

# Nara Women's University

## ネットワーク社会におけるマナーについて

メタデータ	言語: Japanese 出版者: 奈良女子大学情報処理センター 公開日: 2014-09-29 キーワード (Ja): キーワード (En): 作成者: 山下,靖 メールアドレス: 所属:
URL	<a href="http://hdl.handle.net/10935/3842">http://hdl.handle.net/10935/3842</a>

## ネットワーク社会におけるマナーについて

理学部情報科学科 山下 靖

### 1. はじめに

「ネチケット (netiquette)」ということば、聞いたことがありますか？

もちろんそんなことば聞いたことがなくても大丈夫。気にすることはありません。いつものようにいつも使っている WWW の検索のページに行って「ネチケット」または「netiquette」で検索してみましょう。たくさんの検索結果が表示されるはずですよ。さて、どのページを見てみることにしましょうか…

※ ※ ※

このようなことがいつのまにか普通になってしまいました。毎日インターネットを利用して最近ではすっかり離れられなくなってしまった方も多いことでしょう。このように身近になったネットワークは本来自由で便利な社会ですが、どのようなことが常識になっているのかを知らないために、かえって引込み思案になってしまったり、思わぬ迷惑を他人にかけてしまうことだってあるかもしれません。私たちがより積極的に気持ちよくネットワークを利用するためのエチケット、つまりネットワーク・エチケット、これを一語にまとめた造語が「ネチケット」です。

ここではネチケットを中心に、インターネットを利用する上で知っておいた方がよいと思われるヒントについて、筆者の知る範囲で簡単にまとめてみることにします。ただし、書かれていることは筆者の個人的な意見を含み、絶対的なものではないことをお断りしておきます。また、インターネットは日進月歩の世界なので、その変化と共にネチケットなども移り変わっていくことが予想されます。この文章を機会に、実際にネットワーク上でネチケットを紹介しているページなどいくつかご覧になっていただけならと思います。

以下では、まず電子メールについて、その後に WWW に関するものについて、最後に若干一般的なことを書いています。項目ごとに内容はほぼ独立しているので、好きな順番に読んでみてください。

### 2. 電子メール

まずは電子メールについてです。普通の郵便で気をつけることについては電子メールにおいても同様ですが、それ以外にもいくつか知っておくとよいことがあります。以下では項目の数が多くなってしまったので、こんなに気を使うなんて面倒くさい、読むのがイヤになった、という方もいらっしゃるかもしれませんが、あまり気にしすぎることもないと思います。筆者自身、以下の点について全てしっかり実行しているわけではありません。まずはざっと眺めてみて、自分にとって重要と思われる点について考えてみてください。

## 2-1. 自分のメールアドレスを正しく覚える

「これはエチケット以前の問題じゃないの？」と言われてしまいそうですが、不注意な方は結構いるものです。筆者は附属図書館にある学生向けの電子メールシステムの管理者の一人なのですが、毎年年度のはじめの時期にはメール発信者が正しい自分のメールアドレスを附属図書館のパソコンのメールソフト（AL-Mail）に正しく設定していないことによるメール配送失敗がよく発生しています。特に多いのが、アドレス中のピリオド「.」をコンマ「,」にしてしまう間違いや、nara-wu 中のハイフン「-」をアンダーバー「\_」にしてしまうことが多いようです。また、メールアドレスに空白を入れて、

```
abc @ cc . nara-wu . ac . jp
```

などとされてしまうと、計算機は気が利かないのでうまくメールが配送されません。もし皆さんの周りでメールが全然使えないという方がいたら、まず第一にこの問題を確認してみてください。

## 2-2. メールの受信者が人間であることを忘れない

ちょっと説教臭いので書きにくいのですが、メールはコンピュータのディスプレイに向かって書くためか相手への配慮を忘れてしまい、時としてかなり強い表現でメールを出してしまう人がいます。このため、気持ちがイライラしているときにはメールを出す前に次の確認をしてみましょう。

