JPCERT CC®

はじめての暗号化メール(Thunderbird 編)

一般社団法人 **JPCERT** コーディネーションセンター

2012 年 **8** 月 **29** 日

目次

1　はじめに

電子メールで情報交換を行う際に、改ざんされていないことを確認したり、第三者への漏洩を防いだりするため、インシデントや脆弱性の取扱においては、伝統的に PGP（Pretty Good Privacy/プリティー グッド プライバシーの略）による電子署名や暗号化が利用されています。

本書は、初めて PGP を使用する方々のための、PGP のインストールから PGP を使ったメッセージ交換までをカバーするガイドブックです。本書では、PGP を使用した暗号化や電子署名が付されたメールを、「PGP メール」と表します。なお、PGP は、種々の環境で利用できますが、本書では、Microsoft Windows 上で動作している Thunderbird の電子メール利用環境を前提として説明します。

本書の 2 章では PGP の概要や構成を、3 章では使用方法を説明します。なお、本書では、初心者が PGP をインストールし、基本機能を利用するために欠かせない事項だけに説明を絞り込んでいます。本書でカバーしていない暗号方式や暗号アルゴリズムなどの詳細については RFC4880 の情報を参照してください。

RFC 4880: OpenPGP Message Format
https://tools.ietf.org/html/rfc4880

参考：　PGP/OpenPGP とは

PGP は、個人のプライバシーを守る目的で 1990 年頃に Philip R. Zimmermann（フィリップ R. ジマーマン）氏により開発された暗号ソフトウエアです。PGP は、機密性の高い情報などを交換するための暗号化（および復号）の機能と、発信した情報が改ざんされていないことを検証する為の電子署名（および電子署名の検証）の機能を備えています。その後、PGP（バージョン 5.x）の仕組みをもとにして「OpenPGP Message Format」（RFC 2440；2007 年に更新され、最新版は RFC 4880）が定義されました。

2　PGP メールの概要

2.1　暗号化と電子署名

PGP は、暗号化（および復号化）や電子署名（および電子署名の検証）などの機能を実現しています。PGP の利用者は、あらかじめ PGP の秘密鍵と PGP の公開鍵からなる一対の鍵（PGP の鍵ペアと呼ぶこともあります。）を各自が作成し用意します。PGP の秘密鍵（以下、秘密鍵といいます。）や PGP の公開鍵（以下、公開鍵といいます。）には、誰の鍵かを容易に特定するための「ユーザ ID」の情報が含まれます。ユーザ ID は、名前、メールアドレス、コメントといった項目から構成されます（PGP の鍵ペアの作成方法は 3.3.1 で説明します）。

PGP を利用して電子メールを暗号化すれば、送信者（図 1 の A さん）が「指定」した受信者（図 1 の B さん）のみが電子メールの本文や添付ファイルの内容を見えるようにできます。もし、第三者が盗聴したとしても、暗号化された解読しがたいデータしか見ることができません。送信者が To または CC フィールドで指定した受信者の公開鍵を用いて暗号化が施されます。送信者が受信者の公開鍵を持っている必要があります。メールを暗号化して送る方法は 3.4.1 で、また、PGP メールを復号する方法については、3.5.1 で説明します。

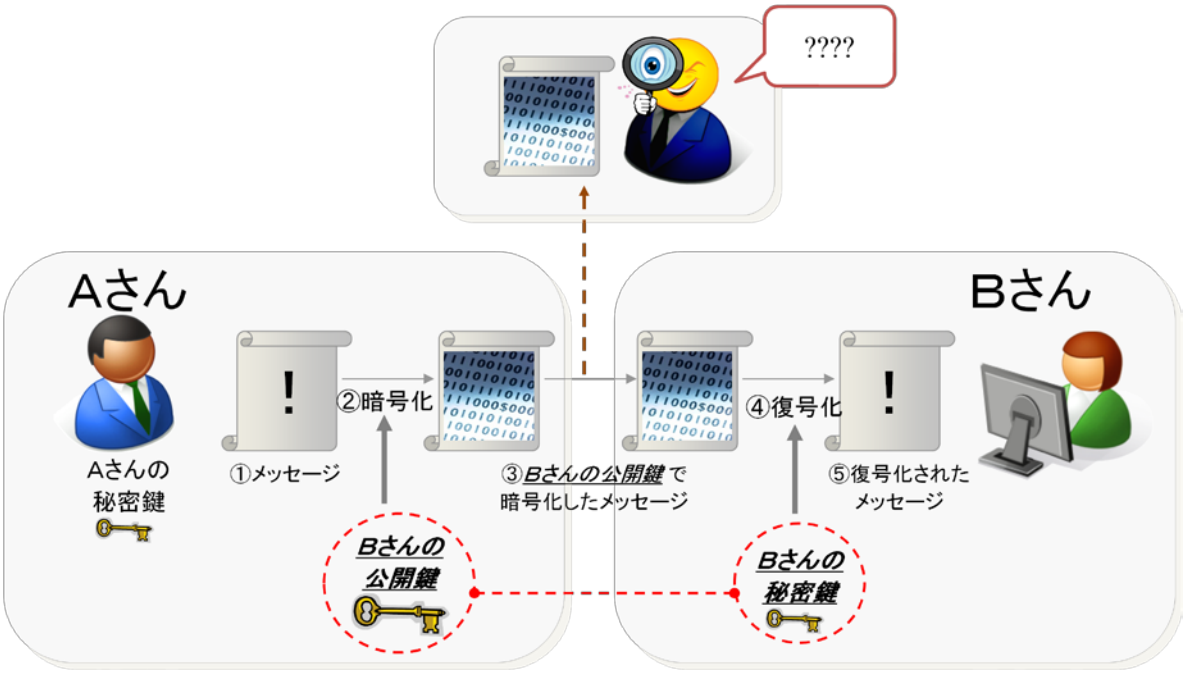

図 1. PGP メール（暗号化）のイメージ

発信者が電子メールに自分の秘密鍵を使って電子署名を付していれば、それを送った人が本当に送信者（図 2 の A さん）であり、当該電子メール（本文や添付ファイル）が第三者によって改ざんされていな

いことを、受信者（図 2 の B さん）が確認できます。こうした確認を検証と言います。受信者が電子署名を検証するには、発信者が電子署名に用いた秘密鍵に対応する公開鍵をもっている必要があります。電子署名を付ける方法については 3.4.2 で、また、PGP メールの電子署名を検証する方法については 3.5.2 でそれぞれ説明します。なお、電子署名を付しただけのメールは、盗聴などされると第三者も内容を見ることができます。それを防ぎたい場合には、電子署名を付すとともに暗号化も施します。

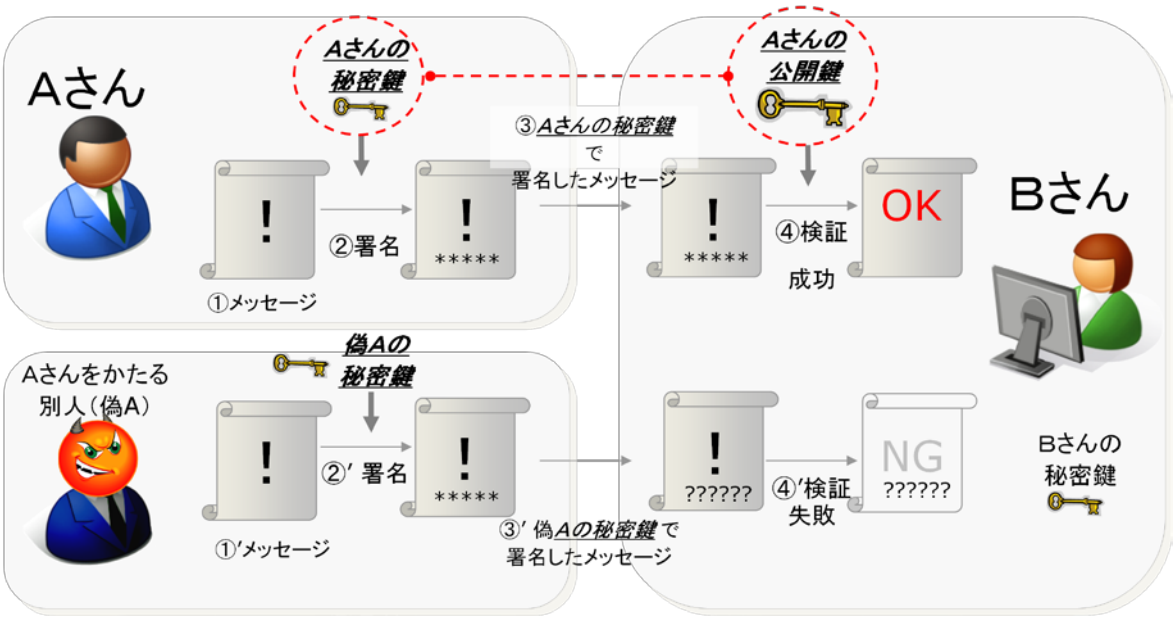

図 2. PGP メール（電子署名）のイメージ

上述のように、PGP メール（暗号化）を送ったり、電子署名を検証したりするためには、相手の公開鍵をあらかじめ入手しておく必要があります。自分の公開鍵を相手に渡したり、相手の公開鍵を受け取ったりすることを、「鍵を交換する（鍵交換）」と呼びます。交換した公開鍵が正しくなかった場合には、暗号化メールや電子署名の検証結果も意味をなしません。したがって、鍵交換に際して、確かに相手の公開鍵であることを十分に確認しなければなりません。具体的な公開鍵の確認方法は、3.3.2 を参照してください。

