Dekart Private Disk
テクニカルガイド

Rev. 2.3 更新 2008 年 3 月 28 日
株式会社ネクステッジテクノロジー
http://www.nextEDGEtech.com

nextEDGE TECHNOLOGY

はじめに

本ドキュメントは、仮想暗号化ディスク ソフトウェア Dekart Private Disk をより適切な環境で効果的にご利用して頂くために必要な技術情報、利用用途例について高度な技術者を対象に解説しています。製品に関する基本的な機能や操作方法に関しては、製品カタログやユーザガイドを参照してください。

目次

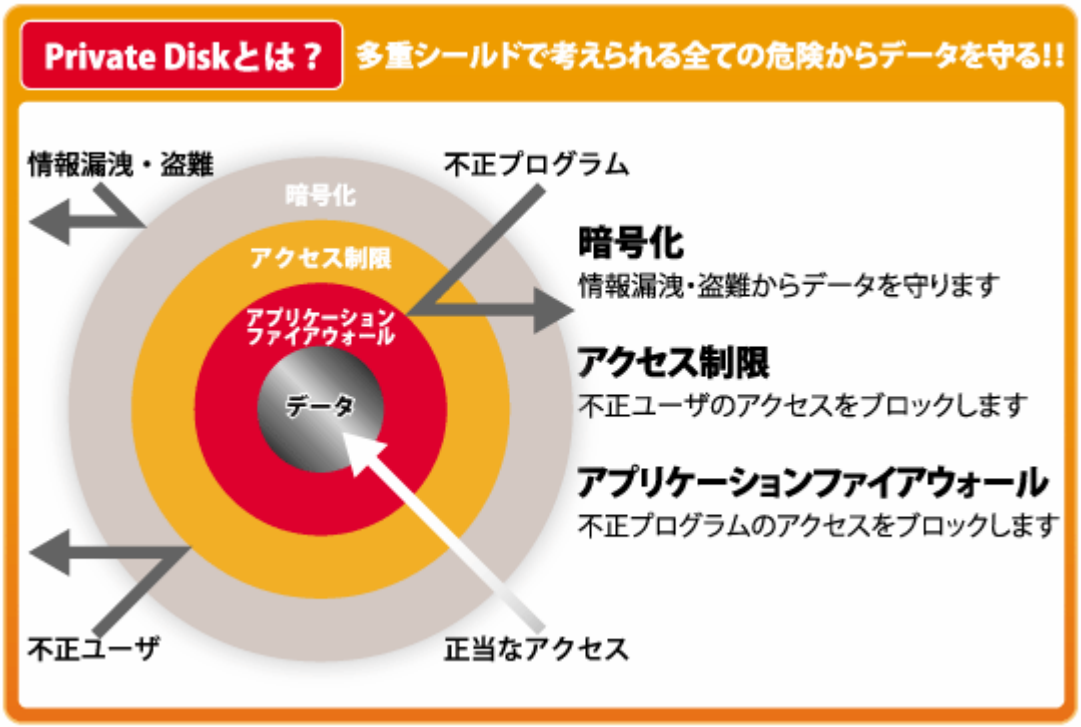
nextEDGE TECHNOLOGY

製品概要

Dekart社のPrivate Disk は、アクセス権を持たない人に盗み見られたり、改ざんされたりしないよう大切なデータを自動的に暗号化し、個人的な機密データやプログラムを常に安全な環境下で使用するための仮想ディスク暗号化ソフトウェアです。

米国標準技術局(NIST)による、米国政府の次世代標準暗号化方式 AES アルゴリズム（256 ビット キー長、CBCモード）を採用しているため信頼性が高く、プライベートな書類や画像、銀行口座情報、ビジネスプランなどを安全で強力に保護することが可能な Windows プログラムです。

