入門者のための FAQ

Frequently Asked Question

このコーナーでは、みな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ついてお答えしていきます。日頃からわからないなあと思っている疑問、困っていることなどありましたらどんなことでもけっこうですから質問を編集部までお寄せください。宛先は ip-faq@impress.co.jp です。電子メールでの回答はできませんのでご了承ください。

先日、ある洋雑誌の出版社から電子メールで購読継続の催促がきたのですが、「返信は電子メールでもよい。我々はPGPで暗号化されたメールを受け付けます。公開鍵（public key）は下記の通り・・・」とありました。PGPとは何だと思い、調べた結果、PGPとはPretty Good Privacyの略であること、マッキントッシュ用にはMac PGPというのがあることはわかったのですが（ダウンロードさせてもらいました）、しくみと使い方がわかりません。この辺りをやさしく教えてください。

（長谷川恵司さん）

A. PGPは、Pretty Good Privacyという名前からすぐに想像できませんが、暗号化電子メールの1つの方式なのです。実は、インターネットの世界には、PEM（Privacy Enhanced Mail）と呼ばれる暗号化電子メール方式があり、双方が争っている（?）状況なのです。

電子メールでは、セキリティ上の問題として、

❶ 内容の盗聴
❷ 内容の改竄
❸ なりすまし
❹ 不要なメールの発信

の4つが考えられています。「盗聴」は、電子メールが配送される途中の経路で情報を盗み読むこと、「改竄」は途中で電子メールの内容を変更してしまうこと、「なりすまし」は他人のふりをして電子メールの発信を行うことです。また、4番目の問題は巨大なメールや意味のないメールを相手に送りつけて、相手のスプールディレクトリ（配送されてきた電子メールが保存されるディスク）をパンクさせて、本来必要な電子メールを受けとることができないようにしてしまういやがらせです（ディスクが溢れないまでも、無駄なメールの整理に忙殺されるのはいやですよね）。

PGPやPEMというシステムでは、こうした問題のうち1～3を解決するために用意されました。残念ながら、4の問題については今のところ有効な解決手段はないようです。

さて、PGPでは、こうした問題を解決するために、メッセージの内容を暗号化して送るという方法を採用しています。そして、この暗号化のアルゴリズムとしてRSA（開発者の名前の頭文字から付けられた）と呼ばれるものを採用しています。このRSAは公開鍵暗号と呼ばれており、公開鍵と秘密鍵と呼ばれる2つの鍵を利用して暗号化と復号化の手続きを行います。通常の暗号（共有鍵暗号や慣用暗号と呼ばれる）では、図1に示すように、ある鍵でテキストの暗号化を行い、それを元のテキストに戻す（復号化）には同じ鍵を利用するようになっています。これに対して公開鍵暗号では、図2に示すようにテキストの暗号化には公開鍵を用いて処理を行い、復号化には秘密鍵と呼ばれる別の鍵を利用するのです。つまり、暗号化と復号化には別の鍵を利用するところがポイントです。

たとえば、AさんがBさんにメッセージを送る場合を考えてみましょう。このとき、Bさんはあらかじめ A さんに公開鍵を渡しておきます。そして、AさんはBさんに送るメッセージをBさんの公開鍵で暗号化してメッセージを発信するのです。そのメッセージを受けとったBさんは自分の秘密鍵を利用して復号化を行えばよいわけです。このとき公開鍵は、メッセージの暗号化のためだけにしか利用できないことに注意してください。

つまり、Bさんの公開鍵を世界中の人が知っていても、Bさん宛の暗号メッセージを解読することはできないわけです。

以上がPGPの基本的なしくみです。実際には、複数の相手にメッセージを発信する場合の処理や、「署名」といってメッセ

回答者●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
電気通信大学情報工学科助教授（併任）
WIDEプロジェクト・ボードメンバー。
日本でのインターネット普及のために
研究と後輩の指導に努めている。

