マルチメディア通信と分散処理 30－10
（１９８６．７．２５）

セキュリティ機能を持ったゲートウェイの開発

田中幹夫　石沢良一
情報処理振興事業協会

異種ネットワークの相互接続に際し、ネットワーク内の情報資源を、そのセキュリティを確保しつつ外部に提供する為の機能要件と方策について考察する。そしてＵＮＩＸ系ネットワークとメイン・フレーマー系ネットワーク（ IPACS = ACOS+HITAC+FACOM ）とを相互接続した環境にて、そのプロトタイプを開発した結果を紹介する。

ここでは、SUN ワークステーションを両者間のゲートウェイとして使用し、そこにネットワーク間認証機能、アクセス権制御機能、資源管理機能、自動アクセス機能、ネットワーク接続監視機能等を実現した。これにより、UNIX側のユーザーは、IPACS の内部構造について知識を有する事なしに、要求するファイル名のみでIPACS 内ファイルを取り出す事が可能であり、かつセキュリティ上の条件のチェックも行なわれる。

A Gateway with Security Mechanisms

Mikio Tanaka , Yoshikazu Ishizawa
Information-technology Promotion Agency
3-1-38 , Shiba-koen
Minato-ku , TOKYO , JAPAN

This paper introduces a development of a gateway with security mechanisms and auto-access mechanisms, which is located between a requester-network and a server-network. And then shows its implementation as a prototype in a network of I.P.A.

This gateway offers high grade inter-network services to network users. For example users, from requester-network, can get files in a server-network easily without any information about the location of the file in the server-network. And at the same time this mechanism helps file owners to protect their secret data from unauthorized access from untrusted networks.

セキュリティ機能を持ったゲートウェイの開発

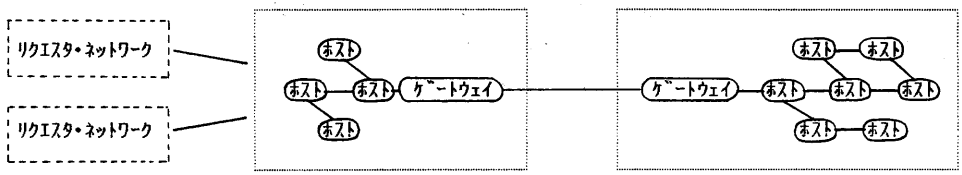
情報処理振興事業協会（ＩＰＡ）
田中幹夫　　石沢良一

［１］はじめに

今後のネットワーク利用にあたっての重要な課題の一つとして、異種ネットワークの相互接続によるネットワークを超えたサービス（以下ネットワーク間サービスとする）の実現と、その際のセキュリティ対策があげられる。（参考文献１）　ここでは、ネットワーク相互接続に際し、ネットワーク内の情報資源を、そのセキュリティを確保しつつ外部に提供する為の機能要件と方策について考察する。　そして、UNIX系ネットワークとメインフレーマー系のネットワーク（IPACS = FACOM + HITAC + ACOS）とを相互接続した環境にて、そのプロトタイプを開発した結果について述べる。

［２］ネットワーク間サービスのモデル化

あるネットワーク内の資源を外部に提供する場面を想定し、以下のようにモデル化できるものとする。



リクエスタ・ネットワーク（ユーザーが存在）　　サーバー・ネットワーク（資源が存在）

［図１　ネットワーク環境のモデル］

ここでサーバー・ネットワークとは、要求される資源が存在するネットワークであり、リクエスタ・ネットワークとは、資源を要求するユーザーが存在するネットワークである。リクエスタ・ネットワークを複数経由して、サーバー・ネットワークに達する場合もあるものとする。

ネットワークとは、ある運用管理体制のもとで複数のコンピュータが結合したものを想定しているが、単一コンピュータの場合でも同様である。　ゲートウェイは、他ネットワークとの接点に位置しているものであるが、一般のホストが兼ねる場合も有る。

