Solaris スマートカードの管理

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 816–3962–10
2002 年 5 月

原典: *Solaris Smartcard Administration Guide*

Part No: 806-7010-10

Revision A

020327@2851

目次

はじめに

Solaris™ スマートカードを使用すると、Solaris 8 または Soraris 9 デスクトップ環境に安全にログインできます。スマートカードはプラスチック製のカードです。このプログラム可能なカードをカードリーダーに挿入するだけで、システムにアクセスできます。このマニュアルでは、スマートカードを使用して認証を行うためのシステムとスマートカードの構成方法について説明します。また、構成後のスマートカードの使用方法についても説明します。

対象読者

このマニュアルは、Solaris スマートカード 環境を設定および管理するシステム管理者を対象としています。 ここでの説明を理解するためには、認証やそれに関連するネットワークセキュリティの概念について十分に理解している必要があります。

Solaris スマートカードをユーザーとして使用する (管理作業は行わない) 方は、このマニュアルを読む必要はありません。システムのプロンプトが表示された場合には、各自のスマートカードをコードリーダーに挿入し、PIN (Personal Identification Number) を入力するだけです。

関連情報

Solaris スマートカードは、Solaris 管理ツールまたは Solaris のコマンドや手順と合わせて使用できます。Solaris のインストールや管理の手順についての詳細は、次のマニュアルを参照してください

- 『*Solaris 9* インストールガイド』

- 『*Solaris* のシステム管理 (基本編)』
- 『*Solaris* のシステム管理 (上級編)』
- 『*Solaris* のシステム管理 (*IP* サービス)』
- システムに付属するその他のソフトウェアマニュアル

Sun のオンラインマニュアル

docs.sun.com[SM] では、Sun が提供しているオンラインマニュアルを参照することができます。マニュアルのタイトルや特定の主題などをキーワードとして、検索を行うこともできます。URL は、`http://docs.sun.com` です。

表記上の規則

このマニュアルでは、次のような字体や記号を特別な意味を持つものとして使用します。

表 **P–1** 表記上の規則

字体または記号	意味	例
`AaBbCc123`	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例を示します。	`.login` ファイルを編集します。 `ls -a` を使用してすべてのファイルを表示します。 `system%`
`AaBbCc123`	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して示します。	`system%` **`su`** `password:`
AaBbCc123	変数を示します。実際に使用する特定の名前または値で置き換えます。	ファイルを削除するには、`rm` *filename* と入力します。
『 』	参照する書名を示します。	『コードマネージャ・ユーザーズガイド』を参照してください。
「 」	参照する章、節、ボタンやメニュー名、強調する単語を示します。	第 5 章「衝突の回避」を参照してください。 この操作ができるのは、「スーパーユーザー」だけです。

表 **P–1** 表記上の規則　　*(続き)*

字体または記号	意味	例
\	枠で囲まれたコード例で、テキストがページ行幅を超える場合に、継続を示します。	`sun% grep '^#define \` `XV_VERSION_STRING'`

コード例は次のように表示されます。

- C シェル

  `machine_name% command y|n [filename]`

- C シェルのスーパーユーザー

  `machine_name# command y|n [filename]`

- Bourne シェルおよび Korn シェル

  `$ command y|n [filename]`

- Bourne シェルおよび Korn シェルのスーパーユーザー

  `# command y|n [filename]`

[ ] は省略可能な項目を示します。上記の例は、*filename* は省略してもよいことを示しています。

| は区切り文字 (セパレータ) です。この文字で分割されている引数のうち 1 つだけを指定します。

キーボードのキー名は英文で、頭文字を大文字で示します (例: Shift キーを押します)。ただし、キーボードによっては Enter キーが Return キーの動作をします。

ダッシュ (-) は 2 つのキーを同時に押すことを示します。たとえば、Ctrl-D は Control キーを押したまま D キーを押すことを意味します。

第 1 章

Solaris スマートカード (概要)

この章では、Solaris スマートカードの機能の概要、サポートされているスマートカードとカードリーダー、およびスマートカードの構成の計画について記述します。

スマートカードの機能

Solaris スマートカードを使用すると、標準 UNIX ログインよりも安全にスマートカードを使って Solaris デスクトップ環境にログインできます。これは、スマートカードに格納された情報を使って、ログイン時にユーザーの ID を確認できるためです。スマートカード上のログイン情報と同じ情報を提供できないユーザーは、Solaris デスクトップへのアクセスを拒否されます。Solaris スマートカードソフトウェアには、次の機能があります。

- スマートカード用のオープンカードフレームワーク (OCF) 1.1 規格の実装
- さまざまなカードリーダーのサポート
- 一般的に使用されている 3 種類のスマートカードのサポート
- Solaris Smartcard Console または Solaris コマンド行からの管理
- デスクトップ環境へのログインの PIN 認証による保護と、カードリーダーからスマートカードを取り出した際の `dtsession` による画面ロック
- ユーザーのセキュリティ資格情報をカード上に直接格納 (Java™ カードのみ)

スマートカードの要件

Solaris スマートカードソフトウェアを使用するには、次の条件が必要です。

- Solaris 8 または Solaris 9 オペレーティング環境で SPARC システムが動作していること
- 内蔵または外付けのカードリーダーおよびスマートカードがサポートされていること。

Solaris スマートカードは、次のスマートカードとカードリーダーをサポートしています。

- PayFlex カード
- iButton カード
- CyberFlex カード
- Sun SCRI External Serial Card Terminal Reader
- Sun SCRI Internal Card Terminal Reader
- iButton External Serial Card Terminal Reader

スマートカードによるログイン

構成した Solaris スマートカードを使用したログインをユーザーに要求することで、セキュリティ保護されているデスクトップ環境を保護できます。ここでは、ログインするときの手続きについて説明します。

1. `dtlogin` デーモンにより、ユーザーはスマートカードを挿入してから PIN を入力するように要求されます。
2. `pam_smartcard` モジュールにより、入力された PIN とカードに格納されている PIN が照合されます。
3. 入力された PIN とカードに格納されている PIN が一致した場合、`/etc/nsswitch.conf` に指定されたパスワードの検索順序に基づいて、ユーザー名とパスワードがカードから読み取られユーザーの認証に使用されます。

パッケージの説明

次の表では、Solaris 9 のインストール時に追加される Solaris スマートカードパッケージを一覧表示します。

表 **1–1** Solaris スマートカードパッケージ

パッケージ名	説明
SUNWjcom	スマートカードをサポートする Java 通信 API - Java コードとネイティブコード
SUNWjcomx	スマートカードをサポートする Java 通信 API - ネイティブコード (64 ビット)
SUNWjib	Dallas Semiconductor 社製シリアル iButton 用 OCF カード端末ドライバ
SUNWocf	OCF (オープンカードフレームワーク) - コアライブラリとユーティリティ
SUNWocfr	OCF (オープンカードフレームワーク) - 構成ファイル
SUNWocfh	オープンカードフレームワーク - ヘッダーファイル
SUNWocfx	OCF (オープンカードフレームワーク) - コアライブラリ (64 ビット)
SUNWpamsc	スマートカード認証用の接続可能な認証モジュール
SUNWpamsx	スマートカード認証用の接続可能な認証モジュール (64 ビット)
SUNWscgui	Solaris スマートカード Console
SUNWscmos	SCM カード端末ドライバによって使用される Smart OS
SUNWscmsc	Sun SCRI OCF カード端末ドライバ

