ネットワーク上のトラブルに巻き込まれないために

理工学部知能情報システム学科
渡辺 義明

1　はじめに

ネットワークへの接続が急激に増加する中、ネットワークを巡るトラブルもまた急激に増加しています。トラブルに巻き込まれないためのネットワークのエチケット (Network Etiquette) を略してネチケット (Netiquette) と言います。ネチケットは数多く挙げられていますが、ここではインターネットに接続して電子メール、WWW、ネットニュースを利用する場合を想定し、注意すべき主な点を簡単に取りまとめます [1、2]。関連して様々な悪意を持った攻撃から身を守るため、セキュリティ面での注意点も述べます [3、4、5、6]。

2　一般的注意点

インターネットを利用する上での注意点と言っても特別なことではありません。現実社会での行動と同様な注意を心掛けることです。インターネット上には理想社会があると錯覚してはいけません。インターネットに参加しているのは、現実社会で見かけるのと同じ人間です。しかも多様性と人数は、大学内で現実に会う人間より格段に大きくなります。

インターネットでの発言は、顔の見えない何万人もの人達を前に記録を残しながら発言しているようなものです。ことの重大さを認識しましょう。犯罪行為や、犯罪にはならなくても人が迷惑に思ったり嫌悪する行為、利用している計算機やネットワークにふさわしくない行為は止めましょう。また流れて来る情報も多様な人間が流しているものです。偽情報や詐欺話などが大量に存在します。一般常識を働かせて判断しましょう。

インターネットには以下のような特性があることを心得て下さい。

1. **コミュニケーションの幅が小さく、相手の反応が見えにくい。**
   - 現実社会では言葉だけでなく表情や手ぶり等で多様な信号を送り、また相手の反応を見ながら修正をしていくことが可能ですが、インターネット上の情報伝達の幅は極めて制限されています。
   - 「xx をやって下さい」と言うメッセージは、「命令」・「依頼」・「哀願」のどれでしょうか。また、「xx は分かりますか」は、「軽蔑 (君には分からないと思うけど)」・「質問 (私は分からないので知りたいが)」・「確認 (説明を略して話したいが)」のどれでしょうか。十分に吟味した丁寧かつ冗長な言葉を使い、こちらが意図した通りに相手に受け取られようにしましょう。冗談は冗談と受け取られないと考えて下さい。
2. **簡単な操作が広く影響をおよぼす。**
   - インターネットでの情報は高速に広範囲に広がります。世界に公開する覚悟をして送信下さい。間違いを後で訂正するのは大変です。発信する前にもう一度、考えて下さい。特に感情的な内容の場合は、送信の前に十分な時間を置きましょう。
   - 他人が自分と同じ行動をしたらどうなるかを考えましょう。みんなが一人にメールを出すと、受信者のシステムはパンクします。また、メールを次々に転送するとネズミ算的に広がります。受

信者が次々に 10 人にメールを転送したら、1 → 10 → 100 → 1000 と増え、10 回も転送すれば世界人口を突破します。

3. **匿名での行動ができる。**
   - 現在、インターネットでは自分の正体を隠したまま行動することが可能になっています。このため勝手な行動や犯罪が起こりやすくなります。儲け話などのうまい話は警戒し、自分のことは自分で守れるよう行動しましょう。自分の行動は自分の責任になります。相手の肩書やアドレス等は架空のものであるかも知れません。また本人でないかも知れません。
   - 自分の名前を出して発言しましょう。匿名での行動は取らないで下さい。
4. **多数の計算機と人間が有限の資源を共有している。**
   - 有限の資源を浪費することのないようにしましょう。自分と同じことを他人もしたらどうなるかを考えて下さい。
   - インターネットを流れる情報の秘匿性は高くありません。秘匿したい情報は暗号化などの対策を取りましょう。
   - 一ヶ所が破られるとそこを足掛かりにして周辺が被害を受けます。あなたのパスワードが破られると、その計算機の他のユーザーおよび周辺の計算機が「あなたの名前」で荒らされ、あなたが非難されます。パスワードには十分に注意して下さい。
   - インターネットがスムーズに動くには、各計算機の管理を行なっている人達の努力が必要です。その負荷を正当に評価し、無用な負荷を掛けないで下さい。
   - みんなの持っている知識、信念、考え方などは共通ではありません。自分の常識は決してみんなの常識ではありません。インターネット上の議論に参加するには、その前提を十分理解して下さい。
   - お互いが快適に利用できるようにするため、機器を占有しないで下さい。また他人の利用権を侵害しないで下さい。

