



HP ProtectTools for Small Business セ キュリティ ソフトウェア バージョン 5. 10

ユーザー ガイド

© 2010 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、Windows および Windows Vista は米国またはその他の国における Microsoft Corporation 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限定的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。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。

HP ProtectTools for Small Business セキュリティ ソフトウェア バージョン 5.10 ユーザー ガイド

HP Business PC

改訂第 1 版：2010 年 5 月

製品番号：610663-292

このガイドについて

このガイドでは、HP ProtectTools for Small Business セキュリティ ソフトウェアに関する情報を提供します。

- △ **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おそ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おそれがあるという注意事項を表します。
 - ☞ **注記：** 重要な補足情報です。
-

目次

1 セキュリティの概要	1
HP ProtectTools の機能	2
2 最も役立つオプションのための Easy Setup Guide	4
お使いになる前に	4
Credential Manager for HP ProtectTools (パスワード マネージャー)	6
Credential Manager に保存されている認証の表示および管理	8
File Sanitizer for HP ProtectTools	11
Device Access Manager for HP ProtectTools	14
Drive Encryption for HP ProtectTools	16
3 HP ProtectTools for Small Business の利点	18
HP ProtectTools for Small Business セキュリティ ソフトウェアへのアクセス	18
主なセキュリティの目的の実現	18
機密データへのアクセス制限	18
内部または外部の場所からの不正なアクセスの防止	19
強力なパスワード ポリシーの作成	19
その他のセキュリティ対策	19
セキュリティの役割の割り当て	19
HP ProtectTools のパスワードの管理	20
安全なパスワードの作成	20
証明情報および設定のバックアップ	21
4 HP ProtectTools Security Manager 管理者コンソール	22
HP ProtectTools 管理者コンソールについて	22
管理者コンソールの使用	22
セットアップ ウィザードの使用開始準備	23
システムの設定	23
セキュリティ機能の有効化	24
Security Manager 認証ポリシーの定義	24
[ログオン]タブ	24
[セッション]タブ	25
設定の定義	25

ユーザーの管理	25
ユーザーの追加	25
ユーザーの削除	26
ユーザーの状態の確認	26
アプリケーションの設定の構成	26
ドライブの暗号化	27
デバイス アクセスの管理	27
5 HP ProtectTools Security Manager (HP ProtectTools セキュリティ マネージャー)	28
パスワードの管理	28
証明情報の設定	28
Windows パスワードの変更	29
ファイルのシュレッドまたはブリーチ	29
ドライブの暗号化の状態の表示	29
デバイス アクセスの表示	29
アプリケーションの追加	30
設定のオプション	30
バックアップおよび復元	30
データのバックアップ	31
データの復元	31
Windows のユーザー名および画像の変更	32
6 Drive Encryption for HP ProtectTools	33
セットアップ手順	34
Drive Encryption を開く	34
一般的なタスク	34
Drive Encryption の有効化	34
Drive Encryption の無効化	34
Drive Encryption の有効化後のログイン	34
高度なタスク	34
Drive Encryption の管理 (管理者のタスク)	34
個々のドライブの暗号化または暗号化の解除	35
バックアップおよび復元 (管理者のタスク)	35
バックアップ キーの作成	35
7 Credential Manager for HP ProtectTools (パスワード マネージャー)	36
ログオン情報の追加	37
ログオン情報の編集	38
ログオン メニューの使用	38
ログオン情報をカテゴリ別に整理	38
ログオン情報の管理	39
パスワード強度の評価	39

[パスワード マネージャー]アイコンの設定	40
8 File Sanitizer for HP ProtectTools	41
セットアップ手順	42
File Sanitizer の起動	42
空き領域ブリーチのスケジュール設定	42
シュレッド スケジュールの設定	43
シュレッド プロファイルの選択または作成	43
あらかじめ定義されているシュレッド プロファイルの選択	43
高度にセキュリティ設定されたシュレッド プロファイルのカスタマイズ	44
シンプル削除プロファイルのカスタマイズ	44
一般的なタスク	45
キーの組み合わせによるシュレッドの開始	45
[File Sanitizer]アイコンの使用	46
単一のファイルやフォルダーの手動シュレッド	46
選択されているすべてのファイルやフォルダーの手動シュレッド	46
空き領域ブリーチの手動実行	47
シュレッド操作または空き領域ブリーチ操作の停止	47
ログ ファイルの表示	47
9 Device Access Manager for HP ProtectTools	48
バックグラウンド サービスの開始	48
簡易構成	48
デバイス クラス構成（詳細設定）	49
ユーザーまたはグループの追加	49
ユーザーまたはグループの削除	49
ユーザーまたはグループのアクセス拒否または許可	50
ユーザー アクセス設定（詳細設定）	51
ユーザーまたはグループの追加	51
ユーザーまたはグループの削除	51
アクセスの許可または拒否	51
用語集	53
索引	55

1 セキュリティの概要

HP は、お客様の時間がきわめて貴重であり、お客様が PC やデータ、およびビジネスを守るための適切なセキュリティ ソフトウェアについて心配するよりも、ビジネスの運営や成長に集中する必要があることを理解しています。

使いやすいだけでなく、ビジネス資産に対する強力な保護を提供するセキュリティ ソリューションを予防的に検討することが重要です。セキュリティは「あるとよいもの」ではなく、「必須事項」です。

HP は、容易に実装でき、しかも簡単に使える、HP ProtectTools for Small Business と呼ばれる保護機能を提供しています。

HP ProtectTools for Small Business は、コンピューターおよび重要なデータを不正なアクセスから保護するために役立つ機能を提供するセキュリティ ソフトウェアです。さまざまな HP ProtectTools ソフトウェア モジュールによって、高度なセキュリティ機能が提供されます。

HP ProtectTools for Small Business では、2 つのバージョンを利用できます。HP ProtectTools Security Manager 管理者コンソールおよび HP ProtectTools Security Manager (一般ユーザー用) です。管理者用バージョンもユーザー用バージョンも、[スタート]→[すべてのプログラム]メニューから利用できます。

バージョン	機能
HP ProtectTools Security Manager 管理者コンソール	<ul style="list-style-type: none">• アクセスするには、Microsoft® Windows®システム管理者のアクセス権が必要です• 各モジュールへのアクセスは管理者が設定するものであるため、一般ユーザーは使用できません• すべてのユーザー用の初期セキュリティを設定したり、オプションや必須要件を構成したりできます
HP ProtectTools Security Manager (一般ユーザー用)	<ul style="list-style-type: none">• 管理者によって提供されたオプションをユーザーが構成できません• アクセスを制限して、一部の HP ProtectTools モジュールの限られた調整機能しかユーザーが使用できないようにすることができます

HP ProtectTools ソフトウェア モジュールは、プリインストールまたはプリロードされている場合と、設定可能なオプションまたは製品購入後のオプションとして導入できる場合があります。詳しくは、<http://www.hp.com/jp/>を参照してください。

HP ProtectTools の機能

以下の表で、HP ProtectTools for Small Business モジュールの主な機能を詳しく説明します。

モジュール	主な機能
HP ProtectTools Security Manager 管理者コンソール	<ul style="list-style-type: none">• Security Manager のセットアップ ウィザードは、セキュリティ レベルおよびセキュリティ ログイン方法をセットアップしたり設定したりするために管理者が使用します• 基本ユーザーからは非表示になっているオプションを設定します• Device Access Manager の設定およびユーザー アクセスを設定します• 管理者ツールは、HP ProtectTools ユーザーの追加と削除、およびユーザーの状態の表示に使用します
HP ProtectTools Security Manager (一般ユーザー)	<ul style="list-style-type: none">• ユーザー名およびパスワードを構成、設定、および変更します• Windows パスワードやスマート カードなどの、ユーザーの証明情報を設定および変更します• File Sanitizer のシュレッド、ブリーチ、および設定を構成および変更します• Device Access Manager の設定を表示します• [設定]オプションや[バックアップおよび復元]オプションを設定します
Credential Manager for HP ProtectTools (パスワード マネージャー)	<ul style="list-style-type: none">• ユーザー名とパスワードを保存、構成、および保護するように設計されています• Web サイトおよびプログラムにすばやく安全にアクセスできるように、ログオン画面を設定できます• さまざまな Web サイトにアクセスするときにユーザー名とパスワードを保存したい場合は、ユーザー名とパスワードをパスワード マネージャーに入力しておけば、再び思い出す必要がなくなります。次回そのサイトにアクセスしたときは、パスワード マネージャーが自動的にこのデータを入力して送信します• 書き留めておいたり覚えておいたりする必要がない強固なパスワードを作成して、アカウントをより安全にすることができます
Drive Encryption for HP ProtectTools	<ul style="list-style-type: none">• ボリューム全体にわたる完全なハードディスク ドライブの暗号化が可能です• ハードディスク ドライブ上のデータの暗号化解除やデータへのアクセスにブート前認証が使用されます• 法的または業界での要件を満たして機密データを保護するために役立ちます• ハードディスク ドライブ全体を暗号化することによって不正なアクセスからデータを保護します。 コンピューターが盗まれ、ドライブが元のシステムから取り外されて異なるシステムに接続されたとしても、データは危険にさらされません

モジュール	主な機能
File Sanitizer for HP ProtectTools	<ul style="list-style-type: none"> Windows でデータを削除しても、その内容がハードディスク ドライブから完全に削除されるわけではありません。Windows はデータの参照情報のみを削除します。別のファイルによってハードディスク ドライブ上のその同じ領域が新しい情報で書き込まれるまで、データはハードディスク ドライブに引き続き残ったままとなります。ただし、File Sanitizer を使用すると、ドキュメント、Web ブラウザーの履歴、一時ファイルなどを完全に、かつ自動的に消去できます コンピューター上の重要なファイルやフォルダー（個人情報や個人ファイル、履歴データや Web 関連データ、その他のデータコンポーネント）を安全に消去（またはシュレッド）したり、ハードディスク ドライブを定期的にブリーチ（以前に削除されたデータを書き直すこと）したりできます
Device Access Manager for HP ProtectTools	<ul style="list-style-type: none"> ユーザー プロファイルに基づいて、メディア ドライブ、USB、その他のハードウェア デバイスへのアクセスを制御するために使用できます 重要なデータを保存するユーザーの機能を制限できます ユーザーが、PC またはネットワークからデータをコピーできないようにするために、個人用音楽プレーヤーなどの外付けの記憶装置を使用できないようにします ユーザーが外部のメディアからシステムにウィルスを侵入させることができないようにします ユーザーまたはユーザーのグループごとに、デバイスのグループ（USB キー、書き込み可能なデバイス、個人用音楽プレーヤーなど）を個別に無効にできます。管理者パスワードを持つユーザーはログオンして PC から情報をコピーできますが、他のユーザーはできません

2 最も役立つオプションのための Easy Setup Guide

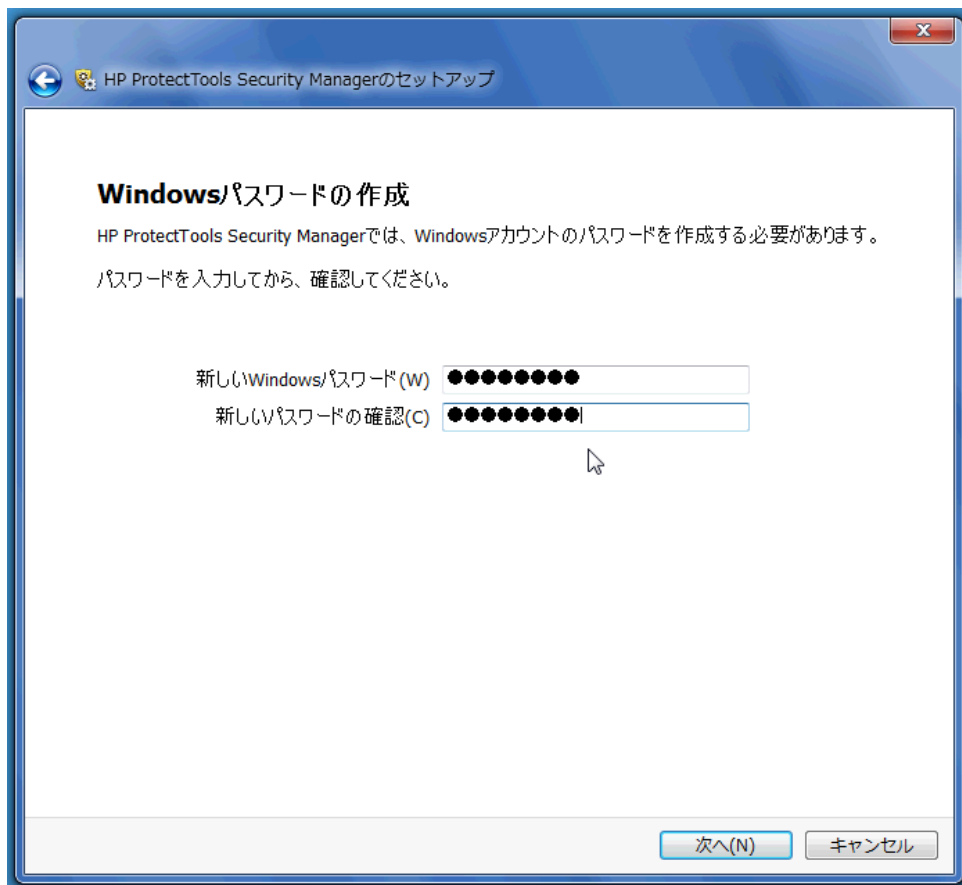
この Easy Setup Guide は、HP ProtectTools for Small Business 内の最も一般的で、かつ最も役立つオプションを有効にするための基本的な手順を示すように設計されています。このソフトウェアには、設定を微調整したり、アクセス制御を設定したりするために使用できる多数のツールやオプションが含まれています。Easy Setup Guide は、各モジュールを最小限の設定作業および時間で動作させることに重点を置いています。詳細情報を表示するには、単に対象のモジュールを選択し、右上隅にある「?」または[ヘルプ]ボタンをクリックします。このボタンによって、現在表示されているウィンドウでの作業に役立つ情報が自動的に表示されます。

お使いになる前に


1. [ガジェット]アイコンまたはタスク バーにあるアイコン（金色の盾）から HP ProtectTools Security Manager を開くか、または[スタート]→[すべてのプログラム]→[HP]の順にクリックします。