このモデルでは、以下の項目を基本的な前提とする。

＊ネットワーク内の一般ホストは、自ネットワーク以外のユーザーに関する知識、他ネットワークの内部構造に関する知識（資源のアドレス、アクセス手順等）を有しない。

＊ネットワーク内の一般ホストの通信機能としては、隣接ホストとの仮想端末機能程度である。

＊リクエスタ・ネットワークのユーザーは、要求するサービスを受ける為にサーバー・ネットワークに接続されているゲートウェイに、仮想端末機能等によってセッションを開設するものとする。

［３］ネットワーク間サービスの機能要件

上記のようなモデルで、ネットワーク間の情報提供サービスを実現する為に必要な機能要件の整理を試みる。

（１）サーバー・ネットワーク側ゲートウェイに必要となる機能

(1-1) プロトコル変換機能

基礎的コミュニケーションを実現する為のプロトコル変換の機能。

(1-2) 接続ネットワーク認証機能

サーバー・ネットワークに接続されうるネットワークを特定化する機能。

(1-3) 外部アクセス権制御機能

要求されるサービス名と要求者側情報に基づいて、サーバー・ネットワーク内の資源別に、それにアクセスできる外部ユーザー、外部バスを限定する機能。

(1-4) 資源管理機能

ユーザーの要求する資源名（外部からみた資源名）をサーバ・ネットワーク内での資源名に翻訳し、所在情報を提供する機能。

(1-5) アクセス手順管理（自動アクセス）機能

ユーザーの要求する資源へアクセスする為のサーバー・ネットワーク内の手順を提供する機能、あるいは自動アクセスを行なう機能。

(1-6) 接続ネットワーク監視機能

外部ネットワークとの接続を監視、モニタする機能。

（2）リクエスタ・ネットワーク側ゲートウェイに必要となる機能

(2-1) プロトコル変換機能

基礎的コミュニケーションを実現する為のプロトコル変換の機能。

(2-2) 接続ネットワーク認証機能

リクエスタ・ネットワークに接続されるネットワークを特定化す機能。

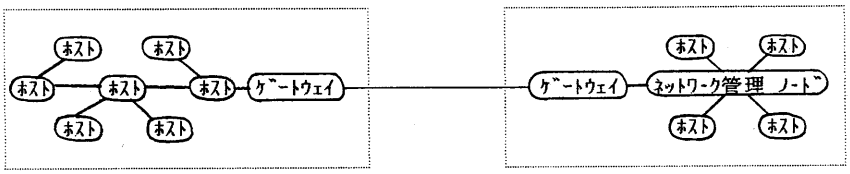
(2-3) 要求するサービスの内容のサーバー側への伝達機能

ユーザーの要求するサービス名（読み出したいファイル名等）をサーバーへ伝達する機能。

(2-4) 要求者側情報の、サーバー側への伝達機能

ここで要求者側情報とは、サーバー・ネットワーク側でアクセス権を決定する為に必要となる、ユーザーに関する情報、及びアクセスに使用しているバスに関する情報である。

前章のような前提の結果、サーバー・ネットワーク側のゲートウェイに担わせる機能はかなり拡張されている。 (1-1) は通常言われている基本的ゲートウェイ機能と言えよう。 (1-2) はセキュリティ確保の為のネットワーク間の認証機能である。 (1-3) (1-4) (1-5) はサーバー・ネットワークのネットワーク管理の機能とも解釈できる。 なお、サーバー・ネットワークがネットワーク管理ノードを持っており、そこで集中的にネットワーク内の資源管理、アクセス手順管理等が実現されていれば、(1-3) (1-4) (1-5) 等は、このノードに担わせる事が可能となる。その場合は、［図２］のような形態となり、ゲートウェイの負担は小さくなる。



リクエスタ・ネットワーク（ユーザーが存在）　　サーバー・ネットワーク（情報資源が存在）

［図２　ネットワーク管理ノードを持つ場合のモデル］

現実問題として、このようなネットワーク管理ノードを装備している例は少ないと思われる。 サーバー・ネットワーク内にネットワーク管理ノードを設けるか、ゲートウェイに負担させるかは、ネットワークの規模、性質によって、選択されるべきであろう。以下では［図１］のモデルで想定する。

