



PGP Desktop について

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し、企業、ワークグループ、および個人が、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、機密情報を保護できるようにします。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します。

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 9.6** には、PGP Desktop Email および PGP ディスク全体暗号化が含まれています。
- **PGP Desktop Storage 9.6** 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 9.6** には、PGP Desktop Email、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 Email

PGP Desktop Email を使用すると、管理者によってユーザーのために定義されたポリシー、または PGP Universal 管理環境がない場合にユーザーが管理するポリシーに基づいて、電子メールを自動的かつ透過的に暗号化、署名、復号化、および検証できます。

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することができます。

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。

また、PGP Desktop では、次の操作を実行できます。

- 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。
- 保護されたジップ アーカイブを作成します。
- 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。

初めて PGP Desktop をご使用になる方へ

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 Desktop をインストールする際の手助けとなります。
- 『PGP Desktop ユーザー ガイド』には、PGP Desktop 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ご案内します。
- PGP Desktop 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 Desktop について	1
■ インストールされる内容について	2
■ 基本事項について	3
■ PGP Desktop のインストール	4
■ PGP Desktop の使用方法	4
■ PGP Desktop のメイン画面	5
■ PGP Desktop Email の使用	6
■ メッセージが暗号化されているかどうか	7
■ PGP NetShare の使用	8
■ PGP 仮想ディスク ボリュームの作成	9
■ PGP WDE のベスト プラクティス	10
■ PGP WDE を使用したドライブのディスク全体暗号化	12
■ PGP ジップ アーカイブの作成	13
■ ファイルの細断処理	16
■ 空き領域の細断処理	17
■ 詳細情報	18

アイコン表記



メモ



注意

- ファイルおよびフォルダを完全に破棄するので、いかなる方法で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。

システム要件

- Windows Vista、Windows XP (SP 1 または 2) Windows 2000 (SP 4)、および Windows 2003 Server (SP 1)
(PGP WDE は、Windows 2000 および Windows 2003 Server 上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

インストールされる内容について

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 Desktop Email は、PGP Desktop ファミリーのアプリケーションの 1 つです。PGP Desktop Email を使用して、自動的かつ透過的に、電子メール メッセージの暗号化、署名、復号化、および検証を行うことができます。PGP Desktop Email を使用して、AIM や iChat など、クライアントの IM セッションを暗号化することもできます。両方のユーザーで PGP Desktop Email を有効にする必要があります。



PGP NetShare は、PGP Desktop ファミリーのアプリケーションの 1 つです。PGP NetShare を使用すると、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。保護フォルダの暗号化されたファイルは、承認されたユーザーに対しては通常のアプリケーション ファイルとして引き続き表示されます。そのファイルへ物理的にアクセスできるそれ以外のユーザーは、ファイルを参照することはできますが、使用することはできません。



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、適切なパスキーが必要となります。

PGP Desktop Email 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 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 メッセージングまたは 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 シュレッダ — 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。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 シュレッダは、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 メッセージングは、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、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

PGP Desktop は、鍵を使用してメッセージの暗号化、署名、復号化、および検証を行います。

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、あなたになりす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。



