OCSPレスポンスキャッシュを利用したX.509認証パス検証の高速化

佐藤　茜†　藤城　孝宏†　熊谷　洋子†　羽根　慎吾†
†株式会社 日立製作所

1. はじめに

日本政府では，電子文書の真正性を保証するための仕組みとして，公開鍵認証基盤(PKI)を採用し，複数の認証局(CA)を構築，運用している．複数のCA間の連携のために，ブリッジ認証局方式を採用しているが，証明書の検証処理が複雑になるという課題がある．このため，著者らは，利用者側の負担軽減と，処理高速化を目的とし，検証処理をサーバ側で行うことを提案してきた．本論文では，従来の証明書やCRLのキャッシュに加え，OCSPレスポンスをキャッシュすることにより，証明書の検証処理を高速化する手法を提案し，さらに，その提案手法の性能評価と安全性に関する検討を行った．

2. 公的認証基盤の概要

日本の公的認証基盤は，以下の様な複数の認証基盤から構成されている．政府認証基盤(GPKI)[1]では，各府省が共用する官職認証局が，処分権者である官職に対し，証明書を発行している．同じく，地方公共団体における組織認証基盤(LGPKI)では，都道府県，市区町村の職責者を対象に証明書を発行している．また，公的個人認証サービスでは，市区町村を窓口として，住民に証明書を発行している．さらに，法人代表者を対象とする商業登記認証局[2]や，電子署名法に基づく特定認証業務の認定を受けた事業者によるCAが運営されている．これらの認証基盤はGPKIのブリッジ認証局と相互認証を行い，各認証基盤との信頼の関係を築いている．

3. 証明書検証方法

電子文書に付与された電子署名の信頼性を確認するためには，検証者は署名者の証明書で電子署名を検証し，さらにその証明書の有効性を検証する必要がある．証明書の検証を行うには，次のような2つの処理を実行する[3]．

(1) 認証パス構築

検証者の信頼するCA(トラストアンカ(TA))の自己署名証明書から，検証対象証明書まで，相互認証証明書等により信頼関係がつながっているかどうかを検索し，一連の証明書群からなる認証パスを構築する．

(2) 認証パス検証

認証パス構築で得られた一連の証明書群について，各証明書の署名検証や，失効確認等を行い，認証パスの有効性を確認する．

図1に，認証パス構築と検証の概要を図示する．

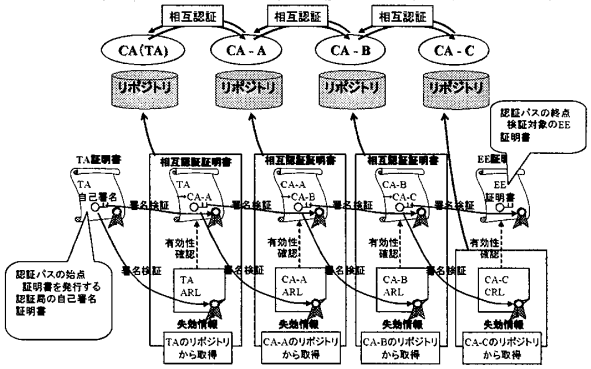

図1　認証パスの構築と検証

4. 証明書検証サーバ

4.1. 証明書検証サーバ概要

証明書の検証処理は，複雑な認証パスの構築や，リポジトリからの証明書・失効情報の取得など，検証者の負担が大きいことが課題である．そのため，証明書の検証を利用者の代理で行い，利用者に対して検証結果を応答する機能を持つ証明書検証サーバモデル(図2)が存在する．

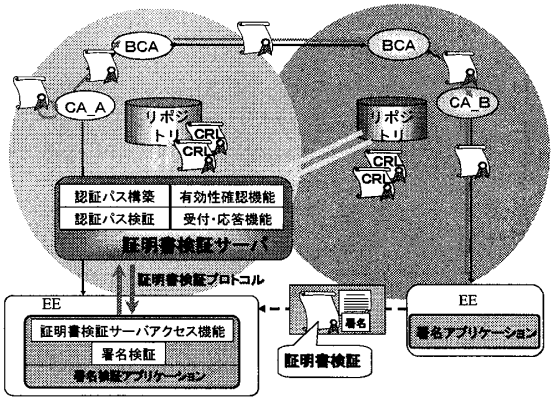

図2 証明書検証サーバモデル

4.2. 証明書検証処理の高速化

著者等は，証明書検証サーバモデルとして，認証パス情報，証明書並びに証明書失効リスト(CRL／ARL)をキャッシュし，再利用することで，ネットワークを通じたファイル取得時間や認証パス構築時間を短縮し，証明書の検証処理を高

Speeding Up X.509 Certification Path Validation Using OCSP Response Cache

Akane SATO†, Takahiro FUJISHIRO†, Yoko KUMAGAI† and Shingo HANE†
†Hitachi, Ltd., Systems Development Laboratory, 292, Yoshida-cho, Totsuka-ku, Yokohama-shi, Kanagawa-ken, 244-0817 JAPAN

速化する手法を提案している[4].

