Agent Mediated Communicatorにおける ネットワークセキュリティ

北村泰彦，回り道康博，辰巳昭治
大阪市立大学工学部情報工学科
〒558-8585　大阪市住吉区杉本3-3-138
kitamura@kdel.info.eng.osaka-cu.ac.jp
http://www.kdel.info.eng.osaka-cu.ac.jp/~kitamura

Abstract

現在のインターネット上のコミュニケーションには「場」の概念が希薄である．そのゆえにSPAMメールを初めとするさまざまなセキュリティに関する問題が発生していると考えられる．本稿では，インターネット上のコミュニケーションに「場」の概念を導入したAMC(Agent Mediated Communicator)を提案する．AMCではエージェントを「場」へ送り込むことで，サービスを受けたり，その場を訪れている他のエージェントとコミュニケーションを行うことができる．本稿ではAMCにおけるネットワークセキュリティに関して議論を行う．

1　はじめに

我々の行うコミュニケーションでは,「場」の共有が前提となっていた．例えば，もっとも原始的なコミュニケーション手段である対面会話は，話し手と聞き手が同じ場所にいることによって成立する.「場」の共有はこれまで，自由なコミュニケーションに対する一つの制約と考えられてきた．そしてこの制約を緩和するために郵便や電話など，様々な手段や技術が開発されてきたといえる．郵便や電話を利用することにより，私たちは物理的に「場」を共有することができない遠隔地にいる人々とコミュニケーションを図ることができるようになった．

インターネットをはじめとする情報ネットワーク技術は,「場」の制約をさらに緩和することに成功している．電子メールにより，我々は地球の裏側にいる人と瞬時にしてメッセージの交換を行うことができる．またWWWによって世界中から膨大な量の情報を入手すること，逆に世界中へ向けて情報発信を容易に行うこともできるようになった．我々は現在，この電子コミュニケーションを駆使して，地球全体に垣根の無い，平坦なネットワーク社会を作り出そうとしている．

しかし一方で，このネットワーク社会には様々な問題が生じている．われわれは日々，SPAMやジャンクメールと呼ばれるメールに悩まされている．現在のメールシステムでは一度に何千人にも，あるいはある特定の個人に向けて何百通ものメールを送りつけることが可能である．またWWWを介して公開されることが不適切な情報が国境を越えて流れ込んでくる．一部の人々に向けての私的な情報発信を行ったはずの個人情報が，見ず知らずの人間によって意図しない目的に利用されていることもある．これらの問題はネチケットなどモラルの問題として片付けられている場合も多いが，現実にはそれほど簡単な問題ではない．

これらの原因の一つは，インターネット上にネットワーク社会が構築される際,「場」の役割が軽視されたためである．我々の行う原始的コミュニケーションは常に場をわきまえて行われる．簡単な挨拶ならば廊下でも，エレベータでも場所を問わず行う．しかしビジネスや研究の打ち合わせであればある程度隔離された会議室を利用し，話の内容がプライバシーを含む個人的な内容であれば，第三者に聞かれることが

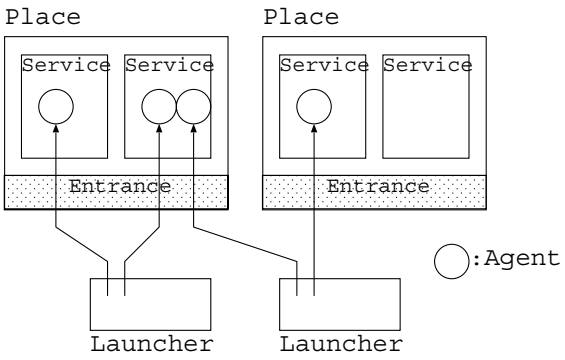

図 1: AMC の全体構成

ないよう当事者だけが完全に隔離された場所で行うのが普通である．すなわち「場」とは,「暗黙的に，どのような人がその場にいることが可能かを決定することのできる概念」として定義することができる．その「場」にふさわしくない人間は「場」に入ることを拒絶され，場合によっては強制的に排除されるのである．このように，私たちはふさわしい「場」に身を置くことによって，その「場」にいる人々と安心してコミュニケーションを行うことができるのである．

