社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
IT2005-59 (2005-09)

モバイル向け証明書検証サーバの開発

梅澤 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[††]

† (株) 日立製作所 システム開発研究所 〒212-8567 神奈川県川崎市幸区鹿島田 890 日立システムプラザ新川崎
†† 早稲田大学大学院理工学研究科 〒169-8555 東京都新宿区大久保 3-4-1
E-mail: †{ume,aytkhs,uchiyama,sakazaki,moikawa,susaki}@sdl.hitachi.co.jp,
††hirasawa@hirasa.mgmt.waseda.ac.jp

あらまし 通信相手の正当性を確認するためには，公開鍵証明書を厳密に検証することが必須である．証明書の有効性確認の方式は，CRL 方式や，OCSP 方式，CVS 方式などいくつか提案されている．本報告では，上記 3 方式のシステム全体としての通信量の理論式を導出し，モバイル環境における 3 方式の通信量の振る舞いを示す．さらに，そこで得られた知見を元に開発したモバイル向け証明書検証システム（プロトタイプ）の概要を述べ，実測値を評価する．
キーワード モバイル PKI, 証明書検証サーバ，有効性確認，CRL，OCSP，CVS

Development of certificate verification system for mobile services

Katsuyuki UMEZAWA[†,††], Aya TAKAHASHI[†], Hiroki UCHIYAMA[†], Hisao SAKAZAKI[†],
Mitsuhiro OIKAWA[†], Seiichi SUSAKI[†], and Shigeichi HIRASAWA[††]

† Hitachi, Ltd. Systems Development Laboratory Hitachi System Plaza Shinkawasaki, 890, Kashimada, Saiwai-ku, Kawasaki-shi, Kanagawa, 212-8569
†† Graduate School of Science & Engineering, Waseda University 3-4-1, Okubo, Shinjuku-ku, Tokyo 169-8555
E-mail: †{ume,aytkhs,uchiyama,sakazaki,moikawa,susaki}@sdl.hitachi.co.jp,
††hirasawa@hirasa.mgmt.waseda.ac.jp

Abstract It is indispensable to verify a public key certificate strictly in order to check a communication partner's justification. As for the system of a validity check of a certificate, CRL system, OCSP system, CVS system, etc. are proposed partly. This report draws the theoretical formula of the amount of communications as the whole system of those three systems, and shows behavior of the amount of communications of those three systems in mobile environment. In addition, the outline of the certificate verification system for mobile (prototype) that developed based on the acquired knowledge is described, and an actual measurement is evaluated.
Key words mobile PKI, Certificate verification, CRL, OCSP, CVS

1. まえがき

モバイル環境において ID/Password に変わる PKI 認証基盤が整いつつある．携帯端末等を用いたモバイル情報通信サービスにおいて，通信相手の正当性を確認するためには，公開鍵証明書（以下証明書）を厳密に検証することが必須である．証明書の有効性確認の方式は，CRL 方式や，OCSP 方式，CVS 方式などいくつか提案されている．本報告では，上記 3 方式の，システム全体としての通信量の理論式を導出し，モバイル環境における 3 方式の通信量の振る舞いを示す．さらに，そこで得られた知見を元に開発したモバイル環境向けに最適化した証明書検証システムの概要を述べる．以下では，まず，2 章で現状の証明書の有効性確認方式について説明する．次に，3 章でシステム全体としての通信量の理論式を導出し，4 章で開発したモバイル向け証明書検証システムの概要を示す．さらに 5 章で評価を行い，6 章でまとめと今後の課題を示す．

2. 従来技術

証明書検証者が行う検証手順は，以下に示すように，「認証パスの構築」「認証パスの検証」「証明書の有効性確認」の3つに大別される．

2.1 認証パスの構築

「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．検証者がリポジトリにアクセスして必要な証明書を取得する方式か，署名者が送付する署名データに証明書群を添付する方式がとられる．

2.2 認証パスの検証

「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主に以下の項目を実施することである．

- 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
- 検証対象証明書の証明書ポリシーが検証者の受入可能な証明書ポリシーに適合していること
- 検証日時が証明書の有効期間内であること
- 認証パス中の証明書が証明書の拡張部分に記載された各種制約条件に違反していないこと

