プライバシ強化メールPEMにおける証明書配布局の実装と評価

菊池浩明† 黒田康嗣† 永井 武†

プライバシ強化メールPrivacy Enhanced Mail (PEM)がインターネット標準案RFC 1421-1424にて提案されている．PEMでは，公開鍵アルゴリズムを用いることで，ユーザ認証，完全性，電子メール本文の機密性を提供している．インターネットにおけるPEMの実用化に大きな課題となっているのは，ユーザの識別子と公開鍵を運ぶ証明書の配布方法である．そこで本論文では，WHOISプロトコルを用いた証明書配布システムを提案し，現実の電子メール送信の統計情報に基づいて，その性能評価を行う．主要な結論は，1週間分の証明書のキャッシングが，証明書配布サーバへの通信要求を2/5に削減することを示したことである．

Performance Evaluation of an Implementation of Certificate Distribution System in Internet Privacy Enhanced Mail

HIROAKI KIKUCHI,† YASUTSUGU KURODA † and TAKESHI NAGAI †

Privacy Enhanced Mail (PEM) is proposed in Internet standard RFC 1421-1424. Using public key cryptosystem, PEM provides the user authentication, integrity, and the confidentiality of contents of electronic mail. The distribution of certificate which contains a user identifier and the public key is current issue for a practical use of PEM in the Internet. This paper proposes a public key certificate distribution system using the WHOIS protocol, and evaluates the performance of an implementation based on the statistics of electronic mail sending. Main result is that a local certificate cache for a week reduces the traffic of requests to certificate distribution server by 2/5.

1. はじめに

計算機の相互接続による広域ネットワークInternetの商用化に伴い，ネットワークサービスの多様化が進んでいる．Internetを利用した企業間の共同作業も，今後より盛んになることが予想される．ところが，Internetは元来学術ネットワークとして発達してきたため，セキュリティに関する考慮が十分ではない．特に，最も基本的なネットワークアプリケーションである電子メールは，いくつもの計算機間でメッセージの交換と蓄積を繰り返して伝送されるため，その中継中のセキュリティが問題視されている[1)~3)]．

1992年2月，Internetのような大規模広域環境を対象としたプライバシ強化メールPrivacy Enhanced Mail (PEM)が，Internetの標準化文書RFCにて提案されている[4)~7)]．盗聴や改竄，なりすましなどの電子メールの問題点に対して，PEMでは(1)秘密鍵暗号による本文の暗号化，(2)公開鍵暗号による電子署名，(3)公開鍵証明書（以後，単に証明書と呼ぶ）によるユーザ認証，の三つの技術で対応している．

現在，世界各国でこのRFC標準案に従ったPEMの実装と，相互接続実験が始まっている．しかしながら，これらの実装の多くはまだ実験レベルにとどまっており，現実のネットワーク環境での実用性は不確かなままである．この理由の一つは，証明書を配布する仕組みに問題があるためである．

PEMで通信するためには，発信者が受信者の証明書をあらかじめ入手しておく必要がある．RFCでは，ローカルな課題として，この配布の機構については標準化していない．いくつかの実装では，ニュースシステムや，X.500ディレクトリシステム[8)]などを用いて証明書を交換しているが，応答時間などの面で課題が残る．

そこで，我々は，これらの問題を検討し，プライバシ強化メールシステムFJPEMを実装した[9),10)]．FJPEMでは，一度受信した証明書をキャッシュすることと，多くの計算機で採用されているWHOISプロトコル[11)]を併用することで証明書の配布を実現した．

† (株)富士通研究所
Fujitsu Laboratories Ltd.

本稿では，証明書配布システムの実装について述べ，その処理性能を報告する．更に，現実の電子メールの負荷に基づいて見積もったFJPEMでの証明書配布機構の効果を明らかにする．

2. プライバシ強化メールPEM

2.1 概　　要

プライバシ強化メールPEM（Privacy Enhanced Mail）は，Internetの標準化文書RFC-1421，1422，1423，1424[4)~7)]で提案されているプライバシ強化メールの標準形式である．PEMを利用するユーザは，証明書発行局から証明書を発行してもらい，その証明書を使うことによって，本文の暗号化，復号化と電子署名による改竄の検出，ユーザ認証を実現している．**図1**に本システム全体の構成を示す．ここで，PEMの発信者をA，受信者をB，発行局をW，配布局（後述）をSで表している．ただし，公証人Cとは，証明書の発行の際に申請者の身元保証を行うユーザであり[10)]，本稿ではこれ以上深く触れない．

