コンピュータ・ネットワーク・ゲートウェイにおける安全化機構

5U-6

石沢良一　田中幹夫
(情報処理振興事業協会　技術センター)

1．はじめに

ネットワークサービス利用環境の基盤の一つとして，コンピュータ・ネットワーク相互接続におけるセキュリティ（安全性）の確保がある．[1]

本稿では，情報資源の利用というネットワークサービスを取上げ，接続他ネットワークからの不正アクセスを排除するセキュリティ方策を検討し，ゲートウェイ安全化機構を試作したので報告する．

2．セキュリティ方策

考察の対象とするコンピュータ・ネットワークを当技術センターにおけるネットワーク，情報資源をファイル蓄積情報とする．（図1）

IPACS ネットワーク[2](IN) およびUNIXネットワーク(UN)がゲートウェイ方式で相互に接続されている．INはheterogeneous ネットワークであり，各ホストコンピュータは自立分散的に独立して安全性を確保している．

ネットワークサービスは次のようなものである．INに情報資源が在るとすると，INがサーバネットワーク，UNがリクエスタネットワークとなり，UNユーザはゲートウェイを通してIN情報資源を利用する．

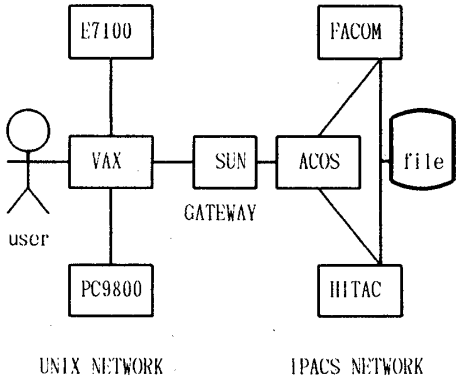

図1　ネットワーク

以上のネットワークサービスにおける，セキュリティ方策を示す．一般的に安全性の確保と利便性，効率，操作性等とは相反するものと考えられるが，ここでは安全性と利便性との両立を試みた．

①それぞれのネットワークは独立性を保持する．
②リクエスタネットワークは，サービス利用を許されたネットワークであることを要する．
③サーバネットワークとしての安全性をホストコンピュータと別に確保する．
④ファイル名や実アドレス等の詳細な属性は公開しないことにし，アクセス要求に対しては仮想的な資源名（外部ファイル名）のみを与える．
⑤利用者が詳細な情報資源の利用法を予め知っていなくても利用できるようにする．

3．セキュリティ方策の実現

以上のセキュリティ方策は，次の機能にまとめられる．

（1）name server 機能：他ネットワーク利用者が示す外部ファイル名から内部ファイル名へ変換する．変換はファイル名DBを使用する．

（2）アクセス権制御機能：ファイルに対してユーザ，パス，を考慮する三次元アクセス・マトリクス[3] によりアクセス権制御を行う．

（3）接続ネットワーク認証機能：相互に正しい鍵を持つものを正当と見なす．このためDES 暗号方式によるハンドシェイクを採用する．

（4）ホストアクセス機能：ゲートウェイからホストに自動リンクを開設し，資源を持ってくる．

これらの機能はresource server (RS)として単一の機構にまとめて実現する．このRSの位置として，複数の箇所が可能である．ここでは，ゲートウェイが他ネットワークとの一般的な接点でありアクセス情報路の途中にあることを考慮して，ゲートウェイ上に置くことにする．

A Security Mechanism on Computer Network Gateway
Yoshikazu Ishizawa, Mikio Tanaka
Information-Technology Promotion Agency

4．実行例

図1で示したネットワークのゲートウェイがRSを持つ．UNからのアクセス要求に対して，RSは次の処理を順に行う．動作例を図2に示す．

①接続ネットワーク認証を行い，ユーザの属するネットワークが接続を許されたネットワークかチェックし，不正接続を排除する．

②要求ファイル名（外部ファイル名）を入力する．外部からの利用名を内部ファイル名とは別にし，ファイル属性を仮想化している．詳細なファイル属性を知らなくても利用でき，知らないので安全性が高まる．

③ユーザの要求ファイル名に対するアクセス権を図3に示すアクセス・マトリクスの内容によりチェックする．サーバネットワークとして不正アクセスを排除する．

④外部ファイル名を図4に示すファイル名ＤＢ内容により内部ファイル名に変換する．

⑤ゲートウェイから該当ホストにアクセスする．同時に内部ファイル名に対するアクセス権チェックを行う．ホストのアクセス権制御はそのままなので，ホストユーザの不正アクセスは独立に排除される．

⑥ネットワークサービスによりファイル内容をユーザが利用する．

```
**** Warning, can't display on PC9801. *****
vax<-sun: @0011001010110100110101110110111111

vax->sun: #1111011010100011010100001100000111

vax<-sun: @0000001101110101001111111110101010

vax->sun: #u213p16

---- Welcome to IPACS-file-service. Please k
test1
----- Now going to get the file. Wait for a
  ( SUN->IPACS connected. )
  ( login ACOS. )
  ( logout ACOS. )
  ( bye-bye IPACS. )
----- File is available. Key-in disp or save
disp
      1       1P **********************
      2       1P * ACOS -- SUN  OK  *
      3       1P **********************
----- IPACS-file-service end. ----------------
Connection closed.
```

図2　動作例（表示右側略）

access-matrix	test1							
path		201hay		221mat		211yam	212ish	
6 term-4	.		.		.		WR	.
10 term-8	.	W	.		.			.
13 Tel-2	.		.		.	W	.	.
17 E-7100	.		.	WX	.		.	.

図3　アクセス・マトリクスの内容

```
test1 ACOS 'KENKYU. ISHIZAWA. TEST'
test2 FACOM TEST. HCOB
test3 HITAC TEST. FORT
test4 FACOMfromH TEST. HCOB
test5 HITACfromF TEST. FORT
test6 ACOS TEST
test7 FACOM TEST. HCOB
```

図4　ファイル名ＤＢの内容

5．おわりに

安全性確保としてname server 機能，アクセス権制御機能，接続ネットワーク認証機能，ホストアクセス機能を持つresource server (RS)を提案した．ネットワークを相互接続する場合，このRSをゲートウェイ上に設置することで，安全性をさらに向上させることができ利便性が得られることを報告した．

今後，情報資源の持ち主がアクセス権を変更する機能を追加する予定である．また，ネットワーク内他ホストユーザの利用の場合を含めたふさわしい設置場所を何処にするかはこの研究をさらに進めて明確にする必要がある．

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イの調査報告書，情報処理振興事業協会，60技-062，1986

[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-025，1984

[3] 田中，石沢，ネットワーク・セキュリテイの為のアクセス権制御，第３２回情報処理学会全国大会論文集，pp35 -36