Solaris スマートカードの管理

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303
U.S.A. 650-960-1300

Part Number 816-0124-10
2001 年 5 月

原典: *Solaris Smart Cards Administration Guide*

Part No: 806-7815-10

Revision A

Adobe PostScript

目次

はじめに

Solaris™ スマートカードを使用すると、Solaris 8 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、スマートカード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。これらの概念については、『*Solaris* のシステム管理 *(*第 *2* 巻*)*』の「システムセキュリティの管理の概要」を参照してください。

スマートカードを使ってシステムに安全にログインする方法については、第 9 章を参照してください。また、スマートカードの概念については、17ページの「スマートカードによるログイン」も参照してください。

内容の紹介

章	説明
第 1 章	スマートカードによる認証方法を紹介し、スマートカードの動作について説明します。
第 2 章	SmartCard Console を起動する作業について、CDE デスクトップを使用する方法と Solaris コマンド行を使用する方法を説明します。
第 3 章	カードリーダーの設定作業について説明します。
第 4 章	スマートカードの設定の概要について説明します。
第 5 章	スマートカードの設定について、SmartCard Console を使用する方法とコマンド行インタフェースを使用する方法を説明します。
第 6 章	スマートカードのデフォルトの属性がサイトのセキュリティ要件に合わない場合、スマートカードの構成を変更する作業について説明します。
第 7 章	スマートカードの構成を変更する作業について説明します。
第 8 章	スマートカードの管理作業および保守作業について説明します。
第 9 章	スマートカードの使用方法について説明します。

注 - 第 1 章から第 8 章までは、システム管理者またはセキュリティ管理者を対象としています。第 9 章は、スマートカードのユーザーを対象としています。

関連マニュアル

Solaris スマートカードは、Solaris 管理ツールおよび 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 8 インストールガイド (SPARC 版)*』
- 『*Solaris のシステム管理 (第 1 巻)*』
- 『*Solaris のシステム管理 (第 2 巻)*』
- 『*Solaris のシステム管理 (第 3 巻)*』
- 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 のマニュアルの注文方法

専門書を扱うインターネットの書店 Fatbrain.com から、米国 Sun Microsystems™, Inc. (以降、Sun™ とします) のマニュアルをご注文いただけます。

マニュアルのリストと注文方法については、`http://www1.fatbrain.com/documentation/sun` の Sun Documentation Center をご覧ください。

Sun のオンラインマニュアル

`http://docs.sun.com` 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。

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。
\	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'**

ただし AnswerBook2™ では、ユーザーが入力する文字と画面上のコンピュータ出力は区別して表示されません。

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。

一般規則

- このマニュアルでは、「IA」という用語は、Intel 32 ビットのプロセッサアーキテクチャを意味します。これには、Pentium、Pentium Pro、Pentium II、Pentium II Xeon、Celeron、Pentium III、Pentium III Xeon の各プロセッサ、および AMD、Cyrix が提供する互換マイクロプロセッサチップが含まれます。

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。

この章では、次の内容について説明します。

Solaris スマートカードの機能

Solaris スマートカードを使用すると、Solaris デスクトップ環境などのアプリケーションに、スマートカードを使って安全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、アプリケーション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
- SmartCard Console または Solaris コマンド行から行う管理
- パスワード、PIN、Challenge-Response 認証方式により、デスクトップ環境や他のアプリケーションへのログインを保護
- 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)

Solaris 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 リリースで SPARC™ システムが動作していること
- サポートされている内蔵または外付けのカードおよびスマートカードであること。サポートされているスマートカードとリーダーのリストについては、次の節を参照してください。

サポートされているスマートカードとリーダー

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。

表 1–1 サポートされているスマートカードのタイプ

カードタイプ	説明	使用されるカードリーダー
iButton	Java の iButton のスマートカード	iButton リーダー
CyberFlex	Java のスマートカード	Sun SCRI External Card Reader 1、 Sun SCRI Internal Card Reader 1
PayFlex	非 Java のスマートカード	Sun SCRI External Card Reader 1、 Sun SCRI Internal Card Reader 1

スマートカードによるログイン

スマートカードを使用すると、これまでログインできなかった、セキュリティ保護されているデスクトップ環境やアプリケーションにログインできます。ここでは、スマートカード (デフォルト設定) を使ってセキュリティ保護されているシステムにログインするときの手続きについて説明します。

1. システムに接続されたカードリーダーにカードを挿入します。
2. この時点では、セキュリティ保護されたアプリケーション (Solaris デスクトップなど) は実行できません。Solaris デスクトップ以外のアプリケーションもスマートカードで保護できます。
3. アプリケーションは、ユーザーに PIN (Personal Identification Number) の入力を要求します。ユーザーが PIN を入力すると、この PIN とカードに格納されている PIN が照合されます。
4. 入力された PIN とカードに格納されている PIN の一致を確認できた場合、アプリケーションは、システムの `/etc/nsswitch.conf` ファイル (NIS、NIS+、またはローカルファイル) に指定されているパスワードデータベースの中からこのパスワードを検索します。
5. このパスワードと同じパスワードが見つかった場合、アプリケーションはユーザーが認証されたものとみなし、ログインを許可します。

スマートカード構成の計画

スマートカードとカードリーダーを購入する前に、ログイン時に認証が必要かどうかを検討します。サイトでスマートカードを使用する理由は次のいずれかです。

- 特定の部署やドメインにあるシステムを承認されていないアクセスから保護する
- セキュリティ保護されたアプリケーションへのアクセスを、承認されたユーザーに限定する

スマートカードを使用できるようにシステムを設定する前に、いくつかの準備作業を行なっておく必要があります。次のチェックリストを使用して、これらの準備作業が完了したかどうかを確認してください。

表 1–2 スマートカード計画のチェックリスト

完了後チェック	作業
	1. サイトで使用するカードリーダーとスマートカードの種類を決定する。詳細は、16ページの「サポートされているスマートカードとリーダー」を参照
	2. スマートカードによるセキュリティ保護されたログインが必要なシステムを決定する
	3. スマートカードによる認証で保護する必要があるアプリケーションを決定する
	4. スマートカードが必要なユーザーのログイン名を取得する。

スマートカードの設定の概要 (タスクマップ)

スマートカード計画のチェックリストで確認後、このタスクマップを使って、スマートカードを設定するためのすべての作業を明確にします。このマップの作業は、Solaris 8 リリースのインストール、カードリーダーの取り付け、スマートカードの設定など、補助的な作業を指します。

表 1–3 スマートカードの設定の概要 (タスクマップ)

作業	説明	参照先
1. Solaris 8 ソフトウェアをインストールする	スマートカードを使用するすべてのシステムに Solaris 8 リリースをインストールする	『*Solaris 8* インストールガイド *(SPARC* 版*)*』
2. SmartCard Console を起動する	SmartCard Console を起動して、スマートカードの設定作業を行う	第 2 章
3. カードリーダーを取り付ける	スマートカードを使用するすべてのシステムにカードリーダーを物理的に取り付けて構成する (内蔵カードリーダーを使用しない場合)	第 3 章

表 1–3　スマートカードの設定の概要 (タスクマップ)　続く

作業	説明	参照先
4. スマートカードを設定する	カードに固有な情報やデフォルトの認証を指定する。その後、スマートカードの操作を有効にする	第 5 章
5. OCF サーバークライアント認証を構成する	(オプション) デフォルトの設定がサイトの要件に合わない場合は、サーバーとクライアントの属性を変更する	第 7 章

スマートカードパッケージの説明

次の表では、Solaris 8 のインストール中に追加される Solaris スマートカードパッケージを一覧表示します。

表 1–4　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)

表 1–4 Solaris スマートカードパッケージ 続く

パッケージ名	説明
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 スマートカードグラフィカルユーザーインタフェース (GUI)
SUNWscmos	スマートカード認証用の接続可能な認証モジュール
SUNWscmsc	Sun SCRI OCF カード端末ドライバ
SUNWjscag	Solaris スマートカードグラフィカルユーザーインタフェース (GUI) 日本語メッセージ

パッケージを削除する場合は、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。

上記コマンドの使用方法については、『*Solaris* のシステム管理 *(*第 *1* 巻*)*』の「ソフトウェアの管理 (手順)」を参照してください。

第 2 章

Solaris スマートカードの基本的な使用方法 (タスク)

この章では、ocfserv サーバーについて説明し、また SmartCard Console の起動および使用方法についても説明します。

この章では、次の内容について説明します。

これより後の章では、スマートカードのサポートを設定および構成する作業について説明します。さらに、各作業を、コマンド行から行う場合と SmartCard Console から行う場合についての補足説明を行います。スマートカードのコマンドの詳細は、smartcard(1M) と ocfserv(1M) のマニュアルページを参照してください。

ocfserv サーバー

OpenCard Framework (OCF) サーバー ocfserv は、システムでスマートカードの通信を管理するプロセスです。

カードリーダーを追加または削除するために SmartCard Console を使用した後、ocfserv を再起動するようプロンプトが表示されます。

ocfserv が動作していない場合は、SmartCard Console を起動するか smartcard コマンドを使用して起動します。

SmartCard Console からのスマートカードの管理

次の節では、SmartCard Console の使用方法を説明します。

SmartCard Console の使用

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。SmartCard Console には 3 つの区画があり、ここから作業を開始したり、情報を表示したりします。

