ネットワークマナー

神戸大学工学部情報知能工学科
藤井 勝宏 *

1 はじめに

多くの人にとって最初にネットワークの恩恵を感じるものは電子メールではないでしょうか。電子メールは始終世話になる機能だと思います。郵便の手紙に一定の慣例があるように、電子メールにもそれなりのマナーがあります。第 2 章では電子メールでの基本的なマナーについて述べます。また、第 3 章でネットニュースへの投稿マナーについて説明します。ところで、コンピュータの高性能、高機能化によってマルチメディア情報に本格的に取り組める状況に相合わせ、ネットワークの基盤整備が整いつつあることは周知の通りです。日本においては、ほんの 1 年ほど前には数えるほどしかなかったインターネット商用サービスプロバイダも 20 を越え、個人で WWW ホームページを開設する人も出てきています。”インターネットカフェ”、”バーチャルカンパニ” など新語が次々と登場し、あおりたてられるように日本はインターネットの世界へと足を踏み入れています。確かに、国や人種を越えて新たなコミュニティを生み出し、ビジネスシーンや学術シーンにおいてもはるかにワールドワイドかつ高機能な双方向のサービス、研究、あるいは教育への展開が期待できます。しかしながら、その活用などが華々しく脚光を浴びるなかで、ネットワークの運用に携わる者としてはセキュリティやプライバシーといった問題を避けて通ることはできません。第 4 章では、この点について一般ユーザが実行すべき、あるいは知っているべきことについて述べます。

2 電子メールマナー

最近はこの手の本が出ているようですし、雑誌などでも書かれていることが多いのでそちらも見ていただくとして、筆者が考える必要最低限のマナーを以下にあげてみました。これらのマナーは絶対守らないといけないということではありませんが、インターネットの世界（主に fj）で培われてきた一種の合意事項でもありますので出来るだけ沿うことを勧めます。

(1) Subject には漢字を使わないこと

中継ホストの配送プログラムが漢字に対応していない場合や相手ホストが対応していない場合があるので使用しないほうが安全です。英数字文字を使って Subject を書く訳ですが、邦人

*scfujii@seg.kobe-u.ac.jp

宛ての場合には辞書を片手に書くよりはローマ字を使ったほうが相手にも分り易いことが多いです。

（2） 本文の 1 行は漢字 35 文字程度とすること

自分の書いたメールの見た目通りに相手に読んでもらいたい、つまり改行する箇所は発信者が決めた通りになってほしいと思いませんか。メール／ニュースリーダには様々なものがあり、1 行の文字数の多い場合は大概は折り返しをしてくれますが、横スクロールしないといけないのもあります。その場合、きっと受信者は面倒です。ですから、1 行は漢字 35 文字程度にし、改行をしておくのです。 また、発信したメールが引用されたときに 1 行文字数が大きくならないように 35 文字程度がよろしいのです。さて、文字を読み書きするだけの電子メール交換は高機能なコンピュータを用いなくても通信とキャラクタ端末的な機能さえあれば基本的には利用可能です。例えば、手近のワークステーションとパソコンを RS232C で接続してパソコン側でターミナルソフトを動かしておき、そこからワークステーションにログインすればそれでメール交換が可能になります。 もちろん、ワークステーションにアカウント登録しておかねばなりませんし、RS232C ポートの設定もしておかねばなりませんが、それは大した作業ではありません。あるいは、パソコンにモデムをつないで公衆電話回線あるいは学内電話回線経由で学内にある KHAN につながったワークステーションなどにログインしてメール交換をすることも可能です。実際にそのような形態で利用している人もいます。ここでこのような話を出したのは、このような形態で利用する場合には画面に表示できる 1 行の文字数は通常は漢字 40 文字であることが多いということを言いたかったからです。つまり、メール交換の相手がこのような環境にいる場合には特に 1 行を 40 文字以内の適当な文字数にしたほうが読み易いのです。端末と言えば 1 行 80 文字（英数半角勘定）という昔のなごりと言えばそうですが、郵便の手紙でも横書きで横方向に長い便箋というのはあまり読み易いものではないはずです。 なお、漢字コードは JIS を使います。

