



PGP ディスク全体暗号化

クイック スタート ガイド

バージョン 9.6

PGP ディスク全体暗号化について

PGP ディスク全体暗号化 (WDE) 製品は、デスクトップ、ラップトップ、およびリムーバブルドライブのデータを保護する複数の方法を提供するソフトウェア ツールです。

PGP WDE を使用して、次の操作を実行できます。

- システムの内容全体、または指定した外部および USB フラッシュ ドライブをロックします。
- 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します。
- 暗号化された安全なジップ アーカイブを作成します。
- PGP WDE または PGP Desktop がインストールされていない Windows システム上で開くことのできる、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入れることができます。
- ファイルおよびフォルダを完全に破棄するので、ファイル回復ソフトウェアを使用してもファイルは回復できません。
- ご使用のドライブの空きスペースを安全に消去するので、削除したデータが完全に回復不可能になります。

初めて PGP Desktop を使用する方へ

この詳細手順を示したガイドを使用して開始してください。PGP Desktop を使用すると、ご使用のデータの保護が鍵をかけるのと同じくらい簡単であることがわかります。

- この『クイック スタート ガイド』は、PGP WDE をインストールする際の手助けとなります。また、PGP WDE および PGP Desktop の一部として含まれている他のセキュリティ機能の使用を開始する際のガイドとしても使用できます。
- 『PGP Desktop ユーザー ガイド』には、PGP WDE に関するより詳細な情報が記載されています。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、および鍵ペアを交換してご使用のデータを暗号化し、データを他のユーザーと安全に共有する方法について学習します。



PGP WDE ライセンスは、PGP Desktop 機能の特定のセットへのアクセス権を提供します。PGP Desktop の他の特定の機能では、異なるライセンスが必要な場合があります。ライセンスの詳細については、『PGP Desktop ユーザー ガイド』を参照してください。

- PGP WDE の導入の管理およびポリシー強制情報については、『PGP Universal 管理者ガイド』を参照してください。

目次

■ PGP ディスク全体暗号化について	1
■ 初めて PGP Desktop を使用する方へ	1
■ システム要件	1
■ インストールする内容について	2
■ 基本事項について	2
■ PGP WDE のインストール	3
■ PGP WDE の起動	3
■ PGP WDE のメイン画面	4
■ PGP WDE のベスト プラクティス	5
■ PGP WDE を使用したドライブのディスク全体暗号化	7
■ PGP 仮想ディスク ボリュームの作成	8
■ PGP ジップ アーカイブの作成	9
■ ファイルの細断処理	12
■ 空き領域の細断処理	13
■ 詳細情報	14

アイコン表記



メモ



注意

システム要件

- Windows Vista、Windows XP (SP 1 または 2) または Windows 2000 (SP 4)
Windows 2000 および Windows 2003 Server ではサポートされません。
- 128 MB の RAM (256 MB を推奨)
- 64 MB のハード ドライブの空き容量

インストールする内容について

PGP Desktop は、ユーザーが購入した機能へのアクセス権を提供するためにライセンスを使用します。ユーザーのライセンスに基づいて、一部またはすべての PGP Desktop ファミリーのアプリケーションがアクティブになります。

このドキュメントには、ご使用のライセンスでアクティブ化された機能を表示するための説明が記載されています。



PGP ディスク全体暗号化 (WDE) は、PGP Desktop ファミリーのアプリケーションの 1 つです。PGP WDE を使用すると、システムの内容全体、または指定した外部および USB フラッシュ ドライブをロックすることができます。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 ドライブのディスク全体暗号化は、ご使用のコンピュータが失われたり盗まれたりしても問題ないことを意味します。攻撃者がデータにアクセスするには、パスフレーズを知る必要があります。

