CORBA セキュリティポリシー管理ツールの実装

梅澤克之[†] 鍛忠司[†] 藤城孝宏[†]
近藤勝彦[††] 洲崎誠一[†]
手塚悟[†] 佐々木良一[†††]

分散オブジェクトの標準技術 CORBA を採用することによってネットワーク上に分散化されたオブジェクトが互いを見つけ出し相互に連携することが可能になる．このような分散化されたオブジェクトにとってセキュリティ機能は重要であり，それらは CORBA Security Service として OMG（Object Management Group）により規定されている．このセキュリティ機能を持つシステムを正しく運用するためには，セキュアオブジェクト呼び出しやアクセス制御，ドメイン管理などで使われる様々な情報（セキュリティポリシー）を適切に設定・管理する必要がある．従来はコマンドラインでのキャラクタベース対話式の設定ツールは存在したが，大規模なユーザの一覧表示や，階層化されたドメイン情報の設定などには不適切であったり，様々なセキュリティポリシーの依存関係も把握しにくいものであった．本論文では，ユーザのグループや役割などのユーザ情報やオペレーション呼び出し時に要求される権利（Required Rights），ドメイン階層情報などの様々なセキュリティポリシーの管理を容易にするためのセキュリティポリシー管理ツールを提案する．

An Inplementation of CORBA Security Policy Management Tool

Katsuyuki Umezawa,[†] Tadashi Kaji,[†] Takahiro Fujishiro,[†]
Katsuhiko Kondo,[††] Seiichi Susaki,[†] Satoru Tezuka[†]
and Ryoichi Sasaki[†††]

The enterprise which constructs Intranet/Extranet system by using CORBA that is the standard technology of distributed object increases rapidly. The decentralized object comes to be able to cooperate by using CORBA between discovering each other on the network. The security function is important for such a decentralized object, and they are provided for as CORBA Security Service by OMG (Object Management Group). It is not easy to manage various information (security policy) on the secure object invocation, the access control, and the domain management, etc. In this paper, we propose the security policy management tool to facilitate the management of a variety of security policies (such as user ID, password, user's groups and roles, right required when operation is called, hierarchical information of domain etc.).

1. はじめに

OMG（Object Management Group）によって標準化が進められている分散オブジェクト技術 CORBA を使ってイントラ/エクストラネットシステムを構築する企業が増加している．CORBA を採用することによってネットワーク上に分散化されたオブジェクトがお互いを見つけ出し相互に連携することが可能になる．このような分散化されたオブジェクトにとってメッセージの機密性や認証，認可などのセキュリティ機能は重要である．OMG では，そのようなセキュリティ機能を CORBA Security Service として規定している．このサービスを利用することによって分散化された複数のオブジェクト間での相互作用を安全に行うことができるようになる．

この CORBA Security Service で規定されている仕様は，(1) 本人であることを確認するためのユーザの識別と認証機能や，(2) ユーザがオブジェクトにアクセスできるかどうかを判断するアクセス制御機能，(3) セキュリティ関連のアクションについての記録をとる

† 日立製作所システム開発研究所
Systems Development Laboratory, Hitachi, Ltd.
†† 日立システムアンドサービスプロダクトソリューション事業部
Product Solution Operations Division, Hitachi Systems & Services, Ltd.
††† 東京電機大学
Tokyo Denki University

セキュリティ監査機能，(4) クライアントとターゲット間で信頼性の確立やオブジェクト間でメッセージ交換の秘密性の確保などを行う通信セキュリティ（セキュアアソシエーション）機能，(5) データの発信元の証明や受信証明などの否認防止機能，(6) セキュリティを適用する領域を管理するためのドメイン管理機能など，多岐にわたる．これらのセキュリティ機能を正しく運用するためには，非常に多くのセキュリティ情報（セキュリティポリシー）を管理者が適切に設定する必要がある．

従来方法としてコマンドラインでの設定ツールは存在した．しかしそれはキャラクタベースの対話型ツールであり，数千，数万という数のユーザの一覧表示には不適切であり，インタフェースとそれに属する複数オペレーションの関係や，ドメインの階層構造，ドメイン間のアクセスポリシーの結合方法なども分かりにくいものであった．また類似の情報を設定することを容易にする複製機能や，複数同時設定などの機能は存在しなかった．このように従来のツールは，様々な点において機能不足であり管理者にとって分かりにくいものとなっていた．

本研究の目的は，(1) ユーザ ID やパスワード，ユーザのグループや役割などのユーザ情報や，(2) ターゲットオブジェクトのオペレーション呼び出し時に要求される権利（Required Rights），(3) セキュリティを適用する領域を指定するためドメイン階層情報やそのドメインに属するポリシー，などを設定・管理するための分かりやすく操作性に優れたセキュリティポリシー管理ツールを開発することである．