パッケージを削除する場合には、標準の `pkgrm` コマンドを使用します。パッケージをインストールし直す場合は、`pkgadd` コマンドを使用します。

これらのコマンドの使用については、『*Solaris* のシステム管理 *(*基本編*)*』の「ソフトウェアの管理 (手順)」を参照してください。

スマートカードのマニュアルページ

スマートカードのコマンドの詳細については、次のマニュアルページを参照してください。

- `ocfserv(1M)`
- `pam_smartcard(5)`
- `smartcard(1M)`

第 2 章

Solaris スマートカードの基本的な使用方法

この章では、Solaris スマートカードの初期構成を設定する方法について説明します。

SmartCard Console の起動または再起動

SmartCard Console は、Solaris スマートカードソフトウェアを管理するためのグラフィカルユーザーインタフェース (GUI) です。

▼ コマンド行から SmartCard Console を起動するには

1. **root** でログインするか、`su` と入力してスーパーユーザになります。

注 – 一般ユーザーでログインしている場合、スマートカードを使用できますが、実行できる作業はアプレットの読み込みと構成の 2 つだけです。

---

2. **SmartCard Console** を起動します。

```
# /usr/dt/bin/sdtsmartcardadmin &
```

注 – デフォルトでは、root は X サーバーにアクセスを認可されいないため、`su` コマンドを入力してスーパーユーザーになる前に、X サーバーによるアクセス制御を無効にする場合があります。X サーバーによるアクセス制御を無効にするには、`/usr/openwin/bin/xhost +` *hostname* を実行します。この場合、*hostname* はローカルホスト名になります。SmartCard Console を起動した後、`xhost -`*hostname* を実行してアクセス制御を再度有効にします。

▼ CDE デスクトップから SmartCard Console を起動するには

1. 共通デスクトップ環境 **(CDE)** にスーパーユーザーとしてログインします。
   既に自分のログイン名で CDE を実行している場合は、CDE を終了して、スーパーユーザーとしてログインします。

注 – 一般ユーザーでログインしている場合には、スマートカードを使用できますが、実行できる作業はアプレットの読み込みと構成の 2 つだけです。

---

2. **CDE** コントロールパネルで、「アプリケーション **(Application)**」サブパネルの上矢印をクリックします。
   デフォルトでは、鉛筆マークをピンで留めた「テキストノート (Text Note)」アイコンが「アプリケーション (Application)」サブパネルを表しています。
3. 「アプリケーション **(Application)**」を選択して、アプリケーションマネージャを表示します。
4. アプリケーションマネージャの「システム管理 **(System_Admin)**」アイコンをダブルクリックします。
5. 「スマートカード **(Smart Card)**」アイコンをダブルクリックして、**SmartCard Console** を起動します。
   「スマートカード (Smart Card)」アイコンを探すには、スクロールダウンしなければならない場合があります。

注 – また、デスクトップの「ワークスペース (Workspace)」メニューから SmartCard Console を起動することもできます。「ワークスペース (Workspace)」メニューの一番上または「ツール (Tools)」サブメニューに「`sdtsmartcardadmin`」があります。

スマートカードによるログイン用のデスクトップの設定

Solaris 8 または Solaris 9 のオペレーティング環境で動作する Sun ワークステーションのデスクトップにスマートカードによるログインを設定するには、次の手順を実行します。一部の作業では、最初にコマンド行の例、その次に SmartCard Console の手順を示します。複雑な作業では、コマンド行の例は後の章に記載されています。

注 – これらのほとんどの作業を実行するには、スーパーユーザーでログインする必要があります。

▼ カードリーダーを有効にするには

新しいワークステーションにカードリーダーが内蔵されている場合でも、使用前にそれを有効にする必要があるので注意してください。外付けカードリーダーを有効にする場合、まず、そのカードリーダーのマニュアルの手順に従って、カードリーダーを物理的にシステムのシリアルポートに取り付ける必要があります。

コマンド行の例

例については、26 ページの「カードリーダーの追加 (コマンド行)」を参照

SmartCard Console の手順

1. **SmartCard Console** のナビゲーション区画で「カードリーダー **(Card Readers)**」をクリックします。

   「カードリーダーを追加 (Add Reader)」アイコンがコンソール区画に表示されます。使用可能なカードリーダーのタイプを表すアイコンも表示されます。

2. コンソール区画で「カードリーダーを追加 **(Add Reader)**」をダブルクリックします。

   「カードリーダーを追加 (Add Reader)」ダイアログボックスが表示されます。

3. 追加または選択するカードリーダーのタイプをダブルクリックし、「了解 **(OK)**」をクリックします。

   Sun 内蔵カードリーダーを有効にするには、「Sun SCRI Internal カード端末 (Sun SCRI Internal Card Terminal Reader)」を選択します。 「カードリーダー (Card Readers)」ダイアログボックスが表示されます。

4. 「基本構成 **(Basic Configuration)**」タブを選択します。

5. そのカードリーダーの名前を「一意のカード端末名 **(Unique Card Terminal Name)**」フィールドに入力します。

   カードリーダーを変更しない場合には、現在の名前のままにしておきます。名前にはスペースを入れないでください。

6. 「デバイスポート **(Device Port)**」の下にある下矢印をクリックします。

7. カードリーダーが取り付けられているポートを選択します。

8. 「了解 **(OK)**」をクリックします。

9. プロンプトが表示されたら、`ocfserv` を再起動します。

   次回に SmartCard Console または `smartcard` コマンドを使用すると、`ocfserv` プロセスが再起動します。

▼ 新しいカードタイプのサポートを追加するには (新しい ATR)

スマートカードの新しいタイプを使用するには、その ATR(Answer to Reset) 属性を `ocfserv` に設定する必要があります。 新しいカードタイプのサポートを追加するには、次の手順を実行します。

コマンド行の例

スーパーユーザーでログインし、次の手順を実行して新しい PayFlex ATR として “12345” を追加します。

```
# smartcard -c admin -x modify "PayFlex.ATR=3B69000057100A9 3B6911000000010100 12345"
```

