

HP ProtectTools セキュリティ マネージャ ガ イド

HP Compaq Business Desktop



© Copyright 2006 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。

Intel および SpeedStep は、米国 Intel
Corporation の米国およびその他の国にお
ける登録商標または商標です。

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
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 セキュリティ マネージャ
ガイド

HP Compaq Business Desktop

初版 2006 年 8 月

製品番号 : 431330-291

このガイドについて

このガイドでは、HP ProtectTools セキュリティ マネージャの設定および使用方法について説明します。



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 はじめに

HP ProtectTools セキュリティ マネージャ	1
ProtectTools セキュリティ マネージャへのアクセス	1
セキュリティの役割について	2
ProtectTools のパスワードの管理	2
マルチファクタ 認証 Credential Manager のログオン	5
セキュリティ保護されたパスワードの作成	5
拡張タスク	7
ProtectTools 設定の管理	7
Java Card 起動時の認証サポートの有効化と無効化	7
Embedded Security の起動時の認証サポートの有効化と無効化	7
コンピュータ セットアップ (F10) ユーティリティのパスワードの管理	8
電源投入時パスワードの設定 (使用できる場合)	8
電源投入時パスワードの変更 (使用できる場合)	9
システム セットアップ	9
起動時の認証サポートの変更	9
ユーザ アカウントの変更	10
コンピュータ セットアップ (F10) ユーティリティの管理者パスワードの 設定	10
コンピュータ セットアップ (F10) ユーティリティの管理者パスワードの 変更	11
起動時の認証での辞書攻撃	12
辞書攻撃、防御	12

2 HP BIOS Configuration for ProtectTools

基本的な概念	13
BIOS の設定の変更	13

3 HP Embedded Security for ProtectTools

基本的な概念	15
セットアップ手順	16

4 HP Credential Manager for ProtectTools

基本的な概念	17
起動手順	17
最初のログオン	18

5 HP Java Card Security for ProtectTools

基本的な概念	19
6 他社のソリューション	
7 HP Client Manager for Remote Deployment	
背景	23
初期化	23
メンテナンス	23
8 トラブルシューティング	
Credential Manager for ProtectTools	25
Embedded Security for ProtectTools	29
その他	36
用語集	39
索引	43

1 はじめに

HP ProtectTools セキュリティ マネージャ

ProtectTools セキュリティ マネージャ ソフトウェアは、コンピュータ本体、ネットワーク、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セキュリティ機能を提供します。以下の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 BIOS Configuration for ProtectTools
- HP Embedded Security for ProtectTools
- HP Credential Manager for ProtectTools
- HP Java Card Security for ProtectTools

コンピュータで利用可能なモジュールは、モデルによって異なる可能性があります。ProtectTools モジュールは、プリインストールされている場合、コンピュータに付属の CD に収録されている場合、および HP の Web サイトから購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。



注記 ProtectTools モジュールについての詳しい説明は、ProtectTools ヘルプを参照してください。

TPM (Trusted Platform Module) を使用するには、TPM を搭載したプラットフォームに TCG ソフトウェア スタック (TSS) と Embedded Security ソフトウェアが必要です。一部のモデルには TSS が含まれていますが、含まれていない場合は HP から購入することができます。また、モデルによっては TPM 対応のソフトウェアを別途購入する必要もあります。詳しくは、「[他社のソリューション](#)」を参照してください。

ProtectTools セキュリティ マネージャへのアクセス

ProtectTools セキュリティ マネージャには、Microsoft Windows の[コントロール パネル]から次の手順でアクセスできます。

- ▲ Windows XP の場合: [スタート]→[コントロール パネル]→[セキュリティ センター]→[**ProtectTools Security Manager**] (ProtectTools セキュリティ マネージャ) の順にクリックします。
- ▲ Windows 2000 の場合: [スタート]→[すべてのプログラム]→[**HP ProtectTools Security Manager**] (HP ProtectTools セキュリティ マネージャ) の順にクリックします。



注記 Credential Manager モジュールを設定した後は、Microsoft Windows のログオン画面から直接 Credential Manager にログオンすることもできます。詳しくは、「[HP Credential Manager for ProtectTools](#)」を参照してください。

セキュリティの役割について

コンピュータのセキュリティを（特に、大きな組織で）管理する上では、責任および権限をさまざまな管理者やユーザに割り当てるのが、重要な作業の1つです。



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。

ProtectTools 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。

- セキュリティ統括責任者：企業またはネットワークのセキュリティ レベルを定義し、Java Card、指紋認証システム、USB トークンなど、配備するセキュリティ機能を決定します。



注記 ProtectTools の機能の多くは、セキュリティ統括責任者が HP と協力してカスタマイズできます。詳しくは、<http://www.hp.com/jp/>を参照してください。

- IT 管理者：セキュリティ統括責任者によって定義されたセキュリティ機能を適用し、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。たとえば、セキュリティ統括責任者が Java Card の配備を決定した場合、IT 管理者は Java Card の BIOS セキュリティ モードを有効にすることができます。
- ユーザ：セキュリティ機能を使用します。たとえば、セキュリティ統括責任者および IT 管理者がシステムで Java Card を有効にしている場合、ユーザは Java Card の PIN を設定し、そのカードを認証に使用できます。

管理者は、最善の方法でエンドユーザの権限を制限し、ユーザのアクセスを制限するようにしてください。

ProtectTools のパスワードの管理

ProtectTools セキュリティ マネージャ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。次の表に、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、IT 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、一般のユーザまたは管理者が設定できます。

表 1-1 パスワードの管理


ProtectTools のパスワード	設定する ProtectTools モジュール	機能
コンピュータ セットアップ (F10) ユーティリティの管理者パスワード	BIOS Configuration、IT 管理者が設定	BIOS のコンピュータ セットアップ (F10) ユーティリティおよびセキュリティ設定へのアクセスを保護します
 注記 BIOS の管理者パスワード、[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		
Power-On password (電源投入時パスワード)	BIOS Configuration	HP ProtectTools の起動時の認証サポートは、起動時にコンピュータへの不正アクセスを防止する目的で作られた TPM ベースのセキュリティ ツールです。起動時の認証サポートでは、HP ProtectTools Embedded Security の基本ユーザパスワードを使用します。コン

表 1-1 パスワードの管理 (続き)

		<p>コンピュータ セットアップ (F10) ユーティリティの電源認証時サポートを有効にすると、最初または次に Embedded Security の基本ユーザ キーを初期化するときに、パスワードが設定されます。Embedded Security TPM チップにより起動時の認証のパスワードが保護されま</p>
<p>Java Card の管理者パスワード</p> <p> 注記 BIOS 管理者カードのパスワードとも呼ばれます</p>	<p>Java Card セキュリティ、IT 管理者が設定</p>	<p>識別の目的で Java Card をコンピュータにリンクします</p> <p>コンピュータの管理者は、コンピュータ セットアップ (F10) ユーティリティのパスワードの有効/無効の設定、新しい管理者カードの作成、リカバリ ファイルの作成によるユーザ カードまたは管理者カードの復元ができます</p>
<p>Java Card の PIN</p>	<p>Java Card のセキュリティ</p>	<p>オプションの Java Card とリーダーが使用されている場合に、Java Card の内容やコンピュータへのアクセスを保護します。Java Card ユーザのパスワードが PIN と同じであることを確認します。このパスワードは Java Card 認証の登録に使用します</p>
<p>Java Card リカバリ ファイルのパスワード (使用できる場合)</p>	<p>Java Card のセキュリティ</p>	<p>BIOS パスワードが含まれているリカバリ ファイルへのアクセスを保護します</p>
<p>Java Card ユーザのパスワード (使用できる場合)</p> <p> 注記 BIOS ユーザ カードのパスワードとも呼ばれます</p>	<p>Java Card のセキュリティ</p>	<p>識別の目的で Java Card をコンピュータにリンクします</p> <p>ユーザがユーザ カードを復元するためのリカバリ ファイルを作成できるようにします</p>
<p>基本ユーザのパスワード</p> <p> 注記 Embedded Security パスワードまたは TPM 起動前パスワードとも呼ばれます</p>	<p>内蔵セキュリティ (Embedded Security)</p>	<p>このパスワードを使用して、安全な電子メール、ファイル、フォルダの暗号化などの Embedded Security 機能にアクセスします。BIOS 起動時の認証サポートパスワードとして有効にすると、コンピュータの起動時や再起動時、またはハイパネーションからの復帰時にコンピュータのデータを保護します。また、PSD (Personal Secure Drive) の認証と TPM 認証の登録にも使われます</p>
<p>緊急リカバリ トークンのパスワード</p> <p> 注記 緊急リカバリ トークン キーとも呼ばれます</p>	<p>Embedded Security、IT 管理者が設定</p>	<p>TPM 内蔵セキュリティ チップ用のバックアップ ファイルである緊急リカバリ トークンへのアクセスを保護します</p>
<p>所有者のパスワード</p>	<p>Embedded Security、IT 管理者が設定</p>	<p>システムと TPM チップを、Embedded Security のすべての所有者機能への不正なアクセスから保護します</p>

表 1-1 パスワードの管理 (続き)

Credential Manager のログオン パスワード	Credential Manager	このパスワードには、次の 2 つのオプションがあります
		<ul style="list-style-type: none"> Windows ログオン プロセスの代わりに使用し、Windows と Credential Manager に同時にアクセスできます Microsoft Windows にログオンした後、Credential Manager にアクセスするための別のログオンで使用できます
Credential Manager リカバリ ファイルのパスワード	Credential Manager、IT 管理者が設定	Credential Manager リカバリ ファイルへのアクセスを保護します
Windows のログオン パスワード	Windows の[コントロール パネル]	手動ログオンで使用するか、または Java Card に保存できます
バックアップ スケジューラのパスワード	Embedded Security、IT 管理者が設定	内蔵セキュリティ用のバックアップ スケジューラを設定します
 注記 内蔵セキュリティ用のバックアップ スケジューラの設定には Windows ユーザのパスワードが使われます		
PKCS#12 のインポート パスワード	Embedded Security、IT 管理者が設定	他の証明書からの暗号化キーに使用するパスワード (インポートされた場合)
 注記 インポートされた証明書にはそれぞれ固有のパスワードがあります		 注記 通常のソフトウェア操作では必要ありませんが、内蔵セキュリティを使用して重要な証明書を送信する場合にこのパスワードの設定を選択できます
パスワード リセット トークン	Embedded Security、IT 管理者が設定	基本ユーザのパスワードがわからなくなった場合に、所有者がそのパスワードをリセットできるように提供されたツール。このリセット操作にパスワードが使われます
Microsoft Recovery Agent の管理者パスワード	Microsoft、IT セキュリティ管理者が設定	PSD (Personal Secure Drive) の暗号化データを回復できるようにします。詳しくは、 http://www.microsoft.com/technet/prodtechnol/winxp/pro/support/dataprot.mspix (英語サイト) を参照してください
 注記 任意のローカル コンピュータの管理者を Recovery Agent とすることができます。Recovery Agent が作成されると、その管理者としてログインする必要があり、パスワードが必要になります。Recovery Agent は、暗号化されたすべてのユーザ データを開くだけで暗号化解除できます (ウィザードは不要です)		 注記 通常のソフトウェア操作では必要ありませんが、内蔵セキュリティを使用して重要な証明書を送信する場合にこのパスワードの設定を選択できます
仮想トークンのマスタ PIN	Credential Manager	Credential Manager を使用して所有者の証明書を格納するカスタム オプション
仮想トークンのユーザ PIN	Credential Manager	Credential Manager を使用して所有者の証明書を格納するカスタム オプション

表 1-1 パスワードの管理 (続き)

