

JanusDGX ユーザーマニュアル

目次

1 JanusDGX について.....	3	3 署名検証のための公開鍵の指定.....	16
1 ソフトウェアの概要.....	3	鍵輪を使用している場合.....	16
2 特長.....	4	鍵輪を使用していない場合.....	16
3 動作環境.....	4	4 復号後のファイルあるいはフォルダの名前を指	
4 使用条件.....	4	定.....	17
5 同梱のファイルについて.....	4	8 署名ファイル作成.....	18
GnuPG.....	4	1 署名作成モードにセット.....	18
GnuWin32.....	4	2 ファイルをドロップ.....	19
2 公開鍵暗号について.....	5	ボタンセレクトモードの場合.....	19
3 セットアップ.....	5	マルチペインモードの場合.....	19
1 運用フォルダの準備.....	5	3 署名ファイルの名前の指定.....	20
2 配布物の展開.....	5	9 署名の検証.....	20
3 初回起動(鍵の作成).....	6	1 署名検証モードにセット.....	21
4 2度目以降の起動.....	7	2 ファイルをドロップ.....	21
4 公開鍵の受け渡し.....	7	ボタンセレクトモードの場合.....	21
1 相手に公開鍵を渡す.....	7	マルチペインモードの場合.....	21
2 相手の公開鍵を受け取る.....	8	3 署名ファイルを指定.....	22
5 データの暗号化(公開鍵暗号).....	9	4 公開鍵ファイルを指定.....	22
1 暗号化モードにセット.....	9	5 検証実施.....	23
2 ファイルをドロップ.....	9	10 その他の機能.....	23
ボタンセレクトモードの場合.....	9	1 受け取った公開鍵が本物かどうかの確認.....	23
マルチペインモードの場合.....	10	鍵輪を使用していない場合.....	23
3 暗号化後のファイルの名前の指定.....	10	公開鍵を送った側の操作.....	23
4 公開鍵の指定.....	10	公開鍵を受け取った側の操作.....	24
鍵輪を使用していない場合.....	10	鍵輪を使用している場合.....	25
鍵輪を使用している場合.....	11	2 ユーザー名、メールアドレスの変更.....	25
5 暗号化完了.....	11	3 秘密鍵へのパスフレーズの付加・変更.....	25
6 データの暗号化(対称暗号).....	12	4 ファイルのアスキー化.....	25
1 暗号化モードにセット.....	12	5 ファイルのバイナリ化.....	26
2 ファイルをドロップ.....	12	6 鍵のバックアップ.....	26
ボタンセレクトモードの場合.....	13	11 カスタマイズ.....	27
マルチペインモードの場合.....	13	1 カスタマイズの方法.....	27
3 暗号化後のファイルの名前の指定.....	13	JanusDGX を起動してカスタマイズ.....	27
4 パスフレーズの入力.....	14	オプションエディタを使用.....	27
5 暗号化完了.....	14	2 カスタマイズして再配布.....	28
7 データの復号.....	14	3 カスタマイズ項目.....	28
1 復号モードにセット.....	14	暗号ファイル形式.....	28
2 ファイルをドロップ.....	15	鍵ファイル形式.....	29
ボタンセレクトモードの場合.....	15	ユーザーインターフェース.....	29
マルチペインモードの場合.....	15	電子署名・検証機能を使う.....	29

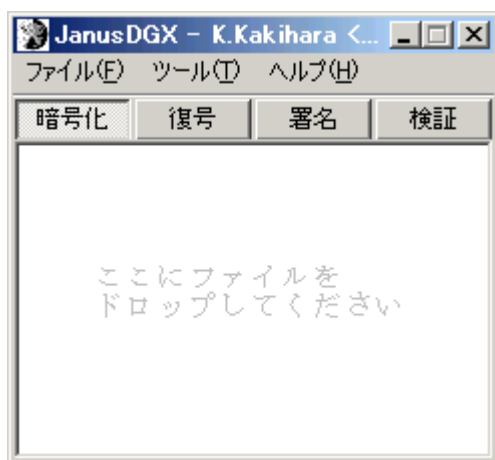
対称暗号も使用する.....	29	鍵輪管理機能を使う.....	30
複数ファイルやフォルダを暗号化する.....	29	JanusDGX でのオプション変更を禁止する..	30
テキスト・バイナリ変換機能を使う.....	29	デバッグ用ログを記録する.....	30
暗号化の際に署名する.....	29	12 バグの報告についてお願い.....	30
復号の際に署名を確認する.....	30		

1 JanusDGX について

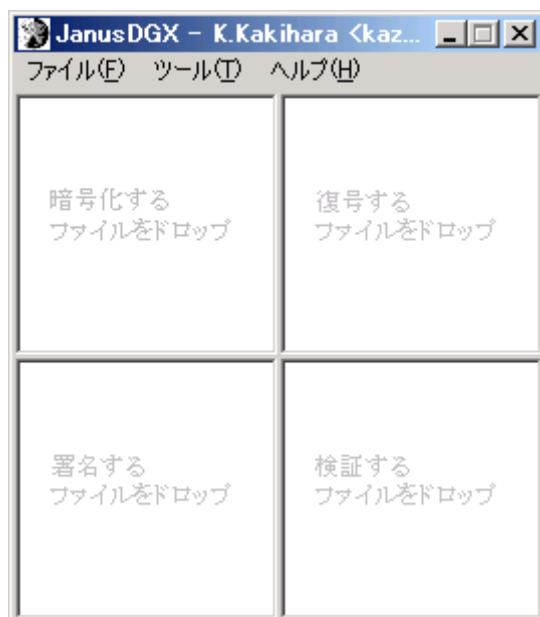
1 ソフトウェアの概要

一言で表現すれば「カスタマイズ可能な JanusDG」です。

もともと JanusDG は「公開鍵暗号」を扱える「シンプル操作」のソフトとして公開しました。そして、この「シンプル操作」を実現するために、いくつもの機能を泣く泣く切り捨てる必要がありました。こうして切り捨てた機能について、それでもカスタマイズで実現できれば便利だろうというものを「オプション」という形で選択利用可能としたのが JanusDGX です。



ボタンセレクトモードの UI



マルチペインモードの UI

2 特長

シンプル操作

JanusDG そのままのシンプルな操作体系は維持しています。ドラッグ&ドロップでファイルを暗号化・復号できます。

カスタマイズ

ファイル形式を ASCII 形式にしたり、対称暗号も併用したりといったオプションを用意しました。ユーザーインターフェースも切り替え可能です。

再配布

JanusDGX を入手した人がカスタマイズを施し、「カスタマイズ後」の JanusDGX を再配布して友人・知人と共用するという運用形態を考慮しました。

公開鍵暗号

JanusDG 同様、公開鍵暗号を利用できます。また、従来型の対称暗号を使用したり、複数ファイル・フォルダを束ねて暗号化したりできます。

3 動作環境

Microsoft Windows XP/Vista での動作を確認しています。

4 使用条件

JanusDGX は JanusDGX 本体(ファイル名 JanusDGX.exe およびその周辺ファイル)と、GnuPG 由来のファイル(gpg.exe)、bsdtar 由来のファイル(bsdtar.exe およびその周辺ファイル)とから構成されています。

JanusDGX 本体については Kazuyoshi Kakihara が著作権を保持しており、利用については GPL3 に従うものとします。JanusDGX 本体はあるがままの形で無保証で提供されるソフトウェアです。著作権表示を保持し、GPL3 を適用する限りにおいて、JanusDGX 本体の複製・改変・再頒布を認めます。

GnuPG、bsdtar については、別途それぞれのソフトウェアのライセンスが適用されます(共通して、自己責任・無保証の条件の下、無償で使用・再配布が可能です)。

5 同梱のファイルについて

GnuPG

bin フォルダ内の gpg.exe は、GnuPG(The GNU Privacy Guard)由来のファイルで、GnuPG のライセンスが適用されます。詳しくは GnuPG のホームページ <http://www.gnupg.org>を参照してください。

GnuWin32

bin フォルダ内の bsdtar.exe, archive2.dll, bzip2.dll, zlib1.dll は GnuWin32 由来のファイルです。これらのファイルについては GnuWin32 のライセンスが適用されます。詳しくは GnuWin32 のホームページ <http://gnuwin32.sourceforge.net/>を参照してください。

2 公開鍵暗号について

公開鍵暗号とは、データの暗号化と復号で、対になる二つの異なる鍵を使う暗号方式です。

暗号化鍵は暗号化専用の鍵となっており、この鍵ではデータを復号することはできません。復号用の鍵でなければ暗号データを元に戻すことはできないので、暗号化鍵を誰かに知られたとしても暗号の安全性には影響が出ないという特徴があります。

実際の運用にあたっては、あらかじめホームページなどで自分の暗号化鍵を公開しておき、誰からのデータであっても自分宛の暗号はすべてその暗号化鍵を使ってもらうようにします。

自分は公開した鍵と対になる復号鍵一つだけを厳重秘密に管理しておきます。

従来型の暗号と比べて、

- パスワードを相手に秘密に伝える必要がない
- 暗号を解くための重要な秘密(パスワード等)を誰かと共有しているわけではない
- たくさんのパスワードを秘密に管理しておく必要がない

以上の点で、運用が容易で、安全性が高くなっているのが公開鍵暗号の特長です。

一般に、暗号化鍵は「公開鍵」、復号鍵は「秘密鍵」とよばれます。

「JanusDGX」では鍵の管理はソフトが行います。ユーザーがしなければならぬことは、一度だけの鍵作成と、あとは公開鍵の受け渡しだけです。

※公開鍵暗号は鍵を人に盗聴されても安全ですが、鍵の詐称(悪意のある人が別人になりすまして、あたかもその人のものであるかのようにして公開鍵を渡す場合など)には対応できませんので注意してください。

