**Gpg4winの概要**

GnuPG for Windowsを使用した安全な電子メールとファイルの暗号化

によるバージョンに基づく

ユートバーン、カールビルマイヤー、マンフレッドJ.ハインツェ、イザベルクレイマー、フランシスレイ博士。

によって大幅に改訂

ヴェルナーコッホ、フロリアン対サムソン、エマニュエルシュッツェ、ヤンオリバーワグナー博士。

元のドイツ語から翻訳

ブリジットハミルトン

Gpg4win Initiativeの発行

2016年11月30日のバージョン3.0.0

**出版社の詳細**

Copyright c 2002 BundesministeriumfürWirtschaft und Technologie 1Copyright c 2005 g10 Code GmbH Copyright c 2009、2010 Intevation GmbH

GNU Free Documentation License、バージョン1.2、またはFree Software Foundationによって発行されたそれ以降のバージョンの条件に基づいて、このドキュメントをコピー、配布、または変更する許可が与えられます。不変セクション、表紙テキスト、裏表紙テキストはありません。ライセンスのコピーは、「GNU Free Documentation License」というタイトルのセクションに含まれています。

1この文書の複製、頒布、および/または変更は、連邦経済産業連盟（連邦経済技術省）との関連を示すものではありません。

**この概要について**

Gpg4win Compendiumは3つの部分で構成されています。

パートI「初心者向け」：Gpg4winのクイックコース。

パートII「上級ユーザー向け」：Gpg4winの背景情報。

付録：Gpg4winに関する追加の技術情報。

パートI「初心者向け」では、Gpg4winプログラムコンポーネントのインストールと日常的な使用に関する簡単なガイドを提供します。練習ロボットAdeleがこのプロセスを支援し、Gpg4winに慣れるまで、（OpenPGPを使用して）暗号化解除および暗号化プロセスを練習することができます。

この簡単なガイドを実行するのに必要な時間は、コンピュータとWindowsに関する知識によって異なります。約1時間かかります。

パートII「上級ユーザー向け」では、Gpg4winのベースとなる基本的なメカニズムを説明する背景情報を提供し、あまり一般的に使用されていない機能のいくつかを説明します。パートIとIIは、互いに独立して使用できます。ただし、最適な理解を得るには、可能であれば、両方の部分を指示された順序で読む必要があります。

付録には、GpgOL Outlookプログラム拡張を含む、Gpg4winを取り巻く特定の技術的な問題に関する詳細が含まれています。

暗号化プログラムパッケージGpg4winと同様に、この大要は数学者、シークレットサービスエージェント、または暗号学者向けではなく、だれでも読んで理解できるように作成されています。

Gpg4winプログラムパッケージと概要は、次の場所で入手できます。

[http://www.gpg4win.org](https://translate.google.com/translate?hl=ja&prev=_t&sl=auto&tl=ja&u=http://www.gpg4win.org)

３

**伝説**

この大要では、次のテキストマーカーを使用しています。

イタリックは、画面に表示されるテキスト（メニューやダイアログなど）に使用されます。また、[ボタン]には角かっこを使用しています。

テキスト内の個々の単語にイタリック体が使用されることもありますが、テキストの流れを乱すことなく、文章内でそれらの意味を強調表示する場合は、太字を使用します（たとえばOpenPGPのみ）。

太字は、特に重要と見なされ、強調表示する必要がある個々の単語または文に使用されます。これらの特性により、読者は強調表示された主要な用語や重要なフレーズをすばやく簡単に見つけることができます。

タイプライターフォントは、すべてのファイル名、パス、URL、ソースコード、および入力と出力（コマンドラインなど）に使用されます。

4

**目次**

|  |  |  |  |
| --- | --- | --- | --- |
| **私。** | **初心者向け** | | **8** |
| **1。** | **Gpg4win –万人向けの暗号化** | | **9** |
| **2。** | **電子メールの暗号化：エンベロープがないため** | | **11** |
| **3。** | **Gpg4winの仕組み** | | **14** |
| **4。** | **パスフレーズ** | | **25** |
| **5。** | **2つの方法、1つの目標：OpenPGPとS / MIME** | | **28** |
| **6。** | **Gpg4winのインストール** | | **30** |
| **7。** | **証明書を作成する** | | **41** |
|  | 7.1。 | OpenPGP証明書の作成。。。。。。。。。。。。。。。。。。。。。。。。。。。。 | 44 |
|  | 7.2。 | X.509証明書の作成。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。 | 50 |
|  | 7.3。 | 証明書作成プロセスが完了しました。。。。。。。。。。。。。。。。。。。。。。。。。。 | 56 |
| **8。** | **公開証明書の配布** | | **58** |
|  | 8.1。 | 電子メールごとに公開し、OpenPGPを実践。。。。。。。。。。。。。。。。。。。 | 59 |
|  | 8.2。 | OpenPGP証明書サーバー経由で公開します。。。。。。。。。。。。。。。。。。。。。。。。。 | 65 |
|  | 8.3。 | X.509証明書の公開。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。 | 67 |
| **9。** | **電子メールの解読、OpenPGPの練習** | | **68** |
| **10.公開証明書のインポート** | | | **72** |
| **11.証明書の検査** | | | **75** |
| **12.電子メールの暗号化** | | | **82** |
| **13.メールに署名する** | | | **86** |
|  | 13.1。 | GpgOLでの署名。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。 | 87 |
|  | 13.2。 | GpgOLによる署名の確認。。。。。。。。。。。。。。。。。。。。。。。。。。。 | 92 |
|  | 13.3。 | 署名が壊れた理由。。。。。。。。。。。。。。。。。。。。。。。。。。。。。 | 93 |
|  | 13.4。 | 暗号化と署名。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。 | 94 |
| **14.暗号化された形式での電子メールのアーカイブ** | | | **95** |

5

Gpg4win Compendium 3.0.0

目次

|  |  |  |
| --- | --- | --- |
| **II。上級ユーザー向け** | | **97** |
| **15.証明書の詳細** | | **98** |
| **16.証明書サーバー** | | **100** |
| 16.1。 | 鍵サーバー構成。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。 | 101 |
| 16.2。 | 証明書サーバーから証明書を検索してインポートします。。。。。。。。。。。。。。。。。 | 103 |
| 16.3。 | 証明書をOpenPGP証明書サーバーにエクスポートします。。。。。。。。。。。。。。。。。。。 | 103 |
| **17.添付ファイルの暗号化** | | **104** |
| **18.ファイルの署名と暗号化** | | **105** |
| 18.1。 | ファイルの署名と確認。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。 | 106 |
| 18.2。 | ファイルの暗号化と復号化。。。。。。。。。。。。。。。。。。。。。。。。。。。。。 | 114 |
| **19.プライベート証明書のインポートとエクスポート** | | **122** |
| 19.1。 | 書き出す 。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。 | 123 |
| 19.2。 | インポートします。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。 | 124 |
| **20. S / MIMEのシステム全体の設定と事前入力** | | **126** |
| **21.既知の問題とヘルプ** | | **128** |
| 21.1。 | OutlookにGpgOLメニューとダイアログが表示されなくなりました。。。。。。。。。。。。。。。。 | 128 |
| 21.2。 | GpgOLボタンはOutlook 2003ツールバーにありません。。。。。。。。。。。。。。。。。。 | 128 |
| 21.3。 | GpgOLボタンは「アドイン」（Outlook 2007）の下にリストされています。。。。。。。。。。。。。。。 | 128 |
| 21.4。 | GpgOLの起動時のエラー。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。 | 128 |
| 21.5。 | 仮想ドライブへのGpg4winのインストール。。。。。。。。。。。。。。。。。。。。。。。 | 129 |
| 21.6。 | GpgOLは「CryptoEx」InlinePGP電子メールをチェックしません。。。。。。。。。。。。。。。。 | 129 |
| 21.7。 | S / MIME操作を許可しません（システムサービス「DirMngr」が実行されていません）。。。。。 | 130 |
| 21.8。 | S / MIME操作は許可されていません（CRLは使用できません）。。。。。。。。。。。。。。。。。 | 130 |
| 21.9。 | S / MIME操作は許可されていません（ルート証明書は信頼できません）。。。。。。。。。。 | 131 |
| **22. Gpg4winのファイルと設定** | | **132** |
| 22.1。 | 個人ユーザー設定。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。 | 132 |
| 22.2。 | キャッシュされた証明書失効リスト。。。。。。。。。。。。。。。。。。。。。。。。。。。 | 132 |
| 22.3。 | DirMngrからの信頼できるルート証明書。。。。。。。。。。。。。。。。。。。。。。 | 133 |
| 22.4。 | DirMngrからの他の証明書。。。。。。。。。。。。。。。。。。。。。。。。。。。。 | 133 |
| 22.5。 | 外部X.509証明書サーバーを使用するためのシステム全体の構成。。。。。。。 | 134 |
| 22.6。 | システム全体で信頼できるルート証明書。。。。。。。。。。。。。。。。。。。。。。。 | 135 |
| 22.7。 | ルート証明書の信頼性のユーザーマーキング。。。。。。。。。。。。。。。。。。 | 136 |
| **23. Gpg4winプログラム（ログファイル）の問題の検出** | | **137** |
| 23.1。 | Kleopatraログファイルをアクティブ化します。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。 | 138 |
| 23.2。 | GpgOLログファイルのアクティブ化。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。 | 139 |
| 23.3。 | DirMngrログファイルをアクティブ化しています。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。 | 140 |
| 23.4。 | GnuPGログファイルのアクティブ化。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。 | 141 |
| 23.5。 | GpgMEログファイルのアクティブ化。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。 | 142 |

6

Gpg4win Compendium 3.0.0

目次

|  |  |  |
| --- | --- | --- |
| **24. Gpg4winが壊れない理由...** | | **143** |
| **25. GnuPGと多数の謎** | | **144** |
| 25.1。 | 残差クラスで計算する。。。。。。。。。。。。。。。。。。。。。。。。。。。。 | 146 |
| 25.2。 | RSAアルゴリズムと残差クラスを使用した計算。。。。。。。。。。。。。。。。。。 | 149 |
| 25.3。 | 少数のRSA暗号化。。。。。。。。。。。。。。。。。。。。。。。。。。 | 150 |
| 25.4。 | 異なる基数を使用して表示します。。。。。。。。。。。。。。。。。。。。。。。。。。 | 155 |

|  |  |
| --- | --- |
| **III。別館** | **162** |
| **A. GpgOL Outlook拡張機能に関する情報** | **163** |
| **B.他の電子メールプログラムでGnuPGを使用する** | **166** |
| **C. Gpg4winの自動インストール** | **167** |
| **D.他のプログラムからの転送** | **169** |
| **E. Gpg4winのアンインストール** | **171** |
| **F.歴史** | **173** |
| **G. GNU Free Documentation License** | **174** |
| **インデックス** | **181** |

7

**パートI**

**初心者向け**

8

**1. Gpg4win –万人向けの暗号化**

Gpg4winとは何ですか？ウィキペディアはこの質問に次のように答えます。

Gpg4winは、Windows（2000 / XP / 2003 / Vista）用のインストールパッケージであり、電子メールとファイルの暗号化のためのコンピュータプログラムとハンドブックが含まれています。GnuPG暗号化ソフトウェアだけでなく、いくつかのアプリケーションとドキュメントも含まれています。Gpg4win自体とGpg4winに含まれるプログラムはフリーソフトウェアです。

「初心者向け」と「上級ユーザー向け」のハンドブックは、「第2版」の名前が「大要」にまとめられました。バージョン2では、Gpg4winには以下のプログラムが含まれています。

GnuPG

GnuPGは、実際の暗号化ソフトウェアであるGpg4winの中核を形成します。

クレオパトラ

Gpg4winの中央証明書管理により、すべての暗号化操作のユーザーナビゲーションが統一されます。

GNUプライバシーアシスタント（GPA）

クレオパトラに加えて、証明書を管理するための代替プログラムです。

Outlook用GnuPG（GpgOL）

Microsoft Outlook 2003および2007の拡張機能で、メッセージの署名と暗号化に使用されます。

GPG Explorer eXtension（GpgEX）

は、Windowsエクスプローラーの拡張機能であり、コンテキストメニューを使用してファイルの署名と暗号化に使用できます。

爪のメール

は、GnuPGに対する非常に優れたサポートを提供する完全な電子メールプログラムです。

GnuPG（GNUプライバシーガード）暗号化プログラムを使用すると、誰でも安全に、簡単に、無料で電子メールを暗号化できます。GnuPGは、個人的または商業的に制限なく使用できます。GnuPGで使用される暗号化技術は安全であり、今日の技術と研究の状況に基づいて解読することはできません。

GnuPGはフリーソフトウェア1です。つまり、各個人がこのソフトウェアを私的または商業的使用のために使用する権利を持っています。各人は、プログラムのソースコードを調査し、必要な技術的知識を持っている場合は修正を加えて、他の人に転送することができます。

セキュリティソフトウェアに関しては、このレベルの透明性（ソースコードへのアクセスの保証）は不可欠な基盤を形成します。これは、プログラミングとプログラム自体の信頼性を実際に確認する唯一の方法です。

1多くの場合、オープンソースソフトウェア（OSS）とも呼ばれます。

9

Gpg4win Compendium 3.0.0

第1章Gpg4win –すべての人のための暗号

GnuPGは国際標準のOpenPGP（RFC 4880）に基づいており、PGPと完全に互換性があり、後者と同じインフラストラクチャ（証明書サーバーなど）も使用します。GnuPGのバージョン2以降、暗号化規格S / MIME（IETF RFC 3851、ITU-T X.509およびISIS-MTT /共通PKI）もサポートされています。

PGP（「Pretty Good Privacy」）はフリーソフトウェアではありません。何年も前に、GnuPGと同じ条件で簡単に入手できました。ただし、このバージョンはしばらくの間、最新のテクノロジーに対応していません。

Gpg4winの前任者は、インターネット上のセキュリティイニシアチブの一部として、連邦議会とテクノロジーによってサポートされました。Gpg4winおよびGpg4win2は、情報技術（BSI）の連邦政府によってサポートされていました。

GnuPGおよびインターネット上のセキュリティのために連邦政府が実施したその他のプロジェクトに関する追加情報は、BundesamtfürSicherheit in der Informationstechnik のWebページ[www.bsi.de](https://translate.google.com/translate?hl=ja&prev=_t&sl=auto&tl=ja&u=http://www.bsi.de)および[www.bsi-fuer-buerger.de](https://translate.google.com/translate?hl=ja&prev=_t&sl=auto&tl=ja&u=http://www.bsi-fuer-buerger.de)にあります。

10

1. **電子メールの暗号化：エンベロープがないため**

メッセージの暗号化は、世界で2番目に古い職業と呼ばれることもあります。暗号化技術は、エジプトのファラオ、クナムホテプ2世まで、そしてヘロドットとシーザーの時代に使用されました。Gpg4winのおかげで、暗号化は王の予備ではなくなりましたが、誰でも無料でアクセスできます。

コンピュータテクノロジーは、世界中でコミュニケーションをとり、情報を入手するための優れたツールを提供してくれました。ただし、他の通信形態で当たり前と見なされている権利と自由は、新しいテクノロジーに関しては依然として確保する必要があります。インターネットは、私たちの権利を維持するのが難しいほどの速度と規模で発展してきました。

昔ながらの手紙の書き方で、書かれた内容は封筒で保護されています。封筒はメッセージをのぞき見から保護し、封筒が操作されたかどうかを簡単に確認できます。情報が重要でない場合のみ、保護されていないハガキに書き込んでください。郵便はがきや他の人も読むことができます。

11

Gpg4win Compendium 3.0.0

第2章電子メールの暗号化：エンベロープがないため

あなたと他の誰もメッセージが重要であるか、機密であるか秘密であるかを決定しません。

電子メールはこの種の自由を提供しません。電子メールははがきのようなもので、常に開いており、電子メールマンや他の人がいつでもアクセスできます。さらに悪いことに、コンピュータ技術は数百万の電子メールを転送および配布するオプションを提供する一方で、人々にそれらをチェックするオプションを提供します。

以前は、すべての手紙とはがきを収集したり、内容を分析したり、送信者と受信者を監視したりすることについて真剣に考える人はいませんでした。それは実行不可能だっただけでなく、時間がかかりすぎていたでしょう。しかし、現代のコンピューター技術はこれを技術的に可能にしました。これはすでに大規模に行われている兆候があります。エシェロンシステム1に関するウィキペディアの記事は、このトピックに関する興味深い背景情報を提供しています。

なぜこれが問題なのですか–エンベロープが欠落しているためです。

1[http://www.heise.de/tp/r4/artikel/6/6928/1.html](https://translate.google.com/translate?hl=ja&prev=_t&sl=auto&tl=ja&u=http://www.heise.de/tp/r4/artikel/6/6928/1.html)

12

Gpg4win Compendium 3.0.0

第2章電子メールの暗号化：エンベロープがないため

ここで提案するのは、本質的には電子メールの「エンベロープ」です。いつ、誰のために、どれくらいの頻度で使用するか-それは完全にあなた次第です。Gpg4winなどのソフトウェアは、選択する権利をあなたに返すだけです。メッセージが重要で保護を必要とするかどうかを選択する権利。

これは、基本法における通信、郵送、電気通信のプライバシーに対する権利の重要な側面であり、Gpg4winプログラムパッケージでは、この権利を行使できます。エンベロープを使用する必要がないのと同じように、このソフトウェアを使用する必要はありません。しかし、あなたには権利があります。

この権利を保護するために、Gpg4winはいわゆる「強力な暗号化技術」を提供しています。この意味での「強い」とは、既知のツールでは壊れないことを意味します。最近まで、強力な暗号化方式は、多くの国の軍や政府機関で使用されてきました。それらをすべての市民がアクセスできるようにする権利は、インターネットユーザーによって擁護され、暗号化の目的でフリーソフトウェアをサポートする場合のように、政府機関の先見の明のある人々の助けを借りることもありました。現在、世界中のセキュリティ専門家は、GnuPGを実用的で安全なソフトウェアと見なしています。

このタイプのセキュリティをどのように評価するかは、あなた次第です。

暗号化の利便性と最高レベルのセキュリティとの関係を決めるのはあなただけです。これらには、Gpg4winを適切に使用できるようにするために実装する必要があるいくつかの重要な予防策が含まれています。この大要では、このプロセスを段階的に説明します。

13

**3. Gpg4winの仕組み**

Gpg4winとその基礎となる「公開キー」方式の特別な機能は、誰でもそれを理解でき、理解する必要があることです。それについて秘密にされているものは何もありません。理解することはそれほど難しくありません。

個々のGpg4winプログラムコンポーネントの使用は、実際の動作はかなり複雑ですが、非常に簡単です。このセクションでは、Gpg4winがどのように機能するかを説明します。詳細については説明しませんが、このソフトウェアの背後にある原理を説明するには十分です。原則に慣れると、Gpg4winが提供するセキュリティにかなりの信頼を得ることができます。

この本の最後の第24章では、「公開鍵」暗号化を取り巻く残りの秘密を解き明かし、現在の技術状態を使用してGpg4winで暗号化されたメッセージを解読できない理由を発見できます。

14

Gpg4win Compendium 3.0.0

第3章Gpg4winの仕組み

**キーホルダーの主**

貴重なものを保護したい人は、鍵でそれをロックします。ユニークで安全な場所に保管される鍵はさらに優れています。

キーが悪用されると、貴重品は安全ではなくなります。それらのセキュリティは、キーのセキュリティと一意性に依存します。したがって、鍵は少なくとも貴重品自体と同様に保護する必要があります。コピーできないようにするには、キーの正確な特性も秘密にしておく必要があります。

15

Gpg4win Compendium 3.0.0

第3章Gpg4winの仕組み

秘密鍵は暗号化では新しいものではありません。メッセージの機密性を保護するために、鍵は常に隠されていました。このプロセスを非常に安全にすることは非常に面倒であり、エラーが発生しやすくなります。

メッセージの「通常の」秘密送信の基本的な問題は、暗号化と復号化の両方に同じキーが使用され、送信者と受信者の両方がこの秘密キーに精通している必要があることです。このため、これらのタイプの暗号化システムは「対称暗号化」とも呼ばれます。

これはかなり逆説的な状況をもたらします：この方法を使用して秘密を伝える前に

（暗号化されたメッセージ）、私達はまた別の秘密を前もって伝えなければなりません：キー。そしてそれがまさに問題です。つまり、第三者によって傍受されないようにしながら、常に鍵を交換しなければならないという常に発生する問題です。

16

Gpg4win Compendium 3.0.0

第3章Gpg4winの仕組み

対照的に–秘密鍵を含まない– Gpg4winは、完全にアクセス可能で公開されている別の鍵で動作します。「公開鍵」暗号化システムとも呼ばれます。

これは矛盾に聞こえるかもしれませんが、そうではありません。手がかり：秘密鍵を交換する必要はもうありません。

逆に：秘密鍵は交換できません！渡すことができる唯一の鍵は、（公開証明書内の）公開鍵で、誰でも知ることができます。

つまり、Gpg4winを使用する場合、実際には秘密鍵と2番目の公開鍵のペアの鍵を使用しています。両方の主要なコンポーネントは、複雑な数式と密接に関連しています。現在の科学的および技術的な知識に基づいて、他を使用して1つの主要なコンポーネントを計算することは不可能であり、したがって、方法を破ることは不可能です。

セクション24では、その理由を説明します。

17

Gpg4win Compendium 3.0.0

第3章Gpg4winの仕組み

公開鍵暗号化の背後にある原則

秘密鍵または秘密鍵は秘密にしておく必要があります。

公開鍵は、できるだけ一般の人がアクセスできるようにする必要があります。

両方の主要コンポーネントには、非常に異なる機能があります。

秘密鍵コンポーネントはメッセージを復号化します。

公開鍵コンポーネントはメッセージを暗号化します。

18

Gpg4win Compendium 3.0.0

第3章Gpg4winの仕組み

**パブリックメールのストロングボックス**

この小さな演習では、「公開鍵」暗号化システムと対称暗号化（「非公開鍵」方式）の違いを説明します...

「秘密鍵方式」は次のように機能します。

家の前に強力なメールボックスをインストールしていて、秘密のメッセージの送信に使用したいとします。

ストロングボックスには、キーが1つしかないロックがあります。このキーがないと、誰も何も箱に入れたり箱から取り出したりすることはできません。このように、秘密のメッセージはかなり安全です。

キーは1つしかないので、メールのストロングボックスを開いてロックしたり、秘密のメッセージを送信したりするには、相手が同じキーを持っている必要があります。

19

Gpg4win Compendium 3.0.0

第3章Gpg4winの仕組み

あなたは秘密のルートを介してその人にこの鍵を与える必要があります。

20

Gpg4win Compendium 3.0.0

第3章Gpg4winの仕組み

彼らは、ストロングボックスを開いてシークレットキーを取得した後でのみ、シークレットメッセージを読むことができます。

したがって、すべてがこの1つの鍵にかかっています。第三者がその鍵を知っている場合、それは秘密のメッセージの終わりです。したがって、あなたとあなたが対応している人は、メッセージ自体と同じくらい秘密の方法で鍵を交換しなければなりません。

しかし、実際には、鍵を渡すときに、秘密のメッセージを伝えることもできます。

これが電子メールの暗号化にどのように適用されるか：世界中では、すべての参加者が秘密鍵を持ち、これらの鍵を秘密に交換してから、電子メールごとに秘密のメッセージを送信する必要があります。

したがって、このオプションを忘れてしまう可能性があります...

21

Gpg4win Compendium 3.0.0

第3章Gpg4winの仕組み

今「公開鍵」メソッド

あなたの家の前にもう一度メールボックスをインストールします。ただし、最初の例のstrongboxとは異なり、これは常に開いています。箱には鍵が掛けられています。これは誰でも見ることができます。鍵は誰でも使用でき、ストロングボックスをロックできます（非対称暗号化方式）。

ロックしますが、開きません：それが違いです！

この鍵はあなたのものであり、またご想像のとおり、それはあなたの公開鍵です。

誰かがあなたに秘密のメッセージを残したい場合、彼らはそれをストロングボックスに入れ、あなたの公開鍵でそれをロックします。キーは誰でも利用できるため、誰でもこれを行うことができます。

他の誰もストロングボックスを開いてメッセージを読むことはできません。ストロングボックスでメッセージをロックした人でさえ、メッセージを変更するためなどに再度ロックを解除することはできません。

これは、公開鍵の半分はロック目的でのみ使用できるためです。

ストロングボックスは、1つのキーでのみ開くことができます。つまり、キーの秘密部分と非公開部分です。

22

Gpg4win Compendium 3.0.0

第3章Gpg4winの仕組み

これが電子メールの暗号化にどのように適用されるかに戻ると、誰でも電子メールを暗号化できます。

これを行うには、秘密鍵は必要ありません。まったく反対ですが、必要なのは完全に非秘密の「公開」鍵だけです。電子メールの復号化に使用できるキーは1つだけ、つまり秘密キーと秘密キーです。

このシナリオを別の方法で再生することもできます。

誰かに秘密のメッセージを送りたい場合は、彼らのメールストロングボックスを自分の公開鍵と自由に利用できる鍵で使用します。

これを行うには、どこにいても公開鍵にいつでもアクセスできるため、メッセージを書いている相手を直接知っている必要はありません。また、相手に話しかける必要もありません。あなたがあなたのメッセージをストロングボックスに置き、それを受信者のキーでロックした場合、あなたを含む誰もメッセージにアクセスできません。受信者だけが自分の秘密鍵で金庫を開いてメッセージを読むことができます。

23

Gpg4win Compendium 3.0.0

第3章Gpg4winの仕組み

しかし、私たちが本当に得たものは、まだ秘密の鍵があります！

ただし、これは「非公開鍵」方式とはかなり異なります。秘密鍵を知って使用するのはあなただけです。キーが第三者に転送されることはありません。秘密でキーを転送する必要はなく、アドバイスもありません。

送信者と受信者の間で、秘密の合意であろうと秘密のコードであろうと、何も秘密裏にやり取りしてはなりません。

そして、それはまさに問題の核心です：鍵が交換されている間に第三者が鍵を取得する機会があるので、すべての対称暗号化方式は破られる可能性があります。

秘密鍵の交換がないため、このリスクはここでは当てはまりません。むしろ、それは1つの非常に安全な場所でしか見つけることができません：あなた自身のキーリング–あなた自身のメモリ。

非秘密鍵と公開鍵、および秘密鍵と秘密鍵の部分を使用するこの最新の暗号化方法は、「非対称暗号化」とも呼ばれます。

24

**4.パスフレーズ**

前の章で見たように、秘密鍵は「公開鍵」または非対称暗号化方式の最も重要なコンポーネントの1つです。秘密に別の関係者と鍵を交換する必要はありませんが、この鍵のセキュリティは、それでも「全体」の暗号化プロセスのセキュリティの「鍵」です。

技術レベルでは、秘密鍵はコンピュータに保存されるファイルにすぎません。このファイルへの不正アクセスを防止するために、2つの方法で保護されています。

まず、コンピュータの管理者は常にすべてのファイルにアクセスでき、コンピュータが失われたり、ウイルス、ワーム、トロイの木馬に攻撃されたりする可能性があるため、他のユーザーがファイルを読み書きすることはできません。

このため、パスフレーズという別の保護レイヤーが必要です。これはパスワードではありません。たとえば、パスフレーズは1つの単語だけで構成するのではなく、1つの文で構成する必要があります。あなたは本当にこのパスフレーズを「頭の中で」保ち、決して書き留める必要はないはずです。

同時に、それを推測することは不可能です。これは矛盾に聞こえるかもしれませんが、そうではありません。非常にユニークで覚えやすいパスフレーズを見つける方法はいくつかありますが、簡単に推測することはできません。

25

Gpg4win Compendium 3.0.0

第4章パスフレーズ

あなたにとても馴染みのあるフレーズを考えてください。例：

ガラスの家の人々は石を投げてはいけません。

ここで、この文の3文字ごとに取ります。

oegsoehloerisn （PE **O**PL **E**における**G**ラ**S**S H **O**米国**E**S S **H**OU **のL**D N **O**のT B **E**番目**R**OW **I**NG **S**に**N**ES）。

この一連の文字を覚えることは簡単ではないかもしれませんが、元の文を覚えている限り、パスフレーズにたどり着く方法を忘れることもほとんどありません。時間の経過とともに、このフレーズをより頻繁に使用するようになると、それをメモリにコミットします。他の誰もパスフレーズを推測することはできません。

あなたが決して忘れないことを知っているイベントを考えてください。多分それはあなたが常にあなたの子供やパートナーと関係するフレーズです、すなわち、それは「忘れられない」になりました。または、あなたにとって個人的に重要な休暇の思い出や歌のテキストの行。

大文字、小文字、数字、特殊文字、スペースを任意の順序で使用します。原則として、ウムラウト、特殊文字、数字など、何でもかまいません。ただし、海外の別のコンピューターで秘密鍵を使用する場合は、すべてのキーボードにそのような特殊文字があるとは限らないことに注意してください。たとえば、ドイツ語のキーボードではウムラウト（ä、ö、üusw.）のみが見つかる可能性があります。

また、意図的に文法を間違えることもあります。たとえば、「間違い」ではなく「誤字」です。もちろん、これらの「間違い」を覚えておく必要もあります。または、フレーズの途中で言語を変更します。文を変更できます：

ミュンヘンでは、ホフブロイハウスです。

このパスフレーズに：

inMinschen stet 1h0f breuhome

意味のない文を考えてみてください。

核の家を嘆く専門家

嵐の中でもアコーデオンを編む。

この長さのパスフレーズは、秘密鍵を適切に保護します。

大文字を使用する場合は、次のように短くすることもできます。

専門家の核兵器ホーム。

パスフレーズは短くなりましたが、覚えるのも難しくなっています。特殊文字を使用してパスフレーズをさらに短くすると、パスフレーズを入力する時間を節約できますが、パスフレーズを忘れてしまう可能性もあります。

以下は、非常に短いが非常に安全なパスフレーズの極端な例です。

R！Qw "s、UIb \*7 \ $

ただし、実際には、そのような文字のシーケンスは、覚える手がかりが少なすぎるため、それほど有用であるとは証明されていません。

26日

Gpg4win Compendium 3.0.0

第4章パスフレーズ

悪いパスフレーズは非常に迅速に「壊れる」可能性があります...

