



## デスクトップ マネジメントについて

### Business PC

製品番号 : 391759-291

**2005年5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 2005 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

Business PC

初版 2005年5月

製品番号：391759-291

日本ヒューレット・パッカード株式会社

---

# 目次

## デスクトップ マネジメント

出荷時設定の変更	2
Altiris Deployment Solution Agent	3
HP Local Recovery	3
リモート システム インストール	4
ソフトウェアのアップデートと管理	5
HP System Software Manager	5
HP Client Manager Software	6
HP Client Management Solutions using Altiris	7
HP OpenView Management Suite for Desktops Using Radia	9
HP Local Recovery	10
Dantz Retrospect Express	11
Proactive Change Notification	13
Subscriber's Choice	13
廃止されたソリューション	14
ROMフラッシュ機能	15
リモートROMフラッシュ機能	15
HPQFlash	16
Boot Block Emergency Recovery Mode	16
リプリケート セットアップ機能	17
デュアル ステート電源ボタンの設定	25
インターネットWebサイト	26
標準規格およびパートナー企業	26
資産情報管理機能およびセキュリティ機能	27
パスワードのセキュリティ	31
セットアップ パスワードの設定	31
電源投入時パスワードの設定	32
ドライブロック (DriveLock)	36
スマート カバー センサ/カバー リムーバル センサ (Cover Removal Sensor)	39
スマート カバー ロック	40
ケーブル ロックの取り付け	42
指紋認証テクノロジー	43
障害通知および復旧機能	43
ドライブ保護システム	44
耐サージ機能付連続供給電源装置	44
温度センサ機能	44

## 索引

---

# デスクトップ マネジメント

HP Client Management Solutions 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 HP Client Management Solutionsの互換性を確保しています。HP Client Management Solutions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



このガイドで説明される機能のサポートについては、機種またはソフトウェアのバージョンにより異なることがあります。

---

## 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 Solution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。

## Altiris Deployment Solution Agent

このプログラムは、コンピュータにプリロードされています。このプログラムをインストールすると、管理者のDeployment Solution コンソールとの通信が可能になります。

Altiris Deployment Solution Agentをインストールするには、以下の手順で操作します。

1. [スタート]をクリックします。
2. [すべてのプログラム]をクリックします。
3. [Software Setup] (ソフトウェアのセットアップ) をクリックします。
4. [次へ]をクリックします。
5. 下へスクロールし、Altiris AClientをインストールするリンクをクリックします。

## HP Local Recovery

Local Recoveryは、データとシステム ファイルをハードディスク ドライブ上の保護された領域にバックアップします。データまたはファイルの損失、削除、破壊のどれかが発生している場合は、Local Recoveryを使用してデータを取得するか、最後の正常なシステム イメージを復元することができます。

このプリロードされているプログラムをインストールするには、以下の手順で操作します。

1. [スタート]をクリックします。
2. [Local Recovery]をクリックします。
3. [次へ]をクリックします。
4. 下へスクロールし、リンクをクリックしてHP Local Recoveryをインストールします。

## 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、コンピュータを起動して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 (15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、ワークステーション、およびノートブック コンピュータのソフトウェアを管理し、アップデートするための以下のツールを提供しています。

- HP System Software Manager
- HP Client Manager Software
- HP Client Management Solutions using Altiris
- HP OpenView Management Suite for Desktops using Radia
- HP Local Recovery
- Dantz Backup and Recovery
- HP Proactive Change Notification
- HP Subscriber's Choice

### HP System Software Manager

HP System Software Manager (SSM) は、ネットワーク上にあるHP Business PCのデバイス ドライバおよびBIOSアップデートのリモート展開を自動化するための、無料のユーティリティです。SSMを実行すると、各ネットワーク クライアント システムにインストールされているドライバおよびBIOSのリビジョン レベルが (ユーザとの対話なしに) 自動的に確認され、このインベントリと、すでにテストされ、中央のファイル格納ディレクトリに格納されているシステム ソフトウェアのSoftPaqが比較されます。SSMでは次に、ネットワークPC上の古いリビジョンのシステム ソフトウェアが、ファイル格納ディレクトリで使用可能な最新のレベルに自動的にアップデートされます。SSMではSoftPaq アップデートが正しいクライアント システム モデルにだけ配布されるため、管理者は確実かつ効率的に、SSMを使用してシステム ソフトウェアを最新版に維持できます。



System Software Manager は、HP OpenView Management Suite using Radia や Microsoft® Systems Management Server (SMS) などのエンタープライズ ソフトウェア配布ツールと統合されています。SSMを使用すると、SSM形式にパッケージ化された、顧客が作成したアップデートや他社製アップデートを配布できます。

SSMは、[www.hp.com/go/ssm](http://www.hp.com/go/ssm) (英語サイト) から無料でダウンロードできます。

## HP Client Manager Software

Altiris社で開発されたHP Client Manager Softwareは、サポートされているすべてのHP Business Desktop PC、ノートブック コンピュータ、およびワークステーション モデルで無料で使用できます。SSMは、HP Client Managerに統合されており、HP クライアント システムのハードウェアの状態を中央から追跡、監視、および管理できるようにします。

HP Client Managerを使用すると、次のことが可能になります。

- CPU、メモリ、ビデオ、セキュリティ設定などの役立つハードウェア情報を取得する
- システム状態を監視して、問題が発生する前に解決できるようにする
- ドライバおよびBIOSアップデートを、各PCの場所まで移動せずにインストールする
- BIOSやセキュリティ設定をリモートで設定する
- ハードウェアの問題を迅速に解決するためのプロセスを自動化する

HP Client Managerは、他のAltirisクライアント ライフサイクル管理ソリューションと同じAltiris インフラストラクチャを使用しています。この設計によって、セットアップおよびメンテナンスが必要なインフラストラクチャが1つだけになるため、IT担当者には大きな利点となります。情報が1つのデータベースに格納されるため、完全で、かつ整合性のあるインベントリ レポート、システム状態、およびセキュリティ情報が取得されます。クライアント システムのハードウェアおよびソフトウェア両方の管理タスクの進行状況をスケジュールして監視するための、単一で、一貫したコンソール インタフェースを使用できます。

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

## HP Client Management Solutions using Altiris

HP Client Managerのハードウェア管理機能を補完するAltirisクライアント管理ソリューションをHPから追加で購入できます。これらのAltirisソリューションは、次に示すクライアントITライフサイクルの各課題に対応しています。

- インベントリの評価
- ソフトウェア ライセンスの準拠
- 個人設定の移行
- ソフトウェア イメージの導入
- ソフトウェアの配布
- 資産管理
- クライアントのバックアップとリカバリ
- 問題の解決

