設定ガイド

iPlanet Trustbase Transaction Manager

Release 2.2.1

2001 年 3 月

目次

図一覧

概要

この章では、このガイドに関連するすべてのドキュメントを紹介します。

全体の構成

ドキュメントセットは、次の各ドキュメントから構成されています。

- iTTM2.2-Utility-Guide.pdf。PKI 証明書管理に役立ついくつかのユーティリティについて説明している
- iTTM2.2-Install-Configuration-Guide.pdf（このドキュメント）。iPlanet Trustbase Transaction Manager のフレームワークを利用するアプリケーションを制作しようとする開発者向け。iPlanet Trustbase Transaction Manager プラットフォームをインストールするために必要な情報を提供するガイド。インストールに先立ち必要なソフトウェアとハードウェア、および CD-ROM から iPlanet Trustbase Transaction Manager をインストールする方法について説明している
- iTTM2.2-Developer-Guide.pdf。独自のサービスを構築および配置する方法について説明している

このガイドで取り上げている内容：

- インストールの概要
- 詳しいインストール手順
- ハードウェア構成に関する事項
- 動的構成

関連ドキュメント

- Solaris 8 および Java Development Kit 1.2.1

  英語 :

  `http://docs.sun.com`

  `http://java.sun.com/products/jdk/1.1/docs/index.html`

  `http://www.sun.com/software/solaris/cover/sol8.html`

  日本語 :

  `http://www.sun.co.jp/software/solaris/cover/sol8.html`

  `http://docs.sun.com/ab2/products_ja/INDEX/@ProductViewer/8339/*;td=1?Ab2Lang=ja&Ab2Enc=euc-jp`

- Java

  英語 :

  `http://www.javasoft.com`

  日本語 :

  `http://java.sun.com/products/jdk/1.2/download-ja-docs.html`

- iPlanet Application Server 6.0

  英語 :

  `http://docs.iplanet.com/docs/manuals/ias.html`

  `http://www.iplanet.com/products/infrastructure/app_servers/index.html`

  `http://www.iplanet.com/products/iplanet_application/home_2_1_1n.html`

  日本語 :

  `http://www.iplanet.ne.jp/products/ias6/index.html`

  `http://docs.iplanet.com/docs/manuals/ias/60/sp2/ja/ReadMe_ja.html`

- iPlanet Web Server 4.1

  英語 :

  `http://docs.iplanet.com/docs/manuals/enterprise.html`

  `http://www.iplanet.com/products/infrastructure/web_servers/index.html`

  `http://www.iplanet.com/products/iplanet_web_enterprise/home_2_1_1m.html`

日本語 :

`http://www.iplanet.ne.jp/products/iws4_1/index.html`

`http://docs.iplanet.com/docs/manuals/enterprise/41/rn41sp5_JP.htm`

`http://docs.iplanet.com/docs/manuals/enterprise/41/ja/ag/contents.htm`

`http://docs.iplanet.com/docs/manuals/enterprise/41/ja/ig/contents.htm`

- iPlanet Certificate Management System

  `http://docs.iplanet.com/docs/manuals/cms.html`

- 『Oracle 8i Installation Guide』および『Oracle 8i Configuration Guide』

  英語 :

  `http://www.oracle.com`

  日本語 :

  `http://www.oracle.co.jp`

- Hardware Security nCipher KeySafe 1.0 および CAFast

  英語 :

  `http://www.ncipher.com`

  日本語 :

  `http://www.tel.co.jp`

- Identrus メッセージ仕様

  `http://www.identrus.com`

  Transaction Coordinator requirements (IT-TCFUNC)

  Core messaging specification (IT-TCMPD)

  Certificate Status Check Messaging specification (IT-TCCSC)

第 1 章

インストールワークシート

この章は、iPlanet Trustbase Transaction Manager をインストールする際に、すべての主な機能の必要要件を確認するためのインストールワークシートです。このワークシートでは、付属のソフトウェア、付属していないソフトウェア、およびダウンロードの必要なソフトウェアをリストし、各ソフトウェアをインストールおよび構成する方法について説明します。

インストールの概要

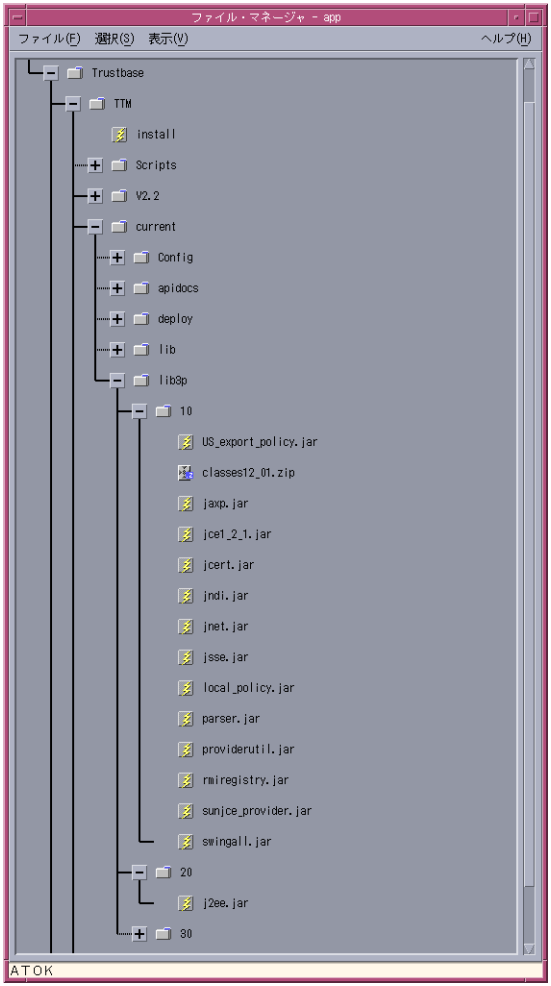
インストールの手順は次のとおりです。

- ソフトウェアの必要要件を確認し、これらの要件が満たされるようにします。
- iPlanet Trustbase Transaction Manager に付属していないソフトウェアをダウンロードします。
- iPlanet Web Server v4.1 をインストールします。
- iPlanet Application Server v6.0 をインストールします。
- iPlanet Trustbase Transaction Manager v2.2 と Identrus 拡張機能をインストールします。
- nFast ハードウェアを設定し、nFast を使用できるように iPlanet Trustbase Transaction Manager を構成します。
- Oracle 8i データベーススキーマを設定します。
- サイト固有の Identrus 設定を指定します。
- iPlanet Trustbase Transaction Manager を起動します。
- CertManager を使用して、Identrus の証明書と鍵を獲得します。

ソフトウェアの必要要件

iPlanet Trustbase Transaction Manager を実行するには、次のソフトウェアがインストールされている必要があります。

図　1-1　　サードパーティによるライブラリの jar ファイル



必要要件

- Microsoft のブラウザ。Web 構成用に Internet Explorer 4.0 以降、または Netscape 4.0 以降

- Oracle 8i
- iPlanet Trustbase Transaction Manager 2.2 には、Solaris 8 オペレーティング環境システムと、JDK 1.2 環境または Java™ Runtime Environment 1.2 が必要
- iPlanet Trustbase Transaction Manager 2.2 には、JDK 1.2 環境が必要。JDK 1.2 は、米国 Sun Microsystems, Inc. の Web サイトから入手可能
  `http://www.javasoft.com`
- JDBC™ for Oracle 8i
  `http://www.oracle.com/java/jdbc/html/jdbc.html`
- Java™ Servlet をサポートする WebServer
  - iPlanet Web Server 4.1
    `http://www.iplanet.com/products/infrastructure/web_servers/index.html`
- アプリケーションサーバ
  - iPlanet Application Server 6.0
    `http://www.iplanet.com/products/infrastructure/app_servers/index.html`
- Identrus 準拠の Validation Authority
- Identrus 準拠の認証局 (Certificate Authority)
- ハードウェアセキュリティモジュール
  - nCipher KeySafe 1.0
    `http://www.ncipher.com`

付属のパッケージ

iPlanet Trustbase Transaction Manager には、次のパッケージが含まれています。

- iPlanet Application Server 6.0
  `http://www.iplanet.com/products/infrastructure/app_servers/index.html`
- iPlanet Web Server 4.1
  `http://www.iplanet.com/products/infrastructure/web_servers/index.html`
- Java™ API for XML Parsing
  `http://java.sun.com/xml`

付属していないパッケージ

インストールの前に、次のソフトウェアをダウンロードする必要があります。

- JDBC™ -Thin / 100% Java API for JDK ™ 1.1.x
  `http://technet.oracle.com/software/download.htm`
  `oracle-jdbc-815.zip.`
- JDK™ 1.2 環境を含む Solaris 8 オペレーティングシステム環境

証明書の必要要件

iPlanet Trustbase Transaction Manager をインストールする前に、PEM 形式でエンコードされた level 1 Certificate Authority の CA 証明書の場所を確認してください。この証明書は、これ以降「L1CA 証明書」と記述します。

注　　すべてのサードパーティ製のソフトウェアは、15ページの図　1–1 に示すように、lib3p/10 に配置します。

システムリソース

- ホスト名を決定します。

```
hostname
domainname
```

- ディスク容量が 1G バイトより大きいことを確認します。

```
df -k
```

- 最低限のメモリ (256M バイト) があることを確認します。推奨のメモリ容量は 1G バイトです。

```
prtconf | grep Mem
```

- Solaris のバージョンが 8 であることを確認します。

```
uname -a
```

- Java のバージョンが 1.2 であることを確認します。

```
java -version
```

Solaris のインストール

iPlanet Trustbase Transaction Manager をインストールするには、稼動中の Web サーバおよびアプリケーションサーバが必要です。

iPlanet Web Server v4.1 のインストール

- ルートとしてログオンし、「setup」スクリプトを探します。このスクリプトの場所は、システムの分散状況によって異なります。
- 「setup」スクリプトを使って、インストールを始めます。
- Web Server をインストールするディレクトリ (< インストールディレクトリ >) を選択します。このディレクトリは、後で iPlanet Application Server をインストールするのと同じディレクトリであることが必要です。

```
# cd /cdrom/cdrom0
# cd iWS
#./setup
```

- Web Server のすべての要素をインストールし、所有者 / グループを「nobody」に変更するオプションを選択します。Web Server を「root」として実行するオプションを選択します。既存のディレクトリサービスは使用しないでください。Web Server のドキュメントディレクトリには、指定したインストール場所の docs サブディレクトリを選択します。プロンプトでは自分の JDK を指定しないでください。

図 1-2 iPlanet Web Server のインストール

```
Would you like to continue with installation?[Yes]:Yes
Do you agree to the license terms?[Yes]:Yes
Choose an installation type [2]: 2
Install location [/usr/netscape/server4]: /app/iws41
Specify the components you wish to install [A] A
Specify the components to install [1, 2, 3, 4, 5, 6, 8]: 1,2,3,4,5,6,8
Computer name [rainstorm.jcp.co.uk]: rainstorm.jcp.co.uk
System User [nobody]: nobody
System Group [nobody]: nobody
Run iWS Administration Server as [root]: root
IWS Admin Server User Name [admin]: admin
IWS Admin Server Password:
IWS Admin Server Password (again):
IWS Admin Server Port [8888]: 8888
Web Server Port [80]: 80
Do you want to register this with an existing Directory Server [No]:No
Web Server Content Root [/app/iws41/docs]:
Do you want to use your own JDK [No]:No
```

注　　これらの設定はメモしておくことをお勧めします。特に、ポート番号は後で必要になる場合があります。

- 次の出力が表示されます。

図 1-3　　iPlanet Web Server のインストール完了

```
                        Sun Netscape Alliance
            iPlanet Web Server Installation/Uninstallation
---------------------------------------------------------------------


Extracting Server Core...
Extracting Java Runtime Environment...
Extracting Java Support...
Extracting SSJS Support...
Extracting SSJS Database Support...
Extracting Web Publishing Support...
Extracting SNMP Support...
Extracting Upgrade Files...


Server Core installed successfully.
Java Runtime Environment installed successfully.
Java Support installed successfully.
SSJS Support installed successfully.
SSJS Database Support installed successfully.
Web Publishing Support installed successfully.
SNMP Support installed successfully.

Press Return to continue...

Go to /app/iws41 and type startconsole to begin
Managing your servers.
```

注　　詳細は、『iPlanet Web Server Installation Guide』を参照してください。<Return> キーを押すと、デフォルトの設定が適用されます。

iPlanet Web Server 4.1 の起動

Web Server のインスタンスのあるディレクトリに移動して、「start」スクリプトを実行します。このディレクトリの形式は、「https-< マシン名 >. ドメイン」です。

次に例を示します。

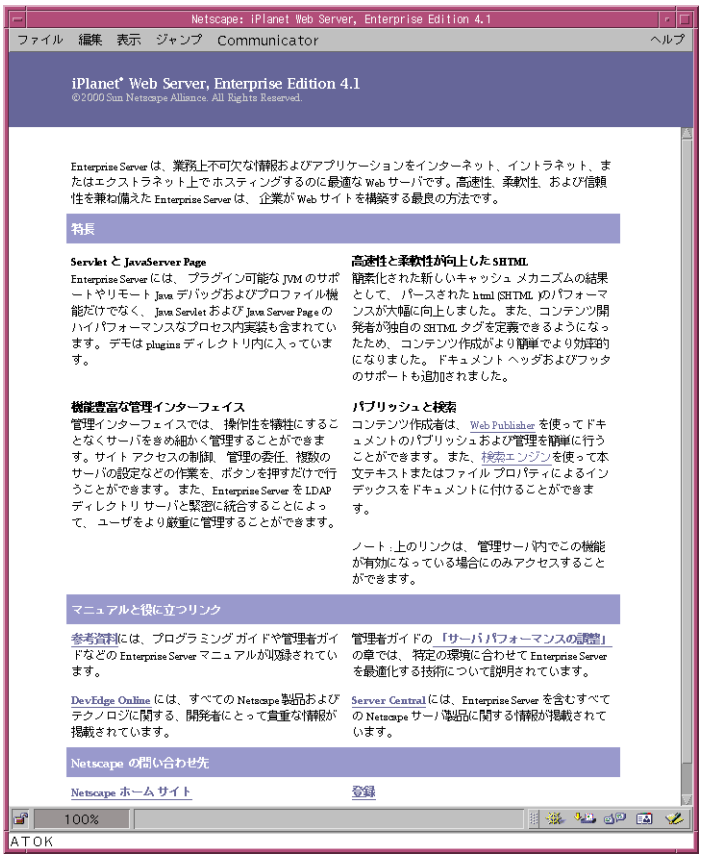
```
cd /app/iws41/https-whelk.jcp.co.uk
./start
```

注　詳細は、『iPlanet Web Server Configuration Guide』の第 1 章を参照してください。

iPlanet Web Server 4.1 の確認

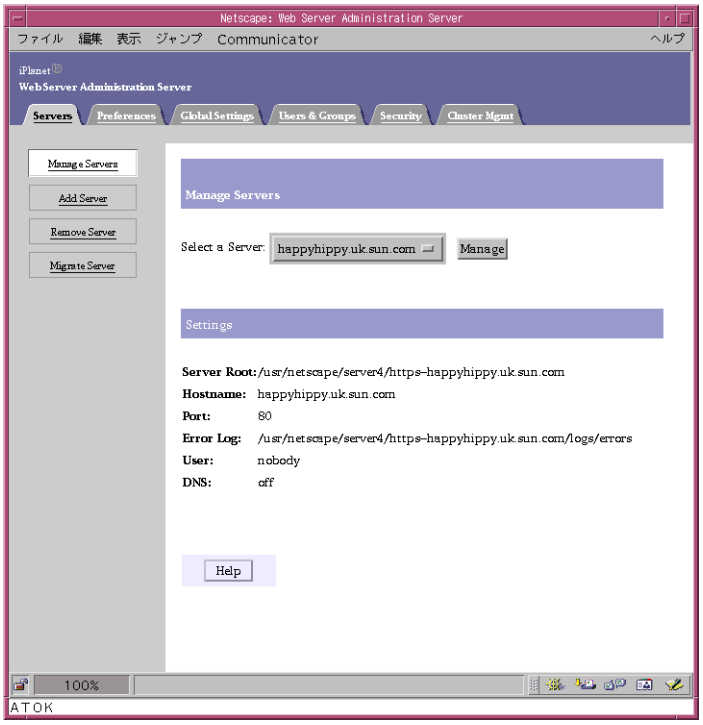
ブラウザで「http://localhost」を開き、iPlanet Web Server が動作していることを確認します。動作している場合は、次のようなメインページが表示されます。

図　1–4　　iPlanet Web Server, Enterprise Edition 4.1



または、Administration Server のコンソールから確認することもできます。

図　1-5　　iPlanet Web Server Administration Server



iPlanet Application Server v6.0 のインストール

- この作業を始める前に、iPlanet Web Server が動作していることを確認してください。
- ルートとしてログオンし、「setup」スクリプトを見つけます。このスクリプトの場所は、システムの分散状況によって異なります。tar ファイルを解凍すると、「setup」ファイルは最上位のディレクトリに配置されます。

```
# cd /cdrom/cdrom0
# cd iAS
# ./setup
```

- 「setup」スクリプトを使って、インストールを始めます。画面に表示される質問に次のように答えて、作業を進めます。

図 1-6 iPlanet Application Server のスクリプトの例

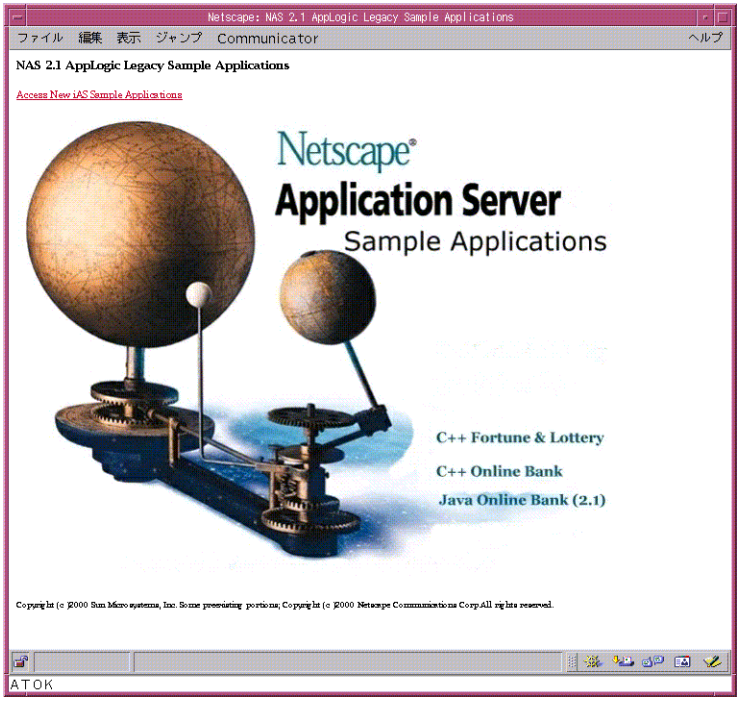
```
Would you like to continue with installation?[Yes]:Yes
Do you agree to the license terms? [No]:Yes
Select the component you want to install [1]: 1
Choose an installation type [2]: 2
Install location [/usr/iplanet/ias6]: /app/ias6
iPlanet Server Products components: Specify the components to install [All]: All
iPlanet Server Family Core: Specify the components to install [1, 2, 3]: 1,2,3
iPlanet Directory Suite components: Specify the components to install [1, 2]: 1,2
Administration Services components: Specify the components to install [1, 2]: 1,2
iPlanet Application Server Suite components: Specify the components you wish to install [1,
2, 3, 4]: 1,2,3,4
Computer name [rainstorm.jcp.co.uk]: rainstorm.jcp.co.uk
System User [nobody]: nobody
System Group [nobody]: nobody
Netscape configuration directory server? [No]:No
Do you want to use another directory to store your data? [No]:No
Directory server network port [389]: 389
Directory server identifier [rainstorm]: rainstorm
administrator ID [admin]: admin
Password:
Password (again):
Suffix [o=co.uk]: o=iplanet.com
Directory Manager DN [cn=Directory Manager]: cn=Directory Manager
Password:
Password (again):
Admin Domain [iplanet.com]: iplanet.com
Administration port [12816]: 12816
Run Administration Server as [root]: root
Product Key: 1111111111-3333333333
Enter the location of your webserver: /app/iws41/https rainstorm.jcp.co.uk
Do you want to enable the user to access the registry and plugin libraries? [y] y
Do you want to continue with the iAS installation? [y] y
Username [admin]: admin
Password:
Password (again):
Do you want to enable I18N support for iAS? [No]:No
Username does not match [No]:Yes
```

注 詳細は、『iPlanet Application Server インストール ガイド』を参照してください。また、これらの設定は後で必要になる場合があるので、メモしておくことをお勧めします。<Return> キーを押すと、デフォルトの設定が適用されます。

iPlanet Web Server と iPlanet Application Server のインストール後の手順

- Application Server が正常にインストールされたことを確認するには、ブラウザで「http:// マシン名 /GXApp」を開きます。「Java Fortune」アプリケーションを選択します。サーブレットによる「ようこそ」のメッセージが表示されたら、Web Server と Application Server は適切に機能しています。『iPlanet Application Server Installation Guide』も参照してください。次に図を示します。

図 1-7 iPlanet Application Server の確認



- インストールを完了したら、すべてのプロセスを停止します。
- ルートとしてログオンします。
- Application Server を停止します。<インストールディレクトリ >/ias/bin/KIVAes.sh stop

```
# cd /app/ias6/ias/bin
# ./KIVAes.sh stop
# ps -ef | grep k.s
```

注　インストール直後にこのスクリプトが機能しない場合は、「ps -ef | grep k.s」を使って iPlanet Application Server のプロセスすべてを表示し、「kill -9 <pid>」ですべてのプロセスを停止します。

- Directory Server を停止します。< インストールディレクトリ >/slapd-< マシン名 >/stop-slapd

```
# cd /app/ias6/slapd-<hostname>
# ./stop-slapd
# ps -ef | grep slap
```

- Web Server を停止します。
  - < インストールディレクトリ >/https-< マシン名 >/stop
  - および < インストールディレクトリ >/https-admserv/stop

```
# ./app/iws41/https-<machine_name>/stop
# ./app/iws41/https-admserv/stop
```