- ナビゲーション区画 - スマートカードの設定に関わる作業の大きなカテゴリが表示されます。作業を選択するには、ナビゲーション区画でカテゴリをクリックします。ナビゲーション区画でカテゴリを選択すると、作業に関連するアイコンがコンソール区画に現れます。
- 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が表示されます。また、カテゴリまたはアイコンに関連する作業を開始するための手順も表示されます。
- コンソール区画 - ナビゲーション区画で選択した作業に関連するアイコンが表示されます。アイコンをダブルクリックすると、関連する作業が始まります。たとえば、ナビゲーション区画で「認証」をクリックすると、コンソール区画には、OCF サーバーで利用可能な認証のタイプを表すアイコンが表示されます。

ダイアログボックス

各作業には 1 つまたは複数の関連するダイアログボックスがあります。このようなダイアログボックスは、コンソール区画でアイコンをダブルクリックすると表示されます。ダイアログボックス内の情報は、必要に応じて、表示、変更、または削除できます。いくつかのダイアログボックスは複数のフォルダタブを持っています。このようなフォルダにアクセスするには、フォルダタブをクリックします。

ほとんどのダイアログボックスには、次の 4 つのボタンがあります。

- 了解 - 変更を保存して、ダイアログボックスを閉じます。

- 適用 - 変更を保存しますが、ダイアログボックスは閉じません。「適用」ボタンを使用するのは、複数のフォルダタブを持つダイアログボックスにおいて、あるフォルダタブで情報を入力した後、別のフォルダタブでも情報を入力する必要がある場合などです。
- 取消し - 変更を保存せずに、ダイアログボックスを閉じます。
- ヘルプ - ダイアログボックスのオンラインヘルプを表示します。

オンラインヘルプシステムの使用

SmartCard Console のヘルプシステムは、次の情報を提供します。

- SmartCard Console による主なスマートカードの作業の操作。ある項目についてのヘルプを表示するには、「ヘルプ」メニューから「INDEX」を選択します。
- SmartCard Console にある各ダイアログボックスの説明。ダイアログボックスの下部にある「ヘルプ」ボタンをクリックすると表示されます。
- SmartCard Console に関するアイテムヘルプ。アイテムヘルプは情報区画に自動的に表示されます。

SmartCard Console のヘルプシステムは、スマートカードについての概念的な情報は提供しません。スマートカードの動作や認証のタイプ、およびその他の概念的な情報については、このマニュアルを参照してください。

SmartCard Console の終了

SmartCard Console を終了するには、「コンソール」メニューから「終了」を選択します。セッション中に行なった変更はすべて保存されます。

SmartCard Console の起動

Solaris 8 ソフトウェアをインストールすると、SmartCard Console が自動的にインストールされます。SmartCard Console には、Solaris デスクトップまたはコマンド行からアクセスできます。

▼ SmartCard Console を起動するには (CDE)

この手順では、CDE のアプリケーションマネージャから SmartCard Console を起動する方法を説明します。

あるいは、CDE の「ワークスペース」メニューから「ツール」を選択して、次に「スマートカード」を選択しても、SmartCard Console を起動できます。

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。

   すで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。

2. デスクトップのメニューバーにあるアプリケーションの上矢印をクリックして、「アプリケーション」アイコンを表示させます。

3. 「アプリケーション」を選択して、アプリケーションマネージャにアクセスします。

4. 「システム管理」アイコンをダブルクリックして、「スマートカード」アイコンにアクセスします。

5. 「スマートカード」アイコンをダブルクリックして、**SmartCard Console** を起動します。

▼ SmartCard Console を起動するには (コマンド行)

1. コマンド行にスーパーユーザーとしてログインします。

2. **SmartCard Console** を起動します。

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

コマンド行からのスマートカードの管理

`smartcard` コマンドの使用により、コマンド行から Solaris スマートカードを管理することができます。これより後の章では、`smartcard` コマンドを使用したスマートカードのタスクの実行手順を示します。

カードリーダーの設定 (タスク)

この章では、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。

この章では、次の手順について説明します。

カードリーダーの設定 (タスクマップ)

次の表に、カードリーダーを設定および保守するために必要なすべての作業を示します。

表 3–1 カードリーダーの設定のタスクマップ

作業	説明	参照先
1. カードリーダーの追加	スマートカードを使用する各システムにカードリーダーを追加します。	27ページの「新しいカードリーダーを追加するには (SmartCard Console)」、または 30ページの「iButton リーダーを追加するには (コマンド行)」、または 31ページの「Sun SCRI External Card Reader 1 を追加するには (コマンド行)」、または 32ページの「Sun SCRI Internal Card Reader 1 を追加するには (コマンド行)」
2. カードリーダーの属性の表示または変更	(オプション) カードリーダーの属性を表示または変更します。	28ページの「カードリーダーの属性を表示または変更するには (SmartCard Console)」
3. カードリーダーの取り外し	(オプション) カードリーダーが不要になった場合は、`smartcard` コマンドでカードリーダーのサポートを論理的に削除してから、カードリーダーをシステムから物理的に取り外すことができます。	34ページの「カードリーダーを取り外すには (SmartCard Console)」または 34ページの「カードリーダーを取り外すには (コマンド行)」

カードリーダーの設定

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 (カード端末の出荷時の名前とリーダーモデル名) を示します。

表 3–2　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
Sun 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 (SmartCard Console)

SmartCard Console でカードリーダーを設定する場合は、ナビゲーション区画で「カードリーダー」を選択します。このオプションでは、次のことを行うことができます。

- 新しいカードリーダーの追加
- 以前に構成済みのカードリーダー用に設定されている属性の表示と変更

▼ 新しいカードリーダーを追加するには (SmartCard Console)

SmartCard Console を起動する方法については、24ページの「SmartCard Console を起動するには (コマンド行)」を参照してください。

1. **(オプション) 外付けカードリーダーがシステムに物理的に取り付けられていることを確認します。**

   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. **ナビゲーション区画で「カードリーダー」をクリックします。**

3. **「Add Reader」をダブルクリックします。**

4. 追加したいカードリーダーのタイプをダブルクリックします。
   「カードリーダー: SunCardReader」ダイアログボックスが表示されます。

5. 「**Basic Configuration**」フォルダタブを選択します。

6. 「**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クリックします。

8. 「了解」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。

カードリーダーの属性の表示または変更 (SmartCard Console)

カードリーダーの「Basic Configuration」フォルダには、次のような属性があります。

- **Unique Card Terminal Name** - カードリーダーを識別するための一意な名前。コマンド行でカードリーダーを追加するときには、*user_friendly_reader* 名と呼ばれます。
- **Model Name** - メーカーが付けた、カードリーダーのモデル名。「Add Reader」ダイアログボックスから選択します。表 3–2 では、*card_reader_model* 名と呼ばれます。
- **Device Port** - カードリーダーが取り付けられているポートの絶対パスによるデバイス名。たとえば、シリアルポート b は `/dev/cua/b` です。

「Advanced Configuration」フォルダには、メーカーが付けた、カードリーダーの *card_terminal_factory_name* が表示されます。メーカーが新しく発行したカードリーダーの名前を変更した場合などを除き、この名前を変更する必要はありません。

▼ カードリーダーの属性を表示または変更するには (SmartCard Console)

カードリーダーの基本属性を表示または変更するには、次の手順を使用します。

1. 「**Unique Card Terminal Name**」フィールドにカードリーダーの一意な名前を入力します。あるいは、デフォルトの名前をそのまま使用します。

同じタイプのカードリーダーを何台もシステムに取り付けている場合は、各カードリーダーの一意なカード端末の出荷時の名前を入力する必要があります。

2. 表示されたモデル名よりも新しいバージョンのカードリーダーを使用している場合は、カードリーダーのモデル名を入力します。

3. 矢印をクリックして、適切なデバイスパスを選択します。

4. ダイアログが表示されたら、`ocfserv` を再起動します。

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 (コマンド行)

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. 外付けカードリーダーがシステムに物理的に取り付けられていることを確認します。

   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。

3. 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。たとえば、次のようにします。

```
# 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/cua/b	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 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 (コマンド行)

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. 外付けカードリーダーがシステムに物理的に取り付けられていることを確認します。

   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。

3. 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。たとえば、次のようにします。

```
# 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 com.sun.opencard.terminal.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/cua/b`	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 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 (コマンド行)

