利用者イーサネット・ジャックおよび無線 LAN システムの更新

後藤 英昭[†]　　花岡 勝太郎[‡]
[†]東北大学サイバーサイエンスセンター スーパーコンピューティング研究部
[‡]東北大学情報部情報基盤課 システム管理係

1. はじめに

センターでは、利用者が持参したノート PC などを学内 LAN およびインターネットに接続できるように、1 階利用者入出力室にイーサネット・ジャックと無線 LAN アクセスポイント(IEEE802.11b 対応)を設置して 2004 年よりサービスを提供してきました[1]。このサービスは、来館時の端末利用や、大判プリンタのデータ転送などに利用できます。

このたび老朽化した機器を更新し、無線 LAN の通信を高速化したので、新しいシステムの使用方法を説明します。

また、本稿では当システムのユーザ認証機構についても解説します。

2. 使用方法

有線接続(イーサネット, 10BASE-T/100BASE-TX 対応)で利用する場合は、利用者入出力室にある「利用者用」の表示のある HUB にケーブルを接続してください。ケーブル 1 本はセンターで用意しています。

無線で利用する場合、SSID と WEP を以下のように設定して接続してください。新しいシステムでは、従来の IEEE802.11b(11Mbps)規格に加えて、11g (54Mbps) と 11a (54Mbps) の両規格にも対応し、通信が大幅に高速化されました。

SSID:　ISC-AP1 (11b/g の場合)　　または　　ISC-AP1a (11a の場合)
WEP:　　使わない

有線・無線とも、端末の IP アドレスと DNS サーバのアドレスは DHCP により自動取得してください。

セキュリティ対策のために、本システムではユーザ認証の手続きが必要になっています。ケーブルや無線で端末を接続しただけでは、大規模科学計算システムや学内ネットワーク、インターネットには接続できません。端末の OS (Windows や MacOS など)に付属のツールを用いて、下記の VPN サーバに接続してください。

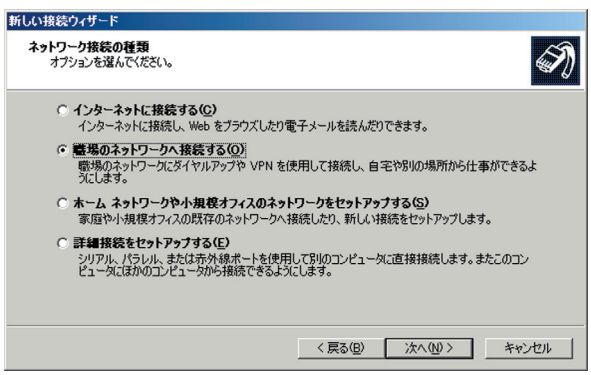
VPN(PPTP)サーバアドレス:　172.18.1.1
認証方式:　MS-CHAPv2
ユーザ ID / パスワード:　(センター内に掲示, 時々変更されます)

イーサネット・ジャック

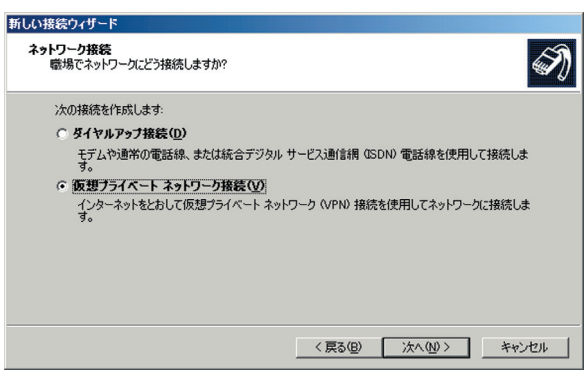
MS-Windows XP による VPN 接続

Windows XP における VPN 接続の手順を以下に示します。

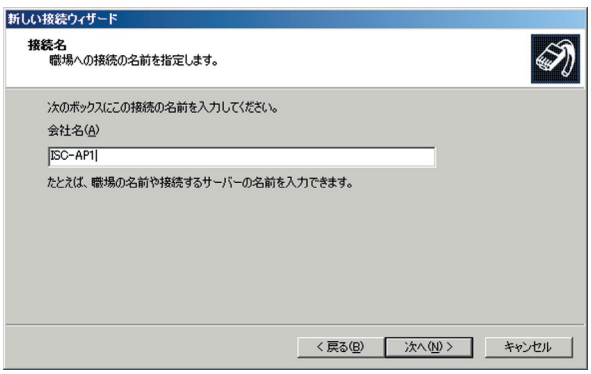
まず「新しい接続ウィザード」を起動し、「職場のネットワークへ接続する」を選択します。



