第3回　システム環境設定ゼミ

1　イーサネットの基礎

PC にネットワーク インターフェイス カード（NIC：Network Interface Card）が標準搭載されることも珍しくなくなり、LAN に接続されるという光景は、もはや当たり前のことになりました．現在、LAN を構築するための製品はイーサネッ（Ethernet）と呼ばれる規格に準じたものがほとんどであり、それ以外のものを見つけるのは難しいです．イーサネットは、「Experimental Ethernet」といわれる 3Mbits/s の伝送速度のものから開発が始まり、10Mbits/s、100Mbits/s、そして 1000Mbits/s と技術の進歩とともに高速化を実現している．ここからは、イーサネットがどのような仕組みで動作しているのかを説明します．

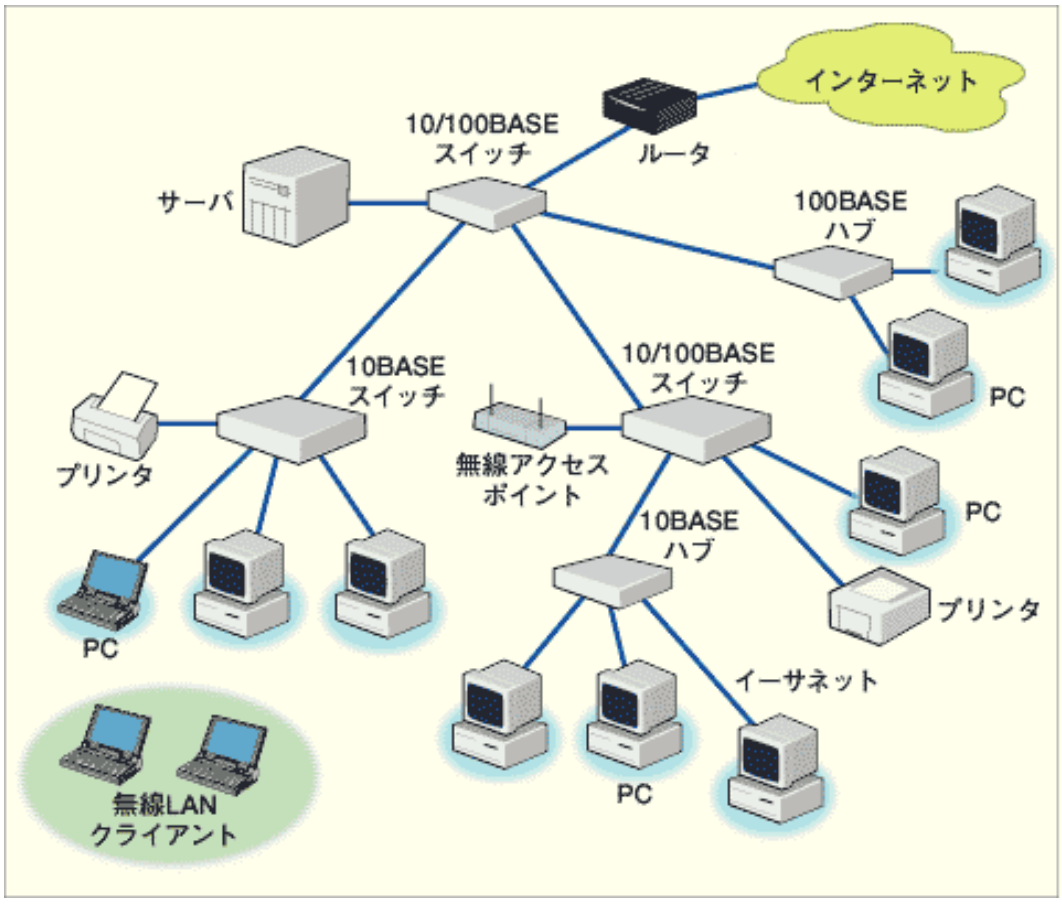

Fig. 1　LAN

1.1　イーサネットの基本的な仕組み

10BASE-T は、伝送速度 10Mbits/s のイーサネットである．数年前までは、伝送メディアとして同軸ケーブルを用いた 10BASE-2 や、10BASE-5 といったものもあったが、現在ではケーブル敷設の簡便さから UTP（Unshield Twist Pair：非シールド ヨリ対線）を利用する 10BASE-T が一般的である．現在、多くの企業が使用しているのが、この 10BASE-T をベースとしたもので、イーサネットといえば 10BASE-T というほどに、広く普及している．10BASE-T は、1990 年に IEEE802.3i（IEEE：米国電気電子学会）として標準化されている（コラム「IEEE802 の各種規格」）．10BASE-T の「T」は、ツイスト ペア ケーブルを意味する文字である．10BASE-T で利用する UTP は、カテゴリ 3

以上の 2 対 4 芯のものだ（ケーブル中に 4 対のワイヤがあっても、そのうち 2 対しか使わない．1 対は 2 芯＝ 2 本のワイヤからなる）．この「カテゴリ」という用語だが、これはケーブルの品質を表す言葉で、数字が大きいほど高品質で、外部からのノイズの受けにくさを示している．

1.2　イーサネットの基本「CSMA/CD 方式」

イーサネットの特徴としてまず挙げられるのが、「共有メディア方式」といわれる伝送方式である．これは文字どおり、伝送メディア（イーサネット ケーブル）をすべての機器で共有しているという意味であり、同じ伝送メディアに接続された機器同士は、この伝送メディアを互いに仲よく分け合いつつ通信を行う．伝送メディアを共有しているため、ある瞬間に通信することができるのは、1 つのペア（送信側機器と受信側機器）のみである．あるペアが通信中であれば、当然それ以外の機器は通信することができない．そこで、各機器の間で伝送メディアの使用の調停をする仕組みが必要となる．イーサネットでは、この調停に CSMA/CD（Carrier Sense Multiple Access with Collision Detection）という方式を採用している．

