



ProtectDrive Version 8.5

管理者ガイド

© 2009 SafeNet, Inc. All rights reserved.

文書番号 007054-001（改訂版 F、2009 年 2 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：
東京都港区新橋 6 丁目 17 番 17 号 御成門センタービル 8F
日本セーフネット株式会社
電話：03-5776-2751

米国本社：
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。

関連マニュアル

トークンのサポートに関する基本的な設定手順については、本マニュアルで説明します。SafeNet の Borderless Security iKey USB トークンに関するインストールおよび設定情報の詳細については、次のマニュアルを参照してください。

- 『Borderless Security PK Administration Guide』
- 『iKey 1000 Series Developer's Guide』

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 の機能の説明.....	3
サポートされるプリブート・ユーザ認証証明情報.....	3
ユーザ認証証明情報を間違えたり、忘れた場合.....	4
自動プリブート認証後の自動での再ブート.....	4
Windows ユーザ認証.....	5
シングル・サイン・オン.....	5
手動での Windows 認証.....	5
Windows 以外の環境におけるシングル・サイン・オン.....	5
ハードディスクおよびリムーバブル・メディアの暗号化および 復号化.....	5
ProtectDrive システムおよびユーザのポリシーの設定.....	6
リモート管理.....	6
ローカル管理.....	6
Active Directory もしくは ADAM による集中管理.....	7
ADAM での ProtectDrive の集中管理.....	7
集中管理のための Windows ドメインの準備.....	8
ProtectDrive の復旧ファイルと鍵管理.....	8
ProtectDrive の障害復旧.....	9
ProtectDrive のライセンス.....	9
License.txt のインストール.....	10
Authorization.txt のインストール.....	10
インターネット・アクセスができない場合の対応方法.....	10
第 3 章 システム要件	13
ハードウェア最小要件.....	13
サポートされるストレージ・ハードウェア.....	13
デバイスのアクセス制御.....	13
サポートされるオペレーティング・システム.....	14
クライアント管理の場合.....	14
クライアントの場合.....	14
サポートされるネットワーク.....	14
第 4 章 ProtectDrive ソフトウェアの互換性.....	15
DOS ドライブおよび TSR.....	15
Windows およびサードパーティ製のブート・マネージャ.....	15
Windows のディスク・マネージャ・ユーティリティ.....	15
Windows のフォルダ圧縮ユーティリティ.....	15
Windows システム復旧ユーティリティ.....	15
Windows 高速ユーザ切り替えユーティリティ.....	15
第 5 章 ProtectDrive のインストール.....	17
作業を開始する前に.....	17

インストール前に	17
ストレージ・システムの準備	17
リカバリ・ディスクの準備	17
セクタ 0 のバックアップ（リムーバブル・メディアのみ）	18
カスタムの鍵セットの作成	18
未使用の ADAM サービス・コネクション・ポイント（SCPs）の手動削除	22
ADAM インスタンスの削除	22
ADAM SCP の削除	23
ADAM のための Windows Firewall の設定	24
ProtectDrive のインストール（MSI）パッケージ	26
MSI パッケージのカスタマイズ	26
ProtectDrive MSI の設定	27
管理者ツールのインストール	30
ProtectDrive のインストールの変更に関して	30
Windows ドメインの準備	30
ProtectDrive 管理ツールのインストール	33
ProtectDrive の管理ツール	35
ProtectDrive Management Console	36
クライアント・コンポーネントのインストール	40
インストールのカスタマイズ	47
以前のバージョンの ProtectDrive からのアップデート	54
アップグレードの前に	54
新しい復旧ファイルセットの作成	55
インタラクティブ・アップグレードに関して	55
サイレントおよび GPO アップグレードに関して	55
アップグレード手順	56
ProtectDrive の削除	57
Windows Vista	57
Windows 2000、2003 および XP	58
リムーバブル・メディアの復旧	59
標準的な復旧手順	59
RmRMBR を使ったリムーバブル・メディアの復旧	60
リムーバブル・メディアの復旧 - その他の方法	60
設定ファイル（.XML ファイル）のエクスポート	61
設定ファイル（.XML ファイル）のインポート	63
第 6 章 シングル・サイン・オン管理	65
はじめに	65
シングル・サイン・オン・アシスタントにアクセスする	65
Windows 認証	66
認証済みアカウント	66
RSA SOM のサポート	67
概要	67
導入	67
考察	67
サードパーティ製品のサポート	68
概要	68
サードパーティ GINA のサポート	68
サードパーティ製品アカウントのサポート	68

管理手順.....	69
既存システムへの ProtectDrive インストール後の設定.....	69
ProtectDrive システムにソフトウェアを追加インストールした後の設定.....	69
チェーンされた GINA を変更する.....	69
GINA を設定する.....	70
認証済みアカウントを作成する.....	71
認証済みアカウントを変更する.....	72
認証済みアカウントを削除する.....	73
認証済みアカウント・フィールドを作成する.....	73
認証済みアカウント・フィールドを変更する.....	74
認証済みアカウント・フィールドを削除する.....	75
SSO 設定をエクスポートする.....	76
第 7 章 マルチブート・システム.....	77
第 8 章 システムおよびユーザ・ポリシーの設定.....	79
Active Directory ユーザとコンピュータ(ADUC) MMC スナップインの標準設定.....	79
ProtectDrive Management スナップインの標準設定.....	80
PD 設定 タブ (デフォルトのシステム・ポリシー).....	81
認証の設定.....	81
高度の設定 — 証明書の利用.....	85
高度の設定 — ブート・マネージャ.....	87
高度の設定 — 標準のパーミッション (デバイスへのアクセス).....	88
高度の設定 — 暗号化.....	88
高度の設定 — 割り込みベクター (アドレス) の更新.....	90
高度の設定 — ロックアウトの設定.....	90
高度の設定 — 管理.....	91
高度の設定 — パスワード・ポリシー.....	92
高度の設定 — ユーザ インターフェース.....	93
PD ユーザ タブ (デフォルトのユーザ・ポリシー).....	95
ライセンス・マネージャ タブ (ライセンスの表示、インストールおよび更新).....	99
ライセンス・マネージャによるフルライセンスへのアップグレード.....	99
「nag」画面でのフルライセンスへのアップグレード.....	100
第 9 章 システムおよびユーザの管理.....	101
サーバからのシステム・ポリシーの管理.....	101
サーバからのユーザ・ポリシーの管理.....	105
コンピュータ・オブジェクト経由でのユーザのクライアントへの割り当ておよびユーザ・ポリシーの管理.....	105
ユーザ・オブジェクトもしくはグループ・オブジェクトでのユーザ・ポリシーの管理.....	105
グループ・オブジェクト経由でのユーザ・ポリシーの管理.....	106
システムおよびユーザ・ポリシーのローカル管理.....	107
PD 設定 タブ.....	108
PD ユーザ タブ.....	108
ローカルの Windows ユーザを ProtectDrive のプリブート・ユーザ・データベース (pduserdb) へ追加する.....	109
プリブート・パスワードの変更.....	110
第 10 章 ユーザ認証.....	111
スマートカードとトークンおよび PIN による認証.....	111
プリブート認証.....	111
Windows 認証.....	112

トークンの削除ポリシー	113
ユーザ名、パスワード、およびドメイン名による認証	113
プリブート認証	113
Windows 認証	114
第 11 章 例外的な認証のシナリオ	115
トークン・ユーザの緊急ログオン手順	116
エンド・ユーザ向け手順	116
システム管理者向け手順	117
ユーザ名を入力する緊急ログオン手順	119
エンド・ユーザ向け手順	119
システム管理者向け手順	120
ユーザ名を入力しない緊急ログオン手順	122
エンド・ユーザ向け手順	122
システム管理者向け手順	123
自動プリブート認証での自動リブート	125
障害復旧ディスク鍵の作成	127
復旧ディスク鍵の作成	127
ディスクの復旧（復号化）	130
第 12 章 障害復旧ツール	131
BACKUP.EXE - ProtectDrive リカバリ・ファイルの作成	131
DISPEFS.EXE - ProtectDrive 診断ユーティリティ	132
DECDISK.EXE - ディスク復号化ユーティリティ	133
リカバリ・ファイルの使用	134
手動での復号化領域の指定	135
RMBR.EXE - MBR 復旧ユーティリティ	136
RMBR 初期状態のチェック	136
RMBR バージョンの互換性チェック	137
ProtectDrive MBR の復旧（RMBR /p）	137
元の MBR の復旧（RMBR /o）	138
PDUSERDB.EXE - プリブート・ユーザ・データベース管理ユーティリティ	139
第 13 章 トラブルシューティング	141
32bit プリブートと 16bit プリブートの切り替え	141
ディスク暗号化に関する警告	142
ProtectDrive ユーザ認証の動作の追跡	142
プリブート・ユーザ名またはパスワードを間違えた場合	143
システムの停止によるプリブート・ログオンの失敗	143
デバイスへのアクセス拒否エラー	143
ローカル Windows 認証の拒否エラー	144
ブート後の Windows ドメイン認証の拒否エラー	144
イベント・ビューアのログ	144
Active Directory および ADAM のレポート・スクリプト	146
Active Directory を使用する ProtectDrive サーバ	146
ADAM を使用する ProtectDrive サーバ	146
レポートの出力例	147

付録 A スマートカードとトークンの PIN でのユーザ認証	149
付録 B ユーザ名、パスワードとドメインでの認証	151
付録 C ブート後の Windows ユーザの認証	153
付録 D システムのデバッグおよび ACS エラー・メッセージ	155
システムのデバッグ	155
ACS エラー・メッセージ	158
付録 E セキュリティに関する追加ガイダンス	163
ProtectDrive 評価版	163
ProtectDrive ユーザのためのガイダンス	163
CC 証明書のその他関連資料	163
製品 ID	164
インストール前:	164
インストール後:	164
組織の要件	164
外部システムとの接続	164
ガイダンス	164
改ざん	164
トレーニング	165
トークン	165
ユーザ	165
デバイスのアクセス許可	165
オペレーティング・システム構成に関するガイダンス	165
全般	165
パスワード・ポリシー	166
画面のロック機能	166
ProtectDrive の管理者に関する情報	166
オペレーティング・システム	166
評価済み項目	166
暗号化アルゴリズム	166
[ディスクが暗号化されていない場合には警告を表示] オプション	167
[自動ブリブート認証] オプション	167
[無効なログオンへの警告の表示] オプション	167
アクセス制御	167
付録 F iKey の管理	169
iKey 1000 の管理	169
iKey SDK による iKey1000 の管理	169
iKey 2032 の管理	171
SafeNet トークン・マネージャ・ユーティリティ	171
Web 登録	173

第1章 はじめに

製品概要

今日のコンピュータの利用において、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）十分なデータ保護を実現できます。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。

このようなデータ・セキュリティのギャップを埋めるために、SafeNet では ProtectDrive（PD）システムによるセキュリティおよびデータ暗号化アプリケーションを開発しました。SafeNet ProtectDrive は、マルチユーザの Windows Active Directory 対応のセキュリティ・アプリケーションです。ProtectDrive の一般的な運用環境では、次のリストに挙げられている機能を使用できます。

プリブート・ユーザ認証	オペレーティング・システムのファイルとその他の暗号化ハードディスクを復号化するための、一意の復号鍵を生成するのに使用します。スマートカードとトークンの PIN、および Windows ドメインのユーザ名とパスワードをサポートします。
緊急時のプリブート・ユーザおよびトークン・ログオンの復旧	スマートカードおよびトークン・ユーザのログオンの復旧と Windows ドメインのユーザのプリブート・ログオンの手順には、プリブート時にユーザ名が必要な緊急時のワнтаイム・ログオン、またはユーザ名が不要な緊急時のワнтаイム・ログオンが含まれます。
Windows のシングル・サイン・オンまたは手動による認証	ProtectDrive では、プリブート認証の成功後に Windows（ドメイン）の自動ユーザ認証を行います。手動での認証も使用できます。
管理可能なシステムおよびユーザのポリシー	固定ディスクおよびリムーバブル・メディアのデバイスのアクセス制御を行います。Microsoft 管理コンソール（MMC）スナップインを使用してポリシーを管理します。システムおよびユーザのポリシー・データを自動的にサーバから複製します。
ハードディスク、リムーバブル・メディアの暗号化	ユーザからは一切見えない形で強力なデータ暗号化を行います。
障害復旧ツール	破損または操作不能になったシステムの復旧に使用する MS-DOS ユーティリティです。

本書の対象読者

本書の対象読者は、一般的に ProtectDrive などのさまざまなコンピュータ・システム・コンポーネントの構成および保守を担当するシステム管理者です。

この担当者は、ProtectDrive のインストールや構成を行う管理者特権を持っている必要があります。本書は、シングルブートまたはマルチブート構成のスタンドアロンまたはネットワーク上のマルチユーザ・コンピュータ・システムにおける ProtectDrive の導入のガイドとして、また ProtectDrive のインストール、データ暗号化、システム管理およびユーザ管理、障害復旧などの問題に関するガイドとして使用します。

第2章

ProtectDrive の機能の説明

サポートされるプリブート・ユーザ認証証明情報

暗号化されたオペレーティング・システムのパーティションをブートするには、オペレーティング・システムをブートする前に ProtectDrive から復号鍵にアクセスできるようにする必要があります。この鍵は、オペレーティング・システムのファイルやその他の暗号化ハードディスクの復号化に使用します。

そのために、ProtectDrive ではプリブート・ユーザ認証を行います。復号鍵は、ユーザ認証証明情報から生成される一意のデータ鍵で暗号化されています。ユーザ認証が完了すると、このディスクの鍵を復号化してオペレーティング・システムをブートできるようになります。この機能をサポートするために、ProtectDrive には独自のプリブート・ユーザ・データベース (**pduserdb**) を保持しています。

この ProtectDrive のプリブート・ユーザ・データベースには、次のような特徴があります。

- ユーザおよび証明書の最大数 – 2,000
- ユーザ名の長さおよび指定方法 – 1~20 文字（半角英数文字）
- パスワードの長さおよび指定方法 – 20 文字まで（半角英数文字、大文字と小文字の区別あり）

注意：実際のユーザの最大数は 2,000 エントリですが、ProtectDrive では、3 つエントリを内部的に使用します。従って、残りの 1,997 が使用可能です。また、各ユーザのユーザパスワード、iKey 1000 で使用される共有鍵および、証明書を利用する場合にそれぞれ 1 つ利用されます。（全てをユーザにそれぞれを設定した場合には、3 つのエントリが利用されます。）

注意：Windows のパスワードも最大で 20 文字です。

注意：10 分以上なにも入力されないと、空白の画面が表示されます。（32 bit モードのみ）

ProtectDrive では、スタンドアロン（ローカルの Windows のみ）および Windows ドメイン・システムのユーザをプリブート認証できます。次の表では、ProtectDrive でサポートされるユーザ認証証明情報について説明します。

**スマートカードとトークン
および PIN**

このユーザ認証方式の場合、トークンまたはスマートカードが必要で、Active Directory 環境の Windows スマートカード・ログオンに使用します。

**共通鍵トークン (iKey 1000)
および PIN**

このユーザ認証方式の場合、プリブート時に共通鍵 (iKey 1000 のみ) が必要となります。プリブート認証の処理後、Windows 認証が必要となります。

注意：iKey 1000 の管理に関する基本的な情報については、169 ページを参照してください。

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 の [Customer Connection Center] Web サイト (<http://c3.safenet-inc.com/secure.asp>) にある最新の ProtectDrive カスタマー・リリース・ノートを参照してください。

ユーザ認証証明情報を間違えたり、忘れた場合

ProtectDrive では、認証証明情報を間違えたユーザにも対応しています。たとえば、ユーザがスマートカードもしくはトークンを無くした場合や、Windows ドメインのパスワードを忘れた場合などがこれに該当します。

ProtectDrive のシステム・ポリシーでは、前述のようなプリブート認証手順を自動的に処理します。

自動プリブート認証後の自動での再ブート

ProtectDrive とは別のさまざまなシステム管理者機能では、多くの場合自動プリブート認証後に自動的に PC を再ブートする必要があります。ProtectDrive では、特殊なユーザ・アカウントを使用してこの機能を実行します。この機能を実行するには、システム・レジストリを変更する必要があります。詳細は、[11 章](#)「自動プリブート認証での自動リブート」を参照してください。

Windows ユーザ認証

シングル・サイン・オン

自動的に Windows のユーザ認証を実行できるように ProtectDrive のシステム・ポリシーを設定できます。ユーザは、プリブート認証の成功後、自動的に自分の Windows ドメインまたはローカルの Windows アカウントへログオンできます。この Windows 認証方式をシングル・サイン・オンといいます。

注意：共通鍵による iKey 1000 でのトークン認証の場合には、シングル・サイン・オンは動作しません。

手動での Windows 認証

シングル・サイン・オンを使用しない場合には、個々の Windows（ドメイン）アカウントに対してユーザを手動で認証後、標準的な Windows 認証画面が表示されるように ProtectDrive のシステム・ポリシーを設定することができます。

Windows 以外の環境におけるシングル・サイン・オン

Windows の場合に限り、シングル・サイン・オンのユーザ認証環境で ProtectDrive を追加設定することなくシームレスに使用できます。

また、シングル・サイン・オン・アシスタント（*C:\Program Files\SafeNet ProtectDrive* にインストールされている）というアプリケーションを使用すれば、Windows 以外を使用するシングル・サイン・オン・ユーザ認証システム環境で、ProtectDrive のシームレスな操作を管理できます。

シングル・サイン・オン・アシスタントの詳細については、[第 6 章](#)「シングル・サイン・オンの管理」を参照してください。

ハードディスクおよびリムーバブル・メディアの暗号化および復号化

データの暗号化処理は、利用者からは見えません（利用者に対して透過的です）。ProtectDrive では、複数の HDD パーティションおよび選択したリムーバブル・メディアを自動的に暗号化および復号化します。（インストール時に作成される）暗号化側のシステム鍵の共有を確認済みのコンピュータは、正しい暗号化パスワードを入力すればリムーバブル・メディアを復号化できます。

暗号化されたデータを読み取る際に、ProtectDrive はそのデータを「オンザフライ」方式で復号化します。つまり、データをすぐに表示することができ、アプリケーションやソフトウェアですぐに使用できるように復号化されます。HDD またはリムーバブル・メディアに書き込まれたデータは、すべて自動的に再暗号化されます。この処理が通常のシステム運用に影響を及ぼすことはありません。

ProtectDrive システムおよびユーザのポリシーの設定

リモート管理

システム・ポリシーは、**ProtectDrive 管理コンソール**によって、ProtectDrive クライアントをリモートで管理することができます。

ProtectDrive の管理者用ツールをインストールするには、Active Directory もしくは ADAM のインストールが必要であり、それぞれのユーザおよびコンピュータの管理（ADUC）から ProtectDrive の管理ができます。ProtectDrive 管理コンソールのインストールは、ProtectDrive のインストールの **セットアップ タイプ** で [管理ツールのインストール] を選択してください。



管理ツールは、クライアントのリモート管理を行うために、管理者によって必要なツールを柔軟にインストールすることができます。（サーバでもワークステーションにでも）

ProtectDrive クライアント毎のユニークな設定オブジェクトを ADUC MMC によって、リモート管理が可能となります。これは、ProtectDrive v8.3 以前の管理方法と何ら変わりません。

ProtectDrive クライアントのグループでは、ProtectDrive 管理スナップインによって同じ設定でリモート管理することができます。いろいろなクライアントのために無制限な数のカスタム設定を作成することができます。新しい設定オブジェクトの作成および追加を ProtectDrive 管理スナップインに行うことができます。クライアントをいつでも設定オブジェクトに追加および削除することが可能です。

ローカル管理

システム・ポリシーは、ProtectDrive のクライアント側コンポーネントのインストールの一環として導入される、ProtectDrive の**ローカル管理コンソール（LMC）** ユーティリティを使用してローカル管理することができます。

LMC では、ProtectDrive をインストール後にローカル設定を行うことができます。クライアントのシステムでのユーザ登録や [PD ユーザ] タブでのデバイス毎のアクセスコントロールの設定を行うことができます。ユーザのポリシーによって、全てのデバイスに対してのユーザ毎の明確なアクセス制限を定義します。

Active Directory もしくは ADAM による集中管理

Active Directory は、ユーザおよびコンピュータを管理するためのほとんどの企業ですでに利用されている管理システムです。ADAM (Active Directory Application Mode) とは、ディレクトリ対応のアプリケーションのさまざまな要求をサポートするための Active Directory の機能です。

Active Directory と ADAM の一番の違いはスキーマを適用する方法です。

- Active Directory と同様に、すべてのドメイン コントローラが同じスキーマを使用します。
- ADAM では、それら自身のスキーマにより複数の ADAM の設定を保持することができます (Active Directory スキーマから完全に独立する)。

Active Directory もしくは ADAM によって、ProtectDrive クライアントを集中管理することができます。

重要なのは、ProtectDrive がアンインストールされても、Active Directory のスキーマ変更が一旦されると、元に戻すことができません。(スキーマの拡張を削除することはできません。) したがって、使用中の Active Directory がアプリケーション特有のスキーマの変更にたいして「変更禁止」であるなら、ADAM を ProtectDrive サーバのために使用するべきです。

Active Directory と ADAM 環境の両方で、Active Directory のユーザとコンピュータ (ADUC) MMC のスナップイン、または、ドメイン・コントローラ (DC) もしくは ADAM サーバ上の ProtectDrive Management 経由でのスナップインによって、コンピュータとユーザのオブジェクトを集中管理することができます。これらのスナップインは、ProtectDrive Administrative Management Tools のインストール中にインストールされます。

ADAM での ProtectDrive の集中管理

ProtectDrive が ADAM で使用されるとき、ProtectDrive パーティション (CD=PDPartition) がある ADAM インスタンスは、Directory Preparation ユーティリティ (PDDirPrep) で実行されるタスクによって、メンバーサーバにインストールされます。このユーティリティに関する詳しい情報については、次のセクションを参照してください。

注意 : ProtectDrive を ADAM で利用する場合には、PDDirPrep を実行する前に、Active Directory サーバ以外のマシンに ADAM をインストールしてください。そして、PDDirPrep は、ProtectDrive Management ツールをインストールする前に、必ず実行してください。

集中管理のための Windows ドメインの準備

Directory Preparation ユーティリティ (PDDirPrep) は、リモートでの ProtectDrive クライアントを管理するために、Windows ドメインの準備を行います。それが必要である場合に、PDDirPrep をインストールすることができます。PDDirPrep では、下記のことが実行できます。

- ProtectDrive ADAM インスタンスを各ドメインで作成してください。
- ProtectDrive のクライアントのシステムとユーザのポリシーを管理するためのプライマリ・ドメイン上で、Active Directory (もしくは ADAM) スキーマを登録してください。
- リモートでのクライアント管理のために、標準設定のオブジェクト作成によって、各ドメインを設定してください。デフォルトで、ドメインにおけるすべての新しいクライアントが ProtectDrive 管理コンソールで、ADUC スナップインによって、自動的に標準の設定オブジェクトにリンクされます。このタスクを実行するためにドメインの管理者としてログインしなければなりません。

Directory Preparation ユーティリティに関する詳細について、41 ページを参照してください。

ProtectDrive の復旧ファイルと鍵管理

ProtectDrive のインストールで復旧ファイルが作成されます。これらのファイルは、障害復旧および緊急ログインで使用されます。また、ProtectDrive のインストール CD 内 (¥tools フォルダ内) の Certificate Wizard ユーティリティを使用することによって、これらのファイルを作成することもできます。復旧ファイルの内容は、以下のとおりです。

- **Master Security Certificate (MSC)** — **PdMaster.cer** と **PdMaster.pfx** ファイルは、公開と秘密鍵ペアで構成されています。**PdMaster.pfx** は、Remote Recovery Console (**rpadmin**) を使用することで、ディスクの鍵リカバリ情報を取り出すために使用されます。**PdMaster.pfx** ファイルは個人に割り当てられ、セキュアな格納および障害復旧を実行することができる個人の特定を可能とします。**PdMaster.cer** は、Master Security Certificate(MSC)の公開鍵であり、各インストールのときに使用されます。
 - **Recovery Support Certificate (RSC)** — **PdRecovery.cer** と **PdRecovery.pfx** ファイルは、公開と秘密鍵ペアで構成されています。**PdRecovery.pfx** は、Remote Recovery Console (**rpadmin**) の緊急ログオンで使用されます。**PdRecovery.pfx** は個人に割り当てられ、セキュアな格納およびパスワード復旧を実行することができる個人 (例えば、ヘルプデスクおよびサポート担当者) の特定を可能とします。**PdRecovery.pfx** は、Recovery Support Certificate (RSC) の公開鍵であり、各インストールのときに使用されます。
 - **Salt** — **salt.cid** ファイルは、ProtectDrive がインストールされた PC の間のリムーバブル・メディアの共有を可能にするために使用されます。ProtectDrive の以前のバージョンからアップグレードする場合に、**syskey.bin** か **syskey.cid** ファイル(存在する場合)が、アップグレードで、**salt.cid** ファイルを作成するために使用されます。アップグレードに関する基本的な情報については、[第 5 章](#) — 「以前のバージョンの ProtectDrive からのアップデート」を参照してください。
-

- 復旧エンベロープ — **RecoveryEnvelope.env** ファイルは、緊急ログオンで **Remote Recovery Console (rpadmin)** ユーティリティを使用するために、全てのクライアント PC に作成されます。クライアント名は、以下のファイル名に含まれています。
<computer name>_RecoveryEnvelope.env

ProtectDrive の障害復旧

障害復旧の準備として、まず定期的に ProtectDrive システム・データのバックアップを実行します。ProtectDrive のバックアップ・ユーティリティにより、**リカバリ・ファイル**が作成されます。以降の破損したシステムの復号化にはこのファイルを使用します。これらのファイルはクライアント・システム以外の場所に保存する必要があります。バックアップ・ユーティリティによって作成されるバックアップ・ファイルは、ディスク鍵の復旧を実行するのに **Master Security Certificate(MSC)**によって使用されます。

注意： ProtectDrive v8.3 以降では、Active Directory からバックアップ復旧ファイル入手することができる場合には、定期的なバックアップは、リモート管理された ProtectDrive クライアントに必要ではありません。

また、ProtectDrive には、データの復号化やプリブート・ユーザ・データベースの管理など、障害復旧作業を実行するための、一連のコマンド・ラインによる復旧ツールがあります。これらの復旧ツールは ProtectDrive の配布 CD に収録されています。また、通常これらのツールを使用するのはシステム管理者のみです。詳細について [第 12 章](#) — 「障害復旧ツール」を参照してください。

ProtectDrive のライセンス

ProtectDrive のライセンスには、ディスク暗号化、リムーバブル・メディア、および Active Directory や ADAM 管理を起動するためのライセンスコードで構成されています。通常、ProtectDrive は、この機能ごとのライセンスと共に販売されます。ProtectDrive の全ての機能をインストールするためには、ライセンスコードまたは認可コードが必要となります。さもないければ、評価目的のために ProtectDrive を 30 日の試用版としてインストールすることができます。ProtectDrive ライセンスを購入するとき、ライセンス・ファイルを証明ファイル（テキスト形式）として受け取ります。

ProtectDrive をインストールする前に、インストール中に参照可能なフォルダにコピーするか、サイレントもしくは GPO インストールのために、**license.txt**、または **authorization.txt** ファイル（ファイル名を変えず）を **SafeNet ProtectDrive.msi** ファイルと同じディレクトリにコピーしてください。

ライセンスの期間が切れたなら、ライセンスの期間が切れた後に定期的に表示するライセンス・マネージャが表示する画面でライセンスをアップデートしてください。その他の詳細について 99 ページを参照してください。

License.txt のインストール

ProtectDrive のインストールの中に、.txt のライセンス・ファイルを参照して、ライセンスをインストールしてください。ProtectDrive のクライアントのインストールのための詳細な手順については、[第 5 章](#)—「クライアント・コンポーネントのインストール」を参照してください。サイレントおよび GPO インストールにおいて、ファイル (**license.txt**) を、**SafeNet ProtectDrive.msi** ファイルと同じディレクトリにコピーしなければなりません。適切なライセンス・ファイルがインストール中に、参照可能な場所に存在することを確認してください。

Authorization.txt のインストール

authorization.txt ファイルは、設定で使用されます。クライアント PC に完全なインストールを行うためには、インターネット・アクセスが必要となります。クライアントのファイアウォールは、ポート **80** もしくは **5094** 上でのインターネットへのアクセスを許可する必要があります。インターネット・アクセスができない場合には、次の章を参照してください。

ProtectDrive インストール中に、.txt の認可ファイルを参照してください。サイレントおよび GPO インストールにおいて、ファイル (**authorization.txt**) は **SafeNet ProtectDrive.msi** ファイルと同じディレクトリに存在する必要があります。SafeNet(または、販売店)サーバは、インターネット経由で、自動的にライセンスの承認を行います。認証コードがサーバに送信された時、ライセンスはクライアントに確かに付与されます。そして、クライアントのインストールが継続可能となります。同時に、顧客のライセンスカウントはライセンス・サーバから 1 つ減少します。

クライアント・ライセンスを全て使用すると、サーバはクライアントに対してこれ以上のライセンスの使用を拒否します。そして、メッセージが表示されインストールができないことを通知します。追加ライセンスを必要とするなら、販売代理店に連絡してください。

ProtectDrive クライアントのインストールのための詳細な手順については、[第 5 章](#)—「クライアント・コンポーネントのインストール」を参照してください。

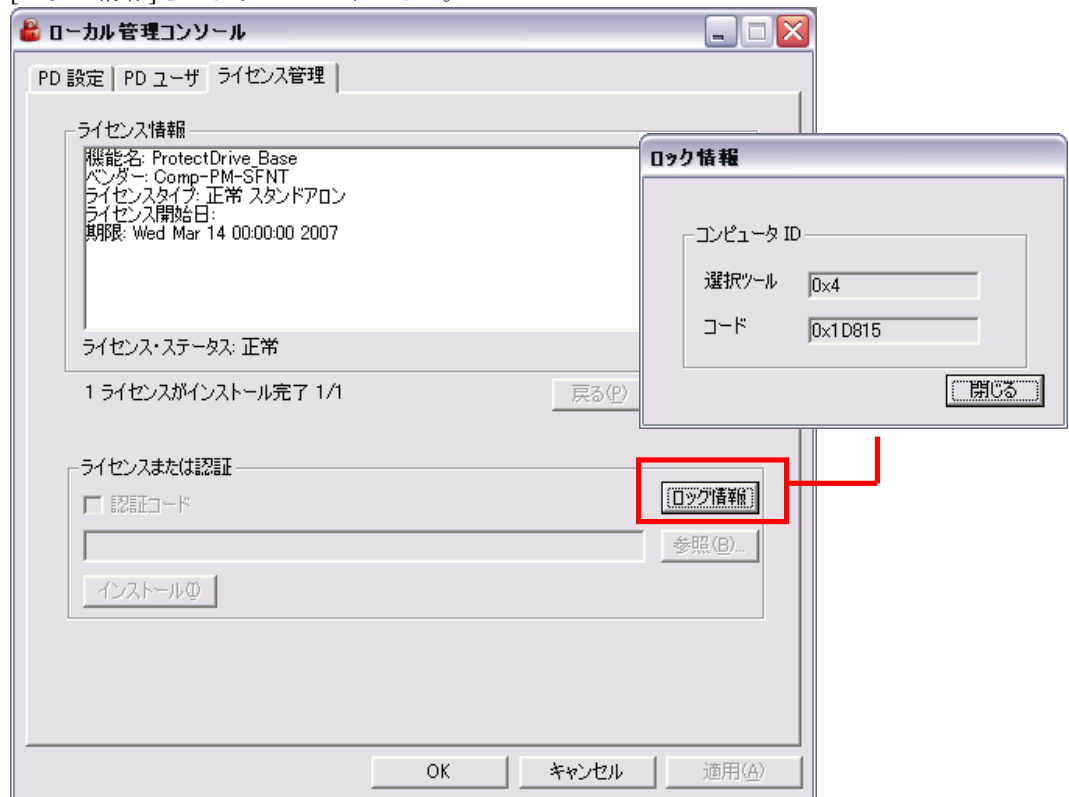
インターネット・アクセスができない場合の対応方法

複数のライセンスの認証を行うもしくは、インターネット・アクセスができない場合には、30 日間の試用バージョンのみがインストール可能です。試用版のインストール後でも、ライセンスを取得すれば、完全なライセンスを保持する ProtectDrive をインストールすることが可能です。

インターネット接続なしでロックされたライセンスを取得するには、SafeNet もしくは販売店のサポート担当に連絡してください。ライセンスを発行するために以下の手順で、必要な情報を取得します。

1. クライアントのローカル管理コンソールを起動してください。
 2. [ライセンス管理]をクリックしてください。
-

3. [ロック情報]をクリックしてください。



4. ロック情報の内容をサポート担当へ連絡してください。
5. サポート担当および SafeNet でライセンスを生成して、**license.txt** でメールなどで送付します。このファイルによって、ProtectDrive クライアントを完全にインストールすることが可能となります。かならず、このファイルをインストール中に参照できる場所にコピーしてください。

完全なインストールをするための手順は、「フルライセンスへのアップグレード」を参照してください。

第3章 システム要件

ハードウェア最小要件

- 32 ビット Intel 互換 CPU を持つコンピュータ・システム
- オペレーティング・システムが実行できるメモリと 30MB の空きディスク・スペース
- CD-ROM ドライブまたはサーバベースのインストール・ディレクトリへのアクセス
- 2TB 以下の HDD
- 80 もしくは 5094 ポートでインターネットにアクセス可能なクライアントのファイアウォールの設定

サポートされるストレージ・ハードウェア

ProtectDrive では、IDE/EIDE、SATA、SCSI ドライブ、RAID アレイなど、ドライブ文字が割り当てられた固定（非リムーバブル）のシステム HDD パーティション、およびリムーバブル・メディア（USB フラッシュ・ドライブや外部ハードディスクなど）を暗号化および復号化できます（隠しパーティションはサポートされていません）。ソフトウェア RAID は、サポートしていません。

ProtectDrive は、次の場合を除き、ストレージ・サブシステムの通常の動作に影響することはありません。

- システム HDD 上のパーティションはフォーマットできません。
- ProtectDrive をインストール後のハードディスクの追加、削除、または交換がサポートされていません。
- インストール中、すべてのパーティションの ProtectDrive アカウントがシステム上にあります。インストール後のパーティション・サイズの変更、変換、マスキングの有効化、またはパーティションの再作成はサポートされていません。マスター・ブート・レコードの操作もサポートされていません。

デバイスのアクセス制御

ProtectDrive のシステム・ポリシーおよびユーザ・ポリシーの管理コンソールでは、構成可能なデフォルトおよび個々のユーザに対する、リムーバブル・メディア、フロッピー、CD-ROM などのデバイスへのアクセス権を定義します。

フロッピーディスク・ドライブ、CD-RW、DVD-RW などのリムーバブル・デバイス、および Iomega 社製の Zip ドライブは、暗号化および復号化の対象から除外されています。ProtectDrive は、これらのデバイスの通常の動作には影響しませんが、これらのデバイスに対する多くの構成可能なユーザの読み取りおよび書き込み特権を制御します。

サポートされるオペレーティング・システム

ProtectDrive では、以下のオペレーティング・システムをサポートしています。

クライアント管理の場合

- Microsoft Windows Server 2003 R2, Service Pack 2 (ProtectDrive サーバのみ、ProtectDrive クライアントのみ、またはクライアントおよびサーバの両方のコンポーネントがサポートされています)。
- Microsoft Windows Server 2003, Service Pack 2
- Microsoft Windows 2000 Advanced Server, Service Pack 4
- Microsoft Windows 2000 Server, Service Pack 4

クライアントの場合

- Microsoft Windows XP Professional, Service Pack 3 (64 ビット版はサポートされていません)
- Microsoft Windows XP Home, Service Pack 3 - 以下を参照してください。
 - XP Home ではローカル・パスワードのみが許可されています。
 - XP Home コンピュータはドメインに参加できません。
 - ProtectDrive では、すべての XP Home アカウントにログオン・パスワードを要求するよう設定する必要があります。
- Microsoft Windows Vista, Service Pack 1

ProtectDrive でサポートされるファイル・システムは、FAT16、FAT32 と NTFS です。

MS-DOS は ProtectDrive の障害復旧中に使用できます。アクセス不可能または破損した ProtectDrive のシステムは、フロッピーディスクまたは CD-ROM から MS-DOS の起動が可能です。特殊な DOS ドライバ (SCSI など) を必要とするドライブ、または TSR は、それぞれのドライブをロードすると、ProtectDrive の復旧ツールのみにアクセスできます。

サポートされるネットワーク

ProtectDrive は、Active Directory に対応していて、Windows ドメインを完全にサポートしています。リモート・デスクトップ接続などの Windows ネットワーク・サービスの通常の動作に影響することはありません。Windows ドメインおよびローカルの Windows ユーザは、ProtectDrive により保護されたシステムを問題なく認証できます。ProtectDrive により暗号化されたすべてのハードディスクのパーティションは、システム管理者の権限で共有ボリュームとして設定できます。

第4章

ProtectDrive ソフトウェアの互換性

ProtectDrive は、Microsoft Windows 互換ソフトウェア、アプリケーション、サービス、およびユーティリティの通常の動作に影響しないことを確認済みです。ただし、以下を使用する場合は注意が必要な場合があります。

DOS ドライブおよび TSR

DOS フロッピー（または CD）から起動する場合は、適切なドライバのロード後に、ProtectDrive が DOS ドライバおよび TSR からハードディスクにアクセスできるかどうか確認します。

Windows およびサードパーティ製のブート・マネージャ

システムのブート時に、ProtectDrive ではマスター・ブート・レコード（MBR）を操作して完全性を確認します。固有の目的で MBR の操作が必要なソフトウェアは、すべて ProtectDrive との互換性がありません。標準の Windows ブート・マネージャの場合も同様です。

Windows のディスク・マネージャ・ユーティリティ

ProtectDrive インストール後のディスク・パーティションの再作成、サイズ変更、およびミラー構成の変更は、すべて禁止されています。これらの操作が必要な場合は、操作を進める前にすべてのディスクを復号化して ProtectDrive をアンインストールしてください。

Windows のフォルダ圧縮ユーティリティ

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・ファイルのディレクトリ（C:\SecurDisk）は圧縮できません。

圧縮済みのシステム・ドライブに ProtectDrive をインストールすることはできません。結果的に C:\SecurDisk が圧縮されることとなり、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。

Windows システム復旧ユーティリティ

ProtectDrive のインストール前に作成された Windows のシステム復旧ポイントは使用できなくなります。システムの復旧は、ProtectDrive のインストール後の復旧ポイントに限られます。

Windows 高速ユーザ切り替えユーティリティ

ProtectDrive では、標準的な Windows の初期画面とユーザ切り替えの機能が無効になっています。

第5章

ProtectDrive のインストール

作業を開始する前に

ProtectDrive をインストールする前に、必ず下記の内容を確認してください。ユーザは、ProtectDrive のインストールや設定を行う管理者特権を持っている必要があります。

インストール前に

インストール前に下記を実行してください。

- ProtectDrive で暗号化するディスクの最適化 (Deflag の実行)
- ディスクのチェック

付属のハードディスクの検査ツールなどを使用して、ディスクを必ず確認してください。

ストレージ・システムの準備

ProtectDrive を導入する前に、次の手順を実行してください。

- データ・ストレージ・システムの計画が整っていること、およびパーティションの再編成が発生しないことを確認します。必要に応じて Windows の [ディスクの管理] を使用して、パーティションの再作成、ディスク・ミラーリングの設定、パーティションのサイズ変更などを行います。
- ハードディスク製造元の診断ユーティリティ **CHKDSK /f** を実行して、暗号化するすべてのドライブのファイル・システムの状態が安定していることを確認します。不正なセクタがある場合は、ProtectDrive で暗号化できるように修正します。
- 重要なデータはすべてディスクを暗号化する前にバックアップしてください。

リカバリ・ディスクの準備

SafeNet では、ProtectDrive の復旧ツールおよびリカバリ・キーなどが格納されたリカバリ・ディスク (フロッピーまたは CD) を準備することをお勧めします。このディスクは次の場合に必要となります。

- ProtectDrive の障害復旧ツール
- プリブート・パスワードの復旧手順

ProtectDrive をシステムへインストール後、次の手順を実行してリカバリ・ディスクを作成してください。

1. **PdMaster.pfx**、**PdRecovery.pfx**、**salt.cid**、および **<computer name>_RecoveryEnvelope.env** ファイルをフロッピーへコピーしてください (これらのファイルはインストール中に作成されます)。

2. `Tools` ディレクトリ (ProtectDrive の復旧ツール) の内容を ProtectDrive のインストール CD から先ほどのフロッピーへコピーしてください。
3. 別のフロッピー (または CD) に EFS リカバリ・ファイル (`backup.exe` を実行すると作成される) をコピーしてください。これらのファイルはサードパーティ製のディスク鍵の復旧に必要となります。この復旧手順の詳細については、130 ページを参照してください。