PGP WDE に含まれる PGP Desktop のその他のコンポーネントは、以下のとおりです。



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します。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。PGP 仮想ディスクは、ご使用の機密ファイルを保管する完全な場所を提供します。これは、それらを金庫に保管するのと同じです。金庫の扉を開ける (ボリュームをマウントする) と、保管されているファイルを変更したり、ファイルを取り出したり、ファイルをボリュームに移動することができます。それ以外の場合 (ボリュームのマウントが解除される)、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 — 暗号化し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します。PGP ジップ アーカイブを作成または開くためには、PGP WDE または PGP Desktop をインストールする必要があります。PGP ジップは、機密データを配布またはバックアップする際に、安全に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 WDE または PGP Desktop がインストールされていない Windows システム上で開くことのできる、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入れます。SDA は、PGP ソフトウェアをインストールしていないユーザーと安全にファイルを交換する完全なソリューションです。



PGP シュレッド — ファイルおよびフォルダを完全に破棄するので、ファイル回復用ソフトウェアを使用してもファイルは回復できません。Windows のごみ箱を使用してファイルを削除しても実際には削除されません。ファイルはドライブ上にあり、最終的に上書きされます。それまでは、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 シュレッドは、ファイルを複数回にわたって直ちに上書きします。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、この機能は、ご使用のドライブの空きスペースを完全に抹消するので、削除したデータが完全に回復不可能になります。

鍵管理 — PGP WDE は、ご使用の鍵ペアおよび他のユーザーの公開鍵の両方の PGP 鍵を管理します。あなたの秘密鍵を使用して、あなたの公開鍵を使用して暗号化されて送信されたメッセージを復号化し、あなたの PGP 仮想ディスク ボリュームを保護します。公開鍵を使用して、他のユーザーへのメッセージを暗号化したり、PGP 仮想ディスク ボリュームにユーザーを追加したりします。

基本事項について

インストール後に、PGP WDE に PGP 鍵ペアを作成するよう表示されます。鍵ペアは、秘密鍵と公開鍵の組み合わせです。

- 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。他のユーザーがあなたの秘密鍵とパスフレーズを入手した場合、他のユーザーがあなたのメッセージを読み、あなたになりますことができます。あなたの秘密鍵は受信する暗号化されたメッセージを復号化し、送信するメッセージに署名します。
- 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、あなたの秘密鍵が復号化でき、あなたの署名を検証できるメッセージのみを暗号化します。

あなたの鍵リングは、あなたの鍵ペアと、暗号化されたメッセージを送信する他のユーザーの公開鍵の両方を保持します。[PGP 鍵] コントロール ボックスをクリックし、鍵リングの鍵を表示します。

- 1 PGP 鍵ペアのアイコンには、秘密鍵と公開鍵を示す 2 つの鍵があります。たとえば、この図では、Alice Cameron は PGP 鍵ペアを保持しています。
- 2 他のユーザーの公開鍵のアイコンには、鍵が 1 つだけ表示されています。たとえば、この図では、Ming Pa の公開鍵が鍵リングに追加されています。

すべての鍵	
名前	
1	 Alice Cameron
	 Example Corp. ADK
	 Example Corp. Revoker
	 Jose Medina
	 Marcus Wagner
2	 Ming Pa
	 Vladimir Toskin
	 鈴木 一郎