PGP Desktop 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。

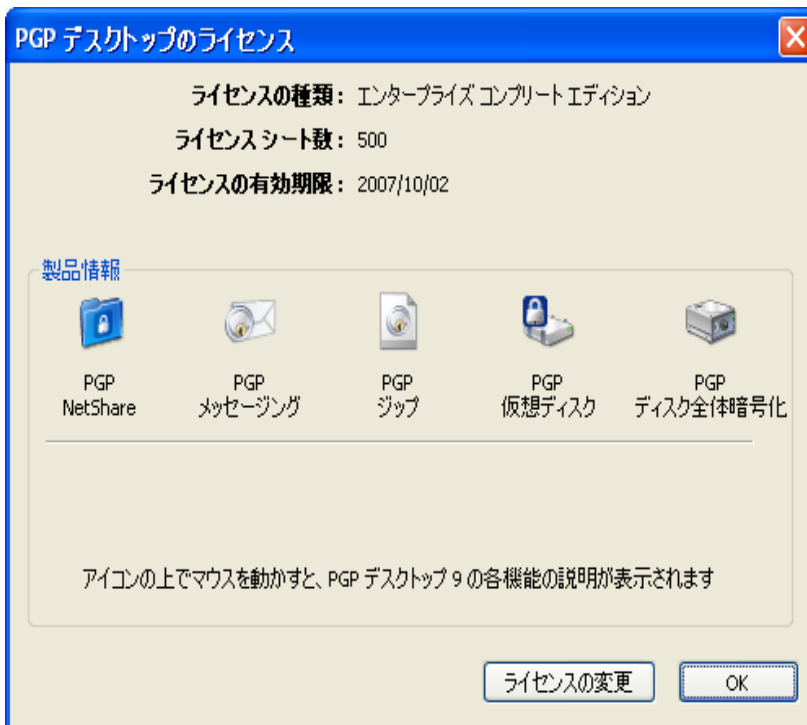
PGP Corporation は、インストールを開始する前に、すべての起動中のアプリケーションを終了することを推奨します。



PGP Universal により管理されている環境で PGP Desktop を使用するときは、ご使用の PGP Desktop インストーラが特定の機能や設定で設定される場合があります。

PGP Desktop をインストールするには、次の操作を実行します。

- 1 PGP メッセージング 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 Desktop を設定してください。



ご使用の PGP ライセンスがサポートす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。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 Desktop、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 Desktop の使用方法

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 トレイ] アイコン

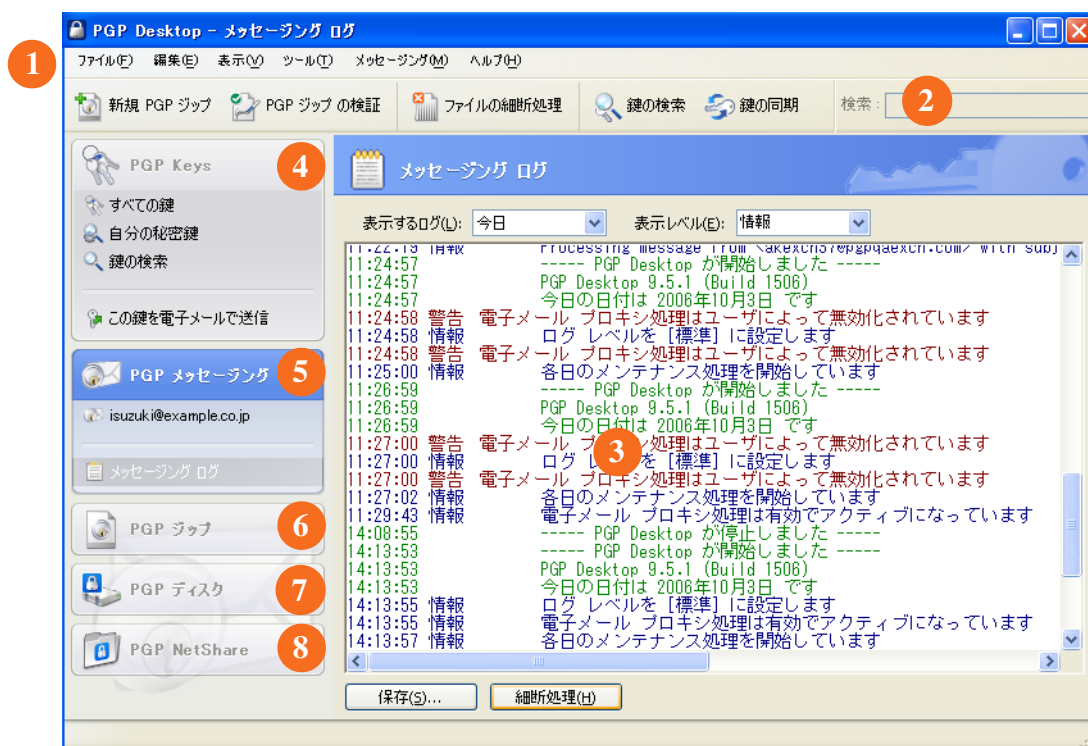
PGP Desktop のメイン画面

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



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。

- 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 Desktop 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 Desktop 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、メッセージング ログが選択された PGP Desktop Email 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 Desktop Email 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]** — PGP NetShare を管理します。

