5Q-05

# CRL 分割の検討と実装

武田 哲　小俣 三郎　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、ネットワーク上における安全な通信手段として、PKI(Public Key Infrastructure)[1]を基にした、公開鍵証明書を用いた署名・親展が行われている。PKI の普及とともに、利用される証明書数の増加が考えられ、様々な理由から失効される証明書数の増加も予想される。証明書の失効リストである CRL(Certificate Revocation List)は、失効した各証明書に対応したエントリ情報を格納しており、失効証明書数の増加により、CRL 内のエントリ情報数が増え、その結果 CRL のデータサイズが大きくなってしまう。このような CRL の増大は、配布時のネットワークトラフィックや、証明書の有効性検証といった処理において高負荷となる恐れがある。本稿では、CRL の大きさを抑制する方法として、ITU-T X.509[2]に定義されている証明書のエクステンションである CRL 配布点を用いて CRL 分割を行う方法について、検討及び実装を行った。

## 2.CRL 分割方法の検討

CRL 分割方法として、証明書に CRL 配布点を設定して発行し、CRL 生成時は失効証明書中の CRL 配布点の設定に合わせて分割する方法[3]について検討を行った。今回、分割の元データとなる CRL 配布点の分け方として、次の 3 方法について検討を行った。

① 失効理由による分割
② 証明書シリアル番号による分割 1 －モジュロ演算結果による分割
③ 証明書シリアル番号による分割 2 －区間による分割

①は ITU-T X.509 における CRL のエントリエクステンション Reason Code 毎に分ける方法である。CRL 数は最大で 7 分割となる。ただし、各 CRL のエントリ情報数を制限できないため、データサイズについて制限することはできない。

②は指定した値で CRL エントリのシリアル番号をモジュロ演算した結果毎に分割する方法である。CRL 数は最大でも指定した値以内になる。ただし、各 CRL のエントリ情報数を制限できないため、データサイズについて制限することはできない。

③は指定した値を同一 CRL へ格納するシリアル番号の区間として分割する方法である。各 CRL のエントリ情報数を制限できるため、データサイズを制限することができる。ただし、CRL 分割数を制限することはできない。

## 3.CRL 分割の実装

今回検討した 3 方法のうち、実装は③の証明書シリアル番号の区間による分割について試みた。③を実装対象とした理由は、一つは各 CRL のデータサイズを小さくすることを第一に考えたためである。証明書の有効性検証時、CRL の取得、検証処理とも、CRL が小さいため高速に行うことが可能となる。また、実現の容易性から考えた場合、①の失効理由による分割では、証明書発行時には CRL 配布点を一つだけ設定することができないため、一つの証明書の中に失効理由毎に複数の CRL 配布点を設定し、CRL 生成時は複数の CRL 配布点から該当するものを選択する必要があり、②、③のように CRL 配布点を一つだけ設定する場合に比べ証明書発行、CRL 生成とも処理時間が掛かることが考えられたためである。

---

A study and implementation of CRL partitioning
Satoshi Takeda, Saburo Omata, Tsutomu Sakagami, Masao Saeki
Information Technology R&D Center,
Mitsubishi Electric Corporation

## 4.CRL 生成結果

実装した分割方法について、連続するシリアル番号の5000エントリを失効したCRLの生成時間の測定を行った。分割区間を変えることにより、生成する CRL の分割数を変化させ測定した。CRL 分割を行わない 5000 エントリを失効した CRL の生成時間を 1 としたときとの比較結果は、表 1 の通りとなった。

| 分割区間 | 250 | 500 | 1000 | 2500 |
|---|---|---|---|---|
| CRL 生成時間比 | 6.31 | 6.44 | 6.37 | 6.41 |

**表 1　分割区間毎の CRL 生成時間（分割しない場合を 1 とした比較結果）**

測定の結果、CRL 分割により CRL 生成時間は約 6.4 倍となることが分かった。また、分割区間による CRL 生成時間の違いはほとんどないことが分かった。

CRL 分割する場合、分割しない場合と比較して以下が異なると考えられる。

1) 各失効証明書からの CRL 配布点の取得
2) CRL 配布点毎のエントリの振り分け
3) 分割した CRL の生成

3)は、分割区間により CRL 分割数が変わり、各 CRL に含まれるエントリ数が異なるため、エントリ数による CRL 生成時間が異なると、全エントリ分の CRL 生成時間に違いが出る。エントリ数毎の CRL 生成時間について測定し、250 エントリを失効した CRL の生成時間を 1 としたときとの比較結果は図 1 及び表 2 の通りとなった。また、CRL のデータサイズの比較も合わせて示す。

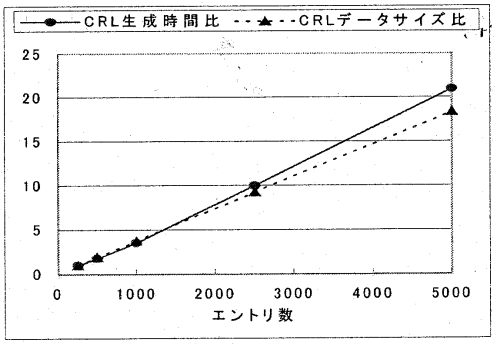


**図 1　エントリ数と CRL 生成時間、データサイズとの関係**

| エントリ数 | 500 | 1000 | 2500 | 5000 |
|---|---|---|---|---|
| CRL 生成時間比 | 1.79 | 3.54 | 10.0 | 21.0 |
| CRL ﾃﾞｰﾀｻｲｽﾞ比 | 1.92 | 3.75 | 9.26 | 18.4 |

**表 2　エントリ数毎の CRL 生成時間、データサイズ（250 エントリの場合を 1 とした比較結果）**

測定の結果、エントリ数にほぼ比例して CRL 生成時間、データサイズともに増加することが分かった。これより、分割による全エントリ分の CRL 生成時間の違いはほとんどないことが分かった。このことから、3)は表 1 で比較元とした CRL 生成時間と同じと考えられ、生成時間が 6 倍以上となった原因は、1)及び 2)にあると考えられる。

CRL 分割により CRL 生成時間は 6 倍となるものの、1000 エントリ以下の CRL データを使った証明書の検証時間は 5000 エントリのときと比較して 1/15 以下に抑えられ[3] CRL 利用時の負荷を軽減できることから、データサイズを制限する CRL 分割は有効であると考えられる。

## 5.おわりに

一つの CRL のデータサイズを制限することを目的とした、証明書のシリアル番号を区間とする CRL 分割方法について、検討及び実装を行った。今後は他の分割方法についても検討を進める予定である。

## 参考文献

[1] http://www.nist.gov/itl/lab/bulletns/archives/july97bull.htm

[2] ITU-T Recommendation X.509(06/97) INFORMATION TECHNOLOGY - OPEN SYSTEMS INTERCONNECTION - THE DIRECTORY: AUTHENTICATION FRAMEWORK, 1997

[3] 小俣他, "PKI における失効管理の高速化に関する考察", 情報処理学会第 60 回全国大会 5Q-04, 2000