

# ProntectDrive

## バージョン 8.2.0 - リリース・ノート

---

本書では、ProntectDrive のリリースに関する情報、補足事項および現状での問題点について説明します。

### 製品の概要

ProntectDrive は、デスクトップまたはラップトップ PC を保護する SafeNet 社の暗号化ソフトウェアです。ProntectDrive は、利用中は完全に透過的に動作するため、ユーザに暗号化に関する知識は必要ありません。

ProntectDrive をインストールすると、有効なユーザ名とパスワードを入力するか、またはトークンと PIN を使用してログオンしない限り PC にアクセスできないようになります。このログオン情報の機密が保たれている限り、権限のない人物が PC にアクセスすることはできません。システムの盗難や紛失の場合でも、ハードディスクに保存された情報は暗号化されているため、セキュリティが保たれます。

### 本バージョンの情報

#### バージョン v8.2.0 での新機能

- Active Directory とセントラル管理プラットフォームとして ADAM をサポート
- 初期ポリシーの XML 構成ファイルによるサポート
- PD ユーザと PD 設定の GUI の簡略化
- RMS ネットワーク・ロック・ライセンスのサポート
- インストール時の秘密鍵をファイルまたはトークンに保存してセキュリティの向上
- リムーバブル・メディアを他のマシン上で復号化し、インストール・ファイル・セットを共用可能
- サンプル・スクリプトを利用した、Active Directory 報告書作成機能
- リムーバブル・メディアに重点を置いた、イベント・ログ拡張機能

## リリース・コンポーネント

ProtectDrive は、Windows 2000、XP、Server 2003 をサポートします。

### クライアント

ProtectDrive のクライアントは、下記のオペレーティング・システムにインストールすることが可能です。

- Microsoft Windows 2000 Professional, Service Pack 4
- Microsoft Windows 2000 Server, Service Pack 4
- Microsoft Windows Server 2003, Service Pack 1
- Microsoft Windows XP Professional, Service Pack 2 (64-bit version は未サポート)
- Microsoft Windows XP Home, Service Pack 2

ProtectDrive では、FAT16、FAT32、NTFS4 および NTFS5 ファイルシステムをサポートします。

---

**メモ：** ProtectDrive の復旧ツールでは、フロッピーもしくは CD-ROM での起動が必要になります。従って、CD-ROM や SCSI などの特別ドライバが起動時に必要な場合には、予め起動してハードディスクが読み込めることを確認してください。

---

### サーバ

ProtectDrive のクライアントを管理するための Microsoft Active Directory および ADAM への拡張スキーマのインストールは、下記のオペレーティングシステムにインストールすることが可能です。

- Microsoft Windows Server 2003, Service Pack 1

ProtectDrive のサーバ・パッケージ（拡張スキーマ）をインストールするために、ライセンスは必要ありません。

## 主なサポート内容

- Active Directory または ADAM (Active Directory Application Mode) を使用することにより、完全な集中管理の元で ProtectDrive クライアント・インストールを Windows 2003 サーバ経由で行なえます。ADAM は Active Directory スキーマの拡張の必要がありません。ADAM は（ドメイン・コントローラーでない）Windows 2003 サーバ・マシン上で構成するだけです。ProtectDrive はドメイン・フォレストの一部をなす、単一ドメインでサポートされます。
- 設定を XML ファイルで保存することが可能です。このファイルは必要に応じてカスタマイズされたローカル・インストールからエクスポートすることができます。このファイルは、AD や ADAM を使用しない小規模デプロイメントに最適です。
- ローカル管理コンソール上の **PD 設定** にある **[高度]** タブは、ツリー構造によって設定の表示や管理を行なうことができます。
- ローカル管理コンソールの **更新状況** および **暗号化状況** タブは、ローカル管理コンソールでは 1 つのタブで、すべての状況情報が表示可能です。
- ローカル管理コンソールの **[PD ユーザー]** タブは、追加、削除、設定の 3 つのタブで構成されます。
- 進行状況表示バーが、リムーバブル・メディアを暗号化したり復号化したりする際に表示されます。

