

目次

はじめに	2
本書の表記	2
商標および著作権について	3
使用上のご注意	4
1 概要	6
2 動作条件	10
3 作業の流れ	11
4 インストールを行う	12
BIOS の設定を変更する	12
ユーティリティをインストールする	14
ユーティリティの設定を行う	15
ユーティリティの確認を行う	18
アプリケーションをインストールする	19
アプリケーションの設定を行う	20
5 運用上の注意	23
セキュリティチップの運用上の注意	23
鍵のバックアップについて	24
鍵の復元について	26
機器監査について	29
ワークステーションの修理について	30
ワークステーションの廃却について	31
6 こんなときには	32
パスワードを変更するには	32
パスワードを忘れた場合には	32
セキュリティチップの鍵を消去する	34
離席時にワークステーションをロックするには	35
新しいユーザを登録する	36
7 トラブルシューティング	38

はじめに

このたびは弊社の CELSIUS ワークステーション（以降、ワークステーション本体）をご購入いただき、まことにありがとうございます。

本書は、ワークステーション本体に搭載されているセキュリティチップ（以降、本製品）の基本的な取り扱い、セキュリティチップを利用するためのソフトウェアのインストール、およびアプリケーションの設定と使い方について説明しています。

ご使用になる前に本書およびワークステーション本体のマニュアルをよくお読みになり、正しい取り扱いをされますようお願いいたします。

2005 年 8 月

■セキュリティ機能について

セキュリティ機能は完全な認証照合、データやハードウェアの保護を保証するものではありません。当社は、お客様がセキュリティ機能を使用されたこと、または使用できなかったことによって生じるいかなる損害に関しても、一切の責任を負いかねますのであらかじめご了承ください。

本書の表記

本文中に記載されている記号には、次のような意味があります。

記号	意味
 重要	お使いになる際の注意点や、してはいけないことを記述しています。必ずお読みください。
 POINT	操作に関連することを記述しています。必要に応じてお読みください。
→	参照ページや参照マニュアルを示しています。

■コマンド入力（キー入力）

CD-ROM ドライブのドライブ名を、[CD-ROM ドライブ] で表記しています。入力の際は、お使いの環境に合わせて、ドライブ名を入力してください。

例：[CD-ROM ドライブ]：¥setup.exe

■連続する操作の表記

本文中の操作手順において、連続する操作手順を、「→」でつなげて記述しています。

例：「スタート」ボタンをクリックし、「すべてのプログラム」をポイントし、「アクセサリ」をクリックする操作

↓

「スタート」ボタン→「すべてのプログラム」→「アクセサリ」の順にクリックします。

■ 製品の呼び方

本文中の製品名称を、次のように略して表記します。
なお、本書ではお使いの機種以外の情報もありますが、ご了承ください。

製品名称		本文中の表記		
CELSIUS J340	J340	本ワークステーション ワークステーション本体		
CELSIUS N440	N440			
CELSIUS H230	H230			
Microsoft® Windows® XP Professional		Windows XP Professional	Windows XP	Windows
Microsoft® Internet Explorer		Internet Explorer		
Microsoft® Word		Word		
Microsoft® Outlook®		Outlook		
Microsoft® Outlook® Express		Outlook Express		
Netscape® または Netscape® Communicator		Netscape		

商標および著作権について

Microsoft、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または商標です。

Netscape は、米国およびその他の国における Netscape Communications Corporation 社の登録商標です。

FeliCa は、ソニー株式会社の登録商標です。

FeliCa は、ソニー株式会社が開発した非接触 IC カードの技術方式です。

その他の各製品名は、各社の商標、または登録商標です。

その他の各製品は、各社の著作物です。

All Rights Reserved, Copyright© FUJITSU LIMITED 2005

画面の使用に際して米国 Microsoft Corporation の許諾を得ています。

使用上のご注意

■セキュリティチップで利用する鍵や証明書、パスワードの管理について

セキュリティチップは、複数の鍵や証明書を扱います。これらの鍵や証明書を紛失した場合は、その鍵によって暗号化されたファイルなどは読めなくなることがありますので注意してください。また、これらの鍵を利用するときにはパスワードが必要です。パスワードを正しく入力しないと鍵が利用できないため、紛失時と同様に暗号化されたファイルなどが読めなくなります。

■セキュリティチップ利用についてのご注意

- ・本製品で使用するユーティリティおよびアプリケーションをインストールするときには、ワークステーション本体またはネットワーク上のワークステーションに、CD-ROMドライブが搭載／接続されている必要があります。
- ・本ワークステーションの出荷時には、セキュリティチップの設定が使用しない設定になっています。セキュリティチップをお使いになる場合は、BIOS セットアップの設定を「使用する」または「Enabled」に変更してください。
- ・セキュリティチップで鍵を生成する場合、数分かかることがあります。
- ・Infineon Security Platform ユーティリティについては、Infineon Security Platform ユーティリティのマニュアルを参照してください。
- ・SMARTACCESS/Trust アプリケーションについては、SMARTACCESS/Trust アプリケーションのマニュアルを参照してください。
- ・ワークステーション本体が故障したり、本ワークステーションの修理・保守を行ったりすると、暗号化ファイルが読めなくなるなど、セキュリティチップに保護された環境が利用できなくなる場合があります。このような状況に備えて、あらかじめセキュリティチップの鍵などのバックアップが必要です。また、鍵のバックアップは、定期的に行ってください。
 - バックアップを行っていなかった場合や、バックアップファイルを紛失したり、パスワードを忘れたりした場合には、セキュリティチップによって保護されている環境を復元することができません。十分注意して保管してください。
 - 暗号化ファイルや証明書なども必要に応じてバックアップをおこなってください。
 - 復元作業は、パスワードの入力が必要なため、弊社で行うことはできません。お客様ご自身で復元を行ってください。
- ・ワークステーション本体の修理・保守を依頼する場合は、Trusted ログオンを解除してください。

Trusted ログオンを解除していない場合、修理・保守ができないことがあります。Trusted ログオンを解除するには、次の手順を行ってください。

1. 「スタート」ボタン→「すべてのプログラム」→「SMARTACCESS Trust V1.0L22」→「ログオン設定ツール」の順にクリックします。
「ログオン設定ツール」が表示されます。
2. 「ログオン方法変更」をクリックします。

3. 「Trusted ログオン」の「使用する」のチェックを外し、「OK」をクリックします。

Trusted ログオンを使用する設定で機器監査機能をご使用になっている場合に、ワークステーション本体を修理したりハードウェアを変更したりすると、Windows にログオンできなくなることがあります。機器監査機能については、強固なセキュリティが実現できる反面、故障状況によっては復旧がすべて行えないケースがあります。

- ・ワークステーション本体の修理・保守が行われた場合には、セキュリティ機能が解除されていることがあります。その場合には環境の再構築が必要となります。また、暗号化されたファイルやメールが復元できなくなる場合があります。

1 概要

■ セキュリティチップとは

セキュリティチップは、TCG^{注1}の仕様にに基づいた TPM^{注2}と呼ばれる IC チップで TCG セキュリティの基本機能を提供します。セキュリティチップを搭載したワークステーションは、ソフトウェアによる攻撃および物理的な攻撃からデータを保護し、より強固なセキュリティを実現します。

注1: TCG は Trusted Computing Group の略称です。

TCG は、信頼性と安全性を持った新しいコンピュータをつくるためのオープンな業界仕様を策定する団体です。

(<https://www.trustedcomputinggroup.org/>)

注2: TPM は Trusted Platform Module の略称です。

■ セキュリティチップの機能

セキュリティチップは、各ユーザに固有の鍵を生成し、証明書を管理します。この鍵と証明書を用いることにより、セキュリティチップは暗号化や認証を行います。セキュリティチップ内に保有する鍵は、取り出すことが不可能なため鍵の解読ができません。そのため暗号化されたデータや認証は安全に行われます。ユーザはこの鍵と証明書を利用するためのパスワードを設定します。

■ セキュリティチップの利用

セキュリティチップを利用するために、次のアプリケーションおよび証明書を使用します。

- Infineon TPM Professional Package (Infineon Security Platform) ユーティリティ
- SMARTACCESS/Trust アプリケーション
- VeriSign 証明書

これらのアプリケーションおよび証明書により、次のことが行えるようになります。

□ IEEE802.1x 認証ファイルの管理

IEEE802.1x で利用する証明書を、セキュリティチップで管理することができます。

□ ファイルとフォルダの暗号化 -EFS (Encrypting File System)

