PGP ®

for Personal Edition Windows User's Guide Version 5.5

Windows 9x/NT 用ユーザガイド　ネットワークアソシエイツ株式会社

PGP for Personal Edition, Version 5.5 for Windows 9x/NT

ライセンス契約書のシリアル番号を余白に記録してください。

本ソフトウェアの一部は米国特許 No. 4.200.770, 4.218.582, 4.405.829 および 4.242.414 に記載され、Public Key Partners が独占ライセンスをもつ公開キーアルゴリズム、米国特許 No.3.214.703 に記載され Ascom Tech AG からライセンスされた IDEA 暗号法の暗号文、Northern Telecom Ltd., からライセンスされた CAST 暗号化アリゴリズムを使用しています。IDEA は Ascom Tech AG の登録商標です。PGP の圧縮コードは Mark Adler と Jean-loup Gaily によるもので、Info-Zip フリーソフトから許可を得て使用されています。LDAP ソフトウェアはミシガン大学 (Ann Arbor) の好意で提供されました (Copyright 1992-1996.Regents of the University of Michigan. All rights reserved) 。ネットワーク・アソシエーツ・インターナショナルは本ソフトウェアまたは説明書の内容を対象とする特許を保有または特許申請中である可能性があります。本ソフトウェアまたは説明書の供給はお客さまに対してこれら特許に関しなんらのライセンスを与えるものではありません。

本書とともに配布されたソフトウェアはエンドユーザライセンス約款及びかかる約款記載の限定保証の下でお客様の個人的使用向けにライセンスが許諾されています。本書の内容は予告なく変更することがあります。ネットワーク・アソシエーツ・インターナショナル及びネットワークアソシエイツ株式会社のいずれも、本書の内容がお客様の要請を満たしていること、あるいは内容に間違いがないことにつき保証いたしません。技術的な不正確さ、誤字・脱字が含まれていることがあります。内容の変更、修正は本書の改訂版に反映される場合があります。

本ソフトウェア及び説明書の輸出は、特定の製品及び技術データの輸出、再輸出を規制する米国商務省輸出管理局によって随時発布される規制や条例により規制される場合があります。**なお、本ソフトウェア及び説明書の日本からの輸出については、日本の外国為替及び外国貿易法およびその規則による規制の対象となります**。

ネットワークアソシエイツ株式会社

〒105　東京都港区虎の門 3-8-21　虎の門 33 森ビル

TEL:03-5408-0700
FAX:03-5408-0780

http://www.nai.com/japan/

はじめに

このマニュアルは Windows 9x および NT 版 PGP for Personal Edition 5.5 の使い方を説明しています。PGP 5.5 で追加された新しい機能については、第 1 章「PGP for Personal Edition の紹介」で説明します。

このマニュアルでは重要な事項に次のような記号を使用しています。

注：例えば PGP/MIME 形式を使っていない場合は、メッセージを送信する前に Windows エクスプローラから添付ファイルとして送信したいファイルを暗号化しなければならないなど、PGP の使い方について補足説明をします。

ヒント：有効なパスフレーズの作成方法など、PGP を効率よく使うためのガイドラインを教えます。

警告：PC を使っている同僚にあなたのキーを送信する場合は、８文字以内のファイル名と３文字のファイル拡張子（例 :e-mail.txt）を入力することなど、約束のロスを防ぐための情報を提供します。

PGP について

PGP およびその製品についての資料は次の方法で入手できます。

PGP ホームページ

PGP は製品、PGP の構成、製品の最新情報およびプライバシー問題などの関連トピックについての情報を PGP ホームページでお知らせしています。ホームページのアドレスは www.nai.com/japan/ です。

サポート

PGP 製品についてのテクニカルサポートは、パッケージ版は 03-5408-0702 までお問い合わせてください。

テクニカルサポートへお電話される時、次の点を確認してからお電話下さい。

- 製品名およびバージョン
- お使いのコンピュータのメーカーおよび機種
- お使いのオペレーティングシステムおよびバージョン
- 問題が発生している場合、その具体的な再現手順

製品に対するご意見、ご要望について

当社では PGP を一層充実させるために改良を重ねており、新バージョン設計についてお客さまのご意見を参考にしています。PGP についてのご感想、製品の内容、機能についてのご意見をお寄せください。特にコーポレート設定用の製品を強化する予定です。お寄せいただいたご意見、ご要望は機能豊富で使いやすいソフトウェアおよびサービスの開発に反映させていただきます。すべてのご提案にお応えすることはできませんが、今後の製品開発の参考とさせていただきます。

目次

第 1 章

PGP for Personal Edition の紹介

PGP へようこそ。Windows 9x および Windows NT 版 PGP for Personal Edition を利用すれば、email メッセージと添付ファイルを宛先の受信人だけが読み取れるように暗号化することで、簡単にしかも確実にプライバシーを保護できます。メッセージとファイルに電子署名を入れ、その認証を保証することもできます。署名入りメッセージはその内容がどうにも改竄されていないことを検証します。

PGP 5.5 の新しい機能とは

PGP 5.5 には次の新しい機能が追加されました。

- 受信人グループを作成できます。－人々のキーのグループを選び、全員へのメールを同時に暗号化できます。
- 新しいキー検索ウィンドウ　－キーホルダーを検索するときに使うのと同じユーザインターフェイスを使って、リモートサーバ上のキーを探すことができます。

- 新しい PGP ツール　－ Windows エクスプローラからファイルの暗号化、署名、復号、認証または完全削除できるようになりました。
- PGP 完全削除機能　－　ソフトウェアツールを使ってファイルを修復できないように上書きします。
- 構成可能な〔表示〕メニュー　－キーホルダーのキーの詳細を表示します。
- 新しいキー署名機能　－署名しようとするキーの所有者が信頼する紹介者またはメタ紹介者かを選べます。署名がエクスポート可（つまりキーサーバまたはキーのコピー先位置から表示可能）　、あるいはエクスポート不可（つまりあなたは署名を表示できるが他の人はできない）　も選択できます。

PGP 5.5 マニュアルセットの新しいものは

このガイドは PGP 5.5 について説明します。PGP マニュアルセットには次の新しいマニュアルが追加されました。

- ユーザ製品向けマニュアルには概念的な説明と PGP の操作手順が含まれます。PGP ユーザ製品のオンラインヘルプはプラグイン毎に作成され、各プラグインでの PGP の使い方を詳しく説明しています。
- Windows 版 PGP 5.5 にはオンラインヘルプが添付され、PGP 5.5 の CD-ROM には Adobe Acrobat 形式の電子マニュアルが保存されています。

PGP の使い方

もっとも便利な PGP の使い方の１つは、プラグインによってサポートされるポピュラーな email アプリケーションから操作する方法です。電子メールアプリケーションを使ってボタンをクリックしてメールを作成したり読みながら、メッセージを暗号化して署名を入れたり、解読して検証することができます。

プラグインによってサポートされていない email アプリケーションを使っている場合は PGP ツールを使って PGP 機能をファイル上で実行できます。大事なデータが修復できないように、PGP を使ってファイルを暗号化、署名して、コンピュータのハードディスクに安全に保管することもできます。

概要

PGP は公開キー暗号法といわれる広く認められた暗号化技術を採用しており、２つの補足しあうキーが安全な通信の維持に使われます。１つのキーはあなたしかアクセスしない秘密キーに指定され、もう１つのキーはあなたが他の PGP ユーザと自由に交換できる公開キーです。秘密キーと公開キーは両方ともキーホルダーファイルに保存され、〔PGP キー〕ウィンドウからアクセスできます。このウィンドウからキーの管理機能をすべて実行します。

誰かにプライベートな email メッセージを送信するには、その人の公開キーのコピーを使って情報を暗号化します。その情報はその人だけが秘密キーを使って解読できます。逆に、誰かがあなたに暗号化したメールを送信したい場合は、あなたの公開キーのコピーを使ってデータを暗号化します。そのデータはあなただけが秘密キーのコピーを使って解読します。さらに PGP を使ってコンピュータに保存されたファイルを暗号化したり、それらに署名を入れて変更されていないことを認証できます。

また、他の人に送信する email に署名を入れたり、ファイルに署名を入れて認証するときにも秘密キーを使います。受信人はその後、あなたの公開キーのコピーを使って、あなたが本当に email を送ったかどうか、それが転送中に変更されたかどうか調べることができます。誰かがあなたに電子署名入りの email を送信した場合、公開キーのコピーを使って電子署名を調べ、誰も改竄していないことを確認します。

PGP プログラムを利用することで、キーを簡単に作成、管理でき、電メールのメッセージ、ファイルおよび添付ファイルの暗号化と署名、解読と確認のあらゆる機能をアクセスできます。

この項の残りでは、PGP を操作中に普通行う手順をざっと説明します。詳しい手順は本書の該当する章を参照してください。

秘密&公開キーペアの作成

PGP の操作を始める前に、キーペアを作成する必要があります。PGP キーペアはあなただけがアクセスする秘密キーと、あなたがコピーして情報を交換する誰もが自由に利用できるようにする公開キーで構成されます。

新しいキーペアは、PGP のインストール手順の終了後すぐに作成オプションがでます。または PGP キーアプリケーションを開いていつでも作成できます。

公開キーを他の人のキーと交換

キーペアを作成した後、他の PGP ユーザと通信を開始できます。あなたは他のユーザの公開キーのコピーが必要で、相手はあなたの公開キーが必要です。あなたの公開キーはテキストブロックなので、誰かとキーをやりとりするのは簡単です。公開キーを email のメッセージに入れる、ファイルにコピーする、公開キーサーバまたはコーポレートキーサーバに掲示して読みたいときに誰でも入手できるようにできます。

キーの有効性の確認

誰かの公開キーのコピーを持っているならば、それをあなたの公開キーホルダーに追加できます。その後、キーが改竄されていないこと、実際に所有者と称している人のものであるか確認するためチェックしなければなりません。これは、誰かの公開キーのコピーにあるユニークな指紋とその人のオリジナルのキーの指紋を照合して行います。有効な公開キーを持っていることが分かったら、キーに署名して安心して利用できるとことを示します。その上で、キーの所有者に、誰か他の人の公開キーの認証を保証するその人をあなたがどの程度信用しているかを示す信用度を授与できます。

email とファイルの暗号化と署名

キーペアを作成し、公開キーを交換した後、email のメッセージとファイルの暗号化と署名を開始できます。

- プラグインによってサポートされる email　アプリケーションを使っている場合はアプリケーションのツールバーから適当なオプションを選び、メッセージを暗号化し、署名できます。

- email アプリケーションがプラグインによってサポートされていない場合は、メッセージをクリップボードへコピーし、そこで適切な機能を実行します。ファイルを email に添付する前に Windows エクスプローラから暗号化し、署名する、ファイルを暗号化してコンピュータに安全に保管する、ファイルに署名して改竄されていないことを検証することもできます。

email とファイルの復号化と認証

誰かがあなたに暗号化された email を送った場合、メールの内容を解読し、書かれたサインを調べて、データが送信人本人で発信されたものか、変更されていないことを確認できます。

- プラグインによってサポートされる email アプリケーションを使っている場合は、アプリケーションのツールバーから適当なオプションを選び、メッセージを復号化し認証できます。
- email アプリケーションがプラグインによってサポートされていない場合は、メッセージをクリップボードへコピーし、そこで適切な機能を実行します。添付ファイルを復号化し認証したい場合は、Windows エクスプローラから実行できます。コンピュータに保存された暗号ファイルを復号化し、署名入りファイルを認証して改竄されていないことを確認できます。

ファイルの完全削除

ファイルを完全に削除する必要があるときは、Secure Wipe 機能を使って、ファイルを修復不能にできます。ファイルは直ちに上書きされるので、ディスク修復ソフトウェアを使って回収できません。

第 2 章

操作を始める前に

この章では PGP の操作方法について説明し、本製品を使用するときに一般に行う手順をおおまかに説明します。PGP キーで使われるアイコン表もあります。

システムの動作環境

PGP 5.5 をインストールするときに必要なシステムの動作環境は次のとおりです。

- Windows 9x または NT（4.0 以降）
- 8 MB RAM
- 15 MB のハードディスク

PGP for Business Security 5.5 について

PGP for Business Security 5.5 を使用する場合、組織のアドミニストレータはたぶん MIS ディレクタ、ネットワーク管理者または MIS アドミニストレータを兼任しているでしょうが、〔PGP アドミニストレーション〕ウイザードを使います。〔PGP アドミニストレーション〕ウイザードは組織内のユーザ用のさまざまな設定オプションを提供します。このオプションにはコーポレート署名キーとマスタ復号キーが含まれます。「コーポーレート署名キー」は、ユーザ全員が他のキーに署名するために信頼するシステム全体のキーとしてアドミニストレータが設計する公開キーです。コーポレート署名キーが署名したキーは信用でき、コーポーレート署名キーが署名していないキーは用心しなければなりません。

PGP では「信頼する紹介者」という概念を取り入れています。これは、あなたに有効なキーを提供してくれると信用できる人です。この概念はビクトリア時代の小説でおなじみのもので、当時の人々は紹介状をお互いに与えました。例えば、あなたのおじさんに遠く離れた町に住む知人がいて、あなたはその人と商売をしたいとします。このとき、おじさんはその知人に紹介状を書きます。PGP を使った場合、ユーザはお互いのキーに署名を入れ、有効であることを示します。誰かのキーに署名して、そのキーが有効であること、つまり本当にその人のキーであることを示します。第 1 章「PGP for Personal Edition の紹介」で説明したように、これはいくつかの方法で行えます。信頼する紹介者が別の人のキーに署名した場合、彼らが署名したキーは有効であると信頼でき、彼らのキーを使う前に確認する必要はないと考えられます。

PGP 5.5 は「*メタ紹介者*」という概念もサポートしています。これは信頼する紹介者の信頼する紹介者です。大企業で働いてる場合、地区アドミニストレータ、すなわちユーザのキーに署名する信頼する紹介者がいます。これらのキーは、地区アドミニストレータが妥当性を確認するための動作を行ったので、有効と信頼できます。組織には、地区セキュリテイ責任者と協力する本部アドミニストレータがいることもあり、西海岸の事務所の人は東海岸の事務所の人を信頼できます。どちらのキーもそれぞれの地区アドミニストレータが署名しているからです。次に、メタ紹介者であるヘッドアドミニストレータがキーを署名しました。このように組織内の信頼性階層の構築できます。

新しいユーザインターフェイスと他の改良点とともに、PGP 5.0 v. と 5.5 は２種類のキーをサポートしています。すなわち RSA と Diffie-Hellman です。PGP 5.0 v 以前は、RSA キーを選べるだけでした。PGP は現在、Diffie-Hellman 暗号化と DSS 電子署名技術をベースにしたキーを提供しています。キーの DSS 部分は署名に使われ、Diffie-Hellman 部分は暗号化に使われます。

PGP 5.0 v 以降を使っている人と email を交換する場合、Diffie-Hellman キーがより強力なセキュリティなどの補助セキュリティ機能を提供します。その上、PGP は、Diffie-Hellman キーへの暗号化では高速処理を行います。

ところが、RSA 暗号化アルゴリズムを使って作成したキーを使っている人と email を交換する必要がある場合は、RSA キーを作成または予約する必要があります。

複数の受信人への email を暗号化する場合、RSA キーを持っている人と DSS/Diffie-Hellman キーを持っている人がいるときは、email は各人に適切なキーを使って暗号化されます。ただし、古いバージョンの PGP を使っている人がこの email を復号化し、検証できるようにするには、まず、この制限をなくした寄せ集めバージョンの１つにアップグレードする必要があります。

PGP/MIME の使い方

PGP/MIME は、PGP 機能をポピュラーな email アプリケーションに直接組み込んでいる一部のプラグインの標準です。PGP/MIME を提供するプラグインによってサポートされる email アプリケーションを使っている場合、email を送信するときに、email メッセージと添付ファイルを暗号化し、署名し、受信するときに自動的に復号化し、確認できます。

ただし、PGP/MIME 形式の email の送信前に、受信人がこの標準をサポートする email アプリケーションを使っているか確認のためチェックしてください。使っていない場合は受信人があなたのメッセージの復号化と確認できないことがあります。また、PGP/MIME 形式を使わずにメッセージとファイルを暗号化することもできます。これには、このオプションを選択メニューで選択しないままにします。

古いバージョンからアップグレードする

PGP の古いバージョン（PGP, Inc または ViaCrypt）からアップグレードするときは、PGP をインストールする前に古いプログラムファイルを削除し、ディスク空間をあけます。そのとき、古いバージョンを使って作成または収集したキーを保存しておいた秘密＆公開キーホルダーファイルを削除しないように注意してください。PGP をインストールしたとき、既存の秘密＆公開キーホルダーを保持するか選択できるので、古いキーをすべてインポートする面倒は起こりません。この項で説明する手順を行って、古いバージョンからアップグレードしてください。

PGP 2.6.2 または 2.7.1 からのアップグレード

1. 現在コンピュータで起動中のプログラムをすべて終了させます。
2. 古い PGP　　キーホルダーを別のボリュームにバックアップします。公開キーは pubring.pgp に、秘密キーは secring.pgp に保存されています。

キーホルダーの２つのバックアップは安全のため２枚のフロッピーディスクに作成しておく場合があります。特に秘密キーホルダーをなくさないように注意してください。秘密キーをなくすと、そのキーを使って暗号化した email メッセージまたは添付ファイルを復号化できくなくなります。キーホルダーはあなたしかアクセスできない安全な場所に保管してください。

3. 古いキーホルダーのバックアップした後、（古い)PGP 2.6.2ソフトウェアをハードディスクから削除または保管します。このとき、次の２つの方法があります。

- 手作業で古い PGP262 ディレクトリ全体とその内容を削除する。
- 手作業でpgp.exe(262)プログラムを削除し、他のファイル、特にconfig.txtとキーホルダーファイルは保管する。

新しく寄せ集めた PGP264 バージョンのコピーを入手した場合、古い 2.6.x ソフトウェアは新しい 5.0 キーホルダー上の RSA キーを読み取りでき、新しい DSS/Diffie-Hellman 形式のキーを見つけたときに失敗しません。

4. 付属の InstallShield 実行可能プログラムを使って PGP 5.5 をインストールします。
5. インストールプログラムが既存のキーホルダーがあるか聞いてきたら、「はい」をク　リックして、古い 262 キーホルダーを探し、指示に従ってそれらのキーを新しい pgp 5.5 キーホルダーにコピーします。
6. コンピュータを再起動します。

PGPmail 4.0 からのアップグレード

この処理は PGP 2.6.2 と同じです（ViaCrypt PGP は手作業で削除または保管しなければなりません）。キーホルダーのバックアップを保管してください。UNIX および DOS の PGP4.0.1 の ReadMe ファイルも参照してください。古い ViaCrpt ソフトウェアを使って PGP 5.5 キーホルダーを読み取るための寄せ集めバージョンの説明があります。

PGPmail 4.5 からのアップグレード

1. 現在コンピュータで起動中のプログラムとプロセスをすべて終了させます。
2. PGP Enclyptor プロセス (enclypt 32.exe) が起動中の場合は、それを終了させて、アンインストールできるようにします。
   Enclyptor が起動中か調べるには、そのフローティングパレットまたは最小化アイコンがタスクバーにあるか探します。[Contorl]+[Alt]+[Delete] キーを押して、タスクマネージャを呼び出し、Enclyptor という名前のプロセスを選択し〔タスクの終了〕ボタンをクリックして終了させることもできます。
3. スタート〕メニューから〔設定／コントロールパネル〕を選びます。
4. 〔プログラムの追加／削除〕をダブルクリックします。
5. PGPmail 4.5 の項目を選択します。
6. 〔追加／削除〕ボタンをクリックします。アンインストールユーティリティが自動的に必要なファイルをすべて削除し、レジストリファイルを一掃します。

アンインストール中に .dll ファイルを削除するか聞かれた場合、削除して構いません。PGP 5.5 ソフトウェアは新しいバージョンの .dll ファイルをインストールします。

7. 〔OK〕をクリックして削除を完了させ、完了したら〔追加／削除〕ウィンドウを閉じます。
8. InstallShield ユーティリティを使い新しい PGP 5.5 ソフトウェアをインストールします。なるべく、インストールプログラムをデフォルトのインストールディレクトリへ送ることをお勧めします。
9. インストールプログラムが既存のキーホルダーがあるか聞いてきたら、「はい」をクリックして、古い PGP 4.5 キーホルダーを探し、指示に従ってそれらのキーを新しい pgp 5.5 キーホルダーにコピーします。

10. コンピュータを再起動します。

PGP 5.0 v からのアップグレード

1. 現在コンピュータで起動中のプログラムとプロセスをすべて終了させます。
2. 起動中の PGP トレイのタスクを終了させ、アンインストールできるようにします。
   PGPtray.exe が起動中であるか調べるには、タスクバーのトレイ部分に小さな PTP エンベロープアイコンがあるかチェックします。そのアイコンがあれば、PGP トレイは起動中です。タスクを終了させるには、PGP トレイアイコンでクリックし、メニュー一番下の〔PGP トレイの終了〕コマンドを選択します。[Contorl]+[Alt]+[Delete] キーを押してタスクマネージャを呼び出し、pgptray プロセスを選択し、〔タスクの終了〕ボタンをクリックする方法もあります。
3. 〔スタート〕メニューから〔設定／コントロールパネル〕を選びます。
4. 〔プログラムの追加／削除〕をダブルクリックします。
5. PGP 5.0bNN の項目を選択します。〔追加／削除〕ボタンをクリックします。〔共有ファイルの削除〕ダイヤログボックスが表示されます。ファイル名と位置を指定するようメッセージがでます。

アンインストール中に .dll ファイルを削除するか聞かれた場合、削除して構いません。PGP 5.5 ソフトウェアは新しいバージョンの .dll ファイルをインストールします。

6. 〔OK〕をクリックしてアンインストールを終了させ、完了したら〔追加／削除〕パネルを終了させます。
7. InstallShield ユーティリティを使い新しい PGP 5.5 ソフトウェアをインストールします。なるべく、インストールプログラムをデフォルトのインストールディレクトリへ送ることをお勧めします。

8. インストールプログラムが既存のキーホルダーがあるか聞いてきたら、「はい」をクリックして、古い PGP 4.5 キーホルダーを探し、指示に従ってそれらのキーを新しい pgp 5.5 キーホルダーにコピーします。
9. コンピュータを再起動します。

これで新しい PGP 5.5 ソフトウェアを起動できます。

PGP 5.5 をインストールする

PGP 5.5 のインストールには次の方法があります。

- CD-ROM から

PGP 5.5 の初期バージョンをインストールしてある場合は、古いバージョンを完全に削除しなければなりません。〔スタート〕メニューに進み、〔設定〕を選びます。〔プログラムの追加／削除〕ボタンをクリックし、〔PGP 5.5 〕を　選んで〔追加／削除〕ボタンをクリックし、〔OK〕をクリックします。

CD-ROM からインストール

1. Windows を起動します。
2. CD ROM をドライブに挿入します。
3. セットアッププログラムを実行します。
4. 画面のプロンプトに従って操作を進めます。

PGP の起動

PGP は他のアプリケーションが作成したデータで機能します。したがって、いつでもそのとき処理しているタスクを元に、適切な PGP 機能が直ちに利用できるように設計されています。PGP には次の主な３つの使い方があります。

- システムトレイから
- サポートされる email アプリケーションから
- Windows エクスプローラの〔ファイル〕メニューから

システムトレイから PGP を使う

主な PGP 機能の多くは普通、システムトレイにあるトレイアイコンをクリックし、適当なメニュー項目を選んでアクセスできます。（このアイコンがシステムトレイにない場合は、〔スタート〕メニューから PGP キーを起動してください）。

クリップボードから PGP 機能を実行する

システムトレイのさまざまなオプションは Windows のクリップボードから実行する PGP 機能を指していることに気がつくでしょう。PGP プラグインによってサポートされていない email アプリケーションを使っている場合、あるいは他のアプリケーションで作成したテキストを処理する場合は、暗号化 / 復号化と署名 / 検証機能は Windows のクリップボードで実行します。例えば、テキストを暗号化したり署名するときは、テキストをアプリケーションからクリップボードへコピーし、適切な PGP 機能を使って暗号化し署名してからそれを送り先の受信人へ送信する前にアプリケーションに貼り付けます。暗号化または署名入り email メッセージを受け取ったとき、単純にこの処理を逆の順序で行い、「サイファテキスト」という暗号テキストをアプリケーションからクリップボードへコピーし、情報を復号化して検証してから、内容を表示します。復号化されたメッセージを表示した後情報を保存するか、暗号文のままで保持するか決めます。

