日本オペレーションズ・リサーチ学会
2004年秋季研究発表会

公開鍵基盤失効リストデータベース構築における CRL最適発行周期

01014433 金城学院大学　＊中村正治 NAKAMURA Syouji
01402793 金城学院大学　荒深美和子 ARAFUKA Miwako
01400043 愛知工業大学　中川覃夫 NAKAGAWA Toshio

1. まえがき

公開鍵基盤 (PKI : Public Key Infrastructure) では，公開鍵の所有者を証明する方法として，認証局 (CA : Certification Authority) が公開鍵証明書を利用者に発行する．もし，なんらかの理由で証明書が有効期限内に，証明書を破棄したい場合は，その証明書を利用できないようにする必要がある．このような場合に，CA は，その証明書を無効にし，証明書の失効情報を PKI ユーザに証明書廃棄リスト (CRL : Certificate Revocation List) として通知する．その通知手段として，発行された CRL をリポジトリと呼ばれるサーバに格納し PKI ユーザに公開する．PKI ユーザは，定期的にリポジトリから CRL を取得して，当該の証明書が有効であることを確認する．[1][2]CA によって，CRL は決められた周期で発行される．CRL の発行周期を，PKI の CRL に関わる各種の費用を設定して，単位時間当たりの期待運用費用を最小にする最適な完全 CRL を作成する間隔について，解析的または数値的に議論する．

2. デルタ CRL 方式

最適なデルタ CRL(完全 CRL 発行以降に発生した証明書失効情報のみの情報) 配布システムの挙動を記述するための確率モデルを構築する [3].

まず，完全 CRL の作成は N 周期間隔で実施されるものとする．すなわち，$N-1$ 個の周期についてデルタ CRL を作成した後，続く第 N 周期について完全 CRL の作成を実施するものと考える [Figure 1]. また，全 CRL の件数が S のとき，デルタ CRL の件数が $100K/S$[%] を超えたならば，それまでのデルタ CRL の作成に関わらず，完全 CRL を作成する．完全 CRL の生成がモデルの再生点となり，完全 CRL の作成から次の完全 CRL の作成までのデルタ CRL 発行件数がモデルの再生時間間隔 (離散型) となる．

次に，各周期の CRL 発生件数を確率変数によって定式化する．完全 CRL が取得されると，完全 CRL が発行された以前のデルタ CRL の内容は，この完全 CRL にとりこまれる．

まず，完全 CRL 配布後に,j 周期目に発生した新規 CRL の件数を W とし，いずれも確率分布 $F(x)$ に従うものとする．これらから，j 番目の周期が終了した時点のデルタ CRL の件数は，$Z_j \equiv \sum_{i=1}^{j} W_i \ (1 \leq j \leq N)$ となる．ここで，$F_j(x)$ が $F(x)$ の j 重畳み込みを表すものとするならば，Z_j の分布 $F_j(x)$ は，

$$F_j(x) \equiv Pr\{Z_j \leq x\} \quad (j = 0, 1, 2, \cdots, N) \qquad (1)$$

で与えられる．ただし，$F_0(x) \equiv 1$ である．

更に，CRL 発生件数が x のとき，デルタ CRL 作成処理に要するオーバヘッドを x の単調増加関数 $c(x)$ で表すものとする．また，完全 CRL を作成する処理に要するオーバヘッドを c_f (定数) で表す．デルタ CRL 件数のしきい値の意味から，明らかに

$$c(K) = c_f \qquad (2)$$

である．

また，デルタ CRL を使用したデータベース構築では完全 CRL のみの運用よりも処理が複雑なことから，データベース構築費用が増大すると仮定する．さらに，その費用はデルタ CRL の回数が増加するに伴って費用が増大する仮定する．したがって，デルタ CRL の処理費用を，

$$v(j, x) = (j-1) \cdot \beta x \qquad (3)$$

とする．

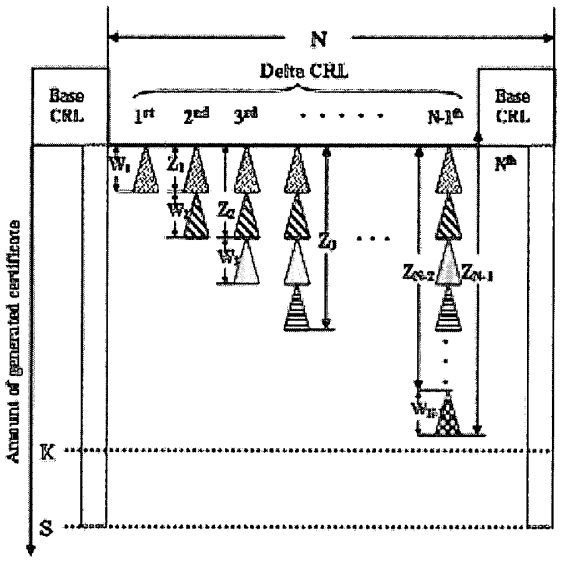

Figure 1: Creation of Delta CRL issues between Base CRL issue.