セクタ 0 のバックアップ (リムーバブル・メディアのみ)

リムーバブル・メディア・デバイスに障害が発生するなど、極端な場合は、ProtectDrive の `rmmbr` コマンドまたは修復手順を実行しても、デバイスを再利用可能な状態に戻すことができない場合があります。このような現象が発生した場合、セクタ 0 のデータをデバイスに復旧する必要があります。

この復旧手順の詳細については、[第 11 章](#) — 「例外的な認証のシナリオ」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 データは、実際に必要となる前に常にバックアップを作成しておいてください。デバイスに障害が発生したときにセクタ 0 のバックアップがない場合、復旧手順を実行できず、リムーバブル・メディア・デバイスを使用できなくなります。

この手順は、導入中の 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. ProtectDrive がインストールされていないコンピュータに USB フラッシュ・ドライブを挿入し、デバイスのドライブが読み取り可能なドライブとして表示されることを確認してください。
2. `dskprobe.exe` ユーティリティを実行してください (このユーティリティは、Microsoft Windows 2000 リソース・キットに収録されています。リソース・キットはインターネットからダウンロードできます)。
3. [ドライブ] > [物理ドライブ] の順に選択してください。
4. リスト中の最後のドライブをダブルクリックしてください。このドライブは通常 USB フラッシュ・ドライブです。このドライブは、画面下の [ハンドル 0] に表示されます。
5. このドライブで [アクティブに設定] を選択して [OK] をクリックしてください。
6. デフォルトの設定は変更しないでください。[セクタ] > [読み取り] の順に選択してから [読み取り] をクリックしてください。セクタ 0 のデータが表示されます。
7. [ファイル] > [名前をつけて保存] の順に選択してください。保護されたハードディスクまたはネットワーク・ドライブなど、保護された場所を選択してください。データの保存場所となるデバイスを明確に識別できるファイル名を指定してください。

カスタムの鍵セットの作成

Certificate Wizard ユーティリティ (`certwizardapp.exe`) は、カスタム復旧鍵ペアを作成する必要がある場合に使用します。Certificate Wizard ユーティリティでのカスタム復旧鍵ペアを作成するための情報は以下のとおりです。

- **Master Security Certificate (MSC)** — **PdMaster.pfx** と **PdMaster.cer** は、Remote Recovery Console (**rpadmin**) を使用することで、ディスクの鍵リカバリ情報を取り出すために使用されます。これらの証明書は、障害復旧を実行することができる個人の特定を可能とします。
- **Recovery Support Certificate (RSC)** — **PdRecovery.pfx** と **PdRecovery.cer** は、Remote Recovery Console (**rpadmin**) の緊急ログオンで使用されます。これらの証明書は、パスワード復旧を実行することができる個人（例えば、ヘルプデスクおよびサポート担当者）の特定を可能とします。
- **Salt** — このファイルは、ProtectDrive がインストールされた PC 間でのリムーバブル・メディアの共有を可能にするために使用されます。

ProtectDrive の v8.2 以前のバージョンからアップグレードする場合には、**salt.cid** は作成しないでください。**syskey.bin** か **syskey.cid** ファイル(存在する場合)が、アップグレードで **salt.cid** ファイルを作成するために使用されます。アップグレードに関する基本的な情報については、54 ページを参照してください。

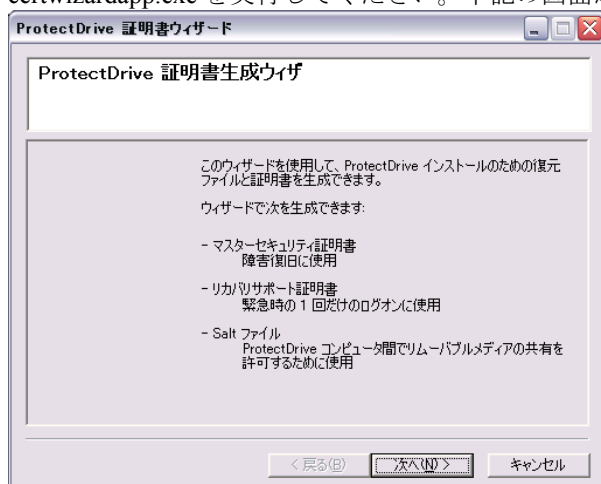
既に ProtectDrive をインストール済で、カスタム復旧鍵ペアを作成する場合には、既存の PdMaster、PdRecovery、および salt ファイルを別の場所に保存してください。さもなければ、これらのファイルは上書きされます。別の場所に、これらのファイルを保存してから、Certificate Wizard ユーティリティを実行してください。

まだ ProtectDrive をインストールしていなくて、インストールでカスタム復旧鍵ペアを使用したい場合には、ProtectDrive をインストールする前に Certificate Wizard 手順に従ってください。

Certificate Wizard ユーティリティは、ProtectDrive 配布 CD-ROM の *Tools* ディレクトリにあります。

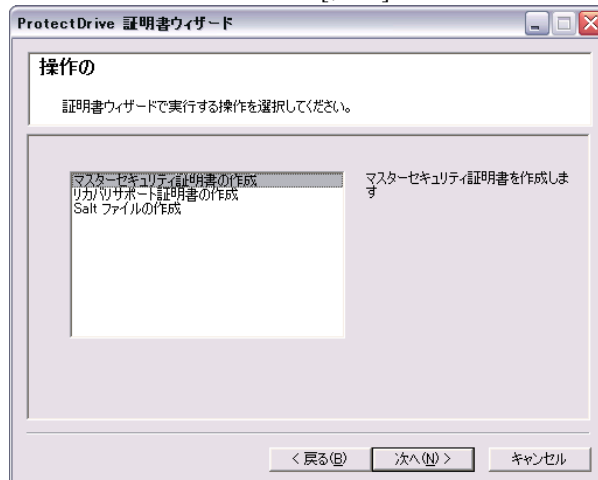
Certificate Wizard の利用方法

1. certwizardapp.exe を実行してください。下記の画面が表示されます。



2. [次へ]をクリックしてください。

3. 実行する内容を選択して、[次へ]をクリックしてください。

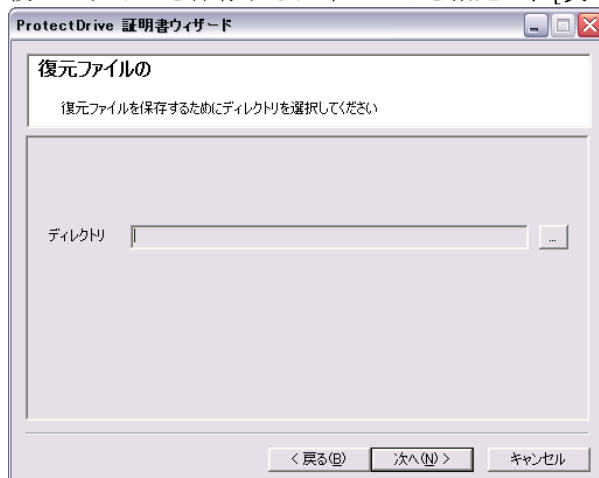


4. もし、Salt ファイルを作成する場合には、5 へスキップしてください。マスター・セキュリティ証明書およびリカバリサポート証明書を作成する場合には、下記の手順を参照してください。

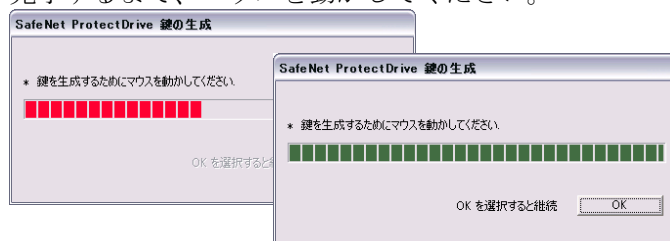


- パスワードで保護された秘密鍵を作成するために、**PFX ファイル** オプションを選択し、適切なパスワードを入力してください。そして、[次へ]をクリックしてください。
- トークンもしくはスマートカードで秘密鍵を作成する場合には、**トークン/スマートカード** を選択し、リストから CSP のプロバイダ名（利用するトークンやスマートカードによって異なる）を選択してください。そして、[次へ]をクリックしてください。

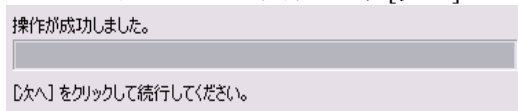
5. 復旧ファイルを保存するディレクトリを指定し、[次へ]をクリックしてください。



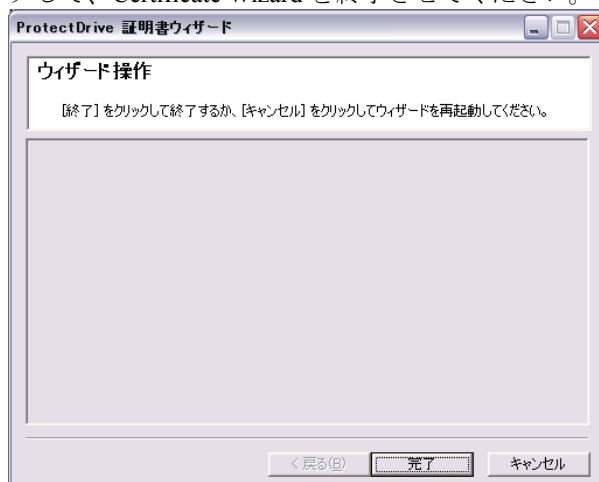
- Salt ファイルの作成の場合には、乱数生成によって復旧ファイルを作成します。完了するまで、マウスを動かしてください。



- MSC もしくは RSC の場合には、復旧ファイルの作成が完了し、下記のメッセージが表示された場合には、[次へ]をクリックしてください。



6. 証明書および Salt ファイルの作成が完了すると下記の画面が表示されます。[完了]をクリックして、Certificate Wizard を終了させてください。



7. 最後にそれぞれ作成したファイルを確認してください。

名前 ▲	サイズ	種類
PdMaster.cer	1 KB	セキュリティ証明書
PdMaster.pfx	2 KB	Personal Informatio...
PdRecovery.cer	1 KB	セキュリティ証明書
PdRecovery.pfx	2 KB	Personal Informatio...
salt.cid	1 KB	CID ファイル

未使用の ADAM サービス・コネクション・ポイント (SCPs) の手動削除

Active Directory 環境で、Active Directory Application Mode (ADAM) は、Active Directory における ADAM サービス情報を公開するのに、サービス・コネクション・ポイント (SCP) を使用します。

SCP は、サービス(ADAM インスタンスなどの)に関する情報を含む Active Directory でのポイントです。そのサービスがどこにあり、どのように接続するかを含んでいます。

ProtectDrive が正しい ADAM インスタンスの場所を見つけるために SCP は重要です。

ADAM インスタンスがコンピュータから取り除かれるとき、ADAM インスタンスは Active Directory からその SCP を削除します。しかしながら、SCP の削除に失敗した場合には、クライアント・アプリケーションは実在しない ADAM インスタンスに関連付けされているかもしれません。

SCP が削除されないいくつかの理由があります。それは、Active Directory がアンインストールできないことや、SCP が手動で作成された場合です。

新しい ProtectDrive ADAM インスタンス作成が可能になる前、もしくは ProtectDrive が Active Directory に情報を格納する前に、SCP を削除しなければなりません。23 ページの手順は、ADAM SCP を削除するために ADSIEdit ユーティリティが必要となります。ネットワーク管理者は、Active Directory の参照および変更をこのユーティリティを使用して実行することができます。ADSIEdit の特徴は、Active Directory のユーザとコンピュータ(ADUC) MMC スナップインですが、ADSIEdit は Active Directory 情報の低レベルの情報も参照可能です。

ADSIEdit ユーティリティは、Windows 2003 サポートツールとして、CD からインストールすることが可能です。もしくは、Microsoft ダウンロード・センター

<http://go.microsoft.com/fwlink/?LinkId=100114> よりダウンロードすることも可能です。

詳細は、<http://technet2.microsoft.com/windowsserver/en/library/007fdeec-81f2-4b6c-b715-bee54c0d5deb1033.mspx?mfr=true> の Administering ADAM service publication を参照してください。

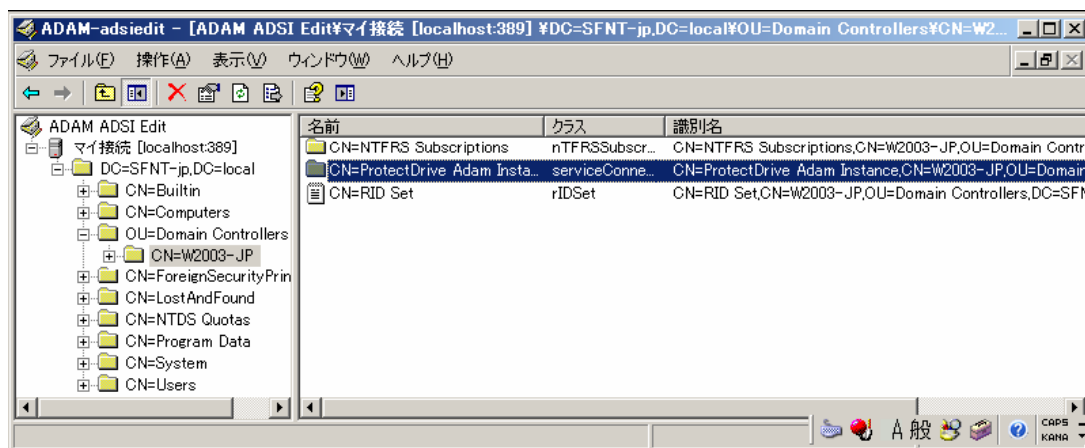
ADAM インスタンスの削除

1. Windows のスタート・メニューから、“プログラム追加／削除”を起動してください。
2. “ADAM Instance ProtectDrive”を選択して、[削除]をクリックしてください。

ADAM SCP の削除

ADAM インスタンスを削除する場合に、SCP も必ず Active Directory から削除しなければなりません。SCP の削除が失敗した場合には、下記の手順で削除してください。

1. プログラムのメニューの ADAM フォルダ内の ADSIEdit を起動してください。
2. 利用中の Active Directory に接続し、ADAM インスタンス内のコンピュータ・オブジェクトを参照してください。



その他のいくつかのオブジェクトが ServiceConnectionPoint クラスに存在します。(上記の画面では、二つ存在します。)

3. オブジェクトを選択し、右クリックし、[プロパティ]を選択してください。そして、属性を選択し、[編集]をクリックしてください。
 - ADAM ADSI 編集画面で、ProtectDrive 値が属性に表示されたなら、それは ProtectDrive ADAM インスタンスのための SCP です。ステップ 4 に進んでください。
 - ADAM ADSI 編集画面で、ProtectDrive 値が属性に表示されなかったなら、それは他のサービスのための SCP です。削除も修正もせず、終了してください。



4. ProtectDrive の SCP を修正後、画面を終了させてください。
5. “ADAM ADSI 編集” で削除する ProtectDrive SCP を選択し、[削除]をクリックしてください。
6. 確認メッセージで[はい]をクリックすると、削除が完了します。

ADAM のための Windows Firewall の設定

ProtectDrive をインストールするサーバおよびクライアントは、セキュリティ強化のために Windows の Firewall を有効にしておくべきです。ADAM によってクライアントのアップグレードを実行するためには、ポート 50000 へのトラフィックを許可するように Windows の Firewall を設定してください。

サーバでの設定

1. コントロール・パネルを開いてください。
2. “セキュリティ センター”を選択して、“Windows ファイアウォール”をクリックしてください。
3. [例外]のタブをクリックしてください。
4. [ポートの追加]をクリックしてください。
5. “名前” にサーバ名を入力してください。
6. “ポート番号” に ADAM のインスタンス作成時に指定したポート番号を入力してください。
7. [OK]をクリックしてください。

クライアントでの設定

1. コントロール・パネルを開いてください。
2. “セキュリティ センター”を選択して、“Windows ファイアウォール”をクリックしてください。
3. [例外]のタブをクリックしてください。
4. [プログラムの追加]をクリックしてください。
5. *C:\Program Files\SafeNet ProtectDrive* を参照してください。
6. **ClientDM** を選択して、[開く]をクリックしてください。
7. [OK]をクリックしてください。

ProtectDrive のインストール（MSI）パッケージ

ProtectDrive は Windows インストーラ（MSI）パッケージを使用して導入します。以下のファイルは、ProtectDrive のサーバ側およびクライアント側コンポーネントのインストールに使用します。

名前 ▲	サイズ	種類	更新日時
Tools		ファイル フォルダ	2008/08/13 18:20
1031.mst (ドイツ語)	99 KB	MST ファイル	2008/08/13 11:38
1033.mst (英語語)	4 KB	MST ファイル	2008/08/13 11:38
1041.mst (日本語)	98 KB	MST ファイル	2008/08/13 11:38
pd_administration_guide.pdf	3,252 KB	Adobe Acrobat Doc...	2008/05/08 2:19
PD_Release_Note_v8 5 0_revC_J.pdf	193 KB	Adobe Acrobat Doc...	2008/12/05 21:29
pd_user_manual.pdf	1,043 KB	Adobe Acrobat Doc...	2008/05/08 2:08
SafeNet ProtectDrive.msi	27,492 KB	Windows インストーラ...	2008/08/13 11:38
Setup.exe	56 KB	アプリケーション	2008/08/13 11:23

また、**SafeNet ProtectDrive.msi** を自動的に起動するための Active Directory のグループ・ポリシー・オブジェクト（GPO）を、複数のクライアント・システムに対して ProtectDrive のネットワーク・ロールアウトを実行するよう設定（カスタマイズ）できます。

ProtectDrive バージョン 8.3 以降では、**ProtectDrive Management Console Configuration Objects** を通してインストールをカスタマイズすることが可能です。

注意：Windows Vista クライアント上で ProtectDrive をインストールする場合は、**SafeNet ProtectDrive.msi** の代わりに **setup.exe** を実行してください。

MSI パッケージのカスタマイズ

（GPO の導入など）自動インストールを行う場合、システム管理者は、インストール中にユーザとの対話が不要になるよう、すべてのパラメータをプロパティ画面で設定する必要があります。そのために、MSI パッケージを変更します。

MSI はデータベース・テーブルの一種で、システム管理者が必要に応じて **SafeNet ProtectDrive.msi** を調整またはカスタマイズできます。MSI パッケージのカスタマイズが可能なツールは、さまざまなものが公開されています。

たとえば、Microsoft からは Orca という無償のデータベース・エディタが提供されています。Orca の詳細については、次の Web サイトを参照してください。

<http://support.microsoft.com/kb/255905/EN-US/>

ProtectDrive MSI の設定

以下の説明では、ProtectDrive のインストールを変更するための MSI の設定を説明します。

ERA_CLIENT_CONFIGURATION_ONLY	このプロパティは、インストールするクライアント構成の種類を定義します。(1) に設定すると、 ローカル管理コンソール 経由でクライアントをローカルに構成します（これにより、Active Directory および ADAM の更新が無効になります）。(0) に設定すると、サーバ上の Active Directory 経由でクライアントを導入します（これにより、 ローカル管理コンソール 経由のローカル変更が無効になります）。
ERA_CONFIG_FILE_IMPORT_FLAGS	このプロパティは、インストール中に XML ファイルを読み込むかを指定します。 (1) を設定すると ERA_CONFIG_FILE_XML_PATH で指定したパスのファイルからユーザのみをインポートします。 (2) を設定すると ERA_CONFIG_FILE_XML_PATH で指定したパスのファイルからデータのみをインポートします。 (3) を設定すると ERA_CONFIG_FILE_XML_PATH で指定したパスのファイルからユーザとデータをインポートします。
ERA_CONFIG_FILE_XML_PATH	このプロパティは、ProtectDrive クライアントの設定のための.xml ファイルの絶対パスを指定します。このファイルは同じ salt.cid を共有する各クライアントでインポートすることができます。 ProtectDrive のインストールでは、SafeNet ProtectDrive.msi が存在するフォルダで.xml ファイルを検索します。クライアント設定の.xml ファイルをインポートする際に、詳細な情報が必要な場合には、63 ページを参照してください。
ERA_ENCRYPT_USE_FIPS	このプロパティを (1) に設定すると、デフォルトで FIPS 認定の暗号方式が使用されます。(0) に設定すると CC EVAL-2 認定ですが、FIPS 未認定の暗号方式が使用されます。
ERA_INSTALL_AD_COMPOBJ_SNAPIN	このプロパティはデフォルトで (0) に設定されています。(1) に設定すると、Active Directory もしくは ADAM の [コンピュータ・オブジェクト] スナップインがインストールされます。
ERA_INSTALL_AD_USEROBJ_SNAPIN	このプロパティはデフォルトで (0) に設定されています。(1) に設定すると、Active Directory もしくは ADAM の [ユーザ・オブジェクト] スナップインがインストールされます。

ERA_INSTALL_ADMIN_GUIDE

このプロパティはデフォルトで (0) に設定されています。『ProtectDrive 管理者ガイド』をインストールする場合は (1) に設定します。このファイルをインストールするには、ファイルが MSI パッケージと同じディレクトリに存在している必要があります。

ERA_INSTALL_CLIENT

このプロパティはデフォルトで (1) に設定されています。(0) に設定すると、クライアント側コンポーネントがインストールされません。

ERA_INSTALL_LOCAL_MC を (1) に設定すると、このパラメータも自動的に (1) に設定されます。

ERA_INSTALL_KEY_RECOVERY

このプロパティはデフォルトで (0) に設定されています。(1) に設定すると、**rpadmin.exe** がインストールされます。

追加情報については、第 11 章 - 例外的な認証のシナリオを参照してください。

ERA_INSTALL_LOCAL_MC

このプロパティはデフォルトで (1) に設定されています。(0) に設定すると、**ローカル管理コンソール・ユーティリティ**がインストールされません。

ERA_INSTALL_USER_MANUAL

このプロパティはデフォルトで (1) に設定されています。(0) に設定すると、『ProtectDrive ユーザ・マニュアル』がインストールされません。このファイルをインストールするには、ファイルが MSI パッケージと同じディレクトリに存在している必要があります。

ERA_KM_REC_FILE_FOLDER_PATH

このプロパティは復旧ファイルセットを含む復旧ファイルのパス (相対、フルもしくはネットワークパス)を定義します。デフォルトの復旧ファイルセットのパスは、ソースディレクトリ (**SafeNet ProtectDrive.msi** ファイルが起動される) です。

ERA_LANGUAGE_CHOICE

このプロパティでは、ラベルおよびテキスト・メッセージに使用する言語が定義されます。オペレーティング・システムの言語はデフォルトで (0) に設定されています。その他の設定は、以下のとおりです。

(1) 英語、(2) ドイツ語、(3) 日本語

ERA_LICENSE_PATH_OR_CODE

このプロパティは、デフォルトで **SafeNet ProtectDrive.msi** ファイル内には存在しません。

このプロパティは、ProtectDrive ライセンス・ファイル、または完全なライセンスコード (license.txt ファイルから読み込まれる) を含むライセンスパス (相対、フルもしくはネットワークパス) を定義します。デフォルトのライセンスファイルパスは、ソースディレクトリ (**SafeNet ProtectDrive.msi** ファイルが実行される) です。

また、authorization.txt が存在する場合には、license.txt を先に読み込みます。そして、ERA_AUTH_PATH_OR_CODE のプロパティを使用してください。どちらのファイルも存在しない場合には、試用ライセンスがインストールされます。

ERA_AUTH_PATH_OR_CODE と
ERA_LICENSE_PATH_OR_CODE は同時に定義され、
ERA_AUTH_PATH_OR_CODE が優先されます。

ERA_NO_NETBSD

このプロパティは、16bit プリブートのインストールもしくはアップグレードを有効にします。(32bit プリブートのインストールが標準設定です。) もし、旧 16bit モードでのインストールを実行する場合には、(1) を設定してください。(1) を設定した場合には、**ERA_VROM_READERS_SET** にも必ず、設定してください。

注意：32bit プリブートで既にインストールされている場合に、16bit でのプリブートに変更したい場合には、パソコンを起動直後に[Shift]を押し続けてください。16bit のプリブート画面が表示されます。

ERA_SETUP_TYPE

このプロパティに “**Client**” を設定すると、クライアントのインストールが実行されます。“**Server**” を設定すると管理ツール (PDDirPrep、snap-ins、Remote Recovery Console など) がインストールされます。

ERA_VROM_READERS_SET

このプロパティは、プリブート認証でサポートされる読取装置を定義します。このプロパティでは、デフォルトで “**INTERNAL**” に設定されます。“**PCMCIA**” に設定した場合には、PCMCIA をサポートする読取装置をインストールしてください。

管理者ツールのインストール

ProtectDrive のインストールの変更に関して

ProtectDrive バージョン 8.3 以前のバージョンでは、“サーバ・コンポーネントのインストール”が含まれていました。“サーバ・コンポーネントのインストール”では、スキーマの拡張とサーバの設定が、同じサーバにインストールされます。

バージョン 8.3 以降では、“サーバ・コンポーネントのインストール”は、“管理ツールのインストール”に変更となりました。

管理ツールとは、ProtectDrive をサーバより管理するためのツールです。このツールは、どのサーバにインストールすることも可能です。

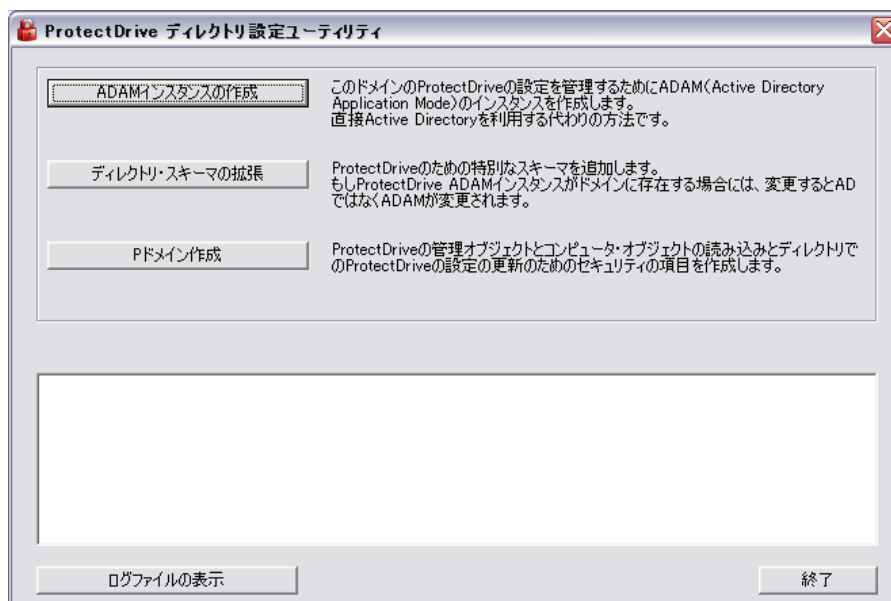
管理ツールは、ProtectDrive クライアントを集中管理する場合に必要となり、鍵の復旧、緊急パスワードの発行などが可能となります。詳細は、35 ページをご確認ください。

注意：ProtectDrive クライアントのインストールは、変更されていません。詳細は、40 ページをご確認ください。

Windows ドメインの準備

Directory 準備ユーティリティ（**PDDirPrep**）によって、ProtectDrive のための Windows ドメインを準備できます。**PDDirPrep** は、ADAM インスタンスを作成するために使用し、Active Directory もしくは ADAM インスタンスのスキーマを拡張し、ProtectDrive クライアントをリモートから管理する準備を行います。

ProtectDrive 管理ツールをインストールする前に、PDDirPrep を実行し準備することをお勧めします。PDDirPrep を使用してドメインを設定するまで、オブジェクトが見つからないなどのエラーを管理ツールは表示します。



PDDirPrep の実行は、1つのフォレストもしくは1つのドメインで一回のみの実行が必要です。しかしながら、何度実行しても問題はありません。変更は、単純に全てのデータを変更するのみです。

以下のように **PDDirPrep** の実行方法は複数あります。

- ProtectDrive のインストール CD の **Tools** フォルダ内の **PDDirPrep.exe** をダブルクリックして起動することができます。
- ProtectDrive の管理ツールをインストールして、起動することができます。
 - ProtectDrive のインストールの最後で“**ディレクトリ標準ユーティリティの起動**”を選択すると、インストール終了後に起動することができます。
 - Windows のスタートメニューから、プログラムの **SafeNet ProtectDrive** フォルダ内の“**Directory Preparation Utility**”から起動することができます。

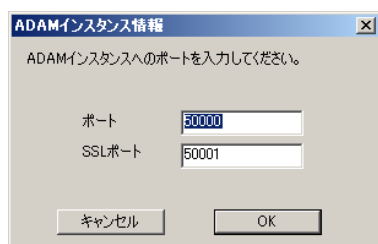
PDDirPrep は、4つの段階で処理を実行します。それぞれの処理が完了すると表示がクリアされ、順番に実行されます。

PDDirPrep の処理が完了後、ProtectDrive の管理ツールをインストールしてください。詳細は、33 ページを参照してください。

ADAM インスタンスの作成

ADAM インスタンスを作成する場合に、以下の手順を参考にしてください。Active Directory が起動しているドメイン・コントローラでなくても実行可能です。ADAM インスタンスは、ドメイン単位で作成されます。

1. **[ADAM インスタンスの作成]**をクリックしてください。



2. **[ポート]**と**[SSL ポート]**に ADAM インスタンスを作成する値を入力してください。
3. **[OK]**をクリックしてください。処理が開始され、ステータスが表示されます。PDDirprep のログファイルも作成されます。

注意：ADAM インスタンスが既にドメインに存在する場合には、エラーが表示されます。

4. **[ディレクトリ・スキーマの拡張]**をクリックしてください。

ディレクトリ・スキーマの拡張

ここでは、Active Directory もしくは、ADAM 内に ProtectDrive のための、スキーマ拡張を実行します。

Active Directory の場合には、プライマリ・ドメインのスキーマが直接拡張されます。これは全てのサブドメインを更新します。Active Directory のスキーマ変更は、フォレスト単位に実行されません。

ADAM の場合には、ADAM インスタンスが実行されるまで、なにも行いません。

1. [ディレクトリ・スキーマの拡張]をクリックしてください。
2. ADAM インスタンスが、すでに存在するかがチェックされます。もし存在しても、ADAM インスタンスは、拡張されます。もし、存在しない場合には、Active Directory のスキーマを拡張するかの、メッセージが表示されます。[はい]をクリックして、処理を継続してください。



3. 処理が開始され、ステータスが表示されます。PDDirprep のログファイルも作成されます。
4. ドメインの作成に続きます。

ドメインの作成

この処理を実行するためには、ドメインの管理者で必ずログオンしてください。この処理により、予め用意している ProtectDrive の属性を既存のコンピュータ・オブジェクトに標準の設定用のオブジェクトとして、Active Directory もしくは ADAM に作成します。

全てのクライアントは自動的に標準の設定オブジェクトとリンクされます。

1. [ドメインの作成]をクリックしてください。
2. ADAM インスタンスが既に存在するか確認します。もし存在する場合には、ADAM インスタンスは変更されます。もし、存在しない場合には、Active Directory へのオブジェクトの作成を警告メッセージ表示します。もし、表示された場合には、[はい]をクリックして、継続してください。



3. 処理が開始され、ステータスが表示されます。PDDirprep のログファイルも作成されます。
-

ログファイルの表示

いつでもログファイルを参照することが可能です。もし、障害が発生した場合には、ログを確認することができます。

全ての処理内容の表示が保存されています。以前の処理で障害が発生しているかを確認することができます。全ての処理は、ログファイルに保存されています。

1. [ログファイルの表示]をクリックしてください。Microsoft Notepad が起動します。
2. Microsoft Notepad でログを確認してください。

ProtectDrive 管理ツールのインストール

インストール前に下記の内容を確認してください。

- ADAM で ProtectDrive を管理する場合には、Active Directory のドメイン・コントローラが起動していないマシン（Windows Server 2003）に ADAM をインストールしてください。
 - ProtectDrive 管理ツールをインストールする前に、PDPrepDir ツールを実行してください。詳細は、30 ページを参照してください。
 - クライアント・コンポーネントをインストールする前に、ProtectDrive 管理者ツールをインストールしてください。これらのツールは、リモートでクライアントを管理するためのものです。それぞれのツールに関しては、35 ページを参照してください。
1. **SafeNet ProtectDrive.msi** を実行すると ProtectDrive のインストール・ウィザードが開きます。
 2. [ようこそ] 画面が表示されたら [次へ] をクリックしてください。
 3. [ライセンス契約] に同意して [次へ] をクリックしてください。

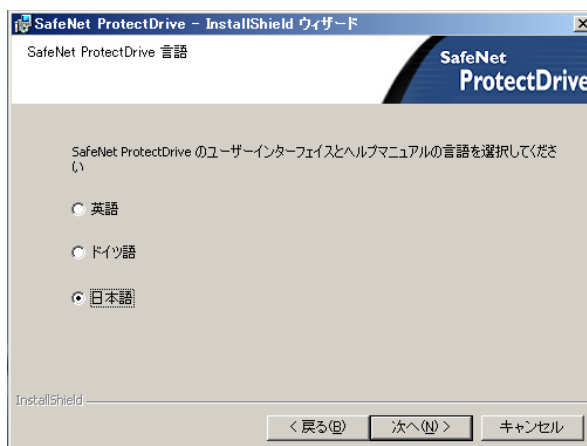


4. [管理ツールのインストール] を選択して [次へ] をクリックしてください。

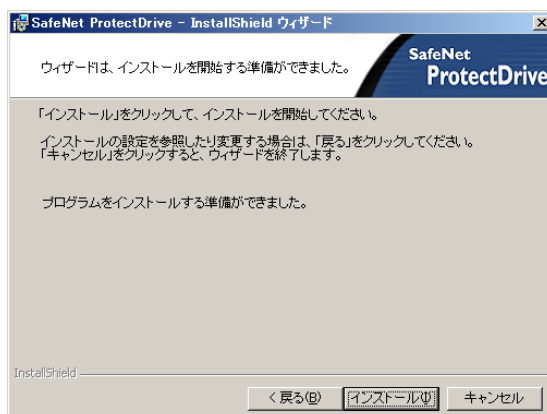


ProtectDrive を集中管理するためのツール、鍵の復旧および緊急パスワードの発行ツールがインストールされます。

5. インターフェースのラベルおよびテキスト・メッセージに使用する言語を選択して [次へ] をクリックしてください。



6. 下記の画面が表示されたら、準備完了です。[インストール]をクリックして、処理を継続してください。




7. インストールが完了すると下記の画面が表示されます。



- “ディレクトリ標準ユーティリティの起動”を選択すると、インストール終了後に PDDirPrep を起動することができます。
- “ディレクトリ標準ユーティリティの起動”を選択しなければ、後で Windows のスタートメニューから、プログラムの SafeNet ProtectDrive フォルダ内の “**Directory Preparation Utility**” から起動することができます。

8. [完了]をクリックしてください。

注意：インストール完了後に、での管理コンソールへのショートカットが Windows デスクトップに作成されます。

ProtectDrive の管理ツール

管理ツールのインストール前に、Directory Preparation Utility (PDDirPrep) を使用して、ドメインとスキーマを設定してください。もしそうでなければ、オブジェクトが見つからないなどのエラーが表示されます。

ProtectDrive の管理ツールを使用すれば、ProtectDrive を集中管理、鍵の復旧および緊急パスワードの発行を実行することが可能となります。Active Directory が稼働しているマシンもしくは、ドメイン・コントローラが実行されていない Windows Server 2003 の ADAM が稼働しているマシンにインストールしてください。

管理ツールとは以下のものです。

- **ProtectDrive Management Console** — ProtectDrive Management Console は、ProtectDrive クライアントを集中管理するためのツールです。Active Directory のユーザとコンピュータの管理と ProtectDrive クライアントのグループのための設定オブジェクトを作成、管理するための ProtectDrive 管理スナップインが含まれます。ProtectDrive 管理コンソールに関しては、次の章で詳細を説明します。

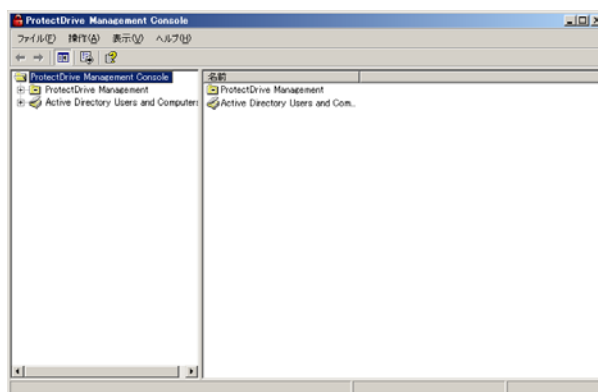
- **Remote Recovery Console** — Remote Recovery Console は、鍵の復旧と緊急パスワードの発行を行うことができます。詳細は、[第 11 章](#) — 「例外的な認証のシナリオ」を参照してください。
- **Directory Preparation Utility (PDDirPrep)** — Directory Preparation Utility は、ProtectDrive クライアントをリモートで管理するためのドメインを設定するツールです。PDDirPrep は、ProtectDrive のインストール CD の *Tools* フォルダ内からでも配布および実行することが可能です。詳細に関して、30 ページを参照してください。

ProtectDrive Management Console

以下の説明では、新しい設定やクライアントのリンクに関して説明します。新しい設定に関しては、ProtectDrive Management Console の ProtectDrive 管理スナップインからのみ追加可能です。

ProtectDrive Management Console を起動するには以下の 2 つの方法です。

- デスクトップの ProtectDrive Management Console のショートカット・アイコンをダブルクリックしてください。ProtectDrive の管理ツールのインストールで ProtectDrive Management Console はインストールされます。
- Windows のスタートメニューを選択し、プログラムの SafeNet ProtectDrive のフォルダから、Management Console を選択して起動してください。



注意：もし、クライアントがクライアントでの設定を実行している場合には、本ツールでの設定ではなく、個別での設定を実行してください。詳細は、39 ページを参照してください。

設定オブジェクト

設定オブジェクトとは、コンピュータを割り当てる ProtectDrive のポリシーです。標準では、全てのクライアントは、標準の設定オブジェクトからポリシーを取得します。

ProtectDrive バージョン 8.3 以前では、リモートのクライアントは、ADUC MMC 標準の設定オブジェクトによってのみ管理が可能で、ドメインでひとつの ProtectDrive のポリシーを使用するだけでした。

バージョン 8.3 以降では、複数の設定オブジェクトの作成と ProtectDrive Management Console で特定のコンピュータにアサインすることが可能です。コンピュータが特定の設定オブジェクトにアサインされる場合に、その設定の更新および変更を反映することができます。

注意：クライアントは、ADUC スナップインによって、ProtectDrive の以前のバージョンと同様に、個別に管理することができます。詳細は、39 ページを参照してください。個別でのクライアント設定は、異なる設定オブジェクトをいつでも設定することが可能です。

新しい設定オブジェクトの作成

1. サーバで ProtectDrive Management Console を起動してください。
2. “ProtectDrive Management” フォルダを開いてください。
3. “設定オブジェクト” を右クリックしてください。リストメニューが表示されます。
4. “New Configuration” を選択してください。
5. 設定オブジェクトの名前を[名前]に入力し、[OK]をクリックしてください。絶対に ‘,’ や ‘?’ などの特殊文字を使用しないでください。
6. 続いて、新しい設定オブジェクトに少なくとも一人のユーザを追加してください。

新しい設定オブジェクトにユーザを追加

いつでも新しい設定オブジェクトを作成することができます。ProtectDrive の設定を変更する前に、必ず一人以上のユーザを登録してください。

1. サーバで **ProtectDrive Management Console** を起動してください。
2. “**ProtectDrive Management**” フォルダを開いてください。
3. “設定オブジェクト” フォルダを開いてください。
4. 追加するオブジェクトを右クリックして、“**プロパティ**” を選択してください。
5. “**PD ユーザ**” タブをクリックしてください。
6. [追加]をクリックして、ユーザを追加してください。
7. [適用]をクリックして、[OK]をクリックしてください。

設定オブジェクトの変更

1. サーバで **ProtectDrive Management Console** を起動してください。
2. “**ProtectDrive Management**” フォルダを開いてください。
3. “設定オブジェクト” フォルダを開いてください。
4. 登録するオブジェクトを右クリックして、“**プロパティ**” を選択してください。
5. “**PD 設定**” タブをクリックしてください。

6. 設定を変更してください。
7. [適用]をクリックして、[OK]をクリックしてください。

ProtectDrive クライアントを設定オブジェクトにアサイン

クライアントを新しい設定オブジェクトや他の設定オブジェクトにアサインすることができます。標準の設定オブジェクト以外の設定オブジェクトにリモートの ProtectDrive クライアントを下記の手順でアサインすることが可能です。