なお文献 7) では，セキュリティポリシーは「セキュリティ・ポリシーとは，当該システムのセキュリティに対する基本的方針であり，さらにポリシーの意図を具体的な指示の形態にしたものが「業務標準」あるいは「規定」である」と定義している．これに対して CORBA Security Service の仕様[6]では「システムのセキュリティサービスがどんな保護を提供すべきかを定義するためのデータである．セキュリティポリシーにはアクセス制御，監査，メッセージ保護，否認防止などの様々なポリシーがある」と定義している．本論文では後者の意味でセキュリティポリシーという言葉を使う．

以下では，まず，2 章で OMG によって規定されている CORBA Security Service の機能と動作概要，アクセス制御，およびドメイン管理について述べる．3 章でセキュリティポリシー管理ツールの実装について述べ，4 章で評価を行い，5 章でまとめを示す．

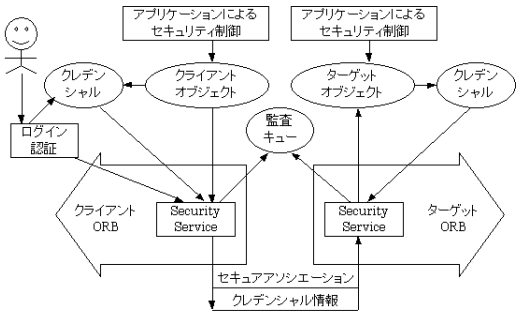

図 1 Security Service システムの動作説明
Fig. 1 Overview of Security Service System.

2. CORBA Security Service の概要

我々が開発したセキュリティポリシー管理ツールは，前章で示した CORBA Security Service 仕様のセキュリティ機能のうち否認防止機能を除いたほとんどの機能をサポートする．その中でもアクセス制御機能は分散環境に適した概念を導入しており CORBA Security Service の中心的な機能として位置付けられる．本論文ではアクセス制御機能に焦点をあてる．

2.1 動作概要

本節では，CORBA Security Service に従って実装されたシステム（以降 Security Service システムと呼ぶ）がどのように働くかを簡単に示す．**図 1** に，Security Service システムの働きについての概要を示す．

Security Service システムでは，プリンシパル（ユーザまたはユーザの代わりに動作するアプリケーション）はログイン認証を行って Security Service システムにログインする．プリンシパルが Security Service システムに正しくログインすると，Security Service システムはクレデンシャル（プリンシパルに対応するセキュリティ属性を収めたオブジェクト）を生成する．これらのセキュリティ属性は，プリビレッジ属性証明書（PAC）に含まれる．クライアントプロセスからサーバプロセスに対する最初の呼び出し時に，Security Service システムはクライアントとターゲットの間でセキュアアソシエーションを確立する．クライアントがターゲットオブジェクトを呼び出す場合，クライアント側の Security Service システムはログイン時に生成したクレデンシャルの情報を取得し，ターゲット側の Security Service システムに渡す．この情報によって，ターゲット側の Security Service システムはクライアントのクレデンシャルのコピーを作成し，そのクレデンシャルをターゲットオブジェクトで使用できるようにする．ターゲットオブジェクトは，コピー

したクレデンシャルを使ってアクセス制御を行う．

2.2 アクセス制御

Security Service システムは，クライアントからのターゲットオブジェクト呼び出し時にアクセス制御の規則（アクセスポリシー）に基づきアクセス制御を行う．

2.2.1 アクセスポリシー

従来のアクセスポリシーは，「誰がどのオブジェクトのどのオペレーションを呼び出すことができるか（できないか）」を定義することであった．しかし，分散システムでのこのようなポリシー設定は，プリンシパルおよびオブジェクトの数が増えるに従って，アクセスポリシーの大きさが膨大になってしまうという問題を含んでいる．CORBA Security Service は，セキュリティ属性，Required Rights，ドメインという概念を用いて，その問題を解決しようとしている．

- **セキュリティ属性**
  セキュリティ属性はプリンシパルをグループ化するものである．プリンシパルに与えるセキュリティ属性は，ユーザ ID やパスワードのほかにグループや役職などを含む．
- **Required Rights**
  Required Rights はオペレーションを呼び出す際に要求される権限を表すものであり，アクション（オペレーション）をグループ化する．Rights には OMG が定義した get(g)，set(s)，manage(m)，および use(u) を使用することができる．また Rights は拡張可能であり独自の Rights を定義することもできる．
- **ドメインアクセスポリシー**
  オブジェクトは起動時に 1 つのドメインに割り当てられグループ化される．各ドメインごとにドメインアクセスポリシーで，プリンシパルに与えられたセキュリティ属性に対してどんな Rights を与えるかを設定する．この Rights を Granted Rights と呼ぶ．

