インターネット社会を安全に暮らすために

ー知識集約型社会における個の自衛ー

ーインターネットとは何なのでしょうー

かつて､電話会社が電話網というネットワークをすべてコントロールしていました。それに替わって､自由に通信網につないでも良い権限を持った通信基盤が現れました。

その通信網は接続している各参加者が末端にさらに通信網をつないでもいいという権限と自由度を持っているかわりに、接続している各個人に責任が課されます。
それがインターネットです。

現在までインターネットは自由度と強力な権限ばかりがクローズアップされ､一緒に付随するはずの責任がないがしろにされてきました。

結果として､ウィルスやスパムメール、ネームサーバー詐称等の無責任かつ違法な通信がまん延し、最終的なインターネット崩壊の危機すら訴える研究者もいます。

ネットワーク社会の秩序を守り、 今後もインターネットの維持を可能にしていくためにはすべての個人が責任について再認識する必要があります。

今後インターネットを使っていく上で、何に気をつけ、
どのように向き合っていけばいいのか、この冊子を読んで一緒に考えてみましょう。

ーインターネットに対する認識ー

「インターネット」という組織や回線は存在しません。いろんな組織や個人のコンピュータやネットワークが相互に繋がって、インターネットを構成しています。

接続しているプロバイダもインターネットの一部です。

もちろんあなたのパソコンもインターネットに接続したらインターネットの一部です。

インターネットの一員になるには次のことを認識しなければいけません。

- 参加を助けてくれるサービスはありますが、「インターネット」という商品は存在しません。
- インターネットは陳腐化した古い技術につぎはぎを当てながら機能しています。
- 世界が繋がっているのは相互理解によるものであり、誰も接続を保障していません。
- 心無い人や自覚の無い人によってインターネットの管理状態は日々悪化しています。

- 加入する「プロバイダ」は、広大なネット上のひとつの「集まり」にすぎません。

- 人に迷惑をかけられることもあれば、知らずに迷惑をかけてしまうこともあります。
- 「人」に裏切られることもあるかも知れませんが、人を助けたり助けられることもあります。
- 非常に簡単に知識を得ることができますが、反面考える力を失う可能性もあります。

ーまず技術を知りましょうー

「ドメイン、DNS って何？」

相互に繋がりインターネットを構成している組織（ドメイン）はそれぞれを区別するために "192.0.2.1" といった番号(IP アドレスといいます)を割り振って管理されていました。

それを " www.example.com" といった名前で検索できるようにしたのが DNS(ドメインネームシステム）です。

たとえばあなたが " http://www.example.jp/" へ接続する際は、一度 DNS というインターネット上のシステムに問い合わせを出し、その名前に対応する番号（IP アドレス）を得ることにより、相手と通信をすることができます。

「電子メールって何？」

個々の「ドメイン」はメールサーバを持つことができます。
ドメイン(多くの場合プロバイダ)に加入していれば､メールを使用することができます。

”あなたが友達にメールを送る”と、あなたのパソコンは、

あなたのドメイン の「メールサーバ」にメールを託し、

▼

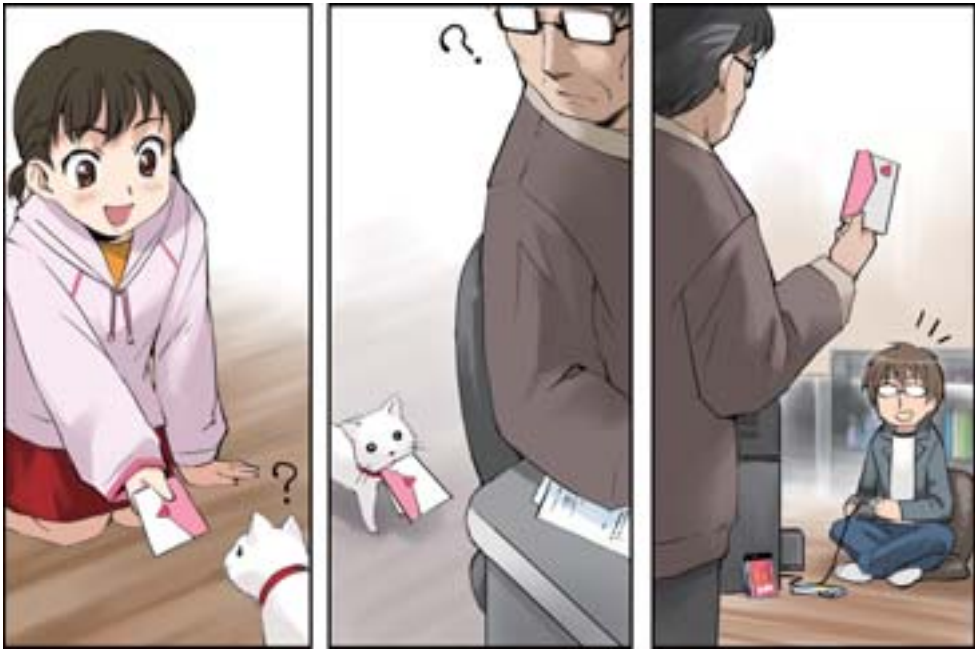
その「メールサーバ」は**あなたの友人の「メールサーバ」**にメールを送ります。

