仙台高専広瀬キャンパス校内無線 LAN システムにおける学生 BYOD 環境の構築

菅野 浩徳, 脇山 俊一郎

仙台高等専門学校

Configuration of the BYOD Environment for Students on the Campus Wireless LAN System in National Institute of Technology, Sendai College, Hirose

Hironori KANNO, Shunichiro WAKIYAMA

National Institute of Technology, Sendai College

概要

ノートパソコンやタブレット，スマートフォンなど，多様かつ高性能な携帯型デバイスを学生も個人で所持できる時代となってきた．学生が所有するこれらのデバイスを学校での学習等に利用したい，との要求の高まりもあり，それらの校内無線 LAN システムへの接続について，申請による許可制として認めることとし，学生 BYOD（Bring Your Own Device）環境を構築した．本稿では，この学生 BYOD 環境の構築に関する検討とその構築の実際について報告する．

1 はじめに

学校教育の IT 化が進む中，教育機関への無線 LAN システムの導入が進められている [1]．仙台高専広瀬キャンパスでも教育利用を主目的に校内無線 LAN システムを導入し，現在，教室や実験室などに 60 台強の無線 LAN アクセスポイント（AP）を設置し運用している [2]．

大学・高専等の高等教育機関における教育に対しては，「学生の能動的な活動を取り入れた授業や学習法（アクティブラーニング）や双方向の授業展開など，教育方法の質的転換」が求められている [3]．

仙台高専は，国立高等専門学校機構（以下，高専機構）から，平成 25 年 9 月に明石高専と共に，アクティブラーニング推進拠点校に指定され，「全ての学生の能力を十分に伸ばす」ことを念頭に置いた新しい教育システムである A^3 を提唱し，その実施に取り組んでいる [4][5]．

本校ではこれまで，学生が個人で所有する情報デバイスの校内無線 LAN システムへの接続は認めて来なかった．しかし，アクティブラーニングの推進なども背景に，学生が個人で所有する携帯型情報デバイス（ノートパソコンやタブレット，スマートフォンなど）を，授業や自学自習等で使用できるようにしたい，という要求の高まりもあり，校内無線 LAN システムへの接続について，申請による許可制として認めることとし，この対応のため，電子的な利用申請や承認処理，未許可デバイスの通信遮断，などを可能とするシステムを導入し，学生 BYOD（Bring Your Own Device）環境を構築した．

本稿では，この学生 BYOD 環境の構築に関する検討とその構築の実際について報告する．

2 校内無線 LAN システム

2.1 機器

本校広瀬キャンパスでは，校内無線 LAN システムを 2 系統（主系統と副系統）運用している（**表 1**）．共に無線 LAN コントローラを備えた集中管理型である．

表 1 無線 LAN 機器

系統	コントローラ（台数）/ アクセスポイント（台数）
主	HP MSM760 Mobility Controller（2） HP MSM460 Dual Radio 802.1n AP（66）
副	Aruba 620 Controller（1） Aruba AP-135 Wireless Access Point（4）

主系統と副系統は並行稼働しており，認証方法など，

その利用において利用者側での顕著な違いが生じないよう配慮している．主系統の無線 LAN コントローラは信頼性確保のため冗長化構成とした．

稼働開始時期は，副系統システム（平成 24 年 9 月稼働）が主系統システム（平成 26 年 4 月稼働）よりも先であるが，信頼性（コントローラの二重化），拡張性（接続可能な AP 数）などの面で優位であることから，後から導入された HP MSM 系システムを，主系統システムと位置づけて運用している．

AP は普通教室（15 教室：3 クラス× 5 学年）全てと，視聴覚教室や共用実験室などに設置している．

2.2 認証方式

校内無線 LAN システムの接続認証は，高専統一認証基盤システムとの連携による．高専統一認証基盤システムは，高専機構本部および各国立高専に配備され，利用者 ID 管理データベース，RADIUS サーバ，LDAP サーバ機能などを備える．教職員は，このシステムで管理される利用者 ID（以下，統一認証 ID）を用いて，IEEE802.1X 認証により無線 LAN システムを利用する．授業などで不特定の教員や学生が使用する共用の PC やタブレットなど，IEEE802.1X 認証による接続認証に不向きなデバイスは，MAC アドレス認証による接続としている．このようなデバイスの MAC アドレスの認証システムへの登録は，デバイスを管理する教職員からの申請により管理者側で行っており，現在，300 台近くのデバイスを認証システムに登録し運用している．

