2003－UBI－2 (1)
2003／11／18

マルチエージェント方式によるセキュアでオープンな情報流通ネットワークの構築

雨宮 聡史† 岩尾 忠重‡ 雨宮 真人†

†九州大学 大学院 システム情報科学研究院
‡富士通研究所 Webテクノロジ研究部

近い将来，広域ネットワーク上の各種の情報資源を公共利用することが一般的となることが予想される．しかし，公共資源と私的資源とを区別して管理することのできる統一化されたセキュリティシステムを内包したネットワーク環境という概念は未だない．本稿では，マルチエージェントシステムをベースにして，統一化されたセキュリティ方式による柔軟で安全な情報流通ネットワークの構築方法を提案する．具体的には，個々の計算資源および情報資源を公共の利用に供するPublic Zoneと外部からのアクセスを禁止するPrivate Zoneとに分離し，個々のPrivate Zoneへのアクセスセキュリティを保証し，かつ，遊休資源を公共の利用に供する情報流通環境を構築する方法を論ずる．

Developing Open Secure Network Environments with Multi-Agent

Satoshi Amamiya†, Tadashige Iwao‡ and Makoto Amamiya†

†Faculty of Information Science and Electrical Engineering,
Kyushu University
‡Web Technology Laboratory, Fujitsu Laboratories, Ltd.

In near future, people will be able to access information or resources on the public open network environments. However, there are currently few network environments which have unified method for information or resource protection. We propose a unified resource protection scheme and its application for developing open and secure networks based on a multi-agent system.

1 はじめに

今後，グリッド・コンピューティングやユビキタス・コンピューティングなど，広域情報共有流通サービスにおいて広域ネットワーク上の各種の計算資源および情報資源を公共利用することが一般的となってくると予想される．また，Peer to Peerの情報交流が一般化し公共資源，私的資源へのアクセスが頻発するようになる予想される．このようなユビキタス情報環境においては，自由にアクセスを許す公共資源と他人からのアクセスを排除する私的資源を明確に区別して管理することのできるセキュリティ管理の問題が重要な技術課題となる．一方，現状のセキュリティ管理では，公共的に利用される資源と私的に使用する資源を明確に区別して統一的なアクセス管理を行うという方法は見当たらない．従来方式では統一化されたセキュリティシステムを内包したネットワーク環境という概念が欠如しているため，個々の情報資源に対するセキュリティはアプリケーションごとに個別に管理するという方法が取られている．たとえば，Adobe PDF文書やMicrosoft Office文書などの独自セキュリティ方式がよく知られているが，これらの方式には互換性はなく，ユー

ザの利便性を考慮しつつ，統一的方法によって十分な保証を与えるということが困難である．

本稿では，２つのマルチエージェントシステム Kodama[4] と VPC[1] を融合させ，個々の計算資源および情報資源を公共の利用に供する Public Zone と外部からのアクセスを禁止する Private Zone という概念 [5] を導入することで，個々の Private Zone へのアクセスセキュリティを保証しつつ，遊休資源を公共の利用に供する情報流通環境を構築する方法を提案する．

なお，以下の議論ではエージェント間のメッセージ通信においてメッセージは既存の暗号アルゴリズムを用いて暗号化されていることを前提とする．

2 エージェントシステム Kodama と VPC

Kodama は静的な環境としての階層性のある論理ネットワーク構築を特徴とし，一方，VPC は動的な環境としての論理的単一空間の形成を指向している．この静と動，多段と単一の融合を計ることは，特に本システムのような現実社会のためのシステムを考える上で都合がよい．

2.1 Kodama

マルチエージェントシステム Kodama は，個々のユーザおよびユーザが属すコミュニティ（企業や私的グループなど各種のコミュニティ）を柔軟に論理ネットワークとして表現できるマルチエージェントシステムである．Kodama におけるコミュニティは図１に示すように階層構造をなしている．個々のユーザは社会構造のどこかのコミュニティに属していると考えるのが普通であり，Kodama におけるコミュニティ構造は人間社会における企業や団体の形成構造に対応させやすい．また，人間のコミュニティはいろいろな活動目的に応じて形成されるので，個人はその活動目的によって複数のコミュニティに属すことも普通なことである．同様に，Kodama エージェントも複数の Kodama コミュニティに属することが可能である．また，Kodama ではコミュニティもエージェントとして扱う．このコミュニティの窓口となるエージェントを特にポータルエージェントと呼んでいる．

