

次世代インターネットを俯瞰する

Digital Xpress 編集部

日々進化し続ける世界にあって、現在私たちが当たり前のように利用しているインターネットの世界も変わりつつあります。すでに、インターネット創成期にはとても考えられなかった、様々なサービスがインターネットを通して行えるようになってきています。

その昔、インターネットと言えば「Yahoo」などに代表されるポータルサイトから発信される情報を閲覧し、そこにあるリンクをたどって、情報を拾い集めるものでした。ところがここ最近のインターネット事情には変化が生じています。社会現象ともなった「ブログ (Blog)」とか「ブロガー」という言葉を聞かれたことがあることでしょうか。個人個人がブログというツールを使用して、情報を簡単に発信できる仕組みが整ったため、情報の発信源、収集対象が無限に広がってくるという現象が生じています。

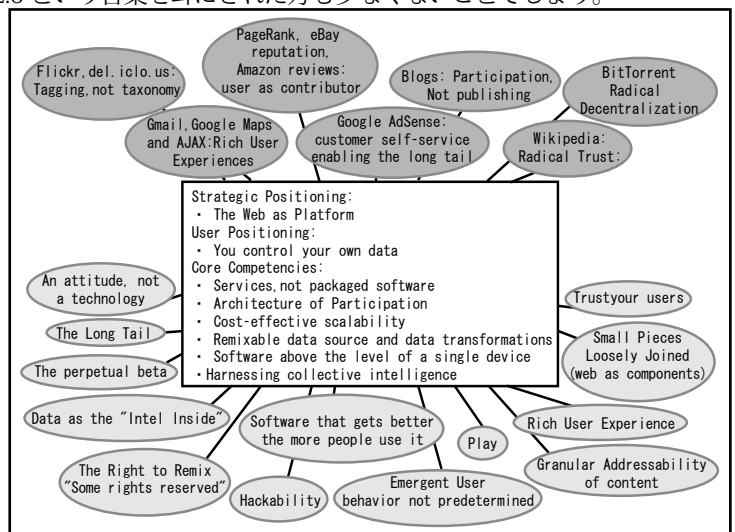
既に、私たちはインターネットの世界の新しい広がりを感じつつあります。この先、インターネットはどのように展開していくのでしょうか？この特集では、次世代を担うであろう、インターネット技術に焦点を当てて、解説をしていきたいと思えます。第1部は、次世代インターネット Web2.0 について、第2部はそれを支えるネットワークについて、そして第3部ではセキュリティに焦点を当てます。

第1部：Web2.0

次世代インターネットそのものの変化を表す言葉の1つに Web2.0¹ があります。最近、いくつかの雑誌で取り上げられるようになり、ブログ上でもとても話題になっているので、Web2.0 という言葉を耳にされた方も少なくないことでしょう。

さて、Web2.0 とは何でしょうか。Web2.0 という言葉を最初に使ったと思われるのは、ティム・オライリー 氏²です。オライリー氏が2005年にまとめた論文が以下のURLです。
<http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-2.0.html>

論文中に掲載されている、Web2.0 を構成する要素について図を掲載します。さて、これをざっと見てもわかるように、Web2.0 というものは、なにか新しい技術の集まり、というわけではありません。では、一体なんなのでしょうか。一言で説明するのは中々難しいのですが、「新しいインターネットのためのサービスフレームワーク」と言うことができそうです。では、その要素のうちの代表的なものをご紹介します。



▲ 図1：Web2.0 Meme Map

ロングテール

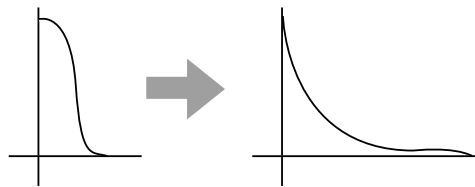
ロングテールの代表としては、アドワーズ、あるいは Google の Adsens 広告モデルが挙げられています。この広告、皆さんもよく目にするのではないのでしょうか。(図2、図3)

このアドワーズ広告のモデルですが、広告主側は特定のキーワードに対して、1クリック何円という形で入札を行います。そして、入札額が高ければ高いほど、検索結果ページの脇に上位に表示される、という仕組みとなっています。これは、検索する際には、何かしらその情報を欲しがっているわけですから、そのキーワードにマッチする広告が表示されれば、ユーザーのクリック率も高まり効果的な広告につながるというわけです。