本校は，広瀬キャンパスと名取キャンパスの 2 つのキャンパスを擁するが，それぞれのキャンパスに高専統一認証基盤システムが設置されており，統一認証 ID のデータは，両キャンパスのシステムおよび高専機構本部のシステムとの間で同期される．このため名取キャンパスの教職員も各自の統一認証 ID で広瀬キャンパスの校内無線 LAN システムを利用できる．

3 学生 BYOD 環境

3.1 検討

学生が個人で所有する情報デバイスの校内無線 LAN システムへの接続は，

- 授業や自己学習などの学習に用いること．
- クラブや学校として参加するコンテスト等の活動に用いること．
- 卒研や専攻研究での調査・研究に用いること．

など，学術的利用に限る．ゲーム機などの接続も，上記目的に合致するものであれば認められるが，単なる遊び目的であれば，許可できない．

本校には，高校生と同世代の学生も多く在籍することもあり，ネットワークの節度ある利用について，学生への意識付けを図るための方策の一つとして，申請による許可制とすることとした．申請には，利用申請するデバイスとその使用目的の記載を必須とし，管理者がその内容を確認し，許可・不許可を判断する．ここで管理者は，申請内容に対し性善寄りの立場をとる．

本校広瀬キャンパスの学生数は約 660 名（本科 3 学科・専攻科 1 専攻）であり，入学・卒業により，毎年 300 名程が入れ替わる．加えて，学生においては，1 人で複数台のデバイスを使用する，買い替え等により使用するデバイスが変更となる，など，その利用と許可に関わる多くの処理が日常的に発生することになる．

本校では，専任のネットワーク管理者はおらず，教職員が本務の傍らネットワーク管理にあたっているのが現状であり，平素より，その管理にかかる負荷は決して少なくない．学生からの利用申請を紙やメールで行う場合，認証システムへの登録を管理者が行うことになり，入力のための多大な負荷がかかる．加えて，デバイス識別のための MAC アドレスなどの入力ミスも懸念される．

これらを踏まえ，学生 BYOD 環境の構築に関しては，特に，以下を要件とした．

1. 学生側および運用管理側の利便性の確保および運用負荷の軽減のため，電子申請の機能を備えること．
2. 利用申請するデバイスを用いて利用申請処理ができ，そのデバイスの MAC アドレスを自動検知し，利用申請処理に反映する機能を有すること．
3. 未許可（未承認・未申請・不許可）デバイスを自動検知し遮断する機能を有すること．
4. 予め設定した期間利用の無いデバイスおよび使用許可期間を過ぎたデバイスを，自動的に使用不可とする機能を有すること．
5. IEEE802.1X 認証が可能であること．

これに対し，既存の無線 LAN システムおよび認証システムと連携して上記要件を満たす PFU iNetSec Smart Finder[6]（以下，SF）を採用し，学生 BYOD 環境を構築した．要件 1〜4 は，SF が，要件 5 は，無線 LAN システムおよび認証システムが担う．

学生 BYOD 環境では，SF が MAC アドレスに基づくデバイス認証（端末認証）を行い，認証システムが IEEE802.1X に基づく利用者認証（個人認証，本人認証）を行う，2 重認証を実現している．

デバイス認証のみでは，例えば，許可済みデバイスであれば，誰でも（本来許可を受けた利用者（学生）以外でも）そのデバイスを使用して，無線 LAN システムに接続できてしまう．また，そのデバイスを使用した利用者（学生）を特定することが容易でない．

当認証方式によれば，利用者認証も必要となるため，デバイスとその利用者（学生）の特定が比較的容易となり，また，学生の利用意識の向上にも資するものと考える．

IEEE802.1X 認証による利用者認証には，学生にも統一認証 ID が入学時に付与されており，校内の共用システム（教育用計算機システムや教務システムなど）の認証にも日常的に用いていることなどから，教職員の利用者認証と同様に，統一認証 ID を用いることとした．

