この文書は書きかけです。

はじめに

はじめに

PGP(GnuPG) を使って、電子情報を暗号化し、全国市民オンブズマン連絡会議事務局宛に電子メールを送る方法について述べる。

警察不正支出問題に関する内部告発などの、盗聴された時に致命的な情報を全国市民オンブズマン連絡会議宛に送付する時を想定している。

なお、簡易版なので、あなた -> 全国市民オンブズマン連絡会議事務局 という方向しか扱わないし、頻繁にやりとりする場合にはこのページの方法はよい方法ではない。

また、MS-Windows 2000/xp のユーザを想定している。ほかの OS のユーザは、自分で調べてほしい。

すでに、PGP や GnuPG を使っているひとは、下記の方法によらず、連絡先に公開鍵のリンクがあるので、通常の方法で暗号化してメールをいただければ幸いだ。なお、こちらからあなたへの復信メールについて、暗号化を希望する場合、その旨を往信メールに書くことと、あなたの公開鍵を往信メールに添付するのをわすれずに。

メールを送る前の " お約束 " の確認

書かないとわからない人がときどきいますので、書いておきます。（ここだけ「ですます」体。）

- 返事があるものと期待しないで下さい。通常は、お返事をさしあげません。
- 全国市民オンブズマン連絡会議は正義のなんでも屋さんではないので、どんなにそれが社会正義の観点からして、問題があっても、わたしたちのミッションに該当しないものは、扱いません。
- 法律相談は、各地に無料相談がありますので、まずはそちらをどうぞ。弁護士会に問い合わせてみてもいいでしょう。
- 弁護士の紹介はしていません。名古屋市内の方なら、栄の中日ビル内に有料相談所がありますので、最初はそこへ行くとよいでしょう。（予約がいるはずです。要確認。）30 分 5250 円です。
- あなたの連絡先がないものは、まずだめです。暗号化して送るのですから、暗号化するファイルの中に、あなたの連絡先を書いておいて下さい。（それに、いただいた情報に本当に価値があって、でも不足部分があって、それさえあれば、なんて時でも、連絡先がないと、話になりません。）

お願い

やってみればわかると思うが、電子メールをただ送るのと違い、暗号化の作業はやはりめんどくさい。これは、暗号化されたものを復号化して読む側（＝全国事務局）とて同じ。メールを読むのにひと手間いる。

全国事務局としては、毎日いそがしいので、できるだけ手間はかけたくない。そこで、お願いがある。

本当に、その情報は暗号化して送らなければならないのか、今一度考えて、それでも必要であれ

ば、暗号化して送ってほしい。そうでなければ、普通のメールにしてほしい。

完璧な匿名性がほしければ、電子メールはあきらめて、その資料をプリントアウトして、封書でわたしたちに送って下さったほうがよいと思う。

身勝手を申しますが、ご協力よろしくお願いいたします。

この文書で _ 扱わない _ こと

- PGP がなんであるのか
- PGP を使うと何がうれしいのか
- 電子メールがどう安全でないのか
- PGP と GnuPG(GPG) の違い
- GnuPG のちゃんとした使いかた

こういったことは、google などを使って、自分で調べてほしい。内部告発などのデリケートな情報のやりとりに、威力を発揮することがわかると思う。

最初に、フォルダオプションの変更（任意）

コントロールパネル -> フォルダオプション -> 表示 の「登録されている拡張子は表示しない」のチェックをはずす。

まず、GnuPG のインストール

まず、ftp://ftp.gnupg.org/gcrypt/binary/ から最新の GnuPG のインストーラをダウンロードしてくる。（2005/8/23 現在、gnupg-w32cli-1.4.2.exe が一番新しい。）

ダウンロードできたら、ダブルクリックして、インストーラを起動する。いろいろ質問されるが、すべて「OK」か「Next」か「Finish」を選択するだけでよい。

※注：Windows 2000/xp Professional な人は、Administrator 権限をもつユーザでないとインストールできない。

暗号化するファイルの用意

次に、暗号化すべきファイルを用意する。

- 文章であれば、メモ帳 (プログラム -> アクセサリ -> メモ帳) か、ワードパッド (プログラム -> アクセサリ -> ワードパッド) で書いておく。
- 画像つき文章であれば、あなたが持っていれば、ワード (2000, xp, 2003) か、一太郎 (13, 2004) で、書いておく。もちろん StarSuite(6, 7) でもよい。そういうソフトはいっさいもっていないのなら、OpenOffice.org(1.1.5, 2.0Beta) でもよい。
- 画像のみであれば、PNG 形式が一番望ましいが、JPEG でもかまわない。
- もちろんあなたがつくれるのなら、PDF でもかまわない。
- これ以外のデータ（例：エクセルのファイル）でもかまわない。（でも、できるだけ汎用性のあるデーターマットにしてね。）
- 複数のファイルになるのであれば、適当な圧縮ソフト (アーカイバ) でひとつのファイルにしてほしい。圧縮ファイルの形式は、zip か lzh にしてほしい。（圧縮ソフトを使ったことがない人は、たとえば、+Lhaca などが初心者むけ。）

暗号化の作業

作業場所をつくる

まず、作業場所をつくる。ここでは、c: の直下に temp というフォルダをつくることにする。

自分でつくれる人は、作る。

やりかたがわからないひとは、スタートメニューの「ファイル名を指定して実行」に

```
cmd.exe /c mkdir c:\temp
```

と入力して、OK をクリック。

暗号化するファイルをコピー

暗号化するファイルを、c:\temp の中にコピーする。

バッチファイルをダウンロード

次に、http://www.ombudsman.jp/gpgsh.bat をダウンロードし、c:\temp の中に置く。

バッチファイルのチェックサム確認

スタートメニューの「ファイル名を指定して実行」に

```
cmd.exe /k "c:\program files\gnu\gnupg\gpg.exe" --print-md sha1 c:\temp\gpgsh.bat
```

