5G-5 UniAddressを用いたFIPAエージェントの検索と認証

小笠原直人*1，佐藤究*1，布川博士*1，白鳥則郎*2
*1 岩手県立大学ソフトウェア情報学部
*2 東北大学電気通信研究所

1．はじめに

Foundation for Intelligent Physical Agents（FIPA）はエージェントを基盤とするアプリケーション，サービス，および装置の出現を促進させることを目的とし，様々なFIPA仕様を作成している．

しかし，現在のFIPAの仕様では，個人秘書，代理人エージェント等の特定のユーザと深く関わりを持つパーソナルエージェントを実現しようとした場合，パーソナルエージェント(PA)とPAを利用するユーザ（オーナ）との関係性を明らかにすることが難しいという問題がある．本稿ではこの問題を解決するために，PAのための新しいエージェントアドレスであるUniAddressと、これを用いたエージェント検索、認証について述べる。

2．FIPA上でのPA実現における問題

現在のFIPAのエージェントプラットフォーム(AP)上でPAを実現しようとした場合，PA，およびオーナがそれぞれエージェントワールド，ユーザワールドを移動することにより２者の関係が他のユーザおよびオーナから判らなくなるという関係性の問題がある．また，この関係性の問題により，PA間で非対称鍵によるオーナの認証や情報の暗号化を行いたい場合に，どの鍵を用いて処理を行うべきか判らないという認証の問題も生じる．

2．１PAとオーナの関係性の問題

FIPAのエージェントはGrobal Unique Identifier (GUID)により識別される．GUIDは，

<name>@<hostname>:<port>/<target>

の形式で記述され，Home Agent Platform(HAP)の通信アドレスとそのAP内での一意な名前を連結したものである．

PAは，その性質上，出張等でオーナと共に地理的移動をすることにより短期的に，また転勤等でオーナの所属が変更になることにより長期的に活動するHAPが変更になることで，そのGUIDが変更になる可能性がある．また，PAがモバイルエージェントとして実装されている場合，オーナから与えられたタスクを処理するためにAP間を自律的に移動することによりGUIDが変更になる場合が多い．PAが自律的に，もしくはオーナの操作により移動し，そのGUIDが変更になった場合，FIPAの規定するAgent Communication Language(ACL)メッセージをPA間でやり取りする上で以下の問題が生じる．

（１）移動したPAから発信されたACLメッセージではどのPAからのメッセージかは判るが，どのオーナからのメッセージかが判らない．

（２）オーナのPAにACLメッセージを送信しようとしても，そのPAのGUIDが変更になっていた場合どのGUIDで送信してよいか判らない．

2．２認証の問題

FIPAの仕様ではエージェントの安全管理を実現するためにエージェントプラットフォームセキュリティマネージャ（APSM）が規定され，これを利用することで，エージェント間通信に非対称鍵による署名や暗号化を行うことが出来るが，PAとオーナの関係性の問題があるために以下の問題が生じる．

移動したPAから署名入りのACLメッセージを受け取った場合，PAのオーナが判らないためにどの公開鍵で署名を検証するかが判らない．

これらの問題はFIPAのエージェントがAPの稼働するホスト名に依存したGUIDによってのみ識別されることに起因しており，オーナがPAを何らかのより判りやすい方法で指定し，通信可能な方法が必要である．

3．UniAddressによるPAの検索と認証

本稿ではこれらの問題を解決するために，PAのためのアドレスUniAddressを提案する．

UniAddressはPAを特定するための一意のIDである．UniAddressでは，PAの移動によるオーナとの関係性を解決するために，PAが活動しているAPのホスト名に依存しないアドレスとして，全エージェントワールド上で一意の文字列を用いる．

Search and authentication of FIPA agent with UniAddress
N. OGASAWARA*1 , K. SATO*1 , H. NUNOKAWA*1 , N. SHIRATORI*2
*1 Faculty of Software and Information Science, Iwate Prefectural University
*2 Research Institute of Electrical Communication, Tohoku University

UniAddressを導入したAPのモデルは通常のFIPAのAP上に，PAのアドレッシングを行うためのUniAddress名前空間（UniAddress Naming Space: UNS)と，UniAddressとGUID間の変換を行うサービスエージェントであるUniAddressトランスフォーマ（UT）が導入されたものとなる．（図１）