- 上記のスクリプトをすべて実行したら、「ps -ef | grep < インストールディレクトリ >」を使って、すべてのプロセスが停止したことを確認します。実行中のプロセスがある場合は、「kill -9 <pid>」を使って停止します。

SSL 接続ログの有効化

iPlanet Trustbase Transaction Manager で SSL 接続の完全なログをとるには、次の手順に従います。

- kregedit を起動します。

```
..../ias6/ias/bin/kregedit
```

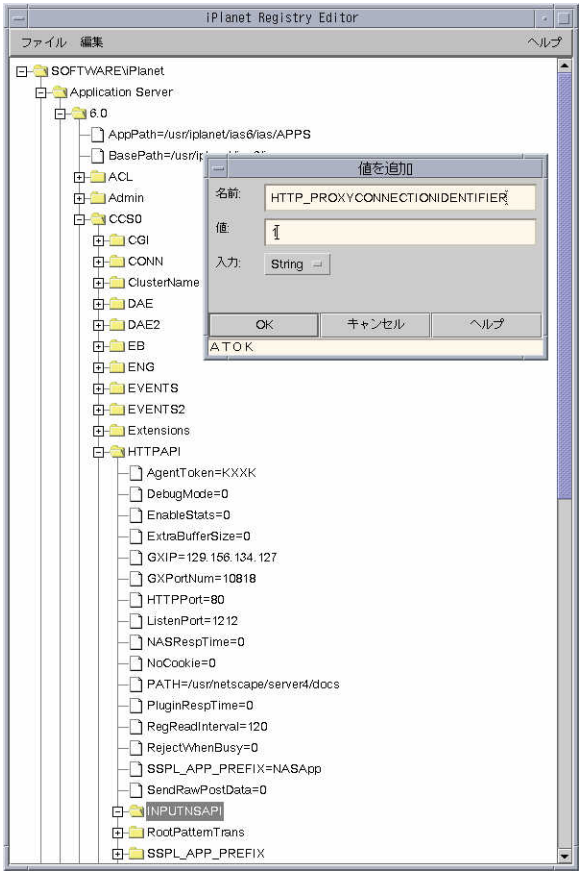
- 次のノードを選択します。

```
SOFTWARE\iPlanet\Application Server\6.0\CCS0\HTTPAPI\INPUTNSAPI
```

- 「編集」メニューの「値を追加」を使って、次の属性に値を追加します。大文字と小文字が区別されるので注意してください。

```
Name=HTTP_PROXYCONNECTIONIDENTIFIER
Value=1
Type=String
```

図 1-8 Kregedit と ConnectionId



- kregedit を終了します。
- この変更は、iPlanet Web Server と iPlanet Application Server を再び起動するまでは適用されません。このインストール手順に従って作業を進めている場合、再起動は 45 ページの「再起動の手順」で行います。

iPlanet Trustbase Transaction Manager のインストール手順

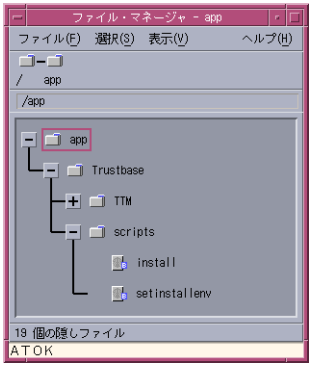
iPlanet Web Server と iPlanet Application Server のインストールが完了したら、iPlanet Trustbase Transaction Manager のインストールに進みます。

インストールには、圧縮された tar ファイルを使います。このインストールプログラムは、Unix Solaris 8 用に設計されています。現在 iPlanet Trustbase Transaction Manager を適切に動作させるには、使用するコンピュータに JDK 1.2 がインストールされていることが必要です。iPlanet Trustbase Transaction Manager を確実にインストールするために、iPlanet Trustbase Transaction Manager の前に JDK 1.2 をインストールすることをお勧めします。JDK 1.2 と iPlanet Trustbase Transaction Manager には、100M バイトのディスク容量が必要です。

- ルートとしてログオンします。
- iPlanet Trustbase Transaction Manager の階層を作成するディレクトリに移動します。
- tar ファイルを現在のディレクトリに解凍します。

```
zcat iTTM-2.2.tar.Z | tar -xvpf -
cd Trustbase/scripts
```

図　1-9　　「install」スクリプトの検索



- Trustbase をインストールする前に、iPlanet Application Server のディレクトリサーバが動作していることを確認します。次に例を示します。

```
cd /app/ias6/slapd-< マシン名 >
./start-slapd
```

- 「install」を実行し、画面の指示に従って作業を進めます。上の例では、「/app/Trustbase/scripts」にこのスクリプトファイルがあります。iPlanet Application Server の場所をたずねられたら、前述の < インストールディレクトリ > を指定します。

```
./install
```

図 1-10 に、iPlanet Trustbase Transaction Manager のインストール方法を示します。

図 1-10 iPlanet Trustbase Transaction Manager のインストール

```
zcat iTTM-2.2.tar.Z | tar -xvpf -'
cd Trustbase/scripts
./install

Copyright (C) 2000 Sun Microsystems, Inc. All rights reserved. Use of
this product is subject to license terms. Federal Acquisitions:
Commercial Software
--- Goverment Users Subject to Standard License Terms and Conditions.

Sun Microsystems, The Sun Logo, iPlanet Trustbase and Java are trademarks
or registered trademarks of Sun Microsystems, Inc. In The United States
and other countries.

Running Installation on sunstorm should I install Trustbase TTM [y/n] y
Trustbase Transaction Manager V2.2 installation script.
Where is your iPlanet Application Server 6.0 installation located?
/app/ias6
Where is your iPlanet Web Server 4.1 documents directory?
/app/iws41/docs
What is the Database User Name which will be used by Trustbase?
tbase
What is the Database Password which will be used by Trustbase?
tbase
On what host is your database stored? sunstorm.jcp.co.uk
On what port is your database running? 1521
On what SID is your database? orcl
What Cryptographic provider do you want to use: NCIPHER or JCP? JCP
On what URL is your local OCSP responder? http://windstorm.jcp.co.uk:8080
What is the AIA of this TC? https://windstorm.jcp.co.uk
```

注 プロクシを別のマシンにインストールする場合、この TC の AIA は、TC ではなくプロクシのホスト名をポイントするようにします。63 ページの「SSL プロクシを別に構成」も参照してください。

- これで iPlanet Trustbase Transaction Manager のインストールが完了しました。次に、ローカル設定と Identrus 設定を構成する作業を行う必要があります。次の各項を参照してください。

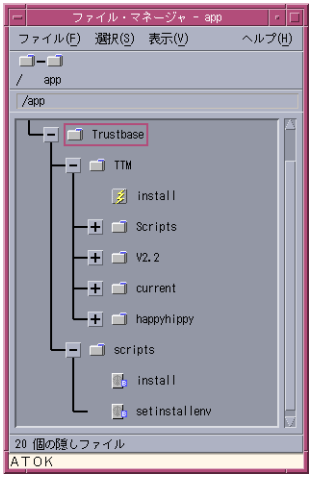
注 <Enter> キーを押すと、デフォルトの設定が適用されます。また、これらの設定は後で必要になる場合があるので、メモしておくことをお勧めします。

インストールの構造

インストールを完了すると、次のディレクトリ構造とサポートファイルが作成されます。

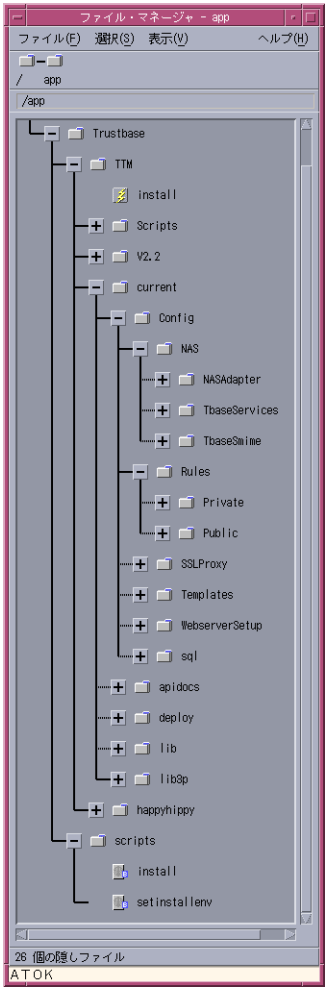
- iPlanet Trustbase Transaction Manager

図 1-11 iPlanet Trustbase Transaction Manager ディレクトリの概要



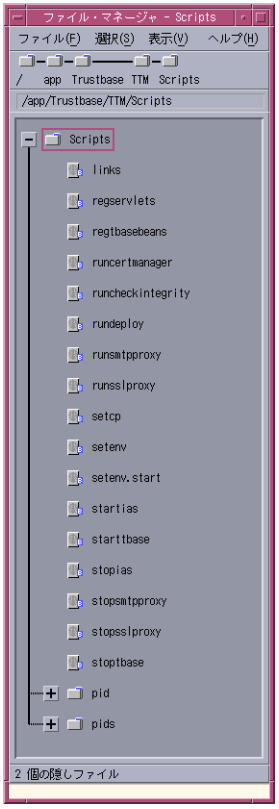
- TTM
  iPlanet Trustbase Transaction Manager には、すべての構成ファイルとライブラリファイル、およびさまざまなデータベースの設定スクリプトを含む SQL ディレクトリがあります。

図 1-12 iPlanet Trustbase Transaction Manager ディレクトリの概要



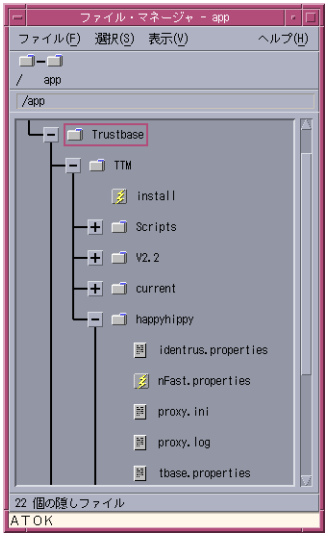
- Scripts
  このディレクトリには、iPlanet Trustbase Transaction Manager の起動と停止に必要なすべてのスクリプトが含まれています。

図 1-13 iPlanet Trustbase Transaction Manager で一般的に使用されるスクリプト



- < マシン名 >
  このディレクトリには、tbase.properties、nFast.properties、identrus.properties、proxy.ini などの、このインストールのすべての設定ファイルが含まれています。これらのファイルは直接の編集はできませんが、このマニュアルで説明する各構成画面から編集できます。

図 1-14 iPlanet Trustbase Transaction Manager の初期化ファイル



- V2.2
  このディレクトリには、すべての TTM バイナリとサポートファイルが含まれています。

その他のディレクトリは必要ありません。

インストール後の手順

iPlanet Trustbase Transaction Manager を最初に起動する前に、さらにいくつかの構成作業を行う必要があります。次にあげる各手順に必要なファイルを見つけるには、前述の「インストールの構造」を参照してください。

- nCipher セキュリティの設定 - 33 ページの「HSM の構成」を参照
- Oracle データベースの設定 - 36 ページの「Oracle データベースの構成」を参照
- Identrus サイト固有の設定 - 39 ページの「Identrus の構成」を参照

HSM の構成

この機能はオプションです。iPlanet Trustbase Transaction Manager をハードウェアセキュリティモジュールなしで設定する場合は、別の暗号化メカニズムを使用できます。ただし、Identrus 準拠のサイトではこの機能が必須になります。

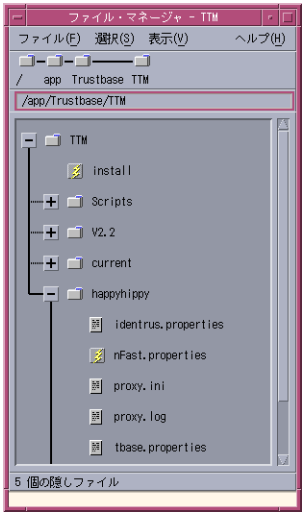
必要要件

iPlanet Trustbase Transaction Manager をインストールするときに、必ず次のように答えてください。

```
What Cryptographic provider do you want to use: NCIPHER or JCP? NCIPHER
```

iPlanet Trustbase Transaction Manager のインストールが完了したら、次の図に示すように、nfast.properties が < インストールディレクトリ >/Trustbase/TTM/< マシン名 > にあることを確認します。

図　1-15　　nfast.properties の検索



nCipher の初期化

共通の鍵データベースを共有する nCipher モジュールの各グループに対し、次の設定作業を行います。

- 付属のマニュアルに従って、nCipher ハードウェアをインストールします。各ユニットが pre-initialisation mode になっていることを確認します。nCipher のマニュアルには、モジュールに「Security World」をインストールし設定する手順が説明されています (nCipher 『KeySafe User Guide』を参照)。
- nFast モジュールでは、ローカルホストからの接続だけが受け入れられます。このため、nFast モジュールは TC の実行に使用するハードウェアドライブ上にあることが必要です。
- nCipher KeySafe ツールを使用して、モジュール上に「Security World」を作成します。
- ほかのモジュールの「Security World」をコピーするには、KeySafe の「restore」機能を使ってこの「Security World」をインストールします。
- nFast サーバが TCP を通じて iPlanet Trustbase Transaction Manager nFast スタブと通信できるように、nFast の起動スクリプトを編集します。この編集を行うには、NFAST_SERVER_PORT 環境変数を定義し、/etc/init.d/nfast にエクスポートする必要があります。iPlanet Trustbase Transaction Manager スタブでは、このポートのデフォルト値は 9000 になっていますが、ほかのポートに設定することもできます。
- これらの設定を行ったら、サーバを再び起動します。nCipher をデフォルトの場所にインストールした場合、入力するコマンドは次のようになります。

```
/app/nfast/sbin/init.d-nfast stop
/app/nfast/sbin/init.d-nfast start
```

注 NFAST_SERVER_PORT の値が 9000 以外の場合は、iPlanet Trustbase Transaction Manager のインストールディレクトリ (/app/Trustbase/TTM/<マシン名 >) にある nFast.properties ファイルを編集して、StandardPort プロパティを一致させる必要があります。

nCipher モジュールの設定と使用

Security World をインストールしたら、次の点を確認します。

- nFast スタブと NCIPHER JCE プロバイダの両方が、nFast.properties ファイルから各設定を読み込むこと。これには次の値が含まれます。
  - AServerAddress。ServerAddress プロパティは、ローカルホストに設定すること。ほかの値が設定されていると、サーバで Unix システムの接続が拒否されることがある。NT システムでは、「localhost」以外のクライアントからの接続が許可されます。デフォルトの値は 127.0.0.1
  - StandardPort。StandardPort　プロパティには、サーバが標準の接続を待機するポート番号が含まれる。デフォルトの値は 9000
  - StandardConnections。StandardConnections プロパティには、nFast モジュールで維持される標準接続の数が含まれる。このプロパティに低い値を設定すると、モジュールの並列処理機能を十分に活用することができない。デフォルトでは、この値はモジュール自体から取得される
  - module.key。module.key プロパティには、ボックス外に保管する際の暗号化キーに使用する、モジュールキーの識別番号が含まれる。標準的なインストールを行い、Security World を適切に設定した場合は、ボックスに次のモジュールキーがインストールされる

    KM0 - ランダムに生成されたモジュールキー。このモジュールキーはエクスポートされない。このキーをデフォルトとして使用した場合、アーカイブしたキーはその特定のモジュールにだけ使用可能。何らかの理由でモジュールを置き換えた場合、すべてのキーを再び生成することが必要

    KM1 - リカバリキーのブートストラップに使用する、よく知られたモジュールキー。このモジュールキーは使用しないこと

    KM2 - Security World のキー。このモジュールキーを使用する

    デフォルトでは、モジュール上に必ず存在するモジュールキーとして KM0（設定値は 0）が使われています。稼動中のシステムでは、この値を常に「2」に設定する必要があります。

```
ServerAddress = localhost
ServerPort = 9000
StandardConnections = 10
PrivilegedConnections = 0
module.key = 2
```

Oracle データベースの構成

TTM と Identrus 拡張機能は、どちらもスキーマがすでに構成されているデータベースへのアクセスを必要とします。インストールには SQL スクリプトが付属しています。これらのスクリプトは、インストール時に指定されたデータベースユーザのテーブルスペースで実行します。次の各項では、ユーザの作成と、そのユーザに対して適切なスキーマを生成する方法について説明します。

- ユーザの生成方法や、定義されているテーブルスペースは、サイトによって異なる場合があります。サイトの DBA に連絡して、指示を受けてください。Trustbase の各インストールでは、1 つの証明書ストアだけを使用します。定義が必要なパラメータは、Oracle のログイン名、Oracle のログインパスワード、Oracle のログインパスワードと同じに設定した PBE パスワード、Oracle のホスト名、Oracle のポート番号、および Oracle SID です。

インストールの必要要件

```
cd /app
cp oracle-jdbc-815.zip /app/Trustbase/TTM/current/lib3p/10
```

iPlanet Trustbase Transaction Manager SQL スクリプトの実行

- 必要であれば、ユーザ名とパスワードを作成するように DBA に依頼します。手順は以下になります。
- Oracle ユーザに切り替え、サーバマネージャを実行します。

```
myhost> su - oracle
Password:
myhost> cd ../Trustbase/TTM/V2.2/Config/sql
myhost> svrmgrl

Oracle Server Manager Release 3.1.5.0.0 - Production

(c) Copyright 1997, Oracle Corporation. All Rights Reserved.

Oracle8i Enterprise Edition Release 8.1.5.0.0 - Production
With the Partitioning and Java options
PL/SQL Release 8.1.5.0.0 - Production

SVRMGR> connect internal
Connected.
```

- データベースで、UTF8 文字セットのサポートを有効にする必要があります。この有効化を行うスクリプトの例を次に示します。

```
SVRMGR> SHUTDOWN;
SVRMGR> STARTUP MOUNT;
SVRMGR> ALTER SYSTEM ENABLE RESTRICED SESSION;
SVRMGR> ALTER SYSTEM SET JOB_QUEUE_PROCESSES=0;
SVRMGR> ALTER DATABASE OPEN;
SVRMGR> ALTER DATABASE CHARACTER SET UTF8;
SVRMGR> SHUTDOWN;
SVRMGR> STARTUP;
```

- iPlanet Trustbase Transaction Manager ユーザを作成します。サイトのポリシーによっては、ユーザ名、パスワード、およびデフォルトのテーブルスペースを変更しなければならない場合があります。

```
SVRMGR> CREATE USER tbase IDENTIFIED BY tbase DEFAULT TABLESPACE USERS
TEMPORARY
TABLESPACE TEMP;
Statement processed.
SVRMGR> GRANT CONNECT TO tbase;
Statement processed.
SVRMGR> GRANT RESOURCE TO tbase;
Statement processed.
SVRMGR> ALTER USER tbase QUOTA UNLIMITED ON USERS;
Statement processed.
SVRMGR> quit
Server Manager complete.
```

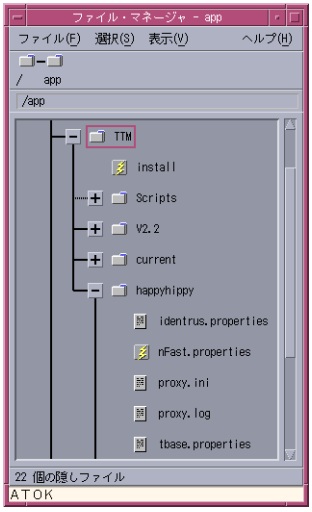
- iPlanet Trustbase Transaction Manager ユーザとして接続し、次のスクリプトを実行します。

```
sunstorm% su - oracle
sunstorm% cd /app/Trustbase/TTM/current/Config/sql
sunstorm% sqlplus
SQL*Plus: Release 8.1.5.0.0 - Production on Fri Sep 22 12:07:11 2000
(c) Copyright 1999 Oracle Corporation. All rights reserved.
Enter user-name: tbase
Enter password:
Error accessing PRODUCT_USER_PROFILE
Warning: Product user profile information not loaded!
You may need to run PUPBLD.SQL as SYSTEM

Connected to:
Oracle8i Enterprise Edition Release 8.1.5.0.0 - Production
With the Partitioning and Java options
PL/SQL Release 8.1.5.0.0 - Production

SQL> @tbase2.sql
```

Identrus の構成

トランザクション コーディネータ (TC) は、iPlanet Trustbase Transaction Manager 内に配置されたすべての Identrus サービスによって構成されます。適切に設定を変更するには、identrus.properties ファイルを編集します。このファイルは、次の図に示すように < インストールディレクトリ >/Trustbase/TTM/< マシン名 > にあります。

図 1-16 identrus.properties ファイルの場所



- 通常、変更しなければならないのは OurAIA と LocalOCSPResponderLocation の場所だけです。次に例を示します。

```
OurAIA = https://rp
LocalOCSPResponderLocation = http://rp:8080
```

- identrus.properties ファイルの例を次に示します。

図 1-17 Identrus.properties の例

```
[CSC]
; OID's for OCSP and TC
TCOID=1.2.840.114021.4.1
OCSPResponderOID=1.3.6.1.5.5.7.48.1

;CaCertificateRole=
;EndEntityCertificateRole=
;SigningCertificateRole=
;RootCertificateRole=

; Local OCSP Responder Communication
SignLocalOCSPRequests=false
OCSPResponderSigningCertificateRole=L1_OCSP_SC
LocalOCSPResponderLocation = identrus_local_resp_url

OurAIA = identrus_our_aia
DNOfAuthority=

; Response Cache Parameters
ApprovedResponseMaxAge=60
ApprovedResponseMaxKeep=60
DebugMode=true
;OCSPRequestorName=CN=KENCO
```

その他の変更できる設定には、次のものがあります。

- OID
  - TCOID。Identrus トランザクションコーディネータの「authority info access」属性の ASN オブジェクト ID (デフォルトを使用可能)。すべての Identrus 証明書にはこの ID があり、Identrus により 1.2.840.114021.4.1 の ID が提供されている
  - OCSPOID。OCSP レスポンダ の「authority info access」属性の ASN オブジェクト ID (デフォルトを使用可能)
- 証明書の役割
  - CaCertificateRole。トランザクションコーディネータの CA 証明書に使用される証明書属性 (デフォルトを使用可能)
  - EndEntityCertificateRole。トランザクションコーディネータの End Entity Signing Certificate に使用される証明書属性 (デフォルトを使用可能)

