社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2003－ＣＳＥＣ－22　(24)
2003／7／18

PKIでの証明書失効に必要な通信量の確率論的評価

田中 直樹　飯野 陽一郎

ソニー株式会社 〒141-0001 東京都品川区北品川 6-7-35

E-mail: NaokiA.Tanaka@jp.sony.com, Yoichiro.Iino@jp.sony.com

あらまし 公開鍵認証基盤（PKI）では，Certificate Revocation List（CRL）と呼ばれる証明書の失効情報を使って，証明書の失効を確認する方法が提案されている．CRLは証明書をもつentityのグループ単位で複数発行されるが，検証者はそのうちの必要なCRLだけを取得すれば良いこと，及び一度取得したCRLを保存しておくことで，同一のCRLの取得は高々1度で済むことにより，CRL取得に必要な通信量が減ることが期待される．本稿では，PKIでの主な証明書の失効方式である完全CRL方式とδ-CRL方式について，確率論的な取り扱いにより，検証者が同一のCRLの取得を高々1度しか行わない場合の通信量の理論式を導いた．その評価結果から，CRLの発行頻度に比べて認証頻度が充分低い領域を除くと，検証者が必要なCRLだけを取得できることによる通信量を下げる効果は有効ではない事が分かった．また，δ-CRL方式については，認証頻度が充分大きい場合には，通信量を最小化するBaseCRLとδ-CRLの発行間隔の比がCAの数とは無関係に決まることを示す．

キーワード 公開鍵認証基盤，証明書失効，通信量，確率論

Volume of Communications Necessary for Certificate Revocation in PKI Estimated Based on Probability Theory

Naoki TANAKA and Yoichiro IINO

Sony Corporation 6-7-35 Kitashinagawa, Shinagawa-ku, Tokyo, 141-0001 Japan

E-mail: NaokiA.Tanaka@jp.sony.com, Yoichiro.Iino@jp.sony.com

Abstract In Public Key Infrastructure (PKI), it is proposed that a verifier checks a validity of certificate by Certificate Revocation Lists (CRLs). Each CRL includes revocation statuses of certificates for a part of entities. A verifier obtains only a necessary part of CRLs and, by preserving a CRL once obtained, a verifier needs not obtain the same one more than once. Therefore CRL is expected to reduce the volume of communications necessary for certificate revocation. In this paper, for full-CRL and δ-CRL methods, we take into account the fact that one CRL is obtained by one verifier at most once and we derive the volume of communications necessary for certificate revocation based on probability theory. The result shows that, unless the frequency of authentications is sufficiently low compared to that of CRL issuances, the effect that a verifier obtains only a necessary part of CRLs is irrelevant to reduce the volume of communications. Furthermore, for the δ-CRL method, it is proved that there exists an optimal ratio between a frequency of BaseCRL issuances and a frequency of δ-CRL issuances independent of the number of CAs if the frequency of authentications is high enough.

Keyword Public Key Infrastructure, Certificate Revocation, Volume of Communications, Probability Theory

1. はじめに

公開鍵認証基盤（Public Key Infrastructure, PKI）は，公開鍵暗号を利用してentity認証を行う認証基盤である．PKIでは，entityに公開鍵暗号の秘密鍵と証明書を持たせる．この証明書には，entityが持つ秘密鍵に対応した公開鍵，entityのID，証明書番号，有効期限が含まれ，さらに改竄を防ぐために証明書発行者（Certificate Authority, CA）の電子署名が付加されている．認証は，検証者が証明書から公開鍵を得て，それを使ってentityが対応する秘密鍵を持つことを確認する事で行われる．証明書によって，ある秘密鍵の持ち主があるIDのentityであることをCAが保証する．証明書の形式は，例えばX.509[1]で規定されている．

証明書の有効期限内に，entityが秘密鍵を紛失した場合や，漏洩させた場合には，ある秘密鍵の持ち主があるIDのentityであることが成立しなくなるので，証明書の失効を行う必要がある．CAは，その場合には，失効された証明書の証明書番号を検証者に通知する．以下では1つないし複数の失効された証明書の証明書番号を失効情報と呼ぶ．失効情報を通知する最も簡単な方法は，証明書が失効されると同時に，その失効情報を検証者全員に通知する方法である．しかし，この

方法には以下の大きく2つの問題がある．

問題1．検証者は認証することのないentityの証明書の失効情報まで受け取ることになる．

問題2．証明書失効の発生は予測不可能なので，検証者は常時失効情報を受け取れるようにすることが必要になる．

これらの問題に対して，検証者が認証で必要になった時に必要な失効情報を取得する方法が提案されている．それを，ここでは便宜上，オンライン型，オフライン型の2つに分けて説明する．

オンライン型では，失効情報は専用のサーバーで管理されていて，検証者はentityの認証時に，その証明書の失効を，サーバーに問い合わせて確認する．この場合，entityの認証が常にentity，検証者，サーバーの3者間の処理になるため，認証の応答性や，可用性の確保が困難になる．本稿では以降，この方法は取り扱わない．オンライン型にはOnline Certificate Status Protocol（OCSP）[3][4]，Naorらの方式[6]，Certificate Revocation System（CRS）[7]などがある．

これに対してオフライン型では，失効情報は失効されかつ有効期限前である証明書の番号のリスト，Certificate Revocation List（CRL）としてCAから発行され，検証者がアクセス可能なRepositoryと呼ばれるサーバーで公開される．検証者は一度取得したCRLを保持しておくと，次に新たなCRLが発行されるまでは，保持しているCRLを使って証明書の失効を確認できるので，entityの認証をentityと検証者の2者間で処理できる．CRLの詳細は，例えばX.509[1]やRFC3280[2]で規定されている．CRLの代表的な運用方式としては，完全CRL方式，δ-CRL方式がある．

