マルチメディア通信と分散処理 86－7
グループウェア 26－7
（1998. 1. 29）

PGP公開鍵サーバの運用と問題点

王 仁峰　　村山 優子　　天野橘太郎

{jinho,murayama,amano}@nets.ce.hiroshima-cu.ac.jp

広島市立大学情報科学部

電子メールやWWWが一般に浸透したネットワークを基盤とした情報社会では、通信は欠かすことの出来ない要素である。通信者の秘匿性や情報の完全保持は今後、さらに重要となる。Pretty Good Privacy(PGP)とは第三者から情報を守り安全な通信を可能にするための公開鍵暗号方式のプログラムである。本研究では、PGPの公開鍵入手を仲介するPGP公開鍵サーバのメカニズムを調査、考察を行ない、現在の公開鍵サーバの欠点と改善方法を提案する。

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

Jinho Oh　Yuko Murayama　Kitsutaro Amano

{jinho,murayama,amano}@nets.ce.hiroshima-cu.ac.jp

Faculty of Information Sciences, Hiroshima CityUniversity

We report our trial to put a PGP key server into operation. Through our trial we found a fundamental problem with existing key servers that the server system is so centralized-structured that a server has to maintain all the key data over the world; the system require a large amount of memory such as 27 Mbytes. We have observed the increase of key database over a few weeks. An idea to distribute such database is proposed.

1 はじめに

現在の情報社会はインターネットに代表されるネットワーク環境や，電子メールなどの通信手段の普及により，安全な情報管理を必要とする.Pretty Good Privacy（PGP）は公開鍵暗号方式のプログラムで主に電子メールなどで活用されている.

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考察を行なう.

2 基本的な暗号方式

暗号方式には大きく分けて共通鍵暗号方式と公開鍵暗号方式が存在する以下にこれらを簡単に説明する.

2.1 共通鍵暗号方式

共通鍵暗号方式は DES，トリプル DES，IDEA などに代表され，情報交換を行なう両者が同じ鍵で暗号化および復号を行なう.

この方式は鍵がともに第三者の手に渡っていないという前提の下に安全性が保たれる.

また，相手に鍵を安全に配送できなければ秘密メッセージを送ることが出来ないため，相手との情報交換を始める環境を整えるのが困難である.

共通鍵暗号の例として Alice, Bob, Chris, Dawn, Eric の 5 人の場合を示す（図 1 参照）.

5 人の状態では鍵の数は 10 個必要となる. これが n 人の場合，$\frac{n(n-1)}{2}$ 個の鍵が必要である.

グループ内の人数が増えるにつれ，鍵の個数の増加は $O(n^2)$ となり，鍵の管理・配送の安全性の低下は確実である.

2.2 公開鍵暗号方式

公開鍵暗号方式は RSA, Diffie-Hellman などに代表され 1 対の公開鍵と秘密鍵で暗号化，および復号を行なう.

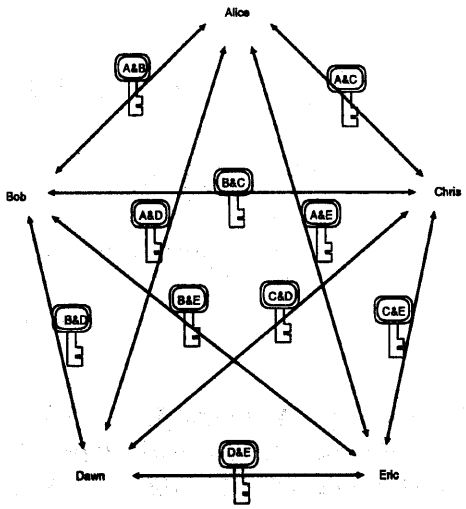

図 1: 5 人による共通鍵暗号

この方式は公開鍵を相手に渡すがこの鍵では復号されないため，管理対象は自分の秘密鍵のみとなる. 従って共通鍵暗号方式と比べ安全性が向上している. しかし，被害が軽減するが，暗号化処理に時間がかかるという欠点がある.

