インターネット情報論の基礎(2)
-インターネットサービスとセキュリティ-

土橋 喜
愛知大学現代中国学部

Introduction to Internet (2)
-Internet Services and Security

Konomu DOBASHI
Faculty of Modern Chinese Studies, Aichi University

目 次

8. 8. 電子メールの特徴

》》》 演習 8 《《《

9. World Wide Web

9. 1. ハイパーテキストの意味と機能

9. 2. Web のしくみ

9. 3. URL

》》》 演習 9 《《《

10. システム管理入門

10. 1. なぜ管理者が必要か

10. 2. システム管理の階層構造

10. 3. システム管理の概要

10. 3. 1. ネットワークレベルの管理

10. 3. 2. コンピュータレベルの管理

10. 3. 3. 個人レベルの管理

10. 4. 管理者としての心得

10. 5. セキュリティ

》》》 演習 10 《《《

11. 情報化社会の問題とセキュリティ

11. 1. セキュリティとリスク管理

11. 2. リスクの種類

11. 3. リスクの分析と管理

11. 4. コンピュータセキュリティ

11. 5. コンピュータ関連設備の保護

11. 6. ハードウエアの保護

11. 7. ネットワークの信頼性

11. 8. アクセスコントロール

11. 9. ソフトウエアの品質管理

11. 10. 不正アクセスとセキュリティ対策

》》》 演習 11 《《《

12. セキュリティ対策の方法

12. 1. 物理的なセキュリティ対策

12. 2. サーバのセキュリティ対策

12. 3. ネットワークのセキュリティ対策

12. 4. データのセキュリティ対策

12. 5. ネットワーク特性とコンピュータ犯罪

12. 6. 情報操作による犯罪

12. 7. 有害情報の流通

12. 8. ハイテク犯罪の状況

引用文献

はじめに

本稿はインターネットを中心にした情報ネットワークの基礎的なしくみやサービスについて，情報リテラシーの学習を終えた文科系または社会科学系の学生を対象に，講義内容をまとめたものです．

これからの情報化社会では，インターネットの普及に見られるように，情報ネットワークが果たす役割はますます重要になり，社会基盤として不可欠のものになっています．現代人は今後益々発展する情報化社会の中で，日常生活の中においても情報ネットワークと関わりを深めるようになります．そのためそれらのしくみや基本的な使い方を理解して上手に活用することが必要になります．

本稿ではインターネットを理解するための基礎的な理論について学びながら，パソコンを使って関連した演習を行うことによって，ネットワークの使い方やしくみを体験し，理解を深める工夫をしています．

講義資料として授業で活用するため，全体は 12 章で構成しています．本稿はそのうち後半部分にあたる第 7 章から第 12 章までをまとめたものです．全体構成および各章の概要については次のとおりです．なお第 1 章から第 7 章までの前半部分は前号に記載されています．

7．インターネットのサービス

各種のインターネットサービスは，そのサービスに応じたプロトコルに従って，コンピュータ同士で情報のやり取りを行うことによって実現されています．インターネットを利用する場合には，そのサービスの意味とサービスを受けるために用意されたソフトウエアの機能や使い方を知る必要があります．第 7 章では telnet や ftp によるサービスを取り上げます．

8．電子メールのしくみ

電子メール(e-mail，electronic mail)サービスはインターネットで広く利用され，WWW とともにインターネットの中心的なサービスのひとつとして重要な存在であり，ユーザにとっても親しみのある通信サービスといえます．第8章では電子メールのしくみについて取り上げます．

9．World Wide Web

これまでのインターネットの発展の中で，最も注目を集めたもののひとつが World Wide Web です．現在ではインターネットだけでなく組織内のネットワークでも，文書の閲覧などに標準的に用いられるシステムになっています．第9章では World Wide Web のしくみについて取り上げます．

10．システム管理の基礎

システム管理では，インストールしてシステムを動かすだけではなく，その後の運用を確実にするため，セキュリティを保つことが極めて重要になっています．第10章ではインターネットへの接続を前提にして，システムを管理する上での心構えや管理の概要を紹介していきます．

１１．情報化社会の問題とセキュリティ

情報技術の発展によってさまざまな情報通信基盤が整備された現代社会では，誰もがどこからでも必要な情報を手軽に手に入れることが可能になります．他方，情報化社会にはさまざまな問題も存在することが明らかになっています．第 11 章では望ましい情報化社会を実現するため，セキュリティ対策のあり方を中心に，解決すべきさまざまな課題を取り上げます．

１２．セキュリティ対策の方法

インターネット上では，毎日のように新しいサイバー犯罪の手法が生まれていると言っても過言ではありません．さまざまな不正アクセスや犯罪が頻繁に起きており，それらからネットワークやシステムを守る必要があります．第 12 章では不正が起こりうるさまざまな観点から，セキュリティ対策の方法について取り上げます．

以下に参考までに前半部分の目次と概要を記載します．

（目　次）

》》》　演習　1　《《《

2．　インターネット入門
2．1．　ネットワークと通信
2．2．　インターネットの歴史
2．3．日本のインターネットの始まり
2．4．インターネットの構成
2．5．学術研究ネットワークと商用ネットワーク
2．6．インターネット関連組織
2．7．インターネットの可能性
》》》　演習　2　《《《

3．　インターネットのしくみ
3．1．プロトコルとは
3．2．会話とプロトコル
3．3．データ通信とプロトコルの特徴
3．4．プロトコルの開発と標準化
3．5．OSI 参照モデル
3．6．OSI 参照モデルとデータ送信
》》》　演習　3　《《《

4．　TCP/IP
4．1．TCP/IP プロトコル
4．2．OSI 参照モデルと TCP/IP
4．3．データの単位と名称
4．4．インターネット層
4．5．トランスポート層
4．6．アプリケーション層
4．7．LAN と TCP のヘッダ形式
4．7．1．イーサネットヘッダ
4．7．2．TCP のヘッダ形式
4．7．3．UDP のヘッダ形式
4．7．4．LAN とパケットの送受信
4．8．ヘッダの処理とデータ送受信

》》》　演習　4　《《《

5.　IPプロトコル
5．1．インターネット層とアドレス
5．2．IPアドレス
5．3．IPアドレスの管理
5．4．IPアドレスと3つのクラス
5．5．クラスA
5．6．クラスB
5．7．クラスC
5．8．IPアドレスの不足
5．9．サブネット
5．10．サブネットマスク
5．11．DHCP
5．12．プライベートIPアドレス
5．13．CIDR
5．14．IPv6
》》》　演習　5　《《《

6.　IPの経路制御
6．1.　IPヘッダのしくみ
6．1．2．IPv4のヘッダ形式
6．1．2．IPv6のヘッダ形式
6．1．3．IPv4とIPv6のヘッダ形式の違い
6．2．経路制御
6．3．ICMPプロトコル
6．4．ARPプロトコル
6．5．ARPのしくみ
6．6．ARPとハードウエアアドレスの取得
6．7．RARPプロトコル
6．8．ポート番号
6．9．ドメインネームシステム
6．9．1．ホスト名の管理とDNS
6．9．2．DNSの役割としくみ

6．9．3．ネームサーバとリゾルバ

6．9．4．ドメイン名の多様化

》》》　演習　6　《《《

引用文献

（概要）

1．ネットワークの基礎

現在コンピュータと通信機器は，人間同士のコミュニケーションの道具として社会に広く普及しており，人々の日常生活において情報伝達を支える基盤となっています．高度に発達した情報通信を基盤とする社会を情報化社会と呼ぶことがあります．第1章では今後も社会を支える重要な基盤である情報ネットワークの基礎を取り上げます．

2．インターネット入門

現在では世界中の多くのコンピュータがインターネットに接続し，いまや世界中と情報のやりとりができるようになっています．現代社会においてインターネットに代表されるコンピュータネットワークは，重要な社会基盤のひとつとして不可欠の存在となっています．そのため第2章ではインターネットのしくみを学ぶ前提として，インターネットが発展してきた歴史的な経緯を取り上げます．

3．インターネットのしくみ

インターネットを上手に活用し，そのしくみや社会的な影響などを考えるためには，インターネットを成り立たせている基本的な技術を理解しておくことが必要です．インターネットの情報交換を支えている主要な技術を理解するために，第3章ではプロトコルの基本的なしくみを取り上げます．

4．TCP/IP

現在のインターネットにおいては，TCP/IPプロトコルが広く使われており，信頼性の高いデータ通信を実現しています．第4章ではTCP/IPプロトコルのしくみについて取り上げます．

5．IPプロトコル

インターネットでは主にTCP/IPによるデータ通信が利用され，その通信を成り立たせるために多くのプロトコルが使われています．なかでもIPプロトコル(Internet Protcol)は，インターネット上で行われる通信の宛先を指定する役割を果たしており，最も重要なものになっています．第5章ではIPプロトコルのしくみと役割について取り上げます．

6．IP の経路制御

インターネットでは IP アドレスを使って経路制御を行い，相手先にデータが送り届けられ，それによって通信が成り立っています．第 6 章では IP の経路制御について取り上げます．

7. インターネットのサービス

インターネットに共通のプロトコルであるTCP/IPによってコンピュータが接続されると，お互いに通信が可能になり，この通信を利用したさまざまなサービスを利用することができます．

インターネット上のコンピュータは，TCP/IPに基づいて相互に通信を行っています．各種のインターネットサービスは，そのサービスに応じたプロトコルに従って，コンピュータ同士で情報のやり取りを行うことによって実現されています．またインターネットを利用する場合には，そのサービスの意味とサービスを受けるために用意されたソフトウエアの機能や使い方を知る必要があります．

インターネットを利用したサービスにはさまざまなものがあり，電子メール(e-mail)，ファイル転送，リモートログイン，ネットニュースなどはインターネットの初期の段階から提供されてきました．

1992年にWWW(World Wide Web)が開発されたことをきっかけに，インターネットの利用は一般の人々にとってもさらに身近なものとなり，日常生活においても欠かせないものとなっています．最近ではインターネット上でさまざまな商品の販売契約や決済を行う電子商取引(electronic commerce)や，インターネット経由で銀行などの金融機関の各種サービスを利用できるネットバンキング(net banking)などのサービスも行われています．

さらにラジオやテレビの放送がインターネット上でも行われ，インターネット電話やテレビ会議システムなども利用できるようになっており，今後のインターネットではマルチメディアの活用がさらに重要なものとなります．

これらインターネットで提供されるサービスを受けるためには，受けたいサービスを提供するソフトウエアを用意し，コンピュータにインストールしておくことが必要ですが，最近のOSにはあらかじめ組み込まれているものも多くなりました．ここでは主要なインターネットのサービスを取り上げます．

7．1．telnetとその機能

ネットワークをとおして，仮想端末機能(virtual terminal)を提供する機能がtelnet（テルネット）です．小文字でtelnetと書くときは，アプリケーションソフトウエアの名前として意味することが多く，大文字でTELNETと書いてプロトコルを意味する場合と区別することがあります．

仮想端末機能とは，遠隔地(remote)からネットワークを経由して，物理的には直接接続していない別なコンピュータを利用するために，相手先のコンピュータを自分のコンピュータの画面上に呼び出して使うことができるしくみです．

基本的にはネットワークに接続しており，TCP/IPが用意されているすべてのコンピュータに接続することができます．しかしセキュリティを守るために接続させないところが多くあります．

telnetの機能によってホストコンピュータと遠隔端末のような通信を行うことができます．telnetを利用すれば，自分の目の前で操作しているコンピュータの画面から，ネットワーク上にある遠隔地のコンピ

ュータとの間に，端末をつなげる通信回線を敷設したような感覚で，他のコンピュータに接続することができるので，あたかも遠隔端末のごとく使うことが可能です（図7.1）．

また実際のところは，コンピュータごとにオペレーティングシステムやモニターなどの仕様に違いがありますが，ネットワーク仮想端末(NVT:Network Virtual Terminal)という標準の端末タイプを定義することによって，telnetを使うときにはこれらの違いをユーザが意識しなくても済むようになっています．

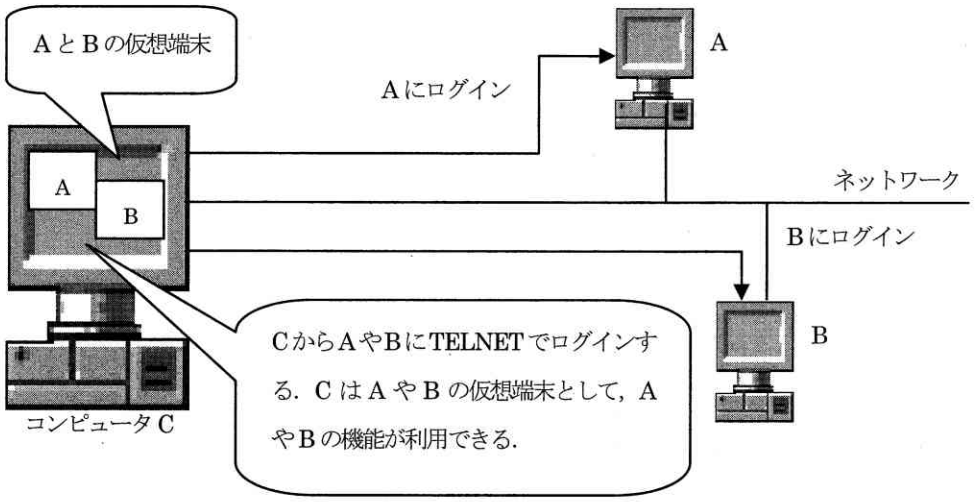

図7.1 TELNETのサービス

TELNETプロトコルを用いたコマンドとして小文字のtelnetが用意されており，相手先のコンピュータにtelnetで接続することをログイン(login)するといい，使い終わって通信を切断することをログアウト(logout)といいます．

使い方の例として，例えば今コンピュータCで作業をしていると仮定したとき，そのときにコンピュータAに置いてあるファイルを参照する必要が発生したとします．そのときはtelnetコマンドを使って，CからAにネットワークを経由してログインし，中にあるファイルを見ることができます．

7．2．telnetのしくみ

telnetによる接続はクライアントサーバ型です．この場合は接続を要求するほうがクライアントで，接続を受け付ける側がサーバになります（図7.2）．

接続を受け付ける側のサーバでは，要求するクライアント側から常に接続要求に応じられるように，デーモンプログラム(daemon program)と呼ばれるものを動かしておく必要があります．

デーモンはオペレーティングシステムによってはシステムプロセス(system process)と呼ばれることも

あります．デーモンというのは元々は守護神という意味です．オペレーティングシステムにおいては，あらかじめデーモンを起動させておき，クライアントから何らかの要求が来るのを待っています．そして要求がきたときに，親のプロセスがその要求を受信し，子のプロセスがその要求に対応して処理を実行するしくみです．親のプロセスはそのまま次の要求がくるのを待機しています．telnet のほかにも ftp や電子メールサーバなど，さまざまな用途のデーモンがあります．

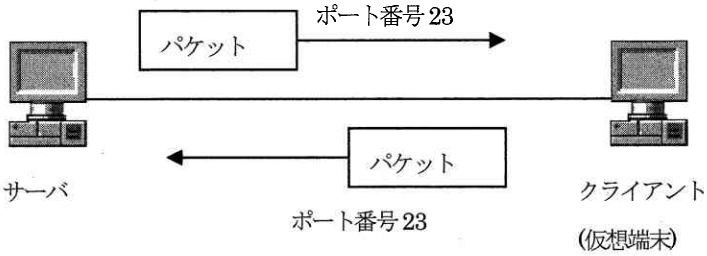

図 7.2 telnet とパケットの送信

Windows(2000 Server, XP Professional)では Telnet サーバがそのデーモンプログラムになっています．また Linux(UNIX)などでは，telnetd(telnet daemon の略)と呼ばれるプロセスか，またはこの telnetd を呼び出す xinetd デーモンというプログラムを常に動作させておくことによって，クライアントからの接続要求に応じられるようにしています．

また telnet では文字データを送受信するため正確な通信が要求され，必ず TCP プロトコルが使われます．また TCP ヘッダに付加される宛先ポート番号は 23 番に決められています（図 7.2）．

telnet では，「telnet ホスト名 [ポート番号]」という形式で，指定したホストのポート番号に対して，TCP のコネクションを確立します．ポート番号が指定されていないときは，23 番のポートにつながり，遠隔ログイン（remote login）とほぼ同じ働きをします．

7．3．telnet の例

以下に telnet で接続した例を示します．接続先のサーバは mc_srv という名前のコンピュータです．( )内はシステムが表示するメッセージに対して説明を加えたものです．

Windows の場合は「スタートメニュー」→「すべてのプログラム」→「アクセサリ」の順にたどり，コマンドプロンプトを起動して行います．

コマンドプロンプトの画面の中で telnet コマンドを入力し，接続したいサーバの名前(または IP アドレス)を指定します．正しく接続すると，login プロンプトが表示され，ユーザ名の入力待ちになります．プロンプト(prompt)は，コンピュータがユーザに対して入力を促すために，英文字や記号使ったメッセージのことです．

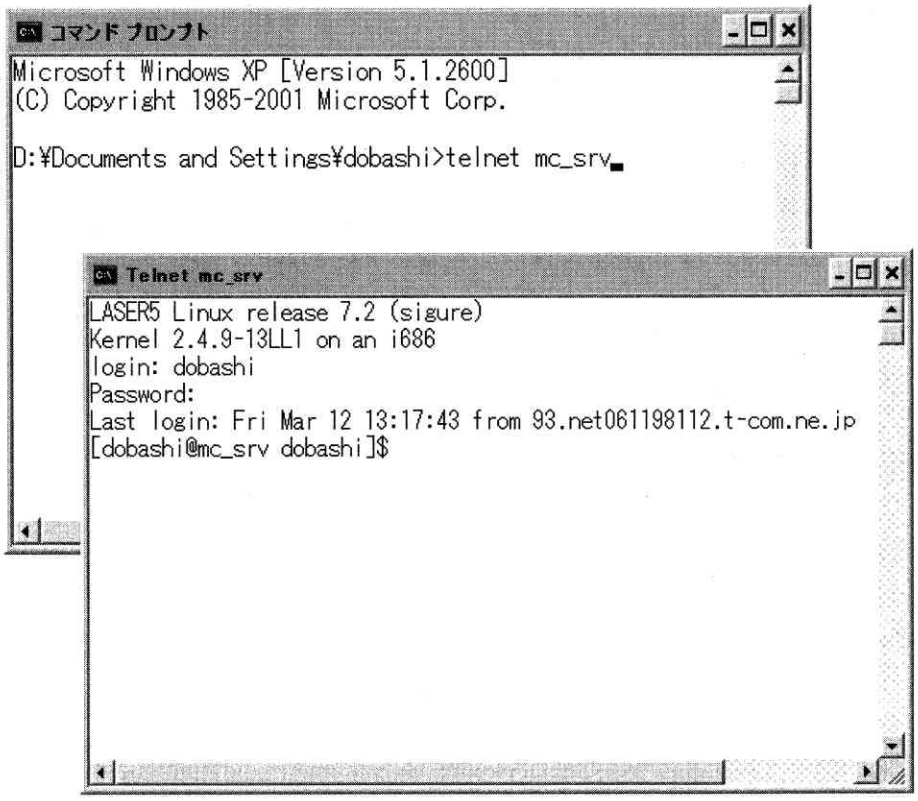

図7.3　コマンドプロンプトからのtelnetの起動と接続例

ユーザ名が入力されて登録されているユーザであることが確認されると，パスワードの入力が要求されます．その際にパスワードはセキュリティ対策のため他人に見られないように，入力しても何も表示されません．これはftpなどのときも同じです．

