

第 2 章

基 礎 調 査

- 2.1 ニーズ調査結果の概要
- 2.2 技術調査
- 2.3 セキュリティ

2.1 ニーズ調査結果の概要

ニーズ調査結果に関しては、「ニーズ調査編」に詳しく記述されている。ここではサマリーのみを記述するので、詳細については「ニーズ調査編」を参照されたい。

(1) 想定した在宅学習システムに対する評価

オンライン調査と郵送調査の合計における在宅学習システムの有効性に対する評価結果は、「役立つ」と「少しは役立つ」の肯定評価が 81%に達し、一方「有効性を感じない」否定評価は 14.9%となっている。すでにネットワークユーザーであるニフティサーブ会員を対象としたオンライン調査結果で見ると、「役立つ」(34.9%)、「少しは役立つ」(49.3%)の肯定評価は 84.2%とさらに高くなり、「有効性を感じない」否定評価は 7.8%に低下している。

(2) 本システムが役に立つ理由

オンライン調査と郵送調査とも、在宅学習システムが役に立つ理由の第一位は「いつでも自分の都合の良い時間に勉強出来るから」。オンライン調査結果の第二位には「自宅で学習出来れば自分自身の仕事の調整が不要になりそうだから」が入り、郵送調査結果の第二位は「自分の理解度に合わせて勉強出来るそうだから」となっている。

(3) 本システムに対して有効性を感じない理由

オンライン調査と郵送調査の合計において、有効性を感じない理由の第一位は「家では学習に集中出来ないから」で、全体の過半数(45.6%)近くを占めている。オンライン調査結果だけを見ると、その第一位は「直接講師に接した方がすぐ質問出来るなど、よく理解できるような気がするから」で 41.7%の割合となっている。

(4) 「有効性を感じない」否定評価者の属性

年齢的には「30～39 才」が多く、「家では学習に集中出来ないから」を理由としてあげた割合が高い。職種としては、技能工・生産工程従事者等ブルーカラー系の割合が高い。パソコン所有状況とその習熟度との関係を見ると、否定評価者は全体の割合に比し、パソコン所有率は低く、かつ習熟度も未経験者の割合が高くなっている。さらに、否定評価者には自己啓発を行ったことがない者が、全体の割合に比し多く含まれている。

(5) 本システムにより学習したい分野・内容

「資格取得を目的とした講座」がオンライン調査と郵送調査の両方において「一番人気」となっており、特にオンライン調査では 56.9%の高い割合となっている。「語学関連の講座」と「OA 機器の習得」に対するニーズも高いものがある。

(6) 本システムによる1日の学習時間とその時間帯

「30分以上～1時間未満」に回答が集中しており、オンライン調査と郵送調査の合計における割合は60%近くに達している。ただし、オンライン調査では通信接続時間をより短くしたいとの意向が窺い知れる。

時間帯については、「午後9時から12時くらいの間」が一番多く、その割合は全体の68.7%と高い。この時間帯に利用が集中すると考えられる。オンライン調査では「深夜12時から2時くらいの間」についても20%近い割合となっている。

(7) 本システムの導入に当たっての初期投資額

オンライン調査と郵送調査では傾向に差が見られ、オンライン調査ではパソコン所有率が高いこと等により負担額は3万円以下に集中しているのに対し、郵送調査では「3～5万円未満」22.4%、「5万円～10万円未満」19.9%、「10万円～20万円未満」15.3%と、ばらつきが見られる。

(8) 毎月のランニングコスト

受講費（教材利用費）や通信費のランニングコスト（月額）は、「3,000円以上～5,000円未満」の割合がオンライン調査と郵送調査ともに最も高いが、オンライン調査では「3,000円未満」が、郵送調査では「5,000円以上～10,000円未満」がそれぞれ第二位の割合となっている。郵送調査の方がランニングコストに対する許容範囲は広いことになるが、10,000円を超えると受講者獲得は厳しくなるといえる。

(9) ネットワークの種類に関する要望

パソコン通信ユーザーを対象としたオンライン調査では「パソコン通信を使用した方が良い」(44.8%)が「インターネットを使用した方が良い」(37.5%)を上回ったが、郵送調査では前者の18.0%に対し、後者は48.1%と順位は逆転している。

(10) 教材に対する要望

オンライン調査では「自学自習のための機能（CAI等）を重視すべきである」(45.7%)、「画像（動画・静止画）、音声を重視すべきである」(42.9%)とその差はわずかであるが、郵送調査では前者の36.3%に対し後者は47.4%とやや開きが見られる。

(11) 面接指導（スクーリング）に関する要望

「ネットワークを利用した一対一の対話方式」と「ネットワークを利用し、質問・相談事項を送信すると翌日には回答が来る通信添削形式」の割合が共に20%以上と高いが、「他の受講者と一緒に集まった集合指導」(16.2%)、「直接講師のいる場所における個別指導」(14.2%)等従来のスクーリング形式を要望する割合も少なくない。運用に当たっては多様なニーズへの対応が

必要となる。

(1 2) 国等への要望

「給付金等の金銭的援助」が 51.3%と過半数を超えており、一番強い要望といえる。「在宅学習システムに係る通信基盤の充実」(32.4%)、「習得した成果に対する評価制度の確立」(29.9%)、「教材の質、量の充実」(27.9%)等の要望についても真剣に取り組まなければならない。

