第２回 情報大学のネットワーク、メール、ssh、scp、VPN 接続

大学 PC 利用 tuispc-2

2-1. 情報大のネットワーク・セキュリティ

コンピュータ実習室の全端末は各種サーバーと接続されているが、ファイヤーウォール、不正侵入防御システム、アンチウィルスゲートウェイを組み合わせたセキュリティの強化により、端末の自由度を確保し、利用者の利便性と安全性を実現した。

ノートパソコンの接続には、SSL 暗号化による認証スイッチを経由して学内 LAN にアクセスすることで、より安全なネットワークサービスを実現している。

(http://www.tuis.ac.jp/facility/1125.html から引用)

2-2. サーバーシステム

情報教育システムの基幹サーバーは、IBM eServer pSeries の高性能ファイルサーバーを中心として、10 台以上のサーバー群と PC サーバー群から構成され、ネットワークサービスを支えている。これらの基幹サーバー群は、Windows 及び Linux の両システムを一括管理するための特別な仕組みを有し、学内 500 台以上の端末に対する Windows 移動プロファイルを可能にするために負荷分散されたサーバー群の構成により、Windows ファイルサーバー・認証サーバーとしての負荷軽減を実現した。

(http://www.tuis.ac.jp/facility/1125.html から引用)

- gateway.edu.tuis.ac.jp 各人のデータを保管するサーバー(Z ドライブ)
- filesvr.edu.tuis.ac.jp 教材用のデータなどを保管するサーバー(Y ドライブ)
- 各自の WEB データを保管するサーバー（W ドライブ）。ただし、Z ドライブの各自のスペースの一部。
- レポート等の提出用のサーバー(V ドライブ)

2-3. 一般教室の情報コンセントと無線ＬＡＮ

(1) 表 2-1 の一般教室にも「情報コンセント」と「電源」を設置し、講義形式の授業においてもノートパソコンを利用することができる。

(http://www.tuis.ac.jp/facility/1125.html から引用)

(2) 無線 LAN ルーターが学内の多くの場所に設置されています。JOHOMOBILE の SSID のワイヤレス接続として PC に認識され、認証手続き後、利用可能となる。

表 2-1　学内の情報コンセントと電源のある教室

建物	フロア	教室番号	情報コンセント	電源
1 号館（本館棟）	1 階	101	あり	あり
	2 階	201・202・221	あり	あり
	3 階	301・302・303・322・323	あり	あり
	4 階	401・402・403・404・421 422・423・424	あり	なし
	5 階	526・527	あり	あり
4 号館（総合情報センター）	1 階	801(メディアホール)	あり	あり
		802（メディア・サブ・ホール）	あり	あり

(1) 情報大ネットツールの利用方法

必携 PC には、図 2-1 の情報大ネットツールが組み込まれている。情報大ネットツールは、左下の「スタートボタン」、「すべてのプログラム」、「情報大メニュー」、「Network」のフォルダに「情報大ネットツール」から選択できる。

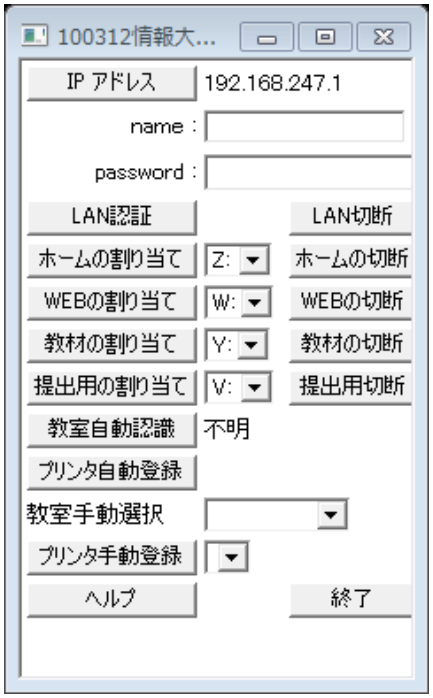


図 2-1　情報大ネットツールの操作画面

情報大ネットツールの name に各自のユーザーID、password にパスワードを入力し、「LAN 認証」をクリックする。教室が認識されるとともに、もよりのプリンタの登録が可能である。情報大学のコンピュータリソースを利用するための便利なツールである。

情報大ネットツールの機能は、Windows により提供される「ネットワークドライブの割り当て」の機能である。

2-4.　メールの設定と利用

(1) 大学の Web メール・サービスの利用

① 在学生・保護者の方へのページへ

図 2-2 に示すように、http://www.tuis.ac.jp から「在学生・保護者の方へ」をクリックする。

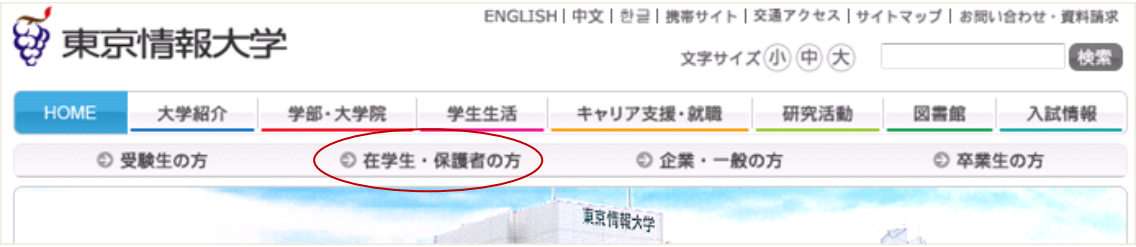


図 2-2　情報大のトップページ(http://www.tuis.ac.jp)

② Web メールへ

図 2-3 に示すように、在学生専用コンテンツのメニューから「Web メール」をクリックする。

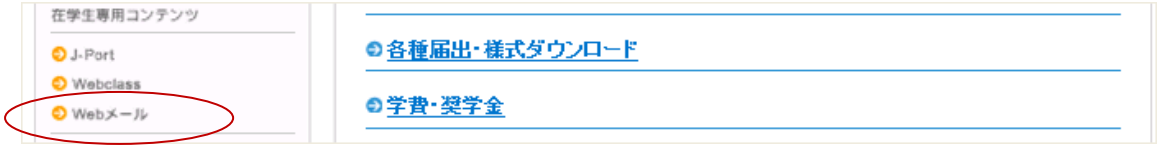
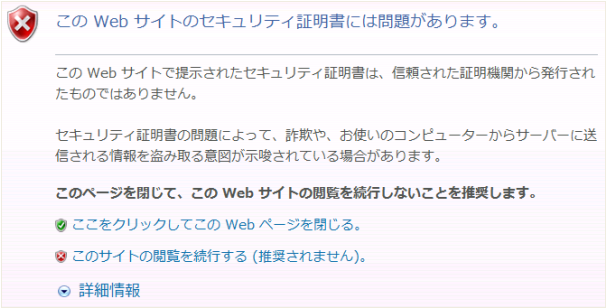


図 2-3　在学生専用コンテンツのメニュー

③ Web メールサイトのセキュリティの警告



②の Web メールへをクリックすると、図 2-4 に示すように、セキュリティ証明書の問題が表示される。大学のサイトであり、問題がないので、「このサイトの閲覧を続行する(推奨されません)。」を選択する。

図 2-4　セキュリティの問題表示

④ Web メールの作成と発信

Web メールのログイン画面(図 2-5)が表示されるので、各自のユーザ ID とパスワードによりログインする。

ユーザ ID：e12xxxaa
パスワード：・・・・・・・・

図 2-5　ログイン画面

次のアドレスを直接入力し、Web ブラウザの「お気に入り」に登録しておくと、便利である。
https://webmail.edu.tuis.ac.jp

⑤　Active! Mail の初期画面

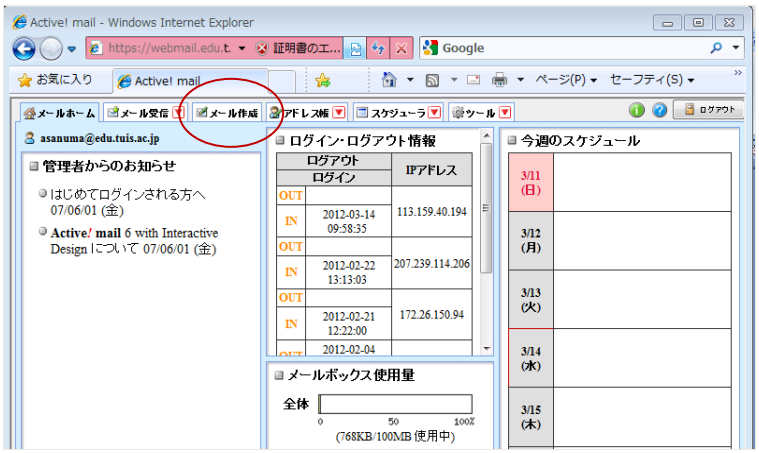


図 2-6　Active! Mail 初期画面

図 2-6 に示すように、Active! Mail の初期画面が表示される。「メール受信」と「メール作成」の他、いくつかの機能が提供される。
ここでは、「メール作成」をクリックする。