3 セットアップ

1 運用フォルダの準備

まず、JanusDGX を運用する専用のフォルダを作成します。運用の利便を考慮し、My Documents 内に作成することを推奨しますが、たとえば USB メモリ等に入れて持ち運びたい場合は、そのようなリムーバブルメディア上で利用することも可能です。ただし、フォルダは必ず書き込み可能でなければなりません。

以後の例では JanusDGX という名前のフォルダを作成しています。

JanusDGX は一時ファイルを除き、このフォルダ以外に勝手にファイルの書き込みを行うことはありません。レジストリを使用することも、Windows のシステムフォルダにファイルを作成することもありません。

2 配布物の展開

JanusDGX は zip 圧縮形式で配布されます。このファイルを上で準備したフォルダ内に展開してください (Windows XP 以降ならば、別途ソフトを用意しなくてもファイルを展開できます)。



例)ここでは JanusDGX というフォルダ内に展開しました

これで JanusDGX を使う準備が整いました。

3 初回起動(鍵の作成)

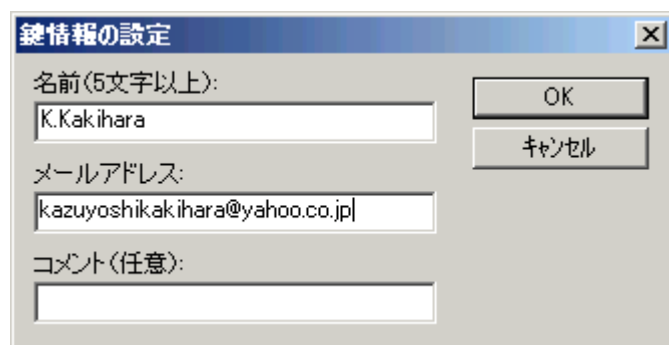
JanusDGX は公開鍵暗号を使用します。このため、通常使用を始める前に、公開鍵(データの暗号化に使用する鍵)と秘密鍵(データの復号に使用する鍵)のペアを作成しておく必要があります。

JanusDGX は初回起動時に強制的にこれらの鍵を作成します。

運用フォルダ内にある JanusDGX.exe が JanusDGX の本体です。

JanusDGX.exe を実行してください。

JanusDGX を初めて起動すると次のような画面が現れます。

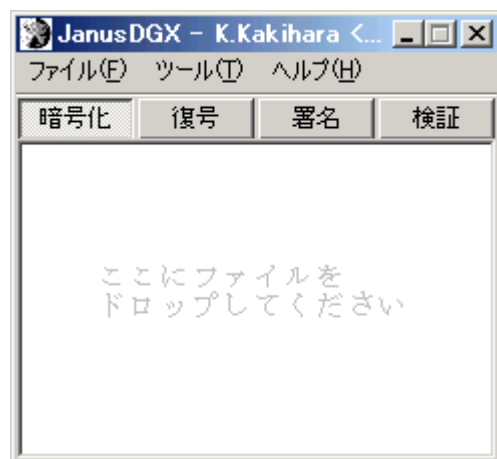


注)ここでは既に名前とメールアドレスが入力されています

鍵の運用者を明示するため、名前(半角英数、ローマ字で表記、5文字以上)、メールアドレスの入力が必要となります。このアドレスが実際のメール送信に使われることはありませんので、現実のメールアドレスである必要はありません。しかし、現実には、管理コストを考え、実際のメールアドレスを使用することをおすすめします。

これで、鍵ペアが作成されますが、この作成作業には最新のパソコンでも少々時間がかかります。参考までに、手元の Duron 1GHz の PC で十数秒から場合によっては 1 分近くが必要でした。

初回起動の際もこれ以後も、JanusDGX では、ソフトが鍵ペアの管理をしますので、ユーザーが鍵ファイル本体を直に目にはありません。直接操作することはありません。



これで JanusDGX のメイン画面が現れます。

4 2 度目以降の起動

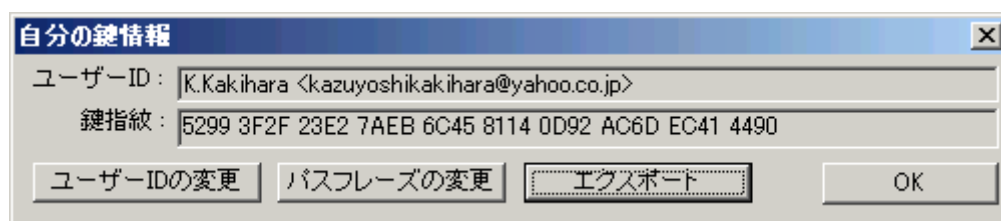
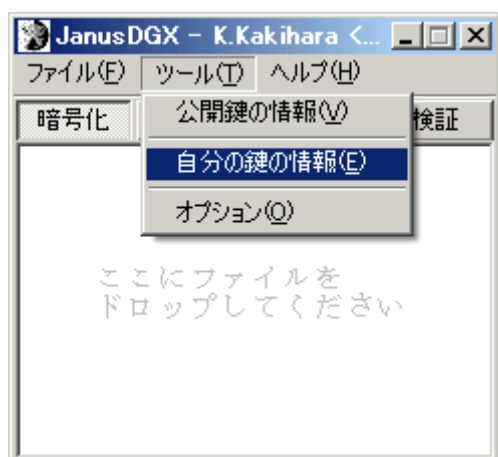
鍵にパスフレーズをかけていない場合、JanusDGX.exe を実行すると、すぐに JanusDGX が起動します。

鍵にパスフレーズをかけている場合は JanusDGX を起動する際にパスフレーズの入力を求められるようになります。

4 公開鍵の受け渡し

1 相手に公開鍵を渡す

誰かに自分宛の暗号化データを作ってもらうには、事前に自分の公開鍵を相手に渡しておく必要があります。JanusDGX を起動し、メニューの「ツール」から「自分の鍵の情報」を選択して鍵マネージャを呼び出し、「エクスポート」で自分の公開鍵をファイルに書き出しておいてください。



公開鍵ファイルを誰かに見られたとしても、コピーされたとしても、暗号の強度に影響はありません。メールに添付したり、フロッピーで郵送したりして、相手に届けてください。

2 相手の公開鍵を受け取る

データを暗号化する前に、データを送る相手の公開鍵を入手しておく必要があります。相手が JanusDGX からエクスポートした鍵を受け取り、運用フォルダ内の `pubkey` というフォルダ内にコピーしておいてください。



この例では「kazuyoshikakihara@yahoo.co.jp.gpg」という公開鍵が一つ見えています。

5 データの暗号化(公開鍵暗号)

JanusDGX は、与えられたデータをもとにして、暗号化されたデータを作成するソフトです。元のデータを上書きして暗号化するわけではありません。また、公開鍵暗号を使用しているため、データを暗号化するにはあらかじめ相手の公開鍵を受け取っておく必要があります。

1 暗号化モードにセット

マルチペインモードではこの作業は必要ありません。ボタンセレクトモードの場合のみこの作業が必要になります。

JanusDGX を暗号化モードにセットします。ツールバーの「暗号化」ボタンをクリックし、ボタンが押された状態にしてください。



2 ファイルをドロップ

JanusDGX では、特にオプションで指定していない限り、一度に暗号化できるファイルは一つだけです。複数のファイルやフォルダをまとめて圧縮暗号化したい場合は、あらかじめオプションで「複数ファイルを扱う」にチェックを入れておいてください。

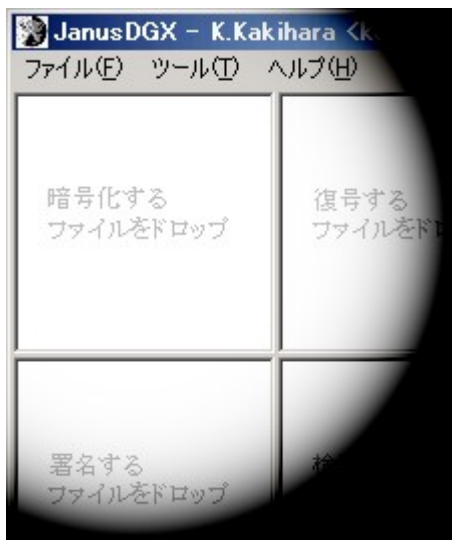
ボタンセレクトモードの場合

暗号化したいファイルをメインウィンドウの「ここにファイルをドロップしてください」という部分にドラッグ&ドロップします。



マルチペインモードの場合

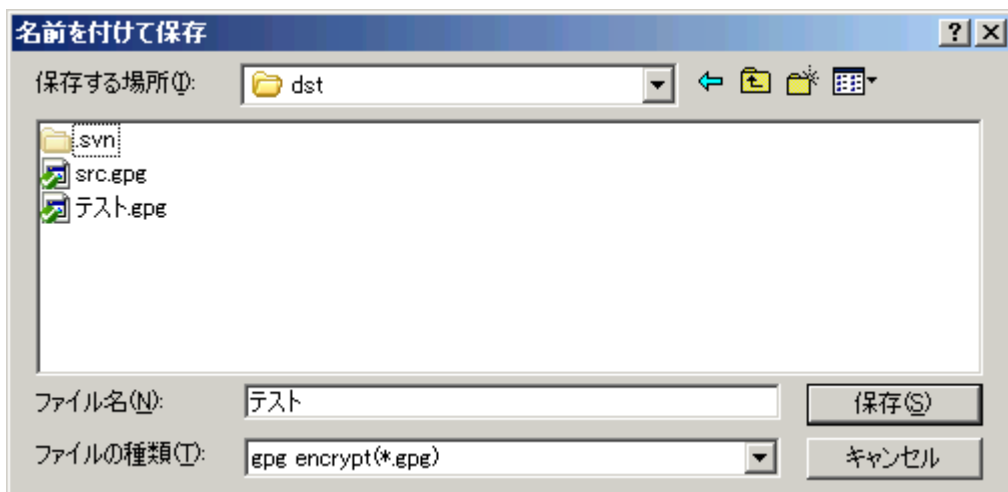
「暗号化するファイルをドロップ」と表示されているペインにファイルをドラッグ&ドロップします。