2.2 技術調査

技術調査は、電機メーカー、ネットワークサービス会社などへアンケートを送付して行った。回答が得られたのは12社からであった。アンケートは2部構成になっており、第一部「家庭を結ぶコンピュータネットワークシステムに対するアンケート」、第二部「教育へ有効利用できるマルチメディア・ネットワーク技術」に関することである。

2.2.1 WWW(World Wide Web)ブラウザ関連

現在までインターネットが普及した要因の一つに WWW ブラウザの登場が挙げられる。WWW ブラウザとは、世界中に広がる WWW サーバーが提供する情報(ホームページ)を個人のパソコンからアクセスするための道具である。WWW サーバが提供する情報は、HTML(Hyper Text Markup Language)という形式言語で記述され、文字、絵などを組み合わせた情報を表現する能力を持っている。最近では、音、動画などを表示させる補助的なツール(プラグイン、ActiveX コントロール)も出来てきて、まさにマルチメディアと呼ぶにふさわしい表現力を持っている。

在宅学習システムでは、本やビデオテープ、カセットテープなどの一方的な教材ではなく、インタラクティブな教材を想定している。インタラクティブな教材を提供するには、WWW の仕組みは有効な手法である。また、WWW は機種に依存しないという特長を持っている。UNIX、マッキントッシュ、Windows など WWW ブラウザさえ用意できれば、ほとんど同じサービスを受けることができる。これは、既に持っているマシンをそのまま利用できるということになるので、専用端末が必要なシステムに比べて、受講者の初期投資負担を軽減できるという効果がある。

WWWブラウザの種類	Netscape Navigator	Internet Explore
開発元	米Netscape Communications社	米Microsoft社
機能拡張	プラグイン	ActiveXコントロール
プラットフォーム	マッキントッシュ、UNIX、DOS/V機 など16のプラットフォームに対応	DOS/V機
シェア	約80%	約15%

表 2-1 Netscape Navigator と Internet Explore の比較

現在世界的に広く使われているブラウザは Netscape Communications 社の Netscape Navigator である。それを追いかける立場にいるのが Microsoft 社の Internet Explore である。他のブラウザもいくつかはあるが、現在はこの二つが主なブラウザとなっている。JAVA アプレットなどにはどちらも対応しており、

機能的にはほぼ同等ではあるが、独自の機能を持つ部分もある。

Netscape Navigator は多くのプラットフォームで動作することもあって、ブラウザの世界では、圧倒的なシェアを誇っていた。しかし、Windows 95 が出てきたと同時に Microsoft 社が無償で提供しだした Internet Explorer が Netscape の牙城を脅かしつつある。今後、どちらかが主流になるか、あるいは、両者共存していくか予測は難しいが、それはどちらがより多くのシェアを持つかによると言っても良い。

2.2.2 WWWとデータベース

最近のホームページには、WWWサーバとデータベースを連携させて、利用者が得たい情報だけデータベースから検索して表示するような仕組みが増えている。このような仕組みを利用すると、受講者が必要とする教材を検索し、それだけを受講者に見せることができるようになる。

在宅学習システムで想定している環境は、教材の素材（文字情報、静止画、動画、音声など）はそれぞれ独立したデータとして、データベースに登録される。それらの素材の上位で、素材間の関係を定義することにより、素材を組み合わせた一つの教材ができあがる。また、受講者の情報は、セッション管理の概念を導入し、受講者を一意に識別できるラベルにより管理され、受講者の過去の受講履歴などは全て蓄積されるようにする。

セッション管理とは、WWWクライアントとWWWサーバ間でマルチステップのトランザクション処理ができないというWWWの欠点を補う手法である。クライアントを一意に識別できるラベルにより管理し、クライアントの情報を逐一記録できるようにする仕組みである。

在宅学習システムにおいて必要となるデータベースの機能は、次のような機能である。

教材	制作	素材をデータとし、リレーションでシナリオを作成する
		素材に映像、音声などマルチメディアコンテンツを含める
	登録	教材の新規登録、削除、更新
	管理	セッション管理を利用した教材の利用頻度等の統計処理
	検索	関連する教材の検索
受講者	登録	新規登録、削除
		全ての受講者を一意に識別できる仕組み
	管理	セッション管理を利用した受講者毎の個人成績、全体の成績作成
	検索	センター側での受講者の検索

表 2-2 在宅学習システムに必要なDBの機能

このような仕組みを実現するには、次のような方法がある。

① CGI(Common Gateway Interface)を利用

CGIとはWWWサーバとクライアント間でデータをやりとりするインターフェースである。WWWサーバ側で別のプログラムを起動する機能があり、データベース検索などの様々な処理を実行できるようになっている。起動されるプログラムはスクリプトと呼ばれ、UNIXのShell、Perl、Visual Basic等で記述される。この方法は、利用しやすい反面、リクエストの度に別のプログラムを起動するというオーバーヘッドの高い仕組みのため、要求

が殺到した場合、反応速度の面で大きな問題を抱えている。

② WWW とデータベース連携ツールを利用

Oracle、Sybase 等のデータベースベンダーは、CGI を介さずに WWW サーバとデータベースを接続するツールを提供している。これらを利用すると WWW サーバがデータベースに直接接続できるので、データベース接続のオーバーヘッドがなくなり、性能的には格段に向上する。

- Oracle WebServer の場合

WRB(Web Request Broker)と呼ばれる CGI に代わる新しいサーバ側処理の手法を導入し高いパフォーマンスを実現している。WRB の仕組みを利用すると、サーバ側の負荷を自動的にかつ継続的に最小に抑え、また、管理者は意図的にサーバ側の負荷を管理することが可能になっている。