PGP キーウィンドウを開く

PGP ポップアップメニューから〔PGP キーの起動〕を選ぶと、PGP キーウィンドウが開き、あなたが自分で作成した秘密&公開キーペアと、公開キーホルダーに追加した他のユーザの公開キーが表示されます。（まだ新しいキーペアを作成していない場合は、キー作成ウイザードが必要な手順をガイドします。なお、新しいキーペアの作成に進む前に各種オプションについて詳しくは第 3 章「作成と交換」を参照してください。）

〔PGP キー〕ウィンドウから、新しいキーペアを作成したり他のキーを管理できます。例えば、あるキーに関する属性を調べたり、キーが実際に所有者本人のものであるかどの程度信頼しているか指定したり、他のユーザのキーの認証を保証するキーの所有者を信頼するかを示す場合です。PGP キーウィンドウで行うキー管理機能について詳細は、第６章「キーの管理と選択の設定」を参照してください。

PGP 環境を設定する

PGP ポップアップメニューから〔 PGP 選択環境〕を選び、〔PGP 選択環境〕ダイヤログボックスをアクセスし、使っているコンピューティング環境でPGP プログラムがどのように機能するかを左右する設定を指定します。適切なタブをクリックして、修正したい環境設定へ進みます。これらの設定について詳しくは、第６章を参照してください。

ヘルプ情報を表示する

PGP ポップアップメニューまたは PGP キーウィンドウから〔ヘルプ〕を選び、PGP ヘルプシステムをアクセスします。たぶん行うだろう手順の概要と説明が表示されます。たいていのダイヤログボックスにも文脈に関連するヘルプ機能があり、ウィンドウの右端にある疑問符をクリックし画面上の知りたい部分をポイントすると、短い説明が表示されます。

PGP トレイを終了する

初期設定により、システムトレイに表示されたトレイアイコンで示されるように、PGP トレイプログラムはコンピュータを起動すると必ず実行します。何かの理由で、システムトレイから PGP トレイの実行を終了する場合は、PGP ポップアップメニューから〔PGP トレイの終了〕を選んで終了できます。

サポートされる email アプリケーションから使う

PGP プラグインによってサポートされるemail アプリケーションを持っている場合は､必要なPGP 機能はアプリケーションのツールバーにある適当なボタンをクリックしてアクセスできます｡例えば､メッセージを暗号化したいならば鍵アイコンをクリックし、署名を入れたければ羽ペンアイコンをクリックします。

別の PGP ユーザからemail を受信したときは、メッセージを復号化し、開いた封筒をクリックしてその人の電子署名を検証します。

キー&封筒ボタンをクリックすると、メッセージに含まれたキーがキーホルダーに追加されます。PGP キーウィンドウは、メールを作成または検索しているときにいつでも 2 つのキーボタンをクリックしてアクセスすることもできます。もっと簡単にいえば､email アプリケーションとPGP/MIME形式をサポートするプラグインを使い、やはりemail アプリケーションがこの形式をサポートしている別のユーザとメールのやりとりをしている場合２人とも email メッセージと添付ファイルを自動的に暗号化、復号化できます。email を送信または検索するときに､〔PGP 選択〕ダイヤログボックスでPGP/MIME暗号化と署名者機能をオンにするだけです。

PGP/MIME機能を使う人からemail を受け取ったとき､メールと一緒にPGP/MIME形式を示す添付アイコンが届きます。テキストとPGP/MIME形式の添付ファイルを復号化して、電子署名を検証するには、開いた封筒アイコンをダブルクリックするだけです。

Windows エクスプローラから使う

ワードプロセッサで作成したドキュメント、スプレッドシートおよびビデオクリップなどのファイルを Windows エクスプローラから直接、暗号化して署名したり、復号化して検証できます。PGP/MIME 標準に対応している Qualcomm Eudora などの email アプリケーション、またはファイルの暗号化、署名に PGP が必要ない Microsoft Exchange や Outlook などのアプリケーションを使っていない場合は、この方法を使って、email メッセージと一緒に送信したいファイルを添付しなければなりません。他の人がアクセスできないように使っているコンピュータに保存するファイルを暗号化、復号化したいこともあります。

PGP 機能を Windows エクスプローラからアクセスするには、マウスの右ボタンを押下し、開いたサブメニューから適当なオプションを選びます。表示されるオプションは選択したファイルの現在の状態によって違います。ファイルがまだ暗号化、署名されていない場合は、これらの機能を実行するオプションがメニューに出ます。ファイルがすでに暗号化または署名されている場合は、ファイルの内容を復号化し検証するオプションが表示されます。

受信人を選択する

email を、PGP プラグインによってサポートされる email アプリケーションを使っている人に送信するときは、内容を暗号化するときにどのキーを使うべきか受信人の email アドレスがを決めます。ところが、公開キーホルダーのいずれのキーにも対応しないユーザ名または email アドレスを入力したり、クリップボードをまたは Windows エクスプローラから暗号化する場合は、手作業で〔PGP キー選択〕ダイヤログボックスから受信人の公開キーを選択しなければなりません。受信人の公開キーを選択するには、そのキーを表すアイコンを〔受信人〕リストボックスにドラッグして〔OK〕をクリックします。

email の暗号化と署名、復号化と検証する方法について詳細は、第 4 章「プライベートな email の送受信」を参照してください。ファイルを暗号化してハードディスクに保存したり、email の添付ファイルとして送信する場合は、第 5 章の「PGP for Secure File Storage の使い方」を参照してください。

ショートカットを利用する

PGP の使い方は簡単なことに気がつくでしょうが、多数のショートカットを利用すれば暗号化作業をさらにスピードアップできます。例えば、PGP キーウィンドウでキーを管理しながら、メニューバーからアクセスするのではなく、右マウスボタンを押して必要な PGP 機能をすべて実行できます。キーを保存したファイルを PGP キーウィンドウにドラックして、キーをキーホルダーに追加することもできます。キーボードのショートカットもたいていのメニュー操作で利用できます。これらのキーボードのショートカットはどの PGP メニューにも表示され、その他のショートカットは本書で説明します。

PGP キーアイコンの定義

次の表は PGP キーウィンドウで使われるミニアイコンの一覧で、それが何を表しているかの説明です。

アイコンが表すもの

- １組のゴールドキーは Diffie-Hellman/DSS キーペアを表します。これは秘密キーと公開キーでできています。
- １つのゴールドキーは Diffie-Hellman/DSS 公開キーを表します。
- １組の青いキーは RSA キーペアを表します。これは秘密キーと公開キーでできています。
- １つの青いキーは RSA 公開キーを表します。
- キーまたはキーペアが薄い表示のときは暗号化と署名が一時的に利用できません。キーは PGP キーウィンドウから無効化でき、めったに使わないキーは〔キー選択〕ダイヤログボックスから片づけます。
- 赤い線が引かれたキーは、そのキーが廃止されたことを示しています。ユーザは、キーが有効でない、または何かで危険にさらされたときにキーを廃止します。キーと赤い X は無効なキーを示しています。

- クロック付きのキーは、キーが期限切れになったことを示します。キーの有効日付はキーが作成されたときに設定されます。
- ダイヤモンドはキーの所有者を表し、キーに関連するユーザ名と email アドレスが表示されます。
- 羽ペンはキーの認証を保証した PGP ユーザの署名を示します。赤線付きの署名は、廃止された署名を表します。赤い X マークの署名は、不良または無効な署名を表します。
- 空白のバーは無効なキーまたは信頼できないユーザを表します。
- 半分のバーは、限界有効レベルのキーまたは限界信頼レベルのユーザを示します。
- フルバーは完全な有効なキーまたは完全に信頼できるユーザを表します。
- ストライプのバーは、暗黙で有効なバーと暗黙で信頼できるキーを表します。この設定は、あなたが作成する秘密＆公開キーペアだけで利用できます。

第 3 章

作成と交換

キー

この章では他の PGP ユーザとのやりとりに必要な公開＆秘密キーペアの作成方法について説明します。自分の公開キーを配布したり他の人の公開キーを入手して、プライベートで差出人が明らかな email の交換を開始する方法についても説明します。

キーの概念

PGP は広く認められた、信頼性の高い公開キー暗号化システムを採用しており、あなたや他の PGP ユーザは秘密キーと公開キーを組み合せたキーペアを作成します。その名前が示すように、秘密キーはあなたしかアクセスできませんが、他の PGP ユーザとメールをやりとりするには受け手の公開キーのコピーが必要で、受け手ではあなたの公開キーのコピーが必要です。他の人に送信する email メッセージと添付ファイルに署名するときと、受け取ったメッセージとファイルを復号化するとき、秘密キーを使います。反対に、送信先の人に暗号化された email を送信するとき、彼らの電子署名を検証するときは受け手の人の公開キーを使います。

技術的に詳しく説明しなくとも、公開キー暗号化方式を使って暗号化されるのは実際は email の内容ではないことに興味をもったでしょう。そうではなく、データはかなり高速のシングルキーアルゴリズムを使って暗号化され、受信人の公開キーを使って実際に暗号化されるのがこのシングルキーです。受信人はその後、秘密キーを使ってこのキーを復号化します。これで暗号データを解読できます。

キーペアの作成

PGP の他のバージョンを使っているときにまだ作成したことがなければ、暗号化され認定された email を送受信する前にまず最初に必要なことは、新しいキーペアの作成です。キーペアは２つのキー、すなわちあなただけが所有する秘密キーとあなたが通信する相手に自由に配布する公開キーの組合せです。新しいキーペアは作成手順をガイドするキー作成ウイザードを利用して PGP キーウィンドウから作成します。

初期バージョンの PGP からアップグレードする場合は、おそらくすでに秘密キーを作成してあり、その照合公開キーを通信したい相手に配布してあります。その場合は、新しいキーペアを作成する必要はありません（次の項で説明します）。その代わり、PGP キーウィンドウを開いたときにキーの場所を指定します。PGP キーウィンドウの〔編集〕メニューに進み、〔選択〕を選びます。〔ファイル〕タブを選択して、既存のキーへの正しいパスはいつでも入力してください。

新しいキーペアの作成

1. Windows の〔スタート〕ボタンをクリックして、〔プログラム〕メニューまたは PGP トレイの〔PGP 〕サブメニューから〔PGP キー〕を選びます。このウィンドウは email アプリケーションのツールバーにある 2 つのキーアイコンをクリックしても開きます。

2. 〔キー〕メニューから〔新規キー〕を選びます。

   キー作成ウイザードに最初の画面の紹介文が表示されます。

3. この説明を読み、〔次へ〕をクリックして次のダイヤログボックスへ進みます。〔PGP　キー作成〕ウイザードにユーザ名と email アドレスを入力するようメッセージがでます。

4. １行めにユーザ名を、２行めに email アドレスを入力します。

   本名、email アドレスでも正しいものの入力が絶対に必要なわけではありませんが、本名を使ったほうが他の人があなたが公開キーの所有者であることを認識しやすくなります。また、正しい email アドレスを使うことで、あなたと他の人は、あなたがある受信人にメールを送ったときに、現在のキーホルダーにある適当なキーを自動検索するプラグイン機能を利用できます。

5. 〔次へ〕をクリックして次のダイヤログボックスへ進みます。

   〔キー作成〕ウイザードにキータイプを選択するようメッセージがでます。

6. キータイプには Diffie-Hellman/DSS または RSA を選択します（Personal 版では RSA は使用できまん）。

PGP の初期バージョンでは RSA という古い技術を使ってキーを作成します。PGP 5.0 以降からは、改良された Diffie-Hellman/DSS 技術をベースにした新しいタイプのキーを作成できます。

- まだ RSA キーを使っている人とデータを交換する場合は、旧バージョンのプログラムと互換性のある RSA キーペアを作成します。
- PGP 5.0 以降を持っている人とデータを交換する場合は、新しい技術を利用して、Diffie-Hellman/DSS キーのキーペアを作成できます。
- PGP ユーザ全員と email を交換できるようにしたい場合は、RSA キーペアと Diffie-Hellman/DSS キーペアを作り、受信人が使っている PGP バージョンに応じて適当なキーペアを使わなければなりません。必要なキーのタイプ毎にキーペアを作成しなければなりません。

7. 〔次へ〕をクリックして次のダイヤログボックスへ進みます。

   〔キー作成〕ウイザードに新しいキーのキー長を指定するようメッセージがでます。

8. キー長に 768 から 3072 ビットを選択するか、または 512 から 4096 ビットまでのカスタムキー長を入力します。なお、RSA キーは PGP の旧バージョンとの互換性を維持するため、2048 ビットまでに制限されています。

使っているコンピュータによってはカスタムキー長の作成にしばらく時間がかかります。

キー長はあなたの電子キーの作成に使われるビット数に対応しています。キーが大きいほど、誰かがそれを判読できる可能性が少ないですが、復号化・暗号化プロセスの実行に時間がかかります。小さいキーを使って PGP 機能を迅速に処理する便利さと、大きいキーによる高いセキュリティレベルのバランスをとる必要があります。誰かが情報を読み取ろうと費用がかかり、多くの時間を必要とする暗号解読の攻撃をしかけようとするほど重要な機密情報を交換しないのならば、1024 ビットのキーを使って安全です。

Diffie-Hellman/DSS キーを作成するときは、キーの DSS 部分のサイズは一定の増分で大きくなり、Diffie-Hellman 部分のサイズよりか小さいまたは同じで、最大サイズは 1024 ビットに制限されます。DSS 1024 ビットの署名キーの効果は 2048 ビットの RSA キーとほぼ同じです。

9. 〔次へ〕をクリックして次のダイヤログボックスへ進みます。

   〔PGP キー作成〕ウイザードにキーペアの有効期間を指示するようメッセージがでます。

10. キーの有効期間を指定します。デフォルト値の〔いいえ〕をそのまま受け入れるか、キーが何日後に期限切れになるかその日数を入力できます。

いったんキーペアを作成し、公開キーを世界に配布した後は、おそらくその時からずっと同じキーを使い続けることになります。ところが、場合によっては、特殊なキーペアを作成して、限られた期間だけ使用したい場合があります。この場合は、公開キーの期限が切れた後はメールの暗号化に利用することはできませんが、電子署名の検　　証には今までどおり利用できます。同様に、キーペアの期限が切れても、公開キーの期限切れの前であればあなたに送信されたメールの復号化に利用できますが、他の人のためのメールの署名には利用できません。アドミニストレータが現場に合わせて PGP を設定済みの場合、あなたのメッセージがメッセージリカバリキーとコーポレート署名キーにそれぞれのキーの名前で暗号化されることを知らせるメッセージが表示されることがあります。

11. 〔次へ〕をクリックして次のダイヤログボックスへ進みます。

    〔キー作成〕ウイザードにパスフレーズを入力するようメッセージがでます。

12. 〔PGP　パスフレーズ入力〕ボックスでは、秘密キーの独占アクセスの維持に使いたい文字または単語を入力します。入力を確認するため、[Tab] キーを押して次の行に進み、もう一度同じパスフレーズを入力します。

    普通、付加セキュリティレベルとして、パスフレーズに入力した文字は画面にはでません。それでも、誰も見ていないことが確かで、入力したパスフレーズの文字を見たい場合は、〔入力非表示〕チェックボックスを解除してください。

パスフレーズには複数の単語を入れてください。スペース、数字、句読文字を入力できます。簡単に覚えられて他の人が思いつかないものを選んでください。パスフレーズは大文字・小文字を区別します。効果的なパスフレーズには大文字と小文字、数字、句読文字そしてスペースを入れます。パスフレーズが長く、各種文字、記号がとり混ぜてあるほど安全です。大文字と小文字、数字、句読点などを入れてみてください。

〔品質バー〕には作成中のキーの効果に比べたあなたのパスフレーズの効果が表示されます。フルバーならばほぼ等しい強さです。

13.〔次へ〕をクリックしてキー作成プロセスを開始します。

〔PGP キー作成〕ウイザードに「最初のプライムナンバを作成しています . . . 」というメッセージがでます。

不適切なパスフレーズを入力した場合、キーが作成される前に警告メッセージがでて不良パスフレーズをそのまま受け入れるか、より安全なパスフレーズを入力し直すか選択できます。

キー作成時に十分なランダム情報がないと、〔PGP ランダムデータ〕ダイヤログボックスが出ます。このダイヤログボックスの指示どおり、マウスを移動して、進行バーが完全に満たされるまででたらめにキーを押します。マウスの動きとキーストロークによってユニークなキーペアの作成に必要なランダム情報が作成されます。

PGP 5.0 以降では、マウスの位置、タイミングおよびキーストロークなどシステムのさまざまなソースからランダムデータを絶えず集めています。〔ランダムデータ〕ダイヤログボックスがでない場合は、PGP はすでに十分なデータを収集しました。新規作成したキーを表すキーペアが PGP キーウィンドウに出ます。古い RSA キーは青いスケルトンキーで、新しい Diffie-Hellman/DSS キーは黄色のモダンキーになっています。

キー作成プロセスが開始した後、しばらくキーの作成に時間がかかります。実際に、Diffie-Hellman/DSS キーにデフォルト値以外のキー長を指定した場合には、高速キー作成オプションは使われず、大きいサイズのキーでは作成に数時間かかります。最後に〔PGP キー作成〕ウイザードにキー作成プロセスが完了したことがでます。

14. 〔次へ〕をクリックして次のダイヤログボックスへ進みます。

以前のキーと同じユーザ名または email アドレスをもつキーを作成する場合は、新しいキーに古いキーの署名を入れる機会が与えられます。これで誰かが新しいキーをキーホルダーに追加したとき、古いキーと同レベルの有効性と信頼性を授けます。有効性は過去にキーに署名した人に基づきますが、あなたの古いキーからの署名は含まれません。

15. 該当する場合は、新しいキーに古いキーで署名し、古いキーのパスフレーズを入力して〔次へ〕をクリックします。

〔キー作成〕ウイザードに新しいキーペアの作成が無事終了したことを知らせ、公開キーをキーサーバへ送信するか尋ねるメッセージがでます。

16. 新しい公開キーをあなたのドメインの適切なキーサーバへ送信するか指定し〔次へ〕をクリックします。公開キーをキーサーバを送信した場合、そのキーサーバをアクセスした人は誰でも、必要なときにあなたのキーのコピーを入手できます。詳しくはこの章の「公開キーの配布」を参照してください。

    キー作成プロセスが完了すると、最後のダイヤログボックスがでます。

17. 〔終了〕をクリックします。

キーを保護する

キーペアを作成した後は、予備のキーペアを作成し、オリジナルのキーペアに何か起きた場合に備えて安全な場所に保管しておくのが賢明です。秘密キーと公開キーは別々のキーホルダーファイルに保存されます。他のファイルと同様、ハードディスクの別の場所またはフロッピーディスクにコピーできます。デフォルト値により、秘密キーホルダー (secring.skr) と公開キーホルダー (pubring.pkr) は他のプログラムファイルと一緒に PGP ファイルディレクトリに保存されますが、バックアップファイルは好きな場所に保存できます。PGP は、あなたが公開キーと秘密キーを作成したときにそのバックアップコピーを作成します。

キーのバックアップコピーを作成するほか、特に注意が必要なことは、秘密キーをどこに保存するかです。秘密キーはあなたしか知らないパスフレーズで保護されていますが、誰かがパスフレーズを見つけて、あなたの秘密キーを利用して email を解読したり、電子署名を偽造することがあります。例えば、誰かがあなたの肩ごしに入力したキーストロークを見たり、それらをネットワーク上または電波をつうじて傍受できます。

あなたのパスフレーズを偶然手に入れた人があなたの秘密キーを利用できないように防止するため、自分のコンピュータに保存するだけにすべきです。あなたのコンピュータがネットワークに接続されている場合は、ファイルがシステム全域のバックアップに自動的に含まれないことを確認すべきです。そうしないと他の人があなたの秘密キーをアクセスできます。ネットワークをつうじてコンピュータを簡単にアクセスできることを考えると極秘情報を扱っている場合は、秘密キーはフロッピーディスクに保存し、プライベートなメールを読んだり署名したいきには必ず旧式キーのようにディスクを挿入して開けたいでしょう。もう１つのセキュリティ上の注意として、あなたの秘密キーホルダーファイルに別の名前を割り当て、それを初期設定の PGP ファイルディレクトリ以外の簡単には探しだせないどこかに保存する方法もよいでしょう。

公開キーを配布する

キーを作成したら、他の人が暗号化された emai を送信し、あなたの電子署名を検証できるように、他の人が利用できるようにする必要があります。公開キーの配布には次の 3 つの方法があります。

- 公開キーを公開キーサーバをつうじて利用できるようにする
- 公開キーを email メッセージに入れる
- 公開キーをエクスポートするか、またはテキストファイルへコピーする

公開キーは基本的にはテキストで構成されるので、公開キーサーバを通じて利用できるようにする、email メッセージに入れる、またはファイルへエキスポートあるいはコピーするのはとても簡単なことです。受信人は一番便利な方法を使って、公開キーを自分の公開キーホルダーに追加できます。

公開キーをキーサーバを通じて利用できるようにする

公開キーを利用できるようにする一番良い方法は、公開キーを誰もがアクセスできるキーサーバに掲示する方法です。そうして、人々はあなたのキーのコピーをはっきり要求する必要なく、あなたに email を送信できます。あなたも他の人もめったに使わない多数の公開キーを覚えている必要はありません。PGP,Inc., が提供しているものを含め、世界中に多数のキーサーバがあり、誰でもキーをアクセスできるようにできます。

PGP for Business Security を使っている場合は、アドミニストレータが使用するキーサーバを教えてくれます。これは普通はすべてが現場で正しく動作するようにあらかじめ構成されています。

公開キーをキーサーバへ送信

1. システムトレイのトレイアイコンをクリックして PGP キーウィンドウを開きます。

2. キーサーバへ掲示したい公開キーを表すアイコンを選択します。

3. 〔キー〕メニューから〔キーをサーバへ送る〕を選びます。別の方法は、右マウスボタンを押して、ポップアップメニューから〔キーをサーバへ送る〕を選択できます。

4. 〔キーをサーバへ送る〕サブメニューから、キーを送信したいキーサーバを選びます。PGP の設定によっていくつか選択できます。

公開キーのコピーをキーサーバに掲示した後、あなたに暗号化 email を送信したい人、またはあなたの電子署名を検証してサーバからあなたのキーのコピーを入手したい人に公表されます。公開キーを指摘しなくとも、キーサーバにあなたの名前または email アドレスがないか検索して、コピーを入手できます。多くの人は email メッセージの最後に公開キーの Web アドレスを入れます。たいてい、受信人はアドレスをダブルクリックするだけで、サーバ上のあなたのキーのコピーをアクセスできます。

email アドレスを変更する必要がある、または新しい署名を取得する場合、古いキーを書き換えるために必要なことは新しいコピーをサーバへ送ることだけで、情報は自動的に更新されます。ただし、キーサーバは情報を追加できるだけで、ユーザ名や署名を削除することはできないことを覚えおいてください。キーが危険にさらされている場合には廃止できます。こうして世界にそのキーは信頼できないことを知らせます。キーの廃止方法について詳しくは第 6 章「キーの管理と環境設定」を参照してください。

公開キーを email のメッセージに入れる

公開キーを誰かに配布するもう１つの便利な方法は、公開キーを email メッセージに入れる方法です。

公開キーを email のメッセージに入れる

1. システムトレイのトレイアイコンをクリックして PGP キーウィンドウを開きます。

2. キーペアを選択し、〔編集〕メニューから〔コピー〕を選びます。

3. email メッセージの作成に使うエディタを開き、カーソルを希望の場所に置き、〔編集〕メニューから〔貼り付け〕を選びます。新しい email アプリケーションでは、キーを PGP キーウィンドウから emal メッセージのテキストへドラッグして、キー情報を転送できます。

誰かにあなたの公開キーを送信するときは、必ず email に署名してください。そうして受信人はあなたの署名を検証し、誰も途中で情報を改竄していないことを確認できます。もちろん、キーに信頼する紹介者の署名がなかった場合は、署名があなたのものであるか本当に確認するにはキーの指紋を検証する方法しかありません。

