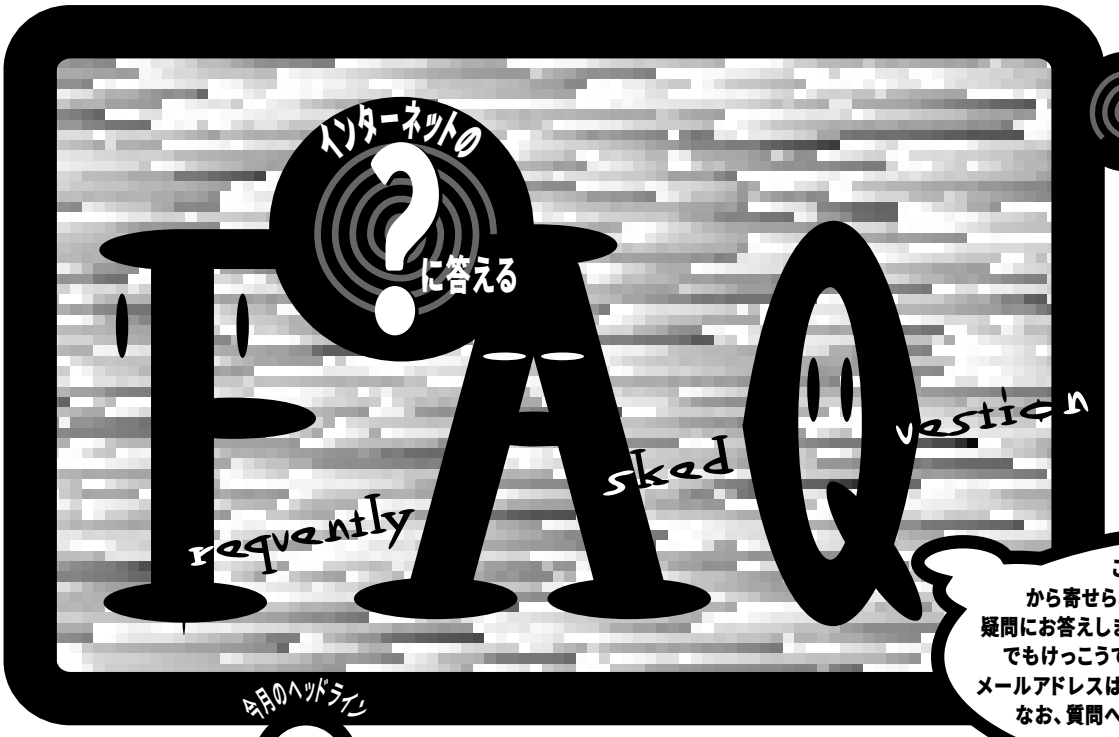


今月の回答者

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

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. プロバイダーには種類があるの？
2. ハードディスクにたまる「ゴミ」について
3. インターネットでの鍵の交換の仕組み

プロバイダーには種類があるの？

Q インターネットマガジンのプロバイダー一覧表の中に「通信事業者の種別」という項目がありますが、「一般第２種」とか「特別第２種」とか「1種」っていったい何がどう違うんですか？ やっぱり2種よりは1種のほうがいいのですかね。プロバイダーにも日本酒みたいな等級があるんですか？

（北九州市 山口敏也さん）

A お酒の等級はそのお酒の品質によって分類されていますが、プロバイダーの分類は必ずしも品質によるものではなく、言うなればそのプロバイダーの事業形態や規模による分類です。

電気通信事業法上では、インターネットサービスプロバイダーは電気通信事業者としていくつかに分類されています。まず、回線設備を自社で保有する会社を「第1種電気通信事業者」といいます。この中にはNTTやDDIや日本高速通信株式会社などがあります。また、第1種電気通信事業者が持つ回線を再販売したり（リセーラー）、その回線を使ったデータ通信サービスを行う会社を「第2種電気通信事業者」といいます。この第2種電気通信事業者には「特別第2種電気通信事業者」と「一般第2種電気通信事業者」の2種類があり、特別第2種電気通信事業者は大規模業者または国際間接続を行う業者をいい、一般第2種電気通信事業者は小規模または特定者向けのサービスを提供する事業者を指します。また、特別第2種電気通信事業は郵政大臣の登録制であるのに対し、一般第2種電気通信事業は郵政大臣への届け出制という点も異なります。

私たちがプロバイダーを選ぶ際、この分類はあまり重要なことではありません。確かに大きな会社だからという安心にはなるので、それも1つの目安かもしれませんが、それよりはサービス料金（定額制か従量制か）やアクセスポイントの場所、ホームページを持つには追加料金が必要なのか、その容量は何Mバイトなのか、などといったサービス内容で選んだほうがいいのではないでしょうか。（編集部）