「そのメールの内容を相手に面と向かって言えますか？」

一度送ったメールは、送った側からは取り消すことはできません。これは一般利用者のみならず計算機の管理者にとっても言えることなのです。筆者にも苦い経験があります。思わずかっとなるメールを受け取ったときは、一晩おいてからもう一度受け取ったメールをゆっくり読み返すことにしましょう。そして相手に出す返事のメールも最後にゆっくりもう一度読み返すことをお勧めします。

## 2-3. 秘密事項は書かない

電子メールは、ネットワーク上の複数の計算機を通じて配送されます。この配送途中であなたの電子メールの内容が何者かによって読まれてしまう可能性は残念ながらゼロではありません。他人に見られては困るようなパスワードやクレジットカードの番号などは、電子メールでは送らないほうがよいでしょう。

世の中に流れている膨大な電子メールの中から、悪者がわざわざ自分のメールを選んで覗き見る可能性は少ないんじゃないの、と思っている方もいるかもしれませんが。しかし悪意を持った人が、ある計算機を通過する何万という電子メール全てに対して、例えば「パスワード」という文字列を含む電子メールを抜き出すようプログラムを組むのはとても簡単です。もちろんそのためにはその計算機の管理者になる権利が必要で、計算機の管理をしている人間は、第三者にそのようなことをされないよう努力をしてはいるのですが…。

また、電子メールが相手に渡ってしまったらもう安心、というわけではありません。途中の計算機が通過した電子メールのバックアップをとっている場合があります。昔の話になりますが、イラン・

コントラ事件の関係者であったオリバー・ノース元中尉は、法律違反の電子メールを自分では消していたのですが、ホワイトハウスの他の場所で計算機管理のスタッフがメール全体のバックアップをとっていたため、それが裁判で彼に不利な証拠になったのだそうです。この文章は犯罪者へのアドバイスではありませんが、私たちにとっても参考になる話ですよね。実際にもしも警察等から奈良女子大学のサーバにある電子メールを読みたいと要請された場合、拒むことは今のところできないのではないのでしょうか。とにかく郵便ならハガキは使わないで封書で送るような内容は、電子メールでは送らないのが賢明でしょう。

ただし、電子メールを暗号化して送受信する場合は上の限りではありません。今後はこうした電子メールの利用が普通になっていくのかもしれませんが。

#### 2-4. signature は自己満足にならないようにする

メールの末尾にいつも決まった文章をつけ加える機能を持ったメールソフトをお使いの方も多と思います。これが signature で、自分の名前、所属、メールアドレスなどを入れておくと、自動的にメールの最後にこれらが加えられるので、とても便利です。

この signature に凝る人がいます。文字を組み合わせると絵のようにしてみたり、お気に入りの文章が書いてあったり、人によって様々です。私がインターネットを使い始めたときは、signature は 4 行以下に、と教えられました。ただしこれはだいぶ昔の話で、そのころは通信速度が遅く、無駄を省くためというのがその主旨だったと思います。現在はだいぶ状況が違うので、これをそのまま当てはめる必要はありませんが、WWW 上のネチケット関係のページをみると、今でも 4 行以下を勧めるものがありました。これについては議論が別れるかもしれませんが、自己満足は避け、簡素なものをお勧めします。

#### 2-5. 自分がどれくらいのサイズのメールを送っているのかを知る

ただ手で文章を打ってメールを送信する場合は、メールはそれほど長いものになることはないでしょう。しかし最近ではメールソフトの「ファイル添付」の機能を使って、画像や音声をメールに入れる方が増えているように思います。これらは、場合によっては非常に大きなサイズとなり、特に通信速度が遅い環境でメールを読んでいる方宛メールの場合、相手に負担となることがあり得ます。大きなメールを送ってはいけないとは言いません。ただ、普通の郵便と違って、インターネットではメールを受け取る人も、受信のために時間とお金を負担していることを覚えておきましょう。

#### 2-6. 「半角カナ」は使わない

電子メールでよく問題になるのが「文字化け」です。皆さんも、

```
0J2<$K!"$H65$(i$1$^$7$?!#$?@$@7$3$I$0$@$ $ $V@N$NOC$G!"$=$N$3$m
```