- SigningCertificateRole。トランザクションコーディネータの Inter Participant Signing Certificate に使用される証明書属性 (デフォルトを使用可能)
- RootCertificateRole。Identrus トランザクションコーディネータにより、Identrus ルートを識別するために使用される証明書属性 (デフォルトを使用可能)

- ローカル OCSP レスポンダの通信
  - SignLocalOCSPRequests。ブール値。未署名のローカル OCSP リクエストではパラメータは「no」、署名済みのローカル OCSP リクエストではパラメータは「yes」
  - OCSPResponderSigningCertificateRole。OCSP 応答の確認に使用される証明書 (signLocalOCSPrequests が true の場合にだけ使用)
  - LocalOCSPResponderLocation。ローカル OCSP レスポンダの URL
- その他の設定
  - OurAIA。この Identrus トランザクションコーディネータのアクセス情報権限 (AIA)
  - DNOfAuthority。Identrus ルートの署名証明書の識別名 (DN)。内部使用専用
- 応答キャッシュパラメータ

  Identrus ルートへ繰り返し呼び出しを行わなくても済むように、自分の証明書のステータスを照会して、一定期間キャッシュに格納できます。ほかの機関にメッセージを送信するときには、このキャッシュされた応答が使用されます。メッセージを受け取った側は、キャッシュされた応答を受け入れるか、自分でルートに問い合わせを行うかを選ぶことができます。信頼カスタマが、キャッシュされた応答が Identrus トランザクションの別の場所で使われていないことを確認したい場合、そのカスタマは送信する OCSP リクエストに臨時応答を使用できます。この臨時応答は、キャッシュした応答を使用しないようにという信号として使用されます。

  キャッシュを行うと、Identrus ルートに繰り返しアクセスする必要がなくなります。キャッシュした証明書のステータスの有効期間は、各機関内に保存されます。また、受信する証明書のステータスの最長有効期限も、各機関内に保存されます。定義が必要なパラメータには、次のものがあります。

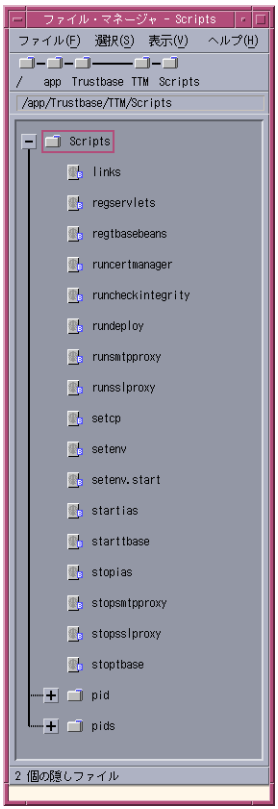
  - ApprovedResponseMaxAge。キャッシュエントリの有効期間 (秒数)
  - ApprovedResponseMaxKeep。提供された応答の受け入れ可能期間 (秒数)
  - DebugMode。内部デバッグのオン / オフ
  - OCSPRequestorName。OCSP レスポンダと通信する際に使う名前。署名が true に設定されている場合 (SignLocalOCSPRequests=true)、この名前は OCSP の署名に使用した証明書の識別名 (DN) に設定することが必要。例では、識別名が共通名 (CN) と組織ユニット (OU) から構成されているため、共通名を識別名として使用

iPlanet Trustbase Transaction Manager の起動

インストールと構成が完了したら、次のディレクトリにあるスクリプトを使って、iPlanet Trustbase Transaction Manager を制御できます。

- /app/Trustbase/TTM/Scripts

図 1-18 iPlanet Trustbase Transaction Manager で一般的に使用されるスクリプト



iPlanet Application Server および TTM のコンポーネントの起動と停止に使用する主なスクリプトは次のとおりです。これらのスクリプトは、Scripts ディレクトリの内部から、ルートとして実行します。

- ./startias
  iPlanet Application Server を起動
- ./starttbase
  iPlanet Trustbase の構成マネージャ、SSL プロクシ、および SMTP プロクシを起動
- ./stopias
- ./stoptbase

この他にも、このディレクトリには次のような便利なスクリプトがあります。

- ./setcp
  このスクリプトを実行すると、CLASSPATH 環境変数が TTM の実行に必要な設定に変更される。このスクリプトは、Scripts ディレクトリ内で、ルートとして、「. ./setcp」を使って実行すること。
- ./runcertmanager
  証明書の構成に使用
- ./runcheckintegrit
  ログの統合性の確認に使用 (135 ページの「Raw_Data と Init_Table のアーカイブ」を参照)

注　Bourne シェル (/bin/sh) では 「. ./setcp」を、c シェル (/bin/csh) では「./setup」を使用します。

停止の手順

システムを停止するには、次の手順に従います。

- ルートとしてログオンします。

```
#!/bin/sh
cd /app/Trustbase/TTM/Scripts
/app/Trustbase/TTM/Scripts/stopias
/app/Trustbase/TTM/Scripts/stoptbase
/app/ias6/slapd-hailstorm/stop-slapd
/app/iws41/https-hailstorm.uk.sun.com/stop
/app/iws41/https-admserv/stop
```

再起動の手順

システムを再起動するには、次の手順に従います。

- ルートとしてログオンし、次のシェルを実行します。

```
#!/bin/sh
/app/ias6/slapd-hailstorm/start-slapd
/app/iws41/https-hailstorm.uk.sun.com/start
/app/iws41/https-admserv/start

cd /app/Trustbase/TTM/Scripts
/app/Trustbase/TTM/Scripts/startias
/app/Trustbase/TTM/Scripts/starttbase
```

再インストール

Trustbase の「install」スクリプトの実行中に行った設定が適切ではなかった場合、すでに行った変更を失うことなく、このスクリプトを再び実行できます。再実行時には、以前に入力した内容が記憶され、デフォルトとして提供されます。

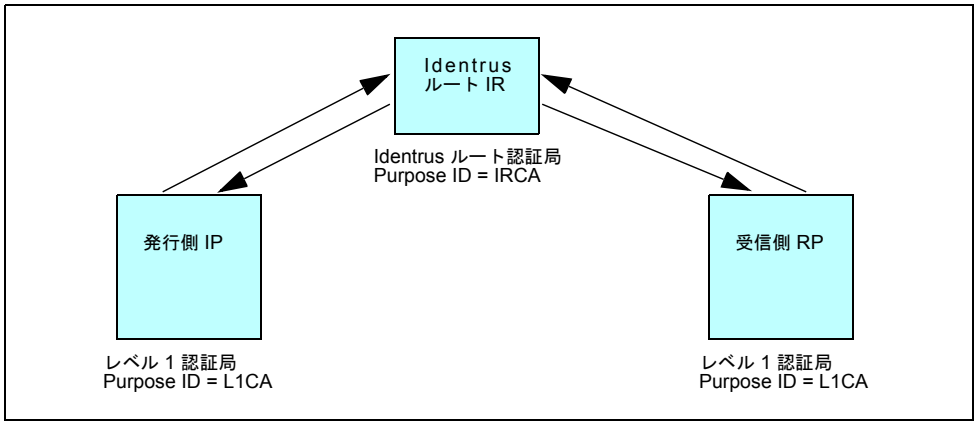
```
sunstorm% cd /app/Trustbase/scripts
sunstorm% ./install
```

再インストールの方法については、iPlanet Application Server、iPlanet Web Server、Oracle、および nCipher のマニュアルを参照してください。

証明書の管理

証明書をインストールする前に、適切な Identrus 認証局によって作成および署名された証明書を持つ CA を設定する必要があります。その後、Certmanager ユーティリティを使って、iPlanet Trustbase Transaction Manager 証明書ストア内の適切な場所に CA 証明書を配置します。

図 1-19 CA 証明書の設定



Certmanager の実行

- CertManager を実行します。

```
# cd /app/Trustbase/TTM/Scripts
# ./runcertmanager
```

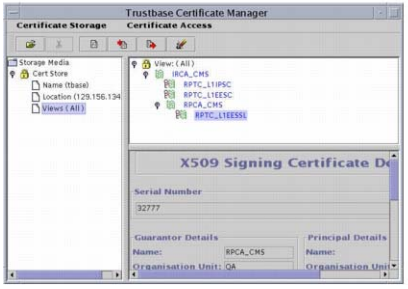
- 次の図に示すように、ストアを開きます。

図 1-20 証明書ストアを開く

PKCS10 リクエストの生成

- 次の図に示すように、Identrus PKI 階層を作成します。

図 1-21 Identrus PKI 階層



- これは、CertManager から、応答を生成する認証局の Web サイトに、生成したデータを貼り付ける作業です。手順は次のとおりです。
  - 「Generate PKCS10 certificate Request (CSR)」を選択して、PKCS-10 証明書のリクエストを生成します。

- 「Add Requested Certificate Response」を選択して、認証局から該当する応答 (PEM 応答と呼ばれることもある) を収集します。

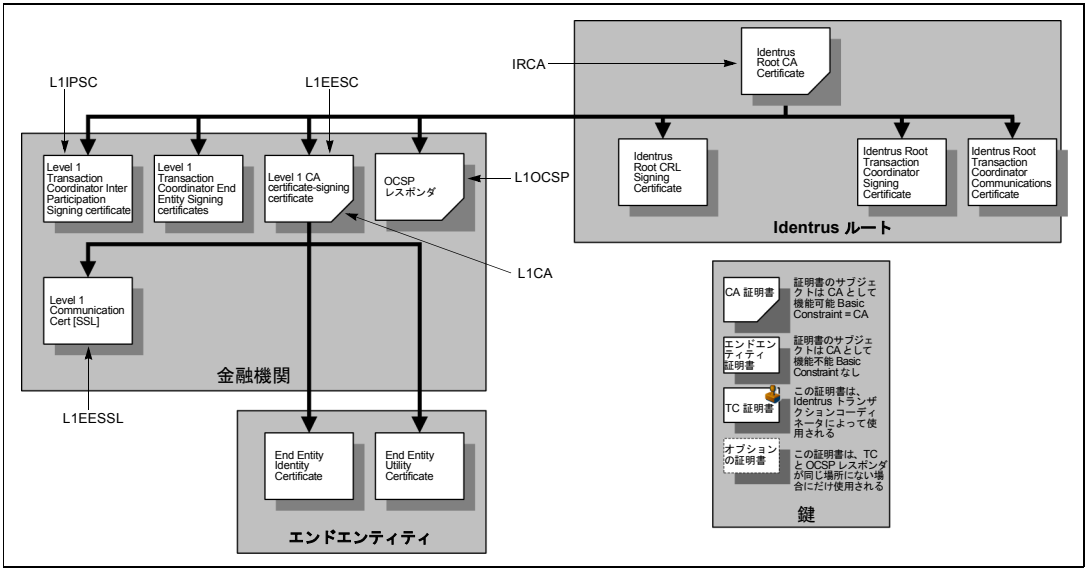
図 1-22 PKCS10 リクエストの生成

注 CertManager の使用方法の詳細は、『ユーティリティガイド』を参照してください。

証明書への属性の割り当て

iPlanet Trustbase Transaction Manager でこれらの証明書を認識するには、CertManager で属性表示を割り当てる必要があります。次の属性表示 / 目的 ID/ 目的属性を定義します。

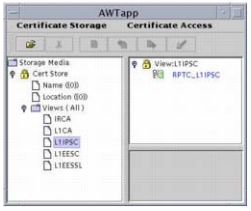
図 1-23 目的属性表示と Identrus PKI 階層



- この場合受け取り側はレベル 1 の CA なので、目的属性 L1CA を証明書 RPCA-CMS に割り当てる。L1CA は CA 証明書の目的 ID である
- 目的属性 L1EESC を証明書 RPTC_L1EESC に割り当てる。L1EESC は、bank/RC または bank/SC のメッセージ署名に使用される目的 ID である
- 目的属性 L1EESSL を証明書 RPTC_L1EESSL に割り当てる。L1EESSL は、bank/RC または bank/SC の SSL 接続に、(サーバとして) 使用される目的 ID である
- 目的属性 L1IPSC を証明書 RPTC_L1IPSC に割り当てる。L1IPSC は、銀行間のメッセージ署名に使用される証明書の目的 ID である
- 目的属性 IRCA を証明書 IRCA_CMS に割り当てる。IRCA は Identrus ルートの証明書である

これは、次の図 1-24 に示すように、iPlanet Trustbase Transaction Manager の CertManager ユーティリティ内に示されています。

図 1-24 目的属性

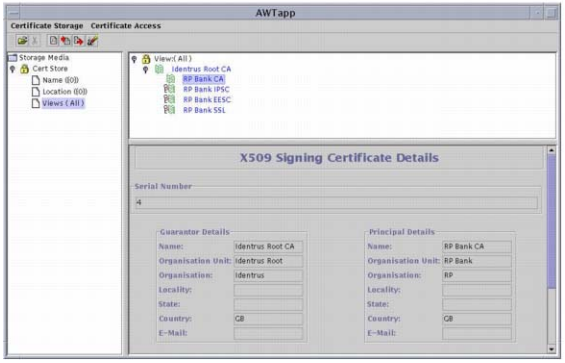


注 証明書の属性表示の作成方法については、『ユーティリティガイド』を参照してください。CertManager の画面では、これは属性表示と呼ばれます。一方、iPlanet Trustbase Transaction Manager 内でトランザクション処理の要件として配置されている場合は、目的属性、または目的 ID と呼ばれます。『ユーティリティガイド』25 ページの「証明書表示」などを参照してください。

Identrus 認可

iPlanet Trustbase Transaction Manager に Identrus メッセージを送信するには、カスタマに対して Identrus 対応のメッセージの送信を可能にする認可を作成する必要があります。次の 3 つの図にこの様子を示します。

図　1-25　　Identrus メッセージの送信を可能にする証明書



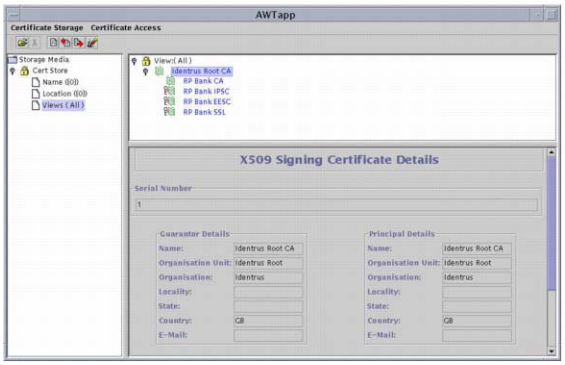
- 「認可」-「証明書の追加」を選択します。

- この例では、発行元の識別名として「CN=Identrus Root CA;OU=Identrus Root;O=Identrus;C=GB」、RP 銀行 CA のシリアル番号として「4」を入力しています。「最大の深さ」は「1」に、「役割」は「Identrus」に設定します。詳細は、80 ページの「証明書の追加」を参照してください。この設定を次に示します。

図 1-26 Trustbase 内での Identrus メッセージを送信可能にする証明書のインストール

ほかの銀行に対しても、Identrus 対応メッセージを送信する認可を作成します。次の 3 つの図にこの様子を示します。

図 1–27 ほかの銀行への Identrus メッセージの送信を可能にする証明書



- 「認可」-「証明書の追加」を選択します。

- 発行元の識別名として「CN=Identrus Root CA;OU=Identrus Root;O=Identrus;C=GB」、RP 銀行 CA のシリアル番号として「1」を入力します。「最大の深さ」は「1」に、「役割」は「Identrus」に設定します。詳細は、80 ページの「証明書の追加」を参照してください。この設定を次の図に示します。

図 1-28 Trustbase 内で Identrus 対応メッセージの送信を可能にする証明書をインストール

最後に、設定を有効にするために iPlanet Trustbase Transaction Manager を再起動します。iPlanet Trustbase Transaction Manager 内で両方の証明書が次の図のようにインストールされていることを確認します。

図 1-29 Trustbase にインストールされた Identrus 対応メッセージ

OCSP レスポンダと署名済み OCSP 応答の確認

メッセージをあるノードに送信すると、応答が返されます。応答の送信者の身元を確認するには、この応答を確認する必要があります。これはオプションの機能で、応答は信用できるという仮定に基づいています。ローカルで使用される OCSP レスポンダでは、通信は保護されているとみなすことができるので、署名の確認を要求されることはまずありません。ただし、OCSP レスポンダがローカルではない場合、または通信が保護されていない場合は、この機能を構成します。

RP 銀行が iPlanet Trustbase Transaction Manager トランザクションコーディネータを持たない IP との通信に失敗する場合は、OCSP レスポンダが必要です。これは、OCSP フォールバックと呼ばれることもあります。

OCSP 応答を確認するには、iPlanet Trustbase Transaction Manager の証明書ストアに署名証明書を入力する必要があります。iPlanet Trustbase Transaction Manager の Oracle 証明書ストアに OCSP の署名証明書をインポートしたら、次のように目的属性を定義します。

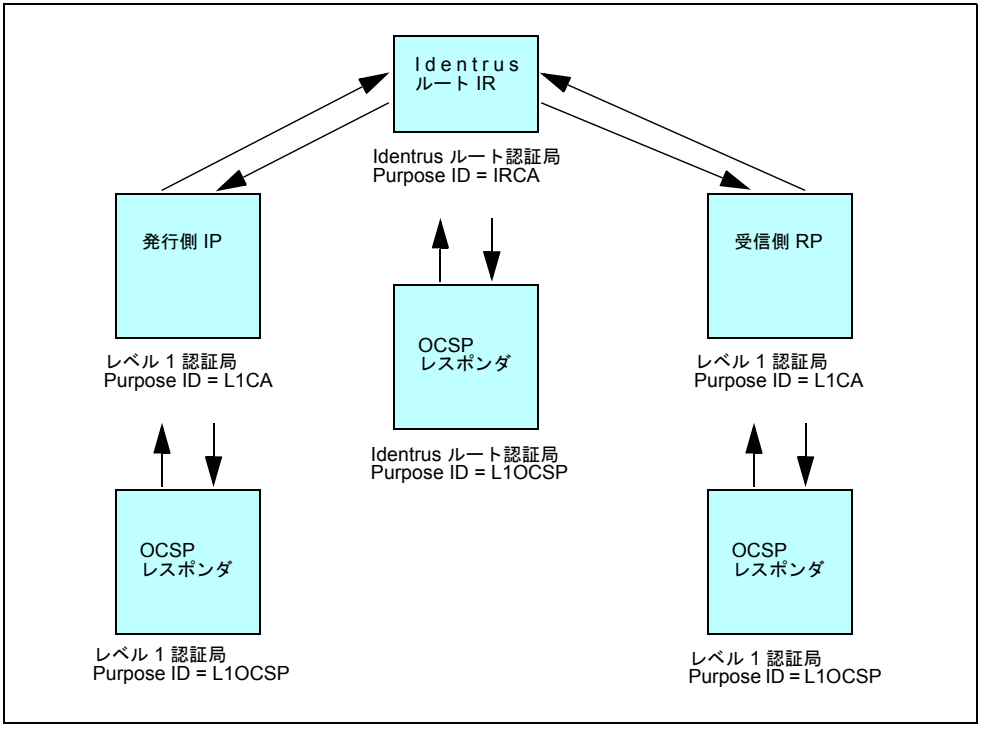
- L1OCSP

iPlanet Trustbase Transaction Manager で署名済み OCSP 応答が受信されると、この属性値のある証明書を使ってデジタル署名が確認されます。

この証明書を入手するには、いくつかの方法があります。

- IRCA 目的属性のある証明書を使用する。ただし、この証明書は IRCA 証明書によって Validation Authority 証明書が発行されている場合にだけ使用可能
- OCSP レスポンダ (Valicert または その他の Identrus 準拠の Validation Authority) から入手する

図 1-30 OCSP レスポンダ



第 2 章

アーキテクチャの構成

iPlanet Trustbase Transaction Manager は、さまざまなハードウェア構成に配置できます。

- 単独もしくはクラスタ状にインストールされている iPlanet Application Server に設定できます。
- DMZ 環境におけるさまざまな設定
- また、ハードウェアセキュリティモジュールを使って設定することもできます。

iPlanet Application Server の構成

iPlanet Application Server は多様な構成で使用でき、次のような要素に対するさまざまな条件をサポートできます。

- スケーラビリティ
- スループット
- フェイルオーバー

iPlanet Trustbase Transaction Manager は、これらの機能を活用できるように設計されており、次の 2 つの主な構成においてテスト済みです。

- 単独の iPlanet Application Server
- クラスタ状の iPlanet Application Server

単独の iPlanet Application Server は、トラフィック量の少ないテスト段階の Transaction Manager 環境でよく使われる構成です。この構成は標準的な iPlanet Trustbase Transaction Manager のインストールとみなされ、『iPlanet Application Server Installation Guide』に説明されている内容以外に、特別なオプションの構成は必要ありません。次に示すのは、推奨される iPlanet Application Server の設定です。

- ホストマシンの各 CPU に単独の KJS
- KJS あたり最低 8、最高 64 のスレッド

iPlanet Trustbase Transaction Manager は、一般的に CPU に結合された処理環境です。つまり、CPU の数を増やしたり、高速の CPU をインストールすると、パフォーマンスが向上します。

iPlanet Trustbase Transaction Manager では、広範囲にわたって Oracle データベースが使用されます。Oracle では、CPU とディスク容量に対する負荷が大きくなります。可能であれば、Oracle を iPlanet Trustbase Transaction Manager とは別のコンピュータに配置してください。

クラスタ状にインストールされた iPlanet Application Server では、単独の iPlanet Application Server で iPlanet Trustbase Transaction Manager を実行する場合に比べ、スケーラビリティ、スループット、およびフェイルオーバーが向上します。クラスタ状の iPlanet Application Server をインストールする場合には、まず次の点を考慮する必要があります。

- iPlanet Application Server を実行する各マシンに nCipher HSM を装備可能かどうか。これは Identrus に準拠するために必要
- クラスタ状の iPlanet Application Server 環境では、負荷が限界状態になると応答が遅くなることがある

