オンライン証明書検証プロトコルのスケーラビリティ

菊池浩明[†] 中西祥八郎[††]

公開鍵証明書によるセキュリティ基盤，すなわち，PKIの構築が進んでいる．そこで，本稿では，ユーザ数 n に対してCRLのサイズがどのように推移するかを確率モデルを仮定して解析する．このモデルの上で，CRLのアプローチが有効な証明書廃止率の上限が0.5であることを示す．さらに，これらの証明書の推移モデルを基に，オンライン証明書検証プロトコルがスケーラビリティの観点から効率に制約があることを示す．

Scalability of Online Public-key Certificate Protocol

Hiroaki Kikuchi[†] and Shohachiro Nakanishi[†]

Public Key Infrastructure (PKI) is one of the key security technologies in the Internet. This paper studies a behavior of size of Certifiacte Revocation List (CRL), which is a standard way for revoking certificate, by introducing probabilistic model for certificate dynamics. The main result is that a meaningful revocation ratio is bounded by 0.5. Under the probabilistic assmuption, an online certificate verification protocol is proved to be not always efficient from the viewpoint of scalability.

1. はじめに

公開鍵証明書によるセキュリティ基盤，すなわち，PKIの構築が進んでいる．X.509では，鍵の紛失や窃盗に対して，CRL（Certificate Revocation List）による証明書廃棄を定めている．CRLは証明書と同様の公開情報であり，それゆえ，伝送における暗号化処理などを必要としない．その反面，CRLには次の問題点がある．

(1) CRLの発行間隔
CRLは定期的に発行されるため，情報の鮮度が悪い．ある証明書（の秘密鍵）が盗まれたとしても，次のCRLの発行日までは不正利用が防止できない．

(2) 通信コスト
CRLの大きさ，すなわち，廃止証明書の数はユーザ数に比例する．したがって，規模が大きくなるほどCRLは肥大化し，通信帯域を圧迫する．しかも，CRLのほとんどは静的な情報なので，同じ情報が何度もネットワークを流れることとなり，効率が悪い．

そこで，CRLに代わって，オンラインで証明書の状態を知らせるオンライン証明書検証プロトコル（以後，オンラインプロトコル）が提案されている．鮫島は，X.509の欠点を補完するサービスとして，VA（Verification Authority）を提案し，その伝送形式を定めて通信実験を行っている[6]．IETF PKIX WGでも，OCSP（Online Certificate Status Protocol）の標準化を行ってきている[1]．

しかしながら，これらオンラインプロトコルは提案者らが主張するほど万能ではない．なぜならば，CAをオンラインにするのはセキュリティ上の脅威を広げて相応しくないので，CAと分離したディレクトリサーバ，あるいは，証明書リポジトリ（以後，検証サーバ）がオンラインで検証結果を配布することとなる．この検証サーバからの検証結果を偽造されたりしてはPKIが根本から崩れてしまうので，ここに新しいセキュリティ強化のためのコストが生じる．よって，検証サーバごとに新たに公開鍵対を割り当てる必要があり，鍵管理の工程が増えるからである．

それどころか，PKIの規模に対するオンラインプロ

† 東海大学電子情報学部情報メディア学科
Department of Information Media Technology, School of Information Technology and Electronics, Tokai University
†† 東海大学電子情報学部情報科学科
Department of Human and Information Science, School of Information Technology and Electronics, Tokai University

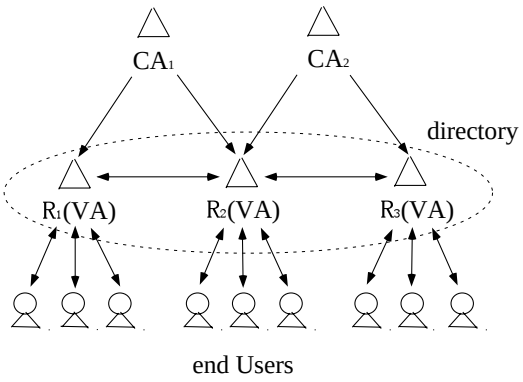

図 1 PKI モデル
Fig. 1 PKI model.