ユーティリティでファイルとフォルダの暗号化を設定することにより、EFS による暗号化に利用される鍵をセキュリティチップで安全に保管します。

重要

- ▶ EFS を利用するには、ハードディスクが NTFS でフォーマットされている必要があります。
- ▶ ハードディスク全体を暗号化することはできません。

□ セキュア E-Mail

ユーティリティで E-Mail の保護を設定することにより、E-Mail の暗号用の証明書をセキュリティチップで安全に管理します。

□ Word マクロへの署名

ユーティリティでセキュリティ機能を設定することにより、Word マクロへの署名をセキュリティチップで安全に保護します。

□ Windows ログオンにセキュリティチップを利用する

SMARTACCESS/Trust で Trusted ログオンを設定することにより、Windows ログオン時のパスワードをセキュリティチップで安全に保存することができます。

□ ワークステーション本体の不正なハードウェアの変更の検出

SMARTACCESS/Trust の「機器監査」機能を利用すれば、Windows ログオン時ワークステーション本体の機器構成のチェックを行います。ハードウェア構成または設定が不正に変更されていることを検出した場合は、Windows ログオンを許可しないようにすることができます。

□ ID・パスワード入力をセキュリティチップで管理する

次の場合に、ID・パスワードを SMARTACCESS/Trust に登録しておくと、セキュリティチップによって保護されるため安全に管理することができます。

- ・アプリケーションによりポップアップ画面に表示される ID・パスワード入力要求
- ・ Internet Explorer によりホームページに表示される ID・パスワード入力要求

また、一度登録すると、ID・パスワードのフォームは自動で認識され、再び入力することなく利用できます。

□ シングルサインオンを利用する

SMARTACCESS/Trust にはシングルサインオンの機能があります。一度セキュリティチップのパスワードを入力するか、Trusted ログオンを行えば、SMARTACCESS/Trust が管理する ID やパスワードは自動で入力されます。

□ VeriSign 証明書の利用

セキュリティチップと連携した VeriSign 発行の証明書を、登録した日から 1 年間無料で利用できます。これを利用することにより、例えばセキュア E-mail を利用する場合などは、VeriSign 認証局に証明された証明書を利用できるため、より安全なデータを送受信することができます。

POINT

- ▶ VeriSign 証明書は、セキュリティチップのユーティリティをインストールし、設定を完了して利用可能にしてからインストールを行ってください。インストールについては、ドライバディスク内の「¥other¥tpm¥ifxsw20¥verisign.txt」をご覧ください。
- ▶ VeriSign 証明書は、登録した日から 1 年間利用できます。それ以降は、E-mail などで証明書を利用することはできません。ただし、古いメールなどで利用していた場合には、読むことのみ可能です。
- ▶ 1 年間の利用期間終了後もご利用を希望の場合は、弊社担当営業員までご連絡ください。その場合有料による継続となります。

□ 他のセキュリティ機能を連携した利用

セキュリティチップは、ワークステーション本体で利用できる他のセキュリティ機能と連携して使用することが可能です。連携できるセキュリティ機能には、次のものがあります。

- ・スマートカード
- ・指紋センサー
- ・FeliCa 対応リーダー／ライター

連携の方法などは、SMARTACCESS/Trust 添付のマニュアルを参照してください。

■セキュリティチップの管理

セキュリティチップには、セキュリティチップの管理を行う「所有者」とセキュリティチップを使用する「ユーザ」を登録します。

所有者およびユーザは次の鍵および証明書やファイルを作成・利用します。

□「所有者」が管理するもの

所有者キーと所有者パスワード

所有者は、所有者であることを証明するキーを作成します。このキーはセキュリティチップにより保護され、所有者パスワードを入力することによって利用することができます。所有者パスワードは忘れないよう注意してください。

自動バックアップファイルと復元用トークン

セキュリティチップで管理しているすべての鍵や証明書のバックアップを行います。バックアップはスケジュールを設定することにより定時に行うことができます。

セキュリティチップが故障しても、新しいワークステーションでこのファイルを用いて復元することにより、以前利用していた暗号化ファイルなどが利用できるようになります。

自動バックアップファイルは、トークンにより暗号化されています。自動バックアップファイルを利用する場合には、トークンファイルとそのパスワードが必要です。トークンファイルを失くしたり、パスワードを忘れたりしないよう注意して管理してください。

パスワードリセットファイルとリセットトークン

ユーザがセキュリティチップのパスワードを忘れた場合に備え、現状のパスワードを新規パスワードに変更することができます。パスワードの変更はユーザが行います。所有者はパスワードリセットファイルを発行することにより、ユーザにパスワード変更の許可を与えます。

パスワードリセットファイルは、トークンにより暗号化されています。パスワードリセットファイルを利用する場合には、トークンファイルとそのパスワードが必要です。トークンファイルを失くしたり、パスワードを忘れたりしないよう注意して管理してください。

□「ユーザ」が管理するもの

ユーザーキーとユーザーキーパスワード

ユーザはセキュリティチップを利用する場合、ユーザーキーを作成します。このキーはセキュリティチップにより保護され、ユーザーキーパスワードを入力することによって利用することができます。キーを紛失した場合は、それ以前に暗号化していたデータやファイルなどを再び利用することができなくなります。管理には注意してください。また、パスワードを忘れた場合も、キーが利用できなくなるため、それまでに暗号化していたデータやファイルを再び利用することができなくなります。パスワードは忘れないよう注意してください。

パスワードリセットファイル

ユーザがセキュリティチップのパスワードを忘れた場合に備えて、現状のパスワードを新規パスワードに変更することができます。このため前もってパスワードリセット用のファイルを作成しておきます。

キーのバックアップ

キーを紛失した場合に備えて、バックアップファイルを作成することが可能です。バックアップファイルはユーザーキーパスワードによって保護されます。

2 動作条件

本製品をご使用になる前に、次の条件を確認してください。

■ 対応機種／OS

本製品が搭載されている CELSIUS ワークステーション／Windows XP

POINT

- ▶ WEB ページをご覧になるためのアプリケーションとして、Internet Explorer 6.0 以降または Netscape 4.78/7.0 以降が必要です。
- ▶ セキュア E-mail を利用するには、Outlook 2000/2002 以降、Outlook Express 6.0 以降、または Netscape 4.78/7.0 以降が必要です。
- ▶ Word マクロへの署名を利用するには、Word 2000/2002 以降が必要です。
- ▶ VeriSign 証明書を利用するには、Internet Explorer 6.0 または Netscape 4.78/7.0 が必要です。
- ▶ SMARTACCESS/Trust での、アプリケーションによりポップアップ画面に表示される ID・パスワード入力要求機能は、Netscape ではお使いになれません。

3 作業の流れ

本製品を使用するまでの手順は次のとおりです。

1 必要なものを用意します。

- ・ワークステーション本体
- ・ドライバズディスク

2 BIOS の設定を変更します。

「BIOS の設定を変更する」(→ P.12)

1. BIOS の「管理者用パスワード」を設定します。
2. セキュリティチップを「使用する」に設定します。

3 ユーティリティをインストールします。

「ユーティリティをインストールする」(→ P.14)

4 ユーティリティの設定を行います。

「ユーティリティの設定を行う」(→ P.15)

「ユーティリティの確認を行う」(→ P.18)

1. 所有者のパスワードを設定します。
2. 緊急時復元用アーカイブを保存します。
3. 緊急時復元用トークンのパスワードを設定します。
4. 緊急時復元用トークンを保存します。
5. 基本ユーザーキーパスワードを設定します。
6. 電子メールの保護と、ファイルとフォルダの暗号化を設定します。
7. 設定の確認を行います。

5 アプリケーションをインストールします。

「アプリケーションをインストールする」(→ P.19)

6 アプリケーションの設定を行います。

「アプリケーションの設定を行う」(→ P.20)

1. Trusted ログオンを設定します。
2. 機器構成を登録し、機器監査を設定します。
3. 一時中止パスワードを設定します。
4. Windows ログオンを Trusted ログオンに変更します。

4 インストールを行う

BIOS の設定を変更する

本製品を使用する前に、必ず BIOS の設定を変更してください。

POINT

- ▶ BIOS セットアップについては、ワークステーション本体の『CELSIUS マニュアル』の「BIOS」を参照してください。

■ J340、N440 の場合

- 1 ワークステーション本体の電源を入れ、BIOS セットアップを起動します。**
BIOS セットアップ画面が表示されます。
BIOS セットアップで管理者用パスワードを設定済の場合は、手順 7 へ進んでください。設定していない場合には、手順 2 へ進んでください。