2.3 有効性確認

証明書を厳密に検証するために，上記「認証パスの検証」以外に，認証パス中の証明書が失効されていないことを確認する必要がある．これを「証明書の有効性確認」という．「証明書の有効性確認」の方法としては，CRL(Certificate Revocation List) 方式[2],[3] や，OCSP(Online Certificate Status Protocol) 方式[4]，CVS(Certificate Validation Server) 方式[5] などがある(注1)．

2.3.1 CRL 方式

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 (CA) 単位で発行・管理される．ある証明書が有効であるかどうかを知りたい場合，その証明書を発行した認証局のリポジトリから CRL をダウンロードして，CRL 内にその証明書のシリアル番号が記載されているかどうかを確認することで判断できる．CRL 内にシリアル番号が記載されていなければ，証明書は失効されていないことになる．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，δ-CRL 方式がある(注2)．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．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．

(注1)：この他に SCVP 方式[6] があるが，現在ドラフト版のため今回の評価からは除外する．

(注2)：この他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，特定の機関が，複数の CA から発行された CRL をまとめて，1 つの CRL として発行する間接 CRL 方式，ハッシュツリーを用いて失効情報を表現する証明書失効ツリー (CRT:Certificate Revocation Tree) 方式などがある．

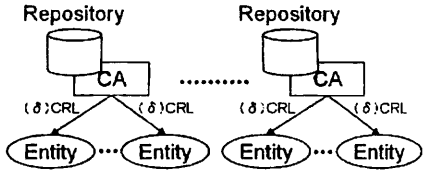

図 1 (δ-)CRL 方式の評価モデル
Fig. 1 Evaluation model for (δ-)CRL system

2.3.2 OCSP 方式

上述の CRL 方式とは別の証明書有効性確認方法として，OCSP 方式がある．OCSP とは，証明書の有効性を，OCSP レスポンダとよばれるサーバにオンラインで問い合わせるためのプロトコルである．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 ID 等）を指定すると，その応答として，有効 (good)，失効 (revoked)，不明 (unknown) の 3 つのいずれかが返信される．

2.3.3 CVS 方式

CRL 方式や OCSP 方式は，証明書の有効性確認を行うための手段であり，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・検証および認証パス中の全証明書の有効性確認を代行する方式である．検証者が，検証サーバ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．

3. システム全体での通信量

本章では，各方式におけるシステム全体での通信量の理論式を導出する．

3.1 CRL 方式の通信量

文献[1] では，オフライン型，つまり，CRL 方式および δ-CRL 方式を用いた場合のシステム全体としての通信量を評価している．文献[1] での評価モデルを図 1 に示す．さらに，評価に必要なパラメータを以下に示す．

p ：1 つの証明書が 1 日に失効される平均回数（失効発生頻度）[回/day]

N ：Entity(認証者) の数 [個]

N' ：被認証者の数 [個]

k ：CA の数 [個]

q ：1 つの Entity が，1 日に認証される平均個数（認証頻度）[回/day・個]

T_C ：完全 CRL 方式での完全 CRL，および，δ-CRL 方式での δ-CRL の発行間隔 [day]

T_B ：δ-CRL 方式の base-CRL の発行間隔 [day]

L ：証明書の有効期間 [day]

l_{sn} ：CRL の項目 1 つあたりのビット数 [bit]

l_{sig} ：CRL の項目数によらない要素（CA の電子署名や発効日など）のビット数 [bit]

文献 [1] では，完全 CRL 方式および δ-CRL 方式での通信量の合計を下記のように導き出している．ただし，文献 [1] では，認証者（証明書を検証する人）と被認証者（証明書を提示する人）を同一として扱いその数を N と置いているが，モバイル環境では認証者と被認証者の数が極端に異なることが想定されるので，認証者と被認証者の数を分け，それぞれ N,N' とした．

(1) 完全 CRL 方式での通信量の合計

$$L_{CRL} = k \cdot N \cdot P(X \geq 1)\big|_{T=T_C} \cdot l_{CRL} \cdot \frac{1}{T_C} = \frac{1}{T_C} \cdot A \cdot N \cdot \left(1 - e^{-\frac{qT_C}{k}}\right) \quad (1)$$

ただし，

$$A = N'pL \cdot l_{sn} + k \cdot l_{sig} \quad (2)$$

(2) δ-CRL 方式での通信量の合計

$$L_{deltaCRL} = \frac{N}{T_B} \cdot A \cdot \left(1 - e^{-\frac{qT_B}{k}}\right) + \frac{N}{T_B} \sum_{n=1}^{\frac{T_B}{T_C}-1} F(n) \cdot \left(1 - e^{-\frac{qT_C}{k}}\right) \quad (3)$$

