CHAPTER 3

CORBA の Secure Sockets Layer サポート

この章では、CORBA（Common Object Request Broker Architecture）における Secure Sockets Layer（SSL）サポートについて説明します。

このシステムは、CORBA アダプタの CORBA Interface Servant（CIS; CORBA インターフェイス サーバント）で SSL モジュールを使用することにより、セキュアな CORBA トランスポートを提供します。Object Management Group（OMG; オブジェクト管理グループ）機構は、Security Attribute Service（SAS）プロトコルが定義された Common Secure Interoperability Specification Version 2（CSIv2）を定義しています。SAS によって、相互運用可能な認証、委任、および特権を導入できます。

SAS プロトコルは、自身のプロトコル要素を、接続ベースのトランスポート上でやり取りされる General Inter-ORB Protocol（GIOP）要求メッセージおよび応答メッセージのサービス コンテキストで交換します。このプロトコルの使用対象となるのは、SSL/Transport Layer Security（TLS）や Internet Inter-ORB Protocol（IIOP）over SSL（SSLIOP）を使用して得られるトランスポート層セキュリティによって、メッセージ保護（つまり、整合性や機密性）、およびサーバからクライアントに対する認証を実施している環境です。このプロトコルは、クライアント認証、委任、および特権に関する機能を提供します。これらの機能を適用すると、基礎となっているトランスポートの対応する不十分な箇所を補完できます。SAS プロトコルは、セキュア トランスポートが統合される部分の上位で高レベル プロトコルとして機能することにより、相互運用を支援します。CIS の SAS 実装は、次の機能を提供します。

- 一般的なトランスポート層セキュリティ メカニズムの使用に基づいた（たとえば、SSL/TLS によって提供される）、セキュアな相互運用性。
- GIOP の入力要求と出力要求の引数を保護するために、トランスポート層で必要に応じて提供されるメッセージ保護。
- トランスポート層で必要に応じて提供される、クライアントによるターゲットの認証。ターゲットが意図したターゲットであることを確認するために、ターゲットの身元を確認します。
- 予備的な要求を発行しなくても、意図したターゲットとの機密アソシエーションをクライアントが確立できる、トランスポート層セキュリティ。
- トランスポート層セキュリティ　メカニズムを使用して認証を受けることができないクライアントのサポート。SAS プロトコルは、トランスポート層よりも上位でのクライアント認証を提供します。
- GIOP サービス コンテキストを使用したセキュリティ コンテキストの形成をサポートするために、SAS プロトコルでセキュリティ コンテキストの確立に必要となるメッセージは、方向ごとに多くとも 1 つです。
- 単一の要求 / 応答ペアが持続している間だけ存在するセキュリティ コンテキストのサポート。
- 複数の要求 / 応答ペアで再利用できるセキュリティ コンテキストのサポート。

この実装は、OpenORB CORBA ディストリビューションで提供されるモジュール拡張を通じて提供されます。

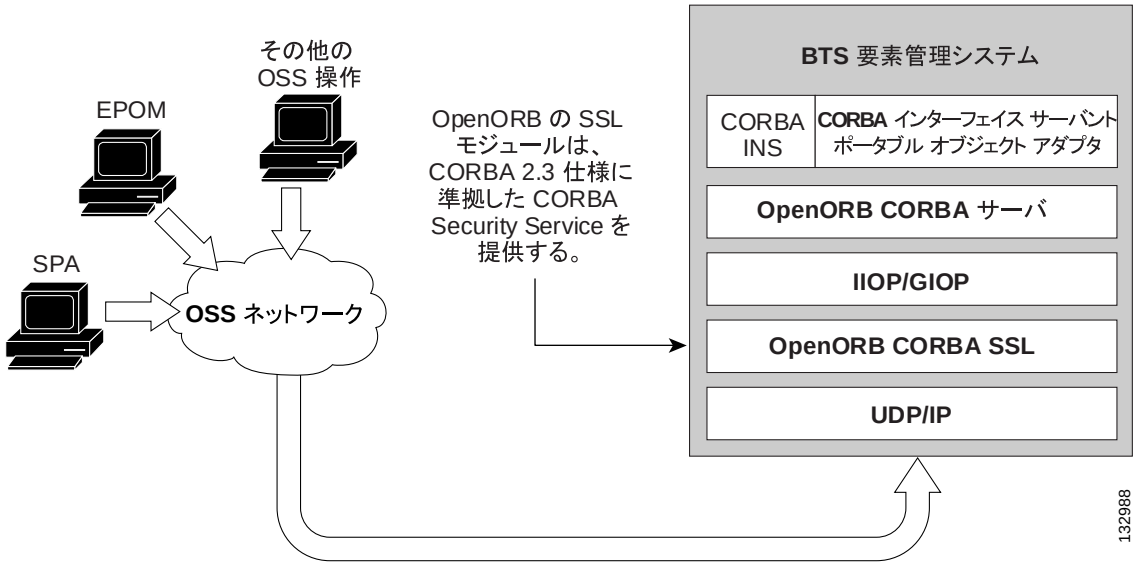
注意　セキュリティに関する予期しない問題を回避するため、CORBA アダプタのデフォルト転送プロトコルには SSL を使用してください。