本稿では，ネットワーク上での電子的コミュニケーションに「場」の概念を復活させた「場指向コミュニケーション」を提案する．また，場指向コミュニケーションを実現するためのシステムとして，Agent Mediated Communicator(AMC) を提案する.「場」には利用者間のコミュニケーションを仲介するモバイルエージェントを登場させ，利用者間のコミュニケーションは同一の「場」に存在するサービスや他のエージェントとの相互作用として実現される．

本稿では以下，2章で AMC の概要を示し，3章で AMC におけるネットワークセキュリティに関する考察を行い，4章で類似システムと比較する．5章で今後の課題を含め，まとめとする．

2 Agent Mediated Communicator

2.1 全体構成

AMC システムの全体構成を図 1に示す．AMC システムはエージェント (agent)，ランチャ(launcher)，プレース (place) から構成される．エージェントはモバイルエージェントであり，利用者の代理人である．エージェントは利用者によってランチャから発射され，指定されたプレースへと移動する．またプレースはエージェントを受け入れ，電子メール，電子掲示板，チャットといった，コミュニケーションを行うための様々なサービス (service) を提供する場である．

プレースで提供される常駐サービスとしてエントランス (entrance) がある．エントランスは，プレースの管理者によって設定された制御情報に従ってエージェントの入場管理を行う．

利用者は，コミュニケーションを開始したい場合，ランチャによって自らのエージェントをプレースへ送り込む．エージェントは初めにまずエントランスを通過し，一旦プレースに入場できればその後はそこで提供されているサービスを受けることができる．一つのプレースには複数のエージェントが同時に入場することが可能であり，エージェントは同じプレースにいる他のエージェントの存在やプロファイルについて情報を得ることができる．

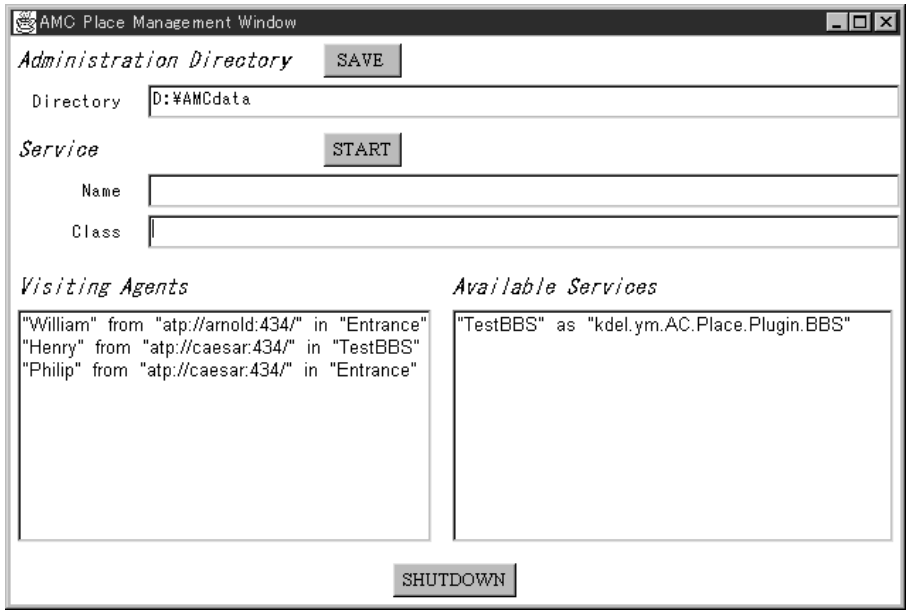

図 2: 稼働中のプレース

2.2 プロトタイプシステム

IBM Aglets[1] を利用することにより AMC プロトタイプを実現した．現在のところ，エージェントの入場管理に関しては実装を行っていない．

プレースは図2に示すようなウィンドウで管理される．

プレースの各項目について，意味や機能を以下に示す．

Administration Directory: プレースで提供している各サービスのログや設定などを保存するためのディレクトリを指定する．

Service: サービスを起動するのに必要なサービス名やクラスを指定する．サービス名はそのサービスの内容を示すもので，プレースを訪れたエージェントにはこのサービス名が引き渡される．例えば車に関する話題を扱う掲示板であれば「車に関する掲示板」といったような具合である．クラスには，そのサービスを実際に提供するクラスの名前を指定する．サービス名とクラスを入力して START ボタンを押すことで，そのサービスが起動する．

Visiting Agents: プレースを訪れているエージェントの名前，エージェントが生成された計算機のアドレス，エージェントが現在提供を受けているサービスの各情報が一覧表示される．