...は既に別の目的で使用されています（例：電子メールアカウントまたは携帯電話）。したがって、同じパスフレーズは、別の、おそらく安全ではないソフトウェアにすでに知られています。ハッカーが成功した場合、パスフレーズは実質的に無意味になります。

...辞書から来ています。パスフレーズ検索プログラムは、単語の1つに一致するまで、数分で完全なデジタル辞書を介してパスワードを実行できます。

...生年月日、名前、またはその他の公開情報で構成されます。あなたの電子メールを解読しようと計画している人は誰でもこの種の情報を入手するでしょう。

...は「あるべきか否か」などの非常に一般的な引用です。パスフレーズ検索プログラムも、パスフレーズを解読するためにこのような引用符を使用します。

...は、1つの単語のみ、または8文字未満で構成されています。より長いパスフレーズを考えることが非常に重要です。

パスフレーズを作成するときは、上記の例を使用しないでください。パスフレーズを手に入れることに真剣に関心のある人なら誰でも、これらの例のいずれかを使用したかどうかが自然にわかるからです。

クリエイティブに！今パスフレーズを考えてください！忘れられない、壊れない。

第7章では、キーペアを作成するためにこのパスフレーズが必要になります。

しかし、それまでは、別の問題に対処する必要があります。誰かがあなたに秘密のメッセージを送りたい人が本物であることを確認する必要があります。

27日

1. **2つの方法、1つの目標：OpenPGP＆**

**S / MIME**

電子メールの「エンベロープ」の重要性と、最新の情報技術のツールを使用して1つを提供する方法を見てきました。メールのストロングボックス。誰でも、ストロングボックスの所有者である暗号化されたメールを送信できます。 。「strongbox」への秘密鍵が秘密のままである限り、暗号化を解読することはできません。

それでも、あなたがそれについて考えるならば、まだ別の問題があります。少し先に、秘密鍵方式とは対照的に、相手が秘密のメッセージを送信できるようにするために、相手と直接会う必要はありません。しかし、どのようにしてこの人が実際に彼らが彼らがそうであると言う人であると確信することができますか？電子メールの場合、個人レベルで対応しているすべての人を知ることはめったにありません。通常、電子メールアドレスの背後に誰がいるのかを見つけることは簡単ではありません。したがって、メッセージの機密性だけでなく、送信者のID、特に信頼性も保証する必要があります。

したがって、誰かがあなたに秘密のメッセージを送りたい人が本物であることを認証しなければなりません。日常生活では、当局や公証人によって認証されたID、署名、証明書を「認証」の目的で使用します。これらの機関は、上位機関から、そして最終的には立法者から公証を発行する権利を引き出します。別の見方をすると、それは「トップ」から「ボトム」まで続く信頼の連鎖を表し、「階層的信頼概念」として記述されます。

Gpg4winまたは他の電子メール暗号化プログラムの場合、この概念はS / MIMEのほとんどミラーのような方法で見つかります。これにisOpenPGPが追加されました。これは、インターネット上でのみこの方法で機能する別の概念です。S / MIMEとOpenPGPには同じタスクがあります。データの暗号化と署名です。どちらも、おなじみの公開鍵方式を使用しています。いくつかの重要な違いがありますが、結局のところ、これらの標準のどれも他のものよりも一般的な利点を提供しません。このため、Gpg4winを使用して両方の方法を使用できます。

28

Gpg4win Compendium 3.0.0

第5章2つの方法、1つの目標：OpenPGPとS / MIME

階層的信頼概念に相当するものは、「Secure / Multipurpose Internet Mail Extension」またはS / MIMEと呼ばれます。S / MIMEを使用する場合、使用する前に、認定組織による鍵の認証が必要です。この組織の証明書は、いわゆるルート証明書に到達するまで、上位の組織などによって認証されました。この信頼の階層チェーンには、通常、3つのリンクがあります。ルート証明書、証明書の発行者の証明書（認証局のCA）、最後に独自のユーザー証明書です。

2つ目の代替で互換性のない公証方法はOpenPGP標準であり、信頼階層を構築せず、「信頼のWeb」を構築します。Web of Trustは、非階層型インターネットとそのユーザーの基本構造を表しています。たとえば、ユーザーBがユーザーAを信頼している場合、このキーがユーザーAによって認証されていれば、ユーザーBは知らないユーザーCの公開キーも信頼できます。

したがって、OpenPGPには、上位の機関による認証なしに、暗号化されたデータと電子メールを交換するオプションがあります。通信相手の電子メールアドレスと関連する証明書を信頼していれば十分です。

信頼階層とWeb of Trustのどちらを使用する場合でも、送信者の認証は、少なくともメッセージの保護と同じくらい重要です。この重要な保護機能については、後で説明します。現時点では、Gpg4winをインストールして次の章を理解するには、この情報で十分です。

OpenPGPとS / MIMEの両方の方法は、必要なセキュリティを提供します。

メソッドは相互に互換性がありません。秘密の通信を認証するための2つの代替方法を提供します。したがって、それらは相互運用可能であるとは見なされません。

Gpg4winでは、両方の方法を並行して簡単に使用できます。暗号化/署名の目的でどちらか一方を選択する必要はありません。

この大要の第7章では、キーペアの作成について説明しているので、分岐して両方の方法について説明します。第7章の終わりに、情報が再び結合されます。

この大要では、これら2つの記号は2つの代替方法を参照するために使用されます。

29日

**6. Gpg4winのインストール**

第1章から第5章では、暗号化に関連する背景について説明しました。Gpg4winはその背後にあるロジックを理解していなくても機能しますが、このプログラムへの秘密の通信を委託しているという点でも他のプログラムとは異なります。したがって、それがどのように機能するかを知ることは良いことです。

この知識があれば、Gpg4winをインストールしてキーペアを設定する準備が整います。

コンピューターにGnuPGベースのアプリケーション（GnuPP、GnuPT、WinPT、GnuPG Basicsなど）が既にインストールされている場合は、既存の証明書の転送について、付録Dを参照してください。

Gpg4winは、インターネットまたはCDからロードしてインストールできます。これを行うには、Windowsオペレーティングシステムの管理者権限が必要です。

Gpg4winをインターネットからダウンロードする場合は、信頼できるサイト（[www.gpg4win.org](https://translate.google.com/translate?hl=ja&prev=_t&sl=auto&tl=ja&u=http://www.gpg4win.org)など）からファイルを取得してください。インストールを開始するには、ダウンロード後に次のファイルをクリックします。

gpg4win-2.0.0.exe （またはそれ以上のバージョン番号）。

CD ROMでGpg4winを受け取った場合は、それを開き、「Gpg4win」インストールアイコンをクリックしてください。

他のすべてのインストール手順は同じです。

プログラムをインストールするかどうかの質問に対する回答は[はい]です。

30

Gpg4win Compendium 3.0.0

第6章Gpg4winのインストール

インストールアシスタントが起動し、インストールプロセスで使用する言語を尋ねます。

[OK]で言語の選択を確認します。

その後、次のウェルカムダイアログが表示されます。

コンピュータで実行中のすべてのプログラムを閉じて、[次へ]をクリックします。

31

Gpg4win Compendium 3.0.0

第6章Gpg4winのインストール

次のページにライセンス契約が表示されます。Gpg4winを変更または転送する場合にのみ重要です。ソフトウェアのみを使用したい場合は、ライセンスを読まなくてもすぐに実行できます。

[次へ]をクリックします。

32

Gpg4win Compendium 3.0.0

第6章Gpg4winのインストール

コンポーネントの選択を含むページで、インストールするプログラムを決定できます。

デフォルトの選択がすでに行われています。後で個々のコンポーネントをインストールすることもできます。

マウスカーソルをコンポーネントの上に移動すると、簡単な説明が表示されます。もう1つの便利な機能は、選択したすべてのコンポーネントに必要なハードドライブ領域の表示です。

[次へ]をクリックします。

33

Gpg4win Compendium 3.0.0

第6章Gpg4winのインストール

システムは、インストール用のフォルダーを提案します。例：C：nProgrammenGNUnGnuPG

提案を受け入れるか、Gpg4winをインストールするための別のフォルダーを選択できます。

次に、[次へ]をクリックします。

34

Gpg4win Compendium 3.0.0

第6章Gpg4winのインストール

これで、インストールするリンクを決定できます。システムは、スタートメニューでリンクを自動的に作成します。このリンクは、Windowsダッシュボードの設定を使用して後で変更できます。

次に、[次へ]をクリックします。

35

Gpg4win Compendium 3.0.0

第6章Gpg4winのインストール

デフォルト設定（スタートメニューとリンク）を選択した場合は、次のページでこのスタートメニューの名前を定義するか、名前をそのまま使用できます。

次に[インストール]をクリックします。

36

Gpg4win Compendium 3.0.0

第6章Gpg4winのインストール

次のインストールプロセス中に、進行状況バーと、現在インストールされているファイルに関する情報が表示されます。[詳細の表示]を押すと、いつでもインストールログを表示できます。

インストールが完了したら、[次へ]をクリックしてください。

37

Gpg4win Compendium 3.0.0

第6章Gpg4winのインストール

インストールが正常に完了すると、インストールプロセスの最後のページが表示されます。

インストールしたGpg4winのバージョンに関する重要な情報を含むREADMEファイルを表示するオプションがあります。このファイルを表示したくない場合は、このオプションを無効にします。

次に[完了]をクリックします。

38

Gpg4win Compendium 3.0.0

第6章Gpg4winのインストール

場合によっては、Windowsを再起動する必要があります。この場合、次のページが表示されます。

これで、Windowsをすぐに再起動するか、後で手動で再起動するかを決定できます。

[完了]をクリックしてください。

インストールされたばかりのGpg4winバージョンの最新情報を含むREADMEファイルをお読みください。このファイルは、たとえばスタートメニューから見つけることができます：Start！Programs！Gpg4win！Documentation！Gpg4win README

39

Gpg4win Compendium 3.0.0

第6章Gpg4winのインストール

以上です！

Gpg4winが正常にインストールされ、プログラムを使用する準備ができました。

ソフトウェア配布システムに関連する可能性があるGpg4winの自動インストールについては、付録C「Gpg4winの自動インストール」を参照してください。

40

**7.証明書を作成する**

GnuPGが非常に安全である理由（第3章）と、適切なパスフレーズが秘密鍵の保護を提供する方法（第4章）がわかったので、独自の鍵ペアを作成する準備ができました。

第3章で見たように、鍵ペアは公開鍵と秘密鍵で構成されています。ペア作成時に入力するメールアドレス、ログイン名など（いわゆるメタデータ）を追加することで、公開鍵と秘密鍵で秘密証明書を取得できます。

この定義は、OpenPGPとS / MIMEの両方に適用されます（S / MIME証明書は、「X.509」として説明されている規格に対応しています）。

鍵ペアを作成するこの重要なステップを練習できたらいいですね……。

心配する必要はありません。それはOpenPGPでのみ可能です。

OpenPGPの認証方法である「Web of Trust」を選択した場合は、非常に快適になるまで、キーペアの作成、暗号化、復号化のプロセス全体を好きなだけ練習できます。

この「ドライラン」は、Gpg4winへの信頼を強化し、OpenPGP鍵ペア作成の「ホットフェーズ」はもはや問題ではなくなります。

この演習のパートナーはAdeleです。Adeleは、GnuPPの前身のプロジェクトからまだ派生しており、現在も稼働しているテストサービスです。この大要では、この練習用ロボットの使用を引き続き推奨しています。この練習用ロボットを操作してくださったgnupp.deの所有者にも感謝します。残念ながら、Adeleが機能していることは保証できません。アデルにはいくつかの問題があることがわかっています。発生する可能性のある問題については、[https：//wiki.gnupg.org/EmailExercisesRobotで](https://translate.google.com/translate?hl=ja&prev=_t&sl=auto&tl=ja&u=https://wiki.gnupg.org/EmailExercisesRobot)お知らせください。

Adeleを使用すると、本格的に使用を開始する前に、間もなく作成するOpenPGP鍵ペアを練習およびテストできます。しかし、その詳細については後で説明します。

41

Gpg4win Compendium 3.0.0

第7章証明書の作成

行こう！Windowsのスタートメニューを使用してKleopatraを開きます。

メインのKleopatra画面が表示されます–証明書管理：

証明書をまだ作成またはインポートしていないため、最初はこの概要は空です。

42

Gpg4win Compendium 3.0.0

第7章証明書の作成

File！New Certificateをクリックします。

次のダイアログで、証明書の形式を選択します。以下から選択できます。

OpenPGP（PGP / MIME）またはX.509（S / MIME）。

2つの形式の違いと共通機能については、第5章で既に説明しています。

要約のこの章は、この時点でメソッドごとに2つのセクションに分かれています。その後、章の最後で情報が結合されます。

OpenPGPまたはX.509（S / MIME）のどちらを選択したかに応じて、次のいずれかを読み取ることができます。

セクション7.1：OpenPGP証明書の作成（次のページを参照）または

セクション7.2：X.509証明書の作成（P. 57）。

43

Gpg4win Compendium 3.0.0

第7章証明書の作成

**7.1。OpenPGP証明書の作成**

証明書のオプションダイアログで、[個人のOpenPGPキーペアを作成する]をクリックします。

次に、次のウィンドウに電子メールアドレスと名前を入力します。名前とメールアドレスは後日公開されます。

キーペアのコメントを追加することもできます。通常、このフィールドは空のままですが、テスト用のキーを作成する場合は、「test」と入力して、テストキーであることを忘れないでください。このコメントはログイン名の一部になり、名前と電子メールアドレスと同じように公開されます。

OpenPGPキーペアを最初にテストする場合は、名前と架空の電子メールアドレスを次のように入力するだけです。

Heinrich Heine およびheinrich@gpg4win.de

詳細設定は、例外的な場合にのみ必要です。詳細については、Kleopatraハンドブック（Help！Kleopatraハンドブック経由）を参照してください。

[次へ]をクリックします。

44

Gpg4win Compendium 3.0.0

第7章証明書の作成

確認のために、すべてのメインエントリと設定のリストが表示されます。（デフォルト）エキスパート設定に興味がある場合は、[すべての詳細]オプションを使用してこれらを表示できます。

すべて正しければ、[キーの作成]をクリックします。

45

Gpg4win Compendium 3.0.0

第7章証明書の作成

次に、最も重要な部分について説明します。パスフレーズの入力です。

キーペアを作成するには、個人のパスフレーズを入力する必要があります。

第4章を読んだことがあれば、覚えやすいが秘密のパスフレーズを解読するのは難しいはずです。上部に表示されるダイアログに入力します。

このウィンドウはバックグラウンドで開かれている場合があり、最初は表示されないことに注意してください。

パスフレーズが短すぎるか、数字や特殊文字が含まれていないために十分に安全ではない場合、システムから通知されます。

この時点で、テストパスフレーズを入力するか、本格的に開始することもできます。それはあなた次第です。

入力ミスがないことを確認するため、パスフレーズを2回入力するように求められます。入力は必ず[OK]で確認してください。

46

Gpg4win Compendium 3.0.0

第7章証明書の作成

これでOpenPGP鍵ペアが作成されました：

これには数分かかる場合があります。下の入力フィールドに情報を入力することで、必要な乱数の作成を支援できます。文字は使用されないため、入力する内容は問題ではなく、各キーストロークの間の期間のみです。コンピューター上の別のアプリケーションを引き続き使用することもできます。これにより、新しいキーペアの品質もわずかに向上します。

47

Gpg4win Compendium 3.0.0

第7章証明書の作成

キーペアの作成が成功するとすぐに、次のダイアログが表示されます。

新しく生成されたOpenPGP証明書の40桁の「フィンガープリント」が結果のテキストフィールドに表示されます。このフィンガープリントは世界中のどこでもユニークです。つまり、他の人が同じフィンガープリントの証明書を持つことはありません。実際、8桁であっても、同じシーケンスが世界のどこかで2回発生することはすでにかなりありそうにありません。このため、多くの場合、使用または表示され、キーIDとして記述されるのは、指紋の最後の8桁のみです。このフィンガープリントは、証明書の身元と人のフィンガープリントを識別します。

ただし、指紋を覚えたり書き留めたりする必要はありません。後でクレオパトラの証明書の詳細に表示することもできます。

48

Gpg4win Compendium 3.0.0

第7章証明書の作成

次に、次の3つのボタンの1つ以上をアクティブ化できます。

**（プライベート）証明書のバックアップコピーを作成しています...**

完全な証明書（新しい鍵のペア、つまり秘密鍵と公開鍵を含む）をエクスポートするパスを入力します。

クレオパトラは、自動的にファイルの種類を選択して、あなたの証明書を格納します.ASC または.gpg ファイル

– ASCII鎧オプションを有効にするか無効にするかによって異なります。エクスポートする場合は、[OK]をクリックします。

重要：ファイルをハードドライブに保存する場合は、できるだけ早く別のデータキャリア（USBスティック、ディスケット、またはCD-ROM）にファイルをコピーし、元のファイルをトレースなしで削除してください。ごみ箱に！このデータキャリアとバックアップコピーを安全な場所に保管してください。

後でバックアップコピーを作成することもできます。これを行うには、Kleopatraのメインメニューから[File！Export private certificate ...]を選択します（第19章を参照）。

**電子メールによる証明書の送信...**

このボタンをクリックすると、新しい公開メールが添付された新しい電子メールが作成されます。もちろん、秘密のOpen PGP鍵は送信されません。受信者の電子メールアドレスを入力します。この電子メール用に準備されたテキストにさらにテキストを追加することもできます。

注意：すべての電子メールプログラムがこの機能をサポートしているわけではありません。もちろんこれもできます

手動：新しい電子メールウィンドウが表示されない場合は、証明書作成アシスタントをシャットダウンし、File！Export証明書を使用して公開証明書を保存し、このファイルを電子メールを介して対応する相手に送信します。詳細については、セクション8.1を参照してください。

**証明書サーバーに証明書を送信しています...**

章では、Kleopatraでグローバルに利用可能なOpenPGP証明書サーバーを設定する方法、およびこのサーバーで公開証明書を公開する方法について説明します16。

これでOpenPGP証明書の作成が完了しました。[完了]でクレオパトラアシスタントを終了します。

次に、56ページのセクション7.3に進みます。その時点から、OpenPGPとX.509の説明は同じになります。

49

Gpg4win Compendium 3.0.0

第7章証明書の作成

**7.2。X.509証明書の作成**

ページの証明書形式選択ダイアログで、43ボタンをクリックします

[ 個人のX.509キーペアと認証リクエストを作成する]。

次のウィンドウで、名前（CN =共通名）、電子メールアドレス（EMAIL）、組織（O）、国コード（C）を入力します。オプションで、場所（L =地域）と部門（OU =組織単位）を追加することもできます。

X.509キーペアの作成プロセスを最初にテストする場合は、名前、組織、国コードの情報を入力し、架空の電子メールアドレスを入力することもできます。例：CN = Heinrich

Heine、O = Test、C = DE、EMAIL = heinrich @ gpg4win.de

詳細設定は、例外的な場合にのみ必要です。詳細については、Kleopatraハンドブック（Help！Kleopatraハンドブック経由）を参照してください。

[次へ]をクリックします。

50

Gpg4win Compendium 3.0.0

第7章証明書の作成

確認のために、すべてのメインエントリと設定のリストが表示されます。（デフォルト）エキスパート設定に興味がある場合は、[すべての詳細]オプションを使用してこれらを表示できます。

すべてが正しければ、[Creat key]をクリックします。

51

Gpg4win Compendium 3.0.0

第7章証明書の作成

次に、最も重要な部分について説明します。パスフレーズの入力です。

鍵ペアを作成するために、パスフレーズを入力するよう求められます。

第4章を読んだことがあれば、覚えやすいが秘密のパスフレーズを解読するのは難しいはずです。上部に表示されるダイアログに入力してください！

このウィンドウはバックグラウンドで開かれている可能性があるため、最初は表示されない場合があります。

パスフレーズが短すぎるか、数字や特殊文字が含まれていないために十分に安全でない場合、システムは通知します。

この時点で、テストパスフレーズを入力するか、本格的に開始することもできます。それはあなた次第です。

入力ミスがないことを確認するため、パスフレーズを2回入力するように求められます。最後に、3回目のパスフレーズの入力を求められます。これにより、担当する認証インスタンスに証明書リクエストが送信されます。入力は必ず[OK]で確認してください。

52

Gpg4win Compendium 3.0.0

第7章証明書の作成

これで、X.509キーペアが作成されました。

これには数分かかる場合があります。下の入力フィールドに情報を入力することで、必要な乱数の作成を支援できます。文字は使用されないため、入力する内容は問題ではなく、各キーストロークの間の期間のみです。コンピューター上の他のアプリケーションを引き続き使用することもできます。これにより、作成される鍵ペアの品質がわずかに向上します。

53

Gpg4win Compendium 3.0.0

第7章証明書の作成

キーペアが正常に作成されるとすぐに、次のダイアログが表示されます。

次のステップは、次のボタンでトリガーされます。

**リクエストをファイルに保存...**

ここでは、X.509証明書リクエストをバックアップするパスを入力し、エントリを確認します。Kleopatraは、保存プロセス中に.p10 で終わるファイルを自動的に追加します。次に、このファイルを認証インスタンスに送信できます（略して、Certificate Au-thorityのCA）。さらに以下では、X.509証明書を無料で発行する非営利の認証インスタンス（CA）であるcacert.orgを紹介します。

**メールでリクエストを送る...**

これにより、添付ファイルに作成されたばかりの証明書リクエストを含む新しい電子メールが作成されます。受信者の電子メールアドレスを入力します。通常は、担当する認証局のアドレスです。この電子メールの準備されたテキストにさらにテキストを追加することもできます。

注意：すべての電子メールプログラムがこの機能をサポートしているわけではありません。もちろん、これを手動で行うこともできます。新しい電子メールウィンドウが表示されない場合は、リクエストをファイルに保存し（上記を参照）、電子メールで認証局（CA）に送信します。

CAが要求を処理するとすぐに、CAシステム管理者が、CAによって署名された完成したX.509証明書を送信します。ファイルをKleopatraにインポートするだけです（第19章を参照）。

[完了]でクレオパトラアシスタントを終了します。

54

Gpg4win Compendium 3.0.0

第7章証明書の作成

**www.cacert.orgを使用してX509証明書を作成する**

CAcertは、X.509証明書を無料で発行する非営利の認証局です。これは、商用ルートCAに代わる手段を提供し、そのいくつかは証明書に非常に高い料金を課します。

CAcertで（クライアント）証明書を作成するには、まず[www.cacert.orgで](https://translate.google.com/translate?hl=ja&prev=_t&sl=auto&tl=ja&u=http://www.cacert.org)登録する[必要があり](https://translate.google.com/translate?hl=ja&prev=_t&sl=auto&tl=ja&u=http://www.cacert.org)ます。

登録直後に、cacert.orgで1つ以上のクライアント証明書を作成できます。十分な長さのキー（2048ビットなど）があることを確認してください。Webアシスタントを使用して、証明書の安全なパスフレーズを定義します。

これでクライアント証明書が作成されました。

その後、新しいX.509証明書と関連するCAcertルート証明書への2つのリンクが記載された電子メールが届きます。両方の証明書をダウンロードします。

指示に従って、ブラウザに証明書をインストールします。Firefoxでは、たとえばEdit！Settings！Advanced！Certificatesを使用して、最初のタブ「Your certificates」で名前（CN）CAcert WoT Userを持つインストール済みの証明書を見つけることができます。

これで、CNフィールドに自分の名前が入った個人のX.509証明書を発行できます。これを行うには、CACert Web of Trustの他のメンバーによって認証されたCAcertアカウントが必要です。このような確認の取得に関する情報は、CAcertのインターネットページにあります。

次に、個人のX.509証明書のバックアップコピーを保存します。末尾の.p12 が自動的にバックアップコピーに適用されます。

注意：この.p12 ファイルには、公開鍵と秘密鍵が含まれています。このファイルが不正アクセスから保護されていることを確認してください。

個人のX.509証明書をKleopatraにインポートする方法については、第19章を参照してください。

次のページのセクション7.3を見てみましょう。ここでも、OpenPGPとX.509の説明が同じになります。

55

Gpg4win Compendium 3.0.0

第7章証明書の作成

**7.3。証明書作成プロセスが完了しました**

これで、OpenPGPまたはX.509キーペアの作成が完了しました。これで、独自の電子キーが手に入りました。

この概要の説明では、サンプルとしてOpenPGP証明書を常に使用しますが、すべての情報はX509証明書にも適用されます。

クレオパトラのメインウィンドウに戻ります。作成されたばかりのOpenPGP証明書は、[証明書]タブの証明書管理にあります。

56

Gpg4win Compendium 3.0.0

第7章証明書の作成

新しい証明書をダブルクリックして、証明書に関連するすべての詳細を表示します。

証明書の詳細はどういう意味ですか？

証明書は無期限に有効です。つまり、「組み込みの有効期限」はありません。有効期限を後で変更するには、[有効期限の変更]をクリックします。

証明書の詳細については、第15章を参照してください。

57

**8.公開証明書の配布**

Gpg4winを日常的に使用する場合、署名を暗号化およびチェックする目的で、公開鍵のみを含む「公開」証明書を常に処理することが非常に実用的です。自分の秘密鍵とそれを保護するパスフレーズが安全である限り、あなたはすでに秘密を確実にするための長い道のりを進んでいます。

誰もがあなたの公開証明書を持つことができ、持つべきであり、あなたはあなたの通信パートナーの公開証明書を持つことができて、持つべきです–多いほど良いです。

なぜなら：

安全な電子メールを交換するには、両方のパートナーが相手の公開証明書を所有して使用する必要があります。もちろん、受信者には、Kleopatra認定管理を備えたGpg4winソフトウェアパッケージなど、証明書を処理できるプログラムも必要です。

したがって、暗号化された電子メールを誰かに送信する場合は、電子メールを暗号化するための公開証明書が必要です。

一方、誰かが暗号化された電子メールを送信したい場合、その人はあなたの公開証明書を持っていて、それを暗号化目的で使用する必要があります。

このため、公開証明書へのアクセスを許可する必要があります。

何人の相手とやり取りするか、またどの証明書形式を使用するかに応じて、いくつかのオプションがあります。たとえば、公開証明書を配布できます...

