第 11 部

セキュリティ

第 1 章

はじめに

近年のワークステーションの低価格化、LAN 環境の広がりによって、Internet Protocol を用いた、LAN の相互接続による組織内のネットワーク環境の拡大や、WIDE に代表される広域ネットワークによる大規模ネットワーク環境が出現してきた。このような環境では、ファイル転送や仮想端末機能から、分散処理の概念に基づいたアプリケーションまで、幅広い利用が行われている。

しかしながら、このような環境をセキュリティの面から考察した場合、さまざまな問題点が指摘されている。ここでは、個々のネットワークが相互に接続され、一つの大きなネットワーク環境、いわゆるインタネット (Internet) 環境におけるセキュリティの問題を考察すると共に、WIDE プロジェクトにおけるセキュリティの取り扱いについて報告する。

第 2 章

インタネットにおけるセキュリティ

WIDE インタネットのような大規模ネットワークにおけるセキュリティ保全の問題は、参加組織がふえ、ネットワークが大きくなり、さらに利用目的が広がるにつれ重要な問題となってきている。インタネットにおけるセキュリティ上の脅威となる行動をいくつかあげる。

- **ネットワーク上にながれる情報の盗聴**
  インタネットでは、データ通信は複数の第 3 者の組織内のネットワーク機器を経由しておこなわれる。データ通信の経路内での盗聴を完全に防ぐことは容易ではない。また、Ethenet のようなバス型の LAN ではケーブルのタッピングは容易である。パーソナルコンピュータレベルのネットワーク接続機器の普及により、そのケーブル内のデータを盗聴することは比較的容易におこなうことができる。データのうちパスワードの盗聴は深刻な問題を含んでいる。

- **ネットワーク上にながれる情報の改ざん**
  ネットワーク上の情報を単に盗聴するだけでなく、内容を勝手に変更することも、簡単なプログラムを作成するだけで可能である。データの内容によってはネットワーク利用者に被害を与えたり、不当な利益を得ることが可能となる。

- **他ホストへのなりすまし**
  TCP/IP では、IP パケット上の発信元アドレスフィールド上の IP アドレスをもとに相手ホストを識別している。これは、IP パケットの発信元アドレスを適当につければ、その IP アドレスをもつホストになりすますことが可能である。

- **ホストへの不正なアクセス**
  ネットワークにつながっているホストやネットワーク資源を本来もっているアクセス権限を越えて不正にアクセスすること。

- **他ホスト、ネットワークへの不要メッセージ発信による運用妨害**
  不要なパケットを送ることによりネットワークやホストに異常な負荷をあたえることにより正常な運用を妨害することができる。

- **トラフィックの解析**
  実際のデータではなく、パケットがどこからどこへどれだけながれているかを調べるだけでも、有効な情報を得ることがある。

さらに、TCP/IP の技術的な脅威としてつぎのようなものがある。

- **ネットワーク制御情報の改ざん、不正発信**
  インタネットでは通信データとネットワーク制御用のデータが同一のネットワーク上をながれている。あやまったネットワーク制御情報をネットワーク上に流すだけで、ネットワーク運用管理を混乱させることができる。たとえば、誤ったルーティング情報を生成することで、ネットワーク運用を停止させることが可能である。

これらの問題を解決するには総合的な対策が必要である。

- セキュリティ保全に関する機能を利用する
- 運用ガイドラインや利用者教育などのネットワーク管理者/利用者のネットワーク技術の向上
- 契約や著作権といった法律による規制

その組織にとって不十分なセキュリティ方策はセキュリティ上の問題を引きおこす可能性があるし、逆に、必要以上のセキュリティ対策は、経済的/利便的な問題を引きおこす。ネットワーク管理者は、セキュリティ保全の具体的な作業をおこなう前に、その組織のセキュリティに関するポリシをまず決めなければならない。そして、組織内の各資源の機密性、重要性などを考慮して、それに見合っただけの具体的なセキュリティ対策をおこなう。セキュリティ対策と利便性は一般的にいって合い反するものであり、オープンポリシをもつ組織では簡単なセキュリティ対策をおこなえばよいし、そうでない場合は要求にあった十分なセキュリティ対策をおこなう必要がある。

2.1　ゲートウエイ

WIDE インタネットと参加組織とを接続するゲートウエイはセキュリティ保全上重要な役割を持っている。すなわち

- 参加組織内のホストの外部からのアクセス制限
- 必要なサービスのみ外部に対して提供する機能
- 通信の記録

などである。

2.1.1 ホストのアクセス制限

IP パケットレベルのアクセス制御は基本的なセキュリティ保全の手法として基本的なものである。外部からアクセスできるホストを制約することによって、そのホストに対してセキュリティ強化を重点的におこなうことができる。アクセス制御の方法として次のような方法がある。

