秘匿性の高い安全なメッセージ伝達システムの実装と応用
Implementation of a Secure Instant Messaging Service and its Application

田中 裕之 †　　**筒井 章博** ‡
Hiroyuki Tanaka　　Akihiro Tsutsui
日本電信電話株式会社　NTT サイバーソリューション研究所
NTT Cyber Solutions Laboratories, NTT Corporation

概要

インターネット上で利用されるネットワークアプリケーションにおいて，利用者の情報を通信当事者以外に対して秘匿することは，個人情報保護の観点から非常に重要である．本研究では，ネットワークアプリケーションの通信内容だけではなく，各利用者の個人情報や利用者間の関連を，ネットワーク/アプリケーション運用者からも秘匿可能なメッセージ伝達システム PIMS (Private Instant Messaging Service) を提案している．本稿では，PIMS と，PIMS の応用事例である，インスタントメッーセジングサービスへの適用例と，DNS(Domain Name System) 名前解決サービスの拡張事例について，その概要と実装を述べる．また，これらの実装の評価結果から，PIMS がメッセージ伝達システムとして実用的な拡張性と応答性を持つことを示す．

1　はじめに

現在一般的に提供されているインターネット接続サービスなど，端末の IP アドレスが動的に変化する環境では，通信対象となるユーザやアプリケーションサービスを特定の IP アドレスに関連づけることが困難である．そこで，ICQ[1] のようなインスタントメッセージング (IM) サービスでは，各ユーザとユーザ端末の IP アドレスとの対応を，独自の位置管理サーバで登録・管理することによって，ユーザ間のメッセージ伝達を実現している．また，DNS サーバの登録情報を動的に更新する，動的 DNS[2] などの機構を利用することによって，端末名に対応する現在の IP アドレスを得る名前解決処理が実現可能である．

これら既存のサービスでは，利用者の情報がサーバで集中管理されているため，各利用者の現在位置や，メッセージ交換による利用者間の交流状況などの，各利用者のプライバシーに関連する個人情報を，サーバ上で逐一把握することが可能である．これは，サーバのセキュリティが一旦が損なわれてしまうと，本来秘匿されるべき各利用者の個人情報が，全て第三者に漏洩する可能性があることを意味している．また，サービス運営者が，各利用者に通知することなく，各利用者の個人情報を収集しこれを再利用する仕組みを，サーバ上に秘かに組みこんだとしても，利用者はこれを察知し阻止することができない．以上のような事例から，既存の IM サービスや動的 DNS では，各利用者が，自らの判断において個人情報の開示範囲を完全に制御可能な，秘匿性の高いサービスは提供困難である．

本研究では，端末の IP アドレスが動的に変化する環境において，ネットワークアプリケーション同士が，種々の通信メッセージを安全に交換することを可能にするフレームワークとして，メッセージ伝達システム PIMS を提案した [3]．本稿では，PIMS の概要と実装について述べる．また，PIMS のアプリケーション例として，IM サービスへの適用事例と，PIMS-DNS の事例について示す．PIMS-DNS とは，インターネットにおける一般的な名前解決方式である DNS のインターフェイスを介して，PIMS を利用した名前解決を既存アプリケーションに提供するサービスとして，本研究で提案している DNS 実装の拡張である [4]．本稿では，これら PIMS アプリケーションの概要と実装，および評価実験の結果について述べる．

†tanaka.hiroyuki@lab.ntt.co.jp
‡tsutsui.akihiro@lab.ntt.co.jp

2　安全なメッセージ伝達システム PIMS

2.1　秘匿性の高いメッセージ伝達の条件

PIMS は，互いに IP アドレスが不確定な送信者と受信者のアプリケーション間で，安全にメッセージを伝達する機能を提供することを目標としている．本研究では，個人情報の秘匿性に優れた，理想のメッセージ伝達システムの必要条件を以下のように定義した．

1. 通信内容の秘匿
   通信当事者以外による通信メッセージの盗聴・解読を阻止することは，秘匿性確保のための第一条件である．また第三者が，本来の送信者になりすましてメッセージを作成したり，元のメッセージを改ざんすることが不可能でなければならない．

2. 利用者の所在の秘匿
   ある利用者が現在使用している端末の IP アドレスを，利用者本人の意思とは無関係に第三者に同定されると，利用者本人を目標として，サービス拒否攻撃などの悪意のある通信を実行可能である．従って，利用者本人が意図しない形で，第三者に利用者の端末アドレスが公開されてはならない．

3. 利用者情報の秘匿
   既存の IM サービスでは，利用者毎に識別子 (ID) を割り当て，ID 単位で利用者を識別・管理する．しかしながら，ID と利用者の個人情報の相関も第三者に対して秘匿されるべき個人情報である．ID に