- Sybase Web.sql の場合

リレーショナルデータベースと Web サーバを接続するツールキットである。Web からリレーショナルデータベースへの高速アクセスを実現している。また、Web ページをダイナミックに生成できる多彩な機能を提供している。

2.2.3 画像圧縮、動画配信、テレビ会議

映像が教育分野で有用であることはよく言われる。在宅学習システムでも映像を教材に組み込むべきである。ここでは、映像を教材に組み込む際の留意点、課題について述べる。

映像をネットワーク経由で伝送する場合、画像の圧縮率とネットワークのパイプの太さが画質を決める大きな要素となる。また、映像をネットワーク経由で伝送する時は、常にある一定量のネットワークの帯域を専有する必要があるということも忘れてはならない点である。

まず、ネットワークの帯域の専有であるが、ネットワークの種類によって事情が若干異なる。テレビ会議で良く使われる衛星通信、専用線、ISDNなどは契約された帯域を保証している。一方で、最近ではインターネットを経由して映像を伝送するソフトもいくつか出てきている。しかし、インターネットの場合、経路も決まっていなくて、帯域も保証されていない。従って、インターネットを経由する場合は、1秒当たりのコマ数はネットワークの混み具合によってしまい、映像が途切れてしまう場合もありうる。

以下、各ネットワークの特長の比較、静止画フォーマットの特長、インターネットを利用した映像伝送ソフト、テレビ会議システム、衛星通信を利用した映像伝送について述べる。

(1) 各ネットワークの特長の比較

衛星通信は、放送型で大容量のデータを多地点に対して同時に伝送する用途に向いている。専用線接続は、特定の2地点間の接続であり、利用時間によって価格が変わらないのが特長である。ISDNは不特定な2地点間で接続できるのが特長である。これら三つのネットワークは契約した帯域幅が常に保証されているので、映像伝送に向いている。

インターネットは表 2-3からも分かるように、距離、時間に価格がよらない（プロバイダまでの電話代は除く）ため、ネットワークとしては非常に魅力的である。ただし、映像伝送という点では、帯域が保証されていないことが大きなネックとなっている。

ネットワークの種類	衛星通信	専用線	ISDN	インターネット
帯域保証	あり	あり	あり	なし
利用距離による価格差	なし	従量制	従量制	なし
利用時間による価格差	従量制	なし	従量制	なし
利用用途	多地点同報	特定2地点間	不特定2地点間	不特定2地点間

表 2-3 ネットワークの比較

在宅学習システムを考える場合、ネットワークの選択は広く普及しているものが大前提になる。また、価格的にも高価なものは実際に利用されるのが難しいという点で問題である。

(2) 静止画フォーマットの特長

図や絵は理解を助けるための有効な手段である。在宅学習システムでも、図や絵を文字ベースの情報に組み合わせて、有効に利用すべきである。

インターネットでよく利用される静止画フォーマットは GIF と JPEG である。

GIF は画像を扱えるほとんどのブラウザが対応しているフォーマットである。インターレース（じわじわと表示される）や透明色、アニメーションなどに対応できる。

JPEG は写真などの自然画像を得意とするフォーマットである。インターレースには対応しているが、透明色、アニメーションなどには対応していない。また、JPEG に対応していないブラウザもあることに注意しなければならない。

(3) インターネットを利用した映像伝送ソフト

在宅学習システムにおいては、映像も教材の素材の一つという位置づけである。ここでは、インターネットを利用した映像伝送ソフトについて記述する。

- StreamWorks(米 XingTechnology 社)

圧縮方式は MPEG-1 を採用している。世界で初のソフトウェア MPEG デコーダを搭載し、特別なハードなしで再生できる。幅広い帯域に対応して、低ビットレート時には、間引きをして送信する。

坂本龍一のコンサート中継などにも利用されている。

- SoftwareVision(NTT)

圧縮方式は国際標準の H.261 を採用している。ネットワークの状況に応じてクライアント主導型の制御を行う。現状はまだ試験段階である。

横浜花火大会の中継などに利用された。

- RealVideo(米 Progressive Networks 社)

独自の AC3 圧縮技術を使用し、ストリーム形式に対応し、ダウンロードなしで、音声や画像を再生できる。インターネットのトラフィックがピークになった際は、データ配信を調整し、再送信する。既存のファイヤーウォールにも対応している。従来のオーディオソフト(Real Audio)は世界 1 5 0 0 万人以上のユーザが利用している。

表 2-4 に示す通りに両者に共通することは、表示画面が小さいという点（パ

ソコンの画面の 1/16 程度)、また、現実的には数秒に一コマ程度しか動かないという点である。せいぜい向こう側の状況がなんとなく分かる程度で、教育に利用しようとしたときには、大きな効果は期待できない。もちろん、最初に述べたように、画像圧縮率の向上、あるいは、ネットワークのパイプが太くなることにより改善されるが、ここ数年での飛躍的な向上は難しいと言わざるを得ない。また、インターネットを経由して動画を伝送する場合には、セキュリティ面での問題がある。現在、組織がインターネットに接続する場合には、ファイアウォールと呼ばれるセキュリティシステムを利用するのが一般的である。ファイアウォールについては後述するが、動画を伝送する場合には、ファイアウォールをそのまま超えて伝送することはできない。なんらかの対策を取らねばならず、今後の検討課題の一つである。