公開キーをファイルへエキスポートする

公開キーを誰かに配布するもう１つの方法は、公開キーをファイルへコピーして、このファイルをあなたとやりとりしたい人が利用できるようにする方法です。公開キーをファイルへコピーする方法は次の３つの方法があります。

- PGP キーウィンドウからあなたのキーペアを表すアイコンを選択し、〔キー〕メニューから〔エクスポート〕を選び、キーを保存したいファイル名を入力する。
- PGP キーウィンドウからあなたのキーペアを表すアイコンをドラッグして、Windows エクスプローラウィンドウの希望の位置にドロップする。
- PGP キーウィンドウからあなたのキーペアを表すアイコンを選択し、〔編集〕メニューから〔コピー〕を選び、〔貼り付け〕を選んでキー情報をテキストドキュメントに挿入する。

他人の公開キーを入手する

なた宛に暗号メールを送信したい人や、あなたの電子署名を検証したい人にあなたの公開キーを配布しなければならないのと同様に、他の人の公開キーを入手して他の人に暗号メールを送る、彼らの電子署名を検証できるようにする必要があります。誰かの公開キーを入手する方法は次の 3 つの方法があります。

- キーを公開キーサーバから入手する
- 公開キーを直接 email メッセージから追加する
- 公開キーをファイルからインポートする

公開キーは実際はテキストで構成されるので、ファイルからインポートしたり、email メッセージからコピーして公開キーホルダーに貼り付けて、キーホルダーに追加するのはとても簡単なことです。

公開キーをキーサーバから取得する

暗号メールを送信したい人が経験豊富な PGP ユーザであれば、公開キーのコピーをキーサーバに掲示してあるかもしれません。PGP 5.5 では、PGP 環境設定で指定されたキーサーバを検索できます。これは、メールを送信したいときに相手の最新のキーのコピーを入手するときに非常に便利で、さらに公開キーホルダーに多数のキーを保存する手間も省けます。

PGP for Business Security 5.5 を使っている場合、組織内でよく使われるキーが保存されているコーポレートキーサーバを使用するよう指示されることがあります。

PGP 5.5 を使っている場合、次の方法を使ってキーサーバ上のキーを検索できます。

- ユーザ ID
- キー ID
- キータイプ (Diffie-Hellman または RSA)
- 作成日
- 有効期間
- 廃止キー
- 無効キー

この操作の逆も利用できます。例えば、「ユーザ ID」が「Bob 」以外を検索できます。

誰かの公開キーをキーサーバから入手する

1. システムトレイのトレイアイコンをクリックして PGP キーウィンドウを開きます。

2．PGP キーウィンドウの〔キー〕メニューから〔検索〕を選びます。〔検索〕ダイヤログボックスがでます。

3．メニューを利用して、ユーザの公開キーを探す検索基準を入力します。

指定したユーザの公開キーが見つかると、あなたの公開キーホルダーに追加するかメッセージがでます。公開キーをキーホルダーに追加すると、そのキーが PGP キーウィンドウに表示され、有効であるか確認のため調べることができます。

email のメッセージから公開キーを追加する

誰かの公開キーのコピーを入手する便利な方法は、その人に公開キーを email メッセージに入れてもらう方法です。PGP プラグインによってサポートされている email アプリケーションを持っていれば、送信人の公開キーはボタンをクリックするだけで公開キーホルダーに追加できます。例えば、email メッセージが誰かの公開キーを含むテキストと一緒に到着した場合は、キー＆封筒ボタンをクリックし、キーを公開キーホルダーに保管します。

PGP プラグインによってサポートされていない email アプリケーションを使っている場合は、公開キーを表すテキストをコピーして、PGP キーウィンドウに貼り付けてキーホルダーに追加できます。

ファイルから公開キーをインポートする

誰かの公開キーを入手するもう１つの方法は、その人に公開キーをファイルに保存してもらい、あなたがそれをインポートするか、コピーして公開キーホルダーに貼り付ける方法です。誰かの公開キーを取り出し、それを自分の公開キーホルダーに追加する方法は３つあります。

- 〔キー〕メニューから〔インポート〕を選び、公開キーを保存するファイル名を入力する。
- 公開キーが書き込まれたファイルを Windows エクスプローラウィンドウから PGP キーウィンドウへドラッグする。

- 公開キーが保存されたテキストドキュメントを開き、キーを表すテキスト部分を選択し、〔編集〕メニューから〔コピー〕を選ぶ。PGP キーウィンドウへ進み、〔編集〕メニューから〔貼り付け〕を選びキーをコピーする。その後、キーは PGP キーチウィンドウにアイコン表示されます。

キーの認証を検証する

キーを誰かと交換するとき、そのキーが本当にその人のものであるか見分けにくいことがあります。PGP にはさまざまな安全機能があり、キーの認証を調べ、キーが特定の所有者のものであることを認定できます。PGP プログラムはまた、あなたが有効でないキーを使うと警告し、最低限有効なキーを使おうとすると初期設定では同じように警告をだします。公開キー暗号化システムの主な脆弱性の１つに、一部の盗み見る人が誰かの公開キーを自分のものと置き換えて「マンインミドル」攻撃をしかけることができることがあります。こうして、その人宛ての暗号化された email を横取りし、自分のキーを使って復号化し、後でその人の本物のキーを使ってもう一度暗号化し、あたかも何も起こらなかったかのように送信することができます。実際、これは真ん中で待ちかまえ、あなたの通信文をすべて解読する複雑なコンピュータプログラムをつうじてすべて自動的に行われます。

このような場合に備え、あなたと、あなたが email を交換する人は、お互いのキーの正当なコピーを持っているか調べる方法が必要です。間違いなく公開キーがその人のものであることを示すベストな方法は、所有者がそれをフロッピーディスクにコピーして、物理的にあなたに手渡すことです。ところが、面と向かって誰かにディスクを手渡すほど近くにいることはめったなく、普通 email を通じて公開キーを交換するか、公開キーサーバから入手します。

これらは少し安全性にかける改竄防止キーの交換方法ですが、それでも、キーが本当にその人のものであるかはキー作成時に作成されたユニークな数字の並び、電子指紋をチェックして調べることができます。

誰かの公開キーのコピーにある指紋とオリジナルのキーにある指紋を照合して、キーの有効なコピーを持っているか確実に確認できます。キーの指紋を探すには、PGP キーウィンドウでキーを選択し、〔キー〕メニューから〔キープロパティ〕を選びます。もっとも確実なキーの指紋のチェック方法は、その人に電話をかけ、電話で指紋を読み上げてもらう方法です。誰かの公開キーの合法コピーを持っていると確信しているならば、そのキーに署名できます。誰かの公開キーにあなたの秘密キーで署名することで、あなたは、そのキーがユーザ本人のものであると世界に認定します。例えば、新しいキーを作成したときは、あなた自身の電子署名で自動的に認定されます。それはキーを作成した人が所有者本人であるという理性的に信頼できる前提があるからです。キーに署名するのは、誰かがキーを修正して、あなたの署名をただちに無効にすることを防止するためです。デフォルト値では、あなたが他のキーにした署名はエクスポートされません。つまりキーはキーホルダーにあるときに署名は適用できるだけです。

信頼する紹介者をつうじてキーを入手する

PGP ユーザは他の信頼するユーザに公開キーに署名してもらい、その認証をさらに証明することがよくあります。例えば、信頼する同僚にあなたの公開キーのコピーを送り、同時に、そのキーを公開キーサーバに掲示するときに同僚の署名を入れることができるようにキーを認定して返送するように頼みます。PGP を使って誰かがあなたの公開キーのコピーを入手したとき、キーの認証をチェックする必要はなく、代わりにあなたのキーに署名した人をどれほど信用しているかにかかります。

PGP には公開キーホルダーに追加する公開キー毎に有効性レベルを設定できる手段があり、各キーに関する信頼の有効性レベルが PGP キーウィンドウに表示されます。つまり、信頼する紹介者の署名入りのキーを誰かから入手した場合は、そのキーが主張しているユーザ本人のものであることを確信できます。キーに署名し、ユーザの有効性を確認する方法について詳しくは第 6 章「誰かの公開キーに署名する」を参照してください。

アドミニストレータは信頼する紹介者になることができ、あなたはコーポレートキーの署名入りのキーならば有効なキーと信用できます。数カ所に分散した大きな会社で働いている場合、まず地区紹介者がいて、アドミニストレータはメタ紹介者または信頼する紹介者のそのまた信頼する紹介者です。

第 4 章

プライベートな email の送受信

この章では他の人へ送る email を暗号化、署名する方法と、他の人があなたに送信した email を復号化、認証する方法を説明します。

email の暗号化と署名

email を暗号化し署名する一番早く、簡単な方法は、PGP プラグインによってサポートされるアプリケーションを使う方法です。手順は email アプリケーションよって少し違いますが、アプリケーションのツールバーにある適切なボタンをクリックして暗号化・署名プロセスを実行します。さらに、PGP/MIME 標準対応または PGP/MIME を必要としないアプリケーションを使っている場合は、email メッセージと添付ファイルは、email を送受信するときに暗号化、署名できます。PGP プラグインをサポートしていない email アプリケーションを使っている場合は、Windows のクリップボードを利用してシステムトレイのトレイアイコンから適当なオプションを選択して email メッセージを暗号化、署名できます。添付ファイルを入れるには、ファイルを添付する前に Windows エクスプローラからそのファイルを暗号化します。

大事な email を送信する場合は、題名ラインを空白のままにするか、暗号メッセージの内容が明らかにならない題名ラインを作成するようにしてください。

PGP によってサポートされていない email アプリケーションを持っていない場合、ファイルの暗号化について詳しくは、第 5 章「PGP for Secure File Storage の使い方」を参照してください。

サポートされる email アプリケーションを使って暗号化し、署名する

PGP プラグインによってサポートされる email アプリケーションを使って暗号化、署名する場合は、受信人がどのタイプの email アプリケーションを使っているかによって２つの中から選択できます。PGP/MIME 標準対応の email アプリケーションを持っている他の PGP ユーザとメール交換をする場合は、PGP/MIME 機能を利用して email メッセージと添付ファイルを送信時に自動的に暗号化、署名できます。PGP/MIME 対応の email アプリケーションを持っていない人とメール交換をする場合は、互換性の問題を避けるため、PGP/MIME 機能をオフにして email を暗号化しなければなりません。この方法の短所は email と一緒に送信したいファイルを別に暗号化しなければならない点です。Exchange などのアプリケーションを使っている場合は例外で、PGP/MIME 機能を使わずに添付ファイルを暗号化、署名できます。

email をすぐに送信せずに、いったん送信箱に保存する場合は、email アプリケーションの中に email が実際に送信されるまでは情報が暗号化されないものがあることに注意してください。暗号化メッセージを待機させる前に、アプリケーションが送信箱のメッセージを暗号化するか調べなければなりません。暗号化しない場合は、送信箱に入れる前にクリップボードをつうじてメッセージを暗号化しておかなければなりません。詳しくは第５章を参照してください。

サポートされる email アプリケーションを使った暗号化と署名

1. email アプリケーションを使って、いつも通り email メッセージを作成します。

2. email メッセージの本文を作成したら、鍵と羽ペンボタンをクリックして、メッセージのテキストを暗号化し、署名するかを指定します。

3. email メッセージをいつもどおり送信します。

暗号データに署名を入れることを選んだ場合、〔パスフレーズ〕ダイヤログボックスがでて、メールを送信する前にパスフレーズを入力するようメッセージがでます。

4. パスフレーズを入力して〔OK〕をクリックします。

   受信人全員の公開キーのコピーを持っているならば、適切なキーが使われます。ところが、対応する公開キーがない受信人を指定すると、〔PGP キーの選択〕ダイヤログボックスがでるので、正しいキーを指定できます。

5. 暗号化された email メッセージのコピーを受け取る人の公開キーを〔受信者〕リストボックスにドラッグします。キーをダブルクリックしても、画面のある場所から他の場所へ移動できます。

   〔有効性〕ボタンは、受信人リスト中の公開キーが有効であることを表す最低の信頼性レベルを示します。有効性はキーに関連する署名を元にし、信頼性は別のユーザのキーの認証を保証するキーの所有者をどの程度信頼できるかを示します。詳しくは第 6 章「キーの管理と環境設定」を参照してください。

   

   PGP/MIME を使っていない、または PGP/MIME を必要としない email の場合は、送信前に送信したいファイルを添付ファイルとして Windows エクスプローラから暗号化しなければなりません。

6. 〔OK〕をクリックしてメールを送信します。

グループについて

PGP を利用してグループを作成できます。例えば、暗号メールを「engineering@xyz.com 」の 10 人に送信したい場合は、その名前でグループを作成できます。メニューに〔グループ〕項目があり、PGP キーウィンドウのグループ部分の表示、非表示を設定できます。グループを作成すると、グループの処理をするときに〔グループ〕ポップアップメニューを使用できます。〔グループ〕ポップアップメニューをアクセスするにはグループを選択し右マウスボタンを押します。グループに貼り付け、グループの削除、サーバからキーの入手およびグループプロパティを調べることができます。

グループの作成

1. 〔グループ〕メニューから〔新規グループ〕を選びます。
2. グループ名を入力します。
3. 必要ならば、グループの説明を入力できます。これはグループプロパティとして表示されます。

メンバをグループに追加

1. PGP キーウィンドウからグループに入れる人のキーを選択します。
2. PGP キーウィンドウからユーザの名前をグループ欄にドラッグしてグループに入れます。

グループの削除

1. PGP キーウィンドウのグループ欄からグループを選択します。
2. 削除キーを押す、またはポップアップメニューから〔削除〕を選びます。

グループを別のグループに追加

1. 別のグループに入れたいグループを選択します。
2. そのグループを入れたいグループにドラッグします。
3. ポップアップメニューから〔グループへ貼り付け〕を選択します。

グループメンバの削除

- 削除するグループメンバを選択する。
- ポップアップメニューから削除を選ぶ。
- 選択の確認メッセージがでる。
- 〔はい〕を押して確定する。

email の復号化と認証

あなた宛に送られた email を復号化し認証する一番早く、簡単な方法は、PGP プラグインによってサポートされるアプリケーションを使う方法です。手順は email アプリケーションによって少し違いますが、アプリケーションのツールバーにある適切なボタンをクリックして復号化・認証プロセスを実行します。さらに、PGP/MIME 標準対応のアプリケーション、または PGP/MIME を必要としないアプリケーションを使っている場合は、email メッセージと添付ファイルを、email に添付されたアイコンをクリックして復号化、認証できます。

PGP プラグインをサポートしていない email アプリケーションを使っている場合は、Windows のクリップボードを利用して復号化、認証できます。さらに、email に暗号化された添付ファイルが含まれている場合は、Windows エクスプローラから別に復号化しなければなりません。

サポートされる email アプリケーションからの復号化し、認証する

他の PGP ユーザとメール交換し、相手がメールを PGP/MIME 標準を使って暗号化、署名している場合は、email を開いたときに鍵付き封筒アイコンが出ます。

この場合、メッセージと添付ファイルはこのアイコンをダブルクリックするだけで、復号化して認証できます。

PGP/MIME 標準対応の email アプリケーションを使っていない相手から email を受け取る場合は、email メッセージはアプリケーションのツールバーの開いた封筒アイコンをクリックして復号化します。また、暗号化された添付ファイルがある場合、そのファイルは Windows エクスプローラから、またはファイルのアイコンをダブルクリックして復号化します。

サポートされる email アプリケーションからの復号化と認証

1. email メッセージを普通どおり開きます。

   email メッセージの本体に判読できない暗号テキストがでます。

2. email メッセージの内容を復号化、認証するため、アプリケーションのツールバーの開いた封筒ボタンをクリックします。

   〔PGP パスフレーズの入力〕ダイヤログボックスがでて、パスフレーズを入力するよう指示されます。

3. パスフレーズを入力して〔OK〕をクリックします。

   メッセージは復号化されます。署名付きの場合は、署名が有効かどうかを示すパネルが出ます。

4. メッセージを読んだ後、復号化された状態で保存するか、または安全のため暗号文のまま保存できます。

クリップボードを復号化し、認証する

email アプリケーションが PGP プラグインによってサポートされていない場合は、メッセージを復号化したり、電子署名を認証するには、その内容をクリップボードにコピーしなければなりません。email にファイルが添付されている場合は、そのファイルを Windows エクスプローラから復号化し、認証します。

クリップボードの復号化と認証

1. email アプリケーションの付属エディタで、暗号化テキストを選択し、それをクリップボードにコピーします。たいていのアプリケーションでは、〔編集〕メニューから〔コピー〕を選び、テキストを Windows のクリップボードへコピーします。

2. システムトレイのトレイアイコンでクリックし、PGP ポップアップメニューを開きます。〔クリップボードの復号化／認証〕を選び、復号化・認証プロセスを開始します。

   〔PGP パスフレーズの入力〕ダイヤログボックスがでて、パスフレーズを入力するようメッセージがでます。

3. パスフレーズを入力して〔OK〕をクリックします。

   メッセージが復号化されます。署名付きの場合は、署名が有効かどうかを示すパネルが出ます。

4. 解読された email メッセージの内容を表示するには、PGP ポップアップメニューから〔クリップボードのテキストの編集〕を選びます。その後、内容をテキストエディタにコピーし、必要ならば保存できます。

Windows エクスプローラから復号化し、認証する

受け取った email にファイルが添付され、PGP/MIME 対応の email アプリケーションを使っていない、または PGP/MIME を必要としないアプリケーションの場合は、添付ファイルは Windows エクスプローラから復号化しなければなりません

Windows エクスプローラからの復号化と認証

1. 〔スタート〕メニューから〔Windows エクスプローラ〕を開きます。
2. 復号化、認証したいファイルを選択します。

   復数のファイルを選択できますが、復号化と認証のプロセスは１つずつのファイルで行わなければなりません。
3. 〔ファイル〕メニューの PGP サブメニューから〔復号化／認証〕を選ぶか、右マウスをクリックしてポップアップメニューを開き、〔復号化／認証〕を選びます。

   〔PGP パスフレーズの入力〕ダイヤログボックスがでて、パスフレーズを入力するようメッセージがでます。
4. パスフレーズを入力して〔OK〕をクリックします。

   メッセージは復号化されます。署名付きの場合は、署名が有効かどうかを示すパネルが出ます。
5. 〔OK〕をクリックします。

   「暗号化ファイルを名前を付けて保存」ダイヤログボックスが出ます。
6. 復号化されたファイルを保存する場所とファイル名を指定します。

   ファイル名を特に指定しないと、オリジナルのファイル名が使われます。
7. 〔保存〕ボタンをクリックして、ファイルを保存します。

   復号化ファイルが指定された場所に保存されます。

第 5 章

PGP for Secure File Storage の使い方

この章では、email プラグインを使わずに PGP 機能を使う方法を説明します。ファイルを暗号化し署名してメールで送受信したり、コンピュータに安全に保管できるようにするため、PGP を使って暗号化、復号化する方法と、クリップボードと Windows エクスプローラから PGP ツールまたは PGP メニューを使ってファイルに署名､認証する方法を説明します。

PGP を使ったファイルの暗号化と復号化

email プラグインを使わずに PGP を使ってファイルを暗号化、署名し、暗号化または署名入りファイルを email の添付ファイルとして送信できます。この章で説明するテクニックを使って、コンピュータまたはファイルサーバに保存しているファイルを暗号化し、署名することもできます。

クリップボードを暗号化し、署名する

PGP プラグインによってサポートされていない email アプリケーションを使っている場合は、Windows のクリップボードでファイルを暗号化、署名できます。これは、システムトレイのトレイアイコンをクリックし、適切なオプションを選択して行います。基本的には、メッセージまたはファイルの内容をクリップボードへコピーし、それを暗号化および / またはその内容に署名します。その後、送信前に email エディタに貼り付けるか、署名入りまたは暗号化ファイルとして保存します。メッセージにファイルを添付する場合には、添付する前に Windows エクスプローラから暗号化しなければなりません。

クリップボードの暗号化と署名

1. email アプリケーションの付属エディタまたは愛用しているワープロソフトを使用してファイルを作成します。

2. メッセージの送信準備ができたら、暗号化したいテキスト部分を選択、または〔編集〕メニューから〔全選択〕を選択します。

メッセージを暗号化するとワープロソフト特有の書式は解除されます。

3. 〔編集〕メニューから〔コピー〕を選び、メッセージの内容をクリップボードへコピーします。

アプリケーションでテキストをコピーまたは切り取ったときは、一時的にクリップボードへ保存されます。

4. システムトレイのトレイアイコンをクリックし、〔クリップボードを暗号化〕〔クリップボードに署名〕または〔クリップボードの暗号化と認証〕を選びます。クリップボードの内容の暗号化を指定すると、〔PGP キーの選択〕ダイヤログボックスがでます。

5. 暗号化された email メッセージのコピーを受け取る人の公開キーを〔受信者〕リストボックスにドラッグします。

   ファイルを暗号化して安全に保存する場合には、自分を受信者に選択してください。

   〔有効性〕ボタンは、受信者リスト中の公開キーが有効であることを表す最低レベルの信頼性を示します。この有効性はキーに関する署名を元にしています。

6. 〔OK〕をクリックします。

   メッセージの署名を選んだ場合、〔PGP 署名パスフレーズ〕ダイヤログボックスがでて、デフォルト値の秘密キーの個人的なパスフレーズを入力するようメッセージがでます。別のキーペアを持っていて、その中の１つを使いたい場合は、矢印でクリックして適当なキーを選択します。

7. パスフレーズを入力して〔OK〕をクリックします。

8. email メッセージで暗号化ファイルを送信する場合は、暗号化されたメッセージを email アプリケーションにコピーします。

9. email を送信するか、または暗号化ファイルをハードディスクあるいはファイルサーバに保存します。

クリップボードを復号化し、認証する

email アプリケーションが PGP プラグインによってサポートされていない場合、あるいは安全に保存するためにファイルを暗号化し署名を入れた場合、メッセージを復号化したり電子署名を認証するには、メッセージの内容をクリップボードにコピーしなければなりません。email にファイルが添付されている場合は、Windows エクスプローラから復号化し認証しなければなりません。

クリップボード復号化と認証

1. email アプリケーションの付属エディタで、暗号化テキストを選択し、クリップボードにコピーします。

   たいていのアプリケーションでは、〔編集〕メニューから〔コピー〕を選び、テキストを Windows のクリップボードへコピーします。

2. システムトレイのトレイアイコンでクリックし PGP ポップアップメニューを開きます。〔復号化／認証〕クリップボードを選び、復号化・認証プロセスを開始します。

   〔PGP パスフレーズの入力〕ダイヤログボックスがでて、パスフレーズを入力するようメッセージがでます。

3. パスフレーズを入力して〔OK〕をクリックします。

   メッセージは復号化されます。署名付きの場合は、署名が有効かどうかを示すパネルが出ます。

4. 解読された email メッセージの内容を表示するには、PGP ポップアップメニューから〔クリップボードテキストのテキスト編集〕を選びます。その後、内容をテキストエディタにコピーし、必要ならば保存できます。

Windows エクスプローラから暗号化し、署名する

Windows エクスプローラから暗号化し、署名する　暗号化ファイルを email メッセージと一緒に添付ファイルとして送信する場合、またはファイルを暗号化して、コンピュータまたはファイルサーバ上で安全に保管したい場合は Windows エクスプローラから暗号化し署名できます。

Windows エクスプローラからの暗号化と署名

1. 〔スタート〕メニューから〔Windows エクスプローラ〕を開きます。

2. 暗号化したいファイルを選択します。

   複数のファイルを選択できますが、ファイルは１つずつ暗号化し署名しなければなりません。

3. 〔ファイル〕メニューの PGP サブメニューから、または右マウスをクリックしてポップアップメニューを開き、希望のオプションを選びます。

   〔PGP キー選択〕ダイヤログボックスがでます。ここで暗号化または署名を入れるファイルの受信者の公開キーを選択できます。

   次のオプションから選択できます。

- ファイルを一部の email アプリケーションを使って添付ファイルとして送信するときは、〔テキスト出力〕チェックボックスを選択し、ファイルを ASCII テキストとして保存しておく必要があります。古い email アプリケーションを使ってバイナリファイルを送信するときに必要な場合があります。
- どの email アプリケーションでも処理できるテキスト形式で保存した暗号化ファイルを出力したい場合は、〔テキスト出力〕チェックボックスを選択します。このオプションを選択すると、ファイルサイズが約 30% 大きくなります。
- 〔コンベンショナル暗号化〕では、従来の暗号化を利用できます。つまり、公開キーによる暗号作成（解読）法ではなく、共通のパスフレーズに頼ります。ファイルはあなたが作成するように指示されたパスフレーズを使って暗号化する、セッションキーを使って暗号化されます。