みたいな謎のメールを受け取ったことがあることでしょうか。私が受けるメールに関する相談のトップが「メールが文字化けして読めないので助けてほしい」というものです。何度も何度も相談を受けた結果、文字化けの原因にはいくつかのパターンがあることが分かっているのですが、ここではいわゆる「半角カナ」文字について述べておきます。

「半角カナ」(より正確には1バイト文字のカナというべきなのかもしれませんが)とは、画面上ではabcなどのアルファベットと同じ位の幅を占める小さなカタカナのことです。メールソフトは「半角カナ」には対応していないことが多いので、もし自分の方ではうまく小さなカタカナを使ってメールの文章を用意しても、そのメールを受信した相手は全く読めないという可能性があります。習慣として、メールでは「半角カナ」は使わないで、他の漢字と同じ幅をしたカタカナ「全角(2バイト)カナ」を使うことをお勧めします。

## 2-7. 意味もなく1行おきに書かない

私はみたことがないのですが、メールソフトによっては、1行おきに書いたほうが読みやすいものがあるでしょう、1行おきに空行を入れたメールを私も受け取ることがあります。しかし受け取る人の環境ではそれが読みやすいとは限りません。例えば私が使っているものは普通に文章を各行に書いてもらった場合に読みやすくなるようになっています。1行おきに書かれるとこの文章のように散漫な感じになってしまい、読みやすくありません。もしお使いのメールソフトではどうしても1行おきに書かないと読みづらい場合、メールソフトを別のものにしてみることを考えてみてください。

## 2-8. チェーン・レターは出さない

これはいわゆる不幸(幸福)の手紙のたぐいですね。当たり前のことですがチェーン・レターを出したり転送してはいけません。

いかにも文面がチェーン・レターといったものではなくても、「全文転送は、ご自由にしてください」というただし書きをつけた善意のメールがチェーン・レターになった事例もあるようです。その事例についてはさらにそのメールがチェーン・レターになっているので転送しないよという警告のメールがチェーン・レター化するということまで起こったそうで、郵便より気軽にメールが出せるインターネットならでの現象であるとともに、チェーン・レターの難しさを表わしているのではないのでしょうか。

ちなみに筆者は、以下のような文面を含むチェーンレターを何度か間隔を数年! あけて全く別の方から全く同じ内容で受け取ったことがあります。まず挨拶のような文章に続いて…

- 先日、ぼくが友達とファミコンをしていると、通りかかった母が「おまえたちはいいねえ、毎日がエブリデイで」と言った。母はいったい何が良かったのだろう…。
- 夫婦ゲンカするとき、父が母に「バカモノ!」と言うのを、間違っ、「バケモノ!」と怒鳴ってしまった。ケンカはさらにひどくなった。
- 先日、父は、男にフラれて落ち込んでいた姉をなぐさめようとして、「おまえ、人間は顔じゃないぞ」と言うところを、「おまえの顔は人間じゃないぞ」と言ってしまった。

こんな感じの文章が延々と続きます。そしてメールの最後にこのメールを何人かの人に送るようお

願いがありました。もしこのようなものを受け取ったら、知人には転送しないでください。チェーン・レターには気をつけましょう。

## 2-9. あやしげなメールへは返事を出さない

全く知らない発信元から、「性的な画像にアクセスできる」、「お金持ちになることができる」などといったメールがなぜか送られてくることがあります。このような話に乗らないのはもちろんですが、もう一つ注意すべきことがあります。よくこの手のメールの末尾に、

「あなたのメールアドレスは当社のサーバに登録されました。

今後当社からのメールが不要な場合は

aaaaaa@bbb.ccc.ddd

に「不要」という内容のメールを出してください」

といった意味のことが書いてあることがあるのです。ここに素直に返事を出してしまうと、相手にそのメールアドレスが確かに実在してしかもちゃんと読まれている、ということが伝わるだけで、かえってこれからもしっかりと変なメールが送られてくる可能性があります。このようなメールは無視するに限るようです。もし頻繁に来て困るようなら、システムの管理者に相談してみるのもよいでしょう。特定の発信元からのメールをシステム（例えば奈良女子大学全体など）として拒否することは可能なので、対応してくれるかもしれません。