エージェントワールドには一つのUNSが存在する，この空間にPAがUniAddressと自分自身のGUIDを登録することにより，PA間でのUniAddressによるACLメッセージの送受信が可能になる．UNSは各AP上のDirectory Facilitator(DF)とUniAddressディレクトリサービスから構成される．

UTはAP上に最低１つ存在するエージェントで，PAから受け取ったreceiverフィールドのUniAddressをGUIDに変換してAgent Communication Channel(ACC)に転送する機能を持つ．また，UniAddressはパラメータとしてACLメッセージの認証，複合化を行うための公開鍵を追加することが出来る．UniAddressの情報として公開鍵も一緒にUniAddress名前空間に登録することにより，UniAddressに基づく公開鍵サーバの機能も実現される．UniAddressによるPAの環境では以下のようにPA間の通信およびPAの認証が行われる．

３．１UniAddress情報の登録

PAは自分自身のUniAddress情報（UniAddress, GUID，公開鍵）をHAP上のDFに登録する．短期的なPAの移動では活動するAPは変更になるが，HAPは変更にならないため，登録するDFに変更は起こらない．

DFは登録要求を受け現在自分で管理しているPAのUniAddressをUniAddressディレクトリサービスに対して登録する．

３．２UniAddressによるPAの検索

PAが他のPAにACLメッセージを送信する際にはsenderとreceiverにUniAddressを用いた次のようなACLをUTに対し送信する．

```
(request
    sender: pa@iiop://...
    receiver ut@iiop://...
    :content (action ut@iiop://...
            (request sender: (UniAddress: xxxx)
                    receiver: (UniAddress: yyyy)
                    :content (...)))
```

ACLを受け取ったUTはDFに対しUniAddressのPAの現在のGUIDを検索する．UTは過去の検索結果のキャッシュを保存しており，過去に検索を行った経験のあるUniAddressであった場合，その時UniAddressの情報を管理していたDFに対し検索要求を行い，経験のない場合はUTのAP上にあるDFに対し検索要求を行う．

UTから検索要求を受け取ったDFは自分がそのUniAddressの情報を管理している場合，検索結果としてPAのGUIDとDF自身のGUIDを返す．管理していない場合はUniAddressディレクトリサービスに対し，UniAddressの情報をどのDFが管理しているかを検索し，その検索結果であるDFのGUIDをUTに返す．

UTは返ってきた検索結果をもとにACLのUniAddressをGUIDに変換しACCに転送する．

３．３UniAddressによるPAの認証

PAが署名付きのACLメッセージを受け取った場合，UniAddressと対応する公開鍵で検証することにより，認証の問題が解決される．また，オーナの鍵が変更され検証できないといった場合もUNSから新たな公開鍵を獲得することが出来るため，鍵の変更が容易に行うことが出来る．

４．まとめ

現在，限られたエージェントスペース内でのUniAddressによるPAのシステムを実装しその評価を行っている．今後，UniAddress発行機構の設計と，UniAddressディレクトリサービスへの検索負荷の検証を行っていく予定である．本研究は，仙台応用情報学研究振興財団と共同で行っているものである．

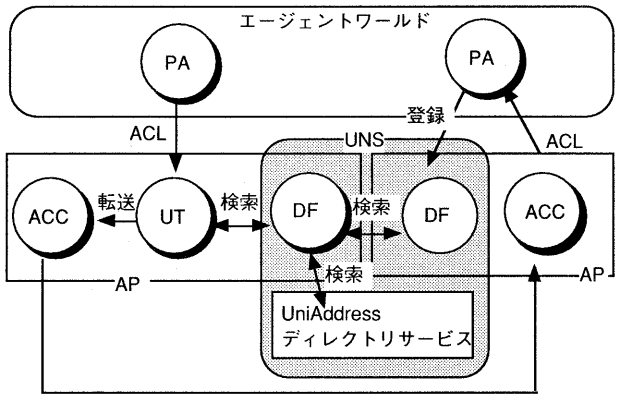

図１：UniAddressによるAPのモデル

参考文献

[1]Foundation for Intelligent Physical Agents: http://www.fipa.org

[2]小笠原，安部，佐藤，布川：MIA(Media Integration Agent)によるシームレスなコミュニケーション環境，日本VR学会CSVC研究会，CSVC99-7, pp.1-5