- 〔オリジナル削除〕を選ぶと、あなたが暗号化または署名を入れるオリジナルのドキュメントは上書きされるので、大事な情報を誰かがあなたのハードディスクをアクセスしても読み取りできません。

仮想メモリを使うシステムでも、PGP はファイルの内容すべてに正しく上書きします。ファイルを暗号化する前に保存してしまうアプリケーションプログラムがファイルの一部とは考えられないファイルの断片をハードディスクに残しても価値はありません。仮想メモリについて第 8 章「セキュリティ機能と脆弱性」の「脆弱性」を参照してください。サードパーティのユーティリティを使って、ディスクの空きペースを整理してこの問題を解決したいことがあります。PGP には現在この機能がありません。

- ファイルに署名した場合は、パスフレーズ指定のメッセージがでます。
- 署名を暗号化ファイルに追加して、その署名を別のファイルに保存したい場合は〔別の署名ファイル〕チェックボックスを選択します。

4. 公開キーを受信者リストにドラッグして選択し、〔OK〕をクリックします。〔暗号化ファイルを保存〕ダイヤログボックスがでます。

5. 暗号化されたファイルを保存したいファイルの場所とファイル名を指定します。ファイル名には自動的に .pgp 拡張子が追加されます。ただし ASCII Armor オプションをオンにしていると、.asc 拡張子が使われます。

6. 〔保存〕ボタンをクリックして、ファイルを指定された場所に保存します。

ファイルを保存したディレクトリを見ると場合、２つのアイコンの１つで表された指定名が付いたファイルが見つかります。暗号化とテキスト出力には拡張子 .ASC が付き、暗号化と標準出力には .PGP 拡張子が付いています。

Windows エクスプローラからの PGP 機能の使い方

PGP ツールと PGP トレイでは、ファイルとフォルダで PGP 機能を使う方法があります。これらの機能をアクセスするには、ファイルを選択し右マウスボタンを押して、PGP ポップアップメニューを開きます。この中に次のオプションがあります。

- 暗号化
- 署名
- 暗号化＋署名
- 完全削除

PGP ツールにアクセスするには、システムトレイ中の鍵付き封筒アイコンをクリックするか、PGP ディレクトリから PGP ツールを選択します。PGP ポップアップメニューに表示される機能のほか、PGP ツールには復号化と認証の機能も含まれています。

ファイルの暗号化と署名について詳しくは、この章の初めの「Windows エクスプローラからの暗号化と署名」を参照してください。

完全削除機能は、ファイルとその内容に上書きし、コンピュータから削除します。完全削除機能はファイルとその内容をコンピュータのハードディスクから完全に削除する安全な方法です。Windows オペレーティングシステムではファイルを削除すると、ファイル名はファイルディレクトリから削除されました。完全削除機能はファイルのデータのすべての痕跡を削除するので、誰もソフトウェアツールを使用してファイルを修復できません。

ファイルの上書き

1. 〔スタート〕メニューから〔Windows エクスプローラ〕を開きます。

2. 完全削除したいファイルを選択します。

3. PGP ポップアップメニューを開く、または PGP ツールをアクセスします。

   PGP メニューを開くには、ファイルを選択して右マウスボタンを押します。PGP を選びます。サブメニューがでて、コマンド〔暗号化〕〔署名〕〔暗号化＋署名〕および〔完全削除〕が表示されます。

4. 〔完全削除〕を選びます。

5. ファイルを選択するか、〔ファイルの選択〕ダイヤログボックスから〔開く〕を選びファイルを完全削除します。

   〔最終変更確認〕ダイヤログボックスがでて、ファイルを本当に削除してよいか確認メッセージがでます。

6. 〔はい〕をクリックして、ファイルを完全削除します。

仮想メモリを使うシステムでも、PGP はファイルの内容すべてに正しく上書きします。ファイルを暗号化する前に保存してしまうアプリケーションプログラムがファイルの一部とは考えられないファイルの断片をハードディスクに残しても価値はありません。第 8 章の「スワップファイルまたは仮想メモリ」を参照してください。また、多くのプログラムは処理中に自動的にファイルを保存するので、削除したいファイルのバックアップコピーがあることに注意してください。

サードパーティのユーティリティを使って、ディスクの空きスペースを整理してこの問題を解決したいことがあります。PGP には現在この機能がありません。

Windows エクスプローラから復号化し、認証する

受け取った email に添付ファイルがあり、PGP/MIME 対応の email アプリケーションを使っていないまたは PGP/MIME を必要としない場合は、添付ファイルを Windows エクスプローラから復号化しなければなりません。

Windows エクスプローラからの復号化と認証

1. 〔スタート〕メニューから〔Windows エクスプローラ〕を開きます。
2. 復号化、認証したいファイルを選択します。

   複数のファイルを選択できますが、復号化と認証のプロセスはファイル毎に行わなければなりません。
3. 〔ファイル〕メニューの PGP サブメニューから〔復号化／認証〕を選ぶか、右マウスをクリックしてポップアップメニューを開き、〔復号化／認証〕を選びます。

   〔PGP パスフレーズの入力〕ダイヤログボックスがでて、パスフレーズを入力するようメッセージがでます。
4. パスフレーズを入力して [OK] をクリックします。

   メッセージは復号化されます。署名付きの場合は、署名が有効かどうかを示すパネルが出ます。
5. [OK] をクリックします。

   〔復号化ファイルを名前を付けて保存〕ダイヤログボックスが出ます。
6. 復号化されたファイルを保存する場所とファイル名を指定します。

   ファイル名を特に指定しないと、オリジナルのファイル名が使われます。
7. 〔保存〕ボタンをクリックして、ファイルを保存します。

   復号化ファイルが指定された場所に保存されます。

第 6 章

キーの管理と環境設定

この章では電子キーホルダーに保管されたキーを調べ、管理する方法を説明します。特定のコンピューティング環境に合わせた環境設定方法についても説明します。

キーを管理する

自分で作成したキーと他の人から集めたキーは電子キーホルダーに保存されます。これは基本的にはハードディスクまたはフロッピーディスクに保存されるファイルです。通常秘密キーは secring.skr という名前のファイルに保存され、公開キーは pubring.pkr という名前の別のファイルに保存されます。これらのファイルは普通、他の PGP プログラムファイルと同じプログラムディレクトリに入っています。次のアイコンは秘密キーと公開キーホルダーファイルを表すときに使われ、ファイルをざっと見たときに簡単に見分けられます。

秘密キーのキーホルダー

公開キーのキーホルダー

キーを通常の場所に保存すると都合が悪い場合は、別のファイル名または場所を選ぶことができます。詳しくはこの章の「環境設定」を参照してください。

時には、キーに関連する属性を調べたり、変更したい場合があります。例えば、誰かの公開キーを入手したとき、そのタイプ（RSA または Diffie-Hellman/DSS） を識別し、指紋を照合し、キーに付けられたデジタル署名を元にその有効性を調べたいことがあります。誰かの公開キーに署名してそれが有効であると信用していることを示したり、キーの所有者に信用度を割り当てる、あるいは秘密キーのパスフレーズを変更したい場合があります。これらは、PGP キーウィンドウからキーサーバ検索とキー管理機能を使って実行できます。

PGP キーウィンドウ

PGP キーウィンドウを開くには、システムトレイのトレイアイコンをクリックし、〔PGP キーの起動〕を選ぶか、または PGP キーアイコンをダブルクリックします。

PGP キーウィンドウにはあなたが自分で作成したキーと、公開キーホルダーに追加した公開キーが表示されます。2 つのキーは自分で作成した秘密＆公開キーペアを表し、1 つのキーは他の人から集めた公開キーを表します。複数のタイプのキーを持っているときは、RSA タイプのキーは青いスケルトンキーで、Diffie-Hellman/DSS は黄色のモダンキーで示されます。

キーをダブルクリックすると、項目ツリーが開き、図形アイコンで表されたキーの所有者のユーザ ID と e-mail アドレスが表示されます。封筒アイコンでは、羽ペンで表されたキーを認定したユーザの署名が調べることができます。キーの情報のレベルをいちいちダブルクリックしたくない場合は、知りたいキーを選択して〔編集〕メニューから〔選択したツリーを開く〕を選んでください。

PGP キー属性の定義

ウィンドウの一番上にはキーに関連する属性に対応するラベルがあります。

名前：キーのアイコンと、所有者のユーザ名と email アドレス、署名者の名前が表示されます。

有効性：キーが実際に所有者と称する人のものであるかの信用度を示します。有効性は誰がキーに署名したか、そしてキーの認証を保証する署名者をあなたがどの程度信用しているかによって決められます。あなた自身が署名した公開キーは、誰かのキーが有効であると信じていなければあなたは署名しないということを前提に、最高レベルの有効性を持ちます。あなたが個人的に署名していない他のキーの有効性は、キーに署名した他のユーザにあなたが授与した信頼レベルによって決まります。キーに関連する署名がなければ有効とはみなされず、このキーを使うたびに有効ではないことを知らせるメッセージがでます。

有効性は絶対的信頼を示すダイヤモンドかストライプのバーと円、不完全な信頼を示す半塗りか空白のバーで示されます。ダイヤモンドまたは円をクリックすると、〔署名キー〕ダイヤログボックスがでます。ここで他のユーザのキーに署名できます。この章の「誰かの公開キーに署名する」を参照してください。有効性はダイヤモンドまたは円で表されます。ダイヤモンドは暗黙の有効性を表し、塗られた円は完全な有効性を表します（〔選択〕ダイヤログボックスの〔詳細〕タブの〔限界有効キーを無効にする〕のチェックボックスが選択されていない場合も、限界有効） 。空の円は有効性なし、または〔限界有効キーを無効にする〕のチェックボックスを選択した場合には限界有効レベルを表します。

信頼性：他人の公開キーの紹介者となるキーの所有者に与えた信頼レベルを示します。この信頼性は、自分で誰かの公開キーの有効性を確認できなく、代わりにキーに署名した他のユーザの判断に委ねるときに働きます。キーペアを作成したとき、キーは、信頼性と有効性バーのストライプまたはダイヤモンドの有効性インディケータによって示されるように、絶対信頼できるとみなされます。

公開キーホルダーにあるユーザのキーの別のもので署名された公開キーを誰かから受け取ったとき、認証レベルはあなたがそのキーの署名者に与えた信頼性を元にします。信頼レベルは〔キープロパティ〕ダイヤログボックスで〔完全に有効〕、〔最低限有効〕または〔無効〕を割り当てます。

信頼性は最初は PGP キーディスプレイに表示されません。〔キー〕メニューから〔表示カラム選択〕を選び、信頼性カラムを表示できます。メインウィンドウの〔有効性〕ボタンをクリックし、「署名キー」ダイヤログボックスを開きます。〔有効性〕ボタンは、キーの有効性が当然であればダイヤモンドに変わります。

「絶対的信頼」が設定されていると、信頼性はダイヤモンドで表示されます。信頼性は〔キープロパティ〕メニューから変更できます。信頼性オプションは「なし」「最低限有効」および「完全に有効」です。

作成日：キーが最初に作成された日付です。キーがどのくらい流通しているかを元にキーの有効性を憶測できるときがあります。キーがしばらく使われていたならば、多数のコピーが出回っているので、誰かがそれを書き換えようとしている見込みは少ないです。作成日だけで有効性を判断してはいけません。

有効期間：キーが期限切れになる日付です。たいていは「なし」に設定されますが、限られた期間キーを使うこともあります。

サイズ：キーを作成するときに使われたビット数を示します。一般的に、キーが大きいほど、危険にさらされる可能性が少なくなります。ところが、大きいキーは小さいキーと比べ、暗号化と復号化に少し時間がかかります。Diffie-Hellman/DSS キーを作成したとき Diffie-Hellman 部分に１つの数字、DSS 部分にもう１つの数字があります。キーの DSS 部分は署名に使われ、Diffie-Hellman 部分は暗号化に使われます。

キープロパティを調べる

PGP キーウィンドウに示された一般属性のほか、他のキープロパティを調べて変更できます。あるキーのプロパティをアクセスするには、希望のキーを選択し、キーメニューから〔キープロパティ〕を選びます。

キー ID：キーに関連する唯一の識別番号。この識別番号は、同じユーザ名と email アドレスを共有する２つのキーを区別するときに便利です。

作成日付：キーが作成された日付

キータイプ：キータイプは RSA または Diffie-Hellman/DSS のどちらかです。暗号は CAST 、Triple DES または IDEA です。これは選ばれた暗号法で、あなたがキーを暗号化するキーの所有者が要求します。アルゴリズムが高度設定で有効になっていれば、このキーを暗号化するときに利用でき、この暗号法はコンベンショナル暗号化から使われます。

有効期間：キーが期限切れになる日付。所有者は、キーを作成するときにこの日付を指定しますが、普通は〔なし〕に設定されます。ところが、所有者がキーを期間限定で使用したい場合には、一部のキーはある日付で期限切れになるように設定されます。

信頼モデル：キーの認定と、誰かほかの人の公開キーの認証を保証する所有者についてのあなたの信頼レベル元に、キーの有効性を示します。信頼レベルは、バーを適当なレベル（「完全に有効」「最低限有効」または「無効」） にスライドさせて設定します。廃止、期限切れおよび暗黙の信頼キーでは自分のキーのようにはバーが表示されません。

指紋：キーが作成されたときに作成されるユニークな識別番号。これは、キーの認証をチェックできる最初の手段です。指紋を照合する１つのよい方法は、電話で所有者に指紋を読みあげてもらい、それを公開キーのコピーに表示された指紋と照らしあわせることです。キーのコピーにある指紋とキーサーバに登録されたものを照合して、誰かのキーの認証をチェックすることもできます。これは、所有者が定期的に点検し、依然として有効であるか確認していると想定されるからです。

有効性：キーが現在、有効であることを示します。キーが無効の場合は、PGP キーウィンドウで暗い表示になり、復号化と認署以外の PGP 機能の実行には利用できませんが、キーはキーホルダーに保存されたままで、いつでも再び有効にできます。キーを有効または無効にするには、〔有効〕チェックボックスを選択またはクリアするか〔キー〕メニューから〔有効〕または〔無効〕を選びます。この機能は、暗号化された email を送信するとときに、PGP キーウィンドウがキーで散らかるの防止するときに役に立ちます。

パスフレーズの変更：秘密キーのパスフレーズを変更します。パスフレーズが盗まれた思ったら（おそらく肩ごしに覗いた人を取り押さえた）、このボタンをクリックし新しいパスフレーズを入力してください。パスフレーズは６ケ月毎に変更するのが賢明です。

デフォルトキーペアを指定する

メッセージまたは誰かの公開キーに署名するときは、デフォルトキーペアが使われます。複数のキーペアを持っていて、１つのキーペアをデフォルトキーペアに指定したい場合があります。現在のデフォルトキーペアは他のキーと区別するため太字で表示されます。

デフォルトキーペアの指定

1. デフォルトキーペアに指定したいキーペアを選択します。

2. 〔キー〕メニューから〔デフォルトキーとして設定〕を選びます。選択されたキーは太字で表示され、デフォルトキーペアとして指定されていることを示します。

新しいユーザ名またはアドレスを追加する

複数のユーザ名または email アドレスを持っていることがあります。同じキーペアを使いたいからです。新しいキーペアを作成した後、キーに別の名前とアドレスを追加できます。秘密キーと公開キーの両方を持っている場合は、新しいユーザ名または email アドレスを追加できるだけです。

新しいユーザ名またはアドレスを既存のキーに追加

1. 別のユーザ名またはアドレスを追加したいキーペアを選択します。
2. 〔キー〕メニューから〔名前の追加〕を選びます。

   〔PGP 新規ユーザ名〕ダイヤログボックスがでます。
3. 新しい名前を入力し、[Tab] キーを押し次のフィールドへ進みます。
4. 新しい email アドレスを入力して、[OK] をクリックします。

   〔PGP パスフレーズの入力〕ダイヤログボックスがでて、パスフレーズを入力するようメッセージがでます。
5. パスフレーズを入力して、[OK] をクリックします。

これで新しい名前がキーに関連するユーザ名リストの最後に追加されます。新しいユーザ名とアドレスをキーの一次識別子に設定したい場合は、名前とアドレスを選択し、〔キー〕メニューを選び、〔プライマリユーザに設定〕をクリックします。

キーの指紋を照合する

キーが特定の人のものであるかは、その人がキーをフロッピーディスクに保存して物理的に手渡さないかぎり、確認はむずかしいことです。このようなキーの交換は普通は現実的ではなく、特に数マイルも離れたユーザどうしでは不可能ですが、キーに関連するユニークな指紋を信頼して、そのキーが確かに所有者と称する人のものであることを認証できます。キーの指紋を照合する方法はいくつかありますが、一番安全な方法はその人に電話をして、指紋を読みあげてもらう方法です。誰がこの偶然の通話を傍受して、あなたの通話相手になりすますことができるとは考えられません。誰かの公開キーのコピーの指紋と公開キーサーバ上のオリジナルのキーに記入された指紋を照合することもできます。

キーの指紋の照合

1. 指紋を照合したいキーを選択します。
2. 〔キー〕メニューから〔キープロパティ〕を選びます。
3. 指紋を書きとめ、オリジナルの指紋と照合します。

誰かの公開キーに署名する

あなたがキーペアを作成したとき、キーはあなたの公開キーを使って自動的に署名されます。同様に、キーが本人のものであるかはっきりしている場合は、その人の公開キーに署名して、あなたがそれを有効なキーと認めていることを示すことができます。

誰かの公開キーに署名

1. 署名したいキーを選択します。

2. 〔キー〕メニューから〔署名〕を選びます。

   〔PGP 署名キー〕ダイヤログボックスがでます。

3. 署名をエクスポートできるようにするか質問がでます。他の人はあなたの署名を信頼することになります。

   あなたの署名をエクスポートしたいならば、このチェックボックスを選択します。

4. あなたの署名を入れたキーをキーサーバへ送信したい場合は、〔選択のサーバタグからキーに署名〕チェックボックスを選択します。サーバ上の公開キーは署名を含めるように更新されます。たいていのユーザは、他の人がキーに署名してよいと自分で決定したがるので、サーバ上のキーに署名を追加するときは、前もって所有者に相談するのが常に賢明です。

   署名はエクスポート可、他の人はあなたの署名を信頼する〕というチェックボックスが表示されます。エクスポートできる署名とは、キーサーバ上でユーザの公開キーが一緒に表示され、サーバへ送信でき、キーを email メッセージにドラッグしてコピーしたときにキーと一緒に移動するものです。

   〔項目増加〕ボタンが表示されます。

5. このボタンをクリックすると、次の署名タイプが表示されます。

    - エクスポート不可：キーは有効と信じても、他人があなたの署名を信頼してほしくない場合、この署名を使用してください。この署名タイプは関連するキーと一緒にキーサーバへ送信できず、どのような方法でもエクスポートできません。
    - エクスポート可：署名はキーと一緒にキーサーバへ送られ、他人があなたの署名を信用し、結果としてあなたのキーを信頼してよければ、エクスポート可の署名を使用してください。これは PGP のすべての旧バージョンで使われた署名です。
    - 信頼する紹介者：あなたがこのキーが有効であり、キーの所有者はあなたをメタ紹介者として指名した人による他のキーの保証を完全に信用すべきであることを認定する場合に使用してください。
    - メタ紹介者：このキーと、信頼する紹介者をもつこのキーで署名されたキーはあなたにとって完全に信頼する紹介者

    - であることを認定します。

6. [OK] をクリックして、キーが実際に所有者と称する人のものであると確信していることを示します。

7. 〔PGP 署名パスフレーズ〕ダイヤログボックスがでます。デフォルトキーペアのパスフレーズを入力するようメッセージがでます。

8. 誰かの公開キーに署名した場合、あなたのユーザ名に関するアイコンがそのキーに表示されます。

キー有効性の信頼性を授与する

キーがある人のものであることを認定するほか、キーのユーザに信頼レベルを割り当てて、あなたが将来、入手するかもしれないキーを持っている他の人の紹介者としてどの程度信用しているか示すことができます。つまりキーを誰かから入手し、そのキーにあなたが信用できると指名した人の署名が入っていた場合、あなたが自分でチェックしたことがなくとも、そのキーは有効とみなされます。

キー有効性の信頼性の授与

1. 信頼レベルを変更したいキーを選択します。
2. 〔キー〕メニューから〔キープロパティ〕を選びます。

   〔プロパティ〕ダイヤログボックスがでます。
3. 信頼レベルのスライドバーを使って、キーの信頼レベル、〔無効〕〔最低限有効〕〔完全に有効〕の中から、適切なものを選びます。
4. [OK] をクリックして、新しい設定を書き込みます。

キーを無効および有効にする

一時的にキーを無効にしたいことがあります。キーを無効にする機能は、将来使うために公開キーをそのままにしておきたい場合には便利ですが、メールを送信するたびに受信者リストをひっくりかえすことはしたくありません。

キーを無効にする

1. 無効にしたいキーを選択します。
2. 〔キー〕メニューから〔無効〕を選びます。

   キーは暗い表示になり、一時的に使用できなくなります。

キーを有効にする

1. 有効にしたいキーを選択します。
2. 〔キー〕メニューから〔有効〕を選びます。

   キーは見えるようになり、今まどおり使用できます。

キーまたは署名を削除する

ある時点で、キー、署名または特定のキーに関連するユーザ ID を削除したいことがあります。

キー、署名またはユーザ ID の削除

1. 削除したいキー、署名またはユーザ ID をキーを選択します。
2. 〔編集〕メニューから〔削除〕を選びます。

パスフレーズを変更する

パスフレーズは６ケ月毎に変更しておくと安全で、変更は簡単にできます。

パスフレーズの変更

1. パスフレーズを変更したいキーペアを選択します。
2. 〔キー〕メニューから〔キープロパティ〕を選びます。

   〔プロパティ〕ダイヤログボックスがでます。
3. 〔パスフレーズ変更〕をクリックします。

   〔パスフレーズ変更〕ダイヤログボックスがでます。
4. 上のフィールドに古いパスフレーズを入力し、[Tab] キーを押して次のフィールドに進みます。
5. 真ん中のフィールドに新しいパスフレーズを入力して、[Tab] キーを押して下のフィールドに進みます。

6. 新しいパスフレーズをもう一度入力して、入力を確認します。

7. [OK] をクリックします。

キーをインポートおよびエクスポートする

生テキストを切り取り、貼り付けて自分の公開キーを配布したり、公開キーサーバまたはコーポレートキーサーバから他の人の公開キーを入手することがよくありますが、キーを別のテキストファイルとしてインポートおよびエクスポートして交換することもできます。例えば、誰かがあなたに公開キーを保存したディスクを手渡したり、あなたの公開キーを FTP サーバ上で利用できるようにすることができます。

キーをファイルからインポート

1. ファイルからインポートしたいキーを選択します。

2. 〔キー〕メニューから〔インポート〕を選びます。

   〔キーが入っているファイルの選択〕ダイヤログボックスがでます。

3. インポートしたいキーが入っているファイルを選択して〔開く〕をクリックします。

   PGP キーウィンドウにインポートされたキーがでます。このキーを使用して、データを暗号化し、誰かの電子署名を認証できます。

キーをファイルへエクスポート

1. ファイルへエクスポートしたいキーを選択します。

2. 〔キー〕メニューから〔エクスポート〕を選びます。

   〔キーをファイルへエクスポート〕ダイヤログボックスがでます。

3. キーをエクスポートしたいファイル名を入力して、〔保存〕をクリックします。

   エクスポートされたキーは指定ディレクトリの指定ファイルへ保存されます。

キーを email のメッセージから追加

同僚があなたに email メッセージとテキストとして同封したキーを送信した場合、あなたはそのキーをキーホルダーに追加できます。

1. email メッセージを開き、PGP キーウィンドウを開きます。
2. PGP キーウィンドウがメッセージウィンドウの背後になるように、２つのウィンドウを並びかえます。
3. 「BEGIN PGP PUBLI KEY BLOCK 」と「END PGP PUBLIC KEY BLOCK」テキストに挟まれるキーテキストを選択します。
4. 〔インポートするキーの選択〕ダイヤログボックスがでて、コピーするキーが表示されます。〔全て選択〕「全て非選択〕〔インポート〕または〔キャンセル〕を選び、コピーしたいキーを選びます。
5. 新しいキーが PGP キーウィンドウにでます。