▼

その友人のドメインの「メールサーバ」がメールをそれを「受け入れれば､」

▼

”あなたの友達はあなたのメールを読むことができます。”



メールの送受信は、あなたのドメインのメールサーバとあなたの友人のドメインのメールサーバの「暗黙の信頼関係」によって可能になっているのです。

その「暗黙の信頼関係」が崩壊してしまうと、メールを送信しても届けることができなくなってしまいます。

「WWW(ワールドワイドウェブ)、URL、ブラウザって何？」

世界中のホームページや各種の電子データにアクセスできる仕組みが「World Wide Web」、俗にいうウェブです。

ホームページを制作し、公開されたコンピュータ (WWW サーバ)に設置することにより、誰もが世界に向けて情報を公開することができます。

ホームページ同士はリンクを使ってお互いを繋ぎあう(ハイパーリンク)ことが可能です。ホームページの住所にあたるものを URL といいます。URLを入力すると、目的のコンピュータに接続し、ホームページ閲覧ソフトで表示します。

ーインターネット接続の心得ー

「自宅でつなぐ」

購入直後のパソコンのＯＳ(基本ソフト)は欠陥が多々あり、常に正しい動作をすることは期待できません。「ルータ」と呼ばれるネットワーク間接続機器を使わず、PCを直接インターネットに繋ぐと、すぐに伝染性の高い悪質なプログラム(自己増殖型の破壊プログラム、ワームと呼ばれる)に感染する可能性があります。

最低限以下のことは行いましょう。

- パソコンを直接回線に繋がず、「ルータ」を入手して繋ぎましょう。
- 基本ソフト(ｳｲﾝﾄﾞｳｽﾞやﾏｯｸOSなど)を自動更新して欠陥を修復するよう設定しましょう。
- 応用ソフト(メールソフトやホームページ閲覧ソフト)を自動更新するよう設定しましょう。
- ウイルス対策ソフトを入れ、自動更新するよう設定しましょう。

（コンピュータ）ウィルスとは主に PC の破壊をすることを目的に人為的に作られたプログラムの総称です。自己増殖や次々に他の PC に移動（感染）して被害を拡大します。

「職場や外で繋ぐ」

PHS、携帯電話、公衆無線 LAN、職場や学校のネットワークに接続する際には十分な注意が必要です。「フラッシュメモリー」等を利用したデータ交換も同様の危険が伴います。繋ぐネットワークや、PC にワームが蔓延している可能性が無いわけではありませんしあなたのパソコンがウィルスやワームをばらまいてしまう可能性もあります。

むやみにつなぐのはやめたほうがいいですが、どうしてもつなぐ必要がある場合は、以下のことに注意して繋ぎましょう。

- ウィルス対策がしっかり機能していることを確認しましょう。
- OS のフィルタリング機能やファイアウォールソフトで不要なサービスへの接続を止めましょう。
- 接続相手が本物であり暗号化が確実であることが確認できない限り、見られて困るデータ (パスワードなど) は送受信しないほうがいいでしょう。

「他人のパソコンを使う」

ネットカフェや公共端末、あるいは知人のパソコンを使用する場合も
危険が伴うことを理解しておきましょう。
パスワードなど個人情報の入力は極力控えるべきでしょう。

以下のことに注意して繋ぎましょう。

● PC の管理者も知らないうちに第三者に盗聴される危険があります。
（PC がスパイウェア (パソコンの利用履歴を盗み出すソフト) に感染している場合もあり、自分や持ち主のプライバシーを漏洩させてしまう可能性があります。）

● 人に自分のパソコンを使われることももちろん危険が伴います。

ーホームページの閲覧の心得ー

ホームページの閲覧にも自衛の意識が必要です。

- 見るだけで**悪質なプログラム**＊に感染してしまうページが存在します。
- 個人情報をパソコンから盗み出すようなページも存在します。
  （銀行をよそおい、暗証番号等をぬすむフィッシング詐欺に注意が必要です。）
- DNS やパソコンに細工されて、偽物のホームページに誘導されてしまうことがあります。
  (あなたが見ているページが本物であることを見分けるのは実は困難です)