...特定の通信パートナーに電子メールで直接–セクション8.1を参照してください。

... OpenPGP証明書サーバー（OpenPGPにのみ適用）–セクション8.2を参照してください。...自分のホームページから。

... USBスティックなどで直接使用します。

次のページの最初の2つのバリアントを見てみましょう。

58

Gpg4win Compendium 3.0.0

第8章公開証明書の配布

**8.1。電子メールごとの公開、OpenPGPの練習**

通信相手に公開証明書にアクセスできるようにしますか？エクスポートしたパブリック証明書を電子メールで送信するだけです。このセクションでは、これがどのように機能するかを示します。

公開OpenPGP証明書を使用してこのプロセスを練習してください！アデルがお手伝いします。次の演習はOpenPGPにのみ適用されます。公開X.509証明書の公開については、67ページを参照してください。

Adeleは、通信の練習に使用できる非常に優れた電子メールロボットです。Adeleが機能していない可能性があることに注意してください。アデルが答えていなくても心配する必要はありません。通常、ソフトウェアではなくスマートな人間とやり取りする方が楽しいので、人間を使って練習する方がよいでしょう（結局のところ、これがアデルです）。このようにアデルを想像することができます：

まず、Adeleに公開OpenPGP証明書を送信します。この証明書の公開鍵を使用して、Adeleは暗号化された電子メールを送信します。

次に、独自の秘密鍵を使用して、Adeleの応答を復号化します。暗号化された電子メールでAdeleに返信できるようにするために、Adeleは自分の公開証明書を添付しています。

アデルは、あなたが対応している本物の人間のように振る舞います。もちろん、アデルの電子メールはあなたが実際に通信している人々からの電子メールほど興味深いものではありません。一方、Adeleを使用して好きなだけ練習することができます。実際の人は、しばらくすると面倒になるでしょう。

そこで、公開OpenPGP証明書をエクスポートし、電子メールでAdeleに送信します。次のページでは、これがどのように機能するかを示します。

59

Gpg4win Compendium 3.0.0

第8章公開証明書の配布

**公開OpenPGP証明書のエクスポート**

Kleopatraでエクスポートする公開証明書を選択し（証明書のリストの対応する行をクリックして）、メニューの[ファイル！証明書のエクスポート...]をクリックします。PC上の適切なファイルフォルダーを選択し、公開証明書をファイルタイプ.asc で保存します（例：mein-OpenPGP-Zertifikat.asc）。選択可能な他のファイルタイプ.gpg または.pgpは、証明書をバイナリ形式で保存します。つまり、.asc ファイルとは異なり、テキストエディターで読み取ることができません。

メニュー項目を選択するときは、公開証明書のみをエクスポートしていることを確認してください。誤って、関連付けられている秘密鍵を持つ鍵ペア全体の証明書はエクスポートしないでください。

Windowsエクスプローラを選択し、エクスポート用に指定したのと同じフォルダを選択して、ファイルをもう一度確認します。

次に、エクスポートされた証明書ファイルをワードパッドなどのテキストエディターで開きます。テキストエディターは、公開OpenPGP証明書を実際のように表示します。これは、テキストと数字のかなりわかりにくいブロックです。

60

Gpg4win Compendium 3.0.0

第8章公開証明書の配布

OpenPGP証明書を電子メールで公開する場合、電子メールプログラムが添付ファイルを送信できるかどうかを考慮できる2つのバリアントがあります。

**バリエーション1：公開OpenPGP証明書を電子メールテキストとして送信する**

このオプションは、ファイルを添付できない場合でも常に機能します。Web上の一部の電子メールサービスの場合と同様です。

また、公開証明書を初めて確認し、その背後にあるもの、および証明書が実際に何で構成されているかを正確に知る方法でもあります。

からテキストエディタでパブリック証明書全体を強調表示します

--- PGP公開キーブロックの開始---

まで

--- PGP公開キーブロックの終了---

メニューコマンドまたはキーショートカットCtrl + C でコピーします。これで、コンピューターのメモリ（Windowsコンテキストのクリップボード）に証明書がコピーされました。

これで、電子メールプログラムを開始できます（どちらを使用してもかまいません）。公開証明書を空の電子メールに追加します。Windowsでは、追加（「貼り付け」）のキーコマンドはCtrl + V です。このプロセス–コピーと貼り付け–を「コピーと貼り付け」としてご存知でしょう。

電子メールプログラムは、HTML形式のメッセージではなく、テキストメッセージのみを送信できるように設定する必要があります（セクション13.3および付録Aを参照）。

次に、この電子メールのアドレスをadele@gnupp.deに送信し、件名に何かを入力します（たとえば、私の公開OpenPGP証明書）。

61

Gpg4win Compendium 3.0.0

第8章公開証明書の配布

これはおおよその電子メールの内容です。

次に、電子メールをAdeleに送信します。必ず送信者として自分の電子メールアドレスを含めてください。そうしないと、アデルの応答を受け取ることはありません...

62

Gpg4win Compendium 3.0.0

第8章公開証明書の配布

**バリエーション2：パブリックOpenPGP証明書を電子メールの添付ファイルとして送信する**

Variant 1の代わりに、エクスポートした公開OpenPGP証明書を電子メールの添付ファイルとして直接送信することもできます。これは多くの場合、より単純で一般的に使用される方法です。上記では、「コピーして貼り付ける」方法について学びました。これは、透明性が高く、理解しやすいためです。

次に、別の電子メールをAdeleに書き込みます。今回は、添付ファイルに証明書ファイルを含めます。

以前にエクスポートした証明書ファイルを、他のファイルの場合と同じように（たとえば、空の電子メールウィンドウにプルするなど）、新しい電子メールに添付ファイルとして追加します。受信者（adele@gnupp.de ）と件名を追加します。例：公開OpenPGP証明書-添付ファイルとして。

もちろん、いくつかの説明文を追加することもできます。ただし、アデルはこのプロセスの練習を支援することだけを目的としているため、この説明は必要ありません。

完成した電子メールは次のようになります。

次に、電子メールと添付ファイルをAdeleに送信します。

63

Gpg4win Compendium 3.0.0

第8章公開証明書の配布

**要するに：**

Kleopatraの公開OpenPGP証明書をファイルにエクスポートしました。その後、ファイルの内容を直接電子メールにコピーし、完全なファイルを電子メールの添付ファイルとして添付しました。どちらの電子メールも他の誰か（この場合はAdele）に送信されています。

公開証明書を実際の電子メールアドレスに送信する場合も、同じプロセスが適用されます。通常、バリアント2で説明されているように、パブリック証明書を添付ファイルとして送信する必要があります。これは、あなたと受信者の両方にとって、最も簡単な方法です。また、受信者が証明書ファイルを自分の証明書管理（Kleopatraなど）に直接インポートできるという利点もあります。

64

Gpg4win Compendium 3.0.0

第8章公開証明書の配布

**8.2。OpenPGP証明書サーバー経由で公開**

注意：OpenPGP証明書は、OpenPGP証明書サーバー経由でのみ配布できます。

数人だけで暗号化された電子メールを交換する場合でも、公開OpenPGP証明書を公開証明書サーバーで公開することは常に良い考えです。これにより、インターネットサーバー上のすべてのユーザーがパブリック証明書にアクセスできるようになります。これにより、対応しているすべての人に証明書の電子メールを送信する必要がなくなり、時間を節約できます。

同時に、証明書サーバーで電子メールアドレスを公開すると、電子メールアドレスがスパムの影響を受けやすくなります。これは、優れたスパム保護でのみ対処できます。

これがどのように機能するかです。Kleopatraで公開OpenPGP証明書を選択し、File！Export server to server ...をクリックします。証明書サーバーを定義していない場合は、警告が表示されます。

公開OpenPGP証明書サーバーには、keys.gnupg.netのデフォルト設定がすでに含まれています。クリック

[ 続行]選択した公開証明書をこのサーバーに送信します。そこで、あなたの公開証明書は、グローバルに接続されたすべての証明書サーバーに配布されます。誰でもこれらのOpenPGP証明書サーバーの1つから公開証明書をダウンロードし、それを使用して安全な電子メールを送信できます。

このプロセスのみをテストする場合は、練習証明書を送信しないでください。上部のダイアログで、[キャンセル]をクリックします。テスト証明書は価値がなく、証明書サーバーによって削除できません。「Julius Caesar」、「Helmut Kohl」、「Bill Clinton」などの名前のテスト証明書がこれらのサーバー上にすでにいくつも存在しているとは思わないでしょう...

65

Gpg4win Compendium 3.0.0

第8章公開証明書の配布

**要するに：**

これで、インターネット上のOpenPGP証明書サーバーで公開OpenPGP証明書を公開する方法がわかりました。

証明書サーバー上で対応している人々の公開OpenPGP証明書を検索する方法については、第16章を参照してください。この機能は、この機能が必要になったときに、後で読むこともできます。

66

Gpg4win Compendium 3.0.0

第8章公開証明書の配布

**8.3。X.509証明書の公開**

パブリックX.509証明書の場合、このプロセスはさらに簡単です。署名するS / MIME電子メールを、対応する相手に送信するだけです。公開X.509証明書はこの署名に含まれており、受信者の証明書管理にインポートできます。

残念ながら、ロボットはOpenPGPしかサポートしていないため、Adeleを使用してX.509証明書を練習することはできません。したがって、あなたはあなたを書くために別の人を選ぶか、あるいは自分自身に書くべきです。

一部の公開X.509証明書は、認証局によって配布されます。これは通常、X.509証明書サーバーを使用して行われますが、OpenPGPキーサーバーの場合のように、グローバルベースでは同期されません。

パブリックX.509証明書をエクスポートする場合、パブリック証明書チェーン全体を強調表示して、ファイル（通常はルート証明書、CA証明書、個人証明書）またはパブリック証明書のみに保存できます。

あなたが対応している人がチェーンの一部を欠落している可能性があるため、最初の方が推奨されます。これを行うには、Shiftキーを押しながらKleopatraで証明書チェーンのすべての要素をクリックし、強調表示された証明書をファイルにエクスポートします。

あなたが対応している人がルート証明書を持っていない場合は、最終的にあなたも信頼するために、その人がルート証明書を信頼していることを示すか、管理者にそれを依頼する必要があります。これが既に行われている場合（たとえば、両方が同じ「ルート」の一部であるため）、このshiopはすでに配置されています。

67

1. **電子メールの解読、OpenPGPの練習**

Gpg4win、キーペアの証明書、そしてもちろんパスフレーズだけで、電子メールを復号化できます。

この章では、Gpg4winプログラムコンポーネントGpgOLを使用してMicrosoft Outlookで電子メールを復号化する方法をステップごとに示します。

最初は、Adeleと公開OpenPGP証明書を使用してこのプロセスを練習できます。次の演習は、OpenPGPにのみ適用されます。S/ MIME電子メールの復号化に関する説明は、この章の最後の71ページにあります。

セクション8.1では、公開OpenPGP証明書をAdeleに送信しました。この証明書を使用して、Adeleは電子メールを暗号化し、メッセージを送信します。しばらくすると、Adeleの応答が届きます。

68

Gpg4win Compendium 3.0.0

第9章電子メールの解読、OpenPGPのための練習

**MS OutlookとGpgOLを使用したメッセージの復号化**

ほとんどの電子メールプログラムには、特別なプログラム拡張機能（「プラグイン」）があり、電子メールプログラムで直接暗号化および復号化プロセスを実行するために使用できます。GpgOLは、MS Outlook用のこのようなプログラム拡張機能で、Adeleのメールを復号化するためにここで使用されます。他のソフトウェアソリューションの詳細については、付録Bを参照してください。このセクションは、今すぐ読むことも、後でこの機能が必要になったときに読むこともできます。

MS Outlookを起動し、Adeleの返信メールを開きます。これまで、証明書管理プログラムとして知られているのはクレオパトラだけでした。ただし、プログラムはそれ以上のことができます。実際のGnuPG暗号化ソフトウェアを制御できるため、証明書を管理するだけでなく、すべての暗号化タスクを（GnuPGの支援を得て）処理できます。Kleopatraは視覚的なユーザーインターフェイスを提供します。そのため、電子メールの暗号化または復号化中にユーザーが見るダイアログが表示されます。

したがって、KleopatraはAdeleの暗号化された電子メールを処理します。これらの電子メールは、公開OpenPGPキーを使用してAdeleによって暗号化されています。

メッセージを復号化するために、Kleopatraは秘密鍵を保護するパスフレーズを要求します。

パスフレーズを入力します。

エラーダイアログが表示されなければ、復号化は成功です。これで、復号化された電子メールを読むことができます。

開いたメールのメニューでExtras！GpgOLの解読/チェックをクリックすると、復号化の正確な結果ダイアログを取得できます。

ただし、確かに結果、つまり復号化されたメッセージも確認したいのですが...

69

Gpg4win Compendium 3.0.0

第9章電子メールの解読、OpenPGPのための練習

**復号化されたメッセージ**

Adeleの復号化された応答は次のようになります1：

こんにちはハインリッヒハイネ、

ここにあなたの電子メールへの暗号化された応答があります。

キーID FE7EEC85C93D94BAおよび名前「Heinrich Heine <heinrich@gpg4win.de>」の公開鍵を受け取りました。

添付されているのは、フレンドリーな電子メールロボットであるadele@gnupp.deの公開鍵です。

よろしく、

adele@gnupp.de

次のテキストブロックは、Adeleの公開証明書です。

次の章では、この証明書をインポートして、証明書管理に追加します。インポートされた公開証明書をいつでも使用して、対応している相手へのメッセージを暗号化したり、署名された電子メールを確認したりできます。

1Adeleのソフトウェアバージョンによっては、外観が異なる場合があります。ドイツ語から翻訳されています。

70

Gpg4win Compendium 3.0.0

第9章電子メールの解読、OpenPGPのための練習

**要するに：**

1. 秘密鍵を使用して電子メールを復号化および暗号化しました。

1. 通信パートナーが独自の公開証明書を添付しているため、暗号化された形式で回答できます。

**S / MIMEを使用した電子メールの復号化**

これが、OpenPGP秘密鍵を使用して電子メールを復号化する方法です–しかし、S / MIMEでどのように機能しますか？

答え：同じです！

暗号化されたS / MIME電子メールを解読するには、Outlookでメッセージを開き、ピン入力ダイアログにパスフレーズを入力します。OpenPGPの場合と同様のステータスダイアログが表示されます。このダイアログを閉じると、復号化されたS / MIME電子メールが表示されます。

ただし、OpenPGP復号化とは異なり、S / MIMEを使用する場合、AdeleはOpenPGPしかサポートしていないため、Adeleを使用して練習することはできません。

71

**10.公開証明書のインポート**

あなたが対応している人は、署名された電子メールをあなたに送信するときに、必ずしも彼らの公開証明書を送信する必要はありません。パブリック証明書を証明書管理者（Kleopatraなど）に保存するだけです。

**公開証明書の保管**

公開証明書をKleopatraにインポートする前に、ファイルに保存する必要があります。証明書を電子メールファイルの添付ファイルとして受信したか、電子メールに含まれるテキストブロックとして受信したかに応じて、次の手順を実行してください。

パブリック証明書が電子メールの添付ファイルとして含まれていた場合は、通常どおりにハードドライブに保存します。

公開証明書が電子メールに含まれているテキストのブロックとして郵送された場合は、証明書全体を強調表示する必要があります。

（公開）OpenPGP証明書の場合は、

--- PGP公開キーブロックの開始---

まで

--- PGP公開キーブロックの終了---

セクション8.1で確認したとおりです。

次に、コピーと貼り付けを使用して、強調表示されたセクションをテキストエディターに挿入し、公開証明書を保存します。ファイル終末について、あなたは使用する必要があります.ASC または.gpg のOpenPGP証明書とのための.pem または.derのX.509証明書。

72

Gpg4win Compendium 3.0.0

第10章公開証明書のインポート

**Kleopatraへの公開証明書のインポート**

公開証明書を電子メールの添付ファイルまたはテキストブロックとして保存したかどうかにかかわらず、どちらの場合も、それをKleopatra証明書管理にインポートします。これを行うには、プログラムがまだ実行されていない場合にKleopatraを起動します。メニューで、File！Import certificate ...をクリックし、保存したパブリック証明書を検索してインポートします。インポートプロセスの結果を示す情報ダイアログが表示されます。

インポートされたパブリック証明書が、Kleopatraの別のタブに表示されます。<証明書ファイルへのパス>というタイトルのインポートされた証明書が表示されます。

ファイルには複数の証明書を含めることができるため、このタブはチェックの目的で使用されます。Fenster！Close tabコマンドを使用するか、ウィンドウの右側にある[Close tab]ボタンを使用して、タブを閉じることができます。

次に、「その他の証明書」タブに切り替えます。インポートした公開証明書も表示できるはずです。

これで、他の誰かの証明書（この場合はAdeleの公開OpenPGP証明書）が証明書管理にインポートされました。いつでもこの証明書を使用して、暗号化されたメッセージを証明書の所有者に送信し、その所有者の署名を確認できます。

73

Gpg4win Compendium 3.0.0

第10章公開証明書のインポート

暗号化された電子メールをより頻繁に、より多くの人と交換するようになったら、グローバルに利用可能なキーサーバーで証明書を検索してインポートすることをお勧めします。この仕組みについては、第16章を参照してください。

**続行する前に、重要な質問：**

公開されているOpenPGP証明書が実際にAdeleからのものであることをどのようにして知っていますか？他の誰かの名前で電子メールを送信することは可能です–この点で、送信者の名前を持っているだけでは何の意味もありません。

それでは、公開証明書が実際に送信者のものであることをどのように確認できますか？

証明書検査に関連するこの重要な質問については、次の第11章で説明します。

74

**11.証明書の検査**

証明書が実際に送信者に属しているかどうかはどのようにしてわかりますか？逆もまた同様です–あなたが書いている人が、あなたが彼に送った証明書が本当にあなたのものであると信じる必要があるのですか？電子メールの送信者の名前は、送信者の名前を封筒に入れるのと同じです。

銀行があなたの名前の付いた電子メールを受け取り、銀行の残高全体をバハマの番号付きアカウントに転送するように要求された場合、電子メールアドレスが何であっても拒否することを希望する必要があります。それ自体では、電子メールアドレス自体は送信者のIDについて実際には何も言いません。

75

Gpg4win Compendium 3.0.0

第11章証明書の検査

**指紋**

非常に小さな人々の輪にのみ対応している場合、彼らの身元を確認するのは簡単です。他の証明書のフィンガープリントを確認します。

各証明書には固有のIDがあり、誰かの指紋よりも優れています。このため、この識別は「フィンガープリント」とも呼ばれます。

証明書の詳細をクレオパトラで表示する場合、たとえば証明書をダブルクリックすると、とりわけ40文字のフィンガープリントが表示されます。

したがって、上記のOpenPGP証明書のフィンガープリントは次のとおりです。

7EDC0D141A82250847448E91FE7EEC85C93D94BA

要するに-フィンガープリントは証明書とその所有者を明確に識別します。

単にあなたが対応している人に電話して、彼らにあなたに彼らの証明書の指紋を読み取らせてください。情報が手元にある証明書と一致する場合、明らかに正しい証明書を持っています。

もちろん、証明書の所有者に直接会うことも、別の方法を使用して証明書と所有者を一致させることもできます。多くの場合、指紋は名刺にも印刷されます。したがって、信頼性が保証されている名刺があれば、電話を節約できます。

76

Gpg4win Compendium 3.0.0

第11章証明書の検査

**OpenPGP証明書の認証**

「フィンガープリントを介して」証明書の信頼性の確認を取得すると、OpenPGPでのみ認証できます。X.509では、ユーザーは証明書を認証できません。これは認証局（CA）のみが実行できます。

証明書を認証することで、他の（Gpg4win）ユーザーに、この証明書が本物であるという意見を持っていることを知らせます–したがって、本物です：あなたはこの証明書の一種の「ゴッドファーザー」として機能しており、一般的なレベルを上げるのに役立ちますその信憑性への信頼の。

では、認証プロセスはどのように機能しますか？

Kleopatraで、本物であり、認証を希望するOpenPGP証明書を選択します。の中に

メニューから次を選択します：証明書！証明書の認証...

[次へ]を使用して、次のダイアログで認証するOpenPGP証明書を再確認します。

77

Gpg4win Compendium 3.0.0

第11章証明書の検査

次のステップで、独自のOpenPGP証明書を選択します。これを使用して、前のステップで選択した証明書を認証します。

ここでは、[個人使用のみを認証する]または[認証してすべてのユーザーに表示する]を決定します。最後のバリアントでは、認証済みの証明書をOpenPGP証明書サーバーにアップロードして、更新された認証済みの証明書を世界中で利用できるようにするオプションがあります。

[認証]で選択を確認します。

電子メールに署名するプロセスと同様に、証明書を（秘密キーで）認証するときにもパスフレーズを入力する必要があります。認証プロセスは、この情報が正しく入力されて初めて完了します。

78

Gpg4win Compendium 3.0.0

第11章証明書の検査

認証が成功すると、次のウィンドウが表示されます。

認証をもう一度確認しますか？これを行うには、認証したばかりの証明書の証明書の詳細を開きます。[ユーザーIDと認証]タブを選択し、[認証の取得]ボタンをクリックします。

この証明書に含まれるすべての認証が、ユーザーIDでソートされて表示されます。認証したばかりの場合は、このリストに証明書が表示されるはずです。

79

Gpg4win Compendium 3.0.0

第11章証明書の検査

**信頼の網**

証明書を認証するプロセスは、Gpg4winユーザーのグループとその対応を超えて広がる「Web of Trust」（WoT）を作成します。つまり、OpenPGP証明書の認証を常に確認する必要はありません。

当然、多くの人に認証されれば、証明書の信頼性は高まります。独自のOpenPGP証明書は、時間の経過とともに他のGnuPGユーザーから認証を受け取ります。これにより、ますます多くの人々がこの証明書が本当にあなたのものであり、他の誰かのものではないと信頼することができます。

この「Web of Trust」の継続的な製織により、柔軟な認証構造が作成されます。

この証明書のテストを無効にする理論的な可能性が1つあります。誰かが間違った証明書をあなたに植え付けます。言い換えれば、あなたはXから来たふりをしているOpenPGP公開鍵を持っていますが、実際には置き換えられましたか？Y.この偽造された証明書が認証された場合、「Web of Trust」に明らかに問題が生じます。このため、証明書を認証する前に、証明書がその所有者であると主張する人物に本当に属していることを確実に確認することが非常に重要です。

しかし、銀行や政府当局が顧客の証明書が本物かどうかを確認したい場合はどうでしょうか。確かに、彼らはそれらすべてを呼ぶことはできません...

