証明書検証サーバの提案と
その実用化に向けた研究

平成 23 年度

藤　城　孝　宏

主　論　文　要　旨

報告番号	㊙ 乙 第　　号	氏 名	藤城 孝宏

主 論 文 題 目 :

証明書検証サーバの提案とその実用化に向けた研究

（内容の要旨）

近年，インターネットの爆発的な普及を受けて，電子商取引や，電子政府が実現されてきている．インターネット上でこれらデータ交換を行う際には,データの盗聴，改ざん，成りすましや，また，事後での否認などへの対策が必須である．

これらセキュリティ対策のためには，公開鍵暗号技術に基づく認証基盤の活用が効果的であり，国内外で多くの認証局が構築されてきている．日本政府においても安心･安全な電子政府実現に向けて，その基盤となる認証システムである政府認証基盤(GPKI)や公的個人認証サービスの構築を行っている．

これら公的な認証基盤では，各府省の認証局間や民間の認証局との間での連携を行うために，ブリッジ認証局方式を採用している．しかしながら，ブリッジ認証局方式には，利用者にとって公開鍵証明書の検証処理が複雑になるという問題がある．

この問題の解決のため，本論文では，従来，利用者側で行っていた検証処理をサーバ側で一括して行うことにより，利用者側の負担軽減と，検証処理の高速化が行えることの提案を行っている．

まず，GPKI のようなブリッジ認証方式を採用している認証基盤において，証明書検証を行う際に必要となる認証パスの構築，検証処理を明確化している．ついで，この証明書検証処理を利用者に代行して行う証明書検証サーバに求められる機能要件，セキュリティ要件，また，証明書検証サーバを利用するためのアクセスプロトコルに求められる要件の定義を行っている．

次に，これら要件を満足させるために，認証パス構築，検証機能の設計を行うともに，認証局の公開する証明書や失効情報の取得を効率化するリポジトリキャッシュや，利用者にとって利便性の高い証明書検証のためのアクセスプロトコルの検討を行い，評価実験によりその有効性の検証を行った結果を示している．

さらに，本論文では，電子政府の利用の拡大にともない，増大する証明書検証要求に対応するために行った証明書検証処理をさらに高速化し，証明書検証サーバの実用性を向上する手法に関して提案を行っている．具体的には，リポジトリキャッシュの課題を改善する証明書のハッシュテーブル格納方式，ならびに，構築した認証パス情報を再利用する認証パス情報のキャッシュ機能の提案を行っている．加えて，実験環境ならびに，実環境を利用した性能評価実験を行い，提案した手法の有効性の検証を行っている．

SUMMARY OF Ph.D. DISSERTATION

School Open and Environmental Systems	Student Identification Number	SURNAME, First name FUJISHIRO Takahiro

Title

Study on Concept of Certificate Validation Server and its Practical Implementation

Abstract

In recent years, various online services like electronic commerce service and electronic government service have been provided over the Internet. To use these online services securely, various security countermeasures are required against tapping of transmitted data, unauthorized modification of data, impersonation and repudiation.

It is widely known that an authentication infrastructure based on public key cryptography, which is called as Public Key Infrastructure (PKI), is useful for above purpose. For example, Japanese government has developed Government Public Key Infrastructure (GPKI) for secure and trusted Electronic Government system.

In GPKI, a Bridge Certification Authority model is adopted to make communication between ministry or agency certification authorities and private certification authorities. However, it is well known as the Bridge Certification Authority model has one problem that the public key certificate validation process for the user is complicated.

This thesis proposes a concept of certificate validation server, which constructs and verifies a certification path on behalf of users to reduce users' cost and to accelerate a certification path validation. In addition, functional requirements and security requirements of certificate validation server and its access protocol are proposed.

At next, this thesis describes an implementation of certificate validation server which consists from a certification path construction function, a certification path validation function, a repository cache function, which retrieves certification authority's certificates and/or certificate revocation information. And also, a specification of certificate validation server access protocol is proposed.

Moreover, methods of faster certification path validation are proposed to support huge number of certificate validation requests. To be more concrete, it proposes a certificate cache method using hash table and a constructed certification path information reuse method.

In addition, this thesis evaluates an implementation of proposed certificate validation server from the viewpoint of practical use.