

土木研究所資料

ネットワーク管理に関する調査

平成8年3月

建設省土木研究所
積算技術研究センター システム課

Copyright © (1996) by P.W.R.I.

All rights reserved. No part of this book may be reproduced by any means, nor transmitted, nor translated into a machine language without the written permission of the Director General of P.W.R.I.

この報告書は、土木研究所長の承認を得て刊行したものである。したがって、本報告書の全部又は一部の転載、複製は、土木研究所長の文書による承認を得ずしてこれを行ってはならない。

ネットワーク管理に関する調査

システム課 研究員 平 城 正 隆
菊 池 克 男
小 野 祐 明
部外研究員 二階堂 尚 宏*

要 旨

建設省専用通信網（マイクロ回線）のデジタル化に伴い、各種情報通信システムのネットワークが従来にも増して推進されているが、これら情報通信システムを有効に機能させるためには、ネットワークの管理が重要である。

本論文では、インターネットの業務利用も含め、建設省におけるネットワーク構築手法及び管理手法について、調査結果を取りまとめたものである。

キーワード：インターネット、建設省専用通信網、ファイアウォール、セキュリティ対策、電子メール、ネットニュース、ファイル転送、WWW、ネットワーク負荷、ユーザー教育、建設省LANアドレス標準、グローバルアドレス、プライベートアドレス、ローカルアドレス、アドレス変換、機器管理、通信機器、ネットワーク機器、コンピュータ機器、障害管理、構成管理、性能管理、機密管理、管理情報、信号情報、SNMP、CMIP、管理専用通信回線、管理対象通信回線、電話回線、分散管理、一元管理、ユーザ管理、アカウント管理、電子メールアドレス管理、セキュリティ管理、パスワード、暗号化技術、DES、RSA、PEM、電子署名、公開鍵証明書、セキュリティ教育

* 部外研究員在職期間（平成7年4月～平成9年3月まで）

は じ め に

建設省においては、従来より河川情報システム、道路交通情報システムを整備・拡充し、各種事業の高度化・効率化を行ってきたが、LAN環境の浸透により、新たな電子計算機の利用として個人ベースの計算機としてのパソコンが普及し、新たなコンピュータの形態、いわゆるクライアント・サーバシステムが生まれつつある。

このクライアント・サーバシステムにおいては、新しいアーキテクチャや新しい概念のソフトウェアが矢継ぎ早に出現し、ユーザが個々の真価を見極める暇も無いほどである。

特に防災に係るシステムのように機能と処理能力を十分に吟味しないと社会資本全体を危うくすることになりかねない重要なシステムの担当者にとって、これらの新しいシステムをどのように捉え、維持管理を進めれば良いのかが大きな課題となっている。

この課題を解決する糸口として、調査では近年急激に普及しているインターネットも含めたネットワークについて、システム全体の最適な設計を念頭に置きつつ、有用性、経済性、信頼性、拡張性などの観点により検討した。

本報告書は、建設省において情報通信システムの構築を担当している方々を対象に、インターネットの業務利用の整理を行い、インターネットと専用通信網との接続手法を提案し、かつ機器管理、ユーザ管理及びセキュリティ管理におけるそれぞれの手法を取りまとめた。

目次

1.	概要	1
2.	インターネットの業務利用に関する調査	4
2. 1.	インターネット接続における危険性	4
2. 1. 1.	ローカルネットワークへの外部からの侵入	5
2. 1. 2.	インターネット上を流れる情報への介入	7
2. 2.	インターネット接続におけるセキュリティ対策	7
2. 2. 1.	ファイアウォール	7
2. 2. 2.	その他のセキュリティ対策	8
2. 3.	業務利用内容と課題	10
2. 3. 1.	電子メール	11
2. 3. 2.	ネットニュース	12
2. 3. 3.	ファイル転送	12
2. 3. 4.	電子掲示板 (WWW)	13
2. 4.	ネットワーク負荷に対する考慮	14
2. 5.	ユーザ教育	15
3.	建設省におけるインターネット接続手法	16
3. 1.	「建設省LANアドレス標準」の位置づけ	16
3. 1. 1.	アドレス管理の重要性	16
3. 1. 2.	アドレス体型の概要	17
3. 2.	グローバルアドレス取得の必要性	20
3. 2. 1.	グローバルアドレス	21
3. 2. 2.	プライベートアドレス	22
3. 2. 3.	ローカルアドレス	22
3. 2. 4.	独自アドレスの問題点	22
3. 3.	「建設省LANアドレス標準」を採用した インターネット接続手法	24
3. 3. 1.	「アドレス標準」とグローバルアドレスの 重複範囲	24
3. 3. 2.	アドレス変換手法の基本	25
3. 3. 3.	機器構成	26
3. 3. 4.	インターネット接続上の考慮点	27
4.	機器管理手法	30
4. 1.	管理対象機器の分類	30
4. 1. 1.	通信機器	30
4. 1. 2.	ネットワーク機器	31
4. 1. 3.	コンピュータ機器	31
4. 2.	管理項目の分類	32
4. 2. 1.	障害管理	32
4. 2. 2.	構成管理	34
4. 2. 3.	性能管理	35
4. 2. 4.	機密管理	36

4. 3	管理情報の収集方式	37
4. 3. 1	信号情報による収集方式	37
4. 3. 2	SNMPによる収集方式	38
4. 3. 3	CMIP方式	39
4. 4	管理情報の伝送方式	40
4. 4. 1	管理専用通信回線による管理情報伝送	41
4. 4. 2	管理対象通信回線による管理情報伝送	41
4. 4. 3	電話回線による管理情報伝送	42
4. 5	その他の機器管理手法	42
4. 5. 1	分散管理と一元管理	42
4. 5. 2	管理情報の表示方法	44
4. 5. 3	障害発生時の通報	44
4. 5. 4	障害発生時の管理体制	45
5.	ユーザ管理手法	47
5. 1	ユーザ管理の必要性	47
5. 2	アカウント管理	48
5. 3	電子メールアドレス管理	51
6.	セキュリティ管理手法	53
6. 1	ネットワークの危険性	53
6. 2	ネットワーク構成によるセキュリティ管理	54
6. 2. 1	ネットワーク階層化によるセキュリティ管理	54
6. 2. 2	ファイアウォールによるセキュリティ管理	56
6. 3	パスワードによるセキュリティ管理	61
6. 3. 1	パスワードの保護	61
6. 3. 2	パスワードの弱点	61
6. 4	暗号化技術によるセキュリティ管理	63
6. 4. 1	共通鍵方式 (DES)	64
6. 4. 2	公開鍵方式 (RSA)	65
6. 4. 3	共通鍵方式と公開鍵方式の併用方式 (PEM)	67
6. 4. 4	電子署名	68
6. 4. 5	公開鍵証明書	70
6. 5	セキュリティ教育	71
7.	今後の課題	73

1. 概 要

マイクロ回線のデジタル化に伴い、各種情報システムのネットワーク化が従来にも増して推進されているが、これらの情報通信システムを有効に機能させるためには、ネットワークの管理が必要不可欠である。すなわち、ネットワーク上のデータを適切に管理・監視したり、障害箇所の早期発見・切り離し等を行なうことにより、情報通信システムの機能を十分に発揮させることが可能となる。

本年度は、インターネットの業務利用に関する調査を行なうとともに、建設省専用通信網におけるネットワーク構築手法および管理手法の検討を行なった。

なお、建設省専用通信網において、ネットワークをインターネットに接続して業務を行なうことについては、セキュリティ・コスト・利便性等、各条件・因子を整理し決定されるものであり、検討を重ねるべきである。

今回は外部用ネットワークとして建設省専用ネットワークを利用した場合を想定したものであり、河川情報システム等の内部用にクローズされたネットワークについては想定していない。

(1) インターネットの業務利用に関する調査

インターネットは世界的なコンピュータネットワークであり、その利用例もさまざまである。インターネットのユーザは不特定多数であり、インターネット接続においては、その危険性とセキュリティ手法を調査し、必要なセキュリティ対策を施すことが重要である。

インターネットが全世界に広がっているという現実には、危険性を伴うものの、その利用効果が非常に高いと推測される。こうした意味からも、インターネット持続による外部との通信による業務利用だけでなく、インターネット手法を使用した建設省内部ネットワークにおける業務利用においても、数多くのメリットを享受できるものと期待できる。

ここでは、建設省専用通信回線を使用したネットワークとインターネットを接続することを念頭におき、インターネットの業務利用に関する次の項目について、調査内容を記述する。

- ① インターネット接続における危険性
- ② インターネット接続におけるセキュリティ対策
- ③ インターネットの業務利用内容と課題
- ④ ネットワーク負荷に対する考慮
- ⑤ ユーザ教育

(2) 建設省におけるインターネット接続手法

コンピュータネットワークおよびインターネットは急速に普及しており、建設省ネットワークにおいても省外への情報発信として、インターネット接続が検討されている。「建設省LANアドレス標準」を採用した建設省ネットワークは、IPアドレスとしてローカルアドレスを採用しており、そのままではインターネ

ット接続はできない。ここでは、「建設省LANアドレス標準」に基づき、建設省専用通信回線におけるネットワーク接続手法に関する次の項目について、調査内容を記述する。

- ① 「建設省LANアドレス標準」の位置づけ
- ② グローバルアドレス取得の必要性
- ③ 「建設省LANアドレス標準」を採用したインターネット接続手法

(3) 機器管理手法

コンピュータネットワークは、通信機器、ネットワーク機器、およびコンピュータなどの様々な機器で構成されている。これらの構成要素を適切に管理し、運用することは重要な位置づけにある。

ここでは、建設省専用通信回線における機器管理手法に関する次の項目について、調査内容を記述する。

- ① 管理対象機器の分類
- ② 管理項目の分類
- ③ 管理情報の収集方式
- ④ 管理情報の伝送方式
- ⑤ その他の機器管理手法

(4) ユーザ管理手法

ネットワーク管理としては、ユーザ管理も重要な管理方法の一つである。システム構成上で十分な機器管理を行なったとしても、肝心のユーザ毎のアカウントや電子メールアドレスの管理を行なわなければ、ネットワークの運用ができなくなることもある。

特にユーザ数が多く、人事異動などでユーザの職場が変わることの多い建設省のような全国的な大規模ネットワークでは、ユーザ管理を十分に検討してネットワーク構築を行なうことが重要となる。

ここでは、建設省専用通信回線におけるユーザ管理手法に関する次の項目について、調査内容を記述する。

- ① ユーザ管理の必要性
- ② アカウント管理
- ③ 電子メールアドレス管理

(5) セキュリティ管理手法

ネットワークが限られた部門内だけの範囲で構築されている間は、セキュリティ管理は、それほど重要視されていなかった。しかし、インターネット接続による商用利用が盛んになるに連れて、セキュリティ管理は必要不可欠となり始めている。ネットワークでコンピュータ同士を接続することは非常に便利な反面、予期せぬ第三者からの侵入の危険性が高いことになる。こうした侵略行為に対して、セキュリティを強化することは重要である。ここでは、建設省専用通信回線における、セキュリティ管理手法に関する次の項目について、調査内容を記述する。

- ① ネットワークの危険性

- ② ネットワーク構成によるセキュリティ管理
- ③ パスワードによるセキュリティ管理
- ④ 暗号化技術によるセキュリティ管理
- ⑤ セキュリティ教育

2. インターネットの業務利用に関する調査

インターネットと接続するには、通信プロトコルとしてIPプロトコルを使用する。インターネット接続するコンピュータが世界標準の通信プロトコルを使うことによって、全世界での相互通信が可能となる。

今日の代表的なアプリケーション・ソフトウェア／共通アクセス手順名および通信プロトコルとインターネットの関係を図 2.1 に示す。

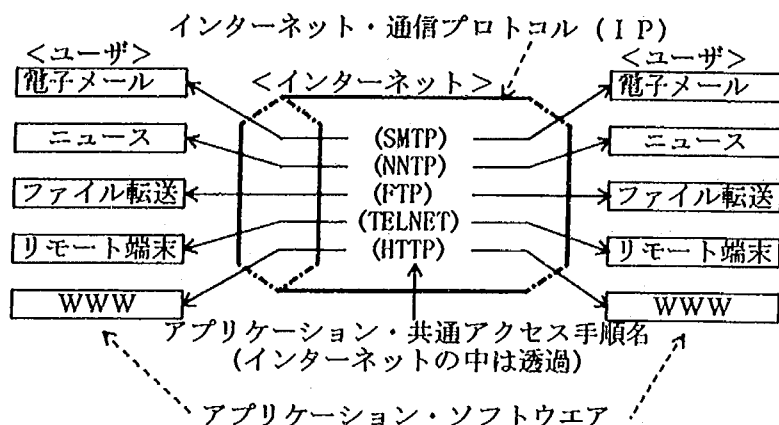


図 2. 1 インターネット接続プロトコル

インターネット接続においては、接続したコンピュータのアドレスが公開され、かつ、アクセス手順が統一されているため、だれでも簡単に使用できる反面、セキュリティには比較的弱い性質がある。インターネット接続には危険が伴うが、その危険を正しく理解してセキュリティ対策を行えば、そのメリットは十分に大きい。

2. 1 インターネット接続における危険性

一般にインターネットにつなぐ場合の脅威は、次の2種類に分類される。また、その概念を図2. 1. 1に示す。

(1) ローカルネットワークへの外部からの侵入

外部ネットワークからローカルネットワークへ侵入されることにより、機密情報やプライバシー情報などの内部情報を盗まれたり（閲覧）、情報操作されたり（改ざん）、消滅されたり（破壊）、さらにはシステムを動作不能にされたり（妨害）する可能性がある。

これらの脅威に対しては、ファイアウォール「防火壁」で対応することができる。

(2) インターネット上を流れる情報への介入

インターネット上を流れる情報を盗まれたり（盗聴）、情報操作されたり（改ざん）する可能性がある。これらの脅威に対しては、暗号化技術などで対応することができる。

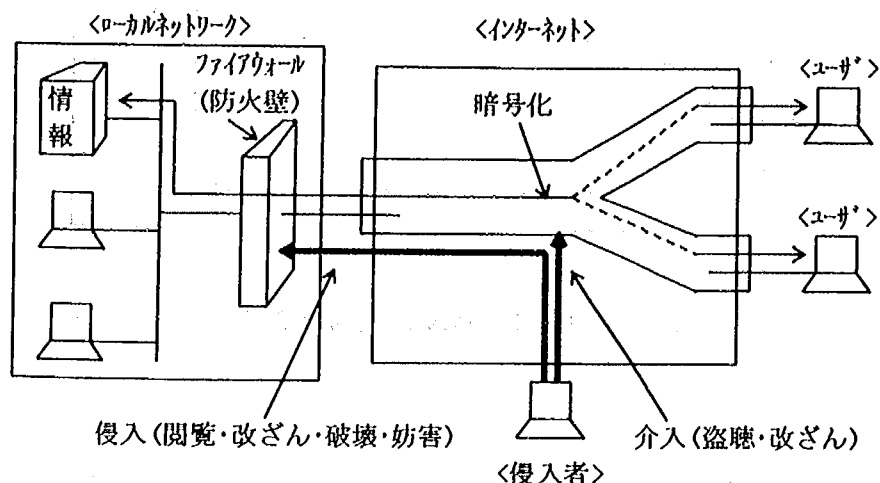


図 2. 1. 1 インターネット接続の脅威

2. 1. 1 ローカルネットワークへの外部からの侵入

一般的にローカルネットワーク内にあるサーバに、TelnetやFTPで情報にアクセスする場合は、ユーザIDやパスワードを使用してユーザの認証を行う。この情報が一般に知れてしまうと、重要な情報が誰にでもアクセスできることになる。

(1) パスワードの不正入手

最近問題になっている「ネットワーク・モニタリング・アタック」の例で説明する。

侵入者はTFTP (trivialFTP) やNIS (network information system) のプロトコルを利用して、ローカルネットワーク内のパスワード・ファイル (/etc/passwd) を盗みだし、ユーザのアカウント (利用権) を不正利用する。いずれもパスワードを取得されやすいプロトコルである。

その後、セキュリティ・ホール (OSのバグや運用上のセキュリティの穴) を利用して特権ユーザの権利 (root特権) を獲得し、各種の情報を不正入手することが可能となる。すでに存在する情報の入手ばかりでなく、他のサーバへの侵入も可能となる。

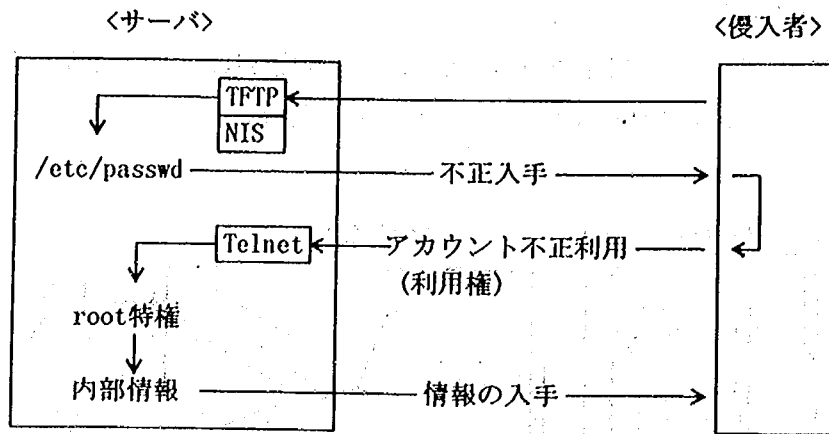


図 2. 1. 1. 1 パスワード不正入手

(2) 情報への侵入

パスワードの不正入手によるサーバへのアクセスが可能となれば、次の操作は簡単に行うことができる。

① 閲覧

機密情報やプライバシー情報を不正入手することができる。この情報の利用のされかたによっては、その影響度は計り知れない。

② 改ざん

情報の意味を知っている侵入者は、特定の情報を改ざんすることで、通常利用者への混乱や不利益を与えることができる。

③ 破壊

情報の破壊は、通常利用者に混乱を与えるばかりでなく、情報の再構築には大きな手間とコストが発生する。

(3) システムへの妨害

ローカルネットワークの安定稼働を妨害する侵入者もある。

① 過負荷状態

電子メールを大量に送りつけると、サーバが過負荷状態となり、通常動作が行えなくなる事態が発生する。また、サーバ内のメモリ不足が発生し、システムダウンにつながることもある。

本ケースは、パスワードの不正入手が無くても可能である。

② システムダウン

コンピュータ・ウイルスを持つプログラムを送りつけ、無制限に増殖したり、システムプログラムを破壊したりして、システムダウンに追い込むことができる。

2. 1. 2 インターネット上を流れる情報への介入

インターネット上を流れる情報への介入としては、情報の流れを止めることなく、かつ利用者に気づかれないように行われることになる。一般的には、情報の盗聴と改ざんが可能となる。

インターネット・バックボーンは、ルータなどのネットワーク機器で構成され、インターネット事業者が管理している。一般企業と比べて、インターネット事業者の侵入対策は比較的しっかりしているといわれている。しかしながら、現実にはインターネット・バックボーンへの介入例も報告されており、万全とは言えない。重要な情報を大量に交換する場合は、インターネット事業者の信頼度も調査したほうが良いとも言われている。

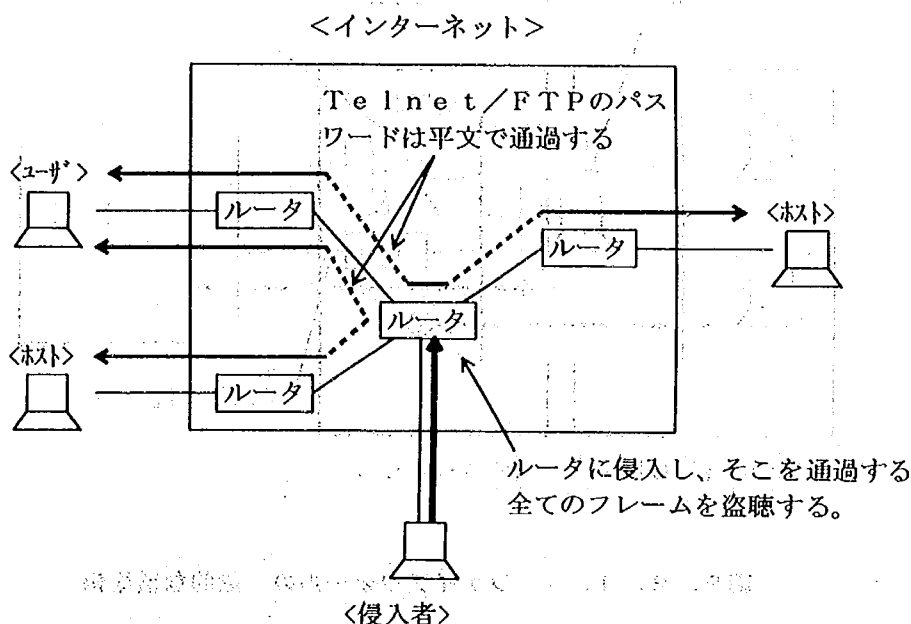


図 2. 1. 2. 1 インターネットへの介入

2. 2 インターネット接続におけるセキュリティ対策

2. 2. 1 ファイアウォール

インターネットと IP 接続する場合、外部からローカルネットワークへの侵入を防ぐためのセキュリティ対策を、ファイアウォール「防火壁」と呼ぶ。

ファイアウォールは、外部からの不正アクセスを防ぐとともに、ローカルユーザに対しては利用できるアプリケーションを制限する役割がある。

ファイアウォール構築の基本は、ローカルネットワークへの入り口を一つにすることである。入り口を一つにすることで効率的にアクセス制限することが可能となる。

さらに、ファイアウォールの外側（インターネット側）に、外部からアクセスできるセグメント（バリア・セグメント）を設ける。バリアセグメントには、外部に公開するためのWWWサーバやFTPサーバを置くこともできる。