⑥　メール作成

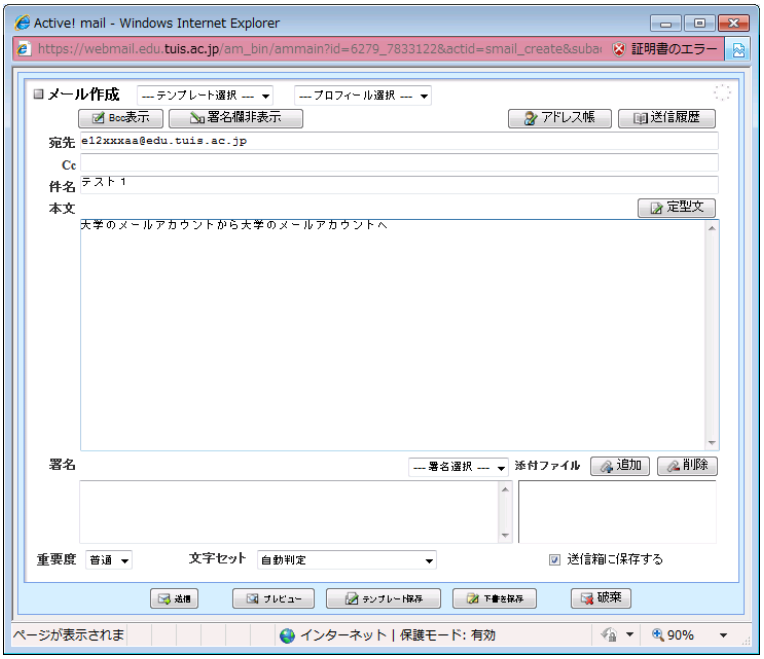


図 2-7　メールの作成画面

図 2-7 のように、メール作成の画面が表示される。
ここでは、自分から自分へメールを送信し、Web メールの機能を確認する。
このため、
宛先：
e12xxxaa@edu.tuis.ac.jp
件名：テスト
本文：
大学のメールアカウントから大学のメールアカウントへ
とし、左下の「送信」をクリックする。

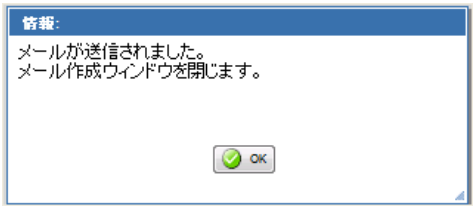
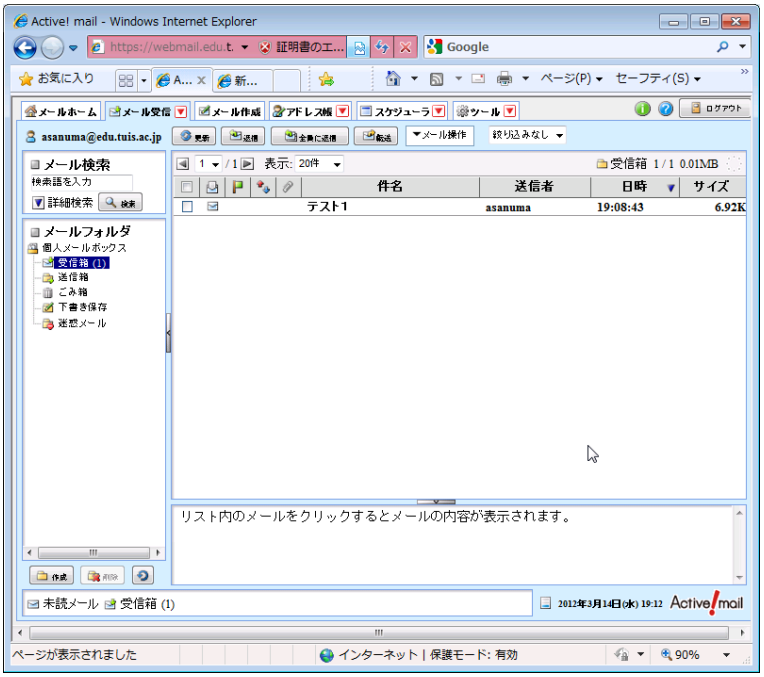


図 2-8　メール送信の正常終了

メールアドレスに誤りがなければ、図 2-8 のように正常に送信された旨、情報が表示される。「OK」をクリックし、メールの送信を終了する。

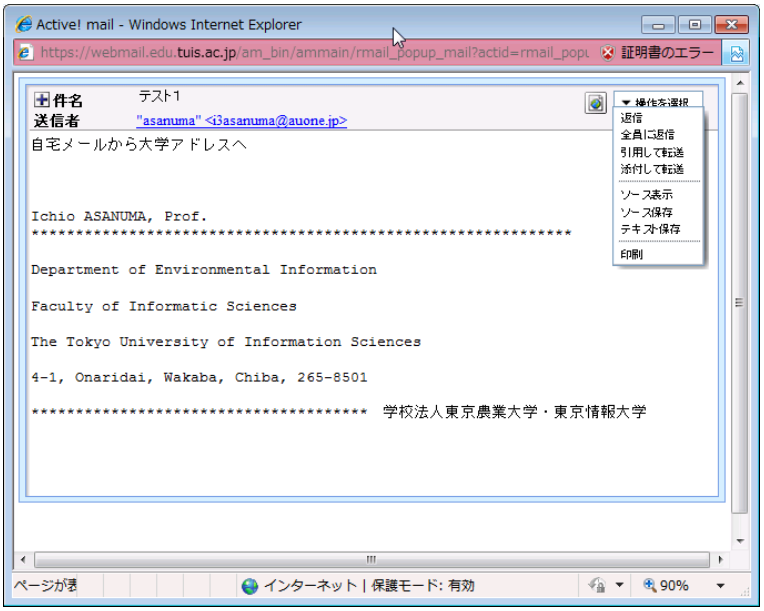
⑦　Web メールの受信と読み込み、プリント、削除



「メール受信」タブをクリックすると、受信メールの一覧が表示される(図 2-9)。

メールをクリックすると、ウインドウの下部にメールの内容が表示される。また、メールへの返信、転送、削除などの作業が可能である。

図 2-9　Web メールのメール受信のウインドウ



メールに対する作業は、メールをダブルクリックすると、図 2-10 のように、メールの内容が表示され、さらに、右上の「操作を選択」をクリックすることで、

返信、全員に返信、引用して転送、添付して転送、ソース表示、ソース保存、テキスト保存、印刷

の作業が可能である。

図 2-10　メールの表示とメールの操作

⑵ メールの送受信

① 必携 PC を利用し､大学のメールアカウントから携帯電話へメールを送信する。

図 2-11 に示すように、

a. Web ブラウザから、情報大のトップページ、在学生保護者の方へ、Web メールを選択し、メール作成を選択する。

b. メール条件
宛先：**e12xxxaa@auone.jp**　　など、自分の携帯のメアド。
CC：　　空白とする。
件名：**テスト１**
本文：**大学の Web メールから携帯へ。**