2.2.2 アクセス制御の具体例

オペレーション呼び出しの可否は，**図 2** に示すように，プリンシパルに与えられてるセキュリティ属性とオブジェクトが属しているドメインに設定されているドメインアクセスポリシーから Effective Rights を求める．図 2 の場合，ドメインアクセスポリシーで CN=George は g,s の Rights，Staff グループは g の Rights が与えられているので，論理和をとり Effective Rights は g,s になる．次に，求めた Effective Rights と Required Rights を Rights Combinator によって比較する．Rights Combinator が All（Any）の場合，Required Rights で指定されているすべて（1 つ以上の）の Rights が Effective Rights に含まれている場合アクセス可となる．よって，George はオペレーション Ope3 以外はアクセス可となる．

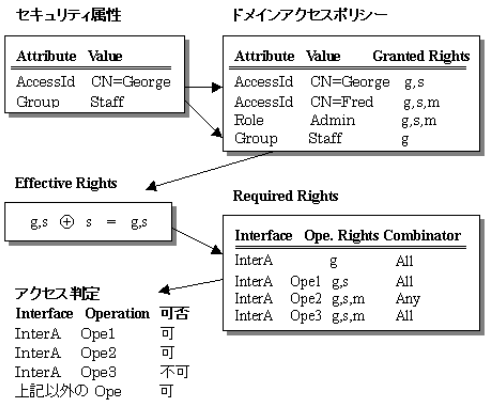

図 2 アクセス制御
Fig. 2 Access control.

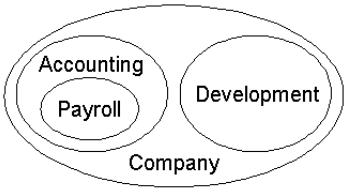

図 3 ドメイン階層の例
Fig. 3 Example of domain hierarchy.

2.3 ドメイン階層とアクセスポリシー

ドメインとは，共通のセキュリティポリシーを持つオブジェクトインスタンスの集まりであり，CORBA Security Service では，階層構造のドメインが規定されている．ただし，**図 3** に示すようにドメインどうしはオーバラップできない．つまり，1 つのオブジェクトは，ただ 1 つのドメインに属することができる．

ドメインごとに設定されたアクセスポリシーにはコンビネータ（論理積，論理和，排他的論理和）を指定し上位ドメインに設定されているアクセスポリシーとの結合方法を設定できる．

2.3.1 ドメインの階層化によるアクセス制御の具体例

具体的な例として図 3 に示すドメイン階層を持つ企業を想定して説明する．ここでは，**表 1** に示すドメインアクセスポリシーが設定されていると仮定する．

この例に基づき，以下のプリビレッジ属性を持つユーザ George を想定する．

表 1 ドメインアクセスポリシーの設定
Table 1 Domain access policy.

Domain	Attribute	G.Rights	Combinator
Company	Group:Staff	g	-
	Role:Admin	g,s,m	-
Accounting	Role:AcctAdmin	g,s	Intersection
	AccId:CN=Fred	g,s,m	Intersection
Payroll	Group:Payroll	m	Union
	AccId:CN=Boris	g	Union
Development	Role:Programmer	g,s	Intersection

- Group:Staff
- Role:AcctAdmin
- Name:George

Payroll ドメインにおける George の Effective Rights は以下のように求める．

(1) Payroll ドメインでの Rights はなし．
(2) Accounting ドメインの [Role:AcctAdmin] からの get と set (g,s) の Rights を得る．
(3) これらを Union で結合した結果，get と set (g,s) が Effective Rights となる．
(4) これらの Rights は次に，Company ドメインの [Group:Staff] 属性からの get(g) と Intersection で結合される．
(5) 最終的に George の Payroll ドメインにおける Effective Rights は，get (g) になる．

3. セキュリティポリシー管理ツールの実装

本章では，我々が開発したセキュリティポリシー管理ツール（以降管理ツール）について述べる．本管理ツールは，いままで述べてきた CORBA Security Service の機能を実現するために必要となるセキュリティポリシーを設定・管理するためのものである．本管理ツールを実装するにあたり機能目標を，従来のコマンドラインでの対話式設定ツールと比べて，情報の依存関係が分かりやすく，さらに設定操作も容易に行えることとした．また性能目標を，管理者の操作性を考慮し，待ちを意識させない程度という観点で，個々の情報の設定操作後のレスポンス時間を，多くとも 1 秒以内になるように設定した．

3.1 位置付け

図 4 に本管理ツールの位置付けを示す．Master Security Server とは，2 章で示したようなクライアントとターゲットオブジェクト間の CORBA Security Service の各種機能を提供するサーバである．本管理ツールは，この Master Security Server が使う様々なセキュリティポリシーを定義・設定するためのツールである．

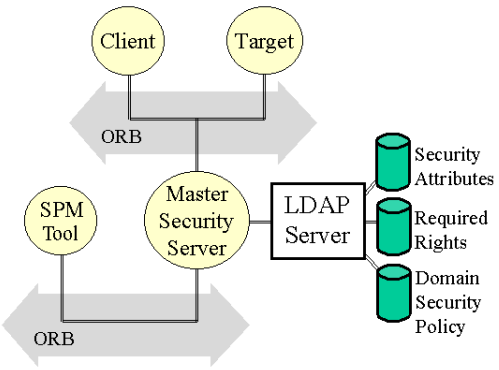

図 4 セキュリティポリシー管理ツールの位置付け
Fig. 4 Position of Security Policy Management (SPM) Tool.