トコルのスループットは CRL にも劣る場合があることを，本稿で示す．まず，CRL を用いたシステムの性能を見積もるために，ユーザ数 n に対する CRL のサイズを明らかにする．その結果を基に，意味のある証明書破棄率の上限を示す．最後に，待ち行列モデルを適用し，n に対する検証サーバのスループットの推移を明らかにする．

2. CRL とオンラインプロトコル

2.1 PKI モデル

PKI は次の構成要素から成る（**図 1** 参照）．

- CA（発行局）
  証明書と CRL を発行する．CA の秘密鍵を安全に管理する．オフラインあるいはファイアウォールなどでアクセス制御されている．
- 検証サーバ（ディレクトリ）
  証明書と CRL を蓄え，エンドユーザからの要求に応じて提供する．他のサーバと連係し，CRL 情報を共有する．リポジトリとも呼ばれる．たとえば，図 1 においては，各々異る CA_1 と CA_2 に属する検証サーバ R_1 と R_2 は，互いに証明書状態を交換して，異る CA に属する証明書の状態をも提供可能にしている．
- 利用者
  証明書を利用するアプリケーション．認証サーバにアクセスする．少なくとも 1 つの CA に属する．

CA-ディレクトリ間は，帯域の小さな，あるいは必要に応じて接続するダイヤルアップの通信路とする．一方，ディレクトリサーバは，大きな帯域の通信路で相互に接続されている．エンドユーザは，ダイヤルアップあるいは，帯域制限された専用線でネットワークに接続されているものとする．ただし，現実のネットワーク環境では，利用者ごとにまちまちの通信品質を持ち，帯域も利用時刻に応じて動的に変化している．当然，これらの不確定性は以降の節で同定していく運用限界に影響を与える．ただし，本稿では運用限界点での厳密な同定よりも，むしろ最悪時が存在することを示すことに興味を置くため，より単純化した静的で平均的な帯域を仮定する．

一般に，CA が複数存在し，いくつかの CA に多重に属するユーザもありうるが，本稿の議論には影響しないので割愛する．

2.2 CRL

CRL とは，無効証明書のシリアル番号とその有効期限のリストに，信頼できる CA が署名したものである．発行間隔と通信コストの問題に対して，次のような改良が提案されている．

(1) Delta-CRL（差分 CRL）
X.509[2)]で提案．新しい CRL が発行されてもその大部分は前回と変わることはないので，変化した部分だけを変換する方式．肥大化の問題には有効である反面，CRL に一意なシリアル番号を振る必要が生じ，データベースの無矛盾性を損なう可能性もある，と否定的な意見も出されている．

(2) CRL Distribution Points
Housley らによる文献 3) で提案されている証明書の拡張子．CRL を獲得する URL を指定する．単一の CA が証明書ごとに異なる CRL 配布先を定めることが許されており，これにより，配布元の負荷を減らし，CRL のサイズを削減することができる．

(3) Indirect CRL（代理 CRL）
X.509[2)]の提案．(2) や (3) とは逆の方向で，複数の CRL を束ねて単一の CRL として取り扱う方法である．CRL 配布専用のサーバを用意することで，各 CA の負担を減らすことを意図している．

2.3 オンラインプロトコル

Online Certificate Status Protocol（OCSP）は，文献 1) で提案されているプロトコルであり，要求に応じてオンラインで証明書の状態を知らせる．単一の CA に問合せが集中することを防止するため，CRL をいくつかの検証サーバに分配し，各検証サーバ CA に代わって検証結果に署名を行う．

結果のみ（CRL に含まれているかどうか）を交換するため，通信コストは小さいが，検証結果の完全性を保証するため電子署名の計算コストが大きい．

3. 解析と評価

3.1 CRL のサイズ解析

ユーザ数 n に対して，CRL のサイズ L がどのように変化するか考える．

定義 3.1 証明書の有効期間（たとえば 2 年）を単位時間とし，有効期限前に破棄される確率を**破棄率**と呼び，p で表す．単位時間内に発行される証明書の総数を m とおく．

