PGP Desktop 電子メール

クイック スタート ガイド
バージョン 9.10

PGP Desktop 電子メールとは

PGP Desktop 電子メールは、PGP Desktop ファミリーのアプリケーションの 1 つです。PGP Desktop 電子メールでは、次の操作を行えます。

- 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かつ透過的に行う。
- 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。
- 安全に保護され、暗号化されたジップ アーカイブを作成する。
- PGP Desktop 電子メール、または 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電子メール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* (2 ページ)
- *PGP Desktop 電子メールのインストール* (3 ページ)
- *PGP Desktop 電子メールの起動* (3 ページ)
- *PGP Desktop 電子メールのメイン画面* (3 ページ)
- *PGP 仮想ディスク ボリュームの作成* (6 ページ)
- *PGP ジップ アーカイブの作成* (6 ページ)
- *ファイルの細断処理* (9 ページ)
- *空き領域の細断処理* (9 ページ)
- *サポート情報* (11 ページ)

初めて PGP Desktop 電子メール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 電子メール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 電子メール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 電子メール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 電子メールのライセンスは、特定の PGP Desktop 電子メール機能へのアクセスを可能にします。PGP Desktop 電子メール機能の中には、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 電子メールの導入、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

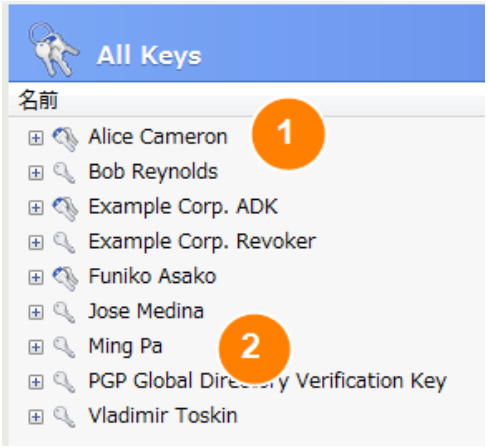
インストール後に、PGP Desktop 電子メールに PGP 鍵ペアを作成するよう表示されます。鍵ペアとは、秘密鍵と公開鍵の組み合わせのことをいいます。

- 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たり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 電子メールでは、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 電子メール 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 Desktop 電子メールには、次のコンポーネントが含まれています。

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 ソフトウェア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 電子メールでは、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限られます。

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

PGP Desktop 電子メールのインストール

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 電子メールを使用する場合、PGP Desktop 電子メール 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。

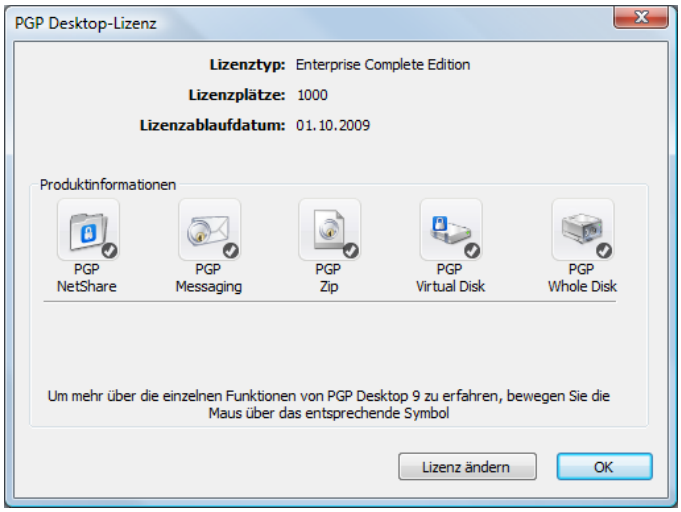
➢ PGP Desktop 電子メールをインストールするには、次の操作を実行します。

1. ダウンロードした PGP Desktop 電子メール 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。
2. インストール プログラムをダブルクリックします。
3. 画面に表示される指示に従います。
4. 指示に従ってシステムを再起動します。
5. システムの再起動後、画面上の指示に従って PGP Desktop 電子メールの設定を行います。

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 電子メールを起動し、**[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 電子メールの起動