HP Client Management Solutions using Altirisについて詳しくは、[www.hp.com/go/easydeploy](http://www.hp.com/go/easydeploy) (英語サイト) を参照してください。

HPとAltiris社はユニークな提携関係にあります。この提携は販売とマーケティングの領域にとどまらず、HPのパートナーおよび顧客に最善のソリューションを提供するための、HPクライアント、サーバ、OpenView、およびサービスグループにわたる共同開発やテクノロジー共有まで拡張されています。

コンパック パーソナル システム グループとAltiris社は1999年、PCハードウェアおよびマネジメントのパイオニアとしてのコンパックの長所と、Altiris社のPC展開および移行機能の長所を結合するための提携関係に入りました。この関係は、コスト削減のための総合的なITライフサイクル管理ソリューションの導入によって戦略的な提携に拡張されました。これらのソリューションには、HP PCに最善のハードウェア管理機能を提供する、共同開発されたHP Client Manager Softwareが含まれています。

パーソナル システム グループの成功に基づいて、業界標準のサーバ グループは2001年、Altiris Deployment SolutionsのOEMバージョンとHPのSmartStart Toolkitが結合された、ProLiant Essentials Rapid Deployment Packを導入しました。HPは、このソリューションを、HPのConsolidated Client Infrastructureの主要コンポーネントであるBlade PCとともにProLiantサーバ（ブレードサーバを含む）のプロビジョニングに使用しています。

HPとコンパックの合併に伴い、この提携は以下のように引き続き拡張されてきました。

- Altiris Deployment Solutionsは、HP Business PCで30日間の無料試用版として使用できます。それ以降はライセンスの購入が可能です。
- クライアントのバックアップ/リカバリ ユーティリティであるHP Local Recoveryは、HP Business PCでは無料で使用できます。
- Altiris Connector for HP OpenViewは、HP OpenView Network Node Manager、Operations、およびService Deskとのクライアント インベントリおよびイベント統合を提供します。
- Altiris Connector for HP Systems Insight Managerにより、HP Systems Insight Manager コンソールからHPクライアントおよびサーバを統合して展開および管理できるようになります。

HPは、PC、ハンドヘルド製品、Thin Client、Windows<sup>®</sup>およびLinuxサーバなどの展開と設定を行うだけでなく、HPの企業管理ツールとのレベルの高い統合を実現する、単一の管理ソリューションおよびコンソールを提供することによって市場をリードしています。HPは、HPのサービス部門およびAltiris社から利用可能な、広範囲のトレーニングおよびサービスの専門知識を提供しています。HP Client Management Solutionsとサービス機能のこの組み合わせによって、クライアント システムの管理にかかるコストと複雑さを軽減したいと考えている顧客に最善の選択が提供されます。

## HP OpenView Management Suite for Desktops Using Radia

HP OpenView Management Suite for Desktops Using Radiaは、管理者が、Webベースのコンソールから異種のデスクトッププラットフォームにわたって効率的に、かつ確実にソフトウェアとコンテンツのインベントリ管理、展開、およびメンテナンスを行うことのできる、拡張性の高い、ポリシーベースの変更および構成管理が可能なソフトウェアです。

HP OpenView Management Suite for Desktops Using Radiaによって、デスクトップアプリケーションの可用性だけでなく、従業員、パートナー、または顧客が必要とするオペレーティングシステム、アプリケーション、およびコンテンツが常に100%正しいことが保証されます。

HP OpenView Management Suite for Desktops Using Radiaは、世界中の企業顧客によって、きわめて複雑かつ大規模なIT環境で、99%を超える展開の信頼性を実現することが実証されています。変更の管理が自動化されるため、ITコストの大幅な削減、ソフトウェアやコンテンツを市場に投入するまでの時間の短縮、およびユーザの生産性と満足度の向上が得られます。

HP OpenView Management Suite for Desktops Using Radiaを使用すると、IT技術者は次のことが可能になります。

- 複数のプラットフォームにわたってハードウェアおよびソフトウェアインベントリを収集する
- 配布の前にアプリケーションパッケージを準備し、影響を分析する
- ポリシーに従い、個々のデスクトップ コンピュータ、ワークグループ、またはデスクトップ コンピュータのグループ全体を対象にして、ソフトウェアとコンテンツの展開およびメンテナンスを行う
- 分散したデスクトップ コンピュータ上にあるオペレーティング システム、アプリケーション、およびコンテンツを任意の場所からプロビジョニングして管理する
- HP OpenView Service Deskやその他のヘルプデスクおよびシステム管理ツールと統合する
- すべての企業ユーザのほぼすべてのデバイス、プラットフォーム、およびネットワーク上でソフトウェアとコンテンツを管理するための共通のインフラストラクチャを活用する

■ 企業ニーズを満たすように拡張する

HP OpenView Management Suite for Desktops Using Radiaは、スタンドアロンソリューションとして提供されます。それと同時に、企業のコンピュータ デバイスに含まれるすべてのソフトウェアの自動化された、継続的なメンテナンスを提供する、HPのユニークな望ましい状態の管理アプローチの不可欠なコンポーネントとして、他のHP OpenView Management Suite using Radia 製品とも完全に統合されています。HP OpenView Management Suite using Radia 製品によって、ソフトウェア インフラストラクチャ全体が常に望ましい状態、つまり最新で、信頼性が高く、セキュリティで保護された状態にあることが保証されます。

HP OpenView Management Suite for Desktops Using Radia について詳しくは、[http://managementsoftware.hp.com/products/radia\\_mdsk/index.html](http://managementsoftware.hp.com/products/radia_mdsk/index.html) (英語サイト) を参照してください。

## HP Local Recovery

Local Recoveryは、HP Business Desktop PC、ノートブック コンピュータ、およびワークステーションモデルに対するデータとシステム ファイルの保護機能を提供します。Local Recoveryを使用すると、データとシステム ファイルを迅速に復旧し、情報が誤って削除されたり、オペレーティング システムが壊れたりする前の状態まで戻すことができます。Local Recoveryは、ネットワーク接続環境にないユーザのために設計されており、定期的に作成されるローカル ハードディスク上の保護された領域に格納されるスナップショットを使用して、HP コンピュータのデータとシステムの状態を保護します。バックアップまたは復元は、ブート前の環境でマウスをクリックするか、**[F11]**キーを押すだけで簡単に実行できます。システムのバックアップとディザスタリカバリは現在、接続状況には関係なく、すべてのユーザにとって容易な作業になっています。