完全CRL方式 CRLに失効情報として，CRLの発行時点で，失効されていてかつ有効期限内である全ての証明書の番号を含める方式である．このようなCRLを，以下では完全CRLと呼ぶ．この場合，完全CRLの発行間隔が短くなると，新旧の完全CRL間の差分が小さくなり，このようなCRLを発行のたびに取得するのは効率的ではないという問題がある．

δ-CRL方式 比較的長い時間間隔で，BaseCRLと呼ばれる完全CRLと同じ情報を含むCRLを発行し，BaseCRLの発行の間では，δ-CRLと呼ばれるBaseCRLより短い発行間隔のCRLを発行する方式である．δ-CRLにはあるBaseCRLの発行以降に，新たに失効されかつ有効期限前である証明書の番号だけが含まれる．これによって，発行間隔が短くなった場合の完全CRL方式の問題を緩和している．

PKI運用に必要なシステム全体の通信量について考える．CRLのサイズは，おおよそ失効された証明書の数，即ちentity数と証明書の失効頻度の積，に比例する．CRLは認証頻度が高ければ全ての検証者が取得するので，最悪の場合，CRL取得に必要な通信量は，entity数と検証者数と証明書の失効頻度の積に比例する．これに対して，認証自体に必要な通信量は，entity数とentityの認証頻度の積に比例する．このため，特にentityが検証者を兼ねる場合のように，entity数と検証者数が同等であるなら，CRL取得に必要な通信量は，entity数の2次に比例するのに対して，認証自体に必要な通信量はentity数の1次に比例する．つまり，CRL取得に必要な通信量の方が，認証自体に必要な通信量よりもスケーラビリティが悪く，PKIの大規模な運用では問題になりやすい．我々は，この点に注目し，本稿ではCRL取得に必要な通信量の見積もりを行う．

National Institute of Standards and Technology（NIST）によるPKIの運用に必要な通信量の見積もり[5]では，検証者がentityを認証する際に，一定の割合でCRLを取得すると仮定して，通信量を見積もっている．しかし，この方法では，同一のCAに属するentityを複数回認証する場合に，同一のCRLを複数回取得することになり，同一のCRLの取得は高々1回で済むという事を取り入れることができなかった．本稿では，entityが一定の確率で認証されるという仮定のもとに，ある検証者は，同一のCRLを高々1回しか取得しない場合の通信量の理論式を確率論的に導く．それに基づいて，完全CRL方式，δ-CRL方式でのCRL取得に必要な通信量の評価を行う．

全体の構成は次の通りである．始めに本稿での評価モデルと評価項目，即ち完全CRL方式，δ-CRL方式でのCRL取得に必要な通信量を定義する．次に，評価項目の理論式の確率論的な導出の説明を行う．理論式の評価と考察を行い，最後に本稿での結果をまとめる．

2. 評価モデルと評価項目

2.1 評価モデル

評価モデルを図1に示す．複数の証明書発行者（CA）と，各CAに付随する形でRepositoryが存在し，CAから証明書を発行されたentityが複数存在する構成である．それぞれのCAには，一定の数のentityが属し，entityの証明書の失効情報は，各entityが属するCAが管理する．CAは，失効情報をCRLとして発行してRepositoryに置く．改竄を防ぐためにCRLにはCAの電子署名が付加される．従って，CRLの正当性を検証するためにはCAの公開鍵が必要になる．CAの公開鍵とCAの関係も，証明書によって保証するために，CAが階層構造を構成し，上位のCAが下位のCAに対して証明書を発行すると仮定する．但し，CAは通常のentityよりも秘密鍵の管理を厳重に行っていると考えられるので，ここでは，CAの証明書の失効は起こら

ない，あるいはentityの証明書の失効に比べて充分に低い頻度でしか発生しないと仮定する．この仮定により，CAが階層構造を構成する場合であっても，CAの証明書の失効確認に必要な上位のCAが発行したCRLの取得で発生する通信量は，entityの証明書の失効確認に必要なCRLの取得で発生する通信量に比べて無視できる．従って，CRLの取得に必要な通信量を考える上では，図1のように，CAが階層構造を構成しないモデルで評価を行うことができる．

証明書は，認証を行うentity（以下では，検証者と呼ぶ）が認証を行うたびに，認証されるentity（以下では，単にentityと呼ぶ）から送られる．entityの証明書から証明書を発行したCA，及び対応するCRLの置かれているRepositoryを特定できるので，検証者はRepositoryから直接CRLを取得できるものとする．検証者はCRLを用いて証明書が失効されていないことを確認した後，entityが対応する秘密鍵を持つことを確認することで，entityを認証する．

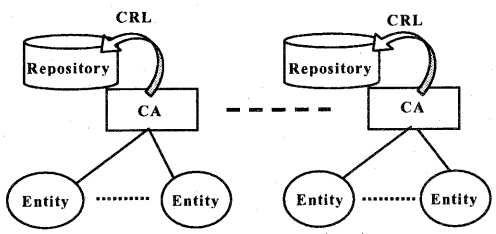

図1　評価モデルの概要

2.2 通信量

ここでは，完全CRL方式とδ-CRL方式での，CRL取得に必要な通信量を定義する．

完全CRL方式でのCRL取得に必要な通信量

システム全体で全検証者が全Repositoryから取得する全ての完全CRLのサイズの総和を，単位時間（1日）あたりで平均した値（ビット数）とする．

δ-CRL方式でのCRL取得に必要な通信量

システム全体で全検証者が全Repositoryから取得する全てのBaseCRLとδ-CRLのサイズの総和を，単位時間（1日）あたりで平均した値（ビット数）とする．