3 暗号化後のファイルの名前の指定

続いて「名前をつけて保存」という画面が現れますので、暗号化後のファイル名を指定してください。

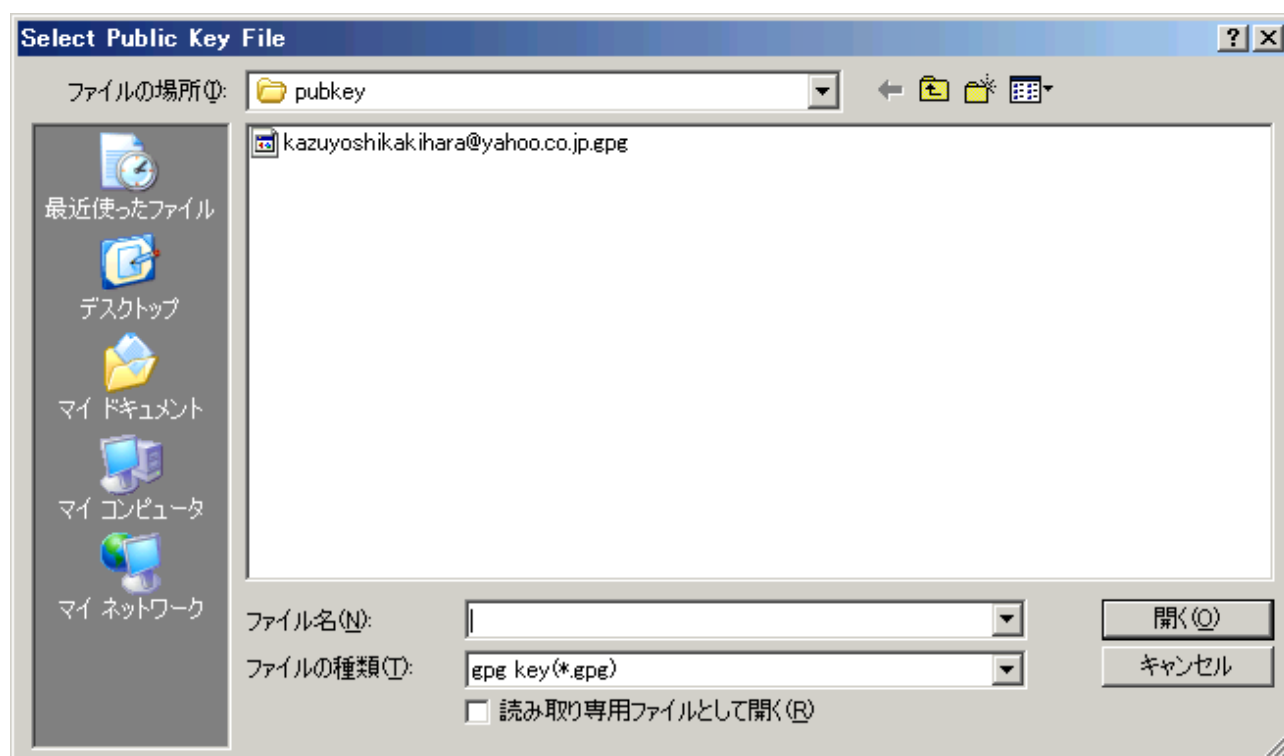
ここで、ファイルの種類が「gpg encrypt」になっている(gpg encrypt symmetric になっていない)ことを確認しておいてください。



4 公開鍵の指定

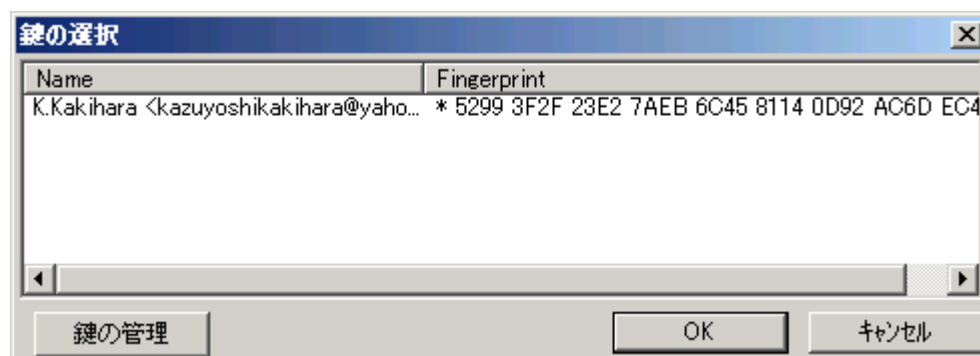
鍵輪を使用していない場合

ファイルをドロップするとすぐに「Select Public Key File」という画面が現れますので、暗号データを受け取る相手の公開鍵ファイルを指定します。



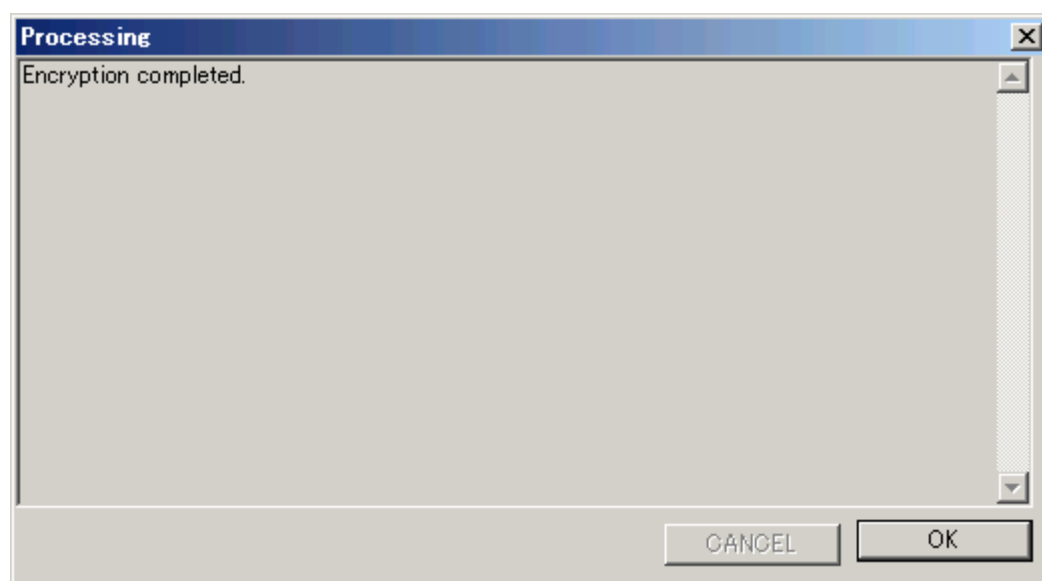
鍵輪を使用している場合

公開鍵を選択するウインドウがあられますので、暗号データを受け取る相手の公開鍵を選択します。



5 暗号化完了

鍵を指定すると、暗号化プロセスを表示するウインドウが現れます。ここで「Encryption Completed」と表示されれば暗号化完了です。



暗号化時に自動的に署名する設定になっている場合は、ここで署名済みの暗号データが作成されます。

6 データの暗号化(対称暗号)

