京都大学における無線 LAN システムの更新

針木 剛 [1)] 山中 香子 [1)]

1) 京都大学

hariki.tsuyoshi.3r@kyoto-u.ac.jp yamanaka.kyoko.3a@kyoto-u.ac.jp

Update of the Wireless LAN System in Kyoto University

Hariki Tsuyoshi[1)] Yamanaka Kyoko[1)]

1) Information Dept., Kyoto Univ.

概要

京都大学では 2009 年度より無線 LAN サービスを開始し 2023 年度には約 3,000 台の無線 LAN アクセスポイント（以下 AP とする）及び無線 LAN コントローラ（以下 WLC とする）を運用していたが、機器の老朽化に伴い 2024 年度に稼働中のすべての機器の更新を実施した。本稿では移行機器の選定や移行作業及び移行時の技術課題、その解決のために得られた知見の情報共有を目的として詳細内容をまとめる。

1 はじめに

1.1 無線 LAN 機器増設の推移

京都大学の無線 LAN サービスにおける AP 設置台数の推移を図 1 に示す。

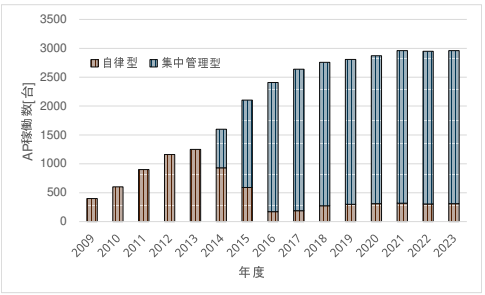

図 1 AP 設置台数の推移

2009 年度にサービス開始した当初は、限られた予算のなかで廉価な自律型 AP を講義室や会議室など公共スペースに限定し設置しサービスを運用していた。

無線 LAN（Wi-Fi）の技術向上に伴い、独自に AP を導入する研究室も増えその運用の安全性の確保や近接 AP との電波干渉の問題から、全学的な無線 LAN 環境整備を目的として 2014 年度から 2016 年度の 3 ヶ年計画で既存 AP1,080 台の更新及び新規 AP1,260 台の増設を実施した。このときの AP は集中管理型で WLC も同時に導入した。なお一部遠隔地に設置した AP は通信帯域を圧迫する懸念もあり既存の自律型 AP の利用を継続した。以降は吉田・宇治・桂のメインキャンパスは集中管理型、その他遠隔地は自律型として利用ニーズに応じて毎年度少しずつ増設を行っていたが、これら機器の老朽化に伴い 2024 年度に WLC 及び全 AP の更新作業を実施した。

1.2 無線 LAN サービスの変化

1.2.1 学内者用サービス

2009 年度の無線 LAN サービスは「みあこネット」とよばれる認証なしの VPN のみ利用可能な特殊なネットワークを提供しており、学内ネットワークとは完全に分離していた。無線 LAN サービス利用者は VPN 接続が必須であり、京都大学構成員も同様に京都大学で VPN 接続操作を求められた。

2014 年度の機器の大規模更新に伴い、利用者利便性を重視し IEEE802.1X 認証で学内ネットワークに直接接続できる新サービス「KUINS-Air」の運用を開始した。[1] 現在では全構成員約 77% が利用する京都大学 ICT の重要な基幹サービスの 1 つとなっている。

1.2.2 学内者用サービスに追加した機能

WLC でユーザ通信が一元集約される特徴を利用して、2017 年度に「KUINS-Air」において研究室ネットワークに直接接続できるダイナミック VLAN サービスを開始した。京都大学ではメインキャンパスを 9 構内に分けて、構内ごとに VLAN 番号を運用しているが、それら VLAN のうちダイナミック VLAN 利用希望者の 1,000 以上の VLAN を QinQ にて基幹スイッチに集約して WLC に出力している。[2]

「KUINS-Air」が多くのユーザに利用されるサービスのため、2022 年度よりセキュリティ e-Learning 未受講者に対し、通信制限と e-Learning サイトへの Web

リダイレクト機能を提供している。ユーザ認証後にLDAP 情報の当該フラグを参照し、radius サーバで通信制限 ACL と Web リダイレクト（キャプティブポータル）を適用する属性を付与することでその機能を実現している。

