インストール、管理、およびユーザガイド

Identrus システムへの iPlanet Portal Server Plug-in

リリース 2.0

2001 年 3 月

目次

図一覧

概要

この章では、Identrus スキーマを使用するために必要な主要コンポーネントについて説明しています。また Identrus システムへの iPlanet Portal Server Plug-in によってどのように電子メールメッセージのセキュリティが保護されるかについても説明します。内容は以下とおりです。

- 本ガイドの構成
- Identrus スキーマ
- スマートカードユーザによる Portal Server へのログオンと電子メールのチェック
- Identrus スキーマまたは適切な認証局によって行われる証明書ステータスチェック

関連ドキュメント

- Solaris 8 および Java Development Kit 1.2.1

  http://docs.sun.com

  http://java.sun.com/products/jdk/1.2/download-docs.html
- iPlanet Portal Server 3.0

  http://docs.iplanet.com/docs/manuals/ips.html
- iPlanet Certificate Management System

  http://docs.iplanet.com/docs/manuals/cms.html
- 『Oracle 8i Installation Guide』および『Oracle 8i Configuration Guide』

  http://www.oracle.com
- Hardware Security nCipher KeySafe 1.0 および CAFast

  http://www.ncipher.com

  http://active.ncipher.com/documentation/PKCS11/solaris-4.01/nforce.pdf
- Identrus メッセージ仕様

  http://www.identrus.com

このガイドの構成

このガイドは、次のユーザを対象としています。

- メールのチェックおよび証明書ステータスのチェックを行う電子メールユーザ
- システムのインストール、構成、および維持を行うシステム管理者 (銀行員または地元の製品サポート担当者など)
- Identrus 対応の Portal Server に独自のアプリケーションを導入する開発者

このガイドは、4 つの章で構成されています。

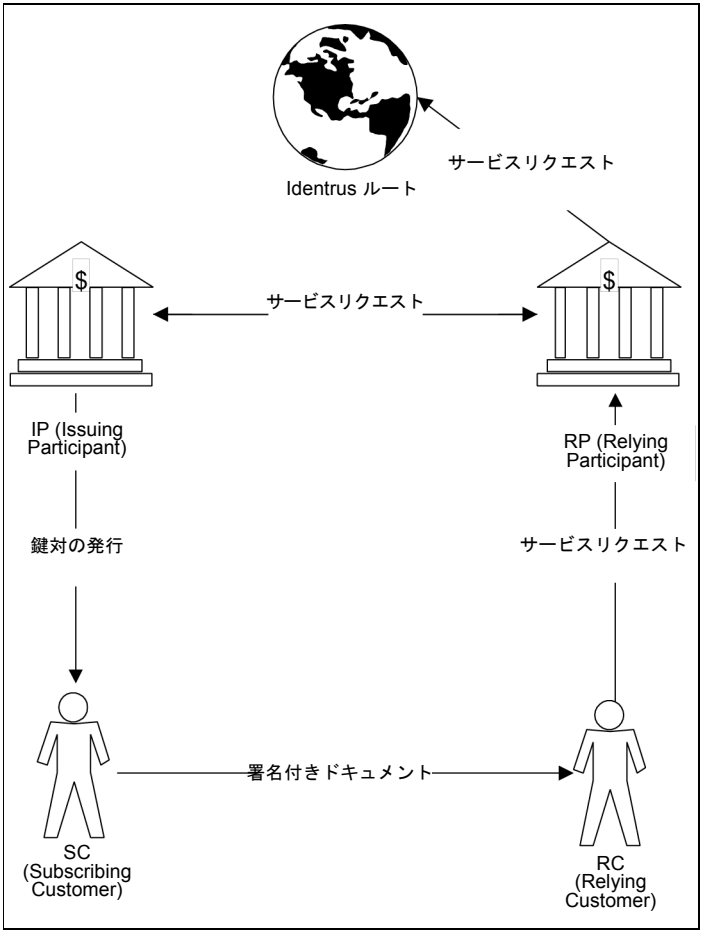
- 第 1 章、「インストール」: 『iPlanet Portal Server 3.0 インストールガイド』に紹介されている、特別な考慮事項について
- 第 2 章、「管理」: Netmail ユーザの設定、証明書の割り当て、Certificate Status Check (CSC) レスポンダの定義などを行う管理者のための情報
- 第 3 章、「ユーザ」: スマートカードを使用したログオン、電子メールメッセージへのデジタル署名、およびセキュリティ保護されたメッセージングについて
- 第 4 章、「アプリケーションを導入する」: Identrus 対応の証明書ステータスチェックを行うために必要なソースコードの開発方法について

Identrus スキーマの概要

Identrus は、インターネットなどの電子ネットワーク上でエンティティを識別するための高度に安全なシステムを確立し、運営するために設立されました。Identrus は、金融機関で構成されて、公開鍵の暗号化と PKI の基本技術を使用し、電子コマースを促進するための共通の運営規則したがって管理されています。

Identrus PKI ネットワークは、次に示す「4 コーナーモデル」を基盤としています。

図 1 Identrus 4 コーナーモデル



4 コーナーは次のエンティティで構成されます。

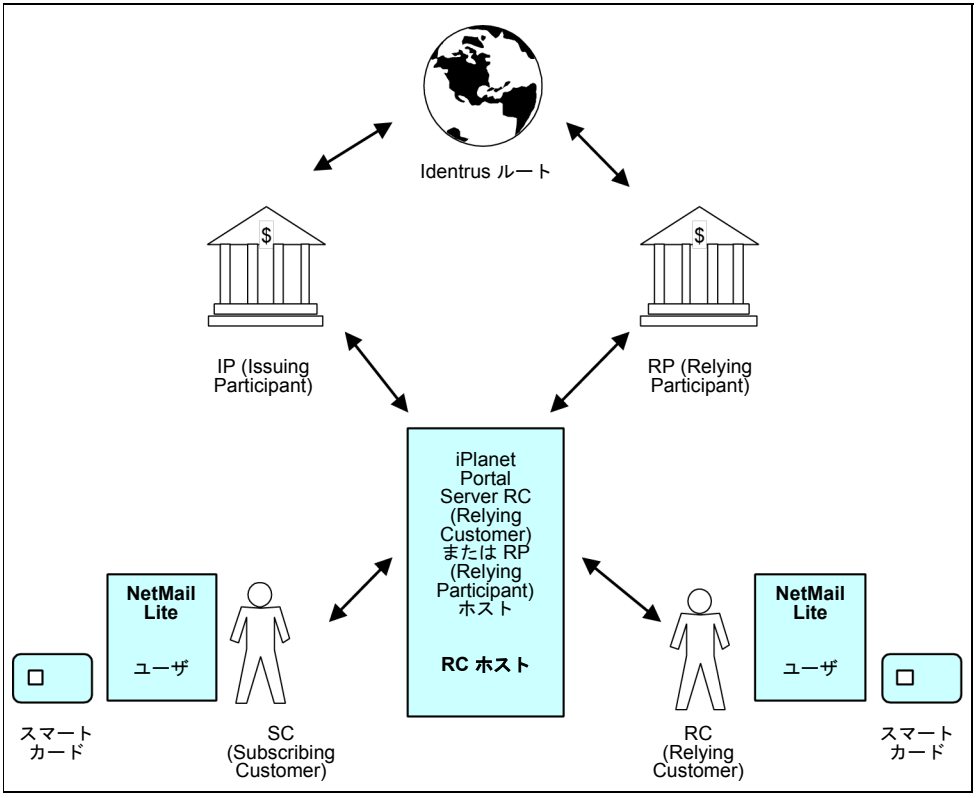
- IP (Issuing Participant) : 秘密鍵および証明書を含むスマートカードを SC に発行する銀行 (またはその他の金融機関)
- SC (Subscribing Customer) : Identrus アクティビティに参加する権限を持つ IP 銀行のメンバー
- RC (Relying Customer) : SC が署名付きトランザクションを開始する相手
- RP (Relying Participant) : SC から受け取った署名付きデータの信頼性をある程度確認するため、RC が問い合わせる銀行 (またはその他の金融機関)

4 コーナーモデルを使用した典型的なトランザクションの流れは次のとおりです。

- SC がスマートカードを使用してトランザクションリクエストに署名し、そのリクエストがシステムから RC に送信される
- RC が、SC から送信された署名付きデータが送信の過程で変更されていないことを確認する
- RC が銀行にサービスをリクエストする。たとえば、SC の証明書が有効である (廃棄されていない) ことを確認するために、銀行にステータスチェックを依頼することが可能
- RP が IP にサービスをリクエストする。また、Identrus ルートに RC のサービスリクエストに対応するようにリクエストする
- 銀行からの応答に基づき、RC が SC からのリクエストを実行または拒否する

Identrus スキーマを利用するために、Identrus システムへの iPlanet Portal Server Plug-in では、次に示すように Portal Server に接続したホストシステムを使用します。

図 2 iPlanet Portal Server と Identrus スキーマ



iPlanet の Portal Plug-in ソリューション

Identrus システムへの iPlanet Portal Server Plug-in は、電子メールメッセージの送受信を行う際に、メッセージ交換を信頼性のあるものにしたいという開発者、ユーザ、および管理者を対象に設計されています。何らかの方法によって次のものが提供される場合、メッセージは意義を持つようになります。

- 認証 : メッセージの送信者を確認できること
- 完全性 : 電子メールメッセージが変更されていないこと
- 否認防止 : 送信者がメッセージを否認できないこと

Identrus システムへの iPlanet Portal Server Plug-in では、次のメカニズムが使用されます。

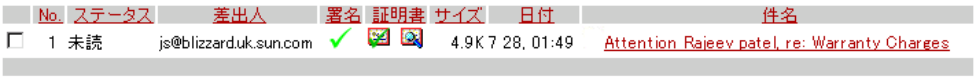
- デジタル署名  : 完全性を実現
- 証明書  : 送信者のメッセージを確認

有効なデジタル署名と、確認済みの証明書がある場合にのみ、メッセージは否認防止性を備えているということができます。これらのメカニズムなしでは、否認防止が可能なメッセージは成り立ちません。このため、このガイドでは次の操作に関連する主なコンポーネントについて説明します。

- システムを構成し、証明書ステータスチェックによってメッセージを認証するために、適切な信頼できる証明書階層を配置する方法
- ユーザが送受信するデジタル署名と証明書付きのメッセージを適切に表示する方法
- 開発者が Identrus 対応の独自のアプリケーションを導入する方法

Identrus システムへの iPlanet Portal Server Plug-in では、送受信するすべての電子メールに対し、NetMail Lite メッセージヘッダーの要約部分に上記のアイコンが表示されます。これにより、ユーザが受信するメッセージのステータスを確認すること、および変更されていないメッセージを送信することが可能になります。

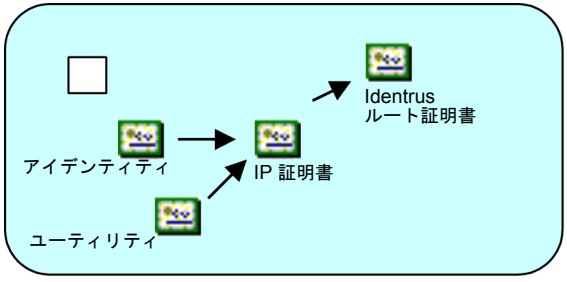
図 3　　メッセージヘッダーの例



Identrus スマートカードのしくみ

Identrus システムへの iPlanet Portal Server Plug-in の設定作業の一環として、ユーザにスマートカードを発行する必要があります。各スマートカードには証明書が含まれています。次の図に示すように、この証明書はどのユーザが Portal Server にログオンできるかを決定する Identrus 階層を持っています。

図 4 スマートカードの証明書階層



特定のスマートカード証明書と信頼できる CA との間に信頼チェーンを構築できる場合、その証明書は信頼できるものとみなされます。このような場合、管理者が Identrus メンバーであるユーザに対して Identrus 証明書階層を含む適切な証明書を設定していれば、そのユーザは Portal Server にログオンできます。

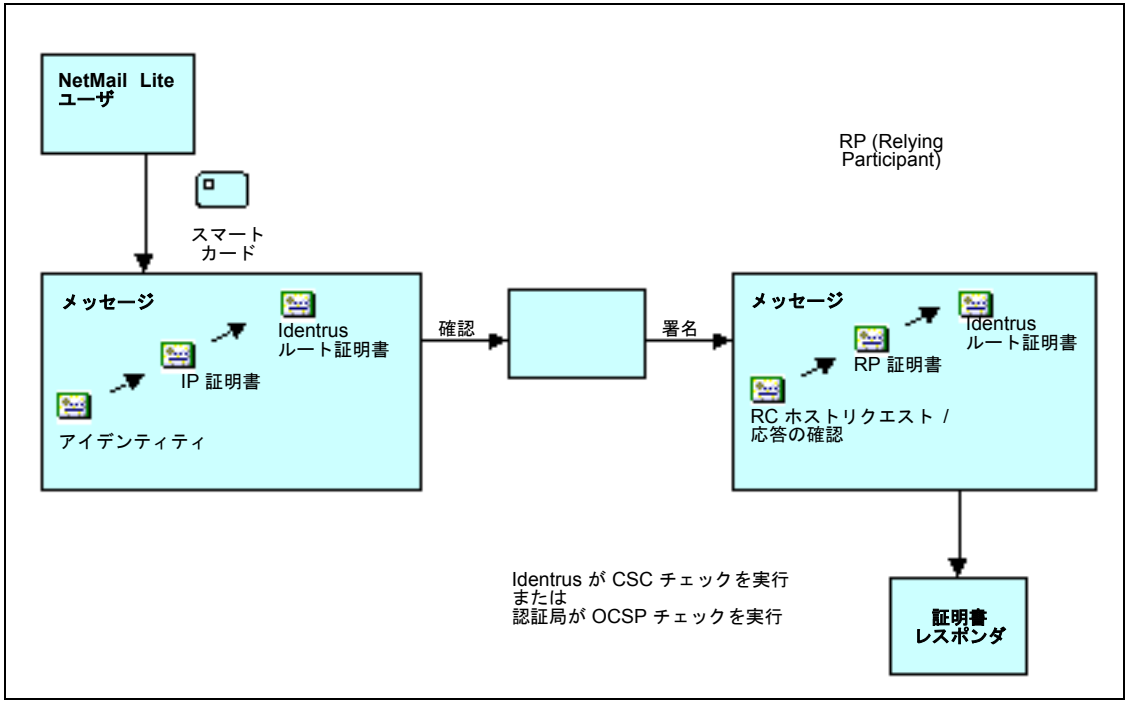
Indentrus を使用するためには、次の証明書が必要です。

- ユーザの身元に関する情報を提供する、Identrus 対応の アイデンティティ証明書
- ユーザのアクセス権に関する情報を提供する、Identrus 対応のユーティリティ証明書
- ユーザのアイデンティティを発行する、Identrus 対応のアイデンティティ CA 証明書
- ユーザのユーティリティを発行する、Identrus 対応のユーティリティ CA 証明書
- Identrus ルート証明書

Identrus 証明書スキーマ

Identrus システムへの iPlanet Portal Server Plug-in をインストールする管理者は、ユーザがこれらの目的を達成するために必要な主要コンポーネントについて認識する必要があります。次の図は、Identrus スキーマ内の適切な認証局によって発行された証明書を使用することによってメッセージの完全性を確認する、一般的な方法の例を示しています。

図 5 Identrus スキーマの証明書確認の概要



電子メールの認証と、送信者 / 受信者の完全性を確保するには、Identrus スキーマに 3 種類の証明書が必要です。

1. アプリケーション認可証明書
   - 信頼できるログイン CA 証明書 : これは通常 RP 銀行であり、この場合、ログインできるのは RP 銀行の顧客のみ。この証明書は確認に使用される
   - 信頼できる電子メール証明書 : これは通常 Identrus ルートであり、この場合、Identrus メンバーが受信したすべての電子メールを確認可能
2. 証明書ステータスチェックの証明書
   - リクエスト署名証明書 : RC ホストから、Identrus CSC または OCSP に送信される。ステータスチェックはこの証明書によって署名される
   - 応答署名証明書 : RC ホストのユーザに返されるステータスメッセージの署名に使用される
   - 信頼できる応答確認証明書 : OCSP か Identrus CSC かにはかかわらず、RC ホストによって応答の確認に使用される
3. トランスポート認証と完全性の証明書
   - SSL クライアント証明書 : クライアントとサーバ間の SSL トランスポートハンドシェイクの署名に使用される

第 1 章

インストール

Identrus システムへの iPlanet Portal Server Plug-in をインストールするには、Portal Server が完全にインストールされていることが前提条件になります。この章では、まずインストールの手順について、次に Identrus のユーザが NetMail Lite を使用するための手順について説明します。この章には、次の項目があります。

- 必要要件
- インストールの手順
- HSM の構成
- インストール後の手順
- ソフトウェアのアンインストール

必要要件

Identrus システムへの iPlanet Portal Server Plug-in をインストールするには、次のソフトウェアとハードウェアの周辺機器があらかじめインストールされている必要があります。