また、仮想ディスクにより実装であるため、ご使用には セキュリティや暗号化に関する特別な知識は一切必要ありません。



nextEDGE TECHNOLOGY

運用例

以下では、Private Disk の運用例について、より具体的に紹介しています。

USBメモリで安全にデータを持ち運ぶ

＜目的＞

USB メモリに大切なデータをコピーして持ち運ぶ場合に最もリスクと考えられるのが、盗難や紛失によるデータ漏えいです。データ漏えいを回避するためにハードウェアにより暗号化/パスワード保護機能を実装した高価な USB メモリを利用するよりも、Private Disk を使って、一般的な USB メモリも利便性を損なうことなくデータ漏えいのリスクを回避することができます。

〈設定方法〉

Private DiskをインストールしたPCでPrivate Diskを起動し、システムトレイのアイコン　メニューから[リムーバブル　ディスクにインストール]を選択し、Private DiskをUSBメモリにインストールします。

仮想暗号化ディスクイメージをUSBメモリ内に作成します。この時、次のようなことを考慮するとより安全性が高まります。

- USBメモリ全体に大きな1つの仮想暗号化ディスクイメージを作成するんではなく、仕事、個人、機密情報など目的に応じて複数の仮想暗号化ディスクを作成する
- 必要に応じて、アプリケーションファイアウォールを設定し、仮想暗号化ディスクへのアクセスを制限する

著作権保護機能付きCD/DVD配布メディアの作成

＜目的＞

デザイン画像などCD/DVDで配布したいが、著作権を保護するために内部のデータを不正コピーをできないようにしたい。

〈設定方法〉

アプリケーション　ファイアウォールを利用することで実現可能です。
まず、データファイルを入れた暗号化イメージ(disk.pdd)を作成し、イメージ内に専用のビューアもコピーします。
以下のオプションをデータを含んだ仮想暗号化ディスクに設定します。

- アプリケーションファイアウォールを有効に設定する（ビューアに許可は必要ありません）
- 自動実行オプションを設定し、仮想暗号化イメージにコピーしたビューアを選択する

CD/DVDが挿入されたら自動的にマウントするためのautorun.infを作成します。

```
[Autorun]
Open=/Dekart/PrivateDisk/PrvDisk.exe /minimize /path:disk.dpd
```

注意: disk.dpdは、作成した仮想暗号化イメージのファイル名です。

作成した仮想暗号化イメージと、autorun.infをCD/DVDに書き込みます。

nextEDGE TECHNOLOGY

管理者権限のないPCでPrivate Diskを実行するには

USBメモリにPrivate Diskをインストールして、Private Diskのインストールされていない他のPCで管理者権限のないアカウントで利用するには、予めドライバのインストール/レジストリの設定をしておく必要があります。

以下の準備を行ってください。(共有ドライブ上にイメージとバッチファイルを設置して、ログインスクリプトなどで実行することができます。)

- *Private Disk* のイメージをターゲット PC にコピーします。コピーする内容は、Private Disk で[リムーバブルにインストール]オプションでインストールしたイメージをそのままコピーします。
- 下記の内容の.BAT ファイル(スクリプト)を作成します。 管理者権限で実行します。

  PrvDisk.exe /installdrivers

- コンピュータを再起動します。

補足: /installdrivers コマンドライン オプションを使って、ドライバのみを強制インストールすることができます。このコマンドは、既に以前のドライバがインストールされている環境に対して、ドライバを更新する場合にも利用することができます。 V2.10 Build 23以降のバージョンが必要です。

正しく動作していない場合は、以下のことを確認してください。

- *マイコンピュータ¥プロパティ¥ハードウェア タブ からデバイス マネージャを開きます。*
- メニュー[表示]->[隠れたデバイス]を表示 を有効にします。
- *[Non-PnP]デバイスを表示します。*
- *PDFILTER, PRVDISK および PDRJNDLを見つけ、ステータスが[Started]になっていることを確認します。*

nextEDGE TECHNOLOGY

使用上の注意と制限

仮想暗号化ディスクのバックアップおよびレストア機能について

バックアップ機能の対象データは指定した仮想暗号化ディスク内のデータであり、仮想暗号化ディスクのプロパティ情報（ex.読み取り専用、共有設定情報）は含まれません。そのためバックアップ　コピーからレストアした仮想暗号化イメージのプロパティ情報はレストア後、目的に応じて適切に再設定する必要があります。なお、仮想暗号化ディスクのプロパティ情報は、”ディスクの暗号化キーの[コピー]”にてバックアップ可能です。

