HP ProtectTools
内蔵セキュリティ ガイド
HP Business Desktop dx5150モデル

製品番号：376352-291

2004年12月

このガイドでは、HP ProtectTools内蔵セキュリティ チップを設定するための
ソフトウェアの使用方法について説明します。

本書の内容は、将来予告なしに変更されることがあります。

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

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

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

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

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

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

以下の記号は、本文中で安全上重要な注意事項を示します。

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

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

HP ProtectTools内蔵セキュリティ ガイド
初版 2004年12月
製品番号：376352-291

日本ヒューレット・パッカード株式会社

目次

HP ProtectTools内蔵セキュリティ

HP ProtectTools内蔵セキュリティ

HP ProtectToolsセキュリティ マネージャは、HP ProtectTools内蔵セキュリティを設定するためのソフトウェアです。このマネージャは、内蔵セキュリティ ソフトウェアのさまざまなオプションにアクセスするためのインタフェース（シェル）です。HP ProtectTools 内蔵セキュリティは、Personal Secure Drive（PSD）、暗号化/TPMチップ インタフェース、セキュリティの移行、アーカイブの作成、およびパスワードの制御などに関するソフトウェアの集合です。

要件

セキュリティ機能を使用するには、次のものが必要です。

- HP ProtectTools内蔵セキュリティ ソフトウェア
- HP ProtectToolsセキュリティ マネージャ ソフトウェア
- HP ProtectTools内蔵セキュリティ チップ（コンピュータに搭載されています）

内蔵セキュリティ ソリューションのセットアップについては、8ページの「セットアップ手順」を参照してください。

ProtectTools内蔵セキュリティの基本概念

ここでは、HP ProtectTools内蔵セキュリティおよびHP ProtectToolsセキュリティ マネージャを使用するために理解しておく必要のある、全般的な概念について説明します。

HP ProtectTools内蔵セキュリティ チップ

内蔵セキュリティ チップは、公開キーと秘密キーを保護するため、セキュリティおよび暗号化機能を提供し、不正防止の記憶領域を備えたハードウェアコンポーネントです。チップは工場で組み込まれるため、HPのサポートまたはサービス担当者以外はアクセスまたは取り外しできません。

Personal Secure Drive（PSD）

Personal Secure Drive（PSD）は、内蔵セキュリティの機能の1つです。PSDは、HP ProtectTools内蔵セキュリティのユーザ初期化プロセス中に、ハードディスク ドライブ上に作成される仮想ドライブです。機密データを保護するための記憶領域を提供し、他のドライブと同じように、ファイルやフォルダを作成したりアクセスしたりできます。

PSDにアクセスするには、PSDが含まれるコンピュータへの物理的なアクセスおよびPSDパスワードが必要です。PSDパスワードを入力すると、PSDが表示されてファイルを使用できるようになります。ログオフして自動的にPSDが非表示になるまで、ファイルにアクセスできます。ネットワーク経由では、PSDにアクセスできません。

暗号化されたデータはPSDに格納されます。ファイルを解読するためのキーはHP ProtectTools内蔵セキュリティ チップに格納されるため、権限のないユーザによるアクセスからデータを保護し、コンピュータからデータが漏えいすることを防ぎます。つまり、保護されたデータは、そのデータが保存されたコンピュータ上でしかアクセスできません。

電子メール

電子メールのセキュリティ保護も、内蔵セキュリティの重要な機能の1つです。この機能を使用すると、情報を機密に交換し、転送中に情報の信頼性が失われていないことを保証できます。電子メールをセキュリティ保護することで、次の操作が可能になります。

- 認証機関（CA）が発行した公開キー証明書を選択する
- メッセージにデジタル署名を付加する
- メッセージを暗号化する

HP ProtectTools内蔵セキュリティおよびHP ProtectToolsセキュリティ マネージャは、メッセージの暗号化、解読、およびデジタル署名に使用されるキーの保護機能を追加することによって、電子メールのセキュリティ保護機能を向上させます。これにより、次の電子メール クライアントで、電子メールのセキュリティを向上できます。

