公証人を用いた暗号メール公開鍵証明書発行方式*

3D−8

菊池浩明　　黒田康嗣†

(株) 富士通研究所‡

1　はじめに

広域ネットワークInternetの商用利用が進むに伴い，電子メールのセキュリティの重要性が問題となっている．現在普及している電子メールシステムでは，中継ネットワークでの盗聴と，改竄に対する考慮がされていないためである．

そこで，暗号技術を適用し電子メールのセキュリティを強化するPEM(Privacy Enhanced Mail)[1]が提案され，現在世界中で盛んに実装と接続実験が繰り返されている[2, 3]．PEMでは，公開鍵暗号と秘密鍵 暗号をハイブリッドに組み合わせて暗号処理を高速化し，信頼できる第三者(発行局)により電子署名された 公開鍵証明書(証明書)によって 公開鍵を安全に，かつ効率的に管理することを主な特徴としている．

ところが，証明書を正しく発行するためには，申請者が正規のユーザであり，偽りのない申請をしているかどうかを確認しなければならず，この証明書発行時のユーザ認証をどのように実現するかが，発行局の大きな課題となっていた．ユーザの規模が小さい場合は，管理者が直接確認したり，信頼できる正規ユーザリストとの照合したりする認証が可能だが，本研究が意図するInternetの様な大規模な環境では現実的ではない．多数の発行局を階層的に組織する提案もあるが，無計画な階層化では，発行局が乱立してユーザ情報が分散し，証明書の検索や配布が困難となる恐れもある．

そこで，本稿では，この課題に対して，公証人による申請方式を提案する．そして，提案方式を実装した発行局での運用実験を行ない，その安全性と広域環境での有効性を検討する．

2　公証人申請方式

公証人とは，新規のユーザの身元を保証する正規ユーザである．本方式では，公証人が新規ユーザに代わってPEMを使って 証明書の申請を行なう．従って，発行局は，公証人の電子署名を 検証することにより，申請者を機械的に認証することが出来る．証明書が発行されたユーザは，他の新規ユーザの公証人となれる．それゆえ，連鎖的に信頼できる証明書を発行していくことにより，大規模のユーザを信頼の鎖で結ぶことが出来る．

以上の手続きを図1で説明する．

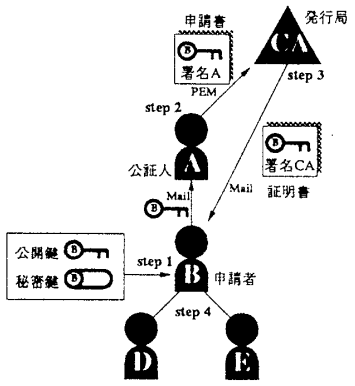

図 1: 公証人申請方式

step1: ユーザ B は，自分で秘密鍵と公開鍵の対を作る．秘密鍵は安全に管理し，公開鍵だけに，名前やメールアドレスなどの個人情報を加えて申請書を用意し，公証人 A に送信する．図2に例を示す．

step2: 公証人 A は，申請書の内容を認めれば，PEMで A の電子署名をして，発行局 CA に送信する．

step3: 発行局 CA は，申請書の公証人の署名を検査し，検証できれば，更に二重申請などのチェックを行なう．検査に合格すれば，申請情報に CA の電子署名を行ない，証明書を発行する．発行した証明書は，内部データベースに 登録し，申請データに基づき，ユーザ B にメールで返送する．

step4: ユーザ B は，証明書を入手し，PEMを利用できる環境となる．また，他のユーザの公証人となり，step1-3 を繰り返す．

```
CN= Yasutsugu Kuroda
N= 7e29b196fd3ecead935ceccabe9076af68671a883
12f565ff4431adb93260b624c10b690e78adc816d79b
MAIL= kuroda@flab.fujitsu.co.jp
O= Fujitsu Laboratories Ltd.
OU= Information Prosessing Network Center
TITLE= researcher
TELEPHONENUMBER= +81 12-428-012
```

図 2: 申請書サンプル

*Issuing Public Key Certificate with Notary for Privacy Enhanced Mail

†Kikuchi Hiroaki, Kuroda Yasutsugu

‡Fujitsu Laboratories Ltd.