2.3 アルゴリズムの比較

例として，共通鍵暗号方式の DES，公開鍵暗号方式の RSA を参考に暗号化手順を比較し，安全性が向上した公開鍵暗号方式が処理に時間をかかることを示す.

2.3.1 DES の暗号化手順

DES は置換による暗号化であり図 2 に手順を示す.

2.3.2 RSA のアルゴリズム

PGP は非常に大きな素数 p,q とその積 n から，e と d を生成し，鍵を生成する. 公開鍵は n,e. 秘密鍵は d によって構成される. なお,e は $(p-1)(q-1)$ と互いに素な値であり，n,d は以下の式で表される.

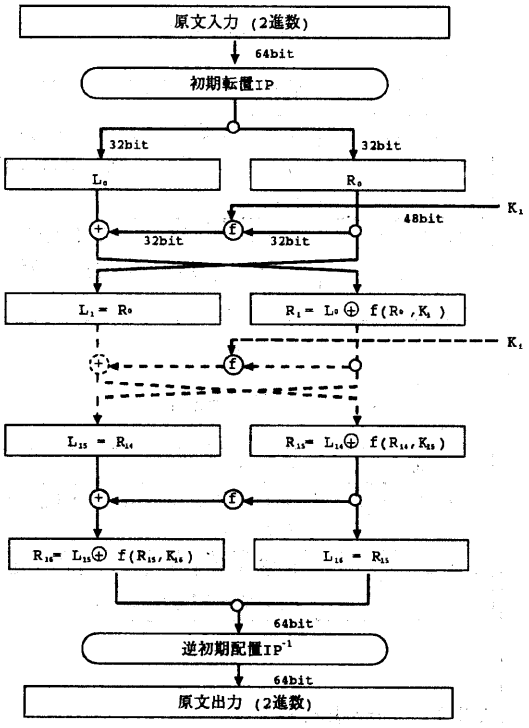

図 2: DES 暗号の組立て手順

$$n = p * q \tag{1}$$

$$d = e^{-1}(mod(p-1)(q-1)) \tag{2}$$

例えば, メッセージ M を公開鍵で暗号化するには

$$C = M^e \bmod n \tag{3}$$

を行ない暗号文 C を得る.

2.3.3 特徴の比較

RSA は桁の大きな数の因数分解が困難であることを利用したアルゴリズムであるため, 扱う数の桁が大きく,DES と異なり, 暗号化に時間がかかる.

2.4 公開鍵暗号の応用

2.4.1 秘匿性

秘匿性とはメッセージの内容を第三者にみられないことである. 公開鍵で暗号化した文章は対になる秘密鍵でしか復号できず, また片方の鍵の情報はもう一方の鍵を知るための情報を与えない. これにより, 自分の秘密鍵が第三者に渡らない限り安全に暗号化, 復号をおこなえる.

2.4.2 完全性

完全性とは, メッセージの内容が第三者により改ざんされないことである. 電子署名は秘密鍵で行なわれ, 所有者しかできず, 受けとり人も偽造できないため, 署名者が言い逃れできないよう将来の正確な裁定を保証する記録として残すことができる.

3 PGP の概要

PGP は RSA アルゴリズムを使用した公開鍵暗号方式の暗号である. 機能は暗号化・復号, 改ざんの検出, そして署名による認証を持つ.

任意の userID, 一意の keyID, 生成日などを持ち, 秘密鍵を必要とする作業をする際はパスフレーズと呼ばれるパスワードを必要とする.

4 PGP 公開鍵サーバ

公開鍵サーバは公開鍵の取得の仲介を目的とし, ボランティアで行なわれている. サーバは登録/更新された公開鍵を保持し, リクエストに応じて, 公開鍵の情報や検索, 配布を行なう.

公開鍵サーバは一般ユーザ用インタフェースとサーバ同士の通信機能を持つ. 以下に内部動作と機能を紹介し, サーバの機構について説明する.

4.1 PGP 公開鍵サーバの内部動作

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.

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形態をとっている.

