石川高専における教育研究利用持ち込み端末の管理運用方法

長岡 健一, 飯田 忠夫, 山田 悟

石川工業高等専門学校

{nagaoka，iida，satoru}@ishikawa-nct.ac.jp

概要： 石川高専では教職員，学生が持ち込む端末を，利便性を確保しつつ安全に利用できるようにするため L2 ベースの管理システムを導入している．本システム導入後 5 年が経過したが，管理運用に関わる負荷が大幅に軽減され，かつ安全に運用を行うことができている．また，システムに付属する統計ツールによって，持ち込み端末数やその内訳などが明らかになった．本稿では本システムの概要や現状について紹介し，運用の課題などについて報告を行う．

1 はじめに

近年，スマートフォンやタブレット端末など無線 LAN（Wi-Fi）の利用を前提としたワイヤレス端末の普及が進んでいる [1]．石川工業高等専門学校（以下，本校）でも例外ではなく，キャンパス LAN（Local Area Network）において無線 LAN を利用する持ち込み端末数は急激に増加している．

Wi-Fi や携帯端末の普及は，ユーザ側ではネットワーク利用の利便性を著しく向上させている一方，管理面においては，セキュリティを確保しつつ，安定して稼働させることが重要な課題となっている．本校では，2001 年にキャンパス無線 LAN が整備されたが [2]，その 5 年後である 2006 年から Radius（Remote Authentication Dial In User Service）による MAC（Media Access Control）認証を行って，ワイヤレス端末接続におけるセキュリティ確保に取組んできたが，2009 年には，さらなる利便性の向上とセキュア環境実現を目的として L2 ベースで管理できるシステムの導入を行っている．また 2011 年にはさらに多くの端末を管理できる上位システムへ移行した．本システムにより，持ち込み端末の利用および管理運用において一定の効果を挙げることができた．本報告では，このような本校の教育・研究用持ち込み端末の管理方法や運用状況などを紹介するとともに，課題についても考察する．

2 キャンパス LAN の概要

本校は，本科 5 学科（機械工学科，電気工学科，電子情報工学科，環境都市工学科，建築学科），専攻科 2 専攻（電子機械工学専攻，環境建設工学専攻）から構成され，学生約 1,100 名，教員約 75 名，事務系職員約 40 名からなる高等教育機関である．学生は，中学校を卒業したばかりの本科 1 年生から大学 4 年生に相当する専攻科 2 年生まで幅広く在籍している．

キャンパス LAN は学生寮を含む学内全域に敷設されており，教育・研究に活発に活用されている．その概要を図 1 に示す．情報処理センターに設置されているコアスイッチを中心に各学科棟は光ファイバーケーブルで接続され，ミドルスイッチ，エッジスイッチを介して各教室，研究室等からの LAN 利用が可能となっている．

ところで近年，ノートパソコンを利用した情報教育が盛んである．本校電子情報工学科では，入学時に学生にノートパソコンを持たせており，授業，実験や演習でこれを利用している．この場合，ネットワーク接続は無線 LAN を主に用いることになる．他学科においても，必須ではないが多くの学生はノートパソコンを所有し，課題の取り組みや自学等で活用している様子が多く見られる．また，学生寮ではほとんどの学生がパソコンをそれぞれの居室で利用している．さらにノートパソコンのみならずタブレット端末やスマートフォンの普及も著しい．このような携帯端末では無線 LAN によるネットワーク接続が一般的である．本校では 2001 年に学内のほぼ全域をカバーするキャンパス無線 LAN システムの運用を開始し，時代に合わせた更新をおこなってきた．現在稼働している無線 LAN システムは 2012 年に導入されている．

次に，本校キャンパス LAN は学科や用途ごとに 32 の VLAN に分けられており，大まかには図 2 に示すようなセキュリティ・ポリシーでグループ化されている [3]．このうち，「パブリックネットワーク」は学内のキャンパス無線 LAN，教室に設置されている情報コンセント，学生寮における LAN グループである．また，「ゲストユーザ用ネットワーク」は，本校で学会やセミナー，会議等で学外の利用者が一時的に接続する LAN グループである．それ以外の LAN グループでは，サーバや固定 IP アドレスで運用される端末の利用が中心となっている．後者の