［４］セキュリティ機能の段階的実現

上記のように機能要件を分析すると、サーバー・ネットワーク内の情報資源のセキュリティを確保する為の対策が、下記のように分担されて実現される事となる。

（１）ネットワーク認証（ゲートウェイにて）

接続される他ネットワークを特定化し、不正な接続、介入による「なりすまし」等を防止する事ができる。

（２）外部アクセス権制御（ゲートウェイにて）

アクセス可能な外部ユーザー、外部パスを限定する。

（３）内部アクセス権制御（資源を保有するホストにて）

アクセス可能な内部ユーザー、内部パスを限定する。

なおここでは以下のように規定している。

・内部ユーザー：サーバー・ネットワークの内部に登録されているユーザー

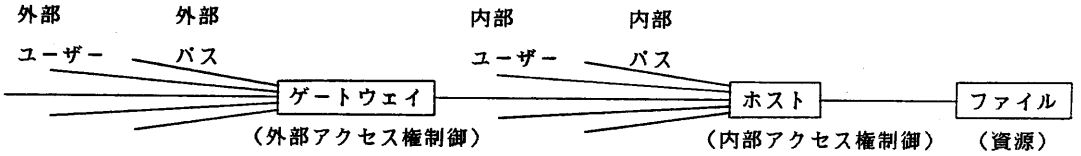
・外部ユーザー：サーバー・ネットワークの外部で登録されているユーザー

（通常、サーバー・ネットワーク内には登録されていない。）

・内部パス　　：サーバー・ネットワークの内部のアクセス経路

・外部パス　　：サーバー・ネットワークの外部のアクセス経路

外部アクセス権制御と内部アクセス権制御の関係を［図３］に示す。

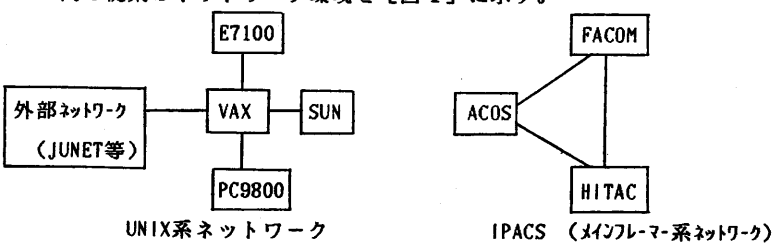


［図３　外部アクセス権制御と内部アクセス権制御］

ネットワーク認証、外部アクセス権制御はネットワーク間サービスの実現に伴って、ゲートウェイに新規に担わせるセキュリティ機能である。内部アクセス権制御は、通常各ホストが所有しているセキュリティ機能である。他ネットワークからのアクセスも、ゲートウェイを通過した後はサーバー・ネットワーク内のユーザー名に変換され、該当ホストへのエントリーも通常の内部ユーザーの形態となる為、内部アクセス権制御とは、結局、従来のアクセス権制御そのものとなる。

［５］ＩＰＡネットワーク環境でのプロトタイプ

ＩＰＡ内の従来のネットワーク環境を［図４］に示す。



［図４　ＩＰＡネットワーク環境］

IPACS（=IPA COMPUTER SYSTEM ）は国産３社の機種を接続したもので、相互に仮想端末機能、ファイル転送機能を実現している（参考文献２）。　ネットワーク管理機能等は持っていない。今回の開発では仮想端末機能のみを使用した。　UNIX系のネットワークは、いわば外部に開かれたOPENなネットワークであり、IPACSの方はCLOSEDなネットワークといえる。

今回この環境にて、以下の項目を実現するプロトタイプを開発する事とした。

（１）IPACS(ACOS,HITAC,FACOM) 内に蓄えられている情報資源（ファイル）をUNIX側から簡単に取り出せる。即ち端末上に表示できる、又はファイル転送ができる。