c. メールの送信
メールを作成後、送信アイコンをクリックする。

d. 携帯電話にメールが届くことを確認する。

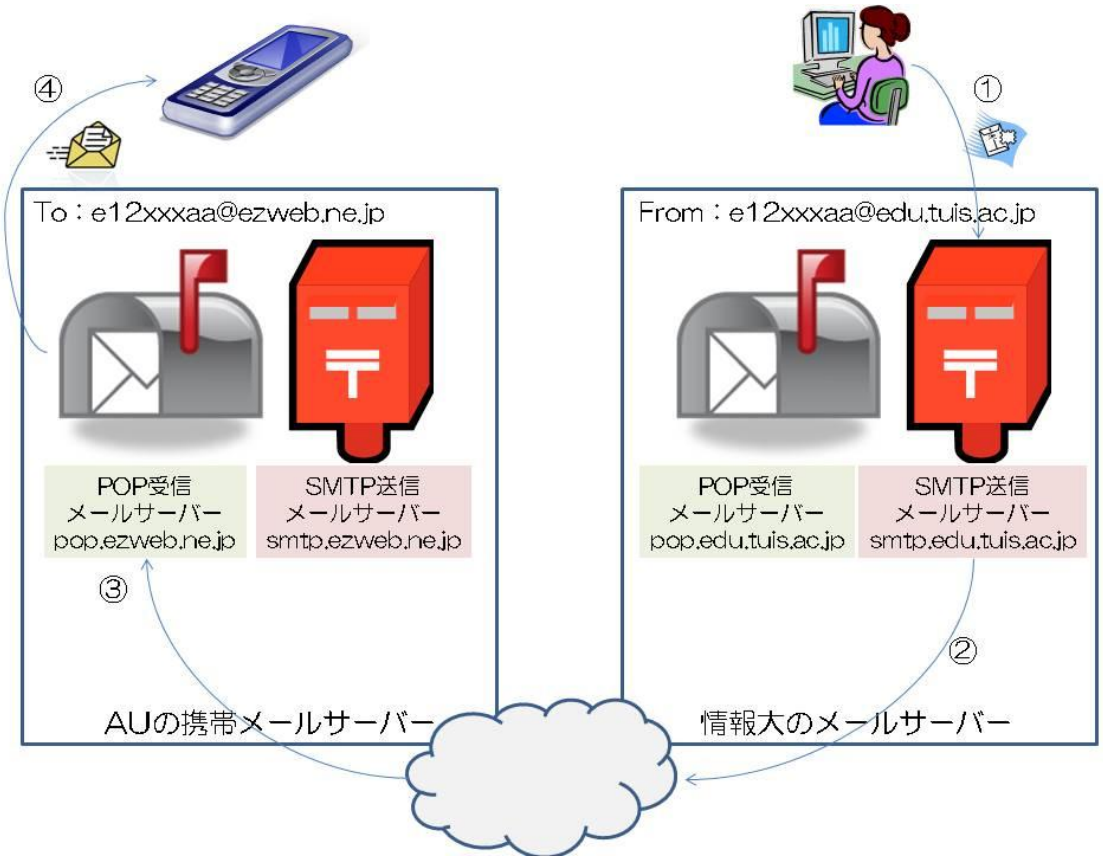


図 2-11　大学の Web メールから各自の携帯へ

② 携帯電話から大学のメールアカウントへメールを送信する。

図 2-12 に示すように、

a. 携帯電話で、大学の自分のメールアカウント宛のメールを作成する。

b. メールの条件
宛先：**e12xxxaa@edu.tuis.ac.jp**　　e12xxxaa は自分の学籍番号とイニシャルである。
件名：**テスト２**
本文：**携帯から大学の Web メールへ。**

c. メールの送信
携帯電話からメールを送信する。

d. メールの確認
Web ブラウザから、情報大のトップページ、在学生保護者の方へ、Web メールを選択し、メール受信を選択する。

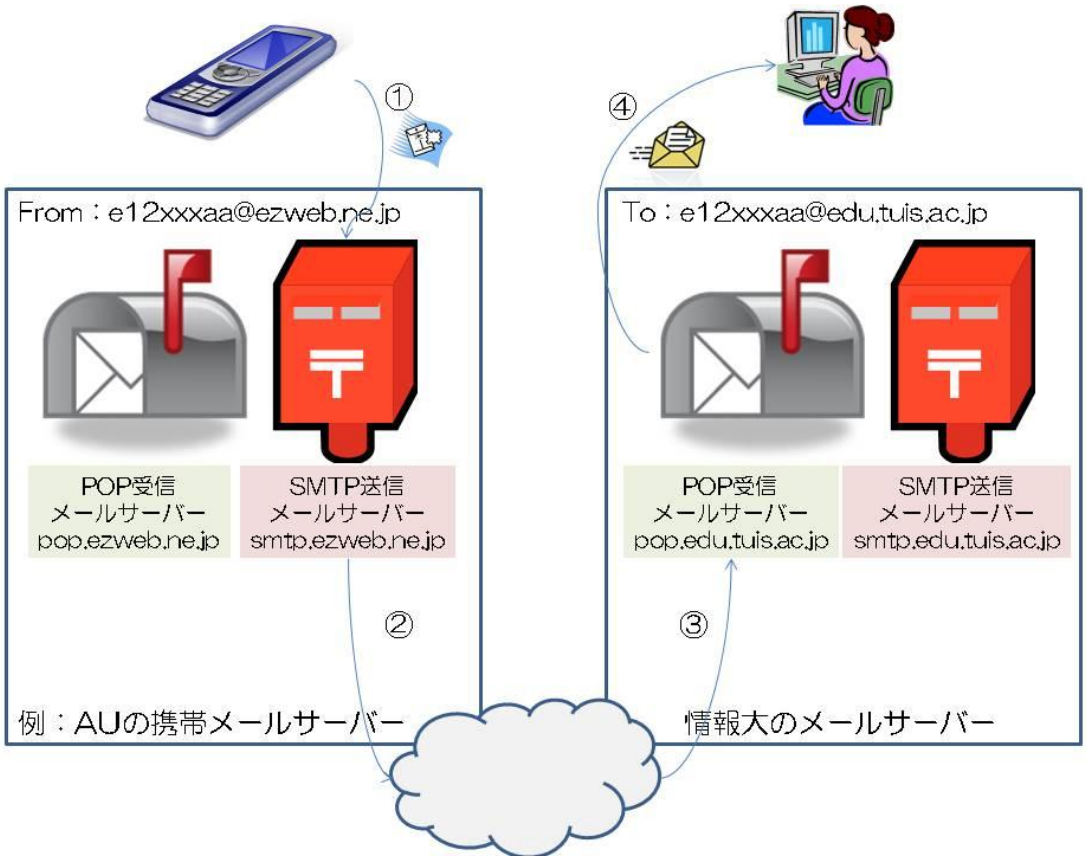


図 2-12　携帯電話から大学の Web メールへ

(3) Outlook などメーラソフトの設定と利用

必携 PC の Outlook メーラソフトを利用して、メールの送受信を行う場合の設定方法の紹介である。

① 送信サーバー（SMTP）と受信サーバー(POP)の設定

マイクロソフト・オフィスのメーラソフトの一つである Outlook のアカウントの設定例を図 2-13 に示す。代表的な POP3(Post Office Protocol version3)の設定例である。POP3 は、ポスト・オフィス・プロトコル(郵便局通信規約)の一つである。

ユーザ情報：電子メールアドレスなどの連絡手段の情報を示す。
名前：myaddress　のように、名前は自由に付けることができる。
電子メールアドレス：連絡をとるためのメールアドレスであるが、メールサーバーへのログオン情報のアカウント名と同じにすると混乱が少ない。

サーバー情報：POP3 対応のメールサーバーを指定する。
受信メールサーバー：ここでは、gmail において利用される pop サーバー名の例を示す。
送信メールサーバー：ここでは、受信メールサーバーと対応した smtp サーバー名を入力する。SMTP(Simple Mail Transfer Protocol)は、簡易メール伝送通信規約であり、送信サーバーのメールサーバーとして利用される。

メールサーバーへのログオン情報：サーバーへのアクセスのためのログイン
アカウント名：ここでは、メール契約先のアカウントとしてメールアドレスを入力する。
パスワード：アカウント用のパスワード。＊としてエコーバックされる。

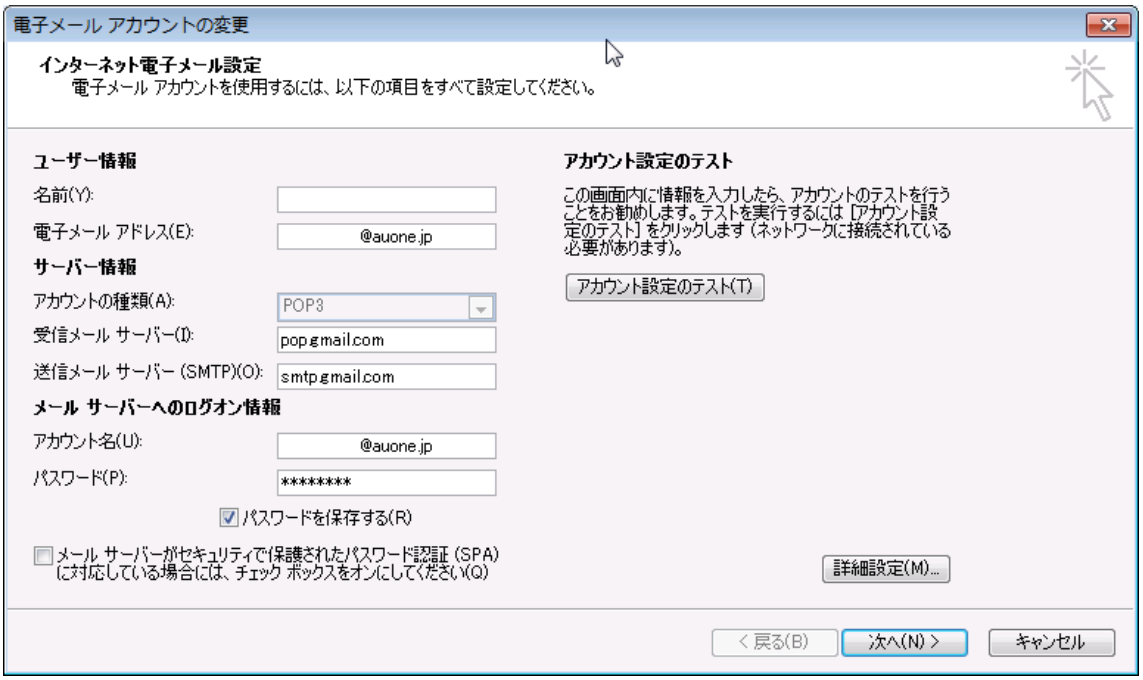


図 2-13　Outlook のメールアカウント設定例

② メールの転送設定

大学のメールアドレスへメールが届いた場合、前述の Web メールを利用し、閲覧する方法が便利である。しかし、Web メールを開ける場所は限定され、緊急の連絡ができない。そこで、メール転送機能を利用すると、例えば、大学のメールアドレスへ届いたメールを、携帯電話のメールアドレスへ転送することができる。さらに、大学のメールサーバーへも届いたメールを残しながら、携帯電話へ転送する設定も可能である。