ユーザ名とパスワードの一致が確認されるとloginが許され，遠隔端末として使えるようになります．さらに前回loginした日時やどこのコンピュータからloginしたかなどが表示され，メールの着信状況なども表示されています．

C:¥Documents and Settings¥dobashi>telnet mc_srv (telnetコマンドと接続先のコンピュータ名を入力)
LASER5 Linux 6.0 (Raiden)
Kernel 2.2.16 on an i686
login: dobashi (ユーザ名の入力)
Password: (passwordの入力．入力しても他人に見られないように何も表示されない)
Last login: Mon Nov 4 11:08:14 from 153.net061211185.t-com.ne.jp (前回のloginの記録)
You have new mail. (メール受信状況のお知らせ)
[dobashi@mc_srv dobashi]$ ls (lsコマンドでディレクトリ内を表示)
Desktop/ book.html menber.html net_ab02_05.doc

```
Mailbox  kisoron02_06.doc  net_ab02_04.doc
[dobashi@mc_srv dobashi]$ exit                                    (telnetの終了)
```

また次の例はaquaというコンピュータにtelnetで接続した例です．このコンピュータには前回loginした日時やコンピュータのIPアドレスは表示されていますが，新しいメールは届いていないためメール着信状況は表示されていません．またシステムのメッセージについて，上の例と同じものの説明は省略しています．

```
C:¥Documents and Settings¥dobashi> telnet aqua
Red Hat Linux release 6.2 (Zoot)
Kernel 2.2.18 on a 2-processor i686
login: 98c1001
Password:
Last login: Tue Nov  5 20:01:33 from 202.250.164.189    (前回ログインした記録)
[98c1001@aqua 98c1001]$ ls
Desktop  cal04.txt  pyth  testfile
[98c1001@aqua 98c1001]$
```

telnet本来の使用目的は，コンピュータを遠隔地から操作して利用することにあります．しかしtelnetとポート番号を組み合わせて使うと，さまざまなアプリケーションと通信を行うことができます．

例えばポート番号80はWebページを送受信する際に使われるので，telnetでこのポート番号を指定すれば，HTTPサーバと通信することができます．

以下の例はwww.aichi-u.ac.jpというWebサーバに，ポート番号を80に指定してtelnetで接続したものです．まず「telnet www.aichi-u.ac.jp 80」を入力します．

すると相手のサーバに接続してTCPのコネクションが確立し，通信可能な状態になりますが，相手のサーバからは何も応答してきません．

そこでHTTPサーバと通信を行うため「GET /index.html HTTP/1.0」と入力します．この命令はHTTPプロトコルにおいてWebページの送受信を要求するもので，HTTPサーバはこの要求に従いindex.htmlのテキストデータを送信してきます．

```
[dobashi@mc_srv dobashi]$ telnet www.aichi-u.ac.jp 80
Trying 203.181.118.184...
Connected to www.aichi-u.ac.jp.
Escape character is '^]'.                              (ここで入力待ちになる)
GET /index.html HTTP/1.0                               (Enterキーを2回押す)
```

(以下にindex.htmlのテキストデータが表示される．画像などは見えない)

この場合にtelnetはHTTPサーバのクライアントになりますが，Webページを表示するブラウザではないため，HTMLの内容を解釈できません．そのためこのようにtelnetでWebページの送受信を行うと，ページ内に画像などのデータが含まれていても，telnetの画面には文字だけが表示されます．つまりindex.htmlのテキストファイルの内容がそのまま表示されることになります．これらの例をとおしてアプリケーションプログラムとtelnetが行われることがわかります。

7. 4. ftp

ftpはTCP/IP通信のアプリケーションソフトウェアのひとつです．ftpはファイル転送(file transfer)を行うためのプロトコルであり，またコマンドの名前にもなっています．プロトコルの意味を強調したいときはFTP(File Trandfer Protocol)と大文字で書くことがあります．

ftpはネットワークに接続したコンピュータとの間でファイルの転送サービスを提供するものです．インターネットの誕生のころから，WWWの利用が盛んになる1990年代の中ごろまで，インターネットを利用する目的のひとつは，遠隔地のコンピュータ上のファイルを転送することにあったといわれています．その際に使われてきたのがFTPです[引用文献16]．

ファイル転送というのは，別なコンピュータの中にあるファイルを自分のコンピュータに持ってきたり，逆に自分のコンピュータの中にあるファイルを別なコンピュータに送り込むことを意味しています(図7.4)．FTPプロトコルを用いたftpプログラムは，任意の大きさのファイルを送受信することが可能になっています．

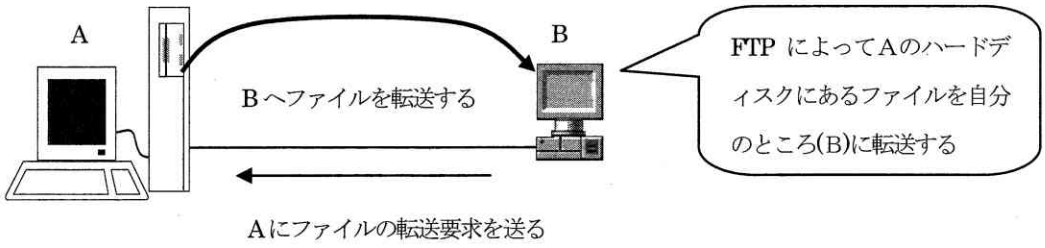

図7.4 FTPとファイル転送

ftpは基本的にはネットワークに接続されているコンピュータとの間で，自由にファイルの転送が行えます．しかしこのサービスを提供するかどうかはセキュリティ対策の問題があり，自由に行えないようにしている場合も多くあり，これはtelnetなど他のサービスにも同様のことがいえます．

ftpでファイルを持ってきたりすることをダウンロードするといい，また送り込むことをアップロードするということがありますが，これらのことができるためにはそのホストにユーザ登録されている必要があります．

現在も広く一般に公開され，誰でもダウンロードできるファイルもいろいろあります．このように誰でもアクセスを許

している ftp を anonymous ftp といい，このようなサービスを提供しているところ（サイト：site）も多数あります．anonymous というのは「匿名」という意味です．anonymous ftp を公開しているところでは，コンピュータにユーザ登録されていなくても，指定されたユーザ名やパスワードで，ftp を利用することができます．

7．5．ftp のしかたとコマンド

最近の WWW ブラウザは ftp に対応しており，それらを使えば Web ページの検索を行うような感覚で簡単に ftp を行えます．しかしディレクトリが WWW に公開されていない場合はブラウザではできませんので，ftp のコマンドを使うことになります（図 7.5）．

ftp のコマンドは Windows でも Linux でもほとんど同じように使えます．しかし dir と ls のようにディレクトリやファイル名を表示するコマンドを使うときには，Windows 上で作業をしているのか，Linux 上で作業をしているのかによって異なり，初心者などの場合は注意が必要になります．

表 7.1 ftp の主なコマンド

open	ftp サーバへの接続をする．open の後ろにホスト名などを書く．
ls	現在作業中のディレクトリのファイル名を表示する(Linux)．
cd	作業するディレクトリを移動する．
get	サーバからファイルを 1 つ転送する．
mget	サーバからファイルを複数転送する．
put	ファイルをサーバへ 1 つ転送する．
mput	ファイルをサーバへ複数転送する．
close	ftp サーバとの接続とやめる．
quit	ftp コマンドを終了する．

7．6．ftp でファイルを受信(get コマンド)

以下では Windows のコマンドプロンプトを使い，Linux の mc_srv というコンピュータに ftp コマンドを使った例を示します．以下の例を見ると，get コマンドによって testfile というファイルを受信していることが分かります．転送するときは，転送間違いを少なくするため，バイナリモード(binary mode)を指定して行います．

ファイルを受信するときは，受信したいディレクトリ（フォルダ）で ftp を起動すると，ファイル名を指定するだけでそのディレクトリに受信できます．

```
C:¥Documents and Settings¥dobashi>ftp mc_srv                    (ftp で mc_srv に接続する)
Connected to mc_srv.aichi-u.ac.jp.                              (mc_srv.aichi-u.ac.jp に接続)
```

```
220 mc_srv.aichi-u.ac.jp FTP server (Version wu-2.6.0(1) Fri Jun 23 09:17:44 EDT2000) ready.
User (mc_srv.aichi-u.ac.jp:(none)): 98c1001                    (ユーザ名の入力)
331 Password required for 98c1001.                             (パスワードの要求)
Password:                                                      (パスワードを入力する)
230 User 98c1001 logged in.                                    (ログインの許可)
ftp> ls                                                        (ls でファイル名を表示)
200 PORT command successful.                                  (コマンドが受け付けられたというメッセージ)
150 Opening ASCII mode data connection for file list.          (ファイル一覧のメッセージ)
cal04.txt
testfile                                                       (受信したいファイル)
226 Transfer complete.                                         (上の2行の転送完了メッセージ)
ftp: 21 bytes received in 0.01Seconds 2.10Kbytes/sec.
ftp> bi                    (バイナリモードを設定するコマンドbi を入力. 転送の間違いが少ない)
200 Type set to I.                                             (バイナリモード設定を完了)
ftp> get testfile                  (get コマンドを入力して testfile ファイルを受信する)
200 PORT command successful.                                  (コマンドが受け付けられた)
150 Opening BINARY mode data connection for testfile (28 bytes).
226 Transfer complete.
ftp: 30 bytes received in 0.00Seconds 30000.00Kbytes/sec.
ftp> close                                                     (close コマンドで接続をやめる)
221-You have transferred 30 bytes in 1 files.
221-Total traffic for this session was 578 bytes in 2 transfers.
221-Thank you for using the FTP service on mc_srv.aichi-u.ac.jp.
221 Goodbye.
ftp> quit                                                      (quit コマンドで ftp を終了する)
C:¥Documents and Settings¥dobashi>                             (コマンドプロンプトに戻る)
```

7. 7. ftp によるファイル送信(put コマンド)

次の例は Windows から Linux の mc_srv というコンピュータに ftp で接続し, put コマンドを使って ipmsg147.lzh というファイルを送信したときのものです.

なおファイルを送信するときは, 送信したいファイルがあるディレクトリで ftp を行うと, ファイル名を指定するだけで行えます.

```
C:¥Documents and Settings¥dobashi>ftp mc_srv                    (ftp コマンドで接続)
Connected to mc_srv.aichi-u.ac.jp.                    (mc_srv.aichi-u.ac.jp.に接続)
220 mc_srv.aichi-u.ac.jp FTP server (Version wu-2.6.0(1) Fri Jun 23 09:17:44 EDT2000) ready.
User (mc_srv.aichi-u.ac.jp:(none)): dobashi                    (ユーザ名の入力)
331 Password required for dobashi.                    (パスワードの要求)
Password:                    (パスワードを入力する)
230 User dobashi logged in.                    (ログインの許可)
ftp> bi                    (バイナリモードを設定するコマンドbi を入力. 転送の間違いが少ない)
200 Type set to I.                    (バイナリモード設定を完了)
ftp> put ipmsg147.lzh                    (put コマンドでファイルを送信)
200 PORT command successful.
150 Opening BINARY mode data connection for ipmsg147.lzh. (バイナリモードでコネクションを確立)
226 Transfer complete.                    (転送の完了)
ftp: 79479 bytes sent in 0.01Seconds 5298.60Kbytes/sec.
ftp> ls                    (ls コマンドでファイル名を確認)
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
ipmsg147.lzh                    (送信されたファイル)
226 Transfer complete.
ftp: 14 bytes received in 0.00Seconds 14000.00Kbytes/sec.
ftp> ls -a                    (ディレクトリ内を全部表示する)
200 PORT command successful.
150 Opening ASCII mode data connection for directory listing.
.
..
.Xdefaults
.bash_history
(中略)
.screenrc
Desktop
Mail
ipmsg147.lzh                    (送信されたファイルの名前)
226 Transfer complete.
ftp: 184 bytes received in 0.00Seconds 184000.00Kbytes/sec.
```

```
ftp> quit                                                    (ftp の終了)
221-You have transferred 79479 bytes in 1 files.
221-Total traffic for this session was 80300 bytes in 2 transfers.
221-Thank you for using the FTP service on mc_srv.aichi-u.ac.jp.
221 Goodbye.
C:¥Documents and Settings¥dobashi>
```

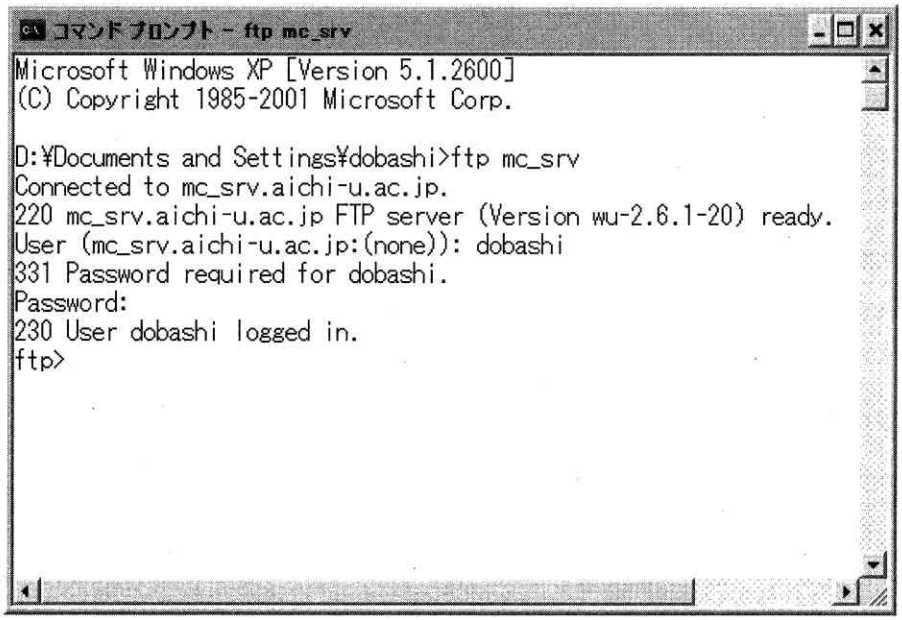

図7.5　コマンドプロンプトからftpを起動してログインした例

》》》 演習 7 《《《

ネットワークを管理するソフトなどを使い次の演習を行ってみよ.

1．telnet(その1)

telnetコマンドを使って，仮想端末の遠隔操作がどのようなものかを体験してみよう．telnetをやめるときはexitコマンドを入力する.

（1）　telnetコマンドを使い，グローバルIPアドレスが割り当ててあるmc_srvというコンピュータにログインし，nslookupを使い南開大学のネームサーバを調べる.

（2）次にpingコマンドを使い，通信ができるかどうかを調べる．上と同じようにGoogleと通信できる

かどうか確認せよ.

（3）Linux では tracert の代わりに traceroute が使われる．mc_srv からも traceroute を試してみよ.

[98c1001@mc_srv 98c1001]$ /usr/sbin/traceroute google.co.jp

2．telnet(その2)

学生の場合は nmoon にメールを送ると，nwmail という Web メール用のサーバで受信することができる．nwmail にメールが溜まっている間は，telnet で接続してメールを確認することができる．次の手順で nwmail で受信したメールを telnet で接続して内容を確認してみよ.

（1）まず自分で nmoon のアドレスにテスト用の数行程度のメールを送る．なお内容を確認するため，ローマ字でメールの本文を作成する(日本語だと文字化けすることがあるため)．本文は「This is a test mail from dobashi.」程度でよい.

（2）そのメールを nwmail で受信する.

（3）Windows のコマンドプロンプトを使い，telnet で nwmail に接続する.

（4）ls コマンドで Mail フォルダを確認し，メールが溜まっているディレクトリに移動する.

（5）less コマンドで自分の送ったものかどうかメールの中身を確認する．以下の部分を参考にせよ.

(nwmail に telnet で接続する)

```
[dobashi@nwmail dobashi]$ ls                                    (ディレクトリ内の表示)
Desktop  Mail  ipmsg147.lzh
[dobashi@nwmail dobashi]$ cd Mail                               (Mail に移動)
[dobashi@nwmail Mail]$ ls                                       (ディレクトリ内の表示)
draft  ginbox  sent  trash
[dobashi@nwmail Mail]$ cd ginbox                                (メールの本文がたまる ginbox に移動)
[dobashi@nwmail ginbox]$ ls                                     (ここでメールの番号が見える)
1  2
[dobashi@nwmail ginbox]$ less 2                                 (less コマンドで2番のメールの内容を表示)
(メールのヘッダ部の前半を省略)
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2800.1106
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1106
X-UIDL: 98~"![9Q"!j^0"!~~:"!

This is a test mail from dobashi.                               (テストメールの本文)
```

3．ftp(その1)

（1）これまでのレジュメを参考に，nwmail に受信したテスト用のメールを，ftp を使い Windows の自分のディレクトリ(マイドキュメント)に持ってきてみよ.

（2）ftp(その2)

ftp を使い，Windows のマイドキュメントにあるファイルを何かひとつ mc_srv に送信してみよ.

》》》 本章の復習 《《《

（1）telnet はどのようなサービスを提供する機能か.

（2）login と logout はどのような意味か.

（3）デーモンプログラムとはどのようなものか.

（4）ftp とはどのよなサービスを提供するものか.

（5）ftp は何の略か.

（6）ftp でファイルを取ってくる命令は何か.

（7）ftp でファイルを送り込む命令は何か.

8. 電子メールのしくみ

電子メール(e-mail, electronic mail)は米国の Ray Tomlinson によって 1971 年に開発されたものが最初であり，ARPANET に接続しているコンピュータを結んで始めての送受信が行われました[引用文献 17].

最近は携帯電話などからも電子メールが使われ，インターネットの中心的なサービスのひとつとして重要な存在であり，Web ページの閲覧と合わせて，一般ユーザにも広く普及した通信サービスになっています．インターネットの世界的な普及と発展の中で，さまざまな人々のコミュニケーションにとって電子メールが果たす役割は大きく，現在でもなお重要な通信手段となっています．

電子メールはコンピュータネットワークにおいて，ファイルの送受信を利用して行う電子的な郵便の配送システムといえます．例えば従来のはがきや手紙による郵便では，相手に届けたいときに，表に届け先の郵便番号・住所・氏名などを書きます．そして発信元として同様に自分の住所氏名などを書き添え，はがきの場合は裏に伝えたい内容を書き，手紙の場合は文書を書いて封筒の中に封入します．それを郵便ポストに投函すれば，あとは郵便局が自動的に相手に配達してくれるしくみになっています．

基本的には電子メールも，手紙や葉書を送る郵便のしくみと同じような考え方に基づいて，システムが考案されています．電子メールではコンピュータで作成した電子的な文書を，インターネットを経由して宛先に届けられるという点が，従来の郵便とは大きく異なる点です．このときの一連の作業は，インターネットに接続しているコンピュータがあれば，自分でメールソフトを操作して簡単に行うことができます．

電子メールは宛先が世界中のどこであっても，あるいは同じ建物の隣の部屋でも同じように送ることができます．メールの到達に必要な時間も，ネットワークが正常ならば，ほとんどの場合は数秒で，長くても数分ほどで済んでしまいます．

相手がすぐさまメールを読んでくれる場合には，リアルタイムに近いやり方でメッセージの交換を行うことができます．しかし実際のところは相手がメールを読んでくれるかどうかは別問題です．

インターネットに接続したコンピュータが使えるときは，電子メールを送り届けるだけなら時差や送信料などのコストを気にすることもありません．自宅から電子メールを使う場合には，インターネットに接続するためにプロバイダと契約して使用料を支払い，その接続料の中に電子メールの使用料も含まれているのが一般的です．

これに対して携帯電話を使った電子メールは，送受信するパケットの通信量を基準に課金される場合や，定額制の使い放題もあるなど，各事業者により課金の方法が多様化しています．

8. 1. 電子メールアドレス

電子メールを送信するときに，送り先の住所と氏名にあたるものが電子メールアドレス(e-mail address)です．これは郵便の場合では，送り先の住所と氏名にあたるものです．

電子メールアドレスも DNS におけるドメイン名の階層構造を利用しており，一般的な形式は次のように

なっています.