1. サーバで **ProtectDrive Management Console** を起動してください。
2. “**ProtectDrive Management**” フォルダを開いてください。
3. “**設定オブジェクト**” フォルダを開いてください。
4. アサインするオブジェクトを右クリックして、“**プロパティ**”を選択してください。
“**クライアントの設定**” タブをクリックしてください。現在のアサインされているクライアントがリストで表示されます。
5. [追加]をクリックしてください。
6. [詳細設定]をクリックしてください。
7. 追加するクライアントを選択して、[OK]をクリックしてください。
8. 登録されたことを表示で確認して、[OK]をクリックしてください。新しく追加したクライアントが、“クライアントの設定” タブに表示されます。

注意：既に別の設定オブジェクトに設定されていたクライアントを選択した場合には、クライアントのアサインを変更するかのメッセージが表示されます。

設定オブジェクトから ProtectDrive クライアントを削除

いつでも設定オブジェクトからクライアントを削除することができます。設定から削除する場合には、クライアントは個別での設定となり、Active Directory のユーザとコンピュータの MMC スナップインからのみ確認できます。いつでも別の設定オブジェクトにアサインすることが可能です。

1. サーバで **ProtectDrive Management Console** を起動してください。
 2. “**ProtectDrive Management**” フォルダを開いてください。
 3. “**設定オブジェクト**” フォルダを開いてください。
 4. 削除するオブジェクトを右クリックして、“**プロパティ**”を選択してください。
 5. “**クライアントの設定**” タブをクリックしてください。現在のアサインされているクライアントがリストで表示されます。
 6. 削除するクライアントを選択して、[削除]をクリックしてください。
 7. 確認メッセージで、[はい]をクリックしてください。
-

8. [適用]をクリックして、[OK]をクリックしてください。

自己管理されたクライアントと設定で管理されたクライアント

自己管理されたクライアントでは、Active Directory もしくは、ADAM と重複した情報が、個別に設定されます。個別でクライアント設定されたクライアントは、Active Directory のユーザおよびコンピュータの MMC スナップインからのみ参照できます。

また、異なる設定オブジェクトによるクライアント管理は、設定で管理されたクライアントとなります。自己管理されたクライアントを異なる設定オブジェクトにいつでも再アサインすることが可能です。

自己管理されたクライアントを設定で管理されたクライアントに変更

1. サーバで **ProtectDrive Management Console** を起動してください。
2. “**Active Directory ユーザとコンピュータ**” MMC スナップインを開いてください。
3. “**Computers**” を選択し、変更するクライアントを右クリックし、“**プロパティ**” を選択してください。
4. [PD 設定]タブを選択し、[設定管理]を選択する。クライアントは、“**自己管理**”に設定されています。
5. [設定での管理]を選択し、設定をリストより選択してください。
6. [適用]をクリックし、[OK]をクリックしてください。ProtectDrive Management スナップインで参照できる新しい設定に接続されます。

設定で管理されたクライアントを自己管理されたクライアントに変更

1. サーバで **ProtectDrive Management Console** を起動してください。
2. “**ProtectDrive Management**” フォルダを開いてください。
3. “**設定オブジェクト**” フォルダを開いてください。
4. 設定するオブジェクトを右クリックして、“**プロパティ**” を選択してください。
5. [クライアントの設定]タブを選択してください。現在設定されているクライアントが表示されます。
6. 反転表示されているクライアントが自己管理となります。
7. [削除]をクリックしてください。
8. 確認画面で[OK]をクリックしてください。
9. [適用]をクリックし、[OK]をクリックしてください。**Active Directory ユーザとコンピュータ** スナップインで参照できます。

クライアント・コンポーネントのインストール

ProtectDrive のクライアント・コンポーネントは、ProtectDrive のスタンドアロンおよびネットワーク・システム（Windows ドメインのメンバ）の管理および暗号化に使用します。

注意：ハードディスクが複数存在するシステムに ProtectDrive クライアント側コンポーネントを導入する場合、ProtectDrive のインストール・ドライブを **disk0** にする必要があります。

カスタム・グラフィック・ファイルの使用

インストール・ファイルのほかに、カスタム・グラフィック・ファイル（**ACSGIF** という名前のファイル）も **¥Install** ディレクトリに格納して、認証画面を変更することが可能です。

このグラフィック・ファイルには、さまざまな ProtectDrive のプリブート認証またはシステム復旧の表示画面の一部として表示される、顧客固有のアートワークが含まれています。このファイルが存在する場合、ProtectDrive インストーラにより、クライアント側コンポーネントのインストールの一部として自動的にこのファイルが追加されます。

注意：このグラフィック・ファイルの作成には、専用のツールが必要であり、作成に関しては、販売店もしくは SafeNet へお問い合わせください。

ProtectDrive のクライアント・コンポーネントのインストール

注意：Windows Vista に ProtectDrive をインストールする場合には、**SafeNet ProtectDrive.msi** の代わりに、**setup.exe** を実行してください。

名前 ▲	サイズ	種類	更新日時
Tools		ファイル フォルダ	2008/08/13 18:20
1031.mst (ドイツ語)	99 KB	MST ファイル	2008/08/13 11:38
1033.mst (英語語)	4 KB	MST ファイル	2008/08/13 11:38
1041.mst (日本語)	98 KB	MST ファイル	2008/08/13 11:38
pd_administration_guide.pdf	3,252 KB	Adobe Acrobat Doc...	2008/05/08 2:19
PD_Release_Note_v8 5 0_revC_J.pdf	193 KB	Adobe Acrobat Doc...	2008/12/05 21:29
pd_user_manual.pdf	1,043 KB	Adobe Acrobat Doc...	2008/05/08 2:08
SafeNet ProtectDrive.msi	27,492 KB	Windows インストーラ...	2008/08/13 11:38
Setup.exe	56 KB	アプリケーション	2008/08/13 11:23

デフォルト言語の変更

ProtectDrive インストール・ウィザードのデフォルト言語は英語です。異なる MST ファイル（以下の例に示す）を使用すると、この言語を変更できます。例として、ProtectDrive インストールを日本語に変更し、DOS プロンプトに移動して、次のコマンド・ラインを入力してください。

```
MSIEXEC /I "SAFENET PROTECTDRIVE.MSI" TRANSFORMS=1041.MST
```

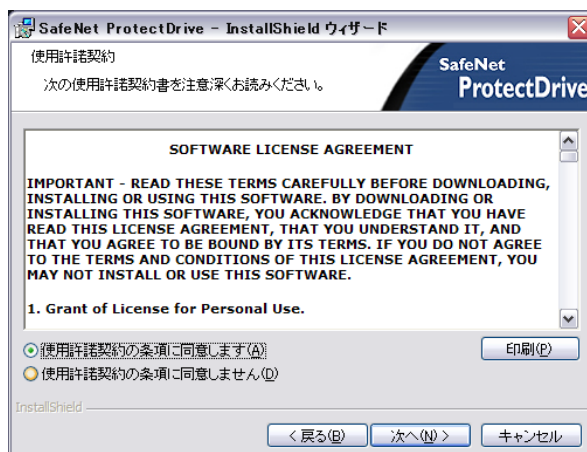
注意：現状、setup.exe は英語でのインストールのみをサポートしています。MSIEXEC での言語の指定は setup.exe ではできません。

ユーザとの対話を最小限に抑えたこのウィザードにより、次の手順で自動的に ProtectDrive クライアント側コンポーネントがインストールされます。

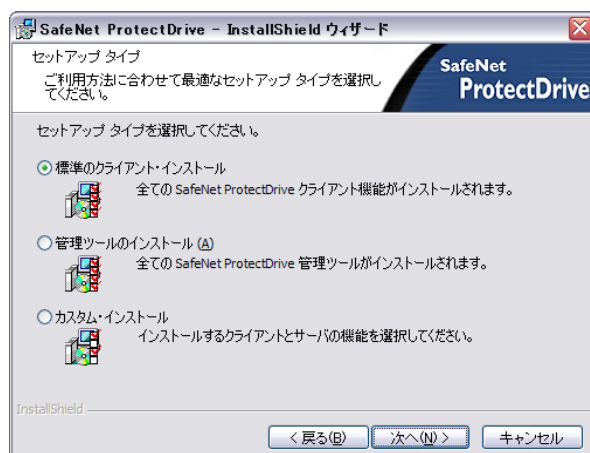
1. **SafeNet ProtectDrive.msi** を実行すると ProtectDrive のインストール・ウィザードが開きます。
2. **【ようこそ】** 画面が表示されたら **【次へ】** をクリックしてください。



3. **【ライセンス契約】** に同意して **【次へ】** をクリックしてください。 .



4. [標準クライアント・インストール] を選択して [次へ] をクリックしてください。



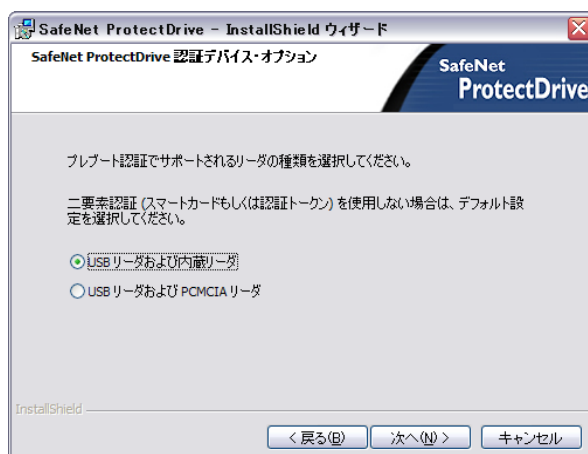
5. インターフェースのラベルおよびテキスト・メッセージに使用する言語を選択して [次へ] をクリックしてください。



6. ライセンスの種類を選択し、[次へ] をクリックしてください。



- [試用バージョン]を選択すると、ProtectDrive の 30 日評価バージョンがインストールされます。(インストールの後に、LMC ライセンス・マネージャの設定で、試用ライセンスを完全なライセンスにアップデートすることができます。)
 - [フルバージョン]を選択すると、有効なライセンスコード (例えば、license.txt) か認証コード (例えば、authorization.txt) のどちらかが必要となります。ライセンスおよび認証ファイルのためのデフォルトパスは、ソースディレクトリ (SafeNet ProtectDrive.msi ファイルが実行される) です。
 - ライセンスコードもしくは、認証コードを入力するために、[参照]をクリックしてファイルを指定し、[次へ]をクリックしてください。
 - 認証コードを入力する場合には、インターネット接続でライセンス・サーバへの接続が必要となります。[認証コード]を選択して、認証ファイルを検索し、[インストール]をクリックしてください。ライセンス・サーバは、接続されて (インターネット接続を通して)、順番にインストールを続けるための認可コードを提供します。
7. プリブート認証で使用する読取装置を選択し、[次へ]をクリックしてください。プリブート環境におけるドライバを限定するために、どのグループのスマートカード・リーダが必要であるかを指定するためです。なにも必要でないなら、デフォルトを選択してください。

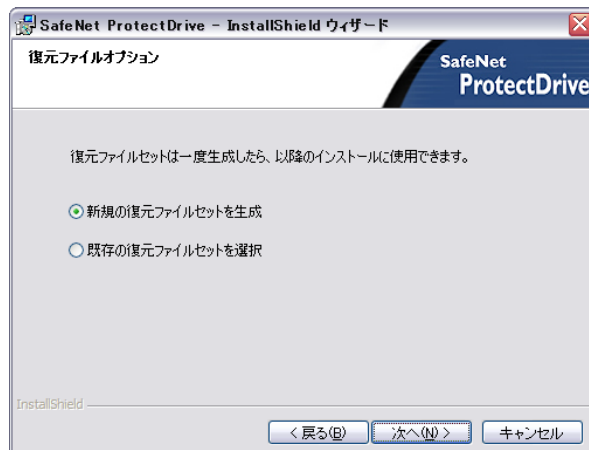


8. 適切な ProtectDrive の設定方法を選択してください。スタンドアロン・インストールのために[クライアントの設定]を選択するか、リモート設定のために Active Directory もしくは ADAM を使用する[リモート設定]を選択し、[次へ]をクリックしてください。リモート設定を選択した場合には、ステップ 11 で使用する既存の復旧ファイルセットがなければなりません。



注意：クライアントの設定を選択した場合には、ローカル管理コンソールの詳細設定内の管理アップデートのオプションが使用できなくなります。これは、Active Directory もしくは ADAM を使用する場合のみ、使用可能となります。

9. 復旧ファイルのオプションを選択して、[OK]をクリックしてください。

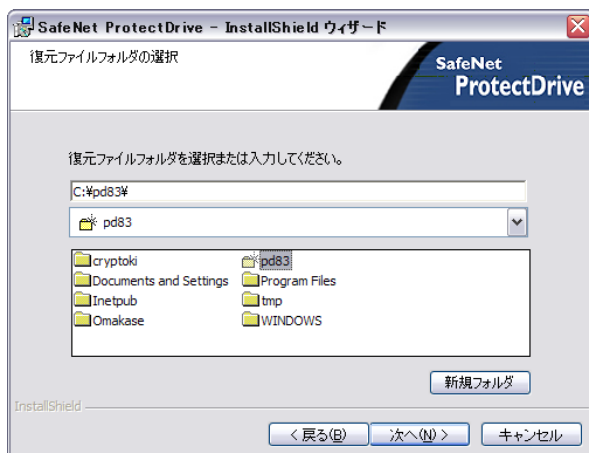


- 既存の“復旧ファイルセットを選択”を選択した場合には、ステップ 12 にスキップしてください。
- 新規の“復旧ファイルセットを生成”を選択した場合には、下記の画面が表示されます。復旧ファイルセットのパスワードを指定して、[次へ]をクリックしてください。

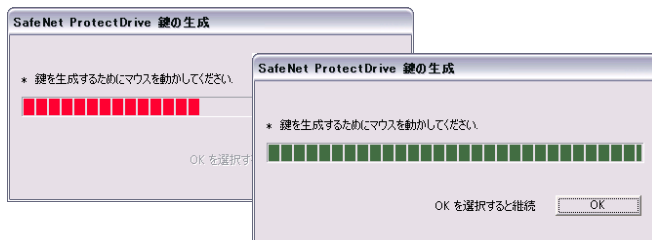


10. 復旧ファイルのフォルダを指定し、[次へ]をクリックしてください。

- [既存の復旧ファイルセットを選択] を選択した場合には、既存のファイルが存在するフォルダを指定してください。
- [新規の復旧ファイルセットを生成] を選択した場合には、新たにファイルを作成するフォルダを指定してください。セキュアな場所であり、ネットワークディスク上やフロッピーディスクなどのローカルディスク以外を推奨します。



11. [新規の復旧ファイルセットを生成]を選択した場合には、復旧ファイルのための鍵の生成が行われます。マウスを動かし、作成が完了したら[OK]をクリックしてください。



12. 生成が完了すると完了画面が表示されます。[OK]をクリックしてください。

13. 下記の画面が表示されたら、[インストール]をクリックして、インストール開始してください。



14. 下記の画面が表示されたら、インストールは完了です。[終了]をクリックしてください。



15. 下記の画面が表示されたら、[OK]をクリックして、必ず P C を再起動してください。



インストールのカスタマイズ

サーバ側コンポーネントとクライアント側コンポーネントのインストール以外に、ProtectDrive にはインストール・コンポーネントをカスタマイズして選択する機能があります。

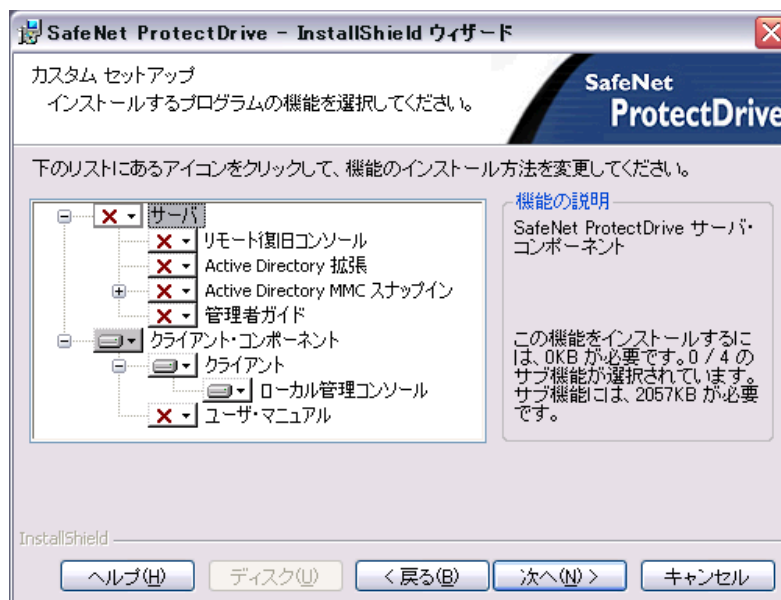
1. **SafeNet ProtectDrive.msi** を実行すると ProtectDrive のインストール・ウィザードが開きます。
2. [よろこそ] 画面が表示されたら [次へ] をクリックしてください。
3. [ライセンス契約] に同意して [次へ] をクリックしてください。



4. [カスタム・インストール] を選択して [次へ] をクリックしてください。



5. インストールするコンポーネントから [サーバ] または [クライアント] を選択して [次へ] をクリックしてください。



サーバ側コンポーネント

鍵復旧 アプリケーション	このコンポーネントを選択すると、 rpadmin.exe がインストールされます。追加情報については、第 11 章 - 例外的な認証のシナリオを参照してください。
Active Directory/ADAM スキーマ拡張	このコンポーネントを選択すると、Active Directory もしくは ADAM スキーマ拡張が適用されます。
Active Directory MMC スナップイン	このコンポーネントを選択すると、サーバの ProtectDrive システムおよびユーザ・ポリシーの管理に必要なすべての MMC スナップインがインストールされます。
管理者ガイド	このコンポーネントを選択すると、『SafeNet ProtectDrive 管理者ガイド』がインストールされます。

クライアント側コンポーネント

SafeNet ProtectDrive クライアント	このコンポーネントを選択すると、ローカル管理コンソール (LMC) アプリケーションが追加されます。このコンポーネントは、ProtectDrive クライアントのローカル管理に使用します。
ユーザ・マニュアル	このコンポーネントを選択すると、『SafeNet ProtectDrive ユーザ・マニュアル』がインストールされます。

6. インターフェースのラベルおよびテキスト・メッセージに使用する言語を選択して [次へ] をクリックしてください。

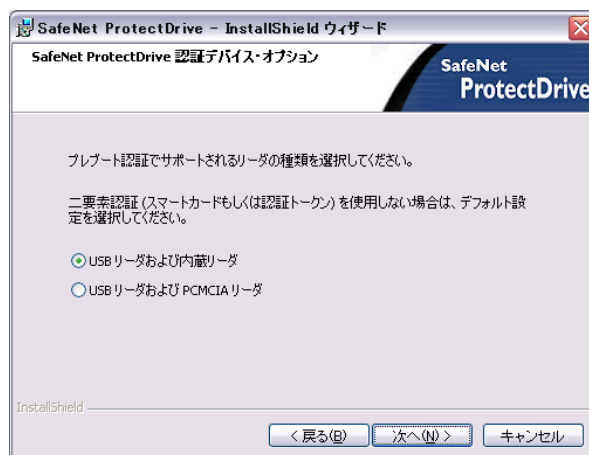


7. ライセンスの種類を選択し、[次へ] をクリックしてください。



- 試用バージョンを選択すると、ProtectDrive の 30 日評価バージョンがインストールされます。(インストールの後に、LMC ライセンス・マネージャの設定で、試用ライセンスを完全なライセンスにアップデートすることができます。)
- フルバージョンを選択すると、有効なライセンスコード（例えば、license.txt）か認証コード（例えば、authorization.txt）のどちらかが必要となります。ライセンスおよび認証ファイルのためのデフォルトパスは、ソースディレクトリ（SafeNet ProtectDrive.msi ファイルが実行される）です。
 - ライセンスコードを入力するために、ライセンス・ファイルを検索し、ファイルを開き、コピー&ペーストでコードを入力し、[インストール]をクリックするか、ライセンス・ファイルを検索し、[インストール]をクリックしてください。

- 認証コードを入力する場合には、インターネット接続でライセンス・サーバへの接続が必要となります。**[認証コード]**を選択して、認証ファイルを検索し、**[インストール]**をクリックしてください。ライセンス・サーバは、接続されて（インターネット接続を通して）、順番にインストールを続けるための認可コードを提供します。
8. ライセンスコードもしくは認証コードがインストールされると確認画面が表示されます。**[OK]**をクリックしてください。
 9. プリブート認証で使用する読取装置を選択し、**[次へ]**をクリックしてください。プリブート環境におけるドライバを限定するために、どのグループのスマートカード・リーダーが必要であるかを指定するためです。なにも必要でないなら、デフォルトを選択してください。

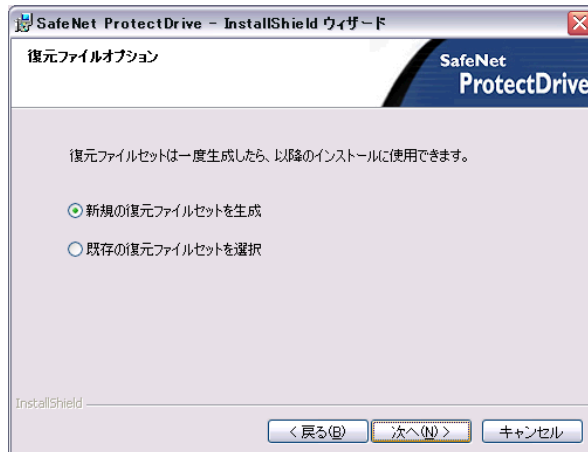


10. 適切な ProtectDrive の設定方法を選択してください。スタンドアロン・インストールのために**クライアントの設定**を選択するか、リモート設定のために Active Directory もしくは ADAM を使用する**[リモート設定]**を選択し、**[次へ]**をクリックしてください。リモート設定を選択した場合には、ステップ 11 で使用する既存の復旧ファイルセットがなければなりません。



注意：クライアントの設定を選択した場合には、ローカル管理コンソールの詳細設定内の管理アップデートのオプションが使用できなくなります。これは、Active Directory もしくは ADAM を使用する場合のみ、使用可能となります。

11. 復旧ファイルのオプションを選択して、[OK]をクリックしてください。



- 既存の復旧ファイルセットを選択を選択した場合には、ステップ 12 にスキップしてください。
- 新規の復旧ファイルセットを生成を選択した場合には、下記の画面が表示されます。復旧ファイルセットのパスワードを指定して、[次へ]をクリックしてください。

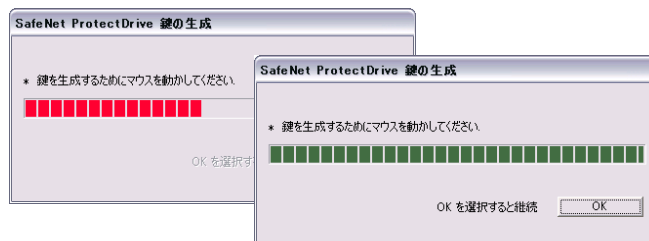


12. 復旧ファイルのフォルダを指定し、[次へ]をクリックしてください。

- **[既存の復旧ファイルセットを選択]**を選択した場合には、既存のファイルが存在するフォルダを指定してください。
- **[新規の復旧ファイルセットを生成]**を選択した場合には、新たにファイルを作成するフォルダを指定してください。セキュアな場所であり、ネットワークディスク上やフロッピーディスクなどのローカルディスク以外を推奨します。



13. **[新規の復旧ファイルセットを生成]**を選択した場合には、復旧ファイルのための鍵の生成が行われます。マウスを動かし、作成が完了したら**[OK]**をクリックしてください。



14. 生成が完了すると完了画面が表示されます。**[OK]**をクリックしてください。

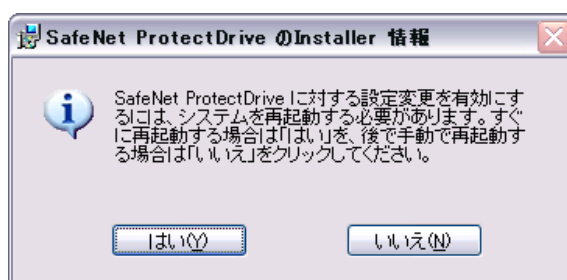
15. 下記の画面が表示されたら、[インストール]をクリックして、インストールを開始してください。



16. 下記の画面が表示されたら、インストールは完了です。[終了]をクリックしてください。



17. 下記の画面が表示されたら、[OK]をクリックして、必ずPCを再起動してください。



以前のバージョンの ProtectDrive からのアップデート

アップグレードの前に

- 最新の ProtectDrive では、バージョン 7.2.3、8.1.0、8.2.0、8.2.1 および 8.3 からのアップグレードをサポートしています。
- Active Directory および ADAM 内の ProtectDrive のスキーマをアップグレードする場合には、**PDDirPrep** を再度実行してください。
- サーバおよびリモート・クライアントをアップグレードする場合には、サーバを最初にアップグレードしてください。
- 8.2 より以前の ProtectDrive のバージョンからアップグレードを始める前に、作成された syskey.bin か syskey.cid ファイルが存在するか確認してください。詳細は、55 ページの *新しい復旧ファイルセットの作成* を参照してください。
- ProtectDrive バージョン 8.2.x より以前から最新版にアップグレードした後に、すべての既存のクライアントが、「セルフ管理」されていると認識されます。アップグレード前と何ら異なることなく利用可能です。最新版にアップグレードされると、既存の設定を変更することが可能です。(アップグレード後に、セルフ管理から別の管理方法に変更が可能です。)
- ProtectDrive をインストールした Windows XP を Vista にアップグレードする場合には、一旦 ProtectDrive をアンインストールしてから、Vista へのアップグレードを行ってください。
- 現在 Active Directory を使用しているなら、変更の必要がない場合には ADAM に変更するより、それを使用し続けることを推奨します。

しかしながら、Active Directory から ADAM に変更する場合には、以下のとおりです。

- ProtectDrive をサーバからアンインストール
- **Administrative Management Tools** をインストール
- **PDDirPrep** を使用して ADAM インスタンスの作成 (ドメインコントローラとは別のマシンに)

注意： Active Directory から ADAM に変更した後に、2 セットのスキーマ拡張したものが存在します。ProtectDrive はアンインストールされて、再インストールされますが、Active Directory サーバから登録したスキーマを取り除くことはできません。

新しい復旧ファイルセットの作成

アップグレードのために新しい復旧ファイルセット（PdMaster.cer、PdMster.pfx、PdRecovery.cer、PdRecovery.pfx、Salt.cid）を作成してください。それぞれの証明書を作成するには、二つの方法があります。

- ProtectDrive の新規インストールで作成
- Certificate Wizard（certwizardapp.exe）を使用して作成

アップグレードを実行するとき、現在インストールされている ProtectDrive のバージョンが作成した syskey.bin か syskey.cid を指定しなければなりません。アップグレード中に、syskey ファイルは、salt.cid ファイルに変換されます。マルチクライアントのアップグレードでは、リムーバブル・メディアを共有するのに使用することができる salt.cid を作成するために同じ syskey を使用しなければなりません。

注意：アップグレードの場合には、Certificate Wizard で salt.cid ファイルは作成しないでください。

インタラクティブ・アップグレードに関して

新しい復旧ファイルセットを作成するか、既存の ProtectDrive バージョン 8.2 ファイルセットを使用するかを選ぶことができます。

- 新しいファイルセットを作成させる場合には、PdMaster と PdRecovery ファイルはインストール中に作成されます。
- 既存のファイルセットを使用する場合には、PdMaster と PdRecovery ファイルは以前のバージョンで作成、もしくは Certificate Wizard から作成されなければなりません。
- マルチクライアントをアップグレードさせるなら、既存のファイルセットを使用することを推奨します。
- サーバおよびクライアントをアップグレードする場合には、サーバを先にアップグレードしてください。

サイレントおよび GPO アップグレードに関して

これは、既存の復旧ファイルセットを使用する場合に必要となります。復旧ファイルセットが SafeNet ProtectDrive.msi ファイルと同じフォルダか、または ERA_km_REC_FILE_FOLDER_PATH MSI のプロパティで定義されるフォルダに存在する場合です。

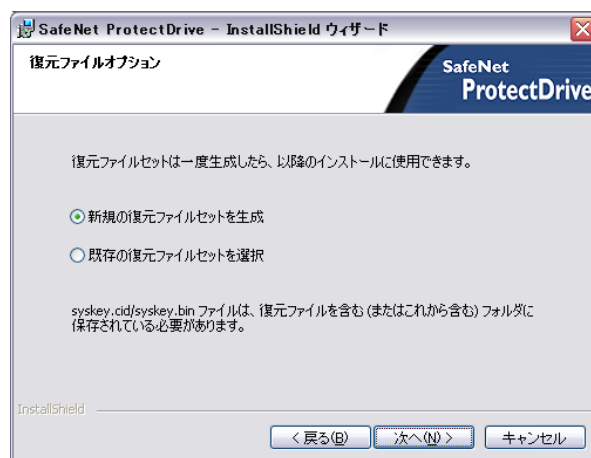
RecoveryEnvelope.env ファイルがこのディレクトリで作成されるので、ここで指定されたディレクトリは「書き込み可能」に必ず設定してください。また、Active Directory か ADAM を使用する場合には、RecoveryEnvelope.env ファイルは管理サーバにコピーされます。

アップグレード手順

ProtectDrive アップグレードは、新規クライアントのインストールと同じ手順で、SafeNet ProtectDrive.msi で実行します。システムは、ProtectDrive の以前のバージョンを検出し、インストールされます。

アップグレード・インストール画面は、新規インストールと基本的に同じです。唯一の違いは、復旧ファイルのオプションを選択して、syskey.bin か syskey.cid ファイルを PdMaster と PdRecovery ファイルと同じフォルダに存在させることです。これは、syskey ファイルが salt.cid に変換されるためです。

下記の復旧ファイルのオプション画面で指定してください。



詳細は、「クライアントのインストール」を参照してください。

ProtectDrive の削除

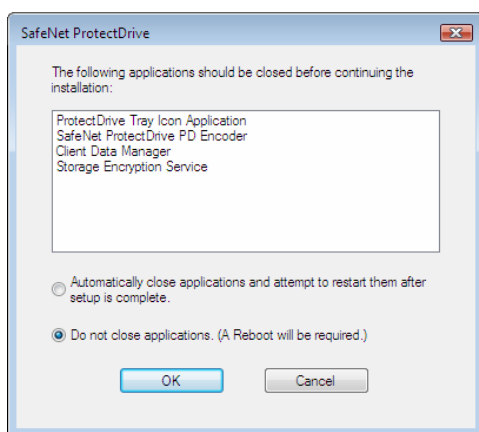
Windows Vista

Windows Vista での ProtectDrive のアンインストールは、下記の手順で行ってください。

1. すべてのパーティションが復号化されていることを確認してください。
2. Windows のコントロール・パネルから [プログラム]>[プログラムと機能] へ移動してください。
3. “SafeNet ProtectDrive “を選択して、[アンインストール]をクリックしてください。



4. 確認メッセージが表示されるので、[はい]をクリックしてください。
5. 現在起動中のアプリケーションが表示されます。“Do not close applications.”を選択して、[OK]をクリックしてください。

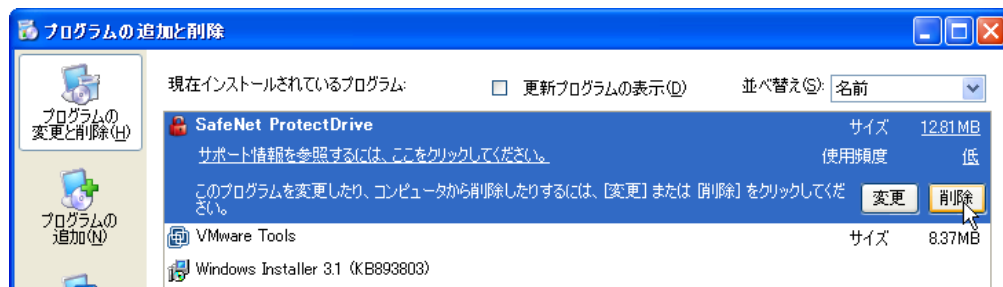


6. コンピュータの再起動の確認画面で、[はい]を選択してください。

Windows 2000、2003 および XP

Windows 2000、2003 および XP での ProtectDrive のアンインストールは、下記の手順で行ってください。

1. すべてのパーティションが復号化されていることを確認してください。
2. Windows のコントロール・パネルから **[プログラムの追加と削除]** へ移動してください。
3. **[SafeNet ProtectDrive]** を選択して **[削除]** をクリックしてください。



4. **[はい]** をクリックして削除を完了します。
5. **[はい]** をクリックしてコンピュータを再起動してください。

注意：Windows Vista では、上記の**[プログラムの追加と削除]**から、削除することができないことがあります。再度、**Setup.exe** を起動して、削除メニューから削除してください。

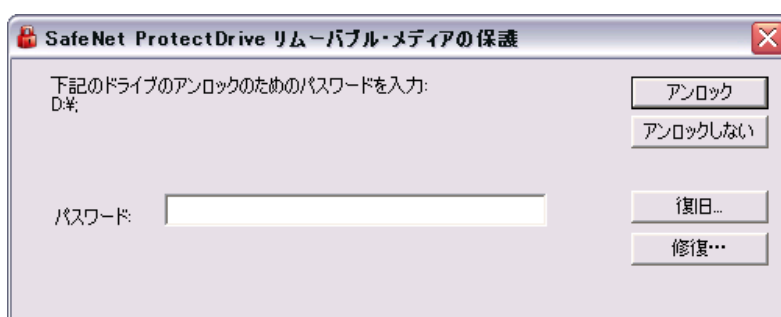
リムーバブル・メディアの復旧

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、メディアを確実に復旧して再利用できるようにするには、一旦フォーマットする必要があります。

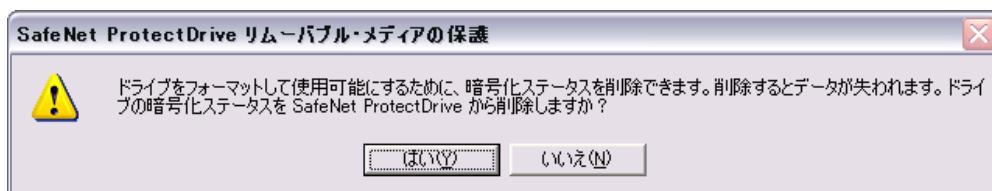
標準的な復旧手順

下記の手順は、それぞれの USB フラッシュ・ドライブで実行してください。

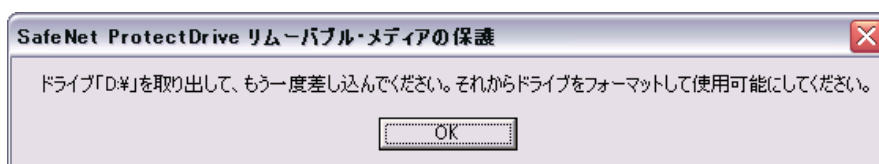
1. 復旧するリムーバブル・メディア・デバイスを接続してください。デバイスを認識すると下記の画面が表示されます。



2. [修復]をクリックしてください。
3. 下記の確認メッセージが表示されたら、[はい]をクリックしてください。



4. また、下記のメッセージが表示されたら、[OK]をクリックして、USB フラッシュ・ドライブを抜いてください。



5. 再度、USB フラッシュ・ドライブを差し込むと、フォーマットを行う必要があります。暗号化の前に、必ずフォーマットを行ってください。

注意：再度差し込んだ場合に、フォーマットをせずに暗号化を実行するとエラーが表示されます。なお、フォーマットは Windows 標準のフォーマット機能をご利用ください。(例：再度差し込んだ後に、ドライブのアイコンをクリックすると、フォーマットが必要であるメッセージが表示されます。そのままフォーマットを実行してください。)

RmRMBR を使ったリムーバブル・メディアの復旧

前のセクションで説明した復旧手順で復旧できない場合には、下記の方法での復旧手順に従ってください。

この手順は配布されるそれぞれの USB フラッシュ・ドライブで実行してください。

1. USB フラッシュ・ドライブを復旧するために、コンピュータに挿入してください。装置ごとの適切な手順に従ってください。
 - もしデバイスが暗号化されている場合には、パスワードの確認画面が表示されます。パスワードを入力して、[OK]をクリックしてください。
 - もしデバイスが暗号化されていない場合には、暗号化の確認画面が表示されます。[暗号化しない]を選択してください。
2. コマンド・ラインからの実行
 - Windows デスクトップのスタートメニューから、“ファイル名を指定して実行”を選択してください。
 - ファイル名を指定して実行ダイアログで、“cmd”を入力して、[OK]をクリックしてください。
3. ProtectDrive のフォルダに移動してください。
cd ¥Program Files¥SafeNet ProtectDrive
4. 復旧ユーティリティを起動してください。
rmrmbrr /d x:¥
(x は、リムーバブル・メディアのドライブ名です。)
5. デバイスから ProtectDrive を削除していいかのメッセージが表示されます。[Enter]を入力して継続してください。(もし中止する場合には、Ctrl+C を入力してください。)
6. 正しくリムーバブル・メディアを抜いてください。
7. 再度リムーバブル・メディアを挿してください。

注意：もし、上記の方法で復旧できない場合には、次の章の方法で復旧してください。

リムーバブル・メディアの復旧 – その他の方法

前のセクションで説明した復旧手順を用いることに代わる手段として、セクタ 0 のバックアップデータでリムーバブル・メディア装置を修復することが可能です。**デバイスを復旧するために、デバイスのセクタ 0 データのバックアップ**（18 ページを参照してください）が、以下の復旧手順で必要となります。

下記の方法に従って、セクタ 0 のデータで USB フラッシュ・ドライブを復旧してください。またデバイスが再利用のために再フォーマットされます。この手順は、それぞれの USB フラッシュ・ドライブで実行してください。

1. USB フラッシュ・ドライブを、ProtectDrive がインストールされていないコンピュータに挿入してください。
2. **dskprobe** ユーティリティを実行してください（このユーティリティは、Microsoft Windows 2000 リソース・キットに収録されています。リソース・キットはインターネットからダウンロードできます）。
3. **[ファイル]>[ファイルを開く]** の順に選択してください。この USB フラッシュ・ドライブのセクタ 0 のデータが保存されたファイルを開きます。
4. **[ドライブ]>[物理ドライブ]** の順に選択してください。
5. リスト中の最後のドライブをダブルクリックしてください。このドライブは通常 USB フラッシュ・ドライブです。このドライブは、画面下の **[ハンドル 0]** に表示されます。
6. デバイスへの書き込みを可能にするために、読み取り専用のオプションの選択を解除してください。
7. このドライブで **[アクティブに設定]** を選択して **[OK]** をクリックしてください。
8. デフォルトの設定は変更しないでください。**[セクタ]>[書き込み]>[このデバイスへの書き込み]** の順にクリックしてください。
9. 警告が表示されたら **[はい]** を選択してください。


ドライブにアクセスしようとする、フォーマットのプロンプトが表示されます。これで安全にフォーマットできます。

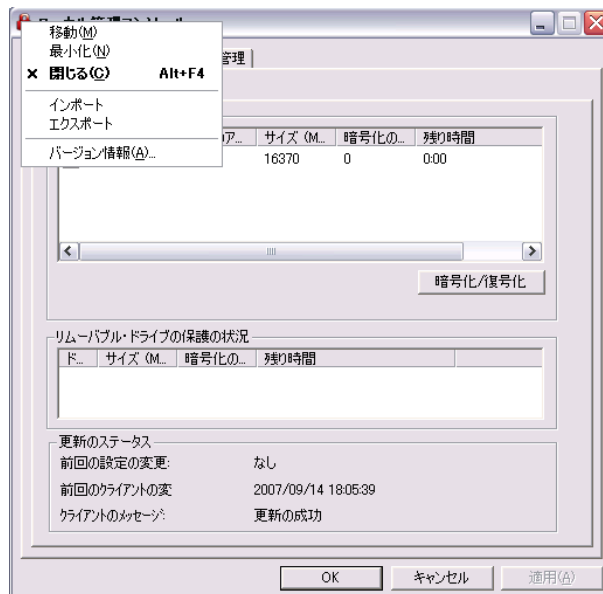
設定ファイル（.XML ファイル）のエクスポート

大規模のインストールにおいて、別クライアントの ProtectDrive の設定を XML ファイルでエクスポートし、ネットワーク上の複数のクライアント PC をすぐに設定することができます。