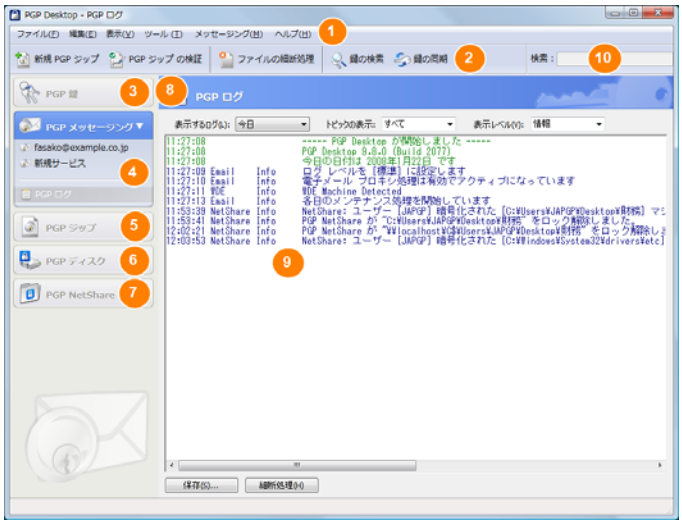
PGP Desktop 電子メールを起動するには、次のいずれかの方法を使用します。

- [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 電子メールを開く]** を選択する。
- **[スタート]** メニューで、**[プログラム] > [PGP] > [PGP Desktop 電子メール]** を選択する。

PGP Desktop 電子メールのメイン画面

PGP Desktop 電子メール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 電子メールのメイン画面には、次の要素が含まれます。

1	**メニュー バー:** PGP Desktop 電子メール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 電子メール作業領域:** 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に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 サーバーの間で稼動し、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/0f5F8QKtY+1NVzwQW4xQ/EPu0D0mLrMZVVNQVn
rYvHPoSAcn6C3zFpO996akjRioOBGa62hkLpkjQi3QEGpBtqMP1F64TUxqHkpLNH
ISN+7zEA7EYTtV+3ErREOH6yQgJ+sQGm6sjRjddYYvTG6hGa9f2wX+ZDLAIK65rA
f4ZNQfNvkowMmJXS78Sz7LEGE5d5wM68kkB/FflvfYz1w360QgauIXmom9F8294p
fNaWAnhQlRif/la/MuYs0WkTLPQpdBXhgZqVKaE85gsCrwqXfMAGDEYfrsCAb1Ne
nMWJNtXsRYVpstmpNBZuVHOljKrXE4YEAPk48MOD1Yi54NJxYwvury79oDoxDljh
o9yh9v5fO71orpLFceW8wmLX4qJaGdsOVqdwQRRnfwbwnbgsdljD2cmijyOq+bcy
3hZknIEGbb7GTKaKo1cj+y9uSaFDh49lA9qLyHTWWLuHYV/j/wtBPfPZpjGYvACV
FqRDEO8hYzxKc/foQwlIMdo+nymZEQItTTdBCaESxm5V+jBWfnOxhUK/EVylkAHm
n27x2m9PdwzxriQjgrxI8Lda7DTJWYmA8ol2OClQZqrqvAmqIKL4CpCkyhPuRwIg
nan8OKN/USfzK+Vi9juxM1lS5oGYzODtL6KnLnGGpTlu6yLsU25B7iIbVe330ukj
zMLXgdLAKQFSItPMVeKqJPxQrMrLlEYr6hE7fcAYmUMwXe8w60e7H2OwEIme2Y9V
eVocs5p9Iau7w987Ifbh1odEb+QEwJMavV5jBcaE1ZhxAYLfrIdXBb1REeuQGjmj
FuCHf6BGgTp9HlNjw92iR5qSintROh2KmwTa5oGbDNnEEAAQJp8sI+6129FLpLgF
z7/wzmnKFngV4OgILxyPCRvS6Pbo30wAgJehhqDzC9kEkmXd6J7t/caDEMUsnHC1
qTBASchRB+8eN5yrUrZ5YUqhNvpR/vVN6odPEnX4mbrMsClv4uXRYSv5ofGHJTOU
=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 (どのような状況にでも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、