３年後期からの就職活動では、企業からのメールを漏れなく、しかも、タイミング良く受け取る必要があり、このメール転送機能は重要な機能である。携帯電話のメールアドレスを変更した場合は、転送設定のメールアドレスを変更する必要がある。転送先が変更になりながら、転送設定をそのままにしておくと、メールが大学のメールサーバーへ届いていながら、転送先へ転送されないため、送信者へは「送信に失敗しました。」とエラーメッセージが送られてしまう。就活先に心配をかけるので、メールアドレスの変更に際しては、最新の注意が必要である。

a. メールの転送設定

メール転送の設定ファイルは、大学の gateway.edu.tuis.ac.jp の.forward(ドット・フォーワード)に記述する。次の例は、

```
.forward
    myaddress@ezweb.ne.jp
    e12xxxaa
```

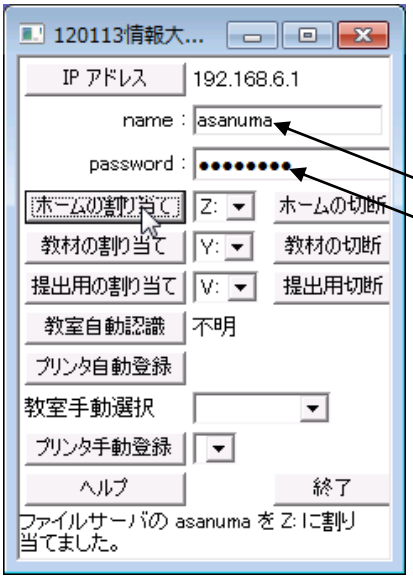
大学宛のメール(To：e12xxxaa@edu.tuis.ac.jp)を AU の契約メールアドレス(To：myaddress@ezweb.ne.jp)へ転送し、さらに、大学のメールサーバーへメールを残す設定である。

学生さんへ：
皆さんは edu ドメインメールのみですので、.forward は gateway.edu.tuis.ac.jp に記載します。ただし、初期状態では.forward は存在しません。新しく、作成します。
先生方へ：
2011 年夏以降、
edu ドメインメールの転送設定(.forward)は、gateway.edu.tuis.ac.jp に記載。
rsch ドメインメールの転送設定(.forward)は、mailhost.rsch.tuis.ac.jp に記載。
のルールとなります。移行に際し、旧システム(gateway.edu.tuis.ac.jp)の.forward を mailhost.rsch.tuis.ac.jp へ転記したそうです。edu に.forward を記載しない場合、edu ドメインメール宛のメールは gateway.edu.tuis.ac.jp に残ります。

b.　.forward の作成あるいは編集方法

- 大学の PC を利用し、ホームディレクトリにおいて、.forward を作成あるいは編集する方法
  大学の実習室の PC を立ち上げると、Z ドライブが各自のホーム・ディレクトリとなる。「.forward」をサクラエディタにより、作成あるいは編集する。

- 学内において、必携 PC に大学サーバーの Z ドライブを接続し、.forward のファイルを作成あるいは編集する方法



a.　図 2-14 に示すように、情報大ネットツールを立ち上げ、ユーザ ID、パスワードを入力後、Z:ドライブであることを確認の上、「ホームの割り当て」のアイコンをクリックする。

学籍番号とイニシャル　　e12xxxaa
パスワード　　・・・・・・

ホームの割り当てが成功すると、メニュー画面下部に「ファイルサーバの xxxxx を Z：に割り当てました。」と成功のメッセージが表示される。

図 2-14　情報大ネットツールのメニュー画面

ネットワークドライブのＺ：としての割り当ての結果、¥¥gateway.edu.tuis.ac.jp の各自のホームディレクトリを、図 2-15 に示すように、必携 PC の Windows で利用可能となる。

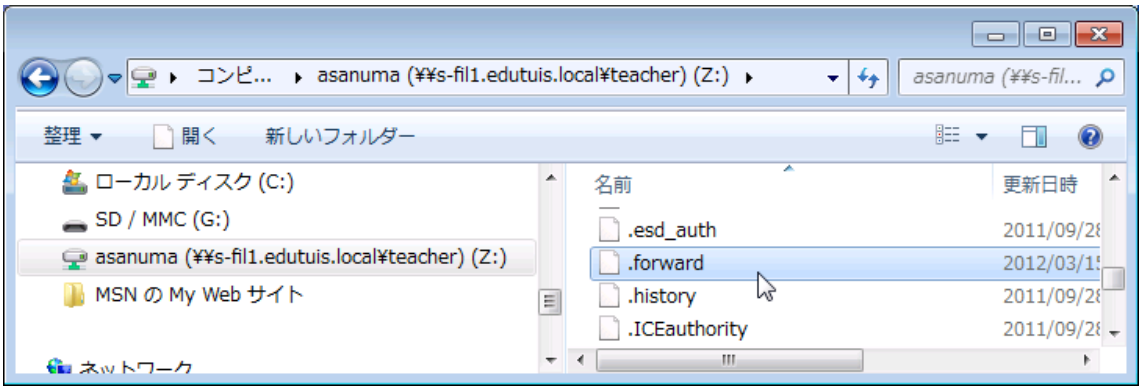


図 2-15　各自のホームディレクトリが Z:ドライブとして利用可能となる。

「.forward」を、サクラエディタを利用して、作成あるいは編集する。図 2-16 に示すように、1 行目に転送先のメールアドレス、2 行目に大学のメールアドレスを入力する。作成あるいは編集終了後、Ｚ：ドライブ(ホームディレクトリ)に、「.forward（ドット・フォワード)」と名前を付けて保存すること。

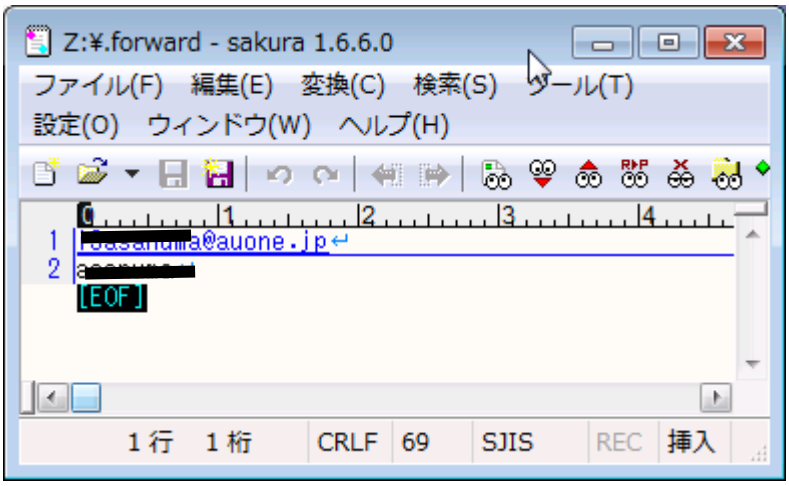


図 2-16　.forward のサクラエディタによる編集

c. 携帯電話から大学のメールアドレスへ送信し、大学の Web メールで確認するとともに、携帯へ戻ってくることを確認する。(図 2-17)

ⅰ） 携帯電話により、大学の自分のメールアドレス宛てのメールを作成し、送信する。図 2-17 の①～③.

宛先：e12xxxaa@edu.tuis.ac.jp

件名：テスト３

本文：携帯から大学の Web メールへ。テスト３。

ⅱ） メールの確認(その１)

Web ブラウザから、情報大のトップページ、在学生保護者の方へ、Web メールを選択し、メール受信を選択する。図 2-17 の④、⑧、⑨

ⅲ） メールの確認(その２)

携帯電話にメールが届いたことを確認する。図 2-17 の④、⑤、⑥、⑦.