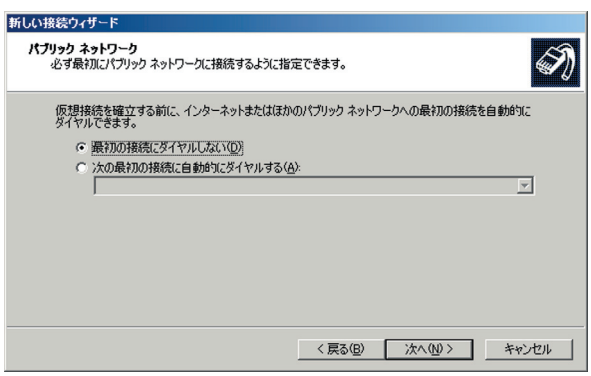
「仮想プライベートネットワーク接続」を選択します。



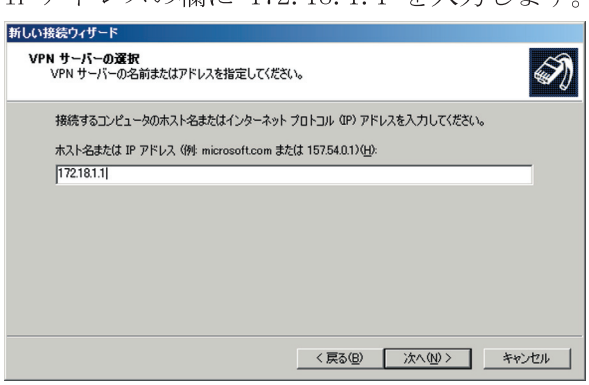
たとえば「ISC-AP1」のように、どこの接続かわかりやすいような名前を指定します。



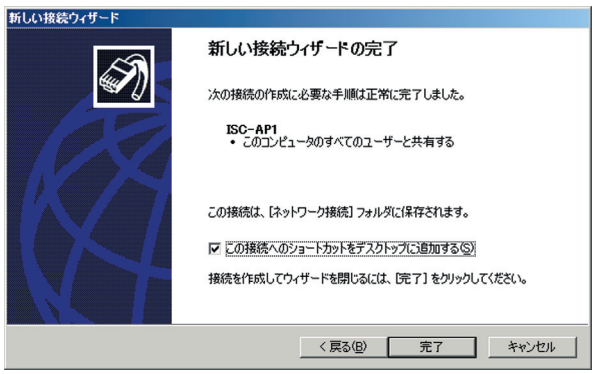
「最初の接続にダイヤルしない」を選択します。



IP アドレスの欄に 172.18.1.1 を入力します。



接続準備を完了します。以上で接続準備は終わりです。

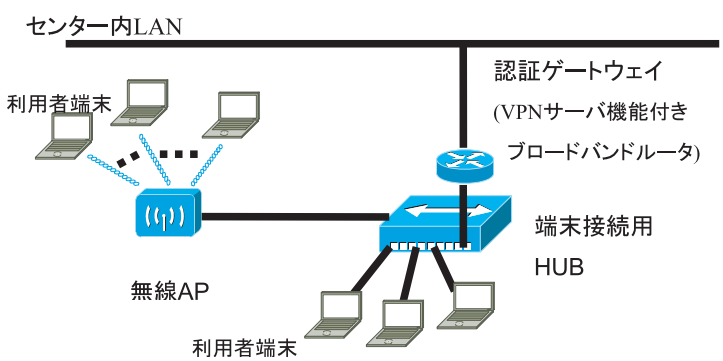


端末を有線または無線で接続した後、VPN 接続のアイコンをクリックして、ユーザ名とパスワードを入力します。「接続」ボタンをクリックすると、学内ネットワークやインターネットに接続できるようになります。

