DEWS2007 D1-6

仮想マシンを用いた階層型認証機構に基づくMANETの実現モデルの提案と実装

小原　奈緒子†　　小口　正人†

† お茶の水女子大学　〒112–8610 東京都文京区大塚2–1–1
E-mail: †naoko@ogl.is.ocha.ac.jp, ††oguchi@computer.org

あらまし　P2P(Peer-to-Peer)通信を利用し固定基盤ネットワークに接続できない状況において集まったモバイルノードがその場のみで構築するネットワークのことをモバイルアドホックネットワーク(MANET)と言う．近年MANETへの需要が高まっているが，同時にセキュリティ上の脆弱性が問題となっている．固定基盤を持たないMANETにおいて，インフラネットワーク接続時と同等の完全な認証を実現することは原理的に不可能である．しかし全てのノードを等しく「未認証」とするより，完全ではないがある程度の信頼性を持つ仮認証などを行い信頼度に差をつけた方が望ましい場合が多い．そこで本研究では認証に段階を付け、それぞれのレベルに応じた安全なコンテンツのやり取りを行うための枠組みを検討する．さらに近年その高い性能やセキュリティ性で注目を浴びている仮想マシンを利用してより安全性の高いMANETの実現モデルを提案する．具体的には仮想マシンXen上の二つのOSに異なる機能を持たせ，ドメイン0（ホストOS）には認証などのセキュリティを任せて，ドメインU（ゲストOS）はサービスのやり取りなどのMANETの利用に専念させる．Xenのドメイン間通信は外部とは独立したネットワークを用いて行い、セキュリティ性が高い．さらにドメインUでMANETのサービスを受けるためにJXTAを動作させ他のノードとP2P通信を行った．

キーワード　仮想マシン, セキュリティ, アドホックネットワーク

Proposal and Implementation of MANET Realization Model using Hierarchical Authentication System

Naoko OHARA† and Masato OGUCHI†

† Ochanomizu University　Otsuka 2–1–1, Bunkyo-ku, Tokyo, 112–8610 Japan
E-mail: †naoko@ogl.is.ocha.ac.jp, ††oguchi@computer.org

Abstract　By using Peer-to-Peer(P2P) communication, mobile nodes organize themselves into a Mobile Ad-hoc Network(MANET) temporally, without fixed infrastructure. Recently, MANET rise in demmand, although security weaknesses become problem at the same time. It's impossible to achieve complete authetication in MANET equivalent to that in an infrastructure network. However, it's more desirable to do even inexhaustive authentication and hierarchize credibility based on it rather than to do nothing. Therefore, we combine different levels of authentication methods to develop hierarchical authentication scheme. Thus members can exchange contents safely depending on thier security level. In addition, since using virtual machine is attracting attention because of its high performance and secure characteristics, we propose and implement a model of mechanism that improves security. We install two OSs with Xen on a PC and each of them has different functions. Since Domain0(host OS) manages security including authentication, DomainU(guest OS) can concentrate on using MANET. We use different network in virtual machine from MANET for communicating between domains in Xen to improve security. In order to receive the benefit of service on domainU, we use JXTA to have P2P communication with domains on other nodes.

Key words　virtual machine, security, adhoc-network

1. はじめに

近年，コンピュータ間通信においてサーバを介さない P2P(Peer-to-Peer) 型通信が広く用いられるようになってきた．この P2P という通信形態を用いて，様々なアプリケーションが実装され，また JXTA [1] [2] のように汎用的な P2P プラットフォームの開発も行われている．無線 LAN などのモバイルネットワークの普及も急速に進んでおり，モバイル向け P2P サービスの実現に対する需要も高まっている．

このようなサービスでは，不正なユーザや機器からの脅威を防ぐために認証処理が必要不可欠である．しかし，インターネットに接続されていない環境において一時的に構築されるモバイルアドホックネットワークでは，PKI(Public Key Infrastructure) を始めとする固定的な認証機構が利用できず，一般的な認証システムを用いることは困難である。ゆえに固定基盤を持たない無線アドホックネットワークでは実用的な認証システムが実現されておらず，セキュリティ上の脆弱性が問題となっている．

そこで本研究では，モバイルアドホックネットワーク内におけるノード間の階層型認証システムを提案し，公開鍵暗号方式を用いて実装する．そして近年その高い性能とセキュリティで注目を集めている仮想マシン上で認証が利用できる MANET の実現モデルを提案し，構築する．

2. 研究背景

2.1 モバイルアドホックネットワーク

現在インターネットでは多くの場合，クライアント・サーバ型システムが用いられている．このクライアント・サーバ型システムではクライアントがサーバに接続して特定のリソースへのアクセス権を得る．しかしサービスを提供するための処理の大部分はサーバで行われるため，クライアントの数が増えるにつれサーバの負荷が増大してしまい，過負荷になるとシステム全体がダウンしてしまう可能性がある．

そのような場合には，P2P 型通信システムが有効になる．このシステムでは中央サーバを設けず，ネットワークを構成する各コンピュータが対等に処理を行う．サービスを提供する責務をネットワーク上の全てのノードが分担するので，単一障害によるサービス停止を回避できる．この P2P 接続を利用し，インターネットなどの固定基盤ネットワークに接続できない環境において集まったノードがその場のみで構築するネットワークを MANET(モバイルアドホックネットワーク) と呼ぶ．これはインフラネットワークが存在しない場面では有効であるが，高度なセキュリティ設定ができないなど機能が限られているという面もある．

