト削減に繋がった．本学の学内 LAN に必要な認証サーバ，DHCP サーバ，DNS サーバの機能性を，いずれも専用機器で実装し，かつ，冗長構成できたことは，安定稼働性と運用コストの低減に大きく資することができたと考えている．

本件に関する初期費や年間固定費などは契約時の時価という側面も少なくないので，費用の単純評価は難しいが，本学の様な小規模校で専任スタッフが不在でも，全館 Wi-Fi 化後の拡大したネットワークの日常運用がアウトソーシング無しで持続しているという事実が，本件のネットワーク運用が低コストで高効率であることを結論付けている．

参考文献・注

[1] 子供たち一人ひとりに個別最適化され，創造性を育む教育 ICT 環境の実現に向けて～令和時代のスタンダードとしての 1 人 1 台端末環境～≪文部科学大臣メッセージ≫ 2019 年 12 月，文部科学大臣　萩生田光一 https://www.mext.go.jp/content/20191225-mxt_syoto01_000003278_03.pdf

[2] GIGA スクール構想の実現パッケージ～令和の時代のスタンダードな学校へ～, 2019 年 12 月

[3] 小規模校におけるパソコン教室の三密対策と遠隔授業, 大学 ICT 推進協議会 2020, 2020 年 12 月，田中健吾

[4] 各自でクライアント証明書のインストールや「教職員用 SSID」を指定して AP へ接続できない場合は，各学科・事務局の情報端末利用運営委員がサポートの一次対応を務め，それでも問題解決しない場合は，情報センターが対応する体制になっている．