注 – 現在の ATR および新しい ATR を入力する必要があります。

SmartCard Console の手順

1. 新しい **ATR** を持つスマートカードをカードリーダーに挿入します。

2. ナビゲーション区画で「スマートカード **(Smart Cards)**」を選択します。

3. 現在挿入されているカードのタイプを表すアイコンをダブルクリックします。

「スマートカード (Smart Card)」ダイアログボックスには、このカードタイプで既にサポートされている ATR のリストが表示されます。

4. 新しい **ATR** の場合には、「追加 **(Add)**」をクリックします。
   「ATR を追加 (Add ATR)」ダイアログボックスが表示され、カードリーダーに挿入されているカードの ATR が「挿入されているカードの ATR (Inserted Card's ATR)」リストボックスに示されます。

注 **–** 挿入されているカードの ATR 値が登録されているかどうかを確認するには、「追加 (Add)」ボタンをクリックします。何も表示されない場合、そのカードの ATR が既に認識されています。それ以外の場合には、次の手順を実行します。

---

5. 挿入されているカードの **ATR** を選択するか、「新しい **ATR (New ATR)**」フィールドに新しい **ATR** を入力します。
   これで、スマートカード製品の新しい ATR 値を表示できます。
6. 「**ATR** を追加 **(Add ATR)**」ダイアログボックスで「了解 **(OK)**」をクリックします。
   新しい ATR が「スマートカード (Smart Card)」ダイアログボックスのリストに追加されます。
7. 「スマートカード **(Smart Card)**」ダイアログボックスのリストから新しい **ATR** を選択します。
8. 「スマートカード **(Smart Card)**」ダイアログボックスで「了解 **(OK)**」をクリックして、その変更を有効にします。

▼ スマートカードのアプレットをスマートカードに読み込むには

Solaris スマートカードのアプレット (`SolarisAuthApplet`) をスマートカードに読み込むには、次の手順を実行します。この手順を実行してから、ユーザープロファイル情報を追加できます。

コマンド行の例

カードリーダーに挿入されているスマートカードを使って、スーパーユーザーでログインし、次のように入力します。

```
# smartcard -c load -i /usr/share/lib/smartcard/SolarisAuthApplet.capx
```

読み込みが終了すると、次のメッセージが表示されます。

```
Operation successful.
```

SmartCard Console の手順

1. スマートカードをカードリーダーに挿入します。
2. ナビゲーション区画から「アプレットを読み込む **(Load Applets)**」アイコンを選択します。
3. コンソール区画で「**SolarisAuthApplet**」アイコンをダブルクリックします。
   「アプレットの読み込み (Load Applets)」ダイアログボックスが表示されます。その後、各種カードタイプに有効なアプレットが左側のリストボックスに表示されます。
4. 初期化するカードタイプを選択します。
   「CyberFlex」、「IButton」、「PayFlex」の中から選択します。
5. **2** つのリストボックス間の矢印をクリックします。
   選択したアプレットが「アプレットのインストールを保留 (Pending Applet Installations)」リストボックスにコピーされ、そのリストボックス内でチェックマークが付けられ、スマートカードの名前が表示されます。カードリーダーにカードが挿入されていない、または間違ったスマートカードが挿入されている場合には、「No compatible devices inserted」メッセージが表示されます。そのメッセージが表示された場合には、適切なカードを挿入します。
6. 「インストール **(Install)**」をクリックします。
   「アプレットをデバイスに読み込む (Loading Applet to Device)」ウィンドウが表示されます。アプレットの読み込みには数分間かかります。インストールが完了すると、確認メッセージ (「アプレットのインストールが完了しました (Applet Installation Successful)」) を含むウィンドウが表示されます。
7. 「了解 **OK)**」をクリックして、そのウィンドウを終了します。
   これで、カードにデフォルト値が保存されます。以前の異なる PIN、またはユーザープロファイル値がカードに保存されている場合には、それらの値は上書きされます。詳細については、33 ページの「PIN 属性」 と 33 ページの「ユーザー属性とパスワード属性」を参照してください。

▼ ユーザープロファイルを設定するには

カードが設定されるアプリケーション (`dtlogin`) に関連付けられるユーザー名とパスワードを指定するには、次の手順を実行します。詳細については、32 ページの「スマートカード上でユーザー情報を作成するには」を参照してください。

コマンド行の例

スーパーユーザーでログインし、 `dtlogin` アプリケーションに対して `xxx` にユーザー名、 `yyy` にパスワードを設定するために、次のように 1 行にコマンドを入力します。この例では、PIN はデフォルト値の `$$$$java` です。

```
# smartcard -c init -A A0000000620304000 -P '$$$$java' user=xxx
password=yyy application=dtlogin
```

注 – 読み込んだアプレット ID と現在の PIN を入力する必要があります。 上記の例では、`-A A000000062030400` は `SolarisAuthApplet` のアプレット ID を示し、PIN はデフォルトの `SolarisAuthApplet` の値です。デフォルトの PIN である `$$$$java` や、シェルの特殊文字 (`$` など) を含む PIN は、単一引用符 (' ') で囲みます。単一引用符で囲まれていない場合、シェルは PIN を変数として解釈しようとし、コマンドが失敗します。

SmartCard Console の手順

1. カードリーダーに構成するスマートカードを挿入します。
2. ナビゲーション区画から「アプレットを構成 **(Configure Applets)**」を選択します。
   カードリーダー内のカードのタイプを示すアイコンがコンソール区画に表示されます。
3. コンソール区画でアイコンをダブルクリックします。
   「アプレットを構成 (Configure Applets)」ダイアログボックスが表示されます。
4. 「アプレットを構成 **(Configure Applets)**」ダイアログボックスにある「`SolarisAuthApplet`」を選択します。
   `SolarisAuthApplet` 構成フォルダがそのダイアログボックスの右側に表示されます。このフォルダには「PIN」と「User Profiles」のタブがあります (一部のスマートカードでは、「RSA Key」と「PKI Cert」のタブも追加されます)。ここでは、ユーザープロファイルの変更だけについて説明します。PIN 変更の詳細については、20 ページの「スマートカードの PIN を変更するには」を参照してください。
5. 「アプレットを構成 **(Configure Applets)**」ダイアログボックスで「**User Profiles**」タブを選択します。
6. 「**User Profile Name**」フィールドに `dtlogin` を入力します。
   これは CDE デスクトップを表します。
7. 「ユーザー名 **(User Name)**」フィールドにユーザー名を入力します。
   これは、カードの使用者となるユーザーの名前です。ユーザー名は 8 文字以内にしてください。

注 – カードに関連付けられた現在のユーザー名を確認するには、「Get」をクリックします。現在のユーザー名を確認したり、またはユーザー名やパスワードを変更するには、PIN を入力する必要があります。

---

8. 「パスワード **(Password)**」フィールドにパスワードを入力します。

これは、上記で入力したユーザー名に関連付けられるパスワードです。パスワードは、/etc/nsswitch.conf (LDAP、NIS、NIS+、またはローカルファイル) の passwd の検索順に基づいて、ユーザーのパスワードと対応付ける必要があります。パスワードは 8 文字以内にしてください。

注 – スマートカードの構成後に、ユーザーのパスワードを変更する場合、管理者またはユーザーがこれらの手順を再び実行して、スマートカードに新しいパスワードを保存する必要があります。パスワードは自動的に更新されません。

