モバイル環境での証明書検証方式の評価

梅澤　克之[†,††]　笈川　光浩[†]　洲崎　誠一[†]　手塚　悟[†]
平澤　茂一[††]

Evaluation of Certificate Verification Methods in Mobile Environment

Katsuyuki UMEZAWA[†,††], Mitsuhiro OIKAWA[†], Seiichi SUSAKI[†], Satoru TEZUKA[†], and Shigeichi HIRASAWA[††]

あらまし　近年，インターネット環境においては，電子入札，電子納税等の公共サービスや，リモートアクセスなど，不正行為を防止するために PKI 技術に基づく認証機能を有するサービスが増加しており，そこで使われる証明書の厳密な検証を行うようになってきている．一方，モバイル環境においても，インターネットを利用した一般のサービス提供者からサービスを享受する機会が急増しており，インターネットの脅威がそのままモバイル環境においても成り立つ状況になってきている．よって，モバイル環境においても，証明書の有効性確認を含む厳密な検証機能を有する PKI 技術は必須と考えられる．現在知られている証明書検証の方式は大別して CRL 方式，OCSP 方式，CVS 方式の 3 方式である．本論文では，上記 3 方式を用いた場合の証明書検証時間を表す理論式を導出することを目的とする．更に理論式に対して，モバイル環境におけるパラメータを当てはめ，それぞれの方式で証明書検証時間を短くすることができる条件を明らかにする．更に実用的モバイル環境で CVS 方式が検証時間の基準で優れていることを示す．

キーワード　モバイル，PKI，CVS，OCSP，CRL

1. まえがき

近年，インターネットを利用したサービスにおいて，不正サイトのフィッシング詐欺によるクレジットカード番号やパスワードの流出，通信路の盗聴，ID の偽造・改ざん等の不正行為が増加している．安心してサービスを提供・享受するためには，サービスを提供する側とサービスを享受する側が正しく相互に認証し合うことが重要である．PKI 技術を用いて相互認証を行うことにより通信相手を確認することはできるが，不正な利用者やサービス提供者を正確に見極めるためには，通信相手が提示する電子証明書（以下，証明書）が失効されていないかを確認する有効性確認を行う必要がある．このような証明書の有効性確認まで行う厳密な証明書検証を行う認証機能を備えたサービスの例としては，電子政府 (GPKI) 等の認証基盤を利用した電子入札，電子納税，商業登記申請等の公共サービスや，民間企業における社外から社内へのリモートアクセス等が挙げられる．これらのサービス以外にも，高額決済を伴うような決して不正が許されないサービスにおいては，そこで使われる証明書の厳密な検証を行うようになってきている．

一方，携帯電話端末を利用して，携帯通信事業者網内に閉じたサービスにとどまらず，インターネットを利用したモバイルサービスが増加し，特定の携帯通信事業者の公式サイトからだけではなく，一般のサービス提供者からサービスを享受する機会が急増している（以降，このような携帯電話端末と携帯通信事業者網及びインターネットを利用するサービス環境をモバイル環境と呼ぶ）．このような状況から，インターネットの脅威がそのままモバイル環境においても成り立つ状況になってきており，モバイル環境においても証明書の利用による PKI 技術を用いた認証方式の確立は必須であると考えられる．既に複数の携帯通信事業者において証明書の利用が始まっているが，携帯電話端末側でサーバ証明書が失効されていないかを確認する

† （株）日立製作所システム開発研究所，川崎市
Hitachi, Ltd., Systems Development Laboratory, Hitachi System Plaza Shinkawasaki, 890 Kashimada, Saiwai-ku, Kawasaki-shi, 212–8569 Japan
†† 早稲田大学大学院理工学研究科，東京都
Graduate School of Science & Engineering, Waseda University, 3–4–1 Okubo, Shinjuku-ku, Tokyo, 169–8555 Japan

有効性確認は行われていない．モバイル環境においても不正が許されないクリティカルなサービスが今後ますます増加することが予想でき，そのようなサービスでは有効性確認を含む厳密な証明書検証を行うことが必要である．

証明書が失効されていないこと（有効性）の確認方法として失効リストを取得し確認する CRL (Certificate Revocation List) 方式や，オンラインでサーバに失効状態を問い合わせる OCSP (Online Certificate Status Protocol) 方式，CVS (Certificate Validation Server) 方式などが提案されている(注1)．

これらの各方式の優劣を比較しようとする場合の評価基準としては，下記のような様々なものが考えられる(注2)．

- 証明書検証にかかる通信量（少ないほどよい）
- 証明書検証にかかる時間（短いほどよい）
- システム導入のコスト（安いほどよい）
- 安全性，信頼性（高いほどよい）
- 利便性（高いほどよい）
- 端末実装の容易性（容易なほどよい）

文献 [1] では，CRL 方式に関して通信量の評価基準で確率論的に評価を行っているが，OCSP 方式や CVS 方式のようなオンライン方式の評価が行われていない．本論文では，評価対象の方式を広げて前述の 3 方式を対象とするとともに，証明書検証の性能は端末における計算時間も含めて評価する必要があると考え，証明書検証にかかる合計時間に着目することとする(注3)．

有効性確認の計算時間だけを考えれば，携帯電話端末の処理性能はサーバに比べて低いので，複雑な計算はサーバで処理させた方がよいと考えられる．しかし，モバイル網の通信速度は一般的に有線（専用線など）の通信速度に比べて低いので，データの送受信にかかる通信時間は逆に多くかかってしまう場合もある．証明書検証にかかる時間は，上記のように端末の計算時間とネットワークの通信時間の関係で解析する必要があるがそのような解析はいまだなされていない(注4)．

本論文では，証明書検証方式に，CRL 方式，OCSP 方式，CVS 方式のそれぞれの方式を用いた場合の証明書検証時間を表す理論式を導出することを目的とする．更に理論式に対して，モバイル環境におけるパラメータを当てはめ，それぞれの方式で証明書検証時間を短くすることができる条件を明らかにする．

以下では，まず，**2.** で証明書の検証に関する従来技術について記述する．**3.** で証明書検証にかかる時間の理論式を導出し，**4.** でモバイル環境のパラメータを当てはめた評価と考察を行う．そして最後に **5.** でまとめと今後の課題を示す．

2. 従来技術

証明書を検証するための手順は，ITU-T X.509 (2000) [5] や RFC3280 [6] にて規定されている．実際に証明書検証者が行う検証手順は，大別すると「認証パスの構築」「認証パスの検証」の二つである．「認証パスの構築」とは，検証者が信頼している認証局（以下トラストアンカーと記す）の証明書から，検証対象となる証明書までの認証パス上のすべての証明書を取得する作業のことである．「認証パスの検証」とは，構築された認証パス上の証明書の正当性を確認するために，証明書のチェーン（信頼鎖）が正しいこと，認証パスの最上位証明書が検証者のトラストアンカーであること，検証日時が証明書の有効期間内であること，検証対象となる証明書が失効されていないこと（有効性確認）等を検証することである．

2.1 証明書検証方式

証明書検証方式は，そこで使われる有効性確認方式や「認証パスの構築」「認証パスの検証」を行う主体によって CRL (Certificate Revocation List) 方式 [5], [6]，OCSP (Online Certificate Status Protocol) 方式 [7]，CVS (Certificate Validation Server) 方式 [8], [9] の三つの方式に大別できる．以下にその概要を示す．

2.1.1 CRL 方式

証明書の有効性確認に CRL を用いる方式である．CRL は失効された証明書のシリアル番号の一覧であり，一般的には認証局 (Certification Authority：CA) 単位で発行・管理される．ある証明書の有効性を確認したい場合，その証明書を発行した認証局のリポジトリから CRL を取得し，CRL 内にその証明書のシリアル番号が記載されているか否かをチェックすることで判断する．CRL は，通常一定の周期ごとに発行され，証明書の有効期間が満了したものについては，CRL から除外される．CRL 方式には，完全 CRL 方式と，

(注1)：このほかに SCVP 方式 [15] があるが，現在ドラフト版であること，及び，理論式導出のためにモデル化すると CVS 方式と同一モデルとして扱えるため今回の評価からは除外する．
(注2)：各評価基準の重要度は構築するシステム要件により異なる．
(注3)：その他の評価基準に関する評価は今後の課題とする．
(注4)：筆者らは文献 [2]～[4] において解析を行っている．本論文では解析を厳密化する．

δ-CRL 方式がある(注5)．完全 CRL 方式は，CRL の発行時点で，失効されていてかつ有効期間内であるすべての証明書の番号を含める方式である．一方，δ-CRL 方式は，比較的長い時間間隔で，base-CRL と呼ぶ完全 CRL と同じ情報を含む CRL を発行し，base-CRL の発行の間では δ-CRL と呼ぶ base-CRL より短い発行間隔の CRL を発行する方式である．δ-CRL には base-CRL の発行以降に新たに失効されかつ有効期間内である証明書の番号だけが含まれる．