JanusDGX は、与えられたデータをもとにして、暗号化されたデータを作成するソフトです。元のデータを上書きして暗号化するわけではありません。

JanusDGX は、オプションで「対称暗号を使用」するように設定されている場合、従来型のパスワード方式によるファイル・フォルダの暗号化が可能です。

1 暗号化モードにセット

マルチペインモードではこの作業は必要ありません。ボタンセレクトモードの場合のみこの作業が必要になります。

JanusDGX を暗号化モードにセットします。ツールバーの「暗号化」ボタンをクリックし、ボタンが押された状態にしてください。



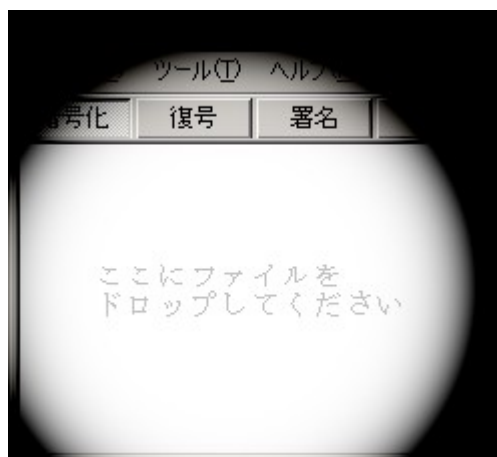
2 ファイルをドロップ

JanusDGX では、特にオプションで指定していない限り、一度に暗号化できるファイルは一つだけです。複数

のファイルやフォルダをまとめて圧縮暗号化したい場合は、あらかじめオプションで「複数ファイルやフォルダを暗号化する」にチェックを入れておいてください。

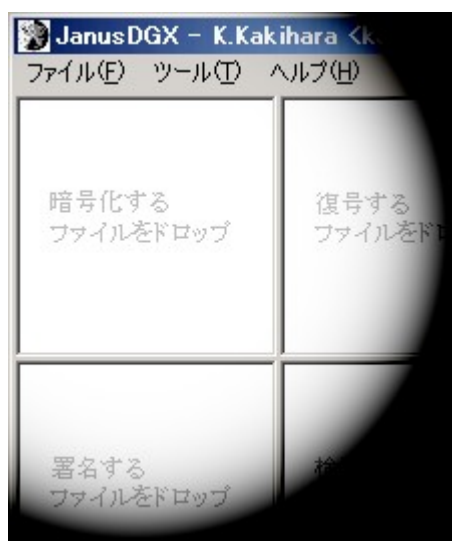
ボタンセレクトモードの場合

暗号化したいファイルをメインウィンドウの「ここにファイルをドロップしてください」という部分にドラッグ&ドロップします。



マルチペインモードの場合

「暗号化するファイルをドロップしてください」と表示されているペインにファイルをドラッグ&ドロップします。



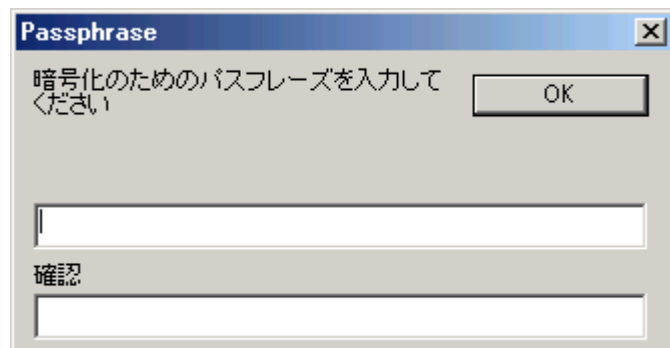
3 暗号化後のファイルの名前の指定

続いて「暗号化後のファイルを指定してください」という画面が現れますので、暗号化後のファイル名を指定してください。

このファイルの種類で「`gpg encrypt symmetric`」を選択しておいてください。

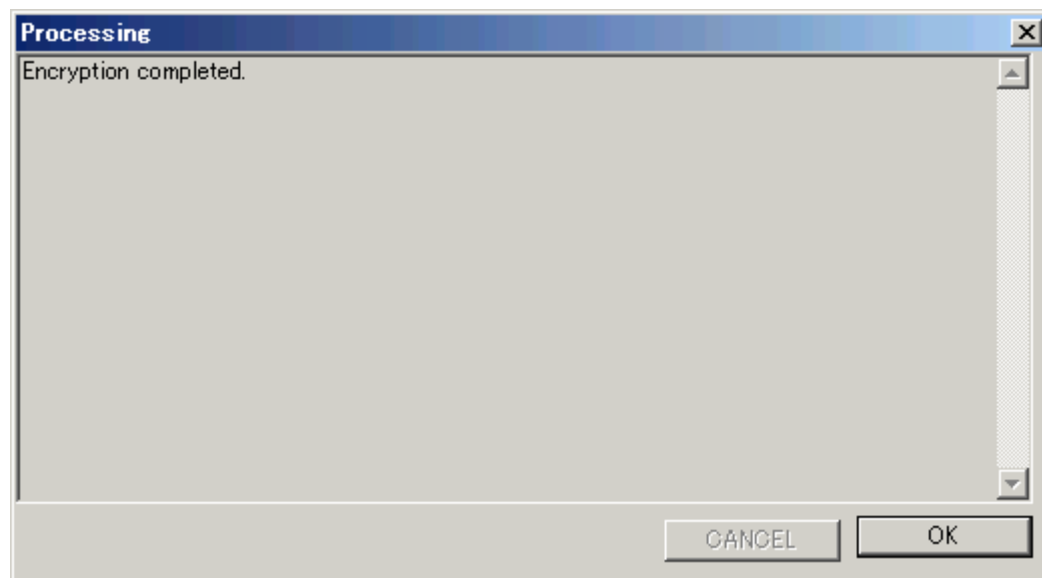
4 パスフレーズの入力

ファイルを暗号化するためのパスフレーズを入力します。GnuPG では、「パスワード」と表現するよりも長い文字列という意味を込めて「パスフレーズ」という用語を使います。パスフレーズは 8 文字以上にしてください。



5 暗号化完了

暗号化プロセスを表示するウィンドウが現れます。ここで「Encryption Completed」と表示されれば暗号化完了です。



7 データの復号

JanusDGX は、与えられた暗号データを元に、復号されたデータを作成するソフトです。元のデータを上書き復号するわけではありません。

1 復号モードにセット

マルチペインモードではこの作業は必要ありません。ボタンセレクトモードの場合のみこの作業が必要になります。

JanusDGX を復号モードにセットします。ツールバーの「復号」ボタンをクリックし、ボタンが押された状態にし

てください。

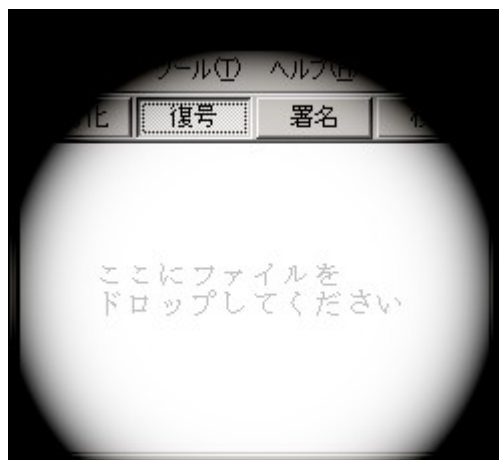


2 ファイルをドロップ

一度に復号できるファイルは一つだけです。

ボタンセレクトモードの場合

暗号化されたファイルをメインウインドウの「ここにファイルをドロップしてください」という部分にドラッグ&ドロップします。



マルチペインモードの場合

「復号するファイルをドロップ」と表示されているペインにファイルをドラッグ&ドロップします。



3 署名検証のための公開鍵の指定

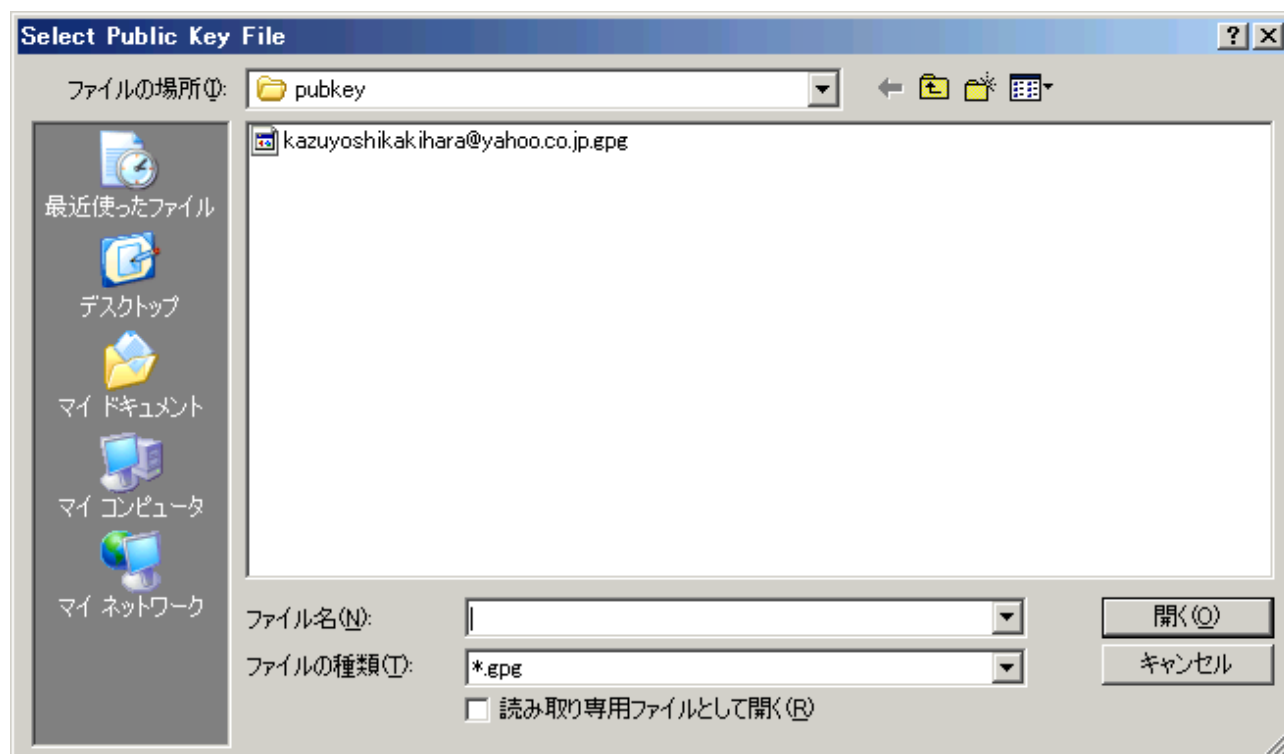
JanusDGX では、暗号ファイルを作成した本人を確認するため、復号の際に暗号ファイルの署名を検証することができます。そのためには、事前に相手の公開鍵を受け取っておき、なおかつ JanusDGX のオプションで「復号時に署名検証する」ように設定されている必要があります。