システム セキュリティ拡張のシステム コンテキスト

この項では、システム セキュリティ拡張のシステム コンテキストについて説明します。システム セキュリティ拡張は、CORBA の SSL モジュール、およびセキュリティ証明書の交換の組み合せで構成されます。

図 3-1 に、システム セキュリティ拡張の影響を受ける関連システム コンポーネントの概要を示します。この概要では、Cisco BTS 10200 ソフトスイッチで影響を受けるシステム コンポーネントを示しています。例外は、ベース Solaris OS プラットフォームです。

図 3-1　CORBA の Secure Sockets Layer 実装



依存関係

この項では、セキュリティ拡張機能のアプリケーション コンポーネントにおける依存関係を示します。依存関係の大部分は、外部コンポーネントに基づいています。

縮小 Solaris イメージ

このアプリケーション コンポーネントには、特定の依存関係は存在しません。ただし、依存関係は Cisco BTS 10200 ソフトスイッチのセキュリティ ニーズに基づいています。

Java の SSL 実装

CIS アプリケーション プログラムは、CORBA のセキュリティ サポートを OpenORB の SSL コンポーネント モジュール実装に依存しています。この OpenORB モジュールは、Sun Microsystems が提供している Java の JSSE（Java Secure Sockets Extension）実装を必要とします。

証明書およびキー パスワード

この項では、証明書、および SSL CORBA のキー パスワードについて説明します。SSL CORBA の主な機能は、暗号化されたトランスポートです。この実装では、公開鍵を使用した自己署名証明書だけを使用し、すべてのユーザが同じキー パスワードを使用します。

この項では、SSL CORBA のキー ストア、トラスト ストア、および証明書が配置されるディレクトリ構造、およびこれらのファイルが従う必要のある命名規則についても説明します。Cisco BTS 10200 ソフトスイッチでは、証明書とキー ストアは Cisco BTS 10200 CIS パッケージ内に構築されます。これらは次の場所にあります。

```
/opt/BTScis/cert
```

証明書とキー ストアは、次の場所にある CORBA SDK パッケージ BTSxsdk でも使用できます。

```
/opt/BTSxsdk/cert
```

トラスト ストアとキー ストアは次のように命名する必要があります。

```
bts10200_ks bts10200_ts
```

使用する必要のある必須キー パスワードは、**Chillan** です（大文字と小文字が区別されます）。

cis-install.sh を使用した CORBA のインストールでは、*SSLIOP enabled* がデフォルトです。クライアント システムは、前述のキー パスワード、キー ストア、および証明書を使用しない限りアクセスできません。自動的な冗長化は行われないため、キー ストアとトラスト ストアは、両方の Element Management System（EMS; 要素管理システム）上にある必要があります。

（注） 以降で示すコマンドは、キー ストアとトラスト ストアを Cisco BTS 10200 ソフトスイッチ上とクライアント側に構築します。キー ストアとトラスト ストアは、デフォルトで Cisco BTS 10200 ソフトスイッチと BTSxsdk に構築され展開されますが、手動で再構築または置換することができます。ここでは、手動による操作はお勧めしません。

パスワード : Chillan

ステップ 1　キーを生成します（有効期間は 8 年）。

```
keytool -genkey -alias bts10200 -keyalg RSA -validity 2840 -keystore bts10200_ks
```

ステップ 2　証明書をエクスポートします。

```
keytool -export -alias bts10200 -keystore bts10200_ks -rfc -file bts10200.cer
```

ステップ 3　証明書をトラスト ストアにインポートします。

```
keytool -import -alias bts10200 -file bts10200.cer -keystore bts10200_ts
```