サイバー空間を活用した新しい学習環境の構築

藤本竜之介[†‡]　飯村伊智郎[†]　國藤進[‡]　松野了二[†]　津曲隆[†]

† 熊本県立大学　総合管理学部
‡ 北陸先端科学技術大学院大学　知識科学研究科

1. はじめに

コンピュータとインターネットを活用したｅラーニングを、教育に積極的に導入しようとする動きが活発である。時間的・地理的制約から教育を解放する可能性を持つため、特にユニバーサル化[(1)]の段階に入り多様な学生を対象とせざるを得なくなったわが国の高等教育では今後――中期的な将来展望の中でだが――必要不可欠なものになっていくものと予測される。実際、文部科学省は遠隔学習による単位取得を大学や大学院において大幅に緩和しており、わが国の高等教育でｅラーニングを推進する体制は既に整っている。運用に至るまでの現場での諸問題を解消できれば普及は時間の問題だと考えられる。

保守的イメージの強い教育界であるが、こういった新しい教育技術の導入には案外と積極的である。流行に関し敏感なのは、大学の場合、教員の研究活動の影響が大きい。常に新しいことにチャレンジする土壌の存在が先端的な教育技術の導入を手助けしている。もっともそういった内部的要因だけでは実験的レベルを超えることはないだろう。それが大学、さらに初等中等教育にまで普及するレベルに達するのは、巨大な市場である教育界に向けた産業界からの後押しといった外部要因が大きく寄与している。

このような内部や外部の要因に駆動されて、教育技術の流行は生み出されているのだが、最近の流行と言えば、CAI (Computer Assisted Instruction) が挙げられよう。CAI は、教育の中でも特に自己学習を強力に支援するツールとして――導入当初は、教育現場で大きな混乱をもたらしたようだが――、わが国では1980年代の後半に導入が本格化した[(2)]。そして、当時のスタンドアロン型のコンピュータとCD-ROM等の大容量メディアを組み合わせることで従来に比べて高度なインタラクティブ性を備えたリッチな教育コンテンツを提供できることから、一定の教育成果を上げてきたのではないかと考えられる。またこれは、純粋な教育面以外に重要な副産物ももたらした。すなわち、CAI の導入が、準静的プロセスの如く情報化を不可逆的に進行させ、教育界をコンピュータ環境に馴化させることになった。それ以降、学習や教育活動の有り様は大きく変化した。例えば、ワープロや電子メール無しに高等教育を行うことは現在では考え

られないと思うが、CAI の導入が、そういった状況をキャンパス内に生みだす契機となったのである[3,4]。教育界のこのような情報環境の変貌が、今日のｅラーニング導入の下準備をすることに繋がっていく。

優れたコンテンツの提供を可能にする CAI であるが、基本的な方向性としては、従来の教育スタイルの延長線上に位置づけられると考えてよい。ｅラーニングも基本的に同じである。ｅラーニングという新語の誕生によって、それまでと異なる新しい教育形態が芽生えているかの印象も受けるが、必ずしもそういうことではない。ｅラーニングの特徴である時間的・地理的制約からの解放という意味であれば、コンピュータを活用しなくても、以前から通信教育でも行われてきたことであって、ｅラーニングによって先の制約が初めて解放されるわけではない。そのため、これまでに論じられている意味でのｅラーニングというのは、基本的に従来の教育スタイルの枠組みの中で、これまでの遠隔教育のスタイルを発展させるツールとして理解すべきものである。

ところで、従来の教育スタイルと上で述べたが、これは「学習は個人的営みである」というテーゼを基本にした教育スタイルを指している。たかだか近代になって誕生した考え方に相違ないこのテーゼは、時代を重ねる中で多くの現代人の意識の深層に沈降して、現代社会におけるひとつの常識を形作っている。当初はいくつもの可能的様態が存在していたに違いない教育機関が、この社会常識とさらに学習を「知識の獲得過程」として捉えることで、個人に対して知識を単方向的に教授することを使命とする機関へと収斂していくことになる。

教育機関のあり方についてのこういった考え方は見事なまでに現在の学校建築の中に表現されている。学校建築に長く従事してきた上野淳によれば、近代日本の学校建築は明治中期頃に完成し、以降100年間、この原型にはほとんど変化はないという[5]。原型とは専門的には「片廊下一文字型校舎」、通称「ようかん型」又は「ハモニカ型」の校舎のことである。南向きに教室、北側に廊下を配置した日本人にとって馴染み深い校舎であり、小学校から大学に至るまで採用されている方式である。この構造の教室では、教師が教卓に立ち、学生全員がそれと正対する形となり、知識のマルチキャスト送信にとって都合の良い１対多の写像関係を強要することになる。当然ながら、そこには学生間の相互作

用ということはほとんど考慮されていない。特に大学で見かける教卓を中心に机・椅子が同心円状に配置され、さらにそれらが床に固定されている大教室等になると、学生間の相互作用に対する配慮は皆無である。

学習が個人的営みであるとの立場に立つならば、相互作用の排除は当然のことである。さらに、この相互作用排除の思想は教室以外の場所においても徹底されている。例えば、図書館。閲覧室で静寂さを要求する図書館という存在は、紛れもなく学習が個人的営みであるとの意識の反映とみなしてよいであろう。その意味で、図書館もこれまでの教育スタイルをキャンパス上で表象している建築物のひとつと言える。図書館に限らず、それ以外の場所でも、学生達の相互作用を積極的に生みだす空間作りを行っているキャンパスはほとんど見受けられない。この意味で、現在のキャンパスは学習者間に相互作用のない離散的な学習環境を基本に構築されていると言ってよいだろう。

個人という近代の産物を思想的枠組みの中心におき、個人の知識獲得の速度を加速するツールとして最新テクノロジはこれまで導入され続けてきたのである。先に述べたように、昨今導入されようとしているｅラーニングもこの思想の枠組みの中にあって、基本的に、CAI と同じく自己学習の支援を主目的にしている。学習が個人的営みとの意識は現在も依然と力強いものがある。もちろん、この考え方は確かな奔流となるべきものとも考えられるのであるが、ところが、近年になってこの流れとは異なる動きが芽生えてきている。新しい流れとは、本論の中で詳しく論じることになるが、学習は集団の中で行われることが本質的であるとする新しい学習観の台頭である。この学習観は、現代の教育改革を促すことになり、そのために教育の現場ではこれまで行われてきた「教える（teaching)」から「学び（learning)」をキーワードとする教育の方向へと方針転換が迫られるようになってきているのである。

ところが、方針転換を行うと言っても、人の行動は不可避的に建築空間の有り様によって規定される。このため、旧来の学校建築においては人の行動は旧来の考え方の枠組みに拘束されてしまうことになり、そこに無理に新しい枠組みを組み込もうとしてもどこかに歪みが生じるだけである。こういった状況では、自然に、“新しい葡萄酒には新しい革袋を”といったきまり文句が想起され