公開鍵とは異なり、秘密鍵は誰にも知られないように管理しなければなりません。万一、自分の秘密鍵が他人の手に渡れば、自分だけしか読めないはずの暗号化メールを見られたり、自分に成りすました電子署名付きメールを作られたりする可能性が生じます。秘密鍵が他人に漏れた（またその可能性がある）場合は、自分の PGP の鍵ペアを失効し、鍵交換を行った相手にも失効証明書を配布しなければなりません。PGP の鍵ペアの失効方法については、3.6 で説明します。なお、失効証明書は、悪用されると他人に公開鍵を失効される危険性がありますので、必要な時のみ配布するようにしてください。

自分自身の PGP の鍵ペアや鍵交換により受け取った相手の公開鍵については、自分の「キーリング（鍵束）」に登録します。キーリングとは鍵を管理するデータベースです。公開鍵をキーリングのファイルに

登録することで、相手の公開鍵の詳細情報（ユーザ ID やフィンガープリントなど）を表示したり、鍵の状態を変更（鍵の失効や無効化）したりできます。キーリングへのインポートや公開鍵の情報を表示する方法については 3.3.2 で説明します。

2.2　ソフトウエア構成

電子メールソフトに、PGP ソフトウエアと関連するアドオンを追加することにより、PGP メールを使用できるようになります。PGP ソフトウエアを電子メールソフトと連携させるために橋渡しするアドオンは、PGP ソフトウエアによっては本体に組み込まれている場合があります。

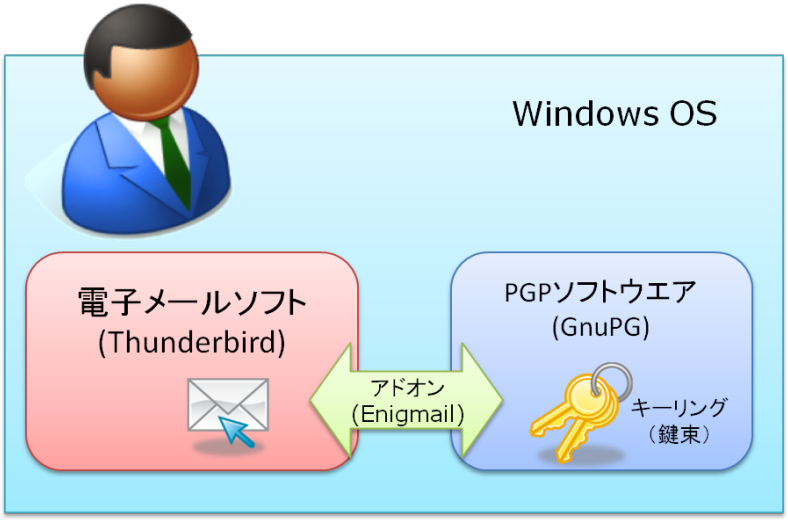

図 3. ソフトウエア構成

表 1 構成の対応表

PGP ソフトウエア	GnuPG
電子メールソフト	Thunderbird
アドオン	Enigmail ※ Enigmail は Thunderbird に GnuPG の機能を連携させるためのアドオンです)

PGP を使用できるソフトウエアは、有償製品から GPL ライセンスに準拠した無料で利用できるものまで、複数の選択肢があります。本書では、表 1 の組合せで利用するケースについて説明します。この組合せは、これまで 10 年以上の利用実績があり、定期的にメンテナンスも行われています(2012 年 8 月現在)。電子メールソフトとして Thunderbird を使用している方は、この組合せでの利用をお勧めします。

3 GnuPG を使った PGP の使用方法

3.1 本章の構成

3 章では、Microsoft Windows 上で動作している Thunderbird の電子メール利用環境に GnuPG をインストールし、PGP メールのメッセージ交換をするまでの手順を説明します。

3.2 では、GnuPG と Enigmail のインストールの手順について説明します。3.3 では、PGP の鍵ペアを作成する手順と、公開鍵、秘密鍵の管理について説明します。3.4、3.5 では、PGP メールの送信、受信の手順について説明します。3.6 では、PC がマルウェアに感染したり、秘密鍵を誤って配布してしまったりした際に行う失効の手順について説明します。

なお、3.2 のインストールは、初回時のみ作業を行い、3.3～3.6 については、必要に応じてその都度操作を行います。

以下の説明では、表 2 の環境を使用しています。

表 2. 環境（バージョン）の一覧

OS	Windows 7 SP1
PGP ソフトウエア	GnuPG 1.4.12
電子メールソフト	Thunderbird 14.0
アドオン	Enigmail 1.4.4

3.2 GnuPG および Enigmail のインストール

3.2.1 GnuPG のインストール

GnuPG の最新のインストール用ファイル（gnupg-w32cli-1.4.12.exe が 2012 年 8 月時点の最新です）を次のサイトからダウンロードしてください。

Download - GnuPG.org
ftp://ftp.gnupg.org/gcrypt/binary/
http://www.ring.gr.jp/pub/net/gnupg/binary/

ダウンロードした GnuPG のインストール用のファイルを実行します（GnuPG のインストールには管理

者権限が必要です)。GnuPG のインストール時のインストールオプションはデフォルトのままで特に変更する必要はありません。

3.2.2 Enigmail のインストール

Thunderbird を起動して、Thunderbird のメニュー「ツール（T)」の「アドオン（A)」から「アドオンマネージャ」の画面（図 4）を表示します。右上の検索ボックスに「Enigmail」と入力してアドオンを検索します。表示された Enigmail の「インストール」のボタンをクリックします（Enigmail は、Thunderbird のバージョンによってインストールすべき Enigmail のバージョンが異なります[8]。アドオンマネージャを使用すれば、適切なバージョンの Enigmail が自動的に選択されます)。

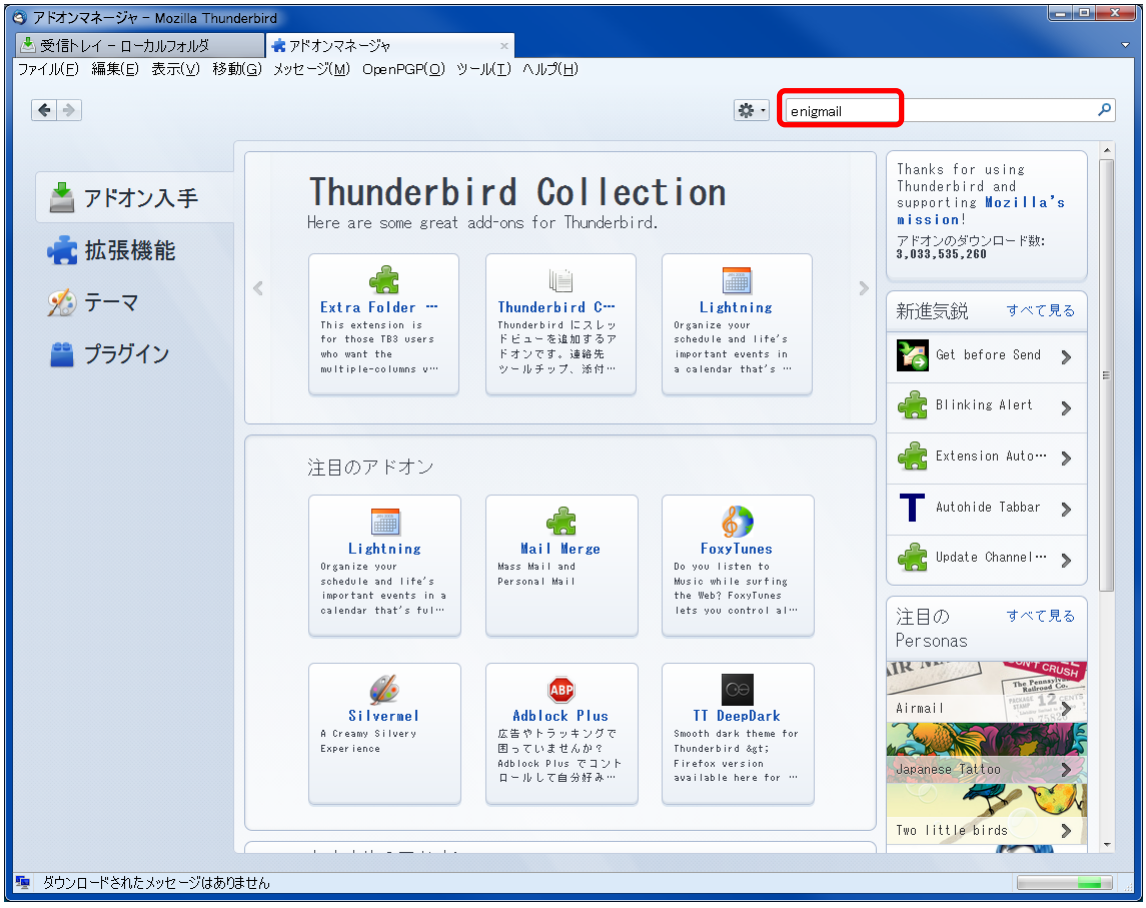

図 4. Thunderbird アドオンマネージャ

Thunderbird でアドオンを追加したことが無い場合は、次のサイトを参考にしてください。

Thunderbird サポート　拡張機能のインストール
http://mozilla.jp/thunderbird/support/kb/002609

カスタマイズ | 使い方ガイド | Thunderbird サポート
http://mozilla.jp/thunderbird/support/tutorials/customize#custom-useaddons