鍵輪を使用している場合

特別な操作は必要ありません。JanusDGX が自動的に鍵輪の中の公開鍵を検索します。

鍵輪を使用していない場合

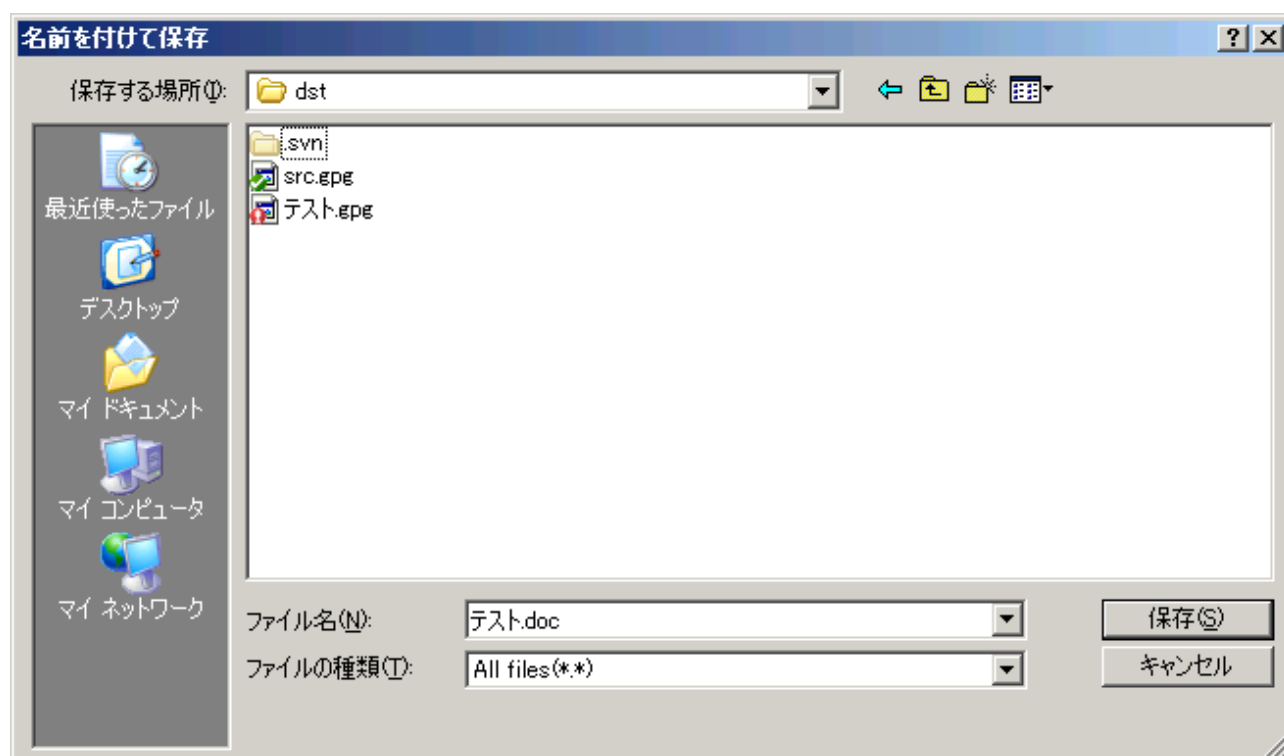
署名検証のための公開鍵を指定する画面が現れます。



暗号化データを作成した人の公開鍵をここで指定してください。

4 復号後のファイルあるいはフォルダの名前を指定

「名前をつけて保存」という画面が現れますので、復号後のファイル名を指定してください。複数のファイルをまとめて暗号化してあった場合は、ここで展開先のフォルダ選択の画面が現れます。



ここでファイル名を指定して「保存」をクリックするとファイルが復号されます。

8 署名ファイル作成

この機能はオプションで「署名機能を使う」設定になっていないと使えません。

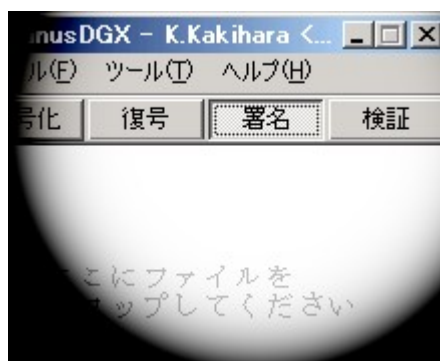
電子署名は公開鍵暗号の応用技術です。ファイルを暗号化するのではなく、電子署名を付けることによって正真性(本人が作成しており、移送途中に変更が加えられてはいないこと)を証明することができます。たとえば、身分証明書など、誰もが読める状態でなければ困るが、データの正真性だけは保証しておきたいというような場合に使います。

データが偽造されていない証拠として、チェックサムをさらに複雑化したような署名ファイルを JanusDGX は作成することができます。相手はやはり JanusDGX を使用して、データの正真性を確認することができます。

1 署名作成モードにセット

マルチペインモードではこの作業は必要ありません。

JanusDGX を署名モードにセットします。ツールバーの「署名」ボタンをクリックし、ボタンが押された状態にしてください。



2 ファイルをドロップ

署名ファイルを作成できるファイルは一度に一つだけです。

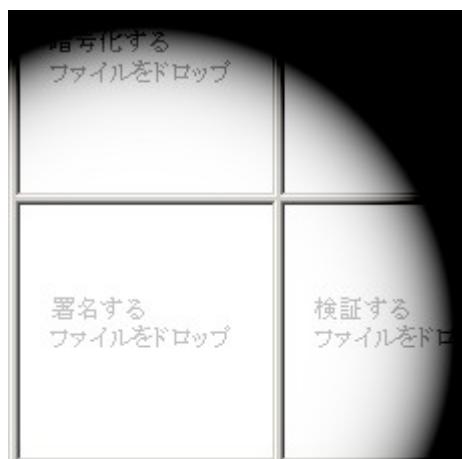
ボタンセレクトモードの場合

署名したいファイルをメインウインドウの「ここにファイルをドロップしてください」という部分にドラッグ&ドロップします。



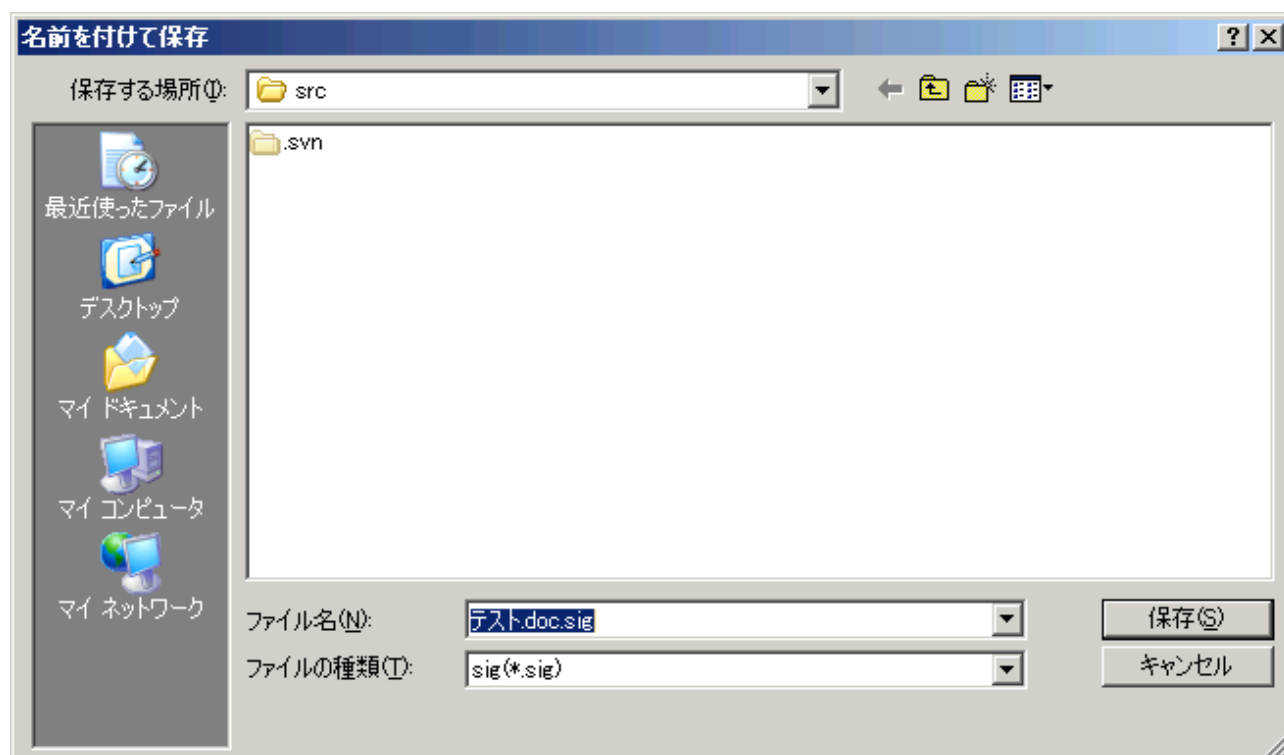
マルチペインモードの場合

「署名するファイルをドロップ」と表示されているペインにファイルをドラッグ&ドロップします。



3 署名ファイルの名前の指定

「名前をつけて保存」という画面が現れますので、作成したい署名ファイルの名前を指定してください。



ここで「保存」をクリックすると署名ファイルが作成されます。

相手には元のファイルと署名ファイルをセットにして届けます(初めての相手には自分の公開鍵もあわせて届ける必要があります)。

9 署名の検証

相手から受け取ったファイルを、署名ファイルと照合することによって、正真性を検証します。

これにはあらかじめ相手の「公開鍵」を入手しておく必要があります。

(鍵輪を使用している場合は相手の公開鍵を鍵輪にインポートしておいてください)