2.1.2 OCSP 方式

証明書の有効性確認をオンラインで行う方式である．OCSP 方式とは，証明書の有効性を OCSP レスポンダと呼ばれる検証局 (Varidation Authority：VA) にオンラインで問い合わせる方式である．要求メッセージとして有効性を確認したい証明書の情報（証明書のシリアル番号等）を送付すると，その応答として，有効 (good)，失効 (revoked)，不明 (unknown) の三つのいずれかが返信される．認証パスの構築及び有効性確認以外の認証パスの検証は，検証者自らが行う必要がある．

2.1.3 CVS 方 式

CRL 方式や OCSP 方式には，証明書検証者が認証パスの構築や証明書の検証を行わなければならず証明書検証者側の負担が大きいといった問題がある．この負担を軽減するために考えられた方式が CVS 方式である．CVS 方式は，本来の証明書の検証者に代わって，認証パスの構築，及び認証パス中の全証明書の有効性確認を含む認証パスの検証を代行する方式である．検証者が，検証局に検証対象となる証明書と信頼する認証局の証明書を送付すると，検証対象証明書の正当性を確認した結果が返信される．本方式に基づいて実装されたシステムとして政府認証基盤 (GPKI) [8] における証明書検証システムが知られており，また，様々な高速化の技術が提案されている [9]〜[14]．

2.2 証明書検証方式の整理

証明書の検証方式を表 1 に整理する．表中の「検証者」は，証明書の検証を行う主体，「検証局」は検証者から証明書の検証あるいは有効性確認を依頼されて代行する機関を表している．3 方式ともに，認証局 (CA) あるいは検証局 (VA) を信頼するモデルであり，CA あるいは VA から取得するデータ，つまり，CRL，OCSP レスポンス，CVS レスポンスは，CA あるいは VA の署名が付与されており，それらを検証することにより通信中の改ざんや偽造を防止しているので安全性は同等と考えられる．

表 1 証明書検証方式の整理
Table 1 Classification of the certificate verification methods.

方式	証明書の検証		
	認証パスの構築	認証パスの検証	有効性確認
CRL 方式	検証者	検証者	検証者
OCSP 方式	検証者	検証者	検証局
CVS 方式	検証局	検証局	検証局

3. 証明書検証時間の理論式の導出

本章では，あるエンティティが相手を認証する際に，相手の証明書を含む認証パス中のすべての証明書を受信した後に，1 回の証明書検証を行う際に必要な検証時間（通信時間＋計算時間）の平均値（平均検証時間）を表す理論式を導出する．

3.1 モデルの定義

まず，表 1 に示した方式に関する証明書検証のモデルを定義する．

図 1 は文献 [1] に示されている (δ-)CRL 方式によるモデルである．図 2 と図 3 は VA とエンティティ間で OCSP 方式を用いるモデルである．図 2 はエンティティが証明書の有効性確認を個別に複数の VA に問い合わせるモデルである．図 3 は証明書パス中のすべての証明書の有効性確認を 1 回の問合せで行うモデルである．図 4 と図 5 は VA とエンティティ間で CVS 方式を用いるモデルである．図 4 と図 5 の違いは，図 4 では VA がすべての CA から CRL を取得するのに対して，図 5 では，VA–VA 間で OCSP 方式の問合せが発生する点である．また，今回の評価では，VA は十分な負荷分散がなされていると仮定する(注6)．

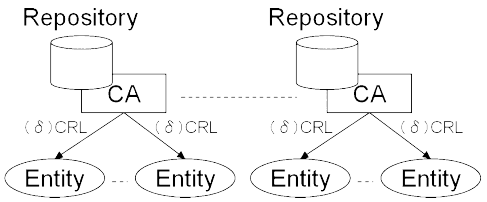

図 1 (δ-)CRL モデル
Fig. 1 (δ-)CRL model.

(注5)：このほかにも失効情報を複数の CRL に分割して公開する区分 CRL 方式や，間接 CRL 方式，証明書失効トリー (CRT：Certificate Revocation Tree) 方式などがある．
(注6)：VA の負荷に関する考察は **4.4** で行う．

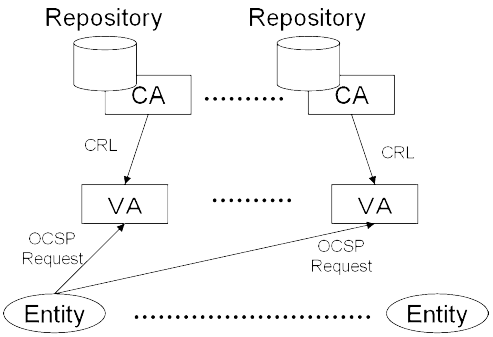

図 2　OCSP モデル 1
Fig. 2　OCSP model 1.

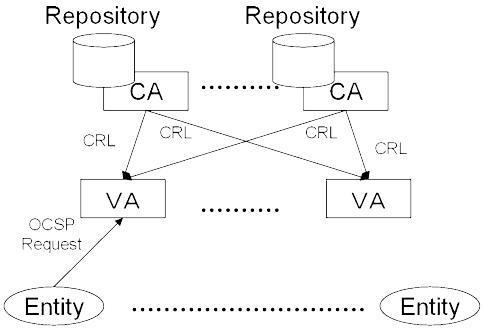

図 3　OCSP モデル 2
Fig. 3　OCSP model 2.

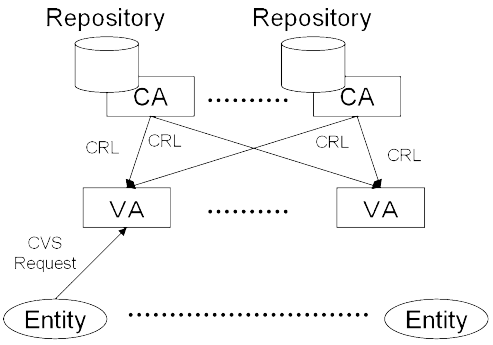

図 4　CVS モデル 1
Fig. 4　CVS model 1.

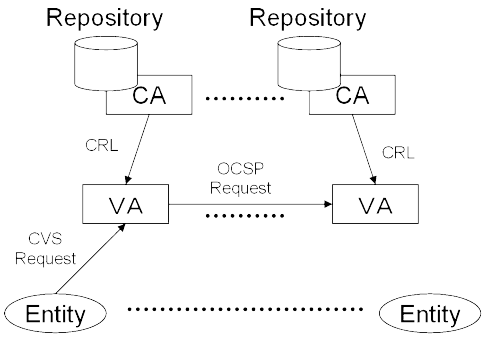

図 5　CVS モデル 2
Fig. 5　CVS model 2.

表 2　記号の定義
Table 2　Notations.

記号	説明
N	エンティティの個数 [個]
N_v	VA の個数 [個]
k	CA の個数 [個]
q	認証頻度（エンティティが 1 日に認証される平均回数）[回/day・個]
r	証明書パスの長さ（CA 階層＋1）[階層]
s	エンティティ–VA 間の網の通信速度 [bit/s]
β	エンティティ–VA 間の網の通信速度に対する VA–CA 間の網の通信速度の倍率
α	エンティティ端末の計算時間に対する VA サーバの計算時間の比
M_1	エンティティ端末における認証パスの構築時間 [s]
M_2	エンティティ端末における証明書の署名の検証時間 [s]
M_3	エンティティ端末における証明書有効性確認要求の生成時間 [s]
M_4	エンティティ端末における CRL を用いた失効確認時間 [s]
M_5	エンティティ端末における証明書有効性確認結果の署名検証時間 [s]
D_{sn}	OCSP 要求の項目一つ当り（証明書シリアル番号等）のビット数 [bit]
D_{sig}	OCSP 要求の項目数によらず一定な要素のビット数 [bit]
D'_{sn}	CVS 要求の項目一つ当り（証明書等）のビット数 [bit]
D'_{sig}	CVS 要求の項目数によらず一定な要素のビット数 [bit]

3.2　証明書検証の平均検証時間

CRL は，**2.1.1** で示したように通常一定の周期ごとに発行されるので，その周期内であれば，一度取得してしまえば 2 度目以降は CRL を取得する必要はない．このように，CRL の取得の必要性は証明書検証の事象が発生する確率によるので，CRL の取得時間は平均値で求める必要がある．CRL の取得時間の平均値を C_x，端末及びサーバで証明書の検証に必要な計算時間を M_x，有効性確認要求時間を R_x とすると，平均検証時間 T_x は，次式で表せる．

$$T_x = C_x + M_x + R_x \tag{1}$$

ただし，x はモデルを表す．次節以降で，モデルごとの C_x，M_x，R_x を導出する．なお，理論式導出の際に用いる記号の定義を表 2 に示す．

3.3　証明書検証を行う確率

C_x を求める前に，まず証明書検証の事象が発生す

る確率を求める．一般的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，ポアソン分布 $P(X) = \lambda^X \cdot e^{\lambda}/X!$ に従うことが知られている．