ファイアウォールの一般的な構築例を図2. 2. 1. 1に示す。詳細については、「6. 2. 2 ファイアウォールによるセキュリティ管理」を参照のこと。

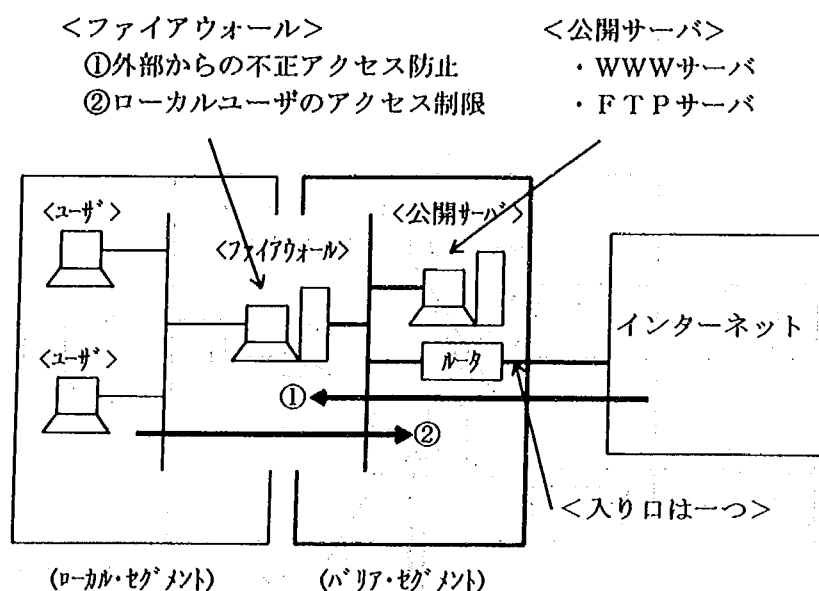


図2. 2. 1. 1 ファイアウォールの一般的な構築例

2. 2. 2 その他のセキュリティ対策

インターネット接続における危険性およびファイアウォールによるセキュリティ対策について述べてきたが、その他にもセキュリティ強化の対策が必要である。

(1) 利用アプリケーションの制約

インターネットはTCP/IPプロトコルで接続されるコンピュータ・ネットワークであり、TCP/IP上のアプリケーションは基本的には全て利用可能である。

しかしながら、インターネット接続における危険性を考慮すると、全てのアプリケーションを利用するのではなく、次の条件で利用アプリケーションを選択することが望ましい。

① 危険性の少ないアプリケーション

盗聴、改ざん、破壊などの情報への侵入は、外部からのコンピュータ内部への侵入により発生する。

コンピュータへの侵入可能なアプリケーションとしては、

1) ファイル転送 : F T P (File Transfer Protocol)

2) 簡易ファイル転送 : T F T P (Trivial FTP)

3) リモート端末 : T e l n e t

などがあり、上記アプリケーションを利用したインターネットとの直接接続は避けるべきである。利用する場合は、外部へのアクセスは許可するが、外部からのアクセスは禁止するような対策を施す必要がある。

② 利用効果の高いアプリケーション

業務利用において利用効果の高いアプリケーションを選択することが望ましい。利用効果が高いという意味では、次の条件などを満たすことが必要である。

- ・多くのユーザと情報交換ができる
- ・インターネット上から短時間で情報収集ができる
- ・インターネット上へ情報公開ができる
- ・業務改善ができる

これらを満たすアプリケーションには、以下のものが考えられる。

1) 電子メール : S M T P

2) ネットニュース : N N T P

3) ファイル転送 : F T P

4) 電子掲示板 (WWW) : H T T P

③ ゲートウェイ方式ファイアウォールが可能なアプリケーション

現時点で、ゲートウェイ式ファイアウォールとして利用可能なアプリケーション・プロトコルには、以下の種類がある。

1) F T P (File Transfer Protocol) : ファイル転送

2) T e l n e t : リモート端末

3) H T T P (HyperText Transfer Protocol) : 電子掲示板WWW

4) G o p h e r : 情報検索

5) S M T P (Simple Mail Transfer Protocol) : 電子メール

6) N N T P (Network News Transfer Protocol) : ネットニュース

(2) 利用者の制約

インターネット接続による業務利用では、次の観点から利用者の制約が必要である。

① セキュリティ対策

ユーザが多いほどパスワードの漏洩や重要情報の漏洩などの事故発生確率が高くなり、セキュリティが甘くなる。

この観点から、強固なセキュリティ対策と、十分なユーザ教育が可能な範囲に利用者数を限定することが望ましい。

② ファイアウォールへの負荷集中対策

アプリケーション・ゲートウェイ型ファイアウォールでは、アクセスするユーザ毎に中継プロセスが生成されるため、同時ユーザ数が増えると急激にレスポンスが低下することがある。

この観点から、ユーザを制限したり、利用可能な端末を制限したりすることが望ましい。

③ ネットワーク負荷増大への対策

自営ネットワーク（WAN構成）において、通常業務用のネットワーク負荷の他に、インターネット接続用負荷が増加することになり、ネットワーク全体のパフォーマンスが低下することが考えられる。

④ 業務利用限定対策

私用利用や業務とは無関係の利用などは、避けなければならない。この対策としては、ユーザ教育（倫理）の徹底が必要となる。

(3) 利用場所の制約

利用場所に関する制約は特には無いと思われる。

ただし、セキュリティの観点からは、外部ユーザが自由に立ち入れるオープンな場所での利用は避けるべきである。

(4) 外部からのアクセス制約

自宅や出張先から、公衆回線経由で内部ネットワークと接続する構成では、接続時のセキュリティ対策やパスワード漏洩対策など、十分なセキュリティ対策と教育が必要となる。

2. 3 業務利用内容と課題

インターネット接続による業務利用形態としては、インターネットと接続して外部と通信するだけでなく、同一のアプリケーションを使用して自営ネットワーク内部で通信する業務利用形態も重要な利用方法である。

上記を踏まえて、業務利用内容と、検討すべき課題を以下に記述する。

2. 3. 1 電子メール

電子メール自体は、電話や郵便の代わりに使用できる便利なアプリケーションとして、広く利用されている。一般的な業務利用としては、次の利用方法が可能である。

- ・業務上の連絡、報告
- ・会議開催通知、資料の事前配布、議事録の配布
- ・電子会議
- ・個人利用
- ・その他の利用

電子メールは便利ではあるが、次の検討すべき課題が存在する。

(1) メールサーバの配置、容量などのシステム設計

大規模ユーザのメールシステムを構築するには、メールサーバの配置、サーバ容量、ユーザ数、および回線速度を含めたメールシステムの設計が重要である。

(2) メール使用可能ユーザの検討

業務利用する場合は、業務の対象となる全ユーザがメール利用可能な環境でなければ効果が薄くなり、メール送信、郵送、電話などの複合管理が必要となる。

メール利用可能なユーザを計画的に選択し、整備状況に合わせて業務利用することが必要となる。

(3) メール送信データ内容に対する考慮

重要な情報やプライバシーに関する情報は漏洩の可能性があるためメール送信してはならない。これはユーザ教育の課題とも言える。

(4) メール送信データ量に対する考慮

メール送信するデータ量には、ある程度の制限が必要である。大量のデータを送信すると、通信回線を占有することにもなるし、メールサーバのディスク容量を圧迫することにもなり、他のユーザに与える影響が大きい。

(5) 送信誤りに対する考慮

メール送信時の宛先を1文字間違えると、全く違うユーザにメールが届く可能性が高い。

このようなミスを犯しにくいメールシステムの運用方法を考慮する必要がある。たとえば、メール送信時の宛先選択には、共有データベースから日本語で確認して選択するなどの工夫が必要である。

2. 3. 2 ネットニュース

ネットニュースは電子会議室の機能であり、通常は世界のニュースグループからの最新の話題を読むことができる。業務利用としては、インターネットからニュースを読むというよりも、自営ネットワーク内部ユーザにおける電子掲示板や電子会議室としての利用が有効となる。一般的な業務利用としては、次の利用方法が可能である。

- ・ 事務情報の掲示
- ・ 各種イベント情報の掲示
- ・ 最新技術情報、動向の問い合わせ
- ・ 有形、無形の探し物の問い合わせ
- ・ その他の利用

ネットニュースを業務利用するに当たって、次の検討すべき課題がある。

(1) ニュースサーバの配置、容量などのシステム設計

大規模ユーザのニュースシステムを構築するには、ニュースサーバの配置、サーバ容量などのニュースシステムの設計が重要である。

(2) ニュースサーバ管理の検討

ニュースサーバ上の情報は、ある程度の情報保持期間を設けて、定期的に削除するなどの管理が必要となる。

また、業務に合わせたトップ・ニュース・グループや階層構造などを決めなければならない。

(3) リアルタイム性が無いという前提での利用

ニュースはニュースサーバ上に掲示されるだけであり、ユーザがニュースを見るタイミングは不明である。したがって、緊急性のある情報はニュースだけにたよることはできない。

(4) だれでも読むことができるという前提での利用

ニュースはだれでも読むことができるため、特定の個人に対する連絡や、公序良俗に反する内容は掲示してはならない。ユーザ教育の徹底が必要である。

2. 3. 3 ファイル転送

ファイル転送はファイルサーバから各種情報を収集する機能であり、ファイルサーバに蓄積されている企業や研究所の公開情報ファイル（科学技術情報やプログラムなど）を短時間で収集することができる。

業務利用としては、インターネット上のファイルサーバから世界の科学技術情報（バックナンバーも含め

て)を収集すること、および、自営ネットワーク内部の情報を公開して、技術情報の共有化を図ることが可能である。一般的な業務利用としては、次の利用方法が可能である。

- ・技術情報のインターネット上からの収集
- ・内部の共有技術情報の公開
- ・内部各種標準規格、標準仕様の公開
- ・標準書式の共有化(最新性の確保)
- ・大量データ転送用のテンポラリファイル
- ・その他の利用

ファイル転送を業務利用するに当たって、次の検討すべき課題がある。

(1) ファイルサーバの配置、容量などのシステム設計

大規模ユーザのファイルサーバ・システムを構築するには、ファイルサーバの配置、サーバ容量などのファイルサーバ・システムの設計が重要である。

(2) ファイルサーバ管理の検討

ファイルサーバ上の情報は、ある程度の情報保持期間を設けて、定期的に削除するなどの管理が必要となる。

また、業務に合わせたディレクトリ構造などを決めて使いやすくしなければならない。

(3) セキュリティの確保

自営ネットワーク内部の使用といえども、重要な情報にはアクセス制限を行う必要がある。個人利用のディレクトリや共有ディレクトリなどの区分を設け、ある程度のセキュリティを確保しなければならない。

2. 3. 4 電子掲示板(WWW)

電子掲示板(WWW)はグラフィックデータを中心とした情報公開が可能であり、全世界に向けて発信することができる。WWWは自営ネットワーク内部での利用も可能だが、どちらかといえば、インターネット上のユーザに向けた情報発信が主な利用方法となる。一般的な業務利用としては次の利用方法が可能である。

- ・業務内容の紹介
- ・地域ガイドの公開サービス
- ・各種窓口案内サービス
- ・各種調査統計資料の公開サービス
- ・各種行政資料の公開サービス
- ・要望受付サービス
- ・その他のサービス

WWWを業務利用するに当たって、次の検討すべき課題がある。

(1) WWWサーバの配置、容量などのシステム設計

WWWサーバ・システムを構築するには、WWWサーバの配置、サーバ容量、ファイアウォールなどのWWWサーバ・システムの設計が重要である。

(2) WWWサーバ管理の検討

WWWサーバ上に情報を公開するためには、情報作成システムおよび情報作成要員などの確保が必要となる。

また、定期的に内容を見直し、最新性を保持しなければならない。

(3) 公正なサービスへの考慮

公共団体の情報サービスの場合は、ある特定のユーザに有利になるようなサービスとならないような配慮が必要である。

電子サービスは、時間、距離、地理などの条件を乗り越えて画一的なサービスが可能となるが、その他の手段におけるサービスとの公正さも必要である。

2. 4 ネットワーク負荷に対する考慮

オンライン・リアルタイム情報処理用ネットワークと、業務利用ネットワークが考えられ、これらを同一に扱うにはネットワーク負荷の相互影響を考慮したネットワーク設計を行わなければならない。

情報処理用データも業務利用データも、最終的にはユーザのパソコン上から同じような操作感覚で扱えれば、情報収集の一元化や状況分析の時間短縮などの、一種の業務改善につながるとも考えられる。

ネットワーク負荷に対しては、次の検討課題がある。

(1) 情報の性質、情報量などの把握

情報特性、情報量、回線速度、情報収集時間などの要素を組み合わせた検討が必要である。

また、マルチメディア情報の取り込みも考慮しなければならない。

(2) 情報処理用ネットワークの検討

オンライン・リアルタイム処理が必要な情報収集系ネットワークと、クライアント／サーバ型でユーザがアクセスする情報サービス系ネットワークなどに分けて考えることも必要である。

これが可能であれば、業務利用ネットワークとの融合検討も比較的容易となる。

(3) 業務利用ネットワークの検討

情報サービス系データや、インターネット利用を含む業務利用データは、マルチメディア化も含めて高速化、大容量化、高精細化が進むと考えられる。

このような見込みに対して、バックボーンLANや通信回線の選択をどうするかについての検討が必要となる。

2.5 ユーザ教育

インターネット接続を使用した業務利用を進展するには、直接的な利用者であるユーザ教育が重要な位置づけにある。

一般的にユーザ教育に必要とおもわれる課題を以下に示す。

(1) 操作方法教育

全てのユーザが問題なくインターネットを利用できるように、基本的な操作教育が必要である。

(2) セキュリティ教育

パスワードの設定・管理やファイル管理などのセキュリティに対する基本的な教育が必要である。

(3) 倫理教育

ネットワーク上を流れる情報のチェックは不可能に近い。したがって、個人利用における情報内容を制限するには倫理教育を徹底することが必要である。

(4) ネットワーク管理者教育

ネットワークの業務利用にあたっては、メールサーバ、ニュースサーバ、ファイルサーバ、WWWサーバ、およびネームサーバなどの各種サーバの管理を行うネットワーク管理者が必要である。

ネットワーク管理者に対しては、ネットワーク構成、サーバ設計、セキュリティ対策、機器管理手法、ユーザ管理手法、障害切り分け方法、ユーザ教育などに関する技術的な教育を行うことが必要である。

3. 建設省におけるインターネット接続手法

「建設省LANアドレス標準」（以下「アドレス標準」という）は、建設省専用通信網に接続されている全てのLANおよびLAN間接続パス（WAN）のアドレス付与に関して適用されるIPアドレス標準であり、「建電通仕第24号」として平成6年2月28日に制定されている。

「アドレス標準」は、いわゆるローカルアドレスとして制定されたIPアドレス体系であり、インターネット上のIPアドレスと重複することから、直接的にはインターネットと接続することはできない。

ここでは、「アドレス標準」を採用している建設省専用通信網LAN（以下「専用LAN」という）をインターネットに接続するための手法について記述する。

3. 1 「建設省LANアドレス標準」の位置づけ

IPアドレスには、全世界でユニークに割り振られたグローバルアドレスがある。これは、米国に本部を置くInterNIC(International Network Information Center)が管理しており、日本ではJPNIC(JapanNIC)に申請して得られる。建設省の情報システムに適用する場合、専用通信網に接続される機器全てに付与するには残りが少ないことと、番号が体系的に付与できないという問題がある。

このため、建設省内の利用には独自の体系（電話の内線番号のような）を持つIPアドレスとして、「アドレス標準」が制定された。

3. 1. 1 アドレス管理の重要性

LAN間接続網（WAN）の構築、利用、運用には十分な計画が必要であり、なかでもIPアドレス管理計画は最も重要といえる。アドレス管理に不備があった場合には、ブロードキャスト・ストームやブラックホールなどの障害が発生し、メルtdown（システム・ダウン）に至ることもある。

「アドレス標準」では、局所的なLAN形態は勿論、建設省専用通信回線を利用した広域的なLAN間接続形態にも矛盾なく対応できるように、アドレス体系が制定されている。この「アドレス標準」の大きな特徴を以下に示す。

(1) IPアドレス付与機構の分散化

「アドレス標準」では、LANやWANのIPアドレス付与のルールが明確化されており、実際のアドレス付与は、各地方建設局などの電気通信課長が行う。

このことは、建設省本省でのアドレス付与に関する一括管理は必要なく、各地方建設局などに分散化されていることを意味し、アドレス管理やトラフィックを考慮したネットワーク設計が、容易かつ迅速に行えることになる。

(2) IPアドレスによるシステム管理の容易化

IPアドレスの数値により、広域的な区分（エリア番号）や所属工事事務所（事務所番号）などが電話番号のように把握でき、システム管理が容易となる。

3. 1. 2 アドレス体系の概要

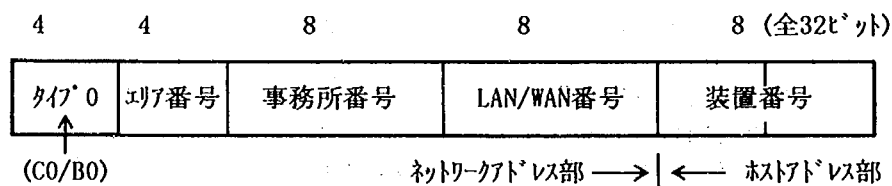
「アドレス標準」のアドレス体系の概要を以下に説明する。詳細は、建電通仕第24号「建設省LANアドレス標準」で参照できる。

(1) アドレス構成

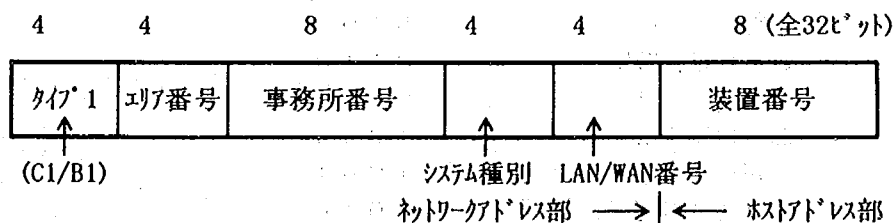
「アドレス標準」では、IPアドレスの数値が電話番号のようにネットワーク構成に対応している。ただし、IPアドレスは8ビット毎に区切って4桁の10進数で表現するため、数値からの直感的な把握はむずかしい面もある。

基本的には3つのタイプから選択して使用できる。タイプ領域からLAN/WAN番号領域までが、ネットワークアドレス部、残りがホストアドレス部となる。

<タイプ0：各種システムの一括管理用>



<タイプ1：システム毎の管理用>



<タイプ2/3：拡張版>

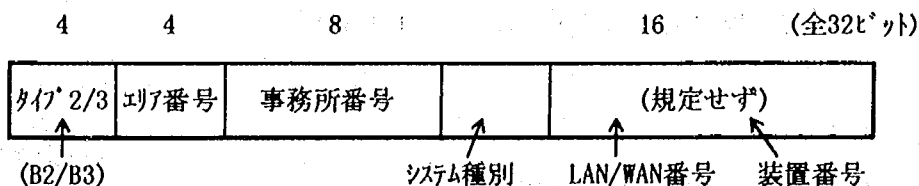


図3. 1. 2. 1 IPアドレスフォーマット

(2) 各番号要素の内容

① タイプおよびクラス

システム構成に合わせて選択できるものであり、グローバルアドレスのクラスB/Cに相当するアドレスの上位4ビットを使用する。

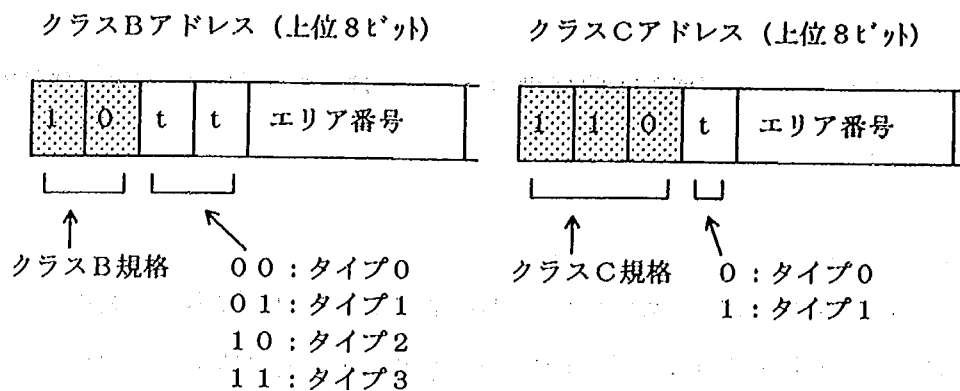


図3. 1. 2. 2 タイプおよびクラスの構成

② エリア番号

広域的な区分を示す番号であり、以下の対応となる。

[エリア名]	[二進数]
建設本省、付属機関	0 0 0 0
北海道開発局、道	0 0 0 1
東北地建、県	0 0 1 0
関東地建、都県	0 0 1 1
北陸地建、県	0 1 0 0
中部地建、県	0 1 0 1
近畿地建、府県	0 1 1 0
中国地建、県	0 1 1 1
四国地建、県	1 0 0 0
九州地建、県	1 0 0 1
沖縄総合事務局、県	1 0 1 0
公団等に対する予備	1 0 1 1
公団等に対する予備	1 1 1 1