Available Services: プレースで既に提供中のサービスのサービス名とクラスが一覧表示される．

Shutdown: ボタンを押すことで，プレースプログラムが終了する．

図2では，arnold という名前の計算機からやってきた William という名前のエージェントがこのプレースを訪問中で，エントランスサービスを受けている．また ceasar から来た Henry と Philip は TestBBS とエントランスサービスをそれぞれ受けている．また現在プレースで稼働しているサービスは，TestBBS という名前の BBS クラスである．なおエントランスサービスは常に動作している．

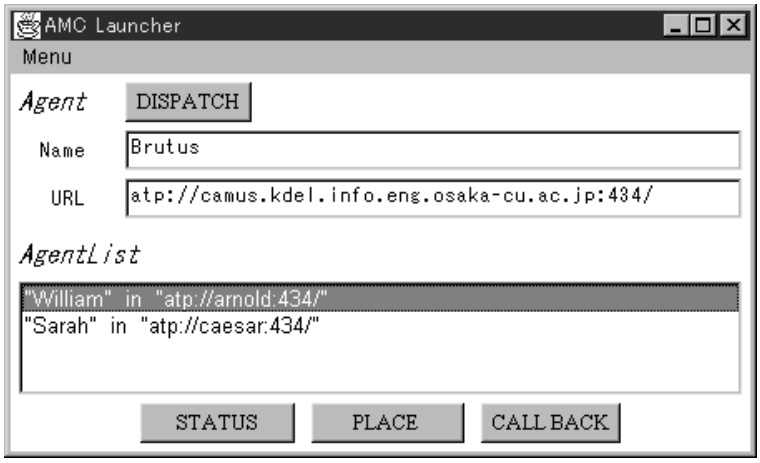

図 3: ランチャ

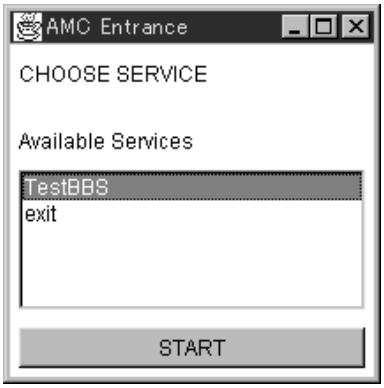

図 4: エントランス

ランチャは図3のようなウィンドウで管理される.
ランチャの各項目について，意味や機能を以下に示す.

Agent: エージェントを識別するための名前と，派遣先のURLを指定する．DISPATCHボタンを押すことで，エージェントが生成され，指定アドレスへ派遣される.

AgentList: ランチャから既に派遣したエージェントの一覧が表示され，下に並ぶボタンを押すことでエージェントに命令することができる．STATUSボタンを押すと，現在エージェントが実行中のプログラムが表示される．PLACEボタンを押すと，そのエージェントが現在訪れているプレースに存在するエージェントの一覧を入手できる．CALLBACKボタンを押すと，エージェントが訪問先のプレースで退室処理を行い，ランチャまで戻ってきて消滅する.

エージェントがプレースに派遣されると，特に指定することが無ければ，図4に示すように，プレースで提供されているサービスの一覧をユーザへ示すエントランスプログラムを携えたエージェント (Entrance-Agent) が送られてくる．ユーザはこのエントランスから各サービスへと移動することになる.

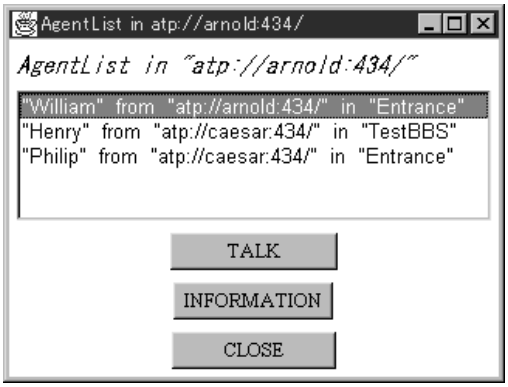

図 5: エージェントの一覧

また同じプレースにいるエージェントは図5により表示される．現在のところ他のエージェントに対しては以下の操作が可能になっている．

TALK: 対象エージェントのユーザとの会話 (Talk) を要請する．TALK ボタンを押すと，通信用ウィンドウが開く．この時，相手ユーザの側でも同じウィンドウが開いており，お互いにメッセージをやり取りすることができる．