（3） 半角カタカナは使わないこと

日本語に対応したメール／ニュースリーダは、ASCII 文字と基本的には JIS 漢字（全角）だけを文字コードの対象としていますので半角カタカナ文字があると変な制御コードが存在することになり画面が乱れたり、表示されなくなったりします。

（4） 引用するなら的確にすること

返事を出す時に、相手の文面のどのことに対する返事なのかを明確にしておかないと、話があいまいになり誤解が生じる恐れもあります。また、沢山のメールをやり取りしていると、何の件に関することなのかが分りにくくなります。このために相手のメールの中の必要な部分を自分のメールの中に取り込み、その行の先頭に「あなたの言葉です」という意味で「>」（大なり記号）などをつけることにしており、この部分を引用と呼んでいます。 この引用部分の次の行から自分の返事や意見などを書いていきます。

ところで、相手の長い（行数が多い）文章に対する返事を書くのに相手の全文を引用したり

する人が見受けられます。こういう場合は、途中をカットし、カットした旨を示すために「(途中略)」などと書くようにします。一般には、引用は返事より行数を少なくし、多くても同じ行数までが目安です。あくまでも目安ですから、全文引用しても構わないと言えば構わないのですが、このことで大へん注意を受けた人を何人か筆者は知っています。

(5) 常用漢字を用いること

日本語入力する時、普段突然読みを問われても回答に窮する漢字も簡単に入力できてしまうことがあります。それをそのまま送信したのでは受信者がすらすら読めない可能性があります。これでは不親切ですし、第一に意志・意味が伝わらない恐れがあります。そういう漢字はひらがなで十分です。

(6) シグネチャは 4 行程度とすること

本文の最後に発信者の氏名、所属、連絡先などを書いたものをシグネチャと言います。"何処そこの, 誰それが書きました"という署名(本当の意味での署名ではない)です。受信者側ではメールヘッダの From: 欄を見れば誰から来たものかは大概分る訳ですが、電話番号などの連絡先は分らないので後で直接連絡を取る時に重宝したりします。

シグネチャは、4 行程度に簡潔に書くのが慣例です。アスタリスクなどで四角で囲ったり、キャラクタを使って絵を書いたり(「ASCII アート」とか言うらしい)とデザインに凝る人が比較的多いのですが、行数の多いのは感心しません。

筆者自身は、メールを送るのが初めての相手、あるいは久しぶりに送る場合はシグネチャを付けるようにしていますが、やり取りの頻度の高い相手には省略しています。それは、筆者は発信メールのブラインドカーボンコピーも含めて受けとったメールをすべて相当長期間保存することにしているのでその保存容量を少しでも抑えたいということ、少しでも伝送容量を少なくしてネットワークのトラフィックを抑えたいということ、いくどものやり取りの中ではあまり意味が認められないなどの理由からです。ただし、頻度の高い相手でも数通に一度は入れます。これは、直接連絡を取りたいときに相手からのメールのシグネチャを頼りにすることがあり、受信メールのシグネチャを手繰ることがあることから来ています。

(7) まず名を名乗る

ところで、通常メールリーダは受けとったメールを表示する時には先頭行から順次 1 ページ(画面)に収まる行数をまず表示します。そのため、シグネチャが次のページ以降に回っているときには、一瞬誰から来たものか分りにくいのです。そこでメール本文の先頭行に、

名前@所属です

と書くことを勧めます。メールアドレスに見立てて書く訳です。所属については、相手が判断できる範囲で省略すればよいでしょう。例えば、

藤井@情報知能工学科です

という具合です。

(8)　顔マークを多用しないこと

気持ちや仕草などを言葉ではなく文字で形作ったマークで表したものを顔マークと言い、「(^_^)」,「 : -)」 などがあります。顔文字とも言います。これは、うまく使わないといけません。2 , 3 年前のネットニュースで次のようなことがありました。