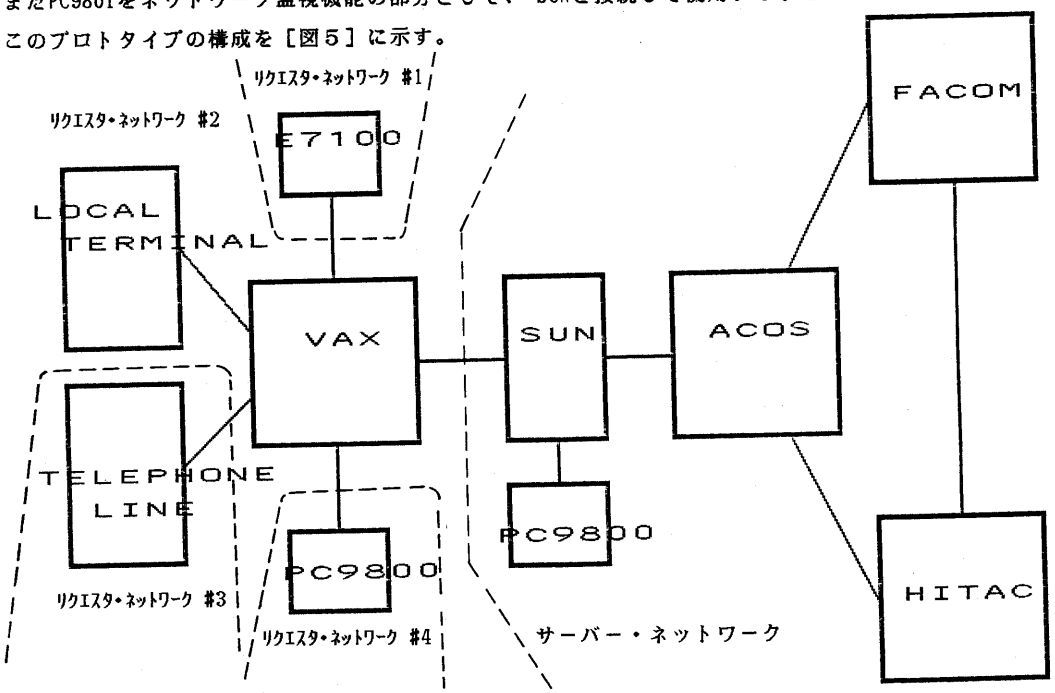
（ここで”簡単に”とは、ユーザーが IPACS内の構造、ファイルのアドレスを意識する必要がなく、UNIX側の１コマンドで実行できる事とする。）

（２）この際セキュリティ管理を行なう。即ち、ファイル別に読み出せるユーザー、パスを限定する。

前記のモデルで、 IPACS側をサーバー・ネットワーク、UNIX側をリクエスタ・ネットワーク群、SUN をサーバー・ネットワーク側のゲートウェイ、VAX をリクエスタ・ネットワーク側のゲートウェイとして使用する事として、この構成のもとに各種機能を実現する事とした。