キーを廃止する

あなた個人のキーペアが信頼できない場合は、廃止を発表して、全員にあなたの公開キーの使用をやめるよう通知できます。廃止キーを広める一番よい方法は、公開キーサーバに置くことです。

キーの廃止

1. 廃止するキーペアを選択します。

2. 〔キー〕メニューから〔廃止〕を選びます。

   メッセージと、キーの廃止に伴う影響について短いお知らせがでて、選択したキーを本当に廃止したいのか指定するようメッセージがでます。

3. 〔はい〕をクリックして、選択したキーの廃止を確認します。

   〔PGP パスフレーズの入力〕ダイヤログボックスがでて、パスフレーズを入力するようメッセージがでます。

4. パスフレーズを入力して、〔OK〕をクリックします。

   キーを廃止すると、赤い×印が付き、有効ではないことを示します。

5. 廃止したキーをサーバへ送り、全員に古いキーを使用していないことを知らせます。

いつかパスフレーズを忘れることがあります。この場合は、キーを二度と使用できなくなり、新しいキーを作成したときに古いキーを廃止することができません。このような場合に備え、秘密キーのコピーを作り、そのコピーを廃止し、オリジナルのキーは安全な所に保管して、廃止キーを作成できます。パスワードを忘れても、後で廃止したコピーを公開キーサーバへ送信できます。ただし、廃止したほうのキーを保存する場所に十分に注意してください。誰かが廃止キーを見つけたら、あなたのキーを承認なしで廃止できます。

環境設定

PGP は一般ユーザのニーズに対応できるように構成されていますが、一部の設定を編集して特定のコンピューティング環境に合わせて構成できます。設定は〔選択〕ダイヤログボックスで指定します。このダイヤログボックスは次の方法でアクセスできます。

- トレイアイコンをクリックして〔選択〕を選ぶ
- PGP キーウィンドウで編集メニューから〔選択〕を選ぶ。

一般環境

一般的な暗号設定は〔一般〕ウィンドウから指定します。

常にデフォルトキーを暗号化：このチェックボックスを選択すると、受信者の公開キーを使って暗号化する email メッセージと添付ファイルはすべて、やはりあなたのデフォルト秘密キーを使って暗号化されます。この設定をオンのままにしておくと、以前に暗号化した email またはファイル内容の復号化を選択できるので、便利です。

復号化パスフレーズのキャッシュ：この設定では暗号化パスフレーズがコンピュータのメモリに保存されている時間（時間： 分： 秒の形式） で指定します。email メッセージを定期的に作成したり、連続して複数のメッセージを読み込む場合は、email をすべて処理するためにパスフレーズを何度も入力しなくてすみように、パスフレーズのキャッシュでの保存時間を長くします。

ただし、パスフレーズをコンピュータのメモリに長く保存するほど、頭のよいスパイがこのひどく危険にさらされている情報を見つける回数が増えることを覚えておいてください。初期設定は２分です。おそらくたいていの PGP 処理はこれで十分で、パスフレーズを何度も入力する必要はありません。一方、あなたがコンピュータのメモリをウロウロしたり、攻撃者がパスフレーズを探しだすには十分な時間ではありません。

署名パスフレーズのキャッシュ：この設定では署名パスフレーズがコンピュータのメモリに保存されている時間（時間：分： 秒の形式） で指定します。email メッセージを定期的に作成したり、連続して複数のメッセージを読み込む場合は、email をすべて処理するためにパスフレーズを何度も入力しなくてすみように、パスフレーズのキャッシュでの保存時間を長くします。

署名のパスフレーズを使うことは、攻撃者があなたになりすまそうとできるので、場合によってはより脅威とみなされます。これは〔署名パスフレーズのキャッシュ〕が復号化とは別に処理されるからです。キャッシュタイマは、あなたがメッセージに署名するたびに作動し、タイマが期限切れになると直ちにパスフレーズをメモリから消去します。このキャッシュの初期値は複雑なセキュリティ関係のためオフになっています。

キーの高速作成：このチェックボックスを選択すると、新しい Diffie-Hellman/DSS キーペアの作成時間が短縮されます。このプロセスは、新しいキーを作成するたびにゼロから時間のかかるプロセスを処理するのではなく、以前に計算された素数セットを使うことで

スピードアップします。ただしキーの高速作成は、キーを作成するときにオプションとして提示された 1024 から 4096 の固定キーサイズでだけ実施され、それ以外の値を入力してあると利用できないことを覚えておいてください。誰かがこれらの同一内容の素数を知識を元にあなたのキーを解くことはほとんど不可能ですが、最高レベルのセキュリティをもつキーペアの作成に特別な時間を費やしたいことがあります。たいていの暗号使用者は、「同一内容の素数」の使用は大きなセキュリティリスクは与えないと信じています。

完全削除確認の表示：この設定を選択すると、ファイルを完全削除する前にダイヤログボックスがでて、PGP がファイルの内容に上書きし、コンピュータから削除する前に気が変わっていないか確認の最後のチャンスが与えられます。

ファイル環境

〔ファイル〕タブでクリックし、秘密キーと公開キーの保存に使うキーホルダーの場所を指定するウィンドウへ進んでください。

公開キーホルダーファイル:PGP プログラムが公開キーホルダーファイルを探そうとする現在の場所とファイル名を表示します。公開キーを別の名前または他の場所でファイルに保存する場合は、その情報をここで指定します。〔参照〕ボタンを使って、パスを入力せずにファイルを検索できます。これは公開キーの自動バックアップが保存される場所でもあります。

秘密キーホルダーファイル:PGP プログラムが秘密キーホルダーファイルを探そうとする現在の場所とファイル名を表示します。秘密キーを別の名前または他の場所でファイルに保存する場合は、その情報をここで指定します。ユーザの中には秘密キーホルダーファイルをフロッピーディスクに保存する人がいます。その場合、メールの署名と復号化が必要なときにはキーのようにこのディスクを挿入します。これは秘密キーの自動バックアップが保存される場所でもあります。

ランダムシードファイル：randseed.bin ファイルの位置を示します。このファイルには暗号化とキー作成中に使われるランダムデータが格納されます。ユーザの中には改竄防止のためランダムシードファイルを安全な場所に保管する人がいます。これで不正使用の攻撃はひどく困難で、PGP にはさまざまな保護機能があります。

email 環境

〔email 〕タブでクリックし、PGP 機能が PGP プラグインによってサポートされる email アプリケーションで実施される方法に影響を与える設定を指定するウィンドウへ進んでください。

email 送信時に PGP/MIME を使用：このチェックボックスを選択すると、email を送信するたびに PGP/MIME をオンにする必要はありません。Eudora を使い、この設定をオンにしてあれば、email メッセージと添付ファイルはすべて自動的に暗号化、署名され、宛先の受信者へ送られます。この設定はクリップボードや Windows エクスプローラで行った他の暗号化には影響しません。PGP/MIME 標準対応ではない email アプリケーションを使っている受信者に email を送る場合は、このオプションを使わないでください。Eudora を使うと、添付ファイルはこの設定に関係なく常に暗号化されますが、受信者が PGP/MIME をサポートしていない場合は、PGP ツールを使いメッセージを復号化しなければなりません。

ワードラップの指定：この設定は、電子署名のテキストを次行へワードラップするのにハードキャリッジリターンが使われるカラム数を指定します。どのアプリケーションも同じようにワードラップを処理しているのではないため、この機能が必要です。

PGP でワードラップ設定を変更する場合は、email アプリケーションのワードラップ設定よりも少なくしてください。同じかまたは長く設定すると、キャリッジリターンが追加され、PGP 署名が無効になります。

デフォルトとして新規メッセージを暗号化：すべての email メッセージを暗号化します。鍵アイコンはインデントされたままで暗号機能がオンになってていることを示します。

デフォルトとして新規メッセージに署名：すべての email メッセージに署名します。羽ペンアイコンはインデントされたままで署名機能がオンになっていることを示します。

オープン時に自動的に復号化 / 署名確認：メッセージを開いたときに、email を自動的に復号化します。

キーサーバ環境

〔サーバ〕タブでクリックし、使用するキーサーバの設定を指定するウィンドウへ進んでください。

サーバ：PGP が公開キーを送信、検索するときに使う公開キーサーバのインターネットのドメインアドレス（例 company.com）を指定します。このドメインは、キーのドメインを元に適切なキーを調べるためにサーバへキーを送るときに使われます。

ポート：公開キーサーバのポートアドレス。このアドレスは http://pgpkeys.mit.edu:11371 のように完全な URL フォーマットで入力しなければなりません。LDAP プロトコルもサポートされます。

サーバとキーを自動同期：このダイヤログボックスで次のオプションを指定し、秘密キーホルダーとキーサーバを同期化します。

- 不明ユーザの暗号化：PGP は、不明受信者があなたのキーホルダーにない場合、メッセージを暗号化するときにサーバ上で検索するので、そのユーザのキーを見つけられます。
- キーへ名前を追加：追加されるキーは追加の前にサーバから更新され、完了時にサーバへ送信されます。処理前のサーバからの更新で、例えば、そのキーが最後に更新されてから廃止されていないことを確認します。
- キーに署名：署名されるキーは署名の前にサーバから更新され、完了時にサーバへ送信されます。処理前のサーバからの更新で、例えば、そのキーが最後に更新されてから廃止されていないことを確認します。
- 廃止：廃止されるキーは廃止の前にサーバから更新され、完了時にサーバへ送信されます。処理前のサーバからの更新で、例えば、そのキーが最後に更新されてから廃止されていないことを確認します。次の設定を使い、キーを自動同期するサーバを選んでください。
- 新規：新しいキーサーバを選びます。キーサーバのドメインを入力し、HTTP または LDAP アドレスを選びます。
- 削除：使用しているキーサーバの１つに登録されているキーサーバを削除します。
- デフォルトを設定：どのキーサーバをデフォルトキーサーバにするか選びます。選ぶデフォルトキーサーバがあるか分からない場合は、アドミニストレータに相談してください。

詳細環境

〔詳細〕タブでクリックし、次の選択を行ってください。

使用可能アルゴリズム：CAST（デフォルト） 、IDEA または Triple-DES の中から、PGP キーの暗号化アルゴリズムを選択できます。IDEA または Triple-DES を使う場合は、キーを作成する前にこの選択を行わなければなりません。CAST は PGP が安全であると信じている新しいアルゴリズムで、Triple-DES はテスト時点で合格した政府のアルゴリズムです。IDEA は PGP で今まで使われたアルゴリズムです。これらのアルゴリズムについて詳しくは、第 8 章「セキュリティ機能と脆弱性」の「PGP 対称アルゴリズム」を参照してください。

PGP で暗号化アルゴリズムを変更できるようにしたのは次の２つの理由からです。

- 従来の暗号化を使う場合は、ここで選択された暗号法が暗号化に使われます。
- キーを作成するとき、選んだ暗号法がキーの一部として記録され、他の人があなた宛を暗号化するときはそのアルゴリズムを使用します。

あるアルゴリズムが安全でないと判断した場合にのみ、このチェックボックスを利用してください。Triple-DES が解かれたことが分かったら、そのボックスを非選択にするだけでメッセージは破られていないアルゴリズムを使って暗号化されます。それ以降に作成されるキーには、Triple-DES は暗号化に利用できないという記録を持ちます。

限界有効レベルの表示：限界有効なキーを表示したり、有効性のオン、オフを表示するときにこのチェックボックスを選択してください。緑の円はキーが有効であることを示します。グレーはキーの有効性が確認されていない、信頼する紹介者やあなたの署名があるまたはあなた自身が作成したキーなので絶対に信頼できることを示します。

限界有効キーを無効にする：限界有効キーをすべて無効にするときにこのチェックボックスを選択してください。このボックスを選択した場合、限界有効キーを暗号化するときにキー選択ダイヤログボックスがでます。

ADK を持つキーでの暗号化を警告：マスタ復号キーを持つキーで暗号化する時、警告を表示するように設定します。

第 7 章

PGP のトラブルシューティング

この章では、起こりえるトラブルとその対応処置について説明します。

表 1：

エラー	考えられる原因	対応処置
出力バッファが小さいため要求された処理は実行できません。	出力が大きく、内蔵バッファが処理できません。暗号化、署名するならば、メッセージを分割して細かく暗号化／署名する必要があります。	復号化、署名確認するならば、送信人に細切れで暗号化／署名し、送信し直すよう頼んでください。
キーが十分な有効性がないため、指定されたキーをこの処理に使用することはできません。	有効性がないキーは処理に使用できません。	キーに自分のキーで署名し信頼できるようにして、やり直してください。
このキーは署名にしか使えませんので、暗号化できませんでした。	指定されたキーは署名にしか使用できません。	別のキーを選ぶか、またはデータに署名できる新しいキーを作成してください。

表 2：

エラー	考えられる原因	対応処置
このキーは暗号化にしか使えませんので、署名はできませんでした。	指定されたキーは暗号化にしか使用できません。	別のキーを選ぶか、またはデータを暗号化できる新しいキーを作成してください。
キーホルダーに秘密キーがありませんでした。	指定された秘密キーがキーホルダーにありません。	PGP キーで自分のキーペアを作成してください。
不正なファイル操作により処理が完了しません。	プロクラムはあるファイルのデータの読み取りまたは書き込みできません。	PGP 選択を変更し、できれば別のファイルを使用してみてください。
指定された署名キーでこのキーは既に署名されています。	既に署名したキーには署名できません。	誤って間違ったキーを選択しました。別のキーを選んで署名してください。
キーホルダーに不正（破壊）PGP パケットが含まれています。処理指定しているメッセージが破壊されているか、キーホルダーが破壊されています。	メッセージが破壊されているか調べるため、差出人にメッセージの再送信してもらいます。	バックアップキーホルダーからキーホルダーを復元してください。

表 3：

エラー	考えられる原因	対応処置
キーホルダーファイルが破壊されています。	プロクラムはあるファイルのデータの読み取りまたは書き込みできません。おそらく破壊または行方不明のファイルがあります。キーホルダーファイルでないかもしれません。	できれば、別のファイル名またはパスを使ってみてください。
メッセージ / データには分離された署名が含まれています。	メッセージまたはファイルの署名が別のファイルにあります。	先に分離された署名ファイルをダブルクリックしてください。
入力したパスフレーズとキーのパスフレーズが一致しません。	入力したパスフレーズが正しくありません。[Caps Lock] がオンになっているか、またはパスフレーズの入力ミスです。	もう一度やり直してください。
PGP ライブラリでメモリが不足しています。	オペレーティングシステムでメモリが不足しています。	起動中の他のプログラムを終了してください。それでも処理できない場合は、マシンのメモリを増設する必要があります。
指定されたキーがキーホルダーにありません。	現在のメッセージの復号化に必要なキーがキーホルダーにありません。	メッセージの送信人にメッセージの再送信と、メッセージをあなたの公開キーへ暗号化したか確認してもらってください。

表 4：

エラー	考えられる原因	対応処置
指定された入力ファイルがありません。	入力したファイル名がありません。	エクスプローラを使って、必要なファイルの正しい名前とパスを探してください。
指定されたキーに既に存在しますので、指定されたユーザ ID は追加できません。	同じユーザ ID がすでにキーにある場合は、追加できません。	別のユーザ ID を追加するか先に同じ ID を削除してください。
キーホルダーのオープン/ 書込み、またはファイルの出力中でエラーが起きました。	必要なファイルがオープンできませんでした。	PGP 選択の設定が正しいか確認してください。PGP をインストールしたディレクトリのファイルを最近削除した場合は、PGP を再スントールする必要があります。
十分なランダムデータがありません。	乱数ジェネレータで適切な乱数を作るためにさらに入力が必要です。	マウスを動かすか、でたらめにキーを押して、入力を作成してください。

表 5：

エラー	考えられる原因	対応処置
このファイルは読取り専用あるいはプロテクトされていますので、処理は実行できません。	キーホルダーファイルを取り外し可能媒体に保存する場合媒体が挿入されていません。必要なファイルが読取り専用ーに設定されているか、または別のプログラムが使用しています。	起動しているプログラムと同じファイルをアクセスしている他のプログラムを終了させてください。キーホルダーファイルをフロッピーに保存するならば、フロッピーディスクがフロッピードライブに入っているか確認してください。

第 8 章

セキュリティ機能と脆弱性

この章では Phil Zimmerman が開発した暗号作成 （解読） 法についての紹介し、その社会的背景について説明します。

「なすことは十分でないが、それをすることが大切である」

マハトマ・ガンジー

私が PGP を作った理由とは

個人的であり、プライベートな理由であり、あなた達以外の誰にも関係なことです。政治キャンペーンを企画したり、税金について議論したり、秘密のロマンスがあるとします。または、弾圧的な国の反体制活動家者と連絡をとりあっているとしましょう。それが何であれ、プライベートな電子メール（email） や機密文書を誰かに読まれたくありません。あなたのプライバシーを主張することは間違ったことではありません。プライバシーは憲法と同じように「米国人が尊重するもの」です。

プライバシーを守る権利は権利宣言にそれとなくもり込まれています。ところが、米国憲法が作られたとき、憲法の起草者はプライベートな会話を守る権利を詳細に書き入れる必要はないと考えました。そもそもそれが愚かなことだったのです。200 年前は、どの会話も秘密でした。誰かが聞こえるところにいたら、納屋の裏にまわって話しをすればよかったのです。知らないうちに人に聞かれることはありませんでした。現代の技術を考えれば、個人の会話を守る権利は、哲学的な意味だけでなく、物理学の法則の意味で当然の権利です。

ところが、電話の発明とともに情報時代になり、すべてが変わりました。現在、私たちの会話の大半は電子的に行われています。これで、とても個人的な会話は私たちが知らないうちに人目にさらされます。携帯電話はラジオを使って誰でも傍受できます。電子メールはインターネットをつうじて送信されますが、携帯電話と同様安全ではありません。電子メールは急速に郵便物にとって代わり、誰にとっても普通のことになり、昔のような目新しさはありません。しかも電子メールは決まりきった手順で自動的に興味のあるキーワードがあるか大規模に調べることができ、何も検出されません。これでは流し網漁のようなものです。

おそらく、あなたの電子メールは暗号化が正しいとは認められないほど合法的と思っているでしょう。あなたが本当に法律を遵守する市民で隠すものは何もないならば、なぜいつもはがきで郵便を送らないのですか？　なぜ要求ありしだい薬物テストに提出しないのですか？なぜ家宅捜索の令状が必要なのですか？　何か隠そうしていますか？　郵便を封筒に隠すのは、あなたが破壊的な活動家や麻薬の売人だからですか、それとも異常に疑い深い変人だからですか？、法律を遵守する市民に電子メールを暗号化する必要がありますか？

一体、法律を遵守する市民はその郵便にはがきを使うべきだと誰が信じていましたか？社会規範に従わない人が封書を使ってプライバシーを守ろうとしたら、疑われるでしょう。おそらく当局は郵便物を開封し、何を隠しているのか調べるでしょう。幸いにも、私たちはそのような世界には住んでいません。誰もたいていの郵便は封書にして守るからです。だから封筒に入れてプライバシーを守っても誰も疑われません。数の上で安全です。同じように、潔白であろうとなかろうと、誰もが email に日常的に暗号文を利用したらすばらしいことで、email のプライバシーを暗号文で守っても誰も疑われません。団結の１つの形と考えましょう。今までは、政府が一般市民のプライバシーを侵害したければ、ある程度の費用と労力を費やして、封書を横取りし、蒸気を使って開封して読まなければなりませんでした。さもなければ、少なくとも自動音声認識技術が実用化するまでは、電話の通話を聞いて録音しなければなりませんでした。このような大きな労働力を要する傍受は大がかりには行われませんでした。お金と労力を費やす価値があると考えられる重大なケースで行われるだけでした。

上院議案 266、1991 犯罪防止法案は人々を不安にさせる法案が隠されていました。この拘束力のない決議案がもし現実の法律になっていたら、安全な通信機器メーカーは製品に特殊な「トラップドア」を組み込むことが義務づけられ、政府は誰かの暗号メッセージを読むことができました。つまり、「電子通信サービスのプロバイダと電子通信サービスの機器メーカーは、法律で妥当と認められた場合に政府が音声、データ、および他の通信の平文テキストを入手できる通信システムを作るというのが議会の意見である」と解釈できます。この議案こそが、私をその年に PGP をフリーソフトウェアとしてダウンロードできるようにさせたのです。一般市民の自由論者や業界グループによる猛烈な抗議にあって法案が否決される直前のことでした。1994 デジタル電話議案は、諜報員が出かけて、わに口クリップを電話線に取り付けずにすむように、電話会社はリモートワイヤタッピングポートを電話局のデジタル交換機に組み込み、「ポイントアンドクリック」盗聴のための新しい技術インフラストラクチャを作ることを命じました。現在、ワシントンの本部に座って、あなたの通話を傍受できます。もちろん、法律上、今でも盗聴には裁判所の命令が必要ですが、技術インフラストラクチャが数世代、存続するうちに、法律と政策は一夜にして変わります。いったん監視に最適な通信インフラストラクチャがゆるぎないものになったら、政策の変化によって、この新しく発見された権限が悪用されるかもしれません。政治状況は新しい政府の選挙とともに変化するかもしれず、連邦政府のビル爆破から突然やってくるかもしれません。

1994 デジタル電話議案が可決された１年後、FBI は電話会社はそのインフラストラクチャに米国の主要都市の全通話の 1% を同時に盗聴できる機能を組み込まなければならないという案を発表しました。1% とは、盗聴できる電話数にすると以前のレベルの千倍以上の増加を表します。それまで米国での裁判所の命令による盗聴は、連邦、州および地方自治体を合わせても、年に約 1000 件しかありませんでした。政府は全通話の 1% の盗聴を許す盗聴命令にサインする人数の判事をどうやって雇うのか想像しにくいことです。リアルタイムでその通話をすべて座ったまま聞く諜報員を雇うのはもっと想像できません。それほどの通話量を処理できると思える方法はただ１つ、すべてを精密に調べる自動音声認識技術の強力な 0rwellian アプリケーションで、興味のあるキーワードを捜したり、特定の話し手の音声を調べます。政府は最初の１％のサンプルでターゲットが見つからないと、ターゲットを探しあてるまで、あるいは全員の電話線で破壊活動の通話がないか調べられるまで盗聴はさらに別の１％を調べることができます。FBI は、将来に備えてこの能力を必要としているという意見です。この案は、少なくとも 1995 年の現時点では、激しい怒りをかい議会で否決されました。ところが、FBI はそれどころかこの広範な権限を要求したという事実だけで彼らの協議事項の表れです。そして、この案の否決は、1994 デジタル電話議案も 1993 年に初めて提出されたときは否決されたということを考えれば、それほど安心できません。技術の進歩は、プライバシーに関するかぎり、現状維持を許しません。現状は流動的です。私たちが何もしなければ、新しい技術は、スターリンが夢みたことがない新しい自動監視能力を政府に与えます。情報時代でプライバシーを防衛する唯一の方法は、強力な暗号作成・解読法です。

政府が暗号作成・解読法を利用したがっていると疑う必要はありません。ビジネスはライバル企業、組織犯罪または外国政府に盗聴されます。例えばフランス政府は、米国の会社に対する信号インテリジェンス機器の使用で悪名高く、フランス企業が競争でリードすることに役立っています。皮肉にも、米国政府の暗号作成・解読法にかんする規制が米国企業の外国の知能組織犯罪への防衛力を弱めました。