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. 次のコマンドを **1** 行に入力して、**Sun SCRI Internal Card Reader 1** を追加します。たとえば、次のようにします。

```
# 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/scmi2c1`	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`*n*)。このとき、`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 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したいとき、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は、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)

SmartCard Console の起動については、24ページの「SmartCard Console を起動するには (コマンド行)」 を参照してください。

1. ナビゲーション区画の「カードリーダー」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」メニューから「ターミナルを削除」を選択します。
4. 「了解」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。

▼ 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 (概要)

この章では、スマートカードの設定の概要を示します。

この章では、次の内容について説明します。

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。SmartCard Console からスマートカードサポートを設定する手順については、第 5 章を参照してください。この章では、コマンド行による設定例も示しています。SmartCard Console を起動する手順については、24ページの「SmartCard Console を起動するには (コマンド行)」を参照してください。

カードサービスの無効化または有効化

デフォルトでは、OCF サーバーは次のカードサービスを認識します。

- Schlumberger CyberFlex
- Schlumberger PayFlex
- Dallas Semiconductor iButton

「カードサービス」ダイアログボックスを使用すると、特定のカードのサービスが有効であるかどうかを確認したり、カードサービスを無効にしたりできます。カードサービスを無効化または有効化する手順は、47ページの「カードサービスを無効または有効にするには (SmartCard Console)」を参照してください。

スマートカードの **ATR** 属性の追加または変更

ATR (Answer-To-Reset) 属性には、スマートカードのバージョンを識別する数値が含まれています。ATR 属性は、スマートカードのメーカーにより提供されています。

サポートされるスマートカードは、次の ATR 属性値を持ちます。

```
PayFlex.ATR      = 3B690005792020101000100A9
                   3B691100000057920201010001 00
IButton.ATR      = 008F0E000000000000000000000004000034909000
CyberFlex.ATR    = 3B169481100601810F 3B169481100601811F
```

初めてスマートカードを設定するときには、スマートカード上の ATR を OCF サーバーに識別させます。

サイト内で使用しているスマートカードのメーカーが ATR 属性の異なる新しいカードタイプを発行した場合、システムの ATR 属性を変更する必要があります。このとき、新しいスマートカードを使用するすべてのシステムで ATR 属性を変更する必要があります。

アプレットを SmartCard Console からロードしようとしていて、次に示すメッセージが表示された場合は、ATR を追加しなければならない場合もあります。

```
No compatible devices inserted
```

新しいスマートカードの ATR を追加または変更する手順については、47ページの「スマートカードの ATR を追加または変更するには (SmartCard Console)」を参照してください。

SolarisAuthApplet アプレットの読み込み

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。

アプレットをスマートカードに読み込む手順については、48ページの「アプレットをスマートカードに読み込むには (SmartCard Console)」を参照してください。

スマートカード上でのユーザー情報の作成

デフォルトのアプレットを読み込んだ後は、スマート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は、ログイン名、パスワード、PIN (Personal Identification Numver)、およびセキュリティ保護されているアプリケーションなど、そのユーザーについての個人情報を指定します。

スマートカード上でユーザー情報を作成する手順については、51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 (SmartCard Console)」を参照してください。

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」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。

表 4–1 スマートカードの認証属性

属性	サポートされているスマートカードのタイプ	説明
PIN	すべて	個人の ID 番号 (PIN: Personal Identification Number)
Password (パスワード)	すべて	ユーザーのパスワード (システムまたはネームサービスのパスワードデータベースにあるパスワードと同じ)
User (ユーザー)	すべて	ユーザーのログイン名 (システムまたはネームサービスのパスワードデータベースにあるログイン名と同じ)
Application (アプリケーション)	すべて	ユーザーが当該スマートカード上の情報を使ってログインする必要があるアプリケーション
Private Key (非公開鍵)	CyberFlex、 iButton	ファイルに署名するときに使用される非公開鍵。詳細は、58 ページの「非公開鍵属性」を参照
Certificate (証明書)	CyberFlex、 iButton	構成可能な属性であるが、Solaris スマートカードには証明書用に定義されたインタフェースは用意されていない。詳細は、`smartcard(1M)` のマニュアルページを参照

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。

注 - `SolarisAuthApplet` アプレット内の各アプリケーションには複数のログイン名とパスワードの組み合わせを定義できますが、このアプレットには PIN は 1 つしか定義できません。

スマートカードの PIN を変更する手順については、49ページの「スマートカード上の PIN を変更するには (SmartCard Console)」を参照してください。

ユーザーは後でこの PIN を変更できます。87ページの「スマートカード上の PIN を変更するには (コマンド行)」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。

ユーザー属性とパスワード属性がどのように機能するか

デフォルトの認証機構 (PIN Password) を使用するシステムでは、`ocfserv` は PIN が認証されていることを確認します (42ページの「PIN Password がどのように機能するか」を参照)。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。

スマートカードには複数のログイン名とパスワードの組み合わせを定義できます。たとえば、スマートカードのユーザーが別のアプリケーションにアクセスするために、異なるログイン名とパスワードを使用する必要がある場合などです。また、システム管理者の場合、通常のユーザーとしてのログイン名とパスワードの他に、

スーパーユーザーとしてのパスワードもスマートカードに定義できます。ただし、スマートカードに定義できる PIN は 1 つだけです。

アプリケーション属性

アプリケーション認証属性を使うと、ユーザーが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。

アプリケーション属性がどのように機能するか

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。

OCF サーバーとクライアントアプリケーションのデフォルトの認証機構の設定

「authmechanism」属性は、クライアントアプリケーションがローカルシステム上で使用する認証機構を定義します。Solaris スマートカードは、次の 3 つの認証機構を提供します。

- **Password** - ユーザーのログイン名に関連付けられたパスワード。スマートカード上に存在するか、クライアントアプリケーションにアクセスしようとするときに入力する必要があります。
- **PIN** - ユーザーの PIN (Personal Identification Number)。スマートカード上に存在するか、クライアントアプリケーションにアクセスしようとするときに入力する必要があります。
- **Challenge-Response** - ユーザーがクライアントアプリケーションにアクセスする前には、システムとスマートカードの間で Challenge-Response 認証シーケンスが発生している必要があります。

デフォルトの「authmechanism」属性は PIN Password です。

PIN Password がどのように機能するか

ocfserv とクライアントアプリケーションのデフォルトの認証機構は PIN Password です。この場合、ユーザーがアプリケーション (デスクトップなど) にログインしようとすると、アプリケーションによりユーザーは PIN の入力を求められます。

ocfserv サーバーは、ユーザーが入力した PIN とスマートカードの PIN を照合して、ユーザーが本人であることを確認します。PIN が一致した場合、アプリケーションへのアクセス権がユーザーに与えられます。あるいは、ocfserv がさらにスマートカード上の補助的な認証属性を読み取ります。

コマンド行からこの属性を設定する手順については、52ページの「サーバーとクライアントアプリケーションのデフォルトの認証機構を設定するには (コマンド行)」を参照してください。

クライアントアプリケーションのデフォルトの認証

ローカルシステムの認証を設定するときは、スマートカード上に対応する認証機構を持っていないユーザーはアクセスできないように設定します。デフォルトでは、スマートカードでログイン中に、ocfserv はサーバーの認証機構を使用します。

ユーザーが異なる認証シーケンスセットでクライアントアプリケーションにアクセスしようとした場合は、ログイン中 ocfserv はクライアントの認証機構を使用します。

クライアントの認証属性を構成する前に、ocfserv の認証機構が有効になっている必要があります。デフォルトでは、Solaris スマートカードがサポートするすべての認証機構は、Solaris 8 リリースをインストールしたときに有効になります。サポートされている認証機構は次のとおりです。

- Password
- PIN
- Challenge-Response

個々の OCF クライアントアプリケーションが使用するデフォルトのスマートカードとデフォルトの認証シーケンスには、属性を定義する必要があります。ローカルシステム上で動作する重要なアプリケーションのセキュリティを保護するには、スマートカードを使用したログインが必要となるように構成します。デフォルトで

は、アプリケーション dtlogin がセキュリティ保護されています。このアプリケーションは、共通デスクトップ環境 (CDE) へのログインを制御します。

アプリケーションは、必ずしも、ocfserv と同じ認証シーケンスを持つ必要はありません。ocfserv の認証シーケンスと異なる場合、クライアントの認証シーケンスが優先されます。たとえば、ocfserv のデフォルトの認証機構として「password」を構成しておいて、クライアントアプリケーション (Solaris デスクトップなど) にアクセスしようとするユーザーの認証シーケンスに PIN 認証を追加することもできます。

コマンド行からこの属性を設定する手順については、52ページの「サーバーとクライアントアプリケーションのデフォルトの認証機構を設定するには (コマンド行)」を参照してください。

スマートカードの操作の有効化

スマートカード設定における最後の手順は、スマートカードの操作を有効にすることです。

スマートカードの操作を有効にする手順は、53ページの「スマートカードの操作を有効にするには (コマンド行)」 を参照してください。

スマートカードを有効化し、かつ以下の状態である場合、dtlogin によるログインはできません。

- 現在使用されているスマートカードを持っていない。
- スマートカードがうま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がなく、スマートカードを有効化する場合は、次のことを行います。

1. 「dtlogin」ログイン画面の「オプション」メニューから「コマンド行ログイン」を選択します。
2. スーパーユーザー (root) としてログインします。
3. スマートカードの操作を無効化します。

スマートカードの操作を無効にする手順は、82ページの「スマートカードの操作を無効にするには (コマンド行)」 を参照してください。

第 5 章

スマートカードの設定 (タスク)

この章では、SmartCard Console からまたはコマンド行からスマートカードを設定する方法を説明します。

この章では、次の手順について説明します。

この章に記述されているタスクでは、サイトでスマートカードをどのように実装するかをユーザーがすでに認識していることが想定されています。また、スマートカードを使用するすべてのシステム上でカードリーダーがすでに設定されていることが想定されています。詳細は、17ページの「スマートカード構成の計画」を参照してください。

スマートカードの設定 (タスクマップ)

表 5–1 スマートカードの設定 (タスクマップ)

タスク (作業)	説明	参照先
1. カードサービスが有効化されていることの確認	ログインに使用するスマートカードのカードサービスが有効であることを確認します。	47ページの「カードサービスを無効または有効にするには (SmartCard Console)」
2. スマートカードの ATR の追加または変更	(オプション) スマートカードの ATR を追加します。あるいは、スマートカードのメーカーが新しいスマートカードを発行した場合は、ATR を変更します。	47ページの「スマートカードの ATR を追加または変更するには (SmartCard Console)」
3. アプレットのスマートカードへの読み込み	`SolarisAuthApplet` アプレットをスマートカードに読み込みます。	48ページの「アプレットをスマートカードに読み込むには (SmartCard Console)」
4. スマートカードの PIN の変更	スマートカードのデフォルトの PIN を変更します。	49ページの「スマートカード上の PIN を変更するには (SmartCard Console)」
5. スマートカード上でのユーザー情報の作成	スマートカードのユーザーについての個人情報を指定します。	51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 (SmartCard Console)」
6. OCF サーバーとクライアントアプリケーションのデフォルトの認証機構の設定	サーバーのデフォルトのサーバー認証機構と、すべてのクライアントアプリケーションのデフォルトの認証機構を定義します。	52ページの「サーバーとクライアントアプリケーションのデフォルトの認証機構を設定するには (コマンド行)」
7. スマートカードの操作の有効化	システムでのスマートカードの操作を有効にします。	53ページの「スマートカードの操作を有効にするには (コマンド行)」

▼ カードサービスを無効または有効にするには (SmartCard Console)

Solaris 8 リリースがインストールされている場合、Solaris スマートカードがサポートするすべてのカードサービスがデフォルトで有効になっています。

SmartCard Console を起動する方法については、24ページの「SmartCard Console を起動するには (コマンド行)」を参照してください。

1. ナビゲーション区画で「カードサービス」をクリックします。
   「カードサービス」ダイアログボックスが表示されます。
2. スマートカードのアイコンをダブルクリックします。
3. 次のいずれかを実行して、カードサービスを有効化または無効化します。
   a. カードサービスを有効のままにしておく場合は、「**Keep *card_type* services activated**」ラジオボタンが選択されていることを確認します。
   b. カードサービスを無効にする場合は、「**Deactivate the *card_type* services**」ラジオボタンを選択します。
4. 「了解」をクリックします。
5. `ocfserv` を再起動するようプロンプトが表示された場合は、「**OCF** を再起動しない」を選択します。

▼ スマートカードの ATR を追加または変更するには (SmartCard Console)

SmartCard Console を起動する方法については、24ページの「SmartCard Console を起動するには (コマンド行)」を参照してください。

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」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: *Card-Type*」ダイアログボックスには、このカードタイプについて認識されている ATR のリストと、新しい ATR を追加するための「追加」ボタンが表示されます。

4. 表示された **ATR** が新しい **ATR** である場合、「追加」をクリックします。変更を有効にするには、「新しい **ATR**」フィールドに新しい **ATR** を入力するか、「挿入されているカードの **ATR**」ボックスに表示された **ATR (**挿入されたスマートカードで読み取られた **ATR)** を選択して、「了解」または「適用」を押します。

   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。

   「挿入されているカードの ATR」ボックスに番号が表示される場合、これらは `ocfserv` が挿入されているカードから読み取って、新しい番号であると判断した ATR 番号です。「挿入されているカードの ATR」ボックスを使用する場合は、「新しい ATR」フィールドに新しい ATR 番号を入力する必要はありません。表示された ATR を選択して、「了解」または「適用」をクリックするだけで、変更は適用されます。

▼ アプレットをスマートカードに読み込むには (SmartCard Console)

SmartCard Console を起動する方法については、24ページの「SmartCard Console を起動するには (コマンド行)」を参照してください。

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」アイコンを選択します。
3. 「**SolarisAuthApplet**」アイコンをダブルクリックします。
4. 初期化したいスマートカードのタイプ用にアプレットを、「**CyberFlex**」、「**iButton**」、または「**PayFlex**」の中から選択します。
5. ウィンドウの中央にある矢印で、選択したアプレットを「アプレットのインストールを保留」領域に移動します。
6. 「インストール」をクリックします。

   ポップアップウィンドウが現れて、「了解」ボタンが表示されます。

「インストール」をクリックすることができず「No compatible devices inserted」メッセージが表示された場合は、そのカードについて正しいアプレットを選択しており、カードの ATR が認識されているものであるかどうかを確認してください。カードの ATR については、前の節を参照してください。

7. 「了解」をクリックします。

   アプレットの読み込みには数分間かかります。ウィンドウが現れて、確認メッセージが表示されます。

▼ アプレットをスマートカードに読み込むには (コマンド行)

SolarisAuthApplet アプレットを Solaris Smart Card がサポートするすべてのカードタイプにロードするには、このコマンドを使用します。

1. スマートカードをカードリーダーに挿入します。

2. スーパーユーザーになります。

3. SolarisAuthApplet アプレットをスマートカードにロードします。

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

   smartcard -c load が終了すると、次のメッセージが表示されます。