使用後は、VPN 接続のアイコンを再度クリックして、「切断」処理を行います。

3．システム構成

当システムは、旧システムと同様に、認証ゲートウェイ、HUB、無線アクセスポイントから成っています。ネットワーク構成を下図に示します。



図：　イーサネット・ジャック／無線 LAN システム

無線アクセスポイントには、IEEE802.11b/g/a に対応した一般的なものを使用しています。
ユーザ認証や暗号化は行っておらず、単なるブリッジとして動作させています。端末によっては 11b/g と 11a の接続がバタついて不安定になることがあるので、SSID を 11b/g と 11a で区別し、利用者が明示的に選択できるようにしました。端末接続用の HUB も一般的な FastEthernet スイッチを用いています。

認証ゲートウェイとして、旧システムでは Linux と authipgate（認証ゲートウェイ用プログラム）を導入した PC を使用して、Secure Shell によるユーザ認証を実現していました。この方式では、大規模科学計算システムと連携して、利用者番号をそのまま用いてユーザ認証が可能でした。一方で、Windows には Secure Shell が標準で付属していないために、予めソフトウェアを入れておく必要がある点が不便でした。

新しいシステムでは、PPTP による VPN 接続を利用してユーザ認証を行っています。PPTP は Windows や MacOS で標準でサポートされているため、利用者への負担は小さくなります。しかし、PPTP におけるパスワードの暗号化方式は UNIX 系システムと互換性がないので、大規模科学計算システムとの認証連携ができないというデメリットが生じます。（統合認証システムを導入すれば、技術的には認証連携も可能です。） 今回のシステム更新では、システム構築の費用と利用者の便を優先させ、センターの来訪者にはゲスト用のアカウントを利用してもらう方針にしました。なお、当センターでは、物理的なセキュリティ確保のために、入口から利用者入出力室に至るまでの間に監視カメラが設置されています。

認証ゲートウェイとして、VPN(PPTP)サーバ機能を有するブロードバンドルータ BHR-4RV（Buffalo 製）を利用しました。ルータの WAN 側ポートをセンター内 LAN に接続し、LAN 側ポートに無線アクセスポイントと端末を接続します。IP アドレスの節約とセキュリティ確保のために、NAT 機能を有効にしてあります。端末への IP アドレスの付与は、ルータの DHCP サーバ機能で行っています。設定の注意点として、DHCP のリース時間を 1 時間(このモデルの最短時間)に設定することが挙げられます。これは、多数の利用者が入れ替わり立ち代り端末を接続しようとした場合に、アドレスの枯渇を避けるためです。リース時間が短く設定されていても、端末は接続されている限りは自動的にリース期間を更新するように動くので、使用中に接続が切られることはありません。なお、このモデルの制約で、同時接続数は 10 台までとなっています。

VPN 接続によるユーザ認証が行われるまでは、端末から学内 LAN への通信を遮断しておく必要があります。ルータのパケットフィルタの機能を用いて、この機能を実現できます。パケットフィルタの設定で、すべての通信(ここでは IP forwarding のこと)を遮断した上で、一部のプロトコルのみを通すようにしておきます。利用の便に配慮して、DNS サーバへの問い合わせだけは特別に許可するようにしました。具体的にはポート 53/tcp,udp を開けています。

4．おわりに

VPNサーバ機能を有する市販の廉価なブロードバンドルータを利用することで、ゲスト用アカウントによる簡易なユーザ認証が可能なイーサネット・ジャック／無線 LANシステムを構築できました。PCや専用の認証スイッチを使う方式と違い、導入コストが低いことはもちろん、管理の手間も非常に小さいのが特長です。また、VPNを利用することで、無線区間の暗号化に頼らなくても端末間の通信の秘匿性を高められるという利点が生じます。

UNIX システムとの認証連携については、当システムだけでは解決できない問題なので、将来の課題となります。

サイバーサイエンスセンター本館では、国際無線LANローミング基盤「eduroam」[2]に対応した無線アクセスポイントも使えます。参加機関のアカウントをお持ちの方はご利用ください。

参考文献

[1] 花岡勝太郎, 後藤英昭, “利用者用イーサネット・ジャックおよび無線 LANについて,” 大規模科学計算機システム広報 SENAC Vol.37, No.2, p.43 (2004).
[2] 後藤英昭, 曽根秀昭, “大学間無線 LAN ローミング eduroam-JP の導入,” 大規模科学計算機システム広報 SENAC Vol.41, No.1, pp.57-61 (2008).