認証用に署名は行われますが、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る)。

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 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。ログには、次の情報が含まれます。

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。

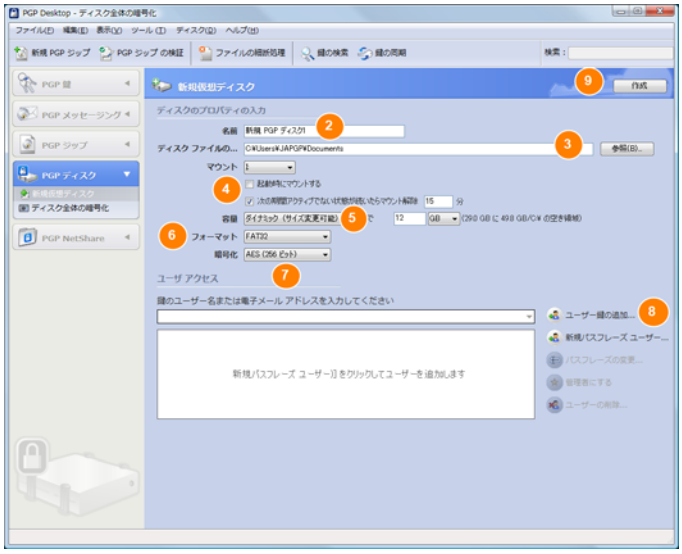
1. 送信メッセージが送信されたこと、送信者、および件名。
2. 暗号化された時刻、暗号化対象の電子メール アドレス、および送信元の電子メール アドレス。

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。

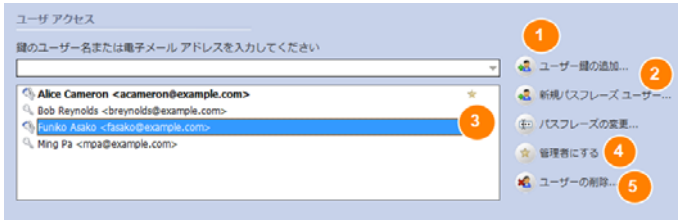
1. [PGP ディスク] コントロール ボックスで **[新規仮想ディスク]** をクリックします。

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。
8. 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。
9. **[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。

1. 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。
2. 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。
3. 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。
4. 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。
5. 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。

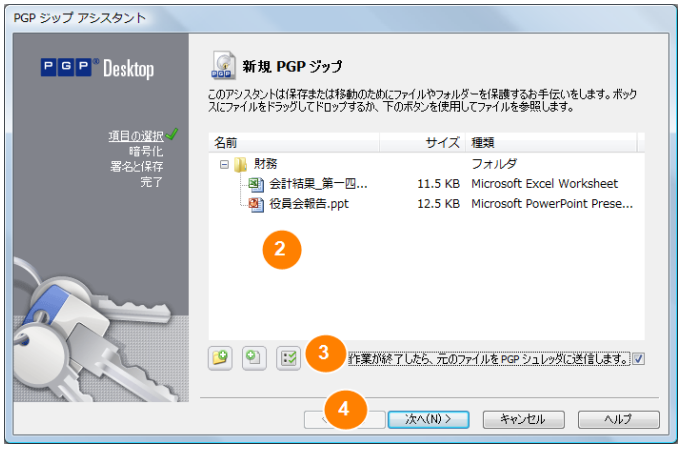
- **受信者鍵**: アーカイブを公開鍵で暗号化します。対応する秘密鍵の所有者のみがアーカイブを開くことができます。これが最も安全な PGP ジップ アーカイブです。受信者は、PGP ソフトウェア (Windows 版または Mac OS X 版) を使用する必要があります。
- **パスフレーズ**: アーカイブをパスフレーズで暗号化します。これは受信者に伝える必要があります。受信者は、PGP ソフトウェア (Windows 版または Mac OS X 版) を使用する必要があります。

- **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が、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がありませんが、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。