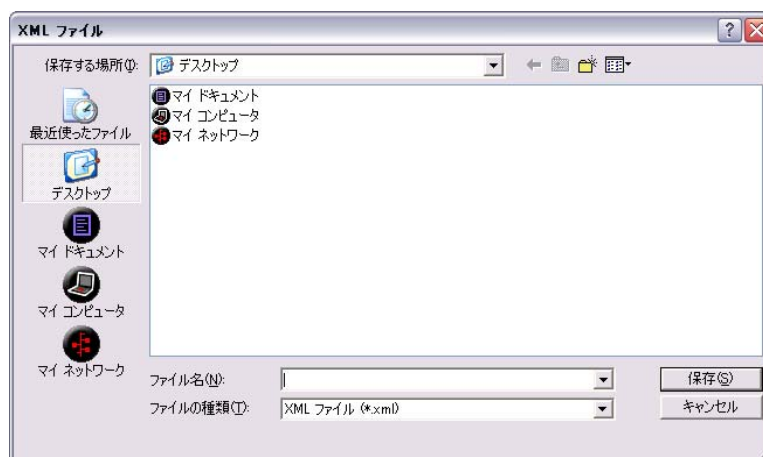
インストールおよび、クライアント PC のために必要な設定をした後に、設定を XML ファイルにエクスポートしてください、次に、ファイルを複数のクライアントにインポートしてください。この XML ファイルは、salt.cid ファイル（リムーバブル・メディア復旧のために使用される）を使用して暗号化され、このファイルを同じ salt.cid を共有するクライアント PC でインポートすることが可能となります。

注意： GPO インストールでカスタム設計された SafeNet ProtectDrive.msi ファイルに、ERA_PATH_XML_CONFIG のプロパティが含まれていることによって、このエクスポートされた XML ファイルを使用することができます。以下の手順に従って、クライアント設定を XML ファイルにエクスポートしてください。

1. クライアントでローカル管理コンソールを起動してください。
2. ローカル管理コンソールの右上の  アイコンを左クリックしてください。
3. **[エクスポート]** をクリックしてください。



4. エクスポートするファイル名を下記の画面で指定して、[保存]をクリックしてください。標準のファイル名は、**PDCconfig.xml** です。




5. 下記の保存が完了したメッセージが表示されたら、[OK]をクリックしてください。エクスポートされた設定ファイルを複数のクライアントでインポートすることが可能です。

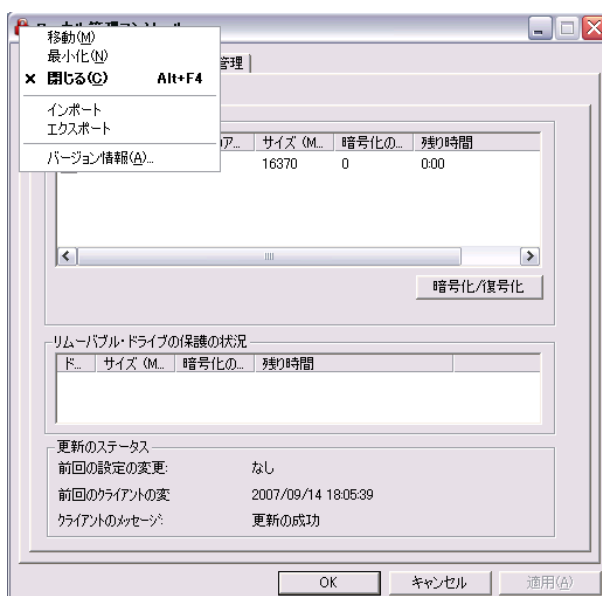


設定ファイル（.XML ファイル）のインポート

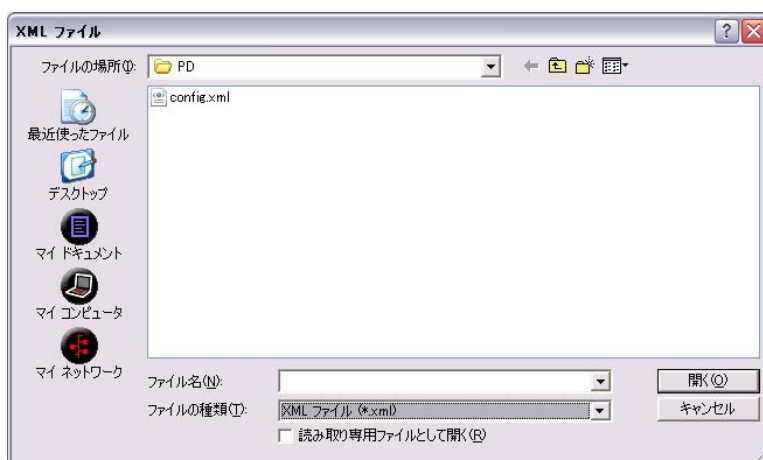
別のクライアント PC で、ProtectDrive のクライアント設定を XML ファイルで保存している場合に、同じ設定を持たせたい他のクライアント PC にインポートすることができます。この XML ファイルは、salt.cid ファイル（リムーバブル・メディア復旧のために使用される）を使用して暗号化され、このファイルを同じ salt.cid を共有するクライアント PC でインポートすることが可能となります。

設定をインポートする前に、必ず ProtectDrive をインストールしてください。

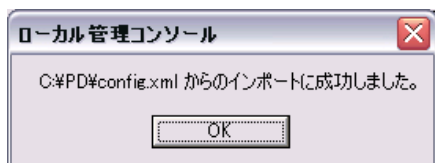
1. クライアントでローカル管理コンソールを起動してください。
2. ローカル管理コンソールの右上の  アイコンを左クリックしてください。
3. [インポート]をクリックしてください。



4. インポートするファイルを選択して、[開く]をクリックしてください。



5. 下記の確認画面が表示されたら、[OK]をクリックしてください。



6. 同じ ProtectDrive 設定を必要とする複数のクライアント PC で、この手順を繰り返してください。そして、同じ salt.cid を使用してください。

第6章 シングル・サイン・オン管理

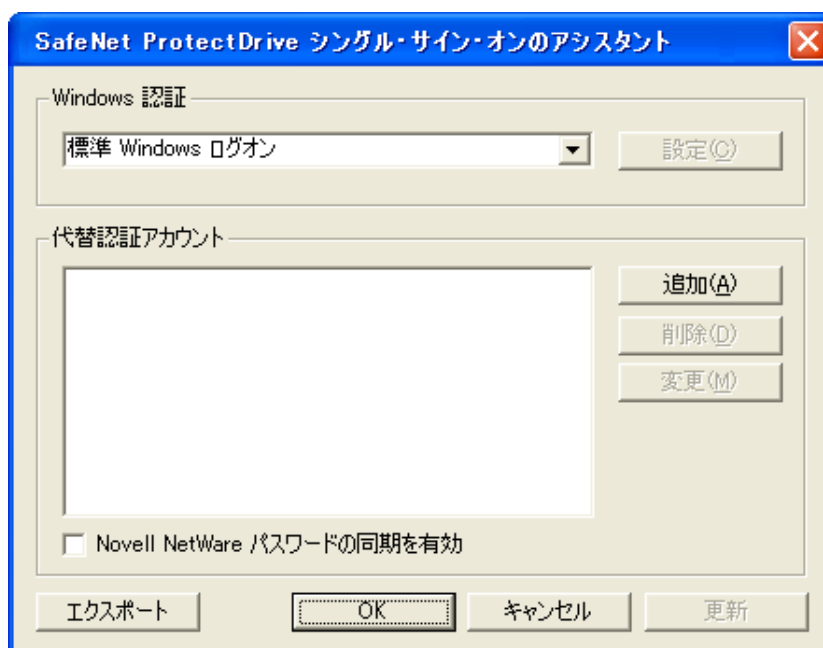
はじめに

シングル・サイン・オン・アシスタントは、ProtectDrive のシングル・サイン・オン全般を管理するためのアプリケーションです。このアプリケーションにより、ユーザはマシンおよびその他のネットワーク・サービスへのログオンを柔軟に設定できます。

シングル・サイン・オン・アシスタントは、Windows 認証アカウントおよび認証済みアカウントという 2 つのコンポーネントを管理します。これらのアカウントについては次の項で説明します。

シングル・サイン・オン・アシスタントにアクセスする

シングル・サイン・オン・アシスタントへアクセスするには、**ssoassistant.exe** ファイルを実行します。このファイルは、インストール・フォルダ（*C:\Program Files\SafeNet ProtectDrive*）にあります。



Windows 認証

Windows 認証のフィールドでは、ProtectDrive で使用する GINA を選択してください。選択できる項目は次のとおりです。

- **標準 Windows ログオン** (msgina.dll)
- **RSA サイン・オン・マネージャ・ログオン** または **RSA セキュア・ログオン** (3-gina.dll)
- **サードパーティ・ログオン**

ProtectDrive は Windows の GINA および RSA セキュリティ（次の **RSA SOM サポート** の項を参照）の GINA をサポートしますが、サードパーティ・ログオンについては、設定する必要があります。

サードパーティ製の GINA を設定すると、GINA DLL を選択し、GINA のダイアログおよびコントロール ID を手動で入力できます。Windows のブート中にアクセスするため、これらの設定は pcvgina.dll のレジストリに保存されます。

認証済みアカウント

認証済みアカウントにより、ユーザはネットワーク・サービスがある複数のアカウントにログオンできます。通常、認証済みアカウントは Novell ネットワークに接続するために使用しますが（67 ページの **Novell クライアント・サポート** の項を参照）、認証済みアカウントを使用することにより、その他の特有なユーザ設定においてもメリットを得られます（68 ページの「サードパーティ製品のサポート」の項を参照）。

各アカウントに追加できるフィールド数に制限はありません。必要な情報（ユーザ名、パスワード、またはドメイン）を入力するアプリケーション・ダイアログ・ボックス内のコントロールを指定し、それぞれのフィールドを設定します。プリブート・ユーザのアカウントの詳細はログオン用に使用するため、ユーザ名、パスワード、およびドメイン名は一致する必要があります。

Windows にログオンするためには、それぞれのアカウントにコマンドを追加します。アプリケーション・ダイアログ・ボックス上のボタンを選択してください。このボタンはログオン・アクションを行う際に使用します。

RSA SOM のサポート

概要

RSA サイン・オン・マネージャ (SOM) は、多くの企業向けアプリケーションでシングル・サイン・オンを行うアプリケーションです。ProtectDrive を RSA SOM と連携させるとことで、大きな効果が得られます。本項では、その方法について説明します。

導入

ProtectDrive GINA (pcvgina.dll) を RSA SOM GINA と組み合わせる (チェーンさせる) ことにより、RSA SOM は ProtectDrive によってサポートされます。チェーンにより RSA SOM は正しく機能し、一方でプリブート・ユーザはシングル・サイン・オンが可能です。

チェーンされた GINA レジストリの値が RSA SOM GINA に設定されると、ProtectDrive GINA は、RSA SOM GINA ダイアログ設定をロードします。この処理は、ProtectDrive シングル・サイン・オン・アシスタントを使用して設定できます。

考察

ここでは、シングル・サイン・オン・アシスタントおよび ProtectDrive GINA は、RSA SOM GINA が標準の場所 (C:\Program Files\RSA Security\RSA Sign-On Manager Client\3-Gina.dll) にあることを想定しています。

上記の場所がない場合、サードパーティ GINA のサポートは、次のダイアログ設定で、シングル・サイン・オン・アシスタント内で使用する必要があります。

タブ	フィールド	値
注意	ダイアログ ID	100
ログオン	ダイアログ ID	113
	ユーザ名コントロール ID	1000
	パスワード・コントロール ID	1008
	ドメイン・コントロール ID	1009
パスワードの変更	ダイアログ ID	800
Ctrl+Alt+Del	ダイアログ ID	400
ロックされた	ダイアログ ID	200
ロック解除	ダイアログ ID	106
	ユーザ名コントロール ID	1000
	パスワード・コントロール ID	1002
	ドメイン・コントロール ID	1009
シャットダウン	ダイアログ ID	500

サードパーティ製品のサポート

概要

ProtectDrive とともによく使用されるサードパーティ製品は多数あります。ProtectDrive が、それぞれの製品の直接サポートを必要とせずに、これらの製品用にシングル・サイン・オンを行えば、大きな効果が得られます。

本項では、シングル・サイン・オン・アシスタントを使用して、簡単に柔軟に、ProtectDrive でサードパーティ製品のシングル・サイン・オンを行う方法について説明します。

サードパーティ GINA のサポート

ProtectDrive GINA では、サードパーティ GINA をチェーンできます。ここでは、チェーンされた GINA のダイアログは、シングル・サイン・オン・アシスタントを使用して設定され、レジストリに保存されます。ProtectDrive GINA はこの設定をブート時にロードし、シングル・サイン・オンを行います。

GINA の置き換えは非常に自由度が高く、この方法がすべてのサードパーティ GINA で有効であるという保証はありません。しかし、GINA 用の「正しく機能する」シングル・サイン・オンであれば可能です。

この段階では、シングル・サイン・オン・アシスタントを使用して、ダイアログおよびコントロール ID を手動で入力します。これらの情報は、サードパーティ製品の販売業者または製造業者から入手できます。認証済みアカウントで使用されるダイナミック・ディスカバリは、今後のリリースで追加される予定です。

サードパーティ製品アカウントのサポート

サードパーティ製品へのログオンは、認証済み用の方法を使用して行います。ここでは、ProtectDrive GINA およびチェーンされた GINA は Windows にログオンするために使用されます。その後、Windows シェルが初期化されるときに、それぞれのサードパーティ製品にログオンします。

これはサードパーティ製品にログオン・アプリケーションがある場合のみ可能です。その後、シングル・サイン・オン・アシスタントを使用して、認証済みアカウントを作成できます。認証済みアカウントを実行すると、ログオン・アプリケーションを使用して製品にログオンできます。

管理手順

既存システムへの ProtectDrive インストール後の設定

1. システムに ProtectDrive をインストールしてください。
2. 次のいずれかの処理を行います。
 - シングル・サイン・オン・アシスタント (`ssoassistant.exe`) を実行して SSO を設定してください。または
 - シングル・サイン・オン・アシスタントからエクスポートしたレジストリ・ファイル (*.reg) を実行し、SSO 構成をインポートしてください。

ProtectDrive システムにソフトウェアを追加インストールした後の設定

1. 置き換える GINA をインストールするソフトウェアを ProtectDrive システムにインストールして追加してください。
2. シングル・サイン・オン・アシスタントを実行してください。シングル・サイン・オン・アシスタントは、新規に置き換える GINA を検出し、置き換える GINA を ProtectDrive GINA にチェーンさせるかどうか尋ねます。
3. 次のいずれかの処理を行います。
 - GINA のチェーンを実行しないオプションを選択してください。このオプションを選択すると、セキュリティの警告が表示されます。ProtectDrive ではシングル・サイン・オンを行えず、このログオン方法を実行できません。または
 - 置き換える GINA をチェーンする場合、シングル・サイン・オン・アシスタントは GINA をチェーンし、ユーザは GINA を設定できます。

注意：ソフトウェアの追加インストール後は、シングル・サイン・オン・アシスタントを実行する必要があります。

チェーンされた GINA を変更する

1. シングル・サイン・オン・アシスタント (`ssoassistant.exe`) を実行してください。
2. シングル・サイン・オン・アシスタントで目的の GINA を選択してください。
3. サードパーティ GINA の場合、シングル・サイン・オン・アシスタントを使用して GINA の設定を指定する必要があります。
4. 次のいずれかの処理を行います。

- **[OK]** または **[適用]** をクリックすると、シングル・サイン・オン・アシスタントは GINA の選択を確定できます。

または

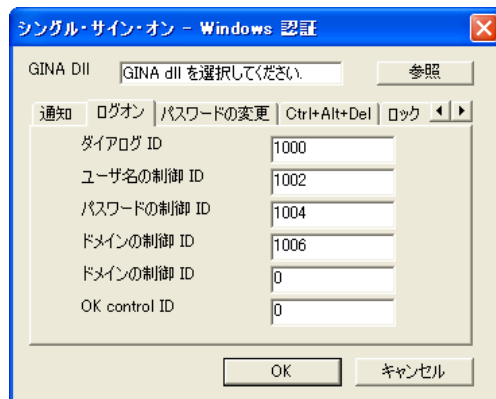
- **[キャンセル]** を選択すると、新規に選択した GINA は削除されます。

5. シングル・サイン・オン・アシスタントを終了してください。

GINA を設定する

1. シングル・サイン・オン・アシスタントを実行してください。
2. サードパーティ GINA を選択してください（標準 Windows GINA および RSA GINA は自動的に設定されます）。
3. **[設定]** をクリックしてください。
4. GINA DLL のファイル名および場所を参照してください。
5. ProtectDrive GINA に関連する各 GINA のダイアログ（**[通知]**、**[ログオン]**、**[パスワードの変更]** など）に対し、サードパーティ GINA 用のダイアログおよびコントロール ID を指定してください（以下を参照）。

ID を指定しない場合、ProtectDrive GINA で予期せぬ動作が起こる可能性があるという警告メッセージが表示されます。



6. 次のいずれかの処理を行います。
 - **[OK]** をクリックしてください。設定が保存されます（ただし、確定されません）。または
 - **[キャンセル]** をクリックしてください。設定が破棄されます。
7. **[GINA 設定]** ダイアログが閉じ、メインの **[シングル・サイン・オン・アシスタント]** ダイアログ・ボックスが表示されます。
8. 次のいずれかの処理を行います。

- **[適用]** または **[OK]** をクリックしてください。設定が確定されます。

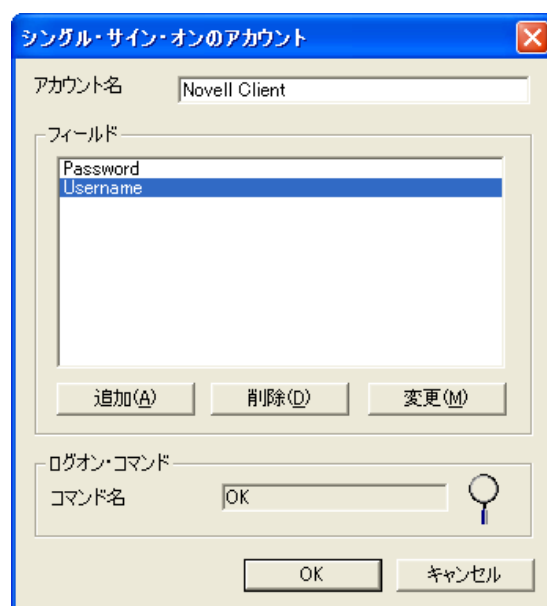
または

- **[キャンセル]** をクリックしてください。設定が破棄されます。

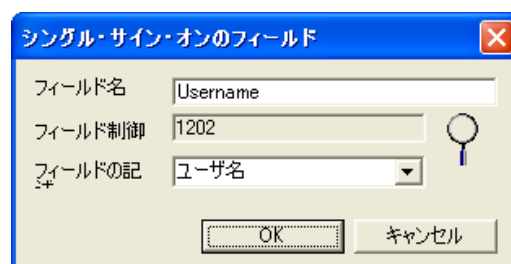
9. シングル・サイン・オン・アシスタントを終了してください。

認証済みアカウントを作成する

1. シングル・サイン・オン・アシスタントを実行してください。
2. **[追加]** をクリックして新しいアカウントを作成してください。[シングル・サイン・オン・アカウント] ダイアログ・ボックスが表示されます。



3. **[アカウント名]** フィールドで一意的な名前を指定してください。
4. アプリケーションを実行してください。これにより、認証済みアカウントのログオンが実行されます。
5. [シングル・サイン・オン・アカウント] ダイアログ・ボックスで **[追加]** をクリックしてください。
[シングル・サイン・オン・フィールド] ダイアログ・ボックスが表示されます。



6. 虫メガネ・アイコンもしくはカーソルを [シングル・サイン・オン・フィールド] ダイアログ・ボックスからアプリケーション・ログオン画面上で必要なフィールドへドラッグしてください。

上記のスクリーン・ショットが示すように、[フィールド名] および [フィールド・コントロール] の詳細が、[シングル・サイン・オン・フィールド] ダイアログ・ボックスに表示されます。
7. [フィールドに入力する値を選択] フィールドで適宜選択し、[OK] をクリックしてください。
8. 追加するフィールドごとに手順 5 から 7 を繰り返してください。
9. [シングル・サイン・オン・アカウント] ダイアログ・ボックスから、虫メガネ・アイコンもしくはカーソルをアプリケーションのボタン上にドラッグして、ログオン・コマンド（アプリケーション上にあるログオンを行うボタン）を選択してください。
10. 次のいずれかの処理を行います。
 - [OK] をクリックしてください。アカウントが確定されます。

または
 - [キャンセル] をクリックしてください。アカウントが作成されません。
11. [シングル・サイン・オン・アカウント] ダイアログ・ボックスが閉じ、メインの [シングル・サイン・オン・アシスタント] ダイアログ・ボックスに戻ります。
12. 次のいずれかの処理を行います。
 - [OK] をクリックしてアカウントを確定してください。

または
 - アカウントを作成しない場合は [キャンセル] をクリックしてください。
13. シングル・サイン・オン・アシスタントを終了してください。

認証済みアカウントを変更する

1. シングル・サイン・オン・アシスタントを実行してください。
 2. [認証済みアカウント] のリストから変更するアカウントを選択し、[変更] をクリックしてください。[シングル・サイン・オン・アカウント] ダイアログ・ボックスにアカウント情報が表示されます。
 3. アカウント情報を必要に応じて変更してください。
-

4. 次のいずれかの処理を行います。
 - **[OK]** をクリックして新しいアカウント情報を保存してください。
 - または
 - **[キャンセル]** をクリックしてアカウント情報を破棄してください。
5. [シングル・サイン・オン・アカウント] ダイアログ・ボックスが閉じ、[シングル・サイン・オン・アシスタント] ダイアログ・ボックスに戻ります。
6. 次のいずれかの処理を行います。
 - **[OK]** をクリックして新しいアカウント情報を確定してください。
 - または
 - **[キャンセル]** をクリックして新しいアカウント情報を破棄してください。
7. シングル・サイン・オン・アシスタントを終了してください。

認証済みアカウントを削除する

1. シングル・サイン・オン・アシスタントを実行してください。
2. **[認証済みアカウント]** のリストから変更するアカウントを選択し、**[削除]** をクリックしてください。
3. 次のいずれかの処理を行います。
 - **[OK]** をクリックしてアカウントの削除を確定してください。
 - または
 - アカウントを削除しない場合は **[キャンセル]** をクリックしてください。
4. シングル・サイン・オン・アシスタントを終了してください。

認証済みアカウント・フィールドを作成する

1. シングル・サイン・オン・アシスタントを実行してください。
2. **[追加]** をクリックして新しいアカウントを作成するか、または **[変更]** をクリックして既存のアカウントを変更してください。
3. 認証済みアカウント・ログオンを行うアプリケーションを実行してください。[シングル・サイン・オン・アカウント] ダイアログ・ボックスが表示されます。
4. **[追加]** をクリックしてください。[シングル・サイン・オン・フィールド] ダイアログ・ボックスが表示されます。
5. **[アカウント名]** で一意のアカウント名を指定してください。

6. 虫メガネ・アイコンもしくはカーソルを、アプリケーション内で入力するコントロールヘッドラッグし、フィールド・コントロールを選択してください。
7. フィールドに入力する情報を選択してください。
8. 次のいずれかの処理を行います。
 - **[OK]** をクリックしてアカウント内のフィールドを保存してください。または
 - **[キャンセル]** をクリックして新しいフィールドを破棄してください。
9. [シングル・サイン・オン・フィールド] ダイアログ・ボックスが閉じ、アカウントのダイアログ・ボックスに戻ります。
10. 次のいずれかの処理を行います。
 - **[OK]** をクリックしてアカウントを保存してください。または
 - **[キャンセル]** をクリックして新しいアカウント情報を破棄してください。
11. [シングル・サイン・オン・アカウント] ダイアログ・ボックスが閉じ、[シングル・サイン・オン・アシスタント] ダイアログ・ボックスに戻ります。
12. 次のいずれかの処理を行います。
 - **[OK]** をクリックしてアカウントを確定してください。または
 - **[キャンセル]** をクリックしてアカウントを破棄してください。
13. シングル・サイン・オン・アシスタントを終了してください。

認証済みアカウント・フィールドを変更する

1. シングル・サイン・オン・アシスタントを実行してください。
 2. **[変更]** をクリックして既存のアカウントを変更してください。
 3. 認証済みアカウント・ログオンを行うアプリケーションを実行してください。[シングル・サイン・オン・アカウント] ダイアログが表示されます。
 4. **[変更]** をクリックしてください。[シングル・サイン・オン・フィールド] ダイアログ・ボックスが表示されます。
 5. ファイル情報を変更してください。
-

6. 次のいずれかの処理を行います。
 - **[OK]** をクリックしてアカウント内の変更済みフィールドを保存してください。
 - または
 - **[キャンセル]** をクリックして新しいフィールド情報を破棄してください。
7. [シングル・サイン・オン・フィールド] ダイアログ・ボックスが閉じ、[シングル・サイン・オン・アカウント] ダイアログ・ボックスに戻ります。
8. 次のいずれかの処理を行います。
 - **[OK]** をクリックしてアカウントを保存してください。
 - または
 - **[キャンセル]** をクリックして新しいフィールド情報を破棄してください。
9. [シングル・サイン・オン・アカウント] ダイアログが閉じ、[シングル・サイン・オン・アシスタント] ダイアログ・ボックスに戻ります。
10. 次のいずれかの処理を行います。
 - **[OK]** をクリックして新しいフィールド情報を確定してください。
 - または
 - **[キャンセル]** をクリックしてアカウントを破棄してください。
11. シングル・サイン・オン・アシスタントを終了してください。

認証済みアカウント・フィールドを削除する

1. シングル・サイン・オン・アシスタントを実行してください。
2. **[変更]** をクリックして既存のアカウントを変更してください。
3. 認証済みアカウント・ログオンを行うアプリケーションを実行してください。[シングル・サイン・オン・アカウント] ダイアログ・ボックスが表示されます。
4. **[削除]** をクリックしてください。
5. 次のいずれかの処理を行います。
 - **[OK]** をクリックしてアカウントからフィールドを一時的に削除してください。
 - または
 - **[キャンセル]** をクリックしてアカウント内のフィールドを維持してください。
6. [シングル・サイン・オン・アカウント] ダイアログ・ボックスが閉じ、メインの [シングル・サイン・オン・アシスタント] ダイアログ・ボックスに戻ります。

7. 次のいずれかの処理を行います。
 - **[OK]** をクリックしてアカウントからフィールドを半永久的に削除してください。
または
 - **[キャンセル]** をクリックしてアカウント内のフィールドを維持してください。
8. シングル・サイン・オン・アシスタントを終了してください。

SSO 設定をエクスポートする

1. シングル・サイン・オン・アシスタントを実行してください。
 2. **[エクスポート]** をクリックしてください。
 3. 設定をエクスポートするファイルを参照して **[保存]** をクリックしてください。
 4. シングル・サイン・オン・アシスタントのレポートのエクスポートが完了したら **[OK]** をクリックしてください。
-

第7章 マルチブート・システム

注意：ProtectDrive バージョン 8.5 では、マルチブート・システムはサポートされていません。

第8章 システムおよびユーザ・ポリシーの設定

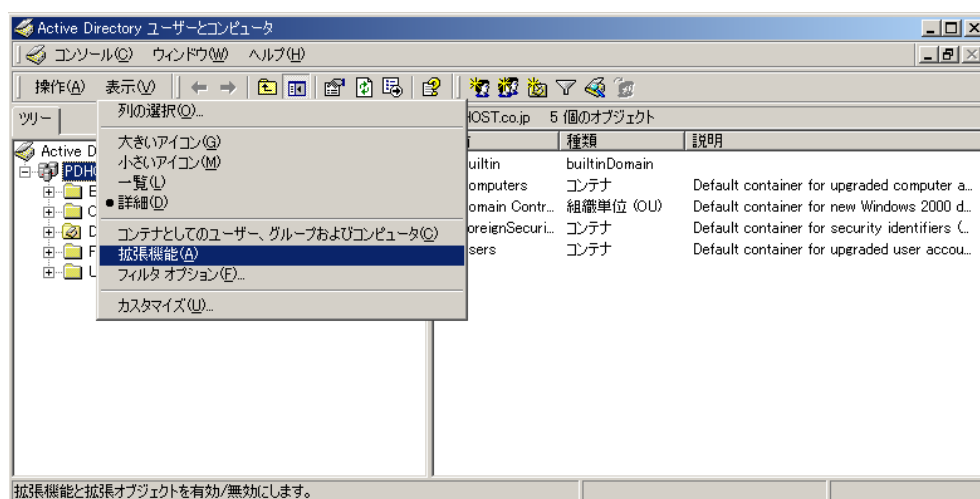
ProtectDrive では、デフォルトのシステムおよびユーザ・ポリシーのインスタンスが Active Directory もしくは ADAM に保存されます。Windows ドメインで新しいコンピュータ・アカウントを作成すると、毎回保存されたデフォルト設定が自動的に適用されます。

自己管理の ProtectDrive クライアントは、**Active Directory ユーザとコンピュータ(ADUC) MMC** スナップインで、**ProtectDrive Management Console** で管理されます。標準の設定オブジェクトもしくは、他のオブジェクトに関連付けられているクライアントを ProtectDrive Management Console によって管理することが可能です。

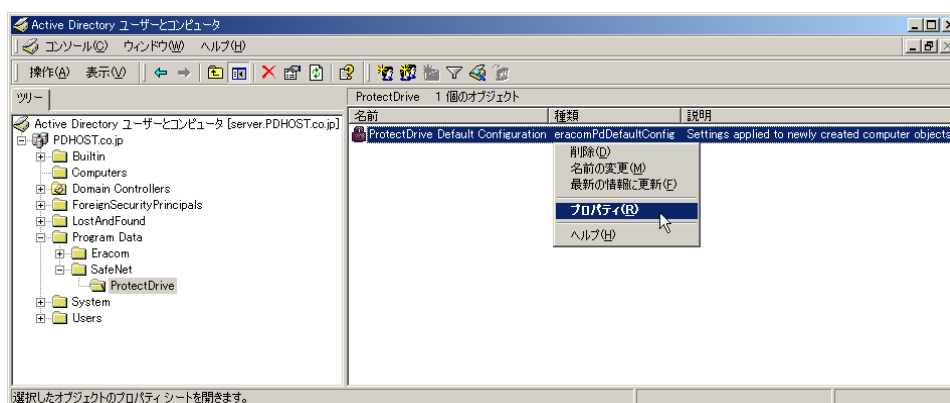
Active Directory ユーザとコンピュータ(ADUC) MMC スナップインの標準設定

ProtectDrive インストール直後に、ProtectDrive を直ぐに初期設定するため、ADUC MMC スナップインを使用します。設定後の設定変更は、ProtectDrive Management Console を使用してください。

1. サーバで **ProtectDrive Management Console** を起動してください。
2. **Active Directory ユーザとコンピュータ MMC** スナップインを開いてください。
3. **[拡張機能]** を選択してください。



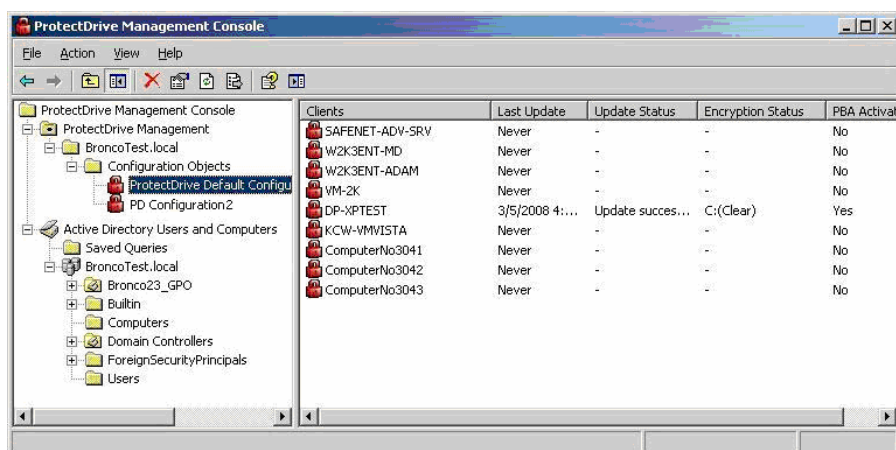
4. **[プログラム・データ] > [SafeNet] > [ProtectDrive] > [ProtectDrive のデフォルト設定]** の順に移動して **[プロパティ]** を選択してください。



5. **[PD 設定]** タブを選択してデフォルトのシステム・ポリシーを設定してください。[PD 設定]に関しては、80 ページを参照してください。
6. **[PD ユーザ]** タブを選択すると、デフォルトでユーザがシステムに割り当てられ、そのユーザのデバイスへのアクセス制御に関するアクセス許可が設定されます。[PD ユーザ]に関しては、95 ページを参照してください。
7. **[適用]** をクリックしてください。
8. **[OK]** をクリックしてください。

ProtectDrive Management スナップインの標準設定

1. サーバで **ProtectDrive Management Console** を起動してください。
2. **ProtectDrive Management** フォルダから、設定オブジェクトを開いてください。



3. **ProtectDrive Default Configuration** を右クリックして、**[プロパティ]**を選択してください。
4. **[PD 設定]** タブを選択してデフォルトのシステム・ポリシーを設定してください。[PD 設定]に関しては、80 ページを参照してください。

5. **[PD ユーザ]** タブを選択すると、デフォルトでユーザがシステムに割り当てられ、そのユーザのデバイスへのアクセス制御に関するアクセス許可が設定されます。 **[PD ユーザ]** に関しては、95 ページを参照してください。
6. **[適用]** をクリックしてください。
7. **[OK]** をクリックしてください。

PD 設定 タブ（デフォルトのシステム・ポリシー）

認証の設定

暗号化 | 認証 | 高度

☒ プリブート認証を有効

認証方法

	Windows	プレブート
ローカル・ユーザのアクセスを許可	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
パスワード・ドメイン・ユーザのアクセスを許可	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
トークン・ドメイン・ユーザのアクセスを許可	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
共通鍵アクセスを許可	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> シングルサインオン		

プレブートのアクセス管理

☒ ユーザ名を使用した緊急ログオンを許可

☒ 緊急ログオン後のシングルサインオン

☒ ユーザ名なしでの緊急ログオンを許可

☐ トークンユーザの緊急ログオンを許可

☐ 共通鍵の登録を許可

☒ Windows ログオン時にユーザを SafeNet ProtectDrive へ追加

プリブート認証を有効

クライアントでディスクの暗号化とプリブート認証を行うには、ProtectDrive でこのチェック・ボックスをオンにする必要があります。

ProtectDrive をアンインストールせずに無効にするには、このチェック・ボックスをオフにしてください。これで、ディスク暗号化など、ProtectDrive のすべての機能が無効になります。このチェック・ボックスをオフにすると、**[認証]** タブでその他の設定を変更できますが、**[プリブート認証を有効]** チェック・ボックスを再度オンにして ProtectDrive を有効にするまで変更は反映されません。この機能が有効かどうかを確認するには、**[動作可]**、**[未決定]**、**[動作不可]** のいずれかのインジケータを参照してください。これらのインジケータは **[プリブート認証を有効]** チェック・ボックスの右側にあります。次に例を示します。

☒ プリブート認証を有効 **未決定**

表示されるステータス・メッセージは、次のとおりです。

動作可	プリブート認証が有効です。
未決定	サーバで現在設定されている状態をクライアントが更新するのを待っている状態です。
動作不可	プリブート認証が無効です。プリブート認証を無効にすると、それまで暗号化されていたドライブが復号化されます。

注意：プリブート認証を無効にすると、ユーザがすべてクライアント・システムの ProtectDrive プリブート・ユーザ・データベースから削除されます。Windows ドメインのユーザは、プリブート認証を再度有効にすると自動的に追加されます。ただし、ローカルの Windows ユーザの場合、自動的に追加してプリブート認証を実行することができません。ローカルの Windows ユーザは、プリブート認証を再度有効にしてから手動で追加する必要があります。

認証方法

ProtectDrive で保護されたシステムにアクセスするには、プリブートと Windows の両方のアクセス・レベルで認証を実行する必要があります。

ローカル・ユーザ、パスワード・ドメイン、およびトークン・ドメインの認証方法の組み合わせは、プリブートと Windows の両方のアクセス・レベルのユーザが使用できます。使用できる組み合わせは、[認証方法]グループ・ボックスで行う設定に応じて決まります。これらの認証方法については、以下で詳しく説明します。

ユーザが認証方法を使用できるようにするには、組織が適用するセキュリティ・ポリシーの要件に応じて、認証方法の隣にある [Windows] または [プリブート] の一方または両方のチェック・ボックスをオンにします。いずれの認証方法でも、[Windows] と [プリブート] の両レベルで最低 1 つのチェック・ボックスをオンにする必要があります。

注意：もし、Windows のログオンのためのトークンのドライバがインストールされていない場合には、トークンおよびスマートカードを使用した Windows ログオンおよび認証のみを許可するように、ProtectDrive を設定しないでください。

もしそのような ProtectDrive 設定を行った場合には、PC がロックされます。PD はトークンでのログオンを許可するだけで、パスワードでそれをアンロックする方法がなくなるためです。ProtectDrive でトークンのみでのアクセスを設定する前に、管理者は、PBA および Windows ログオン（とアンブロック）で確実にトークンが利用できるかを確認する必要があります。

ローカル・ユーザの アクセスを許可	デフォルトで有効になっているこの認証方法により、ローカル Windows ユーザは、ローカル Windows ユーザ名、パスワード、およびローカル・システム名を使用してシステムを認証できます。 ローカル Windows ユーザは、ローカル管理コンソール・ユーティリティを使用して追加するか、または、この [認証] 画面の下で [Windows ログオン時にユーザを ProtectDrive へ追加] を設定している場合、Windows ログオンを使用して追加できます。ローカル Windows ユーザをサーバからクライアント・システムのユーザ・データベースへ追加することはできません。
パスワード・ドメイン・ ユーザのアクセスを許可	この方法により、Windows ドメインのユーザは、Windows ドメインのユーザ名、パスワード、およびドメイン名を使用してシステムを認証できます。
トークン・ドメイン・ ユーザのアクセスを許可	この方法により、Windows ドメインのユーザはスマートカードとトークンおよび PIN を認証に使用できます。
共通鍵アクセスを 許可 (iKey 1000 のみ対 応)	この方法により、共通鍵 (非 PKI) ユーザのプリブート認証が可能になります。このオプションを選択する場合、最低 1 つ Windows 認証方法を選択する必要があります。

トークン・ドメイン・ユーザのアクセスを唯一の認証方法とする場合の注意事項

[トークン・ドメイン・ユーザのアクセスを許可] を唯一有効な認証方法とする場合は、注意が必要です。

次のオプションをすべて無効にすると、スマートカードおよびトークンがプリブート時のシステム認証の唯一の手段となってしまいます。**[ローカル・ユーザのアクセスを許可]**、**[パスワード・ドメイン・ユーザのアクセスを許可]**、**[新規ユーザの追加を許可]**。

スマートカードおよびトークンに問題が発生した場合、システムにアクセスできなくなる場合があります。このため、一時的に **[ローカル・ユーザのアクセスを許可]**、**[パスワードのフォールバックを許可]**、または **[新規ユーザの追加を許可]** を有効にすることをお勧めします。こうすることで、スマートカードおよびトークンの信頼性を回復して ProtectDrive で正しく使用できるように設定するまで、プリブート認証の代替方法を最低 1 つ使用できます。

シングル・サイン・オン

シングル・サイン・オン・モードの場合、ユーザは 1 回ログオンするだけで、プリブート認証と Windows レベルの認証を実行できます。このオプションは、プリブートと Windows の両方のアクセス・レベルで、最低 1 つの認証方法を有効にした場合のみ使用できます。

シングル・サイン・オン・モードを有効にするには、**[シングル・サイン・オン]** チェック・ボックスをオンにしてください。

プリブートのアクセス管理

[ローカル・ユーザのアクセスを許可] および [パスワード・ドメイン・ユーザのアクセスを許可] チェック・ボックスを選択したときに、[プリブート] レベルで認証を有効にすると、[プリブートのアクセス管理] 設定を使用できます。

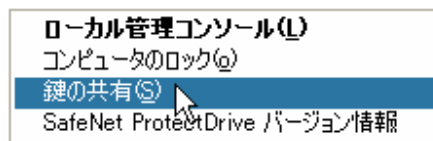
以下で [プリブートのアクセス管理] 設定について説明します。

- | | |
|--------------------------------------|---|
| ユーザ名を使用した
緊急ログオンを許可 | <p>このオプションを有効にすると、ユーザはプリブート・パスワードの復旧手順を呼び出すことができます。この手順は、ユーザが Windows（ドメイン）のパスワード（PIN は未対応）を忘れた場合に使用します。Windows ドメインおよびローカルのパスワードが ProtectDrive に追加されるためです。</p> <p>この手順により、1 回だけプリブート時にシステムへアクセスできます。</p> |
| 緊急ログオン後のシ
ングル・サイン・オ
ン | <p>このオプションを有効にすると、プリブート・パスワードの復旧手順の実行直後に、プリブート時に自動的にユーザの Windows 認証が行われます。</p> <p>[プリブートのアクセス管理] グループ・ボックスをオンにすると、[ローカル・ユーザのアクセスを許可] および [パスワード・ドメイン・ユーザのアクセスを許可] チェック・ボックスをオンにしている、Windows レベルでの認証が有効な場合に、このオプションを選択できるようになります。</p> |
| ユーザ名なしでの緊
急ログオンを許可 | <p>このオプションを有効にすると、新規作成された Windows ドメインまたはローカル Windows ユーザは、プリブート時の新規ユーザの追加手順を呼び出すことができます。</p> <p>この手順により、ProtectDrive のプリブート・ユーザ・アカウントを持たないユーザでも、1 回だけプリブート時にシステムへアクセスできます。</p> |
| トークン・ユーザの
緊急ログオンを許可 | <p>（少なくとも以下のプリブート認証方法のオプションの 1 つが選択される場合にだけ、このオプションは利用可能です。トークン・ドメイン・ユーザのアクセスを許可か共有鍵アクセスを許可を設定してください。）</p> <p>このオプションを有効にすると、スマートカードもしくはトークンのユーザ（トークンをなくしたり、PIN を忘れたり）がトークンの利用手順のために、緊急ログインを許可します。</p> <p>この方法は、トークンなしでシステムへのワнтаイムでのプリブート認証機能を提供します。</p> |