## 2-10. 引用について

あなた宛に来たメールの内容を別の人に宛のメール中で引用する場合は、十分な注意が必要です。基本的には許可を取らずに第三者のメールの内容を引用するべきではないでしょう。これは電子メールに限らず普通の郵便についても言えることなので、ここでわざわざ書く必要はないかもしれません。ただ、ご存じのように電子メールでは他のメールの引用が非常に簡単なので、あえてここで注意しておきます。

## 2-11. 1行の長さは漢字の場合 30～35 文字程度にする

メールを読むためのソフトにはいろいろな種類があり、相手が自分と同じような見え方でメールを読んでいるとは限りません。ただし伝統的というか古いものには1行が漢字 40 文字分であるものが多かったので、引用のためなど少し余裕を見て上のような数字が言われるようになったのでしょう。全く改行のないメールでも読むのに非常に不便というほどのことはないのですが、メールソフトの機能を使って受け取ったメールの引用をする（〈 〉 や 〈 〉 等を行の先頭に加えて引用文をメールに挿入する機能）場合には不便なような気がします。

最近ではモバイル機器などで1行が漢字 40 文字分よりずっと少ない場合も増えてきたので、このような常識はそのうちむしろ非常識になってくるのかもしれません。

## 2-12. メール の 題 名 に 漢 字 を 使 う と き は 注 意 す る

このルールはもう不要なものになってきたかもしれませんが、一応書いておきます。古いメールソ

フトの中には電子メールの題名に漢字を使うことができないものがあります。この場合無理に書こうとしても文字化けになってしまいます。もしあなたのメールが本文は文字化けしていないのに題名だけがどうしても文字化けしてしまうと言われたとき、またはそのようなメールを受け取ったとき、発信者または受信者のメールソフトが古い可能性があるので、

- 題名をアルファベットにする
- 新しいメールソフトに乗り換える

ことを考えてみてください。

## 2-13. 返信先が意図した正しいアドレスか注意する

これも当たり前と言われそうですね。よくあるミスの一つ注意しておきます。

それは、メーリングリストを利用している場合です。受け取ったメールの内容について、メーリングリストのメンバーの中のある一人の人に返信を書くつもりで、メーリングリスト全員に個人的なメールが行き渡ってしまった経験のある人はいませんか？ また、メーリングリストではなくても、多人数宛のメールに返事を出したら CC に本来意図しない人まで入っていて失敗をしたということもあると思います。

返信先が意図した正しいアドレスか注意しましょう。

## 3. World Wide Web

WWW に関しては、WWW の閲覧時に気をつけることと、ページ作成時に気をつけることがあります。閲覧時に気をつけることについて3点述べ、そのあとページ作成について考えてみることにします。

ただ、筆者の知る限り学内で WWW のページを公開している方の数はまだまだ少ないのではないのでしょうか。そういう私自身、たいしたページを公開していないので、偉そうなことを言える立場にはありません。マナーを後回しにしてよいわけではありませんが、より多くの方の情報発信できる環境の整備も必要だと思われます。その際、先に WWW のページを公開するやり方を覚えた方は、他の人に親切に教えることにより情報の共有を図ることもネチケットに含まれることと思います。

### 3-1. ページの内容の信頼性をよく考える

インターネット上の情報は言うまでもなく玉石混交で、中には信頼性に問題があるページも多く見られます。そのこと自体が悪いわけではなく、むしろ筆者にはそれが魅力的でもあるわけですが、見る側が自分の責任で情報の信頼性を判断することが必要になってきます。見ているページの種類にもよりますが、注意する点として