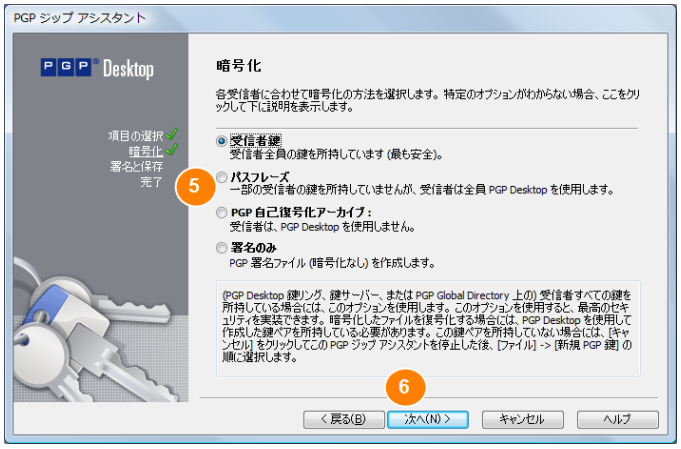
パスフレーズおよび署名のみの PGP ジップの詳細については、『*PGP Desktop ユーザー ガイド*』を参照してください。ここでは簡単に説明します。

1. [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。

2. 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。
3. 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 シュレッダに送信します]** を選択します。
4. **[次へ]** をクリックします。



5. 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。



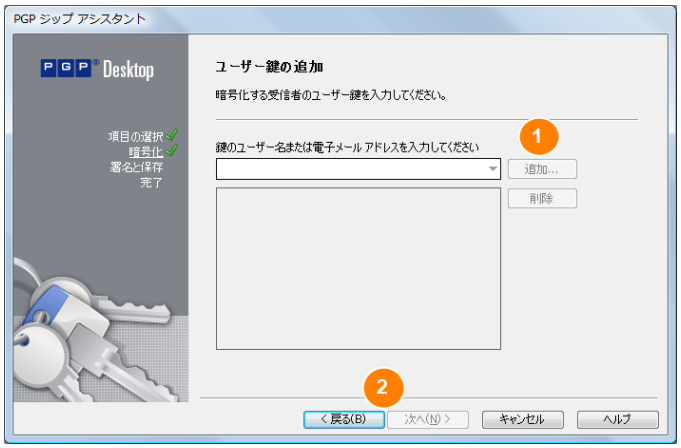
[パスフレーズ] および **[署名のみ]** の詳細については、『*PGP Desktop ユーザー ガイド*』を参照してください。