3.理論式の導出

ここでは§2.2で定義した通信量の理論式を導出する．始めに導出に必要なパラメータの定義と，必要な仮定を示す．次に導出方法を説明する．以降ではCRLに含まれる失効された証明書1つあたりの情報（1つの失効した証明書の番号）を項目と呼ぶ．

3.1 パラメータの定義

評価に必要なパラメータを以下に定義する．

p：1つの証明書が1日に失効される平均回数（失効発生頻度）［回/day］

N：entity数［個］

k：CAの個数［個］

q：1 entityが，1日に認証される平均回数（認証頻度）［回/day・個］

T_C：完全CRL方式での完全CRL，及び，δ-CRL方式でのδ-CRLの発行間隔［day］

T_B：δ-CRL方式のBaseCRLの発行間隔［day］

L：証明書の有効期限［day］

l_{sn}：CRLの項目1つあたりのビット数［bit］

l_{sig}：CRLの項目数によらない要素（CAの電子署名や，発効日など）のビット数［bit］

3.2 仮定

理論式を導く上で必要な仮定を以下に示す．

1. 証明書の失効は，失効発生頻度pのPoisson過程に従って発生する．
2. 認証は，認証頻度qのPoisson過程に従って発生する．
3. 各entityは有効な証明書を1つだけ持ち，証明書が失効すると，すぐに代わりの証明書を取得する．
4. 全てのentityは同等に認証を行う（検証者となる）．
5. 証明書有効期限Lは全ての証明書で同一とする．
6. 証明書の有効期限切れは時間的に一様に発生する．
7. 完全CRL方式での完全CRL，δ-CRL方式でのδ-CRLは発行間隔T_cで定期的に発行される．
8. δ-CRL方式でのBaseCRLは発行間隔T_Bで定期的に発行される．
9. BaseCRLの発行間隔T_Bは，δ-CRLの発行間隔T_cの整数倍である．
10. 各CAには，同数（N/k）ずつのentityが属する．

3.3 導出のポイント

完全CRL方式，δ-CRL方式の通信量の理論式を導出する上でのポイントを説明する．

3.3.1 定常状態での完全CRL，BaseCRLの項目数

完全CRL，δ-CRL方式のBaseCRLの項目数は，無限に大きくなるのではなく，ある時間経過後には，ある一定の数で定常状態になると考えられる．なぜならば，仮定1から，CRLには常に一定数の証明書番号が新たに加わり，仮定6からCRLに含まれる証明書番号のうちの一定数が有効期限切れでCRLから抜けるので，両者がバランスして一定になるからである．

図2を参照しながら，定常状態の項目数を導出する．

定常状態の CRL の項目数を $N_{stable}(N,L,p,k)$ とする．1 つの CA について，1 日に失効される証明書数は Np/k なので，1 日に $N_{stable}(N,L,p,k)$ に追加される項目数は Np/k である．また，有効期限が切れるために 1 日に $N_{stable}(N,L,p,k)$ から除外される項目数は，$N_{stable}(N,L,p,k)/L$ である．定常状態では $N_{stable}(N,L,p,k)$ は変化しないので，新たに加わる項目数と除外される項目数は等しい．

$$Np/k = N_{stable}(N,L,p,k)/L \quad (1)$$

(1) を $N_{stable}(N,L,p,k)$ について解くと，定常状態の CRL の項目数は，以下で与えられる．

$$N_{stable}(N,L,p,k) = NpL/k \quad (2)$$

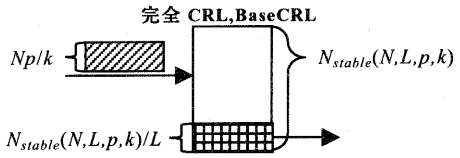

図 2 定常状態の完全 CRL，BaseCRL の項目数

3.3.2 BaseCRL の発行から n 番目の δ-CRL の項目数

δ-CRL には，ある BaseCRL の発行時点以降に，新たに失効されかつ有効期限前である証明書の番号が含まれる．BaseCRL の発行以降に，n 番目に発行された δ-CRL の項目数を P_n とする．1 つの CA について δ-CRL の発行間隔 T_C の間に新たに失効される証明書の数は NpT_C/k である．また，P_n 個の項目のうち，T_C の間に P_nT_C/L 個は有効期限切れで δ-CRL に含まれる必要はなくなる．従って，図 3 に示すように，n+1 番目の項目数 P_{n+1} は，P_n に，NpT_C/k を加え，$P_n \cdot T_C/L$ を削除したものとなり，以下の関係式が成り立つ．

$$P_{n+1} = P_n + NpT_C/k - P_n \cdot T_C/L \quad (3)$$

初項 $P_0 = 0$ として(3)を解くと，一般項 P_n は以下の式で与えられる．但し，n の範囲は $0 \leqq n \leqq T_B/T_C - 1$ である．

$$P_n = \frac{NpL}{k}\left\{1-\left(1-\frac{T_C}{L}\right)^n\right\} \quad (4)$$

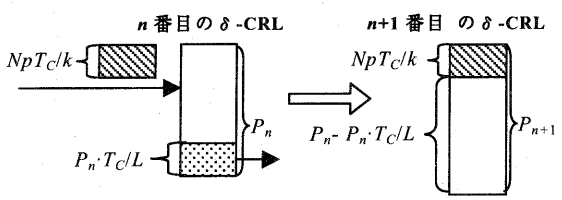

図 3 n, n+1 番目の δ-CRL の項目数

3.3.3 検証者がある時間間隔にある CA に属する entity を 1 回以上認証する確率

完全 CRL 方式，δ-CRL 方式のいずれの場合も，検証者は CRL が発行された後に初めてある CA に属する entity を認証する時だけ，その CA の発行した CRL を取得すればよい．その後は，CRL が再度発行されるまで同一の CRL を再取得する必要はない．従って，ある検証者がある CRL を取得する確率は，その CRL を発行した CA に属する entity を CRL の発行間隔の間に 1 回以上認証する確率に等しい．