Local Recoveryは、HP Business PCでは無料で使用できます。これに加えて、2つのクライアントリカバリ製品も使用できます。これらの製品にアップグレードすると、次に示すリカバリ機能が追加で提供されます。

- **Local Recovery Pro** : Local Recoveryのすべての機能に加えて、セカンダリハードディスク ドライブへのバックアップおよびリカバリと、オープンおよびロック ファイルに対するサポートも提供されます。バックアップスナップショットの作成中は、オープン/ロック ファイルのサポートによって、情報が電子メール メッセージ、プレゼンテーション、ワープロ文書などのオープンアプリケーションに保存されます。
- **Recovery Solution** : 中央管理コンソールから、PCの完全な企業レベルのバックアップおよびリカバリが提供されます。このソリューションは、ローカルハードディスク ドライブ上の保護された領域だけでなく、ネットワーク記憶域へのデータ バックアップもサポートしています。このネットワーク ベースのリカバリ機能によって、ハードディスク ドライブの障害や、PCの盗難または紛失のために消失したデータに対する高いレベルの保護が提供されます。

HP Local Recoveryについて詳しくは、[www.hp.com/go/easydeploy](http://www.hp.com/go/easydeploy) (英語サイト) を参照してください。

## Dantz Retrospect Express

Dantz Retrospect Expressは、単一のWindowsデスクトップまたはノートブックコンピュータを保護します。Retrospect Expressによって、ウィルス、新しくインストールしたソフトウェア、ユーザによるエラー、ハードウェアの損傷、ハードウェアのアップグレード、ハッカー、コンピュータの紛失または盗難などによるデータ損失からのリカバリが可能になります。単純な複製か総合的なバックアップのどちらかを選択でき、直感的なセットアップ ウィザードによって数分でコンピュータを再び稼働させることができます。最善の保護機能を実現するために、Retrospect Expressにはディザスタ リカバリが組み込まれています。各社の製品にRetrospectをバンドルしているハードウェア製造元の一覧と、これらの製品の購入方法を表示するには、[ここをクリックしてください](#)。

Retrospect Expressをインストールして、2分以内に最初のバックアップを実行できます。Retrospectでは、いくつかの簡単な質問に答えるだけでバックアップ計画を実装できます。復元はすばやく簡単に実行されます。復元を実行することが必要になると、そのファイルがどのバックアップメディアに含まれているかを知らなくても、Retrospect Expressが自動的にそのファイルの場所を見つけます。

ボタンを押すだけで、ファイルとフォルダを外付けハードディスク ドライブに複製します。複製操作によって、情報がコンピュータのハードディスク ドライブから外付けハードディスク ドライブにコピーされます (バックアップ ボタンが組み込まれた外付けハードディスク ドライブの場合は、そのボタンを押すだけで簡単に複製を起動できます)。複製を使用すると、外付けハードディスク ドライブ上のファイルとフォルダを、Windowsエクスプローラを使用して簡単に表示、操作、および復元することができます。複製プロセスでは、外付けドライブ上にあった以前のバックアップデータが上書きされるため、領域が節約されます。また、新しいファイルまたは直前のバックアップ以降に変更されたファイルだけがコピーされるため、時間も節約されます。

複数バージョンのファイルとフォルダをバックアップできます。総合的なバックアップでは、以前のバージョンのファイルとフォルダが保持されているため、コンピュータをデータが破壊される前の任意の時点でロールバックできます。バックアップ操作を実行するたびに、Retrospect Expressによって、ユーザがファイルの取得またはコンピュータ全体の復元 (ディザスタ リカバリ) を行うために必要なすべての情報が含まれた復元ポイントが作成されます。この情報には、すべてのオペレーティング システム ファイルと設定、デバイス ドライバ、およびアプリケーションとその設定が含まれます。この復元ポイントは迅速に作成され、それにより、バックアップが実行された任意の時点への100%正確な復元が可能になります。これは、他のバックアップ ソフトウェアの機能より優れています。

Dantz Retrospect Expressについて詳しくは、[http://www.dantz.com/en/products/win\\_express/index.shtml](http://www.dantz.com/en/products/win_express/index.shtml) (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://h30046.www3.hp.com/subhub.php?jumpid=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、製品を使用する際のヒント、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://h30046.www3.hp.com/subhub.php> (英語サイト) を参照してください。



## 廃止されたソリューション

Desktop Management Task Force (DMTF) は、10年近く前にDesktop Management Interface (DMI) 標準を導入しました。Common Information Model (CIM) などの新しい標準が採用されたため、DMTFはDMIの廃止を進めてきました。HP Client Management Solutions、HP Systems Insight Manager、およびWindows Management Instrumentation (WMI) と呼ばれるCIMのMicrosoftによる実装でのその他の進歩に伴い、2004年1月1日以降に導入されたHPの新しい市販のデスクトップ コンピュータ、ワークステーション、およびノートブック コンピュータにはHP Insight Management Agentが含まれなくなっています。

Insight Management (IM) エージェントは、以下の機能を提供していました。

- DMIサポートにより、Insight Manager 7やその他のDMI準拠の管理アプリケーションでクライアント システムを管理できました。
- Web エージェントにより、Web ブラウザでローカルとリモートの両方でシステムを管理できました。
- 状態の警告をユーザに知らせるときに、ローカルに通知するかまたは中央管理コンソールに送信できました。

Insight Managerは現在、HP Systems Insight Manager Software (HP SIM) に置き換わっています。HP SIMは、WMIを使用してクライアント システムの情報を取得します。Altiris Connector for HP Systems Insight Managerが使用可能であり、これによって、HP SIMコンソールからHP Client Management Solutionsを使用できます。

HP Client Management Solutionsでは現在、ローカルの警告はサポートされていませんが、システム管理コンソールに状態の警告が報告されます。Microsoft WMIは、Windows 2000およびWindows XPでの標準です。WMIによって、Windows OSからシステム管理アプリケーションに、ハードウェア インベントリおよび警告情報が直接提供されます。

## 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ディスクレットが必要です。RomPaqディスクレットは、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ディスクレットに付属の説明を参照してください。



**注意:** コンピュータにセットアップ 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ことを防止できます。コンピュータにセットアップ 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セットアップ 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BIOS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BIOS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BIOS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のモデル番号を入力してください。

## Boot Block Emergency Recovery Mode

Boot Block Emergency Recovery Modeによって、ROMフラッシュに失敗した場合も、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。たとえば、BIOSのアップグレード中に電源の障害が発生すると、ROMフラッシュは完了しないまま終了します。これにより、システムBIOSが使用不可能になります。Boot Block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投入時に有効なシステムBIOSイメージをチェックするコードが含まれています。