- 現実世界同様、ホームページの内容自体が
  必ずしも信用できるものばかりではありません。

- 人によっては精神的ダメージを受けるような内容のホームページも存在します。
- 一般にホームページには著作権があり、無断で転用すると罪になります。

＊ウイルス、ワーム、スパイウエア等のマルウエアと呼ばれる一連のソフトウエア

「リンクをクリックする際に考えるべきこと」

- ”重要な情報” や ”ここ見て”など、注意や興味を喚起する内容のがメールが送られてきた場合、本文にリンクのクリックが促されていたら、確実に怪しいと思いましょう。
  （* もしクリックする場合も、クリックする前にリンク先を「よく」確認しましょう。）
- ホームページのリンクやメールアドレスが偽装されている場合があります。
- 気がつかないうちに意図しないサイトを見せられてしまう場合があります。
- 接続先が本物かどうかの判定は”http://”で始まるページでは困難です。
  （”https://”ではじまるサーバの場合も、カギマークの確認など、その信頼性を見分ける知識が必要です。）

- 「これは偽物のページかもしれない」という意識が自衛につながるかもしれません。

「オンラインショッピング／ネット取引の心得」

インターネットでショッピングなどの金銭取引を行ったり、アンケート等で個人情報の提供をする場合は、一度予想されるリスクを考えましょう。
現実であってもネット上であっても、悪意ある罠にかかる危険性は常にあります。

ネット上での取引は特に次のことにしっかり留意して検討しましょう。

- 入力する個人情報／プライバシーは漏洩するかも知れないことを予想しておきましょう。
- もしも情報が漏洩した場合、それを知る手段を検討しましょう
- 決済方法によるリスクの違いを知りましょう。
- 原則として通信販売はクーリングオフできません。
- 取引にトラブルが生じた場合､誰がどのような対処､補償をしてくれるのか確認しましょう。
  (でもその内容自体が偽りのページである可能性もあります。)

- 取引の被害が自分にとって許容できる範囲のものか予想してみましょう。
- 安全性に対する自分の知識を自覚して取引に望みましょう。

個人情報の入力の際に使い捨てのメールアドレスを使用したり、住所の一部に記号を入れるなど、
情報の記述に変化をつけることによって、情報漏洩が起こった場合の手がかりをつことが出来るかもしれません。

決済方法によって､さまざまなリスクが発生します。●先払いによる取引は商品が届かない可能性が０ではありません。●エスクローサービスという危険を担保する制度があります ●代金引換えは開封した場合､基本的に返品､返金に応えてもらえません。 ●クレジットカードは番号が盗まれて悪用される危険性がありますが、重大な過失や故意がない限り､身に覚えのない請求に対する支払を拒否することができます。

これから取引をする予定のお店に、以下の判定はできますか？

- 入力画面や重要な表示が行われるページにおいて、暗号化とサーバ証明書は提供されていますか？
- そのサーバ証明書自体は信用できるものですか？
- 相手のサーバが本物だとして、そのサーバ自体が安全に運用されているかどうかも意識するべきかもしれません。

もちろん 100% の安全は望めません。
トラブルを想定し、自己の許容範囲内で利用しましょう。

（サーバー証明書がある場合でも,その信頼性を見分ける知識が必要です、注文フォーム等、重要な情報を送信するページは枠に鍵マークが表示されているかを確認しましょう。さらにその鍵マークにマウスのアイコンを合わせ、128bit 以上の暗号化されているかどうかを確認しましょう。さらに証明書があなたが通信したい本当の相手に発行されたものかをよく吟味する必要があります。）

「オンラインバンキングは利用しても大丈夫か」

もちろん安全だとはいいきれませんが以下の選択肢があるでしょう。

（1）安全性の判断ができないので利用しない。

（2）安全性をしっかり確認して自己のリスク判断で利用する。

（3）金銭被害が生じたときに補償してくれる銀行を選んで利用する。
（ごく一部の銀行が限度額の範囲内で補償や保険を用意しています）

安全性を確認するうえで以下のことに留意しましょう。

- 入力画面や重要な表示が行われるページにおいて、暗号化とサーバ証明書は提供されていますか？
- そのサーバ証明書自体は信用できるものですか？
  - 128bit 暗号化はなされていますか？（カギマークのクリックで確認）
  - 信頼できる機関から発行されたものですか（ブラウザで確認可能）
  - あなたが思っている組織に与えられた証明書ですか（本物と比較する必要があります）

- 相手のサーバが本物だとして、そのサーバ自体が安全に運用されているかどうかも意識するべきかもしれません。

「コミュニケーションの心得」

電子メールのしくみについて正しい認識を持ちましょう

- 電子メールが必ず相手に届く保証はありません。
- 電子メールが正しい相手に届く保証もありません。
- 電子メールがどれだけの時間で相手に届くかも保証できません。