1.2.3　学外者用サービス

2009 年度の運用当初より学術機関に所属する学外者向けに学術無線 LAN ローミング基盤「eduroam」に参加しサービスを提供している。「eduroam」はIEEE802.1X 認証により他機関の認証が利用できるサービスとなっており、利用者ネットワークは SINET 回線だが学内とは分離した運用となっている。

また一般の学外者向けには 2014 年度の機器更新時に携帯電話 3 社の提供する Wi-Fi サービスを提供を開始した。こちらは携帯電話各社の商用ネットワーク回線で提供していたが、サービス終了等により現在は提供していない。しかし附属図書館など学外者が利用する施設等でニーズがある。

2　新システムの検討

2.1　新システムに求める機能

2021 年度より新システムの調査を開始し、以下の機能を重視して動作検証を行った。

- 全学集約した 1,000 以上のダイナミック VLAN
- 特定認証ユーザの通信制限と Web リダイレクト
- WLC 障害時のサービスリカバリ

特に WLC の障害や今後増加傾向のユーザ通信の不要な集約を避ける観点でクラウド型 WLC についても検証を行った。クラウド型 WLC ではダイナミック VLAN を中継するためオンプレ機器（以下中継機とする）を設置し、ダイナミック VLAN を利用するユーザ通信のみ集約する。これにより主たるユーザ通信は AP から直接通信が可能となり、中継機が障害時にも主たるユーザ通信は継続利用が可能となる。

2023 年度までに JuniperMist と Aruba、CiscoMeraki のクラウド WLC 及び Cisco のオンプレ WLC で検証を実施した結果を表 1 に示す。

表 1　次期システム 2023 年調査結果

WLC 種別	クラウド			オンプレ
メーカ	Mist	Aruba	Meraki	Cisco
ダイナミック VLAN	○	○	△	○
Web リダイレクト	○	○	△	○
WLC・中継機障害	○	△	△	△
運用コスト	×	×	×	○

Meraki は中継機経由での IPv6 アサイン不可やクエリストリングの Web リダイレクト不可など製品として不十分であった。また Aruba と Meraki は radius 問い合わせが中継機経由となるため中継機障害時には AP 単体運用不可となる問題があった。Mist については AP4 台を購入して 1 年間の実運用を行ったが大きな問題もなく運用可能であった。ただし総じてクラウド WLC はサブスクリプションのコスト負荷が大きく、結果として既存同様オンプレ WLC を選択する結果となった。なお WLC 障害については機器の冗長化で信頼性を向上して対応した。

2.2　新システムで導入した機器

調査結果より 2024 年度に Cisco 社の表 2 の機器を導入した。既存機器は遠隔地を自律型としていたが、更新時には遠隔地も十分な通信帯域が確保されていたためすべての AP を集中管理型として導入した。AP は IEEE802.11ax まで対応した 2.4/5/6GHz の 3 帯域が利用できる機種となっている。

表 2　新システム導入機器

機器	機種名	台数
WLC	C9800-80	2 台冗長
検証用 WLC	C9800-L	1 台
AP	CW9162I	2,954 台

3　システム更新作業

3.1　更新スケジュール

2024 年 8 月までに導入業者と WLC の設置と設定を済ませ、9 月から 2025 年 3 月の 7 ヶ月で AP の更新を実施した。AP 更新の作業スケジュールを図 2 に示す。京都大学はメインキャンパスを地理的に 9 構内に分割してネットワークを構成しており、構内ごとに更新作業を実施した。

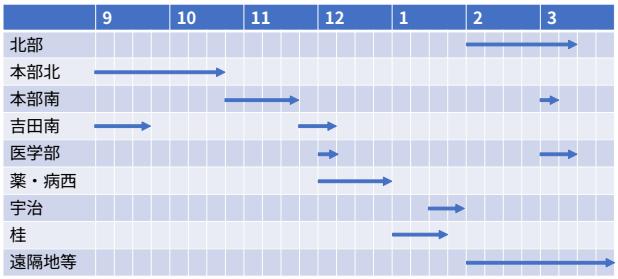

図 2　AP 更新スケジュール

まずは自身の組織の勤務場所である本部北構内の学術情報メディアセンターに先行して導入し問題点を洗い出した。次に授業期間の開始前に吉田南構内の講義室を優先して更新し、以降は構内ごとに順次すすめた。