- iPlanet Portal Server 3.0 SP2 および付属の電子メールアプリケーションである NetMail Lite (`http://www.iplanet.com/downloads/patches/2012.html`)
- iPlanet Certificate Management Server (オプション) (`http://www.iplanet.com/downloads/download/2042.html` などを参照)
- スマートカード (クレジットカードなど)。サードパーティのベンダーによって発行されます。必ず Identrus 対応のスマートカードを使用してください。Identrus Network V2.0 への iPlanet Portal Server Plug-in には、現在 GemPlus SmartCards GemSAFE IS 16000 との互換性があります。詳細は、`http://www.gemplus.com/app/banking/gemsafe_is_mkt.htm` を参照してください。
- ブラウザのプラグインを含むスマートカードリーダ。サードパーティのベンダーによって発行されます。必ず Identrus 対応のスマートカードリーダを使用してください。Identrus Network V2.0 への iPlanet Portal Server Plug-in には、現在 GemPlus Card Reader GemPC430 および GemPC410 との互換性があります。詳細は、`http://www.gemplus.com/products/hardware/index.htm` を参照してください。
- GEMSafe Enterprise Workstation 1.0。このソフトウェアには、Identrus Network V2.0 への iPlanet Portal Server Plug-in との互換性があります。詳細は、`http://www.gemplus.com/products/software/gemsafe/index.html` を参照してください。
- Netscape Navigator v4.7x 以降。Internet Explorer 4.0 および Internet Explorer 5.0。これらのブラウザは、スマートカードとスマートカードリーダに付属のソフトウェアによって自動的に構成されます。
- クライアントのブラウザ。これらのブラウザは、GemPlus SmartCard および Portal Server Plug-in と互換性があることが必要です。サポートされているオペレーティングシステムは、Windows NT 4.0 Service Pack 5 (`http://www.microsoft.com/ntserver/nts/downloads/recommended/sp5/allsp5.asp` を参照) および Windows 98 (`http://www.microsoft.com/Windows98/` を参照) です。
- 暗号処理の強化と鍵の安全な保存を保証するハードウェアセキュリティモジュール、CAFast (`http://www.ncipher.com` を参照)。これは Identrus メンバー銀行の管理者が必要とするもので、ユーザには必要ありません。CAFast は、nFast と呼ばれることもあります。
- Identrus システムへの iPlanet Portal Server Plug-in を使用するには、OCSP レスポンダとしての役割を果たすことのできる銀行または機関と関係を持っていること、あるいは Identrus ネットワークに接続していることが必要です。

- Solaris オペレーティング環境用の Java 2 Standard Edition (1.2.2_06 各国語対応版)。Web サーバとゲートウェイで構成される iPlanet Portal Server V3.0 (`http://docs.iplanet.com/docs/manuals/portal/30/install/overview.htm` を参照)。ゲートウェイと Web サーバは、通常別々のマシンに常駐します。ゲートウェイは、Web サーバへのアクセスを制限します。ゲートウェイと Web サーバを別々のマシンに配置するだけで、これらが確実に別々の VM で動作するようになります。一般的なセットアップとしては、(1) Web サーバを認識できるのはゲートウェイのみ、(2) ゲートウェイがアクセスできるのは Web サーバのみであり、Web サーバと同じ範囲を認識することはできない、(3) クライアントが Web サーバによって提供されている機能にアクセスするには、ゲートウェイを通さなくてはならない、(4) クライアントは Web サーバにはアクセスできない、などのようになります。ゲートウェイとサーバを別々のマシンに配置する場合は、インストールおよび構成の際にすべての必要要件が満たされるため、特に必要要件を考慮する必要はありません。ゲートウェイとサーバを同じマシンに配置する場合 (テストや開発などの場合) は、次の手順に従ってください。(1) `http://www.sun.com/software/solaris/java/download.html` から Java をダウンロードします。(2) これを同じマシンの独立した 2 つのエリアに別々にインストールします。これを反映するように、`ipsgateway` スクリプトおよび `ipsserver` スクリプト内の JAVA_HOME を編集します。この例については、第 4 章、「アプリケーションを導入する」を参照してください。
- Oracle 8.0.5 と Oracle 8.1.5 用の JDBC (`http://www.oracle.com/java/jdbc/html/jdbc.html`)

インストールの手順

『iPlanet Portal Server 3.0 インストールガイド』に説明されているガイドラインに従ってください。Identrus システムへの iPlanet Portal Server Plug-in をインストールする前に、Portal Server を新しくインストールする必要があります。また、後でスクリプトを実行する際に必要になるので、このインストール場所を書きとめておくことをお勧めします。

- ルートとしてログインし、シェルプロンプトで次のように入力します。

```
domainname
```

- 上記のコマンドを入力しても何も返されない場合は、「domainname <domain_name>」の形式で、実際のドメイン名を入力します。次に例を示します。

```
domainname uk.sun.com
```

- インストール CD-ROM のルートディレクトリに移動します。次に例を示します。

```
cd /dev/cdrom
```

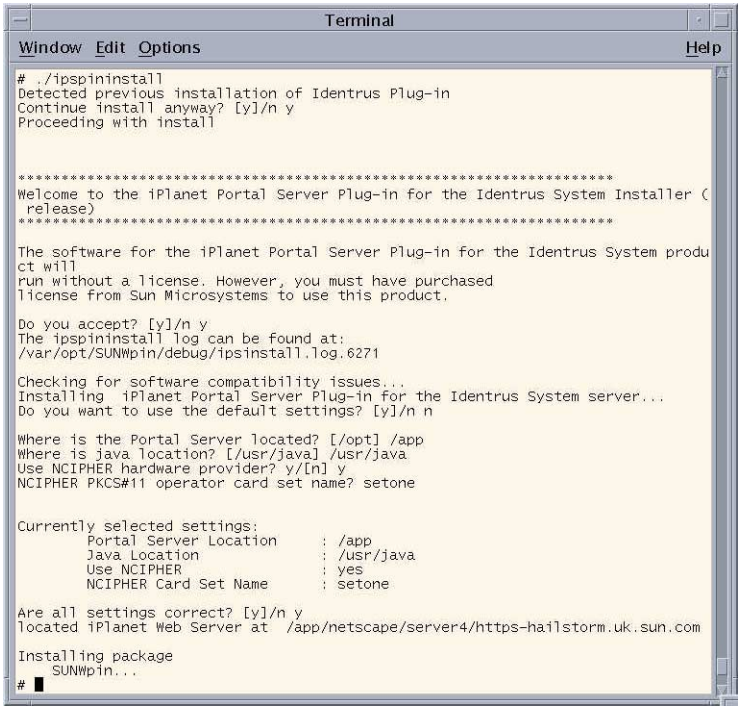
- Portal Server が稼動している必要があります (詳細は iPlanet Portal Server のマニュアルを参照)。
- 次のコマンドを入力して、インストールスクリプトを実行します。

```
./ipspininstall
```

- Portal Server をデフォルトの場所 (`/opt`) にインストールした場合は、Identrus システムへの iPlanet Portal Server Plug-in のインストールにもデフォルトを使用できます。別の場所にインストールした場合は、Portal Server および iPlanet Web Server のインストール場所を指定します。

- 次の図に、一般的なインストール例を示します。

図 1-1 インストールスクリプトの例



- 前述の「必要要件」に示したように、Oracle JDBC ドライバ (通常は `oracle-jdbc-815.zip`) を入手する必要があります。このファイルを次の場所に置きます。

```
<Portal_install_directory>/SUNWips/lib
```

- ファイルを編集することによって、Portal Web Server のディレクトリ内のクラスパスに Oracle のファイル名 (`oracle-jdbc-815.zip`) を反映させます。

```
/opt/netscape/server4/https-hailstorm/config/jvm12.conf
```

- ログイン ID と構成を書きとめて、データベースにアクセスできるようにします。次に、Portal Server Plug-in で要求されるテーブルを設定するために、SQL スクリプトを実行します。

```
<Portal_install_directory>/SUNWpin/sql/OracleCertStore.sql
```

- また、スクリプトを使用してテーブルやデータを削除することもできます。

```
<Portal_install_directory>/SUNWpin/sql/Drop_OracleCertStore.sql
```

- これで Identrus システムへの iPlanet Portal Server Plug-in のインストールが完了しました。Portal Server の起動と停止については、30 ページの「インストール後の手順」を参照してください。
- インストールを確認するには、ブラウザでサンプルの CSC プログラムを実行します。詳細は、96 ページの「サンプルプログラムを実行する」を参照してください。
- HSM の構成方法については、次節「HSM の構成」を参照してください。

HSM の構成

HSM へは、HSM のベンダーによって提供される PKCS#11 ライブラリを通じてアクセスします。HSM を使用するには、まず HSM を PKCS#11 を使う操作のために適切に構成し、次に iPlanet Portal Server Plug-in を HSM を認識するように構成します。

HSM を構成する

HSM を構成する際は、ベンダーの指示に従う必要があります。ここでは、nCipher HSM を使用する場合の手順について簡単に説明し、ベンダーが提供しているマニュアルの参照先を示します。

nCipher HSM を構成する

- 用語の定義、およびセキュリティワールドとオペレーターカードセットについては、nCipher のマニュアルを参照してください。特に、`http://active.ncipher.com/documentation/PKCS11/solaris-4.01/nforce.pdf` の第 6 章と 7 章が参考になります。
- 通常、nCipher PKCS #11 ライブラリは次の場所にインストールします。

```
/opt/nfast
```

- iPlanet Portal Server Plug-in を使用するには、オペレーターカードセットのうち 1 つが PKCS#11 モードで nCipher HSM を使用している必要があります。また、HSM の各モジュールに対して、それぞれ 1 つのオペレーターカードが必要です。nCipher のマニュアルに示される手順に従って、オペレーターカードセットを作成します。使用するパスワードは、Identrus システムへの iPlanet Portal Server Plug-in で構成したものと同じパスワードにします (34 ページの「管理者のログイン手順」を参照)。
- nCipher ソフトウェアをインストールしたディレクトリ (通常は `/opt/nfast`) に新しいテキストファイル `cknfastrc` を作成し、次の行を追加します。

```
CKNFAST_NO_UNWRAP=1
CKNFAST_LOADSHARING=1
CKNFAST_NO_ACCELERATOR_SLOTS=1

export CKNFAST_NO_UNWRAP CKNFAST_LOADSHARING\
CKNFAST_NO_ACCELERATOR_SLOTS
```

- 次のコマンドを使用して、インストールをチェックします。

```
/opt/nfast/bin/ckcheckinst
```

- このマニュアルでは、ベンダーの PKCS#11 ライブラリについて言及することがあります。PKCS#11 ライブラリとは、次のファイルのことです。

```
/opt/nfast/gcc/lib/libcknfast.so
```

- また、秘密鍵を生成および保存する PKCS#11 トークンの名前は、nCipher PKCS#11 インタフェース用に作成するオペレーターカードセットの名前です。

iPlanet Portal Server Plug-in を構成する

iPlanet Portal Server Plug-in の構成は、次の 2 段階に分けて行います。

- Plug-in PKCS#11 暗号化サービスの HSM ベンダーの PKCS#11 ライブラリを識別する
- 鍵の保管に使用する HSM ベースの PKCS#11 トークン用に iPlanet Portal Server Plug-in を構成する (この作業はインストール作業の一部として行うこともできるが、インストール後でも HSM をインストールできるように、ここでは手作業による操作手順を記載)

ベンダーの PKCS#11 ライブラリを識別する

- ディレクトリを次のディレクトリに変更します。.netscape ディレクトリが存在しない場合は、作成します。

```
<Portal_install_directory>/https-<servername>/config/.netscape
```

- .netscape ディレクトリに secmod.db ファイルが存在しない場合は、次のように作成します。

```
<Portal_install_directory>/bin/https/admin/bin/modutil
  -dbdir . -nocertdb -create
```

- modutil により、secmod.db ではなく secmodule.db が作成された場合は、このファイルを移動します。

```
mv secmodule.db secmod.db
```

- 適切なモジュール名 (nCipher nFast モジュールの場合は nFast) を使用して、ベンダーの PKCS#11 ライブラリを PKCS#11 モジュールのデータベースに追加します。

```
<Portal_install_directory>/bin/https/admin/bin/modutil
  -dbdir . -nocertdb
  -add <moduleName>
  -libfile <vendorPKCS#11Library>
  -mechanisms RSA:DSA
```

- 次のコマンドを使用して、モジュールがインストールされたことを確認します。

```
<Portal_install_directory>/bin/https/admin/bin/modutil
  -dbdir . -nocertdb -list
```

- 出力は次のようになります。

```
Using database directory ....
Listing of PKCS #11 Modules
Listing of PKCS #11 Modules
-----------------------------------------------------------
1.<moduleName>
library name: <vendorPKCS#11Library>
slots: # slots attached
status: loaded
slot: ####-####-####-#
token: <tokenName>
slot: ####-####-####-#
token: <anotherTokenName>
...
2. Netscape Internal PKCS #11 Module
slots: 2 slots attached
status: loaded
slot: Communicator Internal Cryptographic Services Version 4.0
token: Communicator Generic Crypto Svcs
slot: Communicator User Private Key and Certificate Services
token: Communicator Certificate DB
-----------------------------------------------------------
```

PKCS#11 トークンを使用するために iPlanet Portal Server Plug-in を構成する

- iPlanet Portal Server Plug-in のインストール時に PKCS#11 トークンを使用するように指定した場合、適切なトークン名を選択してあれば、特に作業を行う必要はありません。Portal Server Plug-in により、HSM を使用して鍵の生成と保存が行われます。
- iPlanet Portal Server Plug-in のインストール時に特定の PKCS#11 トークンを使用するように指定しなかった場合、または指定したトークン名が誤っている場合は、次の手順に従います。
- 次のディレクトリに移動します。

```
cd <Portal_install_directory>/lib
```

- jssconfig という名前の既存のディレクトリをすべて削除します。

```
rm -rf jssconfig
```

- jssconfig.tar アーカイブを解凍します。

```
tar xvf jssconfig.tar
```

- 次のファイルを編集します。

```
<Portal_install_directory>/lib/jssconfig/trustbase/security/
jsstokenkeystore
```

- このファイル内の key.token プロパティ行を、次のように変更します。

```
key.token=<tokenName>
```

- ほかの行はそのままで、ファイルを保存します。
- iPlanet Portal Server を再起動します。これで、鍵の生成と保存用に、指定した PKCS#11 トークンが使用されるようになります。

インストール後の手順

インストールと HSM の構成が完了したら、Portal Server をいったん終了して、再起動します。Portal Server の起動と停止には、必ず次に示す専用のプラグインスクリプトを使用します。

```
<Portal_install_directory>/SUNWips/bin/SUNWpinStart
<Portal_install_directory>/SUNWips/bin/SUNWpinStop
```

注 このスクリプトでは、ゲートウェイは起動しません。ゲートウェイを起動するには、次のコマンドを使用します。

```
<Portal_install_directory>/SUNWips/bin/ipsgateway start
<Portal_install_directory>/SUNWips/bin/ipsgateway stop
```

ただし、Portal ゲートウェイの起動と停止については、Portal Server のマニュアルを参照してください。

```
http://docs.iplanet.com/docs/manuals/portal/30/install/server_i.htm
```

ソフトウェアのアンインストール

Portal Server はインストールしたまま、Identrus システムへの iPlanet Portal Server Plug-in を削除するには、次の手順に従います。

- Portal Server が稼動していることを確認します。
- ルートとしてログインします。
- 次のコマンドを実行します。

```
pkgrm SUNWpinsdskss
```

- Portal Server を停止して、再起動します。方法については、Portal Server のマニュアルを参照してください。

iPlanet Portal Server を削除する方法については、次のサイトを参照してください。

```
http://docs.iplanet.com/docs/manuals/portal/30/install
```

第 2 章

管理

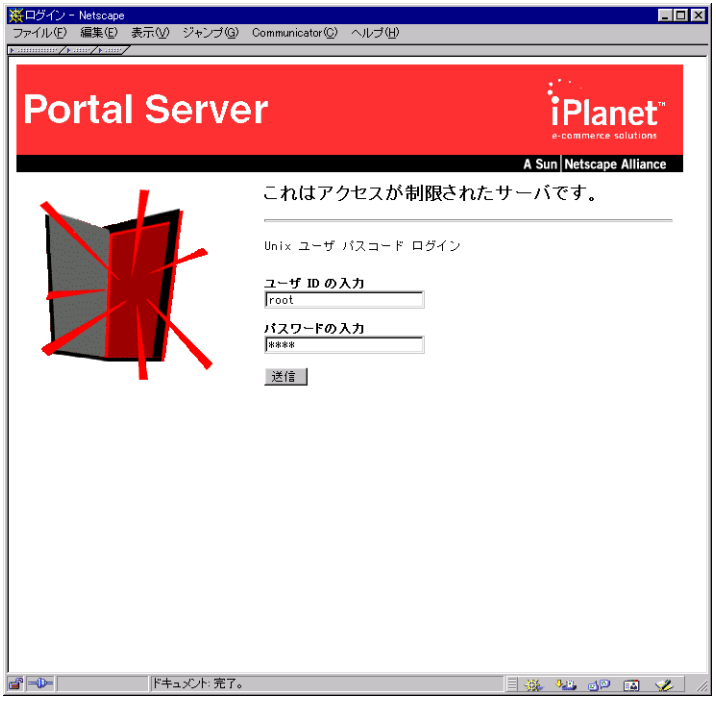
Identrus システムへの iPlanet Portal Server Plug-in の管理作業の一環として、Identrus のメンバーユーザを認証および認可するための、適切な証明書を設定する必要があります。この章には、次の項目があります。

- 管理者のログイン手順
- Identrus 証明書を生成する
- ログインの承認
- Netmail の構成
- CSC の構成
- RC ホストの構成
- 証明書ステータス
- SSL コミュニケーション
- ログ

管理者のログイン手順

- ブラウザで Portal Server の URL を選択します。通常、この URL は http://<machine name>:<port>/console になります (例 : http://firestorm.jcp.co.uk:8080/console)。