ソフトの種類	StreamWorks	SoftwareVision	RealVideo
開発元	米XingTechnology社	NTT	米Progressive Networks社
帯域幅	9.6kbps～3Mbps	200kbps程度まで	28.8～300kbps
コマ数	最大30フレーム/秒	2～3フレーム/秒(28.8kbps)	0.05～15フレーム/秒
符号化方式	MPEG-1	H.261	AC3
画面サイズ	32x32～352x240、352x288	352x288,176x144	取り込む際のデータに依存
解像度	NTSC,PAL	CIF,QCIF	MPEG4に準拠

表 2-4 インターネットを利用して動画を伝送するソフト

(4) テレビ会議システム

在宅学習システムでは、テレビ会議を利用して、擬似スクーリング、遠隔スクーリングを行う予定である。面接指導などの場合に、それほど映像が鮮明でなくとも、相手の表情や雰囲気は多少なりともつかめることができることが重要である。

従来は、テレビ会議システムというと、企業内で設置した大型のものが主流であった。ネットワークも衛星通信や、専用線を利用して、システム自体も高価であるが、回線費も高価であった。しかし、最近はパソコンベースのテレビ会議システムが登場してきた。回線も ISDN(128kbps)を利用し、かなり低価格で利用できるシステムである。インターネットでなく、ISDN を利用する利点は、帯域(128kbps)が必ず確保されているという点である。これにより、安定した映像をやりとりすることができる。

また、パソコンベースのテレビ会議で回線にインターネットを利用するものもある。画質的には、ISDN に比べて相当劣ってしまうが、回線料金が安い点が魅力である。

これらは双方向の映像伝送システムであり、教材という点では双方向である

必要性はない。

(5) その他

デジタル・多チャンネル化の先頭を切って、96年10月からパーフェクTVが本格的サービスを開始した。JCSAT 3号を使い、チャンネル数はテレビ70チャンネル、音声102チャンネルである。デジタル化によりここまでのチャンネル数が実現できたのである。東進Dスクールネットなどの教育用の番組も既に放送されている。また、ディレックTVジャパンがスーパーバードC号を使い、97年12月に約100チャンネルでサービスを開始する予定である。映像が非常に効果がある教育分野では、片方向であり、On Demandではないが、デジタル放送を利用するのも選択肢の一つである。

2.2.4 オーサリングツール

オーサリングツールとは、素材を組み合わせ、マルチメディアコンテンツを制作するツールである。現在、制作されているマルチメディア CD-ROM コンテンツの8割はマクロメディア Director を使って作成されていると言われている。

在宅学習システムでは、マルチメディアコンテンツを制作するので、オーサリングツールが必要であるが、データベースに素材を登録することがオーサリングになってしまうような、データベースオリエンテッドなオーサリングツールが求められる。

以下では、それぞれの製品を紹介する。

- ShockWave Director(Macromedia 社)
テキスト、静止画、アニメーション、ビデオ、音声を組み合わせたマルチメディアコンテンツを制作できる。現在、一番多く使われているオーサリングツールである。
- ShockWave AuthorWare(Macromedia 社)
コースウェア教材のコンテンツを制作するオーサリングツールである。アニメーション等のデータは、クライアント側に完全にダウンロードされる前に再生が始まるようになっている。
- VISUALSHOCK(三菱電機)
さまざまな市販アプリケーションを接続し、自由に簡単に、ビジュアルにマルチメディアコンテンツを制作できる。動画内の移動する特定の対象にリンク付けし、動画再生中に呼び出すことができる。また、VR 空間内の各オブジェクトに、さまざまなマルチメディア情報を簡単にリンク付けできる。
- HIPLUS (日立製作所)
マルチメディア技術と情報ネットワークを融合した、業務遂行・教育／研修支援システムである。文字・静止画・動画・音声を素材として部品化し、データベース登録することにより、素材の共有化と再利用ができる。独自のオーサリング機能により、データベースから素材を自動的に検索し内容を確認できるので、容易にコンテンツの作成ができる。

2.2.5 通信インフラ

在宅学習システムが成立するためには、各家庭からアクセスできる標準的な通信インフラが整備されることが必須である。

昨今のインターネットブームにより、次々と新たなインターネットプロバイダが登場し、バックボーン（基幹回線）も太くなり、インフラとしては着々と整備されてきている。しかし、その分利用者も急増していることにより、各家庭に対するインフラとしては、なかなか整備が追いつかない状況である。また、インターネットプロバイダの乱立状態から、今後プロバイダ淘汰の時期が近い将来にあると見ている人もおり、数年先の各家庭のインフラ整備状況予測は非常に難しい。

