個人情報を守るために

～ PGP for Windows ～

理学部数学科 助手　幸山 直人
nkouyama@sci.toyama-u.ac.jp

1. はじめに

今日の高度情報化社会において、個人情報の安全性を確保することは重要な課題となっています。この問題を解決する方法として、数学的な理論に裏打ちされた暗号という技術がありますが、その中でも、特に、公開鍵暗号方式と呼ばれる暗号技術は重要なキーワードとなります。2002 年度に行われた公開講座でも、「体験 公開鍵暗号」と称して、PGP (Pretty Good privacy)という個人情報を保護するための暗号化アプリケーションを紹介しました。本稿は、そのときの講義の一部をまとめたものです。PGP には新井政悟氏によって日本語化された PGP Version 6.5.8ckt 日本語版を使用し、OS には Microsoft 社の Windows を使用します。

2. PGP について

PGP は、主として Phil Zimmerman 一人が設計し、電子メールやファイルの秘密性と認証(署名)を確保することが可能なアプリケーションとして開発が開始されました。PGP が注目されたのは、暗号の歴史全体において唯一の真に革命的な公開鍵暗号方式を取り入れたことです。公開鍵暗号の仕組み等については、すでに本誌で紹介されているので、そちらを参照してください。

PGP そのものはフリーウェアで、一次配布元は国際化版 PGP の公式ホームページ[1]です。日本では IIJ 技術研究所が運営する(仮)日本の公式 PGP ホームページ[2]からダウンロードすることができます。また、PGP にはサポートが受けられる商用バージョンもあり、「PGP Personal Privacy」という製品が Network Associates 社(日本ではソースネクスト社)から販売されています。ただし、現在は販売を終了しているようです。

PGP で利用できる暗号系アルゴリズムは下表のようになります。なお、Diffe-Hellman は署名機能を持たないため、Diffe-Hellman/DSS のように SHA (Secure Hash Algorithm)を利用した電子署名標準 (DSS; Digital Signature Standard) と組み合わせて利用されます。

公開鍵暗号	RSA, Diffe-Hellman, ElGamal
慣用暗号	3DES, AES, BLOWFISH, CAST5, IDEA, TWOFISH
電子署名	MD5, RIPEMD, SHA, TIGER

3. PGP のインストール

まず、新井政悟氏によって日本語化された PGP Version 6.5.8ckt 日本語版(pgp658ckt08ja3.exe)を新井氏のホームページ[3]からダウンロードします。ダウンロードしたファイルをダブルクリックするとインストーラが起動するので、インストーラの指示に従って PGP をインストールしてください。詳細については、小牧実氏のホームページ[4]を参照してください。なお、Windows 2000 や Windows XP のように 1 台のコンピュータを複数のユーザで利用する場合は、Administrator 権限を持ったユーザでインストールしたほうが良いでしょう。

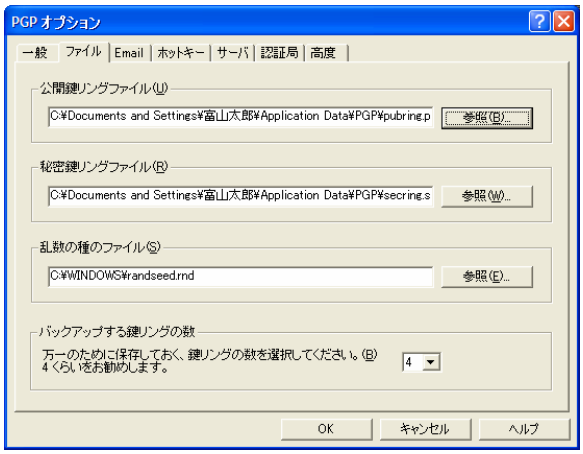
以下にインストールされる主なアプリケーションを挙げておきます。

(1) PGP 本体(PGP.exe) : PGP の本体で、その他のアプリケーションを利用する際にも間接的に呼び出されます(コマンドプロンプトからも利用可能)。
(2) PGPadmin : PGP 全体の振る舞いを管理します。例えば、強制的に復号化が可能な復号合鍵を作成することもできます。