2. Windows パスワードを入力するか、または Windows パスワードを作成します。

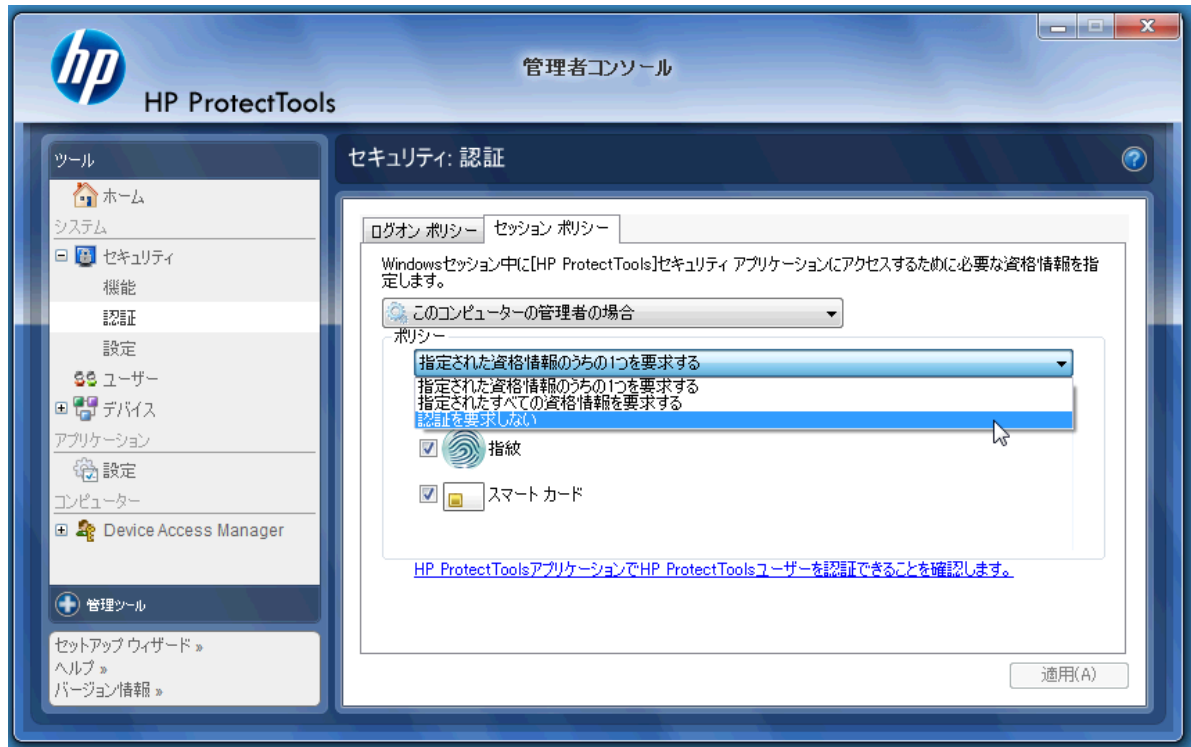


3. セットアップ ウィザードを完了します。

 **注記：** 初期設定では、HP ProtectTools Security Manager は強力な認証ポリシーに設定されています。

この設定は、Windows にログインしている間の不正なアクセスを防止するために設計されており、高いセキュリティ レベルが必要な場合や、ユーザーが 1 日を通して頻繁にシステムから離れている場合に使用されます。この設定を変更する場合は、[セッション ポリシー] タブをクリックし、選択を行います。

セッション全体にわたって最初の Windows ログインのみを使用するように HP ProtectTools Security Manager を設定するには、以下の設定を変更します。



Windows ログイン中に HP ProtectTools Security Manager によって 1 回のみ認証されるようにするには、以下の操作を行います。

1. [スタート]→[すべてのプログラム]→[HP]→[HP ProtectTools 管理者コンソール]の順にクリックします。
2. 左側の[ツール]パネルで、[セキュリティ]グループから[認証]を選択します。
3. [セッション ポリシー]タブをクリックし、[ポリシー]の下のドロップダウン メニューから[認証を要求しない]を選択します。
4. 完了したら、[適用]ボタンをクリックします。

Credential Manager for HP ProtectTools (パスワード マネージャー)

Web サイトに定期的にアクセスする場合や、ログインが必要なアプリケーションを使用している場合は特に、すべてのユーザーがきわめて多くのパスワードを持っています。通常のユーザーは、どのアプリケーションや Web サイトにも同じパスワードを使用するか、または、工夫しすぎてどのパスワードがどのアプリケーションのものかをすぐに忘れてしまうかのどちらかです。

重要でないサイトのパスワードをソフトウェアに自動的に記憶させるか、またはパスワードを記憶するサイトと省略するサイトをユーザーが識別できるようになると便利です。その機能を実現するのが、Credential Manager for HP ProtectTools です。Credential Manager は、ユーザーにその機能を提供するパスワード マネージャーです。PC にサイン オンした後は、必要に応じて、Credential Manager によってパスワードまたは証明情報が提供されます。


証明情報が必要な任意のアプリケーションまたは Web サイトにアクセスすると、Credential Manager がそのサイトを自動的に認識し、ユーザーの情報をソフトウェアで記憶するかどうかをユーザーに尋ねます。ユーザーが同意すると、ユーザーはそのパスワードを再び思い出す必要がなくなります。特定のサイトを除外したい場合は、ユーザーの情報を記憶するという要求を辞退できます。

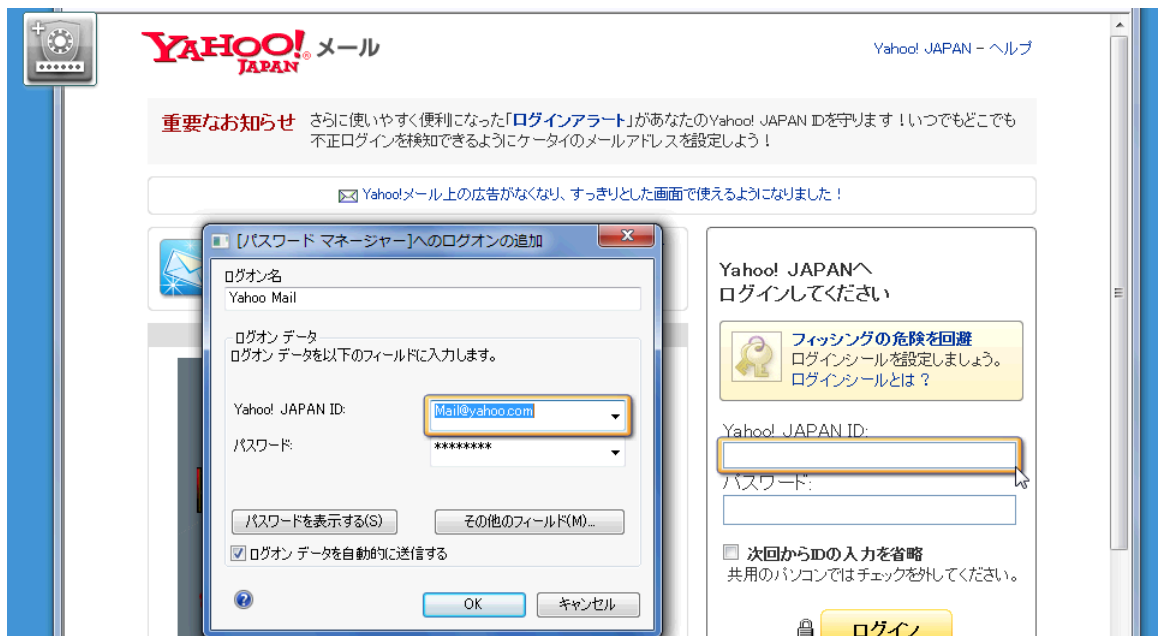
Web の場所、ユーザー名、およびパスワードの保存を開始するには、以下の操作を行います。

1. たとえば、Web メールアカウントに移動し、Credential Manager に指示して（アイコンをクリックして）Web 認証を追加します。

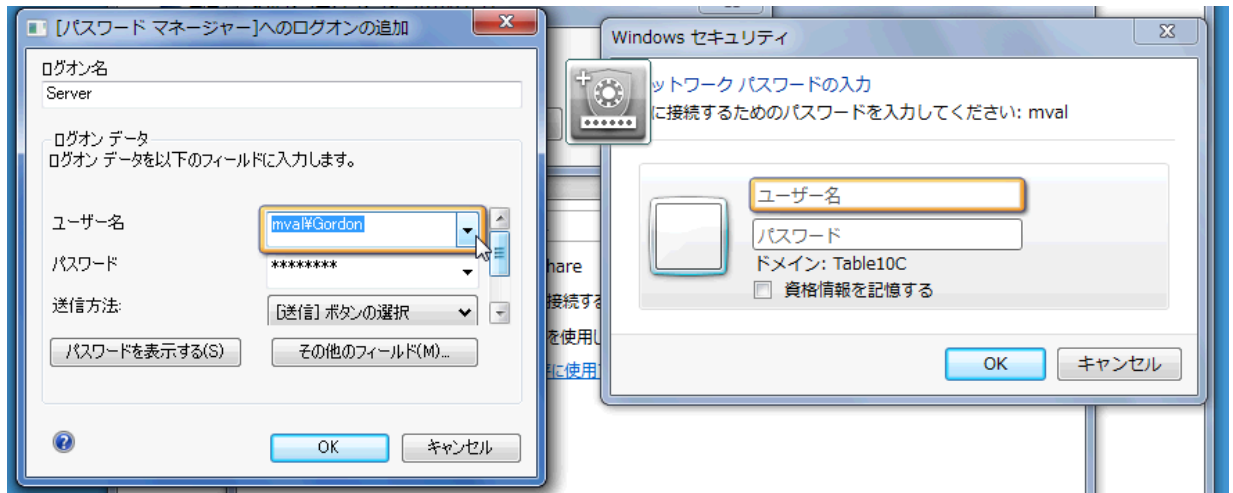


2. リンクに名前を付け（オプション）、Credential Manager にユーザー名およびパスワードを入力します。

 **注記：** Web ページでは、現在および以降のアクセス時に Credential Manager で使用する領域が強調表示されます。



- 完了したら、[OK]ボタンをクリックします。
- Credential Manager には、ネットワーク共有またはネットワーク ドライブの割り当てのためのユーザー名およびパスワードを保存することもできます。



Credential Manager に保存されている認証の表示および管理

Credential Manager の利点は、中心となる場所から認証を表示、管理、バックアップ、および起動できることです。また、Credential Manager では、保存されているサイトの Windows からの起動もサポートされます。

パスワード マネージャーを開くには、以下の 2 つの方法のどちらかを使用します。

- **Ctrl + Windows + H** のキーの組み合わせを使用してパスワード マネージャーを開きます。[開く]を選択すると、保存されているショートカットがすばやく起動され、認証されます。



または

- パスワード マネージャーで[管理]タブを選択して HP ProtectTools Security Manager を開きます。そこで、証明情報を編集できます。



Credential Manager の[編集]オプションを使用すると、名前およびログイン名（ログイン ID）を表示または変更できるほか、パスワードを表示することもできます。



HP ProtectTools for Small Business では、すべての証明情報および設定を別の PC にバックアップしたり、コピーしたりできます。



File Sanitizer for HP ProtectTools

File Sanitizer は、削除したデータの不正なユーザーによる復元を非常に困難にするように設計されています。ブラウザーの履歴を含む選択されたファイルやフォルダーを手動で消去するか、または消去の定期的なスケジュールを確立するために使用できる複数のオプションがあります。

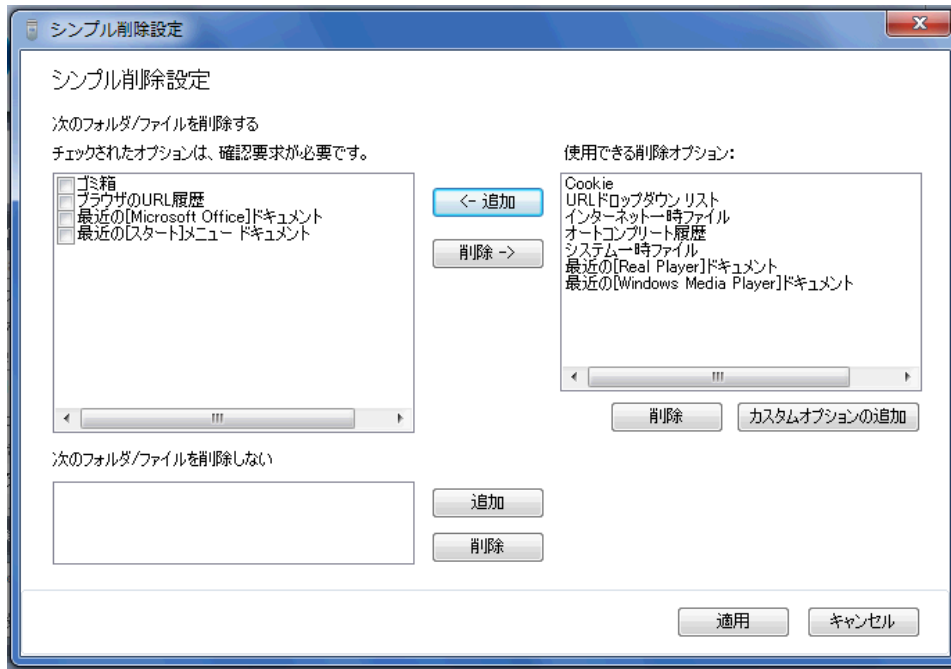
簡易構成の設定の一部を以下に示します。

削除したデータの完全な消去を開始するには、もう必要なくなったファイルまたはフォルダーを選択します。

1. [Security Manager]→[File Sanitizer]→[設定]の順に選択します。[シンプル削除設定]を選択し、[詳細を表示]ボタンをクリックします。