PGP Desktop Email の使用

PGP Desktop Email は、自動的かつ透過的に、送信するメッセージを暗号化して署名し、受信するメッセージを復号化して検証します。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す。PGP Desktop Email 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

インストール後は、PGP Desktop Email が自分自身をご使用の電子メール クライアントとメール サーバー間に挿入し、電子メール トラフィックを監視します。

受信メッセージが到着すると、PGP Desktop Email はメッセージが受信箱に入る前に傍受し、自動的に復号化して検証しようとします。その際には、あなたの秘密鍵を使用して復号化し、他のユーザーの公開鍵を使用して検証します。この作業が完了すると、PGP Desktop Email は、メッセージを受信箱に配信します。

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。

送信メッセージを送信すると、PGP Desktop Email は、ご使用のメール サーバーへ送信される途中でそれらを傍受し、設定されたポリシーに基づいて自動的に暗号化して署名しようとします。

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 Email が残りの処理を実行します。

PGP Desktop Email 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、以下のセクションを参照してください。

受信メッセージ

PGP Desktop Email は、以下のようにメッセージ内容によって受信メッセージを処理します。

- 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 Email 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。メッセージをそのまま読むことができるため、PGP メッセージング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は、PGP Desktop Email がメッセージを読めるように復号化を始めます。そのとき、最初にメッセージを復号化するためのあなたの秘密鍵を鍵リングで検索します。秘密鍵が見つかった場合、PGP Desktop Email はそれを使用してメッセージを復号化し、電子メール クライアントに送信します。秘密鍵が見つからなかった場合、PGP Desktop Email は暗号化されたままの状態メッセージを電子メール クライアントに送信します。たとえば、以下ようになります。

```
-----BEGIN PGP MESSAGE-----
Version: PGP Desktop 9.6
```

```
qANQR1DBwUwMvpgQkaZ1HwBD/0f5F8QktY+1NVzwQw4xQ/EPu0D0mLRMZVVNVQvN
rYVHPo5Acn6C3ZfP0996akjRi0oBGA62hklpkjq13QEGpBTqMP1F64TuxqHkPLNH
ISN+7ZEAT7EYtTv+3ErREOH6yQgJ+sqGm65jRjddYVVTG6hGa9F2wX+ZDLAIK6SrA