1. **IP パケット転送機能をとめる**
   SUN や NEWS といったワークステーションを WIDE と参加組織ネットワークのゲートウェイとして利用している場合に有効な方法である。IP モジュールの IP パケット転送機能を止めることにより、外部からの IP パケットがこのゲートウエイ計算機を介して組織内のネットワークにながれることはない。逆に、組織内からのパケットが外部にながれることはない。このような状況では、組織内から直接組織外のネットワークをアクセスすることはできない。たとえば、ファイル転送の場合、一旦ゲートウエイ計算機にログインしてから、外部のホストにアクセスすることになる。

   このような接続をおこなうことにより、ゲートウエイ計算機のアカウントをもつユーザのみが組織内 (組織外) の資源をアクセスすることができる。

   この方法は、ゲートウェイマシンのアカウント管理をしっかりすればネットワークへの不当な侵入は十分避けられるが、インターネット上のアプリケーションを利用する際に不便な場合がある。分散ネットワーク本来の意味であまり美しい方法とは言えないだろう。また、もう一つの問題は、大きな組織になると、外部のネットワークにアクセスしたい組織内の個人アカウントを全てそのゲートウェイマシン上に持つ必要がある、ということである。

   この IP パケット転送機能をとめる方法は機種や OS のバージョンなどによって異なる。4.3BSD をベースとしたワークステーションでは、カーネル内の変数 _ipfowarding を 0 にすることにより、IP パケット転送機能が抑制される。これはコマンド adb を用いてカーネルに変更を加える。

```
# adb -w /vmunix
ipforwarding?D          <- 現在の値
_ipforwarding:
_ipforwarding:  1
ipforwarding?W 0        <- 値を 0 にする
_ipforwarding:  1       =       0
ipforwarding?D          <- 書換え後の値
_ipforwarding:
_ipforwarding:  0
$q
```

このあと、システムをリブートすることにより、システムはIP パケットの転送はおこなわれなくなる。この方法では、システムを再構成するときに改めて変更作業をおこなう必要がある。上記の方法を/vmunix ではなく/sys/OBJ/ip_input.o に施すことでシステム再構成されても IP パケット転送がおこなれない状態でシステムが構成される。また、システム立ち上げ時のスクリプト /etc/rc で

```
echo "_ipforwarding/W 0" | adb -k -w /vmunix /dev/mem
```

を実行する方法もある。これによりファイルを変更することなしに実行中のメモリイメージのみ変更が加えられる。

なお、機種によっては、カーネルが立ち上がる時にインタフェースが複数ついていると自動的にインクリメントするものもあるようなので注意が必要である。その場合は _ipforwarding の初期値を 0 でなく −1 にしておく必要がある。

2. **静的ホストルーティング制御**
接続可能なホストを制約する方法として静的ホストルーティング制御を用いる方法がある。通常ルータ間では、RIP 等のルーティング情報交換プロトコルを用いた動的なルーティング制御をおこなっている。この動的ルーティング機能をやめて、ルーティング情報を route コマンドによって静的にルーティング表に登録することにより、指定されたネットワークのみアクセス可能となる。ルーティング情報設定時にホストルートを指定することで、ホスト単位でのアクセス制御が可能である。

3. **アクセス制御機能**
ルータ専用機をゲートウェイとして利用している場合は、アクセス制御機能が有効である。この機能は、ゲートウエイ内を通過するパケットの送り先アドレス、発信元アドレスを調べて登録されているパターンと一致した場合は通過を許可 (または禁止) するというフイルタリング機能である。メーカーや機種によっては、アドレスの他にポート番号等でのフィルタリングが可能である。

以下にアクセス制御のテーブルの例を示す。

```
List of access control records:
    Internet source    Mask   Internet dest      Mask
    133.194.10.2     FFFFFFFF 0.0.0.0          00000000
    0.0.0.0          00000000 133.194.10.2     FFFFFFFF
    132.160.245.2    FFFFFFFF 0.0.0.0          00000000
    0.0.0.0          00000000 132.160.245.2    FFFFFFFF
    133.194.10.76    FFFFFFFF 0.0.0.0          00000000
    0.0.0.0          00000000 133.194.10.76    FFFFFFFF
```

上の例は、順に次の意味を持つ。

- ゲートウェイが持つ 133.194.10.2 の内部アドレスからゲートウェイマシン自身宛にきたパケットは通過を許可する。
- ゲートウェイマシン自身から 133.194.10.2 のアドレス宛は通過を許可する。
- 外部側のゲートウェイアドレス 132.160.245.2 からゲートウェイマシン自身宛にきたパケットは通過を許可する。
- ゲートウェイマシン自身から 132.160.254.2 のアドレス宛は通過を許可する。
- 内部のワークステーション 133.194.10.76 からゲートウェイ自身宛は通過を許可する。
- ゲートウェイマシン自身から内部のワークステーション 133.194.10.76 のアドレス宛は通過を許可する。

この例は簡単に言えば、内部ワークステーション 133.194.10.76 のみが直接外部のネットワークと通信可能となる。マスク値を指定することで、ネットワーク単位/サブネット単位の制御も可能である。