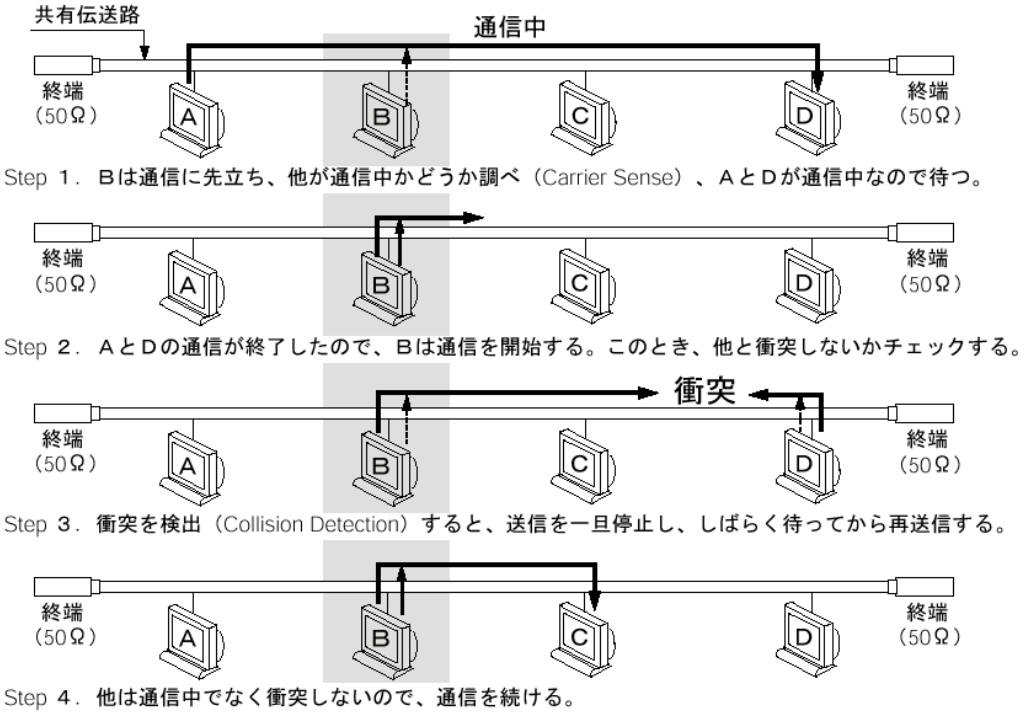

Fig. 2　イーサネットのアクセス制御方法

CSMA/CD の基本ルールは、「すべての機器は伝送メディアを平等に利用でき、機器間で優先度や使用順序は定めない」、加えて「ほかのペアが通信中であったら、その通信が終わるまで送信を待つ．終わったことを確認したら自分が送信を始める」という 2 つだ．まず、ほかのペアが通信中であることを知るために、CSMA/CD では「キャリア検出」を行う．各機器は、自分が送信を開始しようとした際に、伝送メディアであるケーブル上の電気信号の状態を調べ、ほかの機器が送信中かどうか（つまり生じる電気信号の変化がないかどうか）をチェックするのである．電気信号の変化がなければ、伝送メディアが空いているということであり、逆に変化があれば伝送メディアはほかの機器によって使用されているということである．このチェックの結果によって、各機器は自分がただちに送信を開始してよいか、あるいはほかの通信が終了するのを待たなければならないのかを判断する．

2　伝送速度 100Mbits/s の 100BASE-TX

100BASE-TX は、伝送速度が 10BASE-T の 10 倍の 100Mbits/s に引き上げられた、「Fast Ethernet」ともいわれるもので、1995 年に IEEE802.3u として標準化されている．

100BASE-TX は、現在、最も数多くの製品が出荷されているイーサネット製品である．CSMA/CD を採用して点など、10BASE-T と基本的な仕組みは変わっていない．というよりも、むしろ極力違いがないように標準化が進め

られたと言ったほうがよい．10BASE-T と異なる点はといえば、10BASE-T からのアップグレードを簡単にするためのオート ネゴシエーション機能が加えられたことと、伝送速度が 10 倍になったことで、コリジョン ドメインが 10BASE-T の 1/10 である 250m と短くなったこと、ケーブルにカテゴリ 5 の UTP を使用することが必須となったことなどだ．

このように 10BASE-T との差が少ないように標準化された 100BASE-TX だが、10BASE-T と 100BASE-TX は、データ転送速度が異なるため、直接接続できるわけではない点に注意していただきたい．10BASE-T と 100BASE-TX を接続するためには、後述のスイッチなどを利用する必要がある．

100BASE の規格には、伝送メディアの違いなどにより、100BASE-FX や 100BASE-T2、100BASE-T4 といった規格も存在するが、100BASE-TX ほど普及していないので、ここでは説明を割愛する．

2.1 全二重通信

これまでの説明では、受信中はデータが送信されてくるのを待つ、あるいは送信中はほかの機器からの信号は受信しないということになっていたが、接続先がスイッチ（後述）などの場合、実際には送受信を同時に行うといったことが可能だ．これを全二重通信といい、100BASE-TX の場合、帯域は送信、受信それぞれについて 100Mbits/s ずつ、合計 200Mbits/s ということになる．一方、従来の送信・受信を交互に行う方法を半二重通信という．10BASE-T でも原理的には全二重通信が可能であるが、普及したのは 100BASE-TX 対応製品の登場以後である．

2.2 オート ネゴシエーション機能

オート ネゴシエーション機能とは、接続される相手によって、自分の通信速度を切り替える機能である．つまり、相手が 10BASE-T であれば 10Mbits/s に、100BASE-TX であれば 100Mbits/s に、といった具合いに通信速度を切り替える機能だ．この機能は、インターフェイス カードまたはハブでサポートされ、LAN 内での 10BASE-T ／ 100BASE-TX の混在環境を可能にする．たとえば、10BASE-T のハブに、100BASE-TX のインターフェイス カードを接続した場合、カードはこれを自動的に認識し、10BASE-T で接続するようになる．逆に、ハブがオート ネゴシエーション機能付きのものであれば、クライアントのインターフェイス カードに合わせて 10BASE-T と 100BASE-TX が切り替わるので、部分的に 10BASE-T から 100BASE-TX へ移行していくことが可能だ．この機能を使うことで、いっせいに機器を入れ替える必要がなくなるというメリットがある．ただし、過去の製品の中には、自動検出に失敗するものもあった．そのため、手動でも 10BASE-T と 100BASE-TX の切り替えが行えるハブも登場した．

3 ハブ／スイッチ選択の基礎知識

3.1 スイッチの動作について

スイッチは、すでに述べたように、各ポートを流れるパケットから MAC アドレスを読み出し、送信元と宛先が接続されているポート同士で直接データをやり取りし、ほかのポートにはパケットを流さない．この機能を実現するため、スイッチには、MAC アドレスが登録される経路探索テーブルが内蔵されている．

経路探索テーブルは、基本的に自動的に MAC アドレスを収集するように作られている．これは、イーサネットがパケットの送信時に送信元 MAC アドレスをヘッダに書き込んでいるので、それを記憶しておくようにするのが一般的だ．一定時間使われなかった MAC アドレスやポート間のつなぎ変えなどで移動した結果、同じ MAC アドレスが以前と違うポートに存在するような場合、その情報を破棄して再収集する．スイッチのカタログをチェックする際に、アドレス テーブルなどの表記で、この経路探索テーブルの容量や記録可能な MAC アドレス数が掲載されているので必ずチェックしておこう．必ずしも大きいほうが優れているというわけではないが、大規模なネットワークでの利用を考えている場合は、大きいに越したことはない．低価格なスイッチでは、1024〜8192 個程度の MAC アドレスを記憶できるものが多い．これでも通常の利用には十分過ぎるほどだ．