表 2 パッケージ構成
Table 2 Package.

パッケージ	特徴
Tools	汎用的に使われるクラス群
Frames	グラフィックユーザインタフェース処理を行うためのクラス群
Images	アイコンやツールバー，木構造のノードなどのイメージ群
Resource	メニューやラベルなどのリソースを処理するクラス群
Data	内部データ構造を処理するクラス群
Adapter	ORB との接続を行うクラス群

本管理ツールを Master Security Server が稼動するローカルな環境内での使用を前提として実装することは可能であるが，複数の管理者による遠隔地からの管理が行えなくなり利便性が損なわれてしまう．そこで本管理ツール自体を CORBA クライアントとし，Master Security Server に対してリモートアクセスが可能となるように実装を行った．本管理ツールを使う管理者は，管理者権限で Master Security Server にログインし認証され，本管理ツールと Master Security Server の間の通信は CORBA Security Service のセキュアアソシエーション機能により安全性は保たれることになる．このように本管理ツールを CORBA クライアントとすることにより，遠隔地からの管理が可能になるとともに，CORBA Security Service の機能を用いてセキュアな通信が可能となる．

3.2 パッケージ構成

本管理ツールは，前述のように遠隔管理を前提としているため様々なプラットフォームで実行される可能性がある．このようにプラットフォーム非依存性を実現するために Java 言語を用いて実装した．パッケージ構成は，その特徴により**表 2** に示すような構成にし

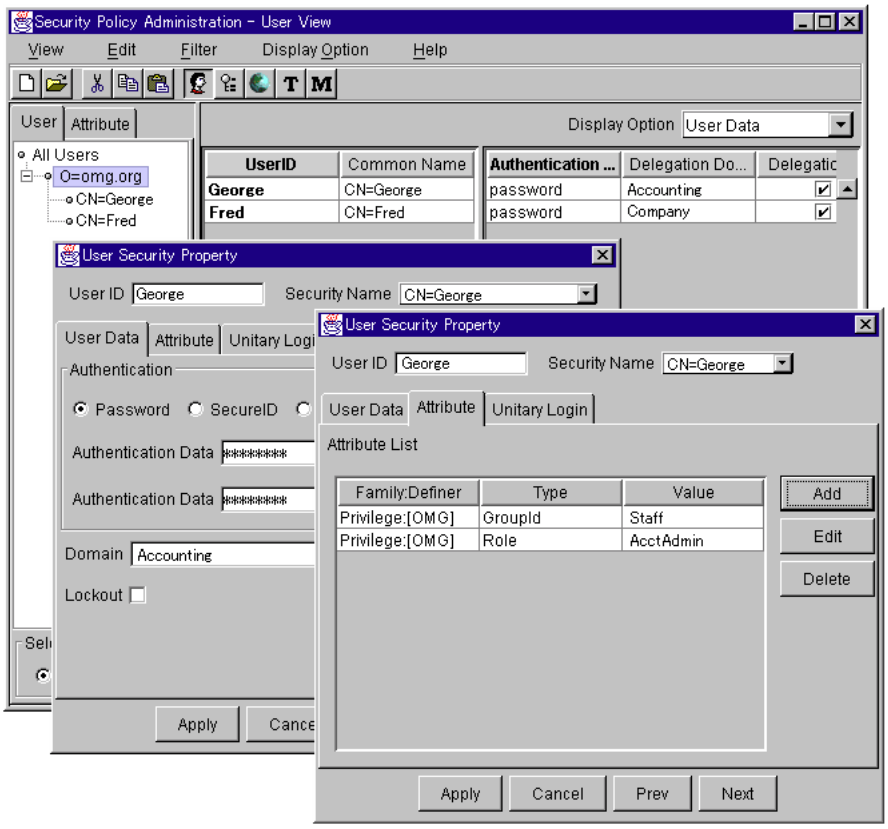

図 5 ユーザ画面
Fig. 5 User screen.