政府は、暗号作成・解読法が人々との力関係で果たすきわめて重要な役割が何であるかを知っています。1993 年 4 月、クリントン政権は大胆で新しい暗号化政策のイニシアチブを明らかにしました。これはブッシュ政権の発足以来、全米安全保障局（NSA） で開発中でした。このイニシアチブのもっとも重要なものは、クリッパークリップといわれる政府製造の暗号装置で、新しい機密扱いの NSA 暗号化アルゴリズムを組み込んでいます。政府は民間産業の傍受される危険がない電話、ファックスなどの通信製品すべてに設計段階でそれを組み込むように奨励しようとしました。AT&T はクリッパーを傍受される危険がない音声製品に組み込みました。手に入れる価値のあるもの：製造時に、クリッパークリップにはユニークなキーがロードされ、政府はキーの保存を始め、エスクロウに預けます。心配することはありません。政府は、「法律で正当と認められた場合」だけこのキーを使ってあなたの通話を読みとると約束しています。』もちろんクリッパーを活用するため、論理的に考えて次は、他の暗号作成・解読法を法的に無効にするでしょう。

政府は最初、クリッパーの使用は自由意思で、誰も他のタイプの暗号作成・解読法の代わりに使うことを強制されないと主張しました。ところが、クリッパーチップに対する一般の反応は強く、政府の予想よりも強いものでした。コンピュータ業界は一致団結してクリッパー使用に反対を発表しました。

FBI ディレクタ Louis Freeh は 1994 年のプレス会議の質問に、クリッパーが一般の支持を得られず、FBI の盗聴が政府以外が管理する暗号作成・解読法で締め出されたら、FBI としては法的な救済方法を探さざるをえない」と答えました。その後、オクラホマシティの悲劇の余波で、Feeh 氏は、強力な暗号作成・解読法の普及を政府が食い止めなければならないと上院司法委員会で証言しました （暗号作成・解読法が爆弾魔によって使われたことは誰も言わなかったけれど） 。電子プライバシー情報センター（EPIC）は情報公開法の下で意味のある書類を入手しました。「暗号化：その脅威、用途および考えられるソリューション」というタイトルで、1993 年 2 月に国家安全保障会議に送られた簡単な報告書の中で、FBI 、NSA および司法省（DOJ） は「技術的な解決策はお粗末ながら、すべての暗号化製品に組み込まなければ役に立たない。このためには、政府承認の暗号製品の使用、または政府の暗号化基準に従うことを命じる法律が必要だ」という結論を下しました。

「政府は市民の自由を決して悪用しない」とは信用できない実績があります。FBI の COINTELPRO プログラムは、政府の政策に反対するグループをターゲットにするものでした。反戦運動や公民権運動をひそかに調査しました。マーチンルーサーキングジュニアの電話を盗聴しました。ニクソンは敵対相手のリストを持っていました。そしとその後、ウォーターゲート事件が起きました。議会は今、インターネット上での市民の自由を制限する法律を通過させようとしています。今だかつて、政治的にこれほど広く一般市民の政府への不信感が広まったことはありません。暗号作成・解読法を法的に無効にしようという、人々を動揺させる政府のこのような動向に抵抗したければ、私たちが利用できる１つの手段それは暗号作成・解読法がまだ合法な今のうちにできるだけ利用することです。強力な暗号作成・解読法の使用が普及すれば、政府が有罪とするのがむずかしくなります。したがって、PGP を使うことは、民主主義を守るために役に立ちます。プライバシー保護が奪われると、アウトローだけがプライバシーを持つことになります。情報局は優れた暗号作成技術を利用できます。そして大物の武器、麻薬商人が利用します。しかし、普通の人や草の根市民団体はたいてい、手頃な値段の「軍レベル」の公開キー暗号法技術を利用できませんでした。今まではですが。

PGP は人々に自分のプライバシーは自分で管理する能力を与えます。

社会のニーズが高まっています。だからこそ、私は PGP を作ったのです。

暗号化の基本

まずはいくつのか基本用語です。メッセージを同僚に送信したいとします。アリスとしましょう。そしてアリス以外は読めないようにしたいとします。図１に示したように、メッセージを暗号化または暗号文にできます。つまり、メッセージを気の遠くなる複雑な方法でスクランブルして、あなたとアリス以外は読めないようにします。あなたはメッセージを暗号化する暗号作成キーを提供し、アリスは同じキーを使って解読または復号化しなければなりません。少なくとも、そのように従来の「秘密キー」暗号化では機能しています。暗号化と復号化の両方で１つのキーが使われます。つまり、このキーをまず盗聴の危険がないチャンネルをつうじて送信し、暗号化されたメッセージが盗聴の危険があるチャンネルをつうじて送信される前に両者がこのキーを知ることができるようにしなければなりません。これでは不便です。キーを交換する安全なチャンネルがあるなら、まず第一になぜ暗号を作成する必要があるのですか？

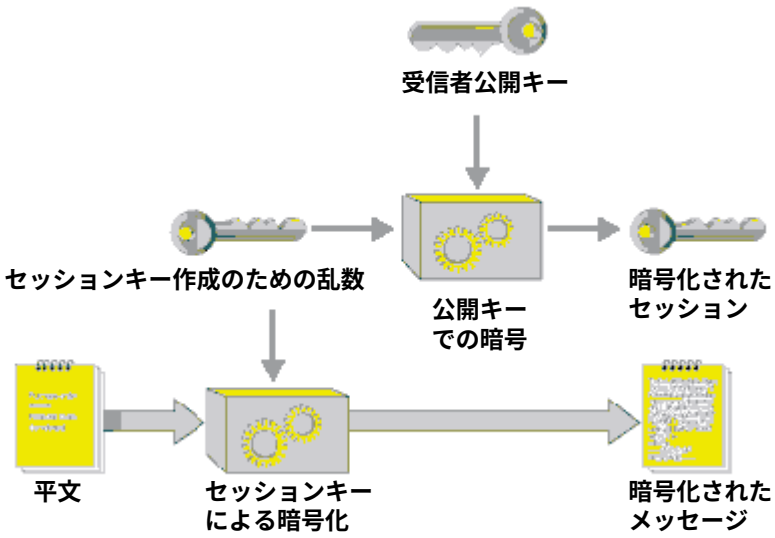

図 1： 暗号化の基本

公開キー暗号作成 （解読） 法はどのうように機能するか？

公開キー暗号作成 （解読） 法では、図２に示したように、誰でも２つの関連する補完キー、公開キーと秘密キーを持っています。それぞれのキーは他のキーが作成するコードのロックを解除します。公開キーを知っていても対応する秘密キーの類推には役に立ちません。公開キーは通信ネットワークをつうじて公表でき、広範に広めることができます。

このプロトコルは、従来の秘密キー暗号化で必要な同じ種類の安全なチャンネルを必要とせずにプライバシーを提供します。

誰でも受信者の公開キーを使ってその人宛のメッセージを暗号化でき、その受信者は自分の対応する秘密キーを使って、そのメッセージを復号化します。他の人はその秘密キーをアクセスできないため、受信人以外の人は復号化できません。受信人の公開キーを使ってメッセージを暗号化した人でさえ、復号化できません。

公開キー暗号作成（解読）法

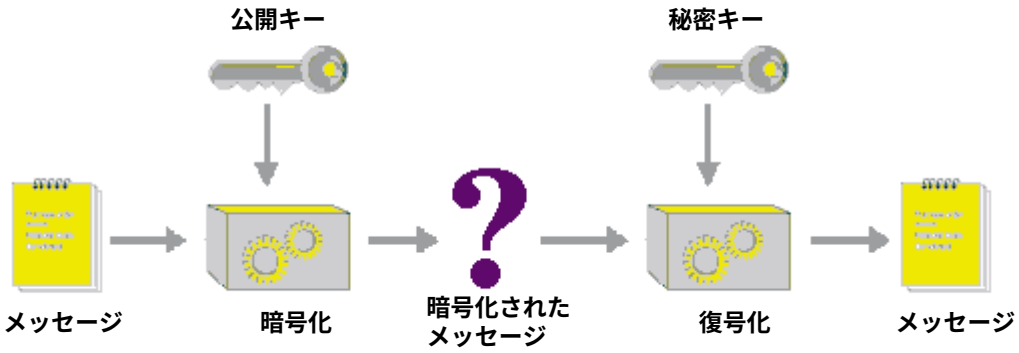

図 2： 公開キー暗号作成（解読）法

ファイルとメッセージはどのように暗号化されるか

公開キー暗号アルゴリズムは従来のシングルキー暗号化よりもかなり遅いため、暗号化は図 3 に示したプロセスを使ったほうが適切に実行されます。

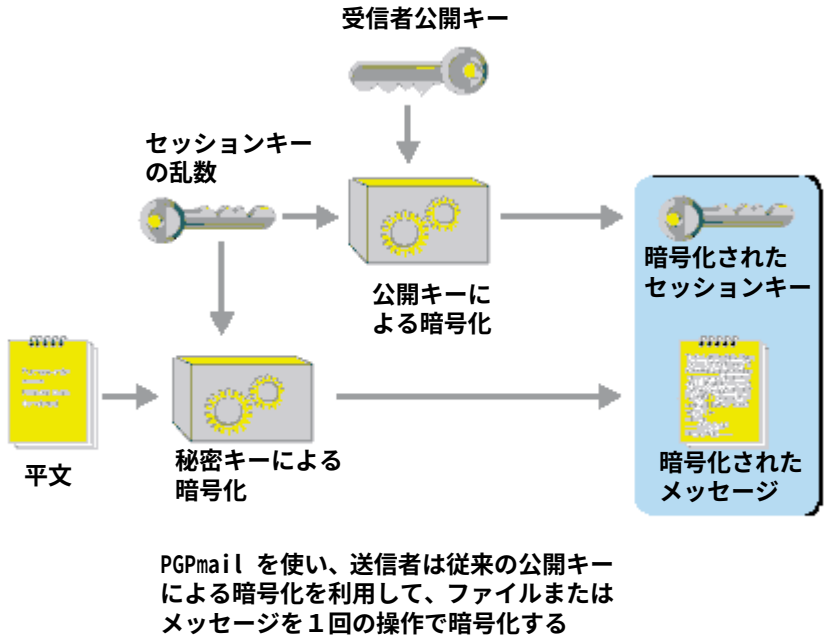

図 3： PGPmail の暗号化

ハイクオリティで高速の従来の秘密キーによる暗号アルゴリズムがメッセージの解読に使われます。このオリジナルの暗号文ではないメッセージは「平文」といわれます。ユーザには見えないプロセスで、この１つの「セッション」のためだけに作成された一時乱数が今までとおり平文ファイルを暗号にするときに使われます。その後、この一時乱数の従来のキーを暗号にするときに受信者公開キーが使われます。この公開キー暗号化の従来の「セッション」キーが暗号テキスト(「サイパーテキスト」といわれる） と一緒に受信者に送られます。

PGP 対称アルゴリズム

PGP ではさまざまな秘密キーアルゴリズムの中から１つ選び、実際のメッセージを暗号化できます。秘密キーアルゴリズムによって、暗号化と復号化の両方に同じキーを使う従来の、または対称的なブロック暗号法を意味します。PGP が提供する３つの対称ブロック暗号法とは CAST、Triple-DES および DEA です。「自家製の」アルゴリズムではありません。これらはすべて有名な暗号作成チームによって開発されました。

暗号作成では珍しいことに、３つの暗号法はどれも 64 ビットブロックの平文とサイパーテキストで働きます。CAST と IDEA のキー長は 128 ビットで、triple-DES は 168 ビットキーを使います。データ暗号化標準（DES） と同様に、これらの暗号法は暗号フィードバック（CFB） と暗号ブロックチェン（CBC） モードで利用できます。PGP は 64 ビット CFB モードで使います。CAST 暗号アルゴリズムは 128 ビットキー長のすぐれたブロック暗号法として将来有望で、高速でフリーなので、PGP に組み入れました。その名前の由来は設計者、Northern Telecom（Nortel）の Carlisle Adams と Stafford Travares の頭文字です。Nortel は CAST の特許を申請しましたが、CAST が使用料なしで誰でも利用できるようにすると書面で公言しました。CAST は非常に良くできたもので、その分野の人から好評です。設計は非常に形式にこだわるアプローチ方法をとり、たぶんキーを徹底的に検討しなければ 128 ビットキーを解けないと信じてよいと思わせる多数の正式に立証できる主張があります。CAST には弱いキーまたは部分的に弱いキーはありません。CAST は、出版された文献の非常に強力な２つの暗号解読法、線形および微分暗号解読の両方に全く動じません。両方とも DES の解読では有効でしたが。CAST は長い実績を積みあげたばかりですが、その正式な設計と設計者の良い評判は疑いなく注目を集め、他のアカデミックな暗号作成社会の暗号解読の攻撃をしかけられるでしょう。私は CAST について、PGP の初期バージョンで選んだ暗号法、IDEA について数年前に感じたのとほぼ同じように直感的に信頼できると感じています。そのとき、IDEA もやはり実績をあげたばかりでしたが、積み上げてきました。

IDEA （International Data Encryption Algorithm） ブロック暗号法は「さまざまな代数グループの演算を混合」という設計コンセプトに基づいています。これはチューリッヒの ETH で James L Massey と Xueja LAI によって開発され、1990 年に発表されました。初期に発表されたアルゴリズムについて論文では IPES（改良型暗号化標準案） と呼ばれましたが、後で名前が IDEA に変わりました。今までのところ、IDEA は FEAL、REAOC-II、LOKI、Snefru、Khafre のような他の暗号法よりかなりよく攻撃に耐えました。そして、IDEA は DES よりも、Biham と Shamir のとても上出来の微分暗号解読攻撃と、線形暗号解読からの攻撃に抵抗力があります。この暗号法は暗号解読の世界のもっとも手強い筋からの攻撃を引きつけ続けているので、IDEA の信頼性は時がたつにつれ高くなっています。残念ながら、IDEA を標準として受け入れをはばむ最大の障壁は、Ascom Systec に設計の特許権があり、DES や CAST とは違って使用料なしで誰もが利用できるわけではないことでした。

逃げ道として、PGP は利用できるブロック暗号法のレパートリーに３キーの triple-DES を含んでいます。DES は 1970 年代中頃に IBM によって開発されました。優れた設計ですが現在の標準では 56 ビットのキー長は小さすぎます。Triple-DES は非常に強力で、何年も十分に研究されたので、CAST や IDEA などの新しい暗号法よりも安全な選択かもしれません。Triple-DES は３つのキーを使って同じデータブロックを３回利用した DES で、２回めの DES 操作だけは復号化モードで逆に実行されます。triple-DES は CAST や IDEA よりもかなり遅いですが、スピードは普通 email アプリケーションではそれほど問題ではありません。triple-DES は 168 ビットのキー長を使い、攻撃者に対する有効なキー強度は最低 112 ビットで、まったく計り知れないデータ保存容量をもっています。Michael Weiner が Crypto96 で発表した論文によると、攻撃者が遠く離れて利用できるデータ保管の量では、129 ビットキーを解くのとほぼ同じ仕事が必要な攻撃を可能にします。Triple-DES はどの特許にも縛られてません。PGP 5.5 以降で作成された PGP 公開キーは、受信者のソフトウェアがどのブロック暗号法を理解するか送信者に知らせる情報が埋め込まれ、送信者のソフトウェアはどの暗号法を利用して暗号化すればよいか知っています。DSS/Diffie-Hellman 公開キーではブロック暗号法として CAST、IDEA または triple-DES を指定でき、初期設定は CAST です。現在は互換性のため、RSA キーにはこの機能はありません。PGP の旧バージョンは RSA と IDEA をサポートするだけなので、RSA キーへメッセージ送信するときには、IDEA 暗号法だけが使われます。

データ圧縮

PGP は普通、平文を暗号化する前に圧縮します。これは平文を暗号化した後で圧縮すると非常に遅いからです。暗号化されたデータは圧縮できません。データ圧縮はモデルの伝送時間とディスクスペースを節約できること、さらに重要なことは暗号作成上のセキュリティ機能を強化することです。たいいていの暗号解読技術は暗号法を見破るため、平文で見つけた冗長性を利用します。データ圧縮は平文でのこの冗長性を減らし、それによって暗号解読への抵抗力を大幅に強化します。平文の圧縮には余分の時間がかかりますが、セキュリティの点から価値があります。

圧縮するには短すぎる、またはうまく圧縮しないファイルは PGP によって圧縮されません。さらに、プログラムは PKZIP などポピュラーな圧縮プログラムによって圧縮されたファイルを認識し、すでに圧縮されたファイルは圧縮しようとはしません。技術的に面白いことに、プログラムは Jean-Loup Gailly 、Mark Adler、Richard B. Wales らが作ったフリーウエアの ZIP 圧縮ルーチンを使います。この ZIP ソフトウェアは、PKWare の PKZIP 2.x. で使われるものと機能的に同じ圧縮アルゴリズムを使います。この ZIP 圧縮ソフトウェアは、主としてかなりよい圧縮比であり高速なので、PGP で採用されました。

セッションキーとして使われる乱数について

PGP は一時セッションキーの作成に、暗号作成上、強力な擬似乱数ジェネレータを使います。このランダムシードファイルがない場合は、自動的に作成され、キーストロークとマウスの移動のタイミングから PGP プログラムによって収集されたランダムイベントから得られた真の乱数でシードされます。このジェネレータは使われるたびに、時刻や他の真の乱数ソースから部分的に得られた新しいデータを混ぜて、シードファイルを再シードします。従来の暗号化アルゴリズムを乱数ジェネレータのエンジンとして使います。シードファイルには、従来の暗号化エンジンを乱数ジェネレータに合わせるために使われるランダムシードデータとランダムキーデータの両方が格納されます。このランダムシードファイルは、攻撃者が次または前のセッションキーを引き出す危険を減らするため、公開されないように保護しなければなりません。ファイルは使用前と後に暗号法上ロンダリングされるので、攻撃者はこのランダムシードファイルを捕らえて何か役に立つものを得ようと大変苦労をします。それにもかかわらず、それが悪の手に落ちないようにすることが賢明です。できれば、ファイルはあなただけが読み取れるようにしてください。これができない場合は、他の人があなたのコンピュータから見境なくディスクをコピーさせないでください。

どのように復号化されるか

図４に示したように、復号化プロセスは暗号化のちょうど逆です。受信者の秘密キーが一時セッションキーの回復に使われ、その後そのセッションキーが高速の従来の秘密キーアルゴリズムの実行に使われ、大きなサイパーテキストメッセージを解読します。

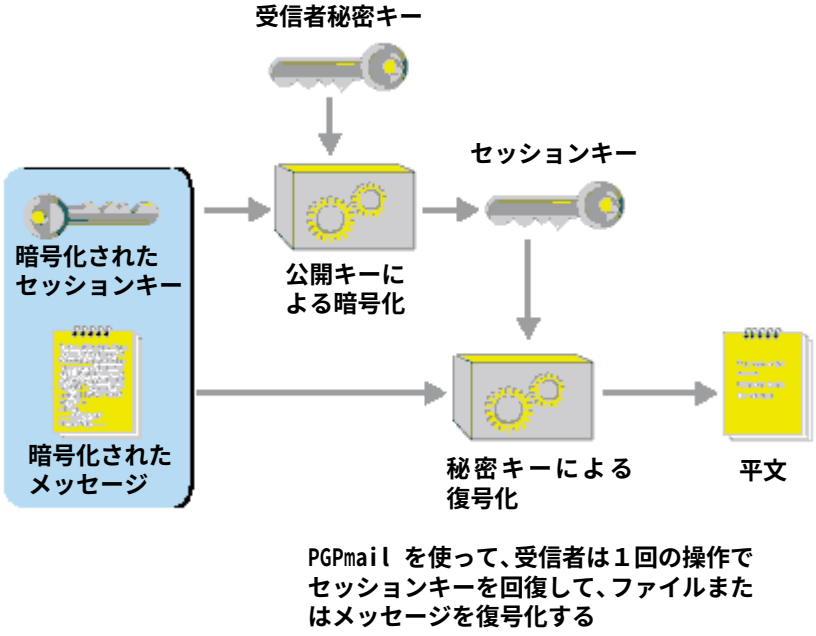

図 4： PGPmail の復号化

電子署名はどのように機能するか

PGP は電子署名を使って、メッセージの認証を行います。送信者独自の秘密キーを使ってメッセージダイジェストを暗号化でき、それによってメッセージに「署名します」。メッセージダイジェストは 160 ビットまたは 128 ビットの暗号法的に強力な単方向ハッシュ関数です。「チェックサム」または CRC エラーチェックコードに少し似たもので、メッセージを簡潔に表し、メッセージの変更を検出するのに利用されます。ところが CRC とは違い、攻撃者が同じメッセージダイジェストを作成する置換メッセージを考案するのはコンピュータ上不可能と信じられています。メッセージダイジェストは送信者の秘密キーによって暗号化され、メッセージの電子署名を作成します。図 5 は電子署名がどのように作成されるかを示しています。

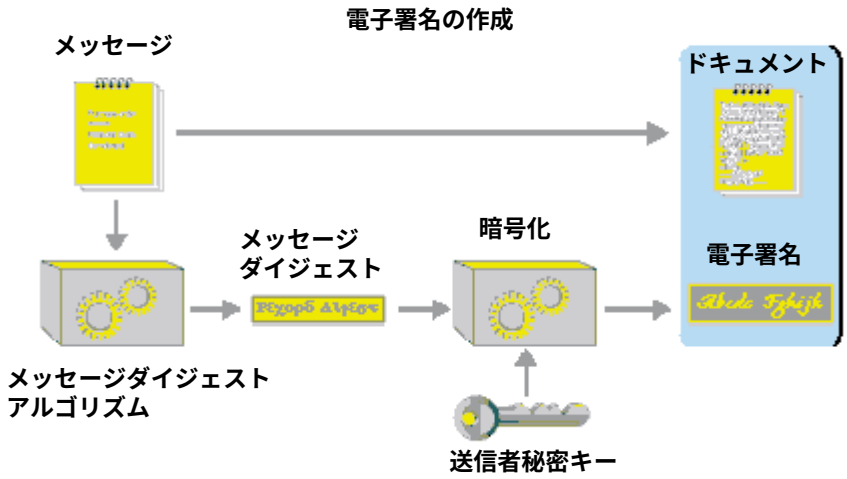

図 5： 電子署名の作成

受信者 （または誰かほかの人） は図６に示したように、送信者の秘密キーを使って電子署名を復号化し、認証できます。これで、送信者がメッセージの本当の発信者で、メッセージはその後、誰かほかの人によって変更されていないことを証明します。送信者だけがその署名を作成した秘密キーを持っているからです。署名入りメッセージの偽造は不可能で、送信者は後でその署名を否認することはできません。

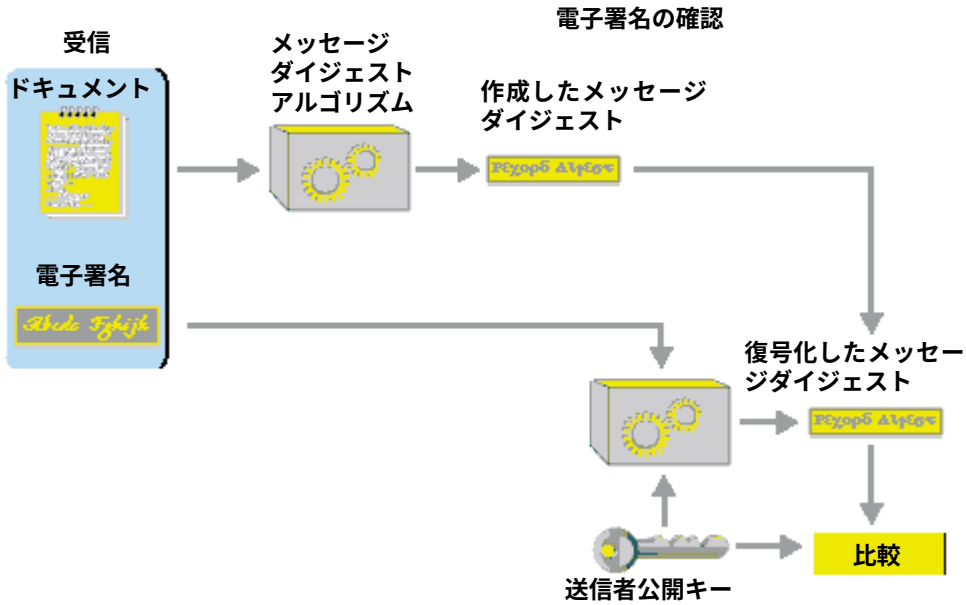

図 6： 電子署名の確認

メッセージダイジェストについて

メッセージダイジェストはメッセージまたはファイルのチェックサムのコンパクトな （160 ビットまたは 128 ビット）「抽出物」です。メッセージまたはファイルの「指紋」と考えることもできます。メッセージダイジェストは、そのメッセージが何らかの方法で変更されると、別のメッセージダイジェストがそれから計算されるように、あなたのメッセージを「表します」。これで、偽造者によるメッセージの変更を見破ることができます。メッセージダイジェストはメッセージの暗号法的に強力な単方向ハッシュ関数を使って計算されます。コンピュータ上では、攻撃者が同じメッセージダイジェストを作成する置換メッセージを考案することは不可能です。その点でメッセージダイジェストはチェックサムよりも優れています。同じチェックサムを作る別のメッセージを工夫して作るのは簡単だからです。ところがチェックサムと同様、メッセージをそのメッセージダイジェストから元のメッセージを導きだすことはできません。