注　パフォーマンスの調整と効率的な配置の詳細は、次を参照してください。

- iTTM (このガイド)。接続の数については第 6 章、「SSL」を、キャッシュにかかる時間については 39 ページの「Identrus の構成」を参照
- 『Oracle 8i Administrators Reference Manual』の第 2 章
- SQL の調整については『Oracle 8i Programmers Guide』
- サーバのパフォーマンスの調整については『iPlanet Web Server 4.1 Administration Guide』
- アプリケーションの配置については『iPlanet Application Server 6.0 Administration and Development Guide』

DMZ の使用

iPlanet Trustbase Transaction Manager では、2 つのファイヤウォール間のプロクシマシンを使用して作成した非武装セグメント (DMZ) 内にアプリケーションサーバを配置するのが、一般的なアーキテクチャモデルです。この構成では、外部のユーザが、認証や認証の必要要件を避けるために、アプリケーション構成ロジックに直接アクセスしたり、ロジックを変更したりすることを防止できます。

DMZ の主ファイヤウォールは、SSL アクセスと SMTP アクセスをサポートするために、2 つの非認証オープンポートを提供する必要があります。これらのポートは、一般的に次のとおりです。

- SSL - ポート 443
- SMTP - ポート 25

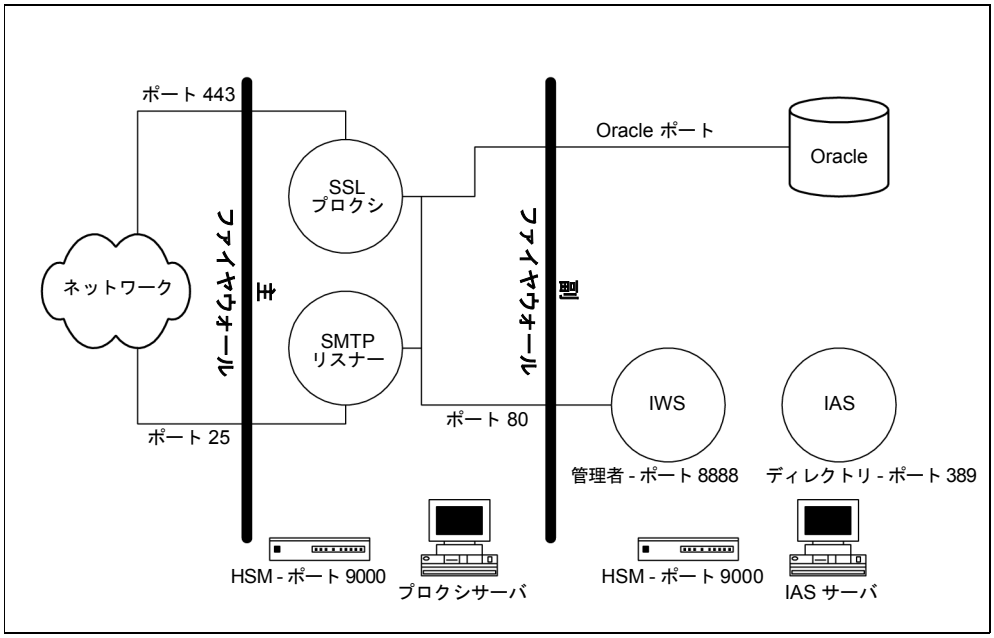
このファイヤウォールの後ろには、SSL プロクシ、SMTP リスナー、および iPlanet Web Server を実行する単独のマシンがあります。副ファイヤウォールには、DMZ マシン専用に構成したオープンポートが 3 つあります。これらの 3 つのポートは次のとおりです。

- iPlanet Application Server ディレクトリポート 389
- iPlanet Web Server
  - HTTP - ポート 80
  - 管理者 - ポート 8888
- Oracle

注 Oracle では多くのポートが使用されます。詳細は、Oracle DBA に問い合わせてください。

SSL プロクシと SMTP プロクシは、副ファイヤウォールの後ろにある iPlanet Web Server との通信に HTTP ポートを使用します。SSL リスナーと SMTP リスナーは、接続情報の格納と構成の受信に、Oracle ポートを使用します。次の図にアーキテクチャを示します。

図 2–1 DMZ アーキテクチャ



この構成では、システム管理者が SSL 証明書なしで HTML ベースの構成画面を使うことができます。構成管理メカニズムはユーザ名とパスワードに基づく認証方式で保護されているため、この方法を使っても認証メカニズムが回避されることはありません。

注 デフォルトの構成では、すべてが単独のマシンで実行されます。iPlanet Application Server 6.0 と iPlanet Web Server 4.1 をインストールすると、ディレクトリサーバがインストールされます。このディレクトリサーバのデフォルトポートは 389、管理者ポートは 8888 になります。

マシンのインストール

場合によっては、一部のコンポーネントソフトウェアを別のマシンにインストールしなければならないことがあります。次の表に、可能な組み合わせをまとめます。

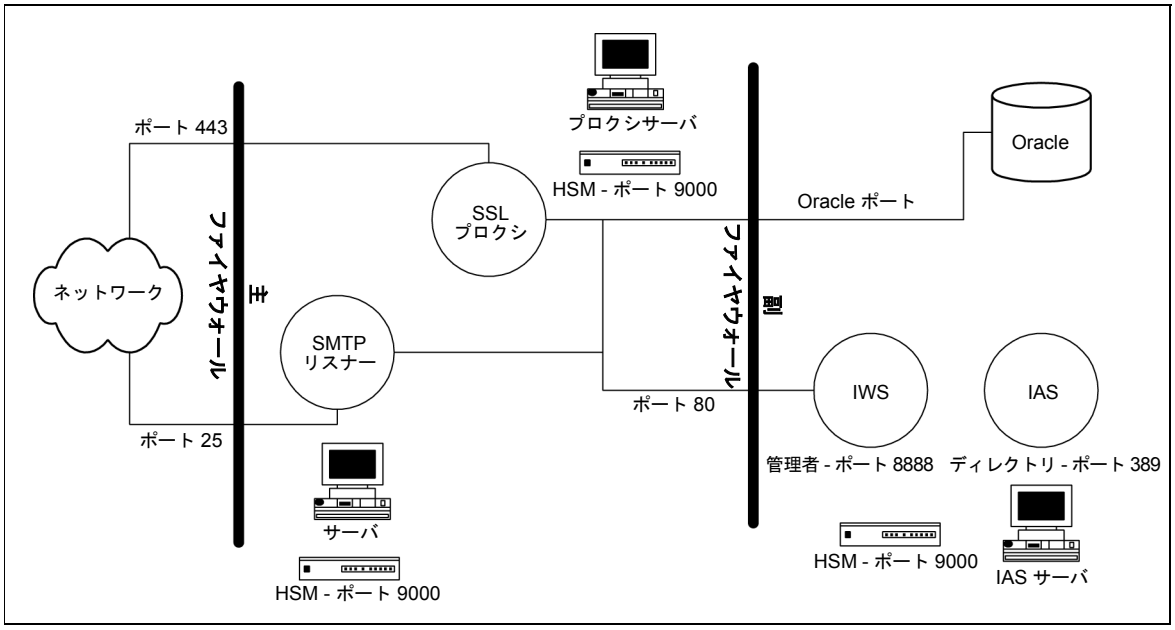
表 2-1 可能なマシンのインストール

分離してインストールする製品のコンポーネント	別のマシンへのインストールの可否	考慮すべき事項
iTTM を IAS から分離	X	IAS と IWS を別のマシンにインストールする場合は、iTTM と IAS が必ず同じマシンにインストールされていること
IWS を IAS から分離	○	Configurator Plug-in に関するセクションを参照 `http://docs.iplanet.com/docs/manuals/ias.html`
Oracle を iTTM から分離	○	36 ページの「Oracle データベースの構成」を参照
SSL プロクシを iTTM から分離	○	63 ページの「SSL プロクシを別に構成」を参照
SMTP プロクシを iTTM から分離	○	65 ページの「SMTP プロクシを別に構成」を参照
IAS をほかの Web サーバとともにインストール	サポートなし	

SSL プロクシを別に構成

場合によっては、SSL プロクシを別のマシンに配置したほうが便利なことがあります。

図 2-2 分離した SSL プロクシの DMZ アーキテクチャ



この構成を使用する場合、システム管理者は、nCipher ボックスが nCipher の Security World を共有するように、nCipher の Security World を構成する必要があります。また、適切な iPlanet Trustbase Transaction Manager ソフトウェアを両方のマシンに確実にインストールするには、独立したスクリプトを使用する必要があります。手順は次のとおりです。

1. インストールディレクトリ (/app) から「tar -cvf Trustbase.tar Trustbase」と入力して、完了した単独マシンのインストールの tar を作成します。
2. この tar ファイルを、プロクシを実行するコンピュータに解凍します。解凍には、元のコンピュータと同じインストールディレクトリ構造 (/app) を使用します。この新しいマシンには、iPlanet Trustbase Transaction Manager、iPlanet Web Server、または iPlanet Application Server をインストールしないでください。

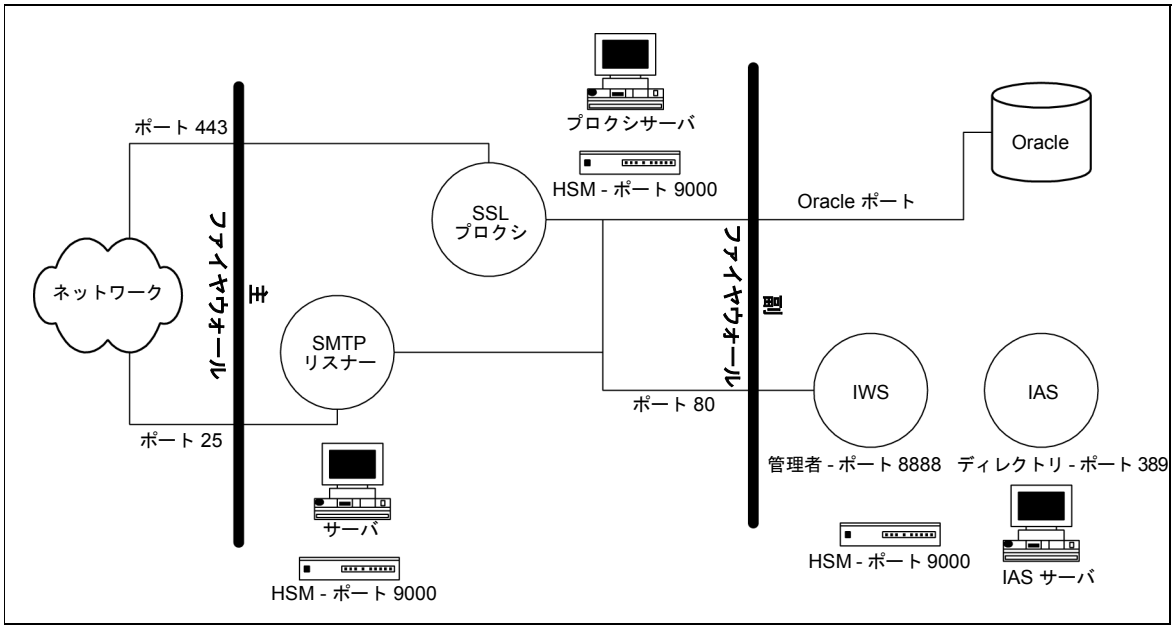
3. < 新規インストールディレクトリ >/Trustbase/TTM に移動して、コンピュータのホスト名であるディレクトリの名前を変更し、この名前が新規ホストのものであることを確認します。< 新規インストールディレクトリ > が異なる場合は、< 新規インストールディレクトリ >/Trustbase/TTM/Scripts.setenv ファイルを編集して、TBASE_INSTALL と TBASE_HOME のディレクトリ名を < 新規インストールディレクトリ > に変更します。
4. プロクシを独自に起動するには、この新しいホスト名のディレクトリの < 新規インストールディレクトリ >/Trustbase/TTM/Scripts を使用します。./runsslproxy スクリプトを実行します。
5. SSL プロクシの元のホストで、< インストールディレクトリ >/Trustbase/TTM/Scripts 内の ./starttbase スクリプトを編集し、SSL プロクシへの参照を削除します。./stoptbase スクリプトに対しても、同様の作業を行います。

プロクシから iPlanet Trustbase Transaction Manager へは通信が行われますが、その逆は行われないので、管理コンソールから構成設定を変更する必要はありません。すべてのエンドユーザの、すべての証明書に対するトランザクションコーディネータの「AIA」フィールドも、SSL プロクシの新しいホストをポイントするようにします。

SMTP プロクシを別に構成

場合によっては、SMTP プロクシを別のマシンに配置したほうが便利なことがあります。

図 2-3 分離した SMTP プロクシの DMZ アーキテクチャ



この構成を使用する場合、システム管理者は nCipher ボックスが nCipher の Security World を共有するように、nCipher の Security World を設定する必要があります。また、適切な iPlanet Trustbase Transaction Manager ソフトウェアを両方のマシンに確実にインストールするには、独立したスクリプトを使用する必要があります。手順は次のとおりです。

1. インストールディレクトリ (/app) から「tar -cvf Trustbase.tar Trustbase」と入力して、完了した単独マシンのインストールの tar を作成します。
2. この tar ファイルを、プロクシを実行するコンピュータに解凍します。解凍には、元のコンピュータと同じインストールディレクトリ構造 (/app) を使用します。この新しいマシンには、iPlanet Trustbase Transaction Manager、iPlanet Web Server、または iPlanet Application Server をインストールしないでください。

3. < 新規インストールディレクトリ >/Trustbase/TTM に移動して、コンピュータのホスト名であるディレクトリの名前を変更し、この名前が新規ホストのものであることを確認します。< 新規インストールディレクトリ > が異なる場合は、< 新規インストールディレクトリ >/Trustbase/TTM/Scripts.setenv ファイルを編集して、TBASE_INSTALL と TBASE_HOME のディレクトリ名を < 新規インストールディレクトリ > に変更します。
4. < 新規インストールディレクトリ >/Trustbase/TTM/Scripts/runsmtpproxy スクリプトを編集して、ローカルホストを iPlanet Trustbase Transaction Manager をインストールしたマシンのホスト名に変更します。次に例を示します。

```
#!/bin/sh
. ./setcp
ulimit -n 128
echo $$ > pids/runsmtpproxy.pid
cd $TBASE_INSTALL
exec java uk.co.jcp.tbaseimpl.smtp.server.SmtpServer -debug 6 -url
http://hailstorm.uk.sun.com/NASApp/TbaseSmime/SmimeServlet -timeout
120000
```

5. プロクシを独自に起動するには、この新しいホスト名のディレクトリの < 新規インストールディレクトリ >/Trustbase/TTM/Scripts を使用します。./runsmtpproxy スクリプトを実行します。
6. SMTP プロクシの元のホストで、<インストールディレクトリ>/Trustbase/TTM/Scripts 内の ./starttbase スクリプトを編集し、SMTP プロクシへの参照を削除します。./stoptbase スクリプトに対しても、同様の作業を行います。

HSM サポート

Identrus を使用するには、iPlanet Trustbase Transaction Manager が共有鍵の暗号化ができる nCipher HSM の使用に依存しています。iPlanet Trustbase Transaction Manager と nCipher ハードサーバ処理の通信は、TCP/IP ソケットを使って行われます。nCipher セキュリティ機能の一部として、ハードサーバはローカルマシンからの接続だけを受け入れます。つまり、iPlanet Trustbase Transaction Manager 処理を実行する各ローカルマシンで nCipher HSM を使用できなくてはなりません。iPlanet Trustbase Transaction Manager で nCipher HSM を使用する場合のデフォルト設定は次のとおりです。

- HSM がソケットモードであること。nCipher のマニュアルを参照
- ハードサーバの構成と Trustbase.properties ファイルで、ポート 9000 が構成されていること。第 1 章、「インストールワークシート」を参照

iPlanet Trustbase Transaction Manager の各インストール (プロクシと iPlanet Application Server の処理) では、鍵マテリアルは暗号化されて共有 Oracle レポジトリに格納されます。デフォルトでは、nCipher HSM でこの鍵マテリアルを共有することはできません。したがって、nCipher の Security World ソフトウェアを使って、共有できるように構成する必要があります。スマートカードにあるモジュールキーを使って鍵を共有する処理については、『iPlanet Trustbase Transaction Manager インストールガイド』を参照してください。

nCipher の Security World 構成では、インストールの HSM デバイスを追加または置き換えることができます。iPlanet Trustbase Transaction Manager の鍵マテリアルを使用できる HSM を装備した新しいマシンを構成するには、次の手順に従います。

- 新しい HSM デバイスが新しいマシンに接続されていることを確認します。
- 元のインストールからの Security World ファイルを、新しいマシンにコピーします。
- 元の HSM インストールからのスマートカードを使って、新しいインストールにモジュールキーを生成します。

この作業の詳細は、nCipher KeySafe 製品のユーザーズマニュアルを参照してください。

第 3 章

ログオン

iPlanet Trustbase Transaction Manager のインストールを完了したら、ログオンして、さまざまな構成オプションを検討できます。これらのオプションには、認可サービス、ユーザ、役割、証明書などがあります。ログのオプションを定義し、SSL トランスポート構成のオプションを選択し、サービスを配置し、テンプレートを使って構成操作のオプションを定義します。

構成管理の概要

iPlanet Trustbase Transaction Manager インストール内のアイテムを確認または編集する場合、管理者は HTML のログオンフォームを使ってログインする必要があります。

```
http://< ホスト名 >/NASAdapter/logon.html
```

管理者は、適切なホーム画面から、さまざまな構成操作を行うことができます。ホーム画面でログアウトを選ぶとセッションが終了されるため、構成画面を使うには再び認証を受ける必要があります。セッションからログアウトすると、iPlanet Trustbase Transaction Manager から管理認証のコンテキストが削除されるため、ブラウザにキャッシュされた HTML 画面を使って iPlanet Trustbase Transaction Manager を構成することはできません。ログインしたセッションで数分にわたって何も操作を行わないと、セッションは自動的に中止されるため、システムにアクセスするにはログイン画面を使って再び認証を受ける必要があります。セッションがタイムアウトになった後に構成画面のボタンをクリックすると、ユーザのブラウザにサーバエラーが返されます。この場合も、iPlanet Trustbase Transaction Manager に再びログインする必要があります。

ログオン画面

iPlanet Trustbase Transaction Manager は、1 つの標準的なユーザ名が作成された状態でインストールされます。すべての管理者は、次の図に示すログオン画面を使ってシステムにアクセスします。

図　3-1　　ログオン画面

ユーザ名とパスワードは次のように設定されています。この設定は、適切なメニューオプションを選択することによって変更できます。詳細は、79 ページの「ユーザを役割に追加」を参照してください。

```
ユーザ名 Administrator
パスワード Administrator
```

注　このパスワードは、Solaris マシンのルートパスワードと同じ役割を持っています。なくさないように注意してください。

構成オプション

次のオプションが用意されています。

- 認可 - 役割、サービス、ユーザ、および証明書を定義

- ログ - システム内のメッセージのクエリ、構成、および表示に使用

- SSL - 使用する証明書ストア設定、サーバのアドレスとポート、SSL レイヤで使用する暗号化アルゴリズム、および同時に許可する接続数を定義することによって、プロクシを構成

- サービス - サービスの登録と配置に使用

- テンプレート - システムに受け入れ可能なメッセージプロトコルを定義

- ログオフ - 構成画面の終了に使用

第 4 章

認可

認可は、役割を割り当てることによってサービスを認証するという考えに基づいて行われます。証明書を役割にリンクすることによって、サービスのある面を認証します。各証明書には、証明書階層内の任意の下位レベルで認証を受けられるように、識別名と役割が割り当てられます。

概要

iPlanet Trustbase Transaction Manager の認可機能を使って、身元不明のユーザがサービスにアクセスするのを防ぐことができます。認可の管理を行う画面では、一連の既知のユーザを編集し、アクセス可能なサービスを指定できます。認可画面で変更を行うと、iPlanet Trustbase Transaction Manager の認可データベースにすぐにその変更が反映されます。

iPlanet Trustbase Transaction Manager は、新規のユーザセッションを開始するリクエストすべてに対し、認可チェックを行います。つまり、ユーザがシステムにログオンしたときや、CSC が受信されたときにチェックが行われます。このチェックにより、ユーザ名または証明書が役割にマップされます。この役割は、リクエストとともにシステム内で送受されます。ルータがサービスを呼び出す前に、認可データベースがチェックされ、役割が該当サービスへのアクセスを許可されているかどうかが確認されます。アクセスが許可されている場合は、処理が許可されます。許可されていない場合は、ルータにより認可エラーが記録され、リクエストは拒否されます。

認証パラメータの編集が必要な機能へは、次に示す「認可」メインメニューからアクセスできます。

図　4-1　　「認可」メインメニュー

ユーザに対するサービスへのアクセスの認可

ユーザに対して特定のサービスへのアクセスを認可する作業は、複数の段階に分けて行います。各段階は次のとおりです。

- 役割の定義 - ユーザを識別するグループを作成します。
- ユーザを役割に追加 - グループのメンバーになるユーザを識別します。
- 役割をサービスにマップ - 特定の役割を持つユーザに対し、サービスの使用を認可します。
- 各役割に証明書を割り当て

次の各項では、各段階について詳しく説明します。

役割の定義

メインメニューから「役割の追加」を選択すると、次の項目を含むフォームが表示されます。

- 名前 - 新規役割のテキストラベル
- 説明 - 役割の説明。テキストを自由に入力できる。認可作業には必要ないが、特定の役割の説明に使用できる
- アクティブ - オフになっていると、役割とサービスのリンクが正しい場合でも、ルータにより認可拒否の応答が返される

フォームを送信すると、認可テーブルがすぐに更新されます。新規役割を追加した後は、「認可」メニューの「すべての役割」オプションを使用して最新の情報を表示できます。「すべての役割」オプションでは、既存の役割を選択して、値を編集できます。デフォルトでは、iPlanet Trustbase Transaction Manager には 3 つのあらかじめ設定された役割があり、特定のユーザにマップされています。

図 4-2 デフォルトの役割のリスト

- ADMINISTRATOR - すべての構成画面に管理者としてアクセス可能な役割
- NoRole - アクティブではない役割で、現在内部のみで使用。これは、「アイテム」に何の役割も割り当てない場合に使用
- Identrus - Identrus サービスへのアクセスが可能な役割。現在、主なサービスとしては IdentrusCSCService がある。このサービスは、証明書のステータスの確認を行い、すべての確認、検証、完全性、および認可の基盤を形成する