るが、しかしそれが簡単に実現できるはずもない。既存のキャンパスを新しい流れを包摂する革袋として改築することは現実問題としては夢物語に近いものがある。

本研究は、この問題に取り組むものである。従来のパラダイムの下で建設されているリアル空間内のキャンパスに、物理的な改良を施すことなく、新しい流れを組み込むひとつの試みである。筆者らはサイバー空間の活用によってこの問題をクリアできないかと考えている。すなわち、従来の思想で構築されたリアル空間にｅラーニングによるサイバー空間を重畳させ、両者が相互補完的に機能するようにデザインすることで、従来のパラダイム下にあるリアル空間が持つ拘束を弱めた新しいキャンパス（ユビキタスラーニングキャンパス）を創出しようと考えているのである。このため、筆者らは、ｅラーニングを講義補足あるいは自己学習のための加速化ツールという従来の見方で捉えるのではなく、旧来パラダイムにある現実のキャンパスに新しい意味を付与するための戦略的ツールとして捉える必要があると考えている。

先に引用した上野の著書「未来の学校建築」の副題は「教育改革をささえる空間づくり」であった。本研究もこれと同様でｅラーニングを建築ツールとして、大学の教育改革をささえる学習環境づくりを狙うものである。ｅラーニングで構築されるサイバー空間の活用によってキャンパスを「教える」ための空間から「学び」の空間へと変えることを目指している。もちろん簡単なことではないだろう。しかし、ともかく第一歩を踏み出そうと思う。その手始めとして、本論文は特にサイバー空間のハードウェア的基礎となるネットワークインフラを中心に述べる。

2. 変革期にある学習環境

2.1. 従来の学習環境――ようかん型校舎の思想

前章でも引用した建築計画を専攻する上野淳は、従来の学校――上野の言葉を借用すれば「20世紀の学校」――について以下のように表現している：

> 20世紀の学校の姿とは「教える学校」であった。閉鎖的な教室で、40名の均質的・固定的な集団に、黒板と教科書で、一斉的に一定の知識を教え込んでいくのが「学校」の姿であったといえる。これには、「気が散らないように」できた閉鎖的な教室を廊下に沿って単調に並べていく方式が最もふさわしかったのである。（文献(5)、p.168）

20世紀は、生徒の知識獲得において「教える」を教育のキーワードとし、それを具現化する建築物として、全国津々浦々に「ようかん型」の校舎が次々と建設されていったわけである。明治期を出発点とする20世紀型の学校パラダイムの流れの慣性は大きく、このパラダイムは以後もほぼ不変のまま維持され、その結果、現代においても教育機関における学習活動では教えることが最前面に出てくることになる。

熊本県立大学においても、現在の旧講義棟は1980年に現在地に移転してきたときに建設されたものだが、見事なまでに片廊下式の「ようかん型」校舎の理念が踏襲されていることは一目瞭然である。また、男女共学化に伴い熊本女子大学から熊本県立大学に改称した1994年、総合管理学部が新設されたのを契機に竣工した新講義棟は、さすがに片廊下式については幾分崩れているものの、基本的に教室の構造は「教える」思想から寸分も逸脱していない。また、同時期に完成し、今後ｅラーニングを実施するには重要な役割を果たすはずの情報処理実習室でさえも基本的に「教える」思想を具体化したレイアウトが採用されている。導入された機器は最新のものであったが、それを活用する思想は愚直なまでに旧来のままであった。20世紀の世紀末になっても「教える」ことを基本にしたパラダイムが、熊本県立大学に限らず、多くの大学で忠実に受け継がれてきたのではないかと考えられる。

20世紀の学校パラダイム下では、「教える」ことで知識を伝授することが学生又は生徒・児童たちの学習（＝知識獲得）活動そのものであると見なされていた。だから「ようかん型」校舎が普及していったわけである。そのパラダイムでは、「教える」ことと「学習する」こととがほぼイコールで結ばれていた。結論的に言えば、両者は概念的に明瞭に分離する必要があるのだが、これまではそれらが渾然一体となって両概念は同一視されてきた感がある。ところが、近

年の認知科学はその認識が誤っていることを教えてくれる。

2.2. 認知科学的視点から眺めた学習

認知科学においては、状況的認知（situated cognition）、あるいは分散認知（distributed cognition）といった概念で捉えられているが、知識とは個人に閉じたようなものではなくて、個人とそれを取り巻く環境あるいは状況に分かちもたれている[6]、とする説が有力である。アフォーダンス理論[7,8]を創始したJ.J.Gibsonなどもこの立場にあって、この流派の状況的認知科学者は知性でさえも個人に閉じたものではなく、状況の中で生まれるとしている[9]。このように、近年の認知科学の知見からすれば、個人的な営みというのは学習の必要条件にはなるであろうが、しかしそれだけでは学習のための十分条件とはならないのである。学習という行為は従来考えられていた以上にずっと複雑なものであり、このため、20世紀型の学校の特徴である1対多写像型の教室空間は「教える」場にはなりえても、「学習」の場としては不十分なものでしかない。この意味で、現在の学習環境は変革せざるを得ない時期に来ているのである。

ところで、学習とは知識の獲得過程であると述べたが、この考え方も近年の新しい学習観においては大幅に修正されている。新しい学習観は、LaveとWengerによる状況的学習理論の研究を起点としている。彼女らは、長年のフィールドワークによって得た知見から学習を次のように定式化した[10]。それによれば、学習とは、彼女らが実践の共同体と呼んでいる共同体において、周辺的位置から中心位置へと参加者（＝学習者）が移動する過程と考える。学習を個人の知識獲得過程と考えていたのとは異なり、Laveらは、それだけでなく何らかの社会的実践に役割を持って共同体に参加することを学習の本質であると主張したのである。個人の内部だけで生起するのではなく、学習は状況の中に埋め込まれているというLaveらが主張するこの新しい学習観は教育界でもすでに標準的なものになっている。さらに今日では教育界だけに留まらない。企業組織でも注目され、社会的に新しい学習観の認知は進んでいるようである——成果主義の導入によって、まるで20世紀の学校的パラダイムに汚染されたかのように個人が極度にクローズアップされ、そのことで生じた弊害から、企業でも実

践の共同体を基礎とする新しい学習観が重要視されるようになっている(11)。新しい学習観において重要な点は、学習のためには、他者（特に練度の異なる複数の他者）から成る共同体を土壌として必要とするということである。このため、「学習」と「教える」ことを概念的に分離せずに、学習を個人的営為とみなしてきた旧来のパラダイムの下では新しい学習観を実践するのは極めて困難となる。

2.3. 新しい学習観の具現化——公立はこだて未来大学の場合

ユニバーサル化を一足早く経験し、多様な学生を相手にする必要に迫られた米国の大学などでは、高等教育の教育改革はわが国よりも進んでいる。その取組みの中で象徴的なのが、新しい学習観の導入であり、従来の「教える」パラダイムから「学習する」パラダイムへと向かった変革であろう。そのための道具立てとして学生の講義への参加そしてさらに学生相互の協同作業が実践されている(12)。新しいパラダイムでは、主体が学生となり、学生による協同学習を推進し、その協同学習が活性化するように裏方で演出することが教師の役割となる。このスタイルにおいては教師と学生間の１対多の写像関係は自然に消滅する。