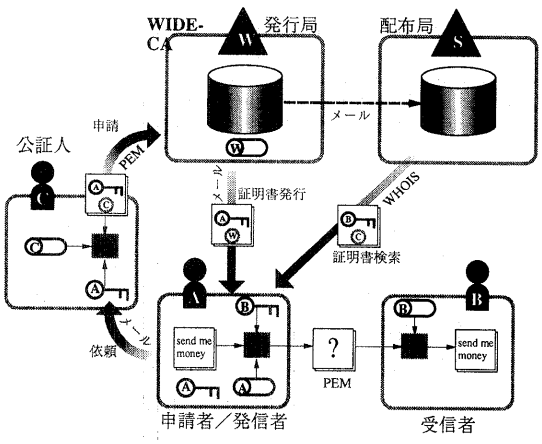


図1　PEMシステム全体の構成
Fig. 1　Configuration of the PEM environment.

2.2 証明書サンプル

証明書は，信頼できる発行局によって電子署名された個人情報と公開鍵である．証明書の中の情報は誰でも読むことができるが，発行局の秘密鍵が盗まれない限り偽造は不可能である．PEMでは，公開鍵は裸のまま直接送受しないで，必ずこの証明書の形式にしてから取り扱う．従って，偽りの公開鍵を正規のものとすり換えて他人になりすます不正行為を防止することができる．図1に示した全体構成では，発行局WからAへ送信されているのがAの証明書であり，Aの公開鍵とWの署名により表現されている．

証明書のサンプルを**図2**に示す．図より明らかなように，証明書は6ビットの英数字と記号により符号化されている．これは，多くのメール転送システムでは，8ビットの値を転送できないためである．この例の証明書に記述されている個人情報の例を**表1**に示す．これらの情報は組織に依存した構造を有するため，一様にOSIの基本符号化規則Basic Encoding Rules (BER)[12)]に従ってデータの列に変換し，相互に交換している．

2.3 配　布　局

本文を暗号化するには，受信者の証明書を取得する必要がある．証明書を公開するために，本実装では，

表1　証明書の中の個人情報
Table 1　Personal information in the certificate.

種類	データ
シリアル番号	38(16進)
署名方式	md2WithRSAEncryption
発行局	WIDE Certification Authority(発行局)
有効期限	93年11月9日～94年9月9日
ユーザ名	Hiroaki Oden Kikuchi
所属	Fujitsu Laboratories Ltd., IP Network Center
公開鍵方式	512-bit RSA

```
Originator-Certificate:
 MIIBOzCCAXECATgwDQYJKoZIhvcNAQECBQAwPjELMAkGA1UEBhMCSlAxDTALBgNV
 BAoTBFdJREUxIDAeBgNVBAsTF0NlcnRpZmljYXRpb24gQXV0aG9yaXR5MB4XDTkz
 MTEwOTExMzY1NFoXDTk0MTEwOTExMzY1NFowgZ4xCzAJBgNVBAYTAkpQMSIwIAYD
 VQQKExlGdWppdHN1IExhYm9yYXRvcmllcyBMdGQuMRowGAYDVQQLExFJUCBOZXR3
 b3JrIENlbnRlcjFPMBsGA1UEAxMUSGlyb2FraSBvZGVuIEtpa3VjaGkwMAYJKoZI
 hvcNAQkBEyNraWtuQG9kZW4uY2VudGVyLmZsYWIuZnVqaXRzdS5jby5qcDBcMA0G
 CSqGSIb3DQEBAQUAA0sAMEgCQQCRQOJNR1JfTQHC7KKYjI+I57XI4l4XwZEC8Wzp
 VuYDV7LIPae2rt2Dy3Mj3E+j3fRRfVIfWZFO4/krHWCQ4ACDAgMBAAEwDQYJKoZI
 hvcNAQECBQADTQA0ogauQdPvICq7FjcO8UbAyNECuYuVFd2Oys9NZW+mKOHMoS1r
 ZbBZCuiEb1hWUWcCy94wlIOXHMk/RclGD3hLbZWOHVsmsP1K4YYn
```

図2　証明書サンプル
Fig. 2　An example of certificate.