INFORMATION: 対象エージェントのユーザ情報を要求する．INFORMATION ボタンを押すと，ランチャで設定したユーザ情報と，ランチャの存在するアドレスが表示される．

3 AMCによるセキュリティの確保

AMCによる場指向コミュニケーションは，これまでの電子コミュニケーション手段では重要視されていなかった「場」の概念を，モバイルエージェント技術を用いることにより復活させている.「場」は我々の日常の安全を考える上でも重要な概念である．通常，不特定多数の人と関わりあう可能性の高い道路や駅といった公共の「場」よりも，ある限られた人しか入ることのできない自宅のような私的な「場」の方が安全性が高い．場指向コミュニケーションでは，電子コミュニケーションにおいても「場」の概念を導入することによりネットワークセキュリティを確保しようとする試みである．

コミュニケーションにおけるセキュリティの確保はこれまでも重要な研究課題であった．現在のセキュリティの確保に対する最も基本的な対策はファイアウォールを設けることであろう [3]．しかしながらこの手法は組織全体のコミュニケーションを制御することであり，利用者が個別にアクセスを制御することは難しい．またWWWサーバのアクセス制限のようにアプリケーション毎に細かな制御をする方法も考えられるが，これは面倒であったり，初心者には難しいという問題を抱えている．また個人が提供可能な情報資源が全体としてどのようなアクセス制限が行われているかが分かりづらいという問題もある．

AMCはモバイルエージェントの概念を用いることによりセキュリティ確保の一つのモデルを提供している．すなわち，エージェントがプレースに入場できるかどうかでプレース内の情報に関するアクセス制御が行われる．さまざまなコミュニケーションや共同作業におけるアクセス制御を，このモデルによって統一的にモデル化することができる．

別のセキュリティ問題の例として，SPAM メールがある．現在の電子メールは特定のアドレスに大量のメールを送ることが可能であり，これが問題を引き起こす原因でもある．また送り手が匿名やなりすまし

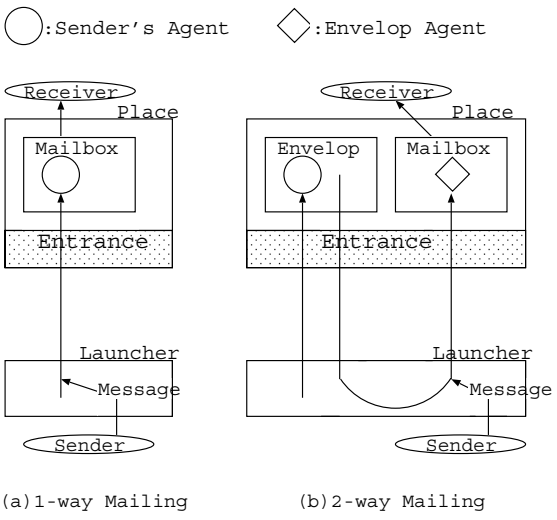

図 6: 二種類の電子メールシステム

のアドレスを用いている場合，これに対処することが難しい．基本的にメールの受信者は，送られてくるメールを制限することができないという問題点を抱えている．

AMCでは，モバイルエージェントを仲介役とすることで，図6で示すように二通りの電子メールシステムが考えられる．

図6(a) に示す一方向メーリング (1-way mailing) では，メッセージを持ったエージェントをランチャからプレースに送り込み，相手のメールボックス (mailbox) へ投函する．これは，エージェントがプレースに入場する前に認証を受けるという違いはあるものの，基本的には従来の電子メールシステムを踏襲している．この手法ではエージェントのもっているプロファイル情報をもとにメールのフィルタリングを行うことは可能である．しかしながら，なりすまし メールに対しては効果的でない．

図6(b) に示す二方向メーリング (2-way mailing) は，プレースに送りこまれたエージェントがエンベロープ (envelope) サービスを起動し，メッセージを送るためのエンベロープエージェントを受信者側から送信者側へ送ってもらう方法である．エンベロープエージェントはメールを記述するためのプログラムを備えており，送信者はエンベロープエージェントが運んできたプログラムを利用してメールを書く．終了すると，エンベロープエージェントはメールを携えて元いたプレースへ戻る．この方法はエンベロープエージェントが送信者のもとにメールを取りに行く手法であるので，DNSが正常であり，またマシンのユーザが一定であるという条件下においては，送信者がなりすまし メールを送れないという利点がある．