共通鍵の登録を許可

このオプションを有効にすると、ユーザは認証用の共通鍵を登録できます。

さらに、ProtectDrive システム・トレイのアイコンを開いたときに **[共通鍵]** メニュー選択画面（右側に表示）を含めるには、このオプションを有効にする必要があります。



Windows ログオン時にユーザを ProtectDrive へ追加

このオプションを有効にすると、新しいユーザの ProtectDrive のプリブート・ユーザ・アカウントがまだ作成されていない場合は、Windows へのログオン時に作成されます。

この機能は、**[ローカル・ユーザのアクセスを許可]**、**[ドメイン・ユーザのアクセスを許可]** または **[トークン・ドメイン・ユーザのアクセスを許可]** の設定により異なります。実行する Windows ログオンの種類に対応する設定が行われている場合のみ、ProtectDrive のプリブート・ユーザ・データベースのユーザに対してエントリが作成されます。

高度の設定 — 証明書の利用



このオプションは、プリブート認証での認証トークンやスマートカードでの証明書の利用に関する設定を行います。

使用

[使用] をクリックすると現在使用可能な証明書のリストが表示されます。それぞれの証明書は名前とオブジェクトの識別子（OID）で表示されます。OID は、プリブート認証で証明書が正しく使用できるかなどを表す数列で表記されています。

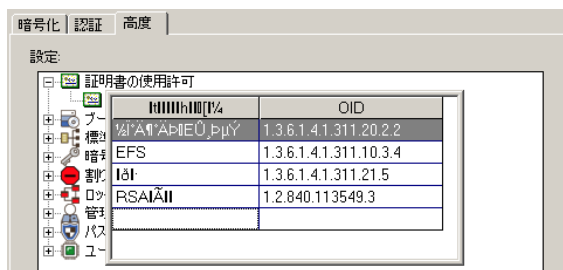
注意：バージョン 8.5 の ProtectDrive の日本語環境では、それぞれの証明書の値が正しく表示されていませんが、機能的には問題ありません。表示内容は、“名前”、“Smart Card Logon”、“EFS”、“Exchange”、“RSA Encryption” です。

それぞれの項目の内容は、下記の通りです。

- **Smart Card Logon** — このオプションを選択すると Windows ログオンで Smart Card Logon が有効となります。
- **EFS** — このオプションを選択すると暗号化ファイル・システム用にサードパーティ製の認証局 (CA) の使用を許可することができます。
- **Exchange** — このオプションを選択すると秘密鍵もしくは、証明書の使用を許可することができます。
- **RSA Encryption** — このオプションを選択する Windows の暗号化に RSA 方式を使用することを許可することができます。

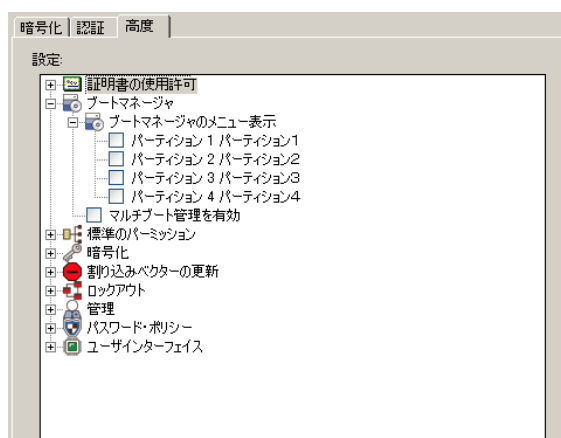
全てもしくは一部の使用を有効にすることができます。また、手動で追加することも可能です。利用できる証明書は、反転表示されます。

- 既存の証明書の許可は、設定する証明書の名前もしくは OID で右クリックし、[Select]を選択してください。選択されると、反転表示されます。



- 選択されている証明書を解除する場合には、設定する証明書の名前もしくは OID で右クリックし、[Unselect]を選択してください。選択されると、通常表示となります。
- 手動で証明書を追加する場合には、空白行をダブルクリックして、名前と OID を入力してください。入力された証明書は、自動で利用可能となります。
- 手動で登録した証明書は、[Unselect]で使用を解除することはできないため、右クリックして、[Delete]を選択して削除してください。

高度の設定 — ブート・マネージャ



注意：バージョン 8.5 では、マルチブート機能は、利用できません。

このグループを使用すると、システムをマルチブート構成にして、マルチブート構成の状態を確認できます。サポートされるブート可能パーティションは、最大 4 つです。マルチブートをいったん有効にすると、以降は無効にすることができません。マルチブート・システムの導入前に、[第 7 章](#)—「マルチブート・システム」の記載の重要な情報を読んで検討してください。

ブート管理メニューの表示文字

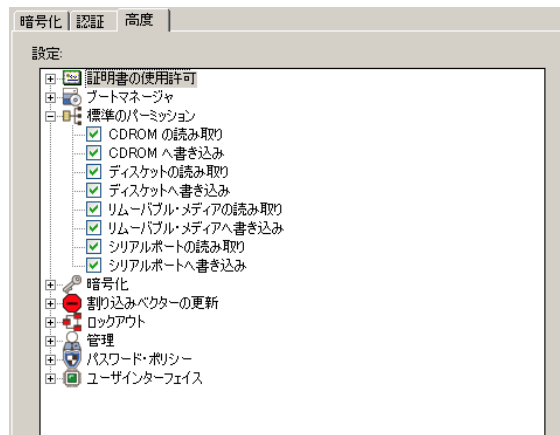
これらのフィールドに入力するテキスト文字列は、マルチブート・メニューでパーティション・メニューのラベルとして表示されます。表示されるテキスト文字列の隣にある **[ブートを有効]** チェック・ボックスをオンにしてください。パーティションが存在していてこのチェック・ボックスがオンになっていれば、システムのブート時にそのパーティションがマルチブート・メニューに表示されます。パーティションが存在していてこのチェック・ボックスが**オフ**になっていれば、システムのブート時にそのパーティションがマルチブート・メニューに表示されません。

パーティションのラベルとブート可能なパーティションを指定する ProtectDrive の最新インストールにより、それまでの割り当てが上書きされるため、マルチブート・メニューに表示されるパーティションとその関連メニュー文字列については、事前にメモを取っておいてください。これまでシステムにインストールされていた ProtectDrive は、ブリブート時のコンポーネント・インストール中および以降のクライアント更新時に、最新の情報により更新されます。パーティションが存在せず、ProtectDrive がすでにシステムにインストールされている場合、最近使用した ProtectDrive パーティションのブート・メニュー情報により、新しいインストールが更新されます。

マルチブート管理を有効化

このチェック・ボックスは情報提供のみを目的としています。つまり、このチェック・ボックスは読み取り専用です。このチェック・ボックスをオンにすると、システムで複数のプライマリ・パーティションがブート可能になっていることを示します。つまり、マルチブート・ウィンドウがシステムのブート時に毎回表示されるということです。

高度の設定 — 標準のパーミッション（デバイスへのアクセス）

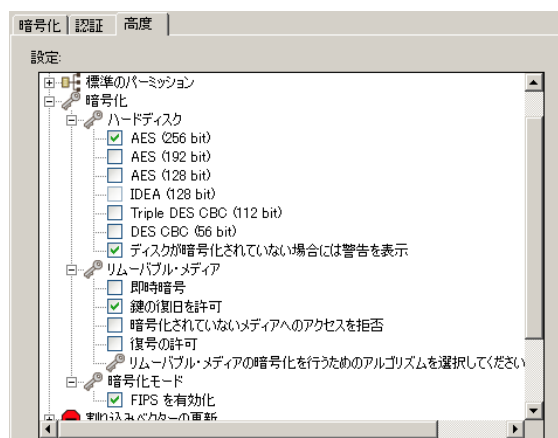


標準のパーミッション は、**[PD ユーザ]** タブで個々のユーザ・ポリシーが明確に定義されていないユーザのみに適用されます。実際に、**[PD ユーザ]** タブで定義される個々のユーザ・ポリシー設定は、**標準のパーミッション** よりも優先されます。

たとえば、Windows ログオン後にユーザが ProtectDrive のプリブート・ユーザ・データベースに追加されます（**認証** タブの **[Windows ログオン時にユーザを ProtectDrive へ追加]** オプションを参照してください）。

このユーザが **[PD ユーザ]** タブを使って明確にシステムへ追加されていない場合、このユーザのデバイスのシステム・リソースへのアクセス許可は、**標準のパーミッション** グループの設定により異なります。

高度の設定 — 暗号化



ハードディスク

ProtectDrive の暗号化中にユーザが使用できる暗号化アルゴリズムを選択してください。ここでユーザが選択するアルゴリズムは、**暗号化ステータス** グループにアルゴリズムの選択肢として表示されます。

ディスクが暗号化されていない場合には警告を表示

このオプションはデフォルトで有効になっています。このオプションを有効にすると、すべてのユーザにディスクの暗号化が不完全である状態を通知する警告メッセージが表示されます。この ProtectDrive 警告メッセージは Windows ログオンの直後に表示されます。

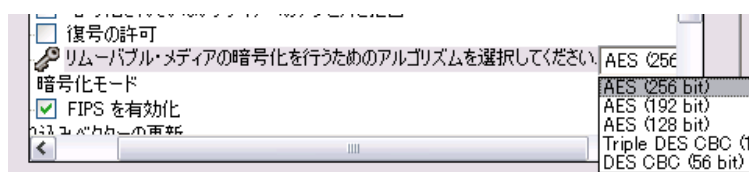
リムーバブル・メディア

ここでは、すべてのリムーバブル・メディアに適用されるオプションを選択してください。

即時暗号	このオプションを有効にすると、保護されていない（暗号化されていない）リムーバブル・メディアが挿入された場合に、メディアを暗号化するかどうか確認するためのプロンプトが表示されます。
鍵の復旧を許可	このオプションを有効にすると、ユーザがパスワードを忘れた場合などに、保護されたリムーバブル・メディアへ再度アクセスできるようになります。
暗号化されていないメディアへのアクセスを拒否	このオプションを有効にすると、暗号化されていないリムーバブル・メディアへのアクセスが拒否されます。このオプションの設定時にリムーバブル・メディアが接続されている場合、安全にデバイスを取り外してから再接続すると、設定が反映されます。
復号化の許可	（[暗号化されていないメディアへのアクセスを拒否] オプションが有効な場合、このオプションを使用できません。）このオプションを有効にすると、ユーザはリムーバブル・メディア・コンポーネントの復号化を実行できます。

リムーバブル・メディアの暗号化を行うためのアルゴリズムを選択してください

ProtectDrive でリムーバブル・メディアの暗号化中に使用するアルゴリズムを選択してください。



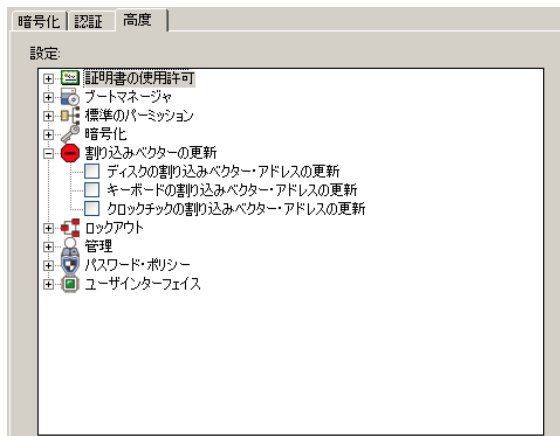
暗号化モード

FIPS モードのライブラリを使用するには、**[FIPS を有効化]** チェック・ボックスをオンにしてください。このオプションを選択すると、ハードディスクとリムーバブル・メディアの IDEA 暗号化アルゴリズムのオプションを使用できません。

もし、このオプションが選択されない場合には、FIPS モードのライブラリが使用されないため、パフォーマンスが向上し、CC EAL-2 の認定レベルとなります。

注意：もし、このオプションを変更した場合には、変更を有効にするために必ずリブートを行ってください。

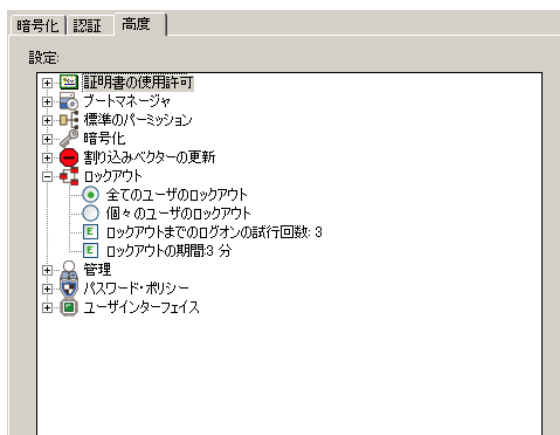
高度の設定 — 割り込みベクター（アドレス）の更新



ProtectDrive では、BIOS の割り込みベクター・アドレスの一部が保存されます。これにより、ProtectDrive で割り込みベクター・アドレスの変更によりマウントされる攻撃を検出できます。BIOS 割り込みベクター・アドレスと ProtectDrive に保存されたコピーの違いを ProtectDrive が検出すると、エラー・メッセージが表示されます。

割り込みベクター・アドレスの変更（BIOS の更新など）が行われると、このエラー・メッセージが表示されたままになります。**割り込みベクターの更新** グループは、ProtectDrive のディスク、キーボード、およびクロック・チップの割り込みベクター・アドレスのコピーを更新することにより、正規の変更を許可するメカニズムを提供します。

高度の設定 — ロックアウトの設定



ロックアウトの設定 グループを使用すると、パスワード推測攻撃を回避できます。ログオンの試行に連続で失敗すると、一定時間それ以上のログオン試行が禁止されます（ログオン試行の失敗やその他のイベントの詳細については、システムの **【イベント・ビューア】** を開いてください。**【イベント・ビューア】** の詳細については、144 ページを参照してください）。

全てのユーザのロックアウト もしくは 個々のユーザのロックアウト

これらの設定により、ログオン試行に連続して失敗した場合に、一定期間すべてのユーザ・アカウントをブロックするか、個々のユーザ・アカウントをブロックするかが決まります。デフォルトは [全てのユーザのロックアウト] です。

ロックアウトまでのログオンの試行回数

ProtectDrive では、プリブート・ログオン画面が表示された時点で、指定した回数ログオン試行に失敗すると、コンピュータがロックされます。デフォルトの値は 3 です。

ロックアウトの期間

この値により、システムへのアクセスまたは個々のアカウントがブロックされる期間が決まります。デフォルトの値は 3 分です。最大ロックアウト期間は 365 日です。

高度の設定 — 管理

このグループ設定では、ProtectDrive クライアントが、Active Directory もしくは ADAM の更新された情報をシステムおよびユーザ・ポリシーから、どのように検索するかを設定します。

注意：これらのオプションは、クライアントでの設定でインストールされた場合には、設定できないようになっています。



再起動を有効

このオプションを有効にした場合には、ProtectDrive は Active Directory および ADAM のポリシー・データをシステムの起動時に取得します。

ログオンを有効

このオプションを有効にした場合には、ProtectDrive は Active Directory および ADAM のポリシー・データを Windows ユーザ・ログオン時に取得します。

シャットダウンを有効

このオプションを有効にした場合には、ProtectDrive は Active Directory および ADAM のポリシー・データをシステムのシャットダウン時に取得します。

注意：Windows 証明書の自動登録（スマートカードおよびトークン利用時のみ）を使用する場合には、このオプションは新しい証明書発行時に、ProtectDrive のプリブート用のユーザ・データベース内の新しいエントリを作成するために、選択する必要があります。

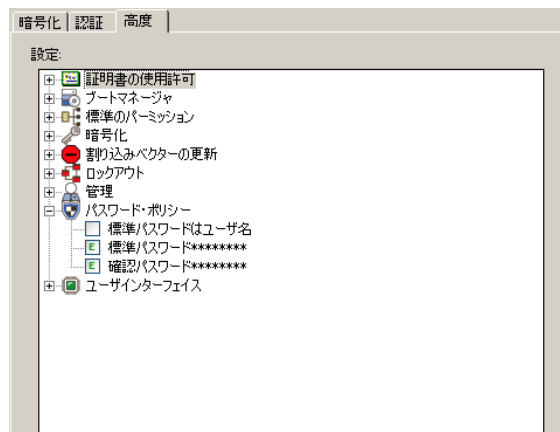
インターバルを有効

このオプションを有効にした場合には、ProtectDrive は Active Directory および ADAM のポリシー・データを**間隔**で指定された時間の間隔で取得します。

間隔

このオプションを選択し、ProtectDrive で Active Directory および ADAM のポリシー・データを取得する間隔を選択してください。

高度の設定 — パスワード・ポリシー



標準パスワードはユーザ名

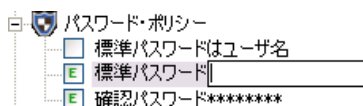
このオプションは、[標準パスワード] の指定に代わるオプションです。この場合、ユーザはプリブート認証時にパスワード（Windows のユーザ名）を手動で入力する必要があります。

パスワードがユーザ名である場合、使用できるのは初回のプリブート認証時のみで、以降は Windows（ドメイン）のパスワードに変わります。

注意：Windows のパスワードは、最大で 20 文字以内です。

標準パスワードと確認パスワード

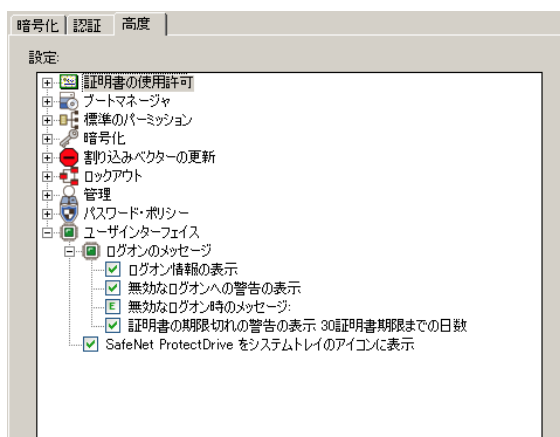
このフィールドには事前に「password」が設定されています。パスワードを変更する場合には、[標準のパスワード]をクリックして、新しいパスワードを入力してください。また、[確認パスワード]に確認のために、パスワードを入力してください。



新規に追加した Windows（ドメイン）ユーザは、初回のプリブート認証時にデフォルトのパスワードの入力を求められます。ユーザが実際の Windows（ドメイン）パスワードを使って Windows 認証を行うと、ProtectDrive の標準パスワードが ProtectDrive のプリブート・ユーザ・データベースにあるユーザの Windows（ドメイン）パスワードに変わります。

注意：Windows のパスワードは、最大で 20 文字以内です。

高度の設定 — ユーザ インターフェース



ログオン情報の表示

デフォルトでは、Windows エクスプローラのシェルをロードする直前に、ProtectDrive の認証情報に関するダイアログが表示されます。このメッセージには、最終ログオンの日時、最終パスワード変更の日時、およびログオンの成功回数が表示されます。このチェック・ボックスをオフにすると、ログオン情報の表示が無効になります。

無効なログオンへの警告の表示

デフォルトでは、プリブート認証の試行に失敗すると警告メッセージが表示されます。この警告は、Windows エクスプローラのシェルをロードする直前に表示されます。このチェック・ボックスをオフにすると、この警告メッセージの表示が無効になります。


無効なログオン時のメッセージ

[無効なログオンへの警告の表示] オプションを選択している場合、[無効なログオン時のメッセージ] フィールドにこのメッセージを入力することで、オプションのメッセージも表示できます。

証明書の期限切れの警告の表示

このオプションを選択すると、スマートカードおよびトークンのユーザに警告メッセージが表示されます。このメッセージは、証明書の有効期限までの残り日数を示します。

システム・トレイに SafeNet ProtectDrive アイコンを表示

ProtectDrive のインストール後、ProtectDrive の小さなアイコン () がデフォルトでシステム・トレイに配置されます。[システム・トレイに SafeNet ProtectDrive アイコンを表示] チェック・ボックスをオフにすると、このアイコンが無効になります。

このオプションを有効にすると、アイコンを右クリックして以下のいずれかを選択できます。

- [ローカル管理コンソール] – ローカル管理コンソールが開きます（アイコンをダブルクリックしても LMC を開くことができます）。
 - [コンピュータをロックする] – Windows デスクトップがロックされます。
 - [共通鍵] – ユーザの共通鍵を管理します。このオプションは、[PD 設定] > [認証] で [共通鍵の登録を許可] を選択した場合のみ表示されます。
 - [SafeNet ProtectDrive のバージョン情報] – ProtectDrive のバージョン、ライセンス、および著作権情報などが表示されます。
-

PD ユーザ タブ（デフォルトのユーザ・ポリシー）

[PD ユーザ] タブのオプションを使用すると、特定の Windows ドメイン・ユーザが自動的に新しく作成したコンピュータ・オブジェクトに割り当てられます。これらのユーザのデバイスへのアクセス制御に関するアクセス許可もここで設定できます。このタブで定義するデバイスへのアクセス制御に関するアクセス許可は、[PD ユーザ] > [詳細] -> [標準のパーミッション] タブのシステム設定よりも優先されます。

ユーザ	証明書	パスワード	パスワードの状態	共通鍵	Windows ログオ
Administrator C	いいえ	はい	標準	はい	いいえ
Safenet (SAFE)	いいえ	はい	設定	いいえ	はい

☐ 証明書ユーザはパスワードアカウントを保持

デバイス制御

- ☒ CDROM の読み取り
- ☒ CDROM へ書き込み
- ☒ ディスケットの読み取り
- ☒ ディスケットへ書き込み
- ☒ リムーバブルメディアの読み取り
- ☒ リムーバブルメディアへ書き込み
- ☒ パラレルポートの読み取り
- ☒ パラレルポートへ書き込み
- ☒ シリアルポートの読み取り
- ☒ シリアルポートへ書き込み

2 ユーザで 0 SafeNet ProtectDrive 証明書

ユーザ

このカラムには、所定のドメインに新しく作成したコンピュータ・オブジェクトに自動的に割り当てられる、個々のドメイン・ユーザおよびグループがリスト表示されます。Active Directory および ADAM からこの列を入力するには、[追加] または [削除] をクリックしてください。

証明書

このカラムには、はい、いいえで証明書の利用を表示します。いいえ ならば、ユーザは、どんな証明書も使用していません。はい ならば、ユーザが与えられたドメインで持っている有効なスマートカードもしくはトークン証明書の数が表示されます。

証明書のあるユーザは、スマートカードおよびトークンを使用して ProtectDrive へログオンできます。割当済み証明書の合計数も、このタブの一番下のリストに表示されます。ProtectDrive のユーザ・アカウントは、スマートカードおよびトークンの証明書ごとに作成されます。

パスワード・ユーザに対して作成されるアカウントを含む、各クライアント・システムのアカウントの合計数は、最大で **2,000** です。

パスワード

このカラムでは、Windows グループのユーザまたはすべてのメンバが、ProtectDrive へログオンするための、初期パスワードアカウントを持っているかどうかを **はい**、**いいえ** で表示します。

パスワード に **はい** が表示される場合は、以下の状態です。

- **[設定]** ボタンを使用してユーザにパスワードが割り当てられた場合
- パスワードアカウントのみが追加された場合
- 証明書ユーザが追加され、**[証明書ユーザはパスワードアカウントを保持]**がチェックされている場合

パスワード に **いいえ** が表示される場合は、以下の状態です。

- 証明書ユーザが追加され、**[証明書ユーザはパスワードアカウントを保持]**がチェックされていない場合

パスワードの状態

このカラムには、**設定**、**標準**、または空白が表示されます。このカラムは、ユーザのパスワードが指定されている（**設定** になっている）か、標準のパスワードが使用されている（**標準** になっている）かを表示します。パスワード・ユーザ、スマートカードおよびトークン証明書ユーザの数は、最大 2,000 です。パスワードは、次のいずれかの方法を使用して割り当てます。

- ユーザのパスワードを指定するには、ユーザ名を強調表示して **[設定]** をクリックしてください。**[標準パスワードを使用]** をオフにし、選択したユーザもしくはグループの一意のパスワードを 2 度入力してください。特定のパスワード設定は、常に標準パスワードよりも優先されます。これで **パスワードの状態** が **設定** に変更されます。
- 標準パスワードを使用するには、ユーザ名を強調表示して **[設定]** をクリックし、**[標準パスワードを使用]** をオンにしてください。ユーザに割り当てる標準パスワードは、**[PD 設定] -> [高度]** の **パスワード・ポリシー** グループで定義することができます。
- グループ・メンバー、パスワードアカウントなど、すべての証明書ユーザを指定するには、**[証明書ユーザはパスワードアカウントを保持]**をオンにしてください。これにより、標準パスワード（**パスワード・ポリシー** グループで定義）が、パスワードの割り当てられていない全てのユーザに割り当てられます（前述の **[設定]** をクリックし、後から標準パスワードを任意のパスワードに変更することも可能です）。

新規に追加したユーザは、初回のプリブート認証時にデフォルトのパスワードの入力を求められます。ユーザが実際の Windows（ドメイン）パスワードを使って Windows 認証を行うと、ProtectDrive の標準パスワードが ProtectDrive のプリブート・ユーザ・データベースにあるユーザの Windows（ドメイン）パスワードに変わります。

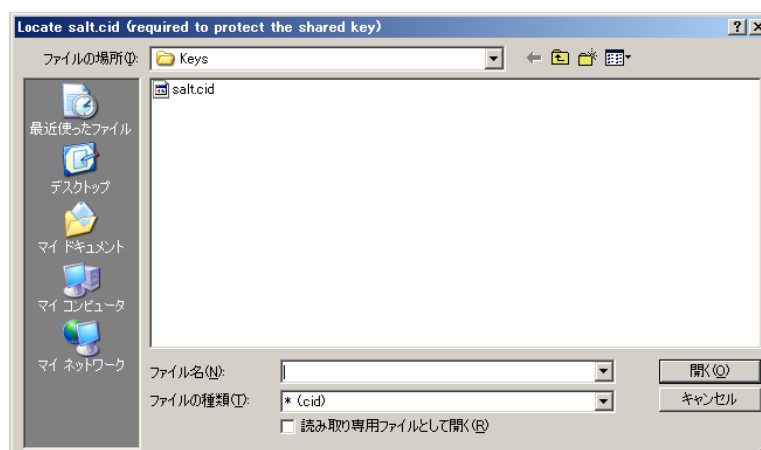
プリブートを無効にしてから再度有効にすると、初回のプリブート時にこのパスワードが再度必要になります。

共通鍵

このカラムでは、ユーザがプリブート認証に使用する共通鍵を登録（生成）しているかどうかを表示します（共通鍵は、LMC または MMC の **[Active Directory ユーザとコンピュータ]** から登録できます）。共通鍵を持つユーザは、共通鍵トークン（iKey 1000）を使用して ProtectDrive へログオンできます。

共通鍵を登録するには、次の手順を実行します。

1. ユーザ名をクリックしてください。
2. **[共通鍵]** ボタンをクリックしてください。
3. 共通鍵トークンを挿入して、**[OK]** をクリックしてください。
4. PIN を入力して **[OK]** をクリックしてください。
 - トークンが初期化されていない場合、新しい共通鍵がトークンに作成されます。
 - 既存の共通鍵がトークンで検出された場合、その共通鍵を使用するかどうか確認するよう要求されます。
 - **[いいえ]** を選択してから **[はい]** を選択すると、共通鍵が上書きされます。
 - 共通鍵をローカルで（ローカル管理コンソールから）設定する場合、この手順を実行します。鍵が更新されたことを示すメッセージが表示されます。
 - 共通鍵を ProtectDrive サーバ（MMC の **[Active Directory ユーザとコンピュータ]** スナップイン）から設定すると、salt.cid ファイルを要求されます。手順 5 へ進みます。
5. salt.cid ファイルを選択して **[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メッセージが表示されます。

注意： システム・トレイの SafeNet ProtectDrive アイコンからアクセスできる **[共通鍵]** オプションからユーザの共通鍵を登録することも可能です。

Windows ログオンに追加

このカラムでは、Windows へのログオン時にユーザが自動的に ProtectDrive のデータベースへ追加されるかどうかを表示します。ProtectDrive のデータベースにユーザが存在せず、**[PD 設定] > [認証]** で **[Windows ログオン時にユーザを ProtectDrive へ追加]** オプションが選択されている場合、そのユーザは Windows ログオン後に ProtectDrive へ追加されます。

デバイス制御

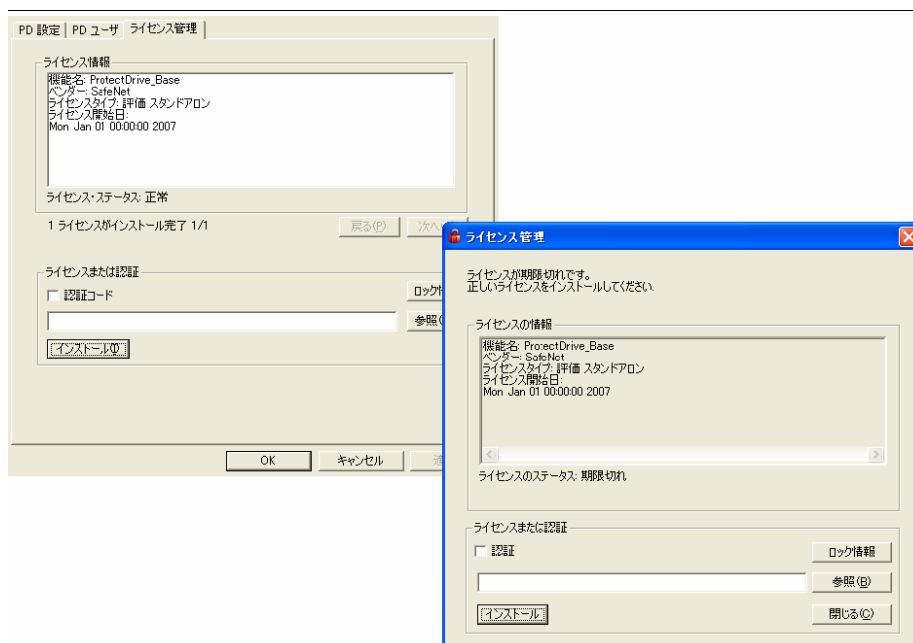
このセクションのこの設定を使用すると、**デバイス制御** グループに表示される各ユーザ（またはグループ）の、デフォルトの読み取りおよび書き込みのアクセス許可が設定可能です。各デバイスの **[書き込み]** 設定は、**[読み取り]** 設定も有効な場合のみ有効にすることができます。必ず **[設定]** をクリックしてこれらの設定を Active Directory に保存してください。そのまま **[OK]** または **[適用]** をクリックすると、これらのアクセス許可が Active Directory に保存されません。

ライセンス・マネージャ タブ（ライセンスの表示、インストールおよび更新）

ProtectDrive は、30 日間限定の評価版（試用版）ライセンスとともに出荷されます。ProtectDrive のインストール時に、試用ライセンスまたはフルライセンスをインストールしてください。機能（リムーバブル・メディアおよびリモート管理など）は、インストールするライセンスに応じて有効または無効になります。

ローカル管理コンソールの **ライセンス管理** タブには、現在インストールされている ProtectDrive のライセンスに関する情報が表示されます。ProtectDrive のインストール後、**ライセンス管理** タブ（左下に表示）を使用して、試用版または期限切れのライセンスをアップグレードできます。


ライセンスの期限が切れている場合、「nag」画面が右下に表示され、有効なライセンスをインストールするまで定期的に表示されます。

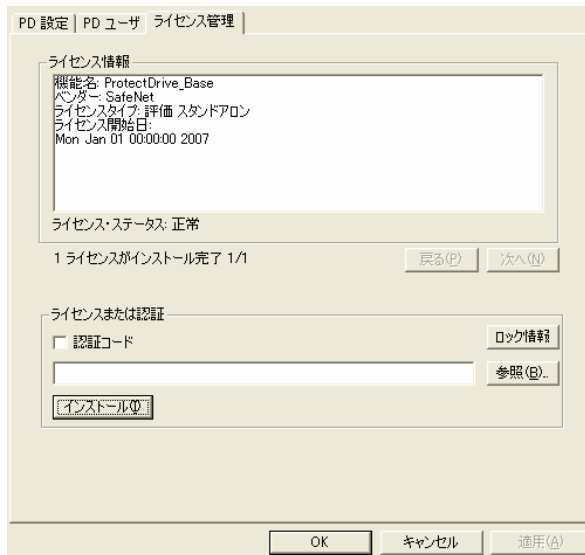


ライセンス・マネージャによるフルライセンスへのアップグレード

現在試用ライセンスがインストールされている場合、またはライセンスの期限が切れている場合には、そのライセンスをアップグレードできます。はじめに、有効な `license.txt`（単一クライアントのインストールの場合）または `authorization.txt`（複数ライセンスのクライアント・インストールの固定ライセンスの場合）が、クライアント PC がアップグレード手順の実行中に参照できる場所へ保存されているかどうか確認してください。

固定ライセンスのインストールを完了するには、クライアント PC からインターネットにアクセスする必要があります。ライセンスの詳細については、8 ページを参照してください。

1. Windows デスクトップのシステム・トレイにある ProtectDrive のアイコン () を右クリックしてから [ローカル管理コンソール] をクリックするか、またはアイコンをダブルクリックしても開くことができます。
2. [ライセンス管理] をクリックしてください。



3. 次のいずれかを実行してください。
 - license.txt ファイルを参照し、[インストール] をクリックしてください。
 - license.txt ファイルを参照して開き、テキスト全体を空白のフィールドへコピー&ペーストし、[インストール] をクリックしてください。
 - [認証コード] をチェックして authorization.txt ファイルを参照し、[インストール] をクリックしてください。
4. authorization.txt ファイルを使用してライセンスを取得する場合、クライアントからライセンス・サーバへアクセスしてください。アクセスが完了したら、ライセンス・サーバからクライアントへ固定ライセンスが送信されます。
5. ライセンスの更新が完了したらメッセージが表示されます。

「nag」画面でのフルライセンスへのアップグレード

「nag」画面でフルライセンスへアップグレードする場合には、前のセクションで説明した手順 3～5 を実行してください。

第9章 システムおよびユーザの管理

ProtectDrive クライアントを Active Directory もしくは、ADAM のシステムおよびユーザ・ポリシーのデータと連携させることで、ProtectDrive Management Console で集中管理することができます。

[Active Directory ユーザとコンピュータ]MMC スナップインは、[PD 設定] および [PD ユーザ] から追加します。また、自己管理および設定での管理が使用可能です。

ProtectDrive Management スナップインは、Active Directory ユーザとコンピュータの MMC スナップインと同様の仮想的なものであり、[PD 設定]および[PD ユーザ]で設定が可能であり、ProtectDrive のクライアントをグループで管理することも可能です。

または、ローカル管理コンソール・ユーティリティを使用してクライアントをローカルで管理することも可能です。ローカル設定を Active Directory および ADAM に保存することもできます。クライアントごとに、更新済みのポリシー・データをサーバに返します。

サーバからのシステム・ポリシーの管理

システムおよびユーザ・ポリシーを設定する前に、[第 8 章](#) – システムおよびユーザ・ポリシーの設定」の内容を確認してください。この内容を確認することで、[PD 設定] タブのフィールドについて理解できます。このタブを使用して、ProtectDrive のシステム・ポリシーを設定します。

Windows ドメインのシステムは、すべて[Active Directory ユーザとコンピュータ] MMC スナップインにある [PD 設定] タブと [PD ユーザ] タブを使用してリモート管理できます。これらのタブの設定は、すべて Active Directory もしくは ADAM に保存され、そこからクライアント・システムへ複製されます。複製されたデータは設定可能です。

または、サーバで適用した [システム・ポリシー] の設定を表示し、クライアント・システムでローカルに変更できます。この変更ができるのは、次のような場合のみです。

- インストール時に [クライアントの設定] オプションが選択されている場合、または
- ローカル管理コンソールからクライアントをローカルで設定するよう、SafeNet ProtectDrive.msi の ERA_CLIENT CONFIGURATION_ONLY プロパティが設定されている場合。

設定例

下記にどのようにクライアントを設定するかを説明します。

1. サーバで、ProtectDrive Management Console を起動してください。
2. Active Directory ユーザとコンピュータ MMC スナップインを開いて、設定するクライアントを右クリックし、**[プロパティ]**を選択してください。
もしくは、
ProtectDrive Management スナップインの設定オブジェクトを開いて、ProtectDrive Default Configuration もしくは、新規作成した設定を右クリックして、**[プロパティ]**を選択してください。
3. **[PD 設定]** タブをクリックし、表示されるタブをすべて使用して、目的の ProtectDrive システム・ポリシーを設定します。
4. ProtectDrive のタブをすべて開き、クライアントのシステム・ポリシーを順次設定します。以下に説明する設定については、特に注意が必要です。

認証

認証方法	Windows	プレブート
<input checked="" type="checkbox"/> ローカル・ユーザのアクセスを許可	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> パスワード・ドメイン・ユーザのアクセスを許可	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> トークン・ドメイン・ユーザのアクセスを許可	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> 共通鍵アクセスを許可		<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> シングルサインオン		

プレブートのアクセス管理

- ☐ ユーザ名を使用した緊急ログインを許可
 - ☐ 緊急ログイン後のシングルサインオン
- ☐ ユーザ名なしでの緊急ログインを許可
- ☐ トークン・ユーザの緊急ログインを許可
- ☐ 共通鍵の登録を許可
- ☒ Windows ログイン時にユーザを SafeNet ProtectDrive へ追加

- **[標準設定の読み込み]** をクリックして ProtectDrive システムおよびユーザ・ポリシーの標準設定が、[第8章](#)で説明した特定の Windows ドメインに対してすでに定義されている場合、**[標準設定の読み込み]** をクリックすると、定義済みの標準設定がこのコンピュータ・グループの全メンバに適用されます。
- **[適用]** または **[OK]** をクリックすると、システムおよびユーザ・ポリシーのデータが Active Directory および ADAM に保存され、最終的にクライアント・システムへ複製できるように、タイム・スタンプが追加されます。**[クライアントの設定]** タブにある **[更新]** 設定に応じて、クライアントに対して行った設定変更が複製されます。
- **[動作可]/[未決定]/[動作不可]** のインジケータに注意してください。次に例を示します。これらのインジケータは、クライアントの ProtectDrive プリブート認証の現状を表します。ProtectDrive クライアントの **[動作可]/[動作不可]** の状態は、**[更新間隔]** タブの設定に応じて更新されます。

[プリブート認証を有効化] オプションの設定を変更すると、ProtectDrive クライアントの [動作可] または [動作不可] の状態が有効になるまでの時間に遅延が生じます。この場合、[未決定] インジケータが表示されます。

☒ プリブート認証を有効

未決定

上の例のインジケータは、プリブート認証が有効になっていても（チェック・ボックスがオンになっていても）、その時点でプリブート・ユーザがクライアントに複製されていないことを示します。そのため、すべての ProtectDrive の機能がしばらくの間無効になります。ProtectDrive を初めてシステムにインストールしたときに、システム・ポリシーが Active Directory からまだ複製されていない場合などがその例です。

また、ユーザがシステムに割り当てられていない場合もこのような現象が起こります。つまり、[未決定] の状態は、システムを正しく設定し、ポリシー・データが問題なくサーバから複製されるまで続くということです。

更新のステータス

- ポリシー・データの変更およびクライアントの更新に関する最新の時間を示すには、このタブを監視します。時間的に見て [前回のクライアントの変更] が [前回の設定の変更] よりも新しい場合、ポリシー・データがクライアントへ問題なく複製されていることを示します。次の例では、PD-DOC-XP でサーバからポリシー・データの更新が完了していることを示します（左のスナップショット）。右のスナップショットは、クライアントが次の更新を待っている状態を示します。

更新のステータス	
前回の設定の変更:	2007/09/06 6:46:26
前回のクライアントの変	2007/09/06 9:20:29
クライアントのメッセージ:	更新の成功