- ユーザが証明書を発行すると、そのユーザが ProtectDrive データベースに追加された時に証明書も自動的に追加されます。
- **RMS** ネットワーク・ロック・ライセンスでのライセンス機能が提供されました。ローカル管理コンソールの [ **ライセンス管理** ] の表示画面は、販売店からの認証コードおよびファイルを取得するためのロック・コードを表示するように変更されました。**RMS** ライセンス生成サーバは、新規のライセンスを生成し、それが正しければ自動的にインストールします。
- 前回バージョン同様、ProtectDrive は評価のための 30 日間の試用期間が適用されます。
- 鍵管理が改善されました。syskey.cid は マスター・セキュリティ (Master Security : MS) 証明書と リカバリ・サポート (Recovery Support:RS) 証明書、RM Salt に置き換えられました。MS および RS に関連する秘密鍵は、.pfx ファイルまたはトークンに保管し、さらに機密性を保つことができます。
- Active Directory レポート作成機能が追加されました。容易にインプリメンテーションできるよう、サンプル・スクリプトがインストール・ファイルと共に提供されます。このスクリプトは、ProtectDrive がインストールされているかどうかといったような簡単なレポートを生成します。ProtectDrive がインストールされたマシンについては、暗号化に関する統計も表示します。
- プレブートの ROM サイズ制限やこのリリースで追加された読取装置の数のため、ユーザはインストール時に 2 組の読取装置を選択することができます。インストール時に、MSI 属性 (ERA\_VROM\_READERS\_SET) を使用して、その読取装置の組み合わせをデフォルトに事前設定することもできます。この属性の有効な値は、PCMCIA または INTERNAL です。
- ProtectDrive バージョン 7.2.3 および 8.1.1 からのアップグレードのみがサポートされます。
- Dell D600 上の DataKey 330 Card のサポートが追加されました。
- CAC カード対応のマシン、読取装置が幅広くサポートされています。
- ログ取得機能が拡張されました。失敗した シングル・サイン・オン同様に、試行された認証 (成功もしくは失敗) なども記録されるようになりました。
- ローカルおよびリモートの設定は、ローカル管理コンソールでは、切り替えできません。
- マルチ PD ユーザーに対する速度が改善しました。
- SafeNet iKey 1000 でのプレブート認証では、シングル・サイン・オンは利用できません。
- SafeNet iKey 1000 のサポートは、PKI を使用せずに共有鍵のみで可能です。
- リモートでのワнтаイム・パスワード発行による復旧およびディスクの復号化ツールをサポートしています。
- ProtectDrive のユーザ・データベースの登録ユーザ数が、200 (v8.1.1) から、2,000 に変更になりました。これにより、Active Directory および ADAM のユーザの登録機能が拡張されています。

## 注意事項

### ウイルス対策ソフトとの共存に関して

- ウイルス対策ソフトウェアが原因で、ProtectDrive のインストールに失敗する場合があります。これは、ウイルス対策ソフトウェアが、ProtectDrive のシステムフォルダー `C:\SECURDSK` へのアクセスを不正なアクセスとして認識するためです。ProtectDrive のインストール中は、ウイルス対策ソフトウェアを停止してください。

### レガシー USB サポートのパソコンへの対応

- パソコンがレガシー USB をサポートしている場合に、USB 接続のスマートカードもしくは認証トークンのプレブート認証が失敗することがあります。BIOS の設定で、レガシー USB の設定を OFF にしてください。

### 本リリースでのアップグレードでの注意事項

ProtectDrive v8.2 では、ProtectDrive v7.2.3、v8.1.1（v7.3 を除く）からのアップグレードをサポートしています。既に暗号化されたハードディスクなども復号化することなくアップグレードを実行することが可能となっています。

- ProtectDrive v8.2 では、v7.2.3 のシステム・エリア（領域）のみの暗号化は対応していません。したがって、システム・エリアのみの暗号化を行っている場合のアップグレードでは、一旦システム・エリアの復号化を実行して、v8.2 のインストールを実行してください。
- ProtectDrive Enterprise Version v8.2 では、v7.2.3 の独自のネットワーク・インストールではなく、Active Directory のグループ ポリシー オブジェクトからのリモート・インストールが実行可能となっています。詳細は、ProtectDrive v8.2 の『管理者ガイド』マニュアルをご確認ください。

### 評価ライセンスに関して

- 評価ライセンスの情報の表示で、“ライセンス開始日”が `Mon Jan 01 00:00:00 2007` と表示されますが、これはインストールした日時ではなく、ライセンスが発行された日時となります。したがって、30 日の評価期間は、インストールした日時を必ず記録して、管理してください。

### シングル・サイン・オンの利用に関して

シングル・サイン・オンが動作しない理由としては、他製品の GINA が動作している可能性があります。もし、他社製の GINA を使用する場合には、ProtectDrive を先にインストールすることで対応可能です。また、ProtectDrive の GINA を調整することも可能です。