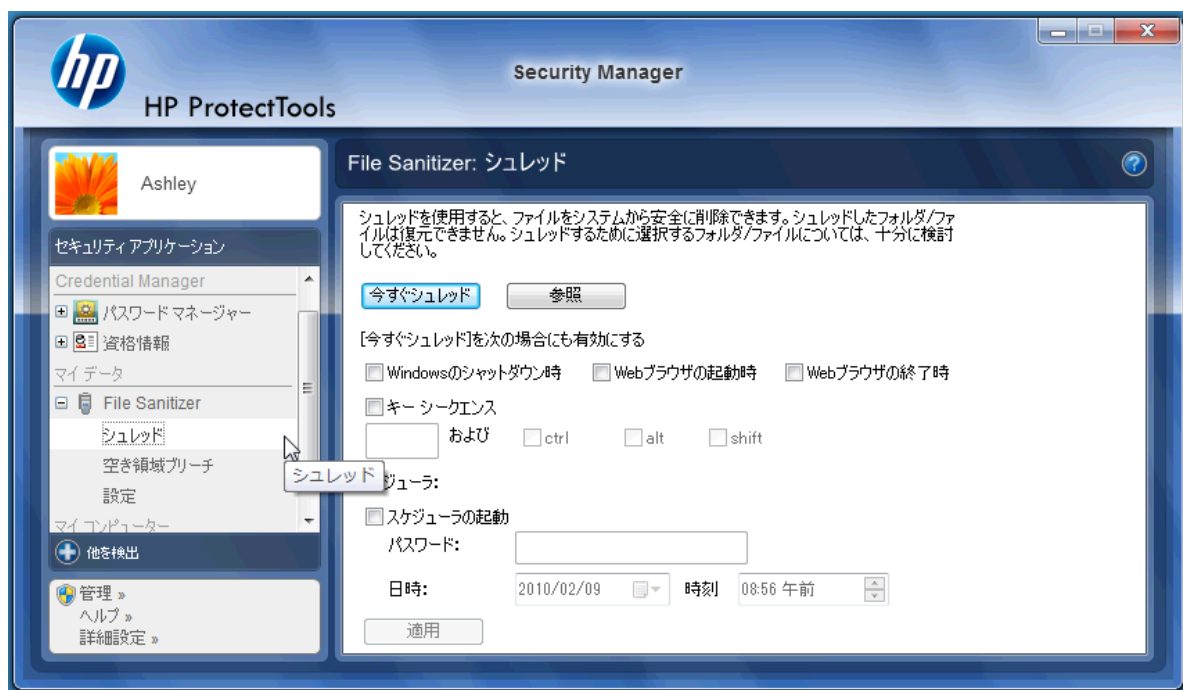


2. [シンプル削除設定]ウィンドウの右側から定期的に完全に削除する項目を選択し、[<-追加] ボタンをクリックして、選択した項目を削除の側に移動します。



3. [ゴミ箱]から始め、シュレッドによって消去する他の項目を追加します。
4. 完全に消去するすべての項目を選択したら、[適用] ボタンをクリックします。

5. [シュレッド]オプションに移動し、いつアクションを実行するかを設定します。[今すぐシュレッド]ボタンをクリックすると、先ほど設定した[シンプル削除設定]ウィンドウで選択されている項目がすぐに消去されます。



6. シュレッドが開始され、完了するたびに、タスク バーに小さなポップアップ バブルが表示されます。

Device Access Manager for HP ProtectTools

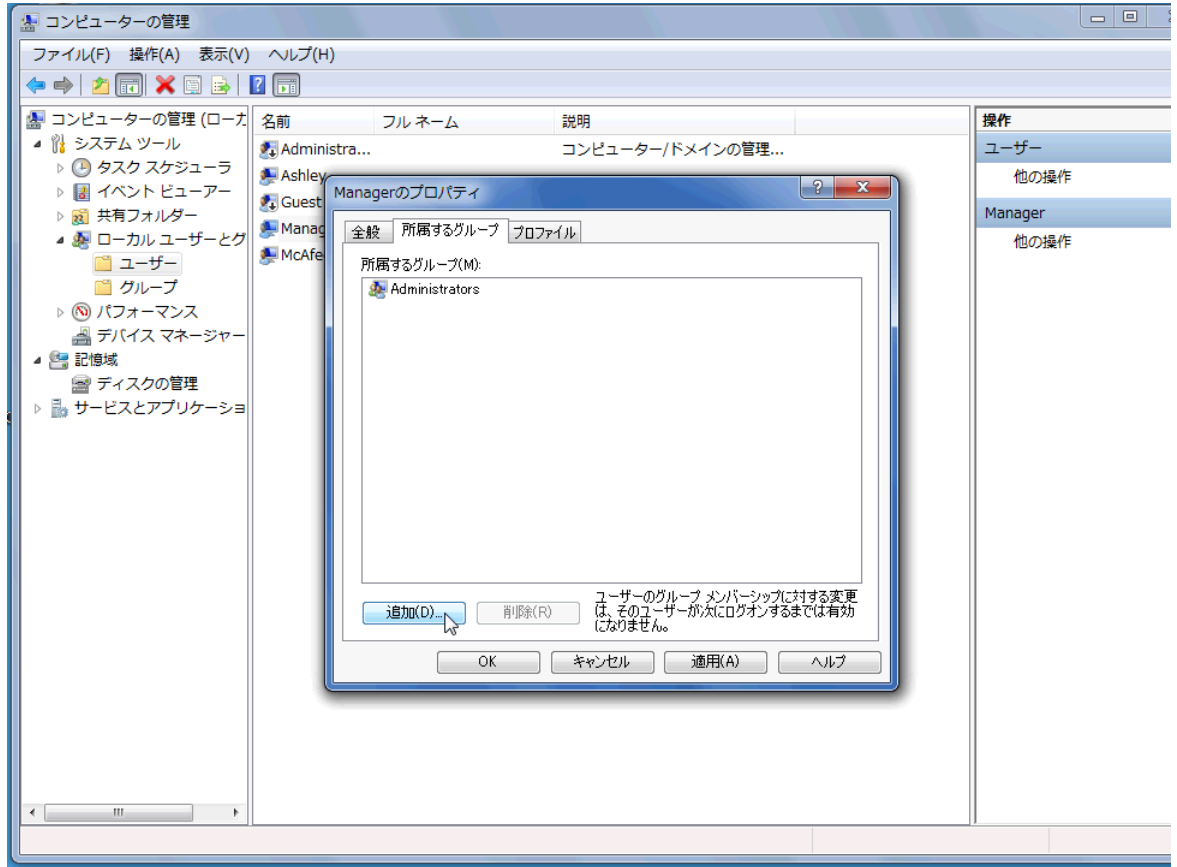
Device Access Manager を使用すると、データがハードディスク ドライブ上に安全な状態で残り、会社の外部に持ち出されることがないように、さまざまな内蔵および外付け記憶装置の使用を制限できます。1つの例として、あるユーザーにデータへのアクセスは許可するが、同じユーザーによるCD、個人用音楽プレーヤー、またはUSBメモリ デバイスへのコピーをブロックすることが考えられます。これを設定するための簡単な方法を以下に示します。

1. [スタート]→[すべてのプログラム]→[HP]→[HP ProtectTools 管理者コンソール]→[Device Access Manager]→[簡易構成]の順にクリックします。
2. 制限するハードウェア デバイスを選択し、[適用]ボタンをクリックして処理を終了します。

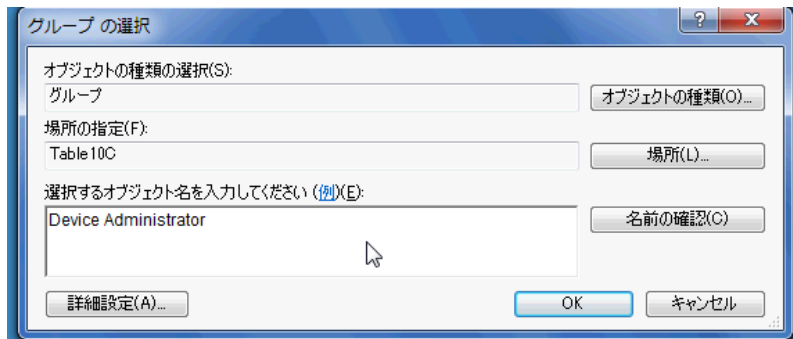


3. 以下に示す次の手順は、他のすべてのユーザーがブロックされた状態で引き続きアクセスが可能なユーザーの選択です。
4. [マイ コンピュータ]に移動して選択し、右クリックして[管理]→[コンピューターの管理]→[システム ツール]→[ローカル ユーザーとグループ]→[ユーザー]の順に選択します。
5. ブロックされたハードウェアへのアクセスを保持するユーザー（この例では「Manager」）をダブルクリックします。

6. [所属するグループ] タブの [追加] ボタンをクリックします。



7. [グループの選択] ウィンドウで、[詳細設定] オプションを使用するか、または単に「Device Administrator」グループと入力することもできます。[OK] ボタンをクリックし、[OK] ボタンをクリックしてウィンドウを閉じます。アクセス権を取得するには、ログオフしてログオンし直す必要があります。



これで、[Device Administrator]グループに含まれているユーザーを除き、CD-ROM の読み出しが可能なオプティカル ドライブ、USB ドライブ、個人用音楽プレーヤーなどを含むすべての内蔵および外付け記憶装置が機能しなくなります。

Drive Encryption for HP ProtectTools

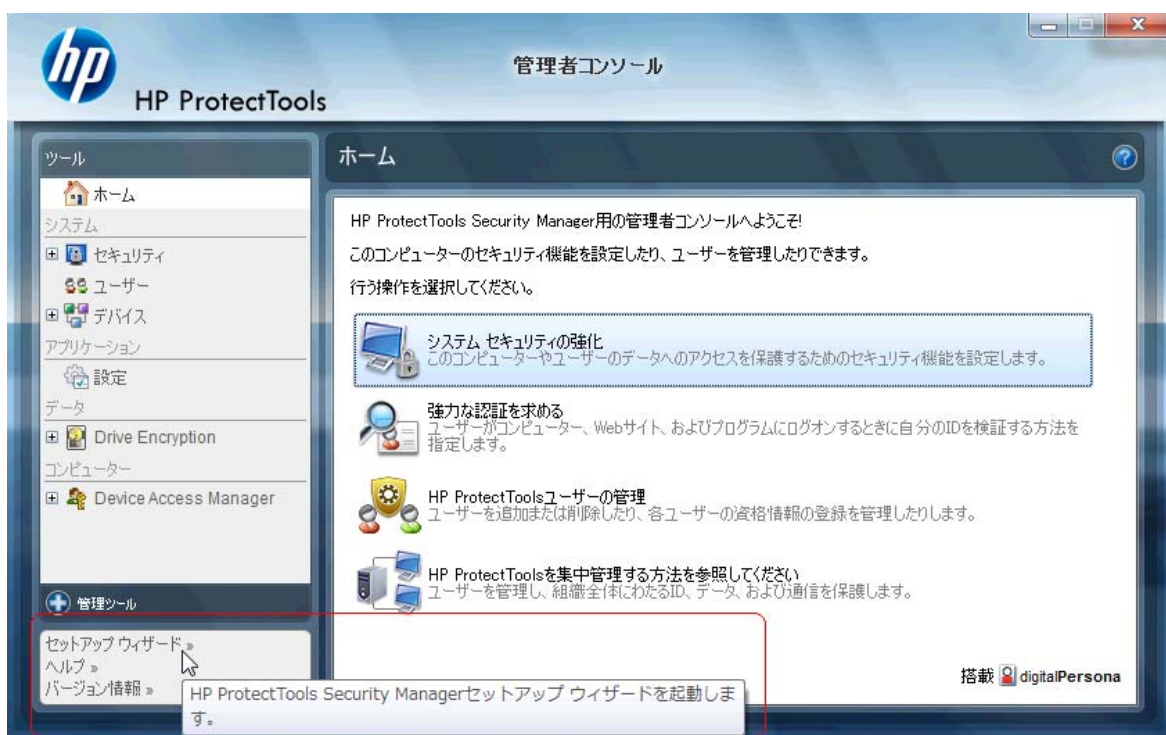
Drive Encryption for HP ProtectTools は、ハードディスク ドライブ全体を暗号化することによってデータ保護を実現するソフトウェアです。 コンピューターが盗まれたり、ハードディスク ドライブが元のシステムから取り外されて異なるシステムに接続されたりしたとしても、ハードディスク ドライブのデータが保護されたままになります。

さらに Drive Encryption によって、システムを起動する前にユーザー名とパスワードを使用して、適切な認証をする必要があるというセキュリティの利点があります。 この認証プロセスはブート前認証と呼ばれます。

Drive Encryption は、Windows ユーザー、ドメイン、Credential Manager for HP ProtectTools、および HP ProtectTools Security Manager とのインターフェイスがあるため、パスワードの同期も簡単です。

Drive Encryption for HP ProtectTools を有効にするには、以下の操作を行います。

1. [スタート]→[すべてのプログラム]→ [HP]→[HP ProtectTools 管理者コンソール]→[管理ツール]→[セットアップ ウィザード]の順にクリックします。 以下の画面が表示されます。




2. [ようこそ]画面で[次へ]を選択します。
3. Windows のパスワードを使用して有効化ウィザードを起動してから、[次へ]を選択します。
4. [Drive Encryption] ボックスにチェックを入れて、[次へ]をクリックします。

5. 以下の Drive Encryption 設定ウィンドウに暗号化できるドライブが表示され、暗号化リカバリキーを保存するための USB フラッシュドライブが要求されます。 起動前パスワードを紛失した場合またはパスワードが機能しない場合に、このリカバリ キーをデータの復元やドライブへのアクセスに使用するため、リカバリ キーは安全な場所に確実に保管してください。



6. **[次へ]**を選択し、手順を完了して、**[完了]**を選択します。メッセージが表示されたら、USB フラッシュドライブを取り外し、準備ができたならシステムを再起動します。
7. システムがハードディスク ドライブから起動したら、Drive Encryption から Windows パスワードが要求されます。パスワードを入力して**[OK]**をクリックします。

 **注記：** ドライブの暗号化処理の進行中は、コンピューターの動作が遅くなったように見える場合があります。完全に暗号化されると、システムは正常に戻ります。ドライブのデータにアクセスされると、必要に応じてデータが暗号化されたり暗号化が解除されたりします。

また Drive Encryption 認証は、Credential Manager の Windows ログインに「チェーン」され、直接デスクトップが表示されます。パスワードを 2 回入力する必要はありません。

3 HP ProtectTools for Small Business の利点

HP ProtectTools for Small Business セキュリティ ソフトウェアへのアクセス

Windows の[スタート]メニューから HP ProtectTools Security Manager にアクセスするには、以下の操作を行います。

- ▲ Windows で、[スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]の順にクリックします。

Windows の[スタート]メニューから HP ProtectTools Security Manager 管理者コンソールにアクセスするには、以下の操作を行います。

- ▲ Windows で、[スタート]→[すべてのプログラム]→[HP ProtectTools 管理者コンソール]の順にクリックします。

主なセキュリティの目的の実現

各 HP ProtectTools モジュールが連携して動作することによって、以下の主なセキュリティの目的を含む、さまざまなセキュリティの問題を解決できます。

- 機密データへのアクセス制限
- 内部または外部の場所からの不正なアクセスの防止
- 強力なパスワード ポリシーの作成

機密データへのアクセス制限

契約検査官がオンサイトで作業しており、機密の財務データの確認のためにコンピューターへのアクセスを許可されているとします。ただし、この検査官がこれらのファイルを印刷したり、CD などの書き込み可能なデバイスに保存できるようにはしたくありません。データへのアクセスを制限するには、以下の機能が役立ちます。