図 2-1 管理者のログイン画面

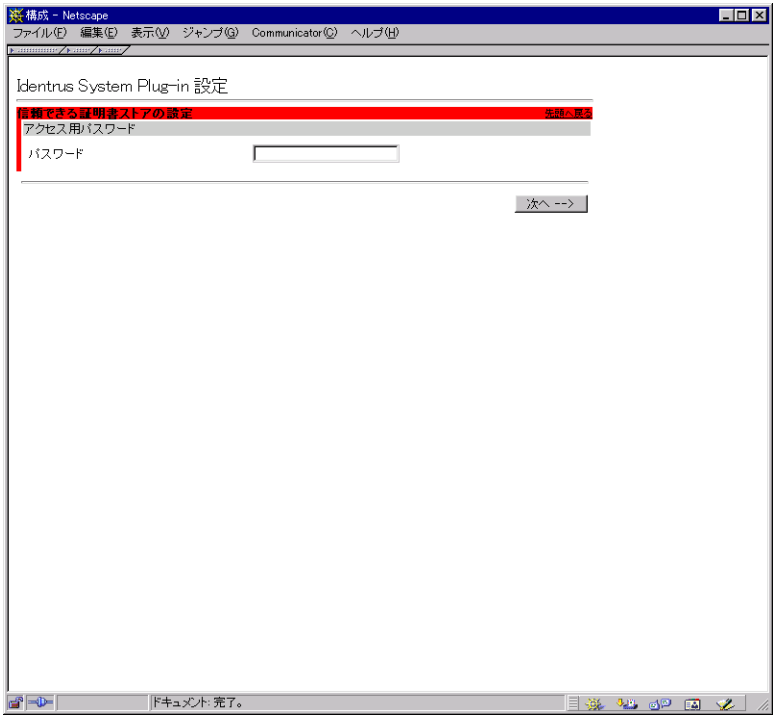


- 管理者のアカウントにログインすると、次の画面が表示されます。

図 2-2 管理メインメニュー

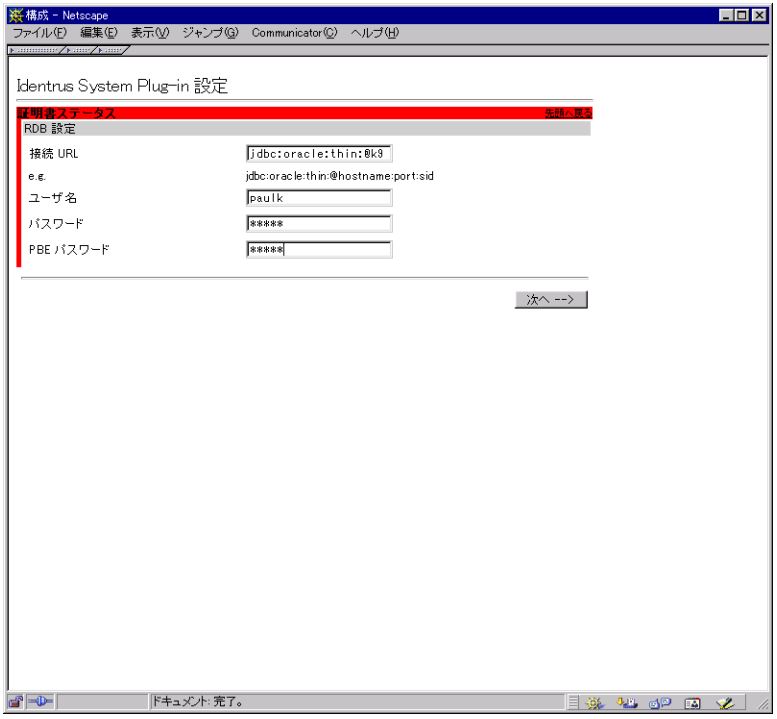
- 「Manage Identrus Plug-in」を選択します。このリンクを初めて選択した場合には、信頼できる証明書ストアのパスワードを入力するための画面が表示されます。証明書ストアへのアクセスに使用するパスワードを入力します。このパスワードは、PKCS11 トークンのパスワードと同じにします (25 ページの「HSM の構成」を参照)。これは、外部 HSM を使用している場合にのみ該当します。

図 2-3 証明書ストアのパスワード



- 「次へ」を選択します。RDB を次のように設定します。

図 2-4 RDB 設定



- 次の設定は必須です。
  - 接続 URL : Oracle データベースの場所
  - ユーザ名 : Oracle フレームワークデータベースへのアクセスに使用するユーザ名
  - パスワード : Oracle フレームワークデータベースへのアクセスに使用するパスワード
  - PBE パスワード : Oracle データベース内で動作する証明書ストア内にある暗号化されたデータへのアクセスに使用するパスワード
- 入力し終えたら、「次へ」を選択します。

- これ以降、「Manage Identrus Plug-in」を選択すると次のメニューが表示されるようになります。

図 2-5 Identrus システムへの iPlanet Portal Server Plug-in メインメニューのオプション

まず、証明書を入手するためのさまざまな手続きを紹介し、次のオプションについて順番に説明します。

- Generate Identrus Certificate : 確認の必要な証明書用
- ログイン認可、Netmail : システムを使用できるユーザ、および各ユーザの権限を決定
- CSC の構成、RC ホスト、証明書ステータス
- SSL コミュニケーション : トランスポートの認証を可能にする

注 すべての構成オプションを順番に検討し、適切なオプションを選択します。選択が終了したら画面右下に向かってスクロールし、保存 をクリックして選択を有効にします。

Identrus 証明書を生成する

次の証明書は署名用に使用され、変更されることを防ぎ、変更された電子メールメッセージが使用されることを防ぎます。このため、これらの証明書には、Identrus システムからの PKCS10 リクエストと、CA からの PKCS7 レスポンスが必要です。

- リクエスト署名証明書
- レスポンス署名証明書
- SSL クライアント証明書 : ハンドシェイクリクエストに署名

その他の証明書は確認 / 検証のために必要で、認証や認可を可能にします。これらの証明書は CA から直接入手します。

- 信頼できるログイン CA 証明書
- 信頼できる電子メール証明書
- 信頼できるレスポンス確認証明書

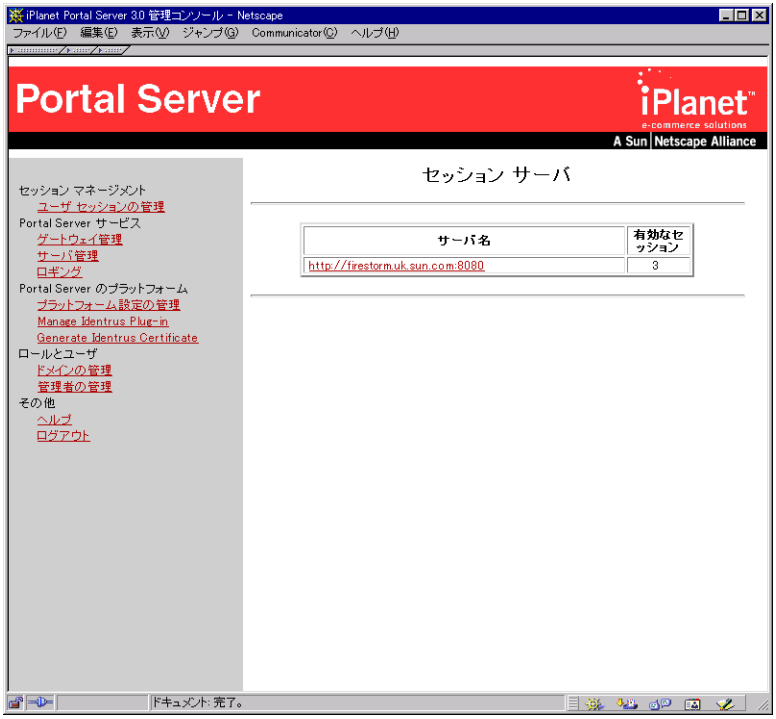
注 CA により指定される手続きは、CA のセキュリティポリシーによって異なります。確かでない場合は、CA のオペレータに証明書の処理を依頼してください。

認証および認可用に証明書を追加する

この場合、PKCS10 リクエストは必要ありません。次の手順に従います。

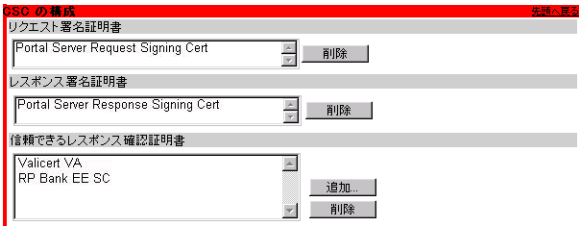
- iPlanet Portal Server のメイン画面で「Manage Identrus Plug-in」を選択します。

図 2-6 Portal 管理者のメイン画面



- 「CSC の構成」を選択し、たとえば次の図の「信頼できるレスポンス確認証明書」で「追加」を選択します。

図 2-7 CSC の構成



- 証明書は、CA から直接入手した証明書を貼り付けることによって追加できます。

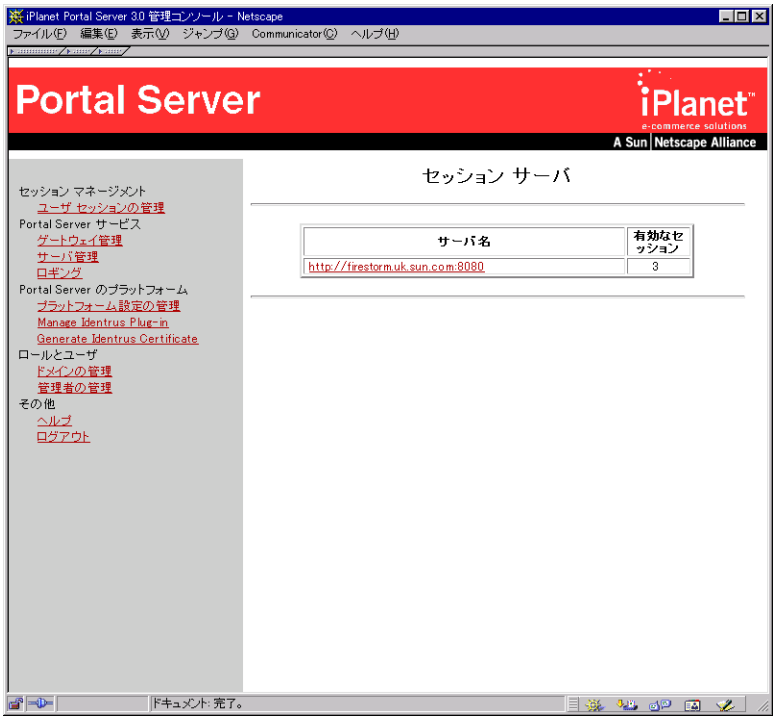
図 2-8 Identrus システムへの iPlanet Portal Server Plug-in に base64 エンコードの証明書を貼り付ける

署名用に証明書を追加する

ここでは、主に 2 つの段階に分けて作業を行います。まず Identrus システムからの PKCS 10 リクエストを使用して署名リクエストを生成し、次に CA から PKCS 7 レスポンスを入手します。

- メインメニューから「Generate Identrus Certificate」を選択します。

図 2-9 Portal 管理者のメイン画面



- 証明書に関する次の情報を指定します。

図 2-10 PKCS#10 証明書リクエストを生成する

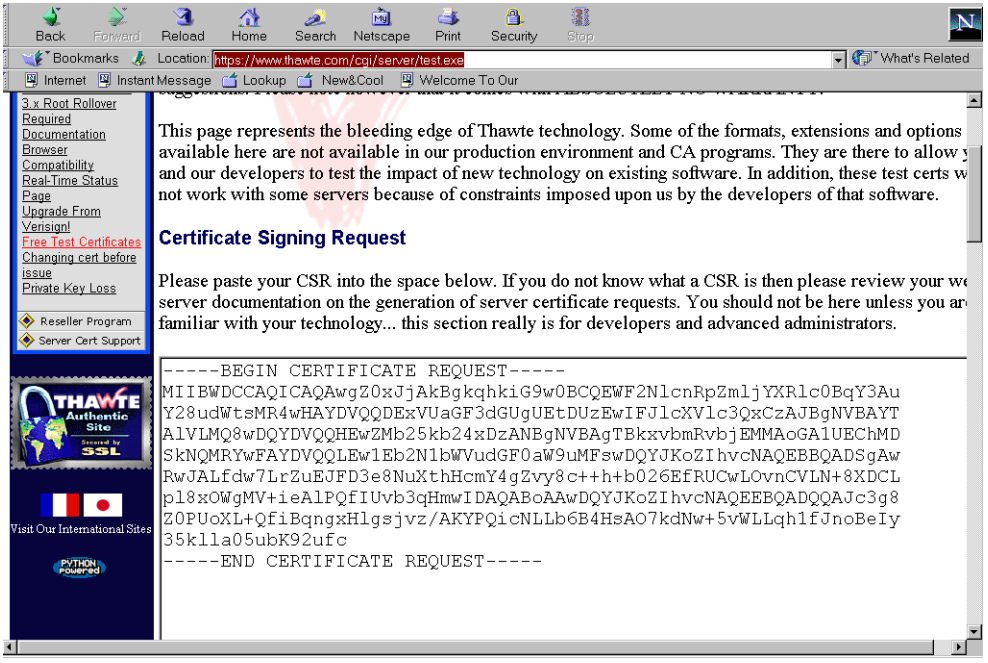
- 鍵の長さ : 512 ビットまたは 1024 ビットから選択
- 共通名 : 証明書に付ける名前 (例 : Portal SSL Certificate)
- 組織単位 : ユーザ / エンティティが所属する組織内の部署
- 組織 : ユーザが作成する証明書の所属先 (例 : iPlanet)
- 国 : ユーザが所在する国。ISO3611 標準 (`http://www.iso.ch`) および X500 標準 (`http://www.itu.int/itudoc/itu-t/rec/x/x500up/x500.html`) によって定義された国名コードに基づく

- 生成 を選択することによって、証明書リクエストを生成します。このリクエストは、base64 でエンコードされた PKCS 10 リクエストです。

図 2-11 PKCS10 リクエストをコピーする

- CA の Web サイトにアクセスし、サーバ証明書の作成に関する説明を参照しながら、PKCS10 リクエストを貼り付けるところまで作業を進めます。

図 2-12 PKCS10 リクエストを CA の Web サイトに貼り付ける



- 切り取りおよび貼り付けることによって、該当する base64 エンコードの証明書レスポンスを収集します。証明書をコピーおよび貼り付ける際には、Ctrl + C キーおよび Ctrl + V キーを使用します。

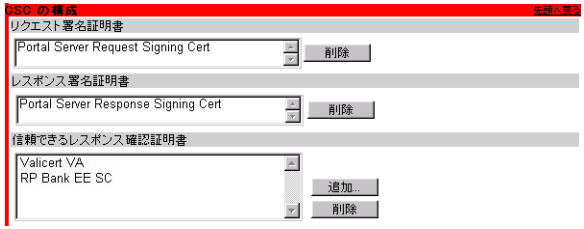
図 2-13 CA からの base64 エンコードの証明書レスポンスをコピーする


```
Here is your certificate:


-----BEGIN CERTIFICATE-----
MIICVzCCAcCgAwIBAgIDdqdHMA0GCSqGSIb3DQEBBAUAMIGHMQswCQYDVQQGEwJa
QTEiMCAGA1UECBMZRk9SIFRFU1RJTkcgUFVSUE9TRVMgT05MWTEdMBsGA1UEChMU
VGhhd3RlIENlcnRpZmljYXRpb24xFzAVBgNVBAsTDlRFU1QgVEVTVCBURVNUMRww
GgYDVQQDExNUaGF3dGUgVGVzdCBDQSBSb290MB4XDTk5MDUyODEyNDgxNloXDTk5
MDYyODEyNDgxNlowgZ0xJjAkBgkqhkiG9w0BCQEWF2NlcnRpZmljYXRlc0BqY3Au
Y28udWtsMR4wHAYDVQQDExVUaGF3dGUgUEtDUzEwIFJlcXVlc3QxCzAJBgNVBAYT
AlVLMQ8wDQYDVQQHEwZMb25kb24xDzANBgNVBAgTBkxvbmRvbjEMMAoGA1UEChMD
SkNQMRYwFAYDVQQLEw1Eb2N1bWVudGF0aW9uMFswDQYJKoZIhvcNAQEBBQADSgAw
RwJALfdw7LrZuEJFD3e8NuXthHcmY4gZvy8c++h+b026EfRUCwLOvnCVLN+8XDCL
pl8xOWgMV+ieAlPQfIUvb3qHmwIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAKJWhyf7
m0sE4YXeHu0F+BzdT8SQ5/tyesw5JiCK28hDH1VkEDUK+MdbDSB/opKhq8RwczJH
pdS6k4Uz8kukkeI59VdTlWwIGItZBn4+6Rscs8t6BiUAGOiBVcXv3Hk9h9rTHaEF
K44C6B4N3oV1aT6AlbcTvLMHD5vezQM+IkQX
-----END CERTIFICATE-----
```

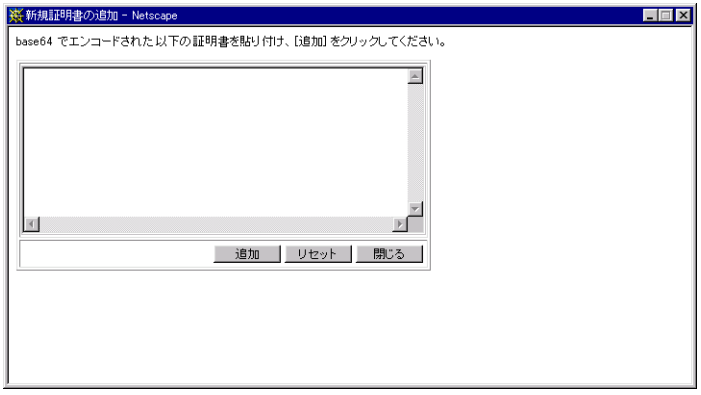
- iPlanet Portal Server のメイン画面で「Manage Identrus Plug-in」を選択します。
- 「CSC の構成」を選択します。
- 「追加」を選択します (次の図を参照)。

