研究報告

リモートアクセス環境の構築と運用に関する研究

学習院大学　計算機センター　村　上　登志男
学習院大学　計算機センター　磯　上　貞　雄
国立情報学研究所　コンテンツ科学研究系　孟　　洋
学習院大学　計算機センター　城　所　弘　泰

研究目的

現在では、電子メールサービスをはじめとする情報センターのコンピューターシステムは 24 時間 365 日無停止で運用することが求められることが多くなってきている。本学計算機センターが管理するコンピューターシステムも同様に無停止運用が求められている。

本学でもこれを実現するためには、少なくとも 24 時間 365 日の監視体制が必要であるが、現状の人員・体制では不可能である。管理者が学内に不在の場合でもネットワーク環境の整った場所にいる場合、セキュアなリモートアクセス環境が提供されていることである程度の対応が可能となる。

既に試験的にリモートアクセス環境を構築し、遠隔からのシステム管理などに一部利用しているが、利用に当たり一定の手続きを必要とし汎用性は高いとは言えない。

そこで、本研究では既存の環境をさらに発展させ、利便性が高く、よりセキュアなリモートアクセス環境の構築と評価を目的とする。

さらに、システム管理利用にとどまらず、一般ユーザーも遠隔地から比較的簡易に利用できる環境の構築と評価を目的とする。

研究の背景と研究方法

研究代表者の村上は、2008 年度から WindowsServer2003 の機能を利用したリモートアクセス環境を構築し、遠隔地からのシステム監視などを行っており、緊急時の対応などを行ってきた。

本研究では、数年にわたる経験を生かし、簡易に利用できるようなインタフェースの開発、汎用性の高いシステムを構築し、実際に様々なネットワーク環境からの遠隔管理の評価を行う。

また、教育研究用コンピューターシステムを利用し、まずは限定されたユーザーが、遠隔地から仮想デスクトップ環境として学内システムを利用できる環境を構築し、利便性などの評価を行う。

インターネットを経由した VPN 接続環境の提供は、学習院・成蹊・成城・武蔵・甲南の 5 大学では成城大学などですでに行われている。これらはもっぱら学内ユーザーに対してオンラインジャーナルをはじめとして、学内からしかアクセスできない資源を学外からアクセスすることができるようにサービスを提供している。

上記のようなサービスは、5 大学に限らず多くの大学で提供されており、本学でも要望の多いサービスの一つである。本学ではセキュリティや接続の容易性などの観点から、現在はサービスの提供を行っていない。また技術的には利用できるアプリケーションやオンラインジャーナルをはじめとして遠隔地からの利用に対応するライセンス契約の締結が行われていないことなどの法的な整備も整っていないこともサービスを提供していない理由の一つである。

本研究では、表 1 の VPN サーバー環境および表 2、3 の学内接続先環境を構築し、さまざまな OS からの接続性、利便性などを調査した。VPN の接続性はもとより、接続完了後に表 4 で列挙したアプリケーションを利用し、学内の Windows 環境にリモートデスクトップ接続を行った。また、表 5 に掲載したアプリケーションを利用し、一般ユーザーが学外から学内の Windows ドメイン環境を利用する場合の利便性を調査した。外部のネットワークから PPTP、SSL-VPN のどちらの接続も不可能な場合に表 6 に挙げた SSH クライアントを利用し、ポート転送機能を利用することで安全にリモートデスクトップ接続ができるかどうかも合わせて確認した。

表 1　VPN サーバー環境

リモートアクセス /VPN サーバー	Windows Server 2003　PPTP（MS-CHAPv2/MMPE）
SSL-VPN アプライアンス装置	Citrix 社製 NetScaler MPX1500
RD ゲートウェイマネージャー（RDP over HTTPS）※ 1	Windows Server 2008 R2、リモートデスクトップゲートウェイマネージャー

※ 1　正確には VPN サーバーではないが、学外から学内へアクセスするためのゲートウェイとして準備したのでこの一覧に載せている。

表 2　学内接続先環境

リモートデスクトップ接続先	Windows Vista Enterprise
リモートデスクトップ接続先	Windows 7 Enterprise
UNIX 系 OS 接続先	FreeBSD 8.2R
SSH 接続先 OS	Vine Linux 6