f4ZnQfNkvomMjX5785Z7LEGE5d5wM68kK8/Ff1vFYZ1w360ggauIXmom9F8294p
fNawAnhQ1R1f/1a/Muys0wKTLQpdpBxhQzqVkaE85gsCwqXfMAGDEYfrScAb1Ne
rPwJNTXsRyVpStmpNBZuVH01jkrXE4YEAPk48m0D1Y154N3XyVuvy790dxdD1Jh
o9yh9v5f071orPLFcw8wMLx4qad50vqdQRRfwbwBosd1jD2cm1jyOq+bcy
3hZknIEGbb7GtKaK01c1jy9U5aFdh491A9GLYHTWkLUHYV7j/wtBPFZPj6VvAcV
FQRDE08hyZKxc/foQw1Imdo+nymZEQ1tTTdBCAEXm5V+jBwfn0xhuk/Evy1KAhm
n27x2m9Pdwzxr1QjgrxI8Lda7DTJwYMA80120C1QZqrqVAmqIKL4CpcKyhPuRwIq
nan80KN/USfZK+v19juxM11550GYZ0DtL6KnLNGGPT1u6yLSU25B71tbve330ukj
ZMLXgdLAKQFSitPMVekqJpXQrMrL1EYr6He7fCAYmUMwX8w60e7H20wEIme2Y9V
eVoc55p9Iau7w987Ifbh1odeB+QEW3MavV5jBcae1ZhxAYLfrIdXBb1REeuQGjmj
FUCHf6GGT9h1Njw921R5q5intROH2KmwTAS0gBDNNEAAQ3p8Si+6129FLpLqF
Z7/wzmKfngv40gILxyPCRV5pBo30wAgJehhQDzC9kEkmd637t/cADEMUSnHC1
qTBASchRB+8eN5yrUrZ5YUghNvPr/vvN6odPEnX4mbrMSc1v4uxRySv50fGJT0U
=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 Email が署名の検証を始めます。そのとき、以下の場所を以下の順番で適切な公開鍵を検索します。デフォルトの鍵リング、keys.domain (domain はメッセージの送信者のドメイン) の鍵サーバー、PGP Global Directory (keyserver.pgp.com)、最後にその他の設定済み鍵サーバー。PGP Desktop Email が適切な公開鍵を見つけた場合は、署名の検証を始め、電子メール クライアントにメッセージを送ります。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を電子メール クライアントに送ります。
- 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、PGP Desktop Email が最初にメッセージを復号化するための秘密鍵を検索し、次にメッセージを検証するための公開鍵を検索します。

送信メッセージ

PGP Desktop Email はポリシー、つまりどのような状況でも処理を設定できる一連の指示に基づいて送信メッセージを処理します。

デフォルトのポリシー