Windows のレジストリの知識が十分で、他社製の GINA の情報が明確であれば、GINA の設定を行うことが可能です。

---

**メモ：** ただし、レジストリを破壊したりすると Windows が起動しないこともあります。このような場合には、セーフモードで Windows を起動してください。レジストリを変更する場合には、必ずバックアップを行ってください。

---

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL を確認してください。GinaDLL の値は、`pcvgina.dll` であるべきです（ProtectDrive GINA）。指定されている値のファイルが、正しい場所に存在するか確認してください。

2. HKEY\_LOCAL\_MACHINE\SOFTWARE\Eracom Technologies Australia Pty. Ltd.\ProtectDrive を確認してください。もし、他社製の GINA をインストールしていないのであれば、ChainedGinag が存在しません。もし、他社製の GINA がインストールされているのであれば、ChainedGinag にそのパスを正しく設定してください。

**メモ：** なお、HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL のキーを削除すれば、Microsoft Windows の標準 GINA が起動されます。

## トークンのサポートに関して

ProtectDrive では、プレブート認証で二要素認証を可能とするスマートカードや USB 認証トークンでの認証をサポートしています。以下に ProtectDrive v8.2 でサポートされているそれぞれのトークンを記載します。

なお、ProtectDrive では、CCID 互換のスマートカード・リーダーがサポートされていますが、下記に記述されている USB および PCMCIA 接続のスマートカード・リーダーは、弊社で検証したものです。

### USB

- DataKey DKR 630 - GemPC430
- DataKey DKR 631 - GemPC USB
- DataKey DKR731 - OmniKey CardMan 3121
- DataKey DKR830 - SCR 331
- Precise 100MC Bio Keyboard (プレブート認証での指紋認証は未サポート)

### PCMCIA

- Datakey DKR 600 - GemPC400
- Datakey DKR 701 - CM 4040
- GemPlus - GPR 400

## サポートしているスマートカードと USB トークンの一覧

製品	必要なソフトウェア
Aladdin eToken	<b>Cryptographic Provider</b> : RTE 3.60 eToken Pro 16k、32k、64k および NG-OTP のサポート 1024 ビット RSA キーのサポート
Aladdin Smart card	<b>Cryptographic Provider</b> : RTE 3.60 2048 ビット RSA キーのサポート (リーダに依存)
Axalto Access 64k および 64k v2	<b>SafeNet CIP Utilities</b> : Borderless Security PK 6.1.2 B4 以降
Gemplus GXP3 64v2n	<b>SafeNet CIP Utilities</b> : Borderless Security PK 6.1.2 B4 以降
Nexus	<b>Nexus Personal CSP</b>
Oberthur Cosmopolle v4	<b>SafeNet CIP Utilities</b> : Borderless Security PK 6.1.2 B4 以降

製品	必要なソフトウェア
Oberthur Cosmo64 v5.2d.	<b>SafeNet CIP Utilities</b> : Borderless Security PK 6.1.2 B4 以降
Oberthur ID one v5.2	<b>SafeNet CIP Utilities</b> : Borderless Security PK 6.1.2 B4 以降
RSA SecurId 5100	<b>RSA Authenticator Utility</b> : Revision 1.0 (Build 25) 1024 ビット RSA キーのサポート
SafeNet Borderless Security Smart Card 330	<b>SafeNet CIP Utilities</b> : Borderless Security PK 6.1.0 以降 CSP: dkrsacsp.dll: 4.7.20.3010 1024、2048 ビット RSA キーのサポート
SafeNet Borderless Security iKey 2032	<b>SafeNet CIP Utilities</b> : Borderless Security PK 6.1.0 以降 CSP: dkrsacsp.dll: 4.7.20.3010 1024、2048 ビット RSA キーのサポート
SafeNet Borderless Security iKey 1000、iKey 1032	認証には必要なし。 別途 PIN の変更には、iKey 1000 SDK v2.2.3 以降が必要
Schlumberger Access 32k v2	<b>SafeNet CIP Utilities</b> : Borderless Security PK 6.1.2 B4 以降
Siemens CardOS v4.3b	<b>Siemens AG</b> : HiPath Scurity Card API V3.0 B

## リムーバブル・メディアのサポート

下記に ProtectDrive v8.2 をインストールして、弊社で暗号化および復号化の検証を行ったリムーバブル・メディアを記載します。特殊な MBR、パーティションおよび他社製品で暗号化されたメディアは、ProtectDrive では利用することはできません。

