



ProtectDrive Version 8.5.0

ユーザ・マニュアル

© 2008 SafeNet, Inc. All rights reserved.

文書番号 007053-001（改訂版 E、2008 年 12 月）

ソフトウェア・バージョン 8.5

すべての知的財産は著作権により保護されています。本書で使用または参照する商標および製品名は、すべて個々の所有者の著作権に属します。SafeNet の事前の書面による許可なく、本書の一部または全部を複製、検索可能なシステムに保存、または電子的、機械的、化学的、複写、記録、またはその他の方法により転記することは、一切禁じられています。

SafeNet は、本書の内容に関する事実表明および保証、特に商品適合性および特定目的における適格性についての黙示的な保証は一切行わないものとします。さらに SafeNet は、本書を改訂する権利を有し、適宜本書の内容を変更します。かかる改訂および変更について、SafeNet から事前に個人や組織に対して通知する義務はないものとします。

SafeNet は、本書の内容に関する建設的なご意見を歓迎します。ご意見については、お客様の氏名または会社名などの詳細情報を添えて、下記までお寄せください。

日本オフィス：
神奈川県横浜市西区みなとみらい 2-3-5 クイーンズタワーC 16F
日本セーフネット株式会社
電話：045-640-5733

SafeNet, Inc.
4690 Millennium Drive
Belcamp, Maryland 21017
USA

技術サポート

本製品のインストール、登録、および操作に関して問題が発生した場合は、マニュアルを読んでご確認ください。それでも問題が解決しない場合は、サプライヤまたは SafeNet サポートへお問い合わせください。

確認事項

ProtectDrive には、Apache Software Foundation (<http://www.apache.org/>) が開発したソフトウェアが含まれています。

目次

第 1 章 はじめに.....	1
製品概要.....	1
本書の対象読者.....	2
第 2 章 ProtectDrive で保護された PC へのログオン.....	3
スマートカード、トークンおよび PIN によるログオン.....	5
ユーザ名、パスワードおよびドメイン名によるログオン.....	5
プリブート・ログオンに失敗した場合の対処方法.....	6
プリブート・ユーザ名またはパスワードを間違えた場合.....	6
システムの停止によるプリブート・ログオンの失敗.....	6
第 3 章 Windows へのログオン.....	7
手動での Windows へのログオン.....	7
スマートカード、トークンおよび PIN による Windows へのログオン.....	8
ユーザ名、パスワードおよびドメイン名による Windows へのログオン.....	8
第 4 章 ProtectDrive での Windows の使用.....	11
ProtectDrive ユーザ認証の動作の追跡.....	11
ディスク暗号化に関する警告.....	12
SafeNet ProtectDrive システム・トレイ・アイコン.....	12
ローカル管理コンソールへのアクセス.....	13
Windows デスクトップのロック.....	13
共通鍵の登録.....	14
SafeNet ProtectDrive に関する情報の表示.....	17
ProtectDrive で保護された PC での Windows フォルダ圧縮アプリケーションの使用.....	17
ProtectDrive で保護された PC での Windows システム復元ユーティリティの使用.....	17
ProtectDrive プリブート・パスワードの変更.....	18
デバイスへのアクセス拒否エラー.....	19
第 5 章 ハード・ドライブおよびリムーバブル・メディアの暗号化.....	20
ハード・ドライブの暗号化.....	20
ドライブの復号.....	22
異なるアルゴリズムを使用したドライブの再暗号化.....	23
リムーバブル・メディア.....	23
リムーバブル・メディアの暗号化.....	23
暗号化プロンプトの自動表示.....	24
Windows エクスプローラによるメディアの暗号化オプション.....	25
リムーバブル・メディアのロック.....	26
リムーバブル・メディアのロック解除.....	26
リムーバブル・メディアの復号.....	27
リムーバブル・メディアの復旧.....	28
標準的なリカバリ手順.....	28
バックアップ・リカバリ手順（オプション）.....	29
リムーバブル・メディアの緊急アクセス.....	29

第 6 章 ProtectDrive ユーザの設定	34
ユーザに対するデバイスへのアクセス制御権の設定	34
ProtectDrive ユーザの追加	35
ProtectDrive ユーザのパスワード変更	35
ProtectDrive ユーザの削除	35
第 7 章 トラブルシューティング	37
スマートカードおよびトークンの配置を間違えた場合、または PIN を忘れた場合の対処方法	37
パスワードを忘れた場合の対処方法	38
ブリーブ・ユーザ・アカウントを持っていない場合の対処方法	39
ユーザ名なしでの緊急ログオン手順	39

第1章 はじめに

製品概要

今日のコンピューティング環境において、ハードディスク・ドライブ（HDD）は機密情報の大規模な保存場所となっています。一般的に使用されている Windows オペレーティング・システムでも、スタンドアロン・マシンであれネットワーク接続されたコンピュータであれ、（大部分の運用環境で）十分なデータのプライバシーを確立できます。ただし、悪意によるシステム（または HDD）の損失となると、データのセキュリティ保護は不十分です。適切なデータ保護手段を講じないと、HDD をシステムから取り外してデータを読み取ることは容易です。

ProtectDrive が提供する PC のセキュリティ機能の 1 つに、システムへのログオンに対するユーザ認証があります。この認証は、以下のとおり、2 段階の連続的なプロセスからなります。

プリブート認証

コンピュータを起動して Windows が起動されるまでの間に、ユーザは有効なログオン認証証明情報を提示する必要があります。ログオン方法については、次のページで説明します。

Windows 認証

これは、ProtectDrive のインストール前に、ユーザに対する既存の Windows 認証方式に基づいて、実際に Windows のログオンを行うものです。

一般的に、ProtectDrive の設定はシステム管理者が行い、自動的に Windows のログオンを実行するため、ユーザ入力是不要です。

ただし、ユーザが ProtectDrive へのログオン（プリブート）とは別に Windows へログオンしなければならない場合もあります。

上の 2 つのユーザ認証方式は、通常システム管理者が設定するユーザの既存の Windows ログオン認証証明情報に依存します。ログオン方式は以下の 2 種類です。

スマートカード、トークン および PIN

この方式の場合、ユーザがスマートカードをリーダーへ挿入し、PIN を入力します。または、ユーザがトークンを USB ポートへ差し込んでから PIN を入力します。

ユーザ名、パスワードおよびドメイン名

この方式の場合、ユーザは Windows のユーザ名、パスワード、およびドメイン名を入力します。

ユーザは ProtectDrive のシステム管理者へ問い合わせ、自分のシステムへログオンする方法について詳細な指示を確認する必要があります。

サポートされるトークンおよびスマートカードのリストについては、SafeNet Web サイトの [サポート] セクションにある最新の ProtectDrive リリース・ノートを参照してください。

本書の対象読者

本書は、ワード・プロセッサ、電子メール、インターネット・アクセスなど、日常的に PC システムを利用するコンピュータのエンド・ユーザを対象としています。

本書は、お使いのコンピュータが IT の専門家（通常システム管理者）により管理されていることを前提としています。その人物は、一般的に ProtectDrive などのさまざまなコンピュータ・システム・コンポーネントの設定および保守を担当する人物を指しています。

本書は、ProtectDrive がインストール済みで使用準備が整っていることを前提としています。本書は、エンド・ユーザの視点から ProtectDrive の基本的な操作方法を説明するものです。また、以下のような ProtectDrive の操作に関する問題を取り扱っています。

- ProtectDrive で保護された PC の電源をオンにする方法およびログオンの方法
- ProtectDrive で保護された PC で Windows へログオンする方法
- スマートカードおよびトークンを無くした場合、または PIN を忘れた場合の対処方法
- パスワードを忘れた場合の対処方法
- ログオンに失敗した場合の対処方法
- ProtectDrive で Windows を使用する方法
- ハード・ドライブの暗号化を実行する方法
- リムーバブル・メディアの暗号化を実行する方法

本書の内容を理解するには、最低限の技術的な知識が必要となります。ProtectDrive のインストール、データの暗号化、システムおよびユーザの管理、障害復旧などの問題については、システム管理者へお問い合わせいただくか、または最新版の『Protect Drive 管理ガイド』を参照してください。

第2章

ProtectDrive で保護された PC へのログオン

ProtectDrive で保護された PC の電源をオンにすると、通常はその PC を起動できます。次に、ユーザのコンピュータに図 1 から図 4 のような [プリブート・ログオン] 画面が表示されます。

- F1 キーを押すことによって [ヘルプ] を表示できます。
- F2 キーを押して、“スマートカード/トークン/PIN” か、“ユーザ名/パスワード/ドメイン” の 2 つのログオン画面を切り替えることができます。