注 iPlanet Trustbase Transaction Manager には、「NoRole」というデフォルトの役割があります。これは iPlanet Trustbase Transaction Manager サービス内部で使われます。編集または削除しないでください。

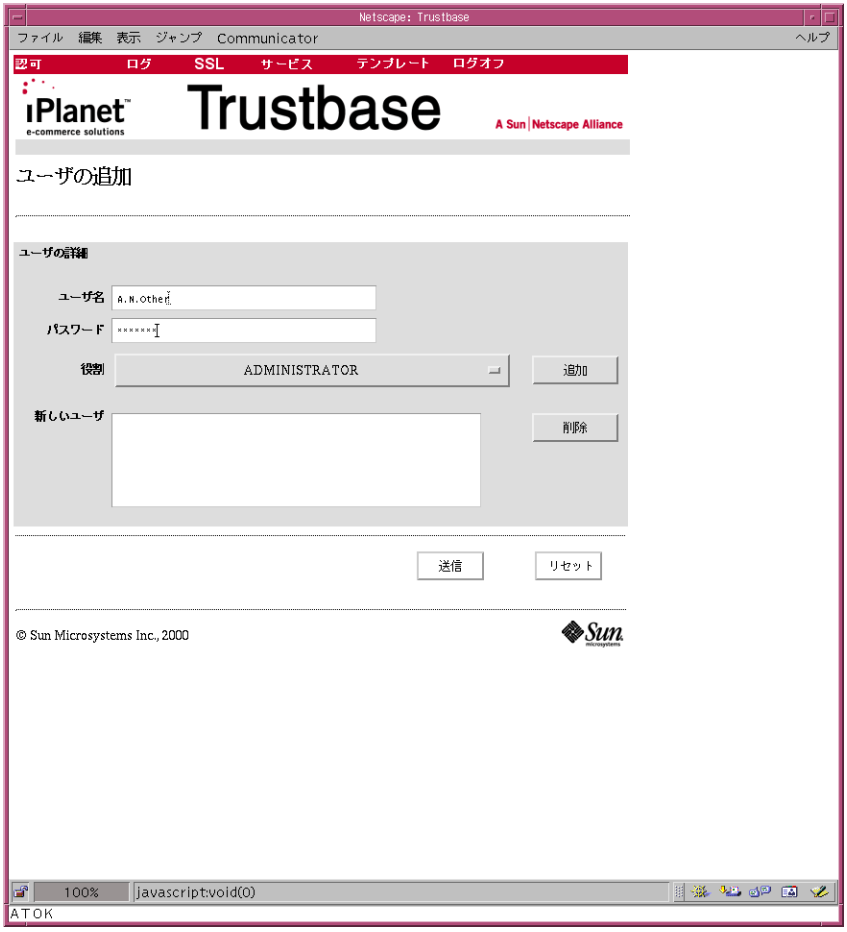
ユーザを役割に追加

ユーザの識別には、次のどちらかを使用できます。

- ユーザ名とパスワード
- 証明書

ユーザ名とパスワードによる認可は、iPlanet Trustbase Transaction Manager の操作管理で一般的に使用されます。この方法では、システムにログオンして、このマニュアルで説明している各管理画面を操作できます。

図 4-3 新規ユーザの追加



新規ユーザは、「認可」ホームページの「ユーザの追加」ボタンを使って追加できます。各ユーザに対し、次の項目を入力します。

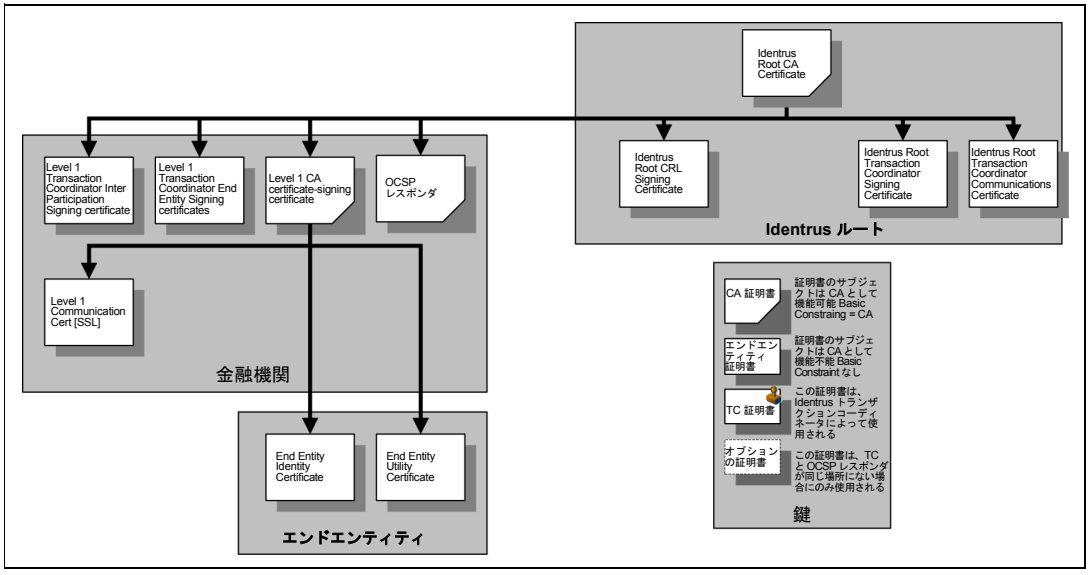
- ユーザ名
- パスワード
- 役割 - 既存の役割からだけ選択可能

複数のユーザを追加してから、フォームを送信することができます。ユーザを追加すると、認可テーブルですぐにアクティブになり、ユーザは割り当てられた役割を使用できるようになります。

証明書の追加

Identrus メッセージには、証明書による認証が使われます。第三者が iPlanet Trustbase Transaction Manager を使用するには、認可システムに証明書の詳細が入力されていることが必要です。iPlanet Trustbase Transaction Manager では、実際の証明書の代わりに親証明書を使用できるため、認可テーブルにすべての既知の証明書を入力しなくても済みます。

図 4-4 Identrus PKI 階層



Identrus PKI 階層内では、レベル 1 CA によって発行された End Entity Identity Certificate は、iPlanet Trustbase Transaction Manager へのリクエストに署名するために信頼カスタマ (RC) によって使用されます。Level 1 Transaction Manager Inter-Participant Signing Certificate は、証明書のステータスの確認時にさまざまな iPlanet Trustbase Transaction Manager 間で作成されたリクエストに署名するために使用されます。

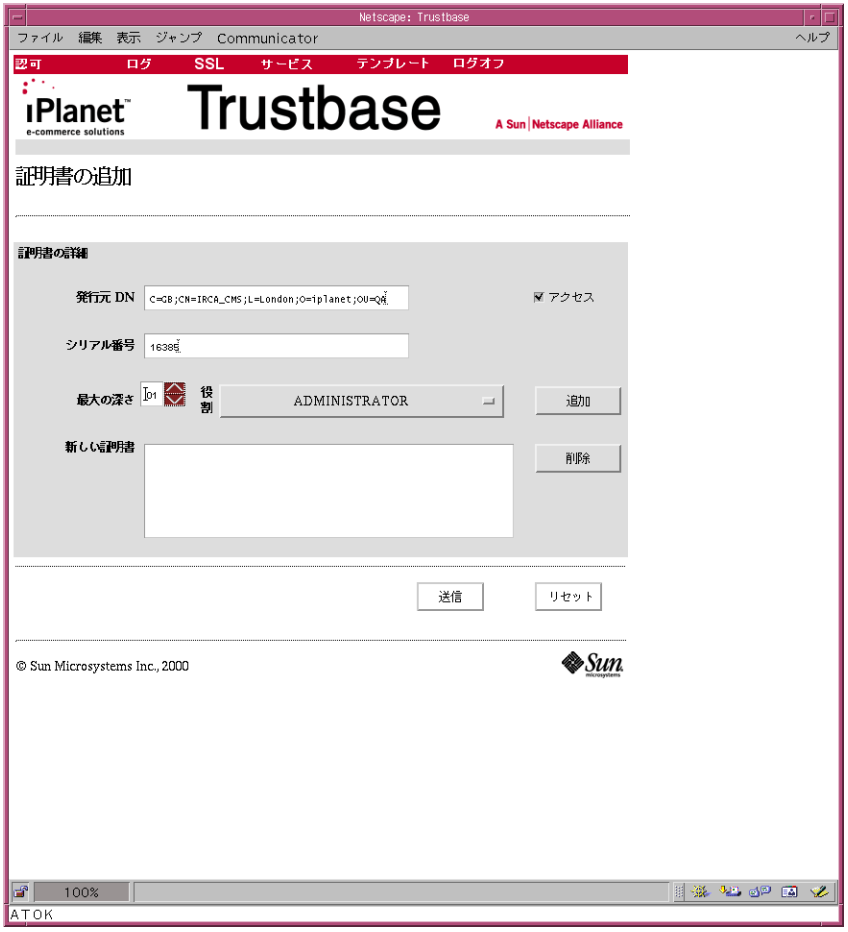
Identrus 処理の完全なセットは、認可システムに単独の証明書を配置することによって認可を受けることができます。この証明書は Identrus ルート CA 証明書 (Identrus Root CA Certificate) と呼ばれます。ルート CA 証明書には、「最大の深さ」の値として「2」を入力します。これは、ルート CA 証明書から下位 2 レベルまでに発行された証明書 (Level 1 Transaction Manager End Entity Signing Certificate と Inter-Participant Signing Certificate) が、Identrus ルート CA 証明書と同じ役割にマップされることを意味します。

証明書に基づいて認可を追加するには、「認可」メインページの「証明書の追加」を選択します。表示されるフォームでは、各証明書に対して次の情報が要求されます。

- 発行元 DN - このフィールドでは大文字と小文字が区別されるため、大文字と小文字を間違えて DN 情報を入力すると、証明書の認可が拒否される
- シリアル番号
- 最大の深さ - この証明書と、この役割を使うことのできる子証明書間のチェーンの最大の長さ
- 役割 - 定義済みの役割のリストから選択

- アクセス - この証明書をアクティブにするにはオンにする

図 4-5 証明書の追加



「アクセス」チェックボックスをオンにすると、継承した認可を明示的に上書きできます。つまり、「アクセス」がオフで認可テーブルに明示的なエントリのあるものを除き、多くの発行済みの証明書を認可するのに親証明書を使うことができます。このメカニズムは、CA によって破棄される前に証明書を保留する期間が必要な場合に便利です。

役割をサービスにマップ

役割を作成し、一連のユーザを役割にマップしたら、最後に役割によるアクセスが可能な一連のサービスを定義します。

各サービスへアクセスできるのは、1 つの役割だけです。このため、既存の認可メカニズムを編集する前に、認可マッピングに関して多少の設計と検討を行うことが必要です。デフォルトでは、iPlanet Trustbase Transaction Manager には次の役割からサービスへのマッピングが含まれています。

- このガイドで説明している構成機能を使って、インストールを構成するユーザ。このユーザは「Administrator」という役割にマップされる
- 許可された Identrus サービスにアクセスする End Entity Certificate を持つユーザ。このユーザは「Identrus」という役割にマップされる

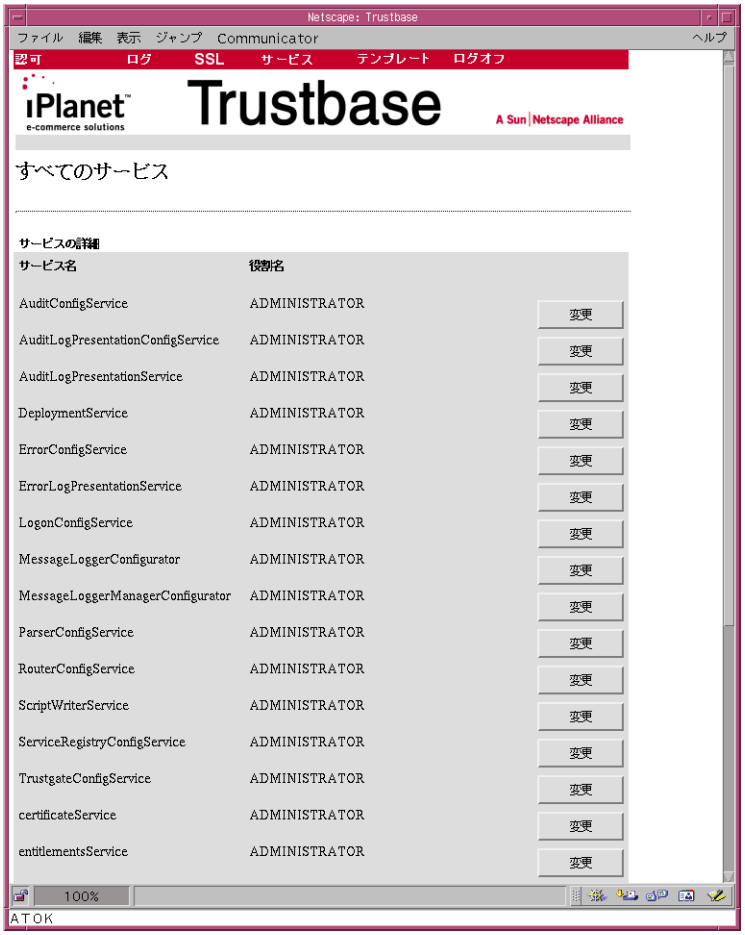
新しいサービスを役割にマップするには、「認可」メインメニューの「サービスの追加」を選択します。フォームでは、次の情報が必要です。

- サービス名 - tbase.properties ファイルに記載されている、サービスの略名
- 役割 - 役割の名前

フォームの下部では、サービスから役割への複数のマッピングを追加できます。追加が完了したら、フォームを送信します。認可データベースにマッピングを送信すると、すぐに有効になります。

サービスから役割への既存のマッピングを編集するには、「認可」メインメニューから「すべてのサービス」を選択します。役割からサービスへのマッピングデータベース全体のリストが表示され、検討することができます。リストで特定のエントリの「変更」リンクを選択すると、そのエントリの詳細を更新できます。

図　4-6　　サービスから役割へのマッピングのリスト



第 5 章

ログ

ログを使用すると、監視とともに、どのようなエラーが発生しているかという観点からメッセージ機能を制御できます。これらのログは表示できます。また、オプションを使用して、画面に表示する詳細のレベルを設定できます。

すべてのメッセージトランザクションの詳細を記録した、原初ログもあります。原初ログは、Oracle の標準的なツールで表示できます。

概要

iPlanet Trustbase Transaction Manager では、次の 3 種類のログを構成できます。このうち 2 つは直接表示できます。

- 監視ログ - iPlanet Trustbase Transaction Manager フレームワーク (メッセージハンドラやルータなど) を通過したメッセージの流れに関するエントリを含むログ。構成に関する問題を診断する場合に便利
- エラーログ - iPlanet Trustbase Transaction Manager フレームワークおよび Identrus 固有のコンポーネントからのランタイムの問題に関するエントリを含むログ
- 原初ログ - 送受信された Identrus メッセージ専用のログ。このログは直接表示できない

図 5-1 「ログ」メインメニュー

監視ログ

監視は、タイプによって構成できます。また、監視をクエリすることも可能です。監視には次のタイプがあります。

Trustbase の監視：

- ROUTER_ABORT_ROUTING
  規則に基づくルータが、不正な規則のためにルーティングを停止した場合に発生
- ROUTER_CONFIG
  規則の構成画面で規則が変更された場合に発生
- ROUTER_CONSTRUCTION
  起動時に新規規則セットが作成された場合に発生
- ROUTER_CONTEXT_DIRECTIVE
  ルータにより、ルータディレクティブ (EndContext、StartContext、または ReturnToUser) が実行された場合に発生
- ROUTER_ROUTE_MESSAGE
  メッセージがサービスにルーティングされた場合に発生
- ROUTER_START
  規則に基づくルータコンポーネントが初期化された場合に発生
- CONFIGURATION_CHANGE
  Trustbase の構成が変更された場合に発生
- OPERATION_ABORT
  サービスによりメッセージの処理が中止された場合に発生
- OPERATION_BEGIN
  サービスによりメッセージの処理が開始された場合に発生
- OPERATION_COMPLETE
  サービスによりメッセージの処理が完了した場合に発生
- PARSER_STARTUP
  メッセージアナライザコンポーネントが起動した場合に発生
- SECURITY_CHANGE
  一般的なセキュリティ関連のイベントが発生した場合に発生
- TAS_SHUTDOWN
  Trustbase が停止した場合に発生
- TAS_STARTUP
  Trustbase が起動した場合に発生

- ROLE_SERVICE_MAPPING_CHANGED
  サービスと役割間のマッピングが、アクセス権の構成で変更または追加された場合に発生
- DEFAULT_SECURITY_ROLE_USED
  認証コンポーネントがユーザと役割間の特定のマッピングを見つけられない場合に発生。そのユーザにデフォルトのセキュリティ役割が適用されたことが表示される
- CERT_BASED_ROLE_MAPPING_CHANGED
  証明書とセキュリティ役割間のマッピングが、アクセス権の構成で作成された場合に発生
- USER_PASS_BASED_ROLE_MAPPING_CHANGED
  ユーザ名 / パスワードとセキュリティ役割間のマッピングが、アクセス権の構成で作成された場合に発生

Identrus トランザクションコーディネータの監視：

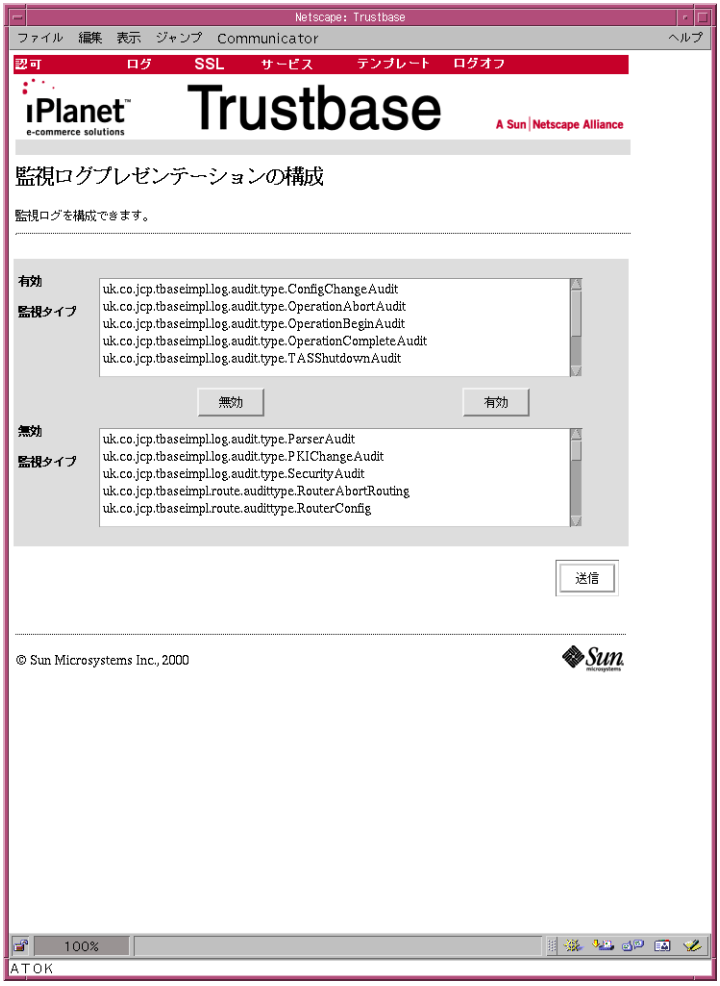
- CSC_PROCESSING
  証明書ステータスの確認 (CSC) が行われた場合に発生
- CSC_DEBUGGING
  証明書ステータスの確認 (CSC) をデバッグする場合に発生

監視の構成

監視ログの設定では、どの監視タイプを実際に表示するかを選択できます。監視タイプは、有効 (ログを実行し、表示可能) または無効 (このタイプに関しては何の情報もログしない) に設定できます。

ログするタイプを構成するには、まず「ログ」メインメニューから「監視構成」を選択します。

図 5-2 監視の構成



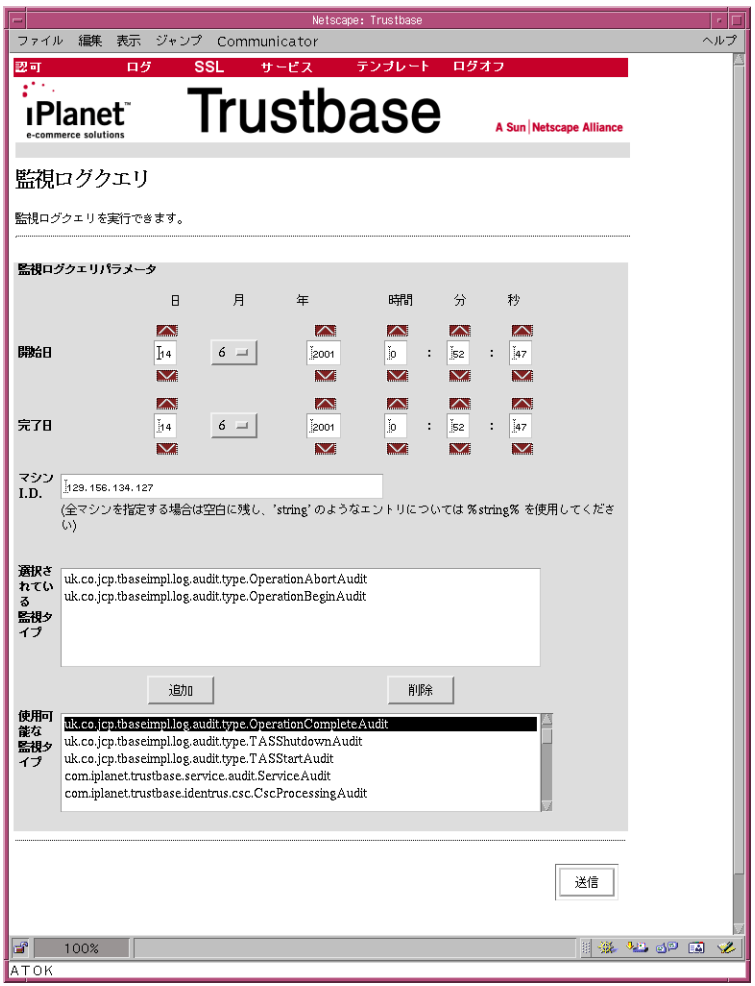
- 有効または無効にする監視タイプを、マウスの左ボタンでクリックします。
- 「有効」または「無効」を選択します。