Adsens は、サイト運用者側の仕組みで、広告を表示することにより、お金を稼ぐというモデルです。今までの広告表示はサイトの内容に関らず、とにかく広告が表示されていましたが、

この広告表示はサイト側の情報を登録することによって、そのサイトの情報にあった広告が表示されるようになるので、広告を出す側にとっても広告を表示する側にとっても、そしてサイトの利用者にとっても非常に効果的であるといえます。

これがロングテールを表す代表例と言えるのはなぜでしょうか？今まで、一般的に、「2割の商品で8割を稼ぐ」と言われていました。しかし、現在では消費者の多様化が進み、必ずしもこの法則は当てはまらなくなっています。では、その分どのような変化が生じたのでしょうか。1つ1つの商品や製品はその市場に占める割合からすると非常に小さいのですが、それが非常に沢山存在するようになったのです。

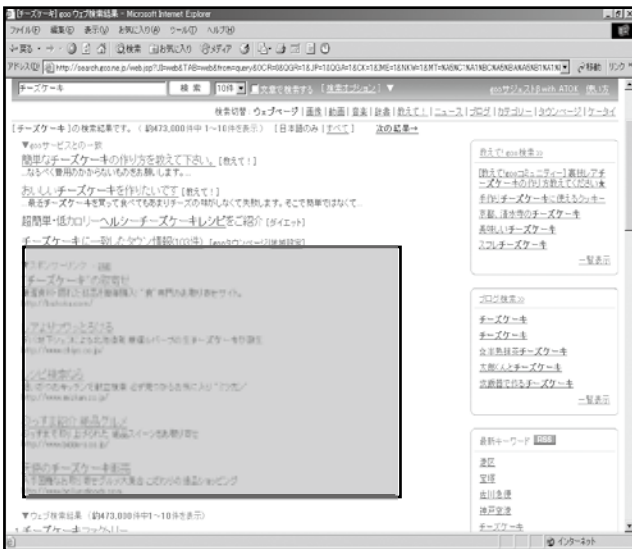


上の図はその様子を表しています。

裾野がある意味無限に広がってきた、といえます。つまり裾野（テール）が広がっている（ロング）というわけです。

こうなるとなにか1つの市場を1つの言葉やパターンで分析するのが難しくなります。また、広告を打つのも難しいといえます。

こうしたニッチとも思えるロングテールに対応した1つの例が先に取り上げた広告です。たとえニッチな商品でも、ユーザが検索した場合それに対して何か興味をもっているわけです。ですから、検索用語に関連した広告が表示されるのは効果的です。また、1単語の入札によって決まりますが、ニッチなものであれば、非常に安い単価ですみます。一般的に広告を打つのは非常に高価ですが、このモデルならユーザが必要としただけ、広告料を払えばよく、ロングテールにマッチしたモデルだといえます。ロングテールの市場を掘り起こし、ニーズに対応できるのも Web2.0 ならではのものです。



▲ 図3：Adsens の例（グレーの枠内）

◀ 図2：アドワーズ広告の例（goo での利用例）³

注1：流行に乗って？こんな会社も出ています。

<http://www.webtwo.co.jp/>

注2：ご存知の方も多いとは思いますが、Perl や UNIX 関連のインターネットを支える様々な技術書解説書を出版しているオライリー社の創設者です。出版事業やその他のコミュニティを通じて

インターネットの先端を走る人の一人。

注3：流行最近はまっている「チーズケーキ」で検索してみました♪ お手軽なところでは、モスのチーズパー（安っ！）。ちょっと一息入れるのに最高です。



▲ 図4：ブログの例



▲ 図5：ユーザによる書評 (Unibookの例) 5



▲ 図6：地図検索の例

ユーザーの参加、およびユーザーの信頼

ユーザーの参加、ユーザーの信頼という意味で代表的な例はブログといえるでしょう。これまでニュースといえば、各報道機関が発表する情報がそのままWebに載せられているだけのものでした。一方、ブログはユーザーが自ら参加し情報を発信していくことができます。(図4)

次にユーザーの信頼が挙げられます。その例としては、「書評サービス」を挙げることができます。これは、本の内容を実際に読んだユーザーが評価をして、その内容を次の購入者に示すことのできるサービスです。一種の「口コミによる評価」ともいえます。(図5)

