



デスクトップ マネジメントについて

HP Business Desktop dx5150モデル

製品番号 : 375370-292

2005年 2月

このガイドでは、一部のモデルにプリインストールされているセキュリティ機能とインテリジェント マネジメント機能の概念および使用手順について説明します。

© Copyright 2004 Hewlett-Packard Development Company, L.P.

本書の内容は、将来予告なしに変更されることがあります。

MicrosoftおよびWindowsは、米国Microsoft Corporationの米国およびその他の国における登録商標です。

その他、本書に掲載されている会社名、製品名はそれぞれ各社の商標または登録商標です。

HP製品およびサービスに対する保証は、当該製品およびサービスに付属の保証規定に明示的に記載されているものに限られます。本書のいかなる内容も、当該保証に新たに保証を追加するものではありません。本書の内容につきましては万全を期しておりますが、本書の技術的あるいは校正上の誤り、省略に対しては、責任を負いかねますのでご了承ください。

本書には、著作権によって保護された所有権に関する情報が掲載されています。本書のいかなる部分も、Hewlett-Packard Companyの書面による承諾なしに複写、複製、あるいは他言語へ翻訳することはできません。

本製品は、日本国内で使用するための仕様になっており、日本国外で使用される場合は、仕様の変更を必要とすることがあります。

本書に記載されている製品情報は、日本国内で販売されていないものも含まれている場合があります。

以下の記号は、本文中で安全上重要な注意事項を示します。



警告：その指示に従わないと、人体への傷害や生命の危険を引き起こす恐れがあるという警告事項を表します。



注意：その指示に従わないと、装置の損傷やデータの損失を引き起こす恐れがあるという注意事項を表します。

デスクトップ マネジメントについて

HP Business Desktop dx5150モデル

初版 2004年12月

改訂第1版 2005年 2月

製品番号：375370-292

日本ヒューレット・パッカード株式会社

目次

出荷時設定の変更	2
リモート システム インストール	3
ソフトウェアのアップデートと管理	3
HP Client Manager Software	4
Altiris Client Management Solutions	4
System Software Manager	6
Proactive Change Notification	6
Subscriber's Choice	7
ROMフラッシュ機能	7
リモートROMフラッシュ機能	8
HPQFlash	8
ブートブロックROM	8
リプリケート セットアップ機能	10
起動可能デバイスの作成	10
デュアル ステート電源ボタンの設定	15
インターネットWebサイト	16
標準規格およびパートナー企業	17
資産情報管理機能およびセキュリティ機能	17
パスワードのセキュリティ	20
スーパーバイザ パスワードの設定	20
ユーザ パスワードの設定	21
ユーザ パスワードの入力	22
スーパーバイザ パスワードの入力	22
ユーザ パスワードまたはスーパーバイザ パスワードの変更	23
ユーザ パスワードを忘れてしまった場合	24
マスタ ブート レコード セキュリティ (Master Boot Record Security)	24
現在の起動可能ディスクのパーティションとフォーマットを変更する前に	27
ケーブルロックの取り付け	28
障害通知および復旧機能	28
耐サージ機能付連続供給電源装置	28
温度センサ機能	28

デスクトップ マネジメント

HPのインテリジェント マネジメント機能は、ネットワーク環境にあるデスクトップ、ワークステーション、およびノートブック コンピュータの管理と制御の分野で、標準のソリューションを提供しています。HPはデスクトップ マネジメントのパイオニアとして1995年に、デスクトップを完全に管理できる業界初のパーソナル コンピュータを世に送り出しました。HPはマネジメント機能の特許を取得しています。以来、デスクトップ、ワークステーション、およびノートブック コンピュータの効果的な導入、設定、および管理に必要な標準化とインフラストラクチャの開発において業界全体の取り組みをリードしてきました。HPは、業界トップクラスの管理ソフトウェア ソリューション提供企業との提携関係により、これらの企業の製品とインテリジェント マネジメント機能の互換性を確保しています。インテリジェント マネジメント機能は、ライフサイクル ソリューションを提供する幅広い取り組みの中でも重要な位置を占めるもので、デスクトップ コンピュータのライフサイクルの4つの側面である計画、導入、管理、移行でユーザをサポートします。

デスクトップ マネジメントの主要な機能と特長は、次のとおりです。

- 出荷時設定の変更
- リモート システム インストール
- ソフトウェア アップデートおよびマネジメント機能
- ROMフラッシュ
- 資産情報管理機能およびセキュリティ機能
- 障害通知および復旧機能

出荷時設定の変更

お使いのコンピュータには、システム ソフトウェア イメージがプリインストールされています。ソフトウェアの設定手順を簡単に済ませると、すぐにコンピュータを使用できます。

プリインストールされたソフトウェア イメージの代わりにカスタマイズされたシステム ソフトウェアおよびアプリケーション ソフトウェアを使うこともできます。カスタマイズされたソフトウェア イメージを展開するには、いくつかの方法があります。

- プリインストールされたソフトウェア イメージを展開した後、追加するアプリケーションをインストールする
- Altiris Deployment Solutionsなどのソフトウェアの導入用ツールを使用して、プリインストール ソフトウェアの代わりにカスタマイズされたソフトウェア イメージを使用する
- ディスク複製手順を使用して、ハードディスク ドライブの内容を別のハードディスクにコピーする

最適なコンピュータ環境の構築方法は、お使いの情報技術環境や作業内容によって異なります。HP ライフサイクル ソリューションに関する弊社のホームページ (<http://whp-sp-orig.extweb.hp.com/country/us/en/solutions.html>、英語サイト) には、お使いの環境に適したコンピュータの導入方法を選択する際に役立つ情報が掲載されています。

Restore Plus! CD、ROMからのセットアップ、およびACPIハードウェアにより、システム ソフトウェアのリストア、コンフィギュレーション マネジメント機能、トラブルシューティング、および省電力機能を利用することができます。

リモート システム インストール

Preboot Execution Environment (PXE) を起動すれば、リモート システム インストールを使用してネットワーク サーバからソフトウェアやコンフィギュレーション情報（コンピュータの設定情報）を取り出して、コンピュータをセットアップすることができます。リモート システム インストールの機能は、通常、システム セットアップやコンフィギュレーションのためのツールとして使用しますが、次のような場合にも使用できます。

- ハードディスク ドライブをフォーマットするとき
- 1台以上の新しいコンピュータにソフトウェア イメージを導入するとき
- フラッシュ ROMを使用してシステムBIOSをリモートでアップデートするとき（8ページの「[リモートROMフラッシュ機能](#)」を参照）
- システムBIOSを設定するとき

リモート システム インストールを起動するには、起動時に表示されるHPロゴの画面の右下隅に[F12 = Network Service Boot]と表示されたら、すぐに[F12]キーを押します。画面のメッセージに従って、リモート システム インストールを起動します。デフォルトの起動順序はBIOSのコンフィギュレーションの設定ですが、常にPXEを起動するように変更できます。