PGP WDE のインストール

インストールプロセスではシステムの再起動が必要です。

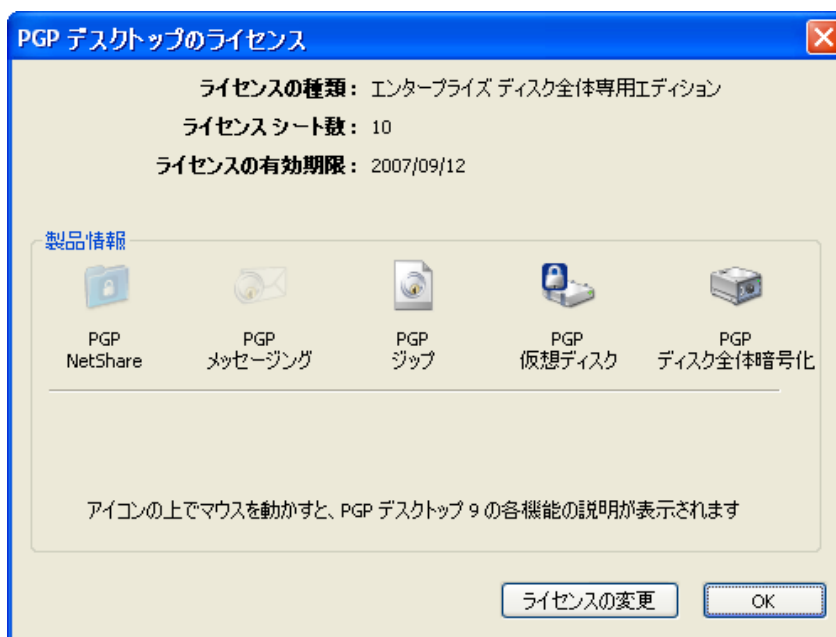
PGP Corporation は、インストールを開始する前に、起動中のアプリケーションを終了することを推奨します。



ご使用のライセンスによっては、PGP Desktop の特定のコンポーネントへのアクセス権がない場合があります。

PGP WDE をインストールするには、次の操作を実行します。

- 1 PGP WDE インストーラ プログラムを探します。
インストーラ 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 インストーラ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 システムを再起動した後は、画面上の指示に従って PGP WDE を設定してください。

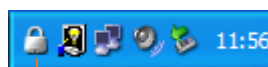


ご使用の PGP Desktop ライセンスがサポートする機能を表示するには、PGP WDE を起動し、[ヘルプ] メニューの [ライセンス] を選択します。緑のチェックマークが付いている機能が、アクティブなライセンスでサポートされています。この図では、PGP ディスク全体暗号化、PGP ジップ、および PGP 仮想ディスクがサポートされています。