```
Operation successful.
```

▼ スマートカード上の PIN を変更するには (SmartCard Console)

SmartCard Console を起動する方法については、24ページの「SmartCard Console を起動するには (コマンド行)」を参照してください。

1. ナビゲーション区画から「アプレットを構成」を選択します。

   カードリーダーに挿入されているスマートカードのタイプを表すアイコンが表示されます。

2. スマートカードのアイコンをダブルクリックします。

   「Configure Applets: *card-name*」ダイアログボックスが表示されます。

3. 「**SolarisAuthApplet**」アイコンをクリックします。

4. 上部にある「**PIN**」フォルダを選択します。

5. 「**Type New PIN**」フィールドに新しい **PIN** を入力して、もう一度、「**Retype New PIN**」フィールドに同じ番号を入力します。

   読み込まれたアプレットのデフォルトの PIN は `$$$$java` です。

6. 「**Change**」をクリックします。

7. ポップアップウィンドウに古い方の **PIN** を入力します。

8. 「**OK**」をクリックします。

▼ スマートカード上の PIN を変更するには (コマンド行)

注意 - 入力した PIN の確認プロンプトは表示されませんので、新しい PIN は正しく入力するように注意してください。

1. スマートカードがカードリーダーに挿入されていることを確認します。

2. スーパーユーザーになります。

3. **PIN** を変更します。

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

   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。

▼ スマートカード上でユーザー情報を作成するには (SmartCard Console)

SmartCard Console を起動する方法については、24ページの「SmartCard Console を起動するには (コマンド行)」を参照してください。

1. ナビゲーション区画から「アプレットを構成」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表示されます。

2. スマートカードのアイコンをダブルクリックします。
   「アプレットの構成: カード名」ダイアログボックスが表示されます。

3. 「**SolarisAuthApplet**」を選択します。
   `SolarisAuthApplet` 構成フォルダがダイアログボックスの右側に表示されます。

4. 「**User Profiles**」フォルダを選択します。

5. 「**User Profile Name**」に `dtlogin` を入力します。

6. スマートカードを使ってログインするユーザーの有効な ***user-name*** と ***user-password*** を指定します。

user-name	ユーザーのログイン名です。
user-password	*user-name* に関連付けられたパスワードです。このパスワードは、システムの `/etc/nsswitch.conf` ファイル (NIS、NIS+、またはローカルファイル) によって定義されたパスワードデータベースの中に存在する必要があります。

注 - スマートカードを構成した後に `passwd` ファイルでユーザーのパスワードが変更された場合は、これらの手順を再び実行して新しいパスワードをそのスマートカードに保存する必要があります。これは自動的に更新されるものではありません。

---

7. 「**Set**」をクリックして、上記属性を設定して保存します。

8. ポップアップウィンドウに **PIN** を入力します。

9. 「**OK**」をクリックします。

10. 初めてユーザープロファイルを作成する場合は、「**Set User Profile: Create New User Profile**」ウィンドウで「**Yes**」をクリックします。

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。スマートカードがカードリーダーに挿入されていることを確認してください。

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。ここで指定する PIN は、49ページの「スマートカード上の PIN を変更するには (SmartCard Console)」 で指定した PIN です。

```
# smartcard -c init -A A000000062030400 -P '001234' username=nigel
password=changeme application=dtlogin
```

▼ サーバーとクライアントアプリケーションのデフォルトの認証機構を設定するには (コマンド行)

1. スーパーユーザーになります。

2. すべてのクライアントアプリケーションについてデフォルトの認証機構を設定します。