80

Gpg4win Compendium 3.0.0

第11章証明書の検査

**認証インスタンス**

この場合、すべてのユーザーが信頼できる「上位の」インスタンスが必要です。結局のところ、市町村役場に電話をかけて自分が知らない人物のIDを個人的にチェックするのではなく、IDを発行したオフィスがこれらの詳細をすでにチェックして認証していることを信頼します。

これらのタイプの認証インスタンスは、OpenPGP証明書の場合にも存在します。たとえばドイツでは、多くの大学がそうであるように、雑誌c 'はそのようなサービスを長い間無料で提供していませんでした。

したがって、そのような認証インスタンスによって信頼性が確認されたOpenPGP証明書を受け取った場合は、それを信頼できるはずです。

そのような認証インスタンスまたは「トラストセンター」は、S / MIMEなどの他の暗号化方式でも提供されます。ただし、これらは「Web of Trust」とは異なり、追加の「サブインスタンス」を認証し、ユーザー証明書を認証する資格を与える「トップ認証インスタンス」を備えた階層構造を備えています（第5章を参照）。

このインフラストラクチャを説明する最良の方法は、シールの例を使用することです。ナンバープレートのステッカーは、そのようなステッカーの発行を許可された機関によってのみ提供され、他の上位機関からその権利を受け取っています。技術的なレベルでは、認証は、認証者が証明書に署名することに他なりません。

もちろん、階層型認証インフラストラクチャは、相互信頼に基づいているGnuPGの緩やかな「Web ofTrust」よりも、政府および公式のインスタンスの要件にはるかに適しています。同時に、認証の主要な側面はどちらも同じです。Gpg4winは、「Web of Trust」（OpenPGP）に加えて、階層認証（S / MIME）もサポートしています。したがって、Gpg4winは、ドイツ連邦共和国の署名法に対応する基準を提供します。

このトピックについて詳しく知りたい場合は、以下のWebサイトで、このトピックおよびその他のITセキュリティトピックに関する詳細情報を提供しています。

[www.bsi.de](https://translate.google.com/translate?hl=ja&prev=_t&sl=auto&tl=ja&u=http://www.bsi.de)

[www.bsi-fuer-buerger.de](https://translate.google.com/translate?hl=ja&prev=_t&sl=auto&tl=ja&u=http://www.bsi-fuer-buerger.de)[www.gpg4win.org](https://translate.google.com/translate?hl=ja&prev=_t&sl=auto&tl=ja&u=http://www.gpg4win.org)

認証インフラストラクチャの問題に関するもう1つのかなり技術的な情報源はGnuPGハンドブックです。これは次の場所にもあります。

[www.gnupg.org/gph/en/manual.html](https://translate.google.com/translate?hl=ja&prev=_t&sl=auto&tl=ja&u=http://www.gnupg.org/gph/en/manual.html)

81

**12.電子メールの暗号化**

今、再びエキサイティングになっています。暗号化された電子メールを送信しています。

この場合、Outlook（または暗号化をサポートする別の電子メールプログラム）、Kleopatra、そしてもちろん通信相手の公開証明書が必要です。

OpenPGPに関する注意：

Adeleを使用して、OpenPGPで暗号化プロセスを練習できます。一方、AdeleはS / MIMEをサポートしていません。暗号化する電子メールをadele@gnupp.deに送信できます。Adeleはメッセージを読み取ることができないため、メッセージに何を書き込んでもかまいません。

S / MIMIEに関する注意：

Gpg4winのインストール後、S / MIME機能はGpgOLですでにアクティブになっています。Outlook独自のS / MIME機能を使用するなど、S / MIMEを（GnuPGで）オフにする場合は、次のGpgOLオプションダイアログのExtras！Options！GpgOLにあるオプションS / MIMEサポートをアクティブにするを無効にする必要があります。

82

Gpg4win Compendium 3.0.0

第12章電子メールの暗号化

**暗号化されたメッセージを送信する**

最初に、Outlookで新規作成し、それをあなたが書いている人に宛ててください。

暗号化された形式でメッセージを送信するには、メッセージウィンドウのメニューで[Extras！Encrypt message]を選択します。ツールバーのロックアイコンが付いたボタンがアクティブになります。ロックを右クリックすることもできます。

Outlookメッセージウィンドウは次のようになります。

次に[送信]をクリックします。

Gpg4winは、対応する人から提供された公開証明書のプロトコル（OpenPGPまたはS / MIME）を自動的に検出します。

受信者の電子メールアドレスと一致する証明書が1つしかない限り、メッセージは暗号化されて送信されます。

83

Gpg4win Compendium 3.0.0

第12章電子メールの暗号化

**証明書の選択**

Kleopatraがle-mailアドレスを使用して受信者の証明書を明確に判別できない場合、たとえば、対応する人物からのOpenPGPおよびS / MIME証明書がある場合、正しい証明書を選択できる選択ダイアログが表示されます表示されます。

Kleopatraがあなたが対応している人の公開証明書を見つけることができない場合、おそらくそれをまだ証明書管理にインポートしていない（第10章を参照）か、おそらくまだ認証していない（OpenPGPの場合;第11章を参照）、または、証明書チェーンのルート証明書に対する信頼を表明していません（S / MIMEについては、22.7章を参照）。

メッセージを暗号化するには、通信パートナーの正しい公開証明書が必要です。

第3章の原則を思い出してください。

暗号化された電子メールを送信するには、誰かの公開証明書を使用する必要があります。

84

Gpg4win Compendium 3.0.0

第12章電子メールの暗号化

**暗号化プロセスを完了する**

メッセージが正常に暗号化されて送信されると、確認メッセージが表示されます。

おめでとう！最初のメールを暗号化しました！

85

**13.メールに署名する**

第11章では、公開OpenPGP証明書の信頼性を確認し、独自の秘密OpenPGP鍵で署名する方法について詳しく学びました。

この章では、証明書だけでなく、完全な電子メールに署名する方法についても説明します。これは、電子署名の形式である電子メールにデジタル署名を適用することを意味します。

この方法で「封印」すると、テキストは誰でも読むことができますが、受信者は配信中に電子メールが操作または変更されたかどうかを確認できます。署名は、メッセージが本当にあなたからのものであることを受信者に知らせます。そして：（何らかの理由で）公開証明書を持っていない誰かと連絡を取り合っている場合は、少なくとも自分の秘密鍵でメッセージを「封印」できます。

このデジタル署名は、電子メールの「署名」と同じではないことに気づいたと思います。電子メールの末尾に含まれている場合があり、電話番号、住所、ウェブサイトなどの項目が含まれています。これらの電子メール署名は単に名刺の一種として機能しますが、デジタル署名は電子メールを操作から保護し、送信者を明確に確認します。

さらに、デジタル署名は、署名法（2001年5月22日）の一部として施行されたため、適格な電子署名と比較することはできません。ただし、プライベートまたはプロの電子メール通信とまったく同じ目的を果たします。

86

Gpg4win Compendium 3.0.0

第13章メールに署名する

**13.1。GpgOLでの署名**

実際、電子メールへの署名は、暗号化よりも簡単です（第12章を参照）。新しい電子メールを作成したら、暗号化プロセスと同様に、次の手順を実行します。

署名付きメッセージを送信証明書を選択

署名プロセスを完了する

これらの手順については、次のページで詳しく説明します。

**署名されたメッセージを送信する**

最初に、Outlookで新しい電子メールを作成し、宛先の宛先に送信します。

メッセージを送信する前に、メッセージに署名を付けて送信するようにシステムに通知します。これを行うには、署名ペンでボタンをアクティブにするか、メニュー項目Format！Signメッセージを有効にします。

電子メールウィンドウは次のようになります。

[送信]をクリックします。

87

Gpg4win Compendium 3.0.0

第13章メールに署名する

**証明書の選択**

電子メールを暗号化する場合と同様に、Gpg4winは、OpenPGPまたはS / MIMEのプロトコルを自動的に検出します。OpenPGPまたはS / MIMEについては、独自の証明書（署名用の秘密鍵を含む）を使用できます。

同じ電子メールアドレスを持つ独自のOpenPGPおよびS / MIME証明書がある場合、Kleopatraは電子メールに署名する前にプロトコルを選択するように求めます。

選択したメソッドに複数の証明書（たとえば、同じ電子メールアドレスの2つのOpenPGP証明書）がある場合、Kleopatraは、証明書（ここではOpenPGP）を表示するウィンドウを開き、それぞれに独自の秘密鍵があります。

[OK]で選択を確認します。

88

Gpg4win Compendium 3.0.0

第13章メールに署名する

**署名プロセスを完了する**

電子メールの署名プロセスを完了するために、次のピン入力ウィンドウで秘密のパスフレーズを入力するよう求められます。

これは次の理由で必要です。

自分の秘密鍵でのみ署名できます。

あなた自身の秘密鍵だけがあなたの身元を確認するので、それは理にかなっています。あなたが対応している人は、あなたがすでに持っているか、または取得できる公開証明書を使用して、自分の身元を確認できます。秘密鍵のみが公開証明書と一致するためです。

[OK]でパスフレーズのエントリを確認します。メッセージが署名され、送信されました。

メッセージが正常に署名されると、次のダイアログが表示されます。

89

Gpg4win Compendium 3.0.0

第13章メールに署名する

おめでとう！最初のメールを暗号化しました！

90

Gpg4win Compendium 3.0.0

第13章メールに署名する

**要するに：**

秘密鍵を含む独自の証明書を使用して電子メールに署名する方法を学びました。

あなたは、あなたが書いている人の公開証明書を使って電子メールを暗号化する方法を知っています。

これで、セキュリティで保護された電子メールを送信するための2つの最も重要な手法である暗号化と署名について理解できました。

もちろん、2つの手法を組み合わせることもできます。今後は、電子メールを送信するたびに、電子メールの重要性と必要な保護レベルに応じて、送信方法を検討してください。

暗号化されていない暗号化

署名した

署名および暗号化（これについては、セクション13.4で詳しく説明します）

これら4つの組み合わせは、OpenPGPまたはS / MIMEのいずれかで使用できます。

91

Gpg4win Compendium 3.0.0

第13章メールに署名する

**13.2。GpgOLで署名を確認する**

あなたが対応している人から署名された電子メールを受け取ったとしましょう。

このデジタル署名の確認は非常に簡単です。必要なのは、通信パートナーの公開OpenPGPまたはX.509証明書だけです。このチェックを実行する前に、彼の公開証明書を証明書管理にインポートしておく必要があります（第10章を参照）。

署名されたOpenPGPまたはS / MIME電子メールを確認するには、電子メールを復号化する場合と同様に進めます（

第9章）：

Outlookを起動し、署名された電子メールを開きます。

GpgOLは、署名チェックのために電子メールを自動的にKleopatraに転送します。クレオパトラはステータスダイアログで結果を報告します、例えば：

署名チェックが成功しました！署名された電子メールを読むためにダイアログに近づいてください。

手動でもう一度確認する場合は、開いているメールのメニューで[Extras！Decrypt / Check GpgOL]を選択します。

署名チェックが成功しない場合は、配信プロセス中にメッセージが変更されたことを意味します。インターネットの技術的な性質により、送信の欠陥により、電子メールが意図せずに変更された可能性があります。それがおそらく最も可能性の高い原因です。ただし、テキストが意図的に変更されたことも意味します。

セクション13.3には、このような場合の対処方法に関する情報があります。

92

Gpg4win Compendium 3.0.0

第13章メールに署名する

**13.3。署名が壊れた理由**

署名が壊れている理由はいくつかあります。

「署名が不正です」または「チェックに失敗しました」というメッセージが表示された場合は、メールが改ざんされている可能性があることを警告しています。つまり、電子メールの内容または件名が変更された可能性があります。

同時に、署名の破損は、必ずしも電子メールが操作されたことを意味するわけではありません。また、送信不良によりメールが改ざんされた可能性もあります。

いずれの場合も、署名の破損を常に真剣に受け止め、送信者に電子メールの再送信を依頼する必要があります。

「HTML」形式ではなく、「テキスト」形式でのみ電子メールを送信するようにプログラムを設定することをお勧めします。ただし、署名または暗号化された電子メールにHTMLを使用する場合、受信者に到達するまでにフォーマット情報が失われ、署名が壊れる可能性があります。

Outlook 2003および2007では、メッセージ形式を[Extras！Options！E-Mail Format]でのみ[Text]に設定できます。

93

Gpg4win Compendium 3.0.0

第13章メールに署名する

**13.4。暗号化と署名**

メッセージは通常、通信パートナーの公開証明書を使用して暗号化されます。通信パートナーは、秘密鍵を使用して電子メールを復号化します。

逆の可能性-秘密鍵による暗号化-は全世界が関連する公開証明書を知っており、メッセージを復号化できるため、意味がありません。

ただし、この章ですでに説明したように、秘密鍵を使用してファイルを作成する別の方法、つまり署名があります。

デジタル署名によって作成者が確認されます。誰かがあなたの公開証明書をこのファイル（署名）に正常に適用した場合、このファイルは秘密鍵によってのみ暗号化された可能性があるためです。そして、あなただけがこのキーにアクセスできます。

両方のオプション、つまり電子メールの暗号化と署名を組み合わせることができます。

1. 自分の秘密鍵でメッセージに署名します。これは、あなたが著者であることを証明します。

1. 次に、通信相手の公開証明書を使用してテキストを暗号化します。

つまり、メッセージには2つのセキュリティ特性があります。

1. メッセージのシール：秘密鍵による署名。

1. 強固な外側の封筒：相手の公開証明書を使用した暗号化。

通信パートナーは、自分の秘密鍵で外側の強力なエンベロープを開きます。このキーだけがテキストのデコードに使用できるため、これにより機密性が保証されます。彼はあなたの公開証明書を使用してシールを読み取ります。これは、あなたが作成者であることを証明します。公開証明書が一致する場合、シール（デジタル署名）は秘密鍵でのみ暗号化できるためです。

考えるとかなりトリッキーですが、とてもシンプルです。

94

**14.暗号化された形式での電子メールのアーカイブ**

重要な（したがって暗号化されている可能性のある）電子メールも1つの方法でアーカイブする必要があります。

暗号化。

もちろん、テキストのクリアテキストバージョンを保存することもできますが、実際には必要ありません。メッセージが秘密であると想定されていた場合は、平文でコンピュータに保存しないでください。したがって、暗号化された送信メールは常に暗号化された形式で保存する必要があります。

あなたはおそらくすでに問題を推測することができます：アーカイブされた（送信された）電子メールを解読するには、受信者の秘密鍵が必要です–持っていないか、持っているでしょう...

じゃあ何をすればいいの？

非常に簡単：自分自身も暗号化します！

メッセージは、書き込み先の実際の人（Adeleなど）に対して一度暗号化され、独自の公開証明書を使用してもう一度暗号化されます。このようにして、後で独自の秘密鍵を使用して電子メールを判読可能にすることができます。

Gpg4winは、暗号化された各メッセージを独自の証明書に自動的に暗号化します。これを行うために、Gpg4winは送信者の電子メールアドレスを使用します。電子メールアドレスに複数の証明書がある場合は、暗号化プロセス中に暗号化する証明書を選択する必要があります。

95

Gpg4win Compendium 3.0.0

第14章暗号化された形式での電子メールのアーカイブ

**要するに：**

1. 相手の公開証明書を使用して電子メールを暗号化し、それを使用して彼に応答しました。

1. Kleopatraはさらに、送信された暗号化された電子メールを独自の公開証明書を使用して暗号化し、メッセージが判読できるようにします。

以上です！この概要の最初の部分の終わりに、Gpg4winに関する多くの入門知識を獲得しました。

無料で安全なメール暗号化の世界へようこそ！

Gpg4winが実際にバックグラウンドでどのように機能するかをさらに理解するには、Gpg4winの概要の2番目の部分を読むことをお勧めします。さらに面白いものが含まれています！

96

**パートII。**

**上級ユーザー向け**

97

**15.証明書の詳細**

第7.3章では、生成した証明書の詳細ダイアログを既に見ました。証明書に関する多くの情報が含まれています。次のセクションでは、OpenPGP証明書とX.509証明書の違いに関する簡単な情報とともに、最も重要なポイントのより詳細な概要を提供します。

ユーザーID

指紋キーID

有効

証明書保有者の信頼（OpenPGPのみ）認証（OpenPGPのみ）

**ユーザーID**は、証明書の作成プロセス中に入力した名前と電子メールアドレスで構成されます。

Heinrich Heine <heinrich@gpg4win.de>

OpenPGP証明書の場合は、Kleopatraを使用して、Certificates！Add user ID ...メニュー項目を使用して、証明書にユーザーIDを追加できます。これは、たとえば、別の電子メールアドレスに同じ証明書を使用する場合に意味があります。

注：Kleopatraでは、OpenPGP証明書のユーザーIDのみを追加できます。X.509は追加できません。

**フィンガープリント**は、複数の証明書を互いに区別するために使用されます。指紋を使用して、グローバルに利用可能なOpenPGP証明書サーバー（鍵サーバー）またはX.509証明書サーバーに格納されている（パブリック）証明書を探すことができます。証明書サーバーの詳細については、次の章を参照してください。

**キーID**は、指紋の最後の8文字で構成され、同じ機能を果たします。一方でより少ない文字は、それが簡単に鍵IDを処理するために作る、彼らはまた、複数のヒット（同じIDを持つ別の証明書）のリスクを高めます。

証明書**の有効性**は、有効期間と有効期限（該当する場合）を示します。

OpenPGP証明書の場合、有効性は通常Indefiniteに設定されます。証明書の詳細で[有効期限の変更]をクリックするか、証明書を選択して、有効期限を変更し、新しい日付を入力して、Kleopatraでこれを変更できます。これは、たとえば、外部の従業員に発行するために、証明書を有効期間限定で宣言できることを意味します。

X.509証明書の有効性は、証明書の発行時に認証局によって定義され、ユーザーが変更することはできません。

98

Gpg4win Compendium 3.0.0

第15章証明書の詳細

**証明書所有者への**信頼は、OpenPGP証明書の所有者が本物（本物）であり、他のOpenPGP証明書も正しく認証するという主観的な信頼を定量化します。証明書の詳細の[証明書の所有者の信頼を変更する]で、またはmenuCertificates！Change trust statusメニュー項目を使用して信頼を設定します。

信頼ステータスは、OpenPGP証明書にのみ関連します。X.509証明書にはそのような方法はありません。

**認証**あなたのOpenPGP証明書のは、これらの証明書の所有者のユーザIDが含まあなたの証明書の信頼性を確信しているので、それを認証しています。証明書の信頼性への信頼は、他のユーザーから受け取る認証の数が増えるほど高くなります。

認証は、OpenPGP証明書にのみ関連します。このタイプの信頼メカニズムは、X.509証明書には存在しません。

Gpg4winを日常的に使用するために必ずしも証明書の詳細を知っている必要はありませんが、新しい証明書を受け取ったり変更したりする場合には、それらが重要になります。

第11章では、他人の証明書を検査および認証する方法と、「Web of Trust」についてすでに学習しました。

99

**16.証明書サーバー**

セクション8.2には、証明書サーバーを使用してパブリック（OpenPGPまたはX.509）証明書を公開する方法に関する多くの情報がすでに記載されています。このセクションでは、証明書サーバーを詳しく見ていき、Kleopatraでそれらを使用する方法を示します。

鍵サーバーは、標準のOpenPGPまたはX.509をサポートするすべてのプログラムで使用できます。Kleopatraは両方のタイプをサポートしているため、OpenPGPとX.509証明書サーバーの両方をサポートしています。

**OpenPGP証明書サーバー**（「キーサーバー」とも呼ばれます）は分散ベースで構成され、グローバルベースで相互に同期します。含まれるOpenPGP証明書の数に関する現在の統計はありません。OpenPGP証明書サーバーのこの共有ネットワークは、可用性を高め、個々のシステム管理者が安全な通信を不可能にする証明書を削除することを防ぎます（「サービス拒否」攻撃）。

**X.509証明書サーバー**は通常、認証局によってLDAPを介して利用可能になり、X.509証明書のディレクトリサービスとして説明されることもあります。

100

Gpg4win Compendium 3.0.0

第16章証明書サーバー

**16.1。鍵サーバー構成**

Kleopatraで設定ダイアログを開きます：

設定 ！クレオパトラを設定...

次に、[新規]ボタンをクリックして、ディレクトリサービスグル​​ープの下に新しい証明書サーバーを設定します。

OpenPGPまたはX.509から選択します。

OpenPGPでは、サーバーアドレスがhkp：//keys.gnupg.net （ポート：11371、プロトコル：hkp）のデフォルトのOpenPGP証明書サーバーがリストに追加されます。このサーバーは変更せずに使用できます。または、次のページで提案されているOpenPGPサーバーアドレスのいずれかを使用できます。

X.509の場合、X.509証明書サーバーの次のデフォルト設定が表示されます（（プロトコル：ldap、

サーバー名：サーバー、サーバーポート：389）。X.509証明書サーバーのサーバー名と基本DNに関する情報を入力し、サーバーポートを確認します。

証明書サーバーでユーザー名とパスワードが必要な場合は、[ユーザー認証が必要]オプションを有効にして、必要な情報を入力します。

以下のスクリーンショットは、構成されたOpenPGP証明書サーバーを示しています。

[OK]を押して設定を確認します。証明書サーバーが正常に構成されました。

証明書サーバーを正しく構成したことを確認するには、サーバーで証明書検索などを開始すると役立ちます（手順については、セクション16.2を参照してください）。

101

Gpg4win Compendium 3.0.0

第16章証明書サーバー

プロキシ設定：ネットワークでプロキシを使用する場合は、ファイルでプロキシを構成する必要があります。

％APPDATA％\ gnupg \ gpg.conf

プロキシを有効にするには、コンテンツを含む新しい行を追加します。

keyserver-options http-proxy = <proxy-adresse>

X.509キーサーバーのシステム全体の構成に関する説明は、セクション22.5にあります。

**OpenPGP証明書サーバーのアドレス**

新しいOpenPGP特性を処理できるのは最新のOpenPGP証明書サーバーのみであるため、最新のOpenPGP証明書サーバーのみを使用することをお勧めします。

以下は、適切に機能する証明書サーバーの選択です。

hkp：//blackhole.pca.dfn.de hkp：//pks.gpg.cz

hkp：//pgp.cns.ualberta.ca hkp：//minsky.surfnet.nl

hkp：//keyserver.ubuntu.com hkp：//keyserver.pramberger.at http://keyserver.pramberger.at http://gpg-keyserver.de

ファイアウォールに問題がある場合は、次のURLで始まる証明書サーバーを試すことをお勧めします。

http：//

アドレスの下の証明書サーバー

hkp：//keys.gnupg.net（Kleopatra事前選択、前のページのスクリーンショットを参照）hkp：//subkeys.pgp.net

これらのサーバーのネットワーク全体の収集ポイントです。具体的なサーバーはランダムに選択されます。

重要：ldap：//keyserver.pgp.com は同期を行うため、証明書サーバーとして使用しないでください。

他のサーバーと統合する（ステータス：2010年5月）。

102

Gpg4win Compendium 3.0.0

第16章証明書サーバー

**16.2。証明書サーバーから証明書を検索してインポートする**

少なくとも1つの証明書サーバーを構成したら、証明書を検索してインポートできます。

これを行うには、Kleopatraで[ファイル]をクリックし、サーバーで証明書を検索します。

証明書所有者の名前、理想的には彼の証明書の電子メールアドレスを入力できる入力フィールドのある検索ダイアログが表示されます。

選択した証明書の詳細を表示するには、[詳細...]ボタンをクリックします。

見つかった証明書の1つをローカル証明書コレクションに追加する場合は、検索結果のリストから証明書を選択して、[インポート]をクリックします。

その後、Kleopatraはインポート結果のダイアログを表示します。[OK]で確定します。

インポートが成功した場合、選択した証明書がKleopatraの証明書管理に表示されます。

**16.3。OpenPGP証明書サーバーに証明書をエクスポートする**

セクション16.1で説明されているようにOpenPGP証明書サーバーを設定している場合、マウスをクリックするだけで世界中の公開OpenPGP証明書が送信されます。

KleopatraでOpenPGP証明書を選択し、メニュー項目[ファイル！サーバーに証明書をエクスポート...]をクリックします。

これらのほとんどすべてがグローバルレベルで同期するため、使用可能なOpenPGP証明書サーバーのいずれかに証明書を送信するだけで済みます。OpenPGP証明書が実際に世界中で利用できるようになるまで1〜2日かかる場合がありますが、その後「グローバル」証明書が作成されます。

最初にOpenPGP証明書サーバーを構成せずに証明書をエクスポートすると、Kleopatraはデフォルトのサーバーhkp：//keys.gnupg.net を提案します。

103

**17.添付ファイルの暗号化**

暗号化された電子メールを送信してファイルを添付する場合は、通常、添付ファイルも暗号化する必要があります。

GnuPGが電子メールプログラムに適切に統合されている場合、添付ファイルは電子メールの実際のテキストと同じように処理する必要があるため、署名、暗号化、またはその両方を行う必要があります。

GpgOLは自動的に添付ファイルの暗号化と署名を想定しています。

電子メールプログラムに統合されていない暗号化ツールの場合は、注意する必要があります。添付ファイルは、暗号化されていない形式で送信されることがよくあります。

そのような場合はどうしますか？簡単：添付ファイルを個別に暗号化してから、電子メールに添付します。

したがって、これは、第18章で説明されているように、単にファイルを暗号化することと同じです。

104

**18.ファイルの署名と暗号化**

Gpg4winを使用して、電子メールだけでなく個々のファイルの署名と暗号化を行うことができます。原理は同じです：

プライベート証明書を使用してファイルに署名し、ファイルが変更されないようにします。

次に、パブリック証明書を使用してファイルを暗号化し、権限のない人に見られないようにします。

GpgEXアプリケーションを使用すると、OpenPGPまたはS / MIMEの両方を使用して、Windowsエクスプローラーからファイルに署名または暗号化できます。この章では、これがどのように機能するかを正確に示します。

電子メールの添付ファイルとしてファイルを送信する場合、たとえば、GpgOLは電子メールと一緒にファイルに署名して暗号化した後、自動的に確認します。他に何もする必要はありません。

105

Gpg4win Compendium 3.0.0

第18章ファイルの署名と暗号化

**18.1。ファイルの署名と確認**

ファイルに署名するときは、主に、ファイルを秘密にしておく（整合性）のではなく、変更されていないことを確認する必要があります。

署名は、WindowsエクスプローラーのコンテキストメニューからGpgEXを使用すると非常に簡単です。1つ以上のファイルまたはフォルダーを選択し、マウスの右キーを使用してコンテキストメニューを選択します。

[署名して暗号化]メニューが表示されます。

106

Gpg4win Compendium 3.0.0

第18章ファイルの署名と暗号化

次のウィンドウで、オプション「署名」を選択します。

必要に応じて、[テキストとして出力]（ASCIIアーマー）オプションを使用することもできます。署名ファイルは、.asc （OpenPGP）または.pem （S / MIME）で終わるファイルを受け取ります。これらのファイルタイプは、任意のテキストエディタで開くことができます。ただし、以前に表示した数字と文字のみが表示されます。

このオプションが選択されていない場合、署名は末尾の.sig （OpenPGP）または.p7s （S / MIME）で作成されます。これらのファイルはバイナリファイルであり、テキストエディタで表示することはできません。

次に、[次へ]をクリックします。

107

Gpg4win Compendium 3.0.0

第18章ファイルの署名と暗号化

次のダイアログで（デフォルトで選択されていない場合）、ファイルに署名するプライベート（OpenPGPまたはS / MIME）証明書を選択します。

[記号]で選択を確認します。

ピン入力ダイアログにパスフレーズを入力します。

108

Gpg4win Compendium 3.0.0

第18章ファイルの署名と暗号化

署名プロセスが正常に完了すると、次のウィンドウが表示されます。

これでファイルに署名できました。

「個別の」署名は常にファイルの署名に使用されます。つまり、署名されるファイルは変更されずに残り、実際の署名を持つ2番目のファイルが作成されます。後で署名を検証するには、両方のファイルが必要になります。

以下の例は、OpenPGPまたはS / MIMEを使用して選択したファイル（ここでは<dateiname> .txt ）に署名した場合に受信する新しいファイルを示しています。結果のファイルタイプには次の4つがあります。

**OpenPGP：**

<ファイル名> .txt！<ファイル名> .txt **.sig**

<ファイル名> .txt！<filename> .txt **.asc**  （text / ASCII-armorとして出力）

**S / MIME：**

<ファイル名> .txt！<ファイル名> .txt **.p7s**

<ファイル名> .txt！<ファイル名> .txt **.pem**（text / ASCII-armorとして出力）

109

Gpg4win Compendium 3.0.0

第18章ファイルの署名と暗号化

**署名を確認する**

次に、署名されたばかりのファイルの整合性を確認します。つまり、ファイルが正しいことを確認します。

終わると、したがってファイル-完全性及び真正性、署名ファイルをチェックする.SIG 、.ASC 、.p7s または.PEM -および署名された元のファイル（オリジナルファイル）同じファイルフォルダ内になければなりません。選択した署名ファイルを復号化し、エントリを選択し、Windowsエクスプローラのコンテキストメニューから確認してください。

110

Gpg4win Compendium 3.0.0

第18章ファイルの署名と暗号化

次のウィンドウが表示されます。

[ファイルを入力]の下に、選択した署名ファイルへのフルパスが表示されます。

入力ファイルを使用して元のファイル（ここでは署名ファイル）に署名しているため、[入力ファイルは別の署名です]オプションがアクティブになります。Kleopatraは、同じファイルフォルダー内の関連する署名された元のファイルを自動的に検索します。