アカウント名@ホスト名．組織名．組織属性．国別コード

アカウント名はメールサーバに登録されているユーザのアカウントになります．電子メールアドレスの後半部分の「組織名．組織属性．国別コード」の部分は，DNS ではドメイン名にあたる部分と同じです．

またドメイン名の先頭にホスト名を加えた「ホスト名．組織名．組織属性．国別コード」の部分，つまり@（アットマークと読む）から右側の部分を FQDN(Fully Qualified Domain Name)と呼ぶことがあります．ホスト名やドメイン名だけでは，インターネット上でそのホストだけを特定することはできません．しかし FQDN による表記を使えばどのホストであるかを確実にひとつだけ特定することが可能になります．

例えば多くの大学では学生のアカウントを登録するときに学籍番号を使います．そのときに 98c1001 という学籍番号をアカウントとして登録されたとすれば，そのユーザの電子メールアドレスは次のようになります．

98c1001@nmoon.aichi-u.ac.jp

この例では学籍番号をそのままアカウント名に使っていますが，suzuki のように別な名前を付けることも可能です．また nmoon はメールサーバのホスト名になっており，このコンピュータに登録されいる人はここにメールが届きます．ホスト名を使うかどうかは，メールサーバの設定により，使わなくてもよい設定を行っているところもあります．例えば次の例のようにドメイン名だけでも使えるようにしているところもあります．

dobashi@aichi-u.ac.jp

メールサーバはこれらのアドレスを見て，決められた送信先へとメールを送り出していきます．

電子メールはインターネット上の多くのコンピュータの中から，アカウントが登録されているコンピュータ（メールサーバ）を探し出して届けられます．そのときにまずホスト名のコンピュータにメールが届き，さらにユーザに配信されます．

8. 2. 電子メールのしくみ

電子メールは，大きく分けて 2 つのソフトから構成されています．ひとつは電子メールのユーザがメールの読み書きを行うソフトであり，あとひとつはインターネット上でメールを指定されたアドレスに配送するソフトです．

電子メールを読み書きする機能は，使用するソフトウエアによって異なります．この機能は我々が手作業で葉書を書いたり，送り先の住所や氏名を書いたりすることに相当する機能です．一般的にメールリーダやメールソフトなどといわれるものが該当するソフトウエアで，さまざまなものが提供されています．

あとひとつは電子メールをネットワーク上の指定されたメールサーバのアドレスに配送するためのもので，郵便局の仕事と同じ役割をするMTA(Message Transfer Agent)という機能がメールサーバに備わっています(図8.1)．

ネームサーバでは，MXレコード(MX record, Mail eXchange Record)と呼ばれる電子メール交換レコードを蓄積しており，このデータはメールサーバのIPアドレスやホスト名などの情報から構成されています．そしてMTAから問い合わせがあったときに，ネームサーバは送信すべきドメイン名に対応するメールサーバのIPアドレスとホスト名を回答してくれます．

MTAは一般ユーザが電子メールを送受信するときは，ほとんど意識しなくても済むようになっています．メールリーダなどの読み書きする機能でユーザが作成した電子メールを，ネットワークをとおして実際に配送します．この機能は郵便の集配局に相当する仕事をしており，作成されたメッセージを指定した送り先のメールサーバへ向けて配信します．

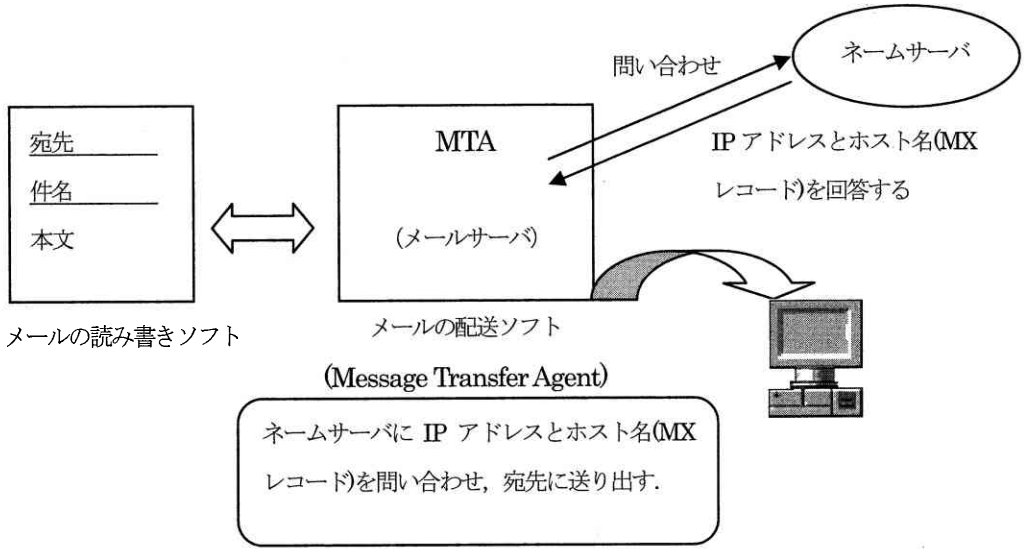

図8.1 電子メールソフトウエアのしくみ

8. 3. 電子メール配信の手順

電子メールは次のような手順で，ネットワークを経由して配信されていきます．

（1）ユーザがメッセージの作成を行い送信する．

（2）メッセージはいったんユーザが登録されたMTAの内部にたまる．

（3）MTAはDNSに対してメールアドレスに対応するIPアドレスとホスト名（MXレコード）の問い合わせを行う．

（4）DNSはMTAへIPアドレスとホスト名を知らせる．

（5）MTAはDNSから知らされたIPアドレスに向けてメールを送信する．

例えば誰かがメールを作成し98c1001@nmoon.aichi-u.ac.jp宛てにメールと送ったとします．するとMTAに送信命令が届き，MTAはDNSに対して98c1001@nmoon.aichi-u.ac.jpに対応するIPアドレスとホスト名を要求します．そしてDNSからIPアドレスが得られると，そのIPアドレスにメールを送り出します．

メールアドレスを間違えると，電子メールは送った人に返送されるようになっています．これはメールアドレスのドメイン名から正しくIPアドレスを知ることができなかったり，届けたいユーザのアカウント名を間違えたために正しく届けられなかったためです．

なお広く使われているMTAソフトウエアにsendmailやqmailなどがあります．

8．4．SMTPプロトコルとメールの配送

インターネットで電子メールの送受信を行う場合，MTA 間で電子メールの配送を行うプロトコルは，SMTP(Simple Mail Transfer Protocol)が使われます．SMTP は TCP/IP の上位層に該当するプロトコルで，TCP のコネクション上で通信を行います．

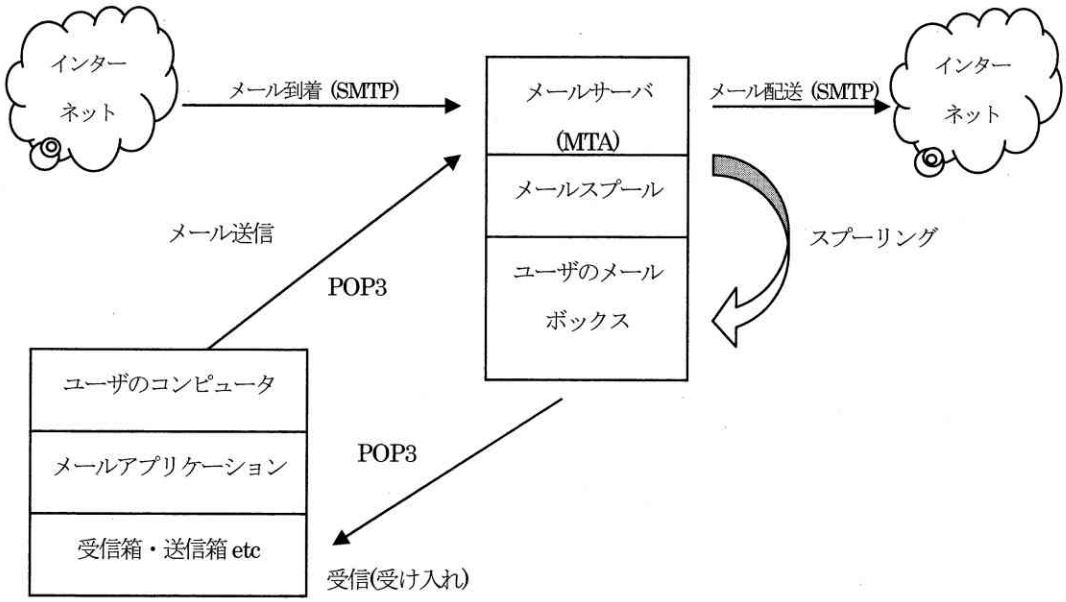

図 8.2 SMTP とメール配送のしくみ

また MTA を動作させているコンピュータをメールサーバといいますが，メールサーバとユーザのメールソフトとの間でメールをやり取りするときは，POP(Post Office Protocol)あるいはより新しい POP3 というプロトコルが多く使われています（図8.2)．

また最近よく使われる IMAP(Internet Message Access Protocol)というプロトコルは，利用法においてより

改良されており，届いたメールはメールサーバ上で管理することができるので，届いたメールの発信者やタイトルを確認してから，受信するかどうかを決めることができます．この点でメールの添付ファイルにウイルスが含まれている場合などは，事前にチェックが可能となり，セキュリティ対策上も効果があります．

また携帯電話や持ち運ぶノートパソコンなどのモバイル環境では，インターネットにつながればどこでもメールを受信できるので便利ですが，サーバがダウンするとすべてのメールが読めなくなる欠点があります．加えてIMAPサーバでは，ユーザのメールをサーバで長期間保存することになるため，サーバ側に大容量の記憶装置とそれに対応した処理能力が必要にもなります．

メールサーバに接続する設定を行うときは，多くの場合POP(POP3)を選んでクライアントの設定を行いますが，IMAPも使えるかどうかはIMAPサーバを動作させておく必要があるため，確認も必要です．

8.5. 電子メールの形式

電子メールが正しく送り先に配送されるためには，MTAとユーザのメールアプリケーションの間でもやはりプロトコルが必要になり，このひとつが上で述べたPOP(POP3)です．

葉書を出す場合でも，相手先の正しい住所や氏名を書かなければ，届かないことになりかねません．郵便などの場合は，宛先などに多少の間違いがあっても，配達する人がいろいろと考えてくれ，相手に正しく届けられることもあります．電子メールの場合は，人間が配達するようなわけには行かず，正確なメールアドレスを書かなければ相手に届かなくなってしまいます．

電子メールについては，TCP/IP通信について取り決めたRFC822という文書に，守らなければならない電子メールの書式などが決められています．ユーザが一般的に使うメールリーダなどのソフトは，この書式に基づいており，この書式を守らないメールは送り先に正確に配送することはできません．

8.6. 電子メールのヘッダ情報

電子メールは，メールの先頭に付加されるヘッダと呼ばれる部分と，主にメールの本文からなるボディから構成されています．ヘッダには電子メールを正確に配送するために必要なさまざまな情報が付加されています（図8.3）．

ヘッダの書式は，インターネットの電子メールの仕様を定めた文書であるRFC822によって，明確に定められています．インターネット上の電子メールは，全てこの文書に定められたヘッダが付加されて送受信されます．このヘッダには，送り先のアドレスや件名など，ユーザが入力した情報から生成されるものもあり，これらの元データはユーザ自身で書き込みます．

Return-Path: <owner-real@bmail.future-s.com>

Delivered-To: dobashi@vega.aichi-u.ac.jp

Received: (qmail 31969 invoked from network); 26 Sep 2000 16:05:55 +0900

Received: from president.dragonfield.com (210.158.212.214) by vega.aichi-u.ac.jp with SMTP; 26 Sep 2000 16:05:55+0900

Received: (qmail 3482 invoked by uid 1001); 26 Sep 2000 15:11:14+0900

Date: Tue, 26 Sep 2000 10:00:00 +0900

From: RealNetworks <mktg@realnet.co.jp>

Reply-to: real@dragonfield.com

Subject: RealNews 2000 Sep. vol.18 (No.30)

Message-Id: <real.20000926@bmail.future-s.com>

MIME-Version: 1.0

Content-Type: text/plain; charset=iso-2022-jp

Content-Transfer-Encoding: 7bit

X-Mail-Agent: BoostMail 3.0

To: dobashi@vega.aichi-u.ac.jp

X-Mozilla-Status: 8001

X-Mozilla-Status2: 00000000

X-UIDL: 7&h!!Im#"!`_="!X$+!!

----------(この線から上がヘッダで下がボディ)

「RealNews」は、Real 製品のダウンロード時、またはインストール時に

入力されたメールアドレスにお送りしています。

図 8.3 電子メールのヘッダとボディ

またボディは電子メールの本文であり，郵便なら通信文の内容にあたります．ボディには特に制限はありませんが，実際には使用する文字コードなどが決められています．

初期のインターネットでは，電子メールはテキスト形式のメッセージを送受信するために，米国の情報交換用標準コードである ASCII(American National Standard Code for Information Interchange)コードが使われていました．この文字コードでは 7 ビットによる表現が使われているため，2 の 7 乗（128 種類）の文字や特殊記号を表現することができました(RFC822)．しかし日中韓などの諸国をはじめ，アルファベットを使わない国々では，この文字コードでは必要な文字を扱うことができませんでした．

そのため 1992 年に，インターネット上の電子メールの送受信を，より多くの言語やテキスト形式以外の

データにも対応させるために，MIME(Multipurpose Internet Message Extensions)という拡張形式が採用されています（RFC1341，RFC1342）.

これによって電子メールのヘッダや本文にも，非 ASCII 文字つまりアルファベット以外の文字を使うことができるようになりました．またテキスト形式で送信する以外に，HTML 形式で Web ページをそのまま送ったり，写真や動画像や音声などのファイルなども送ることもできるようになりました.

テキスト形式以外のデータを送信するときは，メールソフトが送信したいファイルを電子メールで送信できる形式に変換して送ります．このような変換を符号化(encode)と呼んでいます.

この符号化によって，どのようなファイル形式で送信したか，どのような符号化を行ったかがメールヘッダに記録されます．受信する側では，ヘッダの情報に基づいて復号化(decode)し，もとのファイルを復元することによって，内容を見ることができます[引用文献 16].

表 8.1 電子メールヘッダの主なフィールドと意味

フィールド名	意　味
Return-Path	メールの返送先
Delivered-To	メールの配達先
Received	MTA による配信経路情報の記録．中継する MTA は情報を追加する
Date	メールが送信された日時
From	発信者の名前とアドレス
Reply-to	返信メッセージを From で指定したアドレス以外に送る場合に使用
Subject	メールのタイトル，件名，見出し
Message-Id	メールサーバが送信メールに割り当てた識別番号
MIME-Version	電子メールのファイル形式を定めた規格のバージョン
Content-Type	含まれているテキストの種類
Content-Transfer-Encoding	配送時に符号化されたコード名
X-Mail-Agent	送信者が利用したメールソフトの種類とバージョン．「X-」で始まるヘッダは独自に拡張されたヘッダ
To	送り先のアドレス．カンマ(,)で区切ると，複数のアドレスに送信できる
X-UIDL	POP サーバが届いたメールを区別するために割り振る識別番号
Cc	To と Cc フィールドの両方のアドレスにメールを送信する
Bcc	Bcc に指定したアドレスだけにメールのコピーを送る．To と Cc フィールドの人には送信されない

“Content-Type: text/plain; charset=iso-2022-jp”の部分は，本文のデータ形式を示しており，イン

ターネットの初期の規格(RFC822)で配送されたテキスト形式のファイルであることを示しています．また“charset=iso-2022-jp”の部分は，JIS によって定められている日本語の文字コードである iso-2022-jp によって，符号化されていることを示します．

なお日本語の文字コードには，1バイト文字 (ASCII 文字と1バイトのカタカナ) と2バイト文字 (漢字，ひらがな，カタカナ，各種記号) のコードが混在していますが，iso-2022-jp ではエスケープシーケンスを使って，1バイト文字と2バイト文字の識別をおこなっています．

さらに日本語の2バイト文字は8ビットであるため，“charset=iso-2022-jp”の部分は，符号化方式を示していると同時に，8ビットの文字は電子メールで送信できるように，iso-2022-jp で定められた7ビットの文字に変換したことを示しています．

この部分のデータ形式は，HTML 形式で書かれたものには“text/html”と表示され，JPEG(Joint Photographic Experts Group)の画像ファイルのときは”image/JPEG”と表示されます．

“Content-Transfer-Encoding: 7bit”の部分は，送信時の符号化方式を示しており，電子メールは7ビットで送信されるので，この場合は符号化されていない7ビットの文字 (8ビットのうち最上位ビットが0) を使っていることを示します．符号化されている場合は，quoted-printable や base64 など他の符号化方式の名称によって示されます．

図8.3のメールは RealNews 社から筆者へ届いた広告のメールです．このメールは Netscape の Messenger で開きました．ヘッダの主なフィールドの意味はおおよそ表 8.1 のようになっています．なお「X-」で始まるヘッダは，独自に拡張されたヘッダであることを示しています．

8. 7. Cc フィールドと Bcc フィールド

複数の人にメールを送る場合，To と Cc(Carbon Copy)と Bcc(Blind Carbon Copy)のフィールドを使い分けることがあります．例えば，dobashi，suzuki，sato，hayashi の4人にメールを送る場合を考えてみましょう．

全員に同じ内容のメールを送りたいときは，To フィールドを使って全員のアドレスをカンマ（ソフトによってはセミコロンも可能なこともある）で区切って書きます．例えば次のようになります．

To: dobashi@aichi-u.ac.jp, suzuki@aichi-u.ac.jp, sato@aichi-u.ac.jp, hayashi@aichi-u.ac.jp

あるいは Cc フィールドを使い，次のように書くこともできます．

To: dobashi@aichi-u.ac.jp
Cc: suzuki@aichi-u.ac.jp, sato@aichi-u.ac.jp, hayashi@aichi-u.ac.jp

この場合にはCcフィールドのアドレスには参考までにメールを送信するという意味合いが強くなります．従って全員に同じような重要性を持たせてメールを送信したいときは，To フィールドに書いたほうがよいでしょう．Cc フィールドのアドレスには，To フィールドのコピーが送られます．

Bcc はTo やCc で指定した受信者には分からないように送る機能です．

To: dobashi@aichi-u.ac.jp

Cc: suzuki@aichi-u.ac.jp, sato@aichi-u.ac.jp

Bcc: hayashi@aichi-u.ac.jp

例えば上の例のようにメールの送り先を指定したとします．すると Bcc フィールドのアドレスにはこのメールのコピーが送られますが，そのことはTo とCc フィールドの受信者には知らされません．

Cc やBcc フィールドはグループで仕事をしている場合には，役に立つことがあります．しかしメールの前後関係を知らない人に，CcやBcc でメールを送ると混乱する場合がありますので注意が必要になります．

最近の Netscape Messenger や Outlook Express などのメールソフトでは，最初に起動した状態では Cc や Bcc のフィールドが隠れている場合が多く，そのため使いたい場合はメニューを操作してこれらのフィールドを表示させる必要があります．

8. 8. 電子メールの特徴

電子メールには従来の郵便と違い，いくつかの特徴があります．

(1) メールの配信が非常にはやい．ほとんど数秒から数分程度で送り先に到着する．到着はメッセージの大きさや経路などによって多少違いが出る．

(2) 相手が不在の場合でもメッセージは配信される．

(3) 受信者は別な場所からでも自分のメールを読むことができる．

(4) 送信するときは，時差や距離などほとんど気にしなくてもよい．

(5) 複数の受信者に同時に送信することができる．

(6) メールの文章はデジタルデータなので，再利用することができる．

また最近のメールソフトでは，相手がメールを受信したかどうか，受信の確認を行える機能が付いています．しかし相手が受信したことを返信しない場合などは確認できないこともあります．

さらにインターネットを流れる電子メールの形式は，テキストデータそのものになっているため，メールの中継を行っているうちに，内容がどこかで見られる可能性を否定できません．そのため電子メールの機密性やプライバシーを守るため，いくつかの暗号化方式が採用され，実際に使われています．

》》》 演習 8 《《《

次の演習を行ってみよ.