- Microsoft® Outlook Express（バージョン4以降）
- Microsoft Outlook 2000
- Microsoft Outlook 2002
- Netscape Messenger 4.79
- Netscape Messenger 7.0

電子メール クライアントの使用方法については、HP ProtectTools内蔵セキュリティ電子メール統合のヘルプを参照してください。

暗号化ファイル システム（EFS）の機能の向上

EFSは、Microsoft Windows® 2000およびWindows XP Professionalで提供されるファイル暗号化サービスです。EFSは、次の機能を提供することによってデータのプライバシを保護します。

- ディスクへの保存時の、ユーザによるファイルの暗号化
- 暗号化されたファイルへのすばやく簡単なアクセス
- 自動的な（かつユーザが意識することのない）暗号化
- システム管理者により、他のユーザが暗号化したデータの回復が可能

HP ProtectTools内蔵セキュリティおよびHP ProtectToolsセキュリティ マネージャは、データの暗号化および解読に使用されるキーの保護機能を追加することによって、EFSの機能を向上させます。

EFSについて詳しくは、オペレーティング システムのオンライン ヘルプを参照してください。

ユーザおよび管理者

ユーザ

ユーザは、内蔵セキュリティへの基本的なアクセス権を持ち、次の操作を実行できます。

- 暗号化された電子メールの送受信
- ファイルおよびフォルダの暗号化
- 個人の基本ユーザ キーの初期化
- 内蔵セキュリティ内の個人ユーザ アカウントの作成、削除、または変更
- 個別のPSDの設定、作成、使用、および削除

管理者

管理者はコンピュータの内蔵セキュリティ ソリューションを初期化し、また、次の操作を実行できます。

- 内蔵セキュリティのローカル マシン ポリシーおよびユーザ ポリシーの設定
- ユーザ キーおよび証明書の移行の準備
- 内蔵セキュリティ オーナのパスワードの変更
- 内蔵セキュリティの無効化と有効化
- ユーザ キーおよび証明書の移行先コンピュータの認証
- 内蔵セキュリティを使用して保存および暗号化されたデータの回復

内蔵セキュリティのユーザおよび管理者について詳しくは、オペレーティング システムのオンライン ヘルプを参照してください。内蔵セキュリティのオーナについて詳しくは、HP ProtectTools内蔵セキュリティのオンライン ヘルプを参照してください。

デジタル証明書

デジタル証明書は、個人または企業の身元を証明するための、電子的な「キー」の一形態です。キーは、送信者と受信者の両方またはそのどちらか一方のみが知っている数字または文字列です。デジタル証明書は、その所有者が送信する電子メールに添付するデジタル署名を提供することによって、所有者の身元を証明します。

デジタル証明書は、認証機関（CA）によって発行され、次の情報が含まれています。

- 所有者の公開キー
- 所有者の名前
- デジタル証明書の有効期限
- デジタル証明書のシリアル番号
- デジタル証明書を発行したCAの名前
- デジタル証明書を発行したCAのデジタル署名

デジタル署名

デジタル署名には、デジタル証明書を発行したCAの名前が示されます。次のために使用します。

- デジタル文書の送信者の身元確認
- 送信者が文書にデジタル署名した後、その文書の内容が変更されていないことの証明

デジタル署名について詳しくは、オペレーティング システムのオンライン ヘルプを参照してください。

公開キーと秘密キー

内蔵セキュリティで情報の暗号化方法として使用される非対称暗号法では、公開キーと秘密キーの2つのキーが必要になります。

公開キーは多数のユーザに自由に配布できますが、秘密キーは1人のユーザのみが所有します。

たとえば、暗号化された電子メールを送信する場合、ユーザAは、ユーザBの公開キー（自由に入手できます）を使用して電子メールの内容を暗号化し、ユーザBに送信します。ユーザBの秘密キーを所有するのはユーザBだけなので、ユーザAが送信した電子メールの内容は、ユーザBのみが解読できます。