1 署名検証モードにセット

マルチペインモードではこの作業は必要ありません。

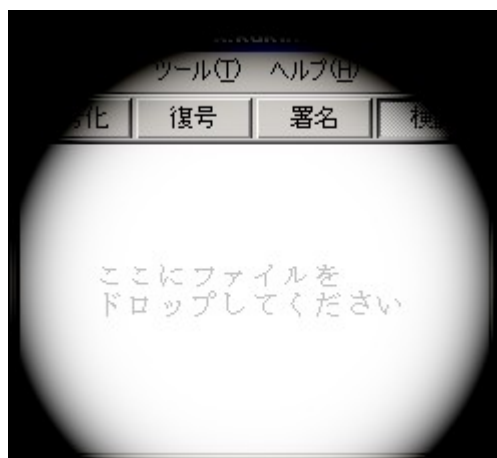
JanusDGX を署名検証モードにセットします。ツールバーの「署名検証」ボタンをクリックし、ボタンが押された状態にしてください。



2 ファイルをドロップ

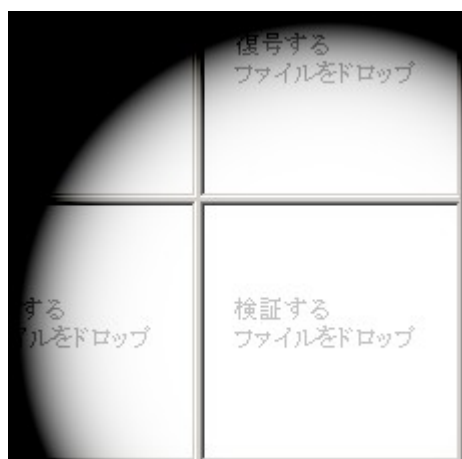
ボタンセレクトモードの場合

署名を検証したいファイル(署名ファイルではなく、ファイル本体のほう)をメインウインドウの「ここにファイルをドロップしてください」という部分にドラッグ&ドロップします。一度に署名検証できるファイルは一つだけです。



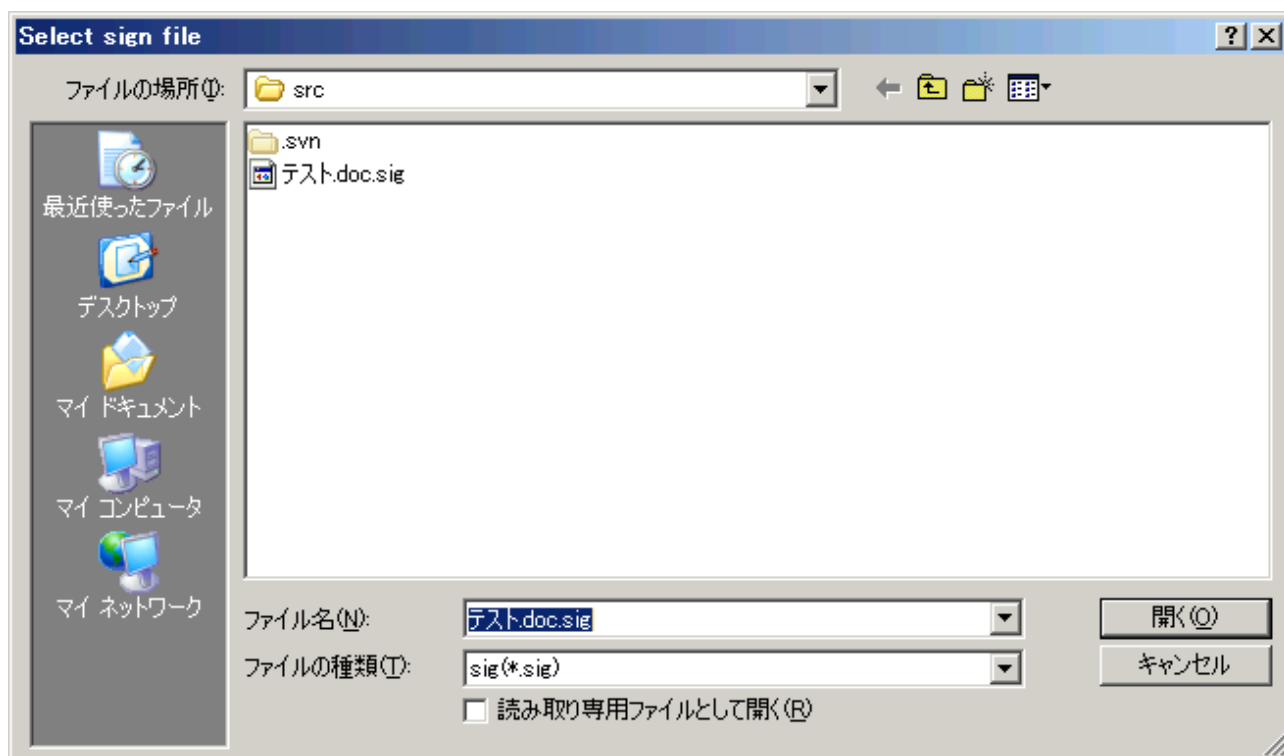
マルチペインモードの場合

署名を検証したいファイル(署名ファイルではなく、ファイル本体のほう)を「検証するファイルをドロップ」と表示されているペインにドラッグ&ドロップします。一度に署名検証できるファイルは一つだけです。



3 署名ファイルを指定

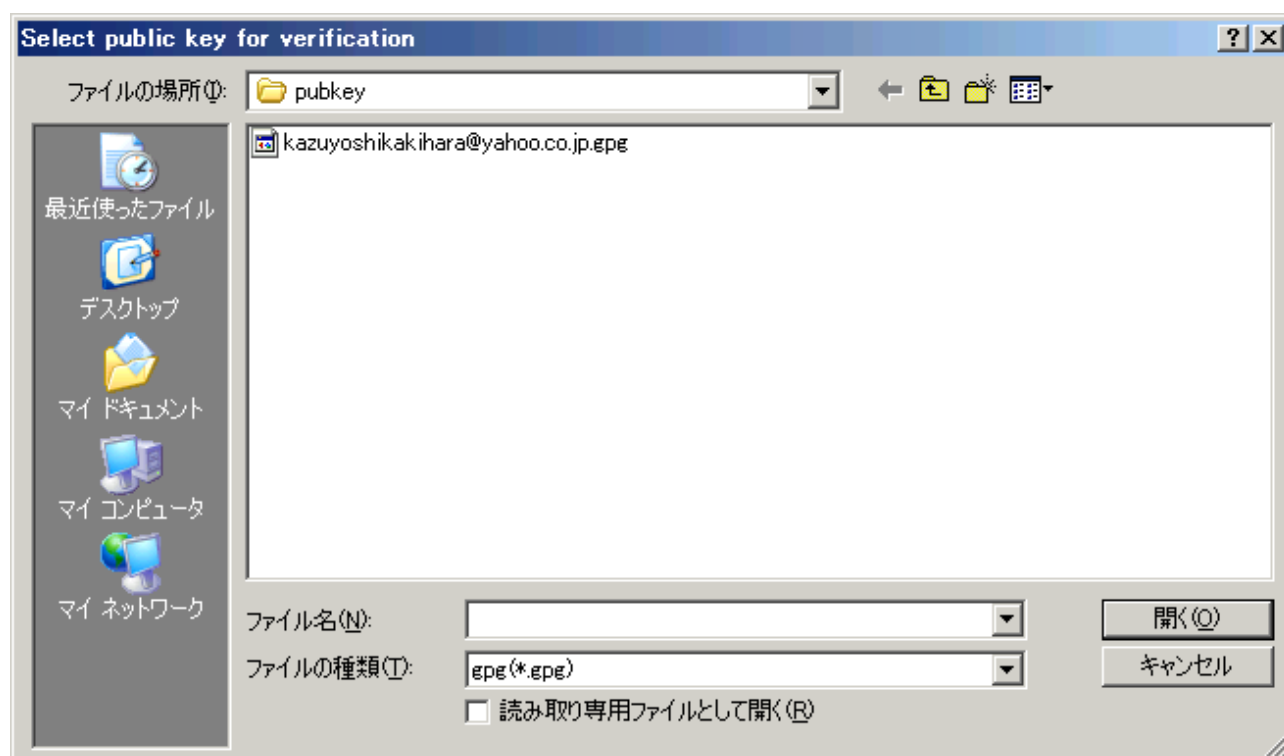
「Select sign file」という画面が現れますので、ファイル本体と対になる署名ファイルを指定してください。



4 公開鍵ファイルを指定

鍵輪を使っている場合はこの作業は必要ありません。JanusDGX が自動的に鍵輪の中の公開鍵を検索します。

鍵輪を使っていない場合は、「Select public key for verification」という画面が現れますので、ファイルに署名した人の公開鍵ファイルを指定してください。



5 検証実施

問題がなければ検証された鍵が表示され、最後に「File Verifed」と表示されます。

10 その他の機能

1 受け取った公開鍵が本物かどうかの確認

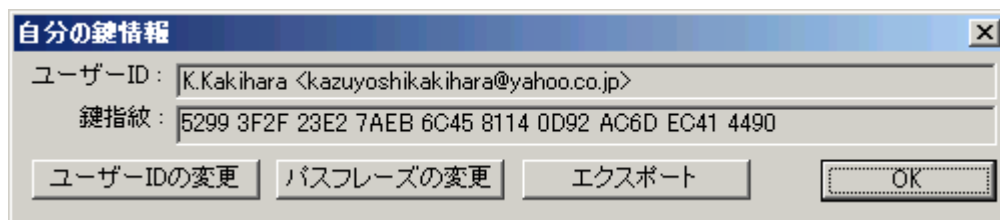
緊急の場合、電子メールなど、途中で改ざんされる恐れのあるような方法で公開鍵をやり取りすることがあるかもしれません。このような場合、公開鍵を使用する前に、それが本当に本物かどうかを確認する必要があります。