ただし，

$$A = N'pL \cdot l_{sn} + k \cdot l_{sig} \quad (4)$$

$$F(n) = N'pL\{1 - (1 - T_C/L)^n\} \cdot l_{sn} + k \cdot l_{sig} \quad (5)$$

さらに文献 [1] では，δ-CRL 方式の場合，最適となる base-CRL の発行間隔 T_B^* の存在を示し，$\partial L_{deltaCRL}/\partial T_B = 0$ を満たす T_B を Newton-Raphson 法による数値計算によって求めている．

3.2 CVS 方式の通信量

まずモデルを定義する．図 2 に示すように認証を行う（証明書の有効性確認を行う）Entity は証明書検証者 (VA) に対して有効性確認の要求を行う．VA は CA から (δ-)CRL を取得し，それを用いた有効性確認を行い結果を Entity に返す．証明書検証に必要なシステム全体の通信量 L_{CVS} は下記の式で表せる．

$$L_{CVS} = L^{CA-VA} + L^{VA-E} \quad (6)$$

ただし，L^{CA-VA} は CA-VA 間の通信量，L^{VA-E} は，VA-E 間の通信量である．

3.2.1 CA-VA 間が完全 CRL 方式の場合の通信量 L_{CRL}^{CA-VA}

まず，CA-VA 間が完全 CRL 方式の場合の通信量 L_{CRL}^{CA-VA} を評価する(注3)．複数グループからの客の到着がポアソン過程に従っているとき，合計した客の到着もポアソン過程に従うことが知られている．よって，ある検証者が，ある CA に属する

(注3)：VA が CA と一体化し CRL の配布が必要ない場合も考えられるが，今回の評価は最悪のケースを考えることとした．

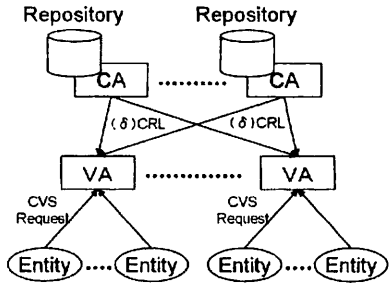

図 2 CVS 方式の評価モデル

Fig. 2 Evaluation model for CVS system

Entity を認証する回数は，$\lambda = qT/k$ のポアソン分布に従うと考えられるので，その Entity から VA への証明書検証要求回数は，$\lambda = qT/k \cdot N/N_V$ のポアソン分布に従うと考えられる．よって VA が時間 T の間に 1 回以上証明書の検証を行う確率 $P(X \geq 1)$ は，以下で与えられる．

$$P(X \geq 1) = \sum_{X=1}^{\infty} P(X) = 1 - P(0)^{-\frac{qT}{k} \cdot \frac{N}{N_V}} \quad (7)$$

式 1 における Entity の数 N を，VA の数 N_V で置き換えることにより CA-VA 間の完全 CRL の通信量が求まる．

$$L_{CRL}^{CA-VA} = k \cdot N_V \cdot P(X \geq 1)\big|_{T=T_C} \cdot l_{CRL} \cdot \frac{1}{T_C} = \frac{1}{T_C} \cdot A \cdot N_V \cdot \left(1 - e^{-\frac{qT_C}{k} \cdot \frac{N}{N_V}}\right) \quad (8)$$

ただし，

$$A = N'pL \cdot l_{sn} + k \cdot l_{sig} \quad (9)$$

3.2.2 CA-VA 間が δ-CRL 方式の場合の通信量 $L_{deltaCRL}^{CA-VA}$

次に，CA-VA 間が δ-CRL 方式の場合の通信量 $L_{deltaCRL}^{CA-VA}$ を導出する．前節の L_{CRL}^{CA-VA} の場合と同様に，Entity から VA への証明書検証要求回数は，$\lambda = qT/k \cdot N/N_V$ のポアソン分布に従うと考えられる．よって，次式が成り立つ．

$$L_{deltaCRL}^{CA-VA} = \frac{N_V}{T_B} \cdot A \cdot \left(1 - e^{-\frac{qT_B}{k} \cdot \frac{N}{N_V}}\right) + \frac{N_V}{T_B} \sum_{n=1}^{\frac{T_B}{T_C}-1} F(n) \cdot \left(1 - e^{-\frac{qT_C}{k} \cdot \frac{N}{N_V}}\right) \quad (10)$$