バックアップ手順

① 読み取り専用ディスクとなっている仮想暗号化ディスクのバックアップは行なえませんので、必要に応じ、ディスクタブ上 [プロパティ]ボタンから、バックアップしたい仮想暗号化ディスクのプロパティを表示し、[読み取り専用ディスク]のチェックを外してください。

② リカバリタブ上[バックアップ]ボタンをクリックし、バックアップしたい仮想暗号化ディスクを選択します。

③ バックアップしたい仮想暗号化ディスクに設定してあるアクセス用のパスワードを入力し、[OK]ボタンをクリックします。

④ バックアップファイルの保存先、およびファイル名を指定し、[保存]ボタンをクリックします。
（拡張子も任意ですが、バックアップファイルと分かるようなもの（例: *.bak）の付加を推奨）

⑤ バックアップファイルを利用する際に必要となるパスワードを指定し、[OK]ボタンをクリックします。

⑥ エラーをチェックするかの質問に回答した後、バックアップ作業が開始されます。
（Windows Vistaの場合、[いいえ]ボタンを選択してください。）

⑦ 「処理が正常に完了しました。」のメッセージに対し、[OK]ボタンをクリックした後、指定した保存先にバックアップファイルが作成されていることを確認します。

レストア手順

① 読み取り専用ディスクとなっている仮想暗号化ディスクに対してレストアは行なえませんので、必要に応じ、ディスクタブ上 [プロパティ]ボタンから、レストア先の仮想暗号化ディスクのプロパティを表示し、[読み取り専用ディスク]のチェックを外してください。

② リカバリタブ上[レストア]ボタン（バックアップボタンの下）をクリックし、レストア先の仮想暗号化ディスクを選択します。

③ 指定した仮想暗号化ディスクにアクセスする為のパスワードを入力し、[OK]ボタンをクリックします。

④ 復元するバックアップファイルを指定すると、レストア先として指定した仮想暗号化ディスク内の内容が削除される旨のメッセージが表示されますので、[はい]ボタンをクリックします。

⑤ 復号化パスワード（バックアップファイル作成時に指定したパスワード）を入力し[OK]ボタンをクリックしま

nextEDGE TECHNOLOGY

す。（バックアップ元の仮想暗号化ディスクへレストアする場合、復号化パスワードの確認は省略されます。）

暗号化キーのコピー及びレストア機能について

暗号化キーのコピー機能は、仮想暗号化ディスクへアクセスする為の認証用のパスワード及びプロパティ情報をバックアップする為の機能で、ユーザは、万が一認証用のパスワードを忘れてしまっても、バックアップした暗号化キーを仮想暗号化ファイルにレストアし新たなパスワードを設定することで、データの参照およびプロパティ情報の復旧が行なえます。
なお、この機能はバックアップ元ディスクの救済を目的としており、バックアップした暗号化キーを異なる仮想暗号化ディスクへレストアした場合、セキュリティの観点からレストア先として指定した仮想暗号化ディスクは初期化（フォーマットが要求されます。）されますのでご注意ください。

暗号化キーのコピー（バックアップ）手順

① リカバリタブ上[コピー]ボタンをクリックし、暗号化キーをコピーしたい仮想暗号化ディスクを選択します。

② 暗号化キーをコピーしたい仮想暗号化ディスクに設定してあるアクセス用のパスワードを入力し、[OK]ボタンをクリックします。

③ 暗号化キーファイルの保存先、およびファイル名を指定し、[保存]ボタンをクリックします。
（拡張子も任意ですが、バックアップファイルと分かるようなもの（例: *.vdk）の付加を推奨）

