The 28th Symposium on Information Theory
and Its Applications (SITA2005)
Onna, Okinawa, Japan, Nov. 20-23, 2005

モバイル向け証明書検証方式の評価

Evaluation of certificate verification method in mobile environment

梅澤 克之*† 笈川 光浩† 洲崎 誠一† 平澤 茂一*
Katsuyuki Umezawa Mitsuhiro Oikawa Seiichi Susaki Shigeichi Hirasawa

Abstract— The PKI certification foundation which changes from ID/Password in a mobile environment service is being completed. It is indispensable to verify a public key certificate strictly in order to check a communication partner's justification in a mobile telecommunication service using such as a cellular phone terminal. As for the system of a validity check of a certificate, CRL system, OCSP system, CVS system, etc. are proposed. However, we show CVS system is the most suitable for mobile environment, and developed the certificate verification system for mobile which optimized the conventional CVS system for mobile environment. This report shows the further restriction of the mobile environment, and shows the performance degradation is the minimum by drawing the theoretical formula about the performance at the time of filling the restriction.

Keywords— Mobile, PKI, Certificate, Verification, CRL, OCSP, CVS

1 はじめに

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が，報告者らは，文献[1][2]でCVS方式がモバイル環境に適していることを示し従来のCVS方式をモバイル環境向けに最適化したモバイル向け証明書検証システムを開発した．本報告では，さらなるモバイル環境の要件（制限）を示し，その制限を満たした場合の性能に関する理論式を導き，性能劣化は極小であることを示す．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記述し，3章でモバイル環境特有の制約について述べる．4章で1回の認証に必要な平均検証時間の理論式を導出し，モバイル環境のパラメータで評価する．さらに5章でまとめと今後の課題を示す．

* 〒169-8555 東京都新宿区大久保 3-4-1, 早稲田大学大学院理工学研究科, Graduate School of Science & Engineering, Waseda University, 3-4-1 Okubo Shinjuku-ku Tokyo, 169-8555 Japan.
† 〒212-8567 神奈川県川崎市幸区鹿島田 890 日立システムプラザ,（株）日立製作所 システム開発研究所, Hitachi Ltd., Systems Development Laboratory, Hitachi System Plaza Shinkawasaki, 890 Kashimada, Saiwai-ku, Kawasaki-shi, Kanagawa, 212-8567 Japan.

2 従来技術

証明書検証者が行う検証手順は，大きく，「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つである．

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，主に以下の項目を実施する必要がある．

- 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

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有効性確認が必要である．「証明書の有効性確認」の方法には，CRL (Certificate Revocation List) 方式[4][5]や，OCSP (Online Certificate Status Protocol) 方式[6]，CVS (Certificate Validation Server) 方式[7]などがある[1]．以下にその概要を示す．

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

[1] この他にSCVP方式[8]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．

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[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．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．

2.3.2 OCSP 方式

OCSP 方式とは，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 ID 等）を送付すると，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・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，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 モバイル特有の要件

モバイル環境において，証明書の検証を行う主体（ユーザあるいはサービス提供者），および検証を代行する証明書検証サーバの設置場所（通信事業者内あるいは第三者環境等）という観点から，証明書の検証モデルの整理を行った結果を図 1 に示す．

モバイル通信事業者が認証局を運営し，携帯電話端末に対して証明書を発行する場合，その失効リストは，契約者の契約解除を意味するため，失効リストを他の通信事業者に洩らしたくないという制約がある．この制約を満たすために，証明書検証サーバ同士で連携し，結果のみ通知しあう方式を実装しシステムに適用した．

[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，間接 CRL 方式，証明書失効ツリー (CRT:Certificate Revocation Tree) 方式などがある．