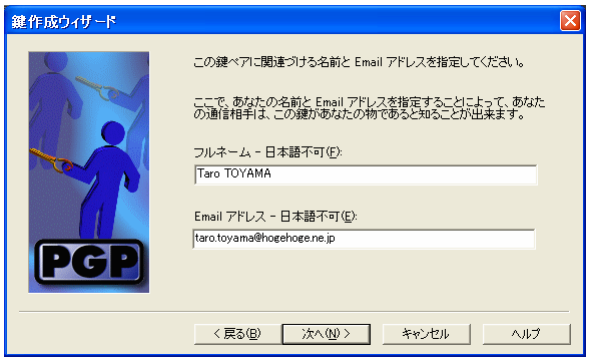
(3) PGPdisk：領域を確保したファイルを仮想ドライブとしてマウントし、この仮想ドライブに保存したファイルは、自動的に暗号化されます(正常に動作しない場合があります)。
(4) PGPlog：暗号化・復号化・署名・認証を行った際のログ(処理結果)を管理します。
(5) PGPtools：ファイル操作に関する PGP の機能(暗号化・復号化・署名など)を画面上から呼び出せるようにしたツール群です(5 節を参照)。
(6) PGPtray：システムに駐在し、PGP の機能をいつでも利用できるようにします。

3. 鍵の作成と公開鍵の公開

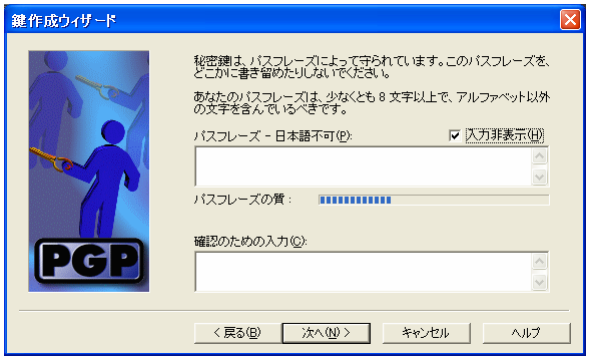
PGP を利用するためには、公開鍵と秘密鍵を作成する必要があります。鍵を作成する人のユーザ名を富山太郎、電子メールアドレスを taro.toyama@hogehoge.ne.jp として話を進めます。ディスクトップの「スタート」メニューから「プログラム」→「PGP」→「PGPkeys」の順で選択し、PGPkeys を起動してください。



公開鍵リングファイルと秘密鍵リングファイルの保存場所を聞かれるので、「C:¥Documents and Settings¥富山太郎¥Application Data¥PGP」(個人用のデフォルト)に設定し、「OK」ボタンをクリックします。鍵作成ウィザードが開始されるので、「次へ」をクリックします。

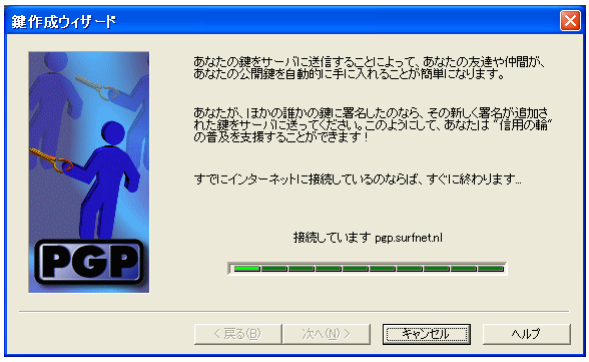


フルネームと E-mail アドレスを入力します。フルネームの欄は日本語不可なので Taro TOYAMA とでも入力しておきます。続けて、作成する鍵ペアの種類・サイズ・期限について選択します(特に変更する必要はありません)。