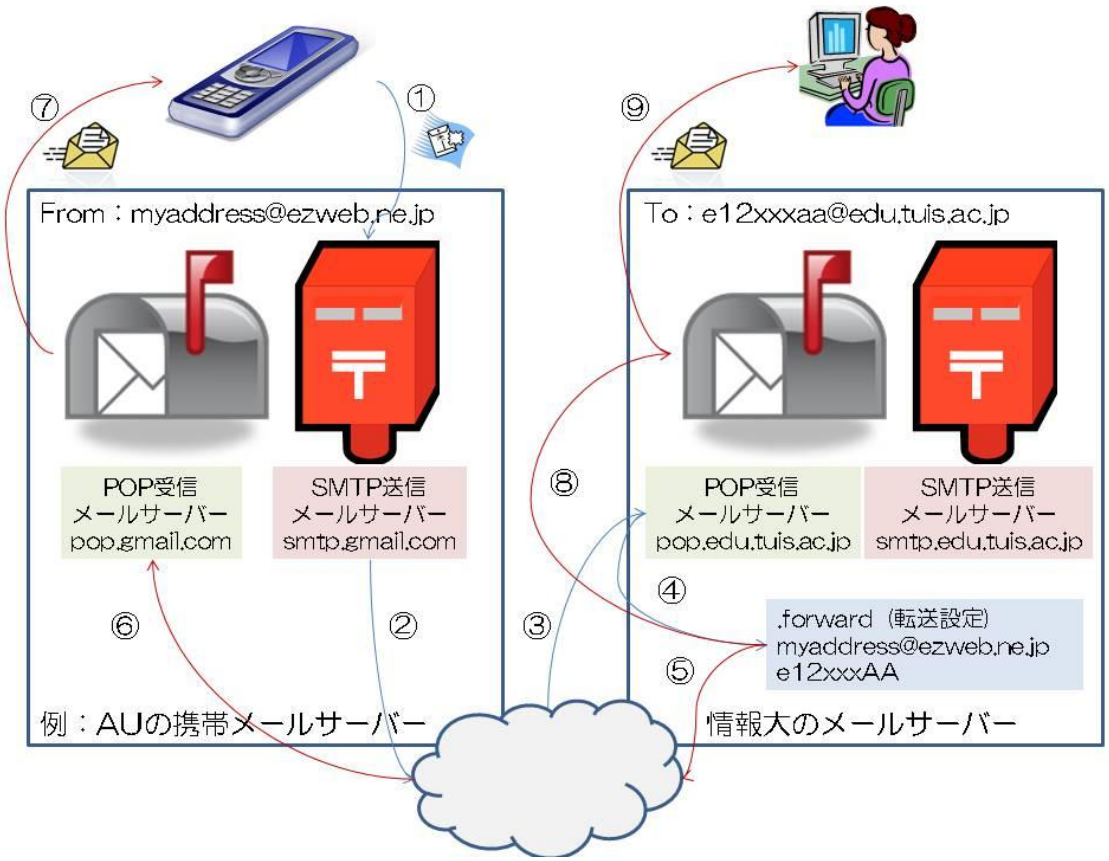


図 2-17　メールの転送設定と動作流れ図

2-5. VPN を利用した外部からの大学サーバーへの接続

(1) VPN とは

図 2-18 に VPN(Virtual Private Network：仮想的専用線)の概念図を示す。通常のインターネットを経由した外部から情報大学の学内サーバーなどへの接続は、ファイヤーウオールが存在し、自由なアクセスは制限される。情報大学のファイヤーウオールでは、外部からアクセス可能なサーバーが登録され、また、そのサーバーとの通信プロトコールもポートナンバーなどにより制限されている。大学のホームページへアクセスする際には、ホームページアクセス用の 80 のポート番号のみが許可されている。ほとんどの場合、ホームページの閲覧、ホームページ経由の J-port へのアクセス、Web メールなどの機能が提供されているので、問題はない。しかし、大学のサーバーへのアクセス、例えば、自分の Web サイトの修正と言った作業は困難である。

このため、VPN による仮想的専用線の機能が提供されている。これは、大学の VPN サイトから VPN の機能をダウンロードし、家庭の PC と大学の学内ネットワークの間に、仮想的な専用線(トンネル)を確立し、http 以外のアクセスを実現する手法である。図 2-18 に示すように、家庭の PC と学内ネットワークとに間に、赤の二重線で示した VPN のトンネルを構築し、トンネルを利用し、学内ネットワークのサーバーと通信を行う。

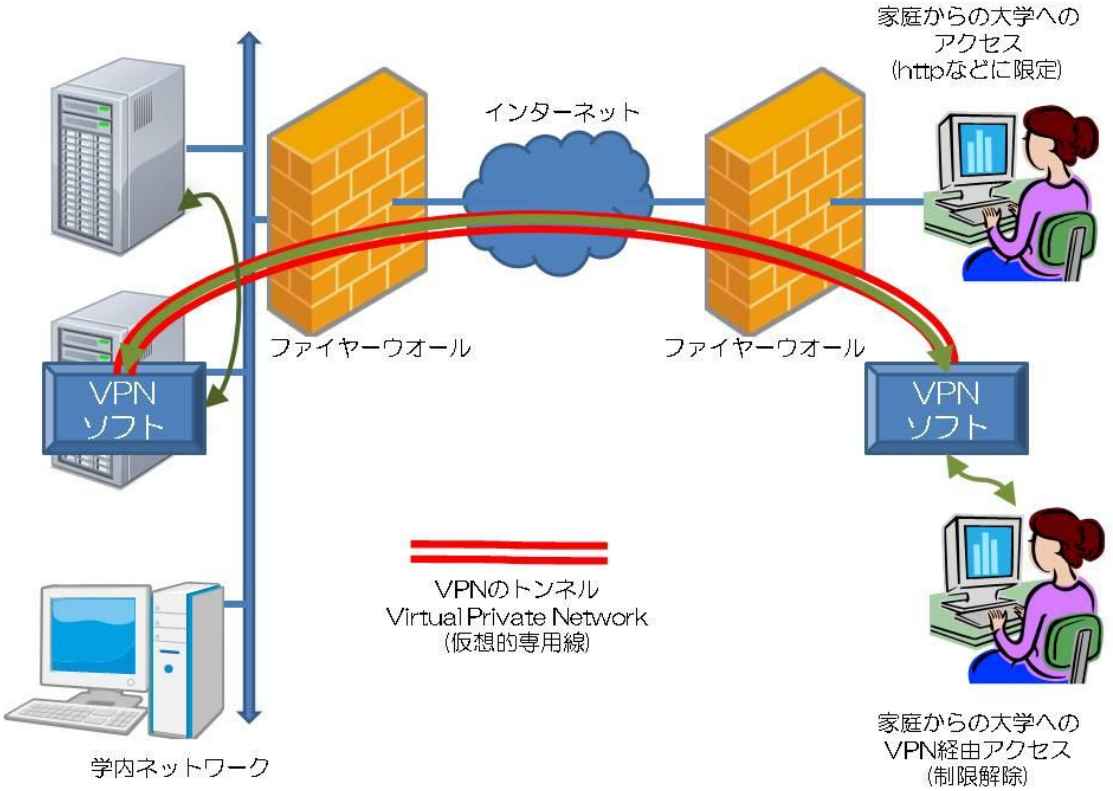


図 2-18 VPN(Virtual Private Network：仮想的専用線)の概念図

(2) 自宅から大学のサーバーへ接続

自宅の PC において、IE などの Web ブラウザを起動し、次のサイトへ接続する。

https://ssl.edu.tuis.ac.jp/

このサイトへのアクセスにより、図 2-19 のセキュリティ証明書による警告について「このサイトの閲覧を続行する。」を選択すると、図 2-20 の SSL VPN Service へのログイン画面が表示される。大学におけるログインと同様に、学籍番号＋イニシャル(e12xxxaa)とパスワードによりログインする。続いて、VPN 接続に必要なプログラムが、家庭の PC へダウンロードされ、続けてインストール作業が始まる。いつくかの質問に答え、VPN 接続を実現する。

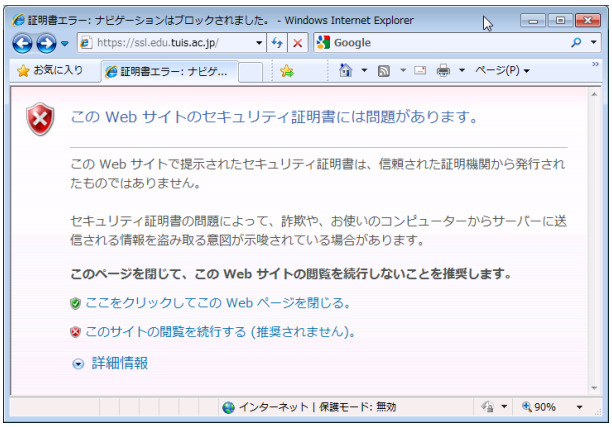


図 2-19　セキュリティ証明書の警告
→閲覧を継続する。

図 2-20　VPN 接続のログイン画面

図 2-21 のセキュリティ警告が表示されるので、情報大のサイトであることを確認しながら接続を行うこと。

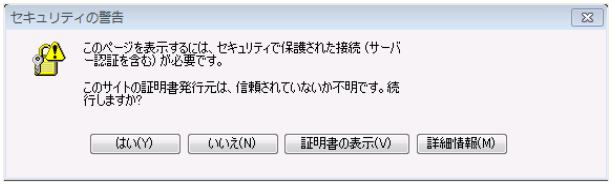


図 2-21　セキュリティ確認

図 2-22 は、VPN 接続が完了した状態のウインドウ画面である。「Connected」が表示され、大学のサーバーに対して、Web ブラウザ以外の操作が可能となる。

図 2-22　VPN 接続完了画面

(3) VPN 接続の遮断

VPN 接続の切断は、図 2-23 に示すように、右下の「隠れているインジケータを表示します」のアイコンをクリックし、「Cisco AnyConnect VPN Client Connected」のアイコンをダブルクリックすると、図 2-24 のウインドウが表示される。「Disconnect」をクリックすることで、VPN 接続が遮断される。

