2003年日本オペレーションズ・リサーチ学会
秋季研究発表会

公開鍵基盤における失効リストの最適発行周期

01014433 金城学院大学　＊荒深美和子 ARAFUKA Miwako
01402793 金城学院大学　中村正治 NAKAMURA Syouji
名古屋商科大学　原田義久 HARATA Yoshihisa
01400043 愛知工業大学　中川覃夫 NAKAGAWA Toshio

1. まえがき

PKIでは，公開鍵とその所有者を証明する手段として，公開鍵証明書を認証局 (CA : Certification Authority) と呼ばれる機関が利用者に発行する．証明書が有効期限内にもかかわらず，証明書の資格が失われた場合は，その証明書を利用できないようにする必要がある．すなわち，秘密鍵を紛失し，第三者に悪用されることが予測される場合や証明書の記載事項に変更があった場合は，CAはその証明書を無効にし，証明書の失効情報をPKIユーザに証明書失効リスト (CRL : Certificate Revocation List) として通知する．発行されたCRLは，リポジトリ (repository) と呼ばれるサーバに格納し利用者に公開する [1][2]．証明書利用者（Relying Party, ユーザ）は，定期的にリポジトリのCRLを取得することで，利用する証明書の有効性を確認することができる．

CRLは決められた周期で発行されるため，証明書が失効された場合でも，次回のCRLが発行されるまでが失効情報が利用者に伝わらない．したがって，CRLの発行周期が長くなると，失効情報が利用者に通知されるまでの時間も長くなる．逆に，発行周期を短くすると，利用者がCRLを取得するための負荷が増大する．CRLの発行周期は，セキュリティポリシーとシステムの要件を考慮して，適切な期間を設定することが重要である．

2. モデル

ユーザはCRL配布ポイントから入手できるCRLから，公開鍵の失効状況を確認しなければならない．確認方法は，発行されている最新の全CRLから毎回検索する．このため，ユーザは，CRL配布ポイントからダウンロードしたデータを基に，なんらかのユーザ用CRLデータベースを作成するとする．ここでは，CRL配布の運用方法による各種の費用を考慮した2つのモデルを提案し，ユーザが新規のCRLを取得できないことに起因する機会損失費用を設定した運用の期待費用を求める．さらに，この期待費用を最小にするCRLの最適周期について議論する．

各モデルにおいて，CAは全CRL作成の周期を決定する．以下のように記号を定義する．

M_0: 全CRLの登録件数.

T: 全CRLの発行周期　$(T = 1, 2, \ldots)$.

μ_i: 全CRLの発行以降で第$i-1$番目の差分CRL発行以降に新規に失効となった公開鍵証明書の平均数 $(i = 1, 2, \ldots, T)$．一般に，μ_iは非減少とする.

c_1: 公開鍵証明書1件あたりの単位ダウンロードの平均費用（通信費用）.

c_2: ダウンロードされた差分CRLファイルのハンドリングの平均費用.

c_3: 新規のCRL情報を取得できないことに起因する単位時間当り機会損失の平均費用を表し，μ_iに比例する.

2.1. モデル1（全CRL運用）の期待費用

全CRLを配布した後，公開鍵の新規失効が発生してもT期間はCRLを配布しない．すなわち，T周期ごとに全CRLを配布する．ユーザは，1度全CRLをダウンロードしてユーザデータベースを構築する．T期間中に発生した公開鍵の新規失効を取得できないことによって，ユーザが受ける機会損失費用は，公開鍵の失効から次の全CRL配布までの時間に比例すると仮定する．モデル1のユーザの期待費用は，以下の全CRLのダウンロード費用と機会損失費用の和で表される．

$$C_1(T) = c_1 M_0 + c_3 \sum_{i=1}^{T} (T-i)\mu_i \quad (T = 1, 2, \ldots) \quad (1)$$

2.2. モデル2(累積型差分CRL運用)の期待費用

このモデルでは，全CRL配布後，T期間は差分CRLの配布を行う．モデル2の差分CRLに含まれるCRLの件数は，全CRL配布後から今回の差分CRL発行直前までに新規に発生した公開鍵の失効件数の累積である．ユーザ用データベースの構築の方法は，全CRLを基にして，直近にダウンロードした累積型差分CRLのみを利用してデータベースに更新を行う．したがって，ダウンロードのたびに取り扱うファイル数はこのファイルのみである．

また，このモデルにおいて，ユーザは，累積型差分CRLの配布により失効情報を短期間に取得できることから，機会損失費用c_3の発生を無視できるものとする．よって，期待費用は，以下の全CRLのダウンロード費用，期間中に累積型差分CRLをダウンロード回数分の費用とファイルのハンドリング数の費用の和で表される．

$$C_2(T) = c_1 M_0 + c_1 \sum_{i=1}^{T} \sum_{j=1}^{i} \mu_j + c_2 T \quad (T = 1, 2, \ldots) \tag{2}$$

