



## PGP Desktop とは

PGP Desktop は、デスクトップおよびラップトップに対して総合的なセキュリティを提供するソリューションです。PGP Desktop を使用すると、既存の IT インフラストラクチャを変更したり、作業プロセスを中断したりすることなく、企業、ワークグループ、および個人の機密情報を保護できます。この受賞歴のある簡単に使用できるソリューションでは、単一のデスクトップアプリケーションから電子メール、ファイル、仮想ボリューム、およびディスク全体を暗号化できます。

PGP Desktop ファミリーのアプリケーションは、複数のバンドルに組み合わされています。

- **PGP Desktop Professional** には、PGP Desktop 電子メールおよび PGP ディスク全体暗号化が含まれています。
- **PGP Desktop Storage** には、PGP ディスク全体暗号化と PGP NetShare が含まれています。
- **PGP Desktop Enterprise** には、PGP Desktop 電子メール、PGP ディスク全体暗号化、および PGP NetShare が含まれています。

## PGP Desktop 電子メール

PGP Desktop 電子メールを使用すると、電子メールの暗号化、署名、復号化、および検証を自動的かつ透過的に行えます。これらの操作は、管理者がユーザーのために定義したポリシー、または PGP Universal Server 管理環境にない場合はユーザーが管理するポリシーに基づいて行われます。

## PGP NetShare

PGP NetShare を使用すると、ファイル サーバー、共有フォルダ、USB リムーバブル ドライブなどの共有場所にある保護されたファイルを、承認されたユーザー間で共有できます。

## PGP ディスク全体暗号化

PGP ディスク全体暗号化 (WDE) を使用すると、システムの内容全体、または指定した外付けドライブや USB フラッシュドライブをロックすることができます。

また、PGP Desktop では、次の操作を行えます。

- ハード ドライブ領域の一部に独自のドライブ文字を割り当て、暗号化された仮想ディスク ボリュームとして使用する。
- 保護されたジップ アーカイブを作成する。
- PGP Desktop のインストールされていない Windows システム上でも開くことのできる、暗号化された単一の圧縮パッケージにファイルおよびフォルダを格納する。
- ファイルやフォルダを完全破棄し、いかなる方法でも回復できないようにする。
- ドライブの空き領域を安全に消去し、削除したデータが完全に回復不可能になるようにする。

## 目次

- PGP Desktop とは (1 ページ)
- 初めて PGP Desktop をご使用になる方へ (1 ページ)
- 基本事項について (1 ページ)
- インストールされる内容について (2 ページ)
- システム要件 (3 ページ)
- PGP Desktop のインストール (3 ページ)
- PGP Desktop の起動 (3 ページ)
- PGP Desktop のメイン画面 (4 ページ)
- PGP 仮想ディスク ボリュームの作成 (7 ページ)
- PGP ジップ アーカイブの作成 (10 ページ)
- ファイルの細断処理 (12 ページ)
- 空き領域の細断処理 (13 ページ)
- サポート情報 (13 ページ)

## 初めて PGP Desktop をご使用になる方へ

このガイドに記載されている手順に従って使い始めてください。PGP Desktop でデータを保護するのは、錠に鍵をかけるように簡単なので、初めての方でも安心してお使いいただけます。

- この『クイック スタート ガイド』では、PGP Desktop のインストール手順および基本的な使用方法について説明します。
- PGP Desktop に関するより詳細な情報は、『PGP Desktop ユーザー ガイド』に記載されています。ここでは、鍵ペアについて、鍵ペアを作成する理由、鍵ペアの作成方法、また、暗号化したデータを他のユーザーと安全に共有するために鍵を交換する方法について説明します。

**メモ:** PGP Desktop のライセンスは、特定の PGP Desktop 機能へのアクセスを可能にします。PGP Desktop 機能の中には、別のライセンスが必要なものもあります。詳細は、『PGP Desktop ユーザー ガイド』のライセンスに関する項を参照してください。

- PGP Desktop の導入、管理、およびポリシー施行についての情報は、『PGP Universal Server 管理者ガイド』を参照してください。

## 基本事項について

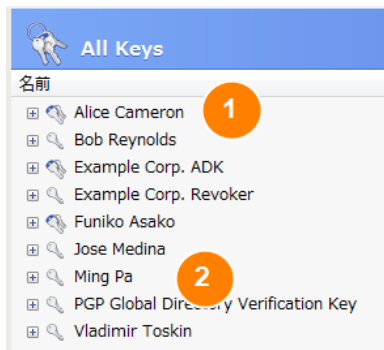
PGP Desktop では、メッセージの暗号化、署名、復号化、および検証を行うのに「鍵」を使用します。

インストール後に、PGP Desktop に PGP 鍵ペアを作成するよう表示されます。鍵ペアとは、秘密鍵と公開鍵の組み合わせのことをいいます。

- 名前が示すように、秘密鍵とそのパスフレーズは秘密にしてください。もしあなたの秘密鍵とパスフレーズが他人の手に渡ってしまった場合、その人があなたのメッセージを読んだり、あなたになりすましてすることができてしまいます。あなたの秘密鍵は、暗号化された受信メッセージを復号化したり、送信メッセージに署名するために使用します。
- あなたの公開鍵は、他のユーザーに渡すことができます。これにはパスフレーズがありません。あなたの公開鍵は、あなたの秘密鍵でしか復号化できないメッセージを暗号化したり、あなたが署名したメッセージを検証したりするために使用します。

あなたの鍵ペアと他ユーザーの公開鍵は、すべて「鍵リング」に保管されます。他ユーザーの公開鍵は、特定ユーザーに暗号化されたメッセージを送信する場合に使用します。鍵リングの鍵を表示するには、[PGP 鍵] コントロール ボックスをクリックします。

1. 2本の鍵が重なったアイコンは、秘密鍵と公開鍵を表しており、PGP 鍵ペアであることを示します。たとえば、この図では、Alice Cameron というユーザーが PGP 鍵ペアを持っています。
2. 鍵が1本だけ表示されているアイコンは、他のユーザーの公開鍵を示します。たとえば、この図では、Ming Pa というユーザーの公開鍵が鍵リングに追加されています。



## インストールされる内容について

PGP Desktop では、購入された機能へのアクセス権を付与するためにライセンスが使用されます。ユーザーのライセンスに基づいて、PGP Desktop ファミリーの一部またはすべてのアプリケーションがアクティブになります。

ライセンスによってアクティブ化されている機能を確認する方法については、後の項で説明します。



**PGP Desktop 電子メール:** PGP Desktop ファミリーのアプリケーションの1つで、電子メールメッセージの暗号化、署名、復号化、および検証を、ユーザーの管理するポリシーを通して自動的にかつ透過的に行うことができます。また、AIM や iChat などのクライアントでの IM セッションを暗号化することもできます。ただし、両方のユーザーによって PGP Desktop 電子メールが有効にされている必要があります。



**PGP NetShare:** PGP Desktop ファミリーのアプリケーションの1つで、会社のファイルサーバー、保護フォルダ、USB ドライブのようなリムーバブル メディアなどの共有場所にある保護されたファイルをユーザー間で共有することを承認できます。承認されたユーザーに対しては、保護フォルダ内の暗号化されたファイルは通常のアプリケーション ファイルとして表示されます。この保護フォルダに物理的にアクセスできるその他のユーザーに対しては、中のファイルは表示されますが、それを使用することはできません。



**PGP ディスク全体暗号化 (WDE):** PGP Desktop ファミリーのアプリケーションの1つで、システムの内容全体、または指定した外付けドライブや USB フラッシュ ドライブをロックできます。ブート セクター、システム ファイル、およびスワップ ファイルのすべてが暗号化されます。ブート ドライブに対してディスク全体暗号化を行うと、ご使用のコンピュータが失われたり盗まれたりした場合でも、適切なパスフレーズがないとデータにアクセスできないので、データ漏えいの心配はありません。