またPC9801をネットワーク監視機能の部分として、 SUNと接続して使用する事とした。

このプロトタイプの構成を［図５］に示す。



［図５　プロトタイプ開発の構成］

［６］プロトタイプの機能

（１）プロトコル変換機能［ＶＡＸ，ＳＵＮ］

両ネットワーク間で基礎的なコミュニケーションを実現する為のプロトコル変換を行なう。

その概要は以下の通りである

(VAX-SUN)　ＴＣＰ／ＩＰ，イーサネット，　全２重，回線速度：10 MBPS，ASCII コード

(SUN-IPACS) 調歩同期式無手順，シリアル回線，半２重，回線速度：1200 BPS，JIS-7 コード

（2）接続ネットワーク認証機能［ＶＡＸ，ＳＵＮ］

サーバー・ネットワーク側（ＳＵＮ）とリクエスタ・ネットワーク側（ＶＡＸ）との間で相互に認証を行なう。（参考文献３）

ここではＤＥＳ暗号を使用して以下のような手順で行なっている［図６］。

(2-1) ＳＵＮにて６４bit の乱数ｘを発生してＶＡＸへ転送

(2-2) ＶＡＸは自分の Key:Fv で、これをＤＥＳ暗号化し、結果 Fv(x)をＳＵＮへ返送

(2-3) ＳＵＮは自分の保有する VAX側 Keyで　x を暗号化した結果と、ＶＡＸからの転送結果とを照合し、一致を確認する。

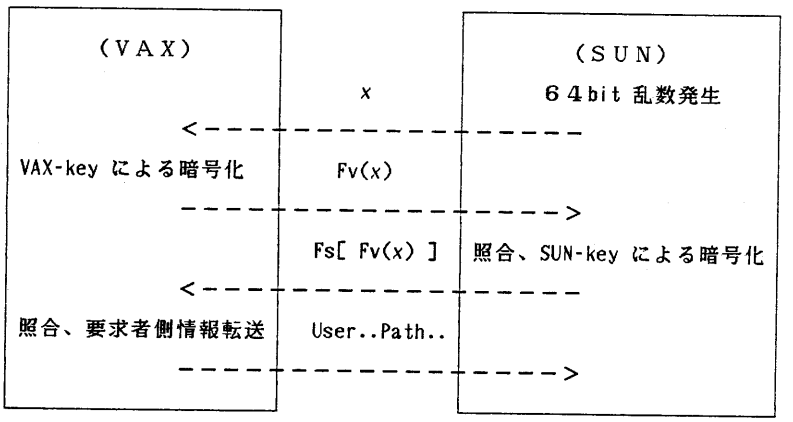
（ＳＵＮがＶＡＸの正当性を確認）

(2-4) ＳＵＮは上記の結果：Fv(x) をＳＵＮの Key:Fs で暗号化し、結果 Fs[Fv(x)] をＶＡＸへ転送する。

(2-5) (2-3) と同様にＶＡＸでは自分側での結果と照合し、一致を確認する。

（ＶＡＸがＳＵＮの正当性を確認）

(2-6) ＶＡＸは、要求者側情報として、ユーザー名，パス名，をＳＵＮへ転送する。



［図６　ネットワーク認証］

（３）外部アクセス権制御機能［ＳＵＮ］

アクセス権は、ファイル名（客体）、ユーザー名（主体）、パス名（アクセス手段）によって決定される（参考文献４）。

ＳＵＮでは、ＶＡＸから転送される要求者側情報よりユーザー名、パス名を得、ユーザーの要求する資源名と組み合わせて、３次元アクセス・マトリクス制御を行なう。これにより、サーバー・ネットワーク内の資源からみて信頼度の低いユーザーや信頼度の低いパスを排除する事が可能となる。　アクセス・マトリクスの内容の例を［図７］に示す。図のように、アクセス権はユーザーとパスとの対毎にテーブル上で設定可能である。又、あるパスに関しては、ユーザーにかかわらず可、あるユーザーに関してはパスにかかわらず可、というような設定も可能としている。

（４）資源管理機能［ＳＵＮ］

前述の資源名はサーバー・ネットワーク外からみた資源名である。これをサーバー・ネットワーク内での資源名（ホスト名＋ファイル名）に翻訳する。

access-matrix	test5									
path	212ish		211yam		213tan		221mat		evrbdy	
1 console	.		.		.	R	.		.	
2 comp-room	.		.	R	.		.		.	
3 PC-9801	.	R	.		.		.		.	
8 term-6	.	R	.		.		.		.	
15 Tel-1	.		.	R	.	R	.		.	
17 E-7100	.		.		.		.		R	
ALL	.		.		.		.	R	.	