ただし，

$$A = N'pL \cdot l_{sn} + k \cdot l_{sig} \quad (11)$$

$$F(n) = N'pL\{1 - (1 - T_C/L)^n\} \cdot l_{sn} + k \cdot l_{sig} \quad (12)$$

3.2.3 VA-E 間の通信量 L_{CVS}^{VA-E}

証明書を含む CVS リクエストのビット数を D[bit] とすると，N 個のエンティティが単位時間 [day] あたりに送信する CVS リクエストの総量 L_{CVS}^{VA-E} は下記のようになる．

$$L_{CVS}^{VA-E} = D \cdot q \cdot N \quad (13)$$

3.2.4 CVS 方式の通信量

以上をまとめると，CA-VA 間が完全 CRL 方式の場合の通信量 L_{CVS1} と CA-VA 間が *delta*-CRL 方式の場合の通信量 L_{CVS2} は，それぞれ下記のようになる．

$$\begin{aligned} L_{CVS1} &= L_{CRL}^{CA-VA} + L_{CVS}^{VA-E} \\ &= \frac{1}{T_C}(N'pL \cdot l_{sn} + k \cdot l_{sig}) \cdot N_V \\ &\quad \cdot \left(1 - e^{-\frac{qT_C}{k} \cdot \frac{N}{N_V}}\right) \\ &\quad + D \cdot q \cdot N \end{aligned} \tag{14}$$

$$\begin{aligned} L_{CVS2} &= L_{deltaCRL}^{CA-VA} + L_{CVS}^{VA-E} \\ &= \frac{k}{T_B} \cdot A \cdot \left(1 - e^{-\frac{qT_B}{k} \cdot \frac{N}{N_V}}\right) \\ &\quad + \frac{k}{T_B} \sum_{n=1}^{\frac{T_B}{T_C}-1} F(n) \cdot \left(1 - e^{-\frac{qT_C}{k} \cdot \frac{N}{N_V}}\right) \\ &\quad + D \cdot q \cdot N \end{aligned} \tag{15}$$

3.3 OCSP 方式の通信量

OCSP 方式は，図 2 のモデルにおいて，Entity から CA への問い合わせが，OCSP リクエストになることのみ異なる．よって，OCSP 方式の通信量は，式 14 および式 15 の D を，OCSP リクエストのサイズ D' で置き換えたものとなる．

3.4 通信量の評価と考察

携帯端末がサーバを認証するときの通信量を評価するにあたり，表 1 のようにパラメータを設定した．パラメータ 1 は N_V, D, D' 以外は文献 [1] と同一の値である．またパラメータ 2 は現状のモバイル環境における実測値に近い値を用いた．パラメータ 2 に関するモバイル環境の特徴は，携帯端末において証明書の検証が行われる(注4)ため，その数 N がかなり大きくなること，携帯端末からの有効性確認は，通信事業者へ問い合わせが行われることが予想されるため VA の数 N_V がかなり小さくなること，様々クライアントから接続要求があるサーバと異なり，携帯端末を有するユーザ自らが接続要求を行ったときに認証が行われるので，認証頻度 q は比較的小となることなどが挙げられる．

パラメータ 1 のとき認証頻度 q を変化させた場合の通信量の関係を図 3 に，パラメータ 2 のときの関係を図 4 に示す．これらのグラフより以下のことがわかる．

- モバイル環境では OCSP 方式と CVS 方式の CA-VA 間の CRL(δ-CRL) の通信量はシステム全体として見たときにはほとんど影響しない．
- CVS 方式の通信量は CVS リクエストのビット数 D に比例するので，そのサイズを小さくすることが重要．

4. モバイル向け証明書検証システムの提案

4.1 モバイル向けアプローチ

モバイル環境では，複数の通信事業者が認証局を設置し，それぞれが独立して，各証明書を発行するものと想定される．そのため，どの通信事業者の認証局が発行した証明書でも同じように検証できる仕組みが有用である．また，文献 [3] では，検証するアプリケーションがサポートすべき範囲を規定している