参考として、アンケートの中で各社、今後（2年後、5年後、10年後）のインフラ整備状況予測を記述していただいたので、まず、それを列挙する。

時期	各社の通信インフラ整備予測
2年後	<ul style="list-style-type: none"> ・現状インフラの低価格化、ISDN64の普及期。 ・バックボーンが大容量化されるが、ユーザ数や利用量が増加するので家庭からみればアクセス環境は余り変わらない。 ・NTTのオープン・コンピュータ・ネットワークの整備計画に依る。また、PHS、CATVの一層の普及を予測している。 ・電話(アナログ28.8kbpsなど)、ISDN(デジタルINS64など64kbps)、CATV-LAN(数Mbps)、OCNサービス(128kbps)、衛星(数Mbps)などの順位で整備 ・64kbps～ ・アナログ56kbps、デジタル128kbps ・データ通信においては、ISDN等利用による64k～128kbps程度の通信が一般的。一部の地域では、CATV網、電話網を利用した数Mbps程度のサービスを行っている。
5年後	<ul style="list-style-type: none"> ・B-ISDN ・CATVや衛星を利用した非対象型(回線容量)の接続で、片方向は大量データの伝送が実用になる。 ・衛星通信の利用者が徐々に増加する。 ・～1.5Mbps ・10Mbpsサービスが開始。
10年後	<ul style="list-style-type: none"> ・Fiber to Homeにより全世帯に高速通信が実現 ・早ければ家庭で1.5Mbps以上の常時接続が可能になる(料金面も含めて) ・FTTHの時代 ・電話幹線が光ファイバー化され移動体通信(PHSや携帯電話)がさらに普及。反面、CATV-LAN、通信衛星を利用したVODなどもかなり普及。10Mbpsや100Mbpsでの通信が家庭でも普及。 ・1.5Mbps～ ・10Mbpsレベルが普及し、一部の家庭向50Mbps、155Mbpsサービスも開始される。

表 2-5 各社の通信インフラ整備予測

単純に、最小値、最大値をとってみると、

時期	インフラ整備予測の範囲
2年後	現状維持～128kbps
5年後	～1.5Mbps、B-ISDN
10年後	1.5Mbps～155Mbps

表 2-6 インフラ整備予測の範囲

のようになっている。ここで、一つの指針となる NTT の OCN(Open Computer Network)サービスの内容と計画について触れてみる。

OCN は世界から遅れぎみな日本のインターネット環境を一気に世界のトップレベルに押し上げることを目標に、NTT が 21 世紀のコンピュータ通信のインフラとして建設に着手したネットワークである。OCN のサービスは表 2-7 に示される 4 種類がある。

NTT の計画では、ダイヤルアクセスサービスに関しては、H9 年度に約 250 アクセスポイント、H10 年度に約 560 アクセスポイントを設置し、おおむね全国どこでも市内通話料金でアクセスできるようにする計画である。エコノミーサービスは H10 年度に全国 200 都市で提供する計画である。

この計画が実現されれば、2 年後の H10 年度に 128kbps のインフラがかなり整備されると考えてもよい。ただし、価格が 38,000 円では多くの家庭に普及するとは思えない。どこまで普及するかは、価格をどこまで下げられるかにかかっていると云ってもよい。

また、表 2-7 のケーブル種類を見ると分かるが、インターネットにおいては、ケーブル種類がメタリック、光ファイバー、CATV 網など種類を問わない点が特長である。

サービス名	ケーブル種類	価格(月額)	内容
ダイヤルアクセス	電話、ISDN	2,300円(15h) 15h超えると 9円/分	電話またはISDNを経由して アクセスするダイヤルアップIP接 続のサービス(通話料別)
エコノミー	メタリック	38,000円	128kbpsの常時接続
スタンダード	光ファイバー(標準)	350,000円	1.5Mbpsの常時接続
エンタープライズ	光ファイバー(高速)	985,000円	6Mbpsの常時接続

表 2-7 NTT の OCN サービス

2.3 セキュリティ

在宅学習システムを構築する場合、セキュリティシステムとして次の点を考慮する必要がある。

- ①センターを守る
- ②受講者を守る

①については、センター側のマシン（LAN）に外部から進入され、受講者管理情報など外部に漏れてはまずい情報を保護する手段を考慮しなければならない。

②については、例えば受講者がセンター側に送って来た情報（パスワード、住所、電話番号など）が通信途中で盗まれるようなことがないように考慮する必要がある。

ここでは、①に関してルータ、ファイアウォールについて、②に関して認証、課金について記述する。

2.3.1 ルータ

ルータはネットワークとネットワークの間を接続するハードウェアである。設定によって、入ってくるパケットに制限を加えることができる。これにより、外部からの進入を阻止することができるが、木目細かな設定はできないので、その場合はファイアウォールを利用しなければならない。

2.3.2 ファイアウォール(FireWall)

組織にインターネットを導入する場合には、ファイアウォールの構築は必須である。なぜなら、世界の情報に自在にアクセスできるインターネットは、オープンであるがゆえに、常に盗聴や不正アクセスの脅威にさらされているからである。自分のネットワークへ外部からの進入を拒否しつつ、WWW サーバーなどへのアクセスは許すなど、アクセスに制限をかける必要がある。最近の製品では、暗号化機能を持つものも有り、同じファイアウォールを二つのネットワークで利用することにより、公衆網を間に挟んでも、セキュリティを保てるようなものもある。これは、バーチャル・プライベート・ネットワーク(VPN)と呼ばれる。