ハードディスクにたまる「ゴミ」について

Q インターネットを使ったり、アプリケーションをいろいろと使ったりしていると、パソコンのハードディスクに「ゴミ」がたまります。「キャッシュ」は捨てていいと人から聞いたのですが、どこにあるのか分かりません。そのほかに「TEMP」フォルダーなども、いつのまにか中身が増えています。ハードディスクの「お掃除」をする際に、捨てていいものを教えてください。（佃さん）

A WWWブラウザーを使っていると「キャッシュ」ファイルが多く作られます。「キャッシュ」とは、インターネットからダウンロードしたデータを一時的にハードディスク上に保存することで、そのページにアクセスするたびに同じデータを繰り返しダウンロードしないでも参照できるようにするものです。キャッシュによって表示速度を改善することができますが、ハードディスクにファイルを作成するために、空き容量の少ないときにはハードディスク容量を圧迫してしまうこともあって不便です。

そのため、ブラウザーではどのタイミングでキャッシュファイルを更新するか、作成したキャッシュファイルをいつ削除するか、保存に利用可能なサイズの上限などを指定することができます。

ウィンドウズ版のインターネットエクスプローラ3.0では、「表示」メニュー→「オプション」→「詳細設定」タグ→「インターネット一時ファイルの設定」ボタンのクリックで現れる設定ウィンドウの現在のフォルダーにキャッシュファイルを保存するフォルダーが設定されています。隣にある「ファイルの削除」ボタンでキャッシュファイルを削除することができますが、その後もWWWブラウザーを使っていると次第に増えていきます。そこで、キャッシュファイルの保存数を抑えるために、同じ設定ウィンドウの「使用するディスク領域」項目で制限するといいでしょう。ネットスケープにもネットワーク設定に同様の項目があります。

もちろん、マッキントッシュ版のインターネットエクスプローラやネットスケープの初期設定項目にもありますから、探してみてください。

そのほかに、「Windows」フォルダーにある「Temp」フォルダーにも多くのゴミファイルがたまります。アプリケーションなどの動作中に一時的にデータをファイル保存したテンポラリーファイルを保存するフォルダーで、ほとんどの場合はアプリケーションの終了とともにファイルは削除されます。しかし、エラー終了した場合や意図的に中断させた場合にテンポラリーファイルが削除されずに残ってしまうことがあり、ほうっておくと数十Mバイトにふくれあがっていくこともあります。そんな場合には、動いているアプリケーションを終了させ、エクスプローラなどで「Temp」フォルダーのいらないファイルを削除していきましょう。ファイルのプロパティを見れば作成日や更新日が確認できるので、長い間更新されてないファイルは区別がつきます。

ディスク容量がないときに忘れているポイントがもう1つ。アプリケーションやOSがプレインストールされているパソコンのハードディスクには、再インストールを行うためのオリジナルのイメージが収録されていることが多くあります。マニュアルなどを参照し、正しくバックアップをとった後に削除すると空き容量が数十Mバイト増加するかもしれません。バックアップをとったのですから、さらに使わない不要なアプリケーションも削除してはいかがでしょうか。最後にスキャンディスクで、破損して利用できないにもかかわらず、ハードディスクに残っているファイルを削除しましょう。

マッキントッシュの場合も同様です。キャッシュフォルダーの整理、プレインストールソフトのバックアップ後に行う不要アプリケーションの削除、「ノートンディスクユーティリティ」などのユーティリティーソフトを使って破損した利用不可能のファイルを検索して削除するとよいでしょう。

さらに、ディスクが空いてきたら、最後にフラグメンテーションを解消しておくとディスクアクセスが高速になります。フラグメンテーションとは、ファイルがまとめて書き込めず、散り散りに分散されて配置されている状態のことで、これによりアクセス速度が低下する症状を起こします。これは、空き容量が増えただけでは解消しないので、ウィンドウズではシステムツールの「デフラグ」を、マックではノートンディスクユーティリティなどのアプリケーションを使うと解決することができます。

（菊地宏明）

▲ウィンドウズ版インターネットエクスプローラでのテンポラリーファイルの設定画面。ハードディスクの空き容量に合わせて、使用するディスクの領域を設定できる。

▲マッキントッシュ版ネットスケープナビゲーターにおけるキャッシュ容量の設定画面。キャッシュフォルダーの容量や場所が設定できる。

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。受信者が解読できるなら、途中で情報をキャッチした者でも解読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）

インターネットでの鍵の交換の仕組み

A 前回は、暗号の仕組みについて簡単に紹介をしました。ここでは「鍵」と呼ばれる秘密の情報を用いて、元の情報を「一見」意味のない情報に変換（暗号化）してネットワークに流すということで、情報を当事者同士以外の第三者から分からないように保護しているわけです。受け手側では「鍵」をもとに情報を復元（復号）することで、発信者からの情報を正しく受信することができるわけです。