1．電子メールソフトの設定

最近は手軽に使えるメールソフトがインターネットに公開されている．公開されているメールソフトを使って，メールの送受信を行うために必要な設定を行ってみよう．ここではnPOPという名前のメールソフトをダウンロードして使うことにする．上記のソフトは以下のURLなどに公開されている．

http://www.nakka.com/soft/npop/

このメールソフトは，メールサーバ(POP3)上にあるメールだけを表示する．サーバから削除されると，クライアントのメール一覧からも削除される．サーバにメールを置いておけば，サーバにアクセスできるところからなら，いつでもメールを見ることができる．

プログラムもコンパクトになっており，フロッピーディスク 1 枚に全体が収まる．しかし表示できるのはテキストだけあり，HTMLなどもテキスト形式で表示されので，Webページ上の画像などは見られない．

添付ファイルをサーバに残したまま本文の受信もできる．そのためウイルス付きの添付ファイルが送られてきたときなどは，その添付ファイルをサーバ上で削除できるので，セキュリティを保つことができる．

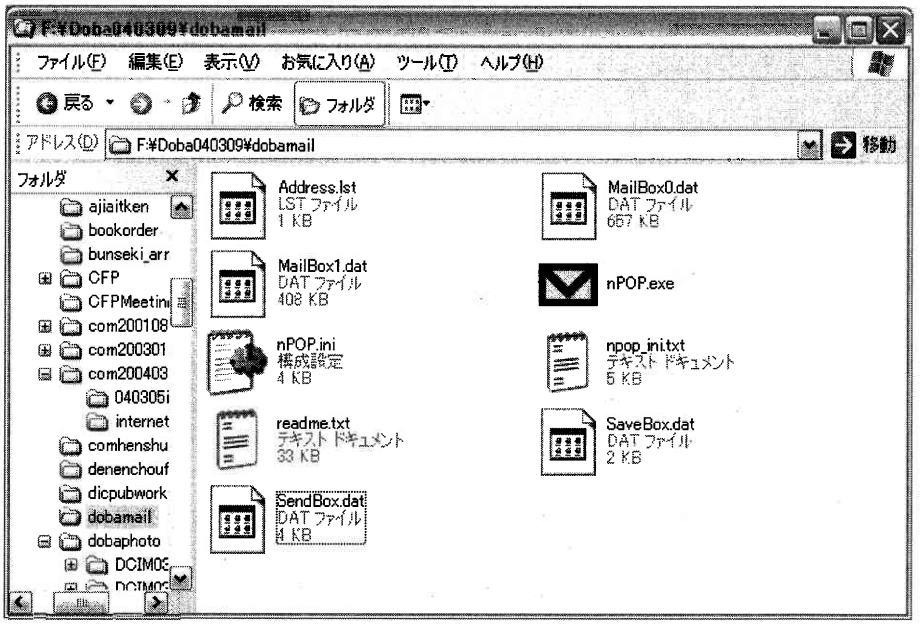

図8.4　nPOPをインストールしたフォルダの画面例

ダウンロードしたnPOPを解凍し，必要な設定を行ってメールの送受信を行うと，受信箱や送信箱などのファイルが生成される（図8.4）．nPOPのプログラム本体と同じディレクトリにインストールすることもで

きるので，持ち歩きたいときに便利である．

以下の図はメールを受信するために必要なアカウントの設定画面である．必要な項目を設定してメールの送受信をしてみよう（図8.5から図8.7）．

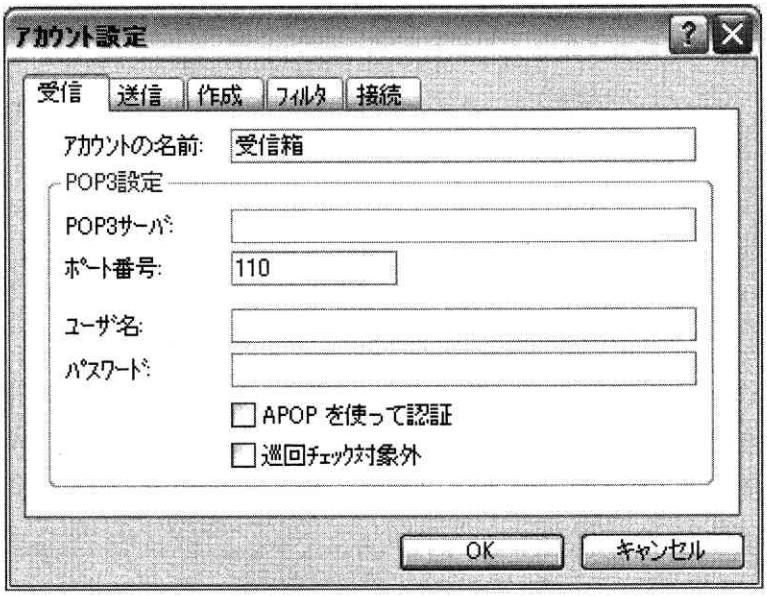

図8.5　アカウント設定画面（受信）

図8.6　アカウント設定画面（送信）

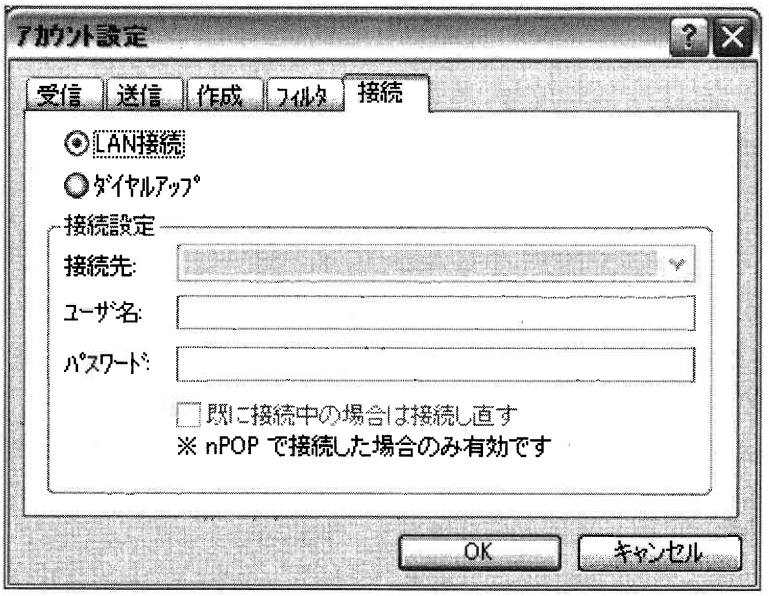

図8.7　アカウント設定画面（接続）

2．ネットミーティング

パソコンとインターネットを利用して，会話や共同作業を行うグループウエアと呼ばれるシステムがある．最近ではインターネット電話や，マルチメディアに対応したビデオ会議，チャットなどいくつかの機能が統合されたソフトが盛んに使われている．

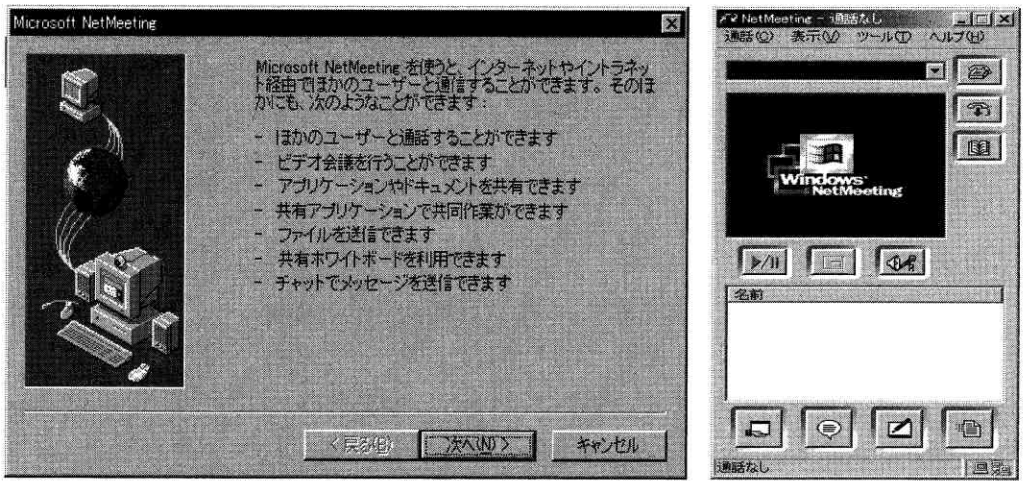

図8.4　ネットミーティングの起動画面

ここではWindowsに付属しているNetMeetingを取り上げ，その活用方法を考えてみたい．以下のURLに詳しい紹介があるので，適宜参考にしてほしい．

http://www.microsoft.com/japan/windows/netmeeting/

2．1．NetMeetingの機能

NetMeetingには次のような機能があるので，NetMeetingの設定を行い，使い方を調べてみよ．

（1）ビデオ会議
（2）インターネット電話
（3）チャット
（4）ファイル転送
（5）リモートディスクトップ機能
（6）インターネットディレクトリ

2．2．NetMeetingを使った演習

次のことを実際に行い，活用方法を考えよ．またシステムの問題点や改善点がないかどうか検討してみよ．

（1）適当な相手を探し，会話してみよ．
（2）複数の人でチャットをしてみよ．
（3）リモートディスクトップ機能で何ができそうか試してみよ．
（4）練習用のファイルを作成し，ファイル転送を試してみよ．
（5）リモートディスクトップ機能はどのように動作するか試してみよ．
（6）インターネットディレクトリはどのように使えるか．

》》》 本章の復習 《《《

（1）MTA(Message Transfer Agent)の役割はどのようなものか．
（2）電子メールのサーバ間で使われるプロトコルは何か．
（3）電子メールとクライアントの間で使われる主なプロトコルは何があるか．
（4）メールのヘッダで発信者の名前やアドレスはどのフィールドにあるか．
（5）Ccはどのような機能か．
（6）Bccはどのような機能か．
（7）返信メールアドレスはどのフィールドに書かれるか．

9. World Wide Web

これまでにおけるインターネットの発展の中で，最も注目を集めたもののひとつとして World Wide Web があります．Web または略して WWW という言い方も広く使われています．最近では単に Web(ウェブ)ということも多くなりました．World Wide Web は，世界中に張りめぐらされた蜘の巣という意味です．

Web はハイパーテキスト(hypertext)によって，インターネット上に分散して存在する情報を互いに関連付けるクライアントサーバ型システムのひとつです．現在ではインターネットだけでなく，組織内のイントラネット(intranet)でも，文書の閲覧などに標準的に用いられるシステムになっています．インターネットに対して，組織内に構築されるネットワークをイントラネットと呼んで区別することがあります．

元々の World Wide Web は，欧州核物理学研究所(CERN: Conseil Europeen pour la Recherche Nucleair)の Tim Berners-Lee や Robert Cailliau が考案したシステムです．当初は研究所内において，論文の整理と検索や閲覧を行うことを目的に研究開発されたものであり，1989 年に開発したシステムを基礎としています[引用文献1]．

その後 1993 年に，米国のイリノイ大学スーパーコンピュータセンター(NCSA: National Center for Supercomputing Applications)において，Marc Andreessen らがインターネットの情報を閲覧するために，Mosaic という名前の最初のブラウザを開発しました．

ブラウザ(browser)というのは，情報をざっと見るためのソフトウエアのことです．Mosaic は文字だけでなく，画像や音声なども手軽に扱えるように設計されていたため，学術雑誌をはじめとしてさまざまなメディアにと取り上げられ，人々の大きな反響を呼びました．さらにインターネット上から無料で提供されたこともあって，瞬く間に世界中に普及しました．これをきっかけにして Web の利用者が爆発的に増加し，情報を発信する Web サーバも急増し，今日の状況に至っています．

その後 Mosaic を開発した研究者らは，大学から離れて新たな企業を起こし，Netscape というブラウザを開発しました．Microsoft の Internet Explorer なども，これらのシステムの成功に刺激されて開発されたものです．Internet Explorer は Windows の普及とともに，多くの利用者を獲得するに至っています．また現在ではベンチャー企業をはじめとした多くの技術者によって，さまざまな機能を持つ Web ブラウザが数多く開発されています．

多くの Web ブラウザは，マルチメディア情報を扱うために，GUI と呼ばれるグラフィカルユーザインタフェース(Graphical User Interface)を備えており，テキストのほかにも静止画，動画，音声などさまざまな情報を扱うことができます．またブラウザの操作がビジュアルで簡単なため，今日ではさまざまな広報や宣伝などの情報発信手段として，一般企業や官公庁だけでなく，個人にも広く普及しています．

Web では，企業や大学に限らず，誰でも簡単に情報の発信者になることができます．つまりホームページなどの提供者になることができます．そのためにはブラウザで見ることのできる自分の Web ページを作る必要があります．

所属の大学や企業において，各人で Web ページを使った情報発信を可能にしているところも多くあります．そのときは作成した Web ページのファイルを，指定された Web サーバの適切な領域にいれて，外部から見られるように設定すれば，世界に向けて情報を送り出すことができます．あるいは自分でプロバイダな

どと契約し，個人が趣味で情報発信することももちろん可能です．今では企業や個人を問わず数え切れないほどのWebページが公開されています．

9．1．ハイパーテキストの意味と機能

コンピュータによって実現されたデジタル情報の世界では，日常的に使っている紙の文書あるいは本や雑誌とは異なる形態が実現されています．例えばWebページでは文書の目次にあたるような部分から，その目次の部分をクリックして内容の部分にジャンプし，即座に移動することができます（図9.1）．

また従来の紙で作られた文書の上では，動画を表示させるようなことはできません．しかしHTMLを使ったWebページのようなデジタルドキュメント(digital document)では，そのようなことも手軽にできるようになっています．

Webページには，クリックすると他のページへ飛び移るリンク(link)が張ってあります．このような機能はHTMLと呼ばれる言語を使って実現されています．HTMLとは，Hyper Text Markup Languageの頭文字を取ったものです．

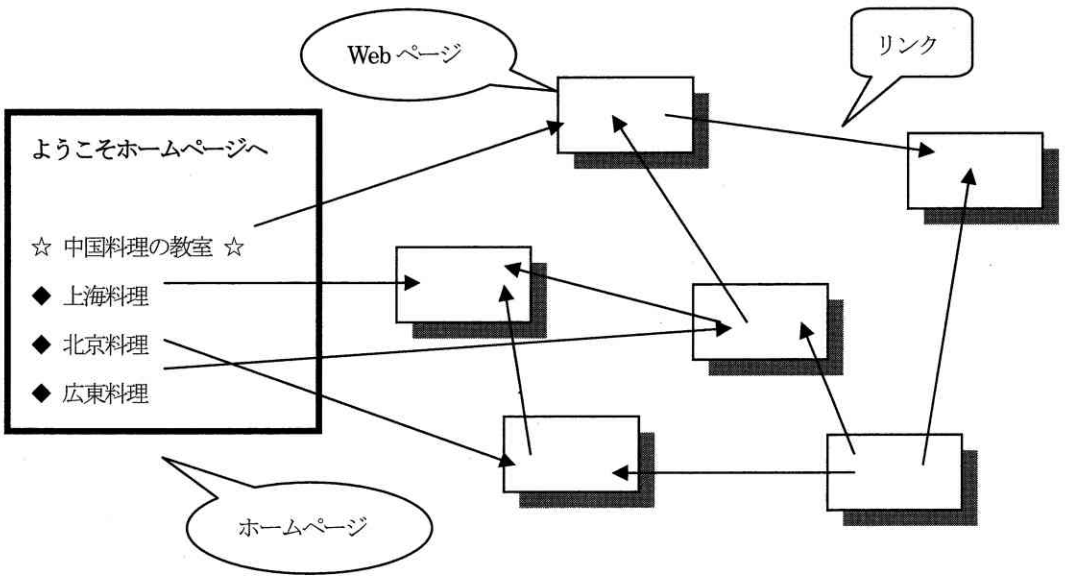

図9.1 ハイパーテキストとWebページの概念図

このようにWebページ上で他の文書に飛び移ったり，画像などを表示したりする機能は，ハイパーテキスト(hyper text)のリンク機能を使っているので，ハイパーリンク(hyper link)または単にリンクと呼ばれています．リンクを設定することを「リンクを張る」というようにいいます．リンクを張ってもそれ自体は目に見えませんが，それを指示した部分の記述はファイルの中に文字で書かれているので，目で読むことができます．リンクにはクリックしたときに表示されるWebページの置いてある場所が示されており，

クリックすることによって，そのページを転送してほしいという要求を届ける処理を行っています．

ハイパーテキストはマルチメディアの基礎になった技術であり，ハイパーテキストには文字のほか写真や絵を表示することができます．ブラウザでインターネットを閲覧していると気づくように，表示している文字や絵や写真などをクリックすると，音声が出たり，動画を動かしたりするようなこともできます．

このような文章や絵を表示している部分は，HTML のリンク機能を用いて書かれています．リンク機能などを含めて作られたテキストデータの集まりすなわちファイルの集まりの全体をさして，ハイパーテキストと呼んでいます．インターネットのホームページの基本的なリンクは，すべて HTML で書かれています．

作成したハイパーテキストの Web ページは，プロバイダなどのインターネットに公開されているサーバの指定された領域に登録すれば，世界中から見えるようになります．

9. 2. Web のしくみ

Web のしくみは，クライアントサーバ型のシステムで構築されていることは既に述べました．まずWeb ページを公開したい人は，Web サーバ(HTTP サーバ)が動いているホストにユーザの登録をしてもらい，公開したい内容を格納したファイルと，それらを入れておくディレクトリを用意します（図9.3）．

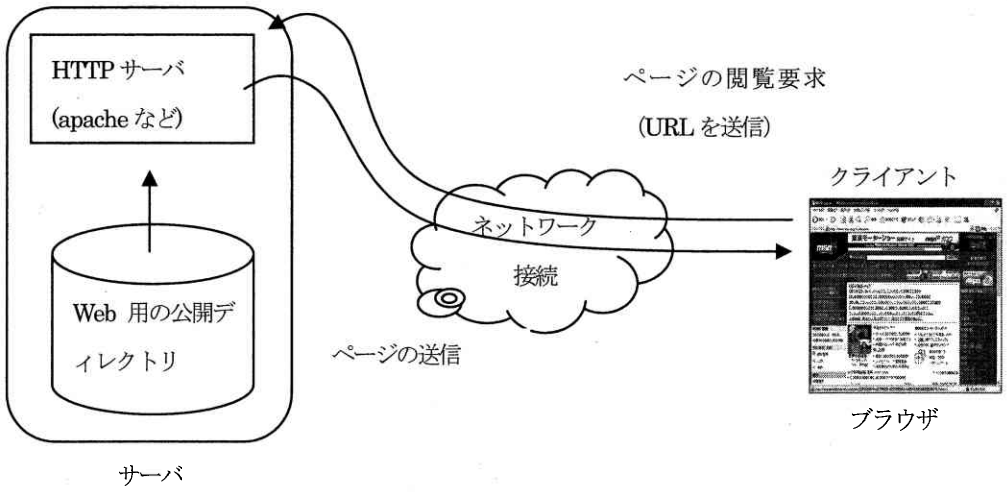

図 9.3 Web のしくみ

他方でブラウザでインターネットの情報を閲覧したい人は，Web ページのある場所を URL(Uniform Resorce Locater)として指定します．つまりブラウザのアドレス入力欄に，http://www.aichi-u.ac.jp/index.html のように入力します．URL はWeb ページの所在を表す方法として使われるものです．

URL を入力して送信すると，ネットワークを経由して公開されているホストの HTTP サーバに，Web ページを要求していることが伝わります．そしてURL に指定したファイル名から，どのページを閲覧したいかということがHTTP サーバ側

で分かります.