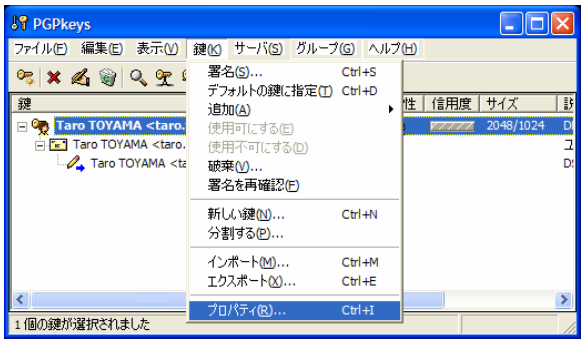
次に、秘密鍵を守るためにパスフレーズを設定します。パスフレーズの質を高めるために、目盛りがいっぱいになるまでパスフレーズを入力してください。確認のためのパスフレーズも忘れずに入力してください。

アニメーションと共に、公開鍵と秘密鍵が生成されます。

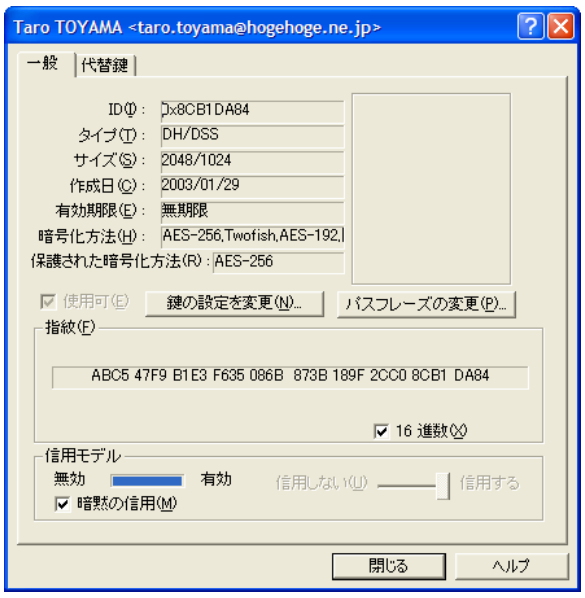


最後に、作成した公開鍵をルートサーバに登録するか聞かれるので、ネットワークに接続された環境であれば「今すぐルートサーバに自分の鍵を送信」にチェックを入れ、「次へ」をクリックします。送信終了後、「完了」ボタンを押してウィザードを終了してください(鍵は後からでも登録できます)。