- システムBIOSイメージが有効な場合は、コンピュータは通常の方法で起動します。
- システムBIOSイメージが有効でない場合は、Boot Block BIOSによって次に示す十分なサポートが提供されます。
  - BIOSイメージ ファイル用のリムーバブル メディアを検索します。適切なBIOSイメージファイルが見つかり、そのファイルがROMに自動的にフラッシュされます。
  - システムBIOSアップグレードユーティリティを自動的に呼び出す、起動可能なリムーバブル メディアからコンピュータを起動します。

無効なシステムBIOSイメージが検出されると、システム電源ランプが8回赤く点滅します（1秒間に1回の点滅）。同時に、スピーカからビーブ音が8回鳴ります。システムROMの中の、ビデオ オプションROMイメージが含まれている部分が壊れていなければ、画面に「Boot Block Emergency Recovery Mode」と表示されます。

Boot Block Emergency Recovery Modeになったら、以下のように操作して、システムBIOSを復旧（アップグレード）してください。

1. コンピュータの電源を切ります。
2. ルート ディレクトリに目的の BIOS イメージ ファイルが含まれているディスク、CD、またはUSBフラッシュ デバイスを挿入します。このメディアは、FAT12、FAT16、またはFAT32ファイル システムでフォーマットされている必要があります。

3. コンピュータの電源を入れます。

適切なBIOSイメージファイルが見つからない場合、Boot Block BIOSは、起動可能なデバイスからコンピュータを起動しようとします。起動可能なデバイスが見つからない場合は、BIOSイメージ ファイルまたはBIOSアップグレードユーティリティが含まれているメディアを挿入するよう指示されます。

システムBIOSの復旧またはアップグレードが正常に完了すると、システムによって電源が自動的に切られます。

4. BIOSのアップグレードに使用したリムーバブル メディアを取り出します。
5. 電源を入れて、コンピュータを起動しなおします。

## リプリケート セットアップ機能

以下のリプリケートセットアップ機能を使用すれば、管理者がコンピュータの設定情報（コンフィギュレーション情報）を他の同じモデルのコンピュータに簡単にコピーすることができます。この機能によって、複数のコンピュータに同じ設定を行う時間を短縮することができます。



これらの手順を行うには、ディスク ドライブ、またはHP USB メモリなどのサポートされるUSBフラッシュ メディア デバイスが必要です。

## 1台のコンピュータへのコピー



**注意:** 設定情報はモデルにより異なります。コピー元とコピー先のコンピュータが別のモデルの場合、ファイルシステムが破損する恐れがあります。たとえば、dc7xxxシリーズのコンピュータからdx7xxxシリーズのコンピュータに設定情報をコピーしないでください。

1. 設定情報コピー元のコンピュータの電源を切ります。Windows を実行している場合は、[スタート]→[シャットダウン] (または[終了オプション]) →[シャットダウン] (または[電源を切る]) の順に選択します。
2. 設定情報保存用ディスクまたはUSBフラッシュ メディア デバイスをここで挿入します。
3. コンピュータの電源を入れます。
4. コンピュータが起動してモニター ランプが緑色に点灯したらすぐに**[F10]** キーを押し、コンピュータ セットアップ (F10) ユーティリティを実行します。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場合は、コンピュータを再起動して、モニター ランプが緑色に点灯したときにもう一度**[F10]** キーを押します。

5. **[ファイル]** (File) →**[複製セットアップ]** (Replicated Setup) →**[リムーバブルメディアに保存]** (Save to Removable Media) の順に選択します。画面上のメッセージに従って操作し、設定情報ディスクまたはUSBフラッシュ メディア デバイスを作成します。
6. 設定情報コピー先のコンピュータの電源を切り、設定情報ディスクまたはUSBフラッシュ メディア デバイスを挿入します。
7. 設定情報コピー先のコンピュータの電源を入れます。
8. コンピュータが起動してモニター ランプが緑色に点灯したらすぐに**[F10]** キーを押し、コンピュータ セットアップ (F10) ユーティリティを実行します。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。
9. **[ファイル]** →**[複製セットアップ]** →**[システム構成の復元]** (Restore from Removable Media) の順に選択したあと、画面上のメッセージに従って操作します。
10. 設定が完了したら、コンピュータを再起動します。

## 複数のコンピュータへのコピー



**注意:** 設定情報はモデルにより異なります。コピー元とコピー先のコンピュータが別のモデルの場合、ファイルシステムが破損する恐れがあります。たとえば、dc7xxxシリーズのコンピュータからdx7xxxシリーズのコンピュータに設定情報をコピーしないでください。

この手順では設定情報ディスクまたはUSBフラッシュ メディア デバイスの作成に少し時間がかかりますが、設定情報をコピー先のコンピュータにコピーする時間は大幅に短縮されます。



この手順を行うため、また起動可能USBフラッシュ メディア デバイスを作成するためには、起動可能ディスクが必要です。起動可能ディスクを作成するためにWindows XPを使用できない場合は、1台のコンピュータへのコピーの手順を実行してください（18ページの「1台のコンピュータへのコピー」を参照）。

1. 起動可能ディスクまたはUSBフラッシュ メディア デバイスを作成します。20ページの「サポートされるUSBフラッシュ メディア デバイス」または23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」を参照してください。



**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、起動可能ディスクを使用してください。

2. 設定情報コピー元のコンピュータの電源を切ります。Windows を実行している場合は、[スタート]→[シャットダウン]（または[終了オプション]）→[シャットダウン]（または[電源を切る]）の順に選択します。
3. 設定情報保存用ディスクまたはUSBフラッシュ メディア デバイスをここで挿入します。
4. 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てモニター ランプが緑色に点灯したらすぐに[F10]キーを押し、コンピュータ セットアップ (F10) ユーティリティを実行します。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場合は、コンピュータを再起動して、モニタランプが緑色に点灯したときにもう一度**[F10]**キーを押します。

6. [ファイル] (File) →[複製セットアップ] (Replicated Setup) →[リムーバブルメディアに保存] (Save to Removable Media) の順に選択します。画面上のメッセージに従って操作し、設定情報ディスクまたはUSBフラッシュメディア デバイスを作成します。
7. BIOS Utility for Replicated Setup (リブリケートセットアップ用BIOSユーティリティ) をダウンロードして、この中に含まれるrepset.exeファイルを設定情報ディスクまたはUSBフラッシュメディア デバイスにコピーします。このユーティリティを入手するには、[tap://welcome.hp.com/support/files](http://welcome.hp.com/support/files)でコンピュータの製品ファミリーを入力します。
8. 設定情報ディスクまたはUSBフラッシュメディア デバイス上で、次のコマンドを含むautoexec.batファイルを作成します。  
**repset.exe**
9. 設定情報コピー先のコンピュータの電源を切ります。設定情報ディスクまたはUSBフラッシュメディア デバイスを挿入し、コンピュータの電源を入れます。設定ユーティリティが自動的に実行されます。
10. 設定が完了したら、コンピュータを再起動します。