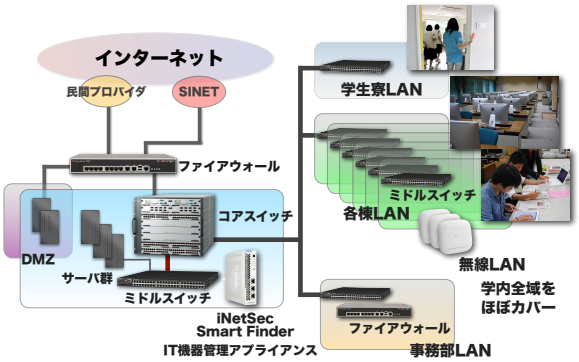


図 1: 本校キャンパス LAN の概要

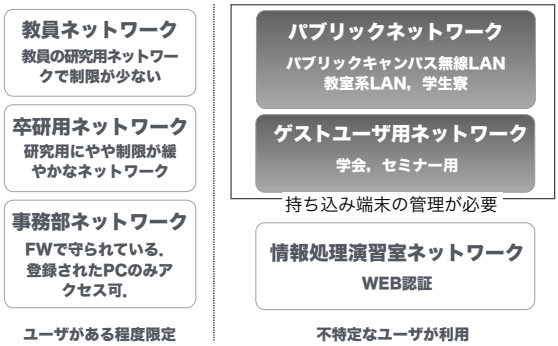
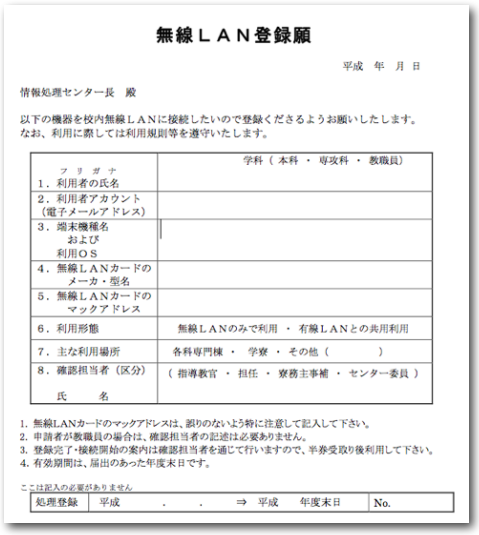


図 2: VLAN のポリシー

グループではユーザと端末がほぼ限定的であり，セキュリティが確保されているが，前者では不特定多数のユーザによるノートパソコン，携帯情報端末の持ち込み端末からの利用となり，トラブル発生時の対応やトレーサビリティ確保のためには，接続を許可するために何らかの認証を導入する必要がある．

3　MAC アドレス認証の導入

本校では，2001 年のキャンパス無線 LAN 導入当初は Wi-Fi 接続時の WEP パスワード以外にはアクセス制限はしていなかった．しかし，2003 年以降，電子情報工学科の学生が入学時からノートパソコンを持つことになり，2005 年頃からは学生寮の学生の半数以上がパソコンを持ち込むようになるなど，無線 LAN 利用の持ち込み端末が大幅に増加した．またこの時期，社会的にもセキュリティ確保の重要性がクローズアップされるようになった．以上のような背景から，不正なクライアントの接続を制限してキャンパス LAN のセキュリティを確保するため，2006 年，MAC アドレス認証の導入を行うこととした．このときの管理方法は，ユーザが図 3 のような書類による申請を行い，提出書類の情報をもとに，管理者が Radius サーバに MAC アドレスを登録することで接続を許可するというものであった．しかし，このような手続きは煩雑で，次のよう