この手法を発展させることで，メールの受信制御も可能になる．例えばエンベロップエージェントのメール回収の数に制限を加えれば，一日に受信するメールの数を制限することができる．すなわち受け手がイニシアティブを取ることのできるメールシステムが実現できる．

4 IRCとの比較

Internet Relay Chat(IRC) という，テキストベースのチャットシステムがある．IRCでは，複数のサーバがIRCネットワークを構成している．利用者はクライアント・アプリケーションを使ってサーバへ接続することで，同じIRCネットワーク内の利用者とコミュニケーション（チャット）を行うことができる．コミュニケーションの方法は，１対１で行うものと，多人数の間で行うものの二種類に分かれる．多人数間

で行うコミュニケーションは，利用者が「チャンネル」へ入ることで行うことができる．利用者は，接続しているIRCネットワークに存在するチャンネルの一覧を取得でき，これを元に各チャンネルへ入室することができる．チャンネルは，利用者が設置することも可能である．なお，同じIRCネットワークに所属するサーバは，チャンネルや利用者の情報を共有している．

チャンネルには普通チャンネルオペレータ（チャンネルを設置した人や，オペレータからオペレータ権限を委譲された人）が一人以上存在する．チャンネルオペレータは管理のために，不適切な利用者をチャンネルから追い出すことができる．また，チャンネルに対して以下のような設定を施すことができる．

- チャンネルに入室するためのパスワードを設定する．
- チャンネルの存在を一般の利用者から隠蔽する．
- 特定の利用者の入室を禁止する．
- 招待した利用者のみ入室できるようにする．

IRCにおけるチャンネルは，AMCのプレースに相当する．セキュリティ面では，いずれのシステムも「チャンネルの管理者」「プレースの管理者」に大きく委ねられており，利用者の視点から見たセキュリティの差異はない.「場」としての機能であるが，チャンネルもプレースも一通りの機能を備えている．チャンネルはそれに加えて利用者の手によって動的に「場」を生成できることができ，この点においてはIRCの方がAMCより優れているといえる．しかしAMCのプレースは単にコミュニケーションを行うこと以外に，情報の蓄積・集積といったコミュニティ形成も視野に入れている．基本的にチャットによるコミュニケーションのみを行うためだけのチャンネルに対して，プレースはサービスを追加することで多様な拡張を行うことができる．この拡張性が，AMCとIRCの相違点である．

5　まとめ

モバイルエージェントに基づく場指向コミュニケーションシステムAMCを提案し，ネットワークセキュリティ確保に関して有効であることを述べた．今後の課題としてはAMCに認証機構を組み込み，その有効性を確認することが挙げられる．モバイルエージェントを利用することにより逆に，エージェントの誘拐，解析，改造新たなセキュリティの問題を引き起こすことが考えられるが，これに関しては今後の課題としたい．

また場指向コミュニケーションはセキュリティの問題だけでなく，コミュニティウェア[2]の構築や実社会システムへの適応性においても有効であると期待される[4]．そこで今後の課題としては，本システムの有効性を示すさまざまなサービスの開発が挙げられる．これにより多様なコミュニケーションが可能になると考えられるが，現実との整合性をできるだけ満たすような形でこれを実現したい．すなわち現在実際に利用されているメールやWWWなどを包含するような形でシステムを実現したいと考えている．

謝辞

本研究の一部は日本IBM東京基礎研究所の援助を受けている．

参考文献

[1] Danny B. Lange, Mitsuru Oshima. "Programming and Deploying Java^{TM} Mobile Agents with Aglets^{TM}", Addison-Wesley, 1998.

[2] Toru Ishida (Ed.): Community Computing: Collaboration over Global Information Networks, John Wiley and Sons, 1998.

[3] Rolf Oppliger: Internet Security: Firewalls and Beyond, Communications of the ACM, 40(5):92–102, 1997.

[4] Yasuhiko Kitamura, Yasuhiro Mawarimichi, and Shoji Tatsumi: Mobile-Agent Mediated Place Oriented Communication, M. Klusch, O. Shehory, G. Weiss (Eds.), Cooperative Information Agents III, Lecture Notes in Artificial Intelligence, 1652:221–231, Springer-Verlag, 1999.