図 2-14 CSC の構成



- 証明書は、結果として返される base64 エンコードの PKCS 7 レスポンスを貼り付けることによって追加できます。

図 2-15 base64 エンコードの証明書レスポンスを貼り付ける



- 「追加」を選択します。

証明書を削除する

証明書は削除することもできます。この場合、ユーザは確認済みのメッセージを送信できなくなります。

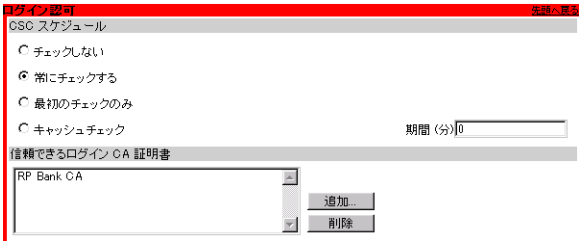
注 証明書のインストール方法について疑問がある場合は、現地の製品サポートの担当者に問い合わせてください。

ログインの承認

このオプションでは、ユーザがログインする際に、ユーザに対してどのようなセキュリティ対策を適用するかを設定できます。次のような設定が可能です。

- ログイン時に証明書ステータスをチェックしない
- ログイン時に常に証明書ステータスをチェックする
- 最初のログイン時のみに証明書ステータスをチェックする
- 証明書ステータスチェックの結果が良好であれば、そのステータスを指定の期間 (分) キャッシュに保存する : キャッシュ期間中に同じユーザが再度ログインすると、最初のログイン時にリクエストされたステータスが使用される。ただし、良好でないレスポンス (無効 / 不明など) はキャッシュに保存されない

図 2-16 ログイン認可の主なオプション



RP (Relying Participant) の銀行の証明書をここで入力します。この Identrus のメンバーである銀行のすべての顧客が、Portal Server にログインできます。信頼できる証明書は、必要に応じて追加および削除できます。この構成インタフェースには、1 つまたは複数の base64 エンコードの証明書を貼り付けることができます。ログイン時に提示されたアイデンティティ証明書をこのスキーマの一部として認識するためには、これらの証明書の 1 つが証明書チェーンに含まれていることが必要です。

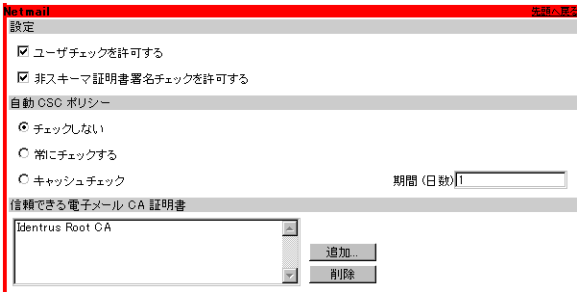
注 この証明書を入手するには、CA の管理者に連絡してください。Identrus メンバーであれば、CA の管理者が必要な Identrus ルート証明書と RP 証明書を所有しているはずです。証明書のインストール方法について疑問がある場合は、現地の製品サポート担当者に問い合わせてください。また、40 ページの「認証および認可用に証明書を追加する」も参照してください。

Netmail の構成

請求書発行の観点から、証明書ステータスを自動または手作業で確認するかどうかを決定する際にはいくつかのケースが考えられます。ほとんどのユーザの身元がわかっている場合には、証明書ステータスのチェックは必要ないこともあります。次の 3 つのオプションがあります。

- 自動的に CSC チェックを実行する
- 手作業によるユーザチェックを許可する
- 非スキーマ証明書署名チェックを許可する：このオプションを選択すると、非スキーマ署名がチェックされ、該当するアイコンが表示される。選択しないと、非スキーマ証明書によって署名されたメッセージの署名チェックは行われない

図 2-17 Netmail の構成オプション



Identrus ルート証明書をここで入力します。Identrus メンバーから送信されたすべての電子メールを確認できます。この構成インタフェースには、その他の base64 エンコードの証明書を貼り付けることもできます。電子メール署名証明書をこのスキーマの一部として認識するには、これらの証明書の 1 つが証明書チェーンに含まれていることが必要です。

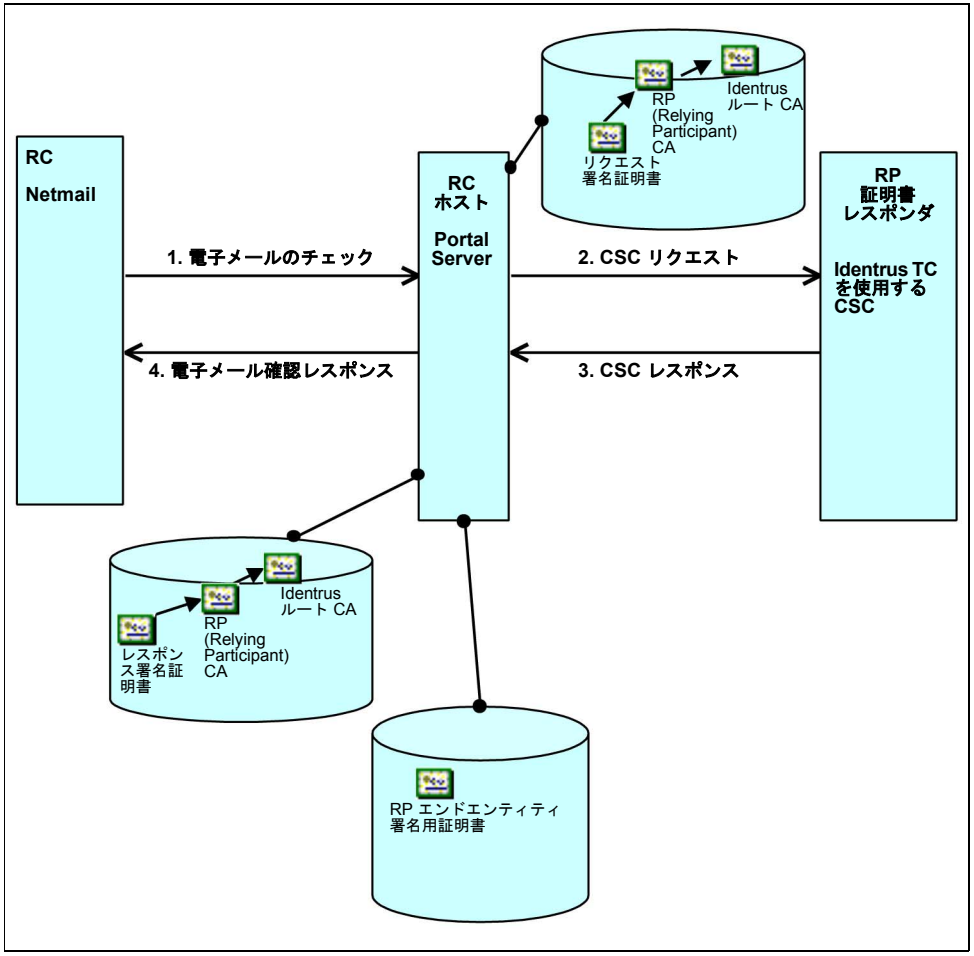
この証明書を入手するには、CA の管理者に連絡してください。Identrus メンバーであれば、CA の管理者が必要な Identrus ルート証明書と RP 証明書を所有しているはずです。

注 証明書のインストール方法について疑問がある場合は、現地の製品サポートの担当者に問い合わせてください。また、40 ページの「認証および認可用に証明書を追加する」も参照してください。

CSC の構成

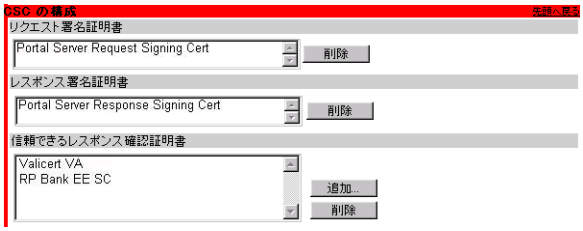
証明書ステータスチェックにより、任意の Identrus メンバーの証明書ステータスを確認することが可能になります。OCSP レスポンダ または Identrus CSC レスポンダが、ローカルのレスポンダに連絡してリクエストにレスポンスする (この組織が証明書を発行した場合) か、証明書を発行した組織のレスポンダにリクエストを転送します。

図 2-18 メッセージの生成および確認に必要な証明書を示す Identrus CSC の例



リクエスト / レスポンス証明書を追加する前に、ルート証明書および対応する CA チェックが構成されていることを確認する必要があります。証明書が個別の base64 エンコード証明書である場合は、ルートを追加して CA に置換し、さらに対応するリクエストとレスポンスの証明書に再度置換することをお勧めします。これにより、ルート /CA/ リクエスト証明書またはレスポンス証明書の完全なチェーンが構成されます。

図 2-19 CSC の構成



ユーザが証明書ステータスのチェックを実行できるようにするには、次の証明書の構成が必要です。

- リクエスト署名証明書 : CSC リクエスト (RC ホストから RP へ送信) の署名鍵は、ハードウェアセキュリティモジュール (HSM) に保持される。鍵の署名を含むすべての秘密鍵に関する処理は、HSM で行われる。この証明書の入手方法については、42 ページの「署名用に証明書を追加する」を参照
- レスポンス署名証明書 : CSC レスポンス (RC ホストから RP へ送信) の署名鍵は、ハードウェアセキュリティモジュール (HSM) に保持される。鍵の署名を含むすべての秘密鍵に関する処理は、HSM で行われる。この証明書の入手方法については、42 ページの「署名用に証明書を追加する」を参照
- 信頼できるレスポンス確認証明書 : 構成インタフェースには、1 つまたは複数の base64 エンコードの証明書を貼り付けることが可能。OCSP レスポンダまたは CSC レスポンダを信頼するには、これらの証明書の 1 つがレスポンダの証明書チェーンに含まれていることが必要 (40 ページの「認証および認可用に証明書を追加する」を参照)。これは、OCSP レスポンダの役割を果たす CA の場合 (VA 証明書) と、Identrus における RP エンドエンティティ署名用証明書 (図 2-19 を参照) の場合がある

注 証明書のインストール方法について疑問がある場合は、現地の製品サポート担当者に問い合わせてください。証明書を追加するには、まず適切な機関から証明書を入手する必要があります。入手方法については、39 ページの「Identrus 証明書を生成する」を参照してください。

RC ホストの構成

次の RC (Relying Customer) 設定が必要です。

- レスポンダタイプ : OCSP (OCSP レスポンダを使用する場合) または Identrus 証明書ステータスチェック (Identrus が完全に実装されている場合) を選択
- レスポンダの URL : https://hailstorm.uk.sun.com:8080 など
- OCSP リクエスタ名 : 署名の際に必要な、OCSP リクエスト元であるエンティティの名前 (通常は URL)

図 2-20 RC ホストの構成

証明書ステータス

これらの設定により、システムが定義され、システム全体のために証明書ステータスチェックを行えるかどうかが決定されます。また、Identrus システムへの iPlanet Portal Server Plug-in で使用されるデータベース接続情報もここで定義されます。管理者がシステムで実行された証明書ステータスチェックを確認するには、監視ログを使用します。詳細は、54 ページの「ログ」を参照してください。

- 「証明書ステータスのチェックを有効にする」をオンにします。

図　2-21　　証明書ステータスの構成

次の設定は必須です。

- 接続 URL : Oracle データベースの場所
- ユーザ名 : Oracle フレームワークデータベースへのアクセスに使用するユーザ名
- パスワード : Oracle フレームワークデータベースへのアクセスに使用するパスワード
- PBE パスワード : Oracle データベース内で動作する証明書ストア内にある暗号化されたデータへのアクセスに使用するパスワード

SSL コミュニケーション

証明書は、SSL ハンドシェイクを行う際に、トランスポート層で必要になります。次の証明書が必要です。

- クライアント証明書 : Portal Server に導入される証明書。署名が必要。この証明書の入手方法については、42 ページの「署名用に証明書を追加する」を参照

図 2-22 SSL コミュニケーションの構成

この証明書を入手するには、CA の管理者に連絡してください。Identrus メンバーであれば、CA の管理者が必要な Identrus ルート証明書と RP 証明書を所有しているはずです。

ログ

構成

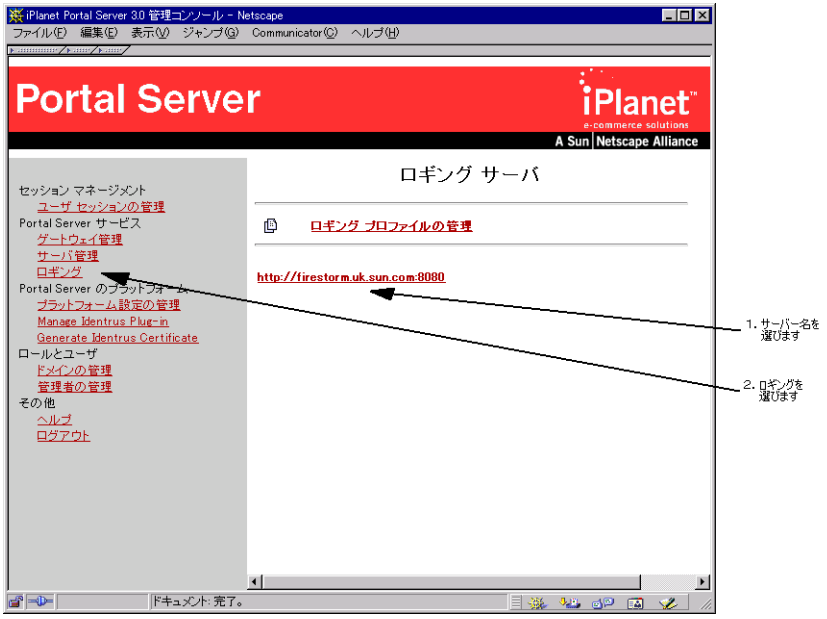
ログは、有効または無効にすることができます。ログが無効の場合、新しいエントリが記録されることはありません。

図　2-23　　ログを構成する

表示

メインメニューから「ロギング」を選択すると、ログのさまざまな面を表示できます。

図　2-24　　ロギングメインメニュー



- 自分のサーバ名 (例 : `firestorm.uk.sun.com:8080`) を選択することによって、さまざまなエラーログを表示できます。

- 「readExceedsMax」エラーのメッセージが表示された場合は、ログファイルが大きいために画面に表示できません。ただし、この場合でもファイルを見ることは可能です。ファイルは Portal デフォルトログディレクトリにあります。

```
/var/opt/SUNWips/logs
```

図 2-25 サーバログファイルの例

必要に応じて特定のログファイルを削除するオプションもあります。これらのログファイルについて説明します。

- iwtAuthentication ： 成功か失敗かにはかかわらず、すべてのログオンの試みを記録。ログオンに失敗した場合は、理由が記録される
- iwtGateway : 標準的な Portal Server ログの一部。詳細は、Portal Server の管理者用マニュアルを参照
- iwtAdmin : 標準的な Portal Server ログの一部。詳細は、Portal Server の管理者用マニュアルを参照
- iacMessageLog ： システムで送受信されたすべての証明書ステータスチェックのメッセージを記録。次の情報が含まれる
  - RC から受信した CSC リクエスト
  - RP に送信された CSC リクエスト

- RP から受信した CSC レスポンス
- RC に送信された CSC レスポンス

- ログレコードに含まれるフィールド
  - 原初メッセージ - 常にタイムスタンプが付けられ、RC、RC ホスト、または CSC レスポンダによって署名される
  - リクエストしているユーザ - これにより、プロファイル時にリクエスタ当たりのリクエストの量とタイプを判別することが可能
  - SC 証明書チェーン
  - 日時 - 秒単位で四捨五入して記録される。タイムスタンプの形式は「YYYMMDDhhmmss」
  - レスポンダの URL - システムのレスポンダの URL は現時点では固定されているが、将来、複数のレスポンダのサポートが必要となった場合や、URL が変更された時などに備えて記録される
  - レスポンスステータス - 成功、失敗 (トランザクションの失敗の原因である、特定の業務要件によるエラー、または技術的エラーも記録)、タイムアウトなど
  - 証明書ステータス - 有効、取り消し済み、または不明
  - トランザクション ID
  - 完全なレスポンスメッセージ
  - リクエストのコンテキスト - 現時点ではメールチェックとログイン
- iacMessageLog-1 : ログファイルのサイズが大きくなった場合、そのファイルの名前は変更され、新しいログファイルが作成される。これは iacMessageLog の変更後の名前
- iwtNetMail : NetMail ログの一部。詳細は、Portal Server の管理者用マニュアルを参照
- iacAppLog : 業務要件によるエラー、技術的エラー、実装上のエラーなど、すべてのエラーを記録。ログエントリには、次のものがある
  - 日時 - 秒単位で四捨五入して記録される。タイムスタンプの形式は「YYYMMDDhhmmss」
  - エラーの原因となったソースコードの行を示す、固有の識別子
  - エラーの説明
  - 該当する場合、エラーに関するデータ (接続時のホスト名エラーなど)
  - エラーによっては、Java 例外の呼び出しスタックが含まれる場合もある

注　場合によっては、より詳細な情報が必要なこともあります。このような場合、これらのログは `/var/opt/SUNWips/logs` ディレクトリにテキストファイルとしても保存されます。

第 3 章

ユーザ

デジタル証明書の設定が終わったら、Identrus システムへの iPlanet Portal Server Plug-in を使用する準備は完了です。NetMail Lite を使用すると、問題なく送信するメッセージにデジタル署名を行ったり、受信するメッセージの完全性や信頼性をチェックしたりすることができます。この章では、これらの操作を行うための、次のような機能について説明します。