ID のバックアップ ウィザードパスワード	Credential Manager、IT 管理者が設定	Credential Manager を使用するとき、ID バックアップへのアクセスの保護に使用します
仮想トークンの認証パスワード	Credential Manager	Credential Manager が仮想トークンの認証の登録に使用します
TPM 認証の別名	Credential Manager	管理者またはユーザの任意で、Credential Manager が基本ユーザのパスワードの代わりに使用します
指紋認証ログオン	Credential Manager	Credential Manager では、Windows パスワードによるログオンの代わりに、便利で安全な指紋認証ログオンを使用できます。指紋認証証明は、パスワードとは異なり、共有したり他人に渡したりできません。また盗まれることも推測されることもありません。Credential Manager が使用します
USB トークンの認証	Credential Manager	Credential Manager がパスワードの代わりにトークン認証として使用します

マルチファクタ認証 Credential Manager のログオン

Credential Manager ログオンにより、Windows オペレーティング システムにログオンするためのマルチファクタ認証テクノロジーが実現します。強力なマルチファクタ認証を必要とするため、標準の Windows パスワードによるログオンよりも安全性が高まります。また、各種ユーザ パスワードを覚えておく必要がないため、毎日のログオン作業がより簡便になります。Credential Manager ログオンの特徴は、複数のアカウント認証情報を 1 つのユーザ ID にまとめられることです。これにより、マルチファクタ認証を 1 回だけ使用すれば、同じ証明書セットを使用した異なる Windows アカウントへのマルチアクセスが可能になります。

マルチファクタ ユーザ認証では、ユーザパスワード、動的またはシングル ユース パスワード、TPM、Java Card、USB トークン、仮想トークン、指紋認証のうち、どの組み合わせもサポートされます。また、Credential Manager は、同一アプリケーションまたはサービスに対するユーザのマルチ アクセス権限を可能にする代替認証方法もサポートします。ユーザは、すべての証明書、アプリケーションパスワード、ネットワーク アカウントをユーザ ID と呼ばれる 1 つのデータ ユニットに統合できます。ユーザ ID は、マルチファクタ認証を使用して常に暗号化され保護されます。

セキュリティ保護されたパスワードの作成

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考慮してください。

- 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、「Mary22Cat45」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次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。

拡張タスク

ProtectTools 設定の管理

一部の ProtectTools セキュリティ マネージャ機能は、BIOS Configuration で管理できます。

Java Card 起動時の認証サポートの有効化と無効化

このオプションが利用できる場合、このオプションを有効にするとコンピュータの電源を投入するときに Java Card を使用してユーザ認証を行うことができます。



注記 起動時の認証機能を完全に有効にするには、Java Card Security for ProtectTools モジュールを使用して Java Card も設定する必要があります。

Java Card の起動時の認証サポートを有効にするには、次の手順で操作します。

1. [スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager] (HP ProtectTools セキュリティ マネージャ) の順に選択します。
2. 左側のパネルで、[BIOS Configuration] (BIOS 設定) を選択します。
3. コンピュータ セットアップ (F10) ユーティリティの管理者パスワードを BIOS 管理者パスワードの入力画面に入力して、[OK]をクリックします。
4. 左側のパネルで、[Security] (セキュリティ) を選択します。
5. [Java Card Security]で、[Enable] (有効) を選択します。



注記 Java Card の起動時の認証サポートを無効にするには、[Disable] (無効) を選択します。

6. [Apply] (適用) をクリックし、[ProtectTools]ウィンドウの[OK]をクリックして変更を保存します。

Embedded Security の起動時の認証サポートの有効化と無効化

このオプションが利用できる場合、このオプションを有効にすると、コンピュータの電源を投入するときに TPM 内蔵セキュリティ チップを使用してユーザ認証を行うことができます。



注記 起動時の認証機能を完全に有効にするには、Embedded Security for ProtectTools モジュールを使用して TPM 内蔵セキュリティ チップも設定する必要があります。

内蔵セキュリティの起動時の認証サポートを有効にするには、次の手順で操作します。

1. [スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager] (HP ProtectTools セキュリティ マネージャ) の順に選択します。
2. 左側のパネルで、[BIOS Configuration]を選択します。
3. コンピュータ セットアップ (F10) ユーティリティの管理者パスワードを BIOS 管理者パスワードの入力画面に入力して、[OK]をクリックします。
4. 左側のパネルで、[Security] (セキュリティ) を選択します。
5. [Embedded Security] (内蔵セキュリティ) で、[Enable Power-On Authentication Support] (起動時の認証有効) を選択します。



注記 Embedded Security の起動時の認証サポートを無効にするには、**[Disable]**（無効）を選択します。

6. **[Apply]**（適用）をクリックし、**[ProtectTools]**ウィンドウの**[OK]**をクリックして変更を保存します。

コンピュータ セットアップ（F10）ユーティリティのパスワードの管理

BIOS Configuration を使用すると、コンピュータ セットアップ（F10）ユーティリティの電源投入時パスワードやセットアップパスワードの設定および変更を行うことができるほか、さまざまなパスワード設定も管理できます。



注意 BIOS Configuration の**[Passwords]**（パスワード）ページで設定したパスワードは、**[ProtectTools]**ウィンドウの**[Apply]**（適用）または**[OK]**ボタンをクリックすると、直ちに保存されます。パスワード設定を元に戻すには、以前のパスワードを指定する必要があるため、設定したパスワードは必ず覚えておくようしてください。

電源投入時パスワードは、コンピュータを不正な使用から保護できます。



注記 電源投入時パスワードを設定すると、**[Passwords]**（パスワード）ページの**[Set]**（設定）ボタンが**[Change]**（変更）ボタンに変わります。

コンピュータ セットアップ（F10）ユーティリティの管理者パスワードは、コンピュータ セットアップ（F10）ユーティリティの設定値とシステム識別情報を保護します。いったんこのパスワードを設定すると、コンピュータ セットアップ（F10）ユーティリティにアクセスするにはパスワードの入力が必要になります。

管理者パスワードを設定している場合は、ProtectTools の BIOS Configuration の部分を起動する前にパスワードを入力するよう要求されます。



注記 管理者パスワードを設定すると、**[Passwords]**（パスワード）ページの**[Set]**（設定）ボタンが**[Change]**（変更）ボタンに変わります。

電源投入時パスワードの設定（使用できる場合）

電源投入時パスワードを設定するには、以下の手順で操作します。

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]**（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]**を選択し、**[Security]**（セキュリティ）を選択します。
3. 右側のパネルで、**[Power-On Password]**（電源投入時パスワード）の横にある**[Set]**（設定）をクリックします。
4. **[Enter Password]**（パスワードの入力）ボックスと**[Verify Password]**（パスワードの確認）ボックスにパスワードを入力して確定します。
5. **[Passwords]**（パスワード）ダイアログボックスで**[OK]**をクリックします。
6. **[Apply]**（適用）をクリックし、**[ProtectTools]**ウィンドウの**[OK]**をクリックして変更を保存します。

電源投入時パスワードの変更（使用できる場合）

電源投入時パスワードを変更するには、以下の手順で操作します。

1. [スタート]→[すべてのプログラム]→[HP ProtectTools Security Manager]（HP ProtectTools セキュリティ マネージャ）の順に選択します。
2. 左側のパネルで、[BIOS Configuration]（BIOS 設定）→[Security]（セキュリティ）の順に選択します。
3. 右側のパネルで、[Power-On Password]（電源投入時パスワード）の横にある[Change]（変更）をクリックします。
4. 現在のパスワードを[Old Password]（古いパスワード）ボックスに入力します。
5. [Enter New Password]（新しいパスワードの入力）ボックスと[Verify New Password]（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て確定します。
6. [パスワード]ダイアログ ボックスで[OK]をクリックします。
7. [Apply]（適用）をクリックし、[ProtectTools]ウィンドウの[OK]をクリックして変更を保存します。

システム セットアップ

1. HP ProtectTools Embedded Security を初期化します。
2. 基本ユーザ キーを初期化します。

電源投入時の基本ユーザ キーと基本ユーザ パスワードが設定されると、HP 起動時の認証サポートが直ちに開始されます。次の再起動後に、HP ProtectTools の起動時の認証サポートが初期化されるので、コンピュータを開始するには基本ユーザ パスワードを使用する必要があります。起動時の認証サポートが機能すると、BIOS セットアップに入るオプションは表示されなくなります。[起動時の認証サポート]ウィンドウでセットアップ パスワードを入力すると、BIOS が表示されます。

Embedded Security の基本ユーザ パスワードがすでに設定されている場合は、起動時の認証を使用してパスワードを変更し、パスワード保護を確立する必要があります。

起動時の認証サポートの変更

パスワードの起動時の認証サポートでは、内蔵の基本ユーザ パスワードを使用します。パスワードを変更するには、以下の手順で操作します。

1. コンピュータ セットアップ（F10）ユーティリティの BIOS 設定に入り（前のセットアップの手順で述べたセットアップ パスワードが必要です）、[セキュリティ]（Security）→[Embedded Security Device]（内蔵セキュリティ デバイス）→[Reset authentication credential]（認証資格情報のリセット）の順に選択します。
2. 矢印キーを押して、設定を[Do not reset]（リセットしません）から[Reset]（リセットします）に変更します。
3. [Security Manager]（セキュリティ マネージャ）→[Embedded Security]（内蔵セキュリティ）→[User Settings]（ユーザ設定）→[Basic User Password]（基本ユーザ パスワード）→[Change]（変更）の順に選択します。
4. 古いパスワードを入力し、次に新しいパスワードを入力して確定します。
5. 再起動して起動時の認証サポートに入ります。

パスワード ウィンドウでは、最初に古いパスワードの入力が要求されます。

6. 古いパスワードを入力し、次に新しいパスワードを入力します。(新しいパスワードの入力を3回間違えると、新しいウィンドウが表示されます。これは、パスワードが無効のため起動時の認証が元の内蔵セキュリティ パスワード F1 = Boot に戻ることを意味します。

この時点で、パスワードは同期されません。したがって、内蔵セキュリティ パスワードを再度変更して再同期する必要があります)。

ユーザ アカウントの変更

起動時の認証サポートでは、一度に1ユーザだけがサポートされます。以下の手順に従って、起動時の認証を制御するユーザ アカウントを変更します。

1. **[F10 BIOS]**→**[Security]** (セキュリティ) →**[Embedded Security Device]** (内蔵セキュリティ デバイス) →**[Reset authentication credential]** (認証資格情報のリセット) の順に選択します。
2. 上下の矢印キーを押してカーソルを横方向に移動し、任意のキーを押して続行します。
3. **F10** キーを2回押し、次に **Enter** キーを押して変更を保存し、終了します。
4. Microsoft Windows ユーザを作成するか、変更する Microsoft Windows ユーザでログオンします。
5. Embedded Security を起動し、新しい Windows ユーザ アカウントの基本ユーザ キーを初期化します。基本ユーザ キーがすでにある場合は、基本ユーザ パスワードを変更して、起動時の認証のオーナーシップを取得します。

この時点では、起動時の認証サポートは、新しいユーザの基本ユーザ パスワードのみを許可します。



注意 ソフトウェア暗号化、ハードウェア暗号化、ハードウェアなどを使用してデータを保護する製品は多数あります。ほとんどの場合、パスワードを使用して管理されます。これらのツールとパスワードの管理に失敗すると、交換するまでにデータの損失やハードウェアのロックアウトなどを引き起こす可能性があります。適切なヘルプ ファイルをすべて参照してから、これらのツールを使用するようにしてください。

コンピュータ セットアップ (F10) ユーティリティの管理者パスワードの設定

コンピュータ セットアップ (F10) ユーティリティの管理者パスワードを設定するには、次の手順で操作します。

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]** (HP ProtectTools セキュリティ マネージャ) の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]** (BIOS 設定) →**[Security]** (セキュリティ) の順に選択します。
3. 右側のパネルで、**[Setup Password]** (セットアップ パスワード) の横にある**[Set]** (設定) をクリックします。
4. **[Enter Password]** (パスワードの入力) ボックスと**[Confirm Password]** (パスワードの確認) ボックスにパスワードを入力して確定します。
5. **[Password]** (パスワード) ダイアログ ボックスで**[OK]**をクリックします。
6. **[Apply]** (適用) をクリックし、**[ProtectTools]** ウィンドウの**[OK]**をクリックして変更を保存します。