Ouputフォルダーにも同じパスが自動的に選択されます。ただし、一度に複数のファイルを処理する場合にのみ関連します。

[復号・確認]で動作を確認してください。

111

Gpg4win Compendium 3.0.0

第18章ファイルの署名と暗号化

署名のチェックに成功すると、次のウィンドウが表示されます。

結果は、署名が正しいことを示しています。したがって、ファイルの整合性が保持され、ファイルが変更されていないことを確認できます。

112

Gpg4win Compendium 3.0.0

第18章ファイルの署名と暗号化

元のファイルに追加された文字が1つだけの場合、または削除または変更された場合でも、署名は壊れていると表示されます（Kleopatraは結果を赤い警告として表示します）。

113

Gpg4win Compendium 3.0.0

第18章ファイルの署名と暗号化

**18.2。ファイルの暗号化と復号化**

電子メールと同じように、ファイルに署名して暗号化できます。次のセクションでは、GpgEXとKleopatraを使用してもう一度練習する必要があります。

1つ（または複数）のファイルを選択し、右マウスキーを使用してコンテキストメニューを開きます。

[署名して再度暗号化]を選択します。

114

Gpg4win Compendium 3.0.0

第18章ファイルの署名と暗号化

ファイルへの署名から、おなじみのダイアログが表示されます（セクション18.1も参照）。

上部のフィールドで、[暗号化]オプションを選択します。

これが必要な場合のみ、暗号化設定を変更する必要があります。

**テキストとして出力（ASCIIアーマー）：**このオプションを有効にすると、.asc （OpenPGP）または.pem （S / MIME）で終わる暗号化ファイルが取得されます。これらのファイルタイプは、任意のテキストエディターで開くことができますが、以前に見た文字と文字の組み合わせのみが表示されます。

このオプションが選択されていない場合、システムは、末尾が.gpg （OpenPGP）または.p7m （S / MIME）の暗号化ファイルを作成します。これらのファイルはバイナリファイルであるため、テキストエディタで表示することはできません。

**暗号化されていないオリジナルを削除：**このオプションを有効にすると、選択したオリジナルファイルは暗号化後に削除されます。

[次へ]をクリックします。

115

Gpg4win Compendium 3.0.0

第18章ファイルの署名と暗号化

誰がファイルを暗号化する必要がありますか？次のダイアログで1つ以上の受信者証明書を選択します。

選択するには、上部で必要な証明書を選択し、[追加]を押します。確認のために、選択したすべての証明書がダイアログ下部に表示されます。

選択した受信者証明書とそのタイプ（OpenPGPまたはS / MIME）に応じて、ファイルはOpenPGPまたはS / MIMEを使用して暗号化されます。したがって、OpenPGP証明書とS / MIME証明書を選択した場合、2つの暗号化されたファイルを受け取ります。暗号化されたファイルの可能なファイルタイプは、次のページにあります。

[暗号化]をクリックします。ファイルは暗号化されています。

116

Gpg4win Compendium 3.0.0

第18章ファイルの署名と暗号化

暗号化が成功すると、結果ウィンドウは次のようになります。

それでおしまい！ファイルの暗号化に成功しました！

ファイルへの署名と同様に、結果は選択した暗号化方式（OpenPGPまたはS / MIME）によって異なります。元のファイル（ここでは<filename> .txt ）を暗号化すると、次の4つのファイルタイプが可能になります。

**OpenPGP：**

<ファイル名> .txt！<ファイル名> .txt **.gpg**

<ファイル名> .txt！<filename> .txt **.asc**  （text / ASCII-armorとしての出力用）

**S / MIME：**

<ファイル名> .txt！<ファイル名> .txt **.p7m**

<ファイル名> .txt！<filename> .txt **.pem**（text / ASCII-armorとしての出力用）

これで、これらの4つの可能な暗号化ファイルの1つを選択した受信者に転送します。ファイルに署名するのとは対照的に、暗号化されていない元のファイルはもちろん転送されません。

117

Gpg4win Compendium 3.0.0

第18章ファイルの署名と暗号化

**ファイルの復号化**

これで、以前に暗号化したファイルをテスト目的で解読できます。

このためには、前の暗号化プロセス中に独自の証明書で暗号化しておく必要があります。そうしないと、秘密鍵でファイルを復号化できません（第14章を参照）。

それで終わるので、1を-暗号化されたファイルを選択し.gpg 、.ASC 、.p7m もしくはの.pem -とエントリを選択

復号化し、Windowsエクスプローラーのコンテキストメニューで確認します。

118

Gpg4win Compendium 3.0.0

第18章ファイルの署名と暗号化

必要に応じて、次の復号化ダイアログで出力フォルダーを変更できます。

[復号化/チェック]をクリックします。

次に、パスフレーズを入力します。

119

Gpg4win Compendium 3.0.0

第18章ファイルの署名と暗号化

結果は、復号化が成功したことを示しています。

これで、復号化されたファイルを簡単に読み取ったり、対応するプログラムで使用したりできるようになります。

120

Gpg4win Compendium 3.0.0

第18章ファイルの署名と暗号化

**要するに**

GpgEXを使用して以下を実行する方法を学習しました。

署名ファイル

署名済みファイルをチェックしてファイルを暗号化する

ファイルを復号化する

**同時暗号化と署名**

このオプションは、対応するダイアログですでにお気づきでしょう。これを選択すると、GpgEXは両方のタスクを1つのステップで結合します。

暗号化プロセスの前に、署名が最初に適用されていることを確認してください。

したがって、署名は常に同時に暗号化されます。ファイルの復号化に成功したユーザーのみが表示および確認できます。

ファイルに署名して暗号化する場合は、現時点ではOpenPGPでのみ行うことができます。

121

1. **プライベート証明書のインポートとエクスポート**

第8章と第10章では、証明書のインポートとエクスポートについて説明しました。公開するために独自の証明書をエクスポートし、通信パートナーの証明書をインポートして、「鍵リング」に添付しました（つまり、証明書管理に受け入れました）。

このプロセスは常に公開鍵を参照していました。ただし、秘密鍵をインポートまたはエクスポートする必要がある場合もあります。たとえば、Gpg4winで既存の（OpenPGPまたはS / MIME）鍵ペアを引き続き使用する場合は、それをインポートする必要があります。または、別のコンピューターからGpg4winを使用する場合は、キーペア全体（公開キーと秘密キー）をそのコンピューターに転送する必要があります。

122

Gpg4win Compendium 3.0.0

第19章プライベート証明書のインポートとエクスポート

**19.1。書き出す**

プライベート証明書を別のコンピューターに転送したり、別のハードドライブパーティションまたはバックアップメディアに保存したりする場合は、Kleopatraを使用してバックアップコピーを作成する必要があります。

OpenPGP証明書の作成プロセスの最後で、このようなバックアップコピーを既に設定している場合があります。OpenPGP証明書は、meintinmeで追加の認証を受け取っている可能性があるため、該当する場合は、もう一度バックアップする必要があります。

Kleopatraを開き、独自の証明書を選択します。File！Export private certificateをクリックします。

出力ファイルのパスとファイル名を選択します。ファイルタイプは自動的に設定されます。プライベートOpenPGPまたはS / MIMEキーのどちらをエクスポートするかに応じて、.gpg （OpenPGP）または.p12 （S / MIME）で終わるファイルがデフォルトで選択されます。これらは、暗号化された証明書（秘密鍵を含む）を含むバイナリファイルです。

オプションでASCII保護（ASCIIアーマー）を有効にすると、末尾が.asc （OpenPGP）または.pem （S / MIME）のファイルが選択されます。これらのファイルタイプは、任意のテキストエディタで開くことができますが、以前に見た数字と文字の「混乱」しか表示されません。

このオプションを選択しない場合、末尾が.gpg （OpenPGP）または.p12 （S / MIME）の暗号化ファイルが作成されます。これらのファイルはバイナリファイルであるため、テキストエディタで表示することはできません。

Kleopatraは、プライベートとパブリックの両方の主要部分を1つのプライベート証明書に格納します。

注意：このファイルは慎重に扱ってください。秘密鍵が含まれているため、セキュリティに不可欠な情報が含まれています。

123

Gpg4win Compendium 3.0.0

第19章プライベート証明書のインポートとエクスポート

**19.2。インポート**

以前にエクスポートしたプライベート証明書をKleopatraにインポートするには、他のパブリック証明書をインポートする場合と同様に進めます（第10章を参照）。

File！Import certificate ...をクリックし、インポートするファイルを選択します。PKCS12ファイル（例えば

.p12と入力すると、システムはまず秘密鍵のロックを解除するためのパスフレーズを要求します。

次に、インポートが完了した後に秘密鍵を保護するために使用される、新しいフレーズの場合もあるフレーズを入力します。

パスフレーズのエントリを繰り返します。パスフレーズが短すぎるか文字のみで構成されている場合、システムは対応する警告を表示します。

124

Gpg4win Compendium 3.0.0

第19章プライベート証明書のインポートとエクスポート

インポートが成功すると、インポートプロセスの結果を示す情報ウィンドウが表示されます。以下は、プライベートOpenPGP証明書の例です。

Kleopatraは、秘密鍵と公開鍵の両方をバックアップファイルからインポートしました。証明書は、Kleoatraの証明書管理の「私の証明書」にあります。

また、可能であれば、物理的に保護された（ボールト内など）外部メディアにプライベート証明書のバックアップコピーを保存してください。次に、ハードドライブから削除し、削除したファイルを「ごみ箱」から削除してください。それ以外の場合、このファイルは秘密の電子メール暗号化に大きなセキュリティリスクをもたらします。

PGP（「Pretty Good Privacy」）でエクスポートされた証明書をインポートできない場合があります。これは、一部のPGPバージョンが、法的な理由でGnuPGでサポートできないアルゴリズム（IDEA）を使用しているためです。

この問題に対処するには、PGPでパスフレーズを変更し、OpenPGP証明書を再度エクスポート/インポートします。これも機能しない場合は、PGPのパスフレーズを「空」、つまり保護なしに設定し、再度エクスポート/インポートします。この場合、ファイルを安全に削除してから、新しい実際のパスフレーズを設定する必要があります。 PGPおよびGpg4win。

おめでとう！キーペアのエクスポートと再インポートが正常に完了しました。

125

1. **S / MIMEのシステム全体の設定と事前入力**

多くのユーザーが1台のコンピューターで作業している中央ソフトウェア配布または環境の一部として、Gpg4winのシステム全体の仕様と事前入力をセットアップすることは理にかなっています。

これは特にS / MIMEに関係します。これは、指定された信頼チェーンの場合、ユーザーが情報を共有することが理にかなっているためです。

いくつかの典型的なシステム全体の設定は次のとおりです。

**信頼できるルート証明書：**各ユーザーが必要なルート証明書を検索してインストールし、同じものの信頼性をチェックおよび認証する必要がある状況を回避するには（セクション22.7を参照）、システム全体に最も多くの事前入力をインストールすると便利です。重要なルート証明書。

このためには、セクション22.3で説明されているように、ルート証明書を保存し、セクション22.6で説明されているように、信頼できるルート証明書を定義する必要があります。

**直接利用可能なCA証明書：**ユーザーが認証局の証明書を検索してインポートするのを防ぐために、最も重要なCA証明書をシステムに事前に入力することも意味があります。説明は、22.4項を参照してください。

**証明書サーバーおよび証明書失効リスト検索のプロキシ：**有効性情報に関して、X.509プロトコルはさまざまなオプションを提供します。ほとんどの認証機関は、証明書失効リスト（CRLとも呼ばれ、RFC5280に従ってサポートされています）およびOSCP（RFC2560に従って）を公開しています。OSCPには最新の情報がありますが、ネットワークトラフィックがOSCPサービスに至るまで発生するため、誰とメッセージが交換されているかを確認できます。GnuPGは両方のオプションで機能します。システム全体のサービスとして実行されるコンポーネント「DirMngr」。

内部ネットワークでは、個々のコンピューターが外部（中央ファイアウォール）に直接接続することを許可できませんが、いわゆる「プロキシ」と呼ばれる代理サービスを提供できます。DirMngrは、HTTPおよびLDAPプロキシも処理できます。

S / MIME証明書には、通常、証明書失効リストを外部から取得できる場所に関する情報が含まれています。多くの場合、HTTPが含まれますが、LDAPを介したディレクトリサービスも含まれます。OpenPGPとは対照的に、クライアントは証明書失効リストを取得する場所を選択できませんが、利用可能な情報に従う必要があります。一部の証明書はLDAP経由でのみ証明書失効リストを提供するため、外部へのHTTPクエリとLDAPクエリの両方を許可する必要があります。可能であれば、代理サービスは、コンテンツレベルで、正しい情報を含むX.509証明書失効リストのみが送信されるようにします。

OpenPGPまたはS / MIMEに必要なHTTPおよびHKPまたはLDAPクエリのプロキシがネットワークに必要な場合は、次の手順に従ってください。

1.セクション22.5で説明されているように、X.509証明書サーバー検索をプロキシに設定します。

126

Gpg4win Compendium 3.0.0

第20章S / MIMEのシステム全体の設定と事前入力

1. 証明書失効リストの検索をプロキシに設定します。これもセクション22.5で説明されています。

1. DirMngrを再起動します（セクション21.7を参照）。

127

**21.既知の問題とヘルプ**

**21.1。OutlookにGpgOLメニューとダイアログが表示されなくなった**

GpgOLによってOutlookに追加されたメニューやダイアログが見つからない場合があります。

これは、OutlookがGpgOLコンポーネントを非アクティブ化する原因となった技術的な問題が原因である可能性があります。

OutlookメニューからGpgOLを再アクティブ化します。

Outlook2007：？！無効化されたコンポーネント

Outlook2003：？！Info！Deactivatedコンポーネント

GpgOLを手動で（非）アクティベートするには、Outlookのアドインマネージャーを使用します。

Outlook2003：Extras！Options！Other！Advanced options ...！アドインマネージャ...

Outlook2007：Extras！Trust Relations Center！Add-Ins –次に、[Manage]で[Exchange-Client exten-sions]を選択し、[Go to ...]をクリックします。

**21.2。GpgOLボタンがOutlook 2003ツールバーにない**

メッセージウィンドウのツールバーに既に多数のボタンがある場合、Outlook 2003は必ずしもGpgOLの署名/暗号化アイコンを表示しません。

これらのボタンを表示するには、ツールバーで下向きの矢印が付いた小さなアイコンをクリックします（ツールバーのオプション）：表示されていないすべてのボタンの概要が表示されます。エントリをクリックすると、ツールバーの表示領域に移動します。

**21.3。GpgOLボタンが「アドイン」の下にリストされている（Outlook 2007）**

Outlook 2007では、いわゆる「リボン」インターフェースが導入されました。Outlookメッセージウィンドウのこの多機能バーには、さまざまなタブがあります。GpgOLボタン（暗号化、署名など）は「アドイン」タブの下に編成されています。Outlookは拡張機能のすべてのボタンをその場所に保存します。たとえば、「メッセージ」の下にGpgOLボタンを統合することはできません。

すばやくアクセスできるようにツールバーを調整し、[アドイン]タブのツールバーコマンドを追加できます。

**21.4。GpgOLの起動時のエラー**

ドライブに最初にGpg4win（したがってGpgOLプログラムコンポーネント）をインストールした場合、それをアンインストールして別のドライブに再インストールしますか？はいの場合、Outlookは最初の（古い）ドライブでGpgOLパスの検索を続行する可能性があります。

128

Gpg4win Compendium 3.0.0

第21章既知の問題とヘルプ

これは、Outlookの起動時にGpgOLプログラム拡張が起動されなくなり、次のエラーメッセージが表示されることを意味します。

拡張機能 ' <gpgol.dllへの古いパス> 'をインストールまたはロードできませんでした。この問題は、ヘルプの「検出と修復」を使用することで解決できます。

この問題は、内部のOutlook（キャッシュ）プログラム拡張パスをリセットすることで解決できます。これを行うには、次のファイルを削除してください。

％APPDATA％\ Lokale Einstellungen \ Application data \ Microsoft \ Outlook \ extend.dat

このプロセス中はOutlookを実行しないでください。次に、Outlookを再起動すると、GpgOLで正常に動作します。

**21.5。仮想ドライブへのGpg4winのインストール**

コマンドsubstでシミュレートされた仮想ドライブにGpg4winをインストールすることはできないことに注意してください。これらの仮想ドライブは、現在のユーザーがローカルでのみ使用できます。DirMngr などのシステムサービスは、これらのドライブを認識しません。したがって、インストールパスは無効です。インストールはエラータイプerror：StartService：ec = 3で停止します。システム全体で使用可能なドライブにGpg4winをインストールしてください。

**21.6。GpgOLは「CryptoEx」InlinePGP電子メールをチェックしません**

Outlookプログラム拡張機能「CryptoEx」によって送信された署名済みまたは暗号化されたInlinePGP電子メールをチェックまたは復号化するには、GpgOLオプションでS / MIMEサポートをアクティブにする必要があります。

OutlookのExtras！Options！GpgOLで次のオプションがアクティブになっていることを確認してください。

S / MIMEサポートをアクティブにします。

129

Gpg4win Compendium 3.0.0

第21章既知の問題とヘルプ

**21.7。S / MIME操作を許可しません（システムサービス「DirMngr」が実行されていません）**

“ Directory Manager”（DirMngr）は、Gpg4winによってインストールされるサービスで、証明書サーバーへのアクセスを管理します。DirMngrの1つのタスクは、S / MIME証明書の証明書失効リスト（CRL）をロードすることです。

DirMngrが使用できないため、S / MIME操作（署名の作成とチェック、暗号化と復号化）を実行できない可能性があります。したがって、Gpg4winのデフォルト設定では、DirMngrが失効リストをチェックするようにする必要があります。これを行わないと、侵害された証明書が使用される可能性があるため、操作を実行できません。

この問題に対処するために、システム管理者はDirMngrを再起動します。これは、システム制御！管理！サービスを介して行われます。リストにDirMngrが表示され、コンテキストメニューからサービスを再起動できます。

**21.8。S / MIME操作は許可されていません（CRLは使用できません）**

CRLが使用できないため、S / MIME操作（署名の作成とチェック、暗号化と復号化）を実行できない可能性があります。したがって、Gpg4winのデフォルト設定では、失効リストがチェックされていることを確認する必要があります。これを行わないと、侵害された証明書が使用される可能性があるため、操作を実行できません。

失効リストを取得するための代理サービス（「プロキシ」）を設定すると、ヘルプが提供されます（セクション22.5を参照）。

緊急時（またはテスト目的で、CRLチェックをオフにすることもできます。これを行うには、Kleopatraメニュー[設定]を開いて、Kleopatraをセットアップしてから、グループS / MIMEチェックを実行します。オプション[アクティブ化リストを参照しない]をオンにします。

注意：これは、侵害された証明書を使用するリスクが高くなることにも注意してください。

失効リストのチェックをオフにすることは、プロキシの設定に代わるものではありません。

130

Gpg4win Compendium 3.0.0

第21章既知の問題とヘルプ

**21.9。S / MIME操作は許可されていません（ルート証明書は信頼できません）**

X.509証明書チェーンを完全に確認するには、それぞれのルート証明書を信頼する必要があります。そうしないと、S / MIME操作（署名の作成とチェック、暗号化と復号化）を実行できません。

ルート証明書への信頼を表すには、2つのオプションがあります。

対応するルート証明書のフィンガープリントをシステム全体の構成ファイルに書き込みます。これで、ルートはすべてのユーザーにとって信頼できます。これを行うには、Windows管理者権限が必要です。詳細については、セクション22.6を参照してください。

ユーザーが設定したルート証明書（システム全体での調整は不要）。これを行うには、Kleopatraの設定で[ルート証明書のマーキングを許可する]オプションを信頼できるものとしてマークする必要があります。その後、新しいルート証明書をインポートするたびに、それを信頼するかどうかを尋ねられます。詳細については、セクション22.7を参照してください。

131

**22. Gpg4winのファイルと設定**

**22.1。個人ユーザー設定**

各ユーザーの個人設定は、ファイルフォルダーにあります。

％APPDATA％\ gnupg

多くの場合、これは次のフォルダーです。

C：\ Documents and settings \ <名前> \ Application data \ gnupg \

これは隠しファイルフォルダーであることに注意してください。表示するには、エクスプローラーエクストラのフォルダービューのタブにある[ファイルとフォルダーの非表示]グループの下にある[すべてのファイルとフォルダーを表示]オプションをアクティブにする必要があります。フォルダーオプションメニュー

このファイルフォルダーには、すべての個人GnuPGデータが含まれているため、秘密鍵、証明書、信頼設定および構成が含まれています。Gpg4winをアンインストールしても、このフォルダーは削除されません。このフォルダの定期的なバックアップコピーを作成してください。

**22.2。キャッシュされた証明書失効リスト**

システム全体のサービスMngr（Directory Manager）は、X.509証明書がブロックされているため使用できないかどうかもチェックします。この目的のために、証明書失効リスト（CRL）は、証明書（CA）の発行局から取得され、有効期間中キャッシュされます。

リストは以下に保存されます：

C：\ Documents and Settings \ LocalService \ Lokale Settings \ Application data \ GNU \ cache \ dirmngr \ crls.d \

これらは保護されたファイルであり、エクスプローラにはデフォルトでは表示されません。ただし、これらのファイルを表示したい場合は、ウィンドウエクスプローラビューの設定で[保護されたシステムファイルを非表示]オプションを無効にします。

このファイルフォルダは変更しないでください。

132

Gpg4win Compendium 3.0.0

第22章Gpg4winのファイルと設定

**22.3。DirMngrからの信頼できるルート証明書**

X.509証明書を完全に確認するには、失効リストへの署名に使用されたルート証明書を信頼する必要があります。

チェックを実行するときにDirMngrがシステム全体で信頼する必要があるルート証明書は、次のファイルフォルダーに格納されています。

C：\ Documents and settings \ All Users \ Application data \ GNU \ etc \ dirmngr \ trusted-certs \

重要：対応するルート証明書は、上記のファイルフォルダーに.crt または.der という名前のDER形式のファイルとして使用できる必要があります。

DirMngrはシステム全体のサービスとして実行され、「信頼できる証明書」ファイルフォルダーに変更が加えられた場合は再起動する必要があります。その後、このフォルダーに保存されたルート証明書は、すべてのユーザーに対して信頼できるように設定されます。

ルート証明書（システム全体）を完全に信頼するには、セクション22.6も参照してください。

**22.4。DirMngrからの他の証明書**

暗号化操作の前にX.509証明書チェーンをチェックする必要があるため、認証インスタンス（「認証局」、CA）の対応する証明書もチェックする必要があります。

すぐに利用できるように、CA証明書はこの（システム全体の）ファイルフォルダーに保存できます。

C：\ Documents and settings \ All Users \ Application data \ GNU \ lib \ dirmngr \ extra-certs \

ここで利用できない、またはユーザーから利用できない証明書は、X.509証明書サーバーによって自動的に読み込まれる必要があります。

ただし、これらのCA証明書は、ユーザーが手動でインポートすることもできます。

システム全体の仕様の一部として、このフォルダに最も重要なCA証明書を格納することは理にかなっています。

133

Gpg4win Compendium 3.0.0

第22章Gpg4winのファイルと設定

**22.5。外部X.509証明書サーバーを使用するためのシステム全体の構成**

GnuPGは、システムが欠落しているX.509証明書または外部X.509証明書サーバー上の証明書失効リストを検索できるように構成できます（第20章も参照）。

X.509証明書の検索を実行するために、システムサービスDirMngrは、ファイルに入力できる証明書サーバーのリストを使用します。

C：\ Documents and settings \ All Users \ Application data \ GNU \ etc \ dirmngr \ ldapservers.conf

これらの証明書サーバーは、すべてのユーザーに使用されます（システム全体）。さらに、ユーザーは証明書検索用に追加のユーザー固有の証明書サーバーを設定することもできます。たとえば、Kleopatraを介して直接（第16.1章を参照）

前述の構成ファイルの証明書サーバーエントリの正確な構文は次のとおりです。

HOSTNAME：PORT：USERNAME：PASSWORD：BASE\_DN

外部X.509証明書サーバーへのアクセスが内部ネットワークのファイアウォールによってブロックされている場合、次のサンプル行に示すように、証明書検索を送信するためにldapservers.conf でプロキシサービスを構成することもできます。

proxy.mydomain.example：389 ::: O = myorg、C = de

証明書失効リスト（CRL）の検索に関しては、同じディレクトリに次の構成ファイルが含まれています。

C：\ Documents and settings \ All Users \ Application data \ GNU \ etc \ dirmngr \ dirmngr.conf

このファイルに書き込むことができるのは管理者だけであることに注意してください。

この構成ファイルに次のプロキシオプションを追加できます（各オプションは続けて）。

http-proxy HOST [：PORT] このオプションは、証明書サーバーへのアクセスにHOST とPORT を使用します。このオプションを有効にすると、環境変数http\_proxy が上書きされます。

例：

http-proxy http：//proxy.mydomain.example：8080

ldap-proxy HOST [：PORT] このオプションは、証明書サーバーへのアクセスにHOST とPORT を使用します。ポート番号がリストされていない場合、標準のLDAPポート389が使用されます。このオプションは、証明書に含まれているLDAP URLを上書きします。LDAPURL が入力されていない場合は、HOST およびPORT を使用します。

only-ldap-proxy このオプションは、DirMngrがldap-proxyで構成されたプロキシのみを使用することを保証します。それ以外の場合、LDAP プロキシ経由の接続が成功しない場合、DirMngrは他の構成済み証明書サーバーを使用しようとします。

134

Gpg4win Compendium 3.0.0

第22章Gpg4winのファイルと設定

**22.6。システム全体で信頼できるルート証明書**

システム全体で信頼できるとみなされる事前入力されたルート証明書は、

C：\ Documents and settings \ All Users \ Application data \ GNU \ etc \ gnupg \ trustlist.txt file。

ルート証明書を信頼できるものとしてマークするには、証明書の対応するフィンガープリント、それに続く空白スペースと大きなSを上記のファイルに入力する必要があります。行がプレフィックス「！」で始まる場合、証明書は明示的に信頼できないとマークされます。」。複数のルート証明書を入力することもできます。その場合、各指紋が新しい行に配置されていることを確認してください。＃で始まる行はコメントとして扱われ、無視されます。

重要：ファイルの最後には、空の行が続く必要があります。

例：

＃CN =ワーゼルZS 3、O = Intevation社、C = DE A6935DD34EF3087973C706FC311AA2CCF733765B S

＃CN = PCA-1-Verwaltung-02 / O = PKI-1-Verwaltung / C = DE DC：BD：69：25：48：BD：BB：7E：31：6E：BB：80：D3：00： 80：35：D4：F8：A6：CD S

＃CN =ルート-CA / O = Schlapphuete / L =プラッハ・イム・イーザルタール/ C = DE 14：56：98：D3：FE：9C：CA：5A：31：6E：BC：81：D3：11：4E：00 ：90：A3：44：C2 S

場合によっては、ルート証明書をチェックする基準を減らすと便利です。これを行うには、Sの後に追加のフラグrelaxを設定します。<FINGERPRINT> S relax

重要：relax を使用するとセキュリティのレベルが低下するため、ケースバイケースで決定する必要があり、問題が発生した場合にのみ使用する必要があります。

詳細については、現在のGnuPGドキュメント（項目「trustlist.txt」）を参照してください。

[http://www.gnupg.org/documentation/manuals/gnupg/Agent-Configuration.html](https://translate.google.com/translate?hl=ja&prev=_t&sl=auto&tl=ja&u=http://www.gnupg.org/documentation/manuals/gnupg/Agent-Configuration.html)