図1 共有鍵暗号

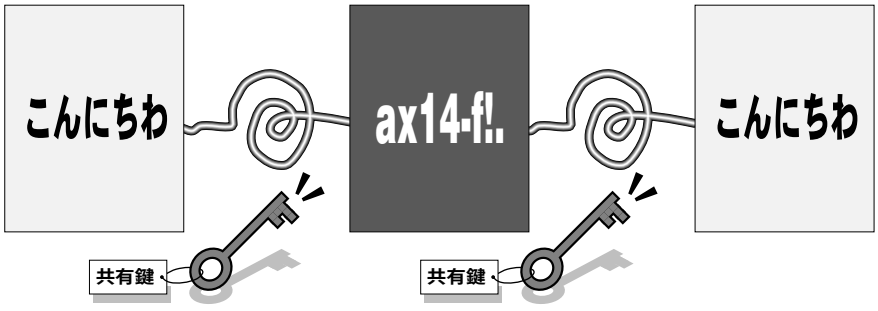
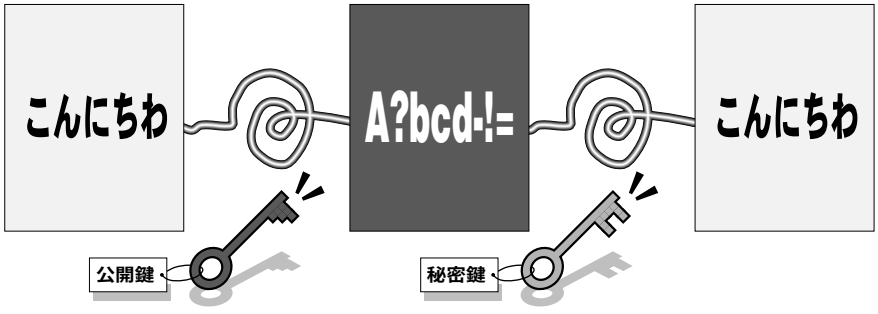


図2 公開鍵暗号



ージ自身の暗号化は行わないが、そのメッセージが確かに自分から発信されたものであることを示すための手続きなどがあるのですが、最近非常に良い書籍などが出てきていますので、興味がある人はそちらを参考にして下さい（参考文献を紹介します）。

さて、PGPの利用方法ですが、以下の5つが基本的な手続きになります（今回は、個々のソフトウェアの詳しい利用方法については誌面の関係で詳細に解説しません。ごめんなさい。また機会があれば取り上げます）。

❶ 自分の秘密鍵と公開鍵の生成
❷ 自分の公開鍵の配布
❸ 相手の公開鍵の登録
❹ メッセージの暗号化と発信
❺ 受信したメッセージの復号

PGPを利用するためには、まず、自分の秘密鍵と公開鍵を生成することになります。PGPを利用する場合にはPGPのソフトウェアの設定後、まずこの作業を行ってください（図3：UnixやMS-DOS上のPGPを利用する場合には、「pgp -kg」を実行すればよい）。

そして、作成された公開鍵を必要な人に配布します。この作業は通常の電子メールなどを利用して行うことになります（「pgp -kxaf 自分のメールアドレス」で得られたメッセージを相手に送ればよいでしょう）。

受け取った相手の公開鍵は自分のデータベースに登録しておきます（「pgp -ka」を用います）。

これで準備は完了です。あとは、暗号化したいメッセージを作成し、暗号化します（大抵のソフトウェアでは自動的に相手用の公開鍵を選択し、暗号化を行うでしょう）。そして、受け取った暗号メッセージは、自分の秘密鍵で復号します。このとき、鍵を生成した時に入力した合い言葉（通常パスフレーズと呼ばれます）の入力を要求されると思いますので、鍵を生成する際に利用したパスフレーズはきちんと覚えておいてください。