重要

- ▶ 本製品を使用するには、BIOS セットアップで管理者用パスワードを設定する必要があります。

- 2 Security メニューで「Set Supervisor Password」を選択して、【Enter】キーを押します。**
パスワード入力用のウィンドウが表示されます。
- 3 8 桁までのパスワードを入力します。**
入力できる文字種はアルファベットと数字です。
入力された文字は表示されず、代わりに「■」が表示されます。
- 4 パスワードを入力したら、【Enter】キーを押します。**
「Confirm New Password」にカーソルが移り、パスワードの再入力を求められます。
- 5 手順 3 で入力したパスワードを再度入力して【Enter】キーを押します。**
「Setup Notice」と書かれたウィンドウが表示されます。
- 6 【Enter】キーを押します。**
再入力したパスワードが間違っていた場合は、「Setup Warning」と書かれたウィンドウが表示されます。【Enter】キーを押して、手順 3 からやり直してください。
- 7 【↑】キーまたは【↓】キーでカーソルを移動し、「Security Chip Setting」を選択して【Enter】キーを押します。**
設定変更画面が表示されます。

- 8 **【Space】キーまたは【-】キーを押して、「Security Chip」の項目を「Enabled」に設定します。**
- 9 **Exit メニューが表示されるまで、何度か【Esc】キーを押します。**
- 10 **【↑】キーまたは【↓】キーを押して「Exit Saving Changes」を選択し、【Enter】キーを押します。**
「Save Configuration Changes and exit now?」と書かれたウィンドウが表示されます。
- 11 **【←】キーまたは【→】キーを押して「Yes」を選択し、【Enter】キーを押します。**
BIOS セットアップが終了し、ワークステーション本体が再起動します。

重要

- ▶ セキュリティチップの設定を有効にするには、BIOS セットアップ終了後にワークステーション本体の再起動が必要です。終了メニューで「Exit Saving Changes」を行っただけで電源を切ってしまうと、設定が正しく行われませんのでご注意ください（次回起動時にエラーメッセージが表示されます）。

■ H230 の場合

- 1 **ワークステーション本体の電源を入れ、BIOS セットアップを起動します。**
BIOS セットアップ画面が表示されます。
BIOS セットアップで管理者用パスワードを設定済の場合は、手順 7 へ進んでください。設定していない場合には、手順 2 へ進んでください。
-  **重要**
 - ▶ 本製品を使用するには、BIOS セットアップで管理者用パスワードを設定する必要があります。
- 2 **セキュリティメニューで「管理者用パスワード設定」を選択して、【Enter】キーを押します。**
パスワード入力用のウィンドウが表示されます。
- 3 **8 桁までのパスワードを入力します。**
入力できる文字種はアルファベットと数字です。
入力された文字は表示されず、代わりに「■」が表示されます。
- 4 **パスワードを入力したら、【Enter】キーを押します。**
「新しいパスワードを確認してください。」にカーソルが移り、パスワードの再入力を求められます。
- 5 **手順 3 で入力したパスワードを再度入力して【Enter】キーを押します。**
「セットアップ通知」ウィンドウが表示されます。
- 6 **【Enter】キーを押します。**
再入力したパスワードが間違っていた場合は、「セットアップ警告」ウィンドウが表示されます。【Enter】キーを押して、手順 3 からやり直してください。

- 7 【↑】キーまたは【↓】キーでカーソルを移動し、「セキュリティチップ設定」を選択して【Enter】キーを押します。
「セキュリティチップ設定」が表示されます。
- 8 【Space】キーまたは【-】キーを押して、「セキュリティチップ」の項目を「使用する」に設定します。
- 9 終了メニューが表示されるまで、何度か【Esc】キーを押します。
- 10 【↑】キーまたは【↓】キーを押して「変更を保存して終了する」を選択し、【Enter】キーを押します。
「セットアップ確認」ウィンドウが表示されます。
- 11 【←】キーまたは【→】キーを押して「はい」を選択し、【Enter】キーを押します。
BIOS セットアップが終了し、ワークステーション本体が再起動します。

重要

- ▶「セキュリティチップ」の設定を有効にするには、BIOS セットアップ終了後にワークステーション本体の再起動が必要です。終了メニューで「変更を保存する」を行っただけで電源を切ってしまうと、設定が正しく行われませんのでご注意ください（次回起動時にエラーメッセージが表示されます）。

ユーティリティをインストールする

BIOS の設定変更後、ワークステーション本体が再起動したら、ユーティリティをインストールします。

重要

- ▶ユーティリティをインストールするには、管理者権限で Windows にログオンする必要があります。

POINT

- ▶ユーティリティをインストールする前に、他の使用中のアプリケーションはすべて終了させてください。

- 1 「ドライバズディスク」をセットします。
- 2 「スタート」ボタン→「ファイル名を指定して実行」の順にクリックします。
- 3 「名前」の欄に次のように入力し、「OK」をクリックします。

[CD-ROM ドライブ] : ¥other¥tpm¥ifixsw20¥install.bat

「Infineon TPM Professional Package 用の InstallShield ウィザードへようこそ」が表示されます。

- 4 「次へ」をクリックします。
「ライセンス契約」が表示されます。
- 5 「はい」をクリックします。
「ユーザ情報」が表示されます。
- 6 ユーザ名と所属を入力し、「次へ」をクリックします。
「セットアップタイプ」が表示されます。

 POINT

▶ 所属は省略することもできます。

- 7 「カスタム」を選択し、「次へ」をクリックします。
「カスタムセットアップ」が表示されます。
- 8 「次へ」をクリックします。
「プログラムをインストールする準備ができました」と表示されます。

 POINT

▶ 「カスタムセットアップ」では何も変更する必要はありません。

- 9 「インストール」をクリックします。
インストールが開始します。しばらくして、インストールが終了すると、「InstallShield
ウィザードを完了しました」が表示されます。
- 10 「完了」をクリックします。
メモ帳が表示されます。読み終わったらメモ帳を終了してください。再起動を要求
するメッセージが表示されます。
- 11 「はい」をクリックします。
ワークステーション本体が再起動します。
- 12 「スタート」ボタン→「ファイル名を指定して実行」の順にクリックします。
- 13 「名前」の欄に次のように入力し、「OK」をクリックします。
[CD-ROM ドライブ] : ¥other¥tpm¥ifxsw20¥F5FPRGCH.exe
「修正を完了しました。」と表示されます。
- 14 「OK」をクリックした後、Windows を再起動してください。

ユーティリティの設定を行う

ユーティリティのインストール終了後、ワークステーション本体が再起動したら、ユーティリティで「プラットフォーム初期化ウィザード」を行い、セキュリティチップの所有者を設定します。その後「ユーザー初期化ウィザード」でユーザの設定を行います。

重要

- ▶ ユーティリティの設定を行うには、管理者権限を持ったユーザとして Windows にログオンする必要があります。

1 管理者権限を持ったユーザーとして、Windows にログオンします。

通知領域の「Infineon Security Platform」アイコンから、「Security Platform が初期化されていません」というメッセージが表示されます。

2 通知領域の「Infineon Security Platform」アイコンをクリックします。

メニューが表示されます。

3 「Security Platform の初期化」を選択します。

「Infineon Security Platform 初期化ウィザードへようこそ」が表示されます。

4 「次へ」をクリックします。

「初期化」が表示されます。

5 「新しく Security Platform を初期化する」にチェックが入っていることを確認し、「次へ」をクリックします。

「Security Platform 所有者を作成します。」が表示されます。

6 「パスワード」と「パスワードの確認入力」に Security Platform 所有者のパスワードを入力し、「次へ」をクリックします。

「機能」が表示されます。

7 「自動バックアップ」および「パスワードリセット」にチェックが入っていることを確認し、「次へ」をクリックします。

「自動バックアップ」が表示されます。

8 「バックアップの場所」にバックアップの場所を設定します。自動バックアップのスケジュールを変更する場合は、「スケジュール」をクリックして設定し、「次へ」をクリックします。