4. **ネームサーバ登録を行なわない**
   ネームサーバにホスト名の登録をおこなわないことにより、ネームサーバを利用している環境では、ホスト名を用いたネットワークアクセスはできなくなる。しかし、この場合 IP アドレスを指定すればアクセスは可能であり、本質的なセキュリティ対策にはなっていない。

2.1.2 必要なサービスのみ外部に対して提供

外部からアクセス可能な計算機や IP 転送機能をとめたゲートウエイ計算機上で外部利用者が利用できるサービスを限定したい場合がある。たとえば、外部の多くの利用者に公開する組織内計算機では、一般の外部利用者に対して一連ネットワークサービスの利用を禁止する必要がある。なぜなら、利用者はこの機能を使ってさらに組織内の計算機に対してアクセスを試みるかもしれないからである。そのためにはこのような機能を提供するコマンド (たとえば rlogin、rcp、rsh、telnet、ftp、netstat) の実行権を制約したり、実行形式ファイルを抹消することが考えられる。このようなコマンドを抹消しても、実行形式を外部よりファイル転送してアタックを試みることを防ぐことはできない。これを完全に防ぐためには UNIX カーネルの若干の改造を必要とする。

サービスを限定する別の方法として、利用者に対してログイン後シェル環境を与えるのではなく、限定された特殊なコマンド環境 (たとえば限定シェル) を提供することも考えられる。この場合もホスト管理者の要求にあった特別なソフトウエアの開発を必要とするかもしれない。

2.1.3　通信の記録

通信状況を示すログは、セキュリティ上の問題が発生したとき、状況を分析し対応策を検討する上で重要な情報となる。ログとしては、ログインやファイル転送といったアプリケーションレベルでのオペレーション情報がある。標準的な UNIX ワークステーションではアノニマス FTP の利用状況ログ、メールのログ、ログインのログなどがとれるようになっており、外部からアクセス可能なホストではこれらの機能を運用するとよい。

また、ルータの種類によっては課金機能を有効にすることにより、IP レベルでの通信状況 (どこからどこでどれだけのパケットが通過したか) が記録される。この情報は不正アクセスがあった場合の不正利用者を特定するときなどに有効である。

2.2　ローカルホストの対策

広域分散ネットワークはローカルネットワークの集合体として考えることができる。そのような見方をした場合、各ローカルネットワークでのセキュリティ対策は全体に及ぼす影響は少ないが重要である。また、前述のアクセスコントロールによる外部から/外部に対してアクセスできるホストを制限した場合でも、アクセス可能なホストのセキュリティ管理は重要である。

2.2.1　アカウントとパスワード

外部からアクセス可能なホストに対しては、必要以上のアカウントを作成しない、プロジェクトなどの共有するアカウントを作成しないなどの配慮が必要である。アカウント管理を正確におこなうことにより、ログ情報等で誰が何をしているかを把握することが可能となる。共用アカウントを防ぐためには、管理者の日頃の教育、指導が重要である。

また、パスワードは UNIX におけるセキュリテイ管理の要であり、その管理は重要である。管理者は、パスワードなしのユーザを禁止するとともに、パスワードに関するユーザの基本的な態度を教育し、ガイドライン等を作成することにより、頑丈なセキュリティを保持する必要がある。以下にあげる様なパスワードの選択は一般に避けるべきである。

- ログイン名に関連するパスワード。逆順にする、大文字化、繰り返し等。
- 自分の名前に関連するパスワード。
- 配偶者、子供の名前に関連するパスワード。
- 電話番号、自分の車の車種、住んでいる地名に関連するパスワード。
- すべて番号や同じ文字だけのパスワード。
- 辞書関係に載っている単語のパスワード。
- ６文字より少ないパスワード。

逆に、次にあげるパスワードの選択は奨励されている。

- 大文字、子文字の混合されたパスワード。
- 数字、句読点の混合されたパスワード。
- 覚え安いパスワード。
- 入力のタイピングが速いパスワード。

管理者はパスワードチェックのためのツールを定期的に動作させて、良くないパスワードがないことを調べる必要がある。UNIX の特権ユーザのパスワードは特に重要なパスワードとして、慎重に管理する必要がある。

2.2.2 その他

システムのセキュリティ状況をチェックするためのプログラムを定期的に起動する。例えば、`/etc/passwd`, `/etc/group`, `/.rhosts` のようなシステムにとって重要と思われるファイルを書き換えると、前日の設定との差分 (diff) がメールで報告されるような機構を準備しておくことで、システムの改変を管理者が容易に知ることができる。

第 3 章

利用者認証技術

ネットワーク環境でのある種のサービスでは、利用者が誰であるかによってサービスの適用範囲を制限したり、あるサービスを特定の利用者にのみに提供する場合がある。例えば、有料のデータベースサービスをネットワーク環境で提供することを考えた場合、利用料金を支払った利用者にアクセスを公開し、さらに、支払った料金に応じてアクセスできるデータを制限することが十分考えられる。このようなサービスを安全に運用するには、ネットワーク内での利用者認証と、各利用者に対して適正な利用許可を発行する機構が必要となる。