## 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

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。HPおよびコンパックのすべてのUSBフラッシュメディア デバイス、またその他のほとんどのUSBフラッシュメディア デバイスにこ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 (23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)。

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。

- 対応するUSBフラッシュメディア デバイス

- 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)
- USBフラッシュ メディア デバイスから起動可能なコンピュータ



**注意：**一部の古いコンピュータでは、USBフラッシュ メディア デバイスから起動できない場合があります。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。

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に近いドライブが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。

---

[19ページの「複数のコンピュータへのコピー」](#)に戻ります。

## サポートされないUSBフラッシュ メディア デバイス

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。

- USBフラッシュ メディア デバイス
- 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)
- USBフラッシュ メディア デバイスから起動可能なコンピュータ



**注意：**一部の古いコンピュータでは、USBフラッシュ メディア デバイスから起動できない場合があります。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。

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。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てモニター ランプが緑色に点灯したらすぐに**[F10]**キーを押し、コンピュータ セットアップ (F10) ユーティリティを実行します。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場合は、コンピュータを再起動して、モニター ランプが緑色に点灯したときにもう一度**[F10]**キーを押します。

6. **[カスタム]** (Advanced) → **[PCIデバイス]** (PCI Devices) の順に選択して PATAおよびSATAコントローラを無効にします。SATAコントローラを無効にするとき、コントローラに割り当てられているIRQを書き留めておきます。後で再びIRQを割り当てる必要があります。変更を確定して、セットアップユーティリティを終了します。

SATA IRQ : \_\_\_\_\_

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てモニタ ランプが緑色に点灯したらすぐに**[F10]**キーを押し、コンピュータ セットアップ (F10) ユーティリティを実行します。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. **[カスタム]**→**[PCIデバイス]**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。SATAコントローラを元のIRQに割り当てなおします。
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 and Diagnostics CD (ドキュメンテーションおよび診断用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。

[19ページの「複数のコンピュータへのコピー」](#)に戻ります。

## 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 Manager、HP Client Manager、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 Embedded Security for ProtectTools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、[www.hp.com/jp](http://www.hp.com/jp)から入手できる、『HP ProtectToolsセキュリティ マネージャ 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HP Embedded Security for ProtectTools、スマートカバー センサ/カバー リムーバル センサ (Cover Removal Sensor)、およびスマートカバー ロック (Smart Cover Lock) 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、メモリ脱着センサおよびスマートカバー センサ/カバー リムーバル センサからの警告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。





HP Embedded Security for ProtectTools、スマートカバー センサ/カバー リムーバル センサ、およびスマートカバー ロックは、一部のシステムにオプションとして装備されています。

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 and Diagnostics 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
セットアップ パスワード (Setup Password)	<p>セットアップ (管理者) パスワードを設定して有効にします</p> <p> セットアップ 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セットアップ パスワードが必要になります</p> <p>詳しくは、Documentation and Diagnostics 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>
電源投入時パスワード (Power-On Password)	<p>電源投入時パスワードを設定して有効にします</p> <p>詳しくは、Documentation and Diagnostics 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>
パスワード オプション (Password Options) (電源投入時パスワードが設定されている場合にのみ表示されます)	<p>ウォーム ブート (<b>[Ctrl]+[Alt]+[Delete]</b>) にパスワードが必要かどうかを指定します</p> <p>詳しくは、Documentation and Diagnostics 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</p>
起動前の承認 (Pre-Boot Authorization)	<p>電源投入時パスワード (Power-On Password) の代わりにスマート カードを使用することを有効/無効にします</p>
	<p>コンピュータ セットアップについて詳しくは、Documentation and Diagnostics 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
スマート カバー (Smart Cover)	<p>次の項目を設定します</p> <ul style="list-style-type: none"> <li>• カバー ロック (Cover Lock) の有効 (Enable) / 無効 (Disable) の設定</li> <li>• カバー リムーバル センサの有効/無効の設定</li> </ul> <p> [ユーザに通知]を設定すると、カバーが取り外されたことをセンサが検知したときにユーザに通知されます。セットアップ パスワードは、カバーが取り外されたことをセンサが検知した場合、コンピュータを起動する際にセットアップ パスワードの入力を要求します</p> <p>一部のモデルでのみサポートされます。詳しくは、Documentation and Diagnostics 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</p>
内蔵セキュリティ (Embedded Security)	<p>次の項目を設定します</p> <ul style="list-style-type: none"> <li>• 内蔵セキュリティ デバイスの有効 (Enable) / 無効 (Disable)</li> <li>• デバイスの出荷時設定へのリセット</li> </ul> <p>一部のモデルでのみサポートされます。詳しくは、<a href="http://www.hp.com/jp">www.hp.com/jp</a>から入手できる『HP ProtectToolsセキュリティ マネージャ 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)、モデルによってはネットワーク コントローラ (Network Controller)、マルチベイ デバイス (Multibay Devices)、およびSCSIコントローラ (SCSI 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 and Diagnostics 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
<p>ネットワーク サービス ブート (Network Service Boot)</p>	<p>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 (LANボード) が搭載されている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)</p>
<p>システムID (System ID)</p>	<p>次の項目を設定します</p> <ul style="list-style-type: none"> <li>• 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 詳しくは、Documentation and Diagnostics 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</li> <li>• 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)</li> <li>• 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</li> </ul>
<p>ドライブロック (DriveLock) (一部のモデルのみ)</p>	<p>ATAハードディスク ドライブにマスタ パスワードまたはユーザ パスワードを割り当てたり、パスワードを変更したりします。この機能が有効の場合は、POST実行中にどちらかのDriveLockパスワードを入力するよう求められます。どちらのパスワードも正常に入力されなかった場合は、次のワールド ブート シーケンスの間にどちらかのパスワードが入力されるまで、ハードディスク ドライブにはアクセスできません</p> <p> この項目は、ATA Securityコマンド セットをサポート するATAハードディスク ドライブが少なくとも1台システムに接続されている場合にのみ表示されます</p> <p>詳しくは、Documentation and Diagnostics 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</p>
<p> コンピュータ セットアップについて詳しくは、Documentation and Diagnostics 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。</p>	<p>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