```
# smartcard -c admin -a default -x modify authmechanism="Pin | Password |
ChallengeResponse"
```

たとえば、クライアントプログラムのデフォルトの認証機構を PIN Password に設定するには、次のように実行します。

```
# smartcard -c admin -a default -x modify authmechanism="Pin Password"
```

その後、`smartcard -c admin` と入力すると、デフォルトの認証機構は次のように表示されます。

```
default.authmechanism      = Pin Password
```

3. サーバーのデフォルトの認証機構を設定します。

```
# smartcard -c admin -x modify authmechanism="Pin | Password | ChallengeResponse""
```

たとえば、`ocfserv` のデフォルトの認証機構を PIN Password にしたい場合は、次のように実行します。

```
# smartcard -c admin -x modify authmechanism="Pin Password"
```

注 - クライアントとサーバーの認証シーケンスが異なる場合、クライアントの認証シーケンスがサーバーの認証シーケンスよりも優先されます。

▼ スマートカードの操作を有効にするには (コマンド行)

スマートカードを有効にした後、ユーザーがこのシステムにログインするには、そのシステムに承認されたスマートカードを使用する必要があります。PIN の入力が必要な場合もあります。スマートカードを使ってログインする方法については、第 9 章を参照してください。

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. 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
```

第 6 章

OCF サーバーとクライアントの追加構成 (概要)

この章では、ocfserv の概要、およびスマートカードの初期の設定後に変更を行いたい場合のクライアント構成について記述します。

この章では、次の内容について説明します。

- 64ページの「クライアントアプリケーションとスマートカードの取り外しタイムアウトの変更」

Solaris スマートカードでは属性グループを変更して、ocfserv とクライアントアプリケーションがどのように動作するかをシステムごとに定義できます。

SmartCard Console からの OCF サーバー属性の変更

ocfserv は、システム上でのスマートカードの操作を行います。SmartCard Console から ocfserv 属性を変更するには、基本的に次の手順を使用します。

1. ナビゲーション区画で「OCF サーバー」アイコンをクリックします。
2. ローカルシステムを表しているアイコンをダブルクリックして、「OCF サーバー構成」ダイアログボックスを表示します。
3. 「OCF サーバー構成」ダイアログボックスで OCF サーバー属性を定義します。

   これらの属性は、サーバーのデフォルトの動作を定義します。クライアントアプリケーション用に定義された属性で上書きされない限り、この属性が優先されます。

   「OCF サーバー構成」ダイアログボックスには、次の 3 つのフォルダがあります。

   - リソース - 「リソース」フォルダは、ローカルシステム上における OCF サーバーのデフォルトの動作を決定する属性を定義します。このフォルダには、「利用可能なリソース」リストと「デフォルト」リストがあります。
   - デバッグ - 「デバッグ」フォルダは、OCF サーバーのデバッグ属性を設定します。デバッグ属性はオプション (省略可能) です。
   - クラスパス - 「クラスパス」フォルダは、OCF サーバーが認識する .jar ファイルを追加または削除します。

   SmartCard Console の使用方法については、22ページの「SmartCard Console の使用」を参照してください。

OCF サーバーの属性の概要

この節では、デフォルトの属性がサイトに適合しない場合に変更する必要がある ocfserv の属性の概要について説明します。次のような場合は、OCF サーバーの属性を変更する必要があることがあります。

- サイトのセキュリティ要件を満たしていない場合
- スマートカードまたはカードリーダーのメーカーが製品を更新して、その製品の ATR 番号やカード端末の出荷時の名前などの情報を変更した場合
- サイトの開発者が開発したカスタムアプリケーションにデフォルト以外のセキュリティ属性が必要な場合

OCF サーバーの属性を変更する手順については、第 7 章を参照してください。

この節では、各 ocfserv 属性について説明し、そのデフォルト値を示します。OCF サーバーの属性を表示するには、SmartCard Console または smartcard -c admin コマンドを使用します。

有効なスマートカードとデフォルトのスマートカードのサーバー属性

「ocf.server.default.validcards」属性は、どのスマートカードのタイプがシステム上で有効であるかを指定します。デフォルトでは、3 つのスマートカードのタイプすべてが有効です。

この属性を変更する手順については、67ページの「サーバーに有効なスマートカードを変更するには (SmartCard Console)」を参照してください。

「ocf.client.default.defaultcard」属性は、どのスマートカードがデフォルトであるかを ocfserv に指定します。デフォルトでは、Solaris スマートカードには指定されているスマートカードはありません。

この属性を変更する手順については、68ページの「サーバーのデフォルトのスマートカードを変更するには (SmartCard Console)」を参照してください。

サポートされているカードリーダーの属性

「OpenCard.terminals」属性は、そのシステムでサポートされているカードリーダーを定義します。たとえば、Sun SCRI External Card Reader 1 を持つシステムの場合、「OpenCard.terminals」の値は次のようになります。

```
OpenCard.terminals          = com.sun.opencard.terminal.scm.SCMStc
.SCMStcCardTerminalFactory|MySCM|SunSCRI|dev/cua/b
```

上記の例では、OpenCard.terminals は現在構成されているカードリーダーとして Sun SCRI External Card Reader 1 を定義しています。カードリーダーを追加すると、smartcard -c admin コマンドで「OpenCard.terminals」属性が表示されます。

カードリーダーを追加する手順については、第 3 章を参照してください。

Open Card サービスの属性

OpenCard.services 属性は、スマートカードに固有なモジュールの位置を指定します。各スマートカードのタイプには、次のモジュールが定義されています。

```
OpenCard.services           = com.sun.opencard.service.cyberflex.CyberFlex
ServiceFactory com.sun.opencard.service.ibutton.IButtonServiceFactory com.
sun.opencard.service.payflex.PayFlexServiceFactory
```

カードサービスの有効化または無効化については、47ページの「カードサービスを無効または有効にするには (SmartCard Console)」を参照してください。

非公開鍵属性

Solaris スマートカードの非公開鍵の機能を使用するには、公開鍵インフラストラクチャ (PKI) をサイトに設定しておく必要があります。スマートカード上で非公開鍵を作成する手順については、76ページの「スマートカード上で非公開鍵を作成するには (コマンド行)」を参照してください。

注 - スマートカードに格納できる非公開鍵は 1 つだけです。

非公開鍵属性がどのように機能するか

スマートカードの PIN とパスワードを認証した後、ocfserv は *key_file_name* で指定されたファイルをスマートカードにコピーします。これ以降、そのスマートカードでは、非公開鍵を補助的な認証として使用して、データに署名できるようになります。ユーザーがデータに署名するコマンド (AMI の amisign など) を実行すると、そのコマンドはユーザーのスマートカード上にある非公開鍵を使用して、署名付きデータを作成します。

サイトのポリシーによっては、システムに格納されているユーザーの非公開鍵ファイルを削除したい場合もあります。このファイルを削除すると、非公開鍵はユーザーのスマートカード上だけに存在することになります。

その他の OCF サーバーの属性

次の表に、変更してはならない属性を示します。

表 6–1 変更してはならない OCF サーバー属性

属性名	説明
initializerlocations	アプレット初期設定機能を持つ Java Class ディレクトリの位置 initializerlocations = com.sun.opencard.cmd.IButtonInit
cardservicelocations	カードサービスモジュールがある Java Class ディレクトリの位置 cardservicelocations = com.sun.opencard.service.common
ocfserv.protocol	ocfserv が使用する TCP プロトコル: ocfserv.protocol = rpc
authservicelocations	認証モジュールがある Java Class ディレクトリの位置 authservicelocations = com.sun.opencard.service.auth

SmartCard Console からの OCF クライアント属性の変更

必要に応じて、次の基本手順を使用して SmartCard Console から OCF クライアント属性を変更します。

1. ナビゲーション区画で「OCF クライアント」アイコンをクリックします。
2. ナビゲーション区画で「CDE」アイコンをダブルクリックします。
3. 「クライアントの構成: CDE」ダイアログボックスで、クライアント属性を変更します。

   「クライアントの構成」ダイアログボックスには、次の 4 つのフォルダがあります。

   - カード/認証 - 「カード/認証」フォルダは、クライアントアプリケーションに有効なスマートカードと認証シーケンスを定義します。
   - デフォルト - 「デフォルト」フォルダは、クライアントアプリケーションのデフォルトの属性を定義します。

     このフォルダには `ocfserv` のデフォルトの定義に使用したものと同じオプションがいくつか含まれていますが、こちらはクライアントのデフォルトを定義しています。
   - **Timeouts** - 「Timeouts」フォルダは、スマートカードが取り外された後、認証プロセスが再起動するまでの、アプリケーションが待機する時間の長さを定義します。
   - **Options** - 「Options」フォルダは、クライアントアプリケーションの動作中にスマートカードが取り外された場合のクライアントアプリケーションの動作を定義します。

   SmartCard Console の使用方法については、22ページの「SmartCard Console の使用」を参照してください。

OCF クライアント属性の概要

この節では、ユーザーのスマートカードの構成に基づいて変更することができるクライアント属性について説明します。これらの属性は、SmartCard Console により、または `smartcard -c admin` コマンドにより表示することができます。