またユーザへの通知と日程調整は下記のように 2 段階で実施した。

1. 2024 年 8 月上旬に事務連絡網により大まかなスケジュールを全学の事務担当者に通知
2. AP 更新の 2〜4 週間前に各建物の事務担当者と詳細日時を調整し、ユーザには事務担当者から通知

なお日程調整箇所が非常に多いため、作業日程表のエクセルファイルはクラウドサービスでファイル共有し最新情報を共有した。

また遠隔地については機器を現地の教職員に郵送して、現地の電気工事業者に交換設置作業をしてもらうよう依頼した。その際の作業費用は無線 LAN システムの更新予算での執行とした。

3.2 新たに用意した機能

3.2.1 遠隔 AP キッティング対応

従来新規購入した AP は AP の IP アドレスや WLC の IP アドレスをコンソールから手動で設定していたためキッティング作業が非常に煩雑で、さらに現地納品前に AP を一旦学術情報メディアセンターで受け取り現地に郵送する作業コストも必要だった。更新後から AP は現地に直接納品に変更し、AP の IP アドレスは DHCP、WLC の IP アドレスは DHCP オプション 43 にて設定する運用に変更した。

なお一括更新の場合は導入業者でテプラ貼り付けから現地設置工事までお願いしたが、今後新規購入した場合についても、業者から納品前に機器の MAC アドレスとシリアル番号を連絡してもらい、その機器の外箱に設置場所と機器本体にホスト名をテプラで貼り付ける「テプラサービス」を依頼して契約する。現地機器 MAC アドレスとシリアル番号から判別して、遠隔からでも AP キッティング作業が可能となる。

3.2.2 監視機能

WLC との通信が途絶えるなど AP の障害検知には、Cisco DNA Center においてサブスクリプションライセンスを契約する必要があるが、コスト的に導入が難しいため代替方法を検討した。

現在京都大学では約 1,600 台のネットワークスイッチ・ルータに対し Zabbix を用いて死活監視、通信量調査、リンクダウン検知、ループ検知、温度検知などを実施しており、当該機器を用いて同様に WLC と AP もヘルスチェックを実施できるか検討した。

3.2.1 のように動的に割り当てた個別 AP に対し IP アドレスによる死活監視が困難なため、WLC から SNMP トラップを受信して AP ホスト名の切断と接続を確認する。今回導入した Cisco 機器であれば下記の情報を受信して検知する。

- 1.3.6.1.4.1.14179.2.6.3.8 (bsnAPDisassociated)
- 1.3.6.1.4.1.9.9.513.0.4(ciscoLwappApAssociated)

同時に WLC 自身の死活監視、CPU メモリ利用量、接続クライアント数、温度検知なども実施する。なお通常運用において少数の切断監視であれば正確に検知できているが、計画停電などで数百台が同時に切断した場合は一部のトラップ情報の取得に失敗し検知が不完全となる問題を確認しており、その場合は計画停電前後の AP 一覧を比較して復旧確認を行う。

3.2.3 最新 AP 情報取得機能

3.2.1 で動的に割り当てた IP アドレスが不明のままだと、例えば AP 障害時の原因調査などの直接リモートログイン接続が難しくなど運用に支障がある。

今回導入した AP は LLDP が利用可能であり、WLC にてそれら情報が一括で取得可能である。WLC の CLI から全 AP のホスト名や IP アドレスが取得でき、LLDP 情報から接続したスイッチホスト名や接続したスイッチポート番号が取得できるため、以下のように対応した。

- Linux サーバにて定期的に WLC にログインし全 AP 情報と全 LLDP 情報を取得し保存
- AP ホスト名を引数にして AP やスイッチ情報をフックして整形表示するシェルスクリプト作成

AP 障害の検知や連絡を受けた際は下記対応となる。

1. Linux サーバにて AP ホスト名を引数に情報確認
2. AP にリモートログインして調査
3. AP 応答が不可ならスイッチにリモートログインして PoE を OFF、ON で強制再起動
4. それでも復旧しない場合は現地交換対応

3.2.4 00000JAPAN 動作検証

新サービスとして大規模災害時に無料開放される公衆無線 LAN「00000JAPAN」を導入した。

国立情報学研究所学術情報ネットワーク加入規約第６条の２に大規模災害時のネットワーク利用が認められていることから、SINET 回線を用いた「eduroam」のネットワークを認証なしで利用できる設定とした。またなるべく多くの方にご利用いただけるように接続する端末あたり 10Mbps の通信制限を設定した。