表 3　仮想デスクトップ環境

VDI in-a-box（Citrix 社製）+ Windows 7 Enterprise

表４　本研究で利用した RDP アプリケーション一覧

開発元	製品名	対応 OS	備考
Microsoft	リモートデスクトップ接続	Windows	OS 標準
Thinstuff s.r.o.	iRdesktop	iOS	無料版
MochaSoft	RDP Lite	iOS	無料版
2X Software	2X Client	iOS/Android/Windows など	無料版
Wyse	PocketCloud リモートデスクトップ RDP/VNC	iOS/Android/Windows など	無料版

表５　仮想デスクトップ接続アプリケーション

開発元	製品名	対応 OS	備考
Citrix	Receiver	iOS/Android	無料

表６　本研究で利用した SSH クライアント一覧

開発元	製品名	対応 OS	備考
オープンソース	Tera Term	Windows	無料
Zatelnet	zatelnet	iOS	無料版
Zinger-Soft	iSSH	iOS	850 円
オープンソース	ConnectBot	Android	無料

構築した環境を利用してのリモートアクセスの実際

概要

学習院外部のネットワークから学習院内部のネットワークに接続するためのリモートアクセスサーバー（RAS サーバー）を研究代表者の村上が Windows Server で本研究に先立ち構築している。その Windows Server で構築した RAS サーバー利用し、様々なプラットホーム、クライアントを用い、様々なネットワークからの接続性を検証する実験を行った。

前述の環境は Windows Server の Point-to-Point トンネリング プロトコル（PPTP）と MMPE・

MS-CHAPv2 を利用した VPN である（図１）。

既に Microsoft Windows Vista/7 に標準で付属している VPN クライアントでの接続は確認できているため、Windows 以外の OS からの接続性の確認を行った。Apple 社の iPod touch /iPad などの iOS に付属している VPN クライアントからの接続テストを行い、VPN 接続が確立できることを確認した。スマートフォンやタブレットなどで利用されている Android OS でも同様に接続確認を行った。さらに、それらの上で動作するリモートデスクトップクライアント（表４）を利用し、学内の Windows 環境にリモートデスクトップ接続を行った。また、SSH クライアントを利用し、学内のネットワークからしかアクセスできない UNIX 系サーバーへの接続を行った。