(注4)：携帯端末をサーバが認証する場合のあるが今回は携帯端末が検証を行う際の評価に限る．

表 1 評価用パラメータ

Table 1 Parameters for evaluation

	パラメータ 1	パラメータ 2
Entity(認証者) の数 N[個]	3,000,000	87,000,000
被認証者の数 N'[個]	3,000,000	3,000,000
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 1 つあたりサイズ 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	500
VA の数 N_V[個]	300,000	10
CVS リクエストサイズ D[bit]	20,464	20,464
OCSP リクエストサイズ D'[bit]	1,336	1,336

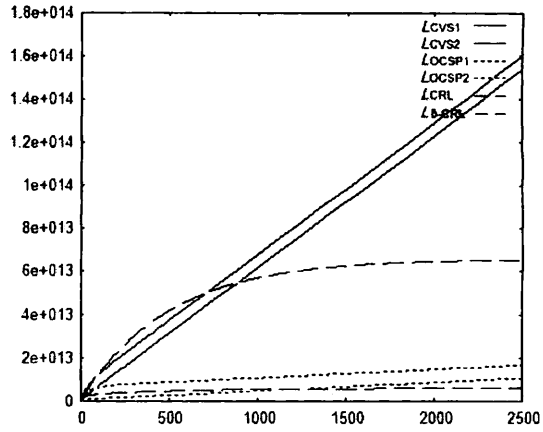

図 3 パラメータ 1 のときの各方式の通信量

Fig. 3 Amount of communication of each method at parameter 1

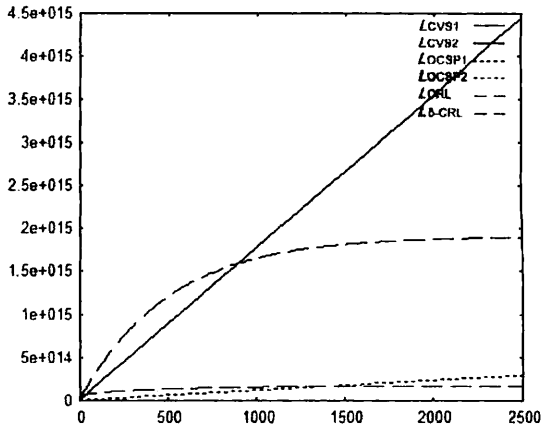

図 4 パラメータ 2 のときの各方式の通信量

Fig. 4 Amount of communication of each method at parameter 2

が，非力な携帯端末において証明書の検証や有効性確認等の処理をPCと同様に実装することは現実的ではない．更に，証明書の有効性確認を行う際，検証者側は多数の認証局へのアクセスが必要となり，ネットワークに負荷がかかる．そのため，検証者側のコスト高や通信の中断等が起こり，ユーザにとっても通信事業者にとっても大きなデメリットとなる．以上のことから，モバイル環境における証明書の検証では，複雑な証明書の検証を検証者に代わって行う証明書検証サーバが必要となる．その際，前節までの結果からもわかるように，証明書の有効性確認のための通信量は有効性確認要求のビット数に比例するので，そのサイズをできるだけ小さくすることが最も重要であるといえる．

4.2 モバイル向け証明書検証要求・応答フォーマット

証明書検証要求フォーマットや証明書検証プロトコル等，モバイル環境に適した方式の検討を行い，できるだけサイズを小さくするために冗長なデータを省いたモバイル向けの証明書の有効性確認要求・応答フォーマットを定義した．検証者がCVSに対して送信する要求メッセージを表2に，CVSが検証者に対して返信する応答メッセージを表3に示す．表3のハッチングの項目はCVSサーバのポリシーにより省略可能であることを示している．

表2 CVS要求メッセージのフォーマット
Table 2 Request data format

フィールド	データ型	設定値の例
(OCSP Request)	SEQUENCE	(OCSP要求)
(Extensions)	SEQUENCE SIZE (1..MAX) OF	(拡張群) ※本フィールド配下には，必要な個数分の拡張が列挙される
(SubscriberCert)	SEQUENCE	(SubscriberCert拡張) ※CVSでは，本拡張は必須項目である
extnValue	OCTET STRING	SubscriberCert拡張の値 (検証対象証明書)
(IntermediateCerts)	SEQUENCE	(IntermediateCerts拡張) ※CVSでは，本拡張はオプション項目である．また，本拡張は複数指定可能である．複数指定する場合，認証パスのトラストアンカー証明書に近い順に指定する
extnValue	OCTET STRING	応答ステータスを必要者の秘密鍵で署名した値
(TrustAnchorCert)	SEQUENCE	(TrustAnchorCert拡張) ※CVSでは，本拡張はオプション項目である．本フィールドが省略された場合，CVSで設定されているルートCA証明書をトラストアンカーとして処理される
extnValue	OCTET STRING	TrustAnchorCert拡張の値 (トラストアンカー証明書)