---

9. 「**Set**」をクリックします。
   「Set User Profile」ポップアップが表示され、現在の PIN を入力するように要求してきます。
10. **PIN** を入力して「了解 **(OK)**」をクリックします。
    これで、新しいユーザー名とパスワードがカードに保存されます。
11. 「了解 **(OK)**」をクリックして、ダイアログボックスを終了します。

▼ スマートカードの PIN を検証するには

スマートカードの PIN を確認するには、次の手順を実行します。

1. カードリーダーにスマートカードを挿入します。
2. スーパーユーザーでログインし、次のように入力してスマートカードの **PIN** を確認します。

   ```
   # smartcard -c init -A A000000062030400 -P 'PIN_number'
   ```

   この場合、*PIN_number* はカードに設定された PIN を表し、A000000062030400 は SolarisAuthApplet のアプレット ID です。
   PIN が無効の場合には、Invalid PIN メッセージが表示されます。PIN が有効な場合は、何のメッセージも出力されません。

▼ スマートカードの PIN を変更するには

スマートカードの PIN を変更するには、次の手順を実行します。

注 – 一般ユーザーが現在の PIN を知っている場合には、一般ユーザーがこの作業を実行できます。

コマンド行の例

カードリーダーにスマートカードを挿入して、スーパーユーザーでログインし、次のように入力してデフォルト PIN (`$$$$java`) を `001234` に変更します。

```
# smartcard -c init -A A000000062030400 -P '$$$$java' pin=001234
```

注 – 読み込んだアプレット ID と現在の PIN を入力する必要があります。 上記の例では、`-A A000000062030400` は `SolarisAuthApplet` のアプレット ID (AID) を示し、PIN はデフォルトの `SolarisAuthApplet` の値です。入力した PIN の確認プロンプトは表示されないので、新しい PIN は正しく入力するように注意してください。デフォルトの PIN である `$$$$java` や、シェルの特殊文字 ($ など) を含む PIN は、単一引用符 (' ') で囲みます。単一引用符で囲まれていない場合、シェルは PIN を変数として解釈しようとし、コマンドが失敗します。

SmartCard Console の手順

1. カードリーダーに構成するスマートカードを挿入します。
2. ナビゲーション区画から「アプレットを構成 **(Configure Applets)**」を選択します。
   リーダーのカードタイプのアイコンがコンソール区画に表示されます。
3. コンソール区画にあるそのアイコンをダブルクリックします。
   「アプレットを構成 (Configure Applets)」ダイアログボックスが表示されます。
4. リストボックスで `SolarisAuthApplet` を選択します。
   `SolarisAuthApplet` 構成フォルダがそのダイアログボックスの右側に表示されます。このフォルダには「PIN」と「User Profiles」のタブがあります (一部のスマートカードでは、「RSA Key」と「PKI Cert」のタブも追加されます)。ここでは、「PIN」の変更だけについて説明します。
5. 「**PIN**」タブを選択します。
6. 新しい **PIN** の入力と再入力を行います。
   PIN は 8 文字以内にしてください。
7. 「**Change**」をクリックします。
   「Change PIN」というポップアップウィンドウが表示されます。
8. そのポップウィンドウに以前の **PIN** を入力して、「**OK**」をクリックします。
   `SolarisAuthApplet` をカードにインストールしたときに、カードに読み込まれるデフォルトの PIN は `$$$$java` です。

▼ システムでスマートカードの使用を有効にするには

次の手順を実行して、システムで Solaris スマートカードの使用を有効にします。この手順は、スマートカード認証を使用する各システム上で実行する必要があります。Solaris スマートカードのコマンドの詳細については、`smartcard(1M)`、`pam_smartcard(5)`、および `ocfserv(1M)` のマニュアルページを参照してください。

コマンド行の例

手順については、35 ページの「スマートカードの使用を有効にするには (コマンド行)」を参照してください。

SmartCard Console の手順

1. ナビゲーション区画で「**OCF** クライアント **(OCF Clients)**」を選択します。
   「CDE」アイコンがコンソール区画に表示されます。
2. 「**CDE**」アイコンをダブルクリックします。
   「クライアントの構成 (Configure Clients)」ダイアログボックスが表示されます。
3. そのダイアログボックスで「カード**/**認証 **(Cards/Authentications)**」タブを選択します。
   スマートカードにサポートされている「CyberFlex」、「IButton」、および「PayFlex」の 3 つが左側のリストボックスに表示されます。
4. 「スマートカード機能を **CDE** アクティブにする **(Activate Desktop's Smart Card capabilities)**」ラジオボタンを選択します。

注 – その後、「クライアントの構成 (Configure Clients)」ダイアログボックスで「了解 (OK)」すると、スマートカードがただちに有効になります。 システムで使用しているカードリーダーであり、各自のユーザー名とパスワードで構成されたスマートカードであることを確認してください。 また、必ずカードの PIN を確認し、システムからロックアウトしてください。スマートカードを使ってシステムにアクセスできない場合、`rlogin` を使ってリモートからシステムにログインしてから、 スーパーユーザーでログインし、`smartcard -c disable` と入力してスマートカードを無効にします。 また、「スマートカード機能を CDE アクティブにしない (Deactivate Desktop's Smart Card Capabilities)」というラジオボタンを選択し、「了解 (OK)」をクリックすることで、「クライアントの構成 (Configure Clients)」ダイアログボックスから スマートカードを無効にすることもできます。

---

5. 「適用 **(Apply)**」または「了解 **(OK)**」をクリックします。
   これで、Solaris スマートカードがシステムで有効になります。

6. **CDE** を終了して、変更を有効にします。

その他の設定作業

スマートカードのタイムアウトとカードの取り外しの動作に関するデフォルト値を使用しない場合、次の手順でそれらの値を変更できます。

▼ スマートカードのタイムアウトを設定するには (Smartcard Console)

1. ナビゲーション区画で「**OCF** クライアント **(OCF Clients)**」を選択します。
2. コンソール区画にある「**CDE**」アイコンをダブルクリックします。
   「クライアントの構成 (Configure Clients)」ダイアログボックスが表示されます。
3. そのダイアログボックスで「タイムアウト **(Timeouts)**」タブを選択します。
4. 各タイムアウトのインジケータをマウスを使ってスライドさせて、タイムアウト値を調整します。
   - カード削除タイムアウト (Card Removal Timeout) – スマートカードが取り外された後、画面をロックするまでの、デスクトップが待機する時間の長さを指定します。これが適用されるのは、オプションタブで「カード削除を無視 (Ignore Card Removal)」ボックスがチェックされていない場合に限ります。「カード削除ログアウトの待ち時間 (Card Removal Logout Wait)」が 0 に設定されている場合、ユーザーはログアウトできません (つまり、画面をロック解除するためにユーザー再認証が行われるまで画面はロックされたままになります)。
   - 再認証タイムアウト (Reauthentication Timeout) – カードを取り外し、画面をロックしたときに、「再認証 (Reauthentication)」画面が表示されるまでの、時間の長さを指定します。
   - カード削除ログアウトの待ち時間 (Card Removal Logout Wait) – 「再認証 (Reauthentication)」画面が表示されたときに、スマートカードが再挿入されるまでの、デスクトップが待機する時間の長さを指定します。カードをその時間内に再挿入しない場合には、ユーザーがログアウトされます。このタイムアウトが適用されるのは、「カード削除後に再認証 (Reauthenticate After Card Removal)」 (「オプション (Options)」タブにある) がチェックされていない場合に限ります。
5. 「適用 **(Apply)**」または「了解 **(OK)**」をクリックします。
6. **CDE** を終了して、変更を有効にします。