ちょっと考えてみてください。私たちが普段買い物をするときに、広告や企業の売り文句だけをみて、決めることができるでしょうか？必ずしもそうではないはずですが、すでに使用しているご近所の評判を聞いて評判の良いものを買うのではないのでしょうか。

これがインターネットの世界でも実現されるようになったことなのです。

まり、今までは情報を受け取るだけだったユーザーが情報を発信し、その情報を信頼して次のサービスにつながる、というモデルです。

ページ上での直感的な操作

既に、ご存知の方も多いと思いますが、「ページ上での直感的な操作」の良い例はgooの地図検索サービスです。今まで、いくつか地図を検索するサービスはありましたが、『goo 地図』の特徴となっているのは、ドラッグによって地図がスクロールできたり、図6のように周辺検索をわかりやすい形で表示できる、といったものです。これは、何も新しいプラグインを作ったものではではありません。JavaScriptやDHTMLといった私たちにも耳慣れた技術をちょっと工夫⁴しているだけなのです。

このように、なにか新しい技術ではなく、使い古された既存の技術を使って利用者に優しい、ページ上で直感的な操作を実現するのも、Web2.0の1つの構成要素なのです。

まとめ

Web2.0の目指す世界に近いサービスをいろいろと実例を交えて紹介しましたが、これはほんの一例に過ぎません。今後、Web2.0のモデルが広まれば、私たちにとっても、そしてサービスの提供側にとっても、便利なサービスが提供されることになるでしょう。

注4：このあたりの方法をAJAXと呼びます。

注5：http://www.utj.co.jp/uni_book/index.asp

注6：日本語でなんと読むんでしょうか、、正解は！！
340 澗 (かん) 2823 溝 (こう) 6692 穂 (じょう) 0938 禾予 (じょう)
4634 垓 (がい) 6337 京 (けい) 4607 兆 (ちょう) 4317 億 (おく)
6821 万 (まん) 1456

第2部：ネットワーク

次世代インターネットの基盤をなす技術はなんと言ってもネットワークでしょう。すでに、日本ではブロードバンドの普及率も上がり、ほとんどの家庭で高速のインターネットを楽しむことができるようになってきました。インターネットで映画を見たり、デジカメで撮った写真をメールで送受信したりすることが気軽にできるようになりました。次世代インターネットではこうした高速ネットワークを基本とし、より生活が便利になるための技術が次々と生み出されています。ということで、第2部は「ネットワーク」です。ここでは少しだけ、その世界をのぞいてみることにしましょう。

IPv6

現在インターネットで使われているIPプロトコルはIPv4であり、32ビットのアドレス空間を持っています。このアドレス空間全てを使ってアドレスを割り振ることができる」とすると「4,294,967,294(約43億)台」の端末を識別することができますが、世界人口約65億(2005年7月現在)の数と比較すると、一人一つのIPアドレスが割り当てられないことになります。

IPv4が制定された1981年頃はこの数で十分と考えられていたのですが、Windows95発売以降インターネットの利用が爆発的に増加したため、IPアドレスの枯渇という問題に直面しています。

IPアドレスを効率的に割り当てるCIDRやNATのアドレス変換技術で、枯渇問題はある程度先延ばしにできていますが、根本的な解決にはなっていません。

そこでIPv6が登場するのです。IPv6は128ビットの広大なアドレス空間を持っています。割り振ることができる端末の台数は、なんと「340,282,366,920,938,463,463,374,607,431,768,211,456台」⁶なんです。これを世界人口65億の一人一人に対して割り振ったとしても一人当たりのIPアドレスの数は天文学的数になり、

ほぼ無限のIPアドレスを使うことができるようになります(もちろん文字通りの無限ではありませんが、滅多なことではアドレスが枯渇するということはないでしょう)。

そうするとネットワーク端末はもとより、ネットワーク対応一般家電や、もし技術的に可能であればわたしたちの身の回りにある、ありとあらゆるものにIPアドレスを振ることが可能なのです。例えば筆者が良く使う蛍光ペンにIPアドレスが振られ、ネットワークにつながっていれば、インクの残りが少ないとアラートで知らせてくれるような仕組みを組み込むことにより、インクの残量をいつでも把握することができます。いざ使おうとしたら書けなかったということとはなくなるでしょう。