しかしながら，従来の高速化手法では，有効性確認手段として OCSP レスポンダを利用する CA を想定していなかった．そのため，証明書によっては，検証毎に OCSP レスポンダに証明書の有効性を問い合わせる必要があり，検証処理時間を短縮できないという課題があった．そこで，従来の認証パス情報，証明書，CRL/ARL に加えて，OCSP レスポンスのキャッシュを用いた高速化の手法を開発し，これらの効果を測定した．

5. 認証パス検証高速化の性能実験

5.1. 評価環境

図3に性能実験で利用した実験環境を示す．

模擬ブリッジCAと模擬官職CAはCRLで，また，模擬商業登記 CA は OCSP レスポンダで失効情報を提供している．

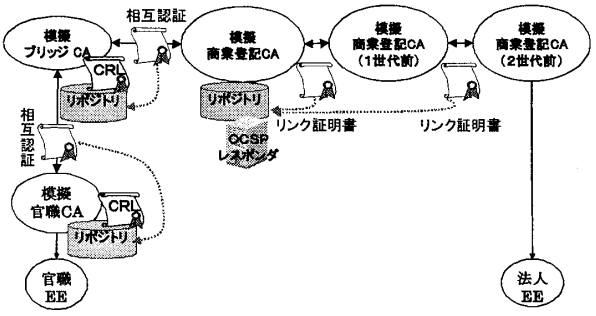

図 3 実験環境

5.2. 評価条件

下記の3つの条件で，官職 CA，商業登記 CA，商業登記 CA(1世代前)及び商業登記 CA(2世代前)を TA として，証明書検証処理の平均応答時間をそれぞれ測定した．検証対象証明書は，商業登記 CA(2世代前)から発行された EE 証明書である．また，全ての条件において認証パス情報，証明書，CRL のキャッシュ機能を有効とした．

条件1：OCSP レスポンスのキャッシュ機能を無効に設定する．

条件2：CA 証明書に対する OCSP レスポンスのキャッシュ機能を有効に設定する．

条件3：EE 証明書及び CA 証明書に対する OCSP レスポンスのキャッシュ機能を有効に設定する．

6. 結果と検討

条件1～3の下での測定結果を表1に示す．

条件1では，TA に設定する商業登記 CA の世代が新しくなるにつれて，リンク証明書に関する OCSP レスポンダへの問い合わせ回数が増えるため，平均応答時間が増加している．一方，条件2では，全ての TA の設定条件において，OCSP レスポンダへの問い合わせ回数は1回(EE 証明書の有効性確認)であるため，平均応答時間に大きな差はない．また，条件3では，証明書検証処理で必要となる全ての情報をキャッシュから取得するため，条件1と比較し，平均応答時間が約30分の1に減少している．

表 1 測定結果

TA の設定	平均応答時間(sec)		
	条件1	条件2	条件3
官職 CA	1.38	0.52	0.06
商業登記 CA	1.34	0.53	0.03
商業登記 CA（1世代前）	0.91	0.48	0.03
商業登記 CA（2世代前）	0.48	0.48	0.02

7. 安全性に関する考察

本来，失効情報を周期的に公開する CRL 方式に対し，OCSP 方式は，利用者からの要求に応じて，適宜，有効性確認情報を提供することを特徴としている．このため，以前に問い合わせた情報を再利用するのは望ましくない．しかしながら，CA の運用ポリシ等により，CRL と同様に有効性確認情報の更新タイミングが特定可能であれば，その更新タイミングで OCSP レスポンスのキャッシュを更新することで，最新の情報で失効確認を行うことができる．そのような場合において，OCSP レスポンスのキャッシュを再利用することに関して，安全性の問題はないと考える．

8. まとめ

多数の CA が連携する認証基盤において，複雑となる証明書検証処理を高速化する手法を提案してきた．従来の手法に加え，OCSP レスポンスをキャッシュすることで，認証パス検証をさらに高速化する手法を研究し，性能実験にて提案した手法の効果を確認した．

参考文献

[1]総務省，”「政府認証基盤(GPKI)について」 http://www.gpki.go.jp/, 2001

[2]法務省，”「商業登記における電子認証制度について」”， http://www.moj.go.jp/ONLINE/CERTIFICATION/, 2000

[3]D. Cooper, et al,"Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, RFC5280, 2008

[4]藤城孝宏,他，”証明書検証サービスの開発”，電子情報通信学会論文誌 D-I Vol.J87-D-I No.8, 2004