- ページ作成者の連絡先が書かれているか
- 情報の出典が確認可能か
- 他の方法で情報の内容が確認できるか

などがあげられるでしょう。

### 3-2. 法律について

言うまでもなくインターネット上でも法律違反は法律違反です。著作権で保護されているものが勝手に無料でダウンロードできるようになっていたり、賭博、ネズミ講を募集しているページなども存在しているようです。法律違反を当然ネチケット以前の話ですが、現実には問題となっているようです。誰も見ていない部屋で一人でインターネットにアクセスできる環境の人が多くいることを考えると、このような問題が発生するものうなずけますが、インターネットの犯罪は決して捕まりにくいものではないことを思い出しておきます。

### 3-3. プロキシサーバを利用する

奈良女子大学でもプロキシサーバを稼働させています。学内から WWW を利用されている方はぜひプロキシサーバを利用してください。

現在奈良女子大学の学内 LAN を OCN に接続し、学外の WWW への接続を高速化しています。そのためにはプロキシ（代理）サーバを経由してアクセスすることが必要となります。また、相手先によっては、今のままの方が高速です。そこで、接続先をうまく使い分けるための自動設定ファイルが

<http://www.nara-wu.ac.jp/proxy/>

以下にあります。これを利用して設定すると「ac.jp」（日本の大学）や一部の学術系サイト、Yahoo! JAPAN など、SINET 経由でも十分速いサイトは SINET-ORIONS-プロキシ経由接続、それ以外の企業・プロバイダには OCN-プロキシ経由接続となります。

また、自動設定を使わない場合は、次のようにしてください。

- 使用するブラウザによって異なりますが、「プロキシ」設定画面から手動設定を選択してください。
- サーバのタイプ（プロトコル）ごとにプロキシが設定できます。  
HTTP、Secure (Security)、FTP、Gopher に対し、  
「サーバアドレス proxy.nara-wu.ac.jp」、「ポート 3128」  
を指定してください。
- ac.jp（大学など）へは直接接続の方が速いので、必ず「例外」（プロキシを使用しない）アドレスを指定してください。Netscape では「ac.jp」のように、Internet Explorer では「\*.ac.jp」のように指定します。

この機能を利用することによって、本学と学外とのネットワークの通信がより効率的になることが期待されます。ご協力をお願い致します。

### 3-4. 作成するページには作成者の連絡先を入れる

公表するページの内容に責任を持つ意味でも、作成したページには作成者の連絡先を入れるようにしましょう。ただし連絡先としてはメールアドレスを使用することをお勧めします。自分の住所や電話番号など個人的な情報を連絡先とするのは、以下でも述べますが避けたほうが無難です。



### 3-5. 作成するページには個人情報のをせない

インターネットはとてとても広く普及してしまったので、ありとあらゆる種類の人がインターネットにアクセスしていると考えerべきでしょう。計算機にアクセスできる人は善良で皆で広く情報を共有したほうがお互い幸せだからと言ってパスワードというアイデアにさえ大反対したある計算機科学者の主張は、はるか彼方の昔話となってしまいました。

作成するページには、個人の住所、経歴、電話番号、自分の写真などは載せないほうがよいようです。それぞれ、どのような形で悪用されるか分からないからです。

自分の作ったものはごく少数の友人どうしでしかリンクをしていないから大丈夫、と思われる方もいるかも知れません。しかしその友人の中の誰かのページへ、どこからかリンクが張ってあるかも知れません。その結果、あなたの作成したページはいつのまにか世界とつながっているかも知れません。また、インターネット上では、全文検索エンジンのデータを作成するために 24 時間動き続けているソフト（ロボットと呼ばれます）がリンクを常にたどり続けていて、今日も新たなデータを蓄積しています。そのため、検索エンジンのページに自分の名前を入れてみたらほとんど誰も知らないと思っていた自分のページがそこから見つかるということが起こったりします。

ロボットを排除する方法は、不完全ではありますがあるにはあります。また、作成したページについて、例えば奈良女子大学外からのアクセスはできなくするなど、アクセスを制限をすることもほとんどの場合可能です。必要ならばシステムの管理者にこれらの方法について問い合わせしてみてください。