**PGP 仮想ディスク ボリューム:** ハード ドライブ領域の一部に独自のドライブ文字を割り当て、暗号化された仮想ディスク ボリュームとして使用できます。PGP 仮想ディスクは、機密ファイルを保管するのに最適な格納場所です。これは、それらを金庫に保管するのと同じです。金庫の扉が開いている間 (ボリュームがマウントされている間) は、保管されているファイルの変更、追加、および取り出しが可能です。それ以外の場合 (ボリュームがマウントされていない)、ボリューム上のすべてのデータは保護されます。



**PGP ジップ:** 暗号化された圧縮アーカイブに、ファイルやフォルダを自由に追加できます。PGP ジップ アーカイブは、PGP Desktop のインストールされているシステム上でのみ作成および開くことができます。PGP ジップは、機密データを他のユーザーに安全に配布したい場合、または機密データのバックアップを取りたい場合などに、暗号化してアーカイブするツールです。

**PGP 自己復号化アーカイブ (SDA):** PGP

Desktop のインストールされていない Windows システム上でも開くことのできる、暗号化された単一の圧縮パッケージにファイルおよびフォルダを格納できます。SDA は、PGP ソフトウェアを使用していないユーザーと安全にファイルを交換するのに最適なソリューションです。



**PGP シュレッダ:** ファイルおよびフォルダを完全に破棄し、ファイル回復用ソフトウェアを使用しても回復できないようにします。Windows システム上でファイルを削除するときに Windows の [ごみ箱] を使用した場合、そのファイル自体は実際には削除されず、ドライブ上に残っています。最終的にファイルが上書きされるまでは、攻撃者がそのファイルを回復することは容易なことです。対照的に、PGP シュレッダでは、ファイルが複数回にわたって直ちに上書きされます。これは、高度なファイル回復用ソフトウェアでもファイルを回復できないほど効果的です。また、この機能ではドライブの空き領域が完全に抹消されるので、削除したデータは完全に回復不可能となります。



**鍵管理:** PGP Desktop では、自分の鍵ペアおよび他ユーザーの公開鍵の両方の PGP 鍵を管理します。あなたの秘密鍵は、あなたの公開鍵で暗号化されたメッセージを復号化したり、あなたの PGP 仮想ディスク ボリュームを保護したりするために使用します。公開鍵は、他のユーザー宛のメッセージを暗号化したり、PGP 仮想ディスク ボリュームにアクセスできるユーザーを追加したりするために使用します。

## システム要件

- Microsoft Windows 2000 (Service Pack 4)、Windows Server 2003 (Service Pack 1)、Windows XP (Service Pack 1、Service Pack 2、または Service Pack 3。32 ビット版および 64 ビット版)、Windows Vista (Service Pack 1 を含むすべての 32 ビット版および 64 ビット版)、Microsoft Windows XP Tablet PC Edition 2005 (付属のキーボードが必要)

**メモ:** 上記オペレーティング システムでのサポートは、Microsoft からのすべての最新ホット フィックスおよびセキュリティ パッチが適用されている場合にに限られます。

PGP ディスク全体暗号化 (WDE) は、Windows 2000 (Service Pack 4) および Windows XP (Service Pack 1 または Service Pack 2) のクライアント版、および Windows Vista に対応しています。Windows 2000 Server および Windows 2003 Server には対応していません。

- 512 MB 以上の RAM
- 64 MB 以上のハード ディスク容量

## PGP Desktop のインストール

インストールを開始する前に、すべての起動中のアプリケーションを終了することを推奨します。また、インストール後にシステムの再起動が必要となります。

**メモ:** PGP Universal Server により管理されている環境で PGP Desktop を使用する場合、PGP Desktop インストール プログラムが特定の機能や設定で構成されている場合があります。

➤ **PGP Desktop をインストールするには、次の操作を実行します。**

- ダウンロードした PGP Desktop インストール プログラムの場所に移動します。  
インストール プログラムは、Microsoft SMS 導入ツールを使用して PGP 管理者により配布されている場合があります。
- インストール プログラムをダブルクリックします。
- 画面に表示される指示に従います。
- 指示に従ってシステムを再起動します。
- システムの再起動後、画面上の指示に従って PGP Desktop の設定を行います。

## ライセンス

現行のライセンスによってサポートされている機能を表示するには、PGP Desktop を起動し、[ヘルプ] メニューの [ライセンス] を選択します。チェックマークが付いている機能が、アクティブなライセンスでサポートされています。



## PGP Desktop の起動

PGP Desktop を起動するには、次のいずれかの方法を使用します。

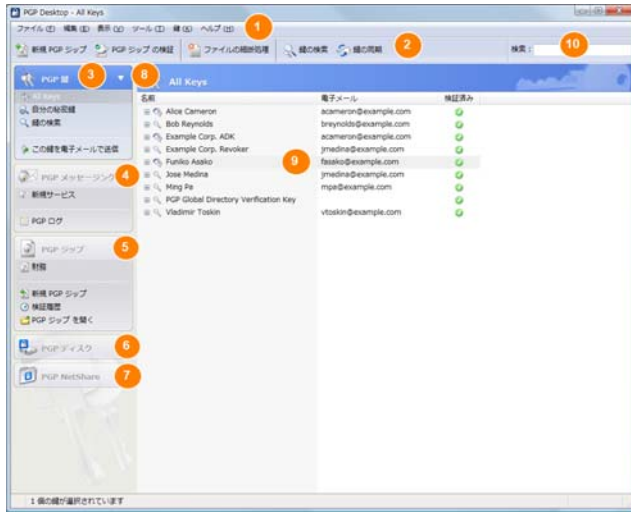
- [PGP トレイ] アイコンをダブルクリックする。



- [PGP トレイ] アイコンを右クリックして [PGP Desktop を開く] を選択する。
- [スタート] メニューで、[プログラム] > [PGP] > [PGP Desktop] を選択する。

## PGP Desktop のメイン画面

PGP Desktop のメイン画面を使用すると、各機能に簡単にアクセスできます。



PGP Desktop のメイン画面には、次の要素が含まれます。

- 1 メニュー バー:** PGP Desktop の各コマンドにアクセスできます。メニュー バーのメニューは、選択されているコントロール ボックスに応じて変わります。
- 2 ツールバー:** よく使用する機能にアクセスできます。新しい PGP ジップ アーカイブの作成、既存の PGP ジップ アーカイブの検証、選択したファイルの細断処理、鍵の検索、鍵の同期、または [PGP 鍵] 作業領域に現在表示されている鍵のユーザー ID のテキスト検索などを行うことができます。
- 3 [PGP 鍵] コントロール ボックス:** PGP 鍵を管理できます。
- 4 [PGP メッセージング] コントロール ボックス:** PGP メッセージングを管理できます。
- 5 [PGP ジップ] コントロール ボックス:** PGP ジップを管理する機能や、新しい PGP ジップ アーカイブの作成を支援する PGP ジップ アシスタントを制御できます。
- 6 [PGP ディスク] コントロール ボックス:** PGP ディスクを管理できます。
- 7 [PGP NetShare] コントロール ボックス:** PGP NetShare を管理できます。
- 8 コントロール ボックスの展開/折りたたみ:** コントロール ボックスを表示または非表示にするために使用します。
- 9 PGP Desktop 作業領域:** 選択したコントロール ボックスに関する情報と実行できる操作が表示されます。
- 10 PGP 鍵の検索ボックス:** 鍵リングにある鍵を検索するために使用します。ボックスにテキストを入力すると、名前か電子メール アドレスによる検索結果が表示されます。

各コントロール ボックスを展開すると、利用できるオプションが表示されます。折りたたむと、コントロール ボックスのタイトルだけが表示されるので、表示領域の節約になります。コントロール ボックスを展開するには、そのタイトルをクリックします。コントロール ボックスを折りたたむには、右上にある [展開/折りたたみ] 矢印をクリックします。

## PGP Desktop 電子メールの使用

PGP Desktop 電子メールでは、送信メッセージの暗号化および署名、また受信メッセージの復号化および検証を、自動的にかつ透過的に行うことができます。ユーザーは今までどおり電子メールを送受信するだけで、PGP Desktop 電子メールが残りの処理をすべて実行します。