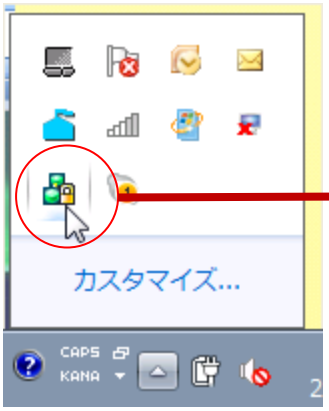


図 2-23　VPN 接続状況のアイコン

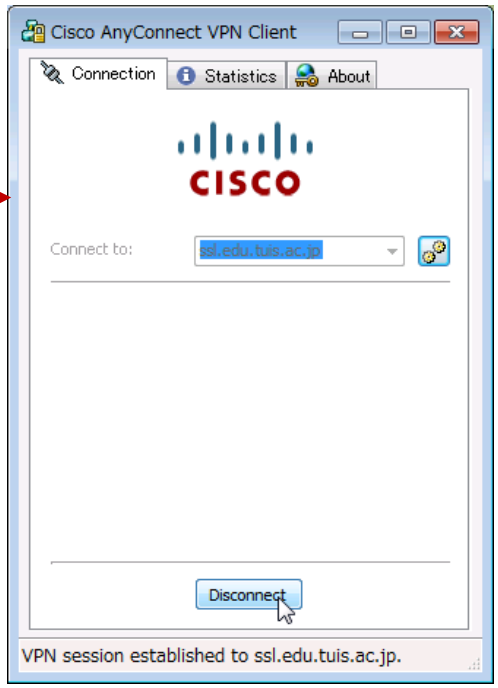


図 2-24　VPN 接続状況のウインドウ

2-6. TCP/IP と通信

(1) TCP/IP

インターネットの初期に定義され、現在も標準的に使われているプロトコルが、TCP(Transmission Control Protocol：伝送制御プロトコル)と、IP(Internet Protocol：インターネット・プロトコル)である。これらの二つのプロトコルとその他のプロトコルとを合わせ、インターネット・プロトコル・スイートと呼ばれるが、TCP/IP にちなみ TCP/IP プロトコル・スイートとも呼ばれる。TCP/IP は、異なるオペレーティングシステム間での通信を可能とするものであり、プロトコルが無料で開放されている。

インターネット・プロトコル・スイートは、①リンク層(ARP など)、②ネットワーク層(IP(IPv4、IPv6)など)、③トランスポート層(TCP など)、④アプリケーション層(FTP、Telnet、SSH、HTTP など)の一式の階層でもある。

TCP/IP プロトコル・スイートを利用し、コンピュータ同士がデータを交換する場合、ネットワーク層においてインターネット・プロトコル(IP)の約束に従い、IP アドレスにより相手側のコンピュータを指定する。さらに、トランスポート層において、トランスミッション・コントロール・プロトコル(TCP)の約束に従い、ポート番号により、コンピュータ上の複数のプログラムの中から通信相手のプログラムを指定する。表 2-1 に示すように、TCP の通信プロトコルにおいて、プログラムとポート番号の組み合わせが決められている。

ファイヤーウオールでは、IP アドレスとポート番号により、通過可能なパケットを制限し、不正なアクセスから内部のコンピュータを防御する。

表 2-1　トランスミッション・コントロール・プロトコル(TCP)におけるポート番号の例

種類	範囲	ポート番号の例	ポート番号の用途
汎用ポート番号	0～1023	20	FTP(データ)
		21	FTP(制御)
		22	SSH
		23	telnet
		80	HTTP
		443	HTTPS
		25	SMTP
		110	POP3
		・・・	
登録済ポート番号	1024～49151		
自由配当ポート番号	49152～65535		

(2) SSH

インターネット初期は、Telnet や FTP により、リモートのホストとのコマンドやデータの送受信を行っていた。しかし、Telnet や FTP がパスワードを保護することなくそのままの形式である平文で送信するため、ネットワーク上で盗聴される可能性が高いことから、この脆弱性(ぜいじゃくせい)が指摘された。このため、通信内容を暗号化し、盗聴対策を施した通信手法が SSH（Secure Shell：セキュア・シェル）である。

① Linux から

SSH を Linux から発行する際は、次のようなコマンドである。

ssh　e12xxxaa@gateway.edu.tuis.ac.jp
e12xxxaa@gateway.edu.tuis.ac.jp`s　password:　・・・・・

ここで、「ssh」は SSH のコマンド、@マークより左側の「e12xxxaa」はログインしようとするホストに登録されたユーザー名、「gateway.edu.tuis.ac.jp」はホスト名である。パスワードはエコーバックされない。

SSH により、ホストのコマンドを実行できる。

② Windows から

Windows において、SSH を実行するには、Tera Term のような SSH のプロトコル機能が組み込まれたフリーソフトを利用する方法が一般的である。

画面左下のスタートボタンから、「すべてのプログラム」、「東京情報大メニュー」、「Network」、「Tera Term」を選択すると、図 2-25 に示すように、Tera Term の初期画面が表示される。「gateway.edu.tui.ac.jp」のようにホスト名を入力する。

図 2-25　Tera Term の初期画面

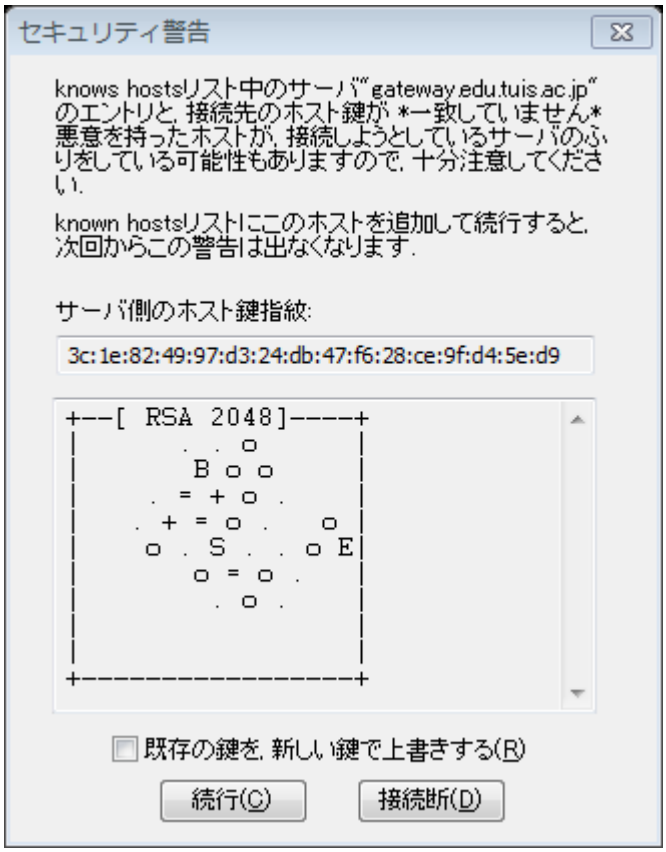
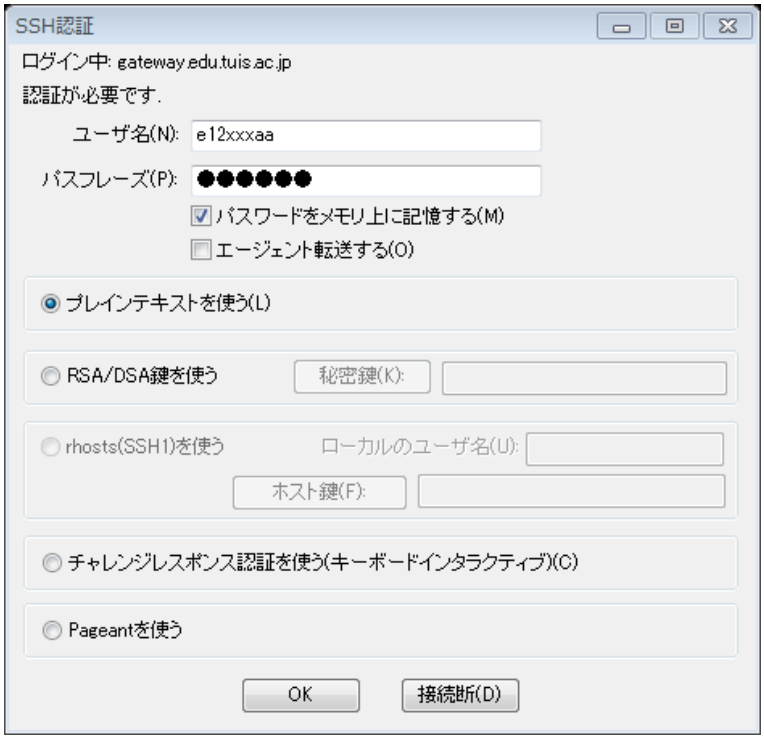


図 2-25 に指定したホストが始めての接続の場合は、図 2-26 に示すように、セキュリティ警告のウインドウが表示される。

このホストへのアクセスが２回目以降は表示されない。ただし、ホストのハードウエアが更新された場合は、ホストの鍵指紋が変更になるので、このセキュリティ警告のウインドウが表示される。