A さんが B さんに対して、高飛車というかちょっと相手をたしなめるような文を書きました。その後ろにスマイルマークがあったのです。A さんは笑い顔で言った、つまり、親しみを込めて言ったつもりだったのだそうですが、B さんがえらく怒り出しました。それで、A さんは、「なんでそんなに怒るねん。スマイルマークを付けといたやろ。意味わからんのか。ワシは怒って言うたんとちゃう。あんたを責めたんともちゃう。微笑み返しやがな。愛情やがな。」と言いました。しかし、B さんは、「それやったらそれでちゃんと文章を書け。マークは単なる飾りであって、深い意味を持たせられても分かれへんがな。あいまいなことすんな。」云々。もちろん実際の語句、言葉使いはこうではありませんでしたが、こういう意味のやり取りがありました。最近は、

スマイル	(^_^)　　: -)
汗タラ	(^_^ !)　(^ ^ ;
ドキッ目が点	(・_・ !)
分らない	(? _ ?)
舌ペロ	(: - P)
バンザーイ	＼(^o^)／
ごめんなさい	_ o _
しくしく	; _ ;
号泣	T_T

などよく使われるものについては、文のニュアンスを伝えるための小道具として定着していますが、あまり使われていなくて、ぱっと見て意味の分かりにくいものなどは、使う時に注意しないといけません。顔マークは、文章に表情と個性を持たせ、微妙なニュアンスを伝える小道具ではありますが、そこにあまり深い意味を持たせると誤解が生じることも有り得ます。ですから、筆者は気心の知れた者同士以外ではあまり使いません。

(9)　日付・時刻が正しいこと

日付・時刻が正しくないと、例えば論文を電子メールで投稿する場合は混乱が生じます。その他に何かと不都合が発生することは容易に想像できると思います。

実は、コンピュータの内部時計は思ったより誤差が大きく、時々補正しておかないといけません。ましてや日付が間違っているのは論外なのですが、それでも時々間違っているホストがあります。補正は UNIX マシンでは管理者であるスーパーユーザしかできません。

(10)　バイナリの送信

バイナリファイルはそのままでは、メール本文としては送れません。そこで uuencode などのプログラムを使って ASCII 文字化して本文に挿入し送ることになります。受信元では uudecode

(uuencode されている場合) などを使って復元します。大きなファイルは予め compress や zip あるいは LHA などを使って圧縮しておきます。Macintosh 同士では自動的にこのようなことを行なってくれるようです。さて、いくらバイナリファイルがこのようにすれば送れるとはいえ、大容量ファイルを一つのメールで送ってしまうのはよろしくありません。中継ホストの容量や回線容量が小さいと送れなかったり他のメールの配送の妨げになったりするからです。たいていは 50KB 程度ずつに分割して送ることが多いようです。UNIX では split というコマンドで分割できます。ネットニュースではこれが大体守られているようです。例えば、fj.source では tar ⟶ gzip (compress) ⟶ uuencode ⟶ split が慣例になっています。しかし最近は anonymous FTP あるいは Netscape や Mosaic による WWW アクセスの増加にみられるように大容量の転送がどんどん行なわれており 1MB 程度なら海外でない限りは大丈夫かもしれません。中継ホストを含む経路状況が把握できていて、かつ迷惑がかからないことが自明であれば (例えばサブネット内) 律義に 50KB に分割する必要はありません。それでも 1MB より大きなものは FTP を使うことを考えるべきではないかと思います。