HPとAltiris社の提携により、企業におけるコンピュータの導入と管理を短時間で容易に実行できるツールが開発されました。このツールを使用すると、TCO（維持管理費）が大幅に削減されます。HPのコンピュータが、企業環境内で最も管理しやすいクライアント マシンになります。

ソフトウェアのアップデートと管理

HPでは、デスクトップ コンピュータおよびワークステーションのソフトウェアを管理し、アップデートするためのツール（HP Client Manager Software、Altiris Client Management Solutions、System Software Manager、Proactive Change Notification（製品変更通知）、およびSubscriber's Choice）を提供しています。

HP Client Manager Software

HP Client Manager Software (HP CMS) は、以下の機能により、クライアントコンピュータのハードウェアの管理に役立ちます。

- 資産管理用のハードウェア インベントリの詳細表示
- コンピュータの状態検査の監視および診断
- ハードウェア環境の変化についての事前通知
- マシン温度についての警告、メモリ異常の警告など、企業活動における重大な状況についての、Webサイトを利用した報告
- システム ソフトウェア (デバイス ドライバやROM BIOSなど) のリモートアップデート
- 起動順序のリモートからの変更
- システムBIOSの設定

HP Client Managerについて詳しくは、<http://www.hp.com/go/im> (英語サイト) を参照してください。

Altiris Client Management Solutions

HPはAltiris社と提携して、HPクライアントPCの所有によるコストを削減する、強力的に統合された包括的なシステム管理ソリューションを提供しています。Altiris Client Management Solutionsは、HP Client Manager Softwareを基礎としており、次の機能があります。

- 資産管理
 - ソフトウェア ライセンスの準拠
 - コンピュータの管理および報告
 - リース契約および固定資産の管理
- 展開と移行
 - Microsoft® Windows® XP ProfessionalまたはHome Editionへの移行
 - システムの展開
 - 個人設定の移行

- ヘルプデスクと問題解決
 - ヘルプデスク チケットの管理
 - リモートでのトラブルシューティング
 - リモートでの問題解決
- ソフトウェアおよび操作の管理
 - デスクトップ マネジメントの実行
 - HPシステム ソフトウェアの展開
 - アプリケーションの自己修復

Altiris Solutionsの詳細情報および30日間試用版のダウンロード方法については、<http://h18000.www1.hp.com/im/prodinfo.html#deploy>（英語サイト）を参照してください。

一部のデスクトップおよびノートブック コンピュータには、工場出荷時にロードされたイメージの1つとしてAltiris マネジメント エージェントが含まれています。このエージェントによりAltiris Development Solutionsとの通信が可能になります。Altiris Development Solutionsを使用すると、簡単なウィザードに従って、新しいハードウェアの展開や新しいオペレーティング システムへの個人設定の移行を完了することができます。Altiris Solutions ソフトウェアには、使いやすいソフトウェア配布機能も含まれています。System Software ManagerまたはHP Client Manager Softwareと組み合わせて使用すると、管理者はROM BIOSとデバイス ドライバのソフトウェアを中央管理コンソールからアップデートすることもできます。

詳しくは、HPのWebサイト、<http://www.hp.com/go/EasyDeploy>（英語サイト）を参照してください。

System Software Manager

System Software Manager (SSM) は、複数のシステムにおいてシステム レベルのソフトウェアを同時にアップデートできるユーティリティです。SSMは、コンピュータのクライアントシステムで使用すると、ハードウェアおよびソフトウェアのバージョンを検出し、ファイル格納ディレクトリと呼ばれる中央のリポジトリから適切なソフトウェアをアップデートします。SSMでサポートされるドライバのバージョンは、ソフトウェアおよびドライバのダウンロードサイトおよびサポート ソフトウェアCDに、独自のアイコンで示されています。ユーティリティのダウンロードまたはSSMについて詳しくは、<http://www.hp.com/go/ssm> (英語サイト) を参照してください。

Proactive Change Notification

Proactive Change Notificationプログラムは、Subscriber's ChoiceのWebサイトを利用して、以下のことを事前にかつ自動的に行います。

- ほとんどの企業向けHP製コンピュータおよびサーバでハードウェアおよびソフトウェアの変更があった場合に、最も早く60日前に電子メールでProactive Change Notification (PCN) を通知する
- ほとんどの企業向けHP製コンピュータおよびサーバについてのCustomer Bulletins、Customer Advisories、Customer Notes、Security Bulletins、およびDriver alertsを含んだ電子メールを送信する

特定のIT環境に該当する情報のみを受け取るようにするため、ユーザ専用のプロファイルを作成します。Proactive Change Notificationプログラムの詳細およびカスタム プロファイルの作成方法については、<http://www.hp.com/go/pcn> (英語サイト) を参照してください。

Subscriber's Choice

Subscriber's ChoiceはHPのクライアントベースのサービスです。ユーザのプロファイルを基に、製品の使用のヒント、特集記事、およびドライバやサポートに関する警告や通知を提供します。Subscriber's Choice Driver and Support Alerts/Notificationsでは、購読するようプロファイルに設定した情報が閲覧および入手可能になると、電子メールで通知します。Subscriber's Choiceの詳細およびカスタム プロファイルの作成については、<http://www.hp.com/go/pcn> (英語サイト) を参照してください。

ROMフラッシュ機能

お使いのコンピュータでは、オペレーティング システムとの情報のやりとりなどを行う基本入出力システム (BIOS) がプログラム可能なフラッシュROMに記憶されているので、必要に応じて簡単にアップグレードすることができます。ROMのアップグレードにはRomPaqディスクが必要です。RomPaqディスクは、インターネットのHPホームページからダウンロードできます。ROMのアップグレード手順については、RomPaqディスクに付属の説明を参照してください。



注意: コンピュータにスーパーバイザ パスワードを設定しておけば、システムROMの内容が不用意に変更されるのを防ぐことができます。コンピュータにスーパーバイザ パスワードが設定されていないと、ROMへの書き込みが禁止されていないので、不用意にROMの内容が変更されてしまう危険があります。

システムROMのバージョンがお使いのコンピュータのモデルやオペレーティング システムに合っていないと、コンピュータが正しく動作しないことがあります。

System Software Managerを使用すると、システム管理者が、複数のコンピュータに同時にスーパーバイザ パスワードを設定することができます。

詳しくは、<http://www.hp.com/go/ssm> (英語サイト) を参照してください。

リモートROMフラッシュ機能

リモートROMフラッシュ機能を利用すれば、システム管理者は、ネットワーク管理端末からリモートでコンピュータのROMを安全に書き換えることができます。複数のHPのコンピュータに対してこのような作業をリモートで行うことができるので、ネットワーク上のコンピュータのROMを適切にアップグレードし、少ない費用で管理することができます。