またNATによるグローバルIPとプライベートIPのアドレス変換の仕組みが必要なくなり、ダイレクトなP2P通信が可能となります。これによりインターネット本来の双方向通信が実現することになります。

それ以外にもセキュリティや暗号化などもIPv4では別機能で実現されていたことが内蔵されていて、ネットワーク的にはとてもシンプルな通信を行うことができます。

すでに大手通信事業者では自前のネットワークをIPv6へと移行を進め

ています。また、一部のプロバイダも一般向けにIPv6のサービスを提供し始めているのです。

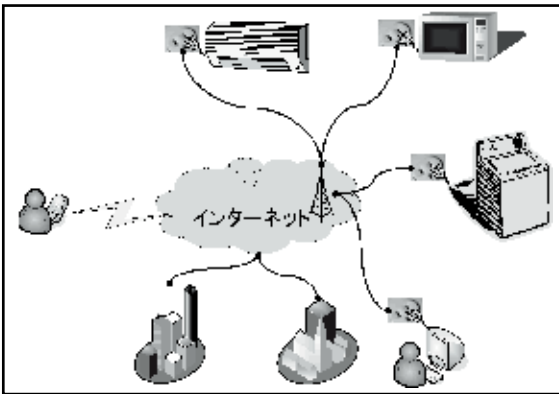
携帯電話やクルマや家電など、ありとあらゆるものにIPアドレスが割り当てられ、ネットワークが当たり前のように私たちの生活になくはならないものとなる時代が、もう、すぐそこまで来ているといえます。

電力線通信

インターネットに接続するためには、通常ADSLや携帯電話・PHSといった方法を使用します。これ、慣れない人には結構複雑です。しかし、次世代はもっと簡単に、便利に接続できるようになるかも知れません。それが電力線通信と呼ばれる(夢のような?)技術です。既に2005年10月4日電力線通信実用化が決まりました。

電力線通信(PLC)は、既設の電線に、電気の周波数50/60Hzよりも高い周波数の信号を乗せて行うデータ通信で、簡単に言うとコンセントにジャックを差し込むだけでインターネット通信ができてしまうという技術です。新しい技術のように思われるでしょうか。いいえ、実はそうではないのです。その昔、家庭用コンセントを利用したインターホンがあったのをご存知でしょうか?それこそが、まさにこの技術の応用なのです。仕組みとし

IPv4のIPアドレス数 : $2^{32} = 4,294,967,296$ 個
IPv6のIPアドレス数 : $2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456$ 個
▲ 図7 : 既存のIPv4とIPv6のIPアドレス数の比較



▲ 図8：電力線通信のもたらす世界（想像）
あらゆる電化製品を簡単にインターネットに！

では、アナログ電話線に高い周波数帯のデータ通信を行う ADSL と似ていると言えるでしょう。

高速電力線通信（高速 PLC）は家庭用の電力線に、電気とは別に周波数 2MHz ~ 30MHz の情報信号を流します。電気のコンセントに PCL モデムという特別なアダプタを接続し、数 Mbps ~ 数百 Mbps のデータ通信が可能になる技術です。コンセントはどこ

の懸念もあるということです。さらに、もう1つはヨーロッパでのテストでのことですが、漏れ電波からパケットの盗聴もできてしまったようです。このように技術面でクリアしなければならない問題が残されているのです。

こうした問題をクリアしようとモデムメーカーは開発を急いでいて、早ければ 2006 年中にも最初のモデムが発売される見通しです⁷。

電力線通信を取り巻く状況は決して楽観視できるものではありません。しかし、近い将来実用化されるとするならば、従来の ADSL や無線 LAN、光ケーブル等既存の通信技術と組み合わせることによって、次世代インターネットの幅をさらに広げてくれる技術となることでしょう！

このように配線工事が不要になるため、インターネット家電の普及の礎と期待できる高速 PCL ですが、いくつかの問題があります。

1 つには、日本の多くの場所で電柱に電線が張り巡らされているが、その電線は、高周波を流すことを想定して設計されていません。そのため、高周波を流すと電線がアンテナの役目をし、電磁波を発生してしまう問題があります（いわゆる漏れ電波と呼ぶそうです）。そして 2 つめにはその周波数帯が短波放送、アマチュア無線、航空無線、防災無線等への影響や家電機器の誤作動