関連した個人情報としては，本名，通称名，連絡先などの本人情報や，通信相手 ID 一覧などの友人情報，通信相手毎のアクセス制限などのサービス利用ポリシといった情報が挙げられる．

4. 送受信者の関連の秘匿
メッセージ伝達サービスにおける通信メッセージの送受信者の関係は，交友関係など利用者間の相関を示す個人情報でもある．従って，通信メッセージの送信者と受信者の相関もまた，第三者に対して秘匿されなければならない．

既存のメッセージ交換サービスにおいても，利用者の個々の端末でメッセージ内容を暗号化・解読することによって，通信内容を秘匿することが可能である [5]．しかしながら，利用者の所在，送受信者の関連，および利用者情報の秘匿については，これらの情報を集中管理する位置情報管理サーバなどのサーバ群，および，その運用者の信頼性に依存せざるを得ないのが現状である．すなわち，サービス提供者によるサーバ運用規定やプライバシーポリシ規定など，サービス提供者と利用者間の利用契約に基づいた信頼関係に依らずして，利用者が秘匿性を獲得することは不可能である．

PIMS の目標は，運用手法と利用契約に頼ることなく，前述した 4 つの必要条件を満たす機能を提供可能なメッセージ伝達の仕組みを実現することにある．

2.2 PIMS の概要

図 1 に PIMS の概要を示す．動的 DNS や既存の IM サービスが採用する集中管理型のアーキテクチャでは，集中管理サーバの運用上，第三者に対して情報を完全に秘匿することが困難である．そこで PIMS では，端末上のメッセージ中継配送アプリケーション (PIMS 転送エンジン) 同士がアプリケーションレベルで相互に接続・通信することによって構成される仮想ネットワークである，「PIMS ネットワーク」による分散管理型のアーキテクチャを採用する．図 1 の例では，端末 N1〜N5 上で動作する PIMS 転送エンジンが相互に接続して 1 つの PIMS ネットワークを構成している．

PIMS におけるユーザやアプリケーションサービスの識別子 (PIMS 識別子) には，OpenPGP[6] などで利用される公開鍵暗号方式の公開鍵を使用する．通信内容を秘匿するため，PIMS で伝達されるメッセージは，発信者の端末で受信者の PIMS 識別子により発信者の署名と共に暗号化される (図 1-(1))．

暗号化されたメッセージは，まず，隣接する PIMS 転送エンジンに受渡される．このとき，送受信者の関連を秘匿するためメッセージには宛先が添付されない．暗号化されたメッセージは，PIMS ネットワーク上を同報中継することによって宛先まで配送される (図 1-(2))．メッセージの配送は，PIMS 転送エンジンで中継される毎にアプリケーションレベルで一旦終端され，発信元および宛先 IP アドレスが変化する．従って，メッセージを含む IP パケットを観測するだけでは，メッセージそのものの発信者・受信者の所在する端末の IP アドレスを確定することができない．

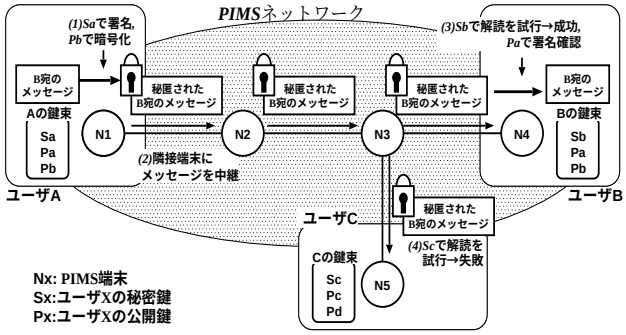

図 1: PIMS の概要

同報配送されてきたメッセージが自分宛であるかどうかは，メッセージが解読可能か否かによって判断する．暗号化されたメッセージを解読できるのは，公開鍵に対応する秘密鍵を所有する宛先人だけであることから，同報されたメッセージの平文は宛先人のみが入手可能である (図 1-(3),(4))．なお，受信したメッセージの署名を確認することによって，メッセージの発信者を確認することが可能である．

PIMS のメッセージ伝達メカニズムでは，利用者情報を秘匿するため，本人および通信相手の PIMS 識別子などの利用者の個人情報を，利用者端末内でのみ管理し，第三者の端末には通知しない．通信相手毎のアクセス制限についても，利用者の端末内で直接判断し，第三者の端末は介在しない．

各利用者の PIMS 識別子の管理に関しては，公開鍵認証局を用いた集中管理・認証方式を採用することが可能である．しかしながら，利用者情報の秘匿のためには，「信頼の輪」(Web of Trust)[7] による分散管理・認証方式を採用することが望ましい．

2.3 システム構成例

図 2 に，PIMS のシステム構成例を示す．PIMS の実装は，秘匿メッセージの中継処理を行なう PIMS 転送エンジンと，メッセージの秘匿処理を行ない，アプリケーションと PIMS 転送エンジン間の処理を仲介する PIMS ライブラリの二つの機能ブロックから成る．

