

砂原秀樹 + 菊地宏明 + 編集部

【アドバイザー】砂原秀樹
奈良先端科学技術大学院大学
情報科学センター助教授
WIDE プロジェクト・ボードメンバー

インターネットの



に答える



このコーナーでは、皆さんから寄せられたインターネットに関する質問や疑問にお答えします。分からないことや疑問はどんなことでもけっこうですので、編集部までお寄せください。メールアドレスは ip-faq@impress.co.jp です。なお、質問へのメールでの回答はできませんのでご了承ください。

今月のヘッドライン

- 1 ホームページにある画像の保存法
- 2 インターネット上での暗号の仕組み
- 3 「オフ会」ってなに？

Q

友人が、一緒に行った旅行の写真を「ホームページにアップしたのでそこから持ってって！」と言っていました。どうやって保存するのか分かりません。こんなことは恥ずかしくて友人にも聞けないので、どうか教えてください。(T.Aさん)

A

デジタルカメラなどで撮影したデジタル画像は、写真と違って焼き増しなどの手間がかかりません。さらに、インターネットを使えば遠く離れた場所にいる人同士でも、手軽に画像のやり取りができるので配布も簡単です。

現在、一般的なWWWブラウザには、ブラウザに表示されている画像を保存する機能がありますので、この機能を使えば

（ ホームページにある画像の保存法 ）

ブラウザ上の画像を取り込むことができます。

ウィンドウズ95の場合、インターネットエクスプローラやネットスケープナビゲーターで表示したWWWページの画像の保存は、マウスの右クリックを使うと簡単に行えます。保存したい画像の上にマウスカーソルを合わせ、右クリックで表示されるメニューから「名前を付けて画像を保存」を選択します。そして、画像を保存するディレクトリを指定すれば、画像の取り込みは完了です。

マッキントッシュの場合、ネットスケープナビゲーターで保存したい画像をクリ

ックするとメニューが現れますので「画像をコピー」を選択すればOKです。また、画像の上にマウスカーソルを合わせて、保存したい場所へドラッグ&ドロップしても取り込むことができます。

デジタル画像はホームページでやり取りするだけでなく、電子メールに添付して送受信することもできますが、その際は添付する画像の大きさにも注意する必要があります。ビットマップ形式などの大きなデータはネットワークに負荷をかけるので、インターネットでの送受信は控えたほうがいいでしょう。

(編集部)

Q

鍵を利用したインターネットの暗号化技術とはどんなものですか？送信者と受信者にしか解読できないとありますが、本当に可能なのか不思議でなりません。受信者が解凍できるなら、途中で情報をキャッチした者でも解凍できるのではないかと思います。鍵の技術について具体的に教えてください。また、送信者と受信者がどうして同じ鍵を使用できるのかも知りたいです。(飯山康彦さん)

A

暗号の話は、前回の圧縮の話と同様に「数学」が鍵の技術です。現在利用されている複雑な暗号技術の話をするに1冊の本が書けるくらいですから、ここではその概要を簡単に説明したいと思います。

暗号の技術の基本的な仕組みは、文字の置き替えです。例えば、ある数字列を暗号に変換する場合を考えてみましょう。このとき、図に示すような表を用いて、元の数字列をa~jで示される文字列に変換す

号化の際に用いられる変換を示す関数なのですが、ここでの例の場合には、暗号表を使った暗号化の手順を示す関数となります。そして、「k」は暗号化の際に用いられるパラメーターで、ここではどの暗号表を使っているかを示すパラメーターとなります。全部で360万以上の暗号表が存在しますが、それらに番号を与え、何番の暗号表を使うかを示しているのが「k」であると考えてもいいでしょう。

実は、この「k」が通常「鍵」と呼ばれるものなのです。つまり、どういうルールに基づいて変換されているかを知っていたとしても(暗号表を用いていること)その際にどのパラメータ(鍵)を用いたかが分からなければ、元の情報に戻すことができないというのが暗号の仕組みなのです。したがって、パラメーターの種類が多ければ多いほど強力な暗号ということになります。実際のインターネットでは、暗号表とは比べものにならないくらい複雑な変換ルールを用いています。そのため鍵の種類も多くなり、非常に強力な暗号となっているのです。

さて、こうなってくるとどうやって送信者は受信者に使っている「鍵」を伝えるかということになります。暗号化された情報と鍵の両方が盗まれてしまうことがあると、どんな暗号でも解読されてしまうことになりますから、「鍵」の取り扱いには非常に慎重に行わなければなりません。これについては次回に説明したいと思います。(砂原秀樹)

インターネット上での暗号の仕組み

るわけです。これを用いることで、数字は

12345	difbj
3000	feee
52973	jihgf
427	big
3001	feed

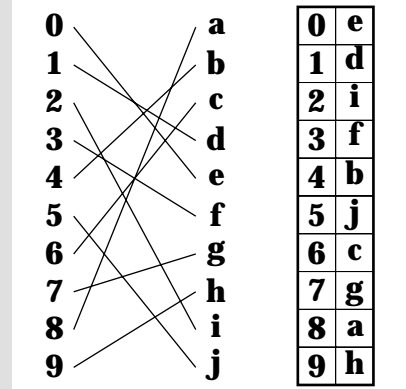
のように文字列に変換されます。ここで重要なことは、変換された文字列を元の数字列に戻すためには、図の暗号表がなければなりません。つまり、変換された文字列がネットワーク中を流れている途中で第三者に盗まれたとしても、その第三者が暗号表を持っていないければ元の数字列に戻すことができないことになります。