③ 事務所番号

建設省専用通信網の電話局番に準拠して定められる。

[事務所名]	[10進数]
建設本省、付属機関	80、93など
地建本局	0
事務所等	電話番号の7xx、8xxの下位2桁

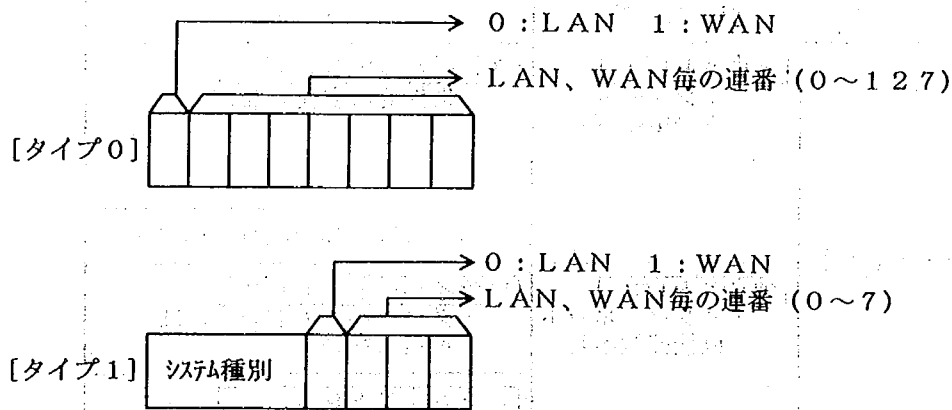
関東地建の番号例を下に示す。

[事務所名]	[電話番号]	[クラスC、タイプ1の場合]
関東地方建設局		2 1 1. 0. x x x. x x x
東京国道	7 0 1	2 1 1. 1. x x x. x x x
東京都	7 0 2	2 1 1. 2. x x x. x x x
埼玉県	7 0 3	2 1 1. 3. x x x. x x x
湾岸道路	7 9 5	2 1 1. 9 5. x x x. x x x

同じ数値を使用する

④ LAN/WAN番号

先頭ビットでLAN/WANの区別を表し、残りビットを連番で使用する。



⑤ システム種別

システムの区別を表し、以下の割り当てとなる。

[システム区分]	[二進数]
複数システムの共用	0 0 0 0
河川情報システム	0 0 0 1
レーダ雨量システム	0 0 1 0
道路交通情報システム	0 0 1 1
電算情報システム	0 1 0 0
予備	0 1 0 1
予備	1 1 1 1

⑥ 装置番号

装置毎に連番で与えられる。ただし、2 5 5は全装置への同報を表し、0は自装置を表す特殊用途に予約されており、使用不可である。

3. 2 グローバルアドレス取得の必要性

(1) アドレスの分類

I Pアドレスには、公式アドレスと独自アドレスの2種類に分類される。

公式アドレスは「グローバルアドレス」と呼び、世界的に重複しないように割り当てられている。この割り当ては、米国に本部を置く I n t e r N I C (International Network Information Center) が管理しており、日本では J P N I C (JapanNIC) に申請して得られる。

また、独自アドレスは正式に割り当てられていないアドレスのことをいう。この独自アドレスは厳密に言えば、さらに2種類に分類され、任意の番号を使用する「ローカルアドレス」と、グローバルアドレスとして割り当てられない領域を使用する「プライベートアドレス」がある。

「アドレス標準」は、「ローカルアドレス」に相当する。

表 3. 2. 1 I Pアドレスの分類

	2. 分 類		3. 分 類	
	I Pアドレス			
	公式アドレス ・インターネット 直接接続可能		グローバルアドレス ・世界的に重複しない	
			(プライベートアドレス部は割り当てない)	
			プライベートアドレス ・グローバルアドレスとは 重複しない	
	独自アドレス ・インターネット 直接接続不可		ローカルアドレス ・グローバルアドレスと 重複する	

(2) アドレスの表現方法

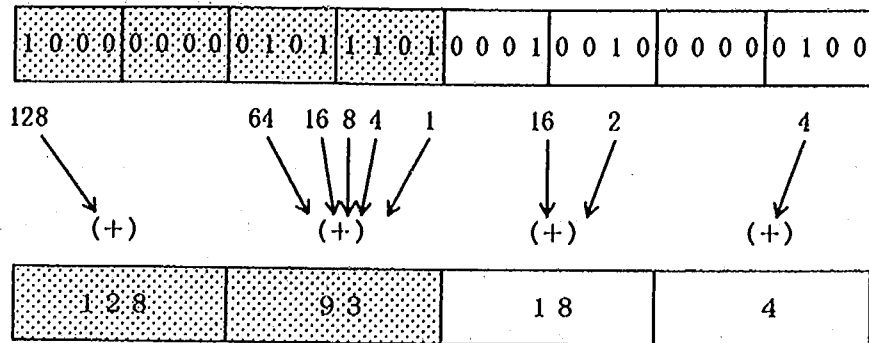
I Pアドレスは32ビット長であり、NICから割り当てられるネットワークアドレス部とユーザが設定するホストアドレス部で構成される。

アドレス表現においては、32ビットを2進数で表現すると長いため、8ビットずつに区切って10進数4桁で表すことが多い。このため、各桁の10進数は0～255の範囲の値となる。

実際の表現は、4桁の10進数をドットで区切って表現する。

(例) 128.93.18.4

< 2進数表現 >



< 10進数表現 >

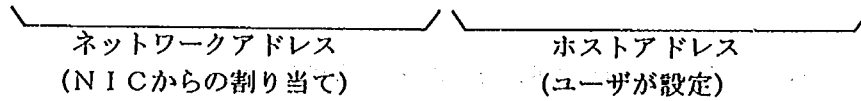


図 3. 2. 1 アドレス表現方法

3. 2. 1 グローバルアドレス

NICのグローバルアドレス管理は、電話番号のように系統だてた管理ではなく、申請順に割り付ける方式である。一番違いの番号が近くのネットワークという訳ではなく、世界のどこかに存在することになる。

グローバルアドレスは下記の範囲を持つ。

[クラスA] nnn=127 / hhh=256x256x256-2=1677726

1 ~ 1 2 7	h h h	h h h	h h h
-----------	-------	-------	-------

[クラスB] nnn=64x256=16384 / hhh=256x256-2=65534

1 2 8 ~ 1 9 1	0 ~ 2 5 5	h h h	h h h
---------------	-----------	-------	-------

[クラスC] nnn=32x256x256=209752 / hhh=1x256-2=254

1 9 2 ~ 2 2 3	0 ~ 2 5 5	0 ~ 2 5 5	h h h
---------------	-----------	-----------	-------

(nnn=ネットワークアドレス部の数 / hhh=ホストアドレス部の数)

図 3. 2. 1. 1 グローバルアドレスの範囲

3. 2. 2 プライベートアドレス

プライベートアドレスは、インターネットの標準規定であるRFC1597で、1994年4月に制定された。

いままではグローバルアドレスとして割り当てられていないアドレスを、プライベートアドレスとして使用することに決めた部分であり、ユーザはローカルネットワーク内では自由に使用することができる。このアドレスと、グローバルアドレスを持つ世界のネットワークとの重複は無いが、インターネット接続する場合はファイアウォールを使用してプライベートアドレスを外部に流さないようにしなければならない。

プライベートアドレスは下記の範囲を持つ。

[クラスA] nnn=1 / hhh=256x256x256-2=1677726

1.0	h h h	h h h	h h h
-----	-------	-------	-------

[クラスB] nnn=16 / hhh=256x256-2=65534

17.2	16~31	h h h	h h h
------	-------	-------	-------

[クラスC] nnn=256 / hhh=1x256-2=254

19.2	16.8	0~25.5	h h h
------	------	--------	-------

(nnn=ネットワークアドレス部の数 / hhh=ホストアドレス部の数)

図 3. 2. 2. 1 プライベートアドレスの範囲

3. 2. 3 ローカルアドレス

NICから正式に割り当てをもらわないで、ユーザが非公式に割り当てて使用するアドレスのことであり、プライベートアドレス以外の範囲のアドレスをローカルアドレスという。

アドレス表現は、グローバルアドレスおよびプライベートアドレスと全く同じ形式となる。なお、アドレス標準はローカルアドレスに当たる。

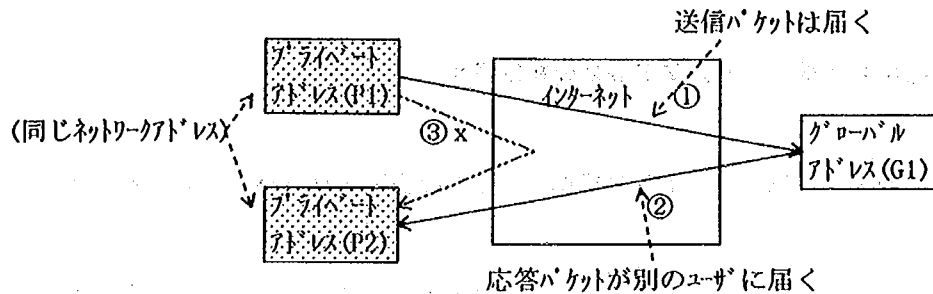
3. 2. 4 独自アドレスの問題点

プライベートアドレスまたはローカルアドレスのままでインターネット接続すると、正しく通信できないだけでなく他のネットワークにも悪影響を与えることになる。インターネット接続する場合は、送信元アドレスとしてグローバルアドレスが必須であり、その理由を以下に示す。

(1) プライベートアドレスによる通信の不具合

プライベートアドレスを送信元アドレスとして持つ packets をインターネットに送信すると、応答 packets が同じネットワークアドレスを持った別のユーザに届くことにもなり、正しく通信できない。

また、プライベートアドレス同士のインターネット接続も、送信 packets がインターネットに送信されない。

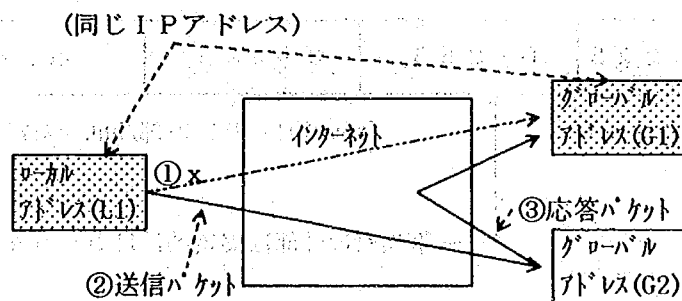


- ① G 1 向けの送信 packets は、G 1 に届く
- ② G 1 からの応答 packets は P 2 に届く
- ③ P 2 向けの送信 packets はインターネットに送信されない

図 3. 2. 4. 1 プライベートアドレス通信の不具合

(2) ローカルアドレスによる通信の不具合

ローカルアドレスのままでインターネット接続すると、そのローカルアドレスと重複したグローバルアドレスを持つネットワークとは接続できないばかりでなく、アドレス重複しない相手に packets 送信したとしても応答 packets が第三者に届いてしまい、通信ができなくなる。



- ① G 1 向けの送信 packets は、インターネットに送信されない
- ② G 2 向けの送信 packets は G 2 に届く
- ③ G 2 からの応答 packets は G 1 に届く

図 3. 2. 4. 2 ローカルアドレス通信の不具合

3. 3 「建設省LANアドレス標準」を採用したインターネット接続手法

「アドレス標準」はいわゆるローカルアドレスであり、そのままではインターネット接続ができないことは、「3. 2」で記述した通りである。

そこで、「アドレス標準」を使用した大規模ネットワークを、インターネット接続するための手法として以下に記述する。

3. 3. 1 「アドレス標準」とグローバルアドレスの重複範囲

インターネット接続を検討するには、「アドレス標準」が、どの程度グローバルアドレスと重複しているかを整理する必要がある。

「アドレス標準」では、クラスAを除いたクラスB/Cの全アドレス空間を制定している。ただし、第二オクテットの事務所番号は、実質的には0～99の範囲を使用するものと見られ、残り100～255は空きと考えるても良い可能性もある。

図3. 3. 1. 1に「アドレス標準」の制定範囲を示す。

[クラスA] ----->未使用

nnn	hhh	hhh	hhh
-----	-----	-----	-----

[クラスB] ----->全範囲を使用

128～191	0～255	hhh	hhh
---------	-------	-----	-----

[クラスC] ----->全範囲を使用

192～223	0～255	0～255	hhh
---------	-------	-------	-----

(nnn=ネットワークアドレス部/hhh=ホストアドレス部)

↑
事務所番号部は実質的には0～99の範囲

図3. 3. 1. 1 「アドレス標準」の制定範囲

3. 3. 2 アドレス変換手法の基本

ローカルアドレスを持つネットワークがインターネットと接続するためには、送信元のローカルアドレスをグローバルアドレスに変換する手法が必要となる。

(1) ルータ型アドレス変換手法

本機能はプライベートアドレスを使用したユーザネットワークを、インターネットと接続する時に使用することができる。

プライベートアドレスはインターネット上の相手との重複がなく、アドレス変換機能により動的にプライベートアドレスと取得済みのグローバルアドレスを変換してIPパケット中継する。

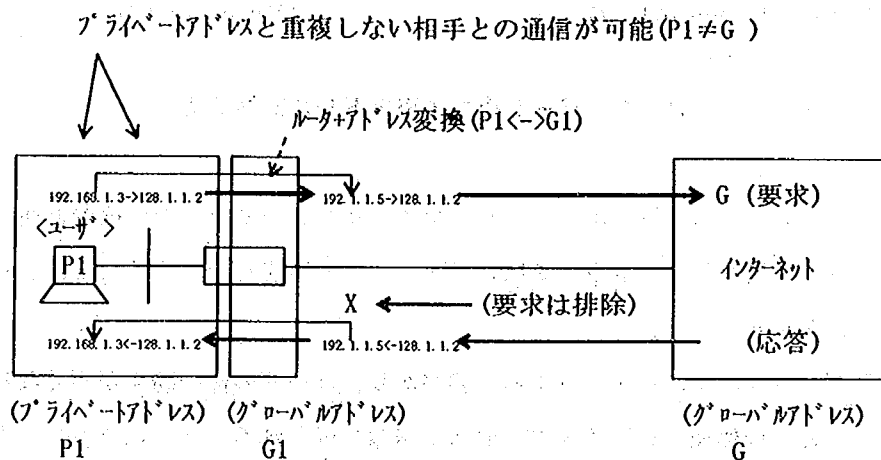


図 3. 3. 2. 1 ルータ型アドレス変換手法

本手法の特徴は、プライベートアドレスを持つユーザがアドレス変換装置を意識することなく、ルータ接続されているかのようにインターネットと通信できることである。

本手法の欠点は、ローカルアドレス使用ユーザの場合は、重複するインターネット上の相手とは通信できないことである。また、インターネット側からユーザネットワーク内部に入ることはいできない。

また、ユーザ認証は、IPアドレスで行なわれるため、ユーザのIPアドレスがインターネット側から見えることである。よって、このIPアドレスを詐称して、インターネット側からユーザネットワーク内部に入ることができるため、セキュリティの面で問題がある。

(2) ゲートウェイ型アドレス変換手法

「アドレス標準」のように、クラスAを除くほとんどのグローバルアドレスとの重複が多い場合は、ルータ型アドレス変換手法は使用できない。

ローカルアドレスとグローバルアドレスをもつゲートウェイ装置に、ローカル側から一度ログインし、そ

こから再度外部に接続する手法である。このとき、ゲートウェイは自身のグローバルアドレスを使用して、代理としてインターネット上の相手と通信する。

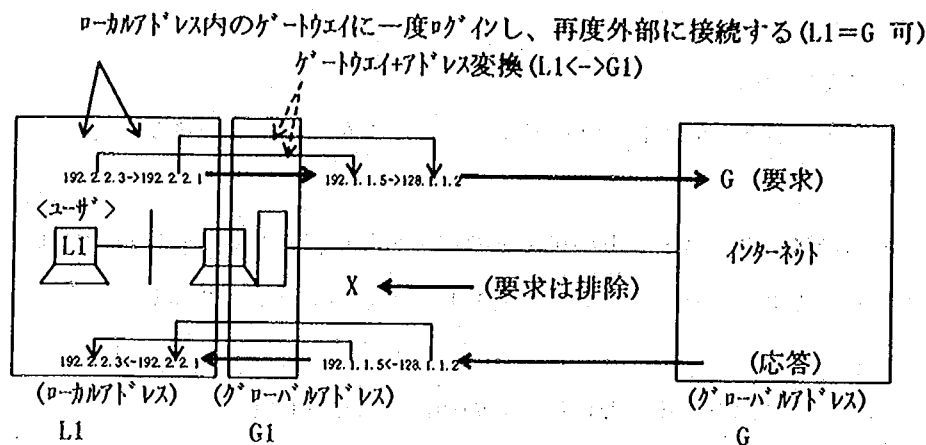


図 3. 3. 2. 2 ゲートウェイ型アドレス変換手法

本手法の特徴は、ローカルアドレスを持つユーザでも、全てのインターネット上の機器と通信できることである。また、インターネット側からゲートウェイにログインできる機能を持たせることにより、ユーザネットワーク内部に入ることが可能である。

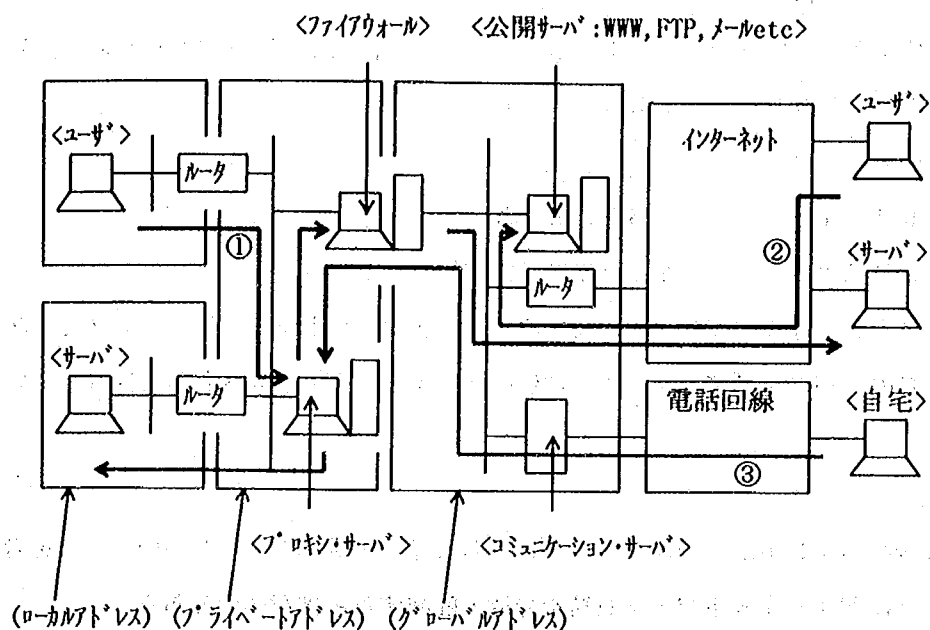
本手法の欠点は、一旦ゲートウェイにログインする必要がある、ユーザの使い勝手が悪くなることである。また、アクセスが集中すると代理処理のUNIXプロセスが多数生成されることになり、レスポンスが低下することもある。

3. 3. 3 機器構成

建設省におけるインターネット接続においては、ユーザのネットワーク内に外部から見える情報サーバがあり、外部から自由にアクセスできると同時に、ユーザが自宅や出張先からユーザネットワークに入り込んで、情報を得ることもできる構成であることが望ましい。

このような情報発信型インターネット接続においては、外部からの不正進入を防ぐためのファイアウォールが必要となる。

また、「アドレス標準」を使用することから、ゲートウェイ型アドレス変換手法が必要であり、ファイアウォールも含めて、図 3. 3. 3. 1 で示す構成が必要となる。



- ① ユーザはプロキシ・サーバにログインし、プロキシ・サーバが代理でファイアウォール経由でインターネットにアクセスする
- ② インターネット・ユーザは、公開サーバまでアクセスできる
- ③ 自宅からプロキシ・サーバにログインし、代理でローカルサーバにアクセスする

図 3. 3. 3. 1 建設省におけるインターネット接続のための機器構成

3. 3. 4 インターネット接続上の考慮点

「アドレス標準」を使用したネットワークは全国規模であり、インターネット接続においては、いくつかの考慮が必要となる。

(1) インターネット接続ポイントの考慮

インターネットとの接続ポイントは、次の観点から、本省及び各地建本局ごとの一カ所とすることが望ましい。

① ファイアウォール構築

ファイアウォール構築の観点で見れば、インターネットとの接続は一カ所で行うのが良い。

② グローバルアドレスの取得数

現在の J P N I C から取得できるグローバルアドレスは、通常はクラス C が一個である。したがって、インターネットと接続するルータは一カ所となる。

③ 本省からのインターネット接続

各地方建設局管内は、専用通信ネットワークで接続されるため、全国的にほぼ同一のネットワークコストでアクセスポイントに到達できる。

(2) プライベートアドレスの選択

「アドレス標準」で使用されないプライベートアドレスとしては、厳密には次の2種類から選択できる。

- ① クラスA [10. h h h. h h h. h h h]

(未使用のアドレス)

- ② クラスC [192. 168. 0~255. h h h]

(エリア番号は本省であり、事務所番号は実質的には未割当)

上記のクラスAは「アドレス標準」では未使用であるが、大きなネットワーク用アドレスでもあり、可能ならば、上記のクラスCの方がファイアウォールの内側のプライベートアドレスとしては適している。

(3) 負荷分散の考慮

インターネットとの接続ポイントが一カ所であること、および全国規模のユーザがいることを考慮すれば、インターネットとの接続に関するネットワーク負荷を分散・軽減する考慮が必要である。

- ① プライベートセグメントまでの経路

建設省内の業務処理ネットワークの経路を使用すると、経路渋滞が発生して情報処理に影響を及ぼすことも考えられる。

プライベートネットワークから各工事事務所までは、インターネット接続専用のルートを、ルータで接続することも望ましい。

- ② プロキシ・サーバおよびファイアウォールの負荷分散

プロキシ・サーバおよびファイアウォールは、アプリケーション・プロセスが要求に応じて起動するため、同時に多数の要求が発生すると、レスポンスが遅くなる可能性がある。

各地方建設局毎に専用のプロキシ・サーバおよびファイアウォールを設置するか、緊急使用および通常使用の数種類のプロキシ・サーバおよびファイアウォールを設置するのが望ましい。