リモートROMフラッシュを使用するには、リモート ウェイク アップ機能を使って、お使いのコンピュータの電源を入れておくか、再起動しておく必要があります。

リモートROMフラッシュについて詳しくは、<http://h18000.www1.hp.com/im/prodinfo.html> (英語サイト) でHP Client Manager SoftwareまたはSystem Software Managerについての説明を参照してください。

HPQFlash

HPQFlashユーティリティは、Windowsオペレーティング システムで個別のコンピュータ上でシステムROMのアップデートや復元を行う場合に使用します。

HPQFlashについて詳しくは、<http://www.hp.com/support/files> (英語サイト) で画面の指示に従ってコンピュータ名を入力してください。

ブート ブロックROM

ブート ブロックROMが装備されているので、システムROMのアップグレード中に電源の障害が発生するなどしてROMの書き換えに失敗した場合も、システムROMを復旧またはアップグレードすることができます。ブートブロックはROMフラッシュの際にも更新されない領域に収められており、コンピュータの電源が入れられるたびにシステムROMフラッシュをチェックし、以下のどれかの方法でコンピュータを起動します。

- システム ROM が有効な場合は、コンピュータは通常の方法で起動しません。

- システムROMが有効でない場合は、システムROMの復旧作業を実行できるように、RomPaqディスクからのコンピュータの起動を、ブートブロックROMがサポートします。



一部のモデルでは、RomPaqCDから復旧することもできます。

ブートブロックROMによりシステムROMが有効でないことが検出されると、システム電源ランプが8回赤く点滅し（1秒間に1回点滅した後に2秒間休止）、同時にビーブ音が8回鳴ります。ブートブロックのリカバリモードのメッセージが、画面に表示されます（一部のモデルのみ）。



ビーブ音は8回鳴り、5回繰り返されてから停止します。ただし、ランプは問題が解決するまで点滅し続けます。

ブートブロックのリカバリモードになったら、以下のように操作して、システムROMを復旧（アップグレード）してください。

1. ディスケットドライブやCDドライブにディスクまたはCDが入っている場合は取り出し、コンピュータの電源を切ります。
2. RomPaqディスクをディスクドライブに挿入します。または、お使いのコンピュータで使用できる場合は、RomPaq CDをCDドライブに挿入します。
3. コンピュータの電源を入れます。

RomPaqディスクまたはRomPaq CDが認識されない場合、RomPaqディスクを挿入してコンピュータを再起動するように指示されます。

スーパーバイザパスワードが設定されている場合、Caps Lockランプが点灯し、パスワード入力を求められます。

4. スーパーバイザパスワードを入力します。


RomPaqディスクからの再起動が正しく行われ、システムROMの復旧またはアップグレードが正常に完了すると、キーボード上の3つのランプが点灯し、ビーブ音が鳴ります。

5. ディスケットまたはCDを取り出して電源を切ります。
6. 電源を入れなおして、コンピュータを起動します。

次の表に、ブート ブロックROMによるさまざまなキーボード ランプの状態（コンピュータにPS/2キーボードが接続されている場合）を示します。また、各ランプの状態の意味およびランプの状態に応じて行う操作も示します。

ブート ブロックROMによるキーボード ランプの状態

ブート ブロック モード	ランプの色	ランプの状態	意味
Num Lock	緑色	オン	RomPaq ディスケットまたはRomPaq CDが挿入されていないか、壊れているか、またはドライブが正常に動作していない
Caps Lock	緑色	オン	パスワードを入力してください
Num、Caps、Scroll Lock	緑色	Num Lock、Caps Lock、Scroll Lockの順に1個ずつ点滅	キーボードがネットワーク モードでロックされた
Num、Caps、Scroll Lock	緑色	オン	ブート ブロックROMフラッシュが完了した。コンピュータの電源を入れなおして、コンピュータを再起動してください

 診断ランプは、USBキーボードでは点滅しません。

リプリケート セットアップ機能

コンピュータの設定情報を他の同じモデルのコンピュータにコピーするために、HPはSystem Software ManagerというWindowsベースのソフトウェアユーティリティ（<http://www.hp.com/go/ssm> からダウンロード可能）およびCMOS Save/LoadユーティリティというDOSベースのソフトウェア（<http://www.hp.com/support/files>からダウンロード可能）を提供しています。HPサポートのWebサイトを表示してから、指示に従ってコンピュータの名前を入力してください。

起動可能デバイスの作成

サポートされるUSBフラッシュ メディア デバイス

HP USBメモリなどのサポートされるデバイスには、そのデバイスを簡単な手順で起動可能にするためのイメージがプリインストールされています。使用しているUSBフラッシュ メディア デバイスにこのイメージが存在しない場合は、後で説明する手順に従ってください（13ページの「サポートされないUSBフラッシュ メディア デバイス」を参照）。



注意：USBフラッシュ メディア デバイスから起動できないコンピュータもあります。コンピュータ セットアップ (F10) ユーティリティに表示されるデフォルトの起動順序で、USBデバイスがハードディスク ドライブより前にある場合、そのコンピュータはUSBフラッシュ メディア デバイスから起動できます。それ以外の場合は、起動可能ディスクレットを使用してください。

起動可能なUSBフラッシュ メディア デバイスを作成するには、次のものが必要です。

- HP Business Desktop dx5150シリーズのコンピュータ (MTまたはSTモデル)

BIOSによっては、将来リリースされるコンピュータでもUSBフラッシュメディア デバイスからの起動がサポートされる場合があります。

- 256MB HP USBメモリIIストレージ モジュール

- FDISKおよびSYSプログラムが格納された、起動可能なDOSディスクレット。SYSがない場合はFORMATを使用できますが、USBメモリ上のファイルがすべて失われます。

1. コンピュータの電源を切ります。
2. USBメモリをコンピュータのUSBポートのどれかに差し込み、USBディスクレット ドライブ以外のすべてのUSBストレージ デバイスを取り外します。
3. FDISK.COMと、SYS.COMまたはFORMAT.COMのどちらかが格納された起動可能なDOSディスクレットをディスクレット ドライブに挿入します。コンピュータの電源を入れて、DOSディスクレットを起動します。
4. A:¥プロンプトで「**FDISK**」と入力して[**Enter**]キーを押し、FDISKを実行します。メッセージが表示されたら、[**Yes (Y)**]をクリックして大容量ディスクのサポートを有効にします。
5. 選択肢の「**5**」を入力してコンピュータのドライブを表示します。一覧のドライブの中で最も容量が近いドライブがUSBメモリで、通常は一覧の最後に表示されます。ドライブ名を書き留めておきます。

USBメモリのドライブ名 : _____



注意：ドライブがUSBメモリと一致しない場合は、データの損失を防ぐため、次の手順に進まないでください。他にストレージデバイスがないか、すべてのUSBポートを確認します。あった場合は取り外してコンピュータを再起動し、手順4に進みます。ない場合、コンピュータがUSBメモリに対応していないか、USBメモリが破損しています。この場合はUSBメモリを起動可能にするための手順を実行しないでください。