以下の属性が OCF クライアントにデフォルトで定義されています。

```
ClientName.PropertyName     Value
  ----------------------     -----
  default.validcards        = CyberFlex IButton PayFlex
  default.authmechanism     = Pin=UserPin
  default.defaultaid        = A000000062030400
```

クライアントのデフォルトのスマートカードとカードリーダー

「`ocf.client.defaultcard`」属性は、(すべての有効なスマートカードのタイプから) クライアントのアプリケーションで使用する必要のある特定のスマートカードのタイプを定義します。Solaris スマートカードでサポートされるスマートカードのタイプは次のとおりです。

- PayFlex
- iButton
- CyberFlex
- OCF サーバーのデフォルト - この値は、クライアントアプリケーションが OCF サーバーのデフォルトのスマートカードとして設定されている値を使用することを示します。

「利用可能なリソース: カードリーダー」カテゴリを使用して、クライアントアプリケーションが認識するデフォルトのカードリーダーを定義します。

これらの属性を変更する手順については、69ページの「クライアントのデフォルトのスマートカードを定義するには (SmartCard Console)」と70ページの「クライアントのデフォルトのスマートカードリーダーを定義するには (SmartCard Console)」を参照してください。

クライアントアプリケーションに有効なスマートカードのタイプとデフォルトのスマートカードのタイプ

2 つのカード属性「defaultcard」と「validcards」により、特定のクライアントアプリケーションまたはシステム上のすべてのクライアントアプリケーションにログインするときに、使用するスマートカードのタイプを指定します。

「validcards」属性では、特定のアプリケーションに有効なスマートカードのタイプをすべて指定します。一方、「defaultcard」属性では、デフォルトのカードとして指定したスマートカードをカードリーダーに挿入するまで、アプリケーションが起動しないように指定できます。

たとえば、アプリケーション B の「validcards」属性として iButton、CyberFlex、およびカード A を指定して、「defaultcard」属性として CyberFlex を指定していると仮定します。アプリケーション B がデフォルトのスマートカードだけを受け付ける場合、ユーザーがカード A を使ってアプリケーション B にログインしようとすると、次のようなメッセージが表示されます。

```
Waiting for Default Card
```

アプリケーション B へのログインは、ユーザーが CyberFlex カードをカードリーダーに挿入するまでブロックされます。

これらの値は、smartcard -c admin を実行すると表示されます。

```
default.validcards        = CyberFlex IButton PayFlex
```

これらの属性を変更する手順については、71ページの「クライアントアプリケーションに有効なスマートカードを変更するには (コマンド行)」と71ページの「クライアントアプリケーションにデフォルトのスマートカードを割り当てるには (コマンド行)」を参照してください。

クライアントアプリケーションのデフォルトの認証機構

「default.authmechanism」属性では、すべてのクライアントアプリケーションのデフォルトの認証機構を指定します。すべてのクライアントアプリケーションのデフォルトは、Pin=UserPin です。また、authmechanism を使用すると、特定のクライアントアプリケーションのデフォルトの認証機構を定義できます。

すべてのクライアントアプリケーションのデフォルトの認証機構を設定する手順については、52ページの「サーバーとクライアントアプリケーションのデフォルトの認証機構を設定するには (コマンド行)」を参照してください。

有効なスマートカードのデフォルトのクライアント認証シーケンス

「ocf.client.default.authmechanism」属性は、クライアントアプリケーションにログインするときに、すべての有効なスマートカードで使用されるデフォルトの認証シーケンスを決定します。

「クライアントの構成: CDE」ダイアログボックスの「使用されるスマートカード」チェックリストには、現在 ocfserv に有効化されているすべてのスマートカードのタイプが表示されます。

「*card_name* 認証」リストには、「使用されるスマートカード」リストから選択したスマートカードのタイプに有効な認証機構が表示されます。

「*card_name* 認証」リストにおける認証機構の順番は、ユーザーが当該クライアントアプリケーションにアクセスするときに ocfserv が実際に試行する認証シーケンスの順番です。

この属性を変更する手順については、70ページの「有効なスマートカードのデフォルトのクライアント認証シーケンスを変更するには (SmartCard Console)」を参照してください。

デフォルトのクライアントアプレットの ID 属性

default.defaultaid 属性は、すべてのアプリケーションに対して実行されるデフォルトのスマートカードアプレットに割り当てられている ID 番号です。デフォルトの ID 番号は、smartcard -c admin を実行すると表示されます。

```
default.defaultaid          = A000000062030400
```

この値は、Solaris スマートカードが実行するデフォルトのアプレット SolarisAuthApplet の AID 属性です。

defaultaid 属性をサイト用にカスタムビルドしたアプレットで置き換える必要がある場合にのみ、defaultaid 属性を変更してください。defaultaid を変更する必要がある場合は、smartcard(1M) のマニュアルページを参照してください。

クライアントアプリケーションとスマートカードの取り外しタイムアウトの変更

「Timeouts」フォルダは、スマートカードが取り外された後、認証プロセスが再起動するまでの、アプリケーションが待機する時間の長さを定義します。

- **Card Removal Timeout** - スマートカードが取り外された後、認証プロセスが再起動するまでの、アプリケーションが待機する時間の長さを指定します。
- **Re-authentication Timeout** - 認証プロセスの再起動後、終了 (またはエラーメッセージが表示される) までの、アプリケーションが待機する時間の長さを指定します。
- **Card Removal Logout Wait Timeout** - スマートカードが取り外された後、ユーザーがログアウトされるまでの、アプリケーションが待機する時間の長さを指定します。

手順については、72ページの「クライアントアプリケーションとスマートカードの取り外しタイムアウトを定義するには (SmartCard Console)」を参照してください。

スマートカードが取り外された場合のクライアントアプリケーションの動作の変更

「Options」フォルダは、クライアントアプリケーションの動作中にスマートカードが取り外された場合のクライアントアプリケーションの動作を定義します。

- **Ignore Card Removal** - スマートカードが取り外された後もアプリケーションの実行を続けるかどうかを決定します。
- **Re-authenticate After Card Removal** - アプリケーションが認証プロセスを再起動して、必要であれば、認証情報 (PIN またはパスワード) を要求するかどうかを決定します。このオプションを選択した場合は、「Timeouts」フォルダに戻って、Re-Authentication Timeout が設定されていることを確認します。

手順については、73ページの「スマートカードが取り外された場合のクライアントアプリケーションの動作を変更するには (SmartCard Console)」を参照してください。

第 7 章

OCF サーバーとクライアントの追加構成 (タスク)

この章では、スマートカードの初期の設定後に行う可能性のある、OCF サーバーとクライアントの追加構成作業について説明します。これらの作業は、SmartCard Console またはコマンド行から行うことができます。

この章では、次の手順について説明します。

- 72ページの「クライアントアプリケーションとスマートカードの取り外しタイムアウトを定義するには (SmartCard Console)」
- 73ページの「スマートカードが取り外された場合のクライアントアプリケーションの動作を変更するには (SmartCard Console)」

OCF サーバーの追加構成のタスク

「OCF サーバー」属性では、各システムにおける `ocfserv` の動作を定義します。これらの属性は、「OCF サーバー構成」ダイアログボックスまたは `smartcard -c admin` コマンドで変更できます。コマンド行から OCF サーバー属性を変更するには、基本的には次の手順を使用します。

1. 属性を変更したいシステム上でスーパーユーザーになります。
2. デフォルトのサーバー属性を変更します。

```
smartcard -c admin -x modify "property_name=property_value"
```

`-x modify`	属性を変更することを示します。
property_name=property_value	変更する属性とその属性に割り当てる値を指定します。

▼ OCF サーバーとクライアントの属性を表示するには (コマンド行)

1. 構成したいシステム上でスーパーユーザーになります。

2. 構成可能な属性を表示します。

```
# smartcard -c admin
```

画面には次のような情報が表示されます。

```
Client Properties:
  ClientName.PropertyName   Value
```

```
  ------------------------   -----
  default.validcards       = CyberFlex IButton PayFlex
  default.authmechanism    = Pin=UserPin
  default.defaultaid       = A000000062030400

Server Properties:

  PropertyName              Value
  ------------              -----
  authmechanism            = Pin Password
  OpenCard.terminals       = com.sun.opencard.terminal.scm.
SCMStc.SCMStcCardTerminalFactory|MySCM|SunSCRI|/dev/cua/b
  ocfserv.protocol         = rpc
  PayFlex.ATR              = 3B690000579202010100010A9 3B691100000057920201010001000
  authservicelocations     = com.sun.opencard.service.auth
  OpenCard.services        = com.sun.opencard.service.cyberflex.CyberFlexServiceFactory
com.sun.opencard.service.ibutton.IButtonServiceFactory com.sun.opencard.service.payflex.
PayFlexServiceFactory abc.class com.sun.services.scm.SCMStcCardTerminalFactory
  initializerlocations     = com.sun.opencard.cmd.IButtonInit
  IButton.ATR              = 008F0E0000000000000000000004000034909000
  cardservicelocations     = com.sun.opencard.service.common
  CyberFlex.ATR            = 3B169481100601810F 3B169481100601811F
  country                  = US
  debugging.filename       = /tmp/ocf_debugfile
  language                 = en
  debugging                = 0
```