### 暗号化された電子メールの送信

インストール後、PGP Desktop 電子メールはお使いの電子メール クライアントとメール サーバーの間で移動し、電子メールのトラフィックを監視します。

メッセージが着信すると、メッセージが受信トレイに届く前に PGP Desktop 電子メールによって傍受され、自動的に復号化および検証されます。復号化には秘密鍵が使われ、検証には他ユーザーの公開鍵が使われます。この作業が完了すると、メッセージが受信箱に配信されます。

多くの場合、特別な作業は必要ありません。復号化された受信メッセージは、他の受信メッセージ同様に受信箱に表示されます。

メッセージを送信する場合は、メッセージがメール サーバーに届く前に PGP Desktop 電子メールによって傍受され、設定されたポリシーに従って自動的に暗号化および署名が試行されます。

ここでも特別な作業は必要ありません。ご使用の電子メール クライアントを使用してメッセージを作成して送信するだけです。PGP Desktop 電子メールが残りの処理を実行します。

PGP Desktop 電子メールが透過的に受信および送信メッセージを処理する方法の詳細については、次のセクションを参照してください。

### 受信メッセージ

PGP Desktop 電子メールでは、次のようにメッセージ内容に応じて受信メッセージが処理されます。

- 暗号化も署名もない場合。**メッセージが暗号化も署名もされていない場合は、PGP Desktop 電子メールによって電子メール クライアントにそのまま送られます。メッセージはそのまま読むことができるため、PGP Desktop 電子メールで行う処理はありません。
- 暗号化されているが署名されていない場合。**メッセージが暗号化されている場合、ユーザーがメッセージを読めるように復号化が試行されます。まず最初に、メッセージを復号化できる秘密鍵があなたの鍵リングにないか、検索されます。秘密鍵が見つかった場合は、それを使ってメッセージが復号化され、電子メール クライアントに送信されます。秘密鍵が見つからなかった場合は、暗号化されたまま電子メール クライアントに送信されます。この場合、メールの内容は次のようになります。

-----BEGIN PGP MESSAGE-----  
Version: PGP Desktop 9.10

qANQR1DBwUwDmVpGQkAZ1HwBD/Of5F8QKtY+1NVzwQw4xQ/EPU0D0mLRmZVVNVQvN  
rYVHPoSACn6C3ZfP0996akjRi00BGa62hklpkjq13QEGpBtqMP1F64TuxqHkPLNH  
ISN+7ZEAEYTTv+3ErEOH6yQgJ+sQgm65jrjddYVVTG6hGa9F2wX+ZDLAIK6SrA  
f4ZnQfNvKwMmJX578S7LEGE5d5wM68kK8/Ff1vFyz1w360ggauIXmom9F8K294p  
fNawAnhQ1R1f/1a/Muys0wkTLPqpd8XhgZqVkaE85gScrwqXfMAGDEYfscAB1Ne  
rMwJNTXSRVpStmPNBZuvH01jKpX4EYAPK48MOD1Yi54NjXyWvury79oDoxD1Jh  
o9yh9v5f071orplFccw8wMLx4qJagds0vqdwQRRnfwbnbgSD1jD2cmi jyoq+bcy  
3hZknIEGbb7G7Kako1cj+y9uSafDh491A9qLyHTwWLuHYV/j/wtBPFpZpjGYVACV  
FqRDE08hyZxKc/foQw1Imdo+nymZEQITTTdBCaESxm5v+jBwf0xhUK/Evy1kaHm  
n27x2m9PdwZxr1o1grxI8Lda7DTJwYMA8o120C1QZqrqvAmqIKL4CpckyhFuRwIg  
nan80KN/USfZk+V19juxM1155oGyz0DtL6KnLNgGpTLu6ylSU2Sb71IbVe330ukj  
ZMLXgdLAKQF5itPMVEKq3PQXqMrL1EYr6He7fCAYmUMWxe8w60e7H20wIme2Y9V  
eVocS5p9Iau7w9871fBh1odeB+QEWJmav55j8caE1ZhxAYLfrIdXBb1REeuQGjmj  
FuCHf68GgTp9H1Njw921R5q51ntRoh2KmwTA50gbdNnEEAAQ3p8sI+6129FLpLgF  
Z7/wzmknFng40gTLxyPCRV5N6Pbo30wAgjehhQDzC9kEkMxd677t/cadEMUsNHCI  
qTBASchRB+8en5YrUrZ5YUqhNvPR/vvN60dPenX4mbrMSc1v4uxRYSv5ofGHJT0U  
=8hvs  
-----END PGP MESSAGE-----

- 署名されているが暗号化されていない場合。メッセージが署名されている場合は、PGP Desktop 電子メールによって署名の検証が試行されます。そのとき、次の順番で適切な公開鍵が検索されます。① デフォルト鍵リング。② keys.domain 上の鍵サーバー (「domain」は、メッセージ送信者のドメイン名)。③ PGP Global Directory (keyserver.pgp.com)。④ その他設定された鍵サーバー。適切な公開鍵が見つかった場合は、署名の検証が試行され、電子メール クライアントにメッセージが送られます。一方、適切な公開鍵が見つからない場合は、未検証のままメッセージが電子メール クライアントに送られます。
- 暗号化および署名されている場合。メッセージが暗号化および署名されている場合は、最初にメッセージを復号化するための秘密鍵が検索され、次に検証のための公開鍵が検索されます。

## 送信メッセージ

PGP Desktop 電子メールでは、ポリシー (どのような状況に対処できるように設定された一連の指示) に応じて送信メッセージが処理されます。

## デフォルトのポリシー

PGP Desktop 電子メールには、次の 4 つのデフォルトのポリシーが含まれています。

- メーリングリストの管理要求:** メーリング リストへのコマンド送信が、クリア テキスト (暗号化や署名なし) で行われます。
- メーリングリストの送信:** メーリング リストに送信する際、認証用には署名は行われませんが、暗号化はされません。
- 暗号化が必要: [PGP] 機密:** 電子メール クライアント上で機密のフラグが付いているか、件名に「[PGP]」というテキストが含まれているメッセージは、受信者の有効な公開鍵で暗号化しない限り送信されません。このポリシーを使用すると、メッセージは暗号化される必要があり、それ以外の場合は送信されないように簡単にメッセージを処理することができます。
- 暗号化できない場合はそのまま送信:** 送信メッセージを暗号化するための公開鍵が見つからない場合、メッセージはすべて暗号化なしで (クリア テキストで) 送信されます。このポリシーをリストの最後に置いておくと、送信相手に対して暗号化するための鍵が見つからない場合でも、クリア テキストでメッセージが送信されるようになります (ただし、メッセージに機密フラグが付いていない場合に限り)。

## 新しいポリシーの作成

PGP Desktop 電子メールには、4 つのデフォルトのポリシーに加えて、追加の新しいポリシーを作成および使用できる機能が含まれています。さまざまな条件に基づいてポリシーを作成することができます。

メッセージング ポリシーの作成および設定の詳細については『PGP Desktop ユーザー ガイド』を参照してください。

## メッセージが暗号化されているかどうか

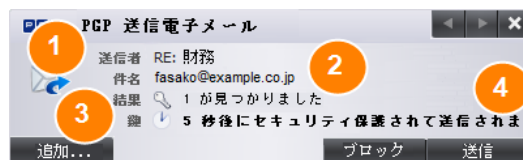
PGP Desktop 電子メールでは作業が自動的にかつ透過的に行われるため、ときとして送信されたメッセージが本当に暗号化されているかどうか確信が持てない場合があります。答えはおそらく暗号化されているということですが、確認する方法もあります。