配布局と呼ぶ証明書を配布するサーバを用意した．配布局は，RFC-954で標準化されているWHOISプロトコル[11]を用いてユーザと通信する．WHOISを採用したのは，Internetで広く利用され，実際に多くのシステムに組み込まれているためである．配布局は，発行局と連携して証明書データベースを管理している．図1は，発信者AがBにPEMを送信する際に配布局SからBの証明書をWHOISで受信している例を示している．証明書の偽造は，発行局の秘密鍵が盗まれない限り困難であるので，配布局は発行局ほど高いセキュリティを必要としない．従って，複数の配布局を用意して，負荷を分散することも可能である．

また，ユーザからの要求に答えて証明書データベースの検索などのサービスも提供する．用意されている検索の種類を**表2**に，検索の実行例を**図3**に示す．この例では，キーワードkurodaによる検索の結果と，該当するユーザの中からシリアル番号19c（16進）のユーザを選び，その証明書を表示させた結果を示している．

2.4 証明書キャッシュ

本実装では，実際に暗号化処理を行いメールの送受をするユーザ支援システムに，一度受信した証明書を格納しておく証明書キャッシュの機能を加えている．例えば，図1において，受信者Bは，Aから届いたPEMに添付されているAの証明書をキャッシュしておくことにより，次にAへ送信する際には配布局をアクセスする必要がなくなる．より一般には，プライバシ強化メール（ENCRYPTEDモード）をユーザAが，

表2 配布局の機能
Table 2 Facilities of certificate server.

検索の種類	内　容
キーワード	組織名や名前の一部などから該当ユーザのリストを出力
シリアル番号	該当するシリアル番号の証明書の情報を出力
メールアドレス	メールアドレスに一致する証明書を出力
廃止証明書	指定する日付以降に廃止された証明書の一覧を出力
新規証明書	指定する日付以降に発行された証明書の一覧を出力

```
% whois -h keyserv.fujitsu.co.jp kuroda
FS3f:   黒田太郎 (Taro Kuroda)          kuroda@lab.aaa.co.jp
FS10b:  黒田生中 (Namachu Kuroda)       kuroda@risotto.go.jp
FS19c:  黒田康次郎 (Yasujiro Kuroda)      kuroda@lab.fff.co.jp

% whois -h keyserv.fujitsu.co.jp FS19c
[登録日時]:     23/03/94 10:23:22 (JST)
[シリアル番号]: FS19c
[名前]:         黒田康次郎
[NAME]:         Yasujiro Kuroda
[ORG]:          FFF Laboratories Ltd.
[NOTARY]:       notary@lab.fff.co.jp
[E-mail]:       kuroda@lab.fff.co.jp
[証明書]:
MIIB0DCCAW4CAgGcMA0GCSqGSIb3DQEBAgUAMD4xCzAJBgNVBAYTAkpQMQ0wCwYD
VQQKEwRXSURFMSAwHgYDVQQLExdDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAeFw05
NDAzMjMwMTIzMjJaFw05NTAzMjMwMTIzMjJaMIGaMQswCQYDVQQGEwJKUDEiMCAG
A1UEChMZRnVqaXRzdSBMYWJvcmF0b3JpZXMgTHRkLjENMAsGA1UECxMESVBOQzFY
MB8GA1UEAxMYWWFzdXRzdWd1IG5hbWFjaHUgS3Vyb2RhMDUGCSqGSIb3DQEJARYo
a3Vyb2RhQG5hbWFjaHUuY2VudGVyLmZsYWIuZnVqaXRzdS5jby5qcDBcMA0GCSqG
SIb3DQEBAQUAA0sAMEgCQQCp+3HwY+FWs3OmxBM74Lj6O5K4smrlRP+VBstB/4VS
Iwg70FqgjopClMiu8M3gFsrM3OAIXsUt7K/sixTtjB17AgMBAAEwDQYJKoZIhvcN
AQECBQADTQAsOyapoVGpSb952H9Lg/g2Fe7OVVIm7YFRNJj/zrZRiJzYd5VsElfr
l0xkY+/HmGD8iPtvJY7PB7gtwYVEVhHcMMnQA4im/CjWXHk7
```

図3 証明書検索例
Fig. 3 An example of looking up certificates.

ユーザBに送信する際の手続きは次のようになる．

A1.証明書キャッシュから受信者Bの証明書を検索する．検索に成功すれば，go to A4.

A2.証明書キャッシュになければ，配布局を検索する．検索に成功すれば，Bの証明書を証明書キャッシュに加え，go to A4.