▼ カード削除のオプションを設定するには (Smartcard Console)

1. ナビゲーション区画で「**OCF** クライアント **(OCF Clients)**」を選択します。
2. コンソール区画にある「**CDE**」アイコンをダブルクリックします。
   「クライアントの構成 (Configure Clients)」ダイアログボックスが表示されます。
3. そのダイアログボックスで「オプション **(Options)**」タブを選択します。
4. チェックボックスをクリックして、切り替えます。
   - カード削除を無視 (Ignore Card Removal) – チェックマークが付いている場合には、カードリーダーからスマートカードを取り外したときに何も発生しません。
   - カード削除後に再認証 (Reauthenticate After Card Removal) – チェックマークがついている場合には、カードを取り外したときにユーザーがログアウトされます。チェックマークがついていない場合には、「カード削除ログアウトの待ち時間 (Card Removal Logout Wait)」の設定 (「タイムアウト (Timeouts)」タブにある) によって動作が決定されます。
5. 「適用 **(Apply)**」または「了解 **(OK)**」をクリックします。
6. **CDE** を終了して、変更を有効にします。

第 3 章

カードリーダー

この章では、各種タイプのカードリーダーを設定および保守する方法を説明します。

サポートされているカードリーダー

Solaris スマートカードは、iButton と Sun SCRI External Card Readr 1 という 2 種類の外付けカードリーダーと Sun SCRI Internal Card Reader 1 という 1 種類の内蔵カードリーダーをサポートしています。

次の表に、サポートされているカードリーダーと、これらのカードリーダーを追加するときに指定する必要がある値を示します。

表 **3–1** サポートされているカードリーダー

カードリーダーのタイプ	カード端末の出荷時の名前	リーダーモデル名
SCRI External Card Reader 1	`com.sun.opencard.terminal.scm.SCMStc.SCMStcCardTerminalFactory`	`SunSCRI`
iButton	`com.ibutton.oc.terminal.jib.iButtonCardTerminalFactory`	`DS1402`
Sun SCRI Internal Card Reader 1	`com.sun.opencard.terminal.scm.SCMI2c.SCMI2cCardTerminalFactory`	`SunISCRI`

カードリーダーの追加 (コマンド行)

コマンド行でカードリーダーを追加するには、`smartcard -c admin` コマンドを次の構文で使用します。

`smartcard -c admin -t terminal -j` *card_terminal_factory_name* `-x add -d` *device_pathname* `-r` *user_friendly_reader_name* `-n` *card_reader_model*

`-c admin`	OCF 属性の表示または変更を指定します。
`-t terminal`	カードリーダーの構成を指定します。
`-j` *card_terminal_factory_name*	カードリーダータイプのカード端末の出荷時の名前を指定します。特定のカード端末の出荷時の名前については、後述の手順を参照してください。
`-x add`	カードリーダーの追加を指定します。
`-d` *device_pathname*	カードリーダーが取り付けられているデバイスポートを指定します。
`-r` *user_friendly_reader_name*	リーダーの一意な名前を指定します。
`-n` *reader_model_name*	カードリーダーのモデル名を指定します。特定のカードリーダーのモデル名については、後述の手順を参照してください。

詳細は、`smartcard(1M)` のマニュアルページを参照してください。

▼ iButton リーダーを追加するには

1. 外付けカードリーダーをシステムに取り付けます。
   カードリーダーのマニュアルの手順に従って、外付けスマートカードリーダーをシリアルポートに物理的に取り付けます。
2. カードリーダーを取り付けるシステム上でスーパーユーザーになります。
3. たとえば、次のコマンドを **1** 行に入力して、**iButton** リーダーを追加します。

```
# smartcard -c admin -t terminal
-j com.ibutton.oc.terminal.jib.iButtonCardTerminalFactory
-x add -d /dev/cua/b -r MyButtonReader -n DS1402
```

`-c admin`	OCF 属性の表示または変更を指定します。
`-t terminal`	カードリーダーの構成を指定します。

`-j com.ibutton.oc.terminal.jib.iButtonCardTerminalFactory`	iButton リーダーのカード端末の出荷時の名前を指定します。 `-j` オプションの後にカード端末の出荷時の名前を入力するときは、上記のように正確に入力してください。文字の間に空白文字や改行は挿入しないでください。
`-x add`	カードリーダーの追加を指定します。
`-d /dev/scmi2c0`	カードリーダーが取り付けられているデバイスポートを指定します。
`-r` *MyButtonReader*	iButton カードリーダーの一意な名前を指定します。
`-n DS1402`	iButton カードリーダーのモデル名を指定します。

4. `ocfserv` を停止します。

```
# pkill ocfserv
```

次回に SmartCard Console または `smartcard` コマンドを使用すると、`ocfserv` プロセスが再起動します。

▼ Sun SCRI External Card Reader 1 を追加するには

1. 外付けカードリーダーをシステムに取り付けます。

カードリーダーのマニュアルの手順に従って、外付けスマートカードリーダーをシリアルポートに物理的に取り付けます。

2. カードリーダーを取り付けるシステム上でスーパーユーザーになります。

3. たとえば、次のコマンドを **1** 行に入力して、**Sun SCRI External Reader 1** を追加します。

```
# smartcard -c admin -t terminal
-j com.sun.opencard.terminal.scm.SCMStc.SCMStcCardTerminalFactory
-x add -d /dev/cua/b -r MyExternalReader -n SunSCRI
```

`-c admin`	OCF 属性の表示または変更を指定します。
`-t terminal`	カードリーダーの構成を指定します。
`-j scm.SCMStc.SCMStcCard TerminalFactory`	Sun SCRI External Card Reader 1 のカード端末の出荷時の名前を指定します。 `-j` オプションの後にカード端末の出荷時の名前を入力するときは、上記のように正確に入力してください。文字の間に空白文字や改行は挿入しないでください。
`-x add`	カードリーダーの追加を指定します。

`-d /dev/scmi2c0`	カードリーダーが取り付けられているデバイスポートを指定します。
`-r` *MyExternalReader*	SCRI External Card Reader 1 の一意な名前を指定します。
`-n SunSCRI`	Sun SCRI External Card Reader 1 のモデル名を指定します。