6. **[Esc]**キーを押してA:¥プロンプトに戻り、FDISKを終了します。
 7. 起動可能なDOSディスクにSYS.COMがある場合は手順8に、ない場合は手順9に進みます。
 8. A:¥プロンプトで「**SYS x:**」(xは書き留めたドライブ名)と入力します。
-



注意：USBメモリのドライブ名を正しく入力したことを確認します。

システム ファイルの転送が完了すると、SYSからA:¥プロンプトに戻ります。手順13に進みます。

9. 保存しておきたいファイルをUSBメモリから別のドライブ (コンピュータの内蔵ハードディスク ドライブなど) の一時ディレクトリにコピーします。
 10. A:¥プロンプトで「**FORMAT /S X:**」(xは書き留めたドライブ名)と入力します。
-



注意：USBメモリのドライブ名を正しく入力したことを確認します。

FORMATでは1つ以上の警告が表示され、次の手順に進む前に毎回確認画面が表示されます。毎回「**Y**」と入力します。FORMATによりUSBメモリがフォーマットされ、システム ファイルが追加され、ボリューム ラベルが要求されます。

11. ラベルを付けない場合は**[Enter]**キーを押し、必要な場合はラベルを入力します。
12. 手順9でコピーしたファイルをUSBメモリにコピーしなおします。
13. ディスケットを取り出し、コンピュータを再起動します。USBメモリがCドライブとして起動されます。



デフォルトの起動順序はコンピュータによって異なり、コンピュータ セットアップ (F10) ユーティリティで変更することができます。

Windows 9xからDOSバージョンを使用した場合、短い間Windowsロゴの画面が表示されることがあります。表示されないようにするには、USBメモリのルートディレクトリにLOGO.SYSというゼロ長のファイルを追加します。

サポートされないUSBフラッシュ メディア デバイス



注意：USBフラッシュ メディア デバイスから起動できないコンピュータもあります。コンピュータセットアップ (F10) ユーティリティに表示されるデフォルトの起動順序で、USBデバイスがハードディスク ドライブより前にある場合、そのコンピュータはUSBフラッシュ メディア デバイスから起動できます。それ以外の場合は、起動可能ディスクセットを使用してください。

起動可能なUSBフラッシュ メディア デバイスを作成するには、次のものがが必要です。

- HP Business Desktop dx5150シリーズのコンピュータ (MTまたはSTモデル)

BIOSによっては、将来リリースされるコンピュータでもUSBフラッシュメディアデバイスからの起動がサポートされる場合があります。

- FDISKおよびSYSプログラムが格納された、起動可能なDOSディスクセット。SYSがない場合はFORMATを使用できますが、USBフラッシュメディアデバイス上のファイルがすべて失われます。
1. SCSI、ATA RAID、またはSATA ドライブが取り付けられたPCIカードがコンピュータにある場合は、コンピュータの電源を切って電源コードを抜き取ります。



注意：電源コードは**必ず**抜き取ってください。

2. コンピュータのカバーを開いてPCIカードを取り外します。
3. USBフラッシュ メディア デバイスをコンピュータのUSBポートのどれかに差し込み、USBディスクドライブ以外のすべてのUSBストレージデバイスを取り外します。コンピュータのカバーを閉じます。
4. 電源コードを差し込んでコンピュータの電源を入れます。

5. コンピュータが起動したらすぐに**[F10]**キーを押したままにし、コンピュータ セットアップを実行します。必要であれば、**[Enter]**キーを押すと、タイトル画面をスキップできます。



適切なタイミングで**[F10]**キーを押せなかったときは、コンピュータを再起動して、もう一度**[F10]**キーを押したままにしてください。

PS/2キーボードを使用している場合、**[Keyboard Error]**というメッセージが表示されることがありますが、無視してかまいません。

6. **[統合周辺機器]** (Integrated Peripherals) → **[South OnChip IDEデバイス]** (South OnChip IDE Device) の順に選択してPATAコントローラを無効にし、**[統合周辺機器]**→**[South OnChip PCIデバイス]** (South OnChip PCI Device) の順に選択してSATAコントローラを無効にします。変更を保存してコンピュータ セットアップを終了します。
7. FDISK.COMと、SYS.COMまたはFORMAT.COMのどちらかが格納された起動可能なDOSディスクレットをディスクレット ドライブに挿入します。コンピュータの電源を入れて、DOSディスクレットを起動します。
8. FDISKを実行してUSBフラッシュ メディア デバイス上にあるパーティションをすべて削除します。新しいパーティションを作成して有効にします。**[Esc]**キーを押してFDISKを終了します。
9. FDISKを終了してもコンピュータが自動的に再起動されない場合は、**[Ctrl] + [Alt] + [Del]**キーを押してDOSディスクレットから起動しなおします。
10. A:¥プロンプトで「**FORMAT C: /S**」と入力し、**[Enter]**キーを押します。FORMATによりUSBフラッシュ メディア デバイスがフォーマットされ、システム ファイルが追加され、ボリューム ラベルが要求されます。
11. ラベルを付けない場合は**[Enter]**キーを押し、必要な場合はラベルを入力します。
12. コンピュータの電源を切って電源コードを抜き取ります。コンピュータのカバーを開き、取り外しておいたPCIカードを取り付けなおします。コンピュータのカバーを閉じます。
13. 電源コードを差し込み、ディスクレットを取り出してコンピュータの電源を入れます。

14. コンピュータが起動したらすぐに**[F10]**キーを押したままにし、コンピュータ セットアップを実行します。必要であれば、**[Enter]**キーを押すと、タイトル画面をスキップできます。
15. **[統合周辺機器]** (Integrated Peripherals) →**[South OnChip IDEデバイス]** (South OnChip IDE Device) の順および**[統合周辺機器]**→**[South OnChip PCIデバイス]** (South OnChip PCI Device) の順に選択して、手順6で無効にしたPATAおよびSATAコントローラを再び有効にします。
16. 変更を保存してユーティリティを終了します。USBフラッシュ メディア デバイスがCドライブとして起動されます。



デフォルトの起動順序はコンピュータによって異なり、コンピュータ セットアップ (F10) ユーティリティで変更することができます。手順については、Documentation CDに収録されている『コンピュータ セットアップ (F10) ユーティリティ ガイド』を参照してください。

Windows 9xからDOSバージョンを使用した場合、短い間Windowsロゴの画面が表示されることがあります。表示されないようにするには、USBフラッシュ メディア デバイスのルート ディレクトリにLOGO.SYSというゼロ長のファイルを追加します。

デュアル ステート電源ボタンの設定

お使いのコンピュータでACPI (Advanced Configuration and Power Interface) を使用している場合は、電源ボタンをコンピュータのオン/オフ スイッチとしての機能のほか、スタンバイ モードを起動するためのボタンとして設定することができます。スタンバイ モードでは、電源を完全に切らずに、コンピュータの消費電力を低い状態に保つことができます。使用中のアプリケーションを終了せずに作業を途中で中断したい場合など、スタンバイ モードに設定しておくことでコンピュータの電力を低く抑えることができます。