コンピュータ セットアップ (F10) ユーティリティの管理者パスワードの変更

コンピュータ セットアップ (F10) ユーティリティの管理者パスワードを変更するには、次の手順で操作します。

1. **[スタート]**→**[すべてのプログラム]**→**[HP ProtectTools Security Manager]** (HP ProtectTools セキュリティ マネージャ) の順に選択します。
2. 左側のパネルで、**[BIOS Configuration]** (BIOS 設定) →**[Security]** (セキュリティ) の順に選択します。
3. 右側のパネルで、**[Setup Password]** (セットアップ パスワード) の横にある**[Set]** (設定) をクリックします。
4. 現在のパスワードを**[Old Password]** (古いパスワード) ボックスに入力します。
5. **[Enter New Password]** (新しいパスワードの入力) ボックスと**[Verify New Password]** (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て確定します。
6. **[Password]** (パスワード) ダイアログ ボックスで**[OK]**をクリックします。
7. **[Apply]** (適用) をクリックし、**[ProtectTools]**ウィンドウの**[OK]**をクリックして変更を保存します。

起動時の認証での辞書攻撃

辞書攻撃とは、セキュリティ システムへの侵入に使われる手法で、可能性のあるすべてのパスワードを定期的に検査することで、セキュリティ システムを突破します。辞書攻撃により、Embedded Security に対して、所有者のパスワード、基本ユーザのパスワード、またはパスワード保護キーの検出が試みられる可能性があります。Embedded Security には、辞書攻撃に対する拡張防御機能があります。

辞書攻撃、防御

Embedded Security では、失敗した認証を検出し、その回数が特定のしきい値に達した場合に一時的に TPM を無効にすることで、辞書攻撃に対する防御を行います。一度この障害しきい値に達すると、TPM が無効になり再起動が必要になるだけでなく、常に増加を続けるロックアウト タイムアウトが適用されます。タイムアウトの間は、正しいパスワードの入力も無視されます。不正なパスワードが入力された場合は、タイムアウト時間は、最後のタイムアウト時間の 2 倍になります。

このプロセスについて詳しくは、Embedded Security のヘルプを参照してください。[Welcome to the HP Embedded Security for ProtectTools Solution] (HP Embedded Security for ProtectTools ソリューションへようこそ) → [Advanced Embedded Security Operation] (拡張内蔵セキュリティ操作) → [Dictionary Attack Defense] (辞書攻撃防御) の順にクリックします。



注記 通常の場合、不正なパスワードが入力されると、ユーザに警告が表示されます。警告には、TPM が TPM 自体を無効にするまで、ユーザは残り何回パスワードの入力を行えるかが示されます。

起動時の認証は、OS (オペレーティング システム) がロードされる前に ROM 内で実行されます。辞書攻撃防御はオプションですが、ユーザに表示される警告は、X 記号のみになります。

2 HP BIOS Configuration for ProtectTools

基本的な概念

BIOS Configuration for ProtectTools を使用すると、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設定にアクセスできます。これにより、コンピュータ セットアップ (F10) ユーティリティで管理されるシステムのセキュリティ機能に Windows から簡単にアクセスできるようになります。

BIOS Configuration を使用すると、次のことができます。

- 電源投入時パスワードおよび管理者パスワードを管理できます。
- Java Card のパスワードや内蔵セキュリティ認証サポートを有効にするなど、他の利用可能な起動時の認証機能を設定できます。
- CD-ROM のブートや各種ハードウェア ポートなど、ハードウェア機能を有効または無効に設定できます。
- マルチブートの有効設定や起動順序の変更など、起動オプションを設定できます。



注記 BIOS Configuration for ProtectTools にある機能の多くは、コンピュータ セットアップ (F10) ユーティリティでも使用できます。

BIOS の設定の変更

BIOS Configuration を使用すると、通常は起動時に **F10** キーを押してコンピュータ セットアップ (F10) ユーティリティを使用することでしかアクセスできない、各種のコンピュータ設定を管理できます。設定と機能について詳しくは、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。BIOS Configuration のヘルプ ファイルにアクセスするには、**[Security Manager]** (セキュリティ マネージャ) → **[BIOS Configuration]** (BIOS 設定) → **[Help]** (ヘルプ) の順にクリックします。



注記 ProtectTools BIOS Configuration について詳しくは、ProtectTools ヘルプを参照してください。

3 HP Embedded Security for ProtectTools

基本的な概念

Embedded Security for ProtectTools が利用可能な場合、ユーザ データや証明書が不正なアクセスから保護されます。このモジュールには、以下のセキュリティ機能があります。

- 高度な Microsoft EFS (Encrypting File System) ファイルおよびフォルダの暗号化
- ユーザ データを暗号化するための PSD (Personal Secure Drive) の作成
- データ管理機能 (キー階層のバックアップや復元など)
- Embedded Security ソフトウェアの使用時にデジタル証明書の操作を保護するための、MSCAPI を使用した他社製のアプリケーション (Microsoft Outlook や Internet Explorer など) および PKCS#11 を使用したアプリケーション (Netscape など) のサポート

TPM (Trusted Platform Module) 内蔵セキュリティ チップを使用すると、ProtectTools セキュリティ マネージャの他のセキュリティ機能を強化したり有効にしたりできます。たとえば、Credential Manager for ProtectTools では、TPM 内蔵チップを Windows へのログオン時の認証要素として使用できます。一部のモデルでは、TPM 内蔵セキュリティ チップを使用して、BIOS Configuration for ProtectTools からアクセスする高度な BIOS セキュリティ機能を有効にすることもできます。

ハードウェアは、Trusted Computing Group による TPM 1.2 標準の要件を満たす TPM で構成されます。このチップはシステム ボードに搭載されています。一部の TPM 実装では、(購入モデルによっては) NIC の一部として TPM が搭載されています。このような NIC や TPM の設定では、オンチップ メモリとオフチップ メモリ、機能、およびファームウェアは、システムボードに内蔵されている外部フラッシュ メモリに格納されます。TPM のすべての機能は、フラッシュ メモリと通信の安全を確保するために暗号化または保護されます。

また、PSD (Personal Secure Drive) という機能も提供されます。PSD は、EFS ベースのファイル/フォルダの暗号化に付け加えられた機能で、AES (Advanced Encryption Standard) 暗号化アルゴリズムを使用します。HP ProtectTools Personal Secure Drive が機能するためには、TPM が再表示されて、所有権のあるインストール済みの適切なソフトウェアを使用して有効になっており、ユーザ設定が初期化されている必要があります。

セットアップ手順



注意 セキュリティ上の危険にさらされないようにするために、IT 管理者が TPM 内蔵セキュリティ チップを直ちに初期化することを強くおすすめします。TPM 内蔵セキュリティ チップを初期化しない場合、不正なユーザやコンピュータ ワームがコンピュータにアクセスしたり、ウイルスが TPM 内蔵セキュリティ チップを初期化してコンピュータへのアクセス権を制限したりする可能性があります。

TPM 内蔵セキュリティ チップは、BIOS のコンピュータ セットアップ (F10) ユーティリティ、BIOS Configuration for ProtectTools、または HP Client Manager で有効にできます。

TPM 内蔵セキュリティ チップを有効にするには、以下の手順で操作します。

1. コンピュータの電源を入れるか再起動し、画面の左下隅に**[F10=ROM Based Setup]**メッセージが表示されている間に **F10** キーを押して、コンピュータ セットアップ (F10) ユーティリティを起動します。
2. 矢印キーを使用し、**[セキュリティ]** (Security) → **[セットアップ パスワード]** (Setup Password) の順に選択します。パスワードを設定します。
3. **[内蔵セキュリティ デバイス]** (Embedded Security Device) を選択します。
4. 矢印キーを使用して、**[無効]** (Embedded Security Device-Disable) を選択します。矢印キーを使用して、**[有効]** (Embedded Security Device-Enable) に変更します。
5. **[有効]** (Enable) → **[変更を保存して終了]** (Save changes and exit) の順に選択します。



注記 ProtectTools Embedded Security について詳しくは、ProtectTools のヘルプを参照してください。

4 HP Credential Manager for ProtectTools

基本的な概念

Credential Manager for ProtectTools では、安全で便利なコンピュータの使用環境を提供します。これらのセキュリティ機能には、以下のものが含まれます。

- Microsoft Windows へのログオン時のパスワードに代わる Java Card や指紋認証システムの使用などの代替機能
- Web サイト、アプリケーション、および保護されたネットワーク リソースでの証明書（ユーザー ID およびパスワード）を自動的に記憶するシングルサインオン機能
- Java Card や指紋認証システムなどの、オプションのセキュリティ デバイスのサポート
- コンピュータのロック解除およびアプリケーションへのアクセスにはオプションのセキュリティ デバイスでの認証を必要とするなどの、追加のセキュリティ設定のサポート
- TPM 内蔵セキュリティ チップが実装されている場合、保存されたパスワードのための強化された暗号化機能

起動手順

Credential Manager（利用できる場合）を起動するには、次の手順で操作します。

1. [スタート]→[コントロールパネル]→[セキュリティ センター]→[ProtectTools Security Manager] (ProtectTools セキュリティ マネージャ) →[Credential Manager]の順にクリックします。
2. パネルの右上隅にある[Log On]（ログオン）をクリックします。

以下のどれかの方法で Credential Manager にログオンできます。

- [Credential Manager Logon Wizard]（証明書マネージャ ログオン ウィザード）（推奨）
- ProtectTools セキュリティ マネージャ



注記 Windows のログオン画面の Credential Manager ログオン プロンプトを使用して Credential Manager にログオンすると、同時に Windows にもログオンします。

最初のログオン

最初に Credential Manager を起動するときは、通常の Windows ログオン パスワードでログオンします。その後、Credential Manager アカウントが、Windows のログオン証明書を使用して自動的に作成されます。

Credential Manager にログオンした後で、指紋や Java Card などの、追加の証明書を登録できます。

次のログオン時には、ログオン ポリシーを選択して、登録された証明書の任意の組み合わせを使用することができます。



注記 ProtectTools セキュリティ マネージャについては、ProtectTools のヘルプを参照してください。

5 HP Java Card Security for ProtectTools

基本的な概念

Java Card Security for ProtectTools は、別売の Java Card リーダーが装備されたコンピュータでの Java Card のセットアップおよび設定を管理します。

Java Card Security for ProtectTools を使用すると、次のことができます。

- Java Card のセキュリティ機能にアクセスできます。
- Credential Manager for ProtectTools などの他の ProtectTools モジュールで使用できるように Java Card を初期化できます。
- ブート前の環境でコンピュータ セットアップ (F10) ユーティリティを使用して Java Card の認証を可能にし、また Java Card を管理者用とユーザ用に分けて設定できます (利用できる場合)。これにより、オペレーティング システムをロードさせるには、ユーザが Java Card を挿入し PIN を入力することが必要となります (PIN の入力オプションです)。
- Java Card のユーザ認証を行うためのパスワードの設定および変更を行えます (利用できる場合)。
- Java Card に格納されている Java Card の BIOS パスワードのバックアップおよびリストア (復元) を行えます (利用できる場合)。
- Java Card に BIOS パスワードを保存できます (利用できる場合)。



注記 ProtectTools セキュリティ マネージャについて詳しくは、ProtectTools のヘルプを参照してください。

6 他社のソリューション

TPM を搭載するプラットフォームには、TSS (TCG ソフトウェア スタック) と Embedded Security ソフトウェアが必要です。すべてのモデルで TSS は提供されますが、一部のモデルでは Embedded Security ソフトウェアを別途購入する必要があります。このようなモデルには、NTRU TSS が提供されているため、他社製の Embedded Security ソフトウェアを購入することもできます。他社製のソリューションについては、Wave Embassy Trust Suiteなどを推奨します。