の懸念もあるということです。さらに、もう1つはヨーロッパでのテストでのことですが、漏れ電波からパケットの盗聴もできてしまったようです。このように技術面でクリアしなければならない問題が残されているのです。

IP 電話・インターネット電話

ここ 1,2 年で固定電話サービスの様相が大きく様変わりしているのをご存知でしょうか。従来電話回線というと NTT で契約するしか手段がなかったのですが、携帯電話に始まり今や IP 電話という選択肢が増えました。

ここで IP 電話とインターネット電話サービスの違いを押さえておきたいと思います。厳密な定義は難しいところではありますが、一般的に IP 電話は「IP プロトコルを使用したプロバ

注 7：さて、これが皆様のお手元に届くことには、出ているでしょうか？

注 8：<http://www.skype.com/intl/ja/>
Skype については、p.22 の「Skype を使ってみよう」もご覧ください。

注 9：最近、実験的にお客様との打ち合わせで一部 Skype を使用してみました。音声は、通常の電話と変わりませんし、

会議通話といって、4 人まで同時に会話できる機能もあるので、電話会議の代わりとして十分に役割を果たせています。残念ながらビデオ通話は 1 対 1 でしかできませんが。

注 10：「敵を知り己を知れば百戦危うからず。」孫子の兵法より。

注 11：PA セキュリティセンター

電話はもっと安くなる??

一般電話は交換回線という通信方式で、電話網の切替によって相手と 1 対 1 で通信回線を確立し通話ができます。つまり通話をしている間は回線を占有しているのです。その接続切替を行う機器が交換機であり、この機器は電話網でしか使用しない、非常に高価な専用機器で、回線事業者はこれらの機器の維持費（固定費）に多額の資金を要しているのです。現在、一般電話の利用が携帯電話や IP 電話などの普及で徐々に下がってきて通話料収入が減少してきていますが、機器の固定費は常に一定であり通信事業者の経費を圧迫しているようです。

一方 IP 電話は、各ユーザが回線を共有し通話の音声データを細切れで相手に送るパケット通信方式となっています。パケット通信はルーター等の汎用的なネットワーク機器で構成されるので、交換機に比べて安い固定費で済むのです。そこで現在、各通信事業者は自前の網設備の IP 化を進めており、IP 化が完了すると固定費が今までの 1/10 程度まで削減できるといいます。

そうなれば今後の更なるサービス向上はもとより、通信費がこれまでより安くなるのが期待できるのです。いずれは電話代というものを意識しない時代が来るのではないのでしょうか。

イダや、回線事業者の IP 網を利用した電話サービス」を指し、インターネット電話は「インターネットを通じて行うデータ通信サービスでその一つが音声による電話サービス」を指します。端的に述べると、IP 電話は電話番号を付与されている電話回線で、インターネット電話は主に PC を利用して通話を行うものです。

IP 電話は、いわゆる YahooBB フォンや NTT のフレッツフォンなどのことです。当初、IP 電話は、音声途切れたり、エコーがかかったりしていたようですが、最近ではほとんど一般電話と変わらない品質を得ることができています。また各 ISP でも IP 電話のサービスを提供し一般電話に比べて安い料金で、場合によっては通話料が無料になります。

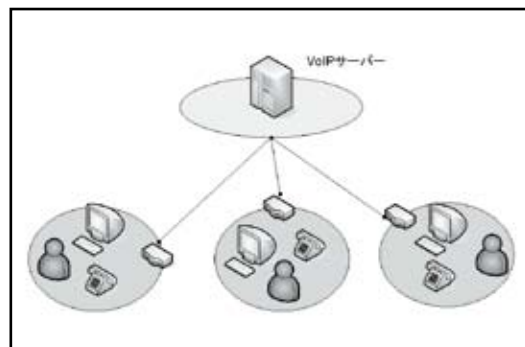
今後 IP 電話に期待されるものとしては、音声サービスに加え TV 電話のような映像サービスや複数の人数で行うことができる TV 会議サービス等が挙げられます。これらは従来の固定電話サービスでも提供されてはいましたが、より低価格で提供することが可能になれば、新たなビジネスチャンスにつながるのではないのでしょうか。

一方、最近注目されているインターネット電話は Skype(スカイプ)⁸です。

すでにご利用になっている方も多いのではないでしょうか。

Skype は Skype Technologies 社が開発・公開している、P2P 技術を応用した無料音声通話アプリケーションで、ユーザー同士の通話は世界中どこでも無料でできます。また SkypeOut という有料オプションで一般電話回線に発信が可能で SkypeIn で(同じく有料オプション)一般電話回線からの着信が可能になります(SkypeIn は日本では認可されていない)。