## 通知機能の警告

PGP Desktop 通知機能の警告は、メッセージの状況を通知し、その管理方法を提供する PGP Desktop 電子メールの機能です。

たとえば、暗号化されたメッセージを送信すると、画面の右下隅に通知機能の警告が表示されます。次の内容が表示されます。

1. 件名
2. 受信者
3. 受信者の見つかった鍵
4. メッセージのステータス



送信されるメッセージについてさらに詳細な情報が必要な場合は、[追加] をクリックします。次の内容が表示されます。

5. PGP Desktop 電子メールがメッセージに対して行った処理
6. メッセージの署名者



通知機能の詳細については、『PGP Desktop ユーザー ガイド』を参照してください。

## PGP ログ

PGP Desktop 電子メールによって実行されるメッセージ保護用のアクションは、すべて PGP ログに記述されます。

たとえば、前述の例で通知機能が表示された送信メッセージでは、PGP ログに次のエントリが生成されています。ログには、次の情報が含まれます。

1. 送信メッセージが送信されたこと、送信者、および件名。

2. 暗号化された時刻、暗号化対象の電子メール アドレス、および送信元の電子メール アドレス。

1 次の件名の Funiko Asako <fasako@example.co.jp> からの送信メッセージを処理しています: 会計結果\_第一四半期  
 2 08:54:30 情報 次の鍵を使用して PGP Partitioned メッセージ (mpa@example.co.jp 宛) を暗号化しています: 'Funiko Asako 08:54:30 情報 <fasako@example.co.jp>' (0xF88C895)

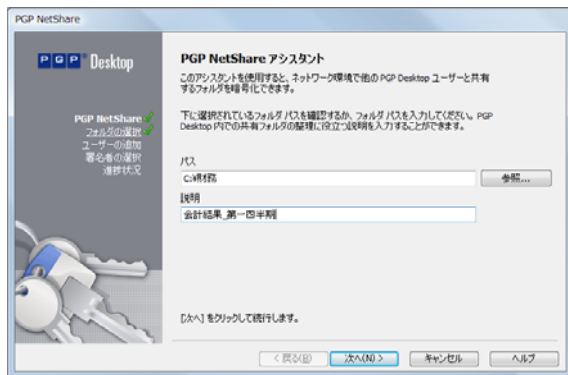
## PGP NetShare の使用

PGP NetShare 機能を使用すると、承認されたユーザーの間で保護されたファイルを共有することができます。最初に保護フォルダを作成し、そのファイルを使用するために承認するユーザーを指定する必要があります。

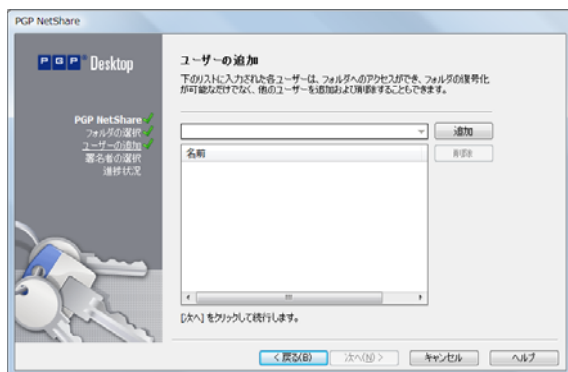
1. [PGP NetShare] コントロール ボックスで、[フォルダの追加] をクリックします。



[フォルダの選択] 画面が表示されます。



2. [参照] をクリックし、保護フォルダにするフォルダを選択します。
3. [説明] フィールドに、作成中の保護フォルダの説明を入力するか、空白のままにしてデフォルトの名前を使用します。
4. [次へ] をクリックします。[ユーザーの追加] 画面が表示されます。



5. 保護フォルダ内のファイルにアクセスできる承認ユーザーを指定するには、下向きの三角形をクリックし、ユーザー

を選択してから [追加] をクリックします。このとき、自分自身も保護フォルダ内のファイルにアクセスする場合は、自分自身も追加してください。

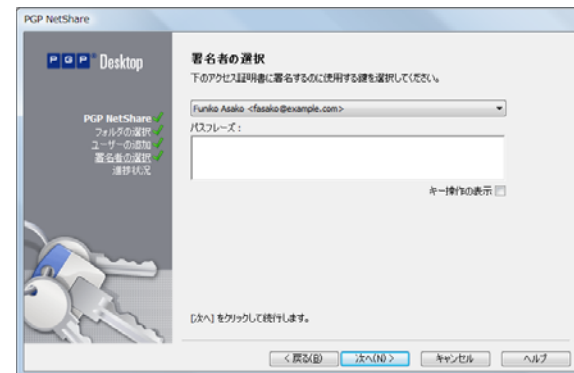
PGP NetShare では、各ユーザーに対して保護ファイルへのアクセスが承認された旨の通知は自動的に行われません。承認された各ユーザーへの通知は、保護フォルダの作成者の責任とします。

6. 各ユーザーに役割を割り当てるには、ユーザー名を右クリックし、次の中から役割を選択します。

- **[管理者]:** PGP NetShare 保護フォルダごとに 1 人の管理者のみを作成します。この役割は、フォルダに対する完全な読み込み/書き込み権限を持ち、ユーザーの追加や削除、および他のユーザーへの役割の割り当てを行うことができます。また、別のユーザーを管理者に昇格させることもできます。
- **[グループ管理者]:** 各 PGP NetShare 保護フォルダに対して、必要な数のグループ管理者を作成します。この役割は、フォルダに対する完全な読み込み/書き込み権限を持ち、ユーザーの追加や削除を行うことができ、別のユーザーを管理者に昇格させることができます。
- **[ユーザー]:** 各 PGP NetShare 保護フォルダに対して、必要な数のユーザーを作成します。この役割は、フォルダに対する完全な読み取り/書き込み権限を持ちます。

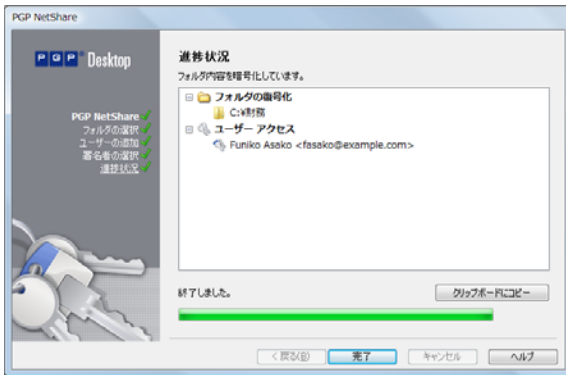
ユーザーの役割は、保護フォルダの作成後にいつでも変更できます。役割を変更するには、PGP Desktop で保護フォルダをクリックし、ユーザー名を右クリックします。

7. [次へ] をクリックします。[署名者の選択] 画面が表示されます。



8. ローカルの鍵リングから秘密鍵を 1 つ選択し、適切なパスフレーズを入力します (パスフレーズがキャッシュされていない場合)。この鍵は、保護フォルダおよびその中のファイルの PGP NetShare 設定情報を安全にするために使用されます。

9. [次へ] をクリックします。[進捗状況] 画面が表示されます。



これで、指定した保護フォルダ内のファイルが暗号化され、指定されたユーザーがファイルを使用できるように承認されました。

10. [完了] をクリックします。

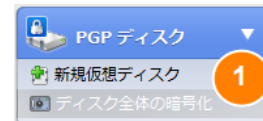
## PGP WDE を使用した ドライブのディスク全体暗号化

PGP WDE 機能を使用すると、システムの内容全体、または指定した外付けドライブや USB フラッシュ ドライブをロックできます。

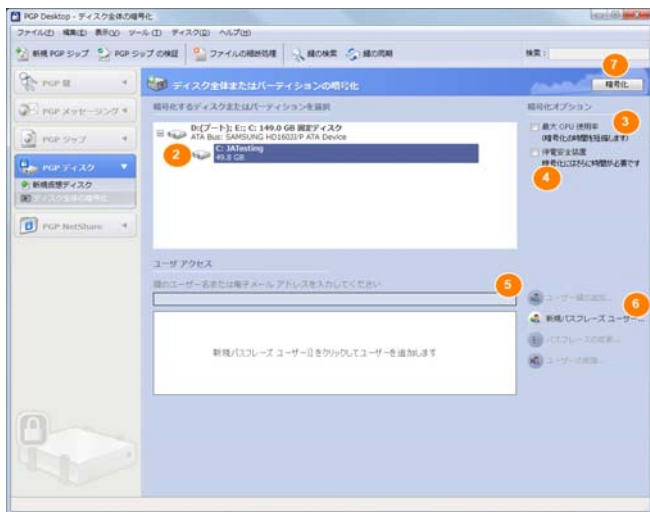
PGP WDE が使用する暗号化アルゴリズムは AES256 です。ハッシュ アルゴリズムは SHA-1 です。FAT16、FAT32、および NTFS でフォーマットされたドライブがサポートされます。最小または最大のサイズ制限はありません。ドライブがオペレーティング システム (またはブートドライブの場合はハードウェア BIOS) でサポートされている場合は、PGP WDE は動作します。