4. `ocfserv` を停止します。

```
# pkill ocfserv
```

次回に SmartCard Console または `smartcard` コマンドを使用すると、`ocfserv` プロセスが再起動します。

▼ Sun SCRI Internal Card Reader 1 を追加するには

1. カードリーダーを取り付けるシステム上でスーパーユーザーになります。
2. たとえば、次のコマンドを **1** 行に入力して、**Sun SCRI Internal Reader 1** を追加します。

```
# smartcard -c admin -t terminal
-j com.sun.opencard.terminal.scm.SCMI2c.SCMI2cCardTerminalFactory
-x add -d /dev/scmi2c1 -r MyInternalReader -n SunISCRI
```

`-c admin`	OCF 属性の表示または変更を指定します。
`-t terminal`	カードリーダーの構成を指定します。
`-j com.sun.opencard.terminal.scm.SCMI2c.SCMI2cCard TerminalFactory`	Sun SCRI Internal Card Reader 1 のカード端末の出荷時の名前を指定します。 `-j` オプションの後にカード端末の出荷時の名前を入力するときは、上記のように正確に入力してください。文字の間に空白文字や改行は挿入しないでください。
`-x add`	カードリーダーの追加を指定します。
`-d /dev/scmi2c0`	カードリーダーが取り付けられているデバイスポートを指定します。たとえば、`/dev/scmi2c` の場合、`scmi2c`*n* の *n* は、システム上で *n* 番目の SunISCRI リーダーであることを示しています。
`-r` *MyInternalReader*	SCRI Internal Card Reader 1 の一意な名前を指定します。
`-n SunISCRI`	SCRI Internal Card Reader 1 のモデル名を指定します。

3. `ocfserv` を停止します。

```
# pkill ocfserv
```

次回に SmartCard Console または `smartcard` コマンドを使用すると、`ocfserv` プロセスが再起動します。

カードリーダーの取り外し

スマートカードが不要になったとき、あるいはカードリーダーを別のシステムに移動するときに、外付けカードリーダーをシステムから物理的に取り外す必要があります。カードリーダーを物理的に取り外す前に、カードリーダーを論理的にも削除する必要があります。

▼ カードリーダーを取り外すには (Smartcard Console)

1. ナビゲーション区画の「カードリーダー **(Card Readers)**」をクリックします。
2. コンソール区画で削除したいカードリーダーを選択します。
3. 「アクション **(Action)**」メニューから「ターミナルを削除 **(Remove Terminal)**」を選択します。
4. 「了解 **(OK)**」をクリックして、カードリーダーを削除します。
5. プロンプトが表示されたら、`ocfserv` を再起動します。

   次回に SmartCard Console または `smartcard` コマンドを使用すると、`ocfserv` プロセスが再起動します。

▼ カードリーダーを取り外すには (コマンド行)

1. カードリーダーを取り外すシステム上でスーパーユーザーになります。
2. カードリーダーを論理的に削除します。

   ```
   # smartcard -c admin -t terminal -r user_friendly_reader_name -x delete
   ```

3. **(**オプション**)** 外付けカードリーダーをポートから物理的に取り外します。
4. `ocfserv` を停止します。

   ```
   # pkill ocfserv
   ```

   次回 SmartCard Console または `smartcard` コマンド使用すると、`ocfserv` プロセスが再起動します。

第 4 章

スマートカードの設定

この章では、スマートカードの設定の概要を示します。スマートカードは、SmartCard Console またはコマンド行から設定できます。この章の手順では、各自のシステムでスマートカードを実装する方法を理解し、スマートカードを使用するすべてのシステムにスマートカードを設定していることを前提とします。この章では、次の内容について説明します。

SolarisAuthApplet の読み込み

ユーザープロファイル情報を追加するためには、デフォルトの SolarisAuthApplet アプレットをスマートカードに追加する必要があります。手順については、17 ページの「スマートカードのアプレットをスマートカードに読み込むには」を参照してください。

スマートカードの初期化

デフォルトのアプレット (SolarisAuthApplet) を読み込んだ後に、カード上でユーザープロファイル情報を作成します。ユーザープロファイル情報では、カードユーザーのログイン名、パスワード、およびセキュリティ保護されているアプ リケーションを指定します。SolarisAuthApplet のデフォルトのPIN は、$$$$java です。

▼ スマートカード上でユーザー情報を作成するには

使用例 - スマートカード上でユーザー情報を作成する (コマンド行)

次のコマンドは、Solaris スマートカードがサポートしているすべてのスマートカードデバイスで使用できます。カードリーダーにスマートカードを挿入します。SmartCard Console の手順については、18 ページの「ユーザープロファイルを設定するには」と 20 ページの「スマートカードの PIN を変更するには」を参照してください。

次のコマンドを 1 行に入力して、スマートカードの PIN、ログイン名、パスワード、およびアプリケーションを設定します。

```
# smartcard -c init -A A000000062030400 -P '$$$$java' user=anyone
password=changeme application=dtlogin
```

この例では、ユーザー名は `anyone` に、パスワードは `changeme` に、アプリケーションは `dtlogin` に設定されています。 ユーザー名とパスワードは任意の値に設定できます。カードの発行時に、システム管理者またはユーザーが任意の値に変更します。手順については、18 ページの「ユーザープロファイルを設定するには」を参照してください。

注 – 読み込んだアプレット ID と現在の PIN を入力する必要があります。 コマンドの `-A A000000062030400` 部分に `SolarisAuthApplet` アプレット ID を指定します。デフォルトの PIN である `$$$$java` や、シェルの特殊文字 (`$` など) を含む PIN は、単一引用符 (' ') で囲む必要があります。単一引用符で囲まれていない場合、シェルは PIN を変数として解釈しようとし、コマンドが失敗します。

スマートカードの認証属性の定義

各スマートカードに属性を設定するときは、ユーザーの要件、サイト内のセキュリティポリシー、および使用しているスマートカードのタイプによる制限に基づいて設定します。各スマートカードに対応する属性を定義するには、「アプレットを構成 (Configure Applets)」ダイアログボックスを使用します。システム上のクライアントおよびサーバープログラムは、スマートカード上の属性を読み取って、特定のアプリケーションへのアクセス権をユーザーに与えるかどうかを決定します。

注 – このような属性は、Solaris スマートカードが提供する SolarisAuthApplet アプレットで初期化されたスマートカードだけに適用されます。異なるスマートカードアプレットを使用している場合、利用可能な属性は異なる場合があります。詳細は、smartcard(1M) のマニュアルページを参照してください。

PIN 属性

PIN 属性は、スマートカードの PIN (Personal Identification Number) を定義する認証属性です。スマートカードに作成されているデフォルトの PIN は $$$$java です。管理者またはユーザーは $$$$java を個人専用の PIN に変更できます。サイトのすべてのユーザーに、同じデフォルトの PIN 名 (たとえば changeme など) を付与することも考えられます。その後、各ユーザーが、その PIN をユーザー自身しか知らない値へ必ず変更するようにします。