### 3-6. 著作権など

作成するページに他人の著作権を侵害するようなものを載せないよう注意しましょう。例えば、

- 他人のメール、ホームページの文章、画像、音声など
- 地図・新聞・雑誌・書籍の文章、画像など
- 歌の歌詞、CD のデータなど

これらには注意してください。ただしきわどい問題もたくさんあって WWW 上での公表はどの程度まで許されるのか、いろいろと議論があるようです。筆者はこの文章を書くためにインターネット上で著作権を扱っているページを見てまわったのですが、考えさせられるものに数多く出会うことができました。もし可能であるならば、いつかこの情報処理センター広報上で筆者より適当な方に、この問題について解説していただけたら有意義なのではないでしょうか。これから WWW でのよりよいページの公表を目指される方は、ぜひ一度この問題について考えていただきたいものです。

また、著作権ではありませんが、他人の登録された商標をあたかも自分の商品のものであるかのような使用もいけません。他にも、本人の許可を得ずにその人の写真などを勝手にページに載せて公表することは肖像権の侵害として訴えられる可能性があります。著作権同様、注意してください。

### 3-7. あまりに大きな画像をトップのページにおかない

アクセスしようとしたら延々と画像をダウンロードしていて、待ちくたびれた頃にやっと出てきたと思ったらあまりにくだらなくて腹が立った経験、皆さんあると思います。自分でつくるときは当然大きな画像もすぐに表示されるので、なかなか相手がどれだけ待っているのか気がつかなくなったりし

ます。見せたい大きな画像がある場合は、その画像の文章による説明または小さくした画像のみをトップのページでは用意して、もとの大きな画像はそこからのリンクでたどれるようにしましょう。さらにその大きな画像がどれくらいの大きさなのかも書いておけば、大きな画像を見ようとする人が、どれくらい待てばよいのかを判断する助けになります。

### 3-8. 他のページへのリンクについて

自分のページから他の人のが作成したページへのリンクを張る場合、事前に許可を得る必要があるのでしょうか。これは人によって意見が異なるようです。ある人は「必ず許可が必要」といい、別の人は、「許可は不要」といい、完全に定まった合意はないようです。ただし私の知る範囲では「許可不要派」の考えのほうが広く認められているような気がします。その場合でも、そのページの作成者にリンクを張っていることを連絡する方がエチケットとしてよいという考えがあるようです。（ただしこれもコンセンサスが得られた考えとはまだ言えないようです）

リンク許可を求める場合は、

- ・メールを出す前に、そのページに無断でリンクしてよい旨が書いてないか確認
- ・どのページからリンクしたいのかをはっきりと
- ・できればリンクを張ったという事後通知ではなく、「返事がない場合は何月何日からリンクさせていただきます」と、猶予期間をみておく

などの点に注意をしてください。

### 3-9. 作成したページの見え方について

あなたの作成したページを見ている人はあなたと同じ環境にいるとは限りません。見え方が人によって異なる可能性があることに注意しましょう。たまに、背景の色と本文の色が似ていたり背景ばかりが目立っていて本文が非常に見づらいページがあります。多分それでもご自分の環境では満足の行く見映えなのでしょうが、こちらとしては見たくても見られないものさえあります。特に凝ったページを用意される方は、できれば複数のブラウザで見え方について確認していただけたらと思います。

また、公的な内容を含むものなど特に広い範囲の人のアクセスを期待するページを用意される方をお願いします。

「障害をもった方への配慮をしてください」

例えば、ほとんど画像のみのページで次のページに進むには画像のある部分をクリックしなければならない場合、視覚に障害を持った方は次のページに進めませんし、そもそもそのページの内容が分かりません。詳しくは、

- ・「こころWeb」 <http://www.jeida.or.jp/document/kokoroweb/> をぜひ一度ご覧ください。

### 3-10. 文字の大きさについて

文字の大きさを完全に指定してページをつくっている方がいます。見る側の環境は作成者のものと同じとは限らないので、閲覧する人にとってはそれがとても小さな文字になることがあります。ブラ