わが国でも先進的な大学においてはこのような取組みが既に始まっていることは言うまでもない。さらに、それに留まらずキャンパス内のハードウェア自体を新しい学習観に適合するよう建設した大学なども出現している。公立はこだて未来大学がその典型例であるが、世紀の変わり目の2000年４月に開学した真新しいこの大学は、20世紀型の従来の学習観とは決別し、「教える」ではなく「学び」をキーワードにキャンパス全体のデザインが施され、その結果従来とはかなり異なる様相を持つキャンパスが出現している(13)。このキャンパスには、新しい学習観をキャンパスに埋め込むために斬新なアイデアが随所に盛り込まれている。そのいくつかをここで紹介しておきたい。

この新しい大学では、様々な「仕切り」を外すことで閉じた空間を排除する建築デザインを随所に採用している。例えば、ガラス張りの教室であるとか、さらには人々が往来する空間に仕切りのない図１のような円形教室をおくなど

して、他者に対して開放的な状況を作り出し、共同体内のアクター同士の相互作用が生まれやすくしてある。また、机、椅子、ホワイドボード、スクリーン、プロジェクタなど全てを可動式にした教室が複数設置してある。単にグループ活動の机が設置してあるのではなく、全てが可動式であることがグループ活動には本質的に重要になるようであり、それを生かして従来の教える授業とは異なる、学習のための授業への取組みがこの教室では盛んに行われているようである。さらに時間外の学習支援のために、ガラス張りの教員研究室の前にスタジオと呼ばれる学生用のグループ活動できる机が用意され、学生は遅くまでそこでグループ学習を行える環境が整備されている（図１の奥に見えるスペースがそれである)。蛇足であるが、教員研究室がガラス張りにしてあるのもスタジオを利用して学習している学生たちと教員との日常的な相互作用を生み出すための工夫に他ならないことを付け加えておきたい。このスタジオのアイデアの秀逸さを紹介するために、文献（13）からスタジオの利用の様子が記述されている部分を以下に引用しておく：

> 「近ごろの学生は大学にいつかない」とよく言われるが、この場所を作ってみると、それは今まで居場所がなかったからではないかと気づく。（中略）共同で問題を解くことや、教え合うことなどを、この場所は可能にしている。ある学生の日記から――「バイトなどが終わったら、また学校に来て勉強します。(中略)「ねえ、ちょっと」と言えば、「うん？」って振り向ける余裕があります。だからみんな気軽に時々話しつつ勉強しています」。
>
> 学生は全員ノート型パソコンを持っており、すべての机には電源や情報コンセントがある。（文献(13)，p.90より引用）

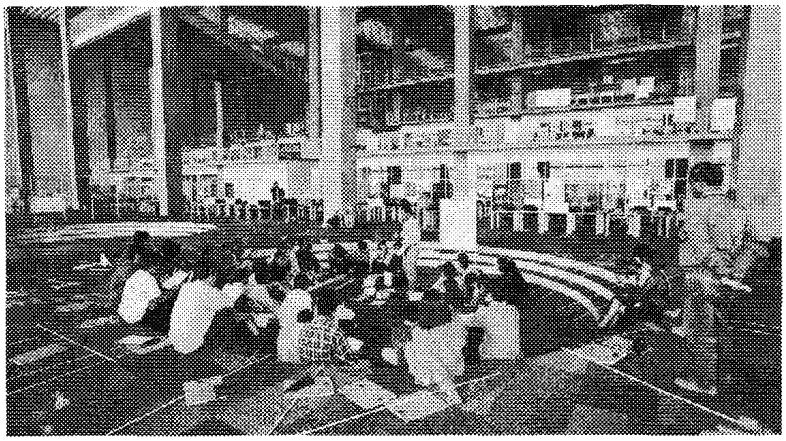

図１　公立はこだて未来大学の一授業風景（文献(13)から引用）

このようにハードウェアとして開放的な空間を創出している先見性は見事というほかない。従来型のキャンパスにはない斬新な工夫が他にも色々なされているが、紹介はここまでにしておきたい。

2.4.「学び」を支援するキャンパスの創出―― eラーニングの新たな可能性

新しい学習観からほど遠い従来型のキャンパスに立っていると、公立はこだて未来大学の保有するリアル空間の優秀さを実感せざるを得ない。目映いばかりであるが、これを既存のキャンパスに物理的に実現するのはほとんど絶望的であると言ってよいだろう。しかし、そうかといって、ただ手をこまねいているだけでは、永遠に新しい学習観を実践できるキャンパスは実現できない。今後、大学全入時代を迎え教育の充実が叫ばれる時代になれば尚更ながら、学びを支援するキャンパスを学生に提供することは必須になるものと考えられる。

リアルな空間において、それを物理的な改良によって対処できないという制約条件下で、様々な思考実験を繰り返していけば、次元の異なる別の空間――サイバー空間――を活用することで実質的な改良ができるのではないかとの着想に自然とたどり着く。恐らくその解しかないだろうと考えているが、そのためのヒントになる実践を新井紀子らが行っている[14,15]。新井らはサイバー空間上にｅラーニングによる情報共有コミュニティを構築し、そこで学びを生み出せる可能性に言及している。実際にネット上の学びの場として「ｅ-教室」を主催し、そこでは子供たち200人以上が参加して自主的に勉強しているようである。そこには、様々な人々が参加する実践の共同体が形成されており、相互に学び合う学習空間が構築されている。新井らの研究からわかるように、ｅラーニングはまさにこういった学びを創発するためのツールとしての利用価値を内在させており、従来の延長線で考えられてきた以上に高いポテンシャルを秘めている。

先にも述べたように、教育改革が叫ばれる中、今後のキャンパスは、リアルな空間の中に如何に学びの環境を提供できるかが問われていくことになるだろう。本研究は、学習環境の変革期にある現在、新井らのようにｅラーニングを遠隔教育の主目的に捉えるだけでなく、ｅラーニングで構築されたサイバー空

間を利用することでリアルなキャンパスに付加価値を与えて、キャンパスで活動する現実の学生たちの間に学びを創出するための試みである。また、現在のｅラーニングについての議論のほとんどは、基本的に従来のパラダイムの中にあって、ｅラーニング（e-Learning）というよりはｅティーチング（e-Teaching）の研究になっていることが多い。それゆえ、この試みは、実空間との協調の中でｅラーニングを字義通りに活用するための提案にもなっていることを追記しておく。