なお，モデル 2 の累積型差分 CRL の運用方法については，X.509 で CA のデルタ (Delta)CRL 使用法が明確に定義されている．このモデルの運用方法は，最新の累積型差分 CRL とこれに対応する全 CRL を確保するだけで，完全 (Full,Complete)CRL を作成できる利点がある．

3. 最適間隔

モデル 1 と 2 に対して，CRL の単位時間当たりの期待費用 $C_i(T)/T \quad (i = 1, 2)$ を最小にする最適周期 T_i^* を求める．

3.1. モデル 1 の最適周期

式 (1) から，

$$\frac{C_1(T)}{T} = \frac{c_1 M_0 + c_3 \sum_{i=1}^{T} (T - i)\mu_i}{T} \quad (T = 1, 2, \ldots) \tag{3}$$

を最小にする T_1^* を求める．

明らかに，$\lim_{T \to \infty} C_1(T)/T = \infty$ より，有限な $T_1^* (1 \leq T_1^* < \infty)$ が存在する．

さらに，$C_1(T+1)/(T+1) \geq C_1(T)/T$ とおくと，

$$c_3 \sum_{i=1}^{T} i\mu_i \geq c_1 M_0 \tag{4}$$

式 (4) の左辺は T の単調増加関数であり，∞ に発散する．したがって，次の最適方策をえる．

(i) もし，$c_3\mu_1 \geq c_1 M_0$ ならば，$T_1^* = 1$

(ii) もし，$c_3\mu_1 < c_1 M_0$ ならば，式 (4) を満たす有限で唯一の最小値 $T_1^* (1 < T_1^* < \infty)$ が存在し，

$$c_3 \sum_{i=1}^{T_1^*} i\mu_i \leq \frac{C_1(T_1^*)}{T_1^*} \leq c_3 \sum_{i=1}^{T_1^*+1} \mu_i \tag{5}$$

3.2. モデル 2 の最適周期

式 (2) から，

$$\frac{C_2(T)}{T} = \frac{c_1 M_0 + c_1 \sum_{i=1}^{T} \sum_{j=1}^{i} \mu_j + c_2 T}{T} \quad (T = 1, 2, \ldots) \tag{6}$$

を最小にする T_2^* を求める．

明らかに，μ_i が非減少より，$\lim_{T \to \infty} C_2(T)/T = \infty$ となり，有限な $T_2^* (1 \leq T_2^* < \infty)$ が存在する．$C_2(T+1)/(T+1) \geq C_2(T)/T$ とおくと，

$$T \sum_{i=1}^{T+1} \mu_i - \sum_{i=1}^{T} \sum_{j=1}^{i} \mu_j \geq M_0 \quad (T = 1, 2, \ldots) \tag{7}$$

式 (7) の左辺を $L_2(T)$ とおくと，

$$L_2(\infty) = \infty \tag{8}$$

$$L_2(T+1) - L_2(T) = (T+1)\mu_{T+2} > 0 \tag{9}$$

よって，$L_2(T)$ は T の単調増加関数より，式 (7) を満たす有限で唯一の最小値 $T_2^* (1 \leq T_2^* < \infty)$ が存在する．

このとき，

$$c_1 \sum_{i=1}^{T_2^*} \mu_i + c_2 \leq \frac{C_2(T_2^*)}{T_2^*} \leq c_1 \sum_{i=1}^{T_2^*+1} \mu_i + c_2 \tag{10}$$

とくに，$\mu_i \equiv \mu$ のとき，モデル 1 の式 (4) は

$$\frac{T(T+1)}{2} \geq \frac{c_1}{c_3} \frac{M_0}{\mu} \tag{11}$$

モデル 2 の式 (7) は

$$\frac{T(T+1)}{2} \geq \frac{M_0}{\mu} \tag{12}$$

とくに，$c_1 = c_3$ すなわち，$\mu c_1 = c_2$，$c_1 = c_3$ のとき，2 つのモデルの最適周期 $T_i^* (i = 1, 2)$ は一致する．

さらに，$\mu_i = \mu$ のとき

$$C_1(T) \geq C_2(T) \Leftrightarrow c_3(T-1) - c_1(T+1) \geq \frac{2c_2}{\mu} \tag{13}$$

4. むすび

本研究では，PKI 技術の CRL 配布方式について，それぞれの方式の配布間隔に着目し，PKI のユーザが CRL をダウンロードする費用，ユーザ用データベースを更新するためのファイルハンドリング費用と最新の CRL を取得できないことによる機会損失費用をあたえて総期待運用費用を評価するためのモデルを提案した．また，単位時間当たりの期待運用費用を最小にする最適全 CRL を作成する周期について議論した．

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).