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

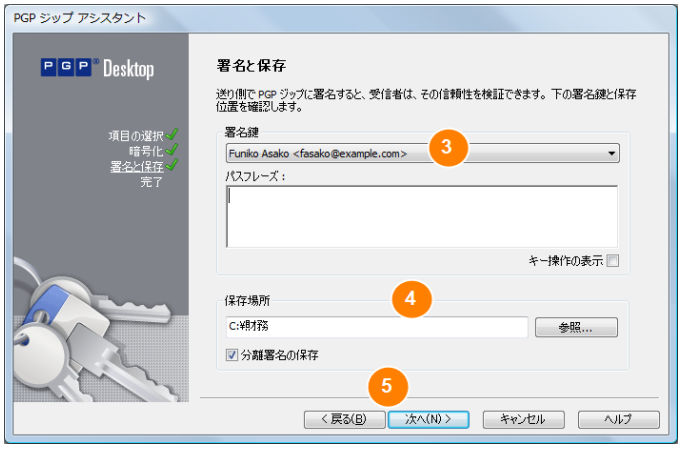
[ユーザー鍵の追加] 画面が表示されます。

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。

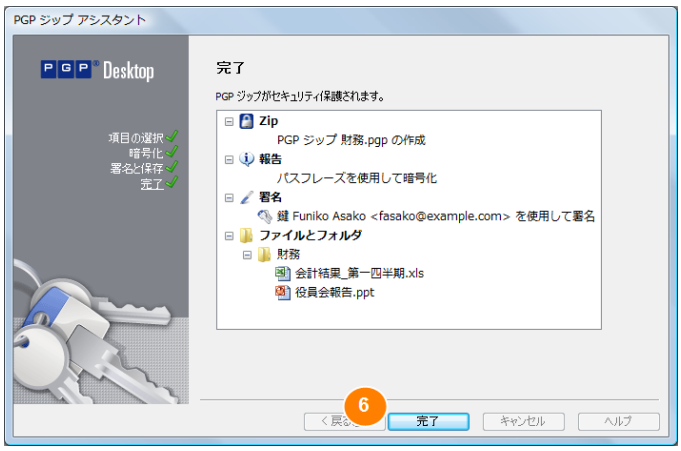


3. アーカイブに署名するために使用するローカル システム上の秘密鍵を選択します。
4. アーカイブの名前および場所を指定します。デフォルトの名前はアーカイブの最初のファイルまたはフォルダの名前であり、デフォルトの場所はアーカイブに含めるファイルやフォルダの場所です。

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フレーズは、受信者鍵とよく似ています。異なる点は、鍵の代わりにパスフレーズがアーカイブを保護するために使用されることです。

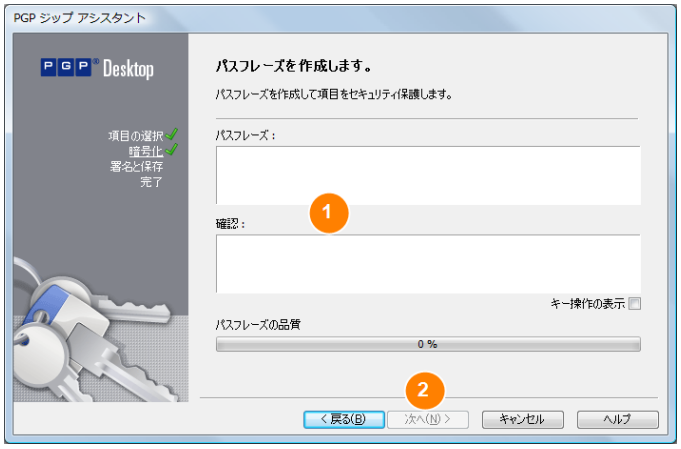
メモ: PGP ジップ アーカイブの種類の署名のみは、受信者鍵と似ています。異なる点は、アーカイブが署名のみされていて暗号化されていないため、公開鍵を選択しないことです。

PGP 自己復号化アーカイブ

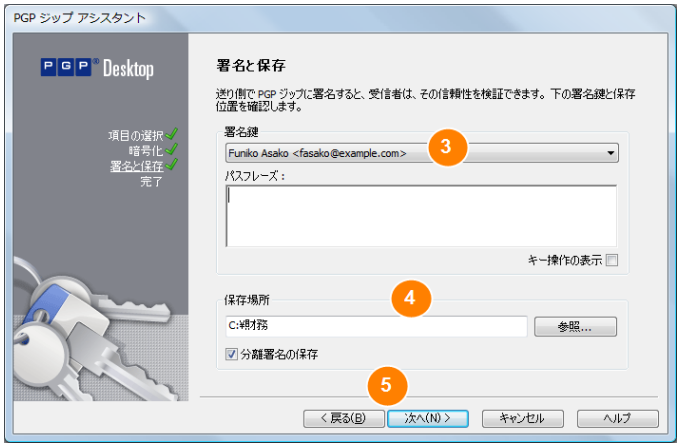
[パスフレーズの作成] 画面が表示されます。

1. PGP ジップ自己復号化アーカイブ (SDA) のパスフレーズを入力し、パスフレーズをもう一度入力します。

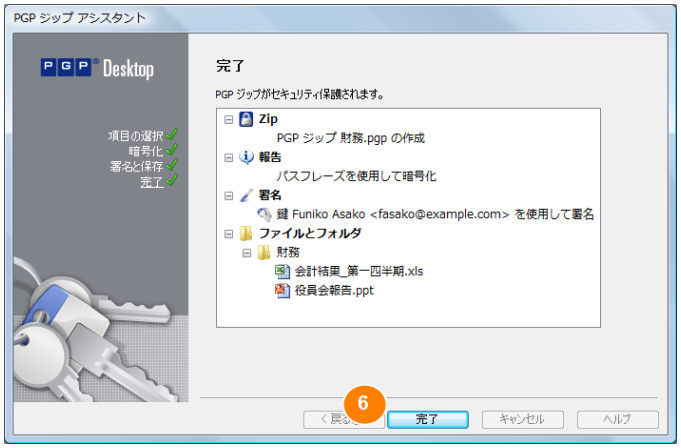
2. **[次へ]** をクリックします。



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 シュレッダ機能では、ファイルおよびフォルダが完全に破棄されるので、高度なファイル回復用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 シュレッダ] と Windows の [ごみ箱] の両方のアイコンが表示されますが、PGP シュレッダだけが、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 シュレッダ] 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 シュレッダ] アイコンの使用