図 1 - 32bit プリブート・ログオン画面（スマートカード/トークン/PIN）

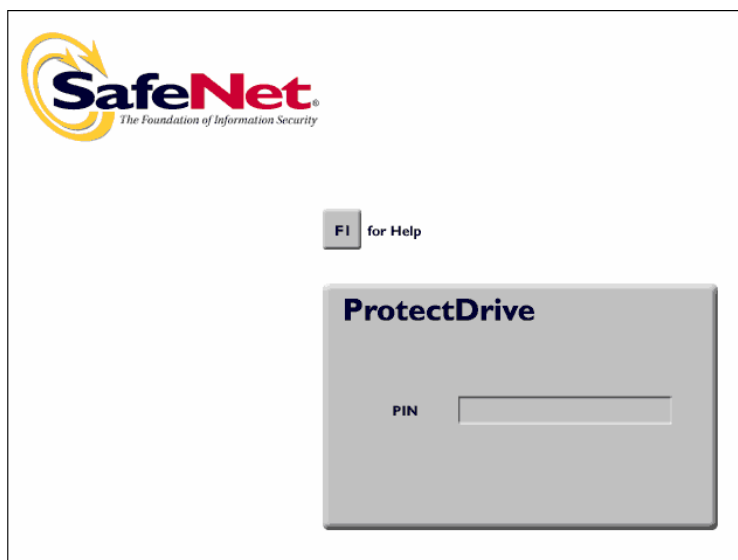


図 2 - 16bit プリブート・ログオン画面（スマートカード/トークン/PIN）



図 3 - 32bit プリブート・ログオン画面（ユーザ名/パスワード/ドメイン）



図 4 - 16bit プリブート・ログオン画面（ユーザ名/パスワード/ドメイン）

注意： 32bit プレブート認証は、ハイレゾ表示のマシンのみで表示されます。ハイレゾ表示できないマシンの場合には、16bit プレブート認証画面が表示されます。

注意： システム管理者がスマートカード、トークンおよび PIN のアクセスとユーザ名、パスワードおよびドメイン名のアクセスを両方許可するようシステムを設定している場合は、F2 キーを押してこれら 2 つのログオン画面を切り替えてください。

注意： 32bit プレブートで、10 分以上ログインせずに放置すると自動的にブランク画面でのスクリーンセーバが起動します。

スマートカード、トークンおよび PIN によるログオン

スマートカード、トークンおよび PIN のユーザは、前ページの図 1 に示すようなプリブート認証画面を使用してください。この画面は、システムの電源をオンにした直後に表示されます。

ログオンするには、次の手順を実行します。

1. スマートカードまたはトークンをリーダーへ挿入してください。
2. PIN を入力してください。
3. Enter キーを入力してください。

これで、Windows が起動されます。共通鍵トークンを使用してログオンしない場合、一般的な ProtectDrive の導入事例では、ユーザは自動的に Windows へログオンします。ただし、ユーザが手動で Windows へログオンしなければならないよう、システム管理者が ProtectDrive を設定する場合があります。

共通鍵トークンを使用してログオンする場合は、必ず Windows にログオンする必要があります。[第 3 章](#) (Windows へのログオン) を参照してください。

ユーザ名、パスワードおよびドメイン名によるログオン

ユーザ名/パスワード/ドメイン名のユーザは、前ページの図 2 に示すようなプリブート認証画面を使用します。この画面は、システムの電源をオンにした直後に表示されます。

ログオンするには、次の手順を実行します。

1. ユーザ名 (ユーザ ID) を入力してください。
2. パスワードを入力してください。
3. 上下の矢印を使用して有効な Windows のドメイン名を選択してください。
4. Enter キーを入力してください。

これで、Windows が起動されます。一般的な ProtectDrive の導入事例では、ユーザは自動的に Windows へログオンします。ただし、ユーザが手動で Windows へログオンしなければならないよう、システム管理者が ProtectDrive を設定する場合があります。[第 3 章](#) (Windows へのログオン) を参照してください。

プリブート・ログオンに失敗した場合の対処方法

プリブート・ユーザ名またはパスワードを間違えた場合

あらかじめ設定された試行回数内（デフォルト値は 3 回ですが、システム管理者の選択により異なります）に、ユーザが ProtectDrive で正しいプリブートのユーザ名またはパスワードを指定することに失敗すると、以下のようなユーザのロックアウト画面が表示されます。



このメッセージが表示されると、カウントダウンが始まり、この間はシステムを操作できなくなります（デフォルト値は 3 ですが、このカウントダウンの期間はシステム管理者の選択により異なります）。詳細なヘルプについては、システム管理者にお問い合わせください。

システムの停止によるプリブート・ログオンの失敗

ProtectDrive のシステム・ファイルまたは暗号化ハード・ドライブ・パーティションのいずれかが破損している場合、ユーザはプリブート時のシステム認証を実行できなくなります。場合によっては、以下の例のように、エラー画面に ACS エラー番号が表示されます。

Error ACS0301

このエラー番号をシステム管理者へ通知してください。

第3章

Windows へのログオン

通常、システム管理者は、プリブート認証の成功後に自動的にユーザが Windows へログオンできるように ProtectDrive システムを設定しています。この場合、それ以上のユーザ入力不要で、通常 Windows が起動されます。

ただし、ユーザが手動で Windows へログオンしなければならない場合もあります。以下のセクションを参照してください。

手動での Windows へのログオン

ユーザが手動で Windows へログオンしなければならないようにシステム管理者がシステムを設定している場合、ユーザのプリブート認証の成功後、図 5 と 6 に示すような Windows の初期画面のいずれかが表示されます。



図 5 - スマートカードおよびトークン/PIN の場合の Windows の初期画面



図 6 - ユーザ名、パスワードおよびドメイン名の場合の Windows の初期画面

スマートカード、トークンおよび PIN による Windows へのログオン

スマートカード、トークンおよび PIN のユーザは、前ページの図 5 に示すような Windows の初期画面を使用します。

Windows へ手動でログオンするには、次の手順を実行します。

1. スマートカードまたはトークンをリーダーへ挿入してください。次のような Windows のログオン画面が表示されます。



2. PIN を入力してください。
3. [OK] をクリックしてください。通常の Windows が起動され、見慣れた Windows デスクトップの画面が表示されます。

ユーザ名、パスワードおよびドメイン名による Windows へのログオン

ユーザ名、パスワードおよびドメイン名のユーザは、前ページの図 6 に示すような Windows の初期画面を使用します。

Windows へ手動でログオンするには、次の手順を実行します。

1. Ctrl、Alt、Del キーを同時に押してください。次のような Windows のログオン画面が表示されます。



2. システム管理者から供給された **Windows** のユーザ名とパスワードを入力してください。
3. [**ログオン先**] のリストから **Windows** のドメインを選択してください。
4. [**OK**] をクリックしてください。通常の **Windows** が起動され、見慣れた **Windows** デスクトップの画面が表示されます。

第4章

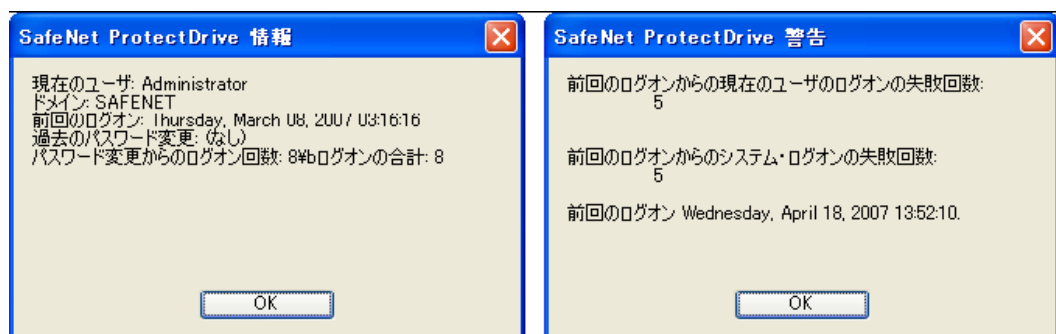
ProtectDrive での Windows の使用

ProtectDrive は、エンド・ユーザへの負担を最小限に抑えて実行するよう設計されています。これは、通常のコンピュータ・システムの動作に影響させないことが目的です。ただし、さまざまな Microsoft Windows プログラムとユーティリティに関する一部の小さなソフトウェア互換性の問題が存在するため、これらの問題を考慮する必要があります。

この章では、さまざまな Microsoft Windows およびソフトウェアの互換性に関する、ProtectDrive で保護されたコンピュータ・システムを運用する際にユーザが考慮すべき事項について説明します。