電源投入時パスワード (Power-on 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。セットアップパスワード (Setup 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。セットアップパスワードを、電源投入時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、電源投入時パスワードの入力を要求されたときに、代わりにセットアップ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セットアップ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、設定されている電源投入時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。

## セットアップパスワードの設定

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、[www.hp.com/jp](http://www.hp.com/jp)から入手できる『HP ProtectToolsセキュリティ マネージャ 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、セットアップ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てモニタ ランプが緑色に点灯したらすぐに[F10]キーを押し、コンピュータ セットアップ (F10) ユーティリティを実行します。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場合は、コンピュータを再起動して、モニタ ランプが緑色に点灯したときにもう一度[F10]キーを押します。

3. [セキュリティ] (Security) →[セットアップパスワード] (Setup Password) の順に選択したあと、画面上のメッセージに従って操作します。

4. 設定を終了するには、[ファイル] (File) →[変更を保存して終了] (Save Changes and Exit) の順に選択します。

## 電源投入時パスワードの設定

[コンピュータ セットアップ ユーティリティ]メニューで、電源投入時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。電源投入時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てモニター ランプが緑色に点灯したらすぐに[F10]キーを押し、コンピュータ セットアップ (F10) ユーティリティを実行します。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場合は、コンピュータを再起動して、モニター ランプが緑色に点灯したときにもう一度[F10]キーを押します。

3. [セキュリティ]→[電源投入時パスワード] (Power-On Password) の順に選択したあと、画面上のメッセージに従って操作します。
4. 設定を終了するには、[ファイル] (File) →[変更を保存して終了] (Save Changes and Exit) の順に選択します。

## 電源投入時パスワードの入力

電源投入時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. 鍵形のアイコンが表示されたら、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、鍵形に×印のついたアイコン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。

## セットアップ 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、[www.hp.com/jp](http://www.hp.com/jp)から入手できる『HP ProtectToolsセキュリティ マネージャ ガイド』を参照してください。

コンピュータでセットアップ 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てモニター ランプが緑色に点灯したらすぐに[F10]キーを押し、コンピュータ セットアップ (F10) ユーティリティを実行します。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場合は、コンピュータを再起動して、モニター ランプが緑色に点灯したときにもう一度[F10]キーを押します。

3. 鍵形のアイコンが表示されたら、セットアップ 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、鍵形に×印のついたアイコン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。

## 電源投入時パスワードまたはセットアップ 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、[www.hp.com/jp](http://www.hp.com/jp)から入手できる『HP ProtectToolsセキュリティ マネージャ 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. 電源投入時パスワードを変更する場合は、手順3に進みます。

セットアップパスワードを変更する場合は、コンピュータが起動してモニターランプが緑色に点灯したらすぐに**[F10]**キーを押し、コンピュータセットアップ (F10) ユーティリティを実行します。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場合は、コンピュータを再起動して、モニターランプが緑色に点灯したときにもう一度**[F10]**キーを押します。

3. 鍵形のアイコンが表示されたら、次のように入力します。

### 現在のパスワード/新しいパスワード/新しいパスワード



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。

4. **[Enter]**キーを押します。

新しいパスワードは、次にコンピュータの電源を入れたときから有効になります。



電源投入時パスワードとセットアップパスワードは、コンピュータセットアップ (F10) ユーティリティの**[セキュリティ]** (Security) オプションを使って変更することもできます。

## 電源投入時パスワードまたはセットアップ パスワードの削除

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、[www.hp.com/jp](http://www.hp.com/jp)から入手できる『HP ProtectToolsセキュリティ マネージャ 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. 電源投入時パスワードを削除する場合は、手順3に進みます。

セットアップパスワードを削除する場合は、コンピュータが起動してモニターランプが緑色に点灯したらすぐに**[F10]**キーを押し、コンピュータ セットアップ (F10) ユーティリティを実行します。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場合は、コンピュータを再起動して、モニターランプが緑色に点灯したときにもう一度**[F10]**キーを押します。

3. 鍵形のアイコンが表示されたら、次のように入力します。

### 現在のパスワード /

4. **[Enter]**キーを押します。



電源投入時パスワードとセットアップパスワードは、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]** (Security) オプションを使って変更することもできます。

## 電源投入時パスワードを忘れてしまった場合

設定しておいた電源投入時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 and Diagnostics 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、[www.hp.com/jp](http://www.hp.com/jp)から入手できる『HP ProtectToolsセキュリティ マネージャ ガイド』を参照してください。

## ドライブロック (DriveLock)

ドライブロックは、ATAハードディスク ドライブにあるデータへの不正アクセスを防止する業界標準のセキュリティ機能であり、コンピュータ セットアップ (F10) ユーティリティの拡張機能として実装されています。この機能は、ATA Securityコマンドセットに対応するハードディスク ドライブが検出された場合にのみ利用できます。ドライブロックは、データのセキュリティを最重要視するユーザ向けに開発されました。このようなユーザにとっては、ハードディスク ドライブのコストとそこに格納されているデータの喪失は、データへの不正アクセスの結果生じる可能性のある損害に比べれば、些細なものです。このレベルのセキュリティの確保と同時に、パスワードを忘れたときの対処もできるように、HPが実装したドライブロックでは、2つのパスワードによるセキュリティ方式を採用しています。一方のパスワードはシステム管理者が設定して使用するもので、もう一方のパスワードは通常、エンドユーザが設定して使用します。両方のパスワードを忘れてしまった場合にドライブをアンロックするための手段はありません。したがって、ハードディスク ドライブに含まれるデータが企業情報システムに複製されているか、または定期的にバックアップが作成されている場合に、ドライブロックを最も安全に使用できます。ドライブロックの両方のパスワードを忘れてしまった場合は、ハードディスク ドライブを使用できなくなります。前に述べたカスタマ プロファイルに適合しないすべてのユーザにとって、この事実は受け入れ難いリスクになる可能性があります。一方、カスタマ プロファイルに適合するユーザにとっては、ハードディスク ドライブに保存されたデータの性質上、許容できるリスクだと言えます。

## ドライブロックの使用法

[ドライブロック] (DriveLock) オプションは、コンピュータ セットアップ (F10) ユーティリティの[セキュリティ] (Security) メニューに表示されます。ユーザには、マスタ パスワード (master password) を設定したりドライブロックを有効にしたりするオプションが提供されます。ドライブロックを有効にするには、ユーザ パスワード (user password) を入力する必要があります。通常、ドライブロックの最初のコンフィギュレーションはシステム管理者が実行するので、マスタ パスワードを最初に設定する必要があります。ドライブロックを有効にするか無効のままにしておくかにかかわらず、管理者はマスタ パスワードを設定することをおすすめします。これにより、将来ドライブがロックされた場合に、管理者はドライブロックの設定値を変更できるようになります。マスタ パスワードが設定されると、システム管理者はいつでもドライブロックを有効にしたり無効にしたりすることができます。