Skype の優れているところはその音質です。Skype はインターネット電話でありながら、その音質は一般電話と引けを取らないほど高いのです⁹。普通このようなサービスは送信側、受信側を管理する、サーバーを必要としますが、Skype はそのような管理サーバーは存在しません。その代わり P2P 技術を使い、各ユーザー PC がネットワーク全体を見ながら自分自身がサーバーに切り替わったりすることを自動的に行うことにより、負荷分散を図り、安定した回線品質をキープしつつ 100 万人の同時利用にも耐えることができるようになってきました。また、最近公開された新しいバージョンの



▲ 図 9 : IP 電話の概略図

Skype ではビデオを併用した会話も可能となり、既存のテレビ電話などにも迫るなど、ますますその活躍の場を広げてきているのです。

このような高品質な通話が可能になったのはアプリケーションの作りによるところも大きいのですが、なんと言ってもネットワークインフラの整備、PC の性能アップなど、さまざまな技術の仕様化等が関係しているといえるでしょう。そうした意味からもこの Skype は Web2.0 の一つと言えるのではないのでしょうか。

そして今後は家庭やオフィスの通信基幹サービスとして需要が高まり、また無線 LAN と融合するならばユビキタス社会における重要なデバイスとしてその確固たる地位を築くものと期待できるのです。

第 3 部 : セキュリティ

年々、いえ、日々ネットワークの環境整備が進み、私たちの生活は非常に便利になってきています。第 2 部で紹介しましたが、IP 電話の普及に伴い、海外や国内の遠方にいる知人・友人とも、電話代を気にせず気軽に話せるようになったのも、ネットワークの整備がもたらした恩恵の 1 つの例と言えます。しかし、便利になった反面、注意しなければならない点も多くなっています。昨今、紙面をにぎわしているコンピュータウイルス (以下、ウイルス) 等に代表されるネットワークセキュリティです。便利になればなるほど危険にさらされる度合いも高くなっており、セキュリティも、複雑かつ確実性が求められるようになってきています。便利なネットワーク社会になってきた昨今のセキュリティ事情とその将来を俯瞰してみましよう。

ウイルス

セキュリティ対策を知る前に、まずは敵を知らなければなりません¹⁰。ほぼ毎日のようにウイルスに関する話題

が、ニュースサイトをにぎわしています。例えば、以下に IPA¹¹ が統計を取っている 2005 年 11 月のウイルス検知数のグラフを引用しました。

なんと、たった 1 ヶ月の間に、500 万個以上のウイルスが検出されているのです。皆さんも毎日受け取るメールの中に、時々ウイルス付きのものが混

ざっていることはないでしょうか？そのように、私たちの身の周りでは、ネットにつながり便利にはなりましたが、その分、多くの脅威にさらされるようになったのです。

さて、ウイルスにはどのような種類のものがあるのでしょうか。サーバーに感染させるタイプのもの（SlammerやCode Redなど）、メールやWebページから一般ユーザに感染させるタイプのもの（NetSkyやMYDOOMなど）などが存在します。これらはすでに有名になったウイルスなので、皆さんも対策を講じられていることでしょう。ここまでのウイルスは単にネットワークの混乱を狙ったものや、作者が自分の技術力を誇示するための道具として利用されたり、ウイルス作者同士の技術の見せ合い、などの類でした。

最近はこのウイルス事情に変化が生じています。2005年で、最も被害が多かったウイルスは何かご存知ですか？以下に、トレンドマイクロ社¹²の集計した表を掲載します。

第一位はRBOTと呼ばれるウイルスです。これは、今までの面白半分のウイルスとは性格を異にしています。それは、金銭や情報詐取の手段・道具としての性格を帯びたウイルスである、という点です。今までは、ネットワークが遅くなる、PCが遅くなる、周りに撒き散らす程度¹³の被害で済みましたが、それでは済まなくなっています。

BOTと総称されるこのウイルスはファイル共有アプリケーションやP2Pアプリケーションなどを通じて感染し、PC内の情報を漏洩させたり、特定のサーバーに対して攻撃を仕掛けたりするなど、明確な目的を持っています。昨年も、個人情報が流出したといったニュースや、プライベートな写真が流出するなどの被害が相次いだことは記憶に新しいでしょう。これは他人事ではありません。オン