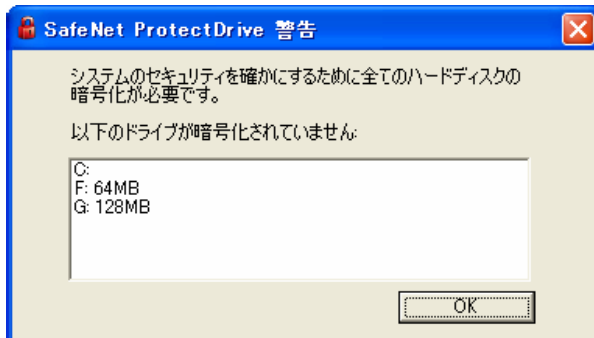
ProtectDrive ユーザ認証の動作の追跡

システム管理者は、お使いの ProtectDrive 認証の動作を通知するようシステムを設定している場合があります。このような場合、Windows 認証に成功してからエクスプローラがロードされるまでの間に、次の ProtectDrive 情報ダイアログが表示され、ユーザにそれまでの ProtectDrive プリブート認証の動作に関する警告を行います。



ディスク暗号化に関する警告

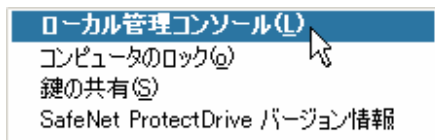
システム管理者が、ハードディスク・パーティションの暗号化が完了していない状態をユーザに警告するようにシステムを設定していて、いずれかのドライブが暗号化されていないことが分かった場合、エクスプローラのロード直後に次の警告メッセージが表示されます。



この警告メッセージが表示された場合は、[OK] をクリックしてからシステム管理者へお問い合わせください。

SafeNet ProtectDrive システム・トレイ・アイコン

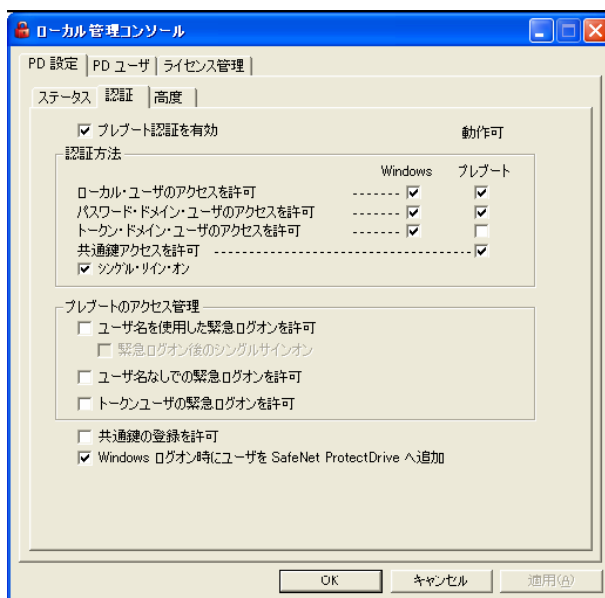
[SafeNet ProtectDrive をシステム・トレイのアイコンに表示] オプション ([PD 設定]-> [高度] -> [ユーザ・インターフェイス]) を有効化するようにシステムが設定されている場合、Windows デスクトップの右下にあるシステム・トレイに ProtectDrive の小さなアイコン (🔒) が配置されます。このアイコンは、PC が ProtectDrive で保護されていることを示しています。



アイコンを右クリックして、ローカル管理コンソールへのアクセス、Windows デスクトップのロック (Windows Vista の場合には、未サポート)、ユーザの共通鍵の登録/管理 (このオプションを設定している場合)、および SafeNet ProtectDrive に関する情報 (バージョン番号、ライセンス、および著作権情報) を表示します。

ローカル管理コンソールへのアクセス

1. システム・トレイのアイコン (🔒) を右クリックしてください。
2. [ローカル管理コンソール] を選択してください。



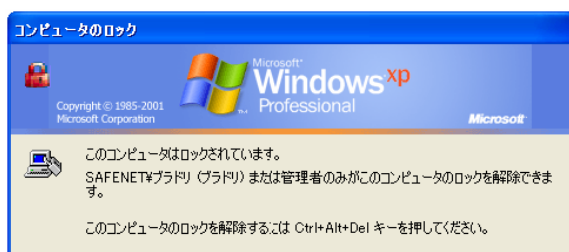
注意：ローカル管理コンソールは、アイコン (🔒) をダブルクリックして開くこともできますが、Windows デスクトップからアクセスすることも可能です。[スタート]-> [プログラム]-> [SafeNet Protect Drive]-> [ローカル管理コンソール] を選択します。

通常、管理者により [PD 設定] が設定されています。これらの設定の詳細については、『SafeNet ProtectDrive 管理ガイド』を参照してください。

Windows デスクトップのロック

この機能は、Windows Vista では、サポートしていません。

1. システム・トレイのアイコン (🔒) を右クリックしてください。
2. [コンピュータをロックする] を選択してください。次のような Windows の画面が表示されます。




3. スマートカードおよびトークンを挿入するか、または Ctrl、Alt、Del キーを同時に押して Windows デスクトップに戻ります。

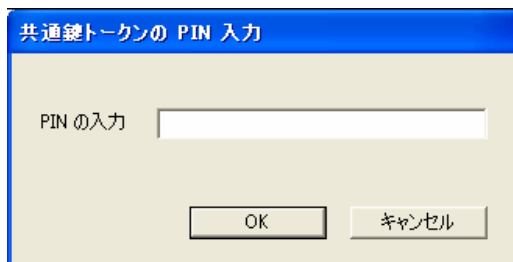
共通鍵の登録

[共通鍵の登録を許可] ([PD 設定] -> [認証]) オプションを有効にすると、SafeNet ProtectDrive システム・トレイ・アイコンのメニューに [共通鍵] という選択項目が表示されます。

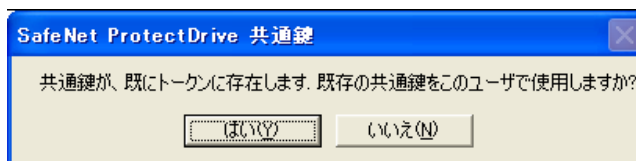
プリブート認証に共通鍵トークンを使用するには、ユーザは共通鍵を登録する必要があります。

トークンのユーザに割り当て済みの共通鍵が不要な場合は、次の手順に従います。

1. システム・トレイのアイコン () を右クリックしてください。
2. [共通鍵] を選択してください。次のような画面が表示されます。



3. トークン・ユーザの PIN を入力して [OK] をクリックしてください。
4. トークンの共通鍵がすでに存在する場合、次のようなメッセージが表示されます。



- [はい] を選択すると、既存の共通鍵がユーザに登録され、次のようなメッセージが表示されます。



[OK] をクリックして手順を完了します。

- [いいえ] を選択すると、次のようなメッセージが表示されます。



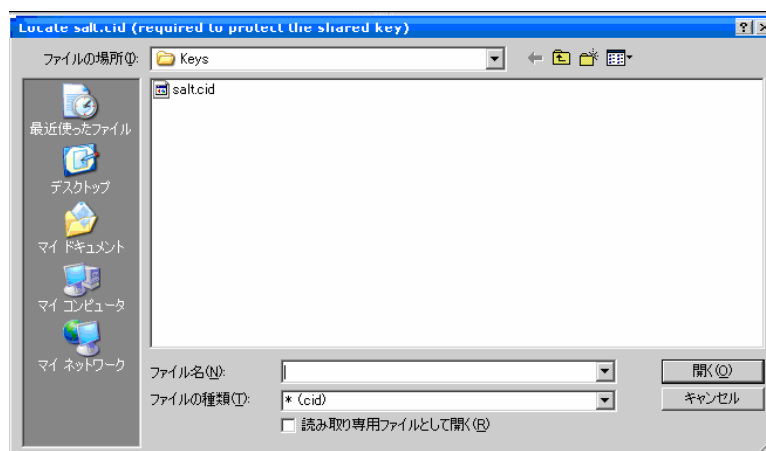
- [はい] を選択すると、新しい共通鍵がユーザに登録され、トークンの既存の共通鍵が上書きされます。

- ✧ 共通鍵をローカル（クライアント）で構成している場合、鍵が更新されたことを示す次のようなメッセージが表示されます。



[OK] をクリックして手順を完了します。

- ✧ 共通鍵を ProtectDrive サーバから構成している場合、salt.cid ファイルを要求されます。




salt.cid ファイルを参照して選択し、[開く] をクリックしてください。鍵が更新されたことを示す次のようなメッセージが表示されます。

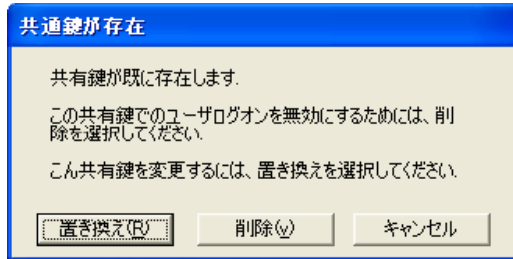


[OK] をクリックして手順を完了します。

- [いいえ] を選択すると、処理がキャンセルされます。共通鍵は作成されないか、またはユーザに割り当てられません。

トークンのユーザが割り当て済みの共通鍵を持っている場合は、次の手順に従ってください。

1. トークンを挿入してシステム・トレイのアイコン () を右クリックします。
2. [共通鍵] を選択します。次のような画面が表示されます。




- [置き換え] を選択する場合は、前のセクション (13 ページ) の手順 3 以降に従います。
- [削除] を選択した場合、既存の共通鍵の ProtectDrive ユーザ・プロファイルへの割り当てが解除されるか、または削除されます。次のような画面が表示されます。