公開キーを利用した技術によって、公共のネットワークを介した個人情報の送受信、デジタル署名を使用した電子メールの信頼性の保証、およびサーバとクライアント間の認証が可能になります。

Emergency Recovery

Emergency Recovery Archiveは、コンピュータとそのユーザに関する機密情報、および暗号化されたデータや個人データの保護に使用される秘密キーに関する機密情報が保存されたファイルです。このファイルは、内蔵セキュリティのセットアップ時に管理者によって作成されます。システムに障害が発生した場合、保護されたデータへのアクセス権を復元するには、この機密情報が必要です。

Emergency Recovery Tokenは、Emergency Recovery Archive内のデータの保護に使用されるキーが保存されたファイルです。このファイルも、内蔵セキュリティのセットアップ時に管理者によって作成されます。トークンは、アーカイブにアクセスするために必要です。Emergency Recovery Tokenへのアクセスは、パスワードによって保護されます。このパスワードは、内蔵セキュリティシステムを復元する場合に必要です。

ポリシー

ポリシーは、コンピュータまたはソフトウェアの動作を規定するルールです。システム管理者は、通常、組織内での内蔵セキュリティの使用の一貫性を保つためにセキュリティ ポリシーを指定します。セキュリティ ポリシーには、マシン ポリシーとユーザ ポリシーの2種類があります。

マシン ポリシー

マシン ポリシーは、特定のコンピュータに関連付けられ、内蔵セキュリティの全体的な動作を規定するルールです。

ユーザ ポリシー

ユーザ ポリシーは、内蔵セキュリティのユーザの権限を規定するルールです。

マシンおよびユーザ セキュリティ ポリシーについて詳しくは、HP ProtectTools内蔵セキュリティのヘルプを参照してください。

セットアップ手順

以下の手順に従って、システムBIOS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、内蔵セキュリティ チップの有効化および初期化を行います。

注意：セキュリティ上の危険を防ぐため、組織内で適切な権限を持つユーザがただちに内蔵セキュリティ チップを初期化することをお勧めします（手順4を参照してください）。内蔵セキュリティ チップを初期化しないと、権限のないユーザ、コンピュータ ワーム、またはウィルスによって、システムのオーナシップを奪われる可能性があります。

チップのコンフィギュレーションにアクセスするには、コンピュータ セットアップ（F10）ユーティリティでBIOSスーパバイザ パスワードを設定する必要があります。詳しくは、コンピュータに同梱のDocumentation CD（ドキュメンテーション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。

チップの有効化

1. コンピュータの電源を入れるか、**[スタート]→[シャットダウン]→[再起動]**→[OK]の順に選択して再起動します。
2. コンピュータが起動したらすぐに**[F10]**キーを押したままにし、コンピュータ セットアップを実行します。

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

3. 矢印キーを使用して**[スーパバイザ　パスワードを設定]**（Set Supervisor Password）を選択し、**[Enter]**キーを押します。
4. スーパバイザ パスワードを入力して**[Enter]**キーを押します。
5. **[スタート]→[シャットダウン]→[再起動]**→[OK]の順に選択してコンピュータを再起動します。
6. [Press any key to enter TPM Configuration]というコマンド プロンプトが表示されたら、すぐに任意のキーを押します。
7. スーパバイザ パスワードを入力して**[Enter]**キーを押します。

8. TPMチップを有効にするには**[E]**キーを押します。

   これでチップが有効になりました。

内蔵セキュリティ チップの初期化

通常は、ITシステム管理者が内蔵セキュリティ チップを初期化します。

1. システム トレイの[HP ProtectTools]アイコンを右クリックし、[Embedded Security Initialization]（Embedded Securityの初期化）を左クリックします。