本例では，PIMS ライブラリでのメッセージの暗号・署名認証処理に OpenPGP を使用し，その公開鍵を各ユーザやアプリケーションサービスの PIMS 識別子として用いている．OpenPGP は，主に電子メールの秘匿のために利用されている公開鍵暗号システムで，暗号化処理だけではなく，暗号鍵ペアの管理や公開鍵の安全な配布など，公開鍵暗号の運用に必須となる機能を持つことから，PIMS の公開鍵暗号系としても適している．

公開鍵暗号系の暗号処理は，他の暗号方式より高い計算処理能力を必要とするため [6][8]，メッセージ解読試行処理の簡略化は，PIMS システム全体の性能向上における重要な課題の 1 つである．OpenPGP の秘匿メッセージには，平文の補助情報中に公開鍵 ID として公開鍵の 64bit ハッシュ値を含める事が可能である．そこで，メッセージ中に公開鍵 ID の情報が存在する場合は，PIMS 転送エンジン内で自エンジンに接続したアプリケーションの公開鍵 ID とメッセージの公開鍵 ID を比較し，一致

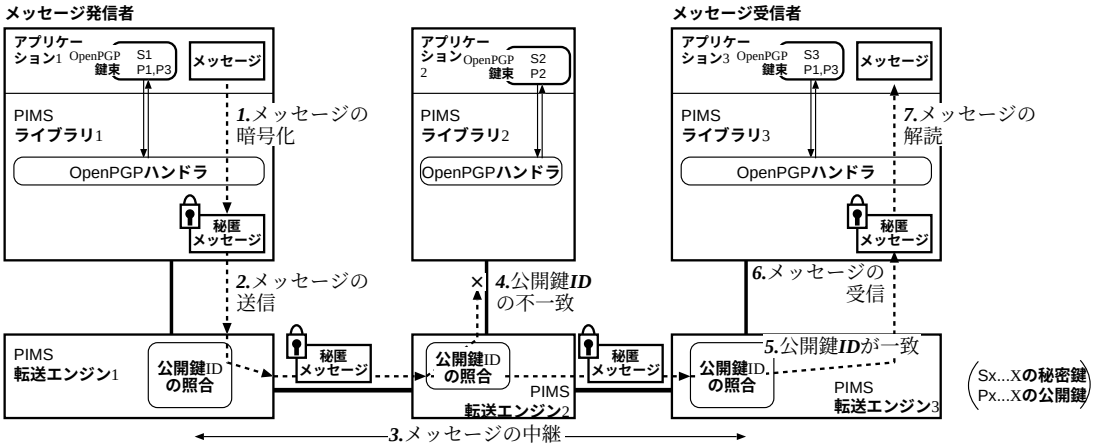

図 2: PIMS システムの構成とその動作概要

した場合のみメッセージの解読を試みることによって，メッセージ解読処理の軽減を図る．

ただし，メッセージ中の公開鍵 ID の情報を利用する場合は，その情報が，第三者にとってはメッセージの宛先，すなわち PIMS 利用者に関する情報源となり得る点に留意する必要がある．第三者がメッセージ中の公開鍵 ID を参照することによって，少なくとも，複数のメッセージの中から同一宛先の可能性が高いメッセージを抽出することが可能である．従って，公開鍵 ID 情報を利用した負荷軽減の利用方法については，上記のような問題点と，その運用規模，求められる秘匿性の程度などを考慮して決定しなければならない．例えば，メッセージに添付されるハッシュ値の有効長を短くすることによって，負荷軽減効果を低くする代わりに宛先の匿名度が高くなるよう調整することが可能である．

新たな端末の接続や既接続端末の切断によってその構成が刻々と変化する PIMS ネットワークでは，ネットワーク内に形成されたループ内をメッセージが無限に同報中継され続ける可能性がある．本例では，この現象を回避するため，各メッセージに 8bit の生存タイマ (TTL: Time To Live) 値を添付する．すなわち，メッセージ生成時に一定の TTL 値を与え，転送エンジンにてメッセージが中継される毎にこれを 1 づつ減ずる．TTL 値が 0 になったメッセージを中継せず破棄することによって，メッセージが無限に転送され続ける可能性を排除する．

2.4 メッセージ伝達の動作

本節では，アプリケーション 1 から 3 にメッセージを伝達する図 2 の例に沿って，PIMS の動作手順について述べる (文中，括弧内の数字は図 2 における註釈の番号に対応する)．