PGP WDE の起動

PGP WDE を起動するには、以下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。

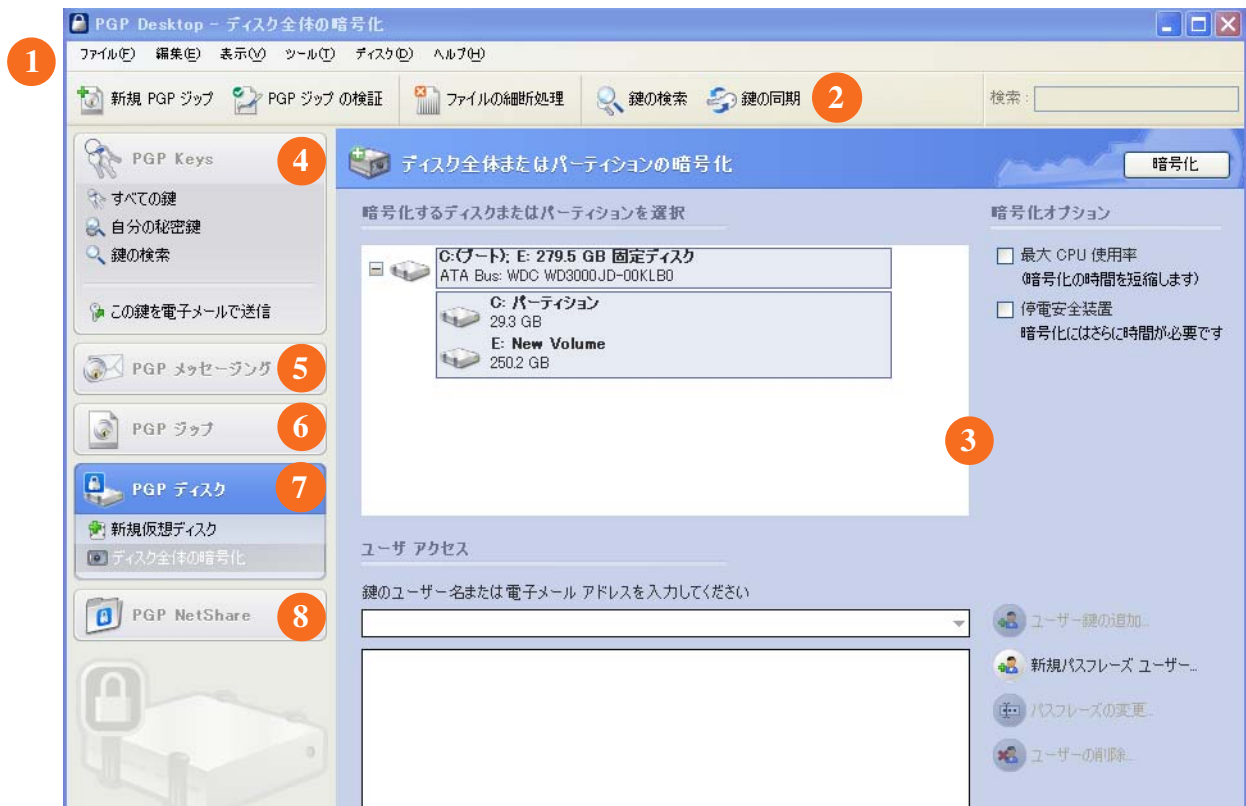


[PGP トレイ] アイコン

PGP WDE のメイン画面

PGP WDE の機能にアクセスする最も簡単な方法は、メイン画面を使用することです。

- 1 **PGP メニュー バー** — メニューとコマンドを使用して、すべての PGP WDE の機能にアクセスできます。
- 2 **PGP ツールバー** — 共通で実行されている複数の PGP WDE タスクにアクセスできます。
- 3 **作業領域** — 作業領域のアクティブな機能を設定します。
この図では、PGP WDE 作業領域を示します。



- 4 **[PGP 鍵]** コントロール ボックス — ご使用の PGP 鍵を管理します。
- 5 **[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します。
- 6 **[PGP ジップ]** コントロール ボックス — PGP ジップアーカイブを管理します。
- 7 **[PGP ディスク]** コントロール ボックス — PGP 仮想ディスク ボリュームおよび PGP ディスク全体暗号化ドライブを管理します。
- 8 **[PGP NetShare]** コントロール ボックス — PGP NetShare を管理します。

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 タイプの詳細については、『PGP Desktop ユーザー ガイド』の第 6 章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、ディスクを複合化できなかったりした場合にデータを失わないように、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](#)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 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](#)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）。**[6 ページの「暗号化中の電源の確保」](#)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 をテストして 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、[6 ページの「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」](#)を参照してください。
- 7 復号化されたディスクにおけるディスク リカバリの実行。**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 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、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。

リカバリ CD の作成

次の説明は、イラストレーションの目的で Roxio を使用した場合の手順です。実際の手順は異なる可能性があります。

- 1 PGP Desktop for Windows 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 を録音] を選択します。**
- 4 [ファイル タイプ] 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。**

- 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。

- 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 [録音の開始] 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。**



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 9.6 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 9.6 ディスクは作動不能になります。

PGP WDE のベスト プラクティス (続き)

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、[電源障害対応] オプションを選択してなければ、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 [電源障害対応] オプションの選択を検討してください。



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。[電源障害対応] 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 には互換性はありません。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以下のとおりです。

- **MBR モードの CompuTrace。** PGP ディスク全体暗号化と互換性があるのは、Absolute Software 社の CompuTrace ラップトップセキュリティおよびトラッキング製品の BIOS 設定のみです。MBR モードで CompuTrace を使用した場合は、互換性はありません。

- **Utimatec Safeguard Easy 3.x** には PGP ディスク全体暗号化機能との互換性はありません。PGP Desktop をインストールしたシステムにはインストールしないでください。また、Utimatec Safeguard Easy 3.x を搭載したシステムにも PGP Desktop をインストールしないでください。
- **GuardianEdge Technologies によるハードディスク暗号化製品：** 前 PC Guardian 製品として知られる Encryption Anywhere ハードディスクおよび Encryption Plus ハードディスク製品。

次のプログラムは PGP Desktop と同一システム上で共存しますが、PGP ディスク全体暗号化機能を妨害します。

- Safeboot Solo
- SecureStar SCPP
- Pointsec.