以下、インターネットの代表的なアプリケーションについて、個別に注意すべきことを述べます。

3 電子メールのエチケット

- 送信の日本語は JIS コードを使い、1 行に 30〜35 文字程度として下さい。半角カタカナや機種独自の特殊文字は使用しないで下さい。受信先で文字化けを起こすことがあります。ヘッダー部分の日本語もトラブルを起こす可能性があります。また、メールにワープロ文書や絵などを添付するときは、先方がそれを読めるか確認してからにして下さい。余りに大きいメールは避けて下さい。

- メールは出せば必ず届くとは保証できません。どこかで迷子になることもあります。また、ネットワークのトラブルで消えることもあります。相手のアドレスは間違えないようにして下さい。必要なら返信を要求下さい。

- 不特定多数の間でメールを次々と転送する行為 (チェーンメール) は止めて下さい。たとえそれが有用な情報だと思われてもいけません。「システム破壊メールに注意」や「不治の病の子供を救済」など、「警告」や「善意」を装ったメールがネットワーク上を何年にも渡ってさまよっています。目的は手段を正当化しません。

- お知らせメールは回数と対象人数を必要最低限に絞って下さい。メールを読むだけで一日が終るような事態の発生は避けましょう。可能であれば WWW など、他の手段を考えましょう。

- 届いたメールを公開する時は送信者の許可を貰って下さい。また、公開時や転送時には、元の主旨を変えるような部分引用は止めて下さい。著作権に注意しましょう。
- メールは毎日確認するようにして下さい。メールも記憶領域を消費します。読まずに貯めることや不要メールまで保存することは止めましょう。
- 即時に応答のある人や一日一回確認の人、アドレスを持っていても全く読んでない人など様々であることを留意した利用をして下さい。
- 当然のことですが、言葉使い、誤字脱字、誤解を招く表現はないかなどは十分に注意して下さい。感情的な応答は避けて下さい。情緒的なことや込み入った議論などは別の手段との併用が必要です。
- メーリングリストに参加すると大量のメールが来ることを認識下さい。参加の際には脱退の手続きを確認し、必要無くなったら速やかに脱退して下さい。

4 WWW と ftp のアクセスのエチケット

- WWW や ftp のアクセスはネットワークが混む時間帯を避けて下さい。ネットワークは様々な用途で利用されています。本当に必要な利用を優先させましょう。
- 取得するデータ量が大きい場合は、回りの迷惑にならない時間帯と間隔で取得下さい。ftp は複数のサイトが同じ内容を持っていることが普通です。なるべくネットワーク的に近いところから取得下さい。一般に大学からは大学関連のサイトが近いです。

5 WWW 発信のエチケット

- 犯罪行為、人権無視、公序良俗違反などの反社会的、反倫理的情報の発信は止めて下さい。また、ホームページの存在する計算機やネットワークにそぐわない情報の発信も避けて下さい。例えば学術ネットワークは学術目的に利用し、商用利用などは止めて下さい。
- ホームページにリンクを入れるには、リンク先の許可を得て下さい。写真、絵、音楽、文章など、他人のデータを利用する際には著作権等に充分注意を払って下さい。

6 ネットニュースのエチケット

- 議論に適切なグループを選んで発言して下さい。複数のグループ間のクロスポストは勧められません。どうしても必要な場合に限って下さい。グループ内の約束事や議論の流れを把握した後に、その場にふさわしい発言をして下さい。ローカルグループとグローバルグループの使い分けをし、近くで片付くことは近くで片付けましょう。テスト投稿はテスト用の場所で行なって下さい。
- ヘッダーに日本語を入れると読めない環境があります。ヘッダーを参照しないで分かる記述をしましょう。また半角カタカナや機種独自の特殊文字は使用しないで下さい。受信先で文字化けを起こすことがあります。
- 単に賛成もしくは反対の発言や感情的な応答、冷やかし、誤解を招く短い発言は止めて下さい。議論を発展させるため、論点を整理し深化させる発言をして下さい。自分の考えを主張すると同時に相手の多様な考えにも寛容な態度を取って下さい。