- [暗号化および復号化] ボタンをクリックして、暗号化するクライアントのパーティションを指定します。

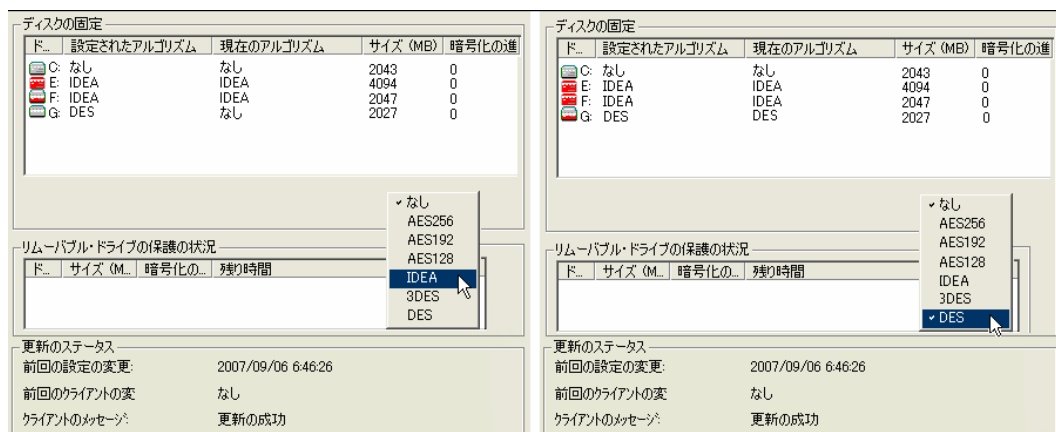
ディスクの固定			
ド.	設定されたアルゴリズム	現在のアルゴリズム	サイズ (MB)
C:	なし	なし	2043
E:	なし	なし	4094
F:	なし	なし	2047
G:	なし	なし	0

ディスクの固定			
ド.	設定されたアルゴリズム	現在のアルゴリズム	サイズ (MB)
C:	なし	なし	2043
E:	IDEA	なし	4094
F:	IDEA	なし	2047
G:	DES	なし	2027

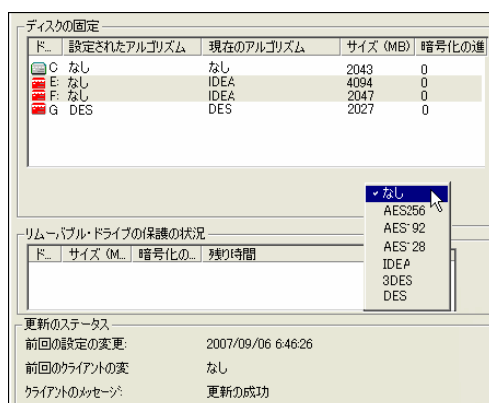
リムーバブルドライブの保護の状況			
ド.	サイズ (MB)	暗号化の進	残り時間

更新のステータス	
前回の設定の変更:	2007/09/06 6:46:26
前回のクライアントの変	なし
クライアントのメッセージ:	更新の成功

- 次のような半分陰になったディスク・ドライブのアイコンで、暗号化の進捗状況が継続的に表示されます（左はドライブ F、右はドライブ G を示します）。



- 任意の暗号化パーティションを復号化するには、[設定されたアルゴリズム] を [なし] に設定してください。次の例では、ドライブ E と F が暗号化対象として設定されています。これらのドライブの暗号化が、[クライアントの;設定] タブの [更新] の設定に応じて、ポリシー・データがクライアントへ複製されると同時に実行されます。



サーバからのユーザ・ポリシーの管理

コンピュータ・オブジェクト経由でのユーザのクライアントへの割り当ておよびユーザ・ポリシーの管理

ユーザ・ポリシーを設定する前に、[第 8 章 - システムおよびユーザ・ポリシー](#)の内容を確認してください。この内容を確認することで、**[PD ユーザ]** タブのフィールドについて理解できます。このタブを使用して、ProtectDrive のユーザ・ポリシーを設定します。

設定例

下記にどのようにクライアントを設定するかを説明します。

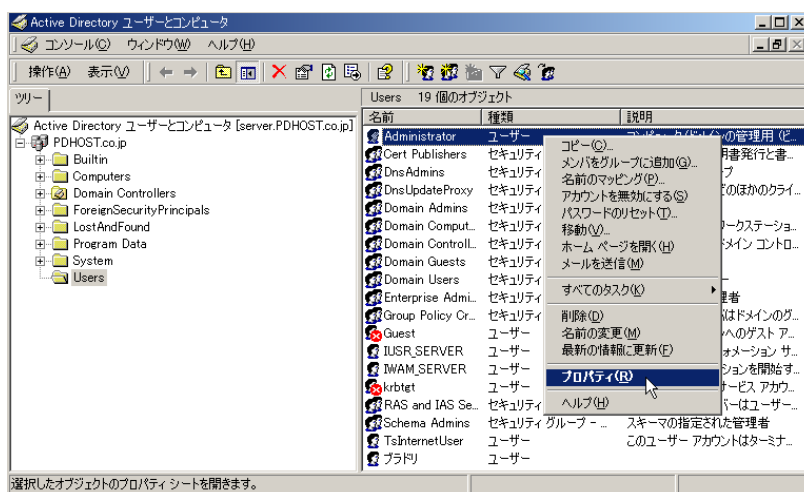
1. サーバで、ProtectDrive Management Console を起動してください。
2. Active Directory ユーザとコンピュータ MMC スナップインを開いて、設定するクライアントを右クリックし、**[プロパティ]**を選択してください。
もしくは、
ProtectDrive Management スナップインの設定オブジェクトを開いて、ProtectDrive Default Configuration もしくは、新規作成した設定を右クリックして、**[プロパティ]**を選択してください。
3. **[PD ユーザ]** タブをクリックします。クライアント・システムでプリブート・アクセスを許可する Windows ドメインのユーザおよびグループをすべて追加します。ユーザまたはグループごとに、**[設定]** をクリックしてデバイスへのアクセス許可を設定します。

ユーザまたはグループのデバイスへのアクセス許可を変更すると、Windows ドメイン全体に適用されます。ここでアクセス許可を変更すると、そのユーザまたはグループがリストに表示されているすべてのクライアント・システムに適用されます。
4. このリストにあるすべてのユーザが **[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]** で定義するパスワード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]** をチェックしてください。

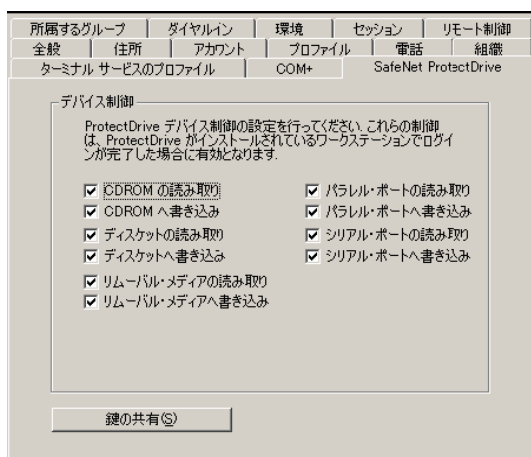
ユーザ・オブジェクトもしくはグループ・オブジェクトでのユーザ・ポリシーの管理

Windows ドメインのユーザごとに、ProtectDrive のデバイスへのアクセス許可を設定します。

1. MMC の **[Active Directory ユーザとコンピュータ]** スナップインで、Windows ドメインのユーザ名を右クリックして **[プロパティ]** を選択してください。



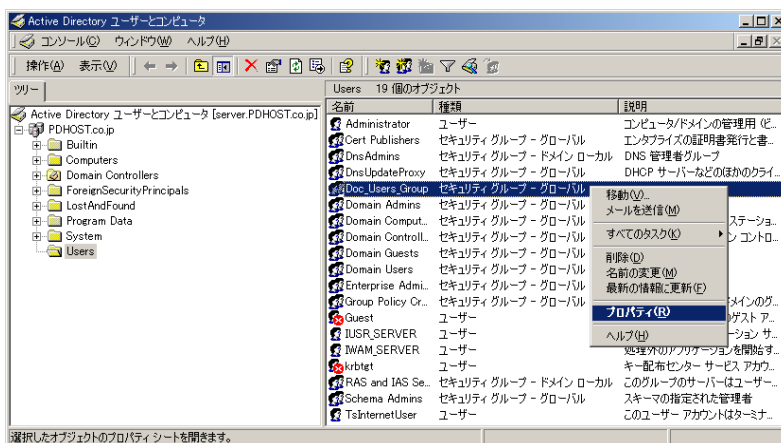
2. **[SafeNet ProtectDrive]** タブをクリックし、デバイスへのアクセス許可を必要に応じて設定してください。これらの設定は、Windows ドメイン全体に適用され、この Windows ドメインのユーザがリストに存在するクライアントすべてで有効となります。



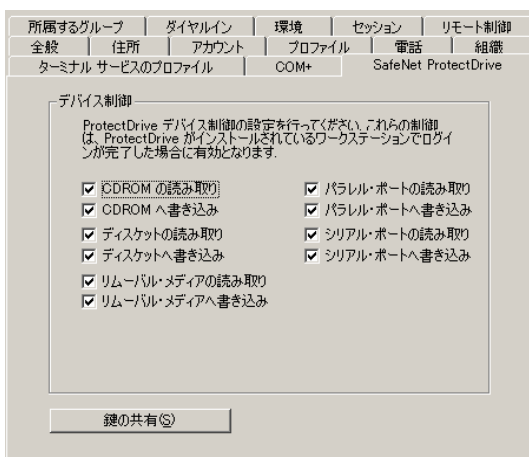
グループ・オブジェクト経由でのユーザ・ポリシーの管理

Windows ドメインのグループごとに、ProtectDrive のデバイスへのアクセス許可を設定します。

1. MMC の **[Active Directory ユーザとコンピュータ]** スナップインで、Windows ドメインのグループ名を右クリックして **[プロパティ]** を選択してください。



2. **[SafeNet ProtectDrive]** タブをクリックし、デバイスへのアクセス許可を必要に応じて設定してください。これらの設定は、Windows ドメイン全体に適用され、この Windows ドメインのユーザ・グループがリストに存在するクライアントすべてで有効となります。

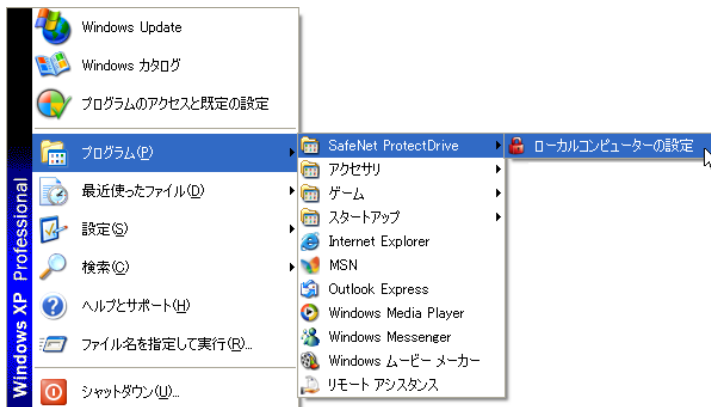


グループのメンバ間で異なる設定は、データが競合しているため無効になります。これらの設定を確認し、必要に応じて設定しなおしてください。

システムおよびユーザ・ポリシーのローカル管理

ローカル管理コンソール (LMC) ユーティリティは、システムおよびユーザ・ポリシーをローカル設定する場合に使用します。[ローカル管理コンソール] タブは、MMC の [Active Directory ユーザとコンピュータ] スナップインのタブとよく似ていますが、次に説明するとおり、細部がいくつか異なります。

Windows デスクトップから LMC を実行するには、[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。



システム・トレイにある ProtectDrive のアイコン (🔒) を右クリックしてから [ローカル管理コンソール] をクリックするか、またはアイコンをダブルクリックしても開くことができます。

PD 設定 タブ

[PD 設定] タブは、MMC の [Active Directory ユーザとコンピュータ] スナップインに相当するため、実質的にローカル管理コンソールと同じです。唯一の例外は [ステータス] タブです。ローカル管理コンソールのこのタブには、さらに [サイズ (MB)]、[暗号化の進捗]、[残り時間] という3つのカラムが追加されています。

サイズ (MB)

このカラムには、ハードディスクのパーティションのサイズを表示します。

暗号化の進捗

このカラムには、ハードディスクのパーティションの暗号化状態を表示します。

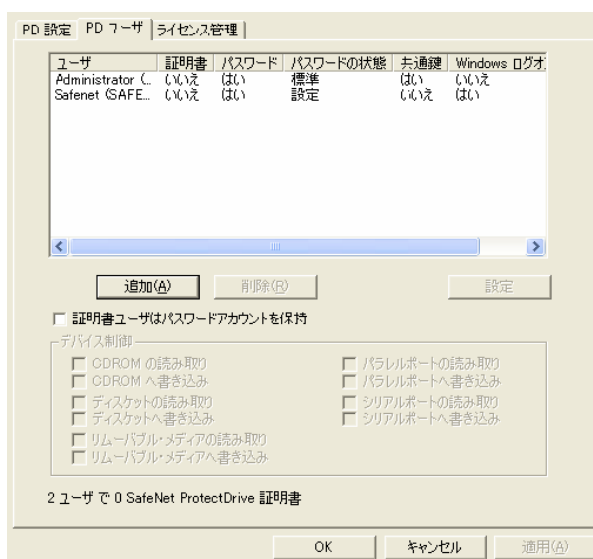
残り時間

このカラムには、実行中の暗号化が完了するまでの残り時間を表示します。

PD ユーザ タブ

[PD ユーザ] タブを使用すると、Windows ドメインのユーザおよびグループをクライアントに追加できます。ここでは、既存のプリブート・ユーザ・アカウントがすべてリストに表示されます。

Windows ドメインのユーザを追加するには、[追加] をクリックします。



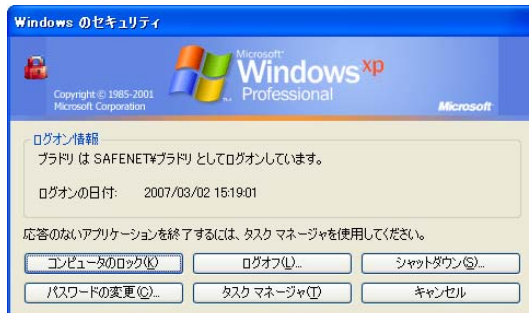
ローカルの Windows ユーザを ProtectDrive のプリブート・ユーザ・データベース (pduserdb) へ追加する

ローカルの Windows ユーザを ProtectDrive のプリブート・ユーザ・データベースへ追加する最も簡単な方法を以下に説明します。作業を始める前に、[PD 設定]->[認証] タブを選択し、[Windows ログオン時にユーザを ProtectDrive へ追加] オプションが有効になっていることを確認してください。

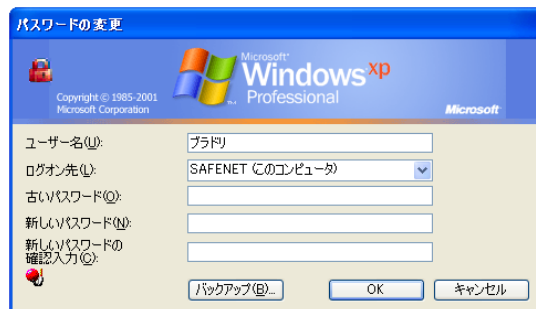
1. クライアント PC で Windows の管理者セッションをログアウトします。
2. ユーザごとにローカルの Windows へログオンします。ログオンが完了したら、プリブート・ユーザ・アカウントが自動的に作成されます。
3. [PD ユーザ] タブを開き、各ユーザが追加されていることを確認します。

プリブート・パスワードの変更

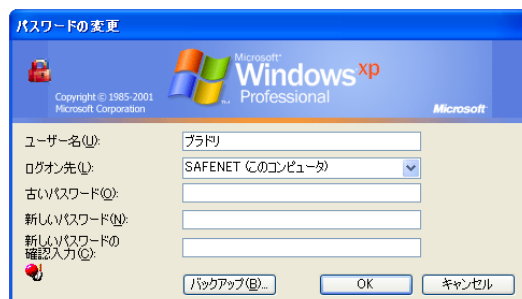
1. **Ctrl、Alt、Del** キーを同時に押して [パスワードの変更] を選択してください。



2. [ログオン先] フィールド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 Windows の場合、新しいパスワードを変更すると、直後にプリブート・ユーザ・データベースに反映されます。
- Windows ドメイン（下）の場合、ユーザは Windows からいったんログアウトしてから、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 Windows ドメインにいったんログオンすると、この新しいパスワードが直ちに使用可能となり、プリブート認証時に使用できるようになります。



第10章 ユーザ認証

注意： プリブート認証が無効になるようシステム・ポリシーを設定している場合（[認証] タブの [プリブート認証を有効化] を参照）、この章の内容は適用されません。その場合、ユーザには標準の Windows ドメイン認証のダイアログが表示され、通常の Windows ログオンが適用されます。

スマートカードとトークンおよび PIN による認証

プリブート認証

スマートカードとトークンおよび PIN を使ったプリブート認証のロジック・フロー図の詳細については、[付録 A](#) を参照してください。

ProtectDrive で [トークン・ドメイン・ユーザのアクセスを許可] または [共通鍵アクセスを許可] の認証オプションが設定されている場合、次のようなプリブート認証画面が表示されます。さらに、[ローカル・ユーザのアクセスを許可] または [パスワード・ドメイン・ユーザのアクセスを許可] の認証オプションが設定されている場合、下の画面が表示されている状態で F2 キーを押すと、ドメイン・パスワードのプリブート認証画面を切り替えることができます。

この時点で、ユーザはスマートカードとトークンおよび PIN または Windows ユーザ名とパスワードおよびドメイン名のいずれかを使ってシステムの認証を実行できます。連続してプリブート認証の試行に失敗した場合、PIN の推測攻撃を回避するために、[ロックアウトの設定] のポリシーが強制的に実行されます（ログオン試行の失敗やその他のイベントの詳細については、システムの [イベント・ビューア] を開いてください。[イベント・ビューア] の詳細については、144 ページを参照してください）。



32bit プリブート認証画面（標準）



16bit プリブート認証画面

注意： 32bit プリブート認証は、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 プリブート認証画面が表示されます。

注意： 共通鍵による iKey 1000 でのトークン認証の場合には、シングル・サイン・オンは動作しません。

Windows 認証

注意： ユーザが Windows へのログオンを完了すると、毎回最新の Windows パスワードが ProtectDrive のプリブート・ユーザ・データベースへ反映されます。

Windows（ドメイン）認証のロジック・フロー図の詳細については、[付録 C](#) を参照してください。

自動 – シングル・サイン・オン・モードがオンの場合

ProtectDrive シングル・サイン・オン・モードがオンになっている場合、ユーザは自動的に適切な Windows ドメインに対して認証されます。

手動 – シングル・サイン・オン・モードがオフの場合

シングル・サイン・オンがオフの場合、次のような標準の Windows ドメイン認証画面が表示されます。



スマートカードまたはトークンをリーダーへ挿入すると、次のような標準の Windows ドメインの PIN 認証画面が表示されます。この時点で、ユーザは PIN を入力してください。



または、[ローカル・ユーザのアクセスを許可] または [パスワード・ドメイン・ユーザのアクセスを許可] 認証オプションが設定されている場合、ユーザが Ctrl、Alt、Del キーを同時に押すと、標準の Windows ドメインのログオン画面が呼び出されます（112 ページを参照してください）。

トークンの削除ポリシー

トークンまたはスマートカードを Windows ドメイン認証に使用するコンピュータの場合、トークンが削除されると自動的にロックされるように設定できます。

この動作は、MMC の [ローカル セキュリティ設定] スナップインにある [スマートカード取り出し時の動作] ポリシーにより制御されます。このポリシーは、デフォルトで [何もしない] または [未定義] に設定されています。

SafeNet では、このポリシーを [ワークステーションをロックする] に設定することをお勧めします。この設定の場合、ユーザがワークステーションに戻る際に、再度トークンを挿入して PIN を入力する必要があります。

ユーザ名、パスワード、およびドメイン名による認証

プリブート認証

ユーザ名とパスワードおよびドメイン名によるプリブート認証のロジック・フロー図の詳細については、付録 B を参照してください。

ProtectDrive で [ローカル・ユーザのアクセスを許可] または [パスワード・ドメイン・ユーザのアクセスを許可] の認証オプションが設定されている場合、次のようなプリブート認証画面が表示されます。



32bit プリブート認証画面（標準）



16bit プリブート認証画面

[ドメイン] フィールドに、システムで使用可能な Windows ドメインがすべてリストに表示されます。[ローカル・ユーザのアクセスを許可] 認証オプションが選択されている場合、次のような ProtectDrive のプリブート認証画面にある [ドメイン] フィールドのリストに、ローカル・システムの名前も表示されます。使用可能なドメインのリストをスクロールするには、上向きまたは下向きの矢印キーを使用します。連続してプリブート認証の試行に失敗した場合、PIN の推測攻撃を回避するために、[ロックアウトの設定] のポリシーが強制的に実行されます（ログオン試行の失敗やその他のイベントの詳細については、システムの [イベント・ビューア] を開いてください。[イベント・ビューア] の詳細については、144 ページを参照してください）。

Windows 認証

注意： ユーザが Windows へのログオンを完了すると、毎回最新の Windows パスワードが ProtectDrive のプリブート・ユーザ・データベースへ反映されます。

ProtectDrive のシングル・サイン・オン・モードがオンの場合

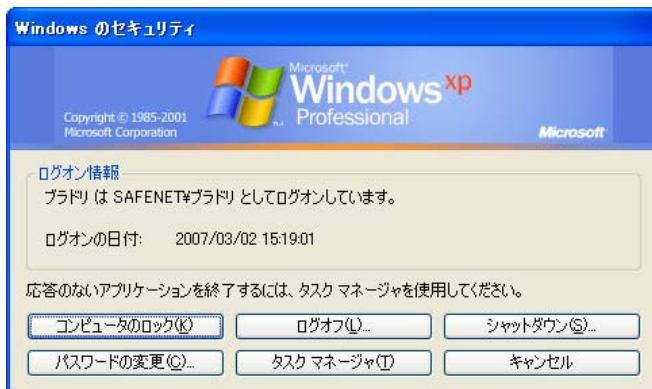
ProtectDrive シングル・サイン・オン・モードがオンになっている場合、プリブート認証の完了後にユーザは自動的に適切な Windows ドメインに対して認証されます。

ProtectDrive のシングル・サイン・オン・モードがオフの場合

シングル・サイン・オンがオフの場合、次のような標準の Windows ドメイン認証画面が表示されます。



Ctrl、Alt、Del キーを同時に押すと、次のような標準の Windows ドメイン認証画面が表示されます。適切な Windows ドメインのユーザ名とパスワードを入力します。



第11章

例外的な認証のシナリオ

注意 1： Active Directory からクライアントのリカバリ・エンベロープを取得してパスワードを復旧するには、クライアントのインストールが Active Directory インストールの [リモート設定] に設定されている必要があります。これにより、クライアントを Active Directory からリモートで設定できます。

クライアントで Active Directory の更新とエンベロープの取得を確実に行うには、SafeNet ProtectDrive.msi の ERA_CLIENT_CONFIGURATION_ONLY プロパティを 0 に設定してください。

インストールを [リモート設定] で行っていない場合、HKLM/Software/SafeNet/ProtectDrive/Installer で ClientConfigurationOnly という DWORD 値のレジストリ設定を 0 にしてからリブートすれば、インストールを変更できます。ただし、この方法では Active Directory からリカバリ・エンベロープを使用できませんが、インストール時に作成した.env ファイルから使用できます。

注意 2： プリブート認証が無効になるようシステム・ポリシーを設定している場合 ([認証] タブの [プリブート認証を有効] オプションを参照)、この章の内容は適用されません。その場合、ユーザには標準の Wnidows ドメイン認証のダイアログが表示され、通常の Windows ログオンが適用されます。通常のプリブート・ユーザ認証のほかにも、次のような例外的な状況にも対応できるよう、システム・ポリシーを設定できます。

- [トークン・ユーザの緊急ログオン手順](#) - この手順は、トークン・ユーザがスマートカードおよび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に使用します。この手順を実行すると、システム管理者のサポートを受けながら 1 回だけシステムにプリブート・アクセスできます。トークン・ユーザの緊急ログオンは、トークン・ユーザがログオンする（この選択を行う）まで実行できません。
- [ユーザ名を入力する緊急ログオン手順](#) - この手順は、Windows ドメインまたはローカル Windows ユーザが Windows パスワードを忘れてしまった場合の対応に使用します。システム管理者のサポートを一部受けながら、システムにプリブート・アクセスできます。ユーザの緊急ログオンは、ユーザがログオンする（この選択を行う）まで実行できません。
- [ユーザ名を入力しない緊急ログオン手順](#) - この手順は、ユーザ名を忘れてしまった場合の緊急ログオンへの対応、あるいはクライアント・システムのプリブート・ユーザ・データベースに新しく Windows ドメインまたはローカル Windows ユーザを追加する場合の対応に使用します。

さらにこの手順は、ユーザが初回のプリブート認証を行う前で、Active Directory のユーザ・ポリシーがクライアント・システムにまだ複製されていない場合に適しています。ユーザがこの手順を実行してから Windows への認証を行うと、ローカル・システムのプリブート・ユーザ・データベースにそのユーザのアカウントが作成されます。

- [自動プリブート認証での自動リブート](#) - 自動リブート後の自動プリブート認証をシステム管理者から要求された場合には、特別なプリブート・ユーザ・アカウントを作成する必要があります。この機能は、システム・ポリシーで制御されません。その代わりに、この章の後半で説明するとおり、システム・レジストリを追加する必要があります。

トークン・ユーザの緊急ログオン手順

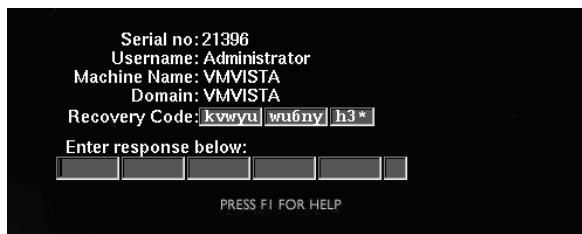
エンド・ユーザ向け手順

スマートカードとトークンおよび PIN のユーザが、スマートカードおよび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。

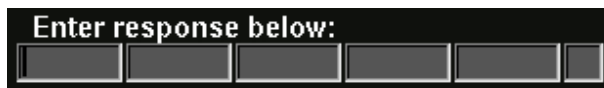
1. カーソルを [PIN] フィールドに合わせて **Shift+F9** キーを押します。



[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、表示されるリカバリ・コード (Recovery Code) 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] フィールドに入力します。



4. この時点で、通常 Windows の起動動作に進み、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システムへログオンします。

システム管理者向け手順

前のページの手順をユーザが実行し、システム管理者に問い合わせます。次にシステム管理者は、[リカバリ・ディスク](#)（ProtectDrive のインストール後にオリジナルを作成）を使用して次の手順を実行し、緊急ログオン手順を完了してください。

1. サーバの¥Program Files¥SafeNet ProtectDrive にある **rpadmin.exe** を実行します。
2. [緊急ログオン] をクリックしてください。
3. [復旧用証明書の鍵] セクションで、適切な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。（パスワードを入力すると、[レスポンスの生成] が有効になります。）
 - [スマートカード] - このオプションを選択する場合は、証明書鍵が保存されている適切なプロバイダをリストから選択してください。
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 ファイルを検索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。（注意：このオプションは、クライアントが Active Directory により、リモート設定でインストールされている場合のみ機能します。）
5. ユーザが提示したコードを [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。

リモート復旧コンソール

緊急ログイン | ディスク鍵の復旧

復旧用証明書の鍵

☐ パーソナルストア

☐ PFX ファイル ファイル: ...

パスワード:

☒ スマートカード プロバイダ:

復旧のエンベロープ

☒ ファイルから取得: ...

☐ AD から取得: ...

復旧の入力

☐ ユーザー名の復旧:

復旧コード(B):

レスポンス (空白は表示目的のみ)

レスポンスの生成(B)

6. 自動的に生成されるレスポンス・コードを [Enter response below] フィールドに入力するようにユーザに指示してください。この時点で、ユーザはシステムへプリブート・アクセスできるようになります。

ユーザ名を入力する緊急ログオン手順

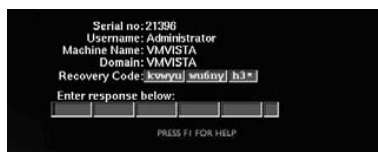
エンド・ユーザ向け手順

ユーザがパスワードを忘れた場合には、「ユーザ名を入力する緊急ログオン手順」に従い、システムへのアクセスを回復してください。

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



2. カーソルを **[パスワード]** フィールドに合わせて **Shift+F10** キーを押します。
[リカバリ & レスポンス] 画面が表示されます。



3. (電話でまたは直接) システム管理者に問い合わせ、表示されるリカバリ・コード (Recovery Code) を通知してください。
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。以下のようにこのコードを **[Enter response below]** フィールドに入力します。



5. この時点で、通常 Windows の起動動作に進み、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システムへログオンします。

システム管理者向け手順

前のページの手順をユーザが実行し、システム管理者に問い合わせます。次にシステム管理者は、[リカバリ・ディスク](#)（ProtectDrive のインストール後にオリジナルを作成）を使用して次の手順を実行し、緊急ログオン手順を完了してください。

1. サーバの¥Program Files¥SafeNet ProtectDrive にある **rpadmin.exe** を実行します。ProtectDrive の [リモート復旧コンソール] ウィンドウが表示されます。

[緊急ログオン] をクリックしてください。
2. [復旧用証明書の鍵] セクションで、適切な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。（パスワードを入力すると、[レスポンスの生成] が有効になります。）
 - [スマートカード] - このオプションを選択する場合は、証明書鍵が保存されている適切なプロバイダをリストから選択してください。
3. 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 ファイルを検索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。（注意：このオプションは、クライアントが Active Directory により、リモート設定でインストールされている場合のみ機能します。）
4. ユーザが提示したコードを [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。
5. 自動的に生成されるレスポンス・コードを [Enter response below] フィールドに入力するようユーザに指示してください。この時点で、ユーザはシステムへプリブート・アクセスできるようになります。

リモート復旧コンソール

緊急ログオン | ディスク鍵の復旧

復旧用証明書の鍵

☐ パーソナルストア

☒ PFX ファイル ファイル: A:\PdRecovery.pfx ...

パスワード: *****

☐ スマートカード プロバイダ: Gemplus GenSAFE Card CSP v1.0

復旧のエンベロープ

☒ ファイルから取得 A:\SAFENET-A6EC36B_RecoveryEnvelope.env ...

☐ AD から取得 ...

復旧の入力

☐ ユーザ名の復旧:

復旧コード(B): wkp0@ yyysj k23

レスポンス (空白は表示目的のみ)

レスポンスの生成(B)

6. セキュリティ上の理由から、Windows へのログオン直後に Windows (ドメイン) パスワードを変更するようユーザーに指示します。

ユーザ名を入力しない緊急ログオン手順

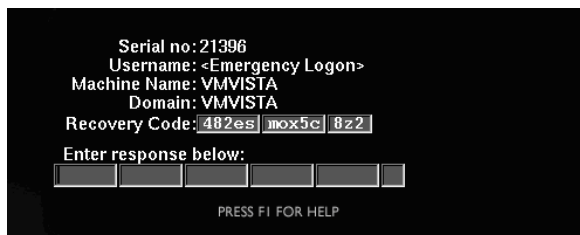
注意： この手順は、スマートカードとトークンの PIN ユーザには適用されません。

エンド・ユーザ向け手順

1. 以下のとおり、[ユーザ名/パスワード/ドメイン名のログオン] 画面の **[ユーザ 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. (電話でまたは直接) システム管理者に問い合わせ、表示されるリカバリ・コード (Recovery Code) 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]** フィールドに入力します。



4. この時点で、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。通常の Windows ログオンを実行します。

システム管理者向け手順

前のページの手順をユーザが実行し、システム管理者に問い合わせます。次にシステム管理者は、[リカバリ・ディスク](#)（ProtectDrive のインストール後にオリジナルを作成）を使用して次の手順を実行し、緊急ログオン手順を完了してください。

1. サーバの¥Program Files¥SafeNet ProtectDrive にある **rpadmin.exe** を実行します。ProtectDrive の [リモート復旧コンソール] ウィンドウが表示されます。
2. [緊急ログオン] をクリックしてください。
3. [復旧用証明書の鍵] セクションで、適切な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。（パスワードを入力すると、[レスポンスの生成] が有効になります。）
 - [スマートカード] - このオプションを選択する場合は、証明書鍵が保存されている適切なプロバイダをリストから選択してください。
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 ファイルを検索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。（注意：このオプションは、クライアントが Active Directory により、リモート設定でインストールされている場合のみ機能します。）
5. [ユーザ名を復旧] をチェックして、ユーザ名を入力してください。
6. ユーザが提示したコードを [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。

リモート復旧コンソール

緊急ログオン | ディスク鍵の復旧

復旧用証明書の鍵

☐ パーソナルストア

☒ PFX ファイル ファイル: A¥PdRecovery.pfx ...

パスワード: *****

☐ スマートカード プロバイダ: Gemplus GemSAFE Card CSP v1.0

復旧のエンベロープ

☒ ファイルから取得 A¥SAFENET-A6EC36B_RecoveryEnvelope.env ...

☐ AD から取得 ...

復旧の入力

☒ ユーザ名の復旧: JSmith

復旧コード(B): ybthi 907je mu2

レスポンス (空白は表示目的のみ)

レスポンスの生成(G)

7. 自動的に生成されるレスポンス・コードを [Enter response below] フィールドに入力するようにユーザに指示してください。この時点で、ユーザはシステムへ一度だけプリブート・アクセスできるようになります。

ユーザがブート後の Windows 認証を完了後、ローカル・システムの ProtectDrive プリブート・ユーザ・データベースに、そのユーザの新しいプリブート・ユーザ・アカウントが作成されます。

自動プリブート認証での自動リブート

一部のシステム管理者のタスクで、自動的にシステムを再起動し、自動的にオペレーティング・システムをロードしなければならない場合があります。このような場合に対応するために、ProtectDrive には、ダミーのプリブート・ユーザ・アカウントを作成する機能があります。

このアカウントを作成し、Windows のレジストリに次のような追加処理を行うと、自動的にプリブート・システム認証を実行できるようになります。自動プリブートを実行すると、システム・ポリシーの設定に関係なくシングル・サイン・オンが無効になります。プリブート時にシステムは自動的にログオンし、Windows をロードし、Windows (ドメイン) のログオン画面で停止します。

自動プリブート認証のセットアップ手順を次に示します。

1. 一意のユーザ名とパスワードを持つプリブート・ユーザ・アカウントを新規作成します。このようなアカウントを作成する方法の 1 つに、**pduserdb.exe** を使用する方法があります (第 12 章を参照してください)。
2. Windows レジストリに次のようなデータを追加します。

HKLM\Software\SafeNet\ProtectDrive\

APB_COUNT	REG_DWORD 0,N	デフォルトで 0 に設定されています。この設定では、自動プリブート認証が無効です。許可する自動プリブート認証の最大回数です。自動プリブート認証の試行に失敗すると、この値が 0 にリセットされます。この値を 0 よりも大きく (N > 0) すると、自動プリブート認証が N 回許可されます。この値を FFFFFFFF に設定すると無制限での自動プリブート認証が設定できます。
APB_USERNAME	REG_SZ	ユーザ名
APB_PASSWORD	REG_SZ	ユーザのプリブート・パスワード、もしくは、APB_TOKEN が設定されている場合には、PIN を入力してください。
APB_DOMAIN	REG_SZ	ユーザのドメイン名
APB_RESETINTVECTS	REG_DWORD 0,1	デフォルトの値は 0 です。この設定の場合、通常の ProtectDrive の動作は変更されません。1 に設定すると、システムの改ざんが検出されても、このオプションにより標準の ProtectDrive 警告メッセージが表示されなくなります。BIOS のアップグレードを実行すると、自動システム・メンテナンスの一環として割り込みベクター・アドレスが変更される可能性があるため、そのような場合に便利です。

APB_TOKEN	REG_DWORD 0,1	1 に設定すると、APB_USERNAME と APB_DOMAIN のエントリを無視し、APB_PASSWORD に設定された PIN を使用してのトークンでのログオンが実行されます。
APB_PERSISTENCELEVEL	REG_DWORD 0,1	0 に設定すると、APB の情報をシャットダウン時に保存します。1 に設定すると APB の情報を Windows 起動時にシャットダウン時と同様に保存します。

障害復旧ディスク鍵の作成

この手順を実行すると、ProtectDrive で暗号化されたコンピュータから Windows へブートできない場合に、この障害復旧ディスク鍵を使って、ハードディスクの復旧処理ができます。

通常、管理者は、**rpadmin** ユーティリティを使用するために、ディスク鍵ファイルを作成します。ディスク鍵ファイルは、パスフェーズで暗号化されており、**decdisk** ユーティリティや EFS リカバリ・ファイル（ProtectDrive の **backup.exe** ユーティリティで作成するか、Active Directory でディスク鍵を生成すると同時に作成）を完全にディスクを復号化と復旧のために使用します。

第 12 章の **backup.exe** と **decdisk.exe** を参照してください。

復旧ディスク鍵の作成

必ず下記の手順を確実にシステム管理者が実行しなければなりません。実行する前に、下記を確認してください。

- **decdisk.exe** ユーティリティ
 - 復旧するシステムの EFS リカバリ・ファイル（ProtectDrive の **backup.exe** ユーティリティで作成するか、Active Directory でディスク鍵を生成すると同時に作成）
 - マスター・セキュリティ証明書の鍵（.pfx ファイル）
1. サーバの¥*Program Files*¥*SafeNet ProtectDrive* にある **rpadmin.exe** を実行します。ProtectDrive の [リモート復旧コンソール] ウィンドウが表示されます。
 2. [ディスク鍵の復旧]のタブをクリックしてください。



3. [マスター・セキュリティ証明書の鍵] セクションで、適切な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。（パスワードを入力すると、[レスポンスの生成] が有効になります。）
 - [スマートカード] - このオプションを選択する場合は、証明書鍵が保存されている適切なプロバイダをリストから選択してください。
 4. [バックアップ・ファイルの保存場所] を指定してください。
 - バックアップ・ファイル（第 12 章の backup.exe 復旧ツールで作成）の保存場所は[...] をクリックしてバックアップの [ファイルのフォルダ] を参照し、[OK] をクリックしてください。
 - Active Directory のサーバ上のバックアップ・ファイルの保存場所は[AD からの取得]を選択し、[...] をクリックしてバックアップ・ファイルを保存するドメインのコンピュータ・オブジェクトを指定し、[OK]をクリックしてください。

注意：ACSVR、DKENV、DKY、DTE および GDA 復旧ファイルは、ディスク鍵（.dke）と同じ場所に保存されます。
 5. [ディスク鍵ファイル] の名前（例：diskkey.dke）を入力し、[...] をクリックしてファイルの保存先となる場所を参照し、[保存] をクリックしてください。
 6. 鍵ファイルのパスフレーズを 2 度入力してください。参考までに、入力を完了した **ディスク鍵の復旧** 画面を下記に示します。
-



7. [ディスク鍵ファイルの生成] をクリックしてください。
8. ディスク鍵ファイルの生成が完了したら [OK] をクリックしてください。

ディスクの復旧（復号化）

はじめに、影響のあるハードディスク、**decdisk.exe** ユーティリティを保存したフロッピーディスク、暗号化された*.dke ファイルと対応するパスフレーズ、および EFS リカバリ・ファイルが正しく送付されていることを確認します。

1. DOS モードで PC をブートしてください。
2. コマンド・ラインから、ProtectDrive の **decdisk** ユーティリティを使用してハードディスクを復号化します。/dk オプションを使用してください。

例：**decdisk -dk diskkey.dke**

3. プロンプトに従いパスフレーズを入力してください（前のセクションの手順 6 で作成）。
4. プロンプトに従い、復号化するディスクの領域を選択してください。
5. ディスクの復号化が完了したら、“**fdisk /mbr**” と入力して ProtectDrive のプリブート認証を削除し、PC を再起動してください。

注意：Windows Vista では、**fdisk /mbr** での復旧は十分ではないかもしれません。代わりに **rmbr /o** を使ってください。RMBR 復旧ツールの詳細は、136 ページを参照してください。

6. PC の再起動後、ProtectDrive をアンインストールしてください。
7. 復旧したハードディスクを ProtectDrive のシステム管理者に返却してください。
8. 暗号化された*.dke ファイルとパスフレーズは、不要なので破棄してください。

第12章

障害復旧ツール

BACKUP.EXE - ProtectDrive リカバリ・ファイルの作成

障害復旧に備えて、ディスクの暗号化ステータス変更後、コマンド・プロンプトの **backup.exe** ユーティリティを使用する必要があります。ラベルがコンピュータ名のフォルダが作成されると、その中に EFS リカバリ・ファイルが含まれます。このファイルはディスクの復旧に必要となります。また、このユーティリティをスケジュール済みの管理タスクとして実行することもできます。

使用例： **BACKUP.EXE [オプション]**

オプション	説明	デフォルト
/? -usage	使用例のヘルプを表示します。	
/v -ver	ユーティリティのバージョンを表示します。	
/t -tgt	リカバリ・ファイルのバックアップに使用するターゲット・ディレクトリを指定します。	現在のディレクトリです。 リカバリ・ファイルはクライアント・システム以外の場所に保存することをお勧めします。こうすることで、クライアント・システムが操作できなくなった場合でも、このリカバリ・ファイルを使用できます。
/n -noverchk	ProtectDrive バージョンの互換性チェックが実行されません。	

ProtectDrive により保護されたシステムが何らかの理由で（データの破損などにより）アクセス不能になった場合、システム管理者は、以下の障害復旧ツールを使用して、システムの診断を実行し、ハードディスクを復号化し、MBR を操作し、プリブート・ユーザ・データベースを管理することができます。

これらのツールは、ProtectDrive 配布 CD の **Tools** ディレクトリに収録されています。これらのツールとオリジナルの **salt.cid** および **EFS リカバリ・ファイル**を使用すると、操作不能になった ProtectDrive システムを復旧するのに十分な機能が実現します。

DISPEFS.EXE - ProtectDrive 診断ユーティリティ

この診断ツールには、ProtectDrive システム・ファイルの内容が表示されます。ProtectDrive では、システム・データが EFS（Embedded File System）に含まれるさまざまなファイルに保存されます。

使用例： **DISPEFS.EXE** [オプション] [>output_text_file]

オプション	説明
/? -usage	使用例のヘルプを表示します。
/a -all	すべての ProtectDrive システム・ファイルの内容を表示します。
/d -dtes	ドライブ・テーブルのエントリを表示します。
/c -cfg	設定データを表示します。
/k -dky	鍵データを表示します。
/x -ex	交換データを表示します。
/u -user	プリブート・ユーザ・データベースを表示します。
/r -rec	リカバリ・ファイルのデータを表示します。
/rp -recpath	リカバリ・ファイルへのパスを指定します。
引数なし	システム・ファイルをすべて表示します。

DECDISK.EXE - ディスク復号化ユーティリティ

この 16 ビット MS-DOS コマンド・プロンプト・ディスク暗号化ユーティリティは、ブート不可能な Windows インストールを復号化する場合（GUI ベースの復号化機能を使用できない場合など）のみ使用できます。Windows がブート可能な場合、[PD 設定] > [暗号化ステータス] から管理コンソールの復号化機能を使用してください。

decdisk を使用して復号化を完了し、Windows のブートが可能になったら、再度ディスクを暗号化します。

使用例： **DECDISK.EXE** [オプション]

オプション	説明	デフォルト
/? -usage	使用例のヘルプを表示します。	
/v -ver	ユーティリティのバージョンを表示します。	
/d -display	暗号化情報のみを表示します。	
/a -all	暗号化されたパーティションをすべて表示します。	ユーザが指定します。
/e -est	復号化と /r オプションのための領域の測定	
/r -rec	暗号化処理にリカバリ・ファイルを使用します。	
/rp -recpath	リカバリ・ファイルへのパスを指定します。 (backup.exe コマンドで作成したバックアップ・ファイルの場所)	現在のディレクトリです。
/dk -diskkeyfile	できるだけこのオプションを指定してください。ディスク鍵の復旧のために暗号化されたディスク鍵を指定するためです。/r と一緒に指定することも可能です。*.dke ファイルから、ディスク鍵を読み込みます。	

Decdisk は、最初に既知のハードディスクすべてに関するパーティション情報を表示します。出力結果は、次ページに示す例のようなものになります。

もし、decdisk で表示された暗号化情報内のディスク番号を間違えて指定した場合には、decdisk を終了して、/e オプションで正しい情報を取得してください。

Partition Information

Disk	Start Sector	End Sector	Megabytes	Type...
1	63	16771859	8189	Primary (Boot)
1	16771923	78140159	29964	Logical
2	63	417689	203	Primary
2	417690	10217339	4784	Primary
2	10217403	12498569	1113	Logical

Area	Disk	Start Sector	End Sector	Algorithm	Megabytes	%	Enc'ed
1.	1	63	16771859	3DES CBC	8189	100.00	
		Primary					
2.	2	6771923	78140159	3DES CBC	29964	100.00	
		Logical					
3.	2	63	417689	3DES CBC	203	100.00	
		Primary					
4.	2	417690	10217339	3DES CBC	4784	100.00	
		Primary					
5	2	10217403	12498569	3DES CBC	1113	100.00	
		Logical					

Select encrypted area to decrypt. (Ctrl-C to exit) _

上の例では、**decdisk** に既知のハードディスク・パーティションすべてに関する情報が表示されます。**Disk** は物理ディスクの番号です。**Start Sector** と **End Sector** は、物理ディスクの起動に関係します。**Decdisk** では、上のパーティションの暗号化ステータスに関する情報も表示されます。**Start Sector** と **End Sector** 列には、暗号化の範囲が表示されます。**Area** セクションの値は、復号化する領域の選択に使用します。

ユーザは、復号化対象となる暗号化領域を 1 つ選択する必要があります。復号化の進捗状況に応じて、次のように、ユーザにまだ復号化されていない暗号化領域の割合と、復号化のおおよその残り時間が通知されます。

75.10% 3hrs:15mins remaining (Press Ctrl-C to stop)

復号化が完了したら、暗号化領域のリストが更新されます。暗号化領域が残っていない場合、次のようなメッセージが表示されます。

No encrypted areas found.