さて、ここで問題となるのが「鍵」と呼ばれる秘密の情報を送信者と受信者で共有しなければならないことです。秘密の情報ですからネットワークに安易に流すことはできません。かといって、暗号化して送ろうにも、送った情報を復号するための「鍵」が相手にないのですから、どうしようもありません。

そこで、通常「鍵」はネットワークを通じて相手に届けるのではなく、たとえば郵便や電話などを利用して別の手段で届けるという方法が利用されてきました。しかし、これだけネットワークでの通信が多くなると、ネットワークを通じて鍵を配布する手段が不可欠になってきます。そこで考え出された方法が公開鍵暗号と呼ばれる暗号の仕組みです。

公開鍵暗号の仕組みを理解するためには、数学の知識が不可欠なのですが、このコーナーに用意された場所だけでは到底説明することは困難なので、ここではその概念だけを理解していただきたいと思います。

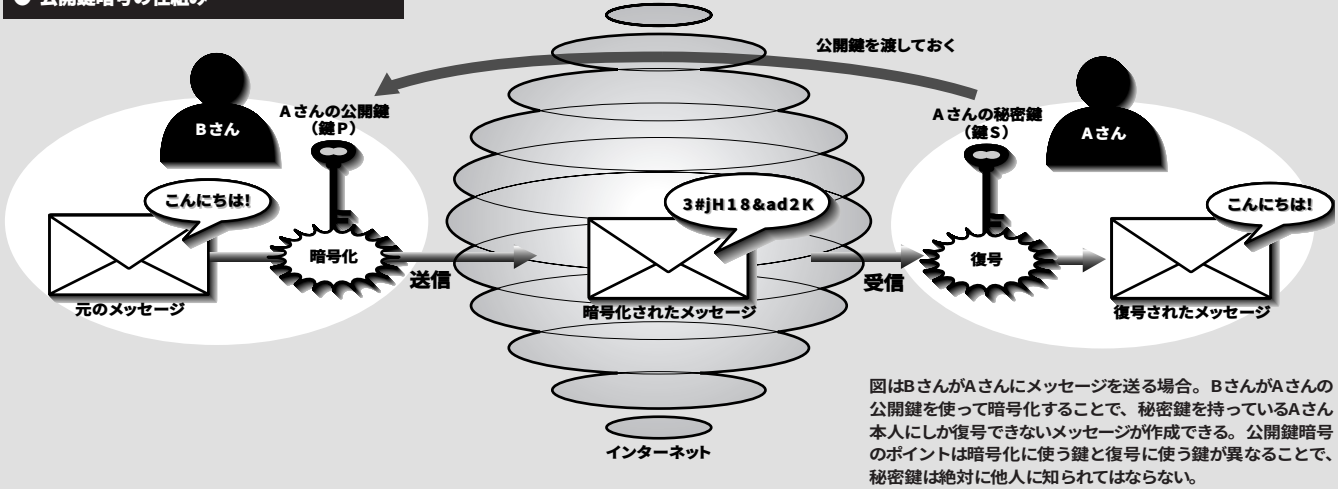
従来の暗号方式では、暗号化と復号の際に用いられる「鍵」は同じものが用いられていました。そのためにこの「鍵」を安全に相手に伝えることが必要だったわけです。このような暗号方式を一般に慣用系暗号と呼びます。

これに対して、暗号化の際に用いる「鍵」と復号の際に用いる「鍵」として別のものを用意することができる暗号方式が考え出されました。つまり、暗号化する際には「P」という鍵を用いて暗号化するのですが、復号の処理は「S」という別の鍵でなければ行うことができないという暗号方式であるわけです。これが公開鍵暗号です。

この方式では、鍵「P」を知っていても復号することができないわけですから、ネットワークを通じて鍵「P」を配布することができるようになるのです。鍵「S」が分からない限り情報を復号できないわけですから、鍵「P」が第三者に盗まれても困らないというわけです。ここで、鍵「P」を公開鍵、鍵「S」を秘密鍵と呼びます。

現在インターネットで利用されているDESやFEALと呼ばれる暗号は、共通の鍵を用いる慣用系暗号、RSA暗号や楕円暗号は公開鍵暗号に属しています。一般に、公開鍵暗号の方が慣用系暗号に比べて処理時間がかかります。そのためインターネットにおいては、公開鍵暗号を用いて慣用系暗号の共通鍵を配布し、実際の通信では慣用系暗号を用いるということが行われています。（砂原秀樹）

● 公開鍵暗号の仕組み



図はBさんがAさんにメッセージを送る場合。Bさんが Aさんの公開鍵を使って暗号化することで、秘密鍵を持っているAさん本人にしか復号できないメッセージが作成できる。公開鍵暗号のポイントは暗号化に使う鍵と復号に使う鍵が異なることで、秘密鍵は絶対に他人に知られてはならない。

［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的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