［図７　アクセス・マトリクスの内容（例）］

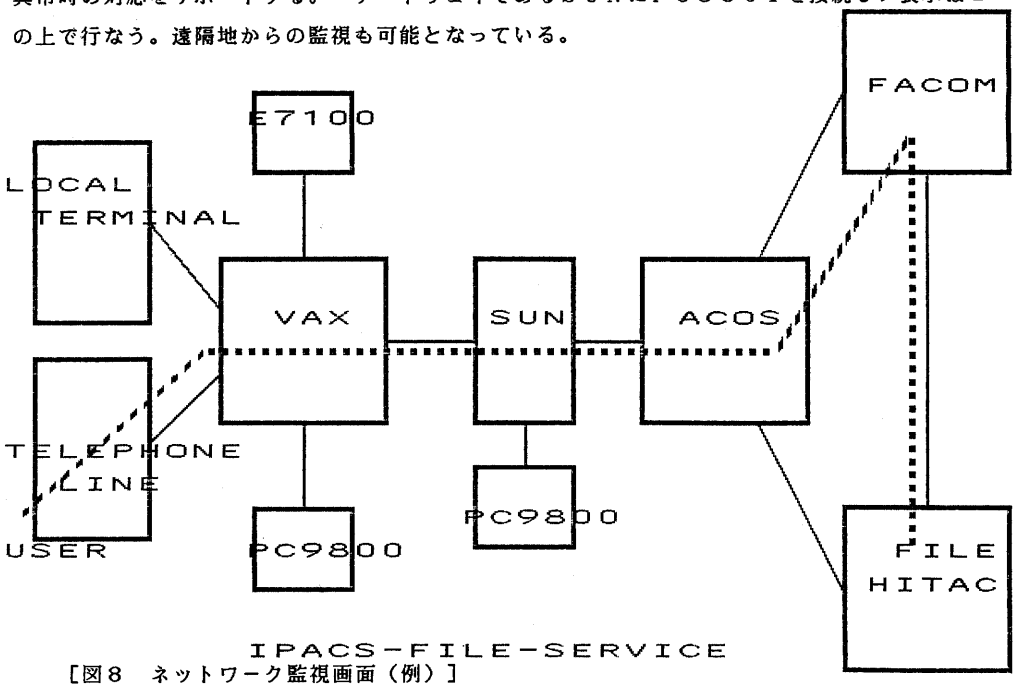
（５）自動アクセス機能［ＳＵＮ］

資源管理機能により、要求された資源の所在、名称が明らかとなっている。ここでは、その所在箇所（特定ホスト）へのアクセス経路、手順を管理し、目的箇所迄、自動的にセッションの開設、ファイルの取り出し、セッションの終了を行なう。

ホストによっては、複数のアクセス経路が存在する。その場合には SUN上に設定されている Availableな経路が選定される。

（６）ネットワーク監視機能［ＳＵＮ，ＰＣ９８０１］

接続ネットワークの状況、サーバー・ネットワーク内のセッション開設・終了の状況をモニタし、異常時の対応をサポートする。　ゲートウェイであるＳＵＮにＰＣ９８０１を接続し、表示はこの上で行なう。遠隔地からの監視も可能となっている。



［図８　ネットワーク監視画面（例）］

［７］実行例

実際の使用手順は以下のようになる。

1)リクエスタ・ネットワーク（UNIX系ネットワーク）のユーザーは、仮想端末機能等を用いてＶＡＸ上にセッションを開設する。

2)該当プログラムを起動する。

3)（ネットワーク認証の完了後）ユーザーは要求する資源名を入力する。

4)ユーザーに対して、要求した資源（ファイル）の内容が表示（あるいは転送）される。

この際のセッション開設状況等のネットワーク監視画面を［図７］に、又、ユーザー・サイドの画面を［図８］に示す。

これは、ユーザーが、ＶＡＸ側より（外部名） test5 というＩＰＡＣＳ内のファイルを要求した例である。ＳＵＮは、ネットワーク認証、外部アクセス権チェックの後、その所在位置（HITAC)を検索し、自動的にアクセスして該当ファイルの取り出し、表示を行なっている。