ロックされたハードディスク ドライブが存在する場合は、POST (Power-On Self Test) によって、そのドライブをアンロックするためのパスワードが要求されます。電源投入時パスワード (power-on password) が設定されていて、そのドライブのユーザ パスワードと一致する場合は、パスワードの再入力が必要されません。一致しない場合は、ドライブロックのパスワードを入力するよう要求されます。マスタ パスワードとユーザ パスワードのどちらも使うことができます。ユーザは、パスワードが正しいと認識されるまで、2回入力できます。2回とも受け入れられない場合でもPOSTは続行されますが、そのドライブにはアクセスできません。



## ドライブロックの使用例

ドライブロックのセキュリティ機能は、企業環境での使用に最も適しています。システム管理者はハードディスク ドライブのコンフィギュレーションを担当しますが、その作業には、ドライブロックのマスタ パスワードを設定することが含まれます。ユーザがユーザ パスワードを忘れた場合や、コンピュータを別の従業員が使うことになった場合、システム管理者はマスタ パスワードを使用して、ユーザ パスワードをリセットしたり、ハードディスク ドライブへのアクセス権を回復したりすることができます。

企業システム管理者は、ドライブロックを有効にする場合、マスタ パスワードの設定とメンテナンスについての企業方針を確立しておくことをおすすめします。これは、従業員が会社を辞める前に意図的に、または誤ってドライブロックの両方のパスワードを設定してしまうという状況を防ぐために必要です。両方のパスワードを設定した従業員が会社を辞めてしまった場合、そのハードディスク ドライブは使用不能となり、交換が必要になります。また、マスタ パスワードが設定されていないと、システム管理者がロックされたハードディスク ドライブにアクセスできなくなり、不正ソフトウェアの日常チェックや、その他の資産管理およびサポートを実行できなくなることがあります。

それほど厳重なセキュリティを必要としないユーザの場合は、ドライブロックを有効にしないことをおすすめします。この種のユーザには、個人ユーザや、機密性の高いデータをハードディスク ドライブに保持しないことを習慣にしているユーザが含まれます。このようなユーザにとっては、両方のパスワードを忘れてハードディスク ドライブが使えなくなることのほうが、ドライブロックにより保護されるデータの価値よりもはるかに大きな問題と言えます。コンピュータ セットアップ (F10) ユーティリティとドライブロックへのアクセスは、セットアップ パスワードによって制限できます。セットアップ パスワードを指定してそれをエンドユーザに公表しないことで、システム管理者はユーザがドライブロックを有効にできないようにします。

## スマート カバー センサ/カバー リムーバル センサ (Cover Removal Sensor)

一部のモデルに搭載されているスマート カバー センサ/カバー リムーバル センサとは、本体のカバーまたはサイド パネルの着脱があったことをユーザーに知らせる、ハードウェア技術とソフトウェア技術を結合した機能です。3段階の設定レベルがあり、本体のカバーの着脱があった後で初めてコンピュータの電源を入れたときの動作が異なります。

### スマート カバー センサ/カバー リムーバル センサの動作

レベル	設定	コンピュータ起動時の動作
0	[無効] (Disabled)	スマート カバー センサ/カバー リムーバル センサは無効 (デフォルト)
1	[ユーザーに通知] (Notify User)	本体のカバーが取り外されたことを知らせるメッセージが画面に表示される
2	[セットアップ パスワード] (Setup Password)	本体のカバーが取り外されたことを知らせるメッセージが画面に表示される セットアップ パスワードを入力するまで、コンピュータを使用できない



これらの設定は、コンピュータ セットアップを使用して変更できます。コンピュータ セットアップについて詳しくは、Documentation and Diagnostics 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。

## スマート カバー センサ/カバー リムーバル センサ (Cover Removal Sensor) の保護レベルの設定

スマート カバー センサ/カバー リムーバル センサ機能を有効に設定するには、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てモニター ランプが緑色に点灯したらすぐに[F10]キーを押し、コンピュータ セットアップ (F10) ユーティリティを実行します。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場合は、コンピュータを再起動して、モニター ランプが緑色に点灯したときにもう一度[F10]キーを押します。

3. [セキュリティ] (Security) →[スマート カバー] (Smart Cover) →[カバー リムーバル センサ] (Cover Removal Sensor) の順に選択した後、必要なセキュリティ レベルを選択します。
4. 設定を終了するには、[ファイル] (File) →[変更を保存して終了] (Save Changes and Exit) の順に選択します。

## スマート カバー ロック

スマート カバー ロックは、コンピュータのカバーのロックをソフトウェアで制御する、一部のHPのコンピュータでサポートされる機能です。スマート カバー ロックを使用して、コンピュータ内部の装置への不正なアクセスを防ぎます。工場出荷時には、ロックが解除された状態になっています。



**注意:** スマート カバー ロックを使用する場合は、必ずセットアップ パスワードを設定して、無断でロックを解除できないようにしておいてください。



スマート カバー ロックは、一部のシステムにオプションとして装備されています。

## スマート カバー ロックの設定

スマート カバー ロックを使ってコンピュータ本体のカバーをロックするには、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てモニター ランプが緑色に点灯したらすぐに[F10]キーを押し、コンピュータ セットアップ (F10) ユーティリティを実行します。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場合は、コンピュータを再起動して、モニター ランプが緑色に点灯したときにもう一度[F10]キーを押します。

3. [セキュリティ] (Security) →[スマート カバー] (Smart Cover) →[カバー ロック] (Cover Lock) →[ロック] (Lock) の順に選択します。
4. 設定を終了するには、[ファイル] (File) →[変更を保存して終了] (Save Changes and Exit) の順に選択します。

## スマート カバー ロックの解除

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てモニター ランプが緑色に点灯したらすぐに[F10]キーを押し、コンピュータ セットアップ (F10) ユーティリティを実行します。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場合は、コンピュータを再起動して、モニター ランプが緑色に点灯したときにもう一度[F10]キーを押します。

3. [セキュリティ]→[スマート カバー]→[カバー ロック]→[アンロック] (Unlock) の順に選択します。
4. 設定を終了するには、[ファイル]→[変更を保存して終了]の順に選択します。