電源ボタンの設定を変更するには、以下の手順で操作します。

1. **[スタート]**ボタンを左クリックし、**[コントロール パネル]**→**[パフォーマンスとメンテナンス]**→**[電源オプション]**の順に選択します。
2. **[電源オプションのプロパティ]**で**[詳細設定]**タブを選択します。
3. **[電源ボタン]**で**[スタンバイ]**を選択します。

電源ボタンにスタンバイ ボタンとしての機能を設定してある場合は、コンピュータの電源が入っているときに電源ボタンを押すと、スタンバイ モードを起動することができます。再び電源ボタンを押すと、直ちにスタンバイ モードから復帰できます。コンピュータの電源を完全に切るには、電源ボタンを4秒以上押し続けます。



注意：システムが応答しない場合以外は、電源ボタンを使って電源を切らないでください。オペレーティング システムを通さずに電源を切ると、ハードディスク ドライブが破損したりデータが損失したりする可能性があります。

インターネット Web サイト

HPの技術者はHP製および他社製のソフトウェアのテストおよび修正を厳密に行い、オペレーティング システムに特化したサポート ソフトウェアを開発しています。このため、HPのコンピュータは優れた性能、互換性、および信頼性を兼ね備えています。

別の種類のオペレーティング システムをインストールしたり新しいバージョンのオペレーティング システムに移行したりする場合、それぞれのオペレーティング システム用に設計されたサポート ソフトウェアを実行してください。お使いのコンピュータにインストールされているバージョンと異なるバージョンのMicrosoft Windowsを実行したい場合、対応するデバイス ドライバおよびユーティリティをインストールして、すべての機能がサポートされ、正しく動作することを確認してください。

HPでは、快適な環境で効率的にコンピュータをお使いいただくために、最新のデバイス ドライバ、ユーティリティ、フラッシュ ROMイメージなどを収録したサポート ソフトウェアを提供しています。サポート ソフトウェアはHPのWebサイト (<http://www.hp.com/support>) からダウンロードできます。

HPのホームページには、HP製のコンピュータでMicrosoft Windowsのオペレーティング システムを実行する際に必要な最新のデバイス ドライバ、ユーティリティ、フラッシュ ROMイメージなどが用意されています。

標準規格およびパートナー企業

HPのインテリジェント マネジメント機能は、各社のシステム マネジメントアプリケーションを取り入れており、次のようなコンピュータ業界の標準規格に準拠しています。

- Web-Based Enterprise Management (WBEM)
- Windows Management Interface (WMI)
- Wake on LANテクノロジー
- ACPI
- SMBIOS
- Pre-boot Execution (PXE) サポート

資産情報管理機能およびセキュリティ機能

コンピュータに搭載される資産情報管理機能を使用すれば、HP Systems Insightマネージャ、HP Client Manager Software、またはその他のシステム管理アプリケーションを使用して管理される資産情報を確認することができます。資産情報管理機能とこれらの管理ソフトウェア製品を統合することにより、お使いの環境に最適な管理ソフトウェアを選択でき、今までお使いになっていたソフトウェアをより有効に活用できます。

さらに、HPでは、コンピュータとデータを不正なアクセスから保護するための機能を備えています。HP ProtectTools内蔵セキュリティがインストールされている場合は、データへの不正なアクセスの防止、システムの整合性の確認、および第三者からのアクセスに対する認証が行われます。(詳しくは、Documentation CDに収録されている『HP ProtectTools内蔵セキュリティガイド』を参照してください。)一部のモデルに装備されているProtectToolsのようなセキュリティ機能は、コンピュータの内部装置への不正なアクセスの防止に役立ちます。パラレルポート、シリアルポート、またはUSBポートを無効にすることにより、またリムーバブルメディアブート機能を無効にすることにより、貴重な資産であるデータを保護できます。これ以外にも、メモリ脱着通知が自動的にシステム管理アプリケーションに転送されることで、コンピュータの内部装置への不正なアクセスを防ぐことができます。






ProtectToolsは一部のシステムに装備されています。

次のユーティリティを使用して、セキュリティ機能の設定を管理できます。



- コンピュータ セットアップ (F10) ユーティリティを使用してローカルで管理します。コンピュータ セットアップ (F10) ユーティリティの詳細な情報と手順については、コンピュータに付属の Documentation CD に収録されている『コンピュータ セットアップ (F10) ユーティリティ ガイド』を参照してください。
- HP Client Manager Software または System Software Manager を使用してリモートで管理します。このソフトウェアにより、簡単なコマンドライン ユーティリティを使用して、ネットワークのセキュリティ機能の設定を確実に、一貫して集中管理することができます。

次の表と各項で、コンピュータ セットアップ (F10) ユーティリティを使ってローカルでコンピュータのセキュリティ機能を管理する方法を説明します。

セキュリティ機能

項目	説明
スーパーバイザ パスワード (Supervisor Password)	<p>スーパーバイザ (管理者) パスワードを設定して有効にします</p> <p> スーパーバイザ パスワードを設定すると、コンピュータ セットアップ ユーティリティの設定を変更したり、ROM をフラッシュしたり、Windows 環境で特定のプラグ アンド プレイ設定を変更したりする場合にスーパーバイザ パスワードが必要になります</p> <p>詳しくは、Documentation CD に収録されている『トラブルシューティング ガイド』を参照してください</p>
ユーザ パスワード (User Password)	<p>ユーザ パスワードを設定して有効にします</p> <p> ユーザ パスワードを設定すると、電源投入後コンピュータにアクセスするためにユーザ パスワードが必要になります</p> <p>詳しくは、Documentation CD に収録されている『トラブルシューティング ガイド』を参照してください</p>
デバイス セキュリティ (Device Security)	<p>シリアル ポート (Serial Port)、パラレル ポート (Parallel Port)、前面の USB ポート (Front USB Port)、システムのオーディオ セキュリティ (Audio Security)、およびモデルによってはネットワーク コントローラ (Network Controller) のデバイス有効 (Enable) / デバイス無効 (Disable) の設定</p>
<p> コンピュータ セットアップについて詳しくは、Documentation CD に収録されている『コンピュータ セットアップ (F10) ユーティリティ ガイド』を参照してください。サポートされるセキュリティ機能は、お使いのコンピュータの構成によって異なる場合があります。</p>	