Device Access Manager for HP ProtectTools を使用すると、管理者は書き込み可能なデバイスへのアクセスを制限して、機密の情報を印刷したり、ハードディスク ドライブからリムーバブル メディアにコピーしたりできないようにできます。[49 ページの「デバイス クラス構成 \(詳細設定\)」](#)を参照してください。

内部または外部の場所からの不正なアクセスの防止

セキュリティ保護されていないビジネス PC への不正なアクセスは、財務サービス、役員、または研究開発チームのデータなどの重要なデータや、カルテや個人の財務データなどの個人情報を非常に大きなリスクにさらすこととなります。不正なアクセスを防止するには、以下の機能が役立ちます。

- ブート前認証機能が有効になっていると、オペレーティング システムへのアクセスを防止することができます。以下の章を参照してください。
 - [36 ページの「Credential Manager for HP ProtectTools \(パスワード マネージャー\)」](#)
 - [33 ページの「Drive Encryption for HP ProtectTools」](#)
- Credential Manager for HP ProtectTools は、不正なユーザーがパスワードを入手したり、パスワードで保護されたアプリケーションにアクセスしたりできないようにできます。以下の章を参照してください。
 - [36 ページの「Credential Manager for HP ProtectTools \(パスワード マネージャー\)」](#)
- Device Access Manager for HP ProtectTools を使用すると、管理者は書き込み可能なデバイスへのアクセスを制限して、機密データをハードディスク ドライブからコピーできないようにできます。以下の章を参照してください。
 - [48 ページの「Device Access Manager for HP ProtectTools」](#)
- File Sanitizer を使用すると、重要なファイルやフォルダーのシュレッドまたはハードディスク ドライブのブリーチ（以前に削除されたがハードディスク ドライブ上にはまだ存在するデータを上書きして、データの復元をさらに困難にすること）によって、データを安全に削除できます。以下の章を参照してください。
 - [41 ページの「File Sanitizer for HP ProtectTools」](#)

強力なパスワード ポリシーの作成


いくつかの Web ベースのアプリケーションやデータベースに対して強力なパスワード ポリシー（ハッキングが困難な複雑なパスワード）を使用する必要がある場合、Credential Manager for HP ProtectTools は、パスワードやシングルサインオンのための保護されたリポジトリを提供します。以下の章を参照してください。

- [36 ページの「Credential Manager for HP ProtectTools \(パスワード マネージャー\)」](#)

その他のセキュリティ対策

セキュリティの役割の割り当て

データを正しく保護するには、重要な作業の 1 つとして、責任および権限をさまざまな管理者やユーザーに割り当てることが挙げられます。

 **注記：** 小さな組織や個人で使用する場合は、1 人がすべての役割を持っていても構いません。

HP ProtectTools for Small Business では、セキュリティの責任および権限を以下の役割に分割できます。

- 管理者：セキュリティ機能を適用および管理します。また、一部の機能を有効または無効にできます。
- ユーザー：セキュリティ機能を使用します。

HP ProtectTools のパスワードの管理

HP ProtectTools Security Manager の機能のほとんどは、パスワードによってセキュリティ保護されています。以下の表に、よく使用されるパスワード、そのパスワードが設定されるソフトウェア モジュール、およびパスワード機能の一覧を示します。

この表には、管理者だけが設定して使用するパスワードも示されています。その他のすべてのパスワードは、一般のユーザーが設定できます。

HP ProtectTools のパスワード	設定する HP ProtectTools モジュール	バージョン
パスワード マネージャーのログオン パスワード	パスワード マネージャー	このパスワードには、以下の 2 つのオプションがあります <ul style="list-style-type: none">Windows にログオンした後、パスワード マネージャーにアクセスするための別のログオンで使用できますWindows ログオン プロセスの代わりに使用し、Windows とパスワード マネージャーに同時にアクセスできます
コンピューター セットアップ (F10) ユーティリティのパスワード	BIOS、管理者が設定	コンピューター セットアップ (F10) ユーティリティへのアクセスを保護します
注記： BIOS 管理者パスワード、F10 セットアップ パスワード、またはセキュリティ セットアップ パスワードとも呼ばれます		
電源投入時パスワード	BIOS	コンピューターの起動時や再起動時、またはハイバネーションからの復帰時にコンピューターのデータを保護します
Windows のログオン パスワード	Windows の[コントロールパネル]	手動ログオンに使用できます

安全なパスワードの作成

パスワードを作成する場合は、まず、プログラムで設定されている仕様に従う必要があります。ただし一般的には、強力なパスワードを作成して、作成したパスワードが危険にさらされないようにするために、以下のガイドラインを参考にしてください。

- 文字数が 6 文字、できれば 8 文字を超えるパスワードを使用します。
- パスワード全体にわたって大文字と小文字を混在させます。
- 可能な場合は常に、半角英数字を混在させ、さらに特殊文字と句読点を含めます。
- パスワード中の文字の代わりに特殊文字または数字を使用します。たとえば、アルファベットの l または L の代わりに数字の 1 を使用します。
- 2 つ以上の言語から取った単語を組み合わせます。
- 単語またはフレーズを数字や特殊文字で分割します。たとえば、「Mary2-2Cat45」とします。
- 辞書に載っているような用語は使用しないでください。

- 名前やその他の個人情報（たとえば、誕生日、ペットの名前、母親の旧姓など）は、たとえ綴りを逆にしたとしても、パスワードには使用しないでください。
- パスワードは定期的に変更してください。いくつかの文字や数字を以下の値に変更するだけでも構いません。
- パスワードをメモした場合は、コンピューターのすぐ近くの、人目につきやすい場所に保管しないでください。
- パスワードを、電子メールなどのコンピューター上のファイルに保存しないでください。
- アカウントを共有したり、パスワードを誰かに教えたりしないでください。

証明情報および設定のバックアップ

HP ProtectTools Security Manager のバックアップと復元ツールを使用して、インストール済みの HP ProtectTools モジュールからセキュリティ証明情報のバックアップと復元をまとめて実行する

4 HP ProtectTools Security Manager 管理者コンソール

HP ProtectTools 管理者コンソールについて

HP ProtectTools Security Manager の管理は、管理者コンソールを通して提供されます。

このコンソールを使用すると、ローカル管理者は以下のことが可能になります。

- セキュリティ機能を有効または無効にする
- コンピューターのユーザーを管理する
- デバイス固有のパラメーターを調整する
- Security Manager アプリケーションを設定する
- Security Manager アプリケーションを追加する

管理者コンソールの使用

Security Manager 管理者コンソールは、HP ProtectTools Security Manager を管理するための中心となる場所です。

コンソールを開くには、以下の操作を行います。

- [スタート]→[すべてのプログラム]→[HP ProtectTools 管理者コンソール]の順に選択するか、または
- Security Manager コンソールの左下隅にある[管理]リンクをクリックします。

管理者コンソールは、左側のパネルおよび右側のパネルの2つのパネルで構成されています。左側のパネルには、管理ツールが含まれています。右側のパネルには、ツールを設定するための作業領域が含まれています。

管理者コンソールの左側のパネルは、以下の領域で構成されています。

- [ホーム]：セキュリティ機能の有効化、セキュリティ証明情報の指定、ユーザーの管理などの、よく使用されるタスクに容易にアクセスできるようにします。
- [システム]：システム全体のセキュリティ機能、ユーザー、およびスマート カード リーダーなどの認証デバイスの設定を管理します。
- [アプリケーション]：Security Manager およびそのアプリケーションの動作を設定するためのツールが含まれています。


- **[データ]** : 暗号化キーをバックアップおよび復元するためのツールを提供します。
- **[コンピューター]** : PC のセキュリティを危険にさらす可能性のあるさまざまな種類のデバイスを個別に禁止したり、さまざまなユーザーおよびグループのアクセス権限を設定したりするための高度なセキュリティ オプションを提供します。
- **[管理ツール]** : 初期設定のブラウザーで、Security Manager の機能を拡張するための追加の管理アプリケーションやツールを見つけることのできる Web ページを開きます。この Web ページでは、新しいアプリケーションやアップデートが使用可能になった場合は常に通知を受信するための方法もわかります。
- **[リンク]** : 以下の機能を提供します。
 - **[セットアップ ウィザード]** : Security Manager の初期設定を実行できるセットアップ ウィザードを起動します。
 - **[ヘルプ]** : Security Manager およびそのアプリケーションに関する情報を提供するヘルプ ファイルを開きます。
 - **[バージョン情報]** : バージョン番号や著作権情報を含む、Security Manager に関する情報を表示します。

セットアップ ウィザードの使用開始準備

HP ProtectTools Security Manager の管理には、管理者権限が必要です。

HP ProtectTools Security Manager セットアップ ウィザードを使用すると、セキュリティ機能を設定できます。ただし、HP ProtectTools Security Manager コンソールから使用できる追加機能も豊富に存在します。追加のセキュリティ機能だけでなく、ウィザードにも存在する同じ設定を、Windows の[スタート]メニュー、または管理者コンソール内のリンクからアクセスするこのコンソールで構成することも可能です。これらの設定は、コンピューターおよびそのコンピューターを共有するすべてのユーザーに適用されます。

初めて Windows にログオンすると、HP ProtectTools Security Manager を設定するよう求めるメッセージが表示されます。**[OK]**をクリックして、このプログラムを設定するための基本的な手順を実行できる Security Manager セットアップ ウィザードを起動します。

 **注記** : 管理者コンソールの左側のパネルの一番下のセクションにある**[セキュリティ ウィザード]**をクリックすることによって、セキュリティ ウィザードを起動することもできます。

セットアップが完了するまで、セットアップ ウィザードの画面の説明に沿って操作します。

このウィザードを完了しない場合、**[今後、このウィザードを表示しない]**をクリックするまで、このウィザードが自動的に起動されます。

HP ProtectTools Security Manager アプリケーションを使用するには、**[スタート]**メニューから、またはタスクバー通知領域（システム トレイ）にある**[Security Manager]**アイコンを右クリックして HP ProtectTools Security Manager を起動します。Security Manager コンソールおよびそのアプリケーションは、このコンピューターを共有するすべてのユーザーが使用できます。

システムの設定

アプリケーションの**[システム]**グループは、管理者コンソールの左側にある**[ツール]**メニューからアクセスされます。

このグループに含まれているアプリケーションを使用すると、このコンピューター、そのユーザーおよびデバイスのポリシーや設定を設定したり管理したりできます。

[システム]グループには、以下のアプリケーションが含まれています。

- **[セキュリティ]**：セキュリティ機能、認証ポリシー、およびコンピューターまたは HP ProtectTools アプリケーションにログオンするときのユーザーの認証方法を管理するその他の設定を管理します。
- **[ユーザー]**：このコンピューターのユーザーを設定、管理、および登録します。
- **[デバイス]**：コンピューターに内蔵または接続されているセキュリティ デバイスの設定を管理します。

セキュリティ機能の有効化

ここで有効にしたセキュリティ機能は、このコンピューターのすべてのユーザーに適用されます。

1. 管理者コンソールの左側のパネルで、**[セキュリティ]**を展開し、**[機能]**をクリックします。
2. セキュリティ機能を有効にするには、**[Windows ログオンのセキュリティ]**か**[ドライブの暗号化]**、またはその両方の横にある対応するチェック ボックスにチェックを入れます。
 - **[Windows ログオンのセキュリティ]**：アクセスするために特定の証明情報の使用を要求することによって、Windows アカウントを保護します。
 - **[ドライブの暗号化]**：ハードディスク ドライブを暗号化して、適切な権限のないユーザーが情報を読み取れないようにすることによってデータを保護します。
3. **[次へ]** ボタンをクリックします。
4. **[適用]** ボタンをクリックします。

Security Manager 認証ポリシーの定義

このコンピューターの Security Manager 認証ポリシーは、ログオンおよびセッションの2つのタブで定義されます。これらのタブでは、ユーザー セッション中にコンピューターや HP ProtectTools アプリケーションにアクセスするときの各クラスのユーザーの認証に必要な証明情報を指定します。

[ログオン]タブ

コンピューターへのアクセスおよび Windows へのログオンに必要な証明情報を指定するには、以下の操作を行います。

1. 管理者コンソールの左側のパネルで、**[セキュリティ]**を展開し、**[認証]**をクリックします。
2. **[ログオン]**タブで、ドロップダウン リストからユーザーのカテゴリを選択します。
3. **[ポリシー]**セクションで、一覧表示された証明情報の横にある、1つ以上のチェック ボックスをクリックすることによって、選択したユーザーのカテゴリに必要な認証証明情報を指定します。少なくとも1つの証明情報を指定する必要があります。
4. **[ポリシー]**セクションのドロップダウン リストで、ユーザーを認証するために、指定した証明情報のどれか1つ（のみ）を要求するか、または指定した証明情報のすべてを要求するかを選択します。
5. **[適用]** ボタンをクリックします。

[セッション]タブ


Windows セッション中に HP ProtectTools アプリケーションにログオンするときのユーザーの認証に必要な証明情報を管理するポリシーを定義するには、以下の操作を行います。

1. 管理者コンソールの左側のパネルで、[セキュリティ]を展開し、[認証]をクリックします。
2. [セッション]タブで、ユーザーのカテゴリを選択します。
3. [ポリシー]セクションで、一覧表示された証明情報の横にある、1つ以上のチェック ボックスをクリックすることによって、選択したユーザーのカテゴリに必要な認証証明情報を指定します。少なくとも1つの証明情報を指定する必要があります。
4. [ポリシー]セクションのドロップダウン リストで、ユーザーを認証するために、指定した証明情報のどれか1つ（のみ）を要求するか、または指定した証明情報のすべてを要求するかを選択します。
5. [適用]ボタンをクリックします。

設定の定義

高度なセキュリティ設定のどれを許可するかを指定できます。設定を編集するには、以下の操作を行います。

1. 管理者コンソールの左側のパネルで、[セキュリティ]を展開し、[設定]をクリックします。
2. 特定の設定を有効または無効にするための適切なチェック ボックスにチェックを入れます。
3. [適用]をクリックして変更を保存します。

 **注記：** [ワン ステップ ログオンを許可する]の設定を使用すると、BIOS レベルで認証が実行された場合、このコンピューターのユーザーは Windows のログオンを省略できます。

ユーザーの管理

[ユーザー]アプリケーション内で、Windows 管理者はこのコンピューターのユーザー、およびそれらのユーザーに影響を与えるポリシーを管理できます。管理者コンソールで[ユーザー]アプリケーションにアクセスするには、[ユーザー]をクリックします。