## Smart Cover FailSafeキーの使用

スマート カバー ロックを使ってコンピュータをロックしたまま、パスワードを入力できなくなってしまった場合、Smart Cover FailSafeキーを使用して、コンピュータ本体のカバーを開ける必要があります。Smart Cover FailSafeキーが必要となるのは、次のような場合です。

- 停電
- 起動障害
- コンピュータ部品（プロセッサや電源など）の障害
- パスワードを忘れてしまった場合



---

**注意：** Smart Cover FailSafeキーは、HPが提供する専用ツールです。必要になる前に、HP製品販売店であらかじめご用意いただくことをおすすめします。

---

Smart Cover FailSafeキーの入手については、HPのサポート窓口にお問い合わせください。

Smart Cover FailSafeキーについて詳しくは、Documentation and Diagnostics 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。

## 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 and Diagnostics 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。

## 指紋認証テクノロジー

HP 指紋認証テクノロジーを使用すると、エンドユーザーのパスワードの入力が不要となるため、ネットワークのセキュリティを強化する一方で、ログイン手順を簡素化し、企業のネットワーク管理に関わる経費を削減することができます。また、手頃な価格のため、もはや一部のハイテク産業や高度なセキュリティを扱う組織や企業だけのものではなくなりました。



モデルによっては、指紋認証テクノロジーがサポートされていない場合があります。

詳しくは、次のWebサイト（英語サイト）を参照してください。

<http://h18004.www1.hp.com/products/security/>

## 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 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。

## ドライブ保護システム

ドライブ保護システム (DPS) は、一部のモデルに搭載されたハードディスクドライブに組み込まれている診断ツールです。DPSを使用して、保証規定が適用されない、ハードディスクドライブの交換に至るような問題を診断します。

コンピュータの組み立て時に各ハードディスクドライブに対してDPSテストが実行され、主要な情報がハードディスクドライブに書き込まれます。この情報は半永久的に記録されます。DPSが実行されるたびに、テストの結果がハードディスクドライブに書き込まれます。DPSの使用手順については、Documentation and Diagnostics 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。

## 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

<b>A</b>			
Altiris	7	Smart Cover FailSafeキー、入手	42
AClient	3	Subscriber's Choice	13
Deployment Solution Agent	3		
<b>D</b>		<b>U</b>	
Dantz Retrospect Express	11	URL (Webサイト)	
		「Webサイト」を参照	
<b>F</b>		USBフラッシュ メディア デバイス、起動可能	20~25
FailSafeキー			
注意	42	<b>W</b>	
入手	42	Webサイト	
FailSafeキーの入手	42	HPQFlash	16
<b>H</b>		Proactive Change Notification	13
HP Client Management Solutions	7	ROMフラッシュ	15
HP Client Manager Software	6	Subscriber's Choice	13
HP Local Recovery	10	コンピュータの導入	2
HP OpenView Management Suite for Desktops Using		指紋認証テクノロジー	43
Radia	9	ソフトウェアのサポート	26
HP System Software Manager	5	リプリケート セットアップ機能	20
HP USBメモリ		リモートROMフラッシュ	16
起動可能	20~25	<b>あ</b>	
HPライフサイクル ソリューション	2	インターネットアドレス	
		「Webサイト」を参照	
<b>L</b>		オペレーティング システム、重要な情報	26
Local Recovery	3	オペレーティング システムの変更、重要な情報	26
<b>P</b>			
PCN (Proactive Change Notification)	13	温度、コンピュータ内部	44
Preboot Execution Environment (PXE)	4	温度センサ機能	44
Proactive Change Notification (PCN)	13	<b>か</b>	
PXE (Preboot Execution Environment)	4	カバー ロック、スマート	40
<b>R</b>		カバー ロックのセキュリティ、注意	40
ROM		起動可能デバイス	
フラッシュ	15	HP USBメモリ	20~25
リモートフラッシュ	15	USBフラッシュ メディア デバイス	20~25
ROMの保護、注意	15	作成	20~24
		ケーブル ロックの取り付け	42



コンピュータ セットアップ (F10) ユーティリティ		統合	2
ティ	17	ドライブ保護システム	44
コンピュータ内部の温度	44	復旧	2
コンピュータの導入	2	リモートROMフラッシュ	15
コンピュータへのアクセスの制御	27	リモートシステムインストール	4
		ソフトウェアのカスタマイズ	2
<b>さ</b>		<b>た</b>	
資産情報管理機能	27	耐サージ機能付連続供給電源装置	44
指紋認証テクノロジー	43	注意	
出荷時の設定	2	FailSafeキー	42
障害通知	43	ROMの保護	15
スマート カバー センサ/カバー リムーバル センサ	39	カバー ロックのセキュリティ	40
設定	40	ディスク、複製	2
保護レベル	39	デュアル ステート電源ボタン	25
スマート カバー ロック	40~42	電源供給、耐サージ機能	44
解除	41	電源投入時パスワード	
設定	41	削除	35
スマート カバー ロックの解除	41	入力	32
スマート カバー ロックの設定	41	変更	34
セキュリティ		電源ボタン	
機能、表	28	設定	25
スマート カバー センサ/カバー リムーバル センサ	39	デュアル ステート	25
スマート カバー ロック	40~42	電源ボタンの設定	25
設定	27	導入用ツール、ソフトウェア	2
ドライブロック	36~38	ドライブ、保護	44
パスワード	31	ドライブロック	36~38
マルチベイ	36~38	<b>な</b>	
セットアップ		入力	
初期設定	2	セットアップ パスワード	33
リブリケート機能	17	電源投入時パスワード	32
セットアップ パスワード		<b>は</b>	
削除	35	ハードディスク ドライブ診断ツール	44
設定	31	ハードディスク ドライブの保護	44
入力	33	廃止されたソリューション	14
変更	34	パスワード	
ソフトウェア		解除	35
Altiris AClient	3	削除	35
Altiris Deployment Solution Agent	3	セキュリティ	31
HP Local Recovery	3	セットアップ	31, 33
アップデートと管理	5	電源投入時	32
コンピュータ セットアップ (F10) ユーティリティ		変更	34
リティ	17	パスワードの解除	35
資産情報管理機能	27	パスワードの削除	35
障害通知および復旧機能	43	パスワードの変更	34

---

複製用ツール、ソフトウェア	2	<b>ら</b>	
復旧、ソフトウェア	2	リモートROMフラッシュ	15
プリインストールされたソフトウェア イメージ	2	リモート システム インストール	4
変更通知	13	アクセス	4
<b>ま</b>		リモート セットアップ	4
マルチペイのセキュリティ	36～38		