A3.配布局になければ，MIC-CLEAR（署名のみ）のモードで送信者Aの電子署名だけを行いBへ送信し終了．

A4.受信者Bの証明書を発行局の公開鍵で検証し，成功すれば，Bの公開鍵でメールを暗号化して（ENCRYPTEDモード），発信者Aの証明書と署名と共に送信して終了．

一方，プライバシ強化メールを受信したBが行う手続きは以下のとおりである．

B1.添付された証明書の電子署名を発行局の公開鍵で検証する．

B2.成功すればその証明書をBの証明書キャッシュに加える．

B3.暗号文をBの秘密鍵で復号化し，証明書から取り出した発信者Aの公開鍵で電子署名を検証する．すべての検証が成功すれば，そのメールは改竄や盗聴が行われていない．

なお，これらの処理は，メールシステムが自動的に実行するため，ユーザが意識する必要はない．なお，証明書キャッシュは，個人の送信先が記録されているため，他人に覗かれるとプライバシーの侵害となる恐れがある．そこで，証明書キャッシュはホスト単位ではなくユーザ個別に行うこととした．

上の手続きのB2において，受信者Bの証明書キャッシュには検証の結果正規と判断された発信者Aの証明書が格納される．従って，互いに署名だけのPEM（MIC-CLEARモード）を1回ずつ送りあえば，各々の証明書キャッシュに相手の証明書がキャッシュされる．すなわち，配布局へのアクセスを全く必要としないでも，安全に公開鍵を交換可能ということである．これにより，WHOISによる配布局のサービスを受けられないネットワークにおいても，PEMを利用することが可能となる．現実には，メール以外の接続性が未整備なネットワークや，セキュリティ上の観点から組織内のネットワークを外部から分離させている接続形態（防火壁）は数多く存在し，配布局を必ずしも必要としないという点は重要である．また，一般には，初対面の相手との通信で暗号化が必要な情報を送ることは稀なので，証明書キャッシュはかなり有効に働くことが考えられる．

3. 運用実験

証明書配布局の機能と証明書キャッシュの有効性を実証するため，WIDE Internet上で運用実験を行った[9),10)]．より多くの環境から参加できるように，実装システムのソースプログラムを匿名FTPサービスやネットワークニュース（電子掲示版）などにより参加を呼びかけた．

配布局は，証明書発行局のデータベースと連携しており，C言語，Perlスクリプトで Sun 4/110 に実装されている．**表3**に実装システムの諸言を示す．配布局は負荷に応じて分散が可能で，本実験では社内ネットワークと外部ネットワークに2台の配布局（ca.fujitsu.

表3 配布局システムの諸言
Table 3 Public key certificate distribution system.

機種	Sun4/110
	CPU:MB86900(14.28Mhz), 7MIPS
メモリ	16 [MB]
ディスク容量	1 [GB]
使用言語	perl（359行）
検索手段	perl組み込み関数

表4 試験運用ログデータ
Table 4 Log data of the experimental run.

運用期間[日]	128
ユーザ数	126
参加組織(ドメイン)数	31
配布局平均処理時間[s]	2.93
配布局1検索回数[回/日]	25.88（最大130）
配布局2検索回数[回/日]	19.41（最大140）

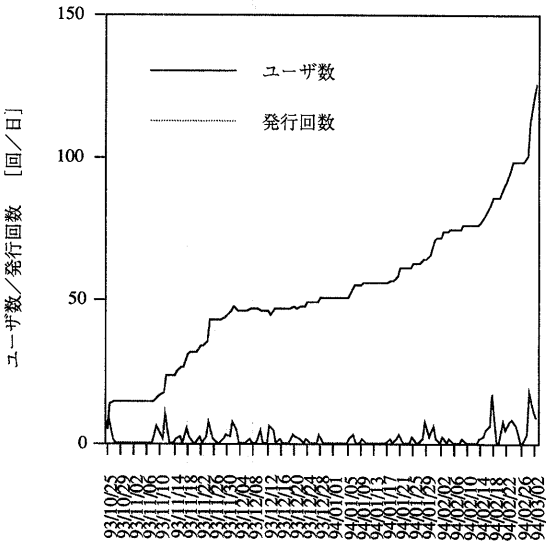


図4 PEMユーザの推移
Fig. 4 Increase in PEM users.