**注意:** ベスト プラクティスとして、ディスクを暗号化する前にデータをバックアップすることをお勧めします。

1. [PGP ディスク] コントロール ボックスの [ディスク全体の暗号化] をクリックします。



2. 暗号化するドライブまたはパーティションを選択します。
3. [最大 CPU 使用率] を選択して、ディスクを直ちに保護します。暗号化プロセスは、システムのその他の操作よりも優先されます。
4. 暗号化プロセス中にシステムの電源が切れる可能性がある場合は、[停電安全装置] を選択します。
- [停電安全装置] が選択されていると、暗号化プロセスは中断した時点から安全に再開します。このオプションを選択すると、完了するのに長い時間がかかることがあります。
5. 公開鍵暗号化方式を使用して、ディスク全体暗号化処理が行われたドライブに対して認証を行うことができるユーザーを追加するには、[ユーザー鍵の追加] をクリックします。
- 固定ドライブを暗号化する際には、Aladdin eToken USB トークン上の PGP 鍵ペアのみ使用できます。パーティションまたはリムーバブル (非固定) ドライブを暗号化する際には、システム上の任意の鍵ペアを使用できます。
6. パスフレーズを使用して認証を行うユーザーを追加するには (USB フラッシュ デバイスを使用して二要素認証を行う場合も含む)、[新規パスフレーズ ユーザー] をクリックします。[PGP ディスク アシスタント] ダイアログ ボックスに表示される指示に従ってください。
- ブート ドライブを暗号化する場合は、Windows ログオン パスフレーズを使用して、起動時に 1 回のみ資格情報を入力するようにすることができます。
7. [暗号化] をクリックします。



**メモ:** フロッピー ディスクまたは CD-RW のデータを暗号化するには PGP 仮想ディスク ボリュームを使用します。PGP WDE は使用しないでください。

PGP ディスク全体暗号化機能はデュアルブート システム上でも使用できますが、PGP ディスク全体暗号化がインストールされている対応オペレーティング システム (Windows XP、Windows 2000、Windows Vista) から起動した場合に限りです。他のオペレーティングシステムは、独立した暗号化されていないパーティションに存在する必要があります。

バックアップ ソフトウェアは、通常どおり PGP WDE と併用できます。ファイルはバックアップされる前に復号化されます。

## PGP WDE のベスト プラクティス

ディスク暗号化の準備に関しては、次のベスト プラクティスを実行することをお勧めします。次の推奨事項に従い、暗号化中のデータおよび暗号化済みのデータを保護してください。

ディスクの初期暗号化を成功させるためには、ディスクを暗号化する前に次のタスクを実行する必要があります。

1. **対象ディスクのサポートを確認します。**PGP WDE 機能は、デスクトップまたはラップトップのディスク (パーティション、またはディスク全体のいずれか)、外付けディスク、および USB フラッシュ ディスクを保護します。CD-RW、DVD-RW、およびサーバーはサポートされていません。サポートされるディスクの種類についての詳細は、『PGP Desktop ユーザー ガイド』の「サポートされるディスクの種類」を参照してください。
2. **ディスクを暗号化する前に、ディスクをバックアップします。**ラップトップまたはコンピュータがなくなったり、盗まれたり、ディスクを復号化できなくなったりした場合にデータを失わないよう、ディスクを暗号化する前に必ずバックアップしてください。
3. **ディスクを暗号化する前に、ディスクに問題がないことを確認します。**暗号化中に PGP WDE によってディスク エラーが検出された場合には、ディスク エラーを修復できるように暗号化が中断されますが、暗号化を開始する前にエラーを修復した方が効率的です。詳細については、「暗号化する前にディスクに問題がないことの確認」(8 ページ) を参照してください。
4. **リカバリ ディスクを作成します。**PGP ディスク全体暗号化

によって保護されているブート ディスクまたはパーティションでマスター ブート レコードが損傷する可能性は極めて低いと言えますが、ゼロではありません。PGP ディスク全体暗号化を使用してブート ディスクまたはパーティションを暗号化する前に、リカバリ ディスクを作成してください。リカバリ ディスクの作成方法については、「リカバリ CD の作成」(8 ページ)を参照してください。

5. **AC 電源を確保します (暗号化プロセス中)。**「暗号化中の電源の確保」(9 ページ) を参照してください。
6. **パイロット テストを実行し、ソフトウェアの互換性を確認します。**優良なセキュリティ プラクティスとして、少数のコンピュータで PGP WDE をテストし、PGP WDE がコンピュータ上の他のソフトウェアと競合しないことを確認してから多数のコンピュータに PGP WDE を展開することをお勧めします。この方法は、標準化された企業業務環境 (COE) イメージを採用する環境では特に有効です。PGP WDE との互換性で問題が確認されているソフトウェアのリストについては、「ソフトウェアの互換性を確認するパイロット テストの実行」(9 ページ) を参照してください。
7. **ディスク リカバリは復号化されたディスクに実行します。**ディスク全体暗号化 (WDE) によって保護されているディスク上でディスクのリカバリ アクティビティを実行する必要がある場合、可能であれば、ベスト プラクティスとして、最初にディスクを復号化することをお勧めします。この処理は、PGP Desktop の [ディスク] > [復号化] オプションで作成済みの PGP WDE リカバリ ディスクを使用するか、または USB ケーブルでこのハード ディスクを第 2 システムに接続し、第 2 システムの PGP Desktop ソフトウェアによって復号化します。ディスクを復号化したら、リカバリ アクティビティを続行します。

## 暗号化する前にディスクに問題がないことの確認

当社は、ドライブを暗号化する場合には意図的に慎重な姿勢を取り、データの喪失を防止しています。ハード ディスクの暗号化処理中に巡回冗長検査 (CRC) エラーが発生することは、珍しくありません。不良のセクターを含むハード ドライブまたはパーティションが PGP WDE によって検出された場合、暗号化プロセスはデフォルトで中断されます。このように中断することで暗号化プロセスを続行する前に問題を修復し、起こり得るディスクの損傷やデータの喪失を回避できます。

暗号化中の損傷を回避するために、暗号化の前にすべてのディスク エラーを修正して問題のないディスクで暗号化を開始することをお勧めします。

- PGP WDE を使用する前に、低レベルの統合性チェックを実行できるサードパーティのスキャン ディスク ユーティリティを使用し、CRC エラーの原因になり得るドライブとの不整合をすべて修復してください。Microsoft Windows のチェック ディスク (chkdsk.exe) ユーティリティでは、対象ハード ドライブ上のこれらの問題を十分に検出できません。代わりに、SpinRite、Norton Disk Doctor™ などのソフトウェアを使用してください。これらのソフトウェア アプリケーションを使用することにより、暗号化を中断させるようなエラーを修正できます。
- ベスト プラクティスとして、暗号化する前に、細かく断片化されたディスクをデフラグすることをお勧めします。

## リカバリ CD の作成

次の手順では、説明を目的として Roxio ソフトウェアを使用

しています。実際の手順は異なる可能性があります。

1. PGP Desktop および Roxio Easy Media Creator または Roxio Easy CD Creator (もしくは ISO イメージから CD を作成できる他のソフトウェア) がシステムにインストールされていることを確認します。
2. Roxio Easy Media Creator または Roxio Easy CD Creator を開き、データ CD プロジェクトの作成を選択します。
3. [ファイル] メニューの [CD イメージから CD を記録] を選択します。
4. [ファイルの種類] メニューの [ISO イメージ ファイル (ISO)] を選択します。
5. PGP ディレクトリにナビゲートします。デフォルトでは、C:\Program Files\PGP Corporation\PGP Desktop\ です。
6. bootg.iso ファイルを選択し、[開く] をクリックします。
7. システムの CD ドライブに空の書き込み可能 CD を挿入します。
8. [レコード CD のセットアップ] 画面で [記録の開始] をクリックします。
9. ファイルが CD に焼かれたら、[OK] をクリックします。
10. ドライブからリカバリ CD を取り出し、適切なラベルを貼ります。