   [HP ProtectTools Embedded Security Initialization Wizard]（HP ProtectTools Embedded Security初期化ウィザード）が表示されます。

2. [Next]（次へ）をクリックします。
3. [Take Ownership]（オーナーシップの設定）パスワードを入力して確定し、[Next]をクリックします。

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

4. [Next]をクリックしてデフォルトのリカバリ アーカイブの場所を確定します。
5. [Emergency Recovery Token]（緊急時復元プロセスの設定）パスワードを入力して確定し、[Next]をクリックします。
6. [Browse]（参照）をクリックして適切な場所を選択します。

注意：Emergency Recovery Tokenキーは、コンピュータや内蔵セキュリティ チップに不具合がある場合に、暗号化されたデータを復元するために使用します。キーがないと、データを復元できません（基本ユーザ パスワードがない場合にも、データにアクセスできません）。このキーは安全な場所に保管してください。

7. [Save]（保存）をクリックしてファイルの場所とデフォルトのファイル名を確定し、[Next]をクリックします。
8. [Next]をクリックして、セキュリティ プラットフォームが初期化される前に設定を確定します。

注意：内蔵セキュリティ機能が初期化されていないというメッセージが表示される場合がありますが、これをクリックしないでください。このメッセージについては後の手順で説明します。メッセージは数秒後に閉じます。

9. ここでユーザ アカウントをセットアップする場合は、[Start Embedded Security User Initialization Wizard]（Embedded Securityユーザ初期化ウィザードを起動する）チェック ボックスが選択されていることを確認します。[Finish]（完了）をクリックします。

ユーザ アカウントのセットアップ

ユーザ アカウントをセットアップすると、次のことができます。

- 暗号化されたデータを保護するための基本ユーザ キーを生成できます。
- 暗号化されたファイルおよびフォルダを保存するための PSD をセットアップできます。

注意：基本ユーザ パスワードは安全な場所に保管してください。暗号化されたデータは、このパスワードがないとアクセスしたり復元したりすることができません。

基本ユーザ アカウントをセットアップし、ユーザのセキュリティ機能を有効にするには、以下の手順で操作します。

1. [Embedded Security User initialization Wizard]（Embedded Securityユーザ初期化ウィザード）が開いていない場合は、システム トレイの[HP ProtectTools]アイコンを右クリックし、[Embedded Security User Initialization]（Embedded Securityユーザの初期化）を左クリックします。

   [Embedded Security User initialization Wizard]が表示されます。
2. [Next]（次へ）をクリックします。
3. 基本ユーザ キー パスワードを入力して確定し、[Next]をクリックします。

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

4. [Next]をクリックして設定を確定します。

5. [Security Features]（セキュリティ機能）から適切な項目を選択し、[Next]をクリックします。
6. ヘルプ ファイルをスキップするには[Next]をクリックします。
7. 複数の暗号化証明書がある場合は、適切な証明書をクリックします。[Next]をクリックして暗号化証明書を適用します。
8. PSDを適切な設定にして[Next]をクリックします。
9. PSDを再び適切な設定にして[Next]をクリックします。