表3 CVS応答メッセージのフォーマット
Table 3 Response data format

フィールド	データ型	設定値の例
(OCSP Response)	SEQUENCE	(OCSP応答)
responseStatus	ENUMERATED	応答ステータス ※以下のいずれかの値が記載される． successful(0) malformedRequest(1) internalError(2) tryLater(3) sigRequired(5) unauthorized(6)
signatureAlgorithm	SEQUENCE OPTIONAL	(署名アルゴリズム(*))
algorithm	OBJECT IDENTIFIER	署名アルゴリズムのオブジェクト識別子
Parameters	ANY	署名アルゴリズムに必要なパラメータ
signature	BIT STRING	応答ステータスを応答者の秘密鍵で署名した値
certs	[0]EXPLICIT OPTIONAL	(証明書群)
(*)	SEQUENCE OF	(証明書群) ※本フィールドの配下には，署名検証に必要な認証パス中の証明書が格納される
(Certificate)	Certificate	上記署名値の検証に必要な公開鍵証明書
:	:	:

4.3 モバイル用の検証プロトコル

検証要求プロトコルとしては，現状の多くの携帯端末でサポートされているHTTPプロトコルのPOSTメソッドを用いることとした．

4.4 証明書検証システム構成要素

以下の3つの構成要素についてプロトタイプの開発を行った．

- 証明書検証サーバ (CVS)
- サービス提供者側の検証モジュール
- 携帯端末側の検証モジュール

「モバイル向け証明書検証サーバ (CVS)」に関しては，複数の認証局が発行した証明書に対し，検証するために必要な認証パスの構築を行う機能，非力な携帯端末に代わり文献[3]に則した認証パスの検証を行う機能，多数の認証局へのアクセスを代行し，検証対象の証明書をはじめ認証パスを構成する全ての証明書の有効性検証を行う機能等を実現した．

「サービス提供者側の検証モジュール」については，署名を検証する機能とCVSにアクセスする機能を実現した．また，複数の通信事業者がCAおよびCVSをそれぞれ独立に設置するモデルにおいては，携帯端末から受け取った各証明書を各通信事業者のCVSに適切に振り分ける必要が生じるため，本開発では，サービス提供者側の検証モジュールにおいて各公開鍵証明書を適切に振り分ける機能も実現した．

「携帯端末側の検証モジュール」については，処理速度・メモリ容量・通信速度・通信安定性・バッテリー容量等のモバイル特有の制約を考慮する必要がある．そのため，非力な携帯端末上で動作する検証モジュールを開発した．具体的には，4.2節で示したように，証明書の検証に必要な最低限の情報をモバイル向けCVS検証要求フォーマットとし，CVSにアクセスする機能を実現した．

4.5 システム構成

通信事業者がCVSを設置し，携帯端末がサービス提供者の証明書を検証する場合のシステム構成を図5に示す．携帯端末は，サービス提供者の証明書を受信し，携帯端末内の検証モジュール（CVSクライアント）から，通信事業者のCVSに対して証明書を送信する．CVSは，サービス提供者用のCAリポジトリに対してCRLの要求を行ない証明書の検証を行う．

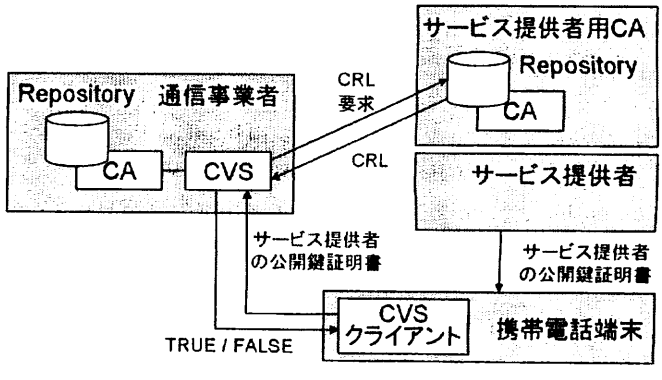

図5 システム構成の概要
Fig. 5 Outline of system configuration

また，図6に携帯端末での検証モジュールの動作画面を示す．ブラウザに組み込みSSL認証時にCVSへの問い合わせが行われる．

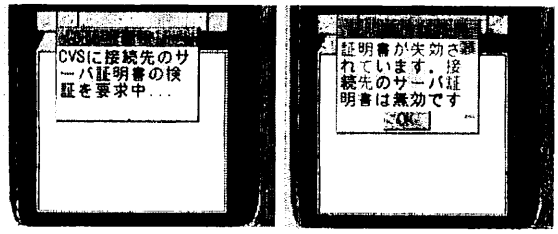

図6　証明書検証モジュールを組み込んだ携帯用ブラウザ
Fig. 6　Mobile browser with certificate verification module