[OK] をクリックして手順を完了します。

SafeNet ProtectDrive に関する情報の表示

1. システム・トレイのアイコン () を右クリックしてください。
2. [SafeNet ProtectDrive のバージョン情報] を選択してください。次のような画面が表示されます。



ProtectDrive で保護された PC での Windows フォルダ圧縮アプリケーションの使用

Windows フォルダ圧縮は完全にサポートされていますが、1 つだけ例外があります。ProtectDrive システム・ファイル・ディレクトリ (C:\\$SECURDSK) は書き込み保護されていて、削除または圧縮はできません。このディレクトリを圧縮すると、ProtectDrive の通常の動作に影響します。

ProtectDrive で保護された PC での Windows システム復元ユーティリティの使用

ProtectDrive のインストール前に作成された Windows システム復旧ポイントは使用できなくなります。システムで復旧できるのは、ProtectDrive のインストール後に作成された復旧ポイントまでです。

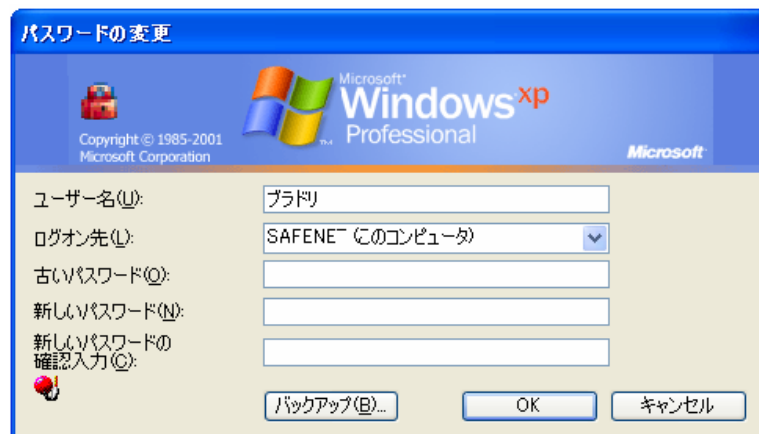
ProtectDrive プリブート・パスワードの変更

1. Ctrl-Alt-Del キーを同時に押して [パスワードの変更] を選択してください。



2. [ログオン先] リストから適切なドメインを選択して新しいパスワードを指定してください。

ローカルの Windows（画面右側に表示される「このコンピュータ」を参照）の場合、新しいパスワードの変更が直ちに有効となります。

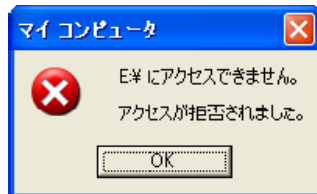


Windows ドメイン、ユーザは Windows からいったんログアウトし、再度ログオンする必要があります。これにより、新しいパスワードが ProtectDrive のプリブート・ユーザのデータベースに反映されます。

ユーザがこの手順を実行しない場合、プリブート時の古いパスワードを使用する必要があります。新しいパスワードでいったん Windows ドメインへログオンすると、この新しいパスワードが ProtectDrive のプリブート・ユーザのデータベースに反映されます。

デバイスへのアクセス拒否エラー

ProtectDrive 管理者は、ユーザがリムーバブル・メディアなど特定のデバイスへアクセスするのを拒否するようシステムを設定できます。デバイスへのアクセス制御権が無効なユーザが特定のデバイスにアクセスしようとする、次のようなメッセージが表示されます。



この場合は、システム管理者にお問い合わせください。

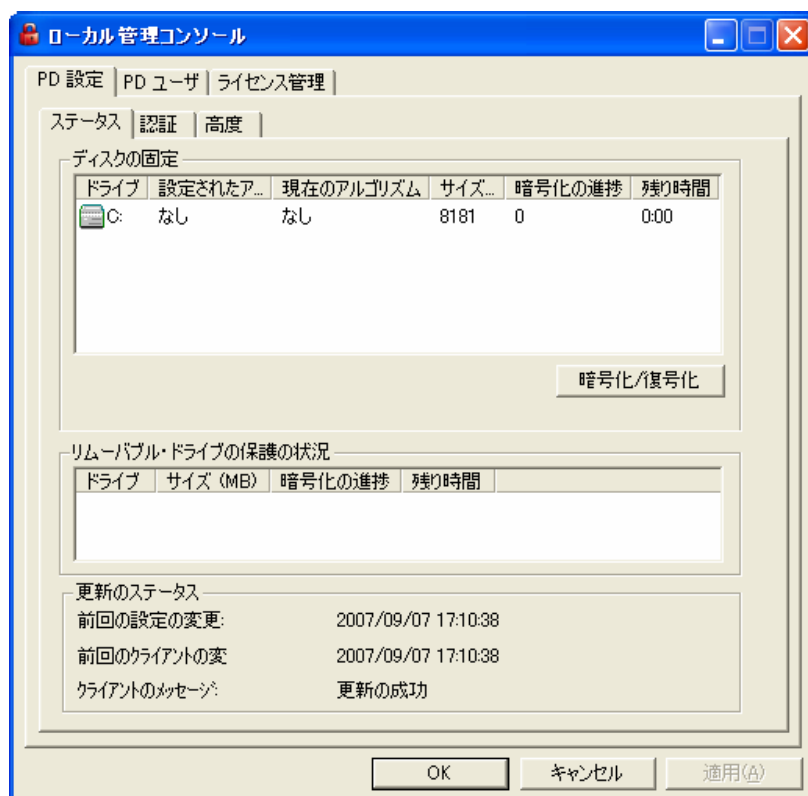
注意：デバイスへのアクセス制御権については、『管理者ガイド』を参照してください。

第5章 ハード・ドライブおよびリムーバブル・メディアの暗号化

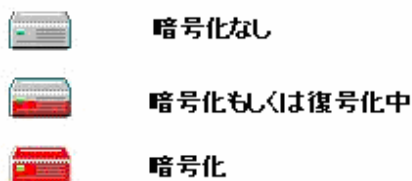
ハード・ドライブの暗号化

ハード・ドライブを暗号化するには、次の手順を実行してください。

1. Windows デスクトップから [スタート] -> [プログラム] -> [SafeNet ProtectDrive] -> [ローカル管理コンソール] を選択してください。
2. [PD 設定] タブをクリックしてください。
3. [暗号化ステータス] タブをクリックしてください。



次のアイコンはドライブのステータスを示します。



表示される列は次のとおりです。

[ドライブ]	パーティションのドライブ文字
[設定されたアルゴリズム]	指定のパーティションの暗号化に選択するアルゴリズム
[現在のアルゴリズム]	暗号化に使用するアルゴリズムが すべての暗号化パーティションに表示されます。
サイズ (MB)	パーティションのサイズ
暗号化の進捗	実行中の暗号化操作のステータス・インジケータ
残り時間	実行中の暗号化操作のステータス・インジケータ

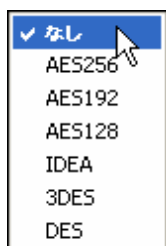
4. 暗号化するドライブをクリックしてください。複数のドライブを暗号化するには、次の手順を実行してください。

- 連続していない複数のドライブを選択するには、**Ctrl** ボタンを押した状態でマウスをクリックします。
- 連続したドライブを一括で選択するには、**Shift** キーを押した状態でマウスをクリックします。

注意：複数のドライブを選択するには、以下の手順 5 で選択する同じアルゴリズムで、それらのドライブすべてを暗号化する必要があります。ただし、必要に応じてドライブの暗号化アルゴリズムを変更できます。『管理者ガイド』の「異なるアルゴリズムを使用したドライブの再暗号化」を参照してください。