最後に、PGPの利用にあたって注意しなければならないことを解説します。

まず、自分の公開鍵を配布するときには、相手に正しい公開鍵が届いているかをなんらかの手段で確認する必要があります。これは、「なりすまし」や「改竄」によって自分の公開鍵が他人のものとすりかわっている可能性があるからです。もし、これに気づかずに相手がメッセージを発信してしまうと、そのメッセージは他人に盗まれてしまう可能性があるわけです。しかも自分では復号化できません。

通常は、フィンガープリントといって、一種のチェックサムを電話などで確認して正しい公開鍵が伝わっていることを確認します（「pgp -kvc」を利用して送られてきた公開鍵のフィンガープリントを知ることができます）。

実は、この部分がPGPの欠点であると言われています。つまり、インターネット上で正しく公開鍵を配布するメカニズムが用意されていないということです。これに対しPEMでは、第三者認証システムと呼ばれるものを利用して、鍵を安全に配布するメカ

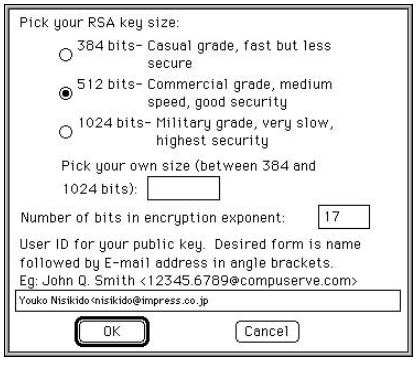


図3　MacPGPのメニューでKeyから「General Key」を選択するとこのウィンドウが現れる。ここでOKをボタンをクリックすると、鍵を生成するメッセージが表示される。

ニズムを用意しているのですが、この第三者認証システムを現在のインターネット上に構築することが非常に難しいためにPEMの普及が遅れているという逆の問題点になっているのです。

ですから、現状で比較的簡単に利用できるということで、インターネットではPGPのほうが広く利用されています。また、PGPはMIMEというマルチメディアメールの形式との相性がよいという特徴も持っています。

そして、もう1つの問題は、非常に深刻なのですが、実はRSAという暗号化のしくみが特許となっており、また、米国からの輸出が禁止されているという問題です。したがって、現在のPGPのソフトウェアを米国外で利用することは非常にグレーな状況になっているのです。この問題は非常に複雑で早く解決されることが望まれていますが、このことに留意して利用するべきでしょう。少なくとも、米国に設置されているanonymous FTPサイトから入手するように心がけたほうがよいでしょう（バージョン2.3以前のものか、それをベースに米国外で改良されたものを利用することをおすすめします）。

【参考文献】
Simson Garfinkel「PGP: Pretty Good Privacy」O'Reilly & Associates, 1995.
山本 和彦「PGP」転ばぬ先のセキュリティ「UNIX Magazine」1995年7月号から連載中.

地方都市に住んでいると、インターネットに興味があってもアクセスポイントが少ないのでなかなかネットサーフはできません。そこで、友人らと集まって、ホストをおいて専用線接続を行い、そこにアクセスしようと考えています。しかし、あるプロバイダーからは難しいという答えが返ってきました。このようなことをしてはいけないのでしょうか？

（小田島慎一さん）

A. 実は、このような接続をしている組織がすでにいくつか存在しています。そのためには、まず小田島さんたちが集まっているグループをJPNICに非営利の組織として登録しなければなりません（つまり、xxx.or.jpというドメイン名を取得する）。

非営利の組織でない場合、通信事業者、つまりプロバイダーと同格に扱われるため、郵政省への登録など面倒な手続きが発生してしまうのです。

そのため、組織において以下の3点を守らなければなりません。

❶ 非営利の団体であること。
❷ 接続の対象が個人であること。
❸ その組織に所属する会員だけが利用していること。

したがって、この活動を通して利益が生まれたり、会社などの組織を接続したりすることは避けなければなりません。また、このインターネット接続は、組織の活動のための接続ということになりますから、ここに参加している人たちのネットワーク利用目的が極度に営利目的にならないようにするべきでしょう。

そこで、このようなことを示すため、組織の規約を作って提出することになります。あまり難しいものである必要はありませんが、以上のことが明示されていること、そして規約の決め方が民主的であることが示されればよいと思います。