7 HP Client Manager for Remote Deployment

背景

TPM (Trusted Platform Module) を搭載した信頼性の高い HP のプラットフォームは、TPM を無効にした状態で出荷されます。TPM は、HP の BIOS 強制ポリシーにより保護された管理オプションを選択することで有効にできます。BIOS Configuration オプション (F10 オプション) を入力して、TPM を有効にできる管理者が必要です。さらに、TCG (Trusted Computing Group) 仕様では、TPM を有効にするには人による (物理的な) 明確な介入が必要とされます。この条件により、ユーザのプライバシーが保護されます (オプトイン モデルを提供する必要があります)。また、不良アプリケーション、ウィルス、トロイの木馬などが TPM を有効にして悪用することもできなくなります。物理的な介入の確立とローカルでの管理者の介入が必要とされるため、大規模な企業内でこのテクノロジーを展開しようとする IT マネージャには、難題がもたらされることとなります。

初期化

HPCM (HP Client Manager) は、企業環境内において、リモートで TPM を有効にする手段と TPM の所有権を取得する手段を備えています。この手段は、IT 管理者の物理的介入を必要としませんが、それでも TCG 要件は満たされています。

HPCM を使用すれば、IT 管理者は、リモート システムの特定の BIOS オプションを設定し、システムを再起動して TPM を有効にできます。再起動中に、BIOS はデフォルトでプロンプト画面を表示します。エンド ユーザはそれに応じて任意のキーを押し、TCG で指示されている物理的介入を行ったことを証明する必要があります。次に、リモート システムはブートを続行します。スクリプトは、システムの TPM の所有権を取得して完了します。この手順を実行している間に、緊急リカバリ アーカイブと緊急リカバリ トークンが作成され、IT 管理者が指定した場所に保存されます。

パスワードはユーザに選択させる必要があるため、HPCM ではリモート システムの TPM ユーザの初期化は行いません。TPM ユーザの初期化は、そのシステムのエンド ユーザが実行する必要があります。

メンテナンス


HP Client Manager を使用すれば、IT 管理者がユーザのパスワードを知らなくても、リモートでそのユーザのパスワードをリセットできます。また、HPCM ではリモートでユーザの証明書を復元することもできます。これらの機能それぞれに適切な管理者パスワードを設定する必要があります。

8 トラブルシューティング

Credential Manager for ProtectTools

簡単な説明	詳しい説明	解決方法
Credential Manager の [Network Accounts] (ネットワーク アカウント) オプションを使用すると、ログインするドメイン アカウントを選択できる。TPM 認証を使用する場合、このオプションは使用できない。他の認証方式はすべて正常に機能する	TPM 認証を使用する場合、ユーザがログインできるのはローカル コンピュータだけです	Credential Manager のシングルサインオン ツールを使用すると、他のアカウントも認証できます
Windows XP SP1 へのログインで、USB トークンの証明書を使用できない	USB トークン ソフトウェアをインストールし、USB トークンの証明書を登録し、Credential Manager をプライマリ ログインとして設定しても、USB トークンはリストに表示されません。また、Credential Manager/gina ログオンで使用することもできません Windows に再度ログインして、Credential Manager からログオフし、もう一度 Credential Manager にログインして、トークンをプライマリ ログインとして再選択すると、トークン ログイン操作が正常に機能します	この現象は、Windows XP Service Pack 1 でのみ発生します。Windows Update を使用して、Windows XP のバージョンを Service Pack 2 に更新すると問題は解決されます Service Pack 1 のままでこの問題を回避するには、別の証明書 (Windows パスワード) を使用して Windows に再度ログインしてから、Credential Manager からログオフし、もう一度 Credential Manager にログインします
一部のアプリケーションの Web ページにエラーが表示され、タスクの実行や完了が不可能になる	シングルサインオンの機能パターンが無効になったことが原因で、一部の Web ベース アプリケーションが機能しなくなりエラーを報告します。たとえば、Internet Explorer では、黄色の三角形の中に [!] のマークが表示され、エラーの発生を通知します	Credential Manager シングルサインオンは、すべてのソフトウェア Web インタフェースをサポートするわけではありません。特定の Web ページでは、シングルサインオン サポートをオフにして、シングルサインオン サポートを無効にしてください。Credential Manager のヘルプ ファイルに用意されている、シングルサインオンについての詳しいドキュメントを参照してください 特定のアプリケーションでシングルサインオンを無効にできない場合は、HP のサポート窓口にお問い合わせください
ログイン プロセスで、 [Browse for Virtual Token] (仮想トークンの参照) オプションが表示されない	Credential Manager では、セキュリティ リスクを避けるために、参照オプションが削除されたため、ユーザは登録した仮想トークンの位置を移動できません	参照オプションを使用できると、ユーザ以外がファイルの削除や名前の変更を行って Windows を制御できるようになるため、今回の製品からは、参照オプションは削除されています


簡単な説明	詳しい説明	解決方法
TPM 認証でログインする場合、 [Network Accounts] (ネットワーク アカウント) オプションが提供されない	[Network Accounts] (ネットワーク アカウント) オプションを使用すると、ログインするドメイン アカウントを選択できます。TPM 認証を使用する場合、このオプションは使用できません	HP では、将来の製品の機能強化に生かせるように、回避策を調査中です
権限がある場合でも、ドメイン管理者が Windows パスワードを変更できない	これは、ドメイン管理者がドメインにログオンし、ドメインとローカル コンピュータで管理者の権限をもつアカウントを使用して、ドメイン ID を Credential Manager に登録した後で発生します。ドメイン管理者が、Credential Manager から Windows のパスワードを変更しようとする、ログオンの失敗を示す次のようなエラー メッセージが表示されます。 [User account restriction] (ユーザー アカウントの制限)	Credential Manager が [Change Windows password] (Windows パスワードを変更する) を使用して、ドメイン ユーザのアカウント パスワードを変更することはできません。Credential Manager が変更できるのは、ローカル コンピュータのアカウント パスワードだけです。ドメイン ユーザは、 [Windows security] (Windows セキュリティ) → [Change password] (パスワードを変更する) オプションを使用して自身のパスワードを変更できますが、ドメイン ユーザはローカル コンピュータに実質的なアカウントを持っていないため、Credential Manager が変更できるのはログインに使用するパスワードだけです
Credential Manager シングルサインオンのデフォルト設定を、ループを防止するメッセージを表示するように設定する必要があります	シングルサインオンのデフォルト設定は、ユーザは自動的にログに記録されません。ただし、パスワード保護された 2 つの異なるドキュメントを作成する場合、2 つ目を作成するときに、Credential Manager は、最後に記録されたパスワード、つまり最初のドキュメントのパスワードを使用します	HP では、将来の製品の機能強化に生かせるように、回避策を調査中です
Corel WordPerfect 12 のパスワード gina に対応していない問題	ユーザが Credential Manager にログインして、WordPerfect でドキュメントを作成し、パスワード保護を使用して保存した場合、Credential Manager は、パスワード gina を手動でも自動でも検出または認識できません	HP では、将来の製品の機能強化に生かせるように、回避策を調査中です
Credential Manager が画面の [Connect] (接続) ボタンを認識しない	リモート デスクトップ接続 (RDP) のシングルサインオン証明書が、 [Connect] (接続) に設定されている場合でも、再起動時のシングルサインオンでは、常に [Connect] (接続) ではなく [Save as] (名前を付けて保存) が入力されます	HP では、将来の製品の機能強化に生かせるように、回避策を調査中です
Credential Manager と共に ATI Catalyst 設定ウィザードを使用できない	Credential Manager のシングルサインオンは、ATI Catalyst 設定ウィザードと競合します	Credential Manager のシングルサインオンを無効にしてください
TPM 認証を使用してログインすると、画面の [Back] (戻る) ボタンが別の認証方式を選択するためのオプションをスキップする	Credential Manager の TPM ログイン認証を使用するユーザが、自身のパスワードを入力する場合、 [Back] (戻る) ボタンは正常に機能しませんが、Windows のログイン画面はすぐに表示されます	HP では、将来の製品の機能強化に生かせるように、回避策を調査中です
Credential Manager がスタンバイ モードから起動しないように設定されている場合でも、スタンバイから起動する	オプションで [use Credential Manager log on to Windows] (Credential Manager の Windows へのログオンを使用する) が選択されていない場合でも、システムが S3 サスペンドに入るのを許可してからシステムをサスペンドからウエイクアップすると、Credential Manager の Windows へのログオンが開きます	この場合、管理者パスワードが設定されていないと、Credential Manager が実行するアカウント制限により、ユーザは、Credential Manager を介して Windows にログオンできません <ul style="list-style-type: none"> Java Card またはトークンがない場合、ユーザは、Credential Manager ログインを取り消すことができ、この場合、Microsoft Windows ログイン

簡単な説明	詳しい説明	解決方法
		<p>が表示されます。ユーザはこの時点でログインできます</p> <ul style="list-style-type: none"> • Java Card またはトークンがある場合、次の回避策をとると、Java Card 挿入時の Credential Manager の起動を有効または無効にすることができます <ol style="list-style-type: none"> 1. [Advanced Settings] (詳細設定) をクリックします 2. [Service & Application] (サービスおよびアプリケーション) をクリックします 3. [Java Cards and Tokens] (Java Card およびトークン) をクリックします 4. Java Card/トークンを挿入したらクリックします 5. [Advise to log-on] (ログオンをアドバイスする) チェックボックスにチェックを入れます
<p>TPM モジュールが取り外されたり破損したりすると、TPM によって保護されていた Credential Manager 証明書がすべて失われる</p>	<p>TPM モジュールが取り外されたり破損したりすると、TPM が保護する証明書がすべて失われます</p>	<p>これは仕様です</p> <p>TPM モジュールは、Credential Manager の証明書を保護するように設計されています。TPM モジュールを取り外す前に、Credential Manager の ID 情報をバックアップすることをおすすめします</p>
<p>Windows 2000 で、Credential Manager がプライマリ ログオンとして設定されない</p>	<p>Windows 2000 のインストール時、ログオン ポリシーは手動または自動のログオンによる管理に設定されます。自動ログオンが選択されている場合、Windows のデフォルト レジストリ設定では、デフォルト AutoAdminLogon 値が「1」に設定され、Credential Manager はこの値を無効にしません</p>	<p>これは仕様です</p> <p>バイパスのための AutoAdminLogon 値のオペレーティング システム レベル設定を変更する場合、編集パスは次のとおりです。HKEY_LOCAL_MACHINE/Software/Microsoft/WindowsNT/CurrentVersion/WinLogon</p>
		<p> 注意 レジストリ エディタを使用して、ご自身の責任で編集してください。レジストリ エディタ (regedit) の使用法を誤ると、重大な問題が発生して、オペレーティング システムの再インストールが必要になる場合があります。レジストリ エディタの使用法を誤って問題が発生した場合、その問題を解決できる保証はありません</p>
<p>指紋認証システムが設置または登録されているかどうかに関係なく、指紋認証ログオン メッセージが表示される</p>	<p>ユーザが Windows ログオンを選択する場合、Credential Manager のタスク バーに次の警告が表示されます。[You can place your finger on the fingerprint reader to log on to Credential Manager] (指紋認証システムの上に指を置くと、Credential Manager にログオンできます)</p>	<p>この警告の目的は、指紋認証が設定されている場合、この認証方式を利用できることをユーザに示すことです</p>
<p>リーダーが接続されていないのに、Windows 2000 用の Credential Manager ログオン ウィンドウに [insert card] (カードを挿入してください) と表示される</p>	<p>Java Card リーダーが接続されていない場合でも、Windows の Credential Manager の[Welcome] (ようこそ) 画面に[insert card] (カードを挿入してください) と表示され、ユーザがカードを挿入してログオンできることが示されます</p>	<p>この警告の目的は、Java Card 認証が設定されている場合、この認証方式を利用できることをユーザに示すことです</p>