スマートカードの PIN を変更する手順については、20 ページの「スマートカードの PIN を変更するには」を参照してください。

ユーザー属性とパスワード属性

ユーザー属性とパスワード属性は、ユーザーを識別して、ユーザーをスマートカードの PIN に関連付ける認証属性です。これらの属性を設定するには、ユーザーのログイン名とパスワードを知っている必要があります。

デフォルトの認証機構 (PIN) を使用するシステムでは、ocfserv を実行して PIN が認証されていることを確認します。次に、ocfserv はスマートカード上のユーザー属性とパスワード属性を読み取ります。スマートカード上のパスワードがシステムのパスワードデータベース内にあるユーザーのエントリと一致する場合、ocfserv はユーザーのそのアプリケーションへのアクセスを許可します。

アプリケーション属性

アプリケーション認証属性 (SmartCard Console では「ユーザープロファイル」と呼ばれる) を使用すると、ログイン名とパスワードを使ってログインする必要があるアプリケーションを指定できます。たとえば、デスクトップにスマートカードを使用したログインが必要な場合、スマートカード上のログイン名とパスワードに関連付けられたアプリケーションとして、dtlogin をアプリケーション属性に指定する必要があります。また、サイトに固有なアプリケーション (財務パッケージや個人データベースなど) にスマートカードを使用したログインが必要な場合、そのアプリケーションの名前をアプリケーション属性に指定します。

スマートカード上でアプリケーションを初期化する前に、ユーザーがスマートカードによる認証を使ってアクセスする必要があるアプリケーションを決定しておきます。root (スーパーユーザー) など、一般のユーザーには使用が制限されているアプリケーションにログインする必要があるユーザー (システム管理者など) 用にスマートカードを用意する場合は、この作業は特に重要になります。

注 – PayFlex カードは複数の属性をサポートしていないため、デスクトップ、および 1 つ以上のセキュリティ保護されたアプリケーションにログインする必要がある場合、あるいは複数のユーザー名を使用する場合には使用できません。

スマートカード上のアプリケーション属性は他の認証属性と共に機能します。たとえば、次の情報を使って、ユーザー Frank のスマートカードを初期化する場合を考えます。

- `A000000062030400` - `SolarisAuthApplet` アプレット
- `'$$$$java'` - このスマートカードのデフォルトの PIN で、後でユーザー Frank が変更することができます。
- `dtlogin` - このスマートカードによるログインが必要なアプリケーション
- `frank` - Frank がデスクトップにログインするときに入力する必要があるログイン名
- `changeme` - Frank がデスクトップにログインするときに入力する必要があるパスワード

これらの情報は、次のようにコマンド行に入力する必要があります。

```
# smartcard -c init -A A000000062030400 -P '$$$$java' application=dtlogin
user=frank password=changeme
```

Frank が自分のスマートカードをカードリーダーに挿入して、デスクトップにログイン (`dtlogin`) しようとすると、`ocfserv` はスマートカードを読み取って、`dtlogin` に関連付けられた認証属性があるかどうかを調べます。`ocfserv` サーバーは、ユーザー属性とパスワード属性が `dtlogin` に関連付けられていることを検出すると、PIN を入力するように Frank に要求します。

PIN が入力されると、スマートカード上に格納された、`dtlogin` アプリケーションに割り当てられている PIN と比較します。また、`ocfserv` は Frank のスマートカード上のログイン名とパスワードがシステムのパスワードデータベース内にある Frank のエントリと一致するかどうかを調べて、Frank が本人であることを確認します。これらの属性が一致した場合、Frank はデスクトップにログインできます。

Solaris スマートカードによるデスクトップへのログインを有効にする

デスクトップシステムの設定で最後に行うことは、Solaris スマートカードを使用したデスクトップへのログインを有効にすることです。手順については、35 ページの「スマートカードの使用を有効にするには (コマンド行)」を参照してください。

スマートカードを有効にし、かつ次の条件に当てはまる場合には、`dtlogin` を使用してログインすることはできません。

- 現在使用されているスマートカードを持っていない。
- スマートカードが正しく構成されていない。

現在使用されているスマートカードの構成を設定が完了する前に、スマートカードを有効にする場合は、次のスマートカードを無効にする手順を実行して、使用するスマートカードを設定できるようにします。

1. `ssh` または `rlogin` コマンドを使って、リモートからシステムにログインします。
2. スーパーユーザー (root) になります。
3. スマートカードの操作を無効にします。

```
# smartcard -c disable
```

▼ スマートカードの使用を有効にするには (コマンド行)

次の手順を実行して、システムで Solaris スマートカードの使用を有効にします。デスクトップでスマートカードを有効にした後、このシステムにログインするには、そのシステムで承認されたスマートカードを使用する必要があります。また、PIN の入力が 必要な場合もあります。

1. スマートカードの操作に使用する各システム上でスーパーユーザーになります。
2. デスクトップを停止します。

```
# /etc/init.d/dtlogin stop
```

3. **Solaris** スマートカードの操作を有効にします。

```
# smartcard -c enable
```

4. デスクトップを再起動します。

```
# /etc/init.d/dtlogin start
```

注 – スマートカードによるログインができるように CDE を構成すると、/etc/pam.conf が変更され、pam_smartcard が取り込まれます。 たとえば、smartcard -c enable を実行すると、次の行が dtlogin と dtsession の auth スタックの先頭に挿入されます。

```
dtlogin auth requisite pam_smartcard.so
dtsession auth requisite pam_smartcard.so
```

第 5 章

問題発生時の解決方法

この節では、Solaris スマートカードに関する問題を解決する方法について説明します。この章では、次の内容について説明します。

デバッグ属性を設定することで、スマートカードの動作をシステム上でデバッグできます。Solaris スマートカードは標準的なデバッグ機能を提供します。指定しておけば、ユーザーの動作を詳細に追跡できます。有効にすると、デバッグ情報がファイルに記録されます。デバッグ情報のレベルおよび量は、0 - 9 段階で制御することができます。デフォルトでは、デバッグは無効になっています。

デフォルトでは、次のデバッグ属性が `ocfserv` 用に定義されています。

```
debugging.filename        = /var/run/ocf.log
debugging                 = 0
OpenCard.trace            = com.sun:9 opencard.core:9
```

注 – Solaris 8 を使用している場合は、デバッグログファイルの名前 が `/tmp/ocf_debugfile` の場合があります。

`/var/run/ocf_log`	デバッグ情報を格納するファイル名
`debugging = 0`	デバッグが無効であることを示す。`debugging = 1` はデバッグが有効であることを示す
`OpenCard.trace`	OpenCard のトレースレベル