HTTP サーバでは要求が届くと，URL に指定されたファイル名からサーバ上にある該当するページ(ファイル)を送り出します．そのファイルがクライアントのコンピュータに届き，ブラウザがファイルを読み込んで，ファイルに書かれている内容や，指示された表示方法に従って画面に表示してくれます.

HTTP サーバではhttpd というデーモンプログラムが複数動作しており，このプログラムがブラウザの要求に応じてファイルを送り出します．このようにWeb を利用するためには，情報を発信する側ではサーバのソフトウエアが必要となり，情報を受け取るクライアント側では，閲覧するためのブラウザのソフトウエアが必要になります.

電子メールではメッセージの発信が，発信者側の意思と判断で起動されます．これに対して Web では，受信者がこのページを見たいというとき，つまり受信者側の要求だけによって情報の送信が開始されることに大きな違いがあります.

電子メールは相手のアドレスが分かれば，基本的には受け取りたくない人にも送信することが可能です．最近は特定のアドレスからの着信拒否も可能になっていますが，これは自分で受け取らないように設定しておくことが必要になります.

Web ページの場合は，基本的に見たい人だけが見るしくみになっています．見たくない人に見せるようにすることは，クリックさせるように何らかの工夫をしておかないとできません．この点において Web を閲覧するブラウザには，使いやすい視覚的なユーザインタフェースを取り入れており，受信者が必要な情報に簡単にアクセスできるようにさまざまな工夫がなされています．インターネットの情報を集めたディレクトリサービス (directory service) や検索サービスを活用すれば，Web ページを公開をしているところなら，世界中のどこからでも情報を取り寄せることができます.

9. 3. URL

Web で情報を公開する場合に，その起点となるのがホームページです．ある Web ページから他の Web ページへと，次々にリンクを張ることによって，世界中の Web ページがリンクでつながります.

World Wide Web の Web にはくもの巣というような意味もありますが，ここでは世界中に張りめぐらされたリンクによるネットワークを意味しています.

インターネットで Web ページの所在を表す方法が URL(Uniform Resorce Locater)と呼ばれるものです．URL はプロトコル名，ホスト名，ファイル名 (またはファイルのある場所)，区切り記号などから構成されています．URL の書き方では，プロトコル名やホスト名などは主に英数字が使われ，コロン(:)やスラッシュ(/)は区切り記号として使われています (図9.2) .

URL の先頭に記された http(HTTP プロトコル：Hyper Text Transfer Protocol) は，情報を送り出す役割をする HTTP サーバとブラウザの間で，データをやり取りするために決められたプロトコルの名前です．「://」はプロトコルとホスト名の区切りを表しており，また「/」はホスト名とディレクトリ名などの区切りに使われます．なおホスト名とドメイン名の区切りやドメイン名の中の区切りは「. 」(ドット)が使われます.

プロトコル名の後にはホスト名とドメイン名が続き，FQDN 形式のホスト名になっています．これによって Web サーバ

の名前とある場所を示しています．さらにその後にはホストの中でファイルのある場所を示すためのディレクトリ名とファイル名が続き，これによって転送するべきファイル名とそのある場所を示しています．

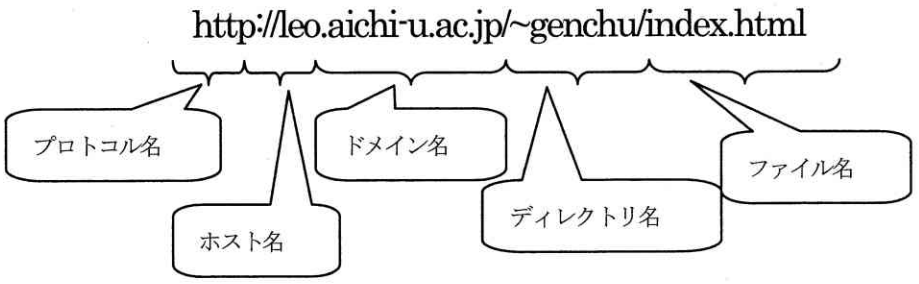

図 9.2 URL の構成

ディレクトリ名やファイル名は，ホスト上において情報のある場所つまりファイルへのパス(pass)を示しており，この部分に何も指定しなくても Web ページが開くことがあります．そのようなときは多くの場合に，トップページにあたる index.html というファイルを転送するように指定しています．

また URL に HTTP プロトコルを指定するときは，ポート番号が添付されることがあります．HTTP プロトコルには 80 番が固有の番号としてあらかじめ割り当てられているため，通常の場合はポート番号を省略することができます．しかし特別な変更を加えて，通常のポート番号以外のものを割り当てている場合には，その番号を URL に指定する必要があります．そのときは FQDN の末尾にコロン付け，その後ろに書きます．

http://www.aichi-u.ac.jp:80/index.html　　(通常のポート番号を使った例)

URL 先頭のプロトコルの部分には，Web ページの転送のときには HTTP プロトコルが使われますが，これ以外にも次のようなものが使われることがあります．

(1) ftp

ftp はファイル転送用に使われるプロトコルであり，これを指定するとブラウザを使ったファイル転送を行うことができます．具体的には ftp://mc_srv.aichi-u.ac.jp/のように指定して，先頭に ftp プロトコルであることを示します．

(2) file

URL の先頭に file と書いて，ホスト内にあるファイルを指定します．ディレクトリ名とともにファイル名を指定し，ブラウザに読み込んで表示させることができます．file://F:¥Doba040602¥webgenchu04¥aichi2003¥index.html のように指定します．Windows の Internet Explorer では，¥マークが区切り記号として使われます．

(3) telnet

telnet は遠隔端末(remote terminal)にアクセスするためのプロトコルであり，これを URL の先頭に指定すると，Windows ではコマンドプロンプトが起動して，telnet を使って URL で指定したホストにアクセスすることができます．

(4) mailto

ブラウザから電子メールを送信するときはmailtoを使うことができます.
例えばmailto:dobashi@vega.aichi-u.ac.jpのようにWebページのなかに記述し，その上をクリックすると，メールを送受信するソフトが起動してきます.

Webページの作成に使われるHTMLは，Webで公開するハイパーテキスト文書を作成するために使われる規格です.HTMLはソフトウエア開発に使われるようなプログラミング言語とは異なり，ブラウザに文書を表示したときに，どのような効果を付加するかを指示するために，Webページのテキストに挿入するマークアップタグの文法を指定するものです.
最近ではXML(extensible markup language)のように，HTMLよりもさらに優れた機能を備えた新たな言語の開発も行われています.

》》》 演習 9 《《《

次の手順に従い，演習を行ってみよ.

1．Webページの作成と公開

簡単な練習用のWebページを作成し，インターネットに公開してみよう.

1．1．HTMLでWebページの作成

HTML を使って簡単な Web ページを作成する．ファイル名はトップページ(ホームページ)なのでindex.html とする．以下に簡単なHTMLファイルの例を示す.
以下のファイルにおいて,左側の<html>のように<>で囲まれた部分はHTMLのタグを示しており,<h1>ここは土橋　喜のホームページです</h1>のように，<h1>と</h1>で囲まれた部分が実際に画面に表示される内容である．また右側のカッコ内は，HTMLタグの意味の説明である.

(ファイル名：index.html)

```
<html>                                                    (HTMLファイルの始まり)
<head>                                                    (ヘッド部の始まり)
<title>                                                   (タイトルの始まり)
Dobashi Home Page                                         (自分の名前を書く)
</title>                                                  (タイトル部の終わり)
</head>                                                   (ヘッド部の終わり)
<body>                                                    (ボディの始まり)
<center>                                                  (中央揃えの始まり)
<h1>ここは土橋　喜のホームページです</h1>                  (自分の名前を書く)
```

```
</center>                                          (中央揃えの終わり)
<hr>                                               (区切り線を引く)
</body>                                            (ボディ部の終わり)
</html>                                            (HTML ファイルの終わり)
```

1．2．ブラウザに表示

作成したページが正しく表示されるかどうか，Internet Explorer に表示して確認する．作成したファイルのアイコンをダブルクリックするなどして，Internet Explorer に読み込ませて表示させる．正しく表示されないときは，正しく表示されるまで間違いを修正する．正しく表示された例は図9.4を参照のこと．

2．公開するディレクトリの作成

ページが正しく表示されたら，サーバから公開する準備を行う．

サーバの IP アドレスは202.250.164.10，ホスト名はmc_srv で，OS はLinux が動いている．

2．1．telnet でログイン

サーバにログインして，Web ページを公開するためのディレクトリを作成する．ディレクトリ名はあらかじめ決められているので，今回はhtml という名前で作成する．手順は以下を参考にする．

```
C:¥My Documents>telnet 202.250.164.10

LASER5 Linux release 7.2 (sigure)
Kernel 2.4.9-13LL1 on an i686
login: dobashi
Password:
Last login: Wed Nov 13 16:07:06 from 192.168.12.6
[dobashi@mc_srv dobashi]$ ls                    (表示できるファイルやディレクトリがない)
[dobashi@mc_srv dobashi]$ mkdir html            (mkdir コマンドでディレクトリを作成)
[dobashi@mc_srv dobashi]$ ls                    (ls コマンドでディレクトリができたことを確認)
html
[dobashi@mc_srv dobashi]$
```

2．2．公開する許可を与える

上で作成した html というディレクトリは，ディフォルトでは誰からでも見えるように許可されている．しかし上の例の dobashi という自分のディレクトリはhtml のディレクトリの上にあり，ディフォルトでは

自分だけしか見えないように設定されている．そのため次のようにコマンドを入力して，誰からも見えるように許可を与える．

以下の chmod go+xr dobashi の部分は，chmod というコマンドを使い，dobashi ユーザのホームディレクトリを誰からでも見えるようにする許可を与える処理を行っている．

```
[dobashi@mc_srv dobashi]$ cd /home
[dobashi@mc_srv home]$ chmod go+xr dobashi                    (許可を与えるコマンドの入力)
[dobashi@mc_srv home]$ ls -adl dobashi
drwxr-xr-x    4 dobashi    dobashi                    (r と x が3つずつ付いていることを確認)
[dobashi@mc_srv home]$
```

2．3．HTML ファイルの送信

次に上で用意したディレクトリに，公開したいテスト用 HTML ファイルを ftp で送信する．ファイルを受信するときは get コマンドを使ったが，送信するときは put コマンドを使う．あらかじめ送信したいファイルが置いてあるディレクトリで ftp を起動するとやりやすい．

```
C:¥My Documents>ftp 202.250.164.10
Connected to 202.250.164.10.
220 mc_srv.aichi-u.ac.jp FTP server (Version wu-2.6.1-20) ready.
User (202.250.164.10:(none)): dobashi
331 Password required for dobashi.
Password:
230 User dobashi logged in.
ftp> ls -a
200 PORT command successful.
150 Opening ASCII mode data connection for directory listing.
.
..
.bash_history
(略)
html                                          (このディレクトリがあることを確認)
226 Transfer complete.
ftp: 173 bytes received in 0.02Seconds 10.81Kbytes/sec.
ftp> cd html                                  (cd コマンドで html に移動)
```

```
250 CWD command successful.                          (コマンドが正しく実行されたというメッセージ)
ftp> bi                                              (バイナリモードの指定)
200 Type set to I.                                   (バイナリモードに設定されたというメッセージ)
ftp> put index.html                                  (公開するHTMLファイルの送信)
200 PORT command successful.
150 Opening BINARY mode data connection for index.html.   (ファイルを送信中)
226 Transfer complete.                               (送信の完了)
ftp: 159 bytes sent in 0.00Seconds 159000.00Kbytes/sec.
ftp> quit                                            (ftpの終了)
```

2．4．テスト用Webページの表示

HTMLファイルの送信が終了したら，Internet Explorerを起動して次のようにURLを入力し，テスト用のページが表示されることを確認する．サーバのホスト名はmc_srvであるが，DNSに登録されていないので，IPアドレスを入力する．またユーザ名の先頭には~(Shift＋ひらがなのへのキー)を付ける．~はtildeと綴り，ティルデまたは波型ダッシュなどと読み，ユーザのホームディレクトリを表す記号として使われる．

```
http://202.250.164.10/~dobashi/                      (ホストのIPアドレスとユーザ名を入力)
```

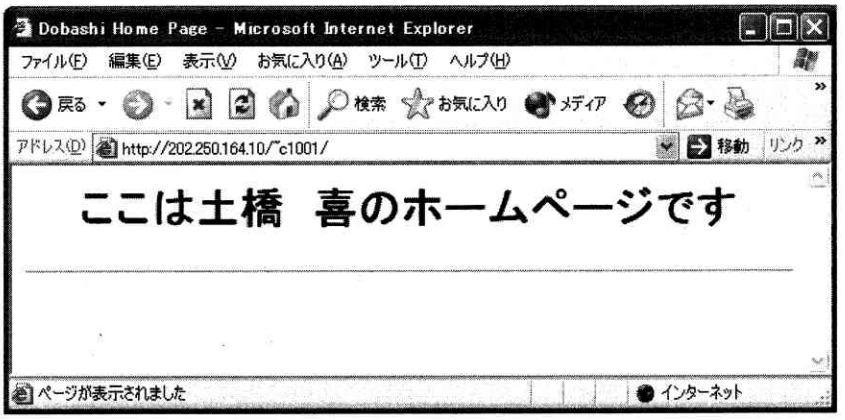

図9.4 表示されたWebページの例

2．5．他の人のページも確認

他の人のページも同じように見られるかどうか試してみよ．

》》》 本章の復習 《《《

（1）WWW はどのような意味か.

（2）ブラウザとはどのような機能を持つか.

（3）ハイパーテキストとはどのようなものか.

（4）HTML は何の略か. それはどのようなものか.

（5）リンクとはどのような機能を実現するもか.

（6）URL とはどのようなものか.

10. システム管理入門

最近は自宅にパソコンを持つ人が多くなり，システム管理(system management)は身近な仕事になりつつあります．自分でパソコンを持っている人なら，あまり意識をしないで既にシステム管理の仕事を実行しているかも知れません．例えばソフトをインストール(install)したり，ディレクトリ(directory)を作成してファイルの整理をしたりすることも，システム管理の初歩的な仕事になります．

システム管理の内容は意外に幅広く，例えばパソコンを一人で使う場合，家族と一緒に使う場合，複数のパソコンを使う場合，あるいは教室のように数十台を同時に移動させる場合などのようにさまざまな事例が考えられます．そしてそれぞれの状況に適したセキュリティ(security)対策を施して対応する必要があります．

システム管理では，インストールしてシステムを動かすだけではなく，その後の運用を確実にするため，セキュリティを保つことが極めて重要になっており，ここではインターネットへの接続を前提にして，システムを管理する上での心構えや管理の概要を紹介していきます．

10. 1. なぜ管理者が必要か

個人でパソコンを持っている人は，誰かに管理を依頼しない限りは，常に自分で管理をして仕事ができる状態を保つことになります．この場合は所有者が管理者を兼ねているわけです．

しかし教室のパソコンの場合は情報センターが管理の責任を持ち，常に授業で使える状態を保っています．電源を入れてもパソコンが動作しないときは，どこが原因かを調べて，ハードウエアの修理をすべきか，あるいはソフトウエアの修復を行うべきかを決め，適切な対策を施します．

このような仕事がシステム管理者の仕事の一部となっており，システム管理者の仕事の中心は，常に使える状態にシステムを維持管理するところにあるといえます．管理者のいないシステムは，いったんシステムが停止すると，再稼動できなくなってしまいます．

コンピュータシステムが不都合なく運用されるためには，それを管理する人が必要です．そのような仕事を担当する人をシステム管理者と呼んでいます．

システム管理者の仕事は，システムの構築や運用方針の決定のようなことから始まり，ニュースやメールの管理といった日常的な仕事もあります．さらにソフトウエアが動かないとか，あのソフトを使いたいというような要望の処理まで，非常に多くの仕事をこなしているのです．

ここではこのようなシステム管理者の仕事のうち，主に技術的な面を取り上げて説明します．システム管理者としてではなく，単にパソコンを使いたいというだけの人は，あまり関係ないと思うかも知れません．しかしシステム管理者がどのような仕事をしているかを知っていれば，システム管理者にどんな仕事をどのように頼めばよいかがわかってきます．

加えて最近は自分でパソコンを持つ人が多くなり，自分のパソコンをある程度は自分で管理できるようになる必要があります．そうすれば何かトラブルが起きたときに，いちいち購入先の管理者に頼まなくても自分自身で解決すること

ができるようになります.

システム管理というと難しいと思うかもしれませんが, しっかり勉強して自分が使うところは自分で管理できるようにしておく必要があります.

10. 2. システム管理の階層構造

システムといっても 1 台だけの小さなものから, 数百台を越す大規模で複雑に関連しあったものまで, 極めて多様な形態となって構築されています. 大規模なシステムの管理は, 「ネットワークレベルの管理」, 「コンピュータレベルの管理」, 「個人レベルの管理」というように階層構造化して考えます (図10. 1) [引用文献18].

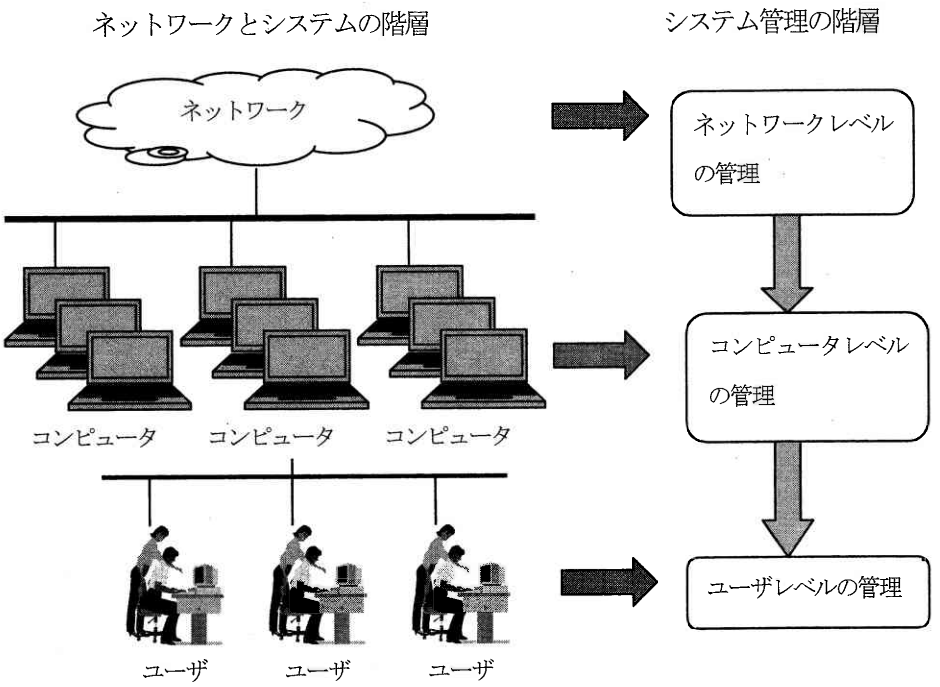

図10.1 システム管理の階層構造

ネットワークレベルの管理は, LAN 間の接続に関する管理, また同一の LAN 内で接続されたコンピュータ同士を正常に運営できるようにするための管理を指しています.