- ③ 接続可能装置の制限

インターネット接続できる装置にある程度の制限を設け、負荷を軽減することも必要である。

以上の負荷分散を考慮したネットワーク構成図を図3. 3. 4. 1に示す。

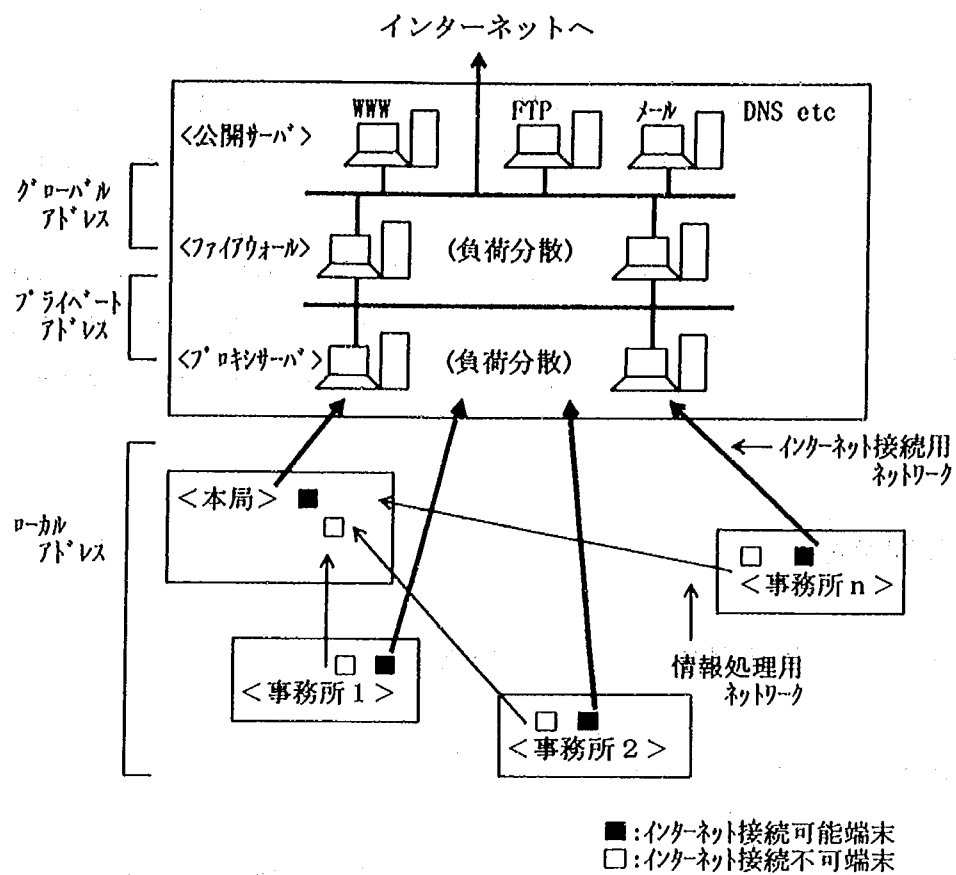


図 3. 3. 4. 1 負荷分散を考慮したネットワーク構成

4. 機器管理手法

コンピュータネットワークは、通信機器、ネットワーク機器、コンピュータ機器などのさまざまな機器で構成される。これらの機器で構成されたネットワークを効率よく稼働させ、常に正常な状態を維持するための監視・管理は重要である。

上記ネットワーク管理の要求を満足するためには、機器の二重化や耐久性のある高機能・高性能な装置を用意する方法もあるが、そのためには膨大な費用がかかることになる。そこで、ネットワーク管理を適切に行い、異常が発生しても迅速に対応できる管理体制を持てば、比較的少ない投資で大きな効果を得ることが可能となる。

4. 1 管理対象機器の分類

ネットワーク管理の対象となる機器について、以下に記述する。

4. 1. 1 通信機器

建設省専用通信回線は自営の通信回線であり、各種通信設備が全国的に配備されている。これらの通信機器に障害が発生すると、それを利用して通信を行うネットワーク全体に障害を及ぼすことになる。

通信機器そのものには、ある程度の二重化や障害回避機能が盛り込まれており、通信路そのものの信頼性が考慮されている。ただし、各通信機器の管理は独自に行われているのが現状であり、これらをコンピュータネットワーク全体としての管理対象にも含めることが、ネットワーク管理としての効果を高めることにもなる。

管理対象となる主な通信機器を以下に示す。

- 1) 多重無線装置 (アナログ、デジタル)
- 2) 無線中継局
- 3) 衛星装置

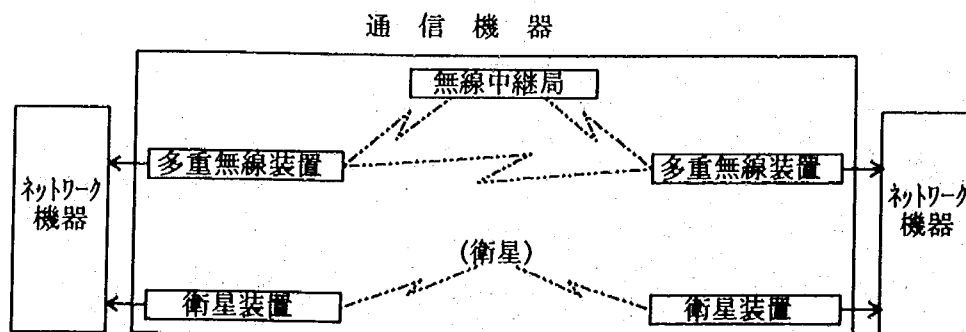


図 4. 1. 1. 1 通信機器の概要

4. 1. 2 ネットワーク機器

コンピュータ機器を接続してLAN (Local Area Network) 機能を提供する機器、および通信機器に接続してLANの相互接続によるWAN (Wide Area Network) 機能を提供する機器が対象となる。

LAN機能を提供する機器の障害は、そこに接続されているコンピュータに対しての一部分の障害となるが、WAN機能を提供する機器の障害はLAN全体に影響することがある。ネットワーク機器の障害への対応は、機器自体での二重化を図るよりもネットワーク構成全体として信頼性を高める方向にあり、ネットワーク上のプロトコルもこの概念で設計されている。

管理対象となる主なネットワーク機器を以下に示す。

- 1) ブリッジ/ルータ/ゲートウェイ
- 2) インテリジェントHUB (リピータ、スイッチ)
- 3) モデム (MODEM)
- 4) ターミナルアダプタ (TA)

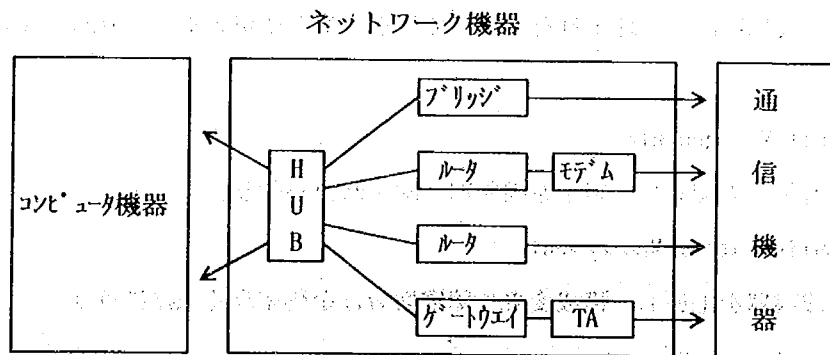


図 4. 1. 2. 1 ネットワーク機器

4. 1. 3 コンピュータ機器

コンピュータ機器は各種アプリケーション機能をユーザに提供するための機器であり、各種サービスを提供するホストコンピュータやサーバから、各種サービスを利用するPCなどのクライアントコンピュータまでが対象となる。

サービスのなかで特に重要な位置づけにあるコンピュータやサーバには、二重化やバックアップ機能などを盛り込むことが多い。その他の機器では、障害の早期検出機能と復旧体制の確立により補われる。

- 1) ホストコンピュータ
- 2) 各種サーバ
- 3) クライアントコンピュータ
- 4) ターミナルサーバ

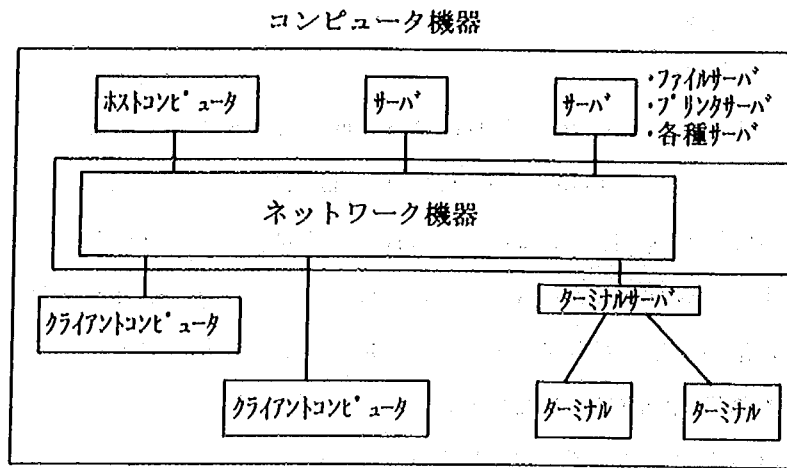


図 4. 1. 3. 1 コンピュータ機器

4. 2 管理項目の分類

ネットワーク管理の実施には、管理項目を分類して整理する必要がある。一般的な管理内容の分類方法と概要を以下に示す。

① 障害管理 (Fault Management)

障害発生時の障害箇所の切分け、障害原因判別、障害回復を行う。

② 構成管理 (Configuration Management)

ネットワーク構成機器を把握し、構成変更や障害切分けを効率良く正確に行う。

③ 性能管理 (Performance Management)

ネットワークのパフォーマンスが保たれているかどうかの監視を行う。

④ 機密管理 (Security Management)

機密性の高いデータやプログラムを、第三者や災害から守る。

4. 2. 1 障害管理

ネットワーク障害は何時発生するかの予測はできないため、常に監視することが必要となる。常に監視することによって、ネットワークが正常に稼働していることを確認し、障害の兆候などを見分け、障害を未然に防止することができる。障害発生時には、障害箇所の切分け、障害原因判別、障害回復を行うことになる。障害発生時の対応は以下の順序で行われる。

- 1) 障害検出
- 2) 障害切分け
- 3) 原因判別

4) 障害復旧

5) 障害報告

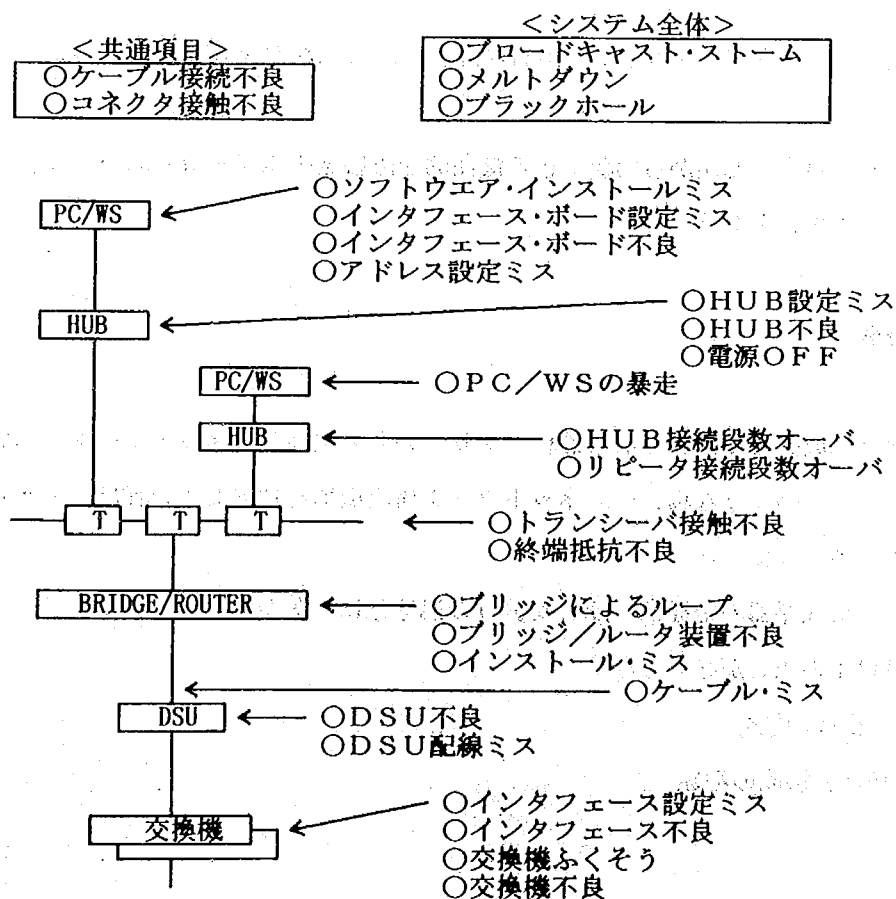
(1) 障害検出

障害の検出は、ネットワーク管理者が発見し、ユーザの知らないうちに復旧するのが理想的である。しかし、通常はユーザが自分の使用する端末から異常を発見し、ネットワーク管理者に通報してくるケースが多い。ユーザにとっての障害には、オペレーションミスや接続ケーブル抜けなどの軽い内容から、機器障害などの重い内容まで混在する。障害の復旧を速やかに行うという目的にたてば、ユーザにも軽い内容かどうかを見分けられる程度のオペレーションマニュアルを整備することも必要である。よくあるオペレーションミスや接続ケーブルのチェック方法などを掲載しておけば、不必要に多くの障害発生 of 通報を受けなくて済むとともに、効率良く障害復旧を行うことができる。

(2) 障害切分け

ネットワークの障害は多種多様であり、障害箇所の特定が困難な場合が多い。障害切分けを行う場合、ネットワークを構成する各機器、接続ケーブル、回線などの各構成要素を順に調べる必要がある。

図4. 2. 1. 1にネットワーク障害原因の一例を示す。



(デジタル交換機を使用したネットワーク接続の例)

図4. 2. 1. 1 ネットワーク障害原因の一例

図4.2.1.1で示すようにネットワーク障害の原因は多種多様であり、ネットワーク接続場所の違うユーザから見れば、障害の見え方が異なる場合も多い。障害の切分けを迅速に行うためには、ネットワーク構成機器全般に対する知識と経験や、ある程度の専門的知識が必要になり、ネットワーク管理者の教育が重要な課題となる。

(3) 原因判別

障害原因の追求には、障害状況、環境変化の有無、各機器が保持するメッセージなどの障害に関連する正確な情報を収集し、解析することになる。

解析に時間を要すると判断した場合は、システムを初期化したり代替え機器と交換したりしてシステムを一旦復旧させ、そのあとで原因究明を行うことが多い。

(4) 障害復旧

障害の切分け後は速やかに復旧作業を行うことが必要となる。

障害復旧を短時間に行うためには、障害箇所によっても異なるが、操作手順書の整備、操作員の教育、および保守体制の整備が必要である。

(5) 障害報告

障害からの復旧後は、障害内容、障害箇所、障害原因、復旧方法などを「障害報告書」として記録に残すことが重要である。

この障害履歴により、障害の兆候から判断できる潜在的な障害発生原因を取り除いたり、類似障害に対しては速やかに対処できる場合もある。

4.2.2 構成管理

ネットワークは徐々に成長して大きくなる性格があり、いちど整備したネットワークの構成機器に変更が生じることが常である。このような場合に、ネットワーク構成機器を把握していれば、変更処理を正確に効率よく行うことができるようになる。

また、ネットワーク構成機器の把握は、障害切分けの迅速化には欠かせない要素である。

構成管理としては以下の項目が必要となる。

- 1) ネットワーク構成の把握
- 2) 構成機器の仕様、機能の把握
- 3) 資産管理
- 4) 変更管理

(1) ネットワーク構成の把握

ネットワークの規模が大きく複雑であるほど、ネットワーク構成の把握方法の確立が必要となる。

大規模ネットワークでは、全体的なネットワーク構成図をはじめとして、詳細度を高めた部分的なネットワーク構成図へと整備する。また、構成図に示すネットワーク資源（機器や回線など）の名前づけの規則を確立し、名前によってその資源名や所在がある程度分かるようにすることにより、速やかにネットワーク構成を把握することが可能となる。

(2) 構成機器の種類、機能、仕様の把握

ネットワークの物理的接続構成だけでなく、構成機器の種類、機能、仕様の把握が必要である。また、コンピュータ機器の場合は、動作しているソフトウェアのバージョンや使用している機能を把握することも重要である。

(3) 資産管理

ネットワーク機器が、実際に設置されている場所の把握を行う。

(4) 変更管理

ネットワークの変更作業に伴い、上記資料の改訂を行うことが必要となる。

最も大切なことは、どのような変更を行ったかの記録を明確に残すことであり、同じような変更作業がある場合は、変更記録を参考として迅速に行うことが可能となる。また、ネットワーク変更に伴い、往々にしてネットワーク障害が発生したりパフォーマンス（レスポンスなど）の低下を招くことがあり、こういう事態における原因追究のためにも、変更管理は重要である。

4. 2. 3 性能管理

コンピュータネットワークの構築時点においては、そのシステムが必要とするパフォーマンス（応答速度）には設計値が定められている。このパフォーマンスを保つために、定常的に測定して管理することが必要である。

性能管理と障害管理には密接な関連がり、ネットワークの応答速度が極端に遅くなった場合は、何らかの障害が発生していることになる。また、転送パケット数や衝突回数などの情報を収集することで、ネットワークの動作条件の改善を図ることも必要となる。

性能管理としては以下の項目が必要となる。

- 1) パフォーマンスの管理
- 2) ネットワーク負荷の管理
- 3) パフォーマンスの改善

(1) パフォーマンスの管理

ネットワークの応答速度を定常的に管理する。

ネットワーク管理装置からコンピュータ機器に対してping (Packet InterNet Gropher : TCP/IPにおけるエコー要求) などによって定期的に応答速度を監視し、極端に遅くなった場合は、ネットワークに何らかの障害が発生していると判断できる。

(2) ネットワーク負荷の管理・分析

ネットワーク上のパケット数や衝突回数、および通信回線の使用率などを収集・管理し、これらを解析することによってネットワークのパフォーマンスが適正に保たれていることを管理する。

また、コンピュータの負荷状態も管理対象となる。クライアント/サーバのネットワークでは、クライアント数の増加により徐々に応答速度が遅くなることがある。これは、サーバの負荷が増大したことによるスループットの低下に起因する。

(3) パフォーマンスの改善

パフォーマンスはネットワーク上の伝送時間と、コンピュータ処理時間の合計で決定できる。

ネットワーク上の伝送時間を短くするためには、ネットワークや通信回線の高速化が必要となる。また、コンピュータ処理時間を短くするためには、コンピュータ処理能力の向上などの改善作業が必要となる。

4. 2. 4 機密管理

コンピュータネットワークではオープン化が進む一方で、相反する機能となる機密管理が重要視されてきている。

ネットワークへの不正侵入による盗聴・改ざん、コンピュータ・ウイルスなどによるシステム破壊、災害による情報消滅に至るまで、さまざまな機密管理が要求されている。

機密管理としては以下の項目が必要となる。

1) 物理的保護

2) 論理的保護

(1) 物理的保護

情報の物理的保護を行うためには、コンピュータールームへの入退室管理、機密保護違反や障害発生時の連絡体制・対処体制の確立が必要となる。

また、災害などに備えて、情報の危険分散を行うことも重要である。

(2) 論理的保護

システムプログラム、ファイル、データへのアクセスには、ユーザ毎にアクセスレベルを設定して論理的

な保護を行うことが必要である。詳細は「5. ユーザ管理手法」で記述する。

また、データの安全性については、暗号化技術などによる機密保護を行わなければならない。暗号化技術の詳細は「6. セキュリティ管理手法」で記述する。

4. 3 管理情報の収集方式

ネットワークの構成機器は、通信機器、ネットワーク機器、およびコンピュータ機器に分類できる。

インターネットプロトコルの普及に伴い、ネットワーク管理プロトコルとしてはSMNP (Simple Network Management Protocol: 簡易ネットワーク管理プロトコル) が標準化され、広く使用されている。ネットワーク機器やコンピュータ機器は、ネットワークの普及に伴いSNMP対応している製品が多くなってきている。一方、通信機器はコンピュータネットワークとは独立して発展してきているため、SNMPへの対応がないのが現実である。

また、OSIにおけるネットワーク管理プロトコルとしてはCMIP (Common Management Information Protocol: 共通管理情報プロトコル) があるが、標準化の遅れにより、あまり普及していない。CMIPはSNMPを複雑化したようなプロトコルである。

このような現状を踏まえた管理情報の収集方式を以下に記述する。

4. 3. 1 信号情報による収集方式

通信機器は製造メーカ毎に独自の管理方式を採用した個別・独立管理がなされており、広範囲な通信回線設備を一元管理できる方式は存在していない。

このような通信機器を統合管理するためには、標準化されたSNMPを利用したLANのネットワーク管理システムに組み込む方式を検討することが必要となる。

具体的な方策としての一例を図4. 3. 1. 1に示す。

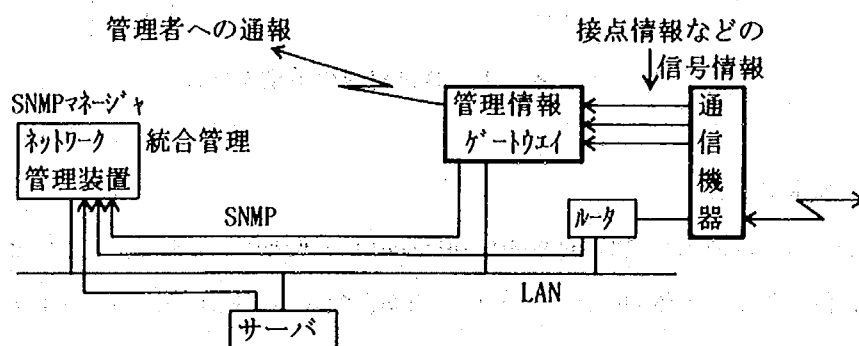


図4. 3. 1. 1 通信機器の情報収集方式

上図の方式は、通信機器自体または通信機器管理システムからの信号（接点情報など）を取り込み、LAN上のネットワーク管理システムに転送できるような、管理情報ゲートウェイ（仮称）を設置する方式である。ネットワーク管理装置への情報転送や、通信機器管理者への通報など、体制に合わせた管理体制に対応することが可能となる。