た．特に Data パッケージはグラフィックに依存しない内部データ構造を保持するクラス群，Adapter パッケージは直接 ORB との接続を行うクラス群である．

3.3 管理シーケンス

前節のパッケージ構成に従って実装した管理ツールを用いて，管理者が Master Security Server に接続し各種セキュリティ情報を設定する際の一般的な動作の流れは以下のとおりである．

(1) まずアクセス権を持っている管理者は，Master Security Server にログインする．
(2) 管理者が管理ツールにより，ユーザ ID やパスワード，その他のセキュリティ属性などを設定する．
(3) 管理者が Master Security Server 側に通知するために Apply ボタンを押下する．
(4) 管理ツール内部でセキュリティ情報を表すデータ構造を構築する．
(5) Adapter を通して Master Security Server のオペレーションが呼び出される（事前に Master Security Server にログインしているためこの呼び出しはセキュアに行える）．
(6) Master Security Server でデータベースを更新し結果が通知される．

3.4 画面構成と特徴

本節では管理ツールの画面構成とその特徴を示す．全体的な画面構成は，CORBA Security Service の概念を直感的に認識しやすいように，2.2.1 項で示したユーザのセキュリティ属性，オペレーションに対する Required Rights，セキュリティポリシーを適用するドメインの 3 要素に対応する 3 画面構成とした．さらにそれらの設定情報の統合チェックのためのテスト画面を実装した．また管理者に対して一貫した操作性を提供するため，ユーザ画面，Required Rights 画面，ドメイン画面は，左側に木構造，右側に一覧表示という構造とした．木構造により目的とする対象を見つけやすくでき，また一覧表示により各種設定情報の視認性を向上させるという効果を狙ったものである．

3.4.1 ユーザ画面

ユーザ画面の外観を**図 5** に示す．木構造による検索性の向上や一覧表示による視認性の向上とともに，

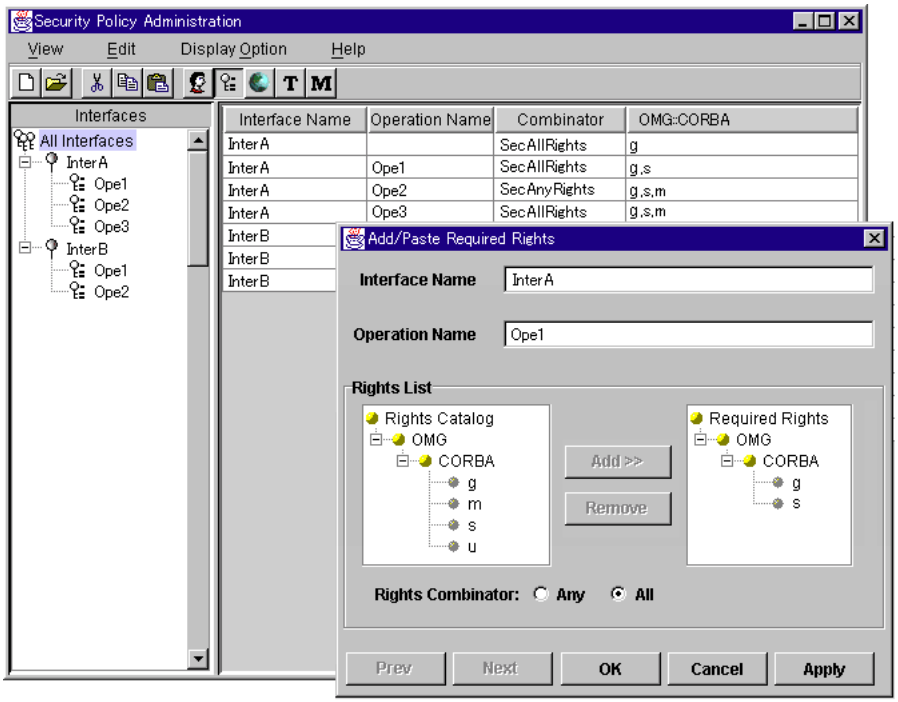

図 6 Required Rights 画面
Fig. 6 Required Rights screen.

選択ボタンによる設定や，複数ユーザの一括設定，セキュリティ属性の複製機能なども実現し操作を向上させた．また CORBA Security Service の仕様では，たとえば，ユーザのセキュリティ属性についてアクセス ID は 2，グループ ID は 4，ロールは 5 というように規定されているが，本管理ツールでは，それらの整数型の情報を隠蔽して使いやすさを向上させた．図 5 はユーザ George の詳細情報を表示・設定する画面であり，George に Group が Staff で，Role が AcctAdmin というセキュリティ属性を設定していることを示している．

3.4.2 Required Rights 画面

Required Rights 画面の外観を**図 6** に示す．ユーザ画面と同様に木構造および一覧表示を採用するとともに，設定方法ではあらかじめ登録されている Rights を選択するだけの簡単な操作で Required Rights の設定を可能にした．また，オペレーション名ではなくインタフェース名に対して Rights を設定することによって，オペレーションに Rights が設定されていないときに使用するデフォルト Rights の設定を可能にした．図 6 はインタフェース InterA のオペレーション Ope1 の Required Rights 情報を表示・設定する画面である．InterA の Ope1 を呼び出すには，“g” と “s” の両方の Rights を持っていなければならないことを示している．