- スマートカードを使用したログイン
- メッセージ確認の概要
- 電子メール署名の例
- 取り消し済みのメッセージ
- 無効な署名
- 証明書ステータスログ

スマートカードを使用したログイン

- ブラウザで、Portal Server にアクセスする URL (例 : `https://firestorm.uksun.com:8080`) を入力します。

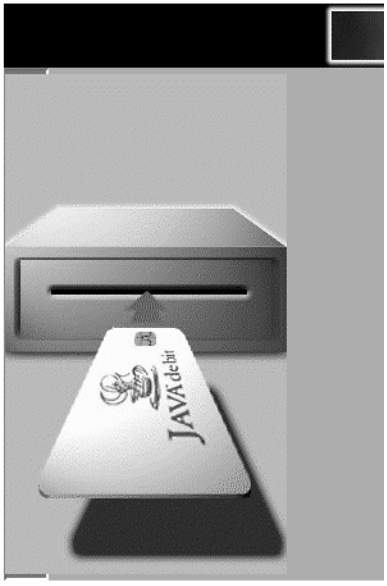
図 3-1 ログインメインメニュー

- 「SmartCardUser」を選択します。

図 3-2 スマートカードを挿入する

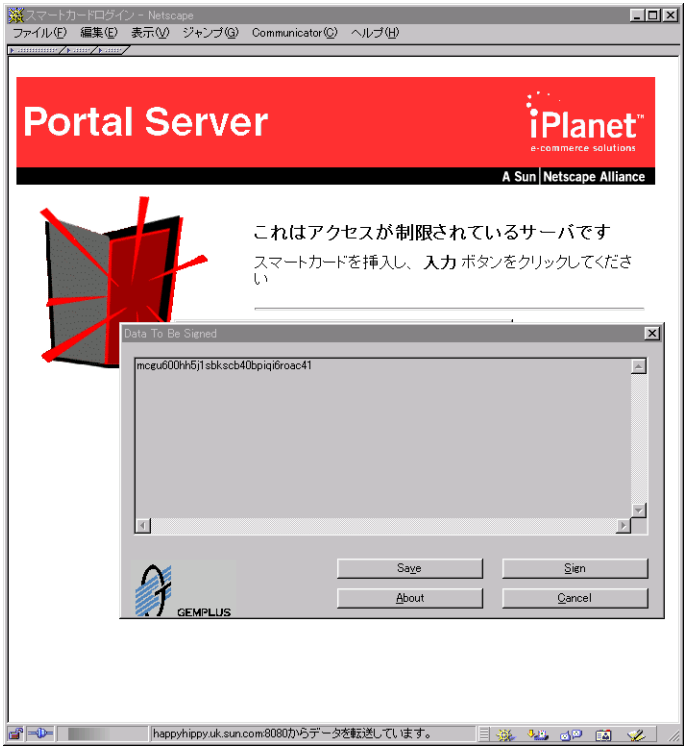
- スマートカードをカードリーダに挿入します。

図 3-3 スマートカードをカードリーダに挿入する



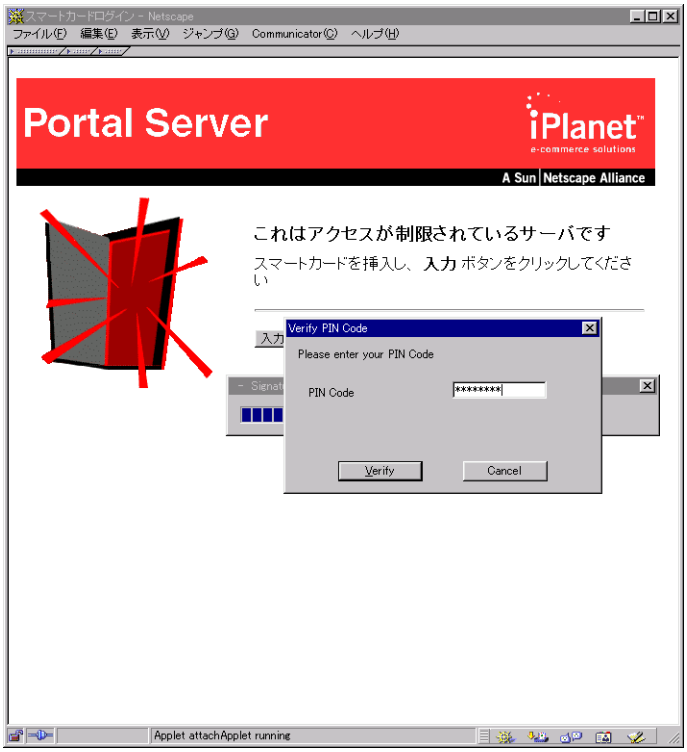
- 「入力」ボタンをクリックすると、ダイアログボックスが表示され、スマートカードの PIN を入力するよう求められます。

図 3-4 スマートカードエントリに署名する



- 「Sign」を選択します。

図　3-5　　スマートカードの PIN を入力する

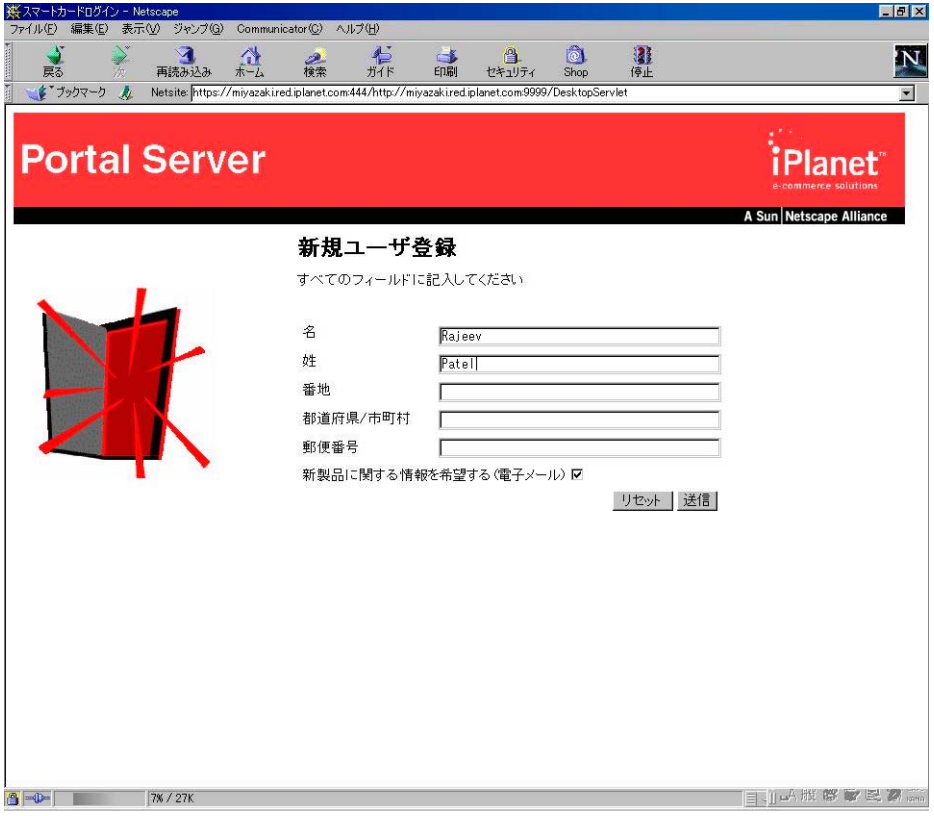


- PIN を入力して「Verify」をクリックすると、情報がサーバに送られます。次の場合には、アクセスが拒否され、対応するメッセージが表示されます。
- スマートカードがリーダに挿入されていない
- 入力したスマートカードの PIN が誤っている
- スマートカードの証明書チェーンが無効
- スマートカードの証明書チェーンに信頼できる CA 証明書が含まれていない
- スマートカードの証明書のステータスが「不明」である。つまり、スマートカードが「スキーマ」の一部ではない
- スマートカード証明書のステータスが「取り消し済み」である

注　　PIN 番号は、スマートカード発行時にスマートカードのサードパーティベンダーから通知されます。

- スマートカードのログインページで「入力」をクリックすると、ログインモジュールによりユーザの個人情報がチェックされ、信頼性が確認されます。次に、ユーザプロファイルが画面に表示されます。システムに初めてログインする場合は、新規ユーザ登録ページが表示されます。このページを送信すると、モジュールにより新規ユーザが作成および追加されます。

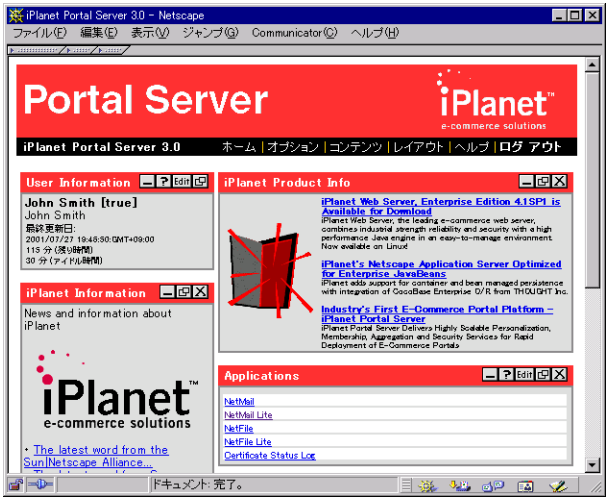
図 3-6 新規ユーザ登録



- 個人情報を入力したら、「送信」をクリックします。Portal Server のメインメニューが開きます。

- 管理者によって構成されたセキュリティポリシーに基づいて、サーバが証明書ステータスチェックを実行します。採用されている証明書ステータスチェックのポリシーに関係なく、クライアントからの署名付きレスポンスの有効性が常に確認されます。また、署名証明書は一般に認められたソースによって発行されたものでなくてはなりません。

図 3-7 Portal Server メインメニュー画面



- 最後に「NetMail Lite」をクリックします。

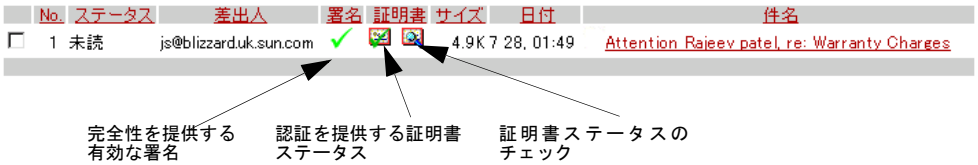
メッセージ確認の概要

電子メールメッセージを確認するには、次の 2 つのオプションがあります。

- 認証を提供する証明書を表示する
- 完全性を提供する署名を表示する

証明書を表示する

図　3-8　　NetMail Lite メッセージヘッダーの例

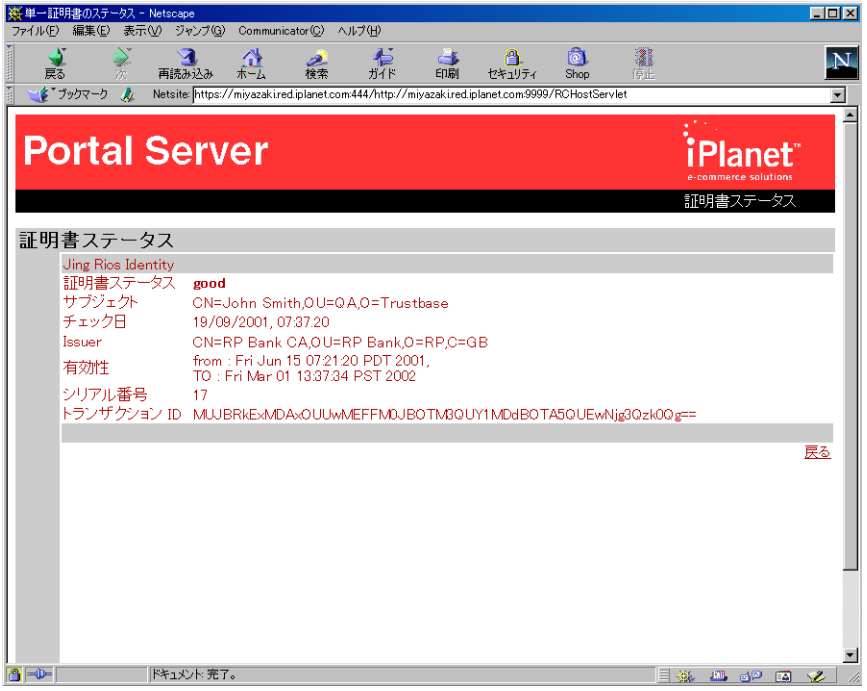


証明書のステータスが、次に示すステータス 1 または 2 以外の場合は、証明書ステータスのアイコン をクリックすると最新のステータスチェックの詳細が表示されます。システムがメッセージ受信時に自動的にステータスチェックを行うように構成されている場合、ステータス 2 が発生することはありません。証明書には、次の 5 種類のステータスがあります。

- ステータス 1 : メッセージがスキーマ証明書によって署名されていない (アイコンなし)
- ステータス 2 : 署名証明書が未チェック (アイコンなし)
- ステータス 3 : 証明書が取り消し済み
- ステータス 4 : 証明書が確認済み
- ステータス 5 : 証明書が不明 、またはステータスの取得中にエラーが発生

証明書ステータスチェックを開始するには、証明書チェックのアイコン  をクリックします。このアイコンをクリックすると、証明書ステータスチェックのリクエストを送信するという旨のメッセージが表示され、ユーザの銀行にこのサービスの手数料が請求されます。リクエストを確認するには、スマートカードを挿入して、PIN を入力する必要があります。PIN を入力して「OK」をクリックすると、署名付きの証明書ステータスチェックのリクエストが Portal Server に送信されます。数秒後、レスポンスが受信されると、証明書ステータスのページが表示されます。

図　3-9　　証明書ステータスチェックの例



RC ホストでは、レスポンス署名証明書 (構成方法については 51 ページの「RC ホストの構成」を参照) を使用して、ステータス情報を表示する HTML ソースが署名され、署名は証明書ステータスページの HTML の一部として base64 エンコードの隠しデータの形態で送信されます。ユーザは、請求書確認などの目的でこの情報が必要になる場合に備え、この HTML ページをローカルディスクに保存することができます。

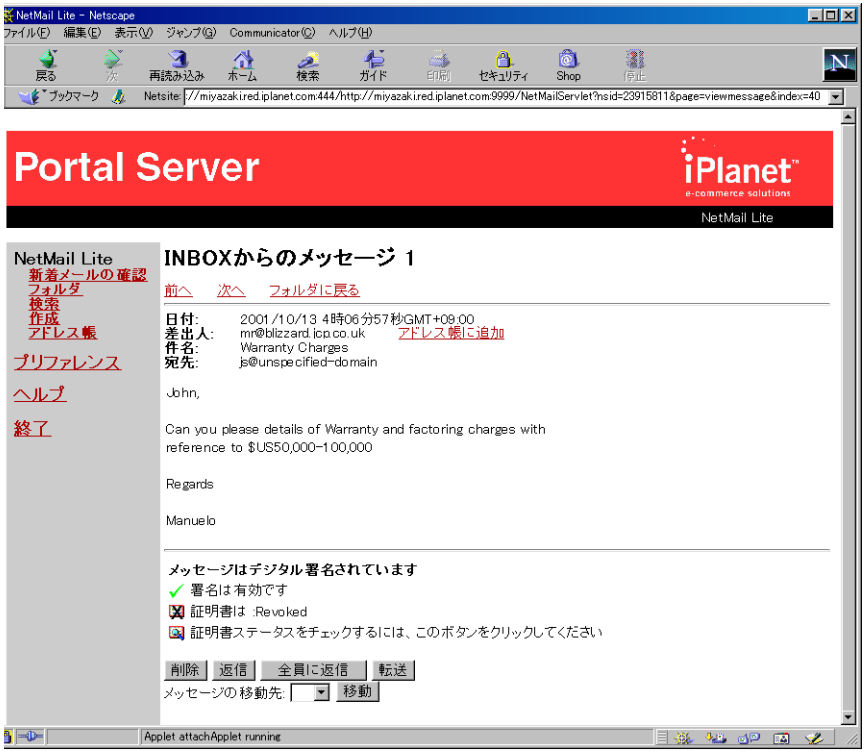
署名を表示する

メッセージには、次の 3 種類のステータスがあります。

- ステータス 1 : 未署名 (アイコンなし)
- ステータス 2 : 署名が無効 X
- ステータス 3 : 署名が有効 ✓

署名の有効性は、証明書ステータスには依存しません。スキーマに属する証明書によって署名されたメッセージの場合は、署名の有効性を示すアイコンが常に表示されます。また、システムは、スキーマに属さない証明書によって署名されたメッセージに対しても、署名の有効性を示すアイコン ✓ を表示するように構成されている場合もあります。

図 3-10 署名の詳細を選択する



署名の詳細ページには、署名および署名証明書の詳細が表示されます。このページを表示するには、メッセージヘッダーのページまたはメッセージのページで、署名の有効性を示すアイコン ✓ をクリックします。✓ アイコンをクリックすると、署名の詳細ページに次の情報が表示されます。

- サブジェクト : 証明書の保持者の識別名
- 発行元 : 証明書の発行元の識別名
- 有効性 : 証明書の有効期限の最初と最後の日
- シリアル番号 : 証明書のシリアル番号
- 署名ステータス :「有効」または「無効」。次のような情報も示される
  - 署名後にメッセージの内容が変更されていないか
  - 署名証明書の有効期限が切れていないか
  - 署名証明書がスキーマのメンバーであるか

図 3-11 署名を表示する

いったんチェックされた後は、証明書は有効なものとして認識されます。ただし、証明書ステータスチェックの数日後に証明書の期限が切れる場合、メッセージの証明書ステータスが有効であるかどうかを確認するために、再度証明書ステータスチェックを実行できます。