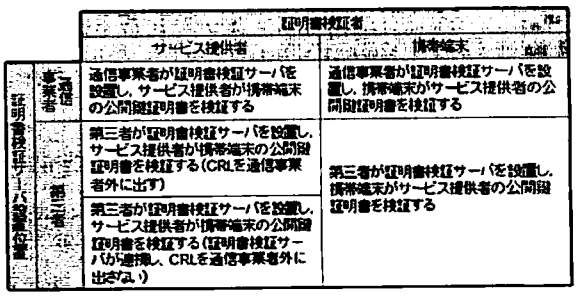

図 1: 証明書検証モデルの分類

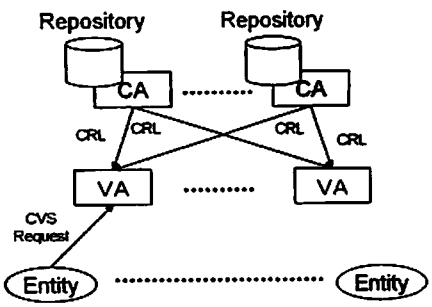

図 2: CVS モデル 1

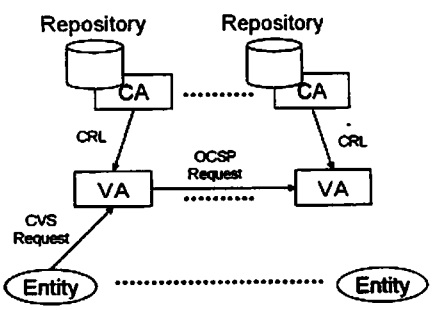

図 3: CVS モデル 2

4 1 回の認証にかかる平均検証時間

本節では，ある Entity が 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）を評価する．

4.1 モデルの定義

まずモデルを定義する．図 2 に従来の CVS 方式 (CVS モデル 1)，図 3 に検証期間 (VA) 同士が連携する CVS 方式 (CVS モデル 2) を示す．図 2 と図 3 の違いは，図 2 では VA がすべての CA から CRL を取得するのに対して，図 3 では，VA は一部の CA (k/N_v) から CRL を取得し，残りの CA が発行した証明書の検証に関しては VA-VA 間で OCSP 方式の問い合わせが発生する点である．

4.2 CRLの平均取得時間

あるVAがN/N_v個のEntityから直接受け取るリクエストの頻度は$q' = \frac{q \cdot N}{N_v}$である．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，残りの$q' \cdot \frac{N_v - 1}{N_v}$は他のVAに依頼する．このとき他のVAから同数の依頼が寄せられることになる．結局，Entityおよび他の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．CVSモデル2では，$k/N_v$個のCAに属するEntity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Entityを認証する回数の期待値は$qT/k \cdot N$回となる．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下記で表せる．

$$p'^{T}_{vX \geq 1} = 1 - e^{-\frac{qT}{k} \cdot N} \tag{1}$$

1回の認証に必要なCA-VA間でのCRL取得に要する平均時間C_{CVS2}は，下記のように表せる．

$$C_{CVS2} = \frac{\frac{k}{N_v} \cdot k \cdot p'^{T_C}_{vX \geq 1} \cdot l_{CRL}}{T_C \cdot q' \cdot \beta s} \tag{2}$$

ただし，q'は1つのVAが1日に行う検証回数の平均回数であり$q' = \frac{q \cdot N}{N_v}$である．また，$\beta(\geq 1)$は，VA-Entity間（モバイル網）の通信速度に対するVA-VA間（バックエンド）の通信速度の倍率である．また，l_{CRL}は，1つのCAが一回に発行するCRLのサイズであり文献[3]より

$$l_{CRL} = \frac{N'pL}{k} \cdot l_{sn} + l_{sig}[bit] \tag{3}$$

である．

4.3 証明書検証時間

相手から証明書を受け取ったEntity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

CVSモデル2では，VAにおいて(1)，(2)および(4)の処理を$\tau - 1$回行う必要がある．また端末において(3)および(5)の処理を，1回行う必要がある．1回の認証にかかる計算時間M_{CVS2}は下記のように表せる．

$$M_{CVS2} = (\tau - 1)(\alpha M + \alpha M'') + M' \tag{4}$$

ただし記号の意味は下記である．

M :Entity端末における認証パスの構築および証明書の署名検証時間 [sec]
M' :Entity端末における証明書検証要求の生成および証明書検証結果の署名検証時間 [sec]
M'' :Entity端末におけるCRLを用いた失効確認時間 [sec]
τ :CAの階層 [階層]
α :Entity端末の計算速度に対するVAサーバの計算速度の比 $(0 < \alpha < 1)$

ここで，計算時間を$\tau - 1$倍しているのは，ルートCA証明書は何らかの方法で既に検証済みでありトラストアンカーとしてEntityは信頼済みという仮定を置いているためである．

4.4 有効性確認時間

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．CVSモデル2ではCVSモデル1と同様に，1つのリクエストに複数の項目を入れることができるので，リクエストのサイズは，$\tau D'_{sn} + D'_{sig}$，リクエストの通信時間は$(\tau D'_{sn} + D'_{sig})/s$，となる．

さらに，CVSモデル2では，自CAに属さないEntity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．

$$R'_{CVS2} = \frac{N_v - 1}{N_v} \cdot \frac{(\tau - 1) \cdot (D_{sn} + D_{sig})}{\beta \cdot s} \tag{5}$$

ただし，$\beta(\geq 1)$は，VA-Entity間（モバイル網）の通信速度に対するVA-VA間（バックエンド）の通信速度の倍率である．また，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．

よって1回の認証における有効性確認要求時間R_{CVS2}は下記のように表せる．

$$R_{CVS2} = \left\{ \frac{\tau D'_{sn} + D'_{sig}}{s} + \frac{N_v - 1}{N_v} \cdot \frac{(\tau - 1)(D_{sn} + D_{sig})}{\beta \cdot s} \right\} \frac{1}{T_C} \tag{6}$$