3.4.3 ドメイン画面

ドメイン画面の概観を**図 7** に示す．CORBA Security Service の仕様では，ドメインは階層型であり，個々のドメインは別々のポリシーを持つことができる．本管理ツールでは，ドメイン間のアクセスポリシーの依存関係を把握しやすくするために，複数のポリシーウインドウを右側フレームに表示することとした．またアクセスポリシーウインドウ内もセキュリティ属性と Rights の複雑な関係を把握しやすくするために木構造を採用した．設定方法は Required Rights と同様に事前登録されているセキュリティ属性と，事前登録されている Rights を選択するだけの簡単な操作方法を実現した．図 7 の左側フレームの木構造は，図 3 で示したドメイン階層を表している．また右側フレームは Payroll ドメインに設定されているアクセスポリシーであり，このドメインで Role が supervisor の人に “s” の Rights を与える設定であることを示している．

3.4.4 テスト画面

これまで Security Service システムの動作概要とそこで使用する各種セキュリティ情報の意味およびそれらを設定するための管理ツールの画面を説明してきた．本管理ツールはこれらの情報が正しく設定できているかどうかを，実際にシステムを運用する前に検証

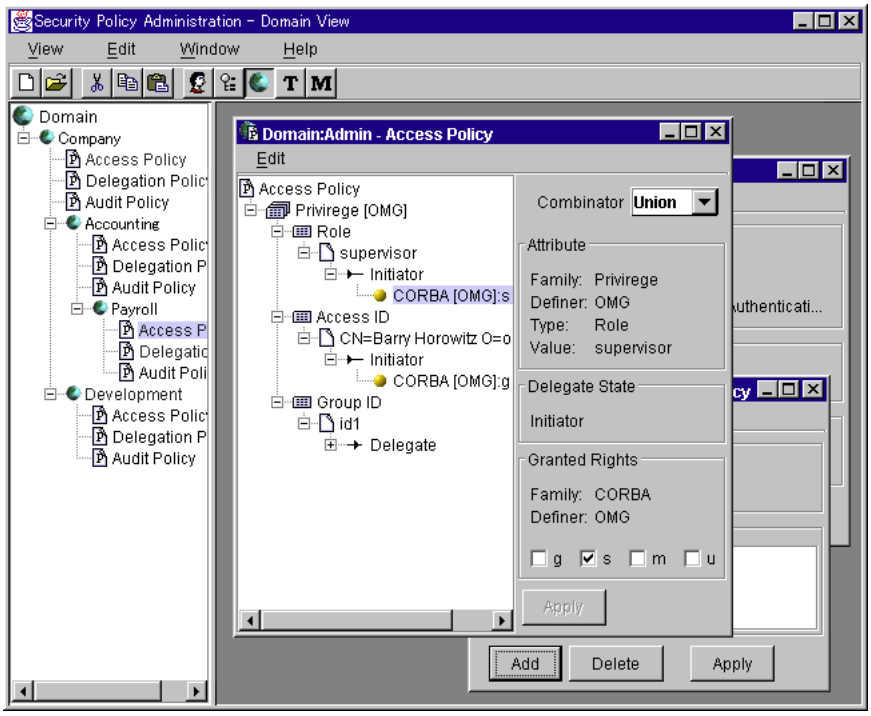

図 7 ドメイン画面
Fig. 7 Domain screen.

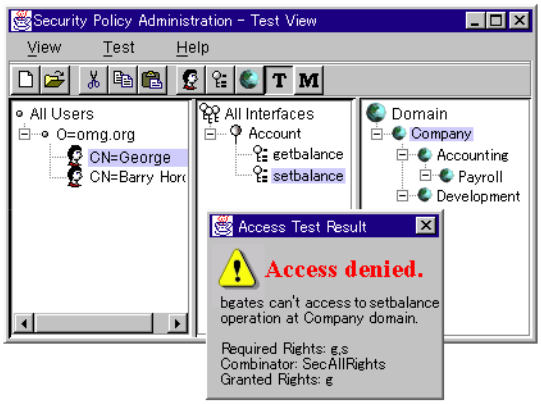

図 8 テスト画面
Fig. 8 Test screen.

することができる機能を提供する．テスト画面の概観を**図 8** に示す．ユーザ情報，Required Rights 情報，ドメイン情報の 3 つの木構造から，アクセス判定を行いたいユーザ，オペレーション，ドメインを選択すると，それらの相互関係からアクセスが許可されるか否かを自動判定できる．本機能により，設定ミスによる管理者の意図しないアクセスを未然に防ぐことが可能となった．図 8 は George が Company ドメインで Account インタフェースの setbalance オペレーションを呼び出せるかどうかをチェックした画面である．

4. 評　　価

4.1 機 能 評 価

従来のコマンドラインの設定ツールと，いままで見てきたようなグラフィカルなユーザインタフェースを持つ本管理ツールを比較し，操作性が向上したかどうかを評価する．本管理ツールはセキュリティ管理者が用いるツールであるので，CORBA Security Service の概念については理解があり，従来のコマンドライン対話式の設定ツールを使った経験のある被験者の中から無作為に 7 人を選びアンケート形式で評価を行った．結果を**表 3** に示す．

ここで必要性とは，従来のコマンドライン設定ツールと比較して本管理ツールの機能の存在価値であり，5 が最高（あると便利），3 が中間（どちらでもよい），1 が最低（ないほうがよい）というランク付けで評価してもらった．また操作性とは，ユーザインタフェースの操作のしやすさであり，5 が最高（操作しやすい），1 が最低（操作しにくい）というランク付けである．

表 3 より，ユーザやインタフェースの複製機能など従来のコマンドライン設定ツールで実現できていなかった機能に対する評価は高いものになっている．ま

表 3 機能評価
Table 3 Function evaluation.