2.2 公開鍵暗号方式

公開鍵暗号方式とは公開鍵と秘密鍵という対になる二つの鍵を使って暗号化・復号を行う方式である．片方の鍵を使って暗号したものはもう片方の対となる鍵を使わなければ復号できないという特徴を持つ．例として A が B を認証する場合を考える．

（1） B が自分の秘密鍵を使ってメッセージを暗号化し，それを A に送る

（2） B から送られてきたメッセージを A が B の公開鍵で復号する

この時 B の公開鍵で復号できれば B だけが持つ秘密鍵で暗号化されたということが言えるので認証が成立したことになる．この逆の手順も行うと，A と B が互いに認証し合うことができる．

2.3 JXTA

JXTA はサン・マイクロシステム社が開発した P2P 型のシステムを構築するための代表的なプロトコル及びツール群である．JXTA 論理レイヤの下位層である JXTA コアや JXTA サービスが P2P の基本的枠組みを提供しているため，その詳細な知識を持っていなくても上位層である JXTA アプリケーションで P2P アプリケーションを開発することができる．

JXTA ピアにはピア同士の出会いの場を提供するランダブーピアや，メッセージの中継や受け渡しなどを行うリレーピアがある．JXTA においてある共通なサービスについて合意しているピアの集合をピアグループと言う．また JXTA ピアは，メッセージを他のピアに送信するために JXTA パイプサービスを使用する．パイプはサービスのコミュニケーションのために使用される非同期かつ単方向のメッセージ転送機構である．受信点である入力パイプと送信点である出力パイプをエンドポイントとして，メッセージを送受信する際にピアのエンドポイントと動的にバインドする．

2.4 仮想マシン:Xen

仮想マシンは仮想的なコンピュータ環境を構築するメカニズムであり，一つの PC の中に複数の仮想的な PC を構築することができる．Xen は専用の仮想マシンモニタを動作させ，その上で動作する OS 環境を制御する．このようにほぼ実ハードウェア上で動作するため，従来の仮想マシンと比べ高い性能を持っている．近年，PC の処理速度の向上により，そのリソースを有効に活用できるアプリケーションとしてニーズが高まっている．Xen は安価にネットワークコンピューティング環境を構築でき，複数のサービスを安全に提供することができる．

Xen において個々のマシンは独立しているので，仮に特定のサービスの不具合によって攻撃されたとしても影響はそのサービスが稼動している仮想マシン内に限られるというように高いセキュリティ特性をもつ．図 1 のように Xen 内には仮想的なインタフェースが存在し，それを利用すると様々なネットワーク形態を構築でき，工夫すればセキュリティ性の高いネットワーク構成とすることが可能である．外部とドメイン U との通信はドメイン 0 の仮想的なインタフェースを介して行われるため，ドメイン 0 の安全性を確保すれば他のドメインの OS も安全であるということができる．

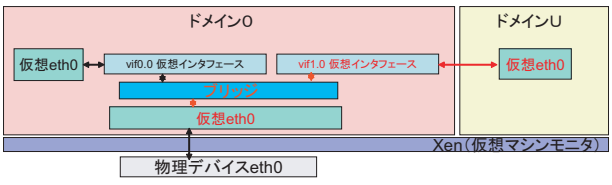

図 1 Xen のネットワーク構成

3. 研究目的

近年 MANET への需要が高まっているが，それと同時にセキュリティ上の脆弱性が問題となっている．固定基盤を持たない MANET において，インフラネットワーク接続時と同等の完全な認証を実現することは原理的に不可能である．しかし全てのノードを等しく「未認証」とするより，完全ではないがある程度の信頼性を持つ仮認証などを行い信頼度に差をつけた方が望ましい場合が多い．

我々はこれまでこれまで MANET において認証に段階を付けて信頼度に応じた安全なコンテンツのやり取りを行うために，階層型認証機構のモデルを提案し，検討してきた [4] [5] [6]．さらに，仮想マシンの高いセキュリティ性を利用して安全性をより向上させることが有効であると考え，階層型認証機構を含めた MANET の実現モデルを，仮想マシンを利用して提案した [7]．本稿では MANET の実現モデルを改良し，MANET におけるノード間でより安全かつ効率の良いコンテンツのやり取りを可能にしたい．

4. 仮想マシンを用いた MANET の実現モデル

4.1 MANET の実現モデルの概要

本研究では，仮想マシンを用いて安全にコンテンツのやり取りを行える MANET の実現モデルを構築することを目標としている．Xen のネットワークでは，2.4 節で述べたようにドメイン 0 のセキュリティを確実に保てばドメイン U も安全と言うことができる．この特徴を利用すると，ドメイン 0 にセキュリティの管理をしっかりさせれば，他の仮想マシンの OS はセキュリティの管理を気にせず他の処理に専念することができ，複数のサービスを安全に提供することができる．

そこで，図 2 のようにドメイン 0 に認証を含むセキュリティの管理を任せ，ドメイン U にはネットワークサービスを享受させるなど MANET の利用に専念させる．環境としては複数の PC に Xen をインストールし，その上で JXTA を動作させ P2P 通信を行う．