CRL によって証明書を廃止するのは，秘密鍵が漏洩したときや証明書で記載される情報に予期しない変更が生じたときであり，その事象の生起は一般には予測がつかない．しかし，十分大きな規模での運用状況においては，これらの破棄を要する事象は各々独立に生じるため全体として平均化され，上で定義する固定の破棄率で十分近似できる．このことを裏付けるために，付録 A.1 に，実際に CRL を基にした平均破棄率の例を示す．

補題 3.1 m 破棄率 p が一定で，破棄は独立な事象であると仮定する．CRL のサイズ s は，次式で与えられる．

$$s = \frac{p}{1-p}n \tag{1}$$

（証明） 独立性の仮定から，m 個中 k 個廃止される確率 $P(k)$ は，p の 2 項分布で与えられる．

$$P(k) = \left(\begin{array}{c} m \\ k \end{array} \right) p^k (1-p)^{m-k}$$

よって，その期待値は，

$$E(k) = \sum_k^m kP(k) = mp$$

で与えられ，同様にして有効な証明書の平均値も $m(1-p)$ となる．これがユーザ数 n に等しくなるので，

$$m = \frac{n}{1-p}$$

を得る．結局，CRL のサイズ s は，n と p で定まり，補題を得る． （証明終）

破棄率 p に対する CRL の大きさを，**図 2** に示す．s は n に比例し，p に単調に増加する関数である．では，$s = n$ となる点，すなわち，CRL のサイズが全ユーザ数に等しくなり，CRL を配るコストが有効である全ユーザリストを配るコストに等しくなるときの p はいくらだろうか? これも自明なことに，$n = np/(1-p)$ を解いて $p^* = 1/2$ が得られる．こうして，廃止率

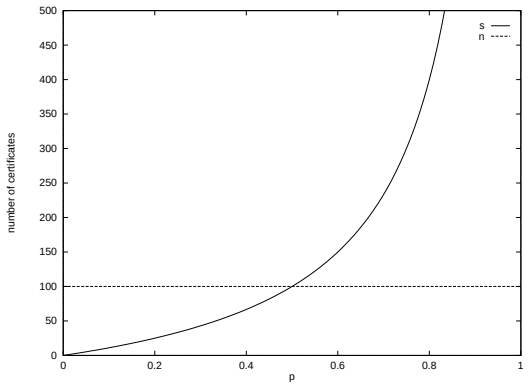

図 2 破棄率 p についての CRL の大きさ（$n = 100$）
Fig. 2 A size of CRL with regards to revocation rate p ($n = 100$).

$p < 0.5$ でないと CRL は意味がないことが示された．

補題 3.2 意味のある破棄率 p はたかだか 1/2 である．

1/2 以上の破棄率があるならば，むしろ有効であるすべてのユーザのリスト，いわゆる「ポジリスト」を配布したほうが通信路の効率が良い（ただし，プライバシの観点からは，有効ユーザが誰であるかが知られてしまうので望ましくない）．

3.2 処理時間についての CRL との比較

ここで，比較のために，検証結果に署名するのではなく，CRL を丸ごと返送するサービスを考えよう．送信にかかる時間 T_{CRL} は，CRL のサイズに比例するが，検証結果に署名する必要がないので，処理コストが小さくすむ．

補題 3.3 ディレクトリの返信帯域を B，廃止証明書数 s のときの CRL のビット長を $L(s)$ とすると，CRL の送信にかかる時間は

$$T_{CRL} = \frac{L(s)}{B}$$

と表せる．

補題 3.4 廃止証明書数を $s = np/(1-p)$ とする．s における CRL のビット長 $L(s)$ は，

$$L(s) = as + b = a\frac{p}{1-p}n + b$$

で与えられる．ここで，1 つのシリアル番号に対する大きさ a，署名やその他固定長の大きさを b とする．

一方，オンラインプロトコルで単一のサービスに要する時間 T_{OCSP} は，ほとんどが署名にかかる時間であり，n に依存する部分は近似的に 0 とおける．よって，処理時間に関して，オンラインプロトコルの効果が生じるユーザ数の下限 n_* が得られる．

