属性証明書検証サーバの開発

笈川　光浩† 洲崎　誠一† 仲小路　博史† 宮崎　豊†
株式会社　日立製作所‡

1　はじめに

近年、ネットワークを介して通信相手を特定する際に公開鍵暗号基盤(PKI)を用いる方法が普及しつつある。PKI で用いる公開鍵証明書は主に通信相手の本人性を確認することを目的としている。一方、通信相手が特定の資格や権限を持っていることを確認するために属性証明書[1][2]の利用が提案されている。しかし、属性証明書を使用して資格や権限を確認する場合、その属性証明書に結びつけられた公開鍵証明書の認証パスも併せて検証を行うことが必要となるため、非常に手間がかかる。

本研究では、属性証明書の検証を行う際に、属性証明書の検証者自身が、認証パスの構築・検証および有効性確認といった検証処理を行うのではなく、それらの処理を属性証明書検証サーバで容易かつ高速に行う方式を開発した。

2　従来の属性証明書検証方法

属性証明書とは、属性証明書保有者の公開鍵証明書へのポインタ、属性認証局名、有効期間、属性（属性証明書保有者の資格や権限）等の情報に対して、属性認証局が電子署名を施した電子データである。

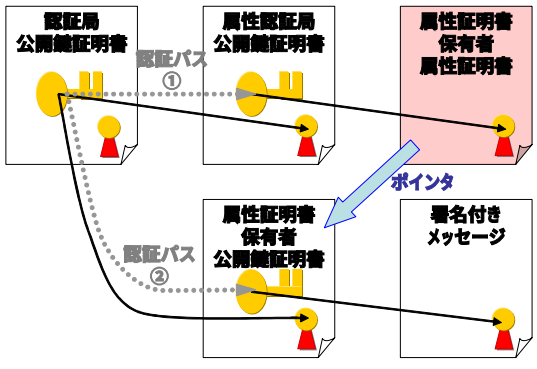

図１　属性証明書を含む認証パスのモデル例

Development of Attribute Certificate Validation Server
† Mitsuhiro Oikawa, Seiichi Susaki, Hirofumi Nakakouji, Yutaka Miyazaki
‡ Hitachi, Ltd.

そのため、検証者が属性証明書の内容の正当性を確認するためには、以下のような 3 つの手順を合わせて行うことが必要となる.

(1) 属性証明書の電子署名の検証

検証者は、まず属性証明書に施された電子署名を、属性認証局の公開鍵証明書を用いて検証し、さらに、検証者が信頼点としている公開鍵証明書から属性認証局の公開鍵証明書までの認証パスを検証する。図１に、検証に必要な認証パスの例を示す。

(2) 正当な属性証明書保有者であることの検証

検証者は、属性証明書保有者の電子署名も併せて取得し、当該電子署名を、属性証明書に関連づけられている属性証明書保有者の公開鍵証明書で検証する。さらに、検証者が信頼点としている公開鍵証明書から属性証明書保有者の公開鍵証明書までの認証パスを検証する。

(3) 属性証明書の有効性の検証

属性証明書に失効の状態がある場合、検証者は、属性証明書が失効されていないことを確認する。

以上のように、属性証明書を検証するためには、属性認証局の公開鍵証明書と属性証明書保有者の公開鍵証明書という２つの認証パスの検証とその有効性確認を行う必要がある。

しかしながら、例えばモバイル端末のようなリソースの限られた装置で、上記に示したような属性証明書の検証機能を実装しようとすると、処理に膨大な時間を要したり、実装自体が困難であったりすることが考えられる。我々は、そのようなリソースの限られた装置においても、属性証明書の検証を容易かつ高速に行うための方式を開発した。

3　属性証明書検証サーバによる検証方法

我々は、属性証明書の検証を代理で行うためのサーバ、すなわち、属性証明書検証サーバ(Attribute Certificate Validation Server)をネットワーク上に設置することで、属性証明書の検証を容易かつ高速に検証する方式を実現した。検証者が、属性証明書検証サーバに検証要求を行うと、属性証明書検証サーバが検証に必