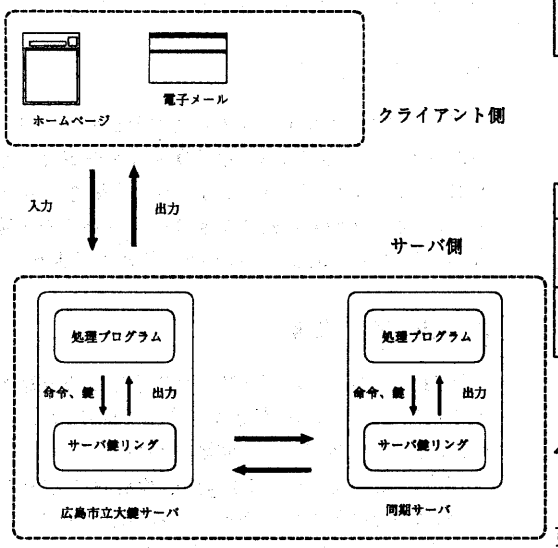

図 3: PGP 公開鍵サーバの処理

4.2 サーバの機能

4.2.1 登録

サーバは公開鍵登録の際, 公開鍵が含まれていれば登録をおこなう. すでに登録されている公開鍵は公開鍵のユーザ識別子, パスワードの機能を果たすパスフレーズ等の変更により更新されていなければ再登録は行なわない. また, 同期サイトがある場合はそのサイトに鍵を転送する.

4.2.2 ユーザ用機能

鍵情報の検索と正規表現や鍵 ID を指定することで目的の鍵を入手できるような命令が用意されている.

表 1: 鍵情報入手命令

命令	処理内容
index	サーバに登録されている鍵 ID のリストや指定された鍵の情報を返す
verbose index	index 命令で得られる情報に更に fingerprint (鍵指紋) 情報を加える

表 2: 鍵入手命令

命令	処理内容
get (userid)	指定された userid の公開鍵を取り出す
mget (regexp)	正規表現 regexp に該当する鍵全てを取り出す

4.2.3 サーバ用機能

鍵の更新情報についての機能が用意されている. 更新された鍵の反映, 入手などが可能で多量の鍵を一度に扱うことができる.

表 3: サーバ情報入手命令

命令	処理内容
last (X)	過去 X 日間の間に更新された鍵を入手する
incremental	更新された鍵を同期サイトに配送する
status	今までにサーバで処理された命令の内訳を入手する

4.3 公開鍵サーバの利用状況

表 4 が示すように現在のサーバは同期サーバからの鍵配送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から一日に 60 個近くの鍵のやりとりがあることになる.

約 20 日と短期間の観測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.

表 4: 処理内容

処理	リクエスト数
unknown	2
get	0
incremental	1190
status	0
last	0
get keyid	0
index	0
help	0
add	24
dup incremental	9
verbose index	0

4.4 鍵リングサイズの成長度

約 20 日間のデータだが, 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, 何らかの対処が必要となるだろう.

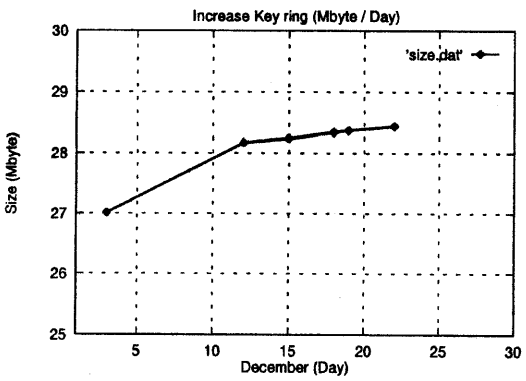

図 4: 鍵リングのサイズ

4.5 現在の公開鍵サーバ

初期の公開鍵サーバは PGP プログラムを使用していた. もともと巨大な鍵データを扱うように設計されていなかったため, 鍵が増えるに従い, 処理効率が悪くなった. 現在では, 鍵データはハッシュ関数で木構造の構成をとるようになり, 高速な検索を可能にしている.