MANET の実現モデルの手順を図 3 を用いて説明する．MANET 内の他のメンバにコンテンツを要求されたら，まずドメイン 0 間で認証を行う．認証が成功したら JXTA パイプサービスを用いてコンテンツをドメイン U 間で送受信する．この時ドメイン 0 上のピアが外部への経路を確保しコンテンツを転送する．

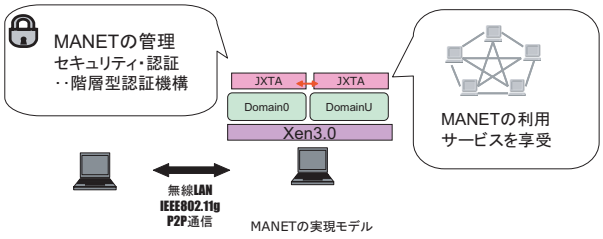

図 2　MANET の実現モデル

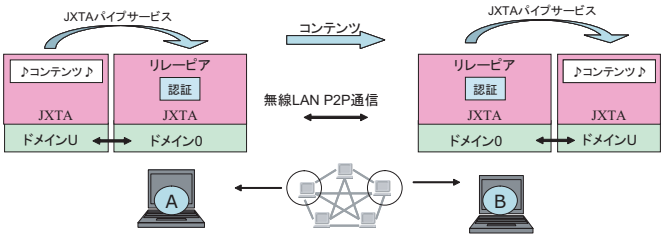

図 3　MANET の実現モデルの手順

4.2 実現モデルのネットワーク構成

PC に Xen を利用してドメイン 0 とドメイン U の二つの OS を動作させる．この時のネットワーク構成は図 4 のようになる．ノード間はドメイン 0 同士で無線通信を行う．そしてマシン内のドメイン 0 とドメイン U 間はそれとは独立した Xen の仮想ネットワークを用いて JXTA 上で行う．具体的にはドメイン 0 の仮想インタフェースである vif1.0 とドメイン U の論理インタフェースである eth0 との間で通信を行う．このようなネットワーク構成をとることにより，例え悪意のある者に侵入されてしまったとしても直接的な被害をドメイン 0 内に留めることができる．ドメイン間で外部と独立したネットワーク構成をとることにより，仮想マシン内の安全性を高めることができる．

さらに，ドメイン U が MANET のサービスを受けることができるようにするために，図 5 のように JXTA のリレーサービスを利用して外部からドメイン U への経路を確保しコンテンツを転送する．

次節より，ドメイン 0 が司る認証処理の手法について説明する．本論文で提案する認証機構自体は Xen に特化したものではなく，Xen 意外の計算機でも動作可能である．しかし，Xen を利用してよりセキュアな環境を生成することが有効であると考え，仮想マシンと認証機構を組み合わせた．

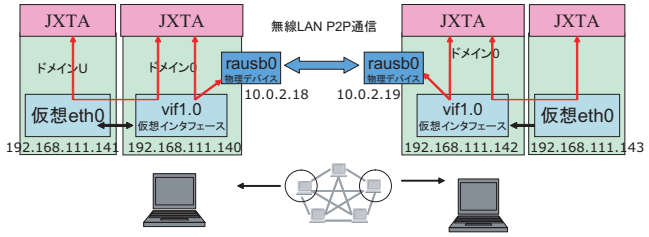

図 4　実現モデルのネットワーク構成 1

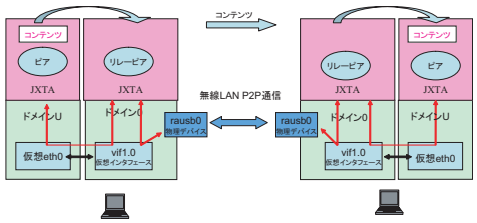

図 5　実現モデルのネットワーク構成 2

5. MANET における認証手法

5.1 前提条件

前節で述べたような複数の OS を持つ仮想マシンが一時的に

集まって MANET を形成し，コンテンツをやり取りする場面を考える．図 6 のように認証はドメイン 0 間でノード単位に行い，サービスはドメイン U 上で受ける．

MANET 内ではそれぞれのノードに属するピアが集まってピアグループを形成し，その中でコンテンツをやり取りしている．ピアは自分の ID を申告しあうことにより図 7 のように MANET 内でピアグループを形成し，通信を始める．ただし，会員サービスが存在し，それに属する場合には会員サービス固有の ID を申告して同じ会員サービスに属するピアグループに参加する場合もある．

この時次の様々な場面が存在する．MANET において個々のノードが認証に関する何らかの情報（他のメンバの公開鍵など）をあらかじめ保持している場合もある．自発的に集まったグループ内でその認証に関する情報を格納する認証データベースが存在し，アクセスポイントなどでアクセスできる場面も考えられる．

また，モバイルユーザが列車に乗り合わせた場合など，MANET 自体が移動している場面では、断続的にアクセスポイントでインフラネットワークに接続できる可能性もある．コンテンツを提供する会員サービスのプロバイダが存在し，会員に証明書を発行して認証局の役割を果たす場面もある．この場合会員同士で会員サービスが提供するコンテンツをやり取りすることができる．