3. 新たな学習観に基づく学習環境とネットワーク技術

２章で述べたように学内キャンパスに現有する建物や設備を活かし、新たな学習観に基づく学習環境を構築するには、サイバー空間を活用することがそのひとつの解となりえる。本章では実際にサイバー空間をキャンパス内に具体化していくために必須となるネットワーク技術について述べる。本学のネットワークインフラは平成16年にその基盤が構築[16]されているが、各棟内のIPアドレスは静的に割り当てられている。そのため、教室や研究室においては、割り当てられたIPアドレスをクライアントPCに設定することで学内LANに接続することが可能となる。しかし、情報コンセントの数は基本的に１つの部屋に１つしかない。そのため、１教室や１研究室で複数のPCを利用するには、必要台数分のHUBを接続するか、DHCPサーバ機能を有するルータを接続する必要がある。

新たな学習観に基づく学習環境を構築するにあたって、本研究ではこれまでに学習環境としての整備が進んでいない学生食堂や学生ロビーなどに注目している。これらの環境では新たにLANケーブルを常設することが困難であるため、近年脚光を浴び始めている無線LAN技術を利用し、動的にIPアドレスを割り当てるネットワークインフラを構築する必要がある。本章では、無線LAN技術の概要から技術的問題を解決する新たな標準規格について解説し、本学において構築したネットワークインフラの構成について述べる。その後、実際に無線LANによる学習環境として稼動させ、ある講義における演習を通して学習環境

としての有用性を検証し、同時に学生の視点からみた学習環境に対する要望やニーズを踏まえて考察する。

3.1.　無線 LAN 技術の概要と課題

現在、ワイヤレス機器はいたるところで使われており、コーヒーショップや空港、スポーツの競技場などさまざまな場所に公衆無線 LAN スポットが設置されるようになっている。2005年のワイヤレス機器の年間販売台数は、ノート PC、携帯電話、PDA (Personal Digital Assistant) を中心に数千万に達すると見られており、現在のノート PC は、ほとんどが Wi-Fi の名称で広く知られる無線 LAN 技術の標準規格である802.11[(17)]に対応している。

802.11 は IEEE (Institute of Electrical and Electronics Engineers Inc.) によって策定された無線 LAN に関する一連の仕様群である。現在、802.11 は世界中で急速に普及しているが、それでもなお 802.11 には多くの技術的な課題が存在する。中でも大きいのは、無線信号到達範囲の問題である。現在、802.11 のアクセスポイントからクライアント機器が妥当な強度の無線信号を受信できるのは、壁などの大きな障害物がない場合で最長約300フィート（約90メートル）以内に限られている。そしてもう１つの大きな問題がセキュリティである。

Wi-Fi/802.11 の起源は、1985年に FCC (Federal Communications Commission) がいくつかの無線周波数帯域を政府の許可なしに利用できるように開放することを決定したことにまでさかのぼる。いわゆる「ガーベージ・バンド」と呼ばれるこの周波数帯域は、電波を使って食品を加熱する電子レンジなどの機器にすでに割り当てられていた。このため、これらの周波数帯を無線通信に使用するには、「スペクトル拡散」テクノロジを利用する必要があった。これは、無線信号を広い周波数帯域に拡散させて送信することで、信号に対する干渉や傍受を避けようというものである。

当初、業界はワイヤレス・ネットワークにおける機器のセキュリティに関して楽観的な見方をしていた。しかしワイヤレス・テクノロジが本来想定されていなかったインフラストラクチャにまで採用されるようになったこともあって、セキュリティの問題は今でも大きな課題として残っている。ワイヤレスへのス

ムーズな移行を阻む基本的な要因としては、以下の点が挙げられる。

- インターネットは本来、ネットワーク上に固定された端末機器を前提に設計されており、モバイル・コンピューティングは想定していないこと。
- ワイヤレス・ネットワーク上ではユーザーが自分自身を認証する手段がないこと。伝統的なネットワーク上では、認証手段はユーザ・アカウントの作成時に情報部門から提供されていた。
- ほとんどのアプリケーションやオペレーティング・システムは固定的なネットワーク構成を前提に設計されていること。このような構成では、ユーザーがネットワークから切断すると致命的なエラーを生じることがある。しかしワイヤレス・ネットワークの場合、ユーザーが移動するたびにネットワークからの切断が頻繁に発生する。
- 有線ネットワークと異なり、ワイヤレス・テクノロジではネットワーク・トラフィックがケーブルや壁などの物理的な拘束を受けないこと。オフィス・ビル外部の公衆スペースに漏れたトラフィックを第三者が盗聴したり、不正なメッセージをワイヤレス・ネットワーク経由で送信されたりすることもある。

IEEE 802.11 の最初の規格は1999年に発表され、この中には機密性を確保するための暗号化オプションも含まれていた。WEP (Wired Equivalent Privacy) と呼ばれるこの方式は、「無線 LAN の認証済みユーザーを安易な盗聴から保護するもの」と定義されていた。このように、WEP が目指したセキュリティ・レベルはもともとそれほど高いものではなかったが、それにしても WEP 暗号化方式はあまりに弱く、802.11 はたちまち「脆弱なセキュリティ」の代名詞的な存在となってしまった。

無線 LAN の導入が広がるにつれ、セキュリティの脆弱性を攻撃するツールもインターネット上で容易に入手できるようになった。しかしここで１つ注意しておきたいのは、WEP の欠陥はセキュリティの専門家によって最初に指摘され、公開されたため、欠陥の修正が行われるまでに十分な時間と情報がもたらされたという点である。このように、セキュリティ・プロトコルの仕様を公開する

ことには、誰もがその内容を詳しく検証できるという利点がある。 セキュリティの専門家が精査した結果、WEP には基本的に以下の４つの欠陥があることが判明した。

・暗号化が適切に利用されていない
・メッセージの改ざんを防ぐ手段がない
・暗号化鍵を再利用しているため、暗号化鍵を知らない他人でもデータを読めてしまう
・認証情報がオープンに送信されるため、攻撃者は自分自身をネットワークに対して容易に認証させること（なりすまし）ができてしまう

3.2. IEEE 802.11i における暗号化技術と認証技術

前節の欠陥を解決するため2004年６月に標準化された規格が IEEE 802.11i である。802.11i は、無線 LAN のセキュリティにおいて従来の WEP を置き換えるべく登場した、無線 LAN セキュリティ技術の本命である。暗号化通信技術の WPA が標準化されたときと同じように、すべての Wi-Fi 準拠をうたう無線 LAN 機器で 802.11i 標準サポートが要求されることになるとみられる。現在発売されている機器においても、その多くがファームウェアのアップデートなどで 802.11i の規格に対応可能になる。

802.11i の基本は、「暗号化通信」と「ユーザー認証」の２つにある。Wi-Fi Alliance*が認証する無線 LAN 機器に標準で装備されている WEP よりも強力な暗号化技術に加え、従来の WEP ではできなかったユーザー認証を行う 802.1x を組み合わせることで、セキュリティ的に懸念される各種の問題を解決する。

従来、企業向けに使用するには WEP では不完全として、セキュリティ・ベンダーの多くは WEP に加え、802.1x などの認証ソリューションを組み合わせてシステムの構築を行っていた。だが WEP 自体の脆弱性が指摘される中で、より強