▼ サーバーに有効なスマートカードを変更するには (SmartCard Console)

SmartCard Console を起動する方法については、24ページの「SmartCard Console を起動するには (コマンド行)」を参照してください。

デフォルトでは、3 種類のスマートカードはすべて OCF サーバーで有効とみなされます。

1. ナビゲーション区画で「**OCF** サーバー」を選択します。
2. ローカルシステムを表しているアイコンをダブルクリックします。
3. 「利用可能なリソース」リストから「有効なスマートカード」を選択します。

4. リストから、有効または無効にしたいスマートカードを示すチェックボックスをクリックします。

5. チェックボックスをクリックしたスマートカードのカードサービスを有効化します。

   カードサービスを有効にする手順については、47ページの「カードサービスを無効または有効にするには (SmartCard Console)」を参照してください。

6. 「適用」または「了解」をクリックします。

▼ サーバーのデフォルトのスマートカードを変更するには (SmartCard Console)

SmartCard Console を起動する方法については、24ページの「SmartCard Console を起動するには (コマンド行)」を参照してください。

1. ナビゲーション区画で「**OCF** サーバー」を選択します。

2. ローカルシステムを示すアイコンをダブルクリックします。

3. 「利用可能なリソース」リストから「デフォルトのスマートカード」を選択します。

4. リストから、デフォルトとして選択したいカードタイプを示すチェックボックスをクリックします。

   デフォルトでは、「なし」が選択されています。これは、デフォルトのスマートカードのタイプが定義されていないということを意味します。

5. デフォルトとして選択したスマートカードのカードサービスを有効にします。

   カードサービスを有効にする手順については、47ページの「カードサービスを無効または有効にするには (SmartCard Console)」を参照してください。

6. 「適用」または「了解」をクリックします。

クライアントの追加構成のタスク

この節で記述されているタスクを実行する前に、次の作業を行なっておく必要があります。

- システムには少なくとも 1 台のカードリーダーを構成します。
- システム上でカードサービスを起動します。
- サイトで使用するデフォルトの認証機構と各認証機構が発生する順番を決定します。
- システム上で動作するアプリケーションの中から、スマートカードを使用したログインでセキュリティ保護される必要があるものを決定します。

▼ クライアントのデフォルトのスマートカードを定義するには (SmartCard Console)

SmartCard Console を起動する方法については、24ページの「SmartCard Console を起動するには (コマンド行)」を参照してください。

1. ナビゲーション区画で「**OCF** クライアント」を選択します。
2. 「**CDE**」アイコンをダブルクリックします。
3. 「デフォルト」フォルダを選択します。
4. 「利用可能なリソース」リストから「スマートカード」を選択します。
5. クライアントのデフォルトとして選択したいスマートカードのラジオボタンを選択します。デフォルトのスマートカードのタイプとして選択できるのは **1** つだけです。

   注 - デフォルトとして選択したスマートカードのタイプは、有効なスマートカードとして定義されていることも必要です。68ページの「サーバーのデフォルトのスマートカードを変更するには (SmartCard Console)」を参照してください。

   ---

6. 「適用」または「了解」をクリックします。

▼ クライアントのデフォルトのスマートカードリーダーを定義するには (SmartCard Console)

SmartCard Console を起動する方法については、24ページの「SmartCard Console を起動するには (コマンド行)」を参照してください。

1. ナビゲーション区画で「**OCF** クライアント」を選択します。
2. **CDE** アイコンをダブルクリックします。
3. 「デフォルト」フォルダを選択します。
4. 「利用可能なリソース」リストから「カードリーダー」を選択します。
5. クライアントのデフォルトとして選択したいカードリーダーのラジオボタンを選択します。デフォルトのカードリーダーとして選択できるのは **1** つだけです。

注 - 選択したカードリーダーは、前に定義したデフォルトのスマートカードに適合している必要があります。

---

6. 「適用」または「了解」をクリックします。

▼ 有効なスマートカードのデフォルトのクライアント認証シーケンスを変更するには (SmartCard Console)

SmartCard Console を起動する方法については、24ページの「SmartCard Console を起動するには (コマンド行)」を参照してください。

1. ナビゲーション区画で「**OCF** クライアント」を選択します。
2. **CDE** アイコンをダブルクリックします。
3. 「カード/認証」フォルダを選択します。
4. 「使用するスマートカード」リストから、**1** つまたは複数の有効なスマートカードのタイプを選択します。

「*card_name* 認証」リストには、Solaris スマートカードが割り当てたデフォルトの認証機構として PIN が表示されます。「タグ」カラムには、アプリケーションに割り当てられている検索値が表示されます。

5. 「追加」をクリックして、コンボボックスを表示します。

6. 矢印で項目を選択して、プルダウンメニューに **OCF** サーバー上で有効な認証機構を表示します。それから、必要に応じて補助的な認証機構を選択します。

7. 有効なカードとして選択したスマートカードのタイプごとに、上記手順を繰り返します。

8. 「適用」または「了解」をクリックします。

▼ クライアントアプリケーションに有効なスマートカードを変更するには (コマンド行)

1. スーパーユーザーになります。

2. デフォルトの有効なスマートカードを変更します。

```
# smartcard -c admin -a default -x modify validcards="IButton | CyberFlex | PayFlex"
```

IButton | *CyberFlex* | *PayFlex* — これらの値の 1 つまたは複数を組み合わせて指定します。

たとえば、すべてのアプリケーションに有効なスマートカードのタイプとして CyberFlex と PayFlex を定義するには、次のように入力します。

```
# smartcard -c admin -a default -x modify validcards="CyberFlex Payflex"
```

▼ クライアントアプリケーションにデフォルトのスマートカードを割り当てるには (コマンド行)

「application_name.authmechanism」属性を使用すると、特定のアプリケーションに 1 つの認証機構を割り当てることができます。

1. クライアント属性を変更したいシステム上でスーパーユーザーになります。

2. アプリケーションにデフォルトのスマートカードのタイプを割り当てます。

```
# smartcard -c admin -a application_name -x add defaultcard=card_name
```

application_name	デフォルトのスマートカードのタイプを割り当てるアプリケーション
card_name	当該アプリケーションにログインするときに使用する必要があるスマートカードのタイプ。CyberFlex、PayFlex、または IButton のいずれか

たとえば、システムのデスクトップのデフォルトのスマートカードのタイプとして iButton を定義するには、次のように入力します。

```
# smartcard -c admin -a dtlogin -x add defaultcard=IButton
```

その後、smartcard -c admin を実行すると、クライアント属性は次のように表示されます。

```
dtlogin.defaultcard       = IButton
default.validcards        = CyberFlex PayFlex
```

▼ クライアントアプリケーションとスマートカードの取り外しタイムアウトを定義するには (SmartCard Console)

SmartCard Console を起動する方法については、24ページの「SmartCard Console を起動するには (コマンド行)」を参照してください。

1. ナビゲーション区画で「**OCF** クライアント」を選択します。

2. 「**CDE**」アイコンをダブルクリックします。

3. 「**Timeouts**」フォルダを選択します。

4. インジケータをスライドさせて、各タイムアウトの値を変更します。
   - Card Removal Timeout
   - Re-authentication Timeout
   - Card Removal Logout Wait Timeout

   各値については、64ページの「クライアントアプリケーションとスマートカードの取り外しタイムアウトの変更」 を参照してください。

▼ スマートカードが取り外された場合のクライアントアプリケーションの動作を変更するには (SmartCard Console)

SmartCard Console を起動する方法については、24ページの「SmartCard Console を起動するには (コマンド行)」を参照してください。

1. ナビゲーション区画で「**OCF クライアント**」を選択します。

2. 「**CDE**」アイコンをダブルクリックします。

3. 「**Timeouts**」フォルダを選択します。

4. 次のオプションを有効または無効にします。
   - Ignore Card Removal
   - Re-authenticate After Card Removal

   各オプションについては、64ページの「スマートカードが取り外された場合のクライアントアプリケーションの動作の変更」 を参照してください。

第 8 章

スマートカードの追加管理 (タスク)

この章では、スマートカードの管理および保守の追加作業について説明します。これらの作業は、SmartCard Console またはコマンド行から行うことができます。

この章では、次の手順について説明します。

スマートカードの追加の管理タスク

▼ スマートカードの PIN を確認するには (コマンド行)

この手順は、Solaris スマートカードがサポートしているすべてのカードに当てはまります。

1. カードリーダーにスマートカードを挿入します。

2. スマートカードの **PIN** を確認します。

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

PIN_number はスマートカードに設定されている PIN です。

PIN が有効でない場合は「暗証番号 (PIN) が無効です」という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。

▼ スマートカード上で非公開鍵を作成するには (コマンド行)

この手順は、Java ベースの iButton と CyberFlex のスマートカードに当てはまります。PayFlex スマートカードには非公開鍵を格納できません。