以下の議論においては，正しい公開鍵で認証されたノードは MANET 内の他のメンバに対して不正を行わず，正しい情報のやり取りを行うものとする．また，データの改ざんを防ぐため，公開鍵暗号方式を用いて通信自体も暗号化する．

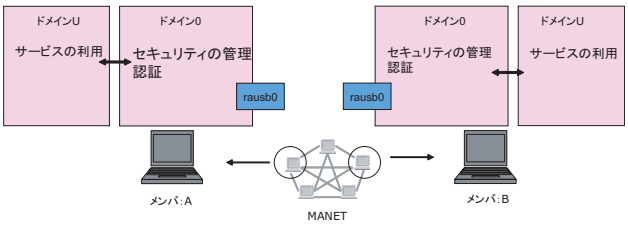

図 6　MANET における認証の前提条件

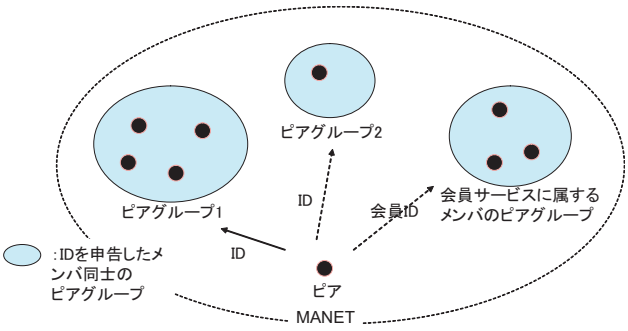

図 7　会員サービスへの参加

5.2　認証手法の提案

階層型認証機構を議論するにあたり，まず初めにインフラネットワーク接続時同等の完全な認証や MANET 内で有効である仮認証といったレベルの異なる認証手法をそれぞれ提案する．

5.2.1　認証手法 1

公開鍵を互いに知っていたメンバが MANET 内に居合わせる場面を考える．A が元から知っていた B の公開鍵を使って 2.2 節で述べた方式を用いて B の認証を行う．この様子を図 8 に示す．

この認証では，MANET を形成する前から知っていた公開鍵を使って認証を行ったので，基本的に不正行為はできずセキュリティレベルは高い．しかし，個々のノードが全員の公開鍵一覧のデータベースを持ち歩く必要があり，全ての通信相手に適用しようとすることは現実的ではない．認証手法 1 は小規模なグループ内でしか利用できないなど，適用できる場面が限られる．

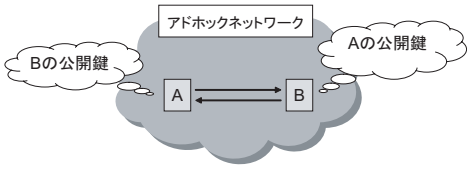

図 8　認証手法 1

5.2.2　認証手法 2

個々のノードが公開鍵一覧のデータベースを持ち歩かなければならないという認証手法 1 の短所を解決するべく，次に互いの公開鍵を知らないメンバが MANET 内に居合わせる場合を考える．A は B の公開鍵を知らなかったので，MANET 内で B の公開鍵を知る第三者ノード T を探す．

認証手法 2 では A は T の公開鍵を知らなかったものとする．A は T から B の公開鍵を受け取り，B の認証を行う．この様子を図 9 に示す．

（1）　A が T から B の公開鍵を受け取る

（2）　B は自分の秘密鍵でメッセージを暗号化して A に送る

（3）　A が B から送られてきたメッセージを B の公開鍵で復号する

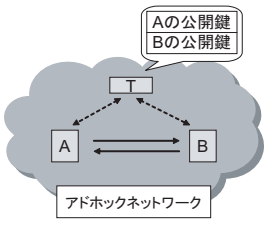

図 9　認証手法 2

認証手法 2 では，あらかじめ個々のノードが互いの公開鍵も T の公開鍵も知らなかったためそれが本物であるという確証が得られず，次のような場面が考えられる．

case1:　T が偽の場合

T が偽の場合，T は A に本物の公開鍵を渡さないため B の認証を行うことができない．

case2:　B が偽の場合

B が偽である場合，A は T から B の正しい公開鍵をもらって復号しようとした際に B が偽であることが分かる

case3:　B も T も偽である場合

このケースでは，偽の B と偽の T が共謀して不正を行うことが可能である．偽の B は自分の秘密鍵を使ってメッセージを暗号化し，A は T から送られてきた B の偽の公開鍵を使って復号すると，認証が成立してしまう．

この認証手法 2 では，T と B が共謀すれば不正を行うことができてしまう．従ってそれはセキュリティレベルの低い仮認証とみなし，価値の低いコンテンツ（例えば天気情報，道路や店舗の混雑状況など）のやりとりに限定することが適切といえる．このセキュリティレベルの低さを解決する方法としては，MANET がインフラネットワークに接続できた時にノード T や B の公開鍵が正しいかどうか判断するなどの対策が考えられる．

5.2.3　認証手法 3

認証手法 2 ではあらかじめ個々のノードが T の公開鍵を知らなかったため，セキュリティレベルの低い認証しか行えなかった．認証手法 3 では，MANET 内に B の公開鍵を知る T が存在し，A があらかじめ T の公開鍵を知っていた場面を考える．A が，あらかじめ知っていた T の公開鍵を用いて T を認証する所から始める．この様子を図 10 に示す．