Enigmail のアドオンインストール後に Thunderbird を再起動してください。再起動すると Thunderbird のメニューに「OpenPGP（O)」が追加され、このメニューを通じて Enigmail が利用できるようになります。

3.3 PGP の鍵ペアの作成と管理

3.3.1 PGP の鍵ペア（公開鍵、秘密鍵）の生成

(1) PGP の鍵ペアを生成するために、Thunderbird の「OpenPGP（O)」の「鍵の管理（Y)」をクリックし、表示された「OpenPGP の鍵の管理」（図 **5**）画面の「生成 （G)」->「新しい鍵（K)」をクリックします。

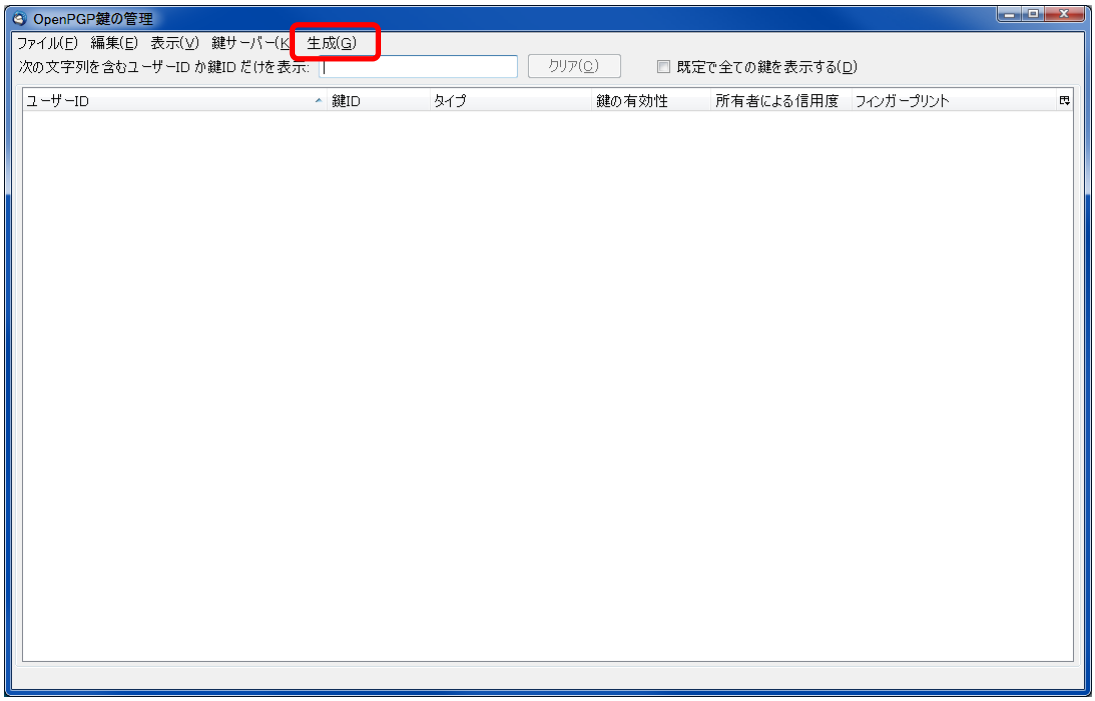

図 5. OpenPGP 鍵の管理画面

表示された「OpenPGP 鍵の生成」（図 **6**）画面で PGP の鍵ペアを作成するアカウント/ユーザ ID（メールアドレス）を選択し、パスフレーズと、鍵の有効期限、中段の「詳細」タブの暗号鍵長（bit)、暗号アルゴリズムを指定します（本章の説明では「pgp-memo@jpcert.or.jp」の仮の電子メールアドレスをアカウント・ユーザ ID として指定しています)。「暗号鍵長（bit)」については、2048 以上を

選択してください。また、「パスフレーズ無し」をチェックしないようにしてください。

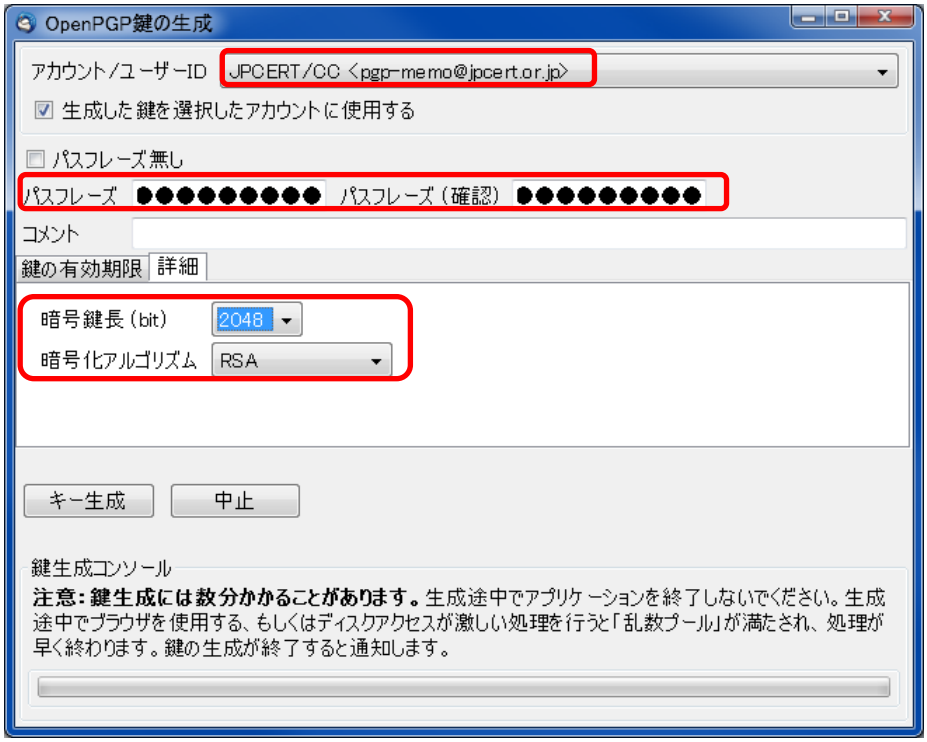

図 6. OpenPGP 鍵の生成画面

PGP の鍵ペアの有効期限の設定は、デフォルトで「5 年」が選択されます。有効期限の設定を望まない場合は「無期限」にチェックを入れてください。

※ JPCERT/CC のインシデントの報告受付アドレス（info@jpcert.or.jp）においては、暗号アルゴリズムを RSA2048 として、3 年毎に更新するポリシとしています。（2012 年現在）

※ PGP の鍵ペアに有効期限を設定している場合は、有効期限が切れる前に PGP の鍵ペアを再度作成して必要に応じて配布します。

参考：公開鍵および秘密鍵の有効期限について

PGP の鍵ペアは有効期限を設定することができます。PGP の鍵の有効期限を過ぎた場合は、自動的に鍵が「失効」と同等の状態になります。「OpenPGP の鍵の管理」では、「鍵の有効性」の列の表示が「期限切れ」となります。PGP の鍵の失効については、3.6 を参照してください。

(2) (1)の選択を終えたら「キー生成」ボタンをクリックします。PGP の鍵ペアの生成が終了すると失効証明書の作成（図 **7**）が促されますので、失効証明書を作成します。この失効証明書は PGP の鍵ペアを削除してしまったり、秘密鍵のデータを盗まれたりした場合に、鍵を無効にする為の証明書です。