定理 3.1 ユーザ数が

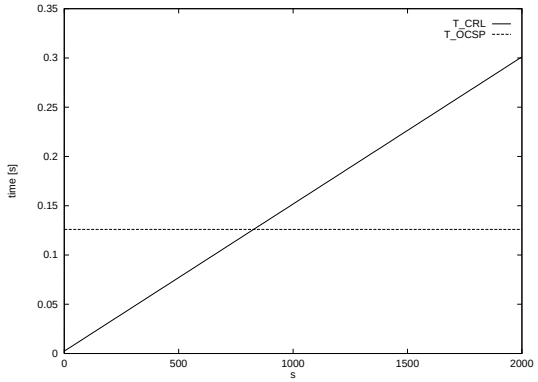

図 3 OCSP における単一トランザクションの処理時間（T_{CRL} は CRL を署名しないで直接送信した場合）
Fig. 3 The processing time for a single transaction in OCSP service (T_{CRL} indicates the case when the server replies without digitally signing).

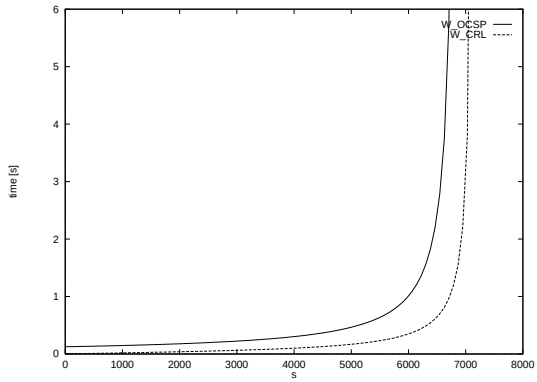

図 4 廃棄証明書数 s についての OCSP サービスの遅延時間（W_{OCSP} は OCSP サービス，W_{CRL} は比較のための CRL 直接送信サービスの遅延時間）
Fig. 4 The delay with regards to the number of revoked certificates s, where W_{OCSP} indicates that of the OCSP service, and W_{CRL} indicates the delay when the whole CRL is sent.

$$n_* = (BT_{OCSP} - b)\frac{1-p}{ap}$$

を超えるとき，オンラインプロトコルの処理時間は単純な CRL よりも小さい．

（証明） 補題より，T_{OCSP} は一定とおいて，

$$T_{CRL} = \frac{L(s)}{B} = (a\frac{p}{1-p}n + b)/B = T_{OCSP}$$

を満たす n が求まる． （証明終）

結局，各々の処理時間は n に対して**図 3** の振舞いをする．ここで，パラメータは一般的な実装例である，SSLeay-0.9 を 167 MHz の UltraSPARC，Solaris2.5 で処理した時間を基にした．RSA1,024 bit の署名で 0.126 s かかり，これを $T_s(= T_{OCSP})$ とおく．CRL のサイズは $a = 224$ bit，$b = 3,608$ bit であった．また，$B = 1.5$ Mbps，$p = 0.1$ としている．よって，この例の場合のユーザ数の下限は，

$$n_* = (1.5 \cdot 10^6 \cdot 0.126 - 3608)\frac{1-0.1}{0.1 \cdot 223} = 7448.7$$

と得られる．この結果は，ユーザ数約 7,000 の規模までの CA ならば，OCSP（OCSP）を用いるよりも CRL をそのまま送信する方が負荷が軽いことを意味している．

3.3 遅延時間からの限界

これらの結果を基に，M/M/1 待ち行列モデルを仮定して，エンドユーザからの検証要求に対する遅延時間を考える．各ユーザが，独立に，平均確率 q で検証要求を発生するとすると，OCSP の検証要求の到着は平均到着率 $\lambda = nq$ のポアソン分布となる．前節の結果より，CRL とオンラインプロトコル各々の単一の要求に対する処理時間が T_{CRL}，T_{OCSP} と分かっているとき，これらを指数時間の平均サービス率 $\mu_{CRL} = 1/T_{CRL}$，$\mu_{OCSP} = 1/T_{OCSP}$ とする．このとき，各々の平均待ち時間は Little の定理[11),12)]より，次のように与えられる．

