PGP 公開鍵サーバの運用と問題点

6F－3

王 仁峰　　村山 優子　　天野 橘太郎

広島市立大学 情報科学部

1　はじめに

インターネットを基盤とした情報社会では電子メールなどの通信手段についての安全性の保持が必要とされる．Pretty Good Privacy（PGP）は公開鍵暗号方式の暗号化プログラムで主に電子メールなどで利用されている．

現在 PGP の公開鍵の取得方法は直接入手する以外に，公開鍵サーバを利用することができる．PGP を用いた通信が今後増えることが予想されるため，利用しやすい PGP 公開鍵サーバの設置が急務である．本予稿ではサーバ管理の安全性，公開鍵データの効率的な利用や分配，また，ネットワーク社会を考慮した PGP 公開鍵サーバの運営についての考察を行なう．

2　PGP 公開鍵サーバ

PGP 公開鍵サーバはユーザに対して基本的に電子メールを利用して公開鍵の登録，検索，取得するサービスを提供している．サーバの本体は，一般ユーザが取得した公開鍵を保存するように，サーバ管理用の架空の人物に公開鍵データを保存させ，一般に公開することで公開鍵サーバとして稼働している．登録要求のあった公開鍵はバッチ処理で定期的に登録，検索などを行ない，サーバの保持する鍵データを更新している．

また，各サーバ間は同期をとることでデータ差の補完を行なう．同期は，登録または更新リクエストをそのまま同期サーバに配送することをいう．現在 Web 上で供給されている登録・検索サービスは公開鍵を即時検索，公開鍵本体の表示をするものである．登録は内部で電子メール形式に変換して処理する．

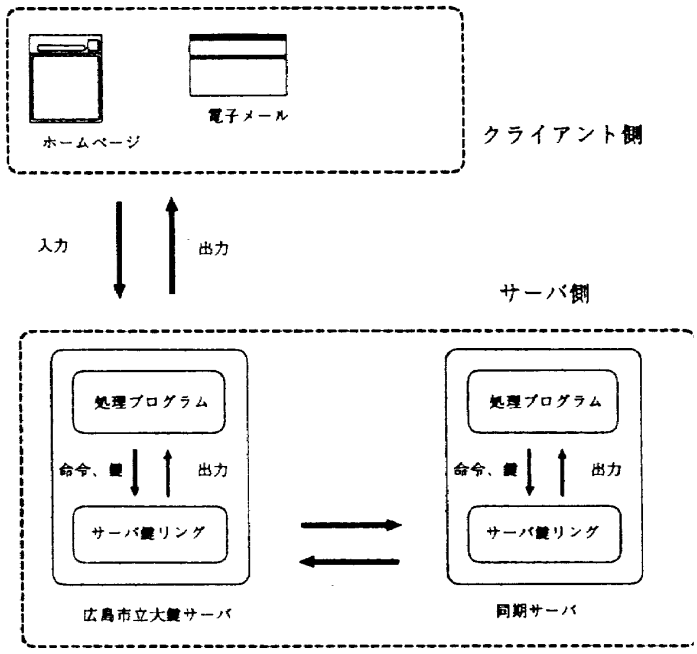

図 1: PGP 公開鍵サーバの処理

3　公開鍵サーバの利用状況

表 1 が示すように現在のサーバは同期サーバからの鍵配送 (incremental) が最も多く鍵の取得命令は行なわれていない．また，登録と同期サーバからの配送で一日に約 30 件近くの鍵の登録あるいは更新があることになる．約 40 日間の観測結果だがサーバは鍵の保存場所としての動作が主となっている．

図 2 に示されるように保存するファイルサイズは，計測期間内に約 1.5$Mbyte$ の増加があった．安全面から鍵の bit 数が更に増やされていくため，今後の増加は間違いなく，何らかの対策が必要である．

Setting a PGP(Pretty Good Privacy) key server into operation

Jinho Oh　Yuko Murayama　Kitsutaro Amano
Faculty of Information Sciences, Hiroshima City University

表 1: 処理内容

処理	リクエスト数
unknown	2
get	0
incremental	1290
status	0
last	0
get keyid	0
index	0
help	0
add	22
dup incremental	9
verbose index	0

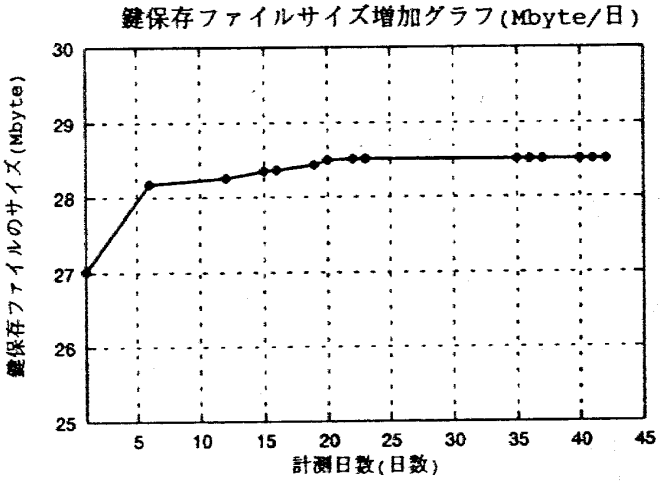

図 2: 鍵保存ファイルサイズ

4　公開鍵サーバの問題点

問題点として以下のものがあげられる.

- 同期をとる各サーバの鍵データの重複が多い
- サーバの鍵データファイルサイズの肥大化
- 同期は登録あるいは更新時のみ鍵配送する

現在の PGP 公開鍵サーバの同期は各サーバが同じ鍵データファイルをもっていることが前提となる. また, 鍵データファイルサイズは今後さらに増加. そして, 同期は登録済みの鍵の配送はしないため, 手動登録等の処理が必要となる. これにより, 公開鍵サーバの新規設置はさらに難しくなる.

5　DNS を応用した新公開鍵サーバ案

以下に Dmain Name System(DNS) を利用し鍵データを分散する 2 案を紹介する.

両案とも鍵データは, ユーザ識別子に示される電子メールアドレスのドメイン名に基づいて分散される.

(1) 鍵データを NS のデータの一部として登録

Name Server(NS) のデータベースに鍵を登録することで分散する. この場合, 鍵データの属性を新たに定義する必要がある. 鍵の検索, 登録は DNS を使用する.

(2) DNS の名前情報分散に基づいた公開鍵サーバの分散

公開鍵サーバはユーザ識別子に各自特定のドメイン名を持つ鍵のみを保存する. 鍵の検索, 登録は NS に登録しているサーバの保持対象を DNS で調べ、該当するサーバにサービスを提供させる。

今後, これらの手法について考察を行なっていきたい.

6　むすび

これから更に増えるであろうユーザに対して公開鍵サーバは有効な鍵入手手段として認識されるだろう. このことから今後のサーバ運営が PGP を支える力になり得るか否かが決まるだろう. 今後 DNS の利用などについて具体的に考えていきたい.

参考文献

[1] Simson Garfinkel 著, 山本 和彦 監訳, "PGP 暗号メールと電子署名", O'Reilly,April 1996.

[2] R. Needham and M. Schroeder, "Using Encryption for Autheniication in Large Networks of Computers", Communications of the ACM, Volume 21,No.12,pp 993–999,dec 1978

[3] P. Mockapetris, "Domain names - Implementation and specification" RFC1035, Novemver 1987