PGP（バージョン 5.0 以降） で現在使われているメッセージダイジェストアルゴリズムは SHA（Secure Hash Algorithm の略）といわれるもので、米国標準技術協会（NIST）の代わりに NSA によって作成されました。

SHA は 160 ビットのハッシュアルゴリズムです。一部の人は、NSA が通信の傍受と暗号の解読を管理しているため、NSA のものに疑惑を抱いています。それでも、NSA は署名の偽造には興味がないこと、政府は、誰も署名を否認できないようにする優れた偽造できない電子署名の標準から利益を得ることは覚えておいてください。それは警察の活動と情報収集に明らかな利益があります。その上、SHA は公開された印刷物で発表されたので、ハッシュ関数を専門とする世界の優秀な暗号作成者の大半によってじっくり検討され、全員一致の意見で、SHA はとてもよく出来ていることです。一部、設計が改良され、アカデミックな暗号作成者によって以前に発表されたメッセージダイジェストアルゴリズムでみられた弱点をすべて克服しました。新バージョンの PGP は、NIST 電子署名標準に準拠する新しい DSS キーを使った署名を作成するためのメッセージダイジェストアルゴリズムとして SHA を採用しています。互換性のため、新バージョンの PGP は RSA 署名には今まで通り MD5 を使用しています。PGP の旧バージョンは RSA 署名に MD5 を使用しているからです。PGP の旧バージョンによって使われるメッセージダイジェストアルゴリズムは MD5 メッセージダイジェストアルゴリズムで、RSA Data Security, Inc. によって公衆ドメインに置かれています。MD5 は 128 ビットのハッシュアルゴリズムです。1996 年、MD5 はドイツの暗号作成者、Hans Dobbertin によってほとんど解読されました。MD5 はそのときは完全に解読されませんでしたが、署名の作成には使い続けるべきではないほどの重大な弱点があることが発見されました。この分野での活動がさらに続き、おそらく完全に解読して署名を偽造できるようになります。将来、偽造された供述書で自分の PGP 電子署名を見たくなければ、電子署名作成に選ぶ方法として、新しい PGP DSS キーへの移行をお勧めします。DSS は安全なハッシュアルゴリズムとして SHA を使うからです。

公開キーを改竄から守る方法

公開キー暗号システムでは、公開キーを公開から守る必要はありません。実際、広範に流布されたほうが都合がよいのです。しかし、公開キーを改竄から守り、公開キーが本当にその人本人ののものであるか確認することが重要です。これがおそらく公開キー暗号化システムの最も重大な脆弱性です。手順は第３章「作成と交換」の「キーの保護」を参照してください。それでは、まず起こりえる事故をみてから、次に PGP を使ってそれを安全に回避する方法について説明します。

プライベートなメッセージをアリスに送りたいとします。あなたは、アリスの公開キー証明書を電子掲示板システム（BBS）からダウンロードします。この公開キーを使ってアリスへの手紙を暗号化し、それを BBS の email 機能をつうじて送ります。

残念ながら、あなたやアリスに知られずに、チャーリーという名の別のユーザが BBS に侵入し、自分の公開キーにアリスのユーザ ID を付けて作成しました。彼は、アリスの本物の公開キーの代わりに、自分のにせのキーを置き換えます。あなたは何も知らずにアリスの公開キーではなくチャーリーのこのにせのキーを使います。このにせのキーはアリスのユーザ ID を持っているのですべて正常に見えます。チャーリーは一致する秘密キーを持っているので、アリス宛のメッセージを解読できます。アリスの本物の公開キーを使って解読したメッセージを再度暗号化して、誰も悪事を働いたことを疑わないように彼女に送ることさえできます。その上、誰もがにせの公開キーを使ってアリスの署名をチェックするので、チャーリーはこの秘密キーを使ってアリスから明らかに正しい署名を作成することすらできます。

この事故を防止する唯一の方法は、誰かが公開キーを使って改竄できないようにすることです。アリスの公開キーを本人から直接受け取ったならば、問題はありません。ところが、アリスが千マイル離れていたり、今行けないならばむずかしいことです。

おそらく、アリスの公開キーはお互いに信頼する友人、デービットから入手し、彼はアリスの公開キーの正しいコピーを持っていると思っています、デービットはアリスの公開キーに署名を入れ、アリスの公開キーの完全性を保証できます。デービットは自分の秘密キーを使ってこの署名を作成します。これで署名入りの公開キー証明書が作成され、アリスのキーが改竄されていないことを知らせます。これには、デービッドの公開キーの知られている正しいコピーを持ち、署名を確認する必要があります。おそらく、デービッドはアリスにあなたの公開キーの署名入りコピーも提供できます。デービッドはこのように、あなたとアリスの間の「紹介者」の役目をします。アリスのこの署名入り公開キー証明書はデービットまたはアリスが BBS へアップロードされ、あなたは後でダウンロードできます。その後デービットの公開キーを通じて署名を確認し、これが本当にアリスの公開キーだと安心していられます。誰も他の人はデービッドが作成した署名を偽造できないので彼のにせのキーをアリスのものと受け入れても、あなたを馬鹿にできる詐欺師はいません。

幅広く信頼される人はさらに、公開キー証明書の署名を提供することで、ユーザにお互いを「紹介する」サービスを提供することを専門にできます。この信頼される人は「認定オーソリティ」と考えることができます。認定オーソリティの署名が入った公開キー証明書はそのキーが本当に本人のものであると信頼できます。加わりたかったユーザは全員、認定オーソリティの公開キーの知られている正しいコピーを必要とします。証明オーソリティの署名が確認できます。認定オーソリティがキーサーバとして働くこともあり、その場合にはネットワーク上のユーザはキーサーバに問い合わせ、公開キーを参照できますがキーサーバがキーを認定しなければならない理由はありません。

信頼される中央認定オーソリティは特に、大きく非人間的な中央管理企業や政府機関に適しています。一部の機関環境は階層型認定オーソリティを使っています。

より多くの分散認定環境では、どのユーザも友人の信頼する紹介者になれることのほうがおそらく、中央キー認定オーソリティよりも適切に機能します。

PGP の魅力的な特長の１つは、認定オーソリティをもつ集中型環境または個人がパーソナルキーを交換するより多くの分散型環境で同じように適切に機能することです。この公開キーの改竄を守ること全体が実用的な公開キーアプリケーションでの１つのむずかしい問題です。これが公開キー暗号法の「アキレス腱」で、多数のソフトウェアの複雑さがこの１つの問題の解決で関連しています。

公開キーは、改竄されていない正しい公開キーであること、実際に関わっていると称する人のものであることが明らかになった後でのみ使用すべきです。この公開キー証明書を所有者から直に受け取ったり、すでに正しい公開キーを持っているあなたが信頼する誰か他の人の署名が入っている場合に、本人のものであると確信できます。さらに、ユーザ ID にはキーの所有者の名前だけでなく、フルネームを入れるべきです。

どのような気持ちになるかに関係なく、あなたが信頼する誰かの署名が入っていなければ、絶対にご都合主義に屈したり、掲示板からダウンロードした公開キーを信用してはいけません。その未認定の公開キーは誰かよって改竄されたかもしれません。掲示板のシステムアドミニストレータによってかもしれません。

誰か他の人の公開キー証明書に署名するよう求められたら、それが本当にその公開キー証明書のユーザ ID に名前を入れた人のものであるか確認してください。これは、公開キー証明書にあるあなたの署名によって、この公開キーは本当に彼女のものであるとあなたが約束するからです。あなたを信頼する他の人はあなたの署名があるので彼女の公開キーを受け入れます。彼女の言ったことに頼るのは軽率です。本当に彼女のものであるか独自の直接得た知識がないならば、公開キーに署名しないでください。なるべくなら、公開キーを彼女から直に受け取った場合にだけ署名すべきです。

公開キーに署名するためには、そのキーを使ってメッセージを暗号化したいだけの場合よりも、そのキーの所有権を確認していなければなりません。キーを利用してよい有効性を納得させるには、信頼する紹介者からの署名の認定で十分です。しかしキーにあなた自身が署名するためには、そのキーを所有する人について独自の直接得た知識が必要です。たぶんキーの所有者に電話をかけ、キーの指紋を読みあげて、あなたが持っているキーが本当に彼女のものであるかを確認できます。そして、あなたが実際に本人と話していることを確認できます。

公開キー証明書にあなたの署名があってもその人の誠実さを保証しているのではなく、その人の公開キーの完全性 （所有権） を保証するだけであることに注意してください。キーが本当に彼のものであるか確実ならば、ソシオパス （社会病質人格者） の公開キーに署名してあなたの信用を危険にさらすことはありません。他の人は、あなたが署名したので（あなたを信用していると仮定して） そのキーは彼のものと受け入れますが、そのキーの所有者を信頼するのではありません。キーを信頼するのとキーの所有者を信頼するのは同じではありません。

自分の公開キーは、たいていの人はあなたの公開キーの有効性を保証する紹介者の中、少なくとも１人は信用するということを期待して、さまざまな「紹介者」からの認定署名のコレクションと一緒に手元に置いておくのがよい考えです。キーは認定署名のコレクションを添付してさまざまな電子掲示板に掲示できます。誰か他の人の公開キーに署名する場合は、それをかれらの公開キーの信用証明書のコレクションに追加できるように、それをあなたの署名と一緒に彼らに戻してください。

誰もあなたの公開キーホルダーで改竄できないようにしてください。新しく署名した公開キー証明書の確認は最終的には、すでにあなたの公開キーホルダーに登録してある信頼する公開キーの完全性に頼らなければなりません。公開キーホルダーは、秘密キーの場合と同様に、リモートタイムシェアリングシステムではなく、なるべくあなた自身のコンピュータ上で物理的に管理してください。これは改竄から守ることで、公表から守ることではありません。公開キーホルダーと秘密キーの信頼できるバックアップコピーを書込み保護した媒体に保存してください。

信頼する公開キーは直接、間接的にキーホルダーに登録された他のキーすべてを認定するための最終オーソルティとして使われるので、改竄から守ることがとても重要です。バックアップコピーを書込み保護したフロッピーディスクに保存したいことがあります。

PGP は一般的に、PGP そのもののコピーのほか、システムとキーホルダーが物理的に安全に管理されていると想定しています。侵入者がディスクを改竄できると、理論的にはプログラムそのものも改竄でき、プログラムの安全機能はキーの改竄を検出しなければならないでしょう。

公開キーホルダー全体を改竄から守る１つ少し複雑な方法は、ホルダー全体にあなたの秘密キーで署名することです。これは公開キーホルダーの分離した署名証明書を作成して行います。

PGP はどのキーが有効かをどのように情報を得るか？

この項を読む前に、前の項「公開キーの改竄を守る方法」を読んでください。

PGP は、公開キーホルダーのどのキーがあなたが信頼する紹介者の署名で認定されているか情報を得ます。あなたは、どの人を紹介者として信用しているか知らせ、キーを最終的に信頼するキーで彼らのキーを認定すればよいだけです。PGP はそこからキーを取り出し、あなたが指名した紹介者の署名が入った他のキーを自動的に有効と認めます。もちろん、より多くのキーに自分で直接署名することもできます。

PGP は公開キーの有効性の判断に２つのまったく別の基準を採用しています。混同しないでください。

1. キーは属しているらしいその人本人のものですか？　つまり、信頼する署名で認定されていますか？
2. キーは他のキーの認定を信用できる人のものですか？

PGP は最初の質問の答えを判断できます。２番めの質問に答えるには、PGP にはっきり伝えなければいけません。あなたが質問２に答えると、PGP はその後あなたが信頼すると指名した紹介者の署名入りの他のキーについて質問１の答えを計算します。信頼する紹介者によって認定されたキーは PGP によって有効とみなされます。信頼する紹介者のものであるキーはそれ自体、あなたはまたは他の信頼する紹介者によって認定さけなければいけません。PGP では、紹介者としてふるまう人について何段階かの信頼レベルの可能性をも考慮しています。紹介者としてふるまうキーの所有者のあなたの信頼はその人の個人的な誠実さの評価を反映するものではありません。キー管理の理解と、キー署名で適切に判断するときに、その人がどれくらい適任であると考えているかを反映すべきです。他の人のキーの認定を信頼しない、最低限信頼する、完全に信頼する人に指名できます。この信頼性情報はキーホルダーにキーと一緒に保存されますが、PGP にキーホルダーからキーをコピーするよう指示したときは、この信頼性に関する個人的な意見は秘密とみなされるたる、信頼性情報はキーと一緒にコピーされません。

PGP が公開キーの有効性を判断しているとき、添付された認定する署名すべての信頼レベルを調べます。有効性の加重スコアを計算します。例えば、２つの最低限信頼できる署名が１つの完全に信頼する署名と同等に信用できるとみなされます。プログラムの疑い度は調整できます。例えば、あるキーを有効と判断するには２つの完全に信頼する署名または３つの最低限信頼する署名が必要となるように調整できます。

あなた自身のキーは PGP では「自明のとおり」有効で、その有効性を確認するための紹介者の署名は必要ありません。PGP は、どの公開キーがあなたのものであるか、秘密キーホルダーで対応する秘密キーを探して知ります。PGP はまた、他のキーを認定するあなた自身を完全に信用していると想定します。時がたち、信頼する紹介者として指名したい他の人からキーが蓄積します。他の人は誰も信頼する紹介者を選びます。そして、誰も次第にキーがたまり、受け取った人が少なくとも１つまたは２つの署名は信用すると期待して、他の人からの認定署名のコレクションをキーと一緒に配布します。このようにして、公開キーの分散型フォールトトレラント （誤り許容） の信頼関係が出きあがります。

このユニークな草の根方式は、集中制御と強制的な集中信頼をベースにしたインターネットプライバシー強化メール（PEM） のように、政府や他の完全に統制された機関によって開発された標準公開キー管理方法とはひどく対照的です。標準方式はあなたが信頼しなければならない人を指図する階層型認定オーソリティに頼っています。公開キーの合法性を調べるためのプログラムの分散確率的方法は、キー管理アーキテクチャのもっとも重要なものです。PGP では、あなただけが誰を信頼するか選び、あなたを公開キー証明ピラミッドの頂点に置きます。PGP は自分のパラシュートは自分で詰めたい人のためのものです。ただし、ここではこの分散型の草の根アプローチが強調されていますが、PGP がより階層型の集中公開キー管理方式では同じように適切に機能しないということではありません。例えば、大企業のユーザはきっと、全従業員のキーに署名する中心人物または人になりたがります。PGP はその集中型シナリオを PGP のより汎用信頼モデルの特殊な退化ケースとして処理します。

秘密キーを公開から守る方法

秘密キーとパスフレーズは細心の注意を払って守ってください。秘密キーが危険にさらされたら、誰かほかの人がそれを使ってあなたの名前で署名を作る前に、そのニュースを急いで関係者全員へ知らせたほうがよいです。例えば、誰かがそれを使ってにせの公開キー証明書に署名できます。これで多くの人にとって、特にあなたの署名が広く信頼されている場合に問題になります。もちろん、秘密キーが危険にさらされるとあなた宛のメッセージはすべて暴露されます。

秘密キーを守るには、まず必ず物理的に管理することから始めます。秘密キーを自宅の自分のパソコンに保存してあれば結構です。またはあなたが持ち歩くノート型パソコンに保存してください。常時物理的に管理しないオフィスのコンピュータを使わなければならないならば、公開＆秘密キーホルダーを書込み保護した取外し可能フロッピーディスクに保存し、オフィスから出るときは置き忘れないでください。秘密キーがリモートダイヤルイン UNIX システムなどのリモートタイムシェアリングコンピュータに常駐できるようにするのはよい考えではりあません。誰かがあなたのモデム回線で盗み聞きして、パスフレーズをとらえ、あなたの実際の秘密キーをリモートシステムから入手できます。秘密キーは、あなたが物理的に管理できるマシン上で使用するだけにしなければいけません。詳しくは第 5 章「PGP for Secure File Storage の使い方」を参照してください。

パスフレーズはあなたの秘密キーファイルがあるコンピュータに保存してはいけません。秘密キーとパスフレーズの両方を同じコンピュータに保存するのは、銀行のキャッシュカードと暗証番号を同じお財布に入れておくのと同じように危険です。パスフレーズと秘密キーファイルの両方が入っているディスクを誰かに触れさせたくありません。パスフレーズを記憶して脳以外のどこにも保存しないのが安全です。パスフレーズを書き留めなければと思うなら、適切に保護してください。秘密キーファイルよりもしっかり保護してください。

そして、秘密キーのバックアップコピーを保管してください。なお、あなたが秘密キーを１つだけ持っていること、これをなくすと世界中にばらまいた公開キーのコピーがすべて役立たずになることを覚えおいてください。公開キーの管理をサポートする分散型の非機関アプローチ方法の PGP に長所はありますが、あいにくキーが危険にさらされたキーの１つの中央管理リストに頼れないことでもあります。これは秘密キー漏洩の損害の封じこめが少しむずかしくします。お知らせを広め、誰もがそれを聞いていると期待するしかありません。

最悪のケースがおきたら、つまり秘密キーとパスフレーズの両方が漏洩した場合 （願わくば何とかこれを発見する） 、「キー漏洩」証明書を発行しなければなりません。このような証明書は、他の人にあなたの公開キーの使用を停止するよう警告するときに使われます。PGP を使って、〔PGP キー〕メニューから〔廃止〕コマンドを使って証明書を作成できます。その後、この漏洩証明書を地球の全員へ、または最低でもあなたの友人とその友人などへなんとかして送らなければなりません。彼らの PGP ソフトウェアはこのキー漏洩証明書を公開キーホルダーにインストールし、自動的に二度と間違ってあなたの公開キーを使えないようにします。その後、新しい秘密＆公開キーペアを作成して、新しい公開キーを公表できます。新しい公開キーと古いキーのキー漏洩証明書の両方を入れた１つのパッケージを送信できます。

秘密キーをなくしたらどうなるでしょうか？

普通、自分の秘密キーを廃止したいときは、〔PGP キー〕メニューの〔廃止〕コマンドを使って、秘密キーで署名した廃止証明書を発行できます。

しかし、その秘密キーを忘れたら、秘密キーが破壊されたらどうしますか？　自分では廃止できません。廃止には秘密キーを使わなければならないからです。誰も持っていないからです。あなたのキーを署名した人１人１人に証明書を廃棄するよう頼みます。その後、あなたの紹介者の１人を信頼してあなたのキーを使おうとした人はあなたの公開キーが信頼できないことを知ります。

スネークオイルに注意

暗号ソフトウェアパッケージを調べたとき、必ずこの製品をなぜ信用すべきかという疑問が残ります。あなたが自分でソースコードを調べるとしても、誰も暗号上のセキュリテイを判断した経験はありません。経験豊かな暗号作成者であっても、アルゴリズムの微妙な弱点は理解できないでしょう。70 年代初めに大学にいたことろ、これはすばらしい暗号方式だと信じたものを考案しました。単純な擬似乱数ストリームを平文ストリームに追加して、サイパーテキストを作成しました。これは一見したところ、サイパーテキストの頻度分析の裏をかき、もっとも資力に富んだ政府の情報局でも解読できません。私は自分の作品の出来に自己満足しました。数年後、これと同じ方式が数冊の入門暗号入門書と手引書にあるのを発見しました。なんということでしょう。他の暗号作成者は同じ方式を考えました。不運なことに、基本的な暗号解読技術を使って、暗号を平凡に解読するという簡単な宿題としてこの方式が提示されました。私のすばらしい方式とはそんなものでした。

この失意の経験から、暗号化アルゴリズムを発明するときはあまりにたやすくセキュリティについて間違った考えに陥ってしまうことを学びました。たいていの人は、資力のある敵から長期間そして徹底的な攻撃に耐えられる暗号化アルゴリズムを作るのがどれほど大変なことか分かっていません。多くの主流のソフトウェアエンジニアは同じように未熟な暗号方式を開発し （よく似た暗号方式のことが多い） 、一部は市販の暗号ソフトウェアパッケージに組み込まれ、妥当な金額で数千の疑わないユーザへ販売されました。

これは、見た目と感じはよくても、低速の衝突テストでスナップが開く自動車のシートベルトを売るようなものです。そんなものに頼るのはシートベルトをしないより悪いでしょう。現実に衝突するまでひどいものとは誰も疑っていません。弱点のある暗号ソフトウェアに頼ることは微妙な情報を知らずに危険にさらすことで、暗号ソフトウェアを何も持っていなければそんな目には合わないのです。おそらく、データが危険にさらされていたと気づくこともないでしょうが。

ときどき市販パッケージは、政府が一般の使用を推奨するかなりよくできた従来のアルゴリズム （不思議なことには機密扱いの情報向きではない） 連邦データ暗号化標準（DES）を使います。DES が使用できる「操作モード」はいくつかあり、一部のモードは他のものよりすぐれています。政府は特に、一番弱い単純なモード、電子コードブック（ECB） モードをメッセージにはを使用しないように推奨し、より強力で複雑な暗号フィードバック（CFB） と暗号ブロックチェン（CBC） モードを推奨しています。

残念ながら、私が調べた市販の暗号化パッケージの大半は ECB モードを使用しています。これら数多くのソフトウェアの著者と話したところ、CBC や CFB モードは聞いたことがないし、ECB モードの脆さも知らないそうです。これらの基本概念を理解するために暗号作成・解読法を十分に学んだことがないという事実がまさに安心できないことです。そして、不適切で安全ではない方法で DES キーを管理することがあります。また、これらの同じソフトウェアパッケージはよく、遅い DES の代わりに利用できるもう１つの早い暗号化アルゴリズムを含んでいます。パッケージの著者はしばしば、所有権のあるより高速なアルゴリズムは DES と同様に安全だと考えていますが、彼に質問した後は普通、大学時代の私のすばらしい方式のバリエーションの１つでしかないと知ります。または、たぶん所有権のある暗号方式がどのように機能するかはっきりは言わないけれど、すばらしい方式であり信頼すべきものだということを確信させました。彼はそのアルゴリズムはすばらしいと思っていますが、それを見ないでどうして分かることができますか？ 公平な立場からいうと、たいたいこれらの恐ろしく弱い製品は暗号技術を専門とする会社のものではないことに注目する必要があります。

正しい操作モードで DES を使う本当にすぐれたソフトウェアパッケージでも、まだ問題があります。標準 DES は 56 ビットキーを使います。これは今日の標準では小さすぎ、特殊な高速マシンで徹底的にキーを検索すれば簡単に解けます。DES はそろそろ寿命の終わりにきましたが、それに頼っているソフトウェアパッケージがあります。

AccessData (87 East 600 South, Orem, Utah 84058) という会社が、WordPerfect 、Lotus 1-2-3 、MS Excel、Symphony、Quattro Pro 、Paradox 、MS Word 、PKZIP で使える組込み暗号方式を解くパッケージを 185 ドルで販売しています。簡単にパスワードを想像しません。本格的な暗号解読を行います。ファイルのパスワードを忘れたときに買う人もいます。警察も買い、押収したファイルを読み取りできます。著者の Eric Thompson と話したところ、彼のプログラムはほんの一瞬で解読してしまうけれど、遅いループを入れて遅くしてあるので顧客はそんな簡単なこととは思っていないと言いました。