発信者がアプリケーション 1 から発したメッセージは，PIMS ライブラリ 1 内で受信者の公開鍵 P_3 で暗号化された，初期 TTL 値を添付された後 (1)，PIMS 転送エンジンに渡される (2)．PIMS 転送エンジンはこの秘匿メッセージの TTL 値を 1 減じて隣接する PIMS 転送エンジン 2 に中継する．また，PIMS 転送エンジン 2 は，同様に PIMS 転送エンジン 3 にこの秘匿メッセージを中継する (3)．なお，TTL 値が 0 になった時点で，メッセージは破棄される．

PIMS 転送エンジンでは，秘匿メッセージの公開鍵 ID と自エンジンに接続するアプリケーションの公開鍵 ID と比較して，一致した場合にのみアプリケーションに秘匿メッセージを受け渡す (4)(5)．

秘匿メッセージを受信した PIMS ライブラリ 3 は，自らの秘密鍵 S_3 で秘匿メッセージの解読を試みる．解読が成功した場合は，署名を確認したうえでアプリケーション 3 にメッセージを渡す (7)．メッセージが PIMS ライブラリ 3 からアプリケーション 3 に渡された時点でメッセージ伝達処理は完了する．

2.5 実装

前節のシステム構成例を元に，Microsoft Windows 2000/XP 上に PIMS を実装した．

Windows 版 PIMS では，PIMS 転送エンジンを端末毎に実行されるサービス，PIMS ライブラリをダイナミックリンクライブラリ (DLL) としてそれぞれ実装した．本試作では，PIMS ライブラリから，GnuPG[7] を外部プログラムとして実行することによって，OpenPGP ハンドラによる公開鍵暗号の処理を実現した．アプリケーションから PIMS 識別子を指定する際には，GnuPG と同様に，指紋 (fingerprint)，鍵 ID，および E-Mail アドレスのいずれかが利用可能である．

PIMS 転送エンジン間の接続には，各隣接端末毎に TCP，UDP ユニキャスト，および UDP マルチキャストの 3 種類の方式を選択可能である．同一サブネット内の端末間の接続など，IP マルチキャストに対応した環境では，UDP マルチキャスト方式で相互に接続することによって，複数の PIMS 転送エンジンに対して一回の送信処理でメッセージを送信することが可能である．

本実装では，PIMS 転送エンジンの起動時に初期隣接端末の IP アドレスを明示的に設定することによって，PIMS ネットワークを形成する．ただし，UDP マルチキャスト接続については，同一のマルチキャストグループ上に存在する別端末の PIMS 転送エンジンを自動検索・隣接することが可能である．

3 PIMS を利用したアプリケーション

本節では，PIMS のメッセージ伝達機能を利用した IM アプリケーションの実装と，PIMS による DNS 名前解

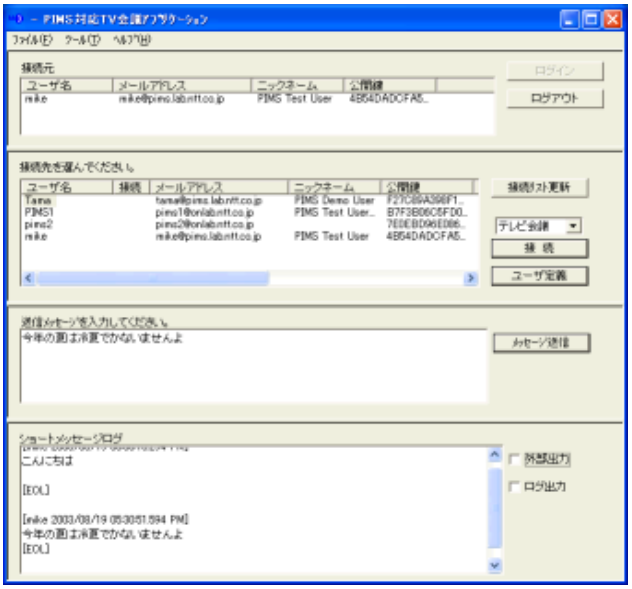

図 3: PIMS-IM アプリケーション (動作画面の例)

決の拡張について述べる．

3.1 PIMS-IM アプリケーション

Windows 版 PIMS の実装を使用して秘匿性の高い IM アプリケーションを実装した (図 3)．PIMS-IM アプリケーションの主な機能を以下に示す．

- ショートメッセージ通信
  テキストベースのショートメッセージ送信機能を提供する．テキストメッセージは，PIMS メッセージとして宛先まで安全に配送される．

- 接続状況の確認
  PIMS メッセージを利用して，通信相手に対して，現在の接続状況 (プレゼンス) を問い合わせて回答を得る手順を実装することにより，通信相手が現在ネットワークに接続しているかどうかを確認する機能を実現した．