無線ＬＡＮ登録願

平成　年　月　日

情報処理センター長　殿

以下の機器を校内無線ＬＡＮに接続したいので登録くださるようお願いいたします。
なお、利用に際しては利用規則等を遵守いたします。

フリガナ 1．利用者の氏名	学科（本科・専攻科・教職員）
2．利用者アカウント（電子メールアドレス）	
3．端末機種名および利用ＯＳ	
4．無線ＬＡＮカードのメーカ・型名	
5．無線ＬＡＮカードのマックアドレス	
6．利用形態	無線ＬＡＮのみで利用 ・ 有線ＬＡＮとの共用利用
7．主な利用場所	各科専門棟 ・ 学寮 ・ その他（　　）
8．確認担当者（区分） 氏　名	（指導教官 ・ 担任 ・ 寮務主事補 ・ センター委員）

1. 無線LANカードのマックアドレスは、誤りのないよう特に注意して記入して下さい。
2. 申請者が教職員の場合は、確認担当者の記述は必要ありません。
3. 登録完了・接続開始の案内は確認担当者を通じて行いますので、半券受取り後利用して下さい。
4. 有効期間は、届出のあった年度末日です。

ここは記入の必要がありません

処理登録	平成　.　.	⇒	平成　年度末日	No.

図 3: 書類による申請

に数々の問題を生じた．

1. 申請者の記入ミス
   - MAC アドレスの読み間違い．
   - MAC アドレスが何かわからないユーザの存在．
   - NIC（Network Interface Card）アダプタの選択ミス（無線で利用したいのに有線 NIC の MAC で申請）．
2. 管理者側の登録作業時の問題
   - 入力ミス．
   - ユーザ数が膨大になるにつれて登録に時間がかかってしまう．

3.1　iNetSec Patrol Cube の導入

このような問題を解決するため，2009 年，PFU 社製の iNetSec Patrol Cube[4] を導入した．これは，LAN 上の端末を把握するセンサと，センサを制御するマネージャソフトウェアからなっている．センサが接続されている VLAN においては，初めてアクセスしようとする端末に，図 4 のような申請画面をブラウザ上に表示させ，許可されていない間はその端末へのフレームは LAN 上で遮断する．ユーザは氏名や利用機器などの情報を入力し申請すると，その端末の MAC アドレスがマネージャに送られ，同時に管理者宛にメールで通知が届く．管理者はブラウザ上で申請内容を確認し，問題が無ければ登録を許可する．許可された端末へのフレームの遮断は解除され，設定された期間その状態が維持される．このシステムは次のように運用が簡単であり，低価格であった．

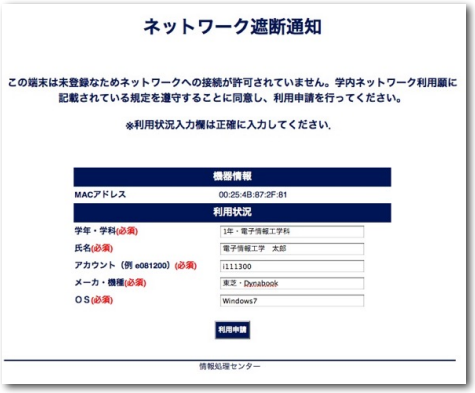


図 4: iNetSec での申請画面

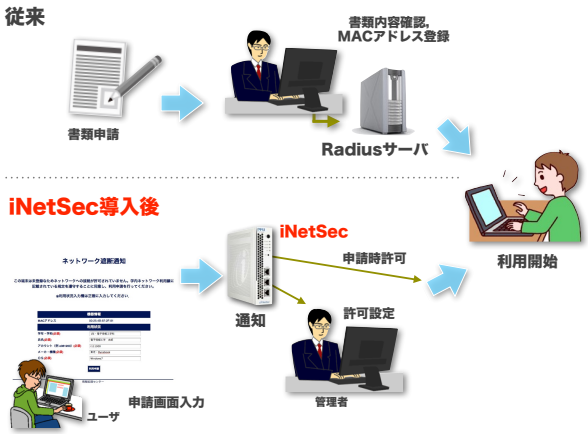


図 5: iNetSec 導入による管理利便性の向上

- 制限したい VLAN のセグメントにセンサを接続するだけ.
- 制限したい VLAN 分，センサを買うだけ.
- 不具合が起こったら抜くだけ.
- マネージャの操作も簡単.