PSDの最小サイズは50 MB、最大サイズは2000 MBです。

10. [Next]をクリックして設定を確定します。

PSDのサイズによっては、確定の処理に数分かかることがあります。

11. [Finish]（完了）をクリックします。
12. [Yes]（はい）をクリックしてコンピュータを再起動します。

よく実行する作業

ここでは、ユーザおよび管理者が最もよく実行する基本的な作業について説明します。

ユーザの作業

ユーザの基本的な作業には、PSDのセットアップ、ファイルやフォルダの暗号化、および暗号化またはデジタル署名された電子メールの送受信が含まれます。

PSDの使用

PSDを使用するには、PSDパスワードを入力します。PSDが表示され、ファイルが解読されます。PSDは他のドライブと同様に使用できます。

PSDを使用し終わったら、適切な手順でログオフしてください。PSDは自動的に非表示になります。

ファイルおよびフォルダの暗号化

Windows 2000およびWindows XP ProfessionalでEFSを操作するときは、以下の点を考慮してください。

- 暗号化できるのは、NTFSパーティション上のファイルおよびフォルダのみです（FATパーティション上のファイルやフォルダは暗号化できません）。
- システム ファイルおよび圧縮ファイルは暗号化できません。また、暗号化されたファイルは圧縮できません。
- 一時ファイルは攻撃者の標的になる可能性があるため、一時フォルダを暗号化しておく必要があります。
- ユーザが初めてファイルまたはフォルダを暗号化すると、回復ポリシーが自動的にセットアップされます。これによって、ユーザは、証明書および秘密キーをなくした場合でも、回復エージェントを使用して自分のデータを解読できることが保証されます。

ファイルおよびフォルダを暗号化するには、以下の手順で操作します。

1. 暗号化するファイルまたはフォルダを選択します。
2. マウスまたはタッチパッドで右クリックします。
3. **[暗号化]**をクリックします。
4. **[このフォルダのみ変更を適用する]** または **[このフォルダ、およびサブフォルダとファイルに変更を適用する]**をクリックします。
5. **[OK]**をクリックします。

暗号化、デジタル署名、またはその両方を使用した電子メールの送受信

電子メールをデジタル署名および暗号化する手順については、電子メール クライアントのオンライン ヘルプを参照してください。

セキュリティ保護された電子メールを使用するには、最初に、内蔵セキュリティで作成されたデジタル証明書を使用するように、電子メール クライアントを設定する必要があります。デジタル証明書を持っていない場合は、認証機関から入手する必要があります。電子メールの設定方法およびデジタル証明書の入手方法については、電子メール クライアントのオンライン ヘルプを参照してください。

暗号化された電子メール メッセージを送信するには、受信者の公開キーまたは暗号化証明書のコピーが必要です（暗号化証明書には、受信者の公開キーのコピーが含まれています）。

Microsoft Outlookでは、受信者の公開キーを使用して電子メールが暗号化されます。そのため、自分の秘密キーを挿入する必要はありません。ただし、暗号化された電子メールを受信したときは、自分の秘密キーが必要になります。解読するには、暗号化に使用された公開キーに対応する秘密キーを使用する必要があるためです。

管理者の作業

管理者は多くの作業を実行できます。以下に、実行できる作業のいくつかを説明します。詳しくは、HP ProtectTools内蔵セキュリティのヘルプを参照してください。

[Embedded Security Migration Wizard]を使用したキーの移行

移行は、キーおよび証明書を管理、復元、および転送するための、上級管理者向けの作業です。

移行の最初の作業では、移行プロセスの認証、セットアップ、および管理を行います。認証が完了したら、ユーザは、移行元のコンピュータから移行先のコンピュータにキーと証明書をエクスポートおよびインポートできます。

移行について詳しくは、HP ProtectTools内蔵セキュリティのヘルプを参照してください。

情報の回復

チップに障害が発生したり、チップを設定しなおしたりした場合は、次のように情報を回復できます。

- [Emergency Restore Wizard]（緊急リストア ウィザード）を使用して、PSDからデータを復元できます。
- PSDでは、暗号化ファイル システム（EFS）と同様に、回復エージェントを使用した回復もサポートされます。

  お使いのコンピュータに登録済みの回復エージェントがあるかどうかを確認するには、**[スタート]→[コントロール パネル]→[パフォーマンスとメンテナンス]→[管理ツール]→[ローカル セキュリティ ポリシー]→[公開キーのポリシー]→[暗号化されたデータの回復エージェント]**の順に選択します。

詳しくは、オペレーティング システムのオンライン ヘルプを参照してください。

Windows XP Professionalでは、登録済みの回復エージェントが自動的には作成されません。登録済みの回復エージェントをセットアップするには、オペレーティング システムの指示に従ってください。