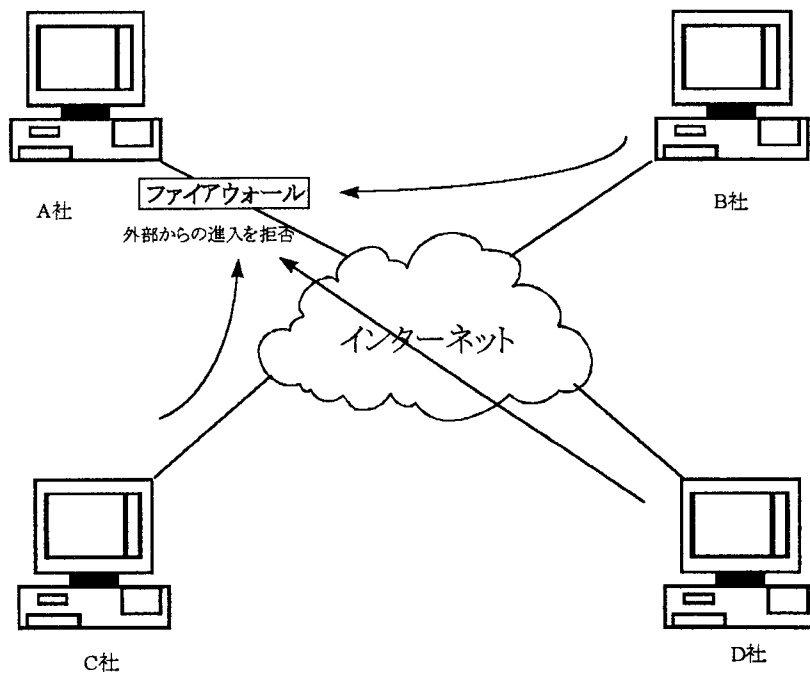


図 2-1 ファイアウォール概念図

ファイアウォールの主な実現方式としては次の二つがある。

①パケットフィルタリング

ファイアウォールを通過するパケットを制限する方法である。この機能を設定すると、内部から外部へのアクセスは許されるが、外部から内部へのアクセスは禁止するといった運用ができる。また、インターネットにアクセスする端末を限定することもできる。

②アプリケーションゲートウェイ

パケットの中継を禁止し、アプリケーションゲートウェイでアクセスを制御する。インターネット側からアクセスできる箇所を限定し、企業内ネットワークには直接アクセスできないようにする。外部から内部にアクセスする場合には、ゲートウェイのログインとパスワードを入力させるように設定し、インターネット側のアクセスに対して認証を行う。これで内部ネットワークには直接アクセスできなくなる。

以下に、各社から供給されているファイアウォール製品の特長を記述する。

● Gauntlet (日立製作所他)

アプリケーションゲートウェイ方式。

アクセスを許可されたクライアントだけが、ファイアウォールを通過できる。

セキュリティルールをWWWブラウザ画面で簡単に設定できる。

仮想プライベートネットワーク(PVN)支援機能によって、インターネットを社内のネットワークの一部と同レベルのセキュリティで使用できる。

- Goah (日本電気他)

サーキットレベルゲートウェイ方式。

PVN 内のコンピュータが外部にアクセスする場合、IP アドレスの付け替えを行うので、IP アドレスが外部に流出することがなく、安全性が高くなる。Goah 間で telnet,ftp など通信する場合、インターネット上で login 名、パスワード、データが全て暗号化されるので、高度な安全性を保ちながら運用できる。

外部から PVN 内へのアクセスは全面的に制御されているが、「ワнтаイム・パスワード」による認証機能により、外出先のパソコンなどから PVN 内のコンピュータにアクセスできる。

不正アクセスをリアルタイムに通知し、アクセスログやシステムログなどの統計情報も通知できる。

- MELWALL (三菱電機)

同一暗号鍵でグループを構成すれば、共用ネットワーク上に、PVN を構築できる。

特定部門にセキュアネットワークを設定しても、一般のサーバや暗号鍵の異なる他のセキュアネットワークとの通信が可能(特例通信)である。同じ端末で一般の WWW や電子メールを利用することができる。

設置は、使用中のシステムにアドオンするだけであり、既存のアプリケーションソフトウェアがそのまま使える。また、ネットワーク機器のメーカ依存性もない。

携帯電話や公衆回線を利用して、オフィスのデータベースにアクセスするモバイルコンピューティング環境にも威力を発揮し、ダイヤルアップ接続に対応している。

暗号アルゴリズムは「線形解読法」や「差分解読法」によって、米国標準商用暗号 DES をしのぐ安全性が証明された強力な暗号方式を採用している。盗聴を防止し、不正アクセスは無効なデータとして捨てられる。

- Solstice FireWall-1 (東芝他)

全てのアプリケーション(TCP,UDP,RPC ベース)に対し、ユーザ認証によってアクセス制限を設定可能なユーザ認証機能をサポートしている。

組織内で使用するプライベート IP アドレスをインターネット上の正規のアドレスに変換するネットワーク・アドレス変換機能(NAT)をサポートしている。

社内 WWW サーバへの社外からのアクセスを可能にする HTTP 認証プロク

シ機能をサポートしている。

ファイアウォール間の通信を暗号化し、インターネットを仮想的な専用線として使用可能にする VPN 機能をサポートしている。

プロトコルに依存しない強力な Packet Filtering により、きめ細かなアクセス制御が可能である。

アクセスログ情報の取得や GUI ベースの管理ツールによりシステム管理を容易にする。

2.3.3 認証

在宅学習システムをネットワーク上で実現する場合、受講者が本当に申し込みをした人なのかを確認する必要がある。これを実現するのが認証の機能である。

ここでは、認証の概念について述べる。ネットワーク社会、特にインターネットの中では、盗聴、改竄、なりすましが、至極簡単にできてしまう。

これらがどういうことか簡単に説明すると、例えば、AさんからBさんにインターネットメールが届いたとする。インターネットはたくさんのネットワークのつながりであるから、AさんからBさんにメールが届くまでに多くのマシンを経由して、AさんのマシンからBさんのマシンに届くことになる。仮に、AさんのマシンからBさんのマシンに届く間にCさんのマシンを経由するとする。この時、CさんはAさんからBさんに宛てたメールを読むことができる（盗聴）。また、それを読むだけでなく、中身を変えてから、何事もなかったかのようにBさんにそのメールを送ることができる（改竄）。そして、CさんにはAさん、Bさんのメールアドレスがあらかじめ分かっていたとしたら、Aさんからメールが来てもいないのに、あたかもAさんからのようなメールをBさんに出すことができる（なりすまし）。