4 TCP/IP

インターネットの標準プロトコルである，TCP[1]と IP[2]は当然セキュリティと深い関係がある．よって，ここでは，TCP/IP について簡単な説明を行う．

[1]Transmision Control Protocol
[2]Internet Protocol

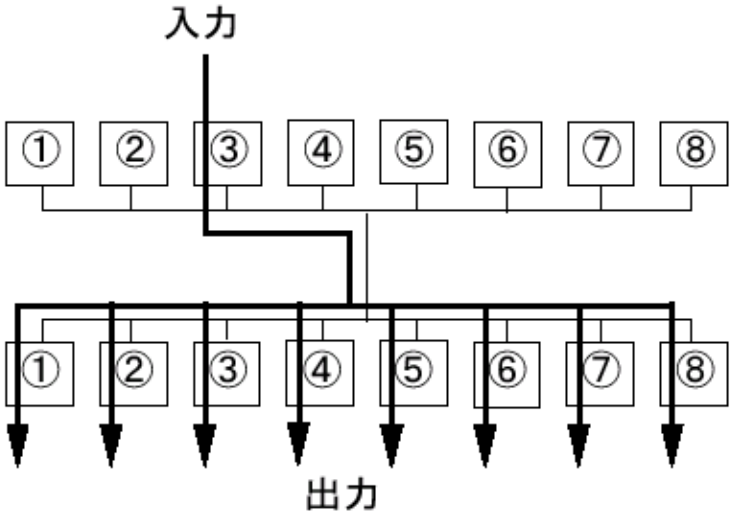

Fig. 3　リピータハブのデータ転送

Table 1　OSI 参照モデル

階層	階層名	役割
第 7 層	アプリケーション層	データ通信を利用した様々なサービスを人間や他のプログラムに提供
第 6 層	プレゼンテーション層	第 5 層から受け取ったデータをユーザが分かりやすい形式に変換したり、第 7 層から送られてくるデータを通信に適した形式に変換
第 5 層	セッション層	通信プログラム同士がデータの送受信を行うための仮想的な経路 (コネクション) の確立や解放
第 4 層	トランスポート層	相手まで確実に効率よくデータを届けるためのデータ圧縮や誤り訂正、再送制御など
第 3 層	ネットワーク層	相手までデータを届けるための通信経路の選択や、通信経路内のアドレス (住所) の管理
第 2 層	データリンク層	通信相手との物理的な通信路を確保し、通信路を流れるデータのエラー検出
第 1 層	物理層	データを通信回線に送出するための電気的な変換や機械的な作業

4.1　OSI 参照モデル

通信を行うためには必要な非常に多くの様々な機能が必要である．通信プロトコルはそのすべての機能を規定しなければならない．しかしながら，非常に多くの機能をその機能ごとに分割して考えることによって，理解しやすく設計も容易になる．

OSI 参照モデルとは，ISO[3]により制定された，異機種間のデータ通信を実現するためのネットワーク構造の設計方針「OSI[4]」に基づき，コンピュータの持つべき通信機能を階層構造に分割したモデルである.「OSI 基本参照モデル」「OSI 階層モデル」とも呼ばれる．通信機能を 7 階層に分け，各層ごとに標準的な機能モジュールを定義している．各階層とその役割について，Table 1 に示す.

4.2　Internet Protocol

第 3 層のネットワーク層に位置する IP は，IP アドレス指定，ルーティング，パケットの分割と再構成の責任を持つルーティング可能なプロトコルである.

4.2.1　IP アドレス指定

それぞれの TCP/IP ホストは，IP アドレスによって識別される．IP アドレスはネットワーク層アドレスで，データリンク層アドレスからは独立している．TCP/IP を使用して通信するホストにはそれぞれ一意の IP アドレスが必要である．それぞれの IP アドレスには，ネットワーク ID とホスト ID があり，それらはサブネットマスクによって IP

[3]国際標準化機構
[4]Open Systems Interconnection

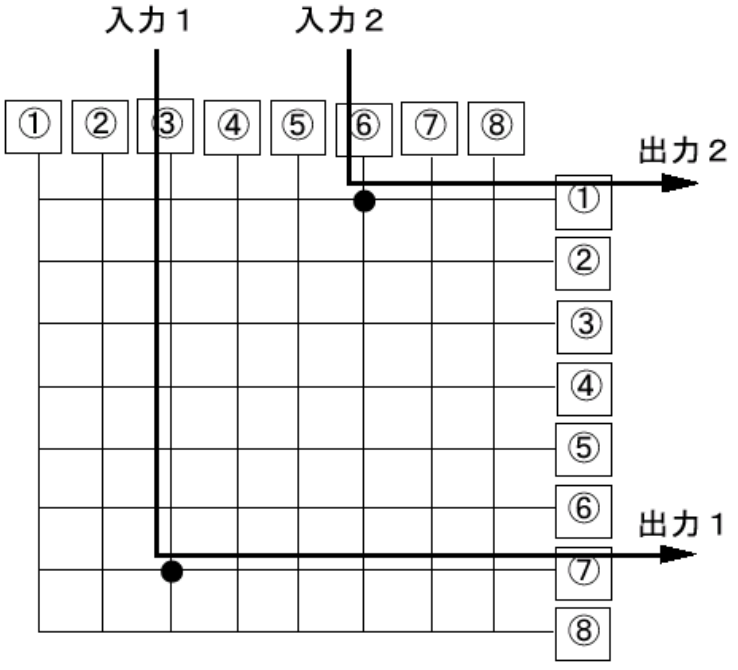

Fig. 4　スイッチングハブのデータ転送

Table 2　ルーティングテーブルの例１

宛先	ネットマスク	ゲートウェイ	インターフェイス	メトリック	目的
0.0.0.0	0.0.0.0	157.55.16.1	157.55.27.90	1	既定経路
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1	ループバック
157.55.16.0	255.255.240.0	157.55.27.90	157.55.27.90	1	直接繋がっているネットワーク
157.55.27.90	255.255.255.255	127.0.0.1	127.0.0.1	1	ローカルホスト
157.55.255.255	255.255.255.255	157.55.27.90	157.55.27.90	1	ネットワークブロードキャスト
244.0.0.0	244.0.0.0	157.55.27.90	157.55.27.90	1	マルチキャストアドレス
255.255.255.255	255.255.255.255	157.55.27.90	157.55.27.90	1	既定ブロードキャスト

アドレスを分割することができる.

4.2.2　IP ルーティング

宛先 IP アドレスに基づいてパケットを転送することを,「ルーティング」と言う．ルーティングは送信側 TCP/IP ホストと IP ルータで行われる.「ルータ」はあるネットワークから別のネットワークにパケットを転送する装置である．送信側ホストとルータのどちらの場合も，パケットの転送先を決定しなくてはならない．そのような決定を行うために，IP 層ではメモリ内に格納されているルーティングテーブルを調べ，最適な経路を選択する．

Table 2 に TCP/IP ホストの既定のルーティングテーブルの例を示す．このホストは一枚のネットワークアダプタを搭載し，IP アドレス 157.55.27.90，サブネットマスク 255,255,240,0(/20)，既定のゲートウェイ 157,55,16,1 である．

また SOB のゲートウェイ sandbox(192.168.6.1) のルーティングテーブルは Table 3 のような構成になっている．

Table 3　sandbox のルーティングテーブルの例

宛先	ネットマスク	ゲートウェイ	インターフェイス	メトリック
202.23.143.0	255.255.255.0	*	eth0	0
192.168.6.0	255.255.255.0	*	eth1	0
192.168.30.0	255.255.255.0	202.23.143.1	eth0	3
default	0.0.0.0	202.23.143.1	eth0	0

Table 4　ウェルノウンポート番号の例

ポート番号	サービス
21	FTP
23	TELNET
25	SMTP
53	DNS
67	DHCP
80	HTTP
110	POP3

4.3 Transmision Control Protocol

第４層のトランスポート層に位置する TCP は，信頼性の高い，１対１のコネクション型の通信サービスを提供する．TCP は TCP 接続の確立，送信されたパケットの順序付けと受信確認，転送中に紛失したパケットの復元に責任を持つ．

4.3.1 TCP ポート

IP アドレスを使うと，コンピュータを特定することができる．しかし，コンピュータの中では，同時に複数のプログラム (サービス) が実行されている．これらのどのプログラム (サービス) を使用するかを区別するものをポート番号という．