この作業には、電話、FAX 等、安全な通信経路が確保されている必要があります。

鍵輪を使用していない場合

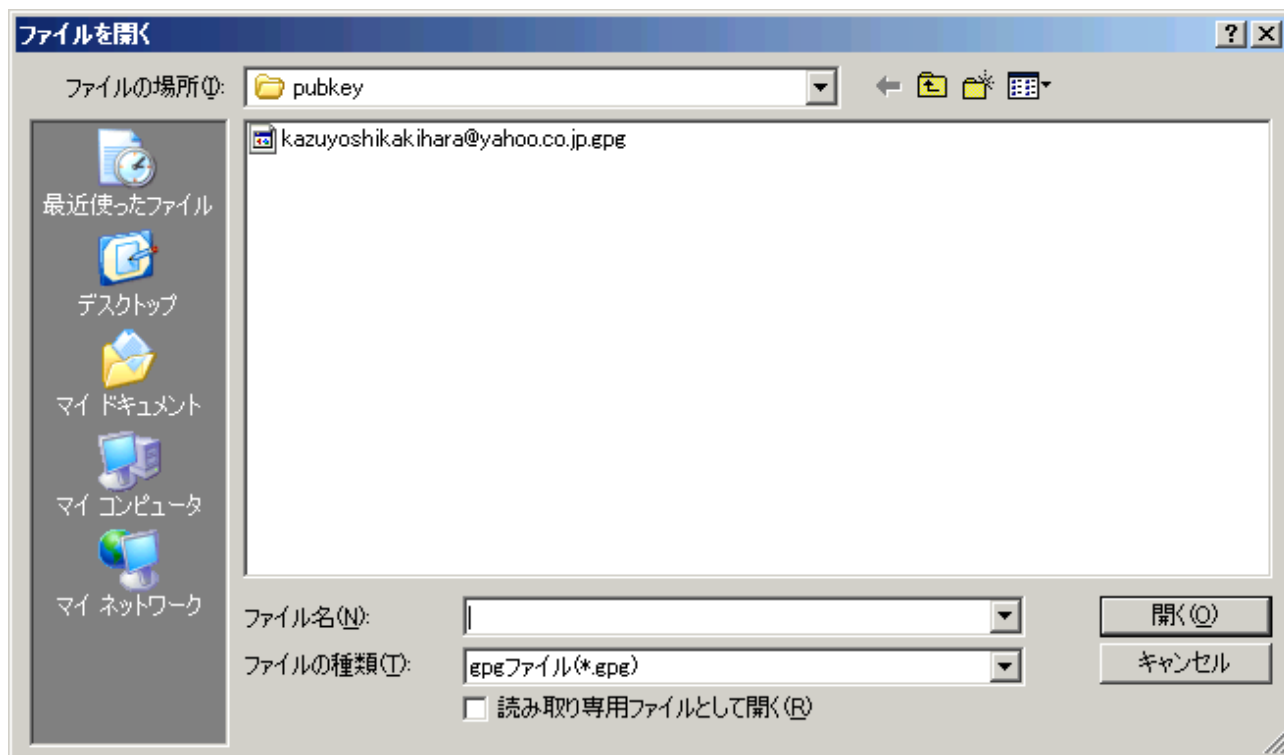
公開鍵を送った側の操作

公開鍵を送った側は JanusDGX を起動し、メニューの「ツール」から「自分の鍵の情報」を選択し、「鍵指紋」を表示させます。

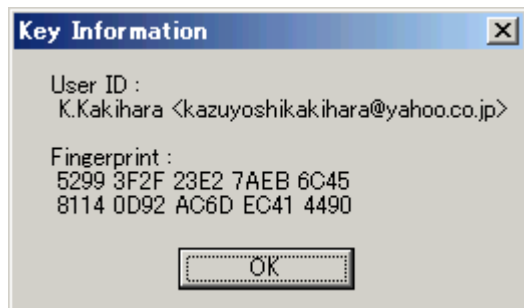


公開鍵を受け取った側の操作

公開鍵を受け取った側は JanusDGX を起動し、メニューの「ツール」から「公開鍵の情報」を選択し、受け取った鍵ファイルを指定することで、受け取った鍵の鍵指紋を見ることができます。



この例では kazuyoshikakihara@yahoo.co.jp.gpg という鍵ファイルの鍵指紋を見ようとしています



ここで表示されているのは K.Kakihara の鍵指紋です。

こうしてお互いに鍵指紋を表示させ、比較することで鍵が本物かどうか確認することができます。

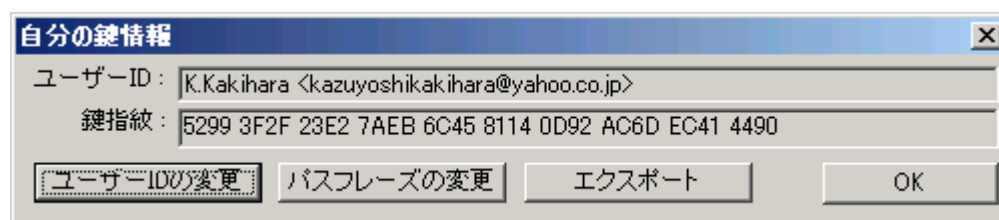
鍵輪を使用している場合

公開鍵を鍵輪にインポートすると、送られた公開鍵の鍵指紋を見ることができます。

これを鍵輪を使用していない場合と同様、鍵を送った相手の「自分の鍵の情報」の鍵指紋と照合します。

2 ユーザー名、メールアドレスの変更

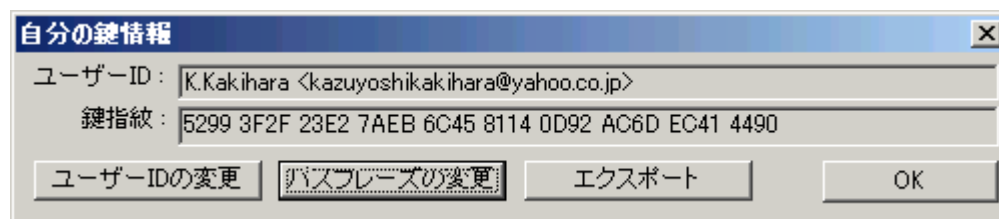
メニューの「ツール」の「自分の鍵の情報」で「ユーザー ID の変更」を選択してください。



3 秘密鍵へのパスフレーズの付加・変更

JanusDGX ではユーザーの秘密鍵を守るため、パスフレーズを付加して、パスフレーズを知った人でなければ秘密鍵を使用できなくすることができます。

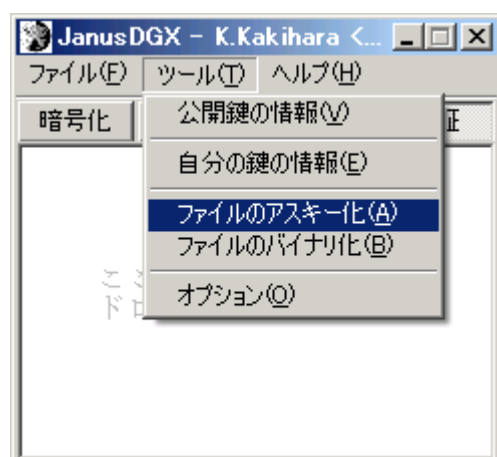
メニューの「ツール」の「自分の鍵の情報」で「パスフレーズの変更」を選択してください。



4 ファイルのアスキー化

JanusDGX で書き出した暗号ファイルや鍵を必要に応じて、メールなどに添付するためにテキストデータに変換することができます。

メニューの「ツール」の「ファイルのアスキー化」を選択し、データをテキスト化してください。

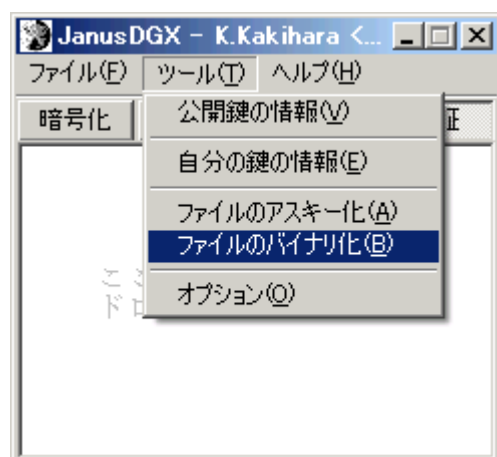


5 ファイルのバイナリ化

「ファイルのアスキー化」機能でテキストデータに変換されたデータを JanusDGX で取り扱えるバイナリ形式のファイルに変換します。

メニューの「ツール」の「ファイルのバイナリ化」を選択肢、データをバイナリ化してください。

(暗号データの復号および鍵のインポートの場合は、テキストデータのままで使用できますのでバイナリ化の必要はありません)



6 鍵のバックアップ

JanusDGX 運用フォルダ内の conf というフォルダ内に自分の秘密鍵が格納されています。

また、受け取った公開鍵は基本的に pubkey フォルダに格納されているはずです。

これらのフォルダをまるごとどこかの媒体にコピーすれば、バックアップになります。

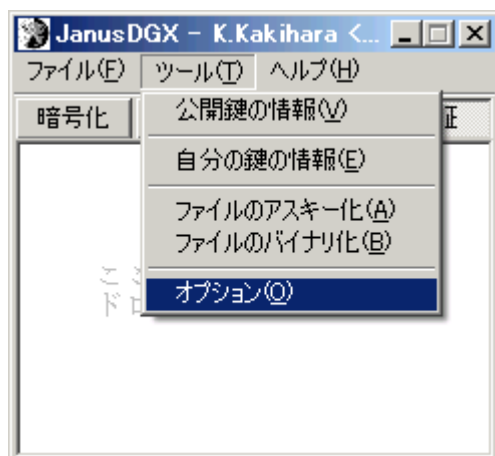
バックアップからのデータのリストアには、これらのデータを元の位置に上書きコピーします。