④ 暗号化キーファイルを利用する際に必要となる復号化キーを指定し、[OK]ボタンをクリックします。

⑤ 「処理が正常に完了しました。」のメッセージに対し、[OK]ボタンをクリックした後、指定した保存先に暗号化キーファイルが作成されていることを確認します。

レストア手順

① リカバリタブ上[レストア]ボタン（コピーボタンの下）をクリックし、レストア先の仮想暗号化ディスクを選択します。

② 指定した仮想暗号化ディスクにアクセスする為のパスワードを入力し、[OK]ボタンをクリックします。

③ レストアする暗号化キーを指定すると、レストア先として指定した仮想暗号化ディスク用の新しい認証用パスワードを確認されます。

④ 新しい認証用パスワードを入力した後、[OK]ボタンをクリックします。

⑤ 「処理が正常に完了しました。」のメッセージに対し、[OK]ボタンをクリックした後、新しく指定した認証用パスワードで仮想暗号化ディスクへアクセスできるか確認します。

nextEDGE TECHNOLOGY

アプリケーション ファイアウォールについて

アプリケーション ファイアウォールを利用する際に下記の点に注意してください。

- アプリケーション ファイアウォール機能を利用する仮想暗号化ドライブに対し、共有設定は行わないでください。
- アプリケーション ファイアウォールは日本語文字（2バイト文字）に対応していません。
- 仮想暗号化ディスク内のプログラムは、デフォルトでホワトリスト(アクセス許可済み)になっています。許可リストに登録する必要はありません。

「指定の期間アイドル時、すべてのディスクのマウントを解除する」オプション

「マウント解除前に開いているファイルをチェックする」と「指定の期間アイドル時、すべてのディスクのマウントを解除する」を併用した場合、開いているファイルが存在する仮想暗号化ドライブは、安全性を考慮し、指定した時間が経過してもアンマウントされません。全てのドライブをアンマウントしたい場合には、「マウント解除前に開いているファイルをチェックする」を無効化してください。

「Private Disk をシステム サービスとして有効にする」オプション

「Private Disk をシステム サービス」として有効にする」は、ログオフしてもマウント状態を継続する為に用意されているオプションですので、サービスへの登録内容などを変更しないでください。また、リムーバブルディスクから起動しているPrivate Diskでは、このオプションを利用しないでください。

その他

- Private Diskの2重起動は行なわないでください。
- Private Diskは、ライセンス確認の為にネットワークを利用する場合がありますが、コンピュータ内の情報収集等は一切行ないません。
- Windows Server OSでの利用には、Server向けライセンスが必要となります。

Windows 2000 での分かっている問題

- Windows 2000 SP4環境にて、Private Disk の起動時にエラーが発生する場合には、Windows 2000 Service Pack 4 (SP4) 用更新プログラムのロールアップ 1（KB891861）を適用してください。

Windows Vista での注意点

- 初めてPrivate Diskを起動させる場合、Private Disk を右クリック→「管理者として実行」を選択し、起動してください。
- スタートメニューに登録されている「アンインストール」から、Private Diskをアンインストールする場合、プログラムを終了した状態で「アンインストール」を右クリック→「管理者として実行」を選択してください。
- 仮想暗号化ディスク内のバックアップを行なう際、エラーチェックを行なうとバックアップに失敗しますので、エラーチェックは行なわないでください。（エラーチェックは、仮想暗号化ディスクをマウントし、マイコンピュータにリストされているドライブを右クリック→プロパティ→ツールタブから行なえます。）
- 暗号化キーのリストアを行なう場合、事前にエクスプローラから復元先仮想暗号化ディスクファイル（*.dpd）のプロパティを表示し、読み取り専用の属性を外してください。
- 「エラーおよび処理のログを記録する」オプションを正常に利用する為には、管理者権限にてPrivate Disk

nextEDGE TECHNOLOGY

を起動する、若しくはUAC機能を無効化する必要があります。

- 「マウント解除前に開いているファイルをチェックする」と「休止状態にする前にすべてのディスクのマウントを解除する」を併用した場合、開いているファイルが存在する仮想暗号化ドライブは、休止状態になる際アンマウントされませんので、全てのドライブをアンマウントしたい場合には、「マウント解除前に開いているファイルをチェックする」を無効化してください。
- 「Private Disk をシステム サービス」として有効にする」は利用できません。

nextEDGE TECHNOLOGY