エージェントやコミュニティはそれぞれ属性をもっており，この属性の管理はポータルエージェントの持つコミュニティ管理機能の一環として行い，後述の VPC 機能のための情報として用いる．

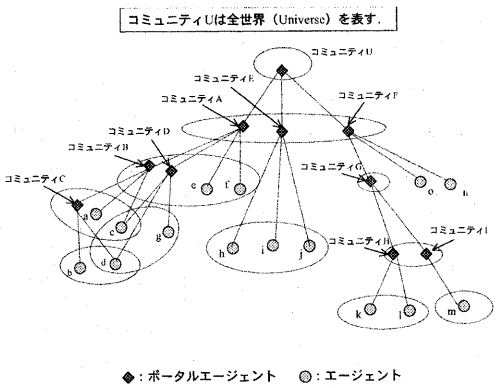

図 1: Kodama のコミュニティ階層構造

エージェントとコミュニティの名前はコミュニティの階層構造に沿ったアドレスとして与えられる．各コミュニティには１個のポータルエージェントが存在し上位コミュニティとのインタェース機能をもつ．ポータルエージェントは図２に示すような上位コミュニティおよび下位コミュニティのテーブルを管理する．上位コミュニティテーブルには自分が所属する上位のコミュニティが登録され，下位コミュニティテーブルには自分が管理するエージェントが登録されている．下位コミュニティはポータルエージェントにとっては一つの資源として扱われ，ポータルエージェントが管理する．また，ポータルエージェントは上位と下位の間のメッセージ転送をセキュリティの観点から制御する．

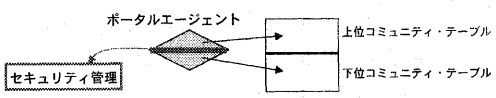

図 2: ポータルエージェントとコミュニティ管理

2.2 VPC

VPC(Virtual Private Community) は，動的な環境における P2P コミュニケーションを意識したマルチエージェントシステムであり，システムの挙動がユーザ属性と所属する環境によって変化することを最大の特徴としている．図３は VPC モデルの概要を示している．

VPC では，エージェントの機能は Role と呼ばれる計算主体の集合で定義される．また，Policy

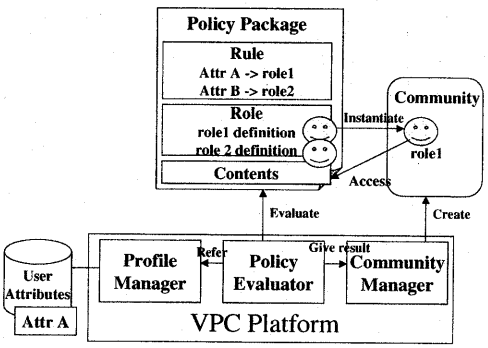

図 3: VPC 概要

Package と呼ばれる属性から Role への写像ルールの集合を評価することで，VPC エージェントは使用する Role を自分の属性の変化に合わせて動的に変更することができる．なお，Role 自体は Policy Package の中で定義されているので，エージェントは新たに Policy Package を得ることで，新しい Role（機能）を手にすることも可能である．

Policy Package は，エージェントがある環境に入った時に，その環境に既に属している他のエージェントより配付される．VPC では，同一の Policy Package を共有しているエージェント群をコミュニティと呼び，グループ化している．このコミュニティは Kodama のコミュニティとは異なり，階層構造をなしていないのでコミュニティ間の繋がりという概念は基本的には存在しない．

VPC におけるセキュリティは，ユーザシステムの属性を一切外部に出さないという思想の基に成り立っており，各エージェントは Policy Package から得られた Role のみで通信を行う．このため，コミュニティ内では，エージェントはお互いの存在を知ることはない．

3 Public Zone と Private Zone

柔軟な論理ネットワークを設定できると同時にセキュリティを確保するために，Public Zone と Private Zone を備えたアーキテクチャを考える．ところで，セキュリティレベルの違う空間を設けることは，さして新しいものではない．古くは MULTICS[3] までさかのぼり，最近では Java 仮想マシンの Sand Box[2] モデルが有名である．本システムでは，概念上，Public Zone は公共広場として位置づけ，いかなるメッセージや情報，資源も通過したり保管することが許される空間である．また，いかなるエージェントもコミュニティに加入するときは，自分の Public Zone 内にコミュニティで指定されたサービスを提供しなければならない．これはコミュニティに参加するための契約条件として提供すべきものであり，Tax と考える．一方，Private Zone は，主に私的利用のための空間であり，厳格にアクセス制限される．Public Zone と Private Zone は，図 4, 図 5 に示すように上下の 2 層構造の関係があり，Private Zone へのアクセスは必ず Public Zone を通過する．この 2 層の間で通信のアクセス管理を行うことで，オープンでかつ安全なシステムを構築することができる．このアクセス制御は VPC のポリシパッケージと Role の概念を応用している．Public Zone と Private Zone の 2 層化の概念を，論理ネットワーク層におけるエージェントコミュニティ管理機能として具体化する．