「緊急時復元」が表示されます。

重要

- ▶ 自動バックアップのアーカイブは大切なファイルです。ハードディスク内の削除されない場所を指定してください。また、保存場所も記憶しておいてください。
 - ▶ スケジュールで設定された時間にワークステーション本体の電源が入っていない場合には、自動バックアップは実行されません。
- #### 9 「新しい復元用トークンを作成する」をチェックし、「ファイルの場所」に緊急時復元用トークンの保存場所を設定します。

 重要

- ▶「ファイルの場所」には仮の場所が表示されています。緊急時復元用トークンは、リムーバブルドライブなど、ワークステーション本体とは別の場所に保管できる媒体に保存することをお勧めします。
- ▶復元用トークンファイルとトークンアーカイブは紛失しないよう注意して管理してください。

10 「パスワード」と「パスワードの確認入力」に緊急時復元用トークンのパスワードを入力し、「次へ」をクリックします。

「パスワードリセット」が表示されます。

11 「新しいトークンを作成する」をチェックし、「ファイルの場所」でパスワードリセットトークンの保存場所を設定します。

 重要

- ▶「ファイルの場所」には仮の場所が表示されています。パスワードリセットトークンは、リムーバブルドライブなど、ワークステーション本体とは別の場所に保管できる媒体に保存することをお勧めします。
- ▶パスワードリセットトークンファイルとトークンアーカイブは失くしたり、忘れたりしないよう注意して管理してください。

12 「パスワード」と「パスワードの確認入力」にパスワードリセットトークンのパスワードを入力し、「次へ」をクリックします。

「サマリー」が表示されます。

13 「次へ」をクリックします。

しばらくすると、「ウィザードが正常に終了しました。」が表示されます。

14 「Security Platform ユーザー初期化ウィザードを起動する」をチェックして「完了」をクリックします。

「Infineon Security Platform ユーザー初期化ウィザードへようこそ」が表示されます。

15 「次へ」をクリックします。

「基本ユーザーキーパスワード」が表示されます。

16 「パスワード」と「パスワードの確認入力」に基本ユーザーパスワードを入力し、「次へ」をクリックします。

「基本ユーザーパスワードリセット」が表示されます。

17 「緊急時の基本ユーザーパスワードのリセットを有効にする」にチェックが入っていることを確認し、「個人シークレットの場所」を設定します。

 重要

- ▶「個人シークレットの場所」には仮の場所が表示されています。個人シークレットファイルは、リムーバブルドライブなど、ワークステーション本体とは別の場所に保管できる媒体に保存することをお勧めします。

18 「次へ」をクリックします。

「パスワードと認証」が表示されます。

19 「次へ」をクリックします。

しばらくすると、「Security Platform の機能」が表示されます。

20 「電子メールの保護」、「暗号化ファイルシステム (EFS) によるファイルとフォルダの暗号化」にチェックが入っていることを確認し、「次へ」をクリックします。

「電子メールの保護の設定をしてください。」が表示されます。

重要

▶「電子メールの保護」と「暗号化ファイルシステム (EFS) によるファイルとフォルダの暗号化」の他に「Personal Secure Drive」が表示されていることがありますが、チェックしないでください。本機能はサポートしていません。

21 「次へ」をクリックします。

「暗号化証明書」が表示されます。

22 「選択」をクリックします。

「Infineon Security Platform 証明書の選択」が表示されます。

23 「作成」をクリックします。

しばらくすると、証明書が作成されます。

24 リストから「発行先」に表示された自分のユーザ ID を選択し、「選択」をクリックします。

25 「発行先」が自分になっていることを確認し、「次へ」をクリックします。

「設定を確認してください。」が表示されます。

26 「次へ」をクリックします。

しばらくすると、「ウィザードが正常に終了しました。」が表示されます。

27 「完了」をクリックします。

以上で、Infineon Security Platform ソリューションによる TCG セキュリティ機能が利用できる環境が整いました。

ユーティリティの確認を行う

ユーティリティのインストールと設定が完了したら、次の手順で正しく設定されたか確認してください。

1 「スタート」ボタン→「すべてのプログラム」→「Infineon Secure Platform ソリューション」の「Security Platform を管理します」の順にクリックします。

「Infineon Security Platform 設定ツール」が表示されます。

- 2 「全般」タブをクリックします。
- 3 「Security Platform の状態」が次の状態になっていることを確認します。
「Chip」：有効
「所有者」：初期化済み
「ユーザー」：初期化済み
- 4 「OK」をクリックし、「Infineon Security Platform 設定ツール」を終了します。

アプリケーションをインストールする

ユーティリティの設定が完了したら、SMARTACCESS/Trust アプリケーションをインストールします。

重要

- ▶ アプリケーションをインストールするには、管理者権限を持ったユーザとして、Windows にログオンする必要があります。

POINT

- ▶ アプリケーションをインストールする前に、他の使用中のアプリケーションはすべて終了させてください。

- 1 「ドライバズディスク」をセットします。
- 2 「スタート」ボタン→「ファイル名を指定して実行」の順にクリックします。
- 3 「名前」の欄に次のように入力し、「OK」をクリックします。
[CD-ROM ドライブ]：¥other¥tpm¥satrtrust¥setup.exe
「SMARTACCESS/Trust V1.0L22 をコンピュータにインストールします。」が表示されます。
- 4 「次へ」をクリックします。
「セットアップは次のフォルダに SMARTACCESS/Trust V1.0L22 をインストールします。」が表示されます。
- 5 インストール先のフォルダを選択して、「次へ」をクリックします。
インストールが開始されます。
しばらくすると、「SMARTACCESS/Trust V1.0L22 のインストールを完了しました。」が表示されます。

POINT

- ▶ インストール先のフォルダは通常変更する必要はありません。変更すると不都合が発生することもあるため、ワークステーションに詳しい方以外は変更しないでください。

6 「完了」をクリックします。

再起動を要求するメッセージが表示されます。

7 「はい」をクリックします。

ワークステーション本体が再起動します。

アプリケーションの設定を行う

アプリケーションのインストールが終わったら、アプリケーションの設定を行います。アプリケーションにより Windows のログオンパスワードなどをセキュリティチップに保存するので、パスワードを安全に管理できます。

POINT

- ▶ 必ず管理者でログオンしてください。
- ▶ 他のアプリケーションはすべて終了させてください。
- ▶ 他のセキュリティ機能により Windows ログオンを行っている場合は、その利用を止めてから設定するか、セキュリティチップで行うのをやめてください。
- ▶ アプリケーションの設定については、SMARTACCESS/Trust アプリケーションのマニュアルを参照してください。

重要

- ▶ 設定の途中で、現在のワークステーション本体の機器構成を登録する作業を行います。機器構成を登録すると、現在の BIOS ハードウェア設定などを保存します。登録を行う前に BIOS 設定を含めたハードウェア設定（機器構成）を完了してから行ってください。

1 「スタート」ボタン→「すべてのプログラム」→「SMARTACCESS Trust」→「ログオン設定ツール」の順にクリックします。

「ログオン設定ツール」が表示されます。

2 ユーザーキーパスワードを入力し「OK」をクリックします。

3 「Trusted ログオン」の「登録」をクリックします。

「Trusted ログオン情報登録」が表示されます。

4 「Windows ログオン」に、Windows ログオン時の「ユーザー名」、「ドメイン名」、「パスワード」、および「パスワード確認入力」を入力します。

POINT

- ▶ ドメインを利用していない場合は「ドメイン名」の入力は不要です。

5 「登録するユーザーのユーザーキーパスワード」に、パスワードを入力し、「OK」をクリックします。

「Trusted ログオン情報を設定しました。」が表示されます。

6 「OK」をクリックします。

「ログオン設定ツール」に戻ります。

□ 機器監査の設定を行う

つづいて、機器監査の設定を行います。機器監査の設定を行わない場合は、「シングルサインオンの設定を行う」(→ P.21)に進んでください。

7 「Trusted ログオン」の「機器構成設定」をクリックします。

「Trusted ログオン機器構成情報登録」が表示されます。

8 「現状登録」をクリックします。

「現在の機器構成を登録しますか?」が表示されます。

9 「はい」をクリックします。

「Trusted ログオン機器構成情報登録」に戻ります。

重要

▶ Windows が起動される直前の機器構成が登録されます。マルチペイの変更など、Windows の起動後に行った機器の変更は登録されませんのでご注意ください。