したがって、trustlist.txtのエントリの正確な構文は次のとおりです。

[！] <FINGERABDRUCK> S [リラックス]

それにより！とリラックスはオプションです。

フラグSの代わりに、値P および\*も提供されます。これらは将来の使用のために予約されています。

重要：ルート証明書をKleopatraで信頼できるものとして完全にマークするには（証明書は青色で強調表示されています）、セクション22.3で説明されているように、ルート証明書もDirMngr用に保存する必要があります。

135

Gpg4win Compendium 3.0.0

第22章Gpg4winのファイルと設定

**22.7。ルート証明書の信頼性のユーザーマーキング**

ルート証明書は、個々のユーザーが信頼できるものとしてマークすることもできます。つまり、システム全体の構成（セクション22.3および22.6を参照）は必要ありません。

Kleopatraメニューの[設定]を開きます。Kleopatraを構成してから、groupo S / MIMEチェックを行います。次に、[ルート証明書を信頼できるものとしてマークできるようにする]オプションを有効にします。これで、以前に信頼できるとマークされていないルート証明書を使用している場合、システムはそれを信頼できるものとして分類するかどうかを尋ねてきます。変更が有効になる前に、gpg-agentを再起動する必要があることを確認してください（たとえば、ログインとログアウトによる）。

信頼できるとマークされた（または明示的に信頼できないとマークされた）ルート証明書

次のファイルに自動的に保存されます。

C：\ Dokumente und Einstellungen \ <Nutzername> \ Application data \ gnupg \ trustlist.txt

セクション22.6で説明されているように、同じ構文がtrustlist.txtにも適用されます。

136

1. **Gpg4winプログラム（ログファイル）の問題の検出**

Gpg4winプログラムコンポーネントの1つが期待どおりに動作しない可能性があります。

多くの場合、これはGpg4winソフトウェア開発者が検出できない作業環境に関連する機能が原因です。

問題の発見を支援するため、またはユーザーが詳細な技術プロセスを確認できるように、Gpg4winプログラムもヘルプを提供します。

ただし、通常、このタイプのヘルプは最初にアクティブにする必要があります。最も重要なツールの1つはログファイルです。ここには、内部の技術プロセスに関する詳細な診断情報が保存されます。ソフトウェア開発者は、ログファイルを確認することで、プログラムが最初は非常に複雑に見えても、多くの場合、問題と可能な解決策をすばやく検出できます。

ソフトウェア開発者にエラーレポートを送信する場合は、次の情報が役立ちます。

[http://gpg4win.org/reporting-bugs.html](https://translate.google.com/translate?hl=ja&prev=_t&sl=auto&tl=ja&u=http://gpg4win.org/reporting-bugs.html)

上記のURLでは「デバッグ情報」として説明されているログファイルは、貴重な情報を提供することが多いため、エラーレポートに添付する必要があります。

この章では、個々のGpg4winプログラムのプログラムプロセス情報（本質的にはログファイル）をアクティブにする方法について説明します。

137

Gpg4win Compendium 3.0.0

第23章Gpg4winプログラム（ログファイル）の問題の検出

**23.1。Kleopatraログファイルのアクティブ化**

Kleopatraログデータは多くのファイルで構成されているため、最初のステップはログファイル用のファイルフォルダーを作成することです（例：C：\ TEMP \ kleologdir）。

これらはユーザー設定であり、システム管理者設定ではないことに注意してください。したがって、Kleopatraログデータを作成するユーザーごとに設定を行う必要があり、異なるkleologdir ファイルフォルダーを使用する必要があります。

このフォルダーへのパスは、新しい環境変数KLEOPATRA\_LOGIDRに記載する必要があります。

これを行うには、コントロールパネルを開き、[システム]を選択して、[詳細設定]タブを選択し、最後にボタンを選択します。

[ 環境変数]。

次の新しいユーザー変数を追加します。

変数の名前：KLEOPATRA\_LOGDIR

変数の値：C：\ TEMP \ kleologdir

入力したファイルフォルダが実際に存在することを確認してください。後で作成することもできます。

ログ機能を有効にするには、Kleopatraをシャットダウンして再起動する必要があります。ログデータのファイルフォルダーが存在し、Kleopatraが書き込みできる必要があります。

Kleopatraが使用されている間、ファイルkleo-log （メインログファイル）だけでなく、次のパターンに従う名前を持つ多くのファイルにもプロセス情報が記録されます。

pipe-in​​put- <タイムスタンプ>-<ランダムな文字>

この情報は、ソフトウェア開発者がエラーを検出するには不十分な場合があります。次に、以前と同じように、別の環境変数を作成するように求められます。

変数の名前：KLEOPATRA\_LOGOPTIONS

変数の値：すべて

ログファイルが非常に急速に大きくなる可能性があります。ログ機能は、特定のエラー機能を誘発する場合にのみ有効にして、記録する必要があります。

その後、環境ファイルを削除するか、その名前を少し変更することで、ログ機能を再びオフにすることができます（後で簡単に再アクティブ化できるようにするため）。ログファイルが非常に大きくなったり、ファイルが多数ある場合は特に、ログファイルを削除または移動することを忘れないでください。新しい記録を開始する前に、ログファイルを削除することも意味があります。

138

Gpg4win Compendium 3.0.0

第23章Gpg4winプログラム（ログファイル）の問題の検出

**23.2。GpgOLログファイルのアクティブ化**

GpgOLログファイルをアクティブにするには、「レジストリエディター」を起動する必要があります。これを行うには、Start！Executeの下または入力要求フィールドにコマンドregedit を入力します。

次に、左側のツリー構造から次のGpgOLキーを選択します。

HKEY\_CURRENT\_USER \ Software \ GNU \ GpgOL

右側には、エントリ（いわゆる文字シーケンス）のリストが表示されます。その一部には、事前に定義された値があります。これらのエントリは、Outlookが最初にGpgOLで起動されたときに作成されます。

GpgOLログファイルをアクティブにするには、エントリenableDebug をダブルクリックし、この値を1に設定します。

logFileの値を設定するには、ログファイルを書き込むファイルの名前を入力します。例：C：\ TEMP \ gpgol.log

Outlookを再起動して、記録プロセスを開始します。

このファイルは非常に大きくなる可能性があることに注意してください。GpgOLログデータの記録が不要になったらすぐに、enableDebug を0に設定します。

特に非常に大きなファイルになっている場合は、ログファイルを削除または移動することも忘れないでください。新しい記録を開始する前に、ログファイルを削除することも意味があります。

enableDebugの可能な値など、GpgOLに関するより高度な技術情報は、技術（英語）GpgOLハンドブックに記載されています。それはあなたのGpg4winインストールディレクトリにあります、通常：

C：\ Programme \ GNU \ GnuPG \ share \ doc \ gpgol \ gpgol.pdf

139

Gpg4win Compendium 3.0.0

第23章Gpg4winプログラム（ログファイル）の問題の検出

**23.3。DirMngrログファイルのアクティブ化**

DirMngrはシステム全体のサービスであるため、ログファイルは管理者権限でのみアクティブ化できます。

ログファイルをアクティブにするには、次の構成ファイルを開きます。

C：\ Documents and settings \ All Users \ Application data \ GNU \ etc \ dirmngr \ dirmngr.conf

構成ファイルに次の2つの行を追加します（もちろん、ログファイルへのパスは調整できます）。

すべてデバッグ

ログファイルC：\ TEMP \ dirmngr.log

次に、システムコントロールの下のDirMngrを再起動します！管理！サービスを変更して、変更された構成ファイルが再インポートされ、新しい設定がアクティブになるようにします。

DirMngrログファイルの記録が不要になり次第、前述の構成ファイル（したがって＃debug-all）で調整をコメント化します。

特に非常に大きなファイルになっている場合は、ログファイルを削除または移動することも忘れないでください。新しい記録を開始する前に、ログファイルを削除することも意味があります。

140

Gpg4win Compendium 3.0.0

第23章Gpg4winプログラム（ログファイル）の問題の検出

**23.4。GnuPGログファイルのアクティブ化**

次の各GnuPGコンポーネントのログファイルの個別作成をアクティブ化できます。

GPGエージェント

OpenPGPスマートカードデーモンのS / MIME GPGのGPG

ユーザーは、これらのプログラムの個人設定を行うこともできます。これには、プログラムプロセスのログファイルの設定も含まれます。

それぞれのログファイルは、GnuPGバックエンドでアクティブ化されます。これには、Kleopatraメニューの[設定]、[Kleopatraの設定...]、[GnuPGシステム]からアクセスできます。この構成ウィンドウには、4つのプログラムのeac hofの2つのデバッグオプションがあります。

オプションデバッグレベルをに設定

ここでは、記録する情報の詳細を定義します。デバッグレベル4-Guruは最高レベルであり、非常に大きなファイルを作成します。これらのファイルが不要になった場合は、デバッグレベルを0（なし）に設定します。

オプションサーバーモードでファイルにログを書き込む

ここでは、すべてのデバッグ情報を保存するログファイルを入力します。例：

C：\ TEMP \ gpg-agent.log

Kleopatraを再起動する（まだ実行されている場合は、タスクマネージャーからpgp-agentをシャットダウンする必要がある場合があります）、またはログアウトしてWindowsシステムに再度ログインします。

特に非常に大きなファイルになっている場合は、ログファイルを削除または移動することも忘れないでください。新しい記録を開始する前に、ログファイルを削除することも意味があります。

141

Gpg4win Compendium 3.0.0

第23章Gpg4winプログラム（ログファイル）の問題の検出

**23.5。GpgMEログファイルのアクティブ化**

GpgME（「GnuPG Made Easy」）のログファイル設定は、Kleopatraと同様に、ユーザーごとに行う必要があります。

Windowsのコントロールパネルを開き、[システム]、[詳細設定]タブ、[ボタン]の順に選択します

[ 環境変数]。新しいユーザー変数を追加します。

変数の名前：GPGME\_DEBUG

変数変数：<DEBUGLEVEL; PFAD> 、zB：5; c：\ TEMP \ gpgme.log

入力したファイルの順序も存在する必要があることに注意してください。後で設定することもできます。

推奨診断レベルは値5 です。ほとんどの場合、このレベルは十分な情報を提供します。そうでない場合、上級ユーザーはこのレベルを徐々に上げることができます。

ログデータの記録をオフにするには、診断レベルを値0 に設定するか、ユーザー変数を削除します。

特に非常に大きなファイルになっている場合は、ログファイルを削除または移動することも忘れないでください。新しい記録を開始する前に、ログファイルを削除することも意味があります。

142

**24. Gpg4winが壊れない理由...**

...少なくとも現在知られている方法ではなく、ソフトウェアにエラーがない場合。

ただし、実際には、ソフトウェアの使用時に秘密情報を取得する機会を提供するのは、まさにプログラム内のエラー、またはオペレーティングシステムに含まれているエラーです。一方、フリーソフトウェアは、これらのタイプのエラーを回避するための実質的に最良の前提条件を提供します。

この大要の各例は、秘密鍵と公開鍵の間に関係があることを示しています。シークレットメッセージは、両方が一致する場合にのみ復号化できます。

この数学的接続の背後にある秘密を実際に知っている必要はありません– Gpg4winはそれなしでも動作します。同時に、素人でもこの複雑な数学的方法を理解できます。特別な種類の加算と乗算を定義するために、基本的な算術方法（加算、減算、乗算、除算）しか使用しないためです。秘密の方法とアルゴリズムがないという事実は、暗号化のセキュリティ哲学とフリーソフトウェアの原則の背後にあるものです。最後に、これはGnuPG（Gpg4winの背後にある実際の機構）が非常に安全である理由を本当に理解する最良の方法でもあります。

つまり、これが必須部分に続く無料プログラムが始まる場所です。

143

1. **GnuPGと多数の謎**

非数学者のための暗号

GnuPGのベース1であるRSAアルゴリズムを「解読」しようとする試みがいくつかあります1。つまり、公開鍵だけがわかっているときに秘密鍵を計算するというものです。ただし、このタイプの計算は、GnuPGで使用されるキー長（1024ビット以上）では成功していません。理論的なレベルでは可能かもしれませんが、十分な時間（数年）と何千ものネットワーク化されたコンピューターがあったとしても、この計算の最後のステップを完了するのに十分なストレージがないため、実際には不可能です。

同時に、ある日独創的な数学的アイデアがRSAの背後にある数学的問題の解決策を提供する可能性は十分にあります。ただし、これがすぐに発生することはほとんどありません。

ドイツ連邦情報技術安全保障局（BSI）は、特定の鍵の長さを絶対的なセキュリティ保証に使用できる期間に関する予測と評価を随時公開しています。GnuPGの標準設定は、これらの最小要件をはるかに超えています。前の章で触れたように、数学的な要素は、実際に適用される暗号の中で最も安全な部分を形成します。

1ここでは、RSAを例として使用します。これは、GnuPGの事前設定として使用されるElGamalアルゴリズムよりも理解しやすいためです。

144

Gpg4win Compendium 3.0.0

第25章GnuPGと多数の謎

次の説明では、この数学的方法がどのように機能するかを示します。すべての詳細がカバーされるわけではありません-これはこのマニュアルの範囲をはるかに超えているため-ある程度の努力を払えば、正しい暗号化/復号化計算を行うことができ、したがって「大きな数の謎」を発見できます。

非数学者や人間でも、この複雑な数学的方法を理解できます。必要なのは、単純な加算と乗算のプロセスをよく理解することだけです。これはフリースケートの概念と比較できます。なぜなら、フリースケートは、必要な要素がはるかに重いショートプログラムよりも、実体についてはるかに重要だからです。しかし、最も重要なことは、GnuPGが非常に安全である理由を理解するのに役立ちます。

しかし、最初にいくつかの用語を取り除きましょう。

アルゴリズムは、データや情報を変更または変換するための数学的な方法です。

算術は、数値を加算および乗算する方法です。

GnuPGを使用した暗号化は、いわゆるRSAアルゴリズム2に基づいています。RSAは、1978年にこのアルゴリズムを発見したRon Rivest、Ami Shamir und Ben Adlemanの姓から派生しています。このアルゴリズムは、剰余類の算術または「モジュラー（またはモジュロ）算術」と呼ばれる算術のタイプを使用します。

2RSAは実際にはオプションです。これは、特許の理由により、離散対数の問題を説明するのがより難しいElGamalアルゴリズムが標準として使用されているためです。

145

Gpg4win Compendium 3.0.0

第25章GnuPGと多数の謎

**25.1。残差クラスを使用した計算**

残差クラスで計算することは、整数による整数除算の後に残る「残差」（または剰余）のみを計算することを意味します。除算が行われるこの番号は、「モジュール」または「モジュラー番号」と呼ばれます。たとえば、係数またはモジュラー数5で計算する場合、これは「算術モジュロ5」と呼ばれます。

剰余類の算術（モジュラーまたは合同算術とも呼ばれます）がどのように機能するかを説明するために、時計の表面を想像してみてください。

この時計は、12を法とする算術演算の例です（したがって、係数も12です）。通常のダイアルを備えた時計です。ただし、12が表示されると予想される場所に0がある場合を除きます。この例を使用すると、簡単にモジュロ演算を記述できます。架空のダイヤルを動かす。

たとえば、3 + 2を計算するには、数字2から始めて、ダイヤルを3桁回します（または、3から始めて2桁回すと、同じ結果になります）。結果は5です。

同じ方法を使用して7 + 8を追加すると、結果は3になります。なぜですか？3は、15（つまり、7 + 8）を12で除算した結果の残差です。5を7で乗算するには、0から始めて、7回ごとに5桁ずつ前進します（または0で始まり、7桁ずつ前進します5回）。どちらの場合も、ダイヤルは11で止まります。これは、11が35（ie7 5）を12で除算して得られる残差だからです。

146

Gpg4win Compendium 3.0.0

第25章GnuPGと多数の謎

したがって、剰余類の算術を使用することにより、日常の算術の従来の規則に従って数を加算および除算し、常に除算後に残った残差のみを使用します。モジュラス（係数）は、従来の算術ではなくモジュラー算術の規則が適用されることを示すために追加されます。したがって、たとえば、「4 modulo 5」、つまり「4 mod 5」と言います。

たとえば、モジュロ5は、5つの数値（0、1、2、3、4）のみを持つクロックで表されるため、次のようになります。

4 mod 5 + 3 mod 5 = 7 mod 5 = 2 mod 5

別の言い方をすると、5を法とする算術演算を使用すると、4と3を加算した結果は2になります。

モジュロ5演算の別の例：

8 mod 5 + 6 mod 5 = 14 mod 5 = 4 mod 5

次のように書くこともできるので、どの順序で進めても問題ないことがわかります。

8 mod 5 + 6 mod 5 = 3 mod 5 + 1 mod 5 = 4 mod 5

3は8と同じで、1は6と同じです。これは、係数5で除算した後に残るそれぞれの残差のみに関心があるためです。

最後の例は、このタイプの算術を使用することにより、いつでもモジュール番号の整数倍（ここでは5）を追加できるという事実を強調していますが、結果は常に同じです。

147

Gpg4win Compendium 3.0.0

第25章GnuPGと多数の謎

このパターンは乗算にも有効です。

例：

4 mod 5 2 mod 5 = 8 mod 5 = 3 mod 5

次のように書くこともできます：

9 mod 5 7 mod 5 = 63 mod 5 = 3 mod 5

60を差し引いて、5を差し引くことができるため、12です。

ただし、次のように書くこともできます。

9 mod 5 7 mod 5 = 4 mod 5 2 mod 5 = 8 mod 5 = 3 mod 5

5で除算した後の残差のみを調べると、4は9に対応し、2は7に対応するためです。

繰り返しますが、5の倍数を単に省略しても問題はないことがわかります。

これによりすべてが非常に簡単になるため、数値を追加または乗算する前にこれを行います。これは、5で割り切れるものをすべて除外できるので、5を法とする算術演算を行う場合に、0、1、2、3、4の数値のみを考慮する必要があることを意味しています。

さらに3つの例：

1. 5 mod 11 3 mod 11 = 15 mod 11 = 4 mod 11

1. 2 mod 7 4 mod 7 = 1 mod 7

1. 13 mod 17 11 mod 17 = 7 mod 17

最後の例は、従来の算術演算13 11 = 143および143 = 8 17 + 7の使用を検討すると明らかになります。

148

Gpg4win Compendium 3.0.0

第25章GnuPGと多数の謎

**25.2。RSAアルゴリズムと残差クラスを使用した計算**

コンピュータは文字を数字として保存します。コンピュータのキーボードにあるすべての文字と記号は、実際には0〜255の数値として格納されます。

その結果、メッセージを一連の数値に変換することができます。このプロセスで使用される方法（またはアルゴリズム）については、GnuPGでの暗号化に使用される方法であるRSAアルゴリズムを紹介する次のセクションで説明します。このアルゴリズムは、一連の数値（メッセージを表すことができる）を別の一連の数値（変換）に変換して、メッセージが暗号化されるようにします。正しい方法を使用して、メッセージは安全にエンコードされ、正しい受信者のみがデコードできます。

これらは、RSAアルゴリズムの背後にある原則です。

証明書を作成するためのパスフレーズを入力したときに、2つの大きな素数を作成しました（これらはpおよびqと記述されています）。これらの2つの素数を知っているのはあなた、または実際にはあなたのコンピュータだけなので、秘密にしておく必要があります。

これらは現在、3つの追加番号の作成に使用されています。

**最初の数値**は、2つの素数を乗算した結果、つまり積です。この積は係数として記述され、文字nで示されます。これは、後で計算に使用するモジュール番号です。

**2番目の数値**は、いわゆる公開指数eであり、特定の要件を持つ数値です（（p 1）（q 1）と互いに素）。多くの場合、41または65537の数字が使用されます。

**3番目の数値**は、公開指数（2番目の数値）と2つの素数から計算されます。この数値は秘密の指数であり、dで記述されます。計算式は次のとおりです。

d = e 1mod（p 1）（q 1）

最初と2番目の番号が公開されます—公開鍵。どちらもメッセージの暗号化に使用されます。3番目の番号（秘密鍵）は秘密にしておく必要があります。その後、2つの素数（p und q）は不要になります。

暗号化されたメッセージを受信すると、最初の（n）と3番目の番号（d）を使用して復号化できます。受信者だけが鍵の両方の部分、つまり公開鍵と秘密鍵を知っています。残りの世界は公開鍵しか知りません（n und e）。

RSAアルゴリズムの秘訣は、公開鍵部分（nとe）から秘密鍵部分（d）を計算できないため、メッセージを復号化できないことです。これは、dを持つ人だけがメッセージを復号化できるためです。

149

Gpg4win Compendium 3.0.0

第25章GnuPGと多数の謎

**25.3。少数のRSA暗号化**

メソッドがどのように機能するかを示すために、最初は小さな数値を使用します。ただし、実際にははるかに大きい複数桁の素数が使用されます。

RSAアルゴリズムに従って、素数7と11を取り、それらを使用して、数値、またはコンピューターにとって同一の文字を暗号化します。

まず公開鍵を作成します

**最初の数値**は77で、2つの素数7と11の乗算の積です。77は後で暗号化および復号化プロセスの係数として使用されます。

**2番目の数値**は、公開指数です。この例では、番号13 を選択しました。

**3番目の数字**は秘密鍵です。この数は次のように計算されます。

最初に、素数7と11（したがって7 1と11 1）のそれぞれから1を差し引き、結果の2つの数値を乗算して60を取得します。（7 1）（11 1）=60。60は、秘密鍵のさらなる計算（ただし、実際の係数77と混同しないでください）。

次に、モジュール60を使用するときに、公開鍵を掛けたときに数値1になる数値を探します。

13 mod 60？mod 60 = 1 mod 60

この要件を満たす唯一の数は37です。

13 mod 60 37 mod 60 = 481 mod 60 = 1 mod 60

37は、モジュール60を使用して13を掛けると1になる唯一の数です。

150

Gpg4win Compendium 3.0.0

第25章GnuPGと多数の謎

**公開鍵でメッセージを暗号化する**

暗号化と復号化の両方がモジュール77（素数7と11から得られた積）を使用するため、メッセージを0から76までの一連の数値、つまり77の数値に分割します。

これらの数値はそれぞれ、77を法とする算術演算のように、13倍されます。

注意：13は公開鍵です。

2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 = 2 13= 8192 = 30 mod 77 であるため、30に変換された数値2を使用した例を考えてみましょう。

別の例：75は47に変換されます。これは、75が13倍されて77で除算され、残りの47が残るためです。

この計算を0〜76のすべての数値に使用し、結果をテーブルに挿入すると、次のようになります。

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | 0 | 1 | 2 | ３ | 4 | 5 | 6 | 7 | 8 | 9 |
|  |  | |  |  |  |  |  |  |  |  |  |
| 0 |  | 0 | 1 | 30 | 38 | 53 | 26日 | 62 | 35 | 50 | 58 |
| 10 |  | 10 | 11 | 12 | 41 | 49 | 64 | 37 | 73 | 46 | 61 |
| 20 |  | 69 | 21 | 22 | 23 | 52 | 60 | 75 | 48 | 7 | 57 |
| 30 |  | 72 | ３ | 32 | 33 | 34 | 63 | 71 | 9 | 59 | 18 |
| 40 |  | 68 | 6 | 14 | 43 | 44 | 45 | 74 | 5 | 20 | 70 |
| 50 |  | 29日 | 2 | 17 | 25 | 54 | 55 | 56 | 8 | 16 | 31 |
| 60 |  | 4 | 40 | 13 | 28 | 36 | 65 | 66 | 67 | 19 | 27日 |
| 70 |  | 42 | 15 | 51 | 24 | 39 | 47 | 76 |  |  |  |

表25.1 .:

左の列は10の倍数を示し、上の行は単位を示します。

151

Gpg4win Compendium 3.0.0

第25章GnuPGと多数の謎

**秘密鍵を使用してメッセージを解読する**

数値2を使用して上記の例を逆にするには、つまりメッセージをデコードするには、30（変換された2）を37倍します（30 37）。結果はモジュール番号77を使用して計算されます。覚えておいてください：37は秘密鍵です。

この繰り返し乗算の結果は2 mod 77になります。他の例：数値47 mod 77は数値75 mod 77にデコードされます。

表25.2は、0〜76の77個の数値の正確な割り当てを示しています。

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | 0 | 1 | 2 | ３ | 4 | 5 | 6 | 7 | 8 | 9 |
|  |  | |  |  |  |  |  |  |  |  |  |
| 0 |  | 0 | 1 | 51 | 31 | 60 | 47 | 41 | 28 | 57 | 37 |
| 10 |  | 10 | 11 | 12 | 62 | 42 | 71 | 58 | 52 | 39 | 68 |
| 20 |  | 48 | 21 | 22 | 23 | 73 | 53 | 5 | 69 | 63 | 50 |
| 30 |  | 2 | 59 | 32 | 33 | 34 | 7 | 64 | 16 | ３ | 74 |
| 40 |  | 61 | 13 | 70 | 43 | 44 | 45 | 18 | 75 | 27日 | 14 |
| 50 |  | 8 | 72 | 24 | 4 | 54 | 55 | 56 | 29日 | 9 | 38 |
| 60 |  | 25 | 19 | 6 | 35 | 15 | 65 | 66 | 67 | 40 | 20 |
| 70 |  | 49 | 36 | 30 | 17 | 46 | 26日 | 76 |  |  |  |

表25.2。秘密鍵を使用した77を法とする数値変換37

表25.2を使用して数値を変換するには、表25.1と同じ方法を使用します。例：60は行60と列0の数値に変換されます。したがって、60は25に変換されます。

表25.1を使用して25の変換の結果が60になると想定する場合、これは当然のことですが、表25.2を使用する場合、60の変換で25を取得する必要があるのは当然です。その際、数値を変換（コード化）するために公開鍵13を使用し、プロセスを逆にする、つまり復号化するために秘密鍵37を使用しました。暗号化プロセスと復号化プロセスの両方にモジュロ77演算を使用しました。

152

Gpg4win Compendium 3.0.0

第25章GnuPGと多数の謎

**エグゼクティブサマリー**

あなたが持っている ...