問題がないことを確認の上、「続行」をクリックする。

図 2-26　ホスト鍵指紋のセキュリティ警告



続いて、図 2-27 に示すように、SSH 認証のウインドウが表示されるので、ユーザ名、パスワードを入力する。

図 2-27　Tera Term の SSH 認証

図 2-28 に示すように、Tera Term のウインドウが開き、ホストの操作画面となる。

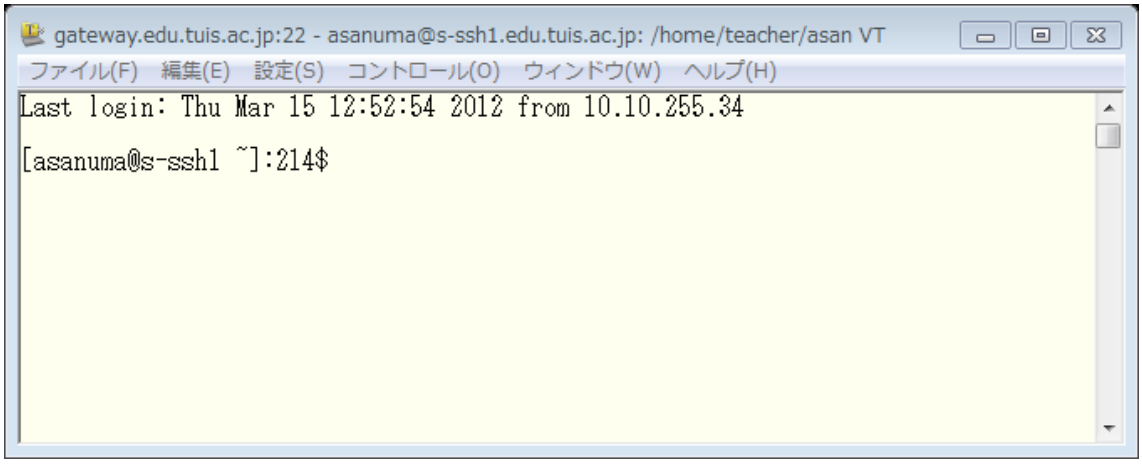


図 2-28　Tera Term 利用画面

(3) SCP

SSH の機能を利用し、セキュリティの保たれたデータの送受信を行うためのコマンドである。ログインのための認証情報、送受信のためのデータともに、暗号化されてネットワーク上を流れる。

① Linux のファイルをホストへアップロードする場合

SCP により Linux のファイルをホストへアップロードする際は、次のようなコマンドである。

scp　aaaaa.txt　e12xxxaa@gateway.edu.tuis.ac.jp：.
e12xxxaa@gateway.edu.tuis.ac.jp`s password:　・・・・・

ここで、「scp」は SCP のコマンド、「aaaaa.txt」はアップロードするファイル名、@マークより左側の「e12xxxaa」はログインしようとするホストに登録されたユーザー名、「gateway.edu.tuis.ac.jp：」はホスト名であり、最後の「.」は同じファイル名で送信することを示すファイル名の省略形である。パスワードはエコーバックされない。

② ホストのファイルを Linux へダウンロードする場合

SCP によりホストのファイルを Linux へダウンロードする際は、次のようなコマンドである。

scp　e12xxxaa@gateway.edu.tuis.ac.jp:bbbbb.txt　.

e12xxxaa@gateway.edu.tuis.ac.jp`s password:　・・・・・

ここで、「scp」は SCP のコマンド、@マークより左側の「e12xxxaa」はログインしようとするサーバーに登録されたユーザー名、「gateway.edu.tuis.ac.jp：」はホスト名であり、「bbbbb.txt」はダウンロードするファイル名、最後の「.」は同じファイル名で受信することを示すファイル名の省略形である。パスワードはエコーバックされない。

③ Windows においてホストとファイルの送受信する場合

Windows において、SCP を実行するには、WinSCP のような SSH/SCP のプロトコル機能が組み込まれたフリーソフトを利用する方法が一般的である。

画面左下のスタートボタンから、「すべてのプログラム」、「東京情報大メニュー」、「Network」、「WinSCP」を選択すると、図 2-29 に示すように、WinSCP の初期画面が表示される。「gateway.edu.tui.ac.jp」のようにホスト名を入力する。

図 2-29　WinSCP 初期画面

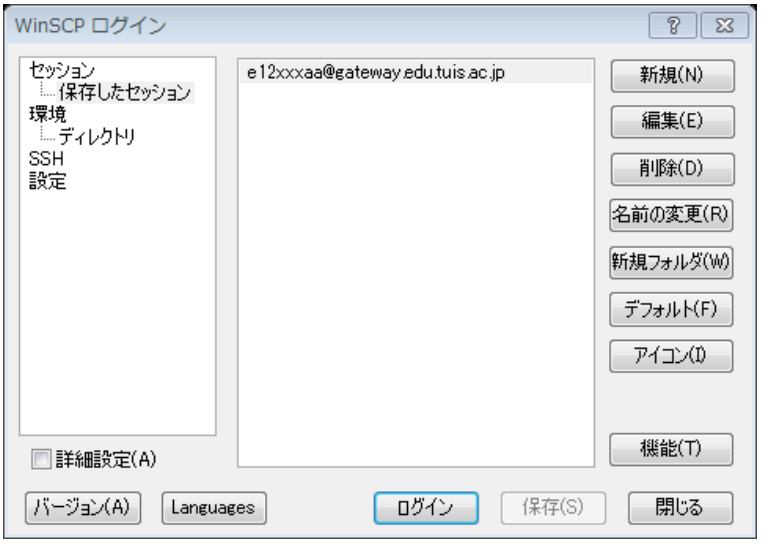


図 2-29 において、「保存」キーをクリックすると、ホストとユーザ名が登録され、2 回目から図 2-30 に示すように、リストから接続するホストを選択することで、WinSCP が開始される。

図 2-30　WinSCP のホストのリスト

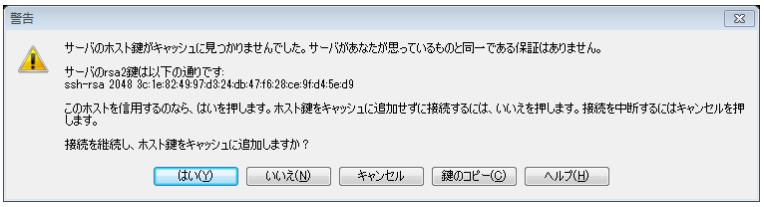


図 2-31　ホスト鍵の警告画面

始めてホストへ接続する際は、図 2-31 に示すようなホスト鍵の警告が表示される。間違いのないことを図 2-30 において、ホスト名に間違いのないことを確認し、「はい」をクリックする。

図 2-32 は、WinSCP の操作画面である。左側が PC、右側がホストに対応する。図 2-32 の例では、PC 側の 2012.txt を選択した状態であり、ウインドウ下部の