5. [暗号化／復号化] をクリックして、暗号化アルゴリズムを表示されたリストから選択します。

表示されるアルゴリズムの選択肢は、システム構成により異なります。システムに最適な暗号化アルゴリズムのガイダンスについては、システム管理者にお問い合わせください。



なし	このカラムを選択すると、暗号化ドライブが復号されます。ハード・ドライブを復号できるのは、システム管理者のみです。管理者特権を持たないユーザの場合、この設定が無効になっています。
AES256 AES192 AES128	この選択肢にある AES (Advanced Encryption Standard) 256 は、256 ビットの鍵を処理する対称ブロック暗号です。ProtectDrive では、CBC モードの暗号を使用します。
IDEA	IDEA (International Data Encryption Algorithm) 暗号は、64 ビット・ブロックと 128 ビット鍵を使用して処理されます。ProtectDrive では、CBC モードの暗号を使用します。
3DES	トリプル DES 暗号は、正式なテスト済みの 112 ビット鍵/64 ビット・ブロック暗号です。ProtectDrive では、CBC モードの暗号を使用します。この暗号の詳細については、さまざまな資料が公開されています。
DES	DES 暗号は、正式なテスト済みの 56 ビット鍵/64 ビット・ブロック暗号です。ProtectDrive では、CBC モードの暗号を使用します。この暗号の詳細については、さまざまな資料が公開されています。

6. [適用] または [OK] をクリックしてください。

- [適用] をクリックした場合、暗号化処理が開始され、ローカル管理コンソールは開いたままになっています。
- [OK] をクリックした場合、暗号化処理が開始され、ローカル管理コンソールは閉じられます。
- [キャンセル] をクリックすると、暗号化が開始されていないすべてのパーティションの暗号化処理がキャンセルされるか、または、所定のパーティションですでに開始されている暗号化処理は一時停止します。

注意：システム管理者がディスクの暗号化を無効にするようシステムを設定している場合、[OK] と [適用] が無効になっています。

ドライブの復号

ハード・ドライブを復号できるのは、システム管理者のみです。管理者特権を持たないユーザはこのオプションを使用できません。

1. Windows デスクトップから [スタート] -> [プログラム] -> [SafeNet ProtectDrive] -> [ローカル管理コンソール] を選択してください。
2. [PD 設定] タブをクリックしてください。
3. [暗号化ステータス] タブをクリックしてください。
4. 復号化するドライブをクリックしてください。

5. [暗号化／復号化] をクリックして [なし] を選択してください。
6. [適用] または [OK] をクリックしてください。ドライブが復号されます。

異なるアルゴリズムを使用したドライブの再暗号化

ドライブが暗号化済みである場合、随時別のアルゴリズムを使用して再暗号化できます。

1. Windows デスクトップから [スタート] -> [プログラム] -> [SafeNet ProtectDrive] -> [ローカル管理コンソール] を選択してください。
2. [PD 設定] タブをクリックしてください。
3. [暗号化ステータス] タブをクリックしてください。
4. 再暗号化するドライブをクリックしてください。
5. [暗号化／復号化] をクリックして別のアルゴリズムを選択してください。
6. [適用] または [OK] をクリックしてください。新しく選択したアルゴリズムによりドライブが再暗号化されます。

リムーバブル・メディア

このセクションでは、リムーバブル・メディアに使用できる機能全般について説明します。暗号化、復号化、ロック、ロック解除など、リムーバブル・メディアの機能の大部分は、Windows のエクスプローラで使用できます。システム管理者がどのようにシステムとユーザのポリシーを設定しているかによっては、これらの機能にアクセスできるユーザが制限されている場合もあります。

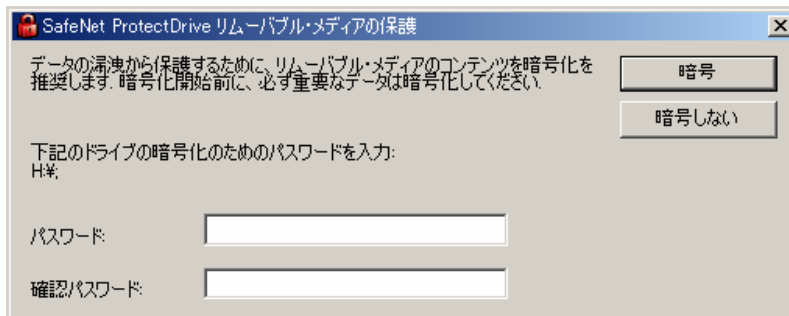
リムーバブル・メディアの暗号化、ロック解除、および復号にはパスワードが必要です。

リムーバブル・メディアの暗号化

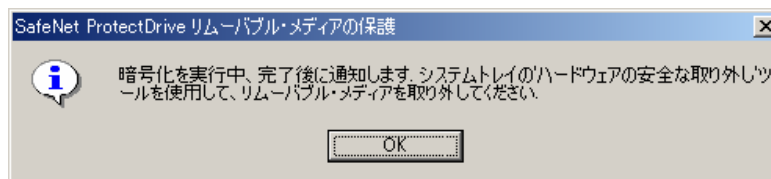
システムでリムーバブル・メディアが検出されると同時に、自動的にそのリムーバブル・メディアを暗号化するかどうかをユーザに確認するプロンプトが表示されるように、システムが設定されている場合があります。また、ユーザは次ページで説明する Windows のエクスプローラを使用して、リムーバブル・メディア・デバイスを随時暗号化できます。

暗号化プロンプトの自動表示

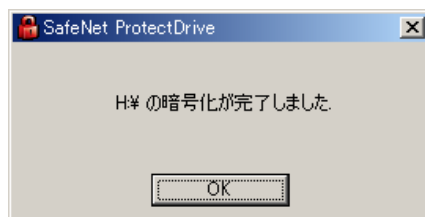
接続時に保護されていないリムーバブル・メディアが自動的に検出されるようシステムが設定されている場合、次のようなプロンプトが表示されます。



1. このデバイスへのアクセスに必要な暗号化パスワードを 2 度入力してから **[暗号化]** をクリックします (**[暗号化しない]** をクリックすると、保護されていないメディアにアクセスできます。これは、システム管理者が保護されていないメディアへのアクセスを許可しているかどうかにより異なります)。
2. 暗号化がすでに開始されていることを確認するプロンプトが表示されたら **[OK]** をクリックしてください。



3. 次のような完了プロンプトが表示されたら **[OK]** をクリックしてください。

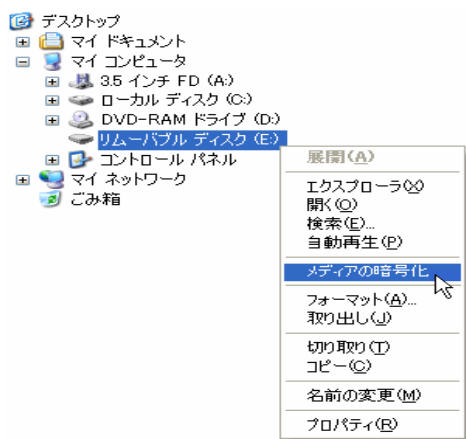


これ以降は、デバイスのロック解除と復号に暗号化パスワードが必要となります。

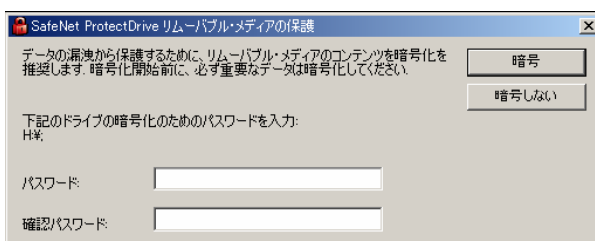
Windows エクスプローラによるメディアの暗号化オプション

Windows エクスプローラからリムーバブル・メディアを暗号化するよう、手動で選択できます。

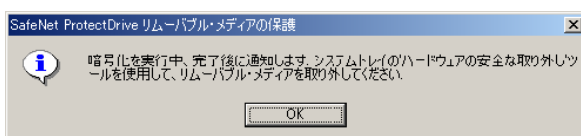
1. Windows エクスプローラでリムーバブル・メディア・デバイスへ移動してください。
2. デバイスを右クリックして [メディアの暗号化] を選択してください。



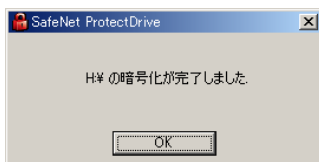
3. デバイスへのアクセスに必要な暗号化パスワードを 2 度入力してから [暗号化] をクリックしてください。



4. 暗号化がすでに開始されていることを確認するプロンプトが表示されたら [OK] をクリックしてください。暗号化されている間はプログレス・バーが表示されます。



5. 次のような完了プロンプトが表示されたら [OK] をクリックしてください。



これ以降は、デバイスのロック解除と復号に暗号化パスワードが必要となります。

リムーバブル・メディアのロック

Windows エクスプローラの [メディアのロック] オプションを使用すると、許可されていないユーザがリムーバブル・メディアへアクセスできなくなります。メディアのロックを解除するには、暗号化パスワードが必要となります。