5 公開鍵サーバの問題点

現在の PGP 公開鍵サーバには以下の問題点がある.

- 同期サーバデータの不完全一致

  同期をとっているサーバのデータが完全一致ではないため, ある公開鍵サーバのデータが失われた場合, そのサーバにしかない鍵が失われる可能性がある.

- 登録あるいは更新時のみの同期

  鍵の同期サイトへの配送は更新時に電子メールで送られる. このため, 同期していない間の鍵データは手動で入手する必要が生じる. また, 鍵の検査をしないため何らかの原因で検索できない鍵や壊れている鍵が増えると他のサイトに不適切な鍵が配布されてしまう.

- ファイルサイズの肥大化

  鍵データの登録数は約 5 万個にのぼるため, サーバマシンのメモリ不足やプロセスの実行優先度の低下などが発生しやすく, 負担がかかることが挙げられる. 登録や更新もファイルサイズが巨大化するに従い処理時間がかかることが予想される.

6 公開鍵サーバの負荷軽減

鍵情報は直接キーリングと呼ばれるデータベースから得ているため, 対象の鍵リングのサイズの巨大化に従い, 処理速度の低下, 処理時間の増加を引き起こす. 今後増え続ける鍵に対処するには, サーバの鍵データの分散が効果的であると考えられる. サーバの鍵データを鍵 ID に明示される電子メールアドレス別に分割する案, 企業や組織が各自のサーバ立ち上げによる分散案, そして同期

サイトからの鍵は情報だけ保持する新たなサーバを構築する案について考察する.

6.1 サーバ内の鍵データ分割

どの鍵IDにも電子メールのアドレスを付記されるためドメイン名や国別でリングを分割し, 一つのキーリング当たりのデータ量を減らすことで鍵処理の負荷を減らす. 欠点として, 鍵の分類先を決定が難しくなることが予想される.

6.2 組織別サーバ立ち上げによるデータ分散

プロバイダや企業が各自, サーバを立ち上げ, 組織内の鍵データを一括管理する. 管理対象が明確になり鍵の更新情報が正確で管理形態として, 最適と思われる.

しかし, サーバを公開し一般の公開鍵の登録などを行なうには制約が多くなり, 内部だけのサービスしか提供できない形になると思われる.

6.3 新たな公開鍵サーバ構造の提案

新たな公開鍵サーバ形態として鍵リングをもたず, その鍵情報のみを保存し, 提供する形態を提案する.
現在サーバで得られる鍵情報は鍵のuserID,keyID, fingerprint (鍵指紋), 鍵の使用可能か否かである. この情報部分だけを更新し, 鍵はその鍵を持つサーバにリクエストを送る形態をとることでサーバは自分に登録された鍵だけをもつだけよい.

6.4 実現の可能性

鍵データの分割は現在サービスを提供しているサーバ内で実現可能である. また新規サーバ立ち上げの際, サービスに必要なキーリングのみを入手すればよいため現時点での最善だと思われる. しかし, 今後の鍵データの増加, 新たな公開鍵サーバの立ち上げを考慮すると, 鍵の所在情報を管理するデータ分散型が将来必要になってくるであろう. 現在, 新たな公開鍵サーバのプロトタイプを構築中である.

7 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. PGPの浸透度に反して, 鍵情報を提供する公開鍵サーバが少なく, 中央機関に相当する公開鍵サーバが存在していない. 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のではないだろうか. 今後はDNS (Domain Name System) などを鍵サーバとして導入可能かどうかも検討していきたい.

8 謝辞

広島市立大学の弘中哲夫氏, PGPサーバの構築, 技術的助言, 協力を頂いたICATの鈴木裕信氏に深謝します.

参考文献

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

[2] Roger M. Needham and Michael D. Schroeder, "Using Encryption for Autheniication in Large Networks of Computers", Xerox Palo Alto Research Center, Volume 21,No.12,pp 993–999, December 1978

[3] P. V. Mockapetris, "Domain name - concepts and facilities" RFC1034, Novemver 1987