**注意:** PGP WDE リカバリ ディスクと互換性があるのは、このリカバリ CD が作成された PGP Desktop のバージョンのみです。たとえば、バージョン 9.0.x のリカバリ ディスクを使用して PGP WDE 9.8 ソフトウェアによって保護されているディスクを復号化する場合、PGP WDE 9.8 ディスクは作動不能になります。

### 暗号化中の電源の確保

暗号化は CPU に負担のかかるプロセスなので、バッテリー電源で稼動するラップトップコンピュータでは暗号化を開始できません。暗号化を実行するコンピュータでは、AC 電源を使用する必要があります。初期暗号化プロセス (または後の復号化プロセスや再暗号化プロセス) 中にラップトップコンピュータがバッテリー電源に切り替わった場合、PGP WDE のアクティビティは中断されます。AC 電源に戻すと、暗号化プロセス、復号化プロセス、または再暗号化プロセスが自動的に再開されます。

どのタイプのコンピュータを使用する場合でも、システムの電源を切断してはいけません。暗号化プロセス中にシステムの電源が切断された場合、[停電安全装置] オプションを選択していなければ、システムが突然シャットダウンします。

暗号化プロセスが終わるまでは、システムから電源コードを引き抜かないでください。暗号化中に停電する可能性がある場合、またはコンピュータに無停電電源装置が搭載されていない場合は、『PGP Desktop ユーザー ガイド』に記載されているように [停電安全装置] オプションの選択を検討してください。

**注意:** これは、USB デバイスなどのリムーバブル ディスクにも該当します。[停電安全装置] オプションを選択していない場合、暗号化中にリムーバブル ディスクを取り外すと、デバイスを損傷する危険があります。

## ソフトウェアの互換性を確認するパイロットテストの実行

一部のディスク保護ソフトウェアと PGP WDE には互換性がありません。また、これらのソフトウェアによってディスク上でデータの喪失を含む深刻な問題が発生する可能性があります。

次の既知の非互換性の問題に注意し、このリストの最新のアップデートについて PGP Desktop のリリース ノートを読み直してください。

互換性のないソフトウェアは次のとおりです。

- Faronics Deep Freeze (全エディション)
- Utimaco Safeguard Easy 3.x
- GuardianEdge Technologies 社のハードディスク暗号化製品: 以前 PC Guardian 製品として知られる Encryption Anywhere Hard Disk および Encryption Plus Hard Disk 製品。

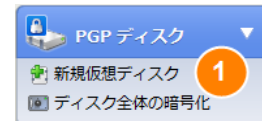
次の各アプリケーションは、PGP Desktop がインストールされたシステムでも正しく機能しますが、PGP ディスク全体暗号化機能をブロックします。

- Safeboot Solo
- SecureStar SCPP

## PGP 仮想ディスク ボリュームの作成

PGP 仮想ディスク ボリューム機能では、ハード ドライブ領域の一部に独自のドライブ文字を割り当て、暗号化された仮想ディスク ボリュームとして使用できます。また、ボリュームに対して追加ユーザーを作成して、承認したユーザーがそのボリュームにアクセスできるようにすることもできます。

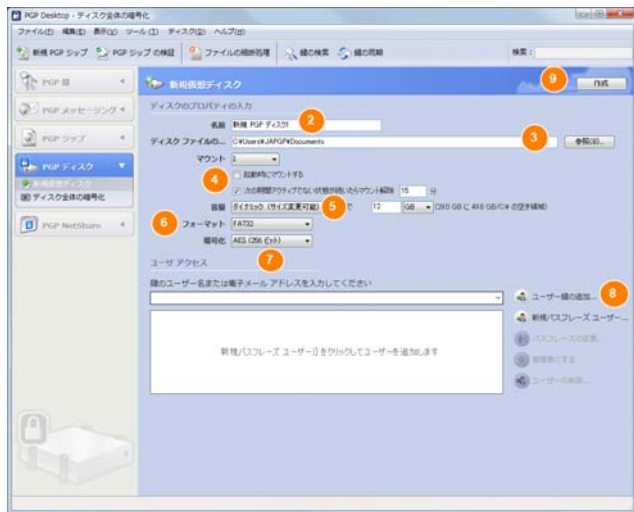
1. [PGP ディスク] コントロール ボックスで [新規仮想ディスク] をクリックします。



2. ボリュームの [名前] を入力します。
3. ボリュームの [ディスク ファイルの場所] を指定します。
4. マウントの設定を選択します。
  - ボリュームのドライブ文字を [マウント] に選択します。
  - 新しい仮想ボリュームがコンピュータの起動時に自動的にマウントされるようにするには [起動時にマウントする] をオンにします。
  - 指定した時間 (分単位) ボリュームが使用されない場合に自動的にマウントを解除するには [次の期間アクティブでない状態が続いたらマウント解除] をオンにします。
5. ファイルが追加されるにつれてボリュームの容量が増加するように設定するには、[容量] から [ダイナミック (サイズ変更可能)] を選択します。ボリュームの容量が常に一定に保たれるようにするには、[固定サイズ] を選択します。
6. ボリュームのファイル システム形式を [フォーマット] で指定します。
7. ボリュームの暗号化に使用するアルゴリズムを [暗号化] で

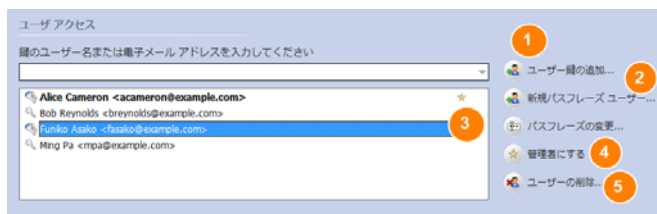
指定します。

- 公開鍵暗号化方式を使用して認証を行うユーザーを追加するには [ユーザー鍵の追加] をクリックし、パスフレーズを使用して認証を行うユーザーを選択するには [新規パスフレーズユーザー] をクリックします。
- [作成] をクリックします。



PGP 仮想ディスク ボリュームの既存のユーザーを管理するには [ユーザー アクセス] セクションを使用します。

- 公開鍵暗号化方式を使用して認証を行うユーザーを追加するには、[ユーザー鍵の追加] をクリックします。
- パスフレーズを使用して認証を行うユーザーを追加するには、[新規パスフレーズユーザー] をクリックします。
- パスフレーズユーザーのパスフレーズを変更するには、そのユーザーを選択し、[パスフレーズの変更] をクリックします。
- ユーザーに管理者権限を付与するには、そのユーザーを選択し、[管理者にする] をクリックします。
- ユーザーを削除するには、そのユーザーを選択し、[削除] をクリックします。



## PGP ジップ アーカイブの作成

PGP ジップ アーカイブを使用すると、圧縮されたアーカイブに、ファイルやフォルダを自由に追加できます。PGP ジップ アーカイブには次の 4 種類があります。

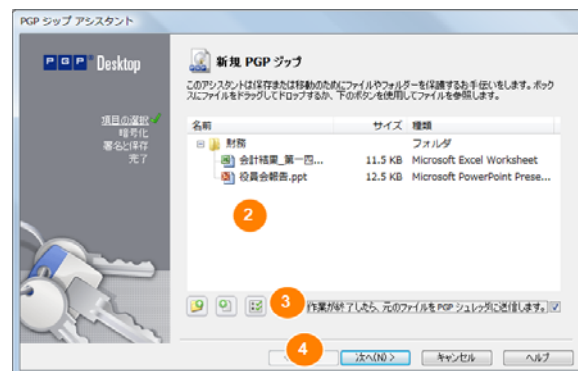
- 受信者鍵:** アーカイブを公開鍵で暗号化します。対応する秘密鍵の所有者のみがアーカイブを開くことができます。これが最も安全な PGP ジップ アーカイブです。受信者は、PGP ソフトウェア (Windows 版または Mac OS X 版) を使用する必要があります。
- パスフレーズ:** アーカイブをパスフレーズで暗号化します。これは受信者に伝える必要があります。受信者は、PGP ソフトウェア (Windows 版または Mac OS X 版) を使用する必要があります。
- PGP 自己復号化アーカイブ:** アーカイブをパスフレーズで暗号化します。受信者はアーカイブを開くのに PGP ソフトウェアを使用する必要はありませんが、Microsoft Windows が稼動しているコンピュータでなければなりません。パスフレーズは受信者に伝える必要があります。
- 署名のみ:** アーカイブを暗号化せずに署名することで、ユーザーが送信者であることを証明します。受信者は、アーカイブを開いて検証するのに、PGP ソフトウェア (Windows 版または Mac OS X 版) を使用する必要があります。