対象となるネットワークが小規模の場合 (例えば、単一の Ethernet セグメントから構成される環境) では、接続されているホストも少なく、その利用者も限定することができる。このため、単一組織によるホストの管理、アカウントやパスワードの管理などが可能である。したがって、利用者の認証はパスワードを用いた方法を利用でき、ファイルのモードの適切な設定によるリソースアクセスとプログラムの実行の制限、利用者名に基づいた利用許可の発行などを行うことでサービスの安全な運用が可能である。また、通信路での盗聴を防ぐための物理的なネットワークの保護も、規模が小さいことから可能である。

一方、広域ネットワーク環境では、ネットワーク自体の規模が大きく、複数の組織が接続され、その利用者数も膨大である。したがって、単一組織による統一的なアカウントやサービスの管理は現実的ではない。また、通信路の物理的な隔離などの方法によって、通信路での盗聴を防ぐことも非常に困難である。このため、広域ネットワークでの安全なサービスの運用を行うためには、従来の方法以外に何らかの通信路における情報の保護、利用者の識別方式と認証、さらに利用者に対しての適正な利用許可の発行の機能が必要である。

WIDE Project では、これらの機構の基礎となる利用者認証機構の開発を進めてきた [98]。ここでは、開発経過と今後の計画について述べる。

3.1 SPLICE/AS

これまで WIDE Project では、広域ネットワークにおける利用者認証機能を提供する SPLICE/AS[98] の開発を続けてきた。

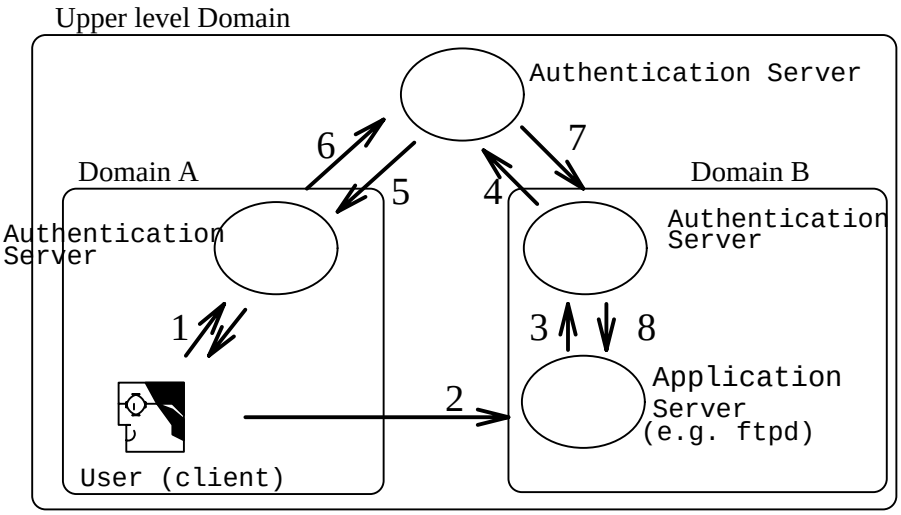

図 3.1: SPLICE/AS におけるドメイン間の認証

SPLICE/AS では、Needham 等によって提案された公開鍵暗号を用いた利用者認証プロトコル [99] を導入した。本システムでは、Needham 等によるプロトコルでは行なえなかった replay attack[100] の発見を、プロトコルを拡張することで可能とした。さらに、広域ネットワークでの運用のために、管理構造として階層的ドメイン構造を導入し、利用者認証のための新たなプロトコルを提案した。この手法では、各ドメインに認証サーバを配置し、各ドメイン内の利用者認証をローカルに行なう。さらに、異なるドメインのプロセスに対して認証を行なう場合は、ドメイン間での鍵の配送を階層的に行なうことで安全性を保証している (図 3.1)。

このような特色を持った SPLICE/AS を開発してきたが、次のような問題点が指摘されている。

暗号の性能: 現在の SPLICE/AS では、公開鍵暗号として RSA を用いているが、その実現はソフトウェアによって行われているため、暗号化、復号化の処理のオーバヘッドが非常に大きくなっており、NFS などの高速の処理が要求されるサービスには適用できない。この問題を解決するには、ハードウェアによる暗号器を実装するのが最も効果的であるが、ハードウェアの暗号器を実装しているホストは国内では稀であり、実現性が低い。このため、

- より処理が簡単な公開鍵暗号系を用いる。
- プロトコルを変更して慣用系暗号を用いたものにする。

等の改善が必要となってきた。

柔軟な運用:　SPLICE/AS では、ドメイン毎に認証サーバを配置している。これは、実際のネットワークの運用で、ドメインが利用者管理の最小単位と SPLICE/AS では仮定していることによる。また、SPLICE/AS でのドメイン構造は、名前サーバなどで扱うドメインと同様に、比較的固定的なものとしてとらえている。