補題 3.5 CRL サービスとオンラインプロトコルの平均待ち時間 W_{CRL}，W_{OCSP} は，次式で与えられる．

$$W_{OCSP} = \frac{1}{\mu_{OCSP} - \lambda} = \frac{1}{1/T_s - nq}$$
$$W_{CRL} = \frac{1}{\mu_{CRL} - \lambda} = \frac{1}{B/(n\frac{p}{1-p}a + b) - nq}$$

ここで，次のパラメータを置いたときの，n に対する遅延時間を**図 4** に示す．ただしここで，T_s，a，b は 3.2 節におけるシステムから抽出した値，検証要求の平均値 q は，1 日 1 人で 100 回検証を要求すると仮定したときの値である．破棄率は，付録 A.1 に示したように，1 日あたりに換算するとほぼ一定の値をとっており，その運用規模に応じて変化する．

$T_S = 0.126$ [s]
$B = 1.5 \cdot 10^6$ [bps]
$a = 224$ [bit]
$b = 3608$ [bit]
$p = 0.1$
$q = 100/24 \cdot 3600 = 0.001$

本数値実験では，OCSP のレスポンスがつねに CRL より悪くなってしまうパラメータを示したが，つねにそうなるのではなく，これらの振舞いは破棄率 p や帯域 B などの運用環境に応じて変化することに注意されたい．たとえば，ここでの $B = 1.5$ Mbps は必ずし

も十分な帯域ではないが，これをより大きな帯域にすればCRLサービスのレスポンスが向上して両者の差はより開く．

一般的には，到着率がサービス率よりも大きくなるとき，待ち行列が無限に長くなりシステムは過負荷となる．

補題 3.6 平均遅延時間の上限 W^* とする．オンラインプロトコルの平均待ち時間に関するユーザ数の上限は，

$$n^* = \left(\frac{1}{T_s} - \frac{1}{W^*}\right)\frac{1}{q}$$

（証明） $W^* = W_{OCSP}$ より明らか． （証明終）

以上の議論より，オンラインプロトコルのユーザ数 n は

$$(T_sB - b)\frac{1-p}{ap} = n_* < n < n^* = \left(\frac{1}{T_s} - \frac{1}{W^*}\right)\frac{1}{q} \quad (2)$$

の範囲内にないとCRLに対して効果がないことがいえる．ところが，先の例では，$n_* = 7400 > n^* = 6900$ となってしまい，式 (2) を満たす解がない．これを一般化すると，次の条件が得られる．

定理 3.2 次の条件を満たすとき，オンラインシステムは意味がない．

$$\frac{(1-p)q}{p} \geq \frac{(W^* - T_s)a}{T_sW^*(T_sB - b)}$$

たとえば，上のパラメータを用いると，この条件を満たす帯域は，$B > 23800$ であり，これはダイヤルアップのモデム程度の値である．

4. おわりに

現在提案されているオンラインの証明書検証プロトコルには，セキュリティと証明書破棄率の観点から制約があり，運用規模と通信環境によっては従来のオフラインのCRLを直接交換した方が効率が良い例があることを示した．ただし，この結果はオンラインプロトコルを否定するものではなく，通信帯域などのパラメータを十分に考慮しないと，期待した効果が得られなくなることを喚起するものである．本稿では，定理3.2により，証明書破棄が独立であり，ユーザ数に比例して検証要求が発生するという仮定の下で，通信帯域などのパラメータが与えられたときのオンラインプロトコルの適切な運用規模の上限と下限を明らかにした．

一方，OCSPのアプローチとは異なるセキュア一方向性関数によるハッシュ木による廃止方法[4),5),10)]などが提案されてきている．これらのアプローチでは，オンラインで検証サービスを提供するエンティティには，OCSPのように署名に用いる鍵を秘密に管理する必要がなく，セキュリティの観点からの運用コストが低い．したがって，オンラインプロトコルにだけ大きく依存することなく，これらのアプローチとの併用を探ることが，より現実的なPKIの構築につながるものと考える．