非公開鍵の機能を使用するには、公開鍵インフラストラクチャ (PKI) をサイトに設定しておく必要があります。

1. サイトの **PKI** に適切なコマンドを使用して、ユーザー用に **1** 組の公開鍵と非公開鍵を作成します。

2. 鍵の組み合わせから非公開鍵の部分を別のファイルにエクスポートします。

   後で非公開鍵属性を設定する際に絶対パス名を指定する必要があるため、このパス名を記録しておきます。

3. スマートカードの初期化に使用するシステム上でスーパーユーザーになります。

4. スマートカードをカードリーダーに挿入します。

5. **Java** のセキュリティディレクトリに移動します。

```
# cd /usr/java1.2/jre/lib/security
```

6. java.security ファイルを編集します。

7. このファイルの中から security.provider の定義を探します。

```
This is the "master security properties file".
#
.
.
# Each provider must implement a subclass of the Provider class.
# To register a provider in this master security properties file,
# specify the Provider subclass name and priority in the format
#
security.provider.<n>=<classname>
```

8. 次の行の前にコメント記号 **(#)** があることを確認します。

```
#    security.provider.<n>=<className>
```

9. 次のテキストを追加します。

```
# Each provider must implement a subclass of the Provider class.
# To register a provider in this master security properties file,
# specify the Provider subclass name and priority in the format
#
#    security.provider.<n>=<className>
security.provider.2=com.sun.ami.common.SunAMI
```

10. 次のコマンドを **1** 行に入力して、スマートカードを初期化します。

```
# smartcard -c init -A A000000062030400 -P 'PIN_number' privatekey=key_file_name
```

PIN_number	スマートカードに割り当てられている PIN を指定します。
key_file_name	ユーザーの非公開鍵が格納されているファイルのフルパス名を指定します。

注 - SolarisAuthApplet には、証明書属性の完全な実装は提供されていません。

スマートカードを複数のシステムで使用する

smartcard -c init コマンドを実行してユーザーのスマートカードを初期化すると、システムとスマートカードの両方に対称鍵が作成されます。ocfserv は /etc/smartcard/.keys というファイルを作成して、システム上で構成されているすべての秘密鍵に関する情報を格納します。スマートカードが作成されたシステム以外のシステムにユーザーがアクセスする必要がある場合、アクセスする必要があるすべてのシステムに /etc/smartcard/.keys ファイルをエクスポートする必要があります。

▼ システムの鍵ファイルをエクスポートするには (コマンド行)

スマートカードが作成されたシステムから /etc/smartcard/.keys ファイルをエクスポートするには、この手順を使用します。

1. スマートカードが作成されたシステム上でスーパーユーザーになります。
2. 当該ユーザー専用の鍵ファイルを別に作成して、/etc/smartcard/.keys の中から、そのユーザーの鍵だけを格納します。
3. /etc/smartcard/.keys をエクスポートします。

```
# smartcard -c admin -k challenge_response -E -o key_file_name
```

key_file_name	ユーザーの対称鍵が格納されているファイルを指定します。/etc/smartcard/.keys ファイルまたは当該ユーザー専用の鍵ファイルのどちらかです。

▼ ユーザーの鍵ファイルをインポートするには (コマンド行)

ユーザーのスマートカードが作成されたシステム以外のシステムにユーザーの対称鍵をインポートするには、この手順を使用します。

1. スマートカードが作成されたシステム以外のシステム上でスーパーユーザーになります。

2. 鍵ファイルを新しいシステムにインポートします。

```
# smartcard -c admin -k challenge_response -I -i key_file_name
```

key_file_name	/etc/smartcard/.keys または当該ユーザー専用に作成した鍵ファイルのどちらかです。

3. ユーザーがスマートカードを使ってアクセスする必要がある各システムについて、手順 **1** と手順 **2** を繰り返します。

スマートカードの操作での問題の解決

スマートカードを使ってログインするときに障害が発生した場合は、この節を参照してください。

デバッグ属性の設定

スマートカードの動作をシステム上でデバッグするには、デバッグ属性を設定します。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」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」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」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. **(**オプション**)** 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」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」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」または「了解」をクリックします。
8. `ocfserv` を再起動するようプロンプトが表示された場合は、「**OCF** を再起動しない」を選択します。

コマンド行からデバッグを有効にする

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 - 以前のリリースの 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 の場合もあります。

/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 (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
```

▼ スマートカードの操作を無効にするには (コマンド行)

スマートカードの構成エラーにより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の操作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. システムをシングルユーザーモードにします。

```
# shutdown -g180 -y
```

3. スマートカードの操作を無効にします。

```
# smartcard -c disable
```

4. システムをマルチユーザーモードにして、デスクトップ環境に戻ります。

```
Entering System Maintenance Mode
Sun Microsystems Inc.   SunOS 5.8       Generic February 2000
# (Press Control-D)
ENTER RUN LEVEL (0-6, s or S) [3]: 3
```

▼ スマートカードの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. 47ページの「スマートカードの ATR を追加または変更するには (SmartCard Console)」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。

▼ スマートカードの ATR の紛失に関する問題を解決するには

SmartCard Console を使ってスマートカードを追加しようとすると、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。

詳細は、47ページの「スマートカードの ATR を追加または変更するには (SmartCard Console)」を参照してください。

使用例 - 紛失したスマートカードの 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。

▼ 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

スマートカードの操作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 SmartCard
```

1. 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ってシステムにログインできない場合は、rlogin または telnet コマンドを使ってリモートからログインしてみます。

2. スーパーユーザーになり、スマートカードの操作を無効にするよう試みます (はじめにシステムをインストールし直そうとするのではなく)。

   スマートカードの操作を無効にすると、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
   ```

第 9 章

スマートカードの使用 (タスク)

この章では、スマートカードを使って Solaris 8 オペレーティング環境に安全にログインする方法を説明します。

この章では、次の内容について説明します。

スマートカードは、Solaris デスクトップや個々のアプリケーションを保護します。スマートカードを使用すると、パスワードによる一般的な UNIX ログインよりも高いセキュリティ効果を期待できます。これは、デスクトップやアプリケーションに対して自分自身を認証させる (自分が本人であることを証明する) ことができるためです。

スマートカードの内容

Solaris スマートカードは、CyberFlex、iButton、PayFlex という 3 種類のスマートカードをサポートしています。ユーザーのコンピュータにスマートカードリーダーを構成し、組織で使用するスマートカードを各ユーザーに支給するのはシステム管理者です。

スマートカードには次の内容が含まれています。内容はスマートカードの設定によって異なります。

- ログイン名
- パスワード
- スマートカード用の PIN (Personal Identification Number)
- スマートカードの PIN を使ったログインが必要なアプリケーションプログラムの名前
- ファイルの署名に使用される非公開鍵

デスクトップへのスマートカードを使用したログイン

セキュリティ管理者から受け取ったスマートカードは、すぐに使用できます。システム管理者がカードをデフォルトの PIN で構成した場合は、ユーザーはログイン後ただちにそれを自分しか知らない値へ変更すべきです。

▼ スマートカードを使用して Solaris デスクトップにログインするには

1. スマートカードをカードリーダーに挿入します。

   PIN の入力画面が表示されます。

2. システム管理者から提供された **PIN** を入力します。変更した **PIN** またはデフォルトの **PIN** のどちらかを入力します。

   正しい PIN を入力すると、次のいずれかの処理が行われます。

   - スマートカードにパスワードが入っている場合は、自動的にデスクトップにログインできます。
   - スマートカードにログイン名とパスワードが入っていない場合は、標準的な UNIX ログインと同様にログイン名とパスワードを入力する必要があります。

正しいログイン名とパスワードを入力すると、デスクトップにログインできます。

▼ セキュリティ保護されているアプリケーションにスマートカードを使ってアクセスするには

1. スマートカードをカードリーダーへ挿入します。

2. セキュリティ保護されているアプリケーションを実行します。

   PIN の入力画面が表示されます。

3. セキュリティ管理者から提供された **PIN** を入力します。変更した **PIN** またはデフォルトの **PIN** のどちらかを入力します。

   正しい PIN を入力すると、次のいずれかの処理が行われます。

   - スマートカードにパスワードが入っている場合は、自動的にアプリケーションにアクセスできます。
   - スマートカードにログイン名とパスワードが入っていない場合は、標準的な UNIX ログインと同様にログイン名とパスワードを入力する必要があります。正しいログイン名とパスワードを入力すると、アプリケーションにアクセスできます。

▼ スマートカード上の PIN を変更するには (コマンド行)

注意 - 入力した PIN の確認プロンプトは表示されませんので、新しい PIN は正しく入力するように注意してください。

1. スマートカードをカードリーダーに挿入します。

2. **PIN** を変更します。

```
% smartcard -c init -A A000000062030400 -P 'old_PIN' pin=new_PIN
```

old_PIN	現在の PIN です。
new_PIN	新しい PIN 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。

用語集

Answer to Reset (ATR)	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。
ATR	「Answer to Reset (ATR)」を参照。
CDE	「共通デスクトップ環境 (CDE)」を参照。
Challenge-Response	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。
Personal Identification Number (PIN)	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。
PIN	「Personal Identification Number (PIN)」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 **(CDE)**	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。
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	Challenge-Response 認証方法で記述される、DES 鍵の別名。
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

S

V

あ

か

く

こ