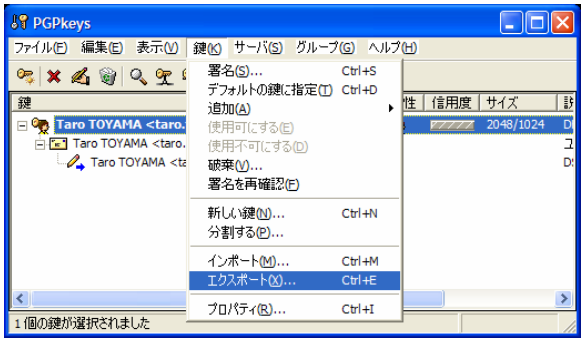
作成した鍵の指紋と公開鍵を見てみましょう。



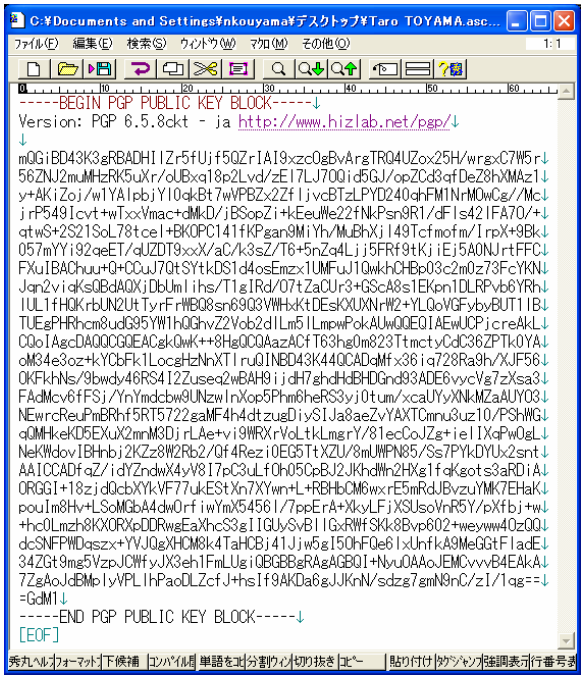
PGPkeys から作成した鍵を選択し、メニューの「鍵」→「プロパティ」を選択します。



指紋の欄に 40 桁の 16 進数で表示されています。この指紋は、公開鍵の認証に用いられるので、電子メールやホームページなどで公開しましょう。



次に、公開鍵を見てみましょう。PGPkeysn のメニューから「鍵」→「エクスポート」を選び、公開鍵をアスキー形式のファイルとして保存します。



このファイルも上記の指紋とあわせて、ホームページ等で公開しましょう。

逆に、他人の公開鍵を登録するには、メニューから「鍵」→「インポート」を選び、新しい公開鍵を登録します。なお、本人のものであることを指紋を使って確認しておきましょう。

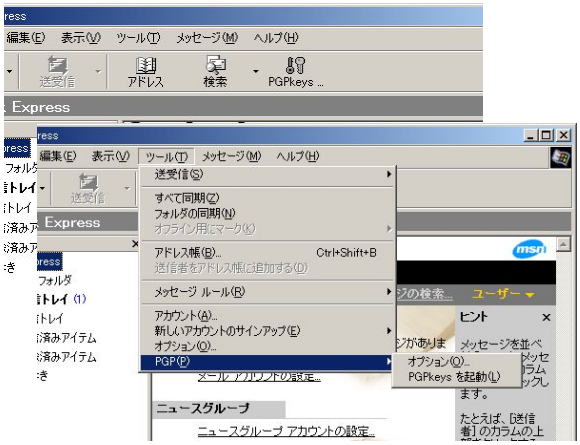
*1 使用しなくなった鍵は、メニューから「鍵」→「破棄」を選択し、ルートサーバに破棄したことを知らせましょう。

4. PGP による安全な電子メールのやりとり

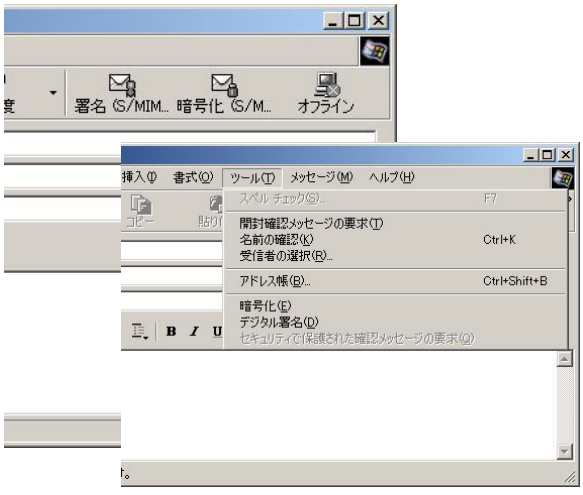
メールクライアントとして Outlook Express を使用されている方は、インストールの際にプラグ

イン(Outlook Express から PGP を使えるように機能拡張する仕組み)もインストールされるので、ボタン一つで暗号化・復号化・署名ができるようになります。