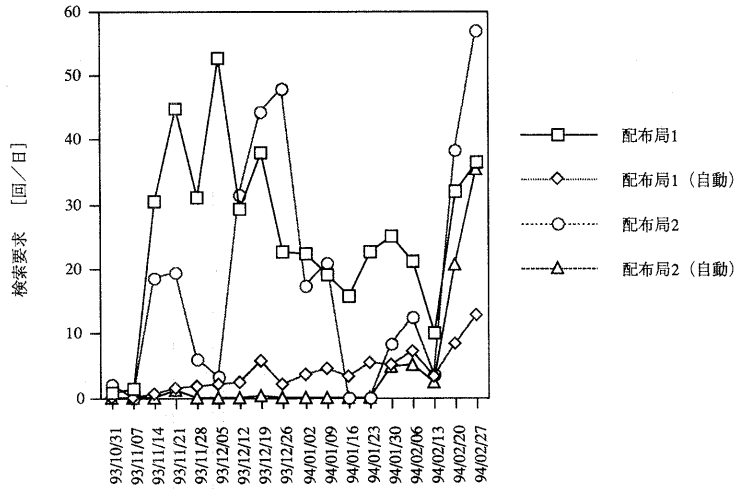


図5 配布局の負荷
Fig. 5 Traffic of certificate servers.

co.jp,keyserv.fujitsu.co.jp）を用いた．

3.1 実験結果

1993年10月25日から1994年3月3日までの実験の，各種ログデータを**表4**に示す．ここで，配布局平均処理時間は，文字列"jp"をローカルにパターン検索した場合をワークステーション組み込みタイマーで100回測定し，その平均をとったものである．そのプロセスのユーザ処理時間のみを測定しており，OSなどによる負荷は含まれていない．ただし，配布局の計算機は配布局サービス専用として実験したため，他の負荷の影響はほとんどないものと考えられる．また，4.1節で後述する配布局への負荷を検討するため，ネットワークの影響も取り除いている．

ユーザ数の推移と1日当たりの証明書発行回数を**図4**のグラフに示す．なお，ここで，ユーザ数とは，発行局に登録しているPEMユーザの数を意味している．ユーザ数が小さく減っている時があるのは，証明書の廃止による．

二つの配布局の負荷を**図5**に示す．グラフでは，5種類の検索サービスの合計（配布局1，配布局2）と，ユーザ支援システムによって自動的に行われる検索の回数（自動）を1週間ごとに平均したものについて示している．検索の種類は，ユーザからのキーワード検索の要求がほとんどである．

4. 評　価

評価項目は次の2点である．

1．配布局の運用限界

実験結果から配布局の運用限界を見積もる．

2．証明書キャッシュの効果

FJPEMシステムでは，配布局と証明書キャッシュを併用して証明書を管理している．メールの場合には，通信先がある程度限定されるため，証明書のキャッシングはかなり有効と考えられる．そこで，現実のメールのトラフィックを解析し，そのデータを元に，証明書キャッシュの効果を見積もる．

4.1 配布局の運用限界

前節の実験結果では，配布局の負荷と増加するユーザ数との顕著な相関関係は認められない．これは，実験期間が短くユーザ数も少ないことと，実験参加者が配布局の動作を確認するために行った検索試験が影響しているものと考えられる．しかし，実際の運用では，配布局への検索はユーザ数に比例して増加することが予想される．ただし，配布局は，発行局とは異なりユーザ情報を一元管理する必要もないので，負荷分散により対処することが可能である．しかも，証明書は更新までの周期が十分長い（本実験では2年間）ため，情報の分散による不一致が生じる危険性も低い．現に，本実験でも2台の配布局を運用し，配布局分散の現実性を実証した．

ならば，Internetの全ユーザに対応するには，いくつの配布局が必要だろうか．すなわち，1台の配布局で対応できるユーザの数はどのくらいであるか，見極める必要が生じる．そこで，本節では，実験結果と待ち行列モデルにより配布局の運用限界を考察していく．

まず，表4の配布局平均処理時間より，配布局の平均サービス率は $\mu_w = 1/2.93 = 0.341$ と定まる．ここで，証明書検索要求の到着間隔をランダムとみなし，検索

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）と仮定する．単位時間(秒)内に検索要求が届く確率は十分小さく，かつ，各ユーザで独立に行われるので，ポアソン到着の仮定は妥当である．この時，配布局での平均応答時間 T_w は次式で与えられる（**図6**）．

$$T_w=\frac{1}{\mu_w-\lambda_w}$$

ここで，λ_w は，証明書検索要求の平均到着率である．

例えば，本公開実験中，証明書検索要求が最大の140回となった日の平均到着率は $\lambda_w=140/(60\times60\times24)=0.00162$ となるので，その平均応答時間は $T_w=1/(0.341-0.00162)=2.95$ [sec] である．つまり，本実験程度の負荷ではほとんど待ち行列を生じさせていないことがわかる．では，運用が困難となるほどの利用率はどのくらいであろうか．