なおここで、ACOSから直接HITAC にアクセスせず、FACOM 経由となっているのは、ACOS-HITAC回線が障害等で使用できない旨がＳＵＮ上に登録されている為である。

```
[tanaka vax . 7] get-ipacs
vax<-sun: @0101111111011010000111010100010000111101010100110100001011001010 1
vax->sun: #1001010000111010101110100010101110100110101111001010110001101010
* vax<-sun: @1110101011001011010010110100011010100111011001001000110010111101
vax->sun: #u213p15
---- Welcome to IPACS-file-service. Please key-in file-name.--
test5
----- Now going to get the file. Wait for a moment.-----------
( SUN->IPACS connected. )
( login ACOS. )
( ACOS->FACOM connected. )
( login FACOM. )
( FACOM->HITAC connected. )
( login HITAC. )
(    getting HITAC-file. )
* ( logout HITAC. )
( FACOM->HITAC disconnected. )
( logout FACOM. )
( ACOS->FACOM disconnected. )
( logout ACOS. )
( bye-bye IPACS. )
----- File is available. Key-in disp or save to what. --------
disp
00010 *********************************************
00020 *                                           *
00030 *               HITAC M160H                 *
00040 *                                           *
00050 *                TEST DATA                  *
00060 *                                           *
00070 *********************************************
----- IPACS-file-service end. -------------------------------
Connection closed.
[tanaka vax . 8]
```

［図９　プログラム実行画面（例）］　（＊は debug　時の出力）

［８］考察

ある想定モデルでのネットワーク間サービスについて、機能要件の整理と、そのプロトタイプの開発を行なった。明らかとなった幾つかの問題について、ここでまとめてみたい。

（１）ゲートウェイ機能とネットワーク管理機能との、ネットワーク内での分担

当モデルでは、ゲートウェイに一種のネットワーク管理機能も持たせ、外部ユーザーに対する、高度の利便性を実現する事ができた。従来のゲートウェイのイメージとは、やや離れたものである。サーバー・ネットワークが大規模となって、ゲートウェイを複数箇所設ける事が必要な際には、後者を分離する事が得策となろうが、当モデルのように外部からのアクセスを一本化できる場合には、明らかにゲートウェイに担わせる方が合理的形態と考えられる。

（２）サーバー・ネットワークのゲートウェイの持つ情報の管理方法

ＳＵＮには資源管理情報、アクセス手順情報、外部アクセス権制御情報等を持たせる事となる。当モデルでは、これらに対して一元的にネットワーク管理者がＳＵＮのオペレーションを行なう事を想定している。サーバー・ネットワーク内の各ホストに登録されている、資源の所有者がこれら情報を参照、変更する簡易な手段を提供する事も必要と思われる。

これについては、今後、開発を進める予定である。

（３）ネットワーク間の認証に使用する暗号鍵の管理方法

ここではアタックの方向としては、主として、（Ｘ）--->ＳＵＮを想定し、相互認証の為に、経路毎に鍵を二つ決めて相互に保有する方法を採用したが、運用管理を、より単純化する為には、今後、更に掘り下げた検討が必要と考えている。

［９］おわりに

利便性と、セキュリティという相反しがちな両者を実現する為の一つの試みについて述べた。高度のセキュリティ対策を実施するのみではなく、セキュリティを確保しつつ、如何に利便性を高めるか、という事が、今後のネットワーク社会の課題と思われる。

今後、ネットワーク形態・サービスに応じた、最適なネットワーク管理機能、セキュリティ機能の実現を目指して開発を進めて行きたいと考えている。

［参考文献］（１）情報処理振興事業協会　技術センター：　コンピュータ・ネットワークにおける
セキュリティの調査報告書　　情報処理振興事業協会　６０技－０６２

（２）川合：　ＩＰＡＣＳにおける異機種間結合実験　分散データベース技術に関する事例
情報処理振興事業協会　５８技－０２５

（３）中尾、浦野：　ＯＳＩにおけるセキュリティ・アーキテクチャの検討
電子通信学会技術研究報告　ＩＮ８６－１～１２

（４）M.Tanaka, Y.Ishizawa：　An Access Control Mechanism for Network Security
Proceedings of COMNET'85