ラインバンキングを利用してれば、そのログイン情報が盗まれてしまうかも知れません。カードを使用して買い物をされていますか？カード情報も簡単に盗まれてしまうかも知れません。BOTと呼ばれるウイルスはそのような情報を盗んだり明らかな被害が出ているのです。

このように、ウイルスは、確実に悪意を増し、より巧妙に入り込んでくるようになっています。インターネットによって便利になっていますが、危険度はますます増しているといえます。

では、ネットワーク社会にあって、ウイルスを完全に防ぐ良い方法はあるのでしょうか？筆者は、結局は個々の意識がもっとも重要だと考えます¹⁴。どんなに良いセキュリティの製品を使ったところで、使っているユーザの意識が低ければ完全には防げないものなのです。セキュリティの警告が出たら、すぐにパッチを当てる、ウイルス対策ソフトを常に最新の状態に保つ、などの対策が重要になるでしょう。

量子コンピュータ

さて、インターネットの世界で身近なセキュリティと言えば何でしょうか？SSL¹⁵に代表される暗号化技術ではないでしょうか。オンラインショッピングで買い物するとき、カード情報や個人情報を入力するページは大抵SSLによって暗号化されています。それらのページでは「安全・安心」に買い物ができるとうたっています。

現時点ではこれ自体に誤りはないのですが、将来的にはこうした暗号化技術が根底から覆るかもしれない、つまり今の暗号化技術はまったく安全ではなくなる、といったら皆さんは驚かれるでしょうか？

脅しから入ってしまいましたが、今注目を集めている次世代コンピュータとして「量子コンピュータ」というも

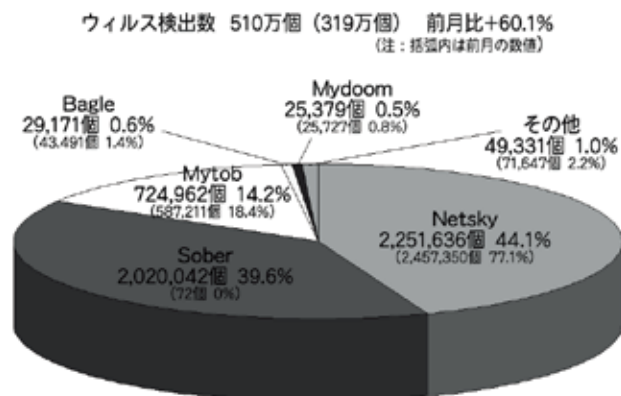
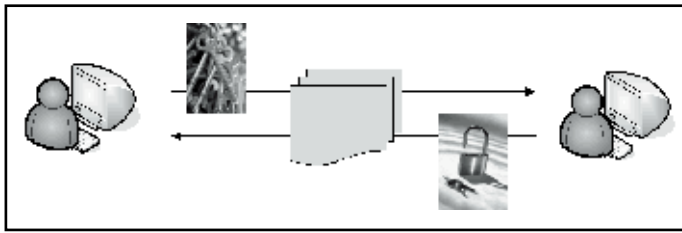


図10：IPAが集計したウイルス検出数（2005年11月）

ウイルス感染被害年間レポート 2005年度（2005/1/1～12/15トレンドマイクロ調べ）

順位	ウイルス名	通称	ウイルスの種類	被害件数	発見時期
1	WORM_RBOT	アールロボット	ワーム型	1180件	2004/3
2	JAVA_BYTEVER	バイトバー	その他	1046件	2003/5
3	TROJ_AGENT	エージェント	トロイの木馬型	915件	2003/8
4	WORM_SDBOT	エステーロボット	ワーム型	827件	2003/10
5	TROJ_SMALL	スモール	トロイの木馬型	803件	—
6	SPYW_GATOR	ゲーター	スパイウェア	705件	2003/10
7	WORM_NETSKY	ネットスカイ	ワーム型	629件	2004/2
8	WORM_AGOBOT	アゴロボット	ワーム型	532件	2002/11
9	TROJ_ISTBAR	イストバー	トロイの木馬	382件	2003/10
10	VBS_REDLOF	レッドロフ	VBScript型	372件	2003/10