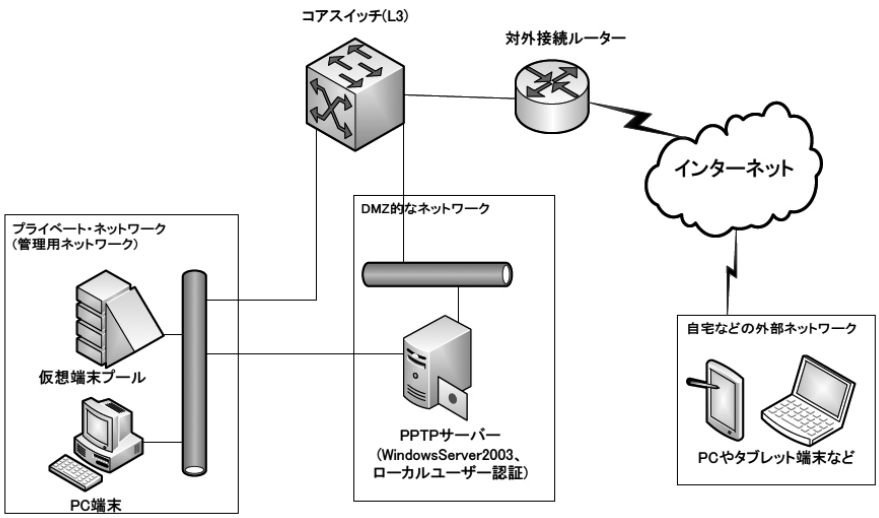

図１　Windows Server 2003 の VPN サーバーを利用したリモートアクセス構成

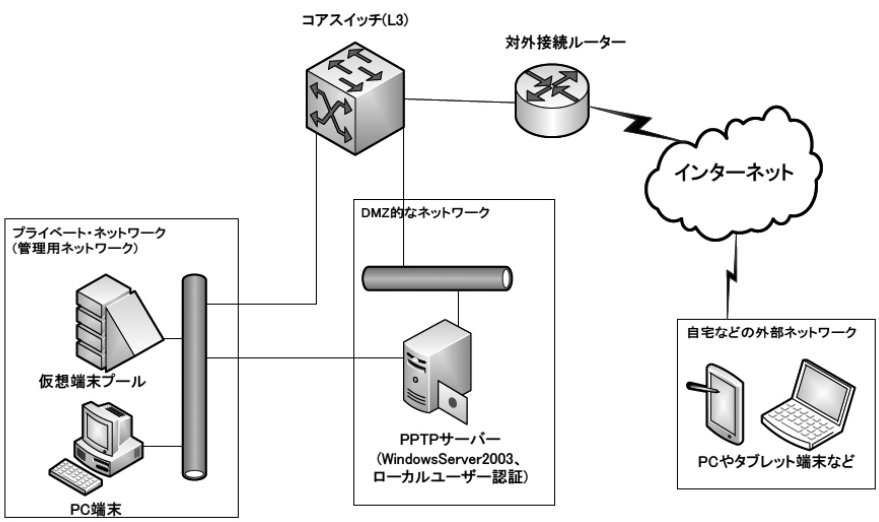

図２　Windows Server 2003 の VPN サーバーを利用したリモートアクセス構成
（ドメインユーザーでの認証）

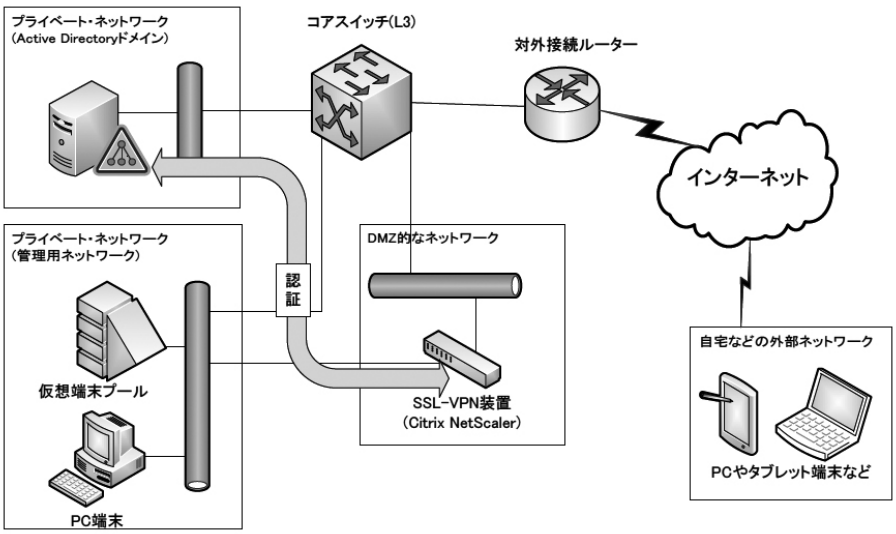

図３　SSL-VPN 装置を用いたリモートアクセス構成

どこからでもアクセスが可能であるということを主眼に置き、様々なネットワークからの接続性の確認として、ゲスト用の接続環境を提供しているいくつかの大学のネットワーク、一般の宿泊施設が提供しているプロバイダのネットワーク、NTT ドコモなどが提供している 3G 回線を利用したネットワーク、モバイル WiMAX を利用したプロバイダのネットワークからのアクセスを行った。

大学や一般の施設のネットワークからは安定した接続が確認されたが、3G 回線やモバイル WiMAX など移動体通信の場合、遅延の度合い (おおむね RTT が 300ms を超えると RDP 接続は不安定となった) などで安定度に差異が生じることが確認された。

VPN 接続の実際

学習院外部のネットワークから学習院内部のネットワークに接続するための環境の構築、および接続試験を行った。クライアントごとの接続性は表 7 にまとめた。

外部ネットワークからの接続のために、Windows Server 2003 の PPTP-VPN サーバー、および SSL-VPN 装置を用い、安全なネットワーク経路を用意した。

本研究グループメンバーにより、PC（Windows Vista/7)、Tablet 端末（iPad, Android)、携帯端末（iPod Touch）などを用い、学習院内の資源にアクセスする実験を行った。

今回の VPN 接続にはユーザー名とパスワードを使ったユーザー認証を利用した。Windows サーバーを利用したものでは、最初にサーバー上のローカルユーザーを利用し接続できることを確認し（図１)、引き続きサーバー自身を学内の Windows ドメイン（Active Directory）に参加させドメインユーザーで接続できることを確認した（図２)。なお、RAS サーバーの接続ポリシーにすべて