ポート番号は 16 ビットの整数で，１つのコンピュータの中で動いているプログラム (サービス) に対して，すべて別の値が割り振られている．パケットには送り先 IP アドレスと送り先ポート番号をヘッダとして付加することで，目的とするプログラム (サービス) にデータを送り届けることができる．

サーバソフトウェアを実装する際，サーバソフトウェアが使うポート番号を自由に決めることができる．一方で，クライアントソフトウェアがサーバと通信するためには，サーバが使うポート番号をあらかじめ知っておかなければ，パケットを送ることができない．よって，インターネットではあらかじめよく使用するサービスに関しては，ポート番号が定められている．このように，前もって決められたポート番号をウェルノウン（Well Known）ポート番号と呼ぶ．

5 FireWall

FireWall はネットワーク上のシステムやデータのセキュリティを守るために重要な技術の 1 つです．

FireWall は組織内部のローカルなネットワーク（Intranet）と，その外部に広がる Internet との間に，外部からの不正なアクセスを防ぐ目的で設置されるルータやホスト，またはその機能的役割の総称を指します．FireWall で重要なことは，基本的に最低限必要なプロトコルだけを通し，それ以外のプロトコルはすべて遮断するということです．その方法としては，パケットフィルタリング方式，コネクションフィルタリング方式（この方式はさらに，アプリケーションゲートウェイ方式とサーキットレベルゲートウェイ方式に分けられます.）などがありますが，実際のシステムではこれらを柔軟に組み合わせて安全性の高い FireWall を構築しています．

5.1 パケットフィルタリング方式

パケットフィルタリング方式は，IP パケット毎にフィルタリングを行う方式です．この方式では，IP データのヘッダ情報，TCP/UDP のパケットのヘッダ情報を参照して，パケットの通過の許可または不許可の制御を行っています．これは，ルータのパケットフィルタリング機能を応用した方式です．外部ネットワークと内部ネットワークの接続は，IP(ネットワーク層) レベルで直接制御されるため、内部ネットワークの IP アドレスが外部に直接見えてしまうという問題があります．

5.1.1 パケットフィルタ

パケットフィルタとはルータの機能を強化して，個々のパケット単位で通過させたり，禁止したりできるようにしたものです．TCP/IP プロトコルならば，IP パケットを単純にフォワードするだけでなく，パケット中に含まれるデータを調べて，送信元や送信先の IP アドレス，プロトコルのタイプ，ポート番号などに基づいてパケットを通過させたり破棄したりします．

パケットフィルタリング方式のゲートウェイで実際に運用する場合は，デフォルトではすべての IP フォワードを禁止しておき，ユーザーに提供したいサービスのパケットだけを通過できるようにフィルタリングルールを設定します．

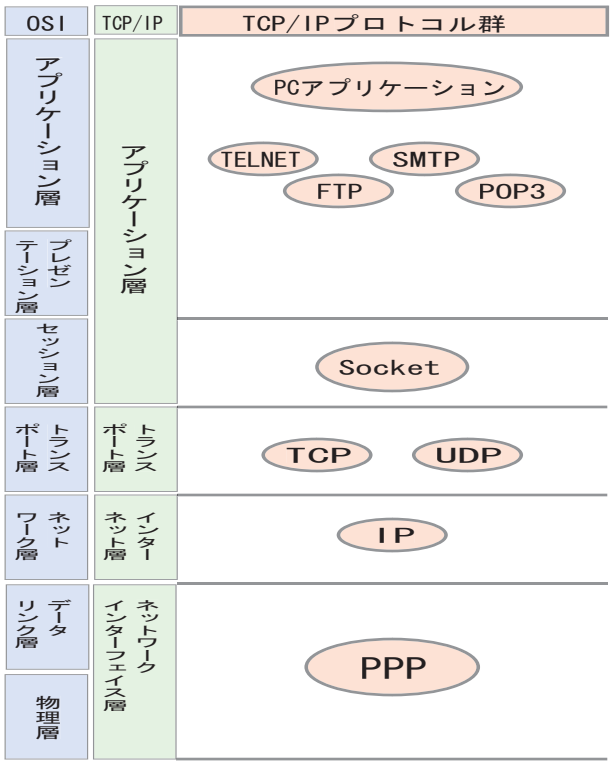

Fig. 5　TCP/IP プロトコル群と OSI 参照モデルとの関係

しかし，使用できるアプリケーションが増えれば，それだけ複雑なフィルタルールを設定しなければならないので，条件の設定をミスしたりするとファイアウォールに思わぬ穴が空くおそれもあります．

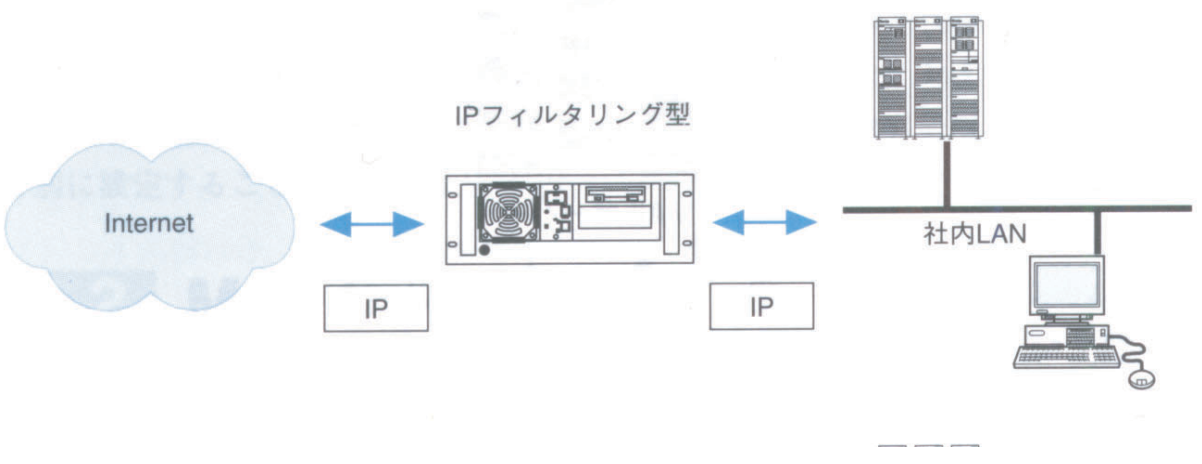

Fig. 6　パケットフィルタリング方式

5.2　コネクションフィルタリング方式

TCP/IP のコネクション要求によって，フィルタリングを行う方式で，外部ネットワークと内部ネットワークを Proxy と呼ばれるゲートウェイマシンが間に入って接続する方式です．Proxy サーバーはインターネットとの接続時に，セキュリティを確保するために設置されるサーバーのことです．この Proxy サーバーによって，ネットワーククライアントのアプリケーションは直接インターネットにアクセスするのではなく，ゲートウェイとの間でデータをやり取りすることになり，実際にはゲートウェイが外部とデータのやり取りをします．また，Proxy サーバーにはセキュリティ機能以外にもキャッシュの機能があります．Proxy サーバーを介して WWW にアクセスした際には，インターネット