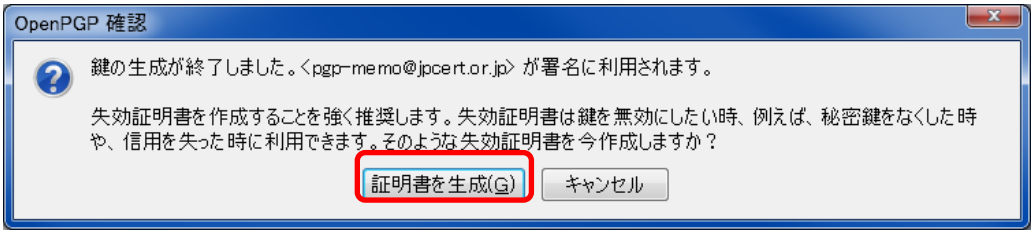

図 7. 失効証明書の生成

(3) 生成された PGP の鍵ペアを確認します。「OpenPGP の鍵の管理」画面を表示します。生成した鍵が表示されていない場合は、「既定ですべての鍵を表示する」のチェックボックスにチェックを入れてください。生成した PGP の鍵ペアをダブルクリックし、鍵のプロパティ画面（図 **8**）で詳細情報を表示します。ユーザ ID、アルゴリズム、鍵長、有効期限が適切にされているか確認してください。

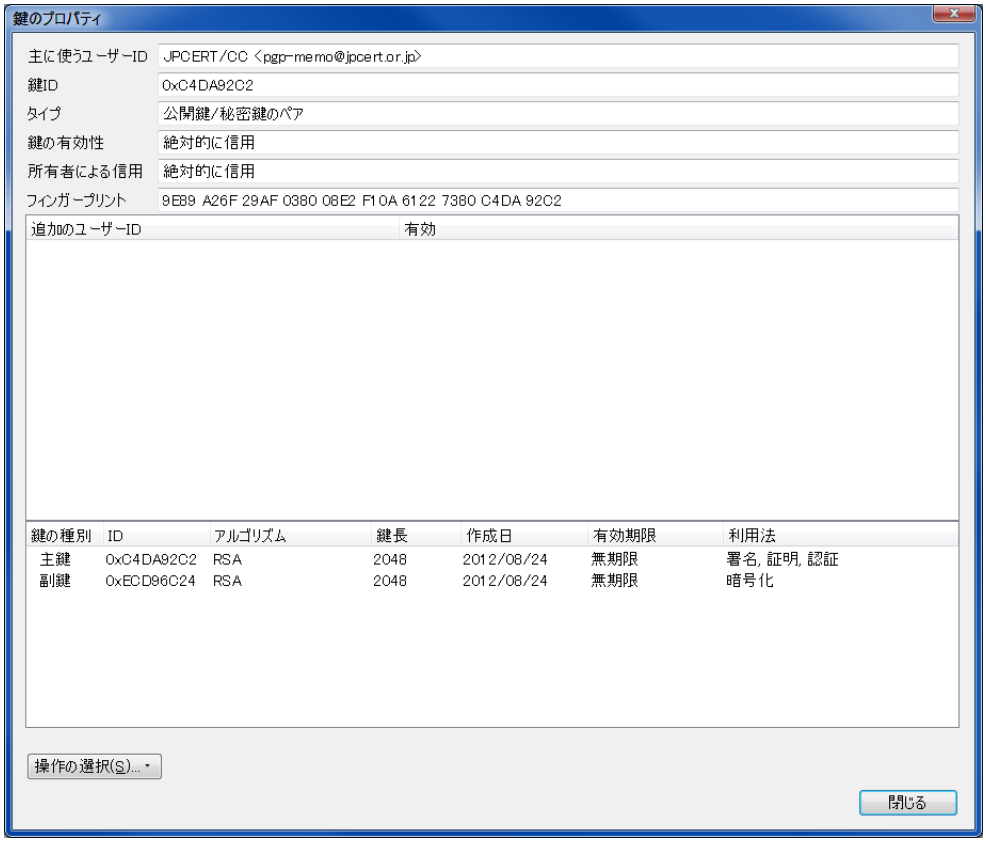

図 8. 鍵のプロパティ画面

※ 作成した鍵ペアと、失効証明書は、念のため、別のシステムや記録媒体にバックアップされるこ

とをお勧めします。鍵のエクスポート方法については、3.3.2 で説明します。

3.3.2　公開鍵、秘密鍵のエクスポート

Thunderbird の「OpenPGP（O)」の「鍵の管理（Y)」をクリックし、「OpenPGP の鍵の管理」（図 **9**）を表示します。「OpenPGP の鍵の管理」画面で、エクスポートする鍵を選択し、「ファイル（F)」の「ファイルへ鍵を書きだす（E)」をクリックします。

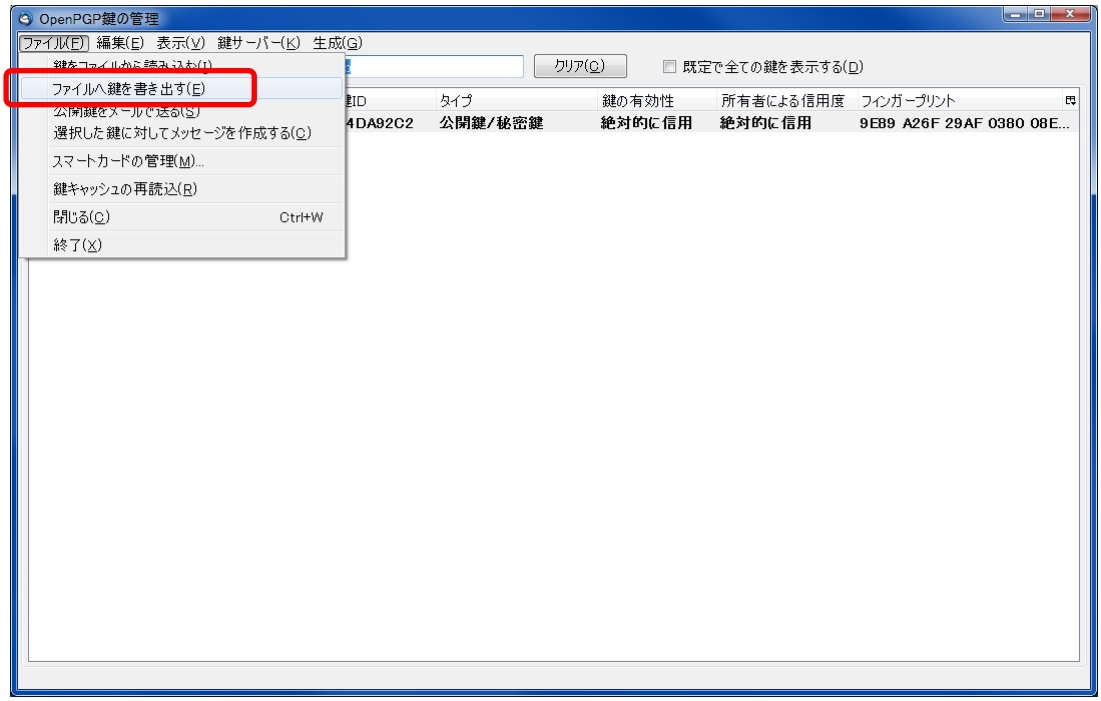

図 9. OpenPGP 鍵の管理画面

秘密鍵を含む鍵を選択した場合は、エクスポートするファイルに秘密鍵を含めるかどうかの確認画面が表示されます。公開鍵を配布する目的の場合は、「公開鍵のみをエクスポート（P)」を選択してください。バックアップを行う目的の場合は、「秘密鍵を含めてエクスポート（S)」を選択してください。

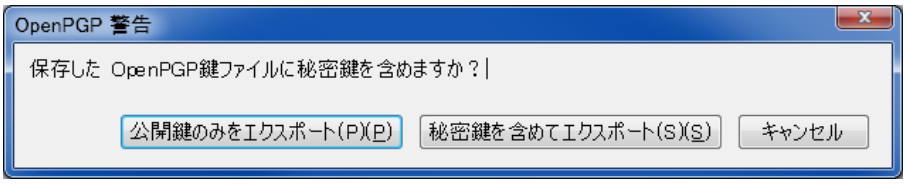

図 10. OpenPGP 鍵のエクスポートの確認画面

3.3.3 鍵交換と相手の公開鍵のインポート

相手と鍵交換を行います。公開鍵の交換は、普段やり取りしている経路など信頼できる経路で行ってください。信頼できない経路（過去にやり取りをしたことが無いアドレスからメールで受信した場合など）や「PGP 公開鍵サーバ/PGP Public Keyserver（PGP 公開鍵サーバはだれでも登録できます。PGP 公開鍵サーバの詳細は[7]を参照してください）」を介して交換した公開鍵の正当性を確認するために、公開鍵から計算される「フィンガープリント」（図 **11**）と呼ばれる文字列（実際には 16 進数データ）を利用することもできます。

BAF4 D9FA B8FB F073 57EE 3C2B 13F0 48B8

図 11. フィンガープリントの例

参考：鍵交換を行う経路の注意事項

公開鍵とフィンガープリントは、別々の経路で確認されることをお勧めします。例えば、公開鍵のファイルを電子メールや Web 経由で受け取り、フィンガープリントは電話や相手に直接会った際に聞いたりするなどの方法があります。

相手の公開鍵とフィンガープリントを入手した時には、相手の公開鍵をキーリングにインポートします。「OpenPGP 鍵の管理」（図 **12**）画面を表示し、「ファイル（F)」の「鍵をファイルから読み込む（I)」か「編集（E)」の「クリップボードから鍵を読み込む（I)」をクリックして、相手の公開鍵をインポートします。