文献 [1] より，認証頻度 q [回/day · 個]，CA の個数 k [個] であるので，時間間隔 T [day] の間にある検証者がある CA に属するエンティティを認証する回数の期待値は qT/k 回になる（付録 **1.** 図 A·1 ②参照）．よって，あるエンティティが，ある CA に属するエンティティを認証する回数は，$\lambda = \frac{qT}{k}$ のポアソン分布に従うと考えられる(注7)．よって，エンティティにおいて時間間隔 T の間に 1 回以上認証が行われる確率 ${p_e}^T_{X\geq 1}$ は下記で表せる．

$$ {p_e}^T_{X\geq 1} = 1 - e^{-\frac{qT}{k}} \tag{2} $$

次に，VA において認証（エンティティからの有効性確認要求に基づく処理）が発生する確率を求める．複数のグループの事象の発生回数 X の確率分布がポアソン分布に従っているときにそれらを合計した事象の発生回数 X' の確率分布もポアソン分布に従うことが知られている．OCSP モデル 1 では，N 個のエンティティから N_v 個の VA に分散されて認証要求がなされる（付録 **1.** 図 A·2 ②参照）．また OCSP モデル 2 と CVS モデル 1，2 では，N/N_v 個のエンティティから一つの VA に認証要求がなされる（付録 **1.** 図 A·3 ②，図 A·4 ②参照）．よって，VA におけるエンティティからの認証頻度は $q' = \frac{q \cdot N}{N_v}$ となる．CVS モデル 2 では，このうち $q' \cdot \frac{1}{N_v}$ は自ら検証を行い（付録 **1.** 図 A·4 ③参照），残りの $q' \cdot \frac{N_v - 1}{N_v}$ は他の VA に依頼する（付録 **1.** 図 A·4 ④参照）．このとき他の VA から同数の検証要求が寄せられることになる．結局，エンティティ及び他の VA からの検証要求の頻度は合計で $q' = \frac{q \cdot N}{N_v}$ となる．OCSP モデル 1，CVS モデル 2 では k/N_v 個，OCSP モデル 2 と CVS モデル 1 では k 個の CA に属するエンティティを認証することになるので，時間間隔 T の間に VA がある CA に属するエンティティを認証する回数の期待値は前者で $qT/k \cdot N$ 回（付録 **1.** 図 A·2 ③，図 A·4 ⑤参照），後者で $qT/k \cdot \frac{N}{N_v}$ 回（付録 **1.** 図 A·3 ③参照）となる．よって，VA において時間間隔 T の間に 1 回以上認証が行われる確率は，OCSP モデル 1 と CVS モデル 2 のそれを ${p'_v}^T_{X\geq 1}$，OCSP モデル 2 と CVS モデル 1 のそれを ${p_v}^T_{X\geq 1}$ とすると下記で表せる．

$$ {p'_v}^T_{X\geq 1} = 1 - e^{-\frac{qT}{k} \cdot N} \tag{3} $$

$$ {p_v}^T_{X\geq 1} = 1 - e^{-\frac{qT}{k} \cdot \frac{N}{N_v}} \tag{4} $$

3.4 CRL の平均取得時間の導出

CRL モデル及び δ-CRL モデルでは CA–エンティティ間で CRL の取得が行われる．また，その他のモデルでは CA–VA 間で CRL の取得が行われる(注8)．CRL の発行間隔 T_C 内に CRL の取得が行われる確率は，ある CA に属するエンティティを 1 回以上認証する確率である．よって CRL モデルにおける 1 回の CRL 取得に要する平均時間 C_{CRL} は，式 (2) の $T = T_C$ とした確率で l_{CRL} を全 CA 数について和をとり時間平均したものを，認証頻度 q 及び通信速度 s で割った値であり，次式のように表せる．

$$ C_{CRL} = \frac{k \cdot {p_e}^{T_C}_{X\geq 1} \cdot l_{CRL}}{T_C \cdot q \cdot s} \tag{5} $$

ただし，l_{CRL} は，一つの CA が 1 回に発行する CRL のサイズであり，次式で与えられる（付録 **2.** 参照）．

$$ l_{CRL} = \frac{N' pL}{k} \cdot l_{sn} + l_{sig} \text{ [bit]} \tag{6} $$

δ-CRL モデルの場合は，base-CRL と δ-CRL の両方を取得するための時間が必要である．前者を $C_{baseCRL}$，後者を C_{delta} とすると，次式が成立する．

$$ C_{deltaCRL} = C_{baseCRL} + C_{delta} \tag{7} $$

δ-CRL 方式の base-CRL は，完全 CRL 方式の CRL と同様の情報を含むので，その取得時間 $C_{baseCRL}$ は，式 (5) における時間間隔を base-CRL の発行間隔 T_B とした次式で表せる．

$$ C_{baseCRL} = \frac{k \cdot {p_e}^{T_B}_{X\geq 1} \cdot l_{CRL}}{T_B \cdot q \cdot s} \tag{8} $$

δ-CRL の取得時間 C_{delta} は，n 番目に発行された δ-CRL のサイズ $l_{delta}(n)$ を時間平均した次式で表せる．

$$ C_{delta} = \frac{k \cdot {p_e}^{T_C}_{X\geq 1} \cdot \sum_{n=1}^{\frac{T_B}{T_C}-1} l_{delta}(n)}{T_B \cdot q \cdot s} \tag{9} $$

$l_{delta}(n)$ は，

$$ l_{delta}(n) = \frac{N' pL}{k} \left\{ 1 - \left(1 - \frac{T_C}{L} \right)^n \right\} \cdot l_{sn} + l_{sig} \tag{10} $$

(注7)：文献 [1] においても同様の仮定をおいている．
(注8)：文献 [1] に従い，CA 証明書の失効頻度は十分小さいのでその検証に必要な CRL 取得のための通信量は無視できると仮定する．

である（付録 **3.** 参照）．

その他のモデルの場合は，すべて CA–VA 間の CRL の取得である．OCSP モデル 1 と CVS モデル 2 は k/N_v 個の CA から CRL を取得するのに対して，OCSP モデル 2 と CVS モデル 1 は k 個のすべての CA から CRL を取得する．よって 1 回の CRL 取得に要する平均時間 C_x（x はモデル）は，式 (3)，(4) の $T = T_C$ とした確率で l_{CRL} をそれぞれのモデルにおける CRL の取得元となる CA 数について和をとり時間平均したものを，認証頻度 q' 及び通信速度 $\beta \cdot s$ で割った値であり，次式のように表せる．

$$C_{OCSP1} = C_{CVS2} = \frac{\frac{k}{N_v} \cdot {p'_v}^{T_C}_{X \geq 1} \cdot l_{CRL}}{T_C \cdot q' \cdot \beta \cdot s} \quad (11)$$

$$C_{CVS1} = C_{OCSP2} = \frac{k \cdot {p_v}^{T_C}_{X \geq 1} \cdot l_{CRL}}{T_C \cdot q' \cdot \beta \cdot s} \quad (12)$$

3.5 平均計算時間の導出

相手から証明書を受け取ったエンティティは一般的に下記の処理を行う．

（1） 認証パスの構築
（2） 証明書の署名の検証
（3） 証明書有効性確認要求の生成
（4） CRL を用いた失効確認
（5） 証明書有効性確認結果の署名検証

これらの計算処理のうち（1）及び（2）の処理はどのモデルにおいても $r-1$ 回行う必要があるが，CVS モデル 1 及び CVS モデル 2 では VA が行うのに対してその他の方式はエンティティが行う点が異なっている．また（3）及び（5）の処理は，オンラインで有効性確認を行わない CRL モデル及び δ-CRL モデルでは行われず，OCSP モデル 1 では，$r-1$ 回，その他のモデルでは 1 回行う必要がある．更に（4）の処理は，CRL モデル及び δ-CRL モデルではエンティティが行うのに対して，その他のモデルでは VA が行う．よって，上記（1）〜（5）の処理時間を M_n $(1 \leq n \leq 5)$ [s] とし，更に $M_{12} = M_1 + M_2$，$M_{35} = M_3 + M_5$，とすると，1 回の証明書検証に必要な計算時間 M_x（x はモデル）は下記のように表せる(注9)．