- ビデオチャット
  Windows 標準のビデオチャットツールである Netmeeting では，通信相手の端末 IP アドレスを指定して Peer-to-Peer のチャットセッションを開くことが可能である．そこで本アプリケーションでは，PIMS メッセージを利用して通話者間で IP アドレスを相互に通知する手順を定め，これを Netmeeting 起動のトリガとすることにより，ビデオチャット機能を実現した．ただし，この機能の利用時に秘匿性が確保されるのは，Netmeeting 起動前の IP アドレス通知に限られる．Netmeeting 自身の通信内容をも秘匿したい場合は，Netmeeting の秘話機能を別途併用しなければならない．Netmeeting への秘話機能の指定は，PIMS-IM アプリケーション上からも可能である．

3.2 PIMS-DNS

3.2.1 PIMS による名前解決

PIMS-IM アプリケーションにおけるビデオチャットの実現例 (3.1 節) のように，PIMS によるメッセージ伝達を利用して，通信を開始しようとする相手に対して直接現在の IP アドレスを問い合わせることによって，秘匿性の高い名前解決が可能である．PIMS-DNS は，この PIMS による名前解決の仕組みを，DNS 参照インターフェイス (リゾルバ) を介して既存のネットワークアプリケーションから利用可能とする機構を実現する PIMS アプリケーションである．PIMS-DNS により，既存のネットワークアプリケーションの実装を改変することなく，名前解決処理の秘匿性を高めることが可能となる．

図 4 に PIMS-DNS の概要を示す．通常，アプリケーションから発行された DNS 参照の要求は，DNS サーバに引き渡される．PIMS-DNS では，この一連の処理の間に PIMS-DNS 選択プロキシを拡張する．アプリケーションから PIMS による名前解決を要求する場合は，PIMS-DNS 選択プロキシが定める切替トリガ名 (例: .pims) を DNS 正引き要求のトップドメイン名として指定する．PIMS-DNS 選択プロキシは，このトリガによって，PIMS による名前解決と通常の DNS 名前解決のどちらに処理を受け渡すかを選択する．

PIMS-DNS では，IP アドレスを解決するために，既存の DNS が利用するドメイン名に加え，ユーザやアプリケーションを直接指定する識別子を用いることができる．個人を特定する E-Mail アドレス等を DNS の正引き要求中にドメイン名の一部として埋め込むと，PIMS-DNS 選択プロキシがこれを PIMS のメッセージ伝達に用いる PIMS 識別子，すなわち個人に対応する公開鍵に変換し，PIMS 名前解決モジュールを経て名前解決が実行される．

これによって，PIMS-DNS では，当事者間で自由に定めた＜個人名＞.pims や＜アプリケーション名＞.pims などの名前から通信先の IP アドレスを取得可能となる．また，被解決先の当事者が，PIMS メッセージの署名によって要求の出自を確認したうえで，名前解決の問い合わせ毎にどのように回答するかを自ら判断できることから，動的 DNS[2] などの既存の名前解決方式より柔軟な運用が可能である．

3.2.2 PIMS-DNS の実装

前節で提案した PIMS-DNS を Microsoft Windows 2000/XP 上に実装した．図 5 に実装の概要を示す．

PIMS-DNS 選択プロキシの実装として，OS のリゾルバライブラリを PIMS-DNS 対応に拡張する方法と，DNS サーバとして PIMS-DNS の機能を実現する方法が考えられる．本実装では，PIMS-DNS 選択プロキシと PIMS 名前解決モジュールの機能を，PIMS-DNS の機能が拡張された DNS サーバプログラムとして実装した．本実装を利用する際には，Windows 標準の DNS サーバ設定を，この DNS サーバプログラムを実行している自端末に変更し，アプリケーションからの DNS 参照要求が，全て PIMS-DNS 選択プロキシを経由するように設定する．