セキュリティ機能（続き）

項目	説明
ネットワーク サービス ブート (Network Service Boot)	ネットワーク サーバにインストールされたオペレーティング システムからコンピュータを起動する機能の有効 (Enable) / 無効 (Disable) の設定 (NICモデルのみで使用でき、ネットワーク コントローラがPCIバス上に存在するか、システム ボードに組み込まれている必要があります)
システムID (System ID)	<p>次の項目を設定します</p> <ul style="list-style-type: none"> • アセット タグ (Asset Tag。18バイトのID) およびオーナーシップ タグ (Ownership Tag。POST実行中に表示される80バイトのID) の入力 • 本体シリアル番号 (Chassis Serial Number) またはUUID (Universal Unique Identifier) の入力 UUIDは現在の本体シリアル番号が無効の場合にのみ更新できます (通常これらの識別 (ID) 番号は工場出荷時に設定され、そのシステムを特定するために使用されます) • キーボード (Keyboard Locale) の設定 英語用やドイツ語用などをシステムIDエントリに対して設定します
マスタ ブート レコード セキュリティ (Master Boot Record Security)	<p>マスタ ブート レコード (MBR) セキュリティを有効 (Enable) / 無効 (Disable) に設定します</p> <p>有効に設定すると、BIOSは、現在の起動可能ディスクのMBRへの書き込み要求をすべて拒否します。コンピュータの電源を入れるか再起動するたびに、BIOSは現在の起動可能ディスクのMBRと前回保存したMBRとを比較します。変更が検出された場合、現在の起動可能ディスクのMBRを保存するか、前回保存したMBRを復元するか、またはMBRセキュリティを無効にすることができます。セットアップ パスワードが設定されている場合は、セットアップ パスワードを入力する必要があります</p> <p> 現在の起動可能ディスクのフォーマットやパーティションを意図的に変更する際は、MBRセキュリティを無効に設定します。一部のディスク ユーティリティ (FDISKやFORMATなど) はMBRを更新しようとして、MBRセキュリティが有効に設定されたままBIOSによってディスク アクセスの処理が行われると、MBRへの書き込み要求は拒否され、ユーティリティはエラーを表示します</p> <p>MBRセキュリティが有効に設定されたままオペレーティング システムによってディスク アクセスの処理が行われると、次の再起動時にBIOSによってMBRの変更が検出され、MBRセキュリティの警告メッセージが表示されます</p>
	<p>コンピュータ セットアップについて詳しくは、Documentation CDに収録されている『コンピュータ セットアップ (F10) ユーティリティ ガイド』を参照してください。サポートされるセキュリティ機能は、お使いのコンピュータの構成によって異なる場合があります。</p>

パスワードのセキュリティ

ユーザパスワード (User password) を設定すると、コンピュータの電源を入れたり再起動したりするたびに、アプリケーションやデータにアクセスするためのパスワードの入力が要求されるので、コンピュータが許可無く使用されることを防止できます。スーパーバイザパスワード (Supervisor password) は、特にコンピュータ セットアップ (F10) ユーティリティへの不正アクセスを防ぎます。スーパーバイザパスワードを、ユーザパスワードの補助手段として使用することもできます。つまり、ユーザパスワードの入力を要求されたときに、代わりにスーパーバイザパスワードを入力してコンピュータにアクセスすることもできます。

ネットワーク全体のスーパーバイザパスワードを設定しておく、システム管理者はネットワーク上のすべてのシステムにログインでき、設定されているユーザパスワードを知らなくてもメンテナンスを行うことができます。



System Software ManagerおよびHP Client Manager Softwareを使用すると、ネットワーク環境のセットアップパスワードおよびその他のBIOS設定をリモートで管理できます。詳しくは、<http://www.hp.com/go/EasyDeploy> (英語サイト) を参照してください。

スーパーバイザパスワードの設定

システムに内蔵セキュリティデバイスが搭載されている場合は、Documentation CDに収録されている『HP ProtectTools内蔵セキュリティガイド』を参照してください。[コンピュータ セットアップ (F10) ユーティリティ]メニューで、スーパーバイザパスワードを設定しておけば、無断でコンピュータの設定が変更されることを防止できます。

1. コンピュータの電源を入れるか、[スタート]→[シャットダウン]→[再起動]→[OK]の順に選択して再起動します。
2. コンピュータが起動したらすぐに[F10]キーを押したままにし、コンピュータ セットアップを実行します。必要であれば、[Enter]キーを押すと、タイトル画面をスキップできます。



適切なタイミングで[F10]キーを押せなかったときは、コンピュータを再起動して、もう一度[F10]キーを押したままにしてください。

PS/2キーボードを使用している場合、[Keyboard Error]というメッセージが表示されることがありますが、無視してかまいません。

3. [スーパーバイザ パスワードを設定] (Set Supervisor Password) を選択してパスワードを入力します。
4. 設定を終了するには、[保存してセットアップを終了] (Save & Exit Setup) を選択します。

ユーザ パスワードの設定

[コンピュータ セットアップ ユーティリティ]メニューで、ユーザ パスワードを設定しておけば、無断でコンピュータが使用されることを防止できます。ユーザ パスワードが設定されていると、コンピュータ セットアップ ユーティリティの[セキュリティ設定] (Security) メニューに[パスワード オプション] (Password Options) が表示されます。パスワード オプションには[ウォーム ブート時のパスワード入力] (Password Prompt on Warm Boot) などが含まれます。[ウォーム ブート時のパスワード入力]が有効にされている場合も、コンピュータを再起動するたびにパスワードを入力する必要があります。

1. コンピュータの電源を入れるか、[スタート]→[シャットダウン]→[再起動]→[OK]の順に選択して再起動します。
2. コンピュータが起動したらすぐに[F10]キーを押したままにし、コンピュータ セットアップを実行します。必要であれば、[Enter]キーを押すと、タイトル画面をスキップできます。



適切なタイミングで[F10]キーを押せなかったときは、コンピュータを再起動して、もう一度[F10]キーを押したままにしてください。

PS/2キーボードを使用している場合、[Keyboard Error]というメッセージが表示されることがありますが、無視してかまいません。

3. [ユーザ パスワードを設定] (Set User Password) を選択してパスワードを入力します。
4. 設定を終了するには、[保存してセットアップを終了]を選択します。

ユーザ パスワードの入力

ユーザ パスワードを入力するには、以下の手順で操作します。

1. コンピュータの電源を入れるか、[スタート]→[シャットダウン]→[再起動]→[OK]の順に選択して再起動します。
2. [パスワードの入力] (Enter Password) ボックスが表示されたら、パスワードを入力して[Enter]キーを押します。



機密保護のため、入力したパスワードは画面に表示されません。パスワードを入力する際は、間違えないよう注意してください。

間違ったパスワードを入力した場合は、[パスワードが無効です。続行するには何かキーを押してください!] (Invalid Password, Press any key to continue!) というメッセージが表示されますので、パスワードを正しく入力しなおしてください。続けて3回間違えた場合は、コンピュータの電源をいったん切って最初から操作しなおす必要があります。

スーパバイザ パスワードの入力

システムに内蔵セキュリティ デバイスが搭載されている場合は、Documentation CDに収録されている『HP ProtectTools内蔵セキュリティ ガイド』を参照してください。