- 一般に発言はその人個人の意見表明で所属組織とは無関係と解釈して下さい。発言の際には名前を出し責任を持って下さい。プライバシー暴露や個人攻撃など、反社会的／反倫理的発言は止めて下さい。
- 故意または過失による間違いやデマ話が多数存在します。少額のお金を払い込めば簡単に大儲けできるなどの詐欺も頻繁に出てます。常識を働かせて下さい。
- ニュースで質問する時は、まず自分自身で解決できるか努力し、その結果分かっていることと分からないこと、その他問題解決に必要な情報を付記した具体的かつ限定なものにして下さい。質問のポイントが相手に伝わらないと満足できる回答は期待できません。

7　セキュリティ

ネットワークは世界に開かれています。そのため様々な攻撃がかけられています。利用時にはセキュリティに対する配慮が必要です。

- メールは封書でなく葉書と心得て下さい。メール以外のデータ伝送も同様です。多数の計算機とネットワークを経由して送られます。伝送途中でデータの盗聴や改ざんが可能です。データに守秘や信用を持たせるには暗号化や電子署名などの対策が必要です。またはネットワーク以外の手段にして下さい。
- パスワードは個人で管理し他人に使わせないで下さい。また、使用中の状態のまま計算機の前を離れないで下さい。あなたのユーザー ID で発生したトラブルの責任はあなたにかかってきます。
- 一人のパスワードが破られるとその計算機の他のユーザー及び近隣の計算機に影響が及びます。侵入された後では、中にどんな仕掛けをされたか分かりませんので、単に穴を塞ぐだけでは済みません。システムの入れ直しやユーザー全員のパスワードの変更など多大な作業が発生する可能性があります。さらに、あなたのユーザー名でよそが攻撃されると、あなたおよびあなたの所属組織が非難されます。
- パスワードは 6〜8 文字からなり、英大文字、小文字、数字をできるだけ多様に含むものが推奨されます。個人情報に関連する事項、辞書にある単語、アイドルやゲームなど趣味や嗜好に関する名前、キーボード配列順などは、簡単に破られます。日本語のローマ字表記も危険です。
- 標準設定のままでは、どこからでも侵入許可となっているソフトがあります。新しいソフトウェアを導入したときは、利用許可の設定は標準で良いか確認して下さい。
- ネットワークから手にいれた身元のはっきりしないソフトウェアはウィルス感染の危険性があります。また、ワープロや表計算ソフト等のデータファイルに取り付くマクロウィルスがあります。身元のはっきりしない添付文書を開く時は注意しましょう。
- WWW を利用したシステム破壊やデータ盗み出しが頻発しています。WWW ブラウザはセキュリティホールの少ない版を利用して下さい。データの送信やソフトのダウンロードなど、セキュリティ上問題がありそうな時には確認メッセージが出ます。メッセージの意味を理解して適切に応答して下さい。OK ボタン一つで、システムを破壊するようなソフトが走ることも起きています。WWW サーバーを動かすと更に危険性が大きくなります。公開と守秘は相反することを認識下さい。
- WWW ホームページ上やネットニュース投稿記事などには、住所や電話番号、生年月日等、自分のプライバシーに関する情報を公開する場合には、悪用される危険性を認識下さい。当然ながら他人のプライバシーも尊重しましょう。

8　おわりに

インターネットは現実社会との結びつきを急速に深めています。しかし、発展が急なため様々な制度、コンセンサスの整備が不十分のままです。今のような自由かつ快適なネットワークが今後ともに続いていけるかどうか分かりません。規制強化や無法地帯化はお互い望みませんが、マナーが悪いとどちらかに陥ります。ネチケットを心掛けましょう。

下の参考文献の情報を参考にさせて頂きました。全てを網羅できていませんので、より詳しくは以下を参照して下さい。

参考文献

[1] S.Hambridge, “Netiquette Guidelines”, RFC1855, 1995.

[2] “ネチケットホームページ (東金女子高等学校)”, http://www.togane-ghs.togane.chiba.jp/netiquette/

[3] 道本健二、三輪芳久、高本優、“インターネットに潜む罠”, 日経バイト、1997年10月号 182-222ページ

[4] “コンピュータ緊急対応センターホームページ”, http://www.jpcert.or.jp/

[5] “日本コンピュータセキュリティ協会ホームページ”, http://www.jcsa.or.jp/

[6] “情報処理振興事業協会コンピュータセキュリティ対策ホームページ”, http://www.ipa.go.jp/SECURITY/index-j.html