1. Windows エクスプローラでリムーバブル・メディア・デバイスへ移動してください。
2. ロックするデバイスを右クリックして [メディアのロック] を選択してください。



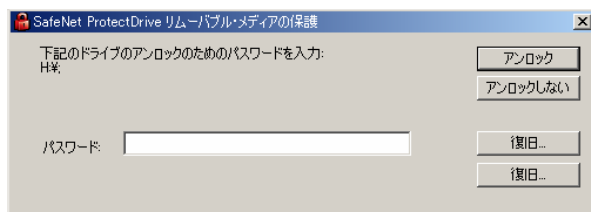
リムーバブル・メディアのロック解除

Windows エクスプローラの [メディアのロック解除] オプションを使用すると、選択したメディアにアクセスできるようになります。この操作には暗号化パスワードが必要です。

1. Windows エクスプローラでリムーバブル・メディア・デバイスへ移動してください。
2. ロックを解除するデバイスを右クリックして [メディアのロック解除] を選択してください。



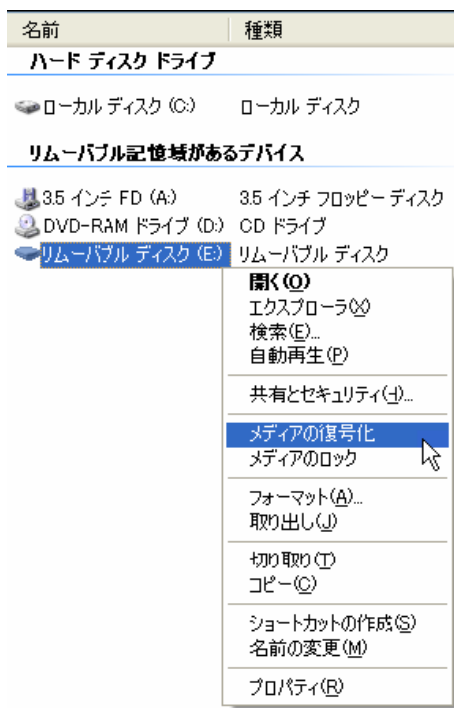
3. プロンプトが表示されたら、暗号化パスワードを入力して [ロック解除] をクリックしてください。



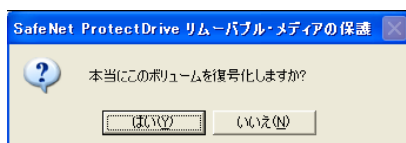
リムーバブル・メディアの復号

ユーザがリムーバブル・メディアを復号できるようにシステムが設定されている場合、Windows エクスプローラの [メディアの復号] オプションを使用します。このオプションを使用するにはパスワードが必要となります。また、復号を実行するにはデバイスのロックを解除する必要があります。

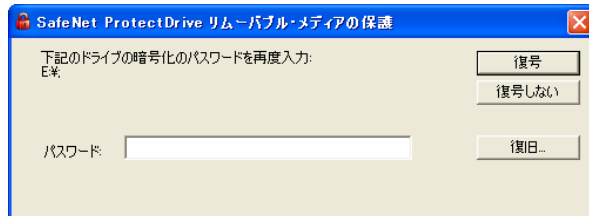
1. Windows エクスプローラでリムーバブル・メディア・デバイスへ移動してください。
2. 復号するデバイスを右クリックして [メディアの復号] を選択してください。



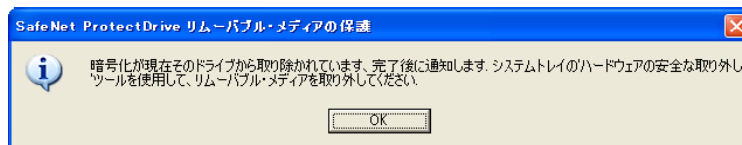
3. [はい] をクリックして復号を確認してください。



4. プロンプトが表示されたら、暗号化パスワードを入力して [復号] をクリックしてください。



5. 復号がすでに開始されていることを確認するプロンプトが表示されたら [OK] をクリックしてください。復号されている間はプログレス・バーが表示されます。



6. 完了プロンプトが表示されたら [OK] をクリックしてください。



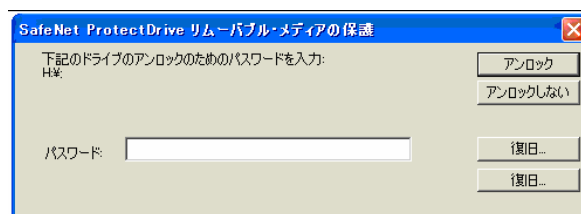
リムーバブル・メディアの復旧

標準的なリカバリ手順

リムーバブル・メディア・デバイスの動作が不安定になったり破損したりした場合に、メディアを確実にリカバリして再利用できるようにするには、次の手順に従ってデバイスの暗号化を解除し、いったんフォーマットしてから再利用できるようにしてください。

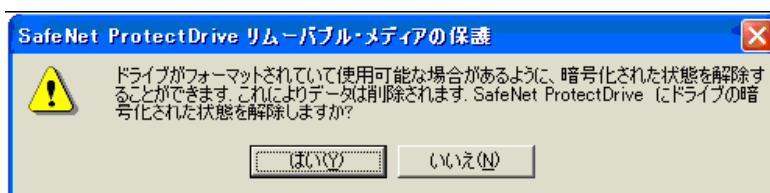
この手順は、利用中の USB フラッシュ・ドライブごとに実行する必要があります。

1. リムーバブル・メディアと PC を接続してください。デバイスが検出されると、次のような画面が表示されます。

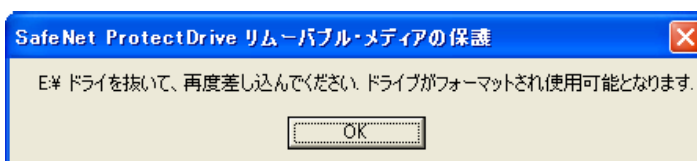


2. [修復] をクリックしてください。

3. 次のようなメッセージが表示されたら [OK] をクリックしてください。



4. [はい] をクリックしてください。
5. プロンプトが表示されたら [OK] をクリックして安全にデバイスを取り外してください。



6. リムーバブル・メディアを再接続し、再利用できるように再フォーマットしてください。再フォーマットは、デバイスが再度暗号化される前に実行してください。

バックアップ・リカバリ手順（オプション）

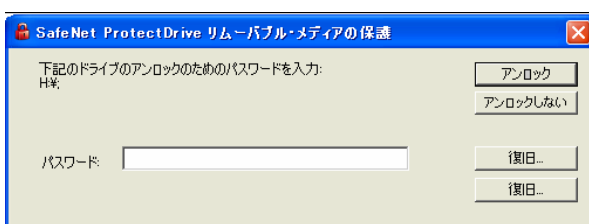
この代替リカバリ手順については、『SafeNet ProtectDrive 管理ガイド』の第 5 章で詳細に説明している「Sector 0 Backup Recovery Procedure」を参照してください。リムーバブル・メディア・デバイスのセクタ 0 のデータが以前にバックアップされている場合は、このリカバリ手順を使用して、そのデバイスを再利用できるように再フォーマットできます。

リムーバブル・メディアの緊急アクセス

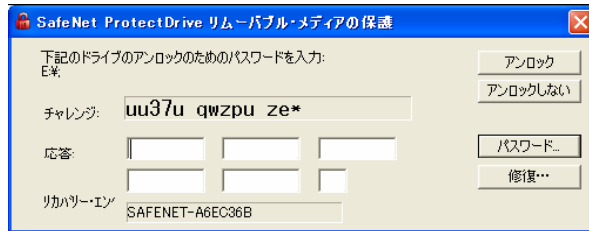
この手順により、ユーザがパスワードを忘れた場合に、リムーバブル・メディアへ一時的に緊急アクセスできるようになります。緊急アクセスとは、ユーザがパスワードなしでアクセスできることを意味します。リムーバブル・メディアへのフル・アクセスを回復するには、デバイスを復号してから再暗号化し、パスワードをリセットする必要があります（これらの手順は、すべてこのセクションに含まれています）。