しかしながら、実際の作業を考えてみると、動的に作業グループが構成され、その単位はドメインにはとらわれないものとなっている。このような動的に構成されるグループに対して利用者認証のサービスを提供する場合、安全性を考えると、そのグループで認証サーバを配置することが必要である。したがって、現在の SPLICE/AS がサポートしているドメインに基づいた管理構造では対応することが難しい。このため、新たな管理構造の導入が必要である。

認証サーバの二重化:　ネットワーク環境での認証サービスは、それが実装された場合には、どのようなサービスにも利用されると考えられる。このため、認証サーバが稼働しているホストがクラッシュしたことによってサービスが停止することはできる限り避けなければならない。

このような問題に対処するため、一般的にサーバの二重化が行われる。これは、ドメインに複数のサーバを配置し、一つをマスタサーバとし、残りをスレーブサーバとして運用をする。クライアントはこれらの内のどれかを選択し、サービスを受ける。そして、もしも利用中のサーバがクラッシュなどで使用できなくなった場合、自動的に他の利用可能なサーバに切替えるという方法である。

現在の SPLICE/AS では、サーバの二重化などの対策をとっていない。より柔軟な運用をするためにはサーバの二重化が必須である。しかしながら、この方法を認証サーバに適用するためには、各ユーザの暗号鍵データベースを、安全にマスタサーバからスレーブサーバに転送するプロトコルが必要である。このサーバの二重化の手法を検討している。

3.2　SPLICE/AS version 2

前節で述べたような問題点に対処するため、新たな利用者認証システム SPLICE/AS-2 の設計と開発を現在行っている。現状では、α リリースを、1991 年 8 月に予定している。

SPLICE/AS-2 では、次のような特徴を持つ。

- 使用する暗号系を、慣用系暗号の DES を用いる。
- 管理構造を固定的な階層構造とせず、より柔軟な構造を導入する。
- インタフェースとして、Kerberos と同様のインタフェースを用意し、既存のソフトウェアへの適用が簡単にできるようにする。

暗号系の変更

先に述べたように、SPLICE/AS で導入した RSA は、その処理のオーバヘッドが大きく、処理速度が問題となるアプリケーションには適用しにくいという問題点があった。そこで、SPLICE/AS-2 では、慣用系暗号の DES を導入する。これは、ソフトウェアによる実装でもオーバヘッドが小さく十分な性能が提供される。また、SPLICE/AS-2 では、簡単に別の慣用系暗号方式に適用できるような実装をしている。

管理構造の変更

SPLICE/AS では、階層的なドメイン構造を取り入れ、ドメインが一つの利用者認証サーバが管理する最小の単位としていた。SPLICE/AS-2 では、ドメインを自由に作成・消去できるような管理構造にし、先に述べた固定的なドメイン構造の問題点を解決する。このために、次のようなモデルを導入する。

- **ドメイン**
  ドメインは、単一の認証サーバがサービスを提供する範囲をあらわす。

- **コミュニティ**
  コミュニティーは、単一または複数のドメインから構成される、認証サーバのグループである。コミュニティー内で発生した、そのコミュニティーに属す利用者の認証は、確実に処理されることを保証する。各コミュニティーは固有の名前 (コミュニティ名) を持ち、識別される。また、各コミュニティーでは、ある特定のサーバ (リーダと呼ぶ) によって、属しているドメインが何であるかを管理する。これによってドメインを自由に作成したり、消去したりすることができる。

- **利用者**
  利用者は、認証サービスを受ける場合は、少なくとも一つ以上のコミュニティーに属さなければいけない。

このようなモデルに基づいて実装を行うことで、柔軟な管理構造を導入することを検討している。

Kerberos インタフェースの提供

MIT Athena Project によって開発された利用者認証システム Kerberos は、これまでに多くのシステムに導入され、数多くのネットワークアプリケーションに適用されている。このようなことから、SPLICE/AS-2 でも Kerberos が提供しているインタフェースと同じものを用意し、既存のアプリケーションへの適用が簡単に行えるようにする。

第 4 章

WIDE への接続形態: セキュリティと使い易さ

各組織のネットワーク (社内ネットワークや学内ネットワークなど) を WIDE に接続する場合、セキュリティと使い易さを考慮しなければならない。一般的に、使い易さとセキュリティの間にはトレードオフが存在し、使いやすさを優先するとセキュリティが弱くなる傾向がある。そこで、本章では、WIDE における幾つかの実際の接続形態を概観し、それぞれについて使い易さとセキュリティの強さについて比較を行う。

現在の WIDE との各組織のネットワークの相互接続は、次に示す 5 つの接続形態に分類することができる。

1. 完全分離型: WIDE と組織内ネットワークを物理的に分離する方式
2. RS-232-C 接続型: RS-232-C を使用して接続する方式
3. IP forwarding 禁止型: WIDE との gateway で IP パケットの forwarding を禁止する方式
4. 選択接続型: 登録された相手とだけ通信できるようにする方式
5. 完全接続型: IP で完全に接続する方式