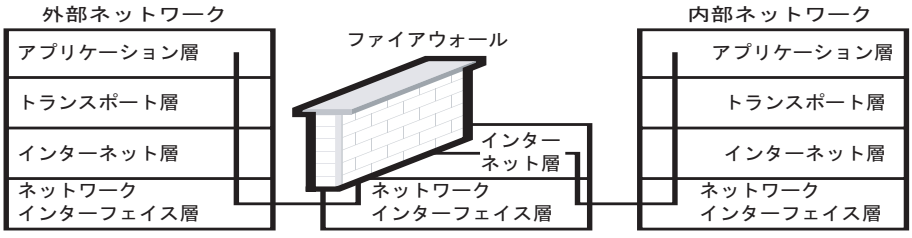

Fig. 7　パケットフィルタリング方式

から送られてきたデータを一時 Proxy サーバーでキャッシュしておきます．そして，以後このデータへのアクセスが要求された場合には，インターネットにアクセスするのではなく，Proxy サーバーにキャッシュされたデータを返すことで，WWW へのアクセスを高速化することができます．

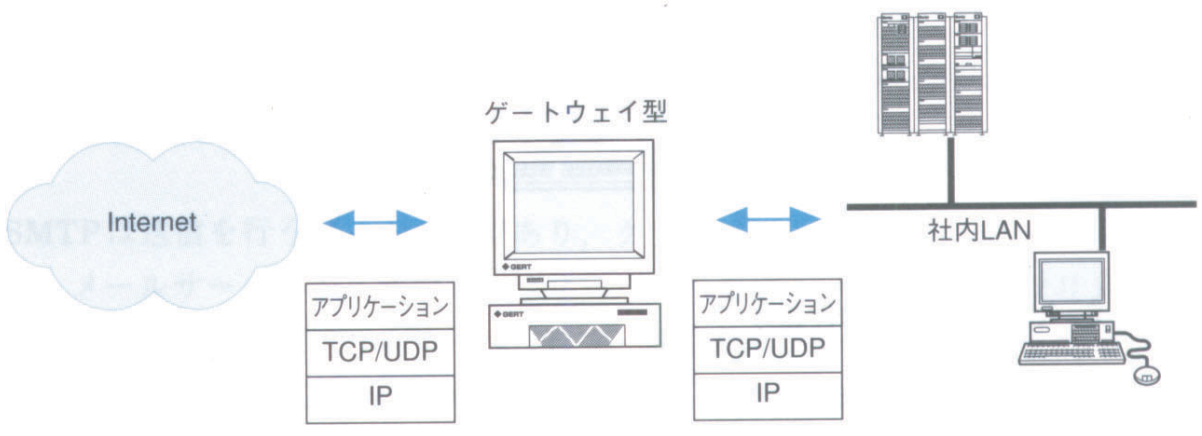

Fig. 8　コネクションフィルタリング方式

5.2.1　アプリケーションゲートウェイ方式

アプリケーションゲートウェイ方式は IP ルーターレベルでのパケットの出入りを禁止して，パケットを利用者のアプリケーションで処理し中継の制御を行う方式です．OSI 階層モデルでいうセッション層，プレゼンテーション層，アプリケーション層でサービスを中継します．それぞれのアプリケーションごとに中継処理を行うサーバを用意して，クライアントはこの代理サーバを通して目的のサーバに接続することになります．この方式はアプリケーション個別にゲートウェイのプログラムを用意する必要があるので複雑になりますが，データのキャッシングやレーティング，各アプリケーションに特化した高度な機能を盛り込みやすいという特徴を持ちます．

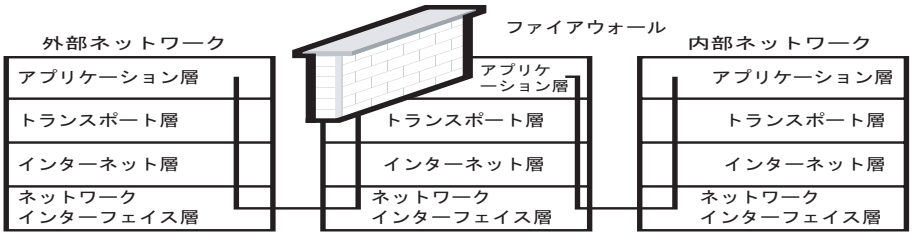

Fig. 9　アプリケーションゲートウェイ方式

5.2.2 サーキットレベルゲートウェイ方式

ソケットレベルで中継を行い，アプリケーションによらない Proxy 機能を実現した方式です．したがって，外部のパケットが内部に流れ込むリスクを根本的に回避できます．しかし，複数のアプリケーションプロトコルを 1 つの仕組みで中継するため，個々のアプリケーションプロトコルで決められたコマンドを細かくチェックすることはできません．この方式の代表的なものに SOCKS があります．SOCKS とは，アプリケーションプロトコルに依存せずに，トランスポートレイヤの上でアクセス制御を行なうためのプロトコルのことです．SOCKS を用いることで TELNET や FTP といった Proxy サーバーでは通すことが困難だったプロトコルに関しても融通が利くようになっています．

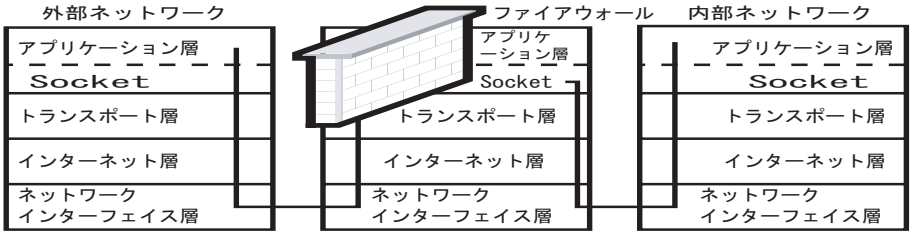

Fig. 10　サーキットレベルゲートウェイ方式

5.3 NAT(Network Address Translator)

インターネットに接続しない閉じられたネットワークの中でのみ利用される IP アドレスをプライベートアドレスと呼び，インターネット空間で一意的に割り当てられる IP アドレスを，グローバルアドレスといいます．

LAN 環境でインターネットに接続する際には内部で利用するプライベートアドレスはグローバルアドレスに変換して接続されるのですが，この時に，単純なパケットのフィルタリングとフォワードだけでなく，同時にアドレス変換やポート番号変換を行う必要があります．このプライベートアドレスとグローバルアドレスを変換する仕組みを NAT と呼びます．この NAT を利用することによりネットワークをプライベートアドレスで運用し，インターネットに接続が必要なときにだけプライベートアドレスをグローバルアドレスに変換することができます．つまり，内部で使用しているプライベートアドレスをインターネットから隠蔽することができ，直接アクセスされることがないようにセキュリティを高めることができます．

5.4 IP マスカレード

NAT による IP アドレスの変換だけでなく、その上位プロトコルである TCP ／ UDP のポート番号も識別することで、異なる通信ポートを利用するものについては、1 つのグローバル IP アドレスを利用して、複数のローカルノードが外部と通信できるようにしたソフトウェアのことです．

6 telnet とは

telnet はもともと TCP/IP 接続されたマシンにネットワークを介して別の計算機にログインしたり，遠隔地のマシンでコマンドを実行したり，他のマシンへファイルを移動するために作られました．離れた所にあるマシンを，まるで自分の前にあるかの様に操れます．ただし，ネットワーク経由でマシンにログインするときに telnet を利用すると，パスワードなどの情報が生のまま（暗号化されず，plain text のまま）で流れてしまいます．そのため，悪意のあるユーザが sniff[5]などのプログラムを用いて，パスワードなどを盗聴する危険性があります．