平均応答時間が t 秒以下となる確率 $P[T_w\leq t]$ は次式で与えられる[13]．

$$P[T_w\leq t]=1-\rho_w e^{-\mu_w(1-\rho_w)t}$$

ただしここで，ρ_w は $\rho_w=\lambda_w/\mu_w$ で与えられる利用率である．仮に運用上実用的な応答時間の最悪値を60秒と考え，この目標を実現する確率を90%以上にするためには，利用率が $\rho<0.893$ を満たさなくてはならない．これを1日当たりの証明書検索要求に換算すると，

$$0.893\times60\times60\times24\times\mu_w=26309.9,$$

すなわち，1日当たりの証明書検索数が26,000回以内であれば，90%以上の確率で60秒以下の応答時間が保証されることが示された．次に，この利用率を実現するユーザ数を実験データより概算してみる．検索要求数はユーザ数に比例すると仮定すると，ユーザ数126名の時に記録された1日当たりの検索要求数の最大140から，最悪の場合でも $26309.9/140\times126=23678.9$ [人]，平均値を取ると，$26309.9/(25.88+19.41)\times2\times126=146392.2$ [人] となる．結局，単一の配布局が対応できるユーザ数は最悪で約2万人，平均的には約14万人までと言うことができる．ただし，これは配布局のCPUパワーと配布にかかる処理時間だけから算出された値であり，ネットワークの混雑度などは無視している．なぜならば，ネットワークの混雑によりパケットが遅延しても，それはユーザからみた応答時間が変化するだけであり，配布局から見た1日当たりの到着パケット数は変わらないためである．ただし，ユーザ数増加によって証明書キャッシュの効率が悪化する可能性があるので，注意が必要である．

4.2 証明書キャッシュの効果

キャッシュの効果を見積もるため，94年2月24日より1週間，富士通研究所の共用マシンから発信したメールの統計を調べた．約1000人のユーザについての次の2種類の平均値を，**図7**のグラフに表す．

$M(x)=x$ 日間に発信したメールの総数（のべ）

$R(x)=x$ 日間に発信した通信者の総数

ここで，$M(x)$ は1通のメールでも複数人に宛てて

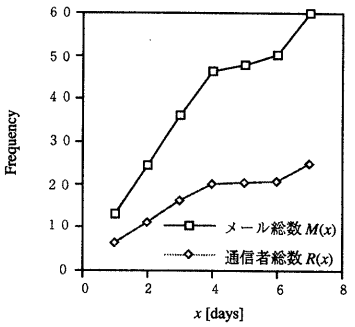


図7 電子メール送信回数
Fig. 7 Frenquency of outgoing emails.

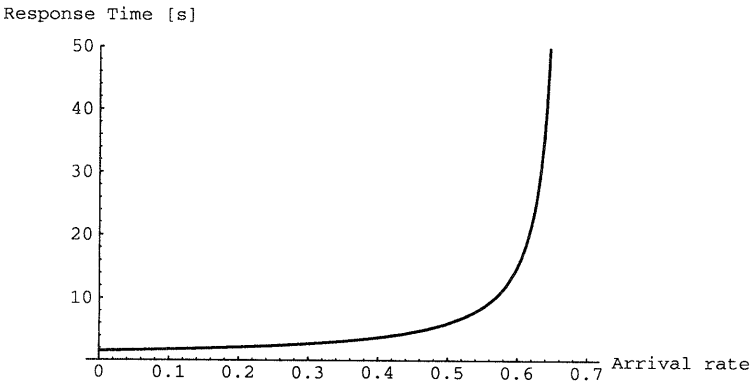


図6 配布局の平均応答時間
Fig. 6 Average responding time of the certification server on number of users.

いる場合は，複数のメールとして数え上げている．逆に，$R(x)$ は，重複を削除している．従って，もしもすべてのメールに PEM を用いたとすると，$M(x)$ の値が x 日間に 1 人が必要とする証明書の平均数を表す．一方，$R(x)$ は証明書がキャッシングされていた場合の必要な証明書の数を表す．x は証明書キャッシュをクリアする間隔のパラメータとなる．

グラフより，メール総数は日数に比例して増加しているが，通信者の数の増加は緩やかである．従って，証明書をキャッシュしておけば，配布局へのアクセスがかなり押えられることがわかる．

