5Q-04　PKIにおける失効管理の高速化に関する考察

小俣 三郎、武田 哲、坂上 勉、佐伯 正夫
三菱電機（株） 情報技術総合研究所

1. はじめに

近年、電子商取引などにおいてセキュアな通信を行うために公開鍵暗号技術を用いた電子認証システム（PKI：Public Key Infrastructure）が発展［1］してきている。PKIでは認証機関（CA：Certification Authority）が公開鍵の所有者に対し、鍵の所有を証明する公開鍵認証書を発行する。認証書を発行されたユーザ同士は認証された公開鍵、および対応した秘密鍵とを用いたセキュアな通信が可能になる。

認証書をもつユーザ同士が通信を行なう際相手のデジタル署名を検証する必要があり、その時用いる相手の認証書が（その時点で）有効かどうかを確認しなければならない。

このような認証書の失効管理において、本稿では認証書の有効性の検証にかかる時間を認証書失効リスト（CRL：Certificate Revocation List）に登録されている失効認証書数（エントリ数）に対して実測した。また検証時間の増大を抑えるための手法としてCRL分割についての考察を行った。

2. 失効管理における問題点

一般的な大規模PKIシステムにおいては、発行される認証書数が多く、それに伴って失効される認証書数も多くなると考えられる。この様な状況で認証書の有効性を検証する場合、CRLにある膨大な失効情報の中に検証したい認証書がふくまれているかどうかを確認するために、クライアントがCRLを取り込んで検証対象の認証書のシリアル番号をCRLから単純に検索するのでは時間がかかり、その時の検証処理が問題になる。

3. 認証書検証モデルの一例（CRL分割）

前記のような大規模PKIシステムではCRLのサイズが限りなく増加する可能性があり、サイズを抑えるためにCRLをある一定のサイズ（システムの規模により制御）の複数CRLに分割する手法が提案されている。［1］

CRL分割手法では認証書を失効させる場合、認証書のシリアル番号がCRL配布点（認証書発行時に指定される拡張領域の情報）［2］で一意に関連づけられたCRLへ登録（図1）される。この場合、クライアントが認証書の検証を行なうためにはCRL配布点によって指定されたCRLをダウンロードすればよい。したがってCRL分割を行なわない場合よりもCRL取り込みにかかる通信オーバヘッド、および処理オーバヘッドを軽減することができる。

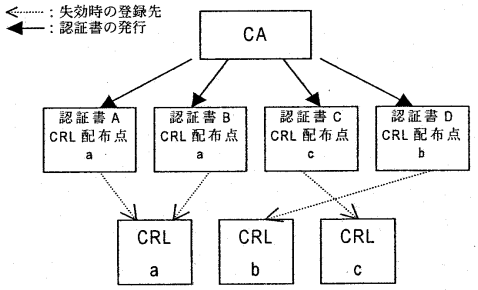

図1 CRL分割の例

4. CRLを用いた認証書検証時間の測定結果

今回、CRLによる認証書の検証においてCRL

A study of revocation management in the PKI
S.Omata,S.Takeda,T.Sakagami,M.Saeki
Information Technology R&D Center
Mitsubishi Electric Corporation

分割が有効となる適当なエントリ数を見積もることを目的として、有効な（CRL に登録されていない）認証書の検証にかかる時間（検証時間が最大）を実測した結果をそれぞれ以下の表１、図２に示す。

CRLエントリ数	検証時間
1	1.0
10	1.8
20	2.5
50	6.7
100	11
200	22
250	28
500	61
1000	170
2000	500
5000	2500
10000	10000

表１ 検証時間の測定値 (エントリ数1の時の時間を1とした)

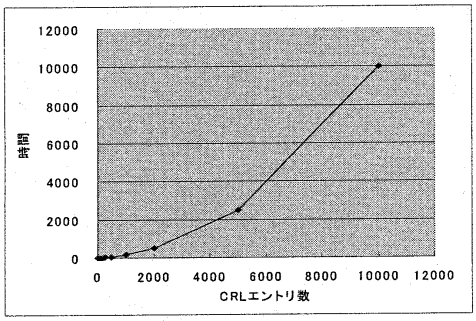

図２ CRL エントリ数と検証時間の関係

検証時間の測定（表１、図２）では、検証したい認証書の発行者と CRL の発行者が一致しているかどうか、認証書が CRL に登録されているかどうかを確認している。その際、認証書の他の項目のチェックや認証書チェーンをルート CA までたどって各上位認証書の署名をチェックするといった処理は行なっていない。

5. 考察

表１の結果から CRL エントリ数に対する検証時間の増加率（隣接する２点の傾きとする）が、エントリ数 500～1000 と 1000～2000 との間で 200％と急激に増加している。したがってこのような検証時間の増加をおさえるためにはそれぞれの PKI システムに要求される範囲内で CRL エントリ数を制限して CRL を分割する手法が有効である。

表１および図２の結果から、検証クライアントが性能劣化で困らないような範囲内で分割するのが適切でありり、エントリ数を 500～1000 くらいにするのがよいだろう。

表１から、例えばエントリ数 10000 の CRL に対してエントリ数を 500 に設定して CRL を分割したとすると、分割をしない場合に比べて分割をした場合の方が検証速度が 160 倍速くなり、エントリ数を 1000 にした場合では、60 倍速くなることが分かる。

6. おわりに

本稿では CRL 分割の概略を紹介し、検証時間を測定することによって認証書の失効管理における CRL 分割の有効性を確認した。

今後は CRL 分割だけでなく他の失効管理技法についても具体的な調査を行ない、当社認証サーバへ適用を検討する予定である。

参考文献

[1] W.Ford,and M.S.Baum 著、山田慎一郎訳、“ディジタル署名と暗号技術”、プレンスティホール（1997）

[2] ITU-T Recommendation X.509(0697) INFORMATION TECHNOLOGY-OPEN SYSTEMS INTERCONNECTION-THE DIRECTORY : AUTHENTICATION FRAMEWORK , 1997