リカバリ・ファイルの使用

重大なシステム障害が発生した場合、ProtectDrive のシステム・ファイルにアクセスできなくなります。このような場合、**decdisk.exe** でバックアップ済みのリカバリ・ファイルが必要となります。これらのファイルは、ProtectDrive の通常の動作中に **backup.exe** を使用して生成します。

次のようなコマンド・ラインのシンタックスにより、ユーザは復号化するパーティションを選択できます。

decdisk -dk l:¥pd¥diskkeys¥computer.dke -r -rp l:¥pd¥backups¥computer¥

l:¥pd¥diskkeys に存在する **computer.dke** はディスク鍵です。**l:¥pd¥backup¥computer** にはバックアップ・ファイル（復旧ファイル）が存在します。

復旧ファイルを使用して **decdisk** 起動後には、**fdisk /mbr** コマンドの実行が必要となります。詳細は、130 ページのディスクの復旧を参照してください。

手動での復号化領域の指定

Decdisk では、セクタ番号により復号化するディスク領域を選択できます (**/e | -est** オプションを使用します)。**Sart Sector** と **End Sector** および **Algorithm** は、ユーザが次のように手動で入力してください。

```
Partition Information
Disk   Start Sector   End Sector   Megabytes   Type...
1      63             16771859    8189        Primary (Boot)

Enter disk number 1
Enter start sector 63
Enter end sector 16771859
Enter Alg (1=DES, 2 = 3DES, 3 = Idea) 3

-----
Area Disk Start Sector   End Sector   Algorithm   Megabytes % Enc'd
1.    1      63             16771859    3DES CBC    8189      100.00

Select encrypted area to decrypt. (Ctrl-C to exit)
```

RMBR.EXE - MBR 復旧ユーティリティ

ProtectDrive のブート・マネージャおよびマスター・ブート・ローダは、システム BIOS のロード直後に実行されるユーティリティです。ProtectDrive のインストール中、MBR の一部が変更されます。これにより、システムのブート時に、他のすべてのディスクからアクセスされる前に、ProtectDrive で組み込みファイル・システムを特定できます。ProtectDrive のインストール後に MBR が変更、置換、または破損した場合、**rmbr.exe** ユーティリティを使用して復旧します。

ProtectDrive の MBR を復旧するには、ブート・パーティションに組み込まれているファイル・システムのセクタを個別に検索する必要があります。組み込みファイル・システムをいったん特定すれば、ProtectDrive の MBR を復旧できます。ProtectDrive をインストールする前の既存のシステム MBR に戻す場合は、**fdisk /mbr** コマンドを使用します。

使用例： **RMBR.EXE** [オプション]

オプション	説明
/? -usage	使用例のヘルプを表示します。
/v -ver	ユーティリティのバージョンを表示します。
/p -pd	ProtectDrive の MBR を復旧します。
/o -original	元のシステム MBR を復旧します。このオプションは fdisk /mbr と同じです。
/r -recovery	ProtectDrive リカバリ・ファイルを使用して、上の操作のいずれかを実行します。
/rp -recpath	ProtectDrive リカバリ・ファイル（ backup.exe で取得もしくは Active Directory で取得したバックアップ・ファイル）を指定します。

注意： **decdisk** を使用して “/r [/rp..]” オプションで、ディスクの復号化でバックアップ・ファイルを指定した場合には、MBR の復旧で **rmbr** コマンドでも “/r [/rp..]” オプションを指定してください。

RMBR 初期状態のチェック

MBR の復旧を実行する前に、**rmbr** を使用して現在の MBR の状態を表示します。ProtectDrive の MBR がインストール時から一度も変更されていない場合、次のようなメッセージが表示されます。

Current MBR is the ProtectDrive MBR

ただし、**rmbr** で ProtectDrive の MBR の変更が検出された場合、次のようなメッセージが表示されます。

Current MBR is not the ProtectDrive MBR

RMBR バージョンの互換性チェック

現在のバージョンの **Rmbr** が ProtectDrive システムで動作するかどうか確認します。

バージョンが間違っている場合は、次のようなメッセージが表示されます。

```
Incompatible versions
ProtectDrive Version:8.1 (example)
RMBR.EXE Version:X.X.X (example)
```

注意： システム・データの破損の度合いによっては、現在インストールされている ProtectDrive システムのバージョンを特定できない場合があります。

ProtectDrive MBR の復旧 (RMBR /p)

RMBR では、最初にすべての ProtectDrive パーティションのリストを表示します。ProtectDrive の MBR を復旧したいパーティションを選択します。

```
Disk   Start Sector   End Sector   Megabytes   Type...
1      63             16771859    8189        Primary (Boot)
(ProtectDrive)
```

```
Select partition to recovery. (Ctrl-C to exit) _
Current MBR is not the ProtectDrive MBR
Searching for super block from sector 63 to sector 20487599
99.99% and 3hrs 20mins remaining. (Press Ctrl C to stop)
```

Rmbr.exe によりディスクのセクタが検索され、ProtectDrive に組み込まれたファイル・システムの先頭に対応する ProtectDrive のスーパーブロックを検索します。インストール済み ProtectDrive システムのデータがディスクに残っている場合があります。スーパーブロックが見つかって、そのブロックが現在の ProtectDrive のインストールと一致しない場合、次のようなメッセージが表示されます。

```
Found super block at sector 1893443
Incorrect super block.Continuing search ..
```

有効なスーパーブロックが見つかり、RMBR によりそのバージョンが表示され、次のようにユーザは確認を求められます。

```
Found super block at sector 1893443
ProtectDrive v8.1
Is this the correct version of ProtectDrive?[Y/N]
```

バージョンが違う場合、「N」と入力して **rmbr** を続行します。バージョンが正しい場合、「Y」と入力すると次のようなメッセージが表示されます。

```
ProtectDrive MBR restored.
Current MBR is the ProtectDrive MBR.
```

元の MBR の復旧 (RMBR /o)

このオプションを使用すると、現在の MBR がインストール時から保存されていた元のシステム MBR に戻ります。このオプションは、現在暗号化されているドライブがシステム上に存在しない場合のみサポートされます。それ以外の場合は、復号化してから作業を進めてください。

PDUSERDB.EXE – プリブート・ユーザ・データベース管理ユーティリティ

この MS-DOS コマンド・ライン・ツールでは、ProtectDrive のプリブート・ユーザ・データベースを操作することにより、ProtectDrive の管理者が次のことを実行できます。

- ProtectDrive プリブート認証の実行を許可されたユーザの名前をリストに表示します。
- ローカルおよびドメイン（トークンおよび PIN ユーザ・アカウントを含む）のユーザ・アカウントを ProtectDrive プリブート・ユーザ・データベースから削除します。
- ローカルおよびドメイン（トークンおよび PIN ユーザ・アカウントを含む）のユーザ・アカウントを ProtectDrive プリブート・ユーザ・データベースへ追加します。

使用例： **PDUSERDB.EXE [オプション]**

オプション	説明
/? -usage	使用例のヘルプを表示します。
/a -add	ユーザをプリブート・データベースへ追加します。
/d -domain	新規追加したユーザが属する Windows ドメイン（通常ローカル・システム名）を指定します。
/f -file	ユーザ証明書を含むファイルの名前を指定します。
/l -list	既存のプリブート・ユーザをすべてリスト表示します。
/n -name	プリブート・データベースへ追加するユーザ名を指定します。
/p -password	新規追加したユーザのパスワードを指定します。
/r -remove	ユーザをプリブート・データベースから削除します。
/v -version	バージョン情報を表示します。

注意：パスワードを変更するには、ユーザ・アカウント（/r）を最初に削除してから、新しいパスワードのアカウント（/a）を追加します。

第13章 トラブルシューティング

32bit プリブートと 16bit プリブートの切り替え

何らかの問題で、32bit プリブートを 16bit プリブートに変更する場合には、以下の手順で行ってください。

1. パソコンの起動が開始されたら、[Shift]キーを押し続けてください。
2. 16bit プリブート認証が起動し、ProtectDrive の以前のバージョンのログオン画面が表示されます。



32bit プリブート認証画面 (標準)



16bit プリブート認証画面

3. 通常通りログオンを実行してください。

注意：再起動時には、再度 32bit プリブートが標準となります。

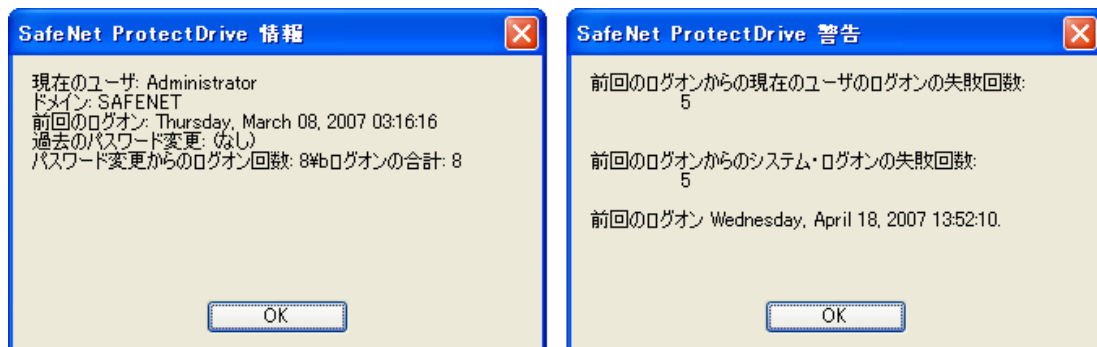
ディスク暗号化に関する警告

システム・ポリシーの [ディスク暗号化] タブで [ディスクが暗号化されていない場合には警告を表示] が設定されている場合は、まったく暗号化されていないか、または完全に暗号化されていないドライブがあることが分かったと、Windows エクスプローラのシェルがロードされた直後に、次のようなメッセージが表示されます。



ProtectDrive ユーザ認証の動作の追跡

システム・ポリシーの [ユーザ・インターフェース] タブで [ログオン情報の表示] または [無効なログオンへの警告の表示] が設定されている場合は、Windows 認証が完了してから Windows エクスプローラのシェルがロードされるまでの間に、次のような 2 つの ProtectDrive 情報ダイアログが表示されます。これらのダイアログは、ユーザにこれまでの ProtectDrive のプリブート認証の動作を警告しています。



プリブート・ユーザ名またはパスワードを間違えた場合

ロックアウト・ポリシーでは、プリブート認証試行の最大失敗回数と、ロックアウトの期間を定義します。ロックアウトが発生すると、次のような画面が表示されます。



[PD 設定] -> [高度] -> [ロックアウト] で定義された間、カウントダウンが行われ、この間はシステムにアクセスできなくなります。

(ログオン試行の失敗やその他のイベントの詳細については、システムの [イベント・ビューア] を開いてください。[イベント・ビューア] の詳細については、144 ページを参照してください)。

システムの停止によるプリブート・ログオンの失敗

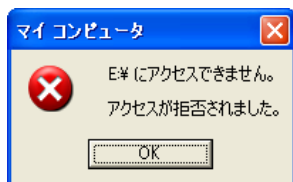
ProtectDrive のシステム・ファイルまたは暗号化ハードディスク・パーティションのいずれかが破損している場合、ユーザはプリブート時のシステム認証を実行できなくなります。場合によっては、以下の例のように、エラー画面に ACS エラー番号が表示されます。ユーザはエラーの内容をシステム管理者に通知する必要があります。

Error ACS0301

ACS エラー・コードの全リストについては、付録 D を参照してください。

デバイスへのアクセス拒否エラー

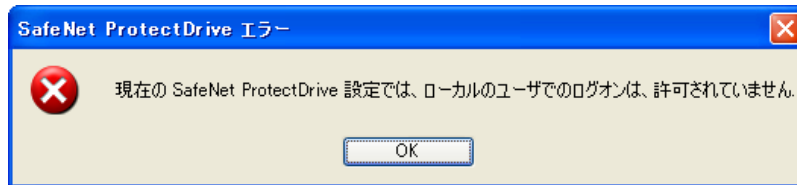
ProtectDrive 管理者は、ユーザがリムーバブル・メディアなど特定のデバイスへアクセスするのを拒否するようシステムを設定できます。デバイスへのアクセス制御権が無効なユーザが特定のデバイスにアクセスしようとする、次のようなメッセージが表示されます。



この場合、システム管理者に問い合わせてください。

ローカル Windows 認証の拒否エラー

システム・ポリシーの [ローカル・ユーザのアクセスを許可] 認証オプションが無効になっている、ブート後に Windows のログオン画面の [ドメイン] フィールドでローカル・システム名を指定してローカルの Windows への認証を実行しようとする、次のようなエラーが表示されます。

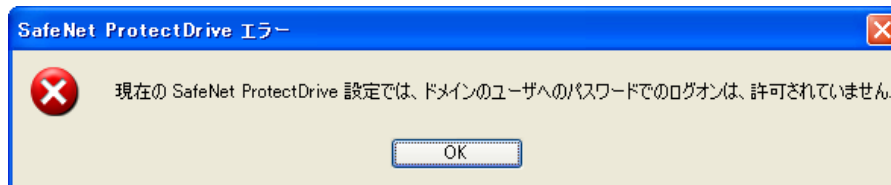


[ローカル・ユーザのアクセスを許可] と [パスワード・ドメイン・ユーザのアクセスを許可] のオプションが両方無効になっている場合、**Ctrl**、**Alt**、**Del** キーを同時に押しても何も起こりません。

同様に、[トークン・ドメイン・ユーザのアクセスを許可] が無効になっている場合も、スマートカードおよびトークンを挿入しても何も起こりません。

ブート後の Windows ドメイン認証の拒否エラー

システム・ポリシーの [パスワード・ドメイン・ユーザのアクセスを許可] 認証オプションが無効になった状態で、Windows のログオン画面を使用してユーザが Windows ドメインへの認証を実行しようとする、次のようなエラーが表示されます。



イベント・ビューアのログ

イベント・ログを注意深く監視すると、プリブート認証試行の成功および失敗、ドライブ暗号化の開始時間や終了時間など、ProtectDrive エラーの詳細を識別および表示できます。

Windows デスクトップからイベント・ビューアへアクセスするには、次の手順を実行してください。

1. [スタート]>[設定]>[コントロール・パネル]>[管理ツール]>[イベント・ビューア] を選択してください。
2. [イベント・ビューア] のツリーから [アプリケーション] をクリックしてください。リストをスクロールしてイベントを表示します。

種類	日付	時刻	ソース	分類	イベントID	ユーザー	コンピュータ名
情報	2007/04/18	135245	SafeNet ProtectDrive	なし	4097	N/A	SAFENET
情報	2007/04/18	134101	SafeNet ProtectDrive	なし	4097	N/A	SAFENET
情報	2007/04/18	134027	SecCli	なし	1704	N/A	SAFENET
情報	2007/04/18	134002	SafeNet ProtectDrive	なし	12289	N/A	SAFENET
情報	2007/04/18	135606	SecurityCenter	なし	1807	N/A	SAFENET
情報	2007/04/18	135606	SafeNet Token Service	なし	0	N/A	SAFENET
情報	2007/04/18	135606	SafeNet Token Service	なし	5	N/A	SAFENET
情報	2007/04/18	135603	vmtools	なし	105	N/A	SAFENET
情報	2007/04/18	135603	StorageEncryptionServ...	なし	4098	N/A	SAFENET
情報	2007/04/18	135558	DKLOG	なし	0	N/A	SAFENET
情報	2007/04/18	135557	ClientDataManager	なし	4098	N/A	SAFENET
情報	2007/04/18	142518	SafeNet ProtectDrive	なし	4097	N/A	SAFENET
情報	2007/04/18	140223	SafeNet ProtectDrive	なし	4097	N/A	SAFENET
情報	2007/04/18	134940	SecCli	なし	1704	N/A	SAFENET
情報	2007/04/18	140559	SafeNet ProtectDrive	なし	4097	N/A	SAFENET
情報	2007/04/18	132631	SafeNet ProtectDrive	なし	4097	N/A	SAFENET
情報	2007/04/18	141402	MainInstaller	なし	11728	Administrator	SAFENET
情報	2007/04/18	131037	MainInstaller	なし	11707	Administrator	SAFENET
情報	2007/04/18	130955	SafeNet Token Service	なし	0	N/A	SAFENET

3. イベントのプロパティや特定の詳細情報を表示するには、そのイベントをダブルクリックしてください。

イベントのプロパティ

イベント

日付(A): 2007/02/18 ソース(S): SafeNet ProtectDrive
時刻(M): 13:30:02 分類(R): なし
種類(E): なし イベント ID#: 12289
ユーザー(U): N/A
コンピュータ(O): SAFENET

説明(D):

プレブート認証に成功しました。 Wednesday, April 18, 2007 13:51:52 パスワード/ログオン。 [SAFENET-INC/Administrator]

データ(T): ☒ バイト(B) ☐ ワード(W)

OK キャンセル 適用(A)

緊急時のワンタイム・ログオン・イベント

緊急時のリカバリ・ログオン手順が発生した場合には、イベント・ログにエントリが追加されます。緊急時のログオン・イベントは、次の例に示すように 40 個のゼロで指定されます。

The screenshot shows the Windows XP Event Viewer window titled "イベントのプロパティ". The left pane shows "イベント" expanded under "ログ". The right pane displays details for event ID 12289:

- 日付(A):** 2007/09/10
- 時刻(M):** 17:58:40
- 種類(E):** なし
- ソース(S):** SafeNet ProtectDrive
- カテゴリ(C):** なし
- イベント ID(I):** 12289
- コンピューター(Q):** SAFENET-A6EC36B

The "説明(D)" field contains the following text:

```

プレブート検証に成功しました。 Monday, September 10, 2007 17:58:14 トークン・ログオン [SAFENET-A6EC36B/System SAFENET-A6EC36B]
{0000000000000000000000000000000000000000}
  
```

A red rectangle highlights the hexadecimal string at the bottom of the description.

Active Directory および ADAM のレポート・スクリプト

PDReport.vbs レポート・スクリプトは、Windows ドメイン内のすべてのクライアント・コンピュータに関する暗号化ステータスを表示する場合に使用します。このツールは、特にコンプライアンスの監査目的で使用されます。**PDReport.vbs** スクリプトは、ProtectDrive インストール CD の *Tools* ディレクトリに収録されています。

PDReport.vbs スクリプトを実行する前に修正する必要はありませんが、修正してカスタマイズすることは可能です。

ProtectDrive クライアントを管理している Active Directory または ADAM サーバでこのスクリプトを実行します。このレポート・スクリプトを実行する手順は、Active Directory サーバと ADAM サーバで若干異なります。これらの手順を次に示します。

レポート・スクリプトを実行すると、**PDReport.csv** ファイルが作成されます。この出力には、クライアント・コンピュータ名の一覧と、以下の情報が含まれます。これらの情報は、Microsoft® Office Excel などの表計算アプリケーションで簡単に表示できます。

- **PDStatus** - クライアントにアクセスできる場合は [アクティブ]、アクセスできない場合は [非アクティブ] となります。
- **LastUpdate** - ProtectDrive サーバによりクライアントが最後に更新された日付と時刻を表示します。
- **EncryptedDrives** - 現在クライアントで暗号化されているドライブを表示します。このカラムが空白の場合、クライアントに暗号化ドライブがないことを示します。

Active Directory を使用する ProtectDrive サーバ

ProtectDrive インストール CD の *Tools* ディレクトリでファイル名をダブルクリックするか、またはコマンド・ラインからファイルを実行すると、**PDReport.vbs** を実行できます。

このファイルを実行するには、コマンド・ラインおよび DOS プロンプトからスクリプトを実行する *Tools* ディレクトリへ移動します。

ADAM を使用する ProtectDrive サーバ

コマンド・ラインもしくは DOS プロンプトから **PDReport.vbs** を実行する必要があります。このファイルを実行するには、コマンド・ラインもしくは DOS プロンプトからスクリプトを実行する *Tools* ディレクトリへ移動し、次のコマンド形式を使用します。

PDReport.vbs <ADAM がインストールされているサーバ名>:<ポート番号>

例 : **PDReport.vbs win2k3ent_server:50000**

レポートの出力例

ComputerName	PDStatus	LastUpdate(UTC)	EncryptedDrives
W2K3ENT-CLIENT1	Active	7/5/2007 18:10	C:D:
W2K3ENT-CLIENT2	Active	6/29/2007 06:08	C:
W2K3ENT-CLIENT3	Inactive		
W2K3ENT-CLIENT4	Active	7/2/2007 10:20	C:

付録A

スマートカードとトークンの PIN でのユーザ認証

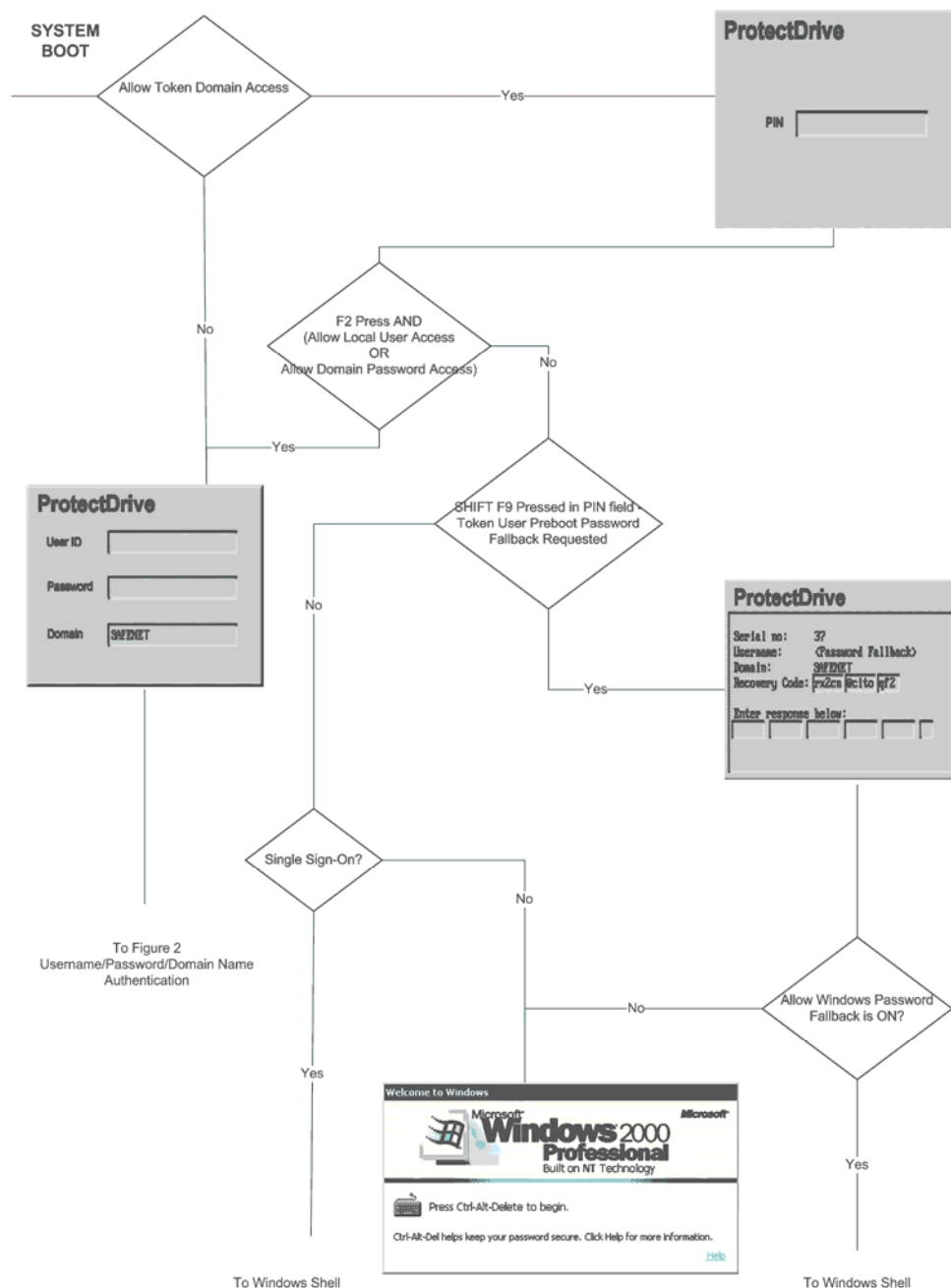


Figure 1
Smartcard/Token/PIN
Preboot Authentication

注意：共通鍵による iKey 1000 でのトークン認証の場合には、シングル・サイン・オンは動作しません。

付録B

ユーザ名、パスワードとドメインでの認証

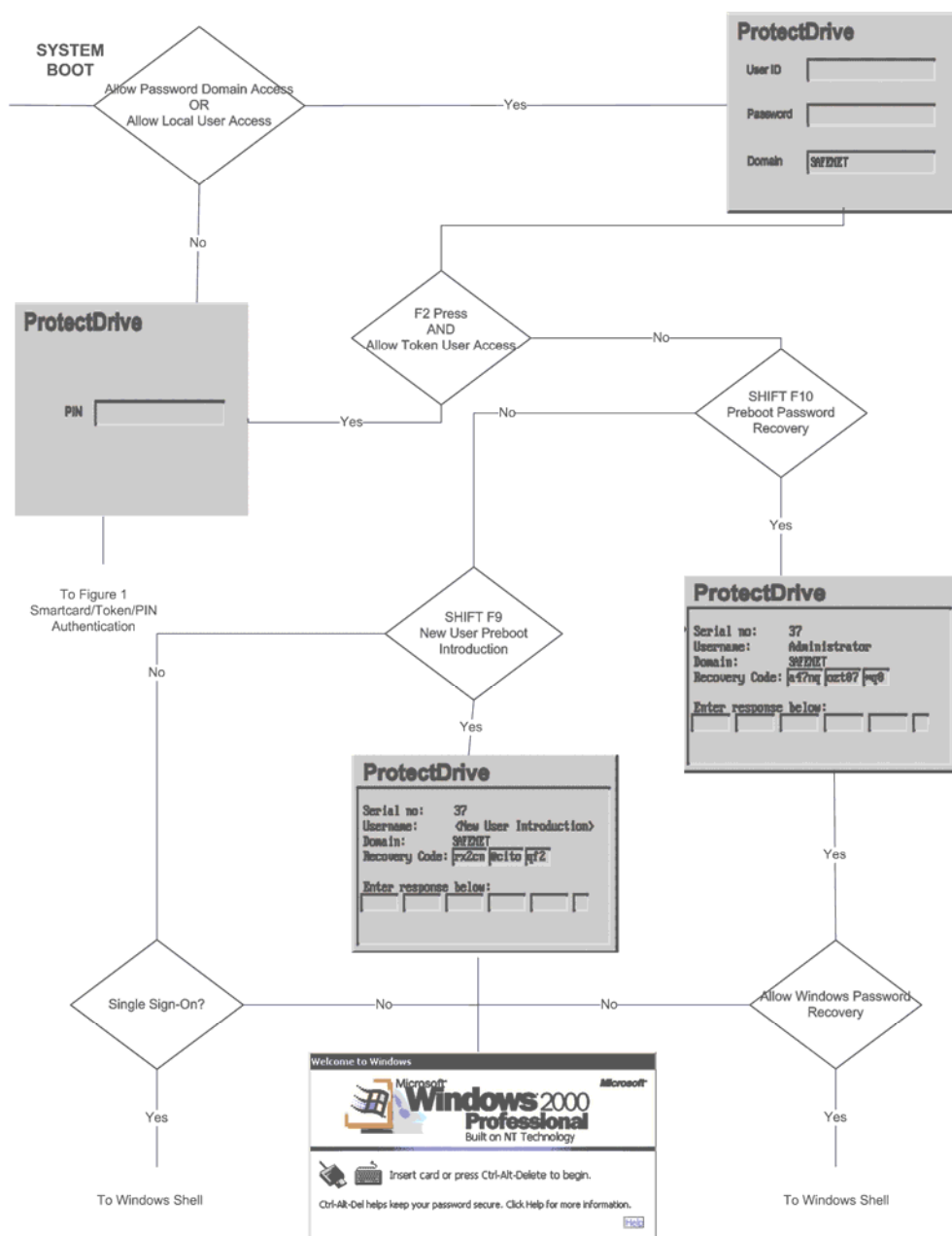


Figure 2
Username/Password/Domain Name
Preboot Authentication

付録C

ブート後の Windows ユーザの認証

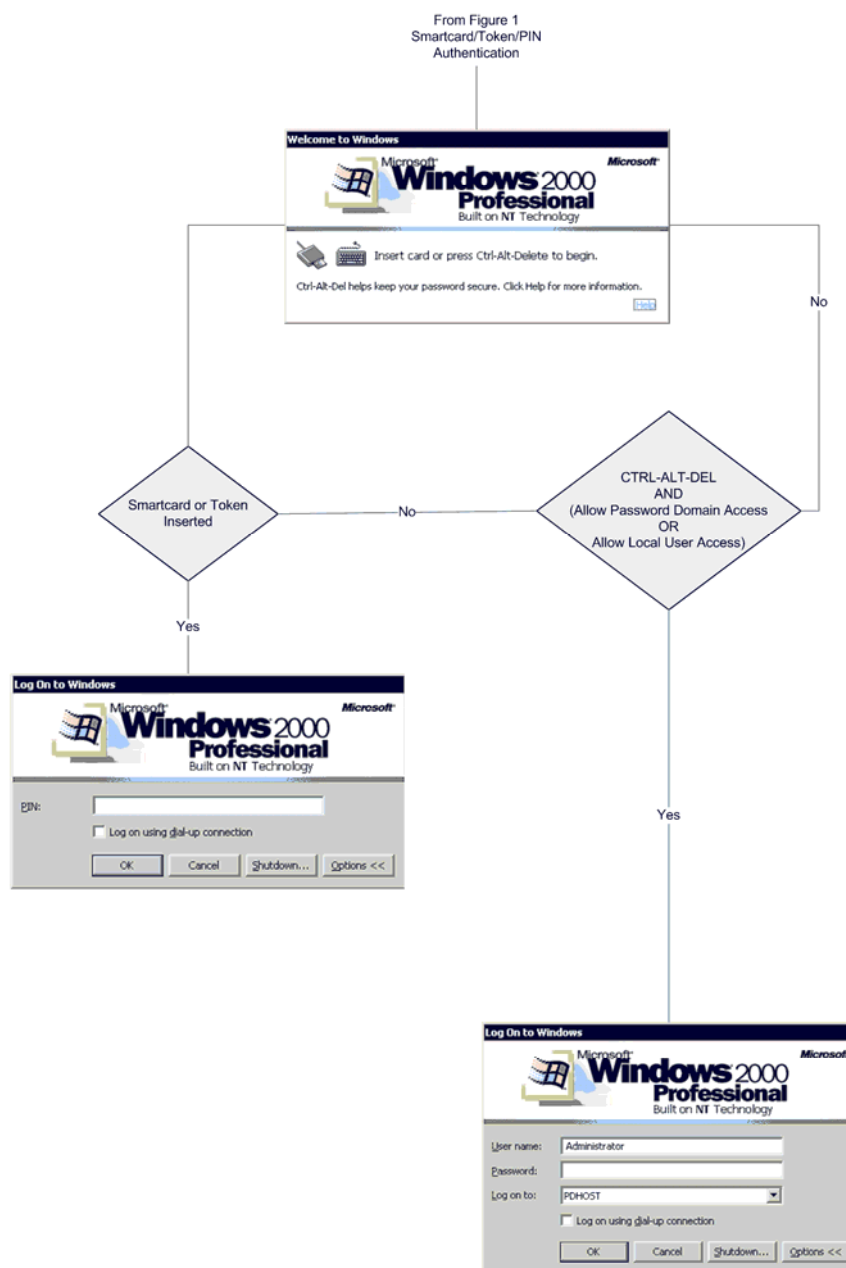


Figure 3
Smartcard/Token/PIN or
Username/Password/Domain
Postboot Authentication

付録D

システムのデバッグおよび ACS エラー・メッセージ

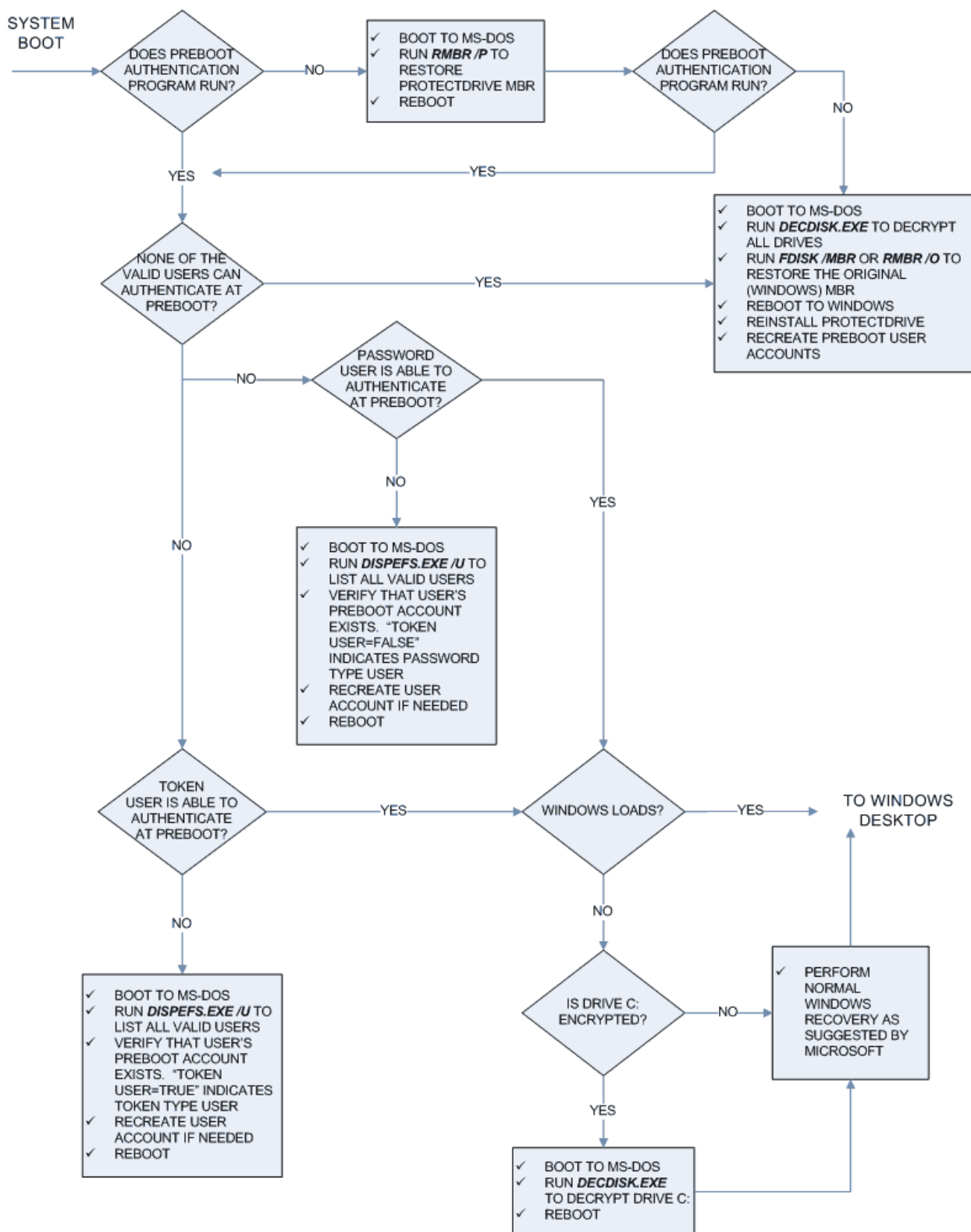
はじめに、[第 12 章 - 障害復旧ツール](#)の内容をよく理解してください。