$$M_{CRL} = (r-1)(M_{12} + M_4) \quad (13)$$

$$M_{deltaCRL} = M_{CRL} \quad (14)$$

$$M_{OCSP1} = (r-1)(M_{12} + \alpha M_4 + M_{35}) \quad (15)$$

$$M_{OCSP2} = (r-1)(M_{12} + \alpha M_4) + M_{35} \quad (16)$$

$$M_{CVS1} = (r-1)\alpha(M_{12} + M_4) + M_{35} \quad (17)$$

$$M_{CVS2} = M_{CVS1} \quad (18)$$

3.6 平均有効性確認要求時間の導出

有効性確認時間は，それぞれの方式の有効性確認要求のデータサイズと通信時間によって導出できる．オンラインで有効性確認を行わない CRL モデル及び δ-CRL モデルでは有効性確認時間は 0 となる(注10)．CVS モデル 1，2 では認証パス中の r 個のすべての証明書，OCSP モデル 1，2 では自らが信頼するルート CA 証明書を除いた $r-1$ 個の証明書の有効性確認要求を行う必要がある．OCSP モデル 1 では，$r-1$ 個のリクエストを生成しなければならないのに対して，OCSP モデル 2 及び CVS モデル 1，2 では，一つのリクエストに複数の項目をまとめることができるので，確認要求データのビット数は，OCSP モデル 1 が $(r-1)(D_{sn}+D_{sig})$，OCSP モデル 2 が $(r-1)D_{sn} + D_{sig}$，CVS モデル 1，2 が $rD'_{sn} + D'_{sig}$ となる．更に，CVS モデル 2 では，自 CA に属さないエンティティからの有効性確認要求を，他の VA に依頼するための VA–VA 間の有効性確認要求が必要になる．VA の数は N_v 個なので上記確認要求が必要な確率は $\frac{N_v-1}{N_v}$ である．よって CVS モデル 2 では下記に示す VA–VA 間の確認要求時間 R'_{CVS2} が余分に必要になる．

$$R'_{CVS2} = \frac{N_v - 1}{N_v} \cdot \frac{(r-1) \cdot (D_{sn} + D_{sig})}{\beta \cdot s} \quad (19)$$

ここで，VA–VA 間は個々の VA に OCSP 方式 1 で問い合わせると仮定した．1 回の証明書検証に必要な有効性確認要求時間 R_x（x はモデル）は下記のように表せる(注11)．

$$R_{CRL} = R_{deltaCRL} = 0 \quad (20)$$

$$R_{OCSP1} = \frac{(r-1)(D_{sn} + D_{sig})}{s} \quad (21)$$

$$R_{OCSP2} = \frac{(r-1)D_{sn} + D_{sig}}{s} \quad (22)$$

$$R_{CVS1} = \frac{rD'_{sn} + D'_{sig}}{s} \quad (23)$$

$$R_{CVS2} = \begin{cases} \frac{rD'_{sn} + D'_{sig}}{s} \end{cases}$$

(注9)：ここで，計算時間を $r-1$ 倍しているのは，ルート CA 証明書は何らかの方法で既検証済みでありトラストアンカーとしてエンティティは信頼済みという仮定をおいているためである．
(注10)：厳密には自身で所持している CRL に検証対象証明書のシリアル番号が含まれているか否かの判定時間は要する．
(注11)：厳密には結果の返答時間がかかるが，そのサイズは小なので省略する．

$$+\frac{N_v-1}{N_v}\cdot\frac{(r-1)(D_{sn}+D_{sig})}{\beta\cdot s}\Bigg\} \quad (24)$$

4. モバイル環境適用時の評価と考察

本章では，モバイル環境適用時のパラメータを当てはめ，クライアント認証時及びサーバ認証時の証明書検証に要する平均計算時間を比較する．

4.1 パラメータ

モバイル環境での証明書検証にかかる時間を評価するにあたり，表 3 のようにパラメータを設定した．パラメータ 1 は携帯電話端末がサービス提供者の証明書を検証するサーバ認証の場合のパラメータであり，パラメータ 2 はその逆のクライアント認証の場合のパラメータである．このときエンティティ端末における証明書の署名の検証時間 M_2 を M とした．本パラメータの設定の根拠を付録 **A.** に示す．

4.2 理論式による評価と考察

4.2.1 各方式の証明書検証時間の比較

本節では，エンティティが処理性能の低い携帯電話端末，エンティティ–VA 間が通信速度の低いモバイル網と仮定して，サービス提供者（サーバ）が提示した証明書の検証を携帯電話端末が行う場合の評価を行う．具体的には，携帯電話端末の処理速度及びモバイル網の通信速度を変動させ，(δ-)CRL モデル，OCSP モデル 1，2，CVS モデル 1 の各方式(注12)の平均検証時間が小さくなる条件を明確にする．

(a) 異なる通信速度における各方式の平均検証時間

式 (1) より平均検証時間 T_x（x はモデル）は $T_x = C_x + M_x + R_x$ であるので，式 (2)〜(23) に対して，モバイル環境を想定した表 3 のパラメータ 1 を適用すると平均検証時間 T_x（x はモデル）は下記のようになる．

$$T_{CRL} = \frac{9813.73}{s} + 2.712M \quad (25)$$

$$T_{deltaCRL} = \frac{7978.59}{s} + 2.712M \quad (26)$$

$$T_{OCSP1} = \frac{0.0212}{\beta\cdot s} + \frac{1408}{s} + (0.712\alpha+4)M \quad (27)$$

$$T_{OCSP2} = \frac{0.2124}{\beta\cdot s} + \frac{1336}{s} + (0.712\alpha+3)M \quad (28)$$

$$T_{CVS1} = \frac{0.2124}{\beta\cdot s} + \frac{19456}{s} + (2.712\alpha+1)M \quad (29)$$

図 6，図 7，図 8 に，それぞれ通信速度が 28.8k, 384k, 2.4M [bit/s] であり，かつ，$\alpha = 0.1$（サーバの処理時間が端末の処理時間の 10 倍），$\beta = 100$（CA–VA 間の通信速度がモバイル網通信速度の 100 倍）のときの平均検証時間を示す．

式 (25)〜(29) より，図 6，図 7，図 8 の Y 軸の切片は CRL の取得時間及び有効性確認要求時間により

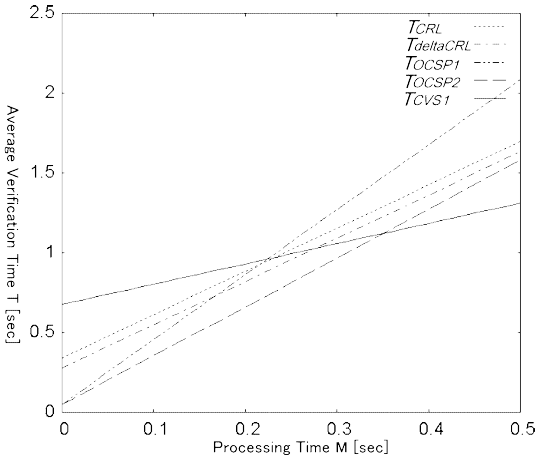

図 6 通信速度が $s = 28.8$k [bit/s] のときの各方式の平均検証時間

Fig. 6 The average of the verification time in the each system when the transaction speed is $s = 28.8$k [bit/s].

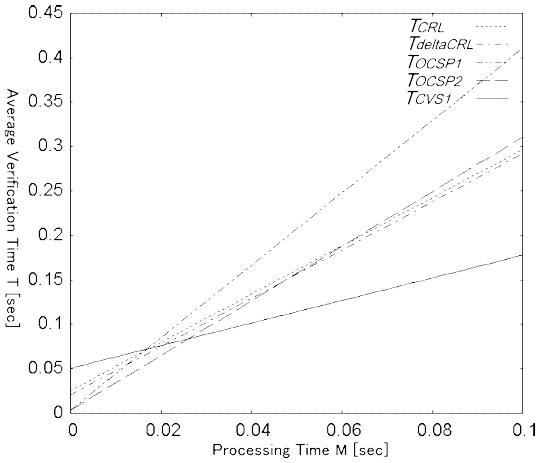

図 7 通信速度が $s = 384$k [bit/s] のときの各方式の平均検証時間

Fig. 7 The average of the verification time in the each system when the transaction speed is $s = 384$k [bit/s].

(注12)：CVS モデル 2 はクライアント認証に関するものでありその評価は次節で行う．

表 3　モバイル環境の評価用パラメータ
Table 3　Parameters for evaluation.