と入力して、OK をクリック。

```
c:\temp\gpgsh.bat: 25D0 07EC 4C60 E26B 5096  FDDE 58A2 ADD9 2A28 52F8
```

と出ていれば OK。ウインドウを閉じる。

もし、違う 16 進数が表示されていれば、バッチファイルが不正に改変されている可能性があるので、ここでおしまい。（できれば、全国事務局にひとこと連絡してほしい。）

gpgsh.bat

■実行

c:\temp の中にある gpgsh.bat をダブルクリックして起動。（公開鍵のインポートも同時に完了する。）

■公開鍵のチェックサム確認

※注：[Enter] は、Enter キー（リターンキーともいう）を押すの意。以下同じ。

黒いウインドウ（コマンドプロンプトという）に、

```
gpg --fingerprint [Enter]
```

と入力すると、

```
pub   1024D/65725B91 2004-03-27
```

```
      Key fingerprint = 26BA 069C BF27 1CE9 5F60  8EE2 7A79 9F90 6572 5B91
uid                  ombudsman office <info@ombudsman.jp>
sub   2048g/4A563821 2004-03-27
```

と出れば OK。もし、Key fingerprint の 16 進数が違うものが表示されていれば、バッチファイルが不正に改変されている可能性があるので、ここでおしまい。（できれば、全国事務局にひとこと連絡してほしい。）

■ファイルの暗号化

コマンドプロンプトに、

```
gpg -a -r info@ombudsman.jp -e 暗号化すべきファイル [Enter]
```

と入力する。

もし、「暗号化すべきファイル」が日本語のファイル名だったり、入力するのがめんどくさければ、

```
gpg -a -r info@ombudsman.jp -e
```

まで入力して（-e の後には半角スペースがある）、Tab キーを何度か押せば、それらしいファイル名を順に表示してくれるので、正しいものを選んで、Enter を押す。

すると、

```
It is NOT certain that the key belongs to the person named
in the user ID.  If you *really* know what you are doing,
you may answer the next question with yes.

Use this key anyway? (y/N)
```

または、

```
この鍵は、このユーザー ID をなのる本人のものかどうか確信でき
ません。今から行うことを＊本当に＊理解していない場合には、
次の質問には no と答えてください。

それでもこの鍵を使いますか？ (y/N)
```

と聞かれるので、y を入力し、Enter を押す。

しばらく待つと、

```
C:\temp>
```

が返ってくるので、無事終了。c:\temp の中に、「暗号化すべきファイル .asc」という暗号化されたファイルができている。

できたファイルを送信

info@ombudsman.jp に、できた暗号化ファイルをメールしてほしい。添付ファイルでもいいし、あなたがマウス操作がきちんとできるひとであれば、できた暗号化ファイルはテキストファイルな

ので、メール本文に全てコピー＆ペーストして送ってもらってもかまわない。

ひとつお願いがある。メール本文に、暗号化ファイルがどういう構成かを書ける範囲で書いてくれるとうれしい。たとえば、

> **ファイルはメモ帳で書きました。**

とか、

> **ワード 2000 のファイルです。**

とか

> **PDF と Excel 2003 のファイルです。zip 形式でひとつのファイルにして、圧縮してあります。**

みたいな感じ。

※注：内容について書く必要はない。「＊＊県警の○○の裏帳簿です」とかメール本文には書いちゃだめ。

あとかたづけ

このあと、たぶんあなたはこの後 GnuPG を使わないと思うので、コマンドプロンプト上で、

```
cd "%USERPROFILE%\Application Data" [Enter]
rmdir gnupg /s /q [Enter]
```

として、インポートした公開鍵を消す。

次に、コマンドプロンプトのウインドウを閉じる。

```
exit [Enter]
```

と入力すれば OK。

次に、作業場所の削除。c:\temp をゴミ箱にポイ、でもよいし、スタートメニューの「ファイル名を指定して実行」に

```
cmd.exe /c rmdir c:\temp /s /q
```

と入力して、OK をクリック、でもよい。

最後に、GnuPG のアンインストール。コントロールパネル -> アプリケーションの追加と削除 から、GnuPG を削除する。

おしまい。

お疲れさまでした。

暗号化の元データは、あなたが安全に保管するなり、なんなりしておくこと。そちらから漏洩したら、元も子もないので。

Q & A

・Q: ほんとに大丈夫？
・A: 一般的な話でいえば、日本の警察やドイツのネオナチの地下組織が使用している（らしい）くらいに安全。まず、PGP(GnuPG) の暗号は解けないと思っていてよいと思う。
・Q: ほんとにほんとに大丈夫？
・A: 理解しなきゃいけないことは、暗号化したファイルを、わたしたちにメールで送った、ということは盗聴でわかるということ。ゆえに、わたしたちにコンタクトをとったという事実自体完全に秘匿したい方にはあまりおすすめできないかな。（信頼できるネットワークから、yahoo や hotmail などの無料メールで捨てアカウントをつくって、そこから出すという手もあるけどね。）
・Q: この文書は＊＊が間違っているよ。
・A: webmaster [at] ombudsman.jp にその内容をメールくれるとうれしいな。