傍受される危険がない電話分野では、あなたの選択は希望がないように見えます。主要製品はモトローラと AT&T が 2,000 ドルから 3,000 ドルで製造し、政府が機密アプリケーションで使用する STU-III（安全電話ユニット） です。強力な暗号法を持っていますが、この強力バージョンの購入には政府からある種の特殊ライセンスが必要です。NSA の便宜上に弱められた STU-III の普及版が販売され、輸出版はさらにひどく弱体化されています。その後、暗号化に政府の有名なクリッパーチップを使用している 1,200 ドルの AT&T Surity 3600 があります。キーは盗聴者に都合よく政府に預託されます。その後、もちろん、スパイになりたい人向けのカタログから購入できるアナログ （非デジタル） 音声スクランブル装置があります。暗号法に関する限り、実際には役に立たない玩具ですが、「安全な」通信製品として、よく知らない顧客に販売されています。ある点、暗号法は医薬品のようなものです。その完全性は絶対に重大です。悪質なペニシリンは良質のペニシリンと同じに見えます。スプレッドシートソフトウェアが間違っていたら教えますが、暗号パッケージに弱点があるときどうやって教えますか？　弱点のある暗号化アルゴリズムによって作成されたサイパーテキストは強力な暗号化アルゴリズムによって作成されたサイパーテキストと同じように見えます。そこには多数のスネークオイルが待ち構えています。多数のもぐり医者が治します。昔の特許のある医薬品の行商人とは違い、これらのソフトウェア製作者は普通、スタッフがスネークオイルとは知りません。優秀なソフトウェアエンジニアかもしれませんが、普通は暗号法の学術論文は読んだことはありません。しかし、よい暗号ソフトウェアを書けると思っています。どうしてですか？　何と言っても、そうするのが直観的に簡単に思えるからです。そのソフトウェアはうまく機能するようにみえます。

解読できない暗号方式を考案したと考える人は信じられないほど稀な天才か、信じやすく未熟かのどちらかです。あいにく、時には自分で設計した暗号化アルゴリズムを追加して PGP を「改良」したいという自称暗号作成者の相手をしなければなりません。

NSA で地位の高い上級暗号作成者、Brian Snow との会話を思い出します。彼は、まず長い時間コードの解読に費やして「お金を得た」ことがない人が設計した暗号化アルゴリズムは絶対に信用しないと言いました。それはいろいろな意味がありました。実際に、民間の暗号作成の世界の誰もこの規準の下で資格のある人はいないと意見を述べました。「その通り」と自信のある笑顔で言い、「NSA での仕事はますます楽になる」と言いました。クールな考えでした。私も資格はありませんでした。

政府はスネークオイルも広めようとしました。第２次世界大戦後、米国はドイツの Enigma 暗号記述マシンを第三世界の政府へ売りました。しかし、彼らには、Allies が戦時中に Enigma コードを解読したことを知らせませんでした。長年機密のままでした。今日でも、世界中の多数の UNX システムはファイル暗号化用の Enigma 暗号を使っています。政府がもっとよいアルゴリズムの使用を阻止する法的な障壁をもうけたせいでもあります。1997 年に RSA アルゴリズムの初版を阻止しようともしました。そして、何年も一般向けの効果的な安全な電話の開発の民間の努力をすべて基本的に押さえこみました。

米国政府の国家安全保障局の基本的な仕事は情報収集です。主に人々のプライベートな通信をこっそり盗聴する方法で（James Bamford の『Puzzle Palace 』を参照） 。NSA はコード解読の相当な技術と資源を蓄積しました。人が自衛のためにすぐれた暗号法を手にできないときは、それは NSA の仕事をさらに簡単にします。NSA はまた暗号化アルゴリズムの承認、推奨も行っています。一部の批評家はこれは鶏小屋を狐に守らせるようなもので、利害の衝突であると非難しています。1980 年代、NSA は彼らが設計した （COMSEC 保証プログラム） 従来の暗号化アルゴリズムを押し進め、それが機密のためどのように機能するかは誰にも言っていません。彼らは他の人がそれを信用し使うことを望みました。しかし、暗号作成者は、よく出きた暗号化アルゴリズムは機密扱いで安全でなければならないと言います。キーだけの保護を必要とすべきです。NSA の機密扱いのアルゴリズムが安全ならばどうして誰かほかの人が知るのか？　誰もアルゴリズムを検討できないなら、NSA が彼らだけが解読できる暗号化アルゴリズムを設計することはそれほど大変ではありません。さらに、現在のクリッパークリップを使って、NSA は設計したもう１つの機密暗号、SKIPJACK を押し進めています。故意にスネークオイルを売るのでしょうか？

次のものは、米国で市販されている暗号ソフトウェアの品質をひそかに傷つけた３つの主要要素です。

- まず第１に、市販の暗号ソフトウェア製作者の競争が事実上、全世界で欠けていることです （これは PGP の公表以来、変化し始めていますが） 。どのソフトウェアエンジニアも暗号作成者気どりです。これで実際に悪質な暗号ソフトウェアが急増しました。
- 第２に、すぐれた市販用の暗号技術を NSA は故意にしかも組織的に法的な威嚇と経済的圧力を加えて押さえつけています。この圧力によって暗号ソフトウェアに厳しい輸出規制が課せられ、ソフトウェア市場の経済によって、国内の暗号ソフトウェアを抑制する最終的な効果があります。
- ３番めの抑制する管理方法は、公開キー暗号化アルゴリズムのすべてのソフトウェア特許を１つの会社に与え、この技術の普及を抑制するための１つの難所を設けることです （この暗号特許カルテルは 1995 年秋に散会しました） 。

これらすべての最終的な効果は、PGP が発表される以前の、米国で利用できる非常に安全な汎用暗号ソフトウェアがほとんどなかった頃のものです。

私は PGP のセキュリティについて、大学のすばらしい暗号ソフトウェアについてかつて思ったほど確信していません。確信しているならば、それは悪い兆候です。ところが私は、PGP に目立つ弱点はないと思っています （バグはあるのは確かですが） 。民間の暗号研究機関の文献から最適なアルゴリズムを選びました。たいてい、これらのアルゴリズムは１つ１つ広範に詳しく検討されました。世界の一流暗号作成者を大勢知っており、何人かと PGP で使われる暗号化アルゴリズムとプロトコルについて話し合いました。十分に研究し、完成に数年かかりました。そして、私は NSA のために働いていません。けれど、ソースコードを利用して楽に詳しく検討できるので、PGP の暗号文の完全性について私の言葉を信用する必要はありません。

私が PGP の暗号文の品質にこだわるもう１つのポイント

初めて PGP を開発し、1991 年にフリーソフトとして発表してから、私は PGP の海外での普及に対して３年間、税関の刑事捜査を受け、刑事訴追と数年の禁固刑の恐れがありました。ついでながら、政府が他の暗号ソフトウェアについて動揺しているとは知りませんでした。PGP がきっかけだったのです。だからといって PGP の強さに関係ありますか？　私はその製品の暗号法の完全性で名声を得ました。私は自分の自由を危険にさらしたので、プライバシーを守る権利へのこだわりを捨てません。私の名前がついた製品に内密の手段をもたせることを許すつもりはありません。

脆弱性

入りこめないデータセキュリティシステムはありません。PGP はさまざまな方法で出し抜かれます。どのデータセキュリティシステムでも、守ろうとする情報は攻撃者にとって攻撃のコストより価値があるか自問すべきです。こうして、費用のかかる攻撃については心配せずに、一番費用のかからない攻撃から自分を守ることにします。

次の議論の一部はひどく偏執症に思えるかもしれませんが、そのような態度が脆弱性問題の理にかなった議論に適切です。

「世界中のパソコンがすべて、つまり２億 6000 万台のパソコンが１つの PGP 暗号化メッセージ上で動作するようになったなら、１つのメッセージを解くのに、それでも平均して宇宙時代のおよそ 1200 万倍かかるだろう」と 1977 年 3 月 20 日に国家安全保障局の副長官、William Crowell が発言しました。

危険にさらされたパスフレーズと秘密キー

たぶん、一番単純な攻撃は、秘密キーのパスフレーズをどこかに書き残した場合におきます。誰かがそれを手に入れ、秘密キーファイルも入手したら、あなたのメッセージを読み取れ、あなたの名前で署名できます。

以下は、パスフレーズを保護するための推奨です。

1. 子供や配偶者の名前のようにすぐに想像できる、見えすいたパスフレーズを使用してはいけない。
2. パスフレーズにはスペースのほか、数字と文字を組み合わせること。パスフレーズを１つの単語で作ると、コンピュータはパスフレーズが見つかるまで辞書にある単語をすべて調べて簡単に見破れます。だから、パスフレーズはパスワードよりも優れているのです。頭のよい攻撃者は名言集をコンピュータで調べ、パスフレーズをし探します。
3. 独創的であること。覚えるのは簡単で、想像するのはむずかしいパスフレーズを使用すること。ばかげた格言やあいまいな文献の引用文を独創的に使って簡単に作れます。

公開キーの改竄

大きな脆弱性は、公開キーが改竄された場合に持ち上がります。これは決定的に公開キー暗号法のもっとも重大な脆弱性でしょう。たいていの初心者がすぐにそれを認識しないのも一因です。この脆弱性の重要性と、適切なウイルス感染防止対策については、この章の「公開キーを改竄から守る方法」で詳しく説明します。

要約

誰かの公開キーを使うときは、それが改竄されていないことを確認してください。他の人の新しい公開キーは、その所有者から直に受け取った、または信頼する人が署名している以外は信頼してはいけません。誰も公開キーホルダーを改竄できないようにしてください。公開キーホルダーと秘密キーは両方とも、リモートタイムシェアリングシステムではなく、なるべくあなた自身のコンピュータで物理的に管理してください。両方のキーホルダーのバックアップコピーを保存してください。

完全には削除されていないファイル

もう１つ考えられるセキュリティ問題は、多くのオペレーティングシステムがファイルをどのように削除するかによって生じます。ファイルを暗号化し、オリジナルの平文ファイルを削除したとき、オペレーティングシステムは実際はデータを物理的に消去していません。それらのディスクブロックに削除マークを付けるだけで、後でそのスペースを再利用できるようにします。これは、機密扱いの書類をシュレッダーではなく資源ゴミとして捨てるようなものです。ディスクブロックには消去したかったオリジナルの機密データが残っていて、おそらくいつか新しいデータで上書きされます。攻撃者がこの削除されたディスクブロックの割り当てが解除された直後に読めば、その平文を回復できます。

実際、これは、ディスクで何か故障が起こり一部ファイルが偶然に削除または破壊された場合にたまたま起きることもあります。ディスク回復プログラムを実行して破損ファイルを回復できますが、これは、一部の以前に削除したファイルが他のものと一緒に復活されることもよくあります。永久に消えたと思った機密ファイルが後で出てきて、破損ディスクを回復しようとする人が調べられます。ワープロやテキストエディタを使ってオリジナルのメッセージを作成しているときでさえ、エディタは内部処理だけのため、ディスクにテキストの複数の一時コピーを作っています。これのテキストの一時コピーは削除されたときにワープロによって消去されますが、これらデリケートな断片はまだディスクのどこかに残っています。

平文の再び出てくるのを防止する方法はただ１つ、削除された平文ファイルにともかく上書きすることです。削除されたディスクブロックがすぐに再利用されることが確かでなければ、積極的な処置を講じて、平文ファイルに、さらにワープロによって残されたディスク上のファイルの断片に上書きしなければなりません。ディスク上の平文ファイルの断片は、ディスク上の未使用ブロックをすべて上書きできるディスクユーティリティを使って処理できます。例えば、MS-DOS 用の Norton Utilites などで上書きできます。

ウイルスとトロイの木馬

もう１つの攻撃は、PGP またはオペレーティングシステムを感染させる、特注の敵意のあるコンピュータウイルスまたはワームに関係します。この仮説ウイルスはパスフレーズや秘密キーまたは解読されたメッセージを検索したり、ひそかに検索した情報をファイルへ書き込んだり、それをネットワークを通じてウイルスの所有者に送るように設計されています。または、PGP の動作を書き換えて署名を正しく確認できないようにします。この攻撃は暗号解読の攻撃より費用がかかりません。

このような攻撃の防衛は、ウイルス感染防止のカテゴリに分類されます。適度な機能をもつウイルス感染防止製品が市販され、感染防止手順に従ってウイルス感染の可能性を大場に減らすことができます。ウイルス感染防止およびワーム感染防止対策の詳しい取扱いはこの説明書の対象範囲ではありません。PGP にはウイルスに対する防衛機能はなく、パーソナルコンピュータが信用できる実行環境であると想定しています。そのようなウイルスやワームが実際に出た場合は、うまくゆけばに知らせが広まり、全員に警告します。同じような攻撃に、ほとんど PGP と同じように動作するけれど、要求されているようには機能しない PGP のより賢い贋物を作り、にせのキー証明書を受け入れできるようにする人がいます。PGP は Pretty Good Privacy から入手するようにしてください。

PGP の改竄を確認する方法は他にもあります。電子署名を使う方法です。別の信頼するバージョンの PGP を使い、疑わしいバージョンの PGP の署名を確認できます。ただし、この方法は、オペレーティングシステムが感染している場合には全く役に立たず、pgp.exe のオリジナルコピーが署名を確認できる機能を不能にするように意地悪く変更されてしまった場合にも検出しません。このテストも、PGP 実行可能プログラムの署名の確認に使う信頼する公開キーのコピーを持っていると想定しています。

スワップファイルまたは仮想メモリ

PGP は元々、今日の標準による単純なオペレーティングシステム、MS-DOS 用に開発されました。しかし、Macintosh Windows や Macintosh OS のように複雑な他のオペレーティングシステムに移植されたので、新しい脆弱性が出現しました。この脆弱性は、これら優れたオペレーティングシステムが仮想メモリという技術を使うことから生じます。仮想メモリでは、コンピュータの半導体メモリチップで利用できる記憶スペースより大きい巨大なプログラムをコンピュータで実行できます。これは、グラフィカルユーザインターフェイスが標準になり、ユーザが同時にいくつもの大きなアプリケーションを実行し始め、ソフトウェアがますます膨らんだため、便利です。オペレーティングシステムはその時使っていないソフトウェアの部分をハードディスクに保存します。つまり、オペレーティングシステムはあなたに知らせずに、あなたはメインメモリだけに記憶されていると思っていたもの、キー、パスフレーズおよび解読された平文などをディスクに書き出します。PGP は必要以上に長くメモリにこのように大事なデータを入れておきませんが、オペレーティングシステムがそれを無造作にディスクに書き出す可能性は少しはあります。

データはスワップファイルというディスクのスクラッチパッド領域に書き出されます。データは必要に応じてスワップファイルから読み出されるので、物理メモリにはいつでもプログラムまたはデータの一部だけしかありません。これらの動作はユーザには見えません。ディスクのカチカチという音をたてているのを見ているだけです。Microsoft Windows は最長時間未使用（LRU） ページ交換アルゴリズムを使って、ページといわれるかなりの量のメモリをスワップします。つまり、長時間アクセスしなかったページが一番先にディスクへスワップされます。このアプローチ方法ではたいてい、大切なデータがディスクへスワップされる危険がかなり低くなります。PGP がそのデータを長くメモリに置いておかないからです。ところが、何も保証はしません。

このスワップファイルはあなたのコンピュータを物理的にアクセスできる人ならば誰でもアクセスできます。この問題が気掛かりならば、スワップファイルを上書きする特殊ソフトウェアを入手して解決できます。もう１つ可能な解決法は、オペレーティングシステムの仮想メモリ機能をオフにすることです。Microsoft Windows ではこれが可能で、Mac OS でもできます。仮想メモリをオフにするということは、RAM にすべてを記憶させるためより多くの物理的な RAM チップをインストールする必要があります。

物理的なセキュリティ違反

物理的なセキュリティ違反をすると、誰かがあなたの平文ファイルまたは印刷したメッセージを物理的に取得できます。断固とした敵は不法侵入、ゴミ箱の回収、不当な捜索や押収、または賄賂の授受、恐喝またはスタッフの潜入を通じて行います。これらの攻撃の一部は、主としてボランティアスタッフに頼る草の根市民団体で特にありそうなことです。暗号ツールを持っているから安全だとだまされないでください。暗号技術はデータが暗号化されている間だけ守ります。直接の物理的なセキュリティ違反はやはり平文データや書類、会話を危険にさらします。

このような攻撃は PGP での暗号分析攻撃よりも費用がかかりません。

大攻撃

設備の整った敵によって行われる別の攻撃にコンピュータからの電磁信号のリモート検出があります。このように費用がかかり、少し人手のかかる攻撃はそれでもたぶん、直接暗号解読による攻撃より費用がかかりません。適切な機器を積み込んだバンがあなたのオフィス近くの公園に停車し、遠く離れてあなたのキーストロークやコンピュータのビデオ画面に表示されたメッセージをすべて傍受できます。あなたのパスワード、メッセージなどすべてが危険にさらされます。この攻撃は、あなたのコンピュータ機器とネットワーク配線すべてを適切にシールドして信号を放出しないようにして防御できます。この「テンペスト」といわれるシールディング技術は一部政府機関や防衛契約者が利用しています。テンペストシールデイングを市販しているハードウェア会社があります。

にせのタイムスタンプに対する保護

PGP の少し分かりにくい脆弱性は、不誠実なユーザが公開キー証明書と署名ににせのタイムスタンプを作成することです。ときどき利用して、分かりにくい公開キープロトコルに深くかかわっていなければ、この項は飛ばしてください。

不正直なユーザがシステムクロックの日付と時刻の設定を変更し、別の時刻に作成されたように見える公開キー証明書と署名を作成するのをやめさせるものは何もありません。実際よりも前または後で署名したように見せたり、秘密＆公開キーペアが早めにまたは後で作成されたように見せることができます。これは、署名を否認できるある種の抜け道を作ることなどで、多少の法的または経済的な利点があります。

このような電子署名での偽造タイムスタンプ問題は、今まで手書きの署名であった問題より悪いとは思いません。誰かが契約書の手書きの署名の隣に日付を書いても、誰もこの事態について用心していないようです。手書きの署名にある「間違った」日付が実際の不正に関係ないこともあります。タイムスタンプは、署名者がドキュメントに署名したことを断言するしたとき、あるいは署名を有効にしたいときです。

署名に実際の正しい日付が記入されていなければならない重大な場合には、人は公証人を使い、手書きの署名に日付を入れます。電子署名でこれと同じようにするには、信頼する第三者に署名証明書に署名してもらい、信頼するタイムスタンプを押すことです。このために風変わりなプロトコルや、あまりにも形式ばったプロトコルは必要ではありません。連署された署名が、ドキュメントに署名されたときの合法的な判断方法として長い間認知されてきました。

信用できる証明オーソリティや公証人は、信頼できるタイムスタンプが記入された公証署名を作成できます。これは必ずしも、中央オーソリティが必要ではありません。おそらく、信頼する紹介者や利害関係のない人が、本物の公証人が現在しているのと同じようにこの役目を果たせます。公証人が他人の署名にサインした場合、それは署名証明書の署名証明書になります。これは現実の公証人が現在、手書きの署名に証人として署名するのと同じように、署名の証拠として働きます。公証人は切り離した署名証明書 （署名された実際の書類なしで） を公証人が管理する特殊日誌に記録できます。誰でもこの日誌を読めます。公証人の署名には、おそらくオリジナルの署名にあるタイムスタンプよりも信頼できるまたはより法的な意義をもつ、信頼するタイムスタンプが記入されています。

IEEE コンピュータの Dennings の 1983 年の記事にこのテーマの適切な対処法があります。将来の PGP 強化版には、信頼するタイムスタンプ付きの公証署名を簡単に管理する機能が加えられます。

マルチユーザシステム上での公開

PGP は元々、あなたが直に物理的に管理するシングルユーザ PC 用に設計されました。誰かがあなたの家に押し入り、PC を盗み、パスワードを教えるように脅されなければ（またはあなたのパスフレーズが簡単に想像できるものでなければ）、家の PC で PGP を実行していれば、あなたの暗号化ファイルは普通は安全です。

PGP はデータが危険にさらされたシステム上で平文の状態では、データを保護するようには設計されていません。また、侵入者が複雑な手段を使って、あなたの秘密キーを読み取ることも防止できません。マルチユーザシステムではこれらの危険を認識し、それに応じて期待と行動を調整する必要があります。おそらく、あなたの立場は、あなたが直接物理的に管理する孤立したシングルユーザシステムで PGP を実行するだけを考えるべきのようなものです。

トラヒック分析

攻撃者があなたの暗号化されたメッセージを読めなくとも、メッセージがどこから来たか、どこへ送られるか、メッセージのサイズ、メッセージが送られた時刻を見て、少なくとも少しは役に立つ情報を推量できます。これは攻撃者があなたの長距離電話の請求書を見て、通話そのものの内容は攻撃者に分からなくとも、誰にいつどの位の時間電話したのかを調べるのと同じことです。これはトラフィック分析といわれます。PGP だけではトラフィック分析から守れません。この問題を解決するには、おそらく何かの暗号作成補助を利用して、あなたの通信環境でトラフィック分析へのデータ公開を減らすように設計された特殊な通信プロトコルが必要です。

暗号解読

費用がかかり、手ごわい暗号分析の攻撃は、政府情報局のように非常に大型のスーパーコンピュータ資源をもつ人がしかけてくることがあるでしょう。暗号文を構成部分に分ける新しい機密の発明を利用してあなたの RSA キーを解読できるでしょう。しかし、一般の研究機関は 1978 年以来、広範囲に攻撃してきましたが成功していません。おそらく政府は PGP で使われる IDEA の従来の暗号化アルゴリズムを解く機密扱いの方法をいくつか持っています。これはどの暗号作成者にとってもひどい悪夢のような状態です。実際の暗号使用で絶対に安全だという保証はありえません。それでも、一部の楽観的な人はもっともだと考えています。IDEA アルゴリズムの設計者はヨーロッパで特に優秀な暗号作成者です。詳しいセキュリティ分析が行われ、機密扱いでない世界の一部の優秀な暗号解読者から同等だという評判を得ました。さまざまな暗号解読を寄せつけない点で、DES よりも優れた設計の利点をもっているようです。

その上、このアルゴリズムに微妙で未知の弱点があっても、PGP は暗号化の前に平文を圧縮します。これでその弱点がかなりカバーできます。解くためのコンピュータの作業負荷は、メッセージの価値よりもかなり高価なものになりそうです。このような能力をもつ手強い攻撃について懸念する立場ならば、たぶん特殊なニーズに合わせた特注のデータセキュリティ方法をデータセキュリティコンサルタントに相談すべきです。

要約すると、データ通信は適切な暗号法による保護がなければ、相手があなたのメッセージを傍受するのにほとんど努力が要らず、お決まりの手順かもしれません。特に、モデムや email システムを通じて送られたメッセージです。PGP を使い、適切な注意事項を守れば、攻撃者はあなたのプライバシー侵害により多くの労力とお金を費やさなければならなくなります。

あなたがもっともシンプルな攻撃から身を守り、決然とし高度な資源をもつ攻撃者によってプライバシーが侵害されないと確信しているならば、おそらく PGP を使うことで安心でしょう。PGP はあなたにかなり満足できるプライバシーを提供します。

推奨する入門書

Bacard, Andre 『Computer Privacy Handbook 』(Peachpit Press, 1995)
Garfinkel, Simson 『Pretty Good Privacy 』(O ュReilly & Associates, 1995)
Schneier, Bruce『Applied Cryptography:Protocols, Algorithms,and Source Code in C 』(John Wiley & Sons, 1996)
Schneier, Bruce 『e-mail Security 』(John Wiley & Sons, 1995)
Stalling, William 『Protect Your Privacy』(Prentice Hall, 1994)

関連資料

Lai, Xuejia 『On the Desian and Security of Block Ciphers Institute for Signal and Information Processing 』(ETH-Zentrum, Zurich, Switzerland, 1992)
Lai Xuejia, Massey James L., Murphy, SEAN Markov『Cipher and Differential Crypta
nalysis Advances in Cryptology - EUROCRYPT'91 』
Rives,t Ronald『The MD5 Message Digest Algorithm MIT Laboratory for Computer Science』1991

Wallich, Paul 『Electronic Envelopes Scientific American』Feb. 1993 、P-30.
Zimmermann, Philip『A Proposed Standard Format for RSA Cryptosystems in Advances in Computer Security』Vol.III、Rein Turm 編集 (Artech House, 1988)

索引

あ

い

え

お

か

き

へ

ほ

む

め

ゆ

ら