仮定 2 より認証頻度は q であり，また 1 つの CA に属する entity 数は N/k なので，1 つの CA に属する entity を認証する回数の期待値は Nq/k 回となる．時間間隔 T［日］の間に，ある検証者がある CA に属する entity を認証する回数の期待値は，検証者数が N なので，qT/k 回になる．一般に，ある時間間隔に平均 λ 回発生する事象の発生回数 X の確率分布は，Poisson 分布 $P(X)=\lambda^X \cdot e^{-\lambda}/X!$ に従う事が知られている．従って，ある検証者が，ある CA に属する entity を認証する回数は，$\lambda = qT/k$ とした Poisson 分布に従うと考えられる．このことから，ある検証者が，T の間に，1 回以上ある CA に属する entity を認証する確率 $P(X \geqq 1)$は，$P(X)$ の X が 1 から∞までの和として，以下で与えられる．

$$P(X \geq 1) = \sum_{X=1}^{\infty} P(X) = 1 - P(0) = 1 - e^{-\frac{qT}{k}} \quad (5)$$

3.4 通信量の理論式の導出

以降では，§2.2 で定義した完全 CRL 方式での CRL 取得に必要な通信量を L_{CRL}，δ-CRL 方式の CRL 取得に必要な通信量を $L_{deltCRL}$ と表す．

3.4.1 完全 CRL 方式での CRL 取得に必要な通信量 L_{CRL} の導出

完全 CRL 方式では，1 つの CA が 1 回に発行する CRL のサイズ l_{CRL} は，(2)の CRL の項目数と CRL の項目 1 つあたりのビット数 l_{sn} の積，及び項目数によらない要素のビット数 l_{sig} の和であり，以下で与えられる．

$$l_{CRL} = N_{stable}(N,L,p,k) \cdot l_{sn} + l_{sig} \quad (6)$$

発行間隔 T_C の間に，検証者がある CA に属する entity を 1 回以上認証する時に，その CA の発行した CRL を取得する必要がある．従って，L_{CRL} は(5)で $T = T_C$ とした確率で l_{CRL} を全 CA 数，全検証者数について和をとってから時間平均することにより，以下の式で与えられる．

$$L_{CRL} = k \cdot N \cdot P(X \geq 1)\Big|_{T=T_C} \cdot l_{CRL} \cdot \frac{1}{T_C}$$

$$= \frac{1}{T_C}\left(NpL \cdot l_{sn} + k \cdot l_{sig}\right) \cdot N \cdot \left(1 - e^{-\frac{qT_C}{k}}\right) \quad (7)$$

3.4.2 δ-CRL 方式での CRL 取得に必要な通信量 $L_{deltaCRL}$ の導出

δ-CRL 方式では，BaseCRL 取得に必要な通信量とδ-CRL 取得に必要な通信量を考慮する必要がある．前者を $L_{BaseCRL}$，後者を L_{delta} と表すことにする．即ち次式が成立する．

$$L_{deltaCRL} = L_{BaseCRL} + L_{delta} \quad (8)$$

1 つの CA が 1 回に発行する BaseCRL のサイズ $l_{BaseCRL}$ は，(6)と同様に，以下で与えられる

$$l_{BaseCRL} = N_{stable}(N, L, p, k) \cdot l_{sn} + l_{sig} \quad (9)$$

BaseCRL の発行間隔 T_B の間に，検証者がある CA に属する entity を 1 回以上認証する時に，その CA の発行した BaseCRL を取得する必要がある．従って，$L_{BaseCRL}$ は，(7)と同様に，(5)で $T = T_B$ とした確率で $l_{BaseCRL}$ を全 CA，全検証者について和をとってから時間平均したものであり，以下の式で与えられる．

$$L_{BaseCRL} = k \cdot N \cdot P(X \geq 1)\Big|_{T=T_B} \cdot l_{BaseCRL} \cdot \frac{1}{T_B} = \frac{1}{T_B}(NpL \cdot l_{sn} + k \cdot l_{sig}) \cdot N \cdot \left(1 - e^{-\frac{qT_B}{k}}\right) \quad (10)$$

最新の BaseCRL の発行以降に，n 番目に発行されたδ-CRL のサイズ $l_{delta}(n)$は，(4)のδ-CRL の項目数 P_n と CRL の項目 1 つあたりのビット数 l_{sn} の積，及び項目数によらない要素のビット数 l_{sig} の和であり，以下の式で与えられる．

$$l_{delta}(n) = P_n \cdot l_{sn} + l_{sig} \quad (11)$$

δ-CRL の発行間隔 T_C の間に，検証者がある CA に属する entity を 1 回以上認証する場合だけ，その CA の発行したδ-CRL を取得する必要がある．従って，L_{delta} は，(5)で $T = T_C$ とした確率で $l_{delta}(n)$を全 CA，全検証者について和をとってから時間平均（$0 \leqq n \leqq T_B / T_C - 1$ で整数 n について和をとり，T_B で割る）したものであり，以下の式で与えられる．

$$L_{delta} = k \cdot N \cdot P(X \geq 1)\Big|_{T=T_C} \cdot \sum_{n=1}^{\frac{T_B}{T_C}-1} l_{delta}(n) \cdot \frac{1}{T_B} = \frac{1}{T_B}\sum_{n=1}^{\frac{T_B}{T_C}-1}\left[\frac{NpL}{k}\left\{1-\left(1-\frac{T_C}{L}\right)^n\right\} \cdot l_{sn} + l_{sig}\right] \cdot k \cdot N \cdot \left(1 - e^{-\frac{qT_C}{k}}\right) \quad (12)$$