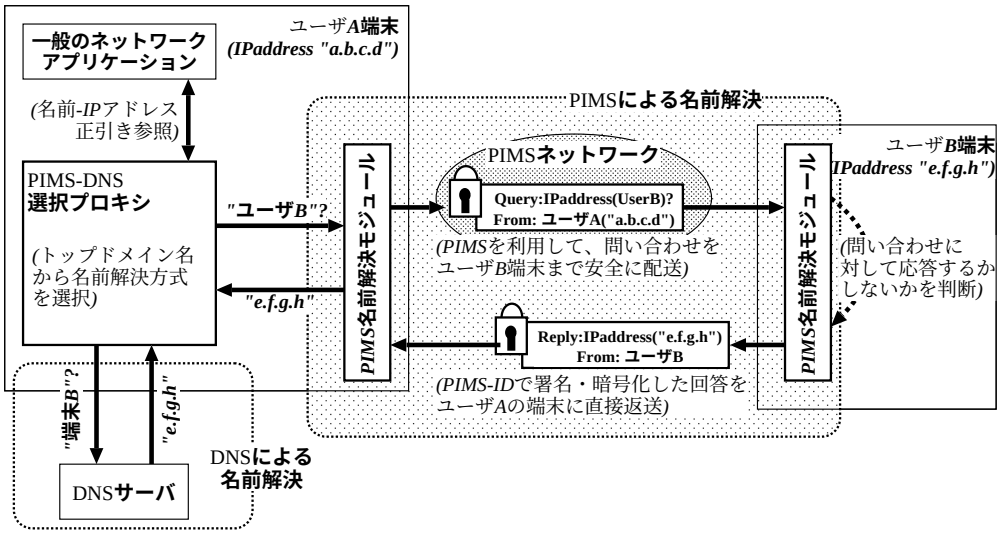

図 4: PIMS-DNS の概要

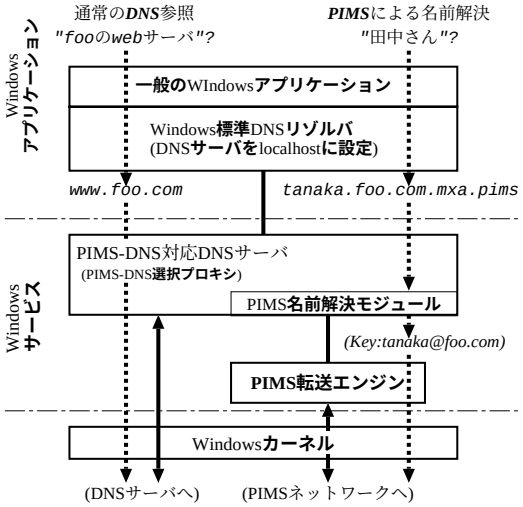

図 5: Windows 版 PIMS-DNS の実装構成

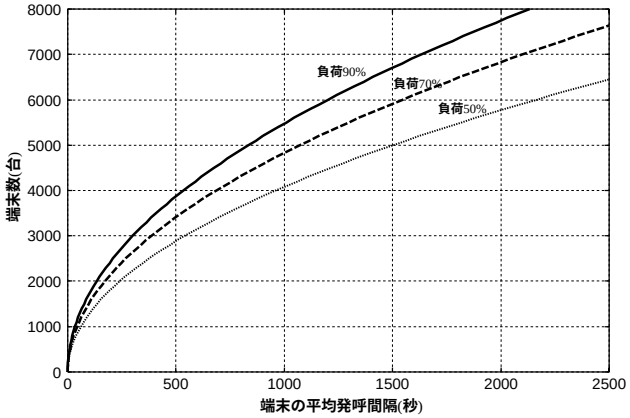

図 6: 端末数と平均発呼間隔の関係 (CPU 負荷別)
(PentiumIII 1.4GHz/512MB RAM, Windows2000 server での実測値に基づく)

PIMS 転送エンジンには，2.5 節で述べた実装を利用する．ネットワークアプリケーションから PIMS 識別子を指定する方法は，PIMS の実装が利用している GnuPG と同様，指紋 (fingerprint)，鍵 ID，および E-Mail アドレスの 3 種類から選択可能である．

4 性能評価

4.1 PIMS の拡張性

PIMS では，PIMS ネットワーク内でメッセージを同報中継することによって宛先まで配送する．従って，PIMS の運用規模，すなわち単一の PIMS ネットワークにおける最大収容ユーザ数，最大メッセージ配送数は，PIMS ネットワークを構成する PIMS 転送エンジンの転送能力に依存すると考えられる．そこで，Windows 上に試作した実装を用いて，PIMS 転送エンジンのメッセージ中継負荷を実測した．測定では，コミュニケーションツールにおける通信相手の探索に PIMS を利用することを想定して，PIMS-DNS の名前解決要求メッセージ (メッセージ長:606 バイト) を中継メッセージとして利用した．

測定の結果， メッセージ中継時の処理負荷は単位時間当りのメッセージ転送数と，自らに隣接した端末数 (PIMS 転送エンジン数) に比例することが判明した．この実測結果を元に，1 つの中継ノードに対して各端末がスター状に接続された，最も PIMS 転送エンジンに負荷のかかる PIMS ネットワークの構成において，中継ノードの CPU 負荷がそれぞれ 90%,70%,50% の状態で中継処理可能な，接続端末数とメッセージ転送頻度との関係を求めた結果を，図 6 に示す．

図6 より，上記のような極端な構成の PIMS ネットワークにおいても，例えば一端末当りの PIMS メッセージ発信頻度が約 10〜15 分間隔以上であれば総端末数 4000〜5000 台程度の規模で PIMS の運営が可能であることがわかる．この結果から，コミュニケーションツールにおける通信相手の探索に PIMS を使用する場合，端末負荷に関しては，本実装を用いても，最大端末数 4000〜5000 台程度のコミュニティであれば実運用可能であることを示している．