10 「起動時に機器監査実行」をチェックします。

11 「起動時に機器構成が異なる場合のログオン」を「ログオンしない」にチェックして、「OK」をクリックします。

「ログオン設定ツール」に戻ります。

重要

▶ 機器監査で検出されるハードウェアの変更については、「機器監査について」(→ P.29)を参照してください。機器構成を不用意に変更すると、ログオンが行えなくなる可能性がありますので十分にご注意ください。再度、機器構成の変更が必要となった場合は、必ず「起動時に機器監査実行」を一度オフにしてから行ってください。

12 「一時中止パスワード」をクリックし、パスワードを入力し、「OK」をクリックします。

「一時中止パスワードを登録しました。」が表示されます。

重要

▶ 一時中止パスワードは、セキュリティチップに不具合が発生したときなど Trusted ログオンができなくなった場合に、一時的に Windows ログオンに切り替えるための手段です。
▶ 一時中止パスワードで Windows にログオンしても、セキュリティチップによって暗号化されたファイルなどは、安全に保護されています。これらファイルは、ユーザーキーパスワードを入力するまで見ることはできません。

13 「OK」をクリックします。

「ログオン設定ツール」に戻ります。

□ シングルサインオンの設定を行う

つづいて、シングルサインオンの設定を行います。シングルサインオンの設定を行わない場合は、手順 16 に進んでください。

14 「その他」の「動作環境設定」をクリックします。

「動作環境設定」が表示されます。

15 「シングルサインオン」の「有効にする」にチェックし、「OK」をクリックします。

「ログオン設定ツール」に戻ります。

16 「ログオン方法変更」をクリックし、「Trusted ログオン」を「使用する」にチェックし、「OK」をクリックします。

「本製品以外のログオン認証が有効になっている場合・・・」の確認画面が表示されます。

17 「OK」をクリックします。

「ログオン方法を変更しました。」が表示されます。

18 「OK」をクリックします。

「ログオン設定ツール」に戻ります。

19 「閉じる」をクリックします。

再起動を要求するメッセージが表示されます。

20 「はい」をクリックします。

ワークステーション本体が再起動します。

 POINT

- ▶ 設定後は、Windows ログオン画面は「ようこそ」表示から「クラシック」表示に切り替わります。
- ▶ Windows ログオンの方法は次の手順になります。
 1. Windows を起動後、画面の指示に従い、【Ctrl】+【Alt】+【Del】キーを押します。
「Trusted ログオン」画面が表示されます。
 2. ユーザー名とユーザーキーパスワードを入力します。
Windows にログオンします。

5 運用上の注意

セキュリティチップの運用上の注意

セキュリティチップを利用するための環境設定が完了すると、ファイルやフォルダの暗号化、メールの証明書の管理などがより安全な環境で運用できるようになります。故障や修理などでワークステーション本体の設定が変更された場合、セキュリティチップにより保護された情報が利用できなくなることがあります。これらの場合に備えて、次の点に注意して運用してください。

□ 定期的にセキュリティチップの鍵のバックアップを行う

必ずセキュリティチップによって管理されている鍵のバックアップを行ってください。

重要

▶ バックアップファイルを紛失したり、パスワードを忘れたりすると、セキュリティチップが利用できなくなります。バックアップファイルやその時に設定したパスワードは、紛失したり忘れたりしないよう注意して管理してください。

バックアップの方法については、「鍵のバックアップについて」(→ P.24)を参照してください。

▶ バックアップを行うと、次のファイルとパスワードが生成されます。

利用者	ファイル	ファイル名
所有者	所有者パスワード	
	システム復旧ファイル	spsystembackup.xml
	緊急時復元用トークン	spemrectoken.xml
	緊急時復元用トークンパスワード	
	パスワードリセットファイル	sppwdresetsecret.xml
	パスワードリセットトークン	sppwdresettoken.xml
	パスワードトークンパスワード	
	(基本) ユーザーパスワード	
ユーザ	(基本) ユーザーパスワード	
	パスワードリセットトークン	sppwdresetsecret.xml
	パスワードトークンパスワード	

▶ 復元作業は、パスワードの入力などが必要なため、弊社で行うことはできません。「鍵の復元について」(→ P.26)に従って注意して復元してください。

□ 機器監査を行っている場合は、修理またはハードウェア変更を行う前に Trusted ログオンを一時的に解除する

Trusted ログオンを使用する設定にして機器監査を行っている場合、修理したり、ハードウェアの設定を変更したりすると、Windows にログオンできなくなることがあります。

必ず Trusted ログオンを使用しない設定に変更してください。

重要

- ▶ ワークステーションの修理またはハードウェアの変更を行う前に、一時的に Trusted ログオンを行わない設定に変更してください。変更方法については、「ワークステーションの修理について」(→ P.30) を参照してください。

POINT

- ▶ 次のような状況が起きた場合に、セキュリティチップが利用できなくなると考えられます。
 - ・セキュリティチップの故障
 - ・ハードディスクのリカバリ
 - ・ワークステーションの部品の交換

鍵のバックアップについて

鍵のバックアップは、利用中のセキュリティチップにより保護された環境に何らかの変更があった場合に、以前の環境を引き続き利用するときに必要な準備をするための作業です。セキュリティチップの中の鍵を取り出して保存することではありません。

所有者でログオンした時に、通知領域から表示される内容により、次の手順に従って処理を行ってください。

所有者はセキュリティチップのバックアップと各ユーザのバックアップを行う必要があります。

各ユーザでバックアップを行う必要はありませんが、復元を行った後ユーザーキーパスワードを入力する必要があります。

重要

- ▶ バックアップ処理は、セキュリティチップを設定した時のパスワードによって保護されています。そのため、セキュリティチップを設定した人が行う必要があります。
- ▶ ほとんどの設定は「Security Platform の初期化」時および「Security Platform のユーザ初期化」時に行われます。そのときに作成したファイルを注意して管理する必要があります。また、修理などを行う前に行っておかなければならない手順もあります。次の手順に従い注意して管理してください。
- ▶ 手順に従ってファイルや設定変更を行わない場合、セキュリティチップで管理していた環境が利用できなくなることがあります。
- ▶ ここで説明する手順は、セキュリティチップの鍵についてバックアップを行う場合の手順です。暗号化ファイルや証明書、および SMARTACCESE/Trust の設定については行われません。必要に応じて別途バックアップを行ってください。SMARTACCESS/Trust のバックアップについては、SMARTACCESS/Trust アプリケーションのマニュアルにある「ログオン情報を移行する」を参照してください。

POINT

- ▶ 操作については、Infineon Security Platform ソリューションのマニュアルを参照してください。

□ 所有者が行う作業

所有者が行う作業は「Security Platform の初期化」時の「自動バックアップ」の設定時にほぼ完了しています。

すぐにバックアップを行う場合には、次の手順で行います。

 重要

- ▶ 自動バックアップファイルは、スケジュールで設定した時刻に作成または更新されます。
- ▶ スケジュールで設定した時刻にワークステーションの電源が入っていなかった場合には、自動バックアップは実行されません。

- 1 「スタート」ボタン→「ファイル名を指定して実行」の順にクリックします。
- 2 「名前」の欄に次のように入力し、「OK」をクリックします。「Infineon Security Platform ソリューション」のインストール場所を変更した場合は、「参照」をクリックして変更先のフォルダ内にある「spbackupwz.exe」を指定し、「名前」の欄に表示されるファイル名に続けて「/backupall」を入力します。

```
"c:\program files\infineon\security platform software\spbackupwz.exe"
/backupall
```

- 3 「OK」をクリックします。

☐ ユーザが行う作業

所有者によって自動バックアップファイルが作成されるため、バックアップなどの準備は必要ありませんが、パスワードを入力する必要があります。
念のためバックアップを行う場合は、次の手順で行います。

 重要

- ▶ 次の手順では、作業を行うユーザの鍵のみがバックアップされます。所有者用の鍵や他のユーザの鍵はバックアップされません。

- 1 通知領域の「Infineon Security Platform」アイコンをクリックし、表示されるメニューから「Security Platform を管理する」を選択します。
「Infineon Security Platform 設定ツール」が表示されます。
- 2 「バックアップ」タブを選択し、「バックアップ」をクリックします。
「バックアップ」が表示されます。
- 3 「参照」をクリックし、鍵(ファイル)をバックアップする場所を選択します。
- 4 「次へ」をクリックします。
「サマリー」が表示されます。
- 5 「次へ」をクリックします。
鍵(ファイル)が保存されると、「ウィザードが正常に終了しました。」が表示されます。
- 6 「完了」をクリックします。