測定対象操作	必要性	操作性
既存ユーザのパスワード変更	4.4	4.0
既存ユーザへグループ属性の追加	4.9	4.4
新規ユーザの追加	4.9	4.0
ユーザの複製	5.0	4.6
既存 Rights の変更	4.7	4.1
新規インタフェースと Rights の追加	4.6	4.3
新規オペレーションと Rights の追加	4.6	4.3
Required Rights の複製	4.7	4.4
インタフェースの複製	4.9	4.6
ドメインの作成	4.7	4.3
子ドメインの作成	4.7	4.3
アクセスポリシーの設定	4.6	4.0
アクセスポリシーの複製	4.7	4.3
テスト機能	4.7	4.1
画面構成	4.6	4.4

必要性 5：あると便利 3：どちらでもよい 1：ないほうがよい
操作性 5：操作しやすい 3：普通 1：操作しにくい

表 4 性能評価
Table 4 Performance evaluation.

測定対象操作	時間
セキュリティ属性として AccessID を設定し，さらにユニタリログイン情報も設定した 3,000 人分のユーザ一覧の初期表示完了	2 分 10 秒（1 分 45 秒）
1000 インタフェース・1000 オペレーションが設定されているときの Required Rights 一覧の初期表示完了	1 分 07 秒（55 秒）
最深階層（121 階層）のドメインからの全 Access Policy 設定ダイアログ表示完了	57 秒
最深階層（121 階層）のドメインからの全 Audit Policy 設定ダイアログ表示完了	37 秒
最深階層（121 階層）のドメインからの全 Delegation Policy 設定ダイアログ表示完了	37 秒

※括弧内はサーバ側処理時間

たテスト機能など管理者の思考を助ける機能も高い評価を得た．操作性に関しては，画面構成は CORBA Security Service の基本概念であるユーザ属性，Required Rights，ドメインポリシーの 3 要素を画面として持ち，またそれぞれの画面の構成も左領域に木構造，右領域に一覧表示という一貫した画面構成を提供することで高い評価が得られたと考えられる．また，その他の操作性に関しても特に操作しにくいという項目もなく，高い評価が得られた．

さらにその他の意見として，情報を視覚的・直感的に把握しやすいという評価を得た．CORBA Security Service で定義しているセキュリティ属性や Required Rights，ドメインアクセスポリシーなどの関係は複雑であるが，本管理ツールを操作することで経験的にそれぞれの設定値がどういう関係にあるのかを理解できるというメリットは大きいと考えることができる．

4.2 性能評価

単一ユーザのセキュリティ属性設定や，単一ドメインの単一のアクセスポリシーの設定などの個々の操作に関しては，どれも 1 秒にも満たない時間で終了しており，管理者に対して待ちを意識させないレベルを実現することができた．

本管理ツールは大規模ユーザや多階層ドメインを想定しているため，大量のデータを扱う場合の性能評価を行った．**表 4** は CPU：Intel PentiumII 450 MHz，メモリ：256 MB のマシンでの測定結果である．

ユーザ一覧や Required Rights 一覧などの一覧表示において多量のデータが存在する場合，サーバ側からの情報取得に時間がかかっている．しかし表 4 に示したように，その処理時間の大部分はサーバ側の処理に要する時間であり，グラフィカル化したことによる性能劣化は少ないと考えられる．また，管理ツール内で情報をキャッシングしているため，同一データを操作する場合には，このキャッシングにより高速な操作を可能にしている．今後さらなる高速化や多量データの操作のためには，マルチスレッドによる情報のバックグランドでの取得や，情報の分割取得（テーブルに初期表示する情報のみ取得）などの対策が考えられる．

5. おわりに

ユーザ ID やパスワード，ユーザのグループや役割などのユーザ情報や，オブジェクトのインタフェース/オペレーション呼び出し時に要求される権利（Required Rights），セキュリティを適用するためのドメイン階層情報やそのドメインに属するアクセスポリシーなどの様々なセキュリティポリシーの管理を行うセキュリティポリシー管理ツールを開発した．従来のコマンドラインでの対話式設定ツールと比べ本管理ツールでは，複雑なセキュリティポリシーの構造を分かりやすく表示することができ，また設定操作を容易に行えるようになった．さらに，運用前テスト機能により，設定ミスなどの管理者の意図しないアクセスを未然に防ぐことができるようになった☆．

