DCEセキュリティ機能を組み込んだ分散オブジェクト環境の実現方法について

1T－3

星原 健二郎*　冨士 隆*　三枝 武男**
*学習情報通信システム研究所　**北海道情報大学

1．はじめに

我々はCORBA対応の開発ツールであるSOM[1]を利用して、教材開発者が作成したマルチメディアデータの教材部品素材をデータベースへ格納し、学習システムの開発情報を統合的に管理、再利用する開発環境（REBECCA）[2]で利用するシステムの開発に取り組んでいる。その機能として教材部品素材を作成する教材開発者の認証や作成した教材部品素材をデータベースへ格納する際の認可、教材開発者情報やアクセス情報の管理などのセキュリティ機能が必要になる。

しかし、CORBA2.0対応のSOMでは認証機能，認可機能、データの機密性・完全性、において問題がある。そこで、本稿では、SOMを利用した分散オブジェクト環境にDCEセキュリティ機能を組み込むことにより、広域分散環境における認証機能、グループなどを利用した認可が可能になったのでその実現方法について述べる。

2．セキュリティ機能の比較

CORBA2.0とSOM、DCEについてセキュリティ機能の比較結果を表1に示す。

2．1 SOMのセキュリティ機能

認可は次のように行なわれる。クライアント・プログラムから要求を受け取ったサーバ・インプリメンテーション内のメソッドが、BOA(基本オブジェクト・アダプタ)を継承したSOMOAのget_principal メソッドを利用して、要求したクライアントのユーザ情報を格納するPrincipalオブジェクトを取得し、そのオブジェクト内のホスト名を利用して認可を行う。ただしSOMは、ネットワーク管理ツールと組み合わせて使用することにより、認証、ユーザ名とホスト名による認可、監査、ユーザ管理が可能となる。しかし、グループなどを利用した認可が行えない、広域分散環境で利用できない、認証やクライアントからサーバへの要求などにおけるデータの機密性、完全性を保証していないなどの問題点がある。

	CORBA 2.0	SOM 3.0	LAN Server	DCE 1.0
認　証	－	－	○	○
認　可	○	○	○	○
監　査	－	－	○	－
機密性	－	－	－	○
完全性	－	－	－	○
否認不可	－	－	－	－
運用管理	－	－	○	○
セキュリティ・ドメイン	－	LAN		広域

表1　セキュリティ機能の比較

2．2 DCEのセキュリティ機能

認証は次のように行なわれる。クライアント・プログラムがセキュリティ・サーバからユーザIDに対応する秘密キーで符号化されたネットワーク証明書を受け取り、パスワードを利用して復号化を行う。復号化が成功すると、クライアント・プログラムはセキュリティ・サーバからPAC（Privilege Attribute Certificate）を受け取る。PACにはユーザ名やユーザのグループなどに関する情報が符号

Implementations of CORBA security features by using DCE security features
Kenjiro Hoshihara*　Takashi Fuji*
Takeo Saegusa**
*Software Research Laboratory
**Hokkaido Information University

化され格納されている。

認可は次のように行なわれる。サーバ・プログラムはクライアント・プログラムからの要求を受け取ることによりPACを取得するので、サーバ・プログラムではこのPAC内の情報を利用して認可を行う。またDCEでは上記で述べた認証や認可時にネットワーク上を移動するデータの機密性、完全性を行っている。

3．DCEセキュリティ機能の組み込み

SOMにDCEセキュリティ機能を組み込んだ時の処理概要を図1に示す。

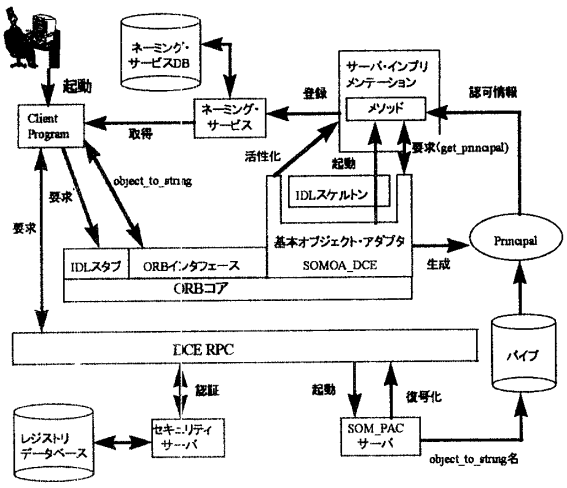

図1 処理概要

3．1 認証機能の組み込み

DCEの認証機能はクライアント・プログラムとDCEセキュリティ・サーバ間で行なわれるので、SOMとは関係なくクライアント・プログラムから、ユーザIDとパスワードを利用して認証を行うDCEのAPIを呼び出すことにより行える。

3．2 認可機能の組み込み

DCEの認可機能を組み込む時の問題点としては、認証で取得したPACの情報をいかにサーバ・インプリメンテーションに渡して認可を行うかである。

そこで以下に示すように、SOMを拡張しパイプでPACの情報を渡し認可を行うようにした。

（1）パイプによるPAC情報の受け渡し

クライアント・プログラムはDCEのサーバ・プログラムであるSOM_PACサーバを呼び出す。これにより、SOM_PACサーバは認証時にクライアント・プログラムが取得したPACを受け取る。SOM_PACサーバはセキュリティ・サーバを利用してPAC内の情報を復号化し、SOMのPrincipalオブジェクトと通信するためのパイプへ復号化したPAC内の情報を書き込む。

（2）SOMの拡張

・get_principalメソッドのオーバーライド

SOMのSOMOAを継承してSOMOA_DCEクラスを作成し、get_princiapalメソッドをオーバーライドした。このメソッドは、Principalオブジェクトを生成し、そのオブジェクトのセットメソッドを呼び出し、Principalオブジェクトを返す。

・Principalクラスの変更

PrincipalクラスはPACの情報を格納するため、データ変数及びセット／ゲットメソッドを変更した。Principalオブジェクトはget_principalメソッドからセットメソッドが呼び出された時に、SOM_PACサーバとパイプで通信し、パイプからPACの情報を取得しセットする。

4．おわりに

SOMにDCEのセキュリティ機能を組み込むことにより、広域分散環境での認証及び認証時のデータ機密性、完全性、PAC内の情報を利用した認可が行えることを確認した。

課題としては、クライアント・プログラムからサーバ・インプリメンテーションへ要求を行った時のデータの機密性、完全性がある。

参考文献

[1] 山本宏、井上重光監訳：SOM/DSOMオブジェクト指向プログラミング、富士ソフト(1996)

[2] 富士隆, 谷川健、三枝武男：ＣＡＩ開発のためのリポジトリの構築と教材部品の再利用、オブジェクト指向‘９５シンポジウム論文集 、pp301-308(1995)