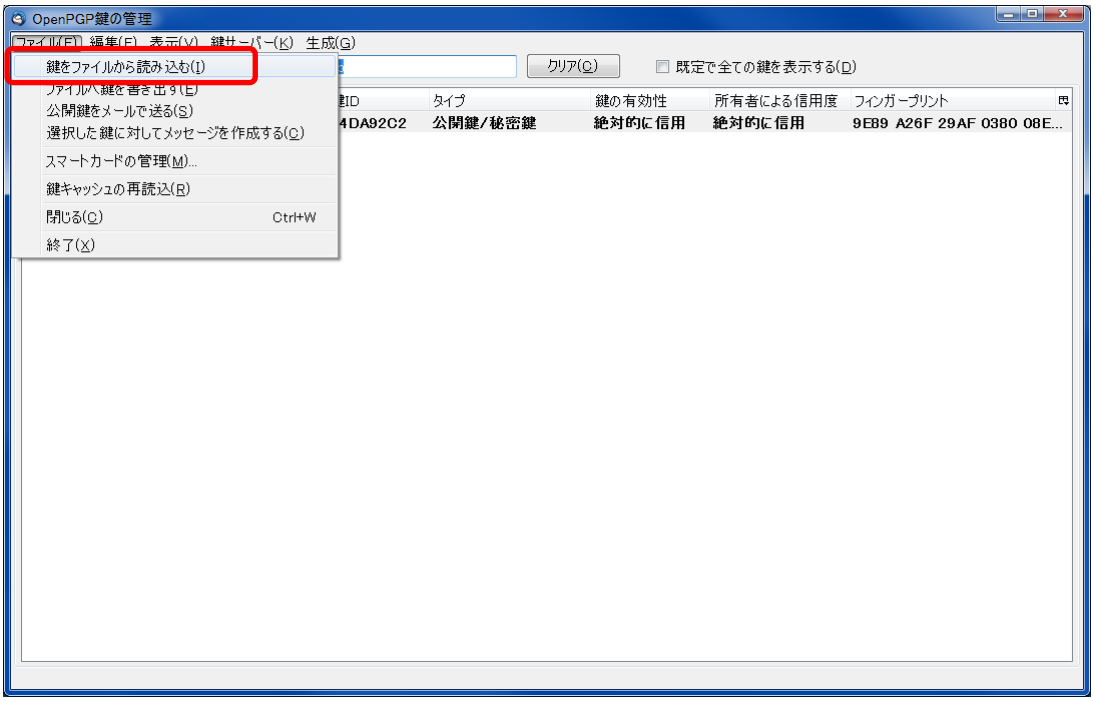

図 12. 公開鍵のインポート

インポートした公開鍵のフィンガープリントは、「OpenPGP 鍵の管理」の画面で表示される相手の公開鍵のプロパティを表示して確認します。プロパティは公開鍵をダブルクリックすると表示されます。もし、受領した相手の公開鍵のフィンガープリントと表示内容が異なるなど、正当性が確認できない公開鍵であれば、キーリングから鍵を削除して、相手から正しい公開鍵を再度入手してください。

3.4　PGP メールの送信

3.4.1　PGP メール（暗号化）の送信

PGP で暗号化したメールを送る相手（複数の相手に対して暗号化した PGP メールを送ることも可能です）の公開鍵を持っているか確認します。

暗号化しないメールの場合と同様に、宛先等に受信者のアドレスを入力し、メール本文を作成し、添付ファイルを指定します。この時、To または、CC に送信者自身のアドレスを追加指定してください。そうしないと、送信したメールの暗号を送信者が解くことができません。メールの作成が終了したら、電子メールの作成画面のメニューの「OpenPGP（N）」で「このメッセージを暗号化（E）」にチェック（図 **13**）します。

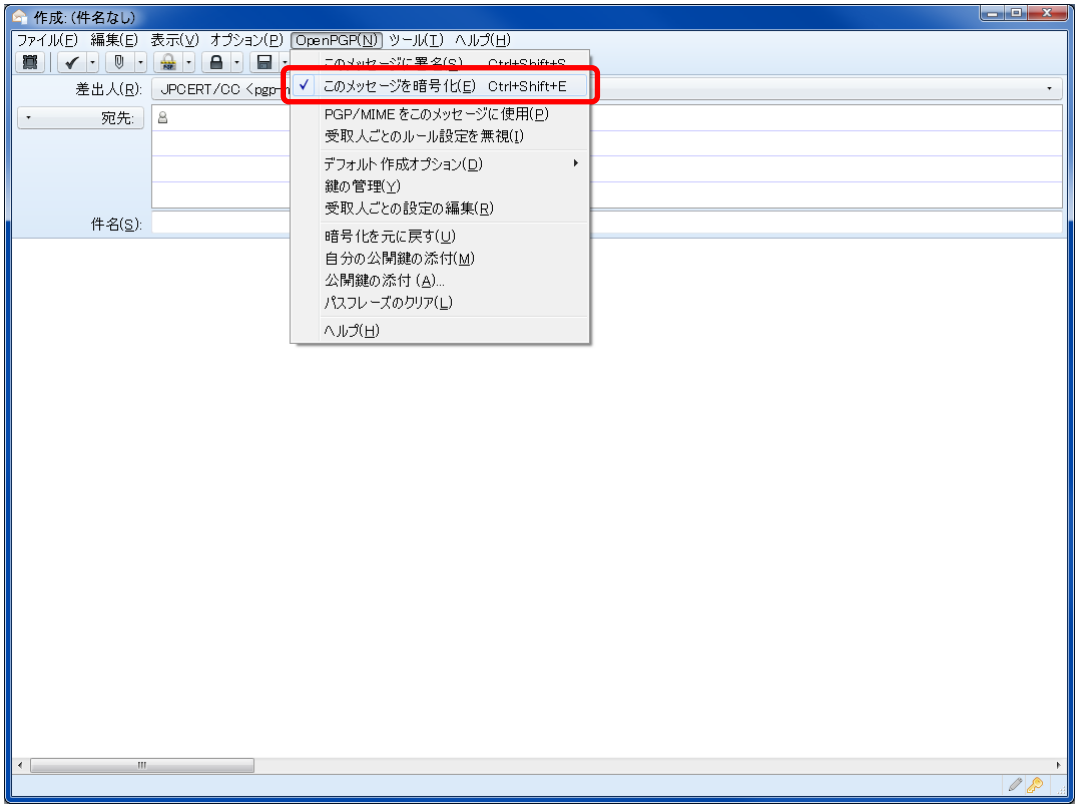

図 13.　メールの暗号化 1

チェックしたら、メールの「送信」ボタンをクリックします。宛先（To、CC の宛先となっているメールアドレス）の公開鍵を使用して暗号化されたメール（図 **14**）が送信されます。