高専においてはシステム管理者の人数も少なく，予算も限られており，iNetSec Patrol Cube は非常に有用であった．そして，従来と比較して作業にかかる労力や設定ミスの大幅軽減を実現できた（図 5）．なお，6ヶ月間に 1 度も接続がないと自動的に登録が削除されるようになっている．また，学会やセミナー開催時のゲスト用ネットワークにおいては，管理者の許可を必要としない「申請時許可」方式とし，最低限のトレーサビリティを確保することで運用を行っている．

3.2 iNetSec Smart Finder への移行

ここ数年，学内におけるスマートフォンやタブレット端末等の携帯端末の普及が著しい．本校では，学生への連絡等に Google Apps を利用しており，学生の携帯端末による LAN 接続を許可している．スマートフォンの普及に伴って登録申請が増加し，2011 年には，iNetSec Patrol Cube で登録できる MAC 数の上限 1,000 を超えた．このときの緊急処置としては，直近に使用していない端末を削除することで対応したが，そのままでは運用の破綻を迎えることが容易に予想されたため，登録 MAC 数の上限が 6,000 の上位システムである iNetSec Smart Finder[5] に移行を行った．これは，登録 MAC の上限数が多いことに加え，タグ VLAN に対応できることや，付属のチャートツール（iNetSec Smart Finder Chart）によって，統計情報の集約が行えるようになっており，これらも移行を決定した要因となった．

4 利用統計

前述の iNetSec Smart Finder Chart は，iNetSec Smart Finder で管理されている端末の統計情報として，以下のような項目が調査でき，図 6 のようにグラフィカルに確認が可能である．

1. 登録機器の統計情報
2. 印刷量の統計情報
3. 電力使用量の統計情報

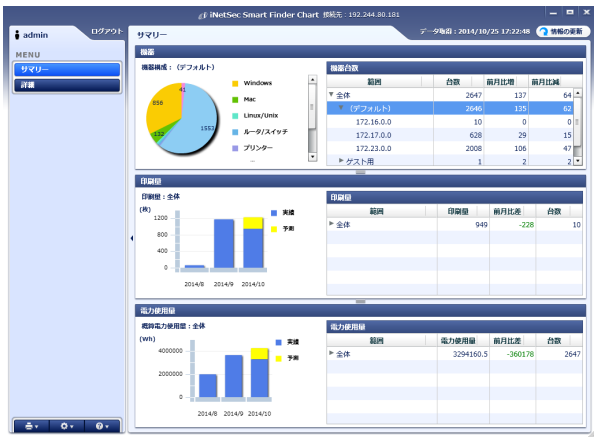
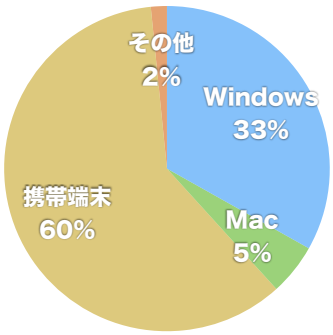
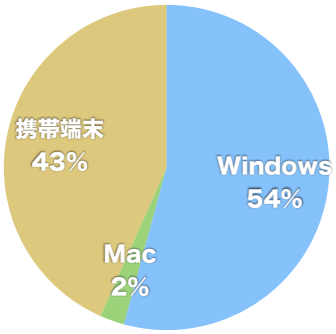