従って，(8)により $L_{deltaCRL}$ は以下の式で表される．

$$L_{deltaCRL} = \frac{1}{T_B}(NpL \cdot l_{sn} + k \cdot l_{sig}) \cdot N \cdot \left(1 - e^{-\frac{qT_B}{k}}\right) + \frac{1}{T_B}\sum_{n=1}^{\frac{T_B}{T_C}-1}\left[NpL\left\{1-\left(1-\frac{T_C}{L}\right)^n\right\} \cdot l_{sn} + k \cdot l_{sig}\right] \cdot N \cdot \left(1 - e^{-\frac{qT_C}{k}}\right) = \frac{N}{T_B} \cdot A \cdot \left(1 - e^{-\frac{qT_B}{k}}\right) + \frac{N}{T_B}\sum_{n=1}^{\frac{T_B}{T_C}-1} F(n) \cdot \left(1 - e^{-\frac{qT_C}{k}}\right) \quad (13)$$

但し，$A = NpL \cdot l_{sn} + k \cdot l_{sig}$，$F(n) = NpL\{1-(1-T_C/L)^n\} \cdot l_{sn} + k \cdot l_{sig}$ とした．

4.完全 CRL 方式，δ-CRL 方式の評価

導出した理論式から，完全 CRL 方式，δ-CRL 方式での CRL 取得に必要な通信量の評価と考察をまとめる．

4.1 パラメータ

評価で用いたパラメータを以下に示す．

- ■entity 数 $N = 3000000$［個］
- ■失効発生頻度 $p = 0.1/365$［回/day］
- ■証明書の有効期限 $L = 365$［day］
- ■完全 CRL，δ-CRL の発行間隔 $T_C = 1$［day］
- ■CRL の項目 1 つあたりのビット数 $l_{sn} = 72$ ［bit］
- ■CRL の項目数によらず一定な要素のビット数［bit］ $l_{sig} = 728$［bit］

$N, p, L, T_C, l_{sn}, l_{sig}$ は，[5]と同一の値を用いた．

4.2 完全 CRL 方式の評価と考察

図 4 は，認証頻度 q，CA の個数 k を変化させた時の完全 CRL 方式での CRL 取得に必要な通信量 L_{CRL} を示す．

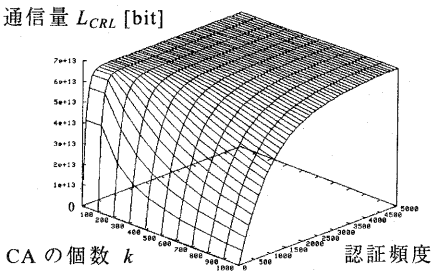

図 4　完全 CRL 方式での CRL 取得に必要な通信量

図から L_{CRL} は，q の小さい領域での q への依存性の大きい振る舞いと，q の大きい領域での q への依存性の小さい振る舞いの 2 つからなることが予想される．実際，q の小さい極限では $qT_C/k \ll 1$ であるので，(7)の L_{CRL} で $e^{-\frac{qT_C}{k}} \cong 1 - qT_C/k$ とした時の近似式 L_{CRL1} は，以下の式で与えられる．

$$L_{CRL1} = \frac{N}{k}(NpL \cdot l_{sn} + k \cdot l_{sig}) \cdot q \quad (14)$$

同様に，q の大きい極限では $qT_C/k \gg 1$ であるので，(7)の L_{CRL} で $e^{-\frac{qT_C}{k}} \cong 0$ とした時の近似式 L_{CRL2} は，以下の式で与えられる．

$$L_{CRL2} = \frac{N}{T_C}(NpL \cdot l_{sn} + k \cdot l_{sig}) \quad (15)$$

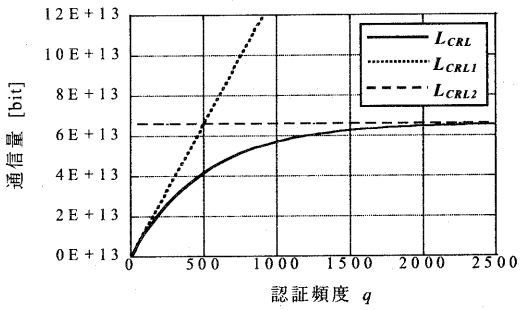

図 5　認証頻度に対する L_{CRL}, L_{CRL1}, L_{CRL2} の比較

図 5 は，CA の個数 $k = 500$ に固定して，q を変化させた時の L_{CRL}, L_{CRL1}, L_{CRL2} を示したものである．L_{CRL1} が q の 1 次に比例しているのは，q が充分小さく同一の CA に属する entity を複数回認証する確率が小さいので，検証者が entity を認証するたびに CRL を Repository から取得することを表している．また，L_{CRL2} は q を含まず，q に非依存である．これは，q が充分大きい場合，検証者は全ての CA に属する entity をほぼ確実に 1 回以上認証することになり，全ての CA で発行される全ての CRL を取得することを表している．