（1）　A は T より T の秘密鍵で暗号化されたメッセージを受け取り，T の公開鍵で復号して T の認証を行う

（2）　A は T から B の公開鍵を受け取る

（3）　B は自分の秘密鍵でメッセージを暗号化して A に送る

（4）　A が B から送られてきたメッセージを B の公開鍵で復号する

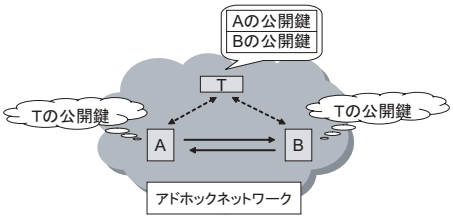

図 10　認証手法 3

この認証手法 3 では認証手法 1 と違い，メンバ全員の膨大なデータベースを持ち歩く必要はない．さらに，T が正しいかどうかを確認できてから B の認証を行うため，基本的にどのノードも不正を行うことはできず，セキュリティレベルが高い．

5.3　認証手法 4

信頼できる会員サービスのプロバイダ（T）が存在し，会員に証明書を発行している場合を考える．会員は T の公開鍵を知っており，T が会員に発行する証明書を用いてお互いを認証する．A はサービスプロバイダ T の公開鍵で B の証明書を検証し，B が正しいことを確認する．この様子を図 11 に示す．

（1）　B が A に自分の証明書を送る

（2）　A は T の公開鍵で B の証明書を検証

（3）　B は自分の秘密鍵でメッセージを暗号化して A に送る

（4）　A が B から送られてきたメッセージを証明書に記載された B の公開鍵で復号する

この時 T の公開鍵で証明書の署名を検証できれば，T だけが持つ秘密鍵で証明書が暗号化されたということが言えるので B の証明書が正しいことが分かる．そしてメッセージが正しく復号できたら，B が証明書の正統な所有者であると認定できる．

この認証手法 4 ではあらかじめ知っていた T の公開鍵を使って認証するためセキュリティレベルが高い．知っておくことが必要なのは T の公開鍵だけであり，MANET 内ではお互いの証明書を交換するだけで簡単に認証できる．ただし，信頼できる会員サービスのプロバイダの証明書が必要になる．認証できた場合には会員サービスが提供するコンテンツを会員同士でやり取りすることができる．

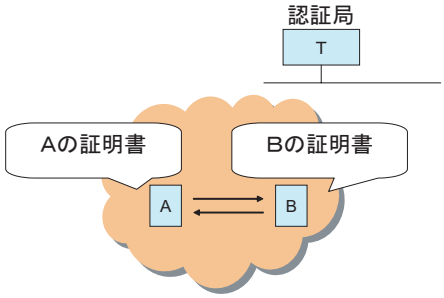

図 11　認証手法 4

6.　認証手法の階層型認証機構への適用

6.1　階層型認証機構の基本的枠組み

本研究では前節で述べた認証手法を利用し，次のような階層型認証機構を提案する．この階層型認証機構を含んだセキュリティの管理は Xen 上のドメイン 0 で行われるので，例え悪意のある者が侵入してきたとしてもドメイン U への直接的な被害を防ぐことができる．

個々のノードは MANET を形成する前から他のメンバの公開鍵を知っている場合があり，それはドメイン 0 上の公開鍵リストに格納される．ノードはインフラネットワークに接続した状態で認証データベースなどにアクセスし，適当なメンバとその公開鍵をこの公開鍵リストに入れることができる場合もある．メンバが信頼できる会員サービスに属しており，それが発行する証明書を保持している場合もあるものとする．

階層型認証機構の概要を図 12 に示す．個々のノードは他のメンバをセキュリティレベルで格付けし，ピアグループ内でそのメンバと公開鍵に関する情報を保有する．これをセキュリティテーブルと呼ぶ．これはメンバそれぞれによって異なる相対的なものであり，ピアグループにジョインする度に生成される．このセキュリティテーブルは高，中，低の三段階のセキュリティレベルを持ち，それは格納されているノードの信頼性はどの程度であるかを示す．あるノードが他のメンバを認証する際に，信用できる公開鍵によって認証が成立した場合には相手

とその公開鍵を高レベルに，そうでない場合は中レベルに相手を追加する．この時，信用できる公開鍵とは公開鍵リスト，もしくは高レベル層にいるメンバの公開鍵のことを指す．信用できるとは言えない公開鍵とはその他全ての公開鍵を指し，公開鍵リストにはなく，高レベル層にも存在しないメンバの公開鍵のことである．また，公開鍵が分からないため，自己申告した ID を用いてオープンな認証のみを行った場合にはそのメンバの ID を低レベルに追加する．

例えばピアグループ内にジョインしたばかりの A が B を認証する場合を考える．図 12 が A のドメイン 0 であると考えると，B が ID を申告してピアグループに参加してきた際にはまず低レベル層に B の ID を追加する [①]．A は B の公開鍵を知らなかったが，たまたま居合わせた T を用いて認証手法 2 を行うことができたら中レベル層に B とその公開鍵を追加し，B のセキュリティレベルを上げる [②]．さらにインフラネットワークに接続して T もしくは B の公開鍵が正しいと確認できたら，認証手法 3 や認証手法 1 を行ったことになり高レベル層まで B とその公開鍵をレベルアップさせる [③]．ただし，B がまだ低レベル層にいた段階でセキュリティレベルの高い認証手法 1 や認証手法 3 を行うことができた場合には飛び越えて一気に最高レベルまで上げる．B が信頼できる会員サービスに属しておりその証明書を持っている場合も認証手法 4 を行い一気にレベルをアップさせる [④]．