簡単な説明	詳しい説明	解決方法
Windows XP Service Pack 1 (このバージョンのみ) でスリープモードからハイバネーションに移ると、Credential Manager にログインできなくなる	システムをハイバネーションやスリープモードに移行できるように設定すると、どのログイン証明書(パスワード、指紋、または Java Card) が選択されている場合でも、管理者またはユーザは Credential Manager にログインできなくなり、Windows のログイン画面が表示されたままになります	<p>この問題は、Microsoft 社の提供する Service Pack 2 で解決されたようです。この問題の原因については、http://www.microsoft.com/japan/で、Microsoft サポート技術情報の記事 813301 を参照してください</p> <p>ログインするには、Credential Manager を選択してログインする必要があります。Credential Manager にログインすると、ログインプロセスを完了するために、Windows (Windows ログイン オプションを選択しなければならない場合があります) にログインするように指示されます</p> <p>初めて Windows にログインする場合は、手動で Credential Manager にログインする必要があります</p>
Embedded Security を復元すると、Credential Manager が機能しなくなる	ROM を工場出荷時の設定に復元した後は、Credential Manager が証明書を登録できなくなります	<p>HP Credential Manager for ProtectTools のインストール後、ROM が工場出荷時の設定にリセットされた場合、Credential Managers が TPM にアクセスできなくなります</p> <p>TPM 内蔵セキュリティ チップは、BIOS のコンピュータ セットアップ (F10) ユーティリティ、BIOS Configuration for ProtectTools、または HP Client Manager で有効にできます。TPM 内蔵セキュリティ チップを有効にするには、以下の手順で操作します</p> <ol style="list-style-type: none"> 1. コンピュータの電源を入れるか再起動し、画面の左下隅に[F10=ROM Based Setup]メッセージが表示されている間に F10 キーを押して、コンピュータ セットアップ (F10) ユーティリティを起動します 2. 矢印キーを使用し、[セキュリティ] (Security) →[セットアップパスワード] (Setup Password) の順に選択します。パスワードを設定します 3. [Embedded Security Device] (内蔵セキュリティ デバイス) を選択します 4. 矢印キーを使用して、[無効] (Embedded Security Device-Disable) を選択します。矢印キーを使用して、[有効] (Embedded Security Device-Enable) に変更します 5. [有効] (Enable) →[変更を保存して終了] (Save changes and exit) の順に選択します <p>HP では、将来のカスタマ ソフトウェア リリースに向けて、解決策を調査中です</p>
セキュリティの[Restore Identity] (ID の復元) プロセスにより、仮想トークンとの関連付けが失われる	ユーザが ID を復元すると、Credential Manager のログイン画面で仮想トークンの位置との関連付けが失われることがあります。Credential Manager が仮想トークンを登録している場合でも、関連付けを復元するには、ユーザがトークンを再登録する必要があります	<p>現在の仕様です</p> <p>ID を維持しないで Credential Manager をアンインストールすると、ID の復元によりトークンのクライアント部分が復元されても、トークンのシステム (サーバ) 部分が壊れ、トークンをログインに使用できなくなります</p> <p>HP では、一時的ではない解決策を調査中です</p>

Embedded Security for ProtectTools

簡単な説明	詳しい説明	解決方法
PSD でフォルダ、サブフォルダ、およびファイルを暗号化すると、エラーメッセージが表示される	ファイルとフォルダを PSD にコピーしてフォルダ/ファイルまたはフォルダ/サブフォルダを暗号化しようとする、 [Error Applying Attributes] (属性適用時のエラー) メッセージが表示されます。別に取り付けたハードディスク ドライブ上の C:\ ドライブで同じファイルを暗号化することはできません	これは仕様です ファイル/フォルダを PSD に移動するとそのファイル/フォルダは自動的に暗号化されます。ファイル/フォルダを二重に暗号化する必要はありません。EFS を使用して PSD のファイル/フォルダを二重に暗号化しようとすると、このエラー メッセージが表示されます
マルチブート プラットフォーム環境で別の OS を使用して所有権を得ることができない	ドライブがマルチ OS ブート用にセットアップされている場合でも、所有権を設定できるのは、1 つのオペレーティング システムのプラットフォーム初期化ウィザードからだけです	これはセキュリティを確保するための仕様です
管理者権限のある不正なユーザが、暗号化された EFS フォルダの内容の表示、削除、名前変更、移動を行える	フォルダを暗号化している場合でも、管理者権限がある不正なユーザは、フォルダの内容の表示、削除、または移動を行います	これは仕様です これは、Embedded Security TPM ではなく EFS の機能です。Embedded Security は、Microsoft EFS ソフトウェアを使用し、EFS がすべての管理者のファイル/フォルダへのアクセス権限を保護します
EFS で暗号化されたフォルダは、Windows 2000 では緑色で強調表示されません	EFS で暗号化されたフォルダは、Windows XP では緑色で強調表示されますが、Windows 2000 ではそのように表示されません	これは仕様です Windows 2000 では暗号化されたフォルダが強調表示されませんが、Windows XP では強調表示されるという現象は、EFS の機能です。これは、Embedded Security TPM がインストールされている場合もされてない場合も発生します
Windows 2000 では暗号化されたファイルを表示するときに EFS がパスワードを要求しない	Windows 2000 システムでは、Embedded Security をセットアップして、管理者としてログオンし、いったんログオフしてからもう一度管理者としてログオンすると、パスワードを入力しなくてもファイルとフォルダを表示できます。この状態は Windows 2000 の 1 番目の管理者アカウントで発生します。セカンダリ管理者アカウントでログインした場合、このような状態は発生しません	これは仕様です これは、Windows 2000 の EFS の機能です。Windows XP の EFS のデフォルト設定では、ユーザはパスワードなしでファイル/フォルダを開くことはできません
FAT32 パーティションの復元で、ソフトウェアをインストールできない	FAT32 を使用するハードディスク ドライブを復元する場合は、EFS を使用してファイル/フォルダを暗号化するオプションが表示されません	これは仕様です Microsoft EFS は、NTFS でのみサポートされており、FAT32 では機能しません。これは、Microsoft EFS の機能であり、HP ProtectTools ソフトウェアとは関係ありません
Windows 2000 ユーザは非表示の (\$) 共有を使用し、任意の PSD をネットワーク経由で共有できる	Windows 2000 ユーザは非表示の (\$) 共有を使用して、任意の PSD をネットワーク経由で共有できます。非表示共有には、非表示の (\$) 共有を使用してネットワーク経由でアクセスできます	PSD は、一般的にネットワークでは共有されませんが、Windows 2000 に限り、非表示の (\$) 共有を使用すると共有できます。このため、ビルトイン アカウントの管理者をパスワードで保護することをおすすめします
ユーザがリカバリ アーカイブ XML ファイルの暗号化または削除を行える	設計では、このフォルダの ACL は設定されていません。このため、意図的かどうかに関係なく、ユーザがこのファイルを暗号化または削除して、アクセスできなくなる可能性があります。ファイルが暗号化または削除されると、TPM ソフトウェアをだれも使用できなくなります	これは仕様です ユーザは、基本ユーザ キーのバックアップ コピーを保存または更新するために、緊急アーカイブにアクセスすることができます。最善のセキュリティ方針を採用し、ユーザがリカバリ アーカイブ ファイルを暗号化または削除しないよう周知徹底する必要があります

簡単な説明	詳しい説明	解決方法
HP ProtectTools Embedded Security EFS と Symantec Antivirus または Norton Antivirus 製品とのやり取りで暗号化/暗号化の解除およびスキャンにかかる時間が延びる	ファイルが暗号化されていると、Symantec Antivirus または Norton Antivirus 2005 のウイルス スキャンが中断されます。スキャン プロセス中、約 10 ファイルごとに、基本ユーザのパスワード プロンプトが表示され、パスワードの入力を求められます。パスワードを入力しなくても、基本ユーザのパスワード プロンプトがタイムアウトするため、Norton Antivirus 2005 はスキャンを続行できます。HP ProtectTools Embedded Security EFS を使用してファイルを暗号化すると、Symantec Antivirus または Norton Antivirus の実行時間が延びます	HP ProtectTools Embedded Security EFS ファイルのスキャンにかかる時間を短縮するには、スキャンの前に暗号パスワードを入力するか、またはスキャンの前に暗号化を解除します HP ProtectTools Embedded Security EFS を使用したデータの暗号化/暗号化の解除にかかる時間を短縮するには、Symantec Antivirus または Norton Antivirus の Auto-Protect を無効にする必要があります
リムーバブル メディアに緊急リカバリ アーカイブを保存できない	Embedded Security の初期化中に、緊急リカバリ アーカイブのパスを作成するとき、MMC または SD カードを挿入すると、エラー メッセージが表示されます	これは仕様です リムーバブル メディアにリカバリ アーカイブを保存することはできません。リカバリ アーカイブはネットワーク ドライブまたは C ドライブ以外のローカル ドライブに保存することができます
Windows 2000 のフランス語環境で、データを暗号化できない	ファイル アイコンを右クリックしても、 [Encrypt] (暗号化) オプションが表示されません	これは、Microsoft オペレーティング システムの制限事項です。 [French (Canada)] (フランス語 (カナダ)) など、他の地域にロケールを変更すると、 [Encrypt] (暗号化) オプションが表示されます これを回避するには、次の手順でファイルを暗号化します。ファイル アイコンを右クリックし、 [Properties] (プロパティ) → [Advanced] (詳細) → [Encrypt Contents] (内容の暗号化) の順に選択します
Embedded Security の初期化中に所有者を設定しているときに電源が切断されるとエラーが発生する	内蔵セキュリティ チップの初期化中に電源が切断されると、次のような問題が発生します <ul style="list-style-type: none">● Embedded Security Initialization Wizard (内蔵セキュリティ初期化ウィザード) の起動を試みると、次のエラー メッセージが表示されます。[The Embedded security cannot be initialized since the Embedded Security chip has already an Embedded Security owner.] (Embedded Security チップに Embedded Security の所有者がすでに設定されているため、Embedded Security を初期化できません)● User Initialization Wizard (ユーザ初期化ウィザード) の起動を試みると、次のエラー メッセージが表示されます。[The Embedded security is not initialized. To use the wizard, the Embedded Security must be initialized first.] (内蔵セキュリティが初期化されていません。ウィザードを使用するには、内蔵セキュリティを最初に初期化する必要があります)	電源が切断された後は、以下の手順に従って回復します  注記 メニューやメニュー項目の選択および値の変更には、特に指定がない場合は、矢印キーを使用します <ol style="list-style-type: none">1. コンピュータを起動または再起動します2. 画面に[F10=Setup]メッセージが表示されたら (またはモニタのランプが緑色に点灯したらすぐに) F10 キーを押します3. 該当する言語オプションを選択します4. Enter キーを押します5. [Security] (セキュリティ設定) → [Embedded Security] (内蔵セキュリティ) の順に選択します6. [Embedded Security Device] (内蔵セキュリティ デバイス) オプションを[Enable] (有効) に設定します7. F10 キーを押して、変更を確定します8. [ファイル]→[変更を保存して終了] (Save Changes and Exit) の順に選択します