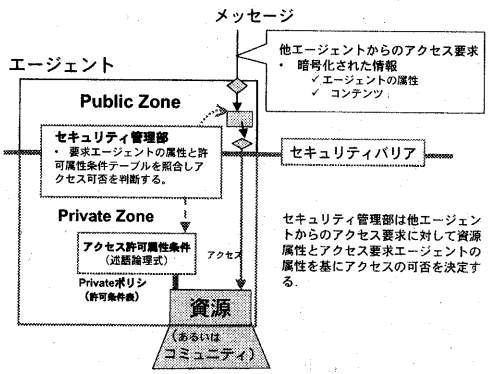

図 4: Private 資源へのアクセス

3.1 資源の管理とアクセス制御

本システムは，あらゆる対象を資源として扱う．具体的には，ファイルとして存在する文書等だけではなく，論理的な存在であるエージェントやコミュニティも資源として扱い，全ての資源に対して属性，アクセスルール等が存在する．これは VPC のポリシを基にしたものである．Public Zone の資源に対しては Public ポリシ，Private Zone の資源に対しては Private ポリシが対応する．

Public ポリシはエージェントがコミュニティ内で提供しなければならないサービス群との対応ルー

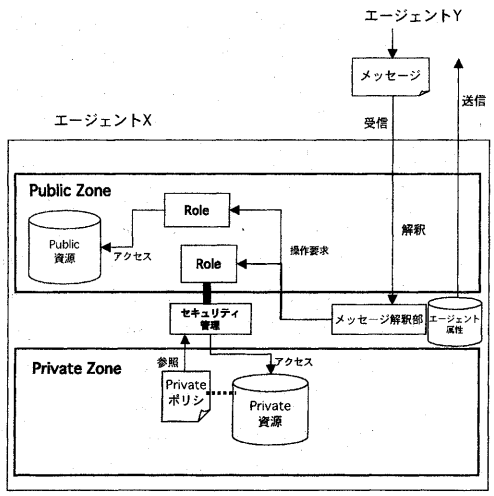

図 5: エージェント内部ブロック図

ル（述語論理式など）で構成されている．Public ポリシはポータルエージェントにより配られ，Public ポリシを受理したエージェントはそのサービスを Public Zone において提供しなければならない．このサービスはエージェント内部では VPC の Role として動作する．Private ポリシはエージェント属性と Private 資源に対するアクセス可否を対応させるルールであり述語論理式で記述される．Private ポリシは Private Zone 内の資源に付加される．(図 5 を参照)

複数のエージェントが互いに通信を行うということは，互いの Public Zone 内で動作している Role を通じて情報のやり取りを行うということを意味している．通常，Role は実行環境のアクセス制御によって Public 資源のみにアクセス可能であり，Private Zone 内の Private 資源にアクセスできない．しかし，エージェントの属性によっては通信相手のエージェントの Private 資源にアクセスすることが許可される．Private 資源に対するアクセス可否は Private ポリシとその資源にアクセスする者（エージェント）の属性の両方に基づいて決定される．

3.2 ポータルエージェントの資源管理

ポータルエージェントは資源属性（コミュニティ属性）の管理に関して、以下のことを行う．

1. コミュニティに加入するエージェントに対して新規加入エージェントの加入条件（契約）の管理を行う．契約を受理するエージェントに対してそのコミュニティ内のエージェントへのアクセス許可属性を付与する．

2. コミュニティ外に対して見せる（このコミュニティがエージェントとして振舞う）ときのエージェント属性を管理する．

3. Public として提供する機能（Public ポリシ）の選択・管理を行う．Public として提供する機能はコミュニティへの加入契約によって定められる．

ポータルエージェントはアクセス制御に関して以下のことをする．

1. 他コミュニティのエージェントからのメッセージはメッセージ受信部で受信される．このメッセージにはメッセージのコンテンツに加えて送信元エージェントの属性が付されている．