データを回復するには、登録済みの回復エージェントがデジタル証明書およびキーを持っている必要があります。データ回復の証明書および秘密キーをディスクにエクスポートし、安全な場所に保管して、データ回復の秘密キーをコンピュータから削除してください。これによって、データを回復できるユーザのみが、データ回復の秘密キーに物理的にアクセスできることになります。

コンピュータ セットアップ（F10）ユーティリティを使用した内蔵セキュリティ チップの工場出荷時設定の復元

注意：この作業では、内蔵セキュリティ チップのオーナシップが解放されます。オーナシップが解放されると、内蔵セキュリティ チップを誰でも初期化できる状態になります。

暗号化されたファイルがある場合、内蔵セキュリティ チップを工場出荷時の設定に戻すと、データが失われる恐れがあります。

内蔵セキュリティ チップを工場出荷時の設定に戻すには、以下の手順で操作します。

1. コンピュータの電源を入れるか、**[スタート]→[シャットダウン]→[再起動]**→[OK]の順に選択して再起動します。
2. [Press any key to enter TPM Configuration]というコマンド プロンプトが表示されたら、すぐに任意のキーを押します。
3. スーパバイザ パスワードを入力して**[Enter]**キーを押します。
4. TPMチップをクリアするには**[C]**キーを押します。
5. **[Y]**キーを押して確定します。

   これでチップがクリアされました。

最適な使用方法

内蔵セキュリティを使用するときは、以下のガイドラインに従うことをお勧めします。

- ITセキュリティ管理者は、ユーザにコンピュータを配布する前に、コンピュータ セットアップ（F10）ユーティリティでBIOSスーパバイザ パスワードを設定し、内蔵セキュリティ チップを初期化してください。
- ITセキュリティ管理者は、内蔵セキュリティ ソリューションのセットアップ プロセス中にEmergency Recovery Archiveをセットアップし、ユーザに、データを定期的に保存およびバックアップするよう指示してください。これはシステムに障害が発生した場合に、暗号化されたデータを回復するための唯一の方法です。Emergency Recovery ArchiveとEmergency Recovery Tokenは、個別に保存してください。
- 個々のファイルではなく、フォルダを暗号化します。これによって、ファイルの編集中に作成される一時ファイルも暗号化されます。
- ドメインのメンバであるコンピュータ上の機密データを暗号化します。これによって、オフラインでの暗号解読攻撃によるデータの漏えいを防ぐことができます。
- サーバベースの暗号化されたデータが保存されているサーバは、サーバ全体を定期的にバックアップします。これによって、データを回復する場合に、解読キーが含まれたプロファイルも復元できることが保証されます。
- **[システムの復元]**の監視対象になっている種類のファイルを暗号化する場合は、**[システムの復元]**の監視対象になっていないボリュームにファイルを置きます。
- 複数レベルの暗号化はサポートされません。たとえば、EFS で暗号化されたファイルをPSDに保存したり、PSDに保存されているファイルを暗号化したりしないでください。

よくある質問

コンピュータにHP ProtectTools内蔵セキュリティ チップが搭載されているかどうかは、どのように確認できますか。

チップは、システムに組み込まれたハードウェア コンポーネントです。このコンポーネントが搭載されている場合は、デバイス マネージャに表示されます。

HP ProtectTools内蔵セキュリティ ソフトウェアはどこで入手できますか。

HPのWebサイト（http://www.hp.com/products/security、英語サイト）で、ソフトウェア、ドライバ、およびオンライン ヘルプをダウンロードできます。

HP ProtectTools内蔵セキュリティ ソフトウェアはアンインストールできますか。また、どのようにアンインストールするのですか。

アンインストールできます。Windows標準ソフトウェアの削除手順を使用してアンインストールします。アンインストールを実行する前に、ユーザ固有の保護されたデータを保存してください。保存しないと、データが失われます。アンインストールの最後の手順として、チップを無効にします。