PGP Desktop Email には、以下の 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 リストへのコマンド送信：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 リストへの登録：メーリング リストに登録する際、認証用に署名を行いますが、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：暗号化する送信相手の公開鍵が見つからないメッセージは、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、暗号化するための送信相手の鍵が見つからない場合でも、メッセージは送信されます (メッセージに機密とフラグを付けていない場合) ようになります (ただし、クリア テキストで送信されます)。

新しいポリシーの作成

PGP Desktop Email 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 Email は作業を自動的かつ透過的に行うため、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 Email 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。以下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関する情報がさらに必要な場合は、[詳細]をクリックします。以下の内容が表示されます。

- 5 PGP Desktop Email 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。



メッセージング ログ

PGP Desktop Email ログは、PGP Desktop Email がメッセージを保護するためのさまざまなアクションについて示します。

たとえば、上記の通知機能が表示されたメッセージは、メッセージング ログでこのエントリを生成したものです。以下の内容が表示されます。

- 7 送信メッセージが送信されたこと、送信者、およびその件名。
18:33:50 情報 Processing outgoing message from 鈴木 一郎 <isuzuki@example.co.jp> with subject: 今月の販売報告
- 8 暗号化された時間、暗号化された電子メールアドレス、および送信された電子メールアドレス。
18:33:57 情報 Encrypting PGP がパーティションされました message to fasano@example.co.jp with key(s):
18:33:57 情報 '鈴木 一郎 <isuzuki@example.co.jp>' (0xB79215FB)

PGP NetShare の使用

PGP NetShare 機能を使用すると、承認されたユーザーが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される必要のあ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の承認された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 [追加] をクリックします。

自分自身が保護フォルダ内のファイルにアクセスするのに承認される必要がある場合は、自分自身を追加してください。



PGP NetShare は、承認されたユーザーに保護されたファイルにアクセスできることを連絡しません。承認されたユーザーに連絡するのは、新規保護フォルダの作成者の責任です。

- 9 [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。