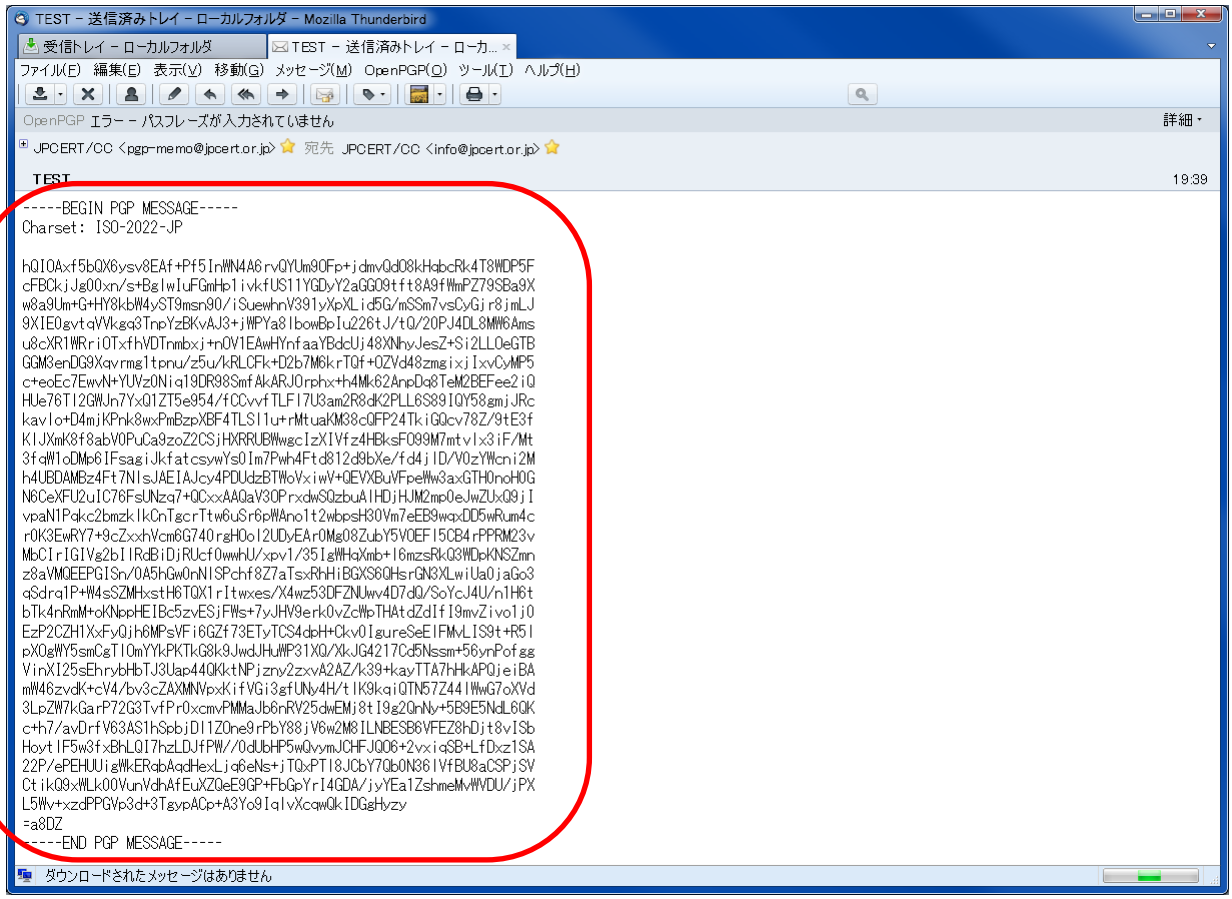

図 14. メールの暗号化 2

添付ファイル付きの PGP メールを送る場合は、以下の画面（図 **15**）が表示され選択が求められます。メール本文だけでなく添付ファイルに対しても暗号化を行う場合は、「添付ファイルは個別に署名/暗号化し、インライン PGP を使用してメッセージを送信する」もしくは、「メッセージ全体を署名/暗号化し、PGP/MIME を使用して送信する」を選択してください。基本的には、「添付ファイルは個別に署名/暗号化し、インライン PGP を使用してメッセージを送信する」を使用してください。※ 3.4.2 で説明する PGP メール（電子署名）の送信の際にも同様の選択が求められます。

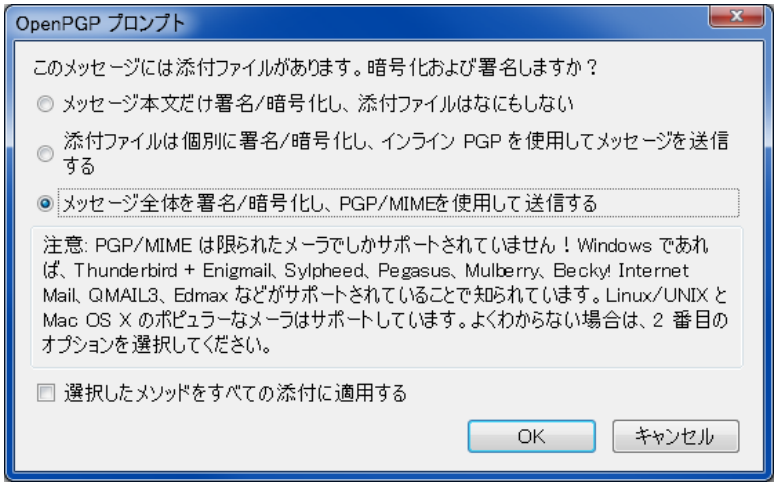

図 15. 添付ファイルつきの電子メールの送信時の選択

3.4.2 PGP メール（電子署名）の送信

メールを作成します。メールの作成が終了したら、「作成」画面で、メニューの「OpenPGP（N)」の「このメッセージに署名」にチェック（図 **16**）されていることを確認してください。チェックを確認したら「送信」をクリックします。メールの送信時に PGP の鍵ペアを作成した際に付与したパスフレーズの入力が求められますので、パスフレーズを入力します（パスフレーズは一定時間保持する設定が可能です。パスフレーズが保持されている時間内は入力を求められません)。

なお、暗号化と電子署名の両方を使用して PGP メールを送る場合は、「このメッセージに署名（S)」と「このメッセージを暗号化（E)」の両方にチェックを入れます。

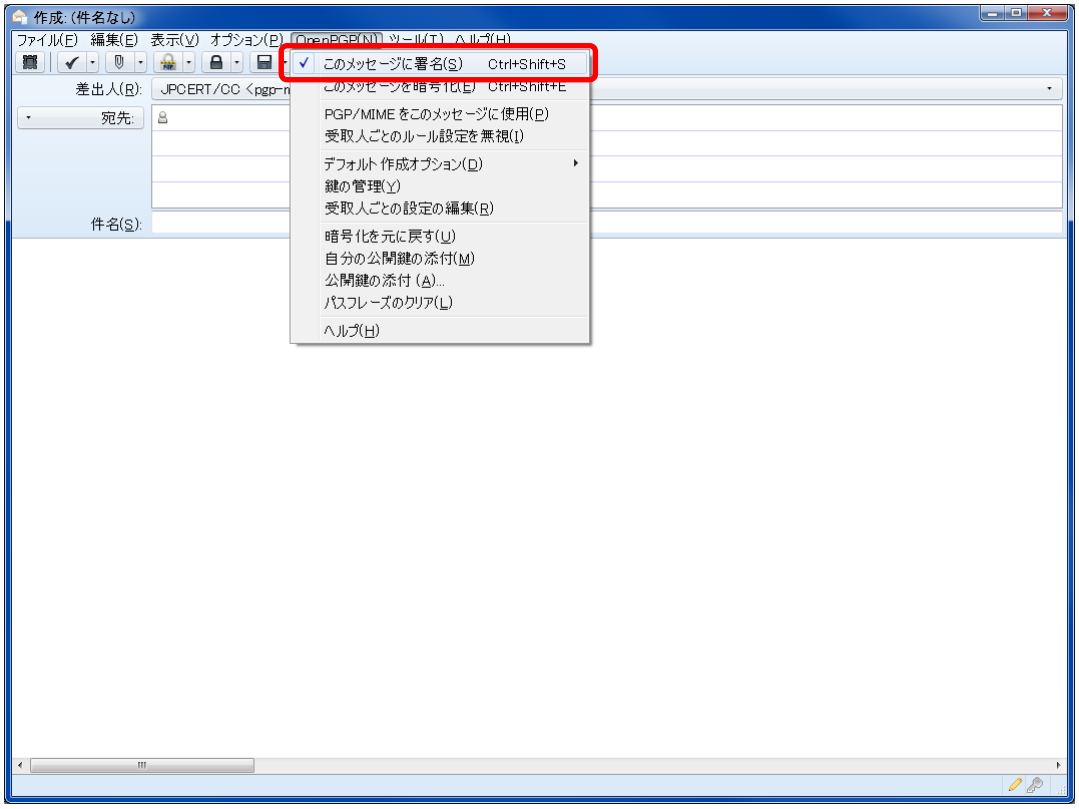

図 16. 電子メールへの電子署名

3.5 PGP メールの受信

3.5.1 受信した PGP メール（暗号化）の復号

OpenPGP(O)メニューの「メッセージを自動的に復号／検証」にチェックが入っているか確認します。

PGP メール（暗号化）をメール一覧で選択（図 **17**）します。PGP の鍵ペアを作成した際に付与したパスフレーズの入力が求められます。正しくパスフレーズを入力します。パスフレーズが正しければ PGP メールが復号され内容が見えるようになります。パスフレーズが保持されている時間内は、パスフレーズを入力しなくても PGP メールが自動的に復号されます。

