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

田中 裕之 † **筒井 章博** ‡

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

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，既存の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，端末の移動に合わせて DNS サーバの登録情報を動的に更新することにより，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るため，サーバのセキュリティが損なわれてしまうと，秘匿されるべき情報が全て第三者に漏洩する可能性がある．また，サービス運営者がサーバ上の個人情報を悪用しようとした場合，利用者はこれを阻止できない．従って既存のサービスでは，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で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ためのフレームワークとして，PIMS (Private Instant Messaging Service) を提案した [1]．本発表では，PIMS の実装およびその応用例として，PIMS を利用した IM アプリケーションと PIMS-DNS のデモンストレーションを行なう．PIMS-DNS は，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．

2　安全なメッセージ伝達システム PIMS

本研究では，通信内容の秘匿，利用者の所在 (IP アドレス) の秘匿，利用者情報 (識別子，本名，通称名など) の秘匿，送受信者間の関連性の秘匿の 4 つを，安全なメッセージ伝達システムに求められる条件と定義した．PIMS の目標は，互いに IP アドレスが不確定な送信者と受信者の間で，これらの必要条件を満たすメッセージを伝達する機能を提供することである．

図 1 に PIMS の概要を示す．PIMS では，各ユーザ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 (PIMS ネットワーク) によって，メッセージの配送を実現する．また，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[2] などの公開鍵暗号方式の公開鍵を使用する．

†tanaka.hiroyuki@lab.ntt.co.jp

‡tsutsui.akihiro@lab.ntt.co.jp

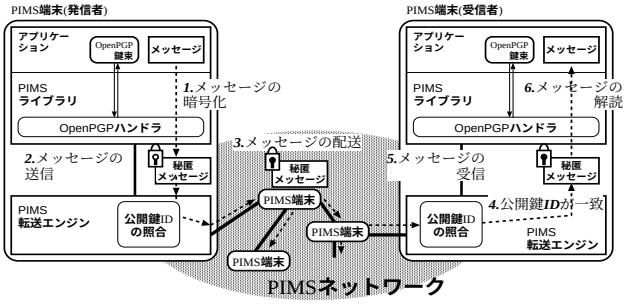

図 1: PIMS の構成例とその動作概要

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上の PIMS アプリケーションインターフェイス (PIMS ライブラリ) 内で，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，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 1-2,3)．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．また，メッセージの発信元および宛先 IP アドレスは，PIMS 転送エンジンで中継される毎に変化するため，中継中の IP パケットを観測しても，発信者・受信者の端末 IP アドレスは確定できない．各端末に配送されてきたメッセージが自分宛であるかどうかは，その解読可否により判断する (図 1-4,5,6)．

3　PIMS-DNS

送受信者間で，互いの端末 IP アドレスが不明な場合に，PIMS によるメッセージ伝達を利用して IP アドレスを通知し合うことによって，秘匿性の高い名前解決が実現できる．PIMS による名前解決では，アドレス問い合わせに対する回答の是非を自ら判断できることから，既存の名前解決方式より柔軟な運用が可能である．

この仕組みを，アプリケーションの DNS 参照インターフェイスを介して利用可能としたのが PIMS-DNS である．PIMS-DNS は，ドメイン名として表記された PIMS 識別子を判別して，PIMS による名前解決と通常の DNS による名前解決を選択実行する機能を拡張した，DNS 参照ライブラリまたは DNS サーバとして実装される．

4　デモンストレーション内容

Microsoft Windows2000/XP 版 PIMS を実装した 2 台の PC を使用して，PIMS を利用した IM アプリケーションによるショートメッセージ通信の実行例を示す．また，PIMS-DNS のデモンストレーションとして，PIMS による名前解決を利用した Web アクセスの実現例を示す．

参考文献

[1] 田中, 筒井, “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”, Internet Conference 2003, Oct. 2003.

[2] RFC2440,“OpenPGP Message Format”