高専統一認証基盤システムでは，利用者区分が設けてあり，本科や専攻科に在籍する一般の学生は「学生」，それ以外の短期留学生や研修生などは「学生 2」に区分される．この区分に基づいて，学生 BYOD 用に VLAN セグメントや IP アドレスブロック，ESSID などを新たに割り当てた（図 1）．

利用者区分	VLAN-ID	アドレスブロック	ESSID（無線LAN）	FWポリシー
学生 学生 2 （短期留学生・研修生等）	070	10.127.70.0/24	ESSID-U （IEEE802.1X 認証デバイス）	学内外アクセス不可 Webアクセス可（制限あり） （教職員からの申請により許可）
			ESSID-U-870 （IEEE802.1X 認証不可デバイス）	

※ VLAN-IDやアドレスブロックは実際とは異なる
※ ESSIDは仮名

図 1　学生 BYOD のネットワーク属性

学生 BYOD 用セグメントから，学内外へのアクセスについては，

- 学内の他のセグメント（研究室や教員室，事務室など）や学外（インターネットなど）へのアクセスは，デフォルトではすべてファイアウォールによって遮断する．授業や研究等でアクセスが必要となるホストやネットワークがあれば，教職員からの申請により許可する．
- 学外（インターネット上などの）サイトへの Web アクセスは，Web フィルタリングにより，安全性や健全性に問題があると思われるサイトへのアクセス制限を施す．授業や研究等でアクセスが必要となるサイトがあれば，教職員からの申請により許可する．

こととした．

IEEE802.1X 認証による接続が不可もしくは不向きなデバイスは，例外的に，MAC アドレス認証での接続を許可する．ESSID-U-870 は，この用途のために設けた．

学生 BYOD 環境での無線 LAN システムの接続仕様を表 2 に示す．

表 2　無線 LAN システムの接続仕様

仕様	
認証方式	IEEE802.1X PEAP/MSCHAPv2
セキュリティ	WPA2-Enterprise
暗号化	AES

3.2　構成

SF は，センサーとマネージャとで構成される．センサーは，申請画面出力や未許可（未承認・未申請・不許可）デバイスの通信遮断，などを担う機器で，監視対象セグメント（VLAN も可）に接続する．マネージャは，センサーの管理やセンサーで検出したデバイスの管理，利用申請に対する承認処理，などを担う．

今回，学生 BYOD 用 VLAN セグメントを監視対象セグメントとし，このセグメントを監視するようセンサーの接続と設定を行った．

マネージャはソフトウェア単体で提供されるため，それを動作させるハードウェア（IA サーバ等）も必要であった．学生 BYOD 環境は広瀬・名取の両キャンパスに構築する計画であり，広瀬キャンパスで先行的に構築し，その後，名取キャンパスに展開する．

そこで，マネージャを商用データセンターの仮想サーバサービス上に配置し，広瀬・名取の両キャンパスでマネージャを共用する構成とした．これは，キャンパス内にマネージャシステムを設置する場合との比較において，

- マネージャのハードウェアが不要となり，マネージャも 1 つで済むため，導入費用を抑えられること．
- マネージャのハードウェアの搬入・設置・調整・保守・撤去および資産管理などが不要となること．
- 停電や災害などによるシステム停止の懸念が少ないこと．