コンピューターを使用して2つのランダムな素数を作成しました。

これらの番号から製品とパブリックおよびプライベートサブキーの両方を作成しました。公開鍵を使用してメッセージを暗号化しました。

秘密鍵を使用してメッセージを復号化しました。

選択された2つの素数は非常に大きいため、既知の製品でそれらを解読することは不可能です。これは、RSAアルゴリズムのセキュリティの基礎です。

単純な例を使用した場合でも、計算が非常に複雑になる可能性があることを確認しました。この場合、キーを公開した人は、77と13を公開キーとして公開しています。この情報を使用すると、表25.1の例のように、誰でもこの方法で、上記の方法を使用して一連の暗号化された一連の番号を送信できます。暗号化された一連の番号の意図された受信者は、番号77と秘密鍵37を使用してこれらをデコードできます。

もちろん、このような単純な例では、77が7と11の積であることは明らかであるため、特に安全な暗号化は保証されません。

その結果、この単純な例のコードを解読するのはかなり簡単でしょう。目の肥えた読者は、数字の11とその倍数（22、33など）などの一連の数字があり、隣接する数字がそれ自体に変換されることにも気づくでしょう。

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | ３ | 4 | 5 | 6 | 7 | 8 | 9 |
|  |  |  |  |  |  |  |  |  |  |  |
| 0 | 0 | 1 | 51 | 31 | 60 | 47 | 41 | 28 | 57 | 37 |
| 10 | 10 | 11 | 12 | 62 | 42 | 71 | 58 | 52 | 39 | 68 |
| 20 | 48 | 21 | 22 | 23 | 73 | 53 | 5 | 69 | 63 | 50 |
| 30 | 2 | 59 | 32 | 33 | 34 | 7 | 64 | 16 | ３ | 74 |
| 40 | 61 | 13 | 70 | 43 | 44 | 45 | 18 | 75 | 27日 | 14 |
| 50 | 8 | 72 | 24 | 4 | 54 | 55 | 56 | 29日 | 9 | 38 |
| 60 | 25 | 19 | 6 | 35 | 15 | 65 | 66 | 67 | 40 | 20 |
| 70 | 49 | 36 | 30 | 17 | 46 | 26日 | 76 |  |  |  |

表25.3：

153

Gpg4win Compendium 3.0.0

第25章GnuPGと多数の謎

これは、この暗号化方式のさらなる弱点のようです。これにより、アルゴリズムのセキュリティが制限されると考えられます。ただし、ランダムに選択された2つの大きな素数の積が次のようになると想像してください。

114,381,625,757,888,867,669,235,779,976,146,612,010、

218,296,721,242,362,562,561,842,935,706,935,245,733、

897,830,597,123,563,958,705,058,989,075,147,599,290、

026,879,543,541

この例では、開始の素数を識別できなくなりました。その結果、公開鍵を使用して秘密鍵を判別することは非常に困難です。世界で最も速いコンピュータでさえ、2つの素数を計算することは非常に困難です。したがって、必要なのは、実際に決定するためのすべての既知の方法を阻止するのに十分な大きさの素数を選択することだけです。さらに、上に25.1と25.2で示したように、それ自体に変換される数の比率は、素数が大きくなるにつれて連続的に減少します。

実際に暗号化に使用する範囲の素数のうち、この部分は非常に小さく、RSAアルゴリズムはそれによって決して制限されません。

素数が大きいほど、暗号化の安全性が高くなります。通常のPCでは、2つの大きな素数から製品を取得することは難しくありません。ただし、世界中のどのコンピュータも、この製品から元の素数を導き出すことはできません。少なくとも予見可能な将来はそうではありません。

154

Gpg4win Compendium 3.0.0

第25章GnuPGと多数の謎

**25.4。異なる基数を使用して表示**

メッセージがどのように暗号化されるかを理解するには、コンピュータが数値を保存する方法、そして何よりも、メッセージが多くの異なる数値ベースでどのように表現されるかを知っている必要があります。

この目的のために、まず数値の力を見てみましょう。

2のように表示される1つの電源には、2つ、1= 2。

2の3乗。23= 2 2 2 = 8 と表示されます。

2の10乗。210= 2 2 2 2 2 2 2 2 2 2 2 = 1024 と表示されます。

ゼロの累乗の各数値は1に等しく、たとえば2 0= 1および5 0= 1です。より一般的に言えば、数値は、累乗の数で示される回数だけそれ自体で乗算されることを意味します。

数値ベースの概念は、車両の走行距離計の例でも見ることができます。右輪は、既知のシーケンスに従って、各キロメートルの後に次の数値までカウントされます：0、1、2、3、4、5。 6、7、8、9、0、1、2、...

右のホイールが0に達するたびに、左のホイールが1レベルずつカウントアップします。そして、この2番目のホイールが0に達するたびに、その左側のホイールも1つずつ上がります。。。等々。

右輪は1キロを数えます。8をマークすると、8キロを意味します。左側のホイールは、10 kmごとに表示されます。5は50 kmを意味します。これに100のインジケータが続きます。7は700キロメートルを意味します。

同じ原則を使用して、0〜9の数字を持つ通常の数値を示します。

たとえば、「578」は5 100 + 7 10 + 8を意味し、578に対応します。

ここには、500を表す「5」、70を表す「7」、8を表す「8」があります。この場合、ベースは10です。

したがって、右側の数字は特定の数値の「単位」を表し（つまり、1を乗算）、左側の数字は「十」（つまり、10を掛けたもの）を表し、次の数字は「数百」（つまり、掛けたもの）を表します

100）など。通常、10の基底を使用して数値を表すため、底を個別に示す必要はありません。より正式なレベルでは、これは55 の数値として55 10と示され、ベースは添え字の番号で表されます。

10の基数を使用していない場合は、対応する添え字を使用して、関連する番号を示す必要があります。

0〜8の数字を使用する代わりに、オドメーターインジケーターには0〜7の数字のみが含まれていると仮定します。したがって、右のホイールは各キロメートルの後で1レベルずつカウントし続け、結果の数値シリーズは次のようになります。

0; 1; 2; 3; 4; 5; 6; 7; 0; 1; 2; :::

155

Gpg4win Compendium 3.0.0

第25章GnuPGと多数の謎

たとえば、底が8の3桁の走行距離計は、次の数値を表します。

356

右輪の6は1キロメートルを数えるので、6 8 0= 6キロメートルになります。

横にあるホイールの5は5 8 1、つまり40キロを表します。

その左の3つは、1回転あたり64キロメートルごとに相当します。この例では、3 8 2キロメートルです。

これは、8を基にして数値を計算する方法です。例：72 8は7 8 1+2 8 0= 58を表します。

この図では、72の「2」は2を表しますが、「7」は7 8を表します。

数値が大きくなると、同じ方法で徐々に組み立てられるため、453 8は実際には4 64 + 5 8 + 3を表し、299 10tになります。

453 8の場合、「3」は3を意味し、「5」は5 8を意味し、「4」は4 64を意味するため、「64」は8 8から派生します。

上記の例では、数字は左から右に8の累乗で乗算されます。右側の数字は8 0（つまり1）で乗算され、左側の数字は8 1（つまり8）で乗算され、左側の数字は8 2（つまり64）で乗算されます。

10を底とする数値を表す場合、9よりも大きい数字はありません（つまり、10から1を引いたもの）。したがって、10以上の数字を表す数字はありません。10を表すには、「10」を書き込むための2桁が必要です。

したがって、0〜9の数字しかありません。

基数8で計算する場合もほぼ同じです。使用可能な数字は0〜7のみです。この基数を使用して7より大きい数を表す場合は、再度2桁を使用する必要があります。例えば、9 10は、11である8、73 10が111である8。

156

Gpg4win Compendium 3.0.0

第25章GnuPGと多数の謎

コンピュータは、一連の0と1として数値を格納します。これは、2進数を使用したバイナリシステムまたは算術と呼ばれます。0と1の数字のみを使用しているためです。0と1の2桁しかないホイールの走行距離計でキロメートルを数えることを想像してください。したがって、バイナリシステムを使用して、たとえば、番号10101 2は次のようになります

1 2 4+0 2 3+1 2 2+0 2 1+1 2 0= 1 16 + 0 8 + 1 4 + 0 2 + 1 = 21

8桁の2進数のグループもコンピュータ技術で使用されます-よく知られた「バイト」。1バイトは、0からバイト00000000 2として表される値および255- バイト11111111 2として表される値のいずれかで構成されます。したがって、1バイトは2 8= 256を底とする数を表します。

さらに2つの例：

10101010 2= 170

00000101 2= 5

コンピュータは文字、数字、記号をバイトとして保存するので、256を底とする表現が果たす役割を見てみましょう。

157

Gpg4win Compendium 3.0.0

第25章GnuPGと多数の謎

音節「うん」を取ろう。コンピュータは「u」を117として、「n」を110として格納します。

これらの数値はすべてのコンピューターで標準であり、ASCIIコードと呼ばれます。

次の番号で音節「un」を表すこともできます。

117 2 8 1+ 110 2 8 0= 117 256 + 110 = 30062

したがって、文字列「und」は数字で表されます。

117 2 8 2+ 110 2 8 1+ 100 2 8 0= 117 65536 + 110256 + 100 = 7695972

「d」は100で表されるため。

したがって、10を基数として2 8= 256を基数とする通常の数値としてコンピューターキーボードで使用できる内部的に表現された数値と記号を使用しています。

したがって、すべてのメッセージを大きな数に変えることができます。長いメッセージは非常に大きな数につながり、RSAアルゴリズムで暗号化したいと考えています。

ただし、メッセージが暗号化される数が素数（モジュラス）の積より大きくならないようにする必要があります。そうしないと、以下に示すように問題が発生します。

次のプロセスはいくつかのステップで構成されているため、まず要約してから、個々のステップを順番に調べてみましょう。

1. 上記のように、メッセージaba、cad、acaは数値に変換されます。

1. たとえば2 2= 4（2 8= 256 ではなく）の基底を使用するこの表現は、10の基底を使用する表現に変換されるので、暗号化の目的で表25.1を使用できます。これは、10の基準を使用してコード化されたメッセージを作成します。

1. コーディングを認識するには、「クリアテキスト」と比較して、10の基準を使用してコーディングされたメッセージを4の基準に戻し、文字シーケンスに戻します。

1. これにより、メッセージaba、cad、acaが暗号化されたメッセージdbb、ddd、dacに変わります。

158

Gpg4win Compendium 3.0.0

第25章GnuPGと多数の謎

そして今、詳細に：

1. メッセージaba、cad、adaを数字に変換します。

これを使用してメッセージを4つの文字a、b、c、dに制限すると仮定します。これは非常に単純な例です。たとえば、4つの文字を0、1、2、3の数値で表すことができます。

a = 0; b = 1; c = 2 und d = 3

次に、メッセージaba、cad、acaを暗号化します。素数7と11を使用してメッセージをエンコードし、公開鍵77と13および関連する秘密鍵37を使用します。この章は、前の章の次の例ですでによく知られています。これを使用して、表25.1および25.2を作成しました。

1. 基底4を使用するこの表現は、基底10を使用する表現に変換されます。これを行うには、暗号化の目的で表25.1を使用できます。これも、基底10の数値を使用します。

メッセージに4文字を使用しているので、4の基準を使用して計算します。モジュロ77計算では、メッセージを3桁ずつに分割する必要があります。4の基準を使用する最大の3桁の数値は333 4。10の基準を使用すると、この数値の値は63になります。

代わりに、メッセージを4文字ずつに分割する場合、3333 4は76 10の値を超え、不要なあいまいさが発生します。

結果として、3桁のメッセージは次のようになります。

アバ; cad; アカ

次に、数値を文字に割り当てます。ピースが4の基底を使用して3桁の数値を表すことを忘れないでください。

a = 0、b = 1、c = 2、d = 3の数字で文字を表しているため、結果のメッセージは次のようになります。

010 4; 203 4; 020 4

10の基底を使用して、このメッセージは4、35、8のシーケンスで表されます。なぜですか。

たとえば、中間部分203 4を考えます。

|  |  |  |
| --- | --- | --- |
| 3 4 0; また3 1; | | また3： |
| 0 4 1; | また0 4; | また0： |
| 2 4 2; | また2 16; | また32： |

159

Gpg4win Compendium 3.0.0

第25章GnuPGと多数の謎

1. 暗号化のために、基底fo 10を使用して計算された151ページの表25.1を使用できるようになりました。この表は、すでにおなじみのキーペアを使用しているために使用します。これにより、10を基準としてコード化されたメッセージが作成されました。

メッセージを暗号化するには、前述の表25.1を使用します。メッセージは、53、63、50（10の基準）の番号シーケンスに変わります。

1. 基底を4に戻すと、メッセージは311 4になります。333 4; 302 4。これを文字シーケンスに変換すると、dbb、ddd、dacが作成されます。これは、元のメッセージとは非常に異なります。

したがって、プロセスを逆にして、表25.2を使用して番号シーケンス53、63、50を変換し、シーケンス4、35、8を取得します。これは、元のメッセージに正確に対応しています。

表25.1および25.2を使用すると、秘密鍵を使用してメッセージを暗号化することもできます（たとえば、最初に表25.2を使用し、次に公開鍵（つまり、表25.1）でデコードして、元の番号を復元します）。これにより、秘密鍵の所有者はRSAアルゴリズムを使用してメッセージを暗号化できるようになり、メッセージは自分からしか送信できないことが証明されます。

160

Gpg4win Compendium 3.0.0

第25章GnuPGと多数の謎

**一番下の行は...**

....このプロセスは詳細が複雑ですが、一方で、原則はかなり簡単です

理解する。結局のところ、メソッドを信頼するだけでなく、少なくともその背後にあるアプローチの理解に基づいて、その動作モードの背後を確認できるようにする必要があります。その他の詳細の多くは、他の書籍（zB：R. Wobst、「Abenteuer Kryptologie」）またはインターネットで簡単に見つけることができます。

いずれにせよ、あなたが知っていることです：誰かが暗号化された電子メールを解読しようとする場合、プロセスはそれらを長い間ビジー状態に保ち、彼らが実際にあなたのメッセージを読むことに興味を失うでしょう。。。...

161

**パートIII。**

**別館**

162

1. **GpgOL Outlook拡張機能に関する情報**

GpgOLはMicrosoft Outlookのプログラム拡張です。GnuPGの操作をOutlookに統合します。

Outlookはプロプライエタリ製品であるため、ソースコード付きのフリーソフトウェアとしては利用できません。この統合には、まだ多くの問題があります。言い換えると、暗号化と署名のコンポーネントが統合された電子メールプログラム（KMail / Kontactなど）で提供される操作ほど快適ではありません。

GpgOLはGpg4winインストールアシスタントによってインストールされます。Outlookの次回の起動時に、メニュー

Extras！OptionsにはGpgOLタブが含まれます。

163

Gpg4win Compendium 3.0.0

付録A. GpgOL Outlook拡張機能に関する情報

GpgOLタブは3つの領域に分かれています。

1. 一般情報：S / MIMEサポートを有効にする

Gpg4winがインストールされると、S / MIME機能がGpgOLでアクティブになります。これは、GnuPGのS / MIMEサポートを指します。Outlook自体もX.509とS / MIMEをサポートしていますが、Gpg4winコンポーネントのGnuPGでは動作しません。つまり、すべての設定、証明書管理、ユーザーダイアログが異なります。Outlook自体はOpenPGPサポートを提供しないことにも注意してください。

OutlookのGpg4winでS / MIMEを使用する場合は、GpgOL-Option Activate S / MIME supportをアクティブのままにしておきます。OutlookでサポートされているS / MIMEを使用する場合は、このGpgOL S / MIMEオプションを無効にします。

1. メッセージの送信：

デフォルト設定で新しいメッセージを暗号化するデフォルト設定で新しいメッセージに署名する

これらの2つのオプションは、新しいメッセージを暗号化するか、デフォルト設定で署名するかを制御します。メッセージの作成時にこれらの設定を変更することもできます。それに応じてボタンのみがアクティブになります。

1. メッセージを読む：

可能な場合はHTML表示を表示する

このオプションは、メッセージのHTMLバージョンを表示するために使用できます。通常、またはHTML形式が利用できない場合、メッセージはテキスト形式で表示されます。

暗号化されたメッセージを添付ファイルとして表示

メッセージの暗号化された部分も添付ファイルとして表示されます。つまり、ユーザーは暗号化された部分を個別に保存したり、別の方法で処理したりできます。

すべてのオプションは、新規インストール後にすでに事前入力されています。

164

Gpg4win Compendium 3.0.0

付録A. GpgOL Outlook拡張機能に関する情報

Outlookを使用して暗号化されたメッセージを送信するには、Microsoft Wordを使用してメッセージを作成しないようにする必要があります。

また、HTMLメッセージを使用しないことをお勧めします。

これらの項目は、[電子メールの形式]タブのメニュー項目[その他！オプション]で制御できます。メッセージ形式はテキストのみに設定する必要があります（強調表示された領域を参照）。ただし、署名または暗号化された電子メールにHTMLを引き続き使用する場合は、メッセージが受信者に届くまでにフォーマット情報が失われる可能性があります。

注意：Gpg4winのプログラム拡張GpgOLを使用すると、Outlook 2003/2007のOpenPGP標準に従って電子メールを処理できます。

WindowsXPおよびOutlook 2003では、Gpg4winを使用すると、Outlook 2007でAES暗号化S / MIME電子メールを復号化および作成することができます。これは、Gpg4winがGnuPGとともに、OutlookおよびWindowsに依存しない独自の暗号化コンポーネントをもたらすためです。Windows VistaのOutlook 2007のみが、Gpg4winなしでAES暗号化S / MIME電子メールを処理できます。

165

**B.他の電子メールプログラムでGnuPGを使用する**

Gpg4winの概要では、主にOutlookの電子メールプログラムを調べます。ただし、GnuPGは他のすべての電子メールプログラムでも使用できます。ただし、ユーザーの快適性には大きな違いがあります。GnuPGが電子メールプログラムに統合されているほど、使いやすくなります。

電子メールプログラムがGnuPGについて何も知らない場合など、最も簡単な方法は、Kleopatraの支援を得て、クリップボードを使用して暗号化することです。これはOpenPGPでのみ機能します。S / MIMEおよび複雑なPGP / MIME電子メールの場合、中間ストレージをファイルとして使用する必要があります。両方の方法は、この概要の最初の部分で説明されています。

現在、GnuPGの統合は、Windowsの以下の電子メールプログラムに提供されています。

**サンダーバード**とEnigmailの1。

**Outlook 2003**とGpgOL **のバージョン2003**。GpgOLはGpg4winパッケージの一部です。

**Claws Mail：**この電子メールプログラムはGpg4winパッケージの一部であり、オプションでインストールできます。このようなインストールでは、PGP / MIMEおよびS / MIMEを使用するためのプログラム拡張がすでに構成されています。ただし、この拡張機能はKleopatraを使用しないため、GpgOL Outlook拡張機能が提供するのと同じ快適さを現在提供していません。

**KMail / Kontact：**KMailとKontactは、GnuPGの快適で実績のある統合を提供します。彼らは、WindowsとMacOSのX.のためにも、最近では、ほぼすべてのGNU / Linuxシステムのために利用可能と

1[http://www.thunderbird-mail.de/wiki/Enigmail\_OpenPGP](https://translate.google.com/translate?hl=ja&prev=_t&sl=auto&tl=ja&u=http://www.thunderbird-mail.de/wiki/Enigmail_OpenPGP)

166

**C. Gpg4winの自動インストール**

この章では、自動インストール（ユーザーダイアログなし）について説明します。

ソフトウェア共有システムなど、場合によっては、ダイアログを使用した対話なしでGpg4winのインストールが機能する必要があります。ただし、すべてのインストール設定を事前に定義するために、Gpg4winはコマンドラインでのインストールパスとその他のオプションの構成、および制御ファイルをサポートしています。

インストールパスは、オプション/ D = <PFAD> で指定できます。これは、コマンドラインの最後のオプションとして送信する必要があります。ファイル名（ここではgpg4win.exe ）はバージョンによって異なる場合があります。コマンドラインで情報を入力するときに大文字を使用するか小文字を使用するかに関係なく、違いがあります。必要に応じて、アクセス権（例：読み取りと書き込み）をインストールフォルダで構成することもできます。例：

gpg4win.exe / D = D：\ Programme \ Gpg4win

オプション/ S を使用すると、インストールは「サイレント」で実行されるため、ダイアログは表示されません。他のパラメータが設定されていない場合、すべてのデフォルト設定が採用されます。

Gpg4winは、いわゆる制御ファイルもサポートしています。オプション/ C = <INIFILE> を使用して、制御ファイルを入力できます（名前は通常.iniで終わります）。

もう一つの例：

gpg4win.exe / S /C=C:\TEMP\gpg4win.ini

この.ini ファイルには、セクションが1つだけ含まれている必要があります[gpg4win] 。ここには、インストールする構成ファイルの絶対パス情報など、さまざまな設定を行うことができます。相対パス、つまり現在の作業ディレクトリに依存するパスは、ここには入力できません。絶対パスには、ドライブ名を含む完全なパスが含まれています。通常、デフォルト設定を使用しない場合は、設定を入力する必要があります。このルールの例外は、次のページの例に記載されています。

167

Gpg4win Compendium 3.0.0

付録C. Gpg4winの自動インストール

これは、すべての許可されたキーワードを表示する制御ファイルの内容の例です。

[gpg4win]

; インストール設定。除外するか空のままにする

; デフォルトの設定

inst\_gpgol = true

inst\_gpgex = true

inst\_kleopatra = true

inst\_gpa = true

inst\_claws\_mail = false

inst\_compendium = true

; リンケージを準備する場所。inst\_start\_menu = true

inst\_desktop = false

inst\_quick\_launch\_bar = false

; 他のオプションとは異なり、このオプションは上書きします

; インストールアシスタントでのユーザーの設定

inst\_start\_menu\_folder = Gpg4win

; 標準構成ファイル。gpg.conf = D：\ config \ gpg-site.conf

gpg-agent.conf = D：\ config \ gpg-agent-site.conf trustlist.txt = D：\ config \ trustlist-site.txt dirmngr.conf = D：\ config \ dirmngr-site.conf dirmngr\_ldapserver.conf = D：\ config \ dirmngr\_ldapserver-site.conf scdaemon.conf = D：\ config \ scdaemon-site.txt

gpa.conf = D：\ config \ gpa-site.conf

制御ファイルgpg4win.ini とインストールパスD：\ Programme \ Gpg4win を使用した自動インストールの対応する要求は、次のようになります。

gpg4win.exe / S /C=C:\TEMP\gpg4win.ini / D = D：\ Programme \ Gpg4win

168

**D.他のプログラムからの転送**

このセクションでは、他のGnuベースのプログラムからGpg4winに転送する方法について説明します。インストールプログラムはこれらのプログラムの一部を認識し、その場合は警告を表示します。

一般に、Gpg4winをインストールする前に、別のGnuPGベースのプログラムの既存のインストールを削除することをお勧めします。インストールプロセスの前に、既存の証明書をバックアップすることが重要です。

これを行うための本当に意味のある唯一の方法は、古いプログラムで利用可能なオプションを使用することです。プライベート証明書をバックアップするためのメニュー項目と、すべての既存のパブリック証明書をバックアップするためのメニュー項目を検索します。次に、それらを1つ以上のファイルにバックアップします。

Gpg4winをインストールしたらすぐに、古い証明書がすでに存在しているかどうかを確認します。これは、KleopatraまたはGPA証明書マネージャーを使用して行うことができます。証明書がすでに存在する場合、古い暗号化システムはすでに証明書の保存場所に関する新しい規則に対応しており、他に何もする必要はありません。

ただし、古い証明書が表示されない場合は、バックアップコピーからインポートしてください。第19章をお読みください。

古い暗号化システムがGPA証明書マネージャーを使用している場合は、このプログラムが提供するバックアップオプションを使用できます。Gpg4winのGPAバージョンの機能と非常によく似ているはずです。

古い証明書を見つける方法が見つからない場合は、Windowsダッシュボードツールを使用して、secring.gpg およびpubring.gpg という名前のファイルを検索し、Kleopatra 1を使用してこれら2つのファイルをインポートしてください。

1これは公式の方法ではありませんが、現在のすべてのGnuPGバージョンで動作します。

169

Gpg4win Compendium 3.0.0付録D.他のプログラムからの転送

**Gpg4win-1.1.xからGpg4win-2.xへの移行**

Gpg4win-2.xをインストールする前に、まずGpg4win-1.1.xをアンインストールすることを強くお勧めします。

**技術的背景**

Gpg4win-1.1.xのアンインストールを含まない移行の問題は、次の順序で強調されています。

1. バージョンXを含むGpg4winのインストール。コンポーネントK.

* 1. バージョンX + 1でのGpg4winのインストール。ただし、コンポーネントKは選択解除されています。結果：古いKコンポーネントはバージョンXにインストールされたままになります。

* 1. バージョンX + 1のGpg4winのアンインストール。

結果：バージョンXのコンポーネントKは「孤立」のままです。

これは、最初のバージョン以降のGpg4winの制限です。

コメント1：1.1.xから2.xに切り替えると、特定のコンポーネントK（GpgEEなど）が存在しないため、このケースは常に発生し、したがって（自動的に）選択解除されたと見なす必要があります。

コメント2：MSIの場合、Windowsは使用されなくなったコンポーネントを削除するタスクを想定しています。これは、上記のシナリオでMSIインストールアシスタントが正しく動作することを意味します（バージョンXの古いコンポーネントKは、手順2の後、オペレーティングシステムに存在しなくなります）。

170

**E. Gpg4winのアンインストール**

Gpg4winをアンインストールする場合は、最初に、不要な他のすべてのアプリケーションをシャットダウンし、すべての証明書をバックアップする必要があります。権限が制限されたコンピューターで作業している場合は、削除を行うために管理者権限で登録する必要があります。ユーザーアカウントを使用してインストールが既に実行されている場合は、管理者権限が付与されています。

重要：

アンインストールプロセスを開始する前に、すべてのGpgOL情報のGpgOLで処理された電子メールをOutlookで「クリーンアップ」することを強くお勧めします。理由：Gpg4win / GpgOLは、Outlookの各暗号メールに特定のマーカーを設定します。プログラムをアンインストールする前にこのマーカーをリセットする必要があります。これにより、他の暗号化ソフトウェアが後で電子メールを正しく読み取って暗号化できるようになります。

この再移行の目的で、GpgOLはOutlookで次の機能を使用できるようにします。電子メールをリセットするOutlook電子メールフォルダーを選択し、[その他]をクリックします。このフォルダからGpgOL機能を削除します。

GpgOLはシャットダウンされます（後続の削除プロセスのため）。[はい]をクリックして、GpgOLマーキングの各フォルダーの電子メールをクリーンアップするかどうかを確認します。次に、すべてのOutlookフォルダーに対してこのコマンドを実行します。

すべてのフォルダをリセットしたら、Gpg4winのアンインストールを開始できます。

プログラムをアンインストールする方法は3つあります。

Microsoft Windowsのダッシュボードツールの使用：

スタート！設定！コントロールパネル！ソフトウェアを開き、GnuPG for Windowsを選択します。

[削除]をアクティブにすると、オペレーティングシステムからすべてのGpg4winプログラムコンポーネントがアンインストールされます。

Gpg4winをアンインストールする別の方法は、exeファイルgpg4win-uninstall.exe を使用することです。このファイルはGpg4winで提供され、インストールフォルダー（通常はC：nProgrammenGNUnGnuPGn ）にあります。インストールプロセス中にデフォルトのパスとは異なるパスを選択した場合、対応する場所に削除プログラムが表示されます。

このexeファイルは、Gpg4winのスタートメニューにもあります。

171

Gpg4win Compendium 3.0.0

付録E. Gpg4winのアンインストール

3つのケースすべてで、すべてのGpg4winファイルは、インストールフォルダー、およびスタートメニュー、デスクトップ、クイックスタートバーのリンクから削除されます。

以下の構成設定を持つユーザー固有のシステム全体のアプリケーションファイルフォルダーは削除されません。

ユーザー固有のGnuPGアプリケーションデータ

に％APPDATA％\ GnuPGは、一般的にファイルフォルダに対応しています。

C：\ Documents and settings \ <Benutzername> \ Application data \ gnupg \

このgnupg ファイルフォルダーには、すべての個人GnuPG情報が含まれているため、プライベート証明書、信頼設定、プログラム構成が含まれています。

システム全体のGnuPGアプリケーションデータ

中％COMMON\_APPDATA％\ GNU 、通常、ファイルフォルダに対応しています。

C：\ Documents and settings \ All Users \ Application data \ GNU \

**Gpg4win-1.1.3のアンインストール**

Gpg4win-1.1.3をアンインストールすると、次のファイルフォルダーまたはレジストリキーが残ります。

ファイル名：

％APPDATA％ngnupg （Gpg4win2インストールで引き続き使用されます。）

重要：ここには、個人のプライベート証明書とパブリック証明書、およびGnuPG設定があります。

レジストリキー：

HKLMnSoftwarenGNUnGnuPG （もはや使用され、「インストール=。Gpg4win2によって）HKCUnSoftwarenGNUnGPG4Win （もはや使用Gpg4win2で」インストール=。）HKCUnSoftwarenGNUnGpgOL （もはや使用Gpg4win2で「インストール=。）HKCUnSoftwarenGPGee （もはや使用Gpg4win2で」=インストール。）

172

1. **歴史**

「GnuPPfürEinsteiger」、第1版2002年3月および「GnuPPfürDurchblicker」、第1版2002年3月、作者：Manfred J. Heinze、TextLabテキスト+メディアコンサルタント：Lutz Zolondz、GNU GmbHイラスト：Karl Bihlmeier、Bihlmeier＆Kramer GbRレイアウト：Isabel Kramer、Bihlmeier＆Kramer GbRテクニカルテキスト：Dr. Francis Wray、e-mediate Ltd.編集者：Ute Bahn、TextLab text + media

出版社：BundesministeriumfürWirtschaft und Technologie（BMWi）[http://www.gnupp.de/pdf/einsteiger.pdf](https://translate.google.com/translate?hl=ja&prev=_t&sl=auto&tl=ja&u=http://www.gnupp.de/pdf/einsteiger.pdf)und [http://www.gnupp.de/pdf/durchblicker.pdfから](https://translate.google.com/translate?hl=ja&prev=_t&sl=auto&tl=ja&u=http://www.gnupp.de/pdf/durchblicker.pdf)入手でき[ます](https://translate.google.com/translate?hl=ja&prev=_t&sl=auto&tl=ja&u=http://www.gnupp.de/pdf/durchblicker.pdf)。

TextLab text + mediaの非公開バージョンを改訂しました。

「Gpg4winfürEinsteiger」および「Gpg4winfürDurchblicker」、2005年12月改訂：Werner Koch、g10 Code GmbH

パブリッシャー：Gpg4win Initiative

2007年11月14日付のBMWiの承認のおかげで、変更不可の「Impres-sum」セクションが削除され、現在のバージョンに適応されました。

「Gpg4win Compendium」は「Gpg4winfürEinsteiger」と「Gpg4winfürDurch-blicker」を組み合わせたもので、2009年から2010年の間にGpg4win2向けに包括的に更新および補足されています。

主な改訂：

Werner Koch、g10 Code GmbH

フロリアン対サムソン、情報技術（BSI）のSideserheit Bundesamt EmanuelSchütze、Intevation GmbH

Jan-Oliver Wagner博士、Intevation GmbH

ドイツ語原文から英語に翻訳：Brigitte Hamilton（[http://www.linguaetc.com](https://translate.google.com/translate?hl=ja&prev=_t&sl=auto&tl=ja&u=http://www.linguaetc.com)）

Gpg4winプログラムパッケージとGpg4win Compendiumは、[http](https://translate.google.com/translate?hl=ja&prev=_t&sl=auto&tl=ja&u=http://www.gpg4win.org)：//www.gpg4win.orgで入手できます[。](https://translate.google.com/translate?hl=ja&prev=_t&sl=auto&tl=ja&u=http://www.gpg4win.org)

173

**G. GNU Free Documentation License**

バージョン1.2、2002年11月

Copyright c 2000,2001,2002 Free Software Foundation、Inc.