電子メール署名の例

次の 4 人のユーザが存在すると仮定し、電子メールメッセージの例を見てみましょう。最初の 3 人のユーザは、有効な証明書を持っています。4 人目のユーザの証明書は取り消し済みで、Identrus スキーマ外で署名されたメッセージを送信しようとしています。

- John Smith (証明書は有効)
- Tom Jones (証明書は有効)
- Rajeev Patel (証明書は有効)
- Manuelo Revoka (証明書は取り消し済み、無効な署名を送信)

Identrus システムへの iPlanet Portal Server Plug-in では、次の機能がサポートされています。

- 署名付きメッセージの作成
- 署名付きメッセージの転送
- 送信者のメッセージに対し、証明書ステータスのリクエストを実行
- 署名付きメッセージの受信
- 署名付きメッセージのステータスの表示
- 取り消し済み証明書の表示
- Identrus スキーマ外の無効な署名の表示

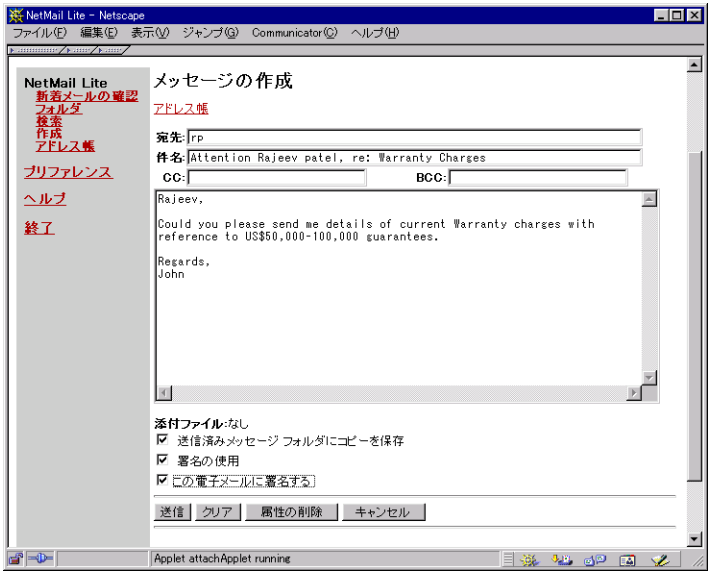
これらの機能を順番に説明します。

署名付きメッセージを作成する

デジタル署名を付けてメッセージを送信すると、受信者に対してメッセージの完全性を提供することができます。

- John Smith が NetMail Lite にログオンし、Rajeev Patel にメッセージを送信するとしましょう。John Smith は、「この電子メールに署名する」を選択することによって、メッセージに署名しています。

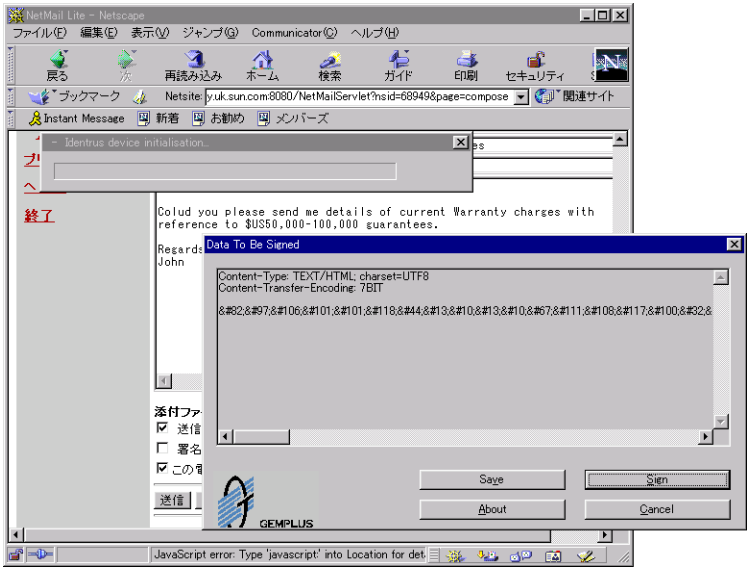
図 3-12 メッセージを作成する



- Identrus システムへの iPlanet Portal Server Plug-in では、署名付きメッセージを作成する際に、次のオプションを選択できます。
  - 送信済みメッセージフォルダにコピーを保存 : メッセージのコピーを保存する
  - 署名の使用 : 文書の最後に、署名のテキストを追加する。このテキストファイルへのリンクを確立するには「プリファレンス」を選択
  - この電子メールに署名する : メッセージにデジタル署名する。これにより、受信者が、送信者が本人であるか、およびメッセージが変更されていないかどうかを確認することができる

- メッセージの送信後、メッセージにどのように署名するかの確認を求められます。「Sign」を選択し、前と同様にスマートカードの PIN 番号を入力します。スマートカードリーダにスマートカードが挿入されていることを確認してください。

図 3-13 メッセージにデジタル署名する



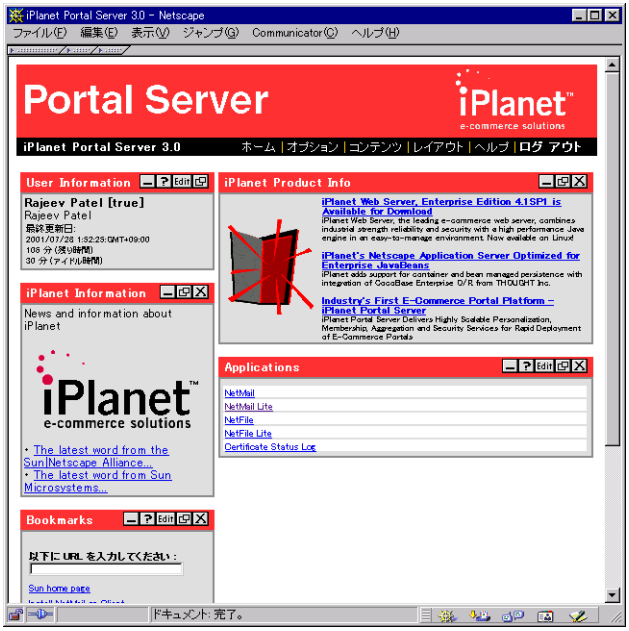
署名付きメッセージを受信する

メッセージヘッダーには、どのメッセージがデジタル署名されているかが示されます。また、受信メッセージの送信者を確認したい場合のために、証明書ステータスチェックの必要なメッセージが示されます。これには次の 2 つの目的があります。

- メッセージの受信者が送信者を確認できる：  アイコンをクリックすると、システムに証明書ステータスチェックのリクエストが送信される。この機能は、自動的に設定することも可能 (詳細は、管理者に問い合わせること)
- メッセージの受信者が、メッセージの内容が有効で、変更されていないことを確認できる：メッセージが有効である場合は、署名欄にはチェックマーク ✓ のアイコンが表示される

- 次に、Rajeev Patel が NetMail Lite にログインし、受信した電子メールを読むとしましょう。

図　3-14　　Rajeev Patel の Portal ホームページ

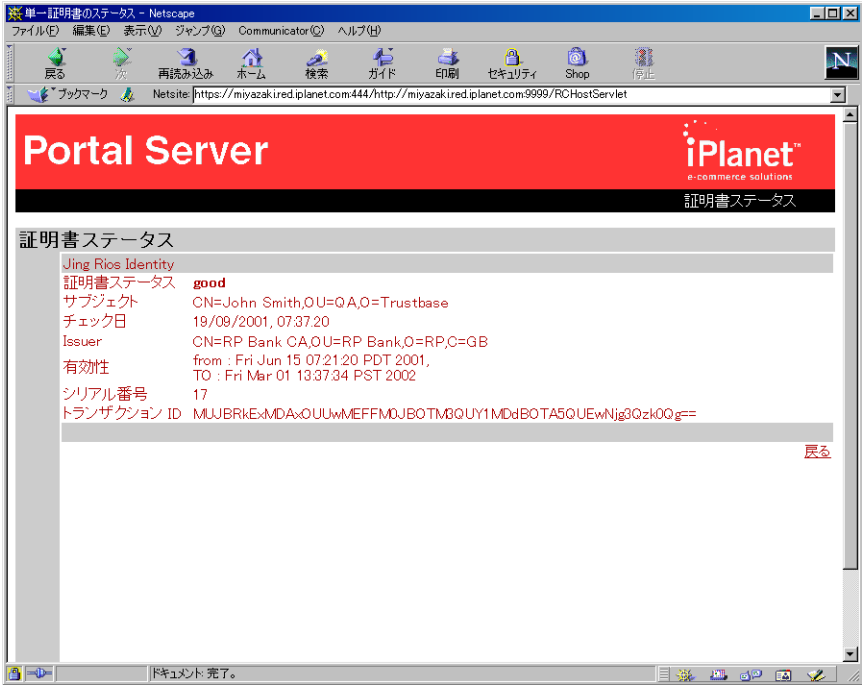


- Rajeev Patel が、John Smith からのメッセージのヘッダーを表示します。

図　3-15　　Rajeev Patel の NetMail Lite メッセージヘッダー

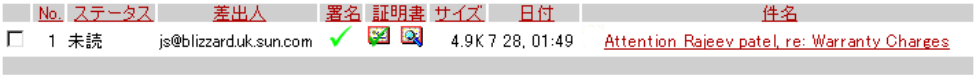
- 証明書チェックのアイコン  を選択することによって、John Smith の証明書が有効であるか、取り消し済みであるかを確認できます。

図 3-16 John Smith に対する証明書ステータスチェック



- 証明書ステータスチェックが完了すると、次に示すように、メッセージヘッダーに証明書のアイコン  が表示されます。

図 3-17 手作業で証明書ステータスチェックを実行したことを示す Rajeev Patel のメッセージヘッダー

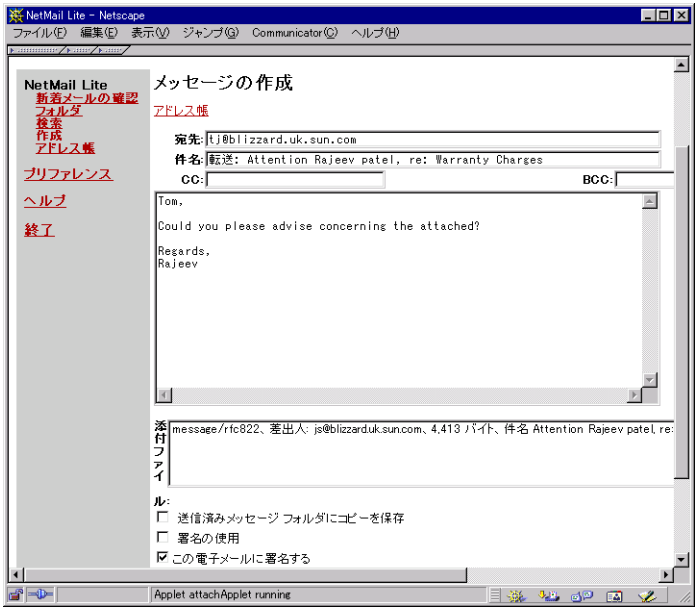


署名付きメッセージを転送する

メッセージを転送する場合にも、メッセージが署名されているか、証明書ステータスチェックを行ったかにはかかわらず、メッセージのステータスを示すことができます。したがって、転送されたメッセージには、未署名の署名や、取り消し済みの証明書が含まれることもあります。このような場合、転送されたメッセージでは階層の一部のみが示されるため、状況をどのように解釈するかはユーザ次第です。転送する埋め込みメッセージの数には、制限はありません。

- Rajeev Patel が内容を確認するために Tom Jones にメッセージを転送するとしましょう。

図　3-18　　メッセージを転送する

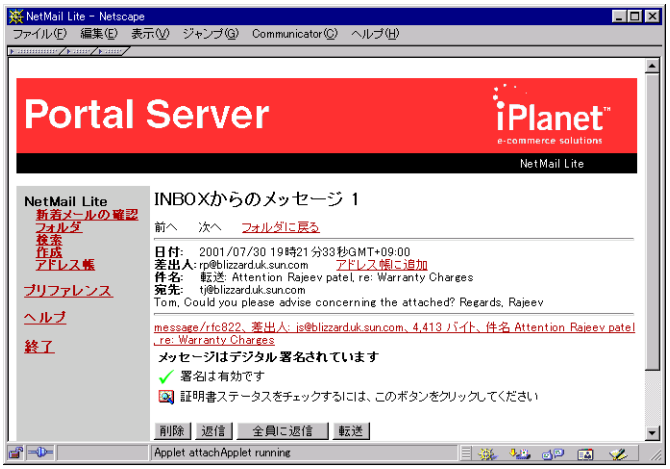


- Tom Jones が NetMail Lite にログインし、受信したメッセージを表示します。

図　3-19　　Tom Jones のメッセージヘッダー

転送メッセージを受信した場合、そのメッセージに添付されているファイルをクリックすると、メッセージがデジタル署名されているかどうかを確認できます。

図　3-20　　転送メッセージ



- 「新着メールの確認」を選択します。証明書チェック済みのアイコンが表示されます。

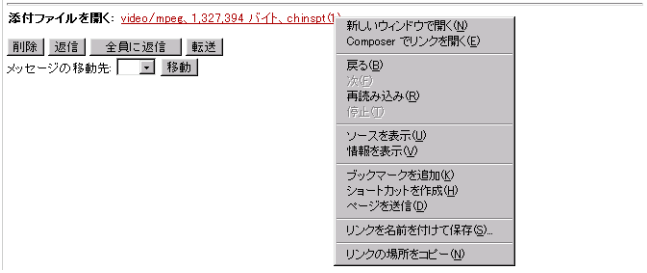
図　3-21　　転送メッセージに対して実行された証明書ステータスチェック

メッセージの転送は、否認防止のためにメッセージデータをまったく変更していない証拠を残しておく必要がある場合に便利です。このような場合には、Identrus ネットワーク内の独立機関にメッセージを転送します。メッセージを開いた時に証明書ステータスが取り消し済みであれば、元の証明書ステータスが作成された時点まで戻らなければなりません。このような場合には、証明書ステータスログを見るか、必要であればステータスログビューを HTML ファイルとしてローカルマシンに保存します。

添付ファイルを保存する

添付ファイルを保存するには、リンクを強調表示してマウスを右クリックし、「リンクを名前を付けて保存」を選択します。

図　3-22　　添付ファイルを保存する

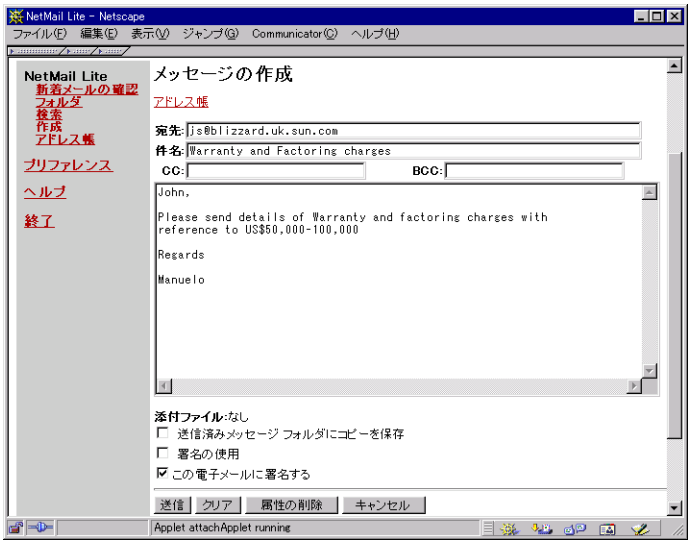


取り消し済みのメッセージ

場合によっては、従業員が退社したり、あるいは過去に有効だった証明書の期限が切れたり、取り消されたりすることがあります。

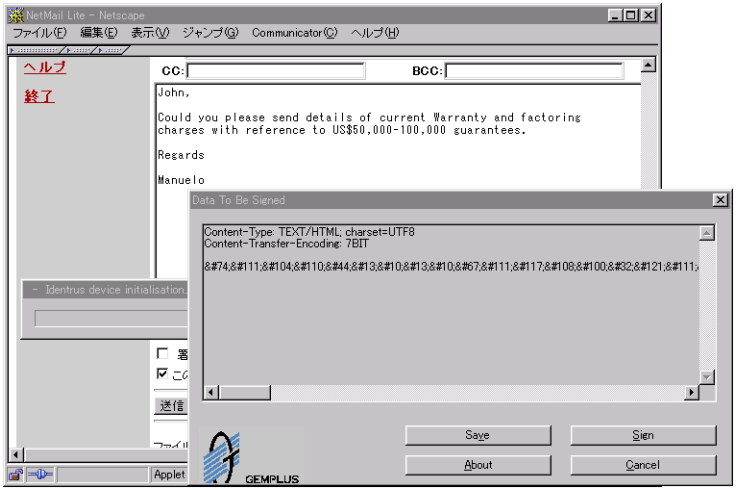
- Manuelo Revoka が NetMail Lite にログオンし、取り消された証明書を使って John Smith にメッセージを送信するとしましょう。