1. コンピュータの電源を入れるか、**[スタート]→[シャットダウン]→[再起動]**→[OK]の順に選択して再起動します。
2. [Press any key to enter TPM Configuration]というコマンド プロンプトが表示されたら、すぐに任意のキーを押します。
3. スーパバイザ パスワードを入力して**[Enter]**キーを押します。
4. TPMチップを無効にするには**[D]**キーを押します。

   これでチップが無効になりました。

トラブルシューティング

内蔵セキュリティが動作しません。どのように対処したらよいですか。

1. システム トレイの[HP ProtectTools]アイコンを右クリックし、[Manage Embedded Security]（Embedded Securityの管理）を左クリックします。
2. [Embedded Security]→[Info]（全般）→[Self Test]（自己診断テスト）の順に選択します。

また、[Embedded Security State]（Embedded Securityの状態）、[Chip]（チップ）、[Owner]（所有者）、および[User]（ユーザ）にチェック マークを入れます。

障害が発生した後でシステムを復元しました。どのような対処が必要ですか。

△ **注意：**通常は、ITシステム管理者がこの手順を実行します。正しく実行されないと、データが永久に失われる恐れがあります。

ProtectToolsチップを交換した後でデータを復元するには、次のものが必要です。

- SPEmRecToken.xml：Emergency Recovery Tokenキー
- SPEmRecArchive.xml：隠しフォルダ。デフォルトの場所は、C:¥Documents and Settings¥All Users¥Application Data¥Infineon¥TPM Software¥Recovery Archive
- ProtectToolsパスワード
  - ❏ Supervisor
  - ❏ Take Ownership
  - ❏ Emergency Recovery Token
  - ❏ Basic User

1. コンピュータの電源を入れるか、**[スタート]→[シャットダウン]→[再起動]→[OK]**の順に選択して再起動します。
2. [Press any key to enter TPM Configuration]というコマンド プロンプトが表示されたら、すぐに任意のキーを押します。
3. スーパバイザ パスワードを入力して**[Enter]**キーを押します。
4. TPMチップをクリアするには**[C]**キーを押します。

5. **[Y]**キーを押して確定します。
6. [**スタート**]→[**シャットダウン**]→[**再起動**]→[OK]の順に選択してコンピュータを再起動します。
7. [Press any key to enter TPM Configuration]というコマンド プロンプトが表示されたら、すぐに任意のキーを押します。
8. スーパバイザ パスワードを入力して**[Enter]**キーを押します。
9. TPMチップを有効にするには**[E]**キーを押します。

   これでチップが有効になりました。
10. Windowsが起動した後、システム トレイの[HP ProtectTools Embedded Security]アイコンを右クリックし、[Embedded Security Initialization]（Embedded Securityの初期化）を左クリックします。
11. [I want to restore the existing Embedded Security]（既存のEmbedded Securityを復元する）チェック ボックスをオンにして、[Next]（次へ）をクリックします。
12. 元のTake Ownershipパスワードを入力して確定し、[Next]をクリックします。
13. [Do not create a recovery archive]（復元用アーカイブを作成しない）→[Next]の順に選択します。

△ **注意：**新しいアーカイブを作成すると、この復元に必要なアーカイブが上書きされるため、データが完全に失われます。

14. リカバリ アーカイブを作成しないで続行するには、[Yes]（はい）をクリックします。
15. [Next]をクリックして設定を確定します。
16. [Browse]（参照）をクリックしてEmergency Archiveの場所を指定します。デフォルトの場所は、C:¥Documents and Settings¥All Users¥Application Data¥Infineon¥TPM Software¥RecoveryArchive¥SPEmRecArchive.xmlです。
17. [Open]（開く）→[Next]の順に選択します。
18. [Browse]をクリックして、最初のHP ProtectTools内蔵セキュリティの初期化で作成されたリカバリ トークンの場所を指定します。トークンをクリックして[Open]をクリックします。
19. トークン パスワードを入力して[Next]をクリックします。