このように L_{CRL} は，q の小さい極限での q の 1 次に比例する漸近的な振る舞いと，q の大きい極限での q に依存しない漸近的な振る舞いの 2 つからなる．そして，それぞれの振る舞いが支配的な領域は，おおよそ L_{CRL1} と L_{CRL2} の値が等しくなる認証頻度 q で切り替わる．(14), (15)より，$L_{CRL1} = L_{CRL2}$ として，q について解くと，以下の関係式が得られる．

$$q = \frac{k}{T_C} \tag{16}$$

このことは，認証頻度 q と CRL の発行頻度 k / T_C がほぼ等しい時に切り替えが起こることを示している．

図 6 は CA の個数 k と認証頻度 q の平面が，L_{CRL1} と L_{CRL2} のそれぞれの振る舞いの支配的な 2 つの領域に，式(16)によって分割されることを示したものである．図 6 の領域 1（$q < k/T_C$）では L_{CRL1} の振る舞いが支配的である．この領域では，CRL の発行頻度に対して認証頻度の方が小さく，検証者は全ての CA の発行した CRL を取得しなくて済むので，CRL を CA 毎に発行して，検証者がそのうち必要なものだけを取得できるようにすることが，CRL 取得に必要な通信量を下げるために有効に働いている．一方，領域 2（$q > k/T_C$）では L_{CRL2} の振る舞いが支配的である．この領域では，CRL の発行頻度に対して認証頻度の方が大きく，全ての CA に属する entity を 1 回以上認証するため，検証者は全ての CA の発行した CRL を取得する．従って，この領域では，CRL を CA 毎に発行して，検証者がそのうちの必要なものだけを取得できることは，CRL 取得に必要な通信量を下げるために有効に働いているとはいえない．特に式(15)からわかるように，領域 2 では CRL 取得に必要な通信量は entity 数の 2 次に比例する．

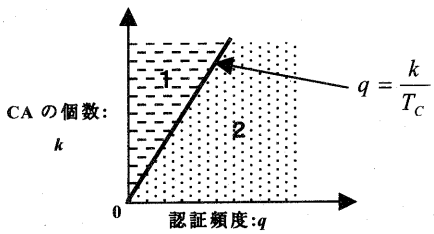

図 6　完全 CRL 方式の CRL 取得に必要な通信量の 2 つの振る舞いのそれぞれが支配的な領域

4.3 δ-CRL 方式の評価と考察

完全 CRL 方式と同様に，δ-CRL 方式での CRL 取得に必要な通信量 $L_{deltaCRL}$ は，認証頻度 q の小さい極限での q に依存する振る舞いと，q の大きい極限での q に依存しない振る舞いの 2 つからなる．実際に，q の小さい極限では $qT_C/k \ll 1$, $qT_B/k \ll 1$ であるので，(13) の $L_{deltaCRL}$ で $e^{-\frac{qT_C}{k}} \cong 1 - qT_C/k$, $e^{-\frac{qT_B}{k}} \cong 1 - qT_B/k$ とした時の近似式 $L_{deltaCRL1}$ は，以下で与えられる．

$$L_{deltaCRL1} = \frac{N \cdot q}{k}\left\{A + \frac{T_C}{T_B}\sum_{n=1}^{\frac{T_B}{T_C}-1} F(n)\right\} \tag{17}$$

同様に，q の大きい極限では $qT_C/k \gg 1$, $qT_B/k \gg 1$ であるので，(13)の $L_{deltaCRL}$ で $e^{-\frac{qT_C}{k}} \cong 0$, $e^{-\frac{qT_B}{k}} \cong 0$ とした時の近似式 $L_{deltaCRL2}$ は以下の式で与えられる．

$$L_{deltaCRL2} = \frac{N}{T_B}\left\{A + \sum_{n=1}^{\frac{T_B}{T_C}-1} F(n)\right\} \tag{18}$$

従って，(17), (18)から $L_{deltaCRL}$ は q の小さい極限での q の 1 次に比例する漸近的な振る舞いと，q の大きい極限での q に依存しない漸近的な振る舞いの 2 つからなる．また，それぞれの振る舞いが支配的な領域は，おおよそ $L_{deltaCRL1}$ と $L_{deltaCRL2}$ が等しくなる認証頻度 q で切り替わる．

$L_{deltaCRL1} = L_{deltaCRL2}$ として，$\Sigma F(n)/A = x$ とすると，次式が得られる．

$$q = \frac{k}{T_B} \cdot \frac{1 + x}{1 + \frac{T_C}{T_B}x} \tag{19}$$

$x \geqq 0$, $0 < T_C/T_B \leqq 1$ なので，$T_C/T_B \leqq (1+x \cdot T_C/T_B)/(1+x) \leqq 1$

である．従って，式(19)の q について

$$\frac{k}{T_B} \le q \le \frac{k}{T_C} \qquad (20)$$

が成立する．このことから，δ-CRL 方式の場合は，q の 1 次に比例する $L_{deltaCRL1}$ の振る舞いが支配的な領域は，完全 CRL 方式の場合よりもさらに認証頻度の低い領域に限られることがわかる．

図 7 は，認証頻度 q と CA の個数 k の値の組(k,q)を，例として(100,100), (80,30), (50,10)にした時の BaseCRL の発行間隔 T_B と CRL 取得に必要な通信量 $L_{deltaCRL}$ の関係を示している．いずれの場合も，$L_{deltaCRL}$ は T_B の増加に伴い減少し，その後再び増加しているので，$L_{deltaCRL}$ が最小になる最適な BaseCRL の発行間隔が存在する．従って，δ-CRL 方式では任意の k と q の値で $L_{deltaCRL}$ が最小になる最適な BaseCRL の発行間隔 T_B^* が存在することが予想される．