2. メッセージ受信部で受信したメッセージはその送信先が他のコミュニティであれば，Public Zone 内で処理され，他のコミュニティに転送される．このとき，Public Zone に置かれている，メッセージのルーティング・転送，他サービスの探索，メッセージ転送のためのアドレスキャッシング，関連情報のキャッシング，などの公共サービスルーティンが動作する．

3. メッセージの送信先がこのコミュニティ内の Private 資源であれば，ポータルエージェント内のセキュリティ管理部がこのメッセージ中の属性を解読し，その送信元の属性がアクセス許可条件にかなうものであるか否かを検査する．許可条件にかなう場合は Private 資源へのアクセスを許可する．

4. Private 資源へのアクセスは次の場合がある．

   - Private 資源がコミュニティ内エージェントの場合は，このメッセージを当該エージェントに転送する．
   - Private 資源がファイル等の場合は，Private Zone 内の資源のなかでアクセス許可属性にかなうものへのアクセスを許可する．

なお，アトミックなエージェントは，図2において，下位コミュニティテーブルが空であるポータルエージェントとして見なすことができるので，ポータルエージェントと全く同様の仕組みを用いてデータやプログラム等の資源に対するアクセス管理ができる．

4 具体的な例

Public と Private という二つの空間と二つのポリシの具体的な使用例として，エージェントがコミュニティに加入するときの様子と，エージェント間での資源のやり取りを紹介する．特に，後者は Digital Rights Management(DRM) に有効であることを示す例である．

4.1 コミュニティへの加入の例

いま，図6に示すようなリサーチコミュニティAというコミュニティがあるとする．リサーチコミュニティAに加入するためにはエージェントは ACM_Member か IEEE_Member という属性を持っていなければならない．また，リサーチコミュニティA の Public ポリシには、" 属性 ACM_Member を持っているエージェントは 100MB のディスクの自由使用サービスを提供し，属性 IEEE_Member を持っているエージェントは 500MB のディスクの自由使用サービスを提供する" という加入条件（契約）が書いてある．

このコミュニティに3つのエージェント X,Y,Z が加入しようとしている状況を考える．X は属性 ACM_Member を持ち，Y は属性 IEEE_Member を持ち，Z は属性 AAAI_Member を持っている．

上記エージェント X の内部動作を図5に従って説明する．

1. エージェント属性の一部である ACM_Member 属性を送信し，リサーチコミュニティA のポータルエージェントから Public ポリシを取得する．
2. ポリシ解釈部はリサーチコミュニティA ポータルエージェントから受け取った Public ポリシを解析して "100MB のディスクスペースの提供" という Role を導出し起動する．
3. このとき起動された Role はファイル（または容量が 100MB のディレクトリ）に対する Read, Write 操作のみの Role となる．

Y と Z についても同様の内部動作が行われ，その結果，X と Y はリサーチコミュニティA に加入できるが，Z は加入することができないことになる．また，リサーチコミュニティA のポータルエージェントが発行する Public に従って X は 100MB, Y は 500MB のディスクスペースを公共資源としてコミュニティ内に提供することになる．

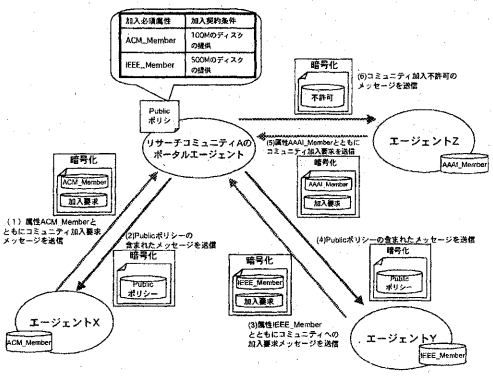

図 6: コミュニティへの加入

4.2 エージェントの資源操作の例

一般的には，各エージェントの通信と内部動作は以下のような手順を踏む（図5を参照）．

1. エージェント Y はエージェント X に情報 I を要求する．この時，Y は自分の属性の一部を X に提示する．
2. X は情報 I を操作するために X の Public Zone 内に情報 I 用の Role を起動する．このとき，Role の属性は Y の属性に設定される．
3. Role の情報 I についての操作はセキュリティ管理部でチェックされる．
4. セキュリティ管理部は Private ポリシと Role の属性を照らし合わせて，この Role のアクセス可否を決定する．
5. アクセス可能であれば X は Y に情報 I に関して返答し，アクセス不可であれば拒否と返答する．