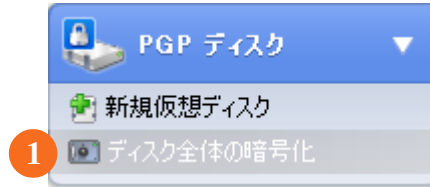
PGP WDE を使用したドライブのディスク全体暗号化

PGP WDE 機能は、システムの内容全体、または指定した外部および USB フラッシュ ドライブをロックします。



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 **【CPU 最大使用】**を選択して、直ちにご使用のディスクを保護します。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、**【電源障害対応】**を選択します。

【電源障害対応】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。

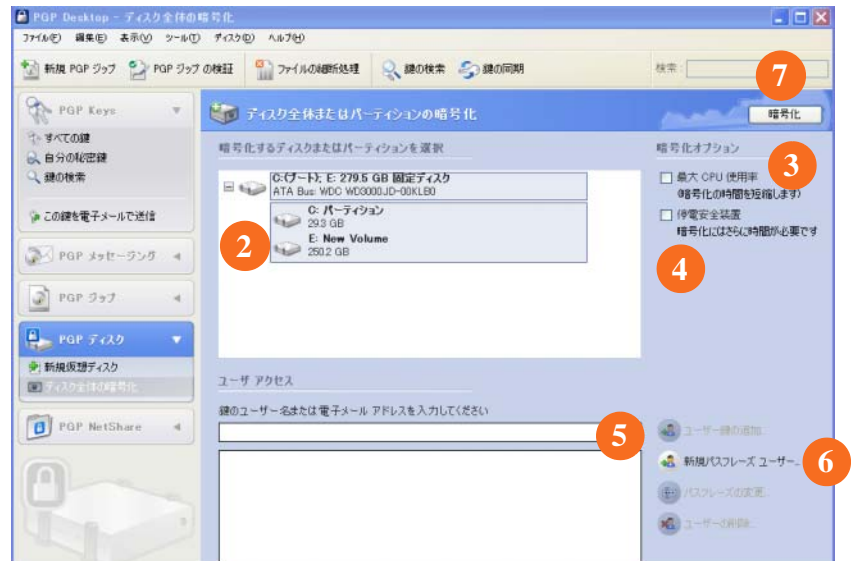
- 5 公開鍵暗号化方式を使用して、ディスク全体暗号化処理が行われたドライブに対して認証を行うことができるユーザーを追加するには、**【ユーザー鍵の追加】**をクリックします。

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、**【新規パスフレーズユーザー】**をクリックします。

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ことができます。

- 7 **【暗号化】**をクリックします。



PGP WDE で使用されてい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 形式でフォーマットされているドライブがサポートされています。容量に一切制限はありません。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) がサポートしているドライブは、PGP WDE で暗号化できるはずですが、

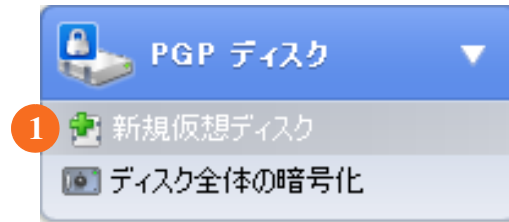


フロッピー ディスクまたは CD-RW のデータを暗号化する際は PGP 仮想ディスク ボリュームを使用します。PGP WDE は使用しないでください。
バックアップ ソフトウェアは、通常どおり PGP WDE と共に使用できます。ファイルはバックアップされる前に復号化されます。