のドメインユーザーを許可するのではなく、特定のセキュリティグループに属するメンバーのみ許可する設定を行った。iOS、Android OS での設定例は、図 4 の通りである。図 4 のように設定自身はシンプルで、VPN サーバーの IP アドレスがわかっていれば設定は完了する。VPN 接続時には、それぞれユーザー名、パスワードの入力を促す表示がなされるので、それらを入力すれば VPN 接続は完了する。

図 4　iOS/Android での VPN クライアント設定画面

Citrix 社製の SSL-VPN 装置を利用した VPN 接続も同様に、ユーザー名とパスワードを使ったユーザー認証を利用し、認証を通過したユーザーのみ学内ネットワークに接続できるよう構成した（図 3）。認証には、Windows ドメインを利用し、前述の環境同様の設定を行った。この SSL-VPN 装置に接続するためには、Citrix 社が用意している Windows 専用のプラグインソフト（無償）を入手し、あらかじめ接続する PC にインストールしておく必要がある。インストール後、Internet Explorer などのブラウザで SSL-VPN 装置に接続し、ユーザー名、パスワードで認証を行う（図 5）。認証を通過し、接続が完了するとそれを示す表示に画面が遷移し、学内の資源にアクセスが可能となる。

図５　SSL-VPN の認証画面 (Internet Explorer)

Windows PC クライアントを利用する場合は、Windows Server で構築した VPN、SSL-VPN アプライアンス製品でのもの、どちらにおいてもクライアント側の VPN 接続設定を一度してしまえば容易に、学習院内のネットワークに接続できることが改めて確認できた。それ以外の端末を利用する場合、今回用意した Citrix 社製の SSL-VPN 装置では、接続のためのソフトウェアが用意されていないため評価ができなかった。他の SSL-VPN 装置を利用する場合も接続のためのソフトウェアが必要な製品の場合は、同様の懸念が残る。SSL-VPN 装置を使う場合、学外でのネットワーク環境にあまり左右されることがないため接続性の観点からは評価できるが、端末の多様性には乏しいので、利用するユーザー側の容易性には疑問が残った。

表７　VPN 接続性

	MS-PPTP	SSL-VPN
PC（Windows Vista）	○	△
PC（Windows ７）	○	△
iPod Touch（iOS ４/ ５）	○	×
iPad（iOS ４/ ５）	○	×
Android（３. １）	○	×
Android（４. ０）	○	×

○：接続可、△：専用プラグインソフトの利用で接続可、×：接続不可

SSH ポート転送による VPN 接続の代用

PPTP、SSL-VPN が利用できない環境の場合でも、SSH が利用できる環境であれば SSH のポート転送機能を利用し、学習院外部のネットワークから学習院内の PC へリモートデスクトップ接続を行うことは可能である。今回は Vine Linux 6 で作成した外部から限られたユーザーのみ接続できる SSH 接続できるサーバーを用意し、それを利用して動作確認を行った。

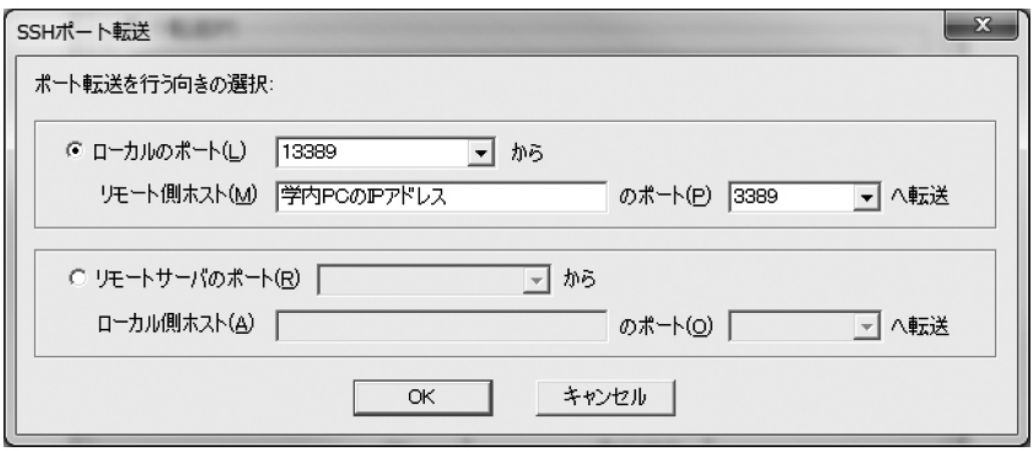

図6　ポート転送設定の一例 (Tera Term)