PIMS の運用規模は，PIMS 転送エンジンの処理能力

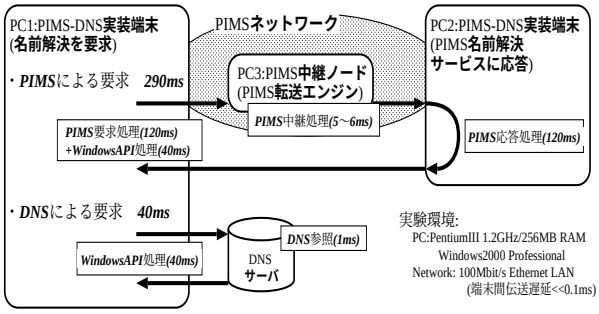

図 7: PIMS-DNS の評価実験 (応答性)

だけではなく，PIMS 転送エンジン間を接続するネットワークの転送能力や，PIMS ネットワークの構造にも依存する．例えば，メッセージ中継負荷測定と同様の条件において，図 6 より中継ノードとしては十分処理可能である，平均発呼間隔 1000 秒 (16 分 40 秒)，総端末数 5000 台という利用状況を想定すると，各端末が受信する IP パケットの転送速度は 約 25Kbit/s 程度となる．従って，総端末数 4000〜5000 台程度のコミュニティで，コミュニケーションツールにおける通信相手の探索に PIMS を適用する場合，各端末にかかる通信負荷もまた，実運用可能な範囲内であると言える．

上記実験のような極端な PIMS ネットワークの構成では，全端末にパケットを複製中継する端末が属しているネットワークに大きな負荷がかかる．しかしながら，実際の PIMS ネットワークの運用では，複数の端末に分散して端末が相互接続されていくことによって，一つの端末に負荷が集中する状況には陥いらないと予想される．また，複数 PIMS 転送エンジン間の接続に UDP マルチキャストを併用することによって，メッセージの同報負荷を軽減することが望ましい．

4.2 PIMS-DNS の応答性

PIMS-DNS では，既存のネットワークアプリケーションが，DNS 参照インタフェースを介して，通常の DNS と同じ条件で PIMS による名前解決を利用する．従って，PIMS-DNS によって拡張された名前解決サービスには，ネットワークアプリケーションからみて，既存の DNS 参照インタフェースと遜色ない応答速度が求められる．そこで，前述した PIMS-DNS の実装を使用して，アプリケーションからみた PIMS-DNS の応答速度を検証した．検証結果を図 7 に示す．

実験では，3 台の PC と DNS サーバを LAN で接続し，1 台の PC 上でアプリケーションが DNS 名前参照を発行してから回答が戻るまでの応答時間を，PIMS-DNS と DNS について計測した．なお，この PIMS ネットワークでは，PC1 からのメッセージは必ず PC3 を経由して PC2 へと配送される．

比較実験の結果，DNS 名前解決の応答時間が 40ms 程度であるのに対し，PIMS-DNS には 290ms の応答時間が必要であることが判明した．しかしながら PIMS-DNS の処理時間の大半 (約 240ms) は GnuPG の暗号処理時間であり，これは PIMS ネットワークの構成に関係なく処理時間がほぼ一定となる．一方で，PIMS ネットワークの構成に依存して累積される中継遅延は，1 中継あたり 5〜6ms 程度に抑えられている．

一般に，DNS 名前解決の応答時間は，DNS サーバの負荷や通信の遅延時間の影響をうけて大きく変動するため，10 秒以上のタイムアウト時間が想定されている．例えば Windows 2000/XP のアプリケーションライブラリにおける，DNS サーバ参照処理のタイムアウト時間は約 17 秒に設定されている．従って，中継回数が 10 回以上，PIMS 中継ノード間のネットワーク遅延が 200ms といった極端な PIMS ネットワークであっても，PIMS-DNS は，アプリケーションからみて実用範囲の応答速度を確保していると言える．

5 関連技術

5.1 公開鍵暗号による通信者情報の秘匿

公開鍵暗号を応用することによって，メッセージの内容だけではなくその送受信者情報の秘匿をも実現した既存の技術として，匿名通信ネットワーク MixNet[9] が挙げられる．MixNet は，PIMS と同様に，公開鍵暗号を用いてメッセージの内容を秘匿する．また，送受信者情報の秘匿は，宛先情報が多重に暗号化されたメッセージを，固有の公開鍵暗号鍵を持つ中継装置 (Mix) を介して，部分的に解読しつつ中継することによって実現される．

MixNet では，Mix を直列に多段接続した中継ネットワークを構築することによって，PIMS よりも強固に通信者の情報を秘匿することが可能である．また，特定の宛先に対して自らの匿名性を確保したままメッセージの交換が可能であるという，PIMS にはない特長も持つ．