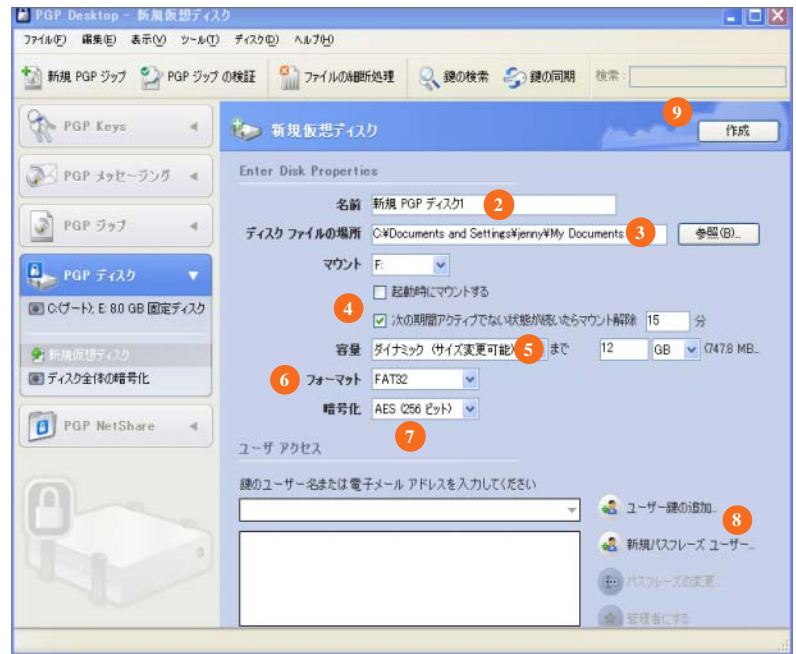
PGP 仮想ディスク ボリュームの作成

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します。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【マウントするドライブ文字】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 【容量】で、ファイルを追加するにつれてボリュームのサイズが増えるようにするには【ダイナミック（サイズ変更可能）】を選択し、ボリュームのサイズを常に一定にするには、【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の【形式】を指定します。
- 7 ボリュームの【暗号化】のアルゴリズムを指定します。
- 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 アーカイブには以下の 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 WDE または PGP Desktop for Windows 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 WDE または PGP Desktop for Windows 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 WDE または PGP Desktop for Windows を使用する必要がありません。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 WDE または PGP Desktop for Windows 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。

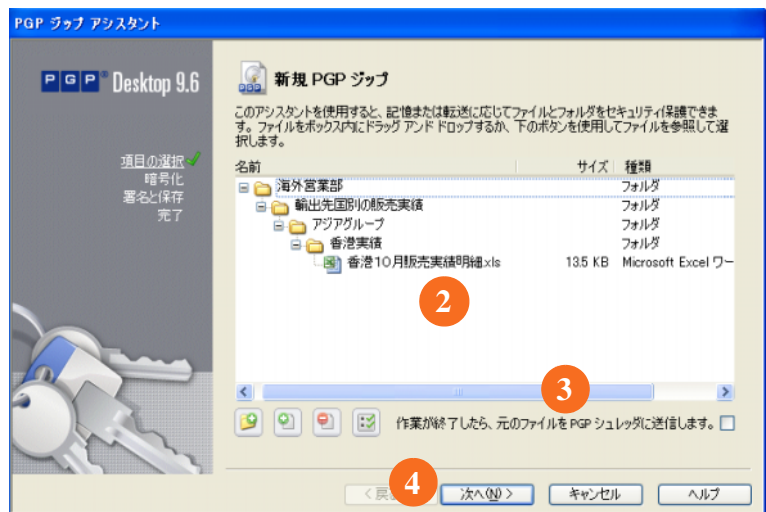
- 1 [PGP ジップ] コントロール ボックスで、[新規 PGP Zip] をクリックします。



- 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、アーカイブに含めた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dda に送信します] を選択します。