(11) アドレスと内容の再チェックを

送信するまえにもう一度送信先のメールアドレスと本文をチェックしましょう。

3 ネットニュース投稿マナー

ネットニュースへの投稿に関しても書き方については前章の電子メールマナーがほぼ適用されます。ここでは特に電子メールと異なる点について述べます。ただし、実際に投稿する場合には参考文献 [1] を熟読の上で行なって下さい。また、WWW ブラウズが可能な場合は次の WWW ページの「fj って何?」や「JUNET 利用の手引」等に目を通して下さい。

http://www.cs.orst.edu/~takikawm/fj/index.html

これらのドキュメントはネットワークからも anonymous FTP で入手できます。なお、筆者の所属する工学部情報知能工学科では現在のところ研究室配属前の学生についてはネットニュースへの投稿を原則として禁止しています。

(1) 引用について

ネットニュースへのポストでは、元記事の message ID をヘッダの Reference: 欄または本文中に入れることによって記事の特定が出来ますので引用部分とともにそれを入れるようにしましょうということになっています。つまり、誰が書いた記事かが分るようにしておくわけです。ネットニュースにおける記事は著作権法でいうところの公表された著作物であり、基本的に、記事の著作権は書いた本人がもっていることになります。通常の発言記事やそれに対するフォロー投稿時の引用ではあまりそのことを意識しないでポストすることが多いのですが、歌詞などを引用する場合には十分注意する必要があります。

(2) シグネチャについて

ネットニュースへのポストには必ず付けるようにしましょう。ネットニュースでは、記事を見た時にシグネチャから誰の記事かがすぐに分り、かつ4行程度に収まっている工夫を凝らしたものが見受けられます。しかし、シグネチャには出来るだけ個人情報を含めないほうがよろしい。シグネチャから得た個人情報を収集して悪用される恐れがあります。

(3) AUP (Acceptable Use Policy) に注意

神戸大学は外部とは WIDE および SINET でつながっています。メール/ニュースポストはこれらを利用することになります。WIDE や SINET は学術研究ネットワークです。つまり営利ネットワークではありません。ですから企業活動は禁止しています。

4 セキュリティとプライバシー

ネットワークの便利さの基盤はシステムの安全保護とユーザのプライバシーの確保があってこそです。そして、これらを支えているのは結局人間自身とその信頼関係であろうと筆者は思います。一般社会においてもそれらが崩れたとき様々な事故や犯罪が起こるのではないでしょうか。この辺りの議論は専門家に任せるとして、さて世の中には途方もなくコンピュータに詳しくてプログラミングが大好きという人がいます。こういう人をハッカー(コンピュータの隅々まで知りたいと望むプログラミング愛好家)と呼んでいますが、彼らによるシステムの不備の指摘には敬意を払うべき部分があります。しかし、クラッカーと呼ばれるコンピュータに不正に侵入しコンピュータそのものの破壊、情報の盗用などを企て実行する犯罪者の存在も嘆かわしくも事実です。マスコミではハッカーという呼び名が後者の意味にも使われていることが多いのですが、ハッカーが侵入したらそのとき彼はクラッカーという呼び名に変わるとでも説明しておきましょうか。

さて、呼び名はさておき以下では一般ユーザがセキュリティやプライバシーを守るためにどのようなことをすべきかをいくつか掲げてみます。セキュリティ技術に関しては参考文献 [2]、[3] が詳しい。ただし、これらは UNIX システムでのシステム管理者を主な対象として書かれていますので一般ユーザにとってはかなり難解で実感が湧かないかもしれません。

(1) パスワードについて

パスワードは、システムとユーザとの共有秘密であり、UNIX ホストではそのスーパーユーザでさえ普通は知り得ないものです。これは、最初にして最大と言って良いくらいの防御手段です。これが悪意を持った者に洩れた場合は、そのシステム全体が危険にさらされる可能性があります。

パスワードは通常何らかのアルゴリズムにより暗号化されてシステムに記録されています。しかし、暗号化されているデータが手に入れば復号することも簡単に可能な場合があります。あるいはそのようなデータが手に入らなくても、推定されてしまう場合(例えば誕生日などを使っていた場合)もあります。できるだけ復号が困難になるように複雑かつ憶え易いという