謝辞 本研究の機会を与えていただいた日立製作所システム開発研究所セキュリティシステム研究センタの宝木和夫センタ長に感謝する．また，本研究を進めるにあたって有益なご意見をいただいた日立製作所ソフトウェア事業部赤尾杉隆氏，CORBA Security Ser-

☆ 本論文ではアクセス制御機能のみについて述べたが，本セキュリティポリシー管理ツールでは委譲ポリシーや監査ポリシーの設定などにも対応済みである．

vice 仕様について多くの有益なコメントをいただいた Hitachi Computer Products (America), Inc. の Bret Hartman 氏に深く感謝する．

参 考 文 献

1) Blakley, B.: *CORBA Security An Introduction to Safe Computiong with Objects*, Addison-Wesley (1999).
2) Mowbray, T.J. and Ruh, W.A.: *Inside CORBA Distributed Object Standards and Applications*, Addison-Wesley (1997).
3) Orfali, R. and Harkey, D.: *Client/Server Programming with Java and CORBA*, John Wiley & Sons (1997). 並河英二，水野貴之，池浦規之（訳）：Java & CORBA C/S プログラミング，日経 BP 社 (1997).
4) 成田，保西，勝亦，島村，島村，杉能：CORBA と Java 分散オブジェクト技術，ソフト・リサーチ・センター (1997).
5) Common Object Request Broker Architecture (CORBA) Specification 2.4, OMG (2000).
6) CORBA Security Service, Version 1.5 Specification, OMG (2000).
7) 広瀬，高橋，土居：コンピュータソフトウェア事典，丸善 (1990).

商標などに関する表示

- CORBA は，Object Management Group が提唱する分散処理環境アーキテクチャの名称です．
- Intel および Pentium は，米国 Intel Corporation の登録商標です．
- Java は米国 Sun Microsystems, Inc. の商標です．

(平成 12 年 12 月 11 日受付)
(平成 13 年 6 月 19 日採録)

梅澤 克之（正会員）

1996 年早稲田大学大学院理工学研究科機械工学専攻修士課程修了．同年（株）日立製作所システム開発研究所入所．以来，企業情報システム，分散オブジェクトシステムのセキュリティ技術等の研究・開発に従事．

鍛 忠司

1996 年大阪大学大学院基礎工学研究科情報工学分野博士前期課程修了．同年，（株）日立製作所勤務．企業情報システム，分散オブジェクトシステムのセキュリティに関する研究開発に従事．

藤城 孝宏

1993 年慶応義塾大学理工学研究科電気工学専攻修士課程修了．同年（株）日立製作所入所，マイクロエレクトロニクス機器開発研究所を経て，現在，システム開発研究所セキュリティシステム研究センタ勤務．ネットワーク管理システム等の研究を経て，現在，セキュリティシステム，特に電子認証の研究開発に従事．電子情報通信学会員．

近藤 勝彦

1986 年愛知県立一宮工業高等学校電気科卒業．同年日立中部ソフトウェア（株）（現（株）日立システムアンドサービス）入社．主に通信システム系の開発業務に従事．1998 年 5 月（株）日立製作所システム開発研究所派遣．以来，分散オブジェクトシステムのセキュリティ技術等の研究・開発に従事．

洲崎 誠一（正会員）

1991 年横浜国立大学電子情報工学科卒業．同年（株）日立製作所システム開発研究所に入所．以来，情報セキュリティ技術の研究開発に従事．現在，同研究所セキュリティシステム研究センタ研究員．1996 年情報処理学会第 52 回全国大会優秀賞，平成 12 年度山下記念研究賞受賞．

手塚　悟（正会員）

1984 年慶応義塾大学工学部数理工学科卒業．同年（株）日立製作所マイクロエレクトロニクス機器開発研究所を経て，現在，システム開発研究所セキュリティシステム研究センタ勤務．パーソナルコンピュータのオペレーティング・システム，デバイス・ドライバ，LAN システムの研究を経て，現在，セキュリティシステム，特に電子認証の研究開発に従事．工学博士．

佐々木良一（正会員）

1971 年 3 月東京大学卒業．同年 4 月日立製作所入所．システム開発研究所にてシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事し，ネットワーク管理システム NETM や各種セキュリティシステム等の製品化に貢献．同研究所第 4 部（ネットワーク関連部）部長やセキュリティシステム研究センタ長，主管研究長等を経て 2001 年 4 月より東京電機大学工学部教授．工学博士（東京大学）．1983 年電気学会論文賞受賞．1998 年電気学会著作賞受賞．著書に，「インターネットセキュリティ 基礎と対策技術」（共著，オーム社，1996），「インターネットセキュリティ入門」（岩波新書，1999），「インターネットコマース新動向と技術」（共編著，共立出版，2000）等．IEEE，電子情報通信学会，電気学会等の会員．情報処理学会コンピュータセキュリティ研究会主査．