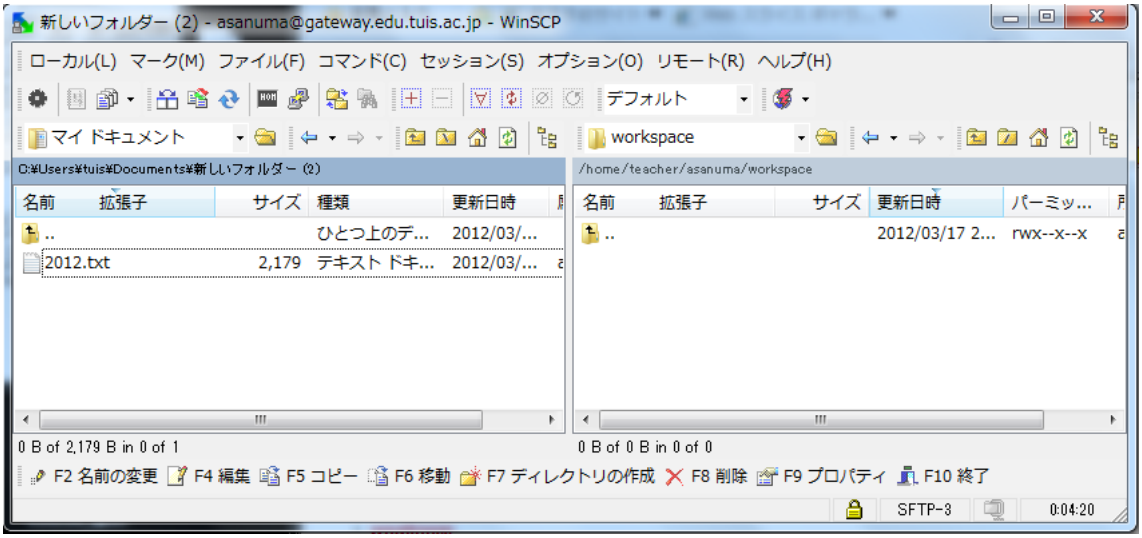


図 2-32　WinSCP の操作画面

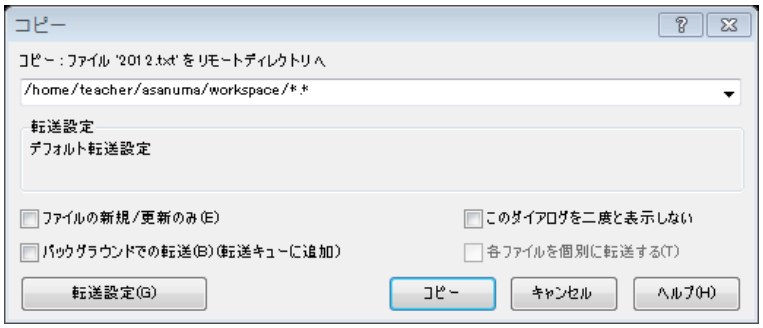


図 2-33 に示すように、一つ、あるいは、一連のファイルの転送について確認を求めるウインドウが開く。「コピー」をクリックする。

図 2-33　コピーの確認

(4) TELNET、FTP

暗号化を施していないコマンド操作のための TELNET や、ファイル転送のための FTP は、大学のファイヤーウオールを通過できないプロトコルである。

2-7　パスワードの変更

パスワードを忘れると、2000 円を情報サービスセンターへ支払い、講習を受けた上で再発行となるので、忘れないように注意すること。

(1) パスワード変更の Web サイト

https://password.edu.tuis.ac.jp

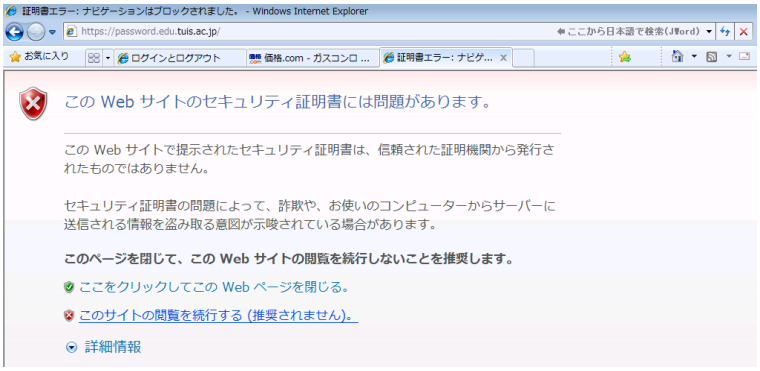


図 2-34 https://password.edu.tuis.ac.jp

ただし、学内からの接続のみとなる。学外から利用する場合は、前節の VPN 接続を確立してからの利用となる。図 2-34 のように、セキュリティの確認後の利用である。

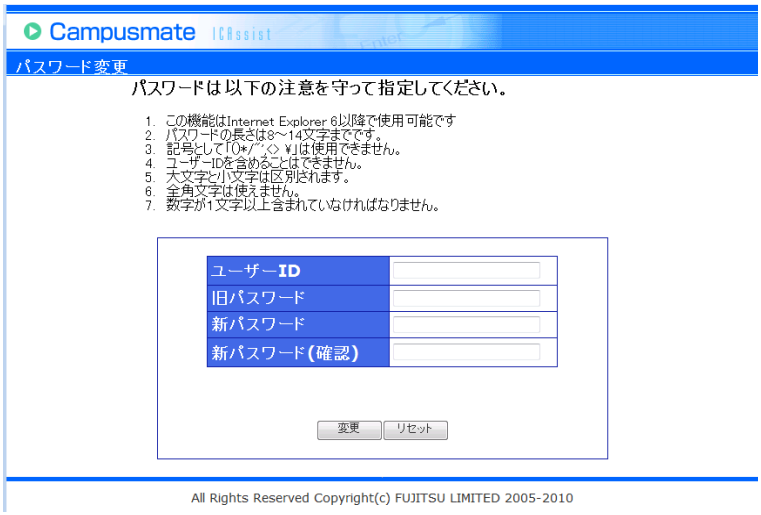


図 2-35 に示すように、ユーザ ID(e12xxxaa は変更できない。)、前のパスワード、新パスワードと確認用の新パスワードを入力する。パスワードは、エコーバックされないので、最新の注意を払うこと。

図 2-35　パスワードの変更

パスワードは以下の注意を守って指定してください。

1. この機能はInternet Explorer 6以降で使用可能です
2. パスワードの長さは8～14文字までです。
3. 記号として「()*/'',<> ¥」は使用できません。
4. ユーザーIDを含めることはできません。
5. 大文字と小文字は区別されます。
6. 全角文字は使えません。
7. 数字が1文字以上含まれていなければなりません。

課題：自分の生まれた年のカレンダを作ろう。

① VMware player を立ち上げ、Vine Linux を機能させる。

② Vine Linux の「アプリケーション」、「アクセサリ」から「端末」を起動する。

③ 端末から次のコマンドを発行する。

cal　1993

を入力し、「Enter」キーをクリックすると、カレンダが表示される。カレンダを確認後、次のコマンドを入力する。

cal　1993　>　1993.txt

ここで、「cal」はカレンダを作成するためのプログラム名、「1993」はカレンダを作成する年、「>」は次に続くファイルへ出力する指示、「1993.txt」は出力ファイル名である。自分の生まれた年を入力すること(図 2-36)。

図 2-36　GNOME 端末からコマンドの入力例

④ GNOME テキスト・エディタを利用し、カレンダに「私の生まれた年」、「学籍番号」と「氏名」を追加し、上書き保存(「ファイル」→「保存」)する(図 2-37)。GNOME テキスト･エディタを終了する。

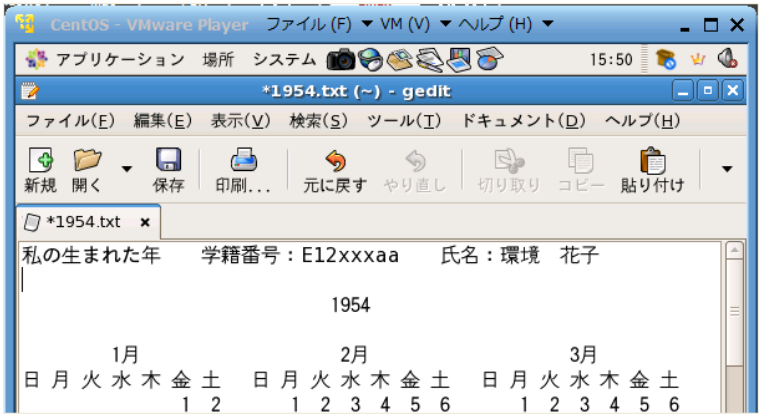


図 2-37　GNOME テキスト・エディタによる操作例

⑤ GNOME 端末から、SCP コマンドにより、作成したテキストファイルを、大学のサーバーへ転送する。

scp 1993.txt　e12xxxaa@gateway.edu.tuis.ac.jp:.

password: ･････

ここで、「scp」は Secure copy command、「1993.txt」は生まれた年のファイル、「e12xxxaa」は学籍番号のユーザ名、「@」で続け「gateway.edu.tuis.ac.jp:」

の転送先のホスト名を指定し、続けて「。」(ドット)を入力する。「。」は、同じ名前でコピーすることを意味する。

自宅等、大学外から操作する場合は、VPN 接続を確立してから実行すること。

⑥ VMware Player を終了する。

⑦ Windows の WinSCP をスタートさせる。ホスト名は、「gateway.edu.tuis.ac.jp」とすること。ユーザ名、パスワードによりホストへ接続する。

自宅等、大学外から操作する場合は、VPN 接続を確立してから実行すること。

⑧ 大学のホスト(gateway.edu.tuis.ac.jp)から、⑤においてコピーしたファイルを Windows のマイドキュメントのフォルダへコピーする。

⑨ コピーしたファイルを２部、プリントし、１部を提出すること。

グーグルのプライバシーポリシー(2012 年３月)

グーグルが、利用者のどのような個人情報を集め、個人情報をどのように利用するかの原則であるプライバシーポリシー(個人情報保護方針)を変更した。60 以上のサービスごとに設けられた個人情報保護方針を一つに設定した。

60 以上のサービスについて、利用者がそれぞれの個人情報保護方針を読み、同意する手続きを簡素化することが一つの目的である。また、サービスごとの検索履歴を、ひとつの個人情報に統合し、システムの簡素化を図ることが別な目的である。

収集される個人情報は、各種のサービスの利用開始時に登録する個人情報であり、氏名、メールアドレス、SNS(ソーシャルネットワーク)利用情報、交友関係、ソフトの購入履歴、クレジットカード番号などが含まれる。

これらの個人情報から利用者の趣味、嗜好、年齢、家族構成、現在地情報などを解析すると、利用者に応じた広告の発信が可能となり、利用者にとっては適切な広告が表れる確率が高くなる。その一方で、利用者が予想もしないような広告が表示される可能性も出てくる。

さらに、グーグルにより収集された個人情報の保護も心配となってくる。過去に有ったように、グーグル内部からの漏えい、あるいは、ハッカーによる攻撃の対象となる可能性もあり、利用者にとって不安が付きまとう。

グーグルのサービスのみではなく、他の企業のサービスを組み合わせるなど、利用者の情報が集中しないように、ネット社会との付き合い方を考え直す必要がある。