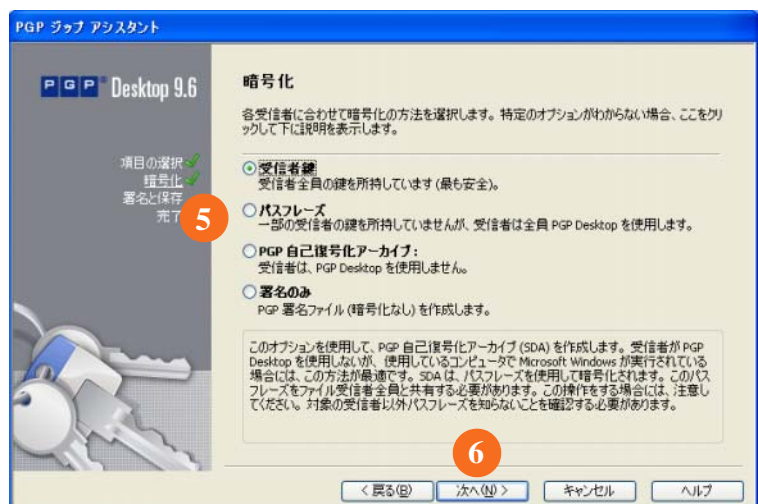
- 4 [次へ] をクリックします。



- 5 必要な種類の PGP ジップ アーカイブを選択します。

- 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 [OK] 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、以下のページの適切なセクションを参照してください。

PGP ジップ アーカイブの作成 (続き)

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、あなた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。

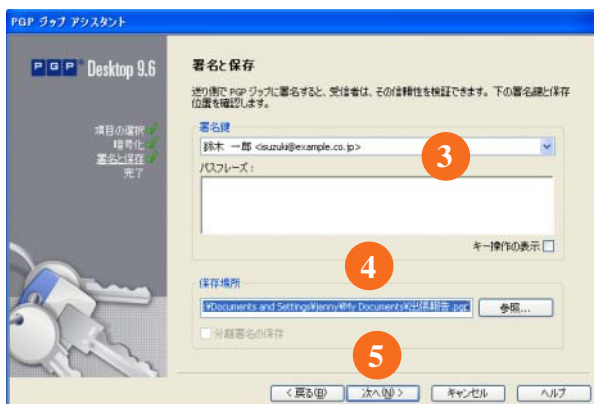
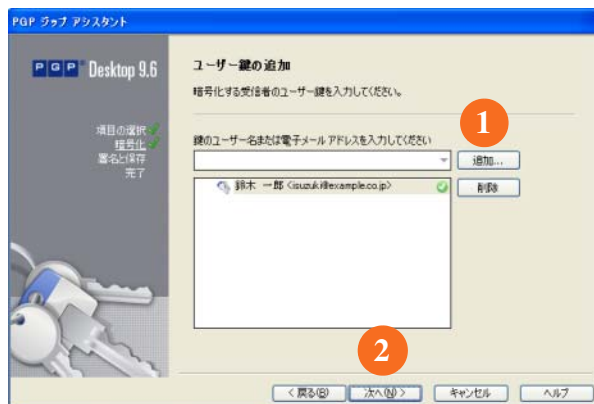
デフォルトの名前はアーカイブの最初のファイルまたはフォルダの名前であり、デフォルトの場所はアーカイブに含めるファイルやフォルダの場所です。

- 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】をクリックしてください。



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。



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 ジップ アーカイブの作成 (続き)

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。



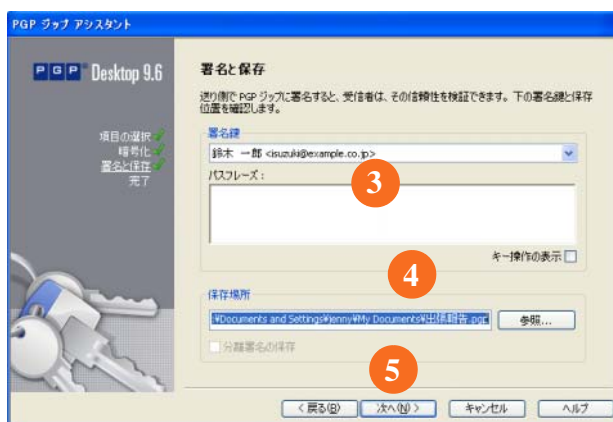
3 アーカイブに署名するために使用するローカルシステム上の秘密鍵を選択します。

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。

これで PGP SDA が作成されました。



6 【完了】をクリックしてください。



ファイルの細断処理

PGP シュレッタ機能は、ファイルおよびフォルダを完全に破棄するので、高度なファイル回復用ソフトウェアを使用してもファイルは回復できません。[PGP シュレッタ] アイコンおよび Windows のごみ箱の両方がデスクトップ上に表示されている場合でも、PGP シュレッタのみが直ちに指定したファイルを上書きするので、回復できません。