これを，具体的に示すために，メールの発信をランダム，配布局での処理時間を負の指数分布に従うもの (M/M/1 モデル) としてシミュレーションを行った．

実測による配布局での平均処理時間 2.93 [s] より，配布局での検索にかかる平均サービス率を $\mu=1/2.93$ とする．n 人のユーザが 1 日当たり必要とする証明書数を c とおくと，配布局への検索要求の平均到着率 λ は，

$$\lambda=\frac{nc}{60\times60\times24}$$

と表せる．c の値は，1000 人の統計値より，**表 5** に従うものと仮定する．すると，配布局での平均応答時間 T は次式で与えられる．

$$T=\frac{1}{\mu-\lambda}$$

この結果を**図 8** に示す．キャッシュがない場合には，一つの配布局で 5,000 人程度までしか運用できないが，7 日分のキャッシュを導入することで，3 倍の 15,000 人のユーザに対応できることが示された．表 5 のデータを見ても，$M(1)=8.53$ に対して $R(7)/7=3.52$ であり，負荷が約 2/5 倍に削減されていることを示している．実際には，証明書が更新されることは稀なので，より長い間隔でキャッシュしていてもよく，配布局への負荷は更に小さくなることが予想される．

表 5 一日に必要とする証明書数 (c)
Table 5 Average numbers of certificates required in a day.

キャッシュなし	$M(1)=8.53$
1 日おきキャッシュをクリア	$R(1)=6.26$
2 日おきキャッシュをクリア	$R(2)/2=5.55$
3 日おきキャッシュをクリア	$R(3)/3=5.30$
4 日おきキャッシュをクリア	$R(4)/4=5.00$
5 日おきキャッシュをクリア	$R(5)/5=4.05$
6 日おきキャッシュをクリア	$R(6)/6=3.41$
7 日おきキャッシュをクリア	$R(7)/7=3.52$

5. おわりに

プライバシ強化メール PEM の運用における証明書を配布する配布局システムを提案し，実装および公開実験を経て，性能評価を行った．その結果，本実装による配布局は 1 台で約 14 万人のユーザにまで，90% の確率で 60 秒以内の応答を得ることが示された．また，ユーザのメール支援システムにおける証明書キャッシュの機能は極めて効果的であり，1 週間分のキャッシュで配布局への証明書検索要求の負荷を約 2/5 に削減できることが明らかになった．

謝辞 本研究を進めるにあたり，WIDE プロジェクトでの議論が大変有益であった．特に，実装上の貴重な御助言を頂いた同セキュリティワーキンググループの奈良先端大学山口英氏，東京大学和田英一氏，富士ゼロックス稲田龍氏，日立ソフトウェア鮫島吉喜氏，同多胡滋氏，NEC 櫻井三子氏，東芝室田真男氏，日本アイビーエム川副博氏，IPA 田中啓介氏，電気通信大学佐久間重雄氏，九州大学山本和彦氏，京都大学中村

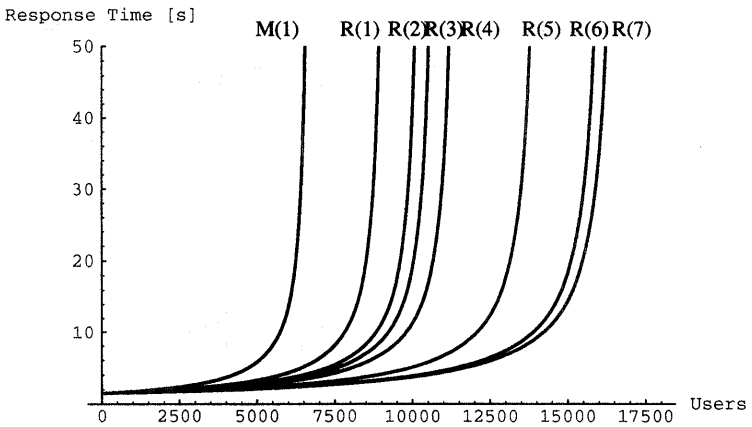


図 8 配布局の応答時間
Fig. 8 Response time for key distribution.