鍵の復元について

鍵の復元は、利用中のセキュリティチップにより保護された環境に何らかの変更があった場合に、以前の環境を引き続き利用するための作業です。

所有者はセキュリティチップの復元と各ユーザの復元を行う必要があります。

ユーザは、復元を行う必要はありませんが、所有者が復元を行った後にユーザーキーパスワードを入力する必要があります。

鍵の復元については、どのような状態から復元を行うかによって作業手順が異なります。

所有者でログオンした時に、通知領域にメッセージが表示されます。表示される内容により、次の手順に従って処理を行ってください。

重要

- ▶ 復元処理は、セキュリティチップを設定した時のパスワードによって保護されています。そのため、復元処理はセキュリティチップを設定した人が行う必要があります。
- ▶ ほとんどの設定は「Security Platform の初期化」時および「Security Platform のユーザ初期化」時に行われます。そのときに作成したファイルを注意して管理する必要があります。また、ワークステーションの修理などを行う前にしておかなければならない作業もあります。次の手順に従い注意して管理してください。
- ▶ 手順に従ってファイルや設定変更を行わない場合、セキュリティチップで管理していた環境が、利用できなくなることがあります。
- ▶ ここで説明する手順は、セキュリティチップの鍵について復元を行う場合の手順です。暗号化ファイルや証明書、および SMARTACCESE/Trust の設定については行われません。必要に応じて別途復元を行ってください。
SMARTACCESS/Trust のバックアップについては、SMARTACCESS/Trust アプリケーションのマニュアルにある「ログオン情報を移行する」を参照してください。

POINT

- ▶ 操作については、Infineon Security Platform ツールのマニュアルを参照してください。

■ 通知領域またはタスクトレイから「Security Platform を復元します。」と表示された場合

□ 所有者が行う作業

- 1** 通知領域の「Infineon Security Platform」アイコンをクリックし、表示されるメニューから「Security Platform を復元する」を選択します。
「Infineon Security Platform 初期化ウィザードへようこそ」が表示されます。
- 2** 「次へ」をクリックします。
「初期化」が表示されます。
- 3** 「バックアップアーカイブから Security Platform を復元する」にチェックが入っていることを確認して、「次へ」をクリックします。
「復元」が表示されます。

- 4 「新しい Trusted Platform Module」にチェックが入っていることを確認し、「復元するバックアップデータのあるファイルを指定する」にバックアップファイルが保存されている場所を指定します。
- 5 「次へ」をクリックします。
「所有者の設定」が表示されます。
- 6 「パスワード」と「パスワードの確認」に所有者のパスワードを入力し、「次へ」をクリックします。
「トークンの選択」が表示されます。
- 7 「緊急時復元用トークンの場所を指定する」に緊急時復元用トークンの保存場所を指定し、「パスワード」に設定済みのトークンのパスワードを入力します。
- 8 「次へ」をクリックします。
「ユーザーの選択」が表示されます。
- 9 「現在のユーザー名」の「ユーザーを選択する ...」から現在のユーザを選択します。また、「ユーザ名」にユーザが表示されている場合は、それぞれのユーザの「ユーザーを選択する ...」から復元するユーザ名を選択します。
- 10 全ユーザの選択が完了したら、「次へ」をクリックします。
「基本ユーザーパスワード」が表示されます。
- 11 「パスワード」に所有者のユーザーキーパスワードを入力し、「次へ」をクリックします。
「サマリー」が表示されます。
- 12 表示されている内容を確認し、「次へ」をクリックします。
しばらく待つと「ウィザードが正常に終了しました。」が表示されます。
- 13 「Security Platform ユーザー初期化ウィザードを起動する」にチェックが入っていることを確認し、「完了」をクリックします。
「Infineon Security Platform ユーザー初期化ウィザードへようこそ」が表示されます。
- 14 「次へ」をクリックします。
「Security Platform の機能」が表示されます。
- 15 「電子メールの保護」と「暗号化ファイルシステム (EFS) によるファイルとフォルダの暗号化」をチェックして、「次へ」をクリックします。
「電子メールの保護の設定をしてください。」が表示されます。
- 16 「次へ」をクリックします。
「暗号化証明書」が表示されます。

- 17** 「発行先」および「発行者」が自分になっていることを確認し、「次へ」をクリックします。

「設定を確認してください。」が表示されます。

- 18** 表示されている内容を確認し、「次へ」をクリックします。
しばらく待つと「ウィザードが正常に終了しました。」が表示されます。

- 19** 「完了」をクリックします。

□ ユーザが行う作業

- 1** **Windows** にログオンします。

通知領域の「Infineon Security Platform」のアイコンから「キーや証明書と設定を復元します。」と表示されます。

- 2** 通知領域の「Infineon Security Platform」のアイコンをクリックし、「Security Platform の機能を復元する」を選択します。

「Infineon Security Platform バックアップと復元ウィザードへようこそ」が表示されます。

- 3** 「次へ」をクリックします。

「基本ユーザーパスワード」が表示されます。

- 4** 「パスワード」にユーザーキーパスワードを入力し、「次へ」をクリックします。

「サマリー」が表示されます。

- 5** 表示されている内容を確認し、「次へ」をクリックします。

しばらく待つと「ウィザードが正常に終了しました。」が表示されます。

- 6** 「Security Platform ユーザー初期化ウィザードを起動する」にチェックが入っていることを確認し、「完了」をクリックします。

「Infineon Security Platform ユーザー初期化ウィザードへようこそ」が表示されます。

- 7** 「所有者が行う作業」(→ P.26) の手順 12 ～ 17 を行います。

■ 通知領域から「他の OS で初期化されました」と表示された場合

□ 所有者が行う作業

- 1** 「こんなときには」－「セキュリティチップの鍵を消去する」(→ P.34) の手順に従って、セキュリティチップの鍵を消去します。

- 2** 「通知領域から「Security Platform を復元します。」と表示された場合」－「所有者が行う作業」(→ P.26) を行います。

□ ユーザが行う作業

- 1** 「通知領域から「Security Platform を復元します。」と表示された場合」
－「ユーザが行う作業」(→ P.28) の手順を行います。

機器監査について

SMARTACCESS/Trust で起動時に機器監査実行」を設定しておく、ワークステーションの電源を入れたときやワークステーションを再起動したときにハードウェアの変更を検出すると、Windows のログオンを禁止することができます。これにより、ユーザが気づかないうちに（帰宅時など）ハードウェアを変更されても、検出することができます。

なお、不正にワークステーションの設定が変更されたときだけでなく、修理により設定が変更された場合でも機器監査変更が検出されることがあります。修理に出す前には「ワークステーションの修理について」(→ P.30) を参照し、前もって設定変更できるようにしてください。

ハードウェアの変更については次の項目が検出されます。

重要

- ▶ 次の変更を行う前には SMARTACCESS/Trust の「起動時に機器監査実行」をオフにし、変更後、再度「現状登録」を行う必要があります。設定方法については、「アプリケーションの設定を行う」(→ P.20) および SMARTACCESS/Trust アプリケーションのマニュアルを参照してください。

POINT

- ▶ ハードウェアの変更については、休止状態からの復帰時にも確認されます。

□ BIOS 設定変更

BIOS でハードウェア構成が変更された場合には、機器監査により通知されます。

□ メモリ構成の変更

メモリスロットの構成に変更があった場合には、機器監査により通知されます。

□ PCI スロット、グラフィックボードの変更 (J340、N440 の場合)

PCI スロットの構成およびグラフィックボードを変更した場合には、機器監査にて通知されます。

□ マルチベイの変更 (H230 の場合)

マルチベイを変更した場合には、機器監査により通知されます。

□ USB デバイスの変更

USB ポートに USB メモリなどのストレージデバイスを接続した場合には、機器監査により通知されます。

POINT

- ▶ USB デバイスの変更を検出するには、BIOS セットアップで次のように設定する必要があります。

セキュリティチップ取扱説明書

- ・ J340、N440 の場合
「Legacy USB Support」: Enabled
- ・ H230 の場合
「レガシー USB サポート」: 使用する