7 ssh とは

三木研究室では，ネットワークを介して別の計算機にログインしたり，遠隔地のマシンでコマンドを実行したり，他のマシンへファイルを移動するときに流れる通信内容を保護するのに ssh[6]という通信経路の安全化を図るツールを用いています．クライアント側では ssh を，ssh でアクセスされる側であるサーバでは sshd を用います．

ssh を使った通信ではパスワードだけではなく，やり取りされるデータも暗号化されるので，通信の途中で傍受される心配がありません．また暗号化されたデータは圧縮されて送られるので転送時間を節約することもできます．さら

[5]ftp,telnet,pop3 などパスワードを暗号化しないで送るプロトコルを盗聴してパスワードを収集するソフト
[6]security shell

に，暗号化には，認証機能を持つ暗号化方式である RSA を採用しているので，IP 偽装による攻撃を防ぐこともできます．ssh は以下に対して防御をおこないます．

- IP スプーフィング (偽装)
  リモートホストが，パケットを他の信頼できるマシンから来たかのように偽装するときに用います．ssh はローカルネットワーク上の偽装者があなたのルータの外から来たかのようになりすますことも防御します．
- IP ソースルーティング
  あるホストが，IP パケットを他の信頼できるホストから来たかのように偽装します．
- 途中にあるホスト上での平文パスワードの傍受
- 途中のホストを操作してのデータ操作 (改ざん)

7.1 SSL について

ssh では，暗号化に SSL[7]を用いています．安全な通信を実現する仕組みです．SSL では，公開鍵暗号（RSA）と秘密鍵暗号を併用しています．公開鍵暗号を使った暗号化・復号化には時間がかかるので，より高速な秘密鍵暗号の鍵を公開鍵暗号で渡すようにしています．SSL が提供するセキュリティ機能は，サーバー（必須）とクライアント（オプション）の認証，およびメッセージの機密性[8]と整合性[9]の保証により，暗号化された安全な通信環境を提供します．SSL 対応のブラウザには，

- Microsoft InternetExplorer（3.0 以降）
- Netscape Navigator（2.0 以降）

などがあります．

8 暗号化の強度

暗号の強度とは暗号化に使われる鍵の強度のことで，鍵のビット数が大きければ大きいほど，暗号化の強度が大きいということを表します．ただし，ビット数が大きすぎると，処理速度が遅くなり，それだけ通信路の危険にさらされる時間が多くなります．

ビット数には 56，64，128 などがありますが，近年，コンピュータの処理速度が増し，56，64 ビット程度では簡単に解かれてまう可能性が生じてきました．ここで，三木研究室では，128 ビット暗号化を推奨します．128 ビット暗号化は，クレジットカードや機密情報をインターネット上でやりとりする場合に，最高水準の安全性を与えてくれます．

暗号化の強度は，以下のようにして[10]確認することができます．まず，Fig. 11 のように，IE を起動させてヘルプのバージョン情報をクリックします．

すると，Fig. 12 の画面が表示されます．この場合，暗号強度が 56 ビットになっています．更新をクリックしてください．

9 Virus

コンピュータウイルス (以下ウイルス) は，悪質なプログラムの一種です．その動作が生物ウイルスに似ているため，ウイルスと呼ばれるようになりました．

9.1 ウイルスの概要

コンピュータウィルスは，通信ネットワークやフロッピーディスクを媒体として増殖，伝染し，貴重なプログラムやデータを消去，改ざんする等の不正な機能を持っている不正プログラムです．

一般に下記の行動パターンを持つ不正プログラムをウイルスといいます．

- 感染：他のファイルにウイルス自身を付着させる

[7]Secure Socket Layer
[8]第 3 者に情報が漏れない
[9]情報に一部でも破損しているところがない
[10]IE の場合

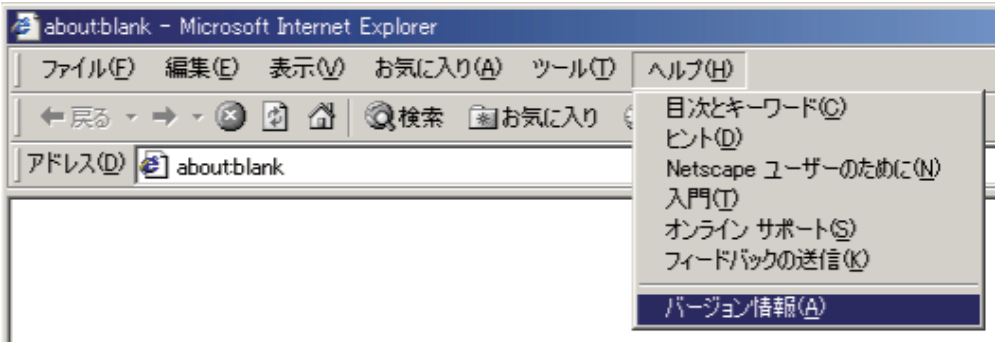

Fig. 11　IE の画面

Fig. 12　IE のバージョン

- 潜伏：一定の条件が揃うのを待って悪質な行動をする
- 発病：データの破壊，動作の不安定などユーザの意図しない行動をする

この他にも，以下のような不正プログラムがあります．

- トロイの木馬：ウイルスのような感染・増殖活動は行わないが，ユーザの個人情報やアカウントを盗んだり，ディスクのフォーマットやファイルの破壊を行います．
- ワーム：単独で自己増殖する不正プログラムで，ネットワーク環境を利用して感染するものをワームと呼びます．ウィルスが他のプログラムに寄生して感染増殖していくのに対し，ワームはそのような寄生対象（宿主）を必要とせず，自己の能力で「タスク間通信」などと呼ばれる技術を用いてネットワーク内を移動し，他のコンピュータに感染していきます．
- 爆弾：自己伝染機能はなく，発病のみを意図して作られたプログラムのことです．時限爆弾や論理爆弾のように潜伏機能を持つものもあります．

1. マクロウイルス
   アプリケーションソフトのデータファイルに含まれるマクロを利用して感染・発病します．マクロウイルスはウイルスであるマクロが添付されたデータファイルを開くと、マクロが自動的に実行され、初期実行ファイル (MS Word ではテンプレートファイル，MS-Excel ではマクロブックなど) にウイルス部分を複製保存するように作成されています．データファイルは，電子メールで添付ファイルとして送付できるため，極めて感染スピード，拡散力が強いウィルスです．

   マクロウイルスが発見される以前，コンピュータウイルスは文書ファイルなどのデータファイルには感染しない，またデータファイルからも感染しないと考えられていました．EXE ファイルや COM ファイルに感染するファイル感染型ウイルスを文書ファイルに感染するようにプログラムすることはもちろん可能ですが，一般的

には文書ファイルがウイルスによって破壊されることはあってもウイルスに感染することはありませんでした．これに対してマクロウイルスは文書ファイルから文書ファイルへと感染していくという特徴をもっています．また，マクロ機能はハードウェアや OS に依存しないため，同じアプリケーションソフトが動作していれば，どんな環境でも感染・発病します．