項目	パラメータ 1	パラメータ 2
エンティティ（認証者）の数 N [個]	77,229,000	633,000
被認証者の数 N' [個]	633,000	77,229,000
認証頻度 q [回/day]	3	366
失効発生頻度 p [回/day]	0.1/365	0.1/365
証明書の有効期間 L [day]	365	365
完全 CRL，δ-CRL の発行間隔 T_C [day]	1	1
CRL の項目一つ当りサイズ l_{sn},[bit]	72	72
CRL の項目によらず一定な要素のサイズ l_{sig} [bit]	728	728
CA の数 k [個]	500	10
VA の数 N_v [個]	10	10
OCSP 要求の項目一つ当り（証明書シリアル番号等）のビット数 D_{sn} [bit]	632	632
OCSP 要求の項目数によらず一定な要素のビット数 D_{sig} [bit]	72	72
CVS 要求の項目一つ当り（証明書等）のビット数 D'_{sn} [bit]	6,464	6,464
CVS 要求の項目数によらず一定な要素のビット数 D'_{sig} [bit]	64	64
base-CRL の最適発行間隔 T_B [日]	495	28
エンティティ端末における認証パスの構築時間 M_1 [s]	0	0
エンティティ端末における証明書の署名の検証時間 M_2 [s]	M	M
エンティティ端末における証明書有効性確認要求の生成時間 M_3 [s]	0	0
エンティティ端末における CRL を用いた失効確認時間 M_4 [s]	$0.356M$	$0.356M$
エンティティ端末における証明書有効性確認結果の署名検証時間 M_5 [s]	M	M

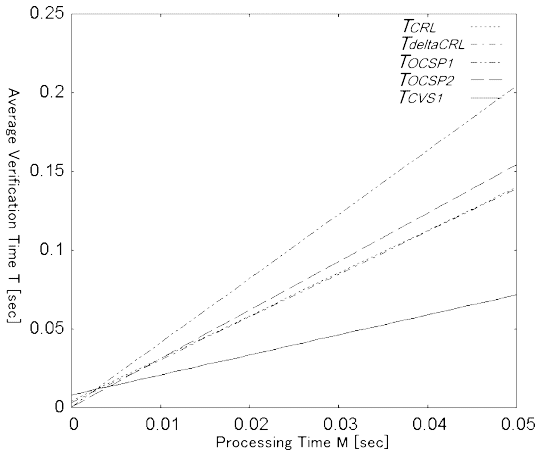

図 8　通信速度が $s = 2.4$M [bit/s] のときの各方式の平均検証時間
Fig. 8　The average of the verification time in the each system when the transaction speed is $s = 2.4$M [bit/s].

決まる値であり，通信速度が速くなればこの Y 軸の切片の値は小さくなることが分かる．また，直線の傾きは端末とサーバの計算速度の差に依存し，その差が大きいほど有効性確認の処理をサーバ側に依頼する CVS 方式の直線の傾きが小さくなり，結果的に CVS 方式の平均検証時間を小さくするといえる．

表 4　図 6，図 7，図 8 における交点 M
Table 4　The value of M that is the intersection in Figs. 6, 7 and 8.

対象	28.8k の場合	384k の場合	2.4M の場合
T_{CRL}	$M = 0.2324$	$M = 0.0174$	$M = 0.0028$
$T_{deltaCRL}$	$M = 0.2766$	$M = 0.0207$	$M = 0.0033$
T_{OCSP1}	$M = 0.2238$	$M = 0.0168$	$M = 0.0027$
T_{OCSP2}	$M = 0.3495$	$M = 0.0262$	$M = 0.0042$

ここでモバイル環境でない場合，つまり端末の性能とサーバの性能が同一 ($\alpha = 1.0$) であり，かつ，利用する網の種類が同一 ($\beta = 1.0$) という状況を考える．このような環境では，例えば OCSP 方式 2 と CVS 方式 1 を比較すると式 (28) と式 (29) より，端末の計算速度 M によらず $T_{CVS1} > T_{OCSP2}$ となるので，CVS 方式が必ずしも有利とは限らない．

図 6，図 7，図 8 のように CVS 方式の直線が他の方式の直線と交わる点をもつのは，端末とサーバの計算速度に差があり，また，モバイル網とバックエンド網の通信速度に差がある場合であり，特にモバイル環境では両者の差が顕著に現れる．

(b) CVS 方式 1 と他の方式の平均検証時間の交点の評価

表 4 に図 6，図 7，図 8 における T_{CVS1} と他の直線との交点の M の値を示す．表 4 より，例えば通

信速度が 384k [bit/s] の場合，$M = 0.0262$ のときに T_{CVS1} と T_{OCSP2} が交わっているので，端末における計算時間が 26.2m [s] より多くの時間がかかってしまう場合には CVS 方式の方が平均検証時間が短くなることが確認できる．

(c) CVS 方式の平均検証時間が小さくなる領域の評価

図 6，図 7，図 8 では，エンティティ端末の計算時間に対する VA サーバの計算時間の比 α を 0.1 と固定したが，図 9 に，α を 0.5 まで動かし，通信速度 $s = 384\text{k}$ [bit/s] と $s = 2.4\text{M}$ [bit/s] のときの OCSP 方式 1，OCSP 方式 2 と CVS 方式 1 の平均検証時間の交点の軌跡を示す．図 9 の各曲線の上側が，CVS 方式 1 の方が平均検証時間が小さくなる領域を示している．

図 9 より，通信速度が速くなるに従って CVS 方式 1 が有利となる領域が増え，かつ，端末とサーバの計算速度の差が大きい（α が小さい）ほど CVS 方式 1 が有利となる領域が増えることが分かる．携帯電話端末の計算速度は年々高性能化されつつあるが，同様にサーバの性能も上がっており，携帯電話端末では電池の寿命等の問題もあり，サーバとの計算速度の差は縮まらないと考えられる．一方，モバイル網の通信速度は年々高速化しており，図 9 に示す曲線は年々下方にスライドすることが予想できる．つまり将来的にますます CVS 方式が有利となる領域が増えると予想できる．

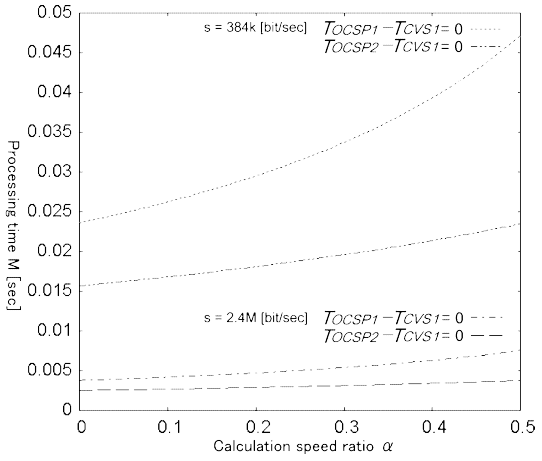

図 9 OCSP 方式 1，2 より CVS 方式の平均検証時間が小さくなる領域

Fig. 9 Areas where average verification time of CVS method becomes small more than OCSP method 1 and 2.

4.2.2 モバイル特有の機能を付加した場合の CVS 方式の性能劣化の評価

通信事業者の失効リスト (CRL) を無条件に公開すると解約者の絶対数や増加率などの積極的には公開したくない情報も公開することになってしまうため，CRL を適切に取り扱う必要がある．CVS モデル 2 は，この要求に対応するためのモデルである(注13)．このモデルでは，VA–VA 間で有効性確認の問合せ処理が発生するため CVS モデル 1 に比べて性能劣化が予想される．本項では，CVS モデル 1 に比べて CVS モデル 2 の性能劣化が小さいことを示す．

この要件は，携帯電話端末の契約者（クライアント）をサービス提供者（サーバ）が検証する際の要件であるため，本項では，エンティティがサービス提供者（サーバ），エンティティ–VA 間が VA–CA 間と同様にインターネットと仮定して，携帯電話端末が提示した証明書の検証をサービス提供者サーバが行う場合の評価を行う．

図 10 に，クライアント認証時のパラメータ（表 3 のパラメータ 2）及び，$\alpha = 0.5$（VA の計算時間がサービス提供者の計算時間の半分），$\beta = 1.0$（CA–VA 間の通信速度と VA–エンティティ間の通信速度は同一），通信速度 $s = 100\text{M}$ [bit/s] のときの CVS モデル 1，2

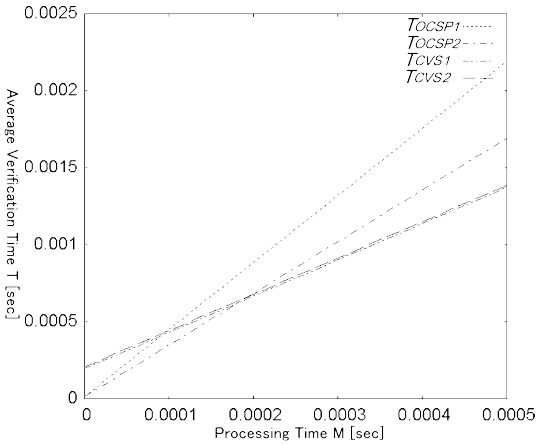

図 10 通信速度が $s = 100\text{M}$ [bit/s] のときの各方式の平均検証時間

Fig. 10 The average of the verification time in the each system when the transaction speed is $s = 100\text{M}$ [bit/s].