相反する条件を備えた文字列を選択する必要があります。具体的には本学科でアカウント登録（UNIX ワークステーション）をするときに以下のような注意を行なっています。

パスワードは、次の条件を満たすように決めて下さい。

(a) 6 文字以上

(b) 英字 2 文字以上と数字 1 文字以上、あるいは 1 文字以上の特殊文字を含める。

(c) 次のようなものはだめである。

- ログイン名、ホスト名、英単語、生年月日、電話番号、ライセンス番号コードなど
- 本人、友人、知人、有名人（歴史的人物、アイドル等）の名前や愛称等
- 自動車（バイク）の名前、愛称、メーカ名など

(d) (c) に掲げたような文字列の反転やずらしなどをしたもの、あるいはこれらの最後に数字や特殊文字を 1 つだけ付け加えたものはだめ。

＜パスワードとして相応しくない例＞

yamada	taro	kobeuniv	computer			
aaaaaaaa	qwerty	asdfgh	12345678	01234567	11111111	8811212
icluna	anulci	kyonkyon	kyon2	hanako3		

そして、パスワードは時々変更しましょう。変更の間隔としては半年に一度くらいで良いと思います。状況によりもっと頻繁に変えることを管理者から要求されるかもしれません。そのときは管理者に従って下さい。ただあまり頻繁に変更すると憶えきれなくて紙に書くことになってしまいますので、これは逆によろしくありません。

(2) アカウントの使い回しをしないこと

アカウントというのは、ユーザ登録制のコンピュータシステム（例えば UNIX コンピュータ）における「ユーザ名」と「パスワード」の 2 つからなります。これを持つということは当然ディスク容量なり周辺装置の使用権などが備わる訳です。これを何人かで一つ持つこと、つまりアカウントを複数人で共有することを "アカウントの使い回し" と呼んでいます。これは非常に危険であることを認識をしていただきたいと思います。なぜなら、第一に複数の人が同じアカウントでログインするということは、最後に使った人の特定が困難になります。その結果、第三者に不正使用されていても気が付くのが遅れたり不明になったりします。第二に、パスワードを決めるときや変更するときにどうしても分かりやすいパスワードを付けようとしますし、一度決めたパスワードは変えにくくなります。パスワードが一つ洩れれば、それを皮きりに非常に深刻な問題が生じる恐れがあるということを認識しておかねばなりません。また、個人に宛てたと思って出していたメールが実は何人かに読まれてしまうというプライバシーの問題も生じます。

(3)　スーパーユーザに求められる高いモラル

電子メール交換にしてもファイル転送にしてもデータはネットワーク上ではパケットという単位に分割（パケット化）されて通信が行なわれます。学内の支線 LAN にはイーサネットが用いられていますが、イーサネット上（ハブのポート等も同様）では、パケットと呼ばれる単位のデータが流れている訳です。パケットにはプロトコルや宛先やらが書かれたヘッダというのが付きます。自分の発信したパケットは、同一セグメント（1 本のイーサネットケーブルと考えて下さい）内のホストには一斉に届きます（正確にはブリッジが入っているかどうかなどで変ってくる）。そして、宛先のホストだけがそのパケットを取り込んで上位のプロセスへ渡します。その他のホストは自分宛でないので廃棄します。すべてのホストが宛先となるパケットとしてブロードキャストパケットというのもありますし、他のセグメントへ出る場合の話しもありますがここでは省略します。

さて、自分宛でないかどうかを判定するために結局はすべてのホストが一旦パケットを取り込んでいます。ですから、これを片っぱしから記録していけばネットワークに掛かっている負荷が分ります。しかし、これは言い替えればいわゆるネットワークの盗聴が出来てしまうということです。通常は、前者の目的のためにネットワークアナライザという装置が存在します。また UNIX マシンにもそのような目的のために色々なツール（コマンド）が用意されていますが、これらのコマンドは悪意を持って後者の目的に使われることを避けるためにスーパーユーザしか使えないようにパーミッション（アクセス権）が設定されています。つまり、スーパーユーザにはそれだけの権限が与えられるとともに非常に質の高いモラルが求められます。