HP ProtectTools ユーザーが一覧表示され、Security Manager で設定された認証ポリシー、およびこれらのポリシーを満たすために必要な証明情報に対して検証されます。

特定のユーザーに対して有効なポリシーを表示するには、一覧からユーザーを選択し、[ポリシーの表示]ボタンをクリックします。


証明情報を登録している間のユーザーを管理するには、一覧からユーザーを選択し、[登録]ボタンをクリックします。

ユーザーの追加


この処理によって、ログオン リストにユーザーが追加されます。ユーザーを追加するには、そのユーザーがコンピューター上で Windows ユーザー アカウントをすでに与えられている必要があります。以下の手順の実行中にはそのアカウントが存在し、パスワードを入力できるようになっている必要があります。

ユーザーをユーザー リストに追加するには、以下の操作を行います。

1. [スタート]→[すべてのプログラム]→[HP ProtectTools 管理者コンソール]の順にクリックします。
2. 管理者コンソールの左側のパネルで、[ユーザー]を選択します。
3. [追加]ボタンをクリックします。[ユーザーの選択]ダイアログ ボックスが表示されます。
4. [詳細]→[今すぐ検索]ボタンの順にクリックして、追加するユーザーを検索します。
5. 一覧に追加するユーザーをクリックして[OK]をクリックします。
6. [ユーザーの選択]ダイアログ ボックスで[OK]をクリックします。
7. 選択したアカウントの Windows パスワードを入力して、[完了]をクリックします。

 **注記：** Windows アカウントは既存のものを使用し、その名前を正しく入力する必要があります。このダイアログ ボックスで Windows ユーザー アカウントを変更または追加することはできません。

ユーザーの削除

 **注記：** この手順を実行しても、Windows ユーザー アカウントは削除されません。Security Manager からアカウントが削除されるだけです。ユーザーを完全に削除するには、Security Manager と Windows の両方からユーザーを削除する必要があります。

1. [スタート]→[すべてのプログラム]→[HP ProtectTools 管理者コンソール]の順にクリックします。
2. 管理者コンソールの左側のパネルで、[ユーザー]を選択します。
3. 削除するアカウントのユーザー名をクリックし、[削除]をクリックします。
4. 確認用のダイアログ ボックスで[はい]をクリックします。

ユーザーの状態の確認

管理者コンソールの[ユーザー]セクションには、各ユーザーの現在の状態が表示されます。


- 緑色のチェック マーク：必須のセキュリティ ログイン方法をそのユーザーが設定していることを示します。
- 赤色の X 印：ユーザーが必須のセキュリティ ログイン方法を設定していないため、ログインしようとしてもコンピューターから拒否されることを示しています。このユーザーは、セットアップ ウィザードを実行して必須のログイン方法を設定する必要があります。
- 表示なし：セキュリティ ログイン方法が必要ないことを示します。

アプリケーションの設定の構成

[設定]ウィンドウには、Security Manager およびそのアプリケーションの動作を設定するためのツールが含まれています。設定を変更するには、以下の操作を行います。

1. [スタート]→[すべてのプログラム]→[HP ProtectTools 管理者コンソール]の順にクリックします。
2. 管理者コンソールの左側のパネルで、[設定]を選択します。

3. [全般]タブで、HP ProtectTools Security Manager の全般的な設定を選択し、[適用] ボタンをクリックします。
4. [アプリケーション]タブで、有効または無効にするアプリケーションを選択し、[適用] ボタンをクリックします。

 **注記：** アプリケーションを有効または無効にしても、コンピューターが再起動されるまで有効にならない場合があります。

ドライブの暗号化

Drive Encryption for HP ProtectTools を使用すると、コンピューターのハードディスク ドライブを暗号化することによって、そのハードディスク ドライブがコンピューターから取り外されたりデータ復旧サービスに送付されたりした場合でも、そのデータにアクセスしようとする不正なユーザーからの読み取りやアクセスを防ぐことができます。

Drive Encryption を有効または無効にするには、管理者コンソールで[セットアップ ウィザード]をクリックします。

- △ **注意：** 暗号化キーを USB フラッシュドライブにバックアップし、その USB ドライブを安全な場所に保管する必要があります。 パスワードを忘れてしまった場合には、この USB ドライブに保存された暗号化キーがハードディスク ドライブにアクセスする唯一の方法となります。

Drive Encryption for HP ProtectTools の使用について詳しくは、[33 ページの「Drive Encryption for HP ProtectTools」](#)を参照してください。

デバイス アクセスの管理

Device Access Manager for HP ProtectTools は、PC のセキュリティを危険にさらす可能性のあるさまざまな種類のデバイスを個別に禁止するための高度なセキュリティ オプションを提供します。 Device Access Manager for HP ProtectTools の使用について詳しくは、[48 ページの「Device Access Manager for HP ProtectTools」](#)を参照してください。

5 HP ProtectTools Security Manager (HP ProtectTools セキュリティ マネージャー)

HP ProtectTools Security Manager を使用すると、コンピューターのセキュリティを大幅に向上させることができます。Security Manager アプリケーションを使用することで、以下のことが可能になります。

- ログオン情報およびパスワードを管理する
- Windows パスワードを簡単に変更する
- 認証証明情報 (スマート カードを含む) を設定する
- ハードディスク ドライブをシュレッドまたはブリーチする
- ドライブの暗号化の状態を表示する
- デバイス アクセスの設定を表示する
- Security Manager のデータをバックアップおよび復元する

パスワードの管理

Credential Manager for HP ProtectTools (パスワード マネージャー) は、ログオン情報を作成および管理します。このログオン情報を使用すると、登録された証明情報で認証されることによって Web サイトを開いてログオンしたり、プログラムを起動してログオンしたりできます。

パスワードの管理について詳しくは、[36 ページの「Credential Manager for HP ProtectTools \(パスワード マネージャー\)」](#)を参照してください。

証明情報の設定

Security Manager の証明情報は、ユーザーが実際に本人であることを確認するために使用します。このコンピューターの管理者は、Windows アカウント、Web サイト、またはプログラムにログオンするときのユーザーの ID を証明するために使用できる証明情報を設定できます。

使用可能な証明情報は、コンピューターに内蔵または接続されているセキュリティ デバイスによって異なる場合があります。サポートされている証明情報は、それぞれ証明情報グループにエントリがあります。

Windows パスワードの変更

Security Manager での Windows パスワードの変更は、Windows の[コントロール パネル]を使用する場合よりも、簡単または迅速です。

Windows パスワードを変更するには、以下の操作を行います。

1. HP ProtectTools Security Manager の左側のパネルで、**[証明書]**をクリックします。
2. **[Windows パスワード]**をクリックします。
3. **[現在の Windows パスワード]**ボックスに現在のパスワードを入力します。
4. **[新しい Windows パスワード]**ボックスおよび**[新しいパスワードの確認]**ボックスに新しいパスワードを入力します。
5. **[変更]**をクリックします。

ファイルのシュレッドまたはブリーチ

File Sanitizer for HP ProtectTools は、ファイルを意味のないデータで上書きすることによってファイルを削除します。「シュレッド」と呼ばれるこの処理によって、削除されたファイルの復元が非常に困難になるため、情報のセキュリティが大幅に向上します。File Sanitizer は、「ブリーチ」と呼ばれる処理を使用してハードディスク ドライブ上の以前に使用された領域を上書きすることによって、情報のセキュリティをさらに向上させます。File Sanitizer を使用して削除されたファイルを、オペレーティング システムやその他の一般に使用可能なファイル回復ソフトウェアで回復することはできません。

File Sanitizer for HP ProtectTools の使用について詳しくは、[41 ページの「File Sanitizer for HP ProtectTools」](#)を参照してください。

ドライブの暗号化の状態の表示

ドライブの暗号化は、管理者コンソールで Windows 管理者によって設定されます。ユーザーは、Security Manager で自分の暗号化の状態を表示できます。

ドライブの暗号化の状態を表示するには、以下の操作を行います。

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**の順にクリックします。
2. Security Manager の左側のパネルで、**[暗号化の状態]**を選択します。**[暗号化の状態]**ページには、ドライブの暗号化が有効になっているか無効になっているか、および各ドライブが暗号化されているかいないかが表示されます。

デバイス アクセスの表示

デバイス アクセスは、管理者コンソールで Windows 管理者によって設定されます。ユーザーは、Security Manager で自分のデバイス アクセスの設定を表示できます。


デバイス アクセスの設定を表示するには、以下の操作を行います。

1. [スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]の順にクリックします。
2. Security Manager の左側のパネルで、[Device Access Manager]を展開します。
3. アクセスを拒否されているデバイスを表示するには、[簡易構成]をクリックします。横にチェック マークが付いているデバイスは、アクセスを拒否されています。
4. アクセスを拒否されているユーザーまたはグループを表示するには、[デバイス クラス構成]をクリックします。
5. デバイスをクリックすると、そのデバイスへのアクセスを拒否または許可されているユーザーまたはグループが表示されます。

アプリケーションの追加

追加のアプリケーションを使用して、このプログラムに新機能を追加できます。

1. [スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]の順にクリックします。
2. Security Manager の左側のパネルで、[他を検出]を選択します。

 **注記：** [他を検出]リンクがない場合は、コンピューターの管理者によってこのリンクが無効にされています。

3. [アプリケーションの追加]タブで、追加のアプリケーションを参照します。
4. [更新およびメッセージ]タブで、[新しいアプリケーションおよび更新に関する通知を受け取る]チェック ボックスにチェックを入れてアップデートを確認する日数を設定することによって、新しいアプリケーションやアップデートに関する通知を常に受信できます。または、[今すぐチェック]ボタンをクリックして、アップデートをすぐに確認することもできます。

設定のオプション

[設定]ページでは、[アイコンをタスクバーに表示]チェック ボックスにチェックを入れて、タスクバー通知領域（システム トレイ）に[Security Manager]アイコンを表示できます。

[設定]ページにアクセスするには、以下の操作を行います。

1. [スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]の順にクリックします。
2. Security Manager の左側のパネルで、[詳細]→[設定]の順にクリックします。
3. [アイコンをタスクバーに表示]チェック ボックスのチェックを入れるか、チェックを外して[適用]をクリックします。

バックアップおよび復元

Security Manager のデータは定期的にバックアップすることをおすすめします。バックアップの頻度は、データが変更される頻度によって異なります。たとえば、新しいログオンを毎日のように定期的に追加している場合は、おそらく毎日データをバックアップする必要があります。

バックアップは、あるコンピューターから別のコンピューターへ移行するためにも使用できます（インポートおよびエクスポートとも呼ばれます）。ただし、この機能では、データのみがバックアップされることに注意してください。

バックアップ ファイルを別のコンピューターに復元する場合や、オペレーティング システムの再インストール後に同じコンピューターに復元する場合は、バックアップ ファイルからデータを復元する前に、HP ProtectTools Security Manager がすでにそのシステムにインストールされている必要があります。

データのバックアップ

データをバックアップする場合は、ログオンおよび証明情報を、入力したパスワードで保護された暗号化ファイルに保存します。

データをバックアップするには、以下の操作を行います。

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**の順にクリックします。
2. Security Manager の左側のパネルで、**[詳細]**→**[バックアップおよび復元]**の順にクリックします。
3. **[データのバックアップ]**をクリックします。
4. バックアップに含めるモジュールを選択します。多くの場合、すべてのモジュールの選択が必要になります。**[次へ]**をクリックします。
5. IDを確認するためのパスワードを入力し、矢印ボタンをクリックします。
6. ストレージ ファイルのパスおよび名前を入力します。初期設定では、ファイルはドキュメントフォルダーに保存されます。別の場所を指定するには、**[参照]**をクリックします。**[次へ]**をクリックします。
7. ファイルを保護するには、パスワードの入力と確認を行います。
8. **[完了]**をクリックします。

データの復元

Security Manager のバックアップおよび復元機能を使用して以前に作成された、パスワードで保護された暗号化ファイルからデータを復元します。

データを復元するには、以下の操作を行います。

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**の順にクリックします。
2. Security Manager の左側のパネルで、**[詳細]**→**[バックアップおよび復元]**の順にクリックします。
3. **[データの復元]**をクリックします。
4. ストレージ ファイルのパスおよび名前を入力するか、または**[参照]**をクリックしてファイルを選択します。
5. ファイルを保護するために使用されたパスワードを入力し、**[次へ]**をクリックします。

6. データを復元するモジュールを選択します。多くの場合、一覧表示されているすべてのモジュールを選択することになります。[次へ]をクリックします。
7. [完了]をクリックします。

Windows のユーザー名および画像の変更

Security Manager の左上隅には、Windows のユーザー名と画像が表示されます。

ユーザー名や画像を変更するには、以下の操作を行います。

1. ユーザー名および画像がある Security Manager の左上のセクションをクリックします。
2. ユーザー名を変更するには、[Windows ユーザー名]ボックスに名前を入力します。
3. 画像を変更するには、[画像の選択]ボタンをクリックし、画像を参照して選択します。
4. [保存]ボタンをクリックして変更内容を保存します。


6 Drive Encryption for HP ProtectTools

 **注記：** Drive Encryption for HP ProtectTools は、一部のモデルでのみ利用できます。

今日では、会社にある自分のコンピューターや他の社員のコンピューターが盗まれて、企業の重要な情報が大きな危険にさらされる可能性があります。コンピューターのハードディスク ドライブ上のデータをすべて暗号化すれば、不正なユーザーがそのデータにアクセスしようとして、ドライブをコンピューターから取り外したりデータ復旧サービスに送ったりしても、読み取ったりアクセスしたりできないようになります。

Drive Encryption for HP ProtectTools ソフトウェアでは、ハードディスク ドライブを暗号化することによる完全なデータ保護が可能です。Drive Encryption を有効にしている場合は、Windows が起動する前に表示される Drive Encryption のログイン画面からログインする必要があります。

Drive Encryption は、同一の Windows セッションの継続中は、不正なアクセスを防止できません。コンピューターを起動してユーザー名とパスワードを入力した後では、ハードディスク ドライブのデータは暗号化されていても、システムのすべてのユーザーがデータにアクセスできます。コンピューターから離れるときは、Windows セッションを必ずパスワードで保護してください。

 **注記：** Drive Encryption for HP ProtectTools の有効化は、HP ProtectTools 管理者コンソールのセットアップ ウィザードからのみ実行できます。

注記： Drive Encryption は、AMD 製プロセッサを使用するシステムで、RAID 構成されている 64 ビット オペレーティング システムではサポートされていません。