図 6 は、SSH クライアントとして Tera Term を利用した場合のポート転送の一例である。ここでは、任意のローカルポート（13389）を待ち受けポートとし、これを接続先のリモートデスクトップ接続を許可した PC の 3389 ポートに転送する設定を例示している。リモートデスクトップ接続では、localhost:13389 を接続先に設定することで、設定してある学内 PC に接続することができる。Windows 端末の場合として Tera Term を例示したが、Android 端末の場合、表 6 の ConnectBot という SSH クライアントで同様の設定を、iOS では iSSH というクライアントで同様の設定ができ、リモートデスクトップクライアントとの組み合わせで同様の接続ができる。Windows、Android の場合、無料のクライアントソフトで実現できたが、iOS では今回無料の SSH クライアント（zatelnet など）ではポート転送の機能を持っておらず、有料のものしか確認が取れなかった。

SSH ポート転送を使うことで、VPN サーバー環境が不要となるが、SSH 接続可能なサーバーやクライアントに複数のソフトウェアのインストールや設定をすることが必要となり、一般ユーザーが利用するのは容易ではない。

リモートデスクトップ接続

VPN 接続を確立させた後、接続先の管理用ネットワーク内にある実 PC（Windows Vista/7）、仮想デスクトップ環境に接続を行った。

実 PC にはアプリケーション一覧（表４）に挙げたソフトウェアを利用し、リモートデスクトップ接続を行った。今回は、どの OS 環境でも無償のソフトウェアを利用したが、特段問題なく接続ができ、操作も特別問題はなかった。それぞれのソフトウェアに特徴はあるものの、管理用として使うには十分な機能とパフォーマンスを備えていた。

リモートデスクトップ接続を行った実 PC には管理用のアプリケーション（TeraTerm, vSphereClient など）、遠隔地から利用できるライセンスを持ったアプリケーション類（MS-Office など）があらかじめインストールされおり、PC 自体は計算機センターで管理している Windows ドメイン環境（GCS09）に参加しているので、ドメインユーザーでリモートデスクトップ接続を行うことができる。本研究で利用した PC は、プロジェクトメンバー個々のもので、接続できるドメインユーザーを個々に制限した。管理用アプリケーションを利用し、実際のサーバーの状況確認や設定変更などを試行的に行っている。

さまざまな端末が利用できるようになったことで、いつでもどこでも管理できるような環境が整いつつあるがどのように運用するかが今後の課題となろう。

仮想デスクトップ環境

一般ユーザーの利用を想定し、特定の端末へのリモートデスクトップ接続ではなく仮想デスクトップ環境（VDI）を用意した。VDI には、VMWare 社の VMWare View、Citrix 社の VDI-in-a-box、Microsoft 社のターミナルサービスなどがあるが、今回は本プロジェクトとは異なるが計算機センター共通設備として導入した Citrix 社のものを利用した。Citrix 社の VDI 上でクライアント OS として Windows 7 Enterprise を使い、既存のドメイン環境（GCS09）に参加させクライアントを構築した。このクライアントも前節のリモートデスクトップ接続用の実 PC と同様にライセンス上問題のないアプリケーションをインストールしクライアントを構築した。アプリケーションには、自製のレポート管理も合わせて導入し、学外からレポート回収やレポート設定ができるように構築した。Citrix 社製の VDI では、独自のプロトコルである ICA プロトコルを利用した通信と、Windows 標準の RDP を使った通信のどちらでも利用が可能となっている。RDP を使った接続では、特別なソフトウェアは必要としないが、動画などではコマ落ちが起きるなど通常の PC と同等に扱うことは厳しい。ICA プロトコルと専用プラグインソフトを利用することで、Citrix 社の HDX 技術を利用した高品質な画面転送を行うことができ、今回利用したモバイル回線や出先のネットワークからのリモートアクセスのように比較的狭帯域でもストレスのないリモートデスクトップ接続が可能である。

この VDI の利用は、Windows 環境では、専用プラグインソフトの併用、iOS や AndroidOS では、専用ソフトウェアの Citrix receiver（無償）を使うことで可能となり、一般ユーザーが学内環境を

利用するのには比較的容易な手段であることが実証できた。

ただし、VDI をセキュリティ上、インターネットには直接設置することができないため、接続するために安全な経路（VPN など）を用意する必要がある。そのため、VPN 接続の設定などが必要となる。