4. 3. 2 SNMPによる収集方式

SNMP (Simple Network Management Protocol:簡易ネットワーク管理プロトコル) は、インターネットプロトコル (TCP/IP) の普及に伴い、標準的に使用されているネットワーク管理プロトコルである。

(1) SNMPプロトコル

SNMPはTCP/IPネットワークの管理プロトコルとしてIAB/IETF (Internet Architecture Board/Internet Engineering Task Force) で標準化され、RFC 1157に定められている。

SNMPでは管理する側を「マネージャ」、管理される側を「エージェント」と呼び、マネージャとエージェントの間で管理項目を通信することによりネットワーク管理を行う。SNMPでは以下の5つのパケットを使用して管理情報の送受信を行う。

- ① GetRequest ----- マネージャからエージェントへの管理オブジェクト (MIB: Management Information Base) の要求
- ② GetNextRequest -- マネージャからエージェントへの次の管理オブジェクトの要求
- ③ SetRequest ----- マネージャからエージェントへの管理オブジェクトの内容設定要求
- ④ GetResponse ----- ①②③に対するエージェントからの応答
- ⑤ Trap ----- エージェントからマネージャへの異常状態の非同期通知

図4. 3. 2. 1にSNMPの管理モデルを示す。

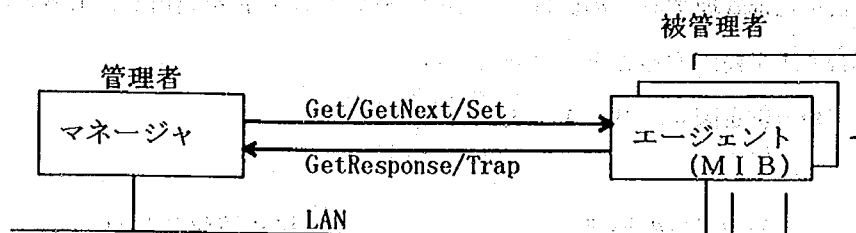


図4. 3. 2. 1 SNMPの管理モデル

(2) 標準MIBと拡張MIB

SNMPで管理する情報はMIB (Management Information Base:管理情報ベース) と呼ばれる管理対象オブジェクトの集合体である。具体的には、CPU使用率、ディスク使用率、パケット数、ネットワーク負荷などの情報を指す。

MIBにはRFCで標準定義されている標準MIBとベンダー独自に設定する拡張MIBがある。拡張MIBを使用することによって通信機器などの管理を行うことができる。この場合、通信機器の管理項目を整

理し、通信機器用拡張MIBの標準を作成すればマルチベンダーの通信機器の統合管理はある程度可能となる。

MIBは図4. 3. 2. 2のようなツリー構造を持ち、通信プロトコル上では、ツリーの中の番号をドットで区切って並べた形式を用いる。

例えば、標準MIBである「sysDescr：システム説明」を表現する場合は、下記となる。

objectID : 1.3.6.1.2.1.1.1

text label : iso.org.dod.internet.mgmt.mib.system.sysDescr

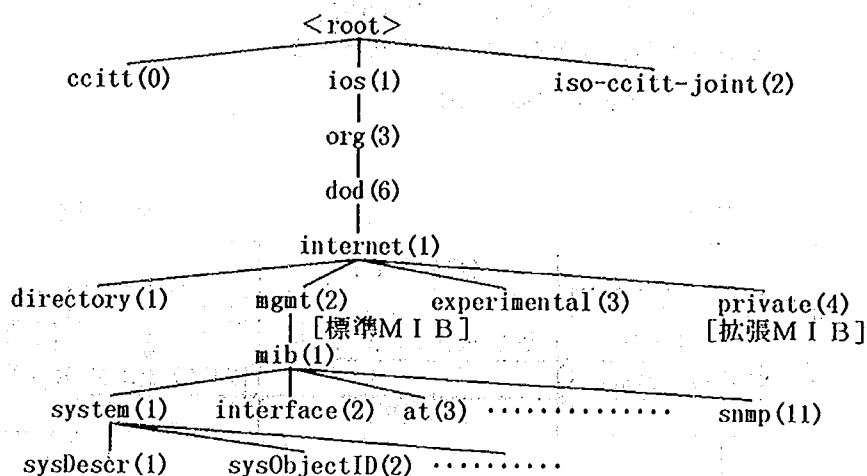


図4. 3. 2. 2 MIBのツリー構造

(3) SNMPによる管理

SNMPを使用してネットワーク管理を行うには、SNMPマネージャだけではなく、各機器のSNMPエージェントとしてのシステムグループ(system)のMIB情報を正しく設定することが必要となる。

正しい設定がされていないと、対象装置の種類や設置場所など、基本的な構成管理もできなくなるからである。ただし、このような設定を行うにも、名前の付与に関する統一規約などを作成することが必要となる。

システムグループのMIB情報には下記7項目がある。

- 1) sysDescr : システムの説明記述 (設定)
- 2) sysObjectID : ベンダー識別子 (設定)
- 3) sysUpTime : 起動後の経過時間 (自動生成)
- 4) sysContact : 装置のコンタクトパーソン (設定)
- 5) sysName : 装置の名前 (設定)
- 6) sysLocation : 装置の配置 (設定)
- 7) sysServices : 装置のサービスセット (設定)

4. 3. 3 CMIP方式

CMIP (Common Management Information Protocol : 共通管理情報プロトコル) は、OSIで標準化中のネットワーク管理プロトコルである。

CMIPはSNMPを複雑化したプロトコルであり、マネージングプロセスとエージェントプロセスで構成される。CMIPでは、マネージングプロセスおよびエージェントプロセスとアプリケーション層との間はCMIS (Common Management Information Service: 共通管理情報サービス) という言語で管理される。

CMISで規定されているコマンドを以下に示す。

- ① GET ----- ある特定の情報を獲得し、通知する。
- ② SET ----- パラメータを設定し、設定の完了を通知する。
- ③ ACTION --- あるアクションを実施し、結果を通知する。
- ④ CREATE --- スレッシュホールドを設定する。
- ⑤ DELETE --- スレッシュホールドを消去する。
- ⑥ CANCEL --- GETサービスプロセスをキャンセルする。
- ⑦ EVENT --- 事象が発生し、報告されたことを通知する。

図4. 3. 3. 1にCMIPの管理モデルを示す。

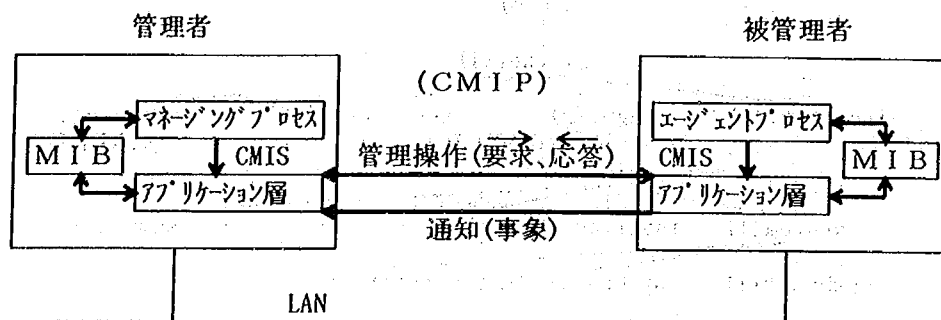


図4. 3. 3. 1 CMIPの管理モデル

4. 4 管理情報の伝送方式

管理対象機器が同一敷地内などの狭い範囲に設置されている場合は、それほど問題ではないが、コンピュータネットワークとしてWANを構成している場合は、ネットワーク管理としては広い範囲の機器が対象となる。

ネットワーク上を流れる情報以外に、ネットワーク管理用の情報をどのように伝送するかが課題となる。一般的な伝送方法として次の3種類の方法が考えられる。

- 1) 管理専用回線を使用
- 2) 管理対象回線を使用
- 3) 電話回線を使用

それぞれの特徴を以下に記述する。

4. 4. 1 管理専用通信回線による管理情報伝送

管理情報を伝送するために、管理対象機器がサービスする管理対象通信回線以外の管理専用通信回線を使用する方法である。

従来から行われている方法であり、下記の特徴がある。

- ① 管理対象通信回線の障害の影響を受ずに管理できる
- ② 管理対象通信回線に対する管理情報の伝送負荷がかからない
- ③ 広域になればなるほど管理用通信回線の整備費用が高価になる
- ④ 管理専用通信回線そのものの障害に対する対策が必要となる
- ⑤ 専用管理プロトコルが必要となる

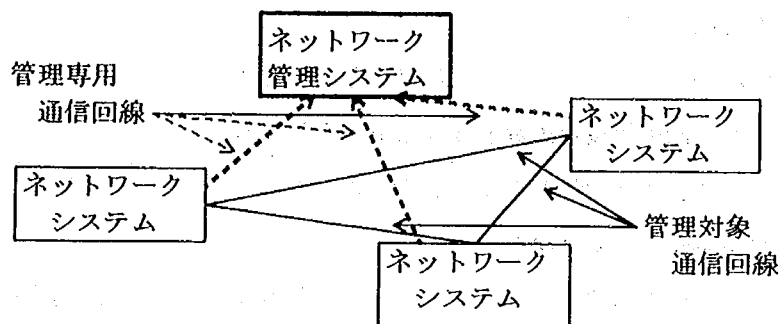


図 4. 4. 1. 1 管理専用通信回線による管理

4. 4. 2 管理対象通信回線による管理情報伝送

管理情報を伝送するために、管理対象機器がサービスする管理対象通信回線そのものを使用する方法である。

コンピュータネットワークで採用されている方法であり、下記の特徴がある。

- ① 管理専用通信回線が不要である
- ② 管理対象通信回線を使用した実応答時間などの管理が可能となる
- ③ 管理対象通信回線の障害時は、管理対象通信回線の迂回経路を使用する
- ④ 管理対象通信回線に対する管理情報の伝送負荷がかかる
- ⑤ 標準ネットワーク管理プロトコルが使用可能

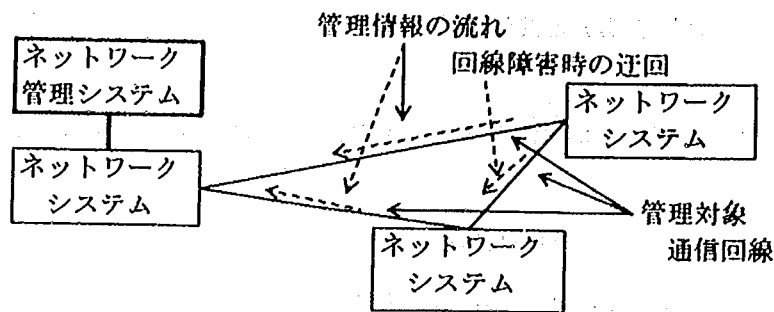


図 4. 4. 2. 1 管理対象通信回線による管理

4. 4. 3 電話回線による管理情報伝送

管理専用通信回線の代わりに電話回線を使用する方法である。

本方式には、下記の特徴がある。

- ① 管理専用通信回線に比べて、管理設備費用が少なくて済む
- ② 回線品質劣化時や回線輻輳時に対する考慮が必要となる
- ③ 回線速度遅いため、管理情報を少なくする必要がある
- ④ 専用管理プロトコルが必要となる

管理対象通信回線による管理情報伝送方式と組み合わせた構成とし、迂回路を持たない管理対象通信回線の障害時におけるバックアップ使用などが有効となる。

4. 5 その他の機器管理手法

4. 5. 1 分散管理と一元管理

ネットワーク管理の形態は、管理対象となるネットワーク規模によってさまざまな形態が採用されている。ネットワークを運用する組織や人員によりネットワーク管理の形態が大きく左右されることになる。

基本的な管理形態には分散管理と一元管理がある。

(1) 分散管理

コンピュータネットワークが複数システムの結合で運用される場合、各システム毎にネットワーク管理システムや管理者を置く形態を、分散管理という。この形態では、各システム毎の管理担当者はコンピュータ機器、ネットワーク機器、および通信機器の各機器に対する幅広い知識が必要となり、高度な専門教育が要求される。また、コンピュータネットワークの拡張に伴い、新たなネットワーク管理者の育成が必要となる。

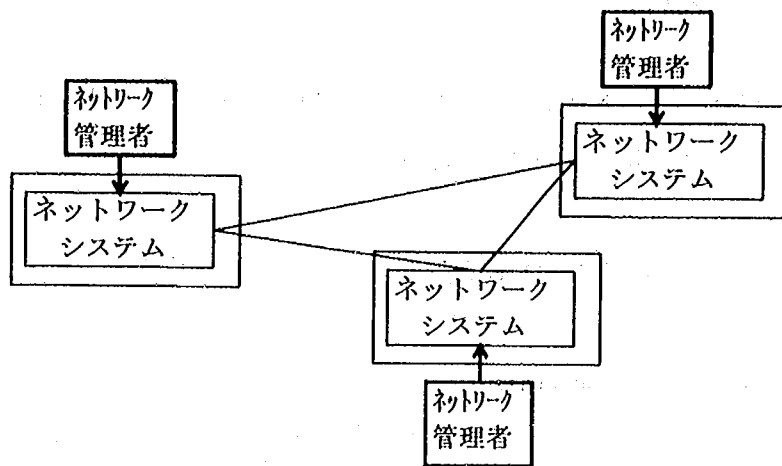


図 4. 5. 1. 1 分散管理

(2) 一元管理

複数システムの結合で運用されるコンピュータシステムにおいて、システムを一元管理できる機器およびソフトウェアを整備し、ネットワーク全体を中央のネットワーク管理システムから管理する形態を一元管理という。

この形態では、中央のネットワーク管理システムのシステム管理者だけが、コンピュータ機器、ネットワーク機器、および通信機器の各機器に対する幅広い知識があればよい。コンピュータネットワークが拡張しても、新たなネットワーク管理者の育成が不要となる。

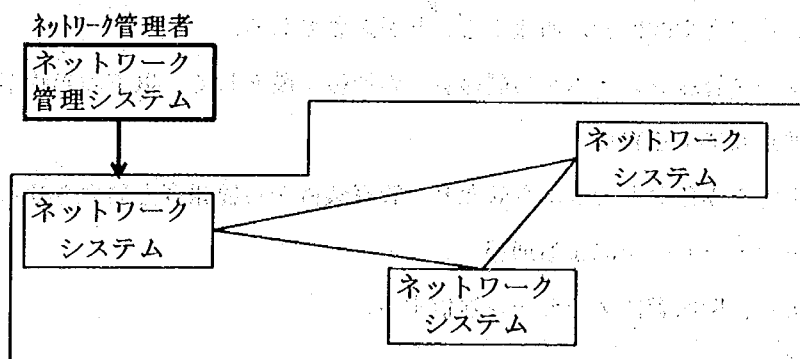


図 4. 5. 1. 2 一元管理

全国規模のネットワークでは一カ所の中央システムからの一元管理は困難な場合が多く、地域毎には一元管理、全国的には分散管理などの、管理形態の複合したシステムが現実的である。

4. 5. 2 管理情報の表示方法

管理情報には前述のとおり以下の各種情報があるが、SNMPを基本としたネットワーク管理システムを構築するソフトウェアは、一般的に以下の機能を持つ。

① 障害管理 (Fault Management)

リレーショナルデータベース (RDB) によるネットワーク資源の構成管理、ネットワーク構成図などの管理。

② 構成管理 (Configuration Management)

障害監視機能、障害発生通知機能、障害記録検索機能、障害履歴の統計処理機能など。

③ 性能管理 (Performance Management)

SNMP標準MIBによるノードの性能表示機能、統計など。

④ 機密管理 (Security Management)

コネクション情報検索機能など。

ネットワーク管理の基本は、ネットワーク管理用の見やすいネットワーク構成マップを作成することであり、ネットワーク構成マップと関連づけた各構成機器の仕様や機能などのデータベースも構築することが重要である。ネットワーク構成マップを使用して各種管理・監視を行うことが、効率よいネットワーク管理・監視となる。また、グラフィカルな表示を多く採用すれば、迅速な状況把握が可能となる。

4. 5. 3 障害発生時の通報

ネットワーク管理者はネットワーク管理システムを常時監視している訳ではない。障害発生時には、適切に速やかにネットワーク管理者や関係者に通報することが必要である。

障害発生時のネットワーク管理システムから関係者への通報手段として、以下の手法が考えられる。

① ネットワーク管理画面による表示

管理画面上に障害箇所を赤色などで表示させたり、管理装置から警報音を発生させる。

② ネットワーク経由のメッセージによる通報

電子メールなどにより、関係者にメッセージ送信する。

③ ポケベルによる通報

ネットワーク管理者にポケベルで障害発生を通報する。

④ 電話通報による通報

電話通報装置からネットワーク管理者に自動的に電話をかける。

⑤ FAXによる通報

ネットワーク管理者に障害発生状況をFAXで送信する。

⑥ 警報表示器による表示

ネットワーク管理者や関係者が常駐する環境に、ランプ表示やブザー吹鳴で通報する。

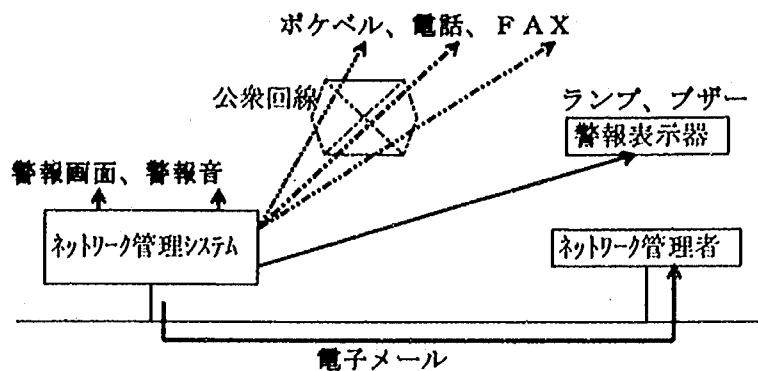


図4. 5. 3. 1 障害発生時の通報手段

4. 5. 4 障害発生時の管理体制

障害発生時の障害復旧処理は、障害内容や規模によって復旧手順が変わることがある。優先的に行わなければならないのは障害復旧作業であり、障害箇所の切分けを短時間で終わなければならない。原因を突き止めるのに時間を要する場合は、障害復旧を優先させ、後で原因を究明できるように障害発生時のさまざまなデータを正確に取得しておく必要がある。

障害発生時の障害復旧処理フローを図4. 5. 4. 1に示す。

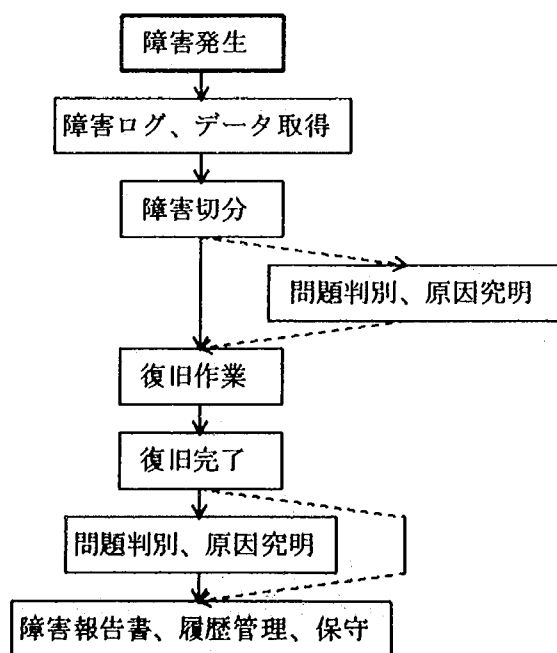


図4. 5. 4. 1 障害発生時の障害復旧処理フロー

上記の障害復旧処理を速やかに行うためには、障害発生時の管理体制の整備が重要である。

ネットワーク管理者はネットワークの監視・管理を中央システムから一元管理できるが、実際の障害内容の状況把握や簡単な障害確認・復旧作業は遠隔地のシステム毎の担当者に依頼する形式となる。またシステム構成機器は単純な機器から専門的技術を要する機器まで多種多様に渡り、全ての機器をネットワーク管理者が理解しておくことは困難である。したがって、ある程度の障害切分けを行った後は、専門業者に障害状況や障害データとともに連絡できる体制が必要である。また、専門業者からの公衆回線経由によるネットワーク管理システムへの接続ルートを用意しておき、専門業者からの遠隔障害診断などができるルートを確認すると、適切かつ早急な障害切分けや障害復旧作業が可能となる場合が多い。

これらを迅速に行うためには、ネットワーク管理システムにおいて機器構成に関連した管理担当者や専門業者の連絡先などをデータベース化しておくことが重要となる。

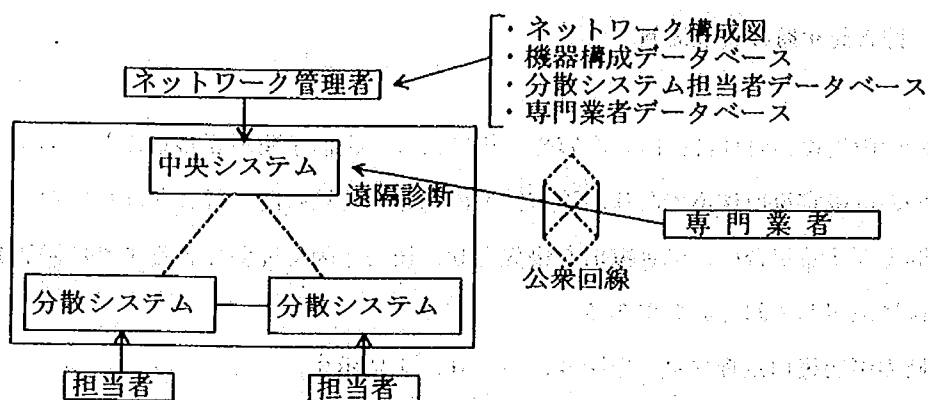


図4.5.4.2 障害発生時の管理体制

5. ユーザ管理手法

ユーザ管理は、ネットワークを適切に運用するために必要不可欠なものであり、各種サーバに対するユーザ毎のアカウント（利用権）管理や、ユーザ毎に付与される電子メールアドレス管理が対象となる。