システムのデバッグ

問題	解決策
パスワード型アカウントのユーザを ProtectDrive のプリブート認証プログラムで認証できない	<p><i>Dispefs.exe /u</i> を実行します。これにより、すべてのユーザとそのアカウントの種類が表示されます。パスワード型アカウントのユーザは、「Token User = False」という設定で表示されます。</p> <p>このユーザがパスワード型アカウントとして表示されている場合、パスワードが無効である可能性があります。パスワードは大文字と小文字が区別されます。</p> <p>最後に、このユーザが正しいパスワードを入力した正規のユーザで、他にログオンできるユーザがない場合、ProtectDrive のファイルが破損している可能性があります。以下の「ProtectDrive が破損している可能性がある」の項目を参照してください。</p>
スマートカードおよびトークン型アカウントのユーザを ProtectDrive のプリブート認証プログラムで認証できない	<p><i>Dispefs.exe /u</i> を実行します。これにより、既存のユーザとそのアカウントの種類がすべて表示されます。スマートカードおよびトークン型アカウントのユーザは、「Token User = True」という設定で表示されます。</p> <p>ユーザが複数のトークン・アカウントを持っても、そのトークンに含まれる証明書が、ProtectDrive のプリブート・ユーザ・データベースにこのユーザのレコード作製するために本来使用されていた証明書と一致しない場合があります。プリブート・ユーザ・データベースにこのユーザ・レコードが複数存在する可能性があります。<i>Dispefs.exe /u</i> を実行して表示される【ハッシュ】フィールドは、Windows で証明書の詳細情報を表示したときに表示される【拇印】フィールドと同じです。</p> <p>最後に、このユーザが有効なトークンを使用する正規のユーザで、他にログオンできるユーザがない場合、ProtectDrive のファイルが破損している可能性があります。以下の「ProtectDrive が破損している可能性がある」の項目を参照してください。</p>

問題	解決策
ユーザがプリブート認証を完了したのに Windows がブートしない	<p>Windows システム・ファイルのいずれかが破損している可能性があります。ドライブ C が暗号化されていない場合、通常の Windows の復旧操作を実行します。</p> <p>ドライブ C が暗号化されている場合、システム・ドライブを復号化してから Windows の復旧ツールを有効にして、システム・ドライブにアクセスします。</p>
ProtectDrive のプリブート認証プログラムを実行できない	<p>fdisk /mbr または別のユーティリティにより ProtectDrive MBR が置き換えられた場合、プリブート認証プログラムを実行できません。</p> <p>システム・ドライブが暗号化されている場合、オペレーティング・システムもロードできません。</p> <p>システム・ドライブは暗号化されていないが他のドライブが暗号化されている場合、オペレーティング・システムのロードは可能ですが、暗号化ドライブへのアクセスは、ProtectDrive のドライバにより拒否されます。</p> <p>この状況を回避するには、rmbr /p を実行します。</p>
ProtectDrive が破損している可能性がある	<p>ProtectDrive が破損している場合、次のいずれかの原因が考えられます。</p> <ul style="list-style-type: none">• プリブート認証プログラムを実行できない、または正常に動作しない• 有効なユーザをプリブート時に認証できない• オペレーティング・システムをロードできない <p>上記の項目がいずれも該当しない、または ProtectDrive の復旧手順を間違えた場合、decdisk.exe を使用して暗号化ドライブをすべて復号化する必要があります。</p> <p>decdisk.exe から ProtectDrive の EFS (Embedded File System) にアクセスできない場合、backup.exe で作成済みのリカバリ・ファイルを使用します。</p> <p>すべてのドライブの復号化が完了したら、fdisk /mbr または rmbr /o を実行して ProtectDrive MBR を復旧します。</p> <p>システム・ドライブの復号化が完了すると、オペレーティング・システムをブートできます。すべてのドライブを復号化するまでは、ProtectDrive をアンインストールすることはできません。</p>

次のページにあるフローチャートは、前述のシステムのデバッグ情報を表しています。この図は情報の補足を目的としています。



ACS エラー・メッセージ

ProtectDrive の ACE (Access Control System) は、ProtectDrive がインストールされたコンピュータを起動すると有効になります。初期化中にエラーが発生した場合、システムでエラー・メッセージが表示されます。このメッセージには、エラー番号と簡単な説明が記述されています。

エラー番号は、次の 3 つのコンポーネントからなります。

CTXX :

- C エラー・コードが発生しているモジュール
- T エラーの種類 ID
- XX 実際のエラー番号

モジュールの識別子は、以下のとおりです。

- 0 マスター・ブート・レコード (MBR)
- 1 VXBIO
- 2 未使用
- 3 VROM

データ型の識別子は、以下のとおりです。

- 0 未使用
- 1 警告
- 2 エラー
- 3 重大なエラー

次ページの表に、ACS エラーの全リストと考えられる原因、および推奨される復旧操作を示します。

ACS エラー	コンポーネント	説明	考えられる原因	復旧操作
0301	MBL	無効なマスター・ブート・レコードのチェックサム	MBR の破損 MBR に対するトロイの木馬攻撃	rmbr.exe を実行して ProtectDrive MBR を復旧してください。
0305	MBL	無効な VXBIO または 暗号化されたリムーバブル・メディア (USB) からブートできない	ディスクの破損により、VXBIO のシグネチャ、チェックサム、またはサイズ検証ができない または リムーバブル・メディアに OS が入っていない	SafeNet サポートにお問い合わせください。 または リムーバブル・メディアを取り外してからリブートしてください。 または BIOS 設定で起動順序を変更し、デバイスの一覧で USB の優先順位を下げてください。
0306	MBL	無効なマスター・ブート・レコードのシグネチャ	MBR の破損 MBR に対するトロイの木馬攻撃	rmbr.exe を実行して ProtectDrive MBR を復旧してください。
0307	MBL	SafeNet のパーティション情報が表示されない	パーティション・テーブルの破損 または変更 ProtectDrive インストール後のハードディスクの追加	rmbr.exe を実行して ProtectDrive MBR を復旧してください。
0313	MBL	セクタ読み取り時のディスク I/O エラーによるスタック	ディスク I/O エラー (ハードディスクの障害) またはパーティション・テーブルの破損	rmbr.exe を実行して ProtectDrive MBR を復旧してください。
0314	MBL	VXBIO 読み取り時のディスク I/O エラー	ディスク I/O エラー (ハードディスクの障害) またはパーティション・テーブルの破損	rmbr.exe を実行して ProtectDrive MBR を復旧してください。
1100	VXBIO	システムを初期化できない	システムからディスク暗号化鍵をロードできない、または DTE EFS が存在しないか破損している	標準的なりカバリ手順
1204	VXBIO	VROM のロード・エラー	VROM ファイルが存在しないか、サイズが間違っているか、または読み取りエラーが発生している	標準的なりカバリ手順
1205	VXBIO	VROM のステータス・エラー	VROM シグネチャ検証に失敗したか、またはプログラム・ローダからエラーがレポートされた	標準的なりカバリ手順

ACS エラー	コンポーネント	説明	考えられる原因	復旧操作
1300	VXBIOS	メモリ不足	VROM メモリの割り当て失敗 使用可能なメモリの不足	リソースを開放してみてください。
1301	VXBIOS	GDA ファイルのロード・エラー	GDA ファイルがないか、または 暗号化情報の初期化をしようとして 読み取りエラーが発生している	標準的なリカバリ手順
1310	VXBIOS	EFS を初期化できない	EFS が破損している	標準的なリカバリ手順
1311	VXBIOS	VROM のロード・エラー	VROM ファイルが存在しないか、 サイズが間違っているか、 または読み取りエラーが発生して いる (ACS1204 エラー後に表示さ れる)	
1312	VXBIOS	VXVECT を保存でき ない	オリジナルのディスク割り込み サービス・ルーチン (ISR) のア ドレスを EFS のスーパーブロック に保存できない EFS が破損している	標準的なリカバリ手順
1313	VXBIOS	SBLK に障害が発生し ている	EFS スーパーブロックを特定でき ない	rmbr.exe を実行して ProtectDrive MBR を復旧してください。
1314	VXBIOS	情報を開くことができ ない	VDX EFS ファイルが存在しない EFS が破損している	標準的なリカバリ手順
1315	VXBIOS	情報を書き込むことが できない	EFS が破損している	標準的なリカバリ手順
1316	VXBIOS	VROM を実行でき ない	VROM を実行できない (ACS1205 エラー後に表示される)	
1317	VXBIOS	情報を読み取ることが できない	EFS が破損している	標準的なリカバリ手順
1318	VXBIOS	フロッピーからブート できない	マスター・ブート・ローダのシグ ネチャ検証に失敗している フロッピーディスクにオペレー ティング・システムが存在しない	ブート可能なフロッピーディスク を使用してください。 フロッピーディスクをドライブ から取り出して、ハードディス クからブートしてください。
1319	VXBIOS	GDA を開くことがで きない	GDA ファイルをロードしようと したが、オリジナルの MBR が存 在しない (実行できない)	標準的なリカバリ手順

ACS エラー	コンポーネント	説明	考えられる原因	復旧操作
1320	VXBIOS	GDA を読み取ることができない	オリジナルの MBR をロード（及び実行）しようとしたが GDA ファイルの読み取りエラーが発生している	標準的なリカバリ手順
1321	VXBIOS	ブートに失敗する	マスター・ブート・ローダのシグネチャ検証に失敗している	標準的なリカバリ手順
3301	VROM	ログオン試行の回数が多すぎる	パスワードを忘れた ユーザ・データベースが破損している	別のユーザとしてログオンします。 ユーザ鍵の復旧を実行してください。 または、dispefs.exe を実行して、ログを取得して、SafeNet へお問い合わせください。
3302	VROM	ディスク読み取り時の I/O エラー	EFS が破損している ハードディスクに障害が発生している	標準的なリカバリ手順
3304	VROM	不明なエラーが発生している	内部プログラムのエラー	標準的なリカバリ手順
3305	VROM	構成ファイルが破損している	構成ファイルの MAC チェックに失敗している EFS が破損している	標準的なリカバリ手順
3306	VROM	ユーザ情報が破損している	ユーザ・データベース・エントリの MAC チェックに失敗している EFS が破損している	プリブート時に別のユーザとしてログオンし、問題の発生しているユーザを Windows へログオンさせます。 ユーザ・データベースのエントリを再生成します。 または、ユーザ鍵の復旧手順を実行してください。

ACS エラー	コンポーネント	説明	考えられる原因	復旧操作
3308	VROM	ProtectDrive 管理者の 情報が破損している	ProtectDrive 管理者の MAC チェッ クに失敗している EFS が破損している	プリブート時に別のユーザとして ログオンし、問題の発生してい るユーザを Windows へログオン させます。 ユーザ・データベースのエント リを再生成します。 または、ユーザ鍵の復旧手順を 実行します。
3309	VROM	構成ファイルが完全に 破損している	EFS が破損している ハードディスクに障害が発生して いる	標準的なリカバリ手順
3310	VROM	トークンの初期化で エラーが発生している	トークン・モジュールを初期化で きないため、パスワードによるロ グオンが許可されていない	このエラーをさらに診断するに は、SafeNet へお問い合わせく ださい。 システムにアクセスするには、 パスワードのフォールバック機 能を実行してください。

付録E

セキュリティに関する追加ガイダンス

ProtectDrive 評価版

この章では、ユーザに ProtectDrive 評価版に関する重要なガイダンスを提供します。ProtectDrive 評価版は、評価のセキュリティ・ターゲットに含まれることを前提にしています。

セキュリティ・ターゲットでは、次を含む評価の基本事項について説明します。

- ProtectDrive の要求するセキュリティに対する脅威
- セキュリティの要求に対応するのに必要な環境および組織の前提条件
- セキュリティの要求を満たすのに必要な ProtectDrive の設定に関する制限事項

ProtectDrive 評価版へ依存するに当たり、ユーザはこの項の推奨事項を守り、セキュリティ・ターゲットの評価を参照し、認定レポートで ProtectDrive 評価版の使用に関するガイダンスを参照してください。

セキュリティ・ターゲットと認定レポートは、Common Criteria の EPL (Evaluated Products List : 評価版製品一覧) に記載されています。ProtectDrive のリストについては、下記を参照してください。

http://www.dsd.gov.au/infosec/evaluation_services/epl/epl.html

セキュリティ・ターゲットと技術評価レポートは、どちらも評価の完了時からオンラインで利用できます。

ProtectDrive ユーザのためのガイダンス

CC 証明書のその他関連資料

このマニュアルと合わせて、次の文書も参照してください。

- セキュリティ・ターゲット
- 認定レポート
- 配布 CD に収録されているリリース・ノート
- 配布 CD に収録されている README.TXT

ユーザは、ProtectDrive 評価版がセキュリティ・ターゲットの対象であることを前提にしていることを理解する必要があります。特に、次の章の内容を理解する必要があります。

- 第3章 – 前提条件

- 第 4 章 – 環境におけるセキュリティ目標

これらの章では、ユーザの責任範囲と、ProtectDrive を安全に利用および管理するのに必要な要件の詳細について説明しています。

製品 ID

お手元の ProtectDrive のコピーが正規のもので正しいバージョンであることを確認するには、次の手順を実行します。

インストール前：

- CD のボリューム・ラベルで製品のバージョン番号を確認します。ボリューム・ラベルのバージョンが PD x.yy.zz となっていることを確認します。x.yy.zz は ProtectDrive のバージョン番号です。ProtectDrive の評価版をお持ちの場合、インストールするバージョンが EPL のリストにあるバージョンと一致することを確認します。
- オンライン・アーカイブから ProtectDrive をインストールする場合、ファイル名が pd_x_yy_zz であることを確認します。x_yy_zz はバージョン番号です。
- 使用する製品のバージョンを参照し、配布 CD に README.TXT とリリース・ノートが収録されていることを確認します。

インストール後：

ProtectDrive のインストール後にバージョン番号を確認します。システム・トレイにある ProtectDrive のアイコンを右クリックして、**[SafeNet ProtectDrive のバージョン情報]** を選択します。

表示されるバージョン番号がインストールされたソフトウェアのバージョン番号と一致することを確認します。

組織の要件

外部システムとの接続

ProtectDrive を使用するシステムの管理責任者は、ProtectDrive のセキュリティ機能を侵害するような外部システムに接続されていないことを確認する必要があります。

ガイダンス

組織内で ProtectDrive を配布、インストール、構成、管理、および運用するための詳細情報を記載したガイダンスを提供する必要があります。

改ざん

製品をインストールするシステムには、物理的な改ざん検出の機能と、改ざんが発生したことをユーザへ明確に通知する機能が必要です。ユーザは定期的にシステムをチェックして改ざんの痕跡がないかどうか確認する必要があります。

トレーニング

管理者特権を持つすべての ProtectDrive ユーザは、ProtectDrive を安全に管理できるように、十分なトレーニングを受ける必要があります。

管理者特権を持つ ProtectDrive のユーザは、評価済みの設定を遵守し、ProtectDrive のインストール、構成、管理、および運用を安全に行うためのガイダンスを導入する責任があります。

トークン

ProtectDrive で使用するスマートカードおよびトークンは、ProtectDrive の認証情報を保護し、ProtectDrive に必要な機能を実行するのに十分なセキュリティのレベルを確保する必要があります。このレベルのセキュリティは、スマートカードとトークンの一方または両方に関する保証と、組織の手順に関する保証を組み合わせではじめて実現できます。

ユーザ

ProtectDrive のユーザは、職務を遂行するのに十分なガイダンスと研修を受ける必要があります。

デバイスのアクセス許可

ProtectDrive では、さまざまな種類のデバイスを安全に使用できるように管理します。設定は、[PD 設定] -> [高度] -> [標準のパーミッション] グループでデバイスごとに読み取りおよび書き込みのアクセス許可を設定することで、システムおよびユーザ・ポリシーに基づいて行います。

オペレーティング・システム構成に関するガイダンス

全般

ProtectDrive では、ブリープ認証や周辺デバイスのアクセス制御、ハードディスクの暗号化などを組み合わせて情報を保護しています。（正しいユーザ認証により）コンピュータへのアクセスが許可されると、ユーザは、使用可能な情報のレベルに関する組織のセキュリティ・ポリシーに従って、そのコンピュータを取り扱う責任があります。

ProtectDrive の管理者は、基盤となるオペレーティング・システムを正しく構成し、組織のセキュリティ・ポリシーを遵守する責任があります。

ProtectDrive がインストールされたコンピュータがネットワーク・ドメインの一部である場合、そのドメインのセキュリティ・ポリシーを正しく構成し、組織のセキュリティ・ポリシーを遵守する必要があります。

パスワード・ポリシー

オペレーティング・システムのパスワード・ポリシーは、組織のポリシーに従って正しく構成し、ProtectDrive の要件を満たす必要があります。次の最小設定を使用する必要があります。

パスワードの履歴を記録する	7つのパスワードまで
パスワードの有効期間	組織のポリシーを遵守
パスワードの変更禁止期間	組織のポリシーのニーズに応じて 1 日以上
パスワードの長さ	組織のポリシーのニーズに応じて 6 文字以上
パスワードは、複雑さの要件を満たす必要がある	有効
暗号化を元に戻せる状態でパスワードを保存する	無効

画面のロック機能

組織の要件に応じて、オペレーティング・システムで**画面のロック**機能を有効にする必要があります。**画面のロック**機能が有効になっていない場合、または正しく設定されていない場合、ProtectDrive のセキュリティ機能に悪影響が及ぶ場合があります。

ProtectDrive の管理者に関する情報

オペレーティング・システム

ProtectDrive の評価版は、特定のバージョンのオペレーティング・システムでテストされています。

本製品はこれ以外の各種 SP およびビルドでも動作すると思われませんが、評価済みの構成で使いたい場合は、上で指定した構成のみで使用するをお勧めします。

評価済み項目

ProtectDrive Server Edition は評価されていません。また、マルチブート・マネージャの機能もありません。さらに、「登録済み製品」のみが評価されています。

暗号化アルゴリズム

政府の助言に従い、AES および 3DES の暗号化アルゴリズムのみが評価されています。また、これらのアルゴリズムをインストール時に選択する必要があります。これにより、正しいコンポーネントがインストールされ、初回の暗号化で使用可能なアルゴリズムの選択肢が AES と 3DES に限定されます。

[ディスクが暗号化されていない場合には警告を表示] オプション

評価構成の場合、作業中のディスクが完全に暗号化されていないかどうかの確認をユーザに求めることができるように、このオプションをオンに設定することを強くお勧めします。このオプションをオンに設定すると、すべてのユーザに警告メッセージが表示されます。

[自動プリブート認証] オプション

このオプションを使用する場合は注意が必要です。また、本書の関連する章の指示に忠実に従う必要があります。

[無効なログオンへの警告の表示] オプション

評価構成の場合、ログオンに失敗した場合にユーザに警告が表示されるように、このオプションをオンに設定することをお勧めします。

アクセス制御

ProtectDrive にはさまざまなアクセス制御オプションがあります。ユーザ ID とパスワード、トークンと PIN、パスワードの復旧およびフォールバック・オプション、新規ユーザの追加などがその例です。

ProtectDrive の評価版には、これらすべてのアクセス制御オプションが含まれているわけではありません。ProtectDrive の評価版を使用する場合、ユーザは評価のセキュリティ・ターゲットを参照し、評価版に含まれているオプションを把握する必要があります。ProtectDrive 評価版に含まれるアクセス制御オプションのみを有効にする必要があります。

付録F

iKey の管理

iKey 1000 の管理

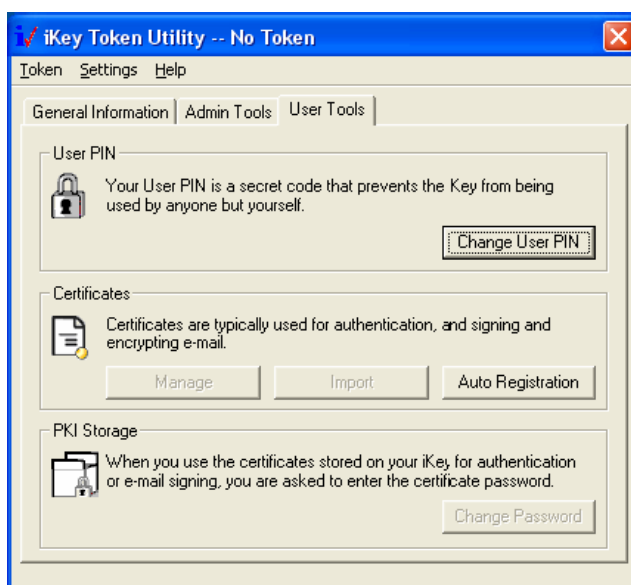
SafeNet の iKey1000 トークンを ProtectDrive と組み合わせて使用すると、保護された二要素認証を簡単に実現できます。このセクションでは、iKey 1000 を標準的な iKey SDK から管理する方法について簡単に説明します。詳細については、『iKey 1000 Series Developer’s Guide』を参照してください。

次の手順は、iKey1000 ソフトウェア（デバイス・ドライバおよび iKeyAPI.DLL を含む）が正しくインストールされていることを前提としています。詳細については、iKey1000 のマニュアルを参照してください。

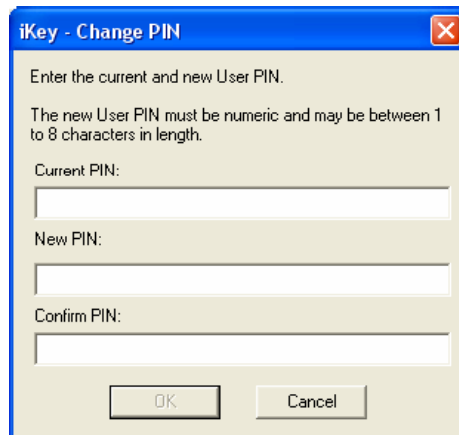
iKey SDK による iKey1000 の管理

PIN を割り当てるには、次の手順を実行します。

1. iKey 1000 トークンを挿入します。
2. Windows のデスクトップで、[スタート]-> [プログラム] -> [SafeNet] -> [iKey Components] -> [iKey Token Utility] の順に選択します。



3. **[User Tools]** タブを選択し、**[Change User PIN]** をクリックしてください。



4. 現在の PIN を入力します（工場出荷時のデフォルトは 12345678）。確認のために新しい PIN を再入力して **[OK]** をクリックしてください。
5. PIN の変更が完了したことを示すプロンプトが表示されたら **[OK]** をクリックしてください。



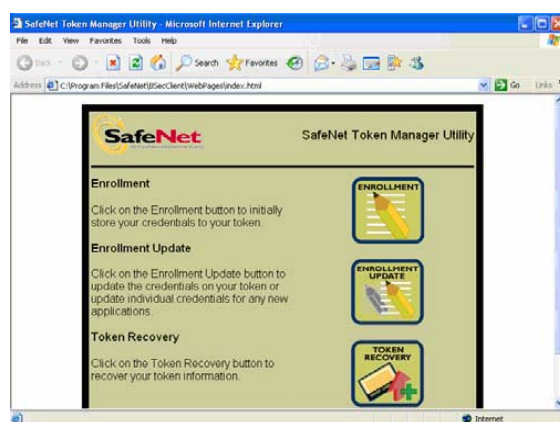
6. これでこのユーザを ProtectDrive データベースへ追加し、ユーザの iKey1000（共通鍵 トークン）を登録できます。この操作は **[PD ユーザ]** タブから実行します。ローカルで実行する場合は LMC から、リモートで行う場合は MMC の **[Active Directory ユーザと コンピュータ]** スナップインから実行します。

iKey 2032 の管理

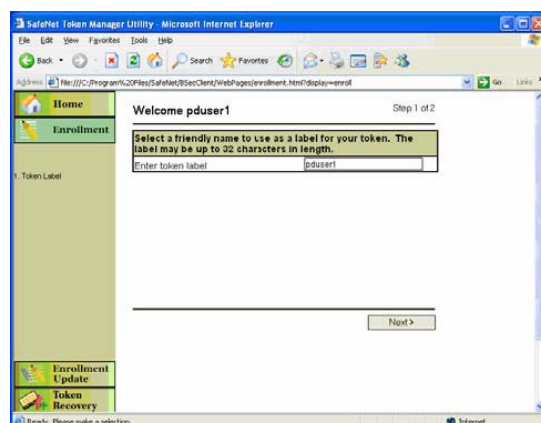
iKey 2032 の管理方法は、SafeNet トークン・マネージャ・ユーティリティと Web 登録の 2 種類があります。

SafeNet トークン・マネージャ・ユーティリティ

1. iKey 2032 トークンを挿入してください。（トークンのライトは点灯したままになっています。）
2. Windows のデスクトップで、[スタート] -> [プログラム] -> [SafeNet] -> [SafeNet Token Manager Utility] の順に選択してください。

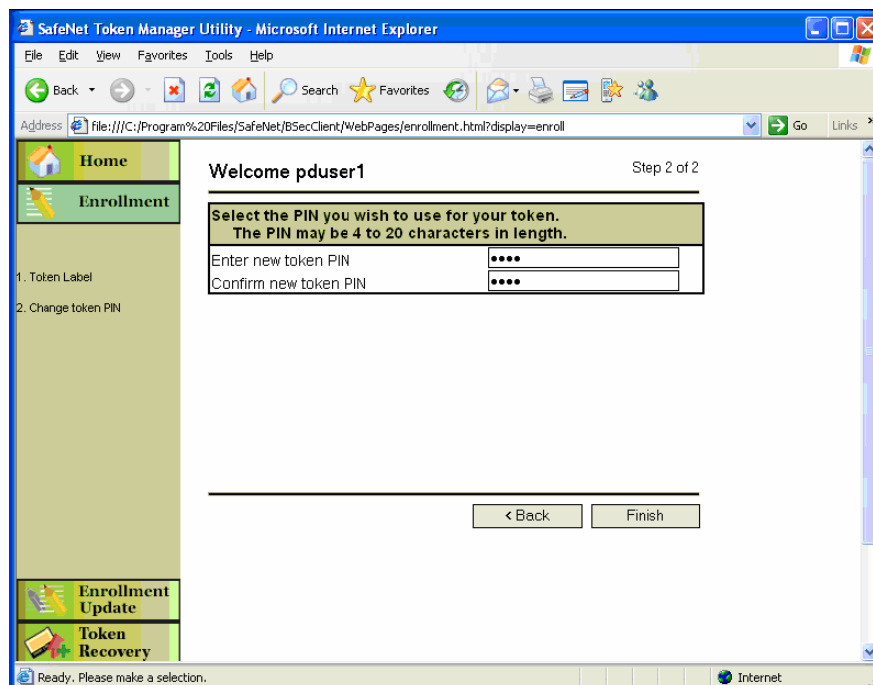


3. [Enrollment] をクリックしてください。
4. プロンプトが表示されたら、このトークンのラベルを入力します（最大 32 文字）。このラベルには、ユーザの名前や、その他の任意の名前を指定できます。



5. [次へ] をクリックしてください。

6. プロンプトが表示されたら、このトークンの PIN を 2 度入力してください（4～32 文字の英数字）。



7. **[Finish]** をクリックしてください。次のようなポップアップ・ウィンドウが表示されます。登録には数分かかります。登録の間、「**Communicating with server**」というメッセージが表示されます。



8. 登録が完了したら **[OK]** をクリックしてください。

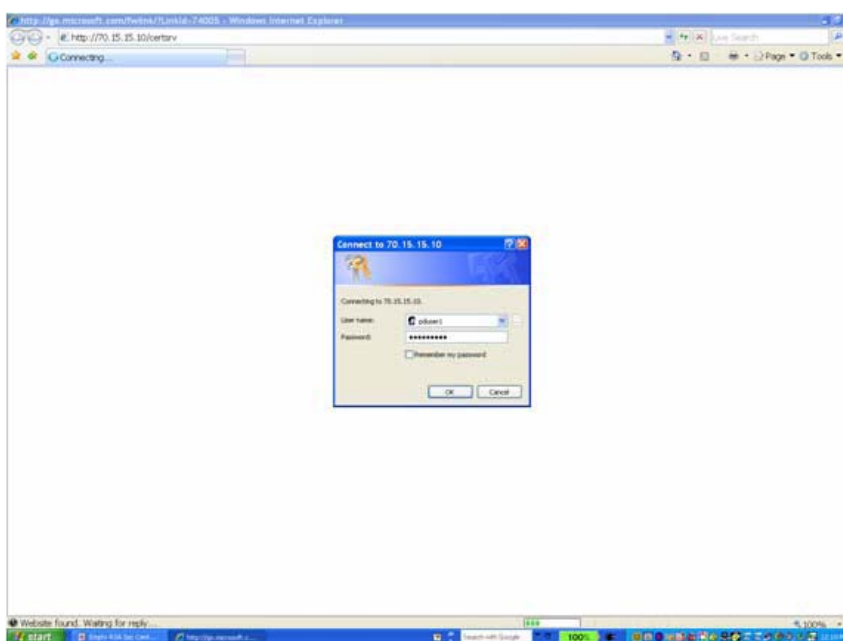


Web 登録

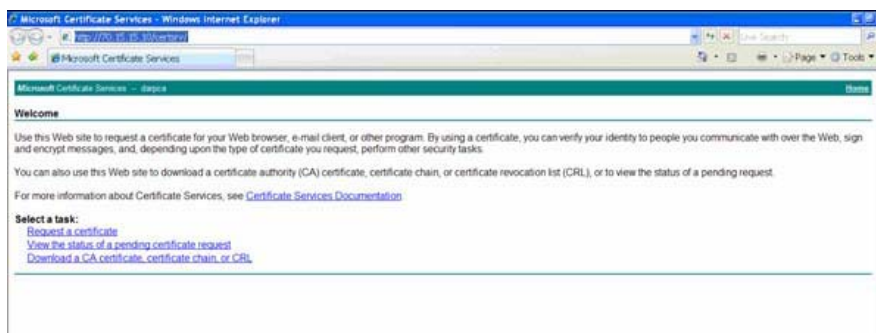
電子認証局からデジタル証明書を iKey にインストールする場合に、下記の手順でデジタル証明書をインストールすることができます。

注意：予め Microsoft Certificate Service および Active Directory の設定は別途行ってください。

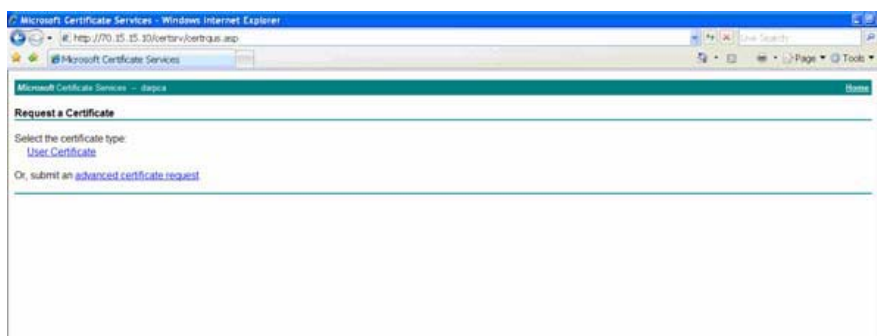
1. 証明書を要求します。Windows Internet Explorer を開き、次のような形式で CA の URL を入力してください。http://<CA の IP アドレス>/certsrv。以下はその例です。
http://70.15.15.10/certsrv
2. プロンプトが表示されたら、有効なユーザ名とパスワードを入力してください。証明書を要求しているユーザの資格情報を指定し、[OK] をクリックしてください。



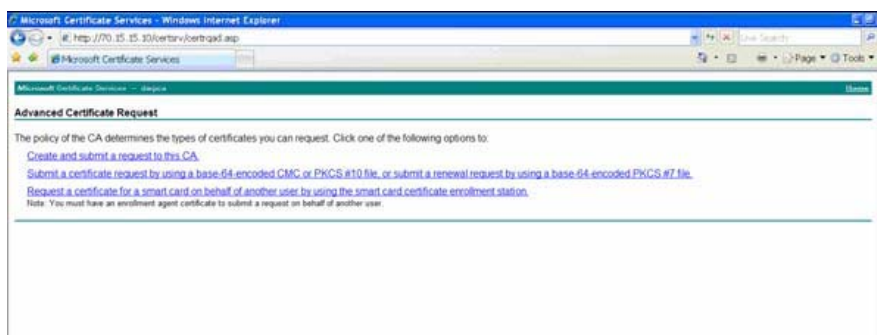
3. 接続されたら、[ようこそ] 画面に CA の [Microsoft Certificate Service] が表示されます。



4. **[Request a certificate]** をクリックしてください。次のような画面が表示されます。



5. **[advanced certificate request]** をクリックしてください。次のような画面が表示されます。



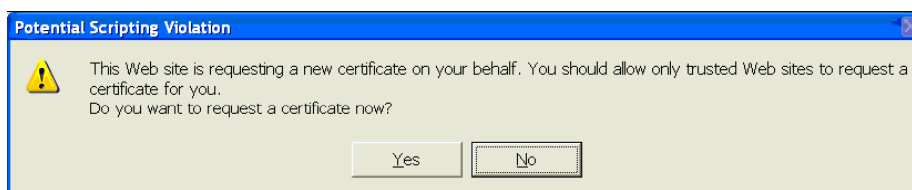
6. **[Create and submit a request to this CA]** をクリックします。次のような画面が表示されます。



7. 以下に説明するオプションを選択してください。その他のオプションについては、すべてデフォルト設定のままにしておきます。

- **[Certificate Template]** - **[Copy of Smartcard Logon]** を選択してください。
- **[CSP]** - **[Rainbow CSP]** を選択してください。
- **[Mark keys as exportable]** - このチェック・ボックスをオンにします。

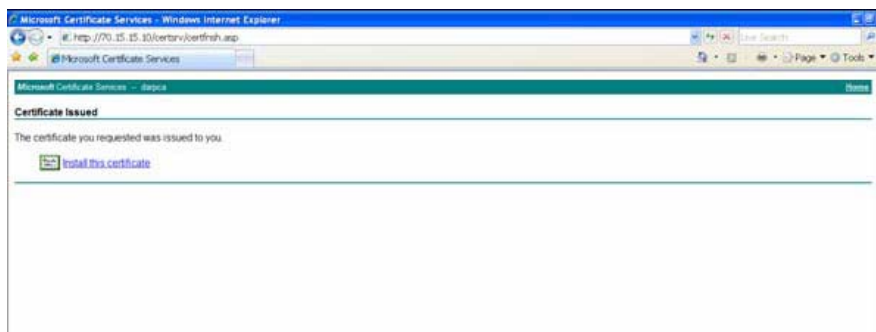
8. [送信] をクリックして続行してください。次のようなメッセージが表示されます。



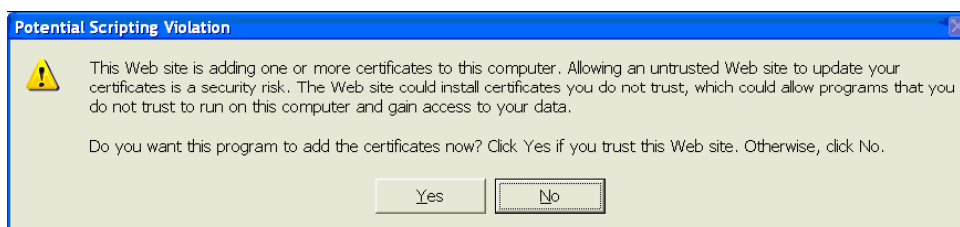
9. [はい] をクリックして続行してください。「Waiting for server response...」メッセージが表示される場合があります。この処理には数分かかります。



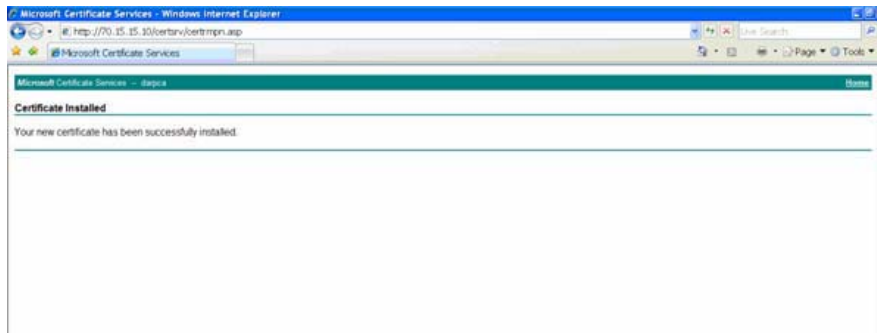
10. [Certificate Issued] 画面が表示されたら、[Install this certificate] をクリックしてください。



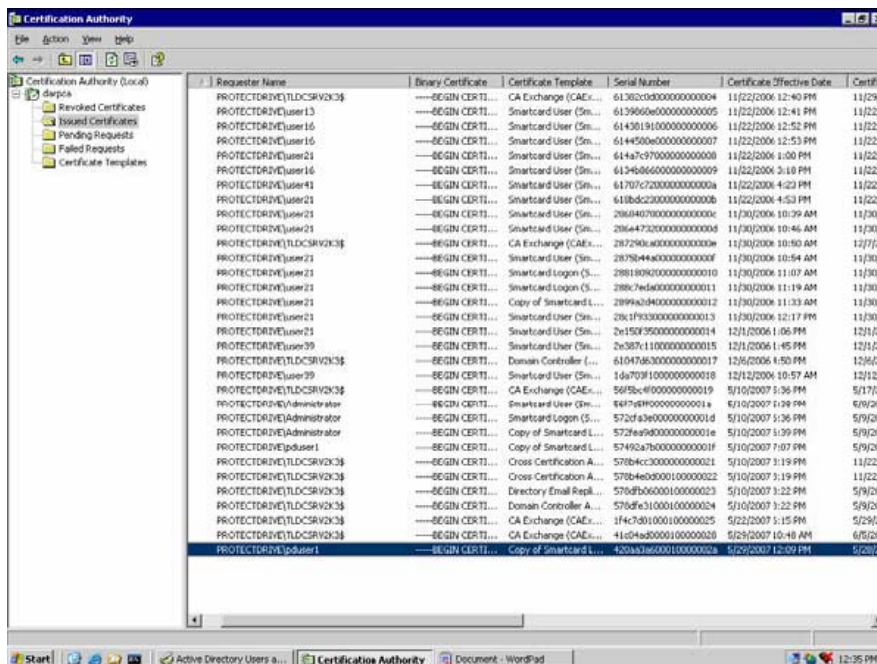
11. プロンプトが表示されたら、iKey 2032 トークンの PIN を入力します。次のような警告を受信する場合があります。



12. [はい] をクリックして続行してください。次のような画面が表示されます。

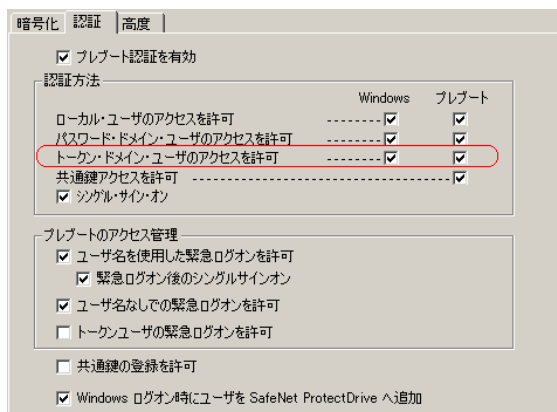


13. これで証明書をトークンとローカル・マシンのストアに登録できます。この証明書のシリアル番号に注意してください。この番号は CA の発行済み証明書の一覧と比較できます（次の例を参照してください）。



14. このユーザをログオフしてから、トークンを Windows ログオンへ再度挿入して Windows ドメインへ再ログオンしてください。
15. プロンプトが表示されたら PIN を入力してください。この証明書を使ってログオンできます。この方法でのログオンにより、ProtectDrive のユーザ・データベースでユーザが証明書ユーザとして更新されます。
16. ProtectDrive の Local Management Console を開いて、[PD ユーザ]タブをクリックして、ユーザ名と証明書の状態を確認してください。

17. リモートからの管理の場合は、Active Directory およびローカルの管理の場合には、Local Management Console の[PD 設定]タブをクリックして、[認証]をクリックし、[トークン・ドメイン・ユーザのアクセスを許可]の“Windows”と“プリブート”がそれぞれチェックされていることを確認してください。



18. パソコンを再起動してください。
19. 再起動後、ProtectDrive のプリブート認証で PIN を入力してください。下記のメッセージが表示されます。
- *Initializing token*
 - *Searching for token certificate*
 - *Deciphering user key*
 - *Deciphering disk key*
20. プリブート認証完了後に、SSO が有効であれば Windows の証明書処理でドメインに自動的にログオンします。

Copyright 2009, 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。

2009 年 2 月