11 カスタマイズ

1 カスタマイズの方法

JanusDGX を起動してカスタマイズ

JanusDGX を起動し、「ツール」から「オプション」を選ぶことで、オプション選択の画面が現れます。



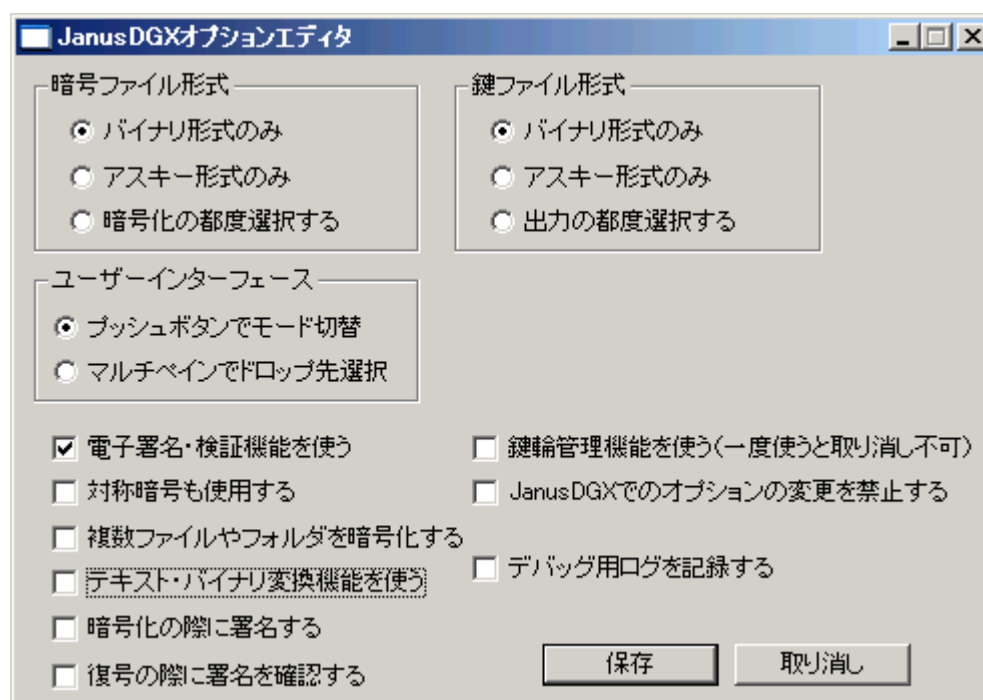
オプションエディタを使用

JanusDGX を一度でも起動してしまうと、自動的に秘密鍵・公開鍵を作らなければならなくなってしまいます。この状態でカスタマイズした JanusDGX を再配布すると、操作を誤った場合、自分の秘密鍵を漏洩してしまう恐れがあります。

このような事故を防ぐため、JanusDGX では、ダウンロード後、一度も JanusDGX を起動することなくオプション項目を変更できるよう、オプションエディタが付属しています。

JanusDGX.exe と同じフォルダにある JanusDGXop.exe を実行してください。

JanusDGX には、オプションエディタを使わなければ変更できないオプション項目もあります。



2 カスタマイズして再配布

JanusDGX では、1 次配布サイトからダウンロードするだけでなく、ダウンロードした人が JanusDGX を使いやすいようにカスタマイズし、知人やビジネス上の取引先に再配布するという利用方法もあらかじめ考慮しています。

JanusDGX をダウンロードしたら、「一度も JanusDGX を起動せず」、オプションエディタ JanusDGXop.exe を起動してください。一度でも JanusDGX を起動してしまうと、強制的に秘密鍵・公開鍵が生成されてしまいます。この状態で操作を誤ると、自身の秘密鍵を漏洩してしまいかねません。

オプションエディタを使用してカスタマイズ項目をセットした後、保存してオプションエディタを終了すると、そのカスタマイズした設定が JanusDGX に反映されます。

この状態で、JanusDGX のパッケージを圧縮し、再配布することで、カスタマイズ後の JanusDGX を相手に使用させることができます。

3 カスタマイズ項目

暗号ファイル形式

暗号ファイルの形式を、GnuPG 本来のバイナリ形式にするか、メール等に添付しやすいテキスト形式にするか、あるいは、ファイル暗号化の都度ユーザーに選択させるか、選択することができます。

バイナリ形式でもテキスト形式でも、特に区別することなく JanusDGX は扱うことができます。

鍵ファイル形式

公開鍵をエクスポートする際のファイル形式を、GnuPG 本来のバイナリ形式にするか、メール等に添付しやすいテキスト形式にするか、エクスポートの都度ユーザーに選択させるか、選択することができます。

暗号ファイル形式とは違い、ここでテキスト形式を選択すると、「鍵輪管理機能を使う」か、「テキスト・バイナリ変換機能」を使ってファイルを一度バイナリ化しないと、鍵が使えませんので注意してください。

ユーザーインターフェース

「プッシュボタンでモード切替」か、「マルチペインでドロップ先選択」かを選択することができます。

「プッシュボタンでモード切替」を選択すると、ファイルのドロップ先のウィンドウが一つとなります。事前にプッシュボタンで「暗号化」「復号」などの機能を選択したうえでファイルをドラッグ&ドロップすることになります。

「マルチペインでドロップ先選択」を選択すると、「暗号化」「復号」などの機能ごとのペインが現れます。ファイルを暗号化したり、復号したりといった目的に応じてそれぞれのペインにファイルをドラッグ&ドロップすることになります。

電子署名・検証機能を使う

このチェックを外すと、電子署名・検証関連の機能が使えなくなります。

電子署名・検証関連の機能が画面からも消えますので、「暗号化」「復号」機能だけしか使いたくないユーザーにとっては、画面がすっきりして使いやすくなります。

対称暗号も使用する

このチェックを外すと、暗号化方式として、対称暗号が選択できなくなります。

相手にどうしても対称暗号を使用させたくない場合(暗号に不慣れでなかなか適切なパスフレーズを設定できない場合)など、このチェックを外して使用してください。

複数ファイルやフォルダを暗号化する

このチェックを外すと、一度に暗号化できるのはファイル一つだけになります。チェックを入れると、`gpg-zip`形式で複数ファイルやフォルダを自動的に一つのファイルにとりまとめて暗号化することができるようになります。

テキスト・バイナリ変換機能を使う

GnuPG 本来のバイナリ形式で暗号化したバイナリファイルをテキストデータ化したり、あるいはその逆をしたりする機能を使うかどうか選択できます。

鍵のファイル形式に「テキスト形式」を選択した場合、鍵輪管理機能を使うか、このテキスト・バイナリ変換機能を使って公開鍵ファイルをテキストデータ化しなければ、その鍵を使用することはできません。

暗号化の際に署名する

このチェックを入れると、公開鍵方式でファイルを暗号化する際、暗号化したひとの正真性を保証するための電子署名が自動的にファイルに組み込まれるようになります。

復号の際に署名を確認する

このチェックを入れると、暗号ファイルを復号する際に、ファイルに施された電子署名を毎回確認するようになります。

鍵輪管理機能を使う

この機能は一度でも使ってしまうと、二度とオフにすることができませんので注意してください。このチェックを入れると、GnuPG 本来の鍵輪管理機能が使えるようになります。

JanusDGX でのオプション変更を禁止する

このオプション項目は、オプションエディタを起動した際にのみ表示されます。JanusDGX の「ツール」で「オプション」を選択した場合には表示されません。

このチェックを入れると、JanusDGX のメニューから「オプション」の項目が消え、ユーザーは JanusDGX のオプション項目を一切変更できなくなります。

デバッグ用ログを記録する

このチェックを入れると、JanusDGX の使用中にエラーが生じた場合、その最終ログがファイルに書き出されるようになります。

JanusDGX にバグを見つけた場合はこの機能をオンにして、なるべく詳細な情報を作者まで連絡してください。

12 バグの報告についてお願い

JanusDGX を使用していて、動作がおかしい場合は kazuyoshikakihara@yahoo.co.jp 宛お知らせいただけると幸いです。

ご報告いただける範囲で結構ですのなるべく

- JanusDGX のバージョン
- OS(Microsoft Windows XP Home Edition、Vista Business Edition など)
- 何をしたいくてどのような操作をしたか
- その結果どのようになったか(どのようなエラーメッセージが表示されたか)
- その現象は再現するか

以上の項目をお知らせください。

また、現象が再現可能であれば、

- JanusDGX のオプションエディタ(JanusDGX.exeと同じフォルダにある JanusDGXop.exe)で「デバッグ用ログを作成」にチェックを入れて保存、終了。
- JanusDGX 本体を起動し、エラー再現。
- JanusDGX.exeと同じフォルダにできている debug.log および gpgstatus.log(ない場合もあります)をメールに添付。

していただければ助かります。

debug.log および gpgstatus.log はテキストファイルです。中を開いて特に都合の悪い項目があるようでしたら、「XXX」などの文字で上書きしていただいて結構です。

2007.12.24

Kazuyoshi Kakihara<kazuyoshikakihara@yahoo.co.jp>

以上