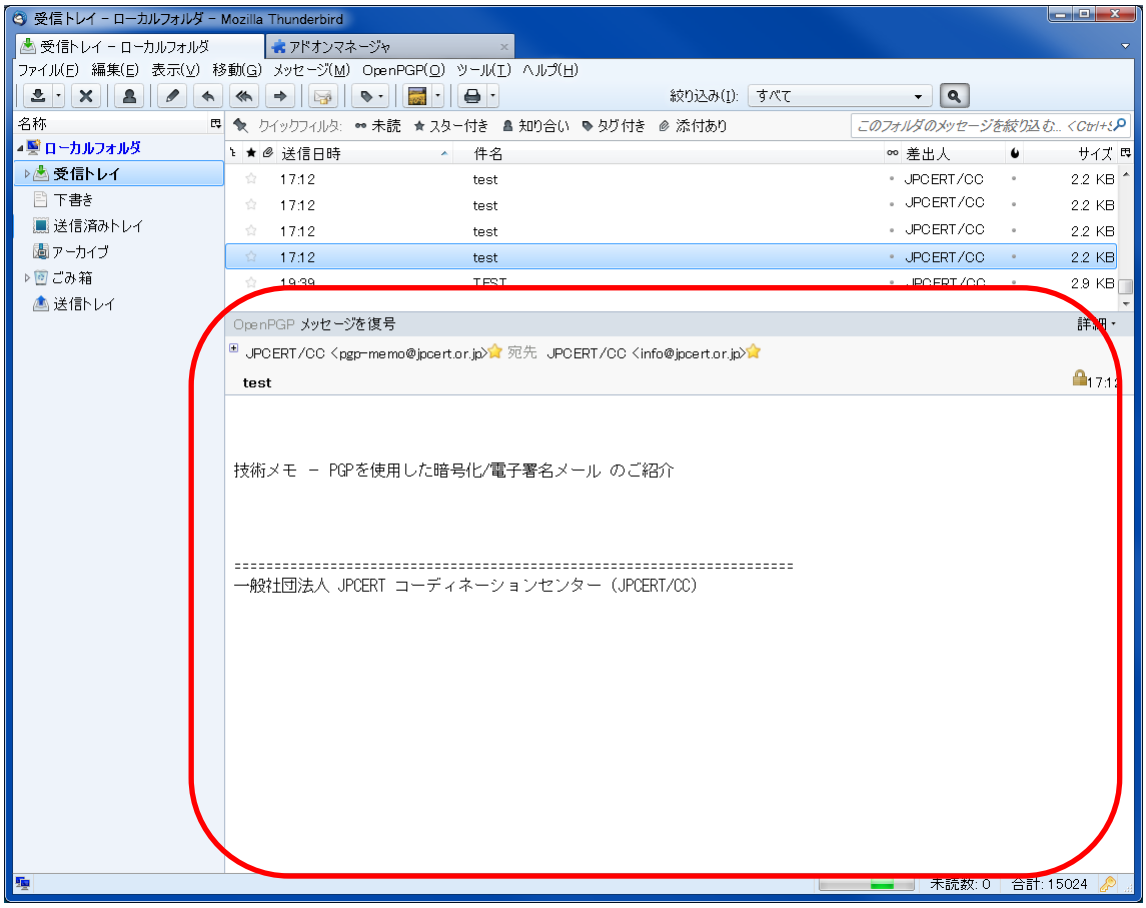

図 17. 暗号化メールの復号

3.5.2　受信した PGP メール（電子署名）の署名検証

メール一覧でメールを選択します。選択したメールが PGP メール（電子署名）であれば、自動的に電子署名の検証が行われます。電子署名の検証が成功した場合は、図 **18** のように表示されます。電子署名の検証では、パスフレーズの入力は求められません。