エンド・ユーザの手順 - チャレンジ・コードの生成

1. リムーバブル・メディアと PC を接続してください。デバイスが検出されると、次のような画面が表示されます。



2. [リカバリ] をクリックしてください。次の例に示すように、[チャレンジ] にコードが表示されます。



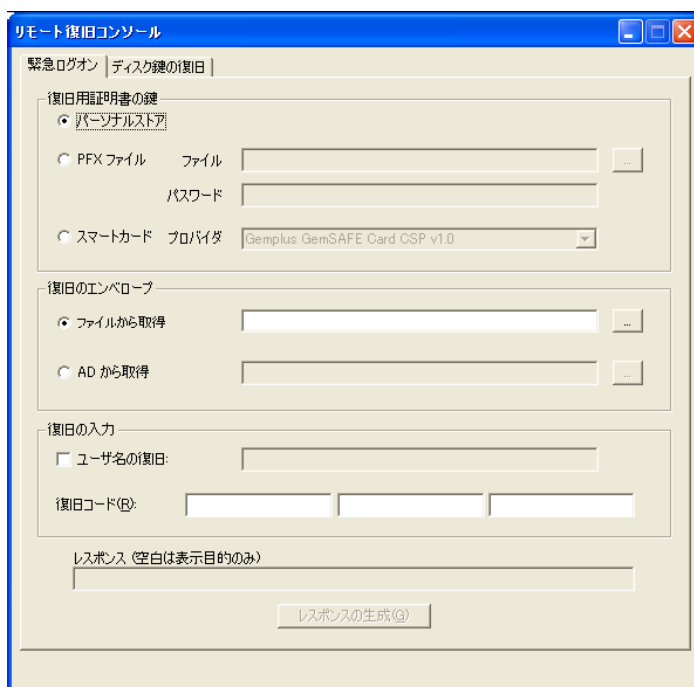
3. (電話または直接) システム管理者に問い合わせ、このチャレンジ・コードを通知してください。
4. システム管理者は `rpadmin` ユーティリティを実行し、チャレンジ・コードに基づいてレスポンスを生成し (詳細な手順については次ページで説明します)、復旧コードを通知してください。このコードを [レスポンス] フィールドに入力してください。
5. [ロック解除] をクリックしてください。この時点で、ユーザが削除するまでの間、リムーバブル・メディアへ一時的にアクセスできるようになります。ユーザがメディアを削除すると新しいパスワードが必要となります。

注意：新しいパスワードをリムーバブル・メディアに割り当てることができるようにするには、まずデバイスを修復する必要があります。リムーバブル・メディアのデータを安全な場所に保存してから、28 ページにあるリムーバブル・メディアの標準リカバリ手順に従って操作します。その後、リムーバブル・メディアが再利用可能になり、そのデバイスを初めて使用するときに新しいパスワードを入力するよう求められます。パスワードを変更した後で、保存しておいたデータをリムーバブル・メディアにコピーしてください。

システム管理者の手順 - リカバリ・レスポンス・コードの生成

システム管理者向けのリムーバブル・メディアの鍵によるリカバリ手順を以下で説明します。

1. サーバの¥Program Files¥SafeNet ProtectDrive にある rpadmin.exe を実行してください。ProtectDrive の [リモート・リカバリ・コンソール] ウィンドウが表示されます。
2. [緊急ログオン] タブをクリックしてください。



3. 次の中から、適切な [復旧用証明書の鍵] オプションを選択してください。
 - パーソナルストア- このオプションを選択する場合は、パーソナルストアから使用するマシンにコピーされたユーザの個人用の復旧鍵の証明書が必要になります。
 - PFX ファイル- このオプションを選択する場合は、[...] をクリックしてから、ユーザの個人用 PdRecovery.pfx ファイルを参照して開いて、パスワードを入力してください。
 - スマートカード- このオプションを選択する場合は、証明書鍵をリストから適切なプロバイダを選択してください。
4. ユーザのコンピュータの 復旧のエンベロープ ファイルを選択してください。
 - ファイルから取得- このオプションを選択する場合は、[...] をクリックしてから、<コンピュータ名>_RecoveryEnvelope.env ファイルを参照して開いてください。
 - AD から取得- このオプションを選択する場合は、[...] をクリックしてから Active Directory のコンピュータを参照し、<コンピュータ名>_RecoveryEnvelope.env ファイルの場所を指定してください。

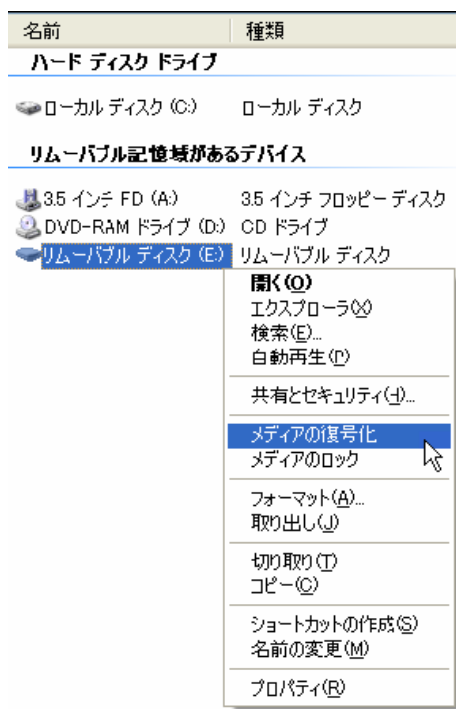
5. ユーザが入力したチャレンジ・コードを [復旧コード] に入力してから [レスポンスの生成] をクリックしてください。
6. 自動生成されたレスポンス・コードをそれぞれの [レスポンス] に入力して、[ロック解除] をクリックするようユーザに指示してください。

この時点で、ユーザが削除するまでの間、リムーバブル・メディアへ一時的にアクセスできるようになり、その時点でユーザは、リムーバブル・メディアを修復する必要があります (28 ページを参照)。リムーバブル・メディアが再利用可能になった後は、新しいパスワードが必要になります。

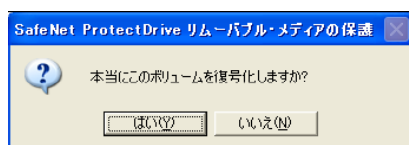
パスワードのリセット手順については、次のセクションを参照してください。

エンド・ユーザの手順 - リムーバブル・メディアのパスワード・リセット

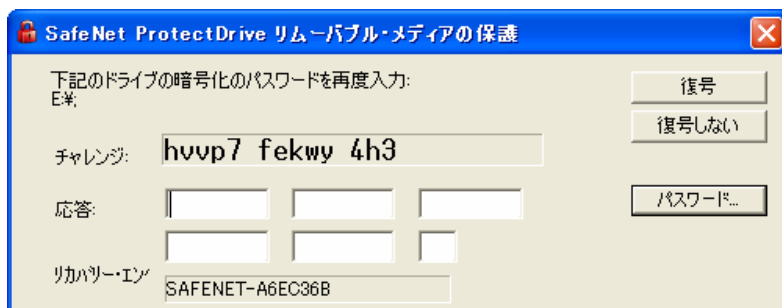
1. 安全にリムーバブル・メディア・デバイスを取り外して再接続します。Windows エクスプローラでリムーバブル・メディア・デバイスへ移動してください。
2. 復号するデバイスを右クリックして [メディアの復号化] を選択してください。



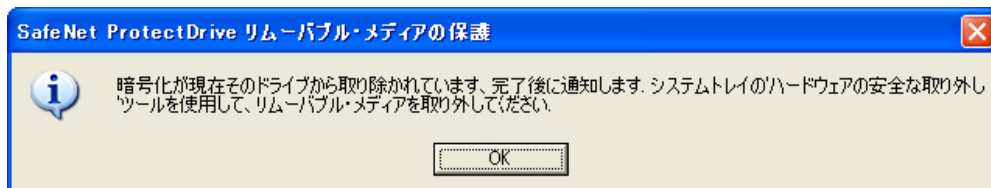
3. [はい] をクリックすると、復号化の確認メッセージが表示されます。



4. [リカバリ] をクリックしてください。次の例に示すように、[チャレンジ] にコードが表示されます。



5. (電話または直接) システム管理者に問い合わせ、このチャレンジ・コードを通知してください。
6. システム管理者は `rpadmin` ユーティリティを実行し、チャレンジ・コードに基づいてレスポンスを生成して (28 ページを参照)、リカバリ・コードを通知してください。このコードを [レスポンス] に入力してください。
7. [復号] をクリックしてください。
8. 復号が開始されたことを確認するプロンプトが表示されたら [OK] をクリックしてください。復号されている間はプログレス・バーが表示されます。