パスフレーズおよび署名のみの PGP ジップの詳細については、『PGP Desktop ユーザー ガイド』を参照してください。ここでは簡単に説明します。

- [PGP ジップ] コントロール ボックスで、[新規 PGP ジップ] をクリックします。



- アーカイブに含めるファイルやフォルダをドラッグ アンド ドロップするか、ボタンを使用してそれらを選択します。
- アーカイブを作成した後、元のファイルやフォルダを細断処理するには、[作業が終了したら、元のファイルを PGP シュレッドに送信します] を選択します。
- [次へ] をクリックします。



- PGP ジップ アーカイブの種類を選択します。

- [受信者鍵]
- [パスフレーズ]

- [PGP 自己復号化アーカイブ]
- [署名のみ]

6. [次へ] をクリックします。



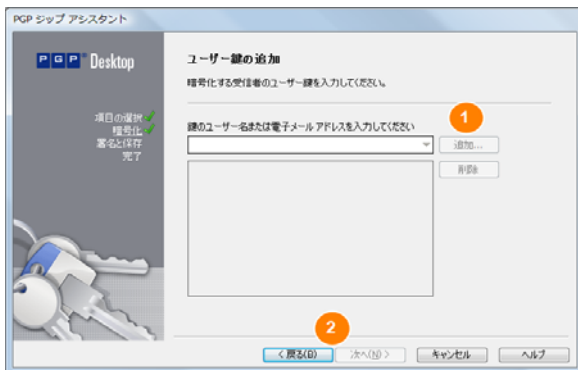
[パスワード] および [署名のみ] の詳細については、『PGP Desktop ユーザーガイド』を参照してください。

指定した PGP ジップ アーカイブの種類に応じて、後に続くページの適切なセクションを参照してください。

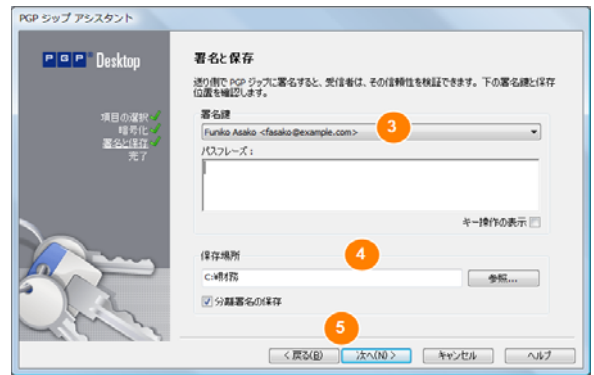
## 受信者鍵

[ユーザー鍵の追加] 画面が表示されます。

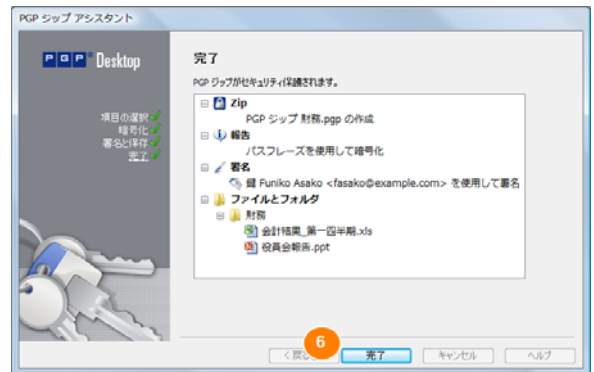
1. [追加] をクリックし、[ユーザー選択] 画面を使用して、アーカイブを開けるようにするユーザーの公開鍵を選択します。自分自身でアーカイブを開けるようにするには、ご自分の公開鍵を含めるようにしてください。
2. [次へ] をクリックします。



3. アーカイブに署名するために使用するローカル システム上の秘密鍵を選択します。
4. アーカイブの名前および場所を指定します。デフォルトの名前はアーカイブの最初のファイルまたはフォルダの名前であり、デフォルトの場所はアーカイブに含めるファイルやフォルダの場所です。
5. [次へ] をクリックします。PGP ジップ アーカイブが作成されます。[完了] 画面に新しいアーカイブに関する情報が表示されます。



6. [完了] をクリックします。



**メモ:** PGP ジップ アーカイブの種類のパスワードは、受信者鍵とよく似ています。異なる点は、鍵の代わりにパスワードがアーカイブを保護するために使用されることです。

**メモ:** PGP ジップ アーカイブの種類の署名のみは、受信者鍵と似ています。異なる点は、アーカイブが署名のみされていて暗号化されていないため、公開鍵を選択しないことです。

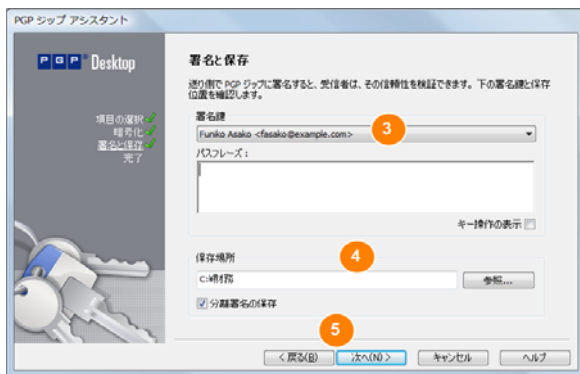
## PGP 自己復号化アーカイブ

[パスワードの作成] 画面が表示されます。

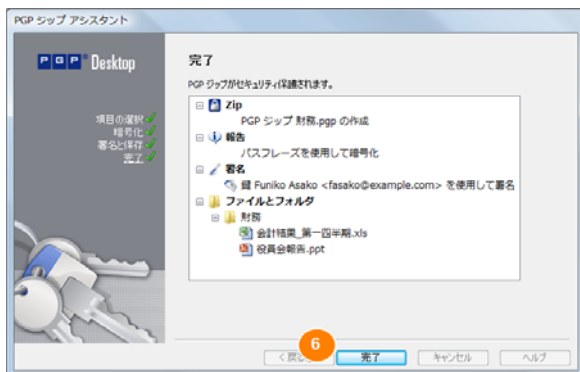
1. PGP ジップ自己復号化アーカイブ (SDA) のパスワードを入力し、パスワードをもう一度入力します。
2. [次へ] をクリックします。



3. アーカイブに署名するために使用するローカル システム上の秘密鍵を選択します。
4. アーカイブの名前および場所を指定します。デフォルトの名前はアーカイブの最初のファイルまたはフォルダの名前であり、デフォルトの場所はアーカイブに含めるファイルやフォルダの場所です。



5. [次へ] をクリックします。PGP SDA が作成されます。



6. [完了] をクリックします。

## ファイルの細断処理

PGP シュレッタ機能では、ファイルおよびフォルダが完全に破壊されるので、高度なファイル回復ソフトウェアを使用しても回復できません。デスクトップには [PGP シュレッタ] と Windows の [ごみ箱] の両方のアイコンが表示されますが、PGP シュレッタだけが、指定したファイルを直ちに上書きし、回復不可能にします。

次のいずれかの方法で、ファイルを細断処理できます。

- [PGP シュレッタ] アイコンを使用する
- PGP ツールバーを使用する
- PGP コンテキスト メニューを使用する

### [PGP シュレッタ] アイコンの使用

- [PGP シュレッタ] アイコンを使用してファイルを細断処理するには、次の操作を行います。

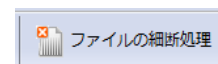
1. Windows デスクトップで、細断処理するファイルおよびフォルダを PGP シュレッタにドラッグします。ファイルを細断処理するかどうかを確認するダイアログが表示されます。
2. [はい] をクリックします。指定したファイルおよびフォルダが細断処理されます。