---

* Wi-Fi Alliance
無線 LAN 機器メーカーのほとんどが参加する業界団体で、新技術の開発や、製品同士の相互運用性の検証を行っている。テストに合格した製品には「Wi-Fi」の認定マークが付けられる。

い暗号化技術の登場が望まれていた。802.11i はそのような背景の中で標準化がスタートしたが、標準化作業が完了するまで時間がかかることが予想されていた。そこで、802.11i の一部仕様を先取りする形で、2002年末に WPA（Wi-Fi Protected Access）が登場した。Wi-Fi 認定機器は WPA サポートが必須とされていたため、2003年春には多くのメーカーが Wi-Fi 認定のために WPA をサポートしている。OS では、Windows XP が SP1 以降でサポートを行っている。ただし、デフォルトの状態では WPA は利用できないようになっているため、Windows XP を SP1 にアップデートして、WPA 対応パッチをさらに当てる必要がある。

そして、WPA よりさらに強力な暗号化技術である WPA2 が、2004年６月に登場した。この WPA2 という暗号化技術が、すなわち 802.11i である。正確には、WPA＋WPA2＋802.1x をすべて包含するものが 802.11i である。以降では、802.11i の暗号化方式とユーザー認証について述べる。

3.2.1. WEP の弱点を解決する「TKIP」暗号化方式

WEP の弱点は、しばしば各種のメディアで指摘されているが、その内容はだいたい次のポイントに集約される。

1）暗号に使う鍵長が短い（64bit 時）
2）初期化ベクタ（IV）が24bit と短い（64bit／128bit 共通）
3）鍵が通信中に変化しないため、一度解読されると暗号化の意味を成さない
4）メッセージの完全性を保証できない（改ざんが可能）
5）鍵はアクセスポイントごとに固定され、鍵を知るユーザーであればアクセス可能
6）ユーザーが接続先の真偽の確認を行えない（偽装アクセスポイントの設置が可能）

WEP において、暗号に使う鍵長は 64bit 暗号時に 40bit と短く、最近の PC であれば多少時間をかければ解読できないことはない。故に 64bit の WEP は使うべきではないといえる。問題なのは、128bit 暗号（鍵長は 104bit）の WEP にお

ける脆弱性である。WEP で暗号化を行う際は、手で入力する WEP キーに加え、無線 LAN 機器が自動的に設定する 24bit の IV と組み合わせることで、暗号化のための暗号鍵を生成している。IV は、通信時に暗号化されないフラットな状態でやりとりが行われるほか、長さからいっても 24bit（3byte）と短く、多少時間をかければ解読することが可能である。また WEP は、アクセスポイントとクライアントで共通の WEP キーを共有することで互いを認識するという機構上、一度 WEP キーが漏洩してしまうと、そのアクセスポイントに接続するすべての通信のセキュリティが脅かされてしまう危険性をはらんでいる。

そこで、WEP の弱点を解決するべく登場した WPA では「TKIP（Temporal Key Integrity Protocol）」という暗号化方式を採用している。TKIP では鍵長の拡張のほか、一定時間ごとに暗号鍵を更新する機構を加えることで、上述の１）～３）の問題を解決している。また４）の問題については、MIC（Message Integrity Code :「マイク」と呼ぶ）と呼ばれるメッセージの完全性を保証する機構を加えることで、セキュリティの３大要素（「盗聴」「なりすまし」「改ざん」）の１つである「改ざん」を防止できるようになった。５）と６）の問題については、802.1x の認証機構と組み合わせて使用することで回避できるようになっている。

WEP では固定の共有キーを用いることが問題になっていたが、TKIP ではそれを避けるため、ユーザー認証後にサーバ側から最初の鍵を交付する方式になっている。後述の 802.1x の認証システムを使って、クライアントは最初にアクセスポイント経由で認証サーバにアクセスして、そこで認証が完了すると、やはりアクセスポイント経由で鍵の交付を受ける。以後は、一定時間ごとに鍵の更新が行われ、同じ鍵が使用され続けることはない。このように鍵の管理方法の変更が TKIP での最も大きなポイントだが、この方式では、TKIP の使用に当たって必ず認証サーバとの組み合わせが必要になってしまう。企業用途では問題ないが、手軽に無線 LAN を使いたいという個人ユーザーにとっては利便性が低い。そこで、個人ユーザー向けに TKIP では「PSK（Pre-Shared Key）」という WEP と同じ共有キー方式も提供している。最初に使用する共有キーをアクセスポイントとクライアント側で共有しておき、後は TKIP により一定時間ごとに鍵を更新する。これを「Home Mode」といい、認証システムを利用する企業向

けソリューションの方を「Enterprise Mode」という。Home Mode では、PSK が認証の役割も果たしている。

TKIP では、IV の鍵長の変更や一定時間ごとの鍵更新などの機能変更こそ行われているものの、実は暗号化アルゴリズム自体は WEP と同じ「RC4 (Ron's Code 4)」という方式がそのまま採用されている。RC4 に加え、MIC 生成用にメッセージ・ダイジェスト関数を用いる以外は、技術的に目新しい部分はないといえる。つまり IV こそ拡張されているものの、ある程度時間をかければ解読は可能である。だが一定時間ごとの鍵更新機能を加えることで、更新のインターバル間での解読を難しくしている。WEP の脆弱性がたびたび指摘されていたため、RC4 自体に問題があるような認識を持ってしまいがちだが、実際には RC4 はそれほど弱い暗号化アルゴリズムではない。長い鍵長で、きちんとした使い方さえしていれば、TKIP のように比較的強力なソリューションを提供可能である。

3.2.2. 強固な暗号化アルゴリズム「AES」

３.２.１節で述べたように TKIP の技術は WEP の延長にある。鍵管理の方法を工夫することでセキュリティの強化を行っていた。だが、暗号化アルゴリズムそのものを強化することで、さらに解読が難しい暗号を実現したのが、WPA2 で採用された「AES（Advanced Encryption Standard)」である。AES は、1990年代後半に米国政府がそれまで使用していた DES (Data Encryption Standard) やトリプル DES に代わる強力な暗号ソリューションを一般公募したものがベースとなっている。最終的に、ベルギーより提案された Rijndael が米国標準技術局（NIST: National Institute of Standards and Technology）に AES として採用された。AES では128／192／256bit の３種類の鍵長を持ち、暗号強度自体も DES などに比べ大幅に強化されている。

つまり、AES のサポートをもって802.11i が完成するのである。802.11i が標準化された段階で、Wi-Fi 認定には AES、すなわち WPA2 のサポートが必須となる。だが AES は強力な分、暗号化に必要な計算量が従来の RC4 などに比べて格段に増えている。個人ユーザー向けのアクセスポイントなどでは、価格引き下げのために比較的低速なプロセッサを採用していることも多く、同時接続ク

ライアント数が増えるとAESの処理が間に合わない可能性もある。標準化以後に登場する新製品では問題ないだろうが、従来製品の中には 802.11i の完全サポートができないものも出てくる可能性がある。無線 LAN 製品の中には、Windows XP をはじめとしてすでにAESサポートの標準化に先行したものもある。その場合、標準化後にファームウェアのアップデートなどが行われることになるかもしれない。