BIOS セットアップについては、ワークステーション本体の『CELSIUS マニュアル』の「BIOS」を参照してください。

ワークステーションの修理について

ワークステーションを修理に出す場合、修理後の設定が修理前の設定と異なることがあります。そのため、修理に出す前や出した後には次の作業が必要になります。

■ 修理前に必要な作業

□ 鍵のバックアップ

「鍵のバックアップについて」(→ P.24) の手順に従って、バックアップを行います。

□ Trusted ログオンを使用しない設定に変更する

機器監査を行っている場合、必ず Trusted ログオンを使用しない設定に変更してください。Trusted ログオンを使用する設定にして機器監査を行っている場合、修理したり、ハードウェアの設定を変更したりすると、Windows にログオンできなくなることがあります。

POINT

▶ Trusted ログオンの設定の変更については、SMARTACCESS/Trust アプリケーションのマニュアルを参照してください。

□ BIOS パスワードを解除する

「インストールを行う」－「BIOS の設定を変更する」(→ P.12) で設定したパスワードを解除してください。

■ 修理後に必要な作業

□ 鍵を復元する

「鍵の復元について」(→ P.26) の手順に従って、鍵を復元してください。

□ BIOS パスワードを設定する

「インストールを行う」－「BIOS の設定を変更する」(→ P.12) の手順 1 ～ 6 に従って、パスワードを設定してください。

□ Trusted ログオンを使用する設定に変更する

Trusted ログオンを使用していた場合には、「インストールを行う」－「アプリケーションの設定を行う」(→ P.20) の手順 1 ～ 6 に従って、Trusted ログオンを使用する設定に変更してください。

なお、Trusted ログオンの設定を変更する前には、あらかじめ現在の機器構成を登録しておく必要があります。「インストールを行う」－「アプリケーションの設定を行う」(→ P.20) の手順 7 ～ 9 に従って、あらかじめ現在の機器構成を登録しておいてください。

ワークステーションの廃却について

ワークステーションを廃却する前には、安全のために、次の手順に従ってセキュリティの鍵や、鍵に関連するファイルを削除してください。

重要

▶ セキュリティチップの鍵や、鍵に関連するファイルを削除すると、セキュリティチップにより保護されていた暗号化ファイルや証明書は利用できなくなります。

- 1 「こんなときには」－「セキュリティチップの鍵を消去する」(→ P.34) の手順に従って、セキュリティチップの鍵を消去します。
- 2 ワークステーション本体の『CELSIUS マニュアル』の「セキュリティ」－「ワークステーション本体廃棄時のセキュリティ」を参照して、ハードディスク内のデータを削除します。

6 こんなときには

パスワードを変更するには

所有者パスワードまたはユーザーキーパスワードの変更は、次の方法で行います。

POINT

- ▶ セキュリティチップのパスワードは、セキュリティ面を考慮し、定期的に変更することをお勧めします。

■ 所有者パスワードの変更方法

- 1** 通知領域の「Infineon Security Platform」アイコンをクリックし、表示されるメニューから「Security Platform を管理する」を選択します。
「Infineon Security Platform 設定ツール」が表示されます。
- 2** 「アドバンス」タブを選択し、「所有者のパスワード」の「変更」をクリックします。
以降の操作は画面の指示に従ってください。

■ ユーザーキーパスワードの変更方法

- 1** 通知領域の「Infineon Security Platform」アイコンをクリックし、表示されるメニューから「Security Platform を管理する」を選択します。
「Infineon Security Platform 設定ツール」が表示されます。
- 2** 「ユーザー設定」タブを選択し、「基本ユーザーキーのパスワード」の「変更」をクリックします。
以降の操作は画面の指示に従ってください。

パスワードを忘れた場合には

ユーザーキーパスワードを忘れてしまったときには、再設定することができます。
ユーザーキーパスワードを再設定する場合には、所有者により再設定を行う承認処理を行った後、各ユーザーで新しいパスワードを設定し直します。

POINT

- ▶ 操作については、Infineon Security Platform ツールのマニュアルを参照してください。

■所有者が行う作業

- 1 「スタート」ボタン→「すべてのプログラム」→「Infineon Security Platform ソリューション」→「Security Platform を管理します」の順にクリックします。
「Infineon Security Platform 設定ツール」が起動します。
- 2 「パスワードリセット」タブをクリックし、「基本ユーザーパスワードのリセット」の「管理タスク」の「準備」をクリックします。
「ユーザーの選択」が表示されます。
- 3 ユーザーを選択し、「次へ」をクリックします。
「トークンの選択」が表示されます。
- 4 「リセットトークンの場所」にリセットトークンが保存されている場所を入力し、「パスワード」に設定済みのパスワードを入力して「次へ」をクリックします。
「リセット承認コード」が表示されます。
- 5 「ファイルの保存」でファイルを保存し、「次へ」をクリックします。
「ウィザードが正常に終了しました」が表示されます。
- 6 「完了」をクリックします。
- 7 保存した「リセット承認コード」ファイルと初期化時に作成した個人シークレットファイル（通常、`sppwdresetsecret.xml`）をユーザに渡します。

■ユーザが行う作業

- 1 「スタート」ボタン→「すべてのプログラム」→「Infineon Security Platform ソリューション」→「Security Platform を管理します」の順にクリックします。
「Infineon Security Platform 設定ツール」が起動します。
- 2 「パスワードリセット」タブをクリックし、「基本ユーザーパスワードのリセット」の「ユーザータスク」の「リセット」をクリックします。
「リセットシークレット」が表示されます。
- 3 「個人シークレット」と「リセット承認コード」に所有者から受け取ったファイルを指定し「次へ」をクリックします。
「基本ユーザーパスワード」が表示されます。
- 4 「パスワード」と「パスワードの確認入力」に新しいパスワードを入力し「次へ」をクリックします。
「設定を確認する」が表示されます。

5 「次へ」をクリックします。

しばらく待つと、「ウィザードが正常に終了しました」が表示されます。

6 「完了」をクリックします。

セキュリティチップの鍵を消去する

ワークステーションを廃却するときには、ワークステーションに残ったデータを復元できないようにすることが重要です。セキュリティチップにより保護されたデータは、セキュリティチップ内のデータを破棄し、復元用ファイルを破棄することで再び復元することができなくなります。

重要

- ▶ この操作はセキュリティチップのデータを破棄するだけで、ハードディスクのデータは破棄されません。
- ▶ セキュリティチップのデータを破棄したことで、ハードディスク内のセキュリティチップで保護されたデータは見るができなくなりますが、ワークステーションの廃却時にはハードディスクのデータをクリアしてください。
- ▶ BIOS セットアップで、セキュリティチップ関連の設定を行うには、管理者用パスワードを設定する必要があります。
- ▶ BIOS セットアップについては、ワークステーション本体の『CELSIUS マニュアル』の「BIOS」を参照してください。

■ J340、N440 の場合

1 「インストールを行う」－「BIOS の設定を変更する」－「J340、N440 の場合」(→ P.12) の手順 1 ～ 6 を行います。

2 【↑】キーまたは【↓】キーを押して、「Clear Security Chip」を選択し、【Enter】キーを押します。

クリアを続行してよいかを確認するウィンドウが表示されます。

3 「Yes」を選択し、【Enter】キーを押します。

4 Exit メニューが表示されるまで、何度か【Esc】キーを押します。

5 【↑】キーまたは【↓】キーを押して「Exit Saving Changes」を選択し、【Enter】キーを押します。

「Save Configuration Changes and exit now?」が表示されます。

6 【←】キーまたは【→】キーを押して「Yes」を選択し、【Enter】キーを押します。

BIOS セットアップが終了し、ワークステーション本体が再起動します。

 重要

- ▶「セキュリティチップ」の設定を有効にするには、BIOS セットアップ終了後にワークステーション本体の再起動が必要です。終了メニューで「Exit Saving Changes」を行っただけで電源を切ってしまうと、設定が正しく行われませんのでご注意ください（次回起動時にエラーメッセージが表示されます）。

H230 の場合

- 1 「インストールを行う」－「BIOS の設定を変更する」－「H230 の場合」(→ P.13) の手順 1 ～ 6 を行います。
- 2 【↑】キーまたは【↓】キーを押して、「セキュリティチップのクリア」を選択し、【Enter】キーを押します。
クリアの続行を確認するウィンドウが表示されます。
- 3 「はい」を選択し、【Enter】キーを押します。
- 4 【↑】キーまたは【↓】キーを押して、「セキュリティチップ」を選択します。
- 5 【Space】キーまたは【-】キーを押して、「使用しない」を選択します。
- 6 終了メニューが表示されるまで、何度か【Esc】キーを押します。
- 7 【↑】キーまたは【↓】キーを押して「変更を保存して終了する」を選択し、【Enter】キーを押します。
「セットアップ確認」が表示されます。
- 8 【←】キーまたは【→】キーを押して「はい」を選択し、【Enter】キーを押します。
BIOS セットアップが終了し、ワークステーション本体が再起動します。