などの点で優位と判断した．なお，当構成の可否はベンダーにも事前に照会し，可，との回答を得て進めた．

3.3　利用

学生 BYOD の利用申請から利用までの流れを図 2 に示す．

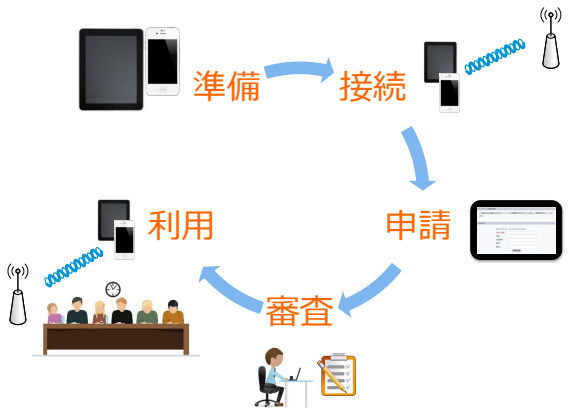

図 2　利用申請から利用までの流れ

準備　利用申請したいデバイスを用意する．校内無線 LAN システムの接続仕様，申請項目（申請者情報や機器情報），などを確認しておく．

接続　利用申請するデバイスを校内無線 LAN システムに接続し，統一認証 ID による認証（利用者認証）を行う．

申請　Web ブラウザで任意の URL にアクセスする．ブラウザに利用申請画面が表示されるので，申請項目（申請者情報や機器情報）を入力し，申請する．

審査　管理者はマネージャにて利用申請を確認し，その可否を審査して，「許可」もしくは「拒否」を設定する．その後，審査結果をメール等によって申請者に通知する．

利用　利用を「許可」されたデバイスで無線 LAN システムに接続（デバイス認証）し，統一認証 ID による認証（利用者認証）を行う．双方の認証を経て利用可となる．

運用においては，システム側の処理により，予め定めた期間（例えば 6 ヶ月間）無接続の場合には使用不可となるようにする．この場合は，再度，利用申請が必要となる．また，利用時間も，場合によっては，システム側の処理により，予め定めた時間（例えば 7:00〜20:00）以外での使用は不可となるよう制限を設ける．

3.4　セキュリティ対策

授業や研究，業務等に通常用いている情報デバイスと同様に，BYOD に用いる情報デバイスにおいても，マルウェアの検知・駆除や，不正な Web サイトのブロックなど，セキュリティ対策が施されていることが求められる．これについては，BYOD デバイスにおけるセキュリティ対策要件を定め，その要件を満たしたデバイスのみ，利用を許可する方針である．

加えて，日頃の生活においても，ネットワークを安全に安心して活用できるよう，特に，低学年からの，より実践的なセキュリティ教育や啓蒙活動などにより，学生のセキュリティスキルや意識の一層の向上を図ることが，喫緊の課題の一つと考えている．

4　おわりに

学生 BYOD 環境に関係するシステムの設定は完了しており，今後，本運用に向けて，学生への利用教育や利用マニュアルの整備，運用体制など，関係者による検討および準備を進める．本運用後は，学生 BYOD 環境についての定量的・定性的な評価により，その最適化を図る．

本校では，平成 29 年度に校内ネットワークシステムの更新（平成 30 年 4 月より正式稼働）が予定されており，無線 LAN システムの整備も含まれる．現在の無線 LAN システム（主系統）は継続使用の予定であり，新たに整備する無線 LAN システムとの共存と有効活用について検討を進めているところである．

参考文献

[1] 文部科学省：平成 26 年度学校における教育の情報化の実態等に関する調査結果（概要）(2015).

[2] 菅野浩徳，脇山俊一郎：仙台高専広瀬キャンパス校内無線 LAN システムの構成と運用，平成 28 年度電気関係学会東北支部連合大会講演論文集，2D05 (2016).

[3] 教育再生実行会議：これからの大学教育等の在り方について（第三次提言）(2013).

[4] 竹島久志，矢島邦昭，早川吉弘，奥村俊昭：仙台高専におけるアクティブラーニング推進に係る進捗報告〜大学教育再生加速プログラムを中心に〜，日本高専学会誌，Vol. 21, No. 2, pp. 9–12 (2016).

[5] A.Takahashi, Y.Kashiwaba, T.Okumura, T.Ando, K.Yajima, Y.Hayakawa, M.Takeshige and T.Uchida: A^3 Learning System: Advanced Active and Autonomous Learning System, *International Journal of Engineering Pedagogy*, Vol. 6, No. Issue2, pp. 52–58 (2016).

[6] PFU: IT 機器管理アプライアンス iNetSec Smart Finder, `http://www.pfu.fujitsu.com/inetsec/products/sf/`.