ただし記号の意味は下記である．

D_{sn} :OCSP要求の項目1つあたりのビット数 [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1つあたりのビット数 [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]
s :VA-Entity間(モバイル網)の通信速度 [bit/sec]

4.5 平均検証時間

以上よりCVSモデル2の1回の認証に必要な平均検証時間をT_{CVS2}は下記となる．

$$T_{CVS2} = C_{CVS2} + M_{CVS2} + R_{CVS2} \tag{7}$$

$$= \frac{\frac{k}{N_v} \cdot k \cdot p'^{T_C}_{v\,X\geq 1} \cdot l_{CRL}}{T_C \cdot q' \cdot \beta s}$$
$$+ \quad (r-1)(\alpha M + \alpha M'') + M'$$
$$+ \quad \left\{ \frac{rD'_{sn} + D'_{sig}}{s} \right.$$
$$\left. + \frac{N_v - 1}{N_v} \cdot \frac{(r-1)(D_{sn} + D_{sig})}{\beta \cdot s} \right\} \quad (8)$$

4.6 比較

携帯端末をサーバが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．本パラメータは文献[1]のパラメータ2を基にしているが，携帯端末を検証するモデルを評価するためEntityの数Nと被検証者の数N'を入れ替えた．また，認証局の数はモバイル通信事業者の数になるためkの値を変更した．

表 1: 評価用パラメータ

	パラメータ
Entity(認証者)の数 N[個]	3,000,000
被認証者の数 N'[個]	87,000,000
失効発生頻度 p[回/day]	0.1/365
証明書の有効期間 L[day]	365
完全CRL,δ-CRLの発行間隔 T_C[day]	1
CRLの項目1つあたりサイズ l_{sn}[bit]	72
CRLの項目によらず一定な要素のサイズ l_{sig}[bit]	728
CAの数 k[個]	10
VAの数 N_V[個]	10
OCSP要求の項目1つあたり(証明書ID等)のビット数 D_{sn}[bit]	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
CVS要求の項目1つあたり(証明書等)のビット数 D'_{sn}[bit]	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

図4に$\alpha = 0.5$（VAの処理速度がサービス提供者の処理速度の2倍），$\beta = 1.0$（CA-VA間の通信速度とVA-Entity間の通信速度は同一），通信速度$s = 100M$[bit/sec]のときのOCSPモデル1と2，CVSモデル1と2の平均検証時間を示す．なお，$M' = M$，$M'' = M$，$q = 3{,}000$として計算した．また，OCSPモデル1と2およびCVSモデル1は，文献[2]の式を用いた．図4より，CVS方式1とCVS方式2の平均計算時間の差は極小であることがわかる．

5 まとめと今後の課題

端末の処理速度やモバイル網の通信速度の制約以外の，失効リストを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，性能劣化は極小であることを示した．

今後は，証明書検証要求サイズの縮小や，検証サーバの最適化により性能向上を行い評価する．

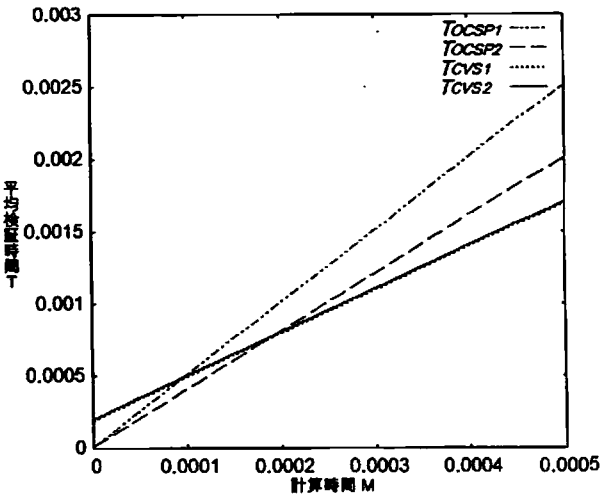

図 4: 通信速度$s = 100M$[bit/sec]のときの平均検証時間

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．

参考文献

[1] 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サーバの開発"，電子情報通信学会技術報告（IT），2005年9月（予定）．

[2] 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，2005年10月（予定）．

[3] 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).

[4] *ITU-T Recommendation X.509 (2000)—ISO/IEC 9594-8:2001: Information Technology - Open Systems Interconnection - The Directory: Public-key and Attribute Certificate Framework*

[5] 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.

[6] 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.

[7] 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．

[8] T.Fressman, R.Housley, A.Malpani, D.Cooper and T.Polk: *Simple Certificate Validation Protocol (SCVP)*, IETF, July. 2005.