注記： Drive Encryption は辞書攻撃からの保護をサポートしていません。

Drive Encryption では、以下の作業を実行できます。

- 内蔵ハードディスク ドライブのすべてのデータを暗号化
- パスワードによる簡単なアクセスおよびブート前認証
- Microsoft Windows XP、Windows Vista®、および Windows 7 をサポート

Drive Encryption for HP ProtectTools では、以下のような、さまざまなタスクを実行できます。

- Drive Encryption の管理
 - 個々のドライブの暗号化または暗号化の解除
- バックアップおよび復元
 - バックアップ キーの作成
 - 復元の実行

△ **注意：** 暗号化キーを USB フラッシュドライブにバックアップし、その USB ドライブを安全な場所に保管する必要があります。パスワードを忘れてしまった場合には、この USB ドライブに保存された暗号化キーがハードディスク ドライブにアクセスする唯一の方法となります。

注意： Drive Encryption モジュールをアンインストールする場合、またはバックアップと復元用のソリューションを使用している場合は、まず暗号化されたすべてのドライブの暗号化を解除する必要があります。そうしないと、暗号化されたドライブ上のデータにアクセスできなくなります。Drive Encryption モジュールを再インストールしても、暗号化されたドライブにはアクセスできません。

セットアップ手順

Drive Encryption を開く

1. [スタート]→[すべてのプログラム]→[HP ProtectTools 管理者コンソール]の順にクリックします。
2. [ドライブの暗号化]をクリックします。

一般的なタスク

Drive Encryption の有効化

Drive Encryption を有効にするには、HP ProtectTools 管理者コンソール セットアップ ウィザードを使用します。

Drive Encryption の無効化

Drive Encryption を無効にするには、HP ProtectTools 管理者コンソール セットアップ ウィザードを使用します。

Drive Encryption の有効化後のログイン

Drive Encryption を有効にし、ユーザー アカウントを登録した後でコンピューターを起動した場合は、Drive Encryption のログオン画面からログインする必要があります。

🔍 **注記：** Windows 管理者が HP ProtectTools 管理者コンソールでブート前セキュリティを有効にしている場合は、Drive Encryption のログオン画面が表示されたときではなく、コンピューターの電源を入れた直後コンピューターにログインされます。

注記： Drive Encryption のログオン画面で復元キーを使用してログオンする場合は、Windows のログオン画面で Windows のユーザー名を選択し、パスワードを入力することも要求されます。


高度なタスク

Drive Encryption の管理（管理者のタスク）

[Drive Encryption]ウィンドウでは、Windows 管理者は Drive Encryption の状態（有効または無効）を表示および変更し、コンピューター上のすべてのハードディスク ドライブの暗号化の状態を表示できます。

個々のドライブの暗号化または暗号化の解除


1. 管理者コンソールの左側のパネルで、[Drive Encryption]を展開して、[暗号化の管理]をクリックします。
2. [暗号化の変更]ボタンをクリックします。
3. [暗号化の変更]ダイアログ ボックスで、暗号化するか、暗号化を解除する各ハードディスク ドライブの横にあるチェック ボックスにチェックを入れるか、またはチェックを外して、[OK]をクリックします。

 **注記：** ドライブの暗号化または暗号化解除が行われている間、現在のセッションで処理が完了するまでの残り時間が進行状況バーに表示されます。暗号化中にコンピューターをシャットダウンするか、スリープまたはハイバネーションを開始してから起動しなおした場合、残り時間の表示はリセットされますが、実際の暗号化は直前に停止した場所から再開されます。残り時間と進行状況の表示がすばやく進み、現在の進行状況が反映されます。


バックアップおよび復元（管理者のタスク）

Drive Encryption の[バックアップおよび復元]ウィンドウでは、Windows 管理者が暗号化キーをバックアップし、復元することができます。

バックアップ キーの作成

 **注意：** パスワードを忘れてしまった場合には、バックアップ キーを含むストレージ デバイスがハードディスク ドライブにアクセスする唯一の方法となるため、このデバイスは必ず安全な場所に保管してください。

1. 管理者コンソールの左側のパネルで、[Drive Encryption]を展開して、[バックアップおよび復元]をクリックします。
2. [キーをバックアップする]ボタンをクリックします。
3. [バックアップ ディスクの選択]ページで、暗号化キーをバックアップするデバイスの名前をクリックし、[次へ]をクリックします。
4. 次に表示されるページの情報を確認してから、[次へ]をクリックします。
選択したストレージ デバイスに暗号化キーが保存されます。
5. 確認ダイアログ ボックスが表示されたら、[OK]をクリックします。

 **注記：** 復元の管理および実行について詳しくは、Drive Encryption for HP ProtectTools のヘルプ ファイルを参照してください。

7 Credential Manager for HP ProtectTools (パスワード マネージャー)

パスワード マネージャーを使用すると、Windows、Web サイト、およびプログラムへのログオンがより簡単かつ安全になります。

パスワード マネージャーでは、Web サイトおよびプログラムにすばやく安全にアクセスできるようにするために、ログオン画面を設定できます。パスワード マネージャーは、まずログオン情報を認識し、各ログオン画面の入力ボックスに入力された個々のデータを記憶します。その後、ログオン画面が表示されると、パスワード マネージャーはユーザーの ID を確認し、そのデータを自動的に入力および送信します。

ホットキーの組み合わせを設定（初期設定は **Ctrl + Windows + H**）して使用すると、すぐにログオン メニューが表示されるため、さらにすばやいアクセスが可能になります。メニューでは、ログオンを選択するだけでパスワード マネージャーが Web サイトまたはプログラムを起動し、ログオン画面に移動して自動的にログインを実行します。

ID を確認するには、Windows パスワードなどの HP ProtectTools for Small Business 証明情報を使用します。つまり、設定したどのログオン画面でも、同じ証明情報を使用してログオンすることになります。したがって、書き留めておいたり覚えておいたりする必要がない強固なパスワードを作成して、アカウントをより安全にできます。

パスワード マネージャーでは、お使いのパスワードにセキュリティ上のリスクがあるかどうかを一目でわかる形で表示し、新しいサイト用に複雑で強力なパスワードを自動作成できます。

パスワード マネージャーでは、ログオン情報やパスワードをいつでも表示したり編集したりできます。あらかじめ設定したプログラムまたは任意の Web サイトのログオン画面がフォーカスされているときに必ず表示される[パスワード マネージャー]アイコンからも、パスワード マネージャーの多くの機能を利用できます。アイコンをクリックするとコンテキスト メニューが表示され、このメニューから以下のオプションを選択できます。

ログオン情報が作成されていない Web ページまたはプログラムの場合

以下のオプションがコンテキスト メニューに表示されます。

- [[パスワードマネージャー]への[任意のドメイン]の追加]：表示中のログオン画面用にログオン情報を追加するために使用します。
- [[パスワード マネージャー]を開く]：[パスワード マネージャー]ページで Security Manager を起動します。

- [アイコンの設定] : [パスワード マネージャー]アイコンを表示する条件を指定できます。
- [ヘルプ] : パスワード マネージャー アプリケーションのオンライン ヘルプを表示します。

ログオン情報が作成されている Web ページまたはプログラムの場合

以下のオプションがコンテキスト メニューに表示されます。

- [ログオン データの入力] : ログオン データをログオン用フィールドに入力してページを送信します (ログオン情報を作成または最後に編集したときに送信を指定していた場合)。
- [ログオンの編集] : 表示中の Web サイト用のログオン データを編集できます。
- [ログオンの追加] : 同じ Web サイトまたはプログラムに別のログオン情報を追加するために使用します。
- [パスワード マネージャーを起動] : [パスワード マネージャー]ページで Security Manager ダッシュボードを起動します。
- [ヘルプ] : パスワード マネージャー アプリケーションのオンライン ヘルプを表示します。

ログオン情報の追加

ログオン情報を追加するには、以下の操作を行います。

1. Web サイトまたはプログラムのログオン画面を表示します。
2. [パスワード マネージャー]アイコンの矢印をクリックし、ログオン画面の種類 (Web サイト用またはプログラム用) に応じて以下のどちらかを選択します。
 - Web サイトの場合 : [[パスワードマネージャー]への[任意のドメイン]の追加]を選択します。
 - プログラムの場合 : [[パスワード マネージャー]へのログオンの追加]を選択します。
3. ログオン データを入力します。画面のログオン用フィールドおよびダイアログの対応するフィールドが、オレンジ色の太い枠線で識別されます。パスワード マネージャーの[管理]タブから[ログオンの追加]を選択するなどして、このダイアログを表示するための、他のオプションを利用することもできます。Ctrl + H ホットキーを使用したりスマート カードを挿入したりするなど、コンピューターに接続されているセキュリティ デバイスに依存するオプションもあります。
 - あらかじめフォーマットが用意された選択肢の 1 つを使用してログオン用フィールドに入力するには、フィールドの右側にある矢印をクリックします。
 - 必要に応じて画面上の他のフィールドをログオン情報に追加するには、[その他のフィールド]をクリックします。
 - ログオン用フィールドの入力後に送信を実行しない場合は、[ログオン データを自動的に送信する]の選択を解除します。
 - このログオン用のパスワードを表示するには、[パスワードを表示する]をクリックします。
4. [OK]をクリックします。[パスワード マネージャー]アイコンのプラス記号 (+) が消え、ログオン情報が作成されたことが示されます。

これで、その Web サイトにアクセスするかそのプログラムを起動すると、その度に[パスワード マネージャー]アイコンが表示され、登録済みの証明情報を使用してログオンできることが示されるようになります。

ログオン情報の編集

ログオン情報を編集するには、以下の操作を行います。

1. Web サイトまたはプログラムのログオン画面を表示します。
2. [パスワード マネージャー]アイコンの矢印をクリックし、**[編集]**を選択して、ログオン情報を編集できるダイアログを表示します。画面のログオン用フィールドおよびダイアログの対応するフィールドが、オレンジ色の太い枠線で識別されます。
3. ログオン情報を編集します。
 - あらかじめフォーマットが用意された選択肢の1つを使用してログオン用フィールドに入力するには、フィールドの右側にある矢印をクリックします。
 - 必要に応じて画面上の他のフィールドをログオン情報に追加するには、**[その他のフィールド]**をクリックします。
 - ログオン用フィールドの入力後に送信を実行しない場合は、**[ログオン データを自動的に送信する]**の選択を解除します。
 - このログオン用のパスワードを表示するには、**[パスワードを表示する]**をクリックします。
4. **[OK]**をクリックします。

ログオン メニューの使用

パスワード マネージャーでは、ログオン情報を作成した Web サイトおよびプログラムをすばやく簡単に起動できます。**[ログオン]**メニューまたは**[パスワード マネージャー]**の**[管理]**タブからプログラムまたは Web サイトをダブルクリックし、ログオン画面を表示して、ログオン データを入力します。初期設定では、ログオン情報もすぐに Web サイトに送信されます。ただし、ログオン情報の最初の設定時または編集時に**[ログオン データを自動的に送信する]**の選択を解除して、送信されないようにできます。

作成したログオン情報は、パスワード マネージャーの**[ログオン]**メニューに自動的に追加されます。

[ログオン]メニューを表示するには、パスワード マネージャーのホットキーを押します。初期設定は **Ctrl + H** ですが、**[パスワード マネージャー]** → **[設定]**の順にクリックしてホットキーの組み合わせを変更できます。

ログオン情報をカテゴリ別に整理

ログオン情報を整理するには、カテゴリを使用します。1つ以上のカテゴリを作成し、ログオン情報を目的のカテゴリにドラッグ アンド ドロップするのみで簡単に整理できます。

カテゴリを追加するには、以下の操作を行います。

1. Security Manager の左側のパネルで、**[パスワード マネージャー]**を選択します。
2. **[管理]**タブを選択し、**[カテゴリの追加]**をクリックします。
3. カテゴリの名前を入力します。
4. **[OK]**をクリックします。

ログオン情報をカテゴリに追加するには、以下の操作を行います。

1. マウス ポインターを目的のログオンの上に置きます。
2. マウスの左ボタンを押したままにします。
3. ログオン情報をカテゴリの一覧にドラッグします。マウス ポインターをカテゴリの上に置くと、そのカテゴリが強調表示されます。
4. 目的のカテゴリが強調表示されたら、マウス ボタンを放します。

ログオン情報は、選択したカテゴリに移動されるのではなく、コピーされるのみです。そのため、同じログオン情報を複数のカテゴリに追加できます。[すべて]をクリックすると、常にすべてのログオン情報を表示できます。

ログオン情報の管理

パスワード マネージャーを使用すると、ユーザー名、パスワード、および複数のログオン アカウントのログオン情報を、中心となる 1 つの場所から簡単かつ直感的に管理できます。

ログオン情報は[管理]タブに一覧表示されます。同じ Web サイトに対して複数のログオン情報が作成されている場合、各ログオン情報は常にその Web サイト名の下に一覧表示され、ログオン情報一覧の中でインデント表示されます。

ログオン情報を管理するには、以下の操作を行います。

Security Manager の左側のパネルで、[パスワード マネージャー]を選択して、[管理]タブをクリックします。

- ログオン情報の追加：[ログオンの追加]をクリックし、画面の説明に沿って操作します。
- ログオン情報の編集：ログオン情報を選択して[編集]をクリックします。ログオン データを目的に合うように変更します。
- ログオン情報の削除：ログオン情報を選択して[削除]をクリックします。

Web サイトまたはプログラムに他のログオン情報を追加するには、以下の操作を行います。

1. Web サイトまたはプログラムのログオン画面を表示します。
2. [パスワード マネージャー]アイコンをクリックして、ショートカット メニューを表示します。
3. [他のログオンの追加]を選択し、画面の説明に沿って操作します。

パスワード強度の評価

証明情報を保護するには、Web サイトおよびプログラムに強固なパスワードを使用することが重要です。

パスワード マネージャーでは、Web サイトおよびプログラムへのログオンに使用されている各パスワードの強度を自動的にすばやく分析することで、セキュリティを簡単に監視および強化できます。ログオンに使用するパスワードの強度は、パスワード マネージャーの[パスワード強度]タブで確認できます。

[パスワード マネージャー]アイコンの設定


パスワード マネージャーでは、Web サイトおよびプログラムのログオン画面の識別が試行されます。ログオン情報が作成されていないログオン画面が検出されると、パスワード マネージャーによってプラス記号（+）の付いた[パスワード マネージャー]アイコンが表示され、その画面用のログオン情報を追加するよう求められます。