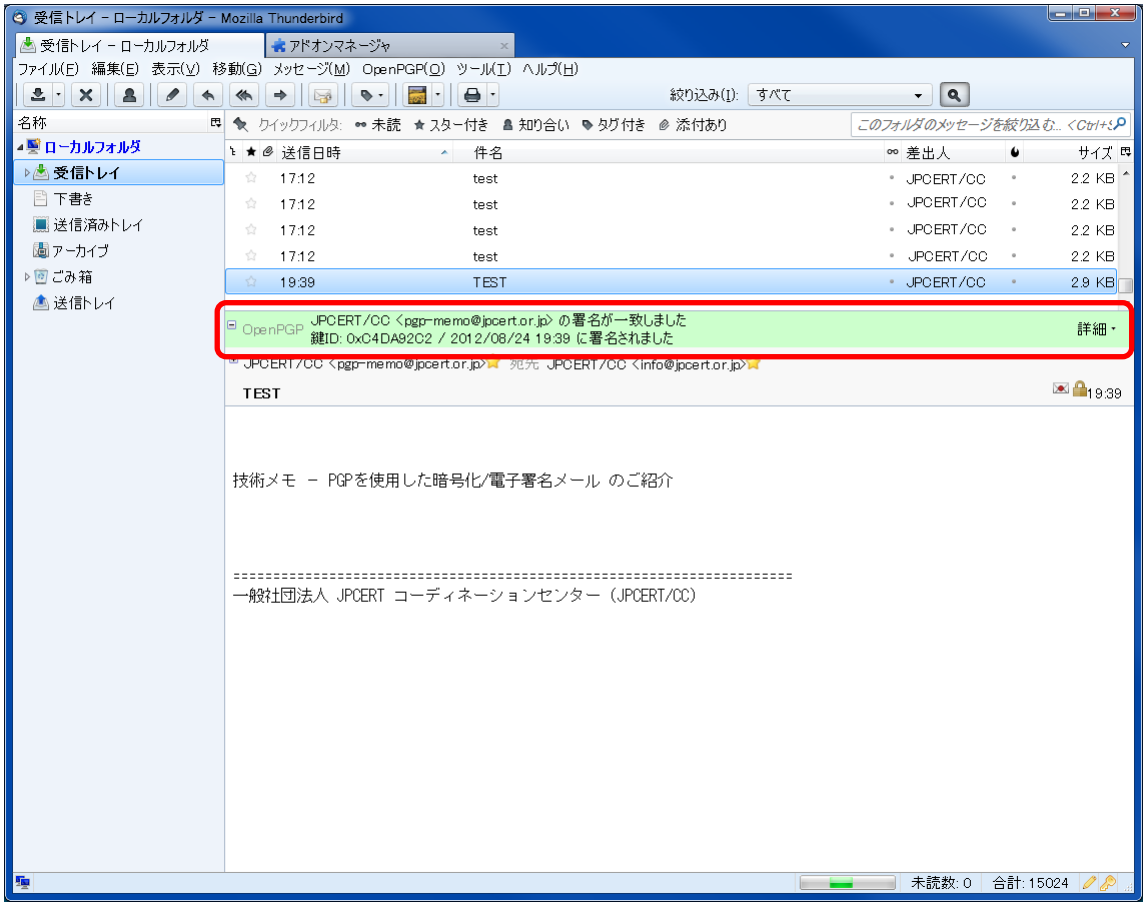

図 18. メールの電子署名の検証（成功）

送信者が電子署名したメールが一部でも書き変わってしまっていた場合には、電子署名の検証が失敗します。検証が失敗した場合、図 **19** のように表示されます。

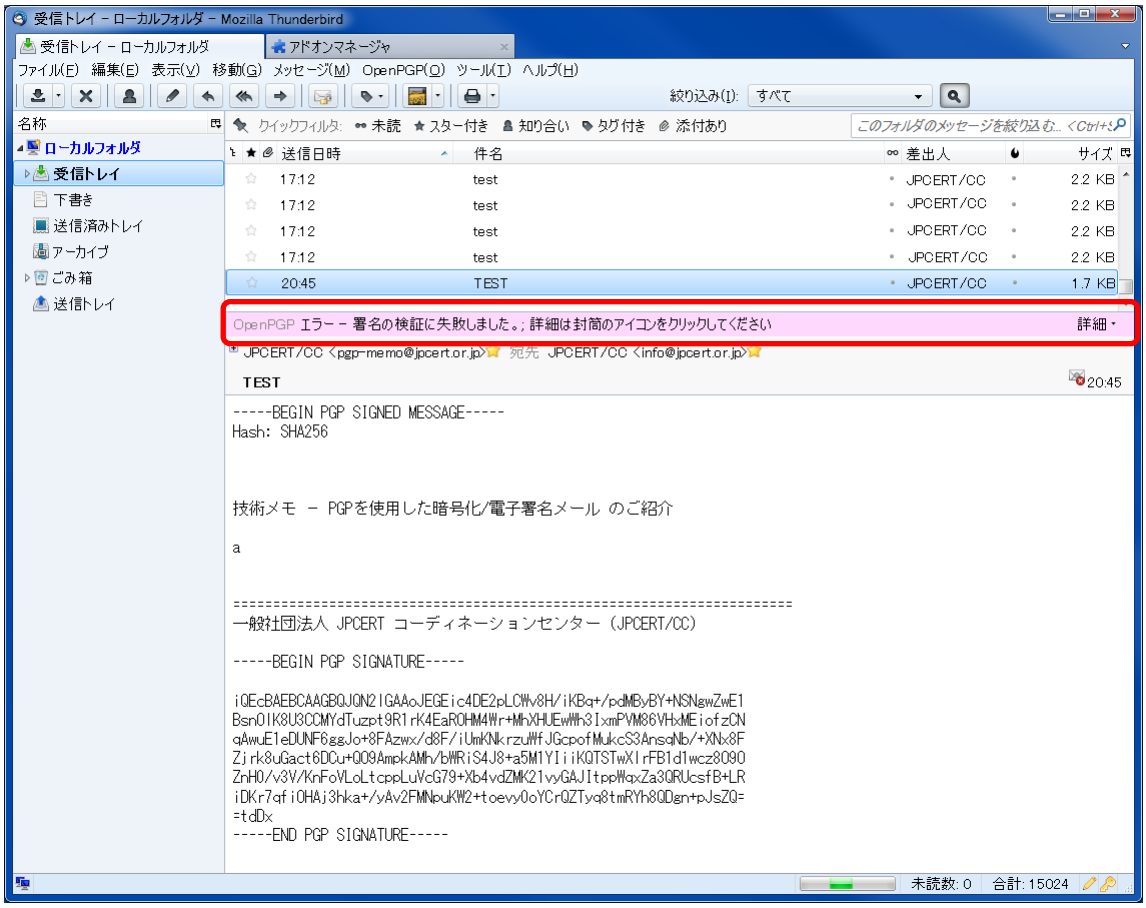

図 19. メールの電子署名の検証（失敗）

公開鍵を持っていない場合は、電子署名の検証ができないため、図 **20** のように表示されます。

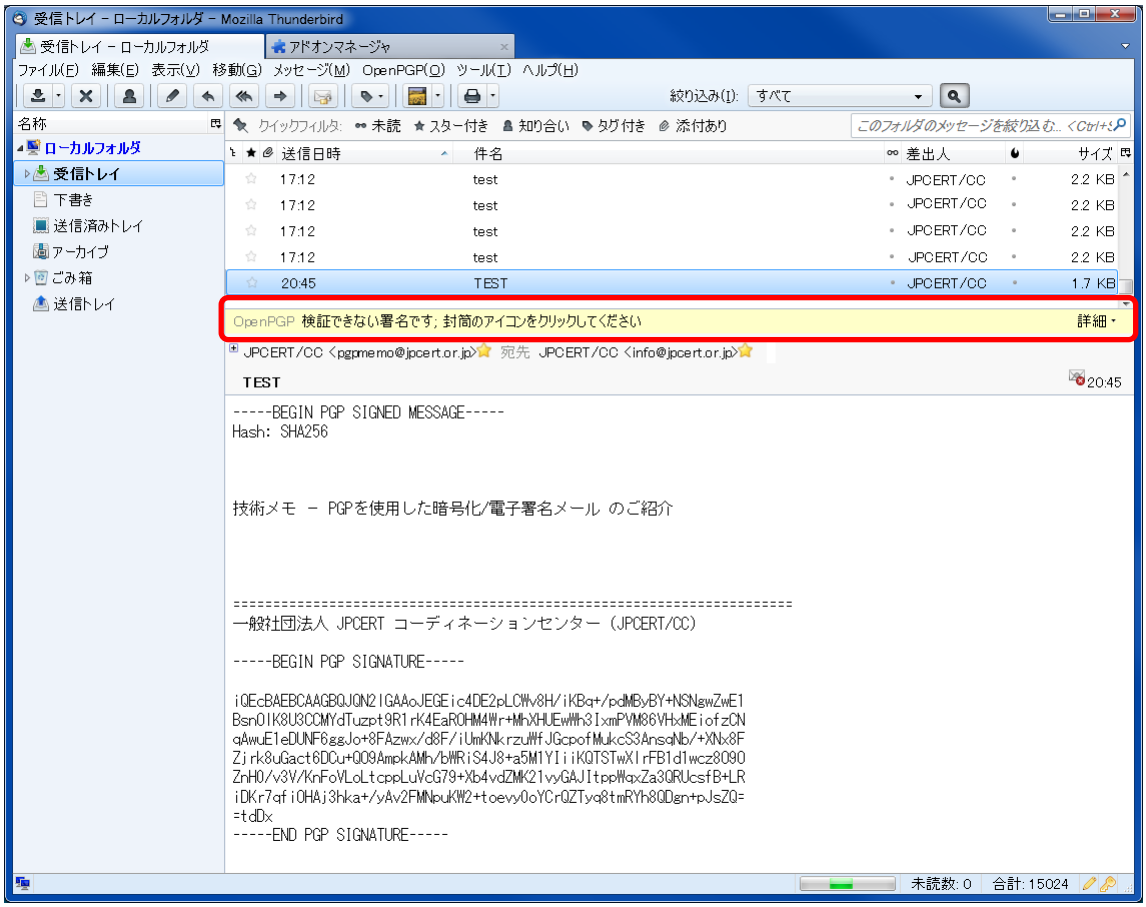

図 20. メールの電子署名の検証（検証できない署名）

3.6 PGP の鍵ペアの失効

秘密鍵、もしくは失効証明書（3.3.1 で作成）で鍵ペアを失効します。「OpenPGP 鍵の管理」画面（図 21）で、「鍵を失効させる」を選択するか、鍵ペア作成時に作成された失効証明書を「ファイル（F)」の「鍵をファイルから読み込む（I)」からキーリングにインポートすることで、鍵ペアが失効します。

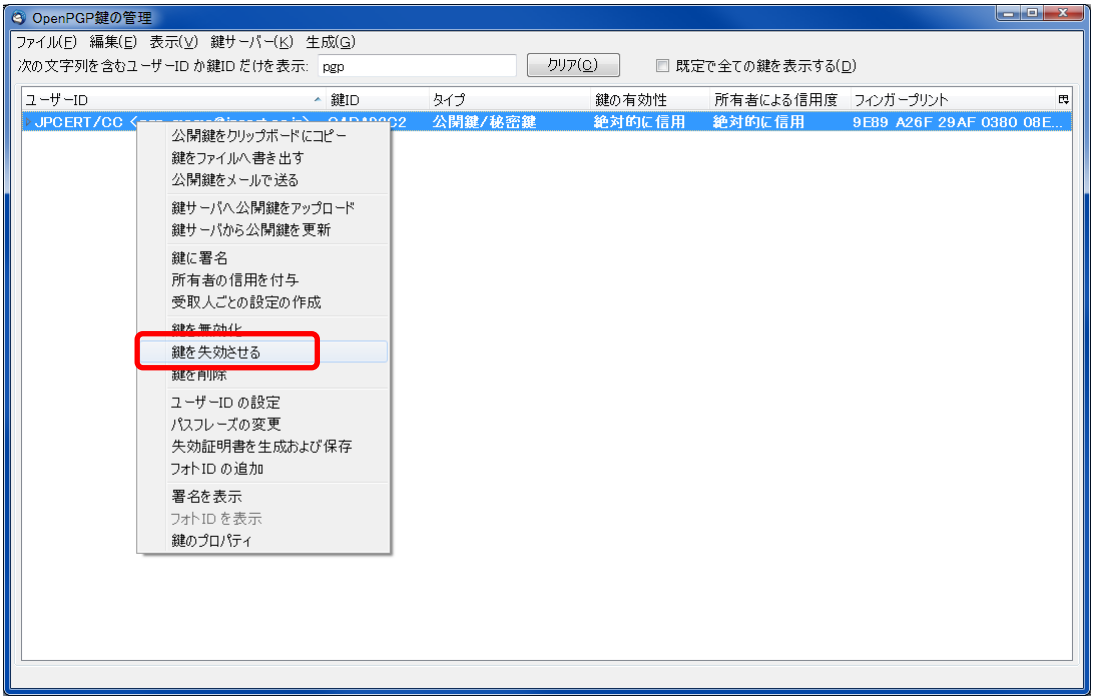

図 21. 鍵の失効

また、鍵交換した相手にも失効証明書をメールなどで配布し、失効証明書をキーリングにインポートするよう依頼してください。なお、公開鍵を公開鍵サーバ[7]に登録している場合は、失効した公開鍵を公開鍵サーバにも登録してください。

なお、鍵交換を行った相手の秘密鍵が他人に漏れてしまった場合も同様に、相手の失効証明書を受け取り、自身のキーリングにインポートします。

参考：公開鍵および秘密鍵の失効について

公開鍵および秘密鍵を失効すると「OpenPGP の鍵の管理」画面で、「鍵の有効性」の列の表示が「失効」となります。失効の状態で公開鍵を使用して暗号化したり、秘密鍵を使用した電子署名したりしようとすると警告が表示され、新たに PGP メールを送信することができません。ただし、過去に受信した暗号化された PGP メールの復号や電子署名された PGP メールの検証を行うことは可能です。

4 まとめ

本ガイドブックでは、PGP メールの概要と GnuPG のインストールから PGP を使ったメッセージ交換について、初めて PGP を使用する方々のために、短時間で基本的な内容を理解して実際に活用いただけるように留意して述べました。本ガイドブックが、暗号化や電子署名を利用したセキュアなコミュニケーションに PGP メールが活用される一助となることを期待しています。

5 参考情報

[1] OpenPGP.org - The OpenPGP Alliance Home Page
http://www.openpgp.org/
[2] MIME Security with OpenPGP
http://www.ietf.org/rfc/rfc3156.txt
[3] The GNU Privacy Guard - GnuPG.org
http://www.gnupg.org/
[4] The GNU Privacy Handbook
http://www.gnupg.org/gph/en/manual/book1.html
[5] JPCERT/CC PGP の説明に役立つデータ
https://www.jpcert.or.jp/csirt_material/files/21_pgp_explanation_data.pdf
[6] Thunderbird と Enigmail のバージョンの対応表
http://enigmail.mozdev.org/download/download-static.php.html
[7] PGP Public Keyserver へようこそ
http://pgp.nic.ad.jp/pgp/index.html

＜お願い＞
引用の際は、引用元名、資料名、URL を明示してください。
なお、引用の際は引用先文書、時期、内容等の情報を JPCERT/CC 広報（office@jpcert.or.jp）までメールにてお知らせください。今後、より良い情報を提供するため、どこで、どのような方に、どのような場面で、お使いいただけているのかを把握し検討するため、ご協力をお願いいたします。