コンピュータでスーパバイザ パスワードを設定しておけば、[コンピュータ セットアップ ユーティリティ]メニューを実行するたびに、必ずパスワードの入力が必要となります。

1. コンピュータの電源を入れるか、[スタート]→[シャットダウン]→[再起動]→[OK]の順に選択して再起動します。
2. コンピュータが起動したらすぐに[F10]キーを押したままにし、コンピュータ セットアップを実行します。必要であれば、[Enter]キーを押すと、タイトル画面をスキップできます。



適切なタイミングで **[F10]** キーを押せなかったときは、コンピュータを再起動して、もう一度 **[F10]** キーを押したままにしてください。

PS/2キーボードを使用している場合、**[Keyboard Error]** というメッセージが表示されることがありますが、無視してかまいません。

3. **[パスワードの入力]** (Enter Password) ボックスが表示されたら、スーパーバイザ パスワードを入力して **[Enter]** キーを押します。



機密保護のため、入力したパスワードは画面に表示されません。パスワードを入力する際は、間違えないよう注意してください。

間違ったパスワードを入力した場合は、**[パスワードが無効です。続行するには何かキーを押してください]** (Invalid Password, Press any key to continue!) というメッセージが表示されますので、パスワードを正しく入力しなおしてください。続けて3回間違えた場合は、コンピュータの電源をいったん切って最初から操作しなおす必要があります。

ユーザ パスワードまたはスーパーバイザ パスワードの変更

システムに内蔵セキュリティ デバイスが搭載されている場合は、Documentation CDに収録されている『HP ProtectTools内蔵セキュリティ ガイド』を参照してください。

1. コンピュータの電源を入れるか、**[スタート]**→**[シャットダウン]**→**[再起動]**→**[OK]**の順に選択して再起動します。
2. **[パスワードの入力]**ボックスが表示されたら、必要であればユーザ パスワードを入力します。
3. **[Enter]**キーを押します。
4. **[F10]**キーを押したままにし、コンピュータ セットアップを実行します。必要であれば、**[Enter]**キーを押すと、タイトル画面をスキップできます。



適切なタイミングで **[F10]** キーを押せなかったときは、コンピュータを再起動して、もう一度 **[F10]** キーを押したままにしてください。

PS/2キーボードを使用している場合、**[Keyboard Error]** というメッセージが表示されることがありますが、無視してかまいません。

5. コンピュータ セットアップにアクセスする際に[パスワードの入力] (Enter Password) ボックスが表示されたら、必要であればスーパーバイザパスワードを入力します。
6. **[Enter]**キーを押します。
7. [スーパーバイザ パスワードを設定] (Set Supervisor Password) または[ユーザ パスワードを設定] (Set User Password) を選択します。
8. [パスワードの入力] (Enter Password) ボックスが表示されたら、新しいパスワードを入力して**[Enter]**キーを押します。
9. 設定を終了するには、[保存してセットアップを終了] (Save & Exit Setup) を選択します。



パスワードを変更するのではなく削除するには、[パスワードの入力]ボックスが表示されたときに新しいパスワードを入力せずに**[Enter]**キーを押します。これにより現在のパスワードが削除されます。

ユーザ パスワードを忘れてしまった場合

設定しておいたユーザ パスワードを忘れると、コンピュータを使用できなくなります。パスワードを解除する方法については、Documentation CDに収録されている『トラブルシューティングガイド』を参照してください。

システムに内蔵セキュリティ デバイスが搭載されている場合は、Documentation CDに収録されている『HP ProtectTools内蔵セキュリティ ガイド』を参照してください。

マスタ ブート レコード セキュリティ (Master Boot Record Security)

マスタ ブート レコード (MBR) には、ディスクから正常に起動して、ディスク上に保存されているデータにアクセスするための情報が入っています。マスタ ブート レコードのセキュリティ機能によって、誤ってMBRを変更したり不正にMBRが変更されたりすると(一部のコンピュータ ウィルスによってデータが変更されたり、ディスク ユーティリティを誤って使用したりするなど)、その変更が検出および報告されます。また、システムの再起動時にMBRへの変更が検出された場合、このセキュリティによって「正常であることが分かっている最新の」MBRを復元することができます。

MBRセキュリティを有効にするには、以下の手順で操作します。

1. コンピュータの電源を入れるか、[スタート]→[シャットダウン]→[再起動]→[OK]の順に選択して再起動します。
2. コンピュータが起動したらすぐに[F10]キーを押したままにし、コンピュータ セットアップを実行します。必要であれば、[Enter]キーを押すと、タイトル画面をスキップできます。



適切なタイミングで[F10]キーを押せなかったときは、コンピュータを再起動して、もう一度[F10]キーを押したままにしてください。

PS/2キーボードを使用している場合、[Keyboard Error]というメッセージが表示されることがありますが、無視してかまいません。

3. [BIOSの詳細設定] (Advanced BIOS Features) →[MBRセキュリティ] (MBR Security) の順に選択して[Enter]キーを押します。
4. [MBRセキュリティ]ポップアップ ボックスで、上下の矢印キーを押して [有効] (Enabled) / [無効] (Disabled) を選択します。
5. 変更を適用するには[Enter]キー、破棄するには[Esc]キーを押します。

MBRセキュリティを有効にすると、BIOSは、MS-DOSやWindowsのSafeモードで現在の起動可能ディスクのMBRが変更されることを防ぎます。



ほとんどのオペレーティング システムは、現在の起動可能ディスクのMBRへのアクセスを制御します。したがって、オペレーティング システムの動作中に行われる変更については、BIOSは阻止できません。

コンピュータの電源を入れるか、再起動するたびに、BIOSは現在の起動可能ディスクのMBRと前回に保存されたMBRとを比較します。変更が検出され、かつ現在の起動可能ディスクが、前回MBRを保存したディスクと同じである場合、次のメッセージが表示されます。

1999 - Master Boot Record has changed. (マスタ ブート レコードが変更されました。)

1. 任意のキーを押して、[コンピュータ セットアップ ユーティリティ]メニューでMBRセキュリティを設定します。

2. [コンピュータ セットアップ ユーティリティ]メニューで、MBRセキュリティ機能を無効にします。

スーパーバイザ パスワードが設定されている場合は、スーパーバイザ パスワードの入力が必要です。

変更が検出され、現在の起動可能ディスクが、前回にMBRを保存したディスクと同じでない場合は、次のメッセージが表示されます。

2000 - Master Boot Record Hard Drive has changed. (マスタ ブート レコードのハードディスク ドライブが変更されています。)

1. 任意のキーを押して、[コンピュータ セットアップ ユーティリティ]メニューでMBRセキュリティを設定します。

2. [コンピュータ セットアップ ユーティリティ]メニューで、MBRセキュリティ機能を無効にします。

スーパーバイザ パスワードが設定されている場合は、スーパーバイザ パスワードの入力が必要です。

万一、前回保存したMBRが破損した場合は、次のメッセージが表示されます。

1998 - Master Boot Record has been lost. (マスタ ブート レコードがありません。)