0~9の数字からa~jの文字への対応は、全部で3628800(=10!)通りの場合がありますから、暗号表は3628800通りのものがあるわけです。この中から利用されている暗号表を見つけ出してくるのは大変だということがわかるでしょう。

暗号の技術は、意味のある情報(ここでは数字列)をある規則(ここでは図の暗号表)に従って変換することによって、一見無意味な情報(ここでは文字列)とすることで成り立っています。これを数学的に表現すると、

$$y=f(x,k)$$

となります。「x」は元の情報、「y」は暗号化された情報です。ここで「f」は、暗



暗号表

WWW ブラウザ上の画像の取り込みかた



ウィンドウズの場合(画面はインターネットエクスプローラ)。画像の上で右クリックすればメニューが表示され、画像を壁紙にすることもできる。



マッキントッシュの場合(画面はネットスケープナビゲーター)。画像をクリックするとメニューが表示される。また、保存したい位置に画像をドラッグ&ドロップしてもコピーできる。

Q

「オフ会」ってなんですか？「～会」というからには、何かの集まりだと思うのですが...。「オフ」って「OFF」のことだと思うのですが、「オフ会」では、いったい、どんな人たちがどのようなことをしているのですか？ また、私のような初心者でも参加できるのでしょうか？ また、「オフ会」における礼儀作法みたいなものはあるのでしょうか？（小西さん）

A

ネットワークや通信では、しばしばオン、オフという言葉を使います。「オンライン」は、「ネットワークにつながった...」という意味です。ですから、ダイヤルアップIP接続を使って、インターネットにアクセス可能な状態を「オンライン状態」といいます。オフラインはネットワークにつながっていないことですから、モデムやパソコンの電源を切ったとき、電話回線が混みあってつながらないときは、オフライン状態といえます。

オフ会（オフラインミーティングとも言います）の「会」は、会議のことです。オフが「ネットワークにつながっていない...」という意味ですから、ネットワークを使わないで会議をすること、すなわち実際に会って会議をしようというものです。取り立てて議題がなければ、集まって話そう、遊ぼう、飲もうということと同じです。オフ会があれば、オン会もあります。オン会については、普通はオン会とは略さずにオンライン会議といいます。メンバーへ告知した時刻にネットワーク上で会議を開くことです。多くはテキストを使ったチャットですが、グラフィックインターフェイスを備え

たチャットソフトも出ています。テキストベースでは、IRCソフトやWWWを使ったものが、グラフィックベースのチャットでは、ウィンドウズ用のWorlds Chat/J2 (<http://www.globewarp.or.jp/index.htm>) やマッキントッシュ用のThePalace (<http://www.nihon.net/palace/palace/>) が有名です。また、最近では、インターネット電話ソフトやネットミーティングを使った音声でのチャット、Enhanced CU-SeeMeなどを使った音声と画像をともなったチャットもあります。

オフ会は連日チャットで盛り上がった話題に花を咲かせたり、新しい友人関係を築いたり楽しいものです。チャットの場合オフ会の告知があったら、ぜひ参加してみてください。

まず、告知された方法で参加意志を表明します。会場の用意や、日程の調整を行うために、主催者は、事前に参加者数を把握しなければなりません。当日いきなり会場へ行くと迷惑をかけることがありますので、注意しましょう。オフ会が近づいたら、日程や会場の変更、中止がないかを確認しましょう。前日に変更になる場合もあります。唯一の連絡手段はチャットの場合であることも考えると、家を出る前にも確認しておきたいものです。

オフ会に行けば、それまでは文字を通してしか知らなかった相手に直接会えることでしょう。そこではまず自己紹介から始めます。ネットワーク上で発揮される個性と実際に会った感じにギャップがあるかもしれません。いつもはギクシャクする相手も、けっこう気のいい人だったりします。気をつけたいのは必要以上に詮索をしないこと



オフ会の告知メール。このようなイベントは、興味があったら積極的に参加してみよう！

です。肩書きを忘れてチャットを楽しむ人は、オフ会でも肩書きをはずしたいと思っています。自分から話すのを待ちましょう。

さらに嫌われる行動は、こっそり会場へ行って、ひそかにオフ会を観察する行為です。このストーカーの行為を嫌って、オフ会参加受け付け後に、参加者だけに限って電子メールでオフ会の連絡をとることもあるくらいです。

このような一般的なマナーに気をつけてさえいれば、あとはオフ会だからといって心配することはないでしょう。いつもの仲間ですから、大いに楽しみましょう。同じ趣味の人たちですから話題も尽きません。夜通し話していることだってあります。ですから、少しだけ周りに気を使ってください。会場となる場所の他の人々に迷惑をかけないようにします。

最後の注意は、オフ会での内容をむやみに公表しないことです。あなたを信頼してくれたから話してくれた内容もあるはずで、それは公表してもよい内容とは限りません。公表したいと思ったならば、関係する人々に許可をもらわないといけません。（菊地宏明）

「オフ会」ってなに？



[インターネットマガジン バックナンバーアーカイブ] ご利用上の注意

このPDFファイルは、株式会社インプレスR&D(株式会社インプレスから分割)が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

<http://i.impressRD.jp/bn>

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容(技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど)は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者(執筆者、写真の撮影者、イラストの作成者、編集部など)が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元(株式会社インプレス R&D)、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D(当時は株式会社インプレス)と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接のおよび間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先

株式会社インプレスR&D

All-in-One INTERNET magazine 編集部

im-info@impress.co.jp