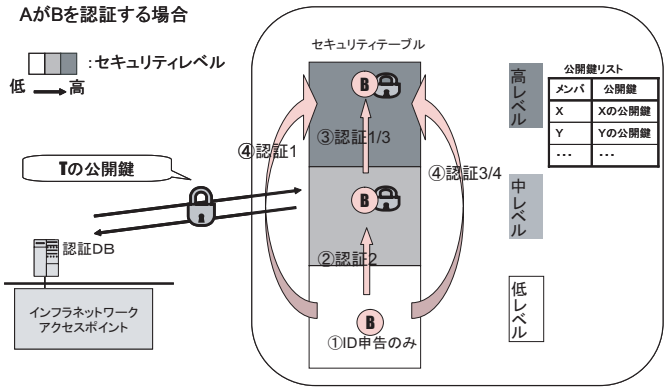

図 12　階層型認証機構の提案モデル

個々のメンバがそれぞれ前節で述べたセキュリティテーブルを保有し，それを参照し合うことによってより多くのメンバとコンテンツのやり取りが可能になる．信頼できる公開鍵によって認証した相手を高レベルに追加した際には，その相手が持つセキュリティテーブルを参照して自分のものを更新する．この際には次のルールに従う．

- 相手のテーブルのみに存在するノードとその公開鍵を追加
- 自分と相手両方のテーブルに存在するノードには，より高いレベルを適用

このように信用できる相手のテーブルを参照することにより更新されたデータも，自分が認証して得たデータと同様に扱う．従って，相手のセキュリティテーブルを参照することによって高レベル層に追加されたメンバ情報も認証を行う際に信用できるものとして利用される．中レベル層に追加された情報は高レベル層のものよりセキュリティレベルが低く，低レベル層に追加された情報はさらに低い．このような過程を経ると，会員サービスのメンバは直接コンタクトを取った数より多くのメンバのセキュリティレベルを知ることになり，信頼の輪が広がっていく．

6.2　動作アルゴリズム

前節で述べた内容に基づき，本研究で提案した階層型認証システムは次のようなアルゴリズムに沿って実行される．まず，ピアグループ内にいる他のメンバを認証する際のアルゴリズムを図 13 に示す．

[認証とセキュリティレベル更新に関するアルゴリズム]

```
if(高レベル層にBが存在){
  高レベル層にある公開鍵を用いてBを確認
}else{
  if (Aの公開鍵リストにBが存在){
    認証手法1で高レベルへBを認定
  }else if (Bが信頼できる証明書を持つ){
    認証手法4で高レベルへBを認定
  }else {
     信用できるBの公開鍵を知っているTを探す
    if (Tが見つかった){
      if (TがAの公開鍵リストまたは高レベル層に存在){
        認証手法3でBとTを高レベルに認定
      }else{
        認証手法2でBを中レベル層に認定
        if(有線でBの公開鍵の情報を取得){
          Bの公開鍵を確認して認証手法3を行いBを高レベル層に更新
        }
      }
    }else if (Tが見つからなかった){
      if (Aの中レベルにBがいる){
        中レベル層にある公開鍵を用いてBを確認
      }else{
        Aのテーブルの低レベルにBを認定
      }
    }
  }
}
```

図 13　認証とセキュリティレベル更新に関するアルゴリズム

次に他のメンバのセキュリティテーブルを参照する際のアルゴリズムを図 14 に示す．A が B を認証し，自分のセキュリティテーブルに加えた後，そのレベルによって B のテーブルを参照するかどうか判断するところから始まる．

[セキュリティテーブル参照と更新のアルゴリズム]

```
if(Bを高レベルに認定){
  Bのテーブルを参照{
        if(Bのテーブルにだけ存在するノードがある){
          そのメンバと公開鍵をBのテーブルと等しいレベルでAのテーブルに追加
        }else if(AとB両方のテーブルに存在するノードがある){
          より高いレベルを適用してそのノードをAのテーブル内で更新
        }
  }
}else if (Bを中レベルもしくは低レベルに認定){
  Bのテーブルを参照しない
}
```

図 14　セキュリティテーブル参照と更新のアルゴリズム

個々のノードは公開鍵で暗号化したコンテンツをピアグルー

プ内でやり取りする．その際には，自分のセキュリティレベルに応じたサービスを受けることができる．例えば図 15 のように ITS による車車間通信を例にあげると，B が低レベル層にいる時には他の車の位置情報しか受け取ることはできない．しかし，中レベルに上がると周辺の道路情報や天気情報などのコンテンツの一部分を受け取ることができる．さらに，最高レベルでは ETC を利用した決済サービスなど全てのコンテンツを利用できるようになる．このように認証レベルが上がるごとに受けることのできるサービスは拡大され，セキュリティレベルに応じたサービスを受けることができる．