次にコンピュータレベルの管理とは, それぞれのコンピュータを運営するための管理を指しています. 個人レベルの管理は, パソコンを使用する個々のユーザに関連した管理のことを指しています. 実際にはコンピュータの管理者もネットワーク管理の一部を受け持ちながら, 個人管理の面倒を見るというように, 管理の運用方法は実際の状況に合わせて多様化しています.

管理の階層の考え方は重要ではありますが, 現実の現場の仕事では, その境界を明確にできないことが多くあります.

いずれにしてもシステム管理者の仕事は，コンピュータ環境を整備し，使いやすい環境をユーザに提供することにあります．

10. 3. システム管理の概要

10. 3. 1. ネットワークレベルの管理

ネットワークレベルの管理では，ネットワークの設計や構築，日々の運用管理，ネットワーク全体のセキュリティ対策などの管理を行う必要があります．

（1）ネットワークの論理的な設計

ネットワークにどのような機能を持たせるか，その機能をどのように役割分担するか，各部門間の接続の形態や方法はどのようにすることが望ましいかなどを決めておきます．

（2）ネットワークの物理的な構成の計画と実施

（3）ネットワークの運営，管理方針の決定，およびユーザへのその周知

ネットワークの運営，管理方針はそのネットワークを構成する部門と協議して決める必要があります．

（4）ネットワーク内での規則の決定およびその周知

ホスト名，ユーザ名，IP アドレスなどネットワーク内での重複があると不都合の原因となるものは，ネットワークの管理者が一括して管理しておきます．なおそれが難しい場合は，その範囲や基準を統一し，関連のある管理者に周知しておく必要があります．

（5）ネットワークのセキュリティの設定と監視

（6）ネットワークトラブルの復旧

（7）ネットワークの変更や拡張の計画と実施

10. 3. 2. コンピュータレベルの管理

コンピュータレベルの管理では以下のような点が重要となります［引用文献18］．

（1）コンピュータと周辺装置の導入と引き上げ

ハードウエアやソフトウエアの新規導入と増設などの場合に，支障なくユーザが使えるようにする必要があります．またコンピュータを引き上げる場合には，残ったコンピュータに影響がでないようにする必要があります．

（2）日常のオペレーション

コンピュータの起動と停止，また使用状況などの管理と改善を行います．個人レベルの管理で行われることもあります．

(3) 定期保守

ファイルのバックアップなどで障害が起きた場合に備えます．また定期的にコンピュータの状態をチェックし，環境の維持に努める必要があります．

(4) 障害対策

障害が発生した時は，応急処置を施し，原因を明らかにする必要があります．障害の程度によっては，適宜上位の管理者や納入業者（ベンダー）と連絡を取ります．さらに障害の再発防止と再度障害がおきた場合の参考にするため，障害の発生状況と内容を記録するようにします．

(5) ユーザの管理と指導

新たなユーザの登録，期限切れユーザの削除などを行います．ユーザからの質問に答えたり，ユーザ自身で個人管理をするよう指導する必要があります．

(6) ネットワークの利用に関わることの周知

ネットワークに関わる連絡事項（停止など）が発生するときは，ユーザに知らせる必要があります．

(7) セキュリティの確保

ユーザの故意または不注意によるシステムの破壊や資源の浪費を防止する必要があります．また外部からの侵入を防止しなければなりません．

10. 3. 3. 個人レベルの管理

個人レベルの管理では以下の項目が重要となり，ユーザ個人が責任を持って実施する必要があります［引用文献18］．

(1) パスワードの管理

自分のパスワードが他人に知られないように管理しなければなりません．

(2) ホームディレクトリの管理

ディスク資源を浪費しないように，時々不要なファイルを削除して整理します．

(3) 個人ファイルのバックアップ

障害の発生に備えて，個人ファイルのバックアップを取っておく必要があります．これはシステム管理者だけなく，一般ユーザも自分で取っておく必要があります．

(4) 自分のシステムを使いやすくする管理

自分で使いやすくするためにいろいろな設定を行ないます．

10. 4. 管理者としての心得

システム管理者としての心構えと注意点を簡単に紹介します［引用文献18］．

(1) 使いやすさと安全性のバランス

システムの管理者は場合によっては，ユーザにとって使いやすくするということと，コンピュータのセキュリティを保つということの相反する２つの仕事を同時に行わなければなりません．

すべての特権を全部のユーザに開放すれば，ユーザは自分の思い通りにコンピュータを使うことができます．しかしセキュリティを確保するためにはこれほど危険なことはありません．システム管理者はこの使いやすさとセキュリティのバランスを保つことが極めて重要です．

システム管理者は，システム全体のセキュリティが保てないと判断した場合，ユーザの要求を拒否しなければならないときがあります．そのとき管理者は，なぜそのサービスが実施できないかを，ユーザに説明する必要があります．

（2）管理作業は慎重に

全体の管理者でなくても，自分のシステムをメンテナンスするときは，最新の注意が必要になります．ちょっとした不注意でコンピュータをダウンさせたり，システムの破壊をしてしまったり，自分のデータを消してしまうこともあります．

この種の不注意で最も多いのは，Windows の delete やLinux などの rm コマンドによるファイルの消去です．例えば，不要になったディレクトリからその中にあるファイルを全部消去しようとして，作業中のカレントディレクトリを確かめないで行ってしまう場合があります．このようなとき Linux などでは，「rm *」というような削除コマンドの使い方をしていることが多いのです．このコマンドを入力するとすべてのファイルを削除してしまいます．

Windows では削除したディレクトリやファイルがごみ箱に残っていることがありますが，ごみ箱から削除してしまえば元に戻すことはできません．Linux などでも一旦削除されたファイルやディレクトリは元には戻せません．このような場合には，削除のコマンドを実行する前に十分確認するようにする以外にありません．こういった注意は，管理者と一般のユーザを問わず，自分で行う必要があります．

10. 5. セキュリティ

Windows やUNIX はセキュリティが甘いと言われることがあります．しかしセキュリティ管理のソフトがいくつも開発され，これらをきちんと利用すれば，通常の使用に必要なセキュリティは十分に確保できます．セキュリティの管理が不十分の場合（セキュリティホールがあるなどということもある）には，次のようなことが起こる可能性があります．

（1）一般ユーザの不注意でシステムが停止したり，時には破壊されたりすることがある．
（2）一般ユーザの不注意により，外部から人間が入り込む隙間が生じることがある．
（3）部外者の侵入により，開発中のプログラムやデータなどが外部に漏洩することがある．
（4）部外者の侵入により，システムが破壊されることがある．

したがって，このようなことを防ぎ，自分たちの資源を守るためにも，セキュリティには常に細心の注意を払わなければなりません．

例えばシステム管理においては，各自のパスワード管理が極めて重要になります．パスワードはログイン名を入力したユーザが本人かどうかを確認するためのものです．パスワードはユーザ自身の情報を保護するだけでなく，コンピュータに登録されたすべてのユーザの情報を保護する上でも，その管理は厳重に行う必要があります．

この点は個人でパソコンを使う場合と大きな違いとなります．悪意のある者（クラッカー）にパスワードが解読されると，コンピュータを通じてネットワークにつながったさまざまなシステムが被害にあう危険性が生じます．

従ってパスワードを人に教えてはいけません．また見えやすいことにメモしておくようなことも絶対にしてはいけません．パスワードを教えられた人がそれを使って行ったことに対しては，パスワードを教えた人の責任も問われることになります．

またパスワードが事前に設定していない場合もあります．この場合は最初にログインしたときに，すみやかにパスワードを設定しなければなりません．パスワードを設定していないと，ログイン名だけ入力すれば誰でもログインできてしまい，極めて危険な状態になります．

ユーザとして登録された利用者は，パスワードを他人に教えたり，覚えられたりしないよう管理する義務があります．そのためにはしばしば利用者自身でパスワードを変更することが必要です．

》》》 演習 10 《《《

次のようにネットワークにおけるセキュリティ対策の演習を行ってみよ．

1．ホームページの公開とセキュリティ

インターネットにホームページを公開するときは，Web ページを入れておくフォルダ（ディレクトリ）だけを公開する．それ以外のディレクトリは公開しないように設定する．ここでは html というディレクトリに Web ページのデータが格納されていることにして進める．

Windows も Linux も自分以外のユーザやグループに対して，ディレクトリの読み取りや書き込みなどの許可や制限をすることができるので，これらの機能を使って Web 用のディレクトリに対して公開・非公開の設定を行う．Linux では次のように行う．

（1）読み取りと実行を許可する

読み取りと実行を可能にすると，Web ページはインターネットに公開される．

以下の chmod go+xr c1001 の部分は，chmod というコマンドを使い，c1001 ユーザのホームディレクトリを誰からも見えるようにする処理を行っている．

```
[c1001@mc_srv c1001]$ cd /home
[c1001@mc_srv home]$ chmod go+xr c1001                    (許可を与えるコマンドの入力)
[c1001@mc_srv home]$ ls -adl c1001
```

```
drwxr-xr-x    4 c1001    c1001          (略)(r と x が 3 つずつ付いていることを確認)
[c1001@mc_srv home]$
```

（2）読み取り不許可にする

読み取り不許可にすると，Web ページは公開されない．

以下の chmod go-xr c1001 の部分（go と xr の間は半角のハイフン）は，c1001 ユーザのホームディレクトリを自分以外のユーザから見えないようにする処理を行っている．

```
[c1001@mc_srv c1001]$ cd /home
[c1001@mc_srv home]$ chmod go-xr c1001                    (許可を与えるコマンドの入力)
[c1001@mc_srv home]$ ls -adl c1001
drwx------    4 c1001    c1001          (略)    (先頭が drwx であることを確認)
[c1001@mc_srv home]$
```

》》》 本章の復習 《《《

（1）システム管理はなぜ必要か．

（2）システム管理の階層構造とはどのようなものか．

（3）個人レベルの管理で重要なものを上げよ．

（4）パスワードは他人に教えてよいか．他人のパスワードを見てもよいか．

（5）管理者権限を教室など多数の利用者と共有するパソコンで試してよいか．

11. 情報化社会の問題とセキュリティ

情報技術の発展によってさまざまな情報通信基盤が整備された現代社会では，誰もがどこからでも必要な情報を手軽に手に入れることが可能になります．そして労働や資源の効率化が達成され，さまざまな消費者の要求に対応可能になり，我々の社会的な欲求が満たされるといわれています．

他方，情報化社会には，システムの脆弱性，法制度の未整備，情報格差などさまざまな問題も存在することが明らかになっており，理想的な情報化社会を実現するには，解決すべき問題に対して慎重に対処していくことが重要になっています[引用文献3]．

（1）情報化社会の脆弱性

情報システムが障害を起こすと，被害の規模や影響および範囲が極めて大きくなる可能性があります．障害を起こす原因は，システムの設計ミス，プログラムの間違い(バグ)，災害や事故，犯罪などさまざまです．

コンピュータやネットワークに対して悪事を働くウイルス(virus)を，ネットワーク上にばらまく犯罪が頻繁に起きています．また他人のコンピュータに無断で侵入して情報を盗み出したり，ホームページの内容を書き換えたりする犯罪も起きています(このように悪意のある犯罪者はクラッカー(**cracker**)と呼ばれ，善意でプログラムを改良するハッカー(hacker)とは区別します)．

（2）法制度の未整備や倫理観の確立が未熟

情報の流通や利用面において，法制度や倫理観の確立が遅れており，社会的な問題を起こしています．情報公開におけるプライバシーの保護，機密漏洩，知的所有権などについて社会基盤と倫理観の確立が必要です．

例えばディジタル情報はその複製や改変が極めて簡単に行えるため，写真や画像などの複製や，音楽データの交換などが容易に行えます．これらはオリジナルと複製の区別が困難なため，創作者の著作権保護について，重要な問題が起きています．

（3）情報格差

情報機器を活用する上での個人差が拡大し，新たな社会問題が生じる可能性があります．若者や高学歴者，高所得者などが，情報技術を活用することによって，ますます高収入や雇用を手にする機会が増えています．しかし他方でコンピュータを使いこなせない高齢者や，貧困のために情報機器を入手できない人々は、情報技術の恩恵を受けることができません．

このように情報技術が社会的な格差を拡大する現象が，情報格差すなわちデジタルデバイド(digital divide)といわれます．このような格差は個人の間だけではなく，国家間や地域間にも存在しています．アフリカなどの途上国では，資金難や人材不足あるいは情報通信基盤の未整備などから，情報技術を活用で

きずに放置された状態となり，経済格差が拡大する傾向にあり大きな問題になっています[引用文献19].

今後の情報化社会では，ネットワークやさまざまなメディアをとおして大量の情報が流通し，我々は常にそれらの情報からいろいろな影響を受けます.

これらの情報とのかかわりにおいて，真実が何であるかを見極めて，自ら適切な判断を下し，行動を決定することが極めて重要になっています.

情報の間違った解釈や，不正確な情報に基づいた判断や行動を行うと，社会秩序の混乱や崩壊を招く危険性も発生することがあります.

11. 1. セキュリティとリスク管理

現状ではコンピュータを利用する場合には，いくつかの危険性が伴い，この危険性のことをリスク(risk)といいます. 例えばソフトやデータが壊れるなどのほか，個人情報の漏洩，プライバシーの侵害，ウイルスや不正アクセス(illegal access)などによるコンピュータ犯罪，あるいは天災や人災による事故などもあります.

現代の経済社会では，コンピュータとネットワークが重要な社会基盤となっており，これらに伴うリスクを放置しておくと，維持管理費が増大したり，社会的な信用を失ったり，基本的人権を侵害したりすることが発生しかねません.

そのため情報システムの設計，構築，開発，運用のそれぞれの段階で，安全性を配慮してリスクを排除する対策をとる必要があります.

このように情報システムのさまざまなリスクを排除して，正常な運用を確保することをコンピュータセキュリティ(conputer security)といいます.

11. 2. リスクの種類

コンピュータを利用し運用管理を行うためには，障害や故障，人為的な過ち，天災，事故，コンピュータ犯罪，プライバシーの侵害，機密の漏洩などの観点から，リスクと対策を考えておく必要があります.

（1）障害・故障

システムが大規模化し，複雑に関連しあっている場合もあるため，障害や故障の原因発見を難しくしています. 障害や故障が発生した場合に，早期にこれらの原因を見出し，適切な対策を施す準備をしておく必要があります.

（2）ヒューマンエラー

ヒューマンエラー(human error)は人為的なミスのことであり，システムの設計やプログラミングあるい

はデータの入力など，さまざまな段階で発生します．これらにはすぐさま発見できる単純なミスもあれば，中にはなかなか発見されずに，何年か後に何かの機会に偶然発見されるようなものまで，実に多様化しています．

これらの多くは犯罪と異なり，悪意のない過失とみなされるものがほとんどです．しかし発生件数や損失金額ともに最大といわれており，ヒューマンエラーを起こさないような管理体制が必要であり，たとえ起きたとしても，速やかに復旧させる対策を取っておく必要があります．

（3）天災・事故

地震などの自然災害による被害や火災などによる被害があります．これらの天災や事故による危険性に耐えうる施設やシステム設計が必要です．

（4）コンピュータ犯罪

システムやデータの破壊を目的とするものや，何らかの利益を狙うものなどがあります．情報化社会の進展に伴い，発生件数が増加傾向にあり，対策を整備しておく必要があります．

（5）プライバシーの侵害

他人を誹謗中傷する情報を Web ページに掲示するなどがプライバシーの侵害となります．嫌がらせを目的に故意に行われる場合だけでなく，過失によって発生する場合もありえるため，法制面や情報倫理の立場からの対応が必要になっています．

（6）機密の漏洩

会社の顧客名簿や営業データを盗むなどが機密の漏洩にあたります．

11．3．リスクの分析と管理

コンピュータシステムを危険から守るためには，システムの企画・設計段階から十分に検討しておくことが必要です．このような分析や検討作業をリスクアナリシス（risk analysis）と呼んでおり，次のような検討事項をあげることができます［引用文献3］．

（1）コンピュータシステムの構築運用費用
（2）データベースに蓄積されている情報の価値
（3）考えられるリスクのタイプ
（4）障害発生の頻度
（5）障害が及ぶ範囲と影響度

（6）損害額の算定と予測
（7）障害復旧の方法と費用
（8）セキュリティ対策
（9）バックアップの体制
（10）保険への加入

以上のようなリスクアナリシスにもとづいて，可能な限り低いコストでリスクから発生する損害を最小限に抑えるため，危機管理の対策をとることをリスクマネジメント(risk management)といいます．コンピュータシステムのリスクマネジメントでは，システムの設置環境も含めた総合的な分析が必要になります．

システムはハードウエアだけで成り立っているものではありません．システムの運用を管理する管理者がおり，さらに実際にシステムを使うユーザというように，多くの人々の中で存在しています．

そのため公共性や社会性の高いシステムでは，セキュリティ対策も技術面だけで解決できるものではなく，経営や労務の管理のほか，社会的責任なども考慮した対応が必要になっています．

11. 4. コンピュータセキュリティ

コンピュータセキュリティを策定する場合は，以下のような観点から総合的な検討を加えることが必要です．

（1）コンピュータ関連施設の保護
（2）ハードウエアの保護
（3）ソフトウエアの信頼性
（4）ネットワークの保護
（5）データとシステムへのアクセス制限
（6）データの品質保護
（7）人間的要因

11. 5. コンピュータ関連設備の保護

コンピュータ関連施設の保護では，外部からの侵入，火災，水害，落雷などから保護することが目的になり，次のような対策を取る必要があります［引用文献3］．

（1）コンピュータシステムを設置する建物を耐火・耐震構造とする．
（2）データなどを耐火・耐水の保管庫で管理し，遠隔地にバックアップを用意する．

（3）消火設備を設置し，排水ポンプなども設置を検討する．

（4）停電時にも稼動できるように，無停電電源装置を用意し，電源を二重化しておく．

（5）人の出入りを監視するため，監視モニターを設置する．

（6）緊急時に速やかに復旧できる体制を整備しておく．

重要なコンピュータが設置された部屋に，関係者以外が立ち入らないようにすることが必要であり，場合によってはガードマンの配置や，指紋や声紋などによる本人認証などのほかIDカードによる確認なども必要になることがあります．また地震の被害に備えて，重要なシステムやデータは，地震の被害が及ばない遠隔地にバックアップを備えることも重要となります．

11. 6. ハードウエアの保護

銀行のオンラインシステムなど社会的に重要なものでは，システムがダウンすると大きな影響を及ぼすことが少なくありません．システムダウンを避けるためには，システムを二重化して対策を取ることもあります．システムの二重化対策としては，デュアルシステム(dual system)やデュプレックスシステム(duplex system)と呼ばれる方法があります．