- 受け取ったメールの差出人 (From:) は簡単に詐称できます。

- 怪しいメール、迷惑なメール (スパムといいます) が送られてきたら無視しましょう。
- 受信を拒否するメールを送信することも、逆効果です。
- チェーンメール(複数の人への転送を要求するメール)も同様に無視しましょう。
- わからない人からの添付ファイルは「絶対」開いてはいけません
- 知人からのメールでも本文で説明のない添付ファイルは開かないようにしましょう。
- 「ウィルス対策の施し方」の書かれたメール」の添付ファイルは危険です。
- HTML 対応のメールソフトは取扱いに注意が必要です。
  (理解して HTML 表示機能を制限しておく必要があります。そのまま使用すると容易に
  ウィルスに感染したり、勝手にメールを開いたことが通知され、迷惑メールがエスカレートします。)

● スパム対策を行うようプロバイダや自組織の管理者に申し入れましょう。

●対策による多少の不便が生じても理解に心がけましょう。

・迷惑メールを受けるのも権利だと思うのはインターネット全体を考える上でエゴイスティックな側面があります。
（メールサーバで受信する行為自体が、サーバやネットワーク全体の負荷になります）
・インターネット利用者全員で対策しないと、「電子メール」というシステム自体が使えなくなる可能性があります。
（すでに電子メールは崩壊しつつあるという人もいます）

● 自分自身がウィルスに感染して迷惑メールをばらまいていないか調べましょう

「文字によるコミュニケーションが、対面による コミュニケーションとは異なる性質を もっていることを理解しましょう。」

● 文字によるコミュニケーションは誤解が生じやすくなります。

- 相手が実際の人物とは異なる人格に「なりきる」場合があります。
- 自分自身もまた、普段と異なる性格になっているかもしれないことを意識しましょう。
- 議論が本題とは関係の無い挙げ足とりや中傷合戦になる場合があります。
- 面識のまったくない人と容易に親しくなることができますが、現実の世界と照らし合わせて、そのリスクを再度よく考えてみましょう。
- 履歴が常に残るので、後で第三者に読まれる可能性があることに留意しましょう。
- コンピュータでのコミュニケーションに浸り、現実のつながりを疎ましがるネット中毒に気をつけましょう。

ー まとめ ー

膨大な知識がネットワーク上に集約され、どんな情報も容易に引き出せるようになりつつあります。その一方で、人々が考えるということをしなくなっているという指摘があります。

結果だけを安易に求めるという意味でショートカット症候群と呼ばれています。しかし、情報は溢れていても、本当に「知識」や「知恵」は容易に手に入るのでしょうか。

皆さんはこれだけの情報が溢れる中にいても、安全を守るためにどんな知識が必要なのか、わからなくなっていることに気がついていませんか？

大切なことは自ら考えることです。
でもそれは安全に関する技術的知識をすべて習得するということではありません。
それはほとんど不可能でしょう。
必要なことは自分の行為がどういうリスクをはらんでいるかを考えることです。
それができれば、 覚悟の上で行動することも回避することもできます。

またリスクを軽減する方法を自ら調べる気になれば、
ネットに集約された知識も、 ネットの先の人々も力になってくれることでしょう。

参考情報
本パンフレットでは技術的な解説は極力避けました。 またネット社会は常に変化しています。 最新の詳しい情報へのリンクは以下のページを御参照ください。

https://www.tokai-ic.or.jp/selfdefense/

鍵マークをクリックしサーバ証明書の Fingerprint を確認してみてください。
SHA1: EB:9B:FD:92:1A:EE:16:55:3C:BE:1C:9B:79:A1:B3:B6:BD:F1:63:1F
MD5: A9:11:28:1F:71:53:8B:9E:01:E7:78:2F:2E:8A:9D:C6

ネット社会同様、現実世界でのトラブルにも十分気をつけましょう。

本パンフレットは日本自転車振興会の補助金を受けて作成されています。

監修・編著
知識集約型ネットワーク社会における個の自衛研究委員会
顧問　福村晃夫 (名古屋大学名誉教授)
委員長 鈴木常彦 (中京大学 情報科学部情報科学科　助教授)

デザイン : 安藤康治 (有限会社デジタルワークショップ)
イラスト : しらゆき昭士郎

発行
財団法人 人工知能研究振興財団

〒461-0011
愛知県名古屋市東区白壁 3丁目12番 13号
(中産連ビル本館 3 階)

TEL 052-932-8951　E-mail info@airpf.or.jp
FAX 052-932-9158　http://www.airpf.or.jp