特にユーザ数が多い全国的な大規模ネットワークや、人事異動などが多いネットワークでは、ユーザ管理を十分に検討してネットワーク構築を行うことが重要となる。

アカウントはユーザIDとパスワードで管理されるが、パスワードは各個人毎の秘密コードであるため、その管理は各個人にまかされる。パスワードに関する注意事項は「6. セキュリティ管理手法」の中で記述する。

5. 1 ユーザ管理の必要性

ファイルサーバにアクセスするためには、ユーザ毎のユーザID/パスワードによるユーザ認証を行うためのアカウント管理が必要となる。また、メールサーバを使用した電子メールシステムを使用するには、ユーザ毎にメールアドレスを付与することが必要となる。

ユーザ管理で重要なことは、ユーザIDや電子メールアドレスに重複が発生しないように管理することとも言える。

(1) アカウント管理

ファイルサーバやメールサーバなどの各種サーバへのアクセスには、そのサーバアプリケーション毎にユーザID/パスワードによるアカウントを獲得することが必要となる。

ユーザIDが重複すると、自分のファイル内容が他ユーザに見えたり、自分のファイルが使用できなくなるなどの事態が発生しかねないため、システム管理者はユーザ名が重複しないように付与しなければならない。

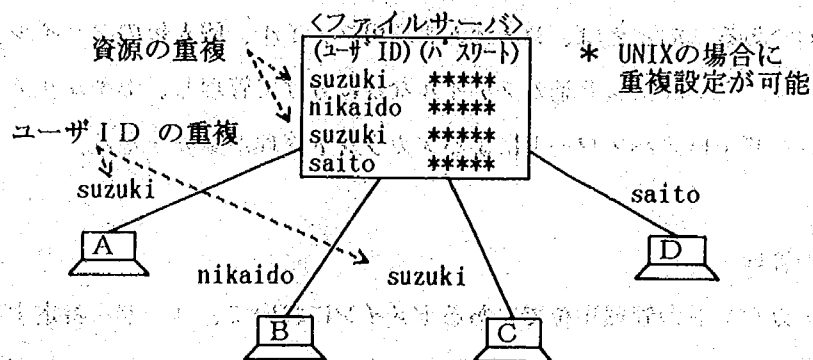


図5. 1. 1 ユーザIDの重複

(2) 電子メールアドレス管理

電子メールを使用するためには、ユーザ毎の電子メールアドレスが必要となる。電子メールアドレスに重複があると、希望する宛先に正しくメッセージが届かなくなり、運用上およびセキュリティ上においても大きな問題が発生する。

さらに、同一組織内における人事異動が頻繁に行われる環境において、その度に電子メールアドレスに変更が発生するようなシステム設計を採用した場合は、電子メールアドレスの重複発生の要因にもつながる。また、アドレスの重複がなくても、新旧アドレスの周知徹底は難しく、結果として別ユーザにメールが届くことにもなりかねない。

大規模ユーザのネットワークほど、メールアドレスの変更が発生しない設計にすることが重要である。

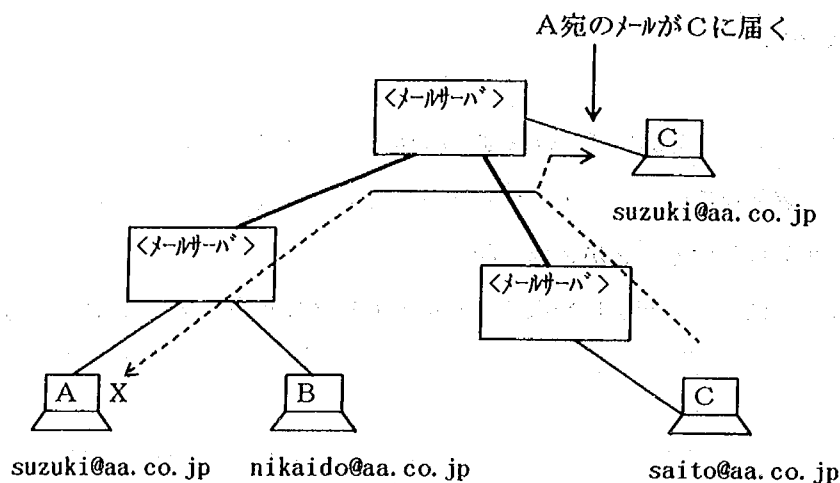


図5. 1. 2 電子メールアドレスの重複

5. 2 アカウント管理

コンピュータネットワーク上のデータへのアクセスは、ユーザ毎にアクセス可能なデータが異なるように管理するのが一般的である。たとえば、システム管理用ファイル、個人毎のファイル、グループ毎のファイル、部門毎のファイル、または全員共通のファイルなどに分けて管理し、セキュリティを高める対策を行う。そのためには、ユーザID/パスワードによるアカウント管理が重要となる。

(1) ユーザIDの管理

ユーザIDは、アカウントの管理単位でもあるドメインにおいて、ユーザを特定するために使用される。このため、同一ドメイン内のユーザIDでは重複が発生しないように管理しなければならない。

一方、大規模ネットワークにおいては、複数のドメインに分割してネットワークを構築することになる。このとき、アカウントの有効範囲が異なるドメイン間では、ユーザIDが重複していても問題はない。

ユーザIDは重複なくユーザ毎の識別ができればよく、IDの割付がしやすいほうが管理しやすいとされている。ただし、管理のしやすさとユーザの使いやすさは相反する場合が多い。

よく使用されているユーザIDの付与方法を以下に示す。

① 名前の組み合わせ

ユーザの名前を使用したユーザIDを使用する。

名前を使用するので、各ユーザは分かりやすい操作となるが、同姓や同姓同名のユーザがいる場合は工夫が必要となり、管理者の確認作業が増える。

[例] 鈴木一郎 : s u z u
鈴木次郎 : j - s u z u k i
鈴木次郎 : j i r o - s u z u k i

② 社員番号

ユーザの社員番号などを使用したユーザIDを使用する。

社員番号などが定められている場合は、管理は簡単になり、ユーザの使い勝手もそれほど悪くない。また、全国規模のユーザにおいても社員番号の管理は組織として行われるはずであり、管理された社員番号を使用すれば、ユーザIDは重複なく管理できることになる。さらに、人事異動などによるアクセスドメインの変更が発生しても、同じユーザIDを異動先でも使用することができる。

[例] 鈴木一郎 : G O 1 2 3 4 5 ——— G O : 共通識別記号
鈴木次郎 : G O 2 3 4 5 6 ——— 12345 : 社員番号
鈴木次郎 : G O 3 4 5 6 7

③ 管理番号

ユーザID用に一連の番号を使用する。

一連の番号を全国的に管理するのは困難であるが、識別記号を先頭に、ドメイン毎に一連番号を管理すれば重複回避は比較的容易である。人事異動などによるアクセスドメインの変更が発生した場合は、異動先で新たにユーザIDを獲得することになる。

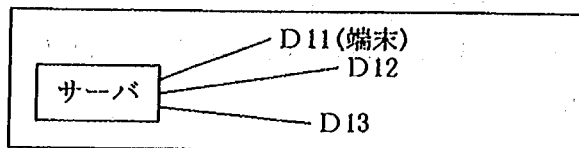
[例] 鈴木一郎 : T H 0 1 0 1 2 3
鈴木次郎 : K T 0 5 0 2 2 2
鈴木次郎 : K K 0 3 0 0 5 0

管理連番
ドメイン番号(事務所番号)
識別記号(地建名)

(2) ドメイン構成とアカウント

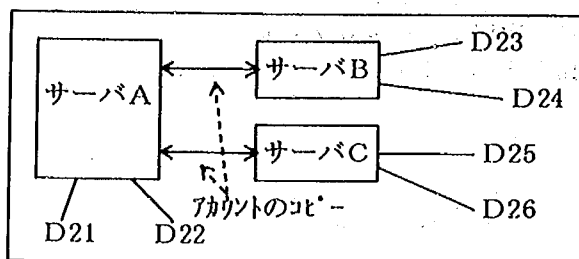
コンピュータネットワークでは、ひとつのドメイン（管理領域）に複数のファイルサーバなどを共存させて協調動作をさせる場合が多い。この場合、あるサーバに対してユーザがアカウントを獲得すれば、ドメイン内の他のサーバには再度ログインすることなく、そのまま使用できるように設計することが望ましい。実現可能なイメージを図5. 2. 1に示す。

(7) 単体サーバのドメイン



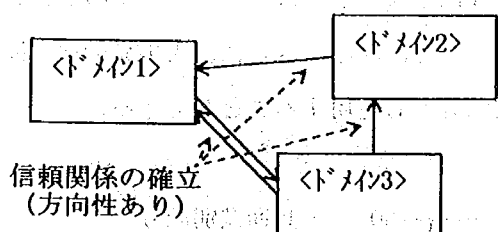
- ・単一サーバに複数の端末が接続

(4) 複数サーバのドメイン



- ・複数サーバに複数の端末が分割接続
- ・サーバBでアクセス権を得れば、サーバA/Cにアクセス可能

(5) 複数ドメイン間の連携



- ・ドメイン間で信頼関係を結び、アクセス権を継承
- ・ドメイン2のサーバでアクセス権を得れば、ドメイン1のサーバにアクセス可能
- ・信頼関係は隣接間だけ有効であり、中継は不可 (<ドメイン2->1->3は不可)

図5. 2. 1 アカウントとドメイン

(3) アクセスレベルの設定

ユーザID/パスワードによりアカウントを得ると同時に、ファイルに対するアクセスレベルを設定して、システムのセキュリティを高めるのが一般的である。システム管理用ファイルの新規作成・変更・削除や、ユーザアカウントファイルの読み込みなどは、システム管理者である特権ユーザにしかアクセスできなくしなければならない。ネットワーク管理者は、アカウントおよびファイルのアクセスレベルの設計・管理を適切に行わなければならない。一般的なアクセスレベルの分類を、表5. 2. 1に示す。

表5. 2. 1 アクセルレベルの分類

レベル	ファイル制御 (作成/削除/変更)	データ変更 (Write)	データ照会 (Read)
1	可能	可能	可能
2	不可	可能	可能
3	不可	不可	可能
4	不可	不可	不可

5. 3 電子メールアドレス管理

電子メールを使用するためには、ユーザ毎の電子メールアドレスが必要となる。電子メールアドレスに重複があると、希望する宛先に正しくメッセージが届かなくなり、運用上およびセキュリティ上においても大きな問題が発生する。

(1) メールアドレスの構成

メールアドレスはドメイン名として表現される。ドメイン名はピリオドで区切られた部分の名前から構成され、全体としてツリー構造を持つ。ドメイン名は右から左の順で責任が委譲されていることを示し、物理的な相互接続の形式とは無関係である。また、ドメイン名がひとつのIPアドレスを示すものではなく、それぞれのツリーの名前を管理するサーバに中継されることを意味する。

〔例〕 `suzuki@gate.abc.co.jp`

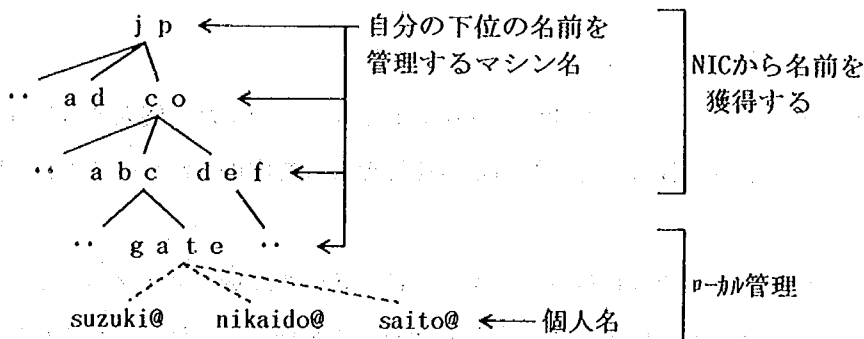


図 5. 3. 1 メールアドレスの構成

(2) メールアドレスの管理

同一組織内における人事異動が頻繁に行われる環境において、その度に電子メールアドレスに変更が発生するようなシステム設計を採用した場合は、電子メールアドレスの重複発生の要因にもつながる。また、アドレスの重複がなくても、新旧アドレスの周知徹底は難しく、結果として別ユーザにメールが届くことにもなりかねない。大規模ユーザのネットワークほど、メールアドレスの変更が発生しない設計にすることが重要である。メールアドレスの設計方法の例を以下に示す。

① サーバに対応したドメイン名の付与

メールサーバの配置に従い、ドメイン名のピリオドで区切られた名前を与える。

この場合、各メールサーバではDNS (Domain Name System: ドメイン名とIPアドレスの対応管理システム) と連携を取りながらメール配送プログラム (MTA: Mail Transfer Agent) を動作させればよい。

また、個人名の部分は最終サーバ名の下での重複がないように管理すればよく、名前を使用したユーザIDと同様の概念で与えることができる。

[例] suzu@jimuso02.tiken1.kensetu.go.jp

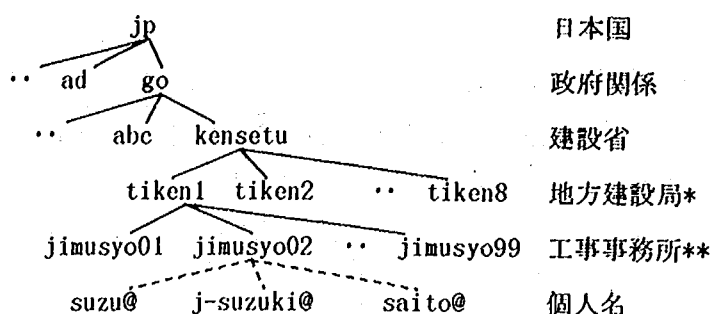


図 5. 3. 2 サーバに対応したドメイン名の付与

本方式で問題になるのは、人事異動による接続ドメインの変更が発生した場合は、ドメイン名の変更および個人名の見直しなど、メールアドレスの変更が発生する。また、アドレスの変更に伴い、内部／外部へのアドレス変更を連絡しなければならない。

② 共通ドメイン名と個人名の付与

メールサーバの配置に関係なく、共通のドメイン名を与える。また、個人名の部分は最終サーバ名の下での重複がないように管理すればよく、社員番号や管理番号を使用したユーザIDと同様の概念で与えることができる。

この場合、各メールサーバではDNSと連携せずに、メール配送プログラムとして使用実績ある sendmail などだけを使用して個人名に対応したテーブルを保持し、テーブルにしたがって順次中継することになる。

本方式の問題点としては、人の異動に伴うメールサーバのテーブル変更が必要となることである。

[例] go001234@kensetu.go.jp

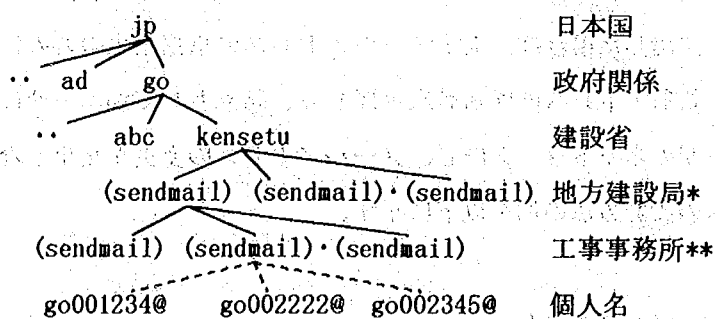


図 5. 3. 3 共通ドメイン名と個人名

6. セキュリティ管理手法

LANや、WANを介してLANを接続した広域ネットワーク上では、全てのコンピュータがネットワークサービスを共有できる。ネットワークサービスとは下記の機能などをいう。

- ・ telnet : ネットワーク上の他のコンピュータにログインできる
- ・ FTP : ネットワーク上の他のコンピュータにあるファイルにアクセスできる
- ・ 電子メール : ネットワーク上の他のコンピュータとメッセージ交換できる

ネットワークでコンピュータ同士を接続することは非常に便利な反面、予期せぬ第三者からの侵入の危険性が高いことになる。こうした侵略行為に対して、セキュリティを強化することは重要である。

6. 1 ネットワークの危険性

ネットワーク上には、機密情報やプライバシー情報などの内部情報のほかに共有データベースなどの重要情報が存在する。

これらの中には、ローカルネットワーク内と言えども、全ての人が自由にアクセスできる情報ばかりではなく、アクセス制限などのセキュリティ管理が必要な情報もある。

一般的に、どのような危険性があるかを以下に示す。

(1) 情報への侵入

パスワードの不正入手によるサーバへのアクセスが可能となれば、次の操作は簡単に行うことができる。

① 閲覧

機密情報やプライバシー情報を不正入手することができる。この情報の利用のされかたによっては、その影響度は計り知れない。

② 改ざん

情報の意味を知っている侵入者は、特定の情報を改ざんすることで、通常利用者への混乱や不利益を与えることができる。

③ 破壊

情報の破壊は、通常利用者に混乱を与えるばかりでなく、情報の再構築には大きな手間とコストが発生する。

(2) システムへの妨害

ローカルネットワークの安定稼働を妨害する侵入者もある。

① 過負荷状態

電子メールを大量に送りつけると、サーバが過負荷状態となり、通常動作が行えなくなる事態が発生する。また、サーバ内のメモリ不足が発生し、システムダウンにつながることもある。

本ケースは、パスワードの不正入手が無くても可能である。

② システムダウン

コンピュータ・ウイルスを持つプログラムを送りつけ、無制限に増殖したり、システムプログラムを破壊したりして、システムダウンに追い込むことができる。

(3) ネットワーク上を流れる情報への介入

ネットワーク上を流れる情報への介入としては、情報の流れを止めることなく、かつ利用者に気づかれないうに行われることになる。

① 盗聴

ネットワーク上を流れる情報を盗聴し、不正入手することができる。

② 改ざん

ネットワーク上を流れる情報の一部を改ざんし、誤った情報を流すことができる。

③ なりすまし

他のコンピュータになりすまし、偽りの情報を流すことができる。

6. 2 ネットワーク構成によるセキュリティ管理

6. 2. 1 ネットワーク階層化によるセキュリティ管理

LANや、WANを介してLANを接続した広域ネットワークには、さまざまな情報を扱う部門のLANが接続される。同じ組織内であるとはいえ、情報アクセスを制限することが必要である。

(1) ブリッジ接続とルータ接続

ネットワークを構成する場合、LAN間接続装置としてブリッジによる接続方法とルータによる接続方法がある。

① ブリッジ接続

ブリッジは、ネットワークの上位プロトコルには関与せず、MACアドレスをもとにデータリンク層でパケット中継する。したがって、ブリッジで接続されたネットワークは同一ネットワークアドレスを持つことになる。

ブリッジにおけるフィルタリング機能もあるが、基本的にはMACアドレスや上位プロトコル種別（TCP/IP、Netwareなど）でフィルタリングする機能である。MACアドレス自体はコンピュータとLANとの接続ポイントを示すものであり、ネットワークの上位アプリケーションに關与したきめ細かな制御はできない。

② ルータ接続

ルータは、ネットワークアドレスとサブネット情報をもとに、ネットワーク層で中継する。

ルータにおけるフィルタリング機能には、ネットワークアドレスを使用してサブネット間の通信を制限したり、上位アプリケーション種類（Telnet、FTPなど）の指定による通信制限など、きめ細かな制御ができる。両者①、②の基本的な処理方法の違いから、セキュリティ管理が必要なネットワーク部分にはルータ接続を使用することが望ましい。ネットワークをルータで接続し、ルータによるアクセス制限を行う事によって、通常ユーザに対するセキュリティ管理としてはかなりの効果を発揮する事になる。

（2）ルータ接続によるセキュリティ管理

ルータ接続により、ネットワークを階層化構成にすれば、ある程度のセキュリティは確保できる。

ネットワーク接続ユーザに共通の情報などは独立したネットワークとし、ある部門内だけに必要なローカル情報は、外部からの通信ができないようにルータで設定することができる。

一般的なルータのアクセス制御に関する設定項目としては、送受IPアドレス、上位プロトコル種別（TCP、UDPなど）、上位アプリケーション種別（Telnet、FTPなど）の組み合わせにより行う。

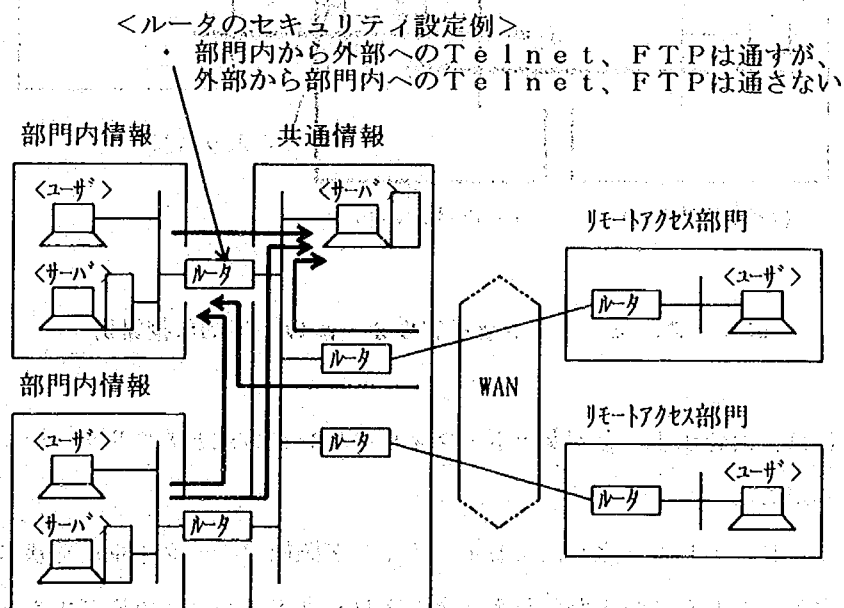


図 6. 2. 1. 1 ルータによるセキュリティ管理構成例

6. 2. 2 ファイアウォールによるセキュリティ管理

外部機関とのネットワーク接続や、インターネットとの接続におけるセキュリティ管理としては、ファイアウォール (Firewall : 防火壁) が重要視されている。

ファイアウォール構築の基本は、ローカルネットワークへの入り口を一つにすることである。入り口を一つにすることで効率的にアクセス制限することが可能となる。

さらに、ファイアウォールの外側 (インターネット側) に、外部からアクセスできるセグメント (バリア・セグメント) を設ける。バリアセグメントには、外部に公開するためのWWWサーバやFTPサーバを置くこともできる。