3 運用実験

提案方式の有効性を実証するため，発行局を実装し，限定ユーザで運用実験を行なった．運用形態は，図2に示す様に，発行局 WIDE-CA, 配布局 Keysev, 暗号メールシステム FJPEM を有するユーザから成る．

暗号メールシステム FJPEM は，C 言語と Perl スクリプトで実現されており，Sun を始めとする 8 社 12 機種のワークステーションでの動作が確認されている．受信した証明書のキャッシュ，配布局への自動証明書参照などの機能を有する．暗号処理性能は文献 [3] に報告されている．RFC の標準案に対して，メールアドレスを証明書に組み込んだ点と，日本語のコード体系を考慮した電子署名処理の点が拡張されている．RSADS 社とロンドン大学の二種類の PEM の実装と相互接続性を確認している．

発行局 WIDE-CA と配布局 Keyserv は，C 言語,Perl スクリプトで共に S4/110 上に実装されている．発行局は，通常のメールインターフェースにより 申請書や証明書を送受信する．

配布局 Keyserv は，発行局と連携しており，ユーザからの要求に答えて 証明書データベースの検索や参照の機能を提供する．ユーザからの問い合わせには，RFC954 WHOIS プロトコルが用いられる．キーワード，シリアル番号，メールアドレス，廃止証明書，新規証明書の 5 種類の検索が機能している．負荷に応じて分散が可能で，本実験では二台の配布局が用いられた．

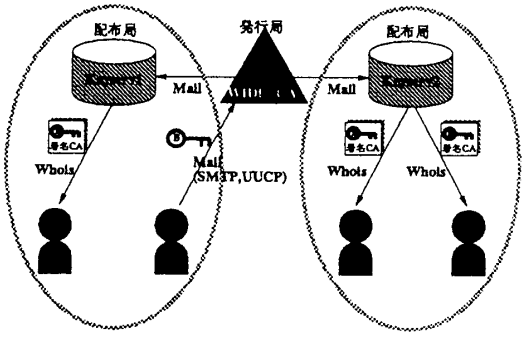

図 3: 運用形態

4 検討

4.1 公証人方式の安全性

1. 申請者は個人情報を偽れない．
   名前などの偽りは，そのユーザの証明書の責任を持つ公証人に 拒否される．また，メールアドレスを偽ると，証明書を受けとることが出来ない．
2. 第三者が申請書を改竄出来ない．
   公証人の電子署名があるため，改竄はもちろん，公証人の なりすましも不可能である．
3. 公証人はうそをつける．
   しかし，発行局に履歴は残るため，その公証人に対してペナルティを与えることが出来る．また，ユーザは公証人を選ぶ権利を持つ．

ユーザ数 [人]	53	
証明書発行処理時間 [sec]	39.0	
証明書発行回数 [回 / 日]	2.64	(最大 19)
配布局処理時間 [sec]	1.5	
配布局検索回数 [回 / 日]	35.44	(最大 130)

表 1: 試験運用結果

4.2 運用限界

3ヶ月 (58 日間) の運用データを表 1 に示す．

申請回数はユーザ数に比例すると仮定すると，ユーザ数 n の時の申請書平均到着率 λ_c は次式で表される．

$$\lambda_c = \frac{2.64}{86400}\frac{n}{53}$$

証明書発行処理時間より，平均サービス率は $\mu_c = 1/39$ と定まる．ここで，申請書の到着間隔をランダムとみなし，発行局処理時間の分布を 負の指数分布に従うもの (M/M/1 モデル) とする．この時，発行局での平均応答時間 T_c は次式で表せる．

$$T_c = \frac{1}{\mu_c - \lambda_c} = \frac{1}{0.026 - 5.8 \times 10^{-7} n}$$

例えば，$n = 10000$ の時の平均応答時間は 50.3 秒, 平均待ち行列数は 0.29 である．ただし，発行局までのメールの転送時間は考慮していない．また，$\lambda_c = \mu_c$ となる n の値を求めると，$n_c = 44475.5$ となる．従って，本実装の発行局が処理できる最大ユーザ数は約 44000 人であると言える．最大ユーザ数は計算機の処理能力に比例しているので，仮に，計算機を S4/110(7MIPS) から SS/2(28MIPS) に置き換えると，約 15 万人までの証明書発行が行なえることとなる．

配布局についても同様の仮定を行ない，平均応答時間 T_w を求めると次式のようになる．

$$T_w = \frac{1}{0.67 - 7.7 \times 10^{-6} n}$$

同様に見積もると，最大ユーザ数は約 86000 人となる．

5 おわりに

大規模広域環境での公証人を用いた証明書申請方式を提案し，安全性を検討した．更に，運用実験を行ない提案方式の評価を行なった．その結果，公証人申請方式のセキュリティは十分であり，発行局では 44,000 名，配布局では 86,000 名までのユーザについて 実用的な運用ができることが明らかになった．今後は，WIDE Internet での本格的な運用を試みていく．

WIDE プロジェクトのセキュリティ WG と 富士通研の pem-dev メーリングリストのメンバーに感謝する．

参考文献

[1] Linn, J., et al., "Privacy Enhancement for Internet Electronic Mail: Part I, II, III, IV," *RFC-1421-1424*, 1993

[2] 松崎他, "暗号電子メールシステム", JUS シンポジウム, 1993

[3] 菊池, 森下, "暗号電子メール PEM(Privacy Enhanced Mail) の 実装と課題", 情処第 46 回全国大会, 1, pp.99-100, 1993