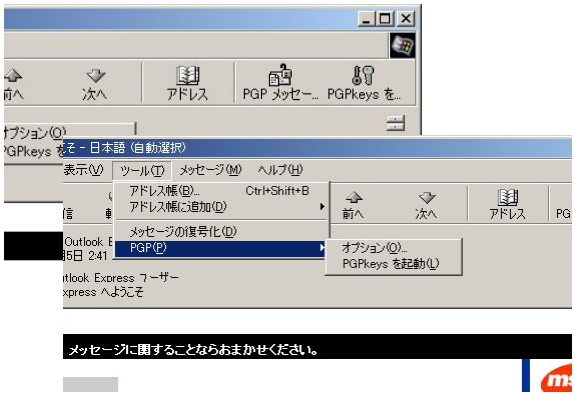
(1) Outlook Express を起動すると、ツールバーに PGPkeys の起動ボタンが追加され、メインメニューの「ツール」に「PGP」の項目が追加されます。



(2) メールを作成するウインドウを開くと、ツールバーに署名と暗号化を行うためのボタンが追加され、メインメニューの「ツール」に「暗号化」と「デジタル署名」の項目が追加されます。

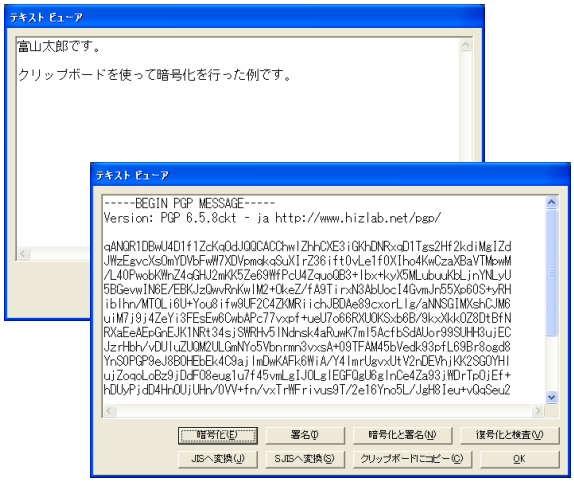


(3) 到着したメールを開くと、ツールバーにメッセージの複合化と PGPkeys の起動ボタンが追加され、メインメニューの「ツール」に「メッセージの復号化」と「PGP」の項目が追加されます。



また、AL-Mail をお使いの方も、AL-Mail のホームページからプラグインをダウンロードしてインストールすることにより、メニューから暗号化・複合化・署名を手軽に行うことができます。ただし、インストールする PGP のバージョを 5.5.3i に変更する必要があります(新井政悟氏のホームページにある PGP Version 5.5.3i 日本語版はインストーラが準備されていないので、インストール方法をよく読んでからインストールしてください)。

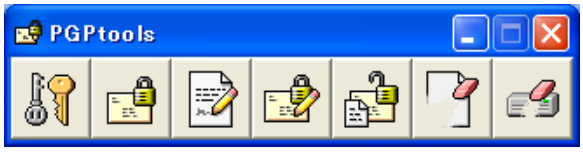
プラグインが準備されていないメールクライアントでも、PGP に付属するクリップボード(タスクバーの PGPtray から起動する)を利用すれば、メールの暗号化・復号化・署名を行うことができます。



5. PGP によるファイル操作(PGPtools)

PGP は、マイコンピュータやマイネットワークから覗くことのできるファイルについて暗号化・復号化・署名およびファイルの完全な削除ができます。

使用方法は、ディスクトップの「スタート」メニューから「プログラム」→「PGP」→「PGPtools」の順で選択し、PGPtools を起動してください。次のようなウインドウが現れます。



左から順に、
(1) PGPkeys の起動
(2) 暗号化
(3) 署名
(4) 暗号化と署名
(5) 復号化／検査(認証)
(6) 完全な削除
(7) フリースペースの清掃
となっています。