ファイアウォールの一般的な構築例を図6. 2. 2. 1に示す。

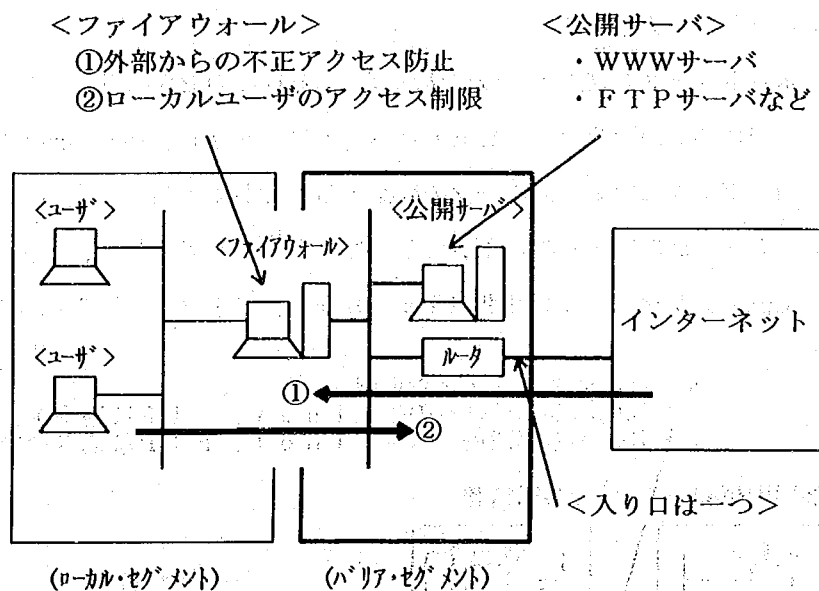


図6. 2. 2. 1 ファイアウォールの一般的な構築例

ファイアウォールには、大分類するとパケット・フィルタリング方式とアプリケーション・ゲートウェイ方式の2種類のしくみがある。

いずれの方式も、TCP/IPカーネルによるルーティング機能（ルータ中継）を基本としており、ファイアウォールに接続される両セグメントから見えるネットワークアドレスに重複があると、ルーティングできなくなる。

その他の方式も含めて以下に説明する。

(1) パケット・フィルタリング方式

IPパケットのヘッダー情報をみて、中継するかしないかを判断する方式である。中継パケットはIPヘッダーを含めてそのまま通過する。

IPヘッダーから得られる情報としては、送信元IPアドレス、発信先IPアドレス、および上位プロトコルの種類がある。これらの組み合わせにより、中継するかしないかを判断できる。

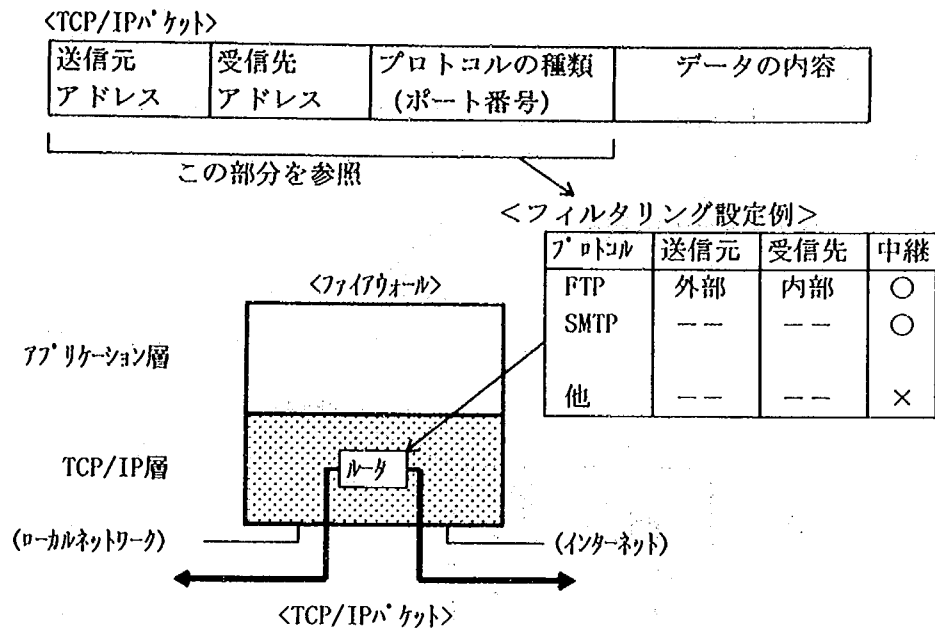


図6. 2. 2. 2 パケット・フィルタリング方式のしくみ

パケット・フィルタリング方式の特徴を以下に示す。

① 処理速度が早い

IPヘッダー情報だけにより中継判断を行うため、中継処理速度が、アプリケーション・ゲートウェイ方式に比べて早い。

② 同時アクセスユーザ数に制限がない

ルータ機能と同様にIPパケットをそのまま中継するだけであり、同時アクセスユーザ数に制限がない。

③ ユーザの使い勝手がよい

ユーザから見ればファイアウォールの存在を意識することなく、インターネットに直接通信できる。したがって、ユーザの使い勝手がよい。

④ セキュリティ機能が弱い

フィルタリングされないで中継されるパケットは、IPヘッダーも含めてそのまま通過する。ユーザ認証はIPアドレスで行われることになる。

このとき、ユーザのIPアドレスが外部に見えることになり、このIPアドレスを詐称して外部から進入することも可能となる。

(2) アプリケーション・ゲートウェイ方式

IPパケットのプロトコル内データ情報に従い、FTP、WWWなどのTCP/IPアプリケーション毎に中継プログラムをファイアウォール上で走らせる方式である。インターネット上からは、アプリケーション・ゲートウェイだけがアクセスしているように見える。

ユーザはアプリケーション・ゲートウェイ経由で外部にアクセスすることになる。このとき、専用のクライアント用ソフトウェアを使用するものもある。

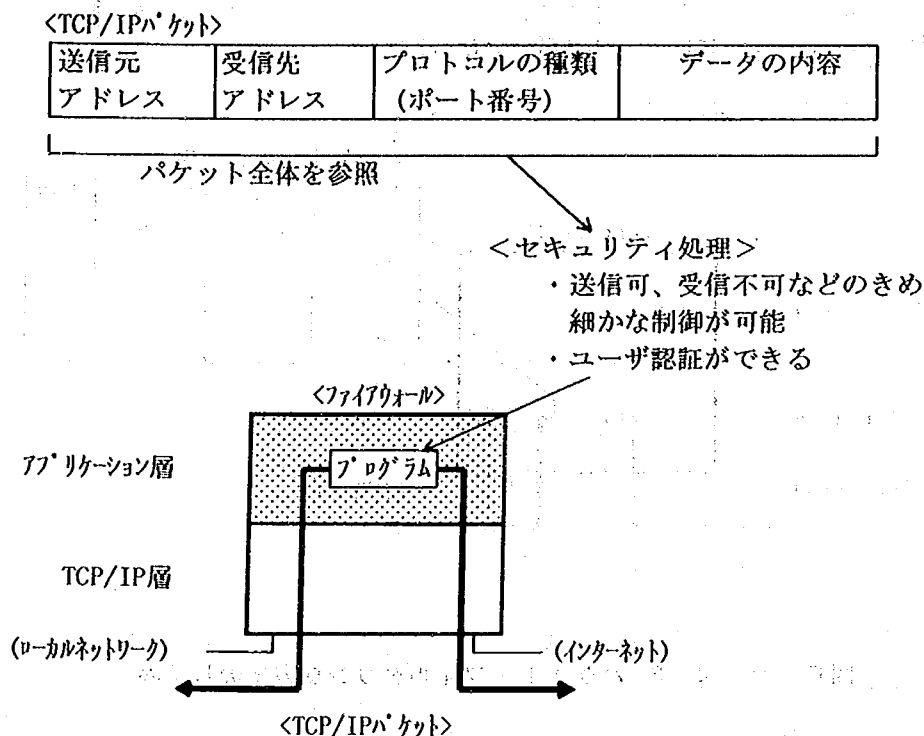


図6.2.2.3 アプリケーション・ゲートウェイ方式のしくみ

アプリケーション・ゲートウェイ方式の特徴を以下に示す。

① きめ細かなセキュリティが可能

TCP/IPのアプリケーション毎に中継プログラムを走らせるため、アプリケーション毎に送信可、受信不可などの、きめ細かなセキュリティ制御が可能となる。

② IPアドレスが外部に漏れない

アプリケーション・ゲートウェイを経由するとき、アプリケーション・ゲートウェイ自身のIPアドレスで外部と通信できるため、IPアドレスが外部に漏れない。

このことは、グローバルでないIPアドレスを、ローカルネットワークで使うことができることも意味する。

③ セキュリティ機能が強い

アプリケーション・ゲートウェイでは、ユーザID／パスワードの認証をおこなうこともできる。

④ 処理速度が遅い

TCP/IPパケットのデータ部まで入り込んでアプリケーション・プログラムで中継するため、パケット・フィルタリング方式に比べて遅くなる。

また、同時ユーザ数が多くなると中継プログラムが多数生成されることになり、極端にレスポンスが低下することもある。

⑤ 同時アクセスユーザ数に制限あり

同時ユーザ数が多くなると中継プログラムが多数生成されることになり、極端にレスポンスが低下することもある。

⑥ ユーザの使い勝手がよくない

内部サーバへのアクセス時とは別に、専用のクライアント用ソフトウェアを使用する場合もある。ユーザはファイアウォールの存在を意識する必要があり、パケット・フィルタリング方式に比べて使い勝手がよくない。

(3) IPアドレス変換方式

① アドレス変換装置

ローカルネットワークから外部にアクセスする場合、ローカルネットワーク側のユーザのIPアドレスを別のグローバルアドレスに変換してルータ中継する方式である。

変換装置では、いくつかのインターネット接続用グローバルIPアドレスを管理し、ローカルユーザからの要求に応じてダイナミックに空きIPアドレスを割り当てて使用する。基本的には、IPアドレスとしてローカルアドレス（独自アドレス）を使用しているユーザが、インターネットに接続する場合のアドレス変換装置として使用される性格を持つ装置である。ただし、ローカルアドレスと重複したIPアドレスを持つインターネット上のサーバには、アクセスできない。本方式では、外部からのアクセスは全て排除されるため、ファイアウォールとしても機能することになる。

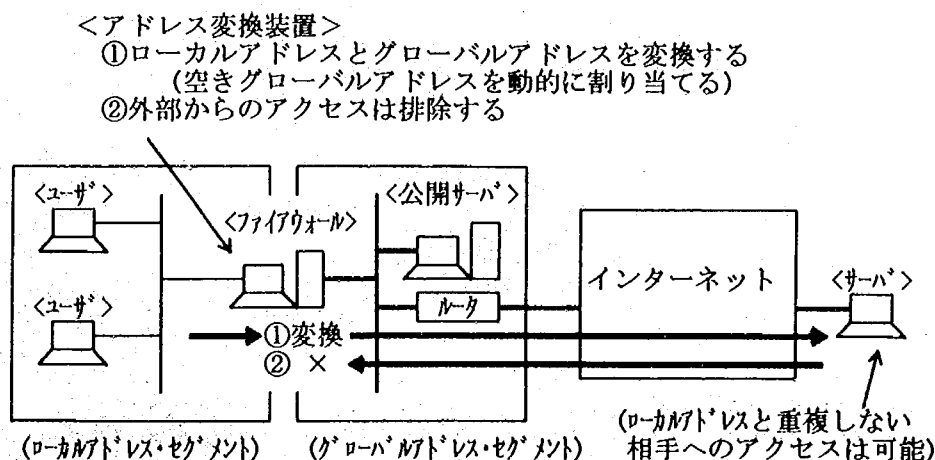


図6. 2. 2. 4 アドレス変換装置のしくみ

② プロキシ・サーバ

アドレス変換装置では外部のアドレスが重複するサーバとの接続はできないが、プロキシ・サーバはそれを可能にする機能を持つ。

ローカルアドレスを持つユーザから、プライベートアドレス上のプロキシ・サーバに一度ログインする。プロキシ・サーバでは、ユーザからの要求に従い、プライベートアドレスを使用して代理でインターネット上のサーバと通信する。このとき、グローバルアドレス上にあるファイアウォールを経由して外部と接続する3段階の方式となる。

ただし、ローカルアドレスの中にプライベートアドレスが含まれないことがここでの前提条件となる。

< 3段階の処理 >

- ① ユーザはプロキシ・サーバにログインする
- ② プライベートアドレスに変換し、代理でファイアウォール経由でインターネットにアクセスする
- ③ グローバルアドレスに変換されてインターネットに送出する

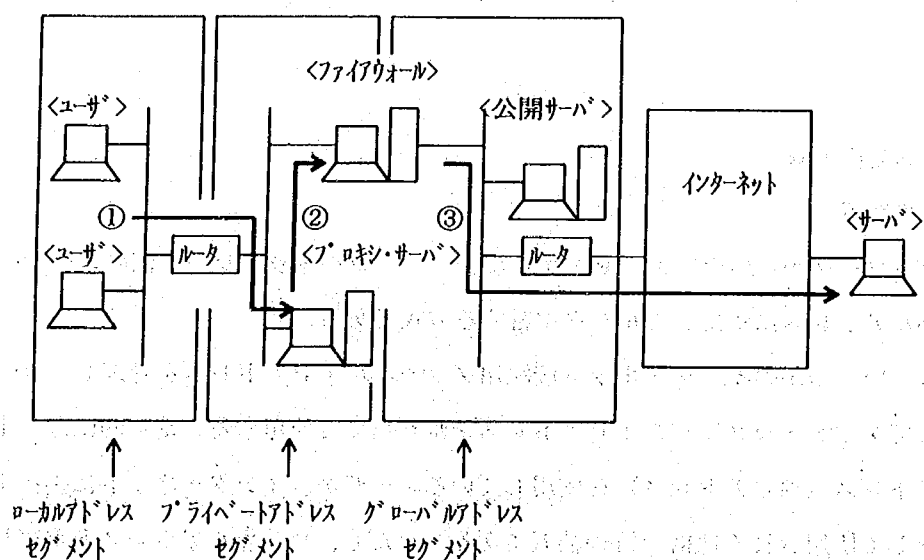


図6. 2. 2. 5 プロキシ・サーバのしくみ

6. 3 パスワードによるセキュリティ管理

6. 3. 1 パスワードの保護

機密情報やプライベート情報などの一般に公開できない情報へのアクセス制限方法として、ユーザID／パスワード認証によるアカウント（利用権）を必要とするセキュリティ管理機能を実装する。

このパスワードを不正な手段で入手すればアカウントを破ることができ、不正に情報を入手することができる。

(1) パスワードファイルを盗まれないようにする

UNIXシステムにおいてはユーザのパスワードファイル（/etc/passwd）を盗まれないようにしなければならない。

たとえば、TFTP（Trivial FTP）などの簡易ファイル転送プロトコルの設定を間違えると、ネットワーク経由で外部から任意のファイルを取得することができる。このようなセキュリティホール（OSのバグや運用上のセキュリティの穴）がないようにチェックすることが必要である。

(2) パスワードを解読されないようにする

パスワードファイルが盗まれても、簡単には解読されないパスワードを設定することが必要である。

UNIXのパスワードは、8文字までの文字列を暗号化してパスワードファイルに保存しておく。ユーザが入力したパスワードを認証するには、同じ暗号化を適用して、登録済み暗号化パスワードと比較する。侵入者は、たとえば辞書に載っている文字列を次々に暗号化し、暗号化パスワードと比較する。

安易なパスワードは簡単に解読されることになり、次に示すように、できるだけ解読されにくいパスワードを設定するように注意しなければならない。

- ① 辞書にない文字列を選ぶ
- ② 辞書にある文字列に1文字付け加えたり、順序を入れ替えたり
2つの単語を合成したものは使わない
- ③ 日本語は使わない
- ④ 人名、地名などは使わない

6. 3. 2 パスワードの弱点

パスワードの最大の弱点は、パスワードそのものが平文（生の入力データ）のままでネットワーク上を流れることである。その危険性と対応策を以下に示す。

(1) ネットワーク・モニタ

ネットワーク上を流れるデータをモニタする機能をネットワーク・モニタという。ネットワーク上を平文で流れるデータをモニタすれば、パスワードの盗聴が可能となる。

UNIX上でのパケットモニタリングできるプログラムはSnifferと呼ばれる。また、LANアナライザなどを接続すれば、同様に全てのデータをモニタすることにもなる。ただし、それぞれ下記の特徴があり、対策は可能である。

① UNIX上でのモニタ

UNIX上でSnifferを動作させてモニタできるのは、そのワークステーションが接続されているセグメント上を流れるデータである。

外部ユーザによるモニタ方法は、パスワードを不正に入手し、ワークステーションの特権ユーザの権利（root特権）を獲得してSnifferプログラムを走らせるケースである。この場合でもパスワードの保護を正しく行えば、防ぐことができる。

内部ユーザに対しては教育による指導を行う必要がある。

② LANアナライザでのモニタ

LANアナライザでモニタできるのは、LANアナライザを接続したセグメント上を流れるデータである。外部ユーザはLANアナライザを持ち込んでモニタすることは不可能に近い。内部ユーザに対しては教育による指導を行う必要がある。

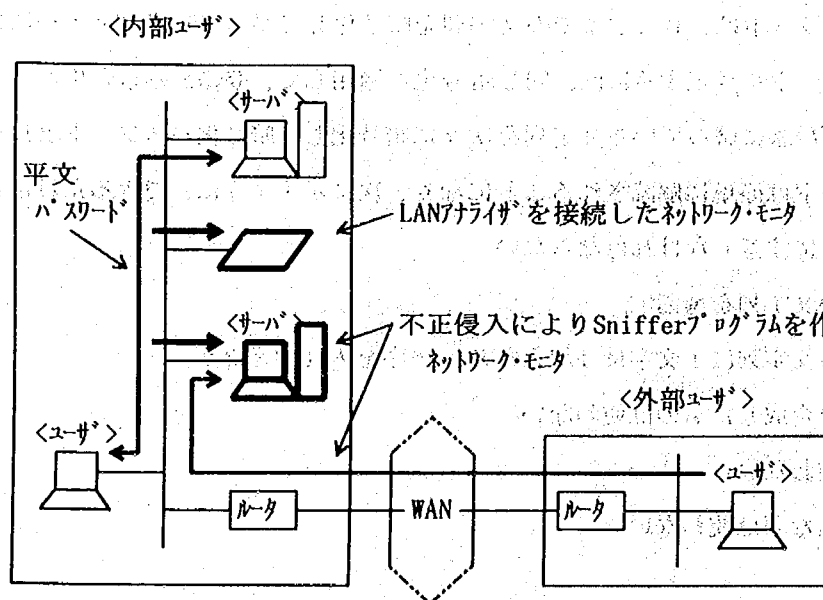


図6.3.2.1 パスワードの弱点

(2) パスワードの暗号化

パスワードが平文のままネットワーク上を流れないようにする工夫としては、パスワードを管理するサーバでランダムに作成した文字列をクライアントに送る方法がある。クライアント側はサーバから受け取った文字列を、専用の符号化用端末で変換し、この結果をサーバに送り返す。サーバ側ではこれを照合し、認証を行う。

6. 4 暗号化技術によるセキュリティ管理

ネットワークが限られた部門内だけの範囲で構築されている間は、暗号化はそれほど重要視されていなかった。しかし、インターネット接続による商用利用が盛んになるにつれ、セキュリティ技術は必要不可欠となり始めている。

(1) 暗号化の重要性

たとえば、電子メールによる商品注文では、クレジットカードの番号と商品名を送ると、通常の手続きよりも早く購入できる。通常、電子メールのメッセージは何も暗号化されないまま配送される。このため、なんらかの方法で電子メールを盗聴すれば、盗聴したクレジットカード番号を使用して商品を購入することも可能となる。

重要な情報をそのまま通信回線で送ると、次の危険性があることを覚悟しなければならない。

- ① 盗聴 ----- 内容が第三者に読まれてしまう
- ② 改ざん ----- 違った内容が相手に届く
- ③ なりすまし ----- 誰かの振りをして誤った情報を送る

これらの危険を回避するために、「盗聴」に対抗する暗号化技術、「改ざん」「なりすまし」に対抗する認証技術が重要視されている。

(2) 暗号化の基本理論

コンピュータが無い時代の暗号化は、乱数を使用したり、文字を一定のルールで入れ替えたり、特別な文字や絵文字に置き換えたりしていた。

インターネット上では、絵文字を送るわけには行かず、「鍵」を使用すれば暗号化／復号化は優しいが、暗号化された情報から「鍵」を解読するには、コンピュータ処理においても数十年以上費やすような理論の暗号処理が採用されている。

6. 4. 1 共通鍵方式 (DES)

「共通鍵方式」(秘密鍵暗号方式、対称暗号方式、慣用暗号方式などとも呼ばれる)は、現在最も普及している暗号方式であり、データの暗号化/復号化に同じ鍵を使う。

(1) 特徴

本方式では、送信者/受信者が「共通鍵」を持ち、送信者が送信時に「共通鍵」を使用して暗号化し、受信者は同じ「共通鍵」を使用して復号化する。

本方式には以下の長所がある。

- ① 暗号アルゴリズムが比較的単純
- ② 処理速度が高い

また、本方式には以下の短所がある。

- ③ 「共通鍵」を事前に送/受信者が持ち合わせなければならない
- ④ 通信相手の数だけ「共通鍵」を持たなければならない
- ⑤ 「共通鍵」の厳重な管理が必要

(2) 製品例

本方式の基本となっているのは、米IBMが開発し、77年に米国の標準暗号方式になった、

- ① 米標準: DES (Data Encryption Standard)