デバッグを有効にするには (Smartcard Console)

ocfserv のデバッグ属性を設定したい場合は、「デバッグ (Debug)」フォルダを使用します。デバッグの設定はオプション (省略可能) です。

1. ナビゲーション区画で「**OCF** サーバー **(OCF Server)**」を選択します。
2. ローカルシステムを表すアイコンをダブルクリックします。
3. 「デバッグ **(Debug)**」フォルダを選択します。
4. **OCF** デバッグレベルスライダのインジケータを右側に動かして、**OCF** サーバーのデバッグレベルを示します。
5. 「**Open Card** トレースレベル **(Open Card Trace Level)**」スライダのインジケータを右側に動かして、**OCF** サーバーのトレースレベルを示します。
6. **(**省略可能**)** デバッグファイルの代わりの名前を指定します。
   a. 「ブラウズ **(Browse)**」をクリックして、システム上のファイルシステムを表示します。
   b. 「**OCF** デバッグファイルの場所 **(OCF Debug File Location)**」フィールドに、デバッグファイルの絶対パス名を入力します。
7. 「適用 **(Apply)**」または「了解 **(OK)**」をクリックします。

デバッグを有効にするには (コマンド行)

スマートカードのデバッグを有効にするには、次の手順を使用します。

1. スーパーユーザーになります。
2. debugging=1 を設定して、スマートカードのデバッグを有効にします。

```
# smartcard -c admin -x modify debugging=1
```

次の例では、-x modify debugging.filename オプションとデバッグファイルの絶対パスによるファイル名を指定することによって、ocfserv デバッグファイルの位置を変更しています。

```
# smartcard -c admin -x modify debugging.filename=/var/tmp/sc.debug
```

スマートカードを無効にするには

スマートカードの設定に関する問題によってユーザーのスマートカードでのログインが許可されない場合、またはシステムがスマートカードによるログインを必要としなくなった場合は、システムでスマートカードを無効にする必要が生じることもあります。

1. スーパーユーザーになります。
2. スマートカードの操作を無効にします。

```
# smartcard -c disable
```

スマートカードを使用したログインに関する問題を解決するには

スマートカードを有効にしたあとで、システムからログアウトすると、CDE ログイン画面には次のようなメッセージが表示されます。

```
Please insert Smart Card
```

スマートカードの設定に関する問題のために、スマートカードを使用したシステムのログインを無効にする場合には、次の手順を実行してください。

1. rlogin または telnet コマンドを使って、リモートからログインします。
2. su と入力してスーパーユーザーになります。
3. 次のように入力して、スマートカードを無効にします。

```
# smartcard -c disable
```

スマートカードを無効にすると、CDE 画面には次のようなプロンプトが表示されます。

```
Enter User Name
```

4. こうしておいて、スマートカードの設定に関する問題を修正します。

構成に関する問題を解決するには

スマートカードの重要な構成情報は /etc/smartcard/opencard.properties ファイルに格納されています。このファイルは管理が不要なので、手動で編集しないでください。ただし、SmartCard Console またはコマンド行からスマートカードを構成するときに問題が発生した場合は、/etc/smartcard/opencard.properties ファイルの前のバージョンをコマンド行から復元できます。

1. スーパーユーザーになります。
2. /etc/smartcard ディレクトリに移動します。
3. 最初に現在のバージョンを保存します。

```
#  cp opencard.properties opencard.properties.bad
```

4. 前のバージョンを現在のバージョンにコピーします。

```
# cp opencard.properties.bak opencard.properties
```

アプレットのダウンロードに関する問題を解決するには

1. アプレットをスマートカードにダウンロードしようとして、次のメッセージが表示された場合、カードリーダーに挿入されているスマートカードの **ATR** が **(**システムが受け付けることができる**)** 有効な **ATR** のリストに追加されていない可能性があります。

```
SmartcardInvalidCardException
```

2. **16** ページの「新しいカードタイプのサポートを追加するには **(**新しい **ATR)**」の手順に従って、スマートカードの **ATR** を更新してください。

ATR の紛失に関する問題を解決するには

SmartCard Console でスマートカードを追加すると、カードリーダーに挿入されているスマートカードの ATR が表示されます。表示された ATR が有効な ATR のリストに存在しない場合は、その ATR を「*card-name*.ATR」属性に追加します。

詳細については、16 ページの「新しいカードタイプのサポートを追加するには (新しい ATR)」を参照してください。また、次のコマンド行の例も参照してください。

使用例 — 紛失した ATR を追加する(コマンド行)

ocfserv 属性を表示して、「*card_name*.ATR」属性が存在するかどうかを調べます。

```
# smartcard -c admin
```

たとえば、ocfserv は「MySCM.0.ATR」属性を表示します。MySCM はカードリーダーのユーザーフレンドリな名前です。この属性は、カードリーダーに挿入されているスマートカードの ATR を反映しています。この属性は一時的なものです。スマートカードをカードリーダーに挿入すると、ocfserv によって追加され、スマートカードをカードリーダーから取り外すと削除されます。

この属性により表示された ATR が有効な ATR のリストに存在しない場合は、その ATR を「*card-name* .ATR」属性に追加します。

用語集

Answer to Reset	メーカーが各スマートカードのタイプに割り当てた、スマートカードのバージョンを示す属性。同等な属性がシステムに格納されて、認証に使用される。略語は ATR。
ATR	「Answer to Reset (ATR)」を参照。
CDE	「共通デスクトップ環境」を参照。
Personal Identification Number	ユーザーが本人であることを確認するための一意な番号。略語は PIN。
PIN	「Personal Identification Number」を参照。
SmartCard Console	管理者が Solaris スマートカードを管理するための GUI ツール。
Solaris スマートカード	Solaris オペレーティング環境でスマートカードを使用するためのソフトウェアの名前。
共通デスクトップ環境	Solaris オペレーティング環境で使用されるデスクトップアプリケーション。略語は CDE。
コンソール区画	さまざまな管理作業を行うためのアイコンが表示される、SmartCard Console の区画。
情報区画	クリックしたカテゴリまたはアイコンの簡単な説明、あるいは、カテゴリまたはアイコンに関連するタスクを開始するための手順が表示される SmartCard Console の区画。
スマートカード	カードリーダーに挿入すると、ユーザーがシステムへのアクセスを許可されるように初期化されているプラスチック製のカード。
対称鍵	チャレンジ応答認証方法で記述される、DES 鍵の別名。
チャレンジ応答	スマートカードをカードリーダーに挿入すると、システムが乱数を生成して、カードリーダーに送信し、この乱数に基づく DES 鍵によって、スマートカードが読み込まれるという認証方法。
ナビゲーション区画	スマートカードの設定に関わるタスクのメジャーカテゴリが表示される、SmartCard Console の区画。

認証	ユーザーが本人であることを確認するためのプロセス。
非公開鍵	公開鍵インフラストラクチャで機能し、鍵の組み合わせを使用する、セキュリティ機能の一つ。鍵の組み合わせの非公開鍵の部分がスマートカードに格納される。

索引

P

S

X

あ

お

か

き

く

こ

と

に

は

ふ

ま

む

も

ゆ