すでに一度プロバイダーに相談されているようですが、このような多少面倒な話については、やはり経験豊富な大手のプロバイダーのほうが親切に対応してくれると思います。多少高いかもしれませんが（笑）、再度プロバイダーに相談されるとよいでしょう。

入門者のための

FAQ

インターネットの話を聞いていると、RFCという言葉をよく耳にします。これはいったい何なのですか？

（近藤聡子さん）

A. RFC（アール・エフ・シー）とはRequest for Commentsの略で、インターネットにおける規格やルール、あるいは有益な情報をまとめた文書です。

たとえば、インターネット上で利用されるアプリケーションでの通信手順（プロトコル）や情報形式などについてはこのRFCに規定されています。わからないことがあったらまずこれらの文書をあたってみることになります。

これらの文書は、RFCとして認められた順に番号が与えられており、RFCの何番と呼ぶようになっています。RFC822はメールの形式に関する規定、RFC793はTransmission Control Protocol（TCP）に関する規定といった具合で、現在RFC1800番台のものが誕生してきています。

インターネットに接続されていれば、RFCは各所のanonymous FTPから入手できますので、興味があれば、自分で調べてみるとよいでしょう（大抵RFCやrfcといったディレクトリの下に置かれているでしょう）。このとき、まず、rfc-index.txt（なんらかの圧縮がされているかもしれません）というファイルをまず入手してみるとよいでしょう。このファイルは現在のRFCの索引になっています。

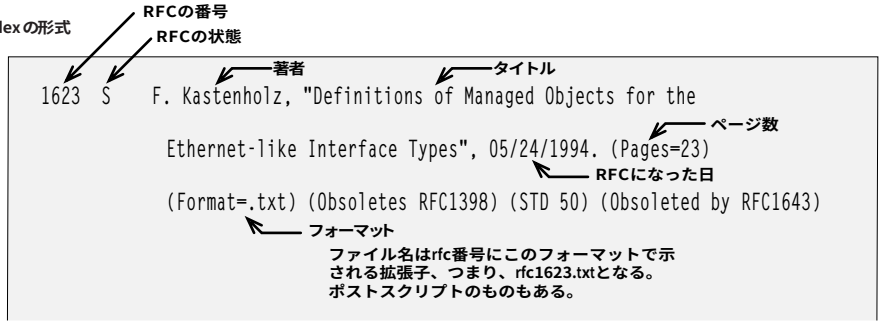
各エントリーは、図4のような形式をしており、最初の番号がrfc番号、次にこのRFCの状態が示されます（ここが空のものもある）。そして、著者、タイトルと続き、RFCとなった日付やページ数、フォーマットが示されます。RFCの状態とは、標準化作業のどの段階にあるかを示しており、PS（Proposed Standard）が標準として提案している段階、DS（Draft Standard）が標準として採用されるためのレビュー段階、S（Standard）は正式な標準として採用された段階を示しています。また、ほかに実験的プロトコルに関する規定であるE（Experimental）やインターネット上でのさまざまな情報をまとめたI（Informational）などがあります。

重要なのは、最後のほうに示されているObsoletesやUpdatesです。

「Obsoletes RFCXXX」はRFCXXXをこのRFCで置き換えることを、「Obsoleted by RFCYYY」はこのRFCをRFCYYYで置き換えることを示しています。したがって、これをきちんと確かめておかないと古い規格を見てしまうことになります。また、「Updates RFCXXX」は、RFCXXXの内容の一部についてこのRFCで追加や変更を行ったことを、「Updated by RFCYYY」は、RFCYYYによって、このRFCの内容の一部が変更されたり追加されたりしていることを示しています。これをきちんと見ておかないと、新たに追加された機能や改善された点などを見落とすことになってしまうのです。

内容は英語ですが、わかりやすく書いてありますので一度眺めてみると面白いと思いますよ。

図4 rfc-indexの形式



［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