本サービスは通常運用時には設定を無効としており、要請に応じて設定を有効に切り替える。

3.2.5 OpenRoaming 動作検証

1.2.3 のように一般の学外者向けの公衆無線 LAN サービスのニーズがあるため、新サービスとして「OpenRoaming」の動作検証を行った。学内仮想基盤にて稼働させた Cisco Spaces Connector の仮想マシンを経由して、クラウド環境の Cisco Spaces を中継して複数の IdP で認証できることを確認した。今後は国立情報学研究所のサービス展開を待って最適なサービス提供方法を検討したいと考えている。

3.3 システム更新時の問題点とその対応

3.3.1 mac 端末での通信不安定

mac 端末において ping 応答において欠落が生じており通信不安定となる問題が確認されたが、5GHz 帯のチャネル幅を 20MHz から 40MHz に変更することで通信が安定することを確認しそのように変更した。

3.3.2 接続断の発生

利用端末の通信が切断し、再認証すると通信が回復する症状が何件も確認された。障害が確認された日時と機器の MAC アドレスから AP 切り替え発生時に FastTransition（IEEE802.11r）の失敗より再接続がエラーとなっていたことを確認し、FastTransition を無効とした。これにより radius 認証回数は増加することになるが、radius サーバの負荷としては問題なかったため無効での運用に変更した。

3.3.3 Android10 の Xperia 端末で接続不可

FastTransition を無効にした直後から Android10 の Xperia 端末で接続不可となる問題が確認された。FastTransition の機能をサポートするために、AP が端末向けに Device Analytics 情報を無線フレームに付与しているが、適切に処理できない特定の Android 端末で接続不可となる情報があり、この設定を無効にすることで接続不可を回避できた。

3.3.4 Android8 以下の端末で接続不可

旧 AP は WPA+WPA2 で運用しており、新 AP は WPA2+WPA3 を検討していたが、AP が混在する環境では WPA2 と WPA3 の切り替えエラーが懸念されたため、移行期間中は新 AP は一旦 WPA2 のみとした。すべての旧 AP の更新後に WPA3 を有効にしたが、その直後から Android8 以下の端末で接続不可となる問題が確認された。調査の結果、WPA の設定変更時に誤って PMF を必須としたことが原因で PMF 非対応の古い端末が接続不可となっていた。PMF を任意の設定に戻すことで復旧した。

3.3.5 一部 AP が 100Mbps/10Mbps でリンクアップ

新 AP を接続すると、1Gbps ではなく 100Mbps や 10Mbps でリンクアップするケースが数十件確認された。UTP ケーブル端子の最成端または UTP ケーブル交換にて概ね復旧した。なお、UTP ケーブル交換でも復旧しない機器についてはログを確認すると短時間にリンクアップダウンを繰り返しており、そのような AP 計 11 台については初期不良として機器交換して復旧させた。

3.3.6 吉田寮が更新不可

京都大学吉田寮において大学と寮生が係争中だったため工事業者が入館できず機器の更新ができなかった。将来的に機器更新を実施予定だが、旧 WLC の撤去のため遠隔から吉田寮の既設 AP18 台の集中管理型 OS を自律型 OS に変更して切り離し、自律用のコンフィグを投入して運用を継続した。

3.3.7 任意の AP が WLC と通信断

任意の稼働中の AP が WLC から切断する症状が 1 日あたり十数件発生する。調査すると下記の 3 パターンが確認されたが、どれも AP のログなどが確認できないため現在も根本原因が不明である。

- 通信が途絶えただけで数分後に復旧する
- AP が再起動しており起動後に復旧する
- AP が停止しており手動で再起動が必要となる

4 まとめ

- 最適なメーカの機器を選定し、WLC と約 3,000 台の AP の設置更新を 7 ヶ月間で実施した
- 運用に必要な監視機能の設定や AP 情報取得スクリプト作成、新たな無線 LAN サービスの検証を実施した
- 移行時に確認された問題点を調査し対応したが、未解決の問題もあり今後の課題である

参考文献

[1] 平成 27 年度国立大学法人等情報化発表会
「京都大学における無線 LAN の構築状況」針木剛 2015 年

[2] 総合技術研究会 2017
「全学無線 LAN での研究室 VLAN 接続サービスの構築」針木剛 2017 年