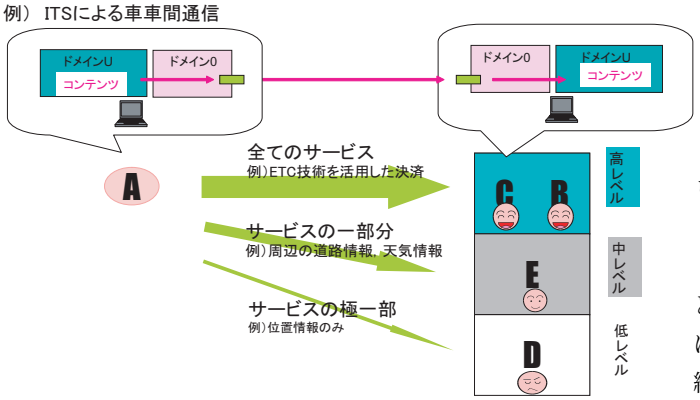

図 15　サービス実現例

6.3　階層型認証機構の適用例

この階層型テーブルを利用した認証システムがどのように動作するか具体例を図 16 に示す．

①まず初めに B が A に認証要求を出したとする．B がセキュリティテーブルにも公開鍵リストにも存在せず証明書も持っていなかったため，A は B の信用できる公開鍵を知っているノードを探す．D が B の公開鍵を知っていると報告したので，D にそれを教えてもらうことによって認証手法 2 を B に実行する．B が確認できたら中レベルにアップさせる．

②次に C が A に認証要求を出したとする．A は自分が持っている公開鍵のリストの中に C の公開鍵を見つけたのでそれを利用して認証手法 1 を C に適用する．C が正しいと判明したら高レベルに追加する．

③この時，高レベルにいる C は信頼できると言えるので C のセキュリティテーブルを参照して A のテーブルを更新する．A のテーブルには存在しなかった E と D が新たに追加される．C と A のテーブルを比較すると，B に対して C は A よりも高度な認証を行うことができたことが言えるため，A のテーブルにある B の公開鍵が C のテーブルにある B の公開鍵と等しいことを確認して，A は B のレベルを上げる．

このセキュリティテーブルの情報を利用することにより，それぞれのメンバは自分のセキュリティレベルに応じたサービスを受けることができる．この時点では低レベルにいる D は少しのサービスしか受けられない．中レベルにいる E はコンテンツの一部を受け取ることができる．さらに高レベルの C と B は全てのコンテンツを A から利用できる．

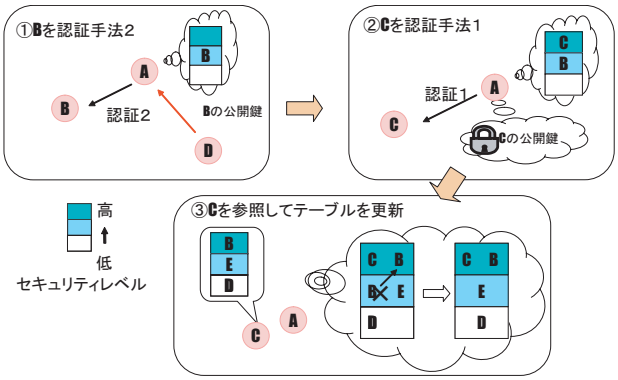

図 16　提案モデルの動作の具体例

7.　階層型認証システムの実装

MANET の実現モデルを実装するために，ピアのディスカバリサービスのプログラムと認証手法 1 のプログラムを実装した．

7.1　実験環境

図 17 のように 2 台のノート PC に Xen3.0 を利用して OS として Linux version 2.6.18 を二つインストールした．その上に JXTAversion2.3.3 を動作させ、これらを IEEE802.11g 無線 LAN で接続し，P2P 通信を行った．ネットワーク構成は 4.2 節で述べたような構成になっており，ドメインUは外部ネットワークとは独立して JXTA を用い，ドメイン 0 を介して通信を行っている．

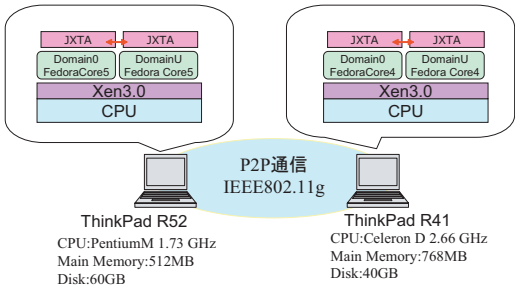

図 17　実験環境

7.2　ピアのディスカバリプログラムの概要と実行結果

2 台のノートＰＣの 4 つのドメイン上の JXTA でピアを発見するプログラムを実装した．まず，JXTA 上でそれぞれ 4 つのピアを作成し，それぞれが他のピアを発見するための DiscoveryRequest 要求を送る．他のピアが発見され，そのピアから DiscoveryResponse メッセージを受け取ったらピア名を出力する．実行結果は図 18 のようになっており，ドメインU上のピアが同じノートＰＣのドメイン０上のピアと他のノートＰＣ上の二つのピアを発見できたことが分かる．

7.3　認証手法のプログラムの概要

本研究で提案した階層型認証機構の一部である認証手法 1 のプログラムをドメイン０上の JXTA 間で動作させた．通信は JXTA パイプサービスを利用して行っている．