ウザの文字の大きさは、そのブラウザの使用者が自分で見やすいように決めるべきで、それを無視して文字の大きさを指定するのはあまり好ましくないのではないのでしょうか。

#### 4. その他のインターネット利用全般について

電子メール、WWW 以外について、少しだけ触れておきます。まず、インターネット利用について一般に言えることですが、もし可能ならばネットワークに負担となる利用（大きなファイルの転送など）はネットワークが混雑していない時間帯に行うのが望ましいでしょう。

以下では上で書けなかった問題として、エチケットというのとは少しずれるかもしれませんが、セキュリティ関係のお話を少しさせていただきます。

##### 4-1. パスワード

インターネットを利用していると、パスワードを決めなければならないことが時々あります。そもそもワークステーションでは使用を開始する（ログインする）ときにパスワードが必要でした。

パスワードは他の人に教えないのはもちろんですが、他人に類推されにくいものを使いましょう。例えば、次のようなものをパスワードとするのはよくありません。

- 自分や自分の家族、ペット、知人などの名前
- （知人でなくても誰かの）名前
- 使用している計算機のシステムの名前やホスト名
- 電話番号
- 自動車のナンバープレート
- 誰かの誕生日
- 英語や日本語の単語
- 地名
- aaaaaa 等の単純な文字列
- qwerty みたいにキーボードで簡単に打てるもの
- 上に含まれる文字列をたんに逆順にしたもの
- 上に含まれる文字列に数字を1つ前か後に加えただけのもの

また、パスワードを紙の上にメモしておくのもよくありません。要求が厳しすぎますか？ もし簡単なパスワードを暗記するか、難しいパスワードを紙に書くかどちらか選べと言われれば、私個人としては簡単なパスワードを暗記する方を選びます。覚えられないパスワードでは役に立ちませんから。

##### 4-2. FTP

これは異なる計算機の間でファイル転送をする場合に用いるものでした。特に、広く配布されているソフトウェアのダウンロードなどを行う場合は、匿名 ftp (anonymous ftp) を利用することになります。これは、ftp でアクセスするときのユーザー名として anonymous または ftp を用い、パスワードとしてはどのような単語を入力しても構わないというものでした。例えば京都大学の ftp サーバにセンターのマシンである narams から接続する場合の実行例は、次のようになります。

```
narams [1] ftp ftp.kuis.kyoto-u.ac.jp
Connected to ftp.kuis.kyoto-u.ac.jp.
220-nylon FTP server (Version 5.60) ready.
220-
<中略>
Name (ftp.kuis.kyoto-u.ac.jp:sf14029): anonymous
331 Guest login ok, send your E-MAIL ADDRESS as password.
Password:
230 Guest 'xxxxxxx@yyy.nara-wu.ac.jp' login ok.
>ftp
```

これ以下の詳しい ftp の説明は省略しますが、波線の部分が使用者が入力する部分です。このときパスワードを入力する直前の行のメッセージからも分かるように、パスワードとして自分のメールアドレスを入力することがエチケットとして期待されています。筆者にとってもメールアドレスを入れるのは、はじめのうちは少し気持ちが悪いものでした。しかし最近では、セキュリティーに厳しい ftp サーバが増えてきたため、正しいメールアドレスを入力しないとアクセスと受け付けてもらえないことが多くなってきました。このためこれはエチケットと言うよりは、アクセスのための最低限の要求と言うべきかもしれません。

実際に入力したメールアドレスを利用してメールが私たちのところに来ることはめったにありません。サーバの側でアクセスの記録をとるだけというのが普通のようなようです。ごくたまに熱心なところでは、誰がどのソフトをダウンロードしたかについて記録をとっておき、そのソフトのバージョンアップの際には連絡を行うなどというところもあるようです。筆者にも一度だけそのような経験があります。