(2)から(6)はファイルに対しての操作で、ボタンをクリックするとファイルの選択ウインドウが開きますので、操作の対象となるファイルを選んで「開く」ボタンをクリックしてください。なお、(2)から(4)の操作については、ファイルの拡張子が pgp または sig に変わります。(5)の操作については、ファイルの拡張子が pgp または sig となるファイルについて、復号化または認証または両方を行い、asc については鍵の指紋を計算します。ただし、これらの方法では、ファイルを利用するたびに暗号化や復号化を行わなければならないので、仮想ディスクとして利用できる PGPdisk を使うか、次節で解説する Windows 2000 と Windows XP に標準搭載された暗号化システムを使うと便利です(紹介したバージョンの PGPdisk は動作しない可能性があります)。

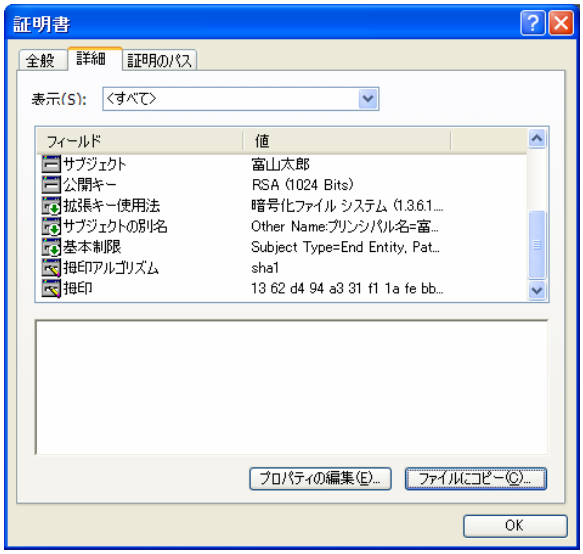
(6)と(7)については、ファイル自体が書きこまれていた領域または空き領域について数回におよび乱数を書き込みます。普通の削除では、ファイル自体を消去するわけではないので、シマンテック社の「Norton Utilities」などを使うと簡単に復元できてしまいます。従って、秘密性の高いデータが入っていたハードディスクやフロッピを廃棄する場合などは、この機能を利用すると安全です。

参考ですが、(2)から(6)の操作は、対象となるファイルを右クリックすることで、Send to メニューの「PGP」から利用することができます。

6. Windows 2000 / XP について

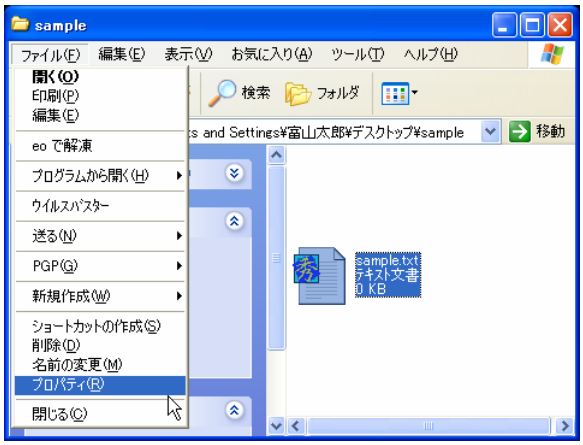
この節では、Windows 2000 と Windows XP に標準搭載されている暗号化システムについて紹介します。仕組みについては、PGP とほぼ同じで、電子メールの暗号化・復号化・署名およびファイルやフォルダの暗号化・復号化を行うことができます。2000 と XP では PGPdisk がうまく動作しないようなので、ファイルやフォルダの暗号化・復号化についてはこの暗号化システムを使うなど、PGP と上手に併用してください。

詳細について確認するには、Internet Explorer を起動後、「ツール」→「インターネット オプション」を選択し、「コンテンツ」タグにある証明書の欄の「証明書」をクリックします。続けて、「個人」タグにある自分のユーザ名を選択し、証明書の目的の欄の「表示」をクリックします。