しかしながら，メッセージが Mix 経由で中継される毎に公開鍵暗号の演算処理が必要なため，MixNet 上で高速にメッセージを伝達することは非常に困難である．従って MixNet は，IM サービスや名前解決サービスのように，リアルタイム性の高いメッセージ伝達が必要とされるサービスには適さない．

5.2 P2P ネットワークを利用した探索技術

PIMS のメッセージ伝達ネットワークである PIMS ネットワークは，各端末上の PIMS 転送エンジンが相互に接続・通信することによってメッセージの宛先を探索する，P2P (Peer-to-Peer) ネットワークであると考えられる．近年，広帯域インターネットアクセスの普及に伴って，Gnutella[10] や Freenet[11][12] などの，P2P 情報 (ファイル) 共有アプリケーションが注目されている．これらのアプリケーションでは，アプリケーションレベルで仮想的な P2P ネットワークを構築し，共有情報を効率的に探索・入手する機能を実現している．従って，既存の P2P ネットワークにおける探索技術を PIMS ネットワーク上での宛先探索に応用できれば，同報中継を使用する PIMS の宛先探索処理の負荷を軽減できる可能性がある．

P2P 情報共有アプリケーションでは，共有対象がファイルなどの複製可能な情報であることを利用して，探索・共有処理の最適化が試行されている．例えば，ある 1 つの情報を複数の端末でキャッシュとして保存することによって，検索・共有効率が向上する．しかしながら，PIMS では特定個人やネットワークアプリケーションのプレゼンスといった複製不可能な情報が探索対象となるため，既存技術を直接適用することは難しい．

また，分散型インデックス検索アルゴリズム [13] など

の，P2P 情報共有ネットワークにおける探索処理最適化の技術には，安全性の確保，すなわち，利用者の所在や送受信者の関連性を秘匿するという観点が不足しているため，PIMS に適用するには更なる工夫が必要である。

既存 P2P ネットワークにおける探索技術の PIMS ネットワークへの応用は，今後の検討課題である．

6 まとめ

本稿では，アプリケーションレベルの Peer-to-Peer 接続による同報通信を基本としたサーバレスのアーキテクチャによって，通信メッセージの内容だけではなく，利用者の所在や個人情報，送受信者間の関連をも秘匿するメッセージ伝達システム”PIMS” を提案し，その概要と実装について示した．PIMS を応用することにより，秘匿性の高いネットワークアプリケーションを構築することが可能となる．本稿では，PIMS を応用した IM アプリケーションと，既存アプリケーションの DNS 参照インターフェイスから PIMS による名前解決を利用可能にする，PIMS-DNS について述べた．

PIMS-DNS の名前解決要求メッセージの中継処理性能の評価結果から，PIMS が名前解決サービスのフレームワークとして実用可能であることを示した．また，PIMS-DNS の応答性の評価結果から，アプリケーションから見て，PIMS-DNS が，DNS と遜色ない性能を有することを示した．

これらの評価結果から，PIMS を利用したアプリケーションを運用する際には，端末の処理性能よりも端末間を接続するネットワークの処理性能がより問題となることが判明した．従って，例えば，メッセージ当りの情報量が PIMS-DNS と同程度であるが，メッセージ発生頻度の高いテキストチャットのような IM アプリケーションに PIMS を適用するためには，ネットワーク負荷の分散に配慮した PIMS ネットワークの構築が不可欠となる．PIMS ネットワークの負荷分散構成法については今後の課題である．

参考文献

[1] ICQ Inc. , http://www.icq.com/

[2] RFC2136,“Dynamic Updates in the Domain Name System (DNS UPDATE)”

[3] 田中, 筒井, 矢田 “公開鍵暗号を用いた安全なメッセージ伝達方式の提案”, IPSJ 全国大会, 1H-03, Mar. 2002.

[4] 田中, 筒井, “安全なメッセージ伝達メカニズムを用いた名前解決方式”, FIT2003, Sep. 2003.

[5] Cerulean Studios, “Trillian”, http://www. trillian.cc/

[6] RFC2440,“OpenPGP Message Format”

[7] The GNU Privacy Guard, http://www.gnupg.org/

[8] Bruce Schneier, “Applied Cryptgraphy ”, John Wiley & Sons, Inc.,1996

[9] David L. Chaum, “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms”, Communications of the ACM, Vol.24, Num.2, Feb. 1981

[10] Gnutella ,http://www. gnutella. com/

[11] Ian Clarke, “A Distributed Decentralised Information Storage and Retrieval System”,Master’s thesis, Univ. of Edinburgh, 1999.

[12] The Freenet Project, http://www. freenetproject.org/

[13] I. Stoica, R. Morris, D. Karger, M.F. Kaashoek, H. Balakrishnan, “Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications”, In Proc. ACM SIGCOMM ’01, Aug. 2001