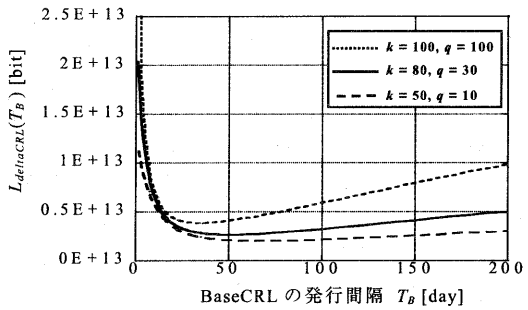

図 7　BaseCRL の発行間隔と δ-CRL 方式の通信量の関係

仮定 9 より T_B は T_C の整数倍であるが，最初にこの条件を無視する．(13)の $L_{deltaCRL}$ で $F(n)$についての和と T_B についての偏微分を解析的に計算して，$L_{deltaCRL}$ を最小にする $T_B = T_B^{\#}$ を，$\partial L_{deltaCRL}/\partial T_B = 0$ を満たす T_B として求める．但し，この方程式を解くために，Newton-Raphson 法による数値計算を用いた．図 8 に k が 1,50,100,500 の場合に，$T_B^{\#}$ と q の関係を示す．図より q が充分大きい場合は，$T_B^{\#}$ は k の値とは無関係にある一定の値（図 8 では，27.7 日）に収束することが確認できる．従って，δ-CRL 方式では，q が充分大きい場合には，k とは無関係に T_B^* が存在すると予想される．

次に，δ-CRL 方式では q が充分大きい場合は k とは無関係に T_B^* が存在することを証明する．BaseCRL の発行間隔 $T_B = T$ の時の δ-CRL 方式での CRL 取得に必要な通信量を $L_{dletaCRL}|_{T_B=T}$ と表す．BaseCRL の発行間隔が最適である時，即ち $T_B = T_B^*$ の時，以下の不等

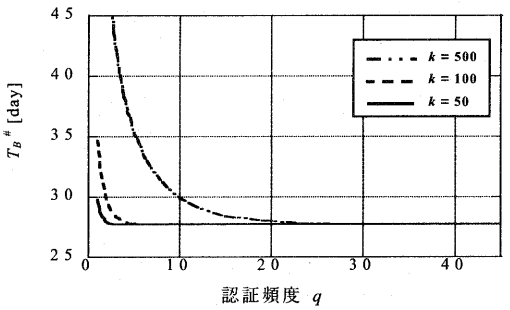

図 8　認証頻度と最適な BaseCRL の発行間隔（L=365，T_C=1）の関係

式が成り立つ．

$$L_{deltaCRL}\Big|_{T_B=T_B^*} - L_{deltaCRL}\Big|_{T_B=T_B^*+T_C} < 0 \qquad (21)$$

$$L_{deltaCRL}\Big|_{T_B=T_B^*} - L_{deltaCRL}\Big|_{T_B=T_B^*-T_C} < 0 \qquad (22)$$

(21)，(22)の左辺は，以下で与えられる．

$$\frac{N}{T_B^*+T_C}\left\{\frac{T_C}{T_B^*}\cdot A\cdot\left(1-e^{-\frac{qT_B^*}{k}}\right)+\frac{1}{T_B^*}\sum_{n=1}^{\frac{T_B^*}{T_C}-1}F(n)\cdot\left(1-e^{-\frac{qT_C}{k}}\right)\right.$$
$$\left.+A\cdot\left(-e^{-\frac{qT_B^*}{k}}+e^{-\frac{q(T_B^*+T_C)}{k}}\right)-F\left(\frac{T_B^*}{T_C}\right)\cdot\left(1-e^{-\frac{qT_C}{k}}\right)\right\} \qquad (23)$$

$$\frac{N}{T_B^*-T_C}\left\{\frac{T_C}{T_B^*}\cdot A\cdot\left(1-e^{-\frac{qT_B^*}{k}}\right)+\frac{1}{T_B^*}\sum_{n=1}^{\frac{T_B^*}{T_C}-1}F(n)\cdot\left(1-e^{-\frac{qT_C}{k}}\right)\right.$$
$$\left.+A\cdot\left(-e^{-\frac{qT_B^*}{k}}+e^{-\frac{q(T_B^*-T_C)}{k}}\right)-F\left(\frac{T_B^*}{T_C}-1\right)\cdot\left(1-e^{-\frac{qT_C}{k}}\right)\right\} \qquad (24)$$

(23)，(24)を，$e^{-\alpha\frac{qT_C}{k}}$（$\alpha$：定数）に依存する項と，依存しない項に分けると，以下の式が得られる．

$$\frac{N}{T_B^*+T_C}\left\{\frac{T_C}{T_B^*}\left\{A+\sum_{n=1}^{\frac{T_B^*}{T_C}-1}F(n)\right\}-F\left(\frac{T_B^*}{T_C}\right)+O\left(e^{-\alpha\frac{qT_C}{k}}\right)\right\} \qquad (25)$$

$$\frac{N}{T_B^*-T_C}\left\{\frac{T_C}{T_B^*}\left\{A+\sum_{n=1}^{\frac{T_B^*}{T_C}-1}F(n)\right\}-F\left(\frac{T_B^*}{T_C}-1\right)+O\left(e^{-\alpha\frac{qT_C}{k}}\right)\right\} \qquad (26)$$