以下の設定を実行できます。

- [常に要求する]：ログオン情報がまだ設定されていないログオン画面が表示されたときに、パスワード マネージャーによってログオン情報の追加を必ず求められるようにするには、このオプションを選択します。
- [この画面では要求しない]：パスワード マネージャーによってこの特定のログオン画面へのログオン情報の追加を今後求められないようにするには、このオプションを選択します。
- [常に要求しない]：ログオン情報が設定されていないログオン画面に対して、パスワード マネージャーによって何も求められないようにするには、このオプションを選択します。

8 File Sanitizer for HP ProtectTools

File Sanitizer は、コンピューター上の重要なファイルやフォルダー（個人情報や個人ファイル、履歴データや Web 関連データ、その他のデータ コンポーネント）を安全に消去したり、ハードディスク ドライブを定期的にブリーチしたりすることができるツールです。

 **注記：** File Sanitizer は現在、ハードディスク ドライブ上でのみ動作します。

シュレッドについて

Windows でファイルやフォルダーを削除しても、その内容がハードディスク ドライブから完全に削除されるわけではありません。Windows は参照情報のみを削除します。別のファイルによってハードディスク ドライブ上のその同じ領域が新しい情報で上書きされるまで、内容はハードディスク ドライブに引き続き残ったままとなります。


データをシュレッドすると、そのデータを取り戻すことは事実上不可能であるため、シュレッドは通常の Windows の削除（File Sanitizer ではシンプル削除とも言います）とは異なります。

シュレッド プロファイル（[セキュリティ設定、高]、[セキュリティ設定、中]、または[セキュリティ設定、低]）を選択すると、あらかじめ定義されているファイルやフォルダーの一覧と除去方法がシュレッドのために自動で選択されます。また、シュレッド プロファイルをカスタマイズして、シュレッド サイクル数、シュレッド対象に含めるファイル、シュレッド前に確認するファイル、およびシュレッド対象から除外するファイルを指定することもできます。

自動シュレッドのスケジュールを設定できます。また、必要に応じていつでもファイルやフォルダーを手動シュレッドすることもできます。

空き領域ブリーチについて

空き領域ブリーチを実行すると、削除されたファイルに対してランダムなデータを安全に上書きできるため、削除されたファイルの元の内容をユーザーは参照できなくなります。

 **注記：** 空き領域ブリーチは、Windows のゴミ箱を使用して削除したファイル、または手動で削除したファイルを対象とする機能です。空き領域ブリーチを実行しても、シュレッドされたファイルにセキュリティが追加されることはありません。

タスクバーの右端の通知領域にある[HP ProtectTools]アイコンを使用して、空き領域ブリーチの自動スケジュールを有効にするか、空き領域ブリーチを手動で実行できます。

セットアップ手順

File Sanitizer の起動


File Sanitizer を起動するには、以下の操作を行います。

1. [スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]の順にクリックします。
2. Security Manager の左側のパネルで、[File Sanitizer]をクリックします。
または
 - [File Sanitizer]アイコンをダブルクリックします。
または
 - タスクバーの右端の通知領域にある[HP ProtectTools]アイコンを右クリックし、[File Sanitizer]を強調表示してから、[File Sanitizer を開く]をクリックします。

空き領域ブリーチのスケジュール設定


空き領域ブリーチのスケジュールを設定するには、以下の操作を行います。

1. Security Manager の左側のパネルで、[File Sanitizer]を展開して、[空き領域ブリーチ]をクリックします。
2. [スケジュールの起動]チェック ボックスにチェックを入れ、Windows のパスワードを入力してから、ハードディスク ドライブをブリーチする日付と時刻を入力します。
3. [保存]アイコンをクリックします。

 **注記：** 空き領域ブリーチ操作は、長い時間がかかる場合があります。空き領域ブリーチはバックグラウンドで実行されますが、プロセッサの使用量が大きくなるため、コンピューターの動作が遅くなる場合があります。

シュレッド スケジュールの設定

1. Security Manager の左側のパネルで、**[File Sanitizer]**を展開して、**[シュレッド]**をクリックします。
2. シュレッド オプションを以下の中から選択します。
 - **[Windows のシャットダウン時]**：選択されているすべてのファイルを Windows のシャットダウン時にシュレッドするには、このオプションを選択します。

 **注記**： このオプションを選択すると、シャットダウン時にダイアログ ボックスが表示され、選択されているファイルのシュレッドを実行するか、シュレッド処理を中止するかを確認するメッセージが表示されます。シュレッド処理に進む場合は[はい]、シュレッドを中止する場合は[いいえ]をクリックします。Windows では、シャットダウンに備えてソフトウェアが終了され、エラーが生成されるため、[はい]または[いいえ]オプションの選択はすぐに行う必要があります。シュレッド処理に進むために[いいえ]を選択すると、File Sanitizer が応答していないことを示すエラー画面が Windows によって表示されることがあります。File Sanitizer がシュレッド処理を完了できるようにしてから、もう一度シャットダウンを開始します。

 - **[Web ブラウザの起動時]**：ブラウザーの URL 履歴など、選択されているすべての Windows 関連ファイルを Web ブラウザーの起動時にシュレッドするには、このオプションを選択します。
 - **[Web ブラウザの終了時]**：ブラウザーの URL 履歴など、選択されているすべての Windows 関連ファイルを Web ブラウザーの終了時にシュレッドするには、このオプションを選択します。
 - **[キー シークエンス]**：キーの組み合わせでシュレッドを開始するには、このオプションを選択します。
 - **[スケジューラ]**：[スケジューラの起動]チェック ボックスにチェックを入れ、Windows のパスワードを入力してから、選択されているファイルをシュレッドする日付と時刻を入力します。
3. **[保存]**アイコンをクリックします。

シュレッド プロファイルの選択または作成

あらかじめ定義されているプロファイルを選択するか、自分のプロファイルを作成して、消去方法を指定したりシュレッドするファイルやフォルダーを選択したりできます。

あらかじめ定義されているシュレッド プロファイルの選択

あらかじめ定義されているシュレッド プロファイル（[セキュリティ設定、高]、[セキュリティ設定、中]、または[セキュリティ設定、低]）を選択すると、あらかじめ定義されている消去方法とファイルの一覧が自動的に選択されます。[詳細を表示]ボタンをクリックすると、シュレッド用に選択されているファイルのあらかじめ定義されている一覧が表示されます。

あらかじめ定義されているシュレッド プロファイルを選択するには、以下の操作を行います。


1. Security Manager の左側のパネルで、**[File Sanitizer]**を展開して、**[設定]**をクリックします。
2. あらかじめ定義されているシュレッド プロファイルをクリックします。
3. **[詳細を表示]**をクリックして、シュレッド用に選択されているファイルの一覧を表示します。

4. [次のフォルダ/ファイルをシュレッドする]で、シュレッド前に確認する各ファイルの横のチェック ボックスにチェックを入れます。
5. [適用]をクリックします。


高度にセキュリティ設定されたシュレッド プロファイルのカスタマイズ

シュレッド プロファイルを作成するには、シュレッド サイクル数、シュレッド対象に含めるファイル、シュレッド前に確認するファイル、およびシュレッド対象から除外するファイルを指定します。


1. Security Manager の左側のパネルで、[File Sanitizer]を展開して[設定]をクリックし、[高度なセキュリティ設定]を選択してから、[詳細の表示]をクリックします。
2. シュレッド サイクル数を指定します。

 **注記：** 各ファイルに対して、指定した数のシュレッド サイクルが実行されます。たとえば、シュレッド サイクルで3を選択すると、データの内容を消去するアルゴリズムが異なる3つの時間に実行されます。高いセキュリティ設定でシュレッド サイクルを選択すると、シュレッドに非常に長い時間がかかる場合があります。ただし、指定するシュレッド サイクル数を大きくするほど、コンピューターのセキュリティは高まります。

3. シュレッドするファイルやフォルダーを選択するには、以下の操作を行います。
 - a. [使用できるシュレッド オプション]で、ファイルをクリックしてから[追加]をクリックします。
 - b. カスタム ファイルを追加するには、[カスタム オプションの追加]をクリックし、ファイル名またはフォルダー名を入力して[OK]をクリックします。カスタム ファイルをクリックして、[追加]をクリックします。

 **注記：** 使用できるシュレッド オプションからファイルを削除するには、ファイルをクリックしてから[削除]をクリックします。


4. [次のフォルダ/ファイルをシュレッドする]で、シュレッド前に確認する各ファイルの横のチェック ボックスにチェックを入れます。

 **注記：** シュレッド リストからファイルを削除するには、ファイルをクリックしてから[削除]をクリックします。


5. [次のフォルダ/ファイルをシュレッドしない]で、[追加]をクリックして、シュレッド対象から除外するファイルを指定します。
6. シュレッド プロファイルの設定を完了したら、[適用]をクリックします。

シンプル削除プロファイルのカスタマイズ


シンプル削除プロファイルは、シュレッドではなく、標準的なファイルの削除を実行します。シンプル削除プロファイルのカスタマイズするには、シンプル削除対象に含めるファイル、シンプル削除の実行前に確認するファイル、およびシンプル削除対象から除外するファイルを指定します。

 **注記：** シンプル削除オプションを使用する場合は、空き領域ブリーチを定期的に行うことを強くおすすめします。

1. Security Manager の左側のパネルで、**[File Sanitizer]**を展開して**[設定]**をクリックし、**[シンプル削除設定]**を選択してから、**[詳細の表示]**をクリックします。
2. 削除するファイルを選択します。
 - a. **[使用できる削除オプション]**で、ファイルをクリックしてから**[追加]**をクリックします。
 - b. カスタム ファイルを追加するには、**[カスタム オプションの追加]**をクリックし、ファイル名またはフォルダ名を入力して**[OK]**をクリックします。カスタム ファイルをクリックして、**[追加]**をクリックします。

 **注記：** 使用できる削除オプションからファイルを削除するには、ファイルをクリックしてから**[削除]**をクリックします。

3. **[次のフォルダ/ファイルを削除する]**で、削除前に確認する各ファイルの横のチェック ボックスにチェックを入れます。

 **注記：** 削除リストからファイルを削除するには、ファイルをクリックしてから**[削除]**をクリックします。

4. **[次のフォルダ/ファイルを削除しない]**で、**[追加]**をクリックして、シュレッド対象から除外するファイルを指定します。
5. シンプル削除プロファイルの設定を完了したら、**[適用]**をクリックします。


一般的なタスク

キーの組み合わせによるシュレッドの開始

キーの組み合わせを指定するには、以下の操作を行います。

1. Security Manager の左側のパネルで、**[File Sanitizer]**を展開して、**[シュレッド]**をクリックします。
2. **[キー シークエンス]**チェック ボックスにチェックを入れます。
3. 使用できるボックスに文字を 1 つ入力してから、**[CTRL]**ボックス、**[ALT]**ボックス、**[SHIFT]**ボックスのどれかまたは 3 つすべてにチェックを入れます。

たとえば、**S** キーと **Ctrl + Shift** キーを使用して自動シュレッドを開始するには、ボックスに **S** と入力してから、**[CTRL]**オプションと**[SHIFT]**オプションにチェックを入れます。

 **注記：** 設定済みの他のキーの組み合わせとは異なるキーの組み合わせを選択してください。

キーの組み合わせでシュレッドを開始するには、以下の操作を行います。

1. 選択した文字を押しながら、**Ctrl + Alt** キーまたは **Shift** キー（またはあらかじめ指定した組み合わせのキー）を押します。
2. 確認用のダイアログ ボックスが表示されたら、**[はい]**をクリックします。

[File Sanitizer]アイコンの使用

△ **注意：** シュレッドしたファイルは復元できません。手動でシュレッドするために選択するファイルやフォルダーについては、十分に検討してください。

1. シュレッドするドキュメントまたはフォルダーに移動します。
2. シュレッドするファイルをデスクトップの[File Sanitizer]アイコンにドラッグします。
3. 確認用のダイアログ ボックスが表示されたら、[はい]をクリックします。

単一のファイルやフォルダーの手動シュレッド

△ **注意：** シュレッドしたファイルは復元できません。手動でシュレッドするために選択するファイルやフォルダーについては、十分に検討してください。

1. タスクバーの右端の通知領域にある[HP ProtectTools]アイコンを右クリックし、[File Sanitizer]を強調表示してから、[単一フォルダー/ファイルをシュレッド]をクリックします。
2. [参照]ダイアログ ボックスが開いたら、シュレッドするファイルに移動してから[開く]をクリックします。

📖 **注記：** 選択できるファイルは、単一のファイルまたはフォルダーです。

3. 確認用のダイアログ ボックスが表示されたら、[はい]をクリックします。

または

1. デスクトップにある[File Sanitizer]アイコンを右クリックしてから、[単一フォルダー/ファイルをシュレッド]をクリックします。
2. [参照]ダイアログ ボックスが開いたら、シュレッドするファイルに移動してから[開く]をクリックします。
3. 確認用のダイアログ ボックスが表示されたら、[はい]をクリックします。

または

1. Security Manager の左側のパネルで、[File Sanitizer]を展開して、[シュレッド]をクリックします。
2. [参照]ボタンをクリックします。
3. [参照]ダイアログ ボックスが開いたら、シュレッドするファイルに移動してから[開く]をクリックします。
4. 確認用のダイアログ ボックスが表示されたら、[はい]をクリックします。

選択されているすべてのファイルやフォルダーの手動シュレッド

1. タスクバーの右端の通知領域にある[HP ProtectTools]アイコンを右クリックし、[File Sanitizer]を強調表示してから、[今すぐシュレッド]をクリックします。
2. 確認用のダイアログ ボックスが表示されたら、[はい]をクリックします。

または

1. デスクトップにある[File Sanitizer]アイコンを右クリックしてから、[今すぐシュレッド]をクリックします。
2. 確認用のダイアログ ボックスが表示されたら、[はい]をクリックします。

空き領域ブリーチの手動実行

1. タスクバーの右端の通知領域にある[HP ProtectTools]アイコンを右クリックし、[File Sanitizer]を強調表示してから、[今すぐブリーチ]をクリックします。
2. ブリーチ操作が始まったことを確認する通知メッセージが表示されます。

または

1. Security Manager の左側のパネルで、[File Sanitizer]を展開して、[空き領域ブリーチ]をクリックします。
2. [今すぐブリーチ]をクリックします。
3. ブリーチ操作が始まったことを確認する通知メッセージが表示されます。

シュレッド操作または空き領域ブリーチ操作の停止


シュレッド操作または空き領域ブリーチ操作の実行中は、通知領域にある[HP ProtectTools Security Manager]アイコンの上にメッセージが表示されます。このメッセージには、シュレッドまたは空き領域ブリーチの進行状況の詳細（完了した割合）と、操作を停止するためのオプションが表示されます。