1. 任意のキーを押して、[コンピュータ セットアップ ユーティリティ]メニューでMBRセキュリティを設定します。

2. [コンピュータ セットアップ ユーティリティ]メニューで、MBRセキュリティ機能を無効にします。

スーパーバイザ パスワードが設定されている場合は、スーパーバイザ パスワードの入力が必要です。

現在の起動可能ディスクのパーティションとフォーマットを変更する前に

現在の起動可能ディスクのパーティションやフォーマットを変更する前に、MBRセキュリティが無効になっていることを確認してください。FDISKやFORMATなど一部のディスクユーティリティは、MBRを更新しようとしません。ディスクのパーティションやフォーマットを変更する際にMBRセキュリティが有効である場合は、次にコンピュータの電源を入れるか再起動したときに、ディスクユーティリティからエラーメッセージが表示されたり、MBRセキュリティから警告が発生したりする可能性があります。

MBRセキュリティを無効にするには、以下の手順で操作します。

1. コンピュータの電源を入れるか、[スタート]→[シャットダウン]→[再起動]→[OK]の順に選択して再起動します。
2. コンピュータが起動したらすぐに[F10]キーを押したままにし、コンピュータセットアップを実行します。必要であれば、[Enter]キーを押すと、タイトル画面をスキップできます。



適切なタイミングで[F10]キーを押せなかったときは、コンピュータを再起動して、もう一度[F10]キーを押したままにしてください。

PS/2キーボードを使用している場合、[Keyboard Error]というメッセージが表示されることがありますが、無視してかまいません。

3. [BIOSの詳細設定] (Advanced BIOS Features) →[MBRセキュリティ] (MBR Security) の順に選択して[Enter]キーを押します。
4. [MBRセキュリティ]ポップアップボックスで、下向きの矢印キーを使用して[無効] (Disabled) を選択します。
5. [Enter]キーを押します。
6. 設定を終了するには、[保存してセットアップを終了] (Save & Exit Setup) を選択します。

ケーブル ロックの取り付け

コンピュータのリア パネルにはケーブル ロックを取り付けられるようになっているので、市販のケーブル ロックを使用して、コンピュータを作業エリアに固定できます。

詳しくは、Documentation CDに収録されている『ハードウェア リファレンス ガイド』を参照してください。

障害通知および復旧機能

障害通知および復旧機能とは、最新のハードウェア/ソフトウェア技術を結合して、重要なデータの損失を防ぎ、故障時間を最小限に抑える機能です。

HP Client Manager Softwareによって管理されるネットワークにコンピュータが接続されている場合、ネットワーク管理ソフトウェアに障害通知が送られます。HP Client Manager Softwareでは、管理されているすべてのコンピュータで診断ユーティリティを実行し、失敗したテストの概要を作成するよう、リモートでスケジュールを設定することもできます。

耐サージ機能付連続供給電源装置

耐サージ機能が付いた連続供給電源によって、急激な電圧の変化に対処することができます。この電源装置は、データの損失やシステム ダウンを引き起こさずに2000 Vまでのサージ電圧に耐えられることが確認されています。

温度センサ機能

温度センサ機能は、ハードウェアとソフトウェアの統合により提供される機能で、コンピュータ内部の温度を監視します。温度が通常範囲を超えると、画面上に警告メッセージが表示されるため、内部部品の故障やデータの損失が発生する前に対処することができます。



モデルにより温度センサ機能はサポートされない場合があります。

索引

A			
Altiris	4	Subscriber's Choice	7
H		System Software Manager (SSM)	6
HP Client Manager Software	4	コンピュータの導入	2
HP USBメモリ		ソフトウェアのサポート	16
起動可能	10~15	リプリケートセットアップ機能	10
HPのインテリジェント マネジメント機能	1	リモートROMフラッシュ	8
P		あ	
PCN (Proactive Change Notification)	6	インターネットアドレス	
Preboot Execution Environment (PXE)	3	「Webサイト」を参照	
Proactive Change Notification (PCN)	6	オペレーティング システム、重要な情報	16
PXE (Preboot Execution Environment)	3	オペレーティング システムの変更、重要な情報	16
R		温度、コンピュータ内部	28
ROM		温度センサ機能	28
アップグレード	7	か	
キーボードランプ、表	10	キーボードランプ、ROM、表	10
無効	9	起動可能ディスク、重要な情報	27
リモートフラッシュ	8	起動可能デバイス	
ROMのアップグレード	7	HP USBメモリ	10~15
ROMの保護、注意	7	USBフラッシュ メディア デバイス	10~15
S		USBフラッシュ メディア デバイス、起動可能	10~15
SSM (System Software Manager)	6	作成	10~15
System Software Manager (SSM)	6	ケーブルロックの取り付け	28
U		コンピュータ内部の温度	28
URL (Webサイト)		コンピュータへのアクセスの制御	17
「Webサイト」を参照		さ	
W		資産情報管理機能	17
Webサイト		システムの復旧	8
Altiris	5	出荷時の設定	2
HP Client Manager	4	障害通知	28
HPQFlash	8	スーパバイザ パスワード	
Proactive Change Notification	6	削除	24
RomPaqイメージ	7	設定	20
ROMフラッシュ	7	入力	22

変更	23	な	
セキュリティ		入力	
機能、表	18	スーパーバイザ パスワード	22
設定	17	ユーザ パスワード	22
パスワード	20	は	
マスタ ブート レコード	24~26	パスワード	
セットアップ		解除	24
初期設定	2	削除	24
ソフトウェア		スーパーバイザ	20, 22
System Software Manager	6	セキュリティ	20
資産情報管理機能	17	入力	22
障害通知および復旧機能	28	変更	23
統合	2	ユーザ	21, 22
ブート ブロックROM	9	パスワードの解除	24
複数のコンピュータのアップデート	6	パスワードの削除	24
復旧	2	パスワードの変更	23
マスタ ブート レコードセキュリティ	24~26	ブート ブロックROM	9
リモートROMフラッシュ	8	複製用ツール、ソフトウェア	2
ソフトウェアのカスタマイズ	2	復旧、ソフトウェア	2
た		プリインストールされたソフトウェア イメージ	2
耐サージ機能付連続供給電源装置	28	変更通知	6
注意		ま	
ROMの保護	7	マスタ ブート レコードセキュリティ	24~26
ディスクのパーティション、重要な情報	27	無効なシステムROM	9
ディスクのフォーマット、重要な情報	27	や	
ディスク、複製	2	ユーザ パスワード	
デュアル ステート電源ボタン	15	削除	24
電源供給、耐サージ機能	28	設定	21
電源ボタン		入力	22
設定	15	変更	23
デュアル ステート	15	ら	
電源ボタンの設定	15	リモートROMフラッシュ	8
導入用ツール、ソフトウェア	2	リモート システム インストール、アクセス	3