2Q - 04　コールバック方式による自動ダイヤルアップ接続方式の検討

2Q－4

祢宜　知孝†　今井　功†　楠　和浩†　高井　伸之†　下間　芳樹†

†三菱電機（株）情報技術総合研究所

1. はじめに

近年，ISP（Internet Service Provider）にダイヤルアップIP接続を行うことによってインターネットにアクセスするユーザが増加した．それに伴い，ダイヤルアップIP接続端末間での通信を実現するための方式がこれまでに提案されている．

ISPにダイヤルアップIP接続する2台のホスト間で通信を行うためには，2台のホストがISPとの接続を完了している必要がある．ところが，ダイヤルアップIP接続は，一般的には，両ホストが独立に接続要求を実行する形態をとるため，接続完了の同期をとることは難しい．そこで，一方のホストからのダイヤルアップIP接続を契機に，ISP間で同期を取り，通信対象ホストとの接続を実現する方式[1]がこれまでに提案されている．

しかしながらこれらの方式は，ユーザ認証などの点で問題がある．本稿では第2節において従来方式の特徴と問題点を示し，第3節でこれらの問題点を解決する方式を提案する．

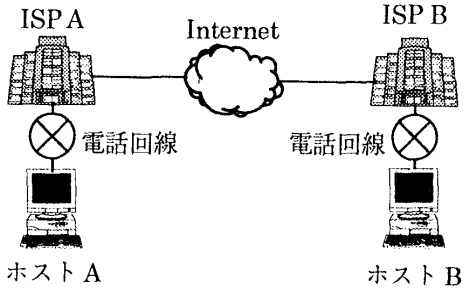

図 1. システム環境

2. 従来方式の問題点

[1]の方式について図 1を用いて説明する．ホストAのユーザAが，ISP BとダイヤルアップIP接続されていないホストBと通信を行う場合の処理の流れを概説する．ユーザAによって，ISP BとダイヤルアップIP接続されていないホストBとの接続要求がISP Aを経てISP Bに伝えられる．そこで，ISP Bは自らホストBにダイヤルアップIP接続をし，その後接続完了をISP Aを経てホストAに通知する．

しかし，[1]の方式では，次の問題点が存在する．

(1) ISPでのユーザ認証の欠如

ISP Bにおいてユーザ Aがホスト Bへのアクセス権を所持しているか否かを認証していない．そこで，誰でもホストBとインターネットを介して通信を行うことが可能である．従って，悪意を持ったユーザがホスト Bとインターネットを介して通信を行い，ホスト Bに対して容易に不正行為を行うことが可能である．

(2) ホストでのISP認証の欠如

ホストBにおいて，正規のISP Bからのダイヤルアップ IP接続要求であるか否かを認証していない．そこで，誰でもホストBに対してダイヤルアップIP接続を行うことが可能である．従って，悪意をもったユーザがISPに成りすまし，ホスト Bに対してダイヤルアップIP接続要求を送信し，ホスト Bとダイヤルアップ IP接続を行うことが可能である．

3. 認証を可能とする方式の提案

上記の問題点を解決するため，ISP Bにおけるユーザ Aの認証と，ホストBからISP Bへのコールバックによるダイヤルアップ IP接続を行う方式を提案

A Study of Automatic Dialup IP Connection Establish Method via callback

Tomonori Negi, Isao Imai, Kazuhiro Kusunoki, Nobuyuki Takai, and Yoshiki Shimotsuma.

MITSUBISHI ELECTRIC CORPORATION

5 - 1 - 1 Ofuna, Kamakura, Kanagawa 247－0056, Japan

する.以下に本稿で提案する方式の実現方法を述べる.

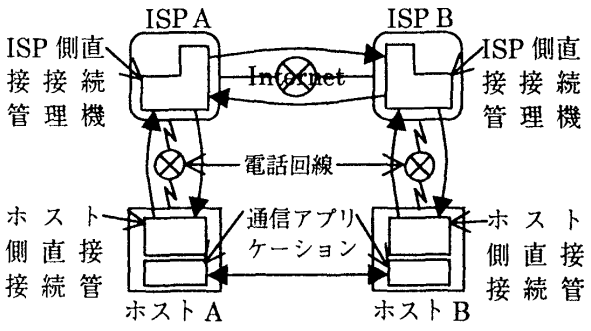

図 2. システム構成図

図 2に示すように，ホストA・ホストB上には，**ホスト側直接接続管理機構**が起動しており，ISP A・ISP B上には，ISP **側直接接続管理機構**が起動している．第2節で挙げた問題点(1)を解決するため，ISP BにおいてISP 側直接接続管理機構が，ホスト A の使用者であるユーザ A の認証を行う．ISP 側直接接続管理機構は，接続要求を送信したユーザを認証する．この認証を行うために，IPS 側直接接続管理機構は，契約ホスト毎にアクセスリストを保持している．このアクセスリストは，アクセスを許すユーザのメイルアドレスと，認証レベル，認証情報から構成されている．処理の流れを以下に示す．

ホスト A の使用者であるユーザ A によってホスト B との通信が要求されると，その要求がホスト A 上のホスト側直接接続管理機構 A，ISP A上の ISP 側直接接続管理機構 A を経て，ISP B 上の ISP 側直接接続管理機構 B に伝えられる．接続要求を受信した ISP 側直接接続管理機構 B は，ホスト B のアクセスリストを検索し，ユーザ A に課す認証レベルを調べ，ホスト A に認証レベルに相当する認証情報を要求する．そして，ホスト A から認証情報が送信されて来ると，アクセスリスト中の認証情報と比較してユーザ A の認証を行う．

また，第2節で挙げた問題点(2)を解決するため，ISP B からの呼び出しに対してホスト B からのコールバックによってダイヤルアップ IP 接続を行う．ホスト側直接接続管理機構は，コールバックをすべき ISP と，その ISP にアクセスするためのユーザ ID とパスワードを保持している．処理の流れを以下に示す．

ISP B においてユーザ A の認証に成功すると，ISP B はホスト B に対して呼び出しをかける．呼び出しを受けたホスト B は，ISP B に対してコールバックにより，ダイヤルアップ IP 接続要求を行い，ユーザ ID とパスワードを返す．ホスト側直接接続管理機構 B は，受信した認証情報とアクセスリストに登録された認証情報を照合し，認証を行う．以上により，ホスト B と ISP B 間のダイヤルアップ IP 接続は完了する．

上記に提案した方式により，特定のユーザのみがアクセスリストで設定されたレベルの認証を経て遠隔のホスト B を ISP B にダイヤルアップ IP 接続させることが可能となる．従って，悪意を持ったユーザがホスト B とインターネットを介して通信を行い，不正行為を行うことが不可能である．

また，上記に提案した方式により，特定の ISP B のみがホスト B とのダイヤルアップ IP 接続が可能となる．従って，悪意をもったユーザが ISP に成りすまし，ホスト B に対してダイヤルアップ IP 接続要求を送信し，ホスト B とダイヤルアップ IP 接続を行うことが不可能である．

4. おわりに

本稿で提案した方式により，従来方式の問題点を解決することができた．しかし，本稿で提案した方式では，ホスト B において不正な呼び出しを防ぐ方法がなく，不正な呼び出しに対しても ISP B へのコールバックを行ってしまう．今後，呼び出しを認証し，不正な呼び出しを受けた際には，ISP B へのコールバックを行わない方法を検討する予定である．

参考文献

[1]. 石井　克也：ネットワーク・システムにおける接続方式，及びサーバ・マシン，特開平 10－11381，1998.1.16