- 10 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。

- 11 [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。

- 12 [完了] をクリックしてください。

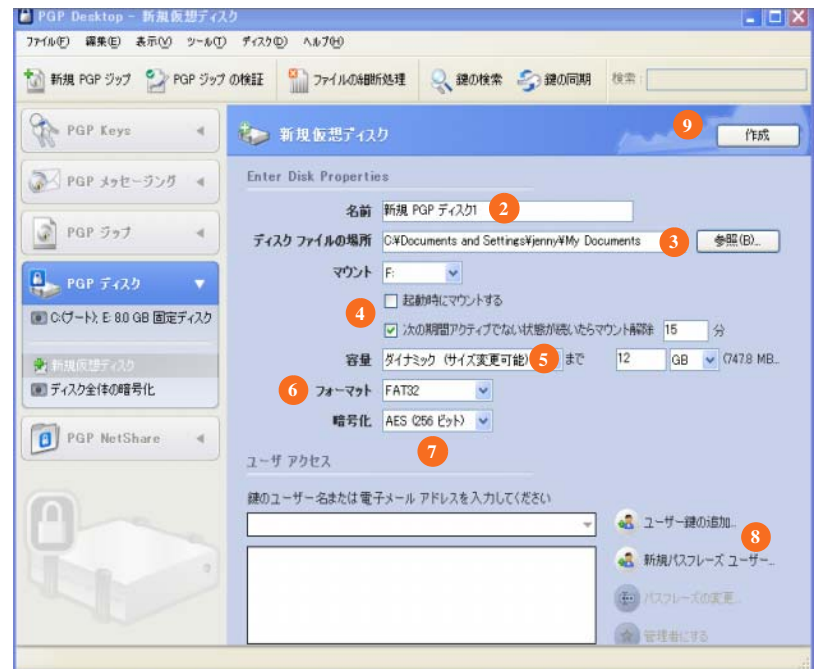
PGP 仮想ディスク ボリュームの作成

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 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、ディスクを復号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）。11 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、11 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。**

- 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 boot.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 [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。**



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、互換性がありません。

- **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

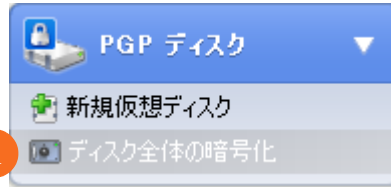
PGP WDE 機能は、システムの内容全体、または指定した外部および USB フラッシュ ドライブをロックします。



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。

1



- 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。

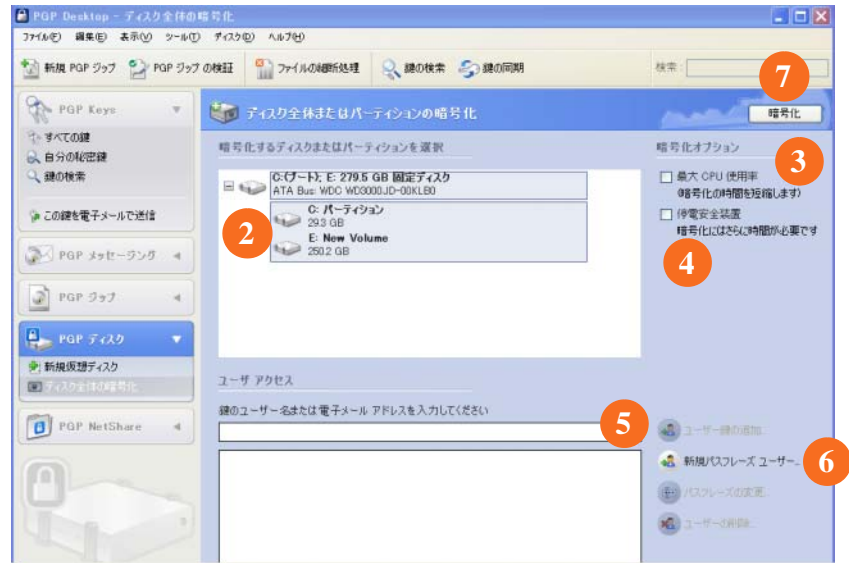
- 5 公開鍵暗号化方式を使用して、ディスク全体暗号化処理が行われたドライブに対して認証を行うことができるユーザーを追加するには、**【ユーザー鍵の追加】**をクリックします。

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。



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。PGP WDE は、デュアル ブート システムとの互換性がありません。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 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 メッセージングまたは 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 メッセージングまたは 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 メッセージングまたは 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 メッセージングまたは 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。