3.2.3. 802.1x の認証プロトコル「EAP」

TKIPとAESが 802.11iの片翼なら、802.1xによる認証はもう片方の翼である。両方そろって、初めてセキュリティ・ソリューションとしての 802.11i が機能する。802.1xは、イーサネットや無線LANを問わず、各種の媒体でユーザー認証とそれによるアクセス・コントロールを実現すべく考案されたセキュリティ規格である。

802.1x では、クライアントはネットワークのアクセス前にまず RADIUS (Remote Authentication Dial-In User Service) などの認証サーバへと接続し、ユーザー認証を受ける必要がある。認証の後、ユーザーは初めてネットワークへのアクセス許可を受けることになる。これを無線LANに当てはめた場合、クライアントはまずアクセスポイントに接続することになるが、さらにそこを経由して認証サーバへとアクセスする。ユーザー認証の方法はさまざまあるが、認証が行われると認証サーバよりアクセスポイント経由で鍵の交付が行われる。これが、Enterprise Mode で最初の通信に用いられる暗号鍵である。クライアントは、この鍵の交付をもって、初めてアクセスポイントを経由したネットワークへのアクセスを許可されたことになる。

クライアント―認証サーバ間のやりとりに用いられるプロトコルを EAP (Extensible Authentication Protocol) と呼ぶ。EAPには表１のような種類のものがあり、用途によって使い分けられる。EAP の最もベーシックなものが MD5 (Message Digest 5) で、ユーザーIDとパスワードによるシンプルな認証ソリューションが提供される。だが難点として、EAP で重要な双方向認証が提供されないため、現在ではほとんど使われることはない。双方向認証とは、サーバがク

ライアントの正当性、また逆にクライアントがサーバの正当性を検証するものである。なぜ双方向認証が必要なのかといえば、サーバがクライアントを認証するのは当然として、逆にクライアントはサーバが本物かどうか（つまり本当に信頼できる相手なのか）を認証できなければ、通信相手となる認証サーバがニセモノで、個人情報の抜き取りなどを目的としている悪意のあるものか否かを判断できないためである。双方向認証によって、クライアントとサーバ、双方の「なりすまし」を防止できるのである。

表1　EAPの認証方式

方式	双方向認証	クライアント証明書	サーバ証明書
EAP-MD5	△	なし	なし
LEAP	○	なし	なし
FAST	○	なし	なし
PEAP	○	オプション	あり
TTLS	○	オプション	あり
TLS	○	あり	あり

EAP には MD5 のほかに、シスコシステムズの LEAP (Light Extensible Authentication Protocol)、マイクロソフトの PEAP (Protected EAP、MS-PEAP とも略すこともある)、PEAP と同等のソリューションを提供する TTLS (Tunneled TLS)、認証に電子証明書を用いる TLS (Transport Layer Security) などの種類がある。LEAP は MD5 の改良型で ID とパスワードによる認証を基調としており、シスコが WEP の補完ソリューションとして長らく提供していた。だが最近になり辞書攻撃に対する致命的な欠陥が指摘され、シスコ自身がより新しい技術である FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling) の使用を推奨している。PEAP は、サーバによるクライアント認証は ID とパスワード・ベースだが、クライアントによるサーバ認証では電子証明書（サーバ証明書）で接続先サーバの信頼性を確かめるようになっている。だが PEAP がサポートするクライアントは Windows に限定される。TTLS も同様のソ

リューションだが、クライアント向けの専用ソフトウェアが必要となる。最後の TLS では、双方向の認証に電子証明書が用いられる。ただし、クライアント証明書が必要となる。どの方式も一長一短なため、これが確実というものはない。どの認証方式を採用するかは、機器側の対応や利用形態を見て判断することになる。

3.3. 無線 LAN 学習環境の構築

無線 LAN 技術の変遷および現在の標準化規格である IEEE802.11i を踏まえ、本学における無線 LAN が利用可能な学習環境を構築する。本学のネットワーク環境には全学的に利用できる無線 LAN アクセスポイントはいまだ設置されていない。そこで、本研究において、実験的に無線 LAN アクセスポイントを設置し、その有用性を検証した。３.２節で述べたように 802.11i の暗号化方式には、WEP, TKIP, AES の３種類がある。WEP は必要ないと思われるが、もしネットワーク内に WEP のみをサポートする製品がある場合には、必然的に WEP を選択せざるを得ない。しかし、本学のネットワーク環境にはまだ無線 LAN アクセスポイントの製品がなく、WEP の脆弱性を無視できないためこれを採用しない。一番高度な暗号化処理を要する AES であるが、本学ではすでに RADIUS 認証サーバを運用しており、同サーバを無線 LAN に接続する際の認証サーバとして利用することで、現在の学内アカウントをそのまま認証の際に利用できるネットワーク環境を構築した。RADIUS 認証サーバのスペックを表２に示す。また、EAP にも多くの認証方式があるが、RADIUS 認証サーバが Windows Server であることと、接続するクライアント PC を Windows マシンであることに限定しているため、EAP の中でも Windows との相性が高い PEAP 方式を採用した。クライアント PC では、Windows に標準で搭載されている機能を利用して、EAP を用いた認証によるネットワーク環境への接続が可能となる。図２に示す認証ダイアログにて、学内アカウントのユーザ名とパスワードを入力することで、RADIUS 認証サーバとの通信を行い、認証が成功すれば学内 LAN に接続できるようになる。

表２　RADIUS 認証サーバのスペック

仕様項目	内容
機種	Express5800/120Re-1
CPU	Xeon 3.6GHz
メモリ	2GB
HDD	36.3GB
OS	Windows Server 2003

図２　認証ダイアログ

無線 LAN アクセスポイントとしては、RADIUS 認証が可能であり、802.11i に対応した BUFFALO 社製の表３に示す製品を選択した。この無線 LAN アクセスポイントを学生食堂、学生ロビー、図書館グループ学習室の３箇所に設置した。5GHz 帯の周波数帯域を利用する IEEE802.11a と 2.4GHz 帯を利用する IEEE802.11b/g を同時に利用することができないため、クライアントの普及率の高い IEEE802.11b/g を運用することにした。

表３　無線 LAN アクセスポイントのスペック

仕様項目	内容
機種	WLM2-A54G54/HA
規格	IEEE802.11a/b/g 準拠
暗号化方式	128(104)/64(40)bit WEP、WPA-PSK(TKIP、AES)
IEEE802.1x/EAP	MD5/TLS/TTLS/MS-PEAP
電源	AC100V 50/60Hz
重量	約665g

3.4. 無線 LAN 学習環境における稼動実験

３.３節で述べた無線 LAN 学習環境を実際に学生に利用してもらい、認証方法の操作性や学習環境としての評価を行った。具体的には、本学総合管理学部「データ分析」の講義において、無線 LAN 学習環境を利用した演習を２名１組の６グループに分かれて行った。各グループは演習に取り組む際に、中央コンピュータ室でノート PC の貸出を受け、各学習環境にてノート PC を無線 LAN アクセスポイントに接続した。同講義では、教材や課題に対する資料が学内 LAN 上に公開されているため、学生は演習に取り組む際に同講義の HP を閲覧することが必然的な作業となっている。12人の被験者のうち、１名は体調不良のため実験に参加できなかったため、アンケートの有効回答数は11である。