5. 評　　価

5.1 理論式による評価

証明書のサイズを800[byte]，CAの階層数を3階層と仮定すると，従来法[5]の要求メッセージのサイズは20464[bit]，4.2節で示したそれは19456[bit]となり，約5%縮小できた．パラメータ2および$D = 19456$としたときの認証頻度qが小さい範囲の振る舞いを図7に示す．認証頻度が小さいときには，CRL方式およびδ-CRL方式よりも，本CVS方式のほうが，システム全体としての通信量は小さくなることが確認できた．

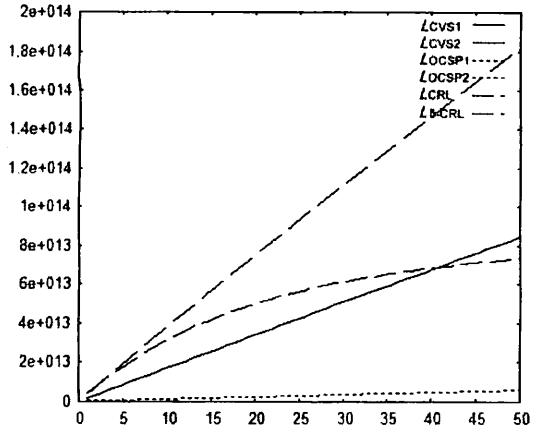

図7　qが小さいときの各方式の通信量
Fig. 7　Amount of communication when value of q is small

5.2 実測値の評価

クライアントとしてCDMA 1x WIN規格の携帯電話機(BREW端末)，サーバとしてCPUにIntel(R) Pentium(R) 4プロセッサ3.4GMHz，メモリ2GB，OSにWindows(R) XP operating systemを搭載したコンピュータで実装したモバイル向け証明書検証システム（プロトタイプ）の性能評価を行った．またこのときの証明書のサイズは，ルートCA証明書568[byte]，検証対象証明書1108[byte]である．表4にサーバの処理時間(注5)，通信時間，および携帯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レスポンス時間を示す．なお表4の数値は100回行った平均値である．

(注5)：プロトタイプの性能であり最適化によりさらなる高速化は可能である．

表4　証明書有効性確認の性能評価
Table 4　Performance evaluation of certificate verification

処理内容	時間 (ms)
サーバの処理時間	2013.89
通信時間	2220.37
合計（携帯端末におけるレスポンス時間）	4234.26

6. まとめと今後の課題

証明書有効性確認の3方式のシステム全体としての通信量の理論式を導出し，モバイル環境における通信量の振る舞いを示した．それに基づき要求フォーマットサイズを縮小したモバイル向け証明書検証システム（プロトタイプ）を開発し，実測値を評価した．

証明書の有効性確認の性能は，今回示したようなシステム全体としての通信量のみでは表しきれない．今後は，携帯端末およびサーバでの計算量を含めた理論式を導出し性能評価を行う予定である[7][8]．

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」の一環として行なわれた．

文　　献

[1] 田中，飯野，"PKIの証明書失効に必要な通信量の確率論的評価"，情報処理学会論文誌，Vol.45 No.12, (2004).
[2] *ITU-T Recommendation X.509 (2000)—ISO/IEC 9594-8:2001: Information Technology - Open Systems Interconnection - The Directory: Public-key and Attribute Certificate Framework*
[3] 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.
[4] 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.
[5] 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．
[6] T.Fressman, R.Housley, A.Malpani, D.Cooper and T.Polk: *Simple Certificate Validation Protocol (SCVP)*, IETF, July. 2005.
[7] 梅澤，高橋，内山，坂崎，笈川，洲崎，平澤，"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，予稿集，October 2005（予定）．
[8] 梅澤，笈川，洲崎，平澤，"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，November 2005（予定）．