また、ProtectDrive v8.2 では、USB v1.0 および USB v2.0 のリムーバブル装置と USB ハードディスクをサポートしています。弊社で暗号化および復号化の検証を行ったものも以下に記載します。

### 検証済の USB リムーバブル装置

- Crucial Gizmo 256MB
- Crucial Gizmo Overdrive 512MB (ソフトウェアなし)
- Edge DiscGO 128MB
- Imation Clip Flask Drive1GB
- Imation Flash Wristband 256MB
- Iomega Micro Mini 512MB
- Kingston DataTraveler mini fun 256MB
- Kingston DataTraveler 256MB
- Kingston U3 DataTraveler 1GB (U3 パスワード認証なし)
- Lexar Jump Drive Elite 128MB
- Lexar Jump Drive Secure 1GB
- Memorex TravelDrive 256MB
- PNY Attache 128MB

- PNY Attache 512MB
- SafeNet 32MB
- SanDisk Cruzer Freedom 256MB
- SanDisk Cruzer Micro U3 1GB (U3 パスワード認証なし)
- SimpleTech Bonzai Xpress 128MB
- Sony MicroVault 512MB
- Sony MicroVault BioMetric 512MB
- Sony POCKETBIT USM 128MB (指紋認証なし)
- Sony POCKETBIT USM-J 128MB, 256MB, 512MB, 1GB, 2GB, 4GB, 8GB
- Verbatim Store 'n' Go 128MB
- Viking 256MB
- Viking Interworks 1GB
- Generic 2.0 USB hard drives

## パソコンのサポート

下記に ProtectDrive v8.2 をインストールして、弊社で暗号化および復号化の検証を行ったパソコンを記載します。

また、ProtectDrive v8.2 では、Microsoft 社より認定されている Windows 2000 および XP が動作するパソコンをサポートしています。

### 動作検証内容

1. パソコンの標準オペレーティングシステムのインストール (付属の CD を利用)
2. Microsoft Windows の CHKDISK の実行
3. ProtectDrive v8.2 のインストール
4. C: ドライブの暗号化 (AES 256)
5. 再起動後、Microsoft Windows の CHKDISK および DEFLAG の実行
6. 再起動後、iKey 1000 用の共通鍵発行および再起動してプレブート認証の検証
7. C: ドライブの復号化
8. 再起動後、ProtectDrive のアンインストール
9. 正常に再起動することを確認

### 検証済のパソコン

下記の検証は、日本語環境での検証機器となります。

- 富士通 FMV-C8200 (FMVNC1DC23)
- 東芝 SatelliteJ40 (PSJ401HL5SR1K)
- 東芝 SatelliteJ50 (PSJ501JL5SR1K)

- 東芝 SatelliteJ60 (PSJ6020DXSRGKW)
- 東芝 SatelliteT20 (PST201MC5N71K)
- 東芝 PORTEGE 2010 (PP201Z-00GPP)
- 東芝 SS 2110 (PP21110L2HGP)

---

**メモ：** 東芝 SS2110 の付属の CD でインストールした場合には、必ず Windows Installer v3.1 を Windows update からインストールしてください。

---

- 東芝 SS S30 (PPS301CSPS6UK)
- 東芝 SS S21 (PPS2112L2J64K)
- 東芝 SS M35 (PPM351RDPSSTK)
- NEC VersaProNX (PC-VY16MEFE1EHX)
- NEC VersaProR (PC-VY17FRFEJEHU)

---

**メモ：** 上記の NEC VersaProNX および VersaProR では、プレブート認証に iKey 1000 は利用できません。これは、BIOS レベルで iKey 1000 を認識できないためです。

---

- NEC VersaProNX (PC-VY21AWZE1)
- NEC VersaProNX (PC-VY22FAGEX)
- NEC VersaProNX (PC-VY17FLVEHWLR)
- NEC VersaProNX (PC-VY17FLVEX)
- NEC VersaProNX (PC-VY12FBHEX)
- 松下電器 Let'sNoteProY2 (CF-Y2FW7AXS)
- 松下電器 Let'sNoteProY4 (CF-Y4JW8AXS)
- 松下電器 Let'sNoteProY5 (CF-Y5LW4AXS)
- 松下電器 Let'sNoteProT5 (CF-T5KW9AXS)
- 松下電器 Let'sNoteProT2 (CF-T2FW1AXS)
- IBM ThinkPad X23 (TYPE 2662)
- IBM ThinkPad X40 (TYPE 2371)
- IBM ThinkPad T60 (TYPE 2007)