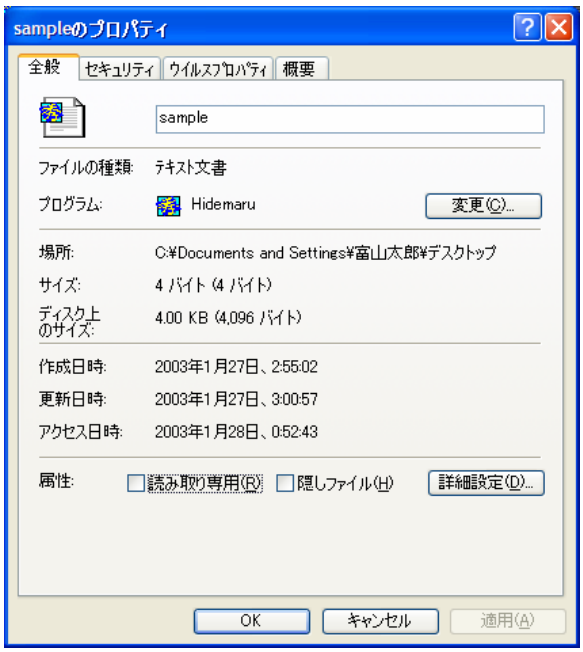


「詳細」タグをクリックすると、公開キーには 1024bit の RSA、拇印(署名)アルゴリズムには SHA1 が利用されていることがわかります。

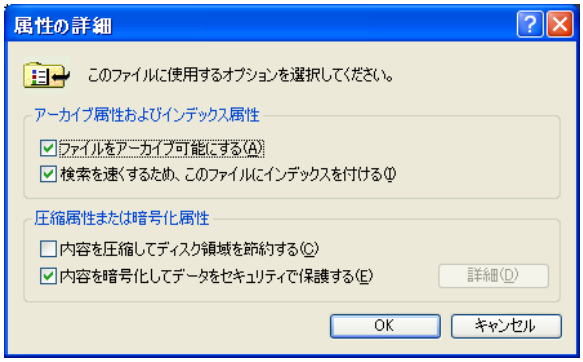
最後に、この暗号化システムを使ったファイルの暗号化について解説しておきます。以後、暗号化するファイルのファイル名を sample.txt として話を進めることにします。



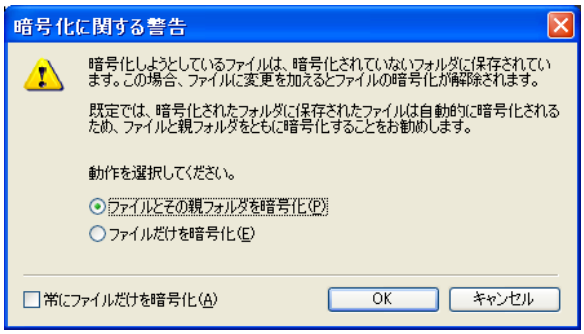
エクスプローラを開き、暗号化するファイルを選択します。メニューから「ファイル」→「プロパティ」の順で選択します(暗号化するファイルを左クリックし、「プロパティ」を選択しても良い)。



属性の欄の「詳細設定」をクリックします。

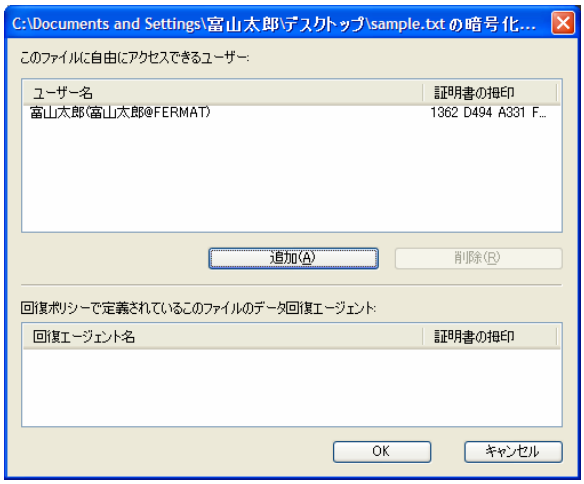


圧縮属性または暗号化属性の欄の「内容を暗号化してデータをセキュリティで保護する」にチェックを入れ、「OK」をクリックします。**暗号化を解除するには、チェックを外してください。**