(注13)：図 5 に示したように，ある CA から CRL を取得する VA は，他の CA からは CRL を取得せず，OCSP リクエストによって他 VA に有効性確認を依頼し結果のみ受信することができるため，他通信事業者から CRL を取得せずに有効性確認が行える．

の平均検証時間を示す(注14)．図 10 より，CVS 方式 1 と CVS 方式 2 の平均計算時間の差は極めて小さいことが分かる．つまり，通信事業者の失効リスト (CRL) を公開することなく証明書検証を行いたいというモバイル特有の要件を，CVS 方式 2 を採用することにより，性能を劣化させずに満たすことができる．

4.3 実測値による評価と考察

CRL 方式や OCSP 方式は，携帯電話端末内で証明書パス構築やパス検証を行う必要があり，実装が容易ではない．本節では CVS 方式に基づいて実装したシステムの実測値を計測し，その結果と **3.** で導出した理論式に基づいて他の方式（CRL 方式や OCSP 方式）で実装した場合を仮定して，各方式の比較を行う．

4.3.1 証明書検証時間の実測

文献 [2] において CVS 方式 1 に基づいて実装したモバイル向け証明書検証サーバを用いて実測値による評価を行った．本評価では，クライアントとして CDMA 1x WIN 規格の携帯電話端末（BREW 端末）及びサーバとして CPU に Intel® Pentium® 4 プロセッサ 3.4 GHz，メモリ 2 GByte，OS に Windows® XP operating system を搭載したコンピュータを用いた．表 5 に，サーバの処理時間 (M_{CVS1})，通信時間 (R_{CVS1}) 及び携帯電話端末における証明書有効性確認要求の開始から確認結果の受信終了までのレスポンス時間 (T_{CVS1}) を示す．ただし CRL の取得時間及び携帯電話端末内での検証結果の署名検証時間は含まれない（つまり $C_{CVS1} = 0$，$M_{35} = 0$）．また，証明書検証要求データサイズは，検証対象証明書サイズが 675 [Byte]，トラストアンカー証明書サイズが 569 [Byte]，その他のデータが 5 [Byte] の計 1249 [Byte] である（つまり $rD'_{sn} + D'_{sig} = 9992$ [bit]）．なお，表 5 は 100 回の計測の平均値である．

4.3.2 署名生成時間の実測

4.3.1 と同じ携帯電話端末及びサーバコンピュータを用いて署名生成時間を実測した．表 6 に，署名生成時間の実測値を示す．なお，表 6 は 100 回の計測の平均値である．これにより携帯電話端末とサーバコンピュータの計算時間の比は $\alpha = 0.16/10.03$ で近似できる．

4.3.3 署名検証時間，CRL 検索時間の実測

表 7 に署名検証時間，CRL 検索時間の実測による比を示す．実測の方法に関しては付録 **A.** M_4 の説明参照．

4.3.4 考　　察

式 (17) と，**4.3.1** のサーバの処理時間の実測値 (28 [ms])，実測の条件，証明書階層は 2 階層 ($r = 2$)，携帯電話端末内の処理は含まない ($M_{35} = 0$)，**4.3.2** の結果 ($\alpha = 0.16/10.03$) より，$M_{12}+M_4 = 1755$ [ms] を得る．本結果と式 (13)，式 (14) より，CRL 方式による証明書検証に必要な計算時間 $M_{CRL} = M_{deltaCRL} = 1755$ [ms] を得る．更に，式 (15)，式 (16) と，表 7 の署名検証時間及び CRL を用いた失効確認時間の比 $M_4 = 0.356M_2$，及び，実測の条件，認証パスの構築時間 $M_1 = 0$ より，$M_{OCSP1} = M_{OCSP2} = 1302$ [ms] を得る．式 (23) と，**4.3.1** の通信時間 (879 [ms])，実測の条件，送信データサイズ 9992 [bit] より，$s = 11367$ [bit/s] を得る．本結果及びパラメータ 1 の OCSP 方式の検証要求サイズ 704 [bit] と，式 (21)，式 (22) より，$R_{OCSP1} = R_{OCSP2} = 62$ [ms] を得る．以上を表 8 にまとめる．

ただし，γ_n ($n = 1, 2, 3$) は，確率的な値ではなく，確率 1 で 1 回の CRL を取得する場合の取得時間

表 5　証明書検証時間の実測値
Table 5　The measurement value of certificate validation time.

処理内容	時間 [ms]
サーバの処理時間 (M_{CVS1})	28
通信時間 (R_{CVS1})	(879)*
携帯電話端末におけるレスポンス時間 (T_{CVS1})	907

* ただし通信時間は逆算値

表 6　署名生成時間の実測値
Table 6　The measurement value of signature generation time.

処理内容	時間 [ms]
携帯電話端末での処理	10.03
サーバでの処理	0.16

表 7　署名検証時間及び CRL を用いた失効確認時間の比
Table 7　The ratio between time of verifying signature and searching CRL.

処理内容	比
署名の検証時間 (M_2，M_5)	1
CRL を用いた失効確認時間 (M_4)	0.356

表 8　各方式の証明書検証時間
Table 8　Certificate verification time of each method.

方式	値 [ms]
T_{CRL}，$T_{deltaCRL}$	$1755 + \gamma_1$
T_{OCSP1}，T_{OCSP2}	$1364 + \gamma_2$
T_{CVS1}	$907 + \gamma_3$

(注14)：比較のために OCSP モデル 1，2 の結果も示す．

である．つまり，式 (5)，(11)，(12) に対して，CRL を発行する CA の個数 k，VA の個数 N_v，時間間隔 T_C，認証頻度 q 及び q' をすべて 1 とし，また，必ず認証が行われる，つまり，${p_e}_{X\geq 1}^{T_C}$，${p_v}_{X\geq 1}^{T_C}$，${p'_v}_{X\geq 1}^{T_C}$ を 1 とした場合が γ_n であり，それぞれ $\gamma_1 = l_{CRL}/s$，$\gamma_2 = \gamma_3 = l_{CRL}/(\beta \cdot s)$ となる．エンティティ–VA 間の網（モバイル網）の通信速度より，VA–CA 間の網（インターネット）の通信速度の方が速いという仮定より，$\beta > 1$ であるので，$\gamma_1 > \gamma_2 = \gamma_3$ という関係が成り立つ(注15)．また，γ の全体に対して占める割合を示すために，インターネット経由で 8143 [Byte] の CRL を取得する別のシステムで計測を行った．この実測では CRL 取得時間は約 106 [ms] であった．式 (6) 及び表 3 のパラメータからの計算値では，CRL のサイズは 1230 [Byte] となるため上記 106 [ms] はより小さな値になると考えられる．よって γ の有効性確認全体に占める割合そのものは小さな値であるということが確認できた．このように，今回の実測環境では CVS 方式が CRL 取得時間を含めた検証時間の評価基準で優れているということができる．また，実際には確率的に CRL 取得が発生するため，CRL 取得時間の平均値は今回の実測値より更に小さな値となる（パラメータ 1 による理論値は付録 **5.** 参照）．

4.4 証明書検証サーバの負荷に関する考察

本論文では，証明書検証サーバは十分な負荷分散がなされていることを仮定して理論式の導出を行ってきた．本節で証明書検証サーバの負荷に関する考察を行う．証明書検証サーバへの検証要求の到着はポアソン分布に従うと仮定しているので，平均到着率 $\lambda = (q \times N/Nv)/(24 \times 60 \times 60)$ の M/M/S 待ち行列として平均応答時間を求めることができる．図 11 に，表 3 のパラメータ 1 の条件で窓口数（証明書検証サーバの数）が異なる場合の平均応答時間のグラフを示す．図 11 より，例えば平均証明書検証時間が 40 [ms] の場合には，15 台の証明書検証サーバを多重化することにより性能劣化を防ぐことができるということが分かる．このように $T = R$ の直線からかけ離れない（発散しない）台数の証明書検証サーバを用意することで十分な負荷分散がなされているという仮定を満足することができ，今回導いた理論式は当てはまることになる．

(注15)：確率 1 で 1 回の CRL を取得することを考慮すると δ-CRL 方式の場合においても CRL 方式と同様に完全 CRL を 1 回取得する必要があるため，δ-CRL 方式の場合と CRL 方式の場合をともに γ_1 とおいている．

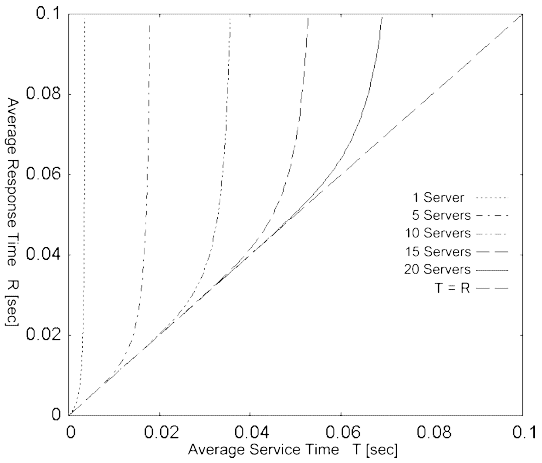

図 11 証明書検証サーバの平均応答時間
Fig. 11 The average response time.