表1トレンドマイクロ社による2005年、ウイルス感染被害レポート



▲ 図 12 暗号化によって安全に買い物ができる

のが存在します。この「量子コンピュータ」が実現すると、今のコンピュータの世界は一新され、特に暗号化技術には革新的な変化をもたらします。

量子コンピュータに触れる前に、なぜ量子コンピュータが暗号化技術を根底から覆すのかをご説明しましょう。いま一般的になっている暗号化技術は RSA というものです。これは端的に言ってしまうと、「素因数分解」¹⁶ を利用した暗号化技術です。大きな数の素因数分解を解くには、たとえコンピュータで計算したとしても、とてつもなく時間がかかり、簡単には解くことはできない、という理論の上に成り立っています。

たとえば、RSA 暗号技術を開発したメンバーの 1 人の言葉を借りると、

▼ 125 桁の数を因数分解するのに 4 京 (40,000 兆) 年かかるだろう ▲

ということです¹⁷。これはとても現実的な時間内に解けるとは思えないですね。つまり大きな桁数の数で暗号化していれば、現在の技術ではそう簡単にやぶれるものではないのです。

しかし、量子コンピュータが実用化されれば「4 京年かかる」といわれる素因数分解もわずか数秒で解いてしまう技術なのです。そうなると、おのずと RSA 暗号化が根底から覆ることになるのです。

量子力学的な重ね合わせを利用した「Shor の因数分解アルゴリズム」というもので、これを用いれば天文学的な時間の掛かる因数分解が簡単に解ける

ようになってしまふのです。

しかし、このような量子コンピュータにも問題はあります。

実際に量子コンピュータを作る

のは非常に難しいという点です。量子コンピュータの動作原理などは確立されていますが、実際に作るには多くの難問が待ち構えているのです¹⁸。

1 つには理論の根底になっている「重ね合わせ」状態で計算を行うためには非常にデリケートな環境が必要で、とてつもなく費用の掛かるような実験施設でないとこの環境を実現できないことが挙げられます。次に「qubit

集積化」という理論を用いるのですが、これを実現するための技術が今のところ見つかっていない、という点です。

このように、暗号化を根底から覆すといわれている量子コンピュータですが、その実現実用化にはまだまだ時間の掛かる夢の? 技術かもしれません。しかし、日進月歩のコンピュータの世界です。そう遠くない将来にはこうした技術が現実のものとなるかも知れません。そのときには、暗号化技術が破られるだけでなく、むしろそれによって良い効果、つまり今よりもっと快適な IT 生活を送れるようになっているのかも知れません。

記事協力：長田 光弘
背番号 25

注 12： <http://www.ipa.go.jp/security/>

注 13：「程度」って、やや表現は悪いんですが。

注 14： と、言ってしまうと、実も蓋もないんですが

注 15：「https」で始まるホームページなんかがそうですね。

注 16： ある正の整数を素数の積の形で表す方法のこと。懐かしいですね。

注 17： コラムもあわせてご覧ください。

注 18： <http://www.brl.ntt.co.jp/J/research/qe/qe.html>

注 19： 実際には、174 桁 (576 ビット) までは 2003 年に解かれてしまっていますが、まだまだ現実的な時間内には終わる処理で無いようです。

量子コンピューティングでなくても、RSA は破れる？

本文の中で「125 桁の数を因数分解するのに 4 京 (40,000 兆) 年かかるだろう」という言葉を紹介しましたが、実はすでにこの前提は崩れています。1994 年に 1600 台ほどのコンピュータを使用して、125 桁の数字の素因数分解に成功しているのです。

<http://www.math.okstate.edu/~wrightd/numthry/rsa129.html>

RSA の技術 が考案されたのが 1977 年ですから、それから 20 年もすれば、コンピュータの処理速度も考えられないほどに向上したため、このような結果になってしまったのです。もちろん今では、125 桁の暗号化ではなく一般的には 160 桁以上 (512 ビット) の暗号化が用いられており、これは今でも現実的な時間で解くことはできないものです¹⁹。

しかし、わずか 20 年足らずで、4 京年かかっても解けないといわれたものを解くことができたのです。コンピュータの処理速度は日進月歩ですし、数学的なアルゴリズムもどんどん見つかり、そういう意味で、量子コンピュータが実用に至らなくても、RSA 暗号化が役に立たなくなるのかもしれないですね。