(25)，(26)で，q を充分大きくすると，$O(e^{-\alpha\frac{qT_C}{k}}) \equiv 0$ となるので，(21)，(22)は各項に共通な $NpL\cdot l_{sn}$ を取り除くと以下で与えられる．

$$\frac{T_C}{T_B^*}+\frac{T_C}{T_B^*}\sum_{n=1}^{\frac{T_B^*}{T_C}-1}\left\{1-\left(1-\frac{T_C}{L}\right)^n\right\}-\left\{1-\left(1-\frac{T_C}{L}\right)^{\frac{T_B^*}{T_C}}\right\}<0 \quad (27)$$

$$\frac{T_C}{T_B^*}+\frac{T_C}{T_B^*}\sum_{n=1}^{\frac{T_B^*}{T_C}-1}\left\{1-\left(1-\frac{T_C}{L}\right)^n\right\}-\left\{1-\left(1-\frac{T_C}{L}\right)^{\frac{T_B^*}{T_C}-1}\right\}<0 \quad (28)$$

(27), (28)は，T_B^*/T_C と L/T_C を変数とする関数についての不等式 $f_1(T_B^*/T_C, L/T_C)<0$ と $f_2(T_B^*/T_C, L/T_C)<0$ の形式である．このことと T_B^* が T_C の整数倍であるという仮定から，(27)(28)を同時に満たす T_B^*/T_C は一意に定まるので，ある1変数の関数 f により $T_B^*/T_C = f(L/T_C)$ の形式に表される．つまり，q が充分大きい場合は，T_B^*/T_C は L/T_C によって一意に定まり，かつ CA の個数に無関係である．

図9は，§4.1 のパラメータを用いて，BaseCRL の発行間隔を図8での最適な発行間隔から T_B^*= 28 [day] にした場合に，δ-CRL 方式での CRL 取得に必要な通信量 $L_{deltaCRL}$ を示したものである．本来ならば，T_B^* は，任意の q, k に対して定まる値であるが，実際のシステムでは，検証者が認証を行う頻度，即ち q は予測不可能なのでシステム側で決めることは難しい．従って，q が充分大きい場合に $L_{deltaCRL}$ を最小化する T_B^* をとることが適当である．これを以下では最適化されたδ-CRL 方式と呼ぶことにする．

図9から，完全 CRL 方式と最適化されたδ-CRL 方式では，CRL 取得に必要な通信量に差があることがわかる．認証頻度が充分大きく，CRL 取得に必要な通信量が認証頻度 q に依存しない領域（完全 CRL 方式では式(15)，δ-CRL 方式では式(18)で表される領域）では，例えば，認証頻度 q = 5000，CA の個数 k = 1000 の場合，最適化されたδ-CRL 方式での通信量は完全 CRL での通信量のおよそ 1/10 になる．

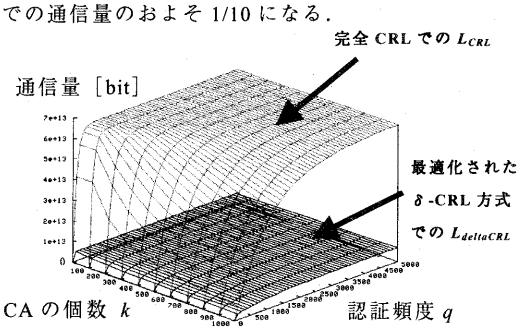

図 9　完全 CRL 方式と，最適化されたδ-CRL 方式の CRL 取得に必要な通信量

5.まとめ

PKI での主な証明書の失効方式である完全 CRL 方式，δ-CRL 方式について，CRL 取得に必要な通信量の理論式を検証者が同一の CRL の取得を高々1度しか行わない事を確率論的に取り入れて導いた．

その評価結果から，CRL 取得に必要な通信量は，認証頻度に依存する振る舞いが支配的な領域と認証頻度に依存しない振る舞いが支配的な領域に分かれることが分かった．そして，CRL を CA 毎に発行して，検証者がそのうちの必要とする CRL だけを取得できることで通信量を下げる効果が有効な領域は，認証頻度の充分低い範囲に限られることを示した．

δ-CRL 方式では，認証頻度が充分大きい場合に，通信量を最小化する最適な BaseCRL の発行間隔とδ-CRL の発行間隔の比が，証明書の有効期限とδ-CRL の発行間隔の比から一意に定まり，それは CA の個数とは無関係であることを示した．

参考文献

[1] ITU, ITU-T Recommendation X.509 Authentication Framework. Technical Report X.509, 2000.

[2] R. Housley, W. Ford, W. Polk, D. Solo, RFC 3280: Internet X.509 public key infrastructure certificate and Certification Revocation List (CRL) profile, April 2002.

[3] X.509 Internet Public Key Infrastructure On-line Certificate Status Protocol -OCSP, 1998.

[4] A. Malpani S. Galperin M. Myers, R. Ankney and C. Adams, RFC 2560: X.509 internet public keyinfrastructure online certificate status protocol - ocsp, June 1999.

[5] S. Berkovits, S. Chokani, J.A. Furlong, J.A. Geiter, andJ.C. Guild, "Public Key Infrastructure Study: Final Report", MITRE Corporation for NIST, April 1994.

[6] Moni Naor, Kobbi Nissim, "Certificate revocation and certificate update", In Proceedings 7th USENIX Security Symposium (San Antonio, Texas), Jan 1998.

[7] S.Micali, "Efficient certificate revocation", Technical Memo MIT/LCS/TM-542b, Massachusetts Institute of Technology, Laboratory for Computer Science, March 1996.