（1）デュアルシステム

通常から2つのシステムに同じ処理を行わせておき，メインシステムがダウンした場合でも，そのままもう一方のシステムで処理を継続することができるように，システムを二重化して準備します．

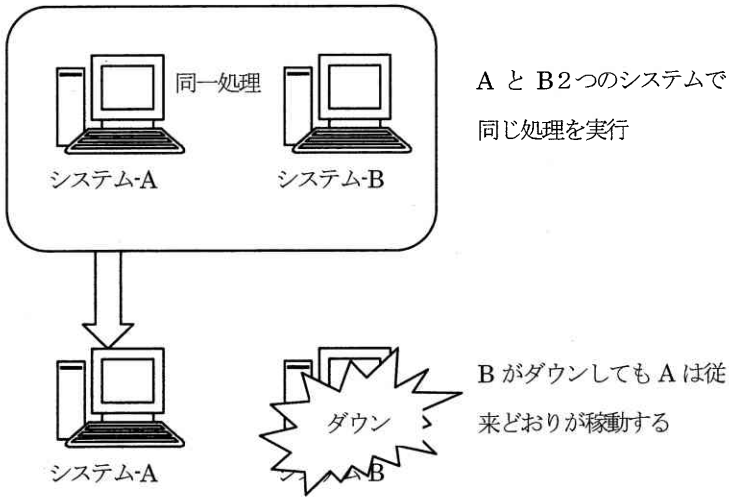

図11.1　デュアルシステムのしくみ

（2）デュプレックスシステム

メインシステムと予備システムを用意しておき，平常時はそれぞれ異なる役割を分担させます．メインシステムがダウンする異常事態が発生した場合に，もう一方の予備システムがメインシステムの機能を続行できるように，システムを二重化しておきます．

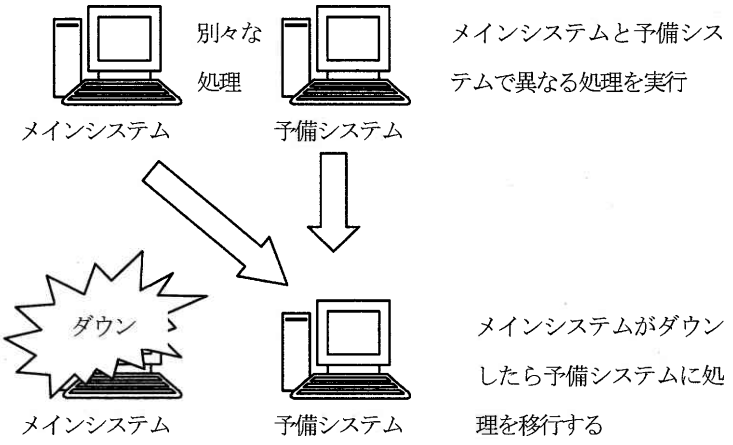

図 11.2　デュプレックスシステム

11．7．ネットワークの信頼性

現代社会ではネットワークが停止すると，インターネットが使えなくなるだけでなく，さまざまな情報交換に支障をきたし，電子商取引などにも影響を与えるため，停止時間を最小限に抑えることが必要です．ネットワークの信頼性とセキュリティを保つためには，次のような対策が必要になります．

（1）ネットワークの二重化

ネットワークの中断を防止するため，ネットワーク回線などの二重化を行います．ネットワークの中心となる幹線部分を二重化し，ネットワークが全面的にダウンすることを回避するように設計します．

二重化していない場合は，ケーブルやネットワーク機器に障害が発生すると，ネットワークは全面的に停止するなどの影響を受けます．しかし二重化しておくことによって，ネットワークが全面的にダウンすることを防ぐことができます．

（2）不正アクセス防止

不正アクセスの防止を行うため，パスワード管理を厳密に行い，適切なセキュリティ対策を施す必要があります．

(a) ゲートウエイとファイアウォールを設置し，内部のネットワークにアクセスするときは，ゲートウエイで中継し，ゲートウエイにファイアウォールを設定します．

(b) ファイアウォールの機能を利用して，許可しない IP パケットを内部のネットワークに通さないように

します.

(c)外部のネットワークからアクセスできるホストを制限します.

(d)パスワード管理を徹底し，場合によっては有効期限を限定した使い捨てのワンタイムパスワード(one time password, One Time Password Authentication)を使用するようにします.

(e)DNS にはコンピュータや OS の種類など，内部のホストの情報を記載しないように設定します．また外部へ不必要な情報が転送されないように転送制限を設定し，ホスト名一覧が外部から参照できないようにします.

(f)アクセスログを監視し，外部から不正アクセスがおこなわれていないかどうかを定期的に監視します.

(g)セキュリティホールを修正するために，OS などのソフトウエアを最新のものに更新します.

(h)セキュリティホールやウイルス，システム攻撃などの情報をチェックするため，公開情報を定期的に確認するための情報収集を行います.

（3）ネットワークの盗聴防止

ネットワークで送受信されるパケットは，暗号化されていないときは，そのまま送信されています．メールの受信時に入力するパスワードや，FTP サーバにログインするときのパスワードもそのまま送信され，メールも暗号化されていなければ読み取ることができる状態になっています.

そのためネットワーク上での盗聴を防ぐため，通信を暗号化するなどの対策をとり，パスワードや電子メールおよび IP 電話などが盗聴されないようにします.

あるいはネットワーク盗聴を発見するソフトエアを導入し，ネットワーク装置の監視を行い，ブロードキャストによって破棄されるパケットが盗聴されないようにします.

パスワードの盗聴に対しては，先に取り上げたワンタイムパスワードを使うなどの対策を取るようにします.

11. 8. アクセスコントロール

ユーザに対してシステムの利用やデータへのアクセスを管理することが，アクセスコントロール(access control)の役割になります.

許可されたユーザ以外はシステムやデータにアクセスできないように運用し，アクセスが許可されているかどうかを必ずチェックします．そのためには次のような対策を取ります.

（1）ユーザの識別

ユーザには ID を発行し，システムにアクセスしたときに登録されているユーザであることを必ず確認するように設定します.

（2）ユーザの認証

ID だけでは他人がなりすますことも可能なため，登録されたユーザであることをユーザ本人に固有の情報（パスワード，指紋，声紋など）を使って確認します．

（3）システム使用の許可

ユーザに与えられた権限のレベルと，システムやデータのセキュリティレベルとの照合により，そのユーザに認められたシステムの利用とデータへのアクセスを許可するようにします．

（4）利用状況の監視

不正アクセスが行われていないかどうか，ユーザごとの利用状況やシステムの稼動状況，および管理者などの操作をモニタリングして記録しておく必要があります．

11. 9. ソフトウエアの品質管理

ソフトウエアのプログラミングに間違い（バグ）があると，障害発生の原因になります．そのため信頼性の高いソフトウエアを開発するためには，プログラミングの間違いを防止することも極めて重要です．

（1）プロトタイプ作成ツール

プロトタイプ（試作品）作成するツールを活用して，システム設計の段階から完成システムの動作までを，あらかじめチェックしておきます．

（2）構造化プログラミング

プログラムの制御構造を逐次処理，分岐条件，繰り返し処理などの限定された方法だけを用いて作成し，誰にでもわかりやすく標準化された形式でプログラミングを行う工夫をします．

（3）モジュラプログラミング

プログラムを小さなモジュールの組み合わせとして開発する方法です．これによってモジュールの再利用を促進し，バグや修正の影響を極力少なくすることができます．

11. 10. 不正アクセスとセキュリティ対策

企業だけでなく個人においても，ネットワークとシステムを不正アクセスから守るため，それらの行為について知っておく必要があります．

不正アクセスの手順はおおよそ次のように行われるといわれています［引用文献8］．

（1）アクセスするための情報収集

はじめに不正アクセスを仕掛ける攻撃対象について，情報収集を行います．会社名，管理者の氏名，IPアドレスの範囲，DNSサーバの所在，DNSゾーンの情報（サーバが管理しているドメイン情報）などが収集の対象となります．

また場合によっては，社員名簿，電話番号簿なども収集の対象となることがあります．これらはユーザ名やパスワードなどに使われる情報が含まれていやすいためです．

これらの情報を集める方法は，Webの公開内容のチェックから，ごみ箱あさりまで広い範囲に行われます．なおこのようにして収集された情報のすべてが利用されるわけではありません．

情報収集は一度で終わるわけではなく，実際に行われる不正アクセスの行為中にもたびたび繰り返されます．これらのほかにもfingerコマンドによる情報の表示からユーザ情報を得る場合もあります．

（2）ポートスキャン

ポートスキャン(port scan)は，サーバの中でどのポートが開いているかを走査する行為のことです．ポートは動いているプロセスのデータの出入り口にあたります．片っ端からドアをノックしてまわり，家に人がいるかどうかを確認するようなやり方に似ています．

コンピュータシステムでは，開いていないポートには一部のDoS攻撃(Denial of Services)を除いて，アクセスすることはできません．

Dos攻撃とはサービス拒否攻撃といわれ，ネットワークを通じた攻撃の一つでしばしば発生します．相手のコンピュータやルータなどに，不正なデータを一度に多量に送信して処理不能に陥らせたり，トラフィックを増大させて相手のネットワークを麻痺させる攻撃のことです．

ポートスキャンは不正アクセスの準備行為となるため，第三者に対して行うことは慎まねばなりません．

セキュリティ管理者やネットワーク管理者は，日常的に自分か管理するシステムに対して，ポートスキャンを行い，不要なポートが開いていないかどうか調査する必要があります．そして不要なポートが開いている場合には，原因を調べてポートを閉じるようにします．

不正アクセスを試みようとするものは，ポートスキャンによって，どのようなポートが開いているか，どのようなアクセス方法が可能か，どのようなOSかなどの情報を知り，不正アクセスできそうな隙間を探します．

（3）システムの弱点を探す

攻撃対象の情報が把握されると，Webなどに公開されている情報を使って，アクセスするための弱点を探します．Webには攻撃ツールそのものが公開されていることもあります．

（4）不正アクセスの開始

一般ユーザのユーザ名とパスワードが漏れると，管理者権限が奪われることがあります．FTP の弱点を攻撃し，リモート・バッファ・オーバーフロー(remote buffer overflow)と呼ばれる方法によって，管理者権限でコマンドが実行されるようになります．

リモート・バッファ・オーバーフローは，遠隔操作によってメモリ上のスタック(stack)をオーバーフローさせ，外部から自由にコマンドが実行できるようにするものです．スタックは最後に入力したデータが先に出力される特徴を持つデータ構造の一種で，多くの CPU ではスタックを処理する命令を用意しており，プログラムによって簡単に利用することができるため，この欠点を悪用した不正アクセスがしばしば起こります．

管理者権限が不正に取得されると，システムの破壊やデータの改ざん，他システムへの侵入などが行われます．

以上の攻撃のほかにも，パスワードファイルの解析ソフトが流通しており，それを使ったパスワードの不正取得によるアクセスなど，さまざまな手法が存在しています．

》》》 演習 11 《《《

次の演習を行ってみよ．

1．セキュリティとパスワード

常に同じパスワードを使っていると，セキュリティ上問題が発生しやすくなる．個人のセキュリティを高めるため，ここでは Linux のパスワードの変更を取り上げる．

（1）変更の手順

```
Z:¥>telnet 202.250.164.10                (コマンドプロンプトを起動して telnet を使う)

LASER5 Linux release 7.2 (sigure)
Kernel 2.4.9-13LL1 on an i686
login: c1001
Password:
                                         (ユーザ名とパスワードを入力してログインする)
[c1001@mc_srv c1001]$ passwd             (パスワードの変更コマンドを入力)
Changing password for c1001
(current) UNIX password:                 (今まで使っていたパスワードを入力)
New password:                            (新しいパスワードを入力)
Retype new password:                     (再度新しいパスワードを入力)
```

```
passwd: all authentication tokens updated successfully　(パスワード変更のメッセージ)
[c1001@mc_srv c1001]$
```

（2）変更後の確認

パスワードの変更を行った後は，新しいパスワードを使ってログインできるかどうか確認しておくことが必要である．なおパスワードを忘れると，次回からログインできないので注意しよう．

》》》 本章の復習 《《《

（1）ディジタル・ディバイドとはなにか．

（2）コンピュータを利用する上でのリスクにはどのようなものがあるか．

（3）リスクアナリシスとはどのようなことか．

（4）不正アクセスでポート・スキャンとはどのようなことか．

（5）アクセスコントロールとはどのようなことか．

12. セキュリティ対策の方法

インターネット上では，毎日のように新しいサイバー犯罪の手法が生まれていると言っても過言ではありません．さまざまな不正アクセスや犯罪が頻繁に起きており，それらから利用者を保護し，ネットワークやシステムを守らねばなりません．完璧な対策を施したと思っても，明日には不正アクセスによって侵入されてしまうかも知れないのが現実です．

また管理者が予想もしなかった設定の間違いや見落としをすることもあります．さらに複数の管理者がいる場合には，管理者間の連絡の手違いによるシステムのトラブルなどが起きないとも限りません．

セキュリティ対策には，100%完璧なものはないと考えるべきです．不正が起こりうるさまざまな観点から考えた対策を，対応できるかぎり実施しておく必要があります．

ここではセキュリティ対策の方法について，システム管理の考え方から，次のように整理して考えます．

（1）物理的なセキュリティ対策
（2）サーバのセキュリティ対策
（3）ネットワークのセキュリティ対策
（4）データのセキュリティ対策

12. 1. 物理的なセキュリティ対策

不正アクセスを試みる者は，攻撃対象となるターゲット(target)について，できる限り多くの情報を集めるといわれます．セキュリティ対策の手始めとして，建物や敷地あるいはサーバなどが設置してある重要な部屋へ，外部者が不正に侵入できないようにする対策を取ります［引用文献3］．

（1）建物への侵入を防ぐ

物理的なセキュリティでは，まず攻撃者を建物内に入れないようにするため，エリアごとに立ち入ることができる対象（人）を明確に定めます．例えば敷地の出入り口で「社員以外立ち入り禁止」にしたり，サーバの管理室では「担当者以外は入室禁止」のように提示したりします．

銀行の預金取引のようにより重要性が高いデータを扱う場合には，これらのセキュリティレベルに対応して，入退出管理を実施し，監視カメラやガードマンなどを置いて，不正な侵入者をチェックします．

（2）コンピュータへの接触を防ぐ

建物や敷地内に出入りが許可されている場合には，攻撃者がコンピュータへ接触することを防ぐ必要があります．社内ネットワークに接続されているコンピュータが，外部者でも直接操作できるようになっていると，社内ネットワークの構成やサーバの情報などを，インターネット経由で調べるよりも極めて容易

に知ることができます.

またコンピュータに触れられる状態になっていると，盗聴用のソフトを仕掛けられ，ネットワークを流れるパケットから，重要な情報が漏れる危険性が発生します．あるいはあらかじめ仕掛けをしておいて，インターネット経由で不正アクセスを行うときに，最初にそのコンピュータに侵入して踏み台にし，他のマシンを攻撃することがあります.

これらのことはコンピュータ本体に限ってのことではなく，使われていない部屋にネットワーク接続用ポートがあると，攻撃者は自分のノートパソコンなどを持ち込んで，社内ネットワークに侵入してしまいます.

そのため日常的に使われていない部屋に，コンピュータやネットワーク接続用ポートなどがあるときは，撤去するか使用できないようにしておく必要があります．また重要なコンピュータが設置されている部屋は，担当者がいなくなるときは鍵を掛け，監視カメラを設置するなどして監視します.

（3）情報の漏洩を防ぐ

攻撃者は何気なく使われている文書のなかからも，攻撃に役立つ情報を得ることがあります．例えばユーザ ID やパスワードに，社員名や役職名，部局に関係の深い単語，内線電話番号などが使われることがあります．これらの情報は社員名簿などから簡単に手に入れることができます.

そのため部外者が立ち入ることができる場所に，これらの情報を掲示しないようにし，また見えやすい場所に置かないように管理して，同時に社外への持ち出しも禁止します．これらの情報が記載された文書が不要になったときは，そのまま捨てると情報が漏れることがあるため，シュレッダーにかけて読めないようにしてから廃棄処分にします.

またバックアップ用のハードディスクなどの記憶媒体や，システムの情報が記載された文書は，攻撃者に悪用される情報をそのまま与えてしまう危険性があるため，厳重に管理する必要があります．サーバなどの重要なマシンのときは，これらの文書をマシンの傍らに置く場合があります．しかしセキュリティ対策を考えるならば，サーバマシンとは別な部屋で管理することが必要です.

12. 2. サーバのセキュリティ対策

サーバのセキュリティ対策を考えるときは 2 つの側面があります．ひとつは攻撃の対象となりそうな要素をできるだけ少なくする予防対策であり，あとひとつは攻撃を受けてしまったときに，できる限り速やかに元の状態に復帰し，運用を再開するための復旧対策が必要になることです［引用文献8］.

（1）サービスとポートの管理

インターネットなどのネットワークを経由した攻撃の場合には，ほとんどがネットワークに対して提供しているサービスを利用して行われます．この場合のサービスはコンピュータ上で運用しているものと，

サービスが可能な状態にポートが開いているものすべてを含みます.

サーバコンピュータの管理よってはサービスを提供していなくても，ポートが開いている状態（プロセスが起動している状態）になることがあります．このようなときはサービスを停止して，ポートを閉じておく必要があります.

（2）アクセス管理

アクセス制御(access control)を行うときは，すべてのポートを閉じた後，必要なポートだけを開くように設定します．そして攻撃を防ぐため，アクセス許可したコンピュータやネットワークまたはドメイン以外からはアクセスできないように設定します.

Linux(UNIX)サーバでは，TCP Wrapper（ラッパー）というソフトが組み込まれており，広くアクセス制御に利用されています．TCP Wrapper は telnet，ftp などのサービスに対して，サービスごとにアクセスを許可する相手を限定することが可能であり，アクセス状況を把握するためのログ（記録）つまりアクセスログを記録します.

以下にLinux(UNIX)で使用しているアクセス制御のファイルを示します．このファイルはhosts.allow という名前が付いており，このファイルに記載されたドメイン名やIPアドレスのコンピュータからのアクセスだけを許可しています.

以下の例では「ALL ： .aichi-u.ac.jp」という設定では，「.aichi-u.ac.jp」というドメイン名のコンピュータからの全てのアクセスを許可します．同じように「ALL ： 192.168.」という設定では，「192.168.」で始まるプライベートIPアドレスが割り当ててあるコンピュータからは，全てのアクセスを許可することになります.

この2つの設定によって，これらに指定された以外のコンピュータからはアクセスを拒否することができます.

```
# hosts.allow   This file describes the names of the hosts which are
#               allowed to use the local INET services, as decided
#               by the '/usr/sbin/tcpd' server.

ALL : 127.0.0.1
ALL : .aichi-u.ac.jp    : allow
ALL : 192.168.          : allow
```

（3）OSとアプリケーションの対策

ウイルスを含む不正アクセスの多くは，OS やアプリケーションソフトウエアが持つセキュリティホール(security hole)と呼ばれる欠点を利用したものがほとんどです．セキュリティホールがあると，不正なアクセスを許してしまいます.

