公開鍵暗号を用いた安全なメッセージ伝達方式の提案*

1H−03

田中 裕之†　筒井 章博　矢田 浩二‡
NTT 未来ねっと研究所§

1 はじめに

近年、インターネットへのアクセス手段の多様化によって、人々はあらゆる場所からインターネットを活用するようになった。またIPアドレスの有効利用のため、PPP/IPCP や DHCP などを用いて、接続端末に対しIPアドレスを動的に設定する機構も広く利用されている。このような環境では、通信対象となるユーザもしくはアプリケーションサービスをIPアドレスによって特定して、端末間で直接通信メッセージを送受信することができない。

そこで本稿では、IPアドレスのわからないユーザやアプリケーションサービスに対して、その所在を探索し、安全にメッセージを伝えるための手法を提案する。

2 既存方式の問題点

本研究では、通信を行なおうとする二者間で安全にメッセージを伝達する際に秘匿すべき情報として、以下に示す 2 つの項目に着目した。

1. 通信メッセージの秘匿
   伝達されるメッセージは、第三者によって盗聴されてはならない。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したことが判別できなければならない。

2. 通信者の秘匿
   第三者が、メッセージの送受信者を特定できてはならない。また、送受信者の所在、すなわちIPアドレスを第三者が特定できてはならない。

現在、互いの端末のIPアドレスがわからないユーザ間でメッセージを交換するための手段として、ICQ[1]などのインスタントメッセージング (IM) サービスが普及しつつある。これら既存の IM サービスは、各ユーザの個人識別情報 (ID) と IP アドレスとの対応を管理するディレクトリサーバと、刻々と変化するユーザの所在をサーバに通知するクライアントから成る、クライアントサーバ型のシステムを構築することによって、IP アドレスと各ユーザとの関連を解決する。

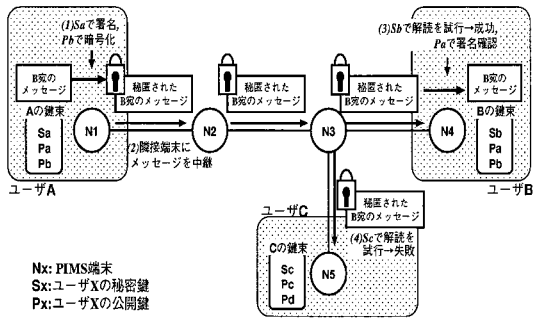

図 1: PIMS の基本概念

しかしながら、このようなサーバ集中型のシステムには、サーバのセキュリティが損なわれると全ての個人情報が漏洩してしまうという危険が潜在する。また、サーバ管理者には IM サービス利用者の個人情報が全て把握可能なため、サーバ管理者を信用することが、秘匿機能実現の大前提となる。そこで本研究では、以上の 2 点を既存 IM サービスの問題点と捉え、これらを解決するメッセージ伝達方式として 新たに Private Instant Messaging Service (PIMS) を提案する。

3 PIMS のアーキテクチャ

既存 IM サービスのようなクライアントサーバ型の通信アーキテクチャでは、通信者の情報を秘匿することが難しい。そこで PIMS では、同報通信を基本としたサーバレスのメッセージ伝達アーキテクチャを採用する。

図 1 に PIMS の基本概念を示す。図 1 の N1〜N5 は、ネットワークに接続された PIMS 対応の通信端末である。図 1 に示すように、各 PIMS 端末は、少なくとも 1 つの PIMS 端末と相互に隣接して、PIMS 端末同士を接続するメッセージ中継ネットワークを構成する。

PIMS では、公開鍵暗号 [2] を用いてメッセージの内容を秘匿する。また、メッセージの発信者を認証するために、発信者が公開鍵暗号を用いて通信メッセージに署名を行なう (図 1-(1) 参照)。

第三者によるメッセージの送受信者を特定不可能とするため、配送される秘匿メッセージには、発信者の IP アドレスや送受信者の識別子など、送受信者やそ

*Secure Message Transmission Protocol using Public-Key Cryptography

†Hiroyuki Tanaka <hiro-tn@exa.onlab.ntt.co.jp>,
‡Akihiro Tsutsui, Kouji Yata
§NTT Network Innovation Laboratories

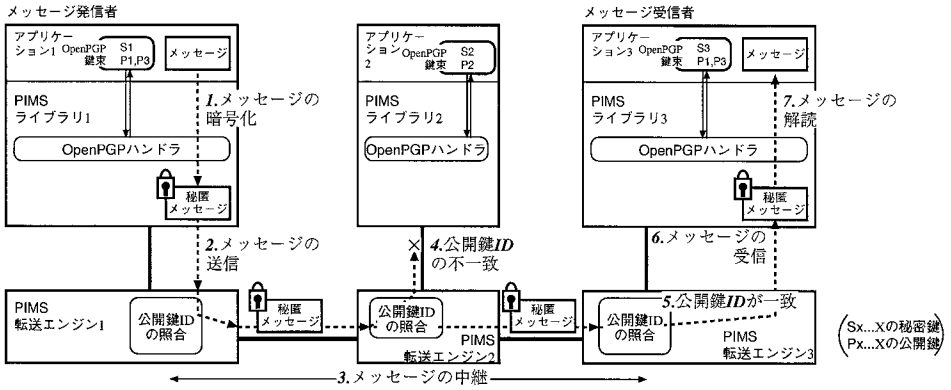

図 2: PIMS システムの構成とその動作概要

の所在を一意に識別可能な情報は平文では添付されない。配送された秘匿メッセージが自分宛であるかどうかは、各自の秘密鍵を用いて受信したメッセージの解読を試み、解読可能か否かによって各 PIMS 端末で判断する (図 1-(3),(4) 参照)。

4 PIMS の実装と動作

4.1 システム構成

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。

PIMS ライブラリでのメッセージの暗号・署名認証処理には、OpenPGP[3] 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 [2][3]、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の 64bit ハッシュ値が公開鍵 ID として含まれている。そこで PIMS では、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。

4.2 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を隣接する PIMS 転送エンジン 2 に中継する。また、PIMS 転送エンジン 2 は、さらに PIMS 転送エンジン 3 にこの秘匿メッセージを中継する (3)。

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。

5 まとめと今後の展望

本稿では、安全なメッセージ伝達手段として PIMS を提案した。PIMS 実現の課題は、公開鍵暗号とブロードキャストを使用することに伴なうシステム負荷の増大に対する対策である。本稿では、OpenPGP の公開鍵 ID を活用した暗号処理の負荷軽減手法を示した。ブロードキャストの抑制手法は今後の課題である。

PIMS を用いれば、IP アドレスのわからないユーザやアプリケーションサービスの間で、直接通信を始めるための情報を安全に交換することが可能である。今後は、PIMS の Peer-to-Peer アプリケーションへの応用についても検討を進める。

参考文献

[1] ICQ Inc. , http://www.icq.com/
[2] Bruce Schneier, “Applied Cryptgraphy ”, John Wiley & Sons, Inc.,1996
[3] RFC2440,“OpenPGP Message Format”