図 3-23 取り消された証明書を使って電子メールメッセージを送信する



- Manuelo Revoka は、取り消された証明書を使用してメッセージに署名しています。

図 3-24 取り消された証明書でメッセージに署名する



- John Smith が NetMail Lite にログオンして、受信した電子メールをチェックします。

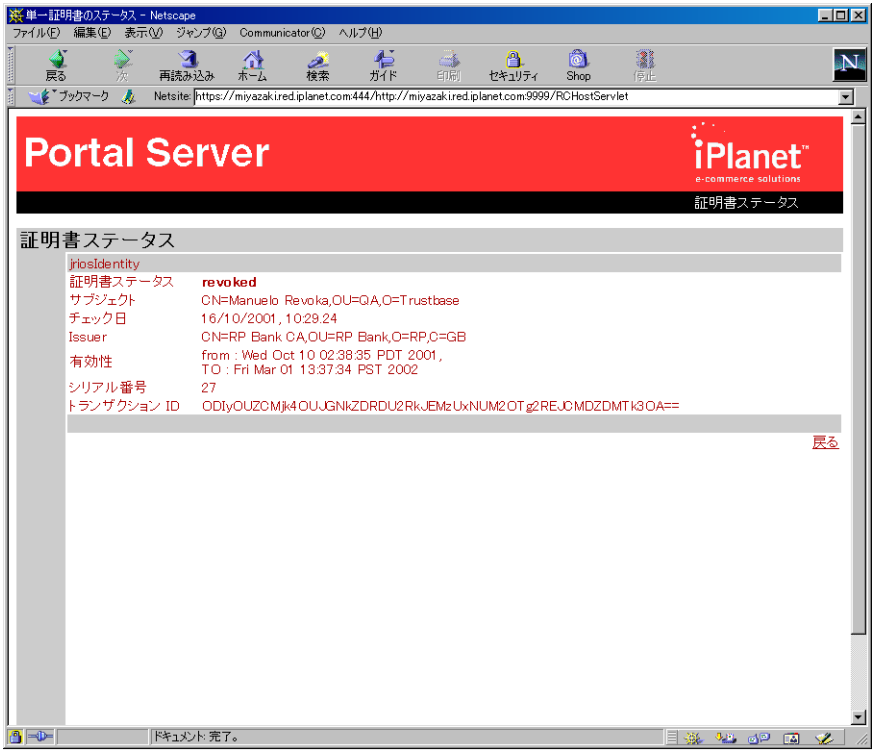
図 3-25 John Smith の Portal ユーザ画面

- John Smith が Manulo Revoka からのメッセージを表示します。

図 3-26 John Smith のメッセージヘッダー

- John Smith は、証明書チェックのアイコン をクリックして、手作業で証明書ステータスチェックを実行します。

図 3-27 取り消された証明書を含むヘッダーの詳細



- 証明書のアイコン が、証明書が取り消し済みであることを示しています。ただし、メッセージのテキストと送信者は、完全性を保っています。

図 3-28 取り消された証明書を含むメッセージヘッダーの概要

無効な署名

無効な署名が発生する理由には、次のようなものがあります。

- 署名が、管理者によって構成された証明書スキーマ外のものである：通常これは Identrus スキーマ。疑問がある場合は、管理者にお問い合わせください。
- メッセージが変更されている：何者かがシステム内に侵入し、メッセージの内容を変更した場合。このような事態が起こることはあまりないが、万が一発生した場合には、システム管理者にすぐにご連絡ください。
- 署名の証明書の有効期限が切れている：この場合には、送信者に署名証明書を更新してメッセージを再度送信するように依頼してください。
- 送信者の電子メールアドレスは、証明書のサブジェクトと同じであることが必要：これは当たり前のように思えるが、送信者が証明書スキーマ内のほかの人物の証明書を使ってメッセージに署名しようとすると、このエラーが発生する

無効な署名の例

- Manuelo Revoka が 証明書スキーマ外の証明書でメッセージに署名し、そのメッセージを Tom Jones に送信するとしましょう。

図 3-29 メッセージヘッダーに表示される無効なデジタル署名の例

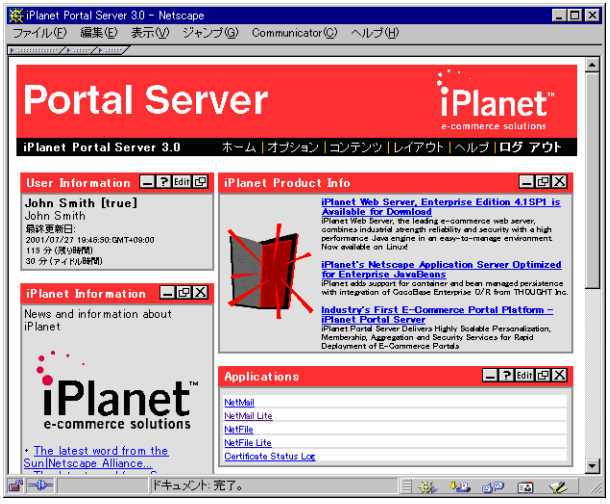
- Tom Jones が X アイコンを選択して、署名が無効な理由を表示します。

図 3-30 無効な署名の詳細

証明書ステータスログ

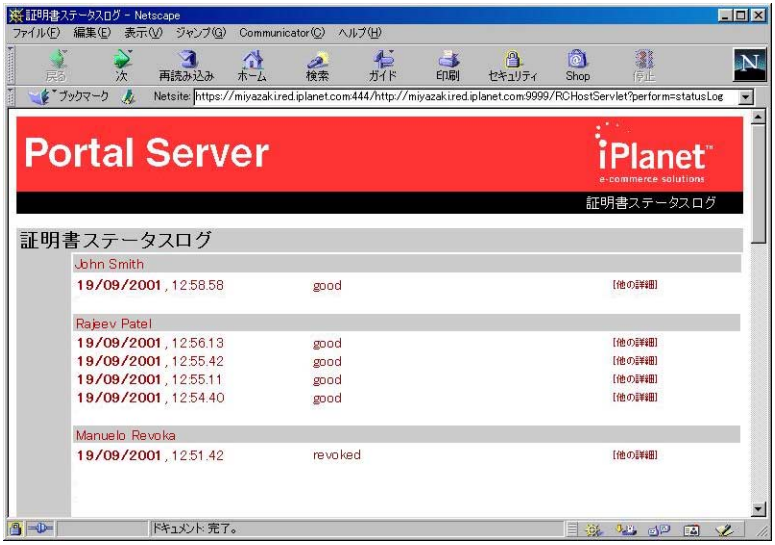
ユーザは、自分が実行したすべての証明書ステータスチェックのログを表示できます。このログにアクセスするには、iPlanet Portal Server のメインページで「Applications」リストのリンクをクリックします (図　3-31 を参照)。「Certificate Status Log」リンクをクリックすると、ブラウザのウィンドウにログページが表示されます。

図　3-31　　iPlanet Portal Server メインページ



このページには、ユーザが実行した証明書ステータスチェックのリストが、新しいものから順に表示されます。

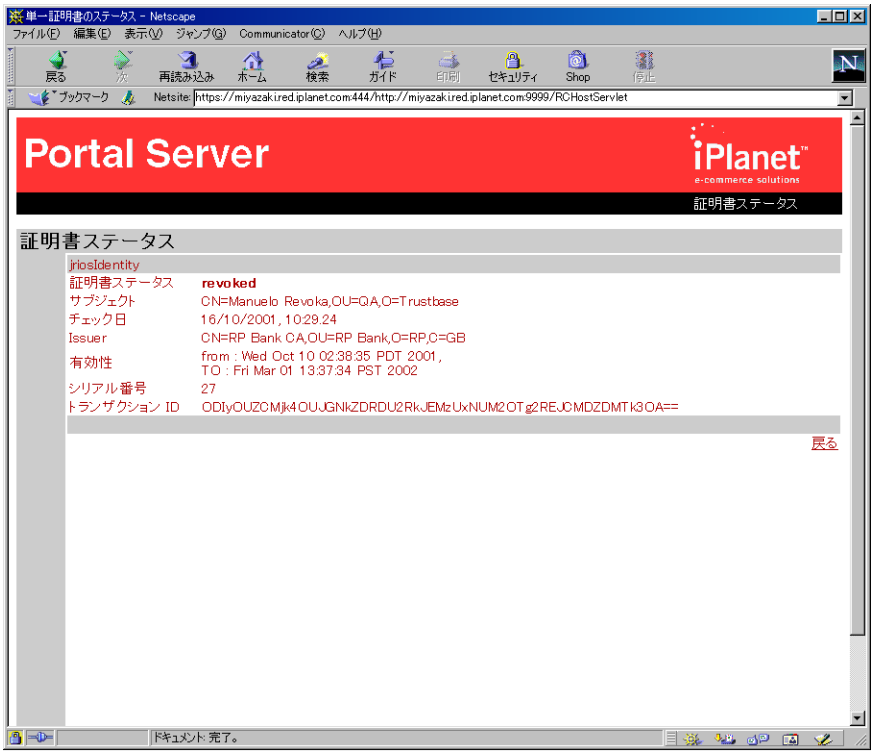
図 3-32 証明書ステータスログ



- 各エントリについて、次のデータが表示されます。
  - サブジェクト：証明書の保持者の共通名
  - 証明書ステータス：証明書ステータスチェックの結果。有効、取り消し済み、または不明
  - チェック日：証明書ステータスチェックの日時

- ユーザ (この場合は John Smith) は、「他の詳細」をクリックすると、そのエントリの証明書ステータスページにアクセスできます。

図 3-33 証明書ステータスの詳細



第 4 章

アプリケーションを導入する

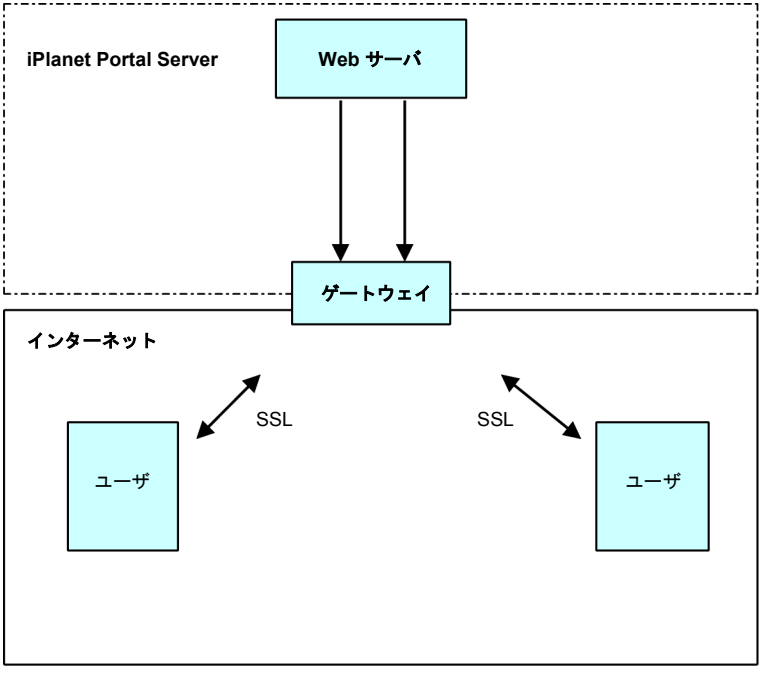
Identrus システムへの iPlanet Portal Server Plug-in を導入するには、Identrus 対応の 4 コーナーモデルを使用して証明書ステータスチェックを行う方法を理解することが必要です。この章には、次の項目があります。

- 開発環境をインストールする
- 証明書ステータスチェック
- CSC チェックを実行する
- 証明書ストアをマップする
- サンプルプログラムをコンパイルする
- サンプルプログラムを実行する

概要

Identrus システムへの iPlanet Portal Server Plug-in には、Identrus 対応の Portal Server に開発者独自のアプリケーションを簡単に統合できるように設計された、API とサンプルの Java ソースコードが付属しています。

図　4-1　　Portal Server ハードウェアの概要



通常、ポータルはサーバとゲートウェイ上に導入されます。したがって、これらのマシン両方に Java がインストールされていることが必要です。この環境を作成するには、次の手順に従います。

開発環境をインストールする

サンプルソースコードと API

Identrus 対応アプリケーションの導入方法を示すソースコードは、次のディレクトリにあります。

```
<Portal_install_directory>/SUNWpin/sample/src/com/iplanet/sample/
SampleCSC.java
```

Identrus 対応のアプリケーションの導入に適した API は、次のディレクトリにあります。

```
<Portal_install_directory>/SUNWpin/apidocs/helper/index.html
<Portal_install_directory>/SUNWpin/apidocs/plugin/index.html
```

Java セキュリティを保護する API については、次の Web サイトの Java 2 に関するドキュメント中で説明されています。

```
http://java.sun.com/j2se/1.3/docs/api/
http://java.sun.com/security/JCE1.2/spec/apidoc/
```

HTML ソース画面は、次のディレクトリにあります。

```
<Portal_install_directory>SUNWips/public_html
```

API パッケージ `com.iplanet.portalserver` は、次のディレクトリにあります。

```
<Portal_install_directory>/SUNWips/public_html/docs/en_US/javadocs/
com/iplanet/portalserver
```

Portal API パッケージ `com.iplanet.portalserver` の導入方法に関する情報は、次のサイトに記載されています。

```
http://docs.iplanet.com/docs/manuals/portal/30/progref/
```

2 つの Java 仮想マシンを作成する

Web サイトから JDK をダウンロードし、/app などの一時ディレクトリに置きます。

```
http://java.sun.com
```

次のように、適切なディレクトリにコピーします。

```
cd/app
mkdir java1.2.2_06
cp -r java1.2/* java1.2.2_06/
```

Portal Server を起動する

Portal Server を起動するスクリプトを次に示します。

```
#!/bin/sh
LD_LIBRARY_PATH=/app/SUNWips/lib
export LD_LIBRARY_PATH
/app/SUNWips/bin/ipsserver start debug > ipsserver.out
JAVA_HOME=/app/java1.2.2_06
export JAVA_HOME
/app/SUNWips/bin/ipsgateway start
tail -f ipsserver.out
```

Portal Server を停止する

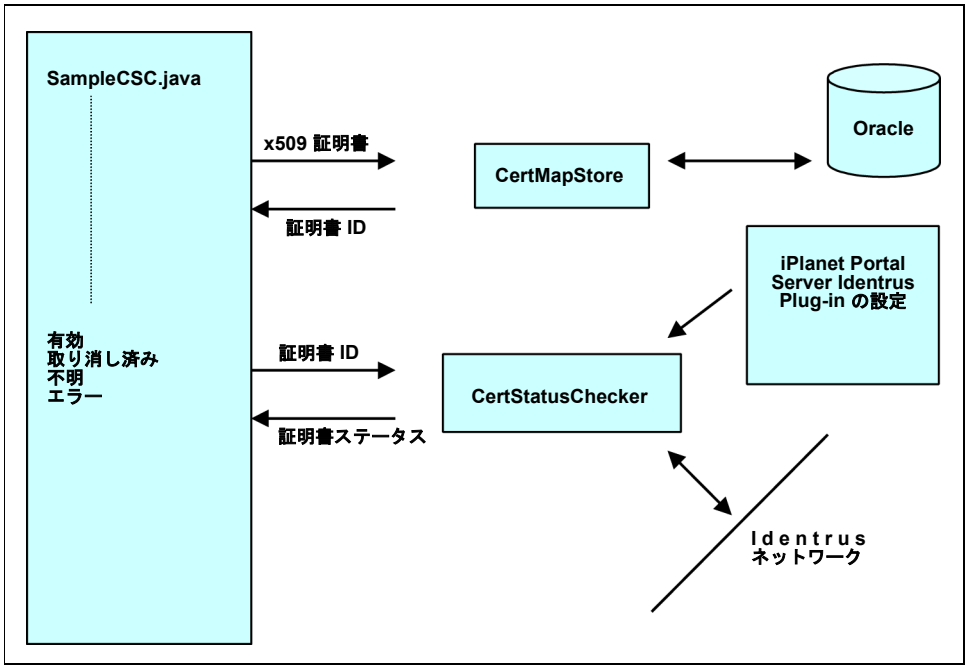
Portal Server を停止するスクリプトを次に示します。

```
/app/SUNWips/bin/ipsserver stop
/app/SUNWips/bin/ipsgateway stop
```

証明書ステータスチェック

証明書ステータスチェックを実行するには、次のインタフェースパッケージを使用します。

図　4–2　　インタフェースパッケージを使用して CSC を実行する



CSC チェックを実行する

CertStatusChecker は、証明書 ID のステータスを取得するための API パッケージです。これは、checkStatus(CertID) を使用して導入できます。返されたプロパティオブジェクトからは、リクエストの時刻、証明書のステータス、レスポンスのステータス、およびトランザクション ID を取得できます。.checkStatus(CertID) を呼び出すと、提供された証明書 ID を使用して、証明書ステータスチェックが実行されます。ただし、レスポンダ URL と署名証明書が Portal Server 内で適切に設定されていないと、証明書ステータスチェックは成功しません。レスポンダ URL と署名証明書を設定するには、管理サーバ (通常は http://127.0.0.1:8080/console) を使用します。次の構成が必要です。

- CSC 構成 : リクエスト署名証明書、レスポンス署名証明書、および信頼できるレスポンス確認証明書
- RC ホスト
- RC 設定 : レスポンダタイプ、レスポンダの URL、OCSP リクエスタ名
- 組織に関する詳細 : 組織 ID、正式名、省略名、ロゴの URL、所在地、および連絡先の情報

次のコードにこの例を示します。

```
 CertStatusChecker statusChecker =
SingletonCertStatusChecker.getChecker( mySessionID );
    Properties certProps = statusChecker.checkStatus( myCertID );
    //Get the Certificate Status
   String certStatus = certProps.getProperty(
CertStatusChecker.CERT_STATUS );
      if (certStatus.equals ( CertStatusChecker.GOOD ) )
   {System.out.println(" 証明書は信頼できます。");}
   else if (certStatus.equals ( CertStatusChecker.REVOKED ) )
   {System.out.println(" 証明書は取り消し済みです。");}
   else if (certStatus.equals ( CertStatusChecker.UNKNOWN ) )
   {System.out.println("CSC は証明書ステータスを認識できません。");}
   else if (certStatus.equals ( CertStatusChecker.ERROR ) )
   {System.out.println(" 証明書ステータスの取得中にエラーが発生しました。");}
    //Get request time
   String requestTime = certProps.getProperty(
CertStatusChecker.REQUEST_TIME );
    System.out.println(" リクエスト時刻 : " + requestTime);
    //Get response status
   // The response code is used to provide more detail of an error if
the cert status was ERROR.
   String requestStatus = certProps.getProperty(
CertStatusChecker.RESPONSE_STATUS );
    System.out.println(" リクエストステータス : " + requestStatus);
    //Get Transaction ID
   String transID = certProps.getProperty( CertStatusChecker.TX_ID );
    System.out.println(" トランザクション ID : " + transID);
```