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、次の操作を実行します。

- 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 ツールバーの **【ファイルの細断処理】** をクリックします。

- 2 細断処理するファイルを指定します。

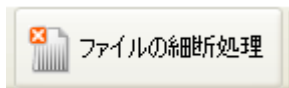
Ctrl キーを押しながらクリックして複数のファイルを選択することも、Ctrl キーを押しながら A キーを押すことすべてのファイルを指定することもできます。

- 3 **【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。

- 4 **【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] > [PGP 細断処理 <ファイル名>]** を選択します。

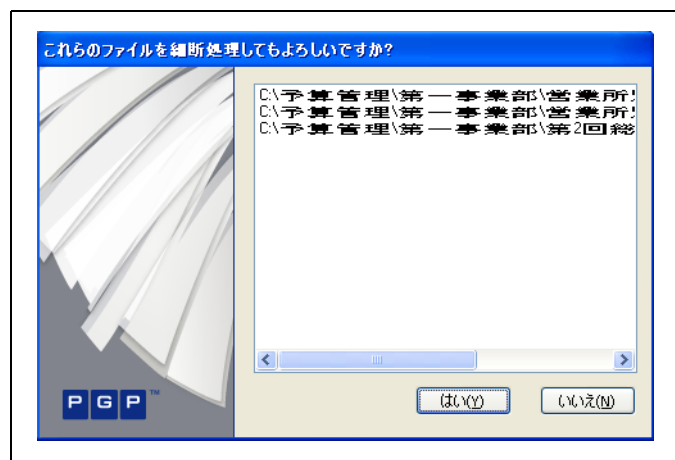
Ctrl キーを押しながらクリックして複数のファイルを選択することも、Ctrl キーを押しながら A キーを押すことすべてのファイルを指定することもできます。

複数のファイルを選択した場合は、テキストで **PGP が x 個** の項目を細断処理しましたと表示されます。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。



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。【オプション】パネルにアクセスして **【ディスク】** タブをクリックし、**【デスクトップ上に [PGP シュレッタ] アイコンを置きます】** オプションを選択解除し、**【OK】** をクリックします。



[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スペース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 【ツール】メニューから **PGP 空き領域細断処理** を選択します。
- 2 最初の画面で説明を読み、【次へ】をクリックします。
- 3 【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：49 パス

ドライブの細断処理：

NTFS

 使用回数

3

 パス

☐ NTFS 内部データ構造の細断処理
この細断方法は安全ですが、細断処理の間はターゲットディスクを他の目的で使えないでください。このオプションはブートパーティションでは実行できません。

- 4 **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。

- 5 【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。



【スケジュールを設定】をクリックして、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。



- 6 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。
- 7 【完了】画面で、【完了】をクリックします。

困ったときには

どの製品ドキュメントを使用できますか。

製品をインストールすると、以下のドキュメントがシステムにインストールされます。

- *PGP Desktop for Windows* ユーザー ガイド
- *PGP Desktop for Windows* リリース ノート

コンテキスト固有の情報については、製品のヘルプ メニューを使用できます。

テクニカル サポートへの問い合わせ方法について教えてください。

- PGP Corporation の製品サポートおよびカスタマー サービスについては、以下の PGP のサポート ポータルにアクセスしてください。

<https://www.pgp.com/support>

- PGP のサポートフォーラムにアクセスするには、以下を参照してください。
forums.pgpsupport.com

PGP Corporation に対して、その他のお問い合わせを行う場合は、以下の PGP Web サイトに移動してください。**www.pgp.com/company/contact.html**