1. 送信側で署名を生成

（1）　公開鍵と秘密鍵のインスタンスを作成

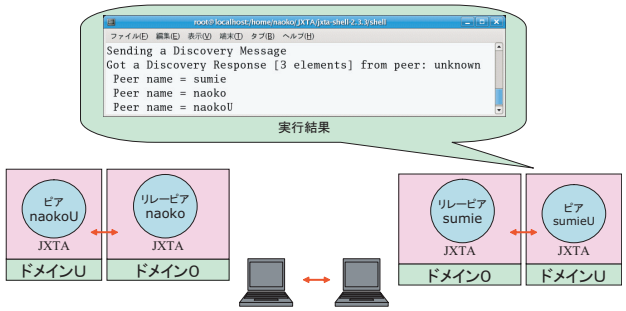

図 18　ピアのディスカバリ

（2）　generateKeyPair() 関数を用いて公開鍵と秘密鍵のペアを作成

（3）　メッセージを秘密鍵で暗号化して署名を生成

2. メッセージと署名の送受信

まず受信側プログラムは入力パイプを生成しその上でメッセージと署名を入力待ちする．一方送信側では出力パイプを生成し，そこから JXTA パイプサービスを利用してメッセージと署名を送信する．出力パイプから送信されたメッセージと署名は入力パイプで受信される．

3. 受信側でメッセージの検証

（1）　検証するための関数 Verify() を公開鍵を指定して初期化

（2）　署名を復号し元のメッセージと比較，検証

（3）　検証の結果を出力

以上の手順を図 19 に示す．

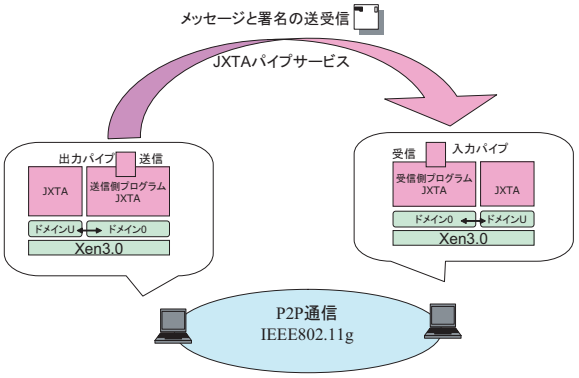

図 19　メッセージと署名の送受信

7.4　認証手法のプログラムの実行結果

前節で述べた認証手法 1 の受信側のプログラムと送信側のプログラムをそれぞれ別のノート PC 上のドメイン 0 で動作させた．受信側の実行結果を図 20 に，送信側の実行結果を図 21 に示す．初めに受信側でパイプサービスのアドバタイズメントを読み込んで入力パイプを生成しメッセージが届くのを待つ [①]．次に，送信側のプログラムが公開鍵と秘密鍵のペアを生成し，署名を作成する [②]．そしてパイプアドバタイズメントを読み込んで出力パイプを作成し，メッセージを送信する [③]．受信側がメッセージを受信し終わったら [④], 送信側が次に署名を送信する [⑤]．署名を受信し終わったら [⑥] メッセージと署名を検証しその正否を出力する [⑦]．以上により，Xen 上のドメイン 0 間の P2P 環境で認証手法 1 を構築した．

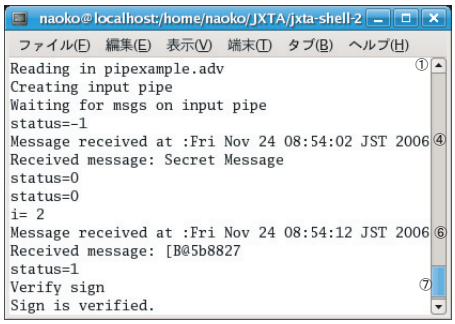

図 20　受信側プログラム実行結果

図 21　送信側プログラム実行結果

8.　まとめと今後の課題

本研究では MANET 内で有効であると考えられる実現モデルを構築するため，仮想マシンを用いて実現モデルの環境を構築し，階層型認証機構の一部をその上で実装した．今後の課題としては，実現モデルのネットワーク構成や階層型認証機構を検討し，実装したい．そして仮想マシンの特徴を生かしたより安全で実用的な MANET の実現モデルを提案して実装したい．

文　　献

[1] http://www.jxta.org/docs/JxtaProgGuide_v2.3.pdf
[2] Brendon J.Wilson　JXTA のすべて, 日経 BP 社
[3] 山本雅也，Xen3.0 による仮想化サーバの構築，秀和システム
[4] 小原奈緒子，小口正人：”モバイルアドホックネットワークにおける階層型認証機構の一検討 ”, 情報処理学会 第 67 回 全国大会，2T-8,2005 年 3 月
[5] 小原奈緒子，小口正人：”モバイルアドホックネットワークにおける認証機構の考察 ”, 第四回情報科学技術フォーラム（FIT2005）,L-051,pp.125-126,2005 年 9 月
[6] 小原奈緒子，小口正人：”MANET における公開鍵暗号方式を用いた階層型認証システムの提案と実装 , DEWS 2006, 2B-i8,2006 年 3 月 ”
[7] 小原奈緒子，小口正人：”仮想マシンを用いた MANET における階層型認証機構の提案と実装, CPSY2006-43, 2006 年 12 月 ”