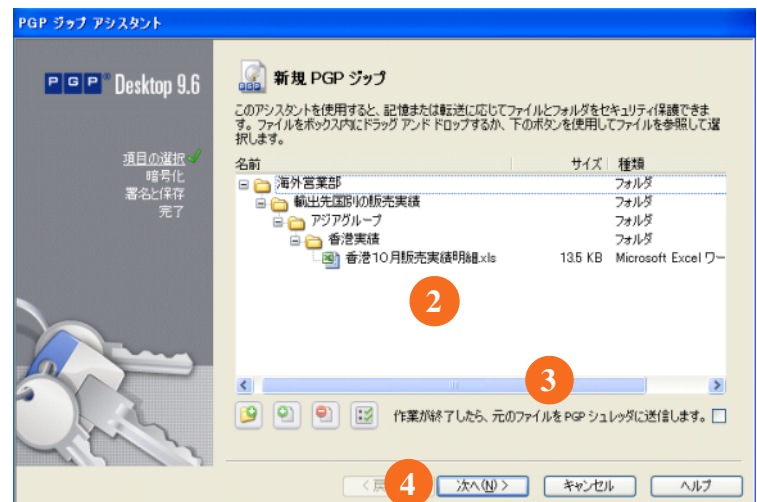
- 1 [PGP ジップ] コントロール ボックスで、[新規 PGP Zip] をクリックします。



- 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。

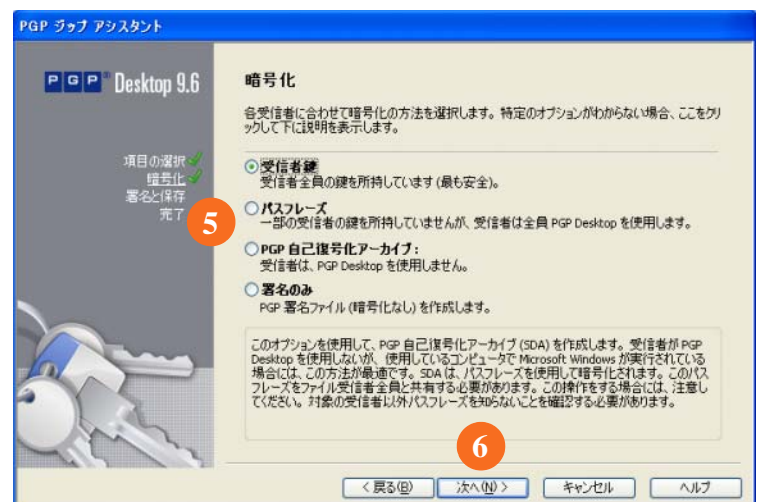
- 4 [次へ] をクリックします。



- 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。

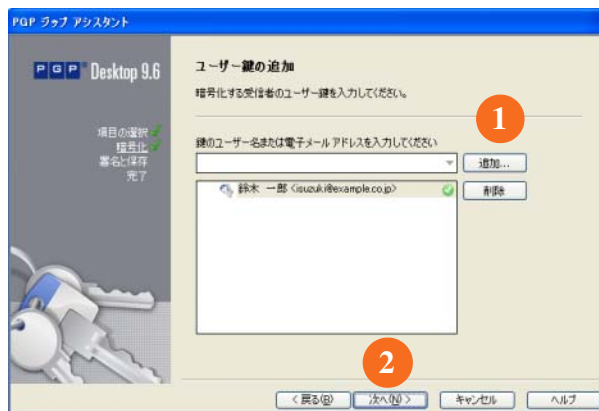
デフォルトの名前はアーカイブの最初のファイルまたはフォルダの名前であり、デフォルトの場所はアーカイブに含めるファイルやフォルダの場所です。

- 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。

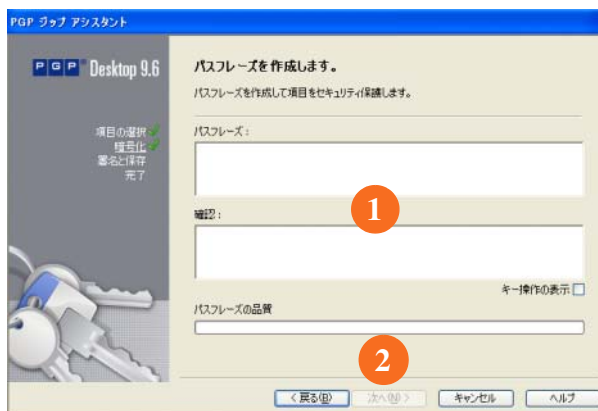
PGP ジップ アーカイブの作成 (続き)

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。



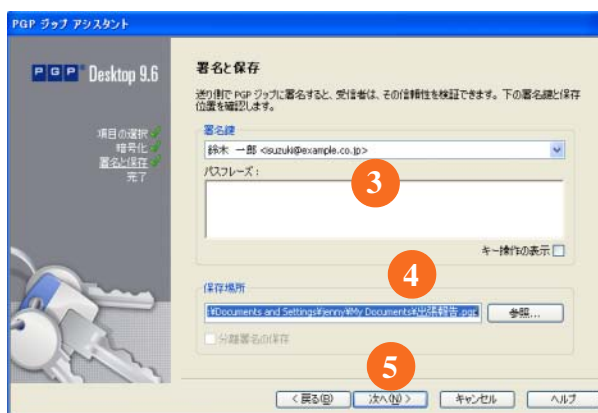
3 アーカイブに署名するために使用するローカルシステム上の秘密鍵を選択します。

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

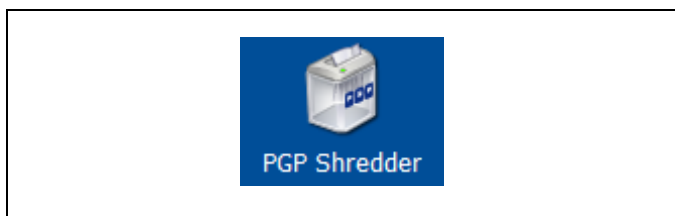
[PGP シュレッタ] アイコンを使用してファイルを細断処理するには、次の操作を実行します。

- 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 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。

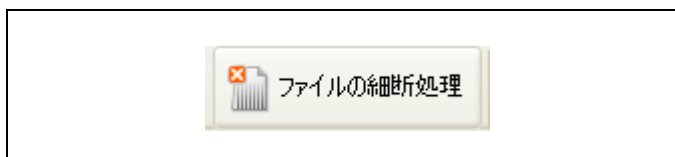
Ctrl キーを押しながらクリックして複数のファイルを選択することも、Ctrl キーを押しながら A キーを押すことですべてのファイルを指定することもできます。

- 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] > [PGP 細断処理 <ファイル名>]** を選択します。

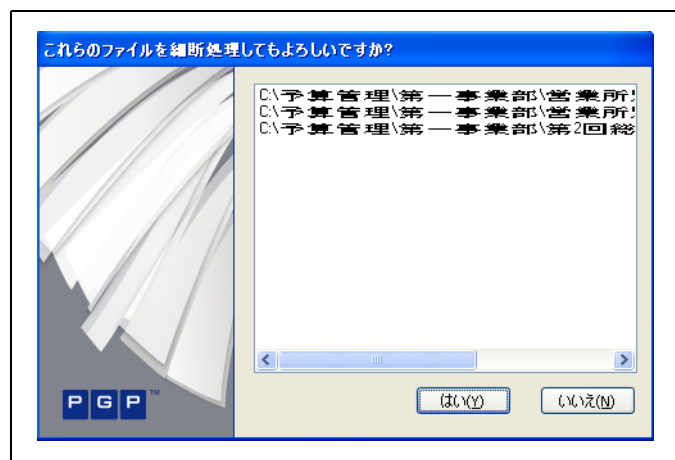
Ctrl キーを押しながらクリックして複数のファイルを選択することも、Ctrl キーを押しながら A キーを押すことですべてのファイルを指定することもできます。

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。

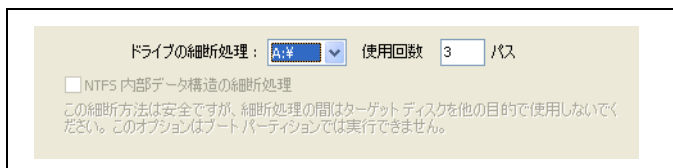
空き領域の細断処理

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



- 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**