## 本リリースでの既知の問題点

- プレブート認証 (PBA) のユーザ名、パスワードおよびドメイン名には、日本語は使用できません。Windows での設定で必ず半角英数字で設定してください。
- ProtectDrive のインストールは、必ず C: ドライブにインストールしてください。  
初期インストールのイメージを別ディスクで保持するパソコンでは、インストール前に確認してください。
- アップグレード・インストールで、“USB もしくは内部リーダ”を選択した場合に、それ以外の読取装置が指定できない。( #31863)

### 「回避策」

ProtectDrive のアップグレード・インストールが完了し、USB もしくは内部リーダの選択を要求された場合 (USB もしくは PCMCIA リーダを選択する以外) は、必ずインストーラの MSI をマイクロソフト ORCA ツールなどで、“ERA\_VROM\_READERS\_SET” の値を “INTERNAL” に変更してください。標準では、空白が設定されています。

- ORCA ツールを使用して MSI インストール中にアクセスした、以下の ProtectDrive インストール変数が作動しない。( #31457)

ERA\_AUTH\_PATH\_OR\_CODE, ERA\_LICENSE\_PATH\_OR\_CODE  
ERA\_KM\_REC\_FILE\_FOLDER\_PATH

### 「回避策」

これらの変数を追加したり修正せず、デフォルト・ロケーション (インストール・ディレクトリ) を使用してください。

- ユーザー名なしの緊急時ログオンが、アップグレード後作動しない。( #31416)

### 「回避策」

アップグレード後、オリジナル (アップグレード前のバージョン) のインストール・ファイルと syskey.bin ファイルを保存してください。オリジナルの rpadmin.exe と syskey.bin ファイルを使用して、ユーザー名なしで緊急時ログインすることができます。

- xml 設定ファイルでインストールすると、緊急ログオン設定が作動しない。( #30863)

### 「回避策」

緊急ログオン設定のどれかを変更し、再びそれをもとに戻し適用 をクリックしてください。

- 大量ユーザーを持つユーザー・グループの追加は、Active Directory とリモート・クライアントの両方で問題を引き起こす可能性がある。( #30697)

### 「回避策」

各グループは、最高 100 ユーザーまでにしてください。

- Active Directory 上の PD サーバーまたはドメイン・フォレストにある ADAM サーバに関連する問題。( #30663, #30697, #30705, #30746)

### 「回避策」

PD サーバを単一ドメイン内の Active Directory または ADAM サーバにインストールしてください。

- PD サーバの管理 のインターバル時間を 1.5 時間に設定すると、2730 日になる。( #29739)

### 「回避策」

インターバルの設定は整数値のみにしてください。

- Windows 2000 のトークンでの SSO 後、スマート・カードまたは eToken を取り外す際、ワークステーションがロックされない。(#29660)

「回避策」

手動 (Ctrl+Alt+Del) でロックしてください。

- DKR731 リーダーは、2048 bit cert を持つ Siemens 製カードで PBA の復号化に失敗する。(#29340)

「回避策」

その他の読取装置、カード、またはより小さなサイズの証明書を使用してください。

- 画面上に PD ログオン情報画面が表示された時に Ctrl+Alt+Del を押すとログオフしてしまう。(#29089)

「回避策」

PD 情報画面が表示されたら、Ctrl+Alt+Del を押す前に、OK をクリックしてください。

- ProtectDrive の SSO では、Novell GINA でのログオンは未サポートです。
- Windows XP 64bit および Windows Vista は、未サポートです。(#5478)  
Windows Vista は、次期バージョンでサポート予定です。
- Entrust 3 Key Pair Token は、PBA をサポートしていません。(#5895)
- Windows XP GPO インストールで、ProtectDrive を正しくインストールするため、2 回リブートすることを要求される。間違ったドメインを選択すると、PBA ログオンが失敗することがある。

「回避策」

PBA プロンプトでドメイン選択をタブし、UP/DOWN キーを使って正しく選択してください。

- SafeNet Borderless Security Token Service は、Wave System の認証システムをサポートしていません。PIN の入力ができなくなります。