また gateway として何を使用するかで、次の 2 種類が考えられる。

- 普通のワークステーションを gateway として使用する方法
- 専用の router を使用する方法

以下、これらについて説明する。なお、以下に示す図では、左側はワークステーションを gateway として使用した場合、右側は専用の router を使用した場合について示している。

4.1 完全分離型

完全分離型の接続形態を図 4.1に示す。この接続法においては、WIDE と各組織内ネットワークとを物理的に分離する。WIDE と組織内ネットワークとは物理的に分離されているため、組織内ネットワークに computer virus や worm が侵入する危険性がない。

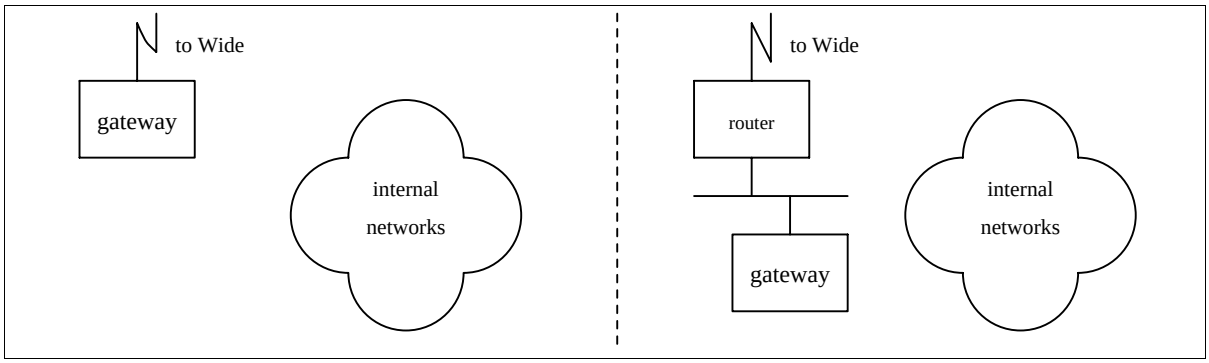

図 4.1: 完全分離型

しかしながら、WIDE にアクセスする場合は gateway machine の端末から gateway machine にログインしなければならないため、使い勝手は良くない。すなわち、自分宛のメールがあるかどうかをチェックしたり、メールを出したりする場合には、いちいち gateway machine の端末がある所まで行かなければならない。また、リモートサイトから ftp などで持ってきたファイルは、テープやフロッピィーディスクなどを使って off line で自分のホストに移す必要がある。

4.2 RS-232C 接続型

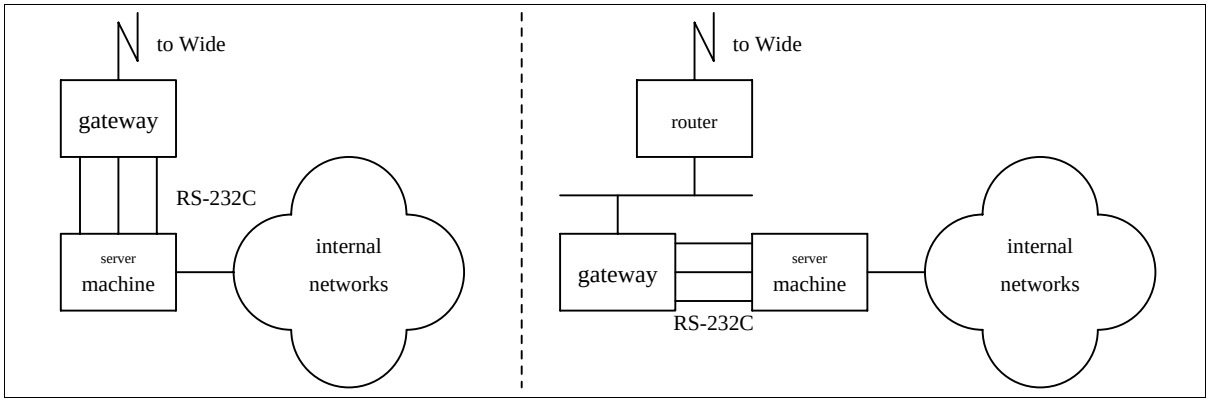

図 4.2: RS-232C 接続型

RS-232C 接続型の接続形態を図 4.2に示す。この接続法では、gateway machine と組織内ネットワーク内の server machine の tty ポート同士を RS-232-C で接続する。server machine 側の tty ポートに getty を走らせておかなければ、gateway machine から server machine にアクセスすることはできないので、組織内ネットワークに関するセキュリティは完全分離型と同様に問題が発生する危険性が無い。

また、各自のホストから WIDE 経由でメールを出す時は SMTP で server machine まで送り、server machine と gateway machine の間は RS232C 上の uucp で送るように設