今回は、VPN 接続から仮想デスクトップへの接続まで一回のログオンで済ませるいわゆるシングルサインオンの環境を構築できなかったため、管理者以外の一般ユーザーが容易に利用する環境を構築するに至らなかった。SSL-VPN 装置との連携などシングルサインオンの環境構築が今後の課題として残った。

まとめと今後の展望

PPTP を利用した VPN 接続は比較的さまざまなプラットホームに対応し接続性が良いことが確認できたが、この接続の認証に利用している MS-CHAPv2 の脆弱性が本稿作成中に報告され、セキュアなサービスとして一般に提供することができなくなった。このため、今後接続性の良い代替手段を検討する必要が出てきた。SSL-VPN も有効な代替手段の一つではある。しかしながら、今回構築した環境（NetScaler+ActiveDirectory）は、現状では専用クライアントソフトウェアが必要で、対応するプラットホームも限られているため汎用性の点で問題が残る。今後 receiver と SSL-VPN 装置の連携が予定されているので、それが実現すると利便性の向上が期待される。また、PPTP の代替として L2TP-VPN なども候補の一つで今後構築が必要となろう。

本プロジェクト終了後ではあるがこのプロジェクトの継続として、2012 年 4 月からの新システムと連携させた Windows Server 2008 R2 を用い、リモートデスクトップゲートウェイサーバー（RDGW サーバー）を試験的に構築した。これは、RDP over HTTPS のゲートウェイサービスを実現するもので、リモートデスクトップ接続を許可している PC に、VPN 接続の設定をすることなく HTTPS のみでインターネットから安全にリモートデスクトップ接続できるものである。今回は、セキュリティ確保のため RDGW サーバーを学習院の内部ネットワークに設置し、インターネットとの接続部分には、このサーバーへの HTTPS（443/TCP）接続のみを代理接続させるリバースプロキシーを設置した。

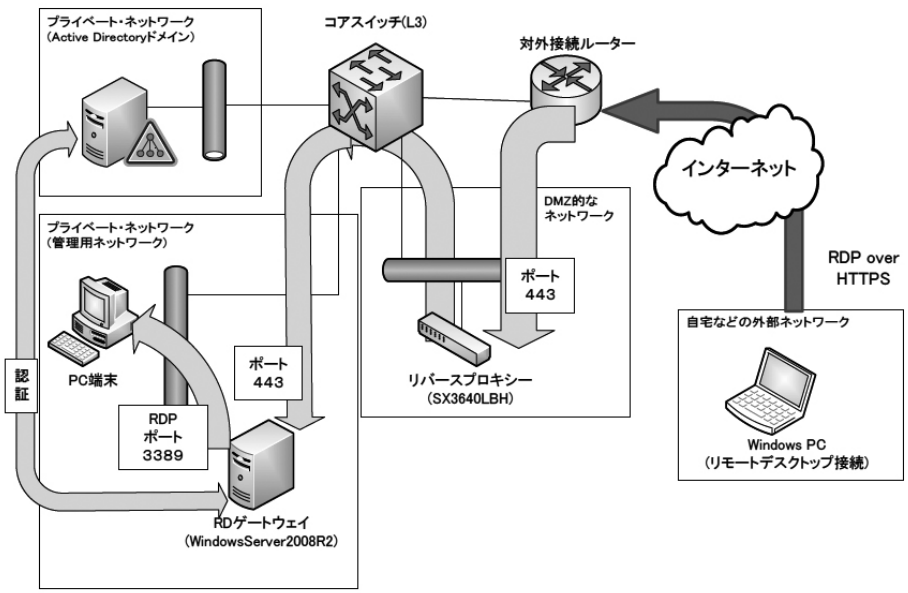

図7　リバースプロキシーと RD ゲートウェイを用いたリモートアクセス構成

Windows PC が利用できる環境にある場合、OS に付属しているリモートデスクトップ接続クライアントと RDGW サーバーを利用することで、一般利用者も比較的容易に学内ネットワーク内の PC に接続できることが分かったが、接続できる PC をどのように用意し提供していくかが今後の課題の一つである。もちろんその場合のライセンスの整備も同時に必要となってくる。

本プロジェクトで物理的な管理用のリモートアクセス環境は整ってきたが、これらを運用するポリシーの制定など運用面が今後の課題の一つである。