2. 従来のウイルス
   従来のウイルスには，以下の 3 種類のものがあります．

   (a) プログラムファイル感染型：プログラムファイルにウイルスを追加，又は上書きするものです．

   (b) ブートセクタ感染型：コンピュータが起動するときにディスクから最初に呼び込まれるプログラムがあるシステム領域に感染するものです．

   (c) 複合感染型：プログラムファイル感染型とブートセクタ感染型の両方の特徴を併せ持ちます．

   次に従来のウイルスとマクロウイルスの感染経路を比較します．ウイルスのうち，ブートセクタ感染型やファイル感染型，複合感染型ウイルスなど，マクロウイルス以前のウイルスの感染経路は，Fig.13 のように FD や CD-ROM などの外部媒体からのものと，ネットワークからのプログラムのダウンロードの際に PC に感染します．また，マクロ感染型ウイルスは Fig.14 のように FD や CD-ROM などの外部媒体からと MS-Word や MS-Excel データファイルを添付したメールやインターネットから MS-Word や MS-Excel のデータをダウンロードすることにより PC に感染します．

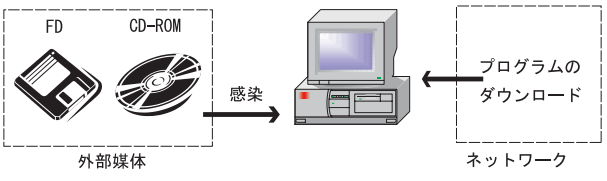

Fig. 13　従来のウイルスの感染経路

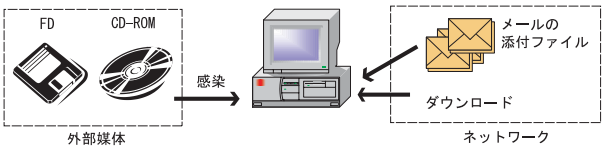

Fig. 14　マクロウイルスの感染経路

9.2　感染した場合の対処方法

ウイルスに感染した場合は、そのままシステムを使用し続けていると，感染拡大の恐れがありますので，速やかに下記を行うことが必要です．

1. システムをネットワークから切り離し，電源を落とす等の処置を行って，使用を中止する．
2. 安全なシステムディスクでシステムの再立ち上げを行い，感染したウイルスに合った適切な修復を行う．

なお，ウイルスの種類によっては，対処方法が異なりますので，必ずシステム管理者に連絡してその指示に従って，システムの復旧を行って下さい．

9.3　駆除方法

ウイルスを駆除するには、ワクチンを使用するのが一番簡単です．ワクチンを使わずに駆除する方法もありますが，詳しくは参考 URL を参照してください．

- ワクチン
  ワクチンには，ウイルス検出のための検査用のワクチンとウイルス除去用ワクチンとがあります．除去用ワクチンの利用は，ブートセクタ感染型ウイルスやファイルに上書きを行わないファイル感染型ウイルスの場合に，効果的です．　また，ウイルスが感染時や発病によってデータの書換え，削除等を行った場合は，ワクチンによってウイルスの除去をすることはできますが，元のデータを復元することはできませんので，当該ファイルの再インストールが必要になります．　ワクチンにはウイルスのコードをデータベース化して用意しておき，それと比較して検出するスキャン方式が一般的に多く見られます．他にも，ウイルスらしい動作と思われるコードを検知する方式 (ヒューリスティック検査方式) や実行可能ファイルが改変されていないかどうかを常時監視する方法 (チェックサム方式) などもあり、未知ウイルスの検出に使われています．

9.4 ウイルス対策の必要性

ウィルス感染により次のような被害を受けます.

- 企業の資産である蓄積されたデータがウィルスによって破壊される
- 感染後の復旧作業に多大な手間とコストがかかる
- 知らぬ間に，加害者になることがある

こうした被害を受けないために，ウィルス対策は必須のものです.

ウィルス侵入を防止，あるいは発見・駆除するために様々な技術が開発され，種々のウィルス対策ソフト（ワクチンソフト）が製品化されています．安全性の高い情報通信ネットワークを維持・運営するためにはウィルス対策ソフトの利用は必須です.

9.5 ウイルス対策の心構え

1. 最新のウイルス定義ファイルに更新しワクチンソフトを活用
   新種ウイルスに対応するために，最新のウイルス定義ファイルに更新したワクチンソフトで検査を行うことが肝要です．ウイルス定義ファイルの更新にあたっては，ワクチンベンダーの Web サイトを定期的にチェックするなどして，最新のバージョンを確認しておくことが重要です.
   また，プリインストールされているワクチンソフトは，機能が限定されている場合もあるので，製品版にアップグレードすることが重要です.

2. メールの添付ファイルは開く前にウイルス検査を行う
   添付ファイルが，テキストファイル，画像ファイル等であればワクチンで検査を行う必要はありませんが，Word, Excel のようなマクロ機能を持ったアプリケーションのファイル，または、実行形式のプログラムファイルであれば，必ずワクチンで検査を行ってから，ファイルを開いたり，実行するようにして下さい．なお，プログラムファイルの場合は、ワクチンでウイルスが発見されなくても，トロイの木馬のような不正なプログラムの可能性もありますので，差出人が不明の場合などのメールについては，添付ファイルごと速やかに削除されることをお勧めします．また，電子メールにファイルを添付するときは，ウイルス検査を行ってから添付します.

3. ダウンロードしたファイルは，使用する前にウイルス検査を行う
   インターネットからファイルをダウンロードした場合は，使用する前にウイルス検査を行います．また、ユーザに被害を与えるプログラム（国際電話やダイヤルQ２に接続するプログラムなどで，ワクチンソフトで発見できない可能性が高い）が潜んでいる場合があるので，信頼できないサイトからのファイルのダウンロードは避けましょう.

4. アプリケーションのセキュリティ機能を活用
   マイクロソフト社の Word や Excel のデータファイルを開くときに，マクロ機能の自動実行を無効にするなどのアプリケーションに搭載されているセキュリティ機能を活用します．また，メーラー，ブラウザのセキュリティレベルを適切 (中レベル以上) に設定しておくことにより，被害を未然に防ぐことができます．(ex. 電子メールの HTML 形式の本文に感染するウイルスがあります．マイクロソフト社の InternetExplorer ５のパッチをあて，セキュリティレベル設定を適切にすることで，このウイルスの自動実行は防止できます．電子メールのテキスト形式の本文に感染するウイルスは有りません．)

5. セキュリティパッチをあてる
   基本的なウイルス対策を行っていても，セキュリティホールのあるソフトウェアを使用していると，ウイルスに感染してしまうことがあります．例えば，電子メールの添付ファイルの自動実行を許してしまうメーラーのセキュリティホールは，ウイルス感染被害を著しく増大させる可能性があります．このようなセキュリティホールは，頻繁に発見されているので，使用しているソフトウェア (特に，メーラー，ブラウザ) に関してベンダーの Web サイトなどの情報を定期的に確認し，最新のセキュリティパッチをあてておくことが重要です.

6. ウイルス感染の兆候を見逃さない
   下記のような兆候を見逃さず，ウイルス感染の可能性が考えられる場合、ウイルス検査を行ってください.