この操作を停止するには、以下の操作を行います。

- ▲ メッセージをクリックしてから[停止]ボタンをクリックすると、操作がキャンセルされます。

ログ ファイルの表示

シュレッド操作または空き領域ブリーチ操作を実行するたびに、エラーのログ ファイルまたは障害のログ ファイルが生成されますこれらのログ ファイルは、最新のシュレッド操作または空き領域ブリーチ操作に従って常に更新されます。

 **注記：** 正常にシュレッドまたはブリーチされたファイルは、ログ ファイルには表示されません。


ログ ファイルには、シュレッド操作について作成されるファイルと空き領域ブリーチ操作について作成されるファイルがあります。どちらのファイルも、ハードディスク ドライブ上の以下の場所に存在します。

- C:\Program Files\Hewlett-Packard\File Sanitizer\[Username]_ShredderLog.txt
- C:\Program Files\Hewlett-Packard\File Sanitizer\[Username]_DiskBleachLog.txt

9 Device Access Manager for HP ProtectTools

このセキュリティ ツールは管理者のみが使用できます。Device Access Manager for HP ProtectTools は、コンピューター システムに取り付けられたデバイスを不正なアクセスから保護する以下のセキュリティ機能を備えています。

- デバイス アクセスを定義するためにユーザーごとに作成されるデバイス プロファイル
- グループ メンバーシップに基づいて許可または拒否可能なデバイス アクセス制御

 **注記：** Device Access Manager は、Windows の[ローカル ユーザーとグループ]を使用してアクセスを管理します。Windows Home Edition では、[ローカル ユーザーとグループ]がサポートされていないため、Device Access Manager は正しく機能しません。ただし、Windows Vista の Home Edition では、DOS コマンドを使用してユーザー設定を行うと Device Access Manager が動作します。手順については、Device Access Manager のヘルプファイルを参照してください。

バックグラウンド サービスの開始

デバイス プロファイルを適用するには、HP ProtectTools Device Locking/Auditing バックグラウンド サービスを実行している必要があります。最初にデバイス プロファイルを適用しようとするとき、HP ProtectTools Administrative Console はダイアログ ボックスを開いて、バックグラウンド サービスを開始するかどうかを確認します。[はい]をクリックしてバックグラウンド サービスを開始し、システムがブートするたびに自動的に開始するように設定します。

簡易構成


Device Access Manager は、管理者としてデバイスへのアクセスまたはデバイスの参照を実行できる、Device Administrators という新しいユーザー グループをインストール時に作成します。Device Access Manager の簡易構成によってアクセスを制御するデバイスに対して、ユーザーを管理者としてアクセスさせる場合は、そのユーザーをこのグループに所属させてください。

この機能を使用して、以下のクラスのデバイスへのアクセスを拒否できます。

- 管理者以外のユーザーによるすべての USB デバイスへのアクセス
- 管理者以外のユーザーによるすべてのリムーバブル メディア（ディスクレット、個人用音楽プレーヤー、USB メモリなど）へのアクセス
- 管理者以外のユーザーによるすべての DVD/CD-ROM ドライブへのアクセス
- 管理者以外のユーザーによるすべてのシリアル ポートおよびパラレル ポートへのアクセス

管理者以外のすべてのユーザーによるデバイス クラスへのアクセスを拒否するには、以下の操作を行います。

1. [スタート]→[すべてのプログラム]→[HP ProtectTools 管理者コンソール]の順にクリックします。
2. 左側のパネルで、[Device Access Manager]→[簡易構成]の順にクリックします。
3. 右側のパネルで、アクセスを拒否するデバイスのチェック ボックスにチェックを入れます。
4. [保存]アイコンをクリックします。

 **注記：** バックグラウンド サービスが実行されていない場合は、ここで起動が試みられます。
[はい]をクリックして起動を許可します。

5. [OK]をクリックします。

デバイス クラス構成（詳細設定）

特定のユーザーまたはユーザーのグループによるデバイスの種類へのアクセスを許可または拒否することもできます。

ユーザーまたはグループの追加

1. [スタート]→[すべてのプログラム]→[HP ProtectTools 管理者コンソール]の順にクリックします。
2. 左側のパネルで、[Device Access Manager]を展開してから[デバイス クラス構成]をクリックします。
3. デバイスの一覧で、設定するデバイス クラスをクリックします。
4. [追加]をクリックします。[ユーザーまたはグループの選択]ダイアログ ボックスが表示されません。
5. [詳細]→[今すぐ検索]の順にクリックして、追加するユーザーまたはグループを検索します。
6. 使用可能なユーザーおよびグループの一覧に追加するユーザーまたはグループをクリックして[OK]をクリックします。
7. [OK]をクリックします。

ユーザーまたはグループの削除

1. [スタート]→[すべてのプログラム]→[HP ProtectTools 管理者コンソール]の順にクリックします。
2. 左側のパネルで、[Device Access Manager]を展開してから[デバイス クラス構成]をクリックします。
3. デバイスの一覧で、設定するデバイス クラスをクリックします。
4. 削除するユーザーまたはグループをクリックして、[削除]をクリックします。

ユーザーまたはグループのアクセス拒否または許可

1. [スタート]→[すべてのプログラム]→[HP ProtectTools 管理者コンソール]の順にクリックします。
2. 左側のパネルで、[Device Access Manager]を展開してから[デバイス クラス構成]をクリックします。
3. デバイスの一覧で、設定するデバイス クラスをクリックします。
4. [ユーザー/グループ]で、アクセスを拒否するユーザーまたはグループをクリックします。
5. アクセスを拒否するユーザーまたはグループの横にある[拒否]をクリックします。
6. [保存]アイコン→[OK]の順にクリックします。

ユーザー アクセス設定（詳細設定）

ユーザー アクセス設定を使用すると、管理者は簡易構成ビューおよびデバイス クラス構成ビューを使用できるユーザーおよびグループを指定できます。

ユーザーまたはグループが簡易構成およびデバイス クラス構成の情報を表示するには、**[構成設定の読み取り（読み取り専用）]**アクセス権が与えられている必要があります。

ユーザーまたはグループが簡易構成およびデバイス クラス構成の情報を変更するには、**[構成設定の変更]**アクセス権が与えられている必要があります。

ユーザーまたはグループが簡易構成ビューおよびデバイス クラス構成ビューで設定を変更するには、**[フル ユーザー管理者権限]**アクセス権が与えられている必要があります。

ユーザーまたはグループの追加

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools 管理者コンソール]**の順にクリックします。
2. 左側のパネルで、**[Device Access Manager]**を展開して、**[ユーザー アクセス設定]**をクリックします。
3. **[追加]**をクリックします。**[ユーザーまたはグループの選択]**ダイアログ ボックスが表示されます。
4. **[詳細]**→**[今すぐ検索]**の順にクリックして、追加するユーザーまたはグループを検索します。
5. 使用可能なユーザーおよびグループの一覧に追加するユーザーまたはグループをクリックして**[OK]**をクリックします。
6. **[OK]**をクリックします。
7. **[保存]**アイコンをクリックします。

ユーザーまたはグループの削除

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools 管理者コンソール]**の順にクリックします。
2. 左側のパネルで、**[Device Access Manager]**を展開して、**[ユーザー アクセス設定]**をクリックします。
3. 削除するユーザーまたはグループをクリックして、**[削除]**をクリックします。
4. **[保存]**アイコンをクリックします。

アクセスの許可または拒否

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools 管理者コンソール]**の順にクリックします。
2. 左側のパネルで、**[Device Access Manager]**を展開して、**[ユーザー アクセス設定]**をクリックします。
3. **[グループ名またはユーザー名]**ボックスで、ユーザーまたはグループの名前を選択します。

4. **[アクセス権]**ボックスで、適切なアクセス権の**[許可]**または**[拒否]**チェックボックスにチェックを入れます。
5. **[保存]**アイコンをクリックします。

用語集

ATM (Automatic Technology Manager) :

ネットワーク管理者がシステムを BIOS レベルでリモート管理できます。

Windows 管理者 :

アクセス権を変更し、他のユーザーを管理するすべての権限を持つユーザー。

Windows ユーザー アカウント :

ネットワークまたは個別のコンピューターへのログオンを承認された個人のプロファイル。

空き領域ブリーチ :

ハードディスク ドライブ上の削除したファイルにランダムなデータを上書きすることによって、削除したファイルの内容が見えないようにし、データの復元がさらに困難になるようにする機能。

管理者 :

「Windows 管理者」を参照してください。

キーの組み合わせ :

特定のキーの組み合わせ。Ctrl + Alt + S キーなどを押すと、自動シュレッドが開始されます。

資産 :

ハードディスク ドライブ上に存在する、個人情報や個人ファイル、履歴データや Web 関連データなどで構成されたデータ コンポーネント。

自動シュレッド :

ユーザーが File Sanitizer for HP ProtectTools で設定したスケジュールに従って実行されるシュレッド。

手動シュレッド :

単一のファイルやフォルダーまたは選択されている複数のファイルやフォルダーに対して、自動シュレッド スケジュールを無視して実行されるシュレッド。

シュレッド :

フォルダーやファイルに含まれるデータの内容をわからなくするアルゴリズムの実行。

シュレッド サイクル :

各ファイルやフォルダーでシュレッド アルゴリズムを実行する回数。選択したシュレッド サイクルの回数が多いほど、コンピューターのセキュリティは高くなります。

シュレッド プロファイル :

あらかじめ指定されている消去方法、およびファイルやフォルダーの一覧。

証明情報 :

ユーザーが認証プロセスで特定のタスクに対する適格性を証明するための方法（ユーザー名やパスワードなど）。

シンプル削除 :

ファイル、履歴や Web 関連情報、またはその他の機密データを含む機密情報を安全に削除します。

セキュリティ ログイン方法：

コンピューターへのログインに使用される方法。

電源投入時認証：

コンピューターの起動時に何らかの形式の認証（パスワードなど）を要求するセキュリティ機能。

ドメイン：

ネットワークの一部であり、共通のディレクトリ データベースを共有するコンピューターの集合。ドメインには一意の名前が付けられ、各ドメインには一連の共通の規則および手順が設定されます。

認証：

ユーザーがタスクの実行（コンピューターへのアクセス、特定のプログラムの設定変更、セキュリティ保護されたデータの表示など）を承認されているかどうかを確認するプロセス。

ネットワーク アカウント：

ローカル コンピューター上、ワークグループ内、またはドメイン上の Windows ユーザーまたは管理者のアカウント。

ブリーチ：

「空き領域ブリーチ」を参照してください。

リブート：

コンピューターを再起動するプロセス。

索引

B

BIOS 管理者パスワード 20

C

Credential Manager for
HP ProtectTools (パスワード マネージャー)

- Easy Setup 6
- アイコンの設定 40
- 機能 2
- パスワード強度 39
- 保存されている認証の表示および管理 8
- ログオン情報のカテゴリ 38
- ログオン情報の管理 39
- ログオン情報の追加 37
- ログオン情報の編集 38
- ログオン パスワード 20
- ログオン メニューの使用 38

D

Device Access Manager for
HP ProtectTools

- Easy Setup 14
- 簡易構成 48
- 機能 3
- デバイス クラス構成 49
- バックグラウンド サービス 48
- ユーザーまたはグループ、削除 49
- ユーザーまたはグループ、追加 49
- ユーザーまたはグループのアクセス拒否 50

Drive Encryption for
HP ProtectTools

- Drive Encryption の管理 34

Drive Encryption の有効化後の
ログイン 34

Easy Setup 16

- 個々のドライブの暗号化 34
- 個々のドライブの暗号化解除 34
- バックアップおよび復元 35
- バックアップ キーの作成 35
- 開く 34
- 無効化 34
- 有効化 34

E

Easy Setup Guide 4

F

[F10]セットアップ パスワード 20

File Sanitizer 45

File Sanitizer for HP ProtectTools

- Easy Setup 11
- [File Sanitizer]アイコンの使用 46
- 空き領域ブリーチの手動実行 47
- あらかじめ定義されているシュレッド プロファイル 43
- キーの組み合わせによるシュレッドの開始 45
- 起動 42
- 機能 3
- シュレッド 41
- シュレッド スケジュールの設定 43
- シュレッド操作または空き領域ブリーチ操作の停止 47
- シュレッド プロファイル 44
- シュレッド プロファイル、選択または作成 43

シンプル削除プロファイル 44

- セットアップ手順 42
- 選択されているすべてのファイルやフォルダーの手動シュレッド 46
- 単一のファイルやフォルダーの手動シュレッド 46
- ブリーチ 41
- ブリーチ スケジュールの設定 42
- ログ ファイルの表示 47

H

HP ProtectTools Security
Manager (HP ProtectTools セキュリティ マネージャー)

- Windows ユーザー名の変更 32
- アプリケーションの追加 30
- 概要 1
- 画像の変更 32
- 機能 2
- 証明情報の設定 28
- 設定 30
- デバイス アクセス 29
- ドライブの暗号化の状態 29
- パスワードの管理 28
- バックアップおよび復元 30
- ファイルのシュレッドまたはブリーチ 29

HP ProtectTools Security
Manager 管理者コンソール

- アプリケーションの設定の構成 26
- 概要 1
- 機能 2
- システムの設定 23
- デバイス アクセスの禁止 27

ドライブの暗号化 27
ユーザーの管理 25
HP ProtectTools セキュリティへの
アクセス 18
HP ProtectTools の機能 2

W

Windows のログオン
パスワード 20
Windows パスワードの変更 29

あ

アクセス
制御 48
不正の防止 19

お

お使いになる前に 4
主なセキュリティの目的 18

か

拡張タスク
Device Access Manager 49

き

機能、HP ProtectTools 2

こ

コンピューター セットアップ
(F10) ユーティリティ
管理者パスワード 20

し

シュレッド プロファイル
あらかじめ定義されている 43
カスタマイズ 44
選択または作成 43
初期セットアップ 23
シンプル削除プロファイル
カスタマイズ 44

せ

制限
機密データへのアクセス 18
デバイス アクセス 48
セキュリティ
主な目的 18
セットアップ ウィザード 23
役割 19
レベル 23
ログオン方法 23

セキュリティ セットアップ パス
ワード 20
セットアップ ウィザード
管理者 23

て

データ、アクセス制限 18
デバイス アクセスの制御 48
電源投入時パスワード
定義 20

と

ドライブの暗号化 33
ドライブの暗号化解除 33

は

パスワード
HP ProtectTools 20
安全、作成 20
ガイドライン 20
管理 20
ポリシー、作成 19
バックアップおよび復元 30
バックグラウンド サービス、
Device Access Manager 48

ふ

不正なアクセス、防止 19

も

目的、セキュリティ 18

ゆ

ユーザーの設定 23