図 6: iNetSec Smart Finder Chart

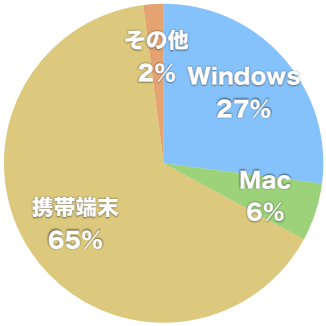
ここでは，上記 1. 登録機器の統計情報について示す．キャンパス LAN に接続を申請した持ち込み端末は，2014 年 10 月 25 日現在で 2,647 台あり，その内の 1,553 件が携帯端末であった．ここで，携帯端末とはスマートフォンやタブレット端末である．また，2 年前の 2012 年 10 月には，全体の機器数は 1,191 台であり，2 年間で約 2.2 倍の数に増加したことがわかる．さらに，登録されている端末種類の内訳は図 7 のようになっている．このうち図 7(a) から図 7(c) はそれぞれ，学生寮を含むキャンパス全体，学生寮，学生寮を除くキャンパス内について示している．



(a) キャンパス全体



(b) 学生寮



(c) 学生寮を除くキャンパス内

図 7: 登録内訳

図 7(a) より，学生寮を含むキャンパス全体では，携帯端末が 60 パーセントを占めていることがわかる．ただし，図 7(b) の学生寮のみを見ると，携帯端末の割合は 43 パーセントと半数を下回っている．学生寮ではほとんどの学生が各居室にパソコンを持ち込んでいるため，相対的に携帯端末の割合が少なくなっていると考えられる．また，図 7(c) の，学生寮を除いたキャンパス内では，携帯端末は 65 パーセントとなっており，その占める割合はより高くなっていることがわかる．教室等で利用する端末はパソコンよりもスマートフォンやタブレット端末が多いためであると考えられる．ちなみに，学生寮を含むキャンパス全体の 2012 年 5 月の調査では，携帯端末の占める割合は 47 パーセントであった．2 年半の間に携帯端末の普及がより顕著になっていることがうかがえる．

5　運用における課題

iNetSec の導入以降 5 年が経過したが，いくつかの課題も見えてきている．まず，ユーザからの虚偽申請への対応である．最近では携帯ゲーム機にも Wi-Fi が搭載されているため，これによる無線 LAN の利用を申請するケースがある．本校ではゲーム機の Wi-Fi 利用は認めていないため許可しないが，これをスマートフォンやパソコンと偽って申請する悪質な事例もある．ほとんどは iNetSec Smart Finder でゲーム機の識別は可能であるが，一部識別できないものがある．また，まれではあるが，サポートが終了した Windows XP での利用申請などもある（誤検知の確率も高い）．このように判断が難しい申請については，個別にユーザに問い合わせ確認を行うことで対処している．さらに，許可後のユーザへの通知がシステムで自動では行われないため，ユーザ自身は申請が許可されたかどうかわからない．管理者側で許可作業に漏れがあった場合には許可されないままになる可能性がある．現状はシステムの改善を待つとともに，許可作業に漏れがないように努めている．

6　むすび

石川高専における持ち込み端末の管理運用方法および利用状況を報告し，現状の課題について考察した．本校で導入した管理システムにより，我々の管理運用における負荷も軽減され，ユーザの利便性も向上した．管理規模やコストを考慮すると有用であったと考えられる．スマートフォンやタブレット端末の普及に伴って，ここ数年で大幅に教育・研究用持ち込み端末が増加したことが明らかになったが，今後もしばらくはこの傾向が続くと思われる．しばらくは，他機関の情報を収集しながら最善の管理運用方法に対する模索が続くが，安全で快適な研究・教育環境を提供できるようにしていきたいと考えている．

参考文献

[1] 総務省, 情報通信白書平成 24 年度版，2012.

[2] 長岡健一，“学内ギガビットイーサネットの紹介”，石川工業高等専門学校 情報処理センター広報，Vol.6, No.1，pp.38-42，2002.

[3] 長岡健一，山田悟，山畑章，“学内 LAN のポリシー別ネットワーク分離”，第 30 回高専情報処理教育研究集会論文集, pp.293-296, 2010.

[4] PFU, 不正 PC 検知・遮断アプライアンス iNetSec Patrol Cube, http://www.pfu.fujitsu.com/inetsec/products/pc/

[5] PFU, 不正接続防止なら iNetSec Smart Finder, http://www.pfu.fujitsu.com/inetsec/products/sf/