「回避策」

パスワードでの認証を利用してください。

- スマートカードまたはトークンが PBA で使用されると、シングル・サイン・オンは、Windows Server 2003 システムでは稼働しない。(#25402)
- Norton Ghost バージョン 10.0 が稼働するシステム上の ProtectDrive のリムーバブル・メディアの問題。リムーバブル・メディアの暗号化またはアンロックに関する ProtectDrive プロンプトが表示されない。(#25654)
- ユーザ削除時に、[PD ユーザ] タブにある、ユーザおよび認証の数が更新されない。(#25657)

「回避策」

ローカル管理コンソールを閉じて、再起動してください。

- Orca での SafeNet ProtectDrive.msi を変更し、オリジナルと違うホルダーに保存した場合に、Active Directory のグループ ポリシー オブジェクトからリモートインストールを行うとエラーとなります。(#25688)

「回避策」

この問題は、オリジナルとはことなるフォルダーに保存した場合に発生する Orca の問題であり、一旦別名で同じフォルダーに保存して、Windows のコピーコマンドで他のフォルダーにコピーしてください。

- ・ "暗号化プロンプト" メッセージが表示され、ProtectDrive なしでリムーバブル・メディアにアクセスしようとする、"アクセス拒否" のメッセージが表示される。[ 非暗号化メディアへのアクセス拒否 ] 設定が選択されていないければ、リムーバブル・メディアへはアクセスできます。(#25297)

#### 「回避策」

リムーバブル・取り外し可能メディアへアクセスする前に "暗号化プロンプト" 画面で、暗号化しない オプションを選択してください。

- ・ [ 非暗号化メディアへのアクセス拒否 ] オプションが選択されていない場合、保護されていないメディアに対するアクセスが拒否される。(#25223)

#### 「回避策 1」

間違ったメッセージ "アクセスが拒否されました" が表示されたら、マイ コンピュータ上のリムーバブル・メディアを右クリックし、メディアの暗号化を選択してください。その後、暗号化しないを再び、"暗号化プロンプト" 画面で選択してください。取り外し可能メディアはアクセス可能になります。

#### 「回避策 2」

[ クライアント設定のみ ] モードであれば、設定を強制更新 (例えば、ロックアウト試行設定) に変更します。[ リモート設定のみ ] モードでこのステップを繰り返し (例えば、インターバルやログオン/ログオフ設定の変更)、更新されることを確認します。設定が更新されたら、(リムーバブル・メディア装置を取り外されていなければいったん取り外して) リムーバブル・メディア 装置を再度挿入します。構成された設定は再び使用中になります。

- ・ ProtectDrive で暗号化された拡張ディスクでのブートはできません。
- ・ Bluetooth接続のUSBおよびレガシータイプのUSBをサポートするパソコンでは、トークンによるプレブート認証時にパソコンがハングアップします。

#### 「回避策」

BIOS の設定で、Bluetooth 接続の USB もしくは、レガシータイプの USB の設定を無効に設定してください。

- ・ プレブート認証でのスマートカードおよび USB 認証トークンの PIN の最大試行回数およびロックアウトに関して。  
現状のプレブート認証でのスマートカードおよび USB 認証トークンの PIN 入力でのロックアウトおよび PIN 入力の最大試行回数は、ProtectDrive で設定するのではなく、それぞれのスマートカードおよび USB 認証トークンの機能に依存します。
- ・ シリアル ATA のパソコンでハイバネーション後にパソコンがブルースクリーン (BSOD) となることがあります。

#### 「回避策」

シリアル ATA のモードを AHCI モードに変更してください。

- ・ リムーバブル・メディアで不正なパーティションテーブル (カスタマイズされた) や他社の暗号化ソフトのための MBR など保持するものは、ProtectDrive では暗号化できません。ProtectDrive は、MBR を持たないメディアに対応しています。このようなデバイスに対しては、エラーメッセージを表示して、暗号化は行われません。
- ・ リモート管理の場合に、クライアントの ProtectDrive のトレイアイコンから、共通鍵の設定が可能となります。

#### 「回避策」

Active Directory の [PD 設定] で、必ずトレイアイコンの表示をオフにしてください。

## お問い合わせ先

本製品に関して、ご質問は下記までお問い合わせください。

### 日本（製品のお問い合わせ先）

インターネット <http://jp.safenet-inc.com>  
E メール [jp-sales@safenet-inc.com](mailto:jp-sales@safenet-inc.com)  
電話 (045) 640-5733

### アメリカ（本社）

インターネット <http://www.safenet-inc.com/>

© Copyright 2007, 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。

2007 年 9 月