定を行う。さらに、gateway machine から先は SMTP で送るようにセットすることで、WIDE とのメイル交換が実現できる。また、メールの受信の場合は、uucp の設定で server machine から gateway machine をポーリングするようにする。この方法では、uucp を使うためメイルの配送に多少の遅延が生じるが、server machine から gateway machine に対するポーリングを頻繁に行なうようにすれば遅延を軽減することが可能である。

この接続法では、WIDE 経由で外部のホストにアクセスできるのは gateway machine に限定される。したがって、組織内ネットワーク内のホストから WIDE 経由で外部のホストに ftp や telnet をする場合は、まず rlogin などのコマンドで server machine にログインし、そこからさらに tip などのコマンドで gataway machine にログインしなければならない。また、ftp などで gateway machine に持ってきたファイルを各自のホストに移すには、メールと同じように uucp で一度 server machine に転送するか、完全分離型と同様にテープやフロッピーディスクを用いなければならない。

一方、WIDE 経由で外部から組織内のホストにログインするためには、server machine の tty ポートに getty を走らせておかなくてはならない。この場合、外部から不正なユーザに侵入される危険性があるので、server machine のアカウントを厳重に管理しなければならない。

4.3　IP forwarding 禁止型

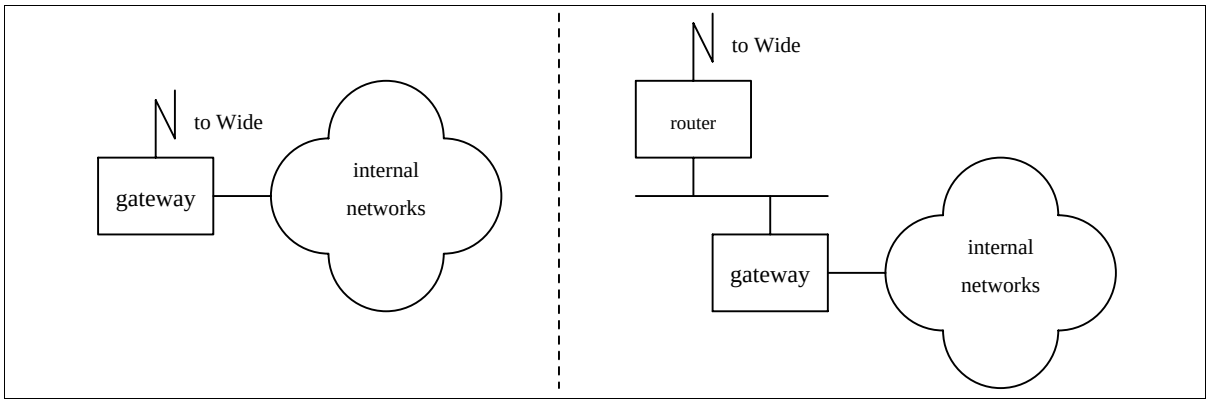

図 4.3: IP forwarding 禁止型

IP forwarding 禁止型の接続形態を図 4.3に示す。この接続法では WIDE と組織内ネットワークを、物理的には IP プロトコルで接続可能な構成をとるが、gateway machine において IP packet の forwarding を禁止することにより、論理的に gateway machine で WIDE と組織内ネットワークを切断する。これは、以下に示す方法で、gateway machine において IP packet の forwarding を禁止する。

- カーネルのソースがある場合は、netinet/ip_input.c で 1 と define されている IPFORWADING を 0 と define してカーネルを作り直す。

- カーネルのソースが無い場合は、adb により vmunix に直接パッチを当てる。パッチは、以下のように int 変数である ipforwarding を 0 とセットする。

```
# adb -w /vmunix
ipforwading?W 0
$q
#
```

これにより、IP レベルでは論理的にネットワークは分離されるが、gateway machine 上のデーモン・プロセス を経由して computer virus や worm が組織内ネットワーク内に入り込むの危険性は依然として存在しており、これを防止するために以下のような項目に注意する必要がある。

- 必要最小限のデーモンしか起動できないようにする。
- バグのあるデーモンなどにはきちんとパッチをあてる。
- 'guest' アカウントを抹消する。
- 各アカウントにきちんとパスワードをつける。

このような項目に注意し、ゲートウェイシステムについてログをきめ細かくとることで、ゲートウェイのセキュリティを保たなくてはならない。

組織内ネットワークから WIDE 経由でメールを出すときは、まず gateway machine へ SMTP で転送し、そこからさらに gateway machine が WIDE へ SMTP で転送するように設定する。メールの受信も同様に、行われる。このため、1 hop 分の遅延が増すだけでメールの送受信が可能である。

内部から外部のホストへ、または外部から内部のホストへ ftp や telnet を行なうには、まず telnet コマンドなどで gateway machine にログインし、そこから目的のホストへ ftp や telnet を行なう必要がある。しかし、ftp などで gateway machine に持ってきたファイルは rcp コマンドなどで各自のホストに持ってこられるので、使い勝手はかなり良いといえる。

4.4 選択接続型

選択接続型の接続形態を図 4.4に示す。この接続方法は、次に述べる完全接続型と物理的には同じ接続形態をとるが、完全接続型とは異なり、外部から組織内に入ってくるパケットについて gateway または router でいくつかの制限を設ける。この制限には以下のようなものがある。