 重要

- ▶「セキュリティチップ」の設定を有効にするには、BIOS セットアップ終了後にワークステーション本体の再起動が必要です。終了メニューで「変更を保存する」を行っただけで電源を切ってしまうと、設定が正しく行われませんのでご注意ください（次回起動時にエラーメッセージが表示されます）。

離席時にワークステーションをロックするには

ワークステーションから離れる場合は、他人にワークステーションを操作されないよう注意が必要です。
次の設定を施すことで、離席時でもワークステーションはセキュリティチップにより安全に保護されます。

 POINT

- ▶ 各設定方法については、Windows のマニュアルを参照してください。

■スクリーンセーバーのパスワード

スクリーンセーバーを設定する場合、「パスワードによる保護」を行えば、パスワードはセキュリティチップにより安全に保護されます。

■コンピュータのロック

「コンピュータのロック」を行うと、復帰時のパスワードはセキュリティチップにより安全に保護されます。

■スタンバイや休止状態から回復するときのパスワード

スタンバイや休止状態の設定をしている場合、「スタンバイから回復するときパスワードの入力を求める」を設定しておく、パスワードはセキュリティチップにより安全に保護されます。

新しいユーザを登録する

Windows に新規ユーザを追加した場合、そのユーザがセキュリティチップを利用するためには、セキュリティチップに新規ユーザの情報を登録する必要があります。

POINT

- ▶ Trusted ログオンを設定している場合は、一度「一時中止パスワード」で Windows にログオンする必要があります。所有者にご相談ください。
- ▶ 事前に Windows にユーザを追加しておく必要があります。所有者にご相談ください。
- ▶ Windows で新規ユーザを「ユーザーは次回ログオン時にパスワードの変更が必要」で作成した場合は、新規ユーザのログオン前に一度 Trusted ログオンを解除してください。Windows のパスワードを変更した後で、再度 Trusted ログオンを設定してください。

■ユーティリティへの登録

1 登録するユーザで、Windows にログオンします。

通知領域の「Infineon Security Platform」アイコンから「Security Platform の機能が初期化されていません。」というメッセージが表示されます。

2 通知領域の「Infineon Security Platform」アイコンをクリックします。 メニューが表示されます。

3 表示されたメニューから「Security Platform のユーザーの初期化」を選択します。 「Infineon Security Platform ユーザー初期化ウィザードによるこそ」が表示されます。

4 「ユーティリティの設定を行う」の手順 15 (→ P.17) 以降を行い、登録します。

5 「ユーティリティの確認を行う」(→ P.18) の手順で、ユーティリティが正しく設定されたかを確認します。

■アプリケーションの設定

引き続き、SMARTACCESS/Trust に登録します。

- 1 「スタート」ボタン→「すべてのプログラム」→「SMARTACCESS Trust」→「ログオン設定ツール」の順にクリックします。
- 2 ユーザーキーパスワードを入力し「次へ」をクリックします。
「ログオン設定ツール」が表示されます。
- 3 「Trusted ログオン」の「登録」をクリックします。
「Trusted ログオン情報登録」が表示されます。
- 4 Windows ログオン時の「ドメイン名」、「パスワード」、および「パスワード確認入力」を入力します。

POINT

▶ ドメインを利用していない場合は、「ドメイン名」の入力は不要です。

- 5 「OK」をクリックします。
「Trusted ログオン情報を設定しました。」が表示されます。
- 6 「OK」をクリックします。
「ログオン設定ツール」に戻ります。
- 7 「閉じる」をクリックします。

7 トラブルシューティング

□ BIOS でセキュリティチップの設定を変更できない

BIOS で、セキュリティチップを使用するかどうかや、セキュリティチップのデータをクリアする設定を行うためには、管理者用パスワードの設定が必要です。管理者用パスワードが設定されているか確認してください。

□ ユーティリティがインストールできない

ユーティリティをインストールするには、BIOS でセキュリティチップを使用する設定になっている必要があります。BIOS の設定を確認してください。

□ SMARTACCESS/Trust が起動できない

SMARTACCESS/Trust を起動するには、ユーティリティが正常にインストールされ、初期化ウィザードとユーザー初期化ウィザードが正常に終了している必要があります。確認してください。

□ Trusted ログオン時に機器が変更された旨のエラーメッセージが表示される

前回の起動からハードウェアの構成や設定が変更された可能性があります。ハードウェア構成や BIOS 設定など変更されていないか確認してください。変更があった場合は、機器を登録したときの状態に戻してください。

□ Trusted ログオン時にパスワードエラーになる

Trusted ログオンを有効にしている場合には、Windows のパスワードではなくセキュリティチップのユーザーキーパスワードを入力してください。

□ Trusted ログオン時に「Security Platform Management Service が～」というメッセージが表示されることがある

BIOS セットアップで「Embedded Security Chip」または「Security Chip」を「Enabled」に設定している場合は、しばらく待つと Windows にログオンできますが、まれにメッセージが表示され続け、Windows にログオンできない場合があります。同封している CD-ROM「Infineon TPM Professional Package Patch Program」内に、この問題を解決する修正プログラムが格納されています。CD-ROM 内の「readme.txt」をご覧になり、修正プログラムを実行してください。

□ EFS が利用できない

EFS を利用するにはハードディスクが NTFS でフォーマットされている必要があります。FAT32 のドライブでは EFS を利用することはできません。

□ セキュリティチップを「Disabled」（J340、N440 の場合）または「使用しない」（H230 の場合）に設定すると、Windows にログオンできなくなった

Trusted ログオンを設定した状態で、セキュリティチップを「Disabled」（J340、N440 の場合）または「使用しない」（H230 の場合）に設定すると、セキュリティチップで保存していた Windows パスワードが利用できないため、Windows にログオンできなくなります。その場合にはセキュリティチップを「Enabled」（J340、N440 の場合）または「使用する」（H230 の場合）にし直すか、「一時中止パスワード」でログオンする必要があります。なお、「一時中止パスワード」でログオンしても、セキュリティチップで保護された環境は安全に管理されています。

□ ハードウェア構成を変更したために Windows にログオンできなくなった

ハードウェアの構成を変更すると、SMARTACCESS/Trust の機器監査機能により Windows にログオンできなくなります。その場合にはハードウェア構成を登録したときの設定に戻すか、機器構成を登録し直す必要があります。詳しい設定方法については、SMARTACCESS/Trust アプリケーションのマニュアルの「3.5 ログオンする」を参照してください。

□ Trusted ログオンでパスワードの入力画面が 2 度表示される

「ユーザーキーパスワード」と「一時中止パスワード」を同じにしている可能性があります。所有者にご相談ください。

□ Trusted ログオン時、内部エラー（0xe0280012）が表示される

セキュリティチップがクリアされた可能性があります。所有者にご相談ください。

□ 「鍵の復元について」を行うとユーザーキーパスワードが変わることがある

「運用上の注意」－「鍵の復元について」（→ P.26）の手順に従って復元した場合、ユーザーキーパスワードには、バックアップを行った時点でのパスワードが設定されます。そのため、バックアップ後にユーザーキーパスワードを変更しても、復元するとバックアップを行った時点でのパスワードに戻ります。

□ 自動バックアップのアーカイブに全ユーザのデータが入らない場合がある

パスワード変更などユーザの状態に変更があった場合は、自動バックアップにその変更が反映されるまでに時間がかかる場合があります。ユーザの状態に変更があった場合は、しばらく（30 分程度）待ってから自動バックアップを行うようにしてください。

CELSIUS Workstation Series

セキュリティチップ 取扱説明書

B6FH-6341-02 Z2-00

発行日 2005 年 8 月

発行責任 富士通株式会社

- このマニュアルの内容は、改善のため事前連絡なしに変更することがあります。
- このマニュアルに記載されたデータの使用に起因する第三者の特許権およびその他の権利の侵害については、当社はその責を負いません。
- 無断転載を禁じます。