要な情報を一括して収集・検証し、属性証明書検証者に属性証明書のステータスを回答する。本システム全体の構成例を図２に示す。

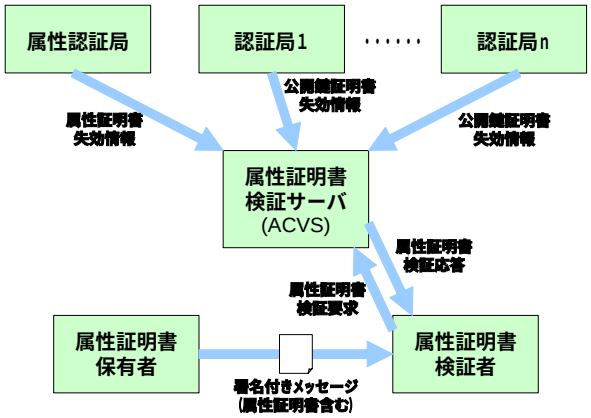

図２　属性証明書検証サーバによる属性証明書検証方式

具体的には、属性証明書検証者側の端末には、以下の(a)～(c)の機能を実装した。

(a) 署名付きメッセージの署名検証
(b) 属性証明書検証要求[3]の生成および送信
(c) 属性証明書検証応答[3]の受信および検証

また、属性証明書検証サーバ側には、以下の(d)～(j)の機能を実装した。

(d) 属性証明書検証要求の受信および解析
(e) 属性証明書の電子署名の検証
(f) 信頼点から属性認証局までの認証パスの構築、検証、および、有効性確認
(g) 信頼点から属性証明書に記載されている属性証明書保有者の公開鍵証明書のポインタが示す公開鍵証明書までの認証パスの構築、検証、および、有効性確認
(h) 権限パスの確認
(i) 属性証明書の有効性確認
(j) 属性証明書検証応答の生成および送信

属性証明書検証サーバには、上記機能に加えて，認証パスの構築時に取得した公開鍵証明書、有効性確認時に取得した失効情報、および、認証パスの検証結果を、それらの情報が有効である間、キャッシュとして保存する機能を設けた。これにより，認証パスの再利用を可能とし、高速な検証を実現した。

４　考察

属性証明書検証サーバを利用することで、検証者は、属性証明書保有者から送信されてきた署名文書の署名検証を行ったのち、属性証明書検証サーバに対して属性証明書の検証を要求し、その応答を検証するだけでよいため、検証者側での複雑な処理を省略することができる。また、属性認証局および属性証明書保有者の公開鍵証明書に関する２つの認証パスは重複する部分が多いため、キャッシュ機能を持たせることにより大幅にパス構築に要する時間を短縮することができる。

このように、属性証明書の検証に関わる複雑な処理を属性証明書検証サーバに代行させることにより、モバイル機器のような低リソースの装置においても属性証明書利用システムを容易に実装可能となる。

５　おわりに

属性証明書検証サーバを利用することにより、属性証明書の検証を容易且つ高速に検証する方式を開発した。

今後の課題としては、属性証明書検証サーバを運用する属性検証局（Attribute Validation Authority）のセキュアな運用方法を確立するとともに、現在、IETF(Internet Engineering Task Force)で議論されている検証プロトコルに関する標準化動向を鑑み、それら標準プロトコルを属性証明書検証サーバに実装していく予定である。

謝辞

本研究の一部は、通信・放送機構の委託研究「属性認証を用いたサービスの相互接続技術に関する研究開発」による。

参考文献

[1] ITU-T Recommendation X.509 (2000) | ISO/IEC 9594-8:2001, Information technology – Open Systems Interconnection – The Directory: Public-Key and Attribute Certificate Frameworks.
[2] Farrell, S. and R. Housley. April, 2002. "An Internet Attribute Certificate Profile for Authorization", RFC3281
[3] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams. “Online Certificate Status Protocol – OCSP”, RFC 2560