参考文献

1) Myers, M., Ankney, R., Malpani, A., Galperin, S. and Adams, C.: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol — OCSP, Internet RFC 2560 (1999).
2) Amendment 1 to ITU-T Recommendation X.509—ISO/IEC 9594-8: 1995, Information Technology — Open Systems Interconnection — The Directory: Authentication Framework.
3) Housley, R., Ford, W., Polk, W. and Solo, D.: Internet Public Key Infrastructure, Part I: X.509 Certificate and CRL Profile, Internet RFC 2459 (1999).
4) Naor, M. and Nissim, K.: Certificate Revocation and Certificate Update, *Proc. 7th USENIX Security Symposium*, pp.217–228 (1998).
5) Kocher, P.: On Certificate Revocation and Validation, *Proc. Financial Cryptography'98*, LNCS 1465, pp.172–177, Springer (1998).
6) 鮫島：X.509 認証フレームワークの問題点と解決案，暗号と情報セキュリティシンポジウム SCIS'97-8B (1997).
7) Micali, S.: Efficient Certificate Revocation, Technical Memo MIT/LCS/TM-542b (1996).
8) Yang, E.: SSLeay, http://www2.psy.uq.edu.au/ftp/Crypto/ (2002年4月参照).
9) SSL Version 3.0, (1996). http://wp.netscape.com/eng/ssl3/ (2002年4月参照).
10) 菊池，安部，中西：2分ハッシュ木を用いた証明書廃止・更新システム，情報処理学会研究報告，Vol.98, No.84, pp.51–56 (1998).
11) Tanenbaum, A.S.: *Computer Networks*, 2nd Edition, Prentice-Hall (1988). 斎藤ら（訳）：タネンバウムコンピュータネットワーク—OSI詳説，付録 待ち行列入門，丸善 (1992).
12) Little, D.: A Proof for the Queueing Formula: $L = \lambda W$, *Oper. Res.*, Vol.9, pp.383–387 (1961).

付録

A.1 CRLからの統計情報

証明書破棄の頻度を示すため，ある商用認証サービスにおける実際のCRLに格納されている統計情報を

表 1 証明書廃止頻度に関する統計情報
Table 1 The statistics on certificate revocation event.

属性	値
CRL の種類	商用サービス個人用証明書（Class 1）
CRL 更新周期	10 日間
対象期間	253 日間（2000 年 4 月 23 日
	～2000 年 12 月 31 日）
総廃止証明書数	10,136
平均破棄率 [回/日]	40.063
最頻値 [回/日]	48
最小値 [回/日]	9
最大値 [回/日]	73
標準偏差	0.81014

表 1 に示す．本データは，公開情報である CRL から，そこに格納されている破棄の日付だけについての統計をとったものである．日常的に証明書破棄が頻繁に生じており，破棄がほぼ均等に生起していて，証明書破棄数が定常状態にあることが観測できる．

(平成 13 年 12 月 19 日受付)
(平成 14 年 6 月 4 日採録)

菊池 浩明（正会員）

1988 年明治大学工学部電子通信工学科卒業．1990 年同大学院博士前期課程修了．1990 年（株）富士通研究所入社．1994 年東海大学工学部電気工学科助手．1995 年同専任講師．1999 年同助教授，1997 年カーネギーメロン大学計算機科学学部客員研究員．2000 年東海大学電子情報学部情報メディア学科助教授，現在に至る．博士（工学）．ファジィ論理，多値論理，ネットワークセキュリティに興味を持つ．1990 年日本ファジィ学会奨励賞，1993 年情報処理学会奨励賞，1996 年 SCIS 論文賞．電子情報通信学会，日本ファジィ学会，IEEE，ACM 各会員．

中西祥八郎

1967 年東海大学工学部電気工学科卒業．1969 年同大学院博士前期課程修了．同年同大学工学部電気工学科助手．1971 年同専任講師，札幌校舎勤務，1973 年同湘南校舎勤務．1985 年同助教授．1991 年同教授，2000 年同電子情報学部情報科学科教授，現在に至る．工学博士．日本ファジィ学会，電気学会，計測自動制御学会，システム制御情報学会，日本神経回路学会，日本経営工学会，IEEE，IFSA 各会員．