監視の表示

監視ログを表示するには、日付の範囲 (開始日と完了日) とマシン ID (IP アドレス) を選択します。この場合のマシン ID とは、ログを作成しているマシンを指します。監視タイプを削除または追加することによって、表示する内容を制限または拡張できます。選択を行うと、日付、マシン ID、監視タイプ、およびメッセージの内容が出力画面に表示されます。

表示内容を選択するには、「ログ」メインメニューから「監視ログクエリ」を選択します。

図　5-3　　監視表示



すべての情報は標準的な Oracle データベースに格納されています。このため、より詳細なログの表示には、サードパーティのデータベースレポートツールを使用することもできます。

画面には、図　5-4 に示すような出力が表示されます。

図　5-4　　監視の結果

結果が 1 ページに収まらない場合は、図に示すように、画面の下部に「インデックス」タブが表示されます。SQL を使って検索を行う場合は、SQL テーブル「AUDITDATA」を参照してください。

原初ログ

Identrus のメンバーは、原初ログを記録およびアーカイブすることを要求されています。原初データのログの目的は次のとおりです。

- 否認防止サポート - トランザクションの証拠となるサポートを提供する、完全なトランザクションログ
- 監視 - iPlanet Trustbase Transaction Manager のアクティビティの監視を助ける完全なトランザクションログ

これらはさまざまな方法で構成できます。特にこの機能では、セキュリティポリシーの観点から、メッセージをどのように作成するかをメッセージロガーで定義できます。

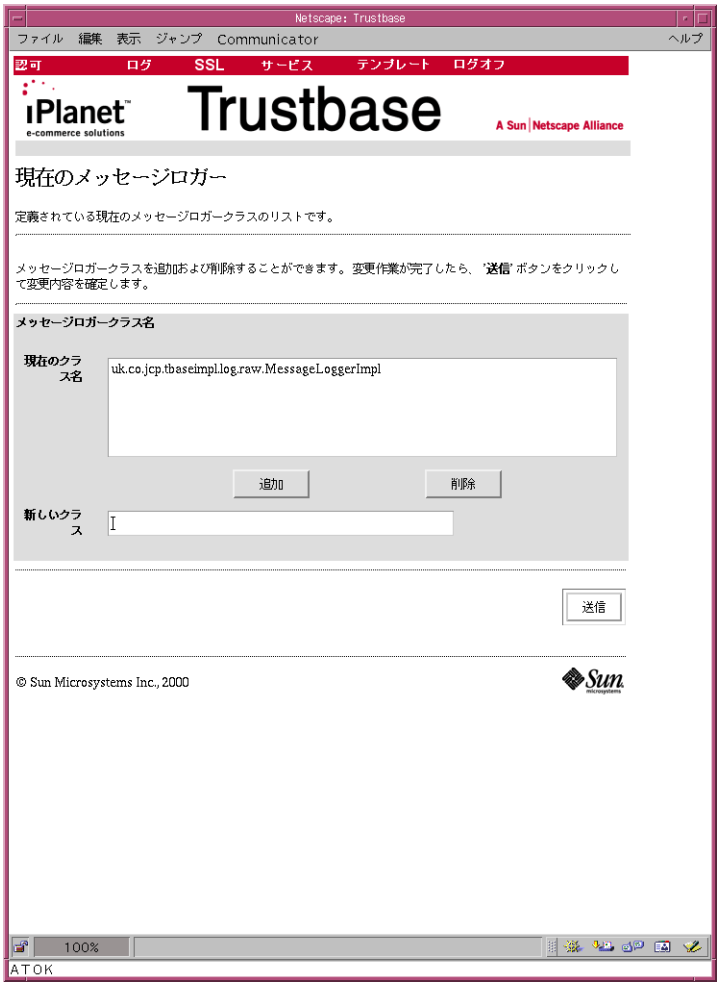
図　5-5　　メッセージログの設定

通常、これらのオプションを変更する必要はありません。次に各オプションについて説明します。

- 署名アルゴリズム - デフォルトでは、原初ログのエントリの署名には SHA-1/RSA アルゴリズムを使用。このオプションは、使用する暗号化セキュリティプロバイダによって異なる
- ダイジェストアルゴリズム - デフォルトでは、原初ログのエントリのダイジェストには SHA-1 アルゴリズムを使用。ダイジェストは、ログの内容の不正な編集を防ぐ原初ログメカニズムの一部として使用される
- 証明書の発行元 DN - 証明書属性のオプションが空欄の場合にだけ使用される。このオプションにより、原初ログの署名に使用する証明書の識別名を指定可能
- 証明書のシリアル番号 - 上記の「証明書の発行元 DN」オプションとともに使用し、原初ログの署名に使用する証明書のシリアル番号を指定する
- 証明書の属性 - 発行者元 DN とシリアル番号のフィールドが空欄の場合にだけ使用される。デフォルトでは、このフィールドには証明書の目的 ID を示す値「L1IPSC」(Inter-Participant Signing Certificate) が含まれる
- シーケンスファクトリタイプ - このオプションは変更しないこと。内部専用で、異なるデータベースプロバイダ (Oracle など) に対する、データの順番の決定に影響を与える
- シーケンスファクトリ名 - このオプションは変更しないこと。内部専用で、異なるデータベースプロバイダ (Oracle など) に対する、データの順番の決定に影響を与える

メッセージロガーは、受信した原初データをログに保管します。サポートする Identrus 固有のトランザクションに関するデータだけがログされます。この原初データには、テキストと base64 エンコーディングによる情報が含まれ、メッセージロガーにより前述の保証を行うために署名が行われます。現時点では、Java メッセージロガークラスの実装は 1 つしかありません。このため、このオプションは変更しないでください。

図 5-6 メッセージロガーの構成



注 原初ログは、RAW_DATA テーブルを使って Oracle から表示できます。この表示を行うには「select * from raw_data displaying MSGRPID」などのように入力します。

エラー

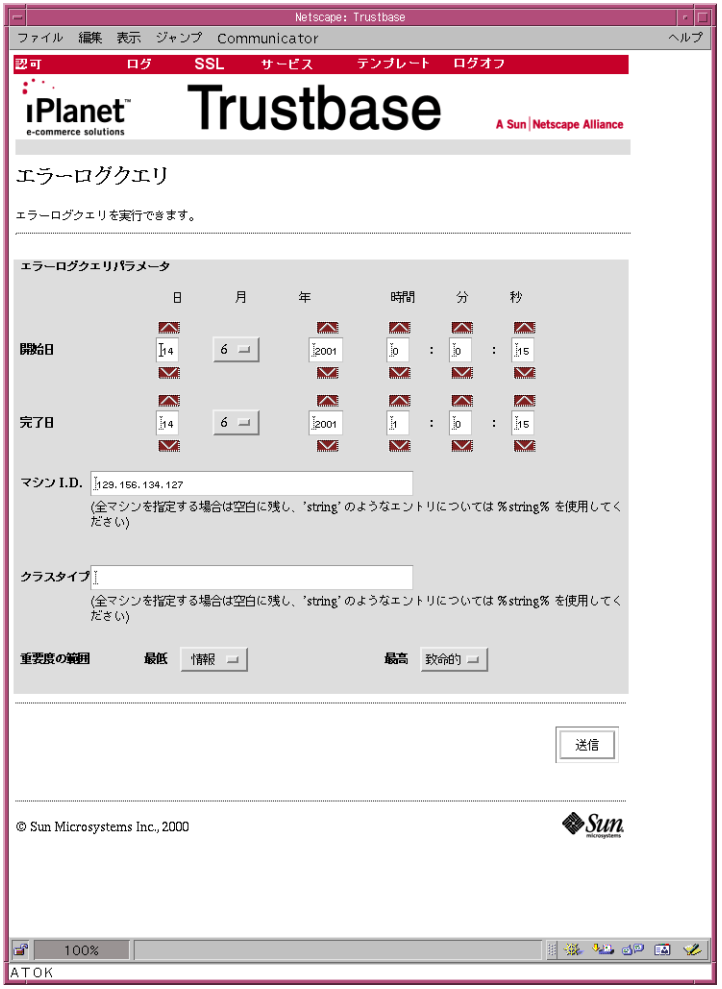
エラーについては、次の 4 つのセクションに分けて説明します。

- エラーの表示方法
- エラーの重要度の意味
- iPlanet Trustbase Transaction Manager のコアエラーメッセージリストの場所
- Identrus 固有のすべてのエラーメッセージの表

表示

エラーログを表示するには、日付の範囲 (開始日と完了日) とマシン ID (IP アドレス) を選択します。重要度の最小値と最大値を指定することによって、表示する内容を制限または拡張できます。また、Java クラスを指定することによって、そのクラスで発生したエラーだけを表示することもできます。選択を行うと、日付、マシン ID、クラスタイプ、およびエラーメッセージの内容が出力画面に表示されます。たとえば、次のように選択を行います。

図　5-7　　エラーログクエリ



エラーログは、ERRORVIEW テーブルを使って Oracle から表示できます。この表示を行うには「select * from ERRORVIEW」などのように入力します。

前のページで示した画面に、次のようなエラーが出力されます。

図　5-8　　エラーログクエリの結果

エラーイベントタイプの構成

このセクションでは、ログをとる最低のエラーレベルを指定できます。ここで指定したよりも低いレベルにタグされたエラーは、記録されません。

図　5-9　　エラーログの構成

iPlanet Trustbase Transaction Manager では、重要度、エラーを定義するオブジェクトのクラス、およびプログラマが定義したメッセージによって、エラーが定義されます。デフォルトの実装では、さまざまな重要度を示す 4 つの定数が定義されています。

- 情報 - 情報に関連するイベント (エラーでない場合もある) のログに使用。あまり多用しないこと
- 警告 - 予期された、処理可能なエラーに使用。動作分析のためのログが必要
- エラー - システム内に本質的な問題があることを示す、重大なエラーに使用。ただし、このエラーでは処理の続行や再試行が可能
- 致命的 - 処理を回復できない、致命的なエラーに使用。これらのエラーが発生すると、処理が放棄される

エラーメッセージ

エラーメッセージは 2 つのカテゴリに分けられます。iPlanet Trustbase Transaction Manager のフレームワークで生成されるものと、Identrus サービスで生成されるものです。たとえば、Identrus のメッセージコードは、次のようなカテゴリに当てはまります。

- メッセージライタのエラー
- メッセージリーダのエラー
- 証明書ステータス確認のエラー

すべての TTM iPlanet Trustbase Transaction Manager コアエラーメッセージの意味については、Oracle データベースのテーブル「error_codes」を参照してください。このテーブルを表示するには、次のように入力します。

図 5-10 Oracle データベースのエラーコードを選択

```
su -
cd /app/Trustbase/TTM/V2.2/Config/sql
sqlplus tbase/tbase
select * from error_codes;
```

第 6 章

SSL

SSL の構成では、ネットワーク上のメッセージ転送に使用されるセキュリティを決定するパラメータを定義できます。構成オプションには、次のものがあります。

- 接続数とプロクシのポート設定の変更方法
- SSL プロトコル設定の変更方法
- SSL プロクシが使用する証明書ストアの変更方法
- SSL プロクシが別の Web サーバを使用するように設定する方法

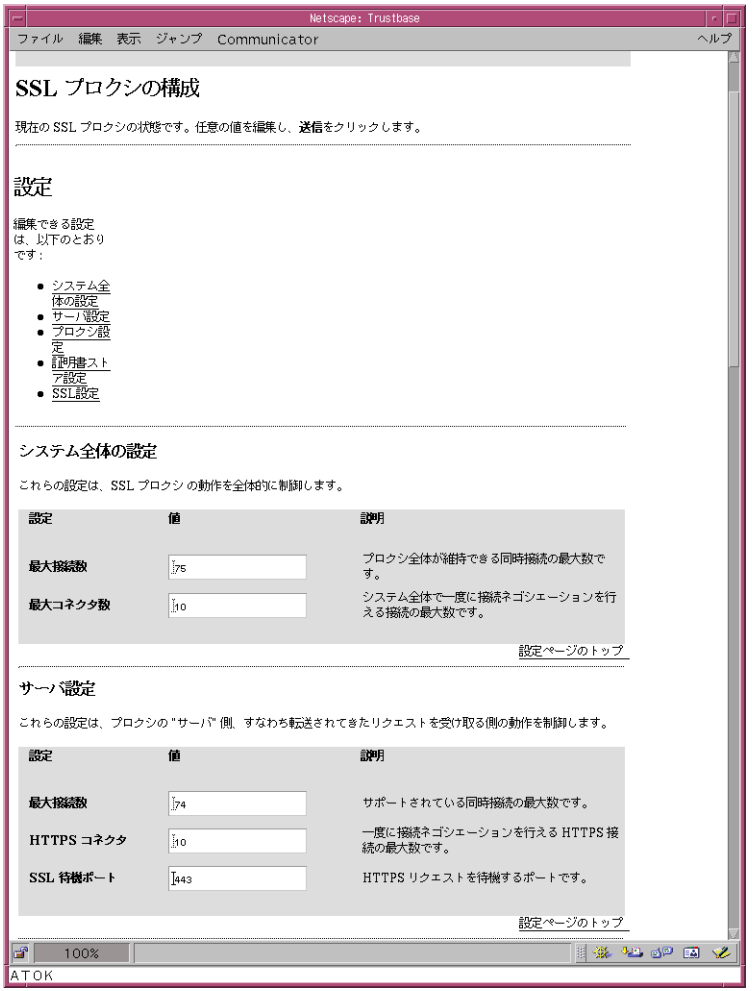
概要

プロクシは、セキュリティユーザログオンを使って構成できます。

図　6-1　　「SSL」メインメニュー

- 「SSL」-「プロクシ構成」を選択すると、「SSL プロクシの構成」ホームページが開きます。

図　6-2　　SSL プロクシの設定



SSL プロクシに関するオプションは、すべて「SSL プロクシの構成」メインページに含まれています。ページの上部でリンクを選択すると、個々のセクションを開くことができます。これらのセクションで必要な入力の詳細は、これ以降の該当するタスクに関する各項で説明します。

フォームでは、必要に応じていくつでも変更を行うことができます。変更が完了したら、ページの下部にあるボタンを使ってフォームを送信します。確認段階で更新に失敗した場合は、変更に失敗した値のレポートが返されます。すべての更新に成功した場合は、操作が完了したという旨のメッセージが表示されます。

注　この画面の最後には、エキスパートユーザ用の設定セクションがあります。このセクションは iPlanet の社員が SSL プロクシの問題点を診断するために使います。通常の SSL プロクシの構成では、このセクションは使わないでください。SSL プロクシを別のマシンにインストールする方法については、第 2 章、「アーキテクチャの構成」を参照してください。

受信する接続の情報の変更

受信する接続の情報は、「SSL プロクシの構成」ページの次のオプションで変更できます。

- プロクシ設定
- システム全体の設定
- サーバ設定

SSL プロクシは、ローカルマシンの特定の TCP/IP ポートで受信する接続を待機します。これは一般にポート 443 で、インストール中にこのデフォルト値に設定されます。プロクシが待機するポートを変更するには、「プロクシ設定」オプションで変更を行い、プロクシを再起動する必要があります。

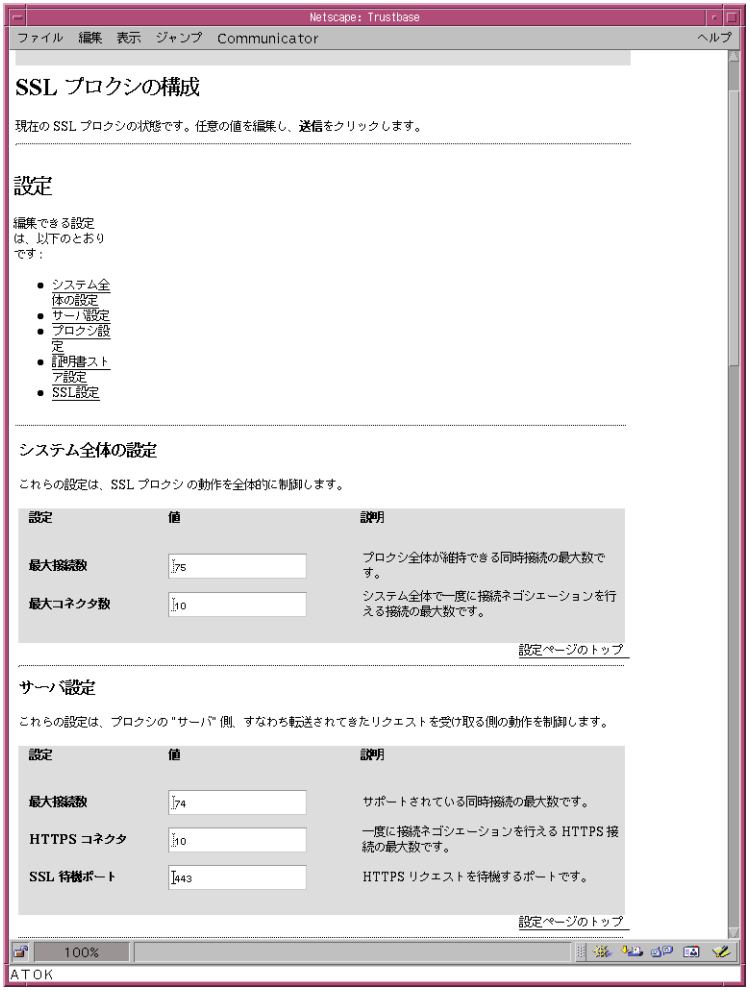
- SSL 待機ポート - サーバがリクエストを受信するポート。HTTPS を使う場合、デフォルトポートは 443

注 ポート 443 は SSL に割り当てられたポートのため、ポート番号を変更する場合は、クライアントに新しい設定を通知する必要があります。iPlanet Trustbase Transaction Manager では、クライアントが使うポート番号は、証明書 AIA にエンコードされています。SSL プロクシポート番号を変更すると、クライアントやほかのトランザクションコーディネータが Identrus トランザクションコーディネータに接続できなくなります。

SSL プロクシの管理における主な条件の 1 つとして、プロクシマシンの負荷により、受信接続が拒否されないことが必要です。各 SSL 接続では、セッションパラメータのネゴシエーション (ハンドシェイク) のために CPU が集中的に使用され、多くの SSL ネゴシエーションを同時に許可すると、クライアントがタイムアウトになることがあります。この状態を避けるために、すでに負荷がある状態では新規接続を拒否するように SSL プロクシを構成できます。

システム全体の設定

図　6-3　　システム全体の SSL プロクシの設定



「システム全体の設定」セクションで提供されているオプションは、次のとおりです。

- 最大接続数 - プロクシで許可される最大接続数。これはハンドシェイクの段階のセッションと進行中のセッションの合計で、通常 80 以下であるが、ホストマシンの構成によって異なる
- 最大コネクタ数 - 同時にハンドシェイクを実行できる最大の接続数。通常 40 以下であるが、ホストマシンの構成によって異なる

サーバ設定

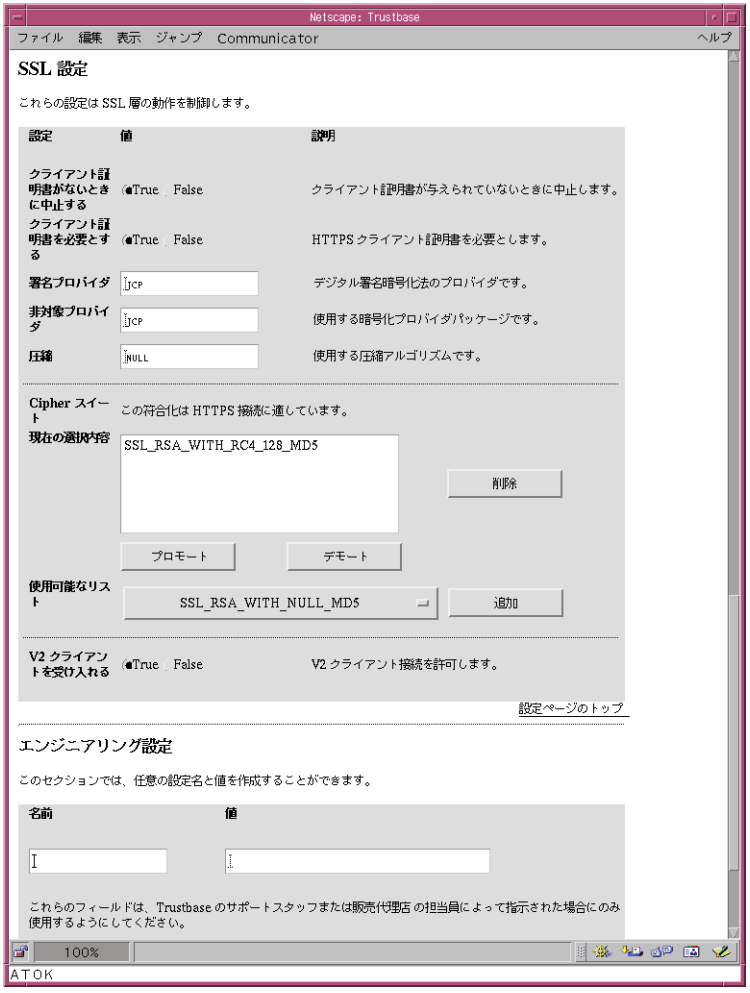
- HTTPS コネクタ - プロクシ接続の最大数と同じ値に設定
- 最大接続数 - プロクシコネクタの最大数に設定

注 SSL プロクシのインスタンスが複数あると、1 つの Java 仮想マシン (JVM) を異なる目的に使用できます。ただし、iPlanet Trustbase Transaction Manager では、SSL プロクシをこのモードで実行することはありません。このため、サーバ設定をシステム全体の設定と同じにします。設定が同じでない場合は、小さい方の値が使用されます。