20. マシン名を選択して[Next]をクリックします。
21. [Next]をクリックして設定を確定します。

    復元が失敗したというメッセージが表示されたら、手順1に戻ります。パスワード、トークンの場所と名前、およびアーカイブの場所と名前をよく確認します。
22. ここでユーザ アカウントをセットアップする場合は、[Start Embedded Security User Initialization Wizard]（Embedded Securityユーザ初期化ウィザードを開始する）チェック ボックスが選択されていることを確認します。[Finish]（完了）をクリックします。

手順23～35を実行すると、基本ユーザ キーが復元されます。これらの手順は各ユーザに対して繰り返してください。

23. [Embedded Security User initialization Wizard]（Embedded Securityユーザ初期化ウィザード）が開いていない場合は、システム トレイの[HP ProtectTools Embedded Security]アイコンを右クリックし、[Restore Embedded Security Features]（Embedded Security機能の復元）を左クリックします。

    [Embedded Security User initialization Wizard]が表示されます。
24. [Next]をクリックします。
25. [Recover your basic user key]（基本ユーザ キーの復旧）→[Next]の順に選択します。
26. ユーザを選択し、そのユーザの元の基本ユーザ キーのパスワードを入力して、[Next]をクリックします。
27. [Next] をクリックして設定を確定し、デフォルトの復元データの場所を確定します。
28. [Security Features]（セキュリティ機能）から適切な項目を選択し、[Next]をクリックします。
29. ヘルプ ファイルをスキップするには[Next]をクリックします。
30. 複数の暗号化証明書がある場合は、適切な証明書をクリックします。

    [Next]をクリックして、暗号化証明書を適用します。
31. 該当する箇所で[I want to change my Personal Secure Drive settings]（PSDの設定を変更する）をクリックして、[Next]をクリックします。
32. セキュリティ機能を確定して[Next]をクリックします。

33. 設定を確定して[Next]をクリックします。
34. PSDパスワードを入力して[OK]をクリックします。
35. [Finish]（完了）→[Yes]（はい）の順に選択して再起動します。

注意：基本ユーザ パスワードは安全な場所に保管してください。暗号化されたデータは、このパスワードがないとアクセスしたり復元したりすることができません。

用語集

Emergency Recovery Archive：他のプラットフォームのオーナ 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。

Personal Secure Drive（PSD）：機密データを保護するための記憶領域を提供する機能。

TPM（Trusted Platform Module）：データにハードウェア レベルのセキュリティを提供する機能。内蔵セキュリティ チップは、システムに組み込まれているため、システムの整合性を確認したり、プラットフォームにアクセスする第三者を認証したりすることができます。一方で、正式なユーザにより完全に制御されます。

暗号化：アルゴリズム、暗号法、または、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手順。データの暗号化にはさまざまな種類があります。暗号化は、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）および公開キー暗号があります。

暗号化サービス プロバイダ（CSP）：明確なインタ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を提供する、プロバイダまたはライブラリ。

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。

暗号法：特定の個人のみが解読できるようにデータを符号化する、暗号化および解読の手法および研究分野。データを暗号化および解読するシステムは、暗号システムと呼ばれます。暗号化と解読には、通常、元のデータ（「平文」）を1つ以上の「キー」と組み合わせるためのアルゴリズムが含まれます（キーは、送信者と受信者またはそのどちらか一方のみが知っている数字または文字列です）。結果の出力は、「暗号文」と呼ばれます。

移行：キーおよび証明書を管理、復元、および転送する作業。

解読（暗号化の解除）：暗号文（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。

公開キー基盤（PIK）：証明書および暗号化キーを作成、使用、および管理するためのインタフェースを定義する規格。

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：デジタル文書の送信者の身元を確認し、送信者が文書に署名した後でその文書の内容が変更されていないことを証明するための機能。

認証機関（CA）：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。