アンケート結果から、認証方法の操作性については図３に示すとおり、操作方法が難しいと感じる学生はいなかった。学生が通常、情報処理実習室を利用する際に入力するユーザー名とパスワードを入力するため、操作方法が簡易に感じられたといえる。

表示速度については図４に示すとおりであるが、格別早いと感じるユーザーは少なかった。パソコンの電源を入れて、インターネットへの接続に伴う認証処理が終了してから、実際にウェブブラウザを起動することになるため、その間の時間が比較的長く感じられる。おそらくこの時間を除けば、ある程度の表示速度は体感できているはずである。ただし、現在の無線 LAN 規格では、

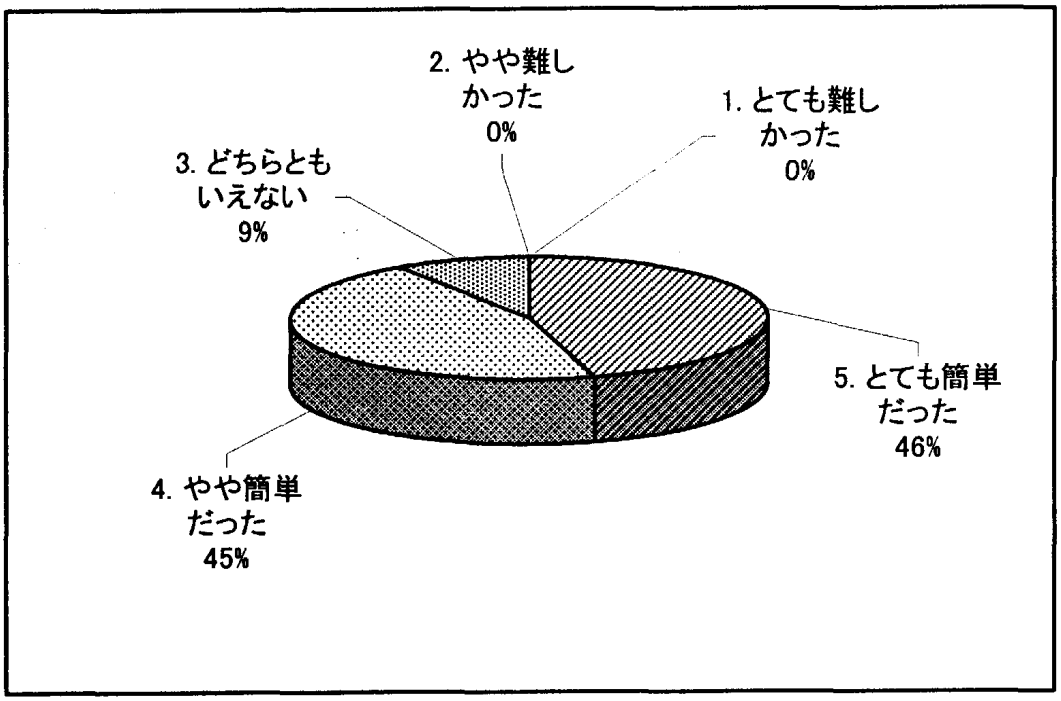

図３　認証方法の操作性

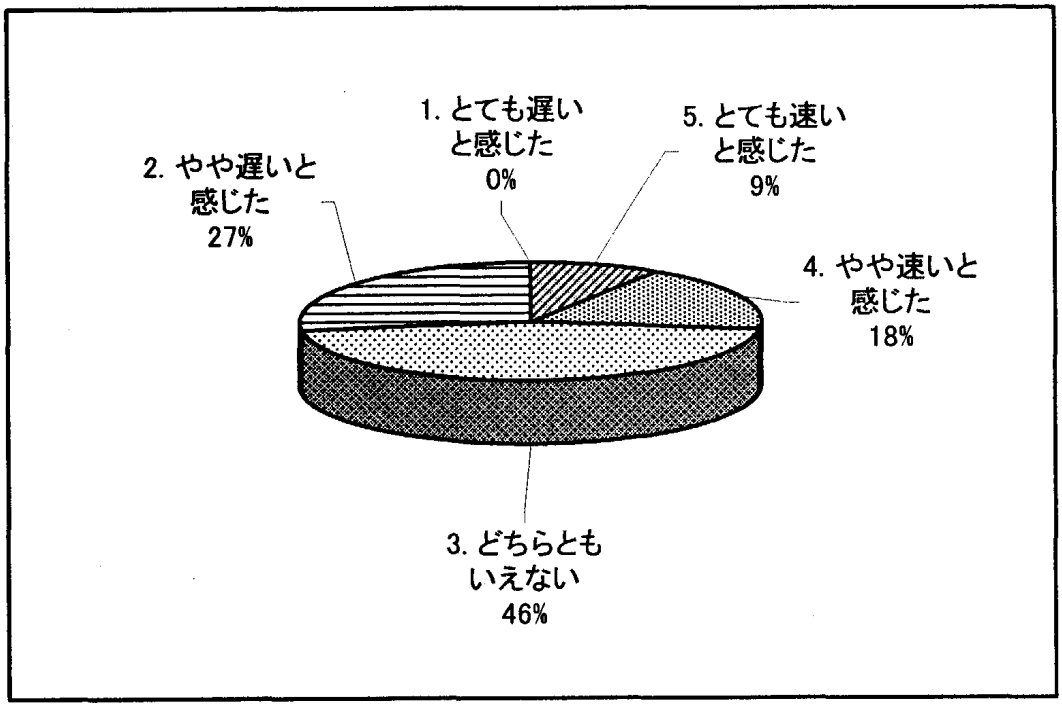

図４　インターネット接続時の表示速度

IEEE802.11g および IEEE802.11a において理論値では最大で 54Mbps の転送速度しかない。学内 LAN における各棟間の通信は光ファイバーケーブルで接続されているため 1Gbps (1000Mbps) であり、LAN ケーブルで研究室内の LAN を構成している場合は、100Mbps の速度が可能となっている。つまり、現状の規格では無線 LAN の速度は有線 LAN には及ばない。現在一般家庭にも普及してきている無線 LAN は、今後さまざまな家電製品を含む電子機器との接続が行われるようになることが予想され、研究されている。そのため、通信速度もこれまで以上の速度を発揮する規格が検討されているため、近い将来において速度の問題は解決されることと思われる。

３つの学習環境（学生食堂、学生ロビー、図書館グループ学習室）を５段階評価で評価した結果を図５に示す。評価値が高い学習環境ほど、学生が集中しやすい学習環境であると判断したことを示す。学生の視点からみると、３つの学習環境を比較すると図書館グループ学習室の評価が最も高い。やはり静かで集中できるという要素がその大きな評価要因となっている。高い集中力を要する学習に取り組む際には、現在の図書館グループ学習室のように静かで集中できる学習環境が求められる。学生食堂と学生ロビーはやはりまだ本学での利用