暗号化に関する警告ウインドウが現れますが、特に何もなければそのまま「OK」をクリックしてください。「ファイルとその親フォルダを暗号化」を選択すると、フォルダ内のファイルやフォルダの暗号化・複合化を自動で行うため、一時的に作業用ファイルを作成するようなアプリケーションについても安全性を保つことができます。

以上で、暗号化は完了となります。上記の手順で作成したフォルダ内では、安全性はもちろんのこと、暗号化や複合化を意識することなく、ファイルやフォルダを普通に扱うことができます。また、暗号化されたファイルやフォルダは、特定のユーザの証明書で認証することにより、安全にファイルを共有することができます。ユーザを追加するには、ファイルのプロパティから「詳細設定」を選択し、属性の詳細の「詳細」を選択します。



暗号化の詳細ウインドウが開くので、「追加」ボタンを押し、必要なユーザを登録してください。

この暗号化システムを利用する上での注意点を挙げておきます。

(1) XP では暗号化されたファイルやフォルダの

名前が緑色に変わりますが、デスクトップにあるファイルやフォルダについては色が変化しないので、プロパティから確認するか、フォルダ(ユーザ名が富山太郎であれば、C ドライブの C:¥Documents and Settings¥富山太郎¥デスクトップ)を開いて緑色になっていることを確認してください。

(2) ショートカット(拡張子が lnk となっているもの)を暗号化してもリンク先のファイルやフォルダまでは暗号化されないので注意してください。

(3) 暗号化することで第三者にファイルやフォルダは覗かれなくなりますが、Administrators など強い権限のグループに属するユーザや自分自身による削除は可能なので、不慮の事故に備え、鍵と合わせて重要なものはバックアップしておきましょう(鍵のバックアップは、証明書の「詳細」タグにある「ファイルにコピー」をクリックし、ウィザードに従って作成してください)。

*1 この暗号化システムの秘密鍵はログオン時のパスワードで保護されているため、パスワードを変更する際は、ファイルやフォルダの暗号化を一旦解除してから再度暗号化する必要があります。

*2 この暗号化システムを利用するには、ローカルまたはネットワークを問わず、ファイルシステムが NTFS でなければなりません。従って、UNIX ファイルシステムを Windows 上で共有する samba では利用できません。

7. さいごに

先日、インターネット弁護士の先駆者である牧野二郎氏による「ネットワークセキュリティと法律」という講演を聞いてきましたが、個人情報を漏洩した場合、一人一人は少なくても数が多くなることでとんでもない賠償額になる事例を紹介されました。改めて、個人情報について自分の身を守るだけでなく、加害者にならないために他人の個人情報を扱う際には十分配慮する必要があることを認識させられました。そういった意味でも、今回の紹介した PGP をぜひ利用していただきたいと思います。

話は変りますが、最後に文部省のホームページをたどっていくと、「インターネット活用ガイドブック～モラル・セキュリティ編～」[5]と「インターネット活用のための情報モラル指導事例集」[6]というセキュリティやインターネット上でのモラルについてのやさしく解説されています。非常に参考になりますので、ぜひ一読してみてください。

リンク

[1] 国際化版 PGP の公式ホームページ
http://www.pgpi.org/

[2] (仮)日本の公式 PGP ホームページ
http://pgp.iijlab.net/

[3] 新井政悟氏のホームページ
http://www.hizlab.net/index.html

[4] 小牧実氏のホームページ
http://www.biwa.ne.jp/~mkoma/pgp.html

[5] インターネット活用ガイドブック
～モラル・セキュリティ編～
http://www.cec.or.jp/books/books11.html

[6] インターネット活用のための
情報モラル指導事例集
http://www.cec.or.jp/books/H12/books12.html