9. 次のような完了プロンプトが表示されたら [OK] をクリックしてください。

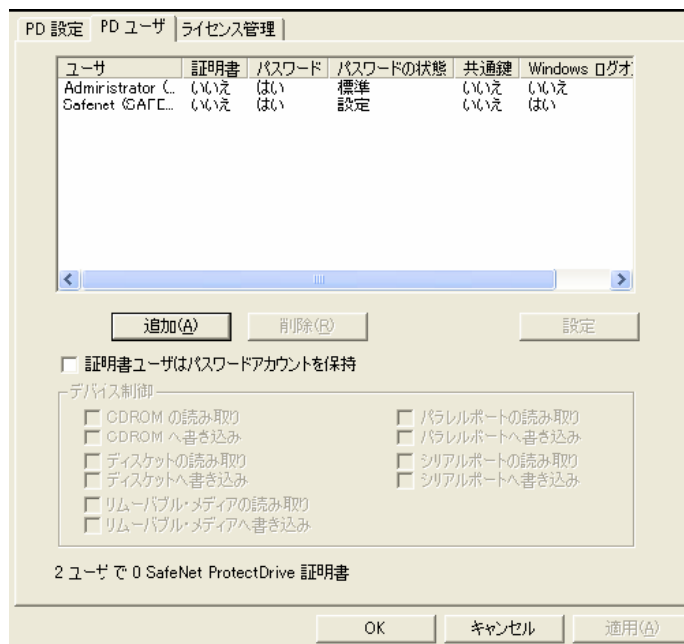


10. 安全にリムーバブル・メディア・デバイスを取り外して再接続してください。新しいパスワードを 2 度入力してから [暗号化] をクリックしてください。
11. 暗号化が完了するまで、残りのプロンプトの指示に従ってください。

第6章 ProtectDrive ユーザの設定

[PD ユーザ] タブには、現在プリブート・ユーザのデータベースに存在するユーザがすべて表示されます。Windows ユーザまたはグループとしてユーザを追加しておくと、ProtectDrive ユーザを追加できます。

また、[PD ユーザ] タブでは、ユーザに対してデバイスへのアクセス制御権を設定、ユーザのアカウントを設定、ProtectDrive ユーザのパスワードを変更、またはユーザを削除することも可能です。



注意：これらの設定を変更するには、管理者特権が必要です。

ユーザに対するデバイスへのアクセス制御権の設定

1. Windows デスクトップから [スタート] -> [プログラム] -> [SafeNet ProtectDrive] -> [ローカル管理コンソール] を選択してください。
2. [PD ユーザ] タブをクリックしてください。
3. ユーザ名をクリックしてください。
4. ユーザの適切な読み取りおよび書き込みのデバイス制御権限を選択し、[設定] をクリックしてください。
5. [適用]、[OK] の順にクリックしてください。

ProtectDrive ユーザの追加

1. Windows デスクトップから [スタート] -> [プログラム] -> [SafeNet ProtectDrive] -> [ローカル管理コンソール] を選択してください。
2. [PD ユーザ] タブをクリックしてください。
3. (オプション) このリストにあるすべてのユーザが標準パスワード ([PD 設定] -> [高度] -> [パスワード・ポリシー] グループの [標準パスワード] で定義) を使用してプリブート・アクセスできるようにするには、[証明書ユーザはパスワードアカウントを取得] を選択してください。
4. [追加] をクリックしてください。
5. 追加するローカル・ユーザまたはグループの名前を入力してから [OK] をクリックしてください。
6. (オプション) ユーザが共有鍵アカウントも持っている場合は、新しいユーザを強調表示して [設定] をクリックしてください。[共有鍵アカウントを使用] をオンにし、[OK] をクリックしてください。

ProtectDrive ユーザのパスワード変更

1. Windows デスクトップから [スタート] -> [プログラム] -> [SafeNet ProtectDrive] -> [ローカル管理コンソール] を選択してください。
2. [PD ユーザ] タブをクリックしてください。
3. ユーザ名をクリックしてから [設定] をクリックしてください。
4. 新しいパスワードを 2 度入力してから [OK] をクリックしてください。

注意： ユーザ・アカウント設定 画面で [標準パスワードを使用] が選択されている場合は、このオプションの選択を解除してユーザのパスワードを変更してください。

ProtectDrive ユーザの削除

1. Windows デスクトップから [スタート] -> [プログラム] -> [SafeNet ProtectDrive] -> [ローカル管理コンソール] を選択してください。
2. [PD ユーザ] タブをクリックしてください。
3. ユーザ名をクリックしてから [削除] をクリックしてください。
4. [OK] をクリックして手順を完了してください。

第7章 トラブルシューティング

スマートカードおよびトークンの配置を間違えた場合、 または PIN を忘れた場合の対処方法

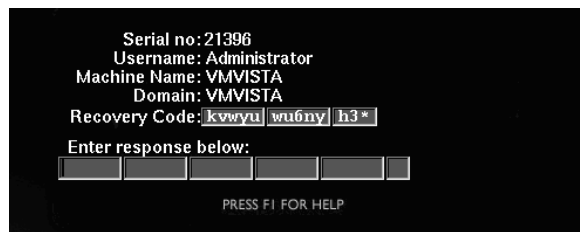
この手順の対象は、スマートカード、トークンおよび PIN ユーザです。

スマートカードまたはトークンを無くした場合、あるいは PIN を忘れてしまった場合、ProtectDrive の「トークン・ユーザの緊急ログオン」手順を実行すれば、システムにアクセスできるようになります。

1. カーソルを **[PIN]** フィールドに合わせて Shift+F9 キーを押してください。



次のような [リカバリ&レスポンス] 画面が表示されます。



2. (電話でまたは直接) システム管理者に問い合わせ、表示される Recovery Code (復旧コード) を通知してください。
3. 応答として、管理者からユーザへレスポンス・コードが通知されます。以下のようにこのコードを **[Enter response below]** に入力してください。



4. この時点で Windows は、通常どおり起動動作に進み、システム管理者の ProtectDrive 設定に応じて自動または手動のどちらかでユーザを Windows へログオンさせます。

手動での Windows ログオンについては、[第3章](#)（Windows へのログオン）を参照してください。

パスワードを忘れた場合の対処方法

この手順の対象は、ユーザ名、パスワードおよびドメイン名のユーザです。

パスワードを忘れた場合、「ユーザ名による緊急ログオン手順」に従ってシステムへのアクセスを復旧します。

1. 以下のとおり、[ユーザ名、パスワードおよびドメイン名のログオン] 画面の **[User ID]** フィールドにユーザ名を入力してください。



2. カーソルを **[Password]** フィールドに合わせて **Shift+F10** キーを押してください。次のような **[リカバリ&レスポンス]** 画面が表示されます。



3. システム管理者に問い合わせて、表示された **Recovery Code**（復旧コード）をユーザ名と一緒に通知してください。
4. 応答として、管理者からユーザへレスポンス・コードが通知されます。このコードを **[Enter response below]** フィールドに入力してください。



5. この時点で Windows は、通常どおり起動動作に進み、システム管理者の ProtectDrive 設定に応じて自動または手動のどちらかでユーザを Windows へログオンさせます。

手動での Windows ログオンについては、[第3章](#)（Windows へのログオン）を参照してください。

プリブート・ユーザ・アカウントを持っていない場合の対処方法

この手順の対象は、ユーザ名、パスワードおよびドメイン名のユーザです。

ProtectDrive で保護された PC に初めてログオンする場合には、システム管理者から次の「ユーザ名を入力しない緊急ログオン手順」を実行するように求められることがあります。

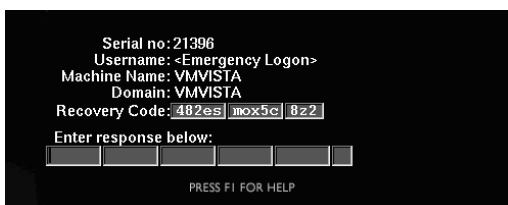
この手順は、ユーザ名/パスワード/ドメイン名の認証方式のみに適用されます。スマートカード、トークンおよび IN の新規ユーザの場合、システム管理者によりプリブート・アカウントがすでに作成されているため、このセクションで説明するような手順を実行しなくてもシステムにログオンできます。

ユーザ名なしでの緊急ログオン手順

1. 以下のとおり、[ユーザ名、パスワードおよびドメイン名のログオン] 画面の [User ID] フィールドにカーソルを合わせ、Shift+F9 キーを押してください。



次のような [リカバリ & レスポンス] 画面が表示されます。



2. システム管理者に問い合わせ、表示された Recovery Code（復旧コード）を通知してください。
3. 応答として、管理者からユーザへレスポンス・コードが通知されます。このコードを [Enter response below] フィールドに入力してください。



システムへのプリブート・アクセスが1回のみ許可されます。

4. この時点で、Windows への通常のログオンが行われます。次のシステムへのログオンは、[第2章](#)（ProtectDrive で保護された PC へのログオン）での説明に従って行われます。

Copyright 2008, SafeNet, Inc.

All rights reserved.

<http://www.safenet-inc.com>

本書に記載される情報は完全かつ正確であるように最善を期しています。本書の誤りまたは情報の欠落による直接的または間接的損害、または事業の損失に対し、SafeNet, Inc. は責任を負いません。本書に記載されている仕様は、予告なく変更される場合があります。

SafeNet、ProtectDrive は、SafeNet, Inc. の商標または登録商標です。

本書で言及しているその他すべての製品名は、各社の商標または登録商標です。

2008 年 12 月