SSL プロトコルと認証の設定

SSL プロトコルには、パフォーマンスや使用に影響する多くのパラメータがあります。これらのパラメータは、「SSL 設定」ページで変更できます。

図 6-4 SSL 設定



これらの設定は次のようにグループ分けできます。

プロトコルの設定

- 圧縮 - 将来使用される予定。現在の設定は NULL
- V2 クライアントを受け入れる - SSL プロクシは SSLV3.0 を実装。この値を「True」に設定すると、SSLV2.0 の hello リクエストを使うクライアントも受け入れ可能。これにより、特定の種類のブラウザとの互換性が提供される
- 非対象プロバイダ - 使用する非対称プロバイダ。nCipher HSM を使う iPlanet Trustbase Transaction Manager インストールのデフォルトは、NCIPHER
- Cipher スイート - SSL ハンドシェイクネゴシエーション中に使う符号化スイート。iPlanet Trustbase Transaction Manager インストールのデフォルトは、SSL_RSA_WITH_NULL_MD5

認証の設定

- クライアント証明書を必要とする - クライアントの SSL セッションの認証用に「True」に設定
- クライアント証明書が正しくないときに中止にする - デフォルトでは「True」に設定され、クライアントがルート不明の証明書または無効な証明書チェーンを示した場合に、SSL ハンドシェイクを中止
- クライアント証明書がないときに中止にする -「True」に設定して、クライアントが認証用に証明書を提供しない場合にハンドシェイクを中止

証明書ストアの場所の変更

SSL プロクシによって使用される証明書ストアは、デフォルトでは iPlanet Trustbase Transaction Manager で使用されるものと同じです。インストール中に、プロクシの初期化ファイルから構成データベースに、Oracle データベースへのパスが読み込まれます。これらの値は、共有証明書データベースではなく、ローカルの Oracle 証明書データベースをプロクシで使うように変更できます。

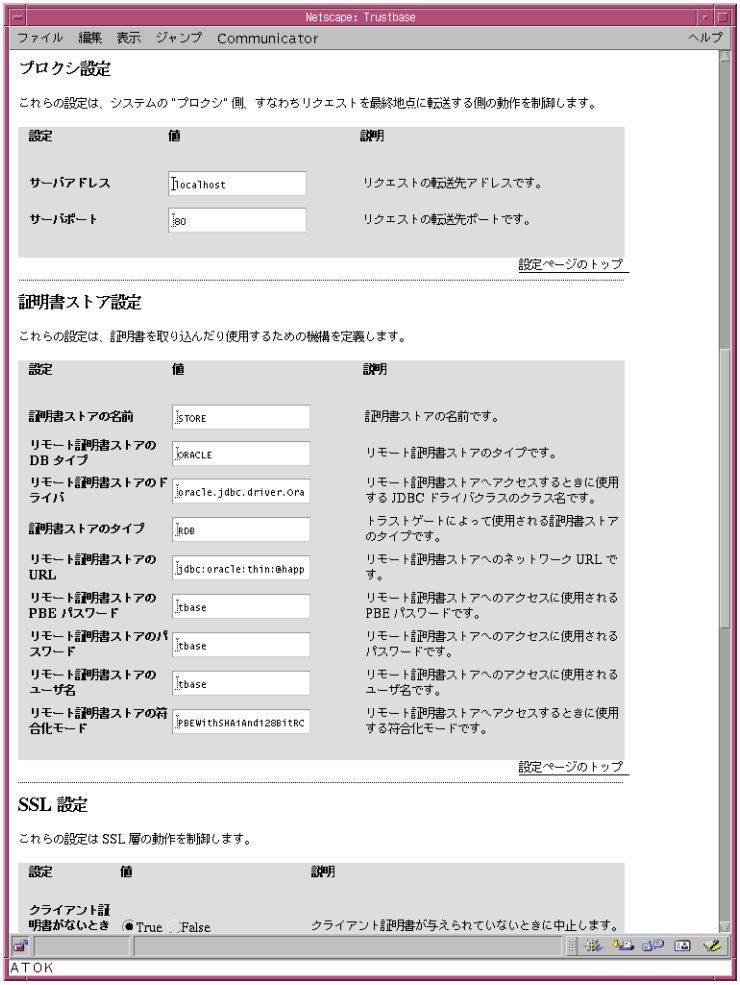
ほとんどのインストールでは、ローカルデータベースを使う必要はありません。証明書と鍵を 2 つの場所で管理する必要が出てくるからです。しかし、組織が副ファイヤウォールを開きたくない場合などには、SSL プロクシでローカルの証明書データベースを使うように、これらの設定を変更できます。

ローカル証明書ストアを使用するには、Oracle ユーザが既知であることと、証明書ストアテーブルを生成する SQL スクリプトがすでに実行されていることが必要です。詳細は、『インストールガイド』を参照してください。次の項目を、新しい証明書ストアをポイントするように変更できます。

- 証明書ストアのパスワード - 証明書ストアのロック解除に使うパスワード
- 認証済み証明書の目的 ID - 一連の認証済み証明書の目的 ID
- サーバ証明書の ID - 使用するサーバ証明書の ID

- 証明書ストアのパス - 証明書ストアへのパス。通常は Oracle データベースに設定

図 6-5 証明書ストアの設定



プロクシの Web サーバへのリダイレクト

SSL プロクシでは、HTTP データが副ファイヤウォールの後ろにある Web サーバに転送されます。マシンにエラーが生じた場合など、Web サーバの場所を変更しなければならないことがあります。このような場合には、SSL プロクシを新しい Web サーバの場所にリダイレクトする必要があります。

このためには、次の設定を使用します。

- サーバアドレス - すべての受信リクエストの転送先のマシン名。SSL プロクシと Web サーバが同じマシンにある場合は、「Localhost」を使用可
- サーバポート - Web サーバが使うソケットのポート番号

第 7 章

SMTP プロクシの構成

SMTP プロクシ構成の一部として、さまざまな S/MIME 設定により、iPlanet Trustbase Transaction Manager がメールに基づくリクエストを受信する方法と、応答の形式を決定できます。たとえば、メッセージを暗号化するかどうか、または応答にどのように署名するかなどです。

S/MIME の設定

<インストールディレクトリ>/Trustbase/TTM/<マシン名> にある tbase.properties ファイルには、多くの S/MIME 設定が含まれています。これらの設定について説明します。

```
[SmimeServlet]
mail.smtp.host=smtphost.smime.com
mail.from=ttm@smime.com
loopback=false
debug=false
smime.capability.store.impl=com.iplanet.trustbase.security.smime.
SimpleSmimeCapabilityStore
smime.mode=SIGN:ENVELOPE
smime.permit.unencrypted=true
smime.signing.cert=TTMEMAIL
smime.encryption.alg=3DES/CBC/PKCS5
```

- SMTP サーバ - 送信メールサーバのホスト名

```
mail.smtp.host=smtphost.smime.com
```

- デフォルトのフォームアドレス - デフォルトの署名証明書の識別名 (DN) 内にある電子メールアドレスと一致させること

```
mail.from=ttm@smime.com
```

- ループバックテストモード - この設定は診断用。通常は使用しない

```
loopback=false
```

- デバッグテストモード - この設定は診断用。通常は使用しない

```
debug=false
```

- この設定は iPlanet Trustbase Transaction Manager の内部用。通常は変更しないこと

```
smime.capability.store.impl=com.iplanet.trustbase.security.smime.
SimpleSmimeCapabilityStore
```

- S/MIME モードパラメータの形式は次のとおり

```
MODE ::= [PROT][:PROT]*
PROT ::= SIGN[,KEY] | CLEAR_SIGN[,KEY] | ENVELOPE[,CIPHER]
```

- S/MIME モードパラメータ - 送信する応答メッセージに関連するパラメータ。電子メールが SIGN パラメータを使って署名されている場合、署名を確認できないとメッセージの内容を読むことはできない。一方、CLEAR_SIGN パラメータが使われている場合は、署名を確認できない場合でも内容を読むことができる。ENVELOPE パラメータは、送信する Trustbase 応答メッセージが暗号化されることを示す

```
smime.mode=SIGN:ENVELOPE
```

- 暗号化されていないリクエストを許可 - 「true」の場合、ENVELOPE による保護がリクエストされても、受信者の鍵がないと、メッセージは暗号化されずに送信される。「false」の場合、メッセージは送信されない

```
smime.permit.unencrypted=true
```

- S/MIME 目的属性 - 送信する応答を署名および暗号化する証明書に割り当てる属性。iPlanet Trustbase Transaction Manager ストア内の証明書に属性を割り当てる方法については、49 ページの「証明書への属性の割り当て」を参照

```
smime.signing.cert=TTMEMAIL
```

- 送信する S/MIME 応答のデフォルトの暗号化アルゴリズム

```
smime.encryption.alg=3DES/CBC/PKCS5
```

第 8 章

サービスの配置

マシン間でのメッセージの送受信に関与するサービスを配置するには、メッセージプロトコルを決定するクラスファイル、Java コード、および tbasesvc.properties ファイルを使ってそれらのマシンを構成します。この Java コードは、さまざまな認可メカニズムを定義する規則セットとともにサービスを定義するものです。また、tbasesvc.properties ファイルでは、そのサービスに対する構成オプションを定義できます。

サービス配置の概要

サービスを配置する際には、構築したサービスの種類に応じてさまざまな構成を行うことができます。たとえば、独自の構成オプションを定義して、テンプレートのオプションを構成することが可能です。また、サービスを認証するために、認可オプションを選択する必要が生じることもあります。

図　8-1　　「サービス」メインメニュー

サービスを配置するには、2 つの主な必要条件があります。

- サービス jar ファイルを iPlanet Trustbase Transaction Manager 内に読み込むことにより、サービスを配置する
- その後、必要に応じてサービスを認証するための役割を割り当てる

注　サービスを配置するには、まず次の手順に従ってサービスを構築する必要があります。

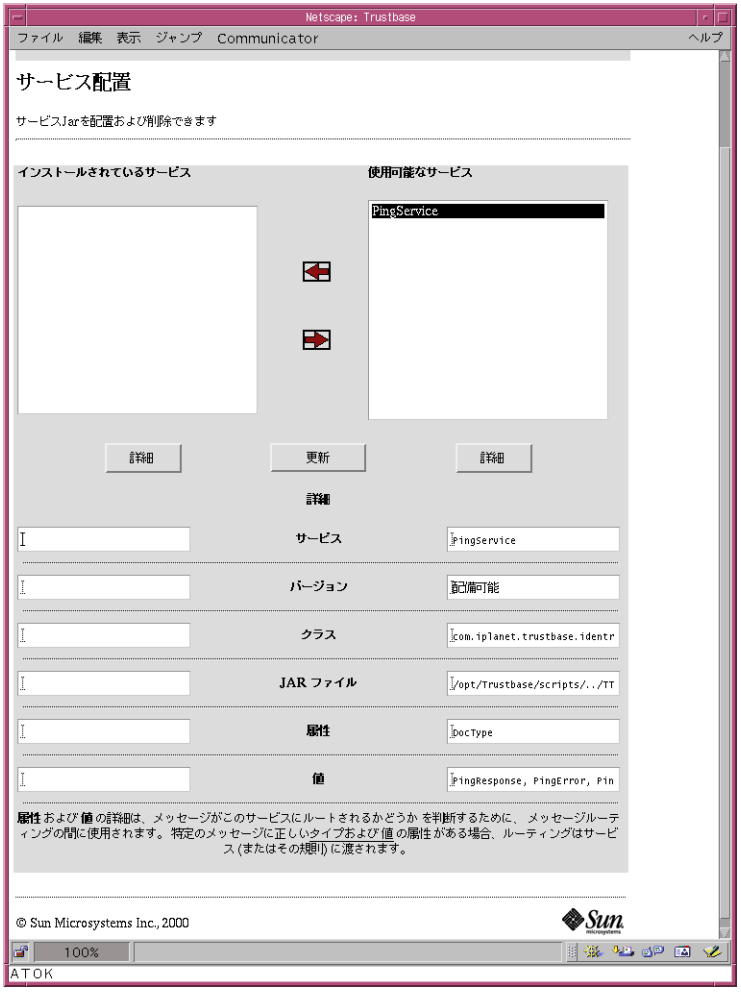
1. システム内に送り出すメッセージの構文構造を指定する DTD 定義を作成します。クラスファイルが生成され、メッセージがクラスファイルから解釈されるようになると、これらの DTD は破棄されます。これには、(a) より速く、(b) より簡単に構築が可能という 2 つの利点があります。
2. Classgen com.iplanet.trustbase.app.classgen.ClassGen を使って、DTD 定義から Java クラスを生成します。
3. Identrus API を配置するサービスの Java コードを書きます。Identrus API は、メッセージ、証明書、鍵、およびデジタル署名の処理と確認を支援するためのものです。
4. 後述の手順に従って、適切な構成オプションを選択して iPlanet Trustbase Transaction Manager 内にサービスを配置します。
5. iPlanet Trustbase Transaction Manager にサービスを配置したら、サービスを実行することができます。

詳細は、『開発者ガイド』を参照してください。

配置

- 「サービス」-「配置」を選択して、サービスを配置します。

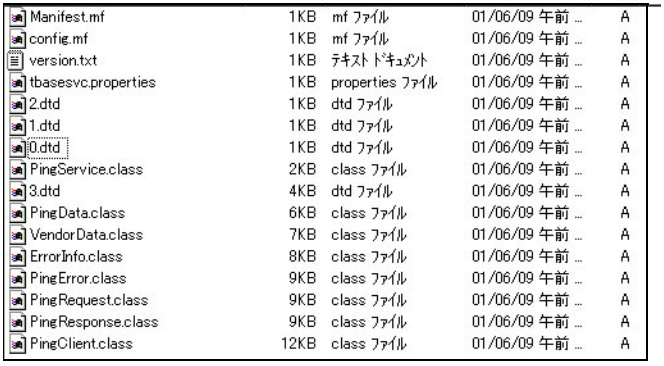
図　8-2　　サービスの配置



- 属性と値の詳細は、メッセージがこのサービスにルーティングされるかどうかを決定するために、メッセージの配信中に使用されます。メッセージに正しいタイプの属性と値が備わっていれば、そのメッセージはサービス (または該当する規則) に渡されます。
- 「サービス」はサービス名です。
- 「バージョン」はユーザが定義したサービスのバージョンです。
- 「クラス」はメインの呼び出しプログラムです。
- 「JAR ファイル」は、サービスとその関連データがすべて含まれている jar ファイルです。

サービスには、1 つの jar ファイル (場所 : /opt/Trustbase/TTM/V2.2/deploy) が含まれています。この jar ファイルには、サービスに関連する Java コードを含んだクラス、サービスを定義する Java コード、およびサービスの構成方法を定義する .properties ファイルのリストがあります。次の図に、その例を示します。

図 8-3 配置するサービスの j ar ファイルの例



- 次の図　8-4 に、サービスを配置するときの出力例を示します。サービスを配置した効果は、iPlanet Trustbase Transaction Manager を再起動したときに現われます。