簡単な説明	詳しい説明	解決方法
コンピュータ セットアップ (F10) ユーティリティのパスワードは、TPM モジュールを有効にした後に削除できる	TPM モジュールを有効にするには、コンピュータ セットアップ (TPM) ユーティリティのパスワードが必要です。モジュールを有効にすると、ユーザはパスワードを削除できます。パスワードを削除すると、システムに直接アクセスするユーザであれば誰でも TPM モジュールをリセットできるため、データ消失の原因になる可能性があります	<p>9. Enter キーを押します</p> <p>10. F10 キーを押して変更を保存し、コンピュータ セットアップ (F10) ユーティリティを終了します</p>
システムがスタンバイ状態からアクティブに切り替わると、PSD のパスワード ボックスが表示されなくなる	PSD の作成後ユーザがシステムにログオンすると、TPM は基本ユーザ パスワードの入力を要求します。ユーザがパスワードを入力しないままシステムがスタンバイ状態になると、ユーザが再開してもパスワード ダイアログ ボックスは表示されません	<p>これは仕様です</p> <p>ユーザがいったんログオフしてからログオンすれば、PSD パスワード ボックスは表示されます</p>
セキュリティ プラットフォーム ポリシーを変更するときに、パスワードを要求されない	セキュリティ プラットフォーム ポリシーへのアクセス (マシンとユーザの両方) では、システムの管理権限を持っているユーザは、TPM パスワードの入力を要求されません	<p>これは仕様です</p> <p>TPM ユーザが初期化されている場合でもされていない場合でも、管理者であればセキュリティ プラットフォーム ポリシーを変更できます</p>
Windows 2000 で Microsoft EFS が完全に機能しない	管理者は、正しいパスワードを知らなくても、システムの暗号化された情報にアクセスできます。管理者が誤ったパスワードを入力した場合やパスワード ダイアログを取り消した場合でも、暗号化されたファイルは正しいパスワードを入力した場合と同じように開きます。この現象は、データを暗号化するときのセキュリティ設定とは関係なく発生します。この状態は Windows 2000 の 1 番目の管理者アカウントで発生します	<p>データ リカバリ ポリシーは、管理者をリカバリ エージェントとして指名するように自動的に設定されません。ユーザ キーを取得できない場合 (誤ったパスワードを入力した場合や、[Enter Password] (パスワードの入力) ダイアログを取り消した場合)、ファイルはリカバリ キーを使用して自動的に暗号化が解除されます</p> <p>この原因は、Microsoft EFS にあります。詳しくは、http://www.microsoft.com/japan/ で、Microsoft サポート技術情報の記事 Q257705 を参照してください</p> <p>管理者以外のユーザがこのドキュメントを開くことはできません</p>
証明書を表示すると、信頼されていないものとして表示される	HP ProtectTools をセットアップして User Initialization Wizard (ユーザ初期化ウィザード) を実行した後、ユーザは発行された証明書を表示できますが、その証明書は信頼されていないものとして表示されます。ここで、インストール ボタンをクリックして証明書をインストールすることはできますが、インストールしても、信頼済みには変わりません	自己署名の証明書は、信頼されません。正しく設定された企業環境では、EFS の証明書は、オンラインの証明機関が発行し、信頼されます
次の暗号化/暗号化の解除エラーが断続的に発生する。 [The process cannot access the file because it is being used by another process.] (ファイルが別のプロセスによって使用されている)	ファイルの暗号化または暗号化の解除中に、ファイルが別のプロセスによって使用されていることが原因のエラーがきわめて断続的に発生します。これは、該当するファイルまたはフォルダがオペレーティング システムまたはその他のアプリケーションで処理されていない場合でも発生します	<p>この問題を解決するには、次の手順で操作します</p> <ol style="list-style-type: none"> 1. システムを再起動します 2. ログオフします 3. 再度ログインします

ため、このプロセスはファイルにアクセスできません)

新しいデータ生成または転送の前にストレージを取り外すと、リムーバブルストレージでデータが消失する

マルチベイ ハードディスク ドライブなどストレージメディアを取り外しても、PSD が使用可能と表示され、PSD のデータを追加または変更するときにエラーが生成されません。システムの再起動後、リムーバブルストレージが使用できなかった期間にファイルに加えられた変更箇所は、PSD に反映されません

この問題は、ユーザが PSD にアクセスした後、新しいデータの生成または転送が完了する前に、ハードディスク ドライブを取り外した場合にのみ発生します。リムーバブルハードディスク ドライブが存在しないときに PSD にアクセスすると、**[the device is not ready]** (デバイスの準備ができていません) というエラーメッセージが表示されます

基本ユーザの初期化が行われていない場合、アンインストールのために管理ツールを開くと、**[Disable]** (無効) オプションが使用できず、アンインストールは管理ツールを閉じるまで作業を停止する

ユーザは TPM を無効にしないでアンインストールを行うか、または最初に TPM を無効にして (管理ツールを使用) からアンインストールを行うかを選択できます。管理ツールにアクセスするには、基本ユーザ キーを初期化する必要があります。基本ユーザ キーを初期化していない場合、ユーザはどのオプションにもアクセスできません

TPM チップを無効にするには、管理ツールを使用しますが、基本ユーザ キーを初期化していない場合は、そのためのオプションは使用できません。基本ユーザ キーを初期化していない場合にアンインストール プロセスを続行するには、**[OK]** または **[Cancel]** (キャンセル) を選択してください

ユーザは、**[Click Yes to open Embedded Security Administration tool]** (Embedded Security 管理ツールを開くには、**[Yes]** (はい) をクリックします) と指示するダイアログボックスで **[Yes]** (はい) をクリックして明示的に管理ツールを開くことを選択しているため、管理ツールが閉じられるまでアンインストールは実行されません。ダイアログボックスで、**[No]** (いいえ) をクリックすると、管理ツールが開かないため、アンインストールは実行されます

128 MB のシステム構成で、2 つのユーザ アカウントで PSD を作成し、高速ユーザ切り替えを使用すると、システムが断続的にロックする

RAM の容量がきわめて少ない状態で高速切り替えを行うと、システムがロックすることがあります。このとき [ようこそ (ログオン)] 画面が表示されず、画面が黒色になり、キーボードとマウスを操作しても応答はありません

メモリ容量の少ない構成で発生するタイミングの問題が、根本原因になっていると思われます

内蔵グラフィックスが UMA アーキテクチャを使用するために 8 MB のメモリが使用され、ユーザ領域として 120 MB だけ残ります。エラーが発生した状況では、2 人のユーザがログインし高速でユーザの切り替えを行っています。エラーの発生時には、120 MB のメモリがこの 2 人のユーザで共有されています

この問題を回避するには、システムを再起動します。また、メモリを増設することをおすすめします (セキュリティ モジュールを搭載し、メモリのデフォルト構成が 128 MB のシステムは販売されていません)

[access denied] (アクセスが拒否されました) というメッセージが表示され、EFS ユーザ認証 (パスワード要求) がタイムアウトする

[OK] をクリックするか、タイムアウト後にスタンバイ状態から復帰すると、EFS ユーザ認証パスワードが再度開きます

これは仕様です。Microsoft EFS で問題が発生しないように、エラーメッセージを生成するために 30 秒程度のウォッチドッグ タイマーが作成されました

日本語のセットアップ時に、機能説明の一部が省略される

インストール ウィザード実行時のカスタム セットアップ オプション段階で、機能説明が省略されています

この問題については、将来のリリースで解決します

簡単な説明	詳しい説明	解決方法
プロンプトでパスワードを入力しなくても EFS 暗号化が行われる	ユーザパスワードのプロンプトのタイムアウトが許可されており、タイムアウトが発生した場合でも、ファイルまたはフォルダを暗号化できます	暗号化は Microsoft EFS 暗号化の機能のため、暗号化にパスワード認証は不要です。暗号化を解除する場合は、ユーザパスワードを入力する必要があります
User Initialization Wizard (ユーザ初期化ウィザード) でチェックを外している場合やユーザ ポリシーでセキュリティ保護された電子メールの設定を無効にしている場合でも、セキュリティ保護された電子メールがサポートされる	Embedded Security ソフトウェアとそのウィザードは、電子メールクライアント (Outlook、Outlook Express、または Netscape) の設定を制御しません	この動作は仕様です。TPM の電子メール設定では、電子メールクライアントの暗号化設定を直接編集することを禁じていません。セキュリティ保護された電子メールの使用は、他社製のアプリケーションが設定し、制御します。HP のウィザードでは、即座にカスタマイズを行う 3 つの参照アプリケーションを関連付けることができます
同じコンピュータまたは以前に初期化したコンピュータで 2 回目の大規模な導入を実行すると、緊急リカバリ ファイルおよび緊急トークン ファイルが上書きされる。新しいファイルは、リカバリに使用できない	以前に初期化した HP ProtectTools Embedded Security システムで大規模な導入を実行すると、既存のリカバリ トークン xml ファイルとリカバリ トークン xml ファイルが上書きされ、使用できなくなります	HP では、この xml ファイルの上書きの問題の解決に向けて取り組みを進めており、将来の SoftPaq で解決策が提供される予定です
Embedded Security でユーザの復元を実行中に、自動ログオン スクリプトが機能しない	ユーザが次の操作を行った後、エラーが発生します <ul style="list-style-type: none"> ● Embedded Security で、所有者とユーザを初期化する (デフォルトの位置の[マイ ドキュメント]を使用) ● BIOS で、チップを工場出荷時の設定に戻す ● コンピュータを再起動する ● Embedded Security の復元を開始する。復元プロセス中、Credential Manager は、システムが Infineon TPM User Authentication へのログオンを自動化できるかどうかをユーザにたずねます。ユーザが[Yes] (はい) を選択すると、テキストボックスに SPEmRecToken の位置が自動的に表示されます <p>この位置が正しい場合でも、次のエラーメッセージが表示されます。[No Emergency Recovery Token is provided. Select the token location the Emergency Recovery Token should be retrieved from.] (緊急リカバリ トークンが入力されていません。緊急リカバリ トークンの取得元にするトークン位置を選択してください。)</p>	画面の[Browse] (参照) ボタンをクリックして位置を選択してください。復元プロセスが続行されます
高速ユーザ切り替え環境で、複数ユーザ PSD が機能しない	複数のユーザが作成され、PSD に同じドライブ文字が割り当てられると、この問題が発生します。PSD がロードされているとき、ユーザを高速で切り替えよ	2 番目のユーザの PSD を使用するには、別のドライブ文字を使用するように設定し直すか、または最初のユーザがログオフする必要があります

簡単な説明	詳しい説明	解決方法
	<p>うとすると、2 番目のユーザの PSD を使用できなくなります</p> <p>PSD を作成したセカンダリ ハードディスク ドライブをフォーマットすると、PSD が無効になり、削除できなくなります。PSD のアイコンは残りますが、PSD へのアクセスを試みると、[drive is not accessible] (ドライブにアクセスできません) というエラー メッセージが表示されます</p> <p>PSD を削除することはできません。次のようなメッセージが表示されます。[your PSD is still in use, please ensure that your PSD contains no open files and is not accessed by another process.] (PSD は使用中です。PSD 上のファイルが開かれていないことと別のプロセスでアクセスされていないことを確認してください) PSD を削除するには、システムを再起動する必要があります。再起動後、PSD はロードされません</p>	<p>これは仕様です。ユーザが強制的に削除したり、PSD データの保存位置から切断したりしても、Embedded Security PSD ドライブ エミュレーションが機能を続行し、存在しないデータとの通信が途切れるため、エラーが生成されます</p> <p>解決策：次の再起動後はエミュレーションがロードされないため、ユーザは古い PSD エミュレーションを削除して、新しい PSD を作成できます</p>
<p>自動バックアップ アーカイブからの復元時に、内部エラーが検出された</p>	<p>ユーザが次の操作を行うと問題が発生します</p> <ul style="list-style-type: none"> ● HPPTSM で、[Embedded Security] (内蔵セキュリティ) の [Restore under Backup] (バックアップに基づいて復元する) オプションをクリックして、自動バックアップ アーカイブから復元しようとする ● [SpSystemBackup.xml] を選択する <p>Restore Wizard (復元ウィザード) が機能しなくなり、次のエラー メッセージが表示されます。[The selected Backup Archive does not match the restore reason. Please select another archive and continue.] (選択したバックアップ アーカイブは復元理由にふさわしくありません。別のアーカイブを選択して続行してください)</p>	<p>SpBackupArchive.xml が必要な場合にユーザが [SpSystemBackup.xml] を選択すると、次のメッセージが表示されて Embedded Security Wizard (Embedded Security ウィザード) が機能しなくなります。[An internal Embedded Security error has been detected] (Embedded Security 内部エラーが検出されました)</p> <p>所定の理由に該当する、正しい.xml ファイルを選択する必要があります</p> <p>プロセスは設計どおりに正しく機能していますが、Embedded Security 内部エラー メッセージが明確でないため、より適切なメッセージを表示する必要があります。HP は、将来の製品で改善するよう取り組んでいます</p>
<p>セキュリティ システムにより、複数のユーザでの復元エラーと表示される</p>	<p>復元プロセス中、管理者が復元するユーザを選択した場合、選択されなかったユーザが後で復元を試みてもキーを復元できません。[decryption process failed] (暗号化の解除プロセスが失敗しました) というエラー メッセージが表示されます</p>	<p>選択されなかったユーザは、次のデフォルトの日常バックアップが実行される前に、TPM をリセットして、復元プロセスを実行し、すべてのユーザを選択すれば、復元できます。自動バックアップが実行されると、復元されていないユーザは上書きされ、そのデータは失われます。新しいシステム バックアップが保存されると、選択されていない以前のユーザを復元することはできなくなります</p> <p>また、ユーザはシステム バックアップ全体を復元する必要があります。アーカイブバックアップは、個別に復元できます</p>