(4)　パソコンの利用について

最近のパソコンの高性能化・低価格化にはまったく驚いてしまいます。一昔まえのワークステーションと呼ばれていたマシンの性能を越えたものが続々と登場しています。もちろんネットワークとの親和性もハードウェア、ソフトウェアともに非常に向上し、2 万円程出費して高速モデムを購入すればストレスの少ない IP 接続も可能となっています。イーサネットインターフェースを標準で搭載した機種では大概はハブの口（10Base-T の場合）さえあればすぐに接続できてしまいます。

ところが、マルチユーザ対応でない OS（MS-DOS, MS-Windows, MacOS 等）を搭載したパソコンというのは、当然 1 ユーザ専用に使われるようにソフトウェアは設計されています。それが故により簡便に利用できるように個人専用の設定が可能なように作られていることが多いのです。つまり、ネットワークアクセスにおけるパスワードなどを登録しておくことによって何度もパスワードを入れる手間を省けたりできる訳です。他人の設定がなされているパソコンの電源を入れるだけでもうその他人になりすますことが出来る訳です。UNIX マシンなどとの違いはまずここにあります。(UNIX マシンでもパスワードをつけていないユーザはもっと質（たち）が悪いかもしれない。)

ですから、共同利用のパソコンでは、個人情報は別々に保管できるように工夫しておく必要があります。例えば WWW ブラウザ として Netscape（これを使えばメールの送信やニュースのブラウズ、ポストなども非常にお手軽に出来る）を備えているなら Preference は面倒でも個々がフロッピーで管理するなどを実施することを推奨します。

他人になりすまして何をするのかと思うかもしれませんが、まずそれ以前にパスワードという壁がまったくなく侵入されている点に注意して下さい。あとは何をするかということは参考文献 [2] などをご参照下さい。参考文献には載っていませんが、そのアカウントからメールを出したとするとどうでしょう。相手は本来の正規ユーザとして応答なりをしようとするでしょう。とんでもない内容をネットニュースへ投稿したとしたらどうでしょう。便利さは危険と裏腹なのです。

(5) 席を離れるときはログアウトすること

UNIX マシンでもログイン状態のままそれを他人が利用すれば、他人になりすますことが可能であることは UNIX マシンの利用者はよくわきまえておかねばなりません。

(6) 電子メールは世界をめぐる

この題は大げさでした。ここで言いたかったことはメールが目的地に届くまで、多くのホストを中継されていくのですよということです。つまり、中継するコンピュータやあるいはケーブルまで含めて必ずしもセキュリティを十分考慮した環境にあるという保障はないのです。また、原理的には中継機で読まれる可能性もあります。もちろん、そのような不届きな中継機の管理者はいないと思いますが、好むと好まざるとに関わらずトラブルの発生時などには目に触れてしまうこともあります。

5 おわりに

電子メールは、今後は音声や画像なども含めたマルチメディアメールへと向かっています。ネットワークは今よりももっと広い帯域を必要としてくることは必至です。KHAN では今後バックボーンのより広帯域化をめざしており、非常に期待をするところです。また、セキュリティに関してもファイヤウォールの設置など積極的に取り組んでいます。

現在、関連学会や企業などにおいて暗号化等の研究が盛んに行なわれているところですが、オンラインショッピングやホームバンキングなどの実現に向けてだけではなく、より安全なネットワーク環境を支える基盤技術として早急に確立したいものです。

参考文献

[1] 「fj の歩き方」 fj の歩き方編集委員会編 オーム社

[2] 「UNIX セキュリティ」 Simson Garfinkel/Gene Spafford 共著 山口 英 監訳 アスキー出版局

[3] 「UNIX システムセキュリティ」 デビッド・カリー 著 小林 憲司 訳 ソフトバンク