このような危険があるような中では、とてもではないが、取引などビジネスにネットワークを利用することは危険である。そこで、これらの危険を取り去ろうというのが、認証などの概念である。

まず、盗聴の危険から守るためにメッセージを暗号化する。この暗号化の方法には、暗号化する側と復号化する側で共通の鍵を利用する方法（秘密鍵方式）と暗号化する側と復号化する側で異なる鍵を利用する方法（公開鍵方式）がある。

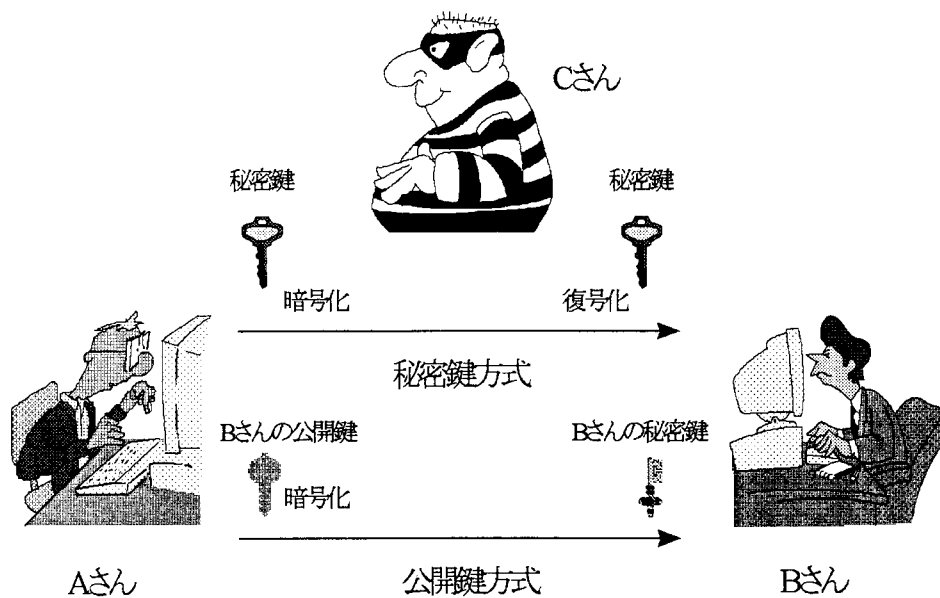


図 2-2 暗号化の方式

秘密鍵方式は暗号化、復号化に同じ鍵を使用する。従って、この鍵が第三者に知られたら、この暗号はやぶられてしまう。ただし、この方式だと、暗号化・復号化の処理が非常に高速に行えるメリットがある(100Mb/s程度)

一方、公開鍵方式は、暗号化鍵を公開してしまう方式である。これは、秘密鍵から公開鍵を求める方法は簡単であるが、公開鍵から秘密鍵を求めるのは非常に困難であるという、一方向性関数（逆関数を求めることが非常に困難な関数）の性質を利用した方法である。この方式では、秘密鍵が流通しないため、鍵が第三者に知られる可能性が非常に低くなる。ただし、この方式では、暗号化、復号化の処理が低速になる(数 10kb/s程度)。

また、この公開鍵暗号方式を利用して、認証機能を実現することができる。例えば、送られてきたメッセージが本当に A さんからのメッセージかどうかを確認したいときには、A さんにいくつかのメッセージを A さんの秘密鍵で暗号化してもらおう。これを A さんの公開鍵で復号化できれば、A さんの秘密鍵は A さんしか知らないものであるから、確かに A さんからのメッセージであると確認できる。

しかし、この公開鍵暗号方式が成り立つためには、「その公開鍵が A さんのものである」ことを証明する信頼できる第三者機関が必要になる。これは、認証機関と呼ばれ、通信当事者から独立した機関である。

暗号化システムとしては次のような製品が提供されている。

- MISTY（三菱電機）
独自の秘密鍵暗号方式を使用している。

暗号化速度は 17Mb/s (Pentium 100MHz 搭載マシン) である。

差分解読法、線形解読法に対して、米国標準の商用暗号 DES よりも十分な安全性を持つことが定量的に証明されている。

- MULTI2/4 (日立製作所)

独自の秘密鍵暗号方式を使用している。

暗号化速度は 2.4~3.2Mb/s (Pentium 133MHz 搭載マシン) である。

アプリケーション・プログラミング・インタフェースをサポート。エンドユーザコンピューティングによるセキュリティの高いシステムを構築できる。

2.3.4 課金

在宅学習システムをネットワーク上で実現する上で、課金は避けて通れない問題である。しかし、現在はまだ方式が確立しておらず、実験レベルのものがほとんどである。ここでは、通産省の電子商取引実証推進事業プロジェクトの紹介にとどめておく。課金の問題については、これからも状況を見つ、今後の課題とする。