具体的な例を図7に従って説明する．この図はリサーチコミュニティB の中でのエージェント間のメッセージのやり取りの様子を示している．

リサーチコミュニティBには属性ACM_Memberを持つエージェントX,Yと属性IEEE_Memberを持つエージェントZが加入しており，Publicポリシにより X,Y,Z はファイル検索というサービスが提供されているとする．また，Xは自分のPrivate Zoneに“属性ACM_Memberを持つエージェントのみ閲覧可能”というPrivateポリシが付加された論文ファイルを保持しているとする．このときのエージェントXの内部動作は以下のようになる．

1. 論文ファイル検索（論文ファイルに対するSearch,Read操作）に対応するRoleの属性がACM_Memberに設定される．
2. ファイル検索Roleのファイル操作がセキュリティ管理部にチェックされる．
3. セキュリティ管理部はファイル検索Roleの要求が論文ファイルのPrivateポリシに合致しているかどうかを検査する．
4. この場合はアクセスが許可されるのでファイル検索RoleはPrivate資源内の論文ファイルにアクセスすることができ，論文ファイルに対するファイル操作が完了する．(エージェントZの場合はここでアクセスに失敗する．)

この動作に基づき，YはXに対して論文ファイルを検索しダウンロードできる．一方，ZはXから論文ファイルを検索することはできるが，ダウンロードして閲覧することはできない．つまり，この例ではACMメンバの間では自由に論文を交換できるが，IEEEメンバにはそれが許されない．

5 おわりに

本稿では，個々の計算資源および情報資源を公共の利用に供するPublic Zoneと外部からのアクセスを禁止するPrivate Zoneとに分離し，個々のPrivate Zoneへのアクセスセキュリティを保証し，かつ，遊休資源を公共の利用に供する情報流通環境を構築することができ，ユビキタス・コンピューティングなど，広域ネットワーク中に散在する各種の計算資源や情報資源を有効利用して広域情報処理サービスを行う情報流通環境を構築する方法を提案した．現在，Kodamaシステムに本稿で説明したセキュリティ方式を実装中である．

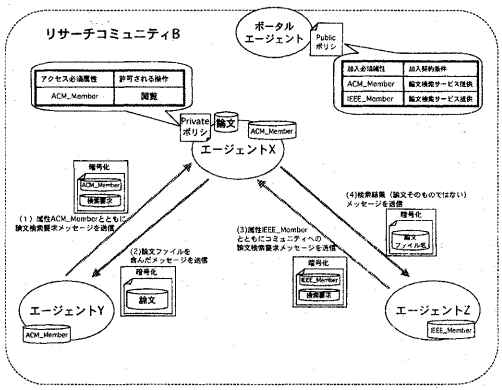

図 7: 資源に対するアクセス制御

今後の課題は，Public, Privateの各ポリシ内に記述するルールを具体化し，より現実的で複雑なアプリケーションを作成して，深い階層を成していてかつネットワーク的に離れているようなコミュニティ間でのメッセージ通信において，セキュリティが確保でき，かつその効率が実用に耐えうるかを検証することである．

なお，本研究は通信・放送機構（TAO）からの委託研究「相互接続時のセキュリティポリシーの管理技術に関する研究開発」の一環として行ったものである．

参考文献

[1] T. Iwao, M. Okada, K. Kawashima, S. Matsumura, H. Kanda, S. Sakamoto, T. Kainuma, M. Amamiya: Large Scale Peer-to-Peer Experiments with Virtual Private Community Framework, Proc. of the 6th International Workshop CIA 2002 on Cooperative Information Agents, pp. 66-82, Sept. 2002.

[2] Java Security Architecture: http://java.sun.com/j2se/1.4.2/docs/guide/security/spec/security-spec.doc.html

[3] E. I. Organick: The Multics System: An Examination of Its Structure, MIT Press (1972)

[4] G. Zhong, S. Amamiya, K. Takahashi, T. Mine and M. Amamiya: The Design and Implementation of KODAMA System, IEICE Transactions INF.& SYST., Vol.E85-D, No 4, pp. 637-646 (2002)

[5] 雨宮真人，雨宮聡史，岩尾忠重，岡田誠，“ネットワークノードマシンおよび情報ネットワークシステム”，特願 2003-284400, 平成 15 年 7 月