簡単な説明	詳しい説明	解決方法
システム ROM をデフォルト設定に戻すと、TPM を認識できなくなる	システム ROM をデフォルト設定に戻すと、Windows が TPM を認識できなくなります。これより、セキュリティ ソフトウェアが正しく動作しなくなり、TPM の暗号化データにアクセスできなくなります	以下の手順に従って、BIOS で TPM を再表示します コンピュータ セットアップ (F10) ユーティリティを開き、 [Security] (セキュリティ) → [Device security] (デバイス セキュリティ) の順に選択し、フィールドを [Hidden] (非表示) から [Available] (使用可能) に変更します
マップされたドライブで自動バックアップが機能しない	管理者が Embedded Security で自動バックアップをセットアップすると、 [Windows]→[Tasks]→[スケジュールされたタスク] にエントリが作成されます。この Windows の [スケジュールされたタスク] は、バックアップ実行権限用に NT AUTHORITY\SYSTEM を使用するように設定されます。この設定は、どのローカル ドライブに対しても有効に機能します 管理者が、自動バックアップでマップされたドライブに保存されるように設定すると、NT AUTHORITY\SYSTEM にはマップされたドライブを使用する権限がないため、プロセスは失敗します ログイン時に自動バックアップが行われるようにスケジュール設定されている場合、Embedded Security の TNA アイコンに次のメッセージが表示されます。 [The Backup Archive location is currently not accessible. Click here if you want to backup to a temporary archive until the Backup Archive is accessible again.] (現在、バックアップアーカイブの位置にアクセスできません。バックアップアーカイブにアクセスできるようになるまで、一時的なアーカイブにバックアップする場合は、ここをクリックしてください) ただし、自動バックアップが特定の時間に実行されるように設定されている場合、バックアップは失敗し、失敗を示すメッセージは表示されません	この問題を回避するには、NT AUTHORITY\SYSTEM を [コンピュータ名][管理者名] に変更してください。これは、スケジュールされたタスクが手動で作成される場合のデフォルト設定です HP では、 [コンピュータ名][管理者名] を含むデフォルト設定を備える製品を将来リリースできるよう取り組みを進めています
Embedded Security GUI で、Embedded Security の状態を一時的に無効にすることができない	最新の 4.0 ソフトウェアは、HP Notebook 1.1B への実装と、HP Desktop 1.2 への実装をサポートすることを目的にして設計されました 無効化のためのこのオプションは、TPM 1.1 プラットフォームのソフトウェア インタフェースでもサポートされています	この問題については、将来のリリースで対応します

その他

影響を受けるソフトウェアの簡単な説明	詳しい説明	解決方法
HP ProtectTools Security Manager で次の警告が表示される。 [The security application can not be installed until the HP ProtectTools Security Manager is installed] (HP ProtectTools セキュリティ マネージャをインストールするまでは、セキュリティ アプリケーションをインストールできません)	Embedded Security、Java Card、指紋認証などのセキュリティ アプリケーションは、すべて HP セキュリティ マネージャ インタフェースの拡張プラグインです。セキュリティ マネージャがインストールされていないと、HP 認定のセキュリティ プラグインをロードすることはできません	セキュリティ プラグインをインストールする前に、HP ProtectTools セキュリティ マネージャ ソフトウェアをインストールする必要があります
dc7600 や Broadcom 対応 TPM を搭載したモデル用の HP ProtectTools TPM Firmware Update Utility : HP のサポート Web サイトを通じて提供されるこのツールで [ownership required] (所有権が必要です) と報告される	<p>これは、dc7600 や Broadcom 対応 TPM を搭載したモデル用の TPM ファームウェア ユーティリティで想定された動作です</p> <p>ユーザは、公認キー (EK) がある場合もない場合も、このファームウェア アップグレード ツールを使用して、ファームウェアをアップグレードできます。EK がない場合は、ファームウェア アップグレードの実行に権限は必要ありません</p> <p>EK がある場合は、アップグレードに所有者の権限が必要なため、TPM 所有者が存在する必要があります。アップグレードが正常に行われた後、プラットフォームを再起動して、新しいファームウェアを有効にする必要があります</p> <p>BIOS TPM が工場出荷時の状態にリセットされると、所有権は削除され、Embedded Security ソフトウェアのプラットフォームとユーザの初期化のためのウィザードの設定が完了するまで、アップデート機能を使用できません</p> <p>*ファームウェア アップデートの実行後に必ずシステムを再起動することをおすすめします。ファームウェア バージョンは、再起動が完了するまでは正しく識別されません</p>	<ol style="list-style-type: none">1. HP ProtectTools Embedded Security ソフトウェアを再インストールします2. プラットフォームおよびユーザの設定ウィザードを実行します3. 以下の手順に従って、システムに Microsoft .NET framework 1.1 がインストールされていることを確認します<ol style="list-style-type: none">a. [スタート]をクリックしますb. [コントロール パネル]をクリックしますc. [プログラムの追加と削除]をクリックしますd. [Microsoft .NET Framework 1.1]があることを確認します4. 以下の手順に従って、ハードウェアとソフトウェアの構成を確認します<ol style="list-style-type: none">a. [スタート]をクリックしますb. [すべてのプログラム]をクリックしますc. [HP ProtectTools セキュリティ マネージャ]をクリックしますd. ツリー メニューから[Embedded Security] (内蔵セキュリティ) を選択しますe. [More Details] (詳細) をクリックします システムは、次のような構成になっている必要があります<ul style="list-style-type: none">● Product version (製品バージョン) = V4.0.1● Embedded Security State (内蔵セキュリティの状態) : Chip State (チップの状態) = Enabled (有効)、Owner State (所有者の状態) = Initialized (初期化済み)、User State (ユーザの状態) = Initialized (初期化済み)

影響を受けるソフトウェアの簡単な説明	詳しい説明	解決方法
HP ProtectTools セキュリティ マネージャ : セキュリティ マネージャ インタフェースを閉じたとき、エラーが返されることがある	すべてのプラグイン アプリケーションのロードが終了する前に、セキュリティ マネージャを閉じようとして画面右上の閉じるボタンを使用すると、エラーが発生することがあります (12 回に 1 回ぐらいの割合)	<ul style="list-style-type: none"> Component Info (コンポーネント情報) : TCG Spec. Version (TCG 仕様バージョン) = 1.2 Vendor (ベンダ) = Broadcom Corporation FW Version (FW バージョン) = 2.18 (または、それ以上) TPM デバイス ドライバライブラリ バージョン 2.0.0.9 (またはそれ以上) <p>5. [FW Version] (FW バージョン) が「2.18」になっていない場合は、TPM ファームウェアをダウンロードして更新してください。TPM ファームウェア SoftPak は、http://www.hp.com/jp/からダウンロードできます</p>
HP ProtectTools *全般 : アクセスが制限されていないことや管理者権限が制御されないことが、セキュリティ リスクにつながる	<p>クライアント コンピュータに対するアクセスが制限されていないため、次のような、さまざまなリスクが発生します</p> <ul style="list-style-type: none"> PSD の削除 ユーザ設定の意図的な改ざん セキュリティ ポリシーやセキュリティ機能の無効化 	<p>これは、セキュリティ マネージャを終了および再起動するときに、そのタイミングがプラグイン サービスロード時間の影響を受けることに関連しています。PTHOST.exe は、他のアプリケーション (プラグイン) を収納するシェルであるため、プラグインのロード時間 (サービス) の終了能力の影響を受けます。この問題の根本原因は、プラグインのロード終了にかかる時間が経過していないのにシェルが閉じられたことです</p> <p>セキュリティ マネージャがサービス ロードメッセージ (セキュリティ マネージャ ウィンドウの上部に表示されます) を完了し、すべてのプラグインが左の列に表示されるまで待ちます。障害の発生を防止するために、これらのプラグインがロードされるまでしばらく待ってください</p> <p>管理者が最善の方法でエンドユーザの権限を制限し、ユーザのアクセスを制限することをおすすめします</p> <p>不正なユーザに管理権限を与えないでください</p>
BIOS と OS の Embedded Security パスワードが同期していない	ユーザが新しいパスワードを BIOS の Embedded Security パスワードとして有効にしなかった場合、BIOS の Embedded Security 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 BIOS 設定を通じて、元の Embedded Security パスワードに戻ります	これは仕様です。このパスワードは、OS の基本ユーザパスワードを変更し、BIOS Embedded Security パスワードのプロンプト画面で認証すれば、再同期されます
BIOS の TPM ブート前認証を有効にした後、1 人のユーザしかシステムにログインできない	TPM BIOS PIN は、ユーザ設定の初期化を初めて行ったユーザに関連付けられています。コンピュータを複数のユーザで利用する場合、基本的に 1 番目のユーザが管理者になります。1 番目のユーザは、ログインに使用する自分の TPM ユ	これは仕様です。ユーザの IT 部門が適切なセキュリティ ポリシーに従ってセキュリティ ソリューションを展開すること、さらに BIOS 管理者パスワードはシステム レベルで保護されるように必ず IT 管理者が設定することをおすすめします

影響を受けるソフトウェアの簡単な説明	詳しい説明	解決方法
	<p>ユーザ PIN を他のユーザに教える必要があります</p>	
<p>TPM を工場出荷時設定にリセットした後、TPM 起動前ブートを機能させるためにユーザが PIN を変更しなければならない</p>	<p>TPM のリセット後に TPM BIOS 認証を機能させるため、ユーザは PIN を変更するか、または別のユーザを作成してユーザ自身の設定を初期化する必要があります。他に TPM BIOS 認証を機能させる方法はありません</p>	<p>これは仕様です。工場出荷時の設定にリセットすると基本ユーザ キーは消去されます。ユーザは PIN を変更するか、または別のユーザを作成して基本ユーザ キーを再初期化する必要があります</p>
<p>Embedded Security の [Reset to Factory Settings] (工場出荷時の設定に戻します) を使用しても、[Power-on authentication support] (起動時の認証サポート) がデフォルトに設定されない</p>	<p>コンピュータ セットアップ (F10) ユーティリティで、Embedded Security デバイス オプションの [Reset to Factory Settings] (工場出荷時の設定に戻します) を使用しても、[起動時の認証サポート] オプションは工場出荷時の設定にリセットされません。デフォルトでは、[Power-on authentication support] (起動時の認証サポート) は、[Disable] (無効) に設定されます</p>	<p>[Reset to Factory Settings] (工場出荷時の設定に戻します) オプションを使用すると、Embedded Security デバイスは無効になり、他の Embedded Security オプション ([Power-on authentication support] など) も認識されなくなります。ただし、Embedded Security デバイスを再度有効にすると、[Power-on authentication support] は有効のままになります</p> <p>HP では解決策に向けた取り組みを進めており、将来の Web ベース ROM の SoftPaq で提供する予定です</p>
<p>起動シーケンスの実行中に、セキュリティの起動時の認証が BIOS のパスワードと重なる</p>	<p>起動時の認証では、ユーザは TPM パスワードを使用してシステムにログオンすることが求められますが、ユーザが [F10] キーを押して BIOS にアクセスする場合は読み込み権限だけが与えられます</p>	<p>BIOS に書き込みできるようにするには、ユーザは、[Power-on Authentication] (起動時の認証) ウィンドウで TPM パスワードではなく BIOS パスワードを入力する必要があります</p>
<p>Embedded Security Windows ソフトウェアで所有者のパスワードを変更した後に、BIOS がコンピュータ セットアップ (F10) ユーティリティを通じて新旧両方のパスワードを要求する</p>	<p>Embedded Security Windows ソフトウェアで所有者のパスワードを変更した後に、BIOS はコンピュータ セットアップ (F10) ユーティリティを通じて新旧両方のパスワードを要求します</p>	<p>これは仕様です。これは、オペレーティング システムが起動されると、BIOS は TPM と通信できず、TPM パス フレーズを TPM キーの blob と照合できないためです</p>