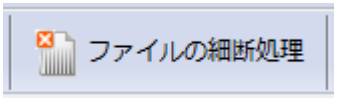
➢ [PGP シュレッダ] アイコンを使用してファイルを細断処理するには、次の操作を行います。

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 シュレッダにドラッグします。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 電子メールを開きます。
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。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指定することもできます。
4. **[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。
5. **[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

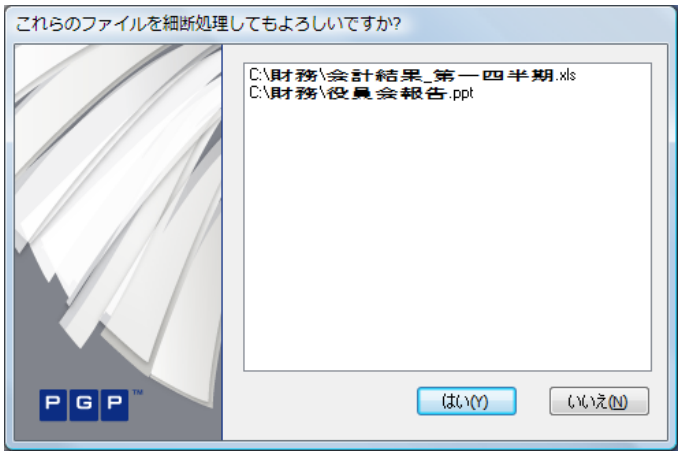
➢ Windows エクスプローラからファイルを細断処理するには、次の操作を実行します。

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指定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 シュレッダ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 シュレッダ] 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 シュレッダ] 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 はそこに何もないかのように動作し、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

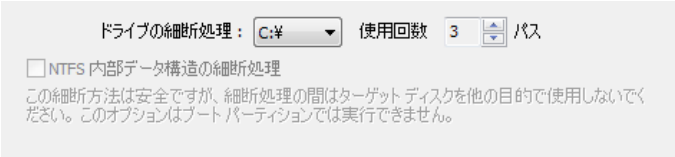
の「空き領域」を上書きするので、ディスク回復ソフトウェアを使用してもそれらのファイルを元に戻すことはできません。

➢ 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 電子メールを開きます。
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

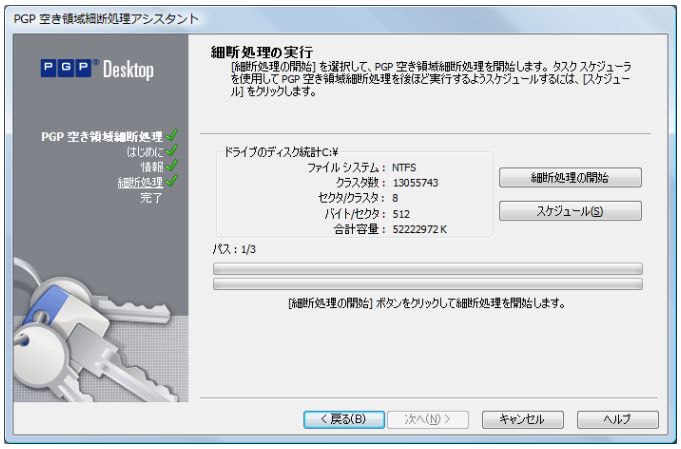


5. NTFS 内部データ構造を抹消するかどうかを選択 (すべてのシステムで使用可能ではありません) し、**[次へ]** を選択します。

   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* (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 電子メールのマニュアルは、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 電子メールには、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