電子商取引実証推進協議会は、コンピュータネットワークを用いて商取引、決済等の活動を行う電子商取引（Electronic Commerce, EC）の実現と普及を図るため、通商産業省のエレクトロニックコマース推進事業を通じ、EC 実現のための共通プラットフォームの構築および EC の実証実験の円滑な推進を図るとともに、EC 実現のために必要な制度的課題の検討を行い、また国際的な連携を図り、もって我が国におけるコンピュータネットワークの利用の促進と産業の高度化に寄与することを目的に設立された。

主な活動内容は、

- EC の共通プラットフォームとなる技術の開発についての検討
- EC 実証実験の支援および調整
- オープンなプロセス実現による相互運用性確保とフリーソフトウェアの配布
- EC の制度的課題の検討
- 各国の EC 関係組織との連携
- EC 情報提供サーバーの運営

である。

全部で19の実験プロジェクトが認定されている。

No	プロジェクト名	主管会社・団体	概要
1	サイバースペース上でのECを利用した商施設プロデュースの実験-まちこ-	NTTデータ通信	インターネット上にVirtual Mallの3次元共有空間を実現。参加者規模は1万人から5万人を予定
2	エレクトロニック・マーケット・プレーズ	日本IBM	電子決済機能、ICカードによるプリペイド機能を有するシステムを構築し、モール及び実店舗での実証実験を実施。参加者規模は1万人を予定。
3	仮想社会実験	上田商工会議所	CATV網上にインターネットを用いた仮想都市を構築し、映像情報配信システムを構築する。参加者の規模は1万人を予定。
4	ジャパンネット	三菱商事	他の電子マーケット、特に海外主要電子マーケットとの相互接続・認証の実現のためのシステムを実現。参加者の規模は5万人を予定。
5	電子商取引実証実験 Smart Colloar Club	三菱総合研究所	クレジットカードを活用する小口電子決済システムと銀行が参加する電子マネー・プールという電子決済システムの開発。参加者の規模は5000人を予定。
6	Cyber net club	ユーシーカード	真に世界に通用する証明書の発行が行えるCA局の立ち上げ、ネットワーク上の新決済方法の検討を行う。参加者の規模は最終的に10万人を予定。
7	多目的ICカードによる利便性の高いショッピングシステムの実験	沖電気工業	クレジット、プリペイド、ポイントサービス等の機能を持つICカード並びにKIOSK端末を開発し、キャッシュレスショッピング及び情報提供サービスを実験。参加者の規模は消費者1万人、小売店100店を予定。
8	CCC(サイバーコマースシティ)	関西情報センター	オープンなネットワークを用いて商取引・決済等を行うことにより、様々な産業分野の生産性・効率性の向上を実現するとともに、新たな市場を創出し、関西の産業活性化を図る。
9	メディアポート名古屋	名鉄コンピュータサービス	大量の情報交換が行われる「メディアポート」を建設し、3次元表示による芸術的な魅力をもった仮想都市を建設する。こうした大きな構想の中で、決済・認証などの技術を実証して行く。5000人が参加予定。
10	電子商取引における認証/暗号/決済の方式開発と実用性の実験 Smart Commerce Japan	東芝	クレジットや電子マネー等、多機能な次世代ICカードを使用して、バーチャルモールとリアルモール(実際の店舗)の双方で電子決済及び相互認証を可能とするセキュリティ技術の開発と実証実験を行う。参加者の規模は8万人を予定。
11	仮想展示会を中心としたECの大規模実証実験	NTTデータ通信	ネットワーク上に仮想の展示会を構築することにより、トラフィック集中等の技術的問題の解決や商取引に伴う認証/決済機能等の実用性について実証。
12	バーチャルシティ構想	日本電気/日本総合研究所	消費者の購買動機の誘引から購入に至る行動を主対象とし、魅力ある商品コンテンツ、安心できるセキュリティを装備した電子モールの実証実験。参加者の規模は5万人を予定。
13	電子公共サービス統合システム 〜ワンストップ・サービスの実現	電算	自治体や公共事業の諸手続を一箇所の「バーチャルセンター」に対するアクセスで完了できるようなシステムの構築および実証実験。
14	カードレス・カードシステム・プラットフォーム(CCP)開発実験	野村総合研究所	与信と認証を一体化したプロトコルにより、ICカード等の物理的なカードを使わずに電子商取引を実施するためのシステムの開発。参加者の規模は6万人を予定。
15	EC実験における複合コンテンツサービス開発・提供プロジェクト	びあ	複数のコンテンツプロバイダーの情報を集積し組み合わせた複合情報を一定のインタフェースで提供するための標準仕様の確立及び技術を開発。
16	会話型マルチメディア情報(MHEG)相互交換実験	NTTソフトウェア	MHEGの実験実装規約の作成、MHEGビューア/オーサリングツールの開発により、各種プラットフォーム上にあるMHEGビューア/オーサリングツール間のマルチメディア情報の相互交換を実証。
17	コマース・ナビゲーション・システム	セン情報システムズ	分散リソースの一元的な取り扱いやより高度なユーザインタフェースを提供するエージェントを開発。また、クレジット処理センターとバーチャルモールとのクレジットカード処理が行えるクレジットゲートウェイを開発。
18	セキュアコマースプロトコルを実現する共通プラットフォームの開発	日立製作所/富士通	受発注業務だけでなく、電子決済も含めた様々なやりとりに対応し、取引毎に異なる暗号処理を施すことができるEC環境のセキュリティに関するプラットフォームを構築。
19	非接触ICカードの実証実験	(財)ニューメディア開発協会	ICカードの実装のためのカード本体及びリーダー/ライタを開発。

表 2-8 電子商取引実証推進事業認定プロジェクト