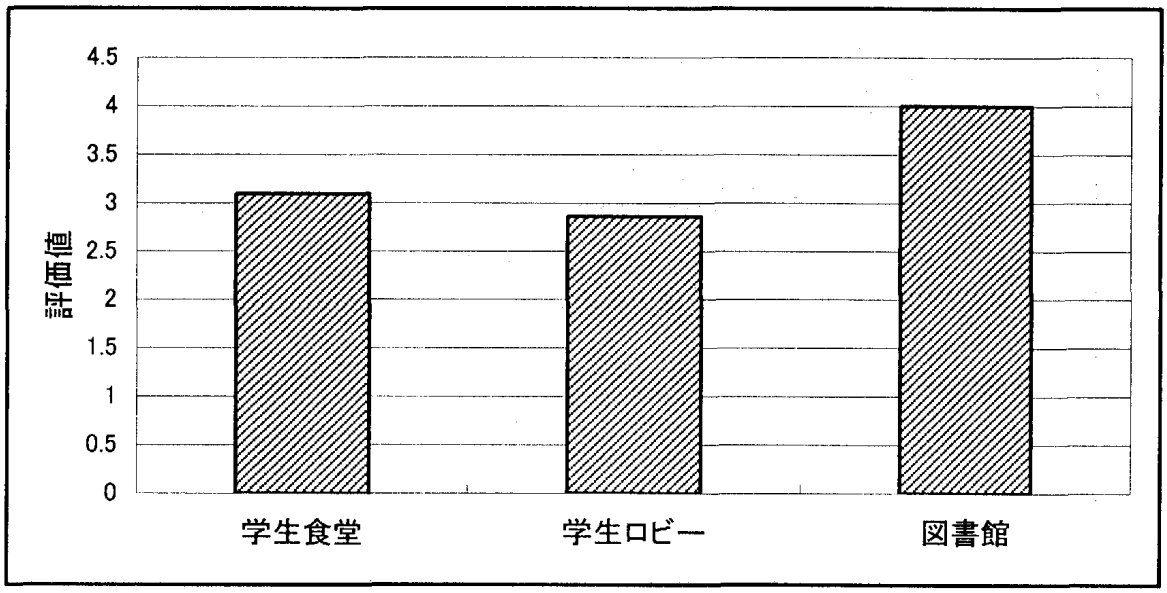

図５　学習環境別の評価

形態として定着していないこともあってか、その場でノートPCを開いて、ネットワークに接続し、学習する形態に恥ずかしさを感じる学生もいた。ただ、図書館グループ学習室に比べて、気軽に足を運び、周囲に大きな注意を払うことなくお互いに話しができることは評価されている。数人の学生が集まって、わいわいガヤガヤとグループ学習を行う場合に利用すると学生のニーズにマッチした学習を実施できると思われる。

4. おわりに

これまでの教育観をベースとした「ようかん型」の学習環境では、「教える」場になりえても「学習する」場としては不十分である。そのため、新しい学習観に基づく学習環境をデザインすることが重要であることを認知科学の視点を踏まえて示唆した。公立はこだて未来大学のキャンパス事例や新井らの研究事例から新しい学習観が生まれ始めており、今後のｅラーニングにおける大きな可能性を秘めていることがわかる。

本学における新しい学習環境をデザインするにあたっては、既設の建物や教室自体に変更を加えることが困難であるため、近年脚光を浴びている無線LAN技術をベースとしたサイバー空間を活用し、新たな学習環境の構築を試みた。その稼動実験の結果より、サイバー空間を活用した学習環境の有用性を示した。ただし、現時点においてはこれまでの教育・学習に慣れた学生の意識からも図書館のような静寂した学習環境において、高い集中力を要する学習に取り組む傾向があることが判明した。一方で、これまで学習環境として広く利用されていなかった学生食堂や学生ロビーは、複数名で話し合いながら協同作業を行うような学習に適した環境であり、ここに無線LANをベースとしたサイバー空間の学習環境を提供することでさらなる学習環境として学習者に有効に働く可能性を示した。今後は、これらの学習環境と実際の講義における講義内容とをリンクさせ、それぞれの講義形態における学習環境としての要素について研究を進めると同時にネットワークインフラを活用した講義支援システム LMS

(Learning Management System) の研究を進めていく予定である。

謝辞

本研究は、平成17年度熊本県立大学地域貢献研究事業から研究費の助成を受けた。ここに深く感謝する次第である。

参考文献

[1] Trow, M.（喜多村和之訳）：高度情報社会の大学ーマスからユニバーサルへ，玉川大学出版部，2000.

[2] 佐伯胖：コンピュータと教育，岩波書店，1986.

[3] Ehrmann, S. C.: LOOKING BACKWARD: U. S. efforts to use technology to transform undergraduate education, http://eee.uci.edu/programs/auctlt/LookingBack.html, 1996.

[4] 木村忠正：オンライン教育の政治経済学，NTT 出版，2000.

[5] 上野淳：未来の学校建築ー教育改革をささえる空間づくりー，岩波書店，1999.

[6] Brown, J. S., Collins, A. and Duguid, P.：状況に埋め込まれた認知と、学習の文化，認知科学ハンドブック，共立出版，pp.36-51，1992 年.

[7] Gibson, J. J.：生態学的視覚論ーヒトの知覚世界を探るー，サイエンス社，1985.

[8] 佐々木正人：アフォーダンスー新しい認知の理論，岩波書店，1994.

[9] 佐々木正人：知性はどこに生まれるか—ダーウィンとアフォーダンスー，講談社，1996.

[10] Lave, J. and Wenger, E.：正統的周辺参加・状況に埋め込まれた学習，産業図書，1993.

[11] Wenger, E., McDermott, R and Snyder, W. M.（野村恭彦監修，櫻井祐子訳）：コミュニティ・オブ・プラクティスーナレッジ社会の新たな知識形態の実践ー，翔泳社，2002.

[12] Johnson, D. W., Johnson, R. T. and Smith, K. A.（関田一彦監訳）：学生参加型の大学授業ー協同学習への実践ガイドー，玉川大学出版部，2001.

[13] 美馬のゆり，山内祐平：「未来の学び」をデザインするー空間・活動・共同体ー，東京大学出版会，2005.

[14] 新井紀子：ネット上に学びの場を創る—情報共有が市民社会にもたらすものー，岩波書店，2003.

[15] 新井紀子：ｅラーニング，デジタルが変える放送と教育，pp.49-80，丸善，2005.

[16] 藤本竜之介，飯村伊智郎，松野了二，桑原毅：熊本県立大学における学内 LAN と教育用システム，アドミニストレーション，Vol.11, No. 3・4, pp.139-158, 2005.

[17] IEEE802.11, http://grouper.ieee.org/groups/802/11/