#### 4-3. POP

この項と次の項は電子メールの項に含めるべきだったかもしれません。パソコン上のメールソフトとメールサーバの通信に関するお話です。

POP とは、メールをパソコンなどから読んでいる場合にメールサーバからパソコンにメールを転送するための仕組みの名前です。POP によってパソコンからサーバにアクセスするときに、サーバにユーザ名とパスワードを送りますが、このパスワード、特に設定をしないと暗号化されないでパスワードのもともとの文字列がそのままサーバに送られます。そのためネットワーク上にいる悪意を持った第三者にパスワードがばれてしまう可能性があります。パソコンからメールを読んでいる方はご存じと思いますが、メールソフトは POP を使って例えば 15 分に 1 回など定期的に繰り返しサーバにアクセスします。従って暗号化されていないパスワードが定期的に何度も繰り返しネットワークを流れてしまうので、この危険性はなかなかあなどれません。奈良女子大学内にはあまり悪い人はいないと仮定して、学内から本学のメールサーバ narams に AL-Mail などでアクセスする分にはそれほど危険はないと思いますが、自宅などからインターネットプロバイダを通して本学のメールサーバにアクセスする場合は、以下に紹介する APOP という仕組みを使うよう、システム管理者に相談してみてください。

APOP というのは上の問題を回避するため、パスワードを暗号化して送るための仕組みです。暗号化していてもその暗号文が読まれてしまったら、同じ暗号文を悪意を持った人間が同じようにメールサーバに送ればメールがその人に読まれてしまいそうですが、APOP ではこれを避けるためにパスワードをを毎回異なる暗号文になるように暗号化して送ります。ただし APOP を使うにはお使いのメールソフトが APOP に対応していなければなりません。確か Eudora や AL-Mail はこれに対応していて、設定メニューを開くと、APOP を使用するかどうかの変更が可能になっていたと思います。その他のものも対応しているものが増えてきているので、マニュアルなどで調べてみてください。ただし APOP を使用するには、メールソフトの設定変更だけではなく、メールサーバの方でも対応した作業が必要なので、こちらについてはサーバの管理者に問い合わせてください。

#### 4-4. SMTP

電子メールは、パソコン上のメールソフトをからメールを中継するサーバに転送され、さらにそのサーバがより遠隔地のサーバに転送を行うなどして配送されます。メールの発信時にメールソフトがアクセスするのが SMTP サーバ、受信時にアクセスするのが POP サーバと呼ばれます。具体的には情報処理センターではどちらも narams がこれを担当しています。この SMTP サーバとしての narams ですが、セキュリティの都合上学外のメールソフトからのメールの中継を現在制限しています。自宅などから学外のプロバイダを経由してインターネットを利用しているときは、その自宅のマシンのメールソフトの SMTP サーバの設定を、そのプロバイダが指定するものにあわせ、narams は使わないようにしてください。そのような設定が不可能な場合は、管理者にご相談ください。

制限を行っている理由を簡単に説明します。

例えば、外部のドメインにあるマシン aaa.bbb.ccc が narams 経由でメールを出そうとしたとき、narams がこれを無制限に許してしまうと、aaa.bbb.ccc の使用者が narams を利用して世界中に何万という（例えば宣伝の）メールを出そうとすることができてしまいます。narams が悪用されるだけでなく、悪用されている間私たちのメールの送受信も停止してしまうこととなります。このような外部からのメールの大量中継を許す SMTP サーバはブラックリストに載り、他の SMTP サーバが通信をしにくくなるという事態も発生しているそうです。そこで narams でもネットワーク的に学外にあるパソコンのメールソフトからの中継を制限することにしました。

#### 5. おわりに

ここまで読まれてどう思われましたでしょうか。内容に対して反論したくなった方も多いかもかもしれません。そのときはその反論を情報処理センター広報に向かって一人ずつぶやくのではなく、よりよい知識をネットワーク社会で共有するためにも、WWW のページなどを用意して、その意見を公表していただければと思います。

最後に一つだけ WWW のページを紹介してこの文章を終わることにします。機会があったらご覧ください。

「ネチケットを笑い飛ばせ」 <http://home.highway.ne.jp/flower/netiquette/>