注　開発者の方は、次のファイルを参照してください。
`<Portal_install_directory>/SUNWpin/apidocs/com/iplanet/portalserver/identrus/statuscheck/CertStatusChecker.html`

また、構成の設定については、『管理者ガイド』の第 3 章を参照してください。

証明書ストアをマップする

CertMapStore は、証明書および 証明書 ID にアクセスするための API パッケージです。証明書 ID は、CertMapStore 内の証明書を識別するために、Portal Server CSC ライブラリによって使用されます。次に、一般的な使用方法の例を示します。

```
 CertMapStore certStore =
SingletonStatusStoreRegistry.getCertMapStore( mySessionID );

 // 例 1 : 単独の証明書 (base64 として提示される場合もあり )

 X509Certificate aPKCS7Cert = convertSomePKCS7DataFromSomeSource (
pkcs7data ) ;

 CertID certID = certStore.getCertID ( aPKCS7Cert ) ;

 performCSCCode ( certID ); // 詳細は CertStatusChecker を参照
```

注 x509 証明書 へのアクセス方法については、次のサイトを参照してください。

`http://java.sun.com/j2se/1.3/docs/api/java/security/cert/X509Certificate.html`

CertMapStore インタフェースについては、次のファイルを参照してください。

`<Portal_install_directory>/SUNWpin/apidocs/com/iplanet/portalserver/identrus/statuscheck/CertMapStore.html`

サンプルプログラムをコンパイルする

CSC アプリケーションの開発に必要なライブラリはすべて、次の場所にあります。

```
<Portal_install_directory>/SUNWips/lib
```

また、このディレクトリには、すべての Portal Server ライブラリに加え、すべての Plug-in ライブラリがあります。サンプルプログラムを MS-DOS から実行およびコンパイルするスクリプトを次に示します。

```
cd <Portal_install_directory>/SUNWips/lib
set
CLASSPATH=sample.jar:activation.jar:asn1.jar:config.jar:ipspin.jar:
dsms.jar:jndi.jar:jaas.jar:jss21.jar:ldapbp.jar:jsskeystore.jar:
ldapfilt.jar:ldap.jar:ocsp.jar:ldapjdk_debug.jar:mail.jar:servlet.jar:
pkcs.jar:tbmail.jar:providerutil.jar:tbutil.jar:ssl.jar:x509v1.jar:
tokenkeystore.jar:country.zip:xml.jar:identrus_update.zip:xml4j.jar:
utiloverride.zip:identrus.zip:oracle-jdbc-815.zip:
tbextlibrary.zip: tblibrary.zip: ips_services.jar: trustbase.zip
export CLASSPATH
javac
<Portal_install_directory>/SUNWpin/sample/src/com/iplanet/sample/
SampleCSC.java
cd <Portal_install_directory>/SUNWpin/sample/src
jar cvf <Portal_install_directory>/SUNWpin/sample/src
/com/iplanet/sample/sample.jar com/iplanet/sample/SampleCSC.class
```

プログラムをコンパイルして sample.jar ファイルに読み込んだら、このファイルを Portal Server_install_directory 内の jar ファイルのディレクトリにコピーします。

```
<Portal_install_directory>/SUNWips/lib/sample.jar
```

サンプルプログラムを実行する

プログラムを実行するには、次の条件を満たすことが必要です。

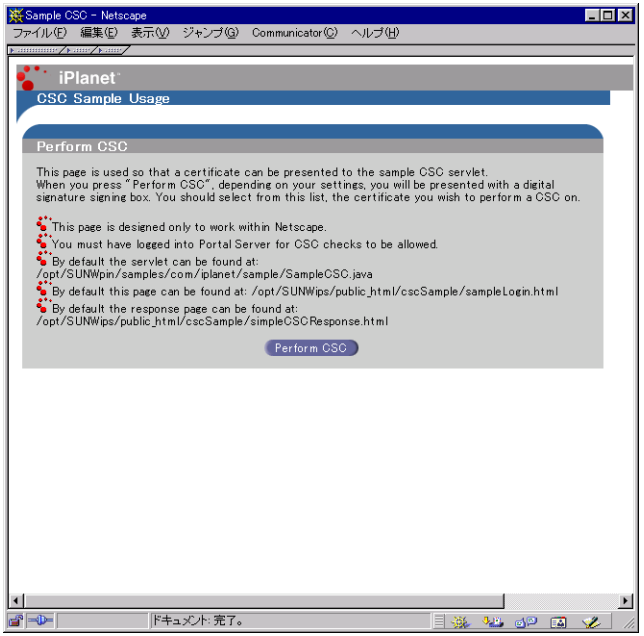
- CSC が設定されていること (第 2 章、「管理」を参照)
- スマートカードユーザとして、または管理コンソールから、ログインしていること

サンプルプログラムを実行するには、次のように入力します。

```
http://hailstorm.uk.sun.com:8080/SampleCSC
```

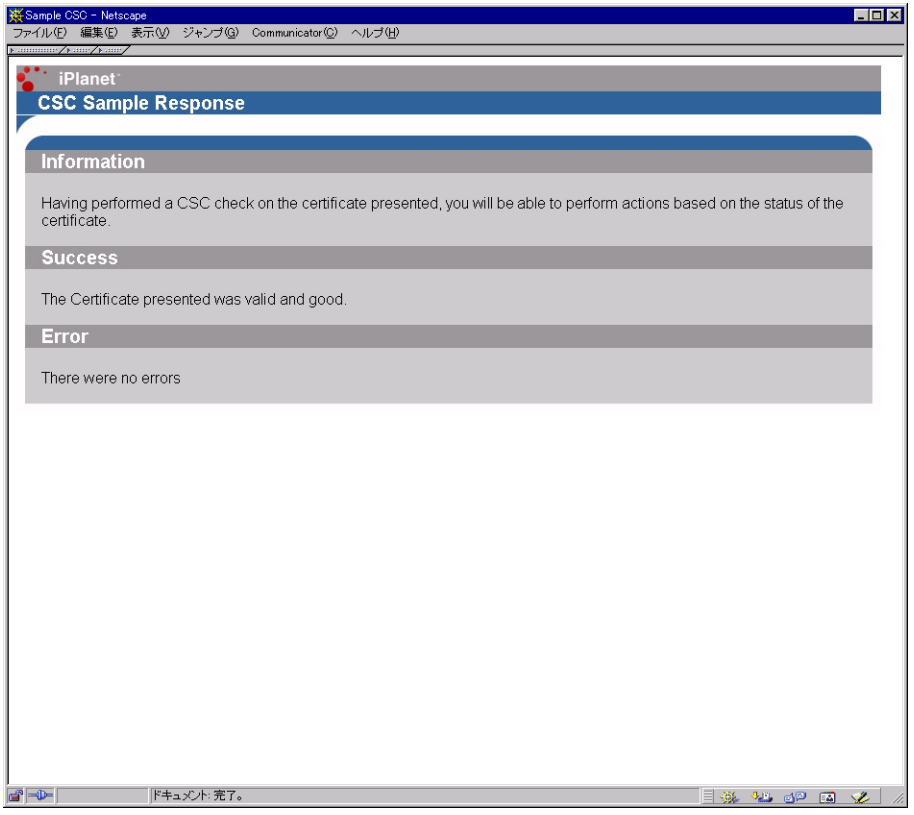
次の画面が表示されます。

図 4-3 サンプル証明書ステータスチェックのメイン画面



「Perform CSC」を選択します。次の出力が表示されます。

図 4-4 サンプル証明書ステータスチェックの出力



用語集および関連サイト

この章には、次の項目があります。

- ソフトウェアプラットフォーム
- プロトコル
- 用語集

ソフトウェアプラットフォーム

Java Development Kit 1.2.1

http://java.sun.com/products/jdk/

Java

http://www.javasoft.com

Java インタフェース

http://java.sun.com/products/jndi/index.html

ホスト iPlanet Portal Server 3.0

http://www.iplanet.com/products/infrastructure/portal/index.html

Hardware Security nCipher KeySafe 1.0 および CAFast

http://www.ncipher.com

Oracle 8i

http://www.oracle.com

GemSAFE IS スマートカードツール

http://www.gemplus.com

プロトコル

S/MIME バージョン 1

http://www.ietf.org/rfc.html (RFC2045、2046、2047、2048、および 2049 を参照)

http://www.imc.org/ietf-smime

http://www.ietf.org/rfc/rfc2311.txt

OCSP

http://www.imc.org/ietf-pkix/

http://www.ietf.org/rfc/rfc2560.txt

IMAP

http://www.cis.ohio-state.edu/htbin/rfc/rfc1730.html

http://www.cis.ohio-state.edu/htbin/rfc/rfc2060.html

SMTP

http://www.imc.org/ietf-smtp/

http://www.cis.ohio-state.edu/htbin/rfc/rfc2156.html

ftp://ftp.isi.edu/in-notes/rfc821.txt RFC 821 および RFC 822 で指定されているクライアントプロトコル

スマートカード規格

http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-11.html

証明書リクエストおよびレスポンス

PKCS10 リクエスト RFC2314 については、http://www.ietf.org/rfc.html を参照

PKCS7 レスポンス RFC2315 については、http://www.ietf.org/rfc.html を参照

HTML

http://www.w3.org/TR/REC-html32.html で指定されている HTML 3.2

HTTP

HTTP/1.0 または 1.1 プロトコル :

http://www.w3.org/Protocols/rfc1945/rfc1945.txt

Identrus

http://www.identrus.com

LDAP

RFC 1777 および RFC 1778 で指定されている、JNDI API によってサポートされる LDAP クライアントプロトコル。
http://www.cis.ohio-state.edu/htbin/rfc/rfc1777.html

用語集

3DES	DES に類似。
AIA	権限情報アクセス (Authority Information Access)。
ASN.1	抽象構文記法 (Abstract Syntax Notation One)。
base64	65 文字から成る U.S. ASCII サブセットを使用した、デジタル形式の文字表現。
BBS	乱数発生アルゴリズムの一種。
BER	X509 で使用される基本エンコーディング規則。
CA	認証局
CBC モード	ブロック符号化方式によって暗号化される平文の各ブロックと、直前の暗号文ブロックの排他的論理和を次の暗号化の入力とするモード (最初の平文ブロックの場合は、初期化ベクトルとの排他的論理和が取られる)。
CN	共通名 (Common Name)。定義については、`http://www.itu.int/itudoc/itu-t/rec/x/x500up/x500.html` などを参照。
CRL	証明書破棄リスト (Certificate Revocation List)。有効期限が切れてはいないが、発行元の CA によって無効化になった証明書のリスト。
CSC	証明書ステータスチェック (Certificate Status Check)。
DER	X509 で使用される特殊エンコーディング規則。
DH	データを暗号化および復号化するための公開鍵暗号化アルゴリズム。
DN	識別名 (Distinguished Name)。定義については、`http://www.itu.int/itudoc/itu-t/rec/x/x500up/x500.html` または `http://search.ietf.org/internet-drafts/draft-zeilenga-ldapv3bis-rfc2253-00.txt` を参照。
DSA	デジタル署名アルゴリズム (Digital Signature Algorithm)。
EE	エンドエンティティ (End Entity) である顧客。証明書チェーン内の最終人物のこと。
HSM	ハードウェアセキュリティモジュール (Hardware Security Module)。
HTML	ハイパーテキストマークアップ言語 (HyperText Markup Language)。
IDEA	Xuejia Lai と James Massey が考案した 64 ビットブロック符号化方式。
IP	秘密鍵および証明書を含むスマートカードを SC (Subscribing Customer) に発行する IP (Issuing Participant) 銀行またはその他の金融機関。
IR	Identrus ルート (Identrus Root)。
LDAP	軽量ディレクトリアクセスプロトコル (Lightweight Directory Access Protocol)。
MD5	任意の長いデータストリームを固定長のダイジェストに変換する、セキュリティ保護されたハッシュ関数。
MIME	多目的インターネットメール拡張仕様 (MultiPURPOSE Internet Mail Extension)。

OCSP オンライン証明書ステータスプロトコル (Online Certificate Status Protocol)。

OU 組織ユニット (Organisation Unit)。定義については、`http://www.itu.int/itudoc/itu-t/rec/x/x500up/x500.html` または `http://search.ietf.org/internet-drafts/draft-zeilenga-ldapv3bis-rfc2253-00.txt` を参照。

PBE パスワードを基盤とした暗号化 (Password based encryption)。

PEM プライバシー強化メール (Privacy enhanced mail)。

OSI 開放型システム間相互接続 (Open Systems Inter-Connection)。

RC2、RC4 RSA Data Security, Inc. が独自に開発したバルク符号化方式。RC2 はブロック符号化方式、RC4 はストリーム符号化方式。

RC Relying Customer の略。SC (Subscribing Customer) が署名付きトランザクションを開始する相手。

RC ホスト Identrus 証明書ステータスチェックスキーマで RC (Relying Customer) の役目を担うサーバソフトウェア。このマニュアルでは、Portal Server がこれにあたる。

RC NetMail Lite または RC Mail 顧客がメッセージの送受信に使用するクライアントソフトウェアインタフェース。このマニュアルでは、NetMail Lite がこれにあたる。

RP Relying Participant 銀行の略。SC (Subscribing Customer) から受け取った署名付きデータの信頼性をある程度確認するため、RC (Relying Customer) が問い合わせる先。

RSA 広く用いられている公開鍵アルゴリズム。暗号化またはデジタル署名に使用できる。

SC Subscribing Customer の略。Identrus アクティビティに参加する権限を持つ IP (Issuing Participant) 銀行のメンバーのこと。

SHA セキュアハッシュアルゴリズム (Secure Hash Algorithm)。20 バイトの出力を行う。FIPS PUB 180-1 で定義されている。

SSL セキュアソケットレイヤ (Secure sockets layer)。

TC トランザクションコーディネータ (Transaction Co-ordinator)。

X509 ASN.1 BER、ASN.1 DER、および base64 に基づく認証フレームワーク。

アプリケーションプロトコル 通常はトランスポート層 (例 : TCP/IP) の上に直接重なっているプロトコル。HTTP、TELNET、FTP、SMTP などがある。

鍵 クライアントが書き込んだデータを暗号化するための鍵。

完全性 電子メールメッセージが変更されていないこと。

クライアント サーバへの接続を開始するアプリケーションエンティティ。

公開鍵暗号化法 2つの鍵による符号化方式を用いる暗号化技術。公開鍵を使って暗号化されたメッセージは、その公開鍵と対になった秘密鍵を使用した場合にのみ復号化できる。逆に、秘密鍵を使って暗号化されたメッセージは、公開鍵を使って復号できる。

公開鍵インフラストラクチャ (PKI) オンラインでのやり取りをサポートするためのプロトコルを定義する。

サーバ クライアントの接続リクエストに応答するアプリケーションエンティティ。受動的であり、クライアントからのリクエストを待つ。

証明書 X.509 プロトコル (ISO 認証フレームワーク) の一部。信頼できる認証局によって割り当てられる。エンティティを識別するためのものであり、そのエンティティの公開鍵を提供することもある。

スタブ CAFast ハードサーバとの通信をサポートする Java インタフェース。

スマートカード 暗号化機能を実装するために 1 つまたは複数の集積回路 (IC) チップを組み込んだハードウェアトークン。不正操作をある程度防止するための固有機能を備える。

セッション SSL セッションとはクライアントとサーバのつながりのこと。セッションは、ハンドシェイクプロトコルによって作成され、一連の暗号化セキュリティパラメータを定義する。複数の接続がこれらのパラメータを共有することも可能。セッションの使用によって、接続ごとに新しいセキュリティパラメータを指定する必要がなくなり、コストを節約できる。

接続 OSI 階層モデルのトランスポートにあたるもので、適切なタイプのサービスを提供する。SSL ではピアツーピア関係を持つ。接続は一時的なものであり、1 セッションに 1 回接続される。

データ暗号化規格 (DES) 広く使用されている対称暗号化アルゴリズム。ブロック符号化方式の一種。

デジタル署名 公開鍵暗号化法と単方向ハッシュ関数によって、認証可能で偽造または否認しにくいデータの署名を作成する。

デジタル署名標準 (DSS) 米国の国立標準技術研究所 (National Institute of Standards and Technology) が認可した、デジタル署名アルゴリズムを含むデジタル署名の標準。1994 年 5 月に米国商務省が発行した NIST FIPS PUB 186「Digital Signature Standard」で定義されている。

認証 あるエンティティが他のエンティティを識別する能力。たとえば、NetMail Lite では電子メールの差出人が分かる。

認証局 証明書を発行する権限を持つ機関 (CA)。

バルク符号化方式 大量のデータを暗号化するために使用される対称暗号化アルゴリズム。

ハンドシェイク トランザクションのパラメータを決定する、クライアントとサーバの初期ネゴシエーション。

否認防止 送信者がメッセージを否認できないようにするため設定されたプロセス。

ブロック符号化方式 ブロックと呼ばれるデータ単位ごとに平文を処理するアルゴリズム。通常、1 ブロックは 64 ビット。

メッセージ認証コード (MAC) メッセージおよび機密データから計算された単方向ハッシュ。メッセージの改ざんを検知するために使用される。

索引

数字

A

B

C

D

G

H

I

J

L

M

N

O

P

R

S

T

X

あ

い

お

か

き

て

と

に

は

ひ

ふ

ほ

む

め

ゆ

よ

ろ