5. むすび

証明書の検証時間という評価基準について端末の計算時間とネットワークの通信速度の関係を考慮した理論式を導出した．更に，モバイル環境における具体的なパラメータを当てはめ，各方式が適している範囲を示した．また，端末の処理時間やモバイル網の通信速度の制約以外の，失効リストを無条件に公開したくないというモバイル環境の特有の要件を満たした場合の性能に関する理論式を導き，性能劣化は極めて小さいことを示した．更に，検証要求頻度の増加に伴う VA の性能劣化に関する評価を行った．今後は，今回取り上げなかった検証時間以外の評価基準についても検討する予定である．

謝辞 本研究は，独立行政法人情報通信研究機構 (NICT) の委託研究「モバイルセキュリティ基盤技術の研究開発」の一環として行われた．

文献

[1] 田中直樹，飯野陽一郎，“PKI の証明書失効に必要な通信量の確率論的評価，” 情処学論，vol.45, no.12, pp.2824–

2833, 2004.
[2] 栢澤克之，高橋　礼，内山宏樹，坂崎尚生，笈川光浩，洲崎誠一，平澤茂一，“モバイル向け証明書検証サーバの開発,” 信学技報，IT2005-59, Sept. 2005.
[3] 栢澤克之，高橋　礼，内山宏樹，坂崎尚生，笈川光浩，洲崎誠一，平澤茂一，“モバイル向け証明書検証システムの開発と評価,” コンピュータセキュリティシンポジウム 2005 論文集，pp.121–126, Oct. 2005.
[4] 栢澤克之，笈川光浩，洲崎誠一，平澤茂一，“モバイル向け証明書検証方式の評価,” 第 28 回情報理論とその応用シンポジウム予稿集，pp.587–590, Nov. 2005.
[5] ITU-T Recommendation X.509 (2000) ISO/IEC 9594-8:2001: Information Technology — Open Systems Interconnection — The Directory: Public-key and Attribute Certificate Framework.
[6] R. Housley, T. Polk, W. Ford, and D. Solo, RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, IETF, April 2002.
[7] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, RFC 2560 - X.509 Internet Public Key Infrastructure — Online Certificate Status Protocol — OCSP, IRTF, June 1999.
[8] 政府認証基盤相互運用性仕様書，H15/12/17 改定，共通システム専門部会了承.
[9] 藤城孝宏，鍛　忠司，羽根慎吾，熊谷洋子，手塚　悟，“証明書検証サービスの開発,” 信学論（D-I），vol.J87-D-I, no.8, pp.833–840, Aug. 2004.
[10] 羽根慎吾，藤城孝宏，橋本洋子，手塚　悟，“X.509 証明書の高速認証パス検証アルゴリズム,” 情報処理学会コンピュータセキュリティ研究会研究報告書，vol.2005, no.33, pp.55–60, 2005.
[11] S. Hane, T. Fujishiro, Y. Hashimoto, T. Kaji, K. Kondo, and S. Tezuka, “Speeding up X.509 certificate path validation,” 4th International Workshop for Applied PKI, IWAP2005, 2005.
[12] 藤城孝宏，鍛　忠司，手塚　悟，“複数 PKI ドメインにおける証明書検証の高速化方式の研究,” コンピュータセキュリティシンポジウム 2002, pp.373–378, 2002.
[13] 藤城孝宏，五島裕加，手塚　悟，“政府認証基盤 (GPKI) における証明書検証方式の提案,” 信学技報，OFS 2001-81, 2001.
[14] 橋本洋子，藤城孝宏，鍛　忠司，羽根慎吾，手塚　悟，“証明書検証サービスにおける認証パスキャッシュ方式の開発,” 情処学コンピュータセキュリティ研報，vol.2005, no.70, pp.295–300, 2005.
[15] T. Fressman, R. Housley, A. Malpani, D. Cooper, and T. Polk, Simple Certificate Validation Protocol (SCVP), IETF, July 2005.
[16] モバイル・コンテンツ・フォーラム（監修），ケータイ白書 2006，インプレス，2005.

付　　録

1. CRL 取得時間の導出過程の説明

図 A·1〜図 A·4 に，それぞれのモデルにおける CRL 取得時間の導出の補足説明図を示す．なお，OCSP モデル 2 と CVS モデル 1 では CRL 取得方法は同一なので一つの図で代表する．

2. l_{CRL} の導出

証明書の失効は，失効発生頻度 p のポアソン過程に従って発生し，証明書の有効期限切れも時間的に一様に発生すると仮定する(注16)と，CRL の大きさはある時間経過後には一定の数で定常状態になると考え

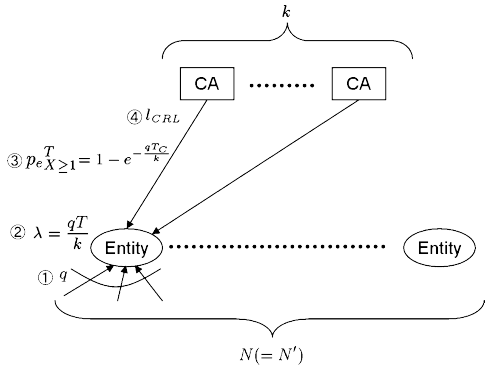

図 A·1　(δ-)CRL モデルの CRL 取得時間の導出
Fig. A·1　Derive the average of the acquirement time of CRL for (δ-)CRL model.

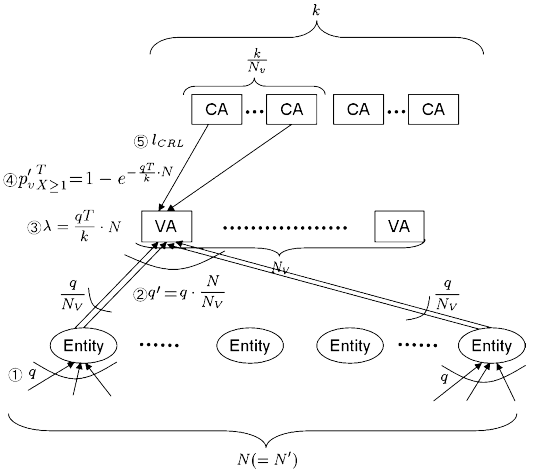

図 A·2　OCSP モデル 1 の CRL 取得時間の導出
Fig. A·2　Derive the average of the acquirement time of CRL for OCSP model 1.

(注16)：本仮定は，文献 [1] と同様の仮定である．

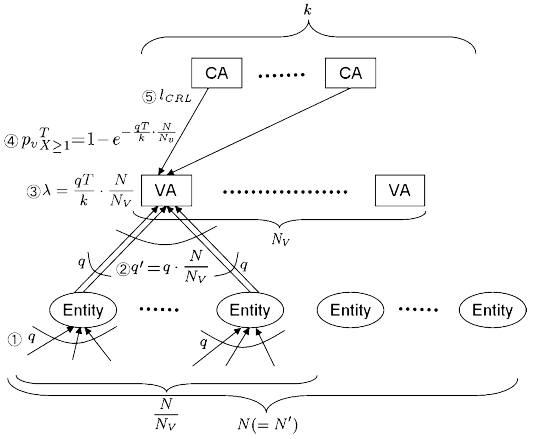

図 A·3 CVS モデル 1 と OCSP モデル 2 の CRL 取得時間の導出
Fig. A·3 Derive the average of the acquirement time of CRL for CVS model 1 and OCSP model 2.

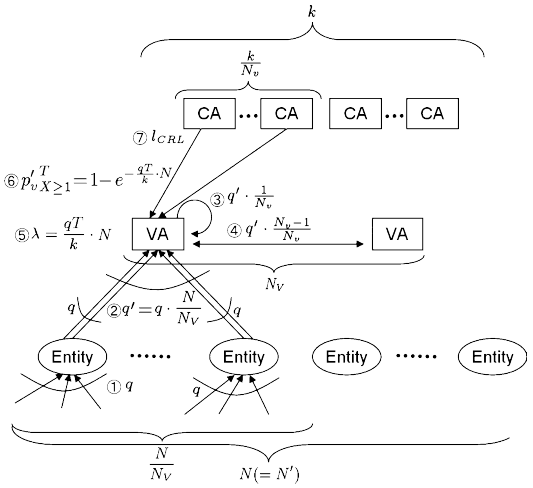

図 A·4 CVS モデル 2 の CRL 取得時間の導出
Fig. A·4 Derive the average of the acquirement time of CRL for CVS model 2.