51 Franklin St、Fifth Floor、Boston、MA 02110-1301 USA

誰もがこのライセンスドキュメントをそのままコピーして配布することが許可されていますが、変更することはできません。

前文

このライセンスの目的は、マニュアル、教科書、またはその他の機能的で有用なドキュメントを自由の意味で「無料」にすることです。商業的または非営利的に、変更の有無にかかわらず、すべての人にコピーと再配布の効果的な自由を保証することです。 。第二に、このライセンスは、作者と出版社が彼らの作品の功績を認める方法を保持しますが、他人が行った変更について責任を負うものではありません。

このライセンスは一種の「コピーレフト」です。つまり、ドキュメントの派生物自体も同じ意味で自由でなければなりません。これは、フリーソフトウェア用に設計されたコピーレフトライセンスであるGNU General Public Licenseを補完します。

無料のソフトウェアには無料のドキュメントが必要なので、無料のソフトウェアのマニュアルに使用するためにこのライセンスを設計しました。無料のプログラムには、ソフトウェアと同じ自由を提供するマニュアルが付属している必要があります。ただし、このライセンスはソフトウェアマニュアルに限定されません。主題や印刷された本として発行されているかどうかに関係なく、あらゆるテキスト作業に使用できます。このライセンスは、主に目的が指示または参照である作品に推奨します。

1.適用性と定義

このライセンスは、著作権者がこのライセンスの条件に基づいて配布できることを示す通知を含む、あらゆる媒体のあらゆるマニュアルまたはその他の作品に適用されます。そのような通知は、本書に記載された条件の下でその作品を使用するための、期間無制限の全世界的なロイヤルティフリーライセンスを付与します。以下の「ドキュメント」は、そのようなマニュアルまたは著作物を指します。一般のメンバーはいずれもライセンシーであり、「あなた」と呼ばれます。著作権法に基づく許可が必要な方法で作品をコピー、変更、または配布する場合は、ライセンスを受け入れます。

ドキュメントの「変更されたバージョン」とは、ドキュメントまたはその一部を含む、逐語的にコピーされた、または変更された、および/または別の言語に翻訳された作品を意味します。

「二次セクション」は、ドキュメントの発行者または作成者とドキュメントの関係を排他的に扱う、ドキュメントの名前付き付録または前書きセクションです。

174

Gpg4win Compendium 3.0.0

付録G. GNU Free Documentation License

全体的な主題（または関連事項）を含み、その全体的な主題に直接該当する可能性のあるものは何も含まれていません。（したがって、ドキュメントが部分的に数学の教科書である場合、二次セクションは数学を説明しない場合があります。）関係は、主題との歴史的関連または関連事項、あるいは法的、商業的、哲学的、倫理的の問題である可能性があります。またはそれらに関する政治的立場。

「不変セクション」とは、ドキュメントがこのライセンスに基づいてリリースされたという通知で、不変セクションのタイトルとしてタイトルが指定されている特定のセカンダリセクションです。セクションが上記のセカンダリの定義に適合しない場合、そのセクションを不変として指定することはできません。ドキュメントには、不変セクションが含まれない場合があります。ドキュメントが不変セクションを識別しない場合は、何もありません。

「カバーテキスト」は、ドキュメントがこのライセンスに基づいてリリースされたという通知に、フロントカバーテキストまたはバックカバーテキストとして記載されている特定の短い文章です。フロントカバーテキストは最大5ワード、バックカバーテキストは最大25ワードにすることができます。

ドキュメントの「透明な」コピーとは、一般的なテキストエディタまたは（ピクセルで構成される画像の場合）汎用ペイントでドキュメントを直接修正するのに適した、仕様が一般に公開されている形式で表された機械可読コピーを意味しますプログラムまたは（図面の場合）広く利用可能ないくつかの図面エディター。テキストフォーマッターへの入力や、テキストフォーマッターへの入力に適したさまざまな形式への自動変換に適しています。マークアップまたはマークアップの欠如がリーダーによるその後の変更を阻止または阻止するように調整されている、それ以外の場合は透明なファイル形式で作成されたコピーは透明ではありません。かなりの量のテキストに使用される場合、画像フォーマットは透過的ではありません。「透明」でないコピーは「不透明」と呼ばれます。

トランスペアレントコピーに適した形式の例には、マークアップのないプレーンASCII、Texinfo入力形式、LaTeX入力形式、公的に利用可能なDTDを使用したSGMLまたはXML、および人間による変更用に設計された標準準拠の単純なHTML、PostScriptまたはPDFがあります。透明な画像形式の例には、PNG、XCF、JPGなどがあります。不透明なフォーマットには、プロプライエタリなワードプロセッサのみが読み取りおよび編集できるプロプライエタリなフォーマット、DTDおよび/または処理ツールが一般に利用できないSGMLまたはXML、および一部のワードプロセッサによって生成された機械生成のHTML、PostScriptまたはPDFが含まれます。出力目的のみ。

「タイトルページ」とは、印刷された本の場合、タイトルページ自体と、このライセンスがタイトルページに表示されるために必要な資料を適切に保持するために必要な次のページを意味します。タイトルページのない形式の作品の場合、「タイトルページ」とは、テキストの本文の先頭に先行する、作品のタイトルの最も目立つ外観に近いテキストを意味します。

「Entitled XYZ」というセクションは、タイトルが正確にXYZであるか、XYZを別の言語に翻訳するテキストに続く括弧内にXYZを含む、ドキュメントの名前付きサブユニットを意味します。（ここでXYZは、「謝辞」、「献辞」、「裏書」、または「履歴」など、下記の特定のセクション名を表します。）ドキュメントを変更するときにそのようなセクションの「タイトルを保持する」とは、ドキュメントを変更することを意味します。この定義によれば、「権利が付与されたXYZ」セクションのままです。

ドキュメントには、このライセンスがドキュメントに適用されることを示す通知の横に保証免責事項を含めることができます。これらの保証の免責事項は、参照により本ライセンスに含まれると見なされますが、免責の保証に関してのみです。これらの保証の免責事項が持つ可能性のあるその他のいかなる意味も無効であり、本ライセンスの意味には影響しません。

175

Gpg4win Compendium 3.0.0

付録G. GNU Free Documentation License

2.逐語的コピー

このライセンス、著作権表示、およびこのライセンスがドキュメントに適用されることを示すライセンス表示がすべてのコピーに複製され、他の条件を追加しないことを条件として、商業的または非営利的に、ドキュメントをコピーして配布することができます。このライセンスのものに。作成または配布するコピーの読み取りまたはそれ以上のコピーを妨害または制御するための技術的手段を使用することはできません。ただし、コピーと引き換えに補償を受け入れることはできます。十分な数のコピーを配布する場合は、セクション3の条件にも従う必要があります。

また、上記と同じ条件でコピーを貸与し、コピーを公開することもできます。

3.数量でのコピー

100を超えるドキュメントの印刷されたコピー（または通常カバーが印刷されているメディアのコピー）を発行し、ドキュメントのライセンス通知にカバーテキストが必要な場合、これらのコピーを明確かつ判読できるようにカバーでカバーする必要があります。表紙テキスト：表紙の表紙テキスト、裏表紙の裏表紙テキスト。どちらのカバーも、これらのコピーの発行者であることを明確かつ読みやすいように識別する必要があります。表紙は、タイトルのすべての単語が等しく目立つように表示された完全なタイトルを提示する必要があります。カバーに他の素材を追加することもできます。変更をカバーに限定してコピーすると、ドキュメントのタイトルが保持され、これらの条件を満たす限り、他​​の点では逐語的なコピーとして扱うことができます。

どちらかの表紙に必要なテキストが大きすぎて読みにくい場合は、最初にリストされているテキストを（適度に多く）実際の表紙に配置し、残りを隣接するページに続けます。

100を超える番号のドキュメントの不透明なコピーを公開または配布する場合は、機械で読み取り可能な透明なコピーを各不透明なコピーと共に含めるか、または各不透明なコピーに、一般的なネットワークからのコンピューターネットワークの場所を記載する必要があります。パブリックを使用すると、パブリックスタンダードのネットワークプロトコルを使用して、ドキュメントの完全な透明なコピーをダウンロードできます。追加の資料は不要です。後者のオプションを使用する場合は、不透明コピーの大量配布を開始するときに、この透明なコピーが指定された場所にアクセスできるように、最後に配布してから少なくとも1年経過するまで、慎重に対処する必要があります。そのエディションの不透明なコピー（直接またはエージェントまたは小売業者を介して）を一般に公開します。

大量のコピーを再配布する前に、ドキュメントの作成者に連絡して、ドキュメントの更新版を提供する機会を与えることが要求されますが、必須ではありません。

4.修正

上記のセクション2および3の条件に基づいて、ドキュメントの修正バージョンをコピーして配布することができます。ただし、修正版を本ライセンスに基づいてリリースし、修正バージョンがドキュメントの役割を満たしている場合は、ドキュメントの修正版の配布および修正が可能です。変更されたバージョンは、そのコピーを所有するすべてのユーザーに適用されます。さらに、変更バージョンでは次のことを行う必要があります。

176

Gpg4win Compendium 3.0.0

付録G. GNU Free Documentation License

1. タイトルページ（およびカバーがある場合は表紙）で、ドキュメントのタイトルと、以前のバージョン（存在する場合は、ドキュメントの[履歴]セクションにリストされている必要があります）とは異なるタイトルを使用します。以前のバージョンの元の発行者が許可した場合、以前のバージョンと同じタイトルを使用できます。

1. タイトルページに、著者として、変更バージョンでの変更の作成に責任を持つ1人以上の人物またはエンティティ、およびドキュメントの主要著者のうち少なくとも5人（すべての主要著者、 5）、彼らがあなたをこの要件から解放しない限り。

1. タイトルページに、変更されたバージョンの発行者の名前を発行者として記載します。

1. ドキュメントのすべての著作権表示を保持します。

1. 他の著作権表示に隣接して、変更に適切な著作権表示を追加します。

1. 以下の補遺に示されている形式で、著作権の通知の直後に、このライセンスの条件に基づいて変更バージョンを使用することを公に許可するライセンス通知を含めます。

1. ドキュメントのライセンス通知に記載されているインバリアントセクションと必要なカバーテキストの完全なリストをそのライセンス通知に保存してください。

1. このライセンスの変更されていないコピーを含めます。

1. 「履歴」というタイトルのセクションを保持し、そのタイトルを保持し、少なくともタイトルページで指定された変更されたバージョンのタイトル、年、新しい著者、および発行者を示す項目を追加します。ドキュメントに「履歴」というタイトルのセクションがない場合は、タイトルページに示されているように、ドキュメントのタイトル、年、著者、および発行者を記載したセクションを作成し、前の文で述べたように変更バージョンを説明するアイテムを追加します。

1. ドキュメントの透明なコピーへのパブリックアクセスのためにドキュメントで指定されたネットワークロケーションを保持します。同様に、以前のバージョンのドキュメントで指定されたネットワークロケーションを保持します。これらは「履歴」セクションに配置できます。ドキュメント自体の少なくとも4年前に公開された作品のネットワークロケーションは省略できます。または、ドキュメントが参照するバージョンの元の公開者が許可を与えている場合は省略できます。

1. 「謝辞」または「献身」と題されたセクションについては、セクションのタイトルを保持し、セクション内で提供された各貢献者の謝辞および/または献身のすべての内容および調子をセクションに保存します。

1. テキストとタイトルは変更せずに、ドキュメントのすべての不変セクションを保持します。セクション番号または同等のものは、セクションタイトルの一部とは見なされません。

1. 「推奨」というタイトルのセクションを削除します。このようなセクションは、変更バージョンに含まれていない場合があります。

1. 既存のセクションのタイトルに「推奨」というタイトルを付けたり、タイトルが不変セクションと競合したりしないでください。

1. 保証の免責事項を保持します。

変更されたバージョンに、副次的なセクションとしての資格があり、ドキュメントからコピーされた資料が含まれていない新しいフロントマターセクションまたは付録が含まれている場合、オプションでいくつかを指定できます。

177

Gpg4win Compendium 3.0.0

付録G. GNU Free Documentation License

または不変としてこれらのセクションのすべて。これを行うには、変更されたバージョンのライセンス通知の不変セクションのリストにタイトルを追加します。これらのタイトルは、他のセクションのタイトルとは異なる必要があります。

「承認」というタイトルのセクションを追加できます。このセクションには、さまざまな関係者による変更バージョンの承認以外は含まれていません。たとえば、査読の声明や、テキストが標準の信頼できる定義として組織によって承認されている場合などです。

変更バージョンのカバーテキストのリストの最後に、フロントカバーテキストとして最大5ワードのパッセージ、バックカバーテキストとして最大25ワードのパッセージを追加できます。フロントカバーテキストの1つのパッセージとバックカバーテキストの1つのパッセージのみが、1つのエンティティによって（またはそれによって行われた取り決めを通じて）追加できます。ドキュメントにすでに同じカバーのカバーテキストが含まれている場合、以前にユーザーが追加した場合、またはユーザーが代理を務めているのと同じエンティティが作成した取り決めによって追加された場合は、別のカバーを追加できません。ただし、古いものを追加した以前の発行元からの明示的な許可を得れば、古いものを置き換えることができます。

ドキュメントの作成者および発行者は、このライセンスでは、変更されたバージョンの宣伝のために、またはそれらを主張または暗示するために、それらの名前を使用することを許可しません。

5.文書の結合

元のすべてのドキュメントのすべての不変セクションを組み合わせて変更せずにリストし、それらをすべてリストすることを条件に、変更されたバージョンについて上記セクション4で定義された条件に基づいて、ドキュメントをこのライセンスに基づいてリリースされた他のドキュメントと組み合わせることができます。ライセンス通知での組み合わせ作業の不変セクションとして、およびそれらのすべての保証免責事項を保持すること。

結合された作業には、このライセンスの1つのコピーのみが含まれる必要があり、複数の同一の不変セクションを1つのコピーに置き換えることができます。同じ名前で内容が異なる不変セクションが複数ある場合は、そのセクションの最後にかっこ内に、そのセクションの元の作成者または発行者の名前（わかっている場合）、または一意の番号。組み合わせ作品のライセンス通知の不変セクションのリストにあるセクションタイトルに同じ調整を行います。

組み合わせでは、さまざまな元のドキュメントの「履歴」というタイトルのセクションを結合して、「履歴」というタイトルの1つのセクションを形成する必要があります。同様に、「謝辞」というタイトルのセクションと「献身」というタイトルのセクションを組み合わせます。「推奨」というタイトルのセクションをすべて削除する必要があります。

6.文書のコレクション

お客様は、このライセンスに基づいてリリースされたドキュメントおよびその他のドキュメントで構成されるコレクションを作成し、さまざまなドキュメント内のこのライセンスの個々のコピーを、コレクションに含まれる1つのコピーに置き換えることができます。他のすべての点での各ドキュメントの逐語的コピー。

このようなコレクションから単一のドキュメントを抽出し、このライセンスに基づいて個別に配布することができます。ただし、抽出したドキュメントにこのライセンスのコピーを挿入し、そのドキュメントの逐語的コピーに関する他のすべての点でこのライセンスに従います。

7.独立した作業の集約

178

Gpg4win Compendium 3.0.0

付録G. GNU Free Documentation License

ストレージまたは配布メディアのボリューム内またはボリューム上での、ドキュメントまたはその派生物と他の個別の独立したドキュメントまたは作品の編集物は、編集物に起因する著作権が法的権利を制限するために使用されていない場合、「集合体」と呼ばれます。個々の作品が許可する範囲を超えた編集のユーザーの。ドキュメントが集合体に含まれている場合、本ライセンスは、それ自体がドキュメントの派生物ではない集合体の他の作品には適用されません。

セクション3のカバーテキスト要件がこれらのドキュメントのコピーに適用される場合、ドキュメントが全体の半分未満である場合、ドキュメントのカバーテキストは、ドキュメントを集約内で囲むカバーに配置するか、またはドキュメントが電子形式の場合、カバーの電子的同等物。それ以外の場合は、骨材全体を囲む印刷されたカバーに表示する必要があります。

8.翻訳

翻訳は一種の修正と見なされるため、セクション4の条件に基づいてドキュメントの翻訳を配布できます。インバリアントセクションを翻訳に置き換えるには、著作権者からの特別な許可が必要ですが、一部またはすべてのインバリアントセクションの翻訳を含めることができます。これらの不変セクションの元のバージョン。このライセンスの原文の英語版とこれらの通知および免責事項の元のバージョンも含めることを条件として、このライセンスの翻訳、およびすべてのライセンス通知をドキュメントに含めることができます。翻訳とこのライセンスの元のバージョン、または通知または免責事項の間に不一致がある場合は、元のバージョンが優先されます。

ドキュメントのセクションに「謝辞」、「献身」、または「履歴」というタイトルが付いている場合、タイトルを維持するための要件（セクション4）（セクション1）は、通常、実際のタイトルを変更する必要があります。

9.終了

このライセンスの下で明示的に規定されている場合を除き、ドキュメントをコピー、変更、サブライセンス、または配布することはできません。ドキュメントをコピー、変更、サブライセンス、または配布するその他の試みは無効であり、このライセンスに基づくお客様の権利は自動的に終了します。ただし、このライセンスに基づいてお客様からコピーまたは権利を受け取った当事者は、完全に準拠している限り、ライセンスが終了することはありません。

10.このライセンスの将来の改訂

Free Software Foundationは、GNU Free Documentation Licenseの新しい改訂版を随時公開することがあります。そのような新しいバージョンは、精神的には現在のバージョンと似ていますが、新しい問題や懸念に対処するために詳細が異なる場合があります。http://www.gnu.org/copyleft/を参照してください。

ライセンスの各バージョンには、区別するバージョン番号が付与されています。ドキュメントに、このライセンスの特定の番号付きバージョン「またはそれ以降のバージョン」が適用されると記載されている場合、その指定されたバージョンまたは公開されたそれ以降のバージョンのいずれかの契約条件に従うオプションがあります（ドラフト）は、Free Software Foundation ドキュメントでこのライセンスのバージョン番号が指定されていない場合は、Free Software Foundationによって（ドラフトとしてではなく）発行された任意のバージョンを選択できます。

179

Gpg4win Compendium 3.0.0

付録G. GNU Free Documentation License

補遺：このライセンスをドキュメントに使用する方法

作成したドキュメントでこのライセンスを使用するには、ドキュメントにライセンスのコピーを含め、タイトルページの直後に以下の著作権およびライセンス通知を記載します。

Copyright c YEAR YOUR NAME。GNU Free Documentation License、バージョン1.2、またはFree Software Foundationによって発行されたそれ以降のバージョンの条件に基づいて、このドキュメントをコピー、配布、または変更する許可が与えられます。不変セクション、表紙テキスト、裏表紙テキストはありません。ライセンスのコピーは、「GNU Free Documentation License」というタイトルのセクションに含まれています。

インバリアントセクション、フロントカバーテキスト、バックカバーテキストがある場合は、「with ... Texts」を置き換えます。これに合わせて：

不変セクションはLIST THEIR TITLES、フロントカバーテキストはLIST、バックカバーテキストはLISTです。

カバーテキストのない不変セクションがある場合、または3つの他の組み合わせがある場合は、状況に合わせてこれら2つの選択肢をマージします。

ドキュメントにプログラムコードの重要な例が含まれている場合は、GNU General Public Licenseなどの選択したフリーソフトウェアライセンスの下でこれらの例を並行してリリースし、フリーソフトウェアでの使用を許可することをお勧めします。

180

**インデックス**

ASCII鎧、107、115、123非対称暗号化、22、24認証、28、41、81認証インスタンス、81認証、28自動インストール、167

BundesamtfürSicherheit in der Informationstechnik、10

BundesministeriumfürWirtschaft und Technologie、10

CAcert、55

証書

認証、77

CA、67、126

チェーン、67、131

作成、41

詳細、98

エクスポート、60、103、123

インポート、72、103、124

公共、58

リクエスト、52

選択、84

ユーザーID、98

有効性、98

証明書管理、9証明書管理、42認証局（CA）、29、54、81証明書発行者、29

証明書失効リスト、126、132、134証明書サーバー、100

OpenPGP、100

証明書の検索、103

セットアップ、101

X.509、100

信頼の連鎖28

小切手

GpgOLによる署名、92

Claws Mail、9、166

対応秘密、13

CRL、「証明書失効リスト」を参照

CryptoEx、129

暗号化、9

サービス拒否、100

診断レベル、142

ディレクトリマネージャー、DirMngrを参照

DirMngr、126、130、132、133、140

Eメール

暗号化された形式のアーカイブ、95

復号化、68

暗号化、82

暗号化および署名、94

サイン、86

エシェロンシステム、12

添付ファイルの暗号化、104

Enigmail、166

封筒、11

有効期限、98

ファイル

署名の確認、110

復号化、118

暗号化、114

サイン、106

指紋、48、76

フリーソフトウェア、9

GNU FDL、174–180

GNU Free Documentation License、GNU FDLを参照

GNUプライバシーアシスタント、GPA GnuPG、9を参照

GnuPG for Outlook、GpgOLを参照

GnuPP、41、173

GPA、9

GPG Explorer eXtension、GpgEXを参照

181

Gpg4win Compendium 3.0.0

付録G. GNU Free Documentation License

|  |  |  |
| --- | --- | --- |
| GpgEX、9、105 | プラグイン、163 |  |
| GpgOL、9 | パスフレーズ、25 |  |
| GpgOLオプション、164 |  |
| PGP、10 |  |
|  |  |
| 階層的信頼概念、28 | ピネントリー、89 |  |
| HTTP、126、134 | 素数、149–159 |  |
| インストール、30 | プロキシ、102、126、134 |  |
| 「公開鍵」方式、14、18 |  |
| 整合性、106 |  |
|  |  |
| キー | GpgOLの再移行、171 |  |
| 残留クラス、146 |  |
| 作成、41 |  |
| ルート証明書、126、131、133、135、136 |  |
| ID、48、98 |  |
| RSAアルゴリズム、144–161 |  |
| ペア、17、24、41、122 |  |
|  |  |
| プライベート、23 | S / MIME、10、28 |  |
| 公共、23 | セキュリティ哲学、143 |  |
| 鍵サーバー、証明書サーバーを参照 | 署名 |  |
| クレオパトラ、9、42 | 壊れた、93 |  |
| KMail、166 | デジタル、86 |  |
| Kontact、166 | 資格のある電子、86 |  |
| LDAP、100、126、134 | 署名法、86 |  |
| 署名法、81 |  |
| ログファイル、137 |  |
| 対称暗号化、16、19 |  |
| DirMngr、140 |  |
|  |  |
| GnuPG、141 | 電気通信の秘密、13 |  |
| GpgME、142 | サンダーバード、166 |  |
| GpgOL、139 | トロイの木馬、25 |  |
| クレオパトラ、138 | トラブルシューティング、128 |  |
| メールの秘密、13 | trustlist.txt、135、136 |  |
| 信頼できるルート証明書、126、133、136 |  |
| メールボックス、19、22、28 |  |
|  |  |
| Gpg4winからの移行、170 | アンインストール、171 |  |
| モジュロ演算、145 | ウイルス、25 |  |
| 「非公開鍵」方式、対称を参照 |  |
|  |  |
| 暗号化 | Web of Trust、29、80 |  |
| OpenPGP、10、28 | Windows-Explorer、9 |  |
| ワーム、25 |  |
| 証明書の作成、44 |  |
|  |  |
| OSCP、126 | X.509、10、41 |  |
| Outlook、68、128、166 | 証明書の作成、50 |  |

182

Google 翻訳

**原文**

The Gpg4win Compendium

翻訳を改善する