1. 送信元の制限: 外部から組織内に入ってくるパケットについて、特定のホストまたはネットワークからのパケット以外はリレーしないようにする。

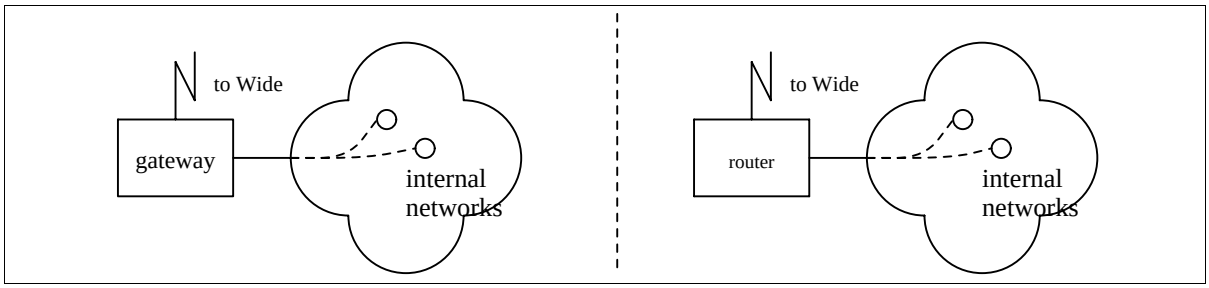

図 4.4: 選択接続型

2. 受信先の制限: 外部から組織内に入ってくるパケットについて、組織内の特定のホストまたはネットワークへのパケット以外はリレーしないようにする。

このような制限を行なうには、以下のような方法がある。

1. filtering: gateway あるいは router で、特定の source address または destination address を持つパケットのみを通過させるように filtering を行なう。この方法では、送信元の制限および受信先の制限のどちらにも適用可能である。

2. route control: gateway または router には、組織内のネットワークに関して特定のホストまたはネットワークに対する経路情報しか持たせないようにする。この方法は、受信先の制限には適用できるが、送信元の制限には適用できない。

送信元を制限した場合、組織内のすべてのホストは外部のホストに対してパケットを送信することが可能だが、gateway や router に登録された外部ホストからしかパケットの受信ができないため、事実上は登録された外部ホストとしか通信はできない。このため、任意のホストとの通信が必要な場合などには使い勝手が悪いといえる。また、セキュリティの面では、登録された外部ホストから virus や worm が組織内に入り込む可能性がある。したがって、各ホストに厳重なセキュリティが要求される。

一方、受信先を制限した場合、gateway や router に登録された組織内のホストのみが外部ネットワークにアクセス可能になる。この場合、組織内の他のホストからは、登録されたホストにまずログインして、それから外部のネットワークにアクセスすることになる。したがって、使い勝手は IP forwarding 禁止型と同レベルとなるが、IP forwarding 禁止型では、外部ネットワークにアクセスしたいユーザをすべて gateway で管理しなければならないのに対し、この方法ではいくつかのホストに分割して管理することができる。

セキュリティの面では登録された内部ホストが virus や worm に感染し、そこから組織内に広まる可能性があり、登録された内部ホストには厳重なセキュリティが要求さる。

4.5　完全接続型

完全接続型の接続形態を図 4.5に示す。この接続法では、WIDE との gateway または router を直接組織内ネットワークに接続する。この方法では全てのホストが IP で接続

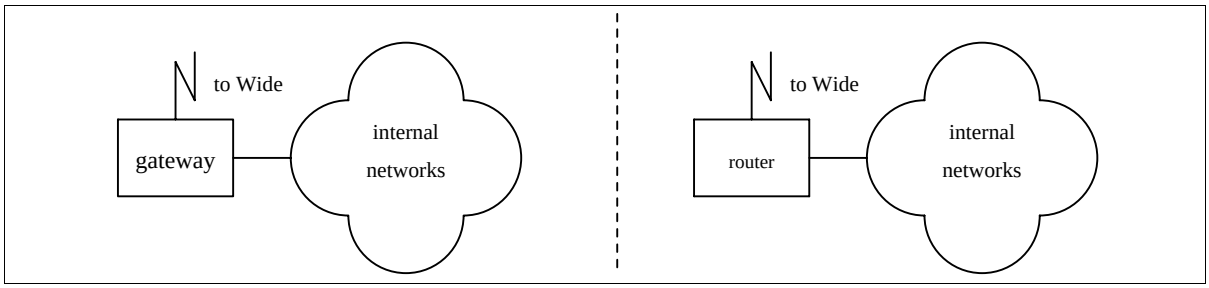

図 4.5: 完全接続型

されるため、各ホストが computer virus や worm の攻撃対象になりうる。したがって、各ホストに厳重なセキュリティが要求される。しかしながら、WIDE に対するアクセスは組織内ネットワークと同様に行なうことが可能である。