である。米国では暗号製品は戦略物資に指定されているために輸出制限がかかる。ただ、暗号アルゴリズムは一般に公開されているため、米国外のメーカーがDESベースの製品を開発したことが普及した大きな理由である。

日本でのDESベースの製品を以下に示す。

- ② NTT: FEAL (Fast data Encipherment Algorithm)
- ③ 富士通: DESAF (Data Encryption Service Advanced Facility)
- ④ 日立: MULTI 2

(3) 鍵とは

データを暗号化/復号化するために必要な数十~数百ビットのデータを鍵という。

DESは56ビット、FEALは64または128ビットである。

(4) DES方式とは

平文を64ビット毎のブロックに区切り、ブロック毎に鍵でかき混ぜて64ビットの暗号文を生成するブロック暗号方式である。転置(データの順序をブロック内で入れ替える)と換字(データを他のデータに替える)を適当に組み合わせた処理を数十段(ループ)繰り返す。

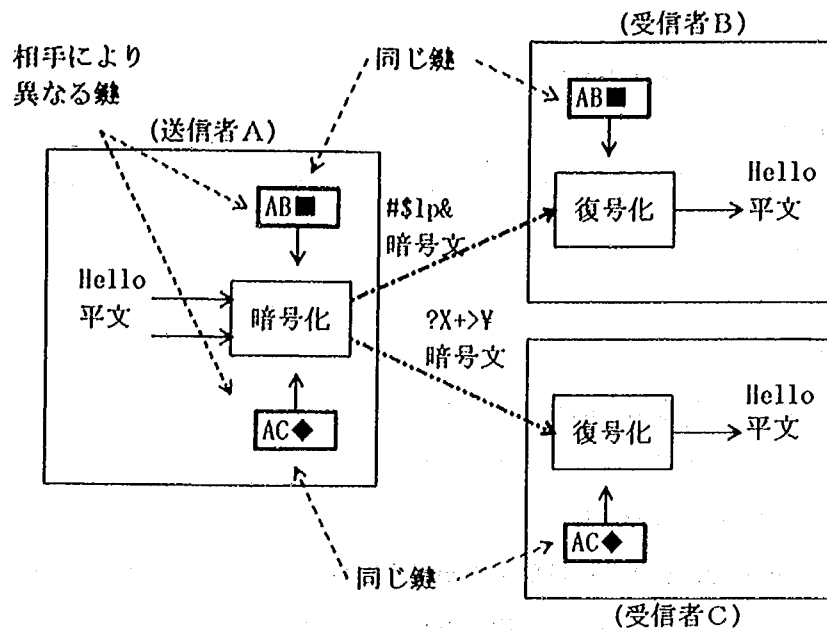


図 6. 4. 1. 1 共通鍵方式 (DES方式)

6. 4. 2 公開鍵方式 (RSA)

「公開鍵方式」はデータの暗号化と復号化に、それぞれ別の鍵を使用する。自分用の鍵として、一般に公開された「公開鍵」と、自分だけが秘密に保持する「秘密鍵」の2種類を持つ。

(1) 特徴

本方式では、通常は送信者が送信時に受信者用の「公開鍵」を一括管理センターから取得して暗号化し、受信者は自分用の「秘密鍵」を使用して復号化する。

本方式には以下の長所がある。

- ① 自分用の「秘密鍵」だけを管理すればよい
- ② 署名機能にも使用できる

また、本方式には以下の短所がある。

- ③ 処理速度が遅い
- ④ 暗号アルゴリズムが複雑

(2) 製品例

本方式の代表例としては下記アルゴリズムがある。

・RSA (Rivest, Shamir, Adleman)

これは、Diffie-Hellman が考案した公開鍵暗号方式の理論を基に、米MITのRivest, Shamir, Adlemanの3氏が1978年に発表したアルゴリズムである。

(3) RSA方式とは

公開されている鍵から暗号情報を引き出そうとしても、莫大な時間（スーパーコンピュータでも何十兆年を要する）がかかるので、事実上は解読が不可能とされている。

RSAは次の性質を利用した方式である。

- ① 2つの大きな素数の積を計算するのは簡単だが、素因数分解するのは容易でない
- ② ある数の累乗を計算するのは簡単だが、根を計算するのは容易でない

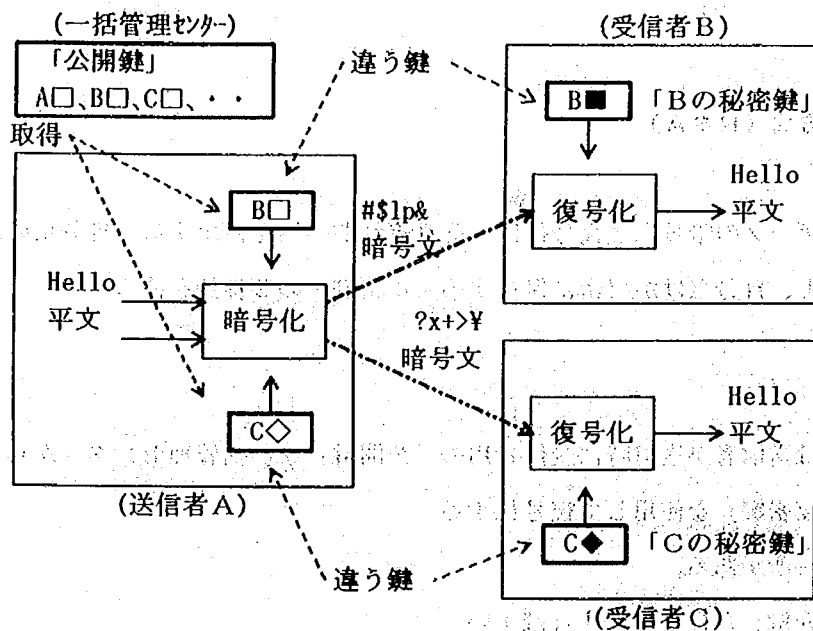


図6. 4. 2. 1 公開鍵方式 (RSA方式)

6. 4. 3 共通鍵方式と公開鍵方式の併用方式 (PEM)

(1) 共通鍵方式と公開鍵方式の比較

両方式は暗号化の基本となっているが、それぞれに一長一短がある。

両者の特質の比較を表6. 4. 3. 1に示す。

表6. 4. 3. 1 共通鍵方式と公開鍵方式の比較

	共通鍵方式	公開鍵方式
鍵の保管	相互に厳重に保管	公開してよい
鍵の保管数	相手数分の保管	自分の秘密鍵のみ保管
鍵の全体数	$1/2 \cdot n \cdot (n-1)$ 個 [100人で4950個]	$2n$ 個 [100人で200個]
暗号化の処理時間	少ない	多い
処理の複雑さ	簡単	複雑
署名機能	なし	あり
実用度	実用段階	実験段階

(2) 共通鍵方式と公開鍵方式の併用方式<ハイブリッド方式>

共通鍵方式と公開鍵方式を併用して、それぞれの長所を生かして短所を補うハイブリッド方式が考案されている。

本方式の例として、インターネット上でプライバシーを強化した電子メール「PEM」(Privacy Enhanced Mail)の開発・実装が進められている。本文の暗号化は高速なDES方式を使い、これを復号するための鍵をさらにRSA方式で暗号化する。

本方式では、以下の特徴をもつ。

- ① 本文を暗号化して内容を盗聴されるのを防ぐ
- ② 電子署名により本文の改ざんを検出できる
- ③ 公開鍵証明書を利用してユーザの認証も可能

<送信者Aの処理>

- ①ランダムに作成したDES用鍵DEK(Data Encryption Key)を使用し、DES方式で本文を暗号化する。
- ②鍵DEKそのものを送信相手Bの公開鍵を使用し、RSA方式で暗号化する。

<受信者Bの処理>

- ③B自身の秘密鍵で、送られてきた鍵DEKを復号化する。
- ④復号化した鍵DEKを使用して、本文を復号化する。

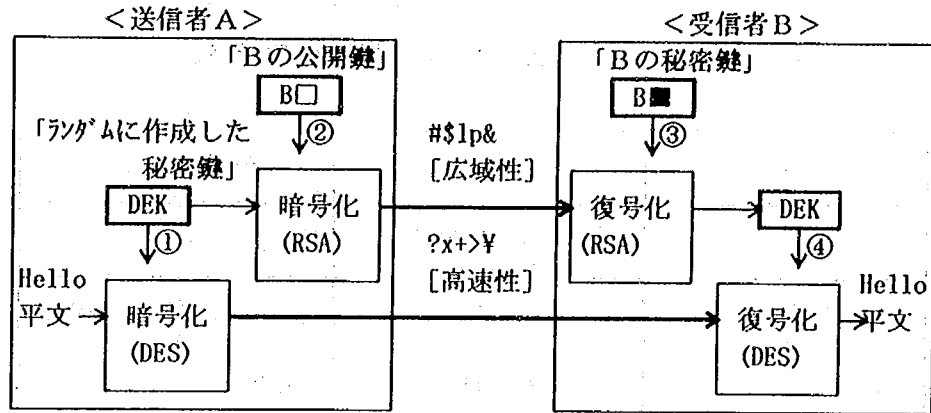


図 6. 4. 3. 1 ハイブリッド方式 (PEM方式)

6. 4. 4 電子署名

担当者が確かに目を通したことや、内容に間違いがないことを証明するために、一般の職場では、書類に押印することが多い。ネットワーク上においても商品発注や電子決済においては、電子的な認証システムは必要となる。

認証システムに必要な機能は、次の2つである。

- ① 本人にしか作成できないメッセージを作成する署名機能
- ② 本人が書いたことを証明する認証機能

これらの機能は電子メールのPEMにも組み込まれている。

通常のメールは、送信者が送信時に受信者用の「公開鍵」を一括管理センターから取得して暗号化し、受信者は自分用の「秘密鍵」を使用して復号化する。これは受信者しか読めないようにするために行う。

電子署名では上記とは逆に、署名情報を送信者が送信時に自分用の「秘密鍵」を使用して暗号化し、受信者は送信者用の「公開鍵」を一括管理センターから取得して復号化する。これは、送信者本人しか作成できないことを意味する署名機能となる。図 6. 4. 4. 1 で、PEMにおける電子署名の概念を示す。

DESで暗号化して送られたメールから作成したダイジェストと、Aしか知らない「Aの秘密鍵」で暗号化して送られたダイジェストが一致したら、そのメールは間違いなくAから送られてきたものであり、途中での「改ざん」や「なりすまし」がないと言える。

<送信者Aの処理>

- ①図6. 4. 3. 1と同じ
- ②図6. 4. 3. 1と同じ
- ⑤本文をハッシュ関数という特殊関数で圧縮し、メッセージ・ダイジェストと呼ぶ数値を算出する。
- ⑥メッセージ・ダイジェストを、送信者Aしか知らない「Aの秘密鍵」で暗号化する。

<受信者Bの処理>

- ③図6. 4. 3. 1と同じ
- ④図6. 4. 3. 1と同じ
- ⑦「Aの公開鍵」で送られてきたメッセージ・ダイジェストを復号化する。
- ⑧送信者と同じハッシュ関数を使用して、メッセージ・ダイジェストを作成する。
- ⑨両方のメッセージ・ダイジェストを比較する。

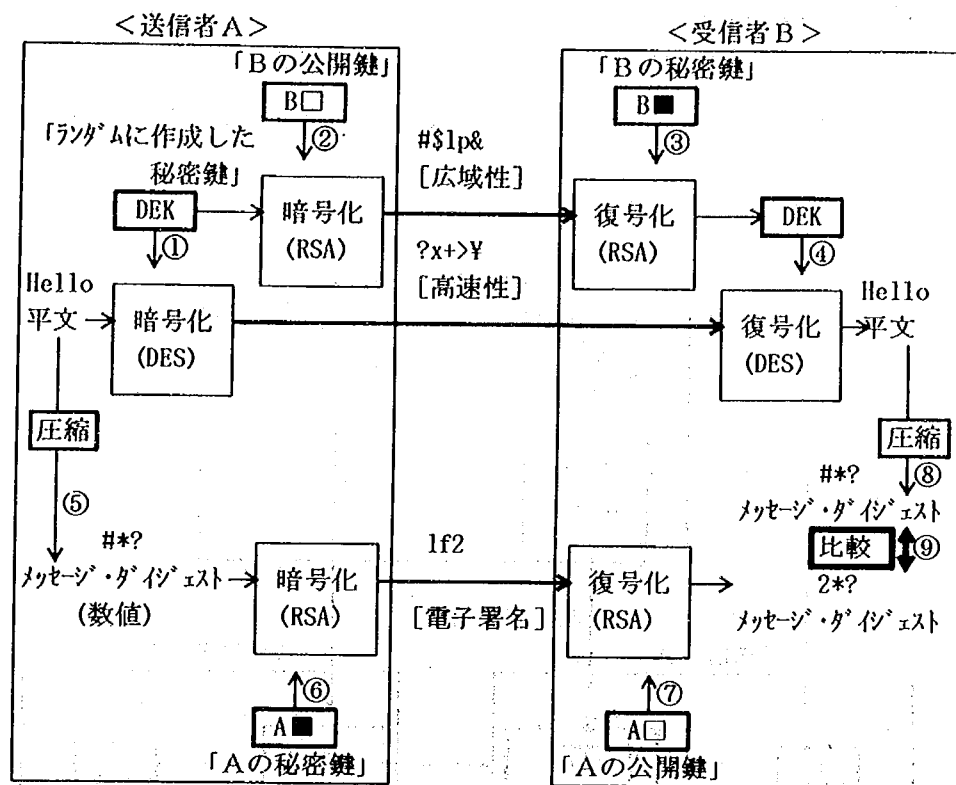


図6. 4. 4. 1 PEMの電子署名

6. 4. 5 公開鍵証明書

「盗聴」と「改ざん」は前記の方式で防止できるが、「なりすまし」は公開鍵の管理をおろそかにすると別の危険の可能性がある。

たとえば、図6. 4. 4. 1において不正ユーザCが、ユーザAの公開鍵を偽りの鍵に置き換えた場合、受信者Bは不正ユーザCとのやりとりをユーザAとのやりとりであると認識することになる。

こうした不正行為を防止するために、PEMには正規の公開鍵であることを示す「公開鍵証明書」という概念がある。[公開鍵証明書発行局] といゆ信頼できる発行局を設け、ユーザが自分の公開鍵を登録して「公開鍵証明書」を発行してもらう。「公開鍵証明書」は[公開鍵証明書発行局]の秘密鍵で暗号化されている。本機能は現在は実験段階である。

使い方は、送信者が電子メールを送る時に、暗号文とともに「公開鍵証明書」を添付して送信する。受信者は[公開鍵証明書発行局]の公開鍵で、送られてきた「公開鍵証明書」を復号化して公開鍵を取得し、署名を復号化する。

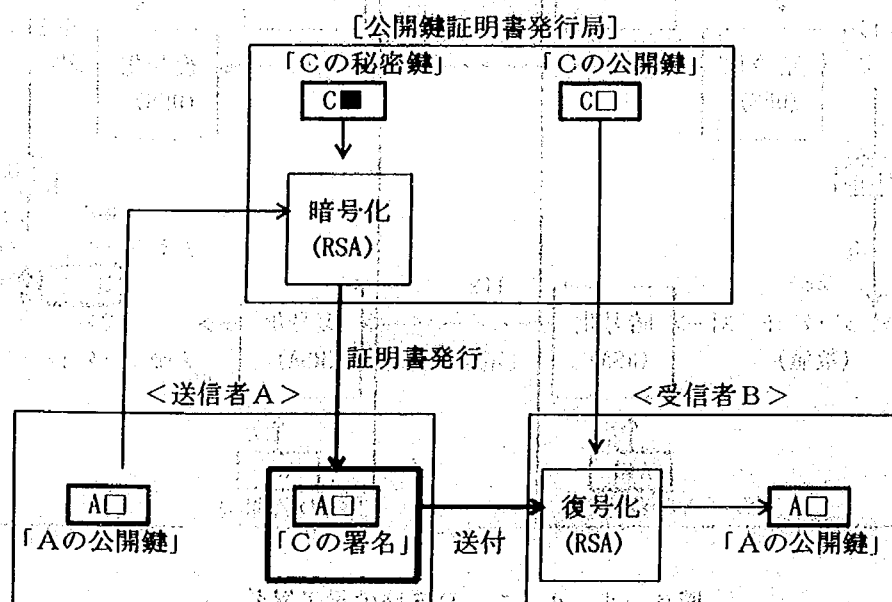


図6. 4. 5. 1 公開鍵証明書

6. 5 セキュリティ教育

セキュリティ管理としては、ユーザ教育も重要な管理方法のひとつである。システム構成上で十分なセキュリティ対策を施したとしても、肝心のユーザのセキュリティ意識がなければ、効果が発揮できなくなることもある。

ユーザ教育は、一般ユーザ向けの教育とネットワーク管理者向けの教育の2種類に分類できる。

(1) 一般ユーザ向けのセキュリティ教育

① パスワードを正しく設定する

ユーザに求められる最大のセキュリティ対策は、パスワードの設定である。通常は、パーソナルコンピュータを使用しているユーザのパスワード使用は行われておらず、慣れないままにパスワード設定すると次のような危険なパスワードを設定することが多くなる。

- ・ログイン名と同じパスワード
- ・性がログイン名で名がパスワード
- ・生年月日
- ・親族の名前
- ・所属している組織の名前や略号
- ・自分の興味があることから付けたもの
- ・よく知られている単語

安全なパスワード設定に関する教育を徹底する必要がある。

② パスワードを漏洩しない

急ぎの仕事の場合に、パスワードを他人に教えて手伝ってもらう場合もある。これも危険な行為であり、注意が必要である。教えた場合は、早い時期にパスワード変更することを忘れてはならない。

③ 個人ファイルのセキュリティ管理

個人が管理している情報（ファイル）の最低限のセキュリティを確保することが必要である。通常は個人でしか参照できないようにするが、作業中のファイルをテンポラリ領域に置く場合、誰にでも見られる状態となり、情報の漏洩の原因となる。

④ 電子メールで送る内容

万一の盗聴や、宛名を一文字間違えて誤った相手に届くという事故の可能性もあり、電子メールでは、機密性の高い情報は送ってはならない。

(2) ネットワーク管理者向けのセキュリティ教育

① セキュリティに対する考え方

セキュリティに対する基本的な考え方を教育する。

② セキュリティ確保の方策

セキュリティ確保の具体的な方策を細かく教育する。

③ ネットワーク侵入手口

ネットワーク侵入手口とその脅威を教育する。それを理解した上での侵入対策は効果的となる。

④ コンピュータ室への入出管理

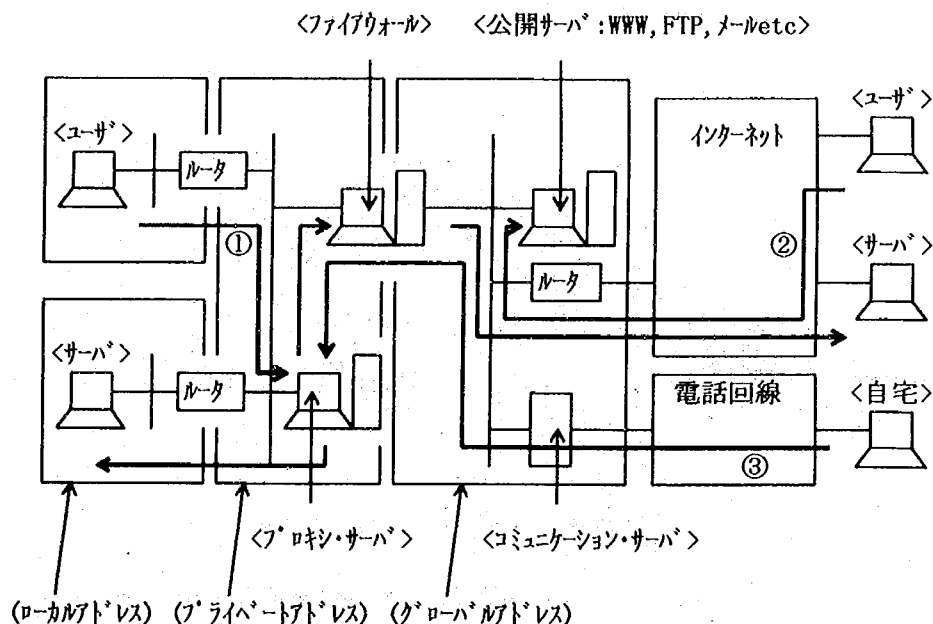
重要なデータの保管をしているコンピュータ室では、データの閲覧が容易な場合が多い。コンピュータ室への入出管理を徹底し、セキュリティを確保する必要がある。

7. 今後の課題

ネットワーク管理は、ネットワークの運用と保守を含めたものであり、その目的は、ネットワークシステムの安全かつ円滑な運用を保証することである。ネットワーク管理にあたっては、各種の情報を管理し、ノウハウを蓄積する必要がある。

本年度は、建設省専用通信回線とインターネットとの接続を考慮したネットワークのあり方について調査し、とりまとめを行なった。

今後は、図7. 1に示すようなテストシステムを構築して、建設省専用通信網におけるネットワークのインターネット接続を想定した実験を行ない、ルーティングプロトコル及びネットワーク管理プロトコルの検討を行なわなければならない。そして、机上検討では予期できないネットワークのストレスやエラー等についても実験を行なう必要がある。また、インターネット接続により、外部と通信だけでなく、同一のアプリケーションを使用して、自営ネットワーク内部で通信する業務利用形態についても重要な利用方法として検討していく必要がある。



- ① ユーザはプロキシ・サーバにログインし、プロキシ・サーバが代理でファイアウォール経由でインターネットにアクセスする
- ② インターネット・ユーザは、公開サーバまでアクセスできる
- ③ 自宅からプロキシ・サーバにログインし、代理でローカルサーバにアクセスする

図7. 1 テストシステムの構成案