用語集

AES (Advanced Encryption Standard) 128 ビットのブロック データ対称暗号化技術。

API (Application Programming Interface) アプリケーションがさまざまなタスクを実行するために使用できる一連のオペレーティング システム内部関数。

BIOS セキュリティ モード 有効にすると、ユーザ認証に Java Card および有効な PIN の使用が必要になる、Java Card Security for ProtectTools での設定。

BIOS プロファイル 他のアカウントに保存および適用できる、BIOS 設定値の集合。

ID ProtectTools Credential Manager 内で、特定のユーザのアカウントまたはプロファイルのように処理される、証明書と設定の集合。

Java Card 所有者に関する識別情報が格納されている、サイズと形状がクレジットカードに似た小さなハードウェア。所有者をコンピュータに対して認証するために使用されます。

Java Card の管理者パスワード 起動時または再起動時の識別のために、コンピュータ セットアップ (F10) ユーティリティで管理者 Java Card をコンピュータにリンクするパスワード。このパスワードは、管理者が手動で設定することも、ランダムに生成することもできます。

Java Card のユーザパスワード 起動時または再起動時の識別のために、コンピュータ セットアップ (F10) ユーティリティでユーザ Java Card をコンピュータにリンクするパスワード。このパスワードは、管理者が手動で設定することも、ランダムに生成することもできます。

LPC (Low Pin Count) プラットフォームのチップセットと接続するために、HP ProtectTools Embedded Security デバイスで使用されるインタフェースを定義します。バスは、4 ビットのアドレス/データ ピン、33 MHz のクロック、複数の制御/ステータス ピンで構成されます。

MSCAPI (Microsoft Cryptographic API、または CryptoAPI) Microsoft 社が提供する API。暗号化アプリケーションのために、Windows オペレーティング システムへのインタフェースを提供します。

PKCS (Public Key Cryptographic Standards) 暗号化と暗号化の解除のための公開キー/秘密キー方式の定義と使用に適用される一連の規格。

PSD (Personal Secure Drive) 機密データを保護するための記憶領域を提供する機能。HP ProtectTools Embedded Security により提供される機能です。このアプリケーションはユーザのコンピュータに仮想ドライブを作成し、そのドライブに移されたファイルやフォルダを自動的に暗号化します。

S/MIME (Secure Multipurpose Internet Mail Extensions) PKCS を使用した安全な電子メッセージングの仕様。S/MIME は、デジタル署名を使用した認証と暗号化によるプライバシー保護を実現します。

TCG (Trusted Computing Group) 「信頼できるコンピュータ」というコンセプトを広めるために創立された業界団体。TCG は TCPA の事業を受け継ぎました。

TCG ソフトウェア スタック (TSS) TPM を最大限に活用するサービスを提供する機能。ただし同様の保護を必要としません。TPM の機能にアクセスする標準のソフトウェア インタフェースを提供します。キーのバック

アップ、キーの移行、プラットフォーム認証と証明など、TPM の機能を最大限に利用するため、アプリケーションは TSS に直接書き込みを行います。

TCPA (Trusted Computing Platform Alliance) 「信頼できるコンピューティング」のための団体。現在、その事業は TCG に受け継がれています。

TPM (Trusted Platform Module) 内蔵セキュリティ チップ (一部のモデルのみ) 機密性の高いユーザ情報を悪意のある攻撃者から保護できる、統合されたセキュリティ チップ。特定のプラットフォーム上の信頼性の基盤です。TPM によって、TCG (Trusted Computing Group) 仕様に適合する暗号化アルゴリズムおよび演算方法が提供されます。TPM ハードウェアとソフトウェアは、EFS および Personal Secure Drive で使用されるキーを保護することにより、EFS と Personal Secure Drive のセキュリティを強化します。TPM のないシステムでは、EFS および PSD で使用されるキーは、通常ハードディスク ドライブに保存されます。しかし、これではキーが盗まれる可能性があります。TPM カードを搭載したシステムでは、TPM の秘密 Storage Root Key が、EFS や PSD で使われるキーを保護します。秘密 Storage Root Key は、TPM チップに格納され TPM から外に出ることはありません。この秘密キーを盗むために TPM に侵入することは、システムのハードディスク ドライブに侵入してキーを盗み出すことよりもはるかに困難です。また、TPM は、Microsoft Outlook および Outlook Express での S/MIME を介したセキュリティ保護された電子メールのセキュリティを強化します。TPM は、暗号化サービス プロバイダ (CSP) として機能します。キーおよび証明書の生成やサポートは TPM ハードウェアが行うため、ソフトウェアのみの実装と比較してセキュリティ レベルがはるかに高くなります。

USB トークン ユーザに関する識別情報が格納されているセキュリティ デバイス。Java Card や指紋認証システムと同様に、所有者をコンピュータに対して認証するために使用されます。

Windows ユーザ アカウント ネットワークまたは個別のコンピュータへのログオンを承認された個人のプロフィール。

暗号化サービス プロバイダ (CSP) 明確なインターフェースを使用して特定の暗号化関数を実行するための暗号化アルゴリズムの提供者またはライブラリ。MSCAPI とのインターフェースとなるソフトウェア コンポーネントです。

暗号化の解除 暗号化されたデータを平文に変換するための、暗号法で使用される手順。

暗号化ファイルシステム (EFS) 選択されたフォルダ内のすべてのファイルおよびサブフォルダを暗号化するシステム。Microsoft 社が Windows 2000 以降で提供する、透過的なファイル暗号化サービスです。

暗号化 権限のない受信者がデータを解読できないように平文を暗号文に変換するための、暗号法で使用されるアルゴリズムなどの手順。データの暗号化にはさまざまな種類があり、ネットワーク セキュリティの基礎として使用されます。一般的な暗号化には、データ暗号化規格 (DES) や公開キー暗号があります。

暗号法 特定の個人だけが解読できるように、データを暗号化および暗号解除する手法。

移行 キーおよび証明書を管理、復元、および転送する作業。

仮想トークン Java Card やリーダーとよく似た働きをするセキュリティ機能。このトークンは、コンピュータのハードドライブ上か、Windows レジストリ内のどちらかに保存されます。仮想トークンでログオンすると、認証を完了するためにユーザ PIN の入力を要求されます。

起動時の認証 Java Card、セキュリティ チップ、パスワードなど、コンピュータの起動時に何らかの形式の認証を要求するセキュリティ機能。

緊急リカバリ アーカイブ 他のプラットフォームの所有者キーを使用して基本ユーザ キーを再暗号化できる、保護された記憶領域。

厳重なセキュリティ 電源投入時パスワード、管理者パスワード、およびその他の形態の、起動時の認証に対する保護機能を強化する、BIOS Configuration にあるセキュリティ機能。

公開キー基盤 (PKI) 公開キー/秘密キーによる暗号化と暗号化の解除を使用するセキュリティ システムの実装を定義する一般的な用語。

証明書 ユーザ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。

シングルサインオン 認証データを格納し、パスワード認証が必要なインターネットおよび Windows アプリケーションに Credential Manager を使用してアクセスできるようにする機能。

デジタル証明書 デジタル証明書の所有者の身元と、デジタル情報の署名に使用される電子キーのペアとを結びつけることによって、個人または企業の身元を証明する電子的な信用証明書。

デジタル署名 資料の送信者を証明し、署名された後にファイルが変更されていないことを証明するファイルとともに送信されるデータ。

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。

認証機関 公開キー基盤の運営に必要な証明書を発行するサービス。

認証 ユーザがタスクの実行（コンピュータへのアクセス、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 コンピュータ上、ワークグループ内、またはドメイン上の Windows ユーザまたは管理者のアカウント。

バイオメトリック 指紋などの身体的な特徴を使用してユーザを識別する認証証明のカテゴリ。

リブート コンピュータを再起動するプロセス。

索引

B

BIOS

- 管理者カードのパスワード、定義 3
- 管理者パスワード、定義 2
- 設定の変更 13
- ユーザカードのパスワード、定義 3

BIOS Configuration for ProtectTools 13

C

Client Manager 23

Credential Manager

- インストール 17
- トラブルシューティング 25
- リカバリ ファイルのパスワード 4
- ログオン パスワード 4
- ログオン 5, 18

E

Embedded Security for ProtectTools

- 起動時の認証 7
- セットアップ 16
- トラブルシューティング 29
- パスワード 3

F

[F10]セットアップパスワード 2

I

IDのバックアップウィザードパスワード 5

J

Java Card

- PIN、定義 3

ProtectTools のセキュリティ 19

- 管理者パスワード、定義 3
- 起動時の認証 7
- ユーザパスワード、定義 3
- リカバリ ファイルのパスワード、定義 3

P

PKCS#12 のインポートパスワード 4

ProtectTools

- Credential Manager 17
- Java Card のセキュリティ 19
- セキュリティ マネージャへのアクセス 1
- セキュリティ マネージャ モジュール 1
- 設定の管理 7
- 内蔵セキュリティ 15
- パスワードの管理 2

T

TCG ソフトウェア スタック (TSS) 1, 21

TPM 起動前パスワード 3

TPM 認証の別名 5

U

USB トークンの認証 5

W

Windows

- ログオンパスワード 4

い

インストール、Credential Manager 17

か

拡張タスク 7

仮想トークンの認証パスワード 5

仮想トークンのマスタ PIN 4

仮想トークンのユーザ PIN 4

き

起動時の認証

Java Card 7

内蔵セキュリティ 7

基本ユーザのパスワード、定義 3

緊急リカバリ トークンのパスワード、定義 3

こ

コンピュータ セットアップ (F10) ユーティリティ

管理者パスワード、定義 2

管理者パスワードの設定 10

管理者パスワード、変更 11

パスワード、管理 8

し

辞書攻撃 12

指紋認証ログオン 5

所有者のパスワード、定義 3

せ

セキュリティ

Embedded Security for ProtectTools 15

Java Card 19

セットアップパスワード 2

役割 2

セキュリティ マネージャ、ProtectTools 1

セキュリティ リカバリ エージェントのパスワード 4

そ

ソフトウェア

ProtectTools セキュリティ マネ
ージャ 1

た

他社のソリューション 21

て

電源投入

辞書攻撃 12
パスワードの設定 8
パスワードの定義 2
パスワードの変更 9

と

トラブルシューティング

Credential Manager for
ProtectTools 25
Embedded Security for
ProtectTools 29
その他 36

は

パスワード

Credential Manager のログオ
ン 4
Credential Manager リカバリ フ
ァイル 4
ID のバックアップ ウィザー
ド 5
Java Card の PIN 3
Java Card の管理者 3
Java Card ユーザ 3
Java Card リカバリ ファイ
ル 3
PKCS#12 のインポート 4
ProtectTools、管理 2
TPM 認証の別名 5
USB トークンの認証 5
Windows のログオン 4
ガイドライン 5
仮想トークンの認証 5
仮想トークンのマスタ PIN 4
仮想トークンのユーザ PIN 4
基本ユーザ 3
緊急リカバリ トークン 3
コンピュータ セットアップ
(F10) ユーティリティ、管
理 8

コンピュータ セットアップ
(F10) ユーティリティの管理
者 2

コンピュータ セットアップ
(F10) ユーティリティの管理
者、設定 10

コンピュータ セットアップ
(F10) ユーティリティの管理
者、変更 11

指紋認証ログオン 5

所有者 3

セキュリティ リカバリ エージェ
ント 4

定義 2

電源投入、設定 8

電源投入、変更 9

電源投入 2

パスワードリセット トーク
ン 4

バックアップ スケジューラ 4

パスワードリセット トークン 4

バックアップ スケジューラのパス
ワード 4

ま

マルチファクタ認証 Credential
Manager のログオン 5

り

リモート展開、Client
Manager 23