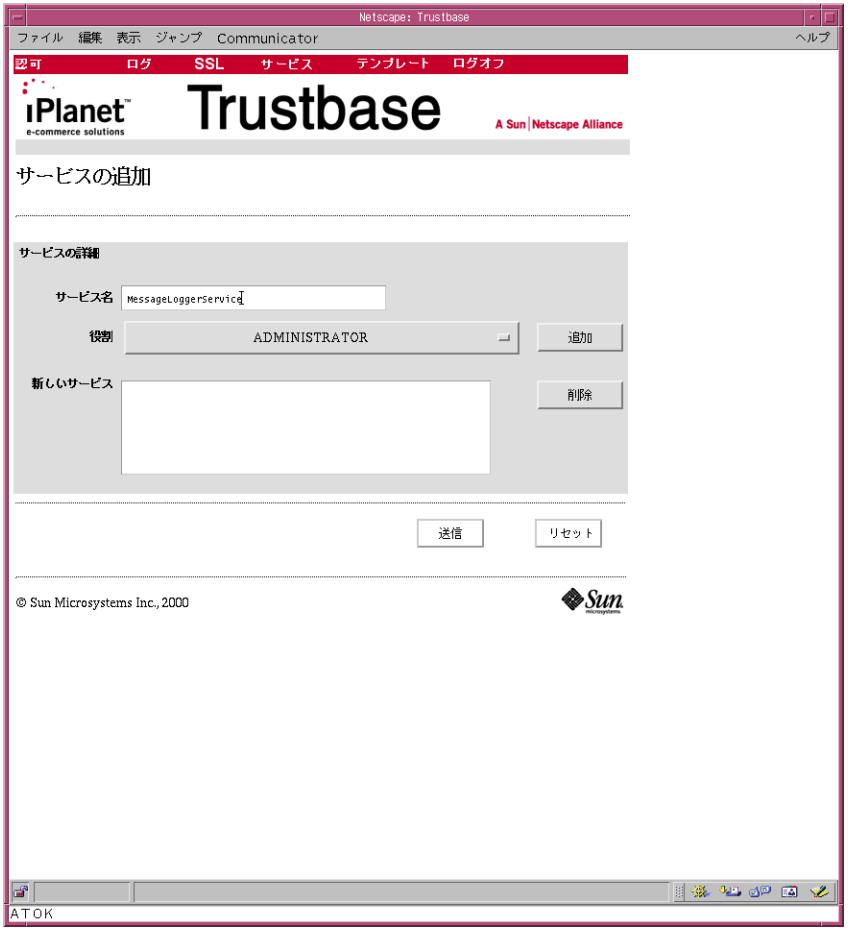
図　8-4　　サービスの配置結果

認可サービス

認可が必要な場合は、次の操作を行う必要があります。

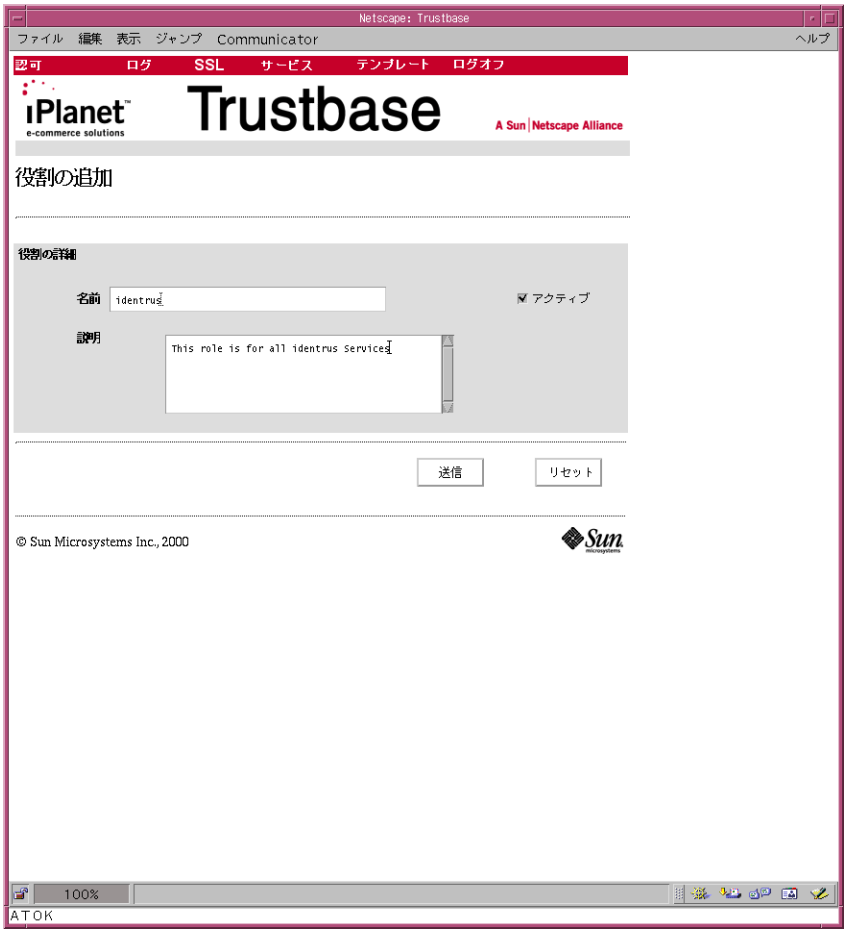
- 「サービスの追加」を選択してサービスを追加します。

図　8-5　　サービスの追加



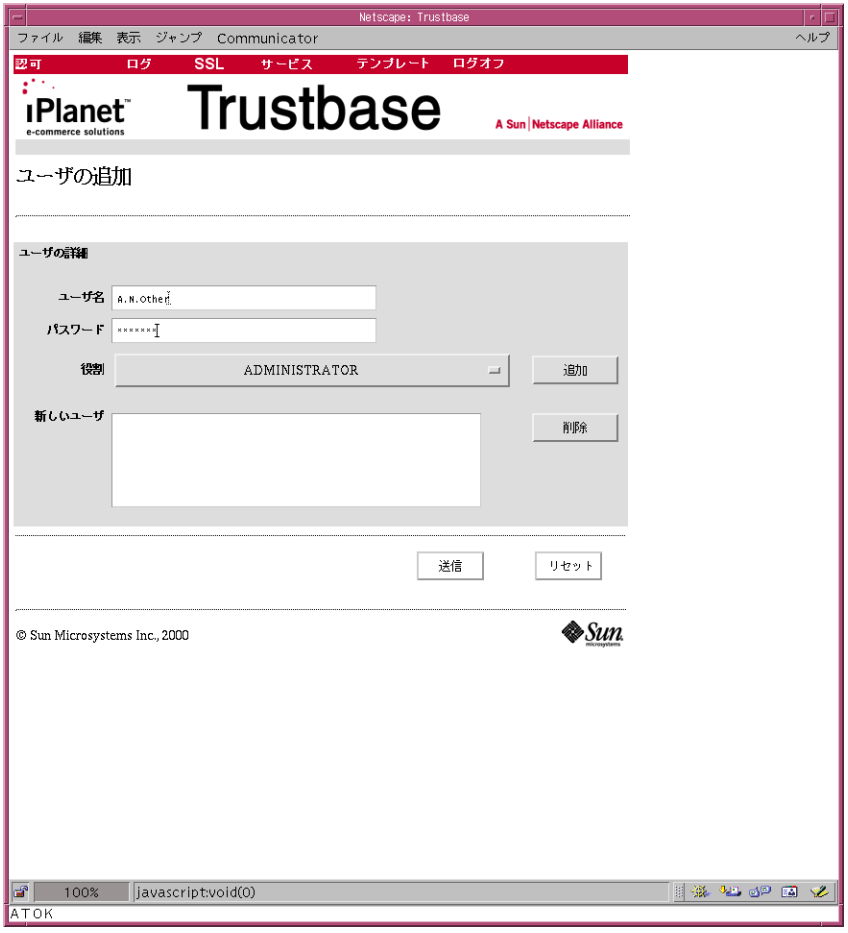
- 「役割の追加」を選択して、このサービスの新しい役割を作成します。

図 8-6 役割の追加



- この役割に対し、何人かのユーザを定義します。

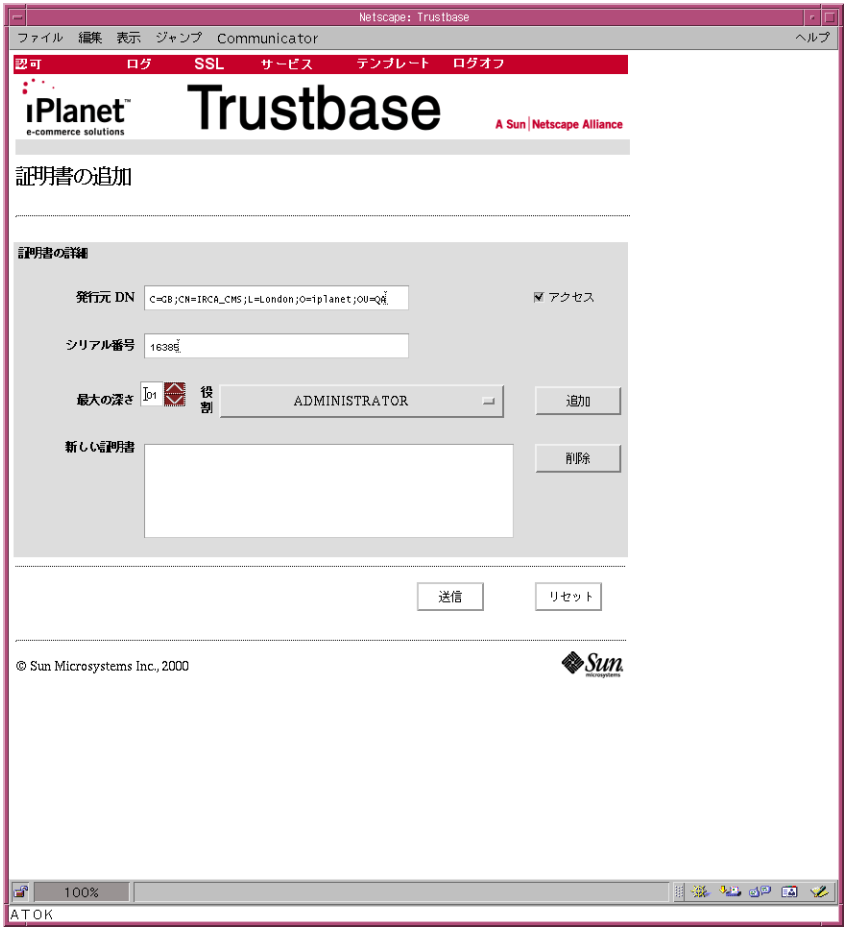
図 8-7　　ユーザの追加



- ユーザに役割を割り当てたら、必ず「追加」をクリックします。
- 「送信」をクリックします。

- 証明書および関連する役割を追加します。

図 8-8 証明書の追加



- ユーザに証明書を割り当てたら、必ず「追加」をクリックします。
- 「送信」をクリックします。

認可を必要としないサービス

配置するサービスが認可を必要としない場合は、単に「サービス」-「配置」を選択し、サービスに役割を割り当てるための手順をスキップします。

登録済みのサービス

配置したサービスを表示するには、「サービス」-「レジストリ構成」を選択します。

図　8-9　　サービスレジストリ

第 9 章

テンプレート

テンプレートを使うと、HTML ベースの応答を配置することができます。これらの応答は、HTML ページに記入されたデータ値を格納する画面に送られます。

通常の環境では、テンプレートを変更する必要はありません。ただし、Trustbase 画面にメッセージを送るような新しいサービスを配置する場合には、この構成画面にテンプレートを配置する必要があります。

図　9-1　　「テンプレート」メインメニュー

図　9-2　　テンプレートの構成

第 10 章

バックアップ

この章では、次の項目について説明します。

- バックアップすべきデータ
- Raw_Data と Init_Table のアーカイブ
- 証明書の有効期限が切れた場合
- 障害回復の方法

バックアップすべきデータ

iPlanet Trustbase Transaction Manager で使用するデータベーステーブルは、次の 2 つのグループに分けられます。

- 常に読み取り専用のもの (構成情報など)
- 頻繁に書き込まれる大きなデータを格納するためのもの (原初ログなど)

次の項では、データベース管理者がアーカイブ方法を決定する際に参考にできるよう、各テーブルの機能および構成について説明します。

読み取り専用のデータ

次の各テーブルは、主に読み取り専用の静的データ用に使用されます。これらのテーブルは比較的小さなサイズのまま維持されるため、アーカイブする必要はありません。また、データはすべてオンラインで維持できます。ただし、初期構成を完了した後や、証明書または構成を変更した後には、バックアップおよび障害回復対策としてこれらのテーブルをバックアップしてください。

- 証明書ストアを構成するテーブル。ストアにアイテムが追加された場合 (まれ) にだけ変更される
  - ATTRIBUTE_KEY_ATTRS
    鍵対に関連する属性を格納する
  - ATTRIBUTE_NAME_ATTRS
    証明書に関連する属性を格納する
  - CERT_TABLE
    X509 証明書を格納する
  - KEY_TABLE
    暗号鍵対を格納する
  - REVOCATION_ATTRS
    証明書破棄リスト (CRL) を格納する
  - REVOCATION_SERIAL_NUM
    証明書破棄リスト内で破棄するよう指定されている証明書のシリアル番号をインデックス化する
  - REVOCATION_TABLE
    エンコードされた X509 証明書破棄リストを格納する
  - SALT_TABLE
    データベース内で使用されるパスワードベース認証用の salt 値を保持する。テーブル内のエントリは 1 つに限られる

- Identrus
  - CERT_DATA
    Identrus Messaging からの固有な証明書
  - BILL_DATA
    処理済み Identrus Messaging の請求レコード
- その他のテーブル
  - AUTHORISATION
    役割名をサービス名にマップする
  - CERTIFICATEAUTHENTICATION
    証明書の詳細を役割にマップする
  - CONFIG
    システム用に構成データを格納する。各システム要素はテーブル内の各行に 1 つずつ記述されるため、このテーブルのサイズは新しいシステム要素が追加された場合にだけ増大する
  - ROLES
    役割に関する情報を格納する
  - USERNAMEPASSWORDAUTH
    ユーザ名とパスワードの組み合わせを役割にマップする
- /opt/Trustbase/TTM/< マシン名 > 内の初期化ファイル (*.properties と proxi.ini)
- nCipher などの HSM を使用する場合は、モジュールキー。nCipher の「Security World」がモジュールキーのバックアップをサポートする。Administrator Card Set の使用方法については、『KeySafe User Guide』を参照

頻繁に書き込まれるデータ用のテーブル

次のテーブルには頻繁にデータが書き込まれるため、テーブルのサイズが急速に増大します。したがって、記憶域の使用容量が限界に近付くにつれ、これらのテーブルのデータをアーカイブする必要があります。また、これらのログには重要な情報が含まれるため、損失しないよう 定期的にバックアップしてください。

- 頻繁に書き込まれるデータ
  - AUDITDATA
    監視ログデータを格納する
  - ERROR
    エラーログデータを格納する

- RAW_DATA
  システムに出入りするすべての原初メッセージデータを格納する。否認防止の目的に使用され、後述の INIT_TABLE によって参照される。したがって、これらの 2 つのテーブルをアーカイブする際には、前述の手順に従うことが必要

```
SQL> desc raw_data;
 Name                           Null?    Type
 ------------------------------ -------- ----
 SESSIONID                      NOT NULL NUMBER(38)
 LOGCONNECTIONID                NOT NULL NUMBER(38)
 RECORDID                       NOT NULL NUMBER(38)
 MSGGRPID                                VARCHAR2(120)
 MSGID                                   VARCHAR2(120)
 DOCTYPE                        NOT NULL VARCHAR2(120)
 RECORDMARKER                   NOT NULL VARCHAR2(240)
 CONNECTIONID                   NOT NULL VARCHAR2(100)
 PROTOCOLTYPE                   NOT NULL VARCHAR2(10)
 INPUT                          NOT NULL NUMBER(38)
 TIMESTAMP                      NOT NULL NUMBER(38)
 RAWDATA                        NOT NULL LONG
 DIGESTOFRECORD                          RAW(2000)
 SIGNEDDIGESTOFCALCULATION               RAW(2000)
```

- INIT_TABLE
  原初ログテーブルの完全性に関する情報を格納する

```
SQL> desc init_table;
 Name                           Null?    Type
 ------------------------------ -------- ----
 SESSIONID                      NOT NULL NUMBER(38)
 TIMESTAMP                      NOT NULL NUMBER(38)
 N_CONNECTIONS                  NOT NULL NUMBER(38)
 SIGDATA                        NOT NULL RAW(2000)
 SERVERCERTISSUERDN                      VARCHAR2(2000)
 SERVERCERTSERIALNUMBER                  VARCHAR2(100)
```

Raw_Data と Init_Table のアーカイブ

ログ init_table と raw_data テーブルは、Identrus 用に連結されています。raw_data レコードには、実際のメッセージデータおよびデジタル形式で署名されたタイムスタンプが保持されます。init_table レコードは、raw_data レコードセットの冒頭部分をポイントします。アーカイブ時の状況には、次の 2 種類があります。

1. **TTM インスタンスが*実行中ではない*場合**。この場合は、raw_data テーブルおよび init_table テーブル内のデータは一般的な方法でアーカイブできます。アーカイブ後のデータを適切に確認できるよう、これら 2 つのテーブルを両方ともアーカイブしてください。システムを再起動すると、init_table 内に新しい初期化レコードが作成され、raw_data 内のエントリがこのレコードから暗号文によってチェーンされます。
2. **TTM インスタンスが*実行中である*場合**。この場合は、原初ログ確認ユーティリティを実行し、ログ終端のリストを提供する必要があります。ユーティリティを実行すると、次のような形式の出力が生成されます。

スクリプトは、次のように実行できます。

```
$ cd <Trustbase インストールディレクトリ >/TTM/Scripts
$ ./runcheckintegrity
```

出力は次のようになります。

```
Trustbase Raw Log Verification Utility
Checking all sessions
Checked chain 0 from session 4,160 with 82 records, ending at 26/02/01
19:41. Endpoint in chain is 81
Checked chain 1 from session 4,160 with 81 records, ending at 26/02/01
19:41. Endpoint in chain is 80
Checked chain 2 from session 4,160 with 81 records, ending at 26/02/01
19:41. Endpoint in chain is 80
Checked chain 3 from session 4,160 with 75 records, ending at 26/02/01
19:41. Endpoint in chain is 74
Checked chain 4 from session 4,160 with 87 records, ending at 26/02/01
19:41. Endpoint in chain is 86
Checked chain 5 from session 4,160 with 85 records, ending at 26/02/01
19:41. Endpoint in chain is 84
Checked chain 6 from session 4,160 with 81 records, ending at 26/02/01
19:41. Endpoint in chain is 80
Checked chain 7 from session 4,160 with 77 records, ending at 26/02/01
19:41. Endpoint in chain is 76
Checked chain 8 from session 4,160 with 82 records, ending at 26/02/01
19:41. Endpoint in chain is 81
Checked chain 9 from session 4,160 with 79 records, ending at 26/02/01
19:41. Endpoint in chain is 78
Checked session 4,160 with total 810 records over 10 connections. Started
at 26/02/01 19:39 Ended at 26/02/01 19:41
```

注 スクリプトを実行する前に、tbase.properties 内のエントリ ([LogManager/MessageLoggerStore] と [LogManager/MessageLogger]) を確認する必要があります。データベース接続文字列、ユーザ、パスワード、およびドライバの設定は、このファイルから読み取られます。また、原初ログレコードおよび署名アルゴリズムの署名証明書も、このファイルから読み取られます。

次に、<インストールディレクトリ >/TTM/Scripts/runcheckintegrity スクリプトの例を示します。

```
. ./setcp
CLASSPATH=$TBASE_INSTALL:$CLASSPATH
cd $TBASE_INSTALL
exec java uk.co.jcp.tbaseimpl.log.raw.tools.VerUtil
```

各セッションには、それぞれ始端と終端を含むチェーンの集まりが保持されています。この時点で、終端までのデータをすべてアーカイブできます。アーカイブ後に原初ログ確認ユーティリティを実行すると、ユーティリティはアーカイブ後に書き込まれたデータを「親のない」データと見なしますが、ユーティリティによるこれらのデータの確認と報告は実行されます。出力は次のようになります。

```
$ ./runcheckintegrity
```

出力は次のようになります。

```
Trustbase Raw Log Verification Utility
Checking all sessions
No init records were found
Orphan chain from session 4,160, Connection 0, startpoint 10, endpoint 81
is valid
Orphan chain from session 4,160, Connection 1, startpoint 10, endpoint 80
is valid
Orphan chain from session 4,160, Connection 2, startpoint 10, endpoint 80
is valid
Orphan chain from session 4,160, Connection 3, startpoint 10, endpoint 74
is valid
Orphan chain from session 4,160, Connection 4, startpoint 10, endpoint 86
is valid
Orphan chain from session 4,160, Connection 5, startpoint 10, endpoint 84
is valid
Orphan chain from session 4,160, Connection 6, startpoint 10, endpoint 80
is valid
Orphan chain from session 4,160, Connection 7, startpoint 10, endpoint 76
is valid
Orphan chain from session 4,160, Connection 8, startpoint 10, endpoint 81
is valid
Orphan chain from session 4,160, Connection 9, startpoint 10, endpoint 76
is valid
Checked session 4,160 with total 710 records over 10 connections. Started
at 26/02/01 19:39 Ended at 26/02/01 19:41
```

レコード ID は、そのレコードの署名とローカルデータベース内に保持されている署名が一致した場合に有効と見なされます。レコードに記述されている終端と親のないデータの始端が符号する場合、そのログの完全性は維持されていると推定できます。さらに、確認結果のレコード ID が、前回実行した確認結果のレコード ID よりも少なくかつ有効であれば、ログの完全性は維持されていると推定できます。それ以外の場合は、アーカイブが正しく実行されなかったか、またはレコードの一部が何者かによって削除または改ざんされた可能性があるため、アーカイブの完全性を確認し直す必要があります。前述の 1 度目の確認では 810 個のレコードがチェックされ、2 度目の確認では 710 個のレコードがチェックされています。これは、2 度目の確認を行う前に、始端が 10 未満のチェーンに含まれる 100 個のレコードがアーカイブされたことを示しています。

デフォルトでは、ツールは原初ログ内のすべてのレコードの完全性をチェックしますが、次のコマンド行スイッチを使用してセッションを個別にチェックすることも可能です。

```
-session <セッション ID>
```

たとえば、次のように入力します。

```
./runcheckintegrity -session 12344
```

証明書の有効期限が切れた場合

証明書の有効期限が切れた場合は、新しい完全なトランザクションコーディネータ証明書セットを生成する必要があります。その前に、ログの内容をアーカイブして、ログが複数の証明書セットによって署名されないようにしておくことをお勧めします。これは、通常のバックアップ作業の一部として実行できます。

注	詳細は、「証明書の管理」を参照してください。新しい証明書を入手する手順は、最初に証明書を入手したときに使用した手順と同じです。

障害回復の方法

ハードウェアやディスクに障害が発生した場合には、回復のための処置を取る必要があります。iPlanet Trustbase Transaction Manager が適切に動作を継続できるよう、次の手順に従ってバックアップからデータを復元してください。

- nCipher ユーザのみ。『KeySafe User Guide』に従って、Administrator Card Set と nCipher バックアップデータを使用して nCipher の「Security World」を復元します。
- iPlanet Trustbase Transaction Manager、アプリケーションサーバ、およびデータベースをインストールし直します。
- /opt/Trustbase/TTM/<マシン名>内の *.properties および proxi.ini を修復します。
- 『インストールガイド』に記載の SQL スクリプト内で指定されているユーザの下に作成されたテーブルのバックアップから、データベースを復元します。必要に応じてデータベース管理者に問い合わせてください。

注 iPlanet Trustbase Transaction Manager のアプリケーションサーバおよびデータベースの設定方法については、「インストールワークシート」の章を参照してください。

用語集と関連サイト

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
  - トランスポートプロトコル
  - セキュリティ関連プロトコル
  - 取引プロトコル
  - メッセージプロトコル
- 用語集

ソフトウェアプラットフォーム

Solaris 8 および JDK

英語：

http://www.sun.com/software/solaris/cover/sol8.html

日本語：

http://www.sun.co.jp/software/solaris/cover/sol8.html

Java

英語：

http://www.javasoft.com

日本語：

http://java.sun.com/products/jdk/1.2/download-ja-docs.html

iPlanet Application Server 6.0

英語：

http://www.iplanet.com/products/iplanet_application/home_2_1_1n.html

日本語：

http://www.iplanet.ne.jp/products/ias6/index.html

iPlanet Web Server 4.1

英語：

http://www.iplanet.com/products/iplanet_web_enterprise/home_2_1_1m.html

日本語：

http://www.iplanet.ne.jp/products/iws4_1/index.html

Oracle 8i

英語：

http://www.oracle.com

日本語：

http://www.oracle.co.jp

Hardware Security nCipher KeySafe 1.0 および CAFast

英語 :

http://www.ncipher.com

日本語 :

http://www.tel.co.jp

トランスポートプロトコル

HTTP

HTTP/1.0 または 1.1 プロトコル :

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

http://www.ietf.org/rfc/rfc1945.txt

SMTP RFC821

ftp://ftp.isi.edu/in-notes/rfc821.txt http://www.imc.org/ietf-smtp/

セキュリティ関連プロトコル

S/MIME バージョン 2 のメッセージ仕様

ftp://ftp.isi.edu/in-notes/rfc2311.txt

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

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

DOMHASH

http://www.ietf.org/rfc/rfc2803.txt

OCSP

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

証明書リクエストと応答

PKCS10 リクエスト RFC2314 :

http://www.ietf.org/rfc.html

PKCS7 応答 RFC2315 :

http://www.ietf.org/rfc.html

取引プロトコル

Identrus

`http://www.identrus.com`

Transaction Coordinator requirements (IT-TCFUNC)

Core messaging specification (IT-TCMPD)

Certificate Status Check Messaging specification (IT-TCCSC)

メッセージプロトコル

DOM

http://www.w3.org/TR/REC-DOM-Level-1/

DTD

http://www.w3.org/XML/1998/06/xmlspec-v20.dtd

XML

http://www.w3.org/TR/REC-xml

XML 構文処理の仕様

http://www.w3.org/TR/xmldsig-core

HTML

HTML 3.2。定義については、以下のサイトを参照

http://www.w3.org/TR/REC-html32.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 ASCII サブセットによる、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 (Certificate Authority)。

CBC モード ブロック符号化方式によって暗合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合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)。`http://www.itu.int/itudoc/itu-t/rec/x/x500up/x500.html` (定義) または `http://docs.iplanet.com/docs/manuals/directory/schema/contents.htm` を参照。

CSC 証明書ステータスの確認 (Certificate Status Check)。

DER X509 で使用される特殊なエンコーディング規則。

DH データを暗号化および複合化するための公開鍵暗合化アルゴリズム。

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。関連情報については、`http://docs.iplanet.com/docs/manuals/directory/schema/contents.htm` 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)。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 共有鍵と証明書を含むスマートカードを契約カスタマに発行する発行提携銀行 (Issuing Participant Bank) またはその他の金融機関。

IR Identrus ルート (Identrus Root)。

IRCA Identrus ルート用の証明書。

L1CA CA 証明書の目的 ID または属性。

L1EESC	銀行と RC、または銀行と SC の間で、メッセージ署名に使用される証明書の目的 ID または属性。
L1EESSL	銀行と RC、または銀行と SC の間の SSL 接続で、サーバとして使用される証明書の目的 ID または属性。
L1IPSC	銀行間でのメッセージ署名に使用される証明書の目的 ID または属性。
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)。
OSI	開放型システム間相互接続 (Open Systems Inter-Connection)。
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。関連情報については、`http://docs.iplanet.com/docs/manuals/directory/schema/contents.htm` を参照。
PBE	パスワードを基づく暗合化 (Password based encryption)。
PEM	プライバシー強化メール (Privacy enhanced mail)。
RC	信頼カスタマ (Relying Customer)。契約カスタマが署名付きトランザクションを開始する相手。
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 NetMail Lite または RC Mail	カスタマ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ーフェイス。このマニュアルでは、NetMail Lite がこれにあたる。
RC ホスト	Identrus 証明書ステータス確認スキーマで RC の役目を担うサーバソフトウェア。このマニュアルでは、ポータルサーバがこれにあたる。
RP	信頼提携銀行 (Relying Participant Bank)。契約カスタマ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、信頼カスタマが問い合わせる先。
RSA	広く用いられている公開鍵アルゴリズム。暗合化またはデジタル署名に使用できる。
SC	契約カスタマ (Subscribing Customer)。Identrus アクティビティに参加する権限を持つ発行提携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 バイトの数を出力する。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)。

UTF8 複数バイト文字エンコーディング形式の一種。`http://www.utf-8.org/` を参照。

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 (TCP/IP など) 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。

完全性 電子メールメッセージが変更されていないこと。

キー (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。

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合化技術。公開鍵を使って暗合化されたメッセージは、その公開鍵と対になった共有鍵だけが復号できる。逆に、共有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。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。

証明書破棄リスト (CRL) 有効期限が切れてはいないが、無効化された証明書のリスト。

スタブ CAFast ハードサーバとの通信をサポートする Java インターフェイス。

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、一連の暗合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ネゴシエートする必要がなくなるため、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 つのセッションにつき 1 つずつ確立される。

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 認証可能で偽造または拒否されにくいデータの署名を作成するために、公開鍵暗合化法と単方向ハッシュ関数を利用したもの。

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。

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拒否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 ビットである。

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。メッセージの変更を検知するために使用される。

索引