新しく見つかったセキュリティホールを攻撃するツールが，インターネット上で頻繁に公開されていま

す．それに対応するため，マイクロソフトなどのソフトウエア会社も，対策を施したパッチ(patch)と呼ばれる修正用の追加ソフトを提供しています．

利用しているOSのバージョンアップやパッチの情報を定期的に調べ，最新バージョンのOSを導入したり，最新のパッチを自動的に適用する設定などを施すことが必要になります．

最近ではこれらの情報を，ソフトウエア会社がそれぞれのWebページで公開しています．またWindowsなどでは，アップデートしたソフトだけを自動的に更新する機能を提供しているので，この機能を使う設定をしておくことも有効です．

（4）ユーザとグループの管理

攻撃者の多くは，サーバに侵入すると，管理者（root）権限を取得しようと試みます．しかし一般のユーザIDとパスワードが取得できても，ネットワークにつながったコンピュータなら攻撃できる範囲が格段に広がってしまいます．

現状では他人でも簡単に推測できそうなパスワードを使っているユーザが多く，セキュリティ対策上問題が発生しやすい状況にあります．

そのため最近のOSではパスワードの有効期限を設定できるようになっており，管理者は必ずこの設定を実施し，一般ユーザが定期的にパスワードの変更を実行するように協力を求めます．よりセキュリティを高める必要がある場合には，一度だけ使用できる使い捨てのワンタイムパスワードを導入する場合もあります．

またサーバによっては未使用のユーザIDや，長い間使われていないユーザIDが登録してあることもあります．これらにパスワードが設定してあると，長期間パスワードの変更が行われず，不正侵入に悪用される危険性があります．このようなユーザIDは，早急に使用禁止にするか，削除しなければなりません．

またユーザのグループ管理を徹底し，ユーザグループごとにアクセス権（読み出し，書き込み，実行）を指定し，OSの設定情報が格納されているファイルに対しては，少なくても一般ユーザは書き込みできないように設定します．さらによりセキュリティを高める必要があるときは，読み込みもさせないように指定します．

（5）アクセスログによる監視

WindowsやLinuxなどほとんどのOSには，他のコンピュータからのアクセス（接続）状況やシステムの稼動状況を，ログファイル(log file)に記録する機能が備わっています．不正アクセスを早期に発見するために，必ずアクセスログ(access log)の監視をします．このログファイルを毎日管理者にメールで送る設定を行い，定期的にログファイルをチェックできるように設定を施します．

以下のログファイルはLinuxの例です．このログファイルからは，3回のftpによるアクセスがあり，その全部がログインに失敗していることが読み取れます．ログインに失敗したのは，許可されていないマシンからアクセスしようとしたためです．

```
 ##################### LogWatch 2.1.1 Begin ######################
 ---------------- Connections (secure-log) Begin ------------------
Connections:
   Service ftp:
      61.185.147.2: 1 Time(s)
      212.114.213.200: 1 Time(s)
      80.116.185.200: 1 Time(s)

**Unmatched Entries**
Dec  9 00:13:43 mc_srv xinetd[15438]: FAIL: ftp libwrap from=80.116.185.200
Dec  9 00:46:30 mc_srv xinetd[15462]: FAIL: ftp libwrap from=212.114.213.200
Dec  9 21:54:22 mc_srv xinetd[16781]: FAIL: ftp libwrap from=61.185.147.2
 ------------------ Connections (secure-log) End -------------------
```

また次のアクセスログからは，3回のアクセスがあり，そのうち2回はftpによるもので，あとの1回はtelnetによるものです．ftpによるものは2回ともアクセスに失敗していますが，telnetのほうは成功していることがわかります．

```
 ##################### LogWatch 2.1.1 Begin ######################
 ---------------- Connections (secure-log) Begin ------------------
Connections:
   Service ftp:
      213.17.194.74: 1 Time(s)
      211.146.115.226: 1 Time(s)
   Service telnet:
      202.250.164.189: 1 Time(s)

**Unmatched Entries**
Dec 10 09:08:11 mc_srv xinetd[17666]: FAIL: ftp libwrap from=213.17.194.74
Dec 10 19:18:08 mc_srv xinetd[18114]: FAIL: ftp libwrap from=211.146.115.226
 ------------------ Connections (secure-log) End -------------------
 ######################## LogWatch End ##########################
```

また攻撃者がコンピュータに侵入すると，アカウント情報やログファイルなどの重要なファイルの改ざんを行うことがあります．このようなときにはファイルに変更が発生するので，ファイルが変更されたことを調べて報告してくれる侵入検知システムを入れておくと，素早く侵入に気づくことができます．

12. 3. ネットワークのセキュリティ対策

ネットワークについても予防と発見の両面からセキュリティ対策を施します．ネットワークのセキュリティ対策を行うには，不正進入を防ぐセキュリティシステムを導入する必要があります．例えばファイアウォールやウイルス対策ソフトあるいは侵入検知システムなどの導入を実施します．

（1）ファイアウォール

ファイアウォール(fire wall)は，内部のネットワークと外部のネットワークとの間で，送受信するデータを制御して，セキュリティ対策を実施するシステムです．ファイアウォールにはパケットフィルタリング(packet filtering)とアプリケーションゲートウェイ(aplication gateway)があります．

パケットフィルタリングでは，それぞれのパケットのヘッダ情報を調べ，発信元と送信元のIPアドレスやポート番号を調べて，そのパケットを通過させるか遮断するかを制御します．

この制御によって，サーバごとにアクセス可能なプロトコル（サービスの種類）を限定したり，特定のサイトからのアクセスだけを許すというような制御ができます．

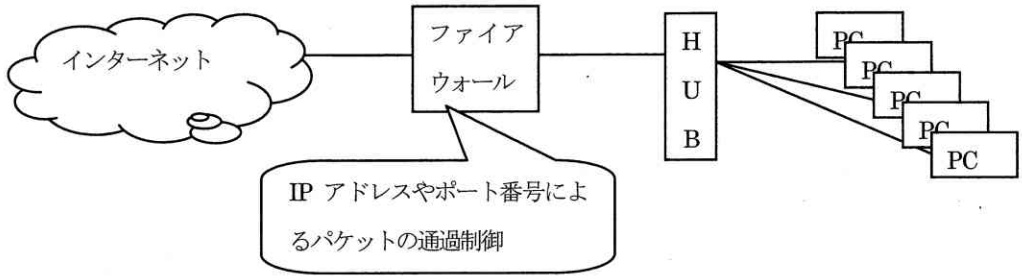

図 12.1 ファイアウォールの位置づけ

（2）プロクシサーバ

アプリケーションゲートウェイでは，telnet や ftp などのアプリケーションごとに用意したプロクシサーバが通信の中継をします．プロクシ(proxy)サーバは代理サーバのことで，実際のサーバとユーザに間に設置され，代理としてインターネットとの接続を行うコンピュータのことです．

例えばユーザが内部のコンピュータから，外部の Web ページを見るときは，プロクシサーバに接続先を伝え，プロクシサーバが実際の Web サーバに接続してデータを送信してもらい，ユーザのコンピュータに

転送するようになります．ユーザには直接相手の Web サーバからデータが送信されているかのように見えます．

（3）ウイルス対策ソフト

ウイルス対策は，ユーザが個人で行う場合は，ウイルス対策ソフトをインストールして設定します。このほか組織全体でメールに添付されたウイルスをチェックする場合があります．この場合には，到着したメールのすべてをチェックし，ウイルスが添付されていないかどうかを調べ，その後ユーザに配信されるようになります．

（4）侵入検知システム

サービスを提供している間は，ファイアウォールやサーバ上でアクセス制御を行っても，提供しているサービスが攻撃に利用される可能性が残ってしまいます．このようなファイアウォールなどで防御することのできない侵入や攻撃を検知するのが，IDS（Instrusion Detection System）と呼ばれる侵入検知システムです．

IDS では，ネットワーク上を流れるパケットを取り込み，IDS の内部に備わっている攻撃パターンのデータベースと比較を行い，そのパケットが攻撃であるかどうかを調べます．従って IDS が持つデータベースの有効性が，侵入検知の性能を決めることになるため，定期的なデータベースの更新が必要になります．

また IDS では侵入を検知した場合に，管理者に通知する機能だけのものから，通信を自動的に遮断したり，ルータやファイアウォールと連携して，パケットフィルタリングの設定を自動的に変更するものなどもあります．

12．4．データのセキュリティ対策

組織や個人を問わず，重要なデータが盗難にあったり改竄されたりしては，データの信頼性が失われてしまい極めて大きな問題となります．このような犯罪も多くなっており，犯罪からデータを守る方法として暗号化とバックアップが有効な手段となります．

（1）データの暗号化

データの内容が他人に見られると，プライバシーが侵害されるだけでなく，犯罪に悪用されこともあり，社会的にも問題を引き起こしてしまいます．暗号化を行う目的は，データの内容を第三者に見られないようにし，データが改竄されていないことや，本人がそのデータを作成したことを保障するためにも利用されます．

暗号化の技術は，暗号化と元に復元する復号化に使われる鍵の種類によって，大きく 2 種類があります．ひとつは共通鍵暗号方式（秘密鍵暗号方式）であり，DES（Data Encryption Standard）が代表的なものです．

この方式では，暗号用と復号用の鍵が同じものとなっている点が特徴です．

あとひとつは公開鍵暗号方式といい，暗号用と復号用の鍵がことなる方式です．データを暗号化する人と復号化する人が同じ秘密鍵を共有しない点で，共通鍵暗号方式よりも公開鍵暗号方式のほうが有効性が高いといわれています．

（2）データのバックアップ

もし不正アクセスや侵入によって，データが消去されたりあるいは改竄されているようなことが判明した場合は，早急にデータを復旧させないとシステムの運用が不可能になってしまします．

そのためには最新でかつ改竄されていない正しいデータのバックアップを用意しておく必要があります．バックアップ作業はデータが大きくなると時間がかかるため，データの重要度や更新頻度を考慮して，バックアップの間隔を設定します．

なおバックアップを作成するときは，全部のデータを完全にバックアップするフルバックアップ(full backup)と，前回から変更された部分だけをバックアップする差分バックアップ(differential backup)を適宜組み合わせて，作業時間を短縮する工夫を行うことも必要になります．

さらに改竄されたデータであることに気づかずにバックアップしたり，記憶媒体の劣化などによってバックアップデータの読み出しができなくなることも起こりえます．そのためバックアップデータを定期的にチェックし，正しいデータがバックアップされ，バックアップデータも正しく読み出せることを確認することが必要になります．これらを怠ると，いざ必要なときにバックアップから復元できなことになりかねません．

12．5．ネットワーク特性とコンピュータ犯罪

コンピュータ犯罪は情報社会特有の犯罪ともいうべきものです．以前は情報技術に熟知している専門家によるものが多く発生していました．しかし情報機器や情報技術の知識が一般に広く普及したことに伴い，不正アクセスなどによる犯罪行為が一般大衆にまで広がる傾向があります．

またインターネットの普及により，ネットワーク上での有害情報の流通が問題となっています．例えばわいせつ情報，差別的な用語による表現，なりすまし，いつわりの情報，電子ストーカー，ウイルスなどがあります．これらの問題はネットワークが持つ犯罪に対する弱さ(脆弱性)から発生しています．

情報化社会において，ネットワークを有効に活用し，犯罪に巻き込まれないためには，ネットワークの犯罪の特性を理解しておく必要があり，次のような点が指摘されます．

（1）匿名性

チャットや電子掲示板などでは，個人を特定する情報が相手に知られにくく，匿名性を悪用した誹謗中傷などの書き込みが行われることがあります．

（2）不特定多数への影響

不特定多数の人が利用することにより，匿名性ともあいまって，犯罪が多くの利用者に及ぶ危険性があります．

（3）時間と空間の超越

世界中に瞬時にアクセスできるため，コミュニケーションがとりやすいが，便利な半面さまざまな形の危険も伴います．ウイルスや不正アクセスなどは，容易に国境を越えてしまいます．

（4）証拠が残りにくい

ネットワークを流通するものが電子データの情報であるため，犯罪の痕跡として残りにくいという特徴があります．

12. 6. 情報操作による犯罪

悪意を持って意図的に情報を隠蔽したり，改造したり，破壊したりすることを情報操作といいます．これらの多くは不正アクセスやウィルス，盗聴などによって行われ，他人の財産権や人格権などを侵害することによって，社会的にもさまざまな問題を引き起こします．

（1）不正アクセス

正規にユーザ登録されていない人やアクセス権を持たない人が，不正にアクセス権を取得してコンピュータに進入したり，勝手に利用したりすると不正アクセス(illegal access)となります．主な不正アクセスの手段は，システムの弱点であるセキュリティホールを悪用して侵入し，プライバシーに関わる個人情報を盗み見たり，ファイルの削除や改ざんなどを行うことです．さらに侵入したコンピュータを踏み台として，他のコンピュータに侵入して同様の不正行為を繰り返すことが多く起きています．

インターネットの普及に伴い不正アクセスも増大したことから，日本では1999年に不正アクセス防止法が成立し，不正アクセスは犯罪行為と見なされるようになっています．

（2）情報の改竄

情報やデータを特定の目的のために改変し，その情報を勝手に流用したり，盗用したりするもので，著作権法などに触れることになります．またシステムに備わっているデータを悪意を持って改変し，間違った情報を提供することによって，他の人に被害を与えたり，人権侵害を引き起こすこともあります．さらに銀行などのデータやクレジットカードなどの情報を改竄して，不当な利益を搾取する場合もあります．

（3）情報の捏造

情報を発信する者が何らかの悪意を持って，偽りの情報を流布させたり，事実とは異なる未確認の情報を流したりすることが情報の捏造にあたります．情報の捏造によっても該当者や団体などに，人格権や財産権などの上で被害を持たらすことがあるばかりでなく，銀行の取り付け騒ぎのように社会的な問題を引き起こすこともあります．

（4）情報の破壊

不正アクセスやウィルスなどによって，情報を悪意を持って破壊し，消滅させる犯罪のことをいいます．

（5）情報の隠蔽

社会的に重要で必要な情報を，個人や組織の利益を優先するあまり，社会に公表しないでいることです．情報の隠蔽の結果として，必要な情報が利用できなくなり，社会に悪影響を与える場合があります．

例えば自動車会社が，車の重大な欠陥を隠してその情報を公開しないと，自動車事故につながりかねず，社会的な問題となるなどが情報の隠蔽にあたります．

12. 7. 有害情報の流通

インターネットの普及は，犯罪の形を変えつつあります．インターネット上にプライバシーを侵害する情報を流したり，ねずみ講などの広告が流れたり，武器などの違法な物品の販売広告が流れることもあります．有害情報の例には次のようなものがあります．

（1）ホームページにわいせつ画像などを掲載
（2）電子掲示板に嫌がらせの書き込み
（3）チャットによる誘惑
（4）ホームページを使った詐欺商法
（5）ねずみ講やマルチ商法の広告

12. 8. ハイテク犯罪の状況

情報通信技術の急速な発展によって，インターネットでは電子メールを始めとしてネットオークション(net auction)，ネットショッピング，ネットバンキング(net banking)などのさまざまなサービスが提供されており、人々の生活を便利にしています．その一方においてインターネット上では，不正アクセスやネットオークションを悪用した詐欺などをはじめとして，ハイテク犯罪の危険性も急激に増加しています．

警察庁は最近のハイテク犯罪の統計データを公開しています．それによれば犯罪の検挙数は増加傾向に

あることが示されています.

表 12.1 ハイテク犯罪の検挙状況(警察庁)

(http://www.npa.go.jp/hightech/toukei/html/html10.htm より引用)

罪　種	平成 12 年	平成 13 年	平成 14 年
コンピュータ、電磁的記録対象犯罪	44	63	30
電子計算機使用詐欺	33	48	18
電磁的記録不正作出・毀棄	9	11	8
電子計算機損壊等業務妨害	2	4	4
ネットワーク利用犯罪	484	712	958
児童買春	8	117	268
児童ポルノ法違反	113	128	140
わいせつ物頒布等	154	103	109
詐欺	53	103	112
青少年保護育成条例違反	2	10	70
名誉毀損	30	42	27
脅迫	17	40	33
著作権法違反	29	28	31
その他	80	151	168
不正アクセス禁止法違反	31	35	51
合　　計	559	810	1,039

12. 9. ハイテク犯罪の種類

警察庁の Web ページ(URL: http://www.npa.go.jp/cyber/)では，ハイテク犯罪を分類して，その実例とともに情報を公開しています．以下は警察庁の Web ページからの引用です．

ハイテク犯罪は，「コンピュータや電磁的記録を対象とした犯罪」と「コンピュータネットワークをその手段とした犯罪」に大きく分けられています．

「コンピュータや電磁的記録を対象とした犯罪」とは，刑法に規定されている電子計算機損壊等業務妨害罪，電子計算機使用詐欺罪等のほか，ウイルスに感染したファイルを送って，コンピュータを正常に使用できない状態にした場合（器物損壊罪）等です．

また「コンピュータネットワークをその手段とした犯罪」とは，パソコン通信の電子掲示板を利用し，覚せい剤等の違法な物品を販売した場合や，コンピュータネットワーク上で他人のパスワードを使用し，

その人になりすまして嘘の広告を掲載し，販売代金をだまし取った場合，あるいはインターネットに接続されたサーバコンピュータにわいせつな映像を置き，これを多くの人に対して閲覧させた場合等です，

》》》 本章の復習 《《《

（1）サーバのセキュリティ対策ではどのようなことを行えばよいか.

（2）ファイアウォールとは何か.

（3）侵入検知システムとはどのようなものか.

（4）コンピュータ犯罪の主なものにはどのようなものがあるか.

（5）不正アクセスとはどのようなことか.

引用文献

(1) CERNのURLにはWeb誕生の経緯が紹介されている(2004.3.3).
http://public.web.cern.ch/public/about/achievements/www/www.html

(2) ドメイン名の取得サービス(2004.3.3). http://www.onamae.com/

(3) 遠藤薫著：システムリテラシー2ーマルチメディアとネットワークー，実教出版，pp.243，1996.

(4) Hagen, Silvia：IPv6 エッセンシャルズ，p.357，2003.

(5) 日立システム&サービス：IT用語辞典(2004.3.3). http://www.hitachi-system.co.jp/index.html

(6) ICANN のURL(2004.3.3). http://icann.nic.ad.jp/

(7) 稲垣耕作著：コンピュータ科学の基礎，コロナ社，pp.216，1996.

(8) 石田晴久監修：要点チェック式インターネット教科書（上），IEインスティテュート，p.381，2000.

(9) 石田晴久監修：要点チェック式インターネット教科書（下），IEインスティテュート，p.389，2000.

(10) 小林浩，江崎浩著：インターネット総論，共立出版，284p，2002.

(11) 久野靖著：UNIXによる計算機科学入門，丸善，pp.347，1997.

(12) 村田正幸ほか著：社会基盤としてのインターネット，岩波書店，pp.291，2001(岩波講座インターネット6).

(13) 日本ネットワークインフォメーションセンター(JPNIC)(2004.3.3). http://www.nic.ad.jp/ja/

(14) RFC（英文）のURL(2004.3.3). http://www.ietf.org/rfc.html

(15) RFC（日本語）のURL(2004.3.3). http://rfc-jp.nic.ad.jp/

(16) 尾家祐二ほか著：インターネット入門，岩波書店，222p，2001(岩波講座インターネット1).

(17) Ray Tomlinsonに関するURL：http://www.bbn.com/presskit/docs/firstemail.pdf,
http://www.bbn.com/email/index.html

(18) 下山智明，城谷洋司著：Sunシステム管理，アスキー，831p，1991.

(19) 総務省：情報通信白書，ぎょうせい，平成15年度版，Web版は以下のURL（2004.3.3).
http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/cover/index.htm

(20) 竹下隆史ほか著：マスタリングTCP/IPーインターネットワーク編ー，オーム社，p.260，1995.

(21) 竹下隆史ほか著：マスタリングTCP/IPー入門編ー，オーム社，p.336，2002.