素典氏に感謝します．米国との相互接続に協力していただいた，RSA Data Security 社の Jeff Thompson 氏，Burton S. Kaliski 氏に感謝します．運用試験にあたって御協力頂いた富士通研究所 pem-dev メーリングリストのメンバに感謝します．本研究の機会を与えて下さった，当研究所情報システムセンタ技術部田村寿彦部長，奈良泰弘担当課長に感謝します．

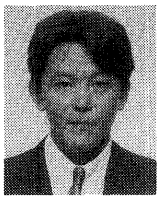
参 考 文 献

1) 曽根，宇野，森井：電子メールシステムでの公開鍵暗号の適用とその一考察，電子通信学会技術研究報告（情報セキュリティ），ISEC 91-44 (1992).
2) 館林，松崎，原田，宮地，多田：暗号化電子メールシステム，第 46 回情報処理学会全国大会論文集，4, pp. 125-126 (1993).
3) 小林，岡本，桜井：親展機能付き電子メールシステム，第 48 回情報処理学会全国大会論文集，7 K-5, pp. 4-299-300 (1994).
4) Linn, J.: Privacy Enhancement for Internet Electronic Mail: Part I—Message Encipherment and Authentication Procedures, *RFC-1421* (1993).
5) Kent, S.: Privacy Enhancement for Internet Electronic Mail: Part II—Certificate-Based Key Management, *RFC-1422* (1993).
6) Balenson, D.: Privacy Enhancement for Internet Electronic Mail: Part III—Algorithms, Modes, and Identifiers, *RFC-1423* (1993).
7) Kaliski, B.: Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services, *RFC-1424* (1993).
8) Rose, M. T.: *The Open Book—A Practical Prespective on OSI,* Prentice-Hall (1989).
9) 菊池，森下：暗号電子メール PEM (Privacy Enhanced Mail) の実装と課題，第 46 回情報処理学会全国大会論文集，1, pp. 99-100 (1993).
10) 菊池，黒田：公証人を用いた暗号メール公開鍵証明書発行方式，第 48 回情報処理学会全国大会論文集，1, pp. 249-250 (1994).
11) Harrenstien, K., Stahl, M. and Feinler, E.: NICNAME/WHOIS, *RFC-954* (1985).
12) Rose, M. T.: *The Simple Book: An Introduction to Management of TCP/IP-based Internets,* Prentice-Hall (1991).
13) Kleinrock, L.: *Queueing Systems Vol. 1,* John Wiley & Sons, New York (1975).
14) Kaliski, B.: The MD2 Message-Digest Algorithm, *RFC-1319* (1992).
15) Rivest, R.: The MD4 Message-Digest Algorithm, *RFC-1320* (1992).
16) Rivest, R.: The MD5 Message-Digest Algorithm, *RFC-1321* (1992).
17) Federal infomation processing standards publication (FIPS PUB) 46-1, "Data encryption standard" (1988).
18) Kent, S.: PEM WG MEETING MINUTES (14-7-93), *NetNews info. pem-dev* (1993).
19) Kent, S.: An Overview of Internet Privacy Enhanced Mail, *Proc. iNET'92,* pp. 217-227 (1992).
20) Kent, S. T.: Internet Privacy Enhanced Mail, *Comm. ACM,* Vol. 36, No. 8, pp. 48-60 (1993).
21) CCITT Recommendation X.509, The Directory Authentication Framework (1988).
22) RSA Data Security, Inc.: *Public-Key Cryptography Standards* (*PKCS*) (1991).
23) Malamud, C.: *STACKS: Interoperability in Today's Computer Networks,* Prentice Hall (1992)（邦訳「インターネット縦横無尽」，後藤滋樹，村上健一郎，野島久雄訳，共立出版）
24) Bertsekas, D. and Gallager, R. G.: *DATA NETWORKS,* Prentice-Hall (1987)（邦訳「データネットワーク」，八星訳，共立出版）

（平成 6 年 9 月 30 日受付）
（平成 7 年 4 月 14 日採録）

菊池 浩明（正会員）

1965 年 4 月 14 日生．1988 年明治大学工学部電気工学科卒業．1990 年同大学大学院修士課程修了．同年（株）富士通研究所入所．1994 年東海大学工学部電気工学科に移籍．現在同大学講師．工学博士．ファジー理論，ネットワークセキュリティの研究に従事．電子情報通信学会，日本ファジー学会各会員．



黒田 康嗣（正会員）

1967 年 1 月 17 日生．1991 年福井大学工学部情報工学科卒業．同年（株）富士通研究所入所．OSI アプリケーション，ネットワークセキュリティの研究に従事．電子情報通信学会会員．

永井 武

1937 年 12 月 13 日生．1961 年早稲田大学第一理工学部卒業．1976 年工学博士．（株）富士通研究所において情報システムセンタ長など歴任．現在新潟国際情報大学に在籍．オープンな情報システムに興味をもつ．著書“世界を結ぶ情報ハイウェイ—インターネット入門（富士通ブックス）”．