- システムやアプリケーションが頻繁にハングアップする．システムが起動しない．
- ファイルが無くなる．見知らぬファイルが作成されている．
- タスクバーなどに妙なアイコンができる．
- いきなりインターネット接続をしようとする．
- ユーザの意図しないメール送信が行われる．
- 直感的にいつもと何かが違うと感じる．

7. ウイルス感染被害からの復旧のためデータのバックアップを行う ウイルスにより破壊されたデータは，ワクチンソフトで修復することはできない．ウイルス感染被害からの復旧のため，日頃からデータのバックアップをとる習慣をつけておく．また，アプリケーションプログラムのオリジナルＣＤ等は大切に保存しておく．万一，ウイルスによりハードディスクの内容が破壊された場合には，オリジナルから再インストールすることで復旧することができる．

9.6 Windows の設定

メールやチャット，Web 閲覧などインターネットのさまざまなサービスを利用しているとき，コンピュータは常にウイルスやトロイの木馬の脅威にさらされています．Windows では，ユーザの目的に合わせてコンピュータのセキュリティレベルが設定できます．ウイルスの脅威が高まっている今， インターネットを少しでも利用するのなら，デフォルトの設定のままでコンピュータを使うのは大変危険です．不注意によるウイルス拡散を少しでも減らすために，Windows のセキュリティレベルを高めに設定しておきましょう．ウイルスに対するセキュリティ強化のためには，以下の方法に従って Windows のシステムを設定することをおすすめします． よりセキュリティが強化されます．

- Windows Scripting Host（WSH）あるいは VBS の機能を無効にする
- すべての拡張子を表示させる
- Internet Explorer のセキュリティ設定を「中」以上に設定する
- メール添付ファイルはローカルディスクに保存しウイルスチェックをする
- マクロウイルス警告を有効にする（Office 97 ／ 2000 ユーザ向け）
- 標準テンプレート変更時に確認メッセージを表示させる（Word 97 ／ 98 ／ 2000 ユーザ向け）
- Microsoft Security Updates を適用する

ウイルスに感染したコンピュータは，上記のような症状が現れる場合があります．これらの中には，ハードウェアやソフトウェアのトラブルと見分けがつきにくいものがあります．ウイルスによるトラブルかどうかを見分けるためには，ウイルス対策ソフトを使用してコンピュータを調べてみるのが的確な方法です．

参考文献

1) ウィルスコンサルティングセンター http://www.vcon.dekyo.or.jp/index.html
2) アンチウイルス http://www.iosnet.ne.jp/anti-virus/
3) トレンドマイクロ http://inet.trendmicro.co.jp/virusinfo/index.asp
4) 情報処理振興事業協会セキュリティセンター (IPA ISEC) http://www.ipa.go.jp/security/antivirus/7kajonew.html

10 セキュリティホール

ソフトウエアのバグなどによって生じるセキュリティ上の問題点のことである．バグではなく，そのソフトウエアの標準設定が問題になるケースもある．セキュリティ・ホールは，第三者にサーバやネットワークへの不正アクセスを許す入り口になってしまう．世の中にあるほとんどのサーバ・プログラムは，過去に何らかのセキュリティ・ホールが見つかっている．特に OS など大規模で複雑なソフトウエアでは多くのセキュリティ・ホールが見つかっている．(多くのソフトは、新しい機能を次々と追加する傾向にあるため，プログラムがどんどん肥大化している．そうなると，限られた時間の中で巨大なプログラムを完全に見直し，不具合がないか確認することは事実上不可能である．こうした状況で，ソフトの開発時に開発者が予測できなかったセキュリティ上の不具合が，ソフトの公開後に多数のユーザーがさまざまな環境で使っていくうちに発見される.）基本的にセキュリティ・ホールは，ソフトウエア・ベンダーが提供するパッチと呼ばれる専用プログラムを適用して対処する．いくら堅牢なシステムでも，たった一つのセキュリティ・ホールを塞がなかったために不正アクセスを許してしまうということは十分あり得るため，ベンダーの提供するセキュリティ・パッチ情報には常に目を配る必要がある．

10.1 パッチとは

一旦完成したプログラムの一部を修正することである．また，修正を行なうために変更点 (差分情報) のみを抜き出して列挙したファイルを意味する.「パッチファイル」「差分ファイル」などとも呼ばれる．バグ (不具合) の修正や，小規模なバージョンアップなどを行なう際に，ソフトウェア全体を入れ替えるのは効率的でないため，修正点だけを抜き出してパッチ作成し，これを既存のソフトに組み込むことで修正を行う．多くはインターネットや CD-ROM などを通じて無償で配布される．なお，パッチを使って修正することを「パッチを当てる」と言う．例えば，ダンボール箱に穴があいていれば，箱の中にあるものが外に漏れたり，ひょっとしたら押入れのネズミが侵入して，中のものをかじって壊すかもしれない．そうならないためにもダンボールにガムテープを貼るなどして，応急処置をしたほうがよい．これと同じようにセキュリティホールの場合でも，応急処置として”セキュリティパッチ”と呼ばれるプログラムをあて，セキュリティホールをふさぐべきである．

10.2 パッチの入手方法

セキュリティホールは発見直後が最も危険である．不具合の内容が報告されるため，その情報をもとに悪意のあるユーザーが侵入することが可能になる．そうした侵入を回避するためには，できるだけ速やかにセキュリティパッチをあてるべきである．そのために，ユーザーの情報収集がカギになり，セキュリティホールの動向を知るためには，積極的にソフト開発者のホームページを訪れたり，ソフトのメーリングリストに加わるなどして，最新情報を収集する習慣をつけるべきである．セキュリティパッチをあてる作業自体は非常に簡単であるし，ダイヤルアップ環境でもダウンロードの負担はほとんどないので，日頃から自分が使っているソフトのセキュリティホールに関する情報が入手できるように準備しておくことが大切である． Windows や IE に対してセキュリティパッチをあてるには，Windows Update のホームページを利用するのが便利である．Windows Update のホームページにアクセスすると，自動的にユーザが利用している OS の種類や Web ブラウザのバージョンを判別して，ユーザ専用のページを表示してくれる．自分のパソコンにどんなソフトがインストールされ，どんなセキュリティパッチをあてるべきなのかが一覧表示されるうえ，チェックボックスをチェックするだけで簡単にセキュリティパッチをあてることができる．

ちなみに，マイクロソフト社製品のセキュリティホールについての情報は，ホームページの「TechNet Online」というコーナーで確認できる．ソフトごとに検索することも可能なので，自分が使っているソフトについてセキュリティパッチが公開されていないか定期的に確認するとよいだろう．また「マイクロソフト プロダクトセキュリティ 警告サービス」というセキュリティ問題についてのメールサービスもあり，日々セキュリティホールの情報や，セキュリティパッチの入手場所が報告されています．マイクロソフト製品のユーザーなら誰でも利用できるため，購読してみてはいかがでしょうか.

・Microsoft Windows Update
http://windowsupdate.microsoft.com/
・TechNet Online - Security
http://www.microsoft.com/japan/technet/security/
・マイクロソフト プロダクト セキュリティ 警告サービス 日本語版のご案内
http://www.microsoft.com/japan/technet/security/bulletin.asp

なお，セキュリティパッチはパソコンで何か他の作業をしているときではなく，時間に余裕があるときにあてるほうがよい．なぜなら，セキュリティパッチをあてた場合，プログラムの一部分が書き換わるため，別の不具合が発生することも考えられます．例えば，IE にセキュリティパッチをあてた場合，外部から IE の機能を利用するソフトが使えなくなったり，ソフトの挙動が変化するかもしれない．不測の自体が起こった場合に落ち着いて対処するためにも、セキュリティパッチをあてる場合は，事後の動作確認時間を見積もっておくべきであろう．