られる．定常状態の項目数を $N_{stable}(N', L, p, k)$ とする．追加される項目数は，一つの CA について 1 日に失効される証明書の数なので $N'p/k$ [個]，除外される項目数は，有効期限が切れる証明書の数なので $N_{stable}(N', L, p, k)/L$ [個] である．定常状態では両者は等しくなるので，等号でつなぎ，$N_{stable}(N', L, p, k)$ について解くと次式を得る．

$$N_{stable}(N', L, p, k) = \frac{N'pL}{k} \qquad \text{(A·1)}$$

CRL のサイズ l_{CRL} は，項目数と項目一つ当りのサイズ l_{sn} の積と，項目によらず一定な要素のサイズ l_{sig} との和であるので式 (6) が成り立つ．

3. $l_{delta}(n)$ の導出

base-CRL 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．一つの CA について T_C 時間の間に新たに追加される項目数は，$N'pT_C/k$ [個]，除外される項目数は，P_nT_C/L [個] である．よって次式が成り立つ．

$$P_{n+1} = P_n + \frac{N'pT_C}{k} - \frac{P_nT_C}{L} \qquad \text{(A·2)}$$

初項 $P_0 = 0$ として解くと，一般項 P_n は次式で与えられる．ただし，$1 \leq n \leq T_B/T_C - 1$ である．

$$P_n = \frac{N'pL}{k}\left\{1 - \left(\frac{T_C}{L}\right)^n\right\} \qquad \text{(A·3)}$$

n 番目に発行された δ-CRL のサイズ $l_{delta}(n)$ は，項目数と項目一つ当りのサイズ l_{sn} の積と，項目によらず一定な要素のサイズ l_{sig} との和であるので式 (10) が成り立つ．

4. モバイル環境におけるパラメータ設定の根拠

以下に表 3 に示したパラメータ設定の根拠を示す．

- パラメータ 1 の認証者の数 N 及びパラメータ 2 の被検証者の数 N' は文献 [16] より 2005 年 9 月における携帯電話契約者数 89,126 千人中の携帯 IP 接続契約者数の総数である．
- パラメータ 1 の被認証者の数 N' 及びパラメータ 2 の認証者の数 N は次のように求めた．日本における会社総数は 104 万社(注17)である．また文献 [16] の資料 3-5-4 モバイルウェブサイト活用経験/活用予定項目より，商品サービスの予約，商品サービスの決済・購入，ディジタルコンテンツ販売の各サービスに関する「活用経験あり」及び「活用する予定」の割合は，それぞれ 26.0%，20.3%，14.6%である．前記 3 種のサービスは品種やコマースのフェーズが異なるので延べ総数として会社総数及び前記割合よりサービス提供者の数を求めた．
- パラメータ 1 の認証頻度 q は，文献 [16] の資料 1-6-5 パケット定額加入者の情報サービスの 1 週間の利用頻度より単純平均(注18)で 9.9 [回/週] である．更に，比較的頻度の多いユーザの平均として上位 5 割（週 5 回以上利用）のユーザの平均をとると 18.3 [回/週] である．これより 1 日の認証頻度を 3 [回/day]

(注17)：国税庁平成 16 年度会社標本調査結果による．
(注18)：週 20 回以上のレンジでは週 30 回として計算した．

と設定した．

- パラメータ 2 の認証頻度 q は，パラメータ 1 からの計算結果である．具体的にはパラメータ 1 の認証者 77,229,000 人が認証頻度 3 [回] で披検証者 633,000 [個] のサーバに検証される頻度であるため 77,229,000 × 3/633,000 より計算した．
- p，L，T_C，l_{sn}，l_{sig} は，文献 [1] と同一の値を用いた．
- 文献 [1] では，エンティティの数を N とおき，特に検証者と被検証者を分けて考えていないが，モバイル環境ではサーバの数とクライアントの数は大きく異なるので，本論文では被検証者の数を N' とし，文献 [1] におけるエンティティの数を当てはめた．
- パラメータ 1 とパラメータ 2 で N と N' が反転しているのは，前者がサーバ認証，後者がクライアント認証を評価するためのパラメータであるためである．
- CA の数 k は，クライアント認証（パラメータ 2）の場合は，通信事業者が CA となるため比較的少ない値となるが，サーバ認証（パラメータ 1）の場合は，比較的大きな値となることが予想できる．
- VA の数 N_v は，携帯通信事業者の数とした(注19)．
- D_{sn} 及び D_{sig} は，文献 [7] からの一般的な計算値である．
- D'_{sn} 及び D'_{sig} は，文献 [3] で示されているモバイル向けに最小化されたリクエストサイズの実測値である．
- T_B は，文献 [1] により示されているようにそれぞれのパラメータにおいて最適値が存在する．今回はあらかじめ全探索により最適値を求めた．
- M_1 は，検証すべき証明書はすべて認証者（検証要求者）から送信されると仮定するので認証パスの構築時間 M_1 は 0 と仮定した．
- M_3 は，有効性確認要求の生成はデータ形式の変換のみであるので 0 と仮定した．
- M_2 及び M_5 はどちらも署名の検証時間であり，M とおいた．
- M_4 の CRL の失効確認は，署名生成時間 M に対する比率を実測値より求めた．具体的には，署名検証を 6 回，CRL のチェックを 3 回，署名生成を 1 回行うシステムにおいて，すべての処理を行う (A)，署名検証を行わない (B)，署名生成のみを行う (C) のそれぞれの速度を計測した．A: 1/7，B: 1/18，C: 1/25（無単位）という速度であった．これより 1 回の署名検証時間と 1 回の CRL 検証時間は 1 : 0.356 となる．定常状態での CRL のサイズ l_{CRL} は，式 (6) 及び表 3 より，$l_{CRL} = 9843$ [bit] となるので，上記結果はほとんど CRL のサイズにはよらないと考えられる．

(注19)：仮想移動体サービス事業者 (MVNO) 等が増える可能性もあり若干現状より大きめの値とした．

5. CRL の平均取得時間の理論値

式 (5)，(7)，(11)，(12) にパラメータ 1 を当てはめると各方式における CRL の平均取得時間は下記のようになる．

$$C_{CRL} = 340.75\,[\mathrm{ms}] \quad \text{(A·4)}$$

$$C_{deltaCRL} = 277.03\,[\mathrm{ms}] \quad \text{(A·5)}$$

$$C_{OCSP1} = 7.37 \times 10^{-6}\,[\mathrm{ms}] \quad \text{(A·6)}$$

$$C_{OCSP2} = 7.37 \times 10^{-5}\,[\mathrm{ms}] \quad \text{(A·7)}$$

$$C_{CVS1} = 7.37 \times 10^{-5}\,[\mathrm{ms}] \quad \text{(A·8)}$$

（平成 18 年 5 月 18 日受付，8 月 23 日再受付）

梅澤　克之

1996 早稲田大学大学院理工学研究科機械工学専攻修士課程了．同年（株）日立製作所システム開発研究所入所．以来，分散オブジェクトシステム，モバイルセキュリティ技術，スマートカードセキュリティ技術などの研究・開発に従事．情報処理学会員．

笈川　光浩

1998 上智大学大学院理工学研究科電気・電子工学専攻博士前期課程了．同年（株）日立製作所システム開発研究所入所．以来，セキュリティ技術の研究・開発，特に電子認証の研究・開発に従事．

洲崎　誠一

1991 横浜国大・電子情報卒．同年 4 月（株）日立製作所システム開発研究所に入所．以来，情報セキュリティ技術の研究開発に従事．工博．情報処理学会会員．1996 情報処理学会第 52 回全国大会優秀賞，平 12 年度山下記念研究賞受賞．

手塚　悟

1984 慶大・工・数理卒．同年（株）日立製作所マイクロエレクトロニクス機器開発研究所を経て，現在，システム開発研究所セキュリティシステム研究センタ勤務．パーソナルコンピュータのオペレーティング・システム，デバイス・ドライバ，LAN システムの研究を経て，現在，セキュリティシステム，特に電子認証の研究開発に従事．工博．

平澤　茂一　（正員：フェロー）

1961 早大・理工・数学卒．1963 同電気通信卒．同年三菱電機（株）入社．1981 早稲田大学理工学部工業経営学科（現経営システム工学科）教授．現在に至る．情報理論とその応用，データ伝送方式，並びに計算機応用システムの開発などの研究に従事．工博．1979 UCLA 計算機科学科客員研究員．1985 ハンガリー科学アカデミー，1986 伊トリエステ大学客員研究員．1993 本会小林記念特別賞，業績賞受賞．1997 IEEE Fellow，2001 本会フェロー，情報理論とその応用学会，人工知能学会，情報処理学会，ACM 等各会員．