## PGP ツールバーの使用

- PGP ツールバーを使用してファイルを細断処理するには、次の操作を実行します。

1. PGP Desktop を開きます。
2. PGP ツールバーの [ファイルの細断処理] をクリックします。
3. 細断処理するファイルを指定します。
4. Ctrl キーを押しながらクリックして複数のファイルを選択することも、Ctrl キーを押しながら A キーを押すことですべてのファイルを選択することもできます。
5. [開く] をクリックします。ファイルを細断処理するかどうかを確認するダイアログが表示されます。
6. [はい] をクリックします。指定したファイルおよびフォルダが細断処理されます。



## PGP コンテキスト メニューの使用

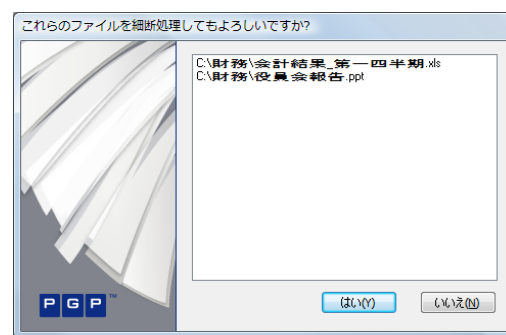
- Windows エクスプローラからファイルを細断処理するには、次の操作を実行します。

1. Windows エクスプローラを開きます。
2. 細断処理するファイルまたはフォルダを右クリックし、[PGP Desktop] > [<ファイル名> の PGP 細断処理] を選択します。Ctrl キーを押しながらクリックして複数のファイルを選択することも、Ctrl キーを押しながら A キーを押すことですべてのファイルを選択することもできます。

**ヒント:** 複数のファイルを選択した場合は、テキストで [PGP 細断処理の件数: X] と表示されます。ここで、「X」は、選択されたファイル数を示します。

ファイルを細断処理するかどうかを確認するダイアログが表示されます。

3. [はい] をクリックします。指定したファイルおよびフォルダが細断処理されます。



**メモ:** PGP シュレッタ機能を頻繁に使用しない場合は、[PGP オプション] を介して、デスクトップから [PGP シュレッタ] アイコンを削除できます。これを行うには、[ツール] > [オプション] を選択して [ディスク] タブをクリックし、[Windows デスクトップ上に [PGP シュレッタ] アイコンを置く] オプションを選択解除し、[OK] をクリックします。

**メモ:** [PGP オプション] を使用して、細断するときには作成されるパスの数 (パスが多くなれば安全になりますが長くなります)、Windows のごみ箱を空にしたときに中のファイルを細断処理するかどうか、および細断処理するときに警告ダイアログを表示するかどうかを管理できます。

## 空き領域の細断処理

PGP 空き領域細断処理機能は、ご使用のドライブの空き領域を完全に細断処理するので、削除したデータが完全に回復不可能となります。「空き領域」は実際には誤った呼称であることに注意してください。PGP 空き領域細断処理は、Windows が空と認識するハード ドライブの一部を上書きします。実際には、その領域は空であるか、Windows が削除したと示すファイルを保持している場合があります。

Windows のごみ箱にファイルを入れて空にしても、ファイルは実際には削除されません。Windows はそこに何もなかったように動作し、最終的にファイルを上書きします。それらのファイルが上書きされるまでは、攻撃者がそのファイルを回復することは容易なことです。PGP 空き領域細断処理は、この「空き領域」を上書きするので、ディスク回復ソフトウェアを使用してもそれらのファイルを元に戻すことはできません。

### ➤ ディスクの空き領域を細断処理するには、次の操作を実行します。

1. PGP Desktop を開きます。
2. [ツール] メニューから [PGP 空き領域細断処理] を選択します。
3. 最初の画面で説明を読み、[次へ] をクリックします。
4. [情報の収集] 画面の [ドライブの細断処理] ボックスで、細断処理するディスクまたはボリューム、および PGP 空き領域細断処理が実行するパスの数を選択します。

パス数を選択する際には、次のガイドラインを参考にしてください。

- 個人ユーザー: 3 パス
- 商用: 10 パス
- 軍事用: 18 パス
- 最大限のセキュリティ: 26 パス



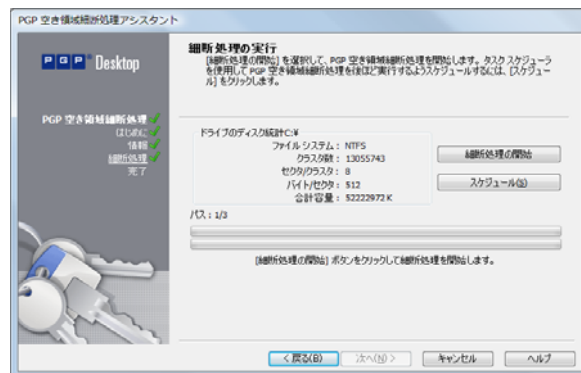
5. NTFS 内部データ構造を抹消するかどうかを選択 (すべてのシステムで使用可能ではありません) し、[次へ] を選択します。

このオプションを使用すると、細断処理されていない可能性のある、内部データ構造の小さい (1 K 未満) ファイルが細断処理されます。

6. [細断処理の実行] 画面で、[細断処理の開始] をクリックします。

**メモ:** 空き領域の細断処理を今実行する代わりに、[スケジュールを設定] をクリックして、スケジュールを設定することができます。Windows タスク スケジューラがインストールされていることを確認してください。

空き領域の細断処理プロセスの長さは、指定したパスの数、プロセッサの速度、実行している他のアプリケーションの数などに左右されます。



7. 細断処理セッションが完了したら [次へ] をクリックします。
8. [完了] 画面で、[完了] をクリックします。

## サポート情報

### テクニカル サポートへのお問い合わせ

- PGP サポート オプションと PGP テクニカル サポートへのお問い合わせ方法の詳細については、PGP Corporation のサポート ホームページ (<http://www.pgp.com/support>) を参照してください。
- PGP サポート のナレッジベースにアクセスしたり、PGP テクニカル サポートにサポートを依頼したりするには、PGP サポート ポータル ウェブサイト (<https://support.pgp.com>) を参照してください。サポート契約がない場合でも PGP サポート ナレッジ ベースの一部にアクセスできますが、テクニカルサポートにサポートを依頼するには、有効なサポート契約が必要です。
- その他の PGP Corporation へのお問い合わせについては、PGP 連絡先ページ (<http://www.pgp.com/company/contact/index.html>) にアクセスしてください。
- PGP Corporation の概要については、PGP の Web サイト (<http://www.pgp.com>) にアクセスしてください。
- PGP サポート フォーラムにアクセスするには、PGP サポート フォーラム (<http://forums.pgpsupport.com>) にアクセスしてください。PGP Corporation が主催するユーザー コミュニティのサポート フォーラムがあります。

### 入手可能なマニュアル

インストール前に、すべての製品マニュアルを PGP サポート のナレッジベース (<https://support.pgp.com/?faq=589>) よりご覧いただけます。

PGP Desktop のマニュアルは、ソフトウェアのインストール中にコンピュータにインストールされます。マニュアルを表示するには、[スタート] > [プログラム] > [PGP] > [マニュアル] を選択します。マニュアルはすべて、Adobe Acrobat PDF ファイルとして保存されています。これらのファイルは、Adobe 社ウェブサイト (<http://www.adobe.com/jp/>) より入手可能な

Adobe Acrobat Reader を使って閲覧および印刷ができます。  
PGP Desktop には、Windows のオンライン ヘルプも含まれています。

## 著作権および商標

Copyright © 1991-2009 PGP Corporation. All Rights Reserved.  
「PGP」、「Pretty Good Privacy」および PGP ロゴは米国およびその他の国における PGP Corporation の登録商標です。本リリースノートに記載されているその他すべての登録商標および未登録商標は、各所有企業に帰属します。