3. 期待費用

デルタ CRL 発行 1 回当たりの期待費用を導出する．

まず，完全 CRL 実施後の第 i 周期において，デルタ CRL 件数がしきい値 K を超えないとき，この周期の終了時に実施されるデルタ CRL 発行の期待費用 h_i は

$$h_i \equiv \frac{\int_0^K [c(x)+v(i,x)]dF_i(x)}{F_i(K)} \quad (1 \leq i \leq N-1) \quad (4)$$

となる．これを用いれば，完全 CRL 実施後にデルタ CRL を $j-1$ 周期繰り返し，第 j 周期 $(1 \leq j \leq N)$ で再び完全 CRL が実施されるとき，$j-1$ 件のデルタ CRL と 1 件の完全 CRL に要する費用は $\sum_{i=1}^{j-1} h_i + c_f$ となる．ここで，$1 \leq j \leq N-1$ の場合は，第 j 周期でデルタ CRL 件数がしきい値 K を超えて完全 CRL が実施される状況に対応する．また，$j = N$ の場合は，その周期でのデルタ CRL の件数とは無関係に，予定通り第 N 周期で完全 CRL が実施される状況に対応する．また，CRL 情報の中には，時間の経過に伴って有効期限の切れれくる公開鍵がある．これらは，不要にもかかわらず存在するが，完全 CRL 発行の再作成の時点でしか削除（有効期限後一定期間保存）できない．以上から，完全 CRL が実施されてから，再び完全 CRL の実施が完了するまでの総期待 CRL 発行運用費用 H は

$$\begin{aligned} H &= \sum_{j=1}^{N-1} \{F_{j-1}(K) - F_j(K)\} \cdot \left(\sum_{i=1}^{j-1} h_i + c_f \right) \\ &\quad + F_{N-1}(K) \cdot \left(\sum_{i=1}^{N-1} h_i + c_f \right) \\ &= c_f + \sum_{j=1}^{N-1} h_j F_j(K) \end{aligned} \quad (5)$$

となる．ただし，$\sum_{j=1}^{0} \equiv 0$ とする．

完全 CRL が実施されてから，再び完全 CRL の実施が完了するまでの期待 CRL 発行件数 M は

$$\begin{aligned} M &= \sum_{j=1}^{N-1} \{F_{j-1}(K) - F_j(K)\} \cdot j \\ &\quad + F_{N-1}(K) \cdot N \\ &= \sum_{j=0}^{N-1} F_j(K) \end{aligned} \quad (6)$$

として得られる．式 (5) および式 (6) から，CRL 発行 1 件当たりの期待運用費用 $C(N)$ は

$$\begin{aligned} C(N) &\equiv H/M \\ &= \frac{c_f + \sum_{j=1}^{N-1} h_j F_j(K)}{\sum_{j=0}^{N-1} F_j(K)} \quad (N = 1, 2, \ldots) \end{aligned} \quad (7)$$

である．

4. 最適完全 CRL 発行間隔

式 (7) であたえられる期待費用 $C(N)$ を最小にする N^* を求める．$C(N+1) - C(N) \geq 0$ とおくと，

$$\sum_{j=0}^{N-1} (h_N - h_j) F_j(K) \geq c_f \quad (8)$$

となる．ただし，$h_0 \equiv 0$ とする．

ここで，式 (8) の左辺を $L(N)$ とおくと，$L(1) = h_1$ である．更に，

$$L(N+1) - L(N) = (h_{N+1} - h_N) \sum_{j=0}^{N} F_j(K) \quad (9)$$

以上から，条件，h_i が i について単調増加関数ならば，$L(N)$ も単調増加関数で，次の最適政策が存在する．

(i) $h_1 \geq c_f$ ならば，$N^* = 1$ で $C(1) = c_f$，すなわち，毎回完全 CRL を作成する．

(ii) $h_1 < c_f < L(\infty)$ ならば，式 (8) を満たし最小となる有限な $N^* (1 < N^* < \infty)$ が唯一存在する．

(iii) $L(\infty) < c_f$ ならば，$N^* = \infty$，すなわち，無限にデルタ CRL 運用を続ける．

明らかに，

$$\begin{aligned} L(N) &= \sum_{j=0}^{N-1} (h_N - h_j) F_j(K) \\ &= \sum_{j=1}^{N-1} (h_N - h_j) F_j(K) + h_N \\ &> h_N \quad (N \geq 2) \end{aligned} \quad (10)$$

したがって，h_j が $j \to \infty$ のとき ∞ ならば $L(N)$ も ∞ となる．

5. むすび

本研究では，PKI における CRL 発行に関わる，デルタ CRL 運用に着目し，完全 CRL 発行処理に要する費用とデルタ CRL 発行に費す費用とのトレードオフによる最適化問題について考察した．デルタ CRL の発行を適用した総期待 CRL 発行運用費用を評価するための確率モデルを提案し，完全 CRL とデルタ CRL を含めた 1 周期当たりの期待運用費用を最小にする最適完全 CRL 発行間隔について解析的または数値的に議論した．

参考文献

[1] PKI 関連技術解説　V1.05，情報処理振興事業協会　セキュリティセンター，(2002).

[2] 大山実，他，X.500 ディレクトリ入門　第 2 版，東京電気大学出版局，(2001).

[3] 中村正治，福本聡，中川覃夫：差分バックップ方式における最適フルバックアップ，電子情報通信学会誌，D-I,Vol,J83-D-I,No.10,pp.1087-1096,(2000).